

CCNA SECFND (210-250) Dumps – Certification Practice Exam Answers

 itexamanswers.net/ccna-secfnd-210-250-certification-practice-exam-answers.html

July 18, 2019

How to find: Press “**Ctrl + F**” in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. Refer to the exhibit. Approximately what percentage of the physical memory is still available on this Windows system?

- 32%
- 53%
- **68%**
- 90%

Explanation: The graphic shows that there is 5.1 GB (187 MB) of memory in use with 10.6 GB still available. Together this adds up to 16 GB of total physical memory. 5 GB is approximately 32% of 16 GB leaving 68% still available.

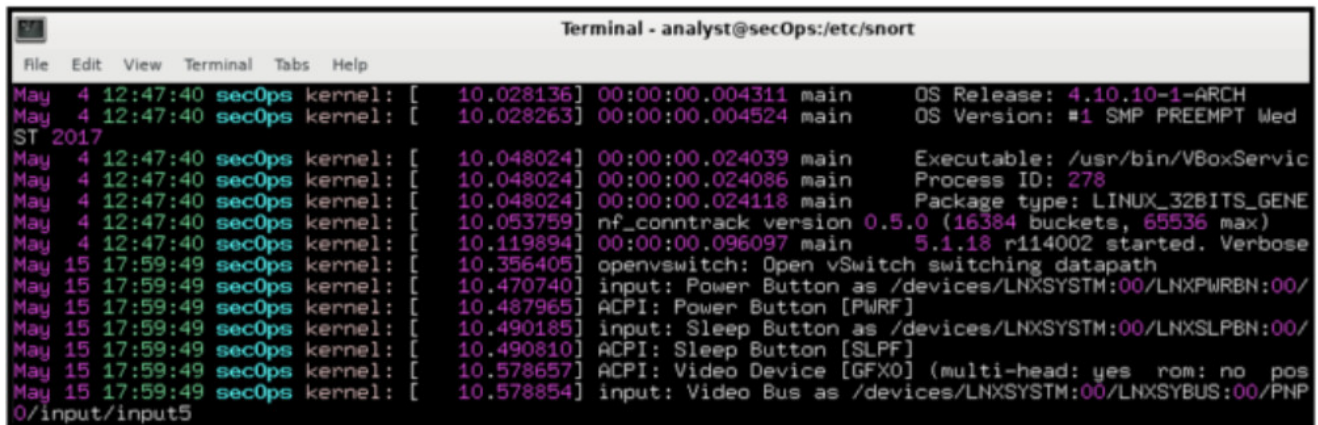
2. Which Windows tool can be used by a cybersecurity administrator to secure stand-alone computers that are not part of an active directory domain?

- **Local Security Policy**
- Windows Defender
- Windows Firewall
- PowerShell



Explanation: Windows systems that are not part of an Active Directory Domain can use the Windows Local Security Policy to enforce security settings on each stand-alone system.

3. Refer to the exhibit. Which technology would contain information similar to the data shown for infrastructure devices within a company?

A terminal window titled "Terminal - analyst@secOps:/etc/snort" displays a series of log messages. The messages are timestamped and include details about system events, such as OS releases, process IDs, and hardware information. The logs are formatted with color-coded fields: timestamps in green, source identifiers in blue, and event details in white. The messages include information about the OS release (4.10.10-1-ARCH), process ID (278), package type (LINUX_32BITS_GENE), and various hardware components like the power button, sleep button, and video device.

```
May 4 12:47:40 sec0ps kernel: [ 10.028136] 00:00:00.004311 main OS Release: 4.10.10-1-ARCH
May 4 12:47:40 sec0ps kernel: [ 10.028263] 00:00:00.004524 main OS Version: #1 SMP PREEMPT Wed
ST 2017
May 4 12:47:40 sec0ps kernel: [ 10.048024] 00:00:00.024039 main Executable: /usr/bin/VBoxService
May 4 12:47:40 sec0ps kernel: [ 10.048024] 00:00:00.024086 main Process ID: 278
May 4 12:47:40 sec0ps kernel: [ 10.048024] 00:00:00.024118 main Package type: LINUX_32BITS_GENE
May 4 12:47:40 sec0ps kernel: [ 10.053759] nf_conntrack version 0.5.0 (16384 buckets, 65536 max)
May 4 12:47:40 sec0ps kernel: [ 10.119894] 00:00:00.096097 main 5.1.18 r114002 started. Verbose
May 15 17:59:49 sec0ps kernel: [ 10.356405] openvswitch: Open vSwitch switching datapath
May 15 17:59:49 sec0ps kernel: [ 10.470740] input: Power Button as /devices/LNXSYSTM:00/LNXPWRBN:00/
May 15 17:59:49 sec0ps kernel: [ 10.487965] ACPI: Power Button [PMRF]
May 15 17:59:49 sec0ps kernel: [ 10.490185] input: Sleep Button as /devices/LNXSYSTM:00/LNXPSPBN:00/
May 15 17:59:49 sec0ps kernel: [ 10.490810] ACPI: Sleep Button [SLPF]
May 15 17:59:49 sec0ps kernel: [ 10.578657] ACPI: Video Device [GFX0] (multi-head: yes rom: no pos
May 15 17:59:49 sec0ps kernel: [ 10.578854] input: Video Bus as /devices/LNXSYSTM:00/LNXPBUS:00/PNP
0/input/input5
```

- Apache server
- firewall
- HIDS
- **syslog server**

Explanation: A syslog server consolidates and maintains messages from infrastructure devices that have been configured to send logging information. Data from the syslog server can be analyzed to detect anomalies.

4. What are three benefits of using symbolic links over hard links in Linux? (Choose three.)

- Symbolic links can be exported.
- They can be encrypted.
- They can be compressed.
- **They can link to a directory.**
- **They can show the location of the original file.**
- **They can link to a file in a different file system.**

Explanation: In Linux, a hard link is another file that points to the same location as the original file. A soft link (also called a symbolic link or a symlink) is a link to another file system name. Hard links are limited to the file system in which they are created and they cannot link to a directory; soft links are not limited to the same file system and they can link to a directory. To see the location of the original file for a symbolic link use the `ls -l` command.

5. Which two protocols are associated with the transport layer? (Choose two.)

- TCP
- IP
- UDP
- PPP
- ICMP

Explanation: TCP and UDP reside at the transport layer in both the OSI and TCP/IP models.

6. Refer to the exhibit. A user reports that resources can no longer be reached on the local 192.168.1.0/24 network nor on the internet. A cybersecurity analyst investigates the issue by reviewing the routing table of the PC in question. What is the reason for the problem reported by the user?

```
IPv4 Route Table
=====
Active Routes:
Network Destination          Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.1.1      192.168.2.2      281
127.0.0.0                  255.0.0.0          On-link          127.0.0.1        331
127.0.0.1  255.255.255.255      On-link          127.0.0.1        331
127.255.255.255  255.255.255.255    On-link          127.0.0.1        331
192.168.2.0    255.255.255.0      On-link          192.168.2.2      281
192.168.2.2    255.255.255.255    On-link          192.168.2.2      281
192.168.2.255  255.255.255.255    On-link          192.168.2.2      281
224.0.0.0      240.0.0.0          On-link          127.0.0.1        331
224.0.0.0      240.0.0.0          On-link          192.168.2.2      281
255.255.255.255  255.255.255.255    On-link          127.0.0.1        331
255.255.255.255  255.255.255.255    On-link          192.168.2.2      281
=====
Persistent Routes:
Network Address          Netmask  Gateway Address  Metric
0.0.0.0                0.0.0.0    192.168.1.1      Default
=====
```

- incorrect host IP address
- incorrect subnet mask
- incorrect default gateway
- incorrect route metric

Explanation: In the routing table of the PC, the default gateway is 192.168.1.1 and the host IP address is 192.168.2.2. These addresses are on different networks. The host should have an IP address on the 192.168.1.0/24 network. To correct this problem the host IP must be changed to an address on the 192.168.1.0/24 local network.

7. What is the function of ARP?

- resolves domain names to IP addresses

- provides automatic IP address assignments to hosts
- sends error and operational information messages to hosts
- **maps IPv4 addresses to MAC addresses**

Explanation: ARP, or Address Resolution Protocol, is used by hosts to resolve a destination MAC address from a given destination IP address.

8. A cybersecurity analyst believes an attacker is spoofing the MAC address of the default gateway to perform a man-in-the-middle attack. Which command should the analyst use to view the MAC address a host is using to reach the default gateway?

- ipconfig /all
- route print
- netstat -r
- **arp -a**

Explanation: ARP is a protocol used with IPv4 to map a MAC address to an associated specific IP address. The command arp -a will display the MAC address table on a Windows PC.

