

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
 - E. Setting up a rogue hot spot
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 tool is able to conduct a man-in-the-Middle Attack on an 802.3 environment?
 - A. Ettercap
 - B. Cain & Abel
 - C. Wireshark
 - D. Nmap
4. What is the difference between a traditional firewall and an IPS?
 - A. Firewalls do not generate logs.
 - B. IPS cannot drop packets.
 - C. IPS does not follow rules.
 - D. IPS can dissect packets.
5. Why is it important to scan your target network slowly?

- A. To avoid alerting the IDS
- B. It is not necessary to scan the network slowly.
- C. To evade the firewall
- D. Services may not have started, so starting slowly ensures that you capture services that started late.

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 user 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. A hacker 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 aspect when 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 2017. What encryption standard will you most likely choose?

- A. RC4
- B. MD5
- C. ECC
- 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 a 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. You recently learned that your web servers have been compromised with the SSL Heart Bleed zero day exploit. What will be your most likely first course of action to defend against?

- A. Patch all systems.
- B. Establish new cryptographic keys.
- C. Shut down Internet-facing web services.
- D. Restrict access to sensitive information.

15. In what phase is an attacker who is currently conducting a successful man-in-the-middle attack?

- A. Gaining access
- B. Maintaining access
- C. Reconnaissance
- D. Covering tracks

16. What method of exploitation allows the adversary to test for 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 values for Microsoft Windows 7 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'or'1'='1`

19. What is the downside of using SSH with Telnet when it comes to security?

- A. SSH encrypts the traffic and credentials.
- B. You cannot see what the adversary is doing.
- C. Data is sent in the clear.
- D. You do not know what keys you are using.

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

- A. 1992
- B. 1989
- C. 1990
- D. 1996

21. Which of the following viruses was the most infectious?

- A. The Melisa virus
- B. I Love You Virus
- C. Blue Cross virus punter
- D. Stuxnet

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. As a network engineer, you received the task of bridging two corporate facilities by way of wireless communication. These facilities are more than 20 miles apart, contain more than 400 employees at each site, and have a \$20,000 budget. Each site has a single-mode fiber connection. Which antenna would you use to bridge the gap?

- A. Multimode fiber
- B. Very small aperture terminal (VSAT)
- C. Omni direction antenna
- D. Directional antenna

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 nonrepudiation 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. HTTP GET request is being dropped at the firewall 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 a 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. There was a DoS attack on the network.
- C. The LAN experienced a switching loop.
- D. There was no baseline established.

30. Which method would be considered a client-side attack?

- A. Cross-site scripting (XSS)
- B. Man-in-the-middle attack
- C. Watering hole attack
- D. Denial of service (DoS)

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 found your target. You spend the next two weeks observing and watching personnel move in and move out of the facility. You also observe how the front desk handles large packages that are delivered as well as people who do not have access badges. You finally come up with a solid schedule of security patrols that you see being conducted. What is it that you are doing?

- A. Casing the target
- B. Gaining access
- C. Maintaining access
- D. Reconnaissance

33. Which scanning tool is more likely going to yield accurate results for the hacker?

- A. Ncat
- B. Nmap
- C. Ping
- D. Nslookup

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

- A. The attacker does not want to attack the system.
- B. The attacker made a mistake using the `nmap` function.
- C. The attacker is trying to connect to network services.
- D. The attacker is trying to see what ports are open for connection.

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 in to 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 the main drawback to using Kerberos?

- A. Symmetric keys can be compromised if not secured.
- B. Kerberos uses weak cryptography and keys can be easily cracked.
- C. Kerberos uses asymmetric cryptography and can be easily exploited.
- D. The adversary can replay the ticket-granting ticket to gain access to a system or service.

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 can bypass IPS/IDS detection because it changes the signature.

41. Which password is more secure?

- A. !9Apple
- B. pass123!!
- C. P@\$w0rd
- D. keepyourpasswordsecuretoyourself

42. Which of the following best describes DNS poisoning?

- A. The adversary intercepts and replaces the victims 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 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. As a network administrator, you see a familiar IP address pinging the broadcast address. What do you believe is happening?

- A. Smurf attack
- B. DNS poisoning
- C. Man-in-the-middle attack
- D. Trojan virus infecting the gateway

47. Which best describes a denial of service (DoS)?

- 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 attributes 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 options shows the well-known ports?

- A. 0 to 1023
- B. 0 to 255
- C. 1024 to 49151
- D. 1 to 128

53. What is war dialing?

- A. An adversary conducting a DoS on a modem
- B. An adversary dialing to see what modems are open
- C. An adversary using a modem as an evil twin
- D. An adversary verifying closed modems

54. Which of the following switches for the Nmap command fingerprints an operating system?

- A. -sO
- 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 over 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. You are the attacker that has successfully conducted a SQL injection vulnerability assessment on a target site. Which keyword would you use to join the target database with your own malicious database as part of the SQL injection?

