UPGRADE YOUR SKILL

IT SECURITY PRACTICE TEST QUESTIONS

1. You have setup a new ACL to block FTP, SSH, and Telnet traffic. After implementing the ACL on a single interface, you notice that network connectivity went down. Why might that be? Select the best answer.

A. The ACL was accidentally configured to block DNS traffic.
B. SSH and Telnet are necessary for simple network connectivity.
C. The ACL has an implicit 'permit all' rule at the end, but you forgot to set the 'permit' bit to '1.'
D. The ACL has an implicit 'deny all' rule at the end.

---

2. What is the name for a subnet that is external to the organization's network and usually sits *in front* of the firewall (instead of behind it), and typically cannot access internal resources? Choose the best answer.

A. OpenVPN
B. LAN
C. Extranet
D. DMZ
E. STP

---

3. In the IP address and subnet mask combination 192.168.3.1/23, what is the subnet number, and is the subnet a public or private subnet?

A. 192.168.2.0/23, private subnet
B. 192.168.2.0/23, public subnet
C. 192.168.3.0/23, private subnet
D. 192.168.3.0/23, public subnet
E. 192.168.0.0/23, private subnet
G. 192.168.0.0/23, public subnet

4.Which of the following are common a loopback addresses? Select all that apply.

A. 127.0.0.254
B. 127.127.0.1
C. 127.0.0.254
D. 127.0.0.1
E. 192.168.1.1
G. 10.0.0.1

---

5. Which of the following are packet capture technologies (which are sometimes called packet sniffers or protocol analyzers)? Select all that apply.

A. Wireshark
B. NMAP
C. Netstumbler
D. TCPdump

---

6. What technology solution allows someone to use a broadband Internet connection to make phone calls that would have been traditionally been completed using POTS (Plain Old Telephone System)? Choose the best answer.

A. H2H
B. GRE
C. IPv6
D. VoIP
E. VoFR

---

7. If you wanted to use the same CPU, RAM, and hardware resources to run multiple instances of different servers, which technology would you use? Choose the best answer.

A. IP address masking
B. RAID
C. Virtualization
D. Virtual drives

---

8. Which of the following IP addresses is associated with a /30 mask, and how many usable IP addresses are there on the same subnet?

A. 192.168.1.0 255.255.255.252, two usable addresses on this subnet
B. 192.168.1.0 255.255.252.0, four usable addresses on this subnet
C. 192.168.1.0 255.252.0.0, two usable addresses on this subnet
D. 192.168.1.0 252.0.0.0, four usable addresses on this subnet
E. 192.168.1.0 255.255.255.255, two usable addresses on this subnet

---

9. When files and background processes are stored in special directories separated from critical system files and denied access to the file system, what is this process known as?

A. Killing a virus
B. Preventing a Trojan
C. Freezing file permissions
D. Quarantining potentially harmful programs

---

10. What is the term for a group of computer systems, which aren't necessarily connected to the same layer 2 device, that still can communicate with broadcasts? Choose the best answer.

A. Broadcast storm
B. Quarantine zone
C. Virtual demarcation point
D. VLAN

---

11. Which of the following technologies can essentially make a host's true IP address invisible, by first changing header information in the IP packet before sending it to a layer 3 device for routing?

A. NAT
B. ACL
C. MAC address spoofing
D. VLAN hopping

---

12. What technique will check critical host system details before permitting access to the local network? For instance, what would the term be used to block hosts from accessing the local network without first updating the latest operating system patches?

A. Role-based ACL
B. NAC
C. PPTP
D. Single sign-on
E. Network layer security

---

13. Which one of the following answers describes a technology that allows a business to purchase servers and IT technology as a service, rather than needing to physically purchase and operate the devices on their own?

A. Cloud computing
B. Virtualization
C. Virtual computing
D. Man-in-the-middle computing

---

14. Which one of the following types of IPsec encryption secures the header information *as well as* the payload data? Choose the best answer.

A. Normal mode
B. Payload mode
C. Tunnel mode
D. Encryption mode

---

15. What types and varieties of computing systems can be the target of phreaking? Choose the best answer.

A. Phone systems
B. Virtual systems
C. Cloud services
D. VPN tunnel connections

---

16. Which of the following protocols or technologies is frequently used to monitor, maintain, and configure hosts that have network access? Choose the best answer.

A. SMTP
B. PPTP
C. Ping (ICMP echo/echo reply)
D. NMAP
E. SNMP

---

17. Select all of the following protocols and technologies that don't send data in an encrypted format. That is, select the options that send data in an ***unencrypted*** format.

A. Telnet
B. PPTP
C. TFTP
D. FTP
E. SSH
G. IPsec

---

18. Which of the following protocols or technologies, if any, improved upon Telnet by adding encryption to prevent compromised usernames and passwords that were stolen during transit to the destination host?

A. IPv4
B. GRE
C. L2TP
D. IKEv2
E. SSH
G. LDAP

---

19. What does the acronym AAA actually stand for? Choose all that apply.

A. Accounting, authorization, and addressing
B. Abstracting, authorization, and authentication
C. Accounting, authorization, and authentication
D. Accounting, adjudication, and addressing
E. Abstraction, authorization, and addressing

20. Which of the following protocols makes it easier for humans to remember where web resources are located by creating an alias for IP addresses?

