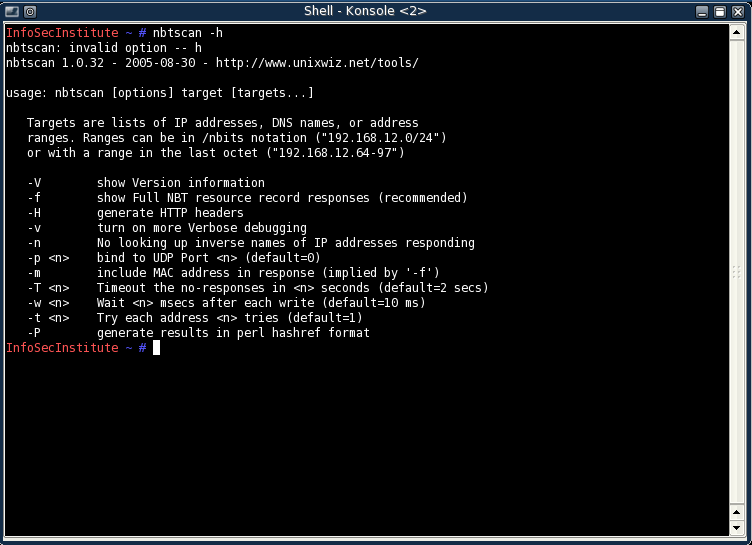
Alexander Cannell

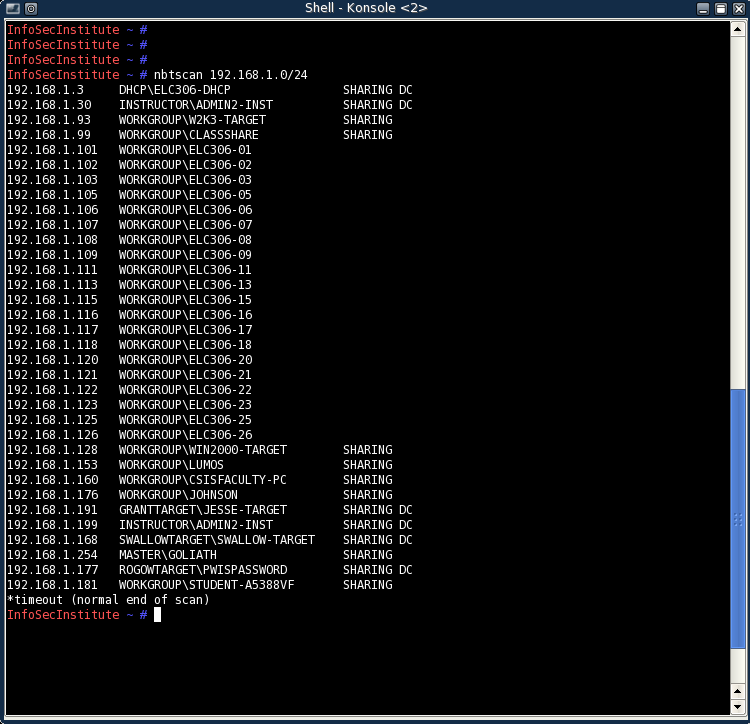
CSIS 3650

Chapter 6 Activities:

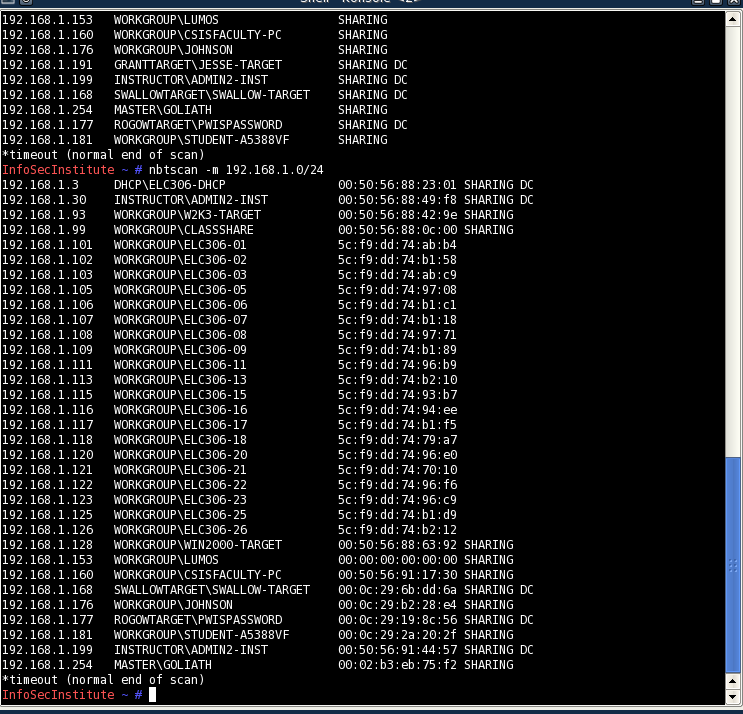
Activity 6-1:



