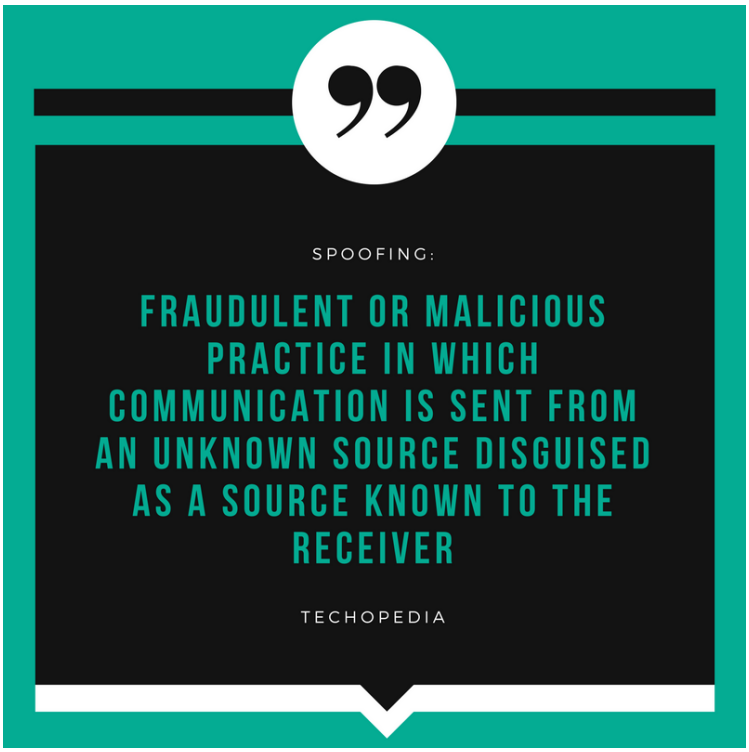
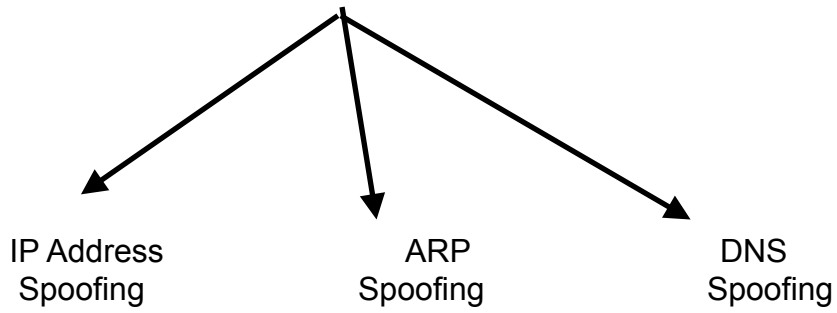
Anti-Spoofing

- What is Spoofing?

In simple terms, A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.



Types Of Spoofing Attacks



IP Address Spoofing Attacks

- IP address spoofing is one of the most frequently used spoofing attack methods.
- An attacker sends IP packets from a false (or “spoofed”) source address in order to disguise itself.

ARP Spoofing Attacks

- ARP is short for Address Resolution Protocol, a protocol that is used to resolve IP addresses to MAC (Media Access Control) addresses for transmitting data.

- In this attack, a malicious party sends spoofed ARP messages across a local area network in order to link the attacker’s MAC address with the IP address of a legitimate member of the network.

- ARP spoofing only works on local area networks that use the Address Resolution Protocol.

DNS Server Spoofing Attacks

- The Domain Name System (DNS) is a system that associates domain names with IP addresses.

- In a DNS server spoofing attack, a malicious party modifies the DNS server in order to reroute a specific domain name to a different IP address.

- In such cases, the new IP address will be for a server that is actually controlled by the attacker and contains files infected with malware.

- DNS server spoofing attacks are often used to spread computer worms and viruses.

Anti-Spoofing

Antispoofing is a technique for identifying and dropping packets that have a false source address.

Anti-Spoofing in Checkpoint

- There are series of actions taken by firewall when packet enters & exit from firewall.

