Network Threats Summary

2.6.1

What Did I Learn in this Module?

Who is Attacking Our Network?
Understanding network security requires you to understand the following terms: threat, vulnerability, attack surface, exploit, and risk. Risk management is the process that balances the operational costs of providing protective measures with the gains achieved by protecting the asset. Four common ways to manage risk are risk acceptance, risk avoidance, risk reduction, and risk transfer. Hacker is a term used to describe a threat actor. White hat hackers are ethical hackers using their skills for good, ethical, and legal purposes. Grey hat hackers are individuals who commit crimes and do unethical things, but not for personal gain or to cause damage. Black hat hackers are criminals who violate computer and network security for personal gain, or for malicious reasons, such as attacking networks. Threat actors include script kiddies, vulnerability brokers, hacktivists, cybercriminals, and state-sponsored hackers. Many network attacks can be prevented by sharing information about IOCs. Many governments are promoting cybersecurity. CISA and NCSA are examples of such organizations.

Introduction of Attack Tools
Threat actors use a technique or tool. Attack tools have become more sophisticated, and highly automated. Many of the tools are Linux or UNIX based and a knowledge of these are useful to a cybersecurity professional. Tools include password crackers, wireless hacking tools, network security scanning and hacking tools, packet crafting tools, packet crafting tools, packet sniffers, rootkit detectors, fuzzers to search vulnerabilities, forensic tools, debuggers, hacking operating systems, encryption tools, vulnerability exploitation tools, and vulnerability scanners. Categories of attacks include eavesdropping attacks, data modification attacks, IP address spoofing attacks, password-based attacks, denial-of-service attacks, man-in the-middle attacks, compromised key attacks, and sniffer attacks.

Malware
Malware is short for malicious software or malicious code. Threat actors frequently try to trick users into installing malware to

help exploit end device vulnerabilities. Often antimalware software cannot be updated quickly enough to stop new threats. Three common types are virus, worm, and Trojan horse. A virus is a type of malware that spreads by inserting a copy of itself into another program. Most viruses are spread through USB memory drives, CDs, DVDs, network shares, and email. Trojan horse malware is software that appears to be legitimate, but it contains malicious code that exploits the privileges of the user that runs it. Often, Trojans are found on online games. Trojan horses are usually classified according to the damage they cause. Types of Trojan horses include remote-access, data-sending, destructive, proxy, FTP, security software disabler, DoS, and keylogger. Worms are similar to viruses because they replicate and can cause the same type of damage. Viruses require a host program to run. Worms can run themselves. Most worm attacks consist of three components: enabling vulnerability, propagation mechanism, and payload. Currently, ransomware is the most dominant malware. It denies access to the infected system or its data. The cybercriminals then demand payment to release the computer system. Other malware examples include spyware, adware, scareware, phishing, and rootkits.

Common Network Attacks – Reconnaissance, Access, and Social Engineering

Threat actors can also attack the network from outside. To mitigate attacks, it is useful to categorize the various types of attacks. The three major categories are reconnaissance, access, and DoS attacks. Reconnaissance is information gathering. Threat actors do unauthorized discovery and mapping of systems, services, or vulnerabilities. Recon attacks precede access or DoS attacks. Some of the techniques used include the following: performing an information query of a target, initiating a ping sweep of the target network, initiating a port scan of active IP addresses, running vulnerability scanners, and running exploitation tools. Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services. These attacks include password attacks, spoofing attacks, trust exploitation attacks, port redirections, man-in-the-middle attacks, and buffer overflow attacks. Social engineering is an access attack that attempts to manipulate individuals into performing unsafe actions or divulging confidential information. These attacks include pretexting, phishing, spear phishing, spam, something for something, baiting, impersonation, tailgating, shoulder surfing, and dumpster diving.