After typing a nbtscan 192.168.1.0/24 which is a full scan.

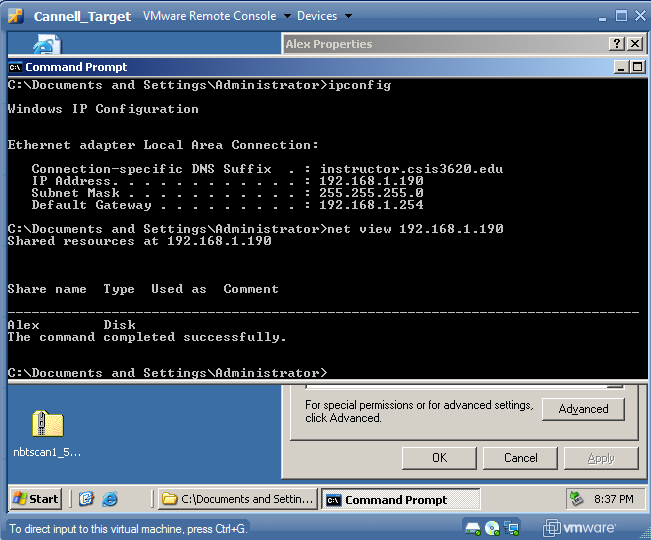


After typing nbtscan -m 192.168.1.0/24, the –m shows all the mac addresses too.

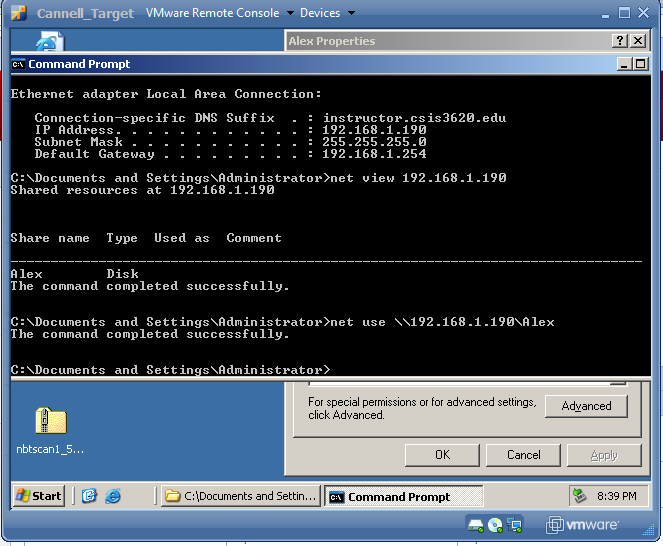


Activity 6-2:

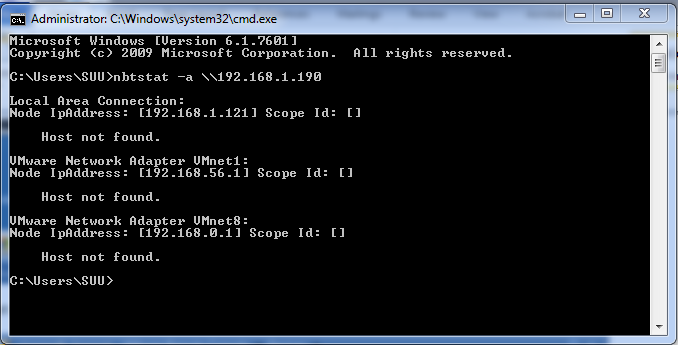
After typing ipconfig and net view \\192.168.1.190



