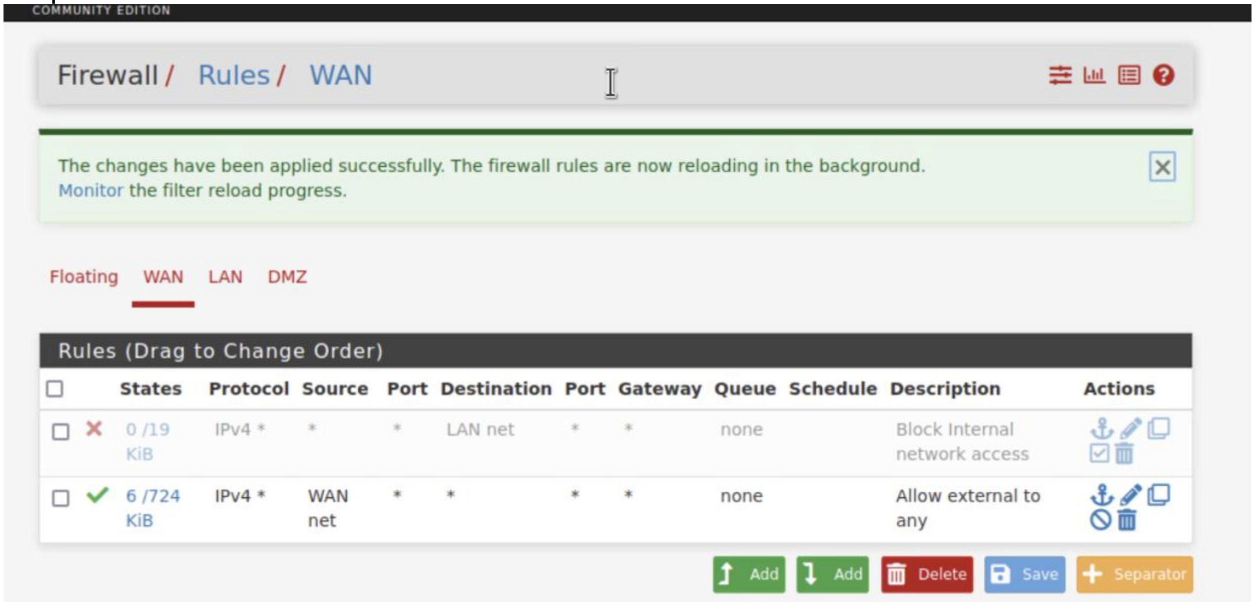
Peter Sanford
IT 2700
NetLab Lab 8
11/04/2023

1.1:
Step 6:



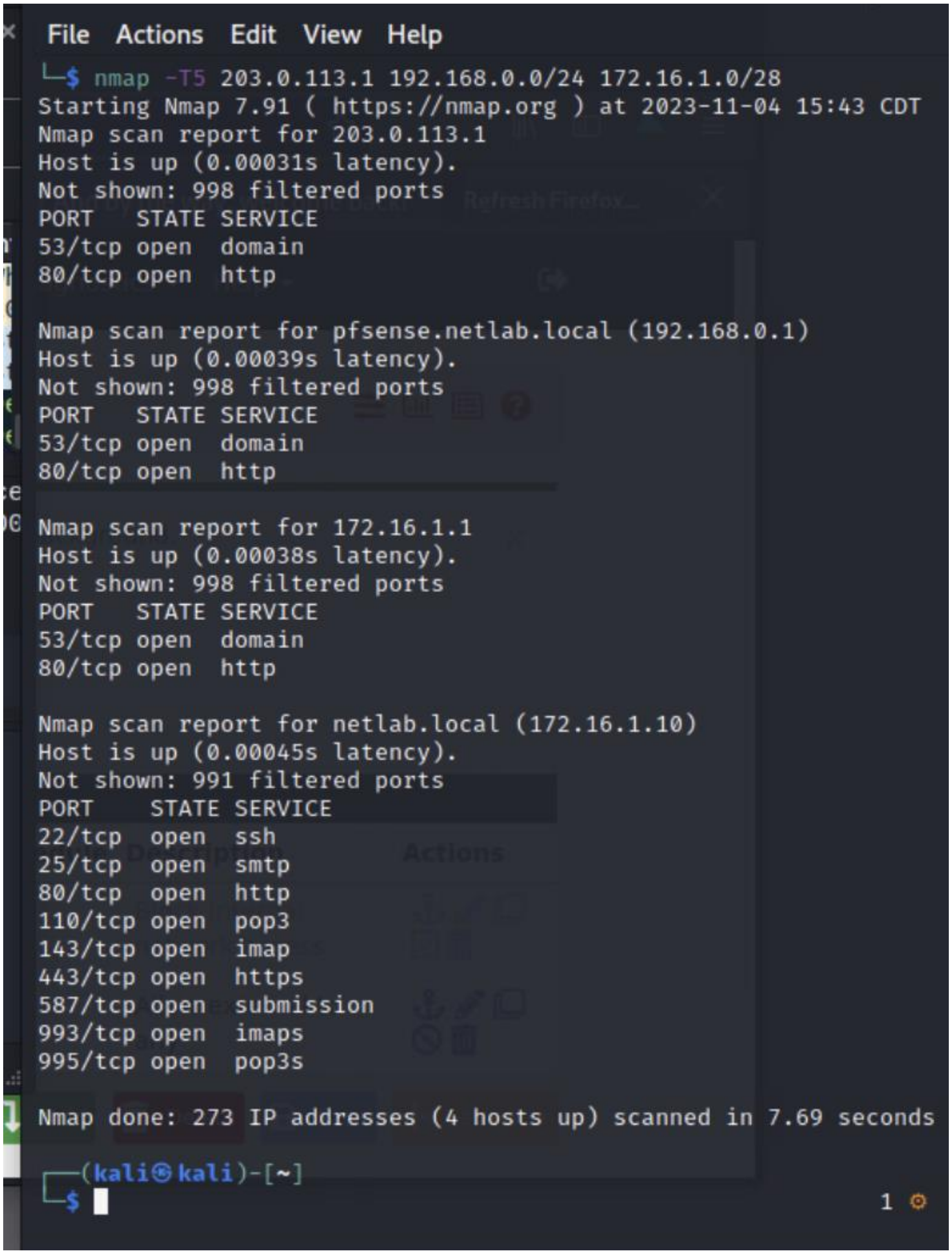
Firewall / Rules / WAN

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Rules (Drag to Change Order)

