1. Which two Linux commands can be used to display currently active processes? (Choose two answers)

□ netstat

□ tcpdump

□ top

□ ifconfig

□ proc

2/2 points

2. What command can you use to determine the MAC address of a Linux-based machine? (Choose one answer)

○ ipconfig

○ ifconfig

○ getmac

○ intmac

1/1 point

3. What three are valid permissions under Linux? (Choose three answers)

□ read

□ shared

□ execute

□ no permissions

□ full control

3/3 points

4. What two Linux commands can be used for pattern matching and filtering of output? (Choose two answers)

□ cat

□ echo

□ find

□ grep

□ more

1/2 points

The more command allows you to quickly view a text file or any section of it. You can also search for a text pattern using the more command using the forward slash and entering an expression to search for. The grep command can use a multitude of pattern matching techniques to filter results.

5. In what two directory locations are non-OS software installed on Linux machines? (Choose two answers)

□ /bin

□ /home

□ /lib

□ /opt

□ /usr/local

2/2 points

6. What is the purpose of the 'sudo' command in Linux? (Choose one answer)

○ Provides a stateful 'undue' of the previous command.

○ Enters the administrator or superuser command mode.

○ Configures the pseudowire interface on Linux machines.

○ Allows a logged in user to run Linux commands as the administrator.

1/1 point

7. Where are user-specific passwords stored in a Linux OS? (Choose one answer)

○ /etc/password

○ /etc/shadow

○ /usr/local

○ /usr/password

1/1 point

8. What command is used to verify disk capacity of Linux hosts? (Choose one answer)

○ chkdsk

○ df

○ du

○ hwinfo

1/1 point

9. What does the linux command 'tar -cvf' do? (Choose one answer)

○ Activates task management and recovery tools.

○ Terminates active running processes specificed by the user.

○ Creates an archive from a set of files without verification.

○ Mounts terminal access ports for use by the Linux kernel.

1/1 point

10. Which command is used to view the contents of a directory within Linux? (Choose one answer)

○ cat

○ df

○ dir

○ ls

1/1 point

11. What function does Snort perform on Linux machines? (Choose one answer)

○ File scanning for malware and virus infections.

○ Simple Network Object management.

○ Real-time traffic analysis and packet logging in IP networks.

○ Simple messaging system for Linux system alerts.

1/1 point

12. What Linux command is used to verify the host network configuration? (Choose one answer)

○ biff

○ cat /etc/hosts

○ ifconfig

○ netconf

1/1 point

13. What three are characteristics of MAC addresses? (Choose three answers)

□ MAC addresses are used to forward packets in LAN switches.

□ MAC addresses are used by routers to build routing tables and make routing decisions.

□ The first three byes are the OUI which identifies the manufacturer of the network interface card.

□ Dynamic MAC addresses are assigned by DHCP.

□ MAC addresses are unique across the global internet.

2/3 points

Lan switches forward based on port to MAC address mappings. OUI is first 24 bits and is called the OUI or organizational unique identiier. Dynamic MAC addresses are assigned by DHCP. MAC addresses are globally unique which is different from IP addresses which are not necessarily unique.

14. How many hosts can be assigned to the 192.168.100.0/24 network? (Choose two answers)

□ 24

□ 100

□ 192

□ 254

1/2 points
With 24 bits of subnetting there are 8 bits of host which is 2^8 or 256. You must remote the zero network and broadcast leaving 254 possible host addresses.

15. What is the purpose of a subnet mask in IPv4 addressing? (Choose one answer)

○ To help hosts determine the gateway address to send non-local packets to.

○ It masks the network in the IPv4 address allowing hosts to know their assigned host address.

○ It masks the IPv4 address to determine the all 1's or broadcast address.

○ It helps determine which portion of an IPv4 address represents the network.

0/1 point
The subnet mask is used in a bitwise AND operation with the IP Address to determine the network portion of the IPv4 address.

16. What three are information stored in routing tables? (Choose three answers)

□ A mapping of layer 2 MAC addresses to layer 3 IP addresses.

□ A metric or cost associated with a particular network destination.

□ A list of outgoing interfaces to reach a particular network destination.

□ A list of MAC addresses used to forward packets onto their next-hop destinations.

□ A list of destination networks.