Net use [\\192.168.1.190\Alex](file:///\\192.168.1.190\Alex)

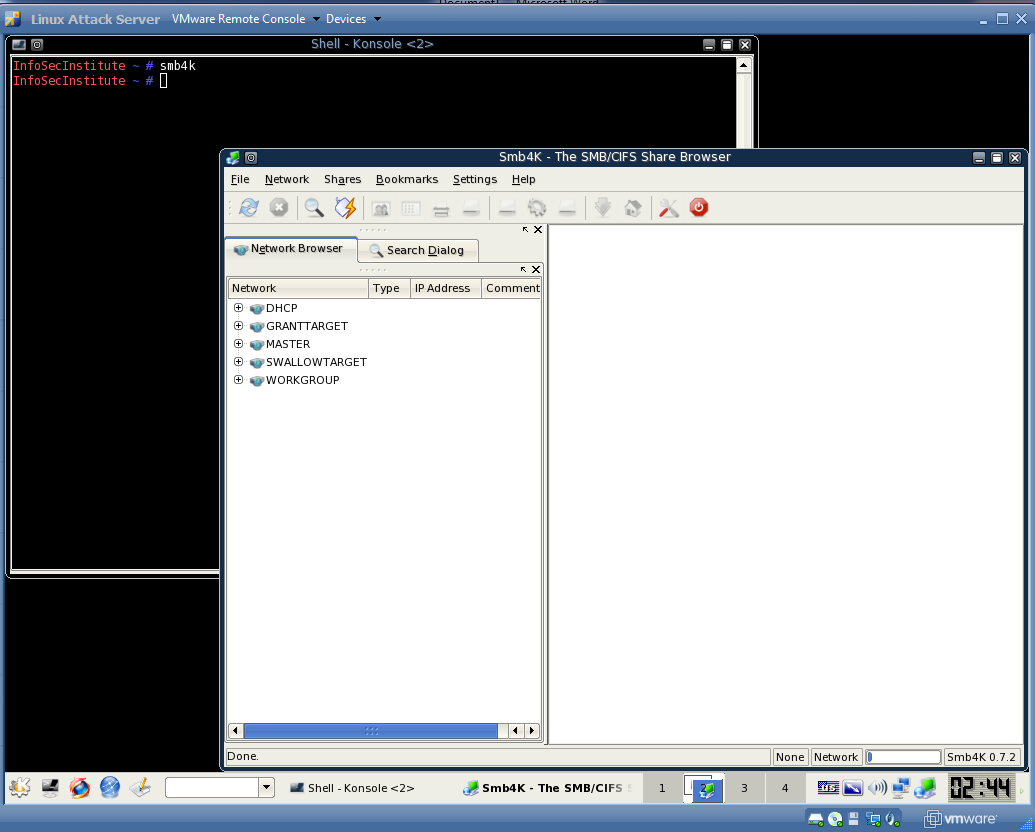


After typing Nbtstat –a [\\192.168.1.190](file:///\\192.168.1.190)