- A. UNION
- B. ADD
- C. SELECT
- D. JOIN

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. Memory overflow
- D. Data overflow

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. 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 port does SSH utilize?

- A. Port 22
- B. Port 21
- C. Port 443
- D. Port 25

[63.](#) As a pentester, 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 of the following best describes what is meant by the term *firewalking*?

- A. Decrementing the TTL value by 1 past the firewall will show if a port is opened.
- B. Causing a denial of service on the firewall with a ping flood
- C. Conducting a ping sweep on the firewall
- D. Setting the TTL passed the router to determine what servers and other hosts are available

[65.](#) Which tool can be used to conduct layer 3 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.](#) What is the role of an individual who interrogates a system with permission?

- A. White hat
- B. Gray hat
- C. Black hat
- D. Red hat

[69.](#) What is patch management?

- A. Deploying patches when they are available
- B. Testing patches in a testing environment before they are deployed to the production environment
- 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. Which exploitation was associated with the heart bleed attack?

- A. Buffer overflow
- B. Man in the middle
- C. Fraggle attack
- D. Smurf attack

72. Which switch in Nmap invokes the XMAS scan?

- A. `-sX`
- B. `-sS`
- C. `-xS`
- D. `-sT`

73. Which of the following best describes a fingerprint scan?

- A. Scanning for vulnerabilities
- B. Using the `-sX` switch for Nmap
- C. Matching characteristics from a scan to a database in Nmap
- D. Check to see what ports are open by firewalking

74. Which option describes a client-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. In a packet analyzer, where can you see where the FIN flag is set?

- A. TCP – Header
- B. TCP – Packet
- C. UDP – Flags
- D. TCP – Flags

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 protocol would you use to conduct banner grabbing?

- A. FTP
- B. IRC
- C. DNS
- 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 protocols periodically force the client and server to challenge each other for mutual authentication?

- A. CHAP
- B. POP
- C. PAP
- D. PPE

[85.](#) Which of the following is part of the account management life cycle?

- 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.](#) What would you call an IP address joined with a port number?

- A. TCP/IP
- B. Connection-oriented protocol
- C. TCP/IP socket
- D. Socket

[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.](#) Which RAID configuration is not viable or used anymore?

- A. RAID-1
- B. RAID-3
- C. RAID-5
- D. RAID-2

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. “Something you are” is considered a part of which authentication factor type?

- A. Type 1
- B. Type 3
- C. Type 2
- D. Multifactor authentication

95. When two or more authentication methods are used, it is 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. Which operating system build provides a suite of tools for network defense purposes?

- A. Kali Linux
- B. Windows Server 2012 R2
- C. FreeBSD
- D. Security Onion

[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 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.](#) Which of the following applications would you use to implement an IDS/IPS solution in order to defend your network?

- A. Kali Linux
- B. Windows Vista
- C. Ncat
- D. Suricata

[101.](#) What is the maximum byte size for a UDP packet?

- A. 65,535
- B. 65,507
- C. 1,500
- D. 65,527

[102.](#) As an attacker, which of the following resources would you start with first to form a footprint of your target during the reconnaissance phase?

- A. Nmap using the `-sO` switch
- B. Kali Linux
- C. The help wanted section in the newspaper
- 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?

- 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 is a Type 2 access control method?

- A. Fingerprint
- B. PIN
- C. GPS location
- D. Token access card

107. What type of attack best defines the following situation? An email contains a link with the subject line “Congratulations on your cruise!” 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.

- A. Email phishing
- B. Spear phishing
- C. Social engineering
- D. Identity theft

108. A network of zombie computers used to execute a DDoS on a target system is 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. In which of the following classifications would a honeypot be in most cases?

- A. Enticement
- B. Entrapment
- C. Social engineering
- D. Honey net

113. At what bandwidth does an 802.11a access point operate?

- A. 54 Mbps
- B. 1 Gbps
- C. 5 GHz
- D. 2.4 GHz

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 to the diagram, what is the IANA ID?

yahoo.com registrar whois Updated 1 hour ago

Domain Name: yahoo.com
Registry Domain ID: 3643624_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2015-08-26T15:30:44-0700
Creation Date: 1995-01-18T00:00:00-0800
Registrar Registration Expiration Date: 2023-01-18T21:00:00-0800
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Yahoo! Inc.
Registrant Street: 701 First Avenue
Registrant City: Sunnyvale
Registrant State/Province: CA
Registrant Postal Code: 94089
Registrant Country: US
Registrant Phone: +1.4083493300
Registrant Phone Ext.
Registrant Fax: +1.4083493301
Registrant Fax Ext.
Registrant Email: domainadmin@yahoo-inc.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Yahoo! Inc.
Admin Street: 701 First Avenue
Admin City: Sunnyvale
Admin State/Province: CA
Admin Postal Code: 94089
Admin Country: US
Admin Phone: +1.4083493300
Admin Phone Ext.

