VSL - VKU Security Lab

Cẩm nang cho người mới.

BẢO MẬT MÁY TÍNH, AN TOÀN THÔNG TIN

Bảo mật máy tính và **an toàn thông tin** là hai khái niệm liên quan chặt chẽ nhưng có một số khác biệt.

1. **Bảo mật máy tính**:
   - Tập trung vào việ và phần cứng khỏi các mối đe dọa như virus, ma .
   - Các biện pháp bả diệt virus, tường lửa, mã hóa dữ liệu và các chí
2. **An toàn thông tin**:
   - Định nghĩa rộng h đến bảo vệ thông tin từ mọi loại mối đe dọa, b
   - An toàn thông tin n bao gồm chính sách, quy trình và người dù h toàn vẹn và khả năng sẵn sàng của thông ti

Cả hai lĩnh vực này đều rất nhân, dữ liệu doanh nghiệp và các hệ thống thông tin qua về một chủ đề cụ thể nào không?

BẢO MẬT MÁY TÍNH, AN TOÀN THÔNG TIN LÀ GÌ?

- https://vnhacker.blogspot.com/2012/05/lam-toan-thong-tin-thi-hoc-gi.html
- https://blog.cyberjutsu.io/2021/08/09/hoc-an-toan-thong-tin/
- https://whitehat.vn/threads/kien-thuc-co-ban-ve-an-ninh-mang.4373/

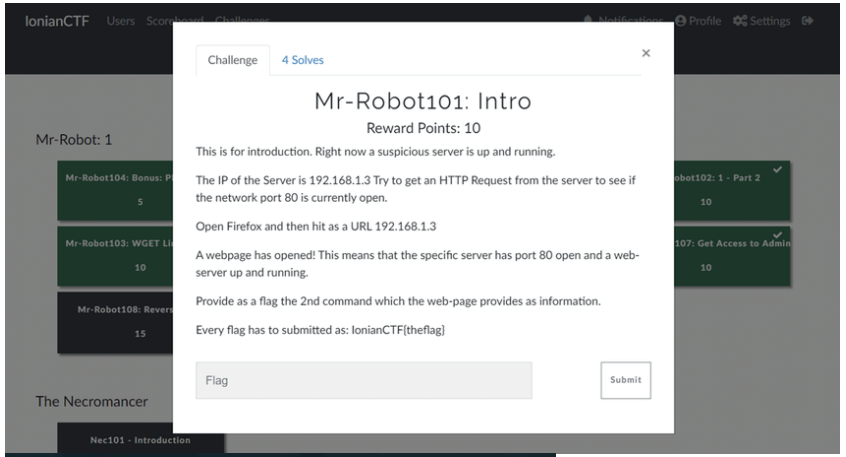
CTF - Capture The Flag

CTF - Capture The Flag: Đây là cuộc thi dành cho giới bảo mật. Cuộc thi này được lập ra để các đôi, chuyên gia bảo mật trên thế giới rèn luyện kỹ năng an ninh mạng và là cơ hội để học hỏi và chia sẻ kiến thức với cộng đồng an toàn thông tin

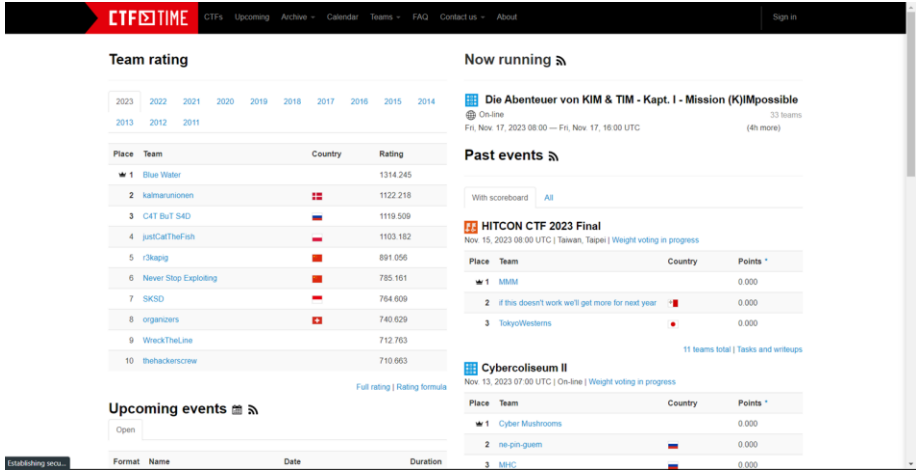
Rất nhiều tổ chức lớn tạo ra các giải CTF để có thể tìm kiếm các nhân sự Bảo mật: Google, FireEyes, DEF CON, các trường đại học lớn, ...

