

OVERVIEW

Network Security Management (NSM) is the comprehensive discipline of administering, monitoring, and maintaining the security policies, procedures, and tools that protect a network's infrastructure, data, and resources from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure. In essence, it is the continuous process of ensuring the Confidentiality, Integrity, and Availability (the CIA triad) of network services and data (Stallings, 2017).

In modern networking, the importance of NSM cannot be overstated. The traditional network perimeter has dissolved with the adoption of cloud services, mobile devices, and the Internet of Things (IoT), creating a vastly expanded and more vulnerable attack surface. This evolution means that a fortress-like defense at the network's edge is no longer sufficient. Modern NSM must adopt a defense-in-depth strategy, implementing multiple layers of security controls throughout the network to protect against sophisticated, multi-vector threats like ransomware, advanced persistent threats (APTs), and insider threats (Cherdantseva & Hilton, 2013).

Key Concepts (Spoonfed for Clarity):

- CIA Triad: The core model of information security.
- Confidentiality: Ensuring that data is only accessible to authorized users. (Think: encryption and access controls).
- Integrity: Guaranteeing that data is accurate and has not been tampered with. (Think: hashing and digital signatures).
- Availability: Ensuring that network systems and data are accessible to authorized users when needed. (Think: preventing Denial-of-Service (DoS) attacks and having good backups).
- Attack Surface: This is the sum of all the different points (vectors) where an attacker could try to break into a network. Every connected device, user account, and software application is a potential part of this surface.
- Defense-in-Depth: Instead of relying on one big wall (like a firewall), this is a strategy of using many different, overlapping security layers. If an attacker bypasses one layer (e.g., the firewall), they are then stopped by the next (e.g., an Intrusion Detection System), and the next (e.g., strict user permissions). It's like having a locked fence, a guard dog, and a safe inside your house.
- Advanced Persistent Threat (APT): This is not a simple virus. An APT is a sophisticated, prolonged, and targeted cyberattack where an intruder gains access to a network and remains undetected for a long period to steal data or monitor activity. Defending against these requires advanced NSM.

Week 11: Network Management

Toledo, Pauline | Tolero, Selwyn

NETWORK SECURITY MANAGEMENT

The Role of the Security Manager:

- Risk Assessment: Identifying what assets need protection and what threats they face.
- Policy Formulation: Creating the rules (e.g., "All emails must be scanned for malware").
- Implementation: Deploying tools like firewalls, antivirus software, and access control lists (ACLs).
- Monitoring & Detection: Using Security Information and Event Management (SIEM) systems to collect logs and look for suspicious activity in real-time.
- Response & Recovery: Having a plan to contain attacks, eradicate the threat, and restore systems (an Incident Response Plan).

In conclusion, effective Network Security Management is the critical, ongoing practice that enables organizations to operate securely in a hyper-connected world. It moves beyond simply installing security software to encompass a strategic, process-driven approach that is adaptive, proactive, and essential for protecting an organization's most valuable digital assets.

THEORIES AND PRINCIPLES

Network Security Management is not a random collection of tools; it is guided by foundational theories and principles that provide a structured framework for defense. Understanding these is crucial for building a robust security posture.

1. The CIA Triad: The Foundational Principle

This is the most fundamental concept in all of information security. It defines the three core goals of security measures.

Theory: All security controls are implemented to achieve one or more of these three principles.

- Confidentiality: Ensuring that information is not disclosed to unauthorized individuals, entities, or processes. This is achieved through encryption (scrambling data so only authorized parties can unscramble it), access control lists (ACLs), and strict authentication protocols.
- Integrity: Guarding against improper information modification or destruction. This ensures the accuracy and trustworthiness of data. Techniques like cryptographic hashing (creating a unique digital fingerprint for a file) and digital signatures are used to verify that data has not been altered.
- Availability: Ensuring timely and reliable access to and use of information by authorized users. This means protecting systems from disruptions, such as Denial-of-Service (DoS) attacks, and ensuring reliability through maintenance, redundancy, and comprehensive disaster recovery plans.



