

Chapter 1

Domain 1.0: Threat and Vulnerability Management

EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ 1.1 Explain the importance of threat data and intelligence.
 - Intelligence sources
 - Confidence levels
 - Indicator management
 - Threat classification
 - Threat actors
 - Intelligence cycle
 - Commodity malware
 - Information sharing and analysis communities
- ✓ 1.2 Given a scenario, utilize threat intelligence to support organizational security.
 - Attack frameworks
 - Threat research
 - Threat modeling methodologies
 - Threat intelligence sharing with supported functions
- ✓ 1.3 Given a scenario, perform vulnerability management activities.
 - Vulnerability identification
 - Validation
 - Remediation/mitigation
 - Scanning parameters and criteria
 - Inhibitors to remediation
- ✓ 1.4 Given a scenario, analyze the output from common vulnerability assessment tools.
 - Web application scanner



- Infrastructure vulnerability scanner
- Software assessment tools and techniques
- Enumeration
- Wireless assessment tools
- Cloud infrastructure assessment tools

✓ **1.5 Explain the threats and vulnerabilities associated with specialized technology.**

- Mobile
- Internet of Things (IoT)
- Embedded
- Real-time operating system (RTOS)
- System-on-Chip (SoC)
- Field programmable gate array (FPGA)
- Physical access control
- Building automation systems
- Vehicles and drones
- Workflow and process automation systems
- Industrial control systems (ICS)
- Supervisory control and data acquisition (SCADA)

✓ **1.6 Explain the threats and vulnerabilities associated with operating in the cloud.**

- Cloud service models
- Cloud deployment models
- Function as a service (FaaS)/serverless architecture
- Infrastructure as code (IaC)
- Insecure application programming interface (API)
- Improper key management
- Unprotected storage
- Logging and monitoring

✓ **1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities.**

- Attack types
- Vulnerabilities

1. Olivia is considering potential sources for threat intelligence information that she might incorporate into her security program. Which one of the following sources is most likely to be available without a subscription fee?
 - A. Vulnerability feeds
 - B. Open source
 - C. Closed source
 - D. Proprietary
2. During the reconnaissance stage of a penetration test, Cynthia needs to gather information about the target organization's network infrastructure without causing an IPS to alert the target to her information gathering. Which of the following is her best option?
 - A. Perform a DNS brute-force attack.
 - B. Use an nmap ping sweep.
 - C. Perform a DNS zone transfer.
 - D. Use an nmap stealth scan.
3. Roger is evaluating threat intelligence information sources and finds that one source results in quite a few false positive alerts. This lowers his confidence level in the source. What criteria for intelligence is not being met by this source?
 - A. Timeliness
 - B. Expense
 - C. Relevance
 - D. Accuracy
4. What markup language provides a standard mechanism for describing attack patterns, malware, threat actors, and tools?
 - A. STIX
 - B. TAXII
 - C. XML
 - D. OpenIOC
5. A port scan of a remote system shows that port 3306 is open on a remote database server. What database is the server most likely running?
 - A. Oracle
 - B. Postgres
 - C. MySQL
 - D. Microsoft SQL
6. Brad is working on a threat classification exercise, analyzing known threats and assessing the possibility of unknown threats. Which one of the following threat actors is most likely to be associated with an advanced persistent threat (APT)?
 - A. Hacktivist
 - B. Nation-state

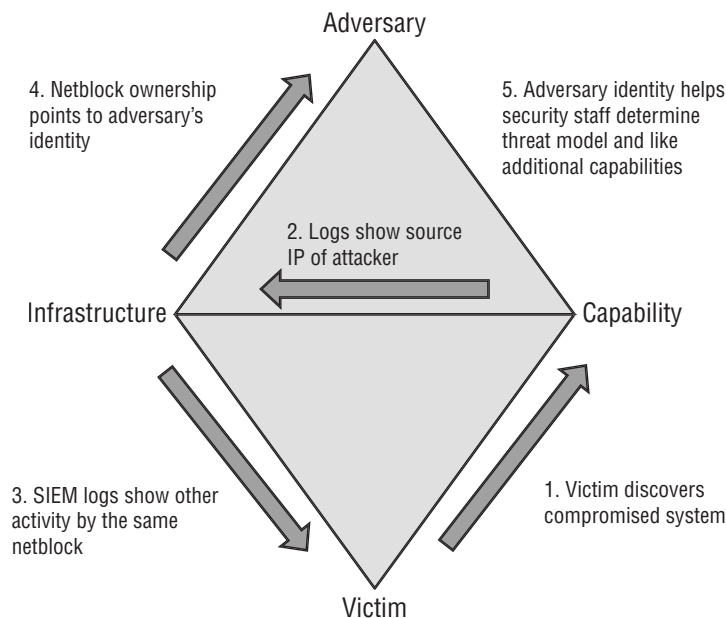
- C. Insider
 - D. Organized crime
7. During a port scan of her network, Cynthia discovers a workstation that shows the following ports open. What should her next action be?

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-26 19:25 EDT
Nmap scan report for deptsrv (192.168.2.22)
Host is up (0.0058s latency).
Not shown: 65524 closed ports
PORT      STATE      SERVICE
80/tcp    open      http
135/tcp   open      msrpc
139/tcp   open      netbios-ssn
445/tcp   open      microsoft-ds
3389/tcp  open      ms-wbt-server
7680/tcp  open      unknown
49677/tcp open      unknown
MAC Address: AD:5F:F4:7B:4B:7D (Intel Corporation)

Nmap done: 1 IP address (1 host up) scanned in 121.29 seconds
```

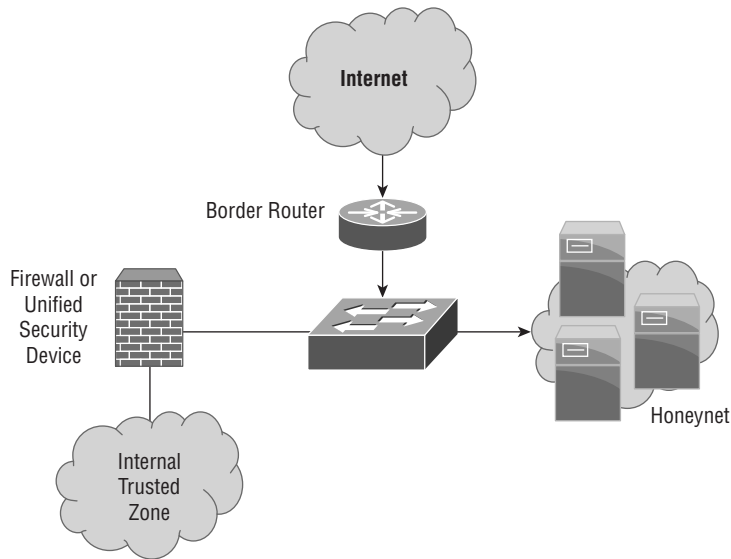
- A. Determine the reason for the ports being open.
 - B. Investigate the potentially compromised workstation.
 - C. Run a vulnerability scan to identify vulnerable services.
 - D. Reenable the workstation's local host firewall.
8. Charles is working with leaders of his organization to determine the types of information that should be gathered in his new threat intelligence program. In what phase of the intelligence cycle is he participating?
- A. Dissemination
 - B. Feedback
 - C. Analysis
 - D. Requirements
9. As Charles develops his threat intelligence program, he creates and shares threat reports with relevant technologists and leaders. What phase of the intelligence cycle is now occurring?
- A. Dissemination
 - B. Feedback
 - C. Collection
 - D. Requirements
10. What term is used to describe the groups of related organizations who pool resources to share cybersecurity threat information and analyses?
- A. SOC
 - B. ISAC

- C. CERT
D. CIRT
11. Which one of the following threats is the most pervasive in modern computing environments?
- A. Zero-day attacks
B. Advanced persistent threats
C. Commodity malware
D. Insider threats
12. Singh incorporated the Cisco Talos tool into his organization's threat intelligence program. He uses it to automatically look up information about the past activity of IP addresses sending email to his mail servers. What term best describes this intelligence source?
- A. Open source
B. Behavioral
C. Reputational
D. Indicator of compromise
13. Consider the threat modeling analysis shown here. What attack framework was used to develop this analysis?



- A. ATT&CK
B. Cyber Kill Chain

- C. STRIDE
 - D. Diamond
14. Jamal is assessing the risk to his organization from their planned use of AWS Lambda, a serverless computing service that allows developers to write code and execute functions directly on the cloud platform. What cloud tier best describes this service?
- A. SaaS
 - B. PaaS
 - C. IaaS
 - D. FaaS
15. Lauren's honeynet, shown here, is configured to use a segment of unused network space that has no legitimate servers in it. What type of threats is this design particularly useful for detecting?



- A. Zero-day attacks
 - B. SQL injection
 - C. Network scans
 - D. DDoS attacks
16. Nara is concerned about the risk of attackers conducting a brute-force attack against her organization. Which one of the following factors is Nara most likely to be able to control?
- A. Attack vector
 - B. Adversary capability

- C. Likelihood
- D. Total attack surface

17. Fred believes that the malware he is tracking uses a fast flux DNS network, which associates many IP addresses with a single fully qualified domain name as well as using multiple download hosts. How many distinct hosts should he review based on the NetFlow shown here?

Date flow start	Duration	Proto	Src	IP Addr:Port	Dst IP
Addr:Port	Packets	Bytes	Flows		
2020-07-11	14:39:30.606	0.448	TCP	192.168.2.1:1451-	
>10.2.3.1:443	10	1510	1		
2020-07-11	14:39:30.826	0.448	TCP	10.2.3.1:443-	
>192.168.2.1:1451	7	360	1		
2020-07-11	14:45:32.495	18.492	TCP	10.6.2.4:443-	
>192.168.2.1:1496	5	1107	1		
2020-07-11	14:45:32.255	18.888	TCP	192.168.2.1:1496-	
>10.6.2.4:443	11	1840	1		
2020-07-11	14:46:54.983	0.000	TCP	192.168.2.1:1496-	
>10.6.2.4:443	1	49	1		
2020-07-11	16:45:34.764	0.362	TCP	10.6.2.4:443-	
>192.168.2.1:4292	4	1392	1		
2020-07-11	16:45:37.516	0.676	TCP	192.168.2.1:4292-	
>10.6.2.4:443	4	462	1		
2020-07-11	16:46:38.028	0.000	TCP	192.168.2.1:4292-	
>10.6.2.4:443	2	89	1		
2020-07-11	14:45:23.811	0.454	TCP	192.168.2.1:1515-	
>10.6.2.5:443	4	263	1		
2020-07-11	14:45:28.879	1.638	TCP	192.168.2.1:1505-	
>10.6.2.5:443	18	2932	1		
2020-07-11	14:45:29.087	2.288	TCP	10.6.2.5:443-	
>192.168.2.1:1505	37	48125	1		
2020-07-11	14:45:54.027	0.224	TCP	10.6.2.5:443-	
>192.168.2.1:1515	2	1256	1		
2020-07-11	14:45:58.551	4.328	TCP	192.168.2.1:1525-	
>10.6.2.5:443	10	648	1		
2020-07-11	14:45:58.759	0.920	TCP	10.6.2.5:443-	
>192.168.2.1:1525	12	15792	1		
2020-07-11	14:46:32.227	14.796	TCP	192.168.2.1:1525-	
>10.8.2.5:443	31	1700	1		
2020-07-11	14:46:52.983	0.000	TCP	192.168.2.1:1505-	
>10.8.2.5:443	1	40	1		

- A. 1
- B. 3
- C. 4
- D. 5




18. Which one of the following functions is not a common recipient of threat intelligence information?
- A. Legal counsel
 - B. Risk management
 - C. Security engineering
 - D. Detection and monitoring
19. Alfonzo is an IT professional at a Portuguese university who is creating a cloud environment for use only by other Portuguese universities. What type of cloud deployment model is he using?
- A. Public cloud
 - B. Private cloud
 - C. Hybrid cloud
 - D. Community cloud
20. During a network reconnaissance exercise, Chris gains access to a PC located in a secure network. If Chris wants to locate database and web servers that the company uses, what command-line tool can he use to gather information about other systems on the local network without installing additional tools or sending additional traffic?
- A. ping
 - B. traceroute
 - C. nmap
 - D. netstat
21. Kaiden's organization uses the AWS public cloud environment. He uses the CloudFormation tool to write scripts that create the cloud resources used by his organization. What type of service is CloudFormation?
- A. SaaS
 - B. IAC
 - C. FaaS
 - D. API
22. What is the default nmap scan type when nmap is not provided with a scan type flag?
- A. A TCP FIN scan
 - B. A TCP connect scan
 - C. A TCP SYN scan
 - D. A UDP scan
23. Isaac wants to grab the banner from a remote web server using commonly available tools. Which of the following tools cannot be used to grab the banner from the remote host?
- A. Netcat
 - B. Telnet

- C. Wget
- D. FTP
24. Lakshman wants to limit what potential attackers can gather during passive or semipassive reconnaissance activities. Which of the following actions will typically reduce his organization's footprint the most?
- A. Limit information available via the organizational website without authentication.
 - B. Use a secure domain registration.
 - C. Limit technology references in job postings.
 - D. Purge all document metadata before posting.
25. Cassandra's nmap scan of an open wireless network (192.168.10/24) shows the following host at IP address 192.168.1.1. Which of the following is most likely to be the type of system at that IP address based on the scan results shown?

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	Dropbear sshd 2016.74 (protocol 2.0)
53/tcp	open	domain	dnsmasq 2.76
80/tcp	open	http	Acme milli_httpd 2.0 (ASUS RT-AC-series router)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
515/tcp	open	tcpwrapped	
1723/tcp	open	pptp	linux (Firmware: 1)
8200/tcp	open	upnp	MiniDLNA 1.1.5 (OS: 378.xx; DLNADOC 1.50; UPnP 1.0)
8443/tcp	open	ssl/http	Acme milli_httpd 2.0 (ASUS RT-AC-series router)
9100/tcp	open	jetdirect?	
9998/tcp	open	tcpwrapped	
Device type: bridge general purpose			

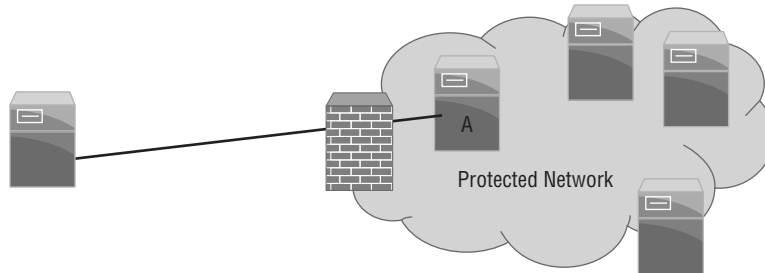
- A. A virtual machine
 - B. A wireless router
 - C. A broadband router
 - D. A print server
26. Several organizations recently experienced security incidents when their AWS secret keys were published in public GitHub repositories. What is the most significant threat that could arise from this improper key management?
- A. Total loss of confidentiality
 - B. Total loss of integrity
 - C. Total loss of availability
 - D. Total loss of confidentiality, integrity, and availability
27. Latisha has local access to a Windows workstation and wants to gather information about the organization that it belongs to. What type of information can she gain if she executes the command `nbtstat -c`?
- A. MAC addresses and IP addresses of local systems
 - B. NetBIOS name-to-IP address mappings

- C. A list of all NetBIOS systems that the host is connected to
 - D. NetBIOS MAC-to-IP address mappings
28. Tracy believes that a historic version of her target's website may contain data she needs for her reconnaissance. What tool can she use to review snapshots of the website from multiple points in time?
- A. Time Machine
 - B. Morlock
 - C. Wayback Machine
 - D. Her target's web cache
29. After Kristen received a copy of an nmap scan run by a penetration tester that her company hired, she knows that the tester used the `-O` flag. What type of information should she expect to see included in the output other than open ports?
- A. OCMP status
 - B. Other ports
 - C. Objective port assessment data in verbose mode
 - D. Operating system and Common Platform Enumeration (CPE) data
30. Andrea wants to conduct a passive footprinting exercise against a target company. Which of the following techniques is not suited to a passive footprinting process?
- A. WHOIS lookups
 - B. Banner grabbing
 - C. BGP looking glass usage
 - D. Registrar checks
31. While gathering reconnaissance data for a penetration test, Charlene uses the MXToolbox MX Lookup tool. What can she determine from the response to her query shown here?

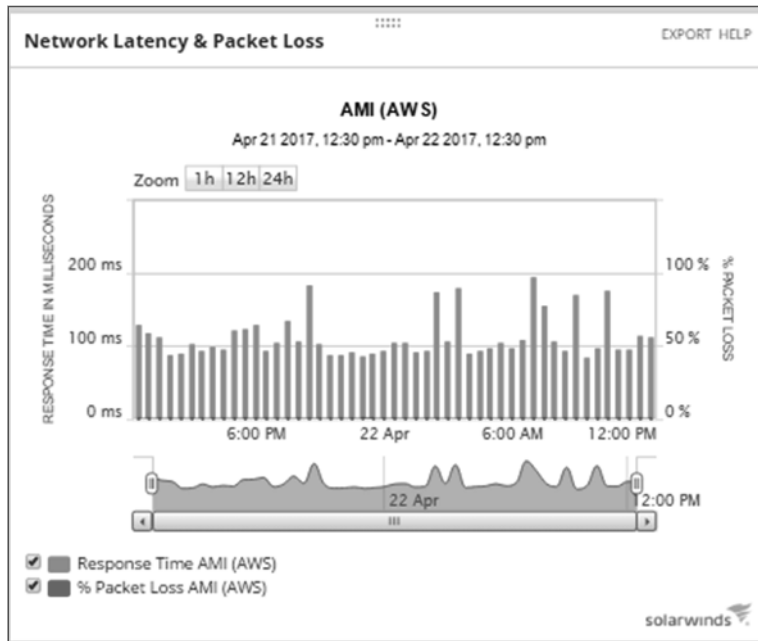
Pref	Hostname	IP Address	TTL		
10	cluster1.us.messagelabs.com	216.82.241.131  New York US MessageLabs Inc. (AS20282)	15 min	Blacklist Check	SMTP Test
20	cluster1a.us.messagelabs.com	216.82.251.230  New York US MessageLabs Inc. (AS20282)	15 min	Blacklist Check	SMTP Test
Test			Result		
	DNS Record Published		DNS Record found		
Your email service provider is "MessageLabs" Need Bulk Email Provider Data?					

- A. The mail servers are blacklisted.
- B. The mail servers have failed an SMTP test.
- C. The mail servers are clustered.
- D. There are two MX hosts listed in DNS.

32. Alex wants to scan a protected network and has gained access to a system that can communicate to both his scanning system and the internal network, as shown in the image here. What type of nmap scan should Alex conduct to leverage this host if he cannot install nmap on system A?



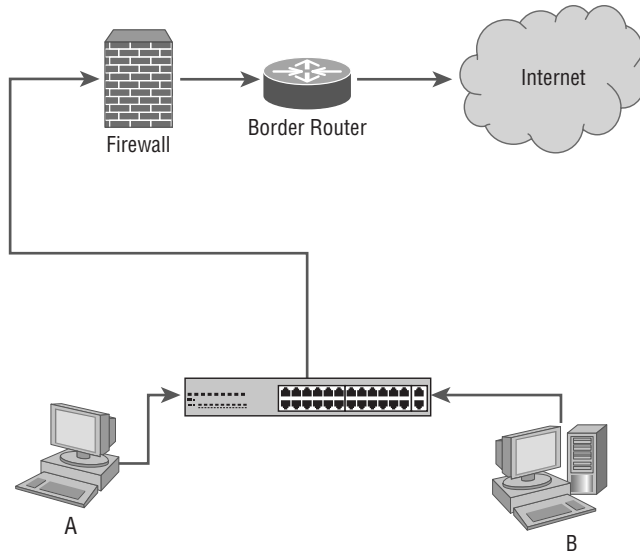
- A. A reflection scan
B. A proxy scan
C. A randomized host scan
D. A ping-through scan
33. As a member of a blue team, Lukas observed the following behavior during an external penetration test. What should he report to his managers at the conclusion of the test?



- A. A significant increase in latency
 - B. A significant increase in packet loss
 - C. Latency and packet loss both increased.
 - D. No significant issues were observed.
34. As part of an organizationwide red team exercise, Frank is able to use a known vulnerability to compromise an Apache web server. Once he has gained access, what should his next step be if he wants to use the system to pivot to protected systems behind the DMZ that the web server resides in?
- A. Vulnerability scanning
 - B. Privilege escalation
 - C. Patching
 - D. Installing additional tools
35. Maddox is conducting an inventory of access permissions on cloud-based object buckets, such as those provided by the AWS S3 service. What threat is he seeking to mitigate?
- A. Insecure APIs
 - B. Improper key management
 - C. Unprotected storage
 - D. Insufficient logging and monitoring
36. Alex has been asked to assess the likelihood of reconnaissance activities against her organization (a small, regional business). Her first assignment is to determine the likelihood of port scans against systems in her organization's DMZ. How should she rate the likelihood of this occurring?
- A. Low
 - B. Medium
 - C. High
 - D. There is not enough information for Alex to provide a rating.
37. Lucy recently detected a cross-site scripting vulnerability in her organization's web server. The organization operates a support forum where users can enter HTML tags and the resulting code is displayed to other site visitors. What type of cross-site scripting vulnerability did Lucy discover?
- A. Persistent
 - B. Reflected
 - C. DOM-based
 - D. Blind

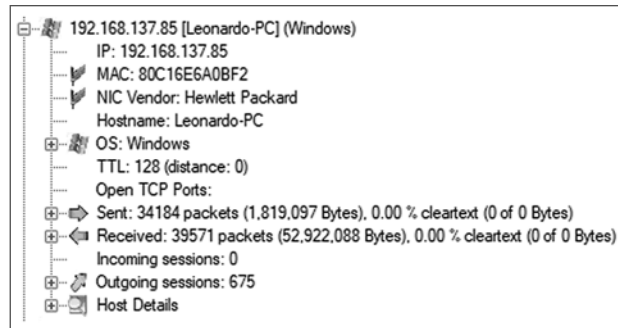
38. Which one of the following tools is capable of handcrafting TCP packets for use in an attack?
- A. Arachni
 - B. Hping
 - C. Responder
 - D. Hashcat
39. Which one of the following IoT components contains hardware that can be dynamically reprogrammed by the end user?
- A. RTOS
 - B. SoC
 - C. FPGA
 - D. MODBUS
40. Florian discovered a vulnerability in a proprietary application developed by his organization. The application performs memory management using the `malloc()` function and one area of memory allocated in this manner has an overflow vulnerability. What term best describes this overflow?
- A. Buffer overflow
 - B. Stack overflow
 - C. Integer overflow
 - D. Heap overflow
41. The company that Maria works for is making significant investments in infrastructure-as-a-service hosting to replace its traditional datacenter. Members of her organization's management have Maria's concerns about data remanence when Lauren's team moves from one virtual host to another in their cloud service provider's environment. What should she instruct her team to do to avoid this concern?
- A. Zero-wipe drives before moving systems.
 - B. Use full-disk encryption.
 - C. Use data masking.
 - D. Span multiple virtual disks to fragment data.

42. Lucca wants to prevent workstations on his network from attacking each other. If Lucca's corporate network looks like the network shown here, what technology should he select to prevent laptop A from being able to attack workstation B?



- A. An IPS
 - B. An IDS
 - C. An HIPS
 - D. An HIDS
43. Geoff is reviewing logs and sees a large number of attempts to authenticate to his VPN server using many different username and password combinations. The same usernames are attempted several hundred times before moving on to the next one. What type of attack is most likely taking place?
- A. Credential stuffing
 - B. Password spraying
 - C. Brute-force
 - D. Rainbow table
44. The company that Dan works for has recently migrated to an SaaS provider for its enterprise resource planning (ERP) software. In its traditional on-site ERP environment, Dan conducted regular port scans to help with security validation for the systems. What will Dan most likely have to do in this new environment?
- A. Use a different scanning tool.
 - B. Rely on vendor testing and audits.
 - C. Engage a third-party tester.
 - D. Use a VPN to scan inside the vendor's security perimeter.

45. Lakshman uses Network Miner to review packet captures from his reconnaissance of a target organization. One system displayed the information shown here. What information has Network Miner used to determine that the PC is a Hewlett-Packard device?



- A. The MAC address
- B. The OS flags
- C. The system's banner
- D. The IP address
46. Kaiden is configuring a SIEM service in his IaaS cloud environment that will receive all of the log entries generated by other devices in that environment. Which one of the following risks is greatest with this approach in the event of a DoS attack or other outage?
- A. Inability to access logs
- B. Insufficient logging
- C. Insufficient monitoring
- D. Insecure API
47. Which one of the following languages is least susceptible to an injection attack?
- A. HTML
- B. SQL
- C. STIX
- D. XML
48. Which one of the following types of malware would be most useful in a privilege escalation attack?
- A. Rootkit
- B. Worm
- C. Virus
- D. RAT

49. Ricky discovered a vulnerability in an application where privileges are checked at the beginning of a series of steps, may be revoked during those steps, and then are not checked before new uses of them later in the sequence. What type of vulnerability did he discover?
- A. Improper error handling
 - B. Race condition
 - C. Dereferencing
 - D. Sensitive data exposure
50. Matthew is analyzing some code written in the C programming language and discovers that it is using the functions listed here. Which of these functions poses the greatest security vulnerability?
- A. `strcpy()`
 - B. `main()`
 - C. `printf()`
 - D. `scanf()`
51. Abdul is conducting a security audit of a multicloud computing environment that incorporates resources from AWS and Microsoft Azure. Which one of the following tools will be most useful to him?
- A. ScoutSuite
 - B. Pacu
 - C. Prowler
 - D. CloudSploit
52. Jake is performing a vulnerability assessment and comes across a CAN bus specification. What type of environment is most likely to include a CAN bus?
- A. Physical access control system
 - B. Building automation system
 - C. Vehicle control system
 - D. Workflow and process automation system
53. Darcy is conducting a test of a wireless network using the Reaver tool. What technology does Reaver specifically target?
- A. WPA
 - B. WPA2
 - C. WPS
 - D. WEP

54. Azra believes that one of her users may be taking malicious action on the systems she has access to. When she walks past her user's desktop, she sees the following command on the screen:

```
user12@workstation:/home/user12# ./john -wordfile:/home/user12/mylist.txt
-format:lm hash.txt
```

What is the user attempting to do?

- A. They are attempting to hash a file.
 - B. They are attempting to crack hashed passwords.
 - C. They are attempting to crack encrypted passwords.
 - D. They are attempting a pass-the-hash attack.
55. nmap provides a standardized way to name hardware and software that it detects. What is this called?
- A. CVE
 - B. HardwareEnum
 - C. CPE
 - D. GearScript
56. Lakshman wants to detect port scans using syslog so that he can collect and report on the information using his SIEM. If he is using a default CentOS system, what should he do?
- A. Search for use of privileged ports in sequential order.
 - B. Search for connections to ports in the /var/syslog directory.
 - C. Log all kernel messages to detect scans.
 - D. Install additional tools that can detect scans and send the logs to syslog.
57. Greg is concerned about the use of DDoS attack tools against his organization, so he purchased a mitigation service from his ISP. What portion of the threat model did Greg reduce?
- A. Likelihood
 - B. Total attack surface
 - C. Impact
 - D. Adversary capability
58. Lucas believes that an attacker has successfully compromised his web server. Using the following output of ps, identify the process ID he should focus on.