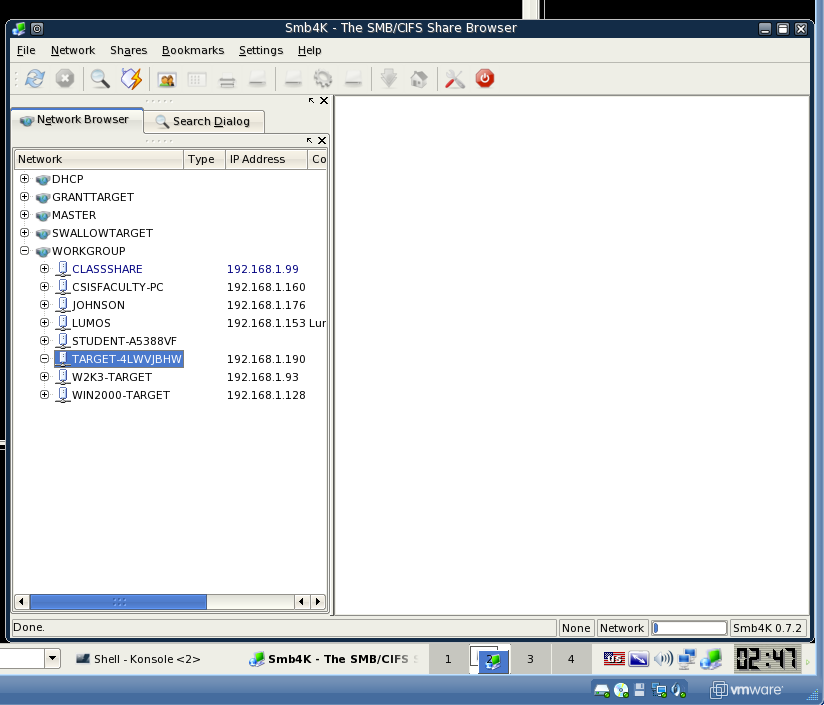


Activity 6-3:

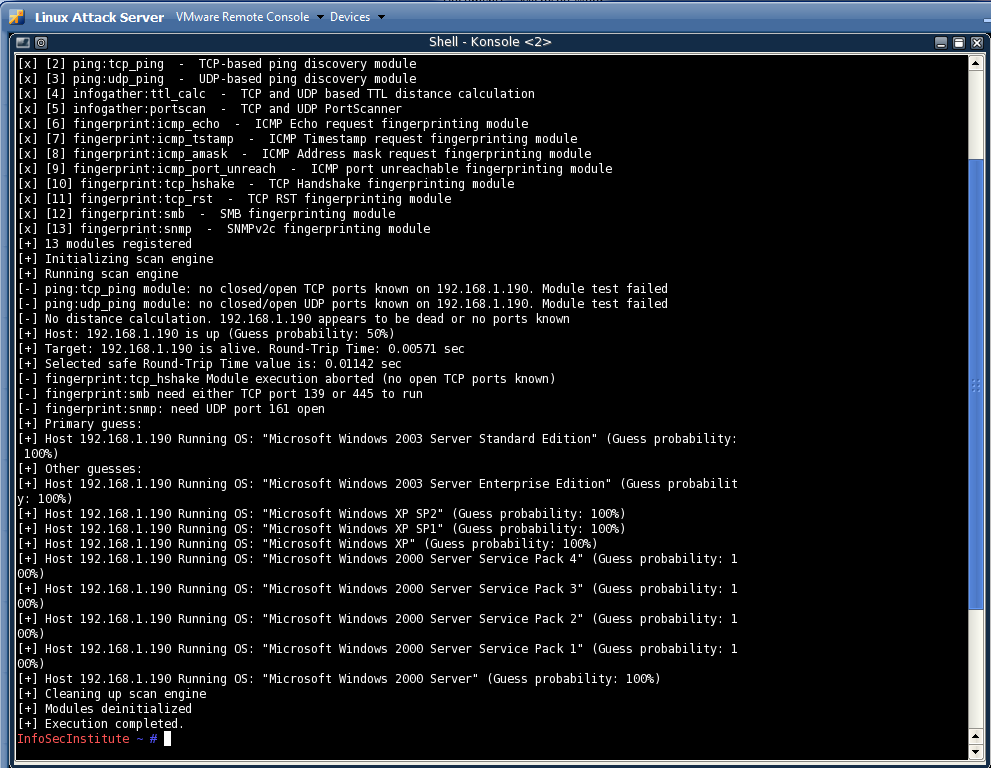
After typing smb4k in linux attack



I couldn’t get print screen to work but you can bring up a window with information on my target server. Like workgroup, ipaddress, host name, and OS on the machine.

