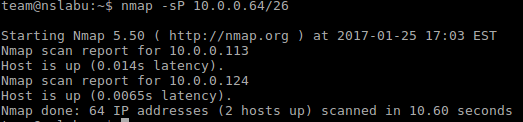
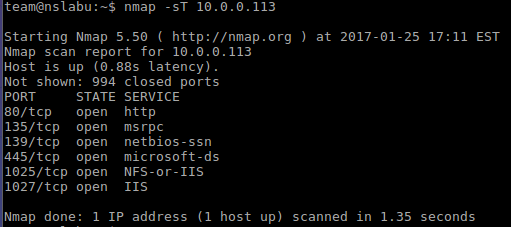
First we look at the functions for command nmap –sS, -sT, -sU, -sP

Parameters for nmap in man page

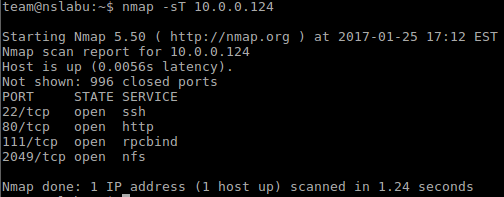
1. By using –Sp parameter, nmap sends each host an ICMP echo and TCP ACK. If the hosts respond to the packages sent by nmap, the response would be retrieved by nmap.

1.Result for nmap –sP 10.0.0.64/26

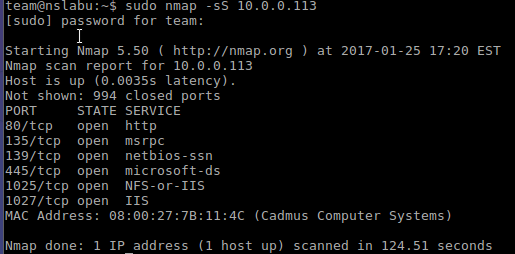
nmap scans each host in 10.0.0.64/26 (64 IP addresses in all). As mentioned in the lab page, 2 systems(10.0.0.113 and 10.0.0.124) were discovered.

2.1 Result for nmap –sT 10.0.0.113

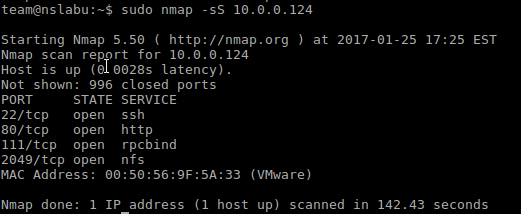
2. For host 10.0.0.113, port 80, 135, 139, 445, 1025, 1027 are open for connection. The type of connection for each port is listed behind.

For host 10.0.0.113, port 22, 80, 111, 2049 are open for connection. The type of connection for each port is listed behind.

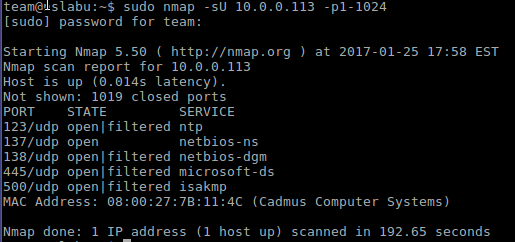
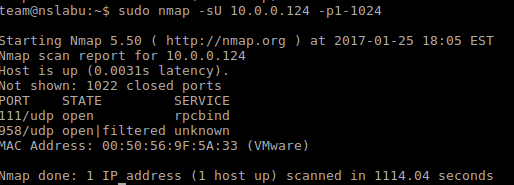
2.2 Result for nmap –sT 10.0.0.124

3. nmap –sS ipaddress is different from –sT. nmap starts by a SYN packet scan, and each host would reply with a SYN ACK. Then nmap sends a RST to stop the connection, thus making less record on the target machine.

