

# 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 -s0` 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 firewall VM.

- Log into the firewall 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 firewall 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?

```
Starting Nmap 7.60 ( https://nmap.org ) at 2023-05-22 21:05 EDT
Nmap scan report for 172.18.46.103
Host is up (0.00052s latency).
Not shown: 496 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   closed https
MAC Address: 00:15:5D:00:24:00 (Microsoft)
Aggressive OS guesses: Linux 3.10 - 4.8 (97%), Linux 3.2 - 4.8 (96%), Linux 3.16
- 4.6 (95%), Linux 2.6.32 - 3.13 (95%), Linux 2.6.22 - 2.6.36 (93%), Linux 3.10
(93%), Linux 2.6.39 (93%), Linux 4.4 (92%), Linux 2.6.32 (92%), Linux 2.6.32 -
3.10 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.18 seconds
```

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

```
Nmap done: 1 IP address (1 host up) scanned in 16.18 seconds
sysadmin@firewalld-host:~$ nmap -sV 172.18.46.103

Starting Nmap 7.60 ( https://nmap.org ) at 2023-05-22 21:08 EDT
Nmap scan report for 172.18.46.103
Host is up (0.00068s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))
110/tcp   open  pop3         Dovecot pop3d
143/tcp   open  imap         Dovecot imapd (Ubuntu)
443/tcp   closed https
587/tcp   closed submission
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.48 seconds
sysadmin@firewalld-host:~$
```

- 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.

```
Nmap done: 1 IP address (1 host up) scanned in 12.10 seconds
sysadmin@firewalld-host:~$ nmap -A -T4 172.18.46.103

Starting Nmap 7.60 ( https://nmap.org ) at 2023-05-22 21:10 EDT
Nmap scan report for 172.18.46.103
Host is up (0.00082s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
110/tcp   open  pop3         Dovecot pop3d
|_pop3-capabilities: SASL CAPA UIDL TOP STLS AUTH-RESP-CODE RESP-CODES PIPELININ
G
|_ssl-cert: Subject: commonName=ubuntu.mshome.net
| Subject Alternative Name: DNS:ubuntu.mshome.net
| Not valid before: 2019-11-22T23:04:29
|_Not valid after: 2029-11-19T23:04:29
|_ssl-date: TLS randomness does not represent time
143/tcp   open  imap         Dovecot imapd (Ubuntu)
|_imap-capabilities: Pre-login post-login IMAP4rev1 STARTTLS SASL-IR have ENABLE
more listed ID LITERAL+ capabilities OK LOGINDISABLEDA0001 LOGIN-REFERRALS IDLE
|_ssl-cert: Subject: commonName=ubuntu.mshome.net
```

```

| ssl-cert: Subject: commonName=ubuntu.mshome.net
| Subject Alternative Name: DNS:ubuntu.mshome.net
| Not valid before: 2019-11-22T23:04:29
|_Not valid after: 2029-11-19T23:04:29
|_ssl-date: TLS randomness does not represent time
143/tcp open  imap      Dovecot imapd (Ubuntu)
|_imap-capabilities: Pre-login post-login IMAP4rev1 STARTTLS SASL-IR have ENABLE
more listed ID LITERAL+ capabilities OK LOGINDISABLEDA0001 LOGIN-REFERRALS IDLE
| ssl-cert: Subject: commonName=ubuntu.mshome.net
| Subject Alternative Name: DNS:ubuntu.mshome.net
| Not valid before: 2019-11-22T23:04:29
|_Not valid after: 2029-11-19T23:04:29
|_ssl-date: TLS randomness does not represent time
443/tcp closed https
587/tcp closed submission
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.53 seconds
sysadmin@firewalld-host:~$

```

- 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?

```
Nmap done: 1 IP address (1 host up) scanned in 12.53 seconds
sysadmin@firewalld-host:~$ sudo nmap -sA 172.18.46.103

Starting Nmap 7.60 ( https://nmap.org ) at 2023-05-22 21:14 EDT
Nmap scan report for 172.18.46.103
Host is up (0.00049s latency).
Not shown: 995 filtered ports
PORT      STATE      SERVICE
80/tcp    unfiltered http
110/tcp   unfiltered pop3
143/tcp   unfiltered imap
443/tcp   unfiltered https
587/tcp   unfiltered submission
MAC Address: 00:15:5D:00:24:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 18.05 seconds
sysadmin@firewalld-host:~$
```

### 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?