```
root      507  0.0  0.1 258268 3288 ?        Ssl  15:52  0:00 /usr/sbin/
rsyslogd -n
message+  508  0.0  0.2  44176  5160 ?        Ss   15:52  0:00 /usr/bin/
dbusdaemon --system --address=systemd: --nofork --nopidfile --systemd-activa
root      523  0.0  0.3 281092 6312 ?        Ssl  15:52  0:00 /usr/lib/
accountsservice/accounts-daemon
root      524  0.0  0.7 389760 15956 ?        Ssl  15:52  0:00 /usr/sbin/
NetworkManager --no-daemon
```

```

root      527  0.0  0.1  28432  2992 ?      Ss   15:52  0:00 /lib/systemd/
systemd-logind
apache    714  0.0  0.1  27416  2748 ?      Ss   15:52  0:00 /www/temp/
webmin
root      617  0.0  0.1  19312  2056 ?      Ss   15:52  0:00 /usr/sbin/
irqbalance --pid=/var/run/irqbalance.pid
root      644  0.0  0.1  245472  2444 ?      Sl   15:52  0:01 /usr/sbin/
VBoxService
root      653  0.0  0.0  12828  1848 tty1    Ss+  15:52  0:00 /sbin/agetty
--noclear tty1 linux
root      661  0.0  0.3  285428  8088 ?      Ssl  15:52  0:00 /usr/lib/
policykit-1/polkitd --no-debug
root      663  0.0  0.3  364752  7600 ?      Ssl  15:52  0:00 /usr/sbin/gdm3
root      846  0.0  0.5  285816 10884 ?      Ssl  15:53  0:00 /usr/lib/
upower/upowerd
root      867  0.0  0.3  235180  7272 ?      Sl   15:53  0:00 gdm-session-
worker [pam/gdm-launch-environment]
Debian+  877  0.0  0.2  46892  4816 ?      Ss   15:53  0:00 /lib/systemd/
systemd --user
Debian+  878  0.0  0.0  62672  1596 ?      S    15:53  0:00 (sd-pam)

```

- A. 508
 - B. 617
 - C. 846
 - D. 714
59. Geoff is responsible for hardening systems on his network and discovers that a number of network appliances have exposed services, including telnet, FTP, and web servers. What is his best option to secure these systems?
- A. Enable host firewalls.
 - B. Install patches for those services.
 - C. Turn off the services for each appliance.
 - D. Place a network firewall between the devices and the rest of the network.
60. While conducting reconnaissance of his own organization, Ian discovers that multiple certificates are self-signed. What issue should he report to his management?
- A. Self-signed certificates do not provide secure encryption for site visitors.
 - B. Self-signed certificates can be revoked only by the original creator.
 - C. Self-signed certificates will cause warnings or error messages.
 - D. None of the above.

61. During the reconnaissance stage of a penetration test, Fred calls a number of staff at the target organization. Using a script he prepared, Fred introduces himself as part of the support team for their recently installed software and asks for information about the software and its configuration. What is this technique called?
- A. Pretexting
 - B. OSINT
 - C. A tag-out
 - D. Profiling
62. Carrie needs to lock down a Windows workstation that has recently been scanned using nmap with the results shown here. She knows that the workstation needs to access websites and that the system is part of a Windows domain. What ports should she allow through the system's firewall for externally initiated connections?

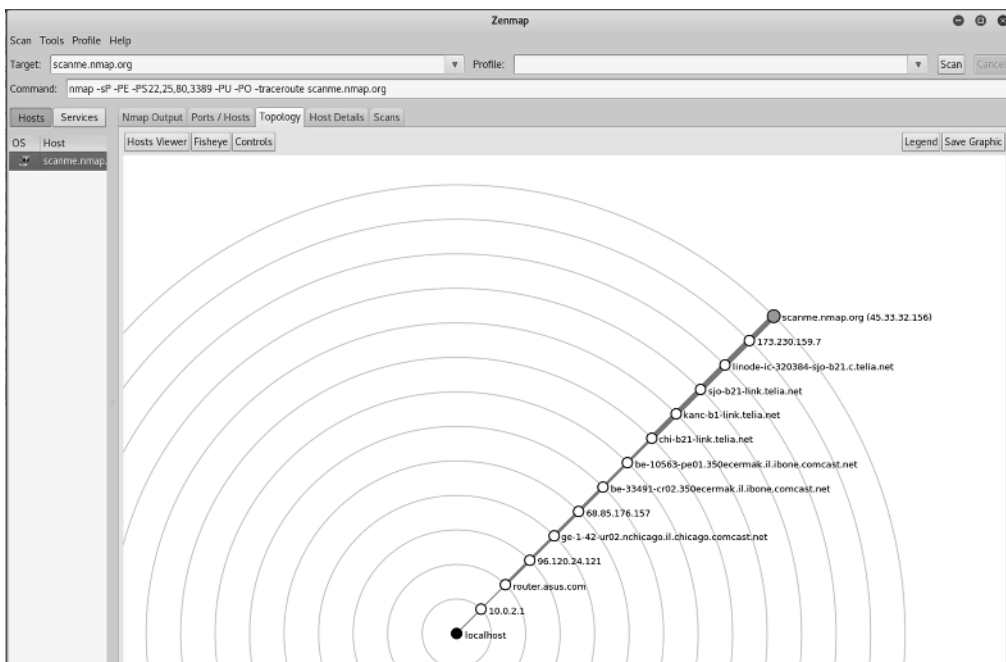
```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-25 21:08 EDT
Nmap scan report for dynamo (192.168.1.14)
Host is up (0.00023s latency)
Not shown: 65524 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
7680/tcp  open  unknown
22350/tcp open  CodeMeter
49677/tcp open  unknown
MAC Address: BC:5F:F4:7B:4B:7D (ASRock Incorporation)

Nmap done: 1 IP address (1 host up) scanned in 105.78 seconds
```

- A. 80, 135, 139, and 445
 - B. 80, 445, and 3389
 - C. 135, 139, and 445
 - D. No ports should be open.
63. Adam's port scan returns results on six TCP ports: 22, 80, 443, 515, 631, and 9100. If Adam needs to guess what type of device this is based on these ports, what is his best guess?
- A. A web server
 - B. An FTP server
 - C. A printer
 - D. A proxy server

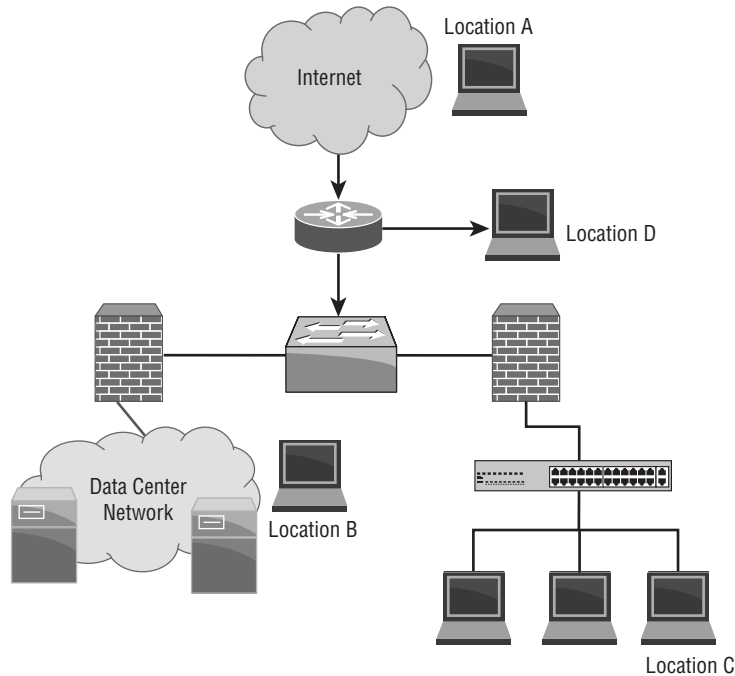
- 64.** In his role as the SOC operator, Manish regularly scans a variety of servers in his organization. After two months of reporting multiple vulnerabilities on a Windows file server, Manish recently escalated the issue to the server administrator's manager.
- At the next weekly scan window, Manish noticed that all the vulnerabilities were no longer active; however, ports 137, 139, and 445 were still showing as open. What most likely happened?
- A.** The server administrator blocked the scanner with a firewall.
 - B.** The server was patched.
 - C.** The vulnerability plug-ins were updated and no longer report false positives.
 - D.** The system was offline.
- 65.** While conducting reconnaissance, Piper discovers what she believes is an SMTP service running on an alternate port. What technique should she use to manually validate her guess?
- A.** Send an email via the open port.
 - B.** Send an SMTP probe.
 - C.** Telnet to the port.
 - D.** SSH to the port.
- 66.** What two pieces of information does nmap need to estimate network path distance?
- A.** IP address and TTL
 - B.** TTL and operating system
 - C.** Operating system and BGP flags
 - D.** TCP flags and IP address
- 67.** Helen is using the Lockheed Martin Cyber Kill Chain to analyze an attack that took place against her organization. During the attack, the perpetrator attached a malicious tool to an email message that was sent to the victim. What phase of the Cyber Kill Chain includes this type of activity?
- A.** Weaponization
 - B.** Delivery
 - C.** Exploitation
 - D.** Actions on objectives

68. During an on-site penetration test of a small business, Ramesh scans outward to a known host to determine the outbound network topology. What information can he gather from the results provided by Zenmap?



- A. There are two nodes on the local network.
- B. There is a firewall at IP address 96.120.24.121.
- C. There is an IDS at IP address 96.120.24.121.
- D. He should scan the 10.0.2.0/24 network.

Use the following network diagram and scenario to answer questions 69–71.

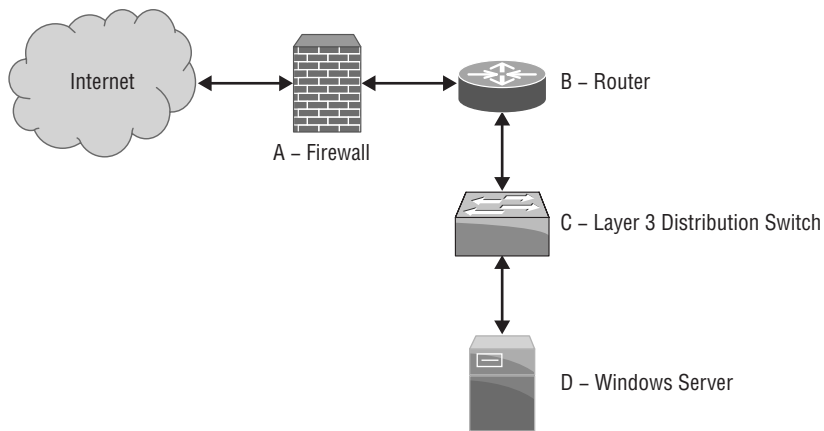


- 69.** Marta is a security analyst who has been tasked with performing nmap scans of her organization's network. She is a new hire and has been given this logical diagram of the organization's network but has not been provided with any additional detail.
- Marta wants to determine what IP addresses to scan from location A. How can she find this information?
- A.** Scan the organization's web server and then scan the other 255 IP addresses in its subnet.
 - B.** Query DNS and WHOIS to find her organization's registered hosts.
 - C.** Contact ICANN to request the data.
 - D.** Use traceroute to identify the network that the organization's domain resides in.
- 70.** If Marta runs a scan from location B that targets the servers on the datacenter network and then runs a scan from location C, what differences is she most likely to see between the scans?
- A.** The scans will match.
 - B.** Scans from location C will show no open ports.
 - C.** Scans from location C will show fewer open ports.
 - D.** Scans from location C will show more open ports.

71. Marta wants to perform regular scans of the entire organizational network but only has a budget that supports buying hardware for a single scanner. Where should she place her scanner to have the most visibility and impact?

A. Location A
 B. Location B
 C. Location C
 D. Location D

72. Andrea needs to add a firewall rule that will prevent external attackers from conducting topology gathering reconnaissance on her network. Where should she add a rule intended to block this type of traffic?



- A. The firewall
 B. The router
 C. The distribution switch
 D. The Windows server
73. Brandon wants to perform a WHOIS query for a system he believes is located in Europe. Which NIC should he select to have the greatest likelihood of success for his query?
- A. AFRINIC
 B. APNIC
 C. RIPE
 D. LACNIC
74. While reviewing Apache logs, Janet sees the following entries as well as hundreds of others from the same source IP. What should Janet report has occurred?

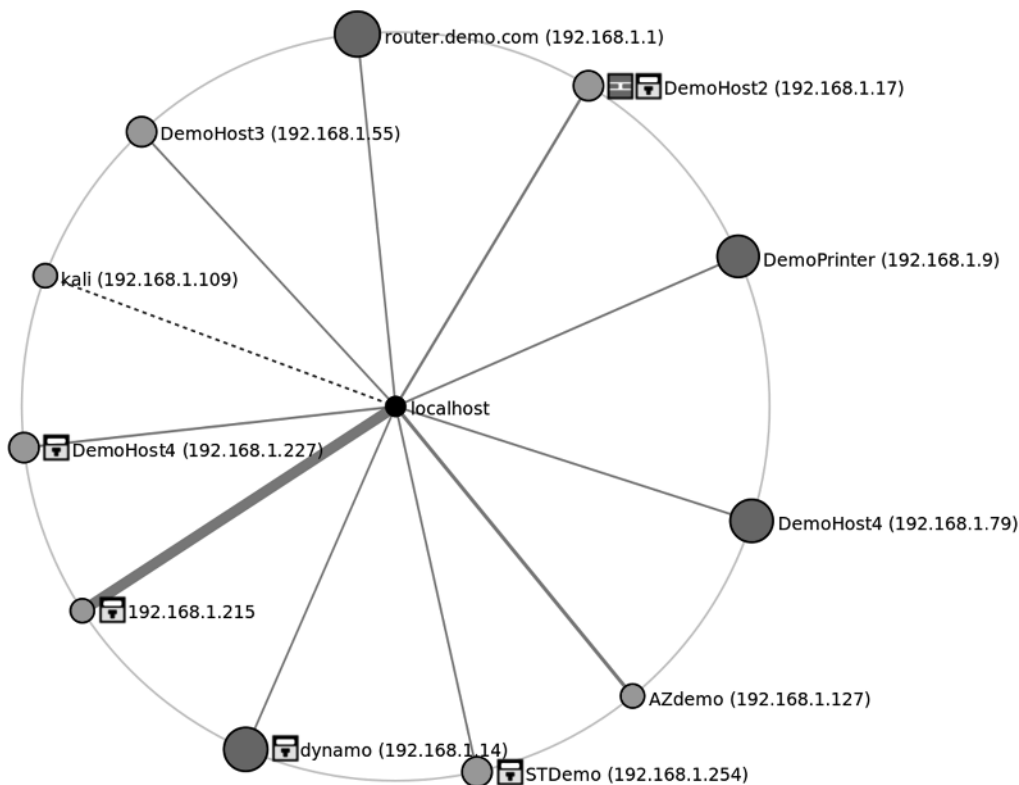
```
[ 21/Jul/2020:02:18:33 -0500] - - 10.0.1.1 "GET /scripts/sample.php"
"- " 302 336 0
```

