Alexander Cannell

2/25/2013

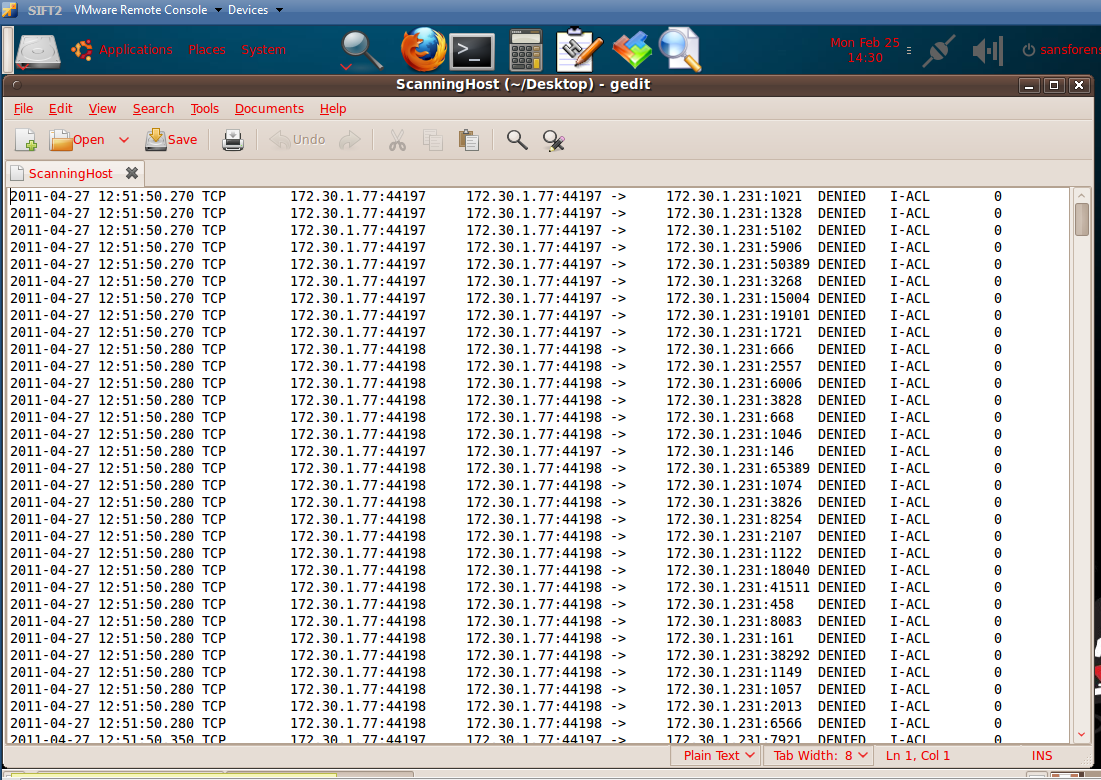
Professor Robertson

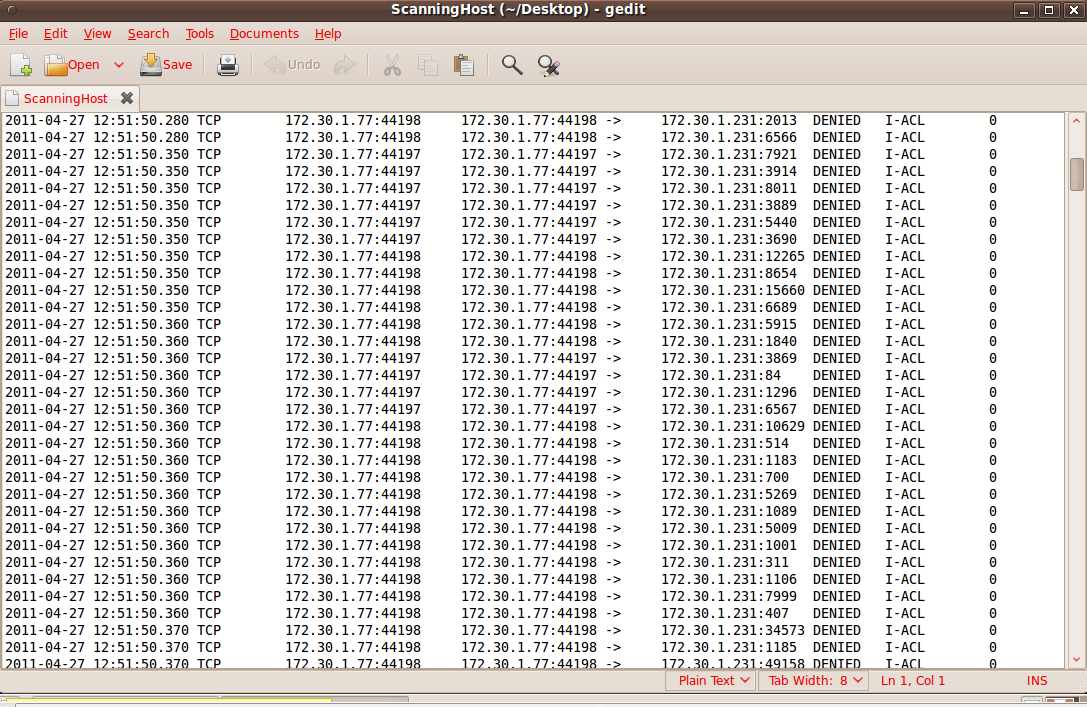
Case Study: The Curious Mr X

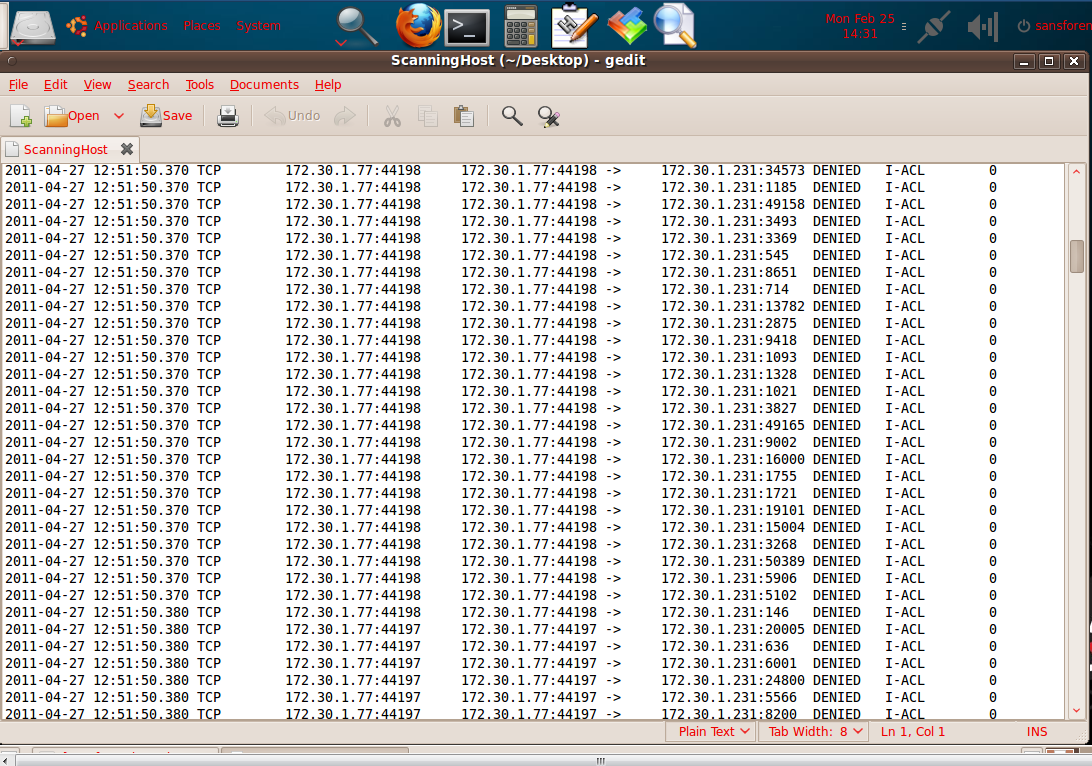
Introduction:

