Name _____ Date _____

Module 3 - Network Security Concepts

Enterprise Networking, Security, and Automation– Semester 3

Student Version

Module 3 Sections:

Required Materials:

Reading Organizer

Packet Tracer Activities: None

Labs: None

Module's 3 - 5 Exam

Page intentionally left blank.

Points_____ / __263___

Name_____ Date _____

Module 3
Reading Organizer
Instructor Version

Note: The Reading Organizer has weighted scoring. Any question with the word **explain**, **define, or describe** in it is expected to have a longer answer and is worth two points each.

After completion of this module, you should be able to:

- Describe the current state of cybersecurity and vectors of data loss.
- Describe tools used by threat actors to exploit networks.
- Describe malware types.
- Describe common network attacks.
- Explain how IP vulnerabilities are exploited by threat actors.
- Explain how TCP and UDP vulnerabilities are exploited by threat actors.
- Explain how IP services are exploited by threat actors.
- Describe best practices for protecting a network.
- Describe common cryptographic processes used to protect data in transit.

3.1 Current State of Cybersecurity

1. Describe the following security terms.

a. Assets –

b. Vulnerability –

c. Threat –

d. Exploit –

e. Mitigation –

f. Risk –

2. Describe what an attack vector is.

3. Explain what a DoS attack is.

4. _____is likely to be an organization's most valuable asset.

5. List common data loss vectors.

a.

b.

c.

d.

e.

f.

3.2 Threat Actors

6. The terms white hat hacker, black hat hacker, and gray hat hacker are often used to describe a type of hacker. Write in the description of each type of hacker.

a. White Hat Hackers -

b. Gray Hat Hackers –

c. Black Hat Hackers –

7. The term threat actor includes hackers, but what else does it include?

8. Describe modern hacking terms shown below.

a. Script Kiddies –

b. Vulnerability Broker –

c. Hacktivists –

d. Cyber criminals –

e. State-Sponsored –

9. What are two examples of hacktivist?

a.

b.

3.3 Introduction to Attack Tools

10. Match the following terms to their definitions

a. Fuzzers to Search Vulnerabilities
b. Password Crackers
c. Vulnerability Scanners
d. Vulnerability Exploitation Tools
e. Wireless Hacking Tools
f. Packet Crafting Tools
g. Network Scanning and Hacking Tools
h. Encryption Tools
i. Debuggers
j. Hacking Operating Systems
k. Forensic Tools
l. Rootkit Detectors
m. Packet Sniffers

_____ These tools are used to capture and analyze packets within traditional Ethernet LANs or WLANs. Tools include Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy, and SSLstrip.

_____ Password cracking tools are often referred to as password recovery tools and can be used to crack or recover a password. This is accomplished either by removing the original password, after bypassing the data encryption, or by outright discovery of the password. Password crackers repeatedly make guesses in order to crack the password. Examples of password cracking tools include John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack, and Medusa.

_____ These are specially designed operating systems preloaded with tools optimized for hacking. Examples of specially designed hacking operating systems include Kali Linux, Knoppix, BackBox Linux.

_____ These tools scan a network or system to identify open ports. They can also be used to scan for known vulnerabilities and scan VMs, BYOD devices, and client databases. Examples of tools include Nipper, Secunia PSI, Core Impact, Nessus v6, SAINT, and Open VAS.

_____ These tools are used to probe and test a firewall's robustness using specially crafted forged packets. Examples include Hping, Scapy, Socat, Yersinia, Netcat, Nping, and Nemesis.

_____ Encryption tools use algorithm schemes to encode the data to prevent unauthorized access to the encrypted data. Examples of these tools include VeraCrypt, CipherShed, OpenSSH, OpenSSL, Tor, OpenVPN, and Stunnel.

_____ Wireless hacking tools are used to intentionally hack into a wireless network to detect security vulnerabilities. Examples of wireless hacking tools include Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep, and NetStumbler.

_____ Network scanning tools are used to probe network devices, servers, and hosts for open TCP or UDP ports. Examples of scanning tools include Nmap, SuperScan, Angry IP Scanner, and NetScanTools.

_____ These tools identify whether a remote host is vulnerable to a security attack. Examples of vulnerability exploitation tools include Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Netsparker.

_____ Fuzzers are tools used by threat actors to discover a computer's security vulnerabilities. Examples of fuzzers include Skipfish, Wapiti, and W3af.

