Bộ tài liệu CTF - guguo

Môn Chủ nghĩa xã hội khoa học (Trường Đại học Tiền Giang)

==========

CTF - WEB

Web Security là khai thác các lỗ hổng tồn tại trên website, khắc phục những lỗ hổng đó đó để trang web trở nên an toàn hơn.

Đi cùng với sự phát triển của Internet, hệ thống các website ngày càng đa dạng. Các dịch vụ web từ blog, mạng xã hội đến các trang web thanh toán online, ... đều đã quá quen thuộc với mọi người. Nhưng đằng sau sự tiện lợi đó luôn tồn tại những rủi ro về bảo mật, đặc biệt là bảo mật thông tin người dùng. Thông qua cách hoạt động của web, attacker/hacker có thể lợi dụng những lỗ hổng để có thể tấn công, cài đặt mã độc và phá hoại các website. Vì thế, Web Security ra đời để chống lại những attacker/hacker ấy.

Để giải quyết các thử thách CTF thuộc lĩnh vực Web Security, các kỹ năng tối thiểu mà một người chơi CTF nên trang bị bao gồm:

- Các kiến thức: HTML, Javascript, PHP, SQL, ...
- Hoạt động của website từ phía client cho đến phía server, HTTP request, HTTP response, HTTP Headers, HTTP methods
- Các câu lệnh của hệ điều hành: Windows (Command Prompt), Linux (Terminal).
- Tìm hiểu các lỗi căn bản từ top 10 OWASP: OWASP Top 10 là một báo cáo được cập nhật thường xuyên về các nguy cơ bảo mật đối với bảo mật ứng dụng web, tập trung vào 10 rủi ro/lỗ hổng quan trọng nhất. Báo cáo được tổng hợp bởi một nhóm các chuyên gia bảo mật từ khắp nơi trên thế giới.

Công cụ dùng trong khai thác lỗ hổng:

- Burpsuite
- Nessus, OWASP ZAP
- Bộ công cụ được cài đặt sẵn trong hệ điều hành Kali Linux: cung cấp rất nhiều công cụ penetration testing như OpenVAS-zap, Metasploit Framework, Sqlmap, Maltego, Nmap, Nikto, ...

Một số lỗ hổng web phổ biến:

- SQL injection: SQL Injection là một kỹ thuật lợi dụng những lỗ hổng về câu truy vấn của các ứng dụng. Được thực hiện bằng cách chèn thêm một đoạn SQL để làm sai lệnh đi câu truy vấn ban đầu, từ đó có thể khai thác dữ liệu từ database.và thực hiện các hành vi bất hợp pháp.
- Cross Site Scripting (XSS): Cho phép attacker/hacker chèn những đoạn mã độc hại của hacker vào website và thực thi tại trình duyệt của người dùng. Mục đích chính của cuộc tấn công này là ăn cắp dữ liệu nhận dạng của người dùng như: cookies, session tokens và các thông tin khác. Như chúng ta biết, cookie giúp chúng tôi đăng nhập tự động. Do đó với cookie bị đánh cắp, chúng ta có thể đăng nhập bằng các thông tin nhận dạng khác. Và đây là một trong những lý do, tại sao cuộc tấn công này được coi là một trong những cuộc tấn công nguy hiểm nhất.
- Local File Inclusion: Cho phép attacker/hacker truy cập vào các file nhạy cảm trái phép.

Một số trang web các em có thể sử dụng để luyện tập CTF rất hiệu quả:

- https://ctflearn.com/: Nền tảng CTF với các challenge do cộng đồng người chơi đóng góp
- https://picoctf.org/: Đây là giải CTF dành cho học sinh, sinh viên mức độ dễ phù hợp cho những người mới chơi CTF

- https://www.root-me.org/?lang=en: Trang CTF của Pháp bao gồm đầy đủ các lĩnh vực với mực đồ đề dễ đến khó, Trong mỗi challenges đều có mô tả và tài liệu về lỗ hổng
- https://ctf.viblo.asia/
- https://webhacking.kr/: Trang CTF chuyên về lỗ hổng bảo mật Web

==========

CTF - COMPUTER FORENSIC

Computer Forensics là việc thu thập, bảo vệ, phân tích chứng cứ số, lập báo cáo và trình bày lại những thông tin thực tế từ các nguồn dữ liệu số để tái hiện lại các sự kiện nhằm tìm ra hành vi vi phạm và dự đoán các hoạt động xâm nhập trái phép, tấn công hoặc gây gián đoạn quá trình làm việc của hệ thống.
Forensic trong CTF là dạng bài yêu cầu kiểm tra, phân tích phần thông tin ẩn trong các tệp dữ liệu tĩnh.

