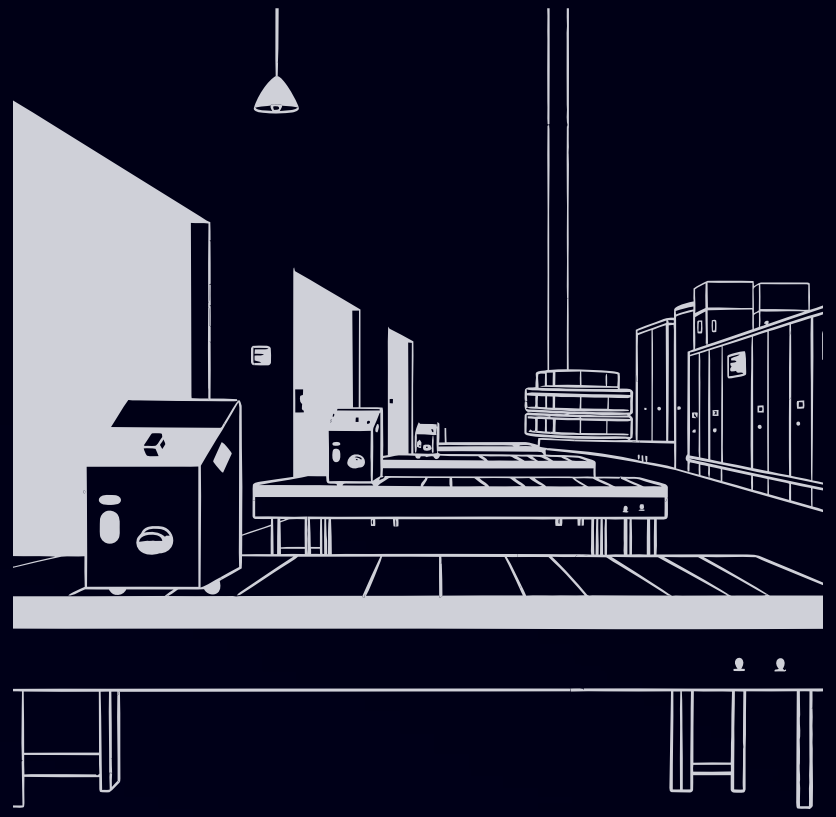
Network Security and Hacking

An exploration of attack and defense methods in modern network security



Presentation Outline

A roadmap of the key topics we'll explore in this deep dive into network security and hacking.

1

Foundations of Hacking & Pentesting

Defining penetration testing, understanding different hacker types, legal context, and ethical considerations.

2

Vulnerability Management

Exploring various methods for disclosing vulnerabilities and the role of bug bounty programs.

3

Offensive Tactics & Reconnaissance

Understanding the Cyber Kill Chain, common network attacks, and techniques for gathering intelligence.

4

Network Defense Strategies

Implementing defensive frameworks, utilizing firewalls, IDS, NAT, honeypots, and attack classification.

What is Penetration Testing?

Penetration testing (often called "pen testing") is a simulated cyber attack against a computer system, network, or web application to check for exploitable security vulnerabilities.

Simulated Attack

Actively mimics real-world attacker techniques to identify weak points before malicious exploitation occurs.

Vulnerability Discovery

The primary goal is to uncover security flaws, misconfigurations, and other exploitable weaknesses.

Enhanced Security

Provides actionable findings and recommendations to significantly improve an organization's security posture.

What is a Hacker?

A hacker is an individual who uses their technical skills to overcome a problem or challenge, often pertaining to computer systems. While commonly associated with malicious activities, the term encompasses a broad spectrum of intentions and ethics.

White Hat

Ethical hackers who use their skills to identify and fix vulnerabilities, working to improve system security.

Black Hat

Malicious actors who exploit system weaknesses for unauthorized access, data theft, or disruption.

Grey Hat

Operate in a morally ambiguous space, often finding vulnerabilities without permission but disclosing them responsibly.

Hacker vs. Penetration Tester

While both roles involve deep technical knowledge of systems and vulnerabilities, their intent, legality, and ultimate goals couldn't be more different.

Penetration Tester

Operate with explicit authorization to identify and report security vulnerabilities, upholding strict ethical and legal standards to enhance system defense.

(Black Hat) Hacker

Act without authorization to exploit weaknesses for personal gain or harm, disregarding ethical principles and legal consequences, often leading to unauthorized access or data theft.

History of Hacking and Legal Context

Early Perception

Initially, hacking was viewed strictly as criminal activity involving unauthorized access and exploitation, setting the stage for legal regulation.

1986 Computer Fraud and Abuse Act

The CFAA established a legal framework criminalizing unauthorized computer access, fraud, and related offenses, distinguishing lawful research from malicious acts.

Legal and Ethical Distinctions

Laws led to clear distinctions between black hat hackers, white hats, and the emergence of grey hats operating in ethical and legal grey areas.

Early Laws and Their Impact

Computer Fraud and Abuse Act (CFAA)

Enacted in 1986, the CFAA criminalizes unauthorized computer access and fraud. While targeting malicious hacking, it also poses legal risks for legitimate vulnerability researchers.

Digital Millennium Copyright Act (DMCA)

Passed in 1988, the DMCA prohibits bypassing digital rights management (DRM). This can impact cybersecurity research by criminalizing certain vulnerability explorations.

Ethics in Hacking

Lawful Operation of Ethical Hackers

Ethical hackers operate strictly within legal boundaries and ethical standards, distinguishing themselves through authorized actions aimed at enhancing cybersecurity.

Variability of Ethics in Hacking

Ethical standards in hacking vary based on individual morals, legal frameworks, and situational context, often requiring organizations to define specific codes of conduct.

Vulnerability Disclosure Methods

Understanding Vulnerabilities

Vulnerabilities are exploitable weaknesses in software that attackers can use to compromise systems or gain unauthorized access, posing significant cybersecurity risks.

Full Vendor Disclosure Method

This method involves privately reporting vulnerabilities only to the vendor, allowing controlled patching without public exposure, enhancing safety but possibly delaying fixes.

Coordinated Disclosure Explained

Vendor Patch Window

Coordinated disclosure provides vendors with a 60-90 day window to fix vulnerabilities before public release, balancing timely patching with minimizing exploitation risks.

CERT/CC's Role

CERT/CC acts as a key intermediary between vulnerability researchers and vendors, facilitating responsible communication and ensuring adherence to disclosure timelines.

Full Public Disclosure Pros and Cons

Pressure for Swift Fixes

Public disclosure compels vendors to address vulnerabilities promptly by exposing issues to a wide audience.

Enhanced Transparency

Making vulnerability information public enhances openness and allows the cybersecurity community to stay informed about threats.

Increased Community Awareness

Public disclosure enables users and security professionals to understand risks and implement timely mitigations effectively.

Full Vendor Disclosure Pros and Cons

In full vendor disclosure, vulnerabilities are exclusively reported to the vendor, with no public details released to ensure controlled handling and patching.

Enhanced Public Safety

This method prevents premature public exposure of vulnerabilities, allowing vendors to develop and distribute patches without risk of immediate exploitation.

Controlled Patch Management

Vendors can effectively manage the patching process, ensuring solutions are thoroughly tested and widely available before information about the flaw becomes public.

Delayed Public Awareness

The lack of public disclosure means users may remain unaware of critical vulnerabilities for an extended period, potentially delaying their ability to take protective measures.

