Mitigation Techniques

by Sophia

WHAT'S COVERED

In this lesson, you will learn about common tools and techniques used to attack networks and computer systems. We will also discuss general approaches to threat mitigation.

Specifically, this lesson will cover the following:

1. Attack Tools

Hackers use a wide variety of tools and techniques to compromise the confidentiality, integrity, and availability of computer systems and networks. We will discuss some of them in this tutorial.

1a. Packet Sniffers

A **packet sniffer** is a software tool that can be incredibly effective in troubleshooting a problematic network, but it can also be a hacker's friend. Here is how it works: A network adapter card is set to promiscuous mode so it will send all packets snagged from the network's Layer 1 (Physical) through to a special application to be viewed and sorted out. A packet sniffer can capture some highly valuable, sensitive data, including, but not limited to, passwords and usernames, making such a tool a prize among identity thieves.

Packet Sniffer

Software designed for checking packets of data transferred over the internet.

1b. Port Scanners

Another example of an attack tool is a **port scanner**. This tool includes programs that ping every port on the target to identify which TCP and UDP ports are open. It does this by pinging the IP address of the target with the port number appended after a colon. If an answer is received, the port is open. Open ports can lead to services the hacker can potentially exploit.

Port Scanner

A program that pings every port on the target to identify which TCP and UDP ports are open.

1c. FTP Bounce

An **FTP Bounce** is a variation of the port scan in that the attacker uses the FTP PORT command to request access to ports indirectly by using the victim machine as a middleman for the request. This cloaks the identity of the device performing the port scan.

FTP Bounce

A variation of the port scan in which the attacker uses the FTP PORT command to request access to ports indirectly by using the victim machine as a middleman for the request.

1d. Port Redirection

A **port redirection** requires a host machine the hacker has broken into and uses to redirect traffic that normally would not be allowed passage through a firewall. The attacker gains access to a trusted computer that is outside the firewall and installs software on the machine. They then redirect traffic bound for a particular port on the trusted but now-compromised host to their machine.

Port Redirection

Occurs when a hacker has broken into the host machine and uses it to redirect traffic that would normally not be allowed passage through a firewall.

1e. Trust Exploitation

Trust exploitation happens when someone exploits a trust relationship in your network. The attacker gains control of a host that is outside the firewall but is trusted by hosts that are inside the firewall. Once compromised, the host outside the firewall can be used as a platform to exploit the fact that it is trusted by those inside the firewall.

TERM TO KNOW

Trust Exploitation

An event when someone exploits a trust relationship in a network.

1f. Misconfigured Firewall

In many cases, security issues arise because of our mistakes rather than the efforts of hackers. Let's take a look at some of the most common misconfiguration errors and omissions.

If the access control lists are misconfigured on a firewall, the resulting damage will fall into one of three categories.

KEY CONCEPT

The damages can fall under one of the following categories:

- Traffic that should not be allowed is allowed.
- Traffic that should be allowed is blocked.
- No traffic is allowed at all.

The first two problems are a matter of specifying the wrong traffic type in a permit-or-deny rule. Because in many cases, the traffic type is specified in terms of a port number, it is critical to know the port numbers of the traffic you are dealing with.

The last problem can either be a simple omission or a complete misunderstanding of how access control lists (ACLs) work. At the end of every ACL is an implied rule that blocks all traffic that has not been allowed by earlier rules in the rule set. This means that all ACLs should have a rule at the end that allows all traffic that should be allowed. An ACL with no permit statements will block all traffic.

1g. Misconfigured ACLs/Applications

Misconfigured applications can also cause issues. Web applications that do not perform proper input validation can allow for attacks such as buffer overflows. In some cases, they can also allow for commands to be executed on the web server. For this reason, web-based applications should undergo strict **code review** and **fuzz testing**, and you should ensure that all input is validated before it is accepted by the application.

TERMS TO KNOW

Code Review

The practice, or an instance, of identifying and verifying the choice of algorithms, coding styles, and compliance with the software design.

Fuzz Testing

A testing methodology in which random data ("fuzz") is supplied as input to a program.

1h. Open/Closed Ports

Destination services and applications are specified in a packet by way of a port number. When a device is open to receiving a connection to a service or application, it is said to be listening on the corresponding port. Therefore, closing or disabling a port eliminates the possibility of a malicious user connecting to that port and leveraging any weakness that may be present with that service.

KEY CONCEPT

It is a standard device-hardening practice to close any ports not required for the proper functioning of a device based on its role in the network. For example, a DNS server should have no other ports open but port 53, which is used to service DNS.

1i. Unpatched Firmware/OSs

The best defense against the majority of malware types and attack modes is to keep up on all current updates. This includes operating system **patches**, **firmware** updates, and application updates. Many devices that fall prey to malware and attacks do so needlessly because a patch existed that would have prevented the attack. A formal update system should be in place to ensure that no updates fall through the cracks.

TERMS TO KNOW

Patch

A file that describes changes to be made to a computer file or files, usually changes made to a computer program that fix a programming bug.

Firmware

Something in between hardware and software. Like software, it is created from source code, but it is closely tied to the hardware it runs on.

