Kiểm thử & đánh giá an toàn hệ thống thông tin

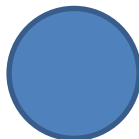
Module 1. Introduction to Pentesting and Methodologies

Thông tin giảng viên

TS. Lại Minh Tuấn

(Khoa ATTT – Học viện Kỹ thuật mật mã)

- Điện thoại: 0907-69-60-66
- Email: lmtuan.1989@gmail.com

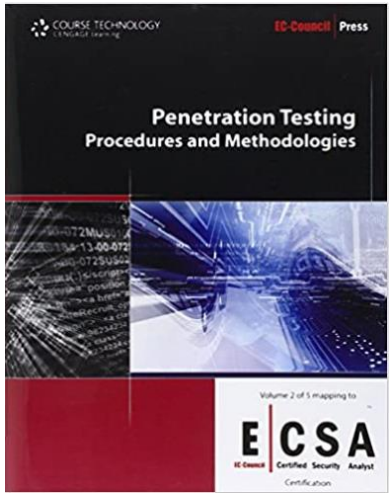


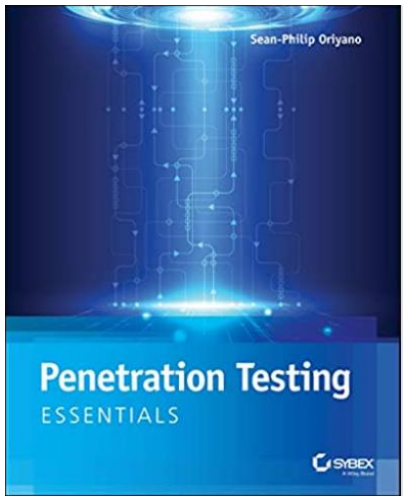
1. Giới thiệu học phần
2. Khái niệm tổng quan
3. Chuẩn bị hạ tầng

1. Giới thiệu học phần
2. Khái niệm tổng quan
3. Chuẩn bị hạ tầng

Giáo trình và Tài liệu tham khảo

1. Giáo trình "**Đánh giá & Kiểm định an toàn hệ thống thông tin**", Học viện KTMM, 2016.
2. EC-Council, **Penetration Testing: Procedures & Methodologies**
3. Wil Allsopp**, Advanced Penetration Testing: Hacking the World's Most Secure Networks**
4. Sean-Philip Oriyano, **Penetration Testing Essentials**
5. OSCP**, PEN-200: Penetration Testing with Kali Linux**
6. SANS**, SEC560: Enterprise Penetration Testing Course**





Nội dung học phần

1. Tổng quan về kiểm thử xâm nhập, quy trình thực hiện.
2. Phương pháp tìm kiếm và thu thập thông tin.
3. Phương pháp kiểm thử xâm nhập hệ thống mạng.
4. Thực hiện phân tích, đánh giá lỗ hổng bảo mật.
5. Tạo báo cáo về kiểm thử xâm nhập.

Cấu trúc học phần

- **Thời lượng**: 3tc = 60 tiết
  - 30 tiết lý thuyết
  - 30 tiết thực hành
- **Đánh giá kết quả học tập**
  - Điểm chuyên cần
    - Đi học đầy đủ, đúng giờ
    - Tham gia xây dựng bài
  - Điểm thực hành + BTL
  - Điểm thi kết thúc học phần: Thi trắc nghiệm

Bài tập lớn

Danh sách và Yêu cầu

1 Giới thiệu học phần

2 Khái niệm tổng quan

3 Chuẩn bị hạ tầng

Defining Terms (1/2)

Vulnerability	A flaw or weakness that can be exploited by a threat actor Examples: Buffer overflow, misconfiguration, design flaws
Exploit	Code or technique that takes advantage of a vulnerability Examples: Public exploit code, upload web shell to server
Threat	An agent or actor that can cause harm Examples: Human attacker, worm, user clicking on links
Risk	Potential for loss or damage Often calculated as: Risk = Likelihood * Impact

Defining Terms (2/2)

Pen Test	Identify security vulnerabilities that could let an attacker either penetrate the environment or steal information
Red Team	Designed to test detection and response capabilities
Purple Team	Cross-functional team consisting of Red and Blue Teamers
Vulnerability Assessment	Identify, quantify, and rank vulnerabilities (no exploitation)
Security Audit	Audit implies testing against a rigorous set of standards

Penetration Testing Goals (1/2)

- Kiểm thử xâm nhập - quá trình kiểm tra và đánh giá hiệu quả của các giải pháp đảm bảo an toàn thông tin được sử dụng trong công ty/tổ chức trước các mối đe dọa từ bên trong lẫn bên ngoài.
  - Mô phỏng lại các kỹ thuật tấn công được attacker sử dụng trên thực tế.
  - Tìm kiếm lỗ hổng (trước khi kẻ tấn công tìm được).
  - Khai thác lỗ hổng dưới một số điều kiện nhất định (theo phạm vi và Quy tắc - Rules of Engagement).

