



Last updated 10/10/2017

Rich's lesson module checklist

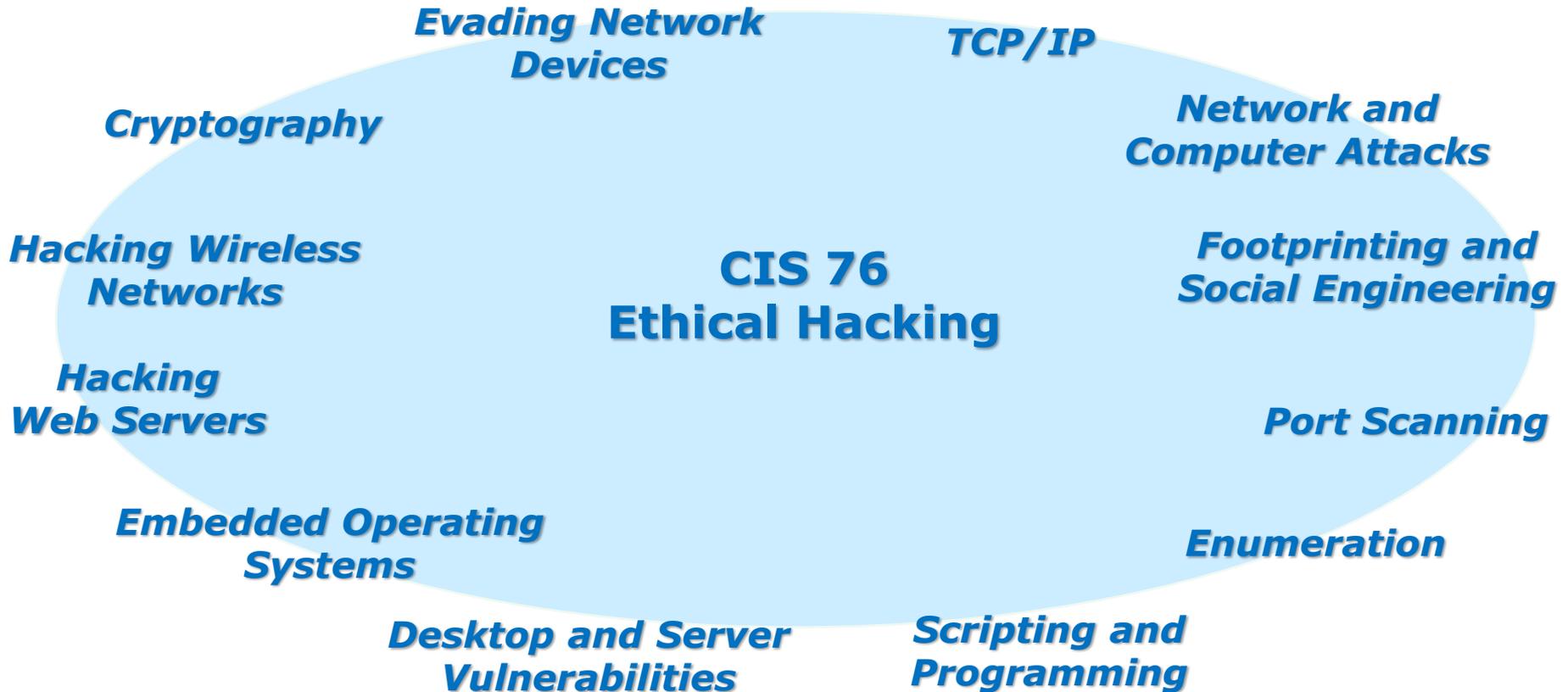
- Slides and lab posted
- WB converted from PowerPoint
- Print out agenda slide and annotate page numbers

- 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

The screenshot shows a web browser window with the URL simms-teach.com/cis90calendar.php. The page title is "Rich's Cabrillo College CIS Classes CIS 90 Calendar". There are navigation tabs for "Calendar" (highlighted), "Course Dates", and "Genda". A sidebar on the left lists various CIS courses, with "CIS 76" highlighted. The main content area shows a table for "CIS 90 (Fall 2014) Calendar" with columns for "Lesson", "Date", "Topics", and "Link". The "Topics" column for Lesson 76 includes "Class and Linux Overview", "Methods", "Supplemental", "Assignments", and "Lab 1". A link for "Presentation slides (download)" is highlighted in the "Link" column. At the bottom of the page, there is a link for "Enter virtual classroom" also highlighted.

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

The screenshot displays a virtual classroom interface. On the left is a Blackboard course page for 'Rich's Cabrillo College CIS 90 Classes'. The main area shows a 'Class Activity - Where are you now?' window with a Google map of the San Francisco Bay Area. A 'CCC Confer' window is overlaid on the map, showing a video feed of 'Rich Simms' and a list of participants including 'Benji Simms' and 'Rich Simms'. A 'cis90lesson01.pdf' window is open in the top right, showing 'The CIS 90 System Playground' slide. A terminal window in the bottom right shows a login prompt for 'Opus' with a password field and a timestamp of '17:10 2015 from c-71-204-162-141.h'. A chat window at the bottom left shows a conversation about textbooks.

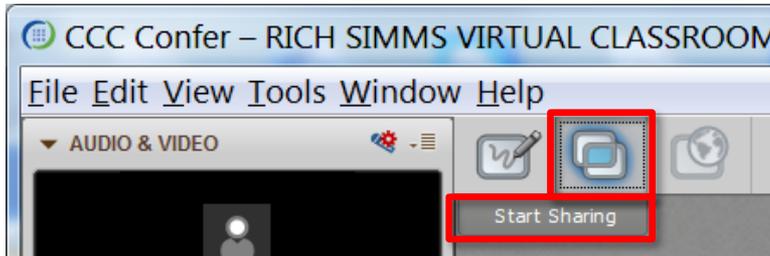
CIS 76 website Calendar page

One or more login sessions to Opus-II

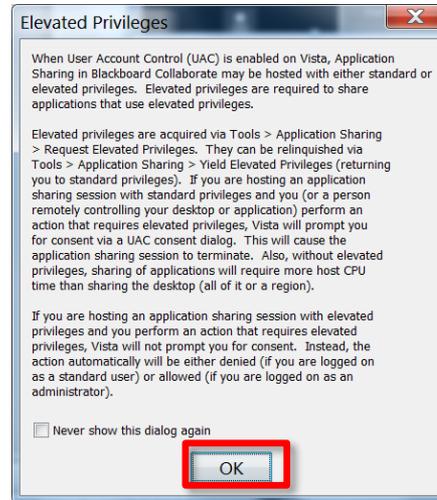


Student checklist for sharing desktop with classmates

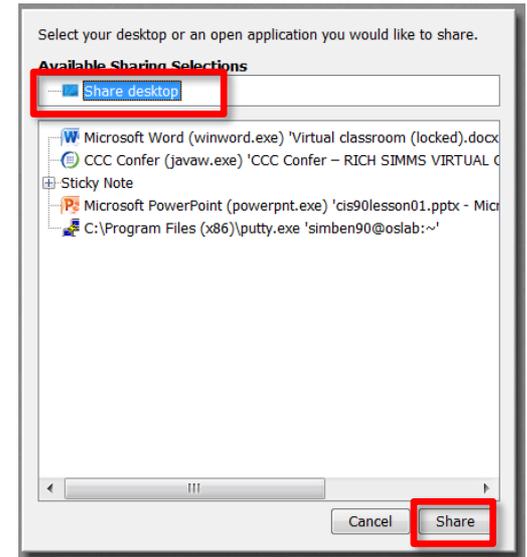
1) Instructor gives you sharing privileges.



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



3) Click OK button.



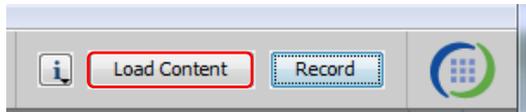
4) Select "Share desktop" and click Share button.



Rich's CCC Confer checklist - setup

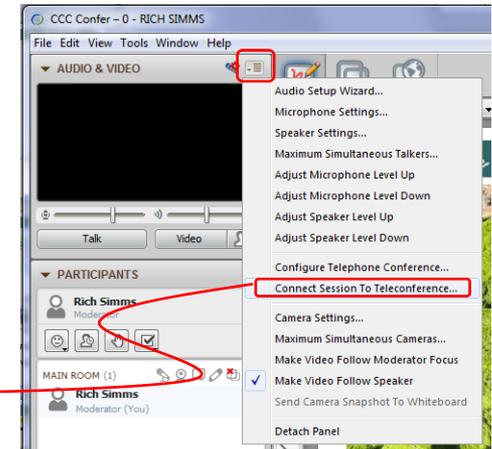
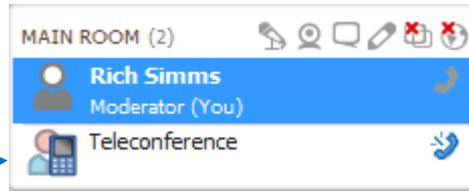


[] Preload White Board

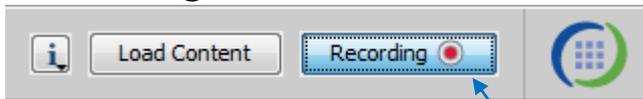


[] Connect session to Teleconference

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



The screenshot displays a desktop environment with several applications open. On the left is a video conference window titled "CCC Confer - 0 - RIC...". In the center, a Foxit Reader window shows a PDF document with a file tree on the left and a main content area. A terminal window titled "simben90@oslab:~" is open, showing a login attempt. On the right, a Chrome browser window displays a document from "simms-teach.com/docs/cis90/cis-90-TEST-1-Fall-12.pdf". In the bottom right, the vSphere Client window is visible, showing a virtual machine named "CIS 192".

Red callout boxes with white text and arrows point to specific elements:

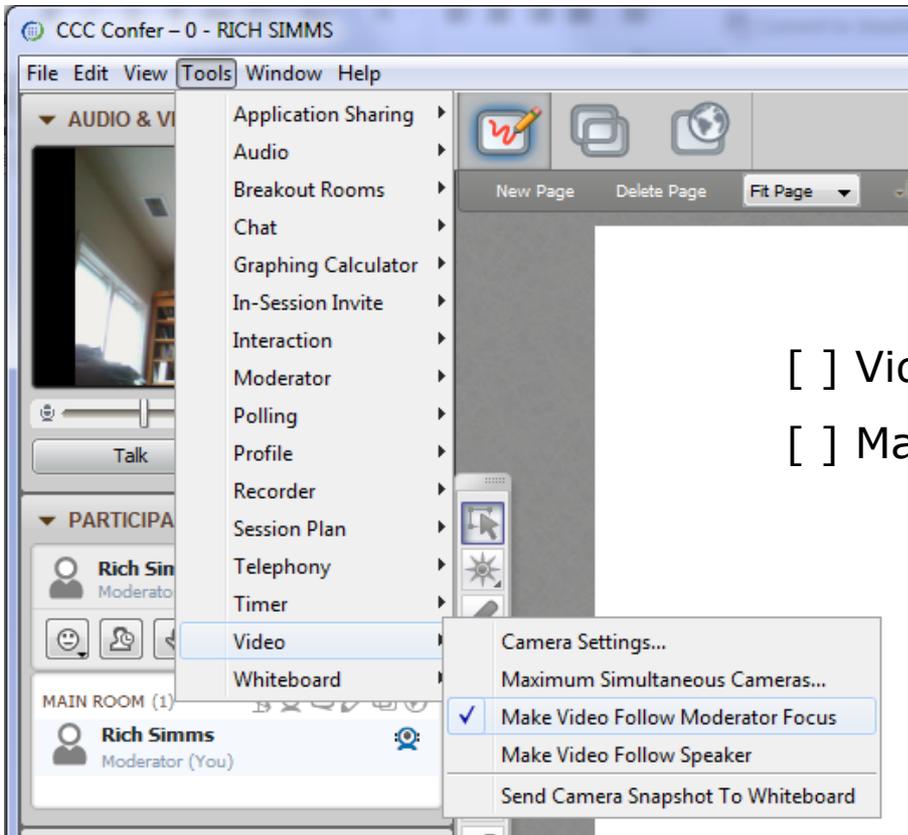
- foxit for slides**: Points to the Foxit Reader window.
- chrome**: Points to the Chrome browser window.
- putty**: Points to the terminal window.
- vSphere Client**: Points to the vSphere Client window.

