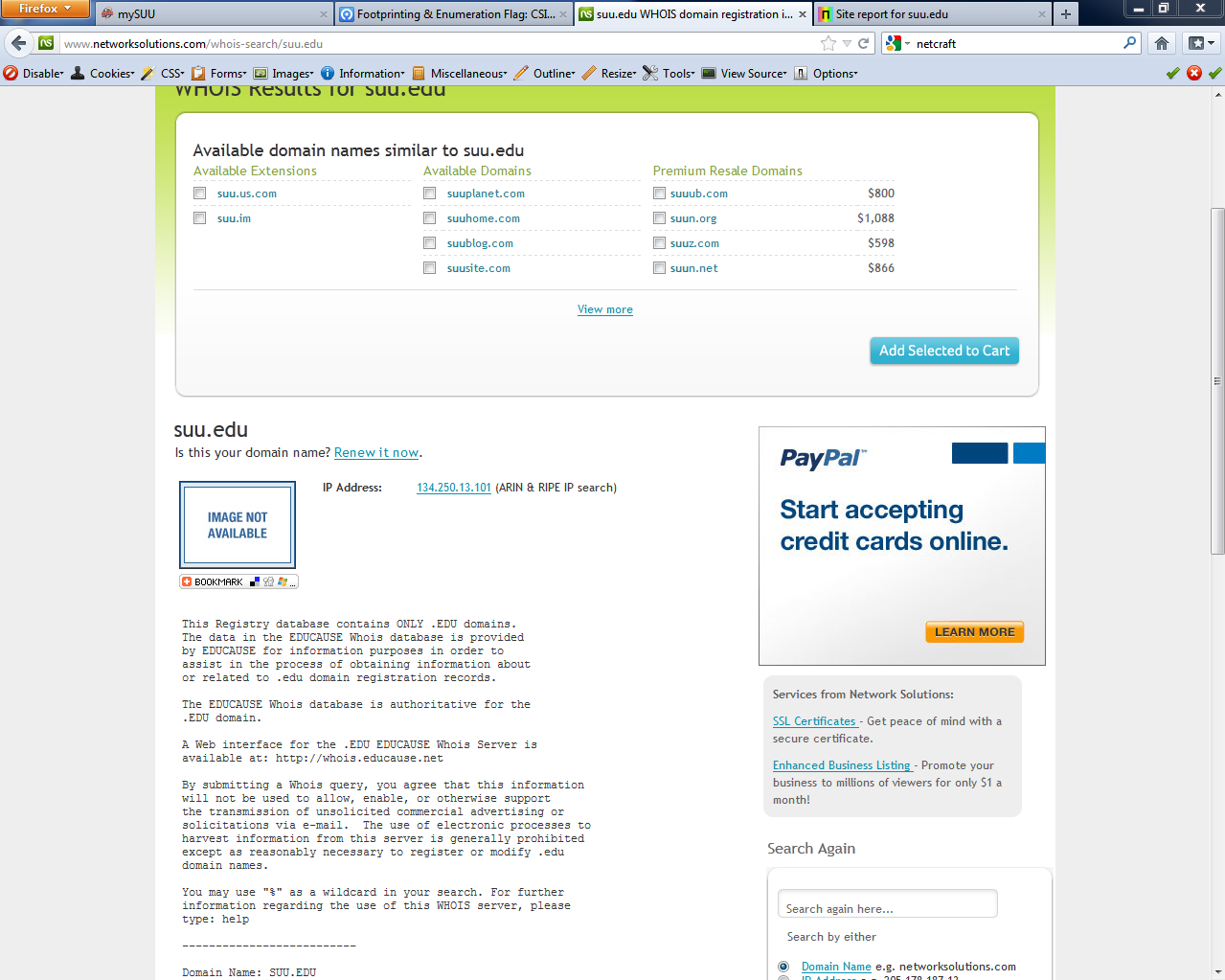
Capture the flag #2: Footprinting and Enumeration

