The case for securing networks

Let's start by answering the question, why do we need secure networks?
As you've learned, networks are constantly at risk of attack from malicious hackers.
Attackers can infiltrate networks via malware, spoofing, or packet sniffing.
Network operations can also be disrupted by attacks such as packet flooding.
As we go along, you're going to learn about these and
other common network intrusion attacks in more detail.

Protecting a network from these types of attacks is important.
If even one of them happens, it could have a catastrophic impact on an organization.
Attacks can harm an organization by leaking valuable or
confidential information.
They can also be damaging to an organization's reputation and
impact customer retention.
Mitigating attacks may also cost the organization money and time.

Over the last few years,
there have been a number of examples of damage that cyber attacks can cause.
One notorious example was an attack against the American home-improvement
chain, Home Depot, in 2014.
A group of hackers compromised and infected Home Depot servers with malware.
By the time network administrators shut down the attack, the hackers had already
taken the credit and debit card information for over 56 million customers.

Now, you know why it's so important to secure a network.
But to keep a network secure,
you need to know what kinds of attacks to protect it from.
Coming up, you'll learn about some common network attacks.

How intrusions compromise your system

In this section of the course, you learned that every network has inherent vulnerabilities and could become the target of a network attack.

Attackers could have varying motivations for attacking your organization’s network. They may have financial, personal, or political motivations, or they may be a disgruntled employee or an activist who disagrees with the company's values and wants to harm an organization’s operations.

Malicious actors can target any network. Security analysts must be constantly alert to potential vulnerabilities in their organization’s network and take quick action to mitigate them.

In this reading, you’ll learn about network interception attacks and backdoor attacks, and the possible impacts these attacks could have on an organization.

Network interception attacks

Network interception attacks work by intercepting network traffic and stealing valuable information or interfering with the transmission in some way.

Malicious actors can use hardware or software tools to capture and inspect data in transit. This is referred to as **packet sniffing**. In addition to seeing information that they are not entitled to, malicious actors can also intercept network traffic and alter it. These attacks can cause damage to an organization’s network by inserting malicious code modifications or altering the message and interrupting network operations. For example, an attacker can intercept a bank transfer and change the account receiving the funds to one that the attacker controls.

Later in this course you will learn more about malicious packet sniffing, and other types of network interception attacks: on-path attacks and replay attacks.

Backdoor attacks

A **backdoor attack** is another type of attack you will need to be aware of as a security analyst. An organization may have a lot of security measures in place, including cameras, biometric scans and access codes to keep employees from entering and exiting without being seen. However, an employee might work around the security measures by finding a backdoor to the building that is not as heavily monitored, allowing them to sneak out for the afternoon without being seen.

In cybersecurity, backdoors are weaknesses intentionally left by programmers or system and network administrators that bypass normal access control mechanisms. Backdoors are intended to help programmers conduct troubleshooting or administrative tasks. However, backdoors can also be installed by attackers after they’ve compromised an organization to ensure they have persistent access.

Once the hacker has entered an insecure network through a backdoor, they can cause extensive damage: installing malware, performing a denial of service (DoS) attack, stealing private information or changing other security settings that leaves the system vulnerable to other attacks. A **DoS attack** is an attack that targets a network or server and floods it with network traffic.

Possible impacts on an organization

As you've learned already, network attacks can have a significant negative impact on an organization. Let's examine some potential consequences.

- **Financial**: When a system is taken offline with a DoS attack, or business operations are halted or slowed down by some other tactic, they prevent a company from performing the tasks that generate revenue. Depending on the size of an organization, interrupted operations can cost millions of dollars. In addition, if a malicious actor gets access to the personal information of the company's clients or customers, the company may face heavy litigation and settlement costs if customers seek legal recourse.
- **Reputation**: Attacks can also have a negative impact on the reputation of an organization. If it becomes public knowledge that a company has experienced a cyber attack, the public may become concerned about the security practices of the organization. They may stop trusting the company with their personal information and choose a competitor to fulfill their needs.
- **Public safety**: If an attack occurs on a government network, this can potentially impact the safety and welfare of the citizens of a country. In recent years, defense agencies across the globe are investing heavily in combating cyber warfare tactics. If a malicious actor gained access to a power grid, a public water system, or even a military defense communication system, the public could face physical harm due to a network intrusion attack.

Key takeaways

Malicious actors are constantly looking for ways to exploit systems. They learn about new vulnerabilities as they arise and attempt to exploit every vulnerability in a system. Attackers leverage backdoor attack methods and network interception attacks to gain sensitive information they can use to exploit an organization or cause serious damage. These types of attacks can impact an organization financially, damage its reputation, and potentially put the public in danger. It is important that security analysts stay educated in order to maintain network safety and reduce the likelihood and impact of these types of attacks. Securing networks has never been more important.

Revision #2
Created 30 June 2023 22:38:37 by naruzkurai
Updated 3 July 2023 10:29:21 by naruzkurai