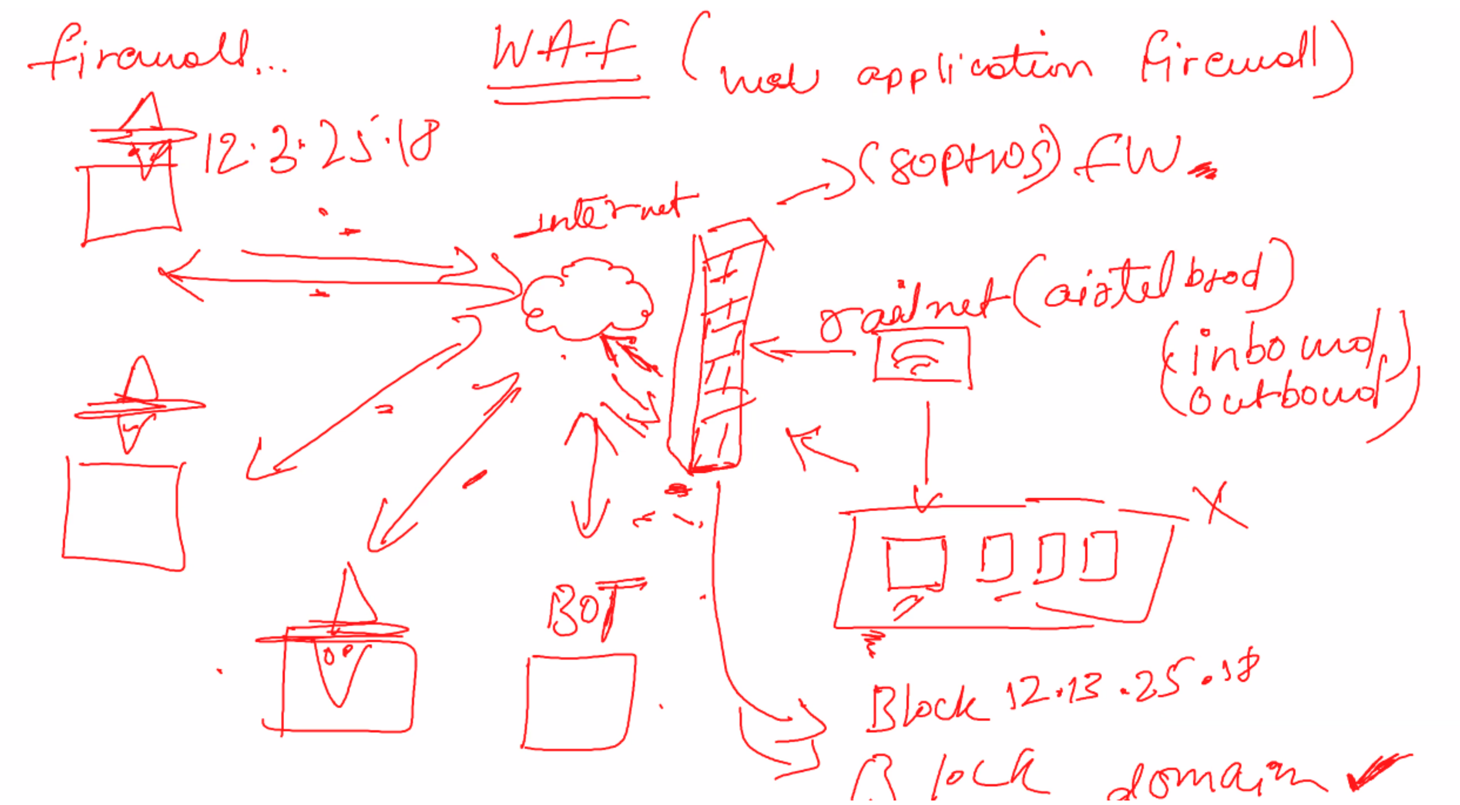