Flag 1

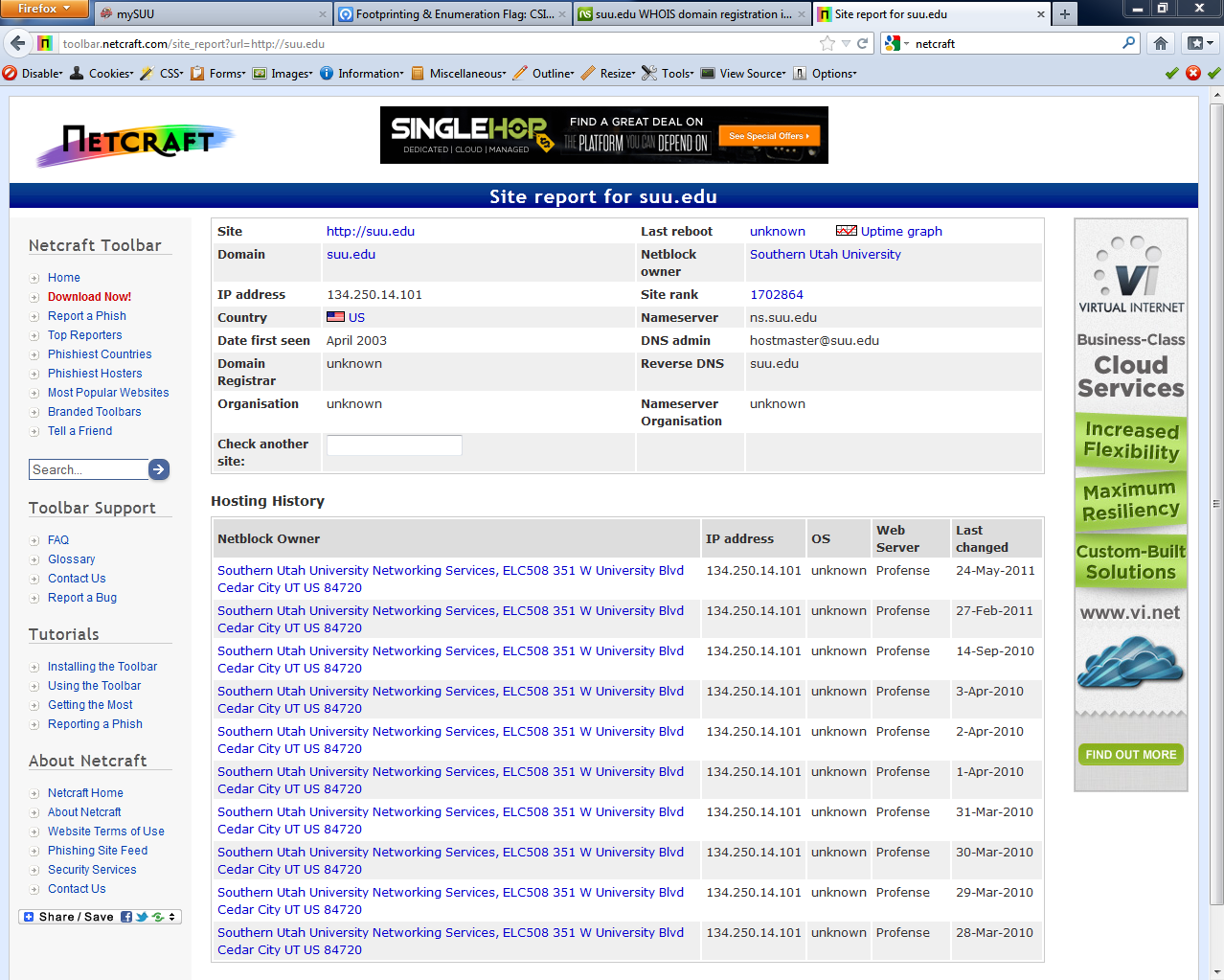
*Instructions: Using only the Internet, find the following information:*

