Chapter

1

Practice Test 1

1. Which of the following is considered a passive reconnaissance action?
   - **A.** Searching through the local paper
   - **B.** Calling Human Resources
   - **C.** Using the `nmap -sT` command
   - **D.** Conducting a man-in-the-middle attack

2. Which encryption was selected by NIST as the principal method for providing confidentiality after the DES algorithm?
   - **A.** 3DES
   - **B.** Twofish
   - **C.** RC4
   - **D.** AES

3. What cloud service would you be most likely to use if you wanted to share documents with another person?
   - **A.** Software as a Service
   - **B.** Platform as a Service
   - **C.** Storage as a Service
   - **D.** Infrastructure as a Service

4. What is the difference between a traditional firewall and an IPS?
   - **A.** Firewalls don't generate logs.
   - **B.** An IPS cannot drop packets.
   - **C.** An IPS does not follow rules.
   - **D.** An IPS can inspect and drop packets.

5. What is one of the advantages of IPv6 over IPv4 from a security perspective?
   - **A.** IPv4 has a smaller address space.
   - **B.** IPv6 allows for header authentication.
   - **C.** IPv6 is more flexible about extensions.
   - **D.** IPv6 is typically represented in hexadecimal.

6. You are the senior manager in the IT department for your company. What is the most cost-effective way to prevent social engineering attacks?
   - **A.** Install HIDS.
   - **B.** Ensure that all patches are up-to-date.
   - **C.** Monitor and control all email activity.
   - **D.** Implement security awareness training.

7. In which phase within the ethical hacking framework do you alter or delete log information?
   - **A.** Scanning and enumeration
   - **B.** Gaining access
   - **C.** Reconnaissance
   - **D.** Covering tracks

8. An attacker is conducting the following on the target workstation: `nmap -sT 192.33.10.5`. The attacker is in which phase?
   - **A.** Covering tracks
   - **B.** Enumeration
   - **C.** Scanning and enumeration
   - **D.** Gaining access

9. Which encryption algorithm is a symmetric stream cipher?
   - **A.** AES
   - **B.** ECC
   - **C.** RC4
   - **D.** PGP

10. What is the most important part of conducting a penetration test?
   - **A.** Receiving a formal written agreement
   - **B.** Documenting all actions and activities
   - **C.** Remediating serious threats immediately
   - **D.** Maintaining proper handoff with the information assurance team

11. You are a CISO for a giant tech company. You are charged with implementing an encryption cipher for your new mobile devices that will be introduced in 2022. What encryption standard will you most likely choose?
   - **A.** RC4
   - **B.** MD5
   - **C.** AES
   - **D.** Skipjack

12. What does a SYN scan accomplish?
   - **A.** It establishes a full TCP connection.
   - **B.** It establishes only a "half open" connection.
   - **C.** It opens an ACK connection with the target.
   - **D.** It detects all closed ports on the target system.

13. What is the major vulnerability for an ARP request?
   - **A.** It sends out an address request to all the hosts on the LAN.
   - **B.** The address is returned with a username and password in cleartext.
   - **C.** The address request can cause a DoS.
   - **D.** The address request can be spoofed with the attacker's MAC address.

14. You are the CISO for a popular social website. Your engineers are telling you they are seeing multiple authentication failures but with multiple usernames, none of them ever repeated. What type of attack are you seeing?

A. Brute force password attack

B. Authentication failure attack

C. Denial-of-service attack

D. Credential stuffing attack

15. What is the purpose of a man-in-the-middle attack?

A. Gaining access

B. Maintaining access

C. Hijacking a session

D. Covering tracks

16. What method of exploitation might allow the adversary to pass arbitrary SQL queries within the URL?

A. SQL injection

B. XSS

C. Spear phishing

D. Ruby on Rails injection method

17. What is the default TTL value for Microsoft Windows 10 OS?

A. 64

B. 128

C. 255

D. 256

18. Which input value would you utilize in order to evaluate and test for SQL injection vulnerabilities?

A. SQL test

B. admin and password

C. `|| or |!`

D. `1=1'`

19. What is the advantage of using SSH for command-line traffic?

A. SSH encrypts the traffic and credentials.

B. You cannot see what the adversary is doing.

C. Data is sent in the clear.

D. A and B.

20. What year did the Ping of Death first appear?

A. 1992

B. 1989

C. 1990

D. 1996

21. Which type of malware is likely the most impactful?

A. Worm

B. Dropper

C. Ransomware

D. Virus

22. You are part of the help desk team. You receive a ticket from one of your users that their computer is periodically slow. The user also states that from time to time, documents have either disappeared or have been moved from their original location to another. You remote desktop to the user's computer and investigate. Where is the most likely place to see if any new processes have started?

A. The Processes tab in Task Manager

B. `C:\Temp`

C. The Logs tab in Task Manager

D. `C:\Windows\System32\User`

23. Your security team notifies you that they are seeing the same SSID being advertised in your vicinity, but the BSSID is different from ones they are aware of. What type of attack is this?