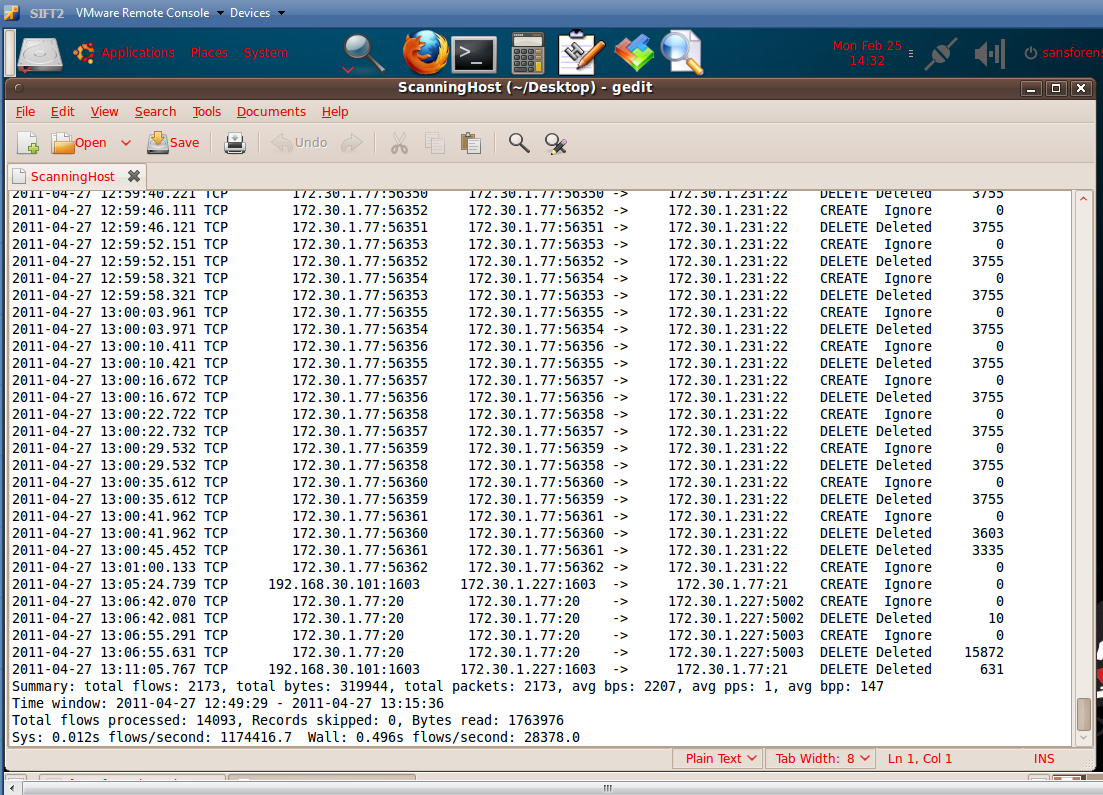
Mr. X is trying to infiltrate the Arctic Nuclear Fusion Research Facility Lab Network remotely. Mr X is not so steathly, we were able to capture the network flows recorded data. We know that Mr. X has been scanning ports, by this we know that his IP address is 172.30.1.77, I’m supposed to analyze his activities and answer three things Identify any compromised systems, Determine what the attacker found out about the network architecture, and Evaluate the risk of data exfiltration. I was able to utilize nfdump and ra/ Argus Client tools.

Executive Summary:

I first analysis the flows using nfdump and scanned the flows just for the known host IP 172.30.1.77, which we know is Mr. X. I used command line and copied and pasted the results into a text file. 

