Penetration Testing and Vulnerability Analysis using Kali Linux and their Countermeasures

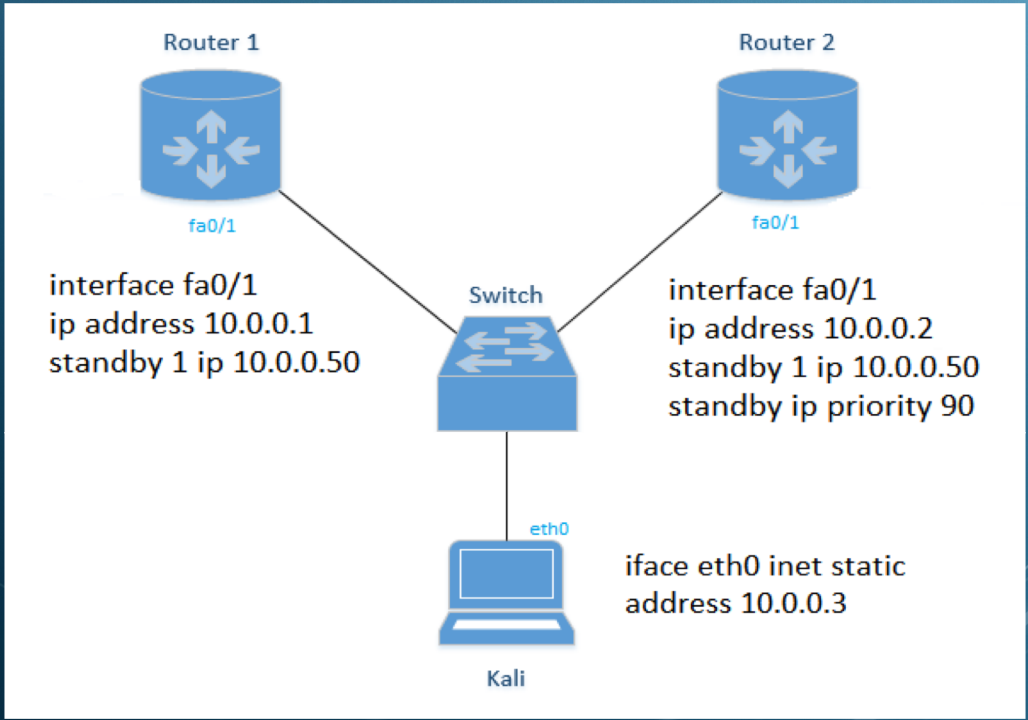
- Apurva Varalikar
- Jugal Shah
- Omkar Dhomane
- Omkar Salunkhe

Attacks Implemented

1. Taking over HSRP
2. Becoming the root bridge of STP
3. DNS spoofing
4. Session Hijacking

Taking over HSRP

Topology



Attack Description

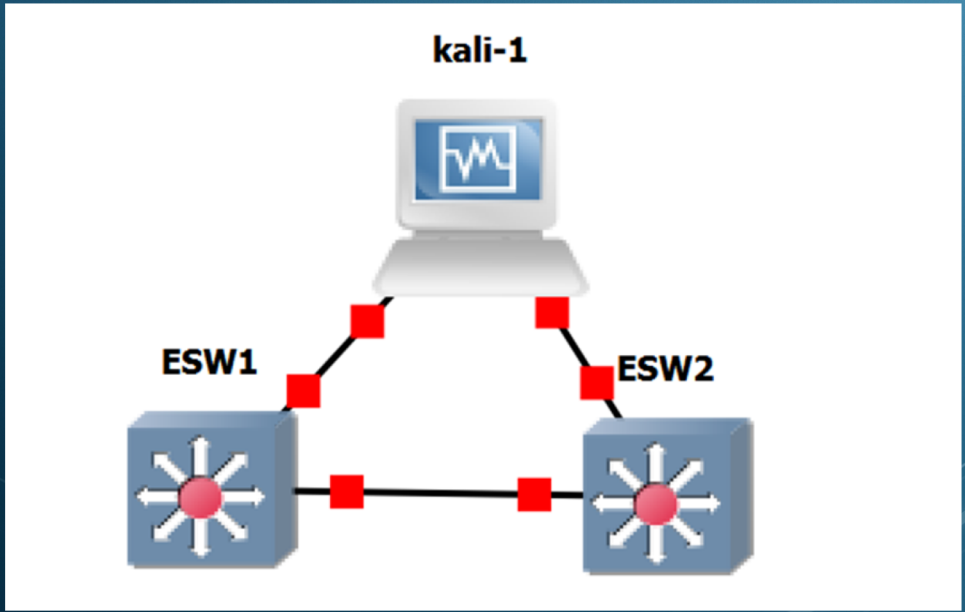
- The malicious entity assumes the role of the active device by increasing its own priority value and overthrowing the existing active device.
- The attacker can then implement either DoS or MITM attack on getting the control of the active default gateway
- Tools: GNS3, Yersinia

