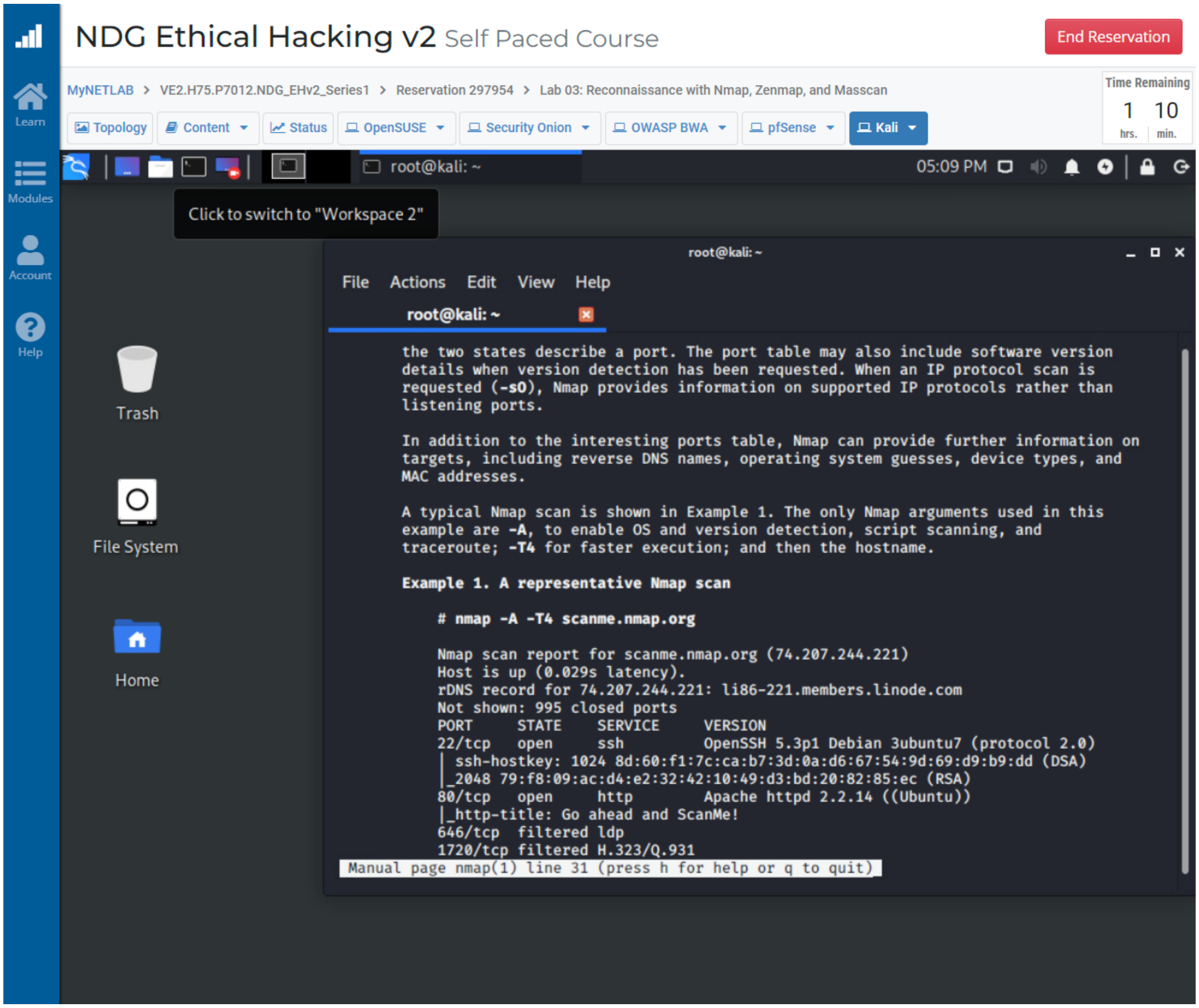
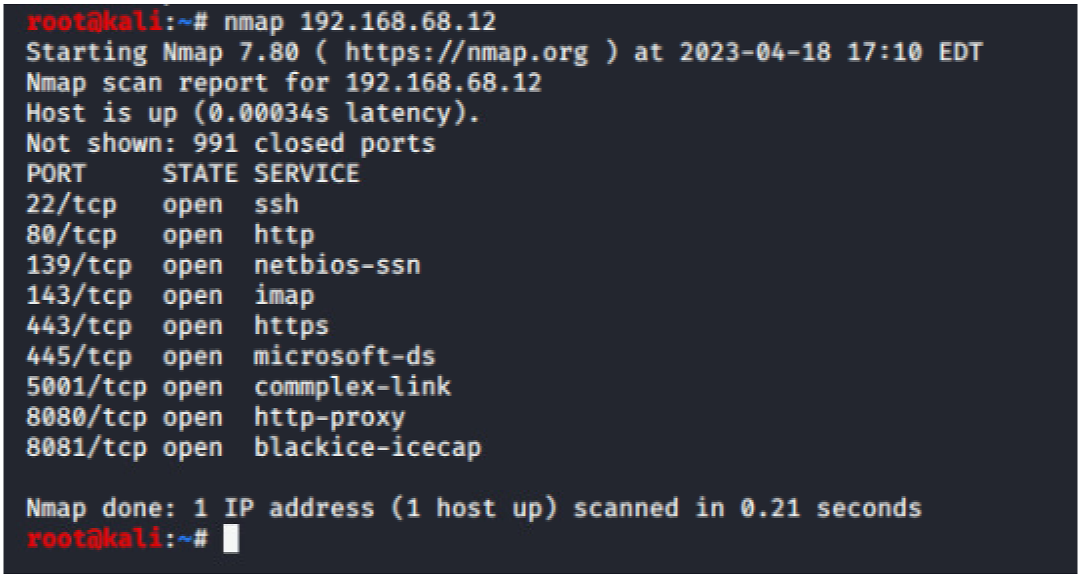
Jason Palmeri
CS53C
Lab 03
Timothy Ryan