[] layout and share apps





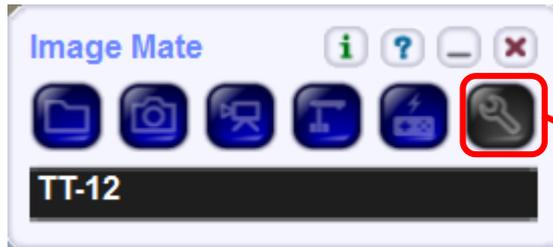
Rich's CCC Confer checklist - webcam setup



- [] Video (webcam)
- [] Make Video Follow Moderator Focus



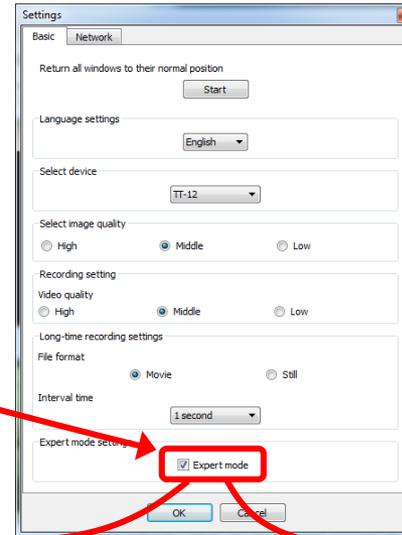
Rich's CCC Confer checklist - Elmo



Elmo rotated down to view side table



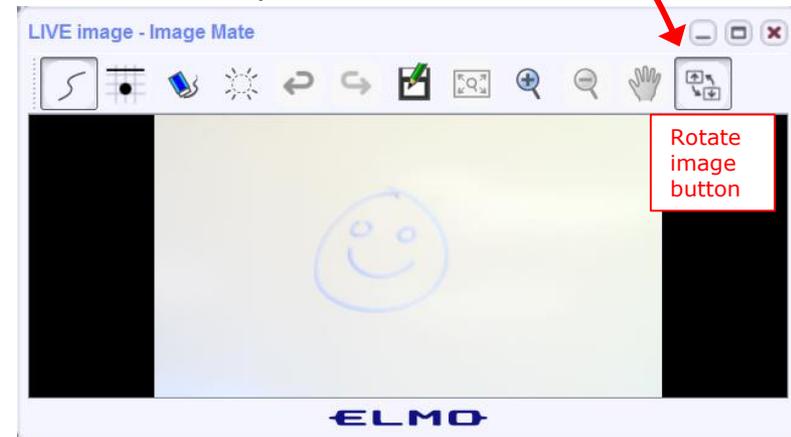
Run and share the Image Mate program just as you would any other app with CCC Confer



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 up to view white board



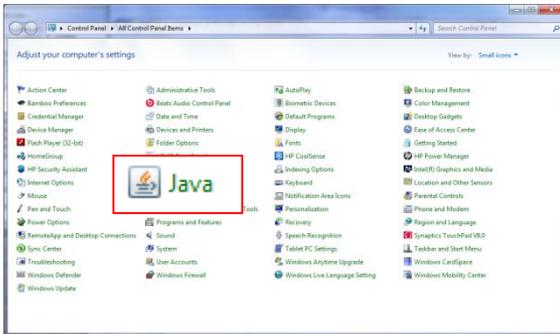


Rich's CCC Confer checklist - universal fixes

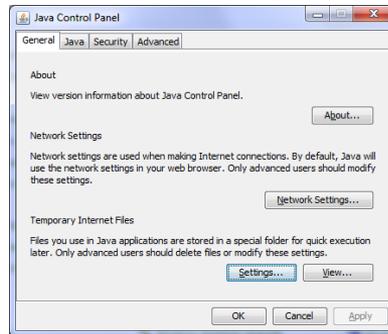
Universal Fix for CCC Confer:

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

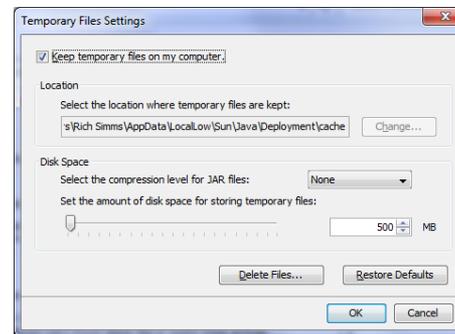
Control Panel (small icons)



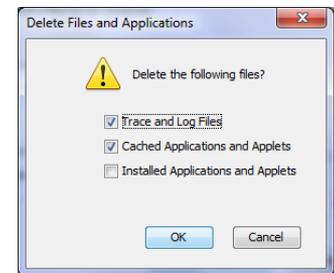
General Tab > Settings...



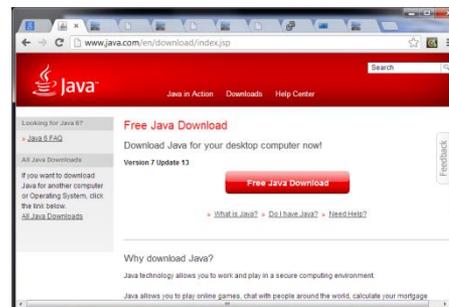
500MB cache size



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.*



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



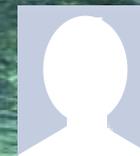
Xu



Mariano



Cameron



Ryan M.



May



Karl-Heinz



Remy

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

- Describe the enumeration step
- Enumerate Windows targets
- Enumerate Unix/Linux targets

Agenda

- 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

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

- NetBios 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.

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>

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

Wireshark interface showing a capture of NetBIOS Name Service (NBNS) traffic on interface eth0. The capture is filtered for 'nbns'. The table below shows the captured frames, with frame 80 highlighted.

No.	Time	Source	Destination	Protocol	Length	Info
7	16.625977670	172.30.10.170	172.30.10.255	NBNS	92	Name query NB ULAB-RASPBX<20>
64	259.009446640	172.30.10.108	172.30.10.255	NBNS	92	Name query NB WORKGROU<1d>
70	263.117787803	172.30.10.162	172.30.10.255	NBNS	92	Name query NB EH-WS2012-DC<00>
73	263.124073973	172.30.10.162	172.30.10.255	NBNS	92	Name query NB EH-WS2012-DC<20>
80	285.955299541	172.30.10.174	172.30.10.255	NBNS	92	Name query NB ULAB-RASPBX<20>
160	559.351323450	172.30.10.108	172.30.10.255	NBNS	92	Name query NB WORKGROU<1d>
169	584.627225386	172.30.10.36	172.30.10.255	NBNS	92	Name query NB WPAD<00>
170	585.387309176	172.30.10.36	172.30.10.255	NBNS	92	Name query NB WPAD<00>
171	586.153019980	172.30.10.36	172.30.10.255	NBNS	92	Name query NB WPAD<00>
180	623.113392836	172.30.10.168	172.30.10.255	NBNS	92	Name query NB ULAB-RASPBX<20>
200	702.898486123	172.30.10.171	172.30.10.255	NBNS	92	Name query NB EH-WIN7<20>
212	715.661564110	172.30.10.171	172.30.10.255	NBNS	92	Name query NB MICROLAB<1b>
213	716.425698640	172.30.10.171	172.30.10.255	NBNS	92	Name query NB MICROLAB<1b>
214	717.189943036	172.30.10.171	172.30.10.255	NBNS	92	Name query NB MICROLAB<1b>
216	718.968597566	172.30.10.171	172.30.10.255	NBNS	92	Name query NB MICROLAB<1b>
217	719.732913786	172.30.10.171	172.30.10.255	NBNS	92	Name query NB MICROLAB<1b>

▶ Frame 80: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
 ▶ Ethernet II, Src: Vmware_af:40:1f (00:50:56:af:40:1f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▶ Internet Protocol Version 4, Src: 172.30.10.174, Dst: 172.30.10.255
 ▶ User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)
 ▼ NetBIOS Name Service

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

NetBIOS Passive Discovery

nbdgm

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.30.10.174	172.30.10.255	BROWSER	243	Host Announcement EH-WINXP, Workstation, S...
9	18.296821890	172.30.10.170	172.30.10.255	BROWSER	243	Host Announcement EH-WS2003, Workstation, ...
10	18.297564440	172.30.10.108	172.30.10.255	BROWSER	263	Host Announcement ULAB-VOLUMIO, Workstatio...
11	18.297583860	172.30.10.109	172.30.10.255	BROWSER	262	Local Master Announcement ULAB-RASPBX, Wor...
12	18.297770150	172.30.10.109	172.30.10.255	BROWSER	254	Domain/Workgroup Announcement WORKGROUP, N...
69	262.695874833	172.30.10.162	172.30.10.255	BROWSER	250	Domain/Workgroup Announcement WHITEHATS, N...
74	268.341484300	172.30.10.171	172.30.10.255	BROWSER	268	Host Announcement EH-WS2008-STD, Workstati...
82	286.606749586	172.30.10.172	172.30.10.255	BROWSER	243	Host Announcement EH-WS2012-DC, Workstatio...
85	292.908346974	172.30.10.162	172.30.10.255	BROWSER	264	Local Master Announcement EH-WIN7, Worksta...
124	424.937505219	172.30.10.36	172.30.10.255	BROWSER	243	Host Announcement MASTER-CYLINDER, Worksta...
135	459.051955062	172.30.10.168	172.30.10.255	BROWSER	243	Host Announcement EH-WS2008-ENT, Workstati...
173	596.599694356	172.30.10.34	172.30.10.255	BROWSER	270	Host Announcement CEH-WIN-2012, Workstatio...
211	715.661349260	172.30.10.171	172.30.10.255	BROWSER	216	Get Backup List Request
215	718.968551963	172.30.10.171	172.30.10.255	BROWSER	216	Get Backup List Request
220	722.275915506	172.30.10.171	172.30.10.255	BROWSER	216	Get Backup List Request
222	722.515757870	172.30.10.174	172.30.10.255	BROWSER	243	Host Announcement EH-WINXP, Workstation, S...

▶ Frame 74: 268 bytes on wire (2144 bits), 268 bytes captured (2144 bits) on interface 0
 ▶ Ethernet II, Src: Vmware_af:b8:4a (00:50:56:af:b8:4a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▶ Internet Protocol Version 4, Src: 172.30.10.171, Dst: 172.30.10.255
 ▶ User Datagram Protocol, Src Port: 138 (138), Dst Port: 138 (138)
 ▶ NetBIOS Datagram Service
 ▶ SMB (Server Message Block Protocol)
 ▶ SMB Mailslot Protocol
 ▶ Microsoft Windows Browser Protocol

NBDGM = NetBIOS Datagram Service on UDP port 138

NetBIOS Passive Discovery

browser

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

browser

No.	Time	Source	Destination	Protocol	Length	Info
534	1723.9995179...	172.30.10.172	172.30.10.255	BROWSER	243	Host Announcement EH-WS2012-DC, Workstatio...
537	1733.2035191...	172.30.10.162	172.30.10.255	BROWSER	264	Local Master Announcement EH-WIN7, Worksta...
564	1813.5169310...	172.30.10.174	172.30.10.255	BROWSER	216	Get Backup List Request
597	1859.3513636...	172.30.10.174	172.30.10.255	BROWSER	216	Get Backup List Request
604	1866.0493490...	172.30.10.36	172.30.10.255	BROWSER	243	Host Announcement MASTER-CYLINDER, Worksta...
605	1874.6868070...	172.30.10.171	172.30.10.255	BROWSER	216	Get Backup List Request
613	1874.7760071...	172.30.10.171	172.30.10.255	BROWSER	216	Get Backup List Request
630	1900.6190631...	172.30.10.168	172.30.10.255	BROWSER	243	Host Announcement EH-WS2008-ENT, Workstati...
658	2035.1298000...	172.30.10.34	172.30.10.255	BROWSER	270	Host Announcement CEH-WIN-2012, Workstatio...
701	2165.4689233...	172.30.10.174	172.30.10.255	BROWSER	243	Host Announcement EH-WINXP, Workstation, S...
702	2176.1405774...	172.30.10.170	172.30.10.255	BROWSER	243	Host Announcement EH-WS2003, Workstation, ...
709	2187.0120388...	172.30.10.109	172.30.10.255	BROWSER	262	Local Master Announcement ULAB-RASPBX, Wor...
710	2187.0121088...	172.30.10.109	172.30.10.255	BROWSER	254	Domain/Workgroup Announcement WORKGROUP, N...
711	2187.0126142...	172.30.10.108	172.30.10.255	BROWSER	263	Host Announcement ULAB-VOLUMIO, Workstatio...
718	2206.8045610...	172.30.10.162	172.30.10.255	BROWSER	216	Get Backup List Request
723	2207.5581846...	172.30.10.162	172.30.10.255	BROWSER	216	Get Backup List Request

