Report_Week_03

Họ và tên: Trần Hân Nhi

MSSV: 2011770131 Lớp: 20DATA1

Ex_01:

- **Chính sách auditing:**

Audit Policy	Audit system events	No auditing
Audit Policy	Audit logon events	No auditing
Audit Policy	Audit object access	No auditing
Audit Policy	Audit privilege use	No auditing
Audit Policy	Audit process tracking	No auditing
Audit Policy	Audit policy change	No auditing
Audit Policy	Audit account management	No auditing
Audit Policy	Audit directory service access	No auditing
Audit Policy	Audit account logon events	No auditing

Tất cả các hạng mục trong chính sách kiểm tra (auditing policy) đều được đặt là "no auditing" (không kiểm tra), điều này có nghĩa là không có hoạt động nào sẽ được ghi lại (audit) hoặc theo dõi trong hệ thống tương ứng. Việc tắt tất cả các kiểm tra có thể có hậu quả là sẽ không có thông tin về các sự kiện bảo mật quan trọng xảy ra trên hệ thống, điều này có thể làm giảm khả năng phát hiện và ứng phó với các vấn đề bảo mật.

- **Kiểm tra User Rights**

584) User Rights Assignment

Policy	Security Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	S-1-5-32-551, Users, Administrators, Everyone
Act as part of the operating system	
Add workstations to domain	
Adjust memory quotas for a process	SQLAgent$SQLEXPRESS, S-1-5-80-3880718306-3832830129-1677859214-2598158968-1052248003, MSSQL$SQLEXPRESS, S-1-5-80-344959196-2060754871-2302487193-2804545603-1466107430, Administrators, NETWORK SERVICE, LOCAL SERVICE
Allow log on through Terminal Services	S-1-5-32-555, Administrators
Back up files and directories	S-1-5-32-551, Administrators
Bypass traverse checking	SQLAgent$SQLEXPRESS, S-1-5-80-3880718306-3832830129-1677859214-2598158968-1052248003, MSSQL$SQLEXPRESS, S-1-5-80-344959196-2060754871-2302487193-2804545603-1466107430, S-1-5-32-551, Users, Administrators, NETWORK SERVICE, LOCAL SERVICE, Everyone
Change the system time	Administrators, LOCAL SERVICE
Change the time zone	Users, Administrators, LOCAL SERVICE
Create a pagefile	Administrators
Create a token object	
Create global objects	SERVICE, Administrators, NETWORK SERVICE, LOCAL SERVICE
Create permanent shared objects	
Create symbolic links	Administrators
Debug programs	Administrators
Deny access to this computer from the network	Guest
Force shutdown from a remote system	Administrators
Generate security audits	NETWORK SERVICE, LOCAL SERVICE
Impersonate a client after authentication	SERVICE, Administrators, NETWORK SERVICE, LOCAL SERVICE
Increase a process working set	Users
Increase scheduling priority	Window Manager Group, Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	Performance Log Users, S-1-5-32-551, Administrators
Log on as a service	
Log on locally	S-1-5-32-551, Users, Administrators, Guest, __vmware__
Manage auditing and security log	Administrators
Manage the files on a volume	S-1-5-80-3880718306-3832830129-1677859214-2598158968-1052248003, MSSQL$SQLEXPRESS, Administrators
Modify an object label	
Modify firmware environment values	Administrators
Profile single process	Administrators
Profile system performance	WdiServiceHost, Administrators
Remove computer from docking station	Users, Administrators
Replace a process-level token	SQLAgent$SQLEXPRESS, S-1-5-80-3880718306-3832830129-1677859214-2598158968-1052248003, MSSQL$SQLEXPRESS, S-1-5-80-344959196-2060754871-2302487193-2804545603-1466107430, NETWORK SERVICE, LOCAL SERVICE
Restore files and directories	S-1-5-32-551, Administrators
Shut down the system	S-1-5-32-551, Users, Administrators
Synchronize directory service data	
Take ownership of files or other objects	Administrators

Cấu hình riêng biệt cho người dùng giao tiếp với hệ thống như: quyền đăng nhập, quyền truy cập từ xa, quyền uỷ thác, quyền quản lý... Một số mục được quét trên máy như:

- Đối với Administrator:

  Cho phép tài khoản được ủy quyền truy cập Credential Manager (quản lý thông tin đăng nhập và chứng chỉ).

  Liệt kê các tài khoản hoặc nhóm người dùng được phép đăng nhập qua dịch vụ Terminal Services.