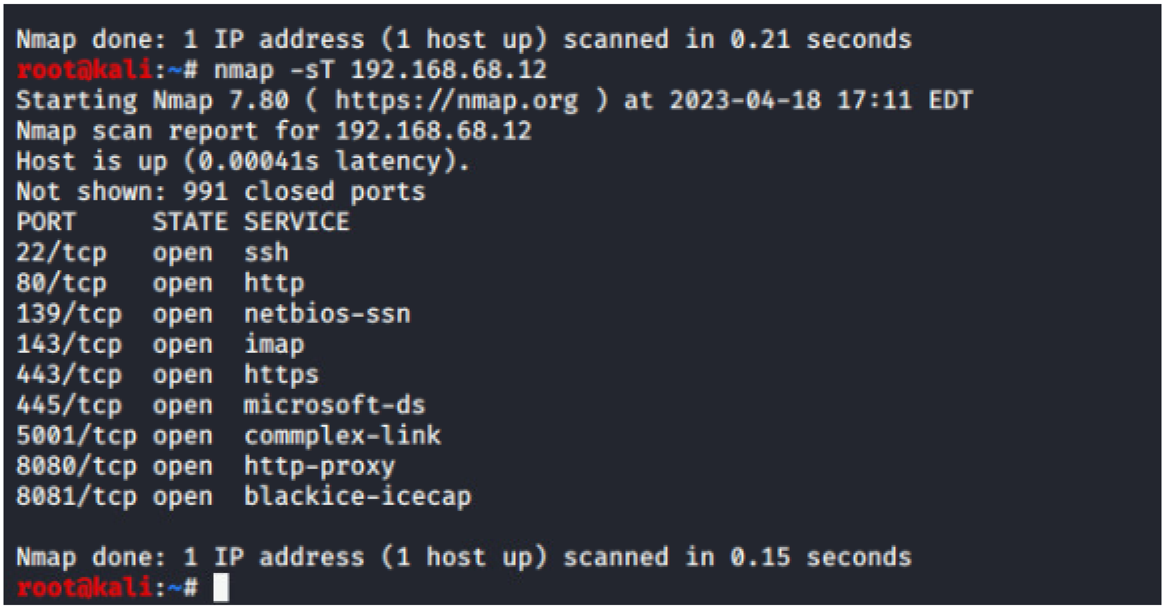
Reconnaissance With Nmap



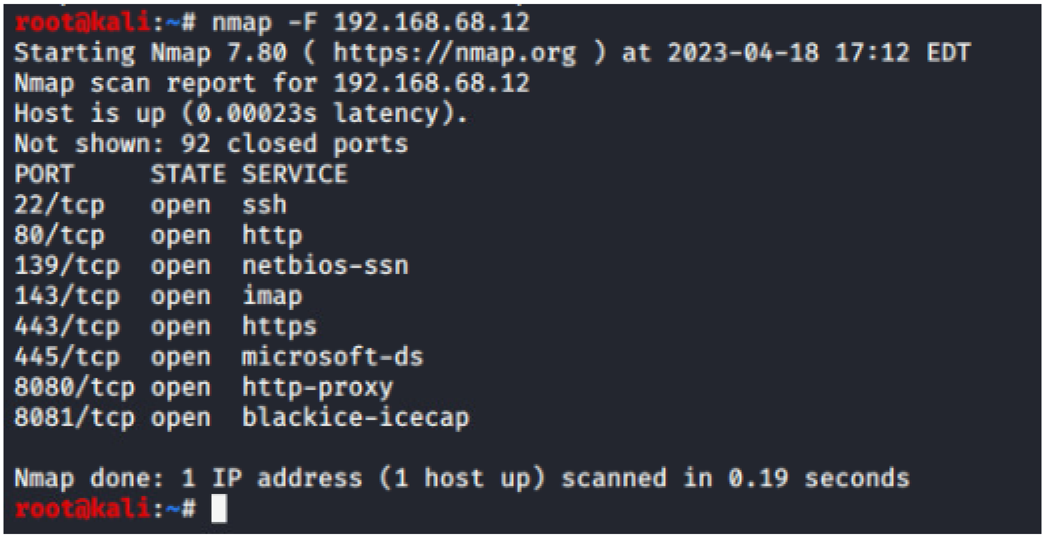
```
       the two states describe a port. The port table may also include software version
       details when version detection has been requested. When an IP protocol scan is
       requested (-sO), Nmap provides information on supported IP protocols rather than
       listening ports.

       In addition to the interesting ports table, Nmap can provide further information on
       targets, including reverse DNS names, operating system guesses, device types, and
       MAC addresses.

       A typical Nmap scan is shown in Example 1. The only Nmap arguments used in this
       example are -A, to enable OS and version detection, script scanning, and
       traceroute; -T4 for faster execution; and then the hostname.

       Example 1. A representative Nmap scan

           # nmap -A -T4 scanme.nmap.org

           Nmap scan report for scanme.nmap.org (74.207.244.221)
           Host is up (0.029s latency).
           rDNS record for 74.207.244.221: li86-221.members.linode.com
           Not shown: 995 closed ports
           PORT     STATE    SERVICE     VERSION
           22/tcp   open     ssh         OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
           | ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
           |_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
           80/tcp   open     http        Apache httpd 2.2.14 ((Ubuntu))
           |_http-title: Go ahead and ScanMe!
           646/tcp  filtered ldp
           1720/tcp filtered H.323/Q.931
 Manual page nmap(1) line 31 (press h for help or q to quit)
```



```
root@kali:~# nmap 192.168.68.12
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-18 17:10 EDT
Nmap scan report for 192.168.68.12
Host is up (0.00034s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
root@kali:~# 
```

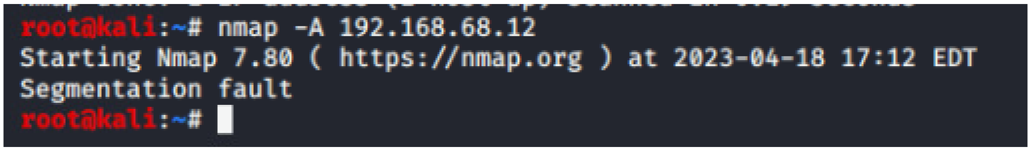


```
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
root@kali:~# nmap -sT 192.168.68.12
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-18 17:11 EDT
Nmap scan report for 192.168.68.12
Host is up (0.00041s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
root@kali:~# 
```



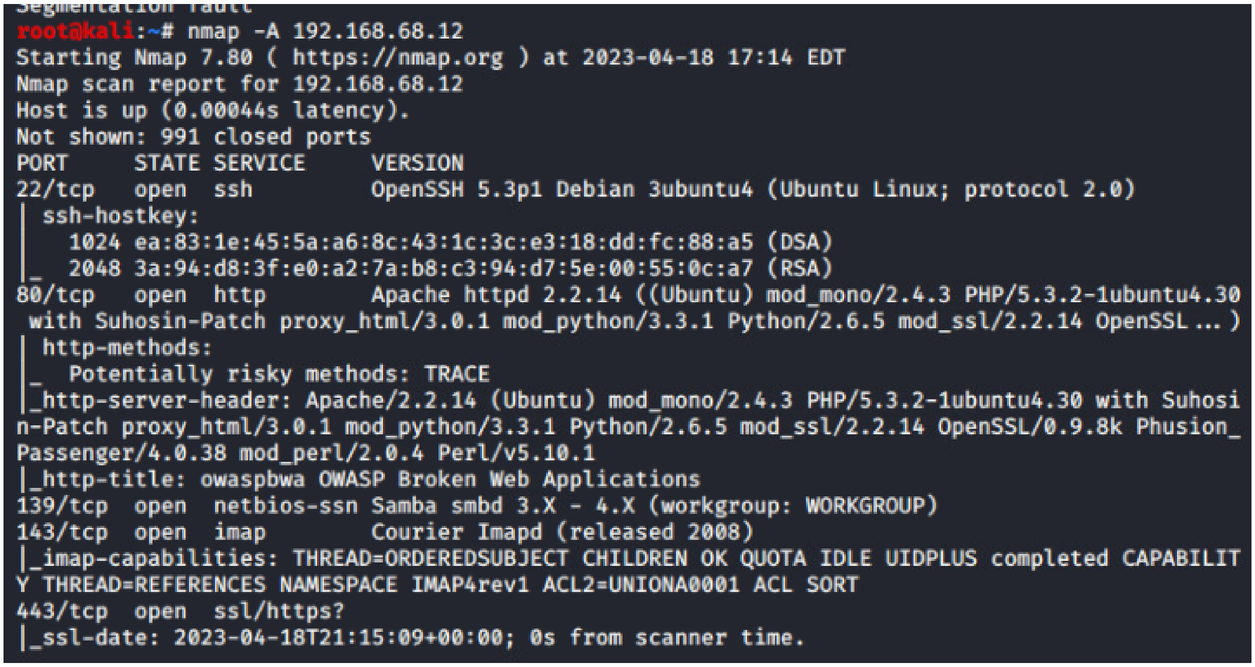
```
root@kali:~# nmap -F 192.168.68.12
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-18 17:12 EDT
Nmap scan report for 192.168.68.12
Host is up (0.00023s latency).
Not shown: 92 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
root@kali:~# 
```

