1. Match the attack type with the goal of the attack.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
|                                                                                                | A malicious invitation is disguised as something legitimate |
|                                                                                                | Targets high-profile individuals |
|                                                                                                | Uses SMS text messages |
|                                                                                                | Targets specific victims who visit a compromised site |
|                                                                                                | Uses legitimate services to send users to a compromised site |
|                                                                                                | Uses voice calls |
|                                                                                                | Targets groups of similar users |
|                                                                                                | Exploits human trust and social behavior |

 |

|  |  |
| --- | --- |
| A. | Phishing |
| B. | Whaling |
| C. | Smishing |
| D. | Watering Hole |
| E. | Pharming |
| F. | Vishing |
| G. | Spear Phishing |
| H. | Social Engineering |

 |

1. Which hashing algorithm has been utilized in this figure for the cisco user account?



|  |  |  |
| --- | --- | --- |
|  |  | MD5 |
|  |  | Clear text |
|  |  | Scrypt |
|  |  | SHA-256 |

3) A Cisco Catalyst switch connects to what should be individual user PCs. Each port has the same port security configuration, configured as follows:



Which of the following answers describe the result of the port security configuration created with these commands? (Choose two answers.)

|  |  |  |
| --- | --- | --- |
|  |  | Prevents unknown devices with unknown MAC addresses from sending data through the switch ports. |
|  |  | If a user connects a switch to the cable, prevents multiple devices from sending data through the port. |
|  |  | Will allow any one device to connect to each port and will save that device’s MAC address into the startup-config. |
|  |  | Will allow any one device to connect to each port but will not save that device’s MAC address into the startup-config. |

4) In the following excerpt from a command on a Mac, which of the following parts of the output represent information learned from a DHCP server? (Choose two answers.)



|  |  |  |
| --- | --- | --- |
|  |  | 00:6d:e7:b1:9a:11 |
|  |  | 172.16.4.2 |
|  |  | 0xffffff00 |
|  |  | 172.16.4.255 |

5) Match the feature terms with their correct definitions.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
|                                                    | Gratuitous ARP |
|                                                    | DHCP Snooping |
|                                                    | Dynamic ARP Inspection |
|                                                    | DHCP Server |

 |

|  |  |
| --- | --- |
| A. | Informs all hosts on a subnet about its current MAC address |
| B. | Can be utilized to mitigate rogue DHCP servers |
| C. | Validates ARP information |
| D. | Provides addresses for end devices |

 |

6) DHCP Snooping has already been configured in the network shown in the figure, and you plan to add DAI configuration that relies on the DHCP Snooping Binding Table. Which answer shows the best configuration for switch SW2, specifically for VLAN 20?

                                   

|  |  |  |
| --- | --- | --- |
|  |  | **ip arp inspection vlan 20interface Gi0/12 ip arp inspection trust** |
|  |  | **ip arp inspection vlan 20interface Gi0/2 ip arp inspection trust** |
|  |  | **ip arp inspection vlan 20interface Gi0/24 ip arp inspection trust** |
|  |  | **ip arp inspection vlan 20interface range Gi0/12,Gi0/24 ip arp inspection trust** |

7) Your organization requires all traffic to be encrypted and communications to be secure. From the different protocols listed, which protocol meets these requirements and supports AAA?

|  |  |  |
| --- | --- | --- |
|  |  | TACACS+ |
|  |  | DNS |
|  |  | RADIUS |
|  |  | HTTP |

8) Which options are true about TACACS+? (Select three answers.)

|  |  |  |
| --- | --- | --- |
|  |  | Uses UDP |
|  |  | Uses TCP |
|  |  | Uses port 49 |
|  |  | Encrypts the entire packet |
|  |  | Doesnâ t encrypt the entire packet |
|  |  | Uses ports 1645 and 1812 |

9) Which one of the following is the goal of a brute-force attack?