  Quyền sao lưu tệp tin và thư mục.

  Thay đổi thời gian, múi giờ của hệ thống

  Tạo các đối tượng toàn cục, thường liên quan đến quyền tạo dịch vụ.

  Quyền gỡ lỗi các chương trình khác.

  Chấp nhận quyền sở hữu của tệp tin hoặc đối tượng khác

  …

- Đối với Users

  Cho phép tài khoản được ủy quyền truy cập Credential Manager (quản lý thông tin đăng nhập và chứng chỉ).

  Quyền đăng nhập trực tiếp vào máy tính

  Quyền tăng kích thước bộ nhớ làm việc của một quy trình.

  …

- Ngoài ra còn có Guest- Tài khoản người dùng có quyền hạn hạn chế nhất trong hệ thống, được sử dụng cho người dùng tạm thời hoặc khách hàng không đăng nhập; LOCAL SERVICE - Tài khoản dịch vụ được sử dụng để chạy dịch vụ hệ thống, nhưng thường có quyền hạn hạn chế hơn so với NETWORK SERVICE, được thiết lập để chạy dịch vụ với các quyền cục bộ; NETWORK SERVICE - tài khoản dịch vụ (service account) được sử dụng trong môi trường Windows để chạy các dịch vụ hệ thống; Everyone - Tất cả tài khoản và người dùng trên hệ thống hoặc tài khoản được áp dụng cho tất cả mọi người, bao gồm cả không đăng nhập, sẽ có quyền truy cập; WdiServiceHost - Tài khoản hoặc dịch vụ này có thể được sử dụng để thực hiện các tác vụ liên

quan đến kiểm tra và chẩn đoán trên hệ thống. Quyền và quyền hạn của nó thường được cấu hình để đảm bảo tính an toàn và hiệu suất của hệ thống; …

- **Kiểm tra Windows Firewall**

585) Windows Firewall

Name	Setting
Firewall Enabled	No
Authorised Application	OpenJDK Platform binary
Authorised Application	Blood Field
Authorised Application	Riot Client
Authorised Application	Java(TM) Platform SE binary
Authorised Application	Steam Web Helper
Authorised Application	Steam
Authorised Service	File and Printer Sharing
Authorised Service	Network Discovery
Authorised Service	Remote Desktop
Authorised Port	TCP:26822:*
Authorised Port	TCP:32683:*

Danh sách này bao gồm thông tin về tường lửa (firewall) trên hệ thống và các ứng dụng, dịch vụ và cổng mạng được phép hoạt động thông qua tường lửa.

- Firewall Enabled (Tường lửa được bật): Trạng thái của tường lửa trên hệ thống. "No" cho biết tường lửa không được kích hoạt. Điều này có thể cho phép các kết nối đến và đi từ hệ thống mà không bị chặn bởi tường lửa.
- Authorised Application (Ứng dụng được ủy quyền): Liệt kê các ứng dụng được phép thông qua tường lửa. Các ứng dụng này được cho phép gửi hoặc nhận dữ liệu qua tường lửa mà không bị chặn.

  OpenJDK Platform binary

  Blood Field

  Riot Client

  Java(TM) Platform SE binary

  Steam Web Helper

  Steam
- Authorised Service (Dịch vụ được ủy quyền): Liệt kê các dịch vụ được phép hoạt động thông qua tường lửa. Điều này có thể bao gồm các dịch vụ hệ thống như "File and Printer Sharing," "Network Discovery," và "Remote Desktop."
- Authorised Port (Cổng được ủy quyền): Liệt kê các cổng mạng được phép mở và sử dụng để giao tiếp qua tường lửa. Cổng TCP là giao thức truyền tải thông

tin qua mạng và các số cổng cụ thể được chỉ định cho các dịch vụ hoặc ứng dụng cụ thể.

TCP:26822:*: Cho phép tất cả kết nối TCP đến cổng 26822.

TCP:32683:*: Cho phép tất cả kết nối TCP đến cổng 32683.

- **Kiểm tra chính sách mật khẩu**

Password Policy	Enforce password history	0 remembered
Password Policy	Maximum password age	42
Password Policy	Minimum password age	0
Password Policy	Minimum password length	0 Characters
Password Policy	Password must meet complexity requirements	
Password Policy	Store password using reversible encryption for all users in the domain	

Cấu hình chính sách mật khẩu là một phần quan trọng của bảo mật hệ thống, nó đảm bảo rằng mật khẩu được sử dụng trong môi trường máy tính tuân thủ các yêu cầu bảo mật cụ thể. Cấu hình cụ thể có thể khác nhau tùy theo yêu cầu bảo mật và môi trường hệ thống cụ thể.