Reduced Accountability Pressure

Without public scrutiny, vendors might face less pressure to prioritize and promptly fix vulnerabilities, potentially leading to slower patch development and deployment.

Bug Bounty Programs

Inception

Bug bounty programs began at Netscape in 1995, establishing organized incentives for security researchers to report vulnerabilities.

Incentives Offered

Programs provide monetary rewards ranging from $150 to over $15,000, along with recognition and exclusive perks to motivate researchers.

Controversies and Incentives in Bug Bounties

Challenges in Vendor-Researcher Relations

Bug bounty programs often struggle with issues such as unfair researcher ranking, poor communication, and conflicts over duplicate reports, hindering effective collaboration and recognition.

Evolution of Bug Bounty Incentives

Initially, incentives were simple swag and recognition. Over time, they have evolved to include substantial financial rewards and exclusive perks, significantly boosting researcher motivation and ethical contributions.

Understanding the Enemy: Black Hats

Criminal Intent

Black hats are malicious hackers driven by personal gain through illegal and harmful activities, causing significant damage to various targets.

Strategic Understanding

Following Sun Tzu’s principle, knowing black hats’ motivations and methods is essential to anticipate and effectively counter cyber attacks.

Advanced Persistent Threats (APTs)

APTs represent sophisticated, well-funded adversaries conducting long-term, stealthy cyber intrusions with advanced tactics and prolonged system access.

Cyber Kill Chain Overview

Seven Phases of a Cyber Attack

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control (C2)
7. Actions on Objectives

The Cyber Kill Chain model outlines these distinct phases from initial reconnaissance to achieving the attacker's objective.

Primary Goal of the Cyber Kill Chain

The main objective is to detect and disrupt attacks early in their progression to prevent critical damage and thwart attacker efforts.

Cyber Kill Chain

Detailed Phases: C2, Objectives, Exploitation, Installation

Command & Control (C2)

Attackers establish covert communication channels to maintain control over compromised systems through methods like beaconing, tunneling, and encryption.

Attacker Objectives

The primary goals for attackers often involve data exfiltration, deploying ransomware, and achieving lateral movement for elevated access within the target network.

Exploitation & Installation

Exploitation leverages vulnerabilities to trigger payload execution, followed by the installation of backdoors or Remote Access Trojans (RATs) for persistent access.

Weaponization, Delivery, and Reconnaissance

Weaponization

This phase involves crafting or customizing malware and exploit code designed to leverage vulnerabilities for unauthorized access or malicious actions.

Delivery

The crafted payload is transmitted to target systems using various methods, such as phishing emails or web-based exploits, to infect them.

Reconnaissance

Attackers gather critical information about the target, identifying potential vulnerabilities and entry points before initiating any attack.

Defensive Frameworks and Summary

Effective cybersecurity defense strategies are built upon understanding and countering threats with robust frameworks.

Core Defensive Actions

Effective cybersecurity defense involves detecting attacks early, denying attacker access, and disrupting their efforts to increase operational costs for adversaries.

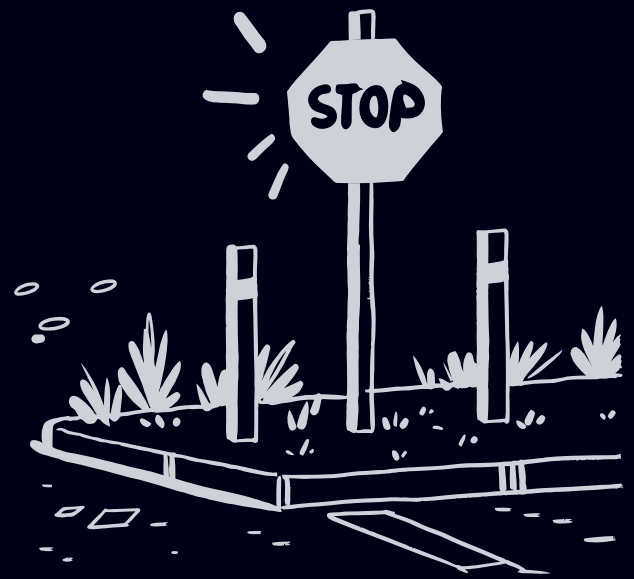
MITRE ATT&CK Framework

MITRE ATT&CK is a detailed knowledge base of adversary tactics, techniques, and procedures, used to enhance threat intelligence and improve defense strategies.

Integrated Defense

Combining ethical hacking with structured frameworks like MITRE ATT&CK enables proactive defense and strengthens overall cybersecurity posture effectively.

Shifting Focus



Common Network Terminology

IP Address

A unique numerical label assigned to each device on a network, enabling identification and location for communication.

Router

A device that directs data packets between different computer networks, crucial for traffic flow on the Internet.

Firewall

A security system that monitors and controls network traffic, acting as a barrier between trusted and untrusted networks.

Packets

Packets are small units of data transmitted over a network, containing both the payload (actual data) and control information such as source and destination addresses. Understanding how packets flow through the network is essential for monitoring and securing communications.

Switch

A switch is a networking device that connects multiple devices within the same network, facilitating efficient data transfer by forwarding packets only to the intended recipient device, reducing network congestion.

Hub

A hub is a basic networking device that connects multiple computers in a network, but unlike a switch, it broadcasts incoming data packets to all connected devices, which can lead to collisions and reduced network efficiency.

What is a Computer Network?

A computer network is a system of interconnected computing devices that can exchange data and share resources with each other, forming the fundamental backbone of modern digital communication.

Interconnectivity

Networks link diverse devices through wired or wireless connections, ensuring seamless data flow across the system.

Resource Sharing

Devices enable the sharing of hardware like printers and software applications, boosting overall efficiency and access.

