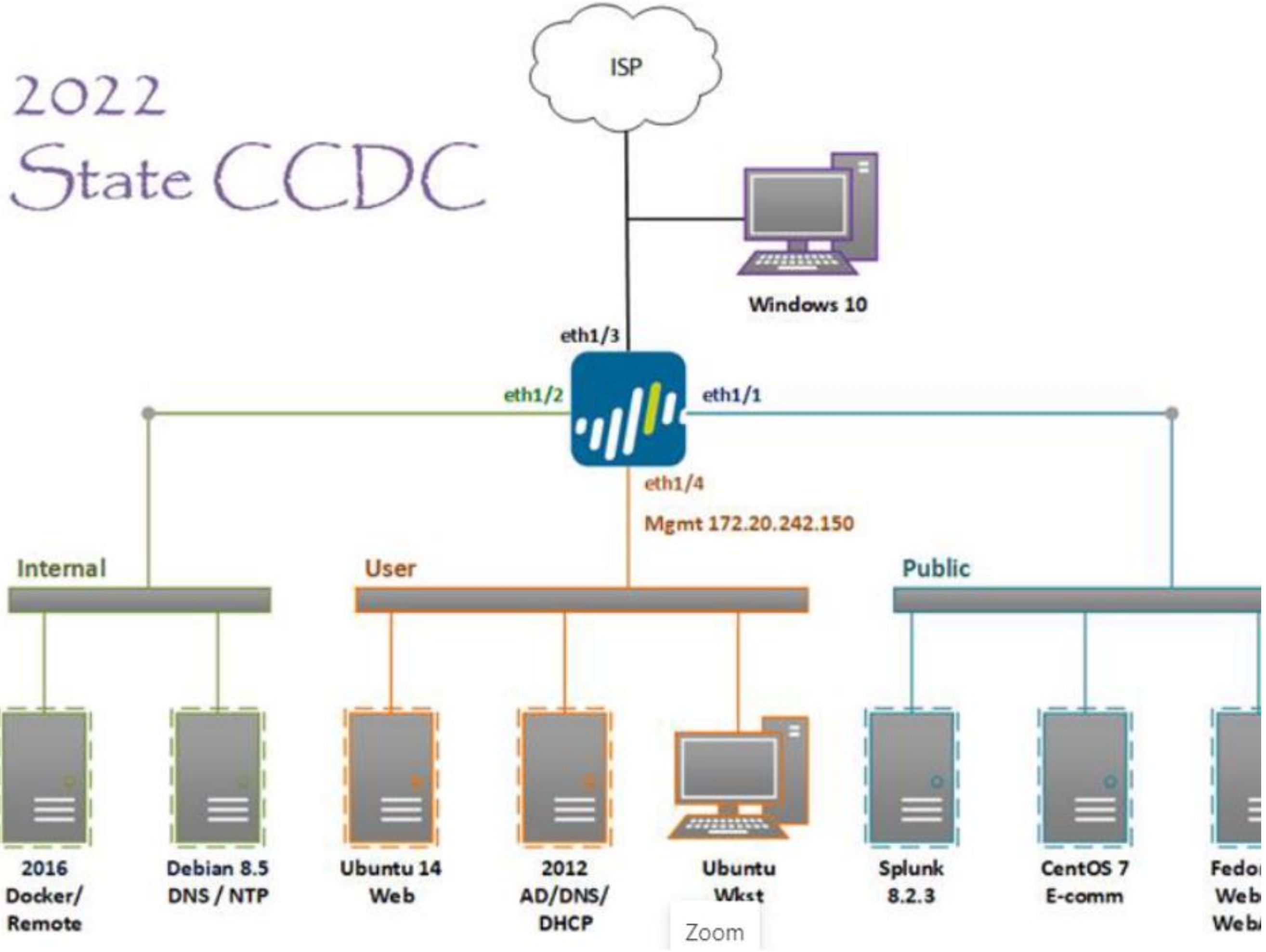
Overview of CCDC Servers/Services



DHCP "Dynamic Host Configuration Protocol"

DHCP is a network protocol used to automatically assign IP addresses and configuration settings to devices on a network. It simplifies the process of network administration by eliminating manual IP address assignment

Windows Server: You can use the DHCP Server role on Windows Server operating systems.