- Enforce password history (Áp dụng lịch sử mật khẩu): Thông số này xác định số lượng mật khẩu trước đây mà người dùng phải thay đổi trước khi họ được phép sử dụng mật khẩu mới. "0 remembered" có nghĩa là người dùng không cần phải thay đổi mật khẩu của họ theo lịch sử mật khẩu trước đó.
- Maximum password age (Số ngày tối đa của mật khẩu): Thông số này xác định khoảng thời gian tối đa mà một mật khẩu có thể tồn tại trước khi người dùng bắt buộc phải thay đổi nó. "42" có thể đại diện cho số ngày, tức là mật khẩu sẽ hết hạn sau 42 ngày.
- Minimum password age (Số ngày tối thiểu của mật khẩu): Thông số này xác định khoảng thời gian tối thiểu mà người dùng phải sử dụng một mật khẩu trước khi có thể thay đổi nó. "0" có thể đại diện cho không có khoảng thời gian tối thiểu.
- Minimum password length (Độ dài tối thiểu của mật khẩu): Xác định số ký tự tối thiểu mà mật khẩu phải có. "0 Characters" có nghĩa là không có yêu cầu về độ dài tối thiểu.

- **Kiểm tra chính sách lock out tài khoản**

Account Lockout Policy	Account lockout duration	10 Minutes
Account Lockout Policy	Account lockout threshold	10 Attempts
Account Lockout Policy	Reset account lockout counter after	10 Minutes

Cấu hình chính sách khoá tài khoản là một phần quan trọng của bảo mật hệ thống, và nó đảm bảo rằng tài khoản không thể bị tấn công bằng cách thử đăng nhập sai mật khẩu quá nhiều lần. Cấu hình cụ thể có thể thay đổi tùy theo yêu cầu bảo mật và môi trường hệ thống cụ thể.

- Account lockout duration (Thời gian khoá tài khoản): Đây là thời gian tài khoản sẽ bị khoá sau khi đạt đến ngưỡng khoá tài khoản (account lockout threshold). "10 Minutes" có nghĩa là sau khi tài khoản bị khoá, nó sẽ tự động mở lại sau 10 phút.
- Account lockout threshold (Ngưỡng khoá tài khoản): Đây là số lần thử đăng nhập không thành công mà một tài khoản có thể thực hiện trước khi bị khoá. "10 Attempts" có nghĩa là sau khi một tài khoản thử đăng nhập sai mật khẩu 10 lần, tài khoản sẽ bị khoá.
- Reset account lockout counter after (Thời gian đặt lại bộ đếm khoá tài khoản): Thời gian mà hệ thống sẽ đặt lại bộ đếm khoá tài khoản sau khi tài khoản đã bị khoá. "10 Minutes" có nghĩa là sau 10 phút, bộ đếm sẽ được đặt lại và tài khoản có thể thử đăng nhập lại.

- **Kiểm tra Window Update**

Automatic Updates	Update status	Scheduled installation
Automatic Updates	Update schedule	

Cập nhật tự động là một phần quan trọng của bảo mật hệ thống, và chúng đảm bảo rằng các bản vá bảo mật và cập nhật hệ thống được cài đặt để bảo vệ hệ thống khỏi các lỗ hổng bảo mật đã biết. Lập lịch cập nhật cụ thể và kiểm tra trạng thái cập nhật thường xuyên là quan trọng để đảm bảo tính bảo mật và ổn định của hệ thống.

- Update status (Trạng thái cập nhật): Mục này cho biết trạng thái hiện tại của cập nhật tự động. Trạng thái "Scheduled installation" có nghĩa là cập nhật sẽ được lên lịch cài đặt vào một thời điểm cụ thể trong tương lai.
- Update schedule (Lịch trình cập nhật): Đây là nơi có thể cấu hình lịch trình cụ thể cho cập nhật tự động. Nếu không có thông tin chi tiết về lịch trình cập

nhật, có thể muốn kiểm tra và cấu hình nó để đảm bảo rằng các cập nhật hệ thống được quản lý và triển khai một cách hiệu quả.