```
[ 21/Jul/2020:02:18:35 -0500] - - 10.0.1.1 "GET /scripts/test.php" "-" 302
336 0
[ 21/Jul/2020:02:18:37 -0500] - - 10.0.1.1 "GET /scripts/manage.php" "-"
302 336 0
[ 21/Jul/2020:02:18:38 -0500] - - 10.0.1.1 "GET /scripts/download.php" "-"
302 336 0
[ 21/Jul/2020:02:18:40 -0500] - - 10.0.1.1 "GET /scripts/update.php" "-"
302 336 0
[ 21/Jul/2020:02:18:42 -0500] - - 10.0.1.1 "GET /scripts/new.php"
"-" 302 336 0
```

- A. A denial-of-service attack
 - B. A vulnerability scan
 - C. A port scan
 - D. A directory traversal attack
75. Chris wants to gather as much information as he can about an organization using DNS harvesting techniques. Which of the following methods will most easily provide the most useful information if they are all possible to conduct on the network he is targeting?
- A. DNS record enumeration
 - B. Zone transfer
 - C. Reverse lookup
 - D. Domain brute-forcing
76. Geoff wants to perform passive reconnaissance as part of an evaluation of his organization's security controls. Which of the following techniques is a valid technique to perform as part of a passive DNS assessment?
- A. A DNS forward or reverse lookup
 - B. A zone transfer
 - C. A WHOIS query
 - D. Using maltego
77. Mike's penetration test requires him to use passive mapping techniques to discover network topology. Which of the following tools is best suited to that task?
- A. Wireshark
 - B. nmap
 - C. netcat
 - D. Angry IP Scanner
78. While gathering DNS information about an organization, Ryan discovered multiple AAAA records. What type of reconnaissance does this mean Ryan may want to consider?
- A. Second-level DNS queries
 - B. IPv6 scans

- C. Cross-domain resolution
- D. A CNAME verification

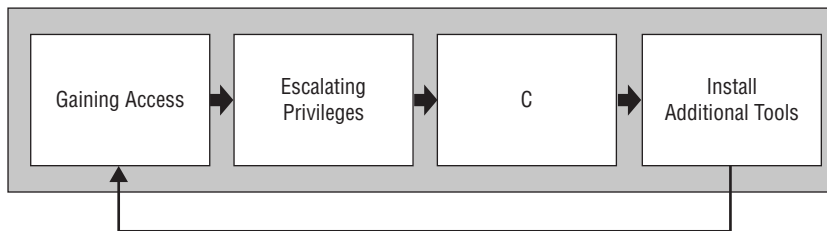
79. After Carlos completes a topology discovery scan of his local network, he sees the Zenmap topology shown here. What can Carlos determine from the Zenmap topology view?



- A. There are five hosts with port security enabled.
 - B. DemoHost2 is running a firewall.
 - C. DemoHost4 is running a firewall.
 - D. There are four hosts with vulnerabilities and seven hosts that do not have vulnerabilities.
80. Scott is part of the white team who is overseeing his organization's internal red and blue teams during an exercise that requires each team to only perform actions appropriate to the penetration test phase they are in. During the reconnaissance phase, he notes the following behavior as part of a Wireshark capture. What should he report?

No.	Time	Source	Destination	Protoc	Length	Info
2180	2.493035366	10.0.2.4	10.0.2.15	TCP	66	80 → 55554 [FIN, ACK] Seq=507 Ack=420 Win=6880 Len=0 TSval=127193 TSecr=317472
2181	2.493271630	10.0.2.15	10.0.2.4	TCP	66	55554 → 80 [FIN, ACK] Seq=420 Ack=508 Win=30336 Len=0 TSval=317472 TSecr=127193
2182	2.493462055	10.0.2.4	10.0.2.15	TCP	66	80 → 55554 [ACK] Seq=508 Ack=421 Win=6880 Len=0 TSval=127193 TSecr=317472
2183	2.498331161	10.0.2.15	10.0.2.4	TCP	66	55552 → 80 [FIN, ACK] Seq=413 Ack=503 Win=30336 Len=0 TSval=317473 TSecr=127192
2184	2.498386675	10.0.2.15	10.0.2.4	TCP	74	55556 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=317473 TSecr=0 WS=128
2185	2.498503116	10.0.2.4	10.0.2.15	TCP	66	80 → 55552 [ACK] Seq=503 Ack=414 Win=6880 Len=0 TSval=127193 TSecr=317473
2186	2.498520426	10.0.2.4	10.0.2.15	TCP	74	80 → 55556 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=127193 TSecr=317
2187	2.498527886	10.0.2.15	10.0.2.4	TCP	66	55556 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=317473 TSecr=127193
2188	2.497238989	10.0.2.15	10.0.2.4	HTTP	492	GET /v1/1/1/200H10N20ALLN20SELECTN20HULLN20HULLN20HULLN20HULLN23 HTTP/1.1
2189	2.497464022	10.0.2.4	10.0.2.15	TCP	66	80 → 55556 [ACK] Seq=1 Ack=427 Win=6880 Len=0 TSval=127193 TSecr=317473
2190	2.497648036	10.0.2.4	10.0.2.15	HTTP	577	HTTP/1.1 404 Not Found (text/html)
2191	2.497665375	10.0.2.15	10.0.2.4	TCP	66	55556 → 80 [ACK] Seq=427 Ack=512 Win=30336 Len=0 TSval=317473 TSecr=127194
2192	2.497689491	10.0.2.4	10.0.2.15	TCP	66	80 → 55556 [FIN, ACK] Seq=512 Ack=427 Win=6880 Len=0 TSval=127194 TSecr=317473
2193	2.502043782	10.0.2.15	10.0.2.4	TCP	74	55558 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=317474 TSecr=0 WS=128
2194	2.502267897	10.0.2.4	10.0.2.15	TCP	74	80 → 55558 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=127194 TSecr=317
2195	2.502284637	10.0.2.15	10.0.2.4	TCP	66	55558 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=317474 TSecr=127194
2196	2.502356539	10.0.2.15	10.0.2.4	HTTP	489	GET /v1/1/1/200H10N20ALLN20SELECTN20HULLN20HULLN20HULLN20HULLN23 HTTP/1.1

- A. The blue team has succeeded.
 B. The red team is violating the rules of engagement.
 C. The red team has succeeded.
 D. The blue team is violating the rules of engagement.
81. Jennifer analyzes a Wireshark packet capture from a network that she is unfamiliar with. She discovers that a host with IP address 10.11.140.13 is running services on TCP ports 636 and 443. What services is that system most likely running?
- A. LDAPS and HTTPS
 B. FTPS and HTTPS
 C. RDP and HTTPS
 D. HTTP and Secure DNS
82. Kai has identified a privilege escalation flaw on the system she targeted in the first phase of her penetration test and is now ready to take the next step. According to the NIST 800-115 standard, what is step C that Kai needs to take, as shown in this diagram?



- A. System browsing
 B. Scanning
 C. Rooting
 D. Consolidation
83. When Scott performs an nmap scan with the -T flag set to 5, what variable is he changing?
- A. How fast the scan runs
 B. The TCP timeout flag it will set
 C. How many retries it will perform
 D. How long the scan will take to start up

84. While conducting a port scan of a remote system, Henry discovers TCP port 1433 open. What service can he typically expect to run on this port?
- A. Oracle
 - B. VNC
 - C. IRC
 - D. Microsoft SQL
85. While application vulnerability scanning one of her target organizations web servers, Andrea notices that the server's hostname is resolving to a `cloudflare.com` host. What does Andrea know about her scan?
- A. It is being treated like a DDoS attack.
 - B. It is scanning a CDN-hosted copy of the site.
 - C. It will not return useful information.
 - D. She cannot determine anything about the site based on this information.
86. While tracking a potential APT on her network, Cynthia discovers a network flow for her company's central file server. What does this flow entry most likely show if 10.2.2.3 is not a system on her network?
- | Date | flow start | Duration | Proto | Src | IP | Addr:Port | Dst | IP |
|----------------|------------|--------------|----------|-----|----------------|-----------|-----|----|
| Addr:Port | Packets | Bytes | Flows | | | | | |
| 2017-07-11 | | 13:06:46.343 | 21601804 | TCP | 10.1.1.1:1151- | | | |
| >10.2.2.3:443 | | 9473640 | 9.1 G | 1 | | | | |
| 2017-07-11 | | 13:06:46.551 | 21601804 | TCP | 10.2.2.3:443- | | | |
| >10.1.1.1:1151 | | 8345101 | 514 M | 1 | | | | |
- A. A web browsing session
 - B. Data exfiltration
 - C. Data infiltration
 - D. A vulnerability scan
87. Part of Tracy's penetration testing assignment is to evaluate the WPA2 Enterprise protected wireless networks of her target organization. What major differences exist between reconnaissances of a wired network versus a wireless network?
- A. Encryption and physical accessibility
 - B. Network access control and encryption
 - C. Port security and physical accessibility
 - D. Authentication and encryption
88. Ian's company has an internal policy requiring that they perform regular port scans of all of their servers. Ian has been part of a recent effort to move his organization's servers to an infrastructure as a service (IaaS) provider. What change will Ian most likely need to make to his scanning efforts?
- A. Change scanning software
 - B. Follow the service provider's scan policies

- C. Sign a security contract with the provider
 - D. Discontinue port scanning
89. During a regularly scheduled PCI compliance scan, Fred has discovered port 3389 open on one of the point-of-sale terminals that he is responsible for managing. What service should he expect to find enabled on the system?
- A. MySQL
 - B. RDP
 - C. TOR
 - D. Jabber
90. Saanvi knows that the organization she is scanning runs services on alternate ports to attempt to reduce scans of default ports. As part of her intelligence-gathering process, she discovers services running on ports 8080 and 8443. What services are most likely running on these ports?
- A. Botnet C&C
 - B. Nginx
 - C. Microsoft SQL Server instances
 - D. Web servers
91. Lauren wants to identify all the printers on the subnets she is scanning with nmap. Which of the following nmap commands will not provide her with a list of likely printers?
- A. `nmap -sS -p 9100,515,631 10.0.10.15/22 -oX printers.txt`
 - B. `nmap -O 10.0.10.15/22 -oG - | grep printer >> printers.txt`
 - C. `nmap -sU -p 9100,515,631 10.0.10.15/22 -oX printers.txt`
 - D. `nmap -sS -O 10.0.10.15/22 -oG | grep >> printers.txt`
92. Chris knows that systems have connected to a remote host on TCP ports 1433 and 1434. If he has no other data, what should his best guess be about what the host is?
- A. A print server
 - B. A Microsoft SQL server
 - C. A MySQL server
 - D. A secure web server running on an alternate port
93. What services will the following nmap scan test for?
- ```
nmap -sV -p 22,25,53,389 192.168.2.50/27
```
- A. Telnet, SMTP, DHCP, MS-SQL
  - B. SSH, SMTP, DNS, LDAP
  - C. Telnet, SNMP, DNS, LDAP
  - D. SSH, SNMP, DNS, RDP

94. While conducting a topology scan of a remote web server, Susan notes that the IP addresses returned for the same DNS entry change over time. What has she likely encountered?
- A. A route change
  - B. Fast-flux DNS
  - C. A load balancer
  - D. An IP mismatch
95. Kwame is reviewing his team's work as part of a reconnaissance effort and is checking Wireshark packet captures. His team reported no open ports on 10.0.2.15. What issue should he identify with their scan based on the capture shown here?

| No. | Time        | Source   | Destination | Protocol | Length | Info                |
|-----|-------------|----------|-------------|----------|--------|---------------------|
| 13  | 0.100180953 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 863 Len=0   |
| 15  | 0.110753561 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 824 Len=0   |
| 17  | 0.110817229 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 113 Len=0   |
| 19  | 0.110841441 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 939 Len=0   |
| 21  | 0.110863163 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 697 Len=0   |
| 22  | 0.111006998 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 621 Len=0   |
| 23  | 0.111027206 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 1383 Len=0  |
| 24  | 0.111030525 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 219 Len=0   |
| 25  | 0.111101199 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 2002 Len=0  |
| 26  | 0.111118867 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 928 Len=0   |
| 27  | 0.111121941 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 708 Len=0   |
| 28  | 0.111185718 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 966 Len=0   |
| 29  | 0.111202390 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 26900 Len=0 |
| 30  | 0.111205511 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 433 Len=0   |
| 31  | 0.111268448 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 187 Len=0   |
| 32  | 0.111286492 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 2241 Len=0  |
| 33  | 0.111349409 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 419 Len=0   |
| 34  | 0.111365580 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 17 Len=0    |
| 35  | 0.111428929 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 10 Len=0    |
| 36  | 0.111446417 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 1542 Len=0  |
| 37  | 0.111508808 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 1349 Len=0  |
| 38  | 0.111524824 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 4008 Len=0  |
| 39  | 0.120479136 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 1472 Len=0  |
| 40  | 0.120534842 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 163 Len=0   |
| 41  | 0.120547451 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 33 Len=0    |
| 42  | 0.120550476 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 557 Len=0   |
| 43  | 0.120553316 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 198 Len=0   |
| 44  | 0.120650965 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 1358 Len=0  |
| 45  | 0.120668622 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 5714 Len=0  |
| 46  | 0.120671933 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 920 Len=0   |
| 47  | 0.120674771 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 677 Len=0   |
| 48  | 0.120754540 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 446 Len=0   |
| 49  | 0.120761057 | 10.0.2.4 | 10.0.2.15   | UDP      | 60     | 41015 → 68 Len=0    |

- A. The host was not up.
  - B. Not all ports were scanned.
  - C. The scan scanned only UDP ports.
  - D. The scan was not run as root.
96. Allan's nmap scan includes a line that starts with cpe:/o. What type of information should he expect to gather from the entry?
- A. Common privilege escalation
  - B. Operating system

- C. Certificate performance evaluation  
D. Hardware identification
97. While scanning a network, Frank discovers a host running a service on TCP ports 1812 and 1813. What type of server has Frank most likely discovered?  
A. RADIUS  
B. VNC  
C. Kerberos  
D. Postgres
98. Nihar wants to conduct an nmap scan of a firewalled subnet. Which of the following is not an nmap firewall evasion technique he could use?  
A. Fragmenting packets  
B. Changing packet header flags  
C. Spoofing the source IP  
D. Appending random data
99. Which of the following commands will provide Ben with the most information about a host?  
A. `dig -x [ip address]`  
B. `host [ip address]`  
C. `nslookup [ip address]`  
D. `zonet [ip address]`
100. Fred's reconnaissance of an organization includes a search of the Censys network search engine. There, he discovers multiple certificates with validity dates as shown here:  
Validity  
2018-07-07 00:00:00 to 2019-08-11 23:59:59 (400 days, 23:59:59)  
2017-07-08 00:00:00 to 2019-08-12 23:59:59 (400 days, 23:59:59)  
2018-07-11 00:00:00 to 2019-08-15 23:59:59 (400 days, 23:59:59)  
What should Fred record in his reconnaissance notes?  
A. The certificates expired as expected, showing proper business practice.  
B. The certificates were expired by the CA, possibly due to nonpayment.  
C. The system that hosts the certificates may have been compromised.  
D. The CA may have been compromised, leading to certificate expiration.
101. When Casey scanned a network host, she received the results shown here. What does she know based on the scan results?

| PORT     | STATE | SERVICE        | VERSION                       |
|----------|-------|----------------|-------------------------------|
| 2000/tcp | open  | cisco-sccp?    |                               |
| 3000/tcp | open  | http           | Apache httpd 2.2.3 ((CentOS)) |
| 6789/tcp | open  | ibm-db2-admin? |                               |

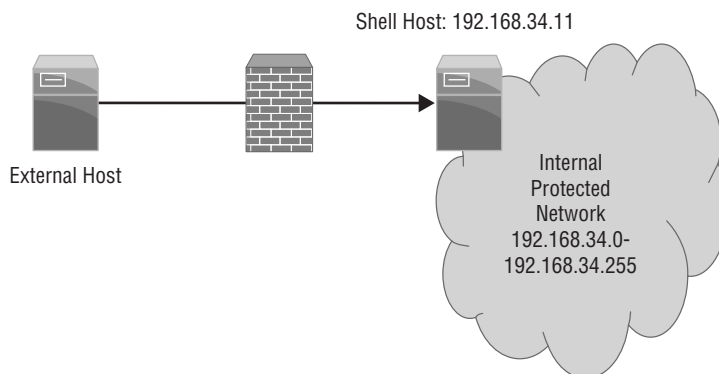
- A. The device is a Cisco device.
  - B. The device is running CentOS.
  - C. The device was built by IBM.
  - D. None of the above.
- 102. Fred conducts an SNMP sweep of a target organization and receives no-response replies from multiple addresses that he believes belong to active hosts. What does this mean?
  - A. The machines are unreachable.
  - B. The machines are not running SNMP servers.
  - C. The community string he used is invalid.
  - D. Any or all of the above may be true.
- 103. Angela wants to gather detailed information about the hosts on a network passively. If she has access to a Wireshark PCAP file from the network, which of the following tools can she use to provide automated analysis of the file?
  - A. Ettercap
  - B. NetworkMiner
  - C. Sharkbait
  - D. Dradis
- 104. While performing reconnaissance of an organization's network, Angela discovers that `web.organization.com`, `www.organization.com`, and `documents.organization.com` all point to the same host. What type of DNS record allows this?
  - A. A CNAME
  - B. An MX record
  - C. An SPF record
  - D. An SOA record
- 105. Aidan operates the point-of-sale network for a company that accepts credit cards and is thus required to be compliant with PCI DSS. During his regular assessment of the point-of-sale terminals, he discovers that a recent Windows operating system vulnerability exists on all of them. Since they are all embedded systems that require a manufacturer update, he knows that he cannot install the available patch. What is Aidan's best option to stay compliant with PCI DSS and protect his vulnerable systems?
  - A. Replace the Windows embedded point-of-sale terminals with standard Windows systems.
  - B. Build a custom operating system image that includes the patch.
  - C. Identify, implement, and document compensating controls.
  - D. Remove the POS terminals from the network until the vendor releases a patch.

- 106.** What occurs when Mia uses the following command to perform an nmap scan of a network?
- ```
nmap -sP 192.168.2.0/24
```
- A.** A secure port scan of all hosts in the 192.168.0.0 to 192.168.2.255 network range
 - B.** A scan of all hosts that respond to ping in the 192.168.0.0 to 192.168.255.255 network range
 - C.** A scan of all hosts that respond to ping in the 192.168.2.0 to 192.168.2.255 network range
 - D.** A SYN-based port scan of all hosts in the 192.168.2.0 to 192.168.2.255 network range
- 107.** Amir's remote scans of a target organization's class C network block using nmap (nmap -sS 10.0.10.1/24) show only a single web server. If Amir needs to gather additional reconnaissance information about the organization's network, which of the following scanning techniques is most likely to provide additional detail?
- A.** Use a UDP scan.
 - B.** Perform a scan from on-site.
 - C.** Scan using the -p 1-65535 flag.
 - D.** Use nmap's IPS evasion techniques.
- 108.** Damian wants to limit the ability of attackers to conduct passive fingerprinting exercises on his network. Which of the following practices will help to mitigate this risk?
- A.** Implement an IPS.
 - B.** Implement a firewall.
 - C.** Disable promiscuous mode for NICs.
 - D.** Enable promiscuous mode for NICs.
- 109.** Wang submits a suspected malware file to malwr.com and receives the following information about its behavior. What type of tool is malwr.com?

Signatures
A process attempted to delay the analysis task.
File has been identified by at least one AntiVirus on VirusTotal as malicious
The binary likely contains encrypted or compressed data.
Creates a windows hook that monitors keyboard input (keylogger)
Creates an Alternate Data Stream (ADS)
Installs itself for autorun at Windows startup

- A.** A reverse-engineering tool
- B.** A static analysis sandbox

- C. A dynamic analysis sandbox
 - D. A decompiler sandbox
- 110.** As part of his active reconnaissance activities, Frank is provided with a shell account accessible via SSH. If Frank wants to run a default nmap scan on the network behind the firewall shown here, how can he accomplish this?



- A. `ssh -t 192.168.34.11 nmap 192.168.34.0/24`
 - B. `ssh -R 8080:192.168.34.11:8080 [remote account:remote password]`
 - C. `ssh -proxy 192.168.11 [remote account:remote password]`
 - D. Frank cannot scan multiple ports with a single ssh command.
- 111.** Angela captured the following packets during a reconnaissance effort run by her organization's red team. What type of information are they looking for?

No.	Time	Source	Destination	Protocol	Length	Info
6855	23.033528285	10.0.2.15	18.0.2.4	HTTP	262	GET /forum1.asp?n=1753&np=nn;.....etc/passwd#00 HTTP/1.1
6856	23.033823693	10.0.2.4	18.0.2.15	HTTP	575	HTTP/1.1 404 Not Found (text/html)
6857	23.03483690	10.0.2.15	18.0.2.4	HTTP	235	GET /forum1.asp?n=1753&np=nn;.....boot.ini HTTP/1.1
6858	23.044847831	10.0.2.4	18.0.2.15	HTTP	575	HTTP/1.1 404 Not Found (text/html)
6859	23.053478224	10.0.2.15	18.0.2.4	HTTP	233	GET /forum1.asp?n=1753&np=nn;.....boot.ini HTTP/1.1
6860	23.05578399	10.0.2.4	18.0.2.15	HTTP	575	HTTP/1.1 404 Not Found (text/html)
6861	23.063452478	10.0.2.15	18.0.2.4	HTTP	288	GET /forum1.asp?n=1753&np=nn;.....etc/passwd HTTP/1.1
6862	23.063736962	10.0.2.4	18.0.2.15	HTTP	575	HTTP/1.1 404 Not Found (text/html)
6863	23.073721012	10.0.2.15	18.0.2.4	HTTP	253	GET /forum1.asp?n=1753&np=nn;.....boot.ini HTTP/1.1
6864	23.07540278	10.0.2.4	18.0.2.15	HTTP	575	HTTP/1.1 404 Not Found (text/html)
6865	23.08344524	10.0.2.15	18.0.2.4	HTTP	238	GET /forum1.asp?n=1753&np=nn;etc/passwd HTTP/1.1
6866	23.08627047	10.0.2.4	18.0.2.15	HTTP	575	HTTP/1.1 404 Not Found (text/html)
6867	23.093291482	10.0.2.15	18.0.2.4	HTTP	233	GET /forum1.asp?n=1753&np=nn;etc/passwd#00 HTTP/1.1
6868	23.093572807	10.0.2.4	18.0.2.15	HTTP	575	HTTP/1.1 404 Not Found (text/html)
6869	23.048375264	10.0.2.15	18.0.2.4	HTTP	238	GET /forum1.asp?n=1753&np=nn;boot.ini HTTP/1.1
6870	23.05578399	10.0.2.4	18.0.2.15	HTTP	575	HTTP/1.1 404 Not Found (text/html)

- A.** Vulnerable web applications
 - B.** SQL injection
 - C.** Directory traversal attacks
 - D.** Passwords
- 112.** Which sources are most commonly used to gather information about technologies a target organization uses during intelligence gathering?
- A.** OSINT searches of support forums and social engineering
 - B.** Port scanning and social engineering

- C. Social media review and document metadata
 - D. Social engineering and document metadata
- 113.** Sarah has been asked to assess the technical impact of suspected reconnaissance performed against her organization. She is informed that a reliable source has discovered that a third party has been performing reconnaissance by querying WHOIS data. How should Sarah categorize the technical impact of this type of reconnaissance?
- A. High
 - B. Medium
 - C. Low
 - D. She cannot determine this from the information given.
- 114.** Rick is reviewing flows of a system on his network and discovers the following flow logs. What is the system doing?

ICMP "Echo request"

Date	flow start	Duration	Proto	Src IP	Addr:Port->Dst IP
Addr:Port	Packets	Bytes	Flows		
2019-07-11 11	924	04:58:59.518 1	10.000 ICMP	10.1.1.1:0->10.2.2.6:8.0	
2019-07-11 11	924	04:58:59.518 1	10.000 ICMP	10.2.2.6:0->10.1.1.1:0.0	
2019-07-11 11	924	04:58:59.518 1	10.000 ICMP	10.1.1.1:0->10.2.2.7:8.0	
2019-07-11 11	924	04:58:59.518 1	10.000 ICMP	10.2.2.7:0->10.1.1.1:0.0	
2019-07-11 11	924	04:58:59.518 1	10.000 ICMP	10.1.1.1:0->10.2.2.8:8.0	
2019-07-11 11	924	04:58:59.518 1	10.000 ICMP	10.2.2.8:0->10.1.1.1:0.0	
2019-07-11 11	924	04:58:59.518 1	10.000 ICMP	10.1.1.1:0->10.2.2.9:8.0	
2019-07-11 11	924	04:58:59.518 1	10.000 ICMP	10.2.2.9:0->10.1.1.1:0.0	
2019-07-11 11	924	04:58:59.518 1	10.000 ICMP	10.1.1.1:0->10.2.2.10:8.0	
2019-07-11 11	924	04:58:59.518 1	10.000 ICMP	10.2.2.10:0->10.1.1.1:0.0	
2019-07-11 11	924	04:58:59.518 1	10.000 ICMP	10.1.1.1:0->10.2.2.6:11.0	
2019-07-11 11	924	04:58:59.518 1	10.000 ICMP	10.2.2.11:0->10.1.1.1:0.0	

- A. A port scan
- B. A failed three-way handshake

- C. A ping sweep
- D. A traceroute

115. Ryan's passive reconnaissance efforts resulted in the following packet capture. Which of the following statements cannot be verified based on the packet capture shown for the host with IP address 10.0.2.4?

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	CadmusCo_fa:25:8e	Broadcast	ARP	42	who has 10.0.2.4? Tell 10.0.2.15
2	0.000258663	CadmusCo_92:5f:44	CadmusCo_fa:25:8e	ARP	60	10.0.2.4 is at 08:00:27:92:5f:44
3	0.023177092	10.0.2.15	192.168.1.1	DNS	81	Standard query 0xfeba PTR 4.2.0.10.in-addr.arpa
4	0.047498670	192.168.1.1	10.0.2.15	DNS	81	Standard query response 0xfeba No such name PTR 4.2.0.10.in-addr.arpa
5	0.071380866	10.0.2.15	10.0.2.4	TCP	58	57352 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	0.071444219	10.0.2.15	10.0.2.4	TCP	58	57352 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	0.071652769	10.0.2.4	10.0.2.15	TCP	60	139 → 57352 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
8	0.071671858	10.0.2.15	10.0.2.4	TCP	54	57352 → 139 [RST] Seq=1 Win=0 Len=0
9	0.071685967	10.0.2.4	10.0.2.15	TCP	60	445 → 57352 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
10	0.071890208	10.0.2.15	10.0.2.4	TCP	54	57352 → 445 [RST] Seq=1 Win=0 Len=0
11	5.070143568	CadmusCo_92:5f:44	CadmusCo_fa:25:8e	ARP	60	who has 10.0.2.15? Tell 10.0.2.4
12	5.070164599	CadmusCo_fa:25:8e	CadmusCo_92:5f:44	ARP	42	10.0.2.15 is at 08:00:27:fa:25:8e

- A. The host does not have a DNS entry.
 - B. It is running a service on port 139.
 - C. It is running a service on port 445.
 - D. It is a Windows system.
- 116.** Stacey encountered a system that shows as “filtered” and “firewalled” during an nmap scan. Which of the following techniques should she not consider as she is planning her next scan?
- A. Packet fragmentation
 - B. Spoofing the source address
 - C. Using decoy scans
 - D. Spoofing the destination address
- 117.** Kim is preparing to deploy a new vulnerability scanner and wants to ensure that she can get the most accurate view of configuration issues on laptops belonging to traveling salespeople. Which technology will work best in this situation?
- A. Agent-based scanning
 - B. Server-based scanning
 - C. Passive network monitoring