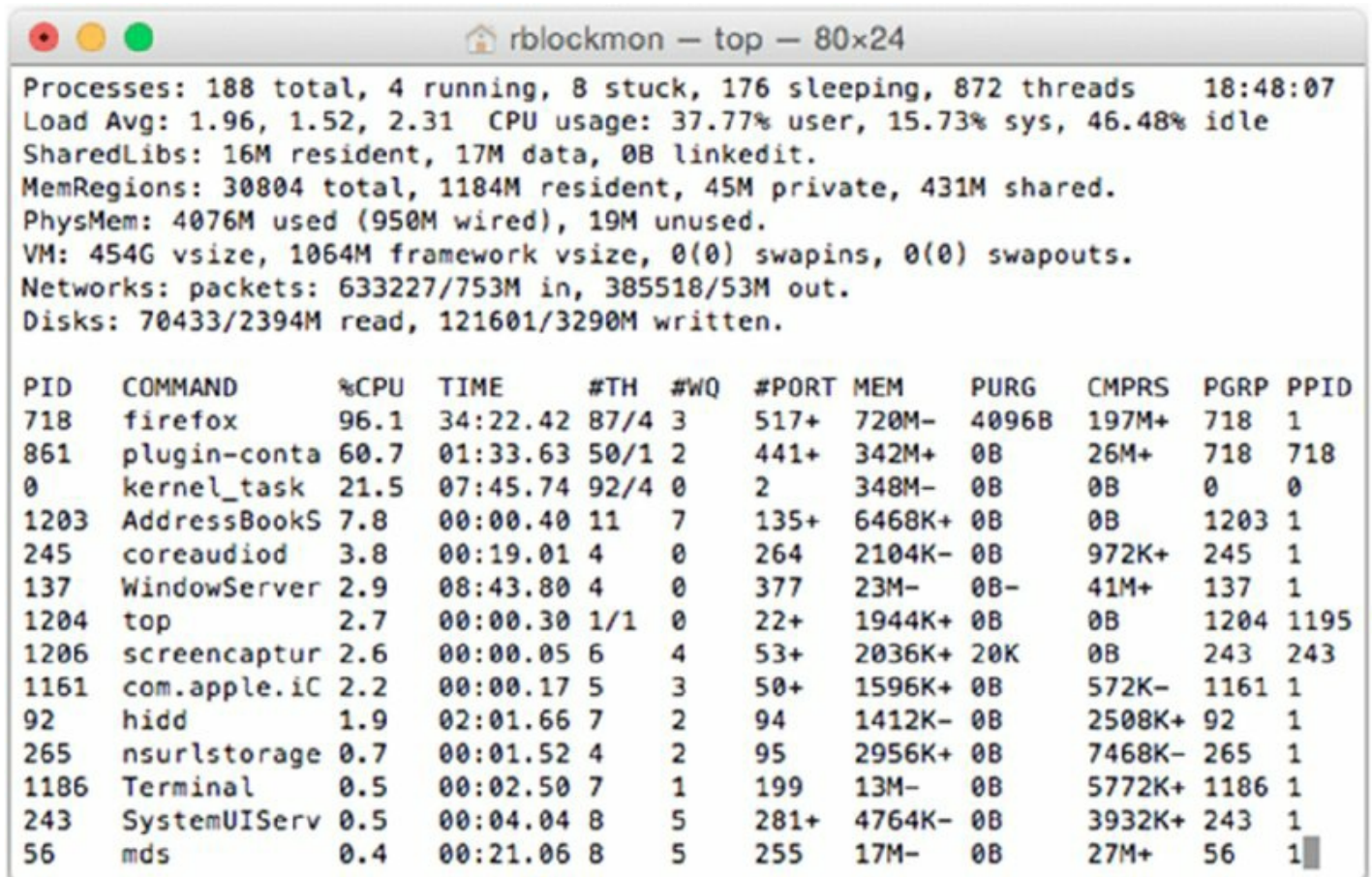
- Unlimited Disk Space
- Unlimited Data Transfer
- Unlimited Databases
- Unlimited Email Accounts
- 30 Day Money Back Guarantee

