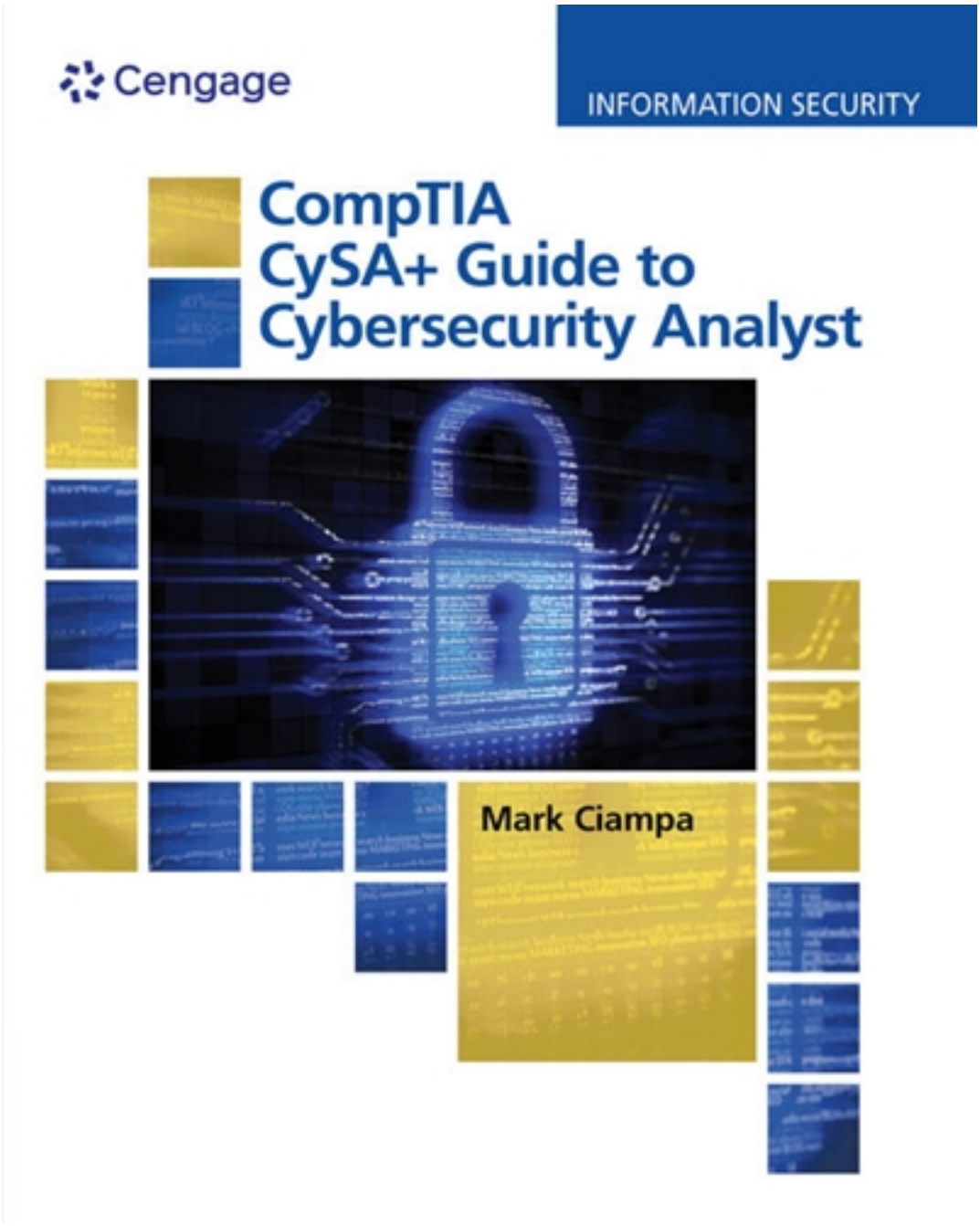
Solutions for CompTIA CySA 1st Edition by Ciampa

CLICK HERE TO ACCESS COMPLETE Solutions



Solutions

Module 1

Applying Environmental Reconnaissance

At a Glance

Instructor's Manual Table of Contents

Lecture Notes

Overview

This module explains the various forms of reconnaissance within the context of cybersecurity—for example, environmental reconnaissance, user reconnaissance, and network reconnaissance. The module also describes some common tasks of reconnaissance to establish and maintain security. Finally, the module identifies relevant networks and tools used in reconnaissance.