1. What is the IP address of the SUU web server?

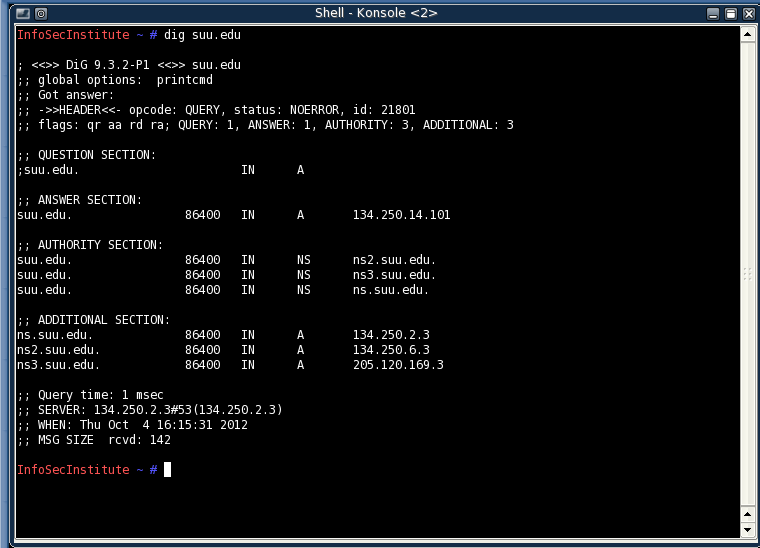
On networksolutions.com – 134.250.12.101