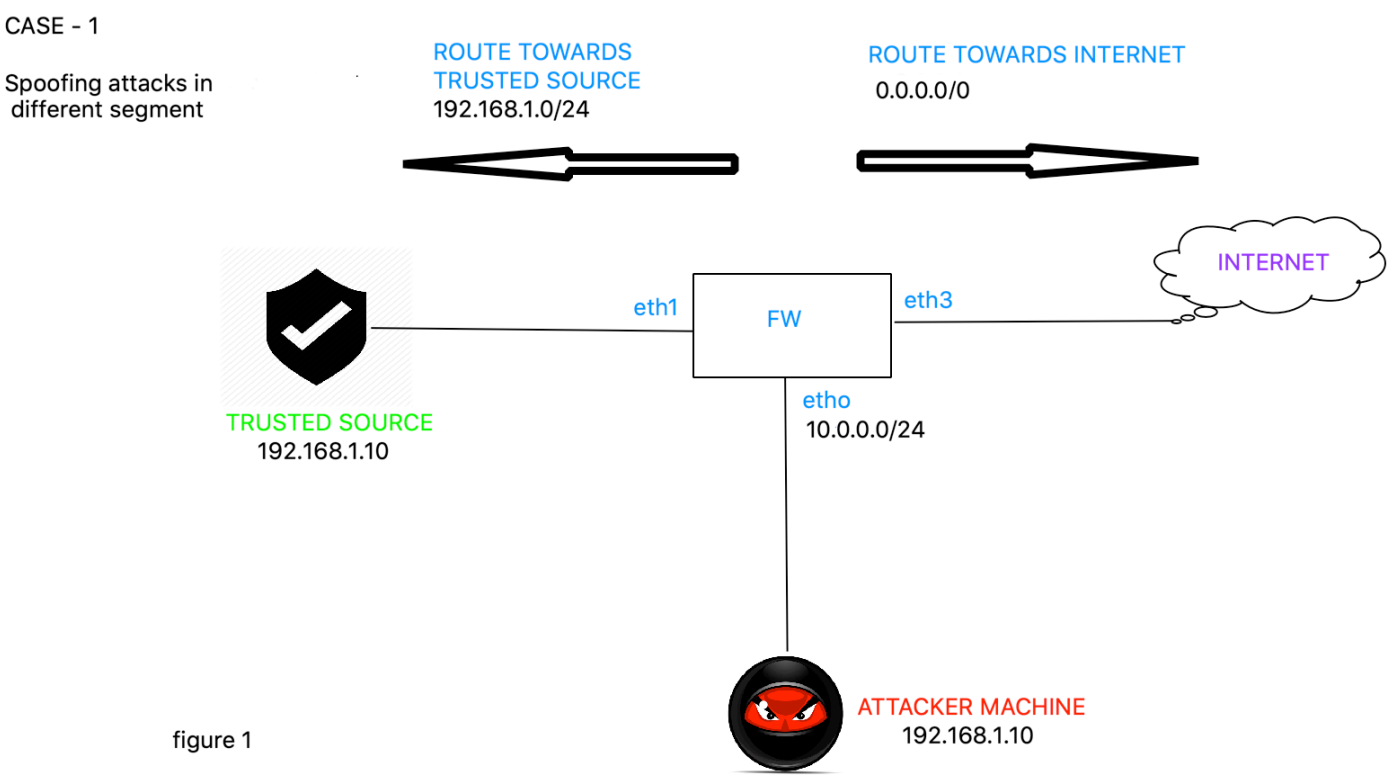


figure 1

CASE - 1 : Spoofing attacks in Different Segment

- Attacker's machine has spoofed IP address 192.168.1.10 and sends traffic to fw via interface eth0.
- Checkpoint GAiA OS will check routing for source IP address.
- 192.168.1.10 is going via interface eth1. Hence, it will drop traffic coming from Attacker's machine.

