EXTRA TRAINING – DAY 2

Cybersecurity Advanced Topics

Learning Objectives

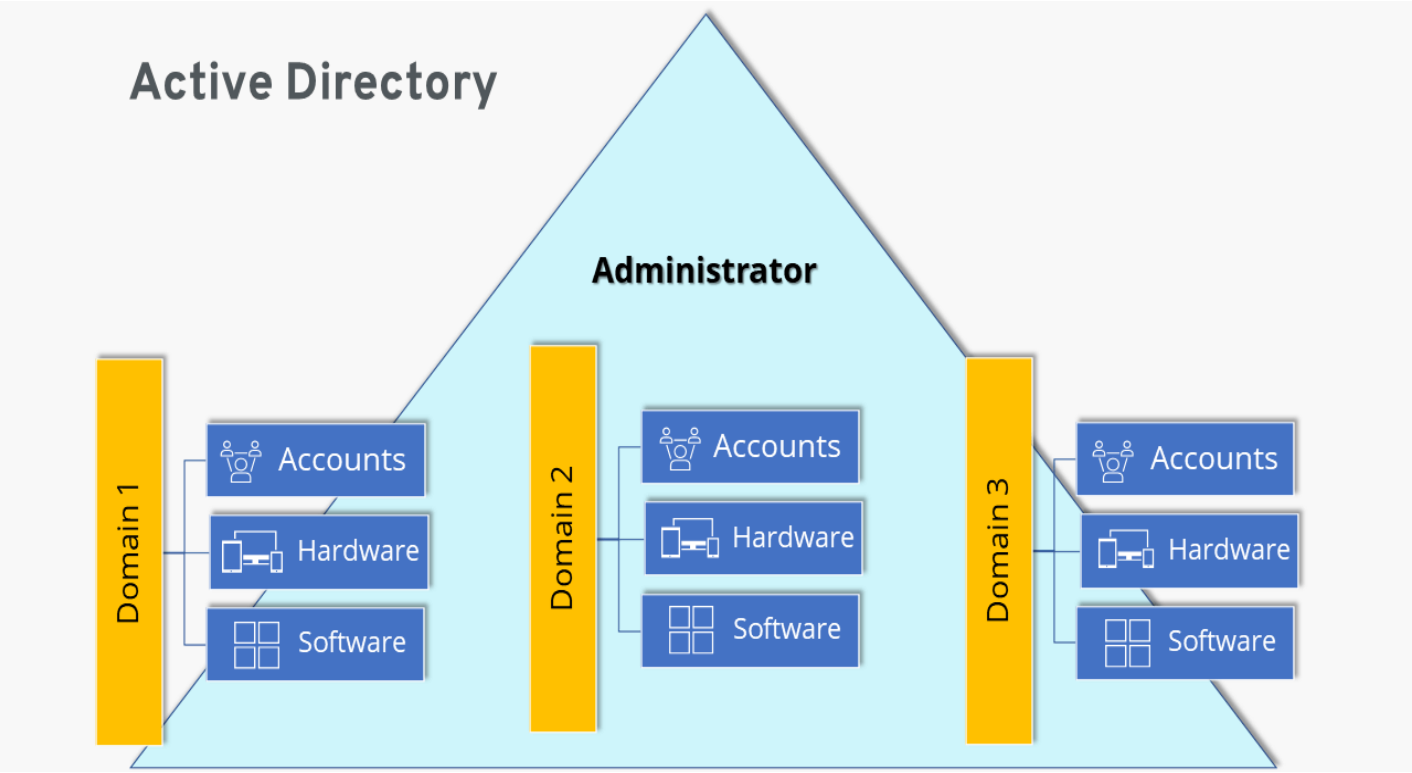
- Identity Security
  - Active Directory
  - Domain Resources
  - Account Federation and Trust
  - Multi-factor Authentication
- Network Security
  - OSI Model
  - Switches | Routers | Firewalls
  - Network IDS/IPS
  - WireShark Packet Capture
  - VPN Technologies
- Application Security
  - Application Program Interface (API)
  - Proxy Services
  - OWASP
  - Mitre Att@ck Matrix
  - Cyber Kill Chain
- Cloud Security
  - Microsoft Defender
  - Azure Sentinel
  - AWS
  - X
  - X

DAY 2 - SECTION 1

Identity Security

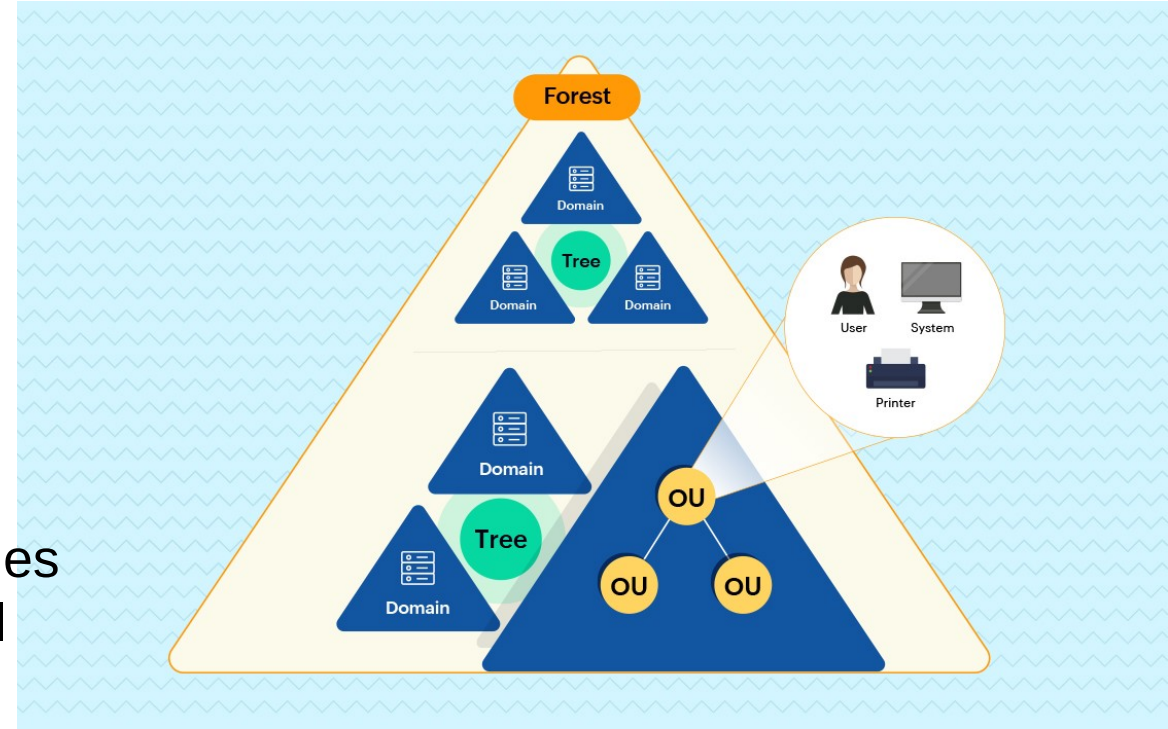
Active Directory

- Built on Domains
  - Each domain is self inclusive
  - .. “*company.com*”
  - Contains all of the associated objects inside a tree structure
  - Domains can have sub-domains defined as internal segments
  - .. “*hr.company.com*”
  - Domain Controllers – Top Level
- Primary Identity Authority
  - Computers are set to domain authentication
  - User objects are contained in the directory and have permissions assigned to log into domain hardware objects



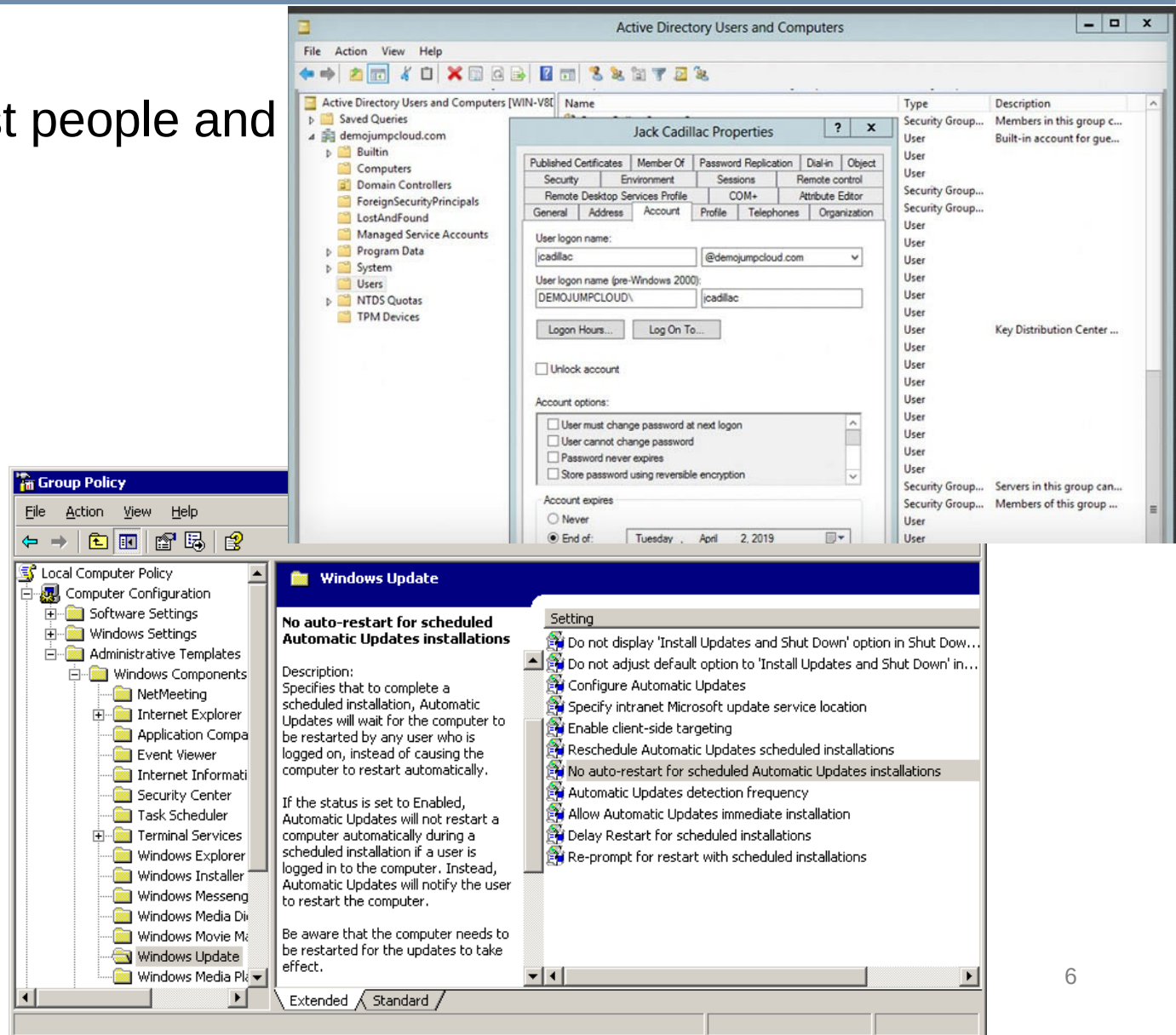
Active Directory

- Organizational Structure
  - Use of Organizational units (OU)
  - Method of grouping like purposed objects and identities together
- Policy Management
  - Allows for application of top level baseline policies to the whole domain, selected OUs or individual objects – as needed
  - Can have overlapping, conflicting policies
- Trees for Forests ...
  - Collection of domains in a Forest
  - Tree architecture organizes OUs like folders
  - Developed in 1990's



