Activity File: Testing Firewall Rules with Nmap

In this activity, you continue in the role of SOC analyst for Better Buys, Inc.

- Better Buys has over 400 physical stores as well as a large online presence, which generates 60% of all sales.

- PCI DSS requires organizations to collect and store payment card information, and conduct vulnerability scans and penetration tests.

- To stay compliant while ensuring a strong security posture, you've been tasked with conducting scans against your network to uncover potential vulnerabilities in your firewall or IDS (intrusion detection system).

- You've decided to perform various network scans to test the integrity of your firewalls using Nmap, identify weaknesses, and use that information to help harden your network.

Use `nmap` to perform network scans.

Use `nmap -sO` to perform an IP protocol scan.

Use `nmap -sV` to enumerate service type.

Use `nmap -A -T4` to perform OS fingerprinting using fast execution.

Use `uname -a` to print the OS type and version.

Use `nmap -sA` to enumerate the type of firewall in use.

Instructions

Before you begin, log into your UFW VM and firewalld VM.

- Log into the firewalld VM using the following credentials:
    - Username: `sysadmin`
    - Password: `cybersecurity`
- firewalld will serve as your attack machine for this activity.

- Log into the UFW VM using the following credentials:
    - Username: `sysadmin`

    - Password: `cybersecurity`
- UFW will serve as the victim.

1. Set up your test environment as follows:

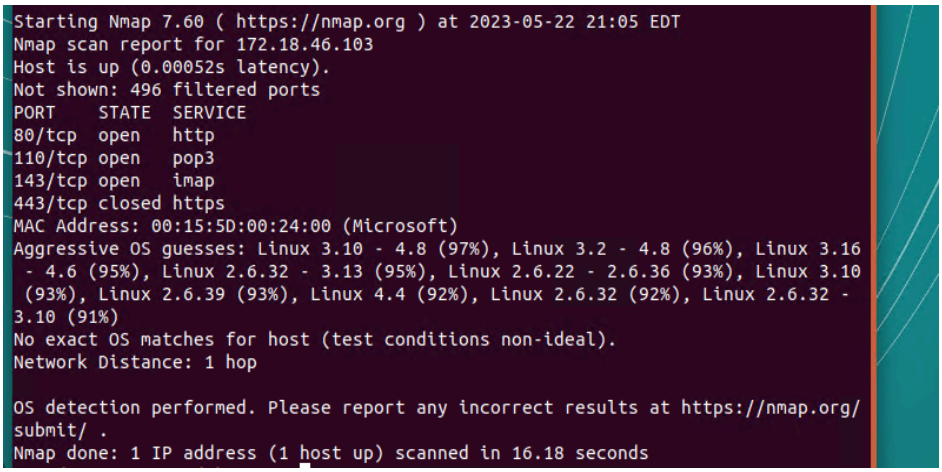
    - Type the following commands in your UFW VM:

        - `sudo ufw reset`
        - `sudo ufw enable`
        - `sudo ufw default deny incoming`
        - `sudo ufw default deny outgoing`
        - `sudo ufw allow 80`
        - `sudo ufw allow 22`
        - `sudo ufw allow 443`

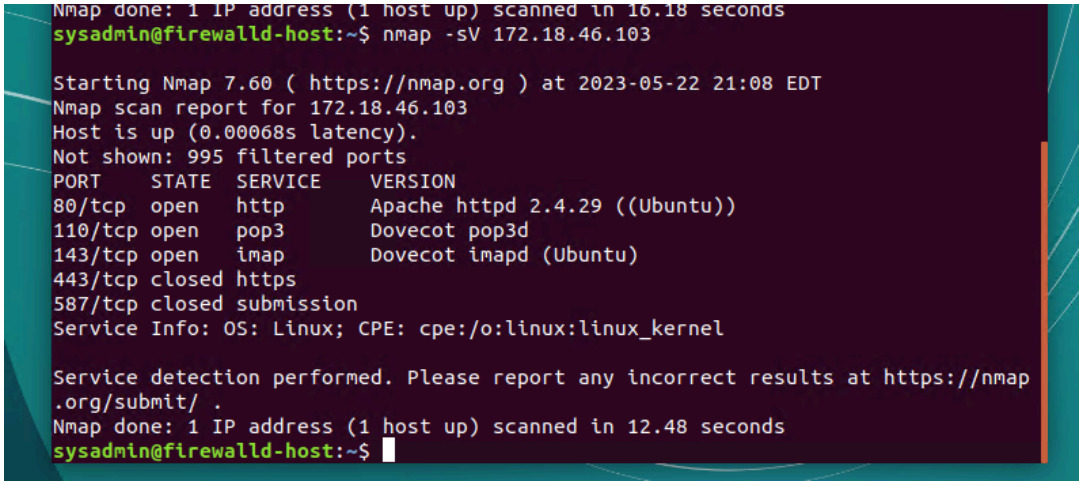
2. From your firewalld VM, perform a basic Nmap scan against the UFW machine to help you determine whether or not the system is up.