_____ These tools are used by white hat hackers to sniff out any trace of evidence existing in a computer. Example of tools include Sleuth Kit, Helix, Maltego, and Encase.

_____ These tools are used by black hats to reverse engineer binary files when writing exploits. They are also used by white hats when analyzing malware. Debugging tools include GDB, WinDbg, IDA Pro, and Immunity Debugger.

_____ This is a directory and file integrity checker used by white hats to detect installed root kits. Example tools include AIDE, Netfilter, and PF: OpenBSD Packet Filter.

11. Threat actors can use attack tools, or a combination of tools, to create attacks. Write in the correct name for each attack shown below.

_____ If a threat actor obtains a secret key, that key is referred to as a compromised key. A compromised key can be used to gain access to a secured communication without the sender or receiver being aware of IP the attack.

_____ This attack occurs when threat actors have positioned themselves between a source and destination. They can now actively monitor, capture, and control the communication transparently.

_____ A threat actor constructs an IP packet that appears to originate from a valid address inside the corporate intranet.

_____ If threat actors discover a valid user account, the threat actors have the same rights as the real user. Threat actors could use that valid account to obtain lists of other users, network information, change server and network configurations, and modify, reroute, or delete data.

_____ This is when a threat actor captures and "listens" to network traffic. This attack is also referred to as sniffing or snooping.

_____ A DoS attack prevents normal use of a computer or network by valid users. A DoS attack can flood a computer or the entire network with traffic until a shutdown occurs because of the overload. A DoS attack can also block traffic, which results in a loss of access to network resources by authorized users.

_____ A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet.

_____ If threat actors have captured enterprise traffic, they can alter the data in the packet without the knowledge of the sender or receiver.

3.4 Malware

12. _____ are particularly prone to malware attacks

13. Viruses hide by attaching themselves to computer code, software, or documents on the computer. When opened, the virus executes and infects the computer. List what viruses can do.

a.

b.

c.

d.

e.

14. Describe what the modern viruses listed below are developed to do.

a. Boot sector virus –

b. Firmware virus –

c. Macro virus –

d. Program virus –

e. Script virus –

15. There are several types of Trojan horses shown below. Write in the correct name for each one.

_____ Trojan horse enables unauthorized file transfer services on end devices.

_____ Trojan horse provides the threat actor with sensitive data, such as passwords.

_____ Trojan horse actively attempts to steal confidential information, such as credit card numbers, by recording key strokes entered into a web form.

_____ Trojan horse slows or halts network activity.

_____ Trojan horse corrupts or deletes files.

_____ Trojan horse enables unauthorized remote access.

_____Trojan horse will use the victim's computer as the source device to launch attacks and perform other illegal activities.

_____ Trojan horse stops antivirus programs or firewalls from functioning.

16. Write one detail or characteristic about each of the different types of malware listed below.

a. Adware –

b. Ransomware –

c. Rootkit –

d. Spyware –

e. Worm –

3.5 Common Network Attacks

17. List the three types of attacks that networks are susceptible to.

a.

b.

c.

18. What is reconnaissance?

19. List some of the techniques used by malicious threat actors to conduct reconnaissance attacks.

a.

b.

c.

d.

e.

20. Access attacks exploit known vulnerabilities in _____, _____, and _____.

21. Threat actors use _____on network devices and computers to retrieve data, gain access, or to escalate access privileges to administrator status.

22. Describe a password attack.

23. Describe a spoofing attack.

24. List and describe the access attack listed below.

a. _____ –

b. _____ –

c. _____ –

d. _____ –

25. Describe social engineering attacks.

26. Identify the following social engineering attacks.

_____ Also known as junk mail, this is unsolicited email which often contains harmful links, malware, or deceptive content.

_____ A threat actor creates a targeted phishing attack tailored for a specific individual or organization.

_____ A threat actor pretends to need personal or financial data to confirm the identity of the recipient.

_____ Sometimes called “Quid pro quo”, this is when a threat actor requests personal information from a party in exchange for something such as a gift.

_____ A threat actor sends fraudulent email which is disguised as being from a legitimate, trusted source to trick the recipient into installing malware on their device, or to share personal or financial information.

_____ This is where a threat actor inconspicuously looks over someone's shoulder to steal their passwords or other information.

_____ A threat actor leaves a malware infected flash drive in a public location. A victim finds the drive and unsuspectingly inserts it into their laptop, unintentionally installing malware.