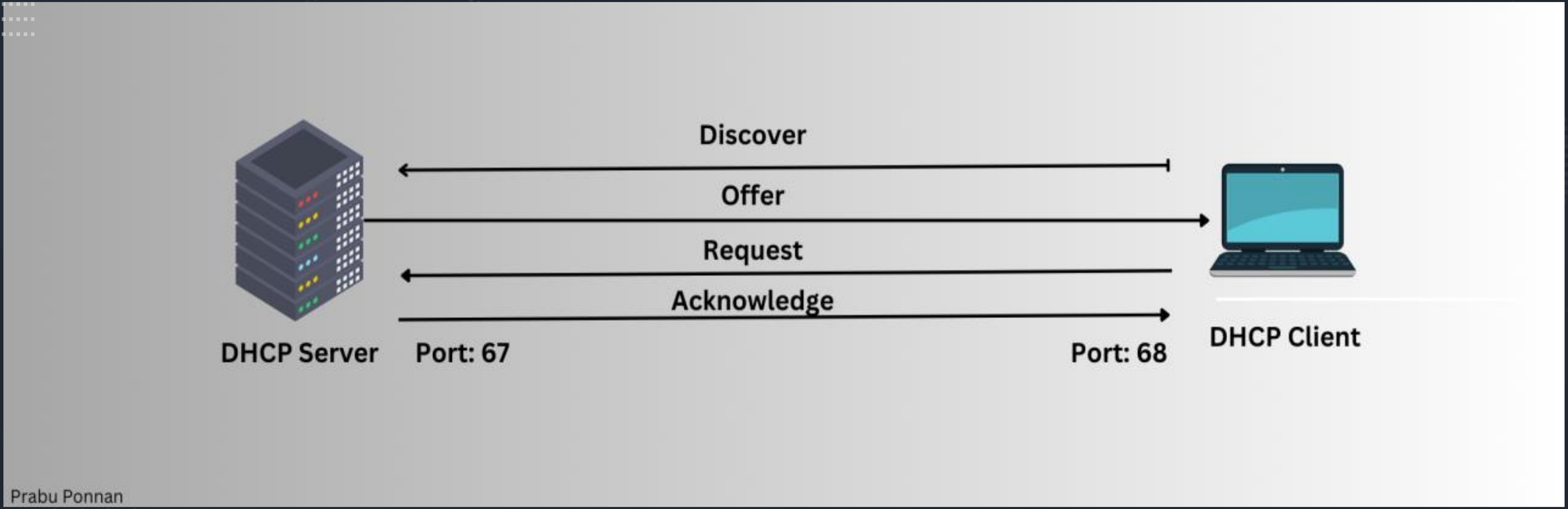
Linux: Popular DHCP server software for Linux includes ISC DHCP (dhcpd) and Dnsmasq.

This service is essential for our network to be able to talk to outside the network

If we see an APIPA address: 169.254. 0.1-169.254. 255.254 (there most likely is something wrong with DHCP)

DORA

- Discover
- Offer
- Request
- Acknowledge



DNS "Domain Name System"