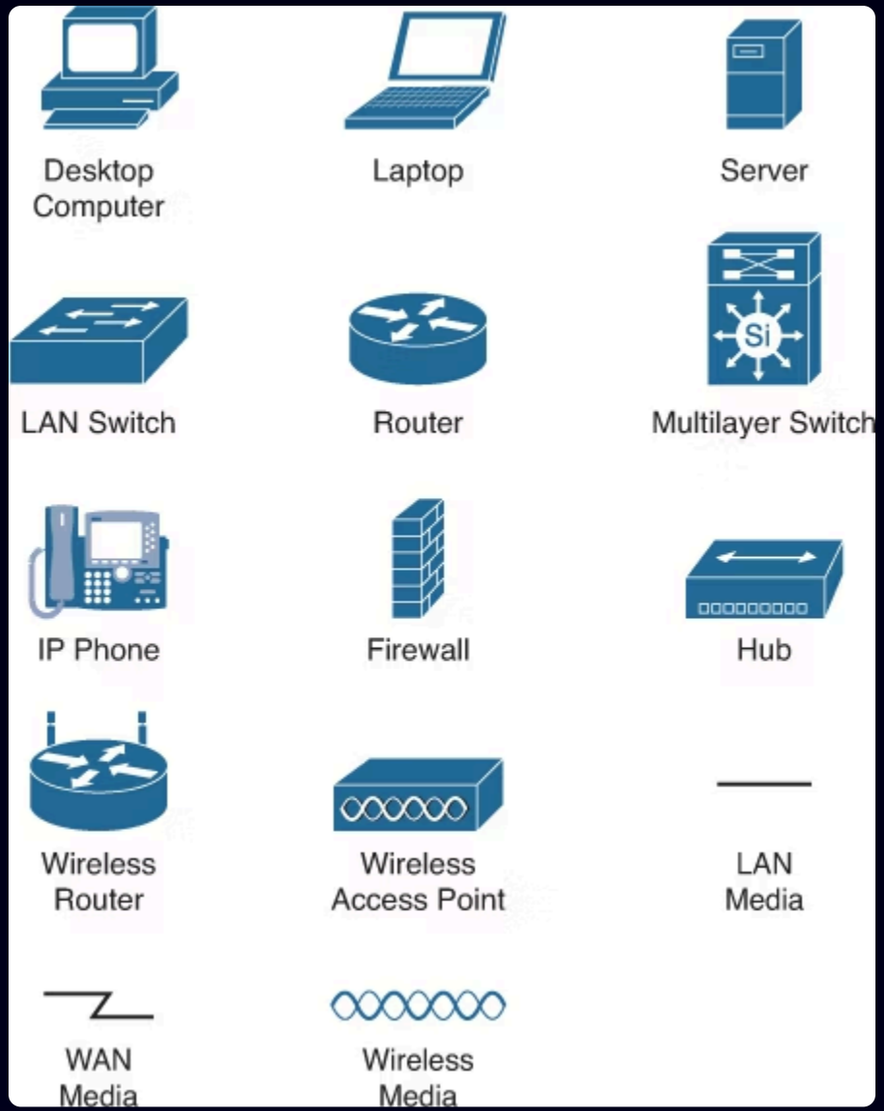
Communication & Collaboration

Networks facilitate instant communication via email, messaging, and video conferencing, enhancing teamwork and collective efforts.

Data Exchange

They ensure efficient and secure transfer of information, supporting distributed data processing and real-time access to shared databases.

Common Network Topology Symbols



Network Topology

Network topology refers to the physical or logical arrangement of connected devices in a computer network. It defines how data flows between different nodes and impacts network performance, reliability, and cost.

Star Topology

All devices connect to a central hub. Easy to manage and identify faults, but the central hub is a single point of failure.

Bus Topology

All devices share a single communication line. Simple and inexpensive to implement, but a break in the main cable disrupts the entire network.

Ring Topology

Each device is connected to exactly two other devices, forming a single continuous pathway for signals. Data flows in one direction, can be slow and a single node failure can take down the network.

Mesh Topology

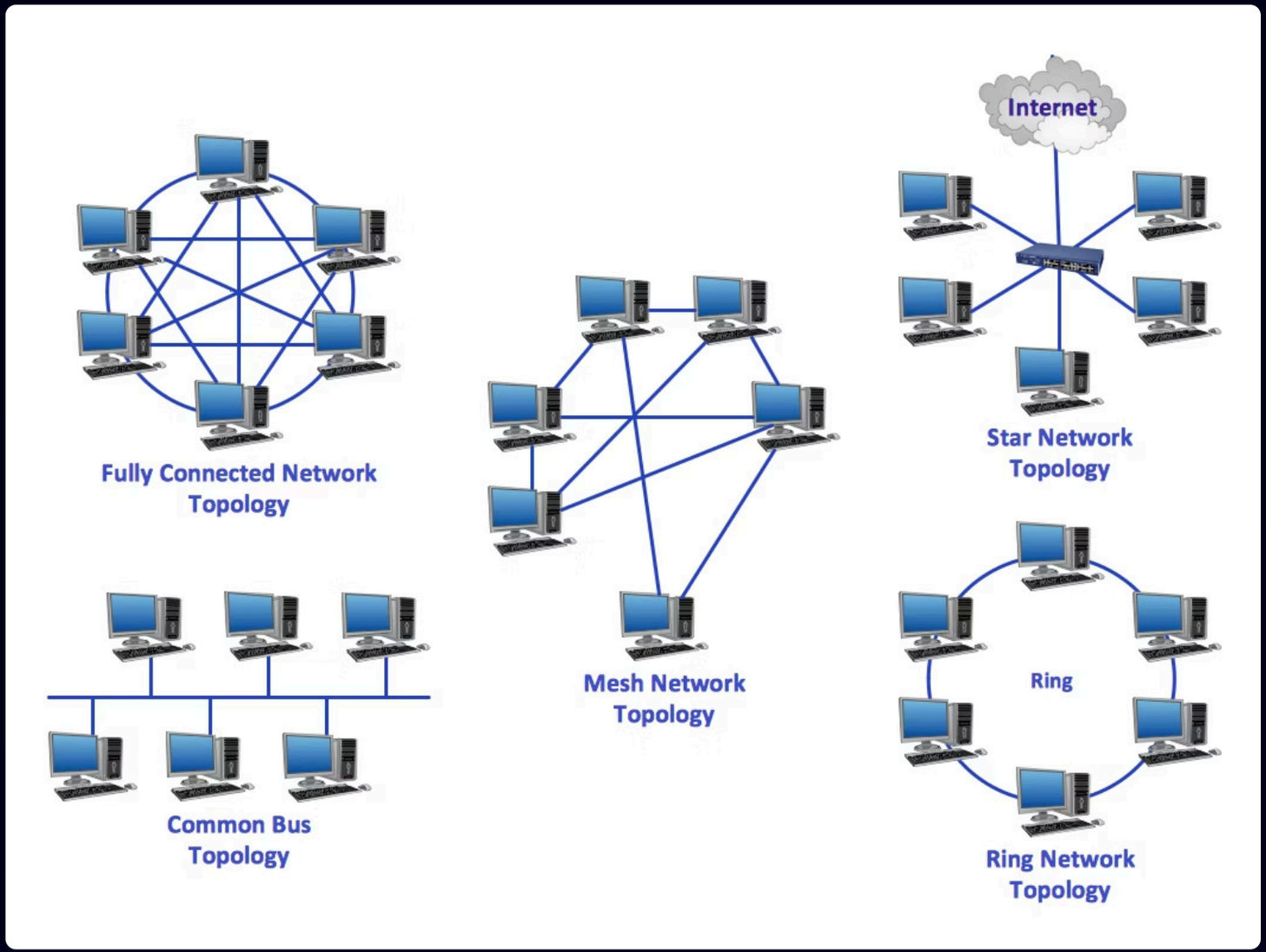
Every device is interconnected with every other device, creating multiple redundant paths. Highly reliable and fault-tolerant but complex and expensive to implement.

