Last updated 10/10/2017

Rich's lesson module checklist

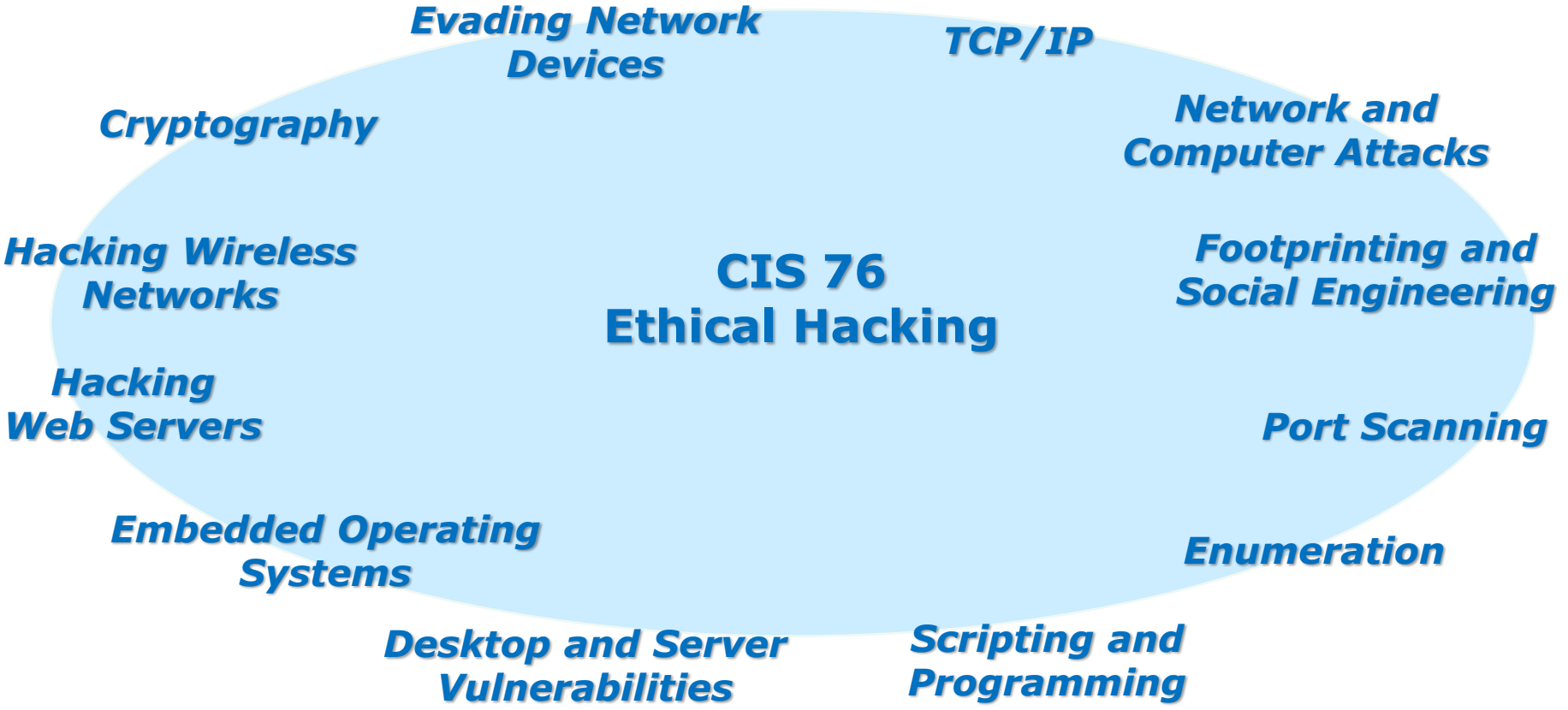
- ❑ Slides and lab posted
- ❑ WB converted from PowerPoint
- ❑ Print out agenda slide and annotate page numbers

- ❑ Flash cards
- ❑ Properties
- ❑ Page numbers
- ❑ 1st minute quiz
- ❑ Web Calendar summary
- ❑ Web book pages
- ❑ Commands

- ❑ Various Windows VMs created and available for enumeration
- ❑ Add CIS 76 students to Whitehats domain
- ❑ Lab 6 posted and tested

- ❑ Backup slides, whiteboard slides, CCC info, handouts on flash drive
- ❑ Spare 9v battery for mic
- ❑ Key card for classroom door

- ❑ Update CCC Confer and 3C Media portals



Student Learner Outcomes

1. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

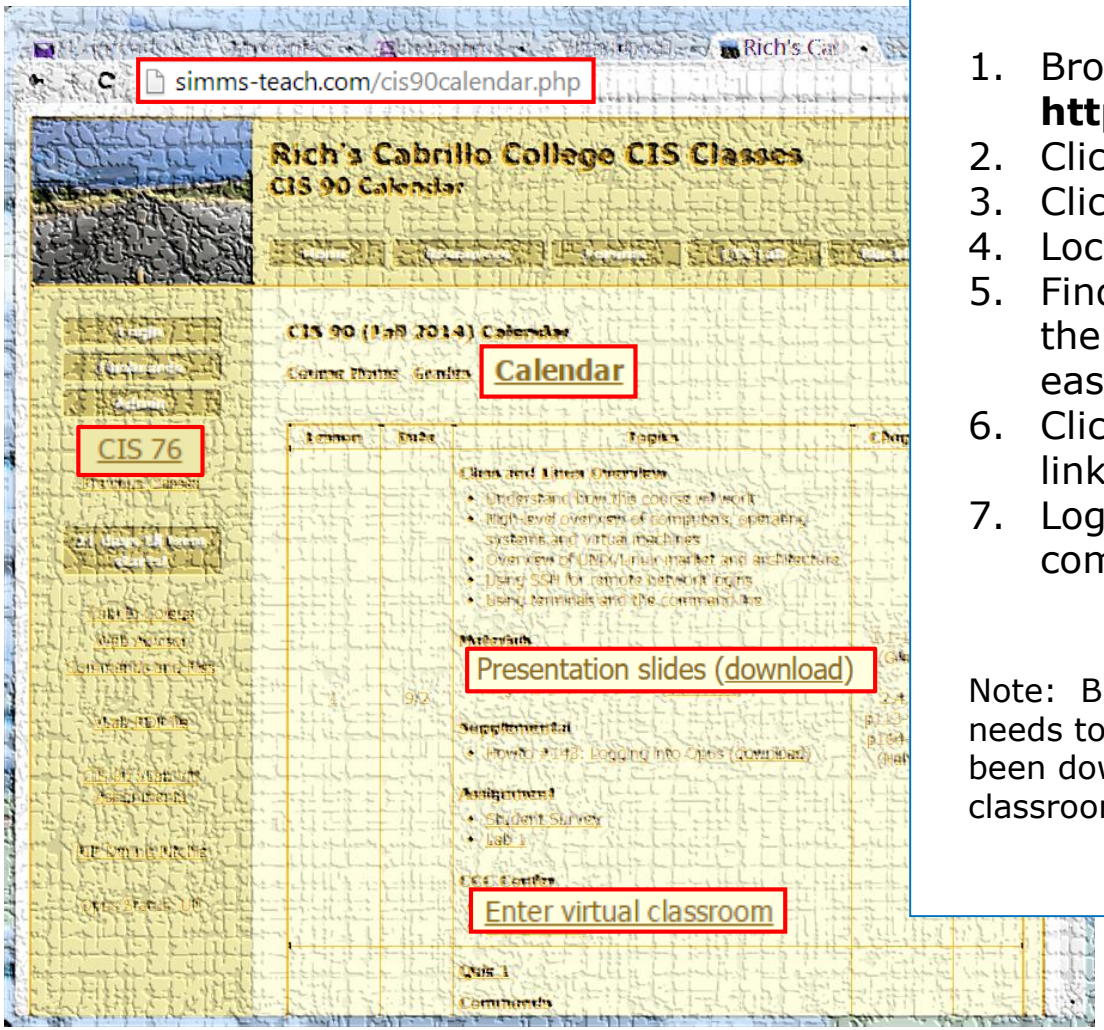
2. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

Introductions and Credits

Rich Simms
- HP Alumnus.
- Started teaching in 2008 when Jim Griffin went on sabbatical.
- Rich's site: http://simms-teach.com

And thanks to:
- Steven Bolt at for his WASTC EH training.
- Kevin Vaccaro for his CSSIA EH training and Netlab+ pods.
- EC-Council for their online self-paced CEH v9 course.
- Sam Bowne for his WASTC seminars, textbook recommendation and fantastic EH website (https://samsclass.info/).
- Lisa Bock for her great lynda.com EH course.
- John Govsky for many teaching best practices: e.g. the First Minute quizzes, the online forum, and the point grading system (http://teacherjohn.com/).
- Google for everything else!

Student checklist for attending class

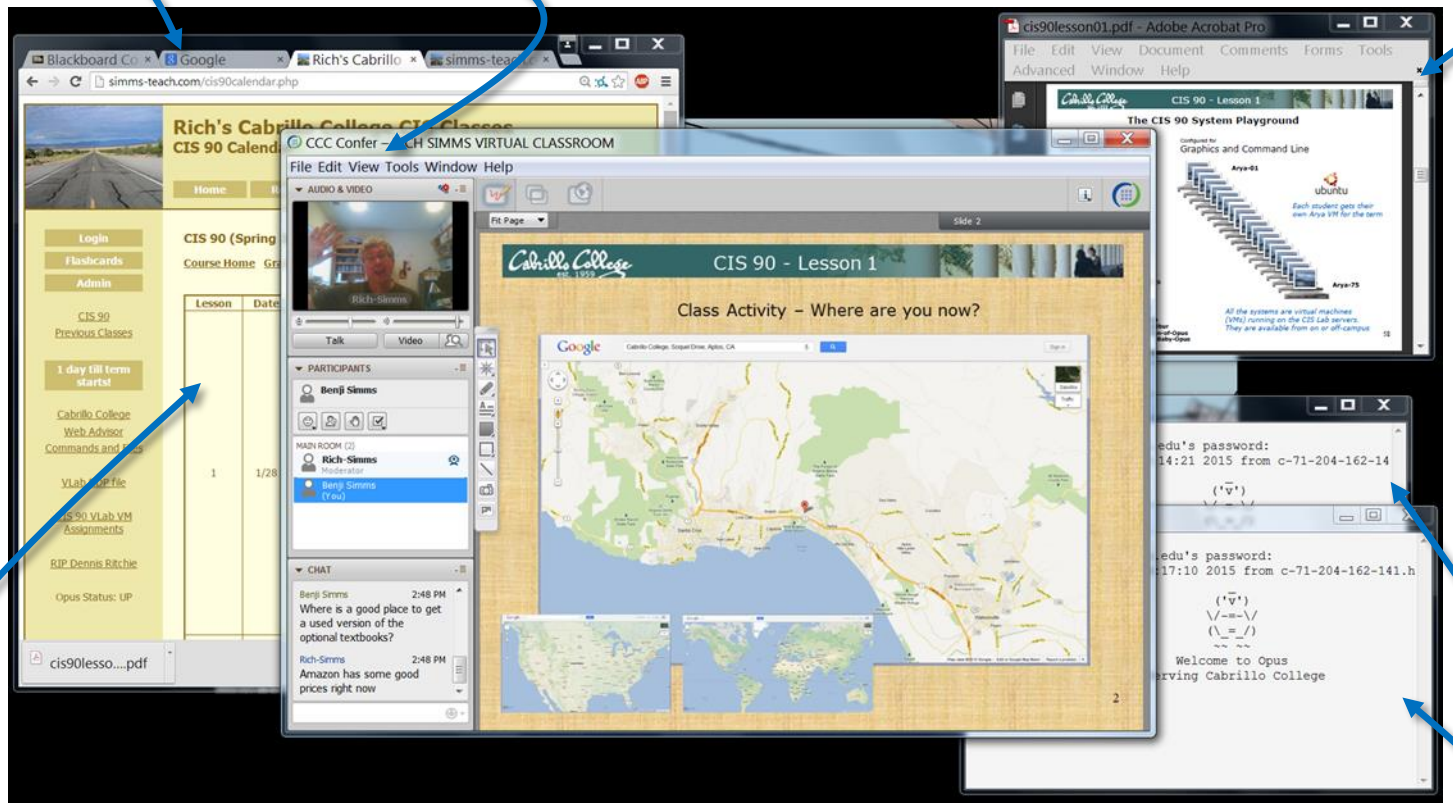


1. Browse to: **http://simms-teach.com**
2. Click the **CIS 76** link.
3. Click the **Calendar** link.
4. Locate today's lesson.
5. Find the **Presentation slides** for the lesson and **download** for easier viewing.
6. Click the **Enter virtual classroom** link to join CCC Confer.
7. Log into Opus-II with Putty or ssh command.

Note: Blackboard Collaborate Launcher only needs to be installed once. It has already been downloaded and installed on the classroom PC's.

Student checklist for suggested screen layout

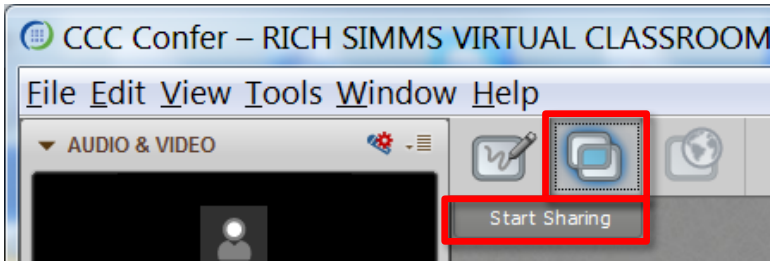
- ❑ *Google*
- ❑ *CCC Confer*
- ❑ *Downloaded PDF of Lesson Slides*



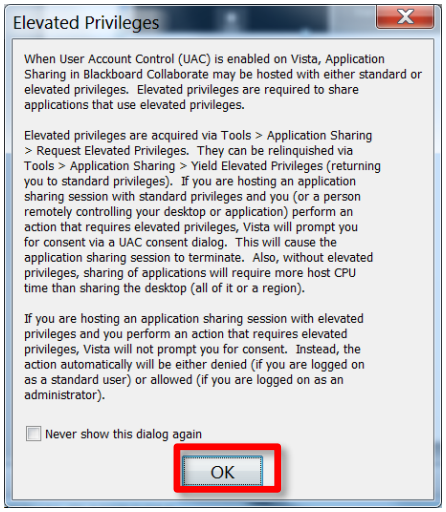
- ❑ *CIS 76 website Calendar page*
- ❑ *One or more login sessions to Opus-II*

Student checklist for sharing desktop with classmates

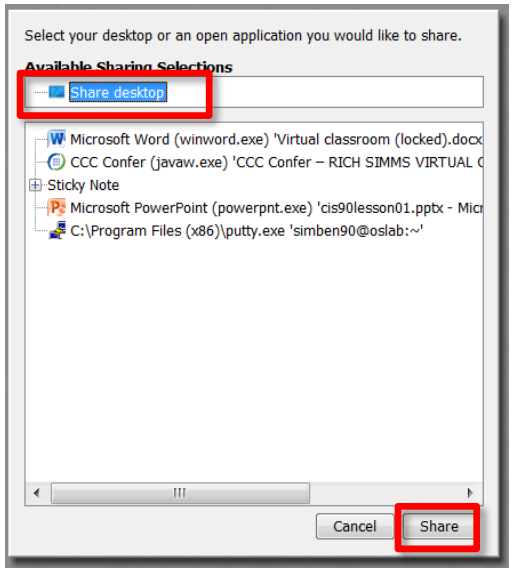
1) Instructor gives you sharing privileges.



2) Click overlapping rectangles icon. If white "Start Sharing" text is present then click it as well.



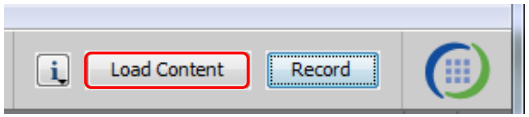
3) Click OK button.



4) Select "Share desktop" and click Share button.

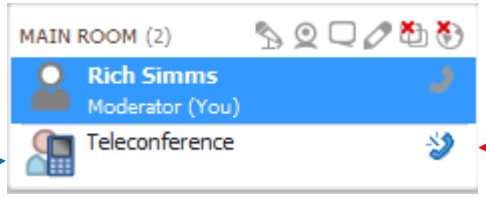
Rich's CCC Confer checklist - setup

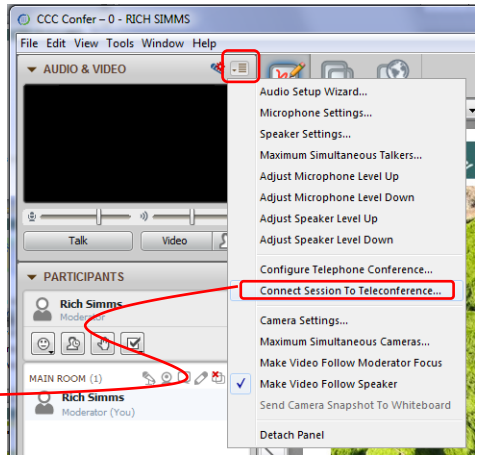
[ ] Preload White Board



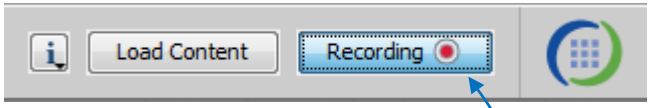
[ ] Connect session to Teleconference

Session now connected to teleconference





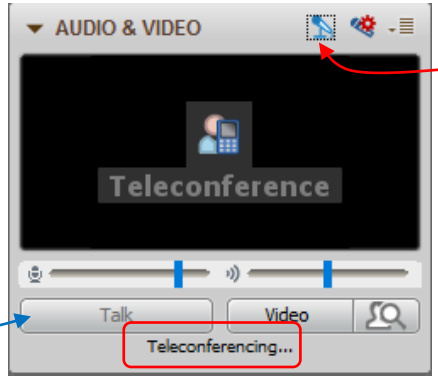
[ ] Is recording on?



Red dot means recording

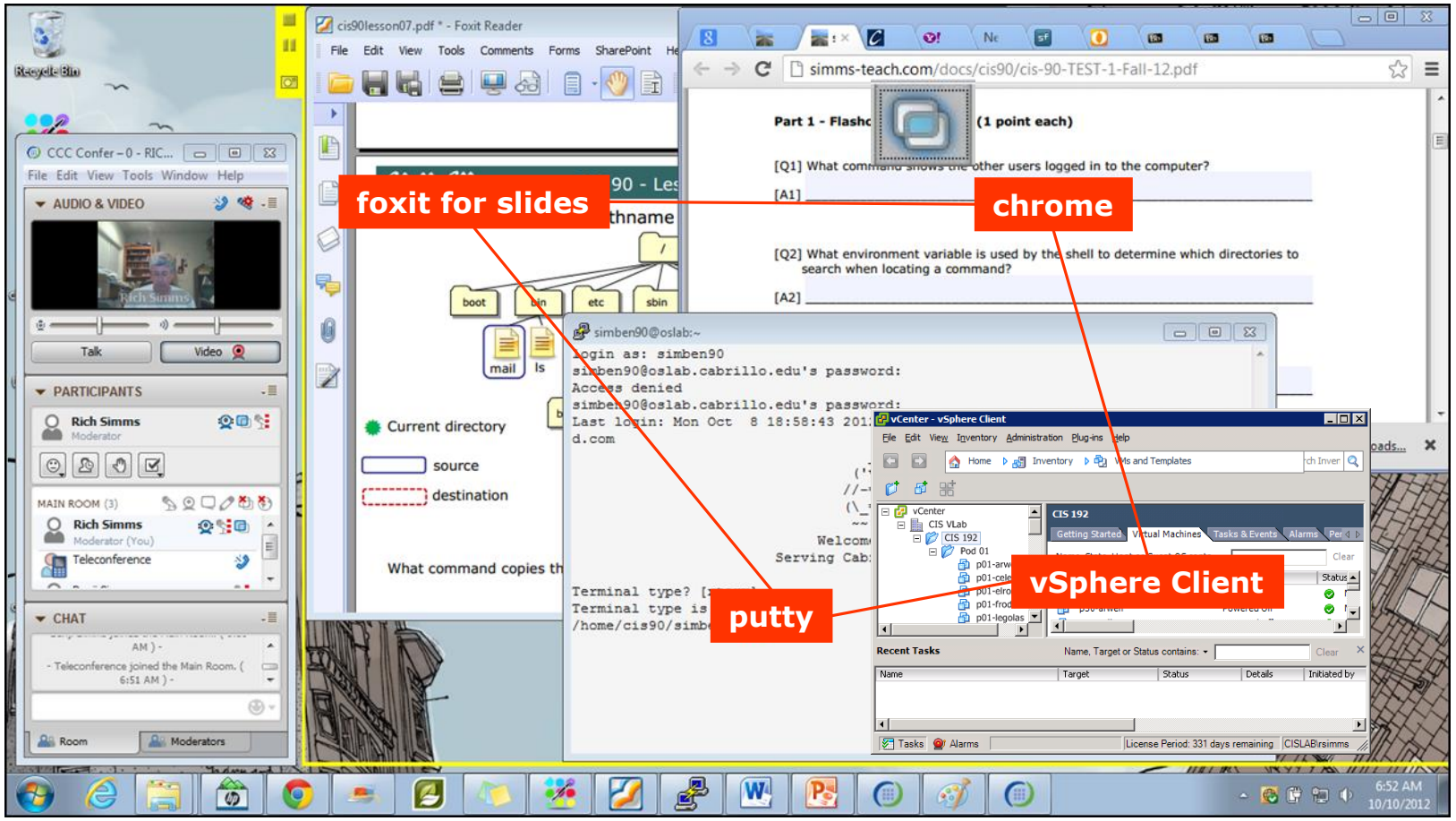
[ ] Use teleconferencing, not mic

Should be grayed out



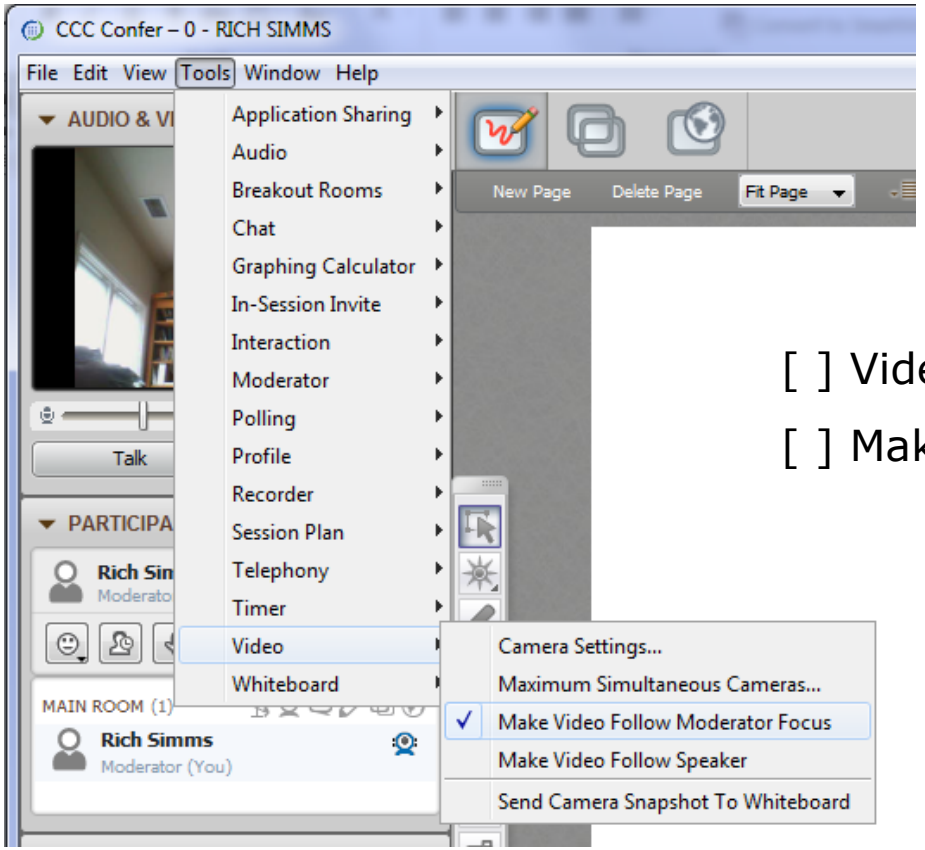
Should change from phone handset icon to little Microphone icon and the Teleconferencing … message displayed