CTF - Capture The Flag

- Mục tiêu: Sử dụng các kỹ năng khai thác lỗi, hacking để có thể lấy được một cờ (Flag) được giấu ở bên trong thử thách. Có thể tham gia theo cá nhân hoặc theo đội nhóm.
- Cờ sẽ có dạng: Flag{...}
- Đội chiến thắng sẽ bằng cách dành lấy các cờ nhanh nhất và đạt điểm tối đa.



CTF - Capture The Flag



- Xem và theo dõi các CTF đang, sẽ và đã diễn ra qua trang CTF Time
https://ctftime.org

- Các cuộc thi CTF được tổ chức diễn ra hằng ngày, hằng tuần theo cả 2 hình thức offline và online.
- Giải thưởng của cuộc thi CTF sẽ là tiền, các chứng nhận và phần quà đặc biệt.

Giới thiệu các mảng trong bảo mật

- Web exploitation: Tấn công và khai thác các lỗ hổng trên ứng dụng web.
- Forensic: Điều tra, thu thập, phân tích các chứng cứ số, ...
- Cryptography: Kỹ thuật mã hóa, khai thác và tấn công các loại mã hóa, nghiên cứu các loại mã hóa mới, ...
- Reverse Engineering: Dịch ngược, xem mã nguồn và cách hoạt động của chương trình.
- Binary Exploitation (PWN): Khai thác các lỗ hổng phần mềm.
- Và nhiều mảng khác...

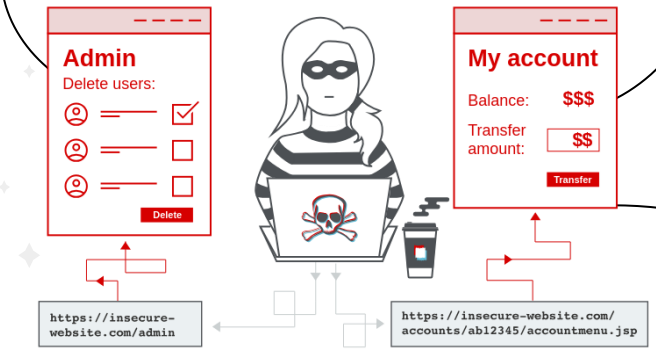
WEB SECURITY

CÔNG VIỆC TIỀM NĂNG

Một trong những chuyên ngành về An Ninh Mạng và đang được săn đón rất nhiều

PHÁT TRIỂN

Có thể phát triển để trở thành một thành viên của **RED TEAM** tài năng.



CÁC CÔNG VIỆC SẼ LÀM

Review Source Code
Kiểm tra những lỗ hổng logic
Hóa thân thành hacker
Xâm nhập vào hệ thống

