Lab environment:

The setup infrastructure includes an interconnected set of virtual hosts and devices running in a virtual machine named eve-ng. Access to the infrastructure is via a web-based interface. The infrastructure includes the following hosts:

* LinuxRouter – router connecting the network to the Internet
* Client – client with a graphical user interface running Ubuntu
* Attacker – attacker running Kali Linux
* Rogue DHCP server – DHCP server connected to the network
* WebServer – machine hosting a web server in the network

Initial Setup:

* Start VMWare Workstation or VMWare Player
* Start the eve-ng17 virtual machine
* Note the IP address of the machine, as in the example below:

A screen shot of a computer

Description automatically generated

Open a Chrome browser and navigate the address listed in the eve-ng prompt (e.g. <http://192.168.0.37> in the example above; *do not enter the address from the above screenshot – check the address on your machine and enter that one*). Login using the following credentials (*use the Chrome browser*):

Username: Admin

Password: eve

Console: HTML5

A screenshot of a login form

Description automatically generated

Click on the **test.unl** file and then **Open**

You should see the following diagram:

A diagram of a computer network

Description automatically generated

We will explore three types of attacks:

* Rogue DHCP server (using the RogueDHCP host)
* DHCP starvation (using a script that you can create)
* Web server DoS (using an attack called Slowloris – details [here](https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/) and tool available [here](https://github.com/gkbrk/slowloris))

In the following activities, in order to access a machine, you must click on the respective icon in the diagram. For example, in order to access the Attacker machine, you must click on the Attacker icon and a separate tab window should open. When connecting to the switches or router, you might be presented with a blank black screen; just press Return and the command prompt will come up.

Machine switched off:

A computer server and globe

Description automatically generated

Machine switched on:

A computer server and a globe

Description automatically generated

Credentials used

* LinuxRouter, WebServer
  + Username: root
  + Pass: Test123
* Client
  + Username: root
  + Pass: Test123
* Attacker
  + Username: root
  + Pass: toor

1. **Identify and eliminate a rogue DHCP server**

A rogue DHCP server may issue IP addresses incorrectly in the network and equivalate with a Denial-of-Service attack – clients cannot get correct IP addresses and will end up unable to access the Internet.

The environment consists of two switches (SW1, SW2) and 4 machines – legitimate DHCP server (LinuxRouter), rogue DHCP server, client (Client), web server (WebServer). To begin with, all the machines should be off. If any machine is still on, right-click on the icon and then click **Stop**

**Task 1: connect the rogue DHCP server**

Click on the orange plug on the DHCP server and connect it to the plug on the switch SW2; in the pop-up window, accept the suggested values.

A computer tower with an orange plug

Description automatically generated A screenshot of a computer

Description automatically generated

Start the devices as follows:

* Start RogueDHCP
* Start SW2
* Start SW1
* Start Client
* Start LinuxRouter

On the Client machine:

* Login (user/Test123) and start a terminal window (Activities/terminal)
* Check current network assignment
  + Correct values: 10.0.0.100-10.0.0.200
  + Incorrect values: 10.20.30.100-10.20.30.200

The Client will receives an incorrect IP address from the rogue DHCP server and cannot connect to the Internet

Blocking the rogue DHCP server from allocating IP addresses

On the SW2:

* Type the following commands:

Switch> **en**

Switch# **configure terminal**

Switch(config)# **ip dhcp snooping**

Switch(config)# **interface Ethernet 0/2**

Switch(config)# **ip dhcp snooping trust**

Switch(config)# **no shutdown**

Switch(config)# **end**

The SW2 switch now allows DHCP allocation of addresses only from port E0/2; any offers from other ports are ignored, hence the RogueDHCP server is blocked

On the Client machine

* Restart the machine
* Verify that the client gets a 10.0.0.0/24 IP address

Delete the connection between the RogueDHCP server and the switch

1. DHCP starvation attack

DHCP starvation attacks take place when an Attacker exhausts all the IP addresses from a DHCP server by spoofing multiple MAC addresses. Legitimate clients are then unable to obtain IP addresses and cannot connect to the Internet.

Stop the Client machine

Start the Attacker machine

A typical DHCP starvation attack is mounted using yersinia, see the description below:

Yersinia – *do not use with the eve-ng as it is rather aggressive and it crashes the switch*.

On the Attacker machine, login and then click on Activities and type yersinia

In the pop-up terminal window, type yersinia -G

In the Yersinia window, click on **Launch attack**, then **DHCP**, and select **sending DISCOVER packet**.

A screenshot of a computer

Description automatically generated

This floods the DHCP server with requests, which will not be able to fulfil any more legitimate requests.

To check whether the switch crashed, go to the switch window and type:

Switch# **show run**

The command should list the current switch configuration. If the command does not have any output (it returns only the Switch# prompt), the switch crashed. You can restart it by going to the topology and right clicking **Stop**, **Wipe**, **Start**.

Instead of yersinia, we can run a “manual” starvation attack using linux commands. See the script below.

Type the following command in terminal: **nano starvation.sh** . A nano editor window should open. Enter the following script

**!#/bin/bash**

**while true**

**do**

**killall -9 dhclient**

**rm /var/lib/dhcp/dhcp.leases**

**macchanger -s ens3**

**dhclient -v**

**sleep 1**

**done**

type **Ctrl+x** and then **Ctrl+o** to save and exit the editor, then **chmod a+x ./starvation.sh** to make the script executable, and then run the script

**sudo ./starvation.sh**

You should see the script securing IP addresses (and hence depleting the pool of the DHCP server).

Start the Client machine, login, and open a terminal window (Activities/terminal) and type **ifconfig**

You will notice that the host has no IP address and there should be an error pop-up.

Mitigation – enable port security on the switch

Open Switch SW2. Type the following commands:

Switch> **enable**

Switch# **configure terminal**

Switch(conf)# **interface range ethernet 0/0-3**

Switch (config-if)# **switchport mode access**

Switch (config-if)# **switchport port-security**

Switch (config-if)# **end**

The client should be able to obtain an IP address in the following 30-60s. (might require restarting the Client machine)

To force the Client to renew its IP address and not use the previous leased IP, run the following commands in a terminal window:

**sudo dhclient -r**

**sudo rm /var/lib/dhcp/dhcp.leases**

**sudo dhclient**

After issuing the above commands, check the IP allocation using **ifconfig** .

1. Web server attack

An attacker can mount a denial of service attack against a server by opening a large number of connections.

Firstly, testing normal conditions:

On the client machine, open a Firefox browser and enter: <http://10.0.0.10>

It should load the Apache server test page on the Web server.

Mount the attack:

On the Attacker machine, open a terminal window and type the following command:

**slowloris.py -s 1000 10.0.0.10**

This will open 1000 concurrent connections which will render the web server unusable

Testing attack:

On the client machine, open a Firefox browser and enter: <http://10.0.0.10>

The browser will be unable to open the Apache server test page.

Mitigation – protect the web server against attacks.

Open the web server machine (click on the WebServer icon)

At the command prompt, login using the credentials root/Test123

Enter the following command:

**iptables -A INPUT -p tcp --syn --dport 80 -m connlimit --connlimit-above 15 --connlimit-mask 32 -j REJECT --reject-with tcp-reset**

On the Client machine, open a Firefox browser and enter: <http://10.0.0.10>

It should load the Apache server test page on the Web server.