|  |  |  |
| --- | --- | --- |
|  |  | Try every possible TCP port until a service answers |
|  |  | Try every possible combination of keyboard characters to guess a userâ s password |
|  |  | Initiate a denial-of-service operation on every possible host in a subnet |
|  |  | Spoof every possible IP address in an organization |

10) A network engineer issues a show running-config command and sees only one line of output that mentions the enable secret command, as follows: enable secret 5 $1$ZGMA$e8cmvkz4UjiJhVp7.maLE1.Which of the following is true about users of this router?

|  |  |  |
| --- | --- | --- |
|  |  | A user must type $1$ZGMA$e8cmvkz4UjiJhVp7.maLE1 to reach enable mode. |
|  |  | The router will hash the clear-text password that the user types to compare to the hash |
|  |  | A no service password-encryption configuration command would decrypt this password. |
|  |  | The router will decrypt the password in the configuration to compare to the clear-text password typed by the user. |

11) You would like to limit telnet connection into your router to a range of IP address. You have created the access list numbered 99, how do you apply this ACL to limit telnet connections?

|  |  |  |
| --- | --- | --- |
|  |  | access-class 99 in under the VTY interface |
|  |  | access-group 99 in under the VTY interface |
|  |  | access-group 99 in under the ethernet interface |
|  |  | access-class 99 in under the ethernet interface |

12) Imagine that you have configured the enable secret command, followed by the enable password command, from the console. You log out of the switch and log back in at the console. Which command defines the password that you had to enter to access privileged mode?

|  |  |  |
| --- | --- | --- |
|  |  | enable password |
|  |  | enable secret |
|  |  | Neither |
|  |  | The password command, if itâ s configured |

13) Which security function would be the best option to mitigate a DoS attack?

|  |  |  |
| --- | --- | --- |
|  |  | Stateless firewall |
|  |  | Router ACL |
|  |  | Stateful firewall |
|  |  | Security zone |

14) A next-generation firewall sits at the edge of a companyâ s connection to the Internet. It has been configured to prevent Telnet clients residing in the Internet from accessing Telnet servers inside the company. Which of the following might a next-generation firewall use that a traditional firewall would not?

|  |  |  |
| --- | --- | --- |
|  |  | Match message destination well-known port 23 |
|  |  | Match message application data |
|  |  | Match message IP protocol 23 |
|  |  | Match message source TCP ports greater than 49152 |

15) The status of a LAN switch interface shows err-disabled. Which of the following would have caused this status?

|  |  |  |
| --- | --- | --- |
|  |  | Port security violation |
|  |  | Administratively shut-down port |
|  |  | Incorrect cable attached |
|  |  | No cable attached |
|  |  | Access-port assignment to nonexistent VLAN |

16) If you wanted to see the configured values for IP address, subnet mask, and default gateway on a Windows device, which command would you issue?

|  |  |  |
| --- | --- | --- |
|  |  | ifconfig |
|  |  | netstat -rn |
|  |  | netstat |
|  |  | networksetup -getinfo Ethernet |
|  |  | ipconfig |
|  |  | networksetup -getdnsservers Ethernet |
|  |  |  |

17) Which command would enable a router WAN interface to act as a DHCP client?

|  |  |  |
| --- | --- | --- |
|  |  | ip dhcp client |
|  |  | dhcp enable |
|  |  | ip helper-address |
|  |  | ip address dhcp |

18) Which of the four messages used by DHCP is sent by the client to look for a DHCP server?

|  |  |  |
| --- | --- | --- |
|  |  | Discover |
|  |  | Request |
|  |  | Ask |
|  |  | Option |

19) Which of the four messages used by DHCP is sent by the client to ask for the server to lease the IPv4 address listed from the server?

|  |  |  |
| --- | --- | --- |
|  |  | Offer |
|  |  | Request |
|  |  | Acknowledgement |
|  |  | Respond |

