Introduction to Firewalls and Network Security

Cybersecurity

Network Security Day 1

Class Objectives

By the end of today's class, you will be able to:

Explain how open ports contribute to a machine's attack surface.

Use firewalls to protect a machine's open ports.

Develop and implement firewall policies with UFW and firewalld.

Today, we will build on our knowledge of basic networking and protocols to implement firewalls that protect networks.

Networking Recap

Networks allow computers to communicate with one another by sending data to and from open ports on other machines.

Devices must expose open ports in order to communicate with other machines on the network.

- It is unwise to assume the only people who will connect to a device are those you trust.
- Malicious actors can and will exploit this assumption to access sensitive information.
- Restricting access to open ports is a fundamental skill for any technical security specialist.

Network Security

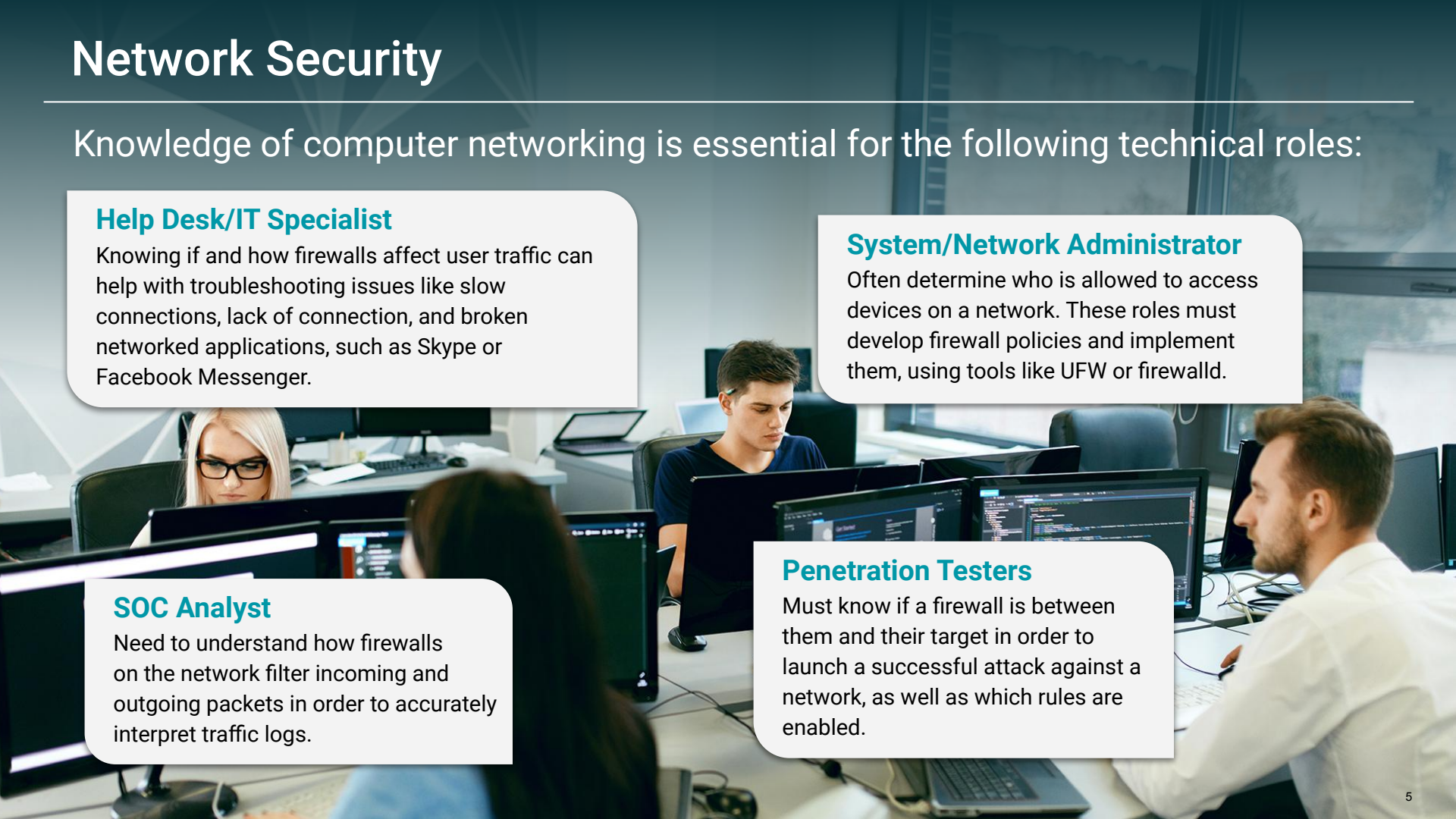
Knowledge of computer networking is essential for the following technical roles:

Help Desk/IT Specialist

Knowing if and how firewalls affect user traffic can help with troubleshooting issues like slow connections, lack of connection, and broken networked applications, such as Skype or Facebook Messenger.

System/Network Administrator

Often determine who is allowed to access devices on a network. These roles must develop firewall policies and implement them, using tools like UFW or firewalld.



SOC Analyst

Need to understand how firewalls on the network filter incoming and outgoing packets in order to accurately interpret traffic logs.

Penetration Testers

Must know if a firewall is between them and their target in order to launch a successful attack against a network, as well as which rules are enabled.

Network Security

The primary purpose of network defense is to protect the CIA triad.

- If any pillar of security information is compromised, the doors swing open for security breaches.
- This can be costly, both in terms of time and resources needed to address the issue, and the damage it can do to an organization's reputation.

Network Security

Consider the following scenario:

- An employee of a major department store forgets their laptop at a cafe. The machine is found by someone with malicious intent, and the company is breached.

- Millions of people's financial information is stolen in this breach. The retailer has a massive drop in sales as a result of this violation of trust.

But what if the laptop had proper security controls in place?

Network Security

What if the laptop had the following security controls?

- **Hard drive encryption**, which protects data at rest from being readable on the hard drive.
- **Firmware passwords**, which prevent attackers from booting the stolen laptop from an external hard drive.
- **GPS**, which provides law enforcement with the ability to track and recover the stolen laptop.
- **VPN**, which protects data in transit across unprotected WiFi.

Security professionals use the concept of **defense in depth** to implement security controls.

Defense in Depth

Defense in depth can be broken down into three security control types:

01

Physical controls
limit or prevent the physical access to a IT network.

02

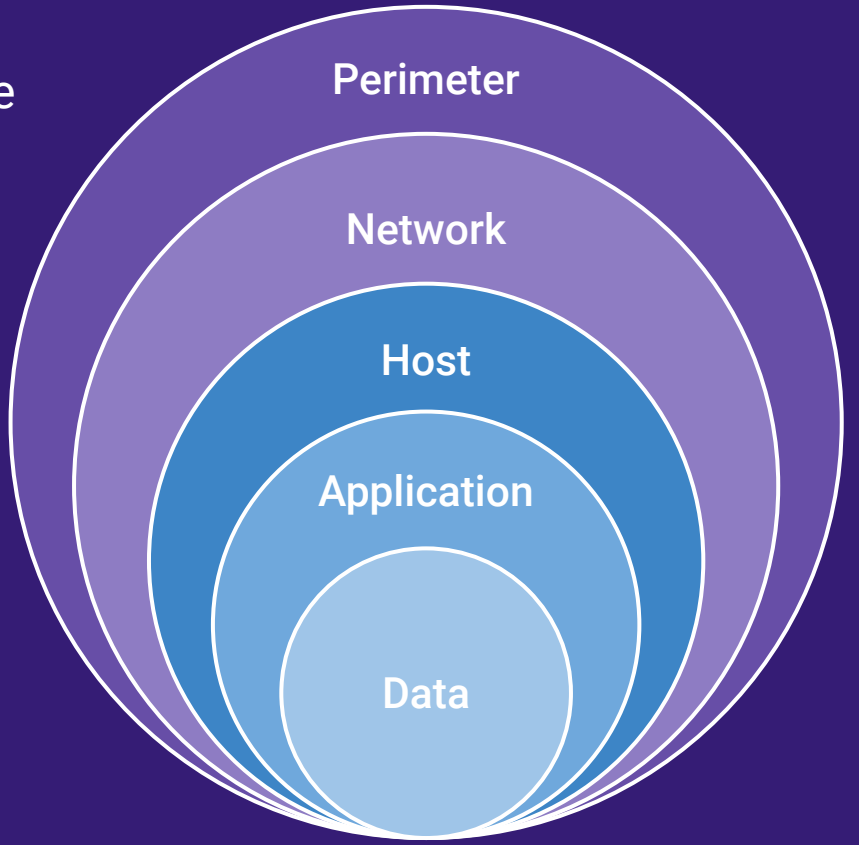
Technical controls
are any firmware, hardware, or software designed to protect networks and resources.