On netcraft.com – 134.250.14.101

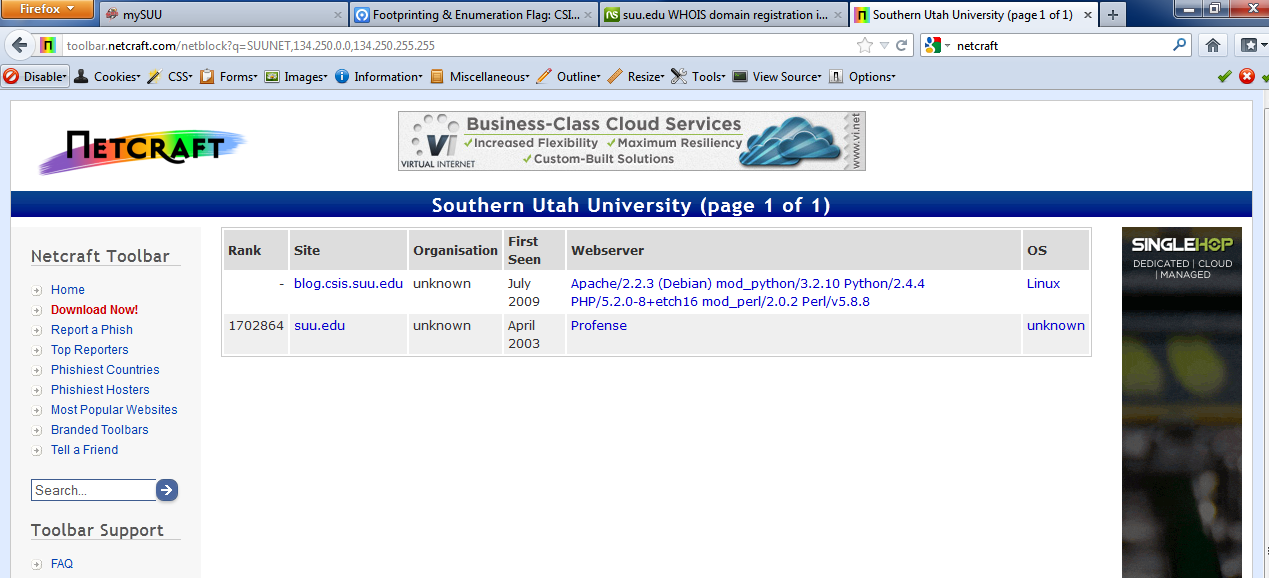


Using the dig tool-134.250.14.101



1. What is the OS running on the SUU web server?

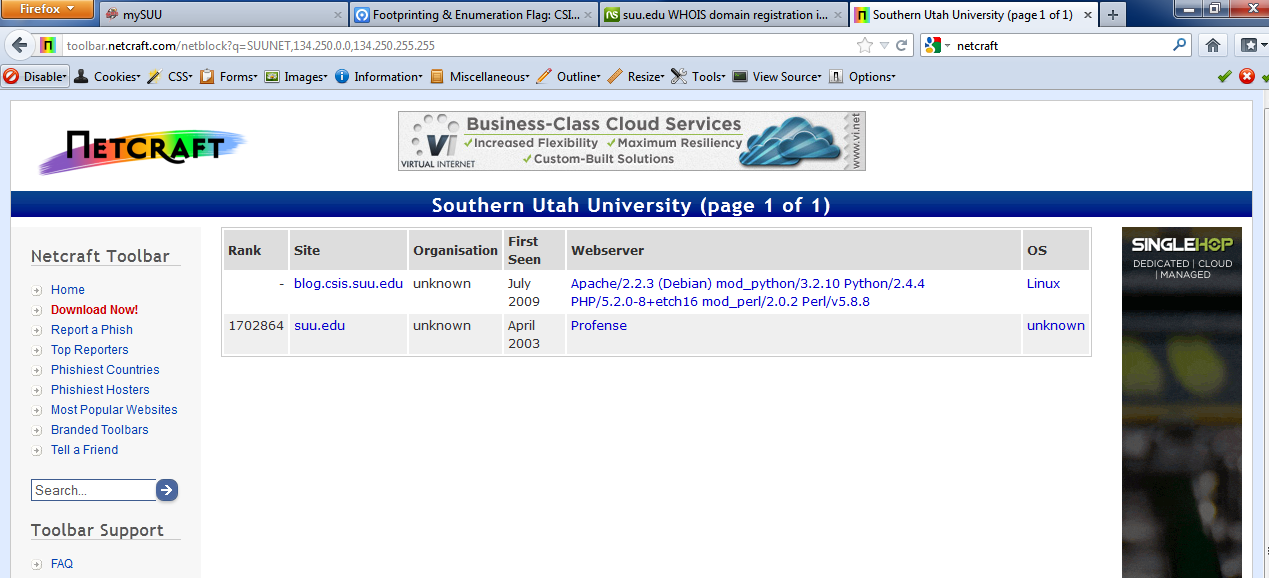
Looks on that ip address 134.250.14.101 a linux



1. What web server is SUU running? (ie. Apache, IIS, etc?)

[Apache/2.2.3 (Debian) mod\_python/3.2.10 Python/2.4.4 PHP/5.2.0-8+etch16 mod\_perl/2.0.2 Perl/v5.8.8](http://uptime.netcraft.com/up/graph?site=blog.csis.suu.edu)

It looks like they are using apache python, php, and perl.

