Assignment 18

1. *Explain the different types of firewalls. Discuss the policies and rules of any firewalls. What are the benefits derived? Discuss the best practices for the firewall configurations.*

Ans:

What is Firewall?

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules accepts, rejects, or drops that specific traffic.

Types of Firewall

Firewalls can be categorized based on their generation.

1. Packet Filtering Firewall

Packet filtering firewall is used to control network access by monitoring outgoing and incoming packets and allowing them to pass or stop based on source and destination IP address, protocols, and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers). Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers. Packet filtering firewall maintains a filtering table that decides whether the packet will be forwarded or discarded.

2. Stateful Inspection Firewall

Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.

3. Software Firewall

A software firewall is any firewall that is set up locally or on a cloud server. When it comes to controlling the inflow and outflow of data packets and limiting the number of networks that can be linked to a single device, they may be the most advantageous. But the problem with software firewall is they are time-consuming.

4. Hardware Firewall

They also go by the name “firewalls based on physical appliances.” It guarantees that the malicious data is halted before it reaches the network endpoint that is in danger.

5. Application Layer Firewall

Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused. In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy.

6. Next Generation Firewalls (NGFW)

NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.

7. Proxy Service Firewall

This kind of firewall filters communications at the application layer, and protects the network. A proxy firewall acts as a gateway between two networks for a particular application.

8. Circuit Level Gateway Firewall

This works as the Sessions layer of the OSI Model’s . This allows for the simultaneous setup of two Transmission Control Protocol (TCP) connections. It can effortlessly allow data packets to flow without using quite a lot of computing power. These firewalls are ineffective because they do not inspect data packets; if malware is found in a data packet, they will permit it to pass provided that TCP connections are established properly.

FIREWALL POLICY

A firewall policy dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types (e.g., active content) based on the organization’s information security policies. Before a firewall policy is created, some form of risk analysis should be performed to develop a list of the types of traffic needed by the organization and categorize how they must be secured—including which types of traffic can traverse a firewall under what circumstances.16 This risk analysis should be based on an evaluation of threats; vulnerabilities; countermeasures in place to mitigate vulnerabilities; and the impact if systems or data are compromised. Firewall policy should be

documented in the system security plan and maintained and updated frequently as classes of new attacks or vulnerabilities arise, or as the organization's needs regarding network applications change. The policy should also include specific guidance on how to address changes to the ruleset.

1. IP Addresses and Other IP Characteristics Firewall policies should only permit appropriate source and destination IP addresses to be used. Specific recommendations for IP addresses include:
2. Traffic with invalid source or destination addresses should always be blocked, regardless of the firewall location. Examples of relatively common invalid IPv4 addresses are 127.0.0.0 to 127.255.255.255 (also known as the localhost addresses) and 0.0.0.0 (interpreted by some operating systems as a localhost or a broadcast address). These have no legitimate use on a network. Also, traffic using link-local addresses (169.254.0.0 to 169.254.255.255) should be blocked.
3. Traffic with an invalid source address for incoming traffic or destination address for outgoing traffic (an invalid "external" address) should be blocked at the network perimeter. This traffic is often caused by malware, spoofing, denial of service attacks, or misconfigured equipment. The most common type of invalid external addresses is an IPv4 address within the ranges in RFC 1918, Address Allocation for Private Internets, that are reserved for private networks. These ranges are 10.0.0.0 to 10.255.255.255 (10.0.0.0/8 in Classless Inter-Domain Routing [CIDR] notation), 172.16.0.0 to 172.31.255.255 (172.16.0.0/12), and 192.168.0.0 to 192.168.255.255 (192.168.0.0/16).
4. Traffic with a private destination address for incoming traffic or source address for outgoing traffic (an "internal" address) should be blocked at the network perimeter. Perimeter devices can perform address translation services to permit internal hosts with private addresses to communicate through the perimeter, but private addresses should not be passed through the network perimeter. Outbound traffic with invalid source addresses should be blocked (this is often called egress filtering). Systems that have been compromised by attackers can be used to attack other systems on the Internet; using invalid source addresses makes these kinds of attacks more difficult to stop. Blocking this type of traffic at an organization's firewall helps reduce the effectiveness of these attacks. Incoming traffic with a destination address of the firewall itself should be blocked unless the

firewall is offering services for incoming traffic that require direct connections—for example, if the firewall is acting as an application proxy.

Organizations should also block the following types of traffic at the perimeter:

5. Traffic containing IP source routing information, which allows a system to specify the routes that packets will employ while traveling from source to destination. This could potentially permit an attacker to construct a packet that bypasses network security controls. IP source routing is rarely used on modern networks, and valid applications are even less common on the Internet.
6. Traffic from outside the network containing broadcast addresses that is directed to inside the network. Any system that responds to the directed broadcast will then send its response to the system specified by the source, rather than to the source system itself. These packets can be used to create huge "storms" of network traffic for denial of service attacks. Regular broadcast addresses, as well as addresses used for multicast IP, may or may not be appropriate for blocking at an organization's firewall. Multicast and broadcast networking is seldom used in normal networking environments, but when it is used both inside and outside of the organization, it should be allowed through firewalls.
7. Firewalls at the network perimeter should block all incoming traffic to networks and hosts that should not be accessible from external networks. These firewalls should also block all outgoing traffic from the organization's networks and hosts that should not be permitted to access external networks. Deciding which addresses should be blocked is often one of the most time-consuming aspects of developing firewall IP policies. It is also one of the most error-prone, because the IP address associated with an undesired entity often changes over time.