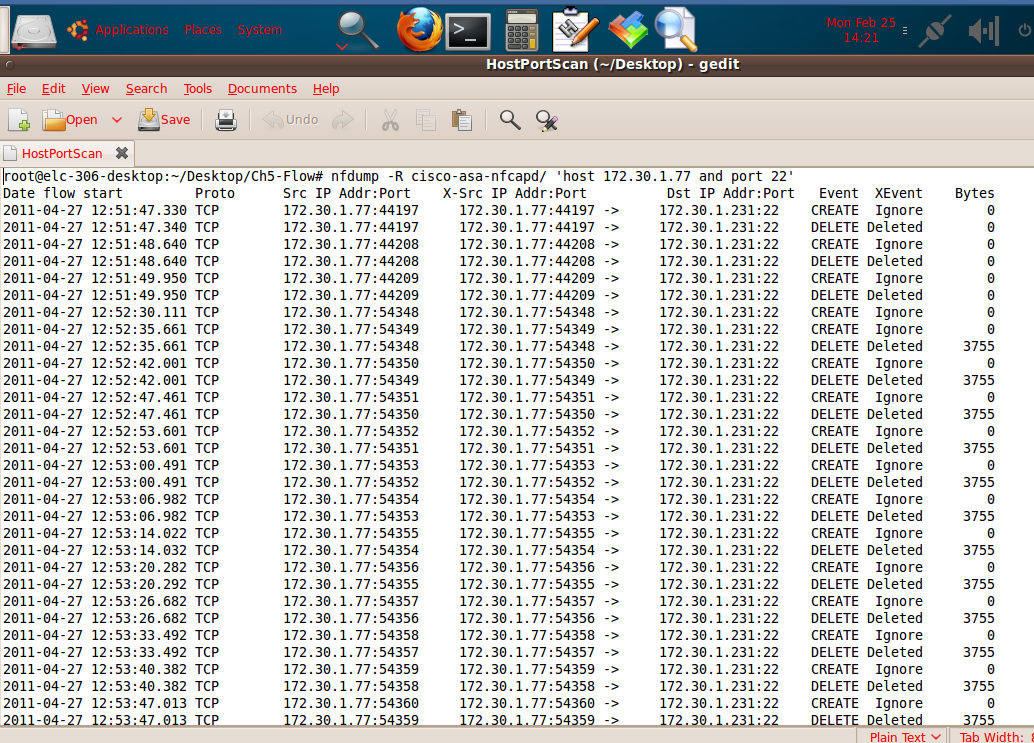


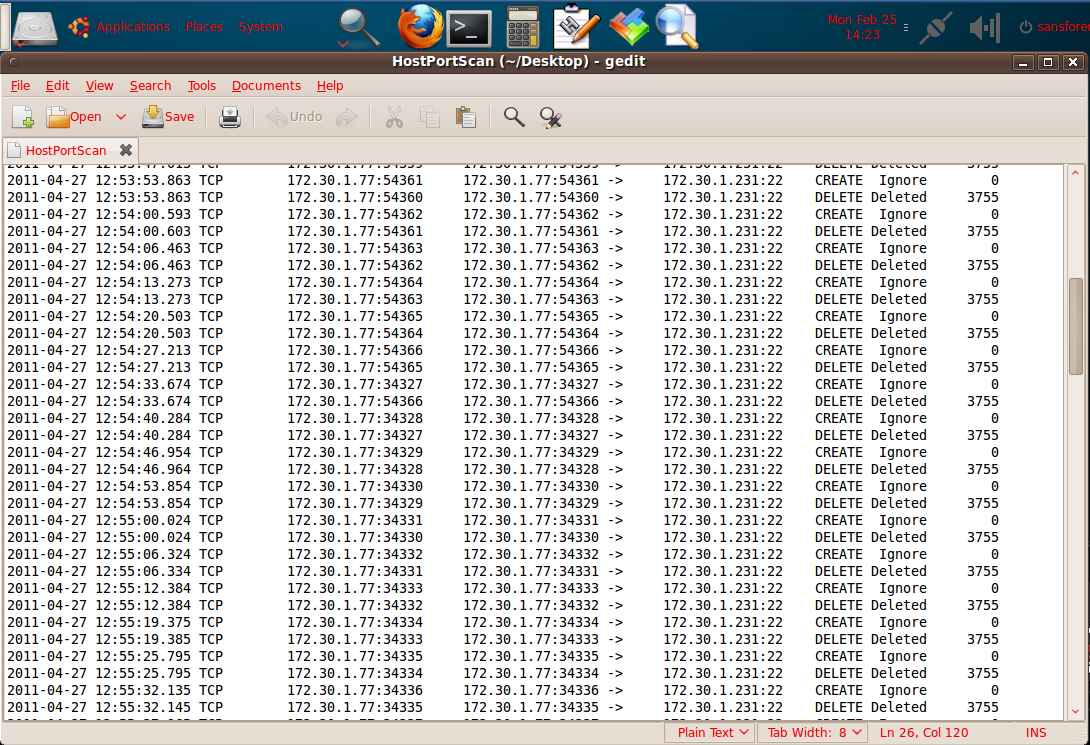


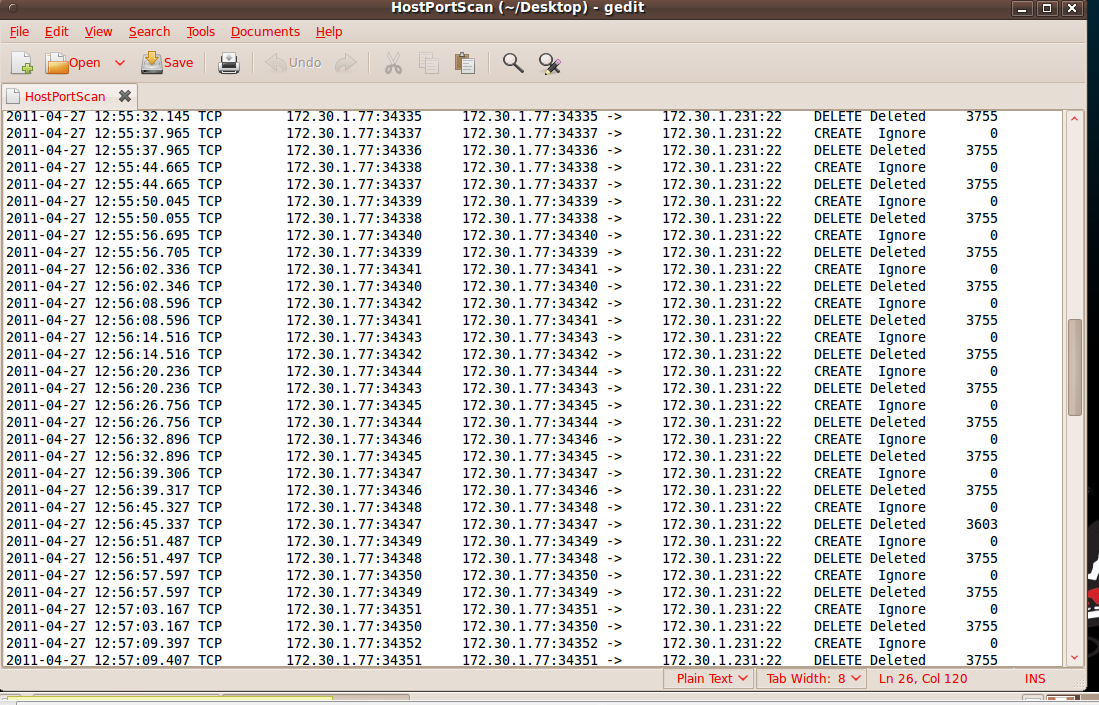


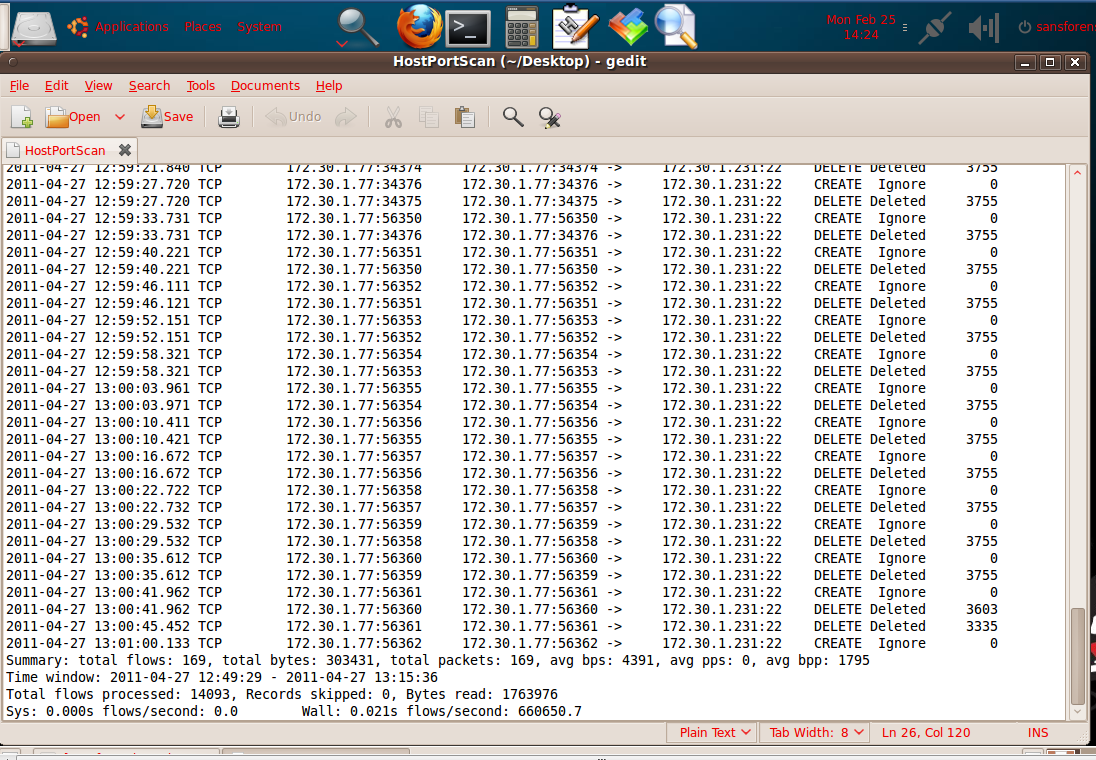
As we can see just by scanning the host Mr X 172.30.1.77 makes an attempt to connect with 172.30.1.231. The total flow: 2173, Total Bytes: 31994, Total Packets: 2173, and the Time Mr X spent was from 04/27/2011 12:49:29 to 04/27/2011 13:15:36.

I than analysis the flows using nfdump and scanned the flows and port tcp 22 for traffic just for the known host IP 172.30.1.77, which we know is Mr. X. I used command line and copied and pasted the results into a text file.