Objectives

After completing this module, students will be able to:

- Define environmental reconnaissance
- Explain common tasks in user and network reconnaissance
- Identify different types of networks
- Describe the tools used for reconnaissance

Teaching Tips

Introduction

1. List some of the statistics that illustrate the threat of malware and other cyberattacks.
2. Explain that a new certification is available to help security professionals learn and hone their skills: the Computing Technology Industry Association (CompTIA) Cybersecurity Analyst, or CySA+ for short.

Reconnaissance Procedures and Common Tasks

1. Mention that military terms are often used in cybersecurity. For example:
   - A war game is a training exercise for military operations.
   - Reconnaissance is information gathering to determine an enemy's strengths and weaknesses before engaging in combat.
2. Explain that an important first step in threat management is applying the concepts of war games and reconnaissance into what is known as environmental reconnaissance.
3. Tell students that by simulating the actions of an attacker, an organization tries to understand its environment and determine what information a threat actor can gather using reconnaissance procedures.

User Reconnaissance and Exploitation

1. Explain that a threat actor's ability to gather information about particular users, such as managers in an organization or technical professionals, can be a key to a successful attack.

2. Note that the ability to compromise a key user can provide a wider opening to executing an attack than compromising an employee with relatively few privileges.
3. Point out that two techniques of user reconnaissance are:
   - Collecting web information
   - Harvesting email addresses
4. Explain that collecting web information is a passive procedure: Attackers accumulate information that is external to a company's protected information without making direct contact with the user.
5. Note that two common techniques for collecting web information are social media profiling and harvesting email addresses.
6. Explain the concept of social media profiling. It's the process of gathering information about a person from social media sites such as Twitter and Instagram to construct a profile that a threat actor can use.
   - Aspects of the profile can include the person's work history, family, background, interests, hobbies, and skills.
   - A threat actor can use people search engines to search social media sites, business web pages, blogs, and news sources for information on an individual target.
7. Explain that threat actors can also use automated tools to harvest email addresses when collecting web information.
8. Point out that once user information has been collected, it can be employed to exploit the users. Two types of user exploitation are:
   - Social engineering attacks
   - Phishing attacks
9. Tell students that social engineering is a way to actively gather information for an attack by deceiving users into revealing the information. It relies on the weaknesses of individuals—most notably, their fear of failure or the desire to please others.
10. List the principles of social engineering for students:
    - Authority—Impersonation of an authority figure or falsely citing their authority
    - Intimidation—An attempt to frighten and coerce by threat
    - Consensus—An attempt to influence based on the alleged actions of others
    - Scarcity—The implication that action is important because a quantity is in short supply
    - Urgency—A demand of immediate action because time is in short supply
    - Familiarity—An attempt to curry favor by asserting that the intended victim is well-known and well-liked
    - Trust—A projection of self-confidence that the threat actor can be believed

11. List some methods that threat actors use during social engineering to gain trust:
    - For example, they provide specific information or tell specific lies to make their interactions seem legitimate.
    - They project confidence.
    - They use evasion and diversion.
    - They use humor to put people at ease.
12. Explain that one of the most common forms of social engineering is phishing: sending an email or displaying a web announcement that claims to be from a legitimate party in an effort to trick users into surrendering private information.
    - Mention that one form of phishing, known as spear phishing, targets specific users with customized messages to make the communication seem legitimate.
    - Tell students that a particular form of spear phishing, called whaling, targets "big fish" within an organization—wealthy individuals or executives who might have large sums of money in a bank account that a threat actor could access in a successful attack.

Teaching Tip	For a variety of links that provide more information on social engineering, go to https://www.techtarget.com/search/query?q=social+engineering.

Network Reconnaissance

1. Point out that gathering information about users is just one step of environmental reconnaissance. Another step is collecting information about an organization's network, which is known as network reconnaissance.
2. Explain that a good way to understand network reconnaissance is to first learn about its goals and then to learn about its methods.

Network Reconnaissance Goals

1. Tell your students that the three primary goals of network reconnaissance are topology discovery, service discovery, and operating system (OS) fingerprinting.
2. Explain that just as geographical maps can be illustrated as three-dimensional topologies, a network topology refers to a layout of physical or virtual network devices and how the components communicate with each other.
3. Define the concept of topology discovery, which is a key goal of a threat actor. It describes an attempt to uncover the layout of an internal network so that an attacker can identify its weak points.+
4. Define service discovery, which is an attempt to determine which services are running on a network.
    - Most communication in TCP/IP networks involves the exchange of information between a service (a.k.a., a program, application, or process) running on one system and the same service or corresponding application running on a remote system.
    - TCP/IP uses a numeric value known as a port number to identify the services and applications on these systems.