BEST PRACTICES :

1. Configure Network Firewalls to Block Traffic by Default

Even when IT teams do their best to follow firewall configuration best practices, they risk missing vulnerabilities that malicious actors can exploit. Setting firewall security to block traffic by default helps address this problem. When IT teams

block all unknown traffic trying to access the network, they make it much more challenging for unethical hackers to infiltrate the system.

2. Follow the Principle of Least Privilege

Of course, some people will legitimately need access to an organization's network. Organizations can configure their network firewall security to allow authorized users, but that doesn't mean that cybersecurity teams need to give them unlimited access. Each account should only have access to the files and tools necessary to do the user's job.

For example, an account belonging to a third-party vendor that fulfills orders only needs access to information about purchased products and where to send them. The vendor does not need any information about business processes, customer payment records, or other sensitive data. Following the principle of least privilege will ensure that all types of firewalls are able to secure the network more effectively.

3. Specify Source IP Addresses Unless Everyone Needs Access

In rare cases, IT teams might want to give everyone access to a part of the network. In these cases, they can configure their source IP addresses as ANY—for example, to let anyone visit a business's website.

If you don't want everyone on the internet to have access to a part of the network, however, specify the source IP addresses. Taking this step will limit the IP addresses to which traffic can connect.

4. Designate Specific Destination Ports

Always make sure that your organization's firewall network configuration designates specific destination ports for connected services. Perhaps a business has a destination port that lets authorized users access client contact information. In that case, establish that destination port as the source of that data and only let authorized accounts connect to it.

5. Open the Firewall Ports That Users Expect

Take the time to learn which ports users expect to find open when they try to access networks. The ports that IT teams open will depend on a few factors, such as the services and data that users tend to access and the types of servers and databases that the organization uses. You can find more information about Microsoft server ports here (Czechowski et al., 2022) and Linux server ports here (Kumar, 2021).

6. Designate Specific IP Address Destinations

Designating specific IP address destinations serves a similar purpose as designating destination ports. Organizations want to limit access to IP addresses to prevent unauthorized traffic from entering their networks.

Additionally, this type of firewall network protection can help prevent distributed Denial-of-Service (DDoS) attacks. DDoS attacks have become increasingly common, especially in the United States, the United Kingdom, and China (Sava, 2022). Implementing defenses against this type of attack is key to ensuring that customers, vendors, and employees can maintain access to the network.

2. *Discuss the configuration and rule sets for Mod Security. Explain briefly the features and functionalities of the Imperva Secure Sphere WAF.*

Ans: Configuration and rule set for mod security .

1. Install mod security
2. Enable mod security
3. Configure mod security
4. Implement rule sets
5. Tune and optimize rule sets
6. Monitor and maintain

Step 1. Install Mod Security

Open a terminal or SSH into your Ubuntu 20.04 server and using the following command the switch to the root user so you have the permission for later operations. Then, input password as prompted.

```
$ sudo -i
```

Next, update the package repositories to ensure you have the latest package information.

```
$ apt update -y
```

```
root@SALES:~# apt update -y
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu focal-security InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
114 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@SALES:~#
```