Penetration Testing Goals (2/2)

- Mục tiêu:
  - Xác định được các hiểm họa và xác suất tấn công lên tài sản.
  - Xác định được các tấn công tiềm tàng và khả năng ảnh hưởng lên công ty, tổ chức trong trường hợp tấn công thành công.
  - Biện pháp đối phó bổ sung để có thể giảm thiểu các mối đe dọa đối với hệ thống.
  - Kiểm tra độ hiệu quả của các giải pháp/ thiết bị bảo mật đang triển khai (firewall, ids…).

Vulnerability Assessment

- Định tính:
  - Lỗ hổng loại A (cao): cho phép người dùng từ xa có thể truy nhập trái phép vào hệ thống.
  - Lỗ hổng loại B (trung bình): cho phép người dùng cục bộ leo thang đặc quyền hoặc truy cập trái phép.
  - Lỗ hổng loại C (thấp): cho phép tấn công từ chối dịch vụ (DoS).
- Định lượng:
  - CVSS Score
  - https://www.first.org/cvss/

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Method

- Kiểm thử hộp đen (Blackbox)
- Kiểm thử hộp trắng (Whitebox)
- Kiểm thử hộp xám (Graybox)

Blackbox pentest (1/2)

- Người kiểm thử chỉ biết 1 số thông tin giới hạn về đối tượng (ip address, domain…)
- Sau khi kiểm thử có thể đưa ra càng nhiều thông tin về đối tượng càng tốt
- Việc kiểm thử mô tả lại quá trình tấn công trên thực tế và thu thập thông tin của đối tượng qua các kênh khác nhau
- Nhược điểm:
  - Không xác định được toàn bộ lỗ hổng trong hệ thống
  - Mang lại nhiều rủi ro cho hệ thống mạng
  - Các tấn công có thể bị hạn chế do tường lửa hoặc các hệ thống phòng thủ mạng

Blackbox pentest (1/2)

- Blind Testing
  - Tính thực tế cao do mô phỏng các phương pháp tấn công thực tế
  - Đội kiểm thử hoàn toàn không có thông tin (hoặc có thông tin giới hạn) về đối tượng
  - Tốn thời gian & công sức
- Double-Blind Testing
  - Chỉ có 1 vài người trong tổ chức biết về việc thực hiện kiểm thử
  - Hữu ích trong việc kiểm tra các biện pháp kiểm soát an toàn về mặt kĩ thuật, thực thi chính sách an toàn, khả năng phát hiện và ứng phó sự cố của nhân viên trong tổ chức

Whitebox pentest (1/2)

- Người kiểm thử biết tất cả thông tin về đối tượng (hạ tầng, topo mạng, thiết bị bảo mật, IP, chính sách bảo mật…)
- Hỗ trợ khả năng tìm bug và lỗ hổng một cách nhanh chóng
- Đảm bảo khả năng kiểm thử toàn diện đối tượng

