

Virtual Learning Tools in Cyber Security Education

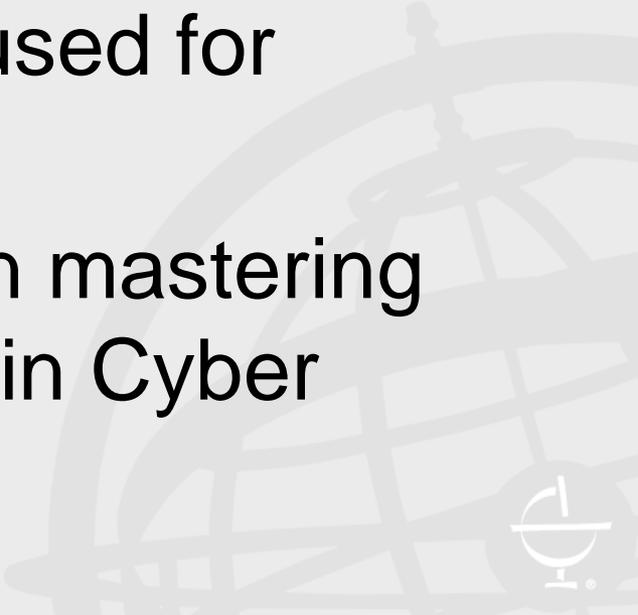
Dr. Sherly Abraham
Faculty Program Director IT and Cybersecurity

Dr. Lifang Shih
Associate Dean

School of Business & Technology,
Excelsior College



Overview

- Importance of electronic training for Cyber security education
 - How technology can be used to enhance the learning process
 - Interactive tools that can be used for identifying security threats
 - Application of practical labs in mastering core technical competencies in Cyber Security
- 

Cyber Security Online Education

- Professional Workforce
 - Shortage of Workforce in Cyber Security
 - Overcome the limitations of time and distance
 - Evolving landscape of Cyber Security threats
 - Bachelor's degree is a common requirement for most cyber security related positions
- 

Cybersecurity Jobs Report

■ Maryland Cybersecurity Job Breakdown

Entry- to mid-level positions requiring a Bachelor's degree dominate cyber security job openings. However, there are plenty of opportunities for high school graduates to engage.

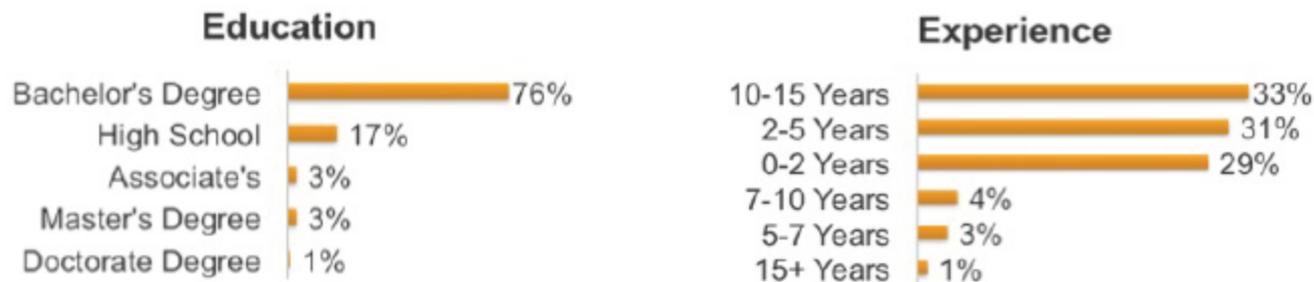


Figure 4: Education and Experience Breakdown



Background

- Excelsior College founded in 1971 (previously Regents College)
- 1998 Private, independent
- Large student body (approximately 33,000 students)
- Distance education, flexible learning format
 - **Philosophy:**
“What you know is more important than where or how you learned it”

Background

- A student centered adult learning model
- Cybersecurity Accreditation
 - CNSS (Committee on National Security Systems)
 - CAE/IA (Center for Academic Excellence in Information Assurance Education) –Pending Approval
 - Middle States (all programs)
 - ABET (specialized accreditation -Technology)
 - IACBE (specialized accreditation –Business)

Degrees Offered in Cyber Security

- Bachelor of Science in IT with Cybersecurity concentration
- Bachelor of Science in IT with Information Security concentration
- Master of Science in Cybersecurity
- Masters of Business Administration with a concentration in Cyber Security Management
- Undergraduate Certificate in Cyber Security
- Graduate Certificate in Cyber Security Management.
- *The programs offers an assortment of courses that focuses on technical, managerial, communicative and soft skills in developing an effective workforce to meet the challenge of next generation cyber security professionals.*

Educational Methods Employed

Interdisciplinary Approach

- Discussion Questions
- Group Projects
- Case Studies
- **Interactive activities**
- **Virtual Labs**



Interactive Activities

- Provides learners with feedback
- Repetitive Learning
- Interesting
- Thought Provoking



Example Interactivity Session

Basic Concepts of Cryptography

Introduction:

Cryptography focuses on the many techniques that can be used to implement secure and trust worthy communication between two communicating parties. The concepts and implementation of cryptography is complicated and requires a large amount of complex programming. In this course you will learn about some of the basic definitions of cryptographic methods. You will now engage in learning some of the basic definitions of concepts in cryptography. It is important to ensure that you clearly understand the concepts highlighted in this activity as it will provide you with a foundation on further learning the concepts of cryptography.

Basic Scenario for Cryptography

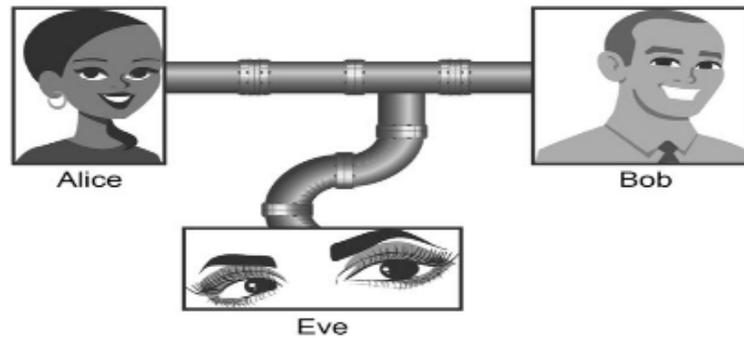


Figure 8.1: The basic scenario for cryptography. Alice and Bob encrypt their communications so that the eavesdropper Eve, can't understand the content of their messages.

Cross Word Puzzle

To complete the crossword puzzle, choose from the following list.