03

Administrative controls
are an organization's policies and procedures designed to ensure the organization handles private information with secure data-handling procedures.

Defense in Depth

Multiple layers of defense will slow down an attack, providing victims with more time to discover and respond to the breach.



Defense in Depth

In the laptop scenario, the few layers of defense put in place are enough to discourage an attacker while also protecting private data.

The possibility of the laptop being recovered is also highly likely.

Defense in Depth

Physical control examples include:

01 Walls

02 Bollards

03 Fences

04 Security guards

05 Dogs

06 Cameras

07 Lighting

Defense in Depth

Technical control examples include:

01 Encryption

02 Biometric fingerprint readers

03 Firewalls

04 Endpoint security

05 Intrusion detection systems

Defense in Depth

Administrative control examples include:

01 Security awareness programs

02 BYOD policies

03 Ethical hiring practices

Layered Defense

These three security control types can be broken down into seven basic layers:

01 Data

02 Application

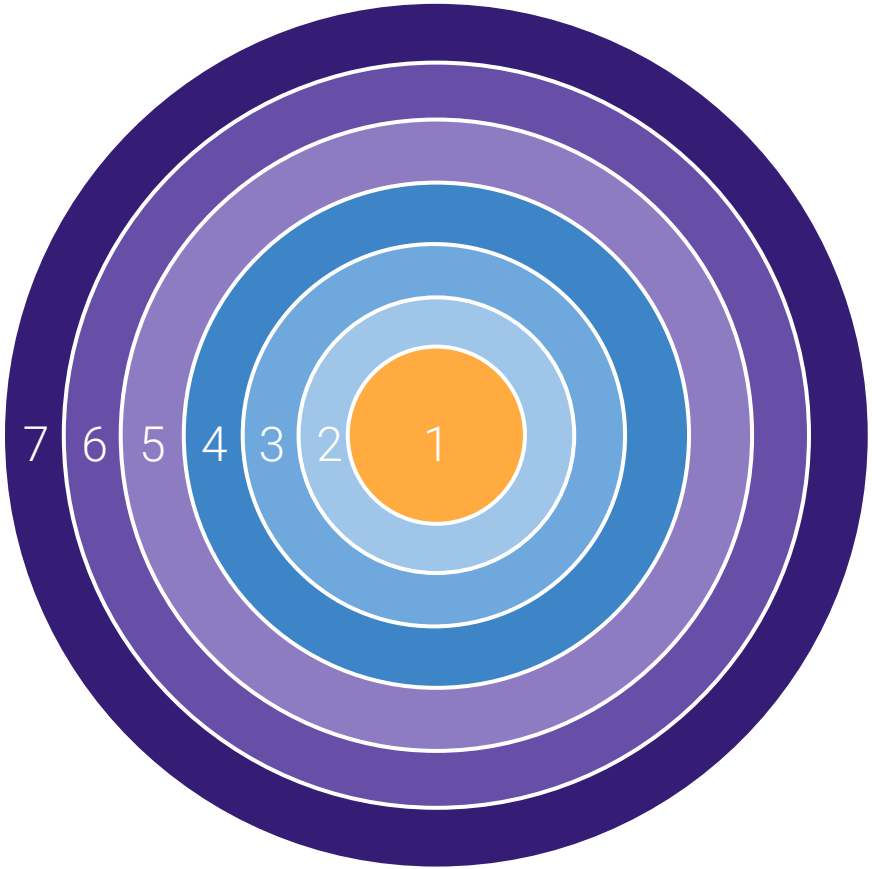
03 Host

04 Internal Network

05 Perimeter

06 Physical

07 Policies, Procedures, Awareness



Layered Defense

These three security control types can be broken down into seven basic layers:

01 **Data:** Actual data, an attacker's ultimate target.

02 **Application:** Software used to defend networks.

03 **Host:** Physical hardware running applications and storing data.

04 **Network:** Internal network consisting of everything between the host and the perimeter defenses.

05 **Perimeter:** Hardware protecting the internal network from everything external to the network.

06 **Physical:** Physical barriers designed to prevent unauthorized access by people.

07 **Policies, Procedures, and Awareness:** Written documentation designed to enforce regulatory compliance, organizational policy, and implementation of security awareness programs.

Lockheed Martin, an aerospace and defense company, developed another form of layered defense: the **cyber kill chain**.

It defines **seven steps** an adversary must complete before being able to act on their objectives.

Reconnaissance
Information gathering against a target.

Weaponization
Establishing attack vectors and technical profiles of targets.

Delivery
Delivering weaponized payload via email, website, USB, etc.

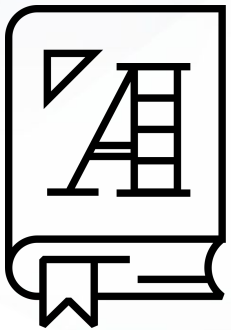
Exploitation
Actively compromising adversary's applications and servers while averting security controls.

Installation
Persistence preparation.

Command and Control (C2)
Command channel used for remote control of victim's machine.

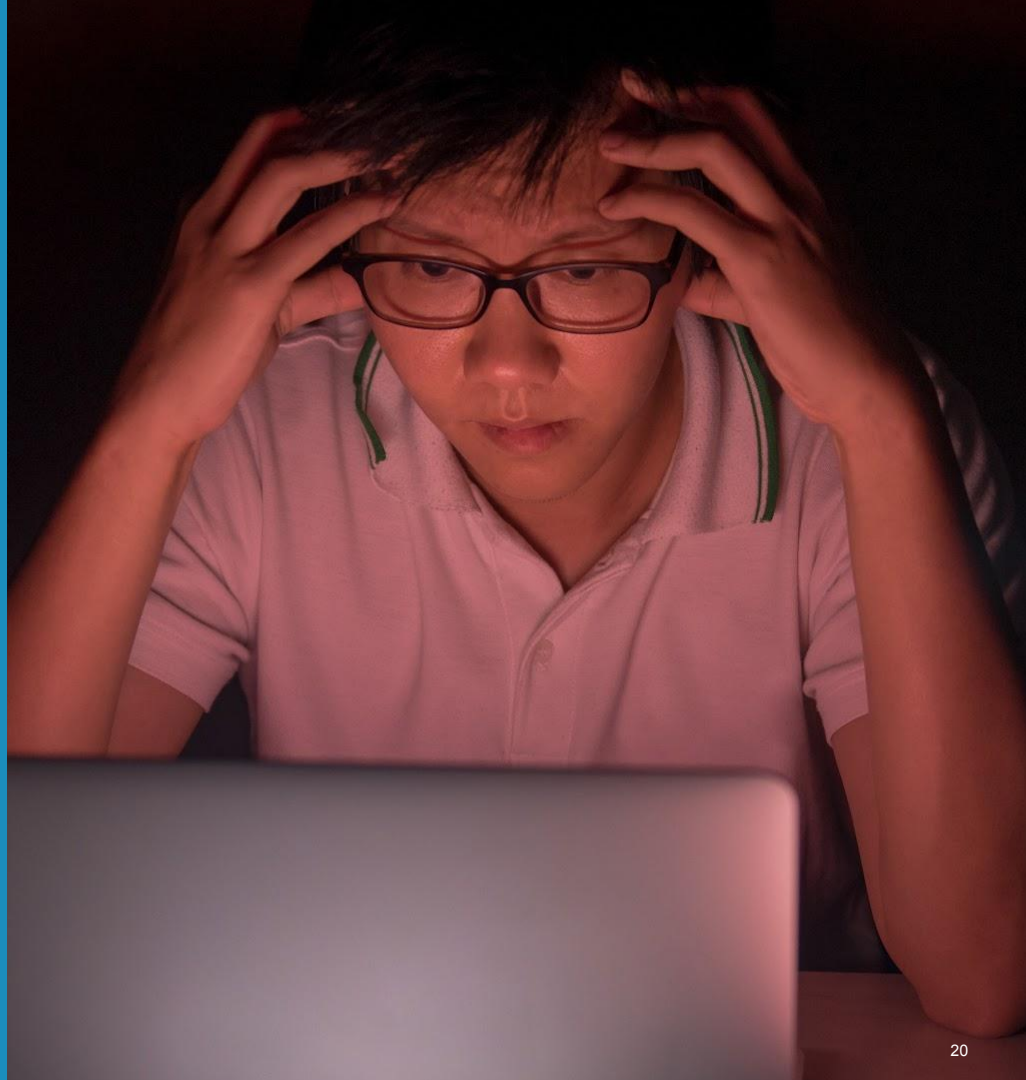
Actions on Objectives
Adversaries can now act on their objectives.