Hybrid Topology

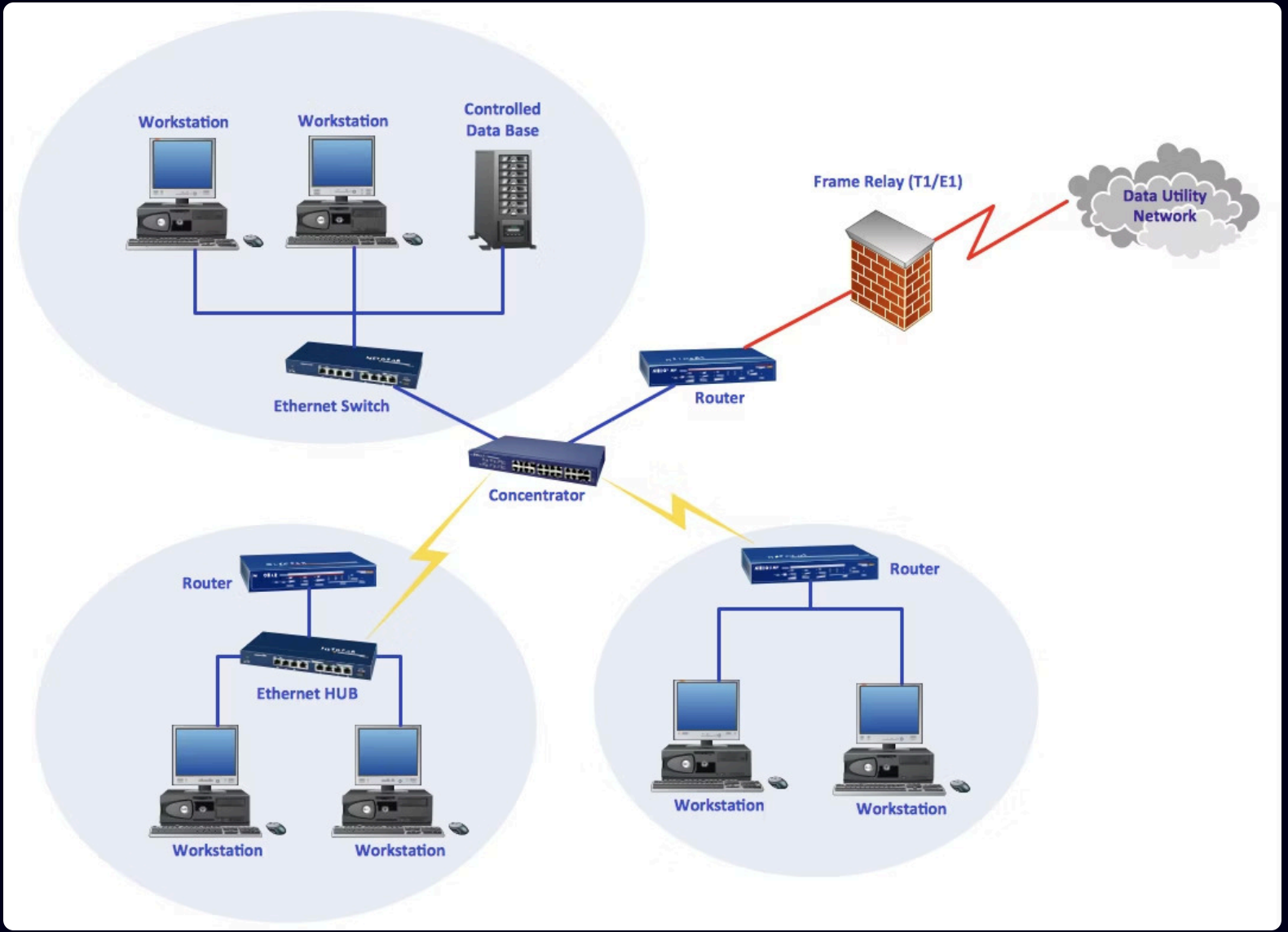
A combination of two or more different topologies. Offers flexibility and scalability but can be more complex to manage due to its varied structure.

Network Topology

Network topology refers to the physical or logical arrangement of connected devices in a computer network. It defines how data flows between different nodes and impacts network performance, reliability, and cost.



Network Topology Example



Tools to help you create your own network diagram

app.diagrams.net

Flowchart Maker & Online Diagram Software

draw.io is free online diagram software for making flowcharts, process diagrams, org charts, UML, ER and network diagrams

Network Attacks

Typical Attack Sequence

Identification of Target

Selecting the victim system or network

Reconnaissance

Gathering information about the target

Intrusion

Gaining unauthorized access

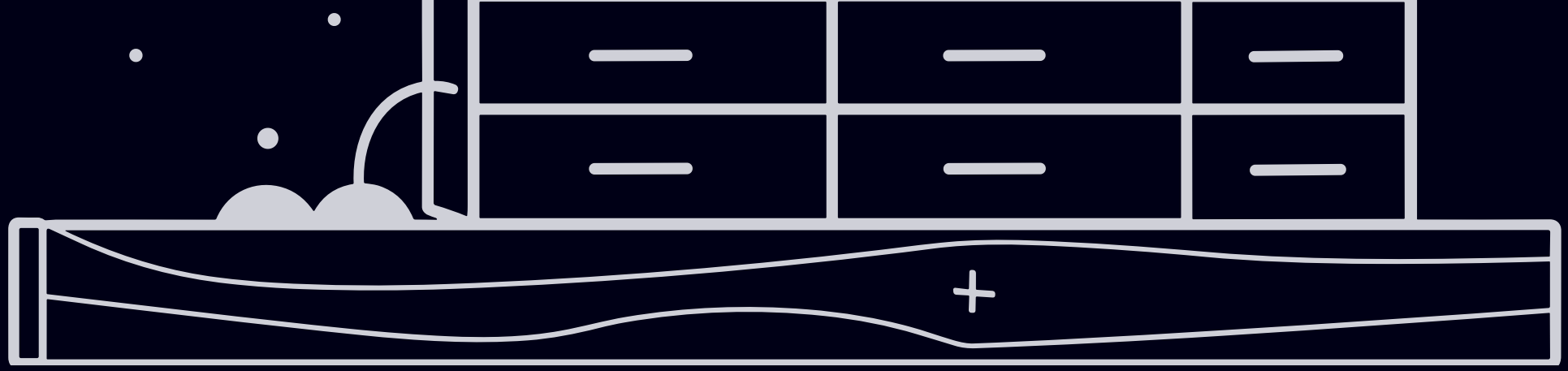
Doing Damage

Executing the attack objective

Covering Up

Hiding evidence of the attack

These steps are repeated as needed throughout the attack lifecycle



Footprinting: Profiling a Network

Domain Information

Gathering domain name details

IP Blocks

Identifying IP address ranges

Service Enumeration

Discovering TCP and UDP services

System Enumeration

- Operating System
- Network Type
- User Names and Groups

Non-Network Search

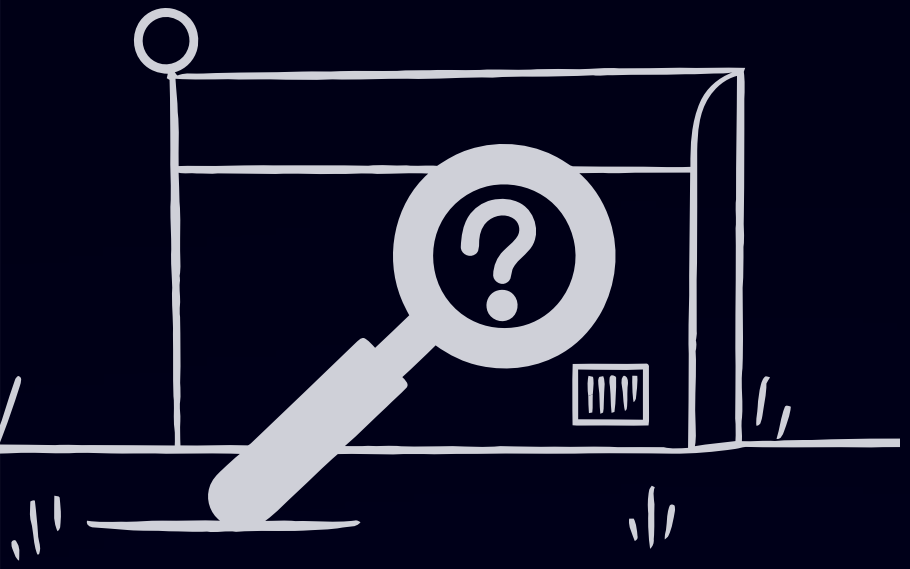
Public Records

Edgar Database (Http://www.sec.gov/)