5. Explain that OS fingerprinting is a way for threat actors to identify an OS through the use of methods that run on specific computers so they can determine which vulnerabilities to exploit.
6. Point out to students that OSs are a key target of attack for various reasons:
   - As more features are added to OSs, their complexity increases, and so do their vulnerabilities.
   - New attack tools can target OS functions and services that were once considered secure.
   - Numerous settings in OSs can fine-tune user privileges, but there are so many settings that it is easy to overlook one and open the door for a threat a+ctor.
   - Any delay in applying an OS patch or update may result in an attacker exploiting an unpatched vulnerability.
7. Explain that OSs come in many types, all of which might require slightly different means of protection:
   - A network OS is software that runs on a network device like a firewall, router, or switch.
   - A server OS is operating system software that runs on a network server to provide resources to network users.
   - A workstation OS is software that manages hardware and other software on a client computer.
   - An appliance OS works in firmware to manage a specific device like a digital video recorder or video game console.
   - A kiosk OS is system and user interface software for an interactive kiosk.
   - A mobile OS is used to run mobile phones, smartphones, tablets, and other handheld devices.

Network Reconnaissance Methods

1. Tell your students that three methods for performing network reconnaissance include capturing packets, reviewing network device information, and harvesting DNS.
2. Explain that capturing packets as they travel across a network can provide valuable information about the devices attached to the network—for example, topology discovery, service discovery, and OS fingerprinting can all be performed by capturing packets.
3. Discuss the point that it is difficult for an outsider to capture packets; the threat actor usually needs physical access to a network, which requires access within a protected building.
4. Point out that several network devices have valuable information that attackers can use in network reconnaissance:
   - A network-based firewall screens packets based on specific criteria, making it essentially a packet filter.
   - A router is a network device that can forward packets across different computer networks.

- Routers can perform a security function by using an access control list (ACL)—a set of rules that acts like a "network filter" to permit or restrict data flowing into and out of the router network interfaces.

5. Explain that the environmental reconnaissance of Domain Name System (DNS) information is called DNS harvesting. Because DNS is the basis for domain name resolution of names to IP addresses—a very important role—DNS can be the focus of attacks, and it can be used to provide valuable network information to threat actors.
6. List the ways that DNS harvesting is typically done:
   - WHOIS—This is a TCP/IP query/response protocol for accessing information about Internet resources, most notably domain names and IP addresses as well as internal contact information for websites.
   - Zone transfers—These transfers are exchanges of information among DNS servers; a poorly configured DNS server could allow threat actors to receive the information in it.
   - Network administration tools—Several of these command-line tools can be used to attempt to receive zone transfers or get basic information about the path a packet takes from its source.

Quick Quiz 1

1. _____ is the process of gathering information about a person from one or more social media sites to construct a "sketch" of that person.

   Answer: Social media profiling

2. Which of the following is not a common use of an automated email harvesting tool?
   a. Discover the address of specific titles of individuals, such as the CEO of a company
   b. Verify the email address of an individual user
   c. Send email under false pretenses to solicit information from a selected victim
   d. Find the email addresses for a list of employees

   Answer: C

3. Which of the following is not a principle that is exploited in social engineering?
   a. Intimidation
   b. Scarcity
   c. Desperation
   d. Urgency

   Answer: C

4. True or False: Topology discovery is an attempt to uncover the layout of an internal network, which is a key goal of a threat actor.

   Answer: True

5. What is the term for sending an email or displaying a web announcement that falsely claims

to be from a legitimate enterprise in an attempt to trick the user into surrendering private information?

Answer: Phishing

Identifying Different Network Types

1. Explain that different network types, sometimes called variables, can have an impact on network security; for example, the vulnerabilities of a wired network are different from those of a wired network.
2. List the four pairs of different network types:
   - Wireless vs. wired
   - Virtual vs. physical
   - Internal vs. external
   - On-premises vs. cloud

Wireless versus Wired Networks

1. Explain that early computer networks were known as wired networks because the devices were connected through cables, or wires, while a modern network that uses radio frequency (RF) or light waves as the transmission medium is called a wireless network.
2. Discuss the point that wired networks have some basic vulnerabilities, such as a networked computer that a user might leave unattended, but wireless networks have more potential vulnerabilities.
3. Explain that a wired network has only one data entry point, but signals from wireless access points (APs) create several data entry points into the network through which threat actors can inject attacks or steal data.
4. Explain further that a wired network is protected by the physical boundaries of a building, but a wireless network has no such protection: A threat actor sitting in a car outside a building's security perimeter can still eavesdrop on wireless data transmissions or inject malware behind the firewall. If an AP's security settings have not been set or are not well-configured, threat actors can access the network.