3.1 Result for nmap –sS 10.0.0.113

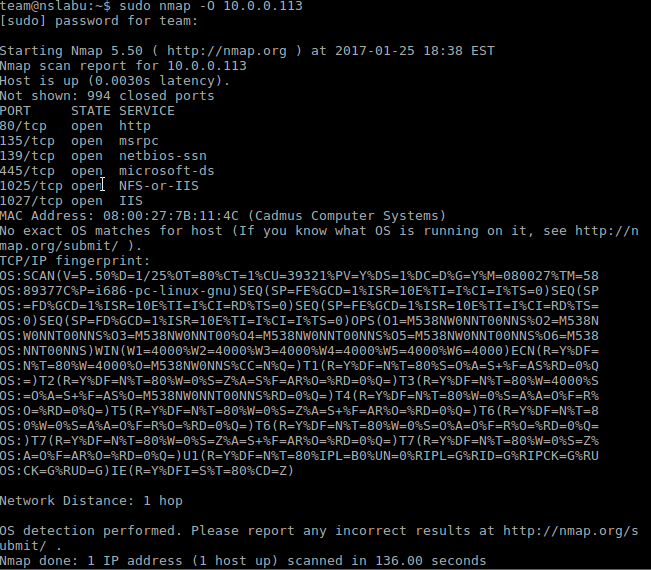
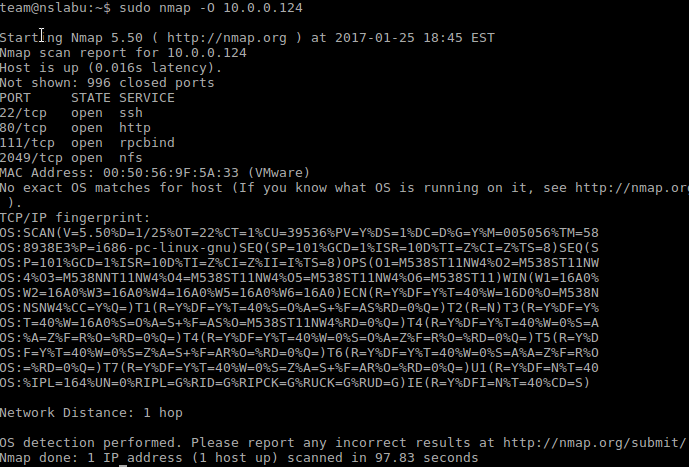
When executing the command for –sS, it needs the root priority. The outcomes for ports of both hosts are the same with those of –sT. But the time consumed is longer.

3.2 Result for nmap –sS 10.0.0.124

4. UDP scan for port 1-1024. The time consumed for this UDP scan is even longer than the previous SYN scan. The UDP scan also needs root authority.

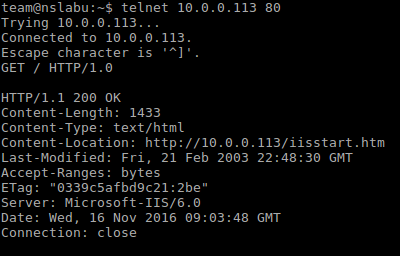
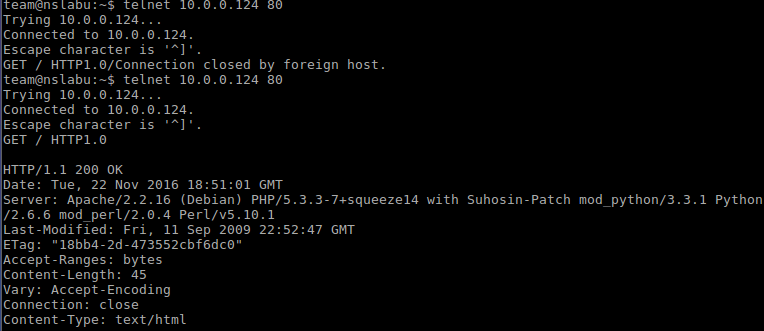
4.2 Result for nmap UDP scan for port 1-1024 for 10.0.0.124