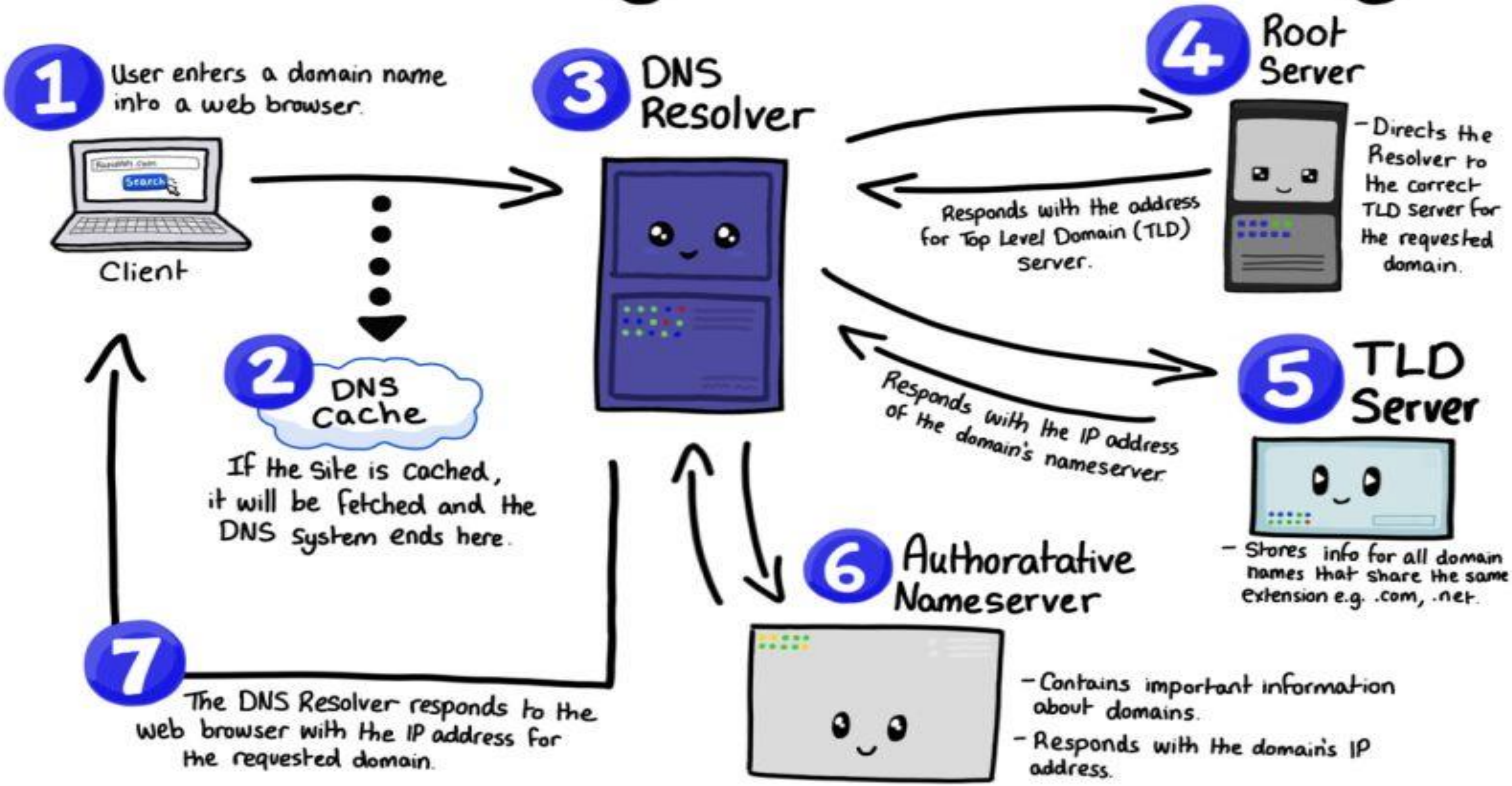
- The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

- Essentially DNS allows us to remember website and domains by actual name instead of having to remember the associated IP address.

- Windows Server - DNS server
- Unix-like – BIND (Berkeley Internet Name Domain)server

@Rapid_API

The DNS System Hierarchy



1 User enters a domain name into a web browser.

2 DNS Cache: If the site is cached, it will be fetched and the DNS system ends here.

3 DNS Resolver

4 Root Server: Directs the Resolver to the correct TLD server for the requested domain.

Responds with the address for Top Level Domain (TLD) server.