2. Defense-in-Depth (The Castle Approach)

Theory: A single layer of defense is weak. A robust security posture employs multiple, layered, and overlapping security controls to protect assets. If one control fails, others will still be in place to thwart an attack.

Think of a castle. It doesn't just have a tall wall; it has a moat, a drawbridge, archers on the walls, and soldiers inside. Similarly, a network should have:

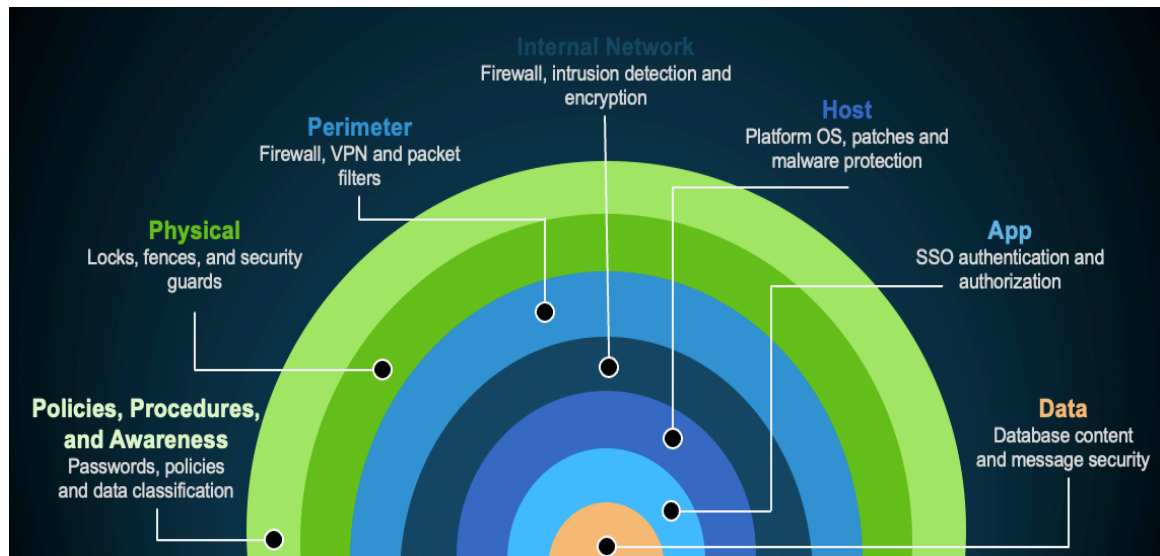
- Physical Layer: Security guards, locked server rooms.
- Technical Layer: Firewalls, Intrusion Prevention Systems (IPS), antivirus software, encryption.
- Administrative Layer: Security policies, user training, incident response plans.

The failure of a firewall (the outer wall) should not lead to a catastrophic breach because the antivirus on the endpoint (the soldiers inside) can still detect and stop the threat.

Week 11: Network Management

Toledo, Pauline | Tolero, Selwyn

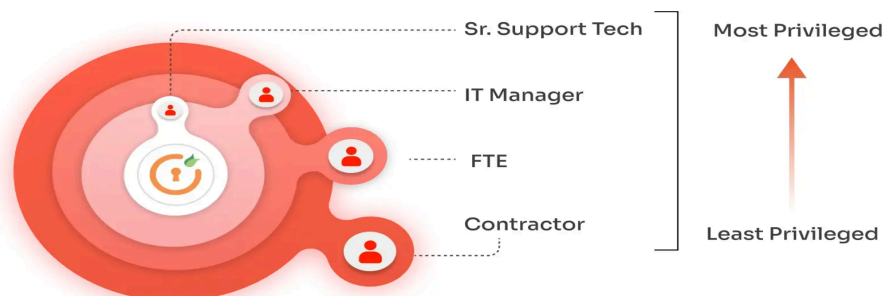
NETWORK SECURITY MANAGEMENT



3. The Principle of Least Privilege (PoLP)

Theory: Every user, process, or system should only have the minimum level of access rights necessary to perform its intended function—and only for the minimum amount of time required.