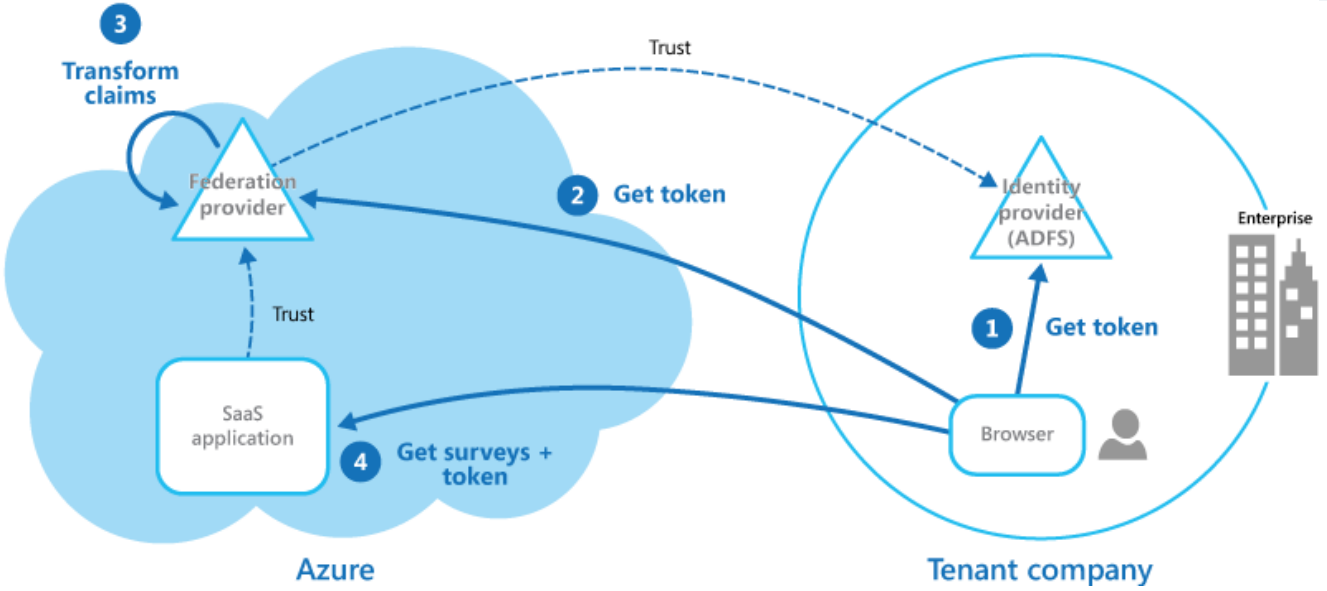
Domain Resources

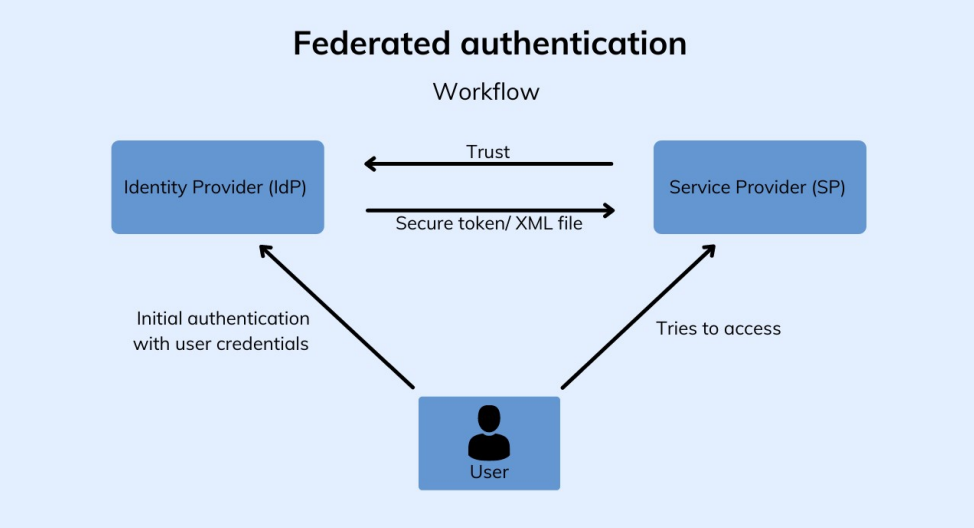
- Resources can include more than just people and computers
  - Shared printer resources
  - Mapped drive storage locations
  - Service accounts
  - Software applications
- Group Policy is pushed down
  - To domain attached PCs
  - To User accounts
  - To Service accounts



Account Federation and Trust

- Company Domain Trusts
  - Can allow users from other domains to resources in company domain
  - Can be two-way or one-way
  - Often seen with Mergers
- Cloud Trusts
  - Microsoft Azure AD (Entra)
  - Allows for Single-Signon (SSO) to various third party applications
- Identity Provider Trusts
  - Third party applications that use a trusted Internet resource
  - Most common are Microsoft, Google, Facebook, LinkedIn
  - Application does not need to know credentials



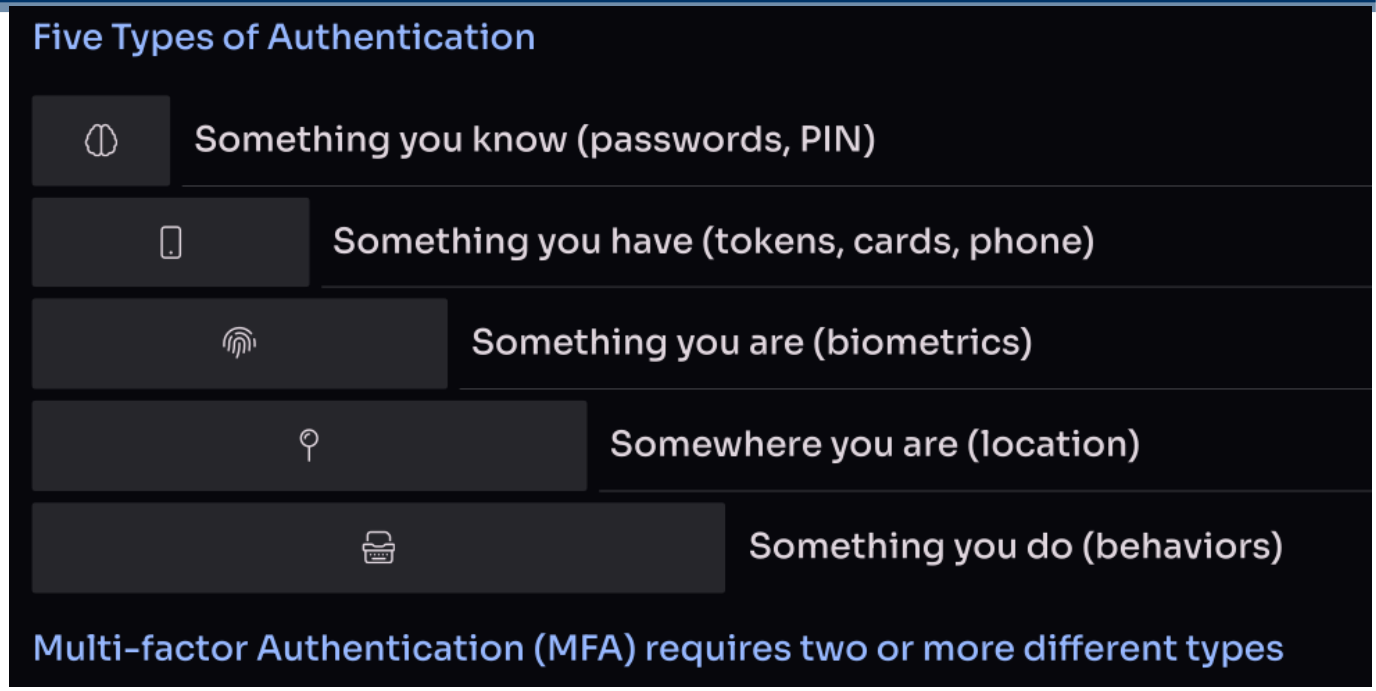


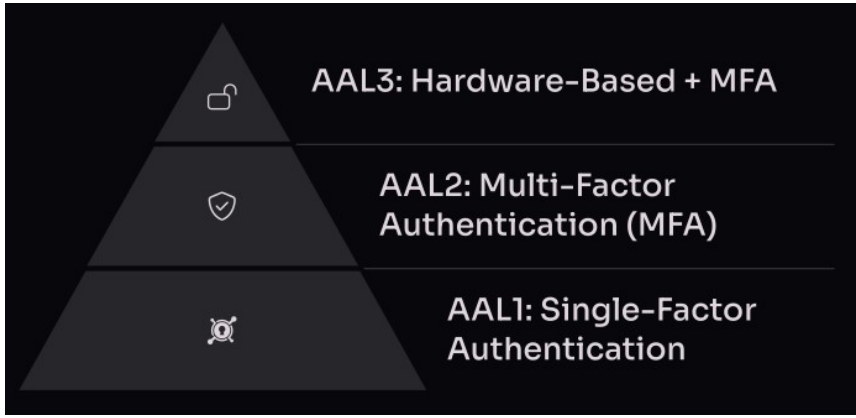
Multifactor Authentication

- Requires the use of additional methods of verifying user
  - Can be for physical access
  - Can be for application access
  - Can be for web site access
- Improved Security Level
  - Ensures that identity logging in is valid using various methods of asserting authentication
  - Comes in varying types of identifiers
  - Sometimes may be coupled together (more than one additional)

Multifactor Authentication

- Five Standard Methods
  - Know: password, PIN .. mos common single factor
  - Have: phone, token, security card
  - Are: biometrics (fingerprint, retina scan, palm print ..)
  - Location: based on GPS, physical location ...
  - Actions: input digits, trace a pattern ...
- Three Levels – US Government use
  - AAL1 – single factor (username/password)
  - AAL2 – multiple factor (UN/pw + 1 factor)
  - AAL3 – use of assigned hardware tokens





