

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



BÁO CÁO THỰC HÀNH
BẢO MẬT INTERNET

Giảng viên hướng dẫn: ThS. Tô Nguyễn Nhật Quang
ThS. Bùi Thị Thanh Bình

Sinh viên thực hiện:	Phạm Tiến Cường	12520551
	Phạm Ngọc Dũng	12520090
	Võ Huỳnh Minh Tân	12520382
	Ngô Nhật Tâm	12520700
	Võ Phước Vinh	12520785

TP. Hồ Chí Minh, tháng 12 năm 2016

MỤC LỤC

Chương 2: CEH v8 Labs Module 02 Footprinting and Reconnaissance	5
2.1. Lab 1: Footprinting a Target Network Using the Ping Utility.....	5
2.2. Lab 2: Footprinting a Target Network Using the nslookup Tool	9
2.3. Lab 3: People Search Using the AnyWho Online Tool.....	Error! Bookmark not defined.
2.4. Lab 4: People Search Using the Spoke Online Tool	Error! Bookmark not defined.
2.5. Lab 5: Analyzing Domain and IP Address Queries Using SmartWhois	Error! Bookmark not defined.
2.6. Lab 6: Network Route Trace Using Path Analyzer Pro.....	Error! Bookmark not defined.
2.7. Lab 7: Tracing an Email Using the eMailTrackerPro Tool	Error! Bookmark not defined.
2.8. Lab 8: Collecting Information about a Target Website Using Firebug	Error! Bookmark not defined.
2.9. Lab 9: Mirroring Website Using the HTTrack Web Site Copier Tool.....	Error! Bookmark not defined.
2.10. Lab 10. Extracting a Company's Data Using Web Data Extractor.....	Error! Bookmark not defined.
2.11. Lab 11: Identifying Vulnerabilities and Information Disclosures in Search Engines using Search Diggity	Error! Bookmark not defined.
Chương 3. CEH v8 Labs Module 03 Scanning Networks	Error! Bookmark not defined.
3.1. Lab 1: Scanning System and Network Resources Using Advanced IP Scanner	Error! Bookmark not defined.
3.2. Lab 2: Banner Grabbing to Determine a Remote Target System using ID Serve	Error! Bookmark not defined.
3.3. Lab 4: Monitoring TCP/IP Connections Using the CurrPorts Tool.....	Error! Bookmark not defined.
3.4. Lab 8: Drawing Network Diagrams Using LANSurveyor....	Error! Bookmark not defined.
3.5. Lab 9: Mapping a Network Using Friendly Pinger	Error! Bookmark not defined.
3.6. Lab 15: Basic Network Troubleshooting Using MegaPing ..	Error! Bookmark not defined.

3.7. Lab 16: Detect, Delete and Block Google Cookies Using G-Zapper**Error! Bookmark not defined.**

3.8. Lab 17: Scanning the Network Using the Colasoft Packet Builder**Error! Bookmark not defined.**

3.9. Lab 18: Scanning Devices in a Network Using The Dude....**Error! Bookmark not defined.**

Chương 4. CEH v8 Labs Module 04 Enumeration Error! Bookmark not defined.

4.1. Lab 1 Enumerating a Target Network Using Nmap.....**Error! Bookmark not defined.**

4.2. Lab 2 Enumerating NetBIOS Using the SuperScan Tool**Error! Bookmark not defined.**

4.3. Lab 3 Enumerating NetBIOS Using the NetBIOS Enumerator Tool**Error! Bookmark not defined.**

Chương 5: CEH v8 Labs Module 05 System Hacking..... Error! Bookmark not defined.

5.1. Lab 2: Ẩn giấu file qua NTFS Stream..... **Error! Bookmark not defined.**

5.2. Lab 3: Tìm file ẩn giấu trong NTFS với ADS SPY**Error! Bookmark not defined.**

5.3. Lab 4: Ẩn giấu file sử dụng The Stealth Files Tool**Error! Bookmark not defined.**

5.4. Lab 5: Trích xuất hash mật khẩu hệ thống bằng PWDUMP7..... **Error! Bookmark not defined.**

5.5. Lab 6: Sử dụng Winrtgen tạo rainbowtables..... **Error! Bookmark not defined.**

5.6. Lab 7: Password cracking sử dụng RAINBOWCRACK.....**Error! Bookmark not defined.**

5.7. Lab 8: Extracting Administrator Passwords Using LophtCrack . **Error! Bookmark not defined.**

5.8. Lab 9: Crack password sử dụng OPHCRACK..... **Error! Bookmark not defined.**

Chương 6. CEH v8 Labs Module 06 Trojans and Backdoors..... Error! Bookmark not defined.