Cryptography

Cipher Text

Encryption

Decryption

Cryptographic Key

Symmetric Cryptography

Asymmetric Cryptography



Solve the crossword puzzle.

Across

- 3.) The process of changing the cipher text back to readable format
- 4.) The unreadable format of text created as a result of the cryptography process
- 5.) Two keys are used,

Down

- 1.) Enables two communicating parties to communicate securely even if their messages are accessed by an eavesdropper
- 2.) The process of

CYS 526

Cyber Attacks and Defenses

- Methodologies, project management tools for penetration testing
- Assess target Systems and networks for vulnerabilities
- Detect security threats
- Recommend and implement defensive, corrective, and preventative measures based on penetration test results.

Scenario Analysis

Types of Hackers

Select your answer and click **Submit**.

1 of 4

A person stumbled upon a distributed denial of service (DDoS) application from a peer-to-peer file-sharing source. He/she downloaded the application and decided to launch it against his or her bank's website to see what it did.

Q What type of hacking is this?

- Black hat
- White hat
- Gray hat



Penetration Testing Guidelines

Pen Test Guidelines

You are an experienced pen tester who has been hired to conduct a security audit of a web server with a backend SQL database.



2 of 4

Q Which guidelines will you choose to complete the audit?

*Enter your answer and click **Submit** to compare it with expert feedback.*

Submit



Identifying Type of Attack Based on Characteristics

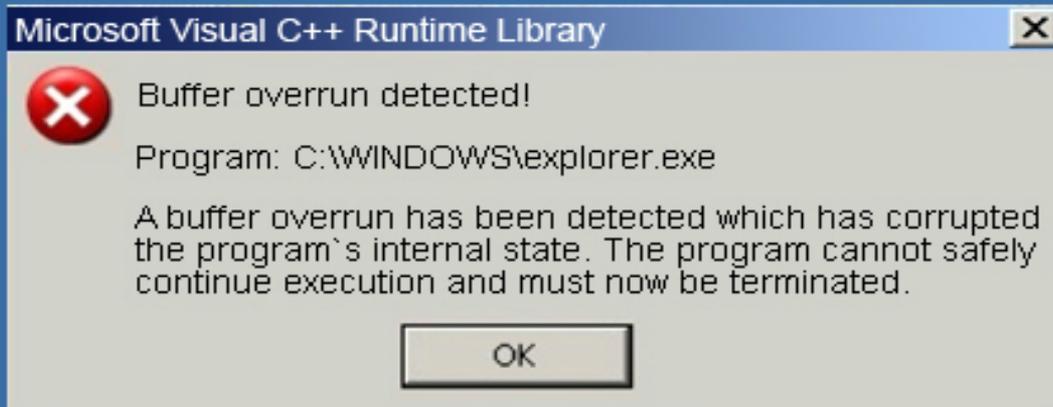
Vulnerability Identification

In this activity, you will identify the type of attack based on the information and image provided in the scenarios.

Enter your answer and click **Submit** to compare it with expert feedback.

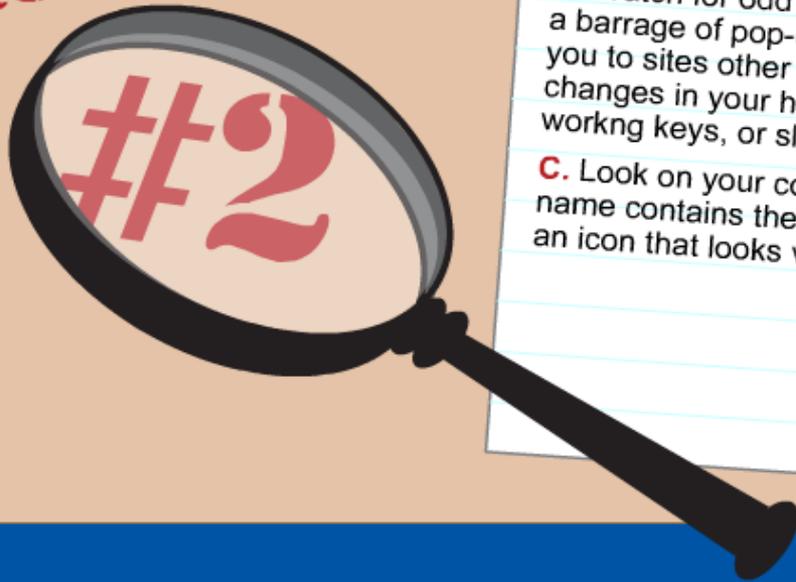
2 of 3

Q2 A program was forced to attempt to execute more data in a buffer than it holds



Identifying Type of Attack Based on Characteristics

QUESTION



Is Someone Watching You?

Individuals or companies can monitor what you do on your computer using "spyware" programs that they secretly install on your computer. How can you tell if your computer is being affected by spyware?

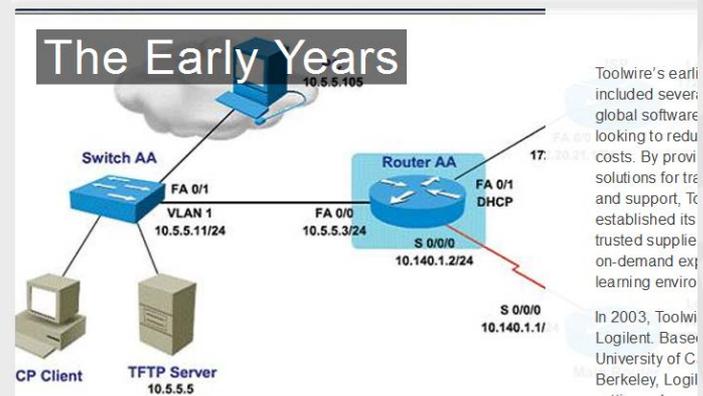
- A.** Look for signs of tampering, such as a missing back panel on your computer, or miniature microphones or cameras hidden nearby.
- B.** Watch for odd computer behavior - such as a barrage of pop-up ads, a browser that takes you to sites other than those you type in, changes in your home page or toolbars, non-working keys, or slow performance.
- C.** Look on your computer for any file whose name contains the word "spyware." It may have an icon that looks very similar to others.