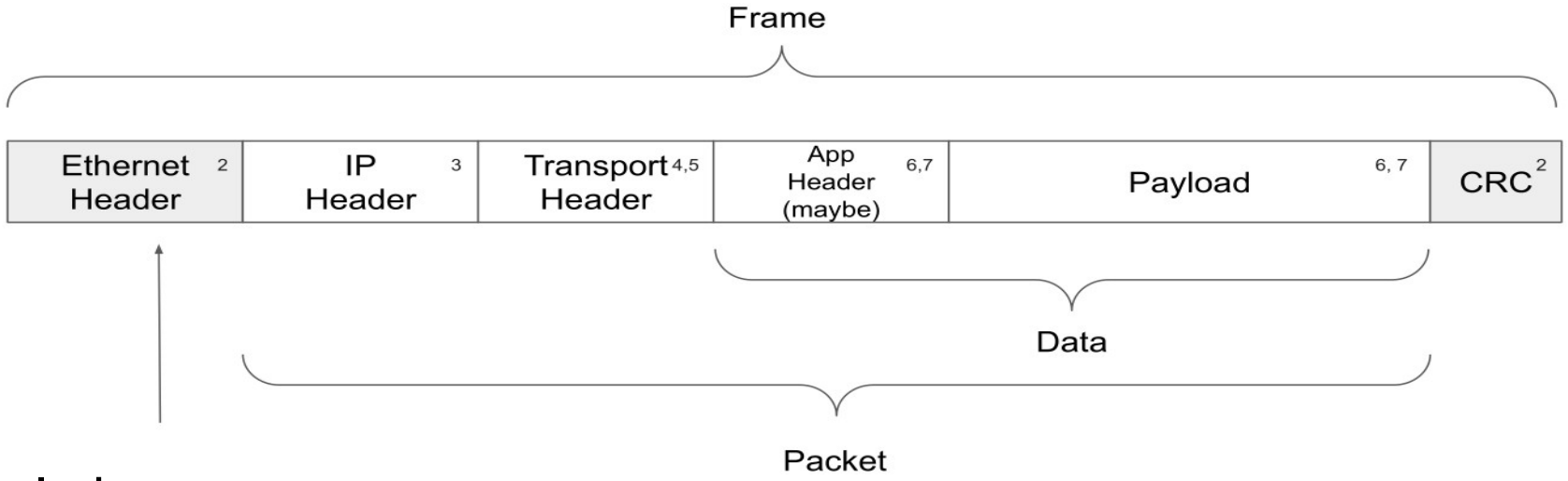
DAY 2 - SECTION 2

Network Security

OSI Model

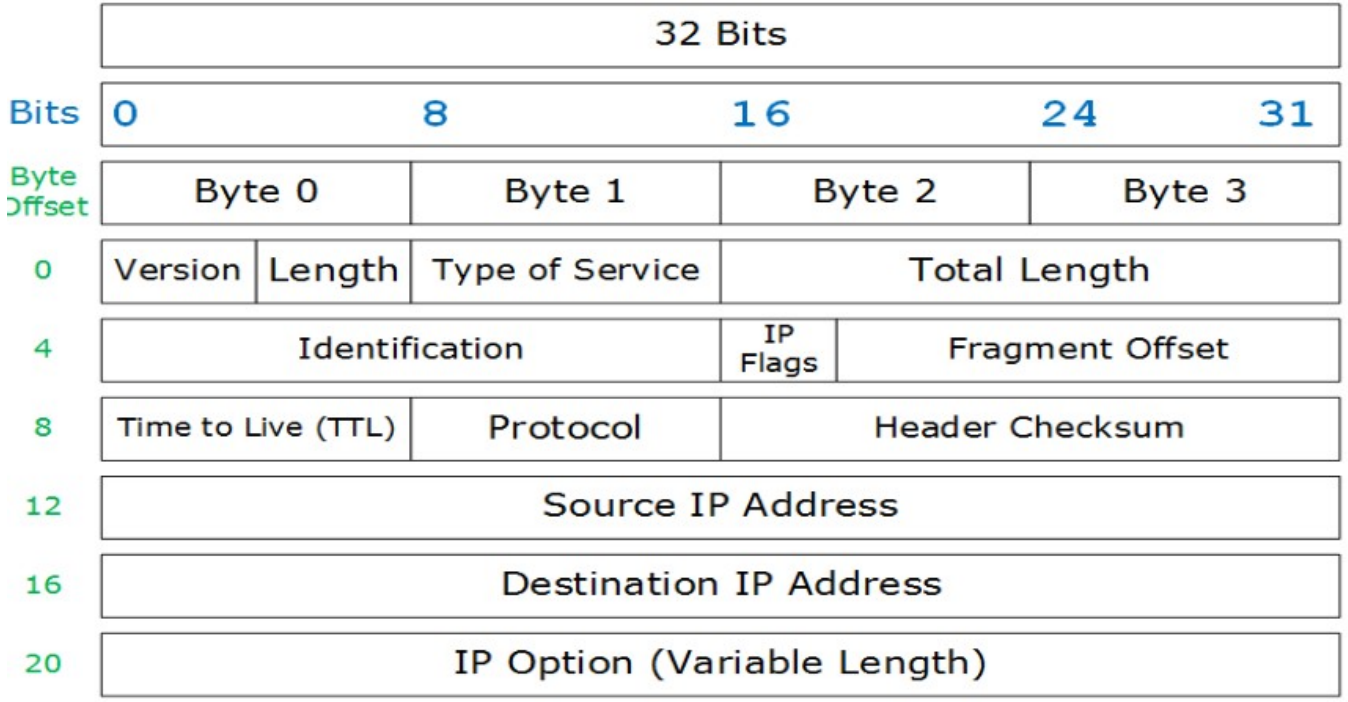
- Standardized model for computer communications
  - Helps in understanding how information flows
  - Defined in 1984 by ISO
  - Compares to TCP/IP (or Web Model)
- Analogy – writing a letter ...
  - I have a thought ...
  - I write it down in block letters ...
  - I do this while sitting at my desk …
  - I put it in an envelope …
  - I address and stamp the envelope …
  - I put it in the mailbox to be picked up …
  - USPS comes to get it !!!

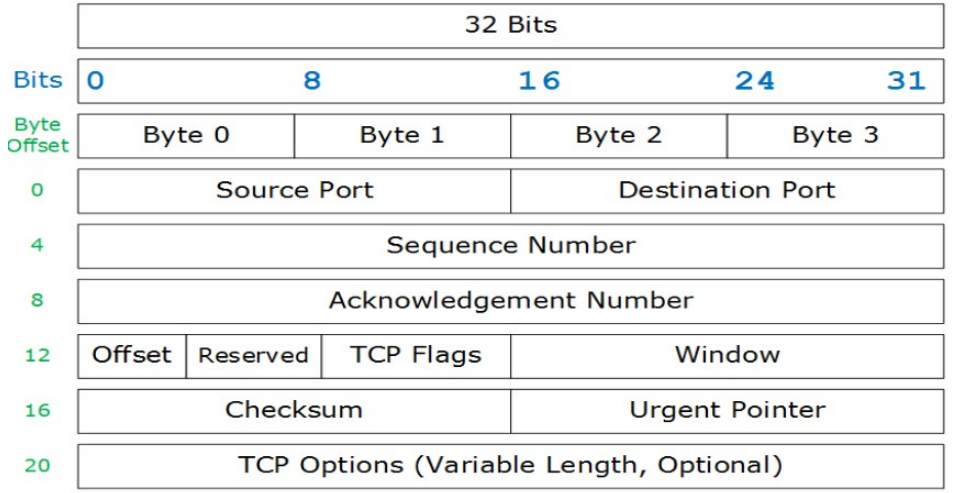
Data Packets

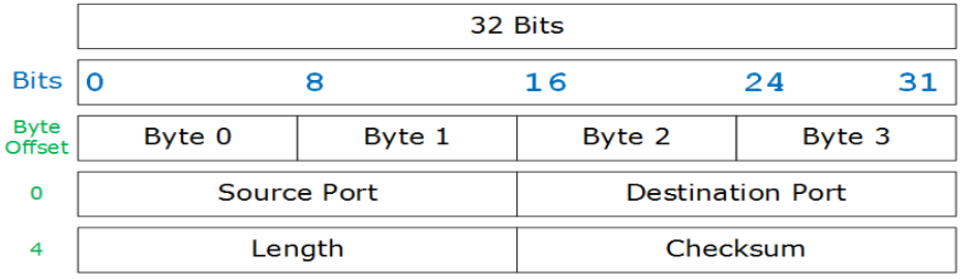


- Concept of Data Encapsulation
  - Data payload from the previous layers is wrapped in a new header as it goes down the stack for transmission
  - As data is received and moves up the stack, the previous header is stripped to eventually reveal the source data
  - Layer 2 also adds a footer to the packet, called a CRC check
- Data encapsulation occurs throughout the life of a data packet, but only the source and destinations do the full extraction
  - Devices along the way only need to decode that portion of the packet to meet its functions
  - Other devices my take the original packets and wrap it into a new protocol for special transmission