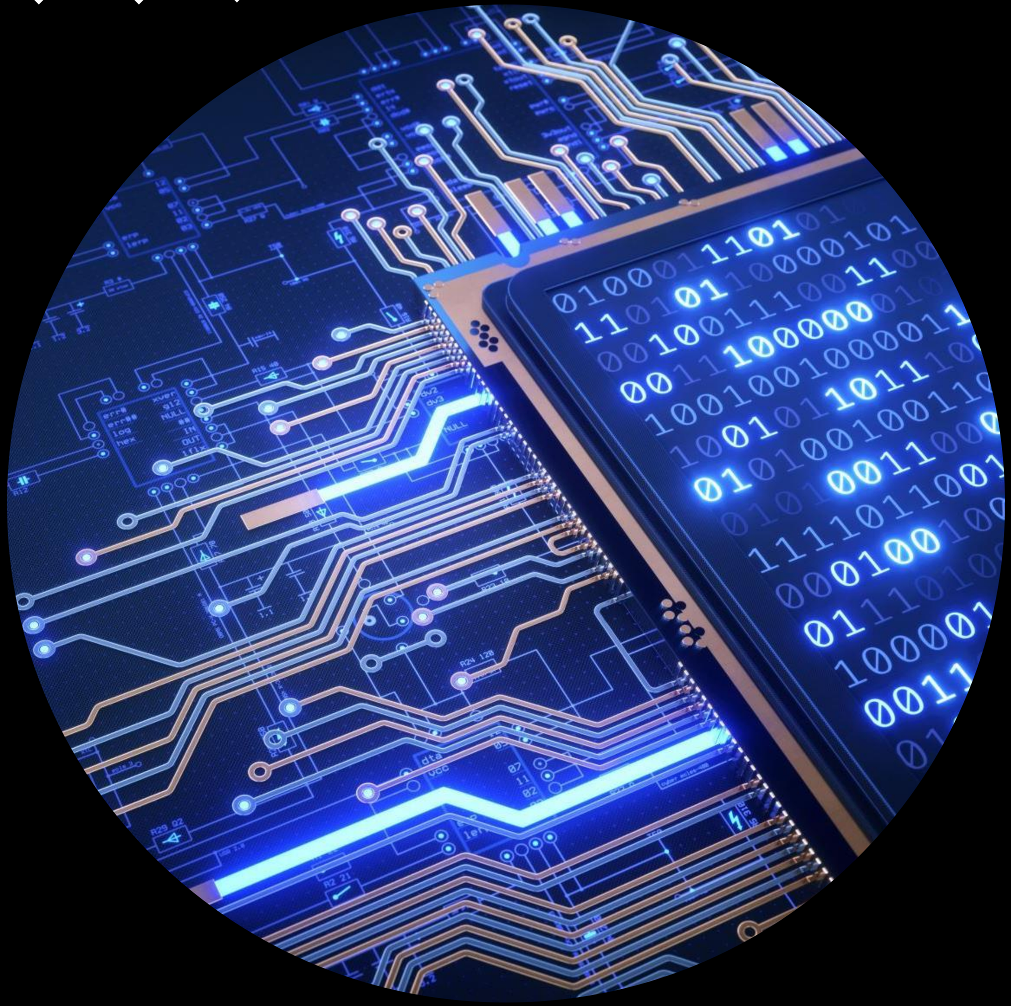
5 TLD Server: Stores info for all domain names that share the same extension e.g. .com, .net.

Responds with the IP address of the domain's nameserver

6 Authoratative Nameserver:

- Contains important information about domains.
- Responds with the domain's IP address.