 - D. Noncredentialed scanning

118. Carla runs a vulnerability scan of a new appliance that engineers are planning to place on her organization's network and finds the results shown here. Of the actions listed, which would correct the highest criticality vulnerability?


















FreeBSD Based Device			
▼ Vulnerabilities (15)			
2	SSL Certificate - Expired	port 443/tcp over SSL	CVSS: - CVSS3: - New
3	WINS Domain Controller Spoofing Vulnerability - Zero Day		CVSS: - CVSS3: - Active
3	NetBIOS Name Conflict Vulnerability		CVSS: - CVSS3: - Active
3	NetBIOS Release Vulnerability		CVSS: - CVSS3: - Active
2	Hidden RPC Services		CVSS: - CVSS3: - Active
2	NetBIOS Name Accessible		CVSS: - CVSS3: - Active
2	NTP Information Disclosure Vulnerability	port 123/udp	CVSS: - CVSS3: - Active
2	SSL Certificate - Self-Signed Certificate	port 443/tcp over SSL	CVSS: - CVSS3: - Active
2	SSL Certificate - Subject Common Name Does Not Match Server FQDN	port 443/tcp over SSL	CVSS: - CVSS3: - Active
2	SSL Certificate - Signature Verification Failed Vulnerability	port 443/tcp over SSL	CVSS: - CVSS3: - Active
1	Presence of a Load-Balancing Device Detected	port 443/tcp over SSL	CVSS: - CVSS3: - Active
1	Presence of a Load-Balancing Device Detected	port 80/tcp	CVSS: - CVSS3: - Active
3	SSL/TLS Compression Algorithm Information Leakage Vulnerability	port 443/tcp over SSL	CVSS: - CVSS3: - Fixed
3	SSL/TLS Server supports TLSv1.0	port 443/tcp over SSL	CVSS: - CVSS3: - Fixed
1	SSL Certificate - Will Expire Soon	port 443/tcp over SSL	CVSS: - CVSS3: - Fixed

- A. Block the use of TLS v1.0.
 - B. Replace the expired SSL certificate.
 - C. Remove the load balancer.
 - D. Correct the information leakage vulnerability.
119. In what type of attack does the adversary leverage a position on a guest operating system to gain access to hardware resources assigned to other operating systems running in the same hardware environment?
- A. Buffer overflow
 - B. Directory traversal
 - C. VM escape
 - D. Cross-site scripting
120. Sadiq is responsible for the security of a network used to control systems within his organization's manufacturing plant. The network connects manufacturing equipment, sensors, and controllers. He runs a vulnerability scan on this network and discovers that several of the controllers are running very out-of-date firmware that introduces security issues. The manufacturer of the controllers is out of business. What action can Sadiq take to best remediate this vulnerability in an efficient manner?
- A. Develop a firmware update internally and apply it to the controllers.
 - B. Post on an Internet message board seeking other organizations that have developed a patch.
 - C. Ensure that the ICS is on an isolated network.
 - D. Use an intrusion prevention system on the ICS network.

121. Vic scanned a Windows server used in his organization and found the result shown here. The server is on an internal network with access limited to IT staff and is not part of a domain. How urgently should Vic remediate this vulnerability?

3 Administrator Account's Password Does Not Expire			
First Detected:	02/04/2020 at 18:02:25 (GMT-0400)	Last Detected:	04/05/2020 at 00:48:55 (GMT-0400)
Times Detected:	22	Last Fixed:	N/A
QID:	90080	CVSS Base:	7.5 ^[1]
Category:	Windows	CVSS Temporal:	7.1
CVE ID:	-	CVSS3 Base:	-
Vendor Reference:	-	CVSS3 Temporal:	-
Bugtraq ID:	-	CVSS Environment:	-
Service Modified:	08/03/2020	Asset Group:	-
User Modified:	-	Collateral Damage Potential:	-
Edited:	No	Target Distribution:	-
PCI Vuln:	Yes	Confidentiality Requirement:	-
Ticket State:	-	Integrity Requirement:	-
		Availability Requirement:	-
THREAT:			
The scanner probed the Security & Accounts Database (SAM) and found that the target Windows box's Administrator account has a password that does not expire.			

- A. Vic should drop everything and remediate this vulnerability immediately.
- B. While Vic does not need to drop everything, this vulnerability requires urgent attention and should be addressed quickly.
- C. This is a moderate vulnerability that can be scheduled for remediation at a convenient time.
- D. This vulnerability is informational in nature and may be left in place.
122. Rob's manager recently asked him for an overview of any critical security issues that exist on his network. He looks at the reporting console of his vulnerability scanner and sees the options shown here. Which of the following report types would be his best likely starting point?

<input type="checkbox"/>  Title	Type	Vulnerability Data
<input type="checkbox"/>  Unknown Device Report		Scan Based
<input type="checkbox"/>  Executive Report		Host Based
<input type="checkbox"/>  High Severity Report		Host Based
<input type="checkbox"/>  Payment Card Industry (PCI) Executive Report		Scan Based
<input type="checkbox"/>  Payment Card Industry (PCI) Technical Report		Scan Based
<input type="checkbox"/>  Qualys Patch Report		Host Based
<input type="checkbox"/>  Qualys Top 20 Report		Host Based
<input type="checkbox"/>  Technical Report		Host Based

- A. Technical Report
- B. High Severity Report
- C. Qualys Patch Report
- D. Unknown Device Report

- 123.** Wendy is the security administrator for a membership association that is planning to launch an online store. As part of this launch, she will become responsible for ensuring that the website and associated systems are compliant with all relevant standards. What regulatory regime specifically covers credit card information?
- A.** PCI DSS
 - B.** FERPA
 - C.** HIPAA
 - D.** SOX
- 124.** During a port scan of a server, Miguel discovered that the following ports are open on the internal network:
- TCP port 25
 - TCP port 80
 - TCP port 110
 - TCP port 443
 - TCP port 1433
 - TCP port 3389
- The scan results provide evidence that a variety of services are running on this server. Which one of the following services is *not* indicated by the scan results?
- A.** Web
 - B.** Database
 - C.** SSH
 - D.** RDP
- 125.** Nina is a software developer and she receives a report from her company's cybersecurity team that a vulnerability scan detected a SQL injection vulnerability in one of her applications. She examines her code and makes a modification in a test environment that she believes corrects the issue. What should she do next?
- A.** Deploy the code to production immediately to resolve the vulnerability.
 - B.** Request a scan of the test environment to confirm that the issue is corrected.
 - C.** Mark the vulnerability as resolved and close the ticket.
 - D.** Hire a consultant to perform a penetration test to confirm that the vulnerability is resolved.
- 126.** George recently ran a port scan on a network device used by his organization. Which one of the following open ports represents the most significant possible security vulnerability?
- A.** 22
 - B.** 23
 - C.** 161
 - D.** 443

Use the following scenario to answer questions 127–129.

Harold runs a vulnerability scan of a server that he is planning to move into production and finds the vulnerability shown here.

SSL/TLS Server supports TLSv1.0		port 3389/tcp over SSL CVSS: - CVSS3: - Active	
First Detected:	03/25/2020 at 01:16:35 (GMT-0400)	Last Detected:	04/09/2020 at 00:58:18 (GMT-0400)
QID:	39628	CVSS Base:	2.6 ^[1]
Category:	General remote services	CVSS Temporal:	2.3
CVE ID:	-	CVSS3 Base:	0 ^[1]
Vendor Reference:	-	CVSS3 Temporal:	0
Bugtraq ID:	-	CVSS3 Environment:	-
Service Modified:	07/14/2020	Asset Group:	-
User Modified:	-	Collateral Damage Potential:	-
Edited:	No	Target Distribution:	-
PCI Vuln:	No	Confidentiality Requirement:	-
Ticket State:	-	Integrity Requirement:	-
		Availability Requirement:	-

127. What operating system is most likely running on the server in this vulnerability scan report?
- A. macOS
 - B. Windows
 - C. CentOS
 - D. RHEL
128. Harold is preparing to correct the vulnerability. What service should he inspect to identify the issue?
- A. SSH
 - B. HTTPS
 - C. RDP
 - D. SFTP
129. Harold would like to secure the service affected by this vulnerability. Which one of the following protocols/versions would be an acceptable way to resolve the issue?
- A. SSL v2.0
 - B. SSL v3.0
 - C. TLS v1.0
 - D. None of the above

130. Seth found the vulnerability shown here in one of the systems on his network. What component requires a patch to correct this issue?

5 VMware ESXi 5.5.0 Patch Release ESXi550-201703401-SG Missing (KB2149576) CVSS: - CVSS3: - New

First Detected:	04/05/2020 at 21:10:27 (GMT-0400)	Last Detected:	04/05/2020 at 21:10:27 (GMT-0400)	Times Detected:	1	Last Fixed:	N/A
QID:	218120	CVSS Base:	6.6				
Category:	VMware	CVSS Temporal:	4.9				
CVE ID:	CVE-2017-4902 CVE-2017-4903 CVE-2017-4904 CVE-2017-4905	CVSS3 Base:	-				
Vendor Reference:	VMSA-2017-0006	CVSS3 Temporal:	-				
Bugtraq ID:	-	CVSS3 Environment:	-				
Service Modified:	04/04/2020	Asset Group:	-				
User Modified:	-	Collateral Damage Potential:	-				
Edited:	No	Target Distribution:	-				
PCI Vuln:	Yes	Confidentiality Requirement:	-				
Ticket State:	Open	Integrity Requirement:	-				
		Availability Requirement:	-				

THREAT:
VMware ESXi is an enterprise level computer virtualization product.
A local user on the guest system can trigger a heap overflow in SVGA to execute arbitrary code on the host system [CVE-2017-4902]. ESXi 6.0 is not affected.
A local user on the guest system can trigger an uninitialized stack memory usage error in SVGA to execute arbitrary code on the host system [CVE-2017-4903].
A local user on the guest system can trigger an uninitialized stack memory usage error in the XHCI controller to execute arbitrary code on the host system [CVE-2017-4904]. On ESXi 5.5, the impact is limited to denial of service conditions.
A local user on the guest system can trigger an uninitialized memory usage error to obtain potentially sensitive information on the host system [CVE-2017-4905].

IMPACT:
A local user on the guest system can gain elevated privileges on the host system.
A local user on the guest system can obtain potentially sensitive information on the host system.

SOLUTION:
To resolve this issue, upgrade to VMware ESXi Build 5230635 or the latest VMware ESXi build.
Refer to VMware advisory [KB2149576](#) for updates and build information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
[VMSA-2017-0006: VMware ESXi 5.5](#)

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

- A. Operating system
- B. VPN concentrator
- C. Network router or switch
- D. Hypervisor

131. Quentin ran a vulnerability scan of a server in his organization and discovered the results shown here. Which one of the following actions is *not* required to resolve one of the vulnerabilities on this server?

Vulnerabilities (15)

- 3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)
- 3 Apache Tomcat Input Validation Security Bypass Vulnerability
- 3 Built-in Guest Account Not Renamed at Windows Target System
- 3 Administrator Account's Password Does Not Expire
- 3 Windows Remote Desktop Protocol Weak Encryption Method Allowed
- 3 SSL/TLS use of weak RC4 cipher
- 3 SSL/TLS Server supports TLSv1.0
- 3 SSL/TLS Server supports TLSv1.0
- 2 NetBIOS Name Accessible
- 2 FIN-ACK Network Device Driver Frame Padding Information Disclosure Vulnerability
- 2 SSL Certificate - Subject Common Name Does Not Match Server FQDN
- 2 SSL Certificate - Signature Verification Failed Vulnerability
- 2 SSL Certificate - Subject Common Name Does Not Match Server FQDN
- 2 SSL Certificate - Self-Signed Certificate
- 2 SSL Certificate - Signature Verification Failed Vulnerability

- A. Reconfigure cipher support.
- B. Apply Window security patches.
- C. Obtain a new SSL certificate.
- D. Enhance account security policies.

132. The presence of _____ triggers specific vulnerability scanning requirements based on law or regulation.

- A. Credit card information
- B. Protected health information
- C. Personally identifiable information
- D. Trade secret information

Use the scenario to answer questions 133–135.

Stella is analyzing the results of a vulnerability scan and comes across the vulnerability shown here on a server in her organization. The SharePoint service in question processes all of the organization's work orders and is a critical part of the routine business workflow.

First Detected:	06/28/2020 at 10:42:15 (GMT-0400)	Last Detected:	04/05/2020 at 00:16:12 (GMT-0400)	Times Detected:	20	Last Fixed:	N/A
QID:	110235	CVSS Base:	9				
Category:	Office Application	CVSS Temporal:	7				
CVE ID:	CVE-2014-0251 CVE-2014-1754 CVE-2014-1813	CVSS3 Base:	-				
Vendor Reference:	MS14-022	CVSS3 Temporal:	-				
Bugtraq ID:	67268	CVSS Environment:	-				
Service Modified:	06/03/2020	Asset Group:	-				
User Modified:	-	Collateral Damage Potential:	-				
Edited:	No	Target Distribution:	-				
PCI Vuln:	Yes	Confidentiality Requirement:	-				
Ticket State:	Open	Integrity Requirement:	-				
		Availability Requirement:	-				
THREAT:							
A remote code execution vulnerability exists in Microsoft Web Applications. An authenticated attacker who successfully exploited this vulnerability could run arbitrary code in the security context of the W3WP service account. (CVE-2014-1813). An elevation of privilege vulnerability exists in Microsoft SharePoint Server. An attacker who successfully exploited this vulnerability could perform cross-site scripting attacks on affected systems and run script in the security context of the logged on user.							
Affected Software:							
Microsoft SharePoint Server 2007, Microsoft SharePoint Server 2010, Microsoft SharePoint Server 2013, Microsoft Office Web Apps 2010, Microsoft Office Web Apps Server 2013, Microsoft SharePoint Services 3.0, and Microsoft SharePoint Foundation 2010, Microsoft SharePoint Designer 2007, Microsoft SharePoint Designer 2010, and Microsoft SharePoint Designer 2013							
This security update is rated Critical for supported editions of Microsoft SharePoint Server.							
IMPACT:							
The most severe of these vulnerabilities could allow remote code execution if an authenticated attacker sends specially crafted page content to a target SharePoint server.							
SOLUTION:							
Customers are advised to refer to MS14-022 .							
Patch:							
Following are links for downloading patches to fix the vulnerabilities:							
MS14-022: Microsoft SharePoint Server 2007 Service Pack 3 (32-bit editions) (Microsoft Windows SharePoint Services 3.0 Service Pack 3 (32-bit versions))							
MS14-022: Microsoft SharePoint Server 2007 Service Pack 3 (32-bit editions) (SharePoint Server 2007 Service Pack 3 (32-bit editions))							
MS14-022: Microsoft SharePoint Server 2007 Service Pack 3 (32-bit editions) (SharePoint Server 2007 Service Pack 3 (32-bit editions))							
MS14-022: Microsoft SharePoint Server 2007 Service Pack 3 (64-bit editions) (Microsoft Windows SharePoint Services 3.0 Service Pack 3 (64-bit versions))							
MS14-022: Microsoft SharePoint Server 2007 Service Pack 3 (64-bit editions) (SharePoint Server 2007 Service Pack 3 (64-bit editions))							
MS14-022: Microsoft SharePoint Server 2007 Service Pack 3 (64-bit editions) (SharePoint Server 2007 Service Pack 3 (64-bit editions))							
MS14-022: Microsoft SharePoint Server 2010 Service Pack 1 (Microsoft SharePoint Foundation 2010 Service Pack 1)							
MS14-022: Microsoft SharePoint Server 2010 Service Pack 2 (Microsoft SharePoint Foundation 2010 Service Pack 2)							
MS14-022: Microsoft SharePoint Server 2010 Service Pack 1 (Microsoft SharePoint Server 2010 Service Pack 1)							
MS14-022: Microsoft SharePoint Server 2010 Service Pack 2 (Microsoft SharePoint Server 2010 Service Pack 2)							

133. What priority should Stella place on remediating this vulnerability?

- A. Stella should make this vulnerability one of her highest priorities.
- B. Stella should remediate this vulnerability within the next several weeks.
- C. Stella should remediate this vulnerability within the next several months.
- D. Stella does not need to assign any priority to remediating this vulnerability.

- 134.** What operating system is most likely running on the server in this vulnerability scan report?
- A.** macOS
 - B.** Windows
 - C.** CentOS
 - D.** RHEL
- 135.** What is the best way that Stella can correct this vulnerability?
- A.** Deploy an intrusion prevention system.
 - B.** Apply one or more application patches.
 - C.** Apply one or more operating system patches.
 - D.** Disable the service.
- 136.** Harry is developing a vulnerability scanning program for a large network of sensors used by his organization to monitor a transcontinental gas pipeline. What term is commonly used to describe this type of sensor network?
- A.** WLAN
 - B.** VPN
 - C.** P2P
 - D.** SCADA
- 137.** This morning, Eric ran a vulnerability scan in an attempt to detect a vulnerability that was announced by a software manufacturer yesterday afternoon. The scanner did not detect the vulnerability although Eric knows that at least two of his servers should have the issue. Eric contacted the vulnerability scanning vendor, who assured him that they released a signature for the vulnerability overnight. What should Eric do as a next step?
- A.** Check the affected servers to verify a false positive.
 - B.** Check the affected servers to verify a false negative.
 - C.** Report a bug to the vendor.
 - D.** Update the vulnerability signatures.
- 138.** Natalie ran a vulnerability scan of a web application recently deployed by her organization, and the scan result reported a blind SQL injection. She reported the vulnerability to the developers, who scoured the application and made a few modifications but did not see any evidence that this attack was possible. Natalie reran the scan and received the same result. The developers are now insisting that their code is secure. What is the most likely scenario?
- A.** The result is a false positive.
 - B.** The code is deficient and requires correction.
 - C.** The vulnerability is in a different web application running on the same server.
 - D.** Natalie is misreading the scan report.

139. Kasun discovers a missing Windows security patch during a vulnerability scan of a server in his organization's data center. Upon further investigation, he discovers that the system is virtualized. Where should he apply the patch?
- A. To the virtualized system
 - B. The patch is not necessary
 - C. To the domain controller
 - D. To the virtualization platform
140. Joaquin is frustrated at the high level of false positive reports produced by his vulnerability scans and is contemplating a series of actions designed to reduce the false positive rate. Which one of the following actions is *least* likely to have the desired effect?
- A. Moving to credentialed scanning
 - B. Moving to agent-based scanning
 - C. Integrating asset information into the scan
 - D. Increasing the sensitivity of scans
141. Joe is conducting a network vulnerability scan against his datacenter and receives reports from system administrators that the scans are slowing down their systems. There are no network connectivity issues, only performance problems on individual hosts. He looks at the scan settings shown here. Which setting would be most likely to correct the problem?

Settings / Advanced

General Settings

- ☒ Enable safe checks
- ☐ Stop scanning hosts that become unresponsive during the scan
- ☐ Scan IP addresses in a random order

Performance Options

- ☐ Slow down the scan when network congestion is detected
- ☐ Use Linux kernel congestion detection

Network timeout (in seconds)

Max simultaneous checks per host

Max simultaneous hosts per scan

Max number of concurrent TCP sessions per host

Max number of concurrent TCP sessions per scan

- A. Scan IP addresses in a random order
- B. Network timeout (in seconds)
- C. Max simultaneous checks per host
- D. Max simultaneous hosts per scan

142. Isidora runs a vulnerability scan of the management interface for her organization's DNS service. She receives the vulnerability report shown here. What should be Isidora's next action?

The screenshot shows a vulnerability scan result window. The title bar reads "2 Cookie Does Not Contain The 'secure' Attribute" with a status of "port 80/tcp Active". The main content area displays the following details:

First Detected:	08/22/2020 at 20:52:54 (GMT-0400)	Last Detected:	08/23/2020 at 05:03:18 (GMT-0400)	Times Detected:	2	Last Fixed:	N/A
QID:	150122						
Category:	Web Application						
CVE ID:	-						
Vendor Reference:	-						
Bugtraq ID:	-						
Service Modified:	06/14/2020						
User Modified:	-						
Edited:	No						
PCI Vuln:	Yes						
Ticket State:							

Below the table, the "THREAT:" section states: "The cookie does not contain the 'secure' attribute."

- A. Disable the use of cookies on this service.
- B. Request that the vendor rewrite the interface to avoid this vulnerability.
- C. Investigate the contents of the cookie.
- D. Shut down the DNS service.

143. Zara is prioritizing vulnerability scans and would like to base the frequency of scanning on the information asset value. Which of the following criteria would be most appropriate for her to use in this analysis?

- A. Cost of hardware acquisition
- B. Cost of hardware replacement
- C. Types of information processed
- D. Depreciated hardware cost

144. Laura is working to upgrade her organization's vulnerability management program. She would like to add technology that is capable of retrieving the configurations of systems, even when they are highly secured. Many systems use local authentication, and she wants to avoid the burden of maintaining accounts on all of those systems. What technology should Laura consider to meet her requirement?

- A. Credentialed scanning
- B. Uncredentialed scanning
- C. Server-based scanning
- D. Agent-based scanning

145. Javier discovered the vulnerability shown here in a system on his network. He is unsure what system component is affected. What type of service is causing this vulnerability?

2 Microsoft SQL Server Compact 3.5 Service Pack 2 Not Installed			
First Detected:	02/28/2020 at 10:42:15 (GMT-0400)	Last Detected:	04/05/2020 at 04:43:21 (GMT-0400)
QID:	105487	CVSS Base:	9.3 ^[1]
Category:	Security Policy	CVSS Temporal:	6.9
CVE ID:	-	CVSS3 Base:	-
Vendor Reference:	Description of SQL Server Compact 3.5 Service Pack 2	CVSS3 Temporal:	-
Bugtraq ID:	-	CVSS Environment:	-
Service Modified:	11/04/2020	Asset Group:	-
User Modified:	-	Collateral Damage Potential:	-
Edited:	No	Target Distribution:	-
PCI Vuln:	Yes	Confidentiality Requirement:	-
Ticket State:	-	Integrity Requirement:	-
		Availability Requirement:	-

- A. Backup service
- B. Database service
- C. File sharing
- D. Web service

146. Alicia runs a vulnerability scan of a server being prepared for production and finds the vulnerability shown here. Which one of the following actions is *least* likely to reduce this risk?

4 OpenSSH AES-GCM Cipher Remote Code Execution Vulnerability	
QID:	42420
Category:	General remote services
CVE ID:	CVE-2013-4548
Vendor Reference:	gcmrkeykey.adv
Bugtraq ID:	63605
Service Modified:	06/16/2020
User Modified:	-
Edited:	No
PCI Vuln:	Yes
Ticket State:	-
<p>THREAT: OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol. A memory corruption vulnerability in post-authentication exists when the Advanced Encryption Standard (AES)-Galois/Counter Mode of Operation (GCM) cipher is used for the key exchange. When an AES-GCM cipher is used, the mm_newkeys_from_blob() function in monitor_wrap.c does not properly initialize memory for a MAC context data structure, allowing remote authenticated users to bypass intended ForceCommand and login-shell restrictions via packet data that provides a crafted callback address. The new cipher was added only in OpenSSH 6.2, released on March 22, 2020. Affected Software: OpenSSH 6.2 and OpenSSH 6.3 when built against an OpenSSL that supports AES-GCM.</p> <p>IMPACT: A remote authenticated attacker could exploit this vulnerability to execute arbitrary code in the security context of the authenticated user and may therefore allow bypassing restricted shell/command configurations.</p> <p>SOLUTION: Update to OpenSSH 6.4 (http://www.openssh.com/txt/release-6.4) to remediate this vulnerability. Workaround: As a workaround, customers may disable AES-GCM in the server configuration. The following sshd_config option will disable AES-GCM while leaving other ciphers active: Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc Patch: Following are links for downloading patches to fix the vulnerabilities: OpenSSH 6.4 (http://www.openssh.com/txt/release-6.4)</p> <p>COMPLIANCE: Not Applicable</p> <p>EXPLOITABILITY: There is no exploitability information for this vulnerability.</p> <p>ASSOCIATED MALWARE: There is no malware information for this vulnerability.</p> <p>RESULTS: SSH-2.0-OpenSSH_6.2 detected on port 22 over TCP.</p>	

- A. Block all connections on port 22.
- B. Upgrade OpenSSH.
- C. Disable AES-GCM in the server configuration.
- D. Install a network IPS in front of the server.

147. After scanning his organization's email server, Singh discovered the vulnerability shown here. What is the most effective response that Singh can take in this situation?

MEDIUM
Microsoft Exchange Client Access Server Information Di...

Description

The Microsoft Exchange Client Access Server (CAS) is affected by an information disclosure vulnerability. A remote, unauthenticated attacker can exploit this vulnerability to learn the server's internal IP address.

Solution

There is no known fix at this time.

See Also

<http://foofus.net/?p=758>

Output