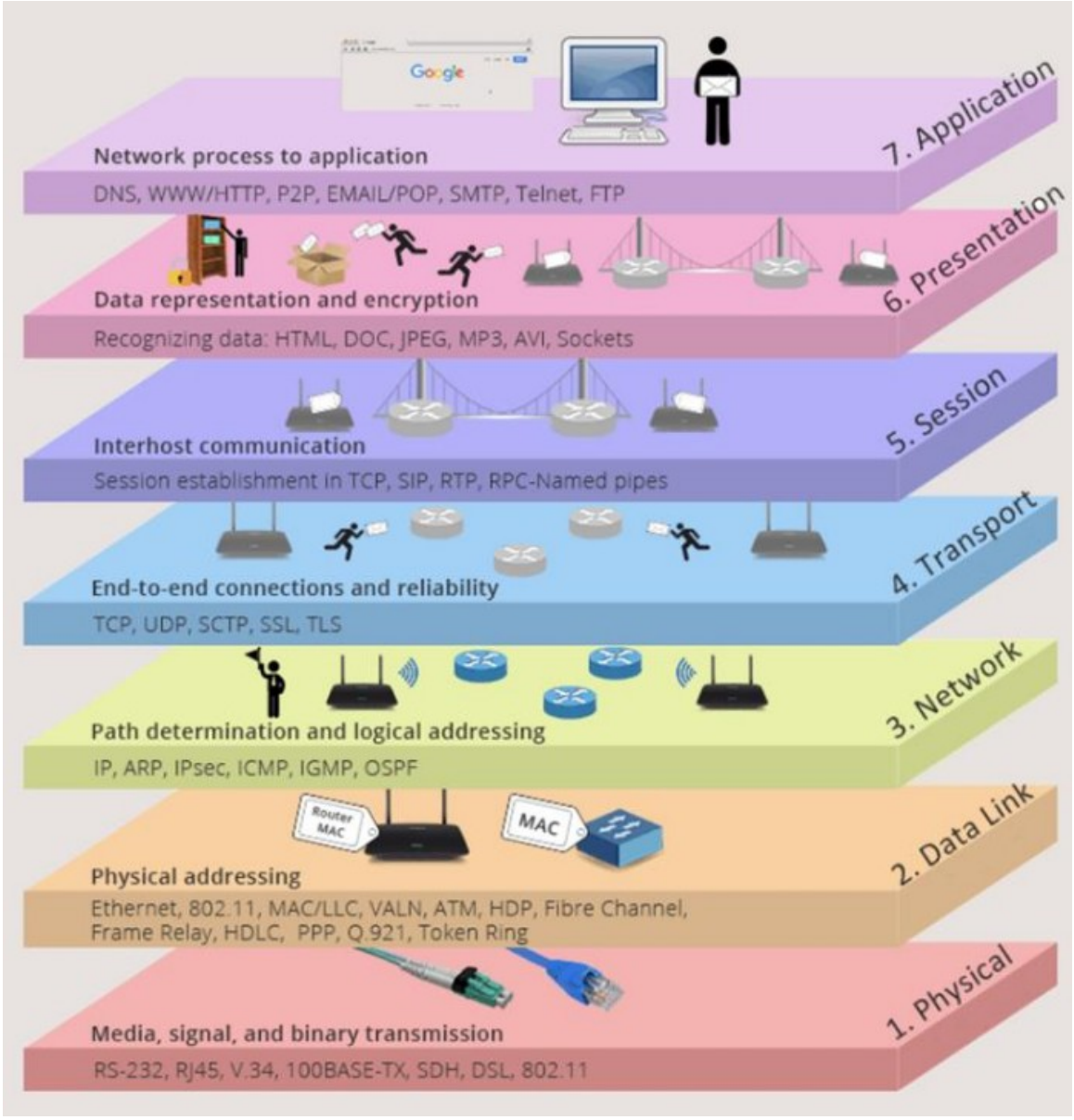
Data Packets – Header Information







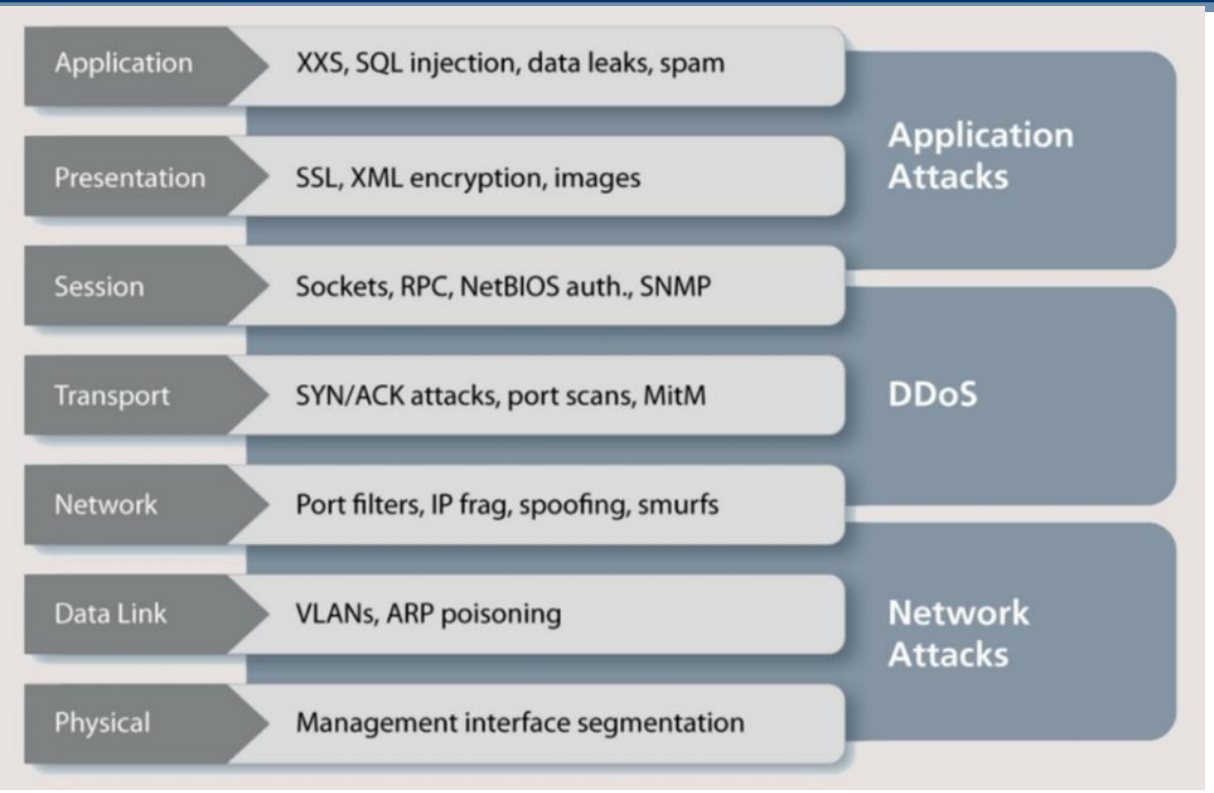
OSI Model



- Protocols differ almost exclusively by layer
  - Each layer will have its own methodology of communicating with the same layer on other devices
  - Protocols from higher layers pass through lower layers within the encapsulation

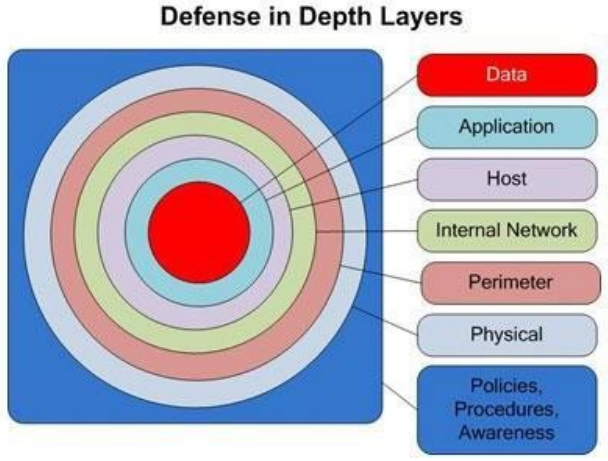
- Primary communication modes
  - Layer 5-7 = inside the computer
  - Layer 4 = Segments
  - Layer 3 = IP Addresses
  - Layer 2 = Frames
  - Layer 1 = bits/bytes/medium specific translation

OSI Model – Defense in Depth



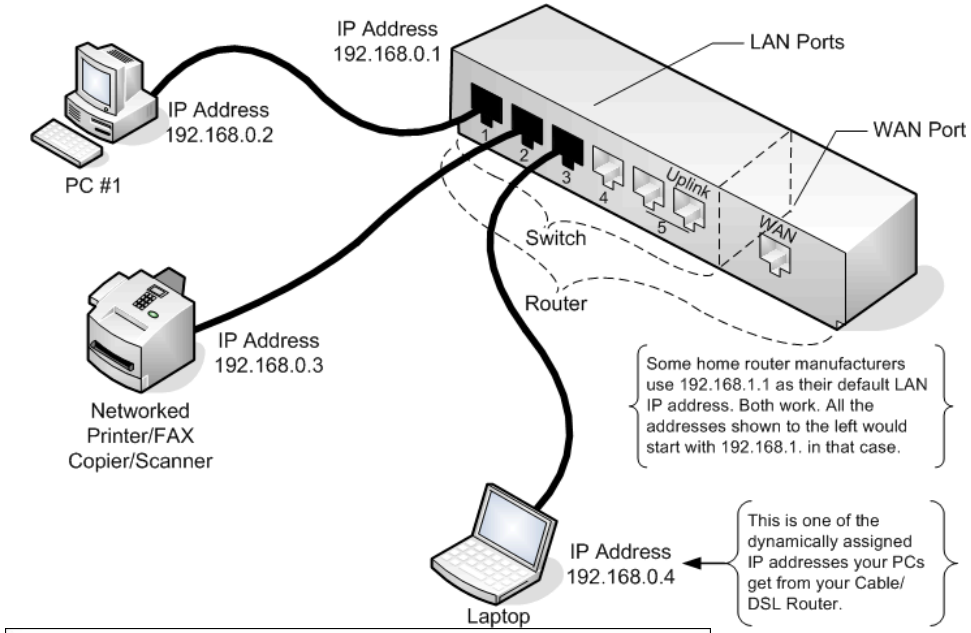
- Also means that the method of attack will be different per layer
  - Application type of attacks
  - Availability type of attacks
  - Network intrusion type of attacks

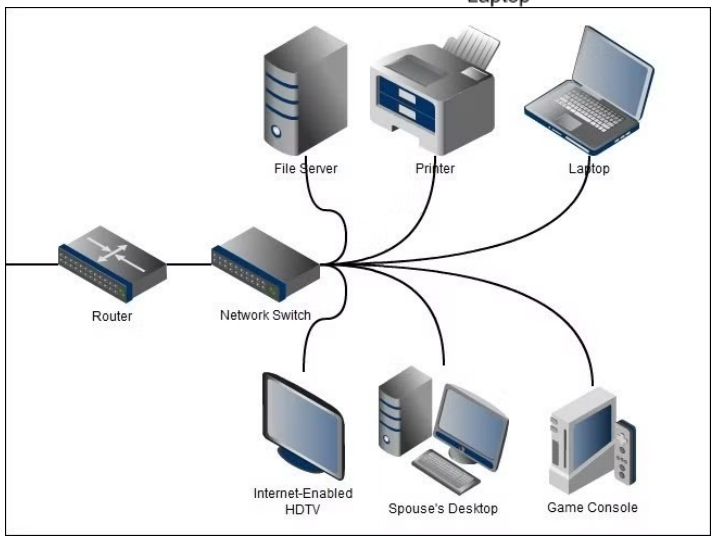
- **Defense in Depth**
  - Method of layer active and passive defensive techniques to better secure an environment
  - Data is the new gold ...
  - Originally know as 0utside-in; or castle-keep mentality



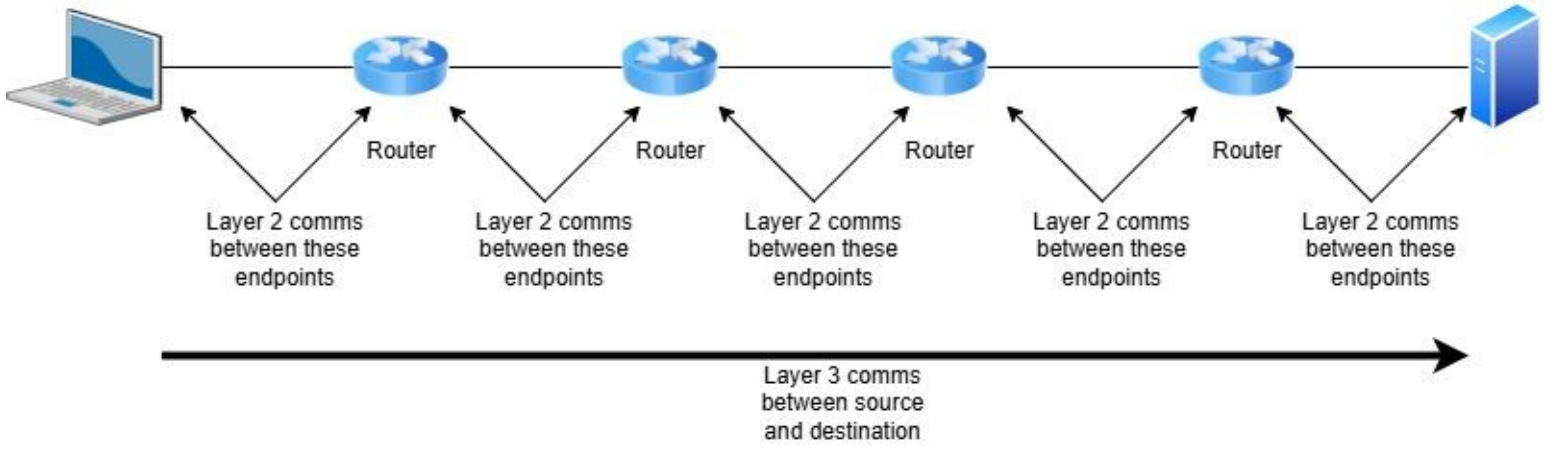
Switches | Routers | Firewalls

- Switches – Layer 2 devices
  - How computers and devices get connected to networks
  - Uses Virtual-LANs or VLAN technology
  - Method of separating traffic by group
  - One collision domain per connection
  - Improvement over hubs
  - Can be interconnected in hierarchy
  - Concerned with Data Frames
- Routers – Layer 3 devices
  - Communicate between other routers
  - Interconnect switches to networks
  - Connect internal networks to external network, or Internet
  - Operate as gateways for networks
  - Concerned with IP Addressing

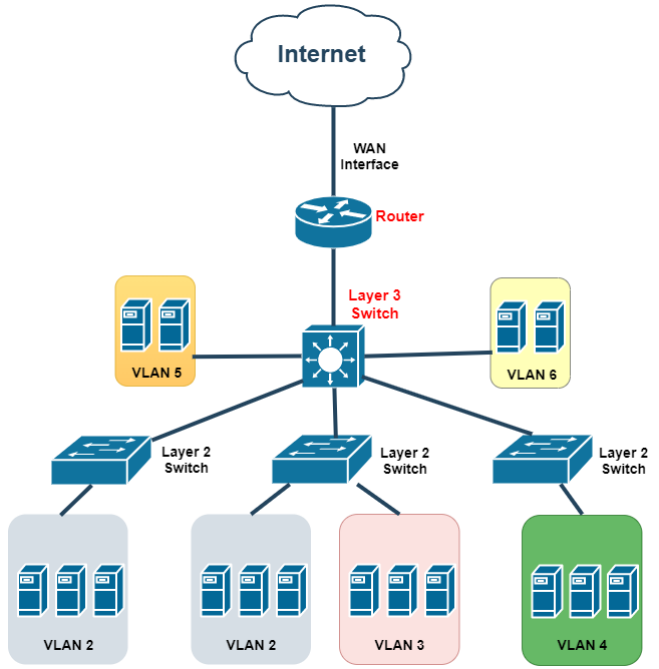




Switches | Routers | Firewalls

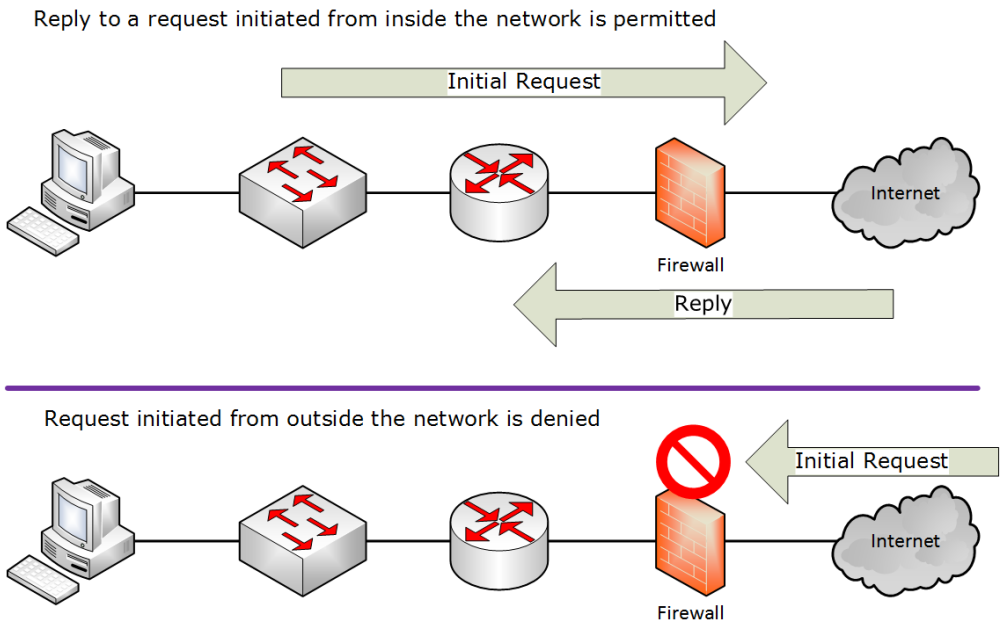


- Encapsulation revisited
  - Network devices deconstruct the packet to get to usable info
  - PC = Layer 7 → Layer 1
  - Switch = Layer 2 → Layer 1
  - Router = Layer 3 → Layer 1
- VLAN Architecture
  - Uses tagging to isolate connected nodes to a data segment
  - Hierarchy of switches from edge to core
  - Switches can have multiple VLANs
  - VLANs can stretch across edge layers