KIẾN THỨC DỰ KIẾN

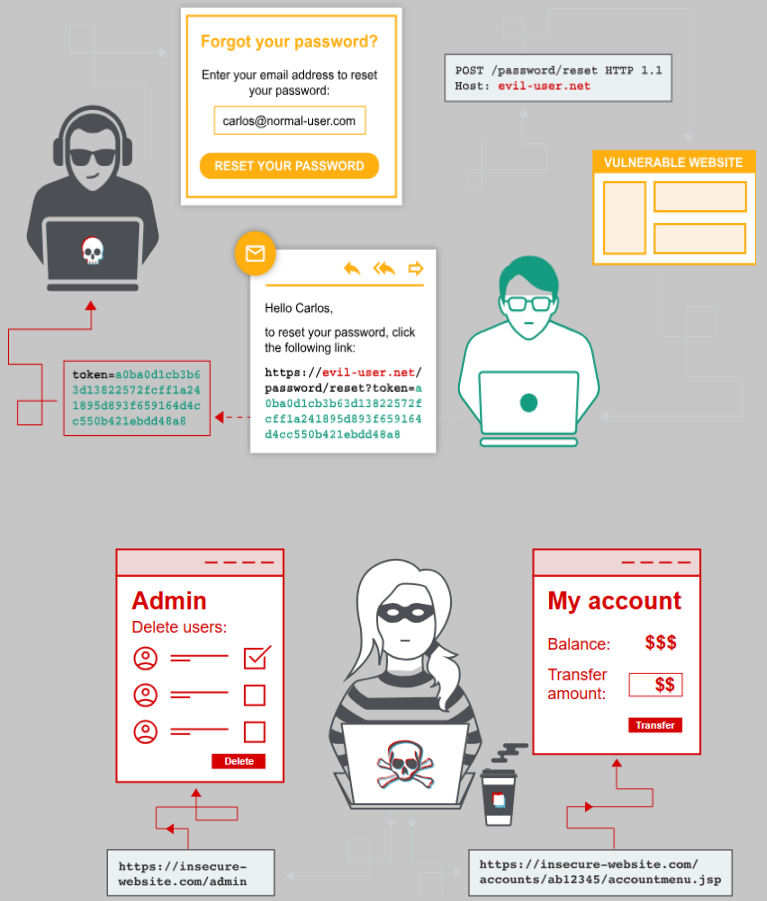
Hệ Điều Hành: Windows, Linux
Ngôn Ngữ: PHP, PYTHON, JAVA
Network: TCP/UDP, SSH, TELNET, ...
Công Cụ: nmap, gobuster, metasploit, docker, ...
Ảo Hóa: Virtualbox, Vmware, Vagrant

WEB SECURITY

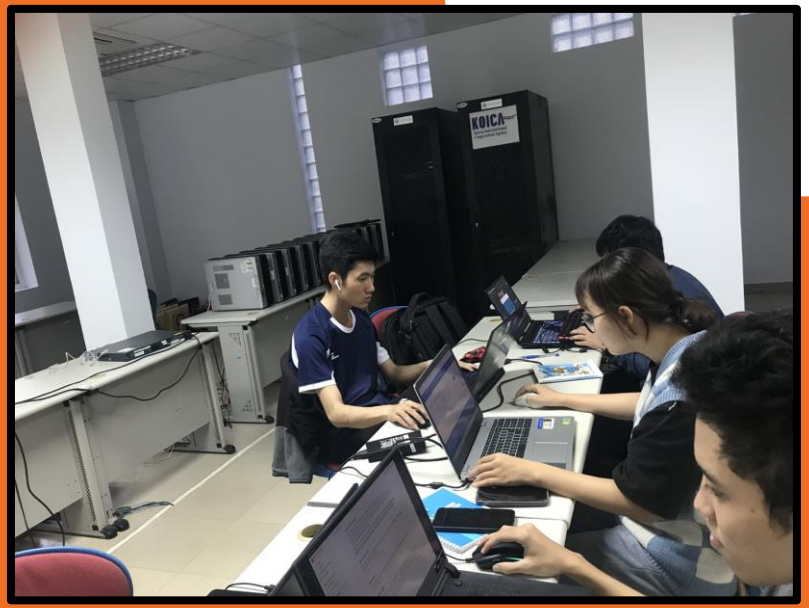
- Hoá thân thành hacker mũ đen và tìm cách đạp đổ công sức tội nghiệp của bọn dev.
- Hoặc hoá thân thành anh hề vui tính bị bọn dev bắt nạt.

Một số lỗ hổng thường gặp

- SQL,OS,Template INJECTION
- Path traversal, LFI, RFI
- XSS, Client side, SSRF
- Upload file, API testing
- Và nhiều thứ khác