Rich's CCC Confer checklist - screen layout



[ ] layout and share apps

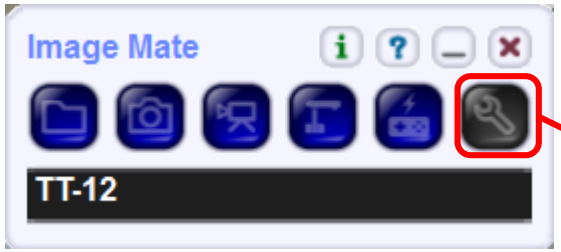
Rich's CCC Confer checklist - webcam setup

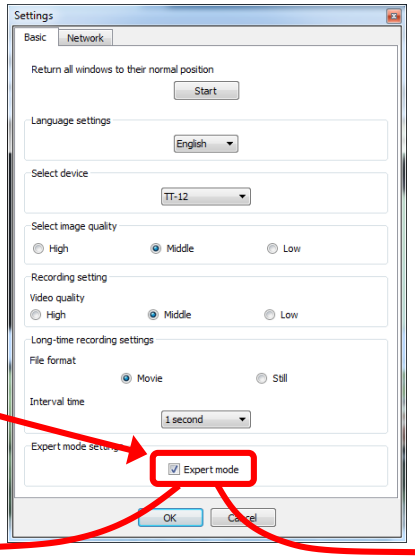


[ ] Video (webcam)

[ ] Make Video Follow Moderator Focus

Rich's CCC Confer checklist - Elmo



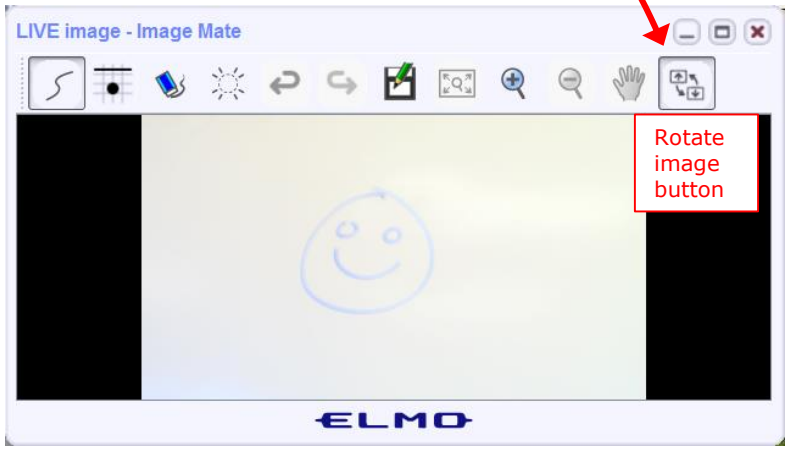


The "rotate image" button is necessary if you use both the side table and the white board.

Quite interesting that they consider you to be an "expert" in order to use this button!

Elmo rotated down to view side table

Elmo rotated up to view white board



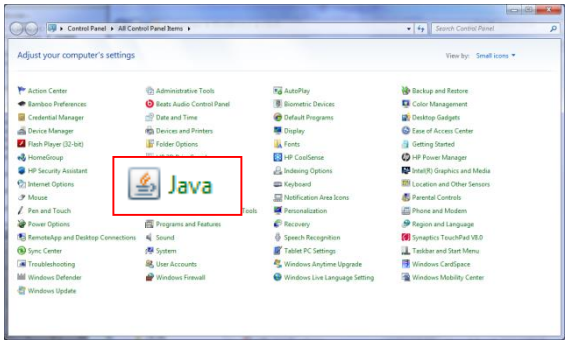
Run and share the Image Mate program just as you would any other app with CCC Confer

Rich's CCC Confer checklist - universal fixes

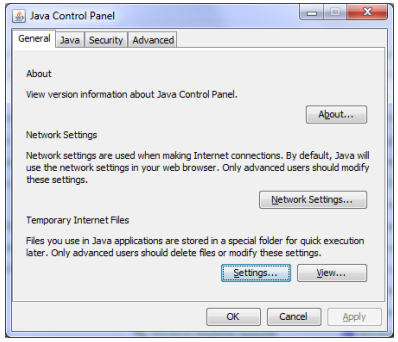
Universal Fix for CCC Confer:

1) Shrink (500 MB) and delete Java cache
2) Uninstall and reinstall latest Java runtime
3) http://www.cccconfer.org/support/technicalSupport.aspx

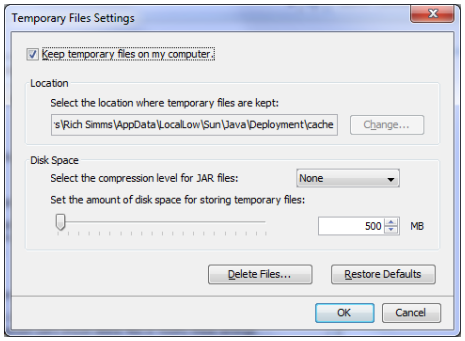
Control Panel (small icons)



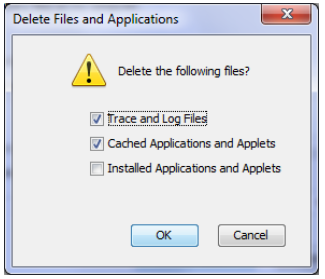
General Tab > Settings…



500MB cache size



Delete these



Google Java download

Start

Sound Check

*Students that dial-in should mute their line using *6 to prevent unintended noises distracting the web conference.*

*Instructor can use *96 to mute all student lines.*

Volume
**4 - increase conference volume.*
**7 - decrease conference volume.*
**5 - increase your voice volume.*
**8 - decrease your voice volume.*

CIS 76 - Lesson 7

Instructor: **Rich Simms**
Dial-in: **888-886-3951**
Passcode: **136690**


Philip


Bruce

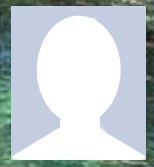

Tre


Sam B.


Sam R.


Miguel


Bobby


Garrett


Ryan A.


Aga


Karina


Chris


Tanner


Helen


Xu


Mariano


Cameron


Ryan M.


May


Karl-Heinz


Remy

Email me (risimms@cabrillo.edu) a relatively current photo of your face for 3 points extra credit

First Minute Quiz

Please answer these questions **in the order** shown:

Use CCC Confer White Board

email answers to: risimms@cabrillo.edu

(answers must be emailed within the first few minutes of class for credit)

Enumeration

Objectives	Agenda
• Describe the enumeration step • Enumerate Windows targets • Enumerate Unix/Linux targets	• Quiz • Questions • Housekeeping • Enumeration • NetBIOS Enumeration • Various Enumeration tools • Linux finger command • Assignment • Wrap up

Admonition

Unauthorized hacking is a crime.

The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

Students that engage in any unethical, unauthorized or illegal hacking may be dropped from the course and will receive no legal protection or help from the instructor or the college.

Questions

Questions?

Lesson material?

Labs? Tests?

How this course works?

- Graded work in home directories
- Answers in /home/cis76/answers

> *Who questions much, shall learn much, and retain much.*
> - Francis Bacon

> *If you don't ask, you don't get.*
> - Mahatma Gandhi

Chinese Proverb	他問一個問題，五分鐘是個傻子，他不問一個問題仍然是一個傻瓜永遠。 *He who asks a question is a fool for five minutes; he who does not ask a question remains a fool forever.*

Power up SLOWLY

Don't everyone do this at once!

Pod VMs to powerup:

EH-pfSense-xx
EH-Kali-xx
EH-WinXP-xx
EH-Win7-xx
EH-OWASP-xx

In the news

Recent news

John Kelly's personal cellphone was compromised, White House believes

http://www.politico.com/story/2017/10/05/john-kelly-cell-phone-compromised-243514

"White House officials believe that chief of staff John Kelly's personal cellphone was compromised, potentially as long ago as December, according to three U.S. government officials."

Recent news

Cabrillo College hack exposed 40,000 students' data

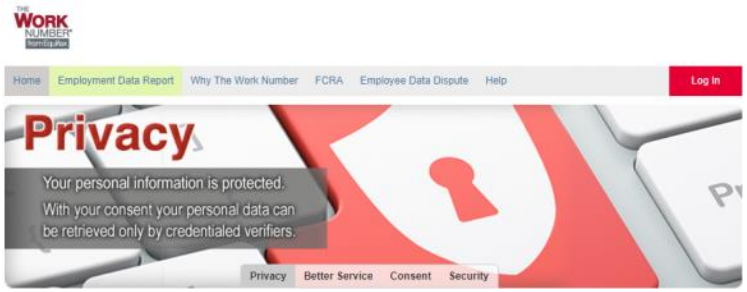
http://www.santacruzsentinel.com/social-affairs/20171009/cabrillo-college-hack-exposed-40000-students-data

"The Social Security numbers of 12,000 students were potentially compromised in the breach as well as passwords, names, dates of birth, addresses and emails of 28,000 additional students, according to Cabrillo spokeswoman Kristin Fabos."

Recent news

Equifax Breach Fallout: Your Salary History

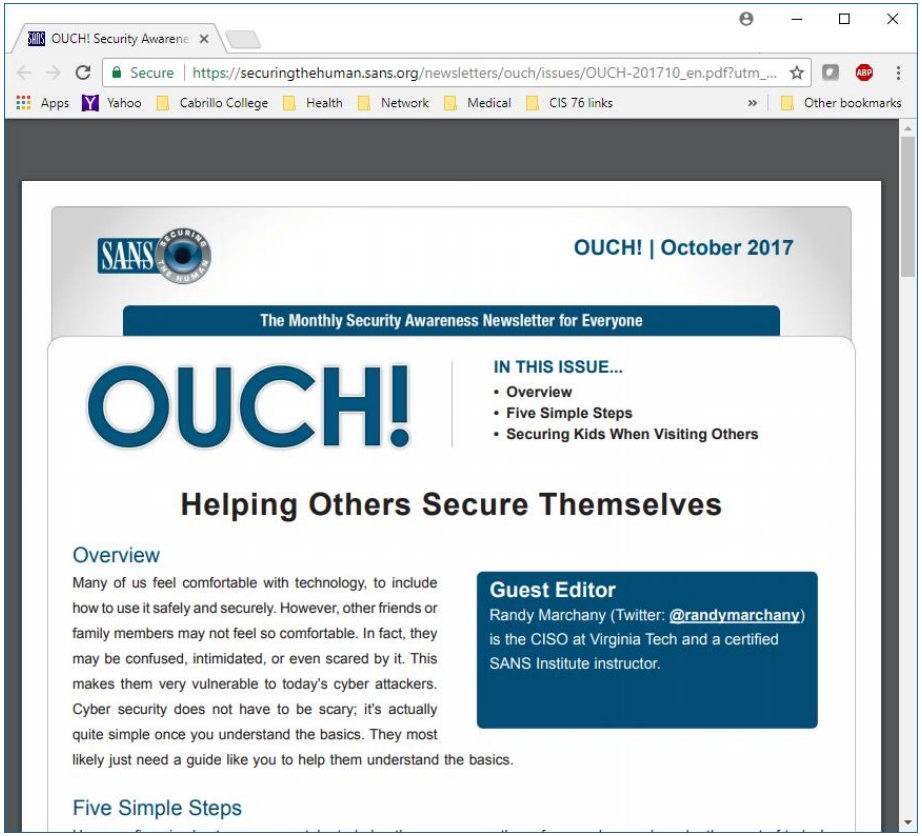
https://krebsonsecurity.com/2017/10/equifax-breach-fallout-your-salary-history/



In May, KrebsOnSecurity broke a story about lax security at a payroll division of big-three credit bureau Equifax that let identity thieves access personal and financial data on an unknown number of Americans. Incredibly, this same division makes it simple to access detailed salary and employment history on a large portion of Americans using little more than someone's Social Security number and date of birth — both data elements that were stolen in the recent breach at Equifax."

Best Practices

SANS October 2017 edition of OUCH!



1) *Social Engineering*
2) *Passwords*
3) *Patching*
4) *Anti-Virus*
5) *Backups*

https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201710_en.pdf

Housekeeping

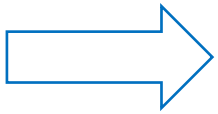
1) Lab 5 is due tonight at 11:59PM.

2) Finished Lab 5 already? Please monitor the forum and help anyone with questions.

3) Next week five forum posts are due!

Enumeration

EC-Council Five Phases of Hacking



Phase 1 - Reconnaissance

Phase 2 - Scanning

Phase 3 - Gaining Access

Phase 4 - Maintaining Access

Phase 5 - Clearing Tracks

http://www.techrepublic.com/blog/it-security/the-five-phases-of-a-successful-network-penetration/

Enumeration

- Enumeration is typically active and intrusive, definitely crossing the legal line.
- Using enumeration techniques without authorization is a crime!
- Active connections are made to target devices to gather more information:
  - Users and groups.
  - System names.
  - Network resources.
  - Network shares.
  - Services.
  - Policies.

NetBIOS Enumeration

NetBIOS

- Network Basic Input Output System.
- Originally an API for accessing shared file and printer services on a LAN.
- NetBIOS names are unique 16 byte identifiers. The first 15 bytes are an ASCII name followed by the 16th byte which is the suffix code.

NetBIOS Suffix Code Table

Name	Number (HEX)	Type	Usage
<computername>	00	U	Workstation Service
<computername>	01	U	Messenger Service
<_MSBROWSE_>	01	G	Master Browser
<computername>	03	U	Messenger Service
<computername>	06	U	RAS Server Service
<computername>	1F	U	NetDDE Service
<computername>	20	U	File Server Service
<computername>	21	U	RAS Client Service
<computername>	22	U	Exchange Interchange
<computername>	23	U	Exchange Store
<computername>	24	U	Exchange Directory
<computername>	30	U	Modem Sharing Server Service
<computername>	31	U	Modem Sharing Client Service
<computername>	43	U	SMS Client Remote Control
<computername>	44	U	SMS Admin Remote Control Tool
<computername>	45	U	SMS Client Remote Chat
<computername>	46	U	SMS Client Remote Transfer
<computername>	4C	U	DEC Pathworks TCPIP Service
<computername>	52	U	DEC Pathworks TCPIP Service
<computername>	87	U	Exchange MTA
<computername>	6A	U	Exchange IMC
<computername>	BE	U	Network Monitor Agent
<computername>	BF	U	Network Monitor Apps
<username>	03	U	Messenger Service
<domain>	00	G	Domain Name
<domain>	1B	U	Domain Master Browser
<domain>	1C	G	Domain Controllers
<domain>	1D	U	Master Browser
<domain>	1E	G	Browser Service Elections
<INet~Services>	1C	G	Internet Information Server
<IS~Computer_name>	00	U	Internet Information Server

http://www.pyeung.com/pages/microsoft/winnt/netbioscodes.html

The suffix code provides additional information about the computer

NetBIOS Enumeration

- Discover computers belonging to a workgroup or domain and what services they provide.
- Discover SMB file shares and printers on the LAN (Windows or Unix/Linux servers running SAMBA).
- Discover additional information as well.

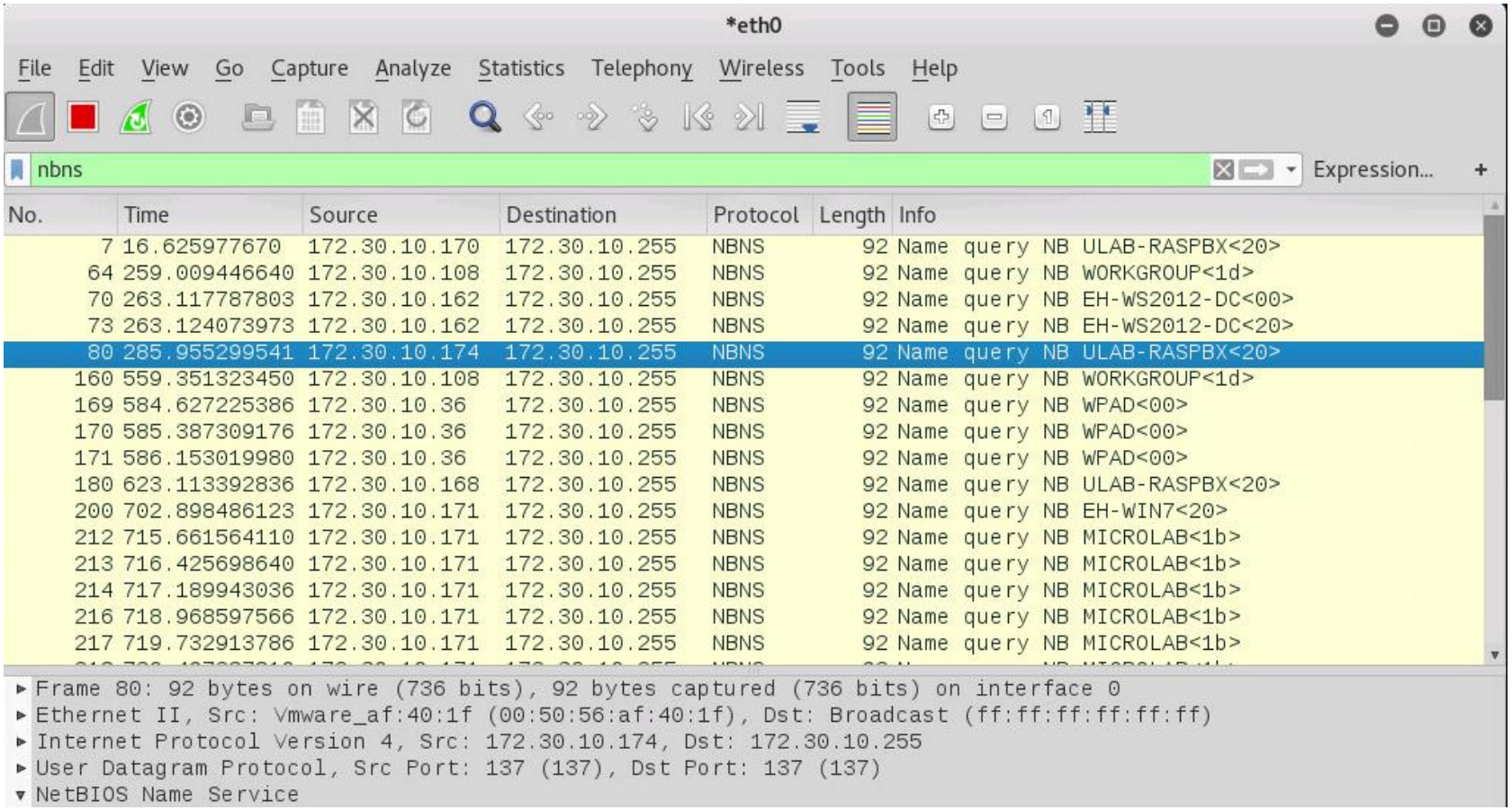
Note: Microsoft does not support NetBIOS for IPV6.

NetBIOS Null Session

- One of the biggest vulnerabilities of NetBIOS systems.
- Anonymous connections without a username and password.
- Still present on Windows XP.
- Disabled by default on Windows 2003.
- No longer present in Vista or Windows 2008 and later.