Switches | Routers | Firewalls

- Firewalls
  - Provide a controlled security barrier between networks
  - Most often at Internet egress point
  - May also segment internal locations (offices from data center; development from production ..)
  - Typically operate at Layer 4 - Segments



- Demilitarized Zone (DMZ)
  - Special segment with limited permissions
  - Often referred to as isolated
  - Useful in creating controlled segments to put Internet facing objects that do not have direct access to the inside

Types:

Standard
Deep Packet Inspection
Next Generation
Web Application
Host Based

Routing and VLANs

- Windows PC Route Table
  - Command line = route print
  - Details the known IP address routing for that PC

- Linux PC Route Table
  - Command line = ip route show
  - Command line = ip route list
  - Details the known IP address routing for that PC
  - May have “blackhole” or “null” routes

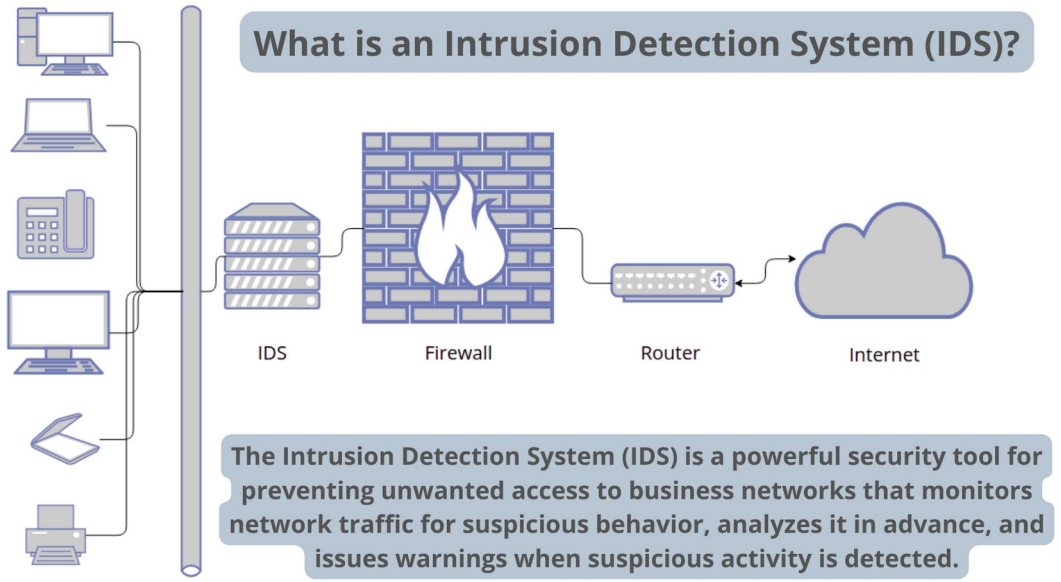
```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0         10.0.0.1       10.0.0.101     45
         10.0.0.0    255.255.255.0         On-link       10.0.0.101    301
       10.0.0.101  255.255.255.255         On-link       10.0.0.101    301
       10.0.0.255  255.255.255.255         On-link       10.0.0.101    301
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link        127.0.0.1    331
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
    192.168.149.0    255.255.255.0         On-link     192.168.149.1    291
    192.168.149.1  255.255.255.255         On-link     192.168.149.1    291
  192.168.149.255  255.255.255.255         On-link     192.168.149.1    291
    192.168.183.0    255.255.255.0         On-link     192.168.183.1    291
    192.168.183.1  255.255.255.255         On-link     192.168.183.1    291
  192.168.183.255  255.255.255.255         On-link     192.168.183.1    291
```

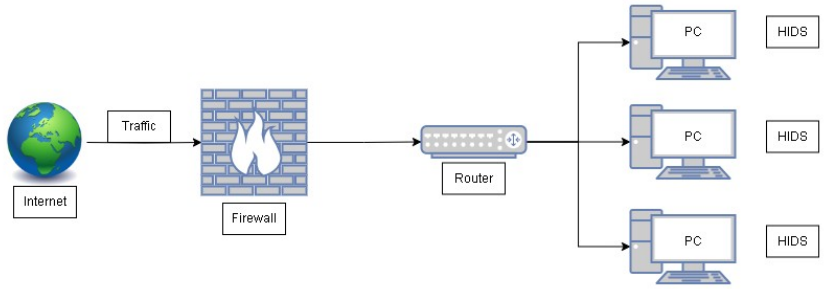
```
cbrenton@fw:~$ ip route show
default via 192.168.0.1 dev enp1s0 proto static
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
172.18.0.0/16 dev br-dacb53d9cf7f proto kernel scope link src 172.18.0.1
192.168.0.0/24 dev enp1s0 proto kernel scope link src 192.168.0.6
192.168.69.0/24 dev enp2s0 proto kernel scope link src 192.168.69.1
blackhole 218.92.0.0/16
cbrenton@fw:~$
```

```
cbrenton@rita-v5:~$ ip route list
default via 192.168.69.1 dev enp6s18 proto dhcp src 192.168.69.196 metric 100
4.0.0.0/8 via 192.168.69.10 dev enp6s18
8.0.0.0/8 via 192.168.69.10 dev enp6s18
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
172.18.0.0/16 dev br-c71ec326373e proto kernel scope link src 172.18.0.1
192.168.69.0/24 dev enp6s18 proto kernel scope link src 192.168.69.196 metric 100
192.168.69.1 dev enp6s18 proto dhcp scope link src 192.168.69.196 metric 100
192.168.69.11 dev enp6s18 proto dhcp scope link src 192.168.69.196 metric 100
cbrenton@rita-v5:~$
```

Network IDS / IPS

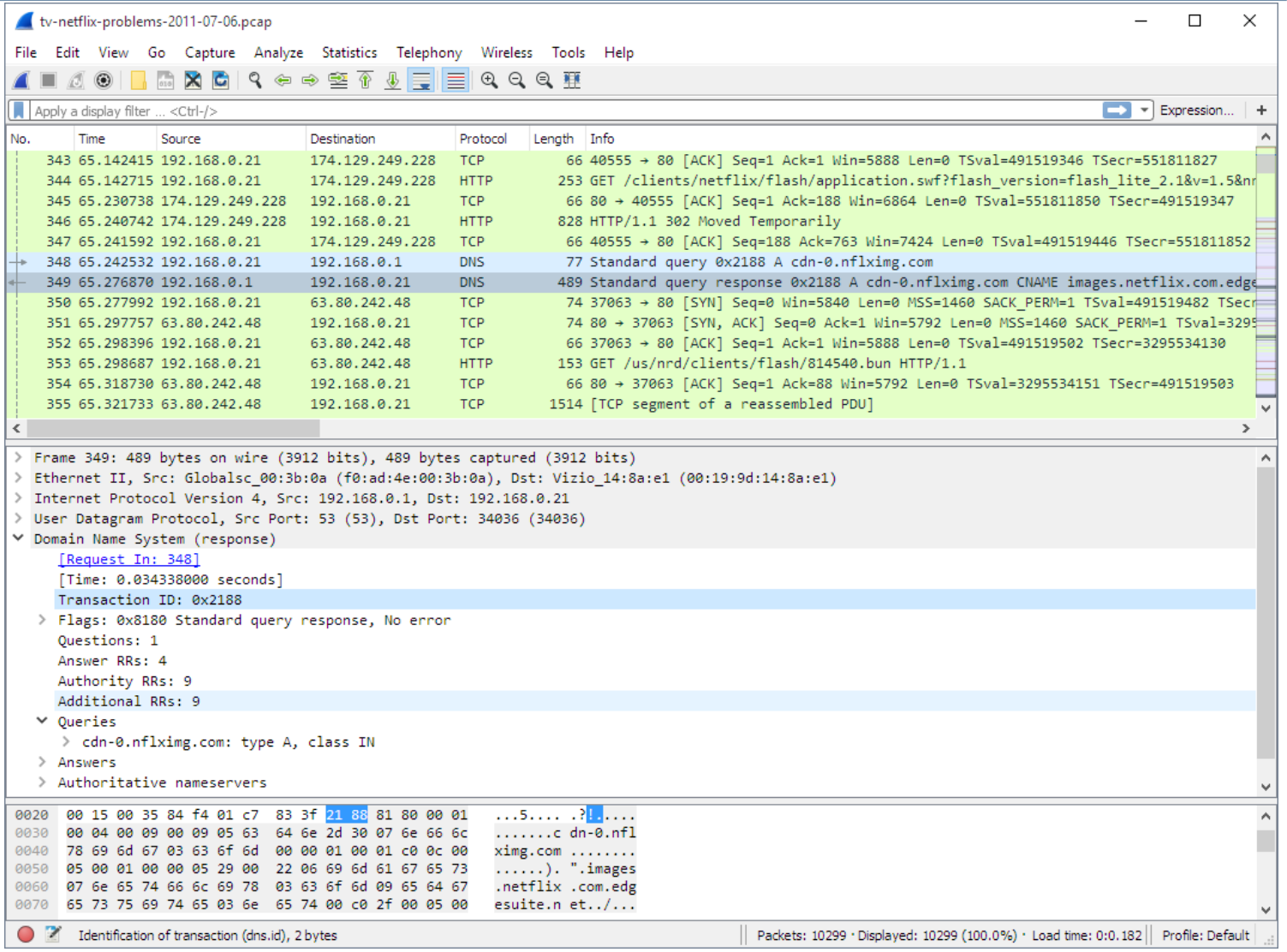
- Network Intrusion Detection
  - Monitors a network or host for suspected intrusions
  - Typically in parallel with network
  - Looking for:
    - Address Spoofing
    - Fragmented connections
    - DDOS/Coordination
  - Alerts and warnings
- Network Intrusion Prevention
  - Actively block known bad or suspicious connections
  - Typically inline (fail open)
  - Signature based or pattern (anomaly) based