Virtual Lab Activities

- ToolWire
- EC Virtual Environment
 - Experimental learning environment
 - Hands on learning
- Simulates practical environments

OUR STORY



EC Virtual Environment

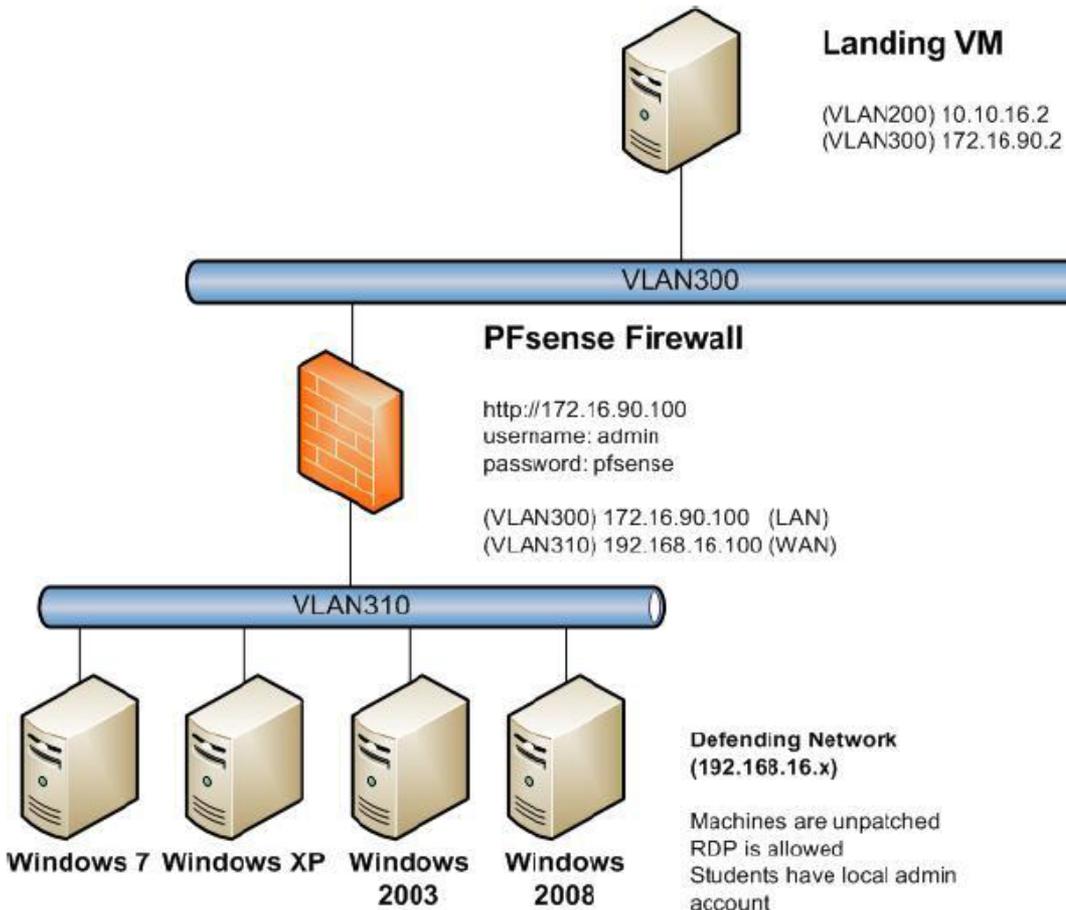
- VMWare Version 5 ESXi hypervisors
 - Hewlett Packard Server Blades
- Dedicated to courses in Cybersecurity
- System
 - 12 Fedora Core 14 64-bit Linux systems
 - 12 Windows Server 2008 R2 64-bit systems
 - 12 Windows 7 Professional 64-bit systems

CYS 501

Communications Security

- Network security fundamentals
- Security policies, networking threats, and technologies
- Design and implementation of secure communications networks
- Network Management and Scanning
- Device hardening, encryption, proxies, firewalls, VPN and remote access design, NAT, DHCP, VoIP
- Honeypots, intrusion detection systems (IDS), and other network defenses are examined.

CYS 501 Communications Security

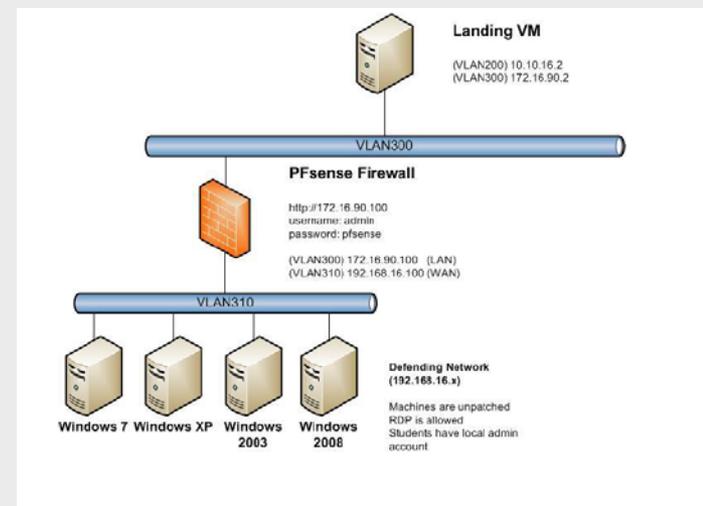


Network Vulnerability Assessment

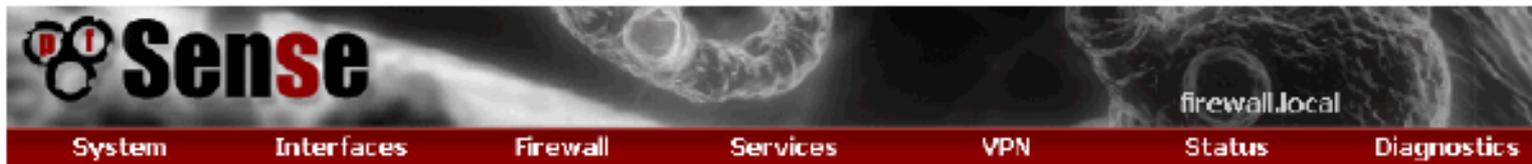
- Tools
 - NMAP
 - Nessus
- Analysis
 - Operating systems and service packs
 - Ports and Services
 - Compare the security level of the different systems
 - Compare the functionality and features of NMAP and Nessus

Securing Network Devices

- Firewall
 - Location of firewall on the network
 - Configure to defend
 - Permit and deny traffic
 - Set rules



Screen Shot



Firewall: Rules

LAN

WAN

	Proto	Source	Port	Destination	Port	Gateway	Schedule	Description	
<input type="checkbox"/>		*	*	*	*	*		Allow ALL	
	pass			block			reject		log
	pass (disabled)			block (disabled)			reject (disabled)		log (disabled)

Firewall Configuration

The screenshot displays the OnDemand Workbench interface. On the left, an Nmap scan of 192.168.16.4 is shown with the following results:

```
nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 192.168.16.4
```