NetBIOS Passive Discovery

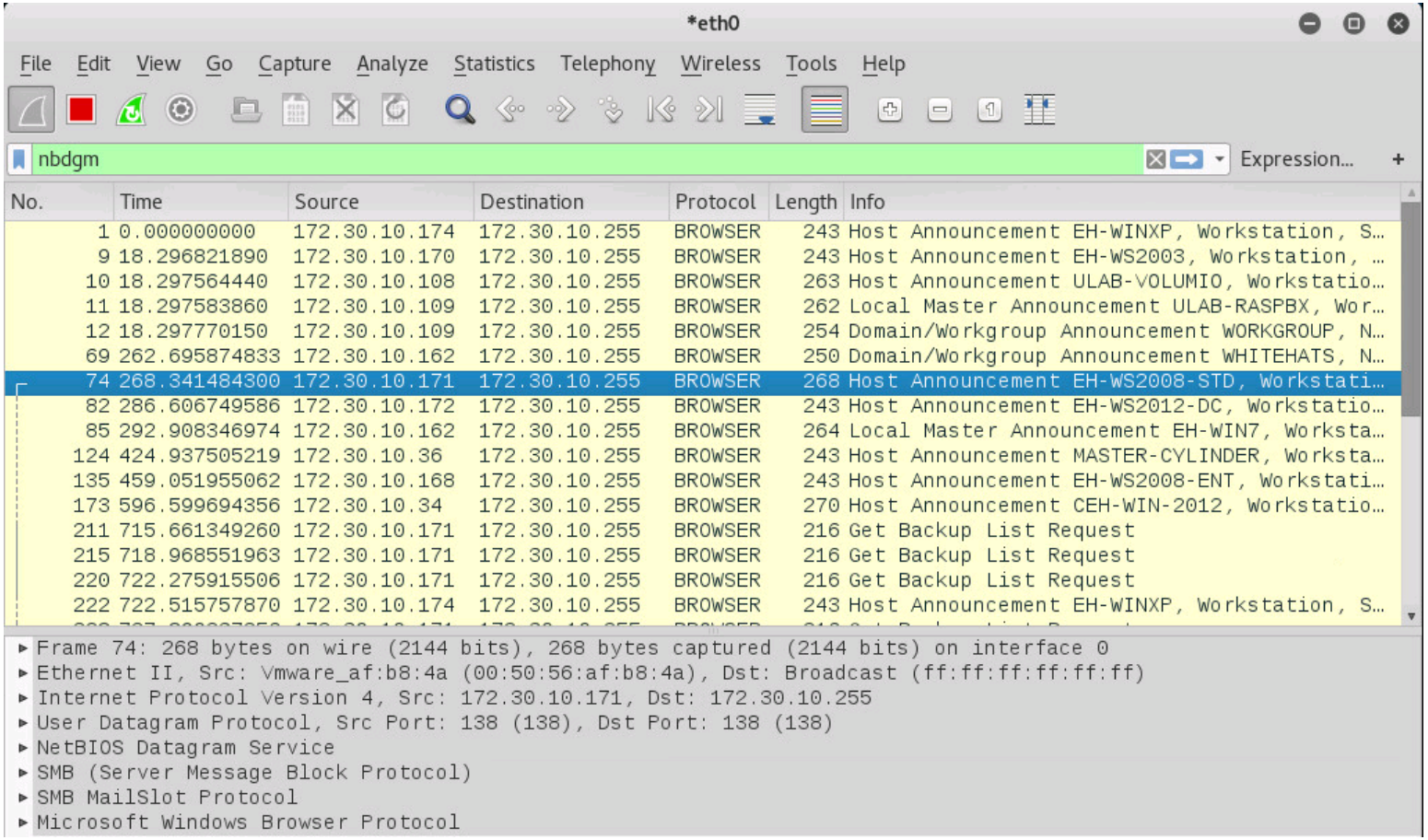
nbns



NBNS = NetBIOS Name Service (WINS) uses UDP port 137

NetBIOS Passive Discovery

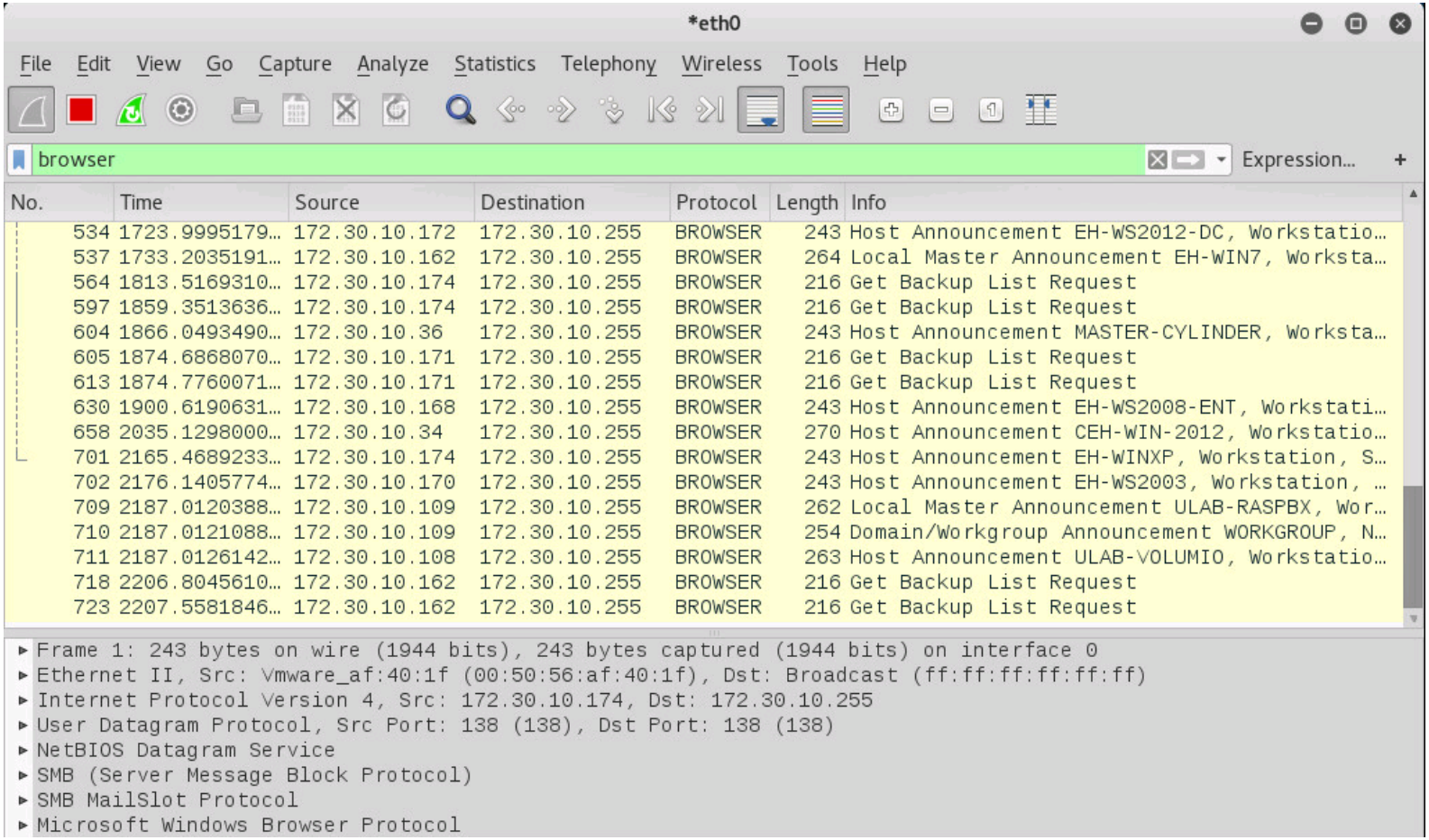
nbdgm



NBDGM = NetBIOS Datagram Service on UDP port 138

NetBIOS Passive Discovery

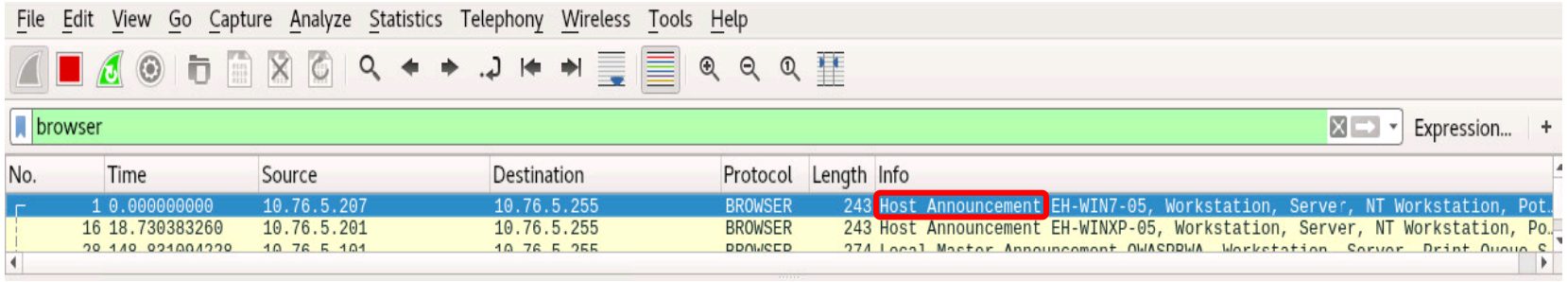
browser

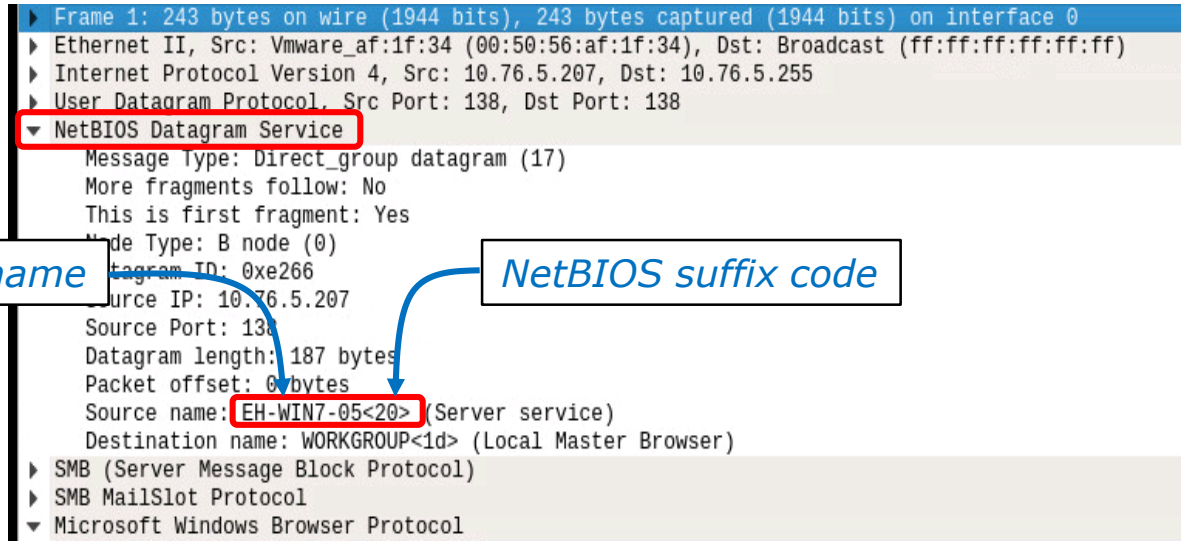


Shows same information

NetBIOS Datagram Service Layer

browser





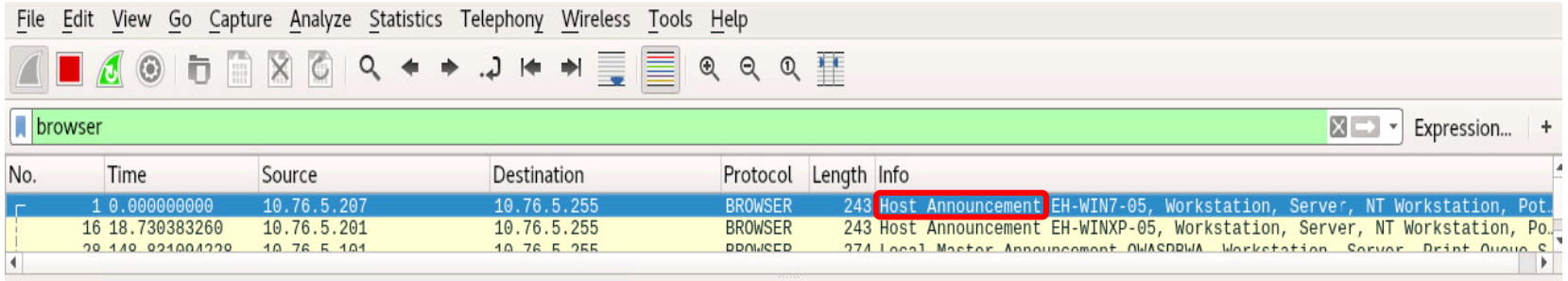
Computer name

NetBIOS suffix code

NetBIOS names are unique 16 byte identifiers. The first 15 bytes are an ASCII name followed by the 16th byte which is the suffix code.

Microsoft Windows Browser Protocol layer Server type section

browser

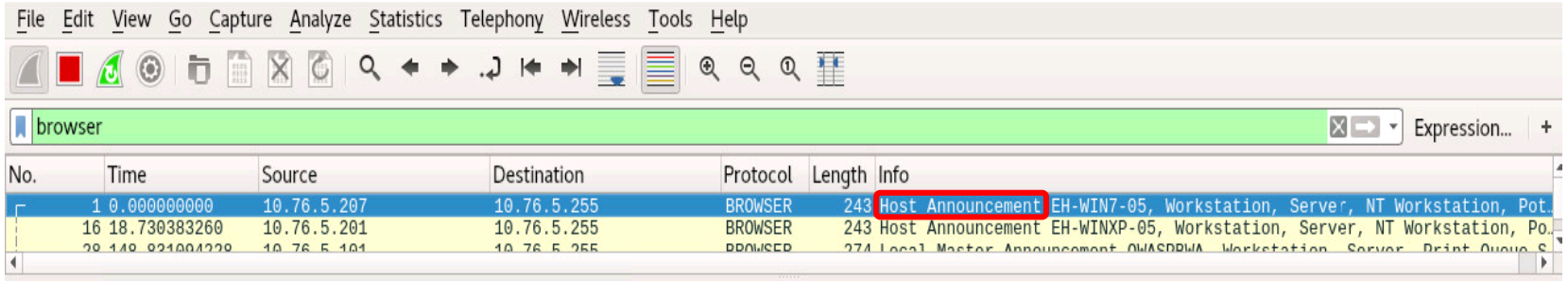



```
▼ Microsoft Windows Browser Protocol
    Command: Host Announcement (0x01)
    Update Count: 0
    Update Periodicity: 12 minutes
    Host Name: EH-WIN7-05
    Windows version: Windows 7 or Windows Server 2008 R2
    OS Major Version: 6
    OS Minor Version: 1
```

Hostname and OS

Microsoft Windows Browser Protocol layer Server type section

browser




```
▼ Microsoft Windows Browser Protocol
  ▼ Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser
      .... .... .... .... .... .... .... ...1 = Workstation: This is a Workstation
      .... .... .... .... .... .... .... ..1. = Server: This is a Server
      .... .... .... .... .... .... .... .0.. = SQL: This is NOT an SQL server
      .... .... .... .... .... .... .... 0... = Domain Controller: This is NOT a Domain Controller
      .... .... .... .... .... .... ...0 .... = Backup Controller: This is NOT a Backup Controller
      .... .... .... .... .... .... ..0. .... = Time Source: This is NOT a Time Source
      .... .... .... .... .... .... .0.. .... = Apple: This is NOT an Apple host
      .... .... .... .... .... .... 0... .... = Novell: This is NOT a Novell server
      .... .... .... .... .... ...0 .... .... = Member: This is NOT a Domain Member server
      .... .... .... .... .... ..0. .... .... = Print: This is NOT a Print Queue server
      .... .... .... .... .... .0.. .... .... = Dialin: This is NOT a Dialin server
      .... .... .... .... .... 0... .... .... = Xenix: This is NOT a Xenix server
      .... .... .... .... ...1 .... .... .... = NT Workstation: This is an NT Workstation
      .... .... .... .... ..0. .... .... .... = WfW: This is NOT a WfW host
      .... .... .... .... 0... .... .... .... = NT Server: This is NOT an NT Server
      .... .... .... ...1 .... .... .... .... = Potential Browser: This is a Potential Browser
      .... .... .... ..0. .... .... .... .... = Backup Browser: This is NOT a Backup Browser
      .... .... .... .0.. .... .... .... .... = Master Browser: This is NOT a Master Browser
      .... .... .... 0... .... .... .... .... = Domain Master Browser: This is NOT a Domain Master Browser
      .... .... ...0 .... .... .... .... .... = OSF: This is NOT an OSF host
      .... .... ..0. .... .... .... .... .... = VMS: This is NOT a VMS host
      .... .... .0.. .... .... .... .... .... = Windows 95+: This is NOT a Windows 95 or above host
      .... .... 0... .... .... .... .... .... = DFS: THis is NOT a DFS server
      .0.. .... .... .... .... .... .... .... = Local: This is NOT a local list only request
      0... .... .... .... .... .... .... .... = Domain Enum: This is NOT a Domain Enum request
  Browser Protocol Major Version: 15
```

"This is ..." and "This is NOT ..." explanations of bit settings

Passive NetBIOS enumeration with Wireshark

1. Power up your Windows pod VMs.

2. Run Wireshark on Kali and set the filter to "browser". It may take a minute or two before you capture any packets.

3. Select any of the "Host Announcement" packets sent by either 10.76.xx.201 or 10.76.xx.207 to the subnet broadcast address.

4. In the center pane, expand the "NetBIOS Datagram Service" layer and look at the "Source name" value.

   What is the NetBIOS name and suffix code?
   What does that suffix code mean?

http://www.pyeung.com/pages/microsoft/winnt/netbioscodes.html

Write your answers in the chat window.

Passive NetBIOS enumeration with Wireshark

5. Next expand the last layer named "Microsoft Windows Browser Protocol" and check the value of the "Windows version".

   What version of Windows is running?

Write your answer in the chat window.

Passive NetBIOS enumeration with Wireshark

6. In the "Microsoft Windows Browser Protocol" layer find and expand the "Server Type: 0x..." section.

   You will see "This is ..." and "This is NOT ..." explanations for each bit setting.

   Regarding only the "This is ..." explanations what can you conclude about this computer?

Write your answer in the chat window.

Passive NetBIOS enumeration with Wireshark

On a Windows LAN the computers hold an "election" to decide who with be the "Master Browser". The Master Browser has the responsibility to keeps track of all active Windows hosts on the LAN.

7. Now explore some of the other BROWSER protocol packets in your Wireshark capture.

Which VM is acting as the NetBIOS Master Browser for your pod?

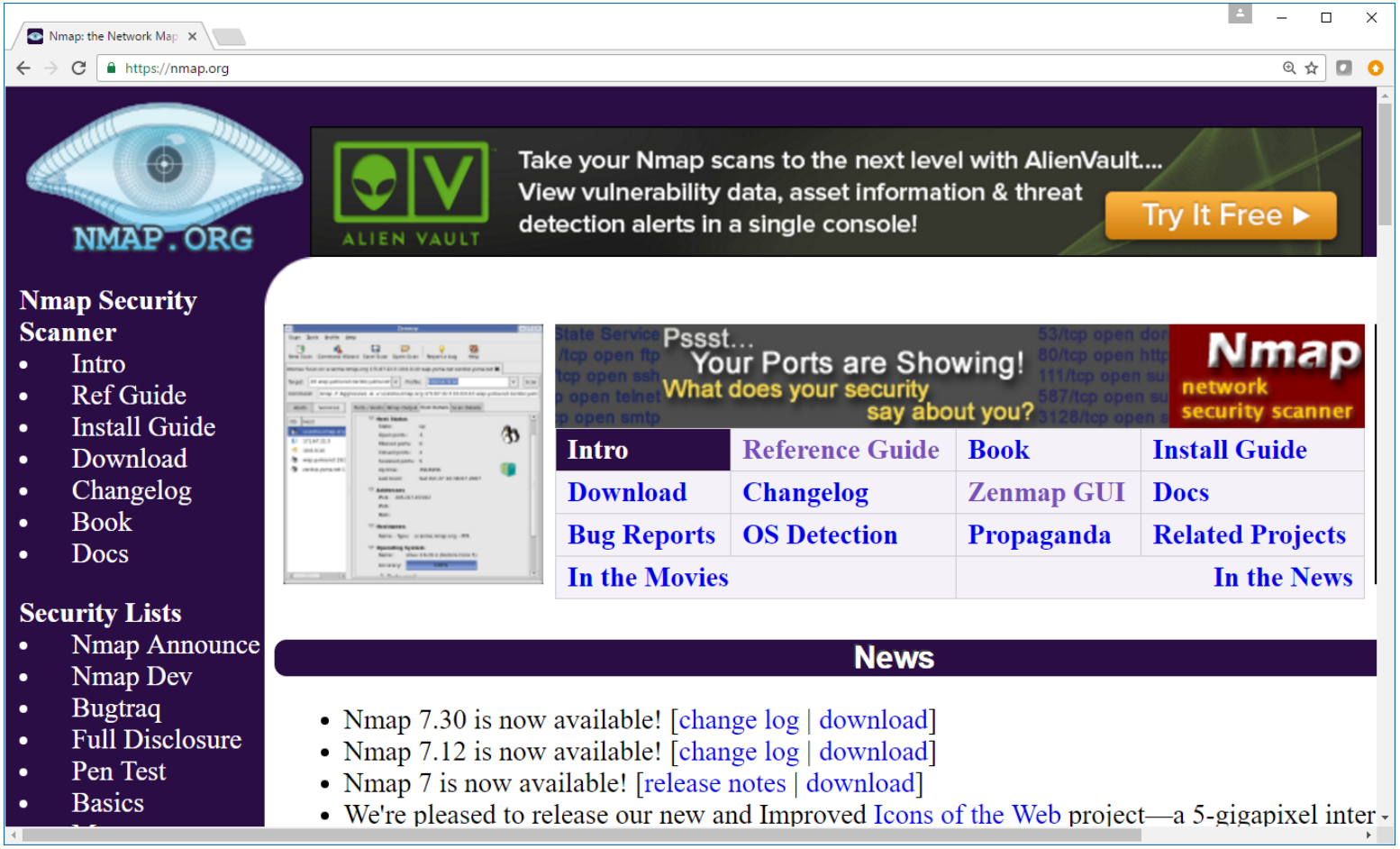
Write your answer in the chat window.

Various Enumeration Tools

Selected from EC-Council, NDG, NISGTC labs and the textbook

Nmap and Zenmap

Nmap and Zenmap



https://nmap.org/

Nmap and Zenmap

Nmap

From Wikipedia, the free encyclopedia

Nmap (*Network Mapper*) is a security scanner originally written by Gordon Lyon (also known by his pseudonym *Fyodor Vaskovich*)[2] used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses.

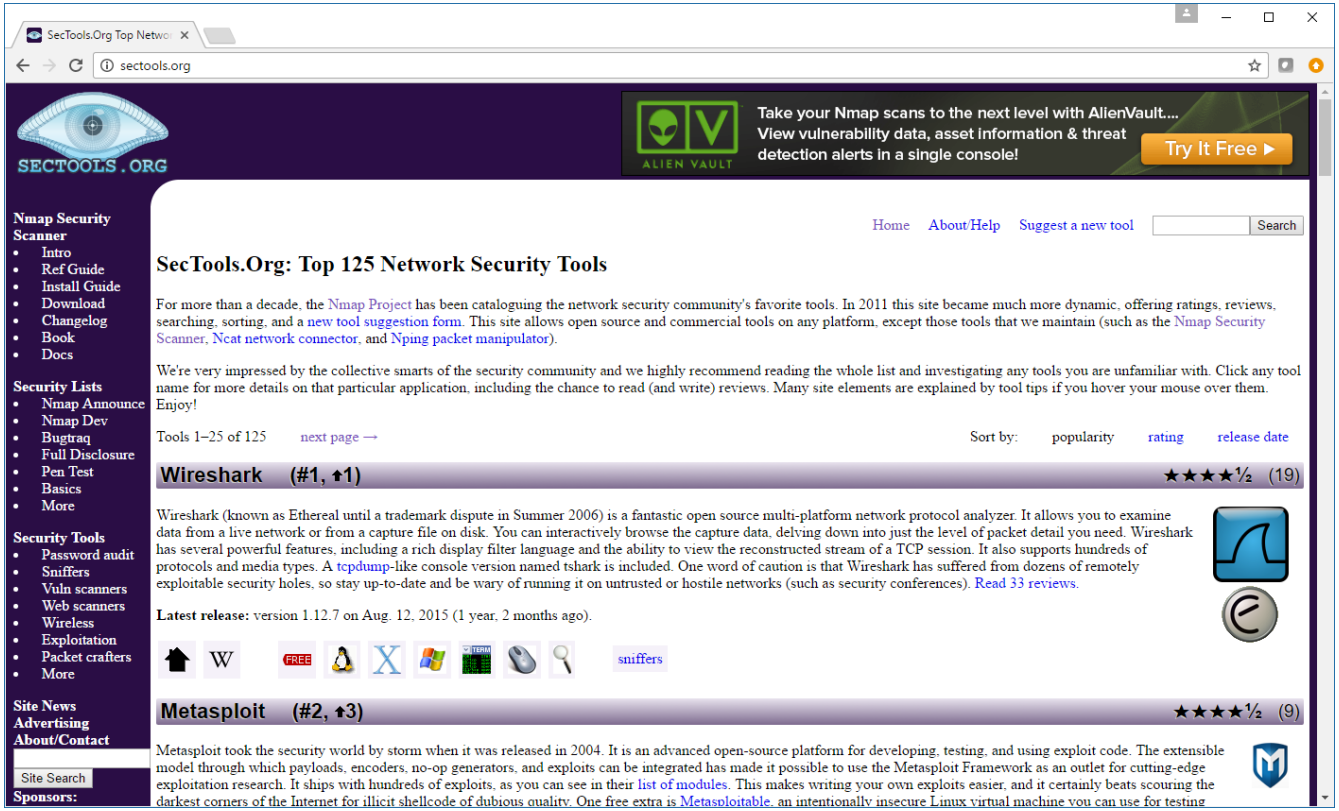
The software provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection,[3] vulnerability detection,[3] and other features. Nmap is also capable of adapting to network conditions including latency and congestion during a scan. Nmap is under development and refinement by its user community.

