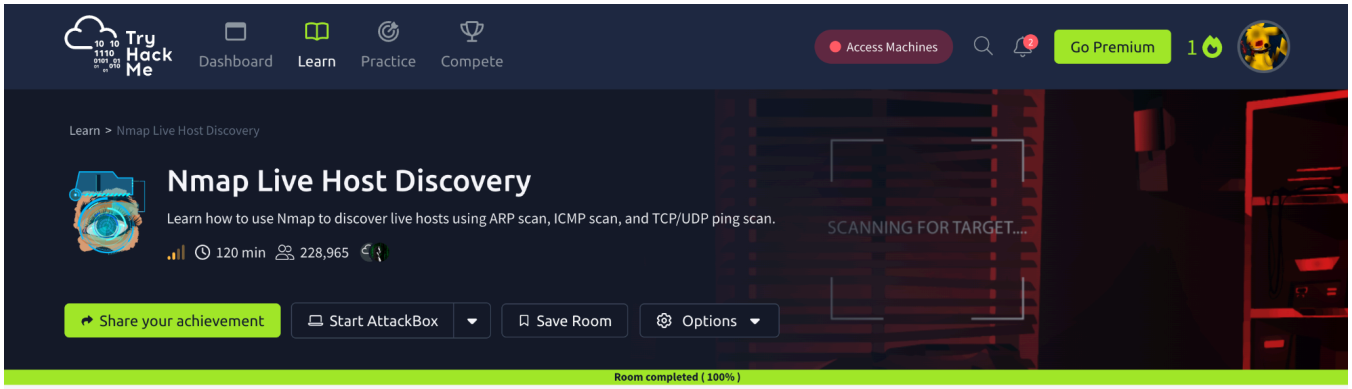
Learning more about nmap:

Prep for at home lab:
Before I started the at home lab on my VM, I gained more understanding about the use of nmap through a TryHackMeLab. The completion of the lab is shown below:



At home lab:

Identifying network interfaces and IP addresses:
The command I used to do this was: ifconfig

```
vansises@sv09:~$ ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.227.129  netmask 255.255.255.0  broadcast 192.168.227.255
        inet6 fe80::20c:29ff:fed9:4265  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d9:42:65  txqueuelen 1000  (Ethernet)
        RX packets 44  bytes 13033 (13.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 93  bytes 11967 (11.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 46  memory 0x3fe00000-3fe20000
```

The purpose of this command is to:

- View network interfaces and their corresponding IP addresses on my VM
- Helps better understand your network configuration

Checking the open ports on my VM:
The command I used to do this was: sudo netstat -tuln

```
vansises@sv09:~$ sudo netstat -tuln
[sudo] password for vansises:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 0.0.0.0:36777           0.0.0.0:*
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 192.168.227.129:68      0.0.0.0:*
udp6       0      0 :::5353                 :::*
udp6       0      0 :::42542                :::*
```

The purpose of this command is to:

- Lists open ports on my vm
- Helps identify open ports that can be closed to defend from attackers
- “-tuln” is used to restrict output to only TCP and UDP ports

Analyzing the network connections to my VM:
The command I used to do this was: sudo lsof -i -P -n

```
vansises@sv09:~$ sudo lsof -i -P -n
COMMAND    PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-n  974 systemd-network   18u  IPv4  22763      0t0  UDP 192.168.227.129:
68
systemd-r  996 systemd-resolve   13u  IPv4  21834      0t0  UDP 127.0.0.53:53
systemd-r  996 systemd-resolve   14u  IPv4  21835      0t0  TCP 127.0.0.53:53 (L
ISTEN)
avahi-dae 1007           avahi   12u  IPv4  22164      0t0  UDP *:5353
avahi-dae 1007           avahi   13u  IPv6  22165      0t0  UDP *:5353
avahi-dae 1007           avahi   14u  IPv4  22166      0t0  UDP *:36777
avahi-dae 1007           avahi   15u  IPv6  22167      0t0  UDP *:42542
cupsd     1064            root    6u  IPv6  22235      0t0  TCP [::1]:631 (LISTE
N)
cupsd     1064            root    7u  IPv4  22236      0t0  TCP 127.0.0.1:631 (L
ISTEN)
```

The purpose of this command is to:

- The function of lsof is to list open files
- The purpose of the “-i” is to list network files
- “-P” flag prevents conversion from port numbers to names (helps output clarity)
- “ -n” flag prevents conversion of IPs to hostnames

Scanning my VM network with nmap:
The command I used to do this was: sudo nmap -sS -O localhost

```
vansises@sv09:~$ sudo nmap -sS -O localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2025-09-25 17:00 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000060s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
631/tcp open  ipp
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```

The purpose of this command is to:

- Scan my VM to identity open ports and the OS
- Checks what is running in the VM
- Discovers hosts and services on a given network
- “-O” flag finds the OS of the target system
- “-sS” flag is for performing a stealth TCP SYN scan

Checking for open ports on my servers network:
The command I used to do this was: sudo nmap -sP 192.168.1.0/24

```
vansises@sv09:~$ sudo nmap -sP 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2025-09-25 17:02 UTC
Nmap scan report for 192.168.1.0
Host is up (0.0060s latency).
Nmap scan report for 192.168.1.1
Host is up (0.0030s latency).
```