For step 12 I got an error



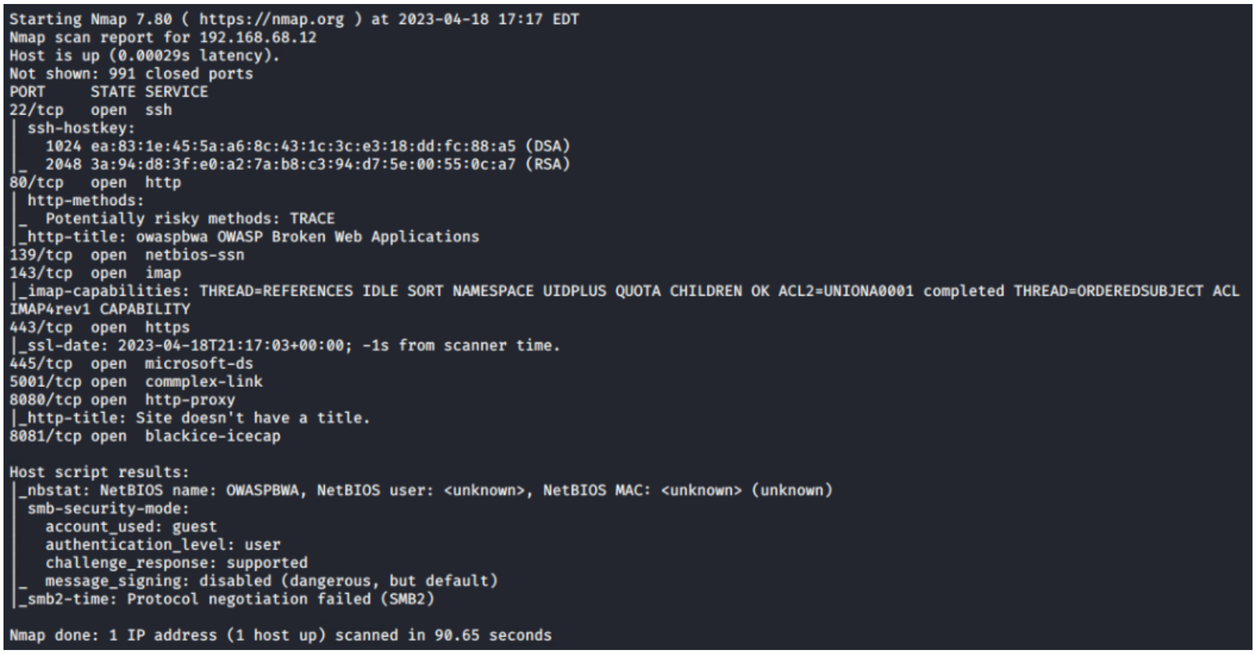
```
root@kali:~# nmap -A 192.168.68.12
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-18 17:12 EDT
Segmentation fault
root@kali:~# 
```