A. Deauthentication attack

B. Wardriving

C. MAC spoofing

D. Evil twin

24. What does a checksum indicate?

A. That the data has made it to its destination

B. That the three-way TCP/IP handshake finished

C. That there were changes to the data during transit or at rest

D. The size of the data after storage

25. Out of the following, which is one of RSA's registered key strengths?

A. 1,024 bits

B. 256 bits

C. 128 bits

D. 512 bits

26. To provide non-repudiation for email, which algorithm would you choose to implement?

- **A.** AES
- **B.** DSA
- **C.** 3DES
- **D.** Skipjack

27. Which of the following describes a race condition?

- **A.** Where two conditions occur at the same time and there is a chance that arbitrary commands can be executed with a user's elevated permissions, which can then be used by the adversary
- **B.** Where two conditions cancel one another out and arbitrary commands can be used based on the user privilege level
- **C.** Where two conditions are executed under the same user account
- **D.** Where two conditions are executed simultaneously with elevated user privileges

28. Your end clients report that they cannot reach any website on the external network. As the network administrator, you decide to conduct some fact finding. Upon your investigation, you determine that you are able to ping outside of the LAN to external websites using their IP address. Pinging websites with their domain name resolution does not work. What is most likely causing the issue?

- **A.** The firewall is blocking DNS resolution.
- **B.** The DNS server is not functioning correctly.
- **C.** The external websites are not responding.
- **D.** An HTTP GET request is being dropped at the firewall, preventing it from going out.

29. You are the security administration for your local city. You just installed a new IPS. Other than plugging it in and applying some basic IPS rules, no other configuration has been made. You come in the next morning, and you discover that there was so much activity generated by the IPS in the logs that it is too time-consuming to view. What most likely caused the huge influx of logs from the IPS?

- **A.** The clipping level was established.
- **B.** A developer had local admin rights.
- **C.** The LAN experienced a switching loop.
- **D.** The new rules were poorly designed.

30. Which method would be targeting the client in a web-based communication?

- **A.** Cross-site scripting (XSS)
- **B.** SQL injection
- **C.** XML external entity
- **D.** Command injection

31. As a penetration tester, only you and a few key selected individuals from the company will know of the targeted network that will be tested. You also have zero knowledge of your target other than the name and location of the company. What type of assessment is this called?

A. Gray box testing

B. White box testing

C. Black box testing

D. Blue box testing

32. As an attacker, you are searching social media sites as well as job listings. What phase of the attack are you in?

A. Casing the target

B. Gaining access

C. Maintaining access

D. Reconnaissance

33. Which scanning tool is more likely going to yield accurate and useful results during reconnaissance and enumeration?

A. ncat

B. Nmap

C. ping

D. nslookup

34. Why would an attacker conduct an open TCP connection scan using Nmap?

A. The attacker does not want to attack the system.

B. The attacker made a mistake by not selecting a SYN scan function.

C. The attacker is trying to connect to network services.

D. The attacker is trying to make the scan look like normal traffic.

35. Why would an attacker want to avoid tapping into a fiber-optic line?

A. It costs a lot of money to tap into a fiber line.

B. If done wrong, it could cause the entire connection signal to drop, therefore bringing unwanted attention from the targeted organization.

C. The network traffic would slow down significantly.

D. Tapping the line could alert an IPS/IDS.

36. You are an attacker who has successfully infiltrated your target's web server. You performed a web defacement on the targeted organization's website, and you were able to create your own credential with administrative privileges. Before conducting data exfiltration, what is the next move?

A. Log into the new user account that you created.

B. Go back and delete or edit the logs.

C. Ensure that you log out of the session.

D. Ensure that you migrate to a different session and log out.

37. What is a common attack type of the Kerberos protocol that can look like legitimate traffic?

A. Kerberoasting

B. Javaroasting

C. Man-in-the-middle

D. Ticket granting compromise

38. Where is the password file located on a Windows system?

A. `C:\Windows\temp`

B. `C:\Win\system\config`

C. `C:\Windows\accounts\config`

D. `C:\Windows\system32\config`

39. Which response would the adversary receive on closed ports if they conducted an XMAS scan?

A. RST

B. RST/ACK

C. No Response

D. FIN/ACK

40. Why would the adversary encode their payload before sending it to the target victim?

A. Encoding the payload will not provide any additional benefit.

B. By encoding the payload, the adversary actually encrypts the payload.

C. The encoded payload can bypass the firewall because there is no port associated with the payload.

D. Encoding the payload may bypass IPS/IDS detection because it changes the signature.

41. Which password is more secure?

A. keepyourpasswordsecuretoyourself

B. pass123!!

C. P@$$w0rD

D. KeepY0urPasswordSafe!

42. Which of the following best describes DNS poisoning?

A. The adversary intercepts and replaces the victim's MAC address with their own.

B. The adversary replaces their malicious IP address with the victim's IP address for the domain name.

C. The adversary replaces the legitimate domain name with the malicious domain name.

D. The adversary replaces the legitimate IP address that is mapped to the fully qualified domain name with the malicious IP address.

43. Which of the following allows the adversary to forge certificates for authentication?

A. Wireshark

B. Ettercap

C. Cain & Abel

D. Ncat

44. Which encryption standard is used in WEP?

A. AES

B. RC5

C. MD5

D. RC4

45. You are sitting inside of your office, and you notice a strange person in the parking lot with what appears to be a tall antenna connected to a laptop. What is the stranger most likely doing?