- **Kiểm tra phần mềm trên máy chủ có phù hợp với chính sách**

4) Installed Programs

5) .NET Android Templates (x64)

Item	Value
Name	.NET Android Templates (x64)
Vendor	Microsoft Corporation
Version	33.0.46.0
Product Language	English
Install Date	20230721
Install Location	
Install Source	C:\ProgramData\Microsoft\VisualStudio\Packages\Microsoft.Android.Templates.33.0.46,version=33.0.46.0,machinearch=x64\
Install State	The product is installed for the current user.
Assignment Type	Per Machine
Package Code	{35EA70D1-3153-4B87-AFD3-912F7129D412}
Package Name	Microsoft.Android.Templates.33.0.46-x64.msi
Local Package	C:\Windows\Installer\202f07b.msi
Product ID	
Registered Company	
Registered Owner	
Times Used	
Last Used	
Executable Path	
Executable Version	
Executable Description	
Software ID	{18E457C6-28EE-43FF-BA34-F0C5AE8AB4E8}

Thông tin về ứng dụng .NET Android Templates (x64) được cung cấp trong danh sách:

- Name (Tên): .NET Android Templates (x64)
- Vendor (Nhà cung cấp): Microsoft Corporation. Đây là một sản phẩm của Microsoft.
- Version (Phiên bản): 33.0.46.0. Đây là phiên bản cụ thể của ứng dụng .NET Android Templates.
- Product Language (Ngôn ngữ của sản phẩm): English (Tiếng Anh).
- Install Date (Ngày cài đặt): 20230721, ngày 21 tháng 7 năm 2023.
- Install Location (Vị trí cài đặt): Thông tin về vị trí cài đặt của ứng dụng không được cung cấp trong danh sách.
- Install Source (Nguồn cài đặt): C:\ProgramData\Microsoft\VisualStudio\Packages\Microsoft.Android.Templates.33.0.46,version=33.0.46.0,machinearch=x64.
- Install State (Trạng thái cài đặt): "The product is installed for the current user" (Sản phẩm đã được cài đặt cho người dùng hiện tại), tức là ứng dụng .NET Android Templates (x64) được cài đặt cho người dùng hiện tại.

- Assignment Type (Loại phân công): "Per Machine" (Cho máy tính), cho biết rằng ứng dụng được cài đặt cho toàn bộ máy tính chứ không chỉ cho một người dùng cụ thể.
- Package Code (Mã gói): 35EA70D1-3153-4B87-AFD3-912F7129D412
- Package Name (Tên gói): Microsoft.Android.Templates.33.0.46-x64.msi.
- Local Package (Gói cục bộ): C:\Windows\Installer\202f07b.msi
- Software ID (ID Phần mềm): ID này là một định danh duy nhất cho ứng dụng .NET Android Templates (x64) trên hệ thống và được sử dụng để theo dõi và quản lý ứng dụng trong hệ thống. ID này là 18E457C6-28EE-43FF-BA34-F0C5AE8AB4E8.

16) Cloudflare WARP

Item	Value
Name	Cloudflare WARP
Vendor	Cloudflare, Inc.
Version	23.7.160.0
Product Language	English
Install Date	20230722
Install Location	
Install Source	C:\Users\NHI\Downloads\
Install State	The product is installed for the current user.
Assignment Type	Per Machine
Package Code	{2BE9BD4E-2C3C-483C-BED6-EFA6AB8733CA}
Package Name	Cloudflare_WARP_Release-x64.msi
Local Package	C:\Windows\Installer\22b5922.msi
Product ID	
Registered Company	
Registered Owner	
Times Used	
Last Used	
Executable Path	
Executable Version	
Executable Description	
Software ID	{30C49141-5DD4-439E-BFC3-0A24DCC930B4}

Thông tin về ứng dụng Cloudflare WARP được cung cấp trong danh sách:

- Name (Tên): Cloudflare WARP
- Vendor (Nhà cung cấp): Cloudflare, Inc. Đây là công ty phát triển và cung cấp ứng dụng Cloudflare WARP.
- Version (Phiên bản): 23.7.160.0. Đây là phiên bản cụ thể của ứng dụng Cloudflare WARP.
- Product Language (Ngôn ngữ của sản phẩm): English (Tiếng Anh).
- Install Date (Ngày cài đặt): 20230722, ngày 22 tháng 7 năm 2023.
- Install Source (Nguồn cài đặt): C:\Users\NHI\Downloads
- Install State (Trạng thái cài đặt): "The product is installed for the current user" (Sản phẩm đã được cài đặt cho người dùng hiện tại), tức là ứng dụng Cloudflare WARP được cài đặt cho người dùng hiện tại.