- 10-Q Reports
- 10-K Reports

These can reveal new acquisitions which are often most vulnerable due to lack of integration

Public information can provide valuable intelligence for attackers



Network Enumeration: WHOIS Servers

Many companies register domain names through various registrars

General WHOIS Resources

- Directory list at http://www.internic.net/
- WHOIS search at http://www.allwhois.com/

Regional WHOIS Servers

- European: http://www.ripe.net/
- U.S. military: http://whois.nic.mil
- U.S. government: http://whois.nic.gov

Exploring Illinois State

www.whois.com

Whois.com – Free Whois Lookup

Whois Domain Name & IP lookup service to search the whois database for verified registration information

WHOIS Information Revealed:

Domain Name: ILSTU.EDU

Registrant: Illinois State University 3380 Administrative Technologies Normal, IL 61790-3380 USA

Administrative Contact: Domain Admin Illinois State University 3380 Administrative Technologies Normal, IL 61790 USA +1.3094383611 email@ilstu.edu

Technical Contact:

Illinois State University
3500 Telecommunications
Normal, IL 61790
USA
+1.3094383611
email@ilstu.edu

Name Servers: ENS1.ILSTU.EDU AWSENS2.ILSTU.EDU

Domain record activated: 11-Jan-1995 Domain record last updated: 04-Dec-2024 Domain expires: 31-Jul-2027

This publicly available information provides attackers with valuable reconnaissance data

IP Block Information

Steps to find

1. use ping command of domain
2. whois lookup of ip

Illinois State IP Details:

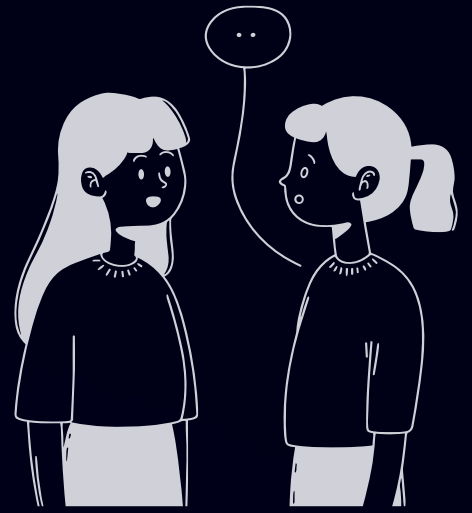
```
NetRange:       138.87.0.0 - 138.87.255.255
CIDR:           138.87.0.0/16
NetName:        ILSTU
NetHandle:      NET-138-87-0-0-1
Parent:         NET138 (NET-138-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Illinois State University (ISU-3-Z)
RegDate:        1990-04-19
Updated:        2023-12-01
Ref:            https://rdap.arin.net/registry/ip/138.87.0.0
```

This information helps attackers understand the network structure and potential points of contact

Zone Transfer

A special type of query that asks a name server for the entire contents of a Zone.

- Cached records are never reported in a zone transfer
- Zone transfers are usually used by secondary servers to update their own zone data from the primary server
- Attackers can use zone transfers to discover internal network structure



Hackers often look for mail servers because they provide clues about firewall location

Finding More About a Domain

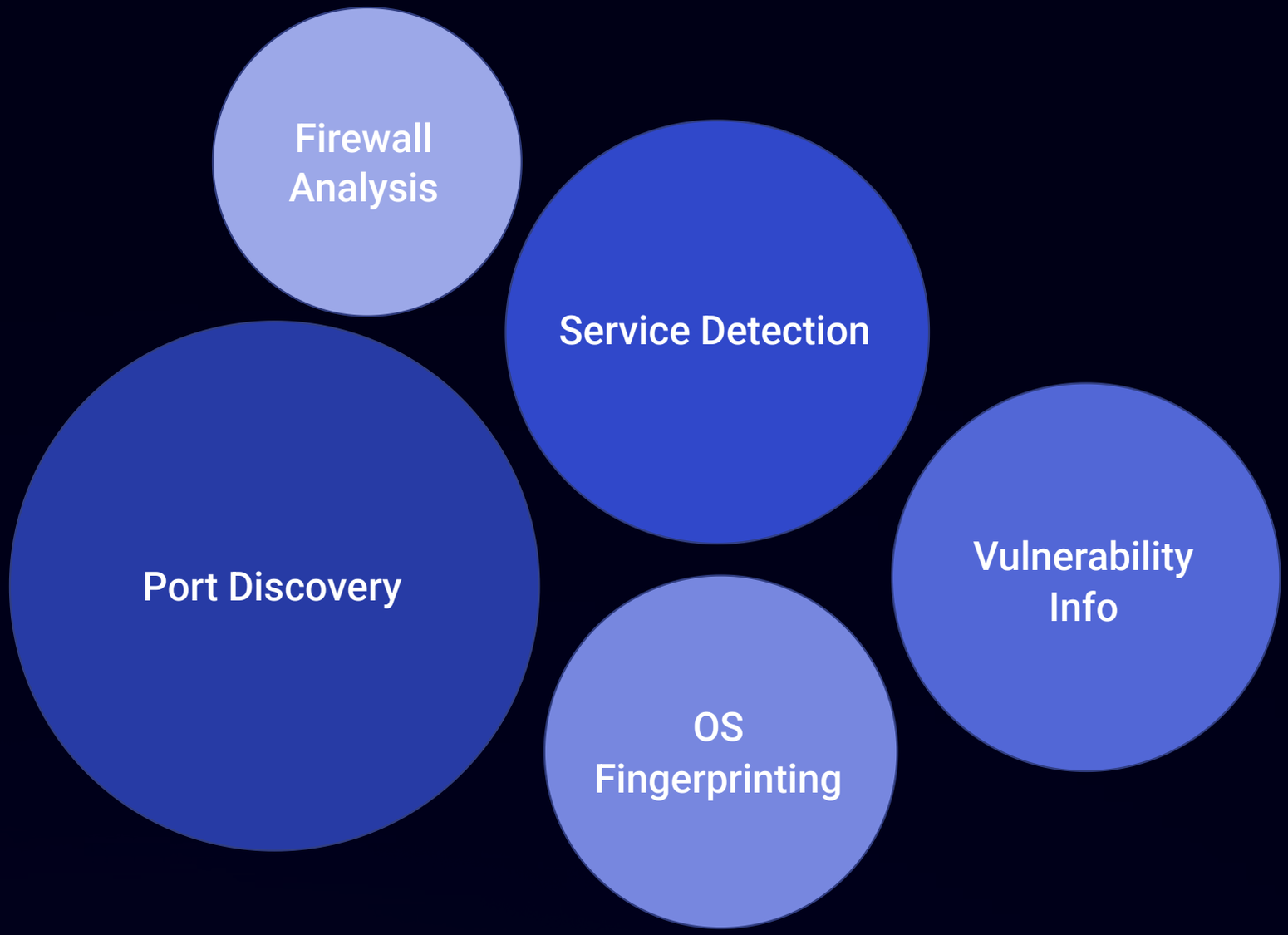
Using nslookup Tool:

```
spsand1@pop-os:~$ nslookup 8.8.8.8
8.8.8.8.in-addr.arpa    name = dns.google.
```

DNS Records to Look For

- A-records: Link domain names to IP addresses
- MX records: Mail servers with priority settings
- CNAME records: Alias host names to other host names
- Other entries: Kerberos servers, LDAP servers, etc.