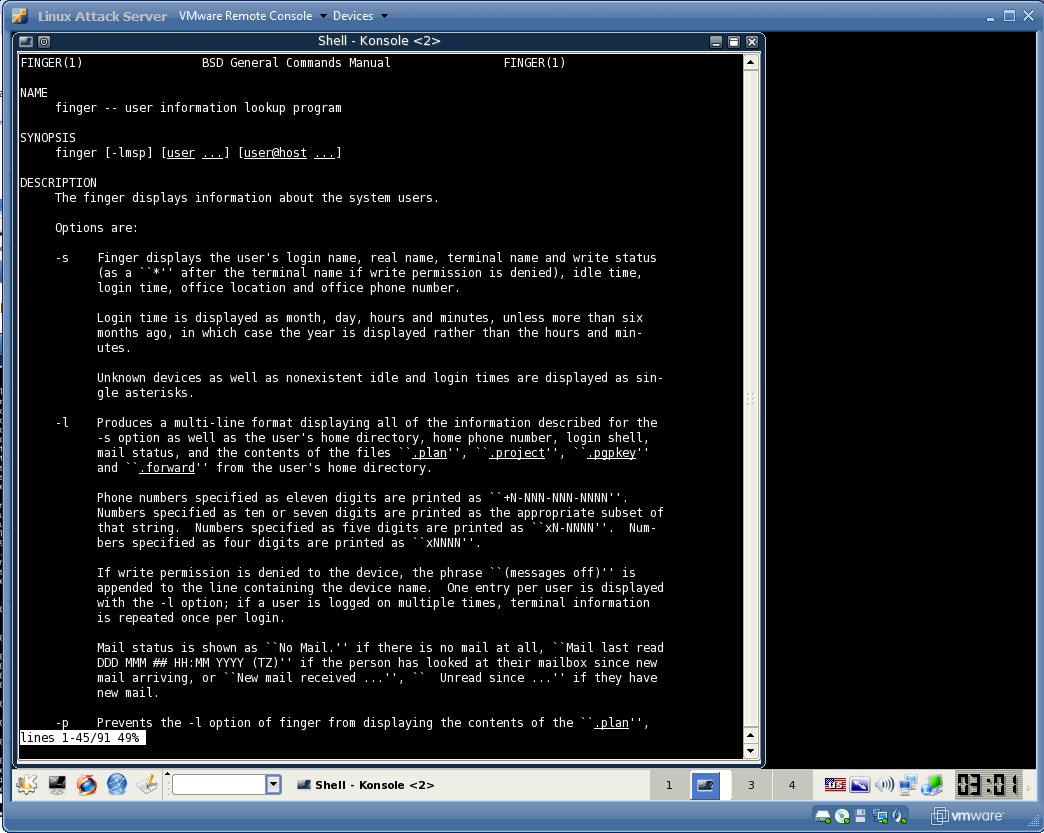


After typing xprobe2 -v 192.168.1.190

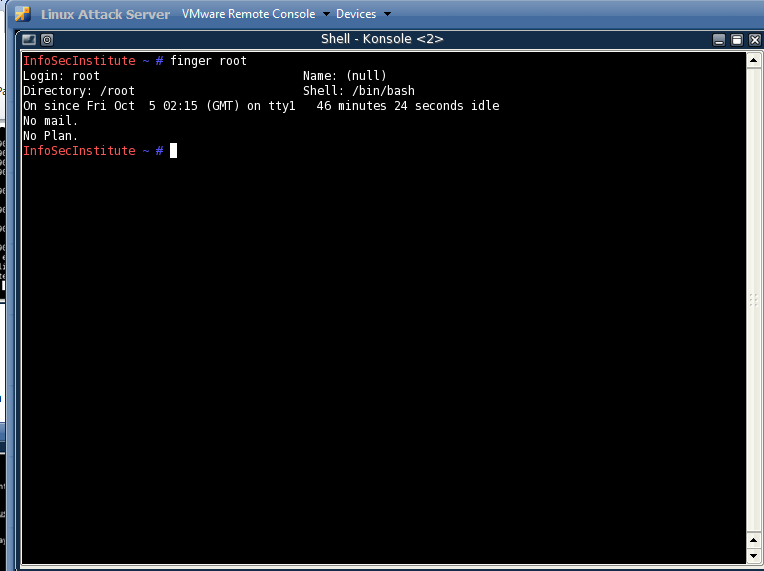


Activity 6-4:

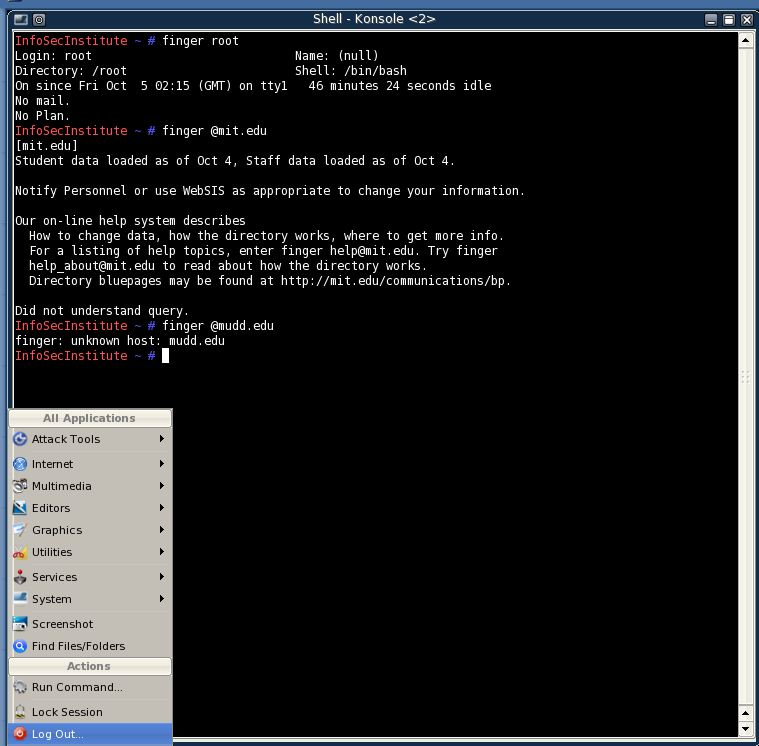
After typing man finger



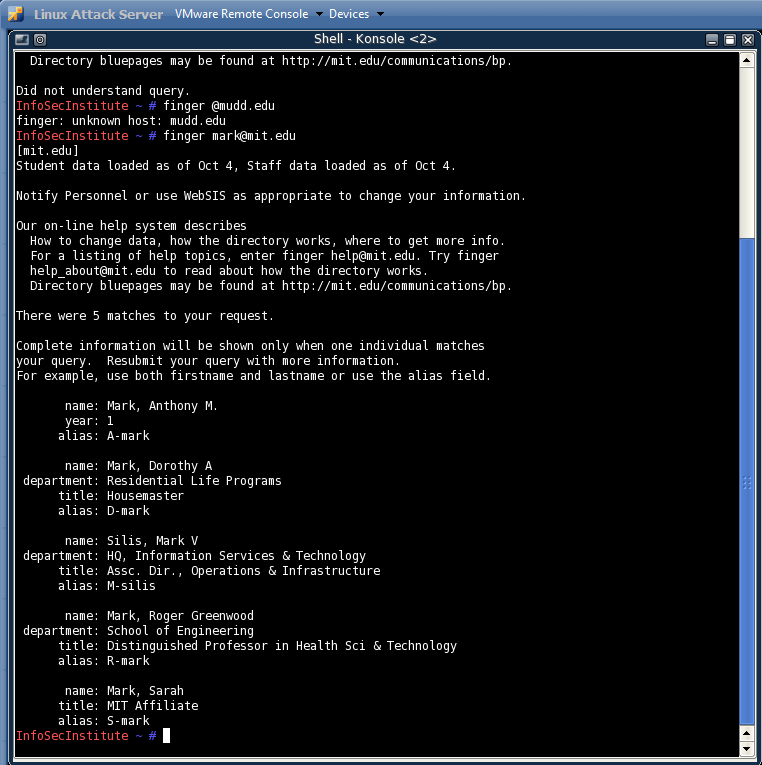
After typing finger root