Virtual versus Physical Networks

1. Discuss the point that physical servers have been replaced in many cases by virtualization, which is a means of managing and presenting computer resources by function without regard to their physical layout or location.
2. Point out that one example of virtualization is host virtualization, in which an entire operating system environment is simulated.
3. List some of the security concerns of host virtualization:
   - A hypervisor manages the operating systems of virtual machines (VMs), but not all hypervisors have the necessary security to defend against threat actors.

- Security tools such as antivirus programs and antispam tools were designed for single physical servers and do not always adapt well to multiple virtual machines.
- VMs must be protected both from outside networks and from other VMs on the same physical computer; in other words, one VM can infect another.
- VMs may be able to "escape" from the contained environment and directly interact with the host operating system, which makes it important to have VM escape protection so that a VM cannot infect the host OS.
- It is easy to create virtual machines, which has led to the problem of VM sprawl—the widespread proliferation of VMs without proper oversight or management.

Internal versus External Networks

1. Explain that it is not a good idea to locate public-facing servers such as web and email servers inside the secure internal network: In such cases, a threat actor must only break through the server's security to access the secure network.
2. Explain that most networks use an external demilitarized zone (DMZ) to give untrusted outside users access to resources such as web servers.

On-Premises versus Cloud Networks

1. Tell students that online cloud networks have gained widespread use as an alternative to traditional on-premises networks, in which organizations purchase all the hardware and software necessary to run their operations.
2. List the three primary service models used in cloud computing:
   - Software as a Service (SaaS)—The cloud computing vendor provides access to its own software applications running on a cloud infrastructure; these applications can be accessed through a web browser and do not require any installation, configuration, or management by the user.
   - Platform as a Service (PaaS)—Consumers can use the PaaS model to install and run their own specialized applications on the cloud, but they do not manage or configure any of the cloud infrastructure.
   - Infrastructure as a Service (IaaS)—This model gives customers the most control; they can deploy and run their own software, including operating systems and applications, and they have some control over operating systems and storage.

Tools for Reconnaissance

1. List the different tools that can be used in an environmental reconnaissance: packet analyzers, intrusion detection and prevention systems, tools for viewing logs, vulnerability scanners, and command-line network utilities that are part of basic operating systems.

Packet Analyzers

1. Remind students that, as mentioned previously, capturing packets that travel across a network can provide valuable information about the devices attached to the network.
2. Discuss packet analyzers, which are useful tools for environmental reconnaissance because they can be used to identify protocols that are running but are prohibited, to identify attacks, and to determine if unencrypted data is being transmitted.
3. Remind students that topology discovery, service discovery, and OS fingerprinting can all be performed by capturing packets.

Intrusion Detection and Prevention Systems

1. Explain that an intrusion detection system (IDS) is a device used to detect an attack as it occurs; an IDS can also be useful for an environmental reconnaissance.
2. Explain that IDSs come in several forms:
   - An inline IDS is connected directly to the network and monitors the flow of data as it occurs.
   - A passive IDS is connected to a port on a switch, which receives a copy of network traffic.
   - A host-based intrusion detection system (HIDS) is a software-based application that runs on a local host computer and can detect an attack as it occurs.
   - A network intrusion detection system (NIDS) watches for attacks on the network and uses sensors to gather information and report back to a central device.
   - An intrusion prevention system (IPS) monitors to detect malicious activities, as an IDS does, and it also attempts to prevent them by stopping the attack.
   - A network intrusion prevention system (NIPS) is similar to an active NIDS in that it monitors network traffic to immediately react to block a malicious attack by following established rules.
   - A host-based intrusion prevention system (HIPS) works like the IPSs described above, but for individual hosts.

Vulnerability Scanners

1. Explain that a vulnerability scanner is actually a generic term for a range of products that look for different vulnerabilities in networks or systems.

2. Mention to students that a vulnerability scanner identifies all the devices connected to the network, including computing devices (servers, desktops, and laptops), network devices (firewalls, switches, etc.), and even virtual machines.
3. Tell students that once the scanner has identified the devices, it creates an inventory, performs OS fingerprinting to identify the operating system running on each device, and then checks each item in the inventory against databases of known vulnerabilities to determine if a device has a vulnerability.

