A Brief Introduction to Network Security and Firewalls

Team 19

Nicole Tran, Jess Fayer, Hunter Horst, David Kneebone, Samson Mulugeta

Above and Beyond:

To go past just what was available in a module, we thought it would be suitable to create a mini lab using software we've already touched on before to model what implementing a firewall might be like. Beyond just doing the learning, it's fun to see how it might be applied, but without the full pressure of a lab. As such, we made a follow-along video to implement a firewall against ICMP protocol messages but to allow IP protocol messages using Cisco Packet Tracer based off of what we saw was being used in some certification courses. In it, we show how to initialize a quick network and set IPs in packet tracer (like what we do in class, but doable from home) and then choose a machine to block messaging to and from.

Main Module

Slides:
https://docs.google.com/presentation/d/1ca4d6IxQIzILoGVAST5SVnjY6-9m-9xiCRf3M2WzLbI/edit?usp=sharing

Lecture Link:

https://youtu.be/EPLXL-Tgqlc

Introduction to Network Security

What Is Network Security:

Network security is "the protection of the underlying networking infrastructure from unauthorized access, misuse, or theft" (Cisco). It's like a digital gatekeeper, ensuring that only the right people or systems have access to sensitive information and resources.

Why Network Security Matters:

Since network security is the gatekeeper that protects a company it is extremely important in today's digital world. It helps serve as a barrier that keeps personal and sensitive information safe, shielding it from potential threats and breaches. Network security also plays a crucial role in preventing unauthorized users from accessing or damaging computer systems. This is important since it helps protect any important company data. It protects businesses and organizations from cyber attacks that result in them getting extreme financial harm which damages the reputation of the company. Network security also ensures safe communication and data exchange over networks which allows for secure interactions to take place. In the end network security is something that is simply a necessity but a critical element in the smooth running of a networked system.

The History of Network Security:

In the early days of computers, they were standalone machines that had limited connectivity with other systems. The way computers were protected at this time was done through physical protection and the use of passwords. Due to this being a time when network security wasn't much of a worry since there weren't many threats due to the isolated nature of the systems.

With the rise of networks and the internet on the other hand, the network security industry took a huge jump. As technology advanced the need for more complex network security grew. The earliest threats for network security were basic viruses and worms which were malicious programs that could spread rapidly across any connected systems which would result in widespread damage and disruption for the network. This resulted in a change of focus on network security instead of just protecting the physical hardware itself securing data and information transmitted across networks. It also set up the stage for the complex and multifaceted approach to network security that we see today

Evolution of Network Security:

The 1990's was the start of the 1st generation of network security and during this period it gave rise to the earliest of firewalls and antivirus software. These were used to protect the network from external threats. Firewalls served as the first line of defense in controlling traffic between trusted networks and untrusted networks. Anti-virus software was made to detect any malicious software and then remove it once detected.

The 2000s had a rise in cybercrime. The complexity and sophistication of them also grew. Hackers began to exploit different vulnerabilities in both software and hardware which resulted in new types of attacks like phishing, denial-of-service (DoS), and man-in-the-middle (MitM) attacks (Avast). This showed the need for more advanced security measures in order to combat the threats as they continued to evolve.

The 2010s brought the rise of a new type of threat called Advanced Persistent Threats (APTs) and also had an increase in data breaches. APTs are a type of long-term attack in which the goal is to steal as much information in an extended period of time (Imperva), Data Breaches also become more common with large amounts of sensitive data being stolen from individuals and companies. This era also highlighted how it was important to have continuous monitoring and proactive defense strategies in network security.

What Network Security Looks Like Today:

Modern Strategies

- **Firewalls:** Even though it was one of the first types of network security firewalls remain a fundamental part of network security, serving as a barrier between trusted and untrusted networks.

- **Intrusion Detection and Prevention Systems (IDPS):** IDPS are used to detect and prevent unauthorized access and threats in real time.
- **Encryption:** Encryption is used to protect data in transit and at rest, ensuring that even if data is intercepted, it cannot be read without the correct decryption key.
- **Multi-Factor Authentication:** MFA provides an extra layer of security by requiring users to give more than just a normal password as a way of verification to further secure whatever you are using
- **Artificial Intelligence (AI) and Machine Learning:** AI and machine learning are being used to predict and identify threats and also have automated responses to them.

Key Challenges

- **Ransomware:** Ransomware attacks are when hackers encrypt a victim's data and demand a ransom or they threaten to release it.
- **Zero-day Vulnerabilities:** Vulnerabilities in software that are unknown at the time. Until the vulnerability is fixed hackers can exploit it to do harm to the network
- **Human Error:** Even with advancements in technology human error isn't something that can really be stopped. People can still fall for things like phishing attacks. They can also have weak passwords, or fail to follow security protocols.

Sources:
https://www.cisco.com/c/en/us/products/security/what-is-network-security.html
https://www.avast.com/business/resources/future-of-network-security#pc
https://www.tripwire.com/state-of-security/understanding-evolution-network-security
https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/

Learning Objectives

Objective 1: Identify and Understand Network Threats and Protections
Students will be able to identify and understand different types of threats such as viruses, worms, zero-day attacks, etc. Additionally, students will learn how to use protective mechanisms to protect themselves from cyber attacks.

Objective 2: Configure Basic Network Security on Simulation Software
Students will be able to use Cisco Packet Tracer to set up network configuration. By using the Cisco Packet Tracer as a tool, students will learn how to implement basic firewalls and see how different protocols can be allowed or disallowed on different endpoint machines.

