Network Security Week CheatSheet

Terms and References

Firewall: A hardware device, or software program that filters packets. They look at each packet's destination and determine if it's allowed according to the rules it has.

> Example: A firewall sees a packet headed to IP 172.16.0.10 on port 22. It looks at it's list of rules and determines if that packet should be allowed to reach it's destination or not. If yes, the firewall allows the packet to pass. If No, the firewall drops the packet.

Access Controls: Firewalls operate using 'Access Controls'.

> Example: Protecting an SSH server by allowing only one IP address to connect is an access control because it restricts *access* to SSH to only a single host.

Web Application Firewall (WAF): A firewall specifically designed to understand application layer protocols.

> Example: It can identify suspicious HTTP traffic, log information about it, and drop it before it gets to the target server.

Host-based Firewall: A firewall used to protect a single host is called a host-based firewall.

> Example: These firewalls run on the computers they are meant to protect, and block traffic to/from that specific device.

Network Firewall: A firewall used to protect a whole network is called a network firewall.

> Example: A network firewall is often placed in front of a router, in order to block malicious traffic from the public Internet from entering the private network.

Firewall Rules: Every firewall has a set of rules that it follows. It is the job of the administrator in charge of setting up the firewall to configure the rules properly.

> Example: Firewalls read their list of rules from top to bottom. Because of this, it is extremely important that the rules are set correctly. For instance, if a block all rule happens first on the list, no traffic will get through, even if there is a following rule that allows traffic

> to a certain port.

Stateless Firewall: Firewalls that work on this "per-packet basis" are called stateless firewalls.

> Example: They are "stateless", because they don't "remember" anything about previous packets they have seen—each packet is treated independently of every other.

Statefull Firewall: These firewalls work by monitoring the whole TCP connection, instead of just its constituent packets.

> Example: These firewalls are able to determine which application protocol is in use, and determine if packets they're receiving belong in the connection. This helps provide insight as to which application-layer services are running on the network, as well as prevent attackers from corrupting data in existing connections.

Crucial Commands

UFW

UFW stands for 'Uncomplicated Firewall' and is the default firewall on most Linux systems.

```
# Check the status of ufw
sudo ufw status
```

Remember that you have to restart ufw before any changes take effect. ```bash

Turn on the ufw firewall or reload it

sudo ufw enable ```

```
# Reset the ufw firewall to default configuration
sudo ufw reset
```

Many times administrators will start by denying ALL traffic to a host, and then only allowing the traffic that it needs.

```
# Deny all traffic
sudo ufw default deny incoming
sudo ufw default deny outgoing
```

You can also deny or allow traffic to specific ports.

```
# Allow traffic to port 80
sudo ufw allow 80
```

You may have to delete a rule from time to time

```
# Delete a ufw firewall rule
sudo ufw delete deny 80
```

Firewalld

Firewalld is more complicated than ufw, but also more flexible. `firewalld` also allows you to organize firewall rules for different interfaces into different **zones**. This makes it easier to make isolated updates to specific interfaces.

Firewalld also doesn't require you to restart it between changes.

```
# Start the firewalld service
sudo /etc/init.d/firewalld start
```

```
# View all the firewall Zones
sudo firewall-cmd --list-all-zones
```

```
# Assign the interface eth1 to zone 'home'
sudo firewall-cmd --zone=home --change-interface=eth1
```

Firewalld also allows you to enable services per zone.

```
# List all available services to allow or deny
sudo firewall-cmd --get-services
```

```
# List all services applied to zone 'DMZ'
sudo firewall-cmd zone=DMZ --list-all
```

Setting rules with Firewalld require a bit more syntax than UFW

```
# Block traffic from address 10.10.10.10 in the office zone.
sudo firewall-cmd --zone=office --add-rich-rule="rule family='ipv4' sourc
e address='10.10.10.10' reject"
```