7 The DNS Resolver responds to the web browser with the IP address for the requested domain.

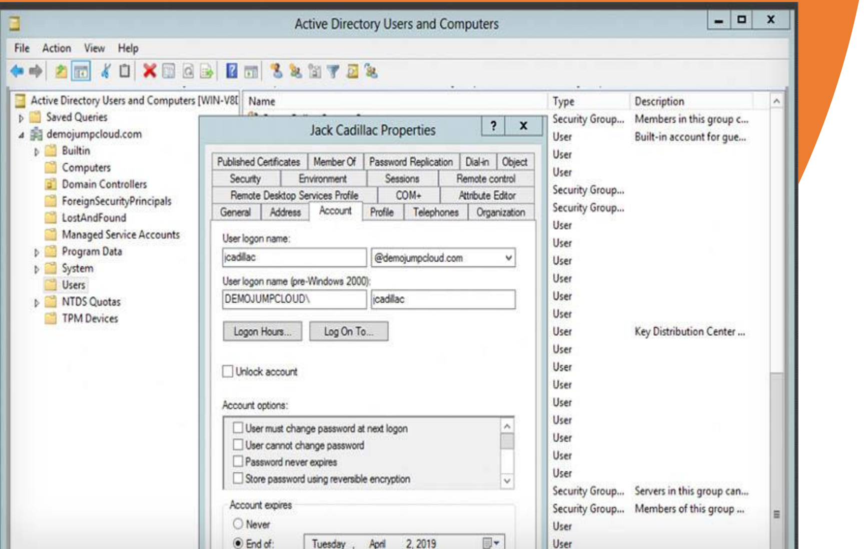


NTP

- Network Time Protocol, is a protocol used in computer networking to synchronize the clocks of computers and other devices on a network. It is essential for ensuring that the time and date on different devices are accurate and consistent, which is crucial for various applications.
- Network Security: Accurate time synchronization is vital for security protocols like Kerberos, which relies on synchronized clocks to prevent replay attacks.
- Logging and Auditing
- Data Replication
- Financial Transactions
- Communication and Collaboration
- NTP operates in a client-server model, where the client requests the current time from a more accurate time server.
- NTP packets contain information about the current time, as well as a timestamp indicating when the packet was sent. By comparing the time at which a packet was received with the timestamp in the packet, the client can calculate the network latency and adjust its clock accordingly.

Active Directory

- Active Directory (AD) is a directory service developed by Microsoft for managing and organizing information about network resources, such as users, computers, printers, and other networked devices, in a Windows domain network.
- It is an essential component of the Windows Server operating system and is commonly used in enterprise environments to centralize and simplify network management tasks.
- **Key aspects and features of Active Directory:**
- Directory Service: Active Directory functions as a centralized directory service, storing information about network objects and their attributes in a hierarchical, tree-like structure.
- Kerberos: A network authentication protocol that ensures secure communication between two entities over a non-secure network, such as the internet.
- Single Sign-On (SSO): AD enables SSO, allowing users to log in once and access various network resources without needing to enter their credentials repeatedly.
- User and Group Management: AD allows administrators to create and manage user accounts, groups, and organizational units (OUs). Users can be assigned various permissions and group memberships, which determine their access to network resources.
- Group Policy: Group Policy Objects (GPOs) allow administrators to define and enforce policies and configurations across the network, ensuring consistency and security.
- LDAP: Active Directory uses the Lightweight Directory Access Protocol (LDAP) for querying and modifying directory data. This allows integration with various applications and services that support LDAP.



User logon name: jcadillac @demojumpcloud.com

User logon name (pre-Windows 2000): DEMOJUMPCLOUD\ jcadillac

□ Unlock account

Account options:

□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires

○ Never
● End of: Tuesday , April 2, 2019

Name	Type	Description
	Security Group...	Members in this group c...
	User	Built-in account for gue...
	User	
	User	
	Security Group...	
	Security Group...	
	User	
	User	
	User	
	User	
	User	
	User	
	User	Key Distribution Center ...
	User	
	User	
	User	
	User	
	User	
	User	
	User	
	User	
	Security Group...	Servers in this group can...
	Security Group...	Members of this group ...
	User	
	User	

Security Information Event Management (SIEM)

- A security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations.