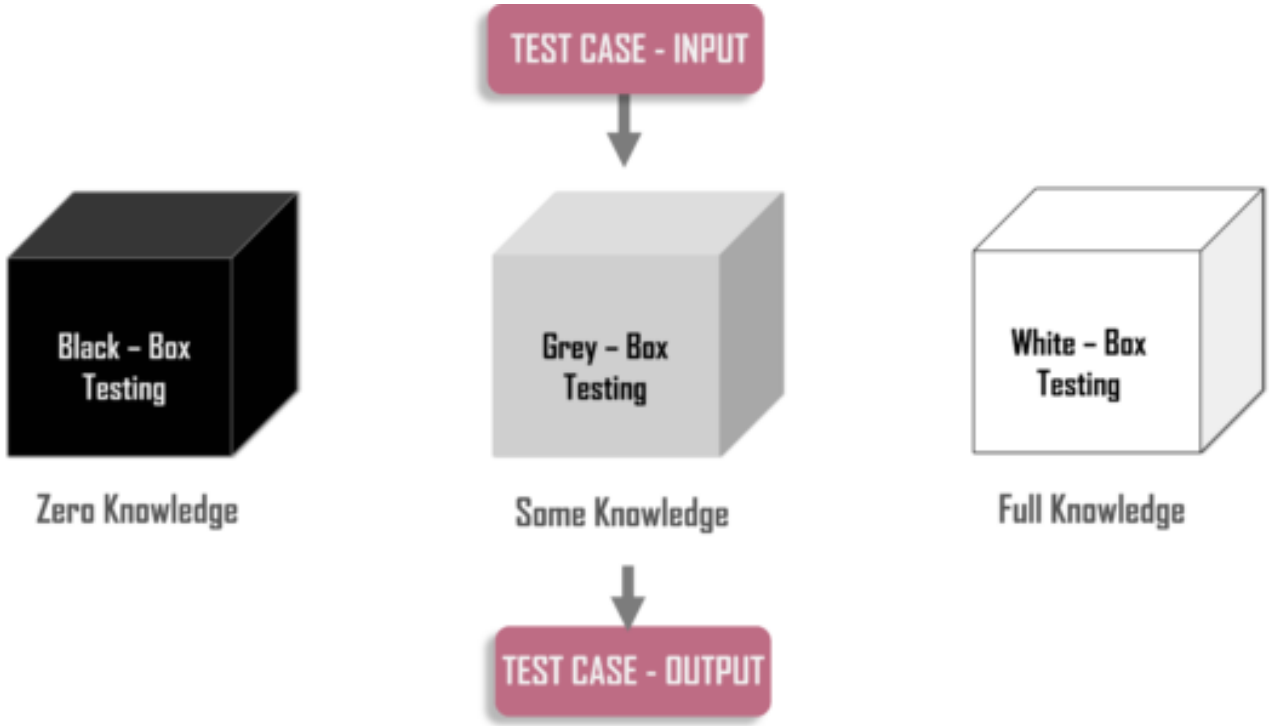
Whitebox pentest (2/2)

- Kiểm thử công khai (Announced Testing)
  - Thông báo cho mọi người trong tổ chức biết về việc thực hiện kiểm thử, đặc biệt là bộ phận IT.
  - Kiểm tra hiện trạng của hệ thống bảo mật trước các lỗ hổng.
- Kiểm thử bí mật (Unannounced Testing)
  - Không thông báo về việc kiểm thử, chỉ có người quản lý cao nhất biết.
  - Kiểm tra hiện trạng của hệ thống bảo mật trước các lỗ hổng và khả năng phản ứng, đối phó sự cố của bộ phận IT.

Graybox pentest

- Người kiểm thử biết giới hạn thông tin về đối tượng
- Thường mô phỏng lại quá trình tấn công từ các mối đe dọa nội bộ
- Việc thực hiện thường diễn ra khi đội kiểm thử đã thực hiện kiểm thử hộp đen và thu được 1 số thông tin nhất định

Blackbox vs whitebox vs graybox



Dạng kiểm thử	Giá thành	Mức độ toàn diện
Hộp đen	$$	x
Hộp trắng	$$$	xxx
Hộp xám	$	xx

Types of Penetration Tests

- Network services
- Assumed breach
- Web application
- SE
  - Email-based/Phone-based
- Wireless security
  - Không chỉ mình Wifi
- Physical security
- Product Test
  - Software package, hardware (IoT)
  - Bypass encryption…

Pentesting Methodology

- Ý nghĩa của phương pháp luận:
  - Cung cấp tính thống nhất và có cấu trúc cho việc đánh giá an toàn, từ đó có thể giảm thiểu rủi ro trong quá trình kiểm thử.
  - Giúp dễ dàng trong việc chuyển giao quy trình kiểm thử nếu có sự thay đổi nhân sự đánh giá.
  - Chỉ ra những hạn chế về tài nguyên kết hợp với các đánh giá an toàn.