QUÁ TRÌNH THAM GIA RED TEAM



Digital Forensics

1

CƠ HỘI NGHỀ NGHIỆP

Ngoài PENTEST ra thì đây là
lĩnh vực đang được tuyển dụng
rất nhiều

2

CÔNG VIỆC SẼ LÀM

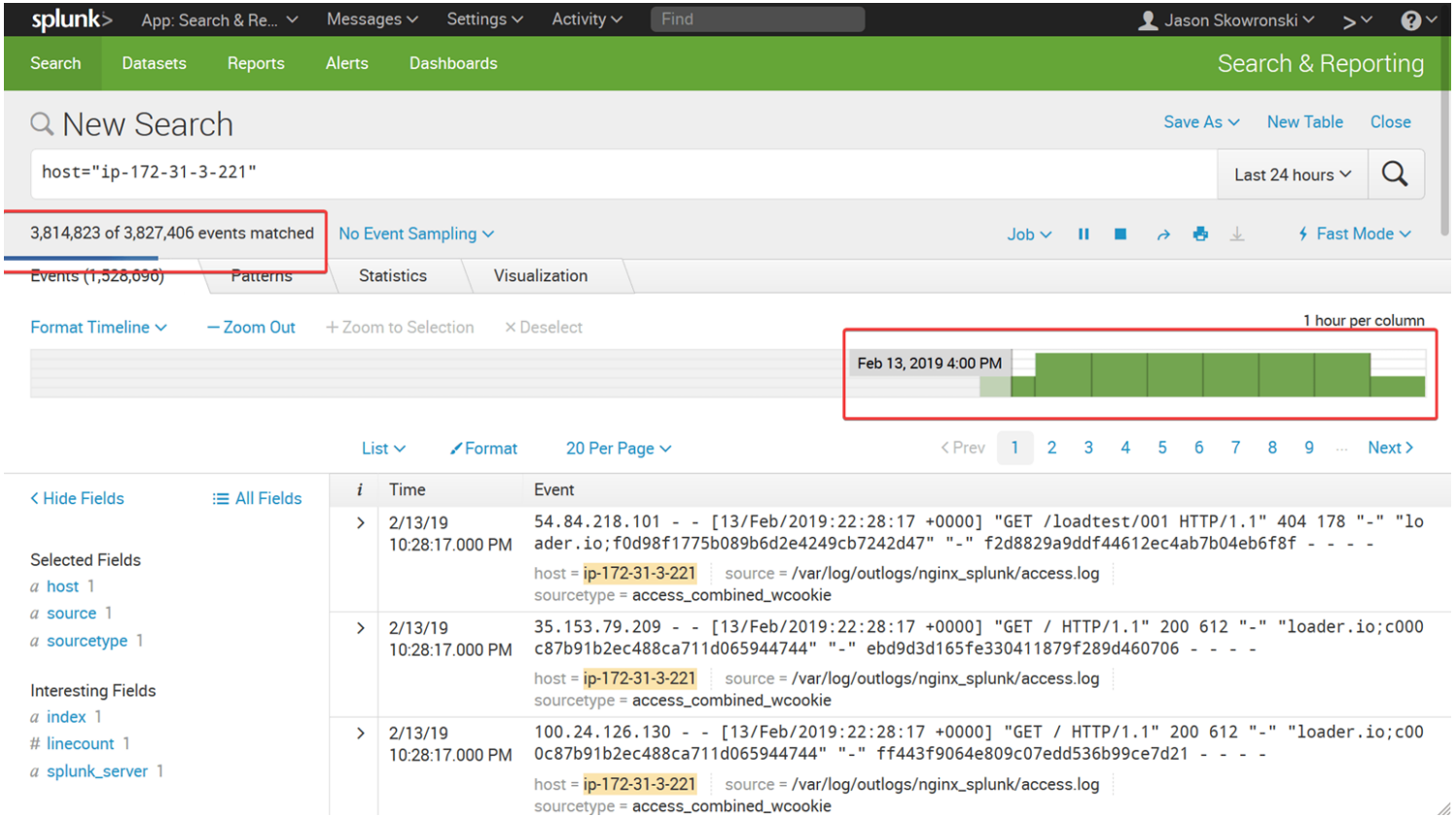
Nhìn màn hình cả ngày
Review Source Code
Ngăn chặn các cuộc tấn công
Là thành viên của **BLUE TEAM**

3

KIẾN THỨC DỰ KIẾN

Hệ Điều Hành: Windows, Linux
Ngôn Ngữ: PHP, PYTHON, JAVA
Network: TCP/UDP, SSH, TELNET, ...
Công Cụ: splunk, docker, ...
Ảo Hóa: Virtualbox, Vmware, Vagrant

