



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 việc bảo vệ dữ liệu khỏi các mối đe dọa như virus, malware, ransomware, v.v.
- Các biện pháp bảo mật bao gồm: tường lửa, phần mềm diệt virus, mã hóa dữ liệu và các chính sách bảo mật.

2. An toàn thông tin:

- Định nghĩa rộng hơn, bao gồm cả việc bảo vệ thông tin khỏi các mối đe dọa, rò rỉ, hoặc mất mát.
- An toàn thông tin bao gồm chính sách, quy trình và người dùng cuối để đảm bảo tính toàn vẹn và khả năng sẵn sàng của thông tin.

Cả hai lĩnh vực này đều rất quan trọng để bảo vệ các hệ thống thông tin của bạn khỏi các mối đe dọa. Nhưng bạn có thể làm gì để bảo vệ mình về một chủ đề cụ thể nào đó?



và phần cứng khỏi các mối đe dọa như virus, malware, ransomware, v.v.

diệt virus, tường lửa, mã hóa

h đến bảo vệ thông tin từ mọi

n bao gồm chính sách, quy trình và người dùng cuối để đảm bảo tính toàn vẹn và khả năng sẵn

nhân, dữ liệu doanh nghiệp và về một chủ đề cụ thể nào



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.

The screenshot displays the IonianCTF website interface. A modal window for the 'Mr-Robot101: Intro' challenge is open, showing a reward of 10 points and instructions to find an HTTP request on a server at 192.168.1.3. Below the modal, a scoreboard is visible, showing a line graph of scores over time and a table of team rankings.

Challenge Modal: Mr-Robot101: Intro
Reward Points: 10
This is for introduction. Right now a suspicious server is up and running.
The IP of the Server is 192.168.1.3 Try to get an HTTP Request from the server to see if the network port 80 is currently open.
Open Firefox and then hit as a URL 192.168.1.3
A webpage has opened! This means that the specific server has port 80 open and a web-server up and running.
Provide as a flag the 2nd command which the web-page provides as information.
Every flag has to submitted as: IonianCTF{theflag}

Scoreboard

filter_	rank_	team_name_	quiz_pts_	flag_pts_	base_pts_	total_pts_
1	1	XSLAY###	85	700	0	785
2	2	TONY_###	75	550	0	625
3	3	MAGDA###	65	580	0	645
4	4	KONGI###	55	550	0	605
5	5	PEPED###	55	500	0	555
6	6	INVISI###	55	500	0	555
7	7	NOK###	55	530	0	585
8	8	SALVA###	45	330	0	375
9	9	CASSI###	55	320	0	375

CTF - Capture The Flag

The screenshot shows the CTFTime website interface. At the top, there's a navigation bar with 'CTF TIME' logo and links for CTFs, Upcoming, Archive, Calendar, Teams, FAQ, Contact us, and About. A 'Sign in' button is on the right. The main content is divided into three sections: 'Team rating', 'Now running', and 'Upcoming events'.

Team rating

Place	Team	Country	Rating
1	Blue Water		1314.245
2	kalmancunnen		1122.218
3	C4T BuT S4D		1119.509
4	justCatTheFish		1103.182
5	r3kapig		891.056
6	Never Stop Exploiting		785.161
7	SKSD		764.609
8	organizers		740.629
9	WreckTheLine		712.763
10	thehackerscrew		710.663

Full rating | Rating formula

Upcoming events

Format	Name	Date	Duration
Open			

Now running

Die Abenteuer von KIM & TIM - Kapt. I - Mission (KIMpossible)
On-line
Fri, Nov 17, 2023 08:00 — Fri, Nov 17, 16:00 UTC (4h more)
33 teams

Past events

HITCON CTF 2023 Final
Nov 15, 2023 08:00 UTC | Taiwan, Taipei | Weight voting in progress

Place	Team	Country	Points *
1	M4M4		0.000
2	if this doesn't work we'll get more for next year		0.000
3	TakyoWestems		0.000

11 teams total | Tasks and writeups

Cybercoliseum II
Nov 13, 2023 07:00 UTC | On-line | Weight voting in progress

Place	Team	Country	Points *
1	Cyber Mushrooms		0.000
2	ne-pin-guam		0.000
3	MEHC		0.000

- 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...