```
Nessus was able to verify the issue with the following request :
GET /autodiscover/autodiscover.xml HTTP/1.0
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, */*

Which returned the following IP address :
192.168.0.111
```

Port ▼	Hosts
443 / tcp / www	

Plugin Details

Severity: Medium
ID: 77026
Version: \$Revision: 1.2 \$
Type: remote
Family: Windows
Published: 2014/08/06
Modified: 2015/09/24

Risk Information

Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P /I:N/A:N
CVSS Temporal Vector: CVSS2#E:ND/RL:U /RC:ND
CVSS Temporal Score: 5.0

Vulnerability Information

CPE: cpe:/a:microsoft:exchange_server
Exploit Available: true
Exploit Ease: Exploits are available
Vulnerability Pub Date: 2014/08/01
Exploited by Nessus: true

Reference Information

BID: 69018

- A. Upgrade to the most recent version of Microsoft Exchange.
- B. Upgrade to the most recent version of Microsoft Windows.
- C. Implement the use of strong encryption.
- D. No action is required.

148. A SQL injection exploit typically gains access to a database by exploiting a vulnerability in a(n)_____.

- A. Operating system
- B. Web application
- C. Database server
- D. Firewall

Use the following scenario to answer questions 149–151.

Ryan ran a vulnerability scan of one of his organization's production systems and received the report shown here. He would like to understand this vulnerability better and then remediate the issue.

4 Microsoft IIS Server XSS Elevation of Privilege Vulnerability (MS17-016)				CVSS: - CVSS3: - New	
First Detected:	04/04/2020 at 21:30:12 (GMT-0400)	Last Detected:	04/04/2020 at 21:30:12 (GMT-0400)	Times Detected:	1
QID:	91339	CVSS Base:	4.3	Last Fixed:	N/A
Category:	Windows	CVSS Temporal:	3.2		
CVE ID:	CVE-2017-0055	CVSS3 Base:	6.1		
Vendor Reference:	MS17-016	CVSS3 Temporal:	5.3		
Bugtraq ID:	98622	CVSS Environment:			
Service Modified:	03/17/2020	Asset Group:	-		
User Modified:	-	Collateral Damage Potential:	-		
Edited:	No	Target Distribution:	-		
PCI Vuln:	Yes	Confidentiality Requirement:	-		
Ticket State:	Open	Integrity Requirement:	-		
		Availability Requirement:	-		
THREAT:					
An elevation of privilege vulnerability exists when Microsoft IIS Server fails to properly sanitize a specially crafted request.					

149. Ryan will not be able to correct the vulnerability for several days. In the meantime, he would like to configure his intrusion prevention system to watch for issues related to this vulnerability. Which one of the following protocols would an attacker use to exploit this vulnerability?

- A. SSH
- B. HTTPS
- C. FTP
- D. RDP

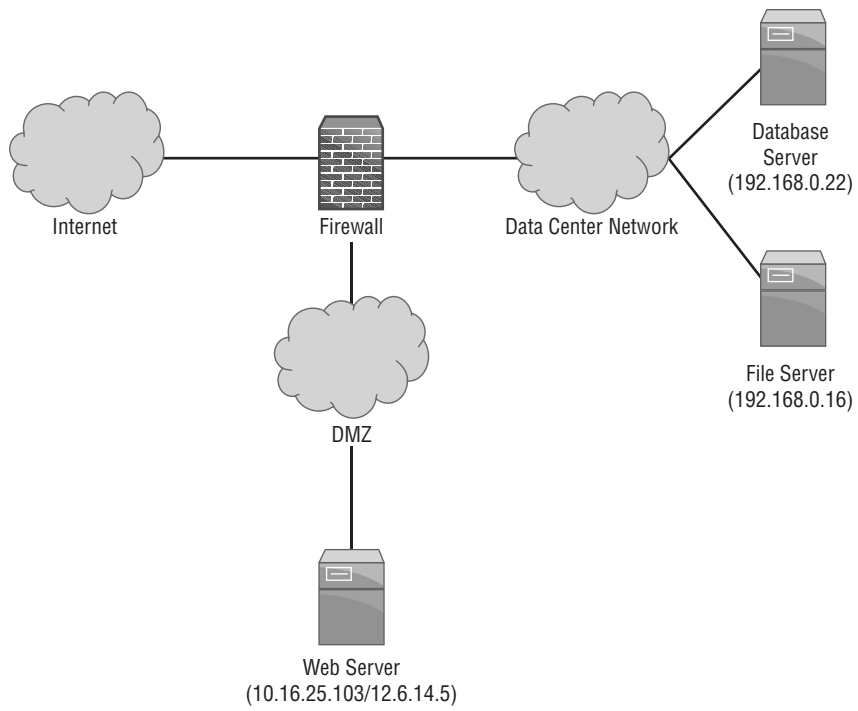
150. Which one of the following actions could Ryan take to remediate the underlying issue without disrupting business activity?

- A. Disable the IIS service.
- B. Apply a security patch.
- C. Modify the web application.
- D. Apply IPS rules.

151. If an attacker is able to exploit this vulnerability, what is the probable result that will have the highest impact on the organization?

- A. Administrative control of the server
- B. Complete control of the domain
- C. Access to configuration information
- D. Access to web application logs

152. Ted is configuring vulnerability scanning for a file server on his company’s internal network. The server is positioned on the network as shown here. What types of vulnerability scans should Ted perform to balance the efficiency of scanning effort with expected results?

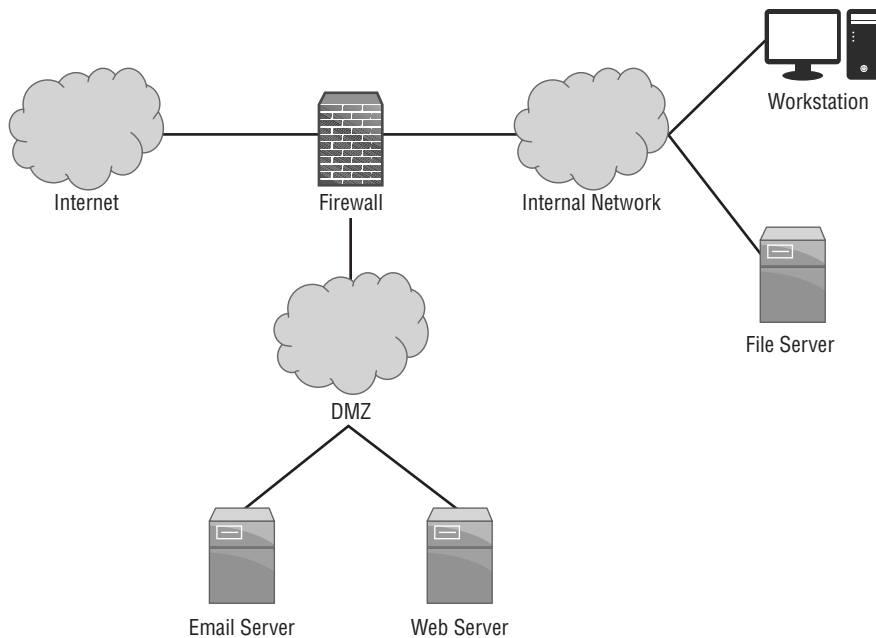


- A. Ted should not perform scans of servers on the internal network.
 - B. Ted should only perform internal vulnerability scans.
 - C. Ted should only perform external vulnerability scans.
 - D. Ted should perform both internal and external vulnerability scans.
153. Zahra is attempting to determine the next task that she should take on from a list of security priorities. Her boss told her that she should focus on activities that have the most “bang for the buck.” Of the tasks shown here, which should she tackle first?

Security Issue	Criticality	Time Required to Fix
1. Outdated ciphers on web server	Medium	6 hours
2. SQL injection vulnerability in employment application	High	3 weeks
3. Security patch to firewall	Medium	2 days
4. Complete PCI DSS audit report	Low	6 hours

- A. Task 1
- B. Task 2
- C. Task 3
- D. Task 4

- 154.** Kyong manages the vulnerability scans for his organization. The senior director that oversees Kyong's group provides a report to the CIO on a monthly basis on operational activity, and he includes the number of open critical vulnerabilities. He would like to provide this information to his director in as simple a manner as possible each month. What should Kyong do?
- A.** Provide the director with access to the scanning system.
 - B.** Check the system each month for the correct number and email it to the director.
 - C.** Configure a report that provides the information to automatically send to the director's email at the proper time each month.
 - D.** Ask an administrative assistant to check the system and provide the director with the information.
- 155.** Morgan is interpreting the vulnerability scan from her organization's network, shown here. She would like to determine which vulnerability to remediate first. Morgan would like to focus on vulnerabilities that are most easily exploitable by someone outside her organization. Assuming the firewall is properly configured, which one of the following vulnerabilities should Morgan give the highest priority?



- A.** Severity 5 vulnerability in the workstation
- B.** Severity 1 vulnerability in the file server
- C.** Severity 5 vulnerability in the web server
- D.** Severity 1 vulnerability in the mail server

156. Mike runs a vulnerability scan against his company's virtualization environment and finds the vulnerability shown here in several of the virtual hosts. What action should Mike take?

INFO HTTP Methods Allowed (per directory) < >

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

- A. No action is necessary because this is an informational report.
 - B. Mike should disable HTTP on the affected devices.
 - C. Mike should upgrade the version of OpenSSL on the affected devices.
 - D. Mike should immediately upgrade the hypervisor.
157. Juan recently scanned a system and found that it was running services on ports 139 and 445. What operating system is this system most likely running?
- A. Ubuntu
 - B. MacOS
 - C. CentOS
 - D. Windows
158. Gene is concerned about the theft of sensitive information stored in a database. Which one of the following vulnerabilities would pose the most direct threat to this information?
- A. SQL injection
 - B. Cross-site scripting
 - C. Buffer overflow
 - D. Denial of service
159. Which one of the following protocols is not likely to trigger a vulnerability scan alert when used to support a virtual private network (VPN)?
- A. IPsec
 - B. SSL v2
 - C. PPTP
 - D. SSL v3

160. Rahul ran a vulnerability scan of a server that will be used for credit card processing in his environment and received a report containing the vulnerability shown here. What action must Rahul take?

2 Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability

First Detected: 02/16/2020 at 12:59:07 (GMT-0400)	Last Detected: 04/05/2020 at 05:08:25 (GMT-0400)	Times Detected: 25	Last Fixed: N/A
--	---	---------------------------	------------------------

QID: 86473	CVSS Base: 5.8
Category: Web server	CVSS Temporal: 5
CVE ID: CVE-2004-2320 CVE-2007-3008	CVSS3 Base: -
Vendor Reference: -	CVSS3 Temporal: -
Bugtraq ID: 24456 9506	CVSS Environment: -
Service Modified: 08/20/2020	Asset Group: -
User Modified: -	Collateral Damage Potential: -
Edited: No	Target Distribution: -
PCI Vuln: Yes	Confidentiality Requirement: -
Ticket State: -	Integrity Requirement: -
	Availability Requirement: -

THREAT:
A Web server was detected that supports the HTTP TRACE method. This method allows debugging and connection trace analysis for connections from the client to the Web server. Per the HTTP information sent to it by the client unmodified and unfiltered. Microsoft IIS web server uses an alias TRACK for this method, and is functionally the same.
A vulnerability related to this method was discovered. A malicious, active component in a Web page can send Trace requests to a Web server that supports this Trace method. Usually, browser sends requests to a Web server, but in this case, the browser sends requests to the Web server that supports this Trace method. Although unlikely and difficult to achieve, it's possible, in the presence of other browser vulnerabilities, for the active HTML content to make external requests to arbitrary Web servers beyond the host. The request is sent to the Web server, and the response also includes cookie-based or Web-based (if logged on) authentication credentials that the browser automatically sent to the specified Web application on the server. The significance of the Trace capability in this vulnerability is that the active component in the page visited by the victim user has no direct access to this authentication information, but gets it after the request is sent to the Web server. Since this vulnerability exists as a support for a method required by the HTTP protocol specification, most common Web servers are vulnerable. The exact method(s) supported, Trace and/or Track, and their responses are in the Results section below. Track / Trace are required to be disabled to be PCI compliance.

IMPACT:
If this vulnerability is successfully exploited, users of the Web server may lose their authentication credentials for the server and/or for the Web applications hosted by the server to an attacker. This can lead to scripting attacks due to input validation errors.

- A. Remediate the vulnerability when possible.
- B. Remediate the vulnerability prior to moving the system into production and rerun the scan to obtain a clean result.
- C. Remediate the vulnerability within 90 days of moving the system to production.
- D. No action is required.

Use the following scenario to answer questions 161–162.

Aaron is scanning a server in his organization's data center and receives the vulnerability report shown here. The service is exposed only to internal hosts.

2 NTP Information Disclosure Vulnerability port 123/udp CVSS: - CVSS3: - Active

First Detected: 03/16/2020 at 20:06:22 (GMT-0400)	Last Detected: 04/04/2020 at 23:18:46 (GMT-0400)	Times Detected: 54	Last Fixed: N/A
--	---	---------------------------	------------------------

QID: 38293	CVSS Base: 2.6
Category: General remote services	CVSS Temporal: 2.1
CVE ID: -	CVSS3 Base: -
Vendor Reference: -	CVSS3 Temporal: -
Bugtraq ID: -	CVSS Environment: -
Service Modified: 06/06/2020	Asset Group: -
User Modified: -	Collateral Damage Potential: -
Edited: No	Target Distribution: -
PCI Vuln: No	Confidentiality Requirement: -
Ticket State: -	Integrity Requirement: -
	Availability Requirement: -

THREAT:
The NTP service running on the host allows queries of NTP variables.

IMPACT:
A remote user can obtain sensitive information about the host by querying various variables. The information obtained can aid in further attacks against the system.

SOLUTION:
Please reconfigure NTP to restrict remote access.
If you require assistance in configuring NTP, please refer to your vendor. For an overview of NTP service access restrictions, please see this [NTP access restrictions](#).

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

- 161.** What is the normal function of the service with this vulnerability?
- File transfer
 - Web hosting
 - Time synchronization
 - Network addressing
- 162.** What priority should Aaron place on remediating this vulnerability?
- Aaron should make this vulnerability his highest priority.
 - Aaron should remediate this vulnerability urgently but does not need to drop everything.
 - Aaron should remediate this vulnerability within the next month.
 - Aaron does not need to assign any priority to remediating this vulnerability.
- 163.** Without access to any additional information, which one of the following vulnerabilities would you consider the most severe if discovered on a production web server?
- CGI generic SQL injection
 - Web application information disclosure
 - Web server uses basic authentication without HTTPS
 - Web server directory enumeration
- 164.** Gina ran a vulnerability scan on three systems that her organization is planning to move to production and received the results shown here. How many of these issues should Gina require be resolved before moving to production?

10.32		HP iLO
Vulnerabilities (5)		
4	RPC Mountd Allows Remote Anonymous File System Root Mount	CVSS: - CVSS3: - Fixed
3	SSL/TLS use of weak RC4 cipher	port 443/tcp over SSL CVSS: - CVSS3: - Fixed
3	SSL/TLS Server supports TLSv1.0	port 443/tcp over SSL CVSS: - CVSS3: - Fixed
3	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	port 443/tcp over SSL CVSS: - CVSS3: - Fixed
3	SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST)	port 443/tcp over SSL CVSS: - CVSS3: - Fixed
10.32		Virtualized Linux Guest
Vulnerabilities (2)		
3	SSL/TLS Server supports TLSv1.0	port 50000/tcp over SSL CVSS: - CVSS3: - Fixed
3	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	port 50000/tcp over SSL CVSS: - CVSS3: - Fixed
10.32		Virtualized Linux Guest
Vulnerabilities (2)		
3	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	port 50000/tcp over SSL CVSS: - CVSS3: - Fixed
3	SSL/TLS Server supports TLSv1.0	port 50000/tcp over SSL CVSS: - CVSS3: - Fixed

- 0
- 1
- 3
- All of these issues should be resolved

165. Ji-won recently restarted an old vulnerability scanner that had not been used in more than a year. She booted the scanner, logged in, and configured a scan to run. After reading the scan results, she found that the scanner was not detecting known vulnerabilities that were detected by other scanners. What is the most likely cause of this issue?
- The scanner is running on an outdated operating system.
 - The scanner's maintenance subscription is expired.
 - Ji-won has invalid credentials on the scanner.
 - The scanner does not have a current, valid IP address.
166. Isabella runs both internal and external vulnerability scans of a web server and detects a possible SQL injection vulnerability. The vulnerability only appears in the internal scan and does not appear in the external scan. When Isabella checks the server logs, she sees the requests coming from the internal scan and sees some requests from the external scanner but no evidence that a SQL injection exploit was attempted by the external scanner. What is the most likely explanation for these results?
- A host firewall is blocking external network connections to the web server.
 - A network firewall is blocking external network connections to the web server.
 - A host IPS is blocking some requests to the web server.
 - A network IPS is blocking some requests to the web server.
167. Rick discovers the vulnerability shown here in a server running in his datacenter. What characteristic of this vulnerability should concern him the most?

4 Microsoft Security Update for Windows Kernel-Mode Drivers (MS17-018) CVSS: - CVSS3: - New

First Detected: 04/05/2020 at 01:18:07 (GMT-0400)	Last Detected: 04/05/2020 at 01:18:07 (GMT-0400)	Times Detected: 1	Last Fixed: N/A
--	---	--------------------------	------------------------

QID: 91342	CVSS Base: 7.2
Category: Windows	CVSS Temporal: 5.3
CVE ID: CVE-2017-0024 CVE-2017-0026 CVE-2017-0056 CVE-2017-0078 CVE-2017-0079 CVE-2017-0080 CVE-2017-0081 CVE-2017-0082	CVSS3 Base: 7.8
	CVSS3 Temporal: 6.8
	CVSS Environment:
Vendor Reference: MS17-018	Asset Group: -
Bugtraq ID: 96029, 96032, 96630, 96631, 96632, 96633, 96634	Collateral Damage Potential: -
Service Modified: 03/17/2020	Confidentiality Distribution: -
User Modified: -	Confidentiality Requirement: -
Edited: No	Integrity Requirement: -
PCI Vuln: Yes	Availability Requirement: -
Ticket State: Open	

THREAT:
Multiple elevation of privilege vulnerabilities exist in Windows when the Windows kernel-mode driver fails to properly handle objects in memory. The update addresses the vulnerabilities by correcting how the Windows kernel-mode driver handles objects in memory. This security update is rated Important for all supported releases of Microsoft Windows.

IMPACT:
The vulnerabilities could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application that could exploit the vulnerabilities and take control of an affected system.

SOLUTION:
Customers are advised to refer to [MS17-018](#) for more information.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
[MS17-018: Windows](#)

EXPLOITABILITY:
There is no exploitability information for this vulnerability.

- It is the subject of a recent security bulletin.
- It has a CVSS score of 7.6.
- There are multiple Bugtraq and CVE IDs.
- It affects kernel-mode drivers.

168. Carla is designing a vulnerability scanning workflow and has been tasked with selecting the person responsible for remediating vulnerabilities. Which one of the following people would normally be in the *best* position to remediate a server vulnerability?
- A. Cybersecurity analyst
 - B. System administrator
 - C. Network engineer
 - D. IT manager
169. During a recent vulnerability scan, Ed discovered that a web server running on his network has access to a database server that should be restricted. Both servers are running on his organization's VMware virtualization platform. Where should Ed look first to configure a security control to restrict this access?
- A. VMware
 - B. Datacenter firewall
 - C. Perimeter (Internet) firewall
 - D. Intrusion prevention system
170. Carl runs a vulnerability scan of a mail server used by his organization and receives the vulnerability report shown here. What action should Carl take to correct this issue?

4 OpenSSL oracle padding vulnerability(CVE-2016-2107) port 443/tcp over SSL Active

First Detected:	08/22/2016 at 20:52:54 (GMT-0400)	Last Detected:	08/26/2016 at 05:02:18 (GMT-0400)	Times Detected:	5	Last Fixed:	N/A
QID:	38626						
Category:	General remote services						
CVE ID:	CVE-2016-2107						
Vendor Reference:	OpenSSL Security Advisory 20160503						
Bugtraq ID:	91787, 89760						
Service Modified:	05/24/2016						
User Modified:	-						
Edited:	No						
PCI Vuln:	No						
Ticket State:							

THREAT:

The OpenSSL Project is an Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols as well as a general purpose cryptography library.

OpenSSL contains the following vulnerability:

A MITM attacker can use a padding oracle attack to decrypt traffic when the connection uses an AES CBC cipher and the server support AES-NI. Affected Versions:

OpenSSL 1.0.2 prior to OpenSSL 1.0.2h OpenSSL 1.0.1 prior to OpenSSL 1.0.1t

- A. Carl does not need to take any action because this is an informational report.
 - B. Carl should replace SSL with TLS on this server.
 - C. Carl should disable weak ciphers.
 - D. Carl should upgrade OpenSSL.
171. Renee is configuring a vulnerability scanner that will run scans of her network. Corporate policy requires the use of daily vulnerability scans. What would be the best time to configure the scans?
- A. During the day when operations reach their peak to stress test systems
 - B. During the evening when operations are minimal to reduce the impact on systems

- C. During lunch hour when people have stepped away from their systems but there is still considerable load
- D. On the weekends when the scans may run unimpeded

172. Ahmed is reviewing the vulnerability scan report from his organization's central storage service and finds the results shown here. Which action can Ahmed take that will be effective in remediating the highest-severity issue possible?

NetApp Release 8.1.4P3 7-Mode			
Vulnerabilities (22)			
5	EOL/Obsolete Software: SNMP Version Detected	CVSS: - CVSS3: -	Active
3	NetBIOS Shared Folder List Available	CVSS: - CVSS3: -	Active
3	NFS Exported Filesystems List Vulnerability	CVSS: - CVSS3: -	Active
3	SSL Server Has SSLv3 Enabled Vulnerability	port 443/tcp over SSL CVSS: - CVSS3: -	Active
3	SSL Server Has SSLv2 Enabled Vulnerability	port 443/tcp over SSL CVSS: - CVSS3: -	Active
3	SSL/TLS use of weak RC4 cipher	port 443/tcp over SSL CVSS: - CVSS3: -	Active
3	Readable SNMP Information	port 161/udp CVSS: - CVSS3: -	Active
2	NetBIOS Name Accessible	CVSS: - CVSS3: -	Active
2	Hidden RPC Services	CVSS: - CVSS3: -	Active
2	YP/NIS RPC Services Listening on Non-Privileged Ports	CVSS: - CVSS3: -	Active
2	Default Windows Administrator Account Name Present	CVSS: - CVSS3: -	Active
2	SSL Certificate - Server Public Key Too Small	port 443/tcp over SSL CVSS: - CVSS3: -	Active
2	SSL Certificate - Self-Signed Certificate	port 443/tcp over SSL CVSS: - CVSS3: -	Active
2	SSL Certificate - Subject Common Name Does Not Match Server FQDN	port 443/tcp over SSL CVSS: - CVSS3: -	Active
2	SSL Certificate - Signature Verification Failed Vulnerability	port 443/tcp over SSL CVSS: - CVSS3: -	Active
2	SSL Certificate - Improper Usage Vulnerability	port 443/tcp over SSL CVSS: - CVSS3: -	Active
2	NTP Information Disclosure Vulnerability	port 123/udp CVSS: - CVSS3: -	Active
1	Non-Zero Padding Bytes Observed in Ethernet Packets	CVSS: - CVSS3: -	Active
1	mountd RPC Daemon Discloses Exported Directories Accessed by Remote Hosts	CVSS: - CVSS3: -	Active
1	"rquotad" RPC Service Present	CVSS: - CVSS3: -	Active
1	Presence of a Load-Balancing Device Detected	port 80/tcp CVSS: - CVSS3: -	Active
1	Presence of a Load-Balancing Device Detected	port 443/tcp over SSL CVSS: - CVSS3: -	Re-Opened

- A. Upgrade to SNMP v3.
- B. Disable the use of RC4.
- C. Replace the use of SSL with TLS.
- D. Disable remote share enumeration.

Use the following scenario to answer questions 173–174.

Glenda ran a vulnerability scan of workstations in her organization. She noticed that many of the workstations reported the vulnerability shown here. She would like to not only correct this issue but also prevent the likelihood of similar issues occurring in the future.

4 Google Chrome Prior to 57.0.2987.133 Multiple Vulnerabilities

CVSS: - CVSS3: - New

First Detected:	04/05/2020 at 03:39:44 (GMT-0400)	Last Detected:	04/05/2020 at 03:39:44 (GMT-0400)	Times Detected:	1	Last Fixed:	N/A
QID:	370356	CVSS Base:	9.3				
Category:	Local	CVSS Temporal:	8.9				
CVE ID:	CVE-2017-5054 CVE-2017-5052 CVE-2017-5056 CVE-2017-5053 CVE-2017-5055	CVSS3 Base:	-				
		CVSS3 Temporal:	-				
Vendor Reference	Google Chrome	CVSS Environment:	-				
Bugtraq ID:	-	Asset Group:	-				
Service Modified:	04/09/2020	Collateral Damage Potential:	-				
User Modified:	-	Target Distribution:	-				
Edited:	No	Confidentiality Requirement:	-				
PCI Vuln:	Yes	Integrity Requirement:	-				
Ticket State:	Open	Availability Requirement:	-				

THREAT:

Google Chrome is a web browser for multiple platforms developed by Google.

This Google Chrome update fixes the following vulnerabilities:

- CVE-2017-5054: Heap buffer overflow in V8.
- CVE-2017-5052: Bad cast in Blink.
- CVE-2017-5056: Use after free in Blink.
- CVE-2017-5053: Out of bounds memory access in V8.
- CVE-2017-5055: Use after free in printing.

IMPACT:

A web page containing malicious content could cause Chromium to crash, execute arbitrary code, or disclose sensitive information when visited by the victim.

SOLUTION:

Customers are advised to upgrade to [Google Chrome 57.0.2987.133](#) or a later version.

Patch:

Following are links for downloading patches to fix the vulnerabilities:

- [Google Chrome: Windows](#)
- [Google Chrome: MAC OS X](#)

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

173. What action should Glenda take to achieve her goals?
- Glenda should uninstall Chrome from all workstations and replace it with Internet Explorer.
 - Glenda should manually upgrade Chrome on all workstations.
 - Glenda should configure all workstations to automatically upgrade Chrome.
 - Glenda does not need to take any action.
174. What priority should Glenda place on remediating this vulnerability?
- Glenda should make this vulnerability her highest priority.
 - Glenda should remediate this vulnerability urgently but does not need to drop everything.
 - Glenda should remediate this vulnerability within the next several months.
 - Glenda does not need to assign any priority to remediating this vulnerability.
175. After reviewing the results of a vulnerability scan, Gabriella discovered a flaw in her Oracle database server that may allow an attacker to attempt a direct connection to the server. She would like to review NetFlow logs to determine what systems have connected to the server recently. What TCP port should Gabriella expect to find used for this communication?
- 443
 - 1433
 - 1521
 - 8080

176. Greg runs a vulnerability scan of a server in his organization and finds the results shown here. What is the most likely explanation for these results?

INFO

HTTP Server Type and Version

Description

This plugin attempts to determine the type and the version of the remote web server.

Output

The remote web server type is :
Microsoft-IIS/6.0

Port

Hosts

80 / tcp / www	
443 / tcp / www	
2025 / tcp / www	
2026 / tcp / www	
2027 / tcp / www	
2028 / tcp / www	
2029 / tcp / www	
2030 / tcp / www	
2031 / tcp / www	
2032 / tcp / www	
2033 / tcp / www	
2034 / tcp / www	
2035 / tcp / www	

Plugin Details

Severity: Info
ID: 10107
Version: \$Revision: 1.120 \$
Type: remote
Family: Web Servers
Published: 2000/01/04
Modified: 2014/08/01

Risk Information

Risk Factor: None

- A. The organization is running web services on nonstandard ports.
 - B. The scanner is providing a false positive error report.
 - C. The web server has mirrored ports available.
 - D. The server has been compromised by an attacker.
177. Binh is reviewing a vulnerability scan of his organization’s VPN appliance. He wants to remove support for any insecure ciphers from the device. Which one of the following ciphers should he remove?
- A. ECDHE-RSA-AES128-SHA256
 - B. AES256-SHA256
 - C. DHE-RSA-AES256-GCM-SHA384
 - D. EDH-RSA-DES-CBC3-SHA

178. Terry recently ran a vulnerability scan against his organization's credit card processing environment that found a number of vulnerabilities. Which vulnerabilities must he remediate in order to have a "clean" scan under PCI DSS standards?
- A. Critical vulnerabilities
 - B. Critical and high vulnerabilities
 - C. Critical, high, and moderate vulnerabilities
 - D. Critical, high, moderate, and low vulnerabilities
179. Himari discovers the vulnerability shown here on several Windows systems in her organization. There is a patch available, but it requires compatibility testing that will take several days to complete. What type of file should Himari be watchful for because it may directly exploit this vulnerability?

4 Microsoft Windows PNG Processing Information Disclosure Vulnerability (MS15-024)			
First Detected:	09/28/2020 at 10:42:15 (GMT-0400)	Last Detected:	04/04/2020 at 19:22:26 (GMT-0400)
Times Detected:	20		
QID:	91026	CVSS Base:	4.3
Category:	Windows	CVSS Temporal:	3.4
CVE ID:	CVE-2015-0080	CVSS3 Base:	-
Vendor Reference	MS15-024	CVSS3 Temporal:	-
Bugtraq ID:	72909	CVSS Environment:	-
Service Modified:	03/11/2020	Asset Group:	-
User Modified:	-	Collateral Damage Potential:	-
Edited:	No	Target Distribution:	-
PCI Vuln:	Yes	Confidentiality Requirement:	-
Ticket State:	Open	Integrity Requirement:	-
		Availability Requirement:	-

- A. Private key files
 - B. Word documents
 - C. Image files
 - D. Encrypted files
180. During a vulnerability scan, Patrick discovered that the configuration management agent installed on all of his organization's Windows servers contains a serious vulnerability. The manufacturer is aware of this issue, and a patch is available. What process should Patrick follow to correct this issue?
- A. Immediately deploy the patch to all affected systems.
 - B. Deploy the patch to a single production server for testing and then deploy to all servers if that test is successful.
 - C. Deploy the patch in a test environment and then conduct a staged rollout in production.
 - D. Disable all external access to systems until the patch is deployed.

- 181.** Aaron is configuring a vulnerability scan for a Class C network and is trying to choose a port setting from the list shown here. He would like to choose a scan option that will efficiently scan his network but also complete in a reasonable period of time. Which setting would be most appropriate?

A screenshot of a configuration window for a vulnerability scan. It contains several radio button options: 'None' (selected), 'Full', 'Standard Scan (about 1900 ports)' with a 'View list' link, and 'Light Scan (about 160 ports)' with a 'View list' link. Below these is an unchecked checkbox labeled 'Additional' and a text input field. At the bottom, there is a small example text '(ex: 1-1024, 8080)'.

- A. None
 - B. Full
 - C. Standard Scan
 - D. Light Scan
- 182.** Haruto is reviewing the results of a vulnerability scan, shown here, from a web server in his organization. Access to this server is restricted at the firewall so that it may not be accessed on port 80 or 443. Which of the following vulnerabilities should Haruto still address?

▼ Vulnerabilities (6)		
▶	5	EOL/Obsolete Software: OpenSSL 0.9.8/1.0.0 Detected
▶	3	Apache HTTP Server HttpOnly Cookie Information Disclosure Vulnerability
▶	3	HTTP TRACE / TRACK Methods Enabled
▶	2	Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability
▶	1	Apache Web Server ETag Header Information Disclosure Weakness
▶	1	Presence of a Load-Balancing Device Detected

- A. OpenSSL version
 - B. Cookie information disclosure
 - C. TRACK/TRACE methods
 - D. Haruto does not need to address any of these vulnerabilities because they are not exposed to the outside world
- 183.** Brian is considering the use of several different categories of vulnerability plug-ins. Of the types listed here, which is the most likely to result in false positive reports?
- A. Registry inspection
 - B. Banner grabbing
 - C. Service interrogation
 - D. Fuzzing

184. Binh conducts a vulnerability scan and finds three different vulnerabilities, with the CVSS scores shown here. Which vulnerability should be his highest priority to fix, assuming all three fixes are of equal difficulty?

Vulnerability 1

CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Vulnerability 2

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Vulnerability 3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

- A. Vulnerability 1
 - B. Vulnerability 2
 - C. Vulnerability 3
 - D. Vulnerabilities 1 and 3 are equal in priority
185. Which one of the following is not an appropriate criterion to use when prioritizing the remediation of vulnerabilities?
- A. Network exposure of the affected system
 - B. Difficulty of remediation
 - C. Severity of the vulnerability
 - D. All of these are appropriate.
186. Landon is preparing to run a vulnerability scan of a dedicated Apache server that his organization is planning to move into a DMZ. Which one of the following vulnerability scans is *least* likely to provide informative results?
- A. Web application vulnerability scan
 - B. Database vulnerability scan
 - C. Port scan
 - D. Network vulnerability scan

187. Ken recently received the vulnerability report shown here that affects a file server used by his organization. What is the primary nature of the risk introduced by this vulnerability?

3 NetBIOS Name Conflict Vulnerability			
First Detected:	02/04/2020 at 21:06:51 (GMT-0400)	Last Detected:	04/04/2020 at 21:22:12 (GMT-0400)
CVSS Base:	5	Times Detected:	3
CVSS Temporal:	4.1	Last Fixed:	N/A
Category:	SMB / NETBIOS	CVSS3 Base:	-
CVE ID:	CVE-2020-0673	CVSS3 Temporal:	-
Vendor Reference:	MS00-047	CVSS3 Environment:	-
Bugtraq ID:	1514, 1515	Asset Group:	-
Service Modified:	03/17/2020	Collateral Damage Potential:	-
User Modified:	-	Target Distribution:	-
Edited:	No	Confidentiality Requirement:	-
PCI Vuln:	Yes	Integrity Requirement:	-
Ticket State:	-	Availability Requirement:	-
THREAT: A malicious user can send a NetBIOS Name Conflict message to the NetBIOS name service even when the receiving machine is not in the process of registering its NetBIOS name. As a result, attempts, which could lead to intermittent connectivity problems, or the loss of all NetBIOS functionality. This is a design flaw problem in the NetBIOS protocol and the WINS dynamic name registration, which is present whenever WINS is supported.			
IMPACT: If successfully exploited, this vulnerability could lead to intermittent connectivity problems, or the loss of all NetBIOS functionality.			
SOLUTION: The best workaround for Microsoft Windows and Samba Server is to block all incoming traffic from the Internet to UDP ports 137 and 138. For Windows platforms, microsoft has released some patches to address this issue. Microsoft has released a patch (Hotfix 269239). After the patch is applied, conflict messages will only be responded to during the initial name registration process. For more information on this vulnerability, Hotfix 269239 mitigates the issue by generating log events for detected name conflicts. Note that while Hotfix 269239 provides notification when name conflicts occur, the system remains vulnerable. The following is a list of Microsoft patches: Microsoft Windows NT 4.0 patch Q269239 Microsoft Windows NT Terminal Server patch Q269239 Microsoft Windows 2000 patch Q269239_W2K_SP2_x86_en For Samba there are no vendor supplied patches available at this time.			