2/3 points
Routers calculate the costs of each path to network destinations so that optimal routing decisions can be made about what paths provide the best route to network destinations. The routing table contains an ordered list of best paths to known networks. The routes may have originated from either the assignment of IP addresses to router interfaces (i.e., the connected routes and the local routes, static routes entered manually by an administrator or learned routes obtained by sharing routes via a routing protocol).

17. What three are types of routes typically found on Cisco routers? (Choose three answers)

□ connected

□ dynamic

□ hybrid

□ source

□ static

2/3 points

Subnets directly connected to a router interface are added to the router's routing table if they are configured with an ip address and in the admin up state. Dynamic routes are routes that are dynamically learned by routers through a routing protocol. A static route is a route created manually by a network administrator.

18. What are three IP address ranges considered routable private address space? (Choose three answers)

□ 10.0.0.0 - 10.255.255.255

□ 127.0.0.1 - 127.255.255.255

□ 172.16.0.0 - 172.31.255.255

□ 192.168.1.0 - 192.168.255.255

□ 224.0.0.0 - 239.255.255.255

3/3 points

19. What two are used for Network Address Translation (NAT)? (Choose two answers)

□ NAT allows 48-bit MAC addresses to be properly mapped into 32-bit IP multicast addresses.

□ NAT allows mapping between Public IP addressing and specific ports so that external hosts can reach inside hosts on specific ports.

□ NAT is Network Address Translation and it is typically used so that public addresses can be assigned on the internal LAN.

□ It enables private IP networks that use unregistered IP addresses to connect to the Internet.

□ NAT allows two different networks using the same network address space to communicate without readdressing hosts.

0/2 points

"NAT allows one or many hosts to share a single public IP address for routing on to the Internet. When many to one NAT is used it is sometimes referred to as Overload. NAT allows users to map a goup of network addresses into a different network address. This use case is most common when two companies or location merge into a single IP network scheme and have independently elected to implement the same address scheme."

20. What is Port Address Translation (PAT) used for? (Choose one answer)

○ One-to-One IP address mapping

○ Many-to-Many IP address mapping

○ Many-to-One IP address mapping

○ One-to-Many IP address mapping

1/1 point

21. What is the decimal equivalent of the binary number 11100000? (Choose one answer)

○ 32

○ 128

○ 224

○ 240

1/1 point

22. What is the function of Virtual Local Area Networks (VLANs)? (Choose one answer)

○ VLANs allow hosts with private IP address to communicate with devices on the Internet.

○ VLANs are used to segment a switch into multiple logical switches and broadcast domains.

○ VLANs are used to create loop-free layer 2 networks.

○ VLANs are used to forward layer two packets between hosts connected to layer 2 switches.

1/1 point

Virtual Local Area Networks (VLANs) are used to segment a switch into multiple logical switches and broadcast domains.

23. Which protocol is used to eliminate layer 2 loops? (Choose one answer)

○ Address Resolution Protocol (ARP)

○ Dynamic Host Configuration Protocol (DHCP)

○ Spanning Tree Protocol (STP)

○ Transmission Control Protocol (TCP)

○ 802.1Q Protocol

1/1 point

24. What is a Default Gateway? (Choose one answer)

○ The default IP address of a local host

○ The IP address of last resort

○ Another name for DHCP server

○ The service that resolves names to IP addresses.

0/1 point

The Default Gateway is the IP address used by an interface as the last resort to send traffic to when no route is known by the host.

25. Which two statements regarding Public and Private IP addressing are correct? (Choose two answers)

□ 224.45.1.1 is a private IP address

□ Private IP addresses can start with 192.168.x.x

□ Private IP addresses are registered

□ Public IP addresses are registered

□ Private IP addresses are not routable

2/2 points

26. What is the binary equivalent of the decimal number 183? (Choose one answer)

○ 10110011

○ 10110111

○ 11010111

○ 11001001

1/1 point

27. Which three are fields contained in an IPv4 header (RFC 791)? (Choose three answers)

□ Destination MAC Address

□ Time To Live

□ Source IP Address

□ Source Port

□ Sequence Number

□ Header Checksum

2/3 points

The Time To Live, or TTL, is one of the 13 fields in the IPv4 Header. This field is used to insure undeliverable packets are discarded. Both the source and destination IP addresses are included in the IPv4 header.