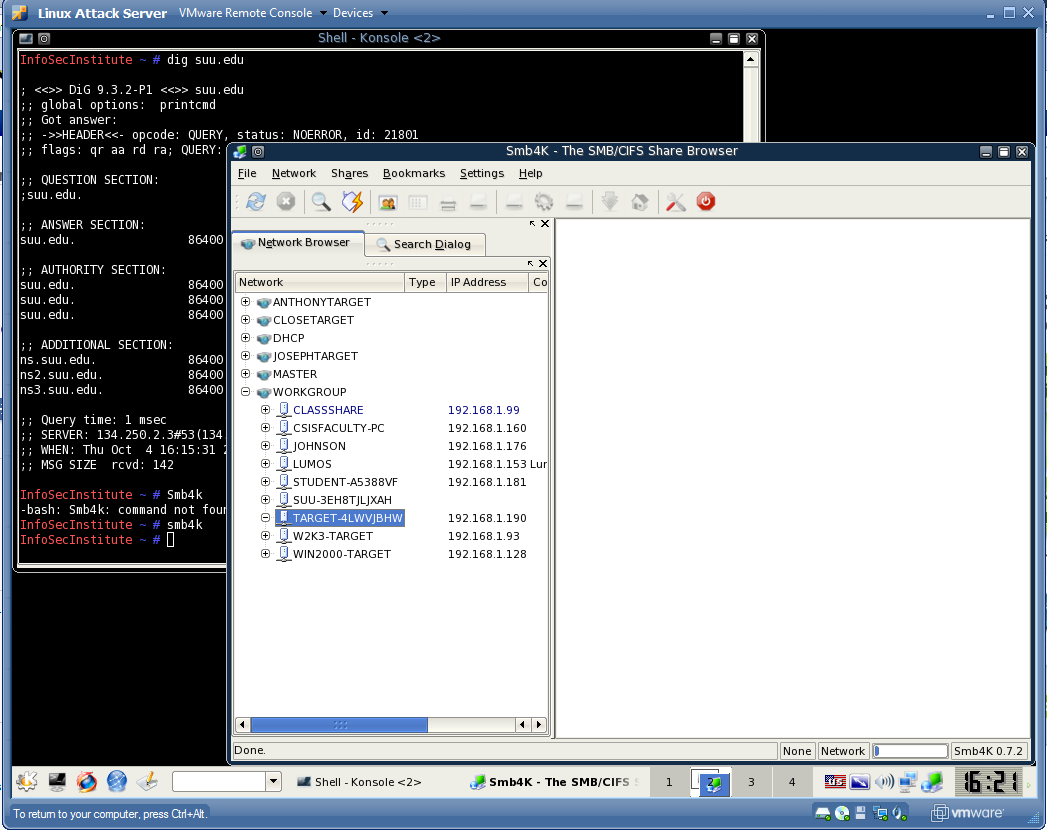


Flag 2

*Instructions: Using the tools from Chapter 6 Activities, gather the following information on your target server.*

1. Shared resources.

Using the smb4k command in linux I was able to bring up the smb/cifs share browser. My target server is 192.168.1.190.



Using nbtscan I found what my target server was sharing.

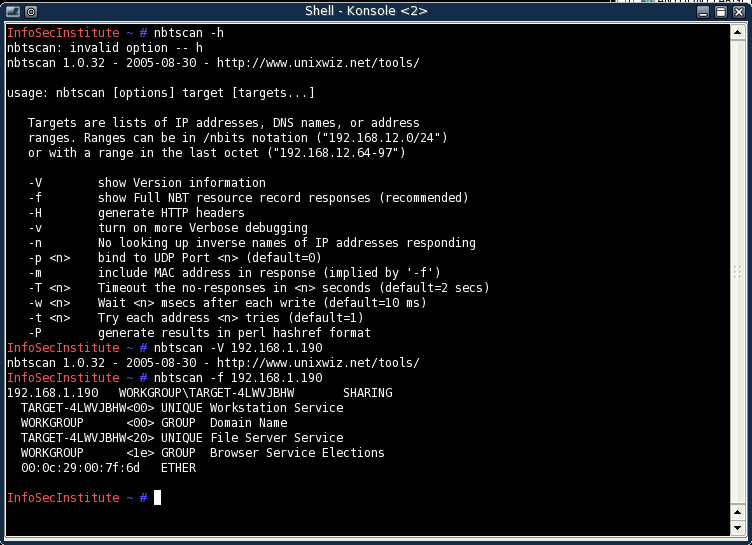
TARGET-4LWVJBHW<00> UNIQUE Workstation Service

