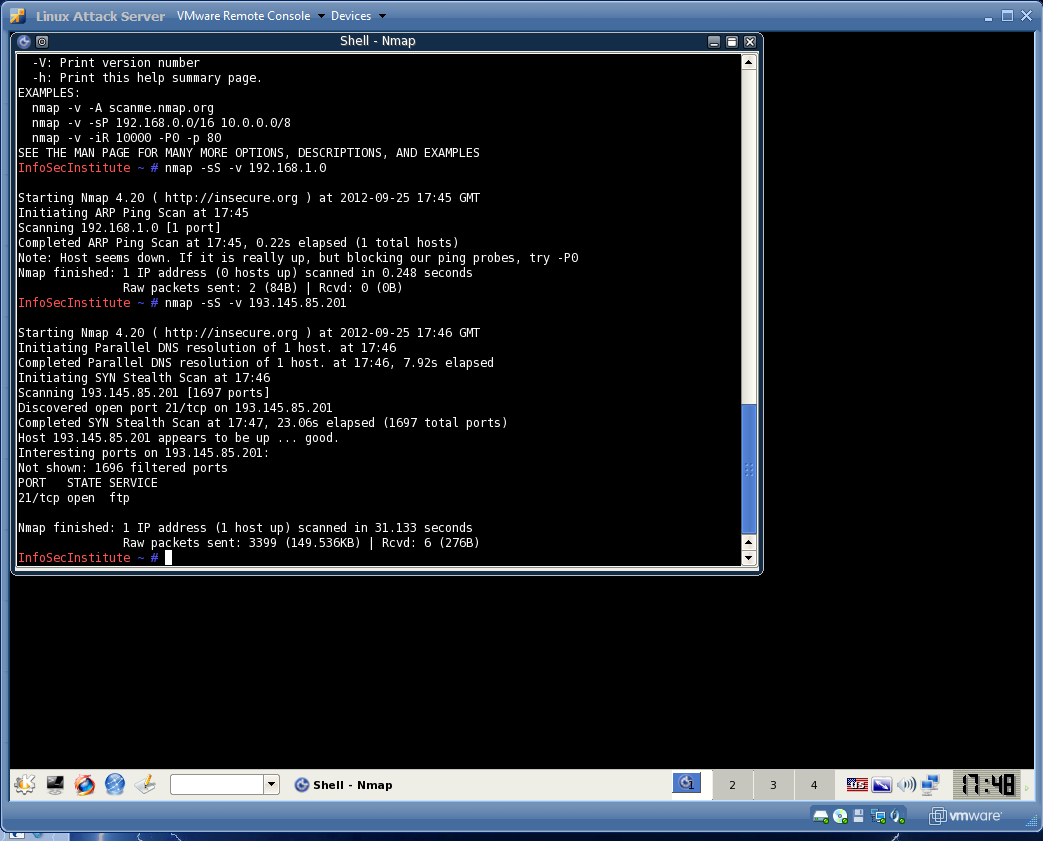
Alexander Cannell

09/25/2012

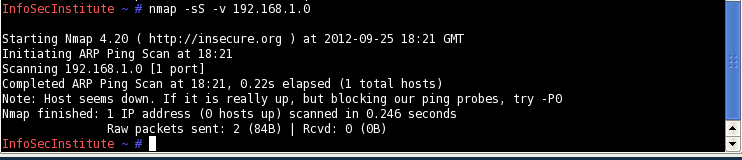
CSIS 3650

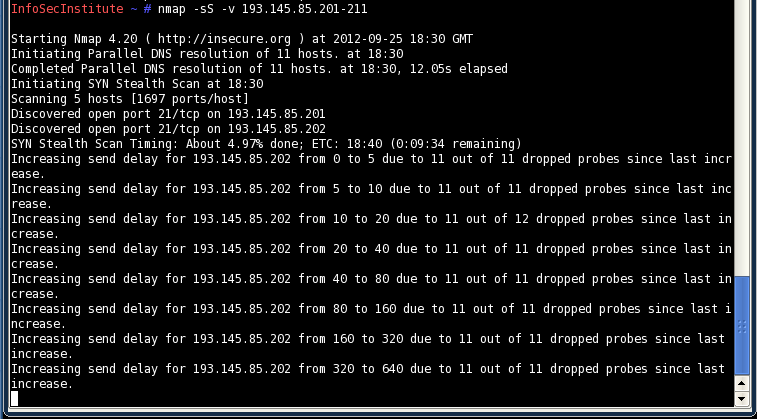
Chapter 5 Activities:

Activity 5-1:

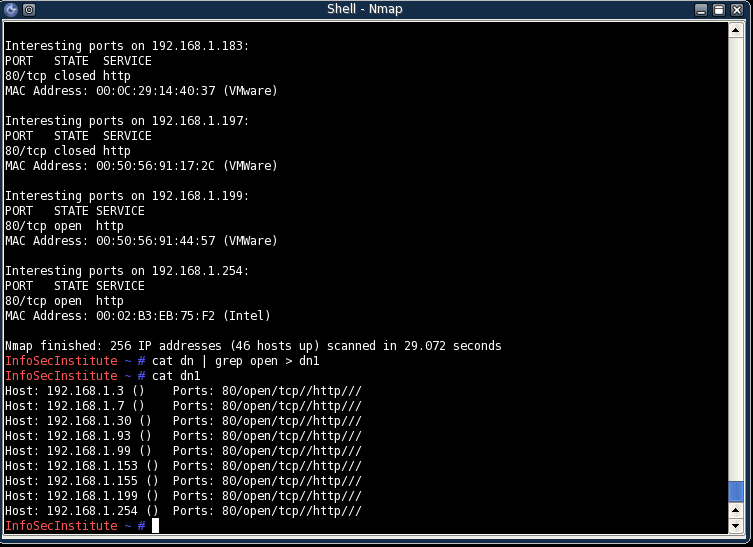


3. In a normal TCP session, a packet is sent to another computer with the SYN flag set.

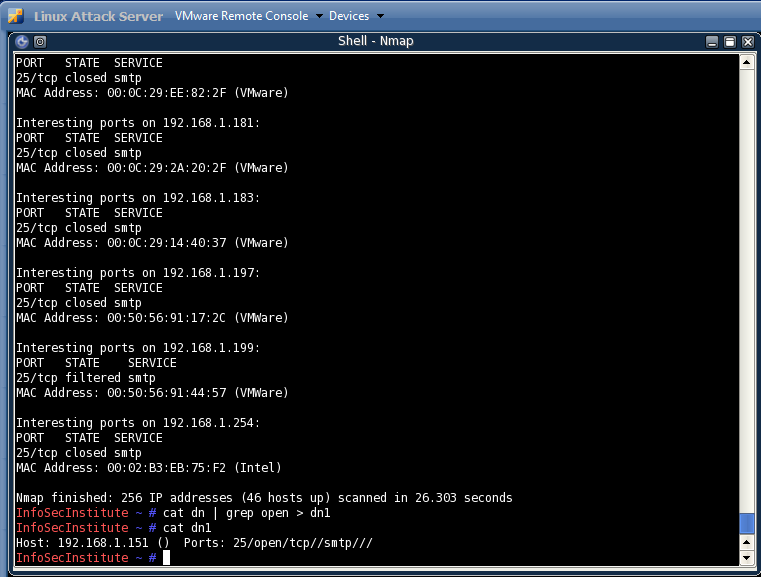
4. the new results are is only one port which makes sense because its my host computer. The first SYN scan had more information on it. Like open ports, interesting ports, not shown filtered ports…

5. This is scanning a range of computer hosts between 201-211. In this one there is a lot of delays and it finds a open ports on each node.

6. Port 80 HTTP Scan

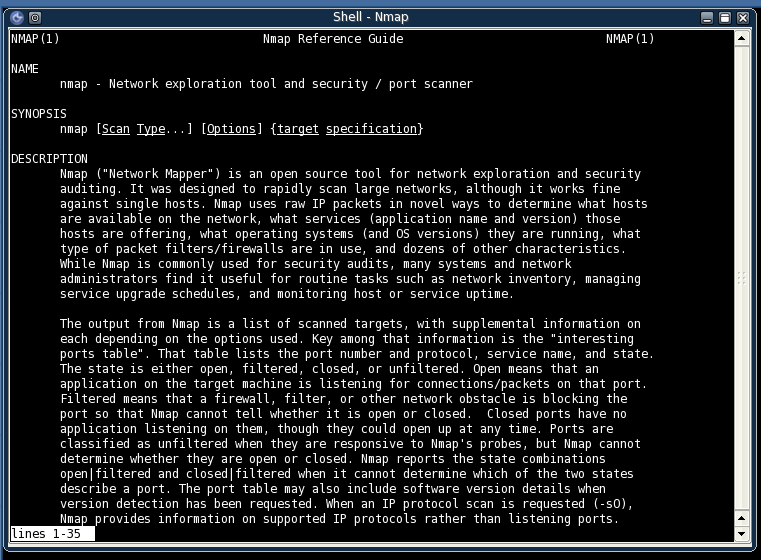


Port 25 SMTP scan which only found one open port.