Viewing Logs

1. Explain that almost all network devices have logs to automatically record any events that occur, and that these logs can be valuable in keeping a network secure.
2. List some of the items that would be recorded and examined in a firewall rule-based log:
   - IP addresses that are being rejected and dropped
   - Probes to ports that have no application services running on them
   - Source-routed packets
   - Suspicious outbound connections
   - Unsuccessful logins
3. Explain that log management can present some problems, including multiple devices generating logs, a very large volume of data, different log formats, and different devices recording log information in different formats.
4. Mention that a solution to the problems of log management is syslog, a universal standard for system messages; virtually all network technology supports the ability to send syslog messages, and messages from different network devices can be sent to a centralized server for review.

Network Utilities

1. Explain that a command-line utility called netstat (network statistics) provides detailed information about current network connections; it is included in almost all operating systems and provides network protocol statistics as well as network connections for the Transmission Control Protocol (TCP), network interfaces, and routing tables.
2. Point out that when you are conducting reconnaissance, netstat can be useful for discovering remote connections to running services.
3. List some operating system tools besides netstat that can be useful in reconnaissance:
   - ipconfig (ifconfig in Linux)—Internet Protocol configuration (ipconfig) is a tool that displays TCP/IP network connection data, such as the IP address, subnet mask, and default gateway for all network adapters. It also displays DNS information.
   - tracert (traceroute in Linux)—This tool can give basic information about the path that a packet takes.

- ping—This tool is a networking program to test whether a particular host can be reached.
- nslookup (dig in Linux)—The name server lookup tool can be used to obtain the IP address or domain name of a host.

4. Mention that a popular open-source utility for network discovery and security auditing is nmap (network mapper), which can determine what hosts are available on a network, what services the hosts are offering, and what types of packet filters or firewalls are in use.
5. Add that nmap can also be used for OS fingerprinting, discovering characteristics of a specific host computer (known as host scanning), and to quickly scan very large networks.
6. Mention that a graphical user interface (GUI) version of nmap called Zenmap is available; it can also be used for network mapping (creating a visual map of a network).

Quick Quiz 2

1. What is a hypervisor?

   Answer: A virtual machine's monitor program is called a hypervisor; it manages the virtual machine's operating systems.

2. Which of the following is not one of the recognized pairs of network types?

   a. Wireless vs. wired

   b. Static vs. dynamic

   c. Virtual vs. physical

   d. Internal vs. external

   Answer: B

3. _____ is a generic term for a range of products that look for different vulnerabilities in networks or systems.

   Answer: Vulnerability scanner

4. Which of the following is a networking program that tests whether a particular host can be reached?

   a. ifconfig

   b. tracert

   c. ping

   d. nslookup

   Answer: C

5. The name of the _____ tool is an abbreviation for "network mapper."

   Answer: nmap

Class Discussion Topics

1. Have the class research social engineering in more detail (for example, using the web links below), and then have class members engage in role-playing exercises in which one student portrays the perpetrator of a social engineering attack and another student portrays the selected victim.
2. Ask the class to do online research of social media profiling, and then select a student who is willing to have a profile developed by the rest of the class. Have the class work together to develop the selected student's profile and then discuss the results.

Additional Projects

1. Have students discuss what types of organizations might gain a competitive advantage by focusing on information security.
2. Have students design some simple components of a war game that might be used to test the security of a small organization.

Additional Resources

Note that the following sites were active at the time of this writing. If a link is no longer active, have students use the keywords to find new links.

1. Defenses against Social Engineering
   https://www.tripwire.com/state-of-security/security-awareness/5-tips-against-social-engineering/
2. Social Engineering Links
   https://www.techtarget.com/search/query?q=social+engineering
3. Performing Reconnaissance
   https://www.sciencedirect.com/topics/computer-science/performing-reconnaissance
4. Cybersecurity TED Talks
   https://www.springboard.com/blog/12-must-watch-cybersecurity-ted-talks/
5. Social Engineering
   https://www.csoonline.com/article/2124681/what-is-social-engineering.html
6. Intrusion Detection and Prevention Systems
   https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

Key Terms

For explanations of key terms, see the "Key Terms" section of the module text.

- capturing packets
- cloud computing
- DNS harvesting
- environmental reconnaissance
- firewall rule-based log
- harvesting email addresses
- host scanning
- host-based intrusion detection system (HIDS)
- host-based intrusion prevention system (HIPS)
- intrusion detection system (IDS)
- intrusion prevention system (IPS)
- log
- netstat
- network intrusion detection system (NIDS)
- network mapping
- nmap
- OS fingerprinting
- packet analyzer
- phishing
- router/firewall ACL review
- service discovery
- social engineering
- social media profiling
- syslog
- topology discovery
- variables
- vulnerability scanner