Countermeasures

- SNMP traps can be setup so that an alert is sent immediately if the bad authentication is seen allowing for network staff to investigate the issue.
- Use MD5 authentication using key chains or key strings or a mixture of the two. Configuration for key strings is very straightforward; add the following command on all routers participating in HSRP for that group: standby <HSRP Group Number> authentication text <Authentication String>
- Once configured, all devices will use this string to hash message data and if a router attempts to join the HSRP group with an incorrect key, a warning is thrown.

Becoming the root bridge on STP

Topology



Attack Description

- The attacker becomes the root bridge of the topology by decreasing its BPDU ID to one that is lower than that of the current root bridge forcing an entire network re-convergence.

- On launching the attack, the kali host becomes the root with all of its ports becoming designated ports.

- Tools: GNS3, Yersinia

Countermeasures

- Root Guard:

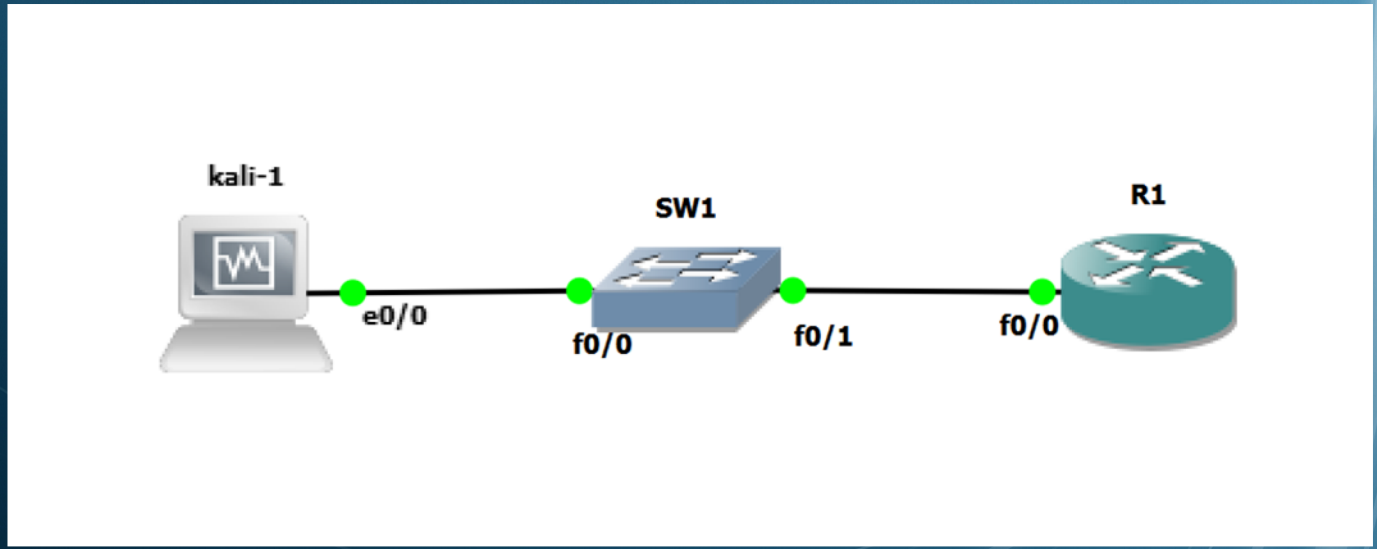
This feature helps control where root bridges can be connected.