Running a second time gave me an output

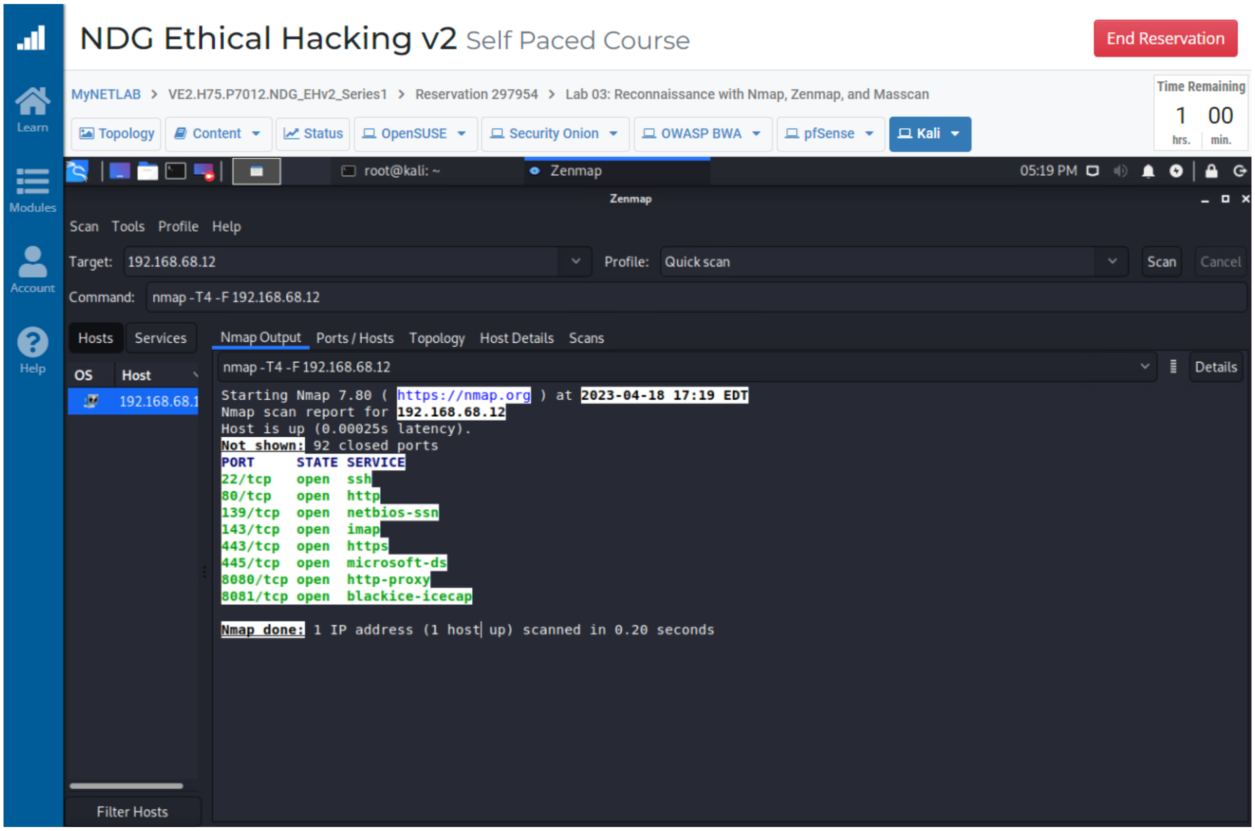


```
Segmentation fault
root@kali:~# nmap -A 192.168.68.12
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-18 17:14 EDT
Nmap scan report for 192.168.68.12
Host is up (0.00044s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ea:83:1e:45:5a:a6:8c:43:1c:3c:e3:18:dd:fc:88:a5 (DSA)
|_  2048 3a:94:d8:3f:e0:a2:7a:b8:c3:94:d7:5e:00:55:0c:a7 (RSA)
80/tcp   open  http        Apache httpd 2.2.14 ((Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30
 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL ... )
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosi
n-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_
Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
|_http-title: owaspbwa OWASP Broken Web Applications
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        Courier Imapd (released 2008)
|_imap-capabilities: THREAD=ORDEREDSUBJECT CHILDREN OK QUOTA IDLE UIDPLUS completed CAPABILIT
Y THREAD=REFERENCES NAMESPACE IMAP4rev1 ACL2=UNIONA0001 ACL SORT
443/tcp  open  ssl/https?
|_ssl-date: 2023-04-18T21:15:09+00:00; 0s from scanner time.
```

Nmap done: 1 IP address (1 host up) scanned in 106.61 seconds



```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-18 17:17 EDT
Nmap scan report for 192.168.68.12
Host is up (0.00029s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   1024 ea:83:1e:45:5a:a6:8c:43:1c:3c:e3:18:dd:fc:88:a5 (DSA)
|_  2048 3a:94:d8:3f:e0:a2:7a:b8:c3:94:d7:5e:00:55:0c:a7 (RSA)
80/tcp   open  http
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: owaspbwa OWASP Broken Web Applications
139/tcp  open  netbios-ssn
143/tcp  open  imap
|_imap-capabilities: THREAD=REFERENCES IDLE SORT NAMESPACE UIDPLUS QUOTA CHILDREN OK ACL2=UNIONA0001 completed THREAD=ORDEREDSUBJECT ACL
IMAP4rev1 CAPABILITY
443/tcp  open  https
|_ssl-date: 2023-04-18T21:17:03+00:00; -1s from scanner time.
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
|_http-title: Site doesn't have a title.
8081/tcp open  blackice-icecap

Host script results:
|_nbstat: NetBIOS name: OWASPBWA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Nmap done: 1 IP address (1 host up) scanned in 90.65 seconds
```