- Assignment Type (Loại phân công): Per Machine (Cho máy tính), cho biết rằng ứng dụng được cài đặt cho toàn bộ máy tính chứ không chỉ cho một người dùng cụ thể.
- Package Code (Mã gói): 2BE9BD4E-2C3C-483C-BED6-EFA6AB8733CA
- Package Name (Tên gói): Cloudflare_WARP_Release-x64.msi.
- Local Package (Gói cục bộ): C:\Windows\Installer\22b5922.msi.
- Software ID (ID Phần mềm): 30C49141-5DD4-439E-BFC3-0A24DCC930B4

531) Zalo 23.08.04

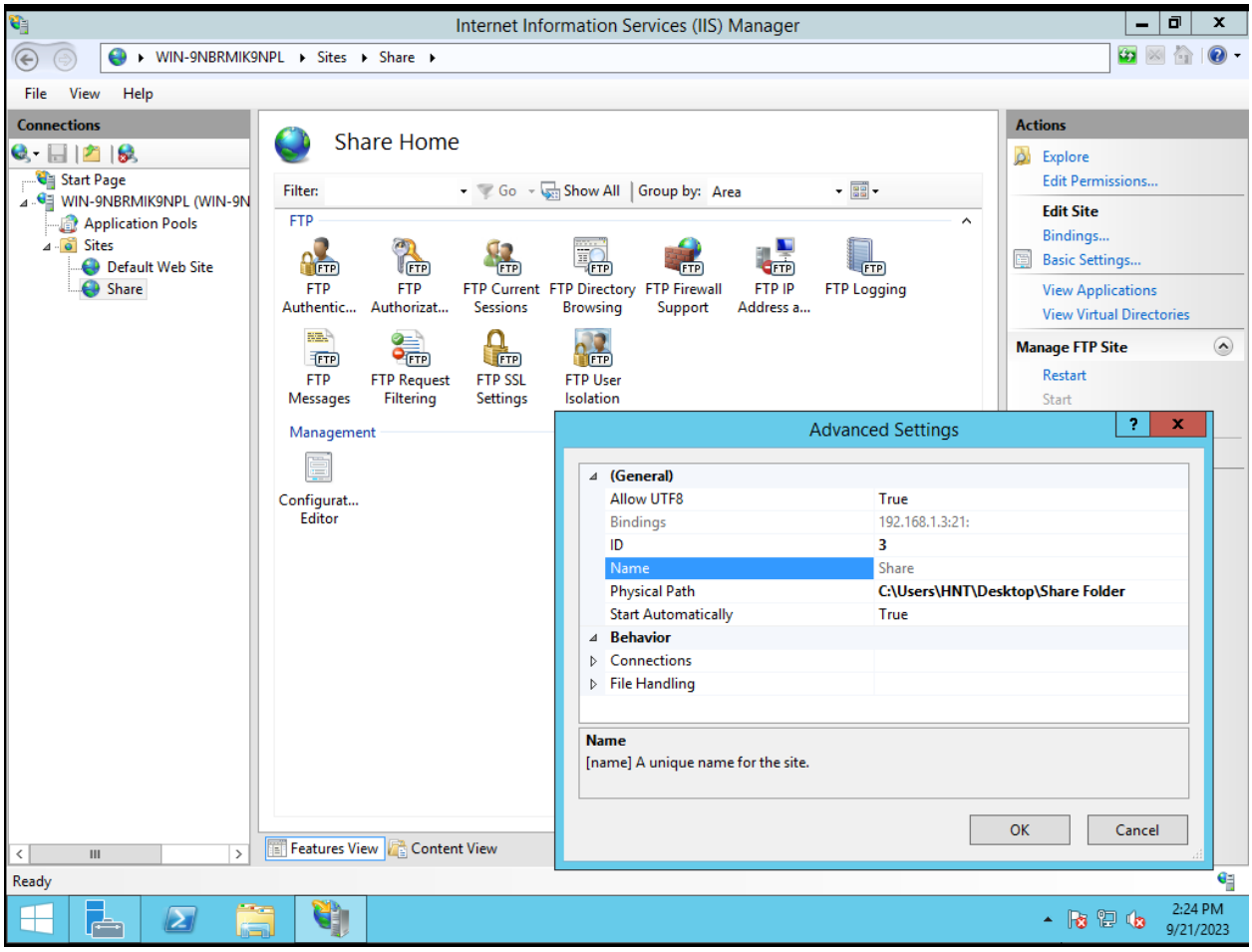
Item	Value
Name	Zalo 23.08.04
Vendor	VNG Corp.
Version	23.08.04
Product Language	
Install Date	20230821
Install Location	
Install Source	
Install State	
Assignment Type	
Package Code	
Package Name	
Local Package	
Product ID	
Registered Company	
Registered Owner	
Times Used	
Last Used	
Executable Path	
Executable Version	
Executable Description	
Software ID	f0c47de4-c117-54e4-97d9-eb3fd2985e6c

Thông tin này cung cấp các chi tiết về phiên bản và thông tin liên quan đến việc cài đặt ứng dụng Zalo trên hệ thống.