- BPDU Guard:
- Concept of Portfast

This feature is enabled by default when Portfast is enabled and helps avert the possibility of a rogue switch becoming the root.

CDP Flooding Attack

Topology



Attack Description

- CDP is a Cisco proprietary protocol which allows Cisco devices to announce and share information to their neighboring devices. These messages contain detailed information about themselves, such as the software version, IP address, platform, capabilities, and the native VLAN.
- An attacker can exploit a vulnerability in CDP that allowed Cisco devices to run out of memory and potentially crash if you sent it tons of bogus CDP packets.
- When a switch is overwhelmed and can no longer forward frames it will start to forward frames out all ports just like a hub.
- Tools: GNS3, Yersinia

Countermeasures

Consider disabling CDP on interfaces which, or being very selective in its use in security sensitive environments.

One way to obviate a CDP flood attack is to disable CDP on the entire switch:

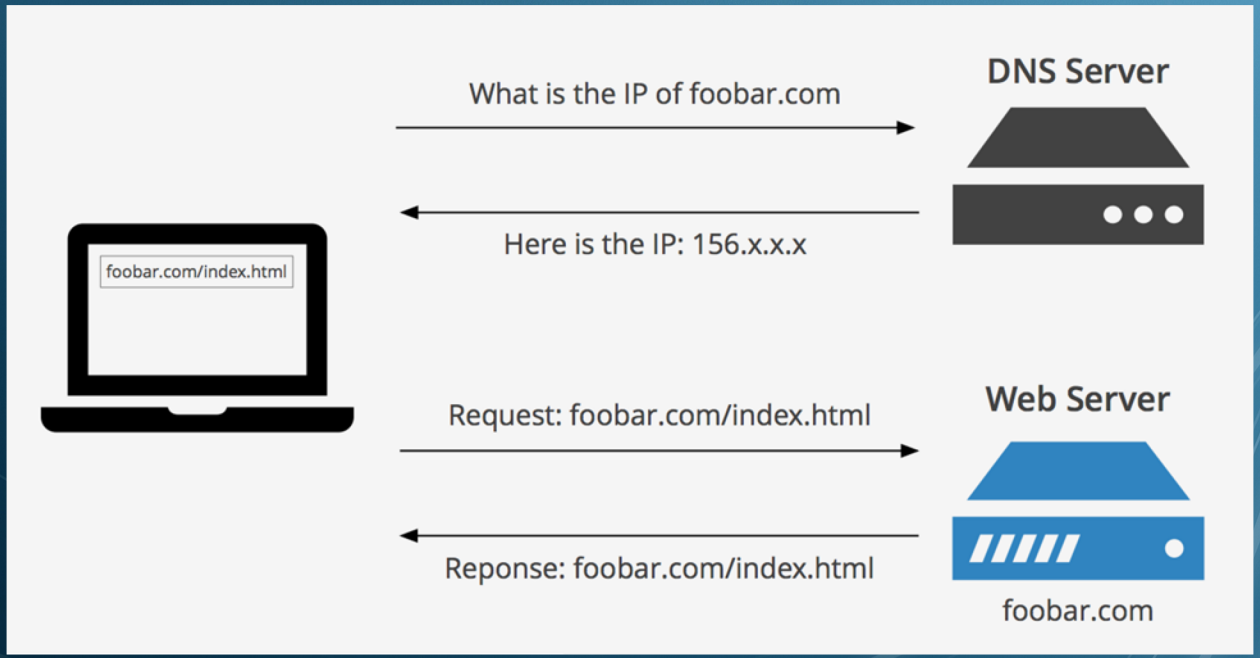
```
config t
no cdp run
```

or you can pick specific interfaces that don’t need it

```
config t
int gi3/0/1
no cdp enable
```

DNS Spoofing

Topology



Attack Description

- The attacker poses to be a legit Domain Name Server and returns incorrect IP address to the user's request
- When the user requests for an address resolution, it is mapped to a malicious DNS server and it leads the user to his intended page, either fake or some other website
- Tools: DNS Spoof (dsniff), Virtualbox

Countermeasures

- Two factor authentication
- DNS change Locking
- IP-dependent log in
- DNSSEC

Thank You!

Any Questions?