NDG Ethical Hacking v2 Self Paced Course

MyNETLAB > VE2.H75.P7012.NDG_EHv2_Series1 > Reservation 297954 > Lab 03: Reconnaissance with Nmap, Zenmap, and Masscan

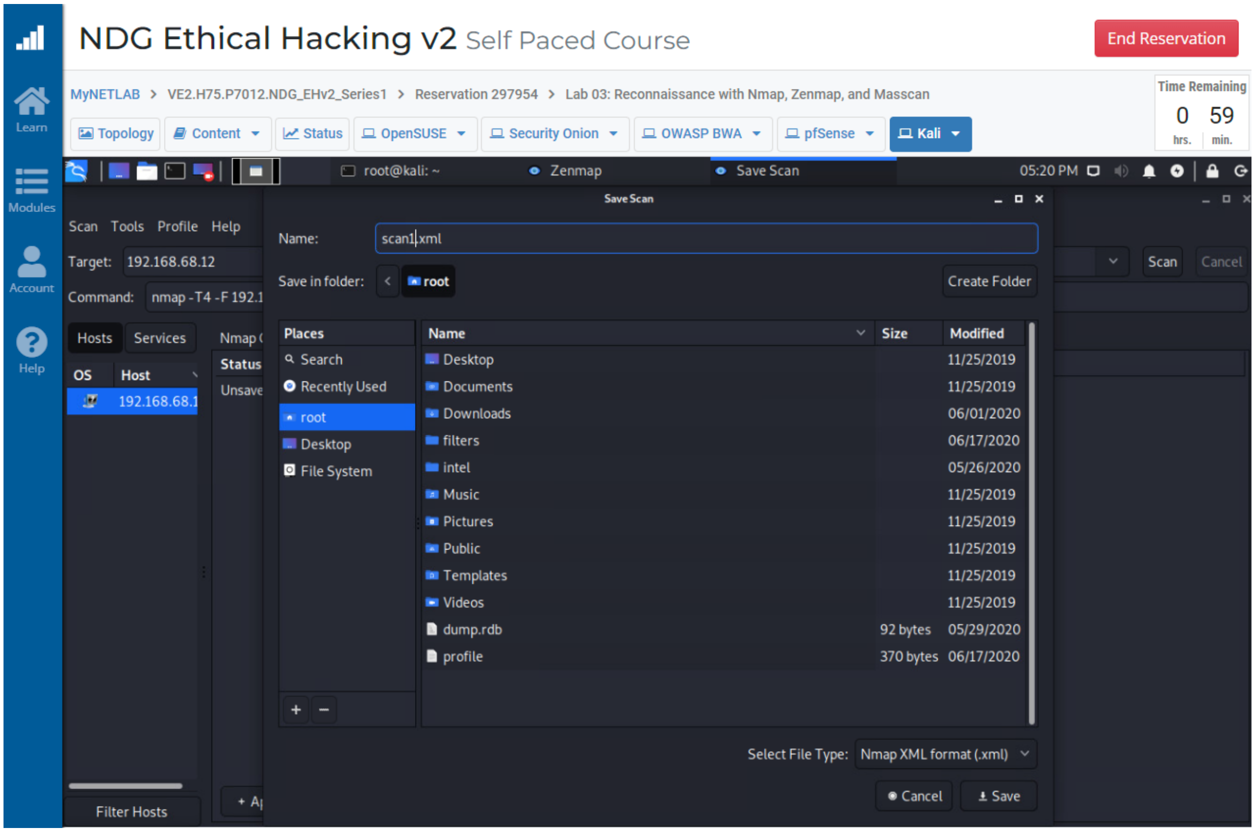
Time Remaining 1 hrs. 00 min.

Target: 192.168.68.12

Profile: Quick scan

Command: nmap -T4 -F 192.168.68.12

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-18 17:19 EDT
Nmap scan report for 192.168.68.12
Host is up (0.00025s latency).
Not shown: 92 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```



NDG Ethical Hacking v2 Self Paced Course
End Reservation
MyNETLAB > VE2.H75.P7012.NDG_EHv2_Series1 > Reservation 297954 > Lab 03: Reconnaissance with Nmap, Zenmap, and Masscan
Time Remaining 0 hrs. 59 min.
Topology Content Status OpenSUSE Security Onion OWASP BWA pfSense Kali
Learn Modules Account Help
root@kali: ~ Zenmap Save Scan 05:20 PM
Scan Tools Profile Help
Create Folder
Places Search Recently Used root Desktop File System
Cancel Save
Filter Hosts