1j. Social Engineering

Hackers are more sophisticated today than they were 10 years ago, but then, so are network administrators.

HINT

Because most system administrators today have secured their networks well enough to make it pretty tough for an outsider to gain access, hackers decided to try an easier route to gain information: they just asked the network's users for it.

Social engineering is the practice of tricking a user into giving, or giving access to, sensitive information, thereby bypassing most or all protection. Social engineers commonly attempt to illegally obtain sensitive information by pretending to be a credible source. Common social engineering tactics include sending emails,

making phone calls, or even starting up a conversation in person. End-user training is typically the best defense against social engineering.

TERM TO KNOW

Social Engineering

The practice of tricking a user into giving, or giving access to, sensitive information, thereby bypassing most or all protection.

1k. Phishing

Phishing is a malicious social engineering act of keeping a false website or sending a false email with the intent of masquerading as a trustworthy entity in order to acquire sensitive information, such as usernames, passwords, and credit-card details. Hackers sending out a mass email that appears as though the message actually came from a bank is a common phishing scam. The email typically indicates that the bank had an issue with one of its servers, so it now requires you to confirm your user-account information to verify that none of your data was lost. When the victim logs in to the lookalike website, the hackers capture the victim's username and password so that they can then use it themselves to commit identity theft.

BIG IDEA

Cybersecurity personnel need to understand the tools and techniques that attackers use so that they can design and implement strong defenses.

TERM TO KNOW

Phishing

A malicious social engineering act of keeping a false website or sending a false email with the intent of masquerading as a trustworthy entity in order to acquire sensitive information, such as usernames, passwords, and credit card details.

---

2. Understanding Mitigation Techniques

While it does not cover all mitigation techniques, this section focuses on methods that will truly protect users from being attacked in general. You will learn enough to make all but the most determined hackers give up on your network and search for easier prey.

Safe networking techniques fall into three major categories: policies and procedures, training, and patches and upgrades. But before we go there, let us cover some of those general defense techniques we just referred to.

KEY CONCEPT

The following are three main ways to detect an intruder and defend yourself against one:

- Active detection, which involves constantly scanning the network for possible break-ins
- Passive detection, which involves logging all network events to a file

- Proactive defense methods, which involve using tools to shore up your network walls against attacks

2a. Active Detection

Active detection is analogous to a security guard walking the premises, rattling doors to make sure they are locked, and checking for intruders and any unusual activity. Similarly, there is special network software that searches for hackers attempting known attack methods and scans for the kind of suspicious activity and weird network traffic that hackers leave behind as they travel through the network. Some sophisticated active systems go a step further and take action by doing things like shutting down the communications sessions a hacker is using as well as emailing or texting you.

2b. Passive Detection

Using video cameras is a good example of using a passive detection system. Their counterparts in networking are files that log events that occur on the network. Tripwire is one of the earliest programs of this variety. It identifies changes in files using checksums. Changes in files indicate that someone has accessed them. Passive detection systems work by examining files and data and then calculating the checksums for each. The checksums are stored in a log file so that if the system admin notices that a security breach has occurred on the network, they can access the log files to find clues about it.

2c. Proactive Defense

A proactive defense is something you do or implement to ensure that your network is impenetrable. You can accomplish a lot through solid research and vigilant maintenance, so you need to stay updated about any known security holes relevant to your type of network and the devices that populate it. You can also use tools like Nmap and Nessus to find the holes in your security walls and plug them with software patches.

BIG IDEA

Benjamin Franklin once said that “an ounce of prevention is worth a pound of cure”. That wisdom may be especially useful to cybersecurity professionals as they work to proactively secure computer systems and networks because recovering from a security incident is often extremely expensive.

SUMMARY

In this lesson, you learned about **attack tools** that are used to mitigate threats to the network. You also learned about other **mitigation techniques** using active/passive detection and proactive defense.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

Code Review

The practice, or an instance, of identifying and verifying the choice of algorithms, coding styles, and compliance with the software design.

FTP Bounce

A variation of the port scan in which the attacker uses the FTP PORT command to request access to ports indirectly by using the victim machine as a middleman for the request.

Firmware

Something in between hardware and software. Like software, it is created from source code, but it is closely tied to the hardware it runs on.

Fuzz Testing

A testing methodology in which random data (“fuzz”) is supplied as input to a program.

Packet Sniffer

Software designed for checking packets of data transferred over the internet.

Patch

A file that describes changes to be made to a computer file or files, usually changes made to a computer program that fix a programming bug.

Phishing

A malicious social engineering act of keeping a false website or sending a false email with the intent of masquerading as a trustworthy entity in order to acquire sensitive information, such as usernames, passwords, and credit card details.

Port Redirection

Occurs when a hacker has broken into the host machine and uses it to redirect traffic that would normally not be allowed passage through a firewall.

Port Scanner

A program that pings every port on the target to identify which TCP and UDP ports are open.

Social Engineering

The practice of tricking a user into giving, or giving access to, sensitive information, thereby bypassing most or all protection.

Trust Exploitation

An event when someone exploits a trust relationship in a network.