- ▶ Frame 1: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface 0
- ▶ Ethernet II, Src: Vmware_af:40:1f (00:50:56:af:40:1f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- ▶ Internet Protocol Version 4, Src: 172.30.10.174, Dst: 172.30.10.255
- ▶ User Datagram Protocol, Src Port: 138 (138), Dst Port: 138 (138)
- ▶ NetBIOS Datagram Service
- ▶ SMB (Server Message Block Protocol)
- ▶ SMB Mailslot Protocol
- ▶ Microsoft Windows Browser Protocol

Shows same information

NetBIOS Datagram Service Layer

browser

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.76.5.207	10.76.5.255	BROWSER	243	Host Announcement EH-WIN7-05, Workstation, Server, NT Workstation, Pot.
16	18.730383260	10.76.5.201	10.76.5.255	BROWSER	243	Host Announcement EH-WINXP-05, Workstation, Server, NT Workstation, Po.
28	149.921004228	10.76.5.101	10.76.5.255	BROWSER	274	Local Master Announcement: QWASDPWA, Workstation, Server, Print Queue S.

```

▶ Frame 1: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface 0
▶ Ethernet II, Src: Vmware_af:1f:34 (00:50:56:af:1f:34), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▶ Internet Protocol Version 4, Src: 10.76.5.207, Dst: 10.76.5.255
▶ User Datagram Protocol, Src Port: 138, Dst Port: 138
▼ NetBIOS Datagram Service
  Message type: Direct_group datagram (17)
  More fragments follow: No
  This is first fragment: Yes
  Node Type: B node (0)
  Datagram ID: 0xe266
  Source IP: 10.76.5.207
  Source Port: 138
  Datagram length: 187 bytes
  Packet offset: 0 bytes
  Source name: EH-WIN7-05<20> (Server service)
  Destination name: WORKGROUP<1d> (Local Master Browser)
▶ SMB (Server Message Block Protocol)
▶ SMB MailSlot Protocol
▼ Microsoft Windows Browser Protocol
    
```

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.76.5.207	10.76.5.255	BROWSER	243	Host Announcement EH-WIN7-05, Workstation, Server, NT Workstation, Pot.
16	18.730383260	10.76.5.201	10.76.5.255	BROWSER	243	Host Announcement EH-WINXP-05, Workstation, Server, NT Workstation, Po.
28	149.921004228	10.76.5.101	10.76.5.255	BROWSER	274	Local Master Announcement QWASDPWA Workstation Server Print Queue S

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.76.5.207	10.76.5.255	BROWSER	243	Host Announcement EH-WIN7-05, Workstation, Server, NT Workstation, Pot.
16	18.730383260	10.76.5.201	10.76.5.255	BROWSER	243	Host Announcement EH-WINXP-05, Workstation, Server, NT Workstation, Po.
28	149.921004228	10.76.5.101	10.76.5.255	BROWSER	274	Local Master Announcement QWASDPWA, Workstation, Server, Print Queue S.

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 will be the "Master Browser". The Master Browser has the responsibility to keep 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

The screenshot shows the Nmap website with the following content:

- Navigation Links:**
 - Nmap Security Scanner**
 - Intro
 - Ref Guide
 - Install Guide
 - Download
 - Changelog
 - Book
 - Docs
 - Security Lists**
 - Nmap Announce
 - Nmap Dev
 - Bugtraq
 - Full Disclosure
 - Pen Test
 - Basics
- Table of Resources:**

Intro	Reference Guide	Book	Install Guide
Download	Changelog	Zenmap GUI	Docs
Bug Reports	OS Detection	Propaganda	Related Projects
In the Movies		In the News	
- News Section:**
 - Nmap 7.30 is now available! [[change log](#) | [download](#)]
 - Nmap 7.12 is now available! [[change log](#) | [download](#)]
 - Nmap 7 is now available! [[release notes](#) | [download](#)]
 - We're pleased to release our new and Improved [Icons of the Web](#) project—a 5-gigapixel inter-

<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]

Nmap and Zenmap

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

The screenshot shows the Sectools.Org website interface. At the top, there is a navigation bar with links for Home, About/Help, and Suggest a new tool. The main content area is titled "SecTools.Org: Top 125 Network Security Tools". Below the title, there is a paragraph of introductory text and a "Tools 1-25 of 125" indicator. The tools are listed in a table-like format, with the top two being Wireshark and Metasploit. Each tool entry includes its name, rank, and a star rating. The left sidebar contains a "Nmap Security Scanner" section with links to Intro, Ref Guide, Install Guide, Download, Changelog, Book, and Docs. Other sections include "Security Lists" (Nmap Announce, Nmap Dev, Bugtraq, Full Disclosure, Pen Test, Basics, More), "Security Tools" (Password audit, Sniffers, Vuln scanners, Web scanners, Wireless, Exploitation, Packet crafters, More), "Site News Advertising About/Contact", and "Sponsors".

Nmap and Zenmap



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>

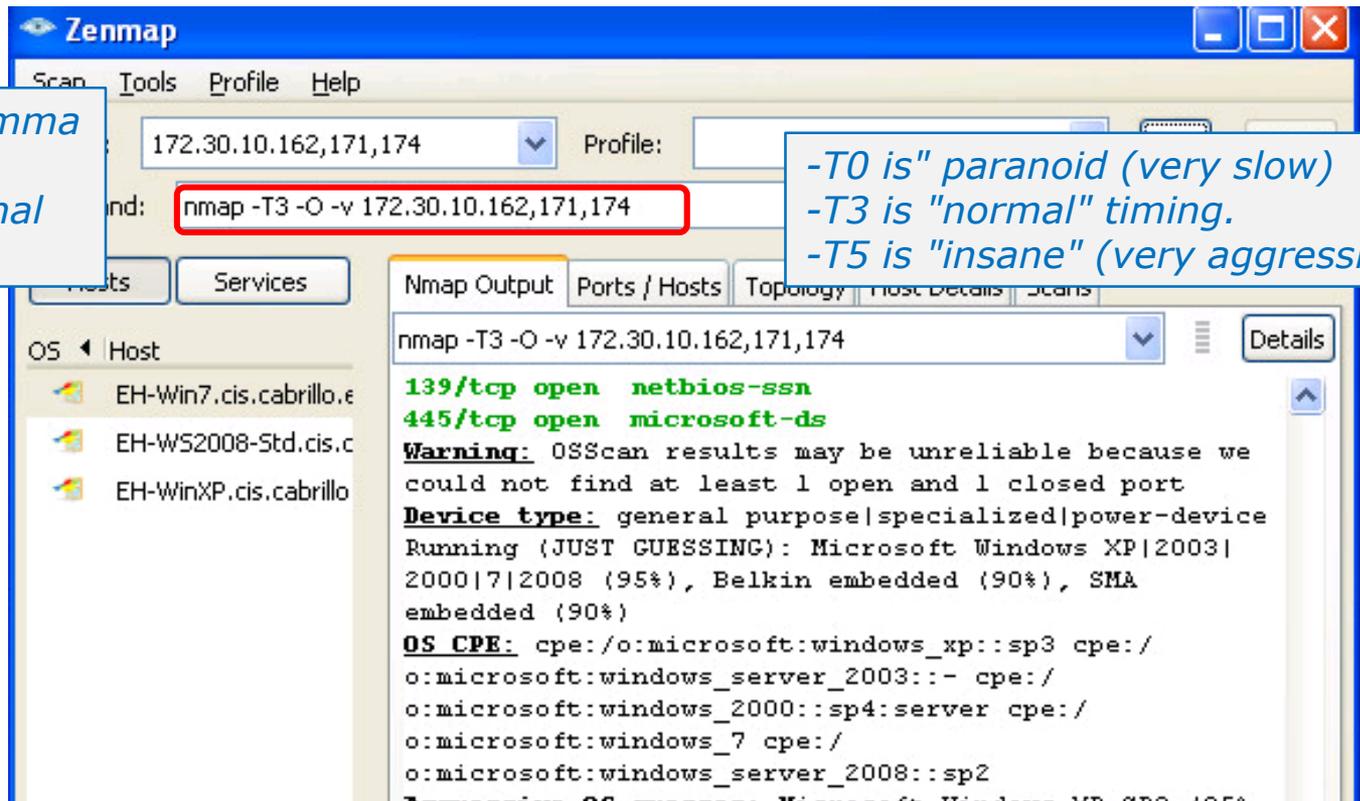
`nmap -T3 -O -v 172.30.10.162,170,172`

*-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

The screenshot shows the Zenmap application window. The title bar reads "Zenmap". The menu bar includes "Scan", "Tools", "Profile", and "Help". The "Target" field contains "172.30.10.162,171,174" and the "Command" field contains "nmap -T3 -O -v 172.30.10.162,171,174". Below the command field are two tabs: "Hosts" (which is selected and highlighted with a red box) and "Services". The "Hosts" pane on the left lists three hosts: "EH-Win7.cis.cabrillo.edu", "EH-WS2008-Std.cis.c", and "EH-WinXP.cis.cabrillo". The "Nmap Output" pane on the right displays the scan results for "EH-WinXP.cis.cabrillo.edu (172.30.10.174)". The output includes the following text:

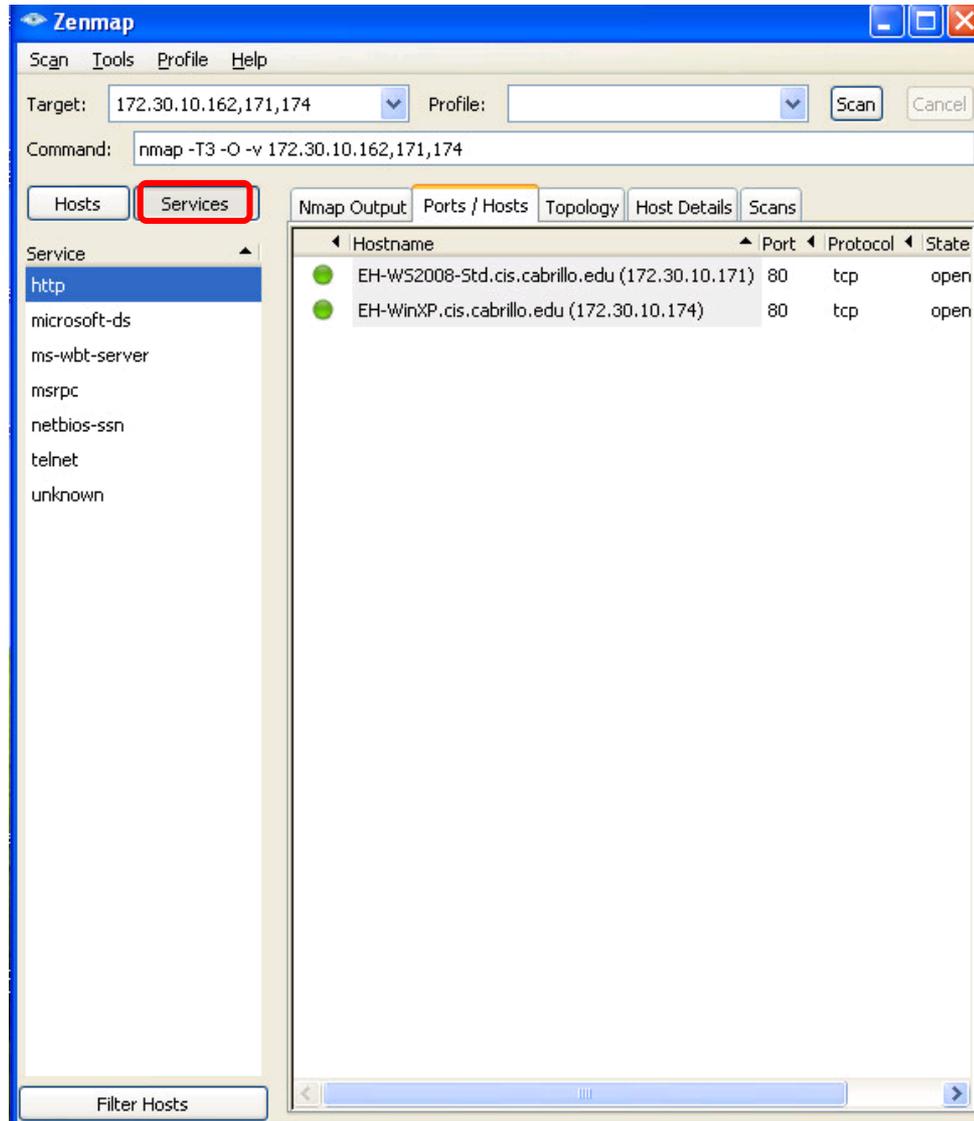
```

Nmap scan report for EH-WinXP.cis.cabrillo.edu
(172.30.10.174)
Host is up (0.00s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
Warning: OSScan results may be unreliable because we
could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|power-device
Running (JUST GUESSING): Microsoft Windows XP|2003|
2000|7|2008 (95%), Belkin embedded (90%), SMA
embedded (90%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/
o:microsoft:windows_server_2003::- cpe:/
o:microsoft:windows_2000::sp4:server cpe:/
o:microsoft:windows_7 cpe:/
o:microsoft:windows_server_2008::sp2
Aggressive OS guesses: Microsoft Windows XP SP3 (95%
), Microsoft Windows XP SP2 (94%), Microsoft Windows
XP SP2 or Windows Server 2003 (93%), Microsoft
Windows 2000 Server SP4 or Windows XP Professional
SP3 (93%), Microsoft Windows Server 2003 SP0 or
Windows XP SP2 (93%), Microsoft Windows XP SP2 - SP3
(93%), Microsoft Windows Server 2003 SP2 (93%),
Microsoft Windows XP SP3 or Small Business Server
2003 (92%), Microsoft Windows XP (92%), Microsoft
Windows Server 2003 SP1 or SP2 (91%)
No exact OS matches for host (test conditions non-
ideal).
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: C:\Program Files\Nmap
OS detection performed. Please report any incorrect
  
```

Show scan
output in right
pane

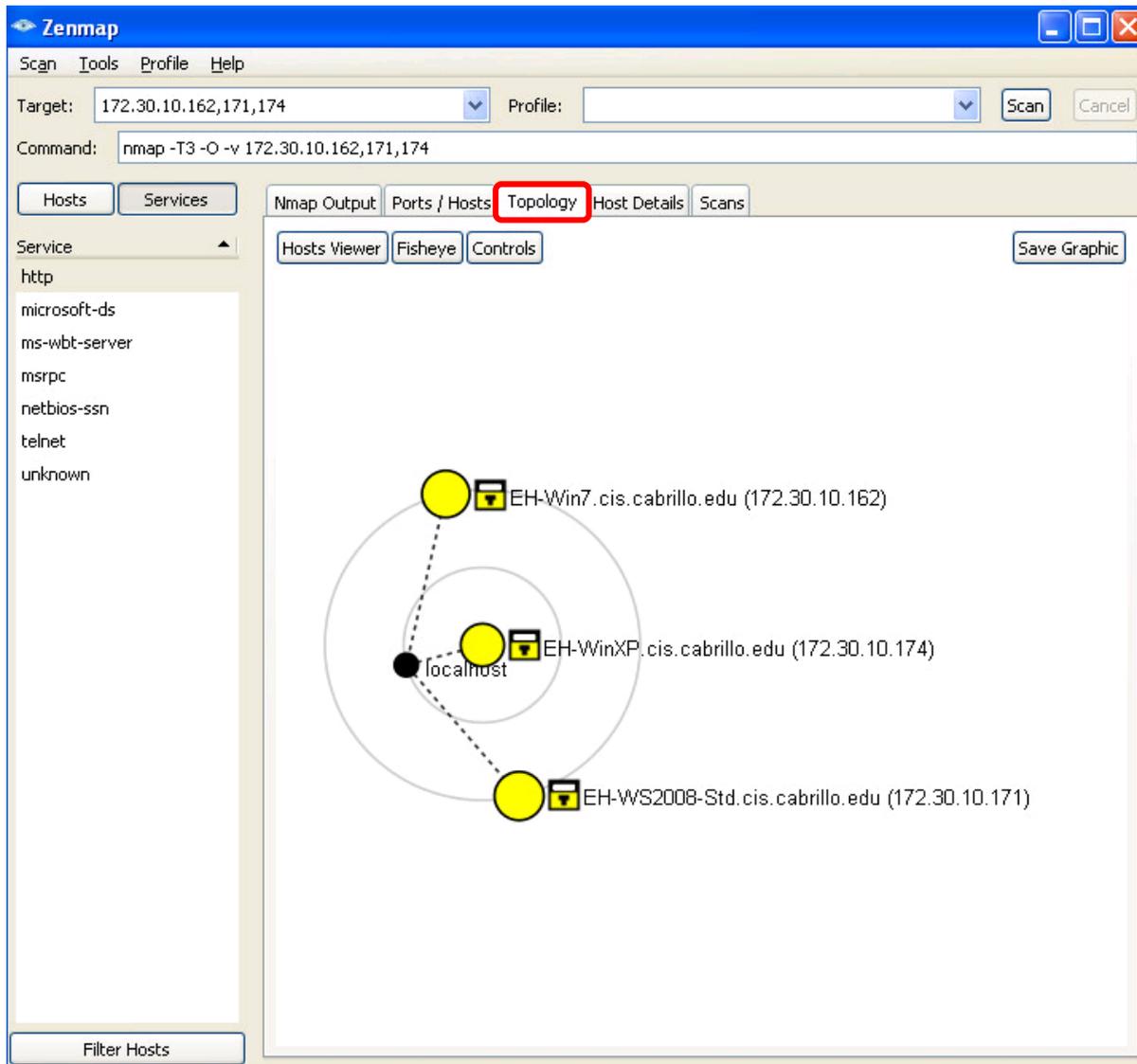
`nmap -T3 -O -v 172.30.10.162,170,172`



*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`

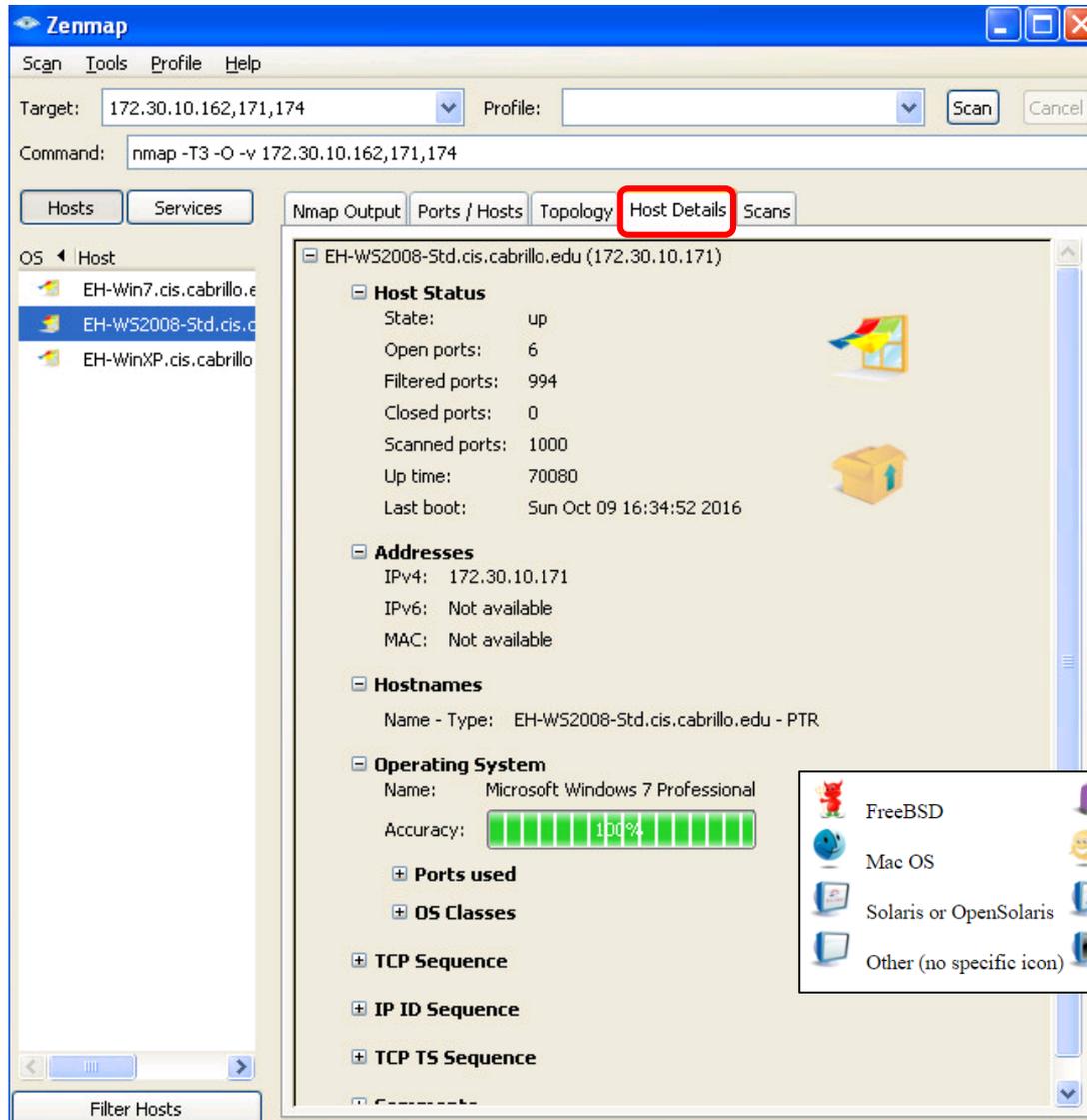


Show a network topology map

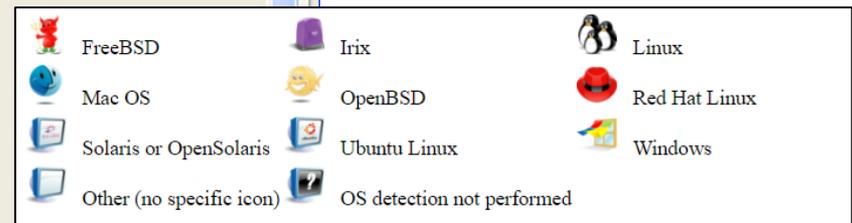
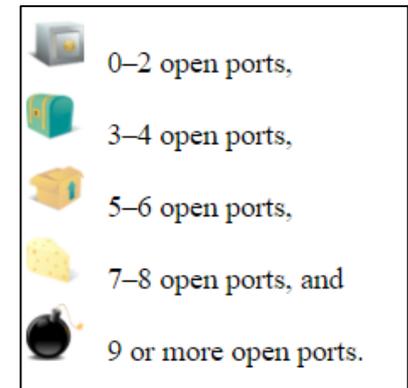
-  Not port scanned
-  < 3 open ports
-  3-6 open ports
-  > 6 open ports
-  Router
-  Switch
-  WAP
-  Firewall
-  Host with filtered ports