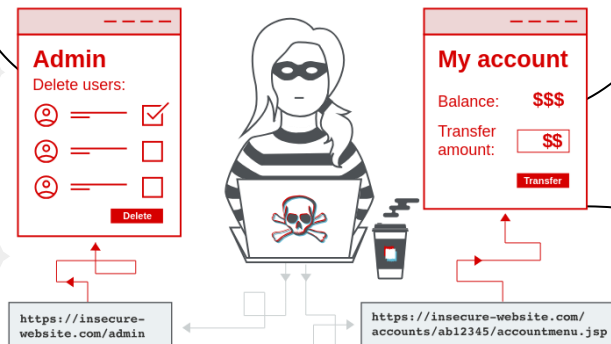
WEB SECURITY

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

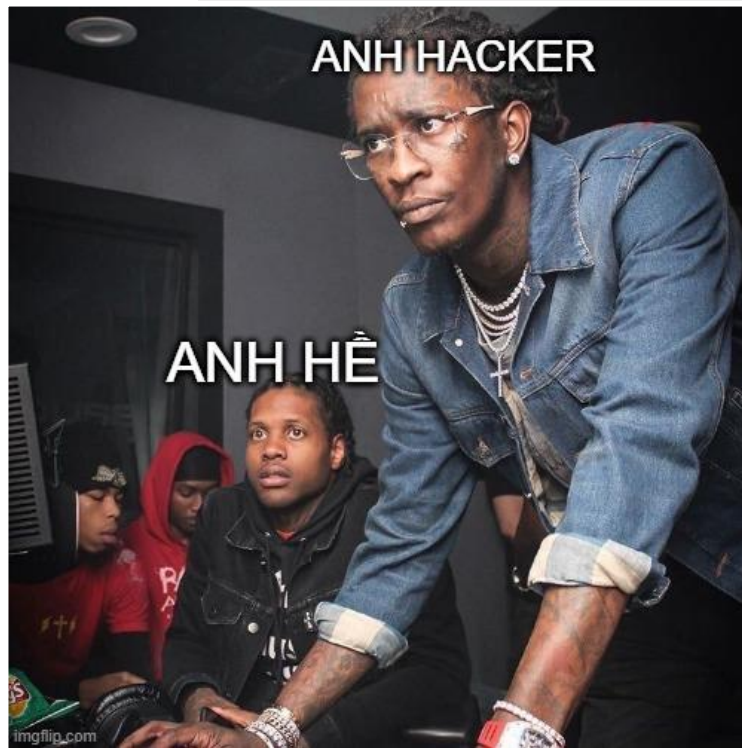
Review Source Code
Kiểm tra những lỗ hổng logic
Hóa thân thành hacker
Xâm nhập vào hệ thống