Digital Forensics



Cryptography - Mật mã học

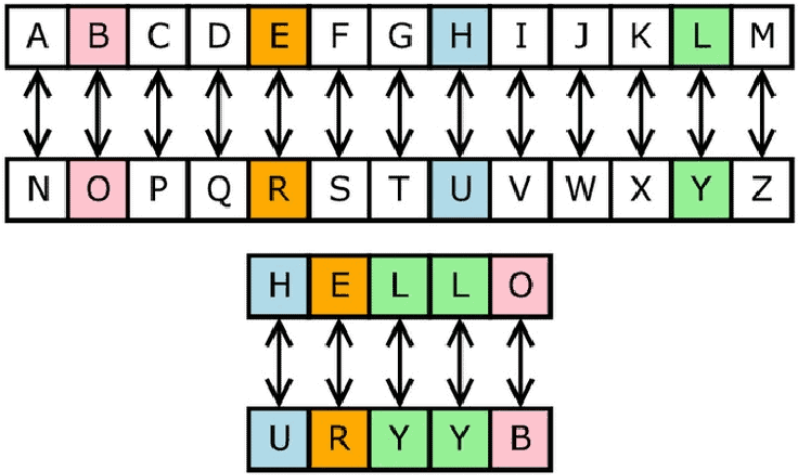
Vai trò và Nhiệm vụ

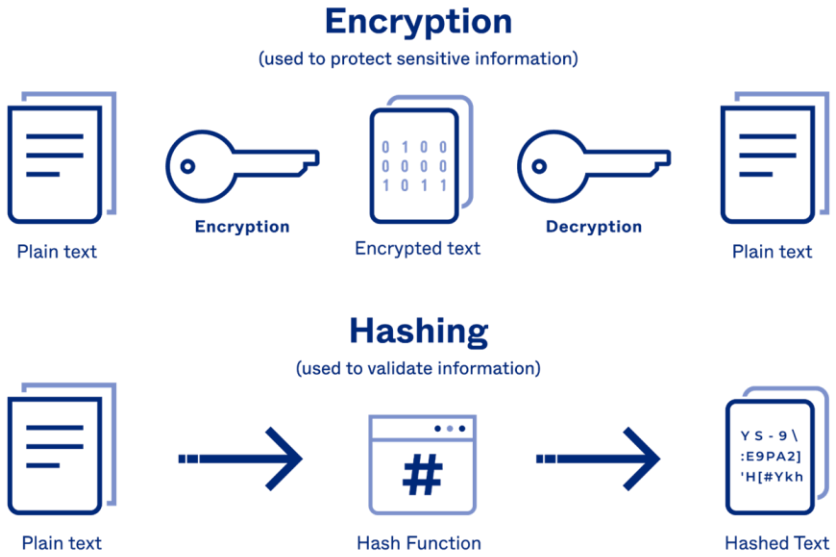
Định hướng phát triển

Cơ hội nghề nghiệp

Kiến thức cần học

Cryptography - Mật mã học





okta

Vai trò và Nhiệm vụ của Mật mã học

1. Nghiên cứu và phát triển các loại mã hóa.
2. Khai thác các loại mã hóa đang có để cải tiến.
3. Bảo mật thông tin của hệ thống và người dùng.
4. Hỗ trợ các mảng khác trong ngành bảo mật

Định hướng phát triển trong Mật mã học

Lập trình

Làm quen với việc lập trình các ngôn ngữ

Mật mã cơ bản

Học về các loại mật mã cổ điển, cơ bản

Mật mã nâng cao

Mã hóa hiện đại, nâng cao, toán học.

Kiến thức cần học

Lập trình

Học về một ngôn ngữ lập trình để có thể làm việc với cách tạo ra một loại mã hóa.

Toán học

Tìm hiểu về toán học: giải tích, toán rời rạc, đại số tuyến tính, ...

Mật mã học

Tìm hiểu các loại mã hóa cổ điển như: Caesar, ROT 13, ...
Các loại mã hóa hiện đại: AES, RSA, ...

Cơ hội nghề nghiệp

01 Chuyên gia An ninh mạng

02 Nhà nghiên cứu mật mã

03 Bug Hunter

Reverse Engineering - Kỹ thuật dịch ngược

Vai trò và nhiệm vụ

Định hướng phát triển

Cơ hội việc làm

Kiến thức cần học

Reverse Engineering - Kỹ thuật dịch ngược

RE là gì?

Là quá trình phân tích, dịch ngược lại một chương trình, đoạn mã để xem mã nguồn, cách thức hoạt động của nó.