9. Which network service is used by clients to resolve the IP address of a domain name?

- DHCP
- **DNS**
- ARP
- ICMP

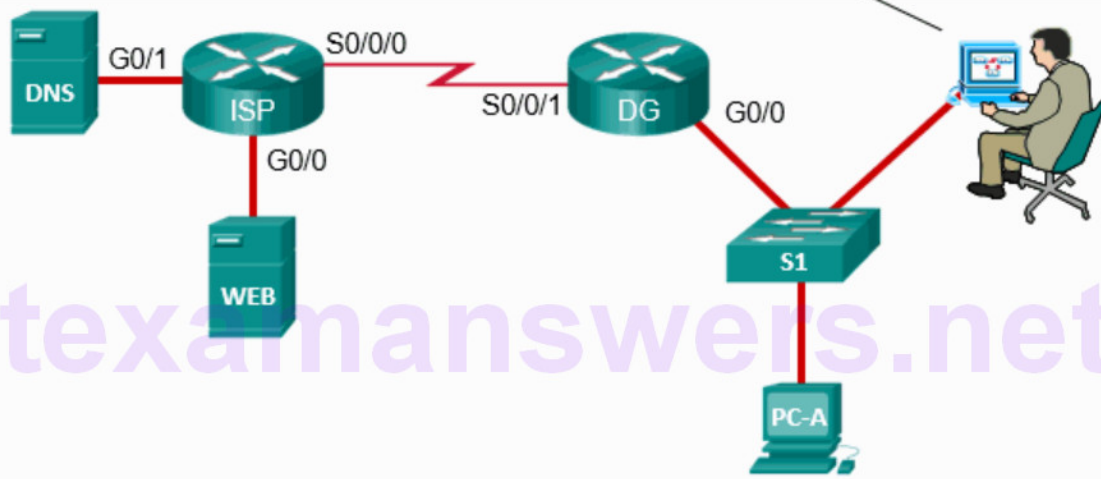
Explanation: The Domain Name System (DNS) is used by clients to resolve the IP address of a domain name. For example, a host may need to connect to www.cisco.com. The host would contact a DNS server to discover the IP address associated with the domain www.cisco.com.

10. Refer to the exhibit. A cybersecurity analyst is viewing captured packets forwarded on switch S1. Which device is the source of the captured packet?

```

> Frame 17: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
> Ethernet II, Src: Micro-St_5c:d5:8a (d8:cb:8a:5c:d5:8a), Dst: Netgear_96:71:22 (50:6a:03:96:71:22)
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.18.47.62
> User Datagram Protocol, Src Port: 61526, Dst Port: 53
> Domain Name System (query)

```



- DNS server
- **PC-A**
- DG router
- ISP router
- web server

Explanation: The Wireshark output is displaying a DNS query that was sent from PC-A to switch S1. DNS queries are sourced from DNS clients, which in this case would be PC-A.

11. What is a purpose of implementing VLANs on a network?

- **They can separate user traffic.**
- They prevent Layer 2 loops.
- They eliminate network collisions.
- They allow switches to forward Layer 3 packets without a router.

Explanation: VLANs are used on a network to separate user traffic based on factors such as function, project team, or application, without regard for the physical location of the user or device.

12. Which type of firewall is a combination of various firewall types?

- packet filtering
- stateful
- proxy
- **hybrid**

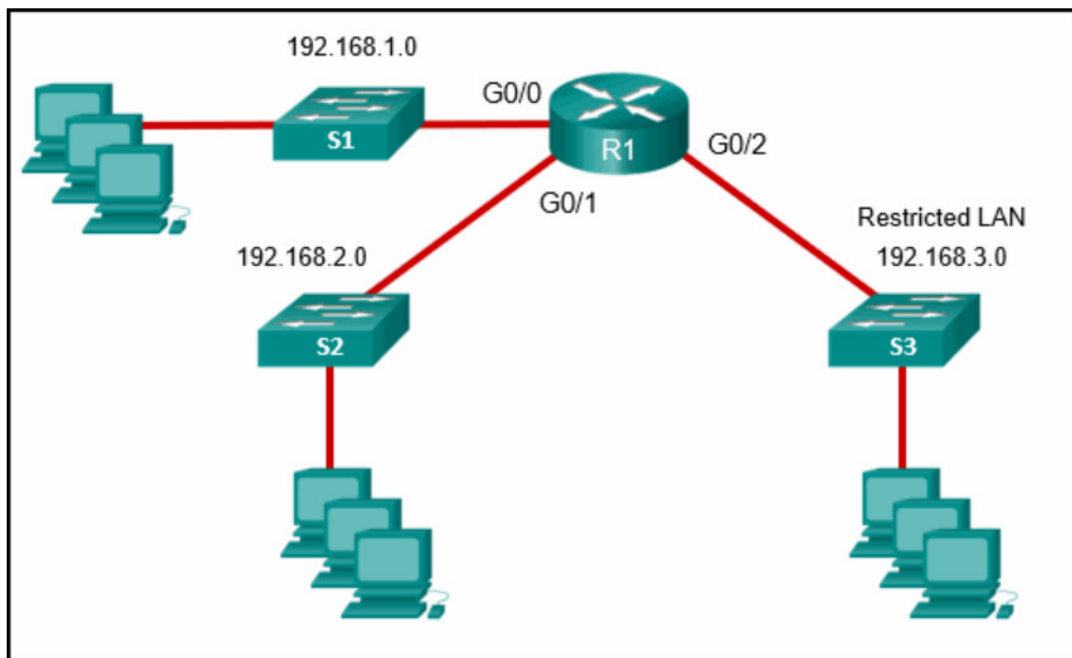
Explanation: A hybrid firewall is a combination of different firewall types such as combining a stateful firewall with an application gateway firewall.

13. What is a feature of an IPS?

- **It can stop malicious packets.**
- It has no impact on latency.
- It is deployed in offline mode.
- It is primarily focused on identifying possible incidents.

Explanation: An advantage of an intrusion prevention systems (IPS) is that it can identify and stop malicious packets. However, because an IPS is deployed inline, it can add latency to the network.

14. Refer to the exhibit. A network administrator has written a standard access control list to prevent packets from the 192.168.2.0 LAN from reaching the restricted LAN 192.168.3.0 while permitting traffic from any other LAN. On what interface and in which direction should the access list be implemented on router R1?



- interface G0/0 inbound
- interface G0/2 inbound
- **interface G0/2 outbound**
- interface G0/1 outbound

Explanation: The access list requires that the source network 192.168.2.0 is denied while other networks are permitted to reach the restricted LAN. The access list must be applied on interface G0/2 in the outbound direction.

15. What is an example of a local exploit?

- Port scanning is used to determine if the Telnet service is running on a remote server.
- A threat actor performs a brute force attack on an enterprise edge router to gain illegal access.
- A buffer overflow attack is launched against an online shopping website and causes the server crash.
- **A threat actor tries to gain the user password of a remote host by using a keyboard capture software installed on it by a Trojan.**

Explanation: Vulnerability exploits may be remote or local. In a local exploit, the threat actor has some type of user access to the end system, either physically or through remote access. The exploitation activity is within the local network.

16. After complaints from users, a technician identifies that the college web server is running very slowly. A check of the server reveals that there are an unusually large number of TCP requests coming from multiple locations on the Internet. What is the source of the problem?

- **A DDoS attack is in progress.**
- The server is infected with a virus.
- There is insufficient bandwidth to connect to the server.
- There is a replay attack in progress.

Explanation: The source of the problem cannot be a virus because in this situation the server is passive and at the receiving end of the attack. A replay attack uses intercepted and recorded data in an attempt to gain access to an unauthorized server. This type of attack does not involve multiple computers. The issue is not the bandwidth available, but the number of TCP connections taking place. Receiving a large number of connections from multiple locations is the main symptom of a distributed denial of service attack which use botnets or zombie computers.

17. A user receives an email requesting verification of the password that is used to access bank files. What type of security threat is this?

- virus
- social engineering
- **phishing**
- malware

Explanation: Phishing is a form of attack that starts with the attacker pretending to be a legitimate entity and then tries to gather information that can be used to conduct the exploit.

18. To which category of security attacks does man-in-the-middle belong?

- DoS
- **access**
- reconnaissance
- social engineering

Explanation: With a man-in-the-middle attack, a threat actor is positioned in between two legitimate entities in order to read, modify, or redirect the data that passes between the two parties.

19. What is the main goal of using different evasion techniques by threat actors?

- to launch DDoS attacks on targets
- to identify vulnerabilities of target systems
- to gain the trust of a corporate employee in an effort to obtain credentials
- **to prevent detection by network and host defenses**

Explanation: Many threat actors use stealthy evasion techniques to disguise an attack payload because the malware and attack methods are most effective if they are undetected. The goal is to prevent detection by network and host defenses.

20. What are two examples of DoS attacks? (Choose two.)

- phishing
- **ping of death**
- SQL injection
- port scanning
- **buffer overflow**

Explanation: The buffer overflow and ping of death DoS attacks exploit system memory-related flaws on a server by sending an unexpected amount of data or malformed data to the server.

21. Which attack is integrated with the lowest levels of the operating system of a host and attempts to completely hide the activities of the threat actor on the local system?

- **rootkit**
- traffic insertion
- traffic substitution
- encryption and tunneling

Explanation: A rootkit is a complex attack tool and it integrates with the lowest levels of the operating system. The goal of the rootkit is to completely hide the activities of the threat actor on the local system.

22. Which evasion method describes the situation that after gaining access to the administrator password on a compromised host, a threat actor is attempting to login to another host using the same credentials?

- **pivoting**
- traffic substitution
- resource exhaustion
- protocol-level misinterpretation

Explanation: Pivoting is an evasion method that assumes the threat actor has compromised an inside host and the actor wants to expand the access further into the compromised network.