- At the most basic level, all SIEM solutions perform some level of data aggregation, consolidation and sorting functions in order to identify threats and adhere to data compliance requirements. While some solutions vary in capability, most offer the same core set of functionality such as:

  -Log Management

  -Event Correlation & Analytics

  -Incident Monitoring and Security Alerts

  -Compliance Management and Reporting

splunk>®

SNORT®

Web Email/Web Apps

- A web server is a software application or hardware device that serves as the foundation for websites and web applications on the internet. Its primary function is to receive and respond to requests from client computers, typically web browsers, by delivering web content (such as HTML pages, images, CSS files, JavaScript, and more) to the requesting clients. Web servers play a crucial role in making websites and web services accessible to users worldwide.

- Configuring and hardening a web-mail server on Fedora 21 involves setting up services like **Postfix** for SMTP and **Dovecot** for IMAP/POP3. Learning to have an understanding of mail transfer protocols will be vital.

- **Database Server:** If your webmail client requires a database (e.g., Roundcube uses a database for storing user preferences), you may need to install and configure a database server like MySQL or PostgreSQL.

E-commerce

- An e-commerce server is a specialized server that hosts an online store or e-commerce website. It enables businesses to sell products or services online and process transactions. The server plays a crucial role in handling customer data, payment processing, inventory management, and website functionality.

- **Web Server:** Common Web servers hosted may be Apache, Nginx

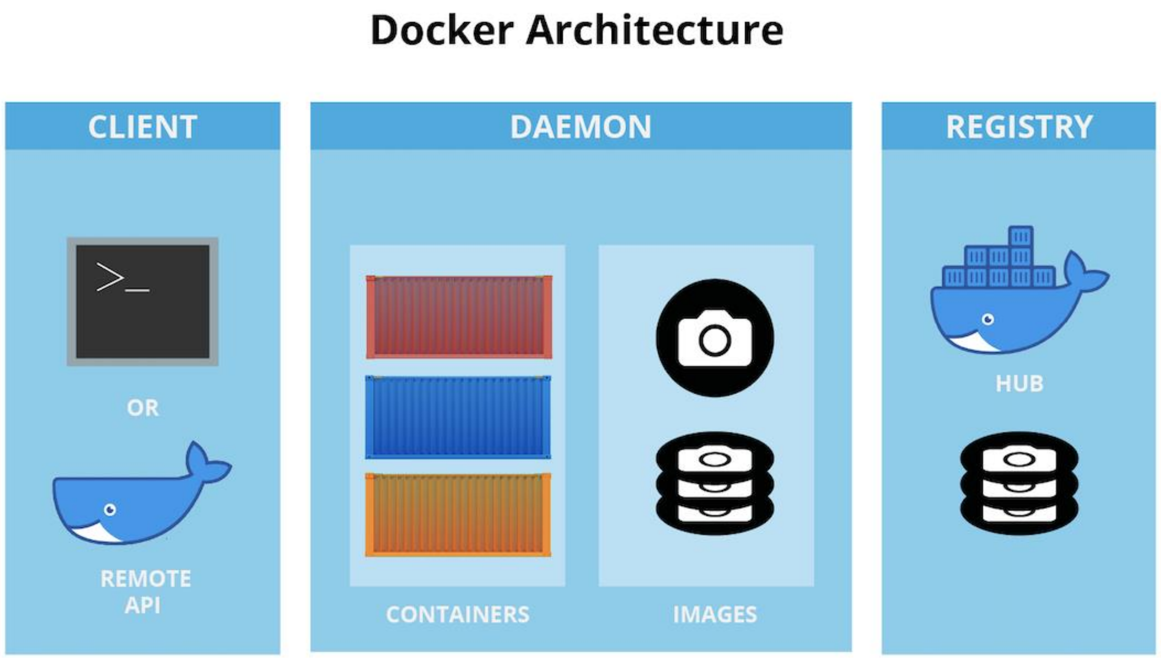
- **E-commerce Platform:** Choose an e-commerce platform like WooCommerce (for WordPress), Magento, Shopify, or build a custom solution. Install and configure the chosen platform according to your requirements.

