**Giải pháp đào tạo doanh nghiệp:**

**Nội dung khóa học CompTIA Pentest + PT0-003**

1. **Tổng quan**

**Tại sao chọn khóa học này?**

1. Truy cập theo yêu cầu: Học theo tốc độ của riêng bạn, mọi lúc, mọi nơi.
2. Phòng thí nghiệm thực hành: Thực hành các kỹ thuật kiểm tra thâm nhập trong thế giới thực.
3. Hướng dẫn của chuyên gia: Học hỏi từ các chuyên gia an ninh mạng hàng đầu trong ngành.
4. Thăng tiến nghề nghiệp: Nâng cao sơ yếu lý lịch của bạn với chứng chỉ được công nhận trên toàn cầu.

Đăng ký ngay bây giờ và bắt đầu hành trình trở thành người kiểm tra thâm nhập được chứng nhận với Khóa học CompTIA Pentest + (PTO-003). Đừng bỏ lỡ cơ hội này để thăng tiến sự nghiệp an ninh mạng của bạn!

**Ai nên đăng ký?**

1. Những người thử nghiệm thâm nhập **đầy** tham vọng  **và tin tặc có đạo đức**.
2. Các chuyên gia CNTT muốn chuyên về **an ninh mạng**.
3. Bất kỳ ai chuẩn bị cho kỳ **thi chứng chỉ CompTIA Pentest +**.
4. **Thời lượng: 5 ngày (6 mô-đun - 90 bài học - 40 giờ theo yêu cầu)**

* 6 mô-đun, 90 bài học, 4 tài nguyên có thể tải xuống
* Truy cập trên thiết bị di động, Máy tính để bàn
* Quyền truy cập trọn đời
* Giấy chứng nhận hoàn thành

1. **Khán giả**
2. Bạn muốn chuyển từ CNTT Cơ bản sang Yêu cầu tiêu chuẩn Triển khai ISO 27001/27002.
3. Bạn muốn tìm hiểu cách áp dụng bảo mật và logic trong cơ sở hạ tầng CNTT có COSO tiêu chuẩn.
4. Bạn muốn giảm bớt căng thẳng khi chuyển từ kiến thức CNTT truyền thống sang kiểm toán CNTT nội bộ, cần khảo sát, phân tích để hiểu và quản lý giám sát hoạt động và nâng cấp vá phần mềm hệ thống kinh doanh và tìm hiểu một cách thay thế để dọn dẹp, chuyển đổi và trực quan hóa phần mềm của tổ chức.
5. **Điều kiện tiên quyết**

Bạn nên có những hiểu biết hoặc kiến thức sau:

1. Hiểu biết về các khái niệm được trình bày trong E-Learning LMS, tự học và Phòng thí nghiệm tự học trực tuyến.
2. Kiến thức về các khái niệm cơ bản về Máy tính, Mạng, Lưu trữ, Quy trình làm việc CNTT và Bảo mật.
3. Có kinh nghiệm sử dụng CEH và hoặc CompTIA Security (nếu có).
4. **Mục tiêu**
5. Giám đốc điều hành CNTT hoặc Quản trị viên CNTT.
6. Phân tích kinh doanh & kinh doanh thông minh.
7. Ngành nghề kinh doanh kiểm toán nội bộ
8. KNIME cho người dùng Excel trong kiểm toán nội bộ.
9. Khóa học này bằng cách cung cấp các dịch vụ giáo dục của bạn để giúp bạn hoàn thành mục tiêu của họ và trở thành người giỏi nhất trong nghề nghiệp của họ hoặc khám phá một con đường sự nghiệp mới.
10. **Yêu cầu**
11. Tôi khuyến khích bạn tham gia khóa học cấp tốc về Nhận thức về An ninh mạng cho người mới bắt đầu trước.
12. Máy tính xách tay / Máy tính để bàn có Wi-Fi / LAN có thể truy cập Internet miễn phí.
13. Trình duyệt web để truy cập Labs Online của Giáo viên đã sẵn sàng (không thể tải xuống).
14. **Đề cương khóa học**