(Lockheed Martin)



The **cyber kill chain** is an intelligence-driven defense framework designed to identify and prevent cyber intrusions.

Observing an attack as it progresses through each level of the **cyber kill chain** enhances visibility and comprehension.



The Cyber Kill Chain

Adversaries are categorized into three designations:

01

Advanced

An adversary who is targeted, coordinated, and purposeful.

02

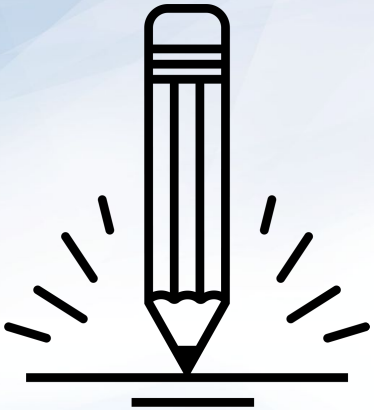
Persistent

An adversary who is relentless and undeterred by time.

03

Threat

An adversary with opportunity, intent, and capability.



Activity: DiD and the Cyber Kill Chain

In this activity, you will reinforce the concepts of defense in depth and the cyber kill chain in order to gain insight into attackers' tactics, techniques, and procedures.

Suggested Time:
10 Minutes

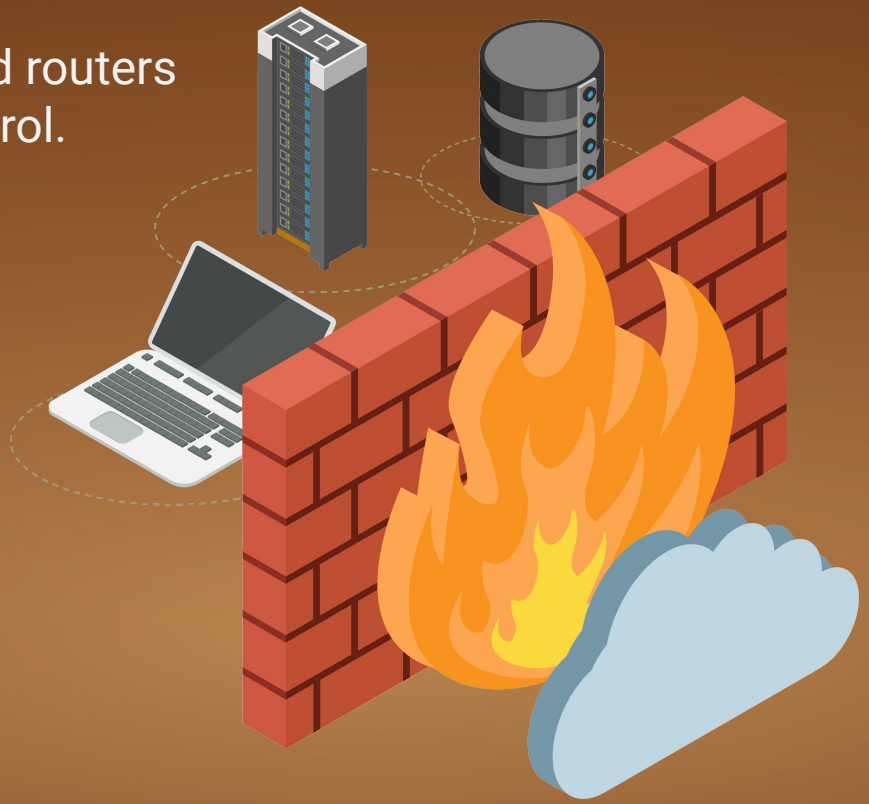
Time’s Up! Let’s Review.

Firewall Architectures and Methodologies

Firewalls provide a layer of protection by analyzing data leaving and entering a network.

Firewalls

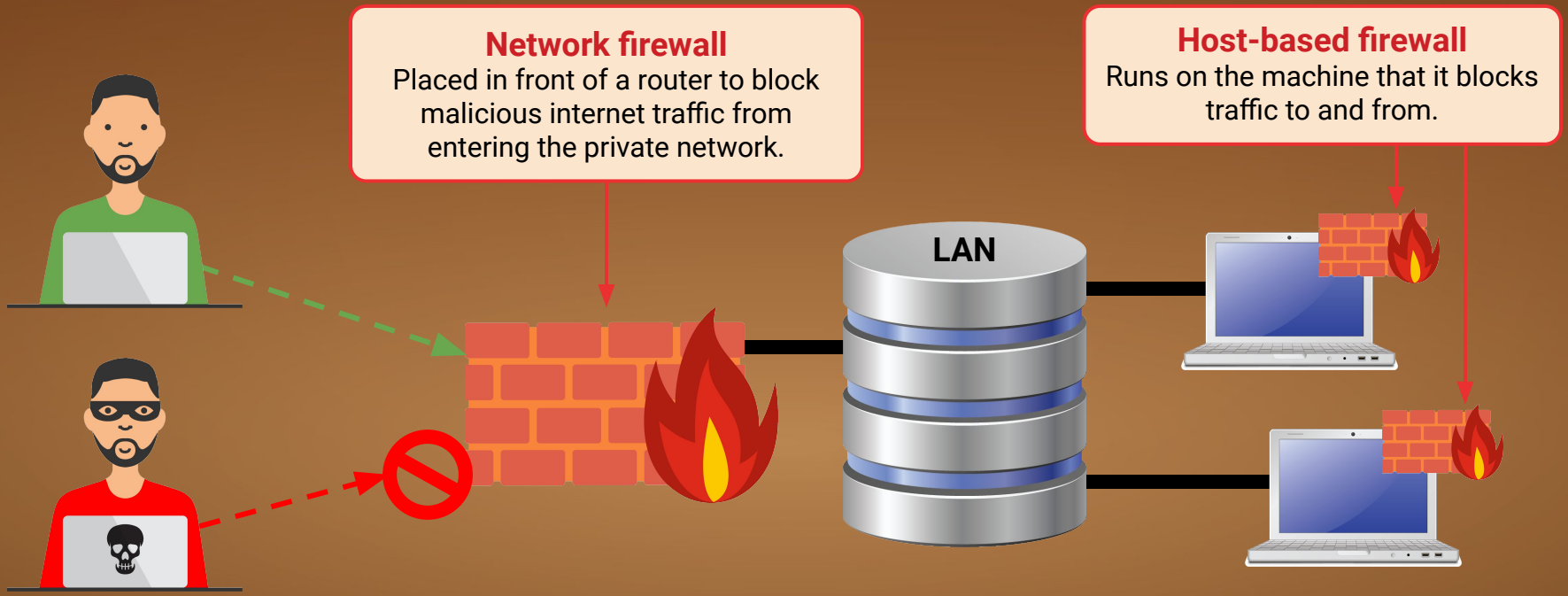
Placed between application servers and routers to provide access control.