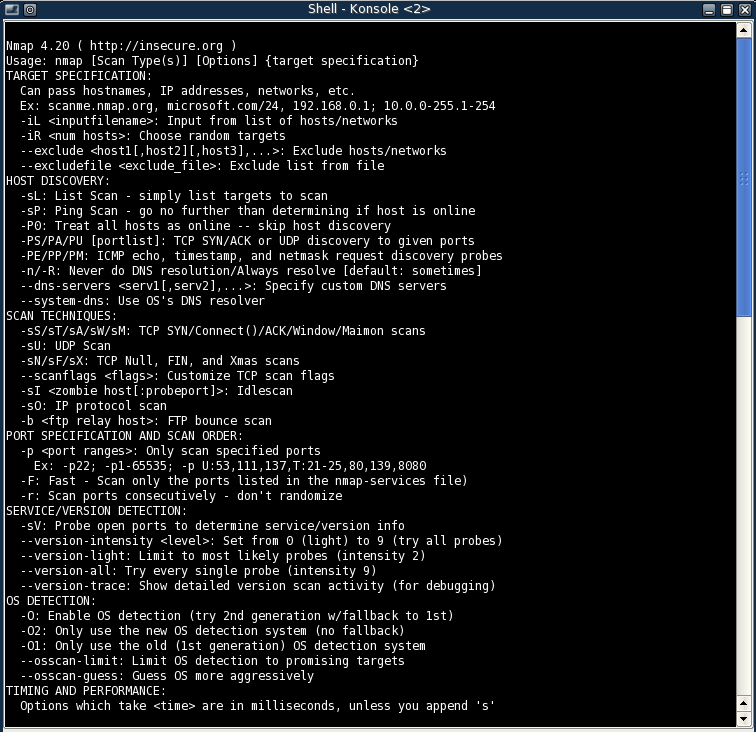


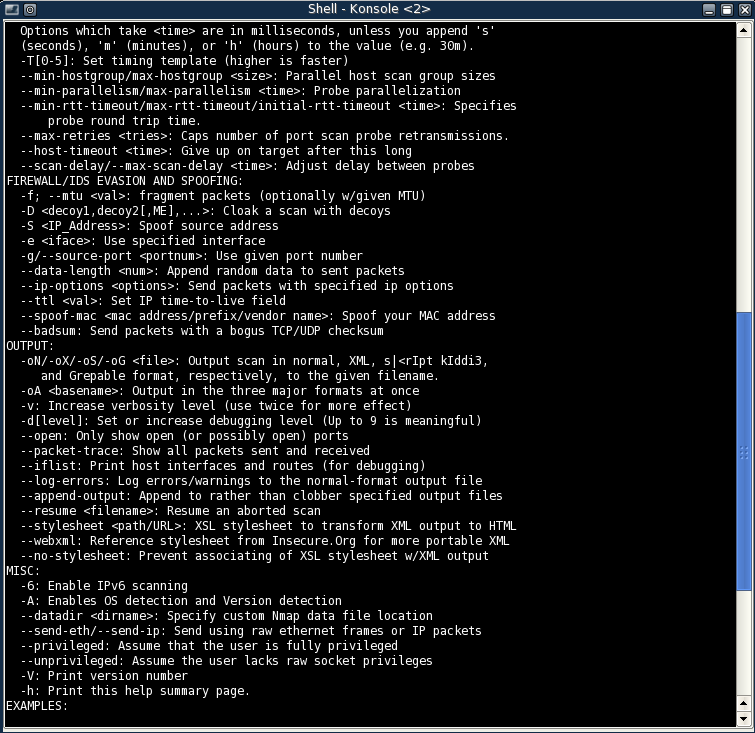
Activity 5-2:

1. After typing “man nmap”

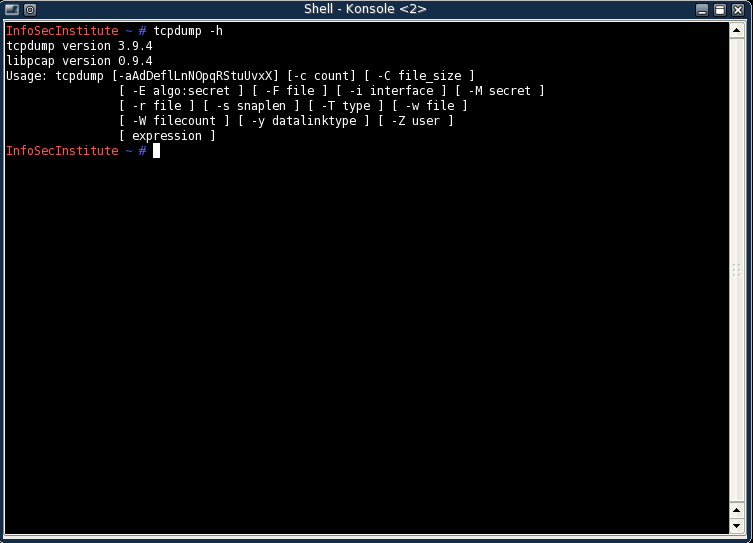


After typing nmap –h



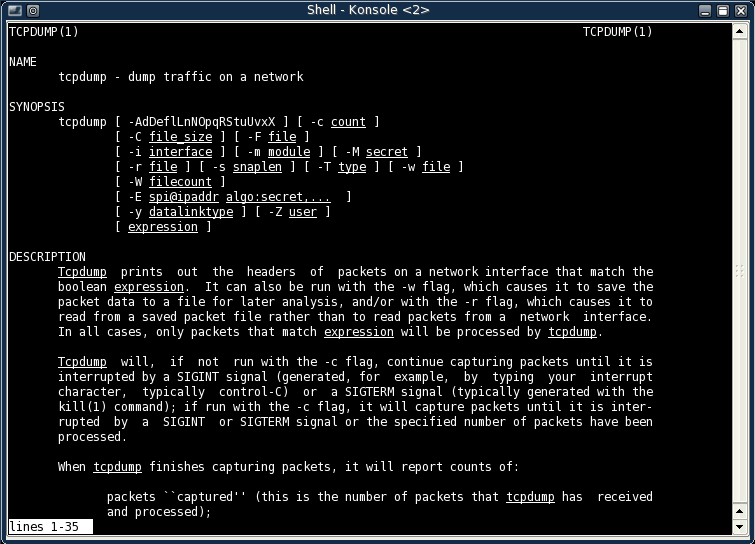


1. After typing tcpdump –h

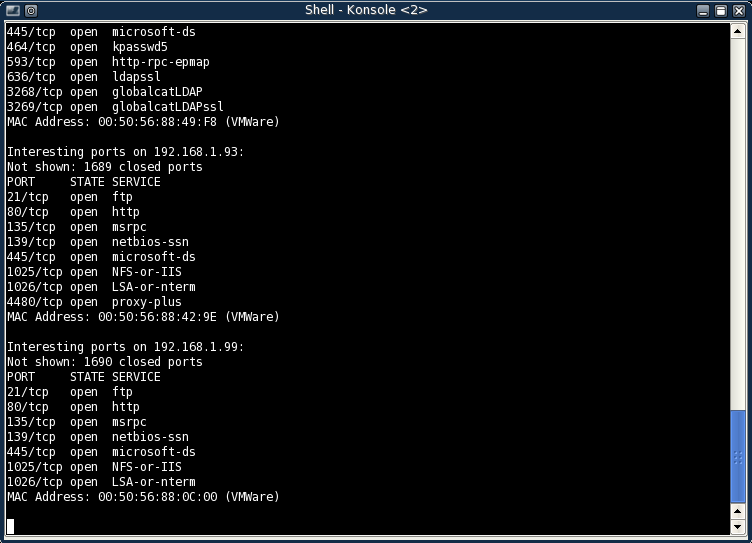


Tcpdump is a packet analyzer like wireshark.