PORT	STATE	SERVICE	VERSION
21/tcp	open	tcpwrapped	
135/tcp	filtered	msrpc	
139/tcp	filtered	netbios-ssn	
445/tcp	open	netbios-ssn	
1688/tcp	open	msrpc	Microsoft Windows RPC
3389/tcp	open	ms-term-serv?	
49152/tcp	open	msrpc	Microsoft Windows RPC
49153/tcp	open	msrpc	Microsoft Windows RPC
49154/tcp	open	msrpc	Microsoft Windows RPC
49155/tcp	open	msrpc	Microsoft Windows RPC
49156/tcp	open	msrpc	Microsoft Windows RPC
49157/tcp	open	msrpc	Microsoft Windows RPC

Below the scan results, the TCP/IP fingerprint is displayed:

```
OS: SCAN( V=5.51%D=3/21%OT=21%CT=1%CU=40940%PV=Y%DS=1%DC=I %G=Y%TM=4F6A2907%P= %S:1686-pc-windows-windows) SEQ( SP=100%GCD=Z%ISR=100% TI=RD%II=RI%TS=21) SEQ( S %S:P=104%GCD=Z%ISR=106%TI=RD%II=RI%TS=22) SEQ( SP=105% GCD=Z%ISR=108%TI=RD%II= %S:RI%TS=22) SEQ( SP=103%GCD=Z%ISR=105%TI=RD%II=RI%TS=21) SEQ( SP=105%GCD=Z%ISR %S:=10C%TI=RD%II=RI%TS=21) OPS( O1=MSB4NW4ST11% O2=M578NW4ST11%O3=M280NW4NNT11 %S:%O4=MSB4NW4ST11%O5=M218NW4ST11%O6=M109ST11) WIN ( W1=FECC%W2=FECC%W3=FECC%W %S:4=FECC%W5=FECC%W6=FECC) ECN( R=Y%DF=Y%T=41%W=FECC% O=MSB4NW4SLL%CC=N%Q=) T1( %S:R=Y%DF=Y%T=41%S=C%A=S+F=AS%RD=C%Q=) T2( R=N) T3( R=N) T4 ( R=N) T5( R=Y%DF=Y%T=8
```

On the right, the firewall.local configuration page is shown. A red banner indicates that firewall rules are reloading in the background. Below the banner is a table of firewall rules:

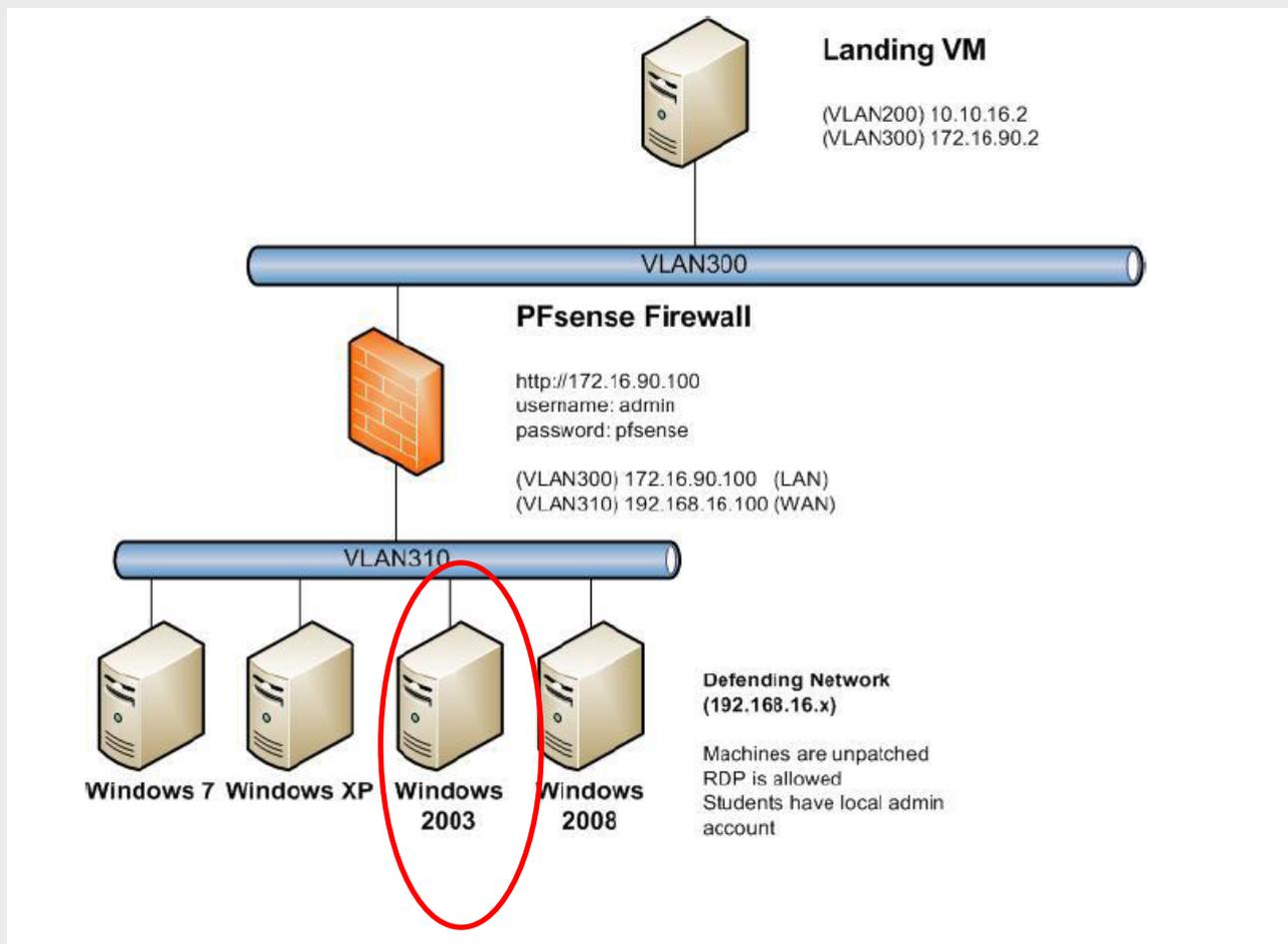
Port	Gateway	Schedule	Description
135	*		Block TCP for port 135
139 (NetBIOS-SSN)	*		Block TCP for NetBIOS port 139
*	*		Allow ALL

The Windows taskbar at the bottom shows the Start button, several application icons, and the system tray with the date and time: 12:17 PM, 3/21/2012.