A. Brute-forcing their personal electronic device

B. Wardriving

C. Warflying

D. Bluesnarfing

46. If a web application is using a RESTful API, NoSQL databases, and microservices in containers, what style of design is it likely using?

A. Model-view-controller

B. Cloud-native design

C. Traditional architecture

D. NoSQL design

47. Which is the best example of a denial-of-service (DoS) attack?

A. A victim's computer is infected with a virus.

B. A misconfigured switch is in a switching loop.

C. An adversary is forging a certificate.

D. An adversary is consuming all available memory of a target system by opening as many "half-open" connections on a web server as possible.

48. In the Windows SAM file, what security identifier would indicate to the adversary that a given account is an administrator account?

A. 500

B. 1001

C. ADM

D. ADMIN_500

49. Which regional Internet registry is responsible for North and South America?

A. RIPE

B. AMERNIC

C. LACNIC

D. ARIN

50. Which of following actions is the last step in scanning a target?

A. Scan for vulnerabilities

B. Identify live systems

C. Discover open ports

D. Identify the OS and servers

51. Which of the following best describes the ICMP Type 8 code?

A. Device is being filtered

B. Network route is incorrect or missing

C. Echo request

D. Destination unreachable

52. Which of the following port ranges will show you the ports requiring administrative access?

A. 0 to 1023

B. 0 to 255

C. 1024 to 49151

D. 1 to 128

53. What is the length of an IPv6 address?

A. 64 bits

B. 128 bits

C. 256 bits

D. 32 bits

54. Which of the following switches for the Nmap command does nothing but fingerprinting an operating system?

A. `-O`

B. `-sFRU`

C. `-sA`

D. `-sX`

55. What command would the adversary use to show all the systems within the domain using the command-line interface in Windows?

A. `netstat -R /domain`

B. `net view /<domain_name>:domain`

C. `net view /domain:<domain_name>`

D. `netstat /domain:<domain_name>`

56. You are a passenger in an airport terminal. You glance across the terminal and notice a man peering over the shoulder of a young woman as she uses her tablet. What do you think he is doing?

A. Wardriving

B. Shoulder surfing

C. War shouldering

D. Shoulder jacking

57. What type of attack is being used if you were to see `<!ENTITY xxe SYSTEM "file:///etc/passwd">` in your web server logs?

A. SQL injection

B. XSS

C. Command injection

D. XXE

58. Which option describes the concept of injecting code into a portion of data in memory that allows for arbitrary commands to be executed?

A. Buffer overflow

B. Crash

C. Heap spraying

D. Format string

59. Of the following methods, which one acts as a middleman between an external network and the private network by initiating and establishing the connection?

A. Proxy server

B. Firewall

C. Router

D. Switch

60. As an attacker, you successfully exploited your target using a service that should have been disabled. The service had vulnerabilities that you were able to exploit with ease. There appeared to be a large cache of readily accessible information. What may be the issue here?

A. The administrator did not apply the correct patches.

B. The web server was improperly configured.

C. You are dealing with a honeypot.

D. The firewall was not configured correctly.

61. Where is the logfile that is associated with the activities of the last user that signed in within a Linux system?

A. `/var/log/user_log`

B. `/var/log/messages`

C. `/var/log/lastlog`

D. `/var/log/last_user`

62. What default TCP port does SSH utilize?

A. Port 22

B. Port 21

C. Port 443

D. Port 25

63. As a pen tester, you are hired to conduct an assessment on a group of systems for your client. You are provided with a list of critical assets, a list of domain controllers, and a list of virtual share drives. Nothing else was provided. What type of test are you conducting?

A. White hat testing

B. Gray hat testing

C. Gray box testing

D. Red hat testing

64. Which type of firewall would you use if you wanted to have the firewall check for malware as it passed through the firewall?

A. Web application firewall

B. Stateful firewall

C. Next-generation firewall

D. Stateless firewall

65. Which tool can be used to conduct layer 4 scanning and enumeration?

A. Cain & Abel

B. John the Ripper

C. Ping-eater

D. Nmap

66. What port number or numbers is/are associated with the IP protocol?

A. 0 to 65535

B. No ports

C. 53

D. 80

67. Which two protocols are connectionless?

A. IP and TCP

B. IP and FTP

C. IP and UDP

D. TCP and UDP

68. Into which phase of the MITRE ATT&CK framework does transmitting files found in an enterprise network by tunneling through DNS requests fall?