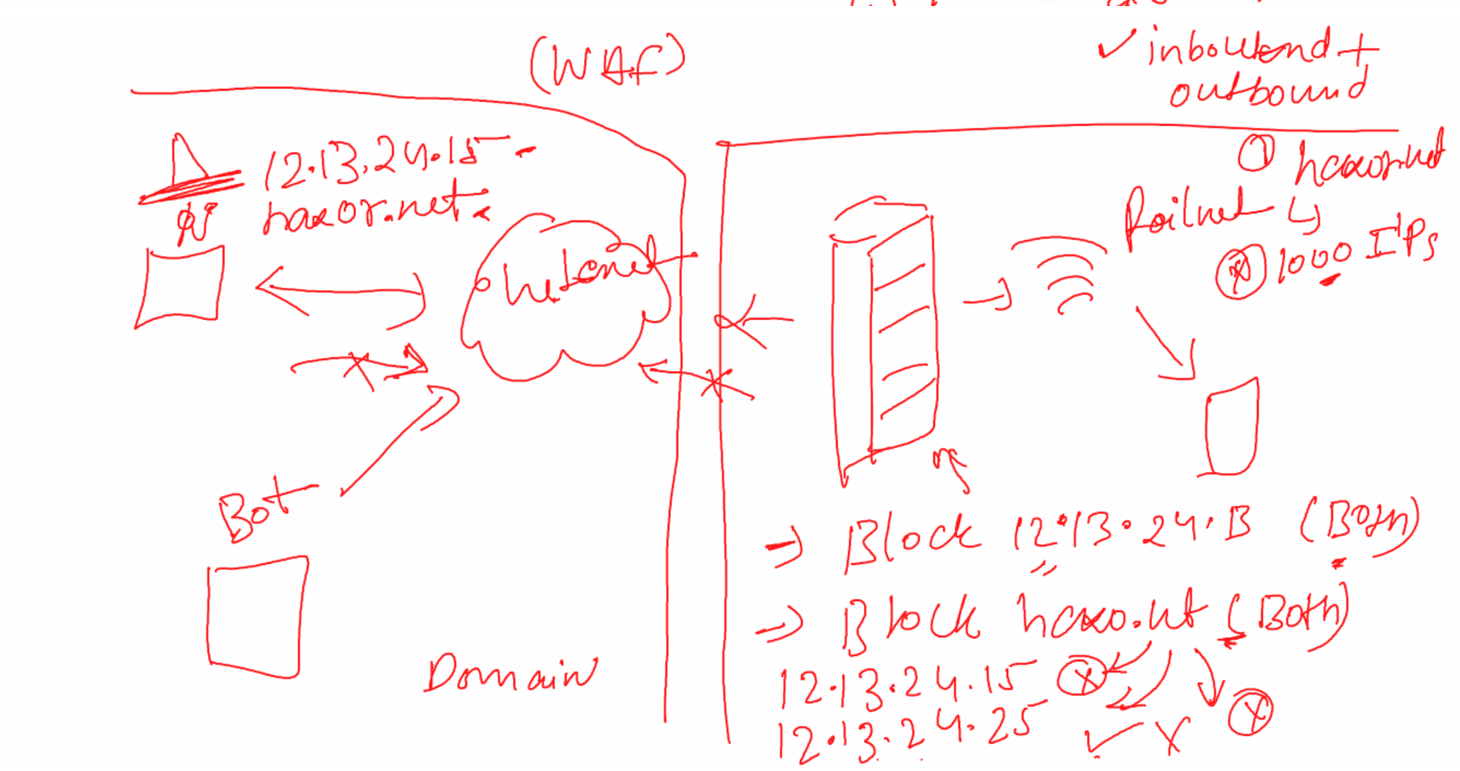
2024-08-02(Firewall+waf+covenant)