Pentesting Methodology: Commercial

- EC-Council's LPT
- IBM
- ISS
- McAfee Foundstone

Pentesting Methodology: Open Source

- OWASP
  - Web Security Testing Guide (WSTG)
  - Mobile Security Testing Guide (MSTG)
  - Firmware Security Testing Methodology
- Penetration Testing Execution Standard
- PCI Penetration Testing Guide
- Penetration Testing Framework (PTF)
- Technical Guide to Information Security Testing and Assessment (NIST 800-115)
- Open Source Security Testing Methodology Manual (OSSTMM)

Sinh viên tham khảo thêm trong giáo trình và internet!!!

OWASP Web Application Security Testing

- 4.0 Introduction and Objectives
- 4.1 Information Gathering
- 4.2 Configuration and Deployment Management Testing
- 4.3 Identity Management Testing
- 4.4 Authentication Testing
- 4.5 Authorization Testing
- 4.6 Session Management Testing
- 4.7 Input Validation Testing
- 4.8 Testing for Error Handling
- 4.9 Testing for Weak Cryptography
- 4.10 Business Logic Testing
- 4.11 Client-side Testing
- 4.12 API Testing

Example – LPT Pentesting Methodology

- Step 1. Information Gathering
- Step 2. Scanning & Reconnaissance
- Step 3. Fingerprinting & Enumeration
- Step 4. Vulnerability Assessment
- Step 5. Exploit Research & Verification
- Step 6. Reporting

Attack Phases

- Các giai đoạn tấn công phổ biến

- Attacker & Red Teams thường đi xa hơn
  - Duy trì quyền truy cập (cài đặt backdoor, rootkit)
  - Xóa hoặc che dấu các hành vi độc hại (sử dụng kênh ngầm, chỉnh sửa log, che dấu file độc hại)
- Các giai đoạn này không phải lúc nào cũng được thực hiện theo thứ tự.
  - Khi có quyền truy cập tới 1 máy -> tiến hành lại quá trình Recon & Scan

Overall Penetration Testing Process

- Chuẩn bị:
  - Ký cam kết không tiết lộ (Non-Disclosure Agreement - NDA).
  - Thảo luận về Quy tắc (Rules of Engagement) và phạm vi của việc kiểm thử.
  - Ký giấy phép và thông báo về nguy cơ khi thực hiện kiểm thử.
  - Giao nhiệm vụ cho team.
- Kiểm thử
- Kết luận
  - Thực hiện phân tích chi tiết.
  - Viết báo cáo.

Overall Penetration Testing Process

- Goals:
  - Dữ liệu quan trọng bị mất sẽ ảnh hưởng như thế nào?
  - Tại sao phải thực hiện test (tuân thủ, triển khai hệ thống mới..)
- Type of tests (Network, web, SE…)
- Scope - IP, subnets, URL, people/roles
  - Những gì nên tránh?
- Rules of Engagement
  - Checklist
  - Thêm ngoại lệ…
- Kickoff Call
  - Xác định phương thức liên lạc, kết nối

1 Giới thiệu học phần

2 Khái niệm tổng quan

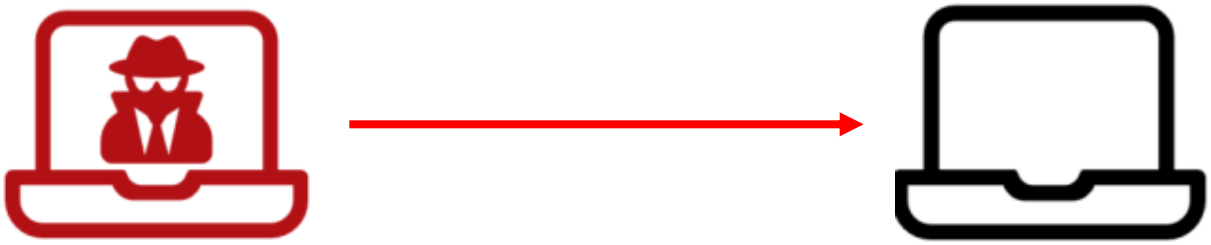
3 Chuẩn bị hạ tầng

Building Infrastructure

- Xây dựng môi trường lab trước khi tiến hành kiểm thử
  - Cơ sở hạ tầng (Infrastructure)
  - Công cụ & kỹ thuật
- Nên sử dụng Windows hay Linux?
  - Nên sử dụng cả 2 bởi vì có những công cụ hoạt động tốt trên Windows nhưng có những công cụ hoạt động tốt hơn trên Linux
  - Chuyển đổi giữa Windows & Linux nếu cần sử dụng VMs
  - Đôi khi cần sử dụng cả MacOS (iOS mobile pentesting)
  - Kali Linux: https://www.kali.org/
  - Parrot Linux: https://parrotlinux.org/

Nomenclature & Iconography

- Testing System/Attack System.
  - Hệ thống được sử dụng bởi pentester/ethical hacker để đánh giá mức độ an toàn của máy tính mục tiêu.
  - Thường được gọi là Máy tấn công (attack machine).
- Target, Victim, User, Server.
  - Hệ thống cần được đánh giá mức độ an toàn.
  - Thường được gọi là Máy nạn nhân (Victim machine).