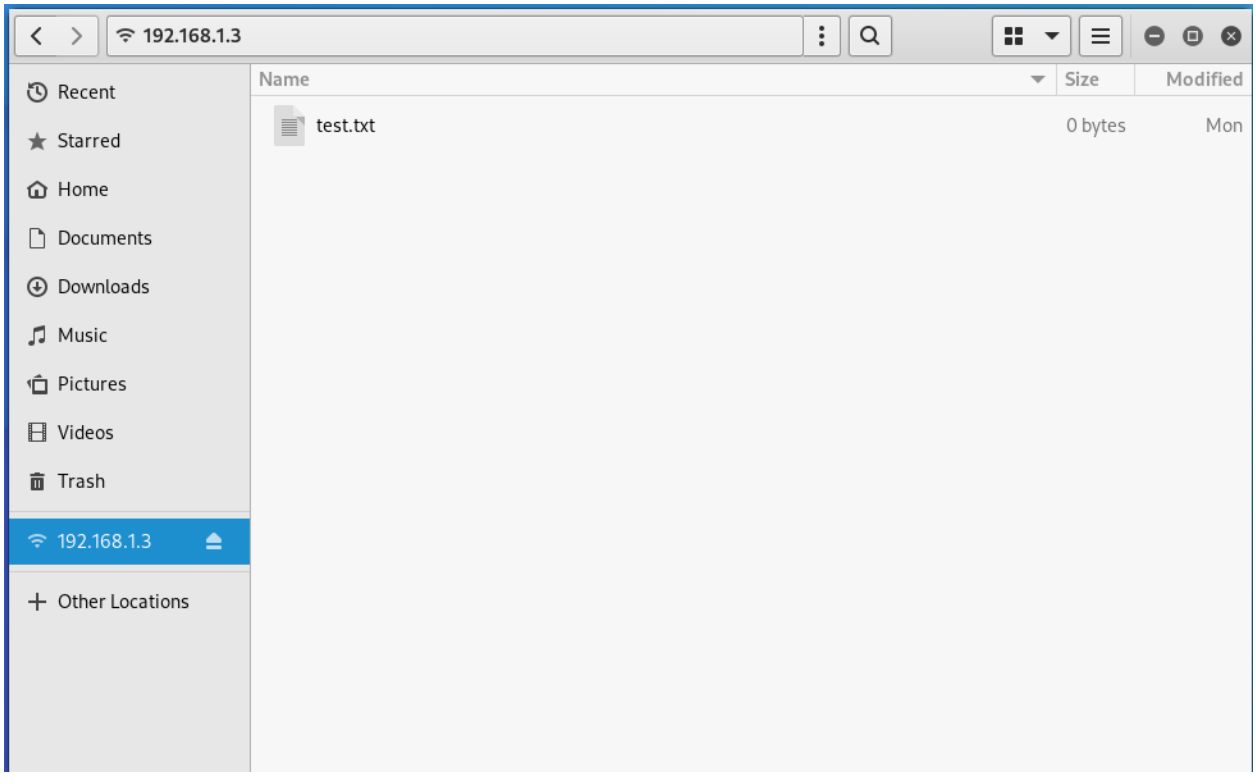
- Name (Tên): Zalo 23.08.04.
- Vendor (Nhà cung cấp): VNG Corp. Đây là công ty phát triển và cung cấp ứng dụng Zalo.
- Version (Phiên bản): 23.08.04. Đây là phiên bản cụ thể của ứng dụng Zalo.
- Install Date (Ngày cài đặt): 20230821, ngày 21 tháng 8 năm 2023.
- Software ID (ID Phần mềm): f0c47de4-c117-54e4-97d9-eb3fd2985e6c

Ex_02:

- Server 2012 đã cài đặt IIS Server, FTP Server. Chọn file Share Folder



- Kali dung để truy cập file share



Ex_03

- **hping3 –A 192.168.1.3**

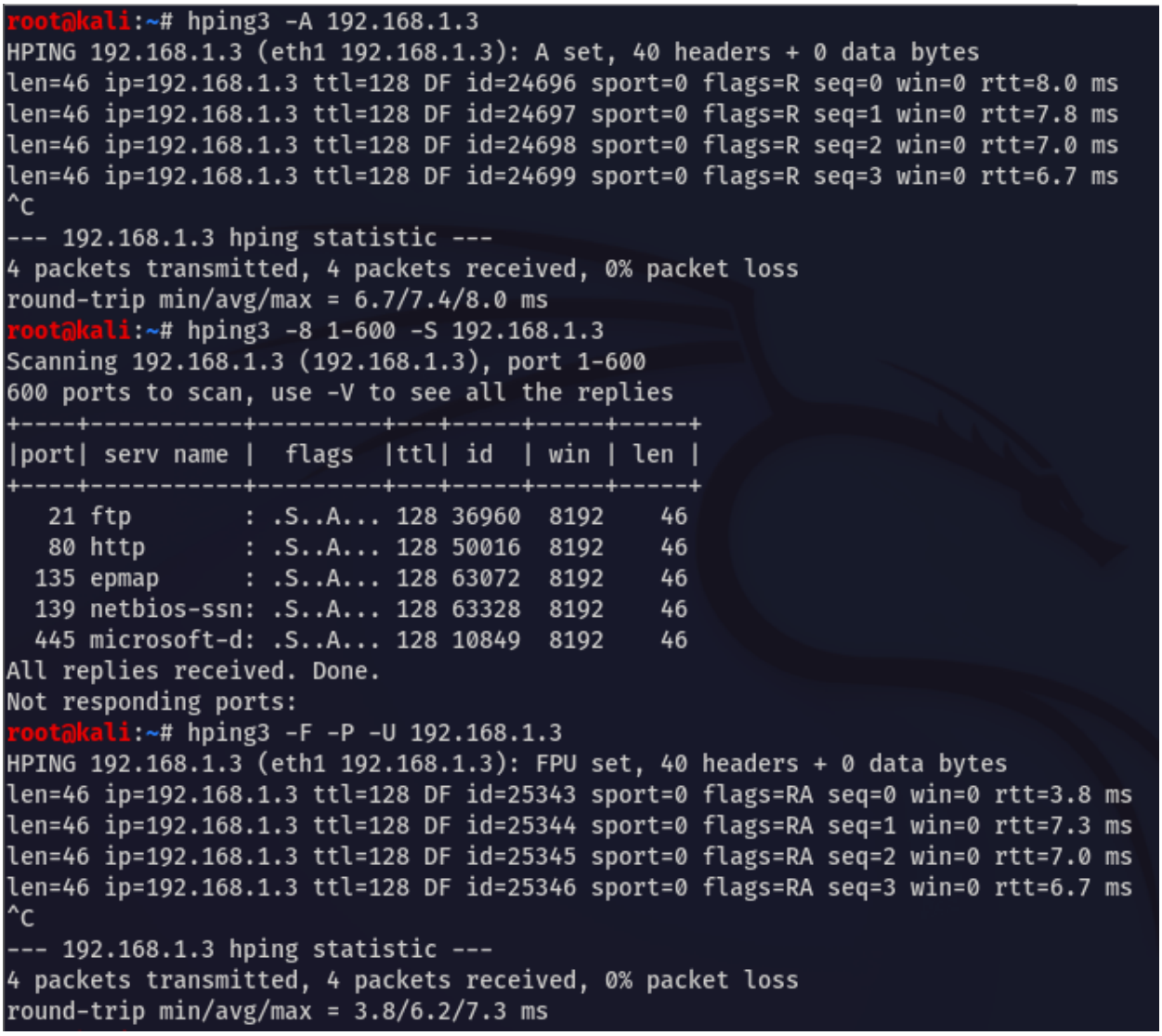
Thử nghiệm kết nối TCP đến máy tính có địa chỉ IP là 192.168.1.3 bằng cách gửi các gói tin ACK đến máy chủ đó và xem phản hồi từ máy chủ

- **hping3 -8 1-600 –S 192.168.1.3**

Lệnh gửi các gói tin ping hoặc gói tin SYN đến các cổng từ 1 đến 600 trên máy chủ có địa chỉ IP là 192.168.1.3 để kiểm tra tính khả dụng của các cổng trên máy chủ hoặc để thực hiện kiểm tra bảo mật để xem xét cổng nào đang mở**.** Trong IP được kiểm tra có 5 cổng đang mở.