_____ This type of attack is where a threat actor pretends to be someone they are not to gain the trust of a victim.

_____ This is where a threat actor rummages through trash bins to discover confidential documents.

_____ This is where a threat actor quickly follows an authorized person into a secure location to gain access to a secure area.

27. The _____(SET) was designed to help white hat hackers and other network security professionals create social engineering attacks to test their own networks.

28. Enterprises must educate their _____about the risks of social engineering, and develop strategies to validate identities over the phone, via email, or in person.

29. List the recommended social engineering protection practices.

a.

b.

c.

d.

e.

f.

g.

h.

30. List and describe the two major types of DoS attacks.

a. _____–

b. _____–

3.6 IP Vulnerabilities and Threats

31. List and describe the following IP related attacks.

a. _____–

b. _____–

c. _____–

d. _____–

e. _____–

32. Threat actors use ICMP for reconnaissance and scanning attacks. If an information-gathering attack is launched what types of information can they gather?

a.

b.

c.

d.

33. Threat actors often use amplification and reflection techniques to create DoS attacks. Explain both of these attacks.

a. Amplification –

b. Reflection –

34. Newer forms of amplification and reflection attacks such as _____ and amplification attacks and _____ amplification attacks are now being used.

35. Describe what happens when an IP address spoofing attacks occur.

36. Spoofing attacks can be non-blind or blind. Describe both types of attacks.

a. Non-blind spoofing –

b. Blind spoofing –

37. When are MAC address spoofing attacks used?

3.7 TCP and UDP Vulnerabilities

38. List and describe the services TCP provides.

a. _____–

b. _____–

c. _____–

39. Describe the three steps used to establish a TCP connection.

1.

2.

3.

40. The _____exploits the TCP three-way handshake.

41. What can a TCP reset attack be used to do?

42. UDP is a _____ transport layer protocol.

43. UDP has a much lower overhead than TCP because it is not connection-oriented. What is it not doing that TCP does?

44. What happens in a UDP flood attack?

3.8 IP Services

45. Explain what an ARP request is.

46. What is a "gratuitous ARP"?

47. Why will a host send a "gratuitous ARP"?

48. ARP cache poisoning can be used to launch various _____ attacks.

49. List the possible DNS attacks.

a.

b.

c.

d.

50. What does it mean when a DNS server is called an open resolver?

A DNS open resolver answers queries from clients outside of its administrative domain.

51. List the vulnerabilities of a DNS open resolver.

a.

b.

c.

d.

52. Explain what a DNS domain shadowing attack does.

53. How do DNS tunneling attacks work?

54. What do DHCP server do?

55. Describe what happens during a DHCP spoofing attack?

56. What type of misleading information can a rouge server provide clients?

a.

b.

c.

3.9 Network Security Best Practices

57. List and describe the CIA information security triad.

a. _____–

b. _____–

c. _____–

58. Most organizations employ a _____ approach to security. This is also known as a layered approach.

59. List the security devices and services that can be implemented to protect an organization's users and assets against TCP/IP threats.

a.

b.

c.

d.

60. What is a firewall?

61. List some of the common properties all firewall share.

a.

b.

c.

62. What is one benefit of using a firewall in a network?

63. What is one limitation present in firewalls?

64. IDS and IPS technologies detect patterns in network traffic using signatures. Explain what a signature is.

65. The Cisco WSA combines advanced _____ protection, _____ and _____, _____ policy controls, and reporting.

3.10 Cryptography

66. What are the four elements of secure communication?

a.

b.

c.

d.

67. _____ are used to ensure the integrity of a message.

68. List three well-known hash functions.

a.

b.

c.

69. What needs to happen to add authentication to integrity assurance.

70. There are two classes of encryption used to provide data confidentiality. Describe the characteristics of both.

Symmetric Encryption –

a.

b.

c.

d.

Asymmetric Encryption –

a.

b.

c.

d.

71. A _____, also called a _____, is known by the sender and receiver before any encrypted communications can take place.

72. List the well-known symmetric encryption algorithms.

a.

b.

c.

d.

d.

73. Asymmetric algorithms, also called _____, are designed so that the key that is used for encryption is different from the key that is used for decryption

74. Asymmetric algorithms use a public key and a private key. Both keys are capable of the encryption process, but the complementary paired key is required for _____.

75. Asymmetric algorithms are substantially _____ than symmetric algorithms.

76. _____ is an asymmetric mathematical algorithm where two computers generate an identical shared secret key without having communicated before.

77. List three examples of instances when DH is commonly used.

a.

b.

c.