Attack machine

Victim machine

Building a Lab

- Thử nghiệm các công cụ và kỹ thuật mới trong môi trường lab.
  - Đảm bảo rằng các công cụ, dòng lệnh hoạt động chính xác sẽ giúp tiết kiện thời gian khi kiểm thử thực tế.
  - Sử dụng VMs: revert, store, clone…để nâng cao hiệu quả.
- Servers.
  - Windows Domain & Domain Controller).
  - Windows File Share & IIS Server.
  - Linux (Centos, Ubuntu, Fedora).
- End User System.
  - Windows 10.

Cloud Infrastructure

- Scanning, exploitation, Command & Control (C2)
  - Nhà cung cấp dịch vụ: Digital Ocean, Amazon, Azure, Linode…
- Password cracking
  - Amazon cung cấp các phiên bản GPU hữu ích cho việc bẻ khóa
  - Bẻ khóa sử dụng NPK trong AWS (https://github.com/c6fc/npk)

Sources for Free Tools and Exploits

- Exploit-DB: https://www.exploit-db.com/
  - Chứa shellcode, exploits, papers
- US-CERT:https://www.cisa.gov/news-events/cybersecurity-advisories
  - Chứa thông tin mới về các lỗ hổng bảo mật
- MITRE CVE Repository: https://cve.mitre.org/
- Luôn luôn kiểm tra công cụ và mã khai thác trước khi sử dụng

Users: Root and non-root

- Nguyên tắc đặc quyền tối thiểu – sử dụng đặc quyền chỉ khi cần (tương tự attacker trên thực tế).
- Non-root users
  - Dấu nhắc "$"
  - Home directory: /home/username
- Root users
  - Dấu nhắc "#"
  - Home directory: /root
- Tạo (backdoor) account: useradd username
- Đổi mật khẩu passwd
  - Đổi mật khẩu tài khoản khác (must be root): passwd username

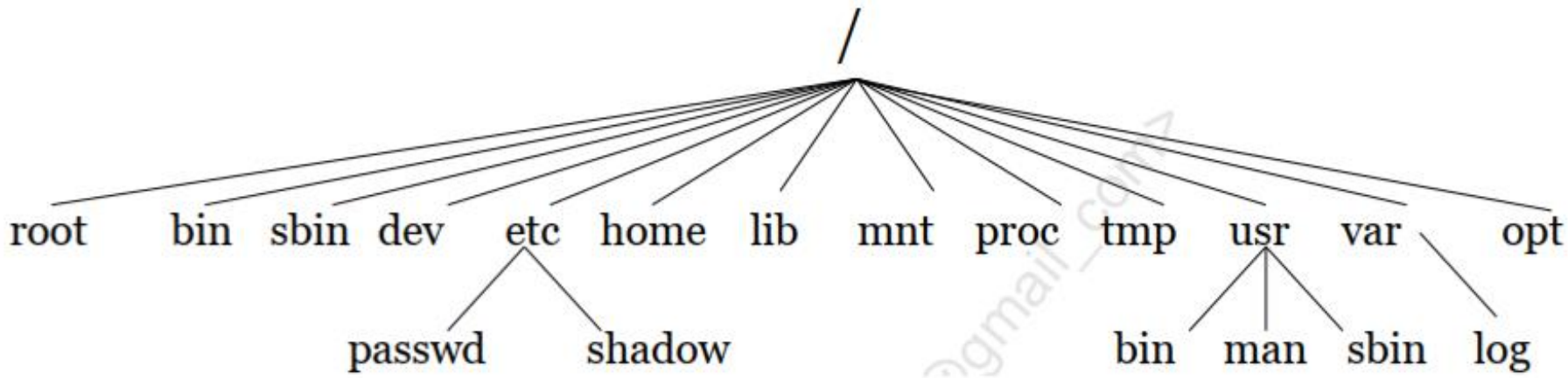
Who Am I?