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

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



Show host details

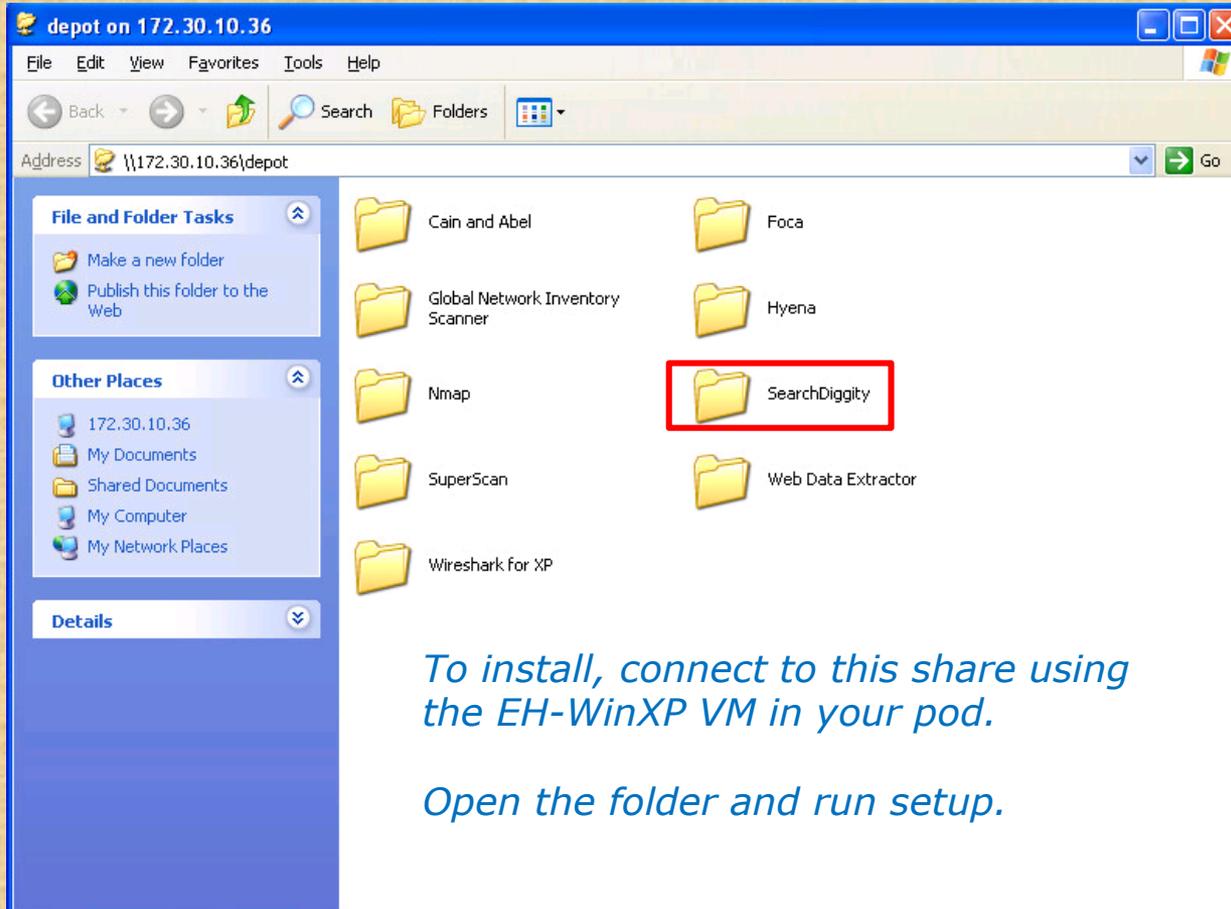


<https://nmap.org/book/zenmap-topology.html#zenmap-topology-legend>

Activity 1

Zenmap Installation on EH-WinXP-xx

Start > Run ... > \\172.30.10.36\depot



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

Open the folder and run setup.

We are not going to use SearchDiggity.

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

depot on 172.30.10.36

File Edit View Favorites Tools Help

Back Forward Search Folders

Address \\172.30.10.36\depot Go

File and Folder Tasks

- Make a new folder
- Publish this folder to the Web

Other Places

- 172.30.10.36
- My Documents
- Shared Documents
- My Computer
- My Network Places

Details

Cain and Abel Foca

Global Network Inventory Scanner Hyena

Nmap SearchDiggity

SuperScan Web Data Extractor

Wireshark for XP

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

Open the folder and run nmap-6.40-setup.

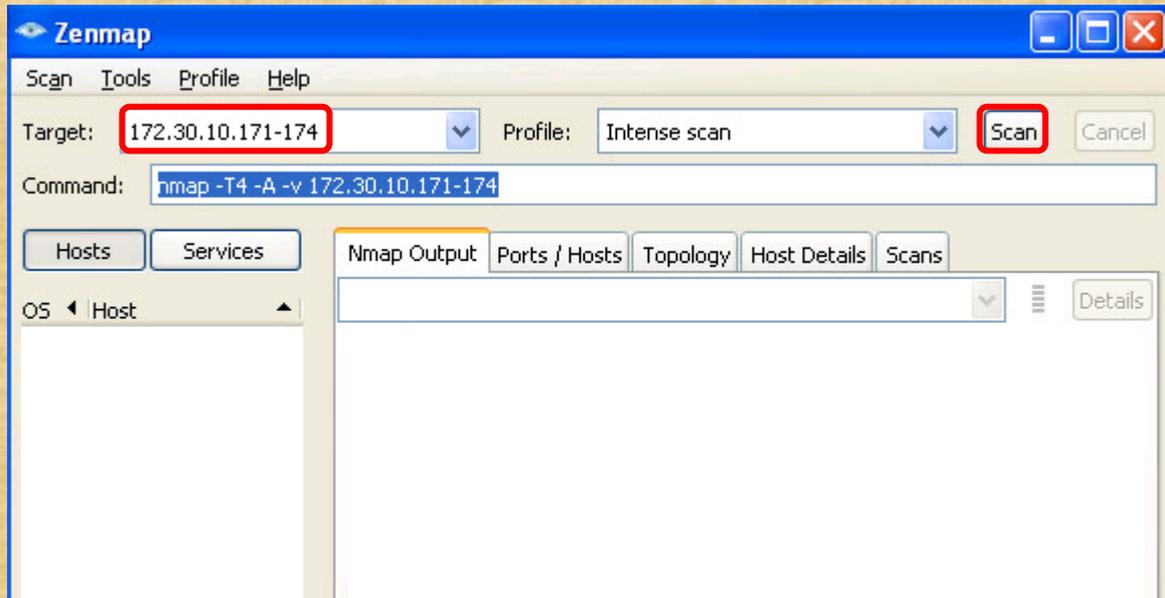
nmap-6.40-setup
Nmap installer
Insecure.org

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

Product: Global Network x

www.magnetosoft.com/product/global_network_inventory/features

magneto
software

Home Products Purchase Download Documentation Partners Company

Home > Products > Network Information Software > Global Network Inventory

Features Screenshots Download Purchase Upgrade License

Global Network Inventory

Global Network Inventory is a powerful and flexible software and hardware inventory system that can be used as an audit scanner in an agent-free and zero deployment environments. If used as an audit scanner, it only requires full administrator rights to the remote computers you wish to scan. Global Network Inventory can audit remote computers and even network appliances, including switches, network printers, document centers, etc.

Global Network Inventory agent can also be deployed to perform regular audits initiated through the domain login script when your users log on the network. In this scenario, Global Network Inventory agent is exported to a shared network directory, and audit results are collected in audit repository directory as snap files and later merged into the main database.

Global Network Inventory key features:

- Scan computers by IP range, by domain, single computers, or computers, defined by the Global Network Inventory host file.
- Reliable IP detection and identification of network appliances such as switches, network printers, document centers, and other devices.
- Scan only items that you need by customizing scan elements.
- View scan results, including historic results for all scans, individual machines, or selected number of addresses.
- Fully customizable layouts and color schemes on all views and reports. Export data to HTML, XML, Microsoft Excel, and text formats.
- Customizable printing.
- Schedule inventory scans to run at specified time, hourly, daily, weekly, monthly, and annually. Ability to generate reports on schedule after every scan, daily, weekly, or monthly.

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**

The screenshot shows the Magneto Global Network Inventory application window. The title bar reads "Global Network Inventory - Unregistered". The menu bar includes File, View, Scan, Tools, Reports, and Help. The toolbar contains various icons for file operations and scanning. On the left, a tree view shows the scan results for "All addresses" under the "WHITEHATS" domain, with "172.30.10.171" selected. The main pane displays a "Scan summary" for this IP address, which is highlighted with a red box. The summary shows the following details:

- Domain: WHITEHATS (COUNT=1)
- IP Address: 172.30.10.171 (COUNT=1)
- Timestamp: 10/10/2016 2:05:12 PM (COUNT=1)
- Com...: EH-WS201, Access de 00-50-56-2, VMware, li

At the bottom of the main pane, there is a table with one row and several columns. The status bar at the bottom indicates "Total 1 item(s)", "Results history depth: Last scan for each address", and "Displayed group: All groups".

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**

The screenshot shows the Magneto Global Network Inventory application window. The title bar reads "Global Network Inventory - Unregistered". The menu bar includes File, View, Scan, Tools, Reports, and Help. The toolbar contains various icons for file operations and scanning. The left pane shows a tree view with "All addresses" expanded to show "WHITEHATS" and "172.30.10.171". The main pane displays the "NetBIOS" scan results for the selected address. The results are organized into a tree structure: "Domain : WHITEHATS (COUNT=3)", "Host Name : EH-WS2008-STD (COUNT=3)", and "Timestamp : 10/10/2016 2:05:12 PM (COUNT=3)". Below this, a table lists the discovered NetBIOS names and their service types.

Name	Type	Usage
- Domain : WHITEHATS (COUNT=3)		
- Host Name : EH-WS2008-STD (COUNT=3)		
- Timestamp : 10/10/2016 2:05:12 PM (COUNT=3)		
EH-WS2008-STD <0x00>	Unique	Workstation Service
EH-WS2008-STD <0x20>	Unique	File Server Service
WHITEHATS <0x00>	Group	Domain Name

Below the table, the text *NetBIOS names and <service types>* is displayed in blue. At the bottom of the main pane, it says "Total 3 item(s)". The status bar at the bottom of the window shows "Ready", "Results history depth: Last scan for each address", and "Displayed group: All groups".

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**

The screenshot shows the Magneto Global Network Inventory application window. The 'Shares' tab is highlighted with a red box. The main display area shows a tree view of scan results for the host 172.30.10.171, with the following data:

Type	Name	Volu...	Serial...	File S...	Size...	Free...
- Domain : WHITEHATS (COUNT=4)						
- Host Name : EH-WS2008-STD (COUNT=4)						
- Timestamp : 10/10/2016 2:05:12 PM (COUNT=4)						
Special share	ADMIN\$				0.00	0.00
Special share	C\$				0.00	0.00
Interprocess...	IPC\$				0.00	0.00
Disk drive	Users		161D88D8	NTFS	39.90	30.20

Below the table, the text *File shares* is displayed. At the bottom of the window, it says "Total 4 item(s)".

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**

The screenshot shows the Magneto Global Network Inventory application window. The left pane shows a tree view with 'All addresses' expanded to 'WHITEHATS' and '172.30.10.171' selected. The main pane shows the 'Logged on' tab, which displays a table of logged-in users. The table has columns for 'User Name' and 'Logon Time'. The data is grouped by Domain, Host Name, and Timestamp.