23. Which two attacks target web servers through exploiting possible vulnerabilities of input functions used by an application? (Choose two.)

- **SQL injection**
- port scanning
- port redirection
- trust exploitation
- **cross-site scripting**

Explanation: When a web application uses input fields to collect data from clients, threat actors may exploit possible vulnerabilities for entering malicious commands. The malicious commands that are executed through the web application might affect the OS on the web server. SQL injection and cross-site scripting are two different types of command injection attacks.

24. What is the first line of defense when an organization is using a defense-in-depth approach to network security?

- IPS
- **edge router**
- firewall
- proxy server

Explanation: A defense-in-depth approach uses layers of security measures starting at the network edge, working through the network, and finally ending at the network endpoints. Routers at the network edge are the first line of defense and forward traffic intended for the internal network to the firewall.

25. What is the benefit of a defense-in-depth approach?

- **The effectiveness of other security measures is not impacted when a security mechanism fails.**

- The need for firewalls is eliminated.
- All network vulnerabilities are mitigated.
- Only a single layer of security at the network core is required.

Explanation: The benefit of the defense-in-depth approach is that network defenses are implemented in layers so that failure of any single security mechanism does not impact other security measures.

26. Which access control model allows users to control access to data as an owner of that data?

- mandatory access control
- nondiscretionary access control
- **discretionary access control**
- attribute-based access control

Explanation: In the discretionary access control (DAC) model, users can control access to data as owners of the data.

27. What is the principle behind the nondiscretionary access control model?

- It applies the strictest access control possible.
- **It allows access decisions to be based on roles and responsibilities of a user within the organization.**
- It allows users to control access to their data as owners of that data.
- It allows access based on attributes of the object to be accessed.

Explanation: The nondiscretionary access control model used the roles and responsibilities of the user as the basis for access decisions.

28. What is an example of privilege escalation attack?

- A threat actor sends an email to an IT manager to request the root access.
- **A threat actor performs an access attack and gains the administrator password.**
- A DDoS attack is launched against a government server and causes the server to crash.
- A port scanning attack finds that the FTP service is running on a server that allows anonymous access.

Explanation: With the privilege escalation exploit, vulnerabilities in servers or access control systems are exploited to grant an unauthorized user, or software process, higher levels of privilege than either should have. After the higher privilege is granted, the threat actor can access sensitive information or take control of a system.

29. Which access control model applies the strictest access control and is often used in military and mission critical applications?

- discretionary
- **mandatory**
- nondiscretionary
- attribute-based

Explanation: Military and mission critical applications typically use mandatory access control which applies the strictest access control to protect network resources.

30. Which data security component is provided by hashing algorithms?

- key exchange
- confidentiality
- **integrity**
- authentication

Explanation: Hashing algorithms are used to provide message integrity, which ensures that data in transit has not changed or been altered.

31. Which two algorithms use a hashing function to ensure message integrity? (Choose two.)

- SEAL
- AES
- 3DES
- **MD5**
- **SHA**

Explanation: Hashing algorithms are used to provide data integrity, which ensures that the data has not changed during transmission. MD5 and SHA are commonly used hashing algorithms.

32. What is a feature of asymmetrical encryption?

- **Different keys are used to encrypt and decrypt data.**
- Key lengths are short.
- It encrypts bulk data quickly.
- It requires fewer computations than symmetric encryption requires.

Explanation: Asymmetric encryption algorithms use different keys for encryption and decryption. These are known as private and public keys. The longer key lengths used by asymmetric algorithms make them slower than symmetrical encryption and inefficient for bulk data.

33. What technology supports asymmetric key encryption used in IPsec VPNs?

- 3DES
- **IKE**
- SEAL
- AES

Explanation: IKE, or Internet Key Exchange, is a protocol to support asymmetric encryption algorithms. It is used to securely exchange encryption keys in the setup of IPsec VPNs.

34. Which security function is provided by encryption algorithms?

- key management
- authorization
- integrity
- **confidentiality**

Explanation: Encryption algorithms are used to provide data confidentiality, which ensures that if data is intercepted in transit, it cannot be read.

35. A security professional is making recommendations to a company for enhancing endpoint security. Which security endpoint technology would be recommended as an agent-based system to protect hosts against malware?

- baselining
- blacklisting
- **HIDS**
- IPS

Explanation: A host-based intrusion detection systems (HIDS) is a comprehensive security application that provides antimalware applications, a firewall, and monitoring and reporting.

36. Which firewall application runs on a Linux host and allows an administrator to configure network access rules as part of the Linux kernel?

- vShield
- nftables
- TCP Wrapper
- **iptables**

Explanation: The iptables is an application that allows Linux system administrators to configure network access rules that are part of the Linux kernel Netfilter modules.

37. Which security endpoint setting would be used by a security analyst to determine if a computer has been configured to prevent a particular application from running?

- services
- block listing
- baselining
- Allow listing

Explanation: Block listing can be used on a local system or updated on security devices such as a firewall. Block lists can be manually entered or obtained from a centralized security system. Block lists are applications that are prevented from executing because they pose a security risk to the individual system and potentially the company.

38. Which technique could be used by security personnel to analyze a suspicious file in a safe environment?

- baselining
- blacklisting
- **sandboxing**
- whitelisting

Explanation: Sandboxing allows suspicious files to be executed and analyzed in a safe environment. There are free public sandboxes that allow for malware samples to be uploaded or submitted and analyzed.

39. Which attack surface, defined by the SANS Institute, is delivered through the exploitation of vulnerabilities in web, cloud, or host-based applications?

- host
- human
- network
- **software**

Explanation: The SANS Institute describes three components of the attack surface:

- Network Attack Surface – exploits vulnerabilities in networks
- Software Attack Surface – delivered through the exploitation of vulnerabilities in web, cloud, or host-based software applications
- Human Attack Surface – exploits weaknesses in user behavior

40. What is an action that should be taken in the discovery step of the vulnerability management life cycle?

- assigning business value to assets

- determining a risk profile
- **developing a network baseline**
- documenting the security plan

Explanation: During the discovery step of the vulnerability management life cycle, an inventory of all network assets is made. A network baseline is developed, and security vulnerabilities are identified.

41. Which security management plan specifies a component that involves tracking the location and configuration of networked devices and software across an enterprise?

- **asset management**
- risk management
- vulnerability management
- patch management

Explanation: Asset management involves tracking the location and configuration of networked devices and software across an enterprise.

42. Which risk management plan involves discontinuing an activity that creates a risk?

- risk reduction
- risk retention
- **risk avoidance**
- risk sharing

Explanation: During a risk assessment it may be determined that an activity involves more risk than benefit. In such a situation an organization may decide to avoid the risk altogether by discontinuing the activity. This is known as risk avoidance.

43. A piece of malware has gained access to a workstation and issued a DNS lookup query to a CnC server. What is the purpose of this attack?

- to request a change of the IP address
- **to send stolen sensitive data with encoding**
- to check the domain name of the workstation
- to masquerade the IP address of the workstation

Explanation: A piece of malware, after accessing a host, may exploit the DNS service by communicating with command-and-control (CnC) servers and then exfiltrate data in traffic disguised as normal DNS lookup queries. Various types of encoding, such as base64, 8-bit binary, and hex can be used to camouflage the data and evade basic data loss prevention (DLP) measures.

44. Why does HTTPS technology add complexity to network security monitoring?

- HTTPS uses tunneling technology for confidentiality.
- HTTPS hides the true source IP address using NAT/PAT.
- **HTTPS conceals data traffic through end-to-end encryption.**
- HTTPS dynamically changes the port number on the web server.

Explanation: With HTTPS, a symmetric key is generated by the client after the client verifies the trustworthiness of the web server. The symmetric key is encrypted with the public key of the web server and then sent to the web server. The web server uses its public key to decrypt the key. The key is then used to encrypt the data requested by the client and the data is sent to the client. This end-to-end encryption complicates inline network security monitoring. The HTTPS port number, typically 443, is configured statically on the web server.

45. Which type of attack is carried out by threat actors against a network to determine which IP addresses, protocols, and ports are allowed by ACLs?

- phishing
- **reconnaissance**
- denial of service
- social engineering

Explanation: Packet filtering ACLs use rules to filter incoming and outgoing traffic. These rules are defined by specifying IP addresses, port numbers, and protocols to be matched. Threat actors can use a reconnaissance attack involving port scanning or penetration testing to determine which IP addresses, protocols, and ports are allowed by ACLs.

46. How can NAT/PAT complicate network security monitoring if NetFlow is being used?

- It changes the source and destination MAC addresses.
- It conceals the contents of a packet by encrypting the data payload.
- It disguises the application initiated by a user by manipulating port numbers.
- **It hides internal IP addresses by allowing them to share one or a few outside IP addresses.**

Explanation: NAT/PAT maps multiple internal IP addresses with only a single or a few outside IP addresses breaking end-to-end flows. The result makes it difficult to log the inside device that is requesting and receiving the traffic. This is especially a problem with a NetFlow application because NetFlow flows are unidirectional and are defined by the addresses and ports that they share.