Explanation: This is a critical tool for limiting the "blast radius" of an attack. If a user's account is compromised, the attacker only gains the limited privileges of that user, not administrative control over the entire network. For example, an accountant does not need to install software privileges on their computer, and a database server does not need unrestricted internet access.



The Principle of Least Privilege

Week 11: Network Management

Toledo, Pauline | Tolero, Selwyn

NETWORK SECURITY MANAGEMENT

4. Risk Management Framework (Identify -> Protect -> Detect -> Respond -> Recover)

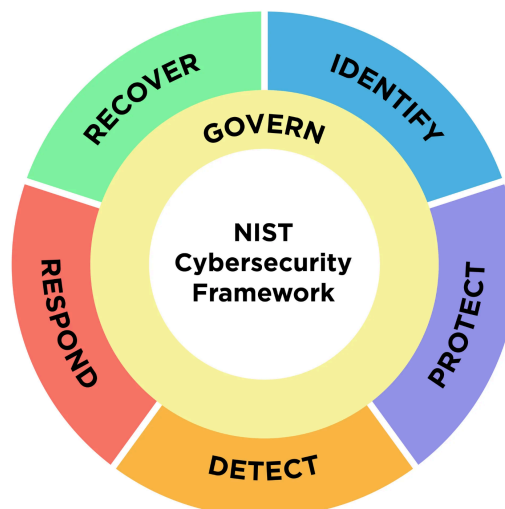
This is not just a theory but a practical, cyclical process that forms the backbone of modern NSM. It is best illustrated by a diagram, such as the one from the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Theory: Security is a continuous cycle, not a one-time project. It involves proactively managing risk through a structured lifecycle.

Explanation of the Stages (as shown in the diagram below):

- Identify: Understand your environment. What assets do you have? What data is critical? What are your threats and vulnerabilities? This is the foundation.
- Protect: Implement safeguards. This is where you deploy your security tools (firewalls, training, access controls) to prevent an incident.
- Detect: Implement activities to identify a cybersecurity event. This includes continuous monitoring with SIEM systems and intrusion detection tools.
- Respond: Take action regarding a detected incident. Activate your Incident Response Plan to contain the damage and eradicate the threat.
- Recover: Restore capabilities and services impacted by the incident. This involves restoring from backups and updating policies to prevent future similar attacks.

The cycle then repeats, learning from the Recover phase to better Identify new risks.



Week 11: Network Management

Toledo, Pauline | Tolero, Selwyn

NETWORK SECURITY MANAGEMENT

REAL-WORLD APPLICATION

Case Study: Segmenting a Hospital Network for Security and Compliance

Scenario: A large hospital's network was flat, meaning medical devices, patient records systems, guest Wi-Fi, and administrative PCs were all on the same network segment. This posed a massive security risk and failed compliance audits (e.g., for HIPAA).

Problem: An infection on a guest's laptop could easily spread to critical systems like MRI machines or electronic health records (EHR), jeopardizing patient safety and data confidentiality.

Solution: A Segmented Network using VLANs and ACLs

The hospital implemented a defense-in-depth strategy centered on network segmentation.

1. Design (Principle of Least Privilege & Confidentiality):

VLAN 10: Clinical Devices VLAN: Isolated network for MRI machines, heart monitors, and other IoT devices. These devices cannot initiate connections to other networks.

VLAN 20: EHR Servers VLAN: Highly restricted network for patient database servers. Access is tightly controlled.

VLAN 30: Staff VLAN: For trusted, authenticated PCs used by doctors and nurses. Needs controlled access to VLAN 20 (EHR).