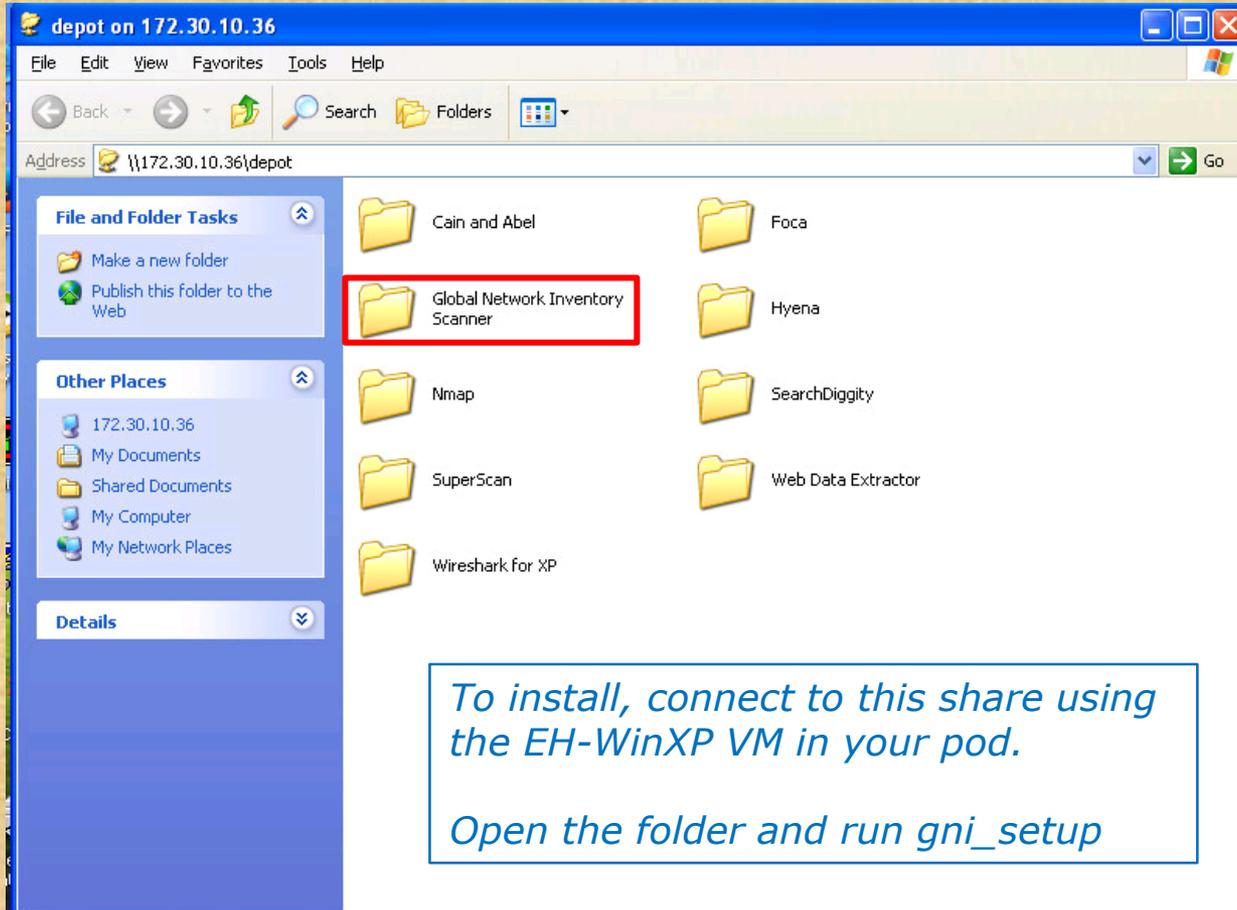
Domain	Host Name	Timestamp	User Name	Logon Time
WHITEHATS (COUNT=2)	EH-WS2008-STD (COUNT=2)	10/10/2016 2:05:12 PM (COUNT=2)	EH-WS2008-STD\Administrator	
			WHITEHATS\simben76	

Below the table, the text *User logged in* is displayed in blue. At the bottom of the main pane, it says 'Total 2 item(s)'. The status bar at the bottom of the window shows 'Ready', 'Results history depth: Last scan for each address', and 'Displayed group: All groups'.

Activity 1

Global Network Inventory installation on EH-WinXP VM

Start > Run ... > \\172.30.10.36\depot



depot on 172.30.10.36

File Edit View Favorites Tools Help

Back Forward Refresh Search Folders

Address <\\172.30.10.36\depot> Go

File and Folder Tasks

- Make a new folder
- Publish this folder to the Web

Other Places

- 172.30.10.36
- My Documents
- Shared Documents
- My Computer
- My Network Places

Details

Cain and Abel	Foca
Global Network Inventory Scanner	Hyena
Nmap	SearchDiggity
SuperScan	Web Data Extractor
Wireshark for XP	

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

Open the folder and run gni_setup

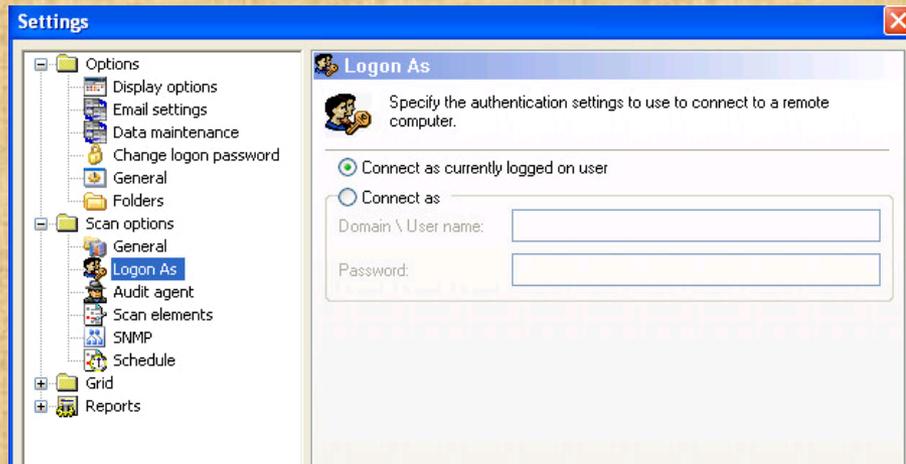
 gni_setup
Setup Launcher
Magneto Software

Use the chat window to indicate you have installed it

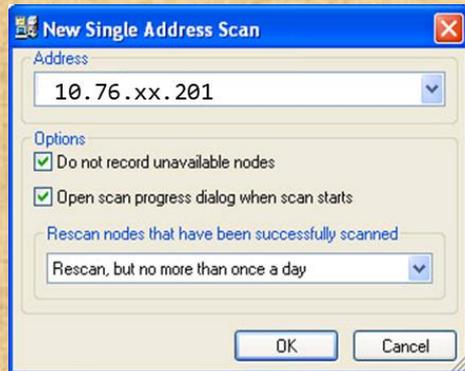
Activity 2

Inventory your pod EH-WinXP VM

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



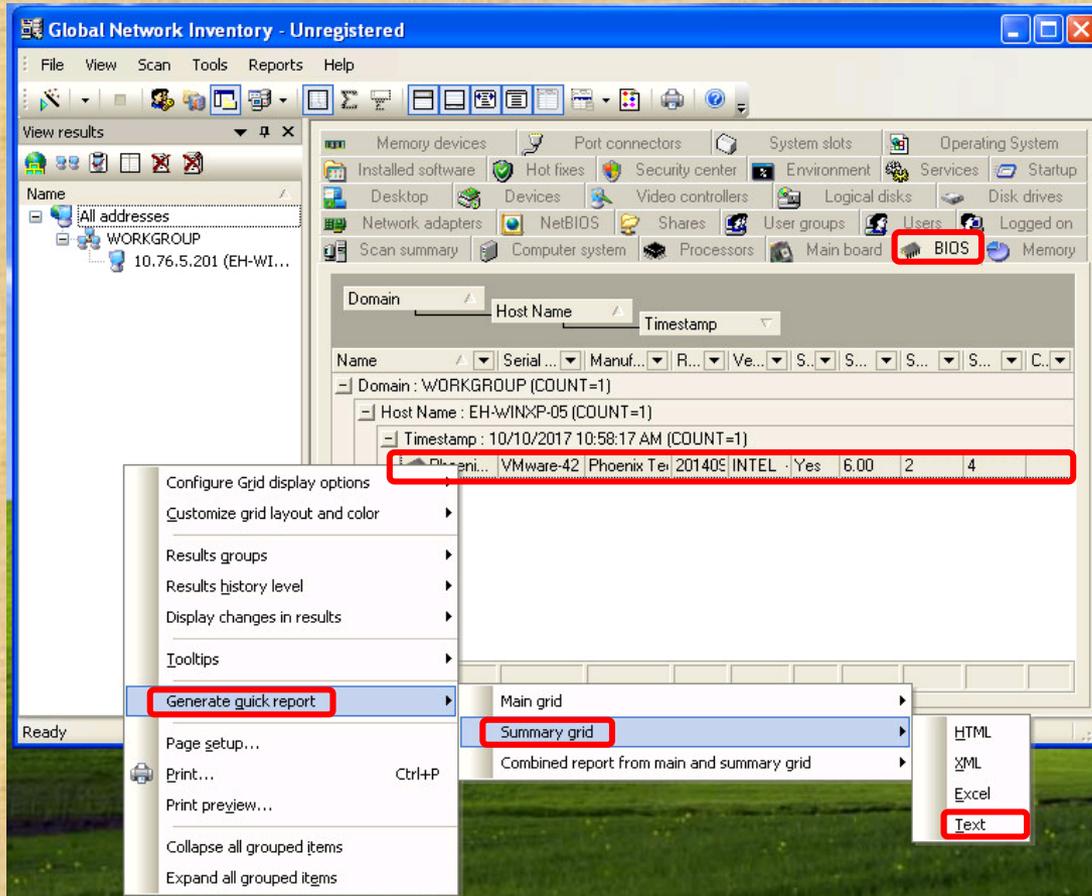
2. **Scan > New Scan > New Single Address Scan > 10.76.xx.201 > [OK]**



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

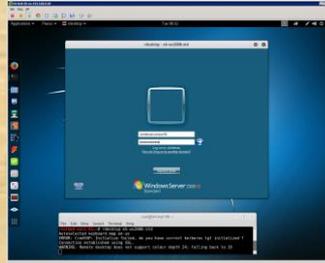
4. Right-click on the BIOS details > Generate Quick Report > Summary grid > Text

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

```

root@eh-kali-05: ~
File Edit View Search Terminal Help
root@eh-kali-05:~# rdesktop 172.30.10.176
Autoselected keyboard map en-us
ERROR: CredSSP: Initialize failed, do you have correct kerberos tgt initialized ?
Connection established using SSL.
WARNING: Remote desktop does not support colour depth 24; falling back to 16
    
```

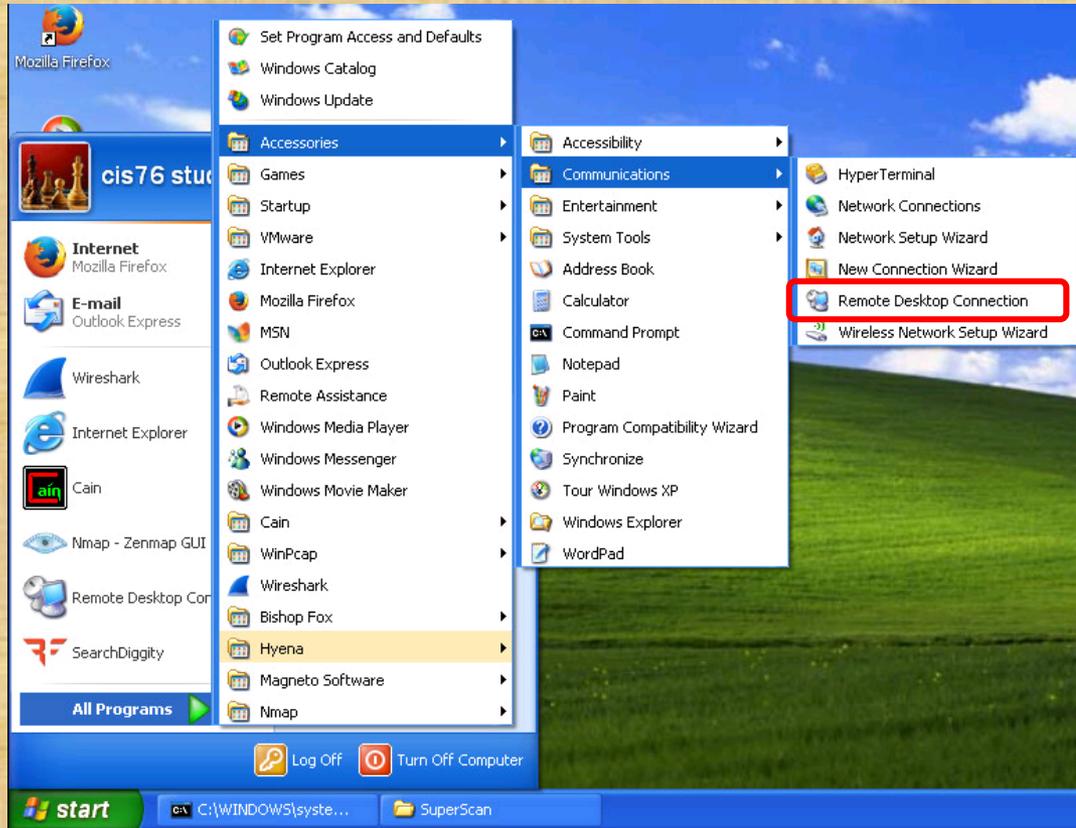


Post in the chat window when you have successfully connected using remote desktop