47. Which statement describes the function provided by the Tor network?

- It distributes user packets through load balancing.
- **It allows users to browse the Internet anonymously.**
- It conceals packet contents by establishing end-to-end tunnels.
- It manipulates packets by mapping IP addresses between two networks.

Explanation: Tor is a software platform and network of P2P hosts that function as Internet routers on the Tor network. The Tor network allows users to browse the Internet anonymously.

48. Refer to the exhibit. A security analyst is reviewing an alert message generated by Snort. What does the number 2100498 in the message indicate?

```
alert ip any any -> any any (msg:"GPL ATTACK RESPONSE id check returned root";  
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown;  
sid:2100498; rev:8;)
```

- the message length in bits
- **the Snort rule that is triggered**
- the session number of the message
- the id of the user that triggers the alert

Explanation: The sid field in a Snort alert message indicates the Snort security rule that is triggered.

49. Which type of data is used by Cisco Cognitive Threat Analytics to find malicious activity that has bypassed security controls, or entered through unmonitored channels, and is operating inside an enterprise network?

- alert
- session
- **statistical**
- transaction

Explanation: Cisco Cognitive Threat Analytics utilizes statistical data for statistical analysis in order to find malicious activity that has bypassed security controls, or entered through unmonitored channels (including removable media), and is operating inside the network of an organization.

50. Refer to the exhibit. A security analyst is reviewing the logs of an Apache web server. Which action should the analyst take based on the output shown?

- Ignore the message.
- **Notify the server administrator.**

- Restart the server.
- Notify the appropriate security administration for the country.

Explanation: An Apache web server is an open source server that delivers web pages. Security access logs for an Apache web server include a 3-digit HTTP code that represents the status of the web request. A code that begins with 2 indicates access success. A code that begins with 3 represents redirection. A code that begins with 4 represents a client error and a code that begins with 5 represents a server error. The server administrator should be alerted if a server error such as the 503 code occurs.

```
HTTP/1.1 503 Service Temporarily Unavailable
Date: Sat, Jul 2017 14:36:45 GMT
Server: Apache
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=3600,public,proxy-revalidate
Retry-After: 60
Content-Length: 4296
Connection: close
Content-Type: text/html
```

51. Which Windows application is commonly used by a cybersecurity analyst to view Microsoft IIS access logs?

- **Event Viewer**
- Notepad
- SIEM
- Word

Explanation: Event Viewer is an application on a Windows-based device used to view event logs including IIS access logs.

52. Which tool captures full data packets with a command-line interface only?

- nfdump
- NBAR2
- **tcpdump**
- Wireshark

Explanation: The command-line tool tcpdump is a packet analyzer. Wireshark is a packet analyzer with a GUI interface.

53. What is a key difference between the data captured by NetFlow and data captured by Wireshark?

- NetFlow provides transaction data whereas Wireshark provides session data.
- NetFlow data is analyzed by tcpdump whereas Wireshark data is analyzed by nfdump.
- **NetFlow collects metadata from a network flow whereas Wireshark captures full data packets.**

- NetFlow data shows network flow contents whereas Wireshark data shows network flow statistics.

Explanation: Wireshark captures the entire contents of a packet. NetFlow does not. Instead, NetFlow collects metadata, or data about the flow.

54. Which Cisco appliance can be used to filter network traffic contents to report and deny traffic based on the web server reputation?

- ASA
- AVC
- ESA
- **WSA**

Explanation: The Cisco Web Security Appliance (WSA) acts as a web proxy for an enterprise network. WSA can provide many types of logs related to web traffic security including ACL decision logs, malware scan logs, and web reputation filtering logs. The Cisco Email Security Appliance (ESA) is a tool to monitor most aspects of email delivery, system functioning, antivirus, antispam operations, and blacklist and whitelist decisions. The Cisco ASA is a firewall appliance. The Cisco Application Visibility and Control (AVC) system combines multiple technologies to recognize, analyze, and control over 1000 applications.

55. Which type of event is logged in Cisco Next-Generation IPS devices (NGIPS) using FirePOWER Services when changes have been detected in the monitored network?

- intrusion
- connection
- host or endpoint
- **network discovery**

Explanation: Network discovery events in Cisco NGIPS represent changes that have been detected in the monitored network.

New Questions for 210-250 Exam (Dump)

61. Which definition of a process in Windows is true?

- **running program**
- unit of execution that must be manually scheduled by the application
- database that stores low-level settings for the OS and for certain applications
- basic unit to which the operating system allocates processor time

62. Which definition of permissions in Linux is true?

- rules that allow network traffic to go in and out
- table maintenance program
- written affidavit that you have to sign before using the system
- **attributes of ownership and control of an object**

63. Which hashing algorithm is the least secure?

- **MD5**
- RC4
- SHA-3
- SHA-2

64. Which protocol is expected to have NTP, a user agent, host, and referrer headers in a packet capture?

- NTP
- **HTTP**
- DNS
- SSH

65. Which definition of a daemon on Linux is true?

- error check right after the call to fork a process
- new process created by duplicating the calling process
- **program that runs unobtrusively in the background**
- set of basic CPU instructions

66. Which definition of vulnerability is true?

- **an exploitable unpatched and unmitigated weakness in software**
- an incompatible piece of software
- software that does not have the most current patch applied
- software that was not approved for installation

67. Which option is an advantage to using network-based anti-virus versus host-based anti-virus?

- **Network-based has the ability to protect unmanaged devices and unsupported operating systems.**
- There are no advantages compared to host-based antivirus.
- Host-based antivirus does not have the ability to collect newly created signatures.
- Network-based can protect against infection from malicious files at rest.

68. Which evasion method involves performing actions slower than normal to prevent detection?

- traffic fragmentation
- tunneling
- **timing attack**
- resource exhaustion

69. Which event occurs when a signature-based IDS encounters network traffic that triggers an alert?

- A. connection event
- B. endpoint event
- C. NetFlow event
- **D. intrusion event**

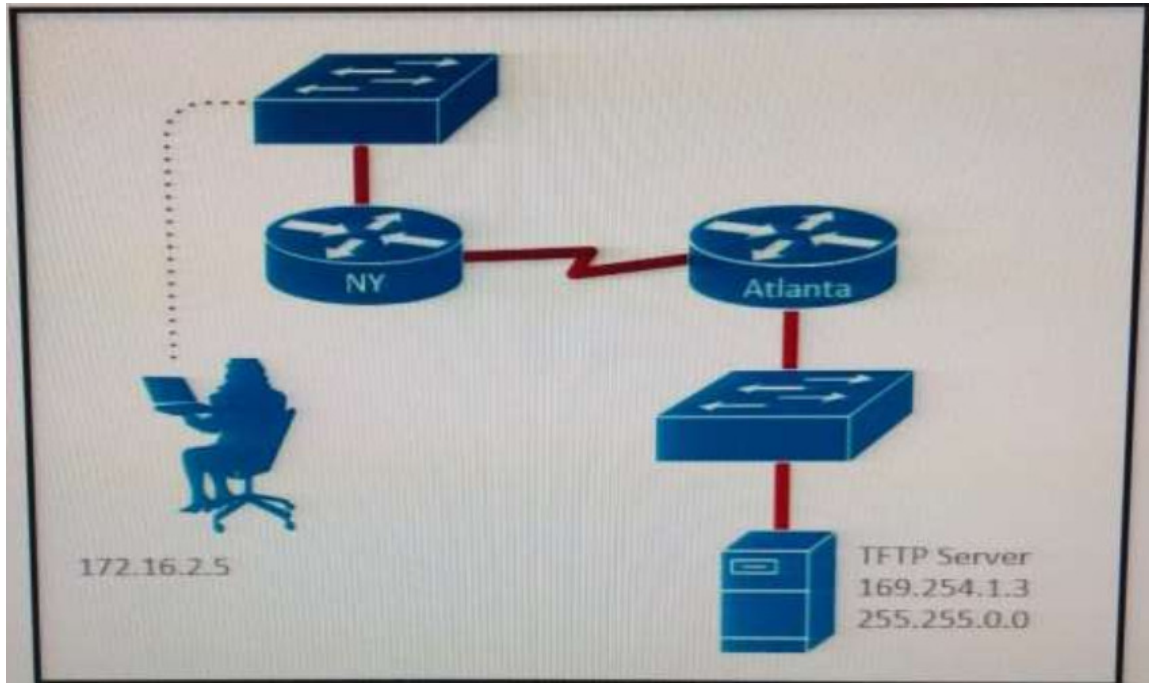
70. Which data can be obtained using NetFlow?

- **session data**
- application logs
- network downtime
- report full packet capture

71. Which term describes the act of a user, without authority or permission, obtaining rights on a system, beyond what were assigned?

- authentication tunneling
- administrative abuse
- rights exploitation
- **privilege escalation**

72. Refer to the exhibit. A TFTP server has recently been installed in the Atlanta office. The network administrator is located in the NY office and has attempted to make a connection to the TFTP server. They are unable to backup the configuration file and Cisco IOS of the NY router to the TFTP server Which cause of this problem is true?



- **The TFTP server cannot obtain an address from a DHCP Server.**
- The TFTP server has an incorrect IP address.
- The network administrator computer has an incorrect IP address
- The TFTP server has an incorrect subnet mask.