Vai trò

Vai trò

Nhiệm vụ

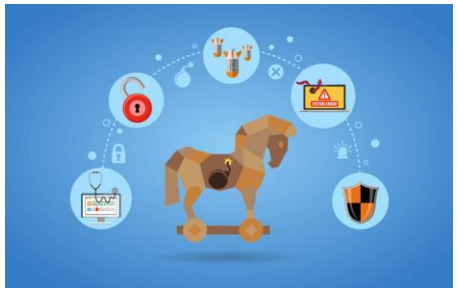
Nhiệm vụ

Vai trò và Nhiệm vụ của RE

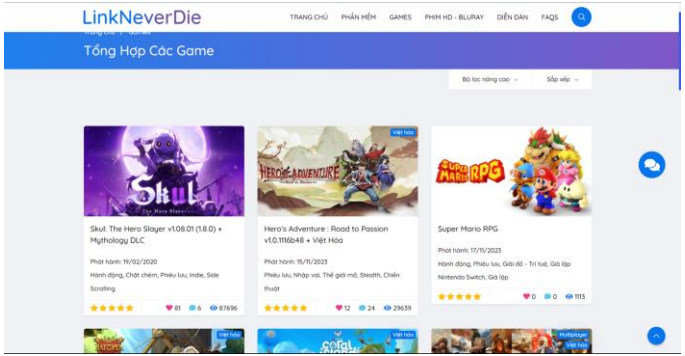
- Đảo ngược mã hóa
- Phân tích phần mềm độc hại
- Kiểm thử phần mềm

- Tối ưu hóa phần mềm
- Bảo mật phần mềm
- Phát triển mã độc

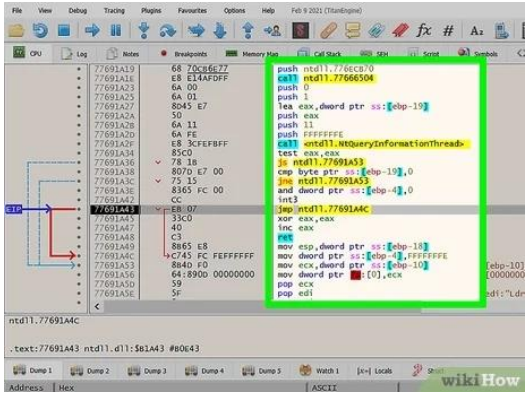
Ứng dụng của kỹ thuật RE



Phân tích mã độc



Bẻ khóa phần mềm trả phí



Xem mã nguồn

Định hướng phát triển của RE

Reverse Engineering

LẬP TRÌNH

Học các ngôn ngữ lập trình

KIẾN TRÚC MÁY TÍNH

Hiểu cách máy tính hoạt động

Kỹ thuật dịch ngược

Làm quen với các kỹ thuật dịch ngược phần mềm

Khai thác nhị phân - Binary Exploitation

Vai trò và Nhiệm vụ

Cơ hội việc làm

Định hướng phát triển

Kiến thức cần học

Vai trò và Nhiệm vụ của Binary Exploitation

- Phân tích bảo mật phần mềm
- Phân tích phần mềm độc hại
- Phân tích hệ điều hành

- Tìm kiếm các lỗ hổng 0-day
- Tham gia CTF
- Phát triển mã độc

Định hướng phát triển của PWN

vtv.vn/cong-nghe/nhom-chuyen-gia-vcs-vo-dich-cuoc-thi-tan-cong-mang-lon-nhat-the-gioi-20231101171219444.htm?fbclid=IwAR02mNeee

Nhóm chuyên gia VCS vô địch "Cuộc thi tấn công mạng" lớn nhất thế giới

PV - Thứ tư, ngày 01/11/2023 19:00 GMT+7

Thích Chia sẻ

Nghe đọc bài 5:10 | 1x | Nữ miền Bắc

VTV.vn - Tại Pwn2Own Toronto 2023, đội ngũ chuyên gia của Viettel Cyber Security lập kỷ lục mới với ngôi vô địch, đạt 30 điểm Master of Pwn và mang về giải thưởng 180.000 USD.