Honeypot

- Honeynet Project
 - <https://honeynet.org/project>
- HoneyBOT
 - <http://www.atomicsoftwaresolutions.com/honeybot.php>
- Valhala Honeypot
 - <http://sourceforge.net/projects/valhalahoneypot/>

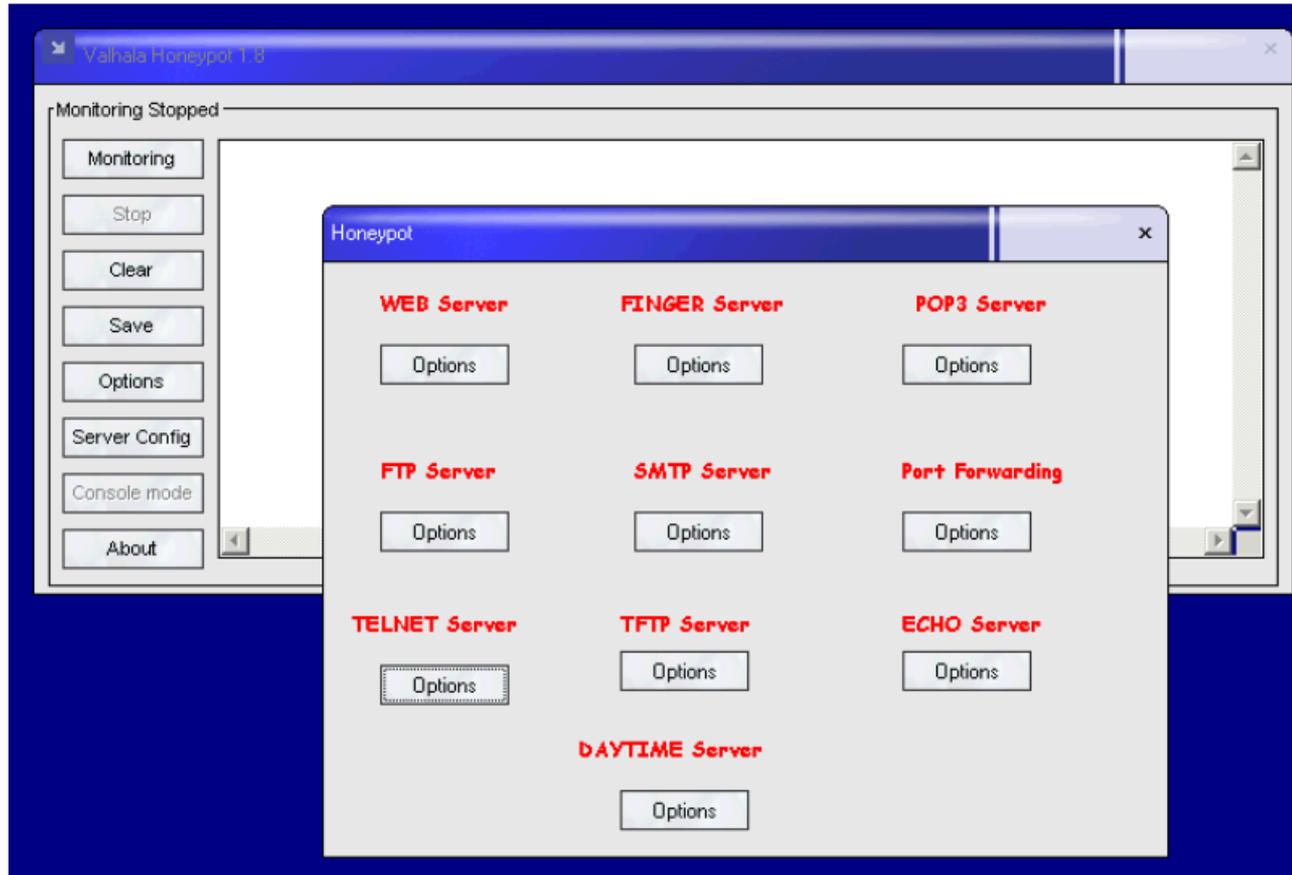
Virtual Lab Design



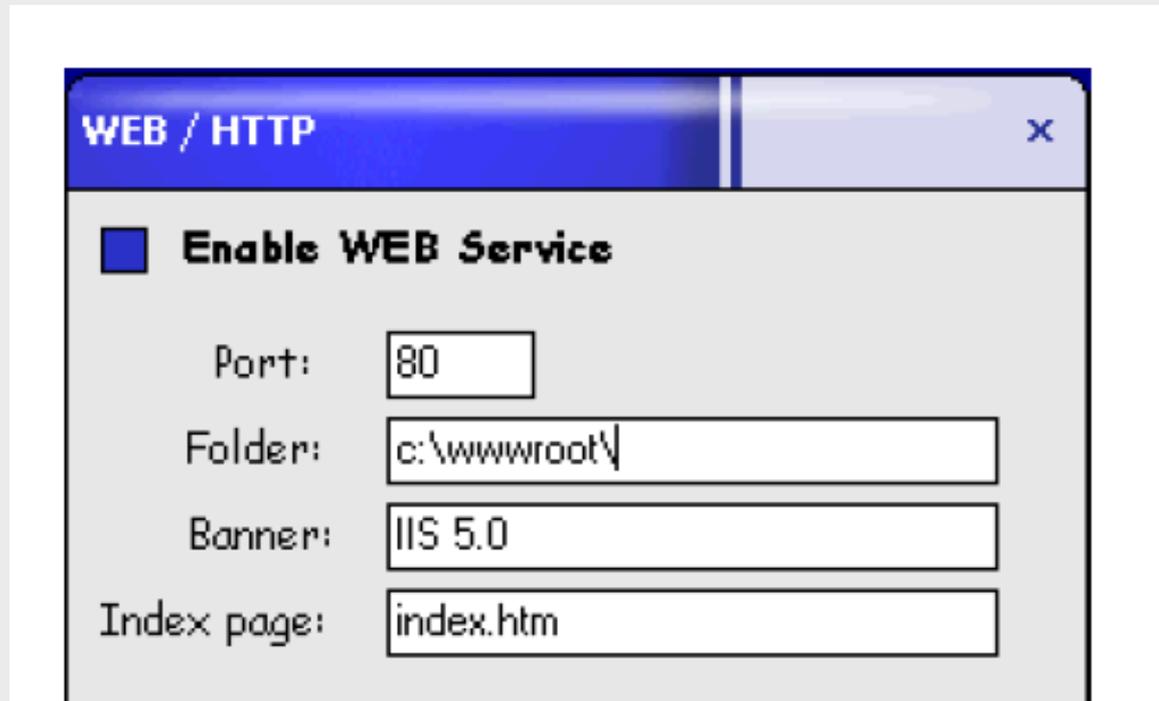
Configure as
honeypot



Configure Honey_pot as a Web Server



Web Server



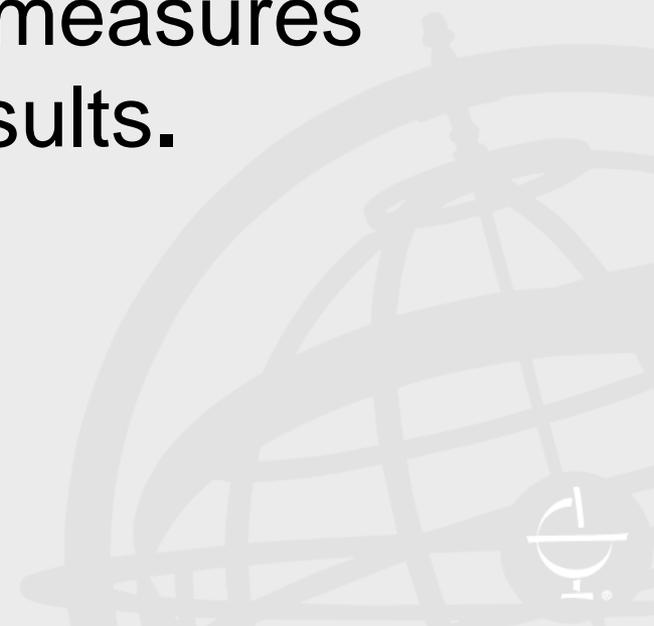
Activities

- Connect to the honeypot from the landing VM
- Conduct an NMAP scan
- Review logs and analyze the details effectiveness in detecting malware activity
- Assess the effectiveness of honeypots



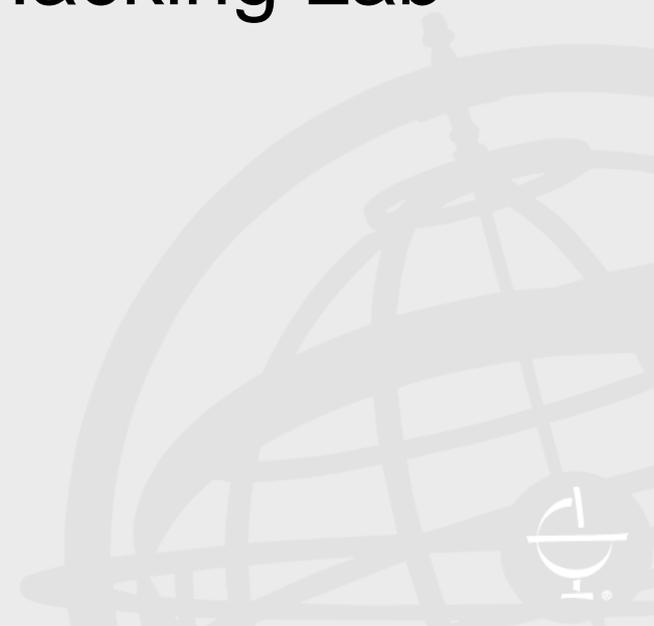
CYS 526 Cyber Attacks and Defenses

- Students will learn to assess target systems and networks for vulnerabilities and exploits, detect security threats, and recommend and implement defensive, corrective, and preventative measures based on penetration test results.



VMs used

- Windows 2003- Landing VM
- Security Onion- Intrusion Detection
- Windows XP Pro- Target System
- WebGoat- Web Application Hacking Lab
- BackTrack 5- Attack System



Active and Passive Info Gathering

- Web Recon
- Identify live hosts using ICMP ping command
- Identify open ports
 - Telnet, NetCat, NetDiscoverer
- Identify ports running services
 - Ports, running services, MAC address, OS
- Advanced NMAP operations
 - NULL Scan
 - XMAS Scan
 - SYN scan, OS scan, probe open ports

Exploiting a Windows target with Metasploit

- Establish Connectivity
- Armitage
- Discover attacks against target
- Research the Hail Mary attack
