Common Network Attacks - Reconnaissance, Access, and Social Engineering

2.4.1

Types of Network Attacks

Malware is a means to get a payload delivered. When it is delivered and installed, the payload can be used to cause a variety of network-related attacks from the inside. Threat actors can also attack the network from outside.

Why do threat actors attack networks? There are many motives including money, greed, revenge, or political, religious, or sociological beliefs. Network security professionals must understand the types of attacks used to counter these threats to ensure the security of the LAN.

To mitigate attacks, it is useful to first categorize the various types of attacks. By categorizing network attacks, it is possible to address types of attacks rather than individual attacks.

Although there is no standardized way of categorizing network attacks, the method used in this course classifies attacks in three major categories.

- Reconnaissance Attacks
- Access Attacks
- DoS Attacks

2.4.2

Reconnaissance Attacks

Reconnaissance is information gathering. It is analogous to a thief surveying a neighborhood by going door-to-door pretending to sell something. What the thief is actually doing is looking for vulnerable homes to break into, such as unoccupied residences, residences with easy-to-open doors or windows, and those residences without security systems or security cameras.

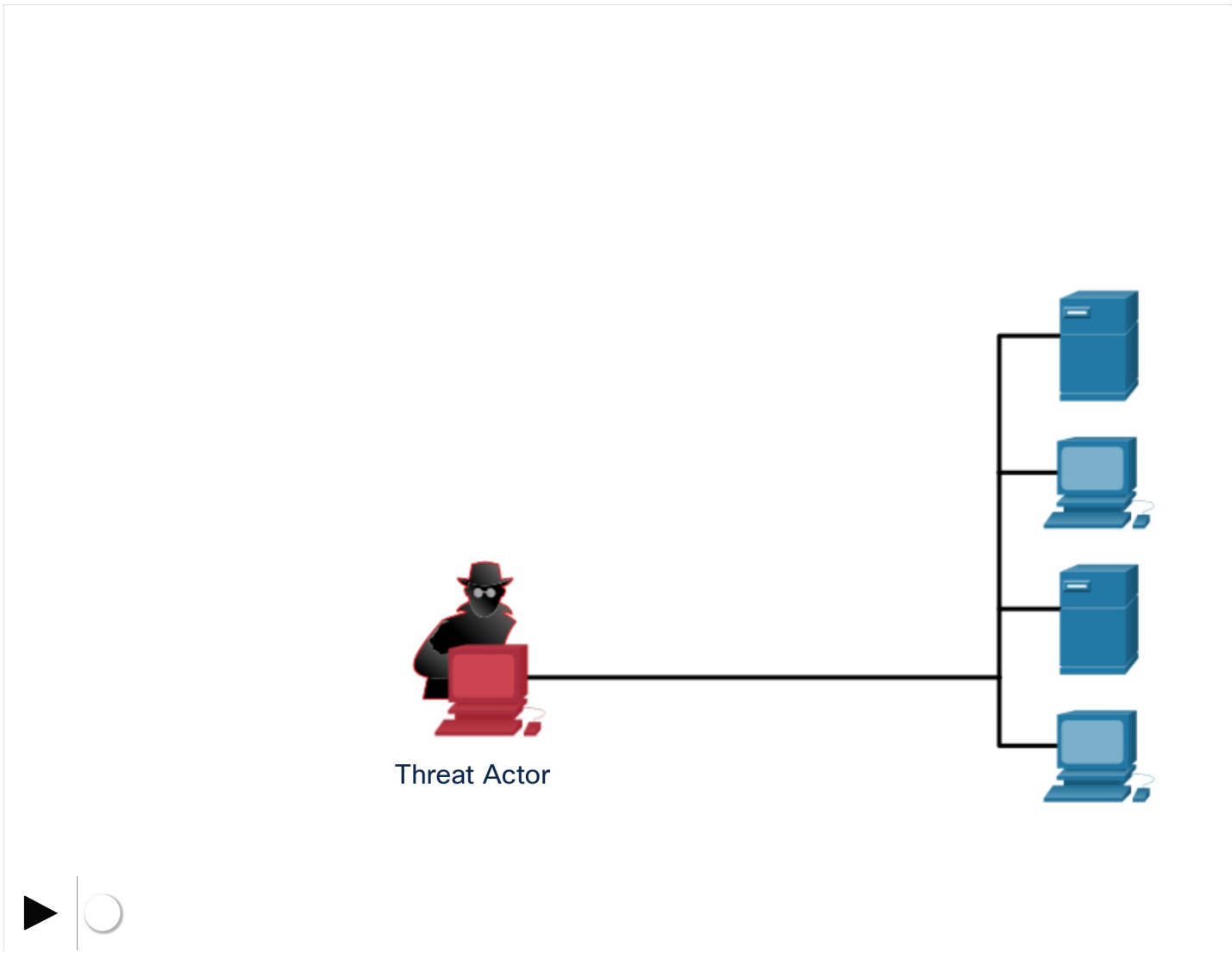
Threat actors use reconnaissance (or recon) attacks to do unauthorized discovery and mapping of systems, services, or vulnerabilities. Recon attacks precede access attacks or DoS attacks.

Some of the techniques used by malicious threat actors to conduct reconnaissance attacks are described in the table.

Technique	Description
Perform an information query of a target	The threat actor is looking for initial information about a target. Various tools can be used, including the Google search, organizations website, whois, and more.
Initiate a ping sweep of the target network	The information query usually reveals the target's network address. The threat actor can now initiate a ping sweep to determine which IP addresses are active.
Initiate a port scan of active IP addresses	This is used to determine which ports or services are available. Examples of port scanners include Nmap, SuperScan, Angry IP Scanner, and NetScanTools.
Run vulnerability scanners	This is to query the identified ports to determine the type and version of the application and operating system that is running on the host. Examples of tools include Nipper, Secuna PSI, Core Impact, Nessus v6, SAINT, and Open VAS.
Run exploitation tools	The threat actor now attempts to discover vulnerable services that can be exploited. A variety of vulnerability exploitation tools exist including Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Netsparker.

