CSE 4481
Computer Security Lab

Mark Shtern

INTRODUCTION

Security

- Our life depends on computer systems
  - Traffic control
  - Banking
  - Medical equipment
  - Internet
  - Social networks
- Growing number of attacks on computer systems

Security

- Results from malicious attack
  - Financial loss
  - Loss of reputation
  - A drop in the value of a company’s stock
  - Legal issues
- Hacker may not be a computer expert
  - Numerous attacking scripts / tools available
  - Hacker training material also available

Statistics (2009)

- 85% of attacks were not considered highly difficult
- 96% of breaches were avoidable through simple or intermediate control
- 48% involved privileges misuse
- 86% of victims had evidence of the breach in their log files

Course Objectives

- Hands on experience in various security topics
  - Execution of popular attacks
  - Attack prevention and risk mitigation

Attack Examples

- Network (sniffing, session hijacking)
- Password Cracking
- Web
- Code injection
- Overflows (Buffer, Number)

Defence Techniques

- Auditing
- Vulnerability scanners
- Firewalls (Network and application)
- Intrusion Preventions and Detections
- Honeypots

Orientation

ATTACK LAB

Attack Lab

- Isolated Lab accessed through an IP KVM
- Attack Lab consists of
  - Physical equipment, such as servers, workstations and network switches
  - Virtual equipment, such as virtual machines and virtual switches
- Attack Lab has monitoring software that audits student activity

Attack Lab Policies

- Physical lab equipment, such as servers, routers, workstations and switches are not to be configured, attacked or modified in any manner
- Data in the attack lab can not be copied out of the attack lab
- The attack lab user password should not be reused in other systems