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

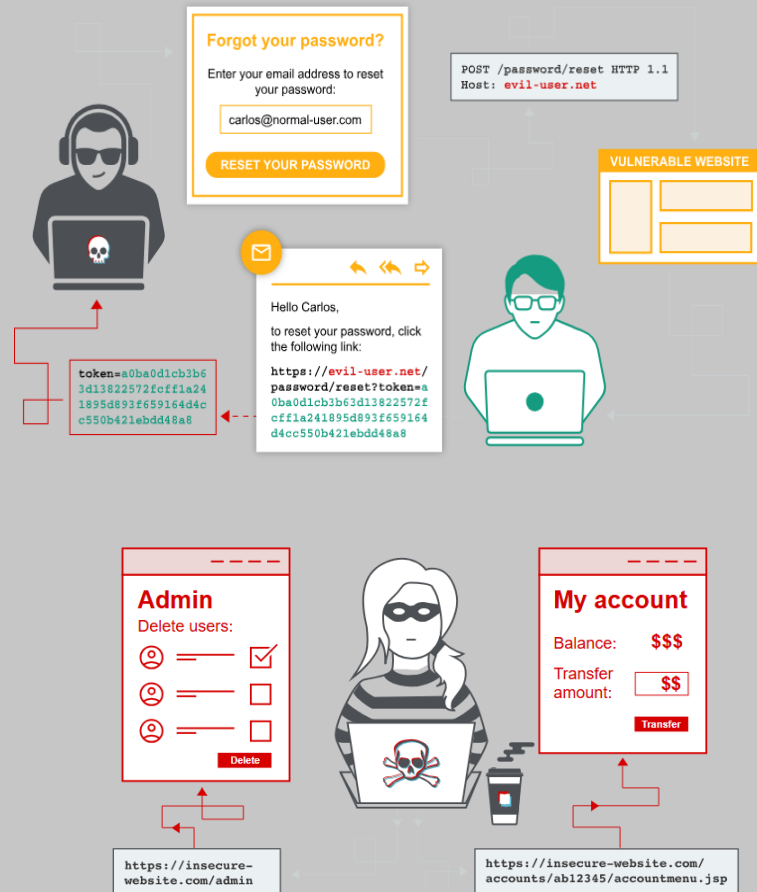
WEB SECURITY

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



Một số lỗi 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

splunk> App: Search & Re... Messages Settings Activity Find Jason Skowronski Search & Reporting

Search Datasets Reports Alerts Dashboards

New Search

Save As New Table Close

host="ip-172-31-3-221" Last 24 hours

3,814,823 of 3,827,406 events matched No Event Sampling

Job Fast Mode

Events (1,528,090) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 hour per column