20) Layer 2 switch SW2 connects a Layer 2 switch (SW1), a router (R1), a DHCP server (S1), and three PCs (PC1, PC2, and PC3). All PCs are DHCP clients. Which of the following are the most likely DHCP Snooping trust state configurations on SW2 for the ports connected to the listed devices? (Choose two answers.)

|  |  |  |
| --- | --- | --- |
|  |  | The port connected to the router is untrusted. |
|  |  | The port connected to switch SW1 is trusted. |
|  |  | The port connected to PC1 is untrusted. |
|  |  | The port connected to PC3 is trusted. |

21) An engineer hears about DHCP Snooping and decides to implement it. Which of the following are the devices on which DHCP Snooping could be implemented? (Choose two answers.)

|  |  |  |
| --- | --- | --- |
|  |  | Layer 2 switches |
|  |  | Routers |
|  |  | Multilayer switches |
|  |  | End-user hosts |

22) On a multilayer switch, a switch needs to be configured to perform DHCP Snooping on some Layer 2 ports in VLAN 3. Which command may or may not be needed depending on whether the switch also acts as a DHCP relay agent?

|  |  |  |
| --- | --- | --- |
|  |  | no ip dhcp snooping information option |
|  |  | ip dhcp snooping limit rate 5 |
|  |  | errdisable recovery cause dhcp-rate-limit |
|  |  | ip dhcp snooping vlan 3 |

23) What are the different DHCP Snooping port states? (Select two answers.)

|  |  |  |
| --- | --- | --- |
|  |  | Untrusted |
|  |  | Trusted |
|  |  | Outside |
|  |  | Inside |
|  |  | LAN |
|  |  | WAN |

24) A Layer 2 switch needs to be configured to use Dynamic ARP Inspection along with DHCP Snooping. Which command would make DAI monitor ARP message rates on an interface at an average rate of 4 received ARP messages per second? (Choose two answers.)

|  |  |  |
| --- | --- | --- |
|  |  | ip arp inspection limit rate 4 burst interval 2 |
|  |  | ip arp inspection limit rate 10 burst interval 2 |
|  |  | ip arp inspection limit rate 16 burst interval 4 |
|  |  | ip arp inspection limit rate 4 |

25) Youâ ve implemented DAI on a Layer 2 switch in your network, and now you want to monitor the ARP message rates with an average of two received ARP messages a second. Which command(s) would need to be utilized to accomplish this? (Select three answers.)

26) Some IOS commands store passwords as clear text, but you can then encrypt the passwords with the service password-encryption global command. By comparison, other commands store a computed hash of the password instead of storing the password. Comparing the two options, which one answer is the most accurate about why one method is better than the other?

|  |  |  |
| --- | --- | --- |
|  |  | Using hashes is preferred because encrypted IOS passwords can be easily decrypted. |
|  |  | Using hashes is preferred because of the large CPU effort required for encryption. |
|  |  | Using encryption is preferred because it provides stronger password protection. |
|  |  | Using encryption is preferred because of the large CPU effort required for hashes. |

27) Refer to the diagram below. What method of authentication is being used?

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |
| --- | --- | --- |
|   |  | Open Authentication |
|  |  | CCMP |
|  |  | WEP |
|  |  | 802.1x |

 |  |

28) Which of the following statements are true about 802.11 wireless communication on a single frequency? Assume all devices are within range of each other. (Select two answers)

|  |  |  |
| --- | --- | --- |
|  |  | Two or more devices can transmit data to each other at the same time. |
|  |  | Two or more devices can receive data at the same time. |
|  |  | Only one device should transmit data at a given time. |
|  |  | Only an access point can transmit data on the frequency |

29) In a split-MAC wireless architecture, a CAPWAP tunnel terminates on which of the following? (Select two answers)

|  |  |  |
| --- | --- | --- |
|  |  | An autonomous AP |
|  |  | A lightweight AP |
|  |  | A wireless LAN controller |
|  |  | A wireless userâ s device |

