



# OSCP VÀ CƠ HỘI NGHỀ NGHIỆP TRONG LĨNH VỰC KIỂM THỬ PHẦN MỀM

Cơ sở an toàn thông tin

Người hướng dẫn: Thầy Trần Nhật Long



**Nhóm 14**

# Thành viên



**Trần Thị Hà**



**Nguyễn Văn  
Hiệp**



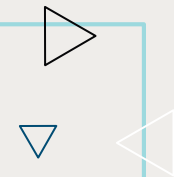
**Nguyễn Thị  
Quỳnh**



**Phạm Đăng  
Chính**

# Nội dung trình bày

- 01** — Kiểm thử xâm nhập
- 02** — Chứng chỉ OSCP
- 03** — Cơ hội nghề nghiệp
- 04** — Thực hành



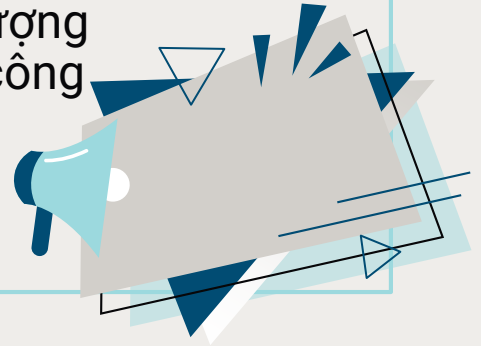
01

# Kiểm thử xâm nhập



# Pentest là gì?

- **Pentest:** Là cố gắng xâm nhập vào hệ thống để phát hiện ra những điểm yếu tiềm tàng của hệ thống mà tin tặc có thể khai thác và gây thiệt hại
- **Đối tượng pentest:** hệ thống máy tính, web app, mobile app, hạ tầng mạng, IoT, ứng dụng và hạ tầng cloud, API, source code, hoặc một đối tượng IT có kết nối với internet và có khả năng bị tấn công



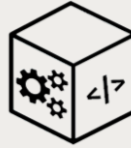


# Các loại pentest



## Black box

Xâm nhập vào hệ thống từ bên ngoài và sẽ hoàn toàn không biết gì về hệ thống đó



## White box

Pentester biết trước các thông tin của hệ thống như: IP, sơ đồ hạ tầng, mã nguồn...



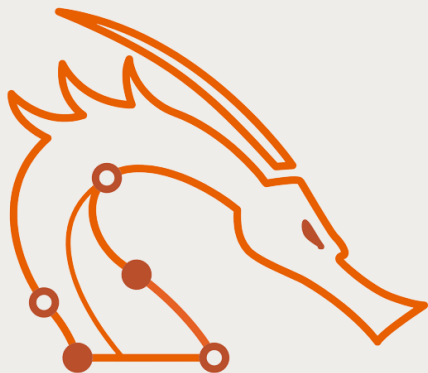
## Gray box

Có thông tin về một số đối tượng của hệ thống nhưng không có quyền truy cập vào toàn bộ đối tượng



02

# Chứng chỉ OSCP



# OSCP là gì?

- Offensive Security Certified Professional
- Hướng đến các Pentester
- Kali Linux
- 100% thực hành



BY OFFENSIVE SECURITY





# PWK/PEN-200



## Individual

**\$1499**

- 90 ngày truy cập phòng lab
- Một lần kiểm tra
- Tự hướng dẫn



## Learn One


**\$2499**

- Một khóa học
- 365 ngày truy cập phòng lab
- Hai lần thi
- Nội dung độc quyền



## Unlimited

**\$5499**

- Tất cả các khóa học
  - 365 ngày truy cập phòng lab
  - Thi không giới hạn
  - Nội dung độc quyền
- 

# Nội dung các khoá học của OffSec



**Kiến thức về các  
lỗ hổng và cách  
khai thác**

**Áp dụng các  
nguyên tắc bảo  
mật thông tin**



**Các giai đoạn  
tấn công**

**Xây dựng tư duy**





# Nội dung khoá học PWK/PEN-200

- Penetration Testing
- Information Gathering
- Getting Comfortable with Kali Linux
- Vulnerability Scanning
- Web Application Attacks
- Command Line Fun
- Buffer Overflows
- Client-Side Attacks
- Practical Tools
- Locating Public Exploits
- Bash Scripting



# Nội dung khoá học PWK/PEN-200

- Fixing Exploits
- File Transfers
- Antivirus Evasion
- Privilege Escalation
- Password Attacks
- Port Redirection and Tunneling
- Active Directory Attacks
- The Metasploit Framework
- PowerShell Empire
- Assembling the Pieces
- Trying Harder: The Labs

# Kiến thức cần thiết

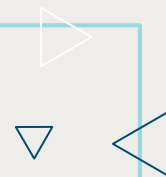
- Kiến thức về mạng máy tính
- Kiến thức về hệ điều hành Linux và Windows
- Kiến thức cơ bản về web server, database
- Thành thạo một ngôn ngữ lập trình (python, C,...)
- Sử dụng google và các công cụ

# Mạng máy tính

## Giao thức TCP/IP:

- Là một bộ các giao thức trao đổi thông tin được sử dụng để kết nối các thiết bị mạng trên Internet.
- Có thể được sử dụng như là một giao thức trao đổi thông tin trong một mạng riêng.