Feb 13, 2019 4:00 PM

List Format 20 Per Page Prev 1 2 3 4 5 6 7 8 9 ... Next

< Hide Fields

All Fields

Selected Fields

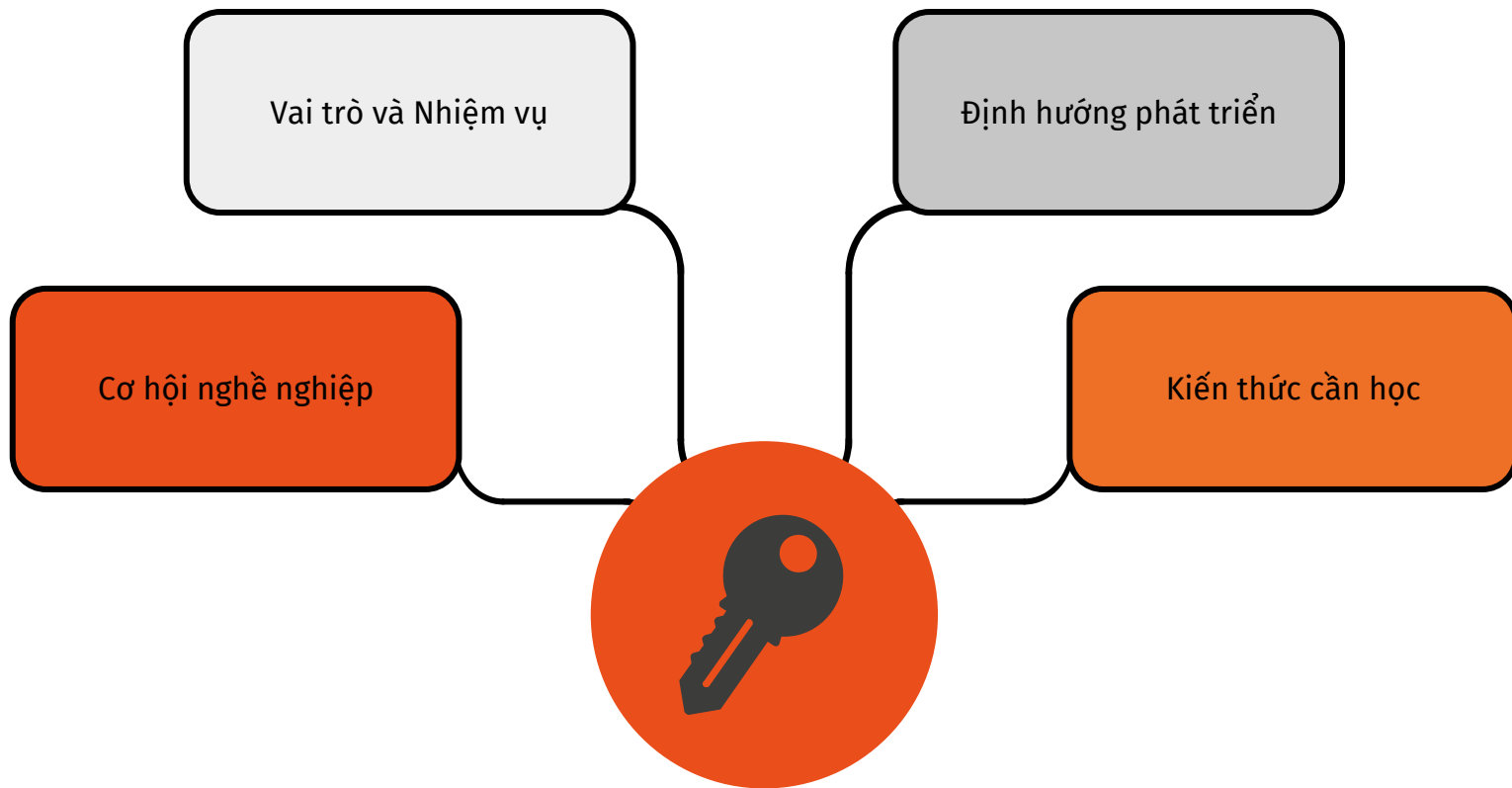
- host 1
- source 1
- sourcetype 1

Interesting Fields

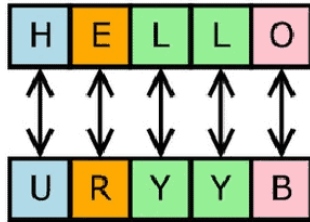
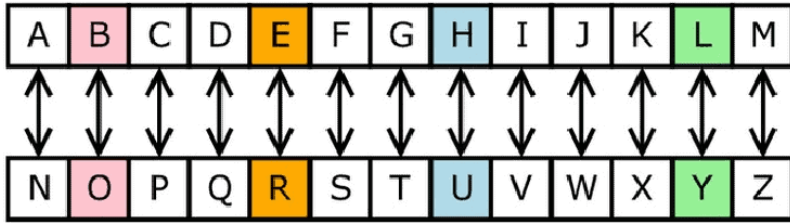
- index 1
- linecount 1
- splunk_server 1

i	Time	Event
>	2/13/19 10:28:17.000 PM	54.84.218.101 - - [13/Feb/2019:22:28:17 +0000] "GET /loadtest/001 HTTP/1.1" 404 178 "-" "loader.io;f0d98f1775b089b6d2e4249cb7242d47" "-" f2d8829a9ddf44612ec4ab7b04eb6f8f - - - host = ip-172-31-3-221 source = /var/log/outlogs/nginx_splunk/access.log sourcetype = access_combined_wcookie
>	2/13/19 10:28:17.000 PM	35.153.79.209 - - [13/Feb/2019:22:28:17 +0000] "GET / HTTP/1.1" 200 612 "-" "loader.io;c000c87b91b2ec488ca711d065944744" "-" ebd9d3d165fe330411879f289d460706 - - - host = ip-172-31-3-221 source = /var/log/outlogs/nginx_splunk/access.log sourcetype = access_combined_wcookie
>	2/13/19 10:28:17.000 PM	100.24.126.130 - - [13/Feb/2019:22:28:17 +0000] "GET / HTTP/1.1" 200 612 "-" "loader.io;c000c87b91b2ec488ca711d065944744" "-" ff443f9064e809c07edd536b99ce7d21 - - - host = ip-172-31-3-221 source = /var/log/outlogs/nginx_splunk/access.log sourcetype = access_combined_wcookie

Cryptography - Mật mã học



Cryptography - Mật mã học



Encryption

(used to protect sensitive information)



Hashing

(used to validate information)