View Plans

Starts @ \$3.88/mo

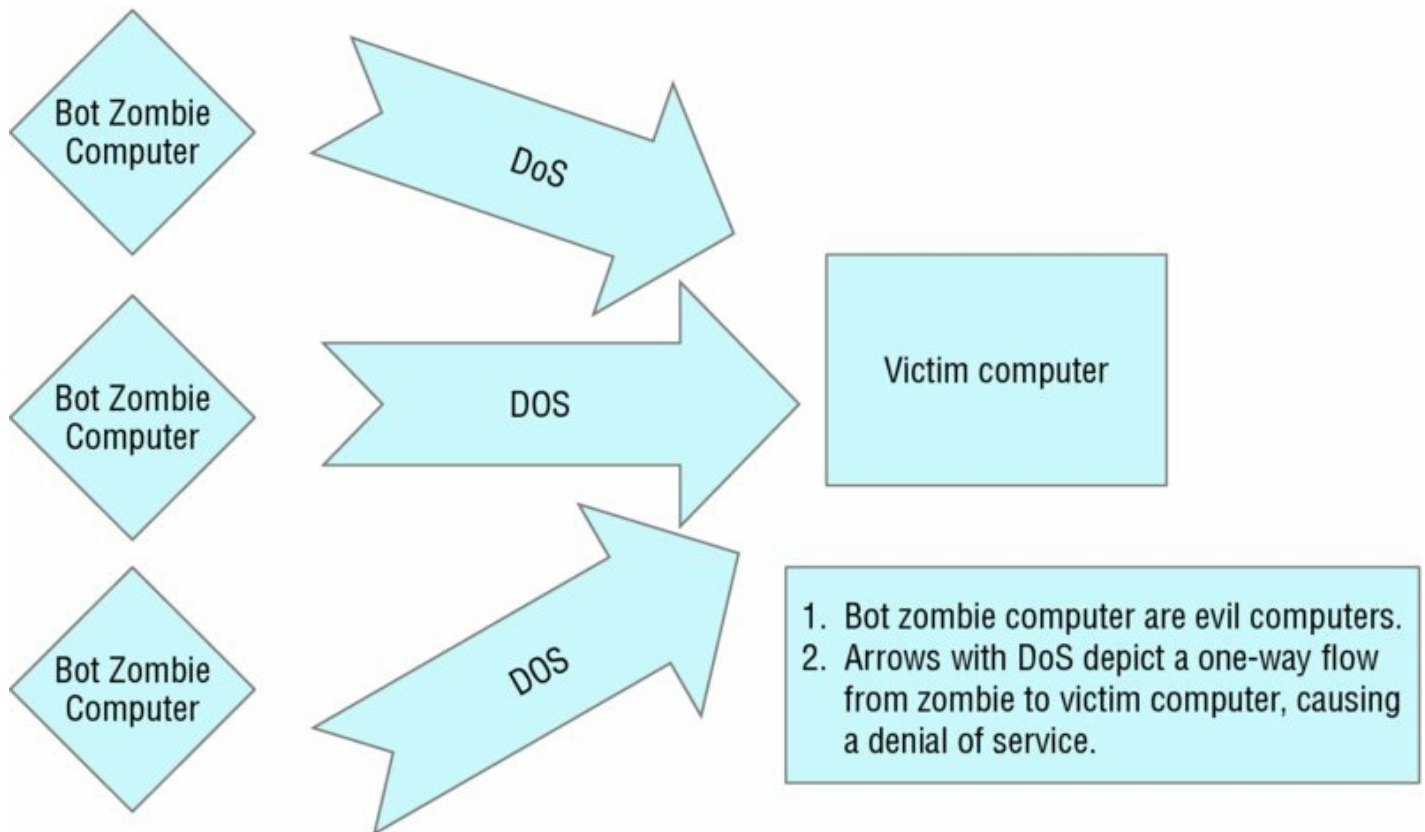
- A. 292
- B. 94089
- C. US
- D. 4083493300