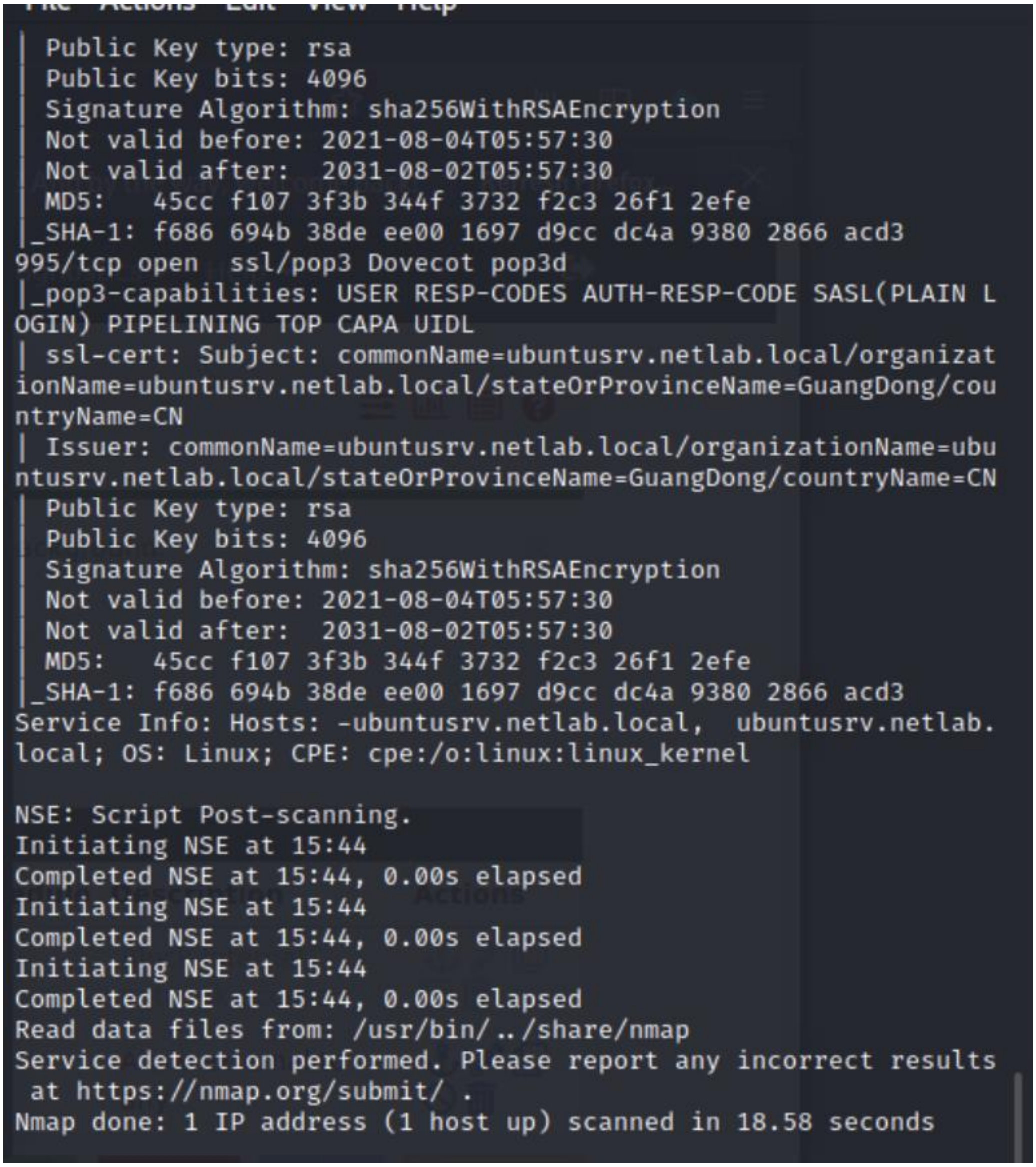
☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✗	0 /19 KiB	IPv4 *	*	*	LAN net	*	*	none		Block Internal network access	
☐	✓	6 /724 KiB	IPv4 *	WAN net	*	*	*	*	none		Allow external to any	

1.2:
Step 6:



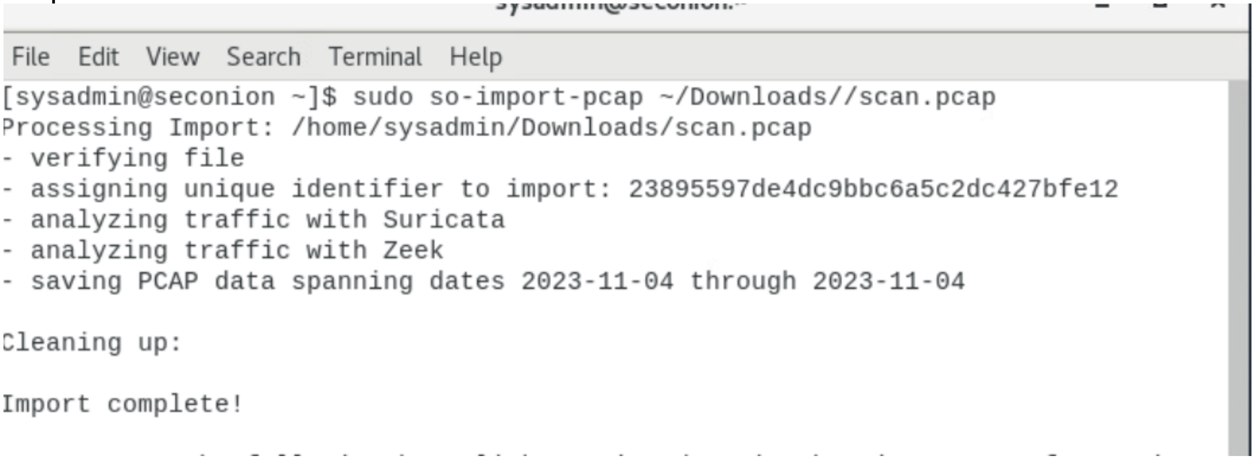
```
└─$ nmap -T5 203.0.113.1 192.168.0.0/24 172.16.1.0/28
Starting Nmap 7.91 ( https://nmap.org ) at 2023-11-04 15:43 CDT
Nmap scan report for 203.0.113.1
Host is up (0.00031s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for pfsense.netlab.local (192.168.0.1)
Host is up (0.00039s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for 172.16.1.1
Host is up (0.00038s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap scan report for netlab.local (172.16.1.10)
Host is up (0.00045s latency).
Not shown: 991 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
443/tcp open  https
587/tcp open  submission
993/tcp open  imaps
995/tcp open  pop3s

Nmap done: 273 IP addresses (4 hosts up) scanned in 7.69 seconds

┌──(kali㉿kali)-[~]
└─$ █                                                        1 ⚙
```

Step 8:



```
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-08-04T05:57:30
| Not valid after:  2031-08-02T05:57:30
| MD5:   45cc f107 3f3b 344f 3732 f2c3 26f1 2efe
|_SHA-1: f686 694b 38de ee00 1697 d9cc dc4a 9380 2866 acd3
995/tcp open  ssl/pop3 Dovecot pop3d
|_pop3-capabilities: USER RESP-CODES AUTH-RESP-CODE SASL(PLAIN L
OGIN) PIPELINING TOP CAPA UIDL
| ssl-cert: Subject: commonName=ubuntusrv.netlab.local/organizat
ionName=ubuntusrv.netlab.local/stateOrProvinceName=GuangDong/cou
ntryName=CN
| Issuer: commonName=ubuntusrv.netlab.local/organizationName=ubu
ntusrv.netlab.local/stateOrProvinceName=GuangDong/countryName=CN
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-08-04T05:57:30
| Not valid after:  2031-08-02T05:57:30
| MD5:   45cc f107 3f3b 344f 3732 f2c3 26f1 2efe
|_SHA-1: f686 694b 38de ee00 1697 d9cc dc4a 9380 2866 acd3
Service Info: Hosts: -ubuntusrv.netlab.local,  ubuntusrv.netlab.
local; OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 15:44
Completed NSE at 15:44, 0.00s elapsed
Initiating NSE at 15:44
Completed NSE at 15:44, 0.00s elapsed
Initiating NSE at 15:44
Completed NSE at 15:44, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results
 at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.58 seconds
```

1.3:
Step 11:



```
[sysadmin@seconion ~]$ sudo so-import-pcap ~/Downloads//scan.pcap
Processing Import: /home/sysadmin/Downloads/scan.pcap
- verifying file
- assigning unique identifier to import: 23895597de4dc9bbc6a5c2dc427bfe12
- analyzing traffic with Suricata
- analyzing traffic with Zeek
- saving PCAP data spanning dates 2023-11-04 through 2023-11-04

Cleaning up:

Import complete!
```

2:
Step 8:
This is where I got stuck, the PCAP wouldn’t import correctly into SO and wouldn’t show up in the web interface.

3.1:
Step 5:

Step 9:

Step 13:

3.2:
Step 8:

Step 13:

3.3:
Step 3:

Step 7:

Commentary:

In this lab we used Wireshark to capture packets and then analyze them as IDS alerts. I learned that nmap is super powerful and packet captures can be super useful in finding threat alerts. Knowing this information, companies can use nmap and packet captures to maintain security from the outside of the network and also analyze potential threats in the network.