A. Privilege escalation

B. Persistence

C. Exfiltration

D. Defense evasion

69. What is patch management?

A. Deploying patches when they are available

B. Making determinations about patch disposition for business systems

C. Deploying patches at the end of the month

D. Determining what vulnerabilities are currently on your network and deploying patches immediately to eliminate the threat

70. At which layer of the OSI model does FTP reside?

A. Session

B. Application

C. Network

D. Transport

71. What open-source tool could you use to gather information about email addresses from various search providers?

A. Nmap

B. theHarvester

C. Netcat

D. John the Ripper

72. Which switch in Nmap invokes the XMAS scan?

A. `-sX`

B. `-sS`

C. `-xS`

D. `-sT`

73. Which of the following best describes fingerprinting?

A. Scanning for vulnerabilities

B. Using the `-sX` switch for Nmap

C. Matching OS characteristics from a scan to a database in Nmap

D. Checking to see what ports are open by firewalking

74. Which option describes a server-side attack targeting web applications?

A. SQL injection

B. Cross-site malware injection

C. Cross-site scripting

D. SQL site scripting

75. What port is used by DNS?

A. 80

B. 8080

C. 53

D. 25

76. In Linux, what file allows you to see user information such as full name, phone number, and office information?

A. Shadow file

B. Passwd file

C. Userinfo file

D. Useraccount file

77. What tool could you use to check flag settings in a TCP segment?

A. Nmap

B. SuperPing

C. Ettercap

D. Wireshark

78. Which type of packet does a Fraggle attack use to create a DoS attack?

A. TCP

B. IP

C. ICMP

D. UDP

79. Which instruction value is used to invoke a NOP (non-operating procedure)?

A. 0x99

B. 0x91

C. 0xGH

D. 0x90

80. What tool would you use to conduct banner grabbing?

A. aescrypt

B. Ettercap

C. netstat

D. Telnet

81. Which of the following functions is no longer utilized within IPv6?

A. Multicast

B. Anycast

C. Unicast

D. Broadcast

82. What are you creating when you set up a server with certain configurations and document step-by-step instructions?

A. Baseline

B. Procedure

C. Technical advisory

D. Guideline

83. Which application uses two ports?

A. Telnet

B. ICMP

C. HTTPS

D. FTP

84. Which of the following capabilities does the MegaPing tool not support?

A. Vulnerability detection

B. Scanning

C. Vulnerability exploitation

D. DNS name lookup

85. Which of the following is part of the account management lifecycle?

A. Account provisioning

B. Access denied

C. User authentication

D. None of the above

86. Which of the following activities describes the act of a person rummaging through a trash container looking for sensitive information?

A. Trash jumping

B. Dumpster party

C. Trash diving

D. Dumpster diving

87. What are two common ports used to connect to a web server?

A. 80 and 25

B. 80 and 8080

C. 443 and 53

D. 20 and 21

88. When considering the risks of local storage vs. third-party cloud storage, which statement is most accurate?

A. Cloud storage is more secure because the commercial vendor has trained security professionals.

B. When storage is local, you are responsible and accountable for the storage services.

C. You can sue the cloud provider for damages.

D. The cloud has more layers of security than traditional local storage infrastructures.

89. Which packet sniffing tool allows you to specify the individual fields you want printed in the output?

A. Nmap

B. tshark

C. tcpdump

D. Snoop

90. A classification label is associated with which of the following?

A. A subject

B. A file

C. An object

D. A folder

91. Which of the following tools allows you to create certificates that are not officially signed by a CA?

A. Cain & Abel

B. Nmap

C. Ettercap

D. Darkether

92. What type of social engineering attack uses SMS (text) messages to communicate with the victim?

A. Smishing

B. Vishing

C. Phishing

D. Kishing

93. This protocol is used for authentication purposes; it sends cleartext usernames and passwords with no forms of encryption or a means of challenging. What authentication protocol is this?

A. CHAP

B. POP

C. PAP

D. MSCHAP

94. What would you use "something you are" for?

A. Challenge-response authentication

B. Token-based authentication

C. Single-factor authentication

D. Multifactor authentication

95. When two or more authentication methods are used, what is it called?

A. Multitiered authentication factor

B. Multifactor authentication

C. Multicommon factor authentication

D. Multiauthentication factor

96. Which of the following has no key associated with it?

A. MD5

B. AES

C. Skipjack

D. PGP

97. What type of authentication is used in WPA2 to ensure the validity of both the client and the access point?

A. Two-way handshake

B. Three-way handshake

C. Four-way handshake

D. Five-way handshake

98. Which operating system build provides a suite of tools for network offensive (attack your target) purposes?

A. Kali Linux

B. Windows Server 2012 R2

C. FreeBSD

D. Security Onion

99. What is a major drawback of most antivirus software?

A. It can be extremely slow.

B. It must have the latest virus definitions.

C. It can take up a lot of host resources.

D. It requires a lot of effort to administer.

100. What is the value of using the four-way handshake in WPA2?

A. Encrypts traffic

B. Prevents replay attacks

C. Ensures multifactor authentication is in use

D. Performs host checking

101. What is the maximum byte size for a UDP datagram payload?

A. 65,535

B. 65,507

C. 1,500

D. 65,527

102. As an attacker, which of the following resources would be the best place to begin reconnaissance of your target?

A. Nmap using the `-sO` switch

B. Suricata

C. LinkedIn

D. Calling the help desk masquerading as an authorized user

103. When sending a packet with a FIN flag set, what will the target respond with if the port is open?

A. RST is returned.

B. No response is returned.

C. RST/ACK is returned.

D. SYN/ACK is returned.

104. What is the result of conducting a MAC flood on a switch?

A. The switch would fail to respond.

B. It would create a DoS.

C. The switch would operate as if it were a hub.

D. The switch would continue to operate as normal.

105. Which of the following is the correct way to search for a specific IP address in Wireshark using a display filter?

A. `ip.addr = 192.168.1.100`

B. `ip == 192.168.1.100`

C. `ip = 192.168.1.199`

D. `ip.addr == 192.168.1.100`

106. Which of the following denial-of-service attacks would be most likely to be successful today?

A. Fraggle

B. Smurf

C. Slowloris

D. None of the above

107. An email contains a link with the subject line "Congratulations on your cruise!" and is sent to the finance person at a company. The email instructs the reader to click a hyperlink to claim the cruise. When the link is clicked, the reader is presented with a series of questions within an online form, such as name, Social Security number, and date of birth. What type of attack would this be considered?