VLAN 99: Guest Wi-Fi VLAN: Completely isolated from all internal networks. Provides internet access only.

2. Implementation (Defense-in-Depth):

Layer 2 Security: Port Security was configured on all switch ports connected to clinical devices to prevent unauthorized devices from being plugged in.

Layer 3 Security (ACLs): Firewalls and Router ACLs were deployed as gateways between VLANs to enforce policy. For example:

An ACL on the router interface for VLAN 30 (Staff) only permits traffic to VLAN 20 (EHR) on the specific database port (e.g., TCP/1433) and denies all other inter-VLAN traffic.

An ACL on VLAN 99 (Guest) explicitly denies all traffic destined for the internal network ranges and only permits outbound internet traffic.

Week 11: Network Management

Toledo, Pauline | Tolero, Selwyn

NETWORK SECURITY MANAGEMENT

Monitoring (Detect/Respond): A SIEM system was implemented to monitor all traffic between VLANs, alerting on any suspicious activity, such as a device from the Clinical VLAN attempting to scan the network.

Outcome:

This architecture directly supported the CIA Triad:

Confidentiality: Patient data in the EHR VLAN was protected from unauthorized access from other segments.

Integrity: Critical medical devices were isolated from potential tampering.

Availability: A ransomware infection on the Guest Wi-Fi was contained and could not spread to shut down critical hospital operations.

This case study demonstrates how theoretical principles (CIA, Least Privilege, Defense-in-Depth) are applied through specific technologies (VLANs, ACLs, Port Security) to solve a real-world enterprise security challenge.

LABORATORY EXERCISE: HOST-BASED FIREWALL LAB

Single-Computer Laboratory Activity: Host-Based Firewall Policy Implementation

1. Learning Objective:

This lab provides hands-on experience with the principle of least privilege and default-deny firewall policies. You will learn to use the host-based Windows Firewall to create security policies that block unnecessary traffic, simulating how security policies are applied to protect a single endpoint—a critical skill in network security.

2. Scenario:

You are hardening your own computer. Your task is to configure its local firewall to implement the following security policy:

Make your computer "stealthy" to basic network discovery by blocking inbound Echo Requests (pings) even from your own network.

Block unencrypted web traffic from being served by your PC by blocking inbound HTTP (Port 80).

Test the policy by attempting to ping yourself and access your own local web server.

3. Materials Needed:

A single computer running Windows 10 or 11.

Week 11: Network Management

Toledo, Pauline | Tolero, Selwyn

NETWORK SECURITY MANAGEMENT

Administrator access on the computer.

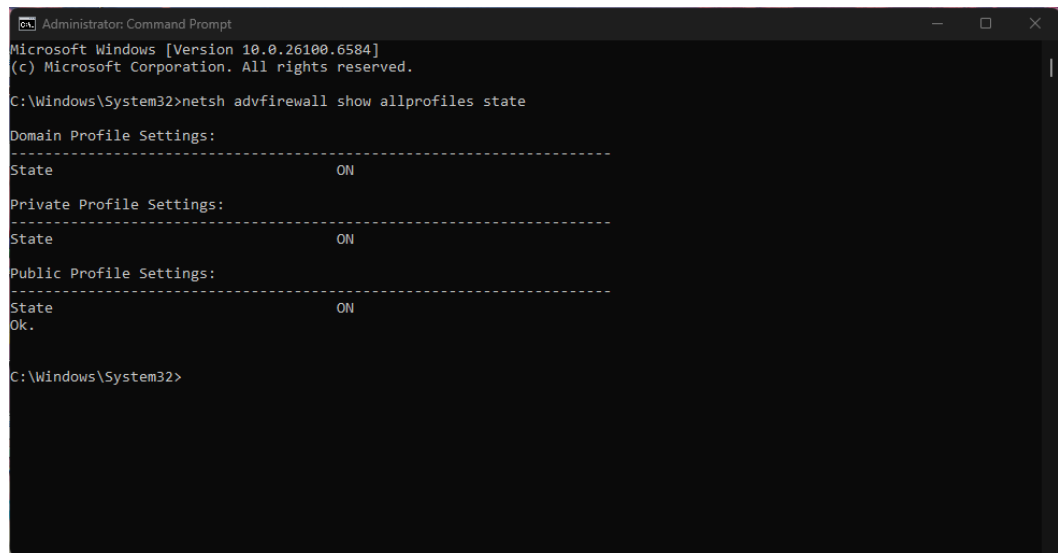
4. Step-by-Step Instructions:

Part A: Establish a Baseline (Test Before Changes)

- **Open Command Prompt as Administrator:** Search for "cmd" or "Command Prompt," right-click, and select "Run as administrator."
- **Check the default firewall state.** Type the following command and press Enter:

```
netsh advfirewall show allprofiles state
```

You should see that the Domain, Private, and Public profiles are ON. This means your firewall is active but mostly allowing responses.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.26100.6584]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>netsh advfirewall show allprofiles state

Domain Profile Settings:
-----
State                        ON
-----

Private Profile Settings:
-----
State                        ON
-----

Public Profile Settings:
-----
State                        ON
Ok.

C:\Windows\System32>
```

- **Test Inbound Ping (Echo Request) to Yourself:** In your Administrator Command Prompt, ping your own computer using its loopback address (127.0.0.1).

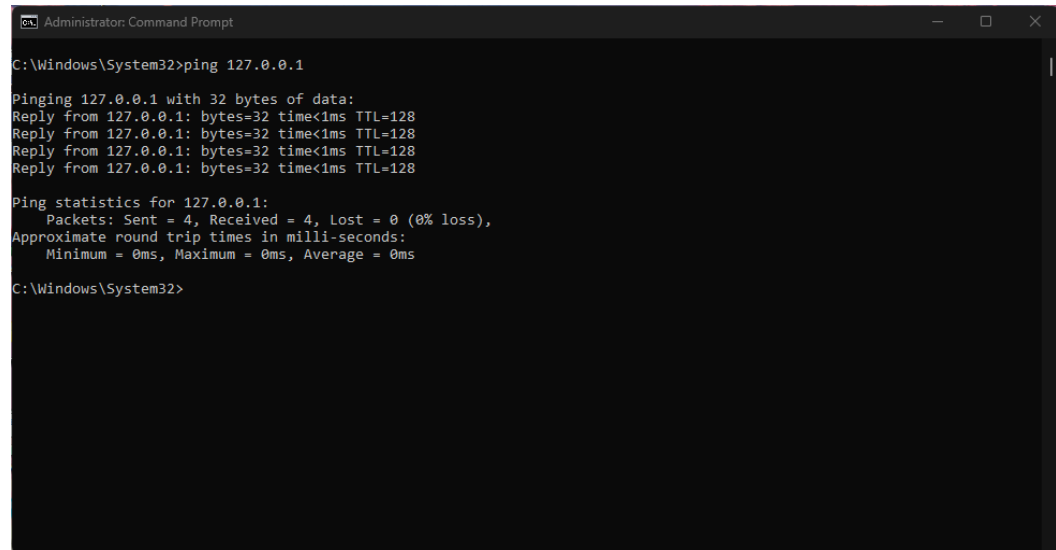
```
ping 127.0.0.1
```

Expected Result: You will get replies from yourself. This shows that the machine currently responds to ping requests.

Week 11: Network Management

Toledo, Pauline | Tolero, Selwyn

NETWORK SECURITY MANAGEMENT



```
Administrator: Command Prompt

C:\Windows\System32>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\System32>
```

- **Test Inbound HTTP (Port 80) to Yourself:** We need to see if Port 80 is open. We'll use a simple, temporary web server.

In the Admin Command Prompt, navigate to your root directory and start a web server on port 80 using a one-line PowerShell command:

```
cd C:\
PowerShell -Command "Start-Process PowerShell
-ArgumentList '-Command & {cd C:\; python -m
http.server 80}' -Verb RunAs"
```

(This command might prompt you for permission. Click "Yes". A new window will open running the server.)

- Open your web browser (Chrome, Edge, etc.) and go to the address: <http://localhost>
- **Expected Result:** You should see a directory listing of your C:\ drive. This is a huge security risk! It means a vulnerable program could open a port and expose your files.

Part B: Configure the Firewall Rules (Implement the Security Policy)

We will now create rules to block this traffic. Keep the web server window open.

1. Open Windows Defender Firewall with Advanced Security:

- Press Windows Key + R, type `wf.msc`, and press Enter. This is the main console for advanced firewall settings.

Week 11: Network Management

Toledo, Pauline | Tolero, Selwyn

NETWORK SECURITY MANAGEMENT

2. Block Inbound ICMP Echo Requests (Pings):

- In the left pane, click on Inbound Rules.
- In the right pane, click New Rule....
- Rule Type: Select Custom and click Next.
- Program: Leave it as "All programs" and click Next.
- Protocol and Ports: From the "Protocol type:" dropdown, select ICMPv4. Click the Customize... button.
- In the new window, select Specific ICMP types, check the box for Echo Request, and click OK. Click Next.
- Scope: Leave the default settings (Any IP address). Click Next
- Action: Select Block the connection. Click Next.
- Profile: Apply to all (Domain, Private, Public). Click Next.
- Name: Give the rule a descriptive name, e.g., Block-Inbound-Ping-Request. Click Finish.
- Block Inbound HTTP (Port 80):
- Click New Rule... again.
- Rule Type: Select Port and click Next.
- Protocol and Ports: Select TCP and specify 80 as the "Specific local ports." Click Next.
- Action: Select Block the connection. Click Next.
- Profile: Apply to all. Click Next.
- Name: Block-Inbound-HTTP-TCP80. Click Finish.

Part C: Verify the Configuration (Test After Changes)

1. **Test Inbound Ping Again:** Go back to your Administrator Command Prompt and ping yourself again.