CASE - 2 : Spoofing Attack in Same Segment

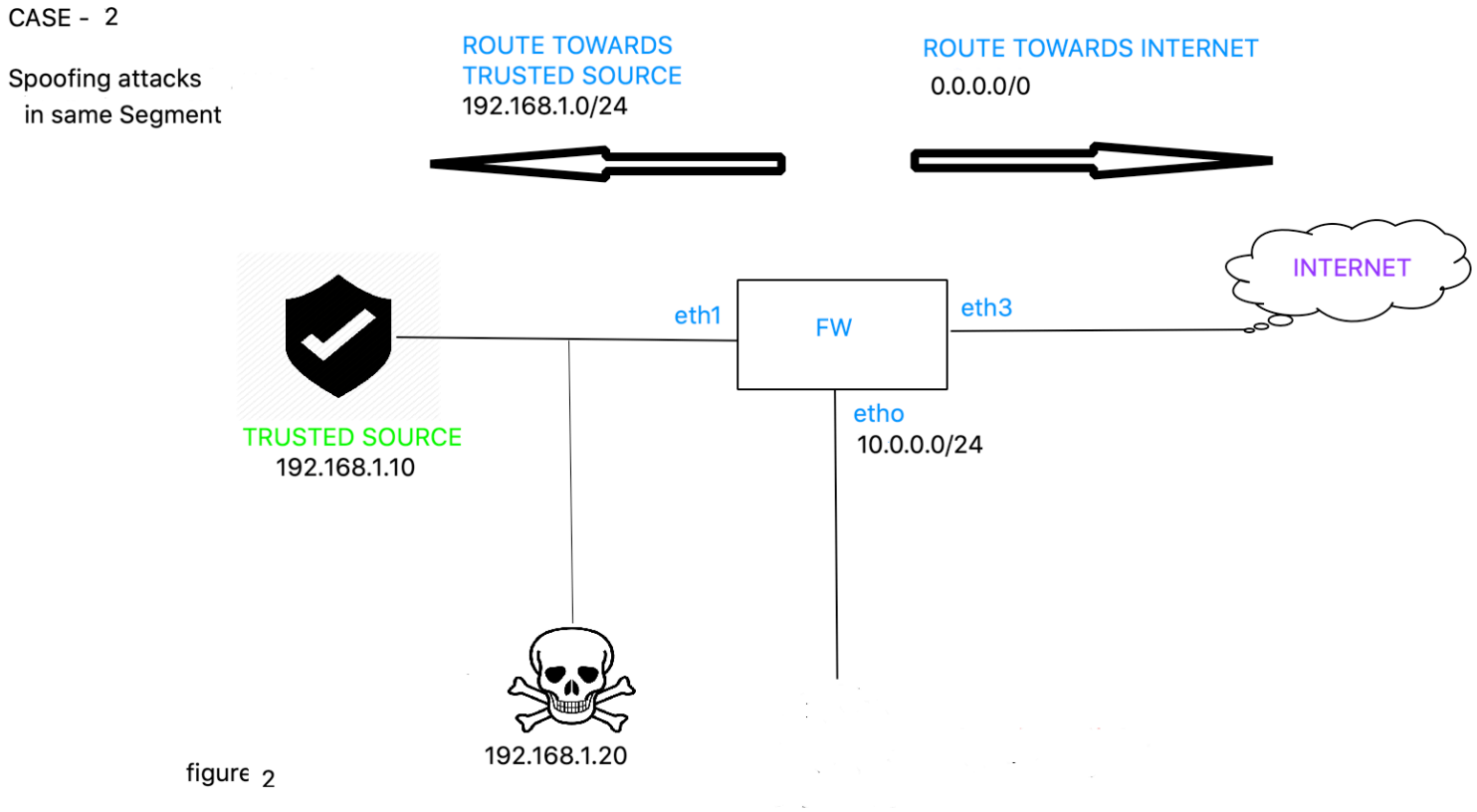


figure 2

- Attacker's machine 192.168.1.20 has spoofed IP address 192.168.1.10 and sends traffic to firewall via interface eth1.
- Firewall can't detect spoofing in same segment as reverse source route is going to be same.

CASE 3: Spoofing Attacks on External Interface

- Fw depends on topology of rest of the interfaces. If IP coming from eth3 (External Interface) is not configured on internal interface, it will be allowed
- If IP coming on Ext Interface is part of topology, it will drop.

SAM Database : Suspicious Activity Monitoring

- SAM database is a database of blacklisted IP addresses. Attacks passing through anti-spoofing reach on SAM database.

There are two ways to build this database.

1) Realistic Approach: Check hits of suspicious IP manually.

2) Proactive Approach: ETM (Enterprise Threat Monitoring) team will give us suspicious IP address, block them and add to SAM database.

How to create SAM rules?

- Refer to Solution ID : sk112061 here .

Other ways to Detect Spoofing

- Use spoofing detection software: There are many programs available that help organizations detect spoofing attacks, particularly ARP Spoofing. These programs work by inspecting and certifying data before it is transmitted and blocking data that appears to be spoofed.

- Use cryptographic network protocols: Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS) and other secure communications protocols bolster spoofing attack prevention efforts by encrypting data before it is sent and authenticating data as it is received.

- Hosts receiving a suspicious packet can also use certain techniques to determine whether or not the IP address is spoofed. The first (and easiest) one is to send a request to the address of the packet and wait for the response; most of the time the spoofed addressees do not belong to active hosts and hence no response is sent.

- Another method is to check the Time to Live (TTL) value of the packet, and then send a request to the spoofed host. If the reply comes, you can compare the TTL of both packets. Most probably the TTL values will not match. But this is not a sure shot method to detect spoofing.

———————-X———————

Documented By:

Rohit Gandas

rohit3120@gmail.com