Nmap was originally a Linux-only utility,[4] but it was ported to Windows, Solaris, HP-UX, BSD variants (including OS X), AmigaOS, and IRIX.[5] Linux is the most popular platform, followed closely by Windows.[6]

https://en.wikipedia.org/wiki/Nmap

Nmap and Zenmap

Gordon Lyon's pseudonym is Fyodor Vaskovich. Besides maintaining the nmap website he also maintains the "Top 125 Netwrok Security Tools" website



http://sectools.org/

Nmap and Zenmap

BBC NEWS

Matrix mixes life and hacking

Reloaded may be wooing some of its audience with its gung-ho gunplay and ferocious special effects but one group of fans are impressed for entirely different reasons.

Trinity: Good with guns and keyboards

The web's hacking community has been impressed by the film's depiction of a hack attempt that employs future versions of tools and techniques widely used now.

Net-based message boards have been buzzing with mentions of the realistic depiction and photos of the hacking scenes from the film are being passed around the web.

The successful hack attack is carried out by Trinity, played by Carrie-Anne Moss, on a power company computer towards the end of the film.

Exploit alert

When actors in films start using computers, reality usually flees the scene.

But The Matrix Reloaded is winning praise from the net's computer experts and hackers because Trinity is seen using a free, popular scanning tool called Nmap.

Nmap, or Network Mapper, is used to remotely scan a computer or set of servers to find out what a target is doing. This can also reveal if it has any vulnerabilities or loopholes to exploit.

Writing about the scene, the author of Nmap, known as Fyodor, said he almost danced in the aisles of the cinema when he saw Trinity using his creation.

Fyodor wrote that the film makers seem to have changed the text output of Nmap to help it fit better on the display Trinity uses in the movie.

He also said that in the future the Matrix films depict, Nmap seems to run much faster than it does now.

No keyboards in sight at the Matrix Reloaded premiere

Trinity goes on to use Nmap to

Future performance improvements?

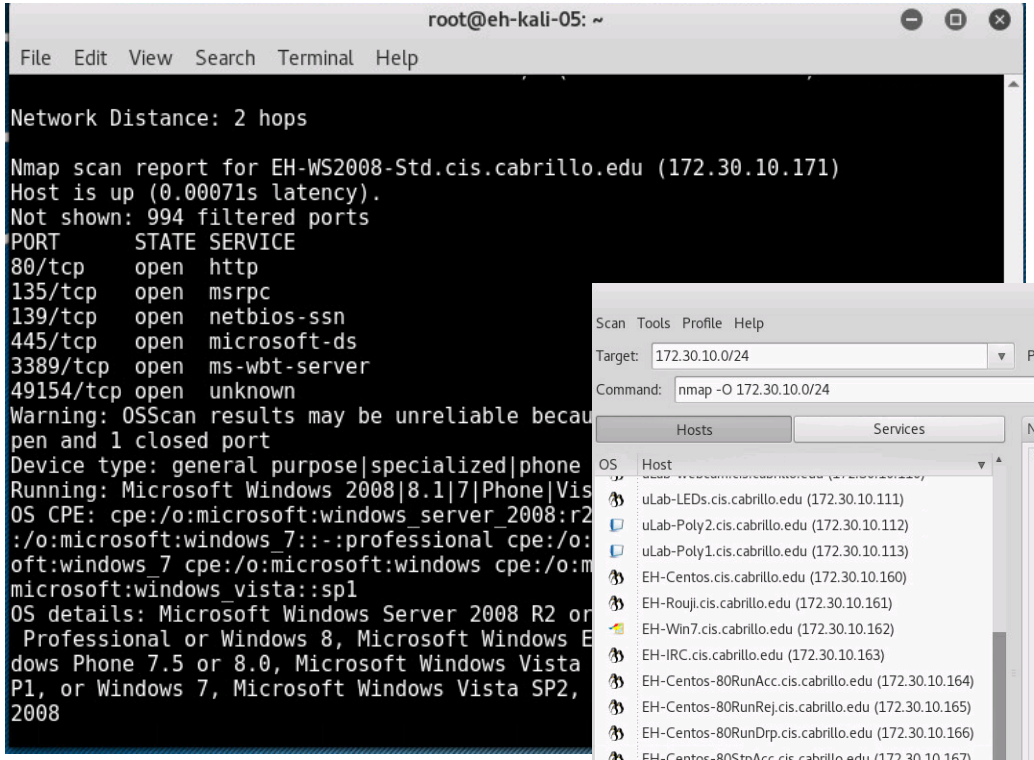
"Fyodor wrote that the film makers seem to have changed the text output of Nmap to help it fit better on the display Trinity uses in the movie.

He also said that in the future the Matrix films depict, Nmap seems to run much faster than it does now."

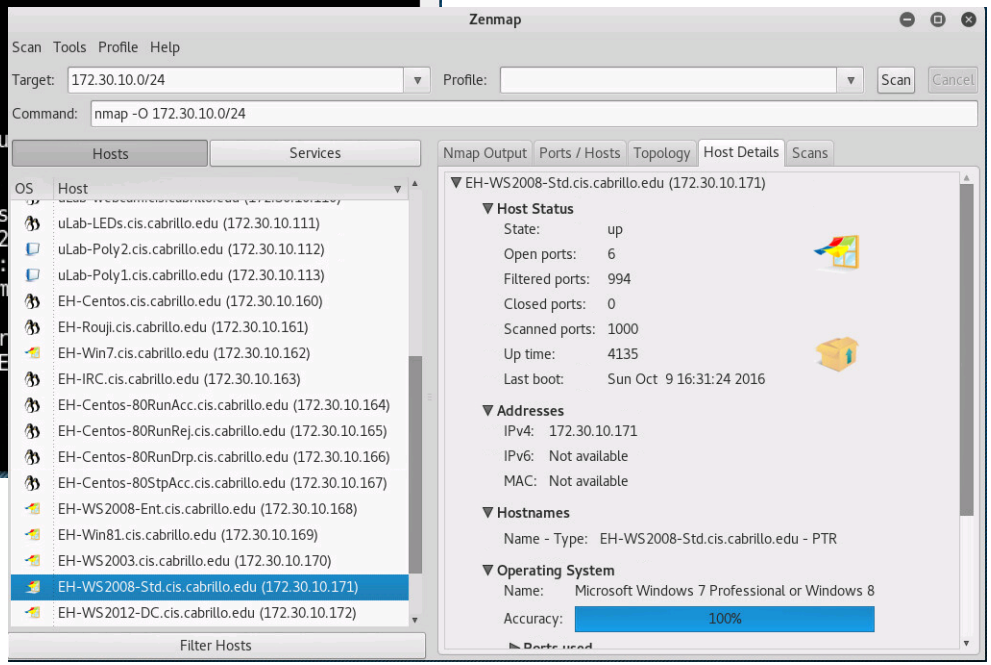
- BBC Article

http://news.bbc.co.uk/2/hi/technology/3039329.stm

Nmap and Zenmap



Nmap



Zenmap

Nmap and Zenmap are already installed on kali

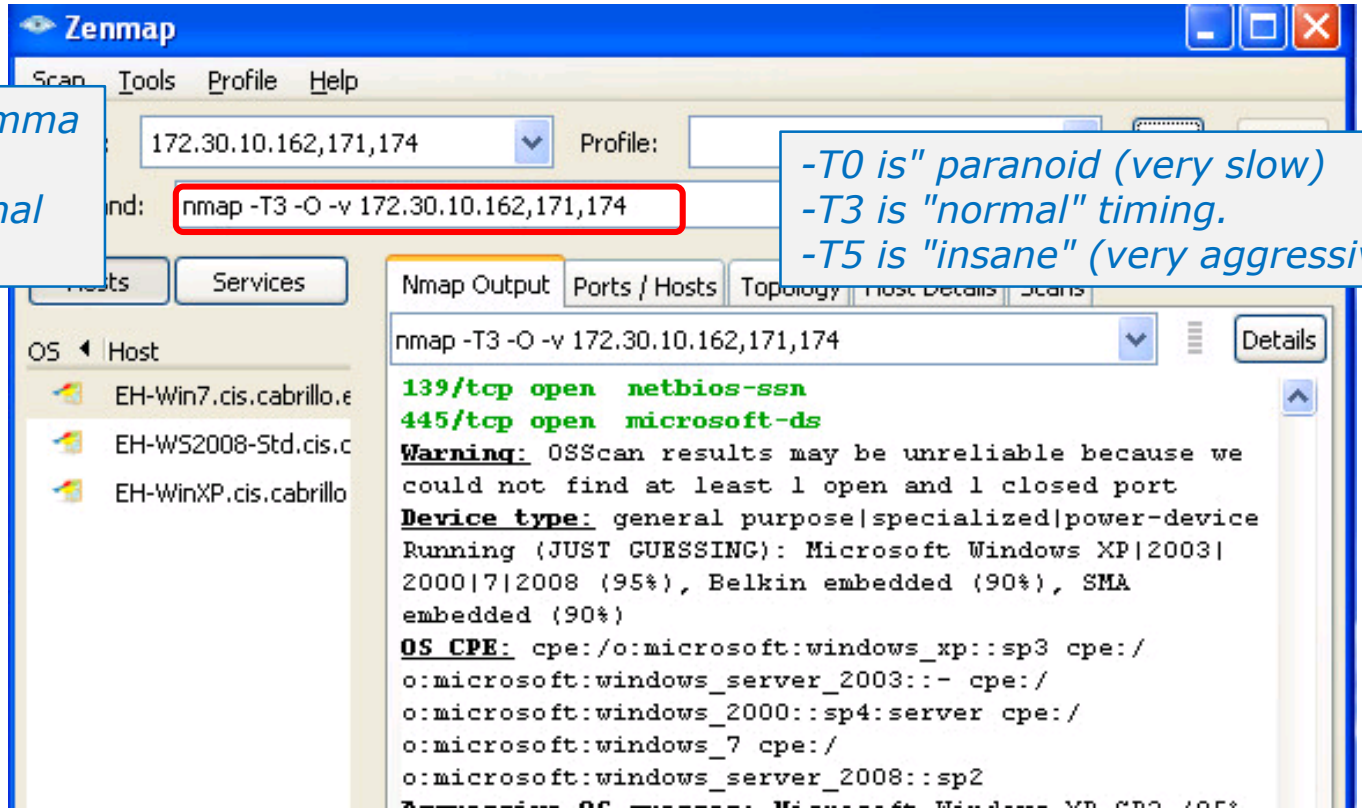
nmap -T3 -O -v 172.30.10.162,170,172

-O detects OS (operating system)

-v is verbose

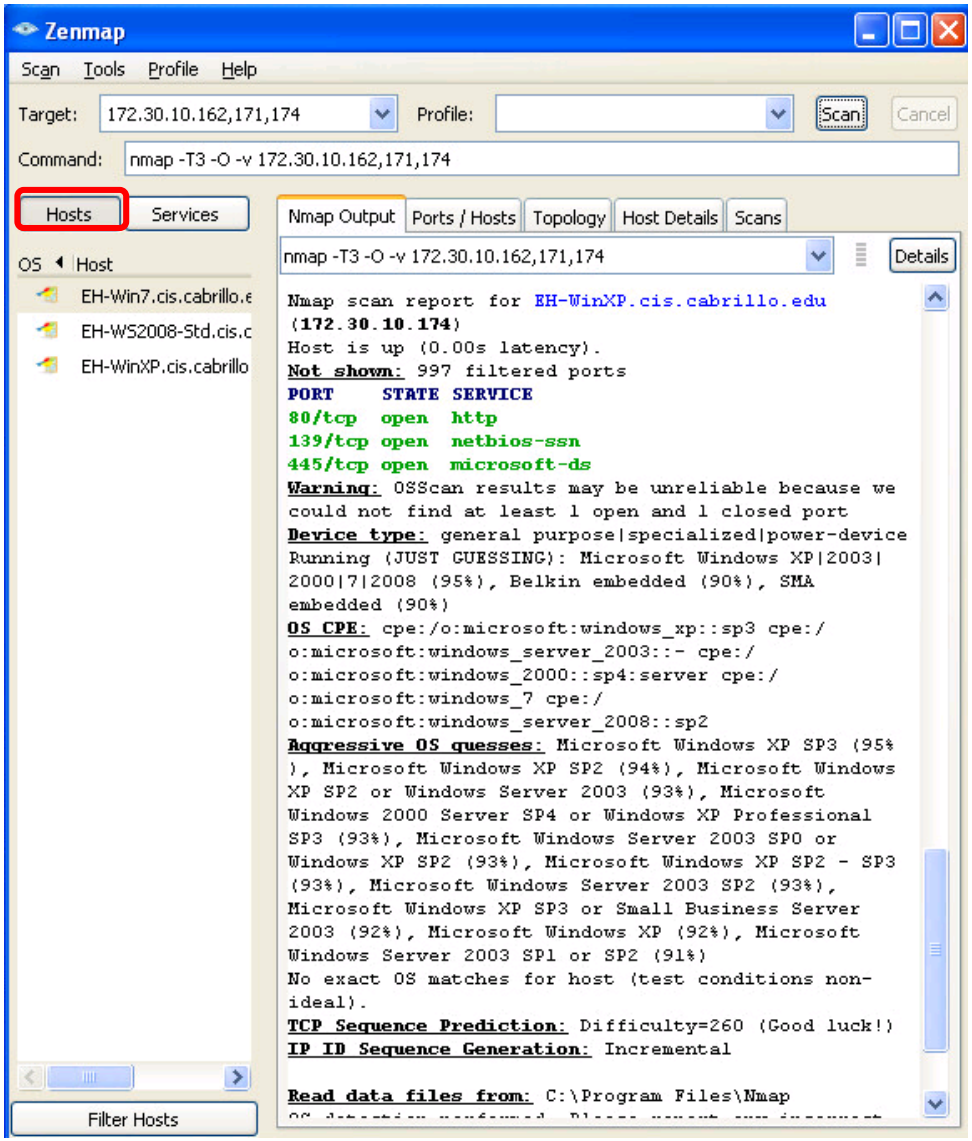
Note how a comma can be used to specify additional hosts

-T0 is" paranoid (very slow)
-T3 is "normal" timing.
-T5 is "insane" (very aggressive)



nmap -T3 -O -v 172.30.10.162,170,172

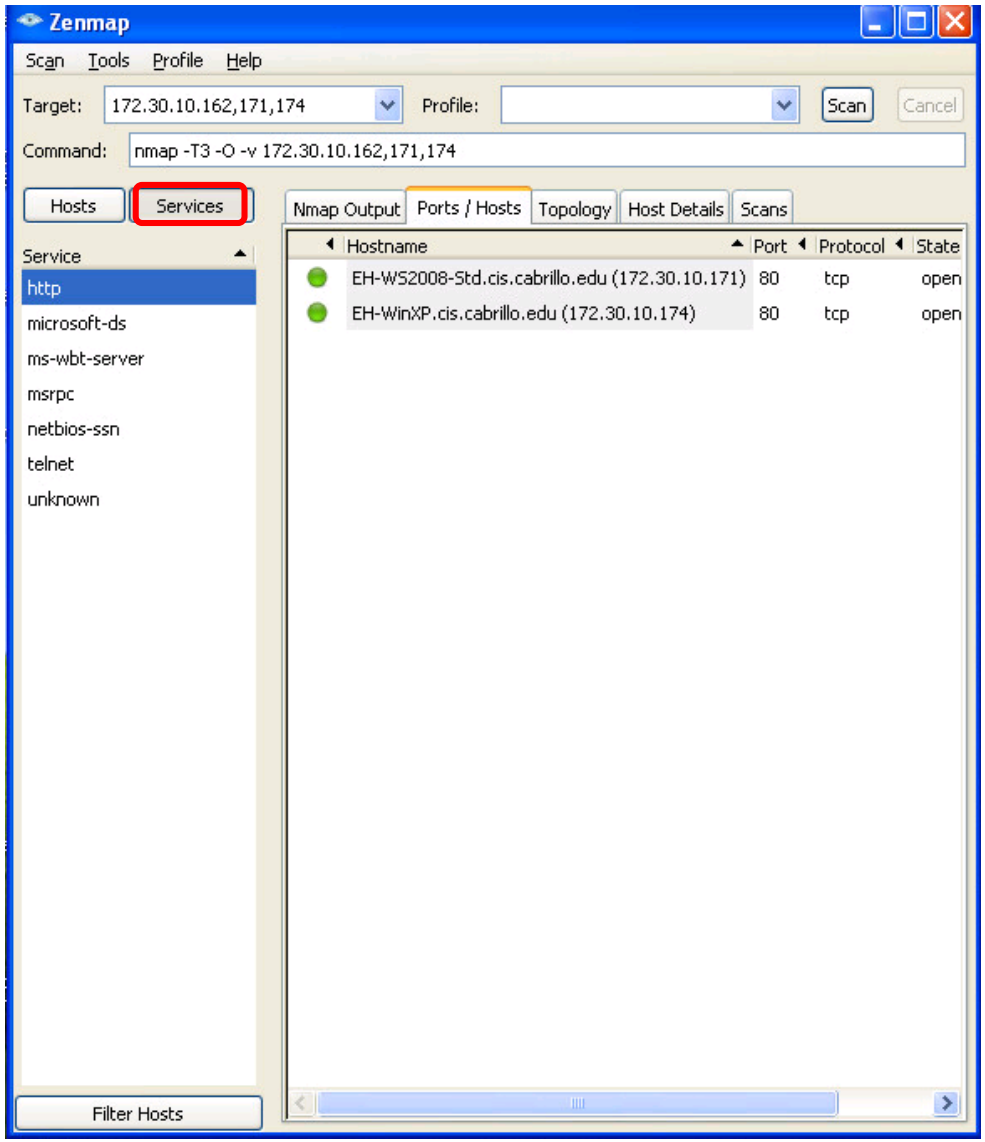
Show hosts in the left pane



Show scan output in right pane

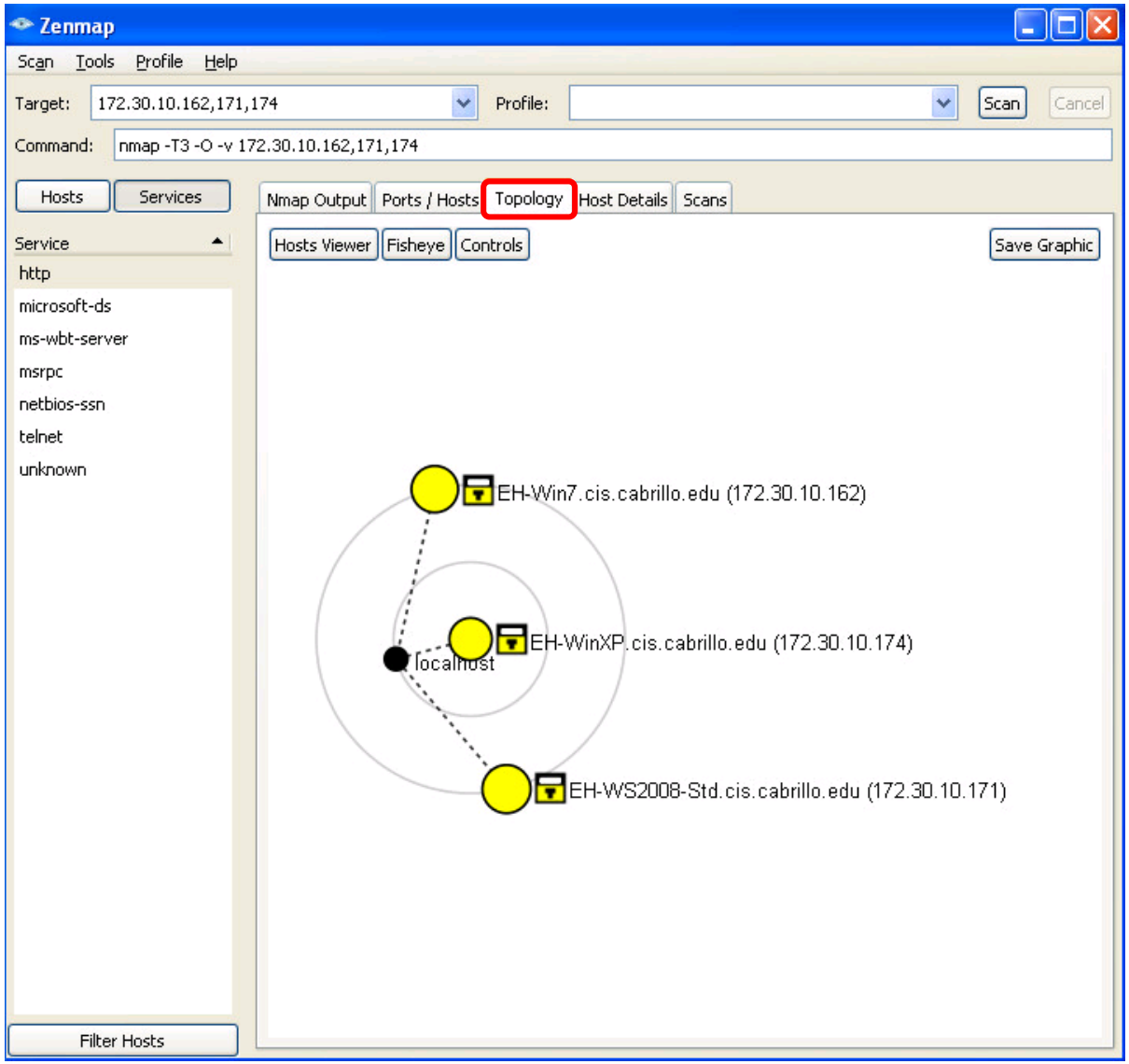
nmap -T3 -O -v 172.30.10.162,170,172

Show services in the left pane



Show hosts with selected service in the right pane

nmap -T3 -O -v 172.30.10.162,170,172



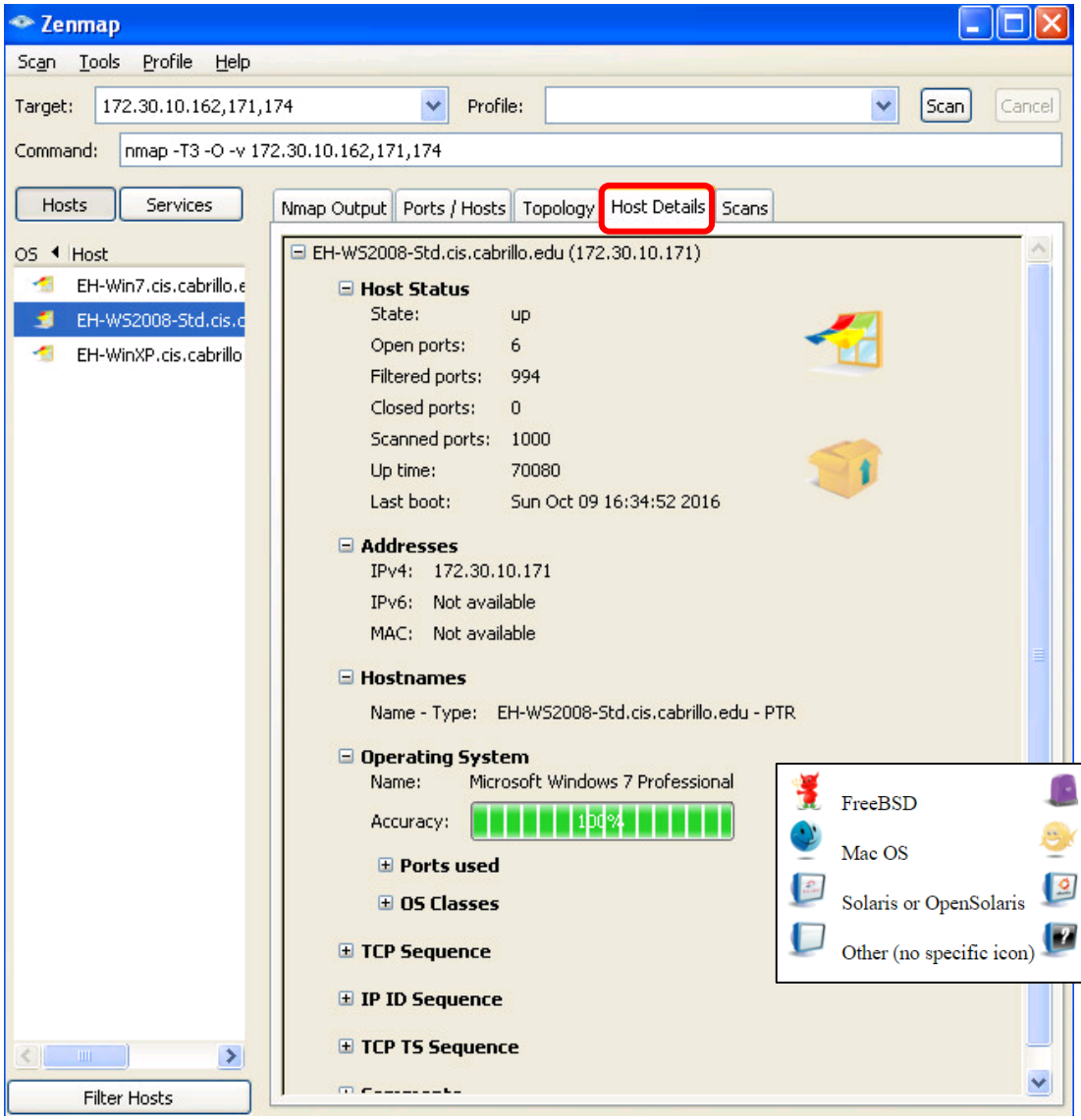
Show a network topology map

- Not port scanned
- < 3 open ports
- 3-6 open ports
- > 6 open ports

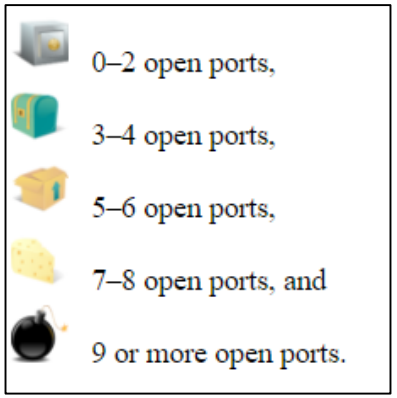
- Router
- Switch
- WAP
- Firewall
- Host with filtered ports