Protect trusted networks by isolating them from untrusted networks, like the internet.

Firewalls

Firewalls can be used to either control access to a single host (host-based firewall) or an entire network (network firewall).



Firewalls

Network-based and host-based firewalls work in the same way:

01

Intercept traffic before it reaches its target host or router.

02

Inspect the source and destination address and ports, TCP flags, and other features of the incoming packets.

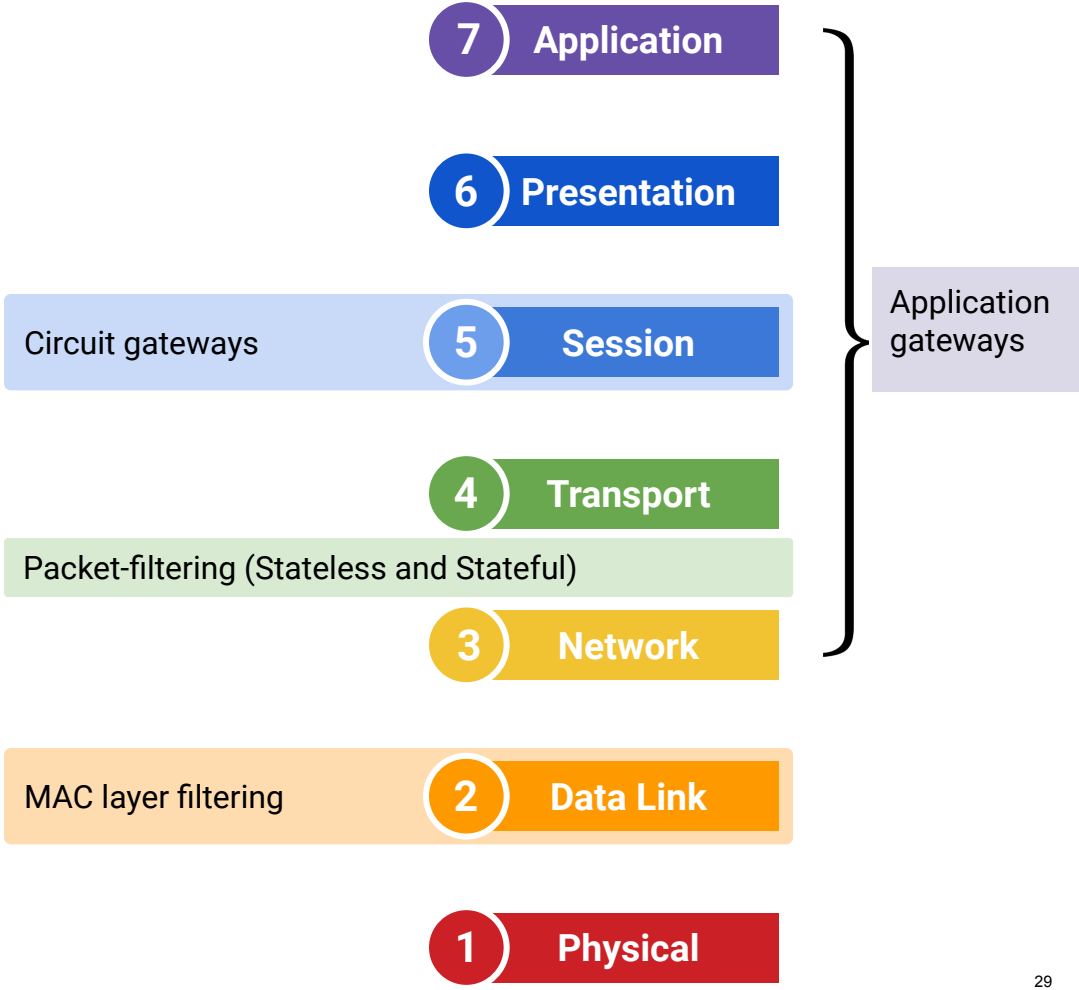
03

Allow packets that come from trusted sources and deny packets that don't.

Firewalls on the OSI

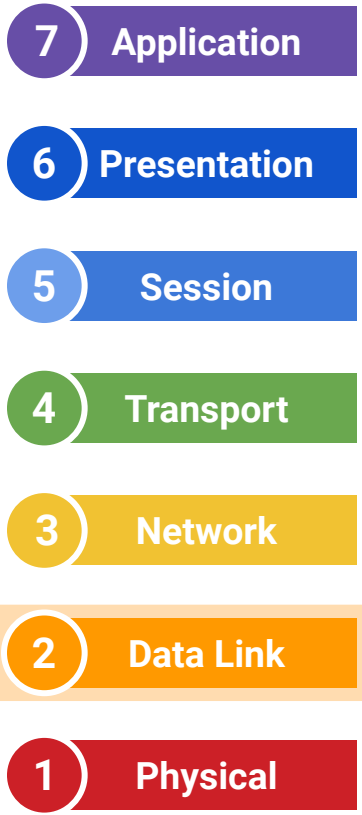
Firewalls operate on multiple layers of the OSI.

They can be broken down into four basic types:



MAC Layer Firewall

MAC firewalls operate on **Layer 2** of the OSI and filter based on source and destination MAC addresses.



Remember: The Media Access Control (MAC) address is a unique hardware ID that helps communicate with each other.

MAC Layer Firewall

Routers compare the MAC address of a device against an approved list.
If there is a match, the traffic is forwarded to that device.

Advantages

Can secure the network from novice attackers.

Disadvantages

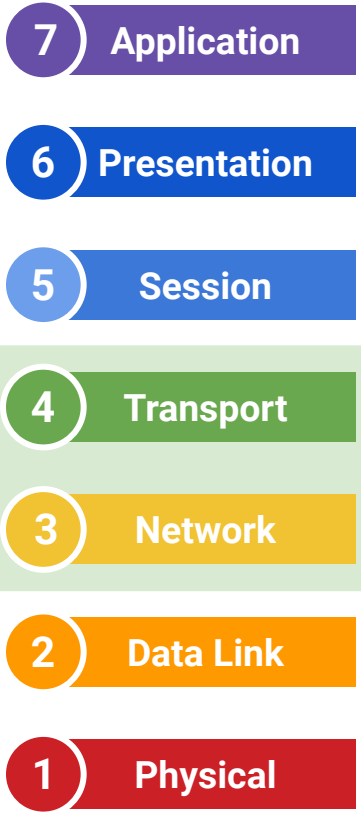
Can be easily bypassed by MAC spoofing.

Packet-Filtering Firewalls (Stateless)

Stateless packet-filtering firewalls operate between **Layer 3** and **Layer 4** of the OSI model.

Use rules based on individual packets:

- Source and destination IP address
- Source and destination port information
- IP protocols
- Ingress and egress interface



Packet-Filtering Firewalls (Stateless)

Stateless packet-filtering firewalls create checkpoints within a router and examine packets as they progress through an interface. If the information does not pass the inspection, it is dropped.

Advantages

Not resource intensive, meaning they are low-cost and do not have a significant impact on system performance.

Work best with small networks.