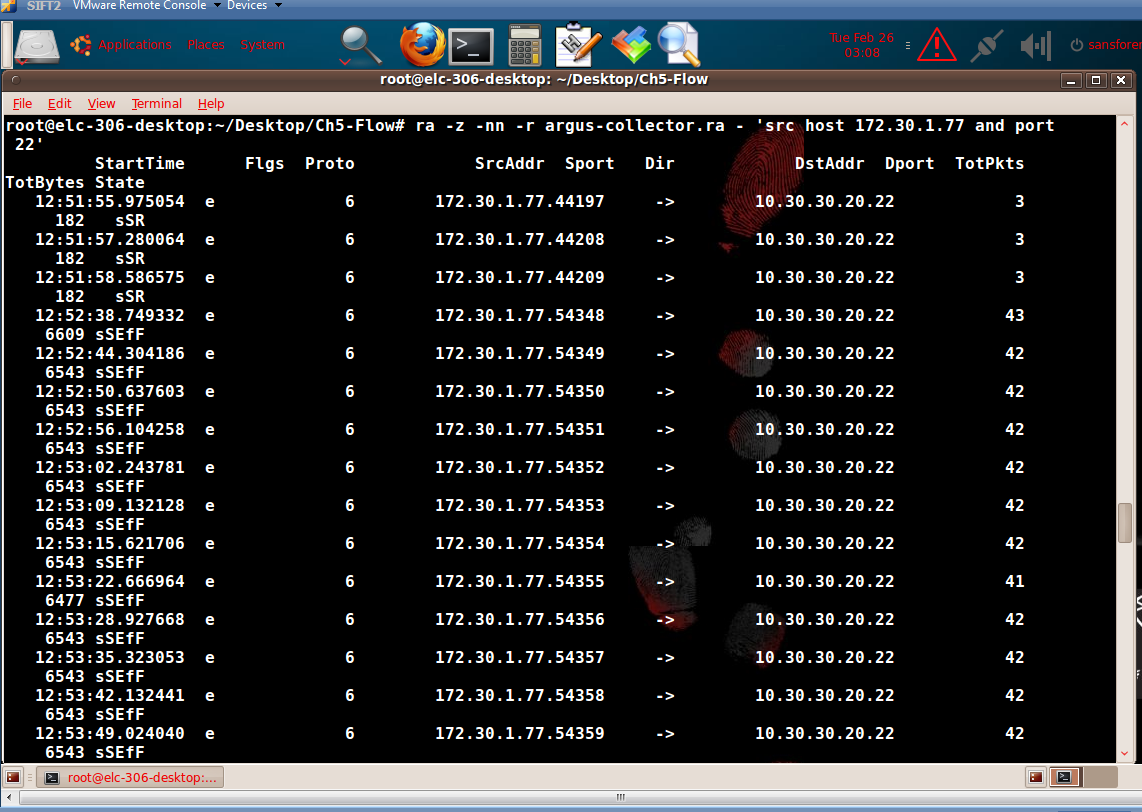


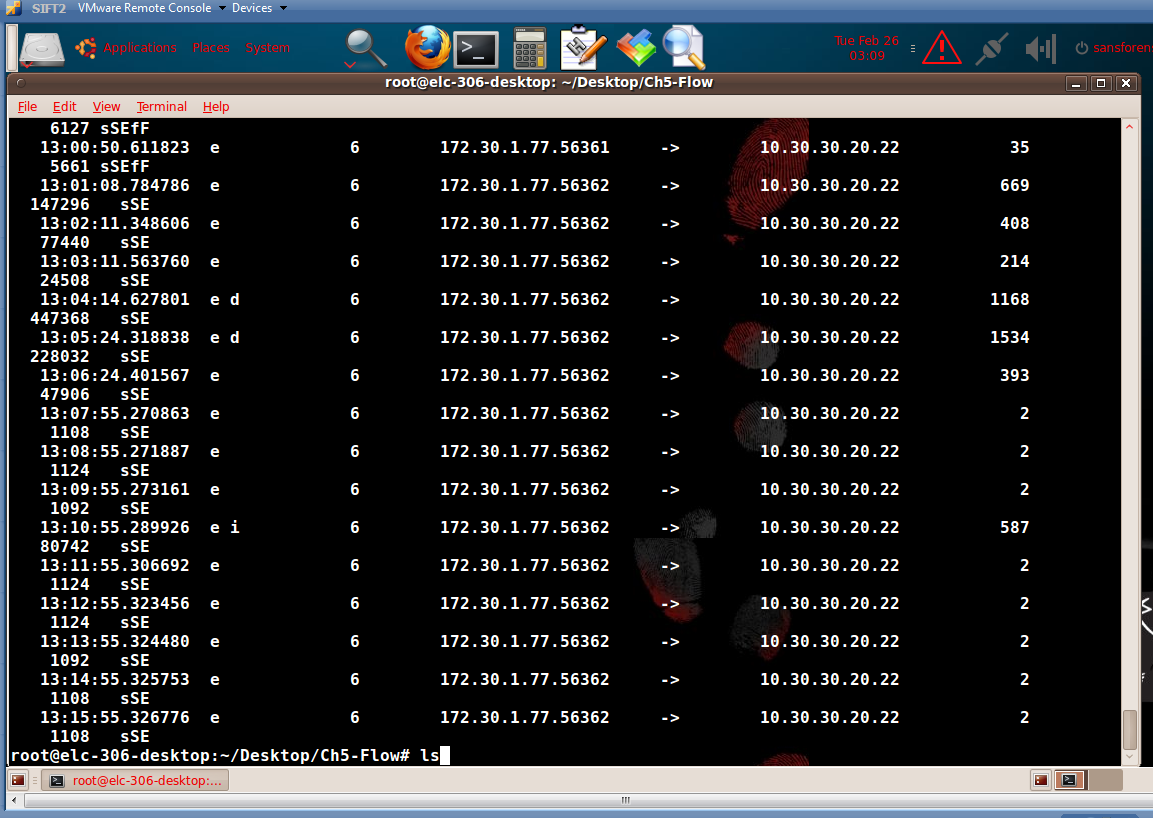




We can see as Mr. X keeps scanning we see the different ports he is scanning through and too rapidly increase. The time Mr X spent was from 04/27/2011 12:49:29 to 04/27/2011 13:15:36, from Port on 44197 to 56362, trying to access the TCP port 22.

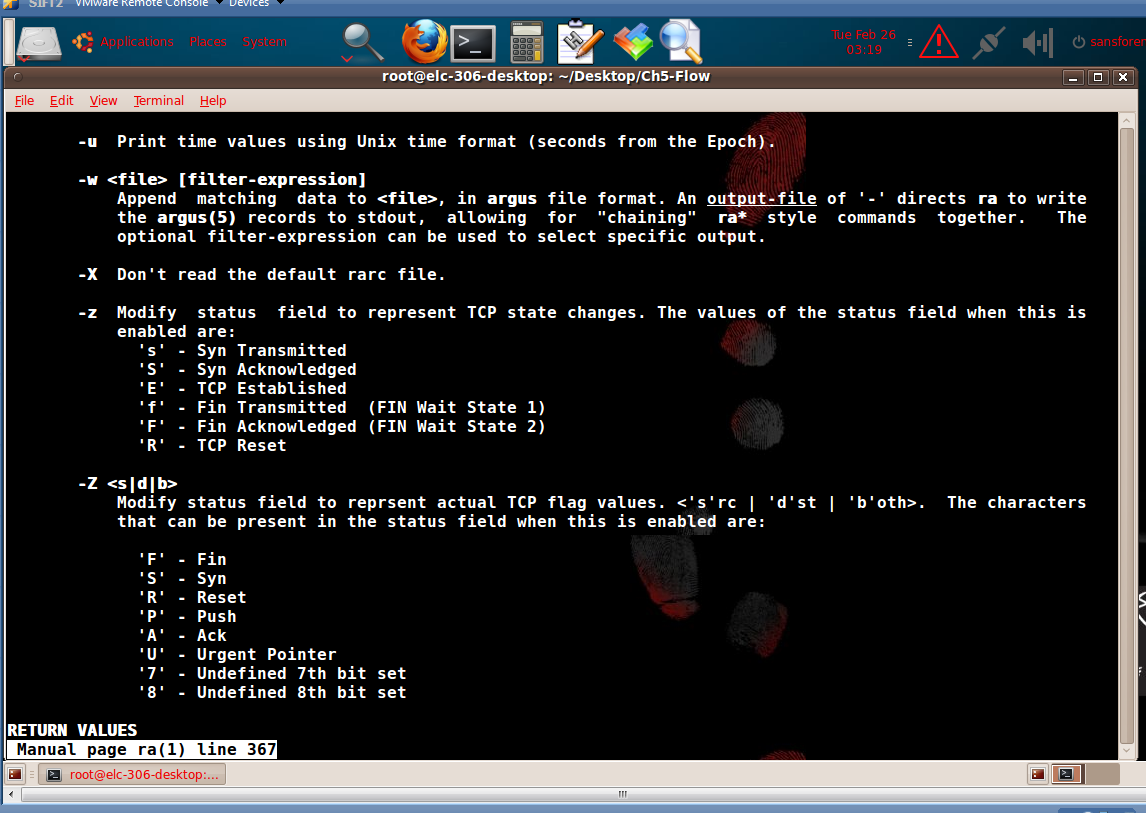
I than analysis the flows using Argus-Collector.ra/Internal Argus Flow and scanned the flows and port tcp 22 for traffic just for the known host IP 172.30.1.77, which we know is Mr. X. I used command line and copied and pasted the results into a text file. Which searches for the specific traffic of the attacker 172.30.1.77 and the TCP 22?