A. Email phishing

B. Spear phishing

C. Social engineering

D. Identity theft

108. What is a network of zombie computers used to execute a DDoS on a target system called?

A. Botnet

B. Whaling

C. Social engineering

D. DoS

109. Cipher locks, mantraps, and bollards are considered what?

A. Physical controls

B. Technical controls

C. Crime prevention through environmental design

D. Physical barriers

110. Which of the following describes the X.509 standard?

A. It defines the LDAP structure.

B. It is a symmetric encryption algorithm.

C. It uses a sandbox method for security.

D. It describes the standard for creating a digital certificate.

111. Which of the following best describes steganography?

A. A symmetric encryption algorithm

B. Allowing the public to use your private key

C. Hiding information within a picture or concealing it in an audio format

D. Encrypting data using transposition and substitution

112. What process would you use to help ensure only the right people got access to sensitive information?

A. Data classification

B. Data masking

C. Data encryption

D. Data processing

113. What do we call the model used to determine who has to handle patching of systems at a cloud services provider?

A. Shared responsibility

B. Bell-LaPadula

C. Carnegie Mellon Maturity

D. Ford model

114. What is the governing council of the CEH exam?

A. $(ISC)^2$

B. EC-Council

C. CompTIA

D. Microsoft

115. What Transport layer protocol does DHCP operate with?

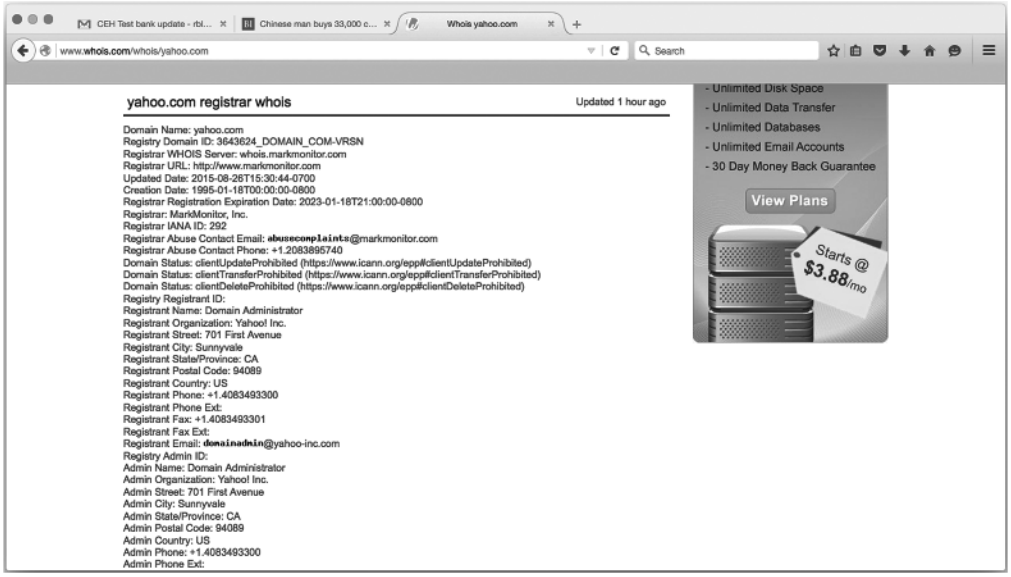
A. IP

B. TCP

C. ICMP

D. UDP

116. According the following screen shot, what is the IANA ID?



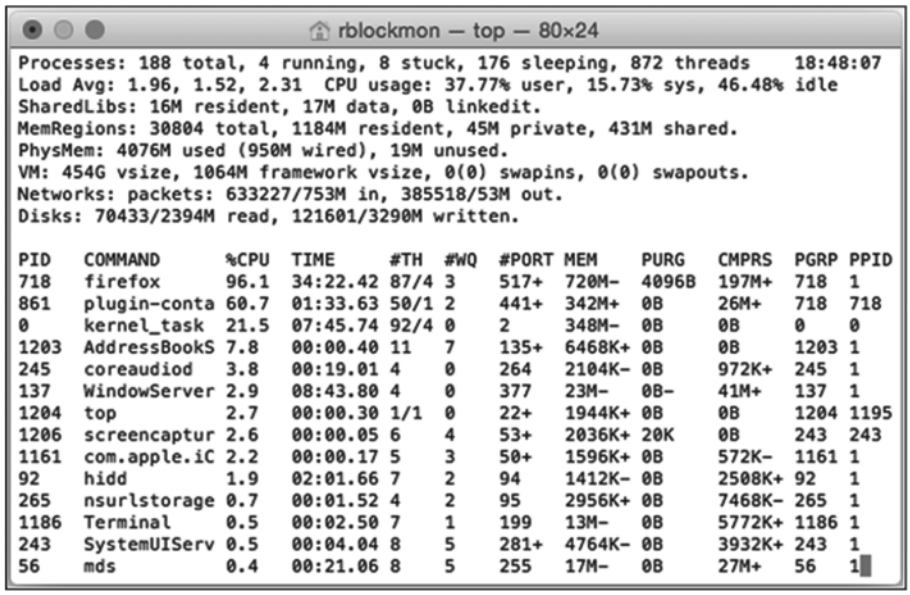
A. 292

B. 94089

C. US

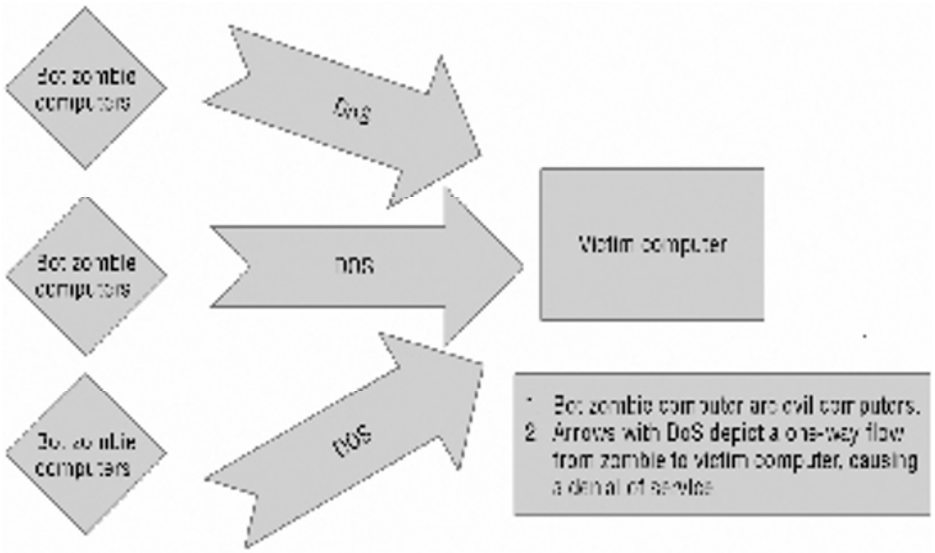
D. 4083493300

117. According to the following screen shot, what process identification is Terminal running?



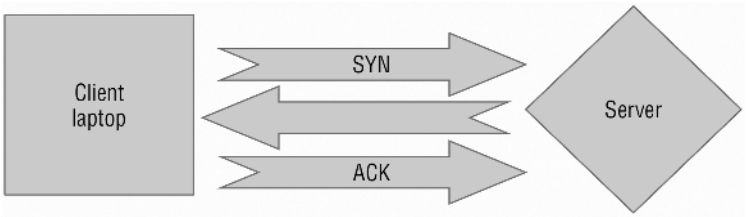
A. 1
B. 708
C. 243
D. 1186

118. As shown in the following image, what type of attack is being conducted?