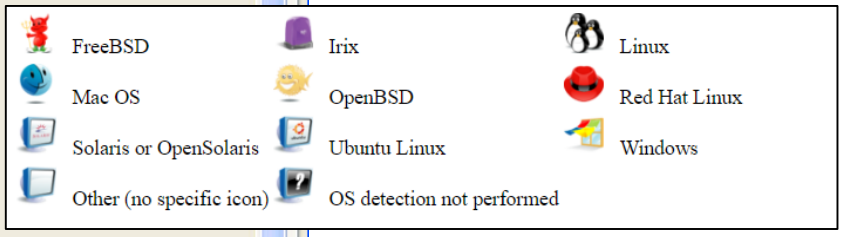
https://nmap.org/book/zenmap-topology.html#zenmap-topology-legend

nmap -T3 -O -v 172.30.10.162,170,172



Show host details



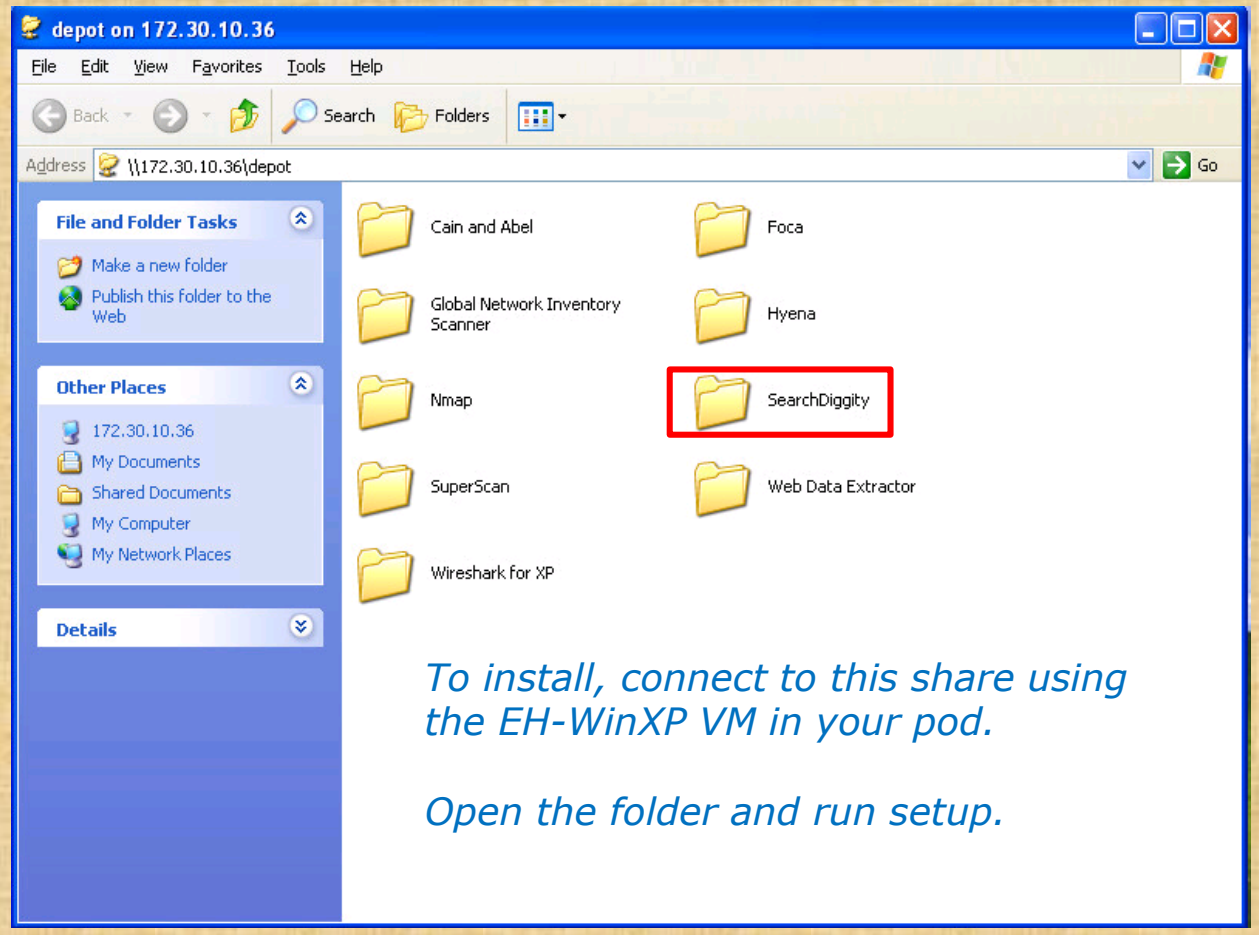


https://nmap.org/book/zenmap-topology.html#zenmap-topology-legend

Activity 1

Zenmap Installation on EH-WinXP-xx

Start > Run … > \\172.30.10.36\depot



We are not going to use SearchDiggety.

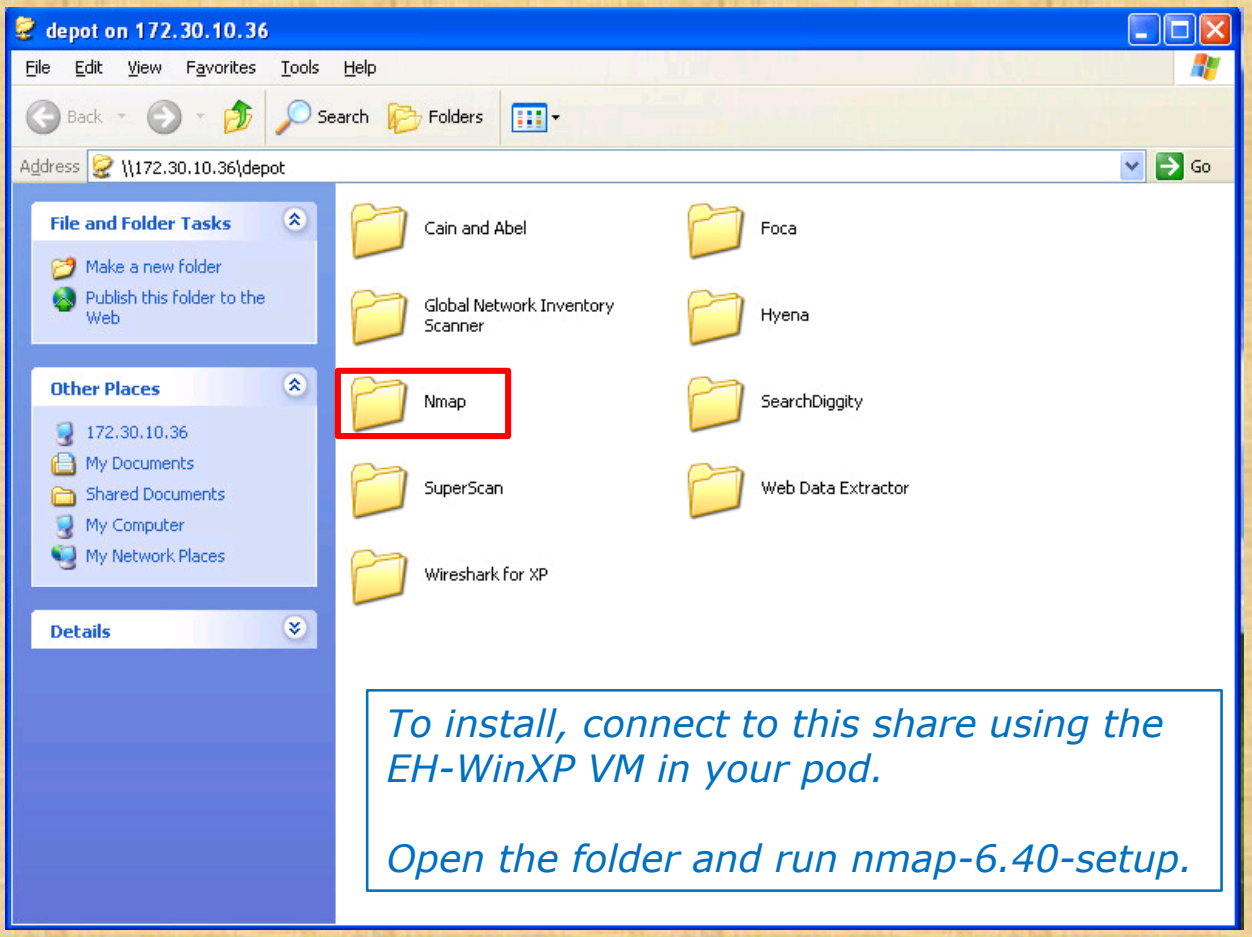
We just need to install it, even though it fails, so we have all the required libraries for Zenmap.

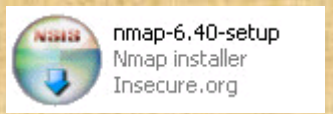
Use the chat window to indicate you have done the "failed" installation

Activity 1

Zenmap Installation on EH-WinXP-xx (continued)

Start > Run … > \\172.30.10.36\depot



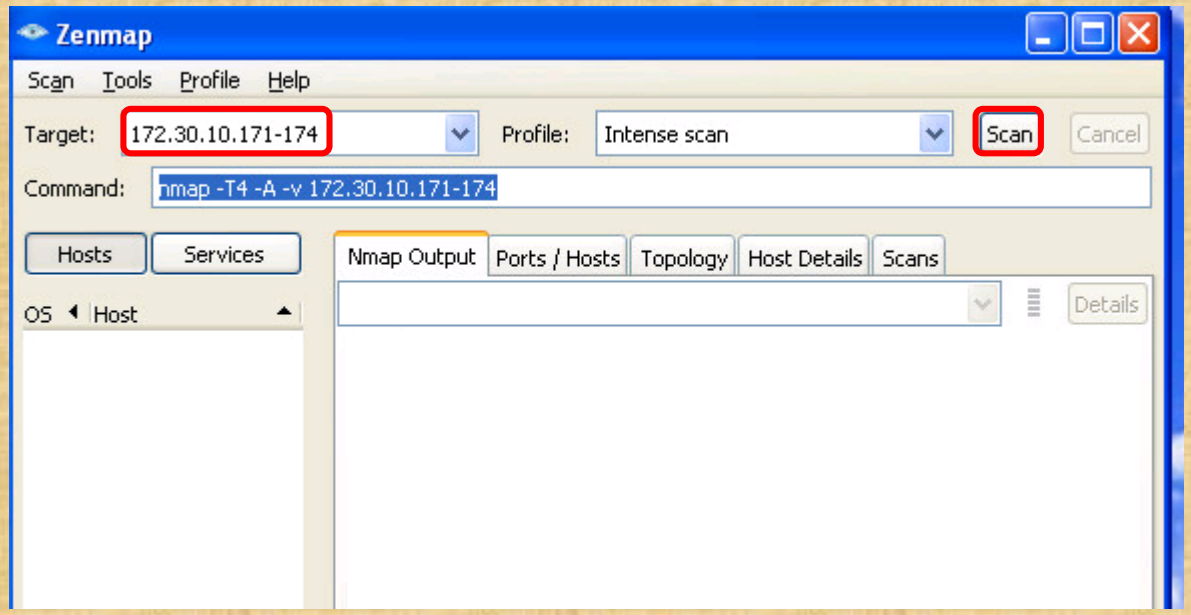


Use the chat window to indicate you have installed it

Activity 2

Scan four systems on the Microlab network

nmap -T4 -A -v 172.30.10.171-174



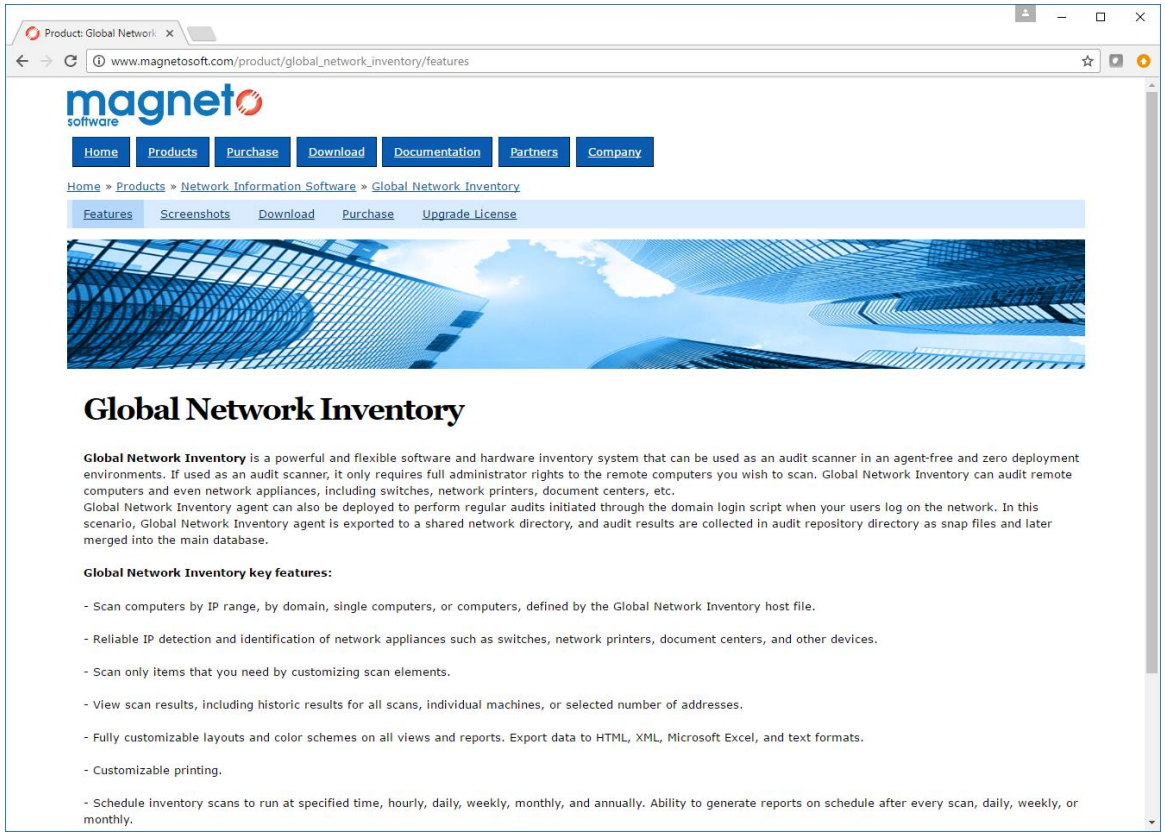
The "Intense scan" profile. -T4 has a more aggressive timing and -A uses several features including OS and version detection.

Question: Examine the "Host Details" tab host details of each host. Which host has the bomb icon (meaning nine or more open ports)?

Write the IP address of this host in the chat window.

Global Network Inventory

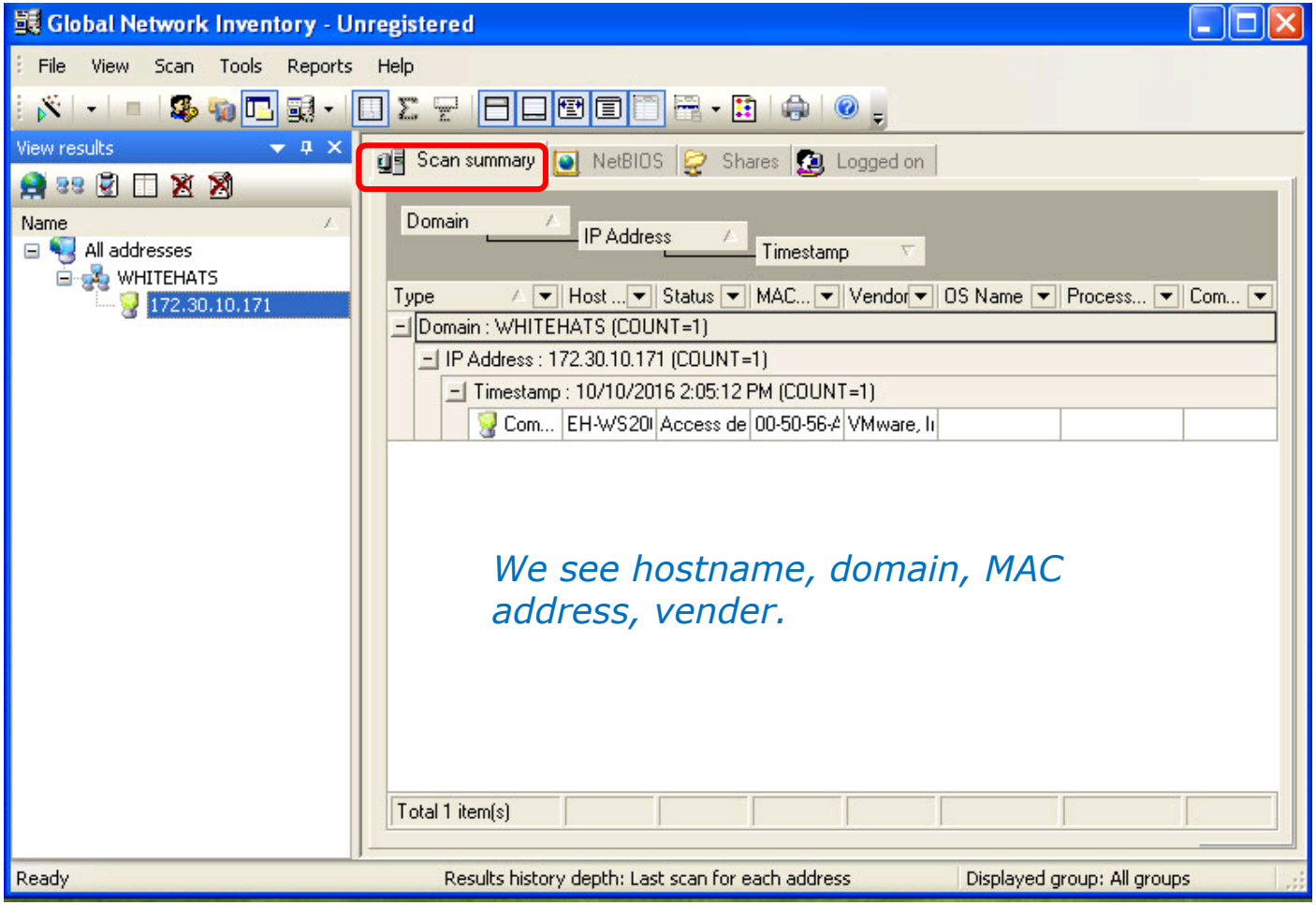
Magneto Global Network Inventory



http://www.magnetosoft.com/product/global_network_inventory/features

Magneto Global Network Inventory

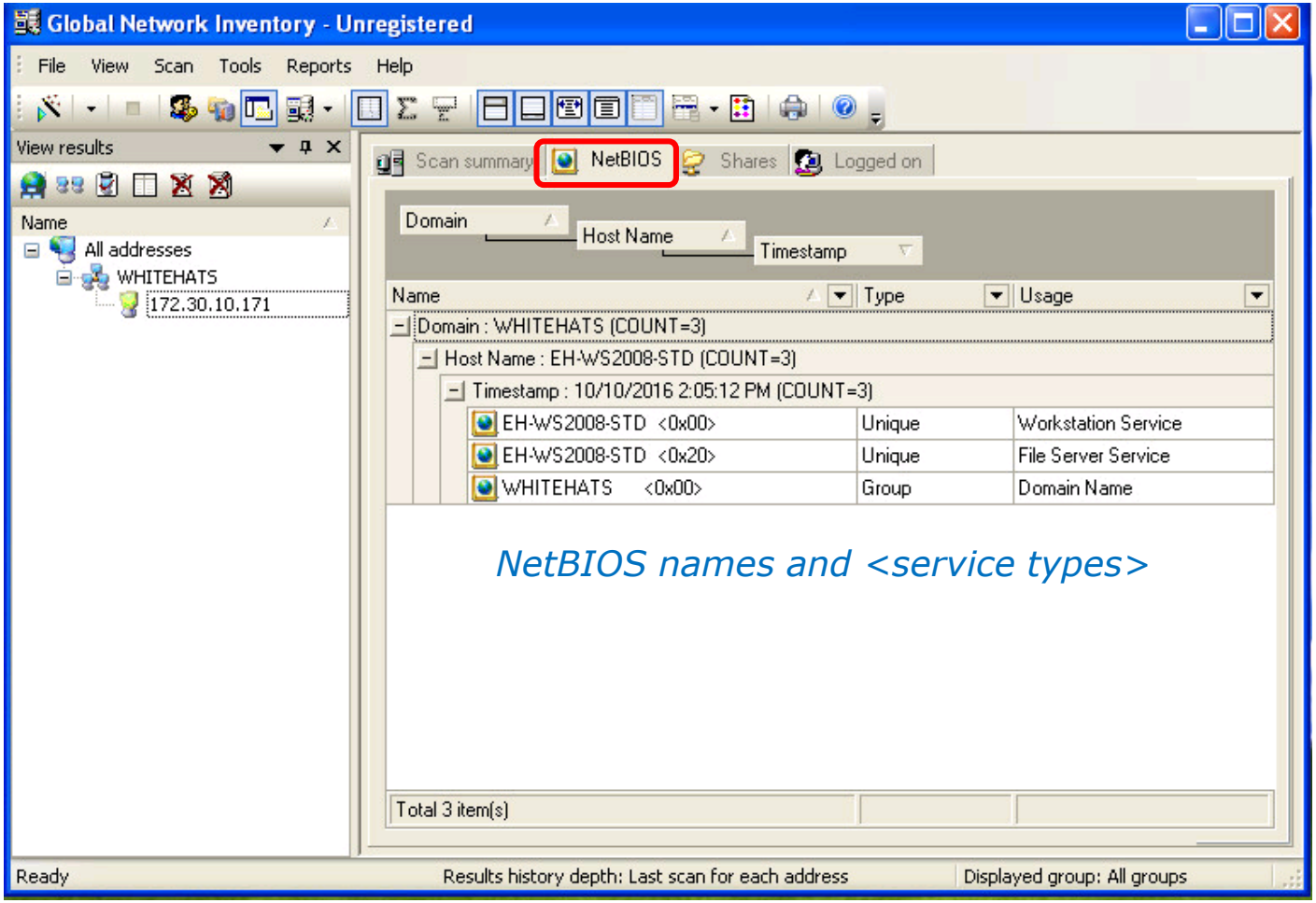
Tools > General Options > Scan Options > Logon As > Currently logged on user
Scan > New Scan > New Single Address Scan > 172.30.10.171



We see hostname, domain, MAC address, vender.