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



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



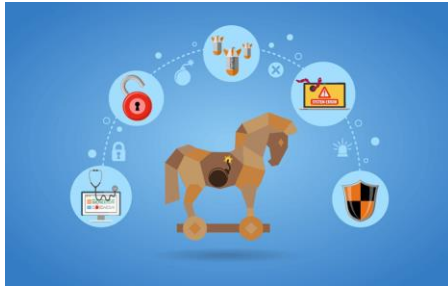
Bảo mật phần mềm



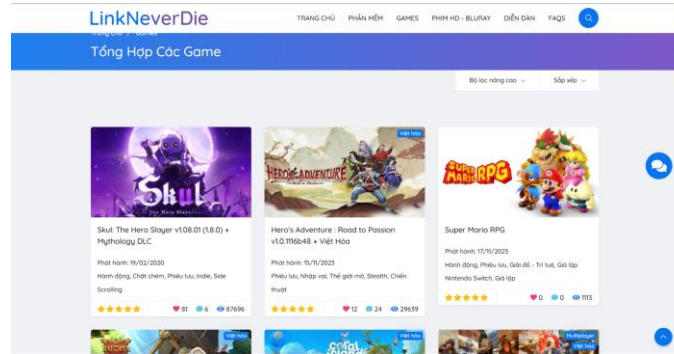
Phát triển mã độc



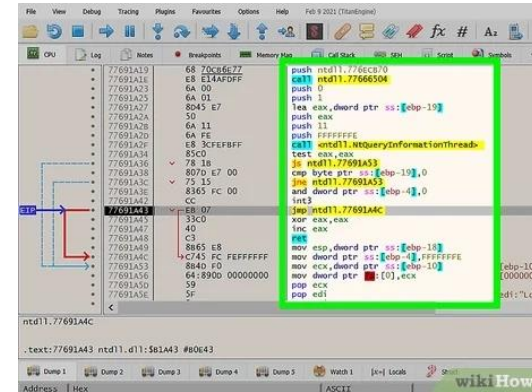
Ứng dụng của kỹ thuật RE



Phân tích mã độ

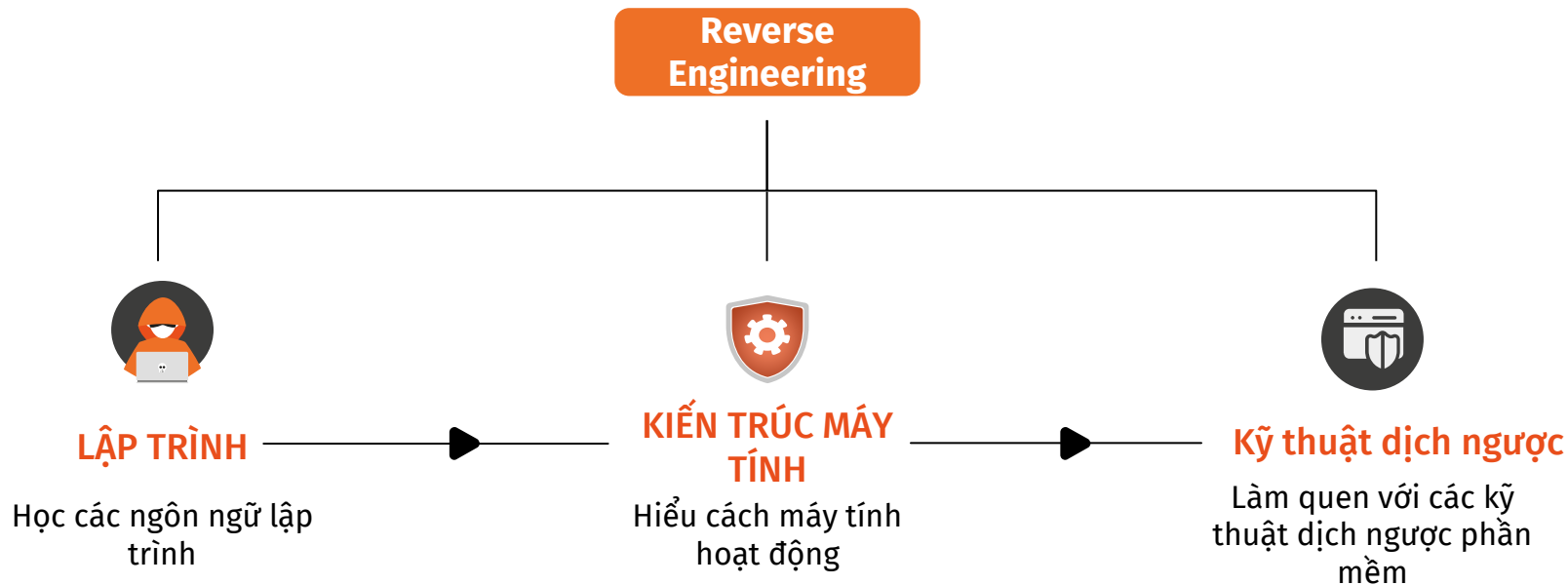


Bẻ khóa phần mềm trả phí



Xem mã nguồn

Định hướng phát triển của RE



Khai thác nhị phân - Binary Exploitation



Vai trò và Nhiệm vụ



Định hướng phát triển