```
ping 127.0.0.1
```

 - Expected Result: You will now see "Request timed out."
 - Explanation: Success! Your new firewall rule is working. Your computer now ignores ping requests, making it less visible on a network.
2. **Test Inbound HTTP Again:** Go back to your web browser and refresh the page at <http://localhost> (or open a new tab and go there).
 - Expected Result: The browser will spin for a while and eventually show an error like "This site can't be reached" or "connection timed out".
 - Explanation: Success! You have successfully blocked all traffic on port 80. Even though the web server is still running, the firewall is now dropping all packets trying to reach it, neutralizing the security risk.
3. **Cleanup:**
 - You can close the web server window you opened earlier.

Week 11: Network Management

Toledo, Pauline | Tolero, Selwyn

NETWORK SECURITY MANAGEMENT

- In wf.msc, you can see your new rules in the Inbound Rules list. You can right-click on them and select Disable Rule to return your firewall to its previous state, or leave them enabled for better security.

1. Expected outcome of the lab (e.g., communication setup, routing table results, ACL results, wireless analysis).

- **Outcome:** After completing the lab, your computer will no longer respond to ping requests and will reject all incoming connection attempts on the unsecure HTTP port (80), even from itself.
- **Explanation:** This lab demonstrates a fundamental concept of security: default deny. Instead of allowing all traffic and trying to block known bad things, you created explicit rules that block specific traffic, and everything else is handled by the default rules. This is the exact logic used in enterprise firewalls and ACLs:
 1. The firewall inspects all incoming data packets.
 2. It matches the packets against your custom rules first.
 3. It sees packets for ICMP Echo or TCP Port 80 and immediately drops them.
 4. This happens before any other general rules can allow the traffic through.

By completing this on your own machine, you have performed a critical task in device hardening, directly applying the network security principles discussed in class.

SUMMARY

From the Lesson:

- Security is a Process, Not a Product: Effective network security is a continuous cycle (like the NIST framework: Identify, Protect, Detect, Respond, Recover), not a one-time setup. It requires ongoing risk assessment, policy enforcement, monitoring, and improvement.
- The CIA Triad is the Core Goal: The fundamental objective of all security efforts is to uphold Confidentiality (preventing unauthorized data access), Integrity (ensuring data is accurate and untampered), and Availability (ensuring systems and data are accessible when needed).
- Defense-in-Depth is Non-Negotiable: A single security layer is fragile. A robust strategy employs multiple, overlapping layers (physical, technical, administrative) so that if one control fails, others remain to stop a threat.
- The Principle of Least Privilege is Foundational: Users, systems, and processes should only have the minimum access necessary to perform their function. This limits the potential damage from accidents or compromised accounts.

Week 11: Network Management

Toledo, Pauline | Tolero, Selwyn

NETWORK SECURITY MANAGEMENT

- Modern Networks Have No Perimeter: Cloud, mobile, and IoT technologies have dissolved the traditional network border, creating a large and dynamic attack surface. Security must be adaptive and integrated throughout the entire network environment.

From the Activity (Host-Based Firewall Lab):

- Theory into Practice: The lab provided direct, hands-on application of the Principle of Least Privilege and a default-deny security policy, moving these core theories from concept to tangible configuration on a real system.
- Endpoint Hardening is a Critical Skill: Securing individual devices (endpoints) with host-based firewalls is a vital last line of defense, protecting the device even if other network security layers are bypassed.
- Proactive Configuration is Key: Security is often about proactively blocking unnecessary network services and ports (like ICMP echo requests and HTTP) to reduce the attack surface and make a system less visible and exploitable.
- Understanding Tools and Logs: The activity built practical competency with essential administrative tools like the command prompt (ping, netsh), the Windows Firewall with Advanced Security console (wf.msc), and the concept of managing traffic based on ports and protocols.

REFERENCES

- Cherdantseva, Y., & Hilton, J. (2013). *A reference model of information assurance & security*. In *2013 International Conference on Availability, Reliability and Security* (pp. 546-555). IEEE. <https://doi.org/10.1109/ARES.2013.72>
- Cisco. (2021). *Configuring Port Security*. *Cisco IOS Security Configuration Guide*. <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/configuration/xr-16/sec-port-security-xr-16-book.pdf>
- National Institute of Standards and Technology (NIST). (2020). *Security and Privacy Controls for Information Systems and Organizations* (NIST Special Publication 800-53, Rev. 5). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.SP.800-53r5>
- Sandhu, R. S. (1996). *Role-Based Access Control Models*. IEEE Computer, 29(2), 38–47.
- Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice (4th ed.)*. Pearson Education.
- Sandhu, R. S., & Feinstein, H. L. (1994). *A role-based access control model*. In *Proceedings of the first ACM workshop on Role-based access control* (Vol. 1, pp. 1-11). National Institute of Standards and Technology.

Week 11: Network Management

Toledo, Pauline | Tolero, Selwyn

NETWORK SECURITY MANAGEMENT

SANS Institute. (2020). *The Zero Trust Security Model*. SANS Reading Room. <https://www.sans.org/reading-room/whitepapers/analyst/zero-trust-security-model-39325>

Scarfone, K., & Hoffman, P. (2009). *Guide to general server security* (NIST Special Publication 800-123). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-123>

Stallings, W. (2017). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson Education.

Week 11: Network Management

Toledo, Pauline | Tolero, Selwyn

NETWORK SECURITY MANAGEMENT

Laboratory Activity Screenshots