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



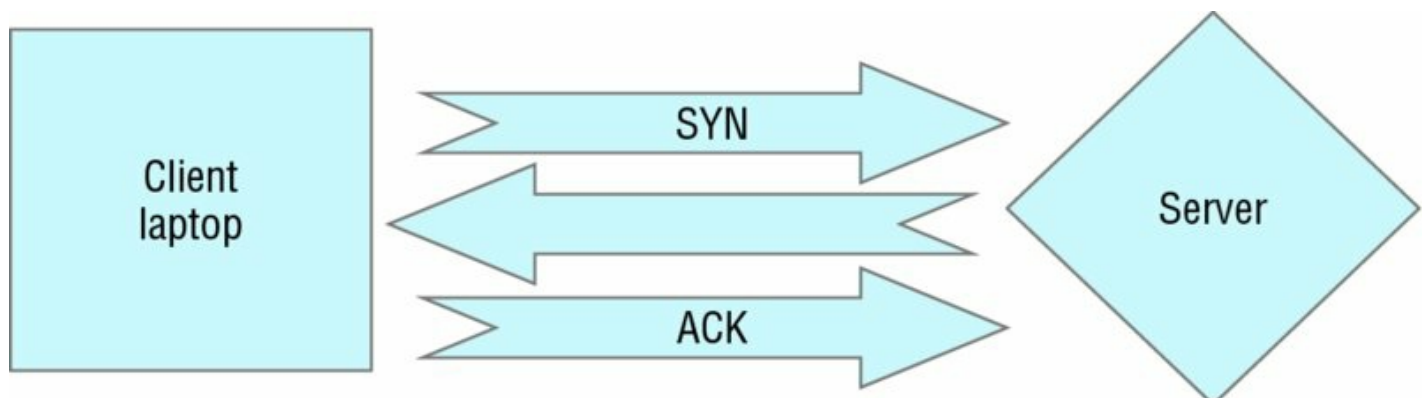
- a. 1
- b. 708
- c. 243
- d. 1186

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



- A. Fragggle
- B. DDoS
- C. DoS
- D. Bot attack

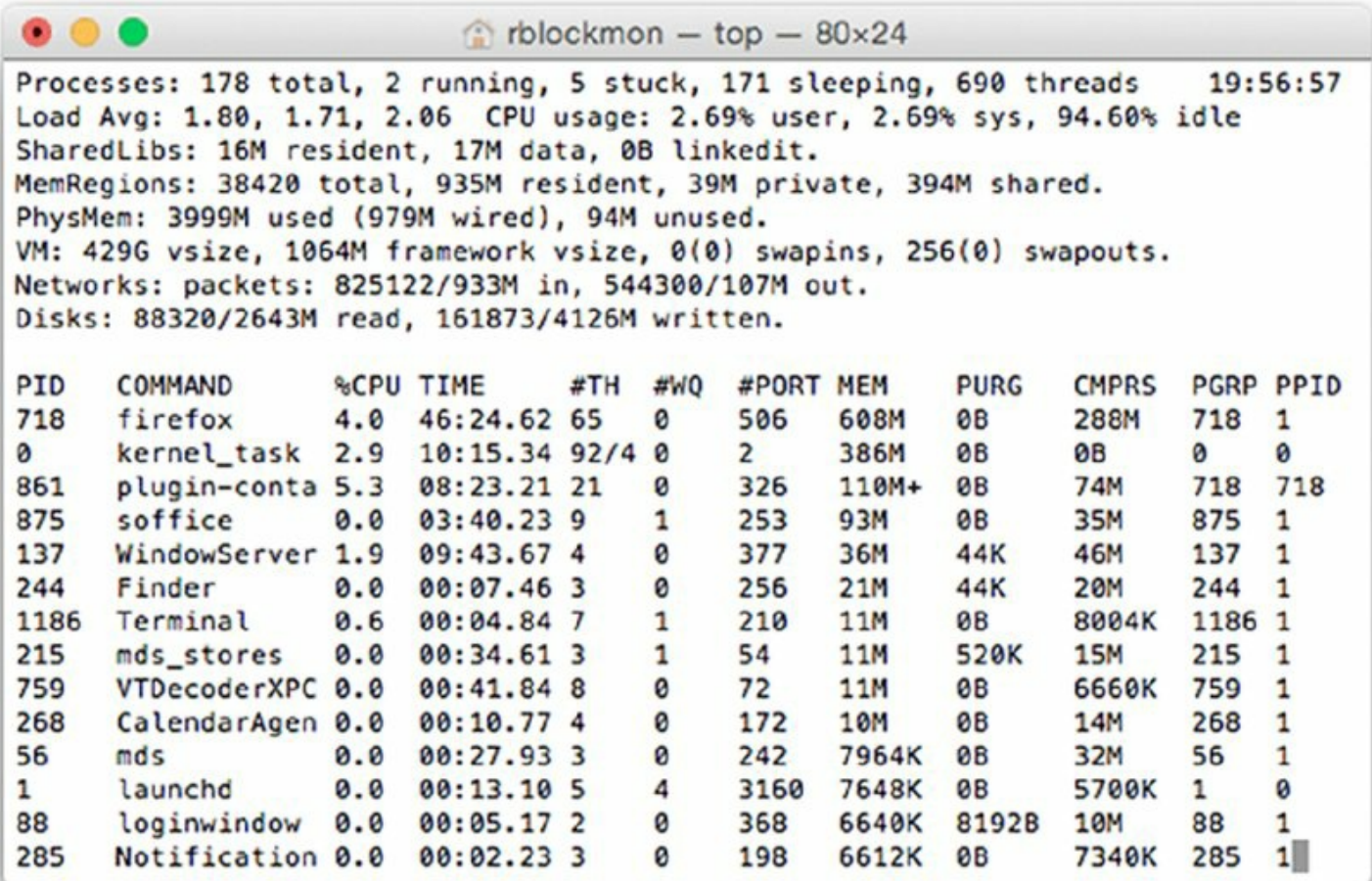
[119.](#) What is missing to complete the three-way handshake shown here?



- 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?

