# Task 1: Getting Started with nmap

1. Run: man nmap
2. What do the following switches do?

|  |  |
| --- | --- |
| **Switch** | **Purpose of switch (taken from the output produced by the “man nmap” command)** |
| -sn | Tells Nmap to not do a port scan after discovering a host, and only print out available hosts that responded to the scan. This is also known as a “ping scan”.  -sn stands for no port scan |
| -PO | Sends IP packets with the specified protocol numbers in the protocol field of the IP headers.  The ultimately purpose of this switch is to look for responses in the same protocol as the probes, or ICMP Protocol Unreachable messages that signify that the specified IP protocol isn’t supported on the host.  -PO stands for IP Protocol Ping |
| -PS | Sends an empty TCP packet with the SYN flag set. Suggests to remote system that we are trying to establish a connection.  If the port is open, we will get back a SYN/ACK TCP packet, to which Nmap will send a RST packet to stop the TCP connection from establishing.  -PS stands for portlist, also known as TCP SYN Ping |
| -sO | Allows us to determine which IP protocols are supported by the target machine. These protocols can include: TCP, ICMP, IGMP, etc.  It is not a port scan, because it cycles through IP protocol numbers rather than port numbers.  -sO stands for IP protocol scan |
| -sV | This switch enables version detection.  Version detection assists with determining which version a server may be running, thus assisting us with determining what the server may be vulnerable to.  -sV stands for version detection |
| -O | This switch enables OS detection.  This switch works by sampling TCP/IP options and comparing it to nmap-os-db. Hence, the patterns of responses can be used to figure out if there is a match for a given OS.  Similar to -sV, knowing the OS of the target assists with determing what the target may be vulnerable to.  -O stands for enabling OS detection |

# Task 2: Using nmap to conduct a reconnaissance of your network

1. **Use a broad ping scan to determine the hosts that are “up” on a portion of your lab network: nmap -n -sn IPaddress**

Quick note: I had to use -sP instead of -sn (I think this is because the metasploit machine which I am using is an older version than what the lab asks for, but I am indeed using the machine provided in the PDF for this lab), and I also used 10.0.0.0/24, since I am on my own network and not a lab network with other peers (I believe this is the intent of the ask for ask 1, here).

1. Record the results.

**Exhibit 1:** The results of running the command, “nmap -n -sP 10.0.0.0/24”

Text

Description automatically generated

1. Why is the -n option used? What happens if you rerun this command without the -n option?

According to the nmap manual, the -n option tells the scan to not perform a DNS resolution on the active IP addresses that are found. Hence, rerunning the command without the -n option makes the scanning time much longer, as nmap is attempting to perform the DNS resolution for each IP address which is “up”.

1. **Conduct an IP protocol ping (switch -PO / -PS / -PU) on the Common Network hosts.**

Quick Note: I believe that the common network is perhaps in reference to a network which other peers would be using. Perhaps such a network would share Common Network hosts, as mentioned in this question. To emulate this, I spun up another VM with the IP address of 10.0.2.13 and performed the protocol ping on this IP address.

1. There are 8 TCP ports that are open
2. There does not seem to be any UDP ports open.

**Exhibit 2:** Results of performing the IP protocol ping on my common network host.

Text

Description automatically generated

1. **Conduct an IP protocol ping on yourself.**

**Exhibit 3:** Ifconfig shows that my IP address is: 10.0.2.15.

**Text

Description automatically generated**

**Exhibit 4:** Results of the scan on 10.0.2.15 (part 1 of the scan)

**Text

Description automatically generated**

**Exhibit 5:** Results of the scan on 10.0.2.15 (part 2 of the scan)

**Text

Description automatically generated**

* 1. How many ports are open?
     1. 22 ports are open.

1. **Conduct an IP protocol scan (switch -sO) on target host.**

Quick note: I decided to run the command on 10.0.2.13, as I had done for question 2, in order to answer the question below.

**Exhibit 6:** Results of running the command, “sudo nmap -sO 10.0.2.13”

Text

Description automatically generated

* 1. Are the results different than that attained with the IP protocol ping? Explain.

Yes, the results are different than those which were attained with the IP protocol ping. Specifically, the scan seems to return more general services than the specific protocols that were returned in the protocol ping.

For example, rather than listing each tcp service, the IP protocol scan returned other services such as icmp, igmp, udp, and udplite. Also, the protocol scan returned whether the service had a state of “open” or “open:filtered”, which was not seen within the scan shown within exhibit 4 or 5.

1. **Performing OS detection on the host**
   1. What operating system does nmap think your Server VM is running?

Quick note: To run this command, I ran it against my other VM running on the IP address of 10.0.2.13. Interestingly, nmap was unable to fingerprint the given VM. It is running Ubuntu 16.04, and is the VM which was provided to our class for purposes of the SEED labs.

**Exhibit 7:** Attempting to find the OS of the Server VM running on 10.0.2.13. I noted that the message returned indicates that nmap was unable to determine the OS.

Text

Description automatically generated

* 1. What is its MAC address?
     1. 08:00:27:A6:95:06 (see exhibit 7)
  2. What OS does nmap think your Linux VM is running?
     1. Linux 2.6.18

**Exhibit 8:** The command which was run against the Linux VM to determine the OS that nmap thought the VM was running.

Text

Description automatically generated

**Exhibit 9:** Presented OS details from nmap

Text

Description automatically generated

1. **Using nmap to perform services/version detection**
   1. What version of ssh is running on your target host?
      1. 2.0
      2. Quick Note: I had restarted my computer which resulted in my target host’s ip changing from 10.0.2.15 to 10.0.2.13.

**Exhibit 10:** Results from attempting to obtain ssh version on target host

Text

Description automatically generated

* 1. What web server is running on your target host?
     1. http via Apache httpd 2.4.18 (Ubuntu)

**Exhibit 11:** Determining the web server that is running on my target host

Text

Description automatically generated

1. Testing for vulnerable services via port scanning:

**Exhibit 12:** TCP Null (-sN) scan

Text

Description automatically generated

**Exhibit 13:** FIN (-sF) scan

Text

Description automatically generated

**Exhibit 14:** Xmas (-sX) scan

Text

Description automatically generated