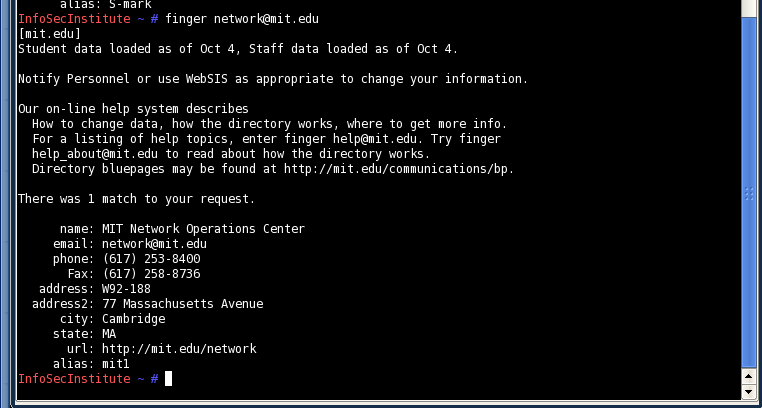
After typing finger @mit.edu



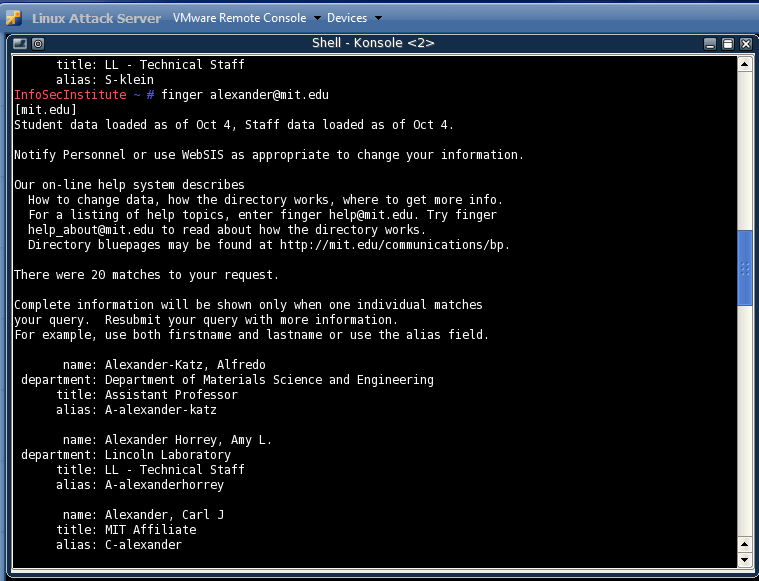
I typed finger [mark@mit.edu](mailto:mark@mit.edu)