Explanation: If a host cannot obtain an IP address from a DHCP server, it automatically assigns itself an Automatic Private IP Addressing (APIPA) IP address until a DHCP server becomes available. The IP address range is 169.254.0.1 through 169.254.255.254.

73. Which term represents a potential danger that could take advantage of a weakness in a system?

- vulnerability
- risk
- **threat**
- Dexploit

Explanation: A threat is any potential danger to assets. An exploit is a method of leveraging a vulnerability to do harm.

74. Which security principle states that more than one person is required to perform a critical task?

- due diligence
- **separation of duties**
- need to know
- least privilege

75. You must create a vulnerability management framework. Which main purpose of this framework is true?

- Conduct vulnerability scans on the network.
- Manage a list of reported vulnerabilities.
- **Identify remove and mitigate system vulnerabilities.**
- Detect and remove vulnerabilities in source code.

76. In computer security, which information is the term PHI used to describe?

- private host information
- **protected health information**
- personal health information
- protected host information

77. Which security monitoring data type requires the most storage space?

- **full packet capture**
- transaction data
- statistical data
- session data

78. Which type of exploit normally requires the culprit to have prior access to the target system?

- **local exploit**
- denial of service
- system vulnerability
- remote exploit

79. Which identifier is used to describe the application or process that submitted a log message?

- action
- selector
- priority
- **facility**

80. Which concern is important when monitoring NTP servers for abnormal levels of traffic?

- **Being the cause of a distributed reflection denial of service attack.**
- Users changing the time settings on their systems.
- A critical server may not have the correct time synchronized.
- Watching for rogue devices that have been added to the network.

81. Which protocol is primarily supported by the third layer of the Open Systems Interconnection reference model?

- HTTP/TLS
- **IPv4/IPv6**
- TCP/UDP
- ATM/ MPLS

82. A firewall requires deep packet inspection to evaluate which layer?

- **application**
- Internet
- link
- transport

83. Which two protocols are used for email (Choose two)

- NTP
- DNS
- HTTP
- **IMAP**
- **SMTP**

84. Which two options are recognized forms of phishing? (Choose two)

- **spear**
- **whaling**
- mailbomb
- hooking
- mailnet

85. While viewing packet capture data, you notice that one IP is sending and receiving traffic for multiple devices by modifying the IP header, Which option is making this behavior possible?

- TOR
- **NAT**
- encapsulation
- tunneling

86. Which definition of an antivirus program is true?

- **program used to detect and remove unwanted malicious software from the system**

- program that provides real time analysis of security alerts generated by network hardware and application
- program that scans a running application for vulnerabilities
- rules that allow network traffic to go in and out

87. Which type of attack occurs when an attacker is successful in eavesdropping on a conversation between two IPS phones?

- replay
- **man-in-the-middle**
- dictionary
- known-plaintext

88. An intrusion detection system begins receiving an abnormally high volume of scanning from numerous sources. Which evasion technique does this attempt indicate?

- traffic fragmentation
- **resource exhaustion**
- timing attack
- tunneling

89. Which type of attack occurs when an attacker utilizes a botnet to reflect requests off an NTP server to overwhelm their target?

- man in the middle
- denial of service
- **distributed denial of service**
- replay

90. In NetFlow records, which flags indicate that an HTTP connection was stopped by a security appliance, like a firewall, before it could be built fully?

- ACK
- SYN ACK
- **RST**
- PSH, ACK

Explanation: When a connection is stopped by a security appliance it will send an RST flag.

91. Which definition of a fork in Linux is true?

- daemon to execute scheduled commands
- parent directory name of a file pathname
- macros for manipulating CPU sets

- **new process created by a parent process**

92. Which two actions are valid uses of public key infrastructure?(Choose two)

- ensuring the privacy of a certificate
- **revoking the validation of a certificate**
- **validating the authenticity of a certificate**
- creating duplicate copies of a certificate
- changing ownership of a certificate

Explanation: The purpose of PKI is the secure distribution of public keys. It helps answer three (3) questions to authenticate a certificate. Is it valid, is it signed and is it revoked.

93. Which two terms are types of cross site scripting attacks? (Choose two)

- directed
- encoded
- **stored**
- **reflected**
- cascaded

94. Which network device is used to separate broadcast domains?

- **router**
- repeater
- switch
- bridge

95. Based on which statement does the discretionary access control security model grant or restrict access ?

- discretion of the system administrator
- **security policy defined by the owner of an object**
- security policy defined by the system administrator
- role of a user within an organization

96. Which cryptographic key is contained in an X.509 certificate?

- symmetric
- **public**
- private
- asymmetric

97. Which two activities are examples of social engineering? (Choose two)

- **receiving call from the IT department asking you to verify your username/password to maintain the account**
- receiving an invite to your department's weekly WebEx meeting
- sending a verbal request to an administrator to change the password to the account of a user the administrator does know
- receiving an email from MR requesting that you visit the secure HR website and update your contract information
- **receiving an unexpected email from an unknown person with an uncharacteristic attachment from someone in the same company**

Explanation: D should say HR not MR, once you get beyond that. Both D & E are possible, E is more practical, IMHO.

98. Which hash algorithm is the weakest?

- SHA-512
- RSA 4096
- **SHA-1**
- SHA-256

99. A user reports difficulties accessing certain external web pages, When examining traffic to and from the external domain in full packet captures, you notice many SYN's that have the same sequence number, source, and destination IP address, but have different payloads. Which problem is a possible explanation of this situation?

- insufficient network resources
- failure of full packet capture solution
- misconfiguration of web filter
- **TCP injection**

100. Which tool is commonly used by threat actors on a webpage to take advantage of the software vulnerabilities of a system to spread malware?

- **exploit kit**
- root kit
- vulnerability kit
- script kiddie kit

101. Refer to the exhibit. During an analysis this list of email attachments is found. Which files contain the same content?

Attachment filename	file size	SHA1 hash
1. scanned_document_876.doc	28954	263d8d12672e65a8868794ff193f146d198b0cf717
2. scanned_document_544.doc	28954	0ca1dc0be4f24091d12cc29edbcf14d10f4e329f
3. scanned_copy_1921.doc	28954	263d8d12672e65a8868794ff193f146d198b0cf717
4. scanned_document_876.doc	28954	95efcc5a0765f7923e4a9eab011e9b1a35235a3
5. invoice.exe	32698	3d570849ab8fb1a049ed15ceda17c417c5a174fc

- 1 and 4
- 3 and 4
- **1 and 3**
- 1 and 2

102. Which term represents the practice of giving employees only those permissions necessary to perform their specific role within an organization?

- integrity validation
- due diligence
- need to know
- **least privilege**

103. Which term represents the chronological record of how evidence was collected- analyzed, preserved, and transferred?

- chain of evidence
- evidence chronology
- **chain of custody**
- record of safekeeping

104. Which two tasks can be performed by analyzing the logs of a traditional stateful firewall? (Choose two.)

- **Confirm the timing of network connections differentiated by the TCP 5-tuple**
- Audit the applications used within a social networking web site.
- Determine the user IDs involved in an instant messaging exchange.
- **Map internal private IP addresses to dynamically translated external public IP addresses**
- Identify the malware variant carried by ^n SMTP connection

105. Which security monitoring data type is associated with application server logs?

- alert data
- statistical data
- session data

- **transaction data**

106. Where is a host-based intrusion detection system located?

- **on a particular end-point as an agent or a desktop application**
- on a dedicated proxy server monitoring egress traffic
- on a span switch port
- on a tap switch port

107. One of the objectives of information security is to protect the CIA of information and systems. What does CIA mean in this context?

- **Confidentiality, Integrity, and Availability**
- Confidentiality, Identity, and Availability
- Confidentiality, Integrity, and Authorization
- Confidentiality, Identity, and Authorization

108. According to RFC 1035 which transport protocol is recommended for use with DNS queries?

- Transmission Control Protocol
- Reliable Data Protocol
- Hypertext Transfer Protocol
- **User Datagram Protocol**

109. Which definition describes the main purpose of a Security Information and Event Management solution ?

- a database that collects and categorizes indicators of compromise to evaluate and search for potential security threats
- a monitoring interface that manages firewall access control lists for duplicate firewall filtering
- a relay server or device that collects then forwards event logs to another log collection device
- **a security product that collects, normalizes, and correlates event log data to provide holistic views of the security posture**

110. Which option is a purpose of port scanning?

- Identify the Internet Protocol of the target system.
- Determine if the network is up or down
- **Identify which ports and services are open on the target host.**
- Identify legitimate users of a system.

111. Which definition of the virtual address space for a Windows process is true?

- actual physical location of an object in memory
- **set of virtual memory addresses that it can use**
- set of pages that are currently resident in physical memory
- system-level memory protection feature that is built into the operating system

112. Which information security property is supported by encryption?

- sustainability
- integrity
- **confidentiality**
- availability

113. Which situation indicates application-level white listing?

- Allow everything and deny specific executable files.
- Allow specific executable files and deny specific executable files.
- Writing current application attacks on a whiteboard daily.
- **Allow specific files and deny everything else.**

114. If a web server accepts input from the user and passes it to a bash shell, to which attack method is it vulnerable?

- input validation
- hash collision
- **command injection**
- integer overflow

Explanation: https://www.owasp.org/index.php/Command_Injection

115. Which encryption algorithm is the strongest?

- **AES**
- CES
- DES
- 3DES

116. Which protocol maps IP network addresses to MAC hardware addresses so that IP packets can be sent across networks?

- Internet Control Message Protocol
- **Address Resolution Protocol**
- Session Initiation Protocol
- Transmission Control Protocol/Internet Protocol

117. Which statement about digitally signing a document is true?

- The document is hashed and then the document is encrypted with the private key.
- **The document is hashed and then the hash is encrypted with the private key.**
- The document is encrypted and then the document is hashed with the public key
- The document is hashed and then the document is encrypted with the public key.