Kết thúc hạng mục thi cuối vào tối ngày 27/10, đội tuyển của Công ty An ninh mạng Viettel (Viettel Cyber Security - VCS) đã chính thức giành chiến thắng cao nhất với 30 điểm Master of Pwn. Kết quả này đã đưa VCS lên ngôi vị vô địch một cách thuyết phục tại cuộc thi bảo mật trước nhiều đội tuyển quốc tế, đồng thời đánh dấu sự bứt phá mới cho ngành An toàn thông tin Việt Nam khi lần đầu lên ngôi vô địch tại một giải đấu quốc tế danh giá.

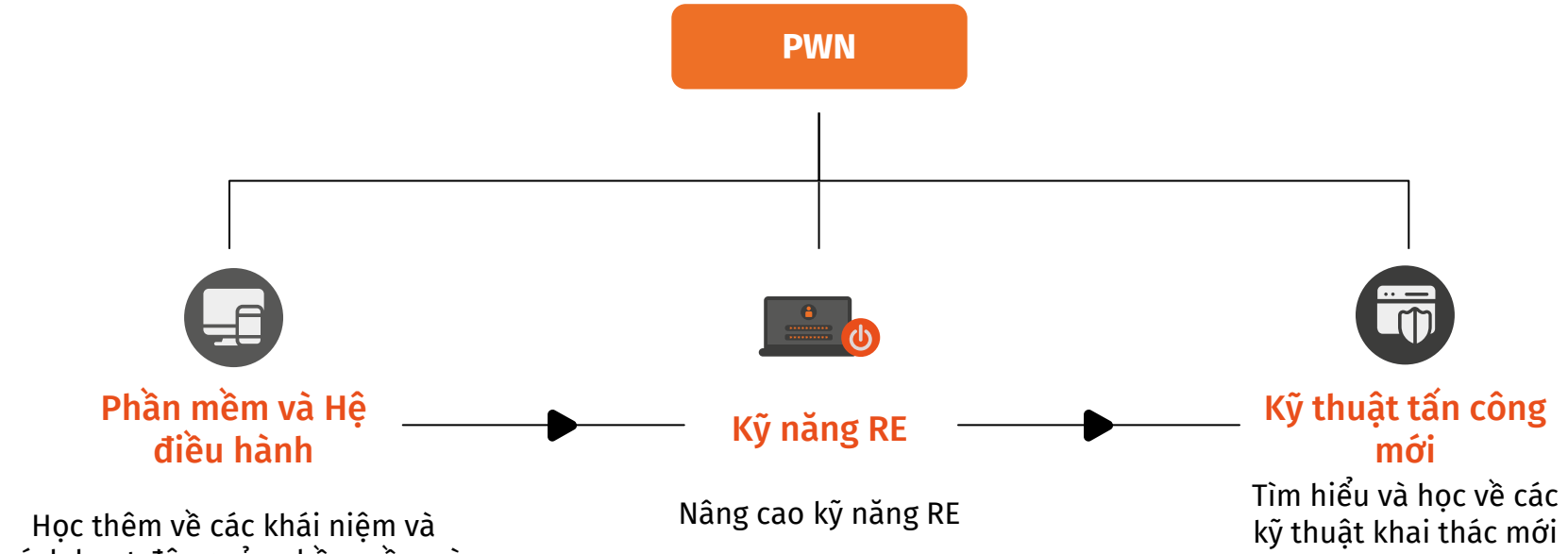
udio from this page

MASTER OF PWN

LEADERBOARD

		PRIZE $	POINTS
1	Team Viettel	$180,000	30
2	Team Orca (Sea Security)	$116,250	17.25
3	(Tie) DEVCORE Intern Interrupt Labs	$50,000	10
4	Chris Anastasio	$100,000	9
5	Pentest Ltd	$90,000	9

Định hướng phát triển của PWN



Kiến thức cần học trong RE và PWN

Lập trình

Ngôn ngữ lập trình như: C/C++, C#, Javascript, ...
Mã máy.

Kiến trúc máy tính

Hiểu cách máy tính, hệ điều hành, phần mềm hoạt động.

Kỹ thuật tấn công

Học về cách dùng các công cụ, các kỹ thuật tấn công.

Cơ hội nghề nghiệp

Chuyên gia phân tích bảo mật, an ninh ứng dụng

Dịch ngược và phân tích các chương trình giúp cải tiến chúng

Chuyên gia mã độc

Nghiên cứu và phân tích cách một mã độc hoạt động.

Freelance

Crack các chương trình trả phí để sử dụng. Bug bounty. Tham gia CTF