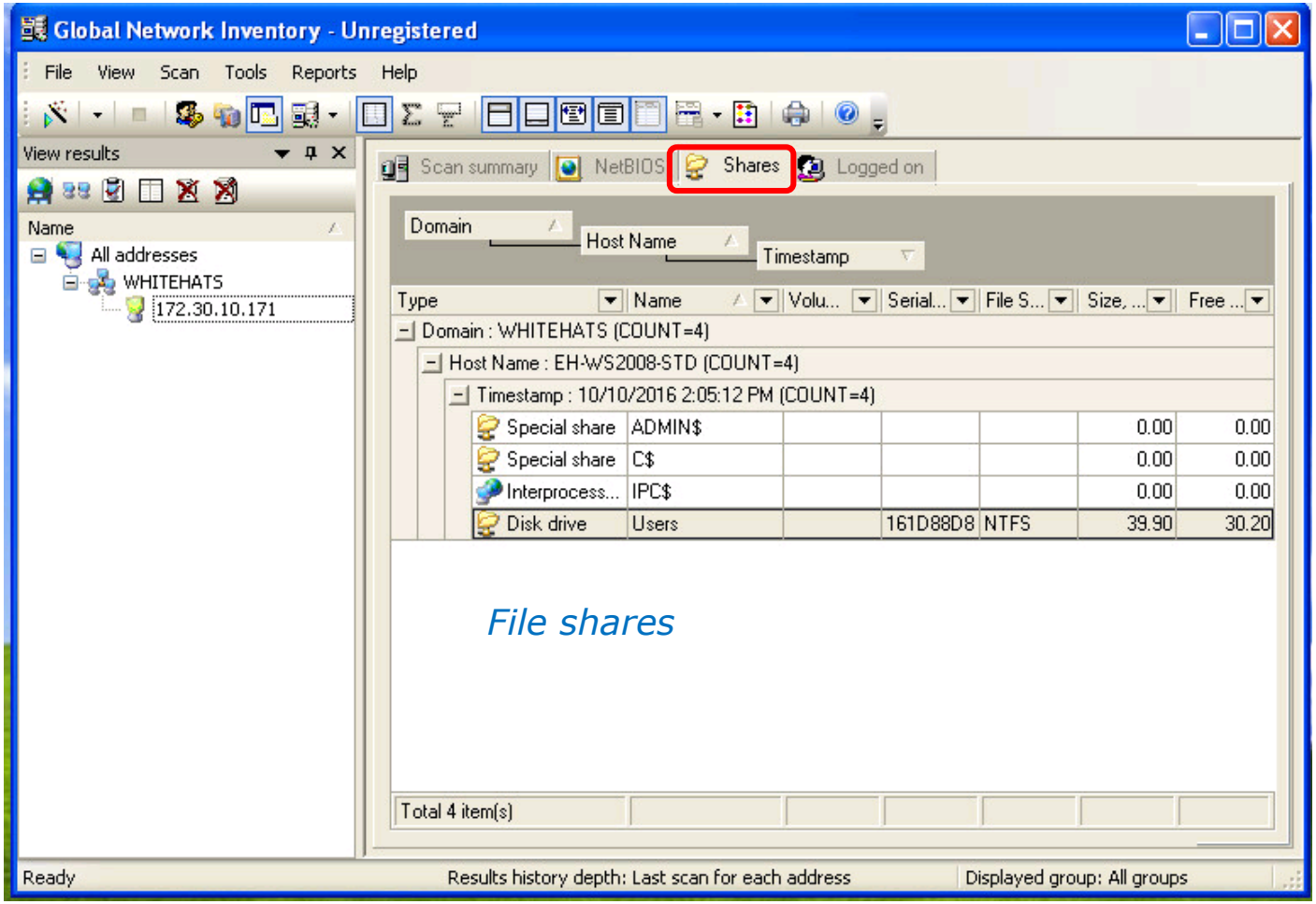
Magneto Global Network Inventory

Tools > General Options > Scan Options > Logon As > Currently logged on user
Scan > New Scan > New Single Address Scan > 172.30.10.171



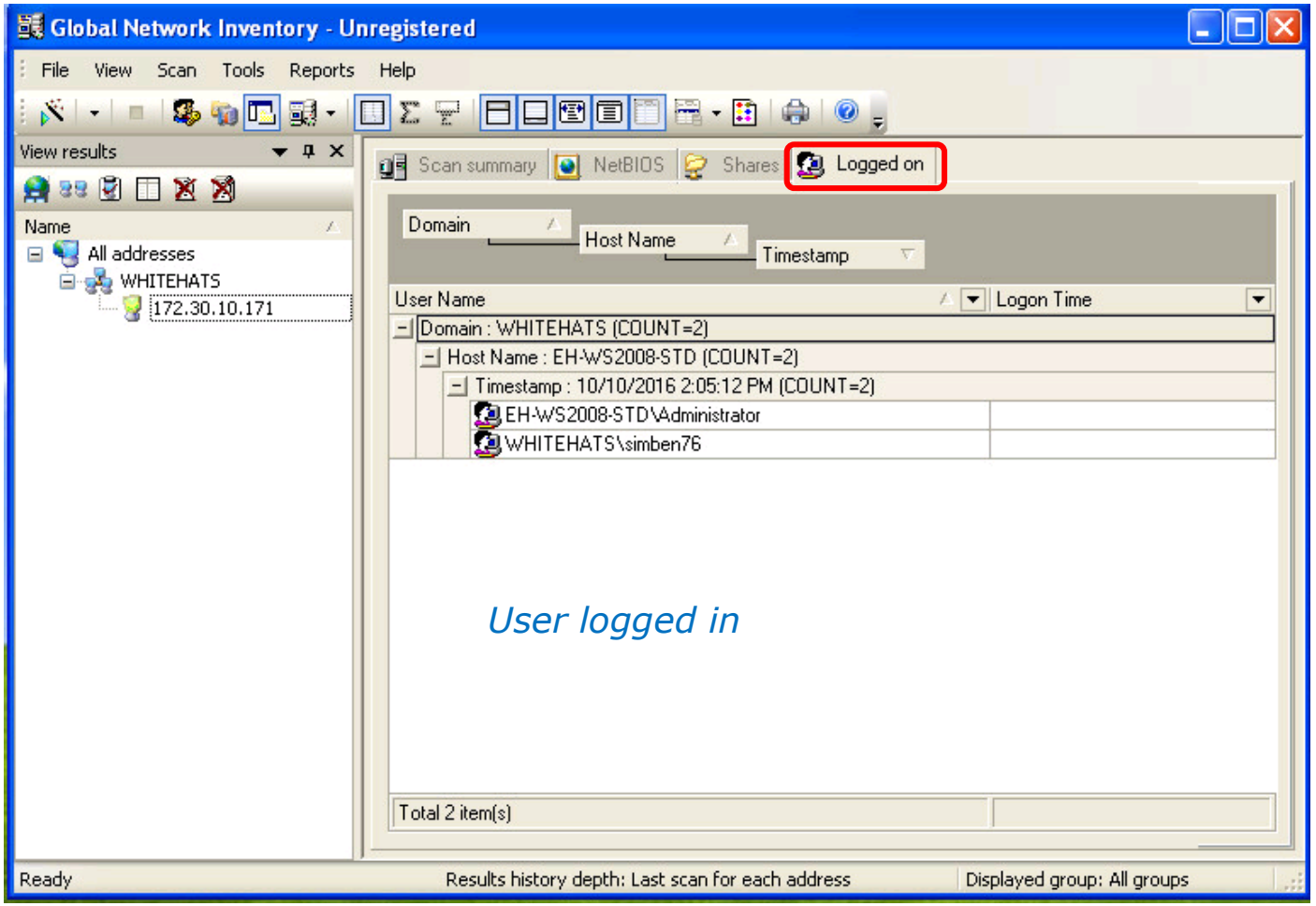
Magneto Global Network Inventory

Tools > General Options > Scan Options > Logon As > Currently logged on user
Scan > New Scan > New Single Address Scan > 172.30.10.171



Magneto Global Network Inventory

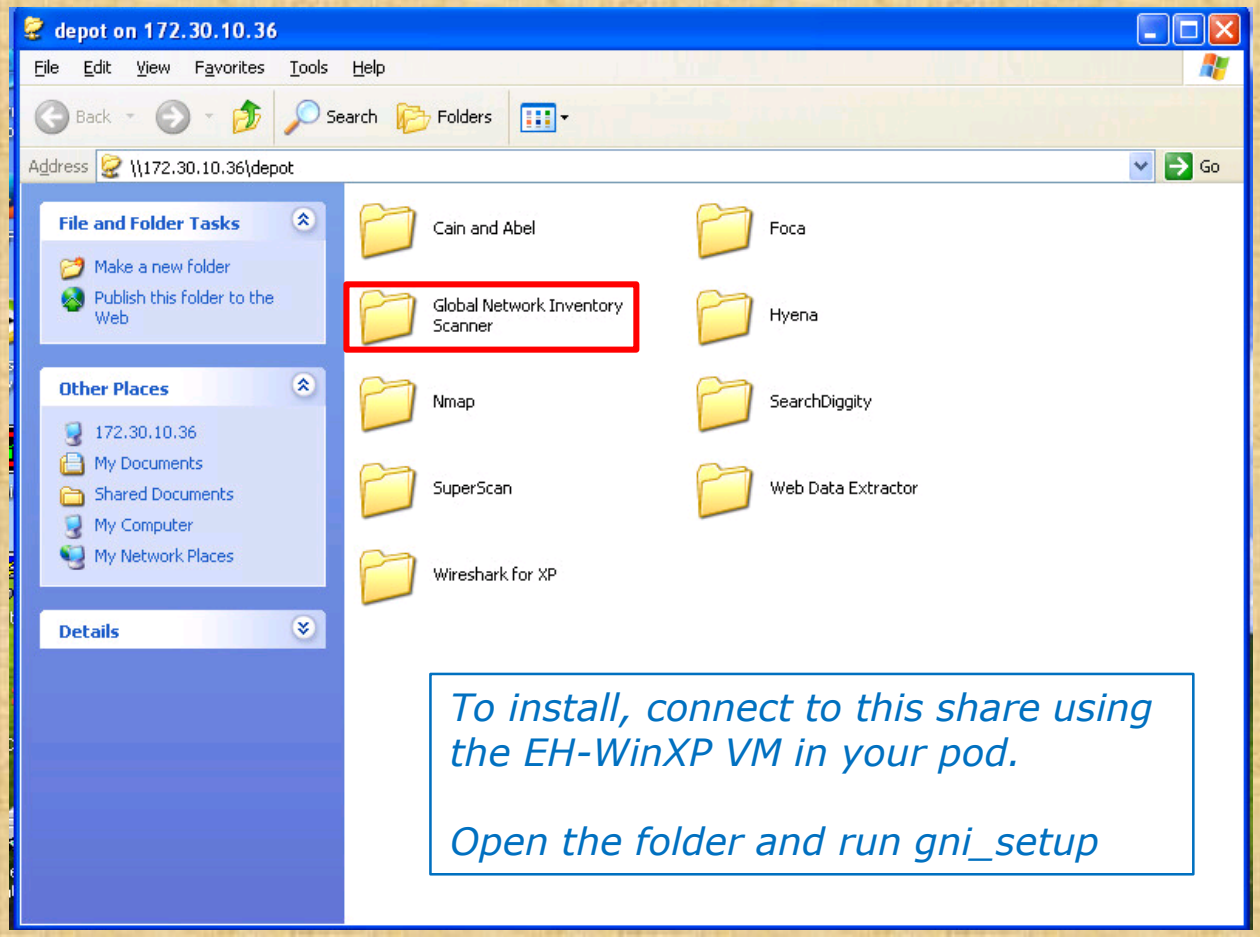
Tools > General Options > Scan Options > Logon As > Currently logged on user
Scan > New Scan > New Single Address Scan > 172.30.10.171



Activity 1

Global Network Inventory installation on EH-WinXP VM

Start > Run … > \\172.30.10.36\depot

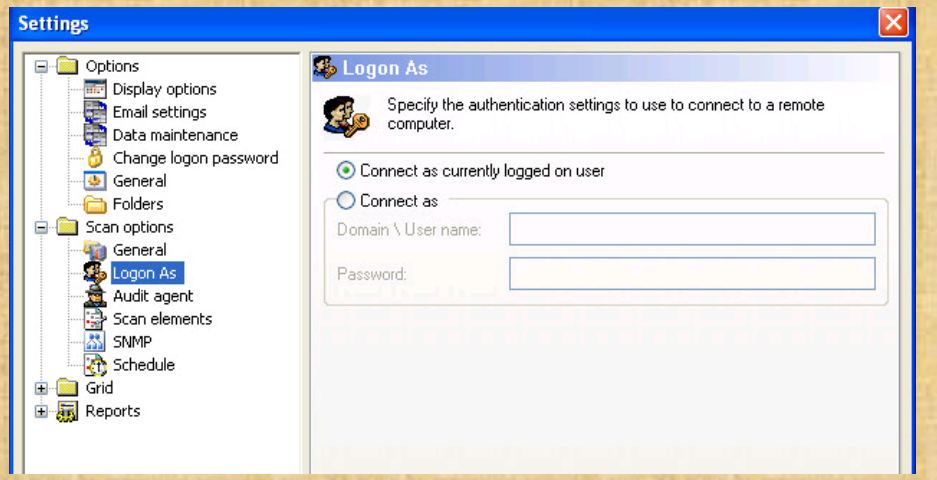


Use the chat window to indicate you have installed it

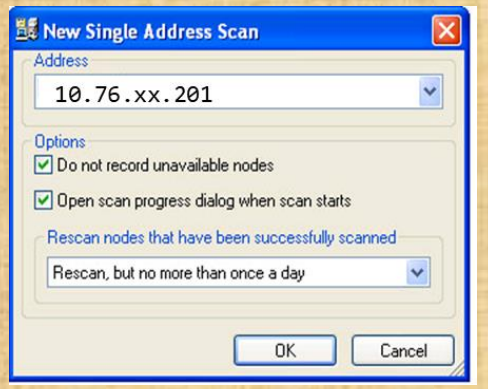
Activity 2

Inventory your pod EH-WinXP VM

1. **Tools > General Options > Scan Options > Logon As > Currently logged on user > [OK]**



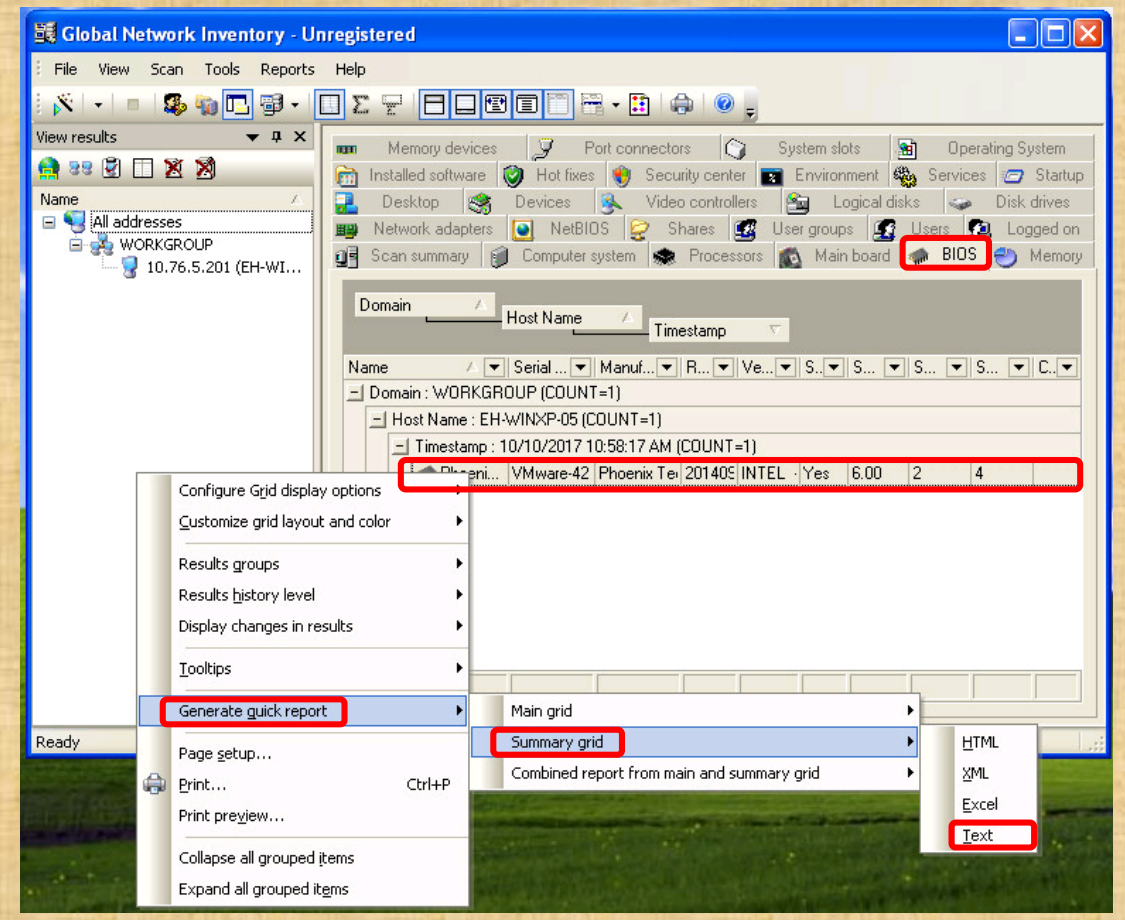
2. **Scan > New Scan > New Single Address Scan > 10.76.xx.201 > [OK]**



Let me know when you finished the scan in the chat window.

Activity 2

Inventory your pod EH-WinXP VM (continued)



3. **Select the "BIOS" tab**

4. **Right-click on the BIOS details > Generate Quick Report > Summary grid > Text**

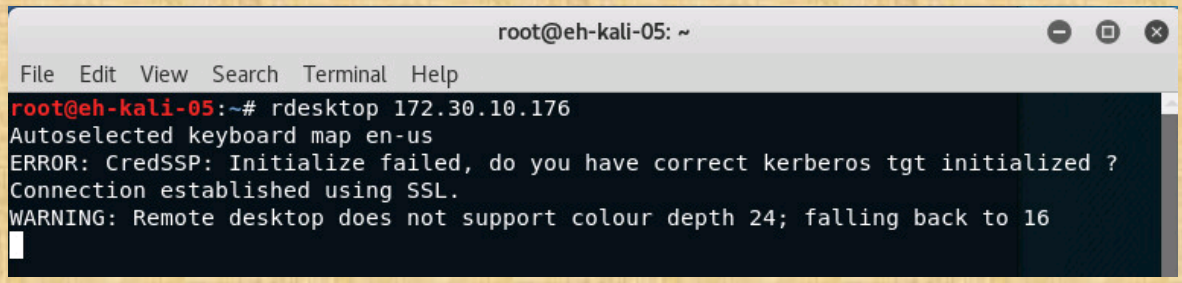
Question: What is the BIOS name and version on your EH-WinXP VM?

Write you answer in the chat window.