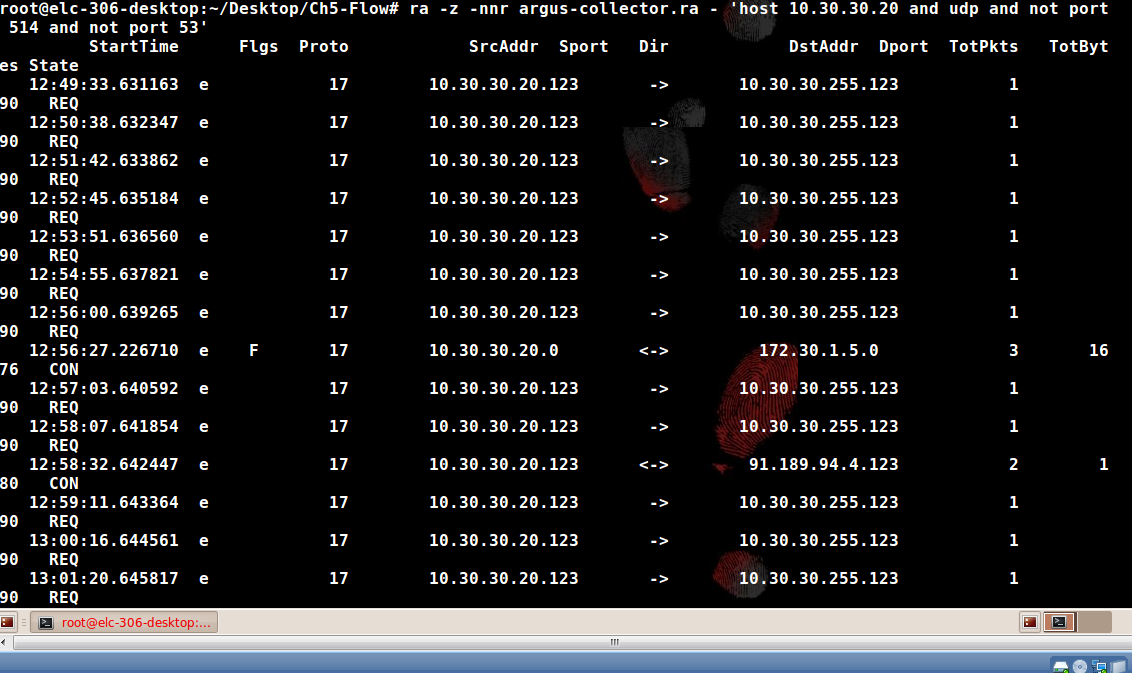
The Destination Address is 10.30.30.20.22. We can see the change of state between sSE and sSEfF, in the TCP Packets. We can see we are getting a lot of sSE States- Syn Transmitted, Syn was Acknowledged, and TCP Established. Also we are seeing a lot of sSEfF States- sSE States- Syn Transmitted, Syn was Acknowledged, TCP Established, Fin transmitted, Fin Acknowledged, and TCP reset.

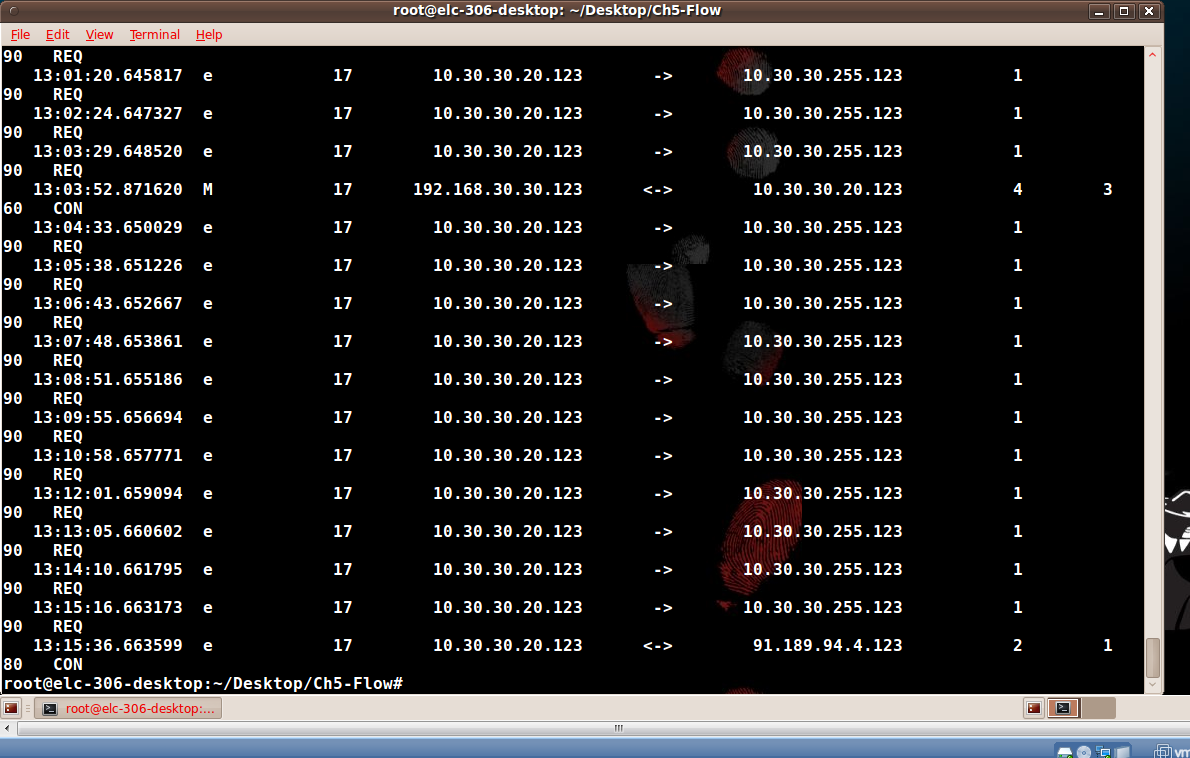
Using the manual to understand the –z command in ra, which can be used as a Modify status field to represent TCP State Change. Looking at the Man ra –z command we can see how a file was received like if it says sSR the Syn Transmitted, Syn was Acknowledged, and TCP reset.