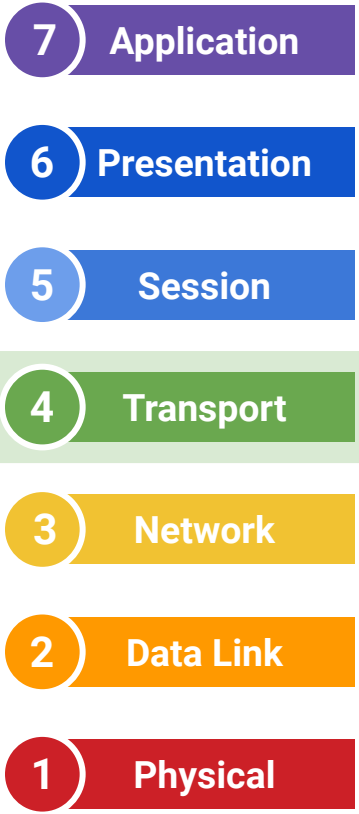
Disadvantages

Easy to subvert compared to more robust firewalls. Only operate at the network layer.

They are vulnerable to spoofing and do not support custom based rule sets.

Packet-Filtering Firewalls (Stateful)

Stateful packet-filtering firewalls operate on **Layer 3** and **Layer 4** of the OSI model.



Rather than look at individual packets, stateful firewalls examine the connection as whole, looking at streams of packets.

They inspect the packets' conversation and routing tables and use a combination of TCP handshake verification and packet inspection technology.

Packet-Filtering Firewalls (Stateful)

Stateful firewalls can determine if a packet is:

- Trying to establish a new connection, known as a NEW state.
- Part of an existing connection, known as an ESTABLISHED state.
- Is neither a new or existing connection, known as a rogue packet.

Advantages

Offer transparent mode, which allows direct connections between clients and servers.

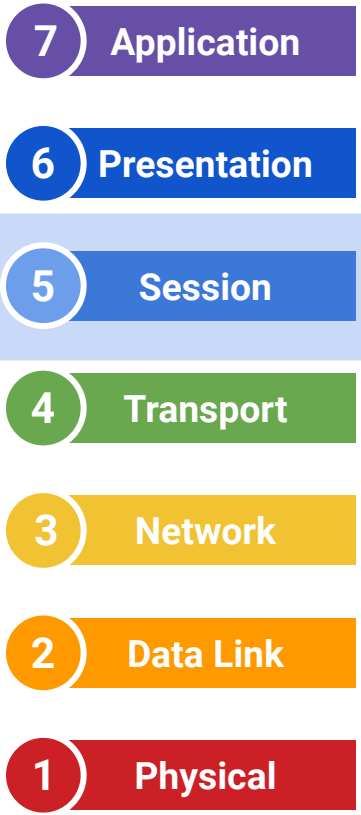
Disadvantages

Are resource-intensive systems.

Circuit-level firewalls

Circuit-level firewalls operate at **Layer 5** of the OSI model.

These firewalls only look at the header of a packet. Once the circuit is allowed to establish an end-to-end connection, all data is tunneled between parties.



Circuit-level firewalls

By verifying the three-way TCP handshake, they ensure that session packets are from legitimate sources.

Advantages

Quickly and easily approve and deny traffic without consuming significant computing resources.

Relatively inexpensive and provide anonymity to the private network.

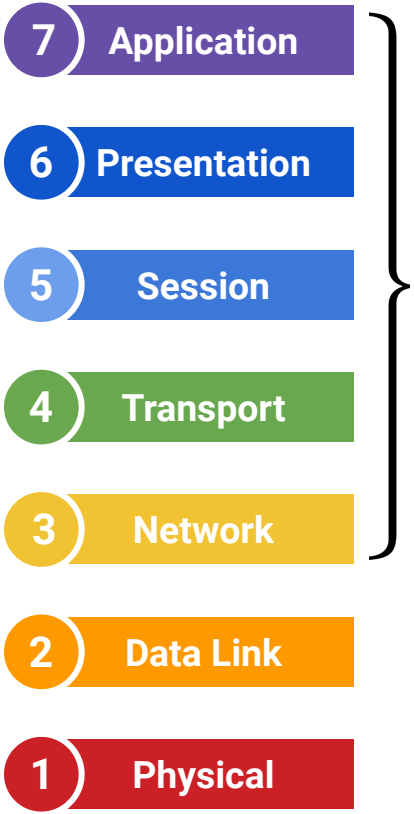
Disadvantages

Do not check the contents of the packet.

If a packet contains malware but has the correct TCP information, the data is allowed to pass through.

Application / Proxy Firewalls

Proxy firewalls operate at **Layer 3** through **Layer 7** of the OSI model.



Proxy firewalls inspect the actual contents of the packet.

It intercept all traffic on its way to its final destination., without the data source knowing. A connection is established to the proxy firewall, which inspects the traffic and forwards it if it's determined to be safe, or drops it if it's determined to be malicious

Application / Proxy Firewalls

Proxy firewalls create an extra layer of protection between the traffic source and its destination behind the network by obscuring the destination from the source creating an additional layer of anonymity and protection for the network.

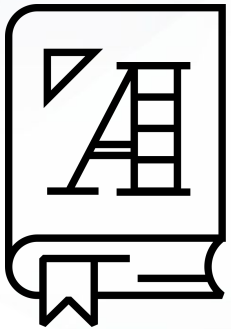
Advantages

More secure than other implementations and provide simple log and file audit management for incoming traffic.

Disadvantages

Resource intensive, requiring robust modern hardware and high costs. Bypassed with encryption.

UFW



A **UFW** is a multifunctional firewall that provides stateless and stateful packet filtering.

Uncomplicated Firewall

UFW provides the following features:

Term	Definition
Host-Based	UFW is most commonly used on hosts.
Logging	UFW has the ability to generate multi-level logs, providing great insight into attacks.
Remote Management	Firewalls can be remotely managed. For example, through SSH via port 22. (*Security concern?)*
Rules for Allow / Deny	Examines source and destination IP addresses, port numbers, and packet types, all without opening the packet. Also uses TCP handshake, packet inspection.
Rate-Limiting	Supports rate-limited connections to protect from brute force attacks.

UFW Demo

In the next demo, we will work with the following scenario:

01

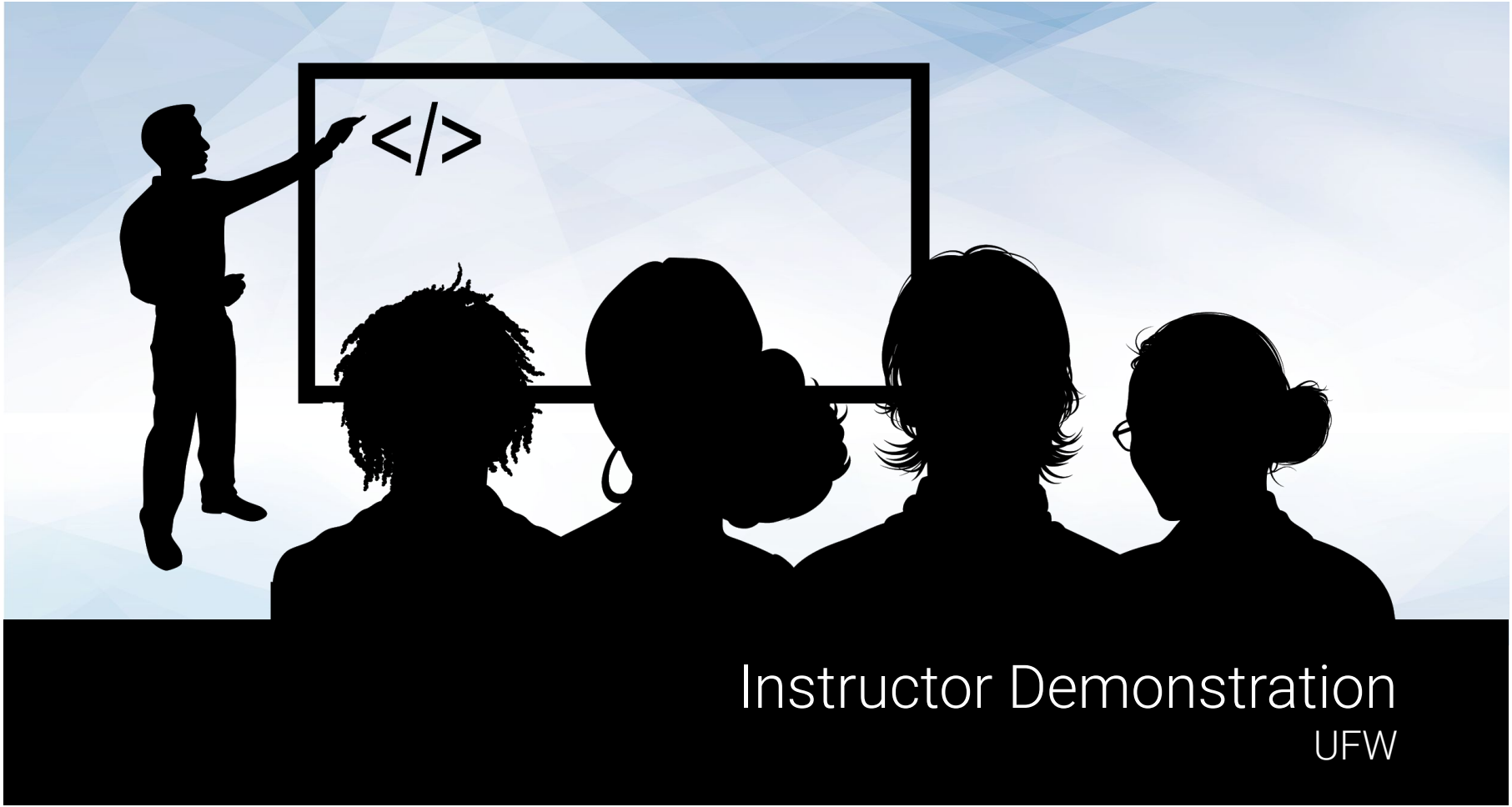
The IT department is hosting a website that requires the use of both normal and encrypted web traffic.

02

Your CISO has released a security advisory authorizing the use of secured remote firewall administration.

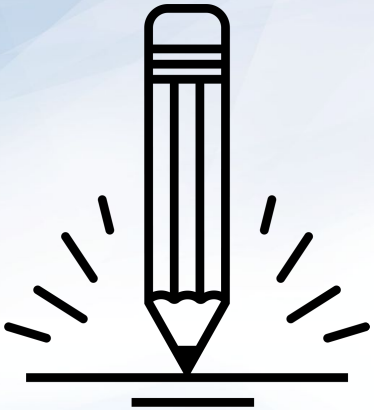
03

Because of this, we need to open ports 22, 80, and 443.



Instructor Demonstration

UFW



Activity: Configuring UFW

In this activity, you will use UFW to harden your system and ensure that your organization complies with PCI DSS (Payment Card Industry Data Security Standard).

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.

Countdown timer

15:00

(with alarm)

firewalld

Introducing firewalld

While UFW allows us to manage multiple networks devices over the command line, it has a major drawback:

- Before firewall rules can be changed or modified, all firewall services must be stopped and restarted. This can be extremely disruptive to an organization's operations.
- **For example:** If you just brought a new host online, you would have to interrupt service on hundreds of other devices before creating a rule for this new host.

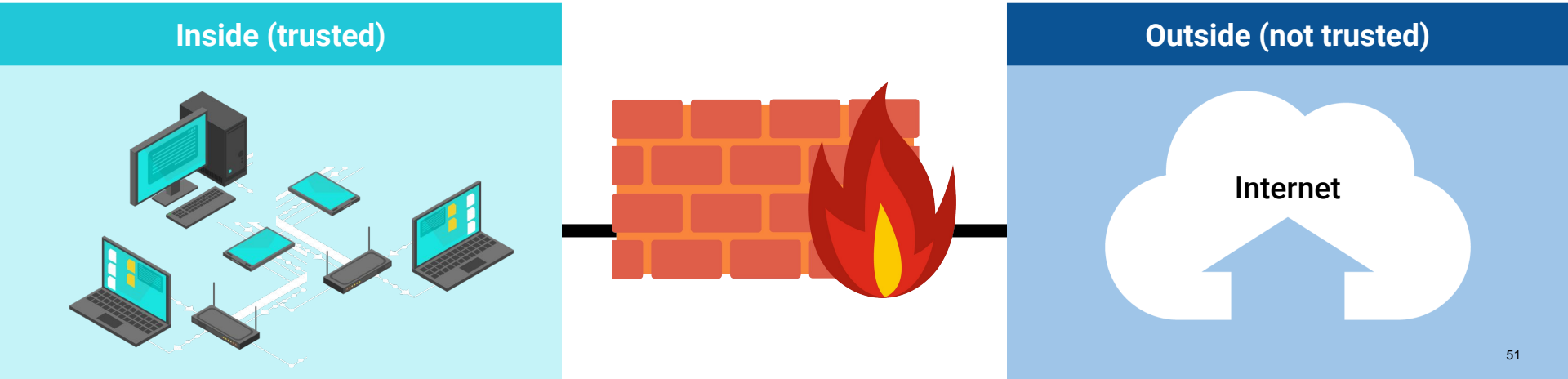
(Source)

firewalld provides similar functionality to UFW but does not require the disruption of services when implementing firewall services.

Introducing firewalld

firewalld uses the concept of **zones** to divide network interfaces into groups of shared trust level. The zones are assigned sets of rules depending on the needs and restrictions of each zone's interfaces.

- Zones are the organization of rules.
- Each zone can contain several rules.
- Through this division of zones, firewalld can manage rulesets *dynamically*, without breaking existing sessions, disrupting services, and bringing down the entire network.



Testing Rules with firewalld

Rules and configurations can be tested in runtime environments.

01 **Runtime configurations**

- Valid until the next system reboot or service reload. Allows us to create settings that are active for a limited amount of time.
- Can be used to test new configurations. Can then be seamlessly saved to permanent environment if deemed good and working.

02 **Permanent configurations**

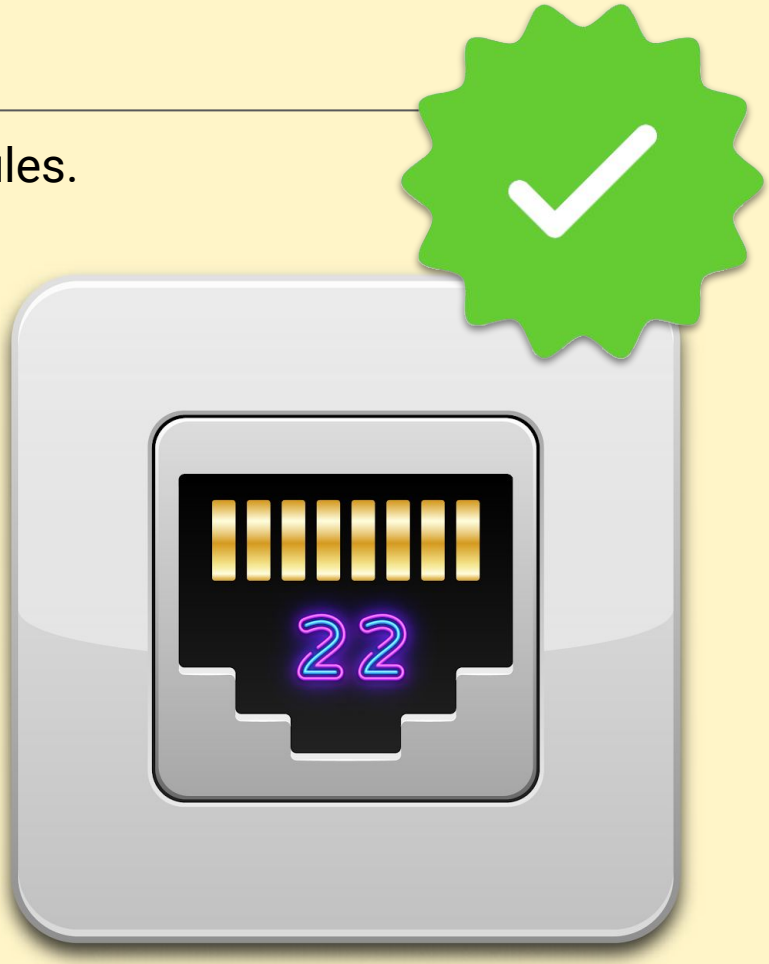
- Loaded with each reboot and reload and become the current runtime environment until new runtime configurations are made.

firewalld and Services

firewalld also uses services to easily configure rules.