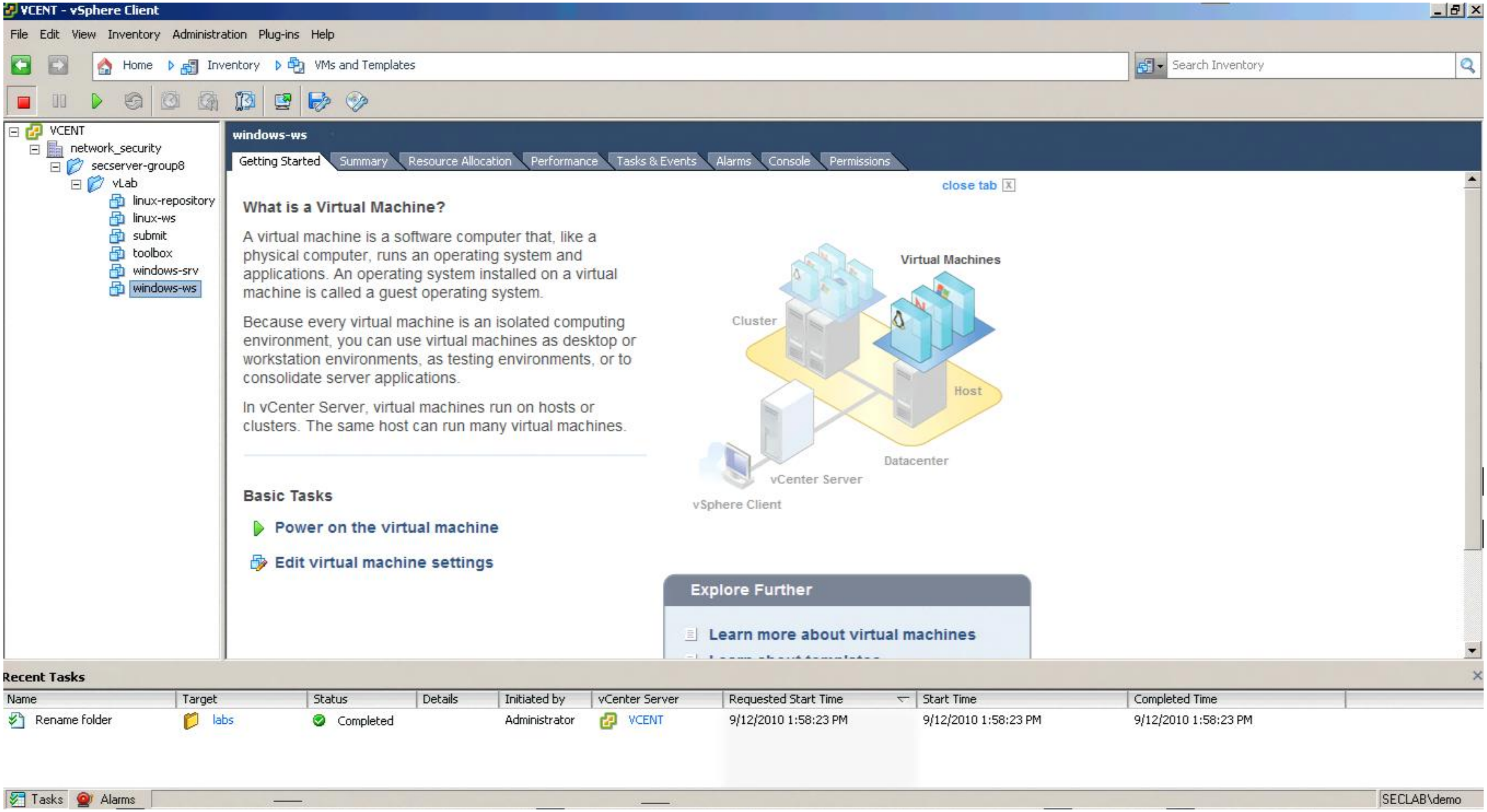
Attack Lab Policies

- Students are allowed to modify, configure, or attack their private Virtual Machines ***only*** within the scope of the lab exercises
- Violation of the Attack Lab policies may be considered an Academic Integrity offence

Access to attack lab

- Sign the security lab agreement to get your password
- Login at https://seclab.cse.yorku.ca / (https://seclab.cse.yorku.ca/install)
  - User name is CSE user name
- Click on vSphereClient
- Select "Use Windows session credentials"
- Click Login button

vLab



What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

In vCenter Server, virtual machines run on hosts or clusters. The same host can run many virtual machines.

Basic Tasks

Power on the virtual machine

Edit virtual machine settings

Explore Further

Learn more about virtual machines

Recent Tasks

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Time	Start Time	Completed Time
Rename folder	labs	Completed		Administrator	VCENT	9/12/2010 1:58:23 PM	9/12/2010 1:58:23 PM	9/12/2010 1:58:23 PM

How to use a VM CD-ROM

- Click on CD-ROM icon
- Select CD/DVD Drive 1
- Select “Connect to ISO image on local disk”
- Browse to “C:\ISOs” folder or your private folder
- Select CD-ROM image
- Access to CDROM from VM

How to transfer files into the lab (1)

- Create an ISO file that contains your files
    - *first.iso*
- Create an ISO file that contains first.iso
    - *second.iso*
- Click on Virtual Media and select *second.iso*
- Click on CDROM in Attack Lab machine and copy *first.iso* into Private Directory

How to transfer files into the lab (2)

- Start vSphere Client
- Select Virtual Machine
- Connect CDROM (the media name is *first.iso*)
- Copy files from CDROM into Virtual Machine

Add/Remove application

- Software package in Linux OS
  - apt-get install <package name>
  - apt-get remove <package name>
- Windows component
  - Insert Windows CD into Virtual Machine
  - Click on Add/Remove Program
  - Select/Deselect windows component

ADMINISTRIVIA

Marking Scheme

- The performance of the students will be evaluated as a combination of
    - 7 labs (50%)
    - Term Project (35%)
    - Project presentation (5%)
    - Game (5% + bonus)
    - Participation (5%)
- One week labs are worth 5%
- Two week labs are worth 10%

Labs

- Lab reports and source code must be submitted before 11:59pm on the day the lab is due
- The lab report must be a short, precise and professional document (title, table of contents, page numbering etc)
- The lab report must contain sufficient evidence that you completed the lab exercise
- Code developed during the labs is expected to be **simple**
- Developed applications are **prototypes**

Report antipattern

- Screenshots are attached
  - Figure number? Figure description?
- “I verified DNS configuration using nslookup”
  - How? Evidence?
- “I created a folder named ‘xxx’ and gave read/write and execute permission ...”
  - How? Evidence?
- “I developed a script ...”
  - Evidence? Script source code?

Term Project

- Teams
  - Teams are constructed by instructor
- Project consists of four phases
  - Implementation
  - Security testing
  - Fixing security bugs
  - QA phase
- Developed application is a **final product**
- The project report must be a detailed, precise and professional document (title, table of contents, page numbering etc)
- Submission by team’s lead only

Report Antipattern

- Design is just a list of functions
- Design justification : “The design is flexible”
  - Why is the design flexible?
- Test case : “Run the application”
  - What are the user inputs?
    What are the expected results?

Game

- Development Team
  - Project presentation
- QA Team
  - Review project design
  - Penetrate other teams’ projects
- IT Security
  - Secure infrastructure

LAB 1

Lab 1

- Read Lab 1
- Ask questions
- Add Administrative user

Lab 1

- Plan
  - Develop naming schema
  - Configure Windows 2003 server
  - Promote server to Domain Controller

Lab 1

- Plan
  - Test Connectivity
  - Test DNS
  - Join Workstation to Domain
  - Configure users

Lab 1

- Plan
  - Social Engineering

QUESTIONS?

Linux Repositories

- Configure static IP address
- cat /etc/apt/sources.list
  - # Karmic - 9.10
    - deb http://IP/ubuntu-karmic karmic main restricted universe multiverse
    - deb http://IP/ubuntu-karmic karmic-security main restricted universe multiverse
    - deb http://IP/ubuntu-karmic karmic-updates main restricted universe multiverse

Linux Repositories (Cont)

- cat /etc/apt/sources.list
  - # Breezy - 5.10
    - deb http://IP/ubuntu-breezy breezy main restricted universe multiverse