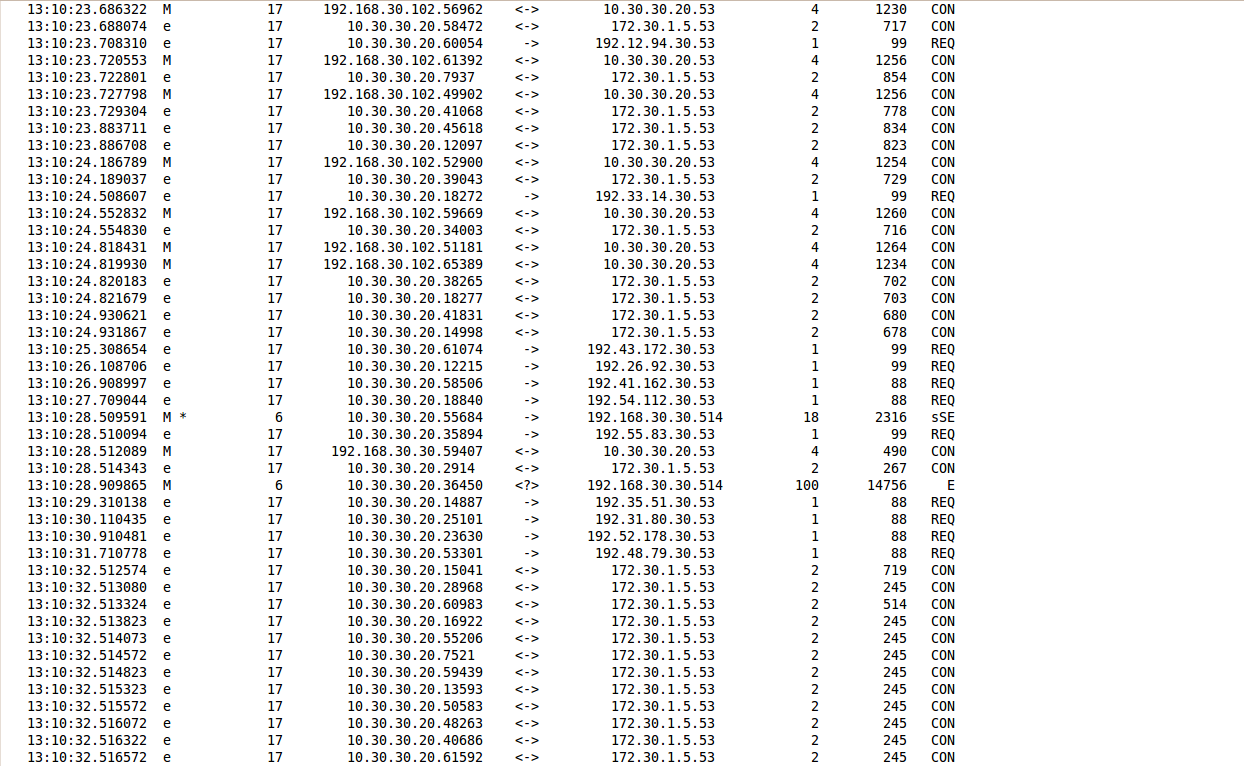
I was unable to get the ra graph to work in SIFT. But the ra graph shows the traffic snippets from 172.30.1.77.

Now, I can do a scan on the targeted host 10.30.30.20 we exclude the udp ports.

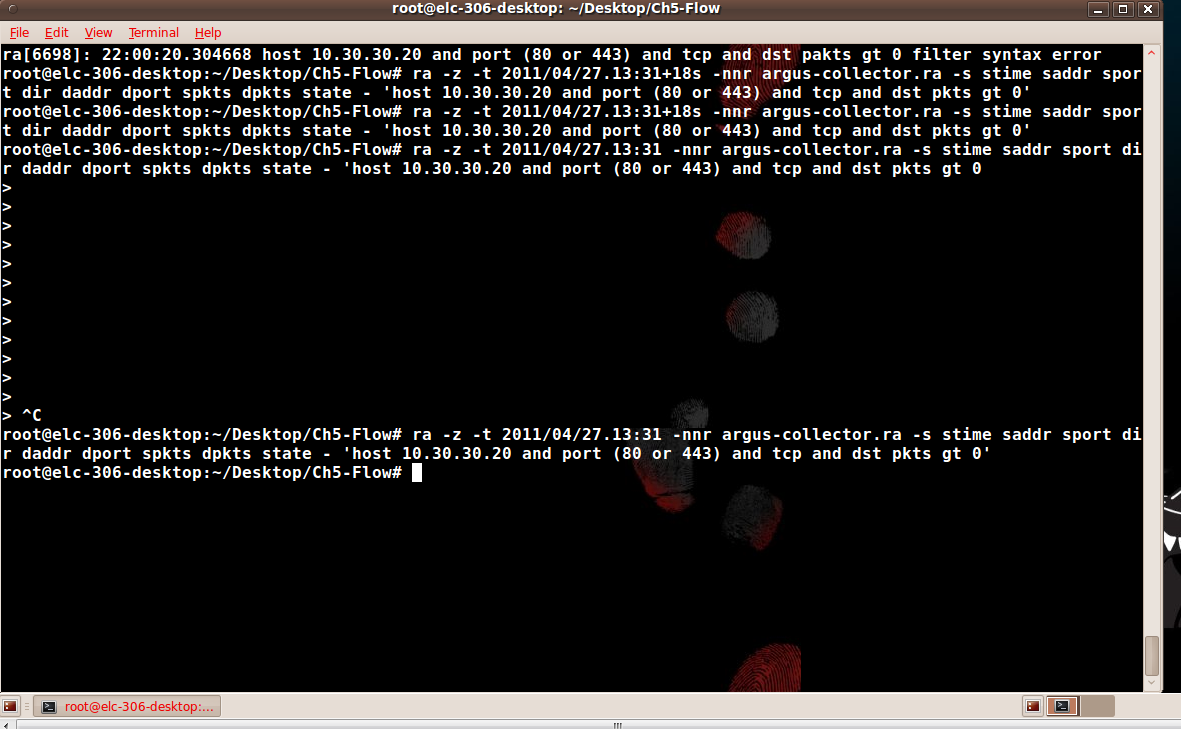




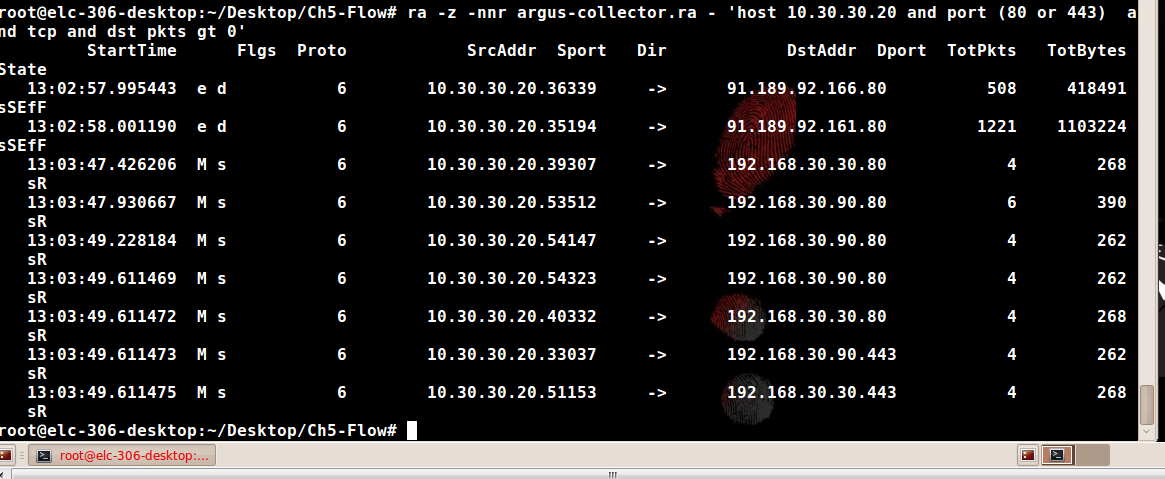
I did a plain host scan after with udp and I got a lot of hits/conversations.