    sudo nmap -O -p 1-500 --osscan-guess 172.18.46.103

    - Which ports are open and what are their associated protocols and service types?

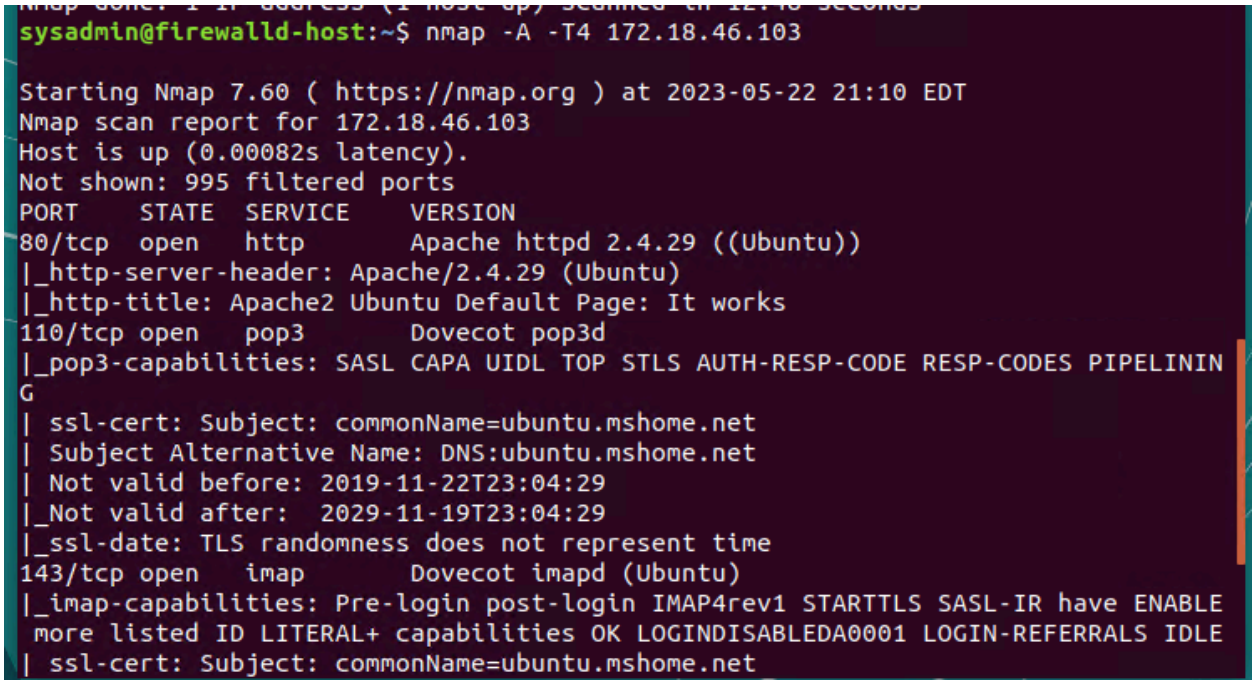


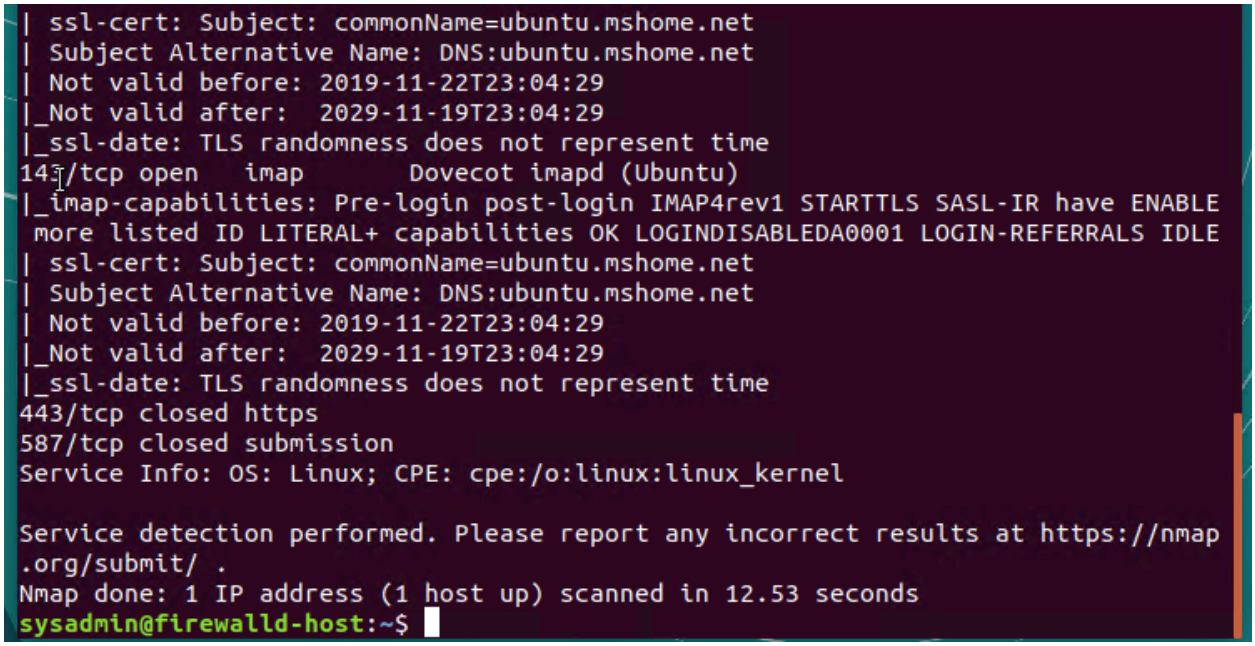
3. Run the command that returns results that include service and daemon type.



   - What versions are returned in the results if any?
   - Why was Nmap able to enumerate these services?

4. With the UFW firewall still enabled, type the command that performs OS detection and service detection using fast execution.

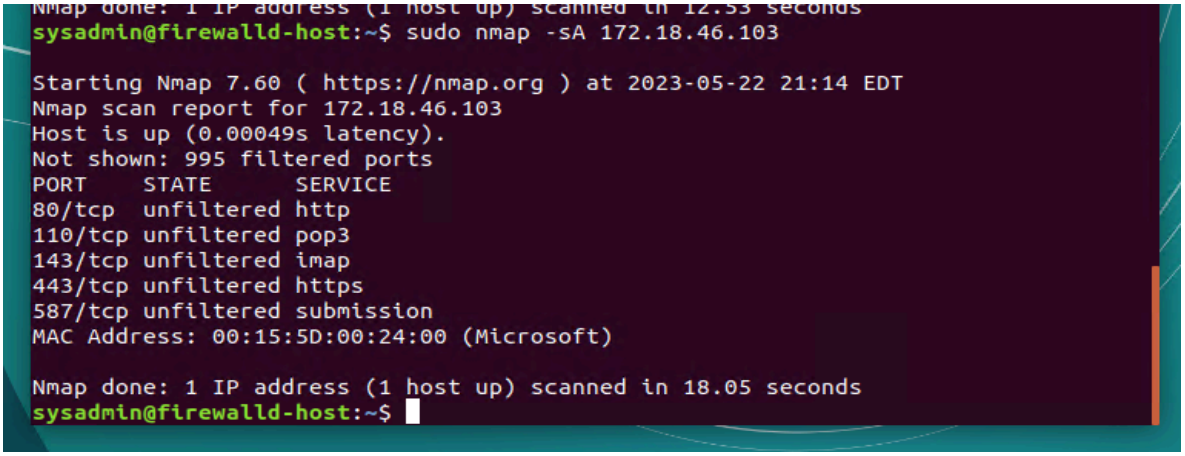




    - Was this nmap scan able to determine what company the MAC address belongs to?
    - Was this nmap scan able to return an exact match for the OS on the host?

- On the victim machine, run `uname -a` and observe the results.
- Does the currently installed version of Linux match any of the version within the "Aggressive OS guesses" section of the nmap scan?

6. Run the Nmap command that will determine whether or not a firewall is stateful.
    - What are the port states?
    - What type of firewall is being used and at which layer of the OSI model does it operate?



Bonus

- What is a SYN scan and what is its primary benefit, from a hacking perspective?
- What are the three possible responses of a SYN scan and what do they mean?