118. For which reason can HTTPS traffic make security monitoring difficult?

- **encryption**
- large packet headers
- Signature detection takes longer.
- SSL interception

Explanation: Encryption itself makes it difficult in that you are unable to view the encrypted traffic for security monitoring purposes.

119. Which directory is commonly used on Linux systems to store log files, including syslog and apache access logs?

- /etc/log
- /root/log
- /lib/log
- **/var/log**

120. Drag and Drop.

Drag the technology on the left to the data type the technology provides on the right.

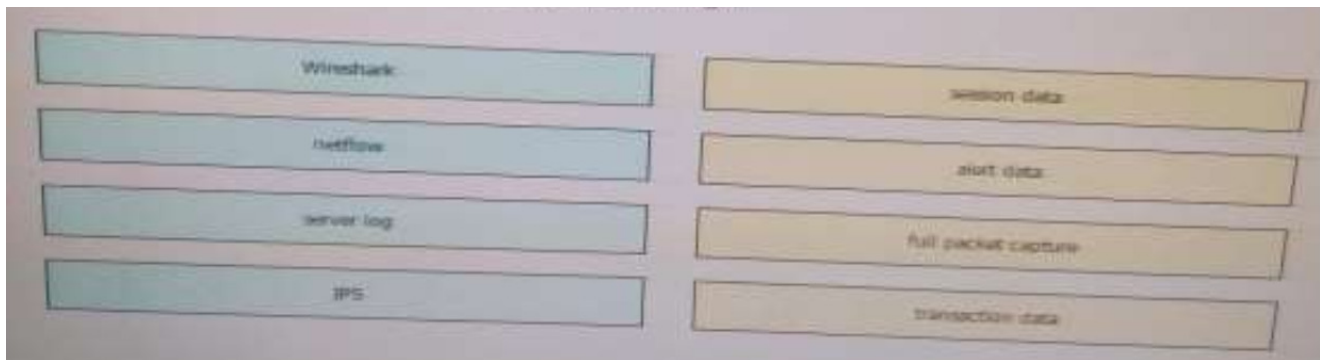
trickleping	session data
web content filtering	full packet capture
traditional stateful firewall	transaction data
netflow	connection speed

Answer:

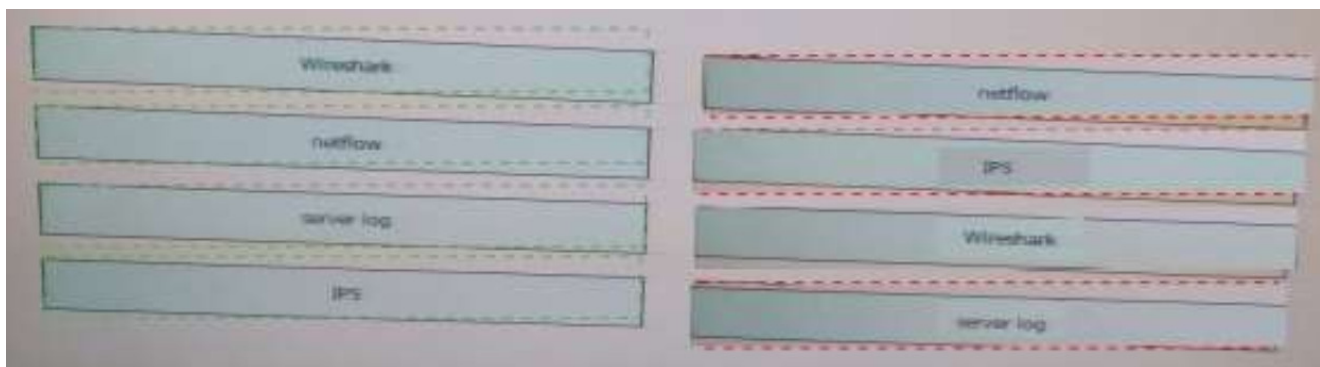
	netflow
	trickleping
	web content filtering
	traditional stateful firewall

121. Drag and Drop.

Drag the data source on the left to the left to the correct data type on the right.



Answer:



122. Which technology allows a large number of private IP addresses to be represented by a smaller number of public IP addresses?

- NAT
- NTP
- RFC 1631
- RFC 1918

123. Which NTP command configures the local device as an NTP reference clock source?

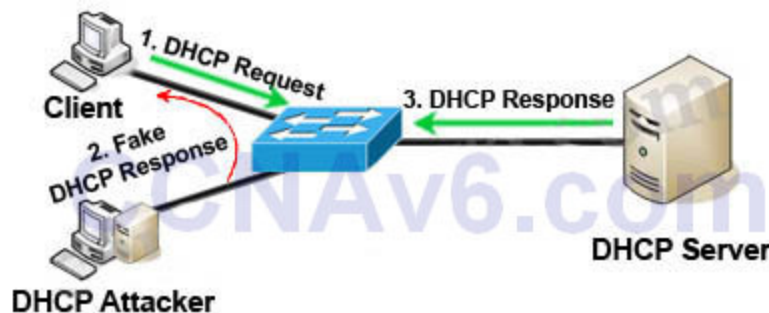
- ntp peer
- ntp broadcast
- **ntp master**
- ntp server

124. Which three options are types of Layer 2 network attack? (Choose three.)

- **ARP attacks**
- brute force attacks
- **spoofing attacks**

- DDOS attacks
- **VLAN hopping**
- botnet attacks

Explanation:

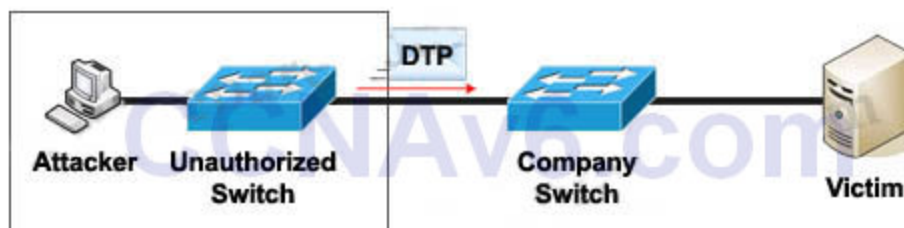


(DHCP) Spoofing attack is a type of attack in that the attacker listens for DHCP Requests from clients and answers them with fake DHCP Response before the authorized DHCP Response comes to the clients. The fake DHCP Response often gives its IP address as the client default gateway -> all the traffic sent from the client will go through the attacker computer, the attacker becomes a “man-in-the-middle”.

The attacker can have some ways to make sure its fake DHCP Response arrives first. In fact, if the attacker is “closer” than the DHCP Server then he doesn’t need to do anything. Or he can DoS the DHCP Server so that it can’t send the DHCP Response.

VLAN Hopping: By altering the VLAN ID on packets encapsulated for trunking, an attacking device can send or receive packets on various VLANs, bypassing Layer 3 security measures. VLAN hopping can be accomplished by switch spoofing or double tagging.

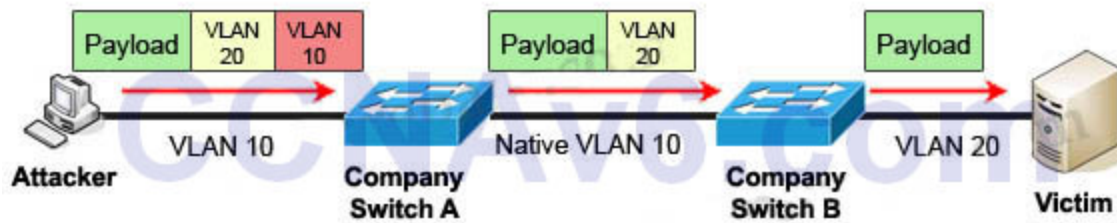
1) Switch spoofing:



The attacker can connect an unauthorized Cisco switch to a Company switch port. The unauthorized switch can send DTP frames and form a trunk with the Company Switch. If the attacker can establish a trunk link to the Company switch, it receives traffic to all VLANs through the trunk because all VLANs are allowed on a trunk by default.

(Instead of using a Cisco Switch, the attacker can use a software to create and send DTP frames).

2) Double-Tagging:



In this attack, the attacking computer generates frames with two 802.1Q tags. The first tag matches the native VLAN of the trunk port (VLAN 10 in this case), and the second matches the VLAN of a host it wants to attack (VLAN 20).

When the packet from the attacker reaches Switch A, Switch A only sees the first VLAN 10 and it matches with its native VLAN 10 so this VLAN tag is removed. Switch A forwards the frame out all links with the same native VLAN 10. Switch B receives the frame with an tag of VLAN 20 so it removes this tag and forwards out to the Victim computer.