Remote Desktop Howto

Remote desktop from EH-Kali-xx

rdesktop 172.30.10.176

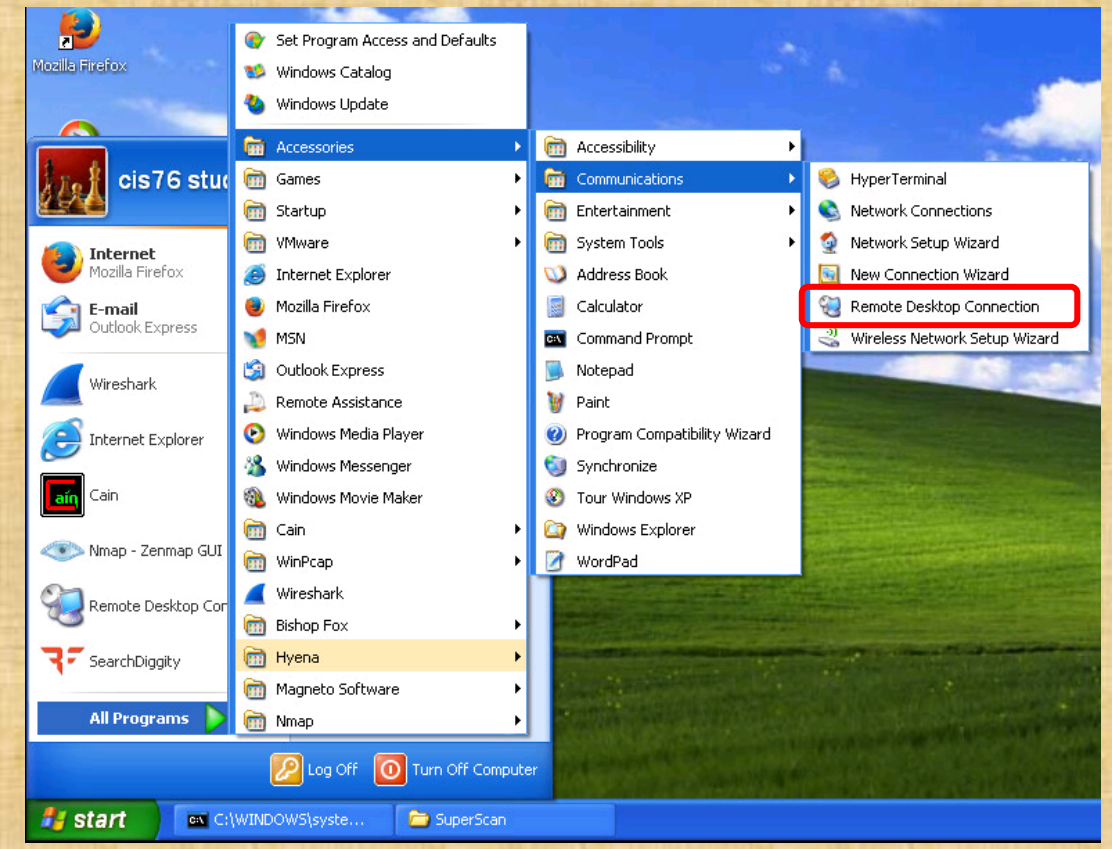


Use your original Opus-II username and password with the whitehats domain

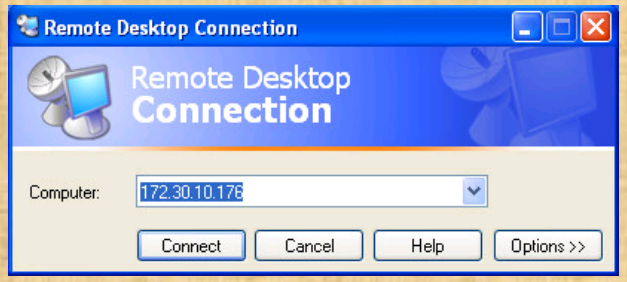
Post in the chat window when you have successfully connected using remote desktop

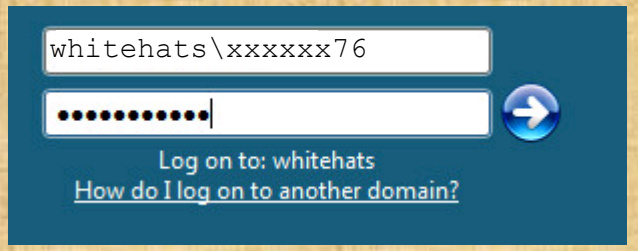
Remote desktop from EH-WinXP-xx

Start > Accessories > Communications > Remote Desktop Connection



172.30.10.176





Use your original Opus-II username and password with the whitehats domain

Post in the chat window when you have successfully connected using remote desktop

Windows nbtstat net view commands

NBTSTAT Command Syntax

Displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP).

```
NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names and their IP
                        addresses
  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via WINS
  -R   (Reload)         Purges and reloads the remote cache name table
  -S   (Sessions)       Lists sessions table with the destination IP addresses
  -s   (sessions)       Lists sessions table converting destination IP addresses to
                        computer NETBIOS names.
  -RR  (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refresh

  RemoteName   Remote host machine name.
  IP address   Dotted decimal representation of the IP address.
  interval     Redisplays selected statistics, pausing interval seconds
               between each display. Press Ctrl+C to stop redisplaying
               statistics.
```

NBTSTAT Command Examples

hostname
nbtstat -a 172.30.10.174

```
c:\>hostname
EH-WS2008-DC

c:\>nbtstat -a 172.30.10.174

Local Area Connection:
Node IpAddress: [172.30.10.176] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    EH-WINXP       <00>  UNIQUE       Registered
    WORKGROUP      <00>  GROUP        Registered
    EH-WINXP       <20>  UNIQUE       Registered
    WORKGROUP      <1E>  GROUP        Registered

    MAC Address = 00-50-56-AF-40-1F
```

From EH-WS2008-DC
Logged in as whitehats\simben76
via remote desktop

hostname
nbtstat -a 172.30.10.174

```
C:\>hostname
EH-WinXP-05

C:\>nbtstat -a 172.30.10.174

Local Area Connection:
Node IpAddress: [10.76.5.201] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    EH-WINXP       <00>  UNIQUE       Registered
    WORKGROUP      <00>  GROUP        Registered
    EH-WINXP       <20>  UNIQUE       Registered
    WORKGROUP      <1E>  GROUP        Registered

    MAC Address = 00-50-56-AF-40-1F
```

From pod EH-WinXP VM
Logged in as the cis76 student

<00> = computer name, <20> = server service (to share files),
<1E> = browser services election is running

NBTSTAT Command Examples

nbtstat -a 172.30.10.172

```
C:\Users\simben76>nbtstat -a 172.30.10.172

Local Area Connection:
Node IpAddress: [172.30.10.171] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    EH-WS2012-DC   <00>  UNIQUE      Registered
    WHITEHATS      <00>  GROUP       Registered
    WHITEHATS      <1C>  GROUP       Registered
    EH-WS2012-DC   <20>  UNIQUE      Registered
    WHITEHATS      <1B>  UNIQUE      Registered

    MAC Address = 00-50-56-A0-FE-FC

C:\Users\simben76>_
```

From EH-WS2008-DC
Logged in as whitehats\simben76
via remote desktop

```
C:\>nbtstat -a 172.30.10.172

Local Area Connection:
Node IpAddress: [10.76.5.201] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    EH-WS2012-DC   <00>  UNIQUE      Registered
    WHITEHATS      <00>  GROUP       Registered
    WHITEHATS      <1C>  GROUP       Registered
    EH-WS2012-DC   <20>  UNIQUE      Registered
    WHITEHATS      <1B>  UNIQUE      Registered

    MAC Address = 00-50-56-A0-FE-FC

C:\>
```

From pod EH-WinXP VM
Logged in as cis76 student

<00> = computer name, <1C> = domain controller,
<20> = server service (to share files), <1B> = a domain master browser

Name	Number (HEX)	Type	Usage
<computername>	00	U	Workstation Service
<computername>	01	U	Messenger Service
<_MSBROWSE_>	01	G	Master Browser
<computername>	03	U	Messenger Service
<computername>	06	U	RAS Server Service
<computername>	1F	U	NetDDE Service
<computername>	20	U	File Server Service
<computername>	21	U	RAS Client Service
<computername>	22	U	Exchange Interchange
<computername>	23	U	Exchange Store
<computername>	24	U	Exchange Directory
<computername>	30	U	Modem Sharing Server Service
<computername>	31	U	Modem Sharing Client Service
<computername>	43	U	SMS Client Remote Control
<computername>	44	U	SMS Admin Remote Control Tool
<computername>	45	U	SMS Client Remote Chat
<computername>	46	U	SMS Client Remote Transfer
<computername>	4C	U	DEC Pathworks TCPIP Service
<computername>	52	U	DEC Pathworks TCPIP Service
<computername>	87	U	Exchange MTA
<computername>	6A	U	Exchange IMC
<computername>	BE	U	Network Monitor Agent
<computername>	BF	U	Network Monitor Apps
<username>	03	U	Messenger Service
<domain>	00	G	Domain Name
<domain>	1B	U	Domain Master Browser
<domain>	1C	G	Domain Controllers
<domain>	1D	U	Master Browser
<domain>	1E	G	Browser Service Elections
<INet~Services>	1C	G	Internet Information Server
<IS~Computer_name>	00	U	Internet Information Server

NetBIOS Suffix Code Table

http://www.pyeung.com/pages/microsoft/winnt/netbioscodes.html

NET VIEW Command Syntax

Displays shared resources

```
NET VIEW [\\computername [/CACHE] | [/ALL] | /DOMAIN[:domainname]]
```

Syntax varies by version of Windows

NET VIEW Command Examples

net view

```
c:\>net view
Server Name            Remark

\\EH-WIN7              Windows 7 (shared PC)
\\EH-WIN81             EH Shared Windows computer
\\EH-WS2008-STD        EH Windows Server 2008 R2
\\EH-WS2012-DC
The command completed successfully.


c:\>_
```

From EH-WS2008-DC
Logged in as whitehats\simben76
via remote desktop

net view

```
C:\>net view
Server Name            Remark

\\EH-WIN7-05
\\EH-WINXP-05
\\OWASPBWA             owaspbwa server (Samba, Ubuntu)
The command completed successfully.


C:\>_
```

From pod EH-WinXP VM
Logged in as cis76 student

NET VIEW Command Examples

net view /domain:workgroup

```
c:\>net view /domain:workgroup
Server Name            Remark

------------------------------------------------------------------------------
\\DESKTOP-LEMM0OD
\\EH-WINXP
\\EH-WS2003
\\EH-WS2008-ENT
\\MASTER-CYLINDER
\\METASPLOITABLE       metasploitable server (Samba 3.0.20-Debian)
The command completed successfully.
```

From EH-WS2008-DC
Logged in as whitehats\simben76
via remote desktop

net view /domain:workgroup

```
C:\>net view /domain:workgroup
Server Name                Remark

------------------------------------------------------------------------------
\\EH-WIN7-05
\\EH-WINXP-05
\\OWASPBWA                 owaspbwa server (Samba, Ubuntu)
The command completed successfully.
```

From pod EH-WinXP VM
Logged in as cis76 student

NET VIEW Command Examples

net view \\172.30.10.174 /ALL

```
c:\>c:\net view ?
'c:\net' is not recognized as an internal or external command,
operable program or batch file.

c:\>net view \\172.30.10.174 /all
Shared resources at \\172.30.10.174


Share name        Type  Used as  Comment

-------------------------------------------------------------------------------
ADMIN$            Disk           Remote Admin
C$                Disk           Default share
Doanld-Pictures   Disk
Documents         Disk
Hillary-Pictures  Disk
IPC$              IPC            Remote IPC
The command completed successfully.
```

From EH-WS2008-DC
Logged in as whitehats\simben76
via remote desktop

net view \\172.30.10.174

```
C:\>net view ?
The syntax of this command is:


NET VIEW
[\\computername [/CACHE] | /DOMAIN[:domainname]]
NET VIEW /NETWORK:NW [\\computername]


C:\>net view \\172.30.10.174
Shared resources at \\172.30.10.174


Share name        Type  Used as  Comment

-------------------------------------------------------------------------------
Doanld-Pictures   Disk
Documents         Disk
Hillary-Pictures  Disk
The command completed successfully.
```

From pod EH-WinXP VM
Logged in as cis76 student

NET VIEW Command Examples

net view \\172.30.10.172 /ALL

```
c:\>net view \\172.30.10.172 /ALL
Shared resources at \\172.30.10.172


Share name   Type   Used as   Comment

-------------------------------------------------------------------------------
ADMIN$       Disk             Remote Admin
C$           Disk             Default share
IPC$         IPC              Remote IPC
NETLOGON     Disk             Logon server share
SYSVOL       Disk             Logon server share
The command completed successfully.
```

From EH-WS2008-DC
Logged in as whitehats\simben76
via remote desktop

net view \\172.30.10.172

```
C:\>net view \\172.30.10.174
Shared resources at \\172.30.10.174


Share name         Type   Used as   Comment

-------------------------------------------------------------------------------
Doanld-Pictures    Disk
Documents          Disk
Hillary-Pictures   Disk
The command completed successfully.


C:\>net view \\172.30.10.172
System error 5 has occurred.

Access is denied.
```

From pod EH-WinXP VM
Logged in as cis76 student

Activity 1
NBTSTAT and NET VIEW commands

1. Remote desktop from either your pod Kali or WinXP VM to 172.30.10.176.
   Kali: rdesktop <*ip address*>
   WinXP: Start > All Programs > Accessories > Communications > Remote Desktop Connection

2. Log in as whitehats\xxxxxx76
   (where xxxxxx76 is your Opus-II username with your original Opus-II password)

3. From 172.30.10.176, view the members of the workgroup named WORKGROUP
   `net view /domain:workgroup`

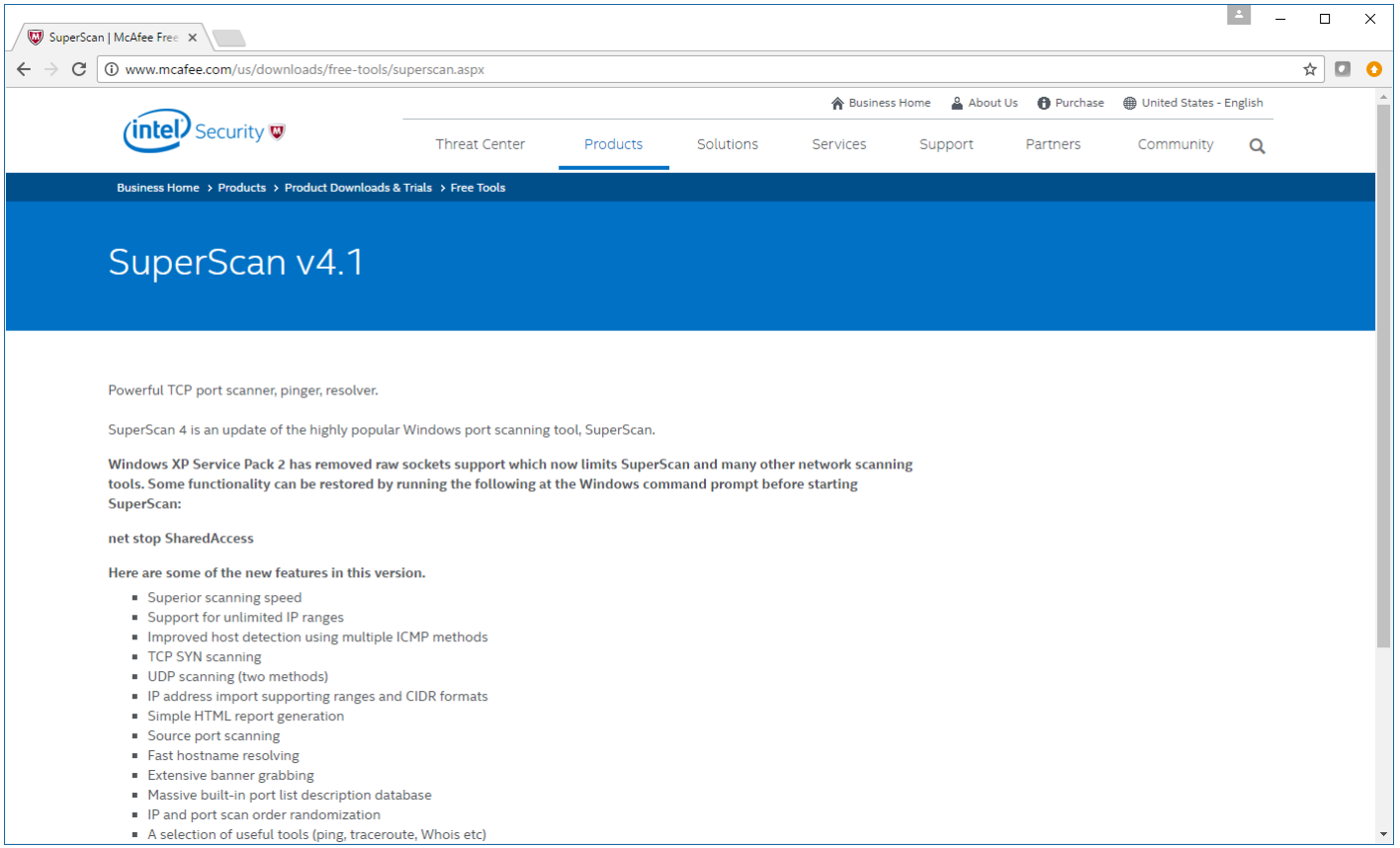
4. Look for a system whose name ends with "-ENT" and get its MAC address
   `nbtstat -a eh-??????-ent`

Question: What is the name of this system and its MAC address?

Write your answer in the chat window.

SuperScan

SuperScan



http://www.mcafee.com/us/downloads/free-tools/superscan.aspx

SuperScan

Superscan

From Wikipedia, the free encyclopedia

This article **relies too much on references to primary sources**. Please improve this by adding secondary or tertiary sources. *(April 2010) (Learn how and when to remove this template message)*

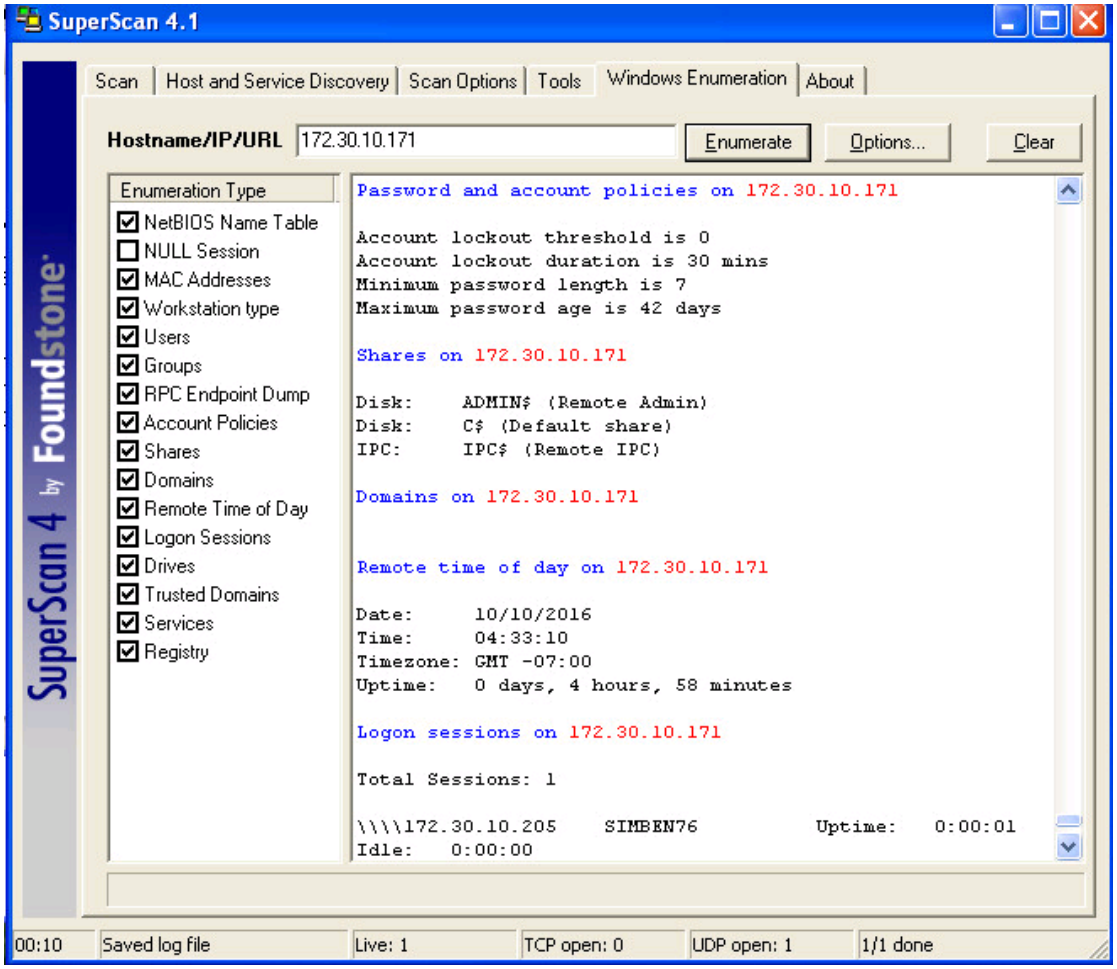
SuperScan is a free connect-based port scanning software designed to detect open TCP and UDP ports on a target computer, determine which services are running on those ports, and run queries such as whois, ping, ICMP traceroute, and Hostname lookups.[1]

Superscan 4, which is a completely rewritten update to the other Superscan (version 3, released in 2000), features windows enumeration, which can list a variety of important information dealing with Microsoft Windows such as:

- NetBIOS information
- User and Group Accounts
- Network shares
- Trusted Domains
- Services - which are either running or stopped

https://en.wikipedia.org/wiki/Superscan

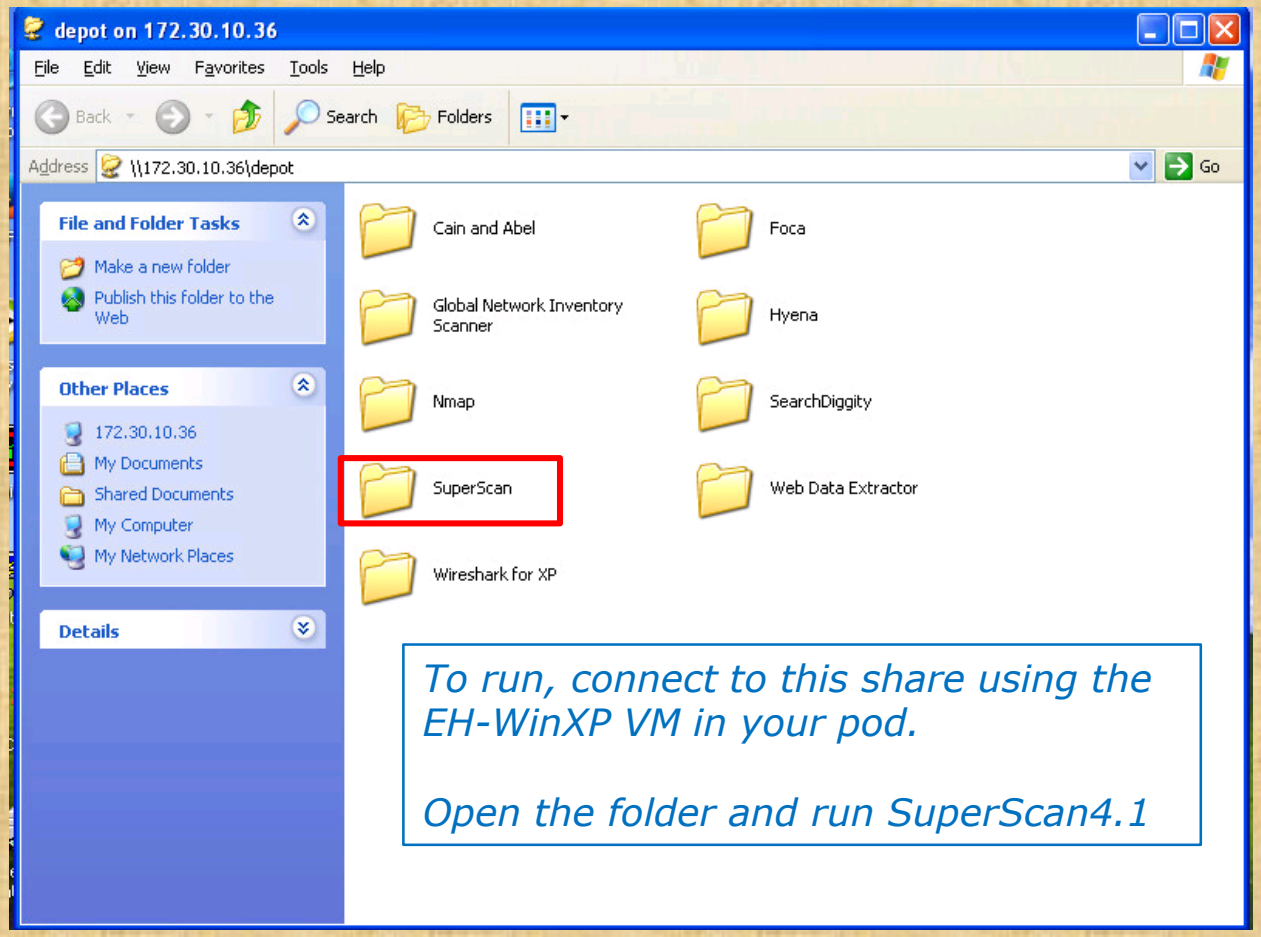
SuperScan 4.1 by Foundstone



http://www.mcafee.com/us/downloads/free-tools/superscan.aspx

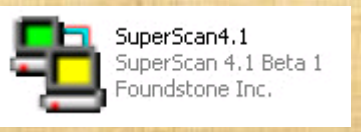
Activity 1
Run SuperScan on your EH-WinXP VM

Start > Run … > \\172.30.10.36\depot



To run, connect to this share using the EH-WinXP VM in your pod.