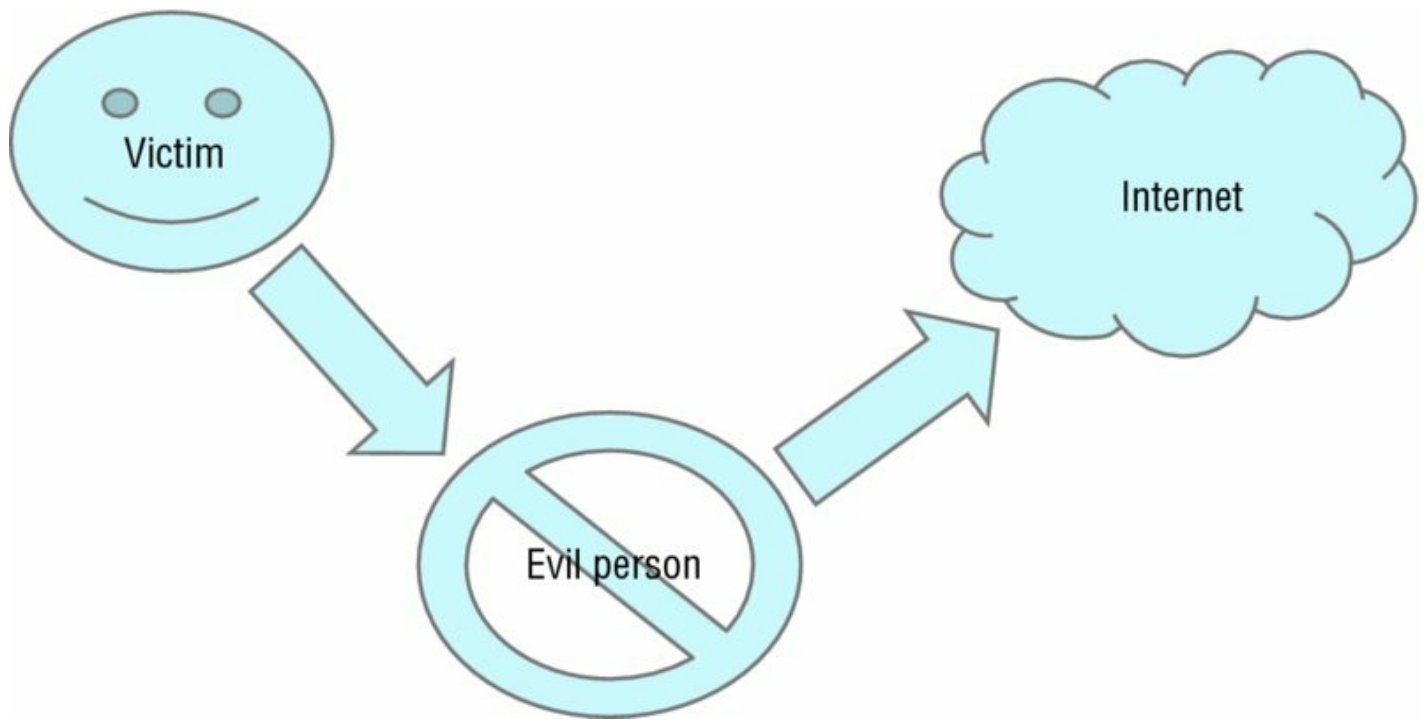


```
Processes: 178 total, 2 running, 5 stuck, 171 sleeping, 690 threads    19:56:57
Load Avg: 1.80, 1.71, 2.06  CPU usage: 2.69% user, 2.69% sys, 94.60% idle
SharedLibs: 16M resident, 17M data, 0B linkedit.
MemRegions: 38420 total, 935M resident, 39M private, 394M shared.
PhysMem: 3999M used (979M wired), 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 had the most ports been scanned?

Scan Result » TCP Port Scan

Params: www.yahoo.com

Raw output: [Save as pdf](#)

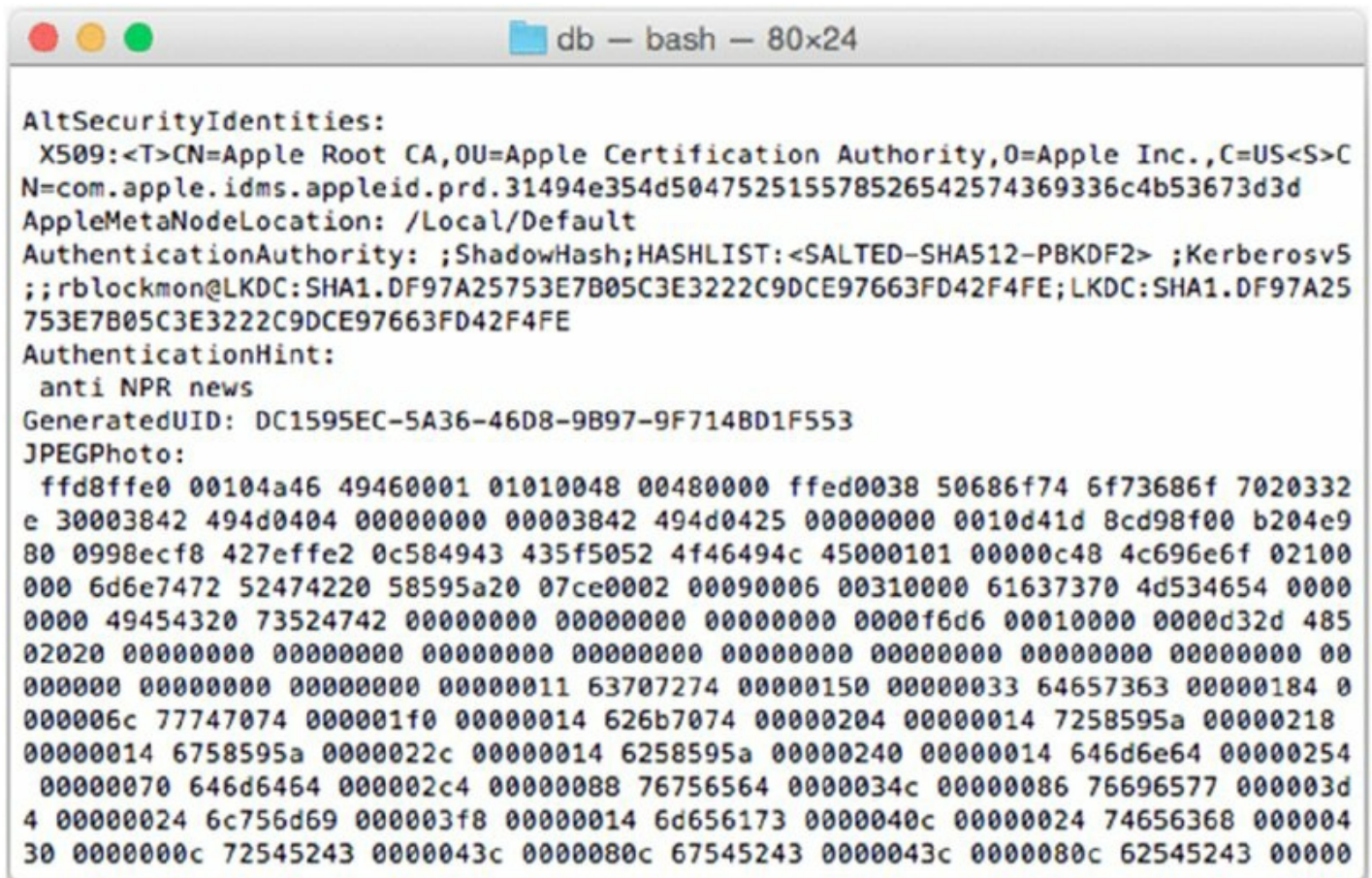
```
Starting Nmap 6.00 ( http://nmap.org ) at 2015-11-22 03:24 EET
NSE: Loaded 17 scripts for scanning.
Initiating Ping Scan at 03:24
Scanning www.yahoo.com (46.228.47.115) [4 ports]
Completed Ping Scan at 03:24, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 03:24
Scanning www.yahoo.com (46.228.47.115) [100 ports]
Discovered open port 80/tcp on 46.228.47.115
Discovered open port 443/tcp on 46.228.47.115
Completed SYN Stealth Scan at 03:24, 2.06s elapsed (100 total ports)
Initiating Service scan at 03:24
```

You should also try

- > UDP Port Scan
- > Ping Sweep
- > Web Server Scan

- 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?