28. What are two features of IPSec? (Choose two answers)

□ Establishes VPN connectivity

□ Authenticates each packet in a data flow

□ Allows encryption the IP header

□ Establishes Secure Shell (SSH) connections

□ Facilitates data link-layer security such as Transport Layer Security (TLS)

1/2 points

IPSec supports VPN connectivity with encryption of IP header and payload, or only the payload, between hosts, using public key exchange protocols. IPSec provides an authentication facility for IP Packets.

29. At which OSI layer does TCP operate? (Choose one answer)

○ data link

○ network

○ session

○ transport

1/1 point

30. What are two uses of DNS? (Choose two answers)

□ Enables use of Private IP addresses when accessing the Internet

□ Used to resolve a Mac address from an IP address

□ Used to resolve domain names from IP addresses

□ Used to resolve IP addresses from domain names

□ Used to dynamically assign IP addresses to hosts

2/2 points

31. What type of incorrect security alert can result from non-malicious activity being seen as malicious? (Choose one answer)

○ True positive

○ False positives

○ False Negative

○ True negative

1/1 point

32. Which of the following is an example of a false negative? (Choose one answer)

○ Anti-virus detects malware on a nonthreatening application

○ The IDS does not identify a buffer overflow

○ A user is locked out after mistyping the password too many times

○ The alarm system is triggered by a book falling off the desk

1/1 point

33. Cache Poisoning is most commonly associated with which protocols? (Choose two answers)

□ NTP

□ ARP

□ DNS

□ NCP

2/2 points

34. Which of the following design components are used to isolate network devices such as web servers? (Choose one answer)

○ A Layer 2 Switch

○ VPN

○ NAT

○ DMZ

1/1 point

35. Which of the following would be used as a secure substitute for Telnet? (Choose one answer)

○ SSH

○ SFTP

○ SSL

○ HTTPS

1/1 point

36. Which of the following could result from a successful attack? (Choose one answer)

○ DoS

○ DNS

○ POP3

○ WINS

1/1 point

37. Which Internet Protocol encrypts and decrypts user page requests, as well as the pages that are returned by a web server using SSL/TLS? (Choose one answer)

○ NNTP

○ FTP

○ HTTP

○ HTTPS

1/1 point

38. Which best describes Least Privilege? (Choose one answer)

○ The minimum number of IP addresses required to construct a DNS server

○ Entry level certificate for security professionals

○ A policy limiting access to resources required for a task

○ An ACL limiting access to only classified data

1/1 point

39. Which of the following is the best example of Defense-In-Depth? (Choose one answer)

○ All enterprise host devices use private IP addresses

○ All enterprise applications leverage TCP and UDP for client sessions

○ An enterprise Firewall and use of private IP addresses

○ An enterprise Firewall and host anti-virus applications

○ An enterprise IDS and use of private IP addresses

1/1 point

40. What is a PIN? (Choose one answer)

○ A Personal Identification Number

○ Performance Infrastructure broken

○ Automated software tools that 'Probe Interior Network' vulnerabilities

○ Private addressing Integration

○ A level 16 access privilege

1/1 point

41. What is the difference between a Firewall and an IDS? (Choose the best answer)

○ A Firewall is used to prevent Malware from entering a network, while an IDS drops Malware packets

○ Firewalls are used to prevent UDP connections, and an IDS is used to prevent TCP connections

○ A Firewall is an active, inline device and an IDS is a passive device that is often installed on a network tap or spanning port

○ Firewalls are used to prevent TCP connections, and an IDS is used to prevent UDP connections

○ Firewalls are only used in the DMZ, while an IDS is only used in the data center

1/1 point

42. What is IP spoofing? (Choose one answer)

○ When you change the file extension to get past malware inspection

○ When you translate a MAC address into an IP address

○ Altering source IP address to evade detection

○ Altering destination IP address to evade detection

○ Using a public IP address to represent a private IP address

1/1 point

43. What is Phishing? (Choose one answer)

○ A process where legitimate administrators perform penetration testing

○ A defensive mechanism network administrators use to identify mobile users

○ The process used to insert malware into a networking device

○ An email-based attack used to compromise hosts through distribution of infected files or links to infected sites

○ An in-depth analysis of a compromised host

1/1 point

44. What is Malware? (Choose one answer)

○ Another name for broken network hardware

○ A file that contains destructive executable code

○ An HTTP feature that prevents web sites from accepting connections from malicious HTTP servers