**Mô-đun 1 - Quản lý tương tác**

***1.1 Hoạt động trước khi tham gia***

***1.2 Hoạt động hợp tác và truyền thông***

***1.3 Khung và phương pháp thử nghiệm***

*1.3.1 Kiểm tra MITRE ATT & CK*

***1.4 Đánh giá quản lý tương tác***

**Mô-đun 2 - Trinh sát và Liệt kê**

***2.1 Trinh sát thụ động***

*2.1.1 Hack của Google*

***2.2 Trinh sát tích cực***

*2.2.1 Quét cổng và lấy dấu vân tay*

*2.2.2 Theo dõi đường dẫn mạng với Traceroute*

*2.2.3 Đánh chặn dữ liệu bằng Wireshark*

*2.2.4 Cạo web*

***2.3 Kỹ thuật liệt kê***

*2.3.1 Liệt kê thư mục*

*2.3.2 Liệt kê email*

***2.4 Tập lệnh trinh sát và liệt kê***

*2.4.1 Sử dụng tập lệnh*

***2.5 Công cụ trinh sát và liệt kê***

*2.5.1 Thực hiện OSINT với Recon ng*

*2.5.2 Thêm khóa API vào Recon ng*

*2.5.3 Khám phá IoT với Shodan*

*2.5.4 Thực hiện tra cứu WHOIS*

*2.5.5 Thực hiện tra cứu DNS*

*2.5.6 Sử dụng tập lệnh NMAP*

*2.5.7 Thực hiện OSINT với theHarvester*

***2.6 Đánh giá trinh sát và liệt kê***

**Mô-đun 3 - Phát hiện và phân tích lỗ hổng bảo mật**

***3.1 Phát hiện lỗ hổng bảo mật***

*3.1.1 Thực hiện quét lỗ hổng với OpenVAS*

*3.1.2 Thực hiện phân tích mã tĩnh*

***3.2 Trinh sát, quét và phân tích đầu ra đếm***

***3.3 An ninh vật lý***

*3.3.1 Sao chép huy hiệu RFID*

*3.3.2 Sao chép NFC với Flipper Zero*

***3.4 Đánh giá phát hiện và phân tích lỗ hổng bảo mật***

**Mô-đun 4 - Tấn công và khai thác**

***4.1 Ưu tiên và chuẩn bị các cuộc tấn công***

***4.2 Tấn công mạng***

*4.2.1 Thực hiện một cuộc tấn công trên đường đi*

*4.2.2 Thực hiện một cuộc tấn công mạng với Metasploit*

*4.2.3 Di chuyển Meterpreter sang một quy trình khác*

*4.2.4 Tạo trình nhỏ phần mềm độc hại với Msfvenom*

*4.2.5 Sử dụng Netcat*

*4.2.6 Chụp tệp bằng Wireshark*

***4.3 Tấn công xác thực***

*4.3.1 Cưỡng bức vũ phu với Medusa*

*4.3.2 Vượt qua hàm băm*

*4.3.3 Phun mật khẩu bằng Hydra*

*4.3.4 Vượt qua đòn tấn công token*

*4.3.5 Xác thực giả mạo với Responder*

*4.3.6 Bẻ khóa mật khẩu Linux với John the Ripper*

*4.3.7 Bẻ khóa mật khẩu Hashcat*

***4.4 Các cuộc tấn công dựa trên máy chủ***

*4.4.1 Leo thang đặc quyền với Eternal Blue*

*4.4.2 Nhật ký Tampering*

*4.4.3 Pwn một mục tiêu Linux từ đầu đến cuối*

***4.5 Tấn công ứng dụng web***

*4.5.1 Thực hiện di chuyển thư mục*

*4.5.2 Lấy mật khẩu với SQL Injection*

*4.5.3 SQLi trên một trang web trực tiếp Phần 1*

*4.5.4 SQLi trên một trang web trực tiếp Phần 2*

*4.5.5 Chèn lệnh*

*4.5.6 Tiêm iFrame với XSS được lưu trữ*

*4.5.7 Phá vỡ DOM*

*4.5.8 Lạm dụng IDOR với Burp Suite*

*4.5.9 Chiếm quyền điều khiển phiên web*

*4.5.10 Tham số Tampering với Burp Suite*

***4.6 Tấn công dựa trên đám mây***

*4.6.1 Hack S3 Buckets*

***4.7 Tấn công không dây***

*4.7.1 WiFi Bí ngô Evil Twin*

*4.7.2 Cuộc tấn công crack WPA2*

*4.8 Tấn công kỹ thuật xã hội*

*4.8.1 Lừa đảo cho thông tin đăng nhập*

*4.8.2 Mồi nhử cáp OMG*

***4.9 Các cuộc tấn công hệ thống chuyên biệt***

*4.9.1 Pwn một thiết bị di động*

*4.10 Tấn công tập lệnh tự động*

*4.11 Đánh giá các cuộc tấn công và khai thác*

**Mô-đun 5 - Hậu khai thác và chuyển động bên**

***5.1 Thiết lập và duy trì sự kiên trì***

*5.1.1 Tạo cửa sau Netcat liên tục*

*5.1.2 Khai thác dữ liệu với một nhiệm vụ đã lên lịch*

***5.2 Chuyển động ngang***

*5.2.1 Chuẩn bị xoay trục*

*5.2.2 Chuyển động ngang thông qua Pivoting*

***5.3 Giai đoạn và Lọc máu***

*5.3.1 Ẩn dữ liệu bằng Steganography*

*5.3.2 Tự động lấy cắp dữ liệu*

***5.4 Dọn dẹp và phục hồi***

*5.5 Đánh giá sau khai thác và chuyển động bên*

**Mô-đun 6 - Diliverables**

***6.1 Các thành phần báo cáo kiểm tra thâm nhập***

***6.2 Báo cáo phát hiện và khuyến nghị***

***6.2.1 Kiểm tra báo cáo Pentest***

***6.3 Đánh giá sản phẩm***

***6.4 Kết luận cuộc đua***

1. **Lộ trình học tập:**

**1. Phân tích khảo sát Pentest (Bạn đang ở đây) > 2. Tổ chức Bảo mật > 3. Attache Đào tạo môi trường mô phỏng > 4. CySA+ (bảo vệ AI/ML) > 5. CASP+**