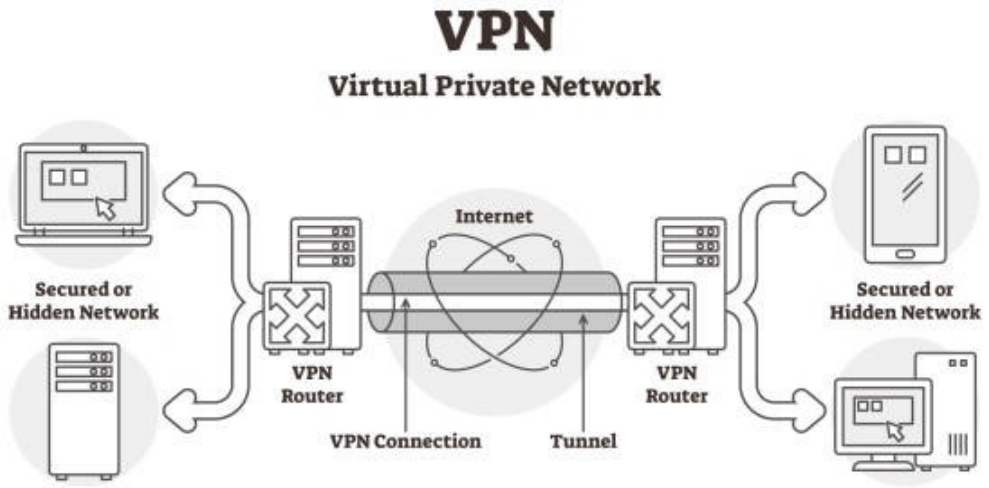
WireShark Fundamentals

- Packet capture and replay tool
  - Useful in network and application troubleshooting
  - Requires capture of inline data at some point on the physical/ logical network
  - Can be run on computers, network devices and network connected objects ..
- Deconstructs the OSI layers
  - Creates graphs and charts
  - Allows selectable view of parts of the packet
  - Able to isolate issues



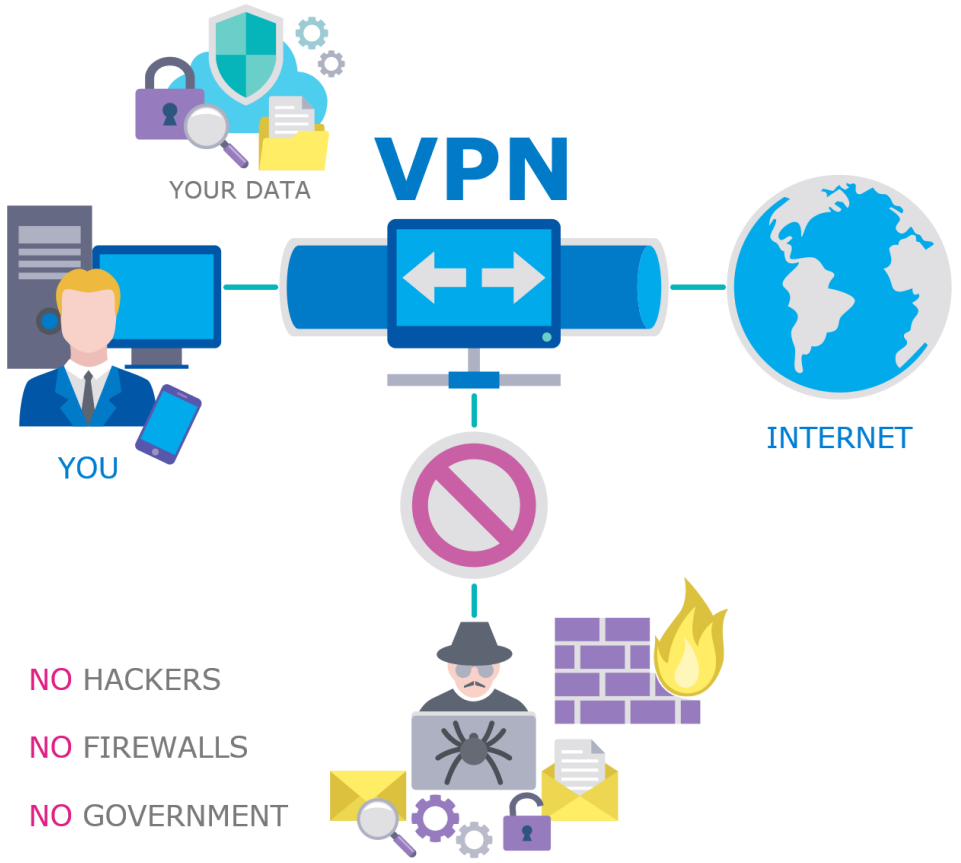
VPN Technologies

- Virtual Private Network (VPN)
  - Used to secure connections between accessible hosts, networks or systems
  - Creates a secure “tunnel” between segments
  - Uses encryption and encapsulation (IPSEC or GRE)
  - Hides sensitive data
- Network Connections
  - Network to Network
  - Host to Network
  - Host to Server



VPN Technologies – User Based

- Modern technology in common use
  - Promoted as anti-hacking tools for everyday user
  - Examples .. NordVPN, NortonSecure ..
  - Mobile friendly
- Connects to Internet Gateway, not to a company or organization infrastructure
- Used in insecure locations
  - Coffee shops
  - Public areas with “Free WiFi”
  - Partially secure

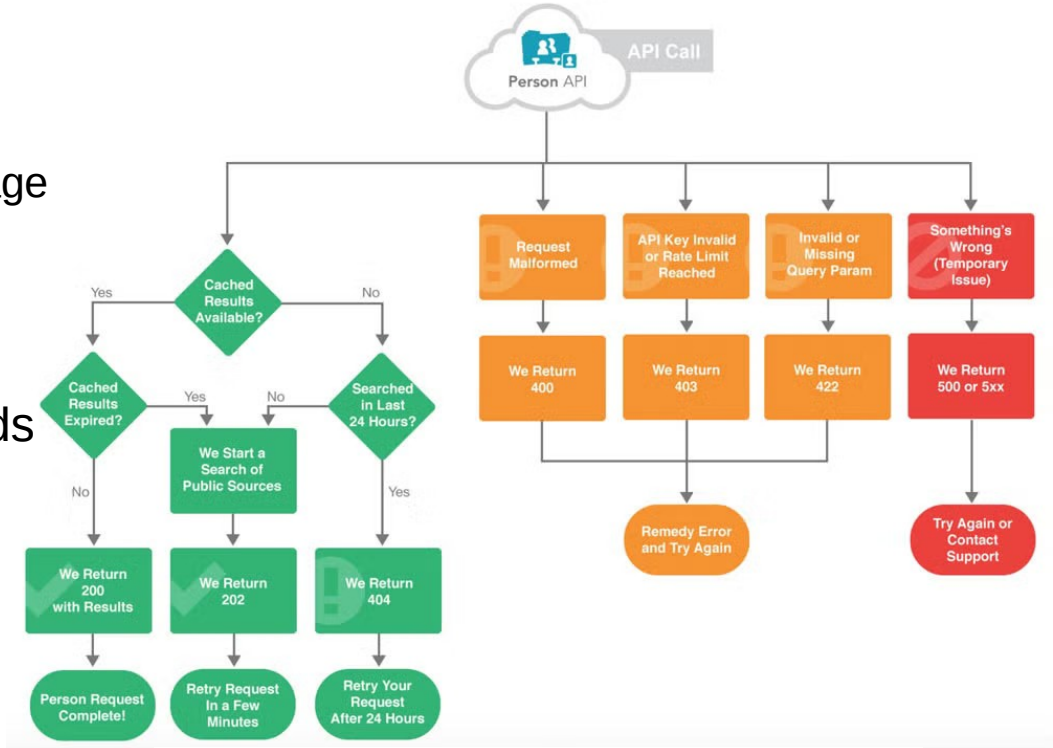


DAY 2 - SECTION 3

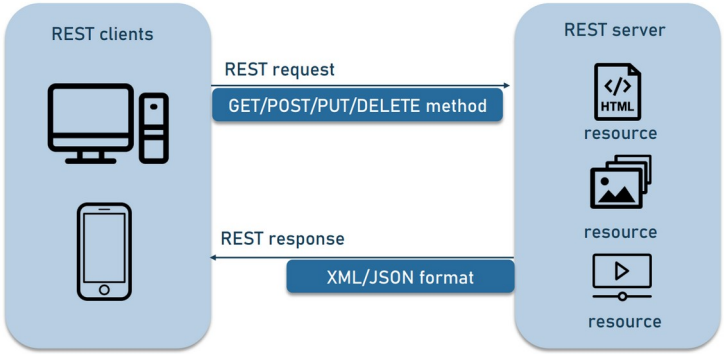
Application Security

Application Programming Interface (API)

- Functions and requests made to web services
  - Defined methods of inputting or outputting data from a web page
  - Typically encoded into the web page and web client
- Types of API Services:
  - REST: most common protocol, based on HTTP methods
  - SOAP: XML based web protocol; stringent messaging
  - GraphQL: defined query language; request exact data
- Common Methods:
  - GET: Used to retrieve data from a server
  - POST: Used to send data to the server to create a new resource or update an existing one
  - PUT: Used to update an existing resource on the server
  - DELETE: Used to remove a resource from the server
  - HEAD: Only retrieves header information, not the body
  - CONNECT: Used to establish a network connection to a server