- **Database Server**: To store product information, customer data, and transaction records. MySQL, PostgreSQL, or Microsoft SQL Server are often used.

- **Security Measures**: SSL/TLS certificates for secure data transmission, firewalls, intrusion detection/prevention systems, and regular security updates.

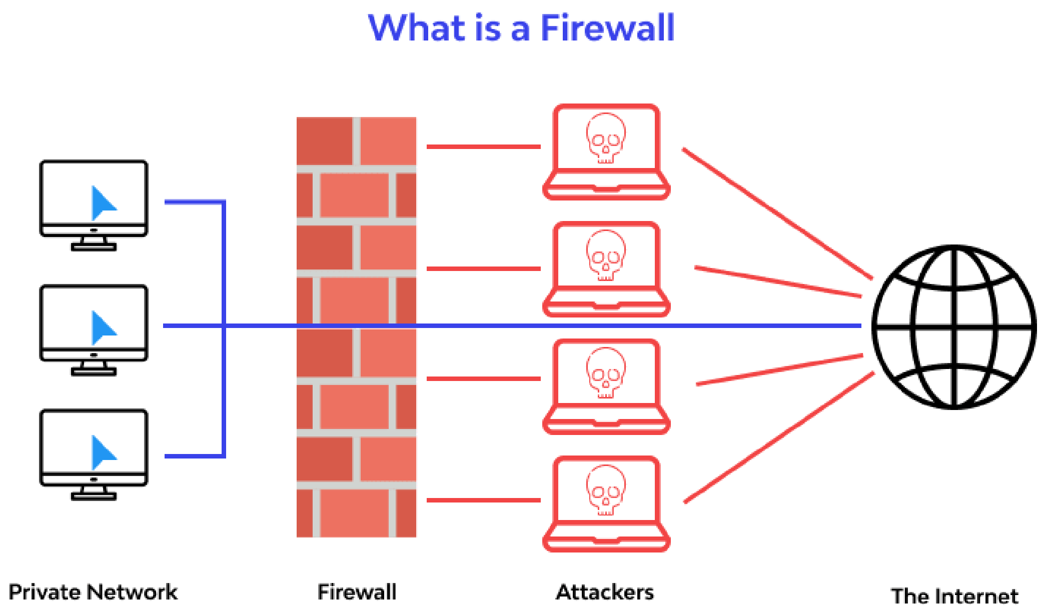
Docker

- What is Docker? Docker is a platform for developing, shipping, and running applications in containers.
- Why Containers? Containers are lightweight, standalone, and executable packages. They contain everything needed to run an application: code, runtime, libraries, and tools. Containers ensure consistency across environments, from development to production.
- Key Benefits: Portability, Isolation, Efficiency, Scalability, Version Control
- Components: Docker Engine, Images, Containers, Docker Compose, Docker Registry
- Use Cases: Application Deployment, Microservices, Continuous Integration/Continuous Deployment (CI/CD), DevOps