Nmap Uses


Firewall Analysis
Service Detection
Port Discovery
Vulnerability Info
OS Fingerprinting

Nmap Commands

Basic Host Scan

```
nmap <target>
```

Performs a basic scan to identify live hosts and open ports.

SYN Stealth Scan

```
nmap -sS <target>
```

Executes a fast, stealthy SYN scan, often used to bypass firewalls and avoid logging.

Service and Version Detection

```
nmap -sV <target>
```

Attempts to determine the version of services running on open ports.

Operating System Detection

```
nmap -O <target>
```

Enables OS detection to identify the target's operating system.

Aggressive Scan

```
nmap -A <target>
```

Activates an aggressive scan mode, which includes OS detection, version detection, script scanning, and traceroute.

Scan Specific Ports

```
nmap -p <port_range> <target>
```

Scans only the specified port or range of ports (e.g., -p 22,80,443 or -p 1-1000).

Other Reconnaissance Means

Target Identification

Identify target from footprinting results

System Scanning

Use tools like LanGuard to scan systems

OS Fingerprinting

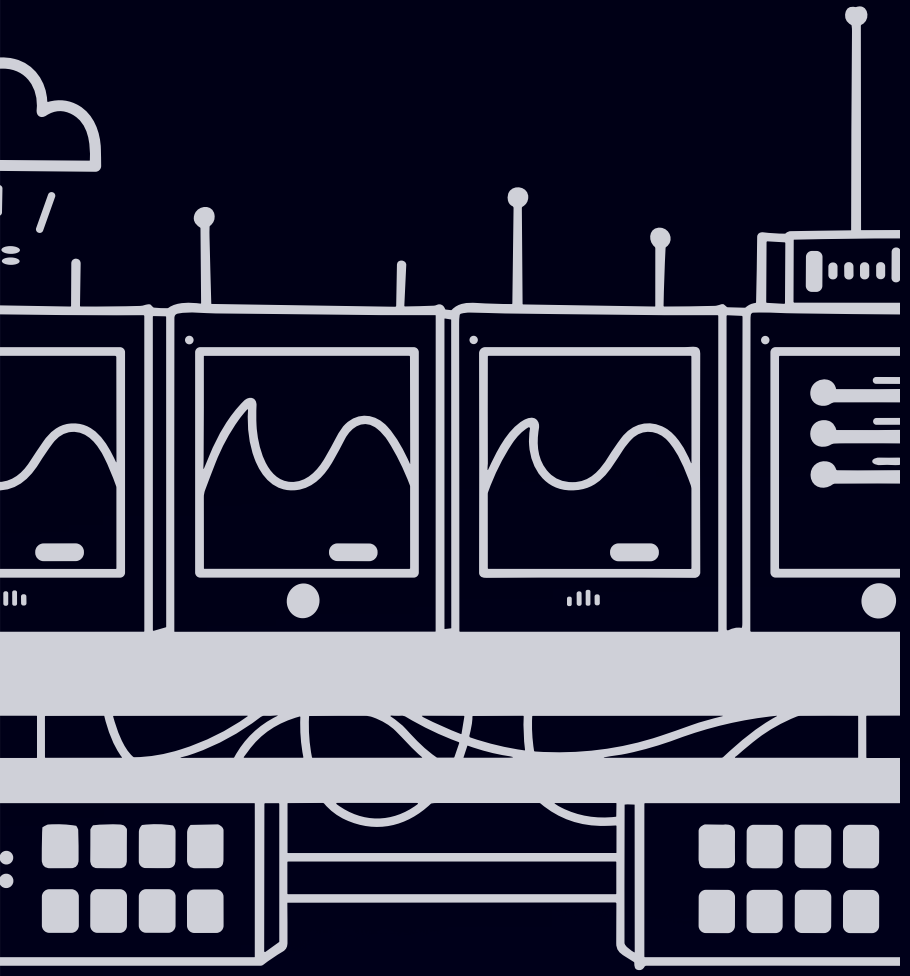
Use TCP packets (often malformed) to identify the target operating system

Banner Grabbing

Examine raw responses from services like HTTP or FTP headers

Vulnerability Assessment

Find vulnerabilities to break in, install backdoors, or launch attacks



Network Defense Overview

Protection

- Firewalls
- Network security threats
- Firewall functionality

Detection

- Intrusion detection systems
- Honeypots
- Monitoring techniques

Companies are creating decentralized computing architectures with centralized corporate network security policies. This center is protected from intruders by firewalls.

IP Packet Screening Routers

- Static data traffic routing service placed between ISP router and corporate network
- Uses screening rules to permit or deny incoming IP packets
- Example rule: If source IP address involves .edu, and protocol is TCP or ICMP, allow access to TCP port 80 (WWW)

Challenges:

- Screening rules difficult to specify due to diverse user needs
- Difficult to change pre-programmed functionality
- Can be fooled by IP spoofing

Typical Filtered Ports:

- FTP: ports 20, 21 (TFTP: port 69)
- X Windows terminal emulation
- RPC: typically on port 111
- Telnet: port 23
- SMTP: port 25
- RIP: port 520
- DNS: port 53

Note: This is why it's sometimes easier to deny all services except approved ones

Other Common Networking Ports

Beyond those typically filtered, many other ports play critical roles in everyday network operations and can be targets for reconnaissance or attack if not properly secured.

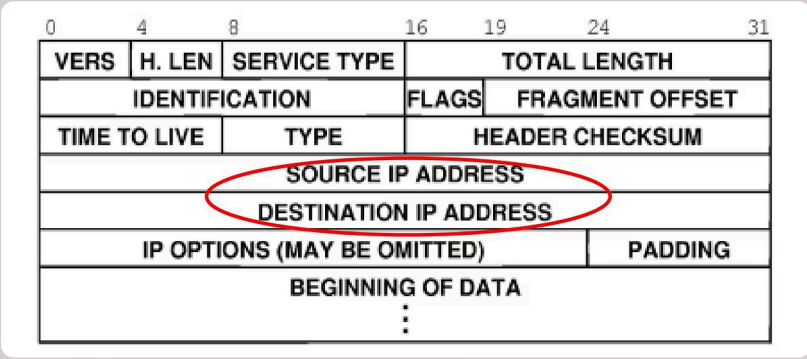
80	HTTP	Used for transmitting unencrypted web pages.
443	HTTPS	Secure HTTP for encrypted web traffic, often used for secure logins and sensitive data.
22	SSH	Secure Shell protocol for remote command-line access, secure file transfers, and tunnel creation.
3389	RDP	Remote Desktop Protocol for providing a graphical interface to connect to another computer.
161/162	SNMP	Simple Network Management Protocol, used for managing and monitoring network devices.
123	NTP	Network Time Protocol, used for synchronizing computer clock times.
445	SMB/CIFS	Server Message Block, used for file sharing, printer sharing, and interprocess communication.

Understanding the purpose of each port is crucial for both network administrators in securing systems and for attackers seeking vulnerabilities.