1. After typing man tcpdump

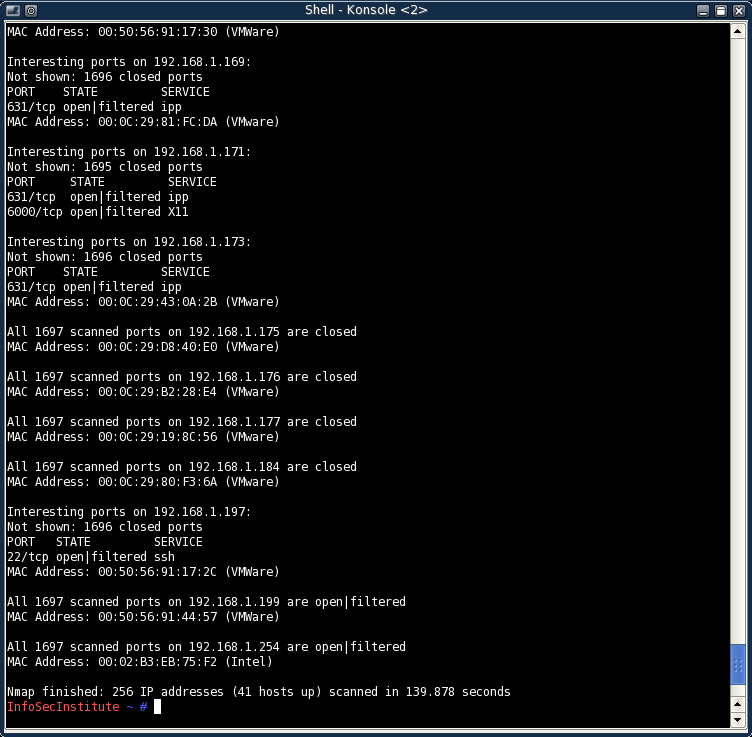


1. After doing a FIN or a SYN scan



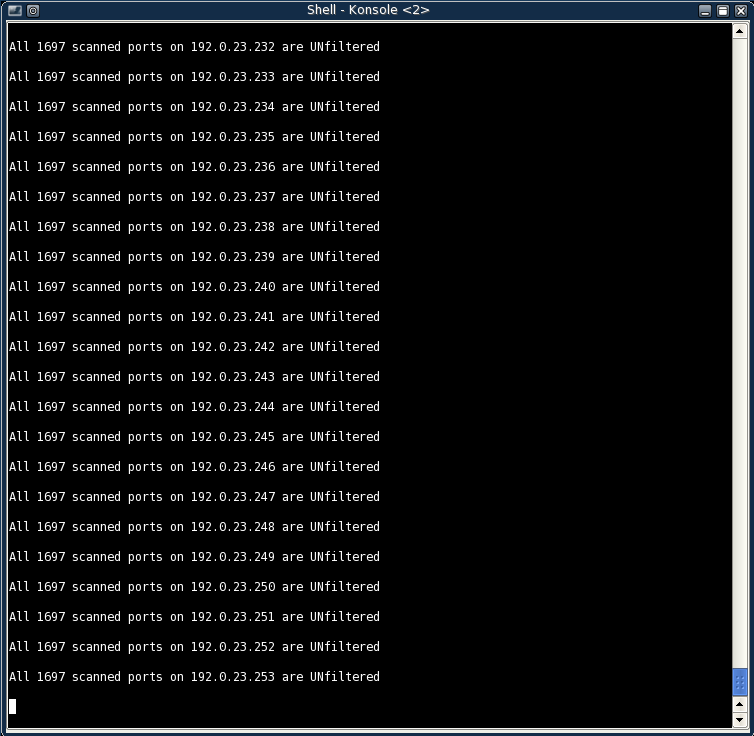
Yeah I got a lot of hits with a listing of the open ports, and IP addresses

1. After doing a XMAS Scan



Told me how many IP address there were and how many hosts are up and running. Also told me open ports that I can use.

1. After sending a ACK command



Its continuing to go through all the ipaddresses and saying unfiltered.

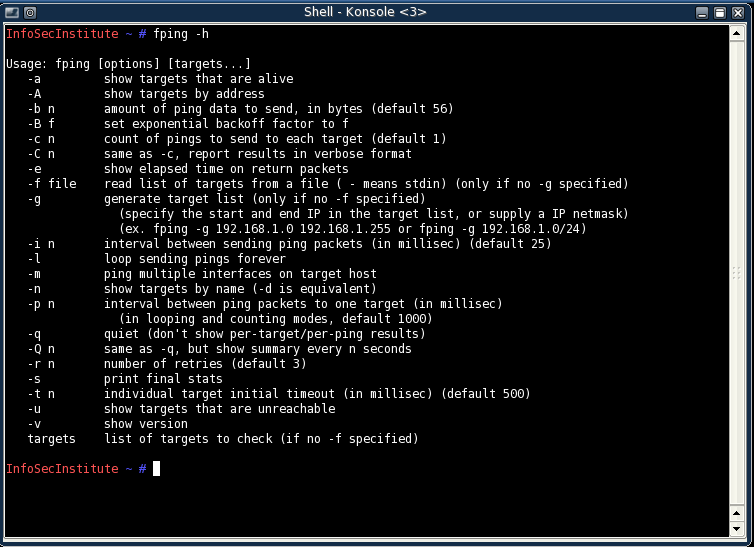
When I enter q it does this:

Stats: 0:14:39 elapsed; 8192 hosts completed (8128 up), 0 undergoing Host Discovery

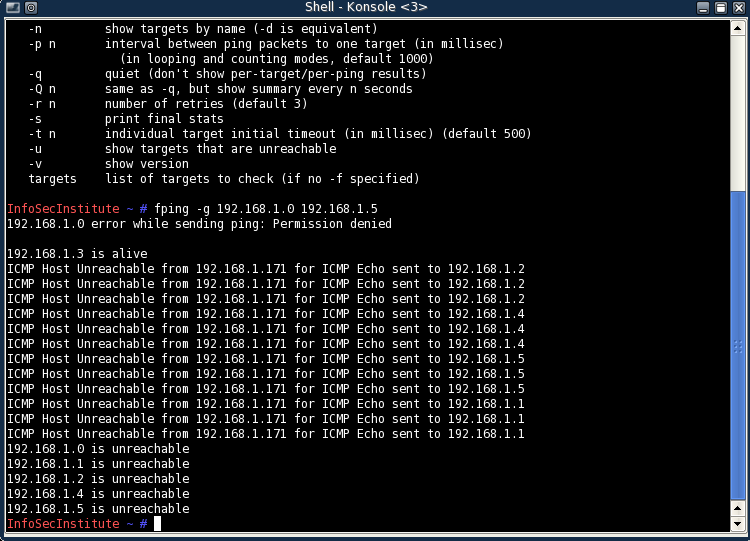
Parallel DNS resolution of 2048 hosts. Timing: About 94.83% done; ETC: 22:20 (0:00:02 remaining)

Activity 5-3:

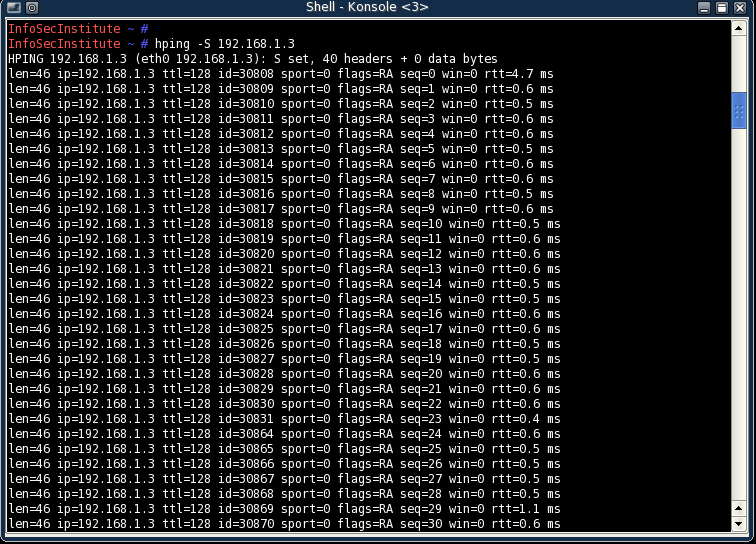
1. After typing fping –h



1. After typing fping -g 192.168.1.0 192.168.1.5



1. After typing hping -S 192.168.1.3



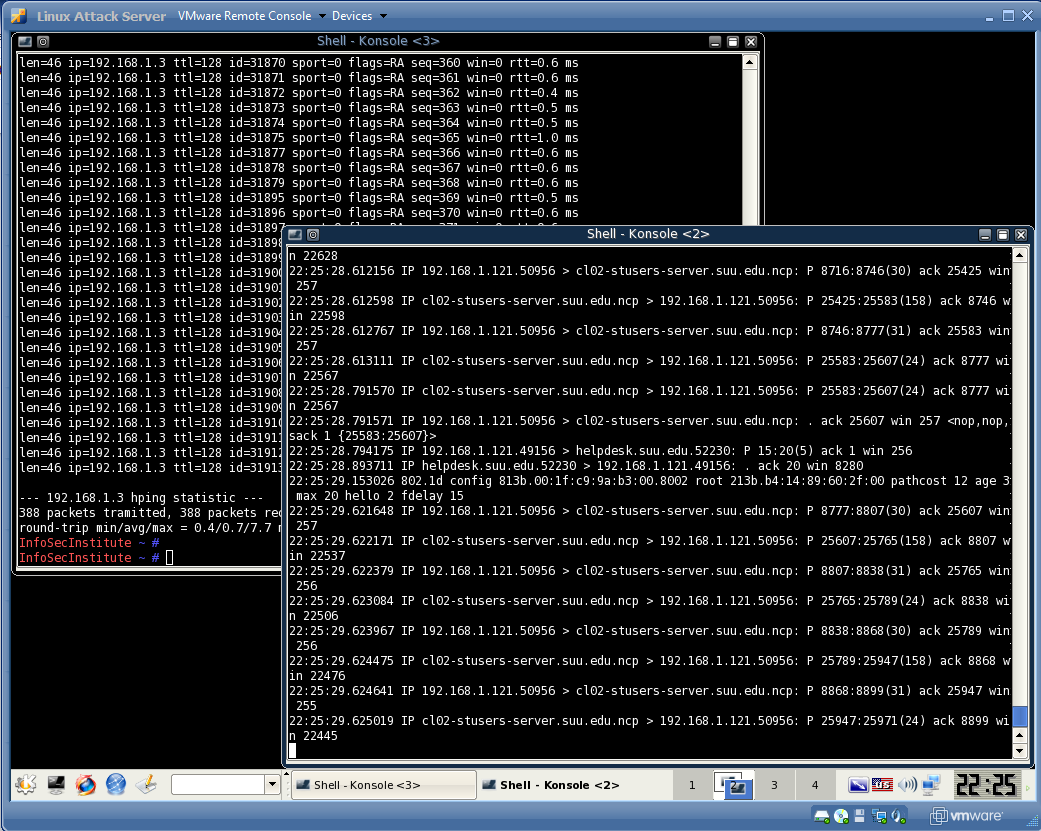
End result:

--- 192.168.1.3 hping statistic ---

388 packets tramitted, 388 packets received, 0% packet loss

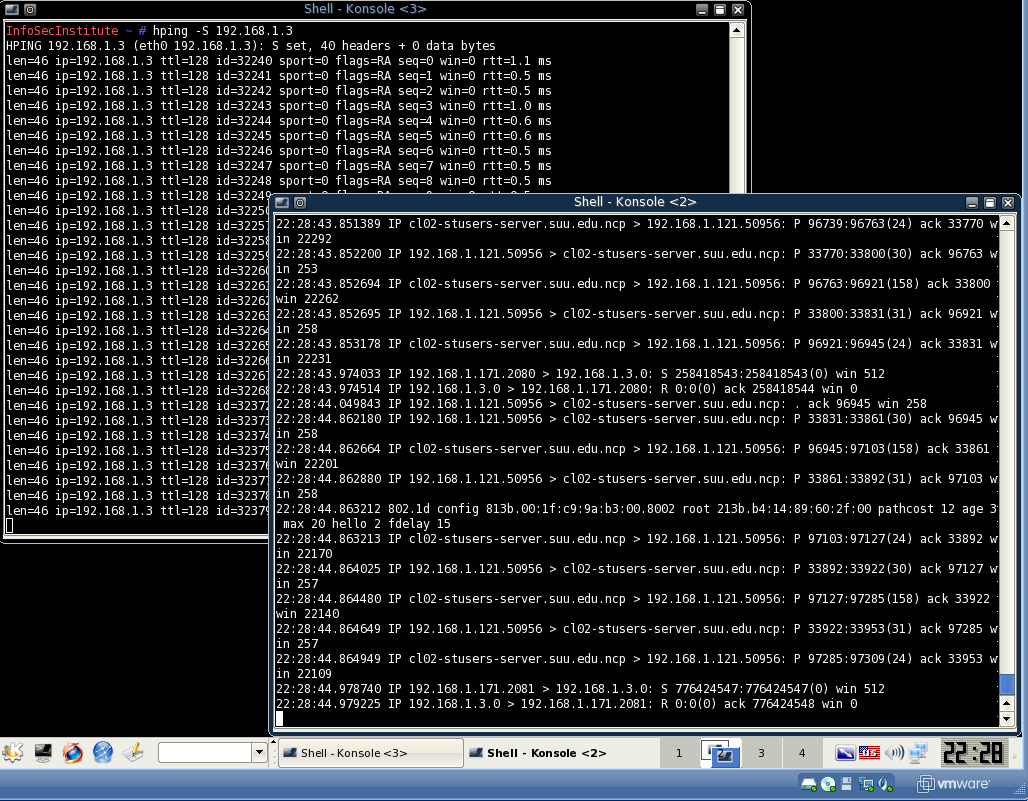
round-trip min/avg/max = 0.4/0.7/7.7 ms

1. After typing tcpdump



It is acting like wireshark and showing packets

1. After doing a hping –S scan the screen just jumped with packets

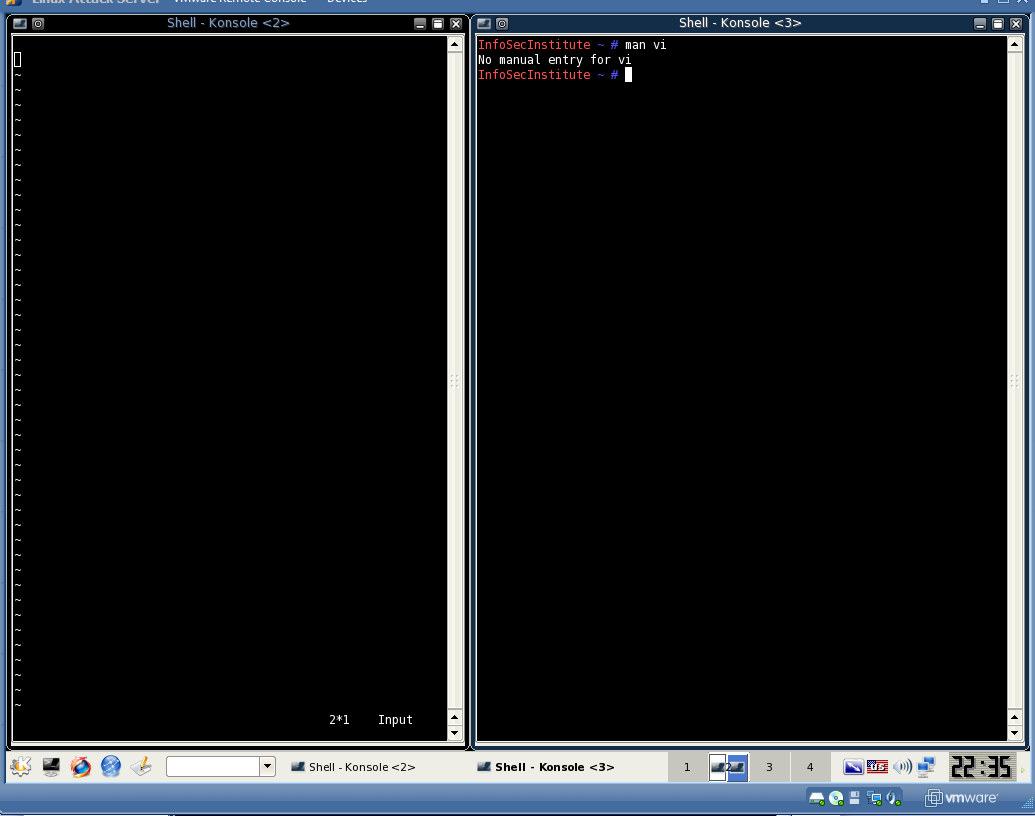


1. FIN scans(-sF) set just the TCP FIN bit. I didn’t see any change in response from the attack computer.

Activity 5-4:

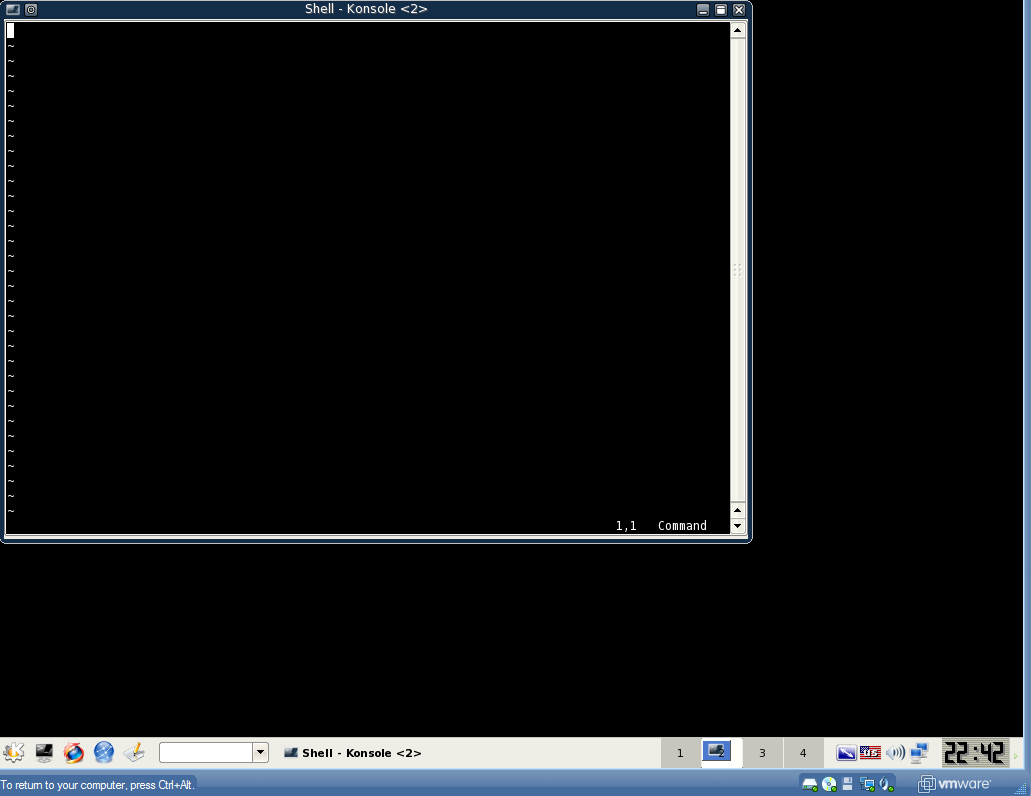






Said there was no manual entery for vi

1. I cant seem to get what the book is telling what I’m supposed to be getting all I’m getting is this:

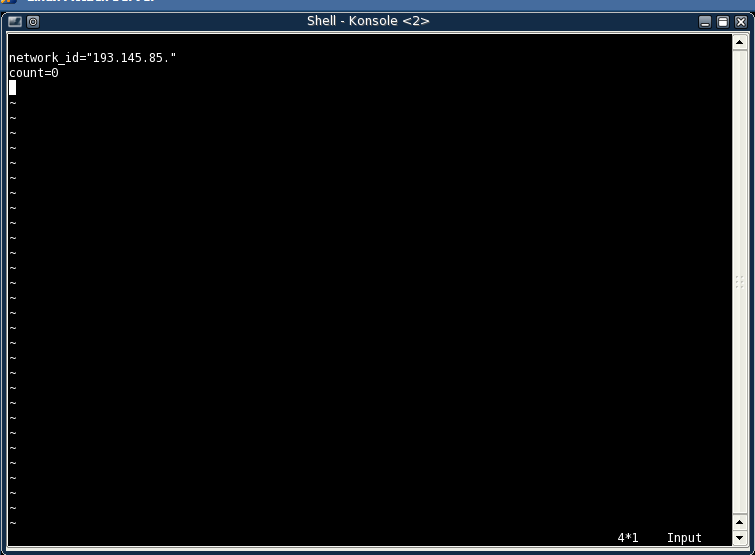


6.



Im still not getting what the book is telling me I should get.

7.



The commands didn’t work for me I don’t know why.