Để giải quyết các thử thách CTF thuộc lĩnh vực Forensics, các kỹ năng hữu ích nhất mà một người chơi CTF nên trang bị bao gồm:

- Biết một ngôn ngữ scripting: Python, bash script,...
- Biết cách thao tác dữ liệu nhị phân (thao tác mức byte) bằng ngôn ngữ lập trình scripting
- Hệ điều hành: Linux, windows,...
- Nhận diện được các định dạng, giao thức (protocol), cấu trúc các tệp (structure) và mã hóa (encoding) trong các tập tin
- "Khả năng ngoại cảm" (khả năng phán đoán, kinh nghiệm khi điều tra)

Trong CTF, Forensics gồm một số dạng bài thường gặp sau:

- Điều tra bộ nhớ (memory forensics: bộ nhớ RAM)
- Ẩn giấu thông tin (Steganography)
- Điều tra bộ nhớ lưu trữ (Hard Drive Forensics)
- Điều tra mạng (Network forensics)
- ...

Một số trang web các em có thể sử dụng để luyện tập CTF rất hiệu quả:

- https://ctflearn.com/: Nền tảng CTF với các challenge do cộng đồng người chơi đóng góp
- https://picoctf.org/: Đây là giải CTF dành cho học sinh, sinh viên mức độ đề dễ phù hợp cho những người mới chơi CTF
- https://www.root-me.org/?lang=en: Trang CTF của Pháp bao gồm đầy đủ các lĩnh vực với mực đồ đề dễ đến khó, Trong mỗi challenges đều có mô tả và tài liệu về lỗ hổng
- https://ctf.viblo.asia/

==========

CTF - CRYPTO

Cryptography (mật mã học) là một ngành chuyên nghiên cứu về những thuật toán biến đổi thông tin từ "tin đọc được" (plaintext) thành "tin mã hóa" (ciphertext) và ngược lại. Trong các thử thách CTF, người chơi sẽ phải tìm ra thuật toán mã hóa và dùng ngôn ngữ lập trình để tìm cách mã hóa đúng thông điệp hoặc giải mã ra tin đọc được để tìm ra câu trả lời.

Để bắt đầu với mảng Crypto bạn cần chuẩn bị:

- Tìm hiểu thêm về các loại mã hóa như MD5, SHA-256, SHA-512,... và 2 chiều như Base64,... hay các cơ số được dùng phổ biến như hex, decimal, binary.

- Ngoài ra khả năng lập trình cũng là một yêu cầu cần thiết, Python là một trong những ngôn ngữ phù hợp với nguồn thư viện rộng lớn và dễ sử dụng nên khá phổ biến trong giới Crypto.

Một số trang web các em có thể sử dụng để luyện tập CTF rất hiệu quả:

- https://ctflearn.com/: Nền tảng CTF với các challenge do cộng đồng người chơi đóng góp
- https://picoctf.org/: Đây là giải CTF dành cho học sinh, sinh viên mức độ dễ phù hợp cho những người mới chơi CTF
- https://www.root-me.org/?lang=en: Trang CTF của Pháp bao gồm đầy đủ các lĩnh vực với mực đồ dễ đến khó, Trong mỗi challenges đều có mô tả và tài liệu về lỗ hổng
- https://ctf.viblo.asia/
- https://cryptohack.org/: Đây là trang web tổng hợp nhiều vấn đề xoay quanh mật mã, được chia thành các chủ đề cụ thể. Bên cạnh việc rèn luyện, CryptoHack còn có cả cộng đồng để thảo luận, trao đổi kiến thức.
- https://cryptopals.com: trang web để học mật mã, gồm những thử thách cơ bản đến những vấn đề vô cùng thực tiễn. Ngoài ra còn giúp các bạn nâng cao kỹ năng lập trình của mình