- **hping3 –F –P –U 192.168.1.3**

Lệnh được sử dụng để thử nghiệm cách máy tính 192.168.1.3 xử lý các gói tin mạng đặc biệt với các cờ TCP đặc biệt.



Xmas Scanning

- **Mở tường lửa**

  Tất cả những port được scan là Open & Filtered (Mở và được lọc). Có nghĩa là khi đó, tường lửa đang hoạt động. Một tường lửa thì cơ bản sẽ không phản hồi những gói tin giả định là các open|filtered port.

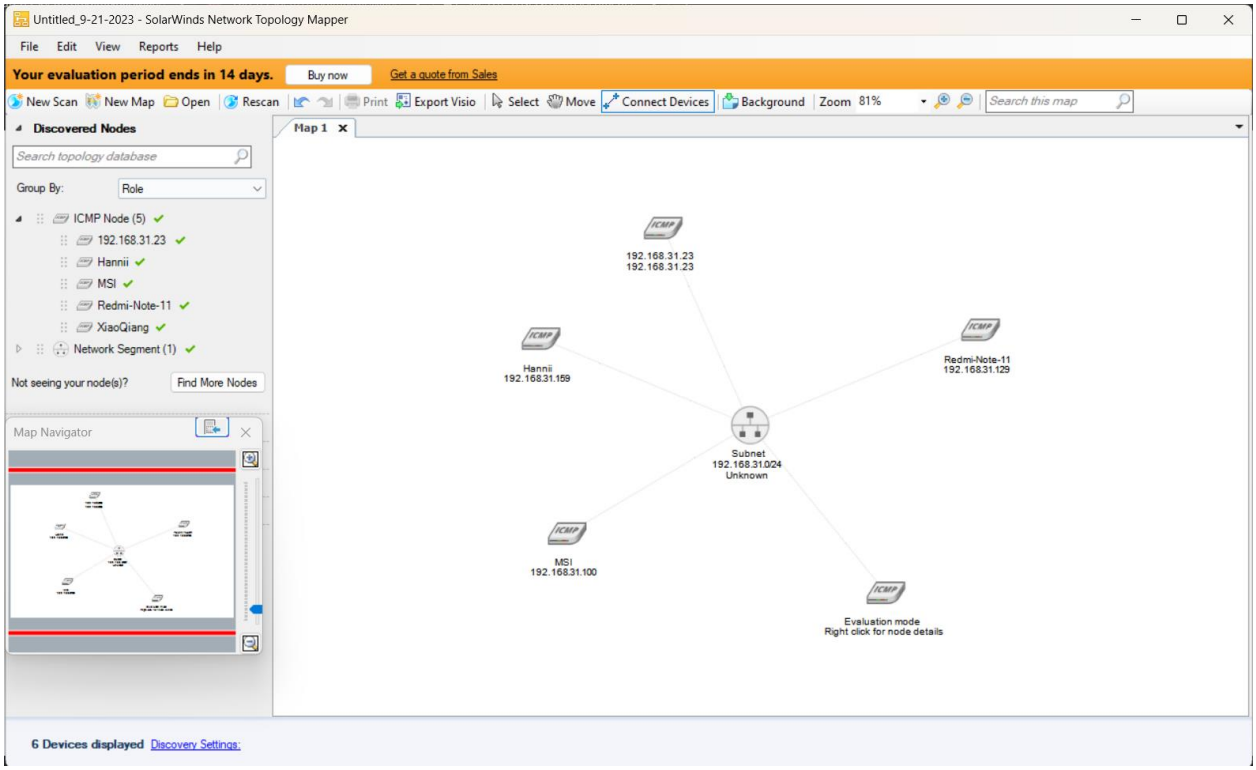
```
root@kali:~# nmap -sX -T4 192.168.1.3
Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-21 03:29 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.3
Host is up (0.00051s latency).
All 1000 scanned ports on 192.168.1.3 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:EE:89:57 (VMware)
```

- **Đóng tường lửa**

  Tường lửa bị vô hiệu hóa, vì vậy tất cả các port được hiển thị là đang đóng.

```
root@kali:~# nmap -sX -T4 192.168.1.3
Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-21 03:28 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.1.3
Host is up (0.0014s latency).
All 1000 scanned ports on 192.168.1.3 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:EE:89:57 (VMware)
```

Ex_04: Network Topology Map



- Subnet address: 192.168.31.0
- Subnet mask: 255.255.255.0
- Có 5 thiết bị trong mạng