- Kiểm tra thông tin tài khoản/quyền truy cập, user id và groups id:
  - whoami
  - id

```
whoami
clark
id
uid=1000(clark) gid=1000(clark) groups=1000(clark),24(cdrom),27(sudo),29(aud…
./exploit
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
```

Linux File System Structure

- Thư mục gốc / (root).
- Filesystem có thể khác nhau đối với các bản phân phối của Linux và BSD.



Where Am I?

```
pwd
/var/www
```

When you gain access to a new system, you may not know your current location. Use `pwd` to "print working directory"

```
cd /etc
pwd
/etc
```

With a continuous shell we can change directories as normal

```
cd /etc
pwd
/var/www
```

With an ephemeral shell, each command is independent, so changing directories doesn't quite work the same

With an ephemeral shell (common with command injection), you will often need to fully path files and directories, such **`ls /etc/apache2`**

```
sec560@slingshot:~/coursefiles$ ls
metadata  sam.txt  sam_lower_case.txt
```

List the contents of a directory with `ls dir`
Use `ls` by itself to look in the current directory

Permissions

```
drwxr-xr-x 2 root sec560   4096  Jun 2 202  metadata
-rwsr-xr-x 1 root root   149080  Jan 1 2023  /usr/bin/sudo
```

Permissions are broken into **4 parts**

Type directory (d), regular file (-), symbolic link (l), FIFO (p), ...

User Read (r), Write (w), and Execute (x) – Also known as owner

Group Read (r), Write (w), and Execute (x)

Other Read (r), Write (w), and Execute (x)

s is executable, but you gain the permission of the owner (SETUID) or group (SEGUID)

Change permissions with the **chmod** command

Escalating with SETUID

```
$ find / -perm -4000 -ls 2>/dev/null
-rwsr-xr-x   1 root     root        43088 Sep 16  2020 /bin/mount
-rwsr-xr-x   1 root     root        44664 Mar 22  2019 /bin/su
-rwsr-xr-x   1 root     root        64424 Jun 28  2019 /bin/ping
-rwsr-xr-x   1 root     root        26696 Sep 16  2020 /bin/umount
-rwsr-xr-x   1 root     root        30800 Aug 11  2016 /bin/fusermount
-rwsr-xr-x   1 root     root       149080 Jan 19  2021 /usr/bin/sudo
-rwsrwxrwx   1 root     root        50472 Jun  5  2021 /usr/local/bin/updater
```

Look for files with the SETUID and SETGID bit set as they may allow escalation!
In this case, we can overwrite "updater" and escalate!

- find / –uid 0 –perm –4000 –type f 2>/dev/null
- find / –perm –2000 –type f 2>/dev/null

Escalation

❑ Một số cách để thực thi câu lệnh với đặc quyền nâng cao:

```
sec560@slingshot:~$ sudo vim /etc/passwd
Password: sec560 account password
```

Run a single command as root
Requires current user's password

```
sec560@slingshot:~$ sudo -i
Password: sec560 account password
root@slingshot:~#
```

Get a root shell
Requires current user's password

```
sec560@slingshot:~$ su -
Password: root account password
root@slingshot:~#
```

Get a root shell and env variables
Requires root's password

Use `sudo -l -l` (two lowercase L's as in list) to list allowed sudo commands
Misconfiguration of `sudoers` often leads to privilege escalation, sometimes without a password!

- Lệnh sudo được cấu hình trong /etc/sudoers
- sudo –u username command

Common Linux commands

Command	Description
`mkdir directory`	Create a directory
`cp file1 file2`	Copy
`rm file`	To delete a directory, use the -rf (recursive, force) flags
`mv obj1 obj2`	Move a file or directory (also for renaming)
`grep somestring [file]`	Search through output for somestring in output or file
`echo sometext`	Display a line of text
`ps aux`	List processes
`cat filename`	Show the contents of a file
`head filename`	Show the first 10 lines of a file, use -n X to specify the number lines
`tail filename`	Show the last 10 lines of a file, use -n X to specify the number lines
`netstat -nap`	Show connections. -n numeric ports. -a listening and established. -p show PID.
`lsof -Pni`	Show connections. -P numeric ports. -n IP address instead of name. -i network.
`man command`	Look at the manual (help) for a command

Thank you & Any questions?