Save Scan

Name: scan1.xml

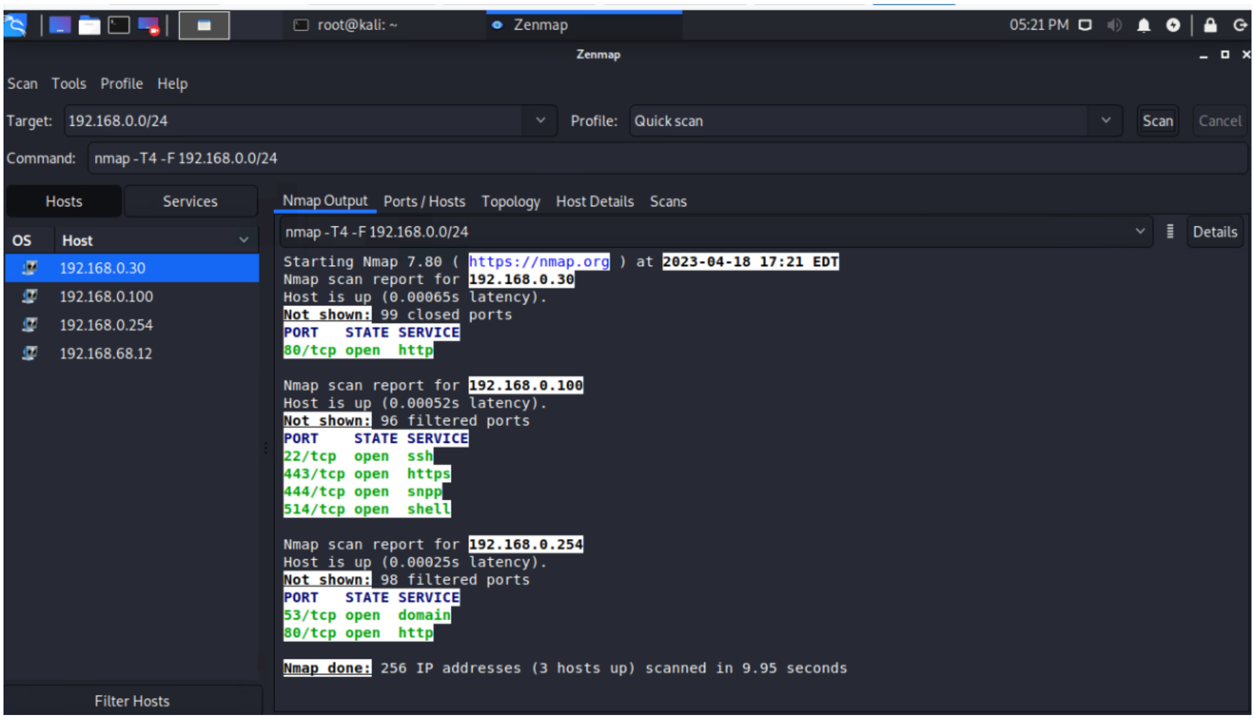
Save in folder: root

Target: 192.168.68.12

Command: nmap -T4 -F 192.1

Name	Size	Modified
Desktop		11/25/2019
Documents		11/25/2019
Downloads		06/01/2020
filters		06/17/2020
intel		05/26/2020
Music		11/25/2019
Pictures		11/25/2019
Public		11/25/2019
Templates		11/25/2019
Videos		11/25/2019
dump.rdb	92 bytes	05/29/2020
profile	370 bytes	06/17/2020

Select File Type: Nmap XML format (.xml)



root@kali: ~ Zenmap 05:21 PM
Zenmap
Scan Tools Profile Help
Scan Cancel
Hosts Services
OS Host
Nmap Output Ports / Hosts Topology Host Details Scans
Details
Filter Hosts