- Launch the Hail Mary attack
- Meterpreter
 - Getuid, getprivs, getsystem, hashdump



Hail Mary Vulnerability Attacks

The screenshot shows a Windows desktop environment with a Metasploit Meterpreter session running in Armitage. The console window displays the output of the 'sessions -v' command, listing active sessions with their IDs, types, information, connections, and via methods.

```
msf > sessions -v

Active sessions
=====

```

Id	Type	Information	Connection	Via
1	meterpreter	x86/win32 NT AUTHORITY\SYSTEM @ WINXP-NSP	172.16.90.4:33816 -> 172.16.90.6:11523	exploit/windows/smb/ms
08_067_netapi				
2	meterpreter	x86/win32 NT AUTHORITY\SYSTEM @ WINXP-NSP	172.16.90.4:32956 -> 172.16.90.6:23852	exploit/windows/smb/ms
06_040_netapi				
3	meterpreter	x86/win32 NT AUTHORITY\SYSTEM @ WINXP-NSP	172.16.90.4:48508 -> 172.16.90.6:5755	exploit/windows/dcerpc
/ms03_026_dcom				
4	meterpreter	x86/win32	172.16.90.4:44445 -> 172.16.90.6:31455	exploit/windows/smb/ms
08_067_netapi				

[*] Meterpreter session 4 opened (172.16.90.4:44445 -> 172.16.90.6:31455) at 2013-04-02 05:53:47 -0700
[*] Meterpreter session 5 opened (172.16.90.4:55735 -> 172.16.90.6:6770) at 2013-04-02 05:53:49 -0700
[*] Meterpreter session 6 opened (172.16.90.4:59459 -> 172.16.90.6:24754) at 2013-04-02 05:53:49 -0700
msf >

Maintaining Access

- Netcat/CryptCat for File Transfer and Backdoor
 - Setup communication between systems
 - Use NetCat/CryptCat to setup communication
 - Wireshark act as network sniffer
 - Use NetCat to setup a backdoor with root access to access BT5 from Security Onoion