Note: This attack only works if the trunk (between two switches) has the same native VLAN as the attacker.

ARP attack (like ARP poisoning/spoofing) is a type of attack in Which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. This is an attack based on ARP Which is at Layer 2.

125. If a router has four interfaces and each interface is connected to four switches, how many broadcast domains are present on the router?

- 1
- 2
- 4
- 8

Explanation: Remember that only route interface can separate broadcast domain (while switch interface separate collision domain) so the broadcast domains are equal to the number of router interfaces, which is four in this case.

126. Where does routing occur within the DoD TCP/IP reference model?

- application
- **internet**
- network
- transport

127. Which two features must a next generation firewall include? (Choose two.)

- data mining
- host-based antivirus
- **application visibility and control**
- Security Information and Event Management
- **intrusion detection system**

128. Which term represents a weakness in a system that could lead to the system being compromised?

- **vulnerability**
- threat
- exploit
- risk

129. Which definition of Windows Registry is true?

- set of pages that are currently resident in physical memory
- basic unit to which the operating system allocates processor time
- set of virtual memory addresses
- **database that stores low-level settings for the operating system**

130. Which definition of the IIS Log Parser tool is true?

- a logging module for IIS that allows you to log to a database
- a data source control to connect to your data source
- **a powerful, versatile tool that makes it possible to run SQL-like queries against log files**
- a powerful versatile tool that verifies the integrity of the log files

131. What is PHI?

- Protected HIPAA information
- **Protected health information**
- Personal health information
- Personal human information

132. Which of the following are Cisco cloud security solutions?

- CloudDLP
- **OpenDNS**
- **CloudLock**
- CloudSLS

133. What is a trunk link used for?

- **To pass multiple virtual LANs**
- To connect more than two switches
- To enable Spanning Tree Protocol
- To encapsulate Layer 2 frames

134. At which OSI layer does a router typically operate?

- Transport
- **Network**
- Data link
- Application

135. Cisco pxGrid has a unified framework with an open API designed in a hub-and-spoke architecture. pxGrid is used to enable the sharing of contextual-based information from which devices?

- From a Cisco ASA to the Cisco OpenDNS service
- From a Cisco ASA to the Cisco WSA
- From a Cisco ASA to the Cisco FMC
- **From a Cisco ISE session directory to other policy network systems, such as Cisco IOS devices and the Cisco ASA**

136. What are the advantages of a full-duplex transmission mode compared to half-duplex mode? (Select all that apply.)

- **Each station can transmit and receive at the same time.**
- **It avoids collisions.**
- It makes use of backoff time.
- It uses a collision avoidance algorithm to transmit.

137. Stateful and traditional firewalls can analyze packets and judge them against a set of predetermined rules called access control lists (ACLs). They inspect which of the following elements within a packet? (Choose Two)

- Session headers
- NetFlow flow information
- **Source and destination ports and source and destination IP addresses**
- **Protocol information**

138. In which case should an employee return his laptop to the organization?

- When moving to a different role
- Upon termination of the employment

- **As described in the asset return policy**
- When the laptop is end of lease

139. Which of the following are metrics that can measure the effectiveness of a runbook?

- Mean time to repair (MTTR)
- Mean time between failures (MTBF)
- Mean time to discover a security incident
- **All of the above**

140. Which of the following access control models use security labels to make access decisions?

- **Mandatory access control (MAC)**
- Role-based access control (RBAC)
- Identity-based access control (IBAC)
- Discretionary access control (DAC)

Explanation: MAC uses security labels for access decisions.

141. Where are configuration records stored?

- **In a CMDB**
- In a MySQL DB
- In a XLS file
- There is no need to store them

142. Which of the following is true about heuristic-based algorithms?

- **Heuristic-based algorithms may require fine tuning to adapt to network traffic and minimize the possibility of false positives.**
- Heuristic-based algorithms do not require fine tuning.
- Heuristic-based algorithms support advanced malware protection.
- Heuristic-based algorithms provide capabilities for the automation of IPS signature creation and tuning.

143. How many broadcast domains are created if three hosts are connected to a Layer 2 switch in full- duplex mode?

- 4
- 3
- None
- **1**

144. What is one of the advantages of the mandatory access control (MAC) model?

- **Stricter control over the information access.**
- Easy and scalable.
- The owner can decide whom to grant access to.
- Complex to administer.

Explanation: Strict control over the access to resources is one of the main advantages of MAC.

145. According to the attribute-based access control (ABAC) model, what is the subject location considered?

- **Part of the environmental attributes**
- Part of the object attributes
- Part of the access control attributes
- None of the above

146. What type of algorithm uses the same key to encryp and decrypt data?

- **symmetric algorithm**
- an asyetric algorithm
- a Public Key infrastructure algorithm
- an IP Security algorithm

147. Which actions can a promiscuous IPS take to mitigate an attack?

- modifying packets
- **requesting connection blocking**
- denying packets
- **resetting the TCP connection**
- requesting host blocking
- **denying frames**

148. Which Statement about personal firewalls is true?

- They are resilient against kernal attacks
- They can protect email messages and private documents in a similar way to a VPN
- They can protect the network against attacks
- **They can protect a system by denying probing requests**

149. Which three statements about host-based IPS are true? (Choose three)

- **It can view encrypted files**

- It can be deployed at the perimeter
- It uses signature-based policies
- **It can have more restrictive policies than network-based IPS**
- It works with deployed firewalls
- **It can generate alerts based on behavior at the desktop level.**

150. An attacker installs a rogue switch that sends superior BPDUs on your network. What is a possible result of this activity?

- The switch could offer fake DHCP addresses.
- **The switch could become the root bridge.**
- The switch could be allowed to join the VTP domain
- The switch could become a transparent bridge.

151. The FMC can share HTML, Pdf and csv data type that relate to a specific event type which event type:

- connection
- Host
- Netflow
- **Intrusion**

Explanation:

The FMC has features that you can use to gather intrusion data in standard formats such as HTML, PDF, and comma-separated values (CSV) files so that you can easily share intrusion data with other entities. For instance, CERT/CC collects standard information about security incidents on its website that you can easily extract from FMC, such as the following:

152. For which purpose can Windows management instrumentation be used?

- **Remote viewing of a computer**
- Remote blocking of malware on a computer
- Remote reboot of a computer
- Remote start of a computer

Explanation:

The purpose of WMI is to define a set of proprietary environment-independent specifications used for management information that's shared between management applications. WMI allows scripting languages to locally and remotely manage Microsoft Windows computers and services. The following list provides examples of what WMI can be used for:

- Providing information about the status of local or remote computer systems
- Configuring security settings
- Modifying system properties
- Changing permissions for authorized users and user groups
- Assigning and changing drive labels
- Scheduling times for processes to run
- Backing up the object repository
- Enabling or disabling error logging

153. Which international standard is for general risk management, including the principles and guideline for managing risk?

- **ISO 31000**
- ISO 27001
- ISO 27005
- ISO 27002

Explanation:

are appropriately managed according to the threats and the nature of those threats. **ISO 31000** is the **general risk management standard** that includes principles and guidelines for managing risk. It can be used by any organization, regardless of its size, activity, or sector. Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats, and effectively allocate and use resources for risk treatment.

154. Which statement about the difference between a denial-of-service attack and a distributed denial of service attack is true?

- **Dos attack are launched from one host, and DDoS attack are launched from multiple host.**
- DoS attack and DDOS attack have no differences
- DDoS attacks are launched from one host, and DoS attacks are launched from multiple host.
- Dos attack only use flooding to compromise a network, and DDoS attacks only use other methods

Explanation:

DDoS refers to a 'distributed denial of service' attack. With this attack a hacker will use multiple servers to attack another target server i.e. the attack is distributed across multiple servers. Traffic associated with a single DDoS attack may originate from hundreds or thousands of compromised servers or PCs.

Whereas a 'denial of service' (DoS) attack is when a single server is used to attack another targeted server.

155. You discover that a foreign government hacked one of the defense contractors in your country and stole intellectual property. In this situation, which option is considered the threat agent?

- **method in which the hack occurred.**
- defense contractor that stored the intellectual property.
- intellectual property that was stolen.
- foreign government that conducted the attack.

Explanation:

A threat is any potential danger to an asset. If a vulnerability exists but has not yet been exploited—or, more importantly, it is not yet publicly known—the threat is latent and not yet realized. If someone is actively launching an attack against your system and successfully accesses something or compromises your security against an asset, the threat is realized. The entity that takes advantage of the vulnerability is known as the *malicious actor*, and the path used by this actor to perform the attack is known as the *threat agent* or *threat vector*.

156. After a large influx of network traffic to externally facing devices, you begin investigating what appear to be a denial of service attack. When you review packets capture data, you notice that the traffic is a single SYN packet to each port. Which kind of attack is this?

- SYN flood.
- Host profiling.
- traffic fragmentation.
- **port scanning.**

157. Which definition of common event format is terms of a security information and event management solution is true?

- a type of event log used to identify a successful user login.
- a TCP network media protocol.
- Event log analysis certificate that stands for certified event forensics.
- **a standard log event format that is used for log collection.**

Explanation:

The Security Information and Event Manager (SIEM) is a specialized device or software for security event management. It typically allows for the following functions:

- **Log collection:** This includes receiving information from devices with multiple protocols and formats, storing the logs, and providing historical reporting and log filtering.