- By designating which services you want to allow, firewalld will automatically open the ports associated to those services.

- **For example:**
  If you enable the SSH service in a zone, it will open port 22 without requiring you to specify the port number explicitly.



Firewalld Demo

We will demonstrate firewalld using the following scenario:

01

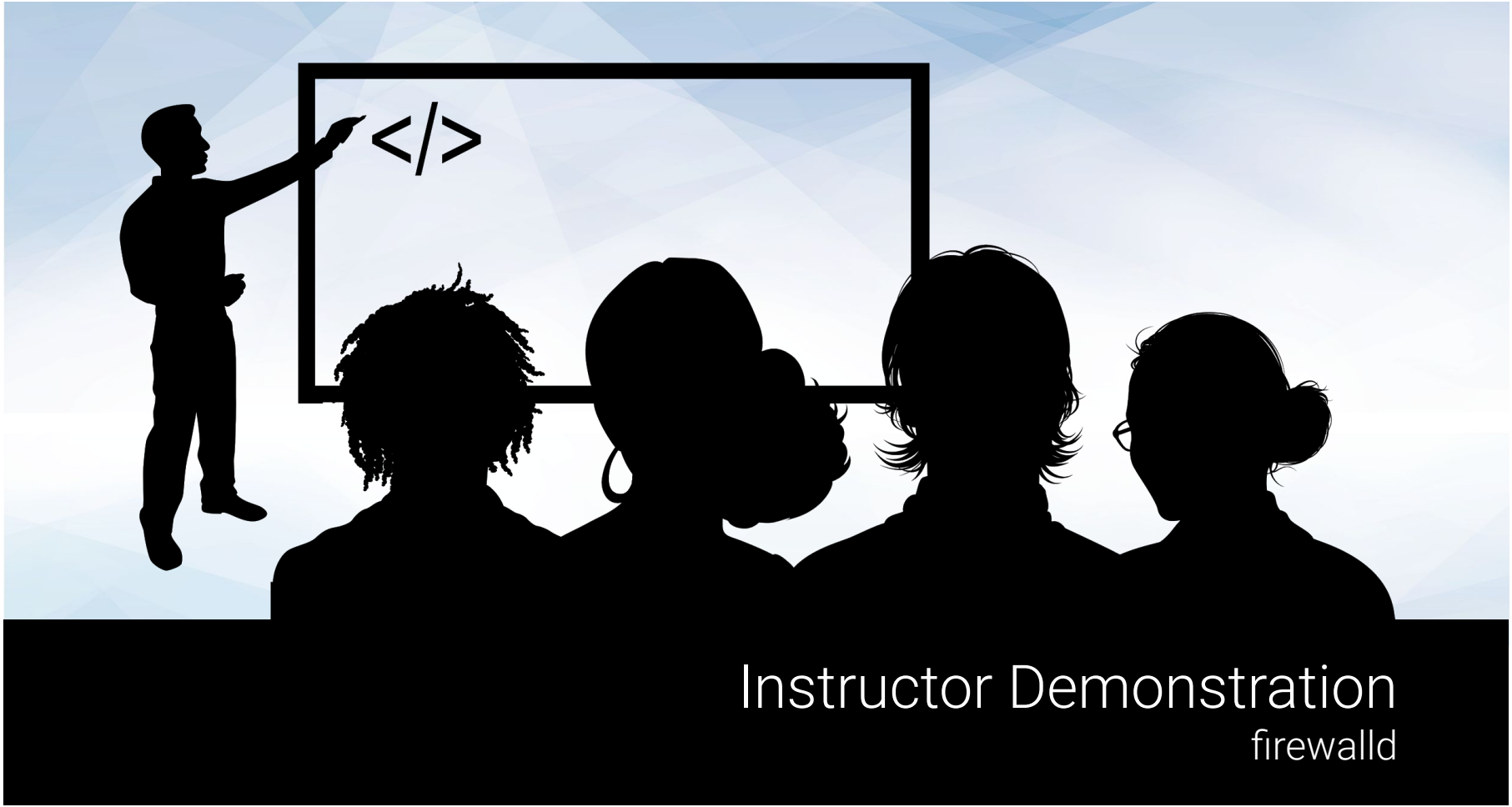
An IT administrator is bringing a new Microsoft Active Directory server online. It will serve several new hosts on the third floor at the main office, which is serviced by eth1 on the firewall.

02

The administrator requested that this new network not be able to transmit or receive data from the Fifth Street office location, which uses an IP address of `10.10.0.10`.

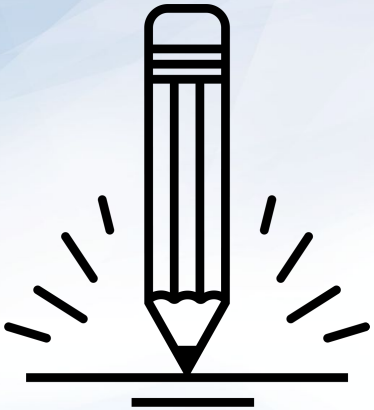
03

Lastly, the administrator asked you to block all ICMP pings on that same interface as an extra level of protection.



Instructor Demonstration

firewalld



Activity: firewalld Configuration

In this activity, you will use firewall to add rules to various zones.