```
db — bash — 80x24

AltSecurityIdentities:
  X509:<T>CN=Apple Root CA,OU=Apple Certification Authority,O=Apple Inc.,C=US<S>C
N=com.apple.idms.appleid.prd.31494e354d504752515578526542574369336c4b53673d3d
AppleMetaNodeLocation: /Local/Default
AuthenticationAuthority: ;ShadowHash;HASHLIST:<SALTED-SHA512-PBKDF2> ;Kerberosv5
;;rblockmon@LKDC:SHA1.DF97A25753E7B05C3E3222C9DCE97663FD42F4FE;LKDC:SHA1.DF97A25
753E7B05C3E3222C9DCE97663FD42F4FE
AuthenticationHint:
  anti NPR news
GeneratedUID: DC1595EC-5A36-46D8-9B97-9F7148D1F553
JPEGPhoto:
  ffd8ffe0 00104a46 49460001 01010048 00480000 ffed0038 50686f74 6f73686f 7020332
e 30003842 494d0404 00000000 00003842 494d0425 00000000 0010d41d 8cd98f00 b204e9
80 0998ecf8 427effe2 0c584943 435f5052 4f46494c 45000101 00000c48 4c696e6f 02100
000 6d6e7472 52474220 58595a20 07ce0002 00090006 00310000 61637370 4d534654 0000
0000 49454320 73524742 00000000 00000000 00000000 0000f6d6 00010000 0000d32d 485
02020 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00
000000 00000000 00000000 00000011 63707274 00000150 00000033 64657363 00000184 0
000006c 77747074 000001f0 00000014 626b7074 00000204 00000014 7258595a 00000218
00000014 6758595a 0000022c 00000014 6258595a 00000240 00000014 646d6e64 00000254
00000070 646d6464 000002c4 00000088 76756564 0000034c 00000086 76696577 000003d
4 00000024 6c756d69 000003f8 00000014 6d656173 0000040c 00000024 74656368 000004
30 0000000c 72545243 0000043c 00000080c 67545243 0000043c 00000080c 62545243 00000
```

- A. SHA-512
- B. Kerberos
- C. AES
- D. SHA-256

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