Network Attacks – Denial of Service, Buffer Overflows, and Evasion

DoS attacks create some sort of interruption of network services to users, devices, or applications. There are two major types: overwhelming quantity of traffic, and maliciously formatted packets. DDoS attacks are similar in intent to DoS attacks, except that the DDoS attack increases in magnitude because it originates from multiple, coordinated sources. The following terms are used to describe DDoS attacks: zombies, bots, botnet, handlers, and botmaster. Mirai is malware that targets IoT devices configured with default login information. Mirai uses a brute force dictionary attack. After successful access, Mirai targets the Linux-based BusyBox utilities that are designed for these devices. The goal of a threat actor when using a buffer overflow DoS attack is to find a system memory-related flaw on a server and exploit it. Exploiting the buffer memory by overwhelming it with unexpected values usually renders the system inoperable, creating a DoS attack. Many attacks use stealthy evasion techniques to disguise an attack payload. Evasion methods include encrypting and tunneling, resource exhaustion, traffic fragmentation, protocol-level misinterpretation, traffic substitution, traffic insertion, pivoting, rootkits, and proxies.

Module 2 - Network Threats Quiz

1. In what way are zombies used in security attacks?

- ( ) They probe a group of machines for open ports to learn which services are running.
- ( ) They are maliciously formed code segments used to replace legitimate applications.
- ( ) They are infected machines that carry out a DDoS attack.
- ( ) They target specific individuals to gain corporate or personal information.

2. What is an example of a local exploit?

- ( ) 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.
- ( ) Port scanning is used to determine if the Telnet service is running on a remote server.

3. Which two statements describe access attacks? (Choose two.)

- [ ] Trust exploitation attacks often involve the use of a laptop to act as a rogue access point to capture and copy all network traffic in a public location, such as a wireless hotspot.
- [ ] Buffer overflow attacks write data beyond the allocated buffer memory to overwrite valid data or to exploit systems to execute malicious code.
- [ ] Password attacks can be implemented by the use of brute-force attack methods, Trojan horses, or packet sniffers.
- [ ] Port redirection attacks use a network adapter card in promiscuous mode to capture all network packets that are sent across a LAN.

- [ ] To detect listening services, port scanning attacks scan a range of TCP or UDP port numbers on a host.

4. Why would a rootkit be used by a hacker?

- ( ) to reverse engineer binary files
- ( ) to gain access to a device without being detected
- ( ) to try to guess a password
- ( ) to do reconnaissance

5. Which statement describes the term attack surface?

- ( ) It is the group of hosts that experiences the same attack.
- ( ) It is the network interface where attacks originate.
- ( ) It is the total number of attacks toward an organization within a day.
- ( ) It is the total sum of vulnerabilities in a system that is accessible to an attacker.

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

- ( ) risk reduction
- ( ) risk retention
- ( ) risk sharing
- ( ) risk avoidance

7. What name is given to an amateur hacker?

- ( ) red hat
- ( ) black hat
- ( ) blue team
- ( ) script kiddie

8. What is the term used when a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source?

- ( ) backdoor
- ( ) phishing
- ( ) Trojan
- ( ) vishing

9. Which two characteristics describe a worm? (Choose two.)

- [ ] executes when software is run on a computer
- [ ] hides in a dormant state until needed by an attacker
- [ ] travels to new computers without any intervention or knowledge of the user
- [ ] is self-replicating
- [ ] infects computers by attaching to software code

10. A user receives a phone call from a person who claims to represent IT services and then asks that user for confirmation of username and password for auditing purposes. Which security threat does this phone call represent?

- ( ) DDoS
- ( ) anonymous keylogging
- ( ) social engineering
- ( ) spam

11. 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?

- ( ) resource exhaustion
- ( ) pivoting
- ( ) traffic substitution
- ( ) protocol-level misinterpretation

12. In what type of attack is a cybercriminal attempting to prevent legitimate users from accessing network services?

- session hijacking
- address spoofing
- DoS
- MITM

Check

Show Me

Reset

2.5 Network Attacks - Denial of Service, Buffer Overflows, ...

3.0 Introduction

Network Security