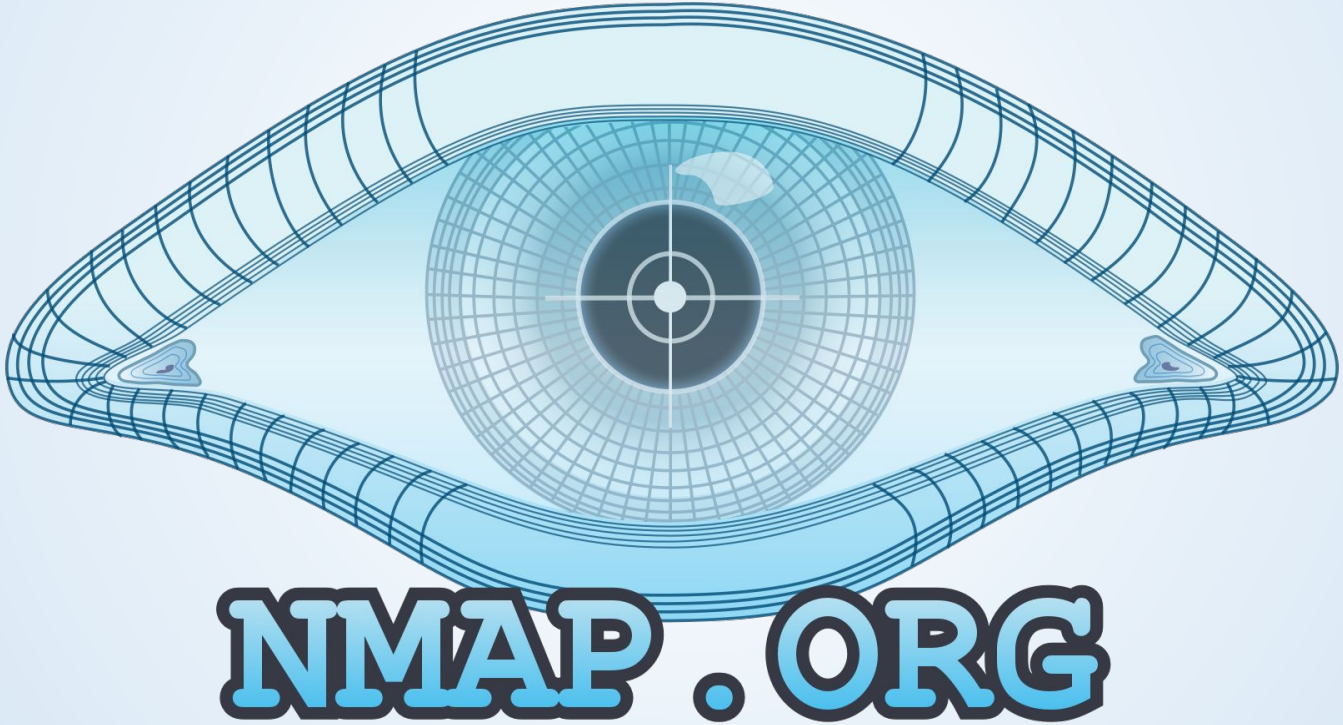
Suggested Time:
20 Minutes

Time’s Up! Let’s Review.

Testing Rules with Nmap

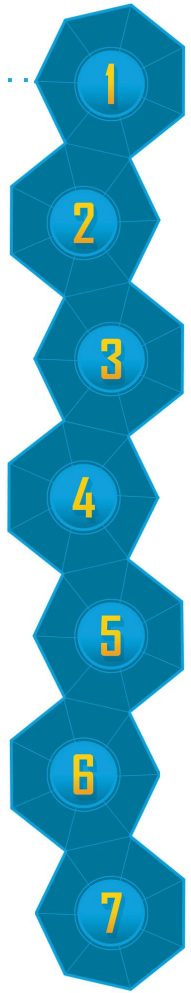
Nmap

Nmap is the industry-standard network scanner.



The first step of the cyber kill chain is **reconnaissance**, in which attackers perform information gathering.

Reconnaissance
Information gathering against a target.



Nmap

Attackers can get the following from network scans:

- Name and version of operating system (OS fingerprinting).
- All open and closed ports.
- All filtered ports (ports behind a firewall).
- Types of services running on a specific port (service and daemon names).
- **Firewalking** allows attackers to perform network analysis to determine which Layer 4 protocols a specific firewall allows.

Nmap Demo

In the following demonstration, we'll perform scans against our UFW firewall. Consider the following scenario:

01

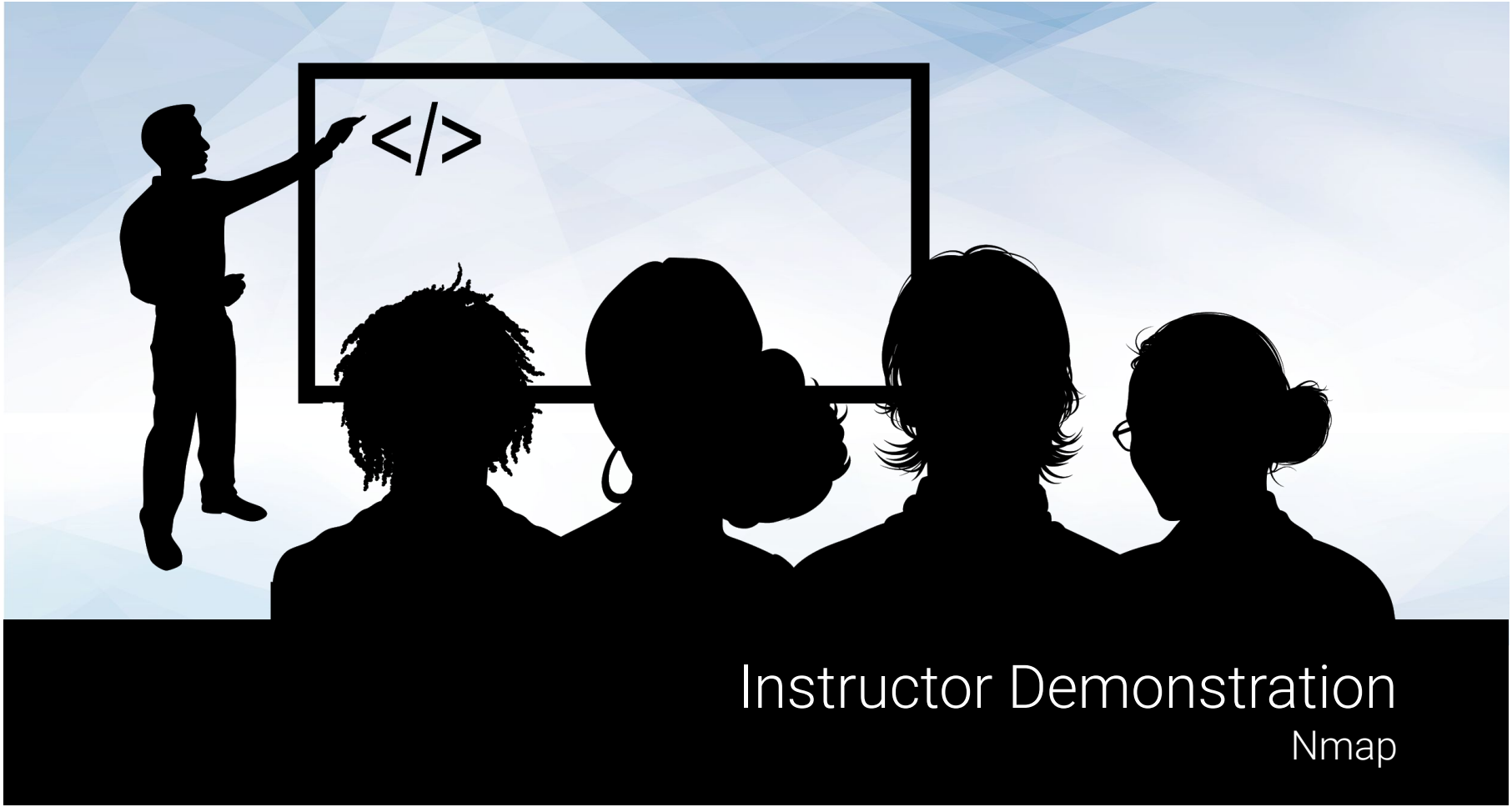
Your security manager has installed a brand new, fully configured firewall and would like you to test it using Nmap.

02

You will use various fingerprinting techniques to reveal the type of operating system, services, daemons, and protocols currently running.

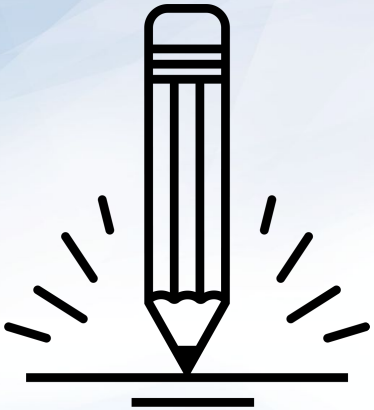
03

You will also test to see which ports are open, closed, and filtered.



Instructor Demonstration

Nmap



Activity: Testing Firewall Rules with Nmap

In this activity, you will perform various network scans to test firewall integrity.

Suggested Time:
10 Minutes

Time’s Up! Let’s Review.

Questions?


The End