Articles/Readings

The 15 Biggest data breaches of the 21st century

Takeaways:

- Network security is extremely serious. It has led to billions of people having their personal info as well as credit info being stolen. Even the 15th place spot for largest data breach involved 153 million Adobe users getting their debit and credit card info stolen.
- 12 of the 15 cases occurred in the 2010's with three being in the 2020's even though this list was only formulated at the end 2022. The dates of these attacks show that data breaches did not get nearly as serious until the 2010's and that since then network security has not improved much more than the ability of hackers to steal data has.
- The people who steal data typically just sell the data to other cybercriminals who will then use the data such as debit or credit card numbers for their own benefit. However, there are some exceptions, some of these attacks were not even done out of ill intent but for personal curiosity and use, nonetheless all attackers were punished legally.
- Many of the companies who received the data breach were fined millions of dollars for not protecting their users data well enough
- Not only do the affected companies face expenses, but these breaches can also seriously damage their reputation.

Top 10 Common Types of Network Security Attacks Explained

Takeaways:

- Computer Virus
    - They are a type of malware that can cause immense damage to a systems network and self replicate to spread between multiple computers.
    - Clicking or downloading links can lead to viruses corrupting a computer's files.
    - At least 30% of the world's computers are infected with one or more viruses.
- Malware
    - Malicious codes that can be used to corrupt files and data. It can affect both internal and external endpoint devices of a network.
- Computer Worm
    - Malicious software that spreads from one infected computer to another by duplicating a copy of itself.
- Phishing
    - A social engineering attack where cybercriminals trick users into clicking an email link that seems legitimate but is really fraudulent. By clicking the link, the user downloads malware onto their device, allowing their sensitive information to be stolen.
- Botnet
    - Botnets are a network of systems and devices that have been taken over by hackers and are connected to the internet. Hackers can use the devices or bots to send spam, perform data theft, and enable Distributed Denial of Service attacks.
- Distributed Denial of Service (DDoS) Attacks
    - Is when multiple bots are launched at a particular site all at once to cripple the IT infrastructure and potentially bring it down.
- Man in the middle

    - When hackers hijack private communication intended between two parties. In doing so, the hacker can monitor and control their messages to disrupt files, steal information, or even spy on the two parties.
- Ransomware
    - When malicious software is used to gain access to a network and lock files until a ransom is paid.
- 5G based attacks
    - When hackers use 5G devices to send swarms of bots to multiple systems, mobiles, and IoT networks.
    - The nature of 5G networks allow for high-speed transfers of data but also increases the risk of cyberattacks.
- SQL Injection Attacks
    - When hackers change the scripts of vulnerable user-input fields in order to inject malicious SQL statements into those fields.
    - These attacks can infect or exploit any website or application that uses an SQL-based database.

Other takeaways

- Many of these attacks included the use of malware

What is Network Security

Takeaways:

- Firewalls (Samson covered)
- Network segmentation
    - When a network is split up into separate roles and functions within an organization so that if one area of a network is compromised, the rest of the network can still be safe.
- Access control
    - Placing limitations and guidelines for who all can access the network, so that there is less risk in the network being accessed by someone with ill intent.
- Remote Access VPN
    - Provides individuals with remote and secure access to a company network. The information sent between the individual and the company’s network is encrypted and unable to be accessed by outside parties.
- Zero Trust Network Access [ZTNA]
    - A model that states that users should only have the access and permissions if they absolutely require them to do their jobs. Similar to access control, it is the mindset of preventing as many people as possible from having access to sensitive information, so that there can be less risk of that information being stolen.
- Email Security
    - Any process, product, or service built to protect email accounts. and the content sent and received by those accounts, from being accessed by external threats.
- Data Loss Prevention [DLP]

    - Data Loss Prevention is a cybersecurity methodology that uses technology and best practices to prevent the exposure of sensitive information outside of an organization.
    - Detects threats and monitors sensitive information
- Intrusion Prevention Systems [IPS] (Samson covered)
- Sandboxing
    - Running code or open files in a safe and isolated environment so that you can look for vulnerabilities and malicious behavior so that they can be prevented in the future.
- Hyperscale network Security
    - The ability of an architecture to scale appropriately with the changes in network security demands. This allows the network greater protection against DDoS attacks or other attacks where certain networks are suddenly put under intense pressure and demand.
- Cloud Network security
    - Any type of protection against attacks on cloud networks. Some strategies are to use Software-defined Networking [SDN] and Software-defined Wide Area Network [SD-WAN] solutions.

Learning Objective Questions

Questions to assess learning:

1. What are some of the most common types of network security attacks?
2. How have the various threats to network security changed over time? How have our security measures improved in return?
3. What measures should you take to minimize your networks' vulnerability? How might malicious actors circumvent your security? Are there threats you have no control over?

Packet Tracer Firewall Mini Lab

Mini Lab Video:

nicole_firewall_lab.mp4

Mini Lab Screenshots:

Firewall Lab Zoomed in Screenshots

Nicole Lab File:

firewall_lab.pkt

This is a simple lab going over how someone might prevent one endpoint in their network from getting permissions for a certain protocol (I used ICMP) but allowing others (like IP). Through testing, we can show that pings are not able to be sent or received by that one PC but are able to be sent by other parts of the network.

Sources:

https://www.youtube.com/watch?v=yLOYd87z2jg

https://www.youtube.com/watch?v=xdbI8nfGg80