30) Suppose several APs are deployed in a cloud-based architecture. Which of the following are correct statements about the control and data planes involved in the wireless network? (Select two answers)

|  |  |  |
| --- | --- | --- |
|  |  | The data plane extends from the wireless users to the Internet cloud, where the APs are managed. |
|  |  | The control plane extends from the APs to the Internet cloud, where the APs are managed. |
|  |  | The data plane extends from the wireless users to the cloud-based AP. |
|  |  | The control plane extends from the wireless users to the cloud-based AP. |

31) If a lightweight AP provides at least one BSS for wireless clients, which one of the folï¿¾lowing modes does it use?

|  |  |  |
| --- | --- | --- |
|  |  | Local |
|  |  | Normal |
|  |  | Monitor |
|  |  | Client |

32) Which one of the following is a wireless encryption method that has been found to be vulnerable and is not recommended for use?

|  |  |  |
| --- | --- | --- |
|  |  | AES |
|  |  | WPA |
|  |  | EAP |
|  |  | WEP |

33) A pre-shared key is used in which of the following wireless security configurations? (Choose two answers.)

|  |  |  |
| --- | --- | --- |
|  |  | WPA2 personal mode |
|  |  | WPA2 enterprise mode |
|  |  | WPA3 personal mode |
|  |  | WPA3 enterprise mode |

34) Which of the following statements correctly describe WLC interfaces and ports? (Select two answers)

|  |  |  |
| --- | --- | --- |
|  |  | Ports are physical connections to a wired network. |
|  |  | Ports are logical connections within a WLC. |
|  |  | Interfaces are physical connections to a wired network. |
|  |  | Interfaces are logical connections within a WLC. |
|  |  | Ports and interfaces are interchangeable terms. |

35) By default, a wireless LAN controller will not allow \_\_\_\_\_\_\_\_\_\_\_\_ traffic initiated from a WLAN?

|  |  |  |
| --- | --- | --- |
|  |  | IP |
|  |  | VLAN |
|  |  | management |
|  |  | encrypted |

36) Based on the command out below, which two solicited-node multicast addresses will the router create? (Select two answers.)

R1# show ipv6 interface GigabitEthernet 0/3

GigabitEthernet0/3 is up, line protocol is up

IPv6 is enabled, link-local address is FE80::AB:ABAB

No Virtual link-local address(es):

Global unicast address(es):

2001:DB8:2211:1::1, subnet is 2001:DB8:2211:1::/64

Joined group address(es):

FF02::1

FF02::2

FF02::5

|  |  |  |
| --- | --- | --- |
|  |  | FF02::1:FF00:1 |
|  |  | FF02::1:FFAB:ABAB |
|  |  | FF01::1:FFAB:ABAB |
|  |  | FF03::1:FF00:1 |

37) Based on the following configuration, what would be the assigned global unicast address?

interface fastEthernet0/0

mac-address 0200.8395.2614

ipv6 address 2500:A4B3.ED81:ACEB::/64 eui-64

|  |  |  |
| --- | --- | --- |
|  |  | 2500:A4B3:ED81:ACEB:0:83FF:FE95:2614 |
|  |  | 2500:A4B3:ED81:ACEB:0:83FF:FF95:2614 |
|  |  | 2500:A4B3:ED81:ACEB:200:83FF:FE95:2614 |
|  |  | 2500:A4B3:ED81:ACEB:200:83FF:FF95:2614  |

38) Which of the following is the unabbreviated version of IPv6 address 2001:DB8::200:28?

|  |  |  |
| --- | --- | --- |
|  |  | 2001:0DB8:0000:0000:0000:0000:0200:0028 |
|  |  | 2001:0DB8::0200:0028 |
|  |  | 2001:0DB8:0:0:0:0:0200:0028 |
|  |  | 2001:0DB8:0000:0000:0000:0000:200:0028 |