Click each button to view the progress of a reconnaissance attack from information query, to ping sweep, to port scan.

Click Play in the figure to view an animation of a threat actor using the whois command to find information about a target.



2.4.3

Video - Reconnaissance Attacks

2.4.4

Access Attacks

Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services. The purpose of this type of attack is to gain entry to web accounts, confidential databases, and other sensitive information.

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

Password Attacks

In a password attack, the threat actor attempts to discover critical system passwords using various methods. Password attacks are very common and can be launched using a variety of password cracking tools.

Spoofing Attacks

In spoofing attacks, the threat actor device attempts to pose as another device by falsifying data. Common spoofing attacks include IP spoofing, MAC spoofing, and DHCP spoofing. These spoofing attacks will be discussed in more detail later in this module

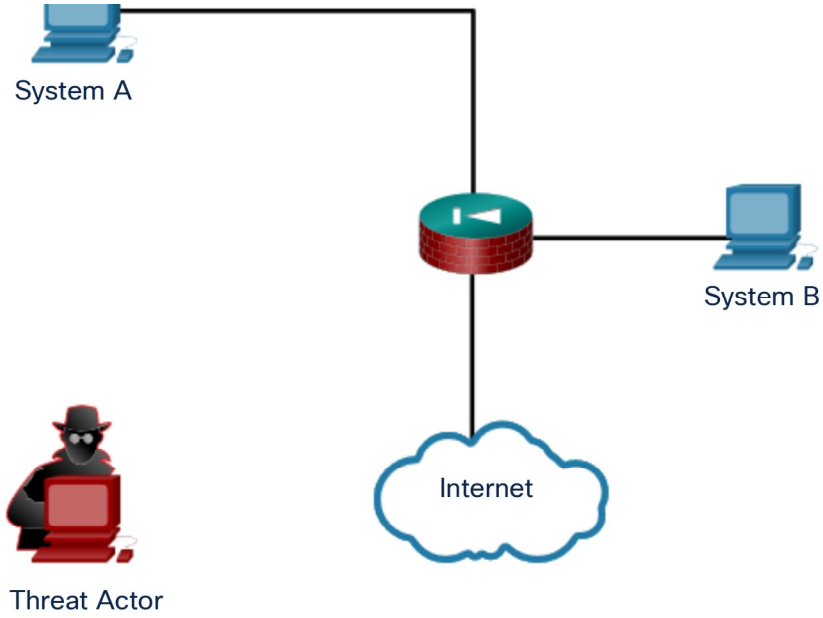
Other Access attacks include:

- Trust exploitations
- Port redirections
- Man-in-the-middle attacks
- Buffer overflow attacks

Click each button to view an illustration and explanation of these access attacks.

Trust Exploitation Example | Port Redirection Example | Man-in-the-Middle Attack Example | Buffer Overflow Attack

In a trust exploitation attack, a threat actor uses unauthorized privileges to gain access to a system, possibly compromising the target. Click Play in the figure to view an example of trust exploitation.



2.4.5

Video - Access and Social Engineering Attacks

2.4.6

Social Engineering Attacks

Social engineering is an access attack that attempts to manipulate individuals into performing actions or divulging confidential information. Some social engineering techniques are performed in-person while others may use the telephone or internet.

Social engineers often rely on people's willingness to be helpful. They also prey on people's weaknesses. For example, a threat actor could call an authorized employee with an urgent problem that requires immediate network access. The threat actor could appeal to the employee's vanity, invoke authority using name-dropping techniques, or appeal to the employee's greed.

Information about social engineering techniques is shown in the table.

Social Engineering Attack	Description
Pretexting	A threat actor pretends to need personal or financial data to confirm the identity of the recipient.
Phishing	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.
Spear phishing	A threat actor creates a targeted phishing attack tailored for a specific individual or organization.
Spam	Also known as junk mail, this is unsolicited email which often contains harmful links, malware, or deceptive content.
Something for Something	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.
Baiting	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.
Impersonation	In this type of attack, a threat actor pretends to be someone else to gain the trust of a victim.
Tailgating	This is where a threat actor quickly follows an authorized person into a secure location to gain access to a secure area.
Shoulder surfing	This is where a threat actor inconspicuously looks over someone’s shoulder to steal their passwords or other information.
Dumpster diving	This is where a threat actor rummages through trash bins to discover confidential documents.

The Social Engineer Toolkit (SET) was designed to help white hat hackers and other network security professionals create social engineering attacks to test their own networks. It is a set of menu-based tools that help launch social engineering attacks. The SET is for educational purposes only. It is freely available on the internet.

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

The figure shows recommended practices that should be followed by all users.

Recommended Social Engineering Protection Practices

2.4.7

Strengthening the Weakest Link

Cybersecurity is only as strong as its weakest link. Since computers and other internet-connected devices have become an essential part of our lives, they no longer seem new or different. People have become very casual in their use of these devices and rarely think about network security. The weakest link in cybersecurity can be the personnel within an organization, and social engineering a major security threat. Because of this, one of the most effective security measures that an organization can take is to train its personnel and create a “security-aware culture.”

2.4.8

Lab - Social Engineering

In this lab, you will research examples of social engineering and identify ways to recognize and prevent it.

Social Engineering

2.3 Malware

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