Network Address Translation (NAT)

The process of converting traffic from internal to external network and back

- Example: Converting from 192.168.15.2 internal address to 70.26.52.36 external address
- Packets are rewritten to replace IP headers
- Provides additional security by hiding internal network structure



Intrusion Detection Systems

The Need:

Too many spoofs and exploits that intruders can use

IDS monitors network activities for suspicious behavior

Often uses packet sniffers like Snort as their backbone

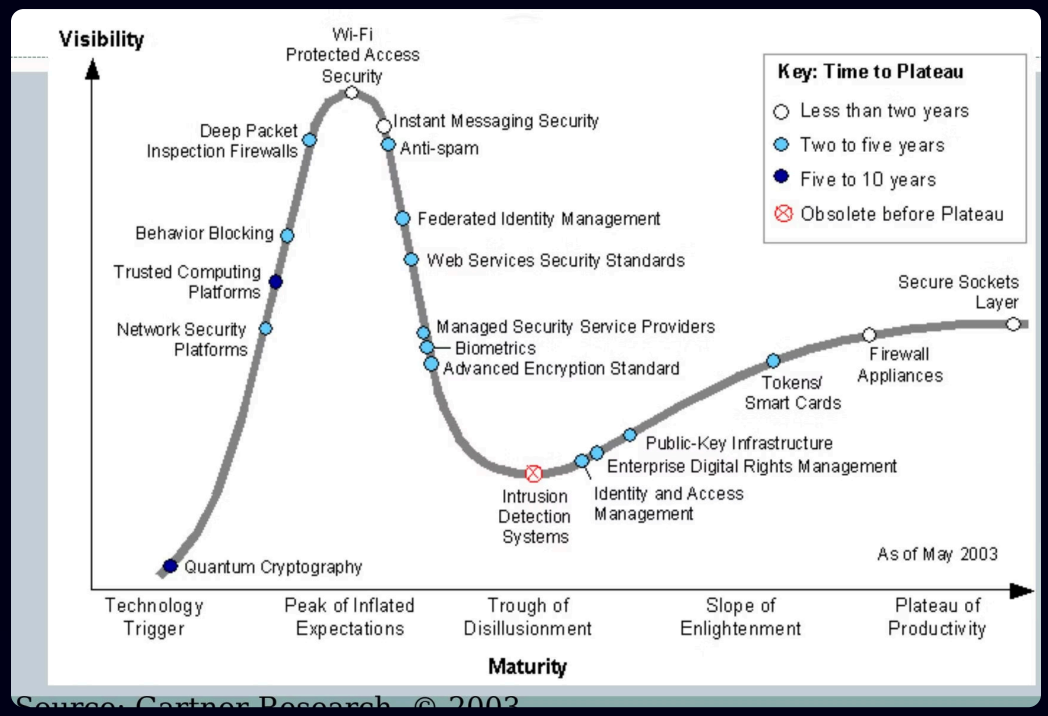
The Problem:

Too many false positives (legitimate activity triggers alarms)

Not all attack forms are known

Hackers mutate attacks to evade detection

Costly downtime if an attack succeeds



Source: Gartner Research, © 2003

Gartner's Security Hype Cycle shows the evolution of security technologies

IDS Categories

Host-Based IDS

Concerned only with activity on an individual system with no visibility into network activity

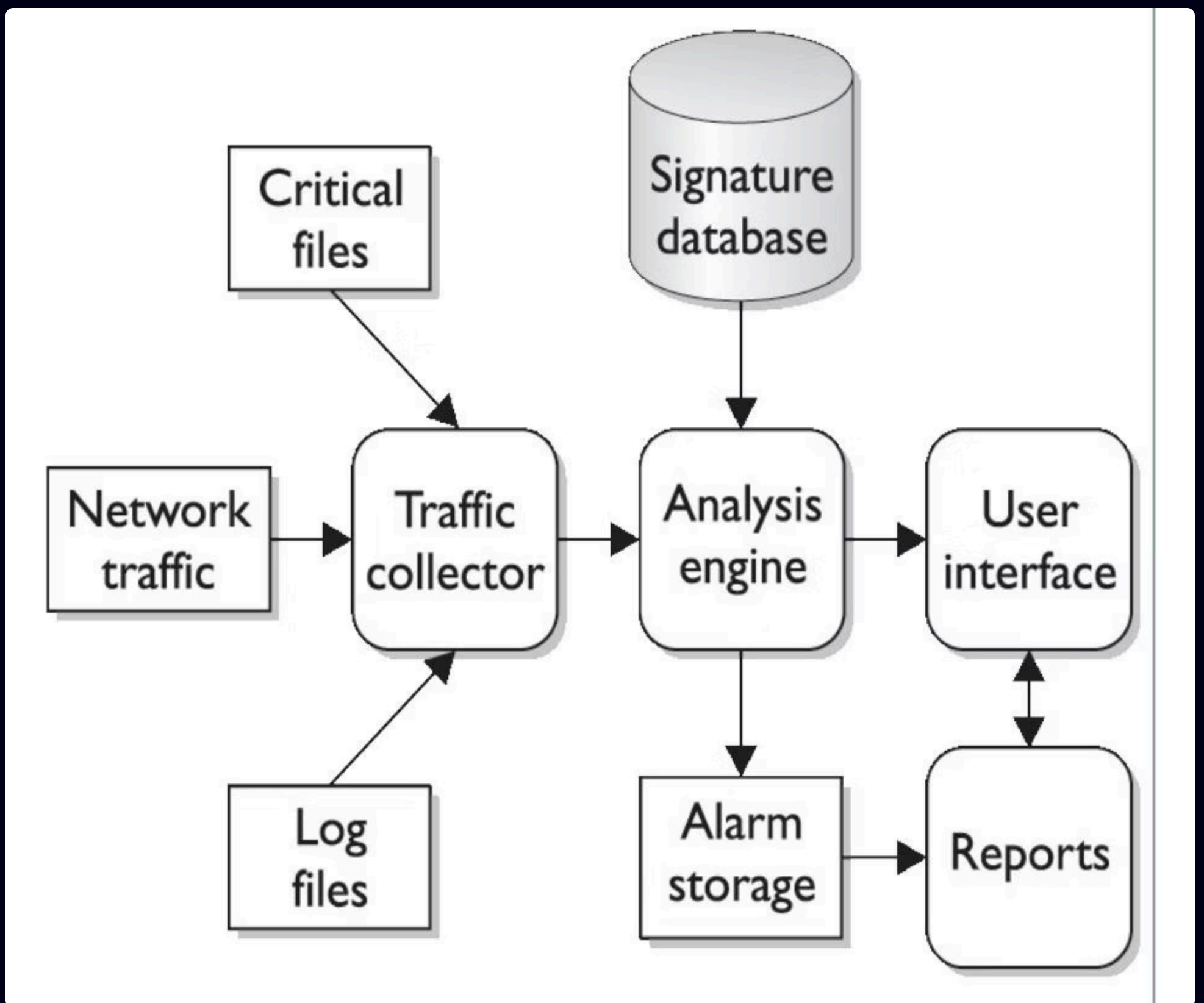
- Monitors log files, audit logs
- Tracks traffic to/from specific system
- Detects local changes and anomalies

Network-Based IDS

Has visibility only into traffic crossing the monitored network link with no awareness of individual systems

- Functions similar to a network sniffer
- Copies and analyzes network traffic
- Identifies suspicious patterns

IDS Components



1

Traffic Collector

Collects activities/events for examination. For host-based IDS, this includes log files and audit logs. For network-based IDS, this copies traffic from network links.