==========

CTF - REVERSE

Reverse Engineering (Kỹ thuật dịch ngược) hay gọi tắt RE là quá trình tìm ra các nguyên lý kỹ thuật của một phần mềm ứng dụng hay thiết bị cơ khí qua việc phân tích cấu trúc, chức năng và hoạt động của nó. Từ đó làm thay đổi cách hoạt động của chương trình đã được lập trình sẵn theo ý muốn của mình

Reverse Engineering được áp dụng cho nhiều mục đích khác nhau:

- Phân tích mã độc
- Cracking là hành động viết ra những chương trình con nhằm vô hiệu hoá đi những giới hạn của nhà sản xuất đối với các phần mềm để từ đó có thể sử dụng lâu dài phần mềm.
- Thẩm định tính an toàn cũng như phát hiện các lỗ hổng của phần mềm, bổ sung thêm tính năng vào chương trình

Để giải quyết các thử thách CTF thuộc lĩnh vực Reverse, các kỹ năng hữu ích nhất mà một người chơi CTF nên trang bị bao gồm:

- Ngôn ngữ lập trình: C/C++, Python.
- Mã máy Assembly x86, x64.

Một số công cụ hỗ trợ dịch ngược:

- Disassemblers: IDA, Radare2
- Decompilers: Công cụ chuyển đổi bytecode của ngôn ngữ bậc cao như C#, Java, ... về mã nguồn gốc (ví dụ: dnSpy, Bytecode Viewer, ...)
- Debuggers: Công cụ phân tích binary cho phép chương trình chạy từng lệnh và hiển thị giá trị trên bộ nhớ và trạng thái của các thanh ghi tại thời điểm đó (ví dụ: OllyDBG, GDB)
- Hex editors: Cho phép nhìn thấy từng byte trong binary và thay đổi chúng (ví dụ: 010 editor, Hex Editor)

Một số trang web các em có thể sử dụng để luyện tập CTF rất hiệu quả:

- https://ctflearn.com/ (Nền tảng CTF với các challenge do cộng đồng người chơi đóng góp)
- https://picoctf.org/ (Đây là giải CTF dành cho học sinh, sinh viên mức độ dễ phù hợp cho những người mới chơi CTF)

+ https://www.root-me.org/?lang=en: Trang CTF của Pháp bao gồm đầy đủ các lĩnh vực với mực đồ đề dễ đến khó, Trong mỗi challenges đều có mô tả và tài liệu về lỗ hổng
+ https://ctf.viblo.asia/
+ http://reversing.kr/: Trang CTF dành cho các bạn yêu thích các thử thách về Reverse

==========

CTF - MISC

Nhiều thử thách trong CTF sẽ hoàn toàn ngẫu nhiên và yêu cầu kết hợp nhiều kỹ năng khác nhau để có thể giải được thử thách, không có một phương thức giải cố định nào có thể áp dụng cho từng thử thách. Để có thể tìm ra được đáp án, bạn cần phải nhanh nhạy, sáng tạo, nghĩ được những cách giải quyết mới, không giống bình thường. Ngoài ra bạn cũng có thể tham gia thật nhiều các cuộc thi CTF để tích lũy thêm kinh nghiệm.

Để giải quyết các thử thách CTF thuộc lĩnh vực Misc, bạn cần trang bị một số kiến thức về các mảng như:

+ OSINT/Recon/Trivia: Điều tra, phân tích thông về các mục tiêu, cá nhân cho trước trên internet
+ System admin: Thiết lập, xây dựng cấu hình, phân tích cấu hình mạng, cấu hình hệ thống
+ Stegano: Sử dụng các kỹ thuật tìm kiếm thông tin ẩn giấu trong các file ảnh, file âm thanh, file mã hóa...

Một số trang web giúp các em luyện tập các thử thách OSINT:

+ https://medium.com/week-in-osint
+ https://www.digital.security/en/blog/write-defcon-25-recon-village-osint-ctf
+ https://www.linkedin.com/pulse/trendmicro-ctf-2017-osint-challenge-write-up-motasem-hamdan/