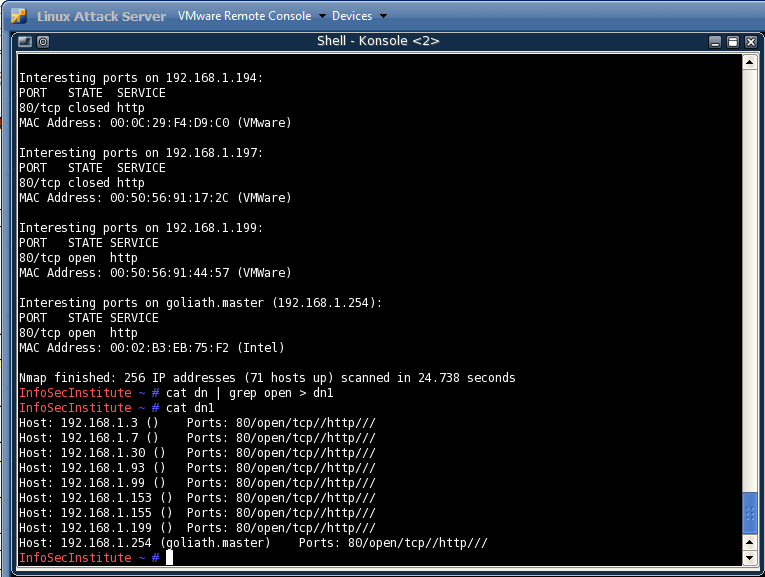
Capture the flag #1: Scanning

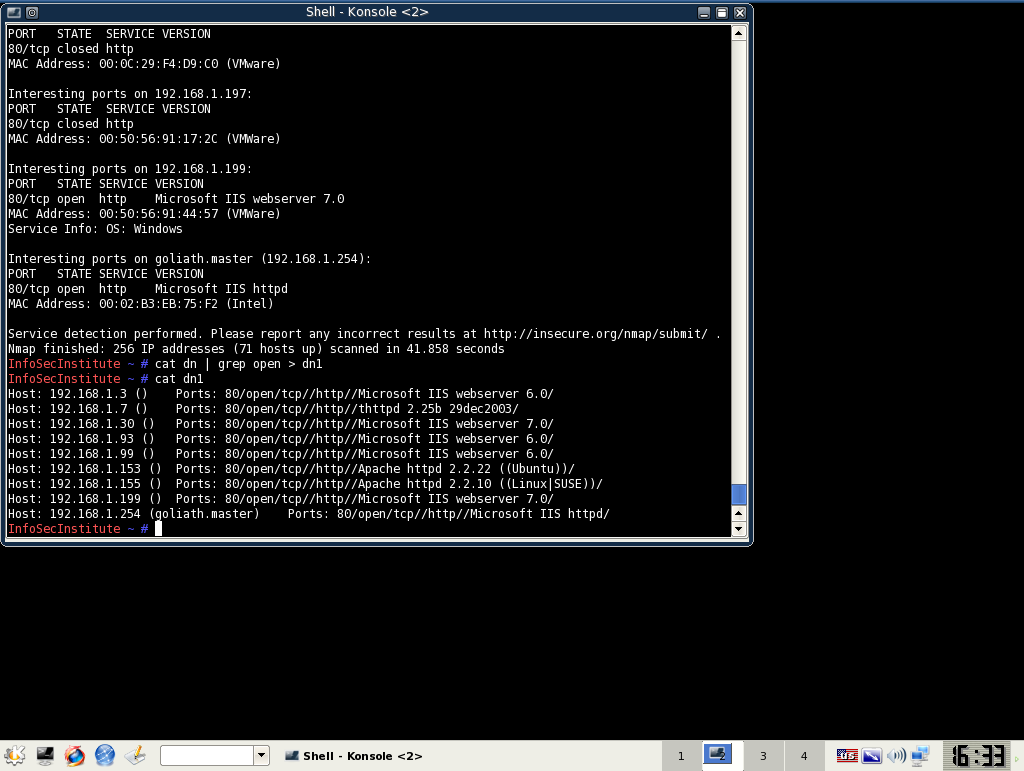
Flag

1. How many web servers are on the class network and what are their IP Addresses?

Nmap –sS –p 80 also using a script



nmap –sV –p80 also using a script

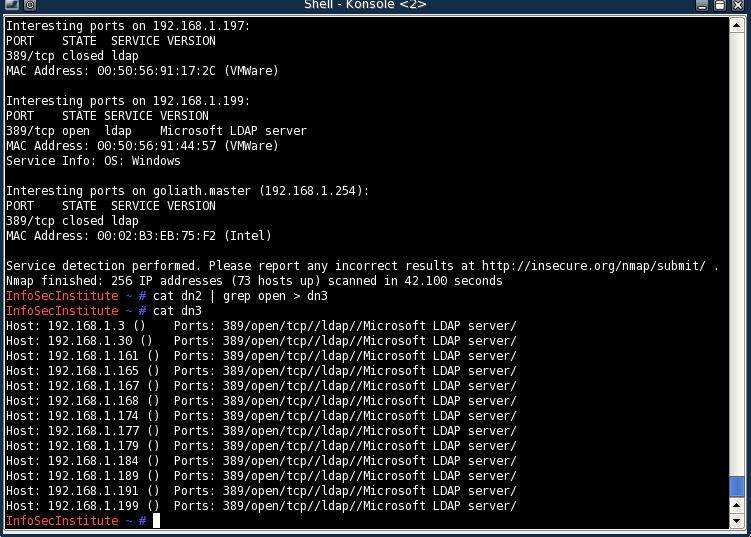


1. Are any servers running Active Directory, if so, what are their IP Addresses? (hint, what does windows use ldap for)

nmap -sV -p 389 192.168.1.0/24 -oG dn2

cat dn2 | grep open > dn3

cat dn3

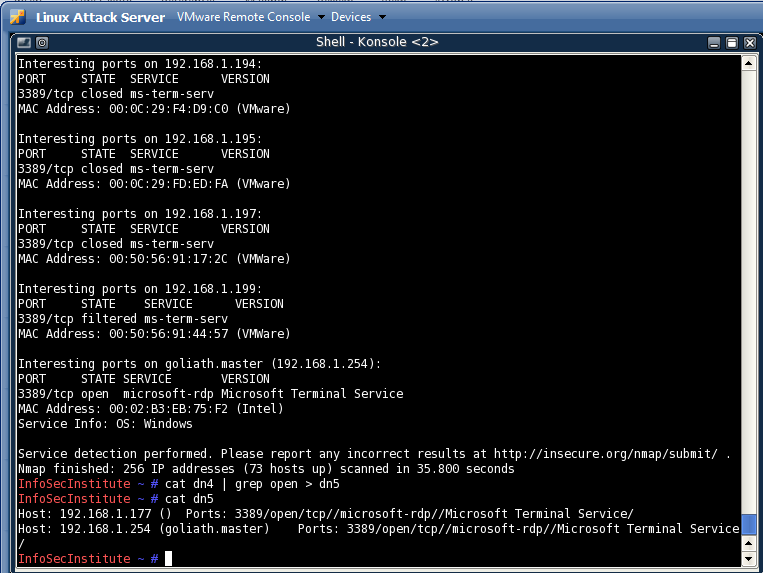