- A. Confidentiality
 - B. Integrity
 - C. Availability
 - D. Nonrepudiation
188. Aadesh is creating a vulnerability management program for his company. He has limited scanning resources and would like to apply them to different systems based on the sensitivity and criticality of the information that they handle. What criteria should Aadesh use to determine the vulnerability scanning frequency?
- A. Data remanence
 - B. Data privacy
 - C. Data classification
 - D. Data privacy
189. Tom recently read a media report about a ransomware outbreak that was spreading rapidly across the Internet by exploiting a zero-day vulnerability in Microsoft Windows. As part of a comprehensive response, he would like to include a control that would allow his organization to effectively recover from a ransomware infection. Which one of the following controls would best achieve Tom's objective?
- A. Security patching
 - B. Host firewalls
 - C. Backups
 - D. Intrusion prevention systems

190. Kaitlyn discovered the vulnerability shown here on a workstation in her organization. Which one of the following is not an acceptable method for remediating this vulnerability?

3 WinRAR Insecure Executable Loading Remote Code Execution Vulnerability CVSS: - CVSS3: - Active

First Detected:	12/04/2020 at 19:06:20 (GMT-0400)	Last Detected:	04/04/2020 at 20:54:02 (GMT-0400)	Times Detected:	5	Last Fixed:	N/A
QID:	370233	CVSS Base:	3.7				
Category:	Local	CVSS Temporal:	3.1				
CVE ID:	CVE-2015-5663	CVSS3 Base:	-				
Vendor Reference:	-	CVSS3 Temporal:	-				
Bugtraq ID:	79566	CVSS Environment:	-				
Service Modified:	11/28/2020	Asset Group:	-				
User Modified:	-	Collateral Damage Potential:	-				
Edited:	No	Target Distribution:	-				
PCI Vuln:	No	Confidentiality Requirement:	-				
Ticket State:	-	Integrity Requirement:	-				
		Availability Requirement:	-				

THREAT:
WinRAR is a shareware file archiver and compressor utility for Windows. It can create archives in RAR or ZIP file formats and unpack numerous archive file formats. The file-execution functionality in WinRAR allows local users to escalate privileges via a Trojan horse file with a name similar to an extensionless filename.
Affected Versions:
WinRAR prior to 5.30 Beta 5

- A. Upgrade WinRAR
 - B. Upgrade Windows
 - C. Remove WinRAR
 - D. Replace WinRAR with an alternate compression utility
191. Brent ran a vulnerability scan of several network infrastructure devices on his network and obtained the result shown here. What is the extent of the impact that an attacker could have by exploiting this vulnerability directly?

3 Readable SNMP Information

First Detected:	07/16/2020 at 20:06:22 (GMT-0400)	Last Detected:	08/05/2020 at 04:15:02 (GMT-0400)	Times Detected:	23	Last Fixed:	10/04/2020 at 18:05:16 (GMT-0400)
QID:	78030	CVSS Base:	10				
Category:	SNMP	CVSS Temporal:	9				
CVE ID:	CVE-1999-0517 CVE-1999-0186 CVE-1999-0254 CVE-1999-0516 CVE-1999-0472 CVE-2001-0914 CVE-2002-0109	CVSS3 Base:	-				
Vendor Reference:	-	CVSS3 Temporal:	-				
Bugtraq ID:	3797 , 2896 , 3795	CVSS Environment:	-				
Service Modified:	05/22/2020	Asset Group:	-				
User Modified:	-	Collateral Damage Potential:	-				
Edited:	No	Target Distribution:	-				
PCI Vuln:	Yes	Confidentiality Requirement:	-				
Ticket State:	-	Integrity Requirement:	-				
		Availability Requirement:	-				

THREAT:
Unauthorized users can read all SNMP information because the access password is not secure.

- A. Denial of service
 - B. Theft of sensitive information
 - C. Network eavesdropping
 - D. Reconnaissance
192. Yashvir runs the cybersecurity vulnerability management program for his organization. He sends a database administrator a report of a missing database patch that corrects a high severity security issue. The DBA writes back to Yashvir that he has applied the patch. Yashvir reruns the scan, and it still reports the same vulnerability. What should he do next?
- A. Mark the vulnerability as a false positive.
 - B. Ask the DBA to recheck the database.
 - C. Mark the vulnerability as an exception.
 - D. Escalate the issue to the DBA's manager.

193. Manya is reviewing the results of a vulnerability scan and identifies the issue shown here in one of her systems. She consults with developers who check the code and assure her that it is not vulnerable to SQL injection attacks. An independent auditor confirms this for Manya. What is the most likely scenario?

HIGH
CGI Generic SQL Injection (blind, time based)
>

Description

By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a slower response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database.

An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

Note that this script is experimental and may be prone to false positives.

Solution

Modify the affected CGI scripts so that they properly escape arguments.

- A. This is a false positive report.
- B. The developers are wrong, and the vulnerability exists.
- C. The scanner is malfunctioning.
- D. The database server is misconfigured.
194. Erik is reviewing the results of a vulnerability scan and comes across the vulnerability report shown here. Which one of the following services is *least* likely to be affected by this vulnerability?

2 X.509 Certificate MD5 Signature Collision Vulnerability

First Detected: 03/11/2020 at 22:38:17 (GMT-0400)	Last Detected: 12/05/2020 at 03:35:56 (GMT-0400)	Times Detected: 86	Last Fixed: 04/05/2020 at 01:21:47 (GMT-0400)
QID: 42012	CVSS Base: 5		
Category: General remote services	CVSS Temporal: 4.3		
CVE ID: CVE-2004-2761	CVSS3 Base: -		
Vendor Reference: -	CVSS3 Temporal: -		
Bugtraq ID: 33055	CVSS Environment: -		
Service Modified: 09/17/2020	Asset Group: -		
User Modified: -	Collateral Damage Potential: -		
Edited: No	Target Distribution: -		
PCI Vuln: Yes	Confidentiality Requirement: -		
Ticket State: -	Integrity Requirement: -		
	Availability Requirement: -		

THREAT:

Hash algorithms are used to generate a hash value for a message (an arbitrary block of data) such that a number of cryptographic properties hold. In particular it is expected to be resistant to collisions, that is the m' such that both have the same hash value.

- A. HTTPS
- B. HTTP
- C. SSH
- D. VPN

Use the following scenario to answer questions 195–196.

Larry recently discovered a critical vulnerability in one of his organization's database servers during a routine vulnerability scan. When he showed the report to a database administrator, the administrator responded that they had corrected the vulnerability by using a vendor-supplied workaround because upgrading the database would disrupt an important process. Larry verified that the workaround is in place and corrects the vulnerability.

195. How should Larry respond to this situation?
- Mark the report as a false positive.
 - Insist that the administrator apply the vendor patch.
 - Mark the report as an exception.
 - Require that the administrator submit a report describing the workaround after each vulnerability scan.
196. What is the most likely cause of this report?
- The vulnerability scanner requires an update.
 - The vulnerability scanner depends on version detection.
 - The database administrator incorrectly applied the workaround.
 - Larry misconfigured the scan.
197. Mila ran a vulnerability scan of a server in her organization and found the vulnerability shown here. What is the use of the service affected by this vulnerability?

LOW

POP3 Cleartext Logins Permitted

Description

The remote host is running a POP3 daemon that allows cleartext logins over unencrypted connections. An attacker can uncover user names and passwords by sniffing traffic to the POP3 daemon if a less secure authentication mechanism (eg, USER command, AUTH PLAIN, AUTH LOGIN) is used.

Solution

Contact your vendor for a fix or encrypt traffic with SSL / TLS using stunnel.

See Also

<http://tools.ietf.org/html/rfc2222>
<http://tools.ietf.org/html/rfc2595>

Output

The following cleartext methods are supported :

USER
SASL PLAIN LOGIN

Port ▼	Hosts
110 / tcp / pop3	

Plugin Details

Severity:

Low

ID:

15855

Version:

\$Revision: 1.20 \$

Type:

remote

Family:

Misc.

Published:

2004/11/30

Modified:

2015/06/23

Risk Information

Risk Factor:

Low

CVSS Base Score:

2.6

CVSS Vector:

CVSS2#AV:N/AC:H/Au:N/C:P/!N/A:N

- Web server
 - Database server
 - Email server
 - Directory server
198. Margot discovered that a server in her organization has a SQL injection vulnerability. She would like to investigate whether attackers have attempted to exploit this vulnerability. Which one of the following data sources is *least* likely to provide helpful information?

- A. NetFlow logs
- B. Web server logs
- C. Database logs
- D. IDS logs

199. Krista is reviewing a vulnerability scan report and comes across the vulnerability shown here. She comes from a Linux background and is not as familiar with Windows administration. She is not familiar with the runas command mentioned in this vulnerability. What is the closest Linux equivalent command?

3

Microsoft Windows "RunAs" Password Length Local Information Disclosure - Zero Day

First Detected:	04/04/2020 at 18:02:25 (GMT-0400)	Last Detected:	04/05/2020 at 02:19:36 (GMT-0400)	Times Detected:	21	Last Fixed:	N/A
QID:	116157	CVSS Base:	4				
Category:	Local	CVSS Temporal:	3.4				
CVE ID:	CVE-2009-0320	CVSS3 Base:	-				
Vendor Reference	-	CVSS3 Temporal:	-				
Bugtraq ID:	33440	CVSS Environment:	-				
Service Modified:	09/04/2020	Asset Group:	-				
User Modified:	-	Collateral Damage Potential:	-				
Edited:	No	Target Distribution:	-				
PCI Vuln:	Yes	Confidentiality Requirement:	-				
Ticket State:		Integrity Requirement:	-				
		Availability Requirement:	-				

THREAT:
RunAs is a service component for Windows, which can be used to execute a second application as a different user, generally for performing privileged operations. RunAs is prone to a local password disclosure vulnerability that allows a malicious user to guess the password length when "runas.exe" is used to launch an application under another's user's privilege. specified user, a local attacker can monitor the "IO Other Bytes" performance of the application to determine the length of the submitted password.

- A. sudo
- B. grep
- C. su
- D. ps

200. After scanning a web application for possible vulnerabilities, Barry received the result shown here. Which one of the following best describes the threat posed by this vulnerability?

Vulnerabilities (1)

3 Web Server Uses Plain-Text Form Based Authentication

First Detected:	03/03/2020 at 12:02:19 (GMT-0400)	Last Detected:	04/09/2020 at 20:31:35 (GMT-0400)	Times Detected:	142	Last Fixed:	N/A
QID:	86728	CVSS Base:	5.0				
Category:	Web server	CVSS Temporal:	3.6				
CVE ID:	-	CVSS3 Base:	-				
Vendor Reference	-	CVSS3 Temporal:	-				
Bugtraq ID:	-	CVSS Environment:	-				
Service Modified:	09/04/2020	Asset Group:	-				
User Modified:	-	Collateral Damage Potential:	-				
Edited:	No	Target Distribution:	-				
PCI Vuln:	Yes	Confidentiality Requirement:	-				
Ticket State:		Integrity Requirement:	-				
		Availability Requirement:	-				

- A. An attacker can eavesdrop on authentication exchanges.
- B. An attacker can cause a denial-of-service attack on the web application.
- C. An attacker can disrupt the encryption mechanism used by this server.
- D. An attacker can edit the application code running on this server.

201. Javier ran a vulnerability scan of a network device used by his organization and discovered the vulnerability shown here. What type of attack would this vulnerability enable?

▼ 2 UDP Constant IP Identification Field Fingerprinting Vulnerability CVSS: - CVSS3: - Active

First Detected:	Last Detected:	Times Detected:	Last Fixed:
03/17/2020 at 01:33:14 (GMT-0400)	04/05/2020 at 01:57:57 (GMT-0400)	613	
11/02/2020 at 07:00:06 (GMT-0400)		5	

QID:	82024	CVSS Base:	4.8
Category:	TCP/IP	CVSS3 Temporal:	-
CVE ID:	CVE-2002-0510	CVSS3 Base:	-
Vendor Reference:	-	CVSS Environment:	-
Bugtraq ID:	4314	Asset Group:	-
Service Modified:	05/07/2020	Collateral Damage Potential:	-
User Modified:	-	Target Distribution:	-
Edited:	No	Confidentiality Requirement:	-
PCI Vuln:	No	Integrity Requirement:	-
Ticket State:	-	Availability Requirement:	-

THREAT:
The host transmits UDP packets with a constant IP Identification field. This behavior may be exploited to discover the operating system and approximate kernel version of the vulnerable system. Normally, the IP Identification field is intended to be a reasonably unique value, and is used to reconstruct fragmented packets. It has been reported that in some versions of the Linux kernel IP stack implementation as well as other operating systems, UDP packets are transmitted with a constant IP Identification field of 0.

- A. Denial of service
- B. Information theft
- C. Information alteration
- D. Reconnaissance

202. Akari scans a Windows server in her organization and finds that it has multiple critical vulnerabilities, detailed in the report shown here. What action can Akari take that will have the most significant impact on these issues without creating a long-term outage?

▼ Vulnerabilities (27)

5	Microsoft Cumulative Security Update for Internet Explorer (MS17-006)	CVSS: - CVSS3: - New
5	Microsoft Cumulative Security Update for Windows (MS17-012)	CVSS: - CVSS3: - New
4	Microsoft Unsubscribe Multiple Remote Code Execution and Information Disclosure Vulnerabilities (MS17-011)	CVSS: - CVSS3: - New
4	Microsoft Security Update for Windows Kernel-Mode Drivers (MS17-018)	CVSS: - CVSS3: - New
4	Microsoft Windows DirectShow Information Disclosure Vulnerability (MS17-021)	CVSS: - CVSS3: - New
4	Microsoft XML Core Services Information Disclosure Vulnerability (MS17-022)	CVSS: - CVSS3: - New
4	Microsoft Windows Kernel Elevation of Privileges (MS17-017)	CVSS: - CVSS3: - New
3	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) port 3389/tcp over SSL	CVSS: - CVSS3: - New
5	Veritas NetBackup Remote Access Vulnerabilities (VTS16-001)	CVSS: - CVSS3: - Active
5	EOL/Obsolete Software: Microsoft VC++ 2005 Detected	CVSS: - CVSS3: - Active
5	Microsoft Foundation Class Library Remote Code Execution Vulnerability (MS11-025)	CVSS: - CVSS3: - Active
4	Microsoft Windows Graphics Component Multiple Vulnerabilities (MS17-013)	CVSS: - CVSS3: - Active
3	Microsoft Windows "RunAs" Password Length Local Information Disclosure - Zero Day	CVSS: - CVSS3: - Active
3	Built-in Guest Account Not Renamed at Windows Target System	CVSS: - CVSS3: - Active
3	Windows Unquoted/Trusted Service Paths Privilege Escalation Security Issue	CVSS: - CVSS3: - Active
3	Microsoft .Net Framework RC4 in TLS Not Disabled (KB2960356)	CVSS: - CVSS3: - Active

- A. Configure the host firewall to block inbound connections.
- B. Apply security patches.
- C. Disable the guest account on the server.
- D. Configure the server to only use secure ciphers.

203. Ben is preparing to conduct a vulnerability scan for a new client of his security consulting organization. Which one of the following steps should Ben perform first?

- A. Conduct penetration testing.
- B. Run a vulnerability evaluation scan.

- C. Run a discovery scan.
 - D. Obtain permission for the scans.
204. Katherine coordinates the remediation of security vulnerabilities in her organization and is attempting to work with a system engineer on the patching of a server to correct a moderate impact vulnerability. The engineer is refusing to patch the server because of the potential interruption to a critical business process that runs on the server. What would be the most reasonable course of action for Katherine to take?
- A. Schedule the patching to occur during a regular maintenance cycle.
 - B. Exempt the server from patching because of the critical business impact.
 - C. Demand that the server be patched immediately to correct the vulnerability.
 - D. Inform the engineer that if he does not apply the patch within a week that Katherine will file a complaint with his manager.
205. During a recent vulnerability scan of workstations on her network, Andrea discovered the vulnerability shown here. Which one of the following actions is *least* likely to remediate this vulnerability?

4 Sun Java Runtime Environment GIF Images Buffer Overflow Vulnerability

First Detected:	08/04/2018 at 18:02:25 (GMT-0400)	Last Detected:	04/05/2020 at 03:40:45 (GMT-0400)	Times Detected:	22	Last Fixed:	N/A
QID:	115501	CVSS Base:	6.8				
Category:	Local	CVSS Temporal:	5.3				
CVE ID:	CVE-2007-0243	CVSS3 Base:	-				
Vendor Reference:	Oracle ID 1000058.1	CVSS3 Temporal:	-				
Bugtraq ID:	22085	CVSS Environment:	-				
Service Modified:	10/21/2020	Asset Group:	-				
User Modified:	-	Collateral Damage Potential:	-				
Edited:	No	Target Distribution:	-				
PCI Vuln:	Yes	Confidentiality Requirement:	-				
Ticket State:	Open	Integrity Requirement:	-				
		Availability Requirement:	-				

THREAT:
The Java Runtime Environment is an application that allows users to run Java applications. The Java Runtime Environment is prone to a buffer overflow vulnerability because the application fails to bounds check user-supplied data before copying it into an insufficiently sized memory buffer. Image from a Java applet.

IMPACT:
A attacker can exploit this issue to execute arbitrary code with the privileges of the victim.

SOLUTION:
This issue is addressed in the following releases (for Windows, Solaris, and Linux):
JDK and JRE 5.0 Update 10 or later
SDK and JRE 1.4.2_13 or later
SDK and JRE 1.3.1_19 or later
J2SE 5.0 is available for download at [JDK Downloads](#).
J2SE 5.0 Update 10 for Solaris is available in the following patches:
J2SE 5.0: update 10 (as delivered in patch 118666-10)
J2SE 5.0: update 10 (as delivered in patch 118667-10 (64bit))
J2SE 5.0_x86: update 10 (as delivered in patch 118668-10)
J2SE 5.0_x86: update 10 (as delivered in patch 118669-10 (64bit))
J2SE 1.4.2 is available for download at [J2SE 1.4.2](#).
J2SE 1.3.1 is available for download at [J2SE 1.3.1](#).
Refer to [Oracle ID 1000058.1](#) for additional information on the vulnerabilities and patch details.
Patch:
Following are links for downloading patches to fix the vulnerabilities:
[Sun Alert ID 102760: all \(J2SE 5.0\)](#)
[Sun Alert ID 102760: all \(J2SE 1.4.2\)](#)
[Sun Alert ID 102760: all \(J2SE 1.3.1\)](#)
[Sun Alert ID 102760: Solaris](#)

- A. Remove JRE from workstations.
 - B. Upgrade JRE to the most recent version.
 - C. Block inbound connections on port 80 using the host firewall.
 - D. Use a web content filtering system to scan for malicious traffic.
206. Grace ran a vulnerability scan and detected an urgent vulnerability in a public-facing web server. This vulnerability is easily exploitable and could result in the complete compromise

of the server. Grace wants to follow best practices regarding change control while also mitigating this threat as quickly as possible. What would be Grace's best course of action?

- A. Initiate a high-priority change through her organization's change management process and wait for the change to be approved.
- B. Implement a fix immediately and document the change after the fact.
- C. Schedule a change for the next quarterly patch cycle.
- D. Initiate a standard change through her organization's change management process.

207. Doug is preparing an RFP for a vulnerability scanner for his organization. He needs to know the number of systems on his network to help determine the scanner requirements. Which one of the following would not be an easy way to obtain this information?

- A. ARP tables
- B. Asset management tool
- C. Discovery scan
- D. Results of scans recently run by a consultant

208. Mary runs a vulnerability scan of her entire organization and shares the report with another analyst on her team. An excerpt from that report appears here. Her colleague points out that the report contains only vulnerabilities with severities of 3, 4, or 5. What is the most likely cause of this result?

Ubuntu / Tiny Core Linux / Linux 2.6.x		
Vulnerabilities (7)		
3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	port 443/tcp over SSL	CVSS: - CVSS3: - New
3 SSL/TLS use of weak RC4 cipher	port 443/tcp over SSL	CVSS: - CVSS3: - Active
3 SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE)	port 443/tcp over SSL	CVSS: - CVSS3: - Active
3 SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST)	port 443/tcp over SSL	CVSS: - CVSS3: - Active
3 SSL/TLS Server supports TLSv1.0	port 443/tcp over SSL	CVSS: - CVSS3: - Active
3 SSL Server Has SSLv3 Enabled Vulnerability	port 443/tcp over SSL	CVSS: - CVSS3: - Active
3 HTTP TRACE / TRACK Methods Enabled	port 443/tcp	CVSS: - CVSS3: - Active
Ubuntu / Tiny Core Linux / Linux 2.6.x		
Vulnerabilities (7)		
3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	port 443/tcp over SSL	CVSS: - CVSS3: - New
3 SSL Server Has SSLv3 Enabled Vulnerability	port 443/tcp over SSL	CVSS: - CVSS3: - Active
3 SSL/TLS use of weak RC4 cipher	port 443/tcp over SSL	CVSS: - CVSS3: - Active
3 SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST)	port 443/tcp over SSL	CVSS: - CVSS3: - Active
3 SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE)	port 443/tcp over SSL	CVSS: - CVSS3: - Active
3 SSL/TLS Server supports TLSv1.0	port 443/tcp over SSL	CVSS: - CVSS3: - Active
3 HTTP TRACE / TRACK Methods Enabled	port 443/tcp	CVSS: - CVSS3: - Active
Ubuntu / Fedora / Tiny Core Linux / Linux 3.x		
Vulnerabilities (1)		
3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	port 443/tcp over SSL	CVSS: - CVSS3: - Fixed
Windows 2012 Standard		
Vulnerabilities (4)		
3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	port 3389/tcp over SSL	CVSS: - CVSS3: - New
3 Windows Remote Desktop Protocol Weak Encryption Method Allowed	port 3389/tcp over SSL	CVSS: - CVSS3: - Active
3 SSL/TLS Server supports TLSv1.0	port 3389/tcp over SSL	CVSS: - CVSS3: - Active
3 SSL/TLS use of weak RC4 cipher	port 3389/tcp over SSL	CVSS: - CVSS3: - Active
Ubuntu / Fedora / Tiny Core Linux / Linux 3.x		
Vulnerabilities (3)		
3 SSL/TLS use of weak RC4 cipher	port 443/tcp over SSL	CVSS: - CVSS3: - Fixed
3 SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST)	port 443/tcp over SSL	CVSS: - CVSS3: - Fixed
3 SSL/TLS Server supports TLSv1.0	port 443/tcp over SSL	CVSS: - CVSS3: - Fixed

- A. The scan sensitivity is set to exclude low-importance vulnerabilities.
- B. Mary did not configure the scan properly.
- C. Systems in the datacenter do not contain any level 1 or 2 vulnerabilities.
- D. The scan sensitivity is set to exclude high-impact vulnerabilities.

209. Mikhail is reviewing the vulnerability shown here, which was detected on several servers in his environment. What action should Mikhail take?

INFO	TCP/IP Timestamps Supported	Plugin Details
Description The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.		Severity: Info ID: 25220 Version: 1.19 Type: remote Family: General Published: 2020/05/16 Modified: 2020/03/20
See Also http://www.ietf.org/rfc/rfc1323.txt		

- A. Block TCP/IP access to these servers from external sources.
 - B. Upgrade the operating system on these servers.
 - C. Encrypt all access to these servers.
 - D. No action is necessary.
- 210.** Which one of the following approaches provides the most current and accurate information about vulnerabilities present on a system because of the misconfiguration of operating system settings?
- A. On-demand vulnerability scanning
 - B. Continuous vulnerability scanning
 - C. Scheduled vulnerability scanning
 - D. Agent-based monitoring

Use the following scenario to answer questions 211–213.

Pete recently conducted a broad vulnerability scan of all the servers and workstations in his environment. He scanned the following three networks:

- DMZ network that contains servers with public exposure
- Workstation network that contains workstations that are allowed outbound access only
- Internal server network that contains servers exposed only to internal systems

He detected the following vulnerabilities:

- Vulnerability 1: A SQL injection vulnerability on a DMZ server that would grant access to a database server on the internal network (severity 5/5)
- Vulnerability 2: A buffer overflow vulnerability on a domain controller on the internal server network (severity 3/5)
- Vulnerability 3: A missing security patch on several hundred Windows workstations on the workstation network (severity 2/5)

- Vulnerability 4: A denial-of-service vulnerability on a DMZ server that would allow an attacker to disrupt a public-facing website (severity 2/5)
- Vulnerability 5: A denial-of-service vulnerability on an internal server that would allow an attacker to disrupt an internal website (severity 4/5)

Note that the severity ratings assigned to these vulnerabilities are directly from the vulnerability scanner and were not assigned by Pete.

- 211.** Absent any other information, which one of the vulnerabilities in the report should Pete remediate first?
- A. Vulnerability 1
 - B. Vulnerability 2
 - C. Vulnerability 3
 - D. Vulnerability 4
- 212.** Pete is working with the desktop support manager to remediate vulnerability 3. What would be the most efficient way to correct this issue?
- A. Personally visit each workstation to remediate the vulnerability.
 - B. Remotely connect to each workstation to remediate the vulnerability.
 - C. Perform registry updates using a remote configuration tool.
 - D. Apply the patch using a GPO.
- 213.** Pete recently conferred with the organization's CISO, and the team is launching an initiative designed to combat the insider threat. They are particularly concerned about the theft of information by employees seeking to exceed their authorized access. Which one of the vulnerabilities in this report is of greatest concern given this priority?
- A. Vulnerability 2
 - B. Vulnerability 3
 - C. Vulnerability 4
 - D. Vulnerability 5
- 214.** Wanda recently discovered the vulnerability shown here on a Windows server in her organization. She is unable to apply the patch to the server for six weeks because of operational issues. What workaround would be most effective in limiting the likelihood that this vulnerability would be exploited?

4 Microsoft Windows Graphics Component Multiple Vulnerabilities (MS17-013)				
First Detected:	03/04/2020 at 21:44:56 (GMT-0400)	Last Detected:	04/04/2020 at 21:57:33 (GMT-0400)	Times Detected: 2 Last Fixed: N/A
QID:	91331	CVSS Base:	9.3	
Category:	Windows	CVSS Temporal:	8.1	
CVE ID:	CVE-2017-0001 CVE-2017-0005 CVE-2017-0014 CVE-2017-0025 CVE-2017-0038 CVE-2017-0047 CVE-2017-0060 CVE-2017-0081 CVE-2017-0082 CVE-2017-0083 CVE-2017-0073 CVE-2017-0108	CVSS3 Base:	7.8	
		CVSS3 Temporal:	7.4	
Vendor Reference	MS17-013	CVSS Environment:		
Bugtraq ID:	96057, 96033, 96013, 96026, 96023, 96034, 96713, 96722, 96637	Asset Group:	-	
Service Modified:	03/14/2020	Collateral Damage Potential:	-	
User Modified:	-	Target Distribution:	-	
Edited:	No	Confidentiality Requirement:	-	
PCI Vuln:	Yes	Integrity Requirement:	-	
Ticket State:	Open	Availability Requirement:	-	
THREAT:				
This security update resolves vulnerabilities in Microsoft Windows, Microsoft Office, Skype for Business, Microsoft Lync, and Microsoft Silverlight.				
The security update addresses the vulnerabilities by correcting how the software handles objects in memory.				
This security update is rated Critical for: All supported releases of Microsoft Windows Affected editions of Microsoft Office 2007 and Microsoft Office 2010 Affected editions of Skype for Business 2016.				
IMPACT:				
The most severe of these vulnerabilities could allow remote code execution if a user either visits a specially crafted website or opens a specially crafted document.				

- A. Restrict interactive logins to the system.
 - B. Remove Microsoft Office from the server.
 - C. Remove Internet Explorer from the server.
 - D. Apply the security patch.
- 215. Garrett is configuring vulnerability scanning for a new web server that his organization is deploying on its DMZ network. The server hosts the company's public website. What type of scanning should Garrett configure for best results?
 - A. Garrett should not perform scanning of DMZ systems.
 - B. Garrett should perform external scanning only.
 - C. Garrett should perform internal scanning only.
 - D. Garrett should perform both internal and external scanning.
- 216. Frank recently ran a vulnerability scan and identified a POS terminal that contains an unpatchable vulnerability because of running an unsupported operating system. Frank consults with his manager and is told that the POS is being used with full knowledge of management and, as a compensating control, it has been placed on an isolated network with no access to other systems. Frank's manager tells him that the merchant bank is aware of the issue. How should Frank handle this situation?
 - A. Document the vulnerability as an approved exception.
 - B. Explain to his manager that PCI DSS does not permit the use of unsupported operating systems.
 - C. Decommission the POS system immediately to avoid personal liability.
 - D. Upgrade the operating system immediately.
- 217. James is configuring vulnerability scans of a dedicated network that his organization uses for processing credit card transactions. What types of scans are least important for James to include in his scanning program?
 - A. Scans from a dedicated scanner on the card processing network
 - B. Scans from an external scanner on his organization's network
 - C. Scans from an external scanner operated by an approved scanning vendor
 - D. All three types of scans are equally important.
- 218. Helen performs a vulnerability scan of one of the internal LANs within her organization and finds a report of a web application vulnerability on a device. Upon investigation, she discovers that the device in question is a printer. What is the most likely scenario in this case?
 - A. The printer is running an embedded web server.
 - B. The report is a false positive result.
 - C. The printer recently changed IP addresses.
 - D. Helen inadvertently scanned the wrong network.

- 219.** Joe discovered a critical vulnerability in his organization's database server and received permission from his supervisor to implement an emergency change after the close of business. He has eight hours before the planned change window. In addition to planning the technical aspects of the change, what else should Joe do to prepare for the change?
- A.** Ensure that all stakeholders are informed of the planned outage.
 - B.** Document the change in his organization's change management system.
 - C.** Identify any potential risks associated with the change.
 - D.** All of the above.
- 220.** Julian recently detected the vulnerability shown here on several servers in his environment. Because of the critical nature of the vulnerability, he would like to block all access to the affected service until it is resolved using a firewall rule. He verifies that the following TCP ports are open on the host firewall. Which one of the following does Julian *not* need to block to restrict access to this service?

5 Microsoft SMB Server Remote Code Execution Vulnerability (MS17-010)					
First Detected:	04/05/2020 at 02:25:12 (GMT-0400)	Last Detected:	04/05/2020 at 02:25:12 (GMT-0400)	Times Detected:	1
QID:	91345	CVSS Base:	9.3	Last Fixed:	N/A
Category:	Windows	CVSS Temporal:	6.9		
CVE ID:	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147	CVSS3 Base:	8.1		
	0148 CVE-2017-0147	CVSS3 Temporal:	7.1		
Vendor Reference	MS17-010	CVSS Environment:			
Bugtraq ID:	96703, 96704, 96705, 96707, 96709, 96706	Asset Group:	-		
Service Modified:	03/15/2020	Collateral Damage Potential:	-		
User Modified:	-	Target Distribution:	-		
Edited:	No	Confidentiality Requirement:	-		
PCI Vuln:	Yes	Integrity Requirement:	-		
Ticket State:	Open	Availability Requirement:	-		
THREAT:					
Microsoft Server Message Block (SMB) Protocol is a Microsoft network file sharing protocol used in Microsoft Windows.					
The Microsoft SMB Server is vulnerable to multiple remote code execution vulnerabilities due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.					
This security update is rated Critical for all supported editions of Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows Server 2012 and 2012 R2, Windows 8.1 and RT 8.1.					
IMPACT:					
A remote attacker could gain the ability to execute code by sending crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.					
SOLUTION:					
Customers are advised to refer to Microsoft Advisory MS17-010 for more details.					

- A.** 137
 - B.** 139
 - C.** 389
 - D.** 445
- 221.** Ted recently ran a vulnerability scan of his network and was overwhelmed with results. He would like to focus on the most important vulnerabilities. How should Ted reconfigure his vulnerability scanner?
- A.** Increase the scan sensitivity.
 - B.** Decrease the scan sensitivity.
 - C.** Increase the scan frequency.
 - D.** Decrease the scan frequency.
- 222.** After running a vulnerability scan, Janet discovered that several machines on her network are running Internet Explorer 8 and reported the vulnerability shown here. Which one of the following would *not* be a suitable replacement browser for these systems?