```
Host is up (0.0059s latency).
Nmap scan report for 192.168.1.255
Host is up (0.0064s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 61.90 seconds
```

The purpose of this command is to:

- Identify all live hosts on the VM

Checking services and versions:
The command I used to do this was: sudo nmap -sV localhost

```
vansises@sv09:~$ sudo nmap -sV localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2025-09-25 17:04 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000010s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE VERSION
631/tcp open  ipp     CUPS 2.4

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.27 seconds
```

The purpose of this command is to:

- Scan for open ports and see what version is running
- “-sV” flag is for version detection

Identifying the vulnerabilities in my VM:
The command I used to do this was: sudo nmap --script vuln localhost

```
vansises@sv09:~$ sudo nmap --script vuln localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2025-09-25 17:05 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000010s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
631/tcp open  ipp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
| http-enum:
|   /admin.php: Possible admin folder
|   /admin/: Possible admin folder
```

```
|   /admin.nsf: Lotus Domino
|   /administrator/wp-login.php: Wordpress login page.
|   /admin/libraries/ajaxfilemanager/ajaxfilemanager.php: Log1 CMS
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: Op
enCart/FCKeditor File upload
|   /admin/includes/tiny_mce/plugins/tinybrowser/upload.php: CompactCMS or B-Hin
d CMS/FCKeditor File upload
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Bl
og / FCKeditor File Upload
|   /admin/jscript/upload.php: Lizard Cart/Remote File upload
|   /admin/jscript/upload.html: Lizard Cart/Remote File upload
|   /admin/jscript/upload.pl: Lizard Cart/Remote File upload
|   /admin/jscript/upload.asp: Lizard Cart/Remote File upload
|   /admin/environment.xml: Moodle files
|   /classes/: Potentially interesting folder
|   /es/: Potentially interesting folder
|   /help/: Potentially interesting folder
|_  /printers/: Potentially interesting folder
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-drown:

Nmap done: 1 IP address (1 host up) scanned in 31.39 seconds
```

The purpose of this command is to:

- Run a script that scans for vulnerabilities through nmap
- Finds common security risks on already installed software

Checking the network traffic through my VM:
The command I used to do this was: sudo tcpdump -i ens160

```
vansises@sv09:~$ sudo tcpdump -i ens160
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens160, link-type EN10MB (Ethernet), snapshot length 262144 bytes
21:59:49.099709 IP6 sv09 > ip6-allrouters: ICMP6, router solicitation, length 16
21:59:50.013176 IP sv09.41153 > 91.189.91.157.ntp: NTPv4, Client, length 48
21:59:50.031917 IP 91.189.91.157.ntp > sv09.41153: NTPv4, Server, length 48
21:59:50.116756 IP sv09.36652 > _gateway.domain: 56128+ PTR? 129.227.168.192.in-
addr.arpa. (46)
21:59:50.120341 IP _gateway.domain > sv09.36652: 56128 NXDomain*- 0/0/0 (46)
21:59:50.121275 IP sv09.40540 > _gateway.domain: 17993+ PTR? 157.91.189.91.in-ad
dr.arpa. (44)
21:59:50.232309 IP _gateway.domain > sv09.40540: 17993 NXDomain*- 0/0/0 (44)
21:59:50.236454 IP sv09.59268 > _gateway.domain: 36074+ PTR? 2.227.168.192.in-ad
dr.arpa. (44)
21:59:50.246870 IP _gateway.domain > sv09.59268: 36074 NXDomain*- 0/0/0 (44)
21:59:55.071516 ARP, Request who-has _gateway tell sv09, length 28
21:59:55.072457 ARP, Reply _gateway is-at 00:50:56:f1:a7:07 (oui Unknown), lengt
h 46
^C
11 packets captured
11 packets received by filter
0 packets dropped by kernel
```

The purpose of this command is to:

- Monitor all network traffic going through my VM
- Helps for detecting suspicious activity or frequent activities / visits

Watching connections to my VM network real time:
The command I used to do this was: sudo watch -n 1 netstat -tulnp

```
Every 1.0s: netstat -tulnp                          sv09: Thu Sep 25 17:09:56 2025

Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
996/systemd-resolve
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
1064/cupsd
tcp6       0      0 ::1:631                 :::*                    LISTEN
1064/cupsd
udp        0      0 0.0.0.0:5353            0.0.0.0:*
1007/avahi-daemon:
udp        0      0 0.0.0.0:36777           0.0.0.0:*
1007/avahi-daemon:
udp        0      0 127.0.0.53:53           0.0.0.0:*
996/systemd-resolve
udp        0      0 192.168.227.129:68      0.0.0.0:*
974/systemd-network
udp6       0      0 :::5353                 :::*
1007/avahi-daemon:
udp6       0      0 :::42542                :::*
1007/avahi-daemon:
```

The purpose of this command is to:

- Second by second I was able to monitor the network connections on my VM

Checking my VM firewalls:
The command I used to do this was: sudo ufw status verbose

```
vansises@sv09:~$ sudo ufw status verbose
Status: inactive
```

The purpose of this command is to:

- Display the firewall rules you currently have configured
  (the result came out as inactive due to this lab being performed before firewalls were added on to this VM)
- Typically this would help users ensure only ports they would like to be open are