A. Fraggle
B. DDoS
C. DoS
D. Bot attack

119. What is missing to complete the three-way handshake shown here?



A. ACK/SYN
B. ACK
C. TCP/IP
D. SYN/ACK

120. In the following screen shot, which process is taking 386 MB of memory from the computer?

```
rblockmon — top — 80×24
Processes: 178 total, 2 running, 5 stuck, 171 sleeping, 690 threads    19:56:57
Load Avg: 1.80, 1.71, 2.06  CPU usage: 2.69% user, 2.69% sys, 94.60% idle
SharedLibs: 16M resident, 17M data, 0B linkedit.
MemRegions: 38420 total, 935M resident, 39M private, 394M shared.
PhysMem: 3999M used (979M wired), 94M unused.
VM: 429G vsize, 1064M framework vsize, 0(0) swapins, 256(0) swapouts.
Networks: packets: 825122/933M in, 544300/107M out.
Disks: 88320/2643M read, 161873/4126M written.

PID   COMMAND      %CPU TIME     #TH  #WQ  #PORT MEM    PURG   CMPRS  PGRP PPID
718   firefox      4.0  46:24.62 65   0    506   608M   0B     288M   718  1
0     kernel_task  2.9  10:15.34 92/4 0    2     386M   0B     0B     0    0
861   plugin-conta 5.3  08:23.21 21   0    326   110M+  0B     74M    718  718
875   soffice      0.0  03:40.23 9    1    253   93M    0B     35M    875  1
137   WindowServer 1.9  09:43.67 4    0    377   36M    44K    46M    137  1
244   Finder       0.0  00:07.46 3    0    256   21M    44K    20M    244  1
1186  Terminal     0.6  00:04.84 7    1    210   11M    0B     8004K  1186 1
215   mds_stores   0.0  00:34.61 3    1    54    11M    520K   15M    215  1
759   VTDecoderXPC 0.0  00:41.84 8    0    72    11M    0B     6660K  759  1
268   CalendarAgen 0.0  00:10.77 4    0    172   10M    0B     14M    268  1
56    mds          0.0  00:27.93 3    0    242   7964K  0B     32M    56   1
1     launchd      0.0  00:13.10 5    4    3160  7648K  0B     5700K  1    0
88    loginwindow  0.0  00:05.17 2    0    368   6640K  8192B  10M    88   1
285   Notification 0.0  00:02.23 3    0    198   6612K  0B     7340K  285  1
```