5

EOL/Obsolete Software: Microsoft Internet Explorer 8 Detected

First Detected:	02/04/2020 at 19:05:19 (GMT-0400)	Last Detected:	04/05/2020 at 02:19:36 (GMT-0400)	Times Detected:	15	Last Fixed:	N/A
QID:	105646	CVSS Base:	9.3				
Category:	Security Policy	CVSS Temporal:	7.9				
CVE ID:	-	CVSS3 Base:	-				
Vendor Reference:	Microsoft Support Lifecycle for Internet Explorer	CVSS3 Temporal:	-				
Bugtraq ID:	-	CVSS Environment:	-				
Service Modified:	03/09/2020	Asset Group:	-				
User Modified:	-	Collateral Damage Potential:	-				
Edited:	No	Target Distribution:	-				
PCI Vuln:	Yes	Confidentiality Requirement:	-				
Ticket State:	Open	Integrity Requirement:	-				
		Availability Requirement:	-				

THREAT:
Microsoft Internet Explorer is a graphical web browser developed by Microsoft and included as part of the Microsoft Windows operating systems. The host is running Internet Explorer 8 software. Microsoft ended support for Internet Explorer 8 on January 12, 2016. No further updates, including security updates, are available for Internet Explorer 8.

IMPACT:
The system is at high risk of being exposed to security vulnerabilities. Since the vendor no longer provides updates, obsolete software is more vulnerable to viruses and other attacks.

- A. Internet Explorer 11
- B. Google Chrome
- C. Mozilla Firefox
- D. Microsoft Edge

223. Sunitha discovered the vulnerability shown here in an application developed by her organization. What application security technique is most likely to resolve this issue?

4

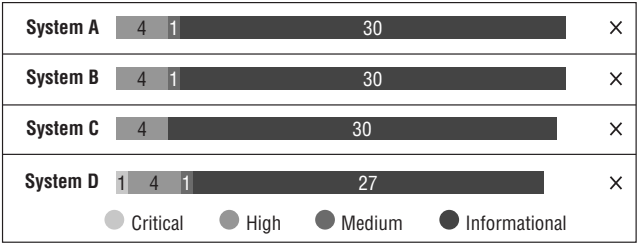
Sun Java RunTime Environment GIF Images Buffer Overflow Vulnerability

CVSS: - CVSS3: - Active

First Detected:	08/04/2018 at 18:02:25 (GMT-0400)	Last Detected:	04/05/2020 at 03:03:58 (GMT-0400)	Times Detected:	22	Last Fixed:	N/A
QID:	115501	CVSS Base:	6.8				
Category:	Local	CVSS Temporal:	5.3				
CVE ID:	CVE-2007-0243	CVSS3 Base:	-				
Vendor Reference:	Oracle ID 1000058.1	CVSS3 Temporal:	-				
Bugtraq ID:	22085	CVSS Environment:	-				
Service Modified:	10/21/2020	Asset Group:	-				
User Modified:	-	Collateral Damage Potential:	-				
Edited:	No	Target Distribution:	-				
PCI Vuln:	Yes	Confidentiality Requirement:	-				
Ticket State:	Open	Integrity Requirement:	-				
		Availability Requirement:	-				

- A. Bounds checking
- B. Network segmentation
- C. Parameter handling
- D. Tag removal

224. Sherry runs a vulnerability scan and receives the high-level results shown here. Her priority is to remediate the most important vulnerabilities first. Which system should be her highest priority?



- A. A
- B. B
- C. C
- D. D

- 225.** Victor is configuring a new vulnerability scanner. He set the scanner to run scans of his entire datacenter each evening. When he went to check the scan reports at the end of the week, he found that they were all incomplete. The scan reports noted the error “Scan terminated due to start of preempting job.” Victor has no funds remaining to invest in the vulnerability scanning system. He does want to cover the entire datacenter. What should he do to ensure that scans complete?
- A.** Reduce the number of systems scanned.
 - B.** Increase the number of scanners.
 - C.** Upgrade the scanner hardware.
 - D.** Reduce the scanning frequency.
- 226.** Vanessa ran a vulnerability scan of a server and received the results shown here. Her boss instructed her to prioritize remediation based on criticality. Which issue should she address first?

<input type="checkbox"/> Severity ▲	Plugin Name	Plugin Family	Count
<input type="checkbox"/> HIGH	Apache 2.2.x < 2.2.28 Multiple Vulnerabilities	Web Servers	2
<input type="checkbox"/> MEDIUM	Apache 2.2.x < 2.2.16 Multiple Vulnerabilities	Web Servers	2
<input type="checkbox"/> MEDIUM	Apache 2.2.x < 2.2.17 Multiple Vulnerabilities	Web Servers	2
<input type="checkbox"/> MEDIUM	Apache 2.2.x < 2.2.18 APR apr_fnmatch DoS	Web Servers	2
<input type="checkbox"/> MEDIUM	Apache 2.2.x < 2.2.21 mod_proxy_ajp DoS	Web Servers	2
<input type="checkbox"/> MEDIUM	Apache 2.2.x < 2.2.22 Multiple Vulnerabilities	Web Servers	2
<input type="checkbox"/> MEDIUM	Apache 2.2.x < 2.2.23 Multiple Vulnerabilities	Web Servers	2
<input type="checkbox"/> MEDIUM	Apache 2.2.x < 2.2.24 Multiple XSS Vulnerabilities	Web Servers	2
<input type="checkbox"/> MEDIUM	Apache 2.2.x < 2.2.25 Multiple Vulnerabilities	Web Servers	2
<input type="checkbox"/> MEDIUM	Apache 2.2.x < 2.2.27 Multiple Vulnerabilities	Web Servers	2
<input type="checkbox"/> MEDIUM	SSH Weak Algorithms Supported	Misc.	1
<input type="checkbox"/> LOW	FTP Supports Cleartext Authentication	FTP	1
<input type="checkbox"/> LOW	SSH Server CBC Mode Ciphers Enabled	Misc.	1
<input type="checkbox"/> LOW	SSH Weak MAC Algorithms Enabled	Misc.	1
<input type="checkbox"/> INFO	Service Detection	Service detection	19
<input type="checkbox"/> INFO	Nessus SYN scanner	Port scanners	15
<input type="checkbox"/> INFO	HTTP Server Type and Version	Web Servers	6
<input type="checkbox"/> INFO	PHP Version	Web Servers	4
<input type="checkbox"/> INFO	IMAP Service Banner Retrieval	Service detection	2
<input type="checkbox"/> INFO	POP Server Detection	Service detection	2

- A. Remove the POP server.
 - B. Remove the FTP server.
 - C. Upgrade the web server.
 - D. Remove insecure cryptographic protocols.
227. Gil is configuring a scheduled vulnerability scan for his organization using the Qualys-Guard scanner. If he selects the Relaunch On Finish scheduling option shown here, what will be the result?

Edit Scheduled Vulnerability Scan Turn help tips: On | Off Launch Help

Scheduling

Task Title >

Target Hosts >

Scheduling >

Notifications >

Schedule Status >

Start: Aug 07, 2020 31 03:00

(GMT -05:00) United States, Connecticut (Eastern Stand: DST

Duration: ☐ Pause after 01 hours

Resume Days: Manually

Occurs:

- ✓ Daily
- Weekly
- Monthly
- Relaunch on Finish
- ☐ Ends after occurrences

Cancel Save

- A. The scan will run once each time the schedule occurs.
- B. The scan will run twice each time the schedule occurs.
- C. The scan will run twice the next time the schedule occurs and once on each subsequent schedule interval.
- D. The scan will run continuously until stopped.

228. Terry is reviewing a vulnerability scan of a Windows server and came across the vulnerability shown here. What is the risk presented by this vulnerability?

▼ 1 Detected Compatibility 8.3 Filename Feature

First Detected:	09/28/2019 at 10:42:15 (GMT-0400)	Last Detected:	04/05/2020 at 04:21:18 (GMT-0400)	Times Detected:	20	Last Fixed:	N/A
QID:	90023	CVSS Base:	0.0				
Category:	Windows	CVSS Temporal:	0				
CVE ID:	-	CVSS3 Base:	-				
Vendor Reference:	-	CVSS3 Temporal:	-				
Bugtraq ID:	-	CVSS Environment:	-				
Service Modified:	05/12/2020	Asset Group:	-				
User Modified:	-	Collateral Damage Potential:	-				
Edited:	No	Target Distribution:	-				
PCI Vuln:	No	Confidentiality Requirement:	-				
Ticket State:		Integrity Requirement:	-				
		Availability Requirement:	-				

THREAT:
NTFS supports backward compatibility with older 16-bit software by restricting the allowed filenames to 8.3 format. This feature seems to be activated on this host.

IMPACT:
16-bit applications are extremely vulnerable and should not be used on a secure server. If you have not installed any 16-bit applications on a Windows NT-based computer, you can turn off automatic short up file and folder access on your computer running Windows NT.

SOLUTION:
We recommend that you remove this compatibility restriction. To do so, locate the following registry key, and then set the REG_DWORD 'NfsDisable8dot3NameCreation' entry to '1':
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem

- A. An attacker may be able to execute a buffer overflow and execute arbitrary code on the server.
- B. An attacker may be able to conduct a denial-of-service attack against this server.
- C. An attacker may be able to determine the operating system version on this server.
- D. There is no direct vulnerability, but this information points to other possible vulnerabilities on the server.

229. Andrea recently discovered the vulnerability shown here on the workstation belonging to a system administrator in her organization. What is the major likely threat that should concern Andrea?

▼ 3 PuTTY Local Information Disclosure Vulnerability

First Detected:	04/05/2020 at 02:19:36 (GMT-0400)	Last Detected:	04/05/2020 at 02:19:36 (GMT-0400)	Times Detected:	1	Last Fixed:	N/A
QID:	123511	CVSS Base:	2.1				
Category:	Local	CVSS Temporal:	1.6				
CVE ID:	CVE-2015-2157	CVSS3 Base:	-				
Vendor Reference:	PuTTY vulnerability	CVSS3 Temporal:	-				
Bugtraq ID:	72825	CVSS Environment:	-				
Service Modified:	03/08/2020	Asset Group:	-				
User Modified:	-	Collateral Damage Potential:	-				
Edited:	No	Target Distribution:	-				
PCI Vuln:	No	Confidentiality Requirement:	-				
Ticket State:		Integrity Requirement:	-				
		Availability Requirement:	-				

THREAT:
PuTTY is a client program for the SSH, Telnet and Rlogin network protocols. It is integrated in multiple applications on multiple operating systems for providing SSH, Telnet and Rlogin protocol support. The ssh2_load_userkey and ssh2_save_userkey functions implemented in vulnerable PuTTY versions, fail to properly wipe SSH-2 private keys from memory.

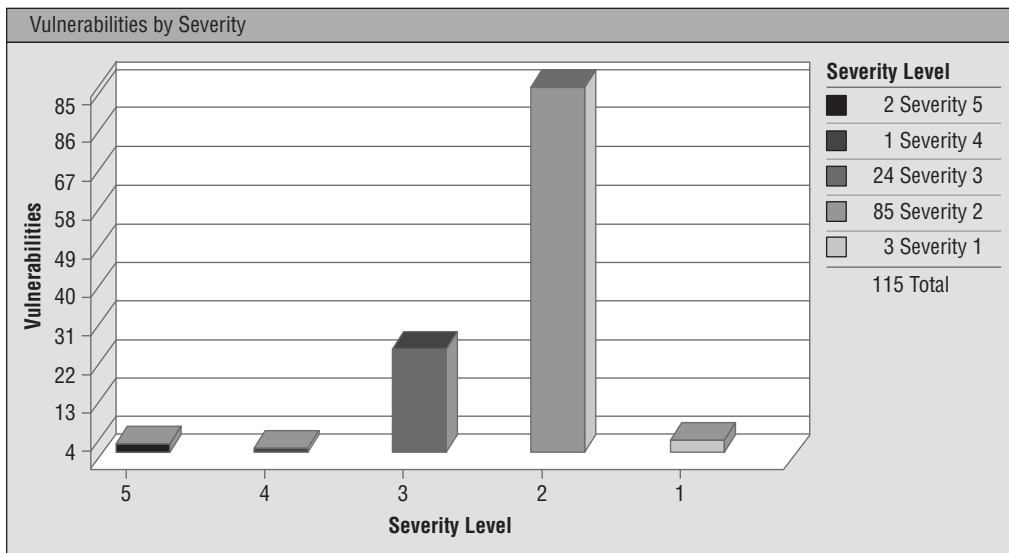
- A. An attacker could exploit this vulnerability to take control of the administrator's workstation.
- B. An attacker could exploit this vulnerability to gain access to servers managed by the administrator.
- C. An attacker could exploit this vulnerability to prevent the administrator from using the workstation.
- D. An attacker could exploit this vulnerability to decrypt sensitive information stored on the administrator's workstation.

230. Mateo completed the vulnerability scan of a server in his organization and discovered the results shown here. Which one of the following is not a critical remediation action dictated by these results?

Vulnerabilities (71)	
5	Google Chrome Prior to 57.0.2987.98 Multiple Vulnerabilities
5	Microsoft Cumulative Security Update for Windows (MS17-012)
4	Google Chrome Prior to 57.0.2987.133 Multiple Vulnerabilities
4	Microsoft Unsubscribe Multiple Remote Code Execution and Information Disclosure Vulnerabilities (MS17-011)
4	Microsoft Security Update for Windows Kernel-Mode Drivers (MS17-016)
4	Microsoft Windows DirectShow Information Disclosure Vulnerability (MS17-021)
4	Microsoft XML Core Services Information Disclosure Vulnerability (MS17-022)
4	Microsoft Windows Kernel Elevation of Privileges (MS17-017)
3	NotePad++ "sclexer.dll" DLL Hijacking Vulnerability
3	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)
5	Oracle Java SE Critical Patch Update - October 2016
5	EOL/Obsolete Software: Microsoft VC++ 2005 Detected
5	Oracle Java SE Critical Patch Update - January 2017
5	Oracle Java SE Critical Patch Update - October 2012
5	Oracle Java SE Critical Patch Update - February 2013
5	Oracle Java SE JVM 2D Subcomponent Remote Code Execution Vulnerability (Oracle Security Alert for CVE-2013-1493)
5	EOL/Obsolete Software: Microsoft .NET Framework 4 - 4.5.1 Detected
5	EOL/Obsolete Software: Microsoft Internet Explorer 8 Detected
5	EOL/Obsolete Software: Oracle Java SE/JRE/JDK 6/1.6 Detected
5	Oracle Java SE Critical Patch Update - April 2013
5	Oracle Java SE Critical Patch Update - June 2013
5	Oracle Java SE Critical Patch Update - July 2014
5	Oracle Java SE Critical Patch Update - October 2014
5	Oracle Java SE Critical Patch Update - January 2015

- A. Remove obsolete software.
- B. Reconfigure the host firewall.
- C. Apply operating system patches.
- D. Apply application patches.
231. Tom's company is planning to begin a bring your own device (BYOD) policy for mobile devices. Which one of the following technologies allows the secure use of sensitive information on personally owned devices, including providing administrators with the ability to wipe corporate information from the device without affecting personal data?
- A. Remote wipe
- B. Strong passwords
- C. Biometric authentication
- D. Containerization

- 232.** Sally discovered during a vulnerability scan that a system that she manages has a high-priority vulnerability that requires a patch. The system is behind a firewall and there is no imminent threat, but Sally wants to get the situation resolved as quickly as possible. What would be her best course of action?
- A.** Initiate a high-priority change through her organization's change management process.
 - B.** Implement a fix immediately and then document the change after the fact.
 - C.** Implement a fix immediately and then inform her supervisor of her action and the rationale.
 - D.** Schedule a change for the next quarterly patch cycle.
- 233.** Gene runs a vulnerability scan of his organization's datacenter and produces a summary report to share with his management team. The report includes the chart shown here. When Gene's manager reads the report, she points out that the report is burying important details because it is highlighting too many unimportant issues. What should Gene do to resolve this issue?



- A.** Tell his manager that all vulnerabilities are important and should appear on the report.
- B.** Create a revised version of the chart using Excel.
- C.** Modify the sensitivity level of the scan.
- D.** Stop sharing reports with the management team.

- 234.** Avik recently conducted a PCI DSS vulnerability scan of a web server and noted a critical PHP vulnerability that required an upgrade to correct. She applied the update. How soon must Avik repeat the scan?
- A.** Within 30 days
 - B.** At the next scheduled quarterly scan
 - C.** At the next scheduled annual scan
 - D.** Immediately
- 235.** Chandra's organization recently upgraded the firewall protecting the network where they process credit card information. This network is subject to the provisions of PCI DSS. When is Chandra required to schedule the next vulnerability scan of this network?
- A.** Immediately
 - B.** Within one month
 - C.** Before the start of next month
 - D.** Before the end of the quarter following the upgrade
- 236.** Fahad is concerned about the security of an industrial control system that his organization uses to monitor and manage systems in their factories. He would like to reduce the risk of an attacker penetrating this system. Which one of the following security controls would best mitigate the vulnerabilities in this type of system?
- A.** Network segmentation
 - B.** Input validation
 - C.** Memory protection
 - D.** Redundancy
- 237.** Glenda routinely runs vulnerability scans of servers in her organization. She is having difficulty with one system administrator who refuses to correct vulnerabilities on a server used as a jump box by other IT staff. The server has had dozens of vulnerabilities for weeks and would require downtime to repair. One morning, her scan reports that all of the vulnerabilities suddenly disappeared overnight, while other systems in the same scan are reporting issues. She checks the service status dashboard, and the service appears to be running properly with no outages reported in the past week. What is the most likely cause of this result?
- A.** The system administrator corrected the vulnerabilities.
 - B.** The server is down.
 - C.** The system administrator blocked the scanner.
 - D.** The scan did not run.
- 238.** Raphael discovered during a vulnerability scan that an administrative interface to one of his storage systems was inadvertently exposed to the Internet. He is reviewing firewall logs and would like to determine whether any access attempts came from external sources. Which one of the following IP addresses reflects an external source?
- A.** 10.15.1.100
 - B.** 12.8.1.100
 - C.** 172.16.1.100
 - D.** 192.168.1.100

- 239.** Nick is configuring vulnerability scans for his network using a third-party vulnerability scanning service. He is attempting to scan a web server that he knows exposes a CIFS file share and contains several significant vulnerabilities. However, the scan results only show ports 80 and 443 as open. What is the most likely cause of these scan results?
- A. The CIFS file share is running on port 443.
 - B. A firewall configuration is preventing the scan from succeeding.
 - C. The scanner configuration is preventing the scan from succeeding.
 - D. The CIFS file share is running on port 80.
- 240.** Thomas learned this morning of a critical security flaw that affects a major service used by his organization and requires immediate patching. This flaw was the subject of news reports and is being actively exploited. Thomas has a patch and informed stakeholders of the issue and received permission to apply the patch during business hours. How should he handle the change management process?
- A. Thomas should apply the patch and then follow up with an emergency change request after work is complete.
 - B. Thomas should initiate a standard change request but apply the patch before waiting for approval.
 - C. Thomas should work through the standard change approval process and wait until it is complete to apply the patch.
 - D. Thomas should file an emergency change request and wait until it is approved to apply the patch.
- 241.** After running a vulnerability scan of systems in his organization's development shop, Mike discovers the issue shown here on several systems. What is the best solution to this vulnerability?

5 EOL/Obsolete Software: Microsoft .NET Framework 4 - 4.5.1 Detected				
First Detected:	02/04/2020 at 19:05:19 (GMT-0400)	Last Detected:	04/05/2020 at 01:00:07 (GMT-0400)	Times Detected: 15
QID:	105648	CVSS Base:	9.3 ^[1]	Last Fixed: N/A
Category:	Security Policy	CVSS Temporal:	7.9	
CVE ID:	-	CVSS3 Base:	-	
Vendor Reference	Microsoft .NET Framework Product Lifecycle	CVSS3 Temporal:	-	
Bugtraq ID:	-	CVSS Environment:	-	
Service Modified:	03/10/2020	Asset Group:	-	
User Modified:	-	Collateral Damage Potential:	-	
Edited:	No	Target Distribution:	-	
PCI Vuln:	Yes	Confidentiality Requirement:	-	
Ticket State:	Open	Integrity Requirement:	-	
		Availability Requirement:	-	

- A. Apply the required security patches to this framework.
- B. Remove this framework from the affected systems.
- C. Upgrade the operating system of the affected systems.
- D. No action is necessary.

- 242.** Tran is preparing to conduct vulnerability scans against a set of workstations in his organization. He is particularly concerned about system configuration settings. Which one of the following scan types will give him the best results?
- A.** Unauthenticated scan
 - B.** Credentialed scan
 - C.** External scan
 - D.** Internal scan
- 243.** Brian is configuring a vulnerability scan of all servers in his organization's datacenter. He is configuring the scan to only detect the highest-severity vulnerabilities. He would like to empower system administrators to correct issues on their servers but also have some insight into the status of those remediations. Which approach would best serve Brian's interests?
- A.** Give the administrators access to view the scans in the vulnerability scanning system.
 - B.** Send email alerts to administrators when the scans detect a new vulnerability on their servers.
 - C.** Configure the vulnerability scanner to open a trouble ticket when they detect a new vulnerability on a server.
 - D.** Configure the scanner to send reports to Brian who can notify administrators and track them in a spreadsheet.
- 244.** Xiu Ying is configuring a new vulnerability scanner for use in her organization's datacenter. Which one of the following values is considered a best practice for the scanner's update frequency?
- A.** Daily
 - B.** Weekly
 - C.** Monthly
 - D.** Quarterly
- 245.** Ben was recently assigned by his manager to begin the remediation work on the most vulnerable server in his organization. A portion of the scan report appears here. What remediation action should Ben take first?
- A.** Install patches for Adobe Flash.
 - B.** Install patches for Firefox.
 - C.** Run Windows Update.
 - D.** Remove obsolete software.

▼ Vulnerabilities (50)	
5	Mozilla Firefox Multiple Vulnerabilities (MFSa2017-05,MFSa2017-06)
5	Adobe Flash Player Remote Code Execution Vulnerability (APSB17-07)
5	Mozilla Firefox Integer Overflow Vulnerability (MFSa2017-08)
5	Microsoft SMB Server Remote Code Execution Vulnerability (MS17-010)
5	Microsoft Cumulative Security Update for Internet Explorer (MS17-006)
5	Microsoft Windows Update for Vulnerabilities in Adobe Flash Player in Internet Explorer and Edge (MS17-023)
4	Microsoft XML Core Services Information Disclosure Vulnerability (MS17-022)
4	Microsoft IIS Server XSS Elevation of Privilege Vulnerability (MS17-016)
4	Microsoft Windows Kernel Elevation of Privileges (MS17-017)
4	Microsoft Uniscribe Multiple Remote Code Execution and Information Disclosure Vulnerabilities (MS17-011)
4	Microsoft Security Update for Windows Kernel-Mode Drivers (MS17-018)
4	Microsoft Windows DirectShow Information Disclosure Vulnerability (MS17-021)
3	NotePad++ "scilexer.dll" DLL Hijacking Vulnerability
3	Microsoft Windows PDF Library Remote Code Execution Vulnerability (MS17-009)
3	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)
5	Mozilla Firefox Multiple Vulnerabilities (MFSa2016-94,MFSa2016-96)
5	Mozilla Firefox Multiple Vulnerabilities (MFSa 2015-116 and MFSa 2015-133)
5	Mozilla Firefox Multiple Vulnerabilities (MFSa2016-89,MFSa2016-90)
5	Mozilla Firefox and Thunderbird SVG Animation Remote Code Execution Vulnerability (MFSa2016-92)
5	EOL/Obsolete Software: Microsoft VC++ 2005 Detected
5	Mozilla Firefox Multiple Vulnerabilities (MFSa2017-01,MFSa2017-02)
5	Adobe Flash Player Remote Code Execution Vulnerability (APSB17-04)
5	Microsoft Windows Update for Vulnerabilities in Adobe Flash Player in Internet Explorer (MS17-005)
5	EOL/Obsolete Software: Microsoft .NET Framework 4 - 4.5.1 Detected
5	Mozilla Firefox Multiple Vulnerabilities (MFSa 2016-85 to MFSa 2016-86)
4	Microsoft Windows .NET Framework Information Disclosure Vulnerability (MS16-091)
4	Mozilla Firefox Multiple Vulnerabilities (MFSa 2016-16 to MFSa 2016-38)

246. Tom is planning a series of vulnerability scans and wants to ensure that the organization is meeting its customer commitments with respect to the scans' performance impact. What two documents should Tom consult to find these obligations?
- SLAs and MOUs
 - SLAs and DRPs
 - DRPs and BIAs
 - BIAs and MOUs
247. Zhang Wei is evaluating the success of his vulnerability management program and would like to include some metrics. Which one of the following would be the *least* useful metric?
- Time to resolve critical vulnerabilities
 - Number of open critical vulnerabilities over time
 - Total number of vulnerabilities reported
 - Number of systems containing critical vulnerabilities

248. Zhang Wei completed a vulnerability scan of his organization's virtualization platform from an external host and discovered the vulnerability shown here. How should he react?

1 Remote Management Service Accepting Unencrypted Credentials Detected			
First Detected:	09/04/2019 at 18:04:22 (GMT-0400)	Last Detected:	04/05/2020 at 00:05:04 (GMT-0400)
QID:	45242	CVSS Base:	4.3[1]
Category:	Information gathering	CVSS Temporal:	3.3
CVE ID:	-	CVSS3 Base:	-
Vendor Reference:	-	CVSS3 Temporal:	-
Bugtraq ID:	-	CVSS Environment:	-
Service Modified:	08/10/2020	Asset Group:	-
User Modified:	-	Collateral Damage Potential:	-
Edited:	No	Target Distribution:	-
PCI Vuln:	Yes	Confidentiality Requirement:	-
Ticket State:	-	Integrity Requirement:	-
		Availability Requirement:	-

- A. This is a critical issue that requires immediate adjustment of firewall rules.
- B. This issue has a very low severity and does not require remediation.
- C. This issue should be corrected as time permits.
- D. This is a critical issue, and Zhang Wei should shut down the platform until it is corrected.
249. Elliott runs a vulnerability scan of one of the servers belonging to his organization and finds the results shown here. Which one of these statements is *not* correct?

Vulnerabilities (29)		
5 Red Hat Update for firefox Security (RHSA-2017:0459)	CVSS: -	CVSS3: - New
3 Red Hat Update for openssl Security (RHSA-2017:0641)	CVSS: -	CVSS3: - New
3 Red Hat Update for coreutils Security (RHSA-2017:0654)	CVSS: -	CVSS3: - New
3 Red Hat Update for glibc Security (RHSA-2017:0680)	CVSS: -	CVSS3: - New
3 Red Hat Update for subscription-manager Security (RHSA-2017:0698)	CVSS: -	CVSS3: - New
3 Red Hat Update for bash Security (RHSA-2017:0725)	CVSS: -	CVSS3: - New
3 Red Hat Update for kernel Security (RHSA-2017:0817)	CVSS: -	CVSS3: - New
3 Red Hat Update for curl Security (RHSA-2017:0847)	CVSS: -	CVSS3: - New
3 Red Hat Update for gnutls Security (RHSA-2017:0574)	CVSS: -	CVSS3: - New
5 Oracle Java SE Critical Patch Update - October 2016	CVSS: -	CVSS3: - Active
5 Oracle Java SE Critical Patch Update - January 2017	CVSS: -	CVSS3: - Active
5 Red Hat Update for Firefox Security (RHSA-2017:0190)	CVSS: -	CVSS3: - Active
4 Oracle Java SE Critical Patch Update - October 2015	CVSS: -	CVSS3: - Active
4 Oracle Java SE Critical Patch Update - January 2016	CVSS: -	CVSS3: - Active
4 Oracle Java SE Critical Patch Update - July 2015	CVSS: -	CVSS3: - Active
4 Oracle Java SE Critical Patch Update - July 2016	CVSS: -	CVSS3: - Active
4 Oracle Java SE Critical Patch Update - April 2016	CVSS: -	CVSS3: - Active
4 Red Hat Update for kernel (RHSA-2016:2006)	CVSS: -	CVSS3: - Active
4 Red Hat Update for kernel (RHSA-2016:2105) (Dirty Cow)	CVSS: -	CVSS3: - Active
4 Red Hat Update for kernel (RHSA-2016:2766)	CVSS: -	CVSS3: - Active
4 Red Hat Update for Kernel Security (RHSA-2017:0036)	CVSS: -	CVSS3: - Active
4 Red Hat Update for mysql Security (RHSA-2017:0184)	CVSS: -	CVSS3: - Active
4 Red Hat Update for Kernel Security (RHSA-2017:0293)	CVSS: -	CVSS3: - Active
3 Red Hat Update for libtiff Security (RHSA-2017:0225)	CVSS: -	CVSS3: - Active
3 Red Hat Update for ntp security (RHSA-2017:0252)	CVSS: -	CVSS3: - Active
3 Red Hat Update for openssl Security (RHSA-2017:0286)	CVSS: -	CVSS3: - Active
3 Red Hat Update for Kernel Security (RHSA-2017:0307)	CVSS: -	CVSS3: - Active
1 Non-Zero Padding Bytes Observed in Ethernet Packets	CVSS: -	CVSS3: - Active
3 Red Hat OpenSSL Denial of Service Vulnerability	CVSS: -	CVSS3: - Fixed

- A. This server requires one or more Linux patches.
- B. This server requires one or more Oracle database patches.
- C. This server requires one or more Firefox patches.
- D. This server requires one or more MySQL patches.

250. Donna is working with a system engineer who wants to remediate vulnerabilities in a server that he manages. Of the report templates shown here, which would be most useful to the engineer?

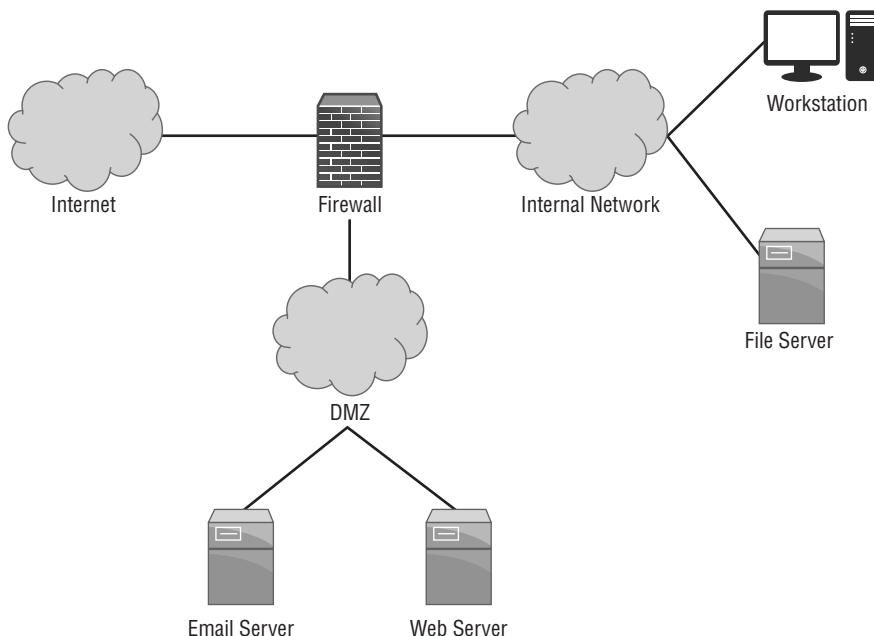
<input type="checkbox"/>	Title	Type	Vulnerability Data
<input type="checkbox"/>	Unknown Device Report		Scan Based
<input type="checkbox"/>	Executive Report		Host Based
<input type="checkbox"/>	High Severity Report		Host Based
<input type="checkbox"/>	Payment Card Industry (PCI) Executive Report		Scan Based
<input type="checkbox"/>	Payment Card Industry (PCI) Technical Report		Scan Based
<input type="checkbox"/>	Qualys Patch Report		Host Based
<input type="checkbox"/>	Qualys Top 20 Report		Host Based
<input type="checkbox"/>	Technical Report		Host Based

- A. Qualys Top 20 Report
 - B. PCI Technical Report
 - C. Executive Report
 - D. Technical Report
- 251.** Abdul received the vulnerability report shown here for a server in his organization. The server runs a legacy application that cannot easily be updated. What risks does this vulnerability present?

4 Unauthenticated Access to FTP Server Allowed			
First Detected:	07/16/2017 at 20:06:22 (GMT-0400)	Last Detected:	04/05/2020 at 00:05:04 (GMT-0400)
QID:	27210	CVSS Base:	7.8 ^[1]
Category:	File Transfer Protocol	CVSS Temporal:	7
CVE ID:	-	CVSS3 Base:	-
Vendor Reference:	-	CVSS3 Temporal:	-
Bugtraq ID:	-	CVSS Environment:	-
Service Modified:	10/25/2020	Asset Group:	-
User Modified:	-	Collateral Damage Potential:	-
Edited:	No	Target Distribution:	-
PCI Vuln:	Yes	Confidentiality Requirement:	-
Ticket State:	Open	Integrity Requirement:	-
		Availability Requirement:	-

- A. Unauthorized access to files stored on the server
- B. Theft of credentials
- C. Eavesdropping on communications
- D. All of the above

252. Tom runs a vulnerability scan of the file server shown here.



He receives the vulnerability report shown next. Assuming that the firewall is configured properly, what action should Tom take immediately?

Vulnerabilities (5)				
3	Windows Remote Desktop Protocol Weak Encryption Method Allowed	port 3389/tcp	CVSS: -	CVSS3: - Active
3	Built-in Guest Account Not Renamed at Windows Target System		CVSS: -	CVSS3: - Active
3	Administrator Account's Password Does Not Expire		CVSS: -	CVSS3: - Active
2	FIN-ACK Network Device Driver Frame Padding Information Disclosure Vulnerability		CVSS: -	CVSS3: - Active
1	Non-Zero Padding Bytes Observed in Ethernet Packets		CVSS: -	CVSS3: - Fixed

- A. Block RDP access to this server from all hosts.
 - B. Review and secure server accounts.
 - C. Upgrade encryption on the server.
 - D. No action is required.
253. Dave is running a vulnerability scan of a client's network for the first time. The client has never run such a scan and expects to find many results. What security control is likely to remediate the largest portion of the vulnerabilities discovered in Dave's scan?
- A. Input validation
 - B. Patching
 - C. Intrusion prevention systems
 - D. Encryption

- 254.** Kai is planning to patch a production system to correct a vulnerability detected during a scan. What process should she follow to correct the vulnerability but minimize the risk of a system failure?
- A.** Kai should deploy the patch immediately on the production system.
 - B.** Kai should wait 60 days to deploy the patch to determine whether bugs are reported.
 - C.** Kai should deploy the patch in a sandbox environment to test it prior to applying it in production.
 - D.** Kai should contact the vendor to determine a safe timeframe for deploying the patch in production.
- 255.** William is preparing a legal agreement for his organization to purchase services from a vendor. He would like to document the requirements for system availability, including the vendor's allowable downtime for patching. What type of agreement should William use to incorporate this requirement?
- A.** MOU
 - B.** SLA
 - C.** BPA
 - D.** BIA
- 256.** Given no other information, which one of the following vulnerabilities would you consider the greatest threat to information confidentiality?
- A.** HTTP TRACE/TRACK methods enabled
 - B.** SSL Server with SSL v3 enabled vulnerability
 - C.** phpinfo information disclosure vulnerability
 - D.** Web application SQL injection vulnerability
- 257.** Which one of the following mobile device strategies is most likely to result in the introduction of vulnerable devices to a network?
- A.** COPE
 - B.** TLS
 - C.** BYOD
 - D.** MDM
- 258.** Sophia discovered the vulnerability shown here on one of the servers running in her organization. What action should she take?

CRITICAL	Microsoft Windows Server 2003 Unsupported Installation Detection
Description	
The remote host is running Microsoft Windows Server 2003. Support for this operating system by Microsoft ended July 14th, 2015.	

- A.** Decommission this server.
- B.** Run Windows Update to apply security patches.
- C.** Require strong encryption for access to this server.
- D.** No action is required.

259. Ling recently completed the security analysis of a web browser deployed on systems in her organization and discovered that it is susceptible to a zero-day integer overflow attack. Who is in the best position to remediate this vulnerability in a manner that allows continued use of the browser?
- Ling
 - The browser developer
 - The network administrator
 - The domain administrator
260. Jeff's team is preparing to deploy a new database service, and he runs a vulnerability scan of the test environment. This scan results in the four vulnerability reports shown here. Jeff is primarily concerned with correcting issues that may lead to a confidentiality breach. Which vulnerability should Jeff remediate first?

				NetApp
Vulnerabilities (2)				
3	Rational ClearCase Portscan Denial of Service Vulnerability	port 371/tcp	CVSS: - CVSS3: -	New
1	Non-Zero Padding Bytes Observed in Ethernet Packets		CVSS: - CVSS3: -	Active
				Linux 2.4-2.6
Vulnerabilities (3)				
4	Oracle Database TNS Listener Poison Attack Vulnerability	port 1521/tcp	CVSS: - CVSS3: -	Active
2	Hidden RPC Services		CVSS: - CVSS3: -	Active
2	UDP Constant IP Identification Field Fingerprinting Vulnerability		CVSS: - CVSS3: -	Active

- Rational ClearCase Portscan Denial of Service vulnerability
 - Non-Zero Padding Bytes Observed in Ethernet Packets
 - Oracle Database TNS Listener Poison Attack vulnerability
 - Hidden RPC Services
261. Eric is a security consultant and is trying to sell his services to a new client. He would like to run a vulnerability scan of their network prior to their initial meeting to show the client the need for added security. What is the most significant problem with this approach?
- Eric does not know the client's infrastructure design.