2

Analysis Engine

Examines collected network traffic and compares it to known patterns of suspicious or malicious activity stored in the signature database.

3

Signature Database

A collection of patterns and definitions of known suspicious or malicious activity.

4

User Interface

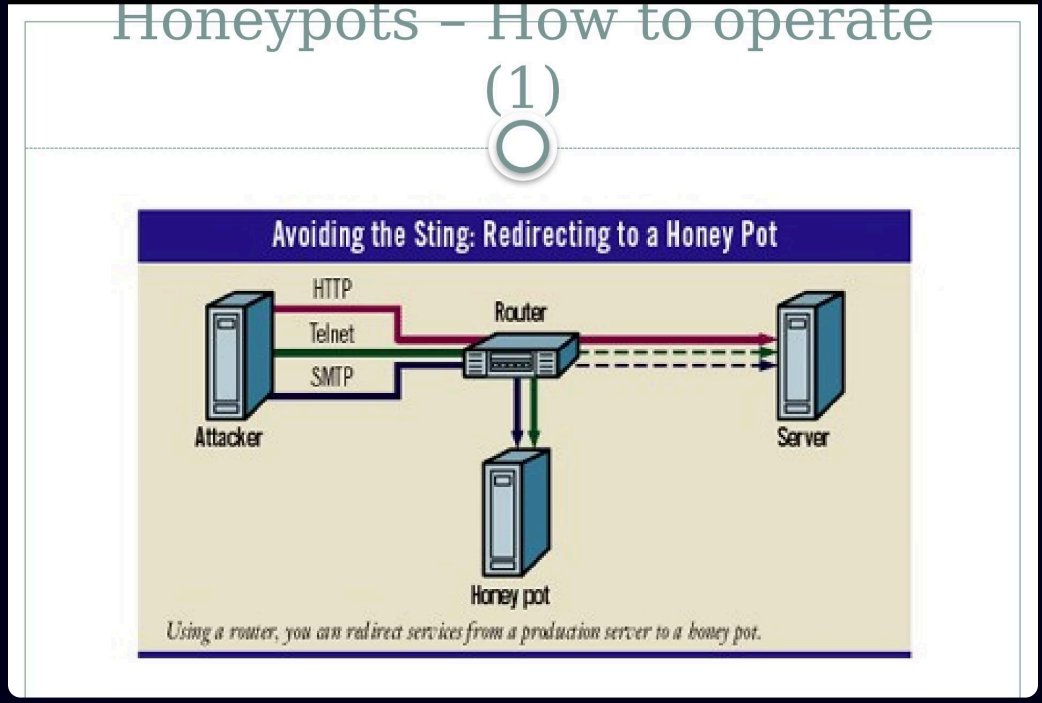
Interfaces with humans, providing alerts and giving users a means to interact with and operate the IDS.

Honeypots: A Deception Approach

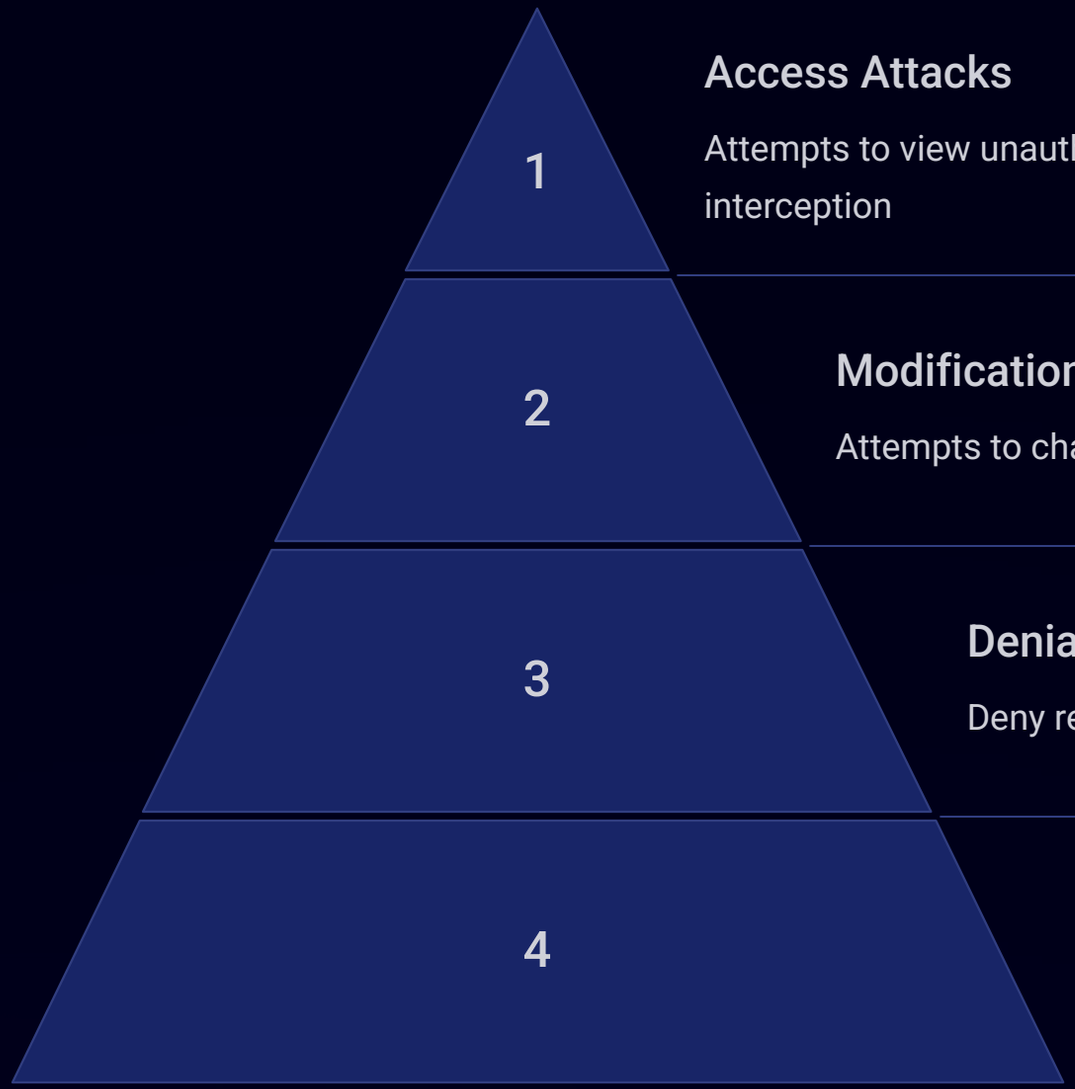
A honeypot is a deception mechanism designed to:

- Emulate production servers while having no production value
- Alert administrators and log activity
- Contain decoy content including usernames

Works on the principle: "If I'm not offering a service and someone is trying to access it, **it must be an intruder**."



Attack Classification



Access Attacks

Attempts to view unauthorized information through snooping, eavesdropping, or interception

Modification Attacks

Attempts to change or delete information without authorization

Denial-of-Service Attacks

Deny resources, information, or capabilities to legitimate users

Repudiation Attacks

Providing false information or denying real events/transactions

Understanding these attack classifications helps organizations develop appropriate defensive strategies and response plans