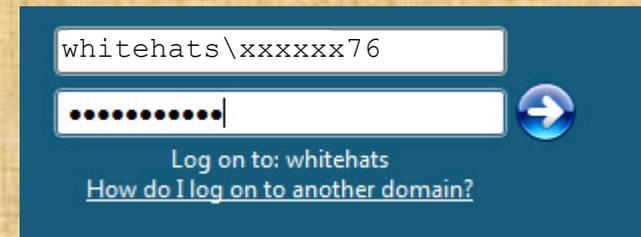
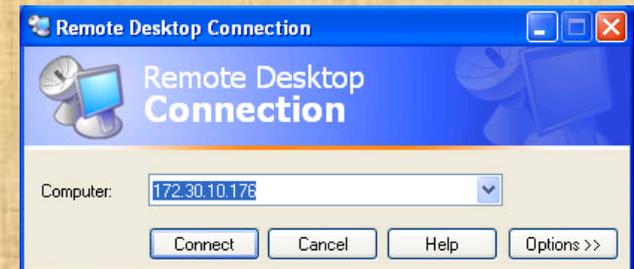
Use your original Opus-II username and password with the whitehats domain

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
```

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

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-LEMM00D
\\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

SuperScan | McAfee Free x

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

Business Home About Us Purchase United States - English

intel Security Threat Center Products Solutions Services Support Partners Community

Business Home > Products > Product Downloads & Trials > Free Tools

SuperScan v4.1

Powerful TCP port scanner, pinger, resolver.

SuperScan 4 is an update of the highly popular Windows port scanning tool, SuperScan.

Windows XP Service Pack 2 has removed raw sockets support which now limits SuperScan and many other network scanning tools. Some functionality can be restored by running the following at the Windows command prompt before starting SuperScan:

```
net stop SharedAccess
```

Here are some of the new features in this version.

- Superior scanning speed
- Support for unlimited IP ranges
- Improved host detection using multiple ICMP methods
- TCP SYN scanning
- UDP scanning (two methods)
- IP address import supporting ranges and CIDR formats
- Simple HTML report generation
- Source port scanning
- Fast hostname resolving
- Extensive banner grabbing
- Massive built-in port list description database
- IP and port scan order randomization
- A selection of useful tools (ping, traceroute, Whois etc)

SuperScan

Superscan

From Wikipedia, the free encyclopedia



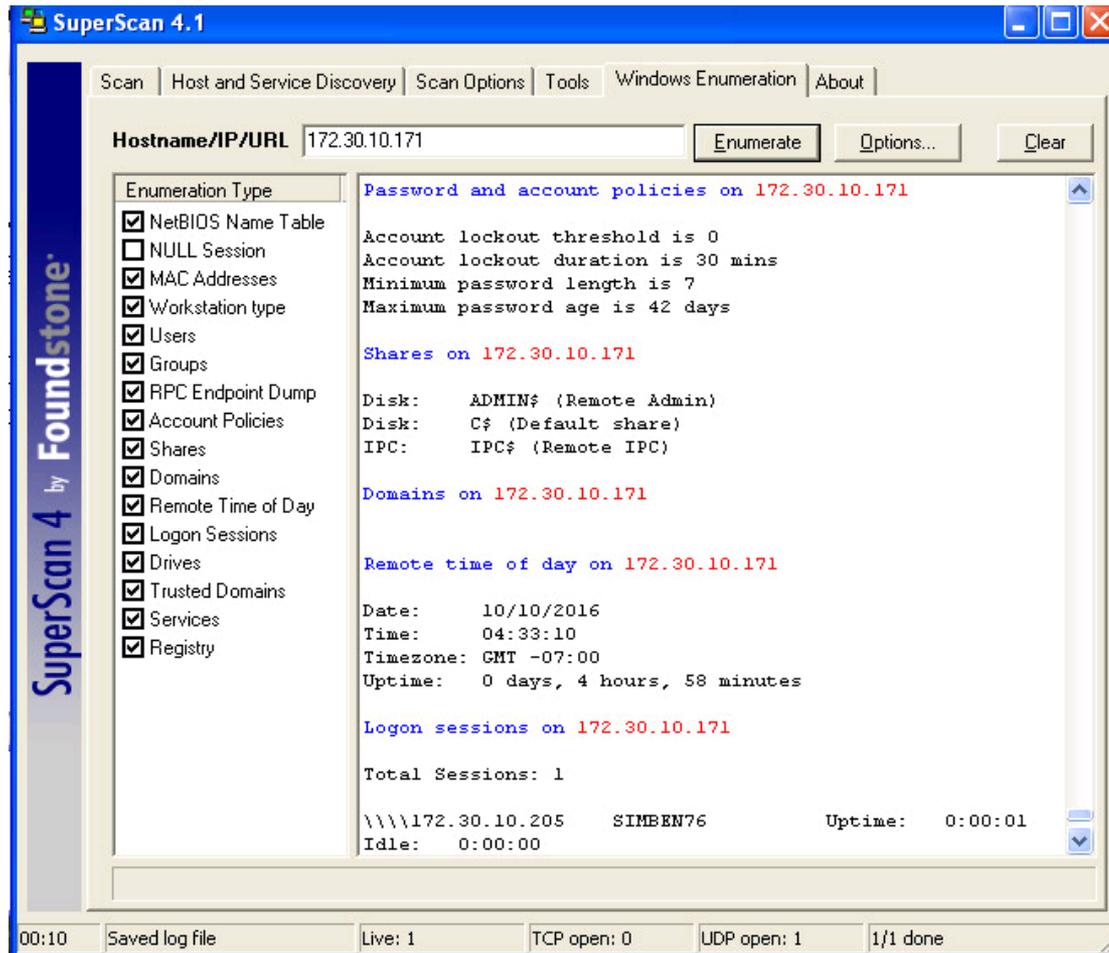
This article **relies too much on references to primary sources**. Please improve this by adding **secondary or tertiary sources**. (*April 2010*) (*Learn how and when to remove this template message*)

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

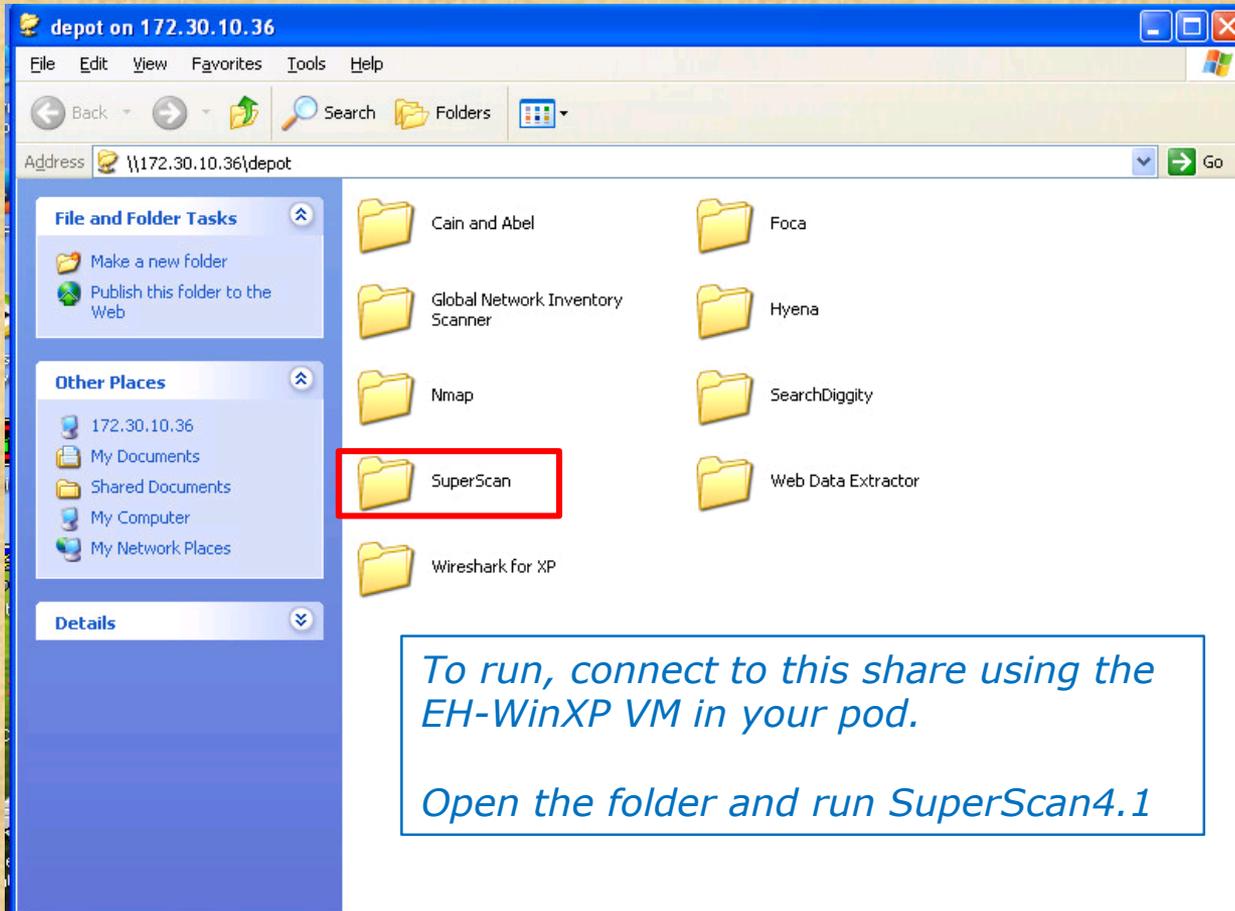
SuperScan 4.1 by Foundstone



Activity 1

Run SuperScan on your EH-WinXP VM

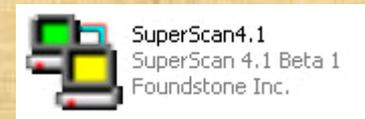
Start > Run ... > `\\172.30.10.36\depot`



The screenshot shows a Windows XP file explorer window titled "depot on 172.30.10.36". The address bar contains the network path "\\172.30.10.36\depot". The main pane displays a list of folders: Cain and Abel, Foca, Global Network Inventory Scanner, Hyena, Nmap, SearchDiggity, SuperScan (highlighted with a red box), and Web Data Extractor. Below the main pane, there is a text box with instructions.

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

System Management Sol x

www.systemtools.com/hyena/

SystemTools® software inc
solutions that work

Home

Follow Us

f t in g+ r

Hyena Features

- General Administration
- Active Directory**
 - AD Management
 - AD Bulk Editing
 - AD Importing
- Server / Workstation
- User and Group Service
- Job / Task Scheduling
- Disk / File Event
- Printer / Print Job
- Exchange Administration
- WMI / Inventory
- Exporting / Reporting
- Bulk Importing

Products

- Hyena
- Free Utilities

Pricing/Ordering

- General Information
- Hyena

Toolnews

Hyena Total System Administration

Features ▾ Pricing ▾ Purchasing Download Free Trial !

Hyena v12.0

Windows 10 Compatible Windows 8 Compatible Compatible with Windows 7

[Click here for a list of new features in v12.0!](#)

Using the built-in Windows administration tools to manage a medium to large Windows 200x network or Active Directory environment can be a challenge. Add multiple domains, hundreds or thousands of servers, workstations, and users, and before you know it, things can get out of hand. Hyena is designed to both simplify and centralize nearly all of the day-to-day management tasks, while providing new capabilities for system administration. This functionality is provided in a single, centralized, easy to use product. Used today by tens of thousands of system administrators worldwide, Hyena is the one tool that every administrator cannot afford to be without.

Hyena uses an Explorer-style interface for all operations, including right mouse click pop-up context menus for all objects. Management of users, groups (both local and global), shares, domains, computers, services, devices, events, files, printers and print jobs, sessions, open files, disk space, user rights, messaging, exporting, job scheduling, processes, and printing are all supported. For an example of a typical enterprise-wide view in Hyena, [click here](#).

In fact, Hyena can be used on any Windows client to manage any Windows NT, Windows 2000, Windows XP/Vista, Windows 7, Windows 8, Windows 8.1, Windows 10 or Windows Server 2003/2008/2012 Installation.

SystemTools Hyena

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

Hyena

Registration

 This is a fully functional copy of Hyena. Registration is required after the 30-day trial period expires. For information on registering Hyena, click the Registration Information button below, or visit:

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

If you have your registration information for Hyena, enter it below, and then click OK. It MUST be entered exactly as provided on Hyena's license certificate. If you want to continue your evaluation, simply click OK (leave the registration key blank).

Days remaining in trial period

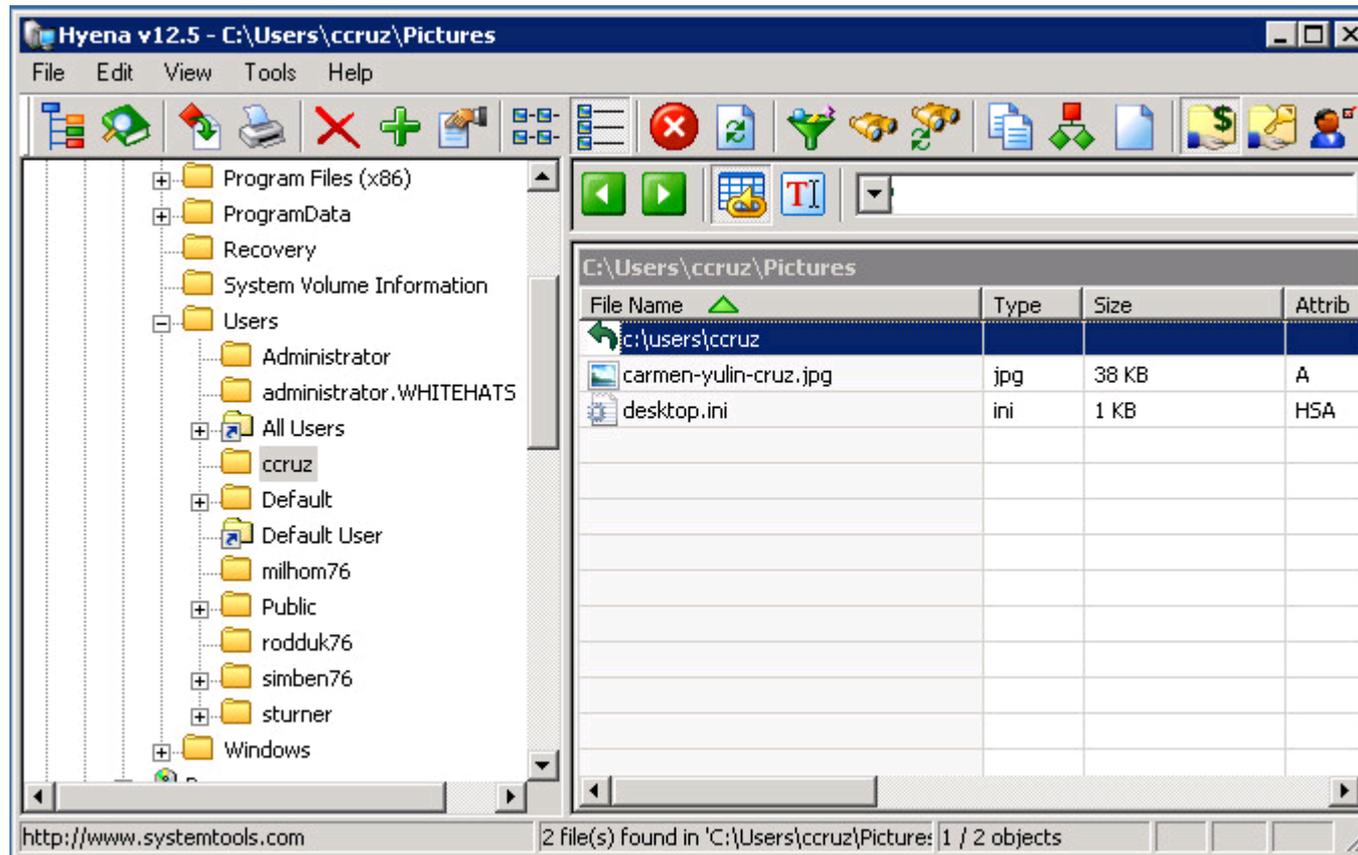
Registration Key

Company / Licensee Name

Your Email Address

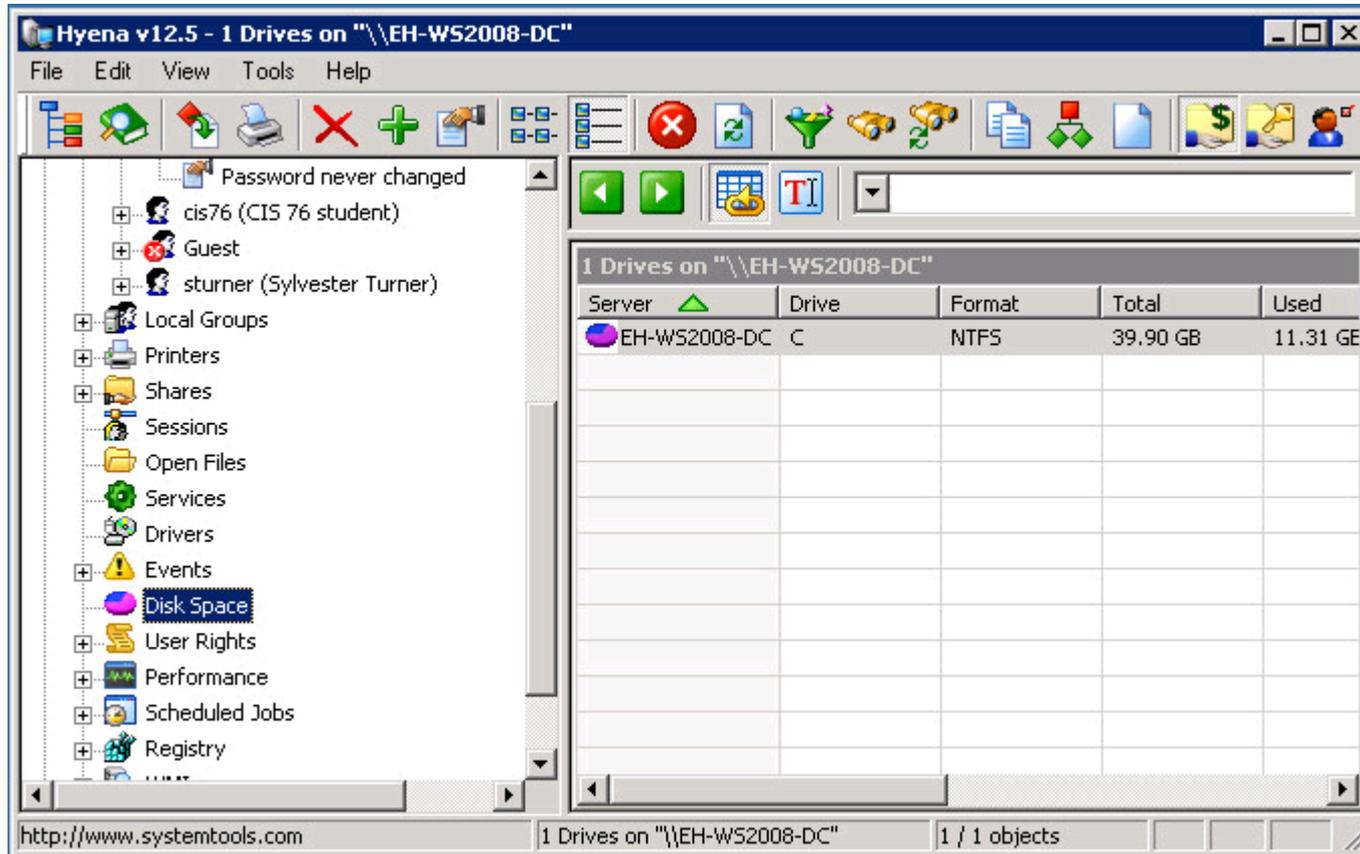
For the 30-day evaluation, just click OK to continue

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

enum4linux | Portcullis Labs

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

Portcullis is now part of Cisco Learn More About Cisco

Portcullis Labs
Research and Development

Phone UK: +44 20 8868 0098

Home Blog Presentations Tools Whitepapers Downloads

enum4linux

Published 16/09/2008 | By MRL

A Linux alternative to enum.exe for enumerating data from Windows and Samba hosts.

 **enum4linux-0.8.9.tar.gz**
April 26, 2013
31.2 KiB
MD5 hash: d1873cdce2db870a7b9e92cbefdfb603
[DETAILS](#)

Key features

- RID cycling (When RestrictAnonymous is set to 1 on Windows 2000)
- User listing (When RestrictAnonymous is set to 0 on Windows 2000)
- Listing of group membership information
- Share enumeration
- Detecting if host is in a workgroup or a domain
- Identifying the remote operating system
- Password policy retrieval (using polenum)

Overview

Enum4linux is a tool for enumerating information from Windows and Samba systems. It attempts to offer similar functionality to enum.exe formerly available from www.bindview.com. It is written in Perl and is basically a wrapper around the Samba tools smbclient, rpcclient, net and nmblookup.

enum4linux

enum4linux -a -u cis76 -p xxxxxx 172.30.10.174

```

root@eh-kali-05: ~
File Edit View Search Terminal Help
root@eh-kali-05:~# enum4linux -a -u cis76 -p xxxxxx 172.30.10.174
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Oct 11 14:31:57 2016

=====
| Target Information |
=====
Target ..... 172.30.10.174
RID Range ..... 500-550,1000-1050
Username ..... 'cis76'
Password ..... 'xxxxxx'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 172.30.10.174 |
=====
[+] Got domain/workgroup name: WORKGROUP

=====
| Nbtstat Information for 172.30.10.174 |
=====
Looking up status of 172.30.10.174
EH-WINXP <00> - B <ACTIVE> Workstation Service
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
EH-WINXP <20> - B <ACTIVE> File Server Service
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

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

=====
| Session Check on 172.30.10.174 |
=====
[+] Server 172.30.10.174 allows sessions using username 'cis76', password 'xxxxxx'

=====
| Getting domain SID for 172.30.10.174 |
=====
smb_signing_good: BAD SIG: seq 1
Cannot connect to server. Error was NT_STATUS_ACCESS_DENIED
[+] Can't determine if host is part of domain or part of a workgroup

=====
| OS information on 172.30.10.174 |
=====
[+] Got OS info for 172.30.10.174 from smbclient: Domain=[EH-WINXP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
[+] Got OS info for 172.30.10.174 from srvinfo:
smb_signing_good: BAD SIG: seq 1

```

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	(hawknnet-wireless-gw-ext.cabrillo.edu)	
frocar76	Carter Frost	pts/4	2:26	Oct 11 12:24	(hawknnet-wireless-gw-ext.cabrillo.edu)	
rsimms	Rich Simms	*pts/7		Oct 3 08:49	(2601:647:cb80:lea4: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



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 ~~SSMTP~~ 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.

Quiz questions for next class:

**Lab 6
and five posts**

- 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