39) When subnetting an IPv6 address block, an engineer shows a drawing that breaks the address structure into three pieces. Assuming that all subnets use the same prefix length, which of the following answers lists the name of the field on the far right side of the address?

|  |  |  |
| --- | --- | --- |
|  |  | Subnet |
|  |  | Interface ID |
|  |  | Network |
|  |  | Global routing prefix |
|  |  | Subnet router anycast |

40) Router R1 currently supports IPv4, routing packets in and out all its interfaces. R1â s configuration needs to be migrated to support dual-stack operation, routing both IPv4 and IPv6. Which of the following tasks must be performed before the router can also support routing IPv6 packets? (Choose two answers.)

|  |  |  |
| --- | --- | --- |
|  |  | Enable IPv6 on each interface using an ipv6 address interface subcommand. |
|  |  | Enable support for both versions with the ip versions 4 6 global command. |
|  |  | Additionally enable IPv6 routing using the ipv6 unicast-routing global command. |
|  |  | Migrate to dual-stack routing using the ip routing dual-stack global command. |

41) A router has been configured with the ipv6 address 3111:1:1:1::1/64 command on its G0/1 interface and ipv6 address 3222:2:2:2::1/64 on its G0/2 interface. Both interfaces are working. Which of the following routes would you expect to see in the output of the show ipv6 route connected command? (Choose two answers.)

|  |  |  |
| --- | --- | --- |
|  |  | A route for 3111:1:1:1::/64 |
|  |  | A route for 3111:1:1:1::1/64 |
|  |  | A route for 3222:2:2:2::/64 |
|  |  | A route for 3222:2:2:2::2/128 |

42) Examine the output of the "show ipv6 interface brief" command shown below.  What two address types are shown?

R1# show ipv6 interface brief

FastEthernet0/0           [administratively down/down]

unassigned

GigabitEthernet1/0       [administratively down/down]

FE80::C800:1FF:FE7E:1C

FD00:1:1:2:C800:1FF:FE7E:1C

|  |  |  |
| --- | --- | --- |
|  |  | Multicast |
|  |  | Anycast |
|  |  | Link-local |
|  |  | unique local |

43)What would happen to an IP Phone that was connected to a PoE port on a switch that had its autonegotiation features turned off?

|  |  |  |
| --- | --- | --- |
|  |  | Normal operations; the IP Phone would power on and function |
|  |  | The IP Phone wouldnâ t power on at all |
|  |  | The IP Phone could receive too much power current |
|  |  | Flapping of the switchport |

44) Each answer lists two Metro Ethernet terms. Which answer(s) lists two terms that both refer to the same Metro Ethernet service? (Select three answers.)

|  |  |  |
| --- | --- | --- |
|  |  | E-Line, point-to-point |
|  |  | E-Line, point-to-multipoint |
|  |  | E-Tree, full mesh |
|  |  | E-LAN, hub-and-spoke |
|  |  | E-Tree, hub-and-spoke |
|  |  | E-LAN, full mesh |

45) Eight virtual machines run on one physical server; the server has two physical Ethernet NICs. Which answers describe a method that allows all eight VMs to communicate?

|  |  |  |
| --- | --- | --- |
|  |  | The VMs must share two IP addresses and coordinate to avoid using duplicate TCP or UDP ports. |
|  |  | The hypervisor acts as an IP router using the NICs as routed IP interfaces. |
|  |  | Each VM uses a virtual NIC that is mapped to a physical NIC. |
|  |  | Each VM uses a virtual NIC that logically connects to a virtual switch. |

46) Of the different public cloud WAN options, which have quality of service capabilities to ensure end-to-end application requirements? (Select three answers.)

|  |  |  |
| --- | --- | --- |
|  |  | Internet |
|  |  | Intercloud exchange |
|  |  | Ethernet WAN |
|  |  | MPLS VPN |
|  |  | Internet VPN |