Cơ hội việc làm



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

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 miễn Bắc

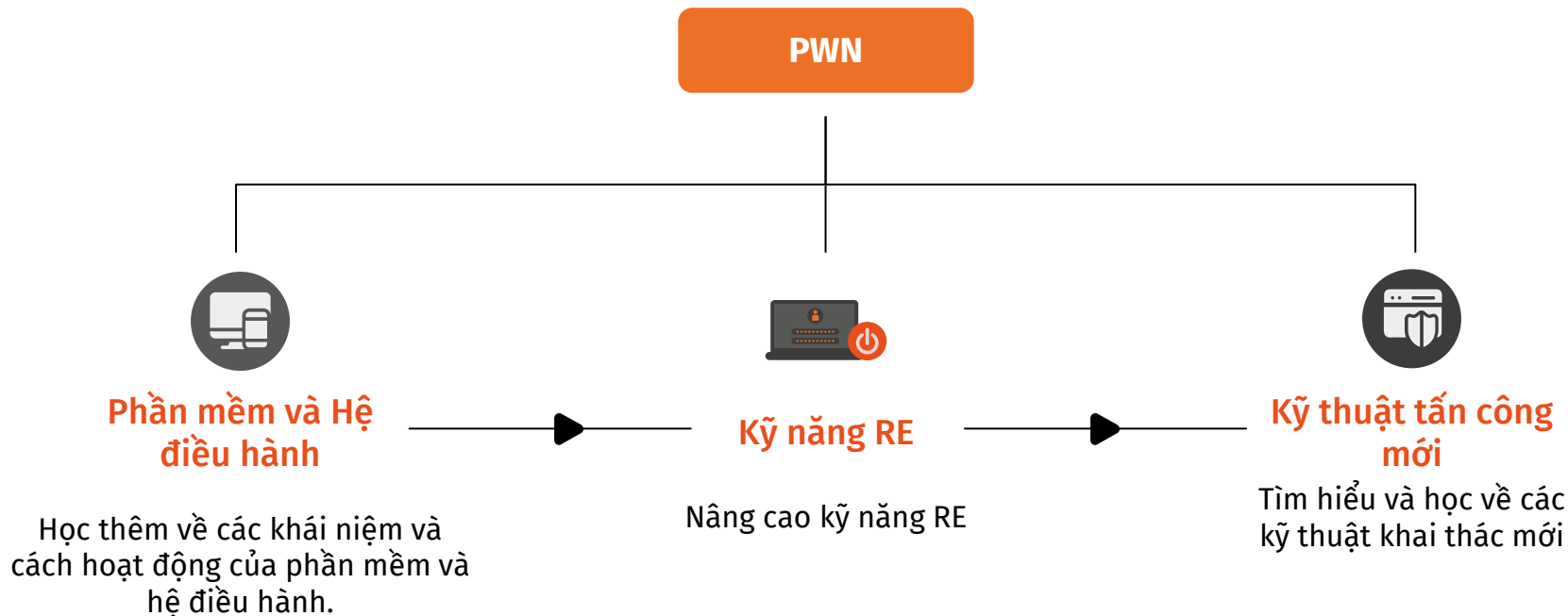
VTV.vn - Tại Pwn2Own Toronto 2023, đội ngũ chuyên gia của Viettel Cyber Security lập kỷ lục mới với ngôi vô địch, đạt 30 điểm Master of Pwn và mang về giải thưởng 180.000 USD.

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.



MASTER OF PWN		PRIZE \$	POINTS	LEADERBOARD
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