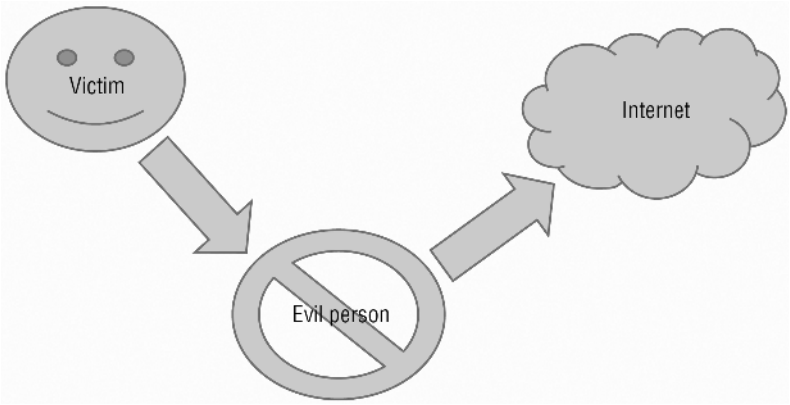
A. Firefox

B. kernel_task

C. Finder

D. WindowServer

121. What type of attack is shown in the following image?



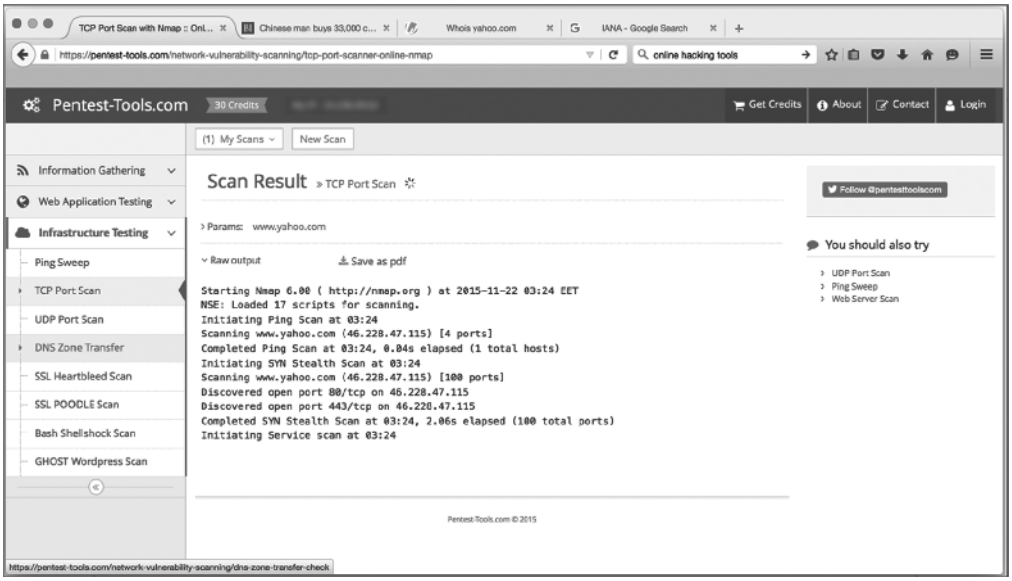
A. Man-in-the-middle

B. DoS

C. DDoS

D. Spear phishing

122. Under which scan has the most ports been scanned?



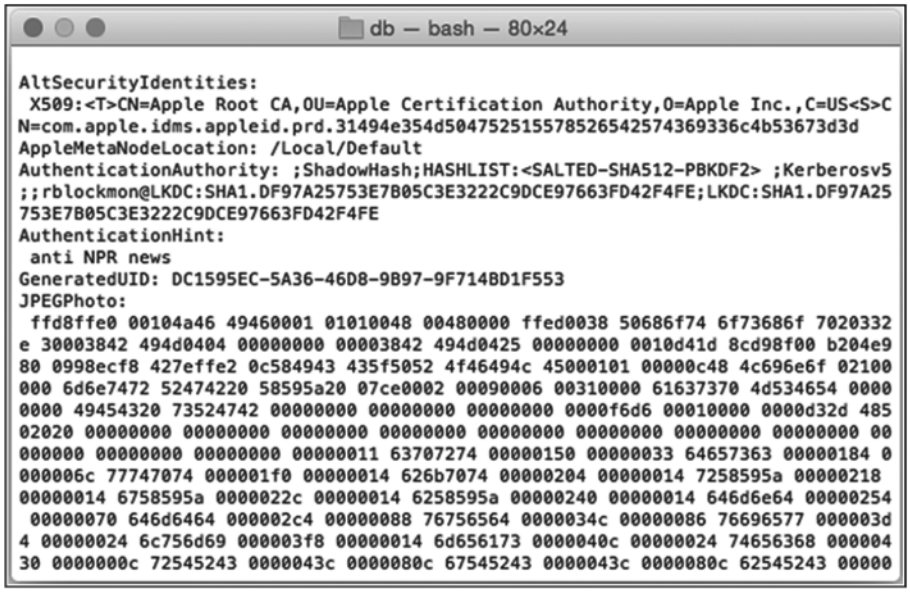
A. Ping

B. SYN stealth

C. SYN

D. DUP

123. As shown in the following screen shot, what type of algorithm was used to hash the user password?