Virtual Lab Setup

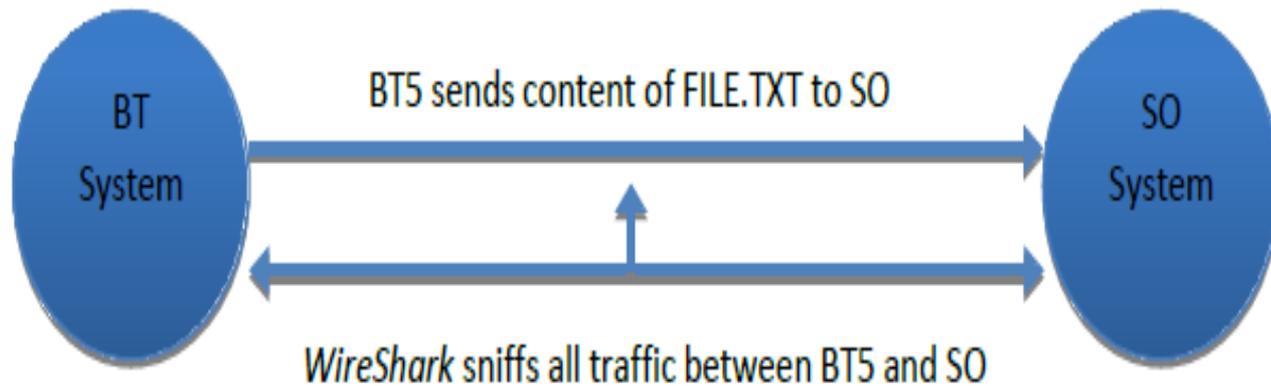


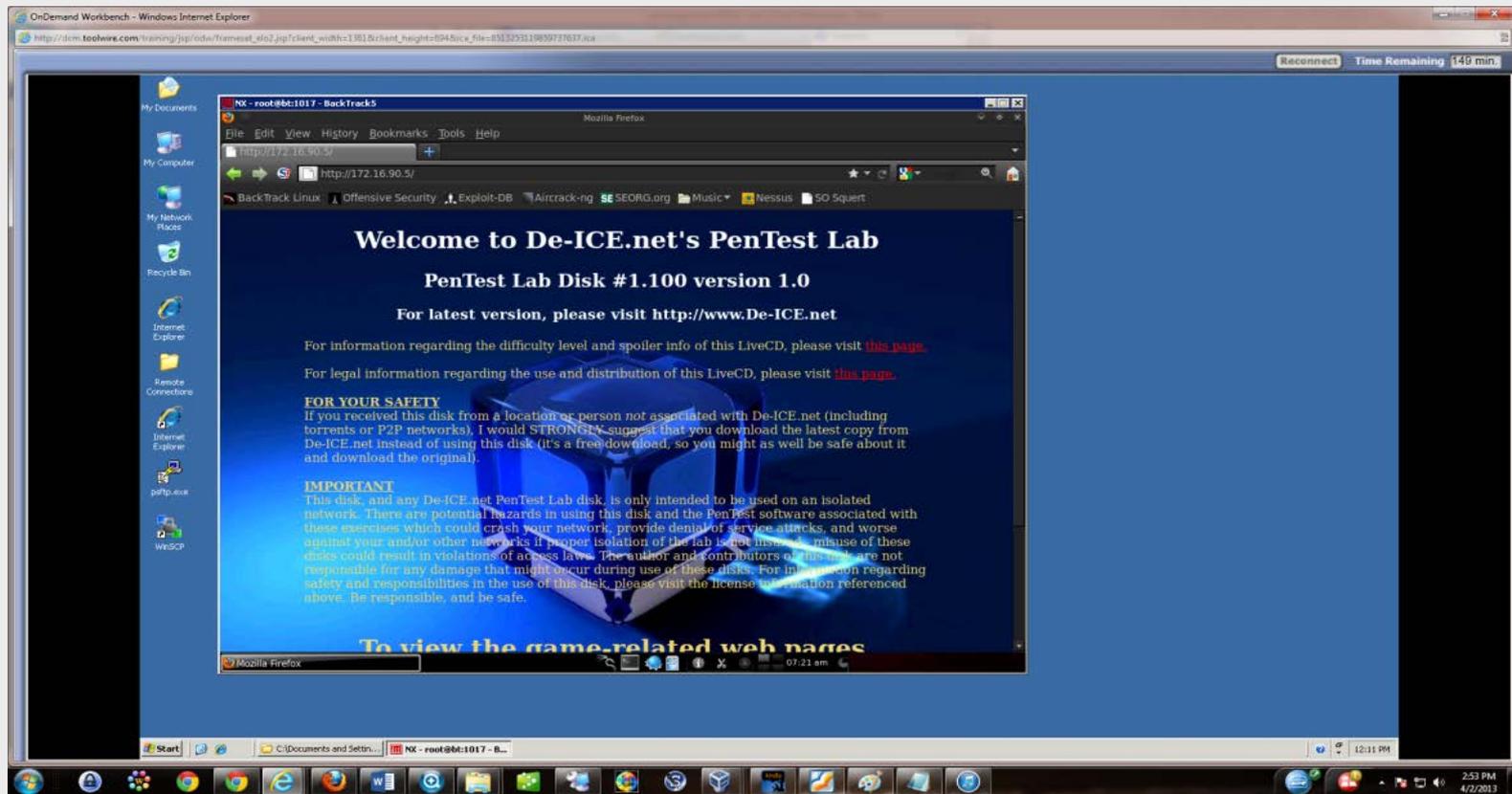
Figure 1: The lab setup with Wireshark

Lessons Learned

- Use of NetCat, Wireshark
- Maintaining access to a target during pen test
- Importance of encryption
- Functionality of backdoor



De-Ice Disk 1.100 Ethical Hacking Challenge



Rootkits and Defenses

- Hacker Defender rootkit
- Install rootkit
- Hxdef100.2INI
- Analyze and report on
 - Hidden services
 - Hidden Regkeys
 - Password to access the victim with infected rootkit



Execution of the Hacker-Defender rootkit:

The screenshot displays a Windows XP desktop environment with the following components:

- File Explorer (hacker_defender_1.0):** Shows the contents of a folder on the desktop. The address bar indicates the path: `C:\Documents and Settings\student\Desktop\Modu\`. The folder contains files: `bdd1100.exe`, `hudef100.2.ini` (Configuration Settings, 4 KB), `readme_en.txt` (Text Document, 36 KB), `readme_fr.txt` (Text Document, 38 KB), and `src.zip` (91 KB). A context menu is open over the folder, showing options like Open, Run as..., Send To, Cut, Copy, Create Shortcut, Delete, Rename, and Properties.
- Windows Task Manager:** Shows the 'Processes' tab with the following data:

Image Name	User Name	CPU	Mem Usage
msmsgs.exe	student	00	1,440 K
jshched.exe	student	00	3,624 K
explorer.exe	student	00	12,604 K
rdpclip.exe	student	00	2,794 K
winlogon.exe	SYSTEM	00	2,084 K
csrss.exe	SYSTEM	00	2,352 K
cmd.exe	student	00	1,072 K
taskmgr.exe	student	00	3,472 K
notepad.exe	student	00	320 K
notepad.exe	student	00	324 K
- Command Prompt (C:\WINDOWS\System32\cmd.exe):** Shows the output of the `netstat` command:

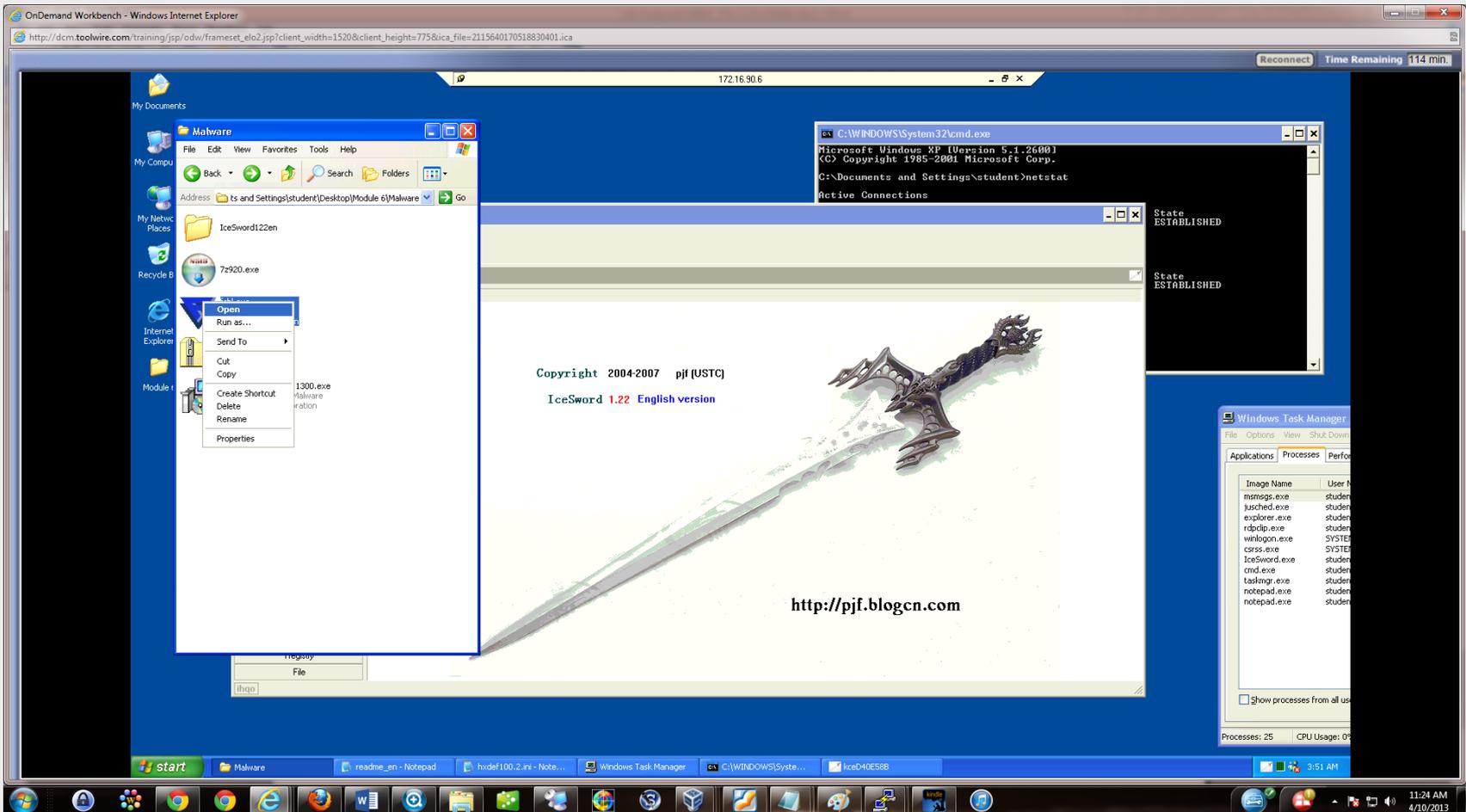
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\student>netstat

Active Connections

Proto Local Address           Foreign Address         State
TCP        winxp-nsp:3389          172.16.98.2:1045       ESTABLISHED
C:\Documents and Settings\student>
```

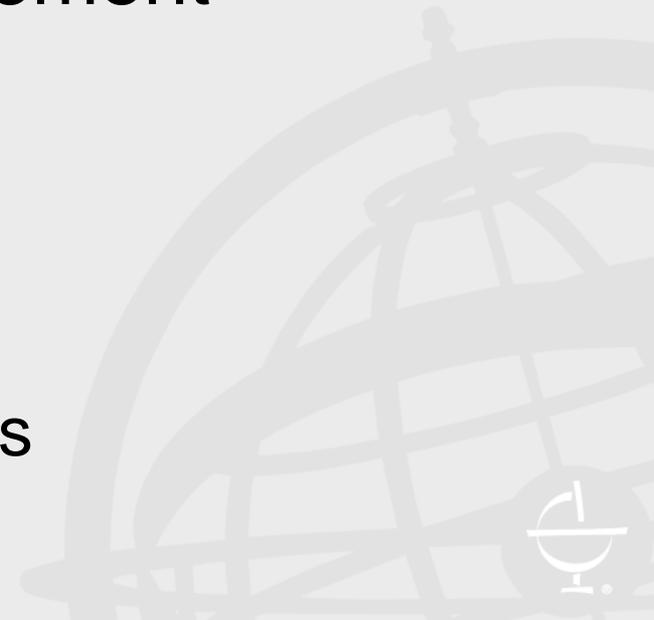
The taskbar at the bottom shows the Start button, several open applications (hacker_defender_1.0, readme_en - Notepad, hudef100.2.in - Note..., Windows Task Manager, C:\WINDOWS\System...), and the system tray with the time 3:46 AM and date 4/10/2013.

Rootkit countermeasures: Black-Light



Conclusion

- Online Education
 - Overcome the limitations of distance and time
- Cyber Security field requires technical and soft skills
- Learning environments to implement technician skills
 - Interactive tutorials
 - Virtual tools
 - Discussions
 - Case Studies and Group Projects



Questions

Dr. Sherly Abraham
Faculty Program Director IT and
Cybersecurity
Sabraham@excelsior.edu

Dr. Lifang Shih
Associate Dean
Lshih@excelsior.edu

School of Business and Technology
Excelsior College
7 Columbia Circle, Albany, NY 12203-515