4.1 Result for nmap UDP scan for port 1-1024 for 10.0.0.113

5. Operation system identification scan

5.2 Result for nmap -O 10.0.0.113

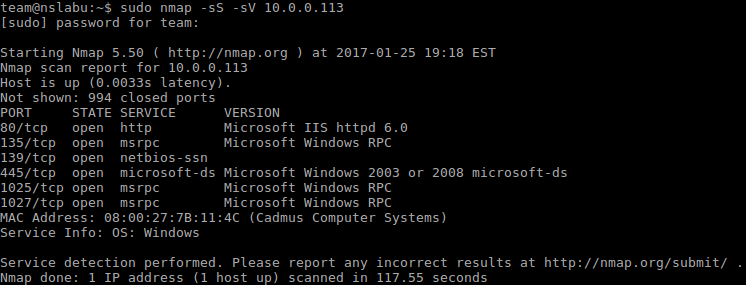
5.1 Result for nmap -O 10.0.0.113

6. Getting server header grab

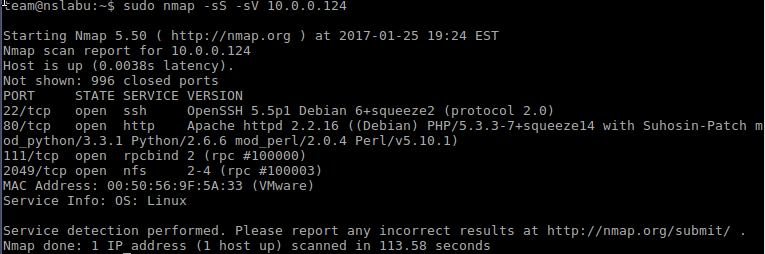
6.2 Result for server\_header grab 10.0.0.124

6.1 Result for server\_header grab 10.0.0.113

The server for 10.0.0.113 is Microsoft-IIS/6.0, and the server for 10.0.0.124 is Apache/2.2.16 (Debian) PHP/5.3.3-7+squeeze14 with Suhosin-Patch mod\_python/3.3.1 Python/2.6.6 mod\_perl/2.0.4 Perl/v5.10.1

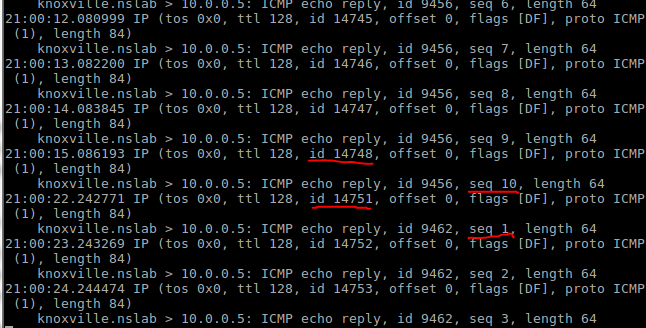
7. Service probes –sS –sV

7.1 Result for service probe 10.0.0.113



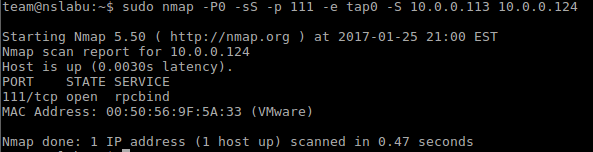
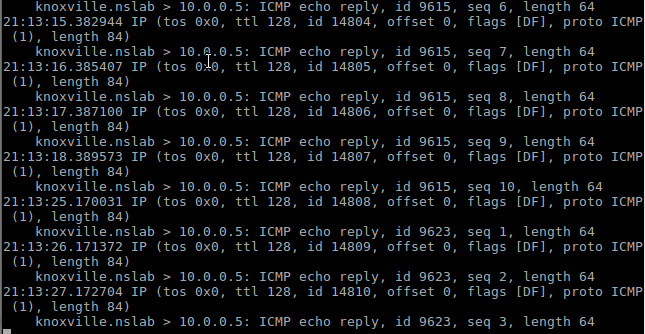
7.2 Result for service probe 10.0.0.124

We can see that the service identification running on port 80 for both systems are exactly the same with the ID we have found in section 6. Besides the service types on other ports are retrieved by command nmap –sS –sV.