Download and install the ModSecurity Apache module using the following command and type y and enter.

```
$ apt install libapache2-mod-security2
```

```
root@SALES:~# apt install libapache2-mod-security2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  liblua5.1-0 libyajl2 modsecurity-crs
Suggested packages:
  lua geoip-database-contrib ruby python
The following NEW packages will be installed:
  libapache2-mod-security2 liblua5.1-0 libyajl2 modsecurity-crs
0 upgraded, 4 newly installed, 0 to remove and 114 not upgraded.
Need to get 547 kB of archives.
After this operation, 4279 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

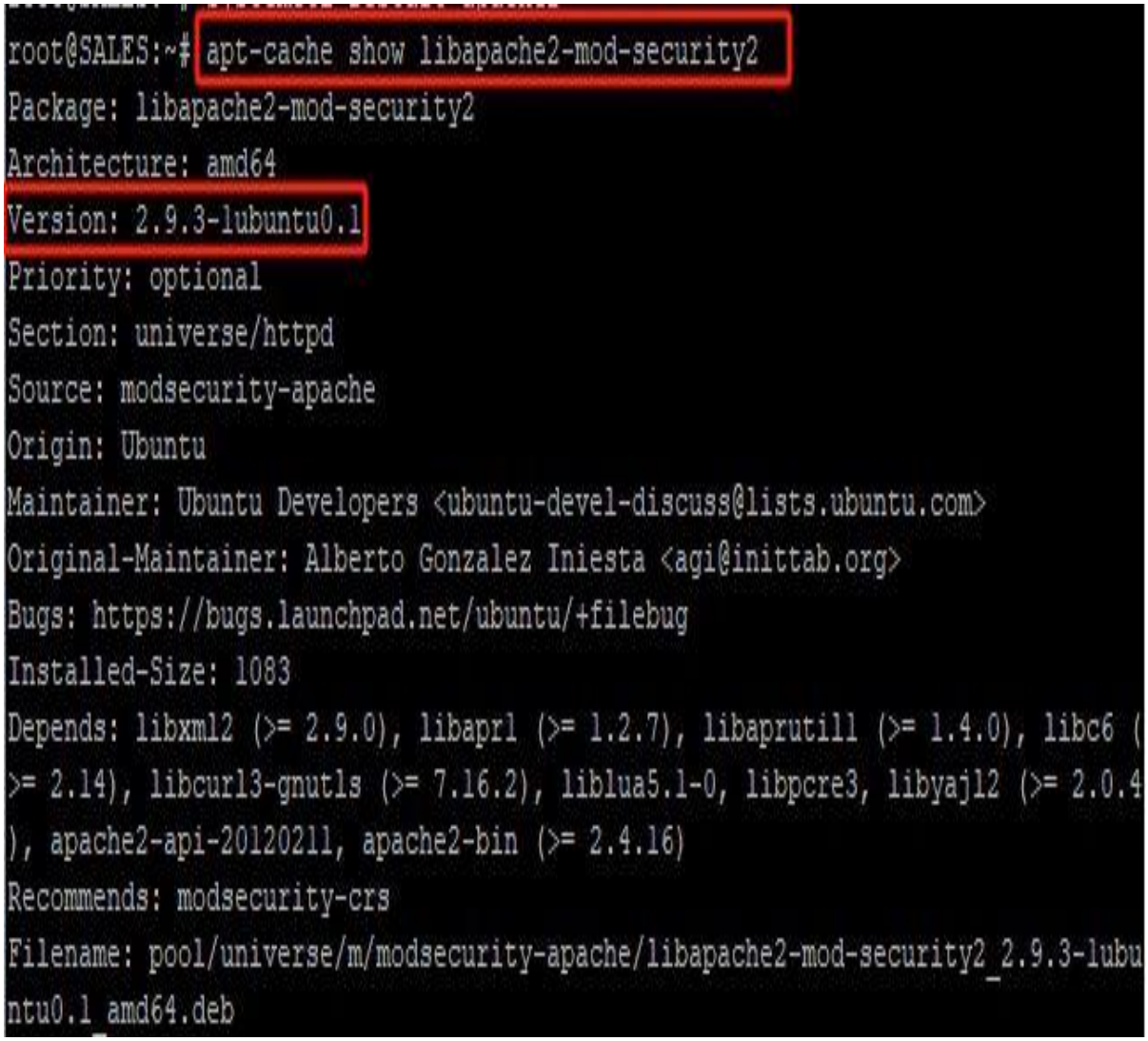
Restart the Apache service

```
$ systemctl restart apache2
```

```
root@SALES:~# systemctl restart apache2
root@SALES:~#
```

Ensure the installed software version is at least 2.9

```
$ apt-cache show libapache2-mod-security2
```



Explain briefly the features and functionalities of the Imperva Secure Sphere WAF.

Features :

1. Real time protection
2. API protection
3. Behavioral analysis
4. Automated policy generation
5. Compliance and reporting
6. Scalability and high availability

Functions :

1. Web application firewall
2. API protection
3. Best management
4. Threat intelligence
5. Behavioral analysis
6. Reporting and analytics .

3. Discuss the features of the Barracuda Web Application Firewall (BWAF). Explain the use-case example of this firewall, including scenarios, challenges, solutions, and benefits.

Ans:

Key Features of BWAF:

Comprehensive security

Data loss prevention

Access control

Load balancing

Easy deployment and management

USE CASES :

E-COMMERCE WEBSITE PROTECTION

SCENARIO :

SOLUTIONS : Deployment

Security Layer

DLP

Load Balancing

Reporting And Analytics

Challenges :

Multiple attack vectors

Security data

Performance

Solutions :

Comprehensive security

Data loss prevention

Access control

Load balancing

Centralized management .

FEATURES :

- Comprehensive protection

OWASP Top 10 Protection

Advanced Threats

Data Loss Prevention (DLP)

- Acces Control

Load Balancing

API Protection

DDoS Protection

Bot Mitigation

Logging And Reporting

Automated Threat Intelligence

Scalability

BENEFITS :

1. Enhanced Security Posture
2. Regularity Compliance
3. Improved Application Performance
4. Reduced Operational Costs
5. Ease Of Management
6. Scalable Deployment
7. Proactive Threat Mitigation
8. Customer Trust .

----------00000----------