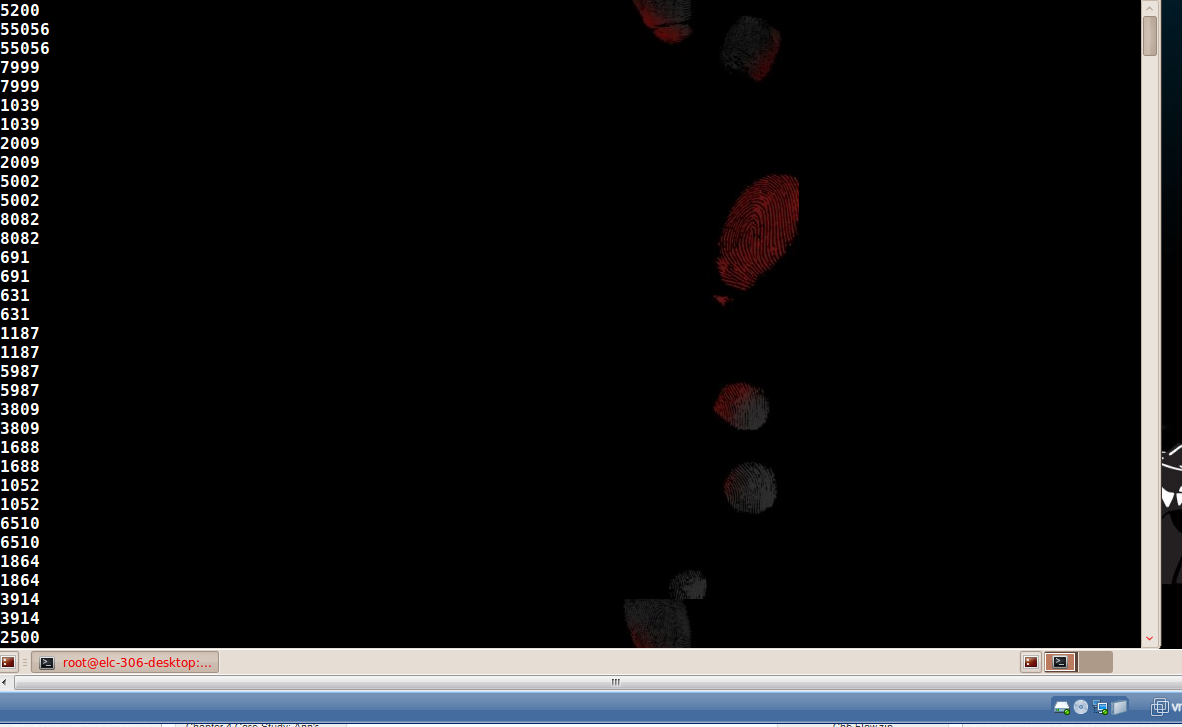
I scanned the flows at 04/27/2011 13:03:31 I didn’t get any hits like the book did, the book shows two hits with a source IP: 10.30.30.20 ports 39307 and 53512, Destination IP 192.168.30.30 and 192.168.30.90 on port 80.



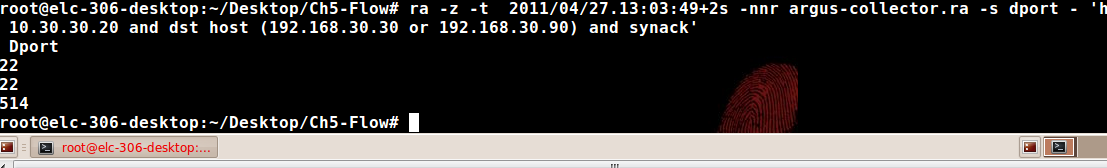
I then took out the –s stime saddr sport dir daddr dport spkts dpkts state and I got some hits/conversations.



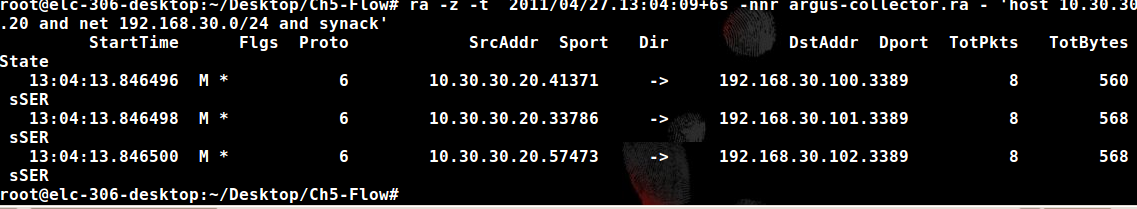
So I then scanned all the ports of the host 10.30.30.20 and the destination host 192.168.30.90 and 192.168.30.30 and got close to a 1000 hits of ports.



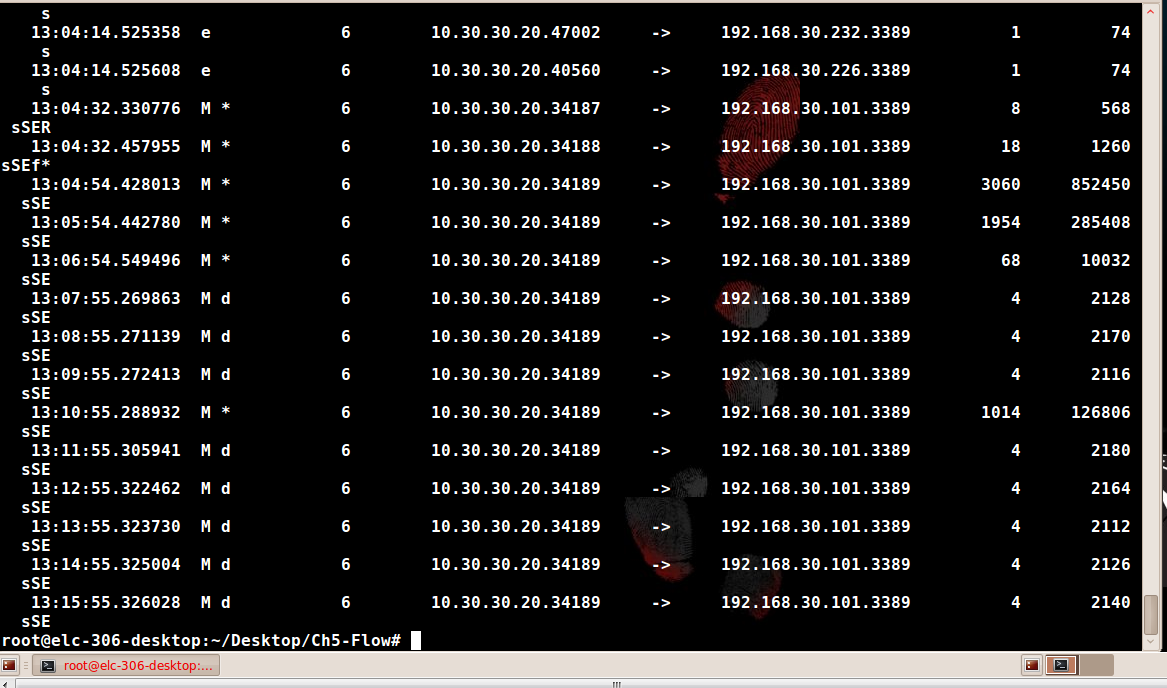
I scanned the ones where acknowledged the syn and only three ports came up. Two 22 tcp ports and one 514 udp port.