8. The annotated snippet of your tcpdump showing the IP ID sequence hole

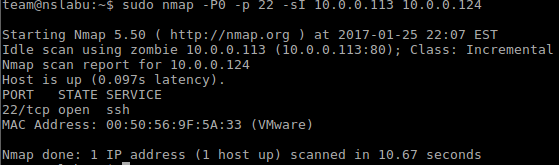
8.1 Result for open port tcpdump

The size of hole for this attempt is 3.



8.3 Result for tcpdump for closed port 112

8.2 Result for nmap scan for open port 111

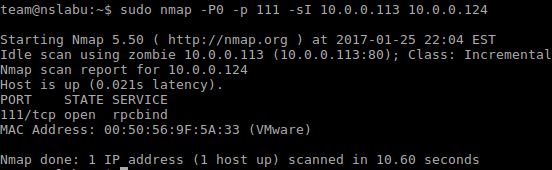
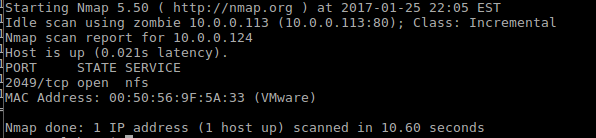
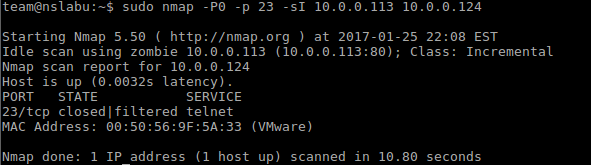
9. nmap idle scan

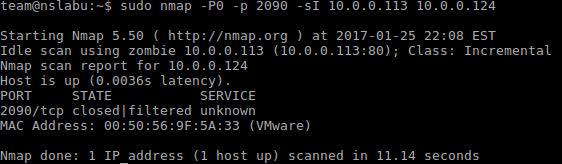
9.4 Result for idle scan for close port 23

9.3 Result for idle scan for open port 2049

9.2 Result for idle scan for open port 111

9.1 Result for idle scan for open port 22





9.5 Result for idle scan for close port 2090

10. What method does nmap use by default to ping a host?

If no host discovery options are given, Nmap sends an ICMP echo request, a TCP SYN packet to port 443, a TCP ACK packet to port 80, and an ICMP timestamp request.

11. Describe how you could use icmp\_ratelimit kernel parameter in Linux to slow down a UDP scan.

12. Which nmap scan typically runs faster, -sS or -sT? Why?

-sS runs faster than –sT. –sS needs to send a RST packet to end this communication between two hosts(no need to complete the connection), while –sT needs to complete the three way handshake.

13. In general, if any port scanner sends a datagram to a specific UDP port on a system and receives NO response, what can be concluded without any other information? (Hint: see the nmap man page, and consider networks which use firewalls.)

14. When running an idle scan against a victim, what happens if a specific port's SYN packets are dropped by the victim's firewall? How does this look to the attacker as compared to an open or closed port? If the scan target were running a tar-pit on every un-used TCP port, how effective would an idle scan be? For more background on this last question, you may want to search for "iptables TARPIT" on the web.

15. There are a number of ways that IP stacks can be written to reduce or eliminate the information leak of system-wide incremental IP IDs. How does Linux's IP stack defend against this? Name two techniques. See the "OS Vendors" section in this previously mentioned reference. How do these help defend against side-channel attacks?