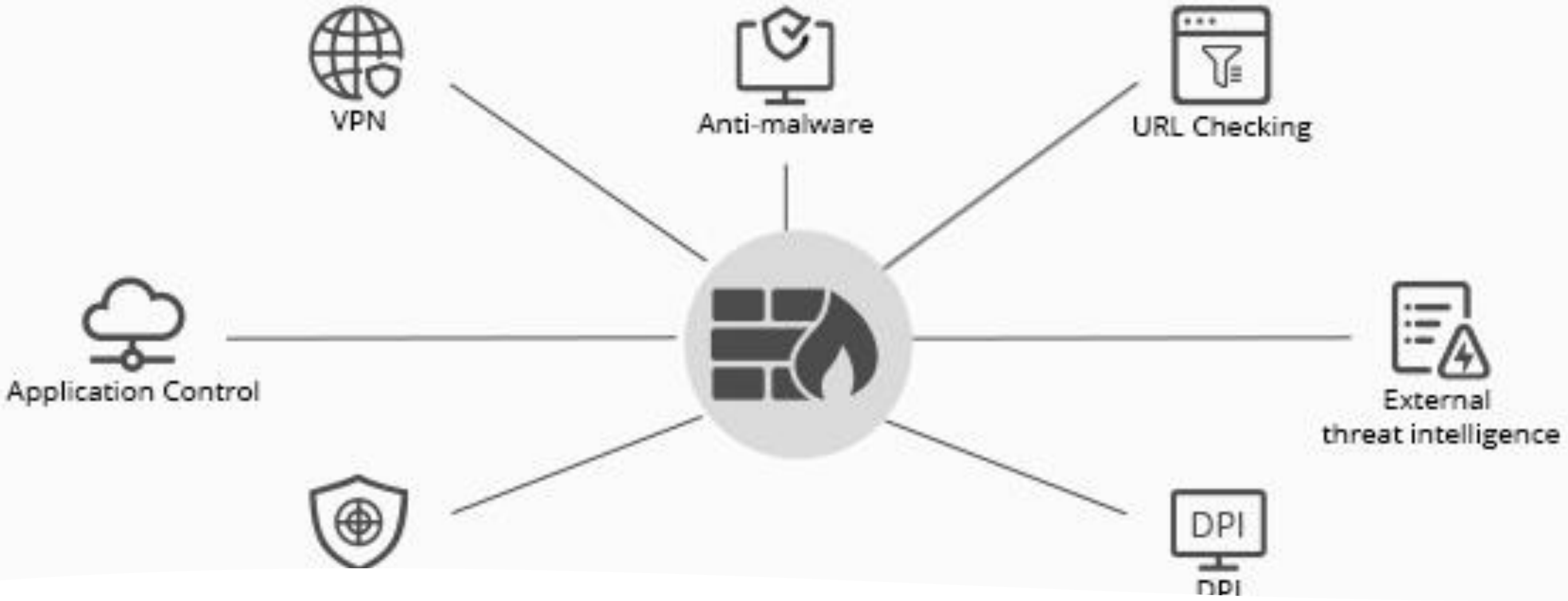
Palo Alto / Firewall

Firewall: Think of it as a digital barrier or gatekeeper that sits between your computer network and the outside world (the internet). Its main job is to monitor and control the traffic entering and leaving your network.



Firewalls

- **Security**: Its primary purpose is to enhance the security of your network. It can detect and prevent various types of cyber threats, such as malware (viruses, trojans), intrusion attempts (hackers trying to break in), and other malicious activities.
- **Features**: Palo Alto's NGFW typically offers a wide range of security features like antivirus, intrusion detection and prevention, content filtering, and more. It can also create rules and policies that specify how different types of traffic should be handled, giving you granular control over your network's security.



Next-Generation Firewall

- Next-Generation: This means it's not just a basic firewall that only looks at the source and destination of data packets. Palo Alto's NGFW goes beyond that. It examines the content of the data packets, understands the applications being used (like email, web browsing, or file sharing), and even identifies users. This allows it to make smarter decisions about what traffic to allow or block.

Scribe/Injects Objectives

- Create a list of items all other groups should send to you within the first 15.
  - Example: Many injects require a list of every servers MAC address. So, receiving this information early on can save time in the long run.
- Work on previous injects and save the final product. Then use that to create a mock template that we could use for the competition.
  - If we have an extensive archive of templates this can save a ton of time when submitting injects.

Scribe/Injects

- Injects GitHub
- Injects are business tasks that teams must address, or respond to, during the competition. Injects range from the very simple (e.g., resetting a user’s password), to the complex (e.g., migrating web servers from IIS to Apache with zero downtime). Many injects have a written portion (e.g., writing a report detailing actions taken by your team or the creation of a new engine will be checking functionality, so it’s not enough to have something “listening” to a specific port. The scoring engine (or scorebot) will check to make sure a web server exists and performing the desired function. For example, the web server is providing the correct content, a mail server sends and receives mail, and the DNS server responds to queries