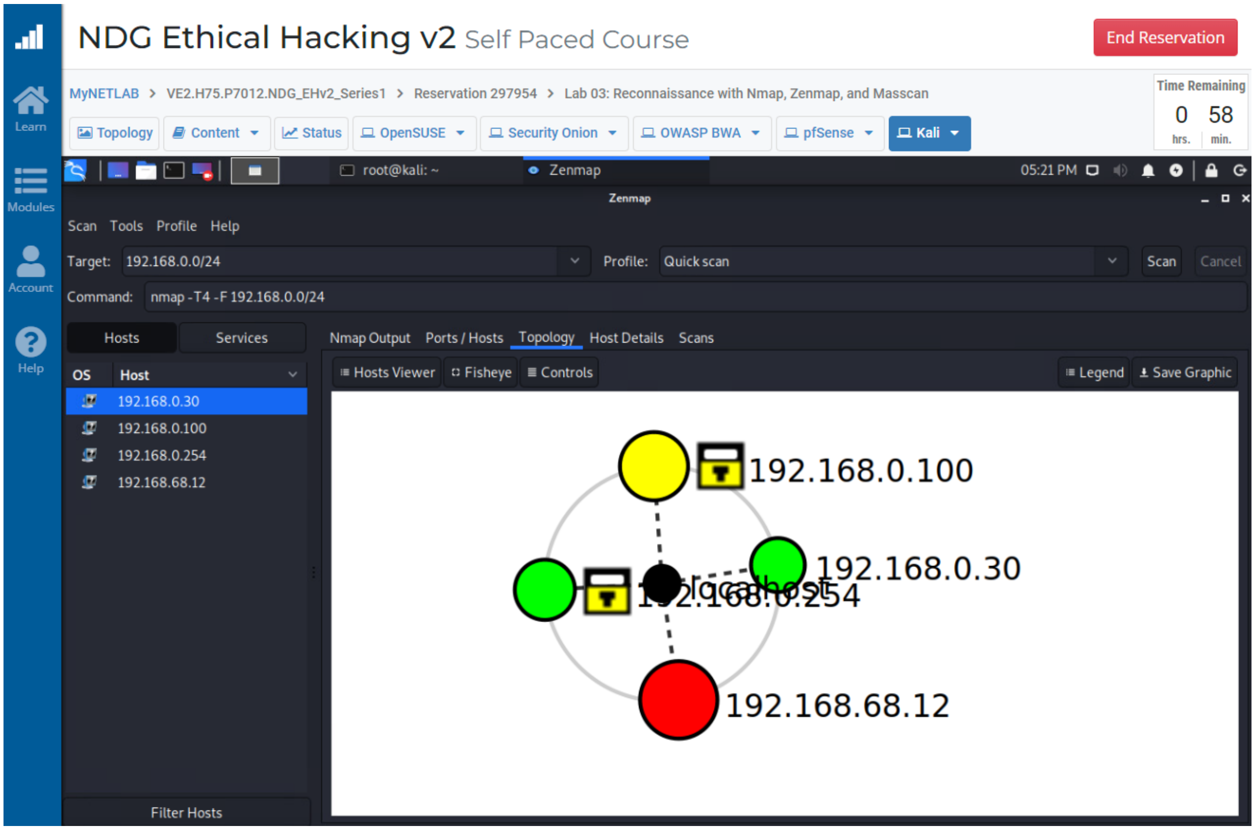
Target: 192.168.0.0/24

Profile: Quick scan

Command: nmap -T4 -F 192.168.0.0/24

Hosts:
- 192.168.0.30
- 192.168.0.100
- 192.168.0.254
- 192.168.68.12

```
nmap -T4 -F 192.168.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-18 17:21 EDT
Nmap scan report for 192.168.0.30
Host is up (0.00065s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for 192.168.0.100
Host is up (0.00052s latency).
Not shown: 96 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
443/tcp open  https
444/tcp open  snpp
514/tcp open  shell

Nmap scan report for 192.168.0.254
Host is up (0.00025s latency).
Not shown: 98 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http

Nmap done: 256 IP addresses (3 hosts up) scanned in 9.95 seconds
```

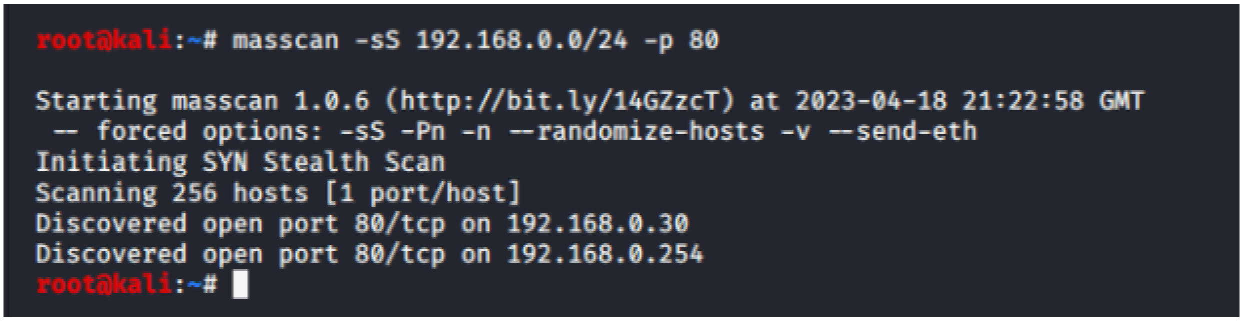


Target: 192.168.0.0/24

Profile: Quick scan

Command: nmap -T4 -F 192.168.0.0/24

192.168.0.30
192.168.0.100
192.168.0.254
192.168.68.12



```
root@kali:~# masscan -sS 192.168.0.0/24 -p 80

Starting masscan 1.0.6 (http://bit.ly/14GZzcT) at 2023-04-18 21:22:58 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [1 port/host]
Discovered open port 80/tcp on 192.168.0.30
Discovered open port 80/tcp on 192.168.0.254
root@kali:~# █
```

This lab was very interesting, and it was nice to see the comparison between a command line interface and graphic interface.