Firewall:

A firewall is a network security device or software designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. Its primary purpose is to establish a barrier between a trusted internal network and untrusted external networks, such as the internet, to protect the internal network from malicious traffic and cyber threats.

Key Functions of a Firewall:

1. **Traffic Filtering:**
   - Firewalls analyze network packets to determine whether to allow or block them based on security rules.
2. **Monitoring:**
   - They monitor network traffic for suspicious activity and provide logging and reporting.
3. **Access Control:**
   - Firewalls enforce policies that define who or what can access the network and what resources they can use.
4. **Preventing Unauthorized Access:**
   - They help prevent unauthorized users or systems from accessing private networks connected to the internet.
5. **Types of Firewalls:**
   - **Packet-Filtering Firewalls:** Inspect packets and allow or block them based on source and destination IP addresses, ports, or protocols.
   - **Stateful Inspection Firewalls:** Monitor the state of active connections and make decisions based on the context of the traffic.
   - **Proxy Firewalls:** Act as intermediaries between end-users and the web, making requests on behalf of the user.
   - **Next-Generation Firewalls (NGFW):** Include advanced features like deep packet inspection, intrusion prevention systems (IPS), and application awareness.

Examples of Firewall Usage:

- **Home Networks:**
  - Many home routers come with built-in firewalls to protect home networks from external threats.
- **Corporate Networks:**
  - Enterprises use firewalls to safeguard sensitive data, manage employee internet usage, and prevent breaches.

Importance of Firewalls:

Firewalls are crucial for maintaining network security, protecting against cyber-attacks, preventing data breaches, and ensuring that sensitive information remains confidential. They form the first line of defense in a comprehensive cybersecurity strategy.

inbound connection : incoming connection
outbound : outgoing communication

what is WAF (web application firewall) ?

A Web Application Firewall (WAF) is a security system designed to protect web applications by monitoring and filtering HTTP/HTTPS traffic between a web application and the internet. Unlike traditional firewalls that create a barrier between internal and external networks, a WAF specifically targets the security of web applications.

Key Features and Functions of a WAF:

1. **Application Layer Protection:**
    - WAFs operate at the application layer (Layer 7 of the OSI model), focusing on the data that web applications handle.
2. **Threat Detection and Mitigation:**
    - They identify and mitigate a variety of web-based attacks, such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).
3. **Rule-based Filtering:**
    - WAFs use rules to detect and block malicious traffic. These rules can be based on known attack patterns, IP addresses, or user behaviors.
4. **Customizable Security Policies:**
    - Organizations can create custom security policies tailored to their specific web applications and business needs.
5. **Logging and Monitoring:**
    - WAFs provide detailed logging and monitoring capabilities, allowing administrators to analyze traffic patterns and detect anomalies.
6. **Real-time Protection:**
    - WAFs offer real-time protection against emerging threats and vulnerabilities by updating rules and signatures.

Benefits of Using a WAF:

- **Enhanced Security:**
    - Protects web applications from a wide range of attacks, including the OWASP Top Ten vulnerabilities.
- **Compliance:**
    - Helps organizations meet regulatory compliance requirements such as PCI DSS by protecting sensitive data.
- **Reduced Risk:**
    - Reduces the risk of data breaches and cyberattacks, safeguarding both customer data and the organization’s reputation.
- **Easy Deployment:**
    - WAFs can be deployed as hardware appliances, software, or cloud-based services, offering flexibility in implementation.

Types of WAF Deployment:

1. **Network-based WAF:**
    - Deployed as a hardware appliance, it sits in front of web servers to filter traffic.
2. **Host-based WAF:**
    - Installed on the same server as the web application, it provides granular control and protection.

3. **Cloud-based WAF:**
    - Offered as a service by cloud providers, it provides scalability and ease of management without the need for physical hardware.

Examples of WAF Solutions:

- **Cloudflare WAF**
- **AWS WAF (Web Application Firewall)**
- **F5 BIG-IP Application Security Manager (ASM)**
- **Imperva WAF**
- **Akamai Kona Site Defender**

By implementing a WAF, organizations can significantly enhance the security posture of their web applications, protecting against common and emerging threats.

covenant installation:
Download .NET Core 3.1 (Linux, macOS, and Windows) (microsoft.com)

https://dotnet.microsoft.com/en-us/download/dotnet/thank-you/sdk-3.1.426-windows-x64-installer
restart
git software download : https://github.com/git-for-windows/git/releases/download/v2.46.0.windows.1/Git-2.46.0-64-bit.exe

```
$ ~ > git clone --recurse-submodules https://github.com/cobbr/Covenant
$ ~ > cd Covenant/Covenant
$ ~/Covenant/Covenant > dotnet run
```

Malicious IP database

URLhaus | Browse (abuse.ch)

Threat intelligence

```
cisco talos
```

Sandbox

```
ANY RUN
```