**Student Name:** Coleton Sanheim **Weight: \_\_\_2.5\_\_\_\_\_%**

**Student ID:** 000862545 **Marks: \_\_\_\_/11\_\_\_\_**

Lab 4: Network Access Control

# Learning Outcomes

* Configure and implement an inline NAC solution (PacketFence).
* Configure web authentication for guest access.
* Test guest zone quarantine access.
* Test authenticated guest access.
* Attack guest zone access.

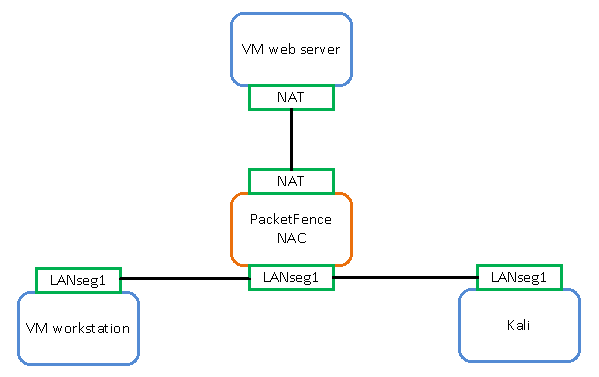
# Purpose

In this lab, you will look at network access control with inline deployment using PacketFence. This type of deployment is useful to provide guest network access, where guest hosts are held in a guest zone until user authentication is completed.

# Tools

* VM PacketFence Server (OVA)
* VM Win 7/10 Workstation
* Kali
* VM Web Server

# Topology



# Activities

## Scan the quarantine environment

1. Using Kali, enter the following command to discover the quarantine subnet:

# netdiscover -i eth0 -r 192.168.3.0/24

1. Demonstrate in Wireshark on the VM workstation that Kali netdiscover is scanning the subnet.

|  |
| --- |
| Insert evidence here |

Question: What protocol is netdiscover using to discover the subnet?

**ARP**

1. Using Kali, open a terminal and enter the following command:

# nmap -A -T5 <VM workstation IP>

1. Demonstrate the result of the Nmap scan on the host.

|  |
| --- |
| Insert evidence here |

1. Demonstrate in Wireshark on the VM workstation that Nmap is scanning the host.

|  |
| --- |
| Insert evidence here |

## Authenticate the VM workstation

1. On the VM workstation, open a web browser to http://<VM\_web\_server>.

Your web request will be directed to the NAC captive portal.

1. Log in to the captive portal with the username: demouser and the password: demouser.
2. Demonstrate that your VM workstation accesses the VM web server default webpage.

|  |
| --- |
| Insert evidence here |

## Rescan the VM workstation

1. Using Kali, open a terminal and enter the following command:

# nmap -A -T5 <VM workstation IP>

1. Demonstrate the result of the Nmap scan on the host.

|  |
| --- |
| Insert evidence here |

1. Demonstrate in Wireshark on the VM workstation that Nmap is scanning the host.

|  |
| --- |
| Insert evidence here |

Note: Even when the VM workstation has authenticated against the NAC, it is still susceptible to scanning from other hosts in the same subnet.

## Analyze the quarantine setting

1. Using Kali, perform a traceroute to 8.8.8.8.

Question: Can you reach 8.8.8.8? Why or why not?

**No, it seems to get stopped by the NAC device**

1. Examine the routing table using the following command:

# ip route

Question: is there a default route?

**Yes, default via 192.168.3.1 dev eth0 proto dhcp metric 100**

1. Manually add a default route in Kali using the following command:

# ip route add 0.0.0.0/0 via 192.168.3.1

1. Examine the routing table again.

Question: What has been added to the routing table?

**default via 192.168.3.1 dev eth0**

1. Perform a traceroute to 8.8.8.8.

Question: What is the reachable last hop?

**2 10.0.2.1 (10.0.2.1) 0.303 ms 0.294 ms 0.284 ms**

1. Observe that the NAC quarantine zone does not allow a host to go beyond the NAC device, even with the proper gateway. The NAC device effectively becomes the firewall for the quarantine zone.