A. NAT
B. DNS
C. PPTP
D. SNMP
E. SMTP
G. SSH

1.
Correct answer: D.

Explanation: Access Control Lists will block all traffic due to an invisible and inherent default 'deny all' rule that serves as the final action should previous rules not find a matching case. Unless you explicitly configure a 'permit all' rule, the ACL will block all traffic that doesn't match previous rules.

2.
Correct answer: D.

Explanation: A DMZ, or a Demilitarized Zone, is a subnet that is separated from the rest of an organization's internal resources. It is usually setup to securely host public servers so that the general public doesn't have access to internal subnets.

3.
Correct answer: A.

Explanation: The 192.168.3.1 IP address belongs to the 192.168.2.0/23 subnet. Notice that in the host address's third octet, the value is '3.' However, the last bit of that octet is excluded from the network portion of the address, since it uses a /23 mask. Also, the RFC 1918 private address specifications indicate that this range is a private subnet.

4.
Correct answer: D.

Explanation: 127.0.0.1 is simply the best choice. Note that some technologies and operating systems will allow you to custom configure any loopback address of your choice. However, the default is most often 127.0.0.1. You can ping that address from a command prompt or terminal windows on an operating system to verify that the network and TCP/IP are working properly.

5.
Correct answer: A, C, D.

Explanation: NMAP is the only option that isn't a packet sniffer. All other options can intercept and analyze network traffic.

6.
Correct answer: D.

Explanation: Voice over IP is the only technology listed above that allows someone to make a voice call using a broadband Internet connection. However, Voice over Frame Relay is a genuine protocol, though it isn't often used. The other options were simply unrelated protocols.

7.
Correct answer: C.

Explanation: Virtualization is the process of abstracting operating systems from the hardware that runs them. Technologies like VMWare allow a single physical computer to run multiple operating systems simultaneously on 'virtual machines.' The remaining answers were not valid, though virtual drives are subset of virtualization technologies. Hence, C is the best answer.

8.
Correct answer: A.

Explanation: Option A is the only one that correctly writes out a /30 subnet mask. Remember that a mask can only be 32 bits long, so only the last two bits are available for addressing – which leaves a total of four possible addresses. However, the first address is the network address, and the highest-order address (192.168.1.3) is the subnet's broadcast address. This only leaves two addresses valid for assignment as follows: 192.168.1.1 and 192.168.1.2. It is fairly typical to use /30 masks on WAN connections such as two PPP hosts.

9.
Correct answer: E.

Explanation: This is simply the definition of quarantining files on a computer. The idea is to detect them as soon as possible and to thwart malware before it has a chance to escalate its privileges or harm the host system.

10.
Correct answer: D.

Explanation: VLAN stands for Virtual Local Area Network Connection. One of it's key defining features is the ability to group hosts into separate broadcast domains, even though they may be physically connected to other switches. VLANs are often used to segment computers into functional groups to increase security and prevent packet capture attacks.

11.
Correct answer: A.

Explanation: NAT stands for Network Address Translation, and it's main purpose is to slow down the exhaustion of IPv4 addresses by allowing one public IP address to be used by multiple private addresses. Though there are many types of NAT, they all function by swapping out the IP address in the packet header for another, and once again translating the address for traffic in the reverse direction.

12.
Correct answer: B.

Explanation: NAC stands for Network Access Control, and it involves a large collection of best practices designed to increase network security by deny clients who don't meet certain criteria.

13.
Correct answer: A.

Explanation: Cloud computing is the latest evolution of the Internet. Before we used more of a client/server model, and before that we used mainframes and thin-clients to share data with other hosts.

14.
Correct answer: C.

Explanation: IPsec encrypts both the payload and header when it operates in tunnel mode. However, when it operates in payload mode, the header information isn't encrypted. The remaining two options aren't valid IPsec tunneling options.

15.
Correct answer: A.

Explanation: Phreaking is another form of hacking, whereby the attacker usually tries to break a system to make calls for free. As such, phreaking attacks typically target phone equipment.

16.
Correct answer: D.

Explanation: SNMP, or the Simple Network Management Protocol, is often used to maintain systems across vast networks. In fact, some software services that use SNMP (such as Solarwinds) can apply scripts to entire groups of networking devices to simply management.

17.
Correct answer: A, C, D.

Explanation: Telnet, TFTP, and FTP don't do anything to secure or encrypt data. As such, that data can easily be intercepted and read by a hacker or nosy eavesdropper. SSH, IPsec, and PPTP all use encryption technologies to secure data.

18.
Correct answer: E.

Explanation: SSH was created to overcome the shortcomings of Telnet – mainly by adding encryption to protect login credentials.

19.
Correct answer: C.

Explanation: AAA is a security and auditing methodology used to construct high level network policies and best practices.

20.
Correct answer: B.

Explanation: DNS, or Domain Name System, translates between hard to remember IP addresses and human-readable textual strings.