WORKGROUP <00> GROUP Domain Name

TARGET-4LWVJBHW<20> UNIQUE File Server Service

WORKGROUP <1e> GROUP Browser Service Elections

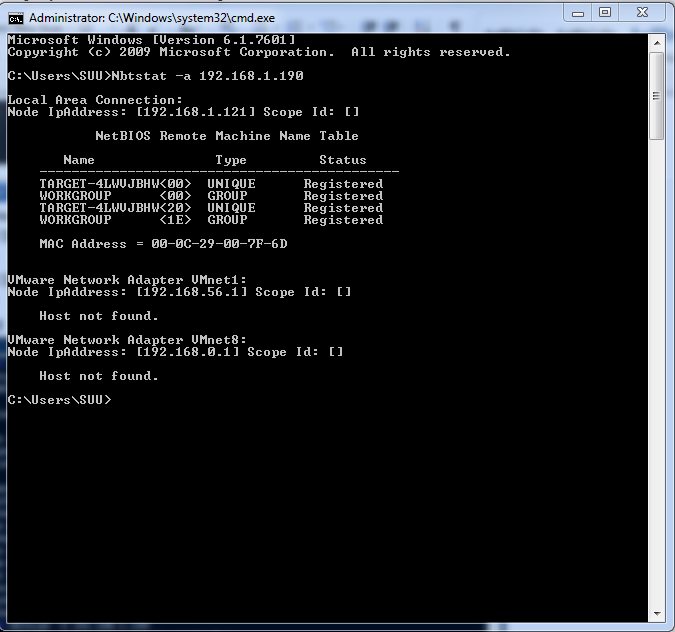
00:0c:29:00:7f:6d ETHER



1. NetBIOS name of your server.

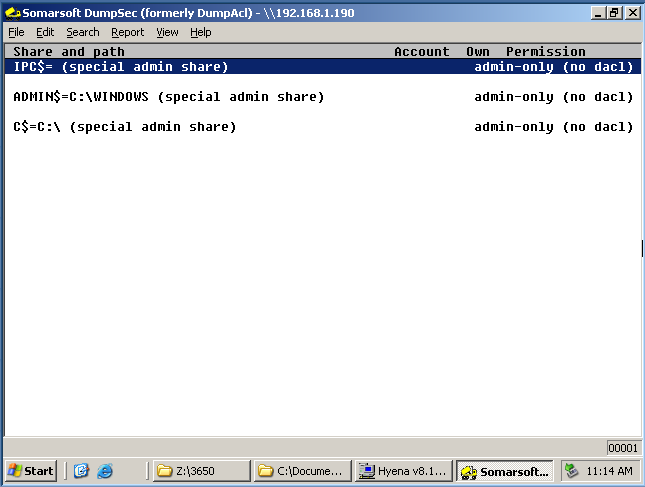
Nbtstat –a 192.168.1.190 the name of my name is TARGET\_4LWVJBHW/192.168.1.190. The workgroup is the domain controller.

Its giving me a node IPAdress and I don’t know what that is, 192.168.1.121

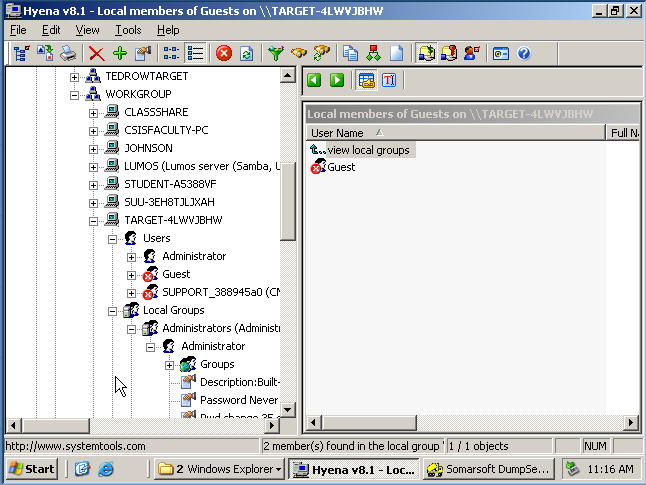


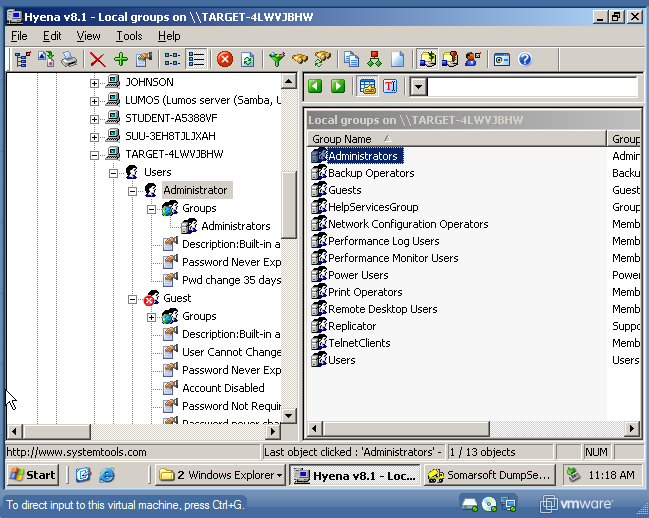
1. Share permissions on your target server.

Using dumpsec you can see who has permissions, and it looks like all my accounts have admin privileges.



Using hydra this is what I get on my target server. The permissions.





You MUST Document your findings. You can do this with screen shots.