 - Eric does not have permission to perform the scan.
 - Eric does not know what operating systems and applications are in use.
 - Eric does not know the IP range of the client's systems.
262. Renee is assessing the exposure of her organization to the denial-of-service vulnerability in the scan report shown here. She is specifically interested in determining whether an external attacker would be able to exploit the denial-of-service vulnerability. Which one of the following sources of information would provide her with the best information to complete this assessment?

MediaWiki Information Disclosure, Denial of Service and Multiple Cross-Site Scripting Vulnerabilities

First Detected:	04/09/2020 at 04:49:37 (GMT-0400)	Last Detected:	04/09/2020 at 04:49:37 (GMT-0400)	Times Detected:	1	Last Fixed:	N/A
QID:	12828	CVSS Base:	7.5				
Category:	CGI	CVSS Temporal:	5.5				
CVE ID:	CVE-2013-6451 CVE-2013-6452 CVE-2013-6453 CVE-2013-6454 CVE-2013-6455 CVE-2013-4570 CVE-2013-4571 CVE-2013-6472 CVE-2013-4574	CVSS3 Base:	-				
		CVSS3 Temporal:	-				
		CVSS3 Environment:	-				
Vendor Reference	MediaWiki	Asset Group:	-				
Bugtraq ID:	-	Collateral Damage Potential:	-				
Service Modified:	03/03/2020	Target Distribution:	-				
User Modified:	-	Confidentiality Requirement:	-				
Edited:	No	Integrity Requirement:	-				
PCI Vuln:	Yes	Availability Requirement:	-				
Ticket State:							

THREAT:

MediaWiki is free and open source wiki software developed by the Wikimedia. It's used to power wiki web sites such as Wikipedia, Wiktionary and Commons. Multiple security vulnerabilities have been reported in MediaWiki, which can be exploited to conduct script insertion attacks and disclose potentially sensitive information.

- Certain input containing specially crafted CSS tags is not properly sanitized before being used. This can be exploited to insert arbitrary HTML and script code
- Certain input containing specially crafted XLS tags within a SVG file is not properly sanitized before being used. This can be exploited to insert arbitrary HTML and script code
- An error within the "UploadBase::detectScriptInSvg()" method can be exploited to upload SVG files containing arbitrary script code
- Certain input containing specially crafted CSS tags is not properly sanitized before being used. This can be exploited to insert arbitrary HTML and script code, which will be executed in the browser
- Errors within the log API, enhanced RecentChanges, and user watchlists can be exploited to disclose certain information about deleted pages.
- A cross-site scripting vulnerability in TimedMediaHandler extension exists due to way it stored and used HTML for showing videos
- NULL pointer dereference in php-luasandbox, which could be used for DoS attacks.
- Buffer Overflow in php-luasandbox.

Affected Version:
MediaWiki version prior to 1.19.10, 1.21.4, or 1.22.1.

- A. Server logs
- B. Firewall rules
- C. IDS configuration
- D. DLP configuration

263. Mary is trying to determine what systems in her organization should be subject to vulnerability scanning. She would like to base this decision on the criticality of the system to business operations. Where should Mary turn to best find this information?

- A. The CEO
- B. System names
- C. IP addresses
- D. Asset inventory

264. Paul ran a vulnerability scan of his vulnerability scanner and received the result shown here. What is the simplest fix to this issue?

MEDIUM Tenable Nessus 6.0.x < 6.6 Multiple Vulnerabilities

Description

According to its version, the Tenable Nessus application installed on the remote host is 6.x prior to 6.6. It is, therefore, affected by multiple vulnerabilities :

- A cross-site scripting (XSS) vulnerability exists due to improper validation of user-supplied input. An authenticated, remote attacker can exploit this, via a specially crafted request, to execute arbitrary script code in a user's browser session. (CVE-2016-82012)
- A denial of service vulnerability exists due to an external entity injection (XXE) flaw that is triggered during the parsing of XML data. An authenticated, remote attacker can exploit this, via specially crafted XML data, to exhaust system resources. (CVE-2016-82013)

- A. Upgrade Nessus.
 - B. Remove guest accounts.
 - C. Implement TLS encryption.
 - D. Renew the server certificate.
265. Kamea is designing a vulnerability management system for her organization. Her highest priority is conserving network bandwidth. She does not have the ability to alter the configuration or applications installed on target systems. What solution would work best in Kamea's environment to provide vulnerability reports?
- A. Agent-based scanning
 - B. Server-based scanning
 - C. Passive network monitoring
 - D. Port scanning
266. Aki is conducting a vulnerability scan when he receives a report that the scan is slowing down the network for other users. He looks at the performance configuration settings shown here. Which setting would be most likely to correct the issue?

Settings / Advanced

General Settings

☒ Enable safe checks

☐ Stop scanning hosts that become unresponsive during the scan

☐ Scan IP addresses in a random order

Performance Options

☐ Slow down the scan when network congestion is detected

☐ Use Linux kernel congestion detection

Network timeout (in seconds)

Max simultaneous checks per host

Max simultaneous hosts per scan

Max number of concurrent TCP sessions per host

Max number of concurrent TCP sessions per scan

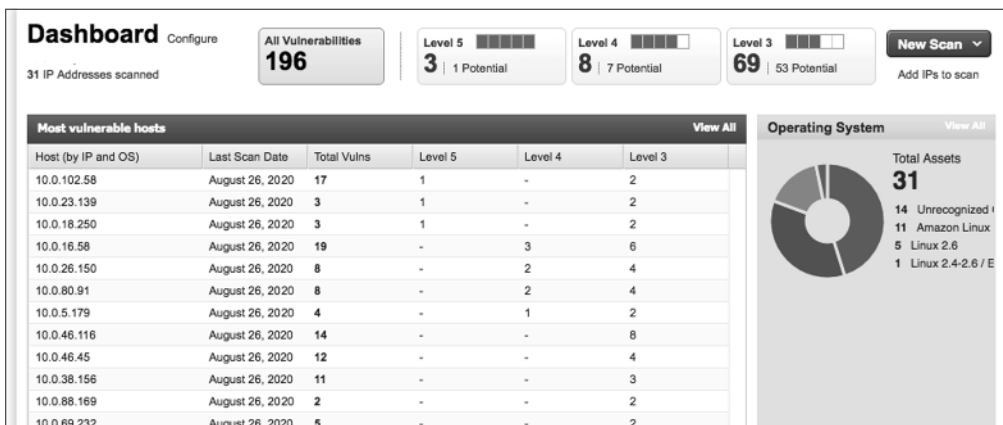
- A. Enable safe checks.
 - B. Stop scanning hosts that become unresponsive during the scan.
 - C. Scan IP addresses in random order.
 - D. Max simultaneous hosts per scan.
- 267.** Laura received a vendor security bulletin that describes a zero-day vulnerability in her organization's main database server. This server is on a private network but is used by publicly accessible web applications. The vulnerability allows the decryption of administrative connections to the server. What reasonable action can Laura take to address this issue as quickly as possible?
- A. Apply a vendor patch that resolves the issue.
 - B. Disable all administrative access to the database server.
 - C. Require VPN access for remote connections to the database server.
 - D. Verify that the web applications use strong encryption.
- 268.** Emily discovered the vulnerability shown here on a server running in her organization. What is the most likely underlying cause for this vulnerability?

4 Microsoft Windows OLE Remote Code Execution Vulnerability (MS16-044)			
First Detected:	04/04/2020 at 18:05:17 (GMT-0400)	Last Detected:	04/04/2020 at 22:07:28 (GMT-0400)
QID:	91198	CVSS Base:	9.3
Category:	Windows	CVSS Temporal:	6.9
CVE ID:	CVE-2016-0153	CVSS3 Base:	7.8
Vendor Reference	MS16-044	CVSS3 Temporal:	6.8
Bugtraq ID:	-	CVSS Environment:	-
Service Modified:	04/12/2020	Asset Group:	-
User Modified:	-	Collateral Damage Potential:	-
Edited:	No	Target Distribution:	-
PCI Vuln:	Yes	Confidentiality Requirement:	-
Ticket State:	Open	Integrity Requirement:	-
		Availability Requirement:	-

- A. Failure to perform input validation
 - B. Failure to use strong passwords
 - C. Failure to encrypt communications
 - D. Failure to install antimalware software
- 269.** Raul is replacing his organization's existing vulnerability scanner with a new product that will fulfill that functionality moving forward. As Raul begins to build the policy, he notices some conflicts in the scanning settings between different documents. Which one of the following document sources should Raul give the highest priority when resolving these conflicts?
- A. NIST guidance documents
 - B. Vendor best practices

- C. Corporate policy
- D. Configuration settings from the prior system

270. Rex recently ran a vulnerability scan of his organization's network and received the results shown here. He would like to remediate the server with the highest number of the most serious vulnerabilities first. Which one of the following servers should be on his highest priority list?



- A. 10.0.102.58
- B. 10.0.16.58
- C. 10.0.46.116
- D. 10.0.69.232

271. Abella is configuring a vulnerability scanning tool. She recently learned about a privilege escalation vulnerability that requires the user already have local access to the system. She would like to ensure that her scanners are able to detect this vulnerability as well as future similar vulnerabilities. What action can she take that would best improve the scanner's ability to detect this type of issue?

- A. Enable credentialed scanning.
- B. Run a manual vulnerability feed update.
- C. Increase scanning frequency.
- D. Change the organization's risk appetite.

272. Kylie reviewed the vulnerability scan report for a web server and found that it has multiple SQL injection and cross-site scripting vulnerabilities. What would be the least difficult way for Kylie to address these issues?

- A. Install a web application firewall.
- B. Recode the web application to include input validation.

- C. Apply security patches to the server operating system.
- D. Apply security patches to the web server service.
- 273.** Pietro is responsible for distributing vulnerability scan reports to system engineers who will remediate the vulnerabilities. What would be the most effective and secure way for Pietro to distribute the reports?
- A. Pietro should configure the reports to generate automatically and provide immediate, automated notification to administrators of the results.
- B. Pietro should run the reports manually and send automated notifications after he reviews them for security purposes.
- C. Pietro should run the reports on an automated basis and then manually notify administrators of the results after he reviews them.
- D. Pietro should run the reports manually and then manually notify administrators of the results after he reviews them.
- 274.** Karen ran a vulnerability scan of a web server used on her organization's internal network. She received the report shown here. What circumstances would lead Karen to dismiss this vulnerability as a false positive?

2 SSL Certificate - Signature Verification Failed Vulnerability		port 3389/tcp over SSL CVSS: - CVSS3: - Active	
First Detected:	05/11/2017 at 02:00:07 (GMT-0400)	Last Detected:	04/04/2020 at 21:30:12 (GMT-0400)
QID:	38173	CVSS Base:	9.4
Category:	General remote services	CVSS Temporal:	6.8
CVE ID:	-	CVSS3 Base:	-
Vendor Reference:	-	CVSS3 Temporal:	-
Bugtraq ID:	-	CVSS Environment:	-
Service Modified:	05/22/2020	Asset Group:	-
User Modified:	-	Collateral Damage Potential:	-
Edited:	No	Target Distribution:	-
PCI Vuln:	Yes	Confidentiality Requirement:	-
Ticket State:	-	Integrity Requirement:	-
		Availability Requirement:	-
THREAT:			
An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority. If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.			
IMPACT:			
By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.			
Exception:			
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.			
SOLUTION:			
Please install a server certificate signed by a trusted third-party Certificate Authority.			
EXPLOITABILITY:			
There is no exploitability information for this vulnerability.			

- A. The server is running SSL v2.
- B. The server is running SSL v3.
- C. The server is for internal use only.
- D. The server does not contain sensitive information.

275. Which one of the following vulnerabilities is the most difficult to confirm with an external vulnerability scan?
- Cross-site scripting
 - Cross-site request forgery
 - Blind SQL injection
 - Unpatched web server
276. Ann would like to improve her organization's ability to detect and remediate security vulnerabilities by adopting a continuous monitoring approach. Which one of the following is *not* a characteristic of a continuous monitoring program?
- Analyzing and reporting findings
 - Conducting forensic investigations when a vulnerability is exploited
 - Mitigating the risk associated with findings
 - Transferring the risk associated with a finding to a third party
277. Holly ran a scan of a server in her datacenter and the most serious result was the vulnerability shown here. What action is most commonly taken to remediate this vulnerability?

3 phpinfo Information Disclosure Vulnerability


















First Detected: 07/17/2019 at 12:02:41 (GMT-0400)	Last Detected: 04/09/2020 at 17:39:08 (GMT-0400)	Times Detected: 38	Last Fixed: N/A
QID: 10464	CVSS Base: 5.1		
Category: CGI	CVSS Temporal: 3.8		
CVE ID: -	CVSS3 Base: -		
Vendor Reference: -	CVSS3 Temporal: -		
Bugtraq ID: -	CVSS Environment: -		
Service Modified: 06/21/2020	Asset Group: -		
User Modified: -	Collateral Damage Potential: -		
Edited: No	Target Distribution: -		
PCI Vuln: Yes	Confidentiality Requirement: -		
Ticket State:	Integrity Requirement: -		
	Availability Requirement: -		

THREAT:
This host has a publicly-accessible PHP file that calls the phpinfo() function (or some other function similar to it). If a user requests this file (such as via an Internet browser), the user may obtain a page containing sensitive information about the Web server host. The information displayed to the user Web Servers, PHP, XML, MySQL), the values of some environment variables (\$PATH, \$SYSTEM_ROOT), paths to various programs (cmd.exe), and much more. To get specific information about the type of data your host displayed, please refer to the "Result" field below.

IMPACT:
By exploiting this vulnerability, any user could obtain very sensitive information about the Web server host. This information may aid in attacks against the host.

- Remove the file from the server.
- Edit the file to limit information disclosure.
- Password protect the file.
- Limit file access to a specific IP range.

- 278.** Nitesh would like to identify any systems on his network that are not registered with his asset management system because he is concerned that they might not be remediated to his organization's current security configuration baseline. He looks at the reporting console of his vulnerability scanner and sees the options shown here. Which of the following report types would be his best likely starting point?

<input type="checkbox"/>  Title	Type Vulnerability Data
<input type="checkbox"/>  Unknown Device Report	 Scan Based
<input type="checkbox"/>  Executive Report	 Host Based
<input type="checkbox"/>  High Severity Report	 Host Based
<input type="checkbox"/>  Payment Card Industry (PCI) Executive Report	 Scan Based
<input type="checkbox"/>  Payment Card Industry (PCI) Technical Report	 Scan Based
<input type="checkbox"/>  Qualys Patch Report	 Host Based
<input type="checkbox"/>  Qualys Top 20 Report	 Host Based
<input type="checkbox"/>  Technical Report	 Host Based

- A. Technical Report
 - B. High Severity Report
 - C. Qualys Patch Report
 - D. Unknown Device Report
- 279.** What strategy can be used to immediately report configuration changes to a vulnerability scanner?
- A. Scheduled scans
 - B. Continuous monitoring
 - C. Automated remediation
 - D. Automatic updates
- 280.** During a recent vulnerability scan, Mark discovered a flaw in an internal web application that allows cross-site scripting attacks. He spoke with the manager of the team responsible for that application and was informed that he discovered a known vulnerability and the manager worked with other leaders and determined that the risk is acceptable and does not require remediation. What should Mark do?

- A. Object to the manager's approach and insist on remediation.
 - B. Mark the vulnerability as a false positive.
 - C. Schedule the vulnerability for remediation in six months.
 - D. Mark the vulnerability as an exception.
- 281.** Jacquelyn recently read about a new vulnerability in Apache web servers that allows attackers to execute arbitrary code from a remote location. She verified that her servers have this vulnerability, but this morning's vulnerability scan report shows that the servers are secure. She contacted the vendor and determined that they have released a signature for this vulnerability and it is working properly at other clients. What action can Jacquelyn take that will most likely address the problem efficiently?
- A. Add the web servers to the scan.
 - B. Reboot the vulnerability scanner.
 - C. Update the vulnerability feed.
 - D. Wait until tomorrow's scan.
- 282.** Vincent is a security manager for a U.S. federal government agency subject to FISMA. Which one of the following is *not* a requirement that he must follow for his vulnerability scans to maintain FISMA compliance?
- A. Run complete scans on at least a monthly basis.
 - B. Use tools that facilitate interoperability and automation.
 - C. Remediate legitimate vulnerabilities.
 - D. Share information from the vulnerability scanning process.
- 283.** Sharon is designing a new vulnerability scanning system for her organization. She must scan a network that contains hundreds of unmanaged hosts. Which of the following techniques would be most effective at detecting system configuration issues in her environment?
- A. Agent-based scanning
 - B. Credentialed scanning
 - C. Server-based scanning
 - D. Passive network monitoring

Use the following scenario to answer questions 284–286.

Arlene ran a vulnerability scan of a VPN server used by contractors and employees to gain access to her organization's network. An external scan of the server found the vulnerability shown here.

MEDIUM **SSL Certificate Signed Using Weak Hashing Algorithm** < >


Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm. These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.







Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunseting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database have been ignored.

- 284.** Which one of the following hash algorithms would *not* trigger this vulnerability?
- A. MD4
 - B. MD5
 - C. SHA-1
 - D. SHA-256
- 285.** What is the most likely result of failing to correct this vulnerability?
- A. All users will be able to access the site.
 - B. All users will be able to access the site, but some may see an error message.
 - C. Some users will be unable to access the site.
 - D. All users will be unable to access the site.
- 286.** How can Arlene correct this vulnerability?
- A. Reconfigure the VPN server to only use secure hash functions.
 - B. Request a new certificate.
 - C. Change the domain name of the server.
 - D. Implement an intrusion prevention system.
- 287.** After reviewing the results of a vulnerability scan, Bruce discovered that many of the servers in his organization are susceptible to a brute-force SSH attack. He would like to determine what external hosts attempted SSH connections to his servers and is reviewing firewall logs. What TCP port would relevant traffic most likely use?
- A. 22
 - B. 636
 - C. 1433
 - D. 1521
- 288.** Joaquin runs a vulnerability scan of the network devices in his organization and sees the vulnerability report shown here for one of those devices. What action should he take?

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN				port 443/tcp over SSL		Active					
First Detected:		08/22/2018 at 20:52:54 (GMT-0400)		Last Detected:		04/11/2020 at 09:54:48 (GMT-0400)		Times Detected:	6	Last Fixed:	N/A
QID:		38170									
Category:		General remote services									
CVE ID:		-									
Vendor Reference		-									
Bugtraq ID:		-									
Service Modified:		08/12/2020									
User Modified:		-									
Edited:		No									
PCI Vuln:		No									
Ticket State:											

- A. No action is necessary because this is an informational report.
 - B. Upgrade the version of the certificate.
 - C. Replace the certificate.
 - D. Verify that the correct ciphers are being used.
289. Lori is studying vulnerability scanning as she prepares for the CySA+ exam. Which of the following is *not* one of the principles she should observe when preparing for the exam to avoid causing issues for her organization?
- A. Run only nondangerous scans on production systems to avoid disrupting a production service.
 - B. Run scans in a quiet manner without alerting other IT staff to the scans or their results to minimize the impact of false information.
 - C. Limit the bandwidth consumed by scans to avoid overwhelming an active network link.
 - D. Run scans outside of periods of critical activity to avoid disrupting the business.
290. Meredith is configuring a vulnerability scan and would like to configure the scanner to perform credentialed scans. Of the menu options shown here, which will allow her to directly configure this capability?

 <p>Manage Vulnerability Scans Launch new vulnerability scans, monitor the status of running scans and view the details of vulnerabilities discovered after scans complete. Watch demo  (8min 0sec)</p>	 <p>Configure Scan Schedules Configure scans to run automatically, or on a recurring basis and monitor results of your scans. Watch demo  (4min 0sec)</p>
 <p>Manage Discovery Scans Use free discovery scans (maps) to discover live devices on your network. Discovered devices can be selected for vulnerability scanning based on the info gathered (OS, ports, etc.) in a map. Watch demo  (6min 6sec)</p>	 <p>Configure Scanner Appliances Scanner Appliances (physical or virtual) are required to scan devices on internal networks. Managers can download appliances and configure them for scanning.</p>
 <p>Configure Scan Settings Customize the various scanning options required to run a scan. These can be saved as profiles for reuse. A default profile is provided for common environments. Watch demo  (9min 28sec)</p>	 <p>Set Up Host Authentication Use the authentication feature (Windows, Linux, Oracle, etc) to discover and validate vulnerabilities by performing an in-depth assessment of your hosts. Watch demo  (9min 28sec)</p>
 <p>Configure Search Lists Apply custom lists of vulnerabilities to scan profiles in order to limit scanning to certain vulnerabilities only.</p>	

- A. Manage Discovery Scans
- B. Configure Scan Settings
- C. Configure Search Lists
- D. Set Up Host Authentication

291. Norman is working with his manager to implement a vulnerability management program for his company. His manager tells him that he should focus on remediating critical and high-severity risks and that the organization does not want to spend time worrying about risks rated medium or lower. What type of criteria is Norman's manager using to make this decision?

- A. Risk appetite
- B. False positive
- C. False negative
- D. Data classification

292. After running a vulnerability scan against his organization's VPN server, Luis discovered the vulnerability shown here. What type of cryptographic situation does a birthday attack leverage?

▼ Vulnerabilities (8)			
3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)			
First Detected: 04/05/2020 at 03:14:48 (GMT-0400)		Last Detected: 04/05/2020 at 03:14:48 (GMT-0400)	
QID: 38657		CVSS Base: 5	
Category: General remote services		CVSS Temporal: 4.3	
CVE ID: CVE-2016-2183		CVSS3 Base: 5.3	
Vendor Reference: -		CVSS3 Temporal: 4.9	
Bugtraq ID: 92630, 95568		CVSS Environment:	
Service Modified: 04/04/2020		Asset Group: -	
User Modified: -		Collateral Damage Potential: -	
Edited: No		Target Distribution: -	
PCI Vuln: Yes		Confidentiality Requirement: -	
Ticket State:		Integrity Requirement: -	
		Availability Requirement: -	

- A. Unsecured key
- B. Meet-in-the-middle
- C. Man-in-the-middle
- D. Collision

293. Meredith recently ran a vulnerability scan on her organization's accounting network segment and found the vulnerability shown here on several workstations. What would be the most effective way for Meredith to resolve this vulnerability?

5 Adobe Flash Player Remote Code Execution Vulnerability (APSB17-07)				
First Detected:	04/05/2020 at 01:00:07 (GMT-0400)	Last Detected:	04/05/2020 at 01:00:07 (GMT-0400)	Times Detected: 1 Last Fixed: N/A
QID:	370337	CVSS Base:	10	
Category:	Local	CVSS Temporal:	7.4	
CVE ID:	CVE-2017-2997 CVE-2017-2998 CVE-2017-2999 CVE-2017-3000 CVE-2017-3001 CVE-2017-3002 CVE-2017-3003	CVSS3 Base:	9.8	
Vendor Reference:	APSB17-07	CVSS3 Temporal:	8.5	
Bugtraq ID:	96860, 96866, 96862, 96861	CVSS Environment:		
Service Modified:	03/17/2020	Asset Group:	-	
User Modified:	-	Collateral Damage Potential:	-	
Edited:	No	Target Distribution:	-	
PCI Vuln:	Yes	Confidentiality Requirement:	-	
Ticket State:	Open	Integrity Requirement:	-	
		Availability Requirement:	-	
THREAT:				
Cross-platform plugin plays animations, videos and sound files in .SWF format.				
These vulnerabilities that could potentially allow an attacker to take control of the affected system. (CVE-2017-2997, CVE-2017-2998, CVE-2017-2999, CVE-2017-3000, CVE-2017-3001, CVE-2017-3002, CVE-2017-3003)				
Affected Versions:				
Adobe Flash Player 24.0.0.221 and earlier				
IMPACT:				
Successful exploitation allows a remote, unauthenticated attacker to execute arbitrary code on a targeted system.				

- A. Remove Flash Player from the workstations.
- B. Apply the security patches described in the Adobe bulletin.
- C. Configure the network firewall to block unsolicited inbound access to these workstations.
- D. Install an intrusion detection system on the network.

294. Nabil is the vulnerability manager for his organization and is responsible for tracking vulnerability remediation. There is a critical vulnerability in a network device that Nabil has handed off to the device's administrator, but it has not been resolved after repeated reminders to the engineer. What should Nabil do next?

- A. Threaten the engineer with disciplinary action.
- B. Correct the vulnerability himself.
- C. Mark the vulnerability as an exception.
- D. Escalate the issue to the network administrator's manager.

295. Sara's organization has a well-managed test environment. What is the most likely issue that Sara will face when attempting to evaluate the impact of a vulnerability remediation by first deploying it in the test environment?

- A. Test systems are not available for all production systems.
- B. Production systems require a different type of patch than test systems.
- C. Significant configuration differences exist between test and production systems.
- D. Test systems are running different operating systems than production systems.

296. How many vulnerabilities listed in the report shown here are significant enough to warrant immediate remediation in a typical operating environment?

▼ Vulnerabilities (22)			
▶	3	NetBIOS Shared Folder List Available	CVSS: - CVSS3: - Active
▶	3	NFS Exported Filesystems List Vulnerability	CVSS: - CVSS3: - Active
▶	3	SSL Server Has SSLv3 Enabled Vulnerability	port 443/tcp over SSL CVSS: - CVSS3: - Active
▶	3	SSL Server Has SSLv2 Enabled Vulnerability	port 443/tcp over SSL CVSS: - CVSS3: - Active
▶	3	SSL/TLS use of weak RC4 cipher	port 443/tcp over SSL CVSS: - CVSS3: - Active
▶	2	Default Windows Administrator Account Name Present	CVSS: - CVSS3: - Active
▶	2	YP/NIS RPC Services Listening on Non-Privileged Ports	CVSS: - CVSS3: - Active
▶	2	NetBIOS Name Accessible	CVSS: - CVSS3: - Active
▶	2	Hidden RPC Services	CVSS: - CVSS3: - Active
▶	2	SSL Certificate - Improper Usage Vulnerability	port 443/tcp over SSL CVSS: - CVSS3: - Active
▶	2	SSL Certificate - Self-Signed Certificate	port 443/tcp over SSL CVSS: - CVSS3: - Active
▶	2	SSL Certificate - Subject Common Name Does Not Match Server FQDN	port 443/tcp over SSL CVSS: - CVSS3: - Active
▶	2	SSL Certificate - Signature Verification Failed Vulnerability	port 443/tcp over SSL CVSS: - CVSS3: - Active
▶	2	NTP Information Disclosure Vulnerability	port 123/udp CVSS: - CVSS3: - Active
▶	1	mountd RPC Daemon Discloses Exported Directories Accessed by Remote Hosts	CVSS: - CVSS3: - Active
▶	1	"quoted" RPC Service Present	CVSS: - CVSS3: - Active
▶	1	Non-Zero Padding Bytes Observed in Ethernet Packets	CVSS: - CVSS3: - Active
▶	1	Presence of a Load-Balancing Device Detected	port 443/tcp over SSL CVSS: - CVSS3: - Active
▶	1	Presence of a Load-Balancing Device Detected	port 80/tcp CVSS: - CVSS3: - Re-Opened

- A. 22
- B. 14
- C. 5
- D. 0

297. Maria discovered an operating system vulnerability on a system on her network. After tracing the IP address, she discovered that the vulnerability is on a proprietary search appliance installed on her network. She consulted with the responsible engineer who informed her that he has no access to the underlying operating system. What is the best course of action for Maria?
- A. Contact the vendor to obtain a patch.
 - B. Try to gain access to the underlying operating system and install the patch.
 - C. Mark the vulnerability as a false positive.
 - D. Wait 30 days and rerun the scan to see whether the vendor corrected the vulnerability.
298. Which one of the following types of data is subject to regulations in the United States that specify the minimum frequency of vulnerability scanning?
- A. Driver's license numbers
 - B. Insurance records
 - C. Credit card data
 - D. Medical records

- 299.** Chang is responsible for managing his organization's vulnerability scanning program. He is experiencing issues with scans aborting because the previous day's scans are still running when the scanner attempts to start the current day's scans. Which one of the following solutions is *least* likely to resolve Chang's issue?
- A.** Add a new scanner.
 - B.** Reduce the scope of the scans.
 - C.** Reduce the sensitivity of the scans.
 - D.** Reduce the frequency of the scans.
- 300.** Trevor is working with an application team on the remediation of a critical SQL injection vulnerability in a public-facing service. The team is concerned that deploying the fix will require several hours of downtime and that will block customer transactions from completing. What is the most reasonable course of action for Trevor to suggest?
- A.** Wait until the next scheduled maintenance window.
 - B.** Demand that the vulnerability be remediated immediately.
 - C.** Schedule an emergency maintenance for an off-peak time later in the day.
 - D.** Convene a working group to assess the situation.
- 301.** While conducting a vulnerability scan of his organization's datacenter, Annika discovers that the management interface for the organization's virtualization platform is exposed to the scanner. In typical operating circumstances, what is the proper exposure for this interface?
- A.** Internet
 - B.** Internal networks
 - C.** No exposure
 - D.** Management network
- 302.** Bhanu is scheduling vulnerability scans for her organization's datacenter. Which one of the following is a best practice that Bhanu should follow when scheduling scans?
- A.** Schedule scans so that they are spread evenly throughout the day.
 - B.** Schedule scans so that they run during periods of low activity.
 - C.** Schedule scans so that they all begin at the same time.
 - D.** Schedule scans so that they run during periods of peak activity to simulate performance under load.
- 303.** Kevin is concerned that an employee of his organization might fall victim to a phishing attack and wishes to redesign his social engineering awareness program. What type of threat is he most directly addressing?
- A.** Nation-state
 - B.** Hacktivist

- C. Unintentional insider
 - D. Intentional insider
- 304.** Alan recently reviewed a vulnerability report and determined that an insecure direct object reference vulnerability existed on the system. He implemented a remediation to correct the vulnerability. After doing so, he verifies that his actions correctly mitigated the vulnerability. What term best describes the initial vulnerability report?
- A. True positive
 - B. True negative
 - C. False positive
 - D. False negative
- 305.** Gwen is reviewing a vulnerability report and discovers that an internal system contains a serious flaw. After reviewing the issue with her manager, they decide that the system is sufficiently isolated and they will take no further action. What risk management strategy are they adopting?
- A. Risk avoidance
 - B. Risk mitigation
 - C. Risk transference
 - D. Risk acceptance
- 306.** Thomas discovers a vulnerability in a web application that is part of a proprietary system developed by a third-party vendor and he does not have access to the source code. Which one of the following actions can he take to mitigate the vulnerability without involving the vendor?
- A. Apply a patch
 - B. Update the source code
 - C. Deploy a web application firewall
 - D. Conduct dynamic testing
- 307.** Kira is using the aircrack-ng tool to perform an assessment of her organization's security. She ran a scan and is now reviewing the results. Which one of the following issues is she most likely to detect with this tool?
- A. Insecure WPA key
 - B. SQL injection vulnerability
 - C. Cross-site scripting vulnerability
 - D. Man-in-the-middle attack

- 308.** Walt is designing his organization's vulnerability management program and is working to identify potential inhibitors to vulnerability remediation. He has heard concern from functional leaders that remediating vulnerabilities will impact the ability of a new system to fulfill user requests. Which one of the following inhibitors does not apply to this situation?
- A.** Degrading functionality
 - B.** Organizational governance
 - C.** Legacy systems
 - D.** Business process interruption