158. Which definition of a Linux daemon is true?

- Process that is causing harm to the system by either using up system resources or causing a critical crash.
- **Long – running process that is the child at the init process**
- process that has no parent process
- process that is starved at the CPU.

Explanation:

Daemons

We opened this chapter by explaining how processes can run in the foreground and background. When a process runs in the background, it is known as a *daemon*. Daemons are not controlled by the active user; instead they run unobtrusively in the background, waiting to be activated by the occurrence of a specific event or condition. UNIX systems usually have numerous daemons running to accommodate requests for services from other computers and responding to other programs and hardware activity. Daemon can be triggered by many things, such as a specific time, event, file being viewed, and so on. Essentially, daemons listen for specific things to trigger their response.

When initiated, a daemon, like any other process, will have an associated process identification number (PID). Daemons are system processes, so their parent is usually the *init* process, which has a PID value of 1 (but this is not always the case). Daemon processes are created by the system using the *fork* command, thus forming the process hierarchy covered previously in this chapter.

159. Which term describes reasonable effort that must be made to obtain relevant information to facilitate appropriate courses of action?

- **Due diligence**
- ethical behavior
- decision making
- data mining.

160. According to the common vulnerability scoring system, which term is associated with scoring multiple vulnerabilities that are exploit in the course of a single attack?

- chained score
- risk analysis
- **Vulnerability chaining**
- confidentiality

Explanation:

Vulnerability Chaining

CVSS is designed to classify and rate individual vulnerabilities. However, it is important to support the needs of the vulnerability analysis community by accommodating situations where multiple vulnerabilities are exploited in the course of a single attack to compromise a host or application. The scoring of multiple vulnerabilities in this manner is termed Vulnerability Chaining. Note that this is not a formal metric, but is included as guidance for analysts when scoring these kinds of attacks.

161. Which Linux terminal command can be used to display all the processes?

- ps -m
- ps -u
- ps -d
- **ps -ef**

Explanation:

To see the processes for all users, you can add the `-e` option. If you combine the `-e` and `-f` options, you get both the full set of columns and processes for all users. You can shorten the options by grouping them after the dash (`-ef`). An example in the command line is:

```
ed@carl:~$ ps -ef
```

162. Which statement about an attack surface is true?

- **It is the sum of all paths for data/commands into and out of the application**
- It is an exploitable weakness in a system or design
- It is the individual who perform an attack.
- It is any potential danger to an asset.

Explanation:

Attack surface is the total sum of all the vulnerabilities in a given computing device or network that are accessible to the attackers. Attack surface may be categorized into different areas, such as software attack surfaces (open ports on a server), physical attack surfaces (USB ports on a laptop), network attack surfaces (console ports on a router), and human/social engineering attack surfaces (employees with access to sensitive information).

163. You get an alert on your desktop computer showing that an attack was successful on the host but up on investigation you see that occurred duration the attack. Which reason is true?

- **The computer has HIDS installed on it**
- The computer has NIDS installed on it
- The computer has HIPS installed on it
- The computer has NIPS installed on it

164. Which process continues to be recorded in the process table after it has ended and the status is returned to the parent?

- daemon
- zombie
- **orphan**
- child

Explanation:

When the process ends, any associated system resources are freed up and any open files are flushed and closed. If a parent is waiting for a child process to terminate, a termination status and the time of execution are returned to the parent process. The same data can be returned to the init process if the process that ended was an orphan process.

An *orphan process* results when a parent process is terminated and the child process is permitted to continue on its own. Orphan processes become the child process of the init process; but they are still labeled as orphan processes because their parent no longer exists. The time between when the child process ends and the status information is returned to the parent, the process continues to be recorded

165. For which kind of attack does an attacker use known information in encrypted files to break the encryption scheme for the rest of

- **known-plaintext**
- known-ciphertext
- unknown key
- man in the middle

Explanation:

• **Known-plaintext attack:** In a known-plaintext attack, the attacker has access to the ciphertext of several messages but also knows something about the plaintext that underlies that ciphertext. With knowledge of the underlying protocol, file type, or some characteristic strings that may appear in the plaintext, the attacker uses a brute-force attack to try keys, until decryption with the correct key produces a meaningful result. This attack may be the most practical attack, because attackers can usually assume the type and some features of the underlying plaintext. If they can only capture the ciphertext. However, modern algorithms with enormous key spaces make it unlikely for this attack to succeed, because on average an attacker has to search through at least half of the key space to be successful.

166. In which technology is network level encrypted not natively incorporated?

- **Kerberos**
- ssl
- tls
- IPsec

167. Which purpose of command and control for network aware malware is true?

- It helps the malware to profile the host
- It takes over the user account
- **It contacts a remote server for command and updates**
- It controls and down services on the infected host

168. Which action is an attacker taking when they attempt to gain root access on the victims system?

- **privilege escalation**
- command injections
- root kit
- command and control

Explanation:

After the initial access to an endpoint, attackers may be confined to using the privileges of employees with very limited access. The attackers may need but not have system-level permissions. Vulnerable services may be running as administrator or root user. The attackers cannot effectively spread throughout the network without escalating their privilege level.

169. Which vulnerability is an example of Shellshock?

- SQL injection
- heap Overflow
- cross site scripting
- **command injection**

Explanation:

The Shellshock vulnerability, also known as [CVE-2014-6271](#), allows attackers to inject their own code into [Bash](#) using specially crafted environment variables, and it was disclosed with the following description:

170. In which format are NetFlow records stored?

- base 10
- ASCII
- **Binary**
- Hexadecimal

Explanation:

Open Source NetFlow Analysis Tools

The number of open source NetFlow monitoring and analysis software packages is on the rise. You can use these open source tools to successfully identify security threats within your network. Here are a few examples of the most popular open source NetFlow collection and analysis toolkits:

- NFDump (sometimes used with NfSen or Stager)
- SiLK
- ELK

NFDump is a set of Linux-based tools that support NetFlow Versions 5, 7, and 9. You can download NFDump from <http://nfdump.sourceforge.net> and install it from source. Alternatively, you can easily install NFDump in multiple Linux distributions such as Ubuntu using `sudo apt-get install nfdump`.

Routers, firewalls, and any other NetFlow-enabled infrastructure devices can send NetFlow records to NFDump. The command to capture the NetFlow data is `nfcapd`. All processed NetFlow records are stored in one or more binary files. These binary files are read by NFDump and can be displayed in plaintext to standard output (stdout) or written to another file. [Example 11-13](#) demonstrates how the `nfcapd` command is used to capture and store NetFlow data in a directory called `netflow`. The server is configured to listen to port 9996 for NetFlow communication.

171. A zombie process occurs when which of the following happens?

- A process holds its associated memory and resources but is released from the entry table.
- A process continues to run on its own.
- A process holds on to associated memory but releases resources.
- **A process releases the associated memory and resources but remains in the entry table.**

Explanation:

- A zombie process is a process that releases its associated memory and resources but remains in the entry table.

172. Early versions of the Microsoft PPTP virtual private network software used the same RC4 key for the sender and the receiver. Which attack is the network vulnerable to when a stream cipher like RC4 is used twice with the same key?

- forgery attack
- meet-in-the-middle attack
- **ciphertext-only attack**
- plaintext-only attack

Explanation: Early versions of Microsoft's PPTP virtual private network software used the same RC4 key for the sender and the receiver (later versions solved this problem but may still have other problems). In any case where a stream cipher like RC4 is used twice with the same key, it is open to ciphertext-only attack.

173. How does NTP help with security monitoring?

- **It synchronizes the time of day so that you can correlate events when you receive system logs.**
- It enables you to look up the IP addresses a browser navigated to using the FQON.
- It allows you receive system-generated email traffic from log servers.
- It uses TCP, which allows you to see the HTTP conversations between servers and clients.

174. Which hash algorithm is cryptography used in certificate generation?

- SHA-256
- **MD5**
- RSA 4096
- SHA-512

175. Which description is an example of whaling?

- when attackers use fraudulent websites that look like legitimate ones
- **when attackers go after the CEO**
- when attackers target specific individuals
- when attackers target a group of individuals

176. Which tool provides universal query access to text based data such as event logs and file system?

- service viewer
- **log parser**
- handles
- Windows Management Instrumentation

Explanation: Log parser is a powerful, versatile tool that provides universal query access to text-based data such as log files, XML files and CSV files, as well as key data sources on the Windows? operating system such as the Event Log, the Registry, the file system, and Active Directory?

177. You have deployed an enterprise-wide host/endpoint technology for all of the company corporate PCs. Management asks you to block a selected set of applications on all corporate PCs. Which technology is the best option?

- antivirus/antispyware software
- **application whitelisting/blacklisting**
- host-based IDS
- network NGFW

178. What does the sum of the risks presented by an application represent for that application?

- **application attack surface**
- security violation
- vulnerability
- HIPPA violation

179. The FMC can share HTML, PDF and CSV data types that relate to a specific event type. Which event type?

- host
- connection
- **intrusion**
- NetFlow