○ Code that monitors malicious web connections and issues warnings

○ TCP connections that stop responding when a service stops running

1/1 point

45. Which service is used to Authenticate users? (Choose one answer)

○ NTP

○ DHCP

○ TACACS

○ ARP

○ STP

1/1 point

46. Which of the following is an example of a "Brute Force" attack? (Choose one answer)

○ The simplest form of attack against a site using repetitive login attempts and rotating usernames and passwords

○ A finely crafted attack that results in physical damage to a host

○ Any attack that results in physical damage to a server

○ A sweep of all open connections to a host followed by a spoofed disconnect for each connection

1/1 point

47. What is used to uniquely identify known Malware? (Choose one answer)

○ The combination of file name and extension are the key identification elements for Malware

○ A hash-based algorithm run against a suspected malware file with the results compared to a database of known malware

○ The source IP address that sent the suspected malware file

○ Detonation of the suspected malware file in a sandbox is the only way to uniquely identify malware

○ There is no way to uniquely identify suspected malware files

0/1 point

A hash-based algorithm run against a suspected malware file with the results compared to a database of know malware.

48. What differentiates a Next Generation Firewall (NGFW) from a standard Firewall (FW)? (Choose one answer)

○ A standard firewall does not maintain a TCP state table

○ A standard firewall looks at OSI layers 2-5; a NGFW looks at layers 3-4

○ A NGFW supports multiple domains; a standard FW only supports one domain

○ Only Cisco markets NGFWs; any other brand is a FW

○ A standard FW looks at OSI layers 3-4; a NGFW looks at more information including the application layer protocol commands.

1/1 point

49. True or False. It is considered a best security practice to place a login banner on Cisco switches and routers using the "banner" command.

○ TRUE

○ FALSE

0/1 point

The answer is false.

50. Which of the following Windows commands can be used to see processes that are running and the TCP port that is being used as well? (Choose one answer)

○ psinfo

○ net session

○ ipconfig

○ netstat

1/1 point

51. What protocol can you use on a Windows machine to allow for secure remote access? (Choose one answer)

○ Bash

○ CMD

○ RSH

○ SSH

○ Telnet

1/1 point

52. As a security administrator for your Windows networked environment, you have been notified that your systems might have been breached by malware that has modified entries in the HOSTS file. Which service can be affected by this breach? (Choose one answer)

○ ARP

○ DNS

○ LMHOSTS

○ NetBIOS

0/1 point

Windows will do a domain name lookup in the local Host file prior to performing a DNS lookup.

53. Which protocol commonly provides the underlying secure authentication in a Windows Active Directory environment? (Choose one answer)

○ Kerberos

○ LDAP

○ RADIUS

○ TACACS+

1/1 point

54. You are tasked with changing the password policy across all Windows PCs in the company? Which would be the BEST way for performing this task with the least amount of overhead? (Choose one answer)

○ Certificate revocation

○ Key escrow

○ Group policy

○ Security group

1/1 point

55. You receive a call that a Windows-based computer is infected with malware and is running too slowly to boot and run a malware scanner. Which of the following is the BEST way to run the malware scanner? (Choose one answer)

○ Kill all system processes

○ Enable the firewall

○ Boot from CD/USB

○ Disable the network connection

1/1 point

56. What is the minimal security access level normally required to add or modify application programs on a Windows PC? (Choose one answer)

○ Administrator

○ Guest

○ Operator

○ User

1/1 point

57. What utility should be used to access the registry on a Windows 7 PC? (Choose one answer)

○ edit

○ hexedit

○ ifconfig

○ msconfig

○ regedit

1/1 point

58. What command is used to open a command line interpreter within Windows? (Choose one answer)

○ cmd

○ putty

○ shell

○ term

1/1 point

59. How do you switch between logged-in user accounts in Windows 7? (Choose one answer)

○ Choose Start -> All Programs -> Switch User

○ Reboot

○ Windows 7 does not support multiple users

○ ctl-alt-del, then choose 'Switch User'

1/1 point

60. How can you determine the last date and time a Windows application file was modified? (Choose three answers)

□ Run 'dir' from the command line

□ Right click on the file name in a directory, and choose properties

□ View file details within a directory

□ Open the associated application and view the file from within the application

2/3 points

There are several ways to view file modification dates using built in file management tools.

61. Performance Monitor (PerfMon) is used for what in the Windows 7 OS? (Choose one answer)

○ To log inbound TCP connection performance

○ To monitor system and program performance

○ To manage user access and permissions which can negatively impact system performance

○ To set memory limits for hosted services

1/1 point