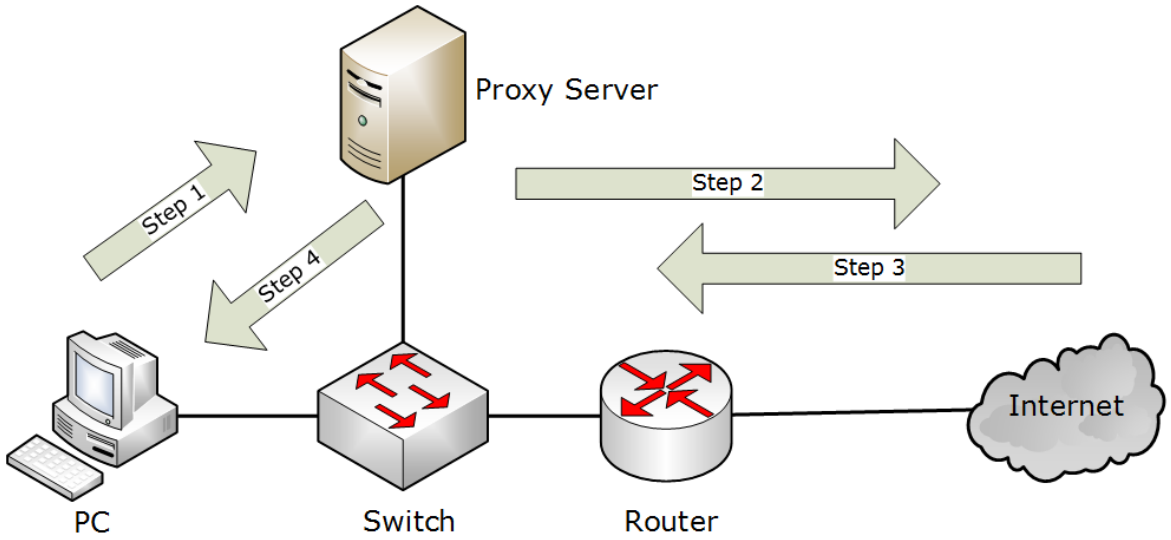


REST API IN ACTION



Proxy Services

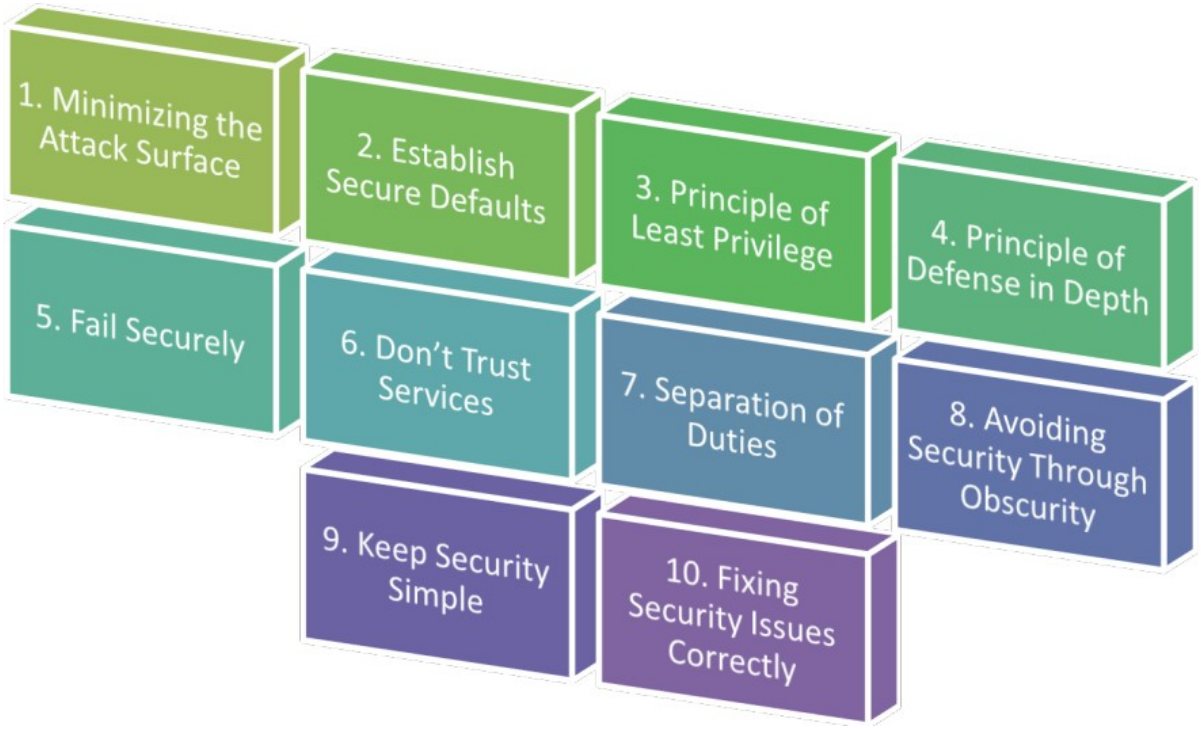
- Proxy Servers are secure redirectors
  - Clients think that they are connecting to the Internet host
  - Instead are redirected to the proxy
  - Proxy makes the website request
  - Return result is sent to original host
- Emulates Man-in-the-Middle attacks
  - Useful in monitoring secure sites
  - Configured at hot or network layer
- Challenges:
  - Digital certificates for some secure sites and applications do not respond well
  - Certificates can be out of sync



Step 1 – PC sends request for an web page on the internet to the proxy
Step 2 – Proxy server forwards the request to the web server on the internet
Step 3 – Reply from the web server is sent back to the proxy server
Step 4 – Proxy server forwards the reply to the PC

OWASP

- **Open Web Application Security Project**
  - International Non-profit organization
  - Dedicated to securing Internet Web Applications
  - Known for their "**Top 10 List**"



- Top 10:
  - Broken Access Control
  - Cryptographic Failures
  - Injection
  - Insecure Design
  - Security Misconfiguration
  - Vulnerable and Outdated Components
  - Identification and Authentication Failures
  - Software and Data Integrity Failures
  - Security Logging and Monitoring Failures
  - Server-Side Request Forgery

Mitre Att@ck Matrix

- Categorized Framework
  - 14-Step Process
  - Organizes how cyber attacks happen by phase
  - Correlation of behaviors
- Tactics, Techniques and Procedures (TTPs)
  - Tactic: why portion of a cyber attack
  - Technique: how attackers get in
  - Procedures: detailed methods of exploitation (step-by-step)
- Why Use Mitre Att@ck
  - Understanding attacker behaviors
  - Developing threat models and prevention strategies
  - Improving Incident Response (IR)

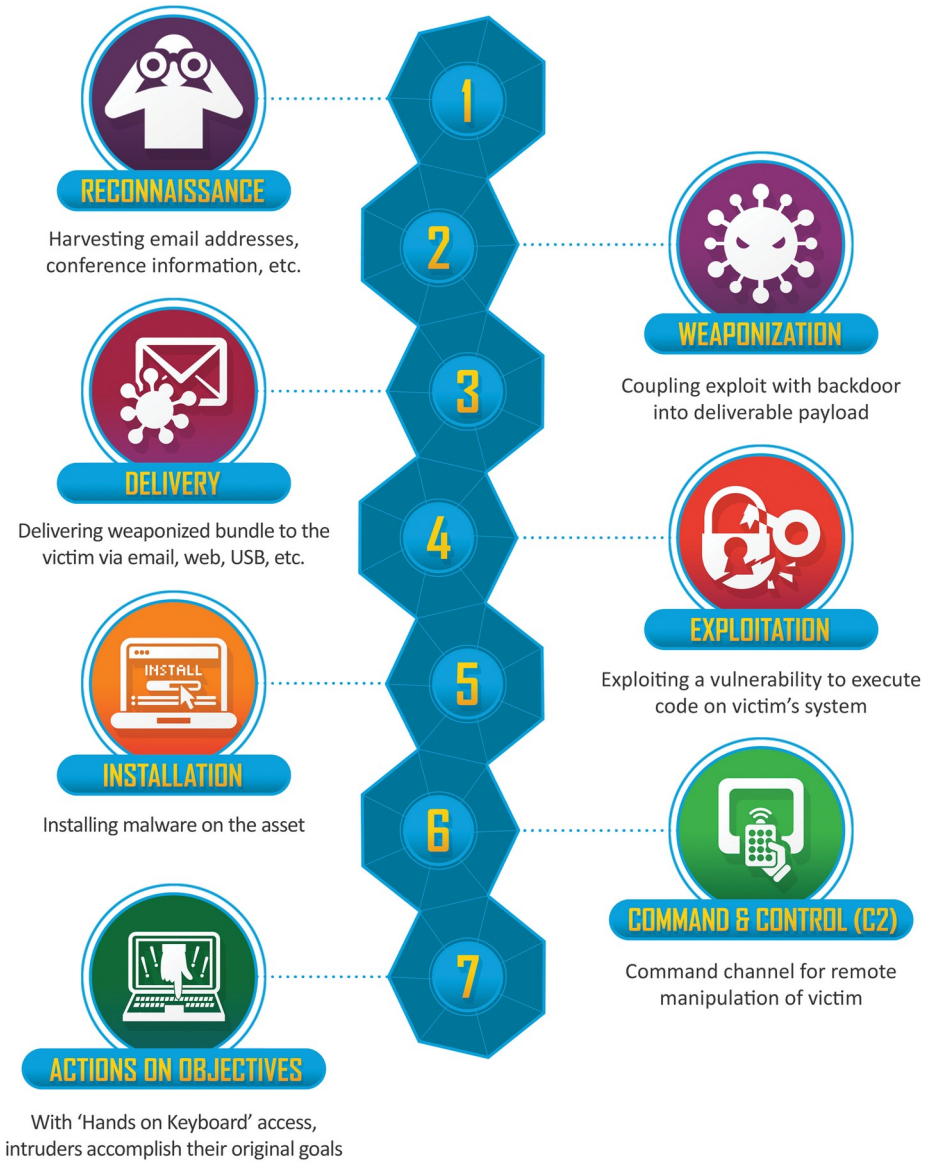
ATT&CK®

https://attack.mitre.org/

Mitre Att@ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		
	Regsvcs/Regasm	External Remote Services	Parent PID Spoofing	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Standard Application Layer Protocol		
	Regsvr32	File System Permissions Weakness	Path Interception	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Cryptographic Protocol		
	Rundll32	Hidden Files and Directories	Plist Modification	Exploitation for Defense Evasion	Steal Web Session Cookie	System Owner/User Discovery			Standard Non-Application Layer Protocol		

Cyber Kill Chain

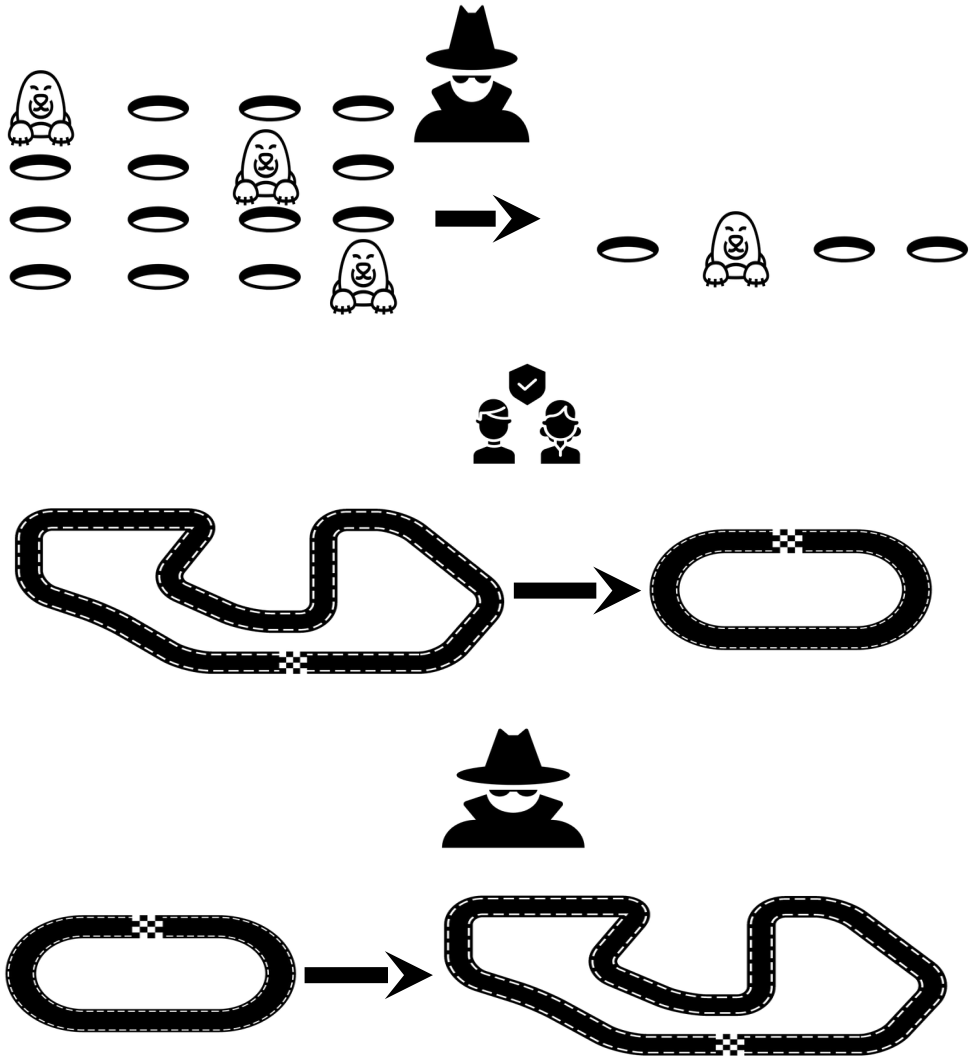


- Developed by Lockheed Martin in 2011
  - Universal model
  - Defines a sequence of cyberattack phases with the goal of:
    - Understanding the mindset of cyberattackers, including their motives, tools, methods, and techniques
    - How they make decisions
    - How they evade detection
- Seven Phases
  1. Reconnaissance: gathers target information
  2. Weaponization: develops a malicious payload
  3. Delivery: transmits the weaponized payload
  4. Exploitation: payload is executed, target exploited
  5. Installation: installs malware/backdoor - persistence
  6. Command and Control: establishes a channel (C2)
  7. Actions on Objectives: goal achieved

Cyber Kill Chain

Defensive Objectives:

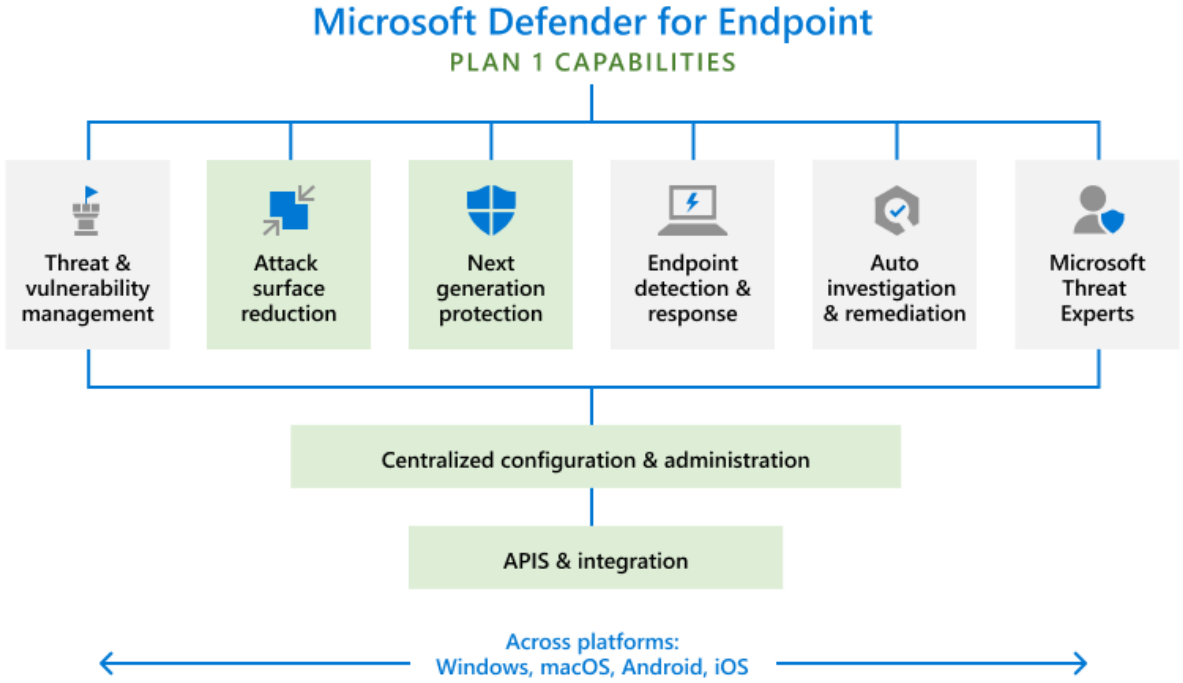
- Reduce the number of ways attacker gain initial access
- Lower the time to detect and respond to an attacker
- Increase the time for an attacker to accomplish their goal

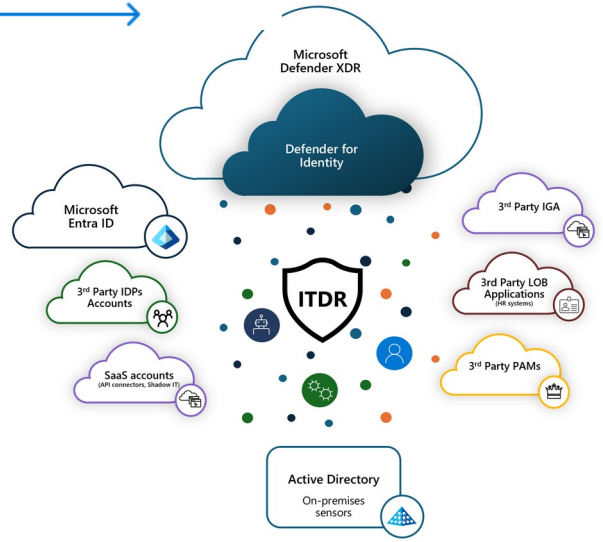


DAY 2 - SECTION 4

Cloud Security

Microsoft Defender





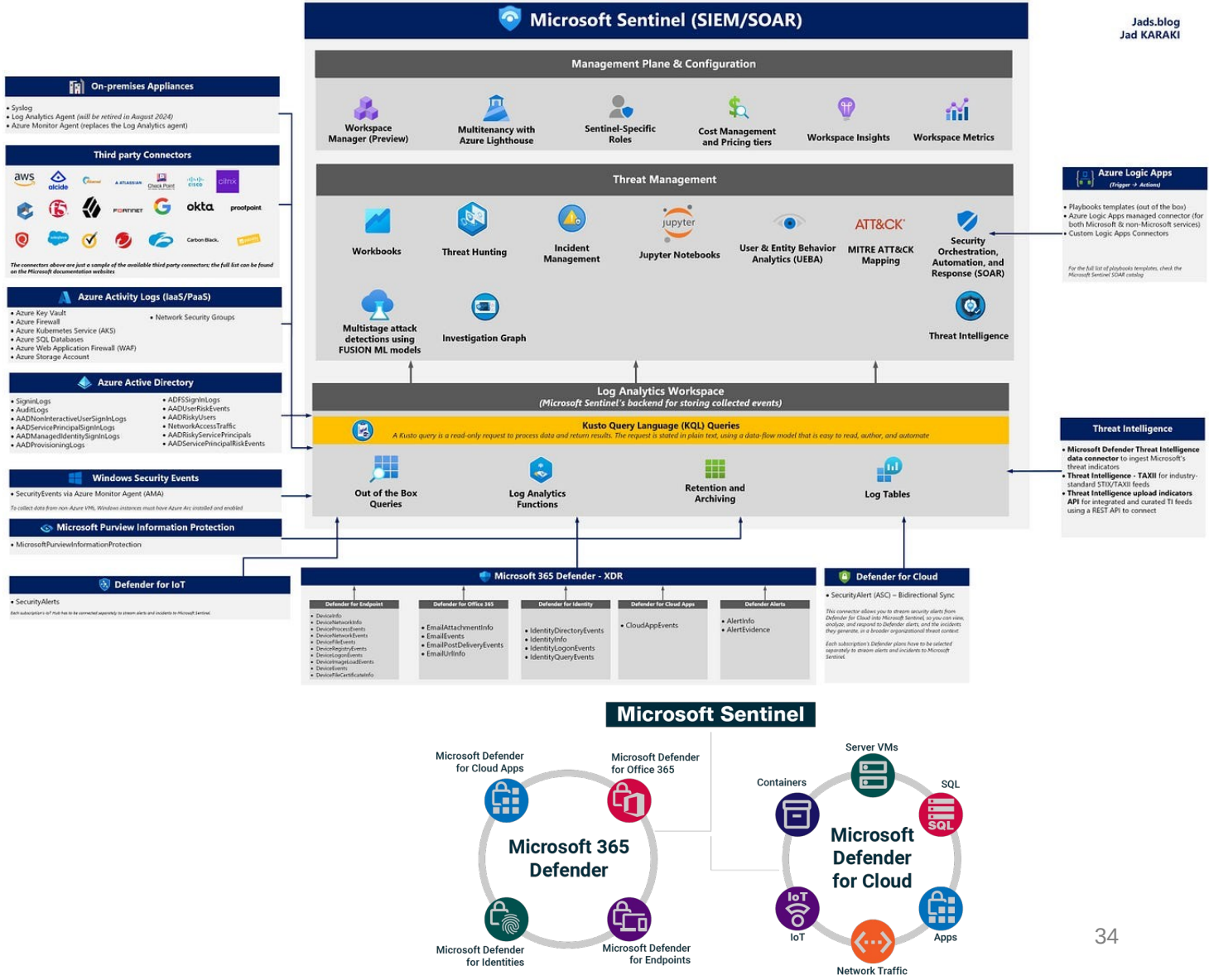
- End-point Detection / Response (EDR)
  - More than anti-virus
  - Includes threat and malware detection
  - Links to SIEM tools transparently across MS platforms

Cloud and premise

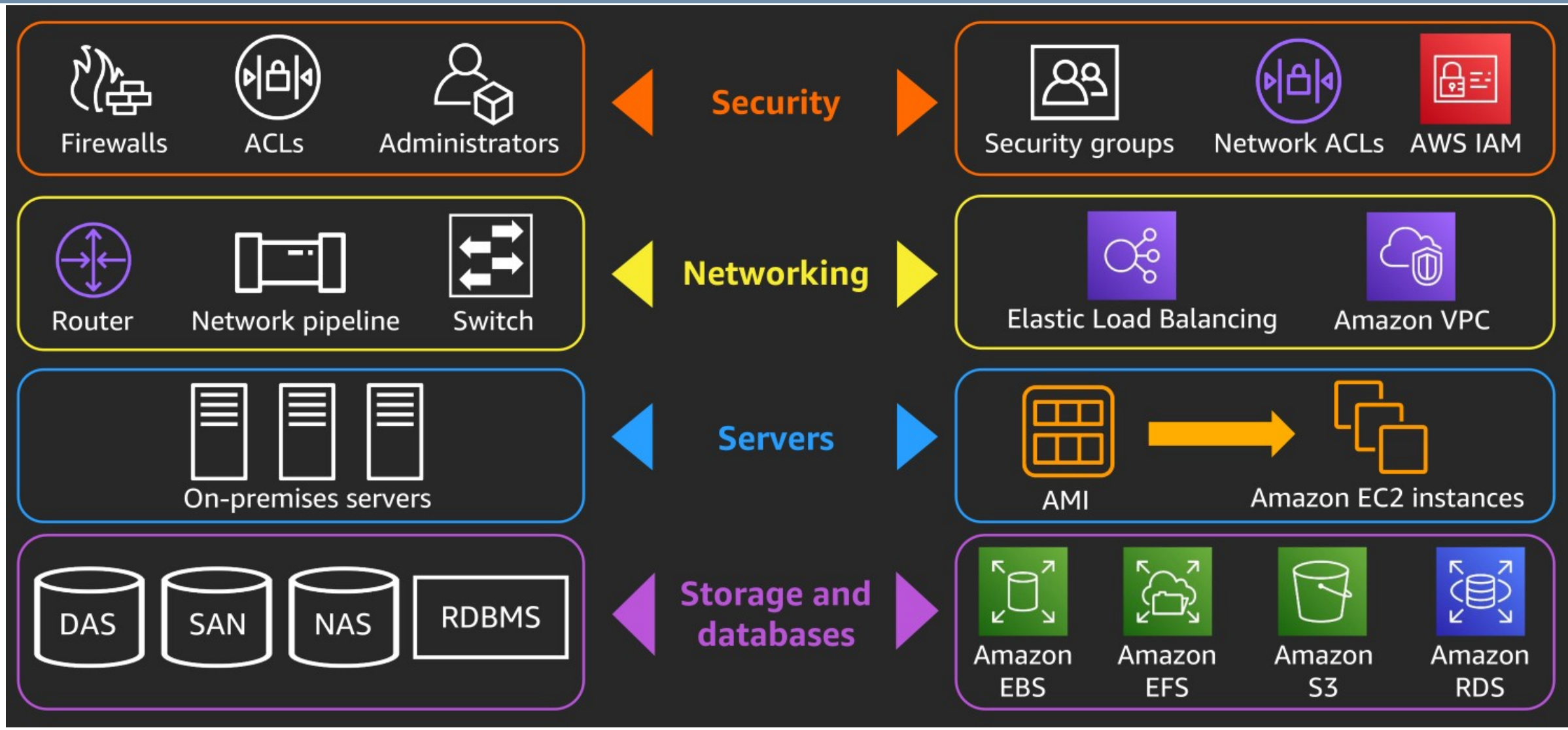
- Runs on Host machines
- Runs on virtual machines
- Run on cloud instances

Microsoft Sentinel

- Security Platform in Cloud
  - Collects EDR data
  - Collects host and server application and security log data
  - Ties into MS and third party applications
- Standard Dashboard for all Azure subscriptions
  - Incident Response Manager
  - Threat Hunting Module
  - Log Analytics
  - Framework interface



AWS Security



AWS Security

- Cloud Defense in Depth
  - Done differently than premise based hosts
  - Can be applied from template/ blueprint
- Concept of private endpoints
- Security Groups unique to cloud
  - Network based
  - Application based