1. Are there any servers which have RDP (remote desktop protocol enabled), if so, what are their IP Addresses?

nmap -sV -p 3389 192.168.1.0/24 -oG dn4

cat dn4 | grep open > dn5

cat dn5

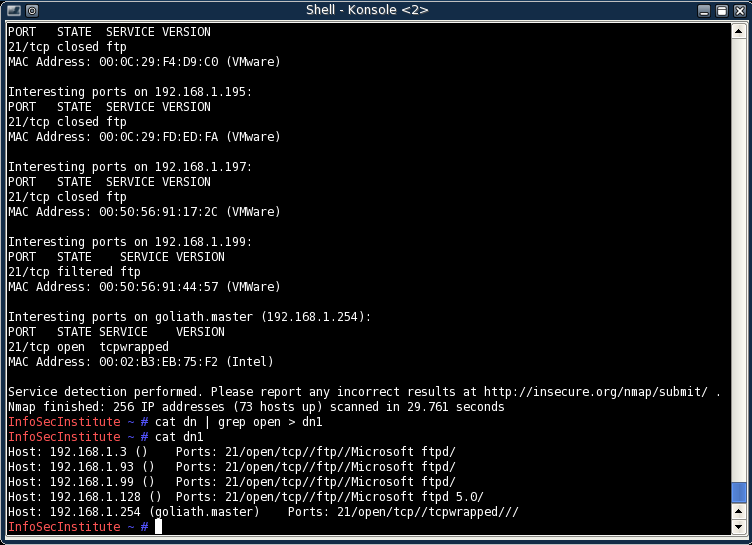


1. Where are the FTP servers what are their IP Addresses?

nmap -sV -p 21 192.168.1.0/24 -oG dn1

cat dn | grep open > dn1

cat dn1



1. What are the FTP server versions/vendor? (not the OS version)

Host: 192.168.1.128 () Ports: 21/open/tcp//ftp//Microsoft ftpd 5.0/

Microsoft ftpd

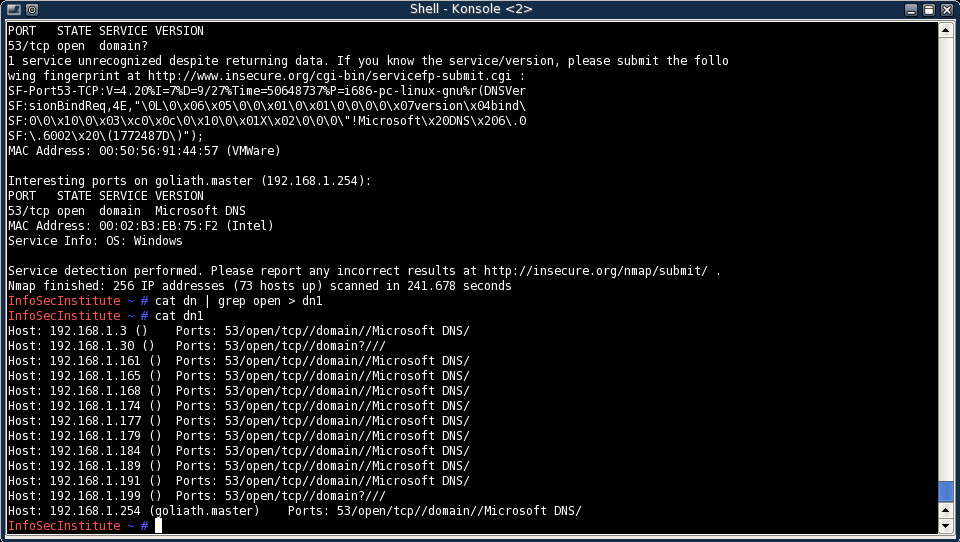
Microsoft ftpd 5.0

1. How many computers are running DNS and what are their IP Addresses?

nmap -sV -p 53 192.168.1.0/24 -oG dn1

cat dn | grep open > dn1

cat dn1



1. Where is the ipad? (what is it’s IP)?

An unique port for the IPad is 62078

(on a wireless network)

nmap -sV -p 62078 192.168.1.0/24 -oG dn1

cat dn | grep open > dn1

cat dn1

192.168.1.60

1. Are there any servers on the network running Windows 2000, if so, what are their IP Addresses? (remember port 445 is always open on Windows Server computers)

nmap -sV -p 53 192.168.1.0/24 -oG dn1

cat dn | grep open > dn1

cat dn1