Same scan but with the entire network instead of two individual hosts.

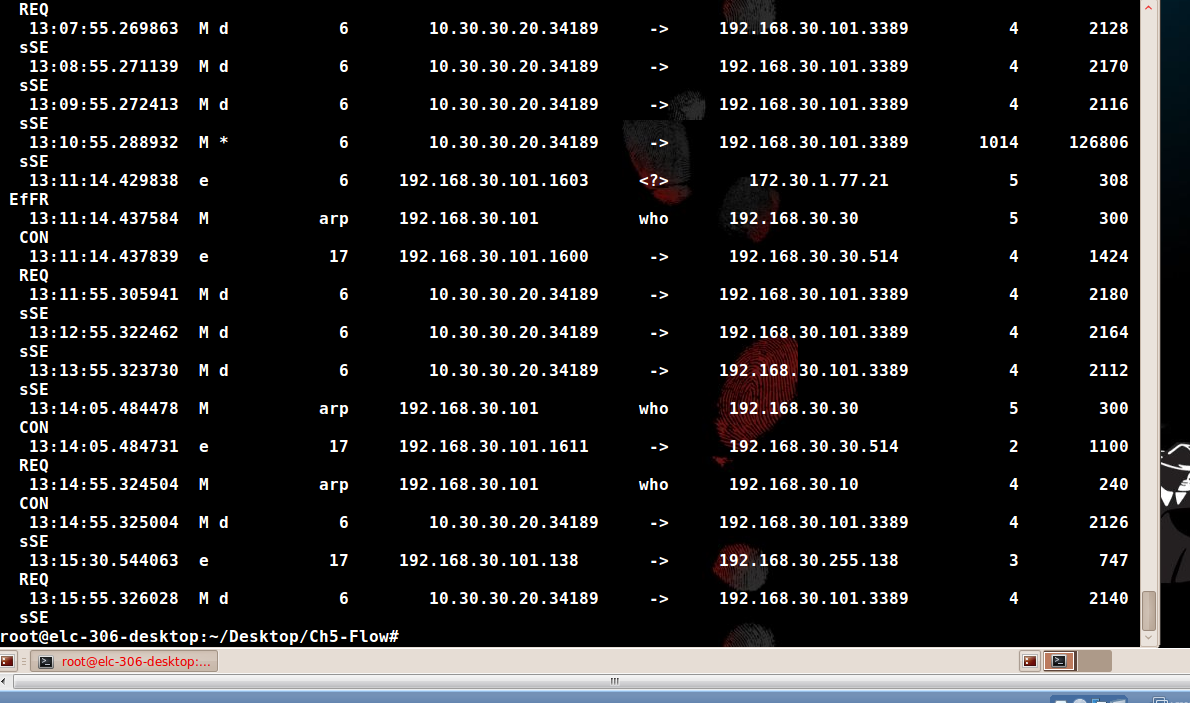


I then scanned host 10.30.30.20 and RDP port 3389.

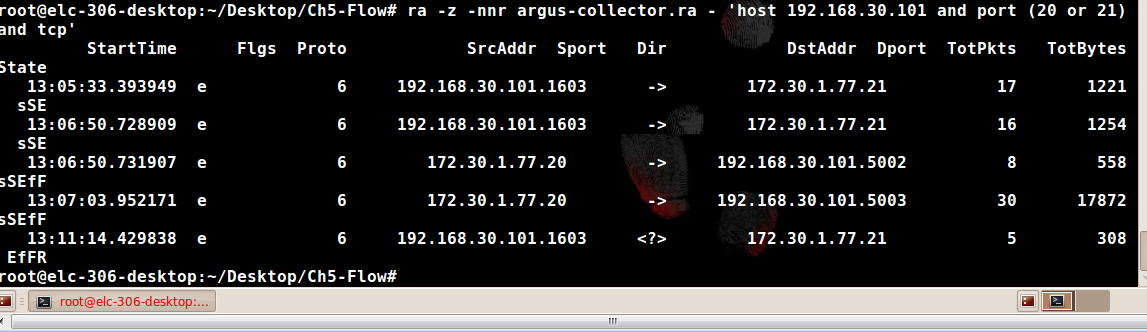


We can now see that 192.168.30.101 was the compromised machine.

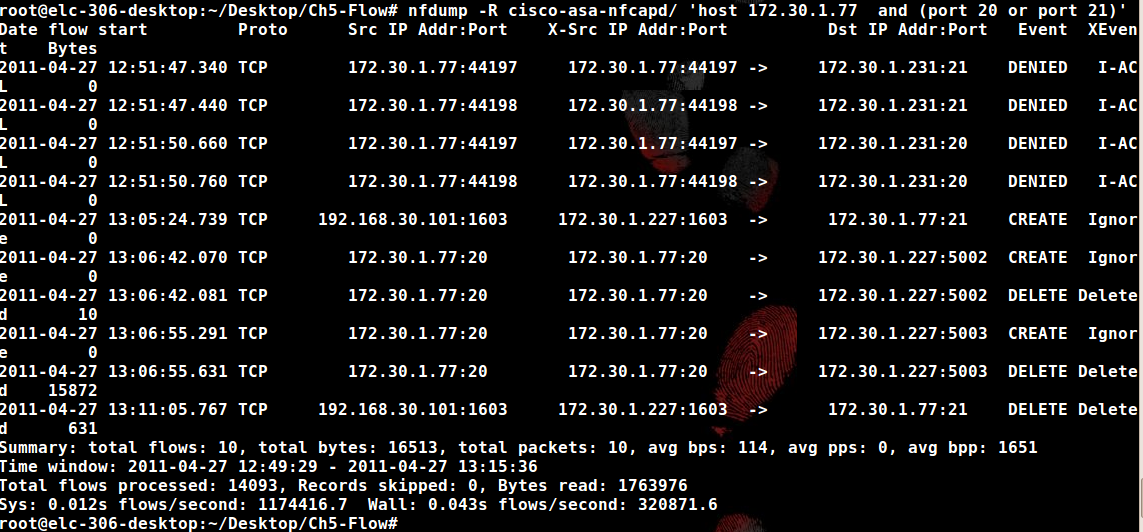
Doing a complete scan of the victim 192.168.30.101 gets us a lot of hits/conversations.



Now scanning the victim and TCP ports including 20 and 21 we get only a few hits/conversations.



And NFDUMP scan on host 172.30.1.77 scanning ports 20 and 21



Examination Details:

1. Identify any compromised systems

172.30.1.31 was compromised through TCP port 22, after gaining access to 172.30.1.31 Mr x uses that system to scan on the internal network to find open ports on the network. Mr x uses 172.30.1.31 to gain access to 192.168.30.101 through port 3389. After connecting to 192.168.30.101 he begins a data transfer to 172.30.1.77 through tcp port 21. so the compromised systems are 172.30.1.31, and 192.168.30.101 through tcp ports 3389, 22, and 21.

1. Determine what the attacker found out about the network architecture

We have a lot of open ports on our network which leads to the ability to steal information.

1. Evaluate the risk of data exfiltration

We can see with this example we have a big risk of data being stolen, through an outward bound FTP connection and open ports on the network. This made it easy for the Attacker to gain our information.

Conclusion:

We can see that the network was compromised by using unused open ports on the network, and one compromised machine was able to access the internal network to get valuable information. I would also like to take a look at the log’s, and analysis the compromised machine to see if there was more information on what mr x did on the network. And what was the 15,879 bytes of information he stole. I would also take the SSH off line. My recommendation is to close all unused ports on the network, and get a flows analyzer like Plixer to analysis the flows on the network so we can better catch and track communications on the network. I mean nfdump and RA Argus are good tools to use after an instant has happened but we need to have real time information about the flows on our network.