Open the folder and run SuperScan4.1



Use the chat window to indicate you have installed it

Activity 2
Enumerate 172.30.10.171

1. Run SuperScan on your EH-WinXP system.
2. Click the Windows Enumeration tab.
3. For hostname/IP enter 172.30.10.171
4. Deselect NULL Session (we will use our credentials instead)
5. Click Options button and enter your "Opus-II" username, original "Opus-II" password, and whitehats as the domain. Click OK to accept.
6. Click the Enumerate button.

Question: Look at the local user accounts on this system. Between Carmen and Sylvester, who logged in last?

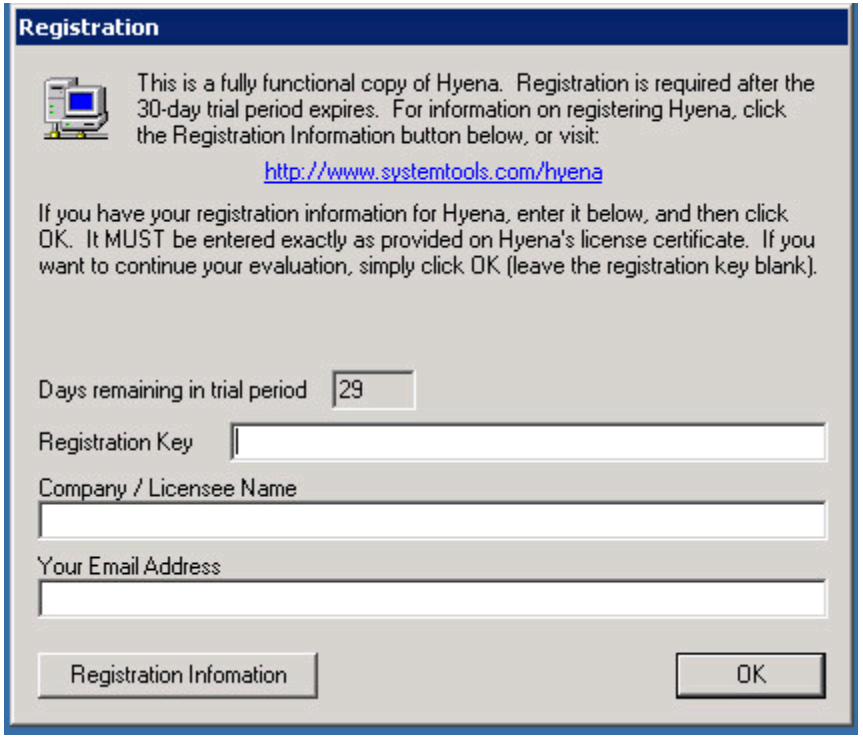
Write your answer in the chat window.

Hyena

Hyena

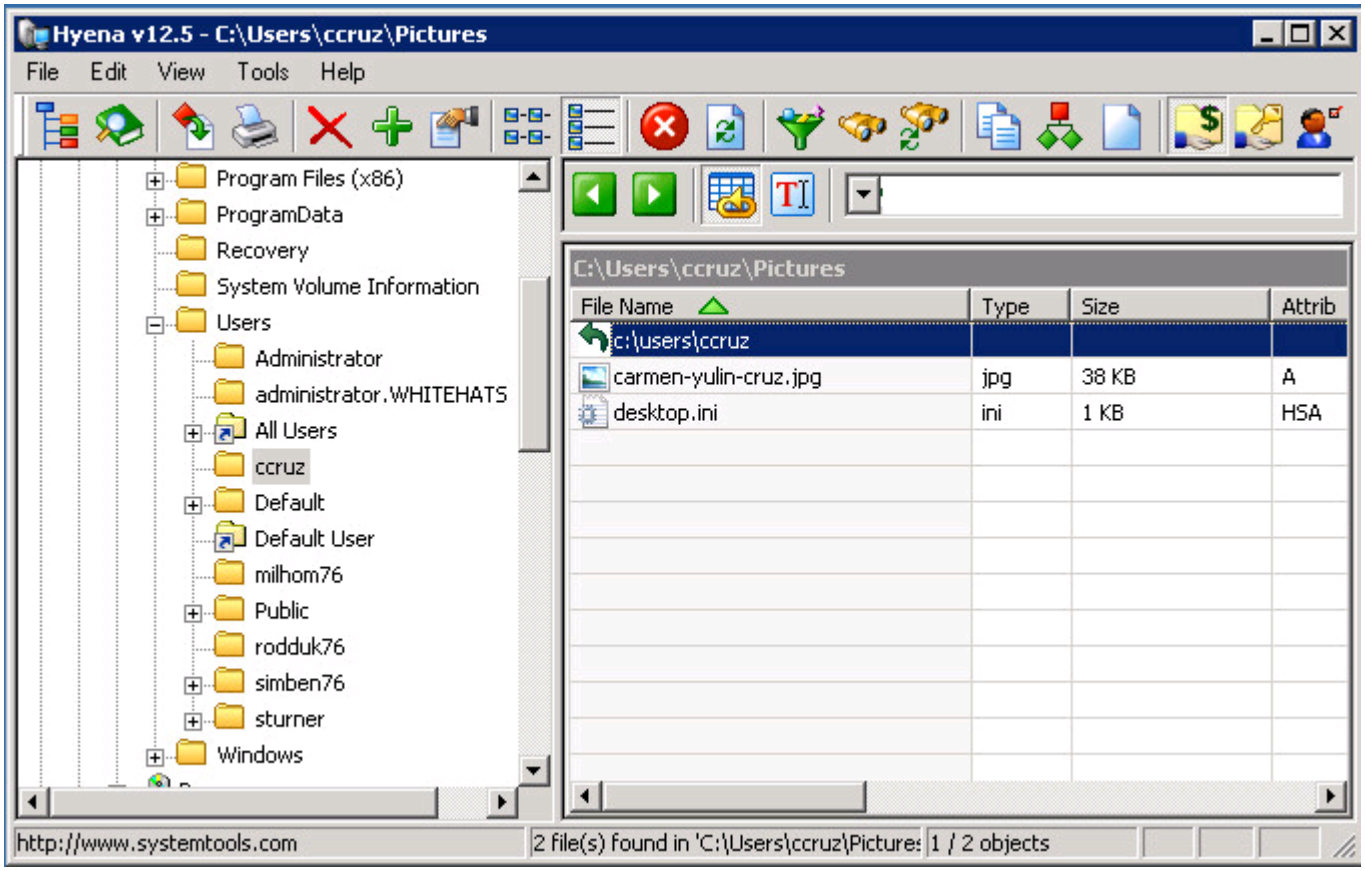
http://www.systemtools.com/hyena/

Hyena



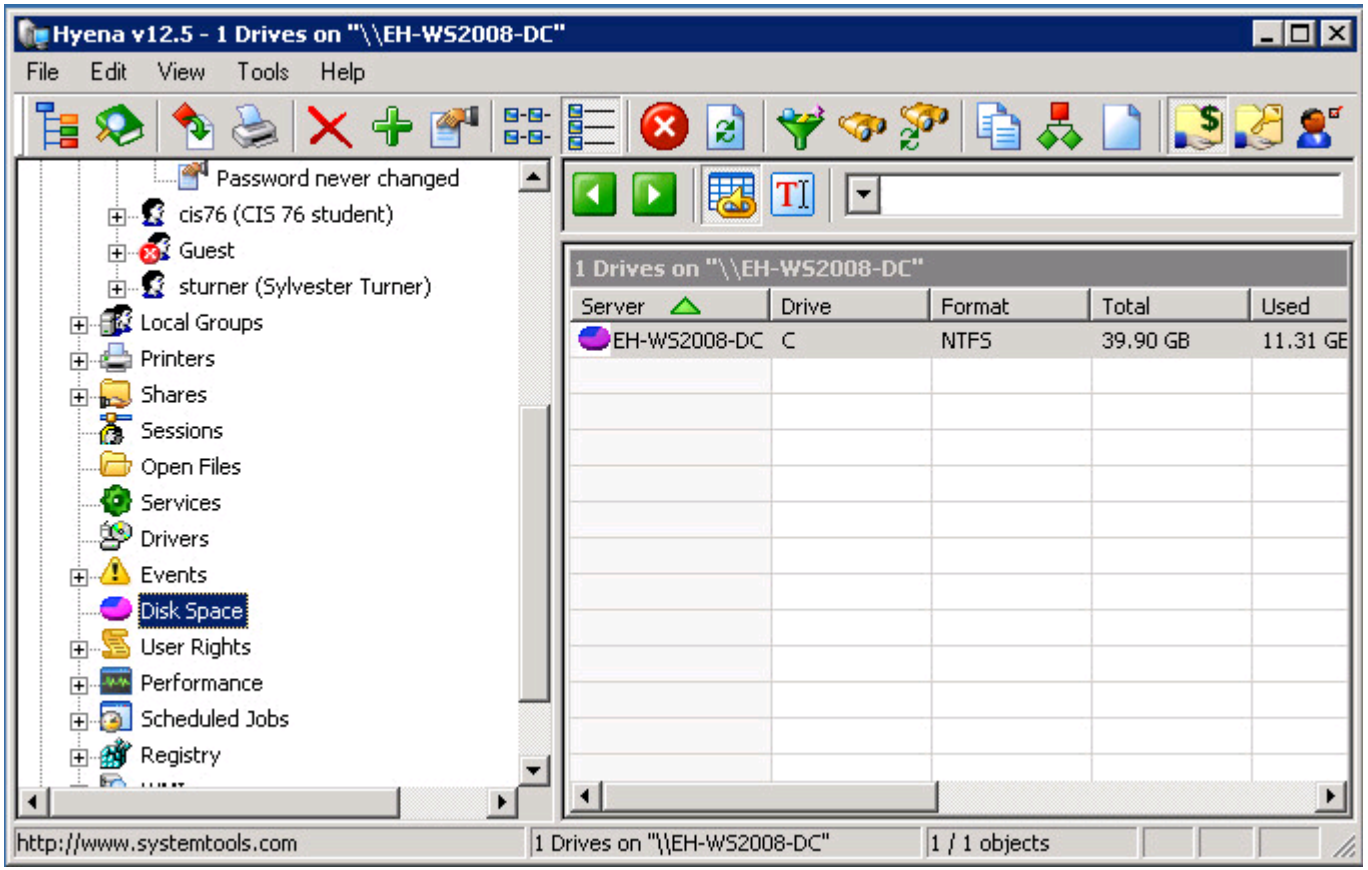
For the 30-day evaluation, just click OK to continue

Hyena



http://www.systemtools.com/index.html

Hyena



Use the explorer style interface to browse the collected information

Hyena

1. Remote desktop from either your pod Kali or WinXP VM to 172.30.10.176.
   Kali: rdesktop <*ip address*>
   WinXP: Start > All Programs > Accessories > Communications > Remote Desktop Connection

2. Log in as whitehats\xxxxxx76
   (where xxxxxx76 is your Opus-II username with your original Opus-II password)

3. Run hyena

4. Expand WHITEHATS.

5. Expand All Users and find your account.

6. Expand your account.

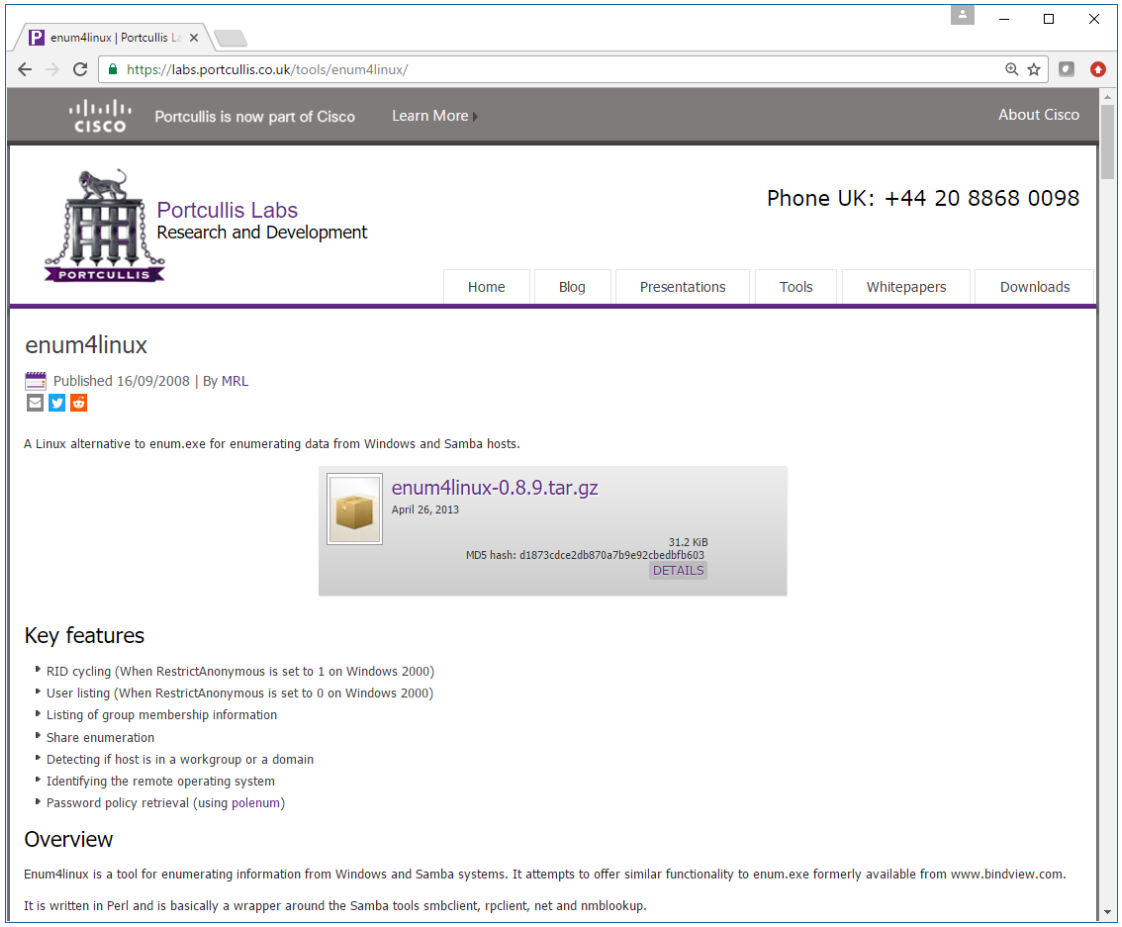
7. Expand Groups.

Question: Besides the Domain Users group, what other groups do you belong to?

Write your answer in the chat window.

enum4linux

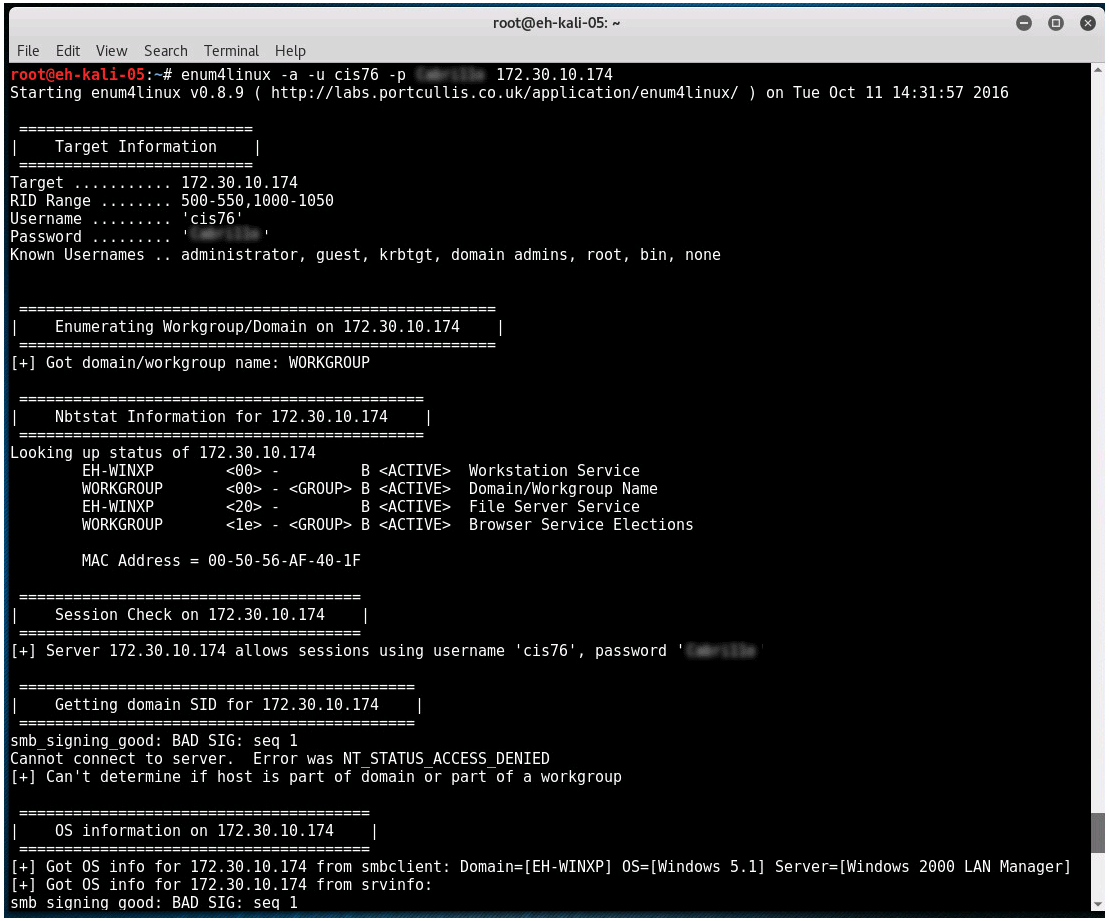
enum4linux



https://labs.portcullis.co.uk/tools/enum4linux/

enum4linux

enum4linux -a -u cis76 -p xxxxxx 172.30.10.174



https://labs.portcullis.co.uk/tools/enum4linux/

enum4Linux

1. Login to your pod Kali VM
2. Bring up a terminal.
3. enum4linux -a -u cis76 -p [redacted] 172.30.10.174
4. Review the sharenames section of the output.

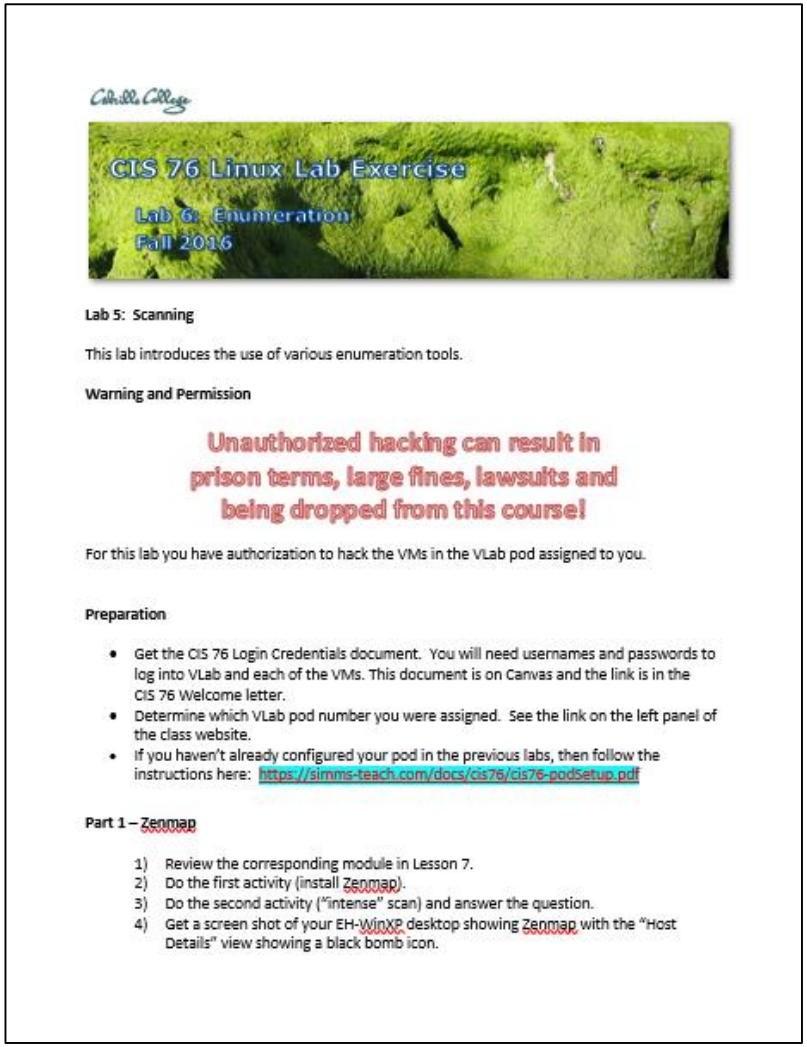
Question: What are the two sharenames that end in "-pics"?

Textbook likes the finger command

```
[rsimms@oslab ~]$ finger
Login      Name            Tty      Idle  Login Time   Office     Office Phone
cis90      CIS90 Student   pts/14     6d  Oct  5 14:13 (2607:f380:80f:f830::90:168)
frocar76   Carter Frost    pts/0      45  Oct 11 13:45 (hawknet-wireless-gw-ext.cabrillo.edu)
frocar76   Carter Frost    pts/4    2:26  Oct 11 12:24 (hawknet-wireless-gw-ext.cabrillo.edu)
rsimms     Rich Simms     *pts/7          Oct  3 08:49 (2601:647:cb80:1ea4:d9b:df45:d753:e88c)
yourya191  Ryan Young      pts/3    2:24  Oct 11 12:07 (2602:306:836d:860:4c0:d778:94d1:28f9)
```

```
[rsimms@oslab ~]$ finger cis90
Login: cis90                            Name: CIS90 Student
Directory: /home/cis90/cis              Shell: /bin/bash
On since Wed Oct  5 14:13 (PDT) on pts/14 from 2607:f380:80f:f830::90:168
   6 days idle
New mail received Wed Oct  5 15:00 2016 (PDT)
     Unread since Fri Aug 19 12:07 2016 (PDT)
Plan:
To pass this course with flying colors!
[rsimms@oslab ~]$
```


Assignment



Cabrillo College

CIS 76 Linux Lab Exercise

Lab 6: Enumeration
Fall 2016

Lab 5: Scanning

This lab introduces the use of various enumeration tools.

Warning and Permission

Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this lab you have authorization to hack the VMs in the VLab pod assigned to you.

Preparation

- Get the CIS 76 Login Credentials document. You will need usernames and passwords to log into VLab and each of the VMs. This document is on Canvas and the link is in the CIS 76 Welcome letter.
- Determine which VLab pod number you were assigned. See the link on the left panel of the class website.
- If you haven't already configured your pod in the previous labs, then follow the instructions here: https://simms-teach.com/docs/cis76/cis76-podSetup.pdf

Part 1 – Zenmap

1) Review the corresponding module in Lesson 7.
2) Do the first activity (install Zenmap).
3) Do the second activity ("intense" scan) and answer the question.
4) Get a screen shot of your EH-WinXP desktop showing Zenmap with the "Host Details" view showing a black bomb icon.

Lab 6 due next week


Wrap up

Next Class

Assignment: Check the Calendar Page on the web site to see what is due next week.

Lab 6 and five posts

Quiz questions for next class:

- What does the NetBIOS suffix code <44> signify?
- What is a NetBIOS null session?
- The network security expert who developed nmap goes by a pseudonym or "handle". This handle was inspired by which Russian novelist?

Backup