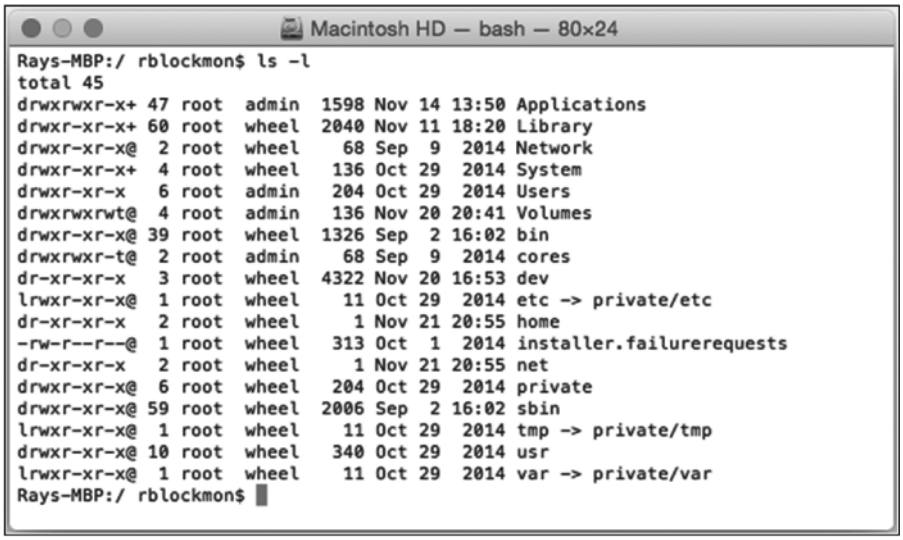
A. SHA-512

B. Kerberos

C. AES

D. SHA-256

124. Which file or application has the permission set with 644?



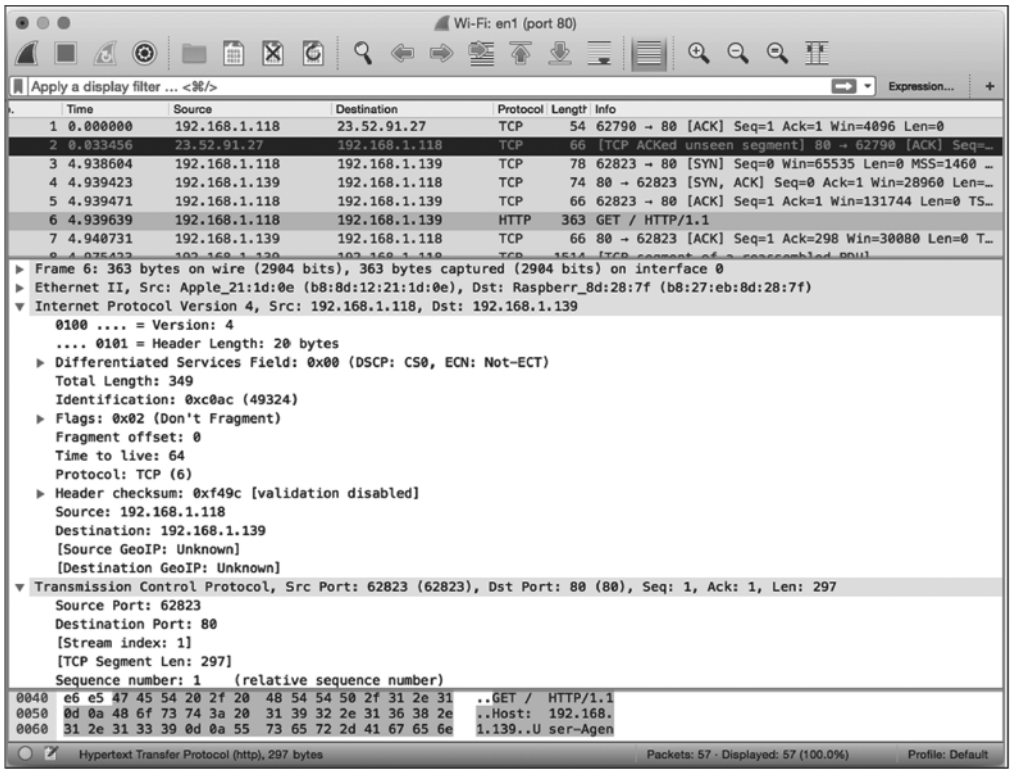
A. usr

B. net

C. Volumes

D. installer.failurerequests

125. From the information given in the Wireshark pcap file, what operating system is the source connecting to a web server?



A. OS X

B. Microsoft

C. Linux

D. Raspbian