# Một số giao thức phổ biến



Port Number	Protocol	Service
20	TCP	File Transfer Protocol(FTP) Data Transfer
21	TCP	FTP Command Control
22	TCP	Sercure Shell (SSH)
23	TCP	Telnet - Remote login service
25	TCP	Simple Mail Transfer Protocol (SMTP) Email Routing
80	TCP	Hypertext Transfer Protocol
110	TCP	Post Office Protocol (POP3)
143	TCP	Internet Message Access Protocol(IMAP)
443	TCP	HTTP Secure (HTTPS) HTTP over TLS/SSL
3389	TCP and UDP	Microsoft Terminal Server (RDP)



# Hệ điều hành

- Làm quen và thành thục với shell trên linux; Powershell, cmd trên Windows như: man, mkdir, ls, apt, grep, curl,...
- Làm quen với một số trình soạn thảo như nano, vim
- Viết shell script, powershell script
- Cấu trúc hệ thống tệp và các file hệ thống



# Database, Web server

- Kiến thức cơ bản về nhiều loại Database như: MySQL, MSSQL Server, Oracle, noSQL,...
- Cổng sử dụng cho từng loại database và cách kết nối tới nó
- Một số kiểu tấn công lỗ hổng web như LFI, RFI, XSS, SQLi, SSRF,...

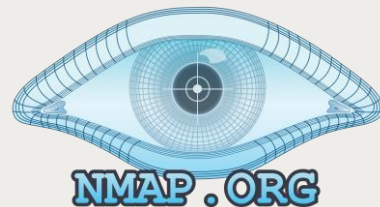
# Ngôn ngữ lập trình

- Kiến thức cơ bản về ngôn ngữ lập trình web như: HTML, Javascript, php,...
- Nên thành thạo một loại ngôn ngữ (đặc biệt là python)



# Công cụ

- Google
- Biết sử dụng các công cụ như: Reconbot, nmap, ffuf, Impacket, hashcat, nuclei, ...



# Hình thức thi

- VPN riêng có chứa các máy để tấn công
- Có 24 giờ để hoàn thành bài thi và 24 giờ để viết báo cáo và tải lên cờ (flag)
- Chia sẻ màn hình, trò chuyện và webcam (không có âm thanh)
- Trên 70 điểm sẽ được cấp chứng chỉ

# Cấu trúc bài thi

**01**

**20 điểm**

Cần 2 bước: lên được shell quyền user thấp và leo quyền lên user cao nhất  
Nếu có BOF thì khai thác thành công chỉ có quyền user thấp, cần phải leo quyền lên

**02**

**20 điểm**

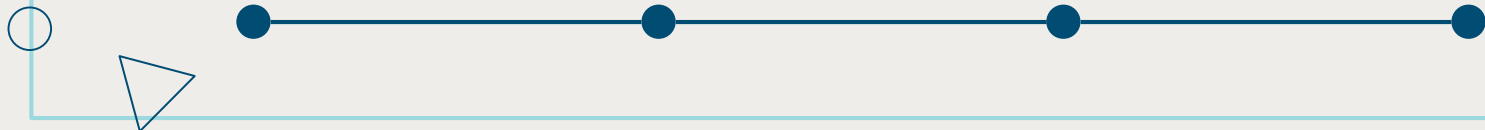
**03**

**20 điểm**

**04**

**40 điểm**

Active Directory  
gồm 2 máy client  
và 1 máy domain  
controller.



# Lưu ý về kỳ thi

## Thí sinh không được phép sử dụng một số công cụ:

- Các công cụ hoặc dịch vụ thương mại như: Metasploit Pro, Burp Pro
- Các công cụ khai thác tự động như: db\_autopwn, browser\_autopwn, SQLmap, SQLninja
- Máy quét lỗ hổng bảo mật hàng loạt như: Nessus, NeXpose, OpenVAS, Canvas, Core Impact, SAINT

03

# Cơ hội nghề nghiệp



# Cơ hội nghề nghiệp

- OSCP đang được đánh giá rất cao trong những chứng chỉ bảo mật hiện nay
- Đạt được chứng chỉ OSCP có thể giúp chứng minh kỹ năng, kiến thức, kinh nghiệm của người đó





# Vị trí công việc



● **Penetration Tester**

● **Security Consultants**

● **Security Auditors**

● **Security Engineers**

04

Thực hành





# THANKS

Do you have any questions?

[nhom14.oscp@gmail.com](mailto:nhom14.oscp@gmail.com)

+84 920 421 838