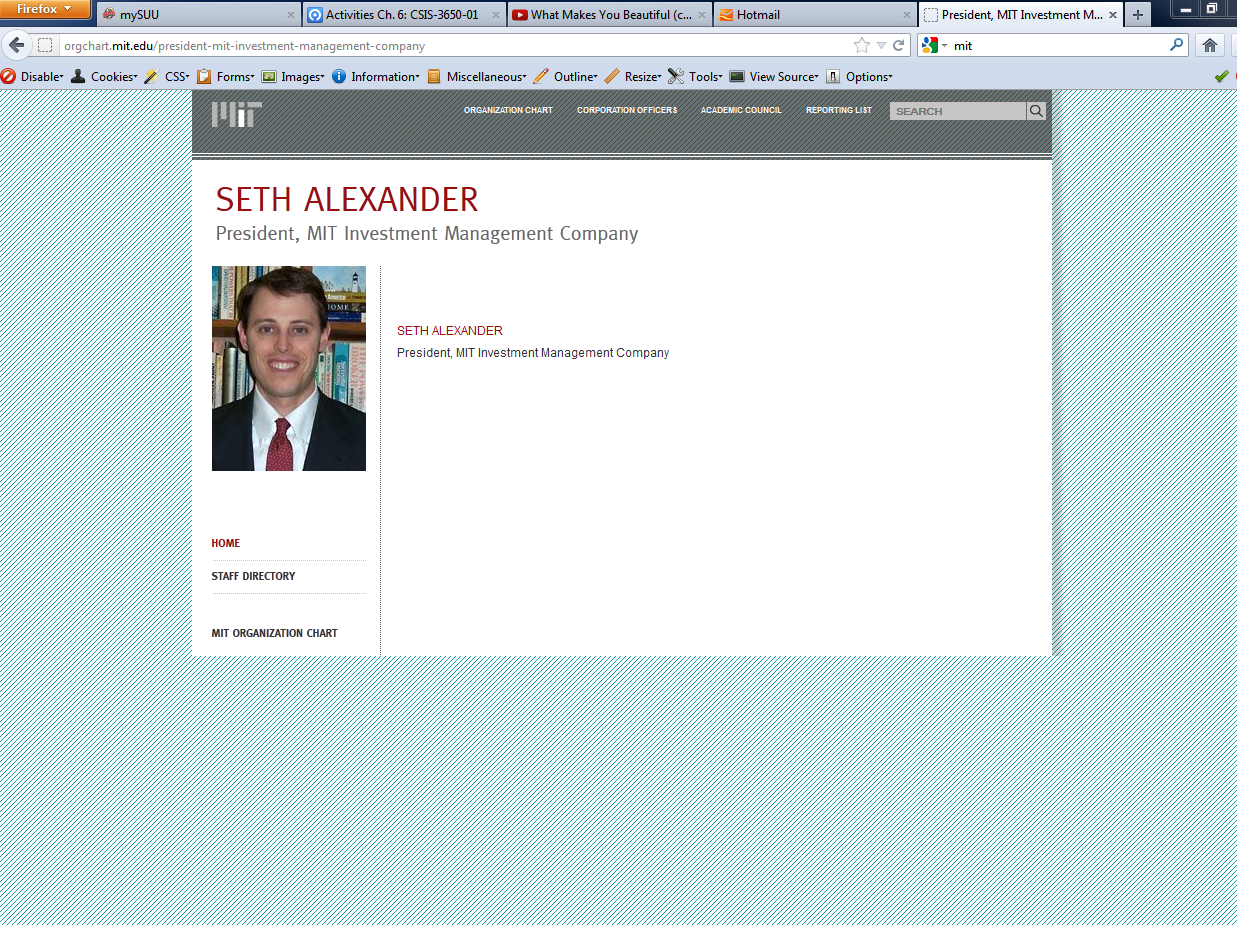
After finger [network@mit.edu](mailto:network@mit.edu)



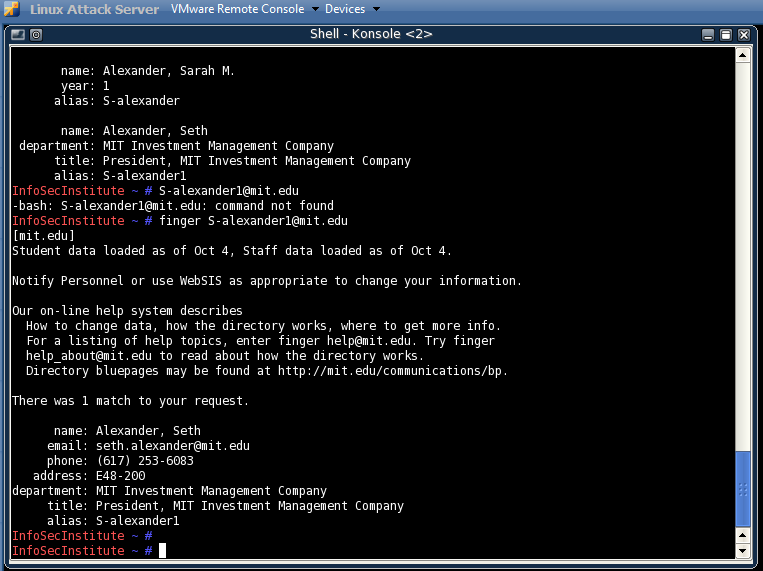
Typing finger [alexander@mit.edu](mailto:alexander@mit.edu) gave me a lot of results.



This is the information I get from seth alexander at mit.edu



After typing finger [S-alexander1@mit.edu](mailto:S-alexander1@mit.edu) we get his phone, email address, department, title, and alias. So using finger tool you can grab a lot of information than from the site.



All these tools are information gathering tools that a hacker could use to use social engineering, physical access, or remote access to get valuable/useful information. As a network security professional it would be good to know these tools so you can better protect against intrusion in your own company.