```
Macintosh HD — bash — 80x24
Rays-MBP:/ rblockmon$ ls -l
total 45
drwxrwxr-x+ 47 root  admin  1598 Nov 14 13:50 Applications
drwxr-xr-x+ 60 root  wheel  2040 Nov 11 18:20 Library
drwxr-xr-x@  2 root  wheel   68 Sep  9 2014 Network
drwxr-xr-x+  4 root  wheel  136 Oct 29 2014 System
drwxr-xr-x   6 root  admin  204 Oct 29 2014 Users
drwxrwxrwt@  4 root  admin  136 Nov 20 20:41 Volumes
drwxr-xr-x@ 39 root  wheel  1326 Sep  2 16:02 bin
drwxrwxr-t@  2 root  admin   68 Sep  9 2014 cores
dr-xr-xr-x   3 root  wheel  4322 Nov 20 16:53 dev
lrwxr-xr-x@  1 root  wheel   11 Oct 29 2014 etc -> private/etc
dr-xr-xr-x   2 root  wheel    1 Nov 21 20:55 home
-rw-r--r--@  1 root  wheel  313 Oct  1 2014 installer.failurerequests
dr-xr-xr-x   2 root  wheel    1 Nov 21 20:55 net
drwxr-xr-x@  6 root  wheel  204 Oct 29 2014 private
drwxr-xr-x@ 59 root  wheel 2006 Sep  2 16:02 sbin
lrwxr-xr-x@  1 root  wheel   11 Oct 29 2014 tmp -> private/tmp
drwxr-xr-x@ 10 root  wheel  340 Oct 29 2014 usr
lrwxr-xr-x@  1 root  wheel   11 Oct 29 2014 var -> private/var
Rays-MBP:/ rblockmon$
```

- 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?

Wi-Fi: en1 (port 80)						
Apply a display filter ... <96/> Expression... +						
	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.118	23.52.91.27	TCP	54	62790 → 80 [ACK] Seq=1 Ack=1 Win=4096 Len=0
2	0.033456	23.52.91.27	192.168.1.118	TCP	66	[TCP ACKed unseen segment] 80 → 62790 [ACK] Seq=...
3	4.938604	192.168.1.118	192.168.1.139	TCP	78	62823 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 ...
4	4.939423	192.168.1.139	192.168.1.118	TCP	74	80 → 62823 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=...
5	4.939471	192.168.1.118	192.168.1.139	TCP	66	62823 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TS...
6	4.939639	192.168.1.118	192.168.1.139	HTTP	363	GET / HTTP/1.1
7	4.940731	192.168.1.139	192.168.1.118	TCP	66	80 → 62823 [ACK] Seq=1 Ack=298 Win=30080 Len=0 T...
8	4.975422	192.168.1.139	192.168.1.118	TCP	1514	[TCP segment of a reconstructed RST]
▶ Frame 6: 363 bytes on wire (2904 bits), 363 bytes captured (2904 bits) on interface 0						
▶ Ethernet II, Src: Apple_21:1d:0e (b8:8d:12:21:1d:0e), Dst: Raspberr_8d:28:7f (b8:27:eb:8d:28:7f)						
▼ Internet Protocol Version 4, Src: 192.168.1.118, Dst: 192.168.1.139						
0100 = Version: 4						
.... 0101 = Header Length: 20 bytes						
▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)						
Total Length: 349						
Identification: 0xc0ac (49324)						
▶ Flags: 0x02 (Don't Fragment)						
Fragment offset: 0						
Time to live: 64						
Protocol: TCP (6)						
▶ Header checksum: 0xf49c [validation disabled]						
Source: 192.168.1.118						
Destination: 192.168.1.139						
[Source GeoIP: Unknown]						
[Destination GeoIP: Unknown]						
▼ Transmission Control Protocol, Src Port: 62823 (62823), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 297						
Source Port: 62823						
Destination Port: 80						
[Stream index: 1]						
[TCP Segment Len: 297]						
Sequence number: 1 (relative sequence number)						
0040	e6 e5 47 45 54 20 2f 20	48 54 54 50 2f 31 2e 31	..GET / HTTP/1.1			
0050	0d 0a 48 6f 73 74 3a 20	31 39 32 2e 31 36 38 2e	..Host: 192.168.			
0060	31 2e 31 33 39 0d 0a 55	73 65 72 2d 41 67 65 6e	1.139..U ser-Agen			
Hypertext Transfer Protocol (http), 297 bytes						
					Packets: 57 - Displayed: 57 (100.0%)	Profile: Default

- A. OS X
- B. Microsoft
- C. Linux
- D. Raspbian