6.1. Lab 1: Creating a Server Using the ProRat **Error! Bookmark not defined.**

6.2. Lab 3: Wrapping a Trojan Using One File..... **Error! Bookmark not defined.**

6.3. Lab 4: Proxy Server Trojan **Error! Bookmark not defined.**

6.4. Lab 5: HTTP Trojan **Error! Bookmark not defined.**

6.5. Lab 6: Creating a Server Using the Theef **Error! Bookmark not defined.**

Chương 7: CEH v8 Labs Module 07 Viruses and Worms Error! Bookmark not defined.

7.1. Lab 1: Creating a Virus Using the JPS Virus Maker Tool....**Error! Bookmark not defined.**

7.2. Lab 3: Virus Analysis Using Virus Total **Error! Bookmark not defined.**

7.3. Lab 4: Scan for Viruses Using Kaspersky Antivirus 2013 ...**Error! Bookmark not defined.**

Chương 8. CEH v8 Labs Module 08 Sniffers..... Error! Bookmark not defined.

8.1. Lab 2: Spoofing MAC Address Using SMAC **Error! Bookmark not defined.**

8.2. Lab 3: Sniffing a Network Using the WinArpAttacker Tool **Error! Bookmark not defined.**

8.3. Lab 4: Analyzing a Network Using the Capsa Network Analyzer**Error! Bookmark not defined.**

8.4. Lab 5: Sniffing Passwords Using Wireshark..... **Error! Bookmark not defined.**

8.5. Lab 6: Performing Man-in-the-Middle Attack Using Cain & Abel**Error! Bookmark not defined.**

8.6. Lab 7: Detecting ARP Attacks with the XArp Tool**Error! Bookmark not defined.**

8.7. Lab 8: Detecting Systems Running in Promiscuous Mode in a Network Using PromqryUI **Error! Bookmark not defined.**

8.8. Lab 9: Sniffing Password from Captured Packets using Sniff - O – Matic**Error! Bookmark not defined.**

Chương 9: CEH v8 Labs Module 09 Social Engineering Error! Bookmark not defined.

9.1. Lab 1: Detecting Phishing Using Netcraft..... **Error! Bookmark not defined.**

9.2. Lab 2: Detecting Phishing Using PhishTank..... **Error! Bookmark not defined.**

Chương 11: CEH v8 Labs Module 11 Session Hijacking Error! Bookmark not defined.

11.1. Lab 1: Tấn công Session Hijacking sử dụng ZAP**Error! Bookmark not defined.**

Chương 12: CEH v8 Labs Module 12 Hacking Webservers..... Error! Bookmark not defined.

12.1. Lab 1: Footprinting Webserver Using the httprecon Tool ..**Error! Bookmark not defined.**

12.2. Lab 2: Footprinting a Webserver Using ID Serve **Error! Bookmark not defined.**

Chương 13: CEH v8 Labs Module 13 Hacking Web Applications Error! Bookmark not defined.

13.1 Lab 2: Website Vulnerability Scanning Using Acunetix WVS . **Error! Bookmark not defined.**

Chương 14: CEH v8 Labs Module 14 SQL Injection Error! Bookmark not defined.

14.1. Testing for SQL Injection Using WebCruiser Tool**Error! Bookmark not defined.**

14.2. Testing for SQL Injection Using NStalker Tool .. **Error! Bookmark not defined.**

Chương 15: CEH v8 Labs Module 15 Hacking Wireless Networks... Error! Bookmark not defined.

15.1. Lab 3: Sniffing the Network Using the OmniPeek Network Analyzer**Error! Bookmark not defined.**

Chương 17: CEH v8 Labs Module 17 Evading IDS, Firewalls and Honeypots.. Error! Bookmark not defined.

17.1. Lab 1: Logging Snort Alerts to Kiwi Syslog Server**Error! Bookmark not defined.**

17.2. Lab 2: Detecting Intruders and Worms Using KFSensor Honeypot IDS**Error! Bookmark not defined.**

Chương 18: CEH v8 Labs Module 18 Buffer Overflow .. Error! Bookmark not defined.

18.1. Lab 1: Buffer Overflow Attack **Error! Bookmark not defined.**

Chương 19. CEH v8 Labs Module 19 Cryptography Error! Bookmark not defined.

19.1. Lab 1: Basic Data Encrypting Using Hash Calc .. **Error! Bookmark not defined.**

19.2. Lab 2: Basic Data Encrypting Using MD5 Calculator**Error! Bookmark not defined.**

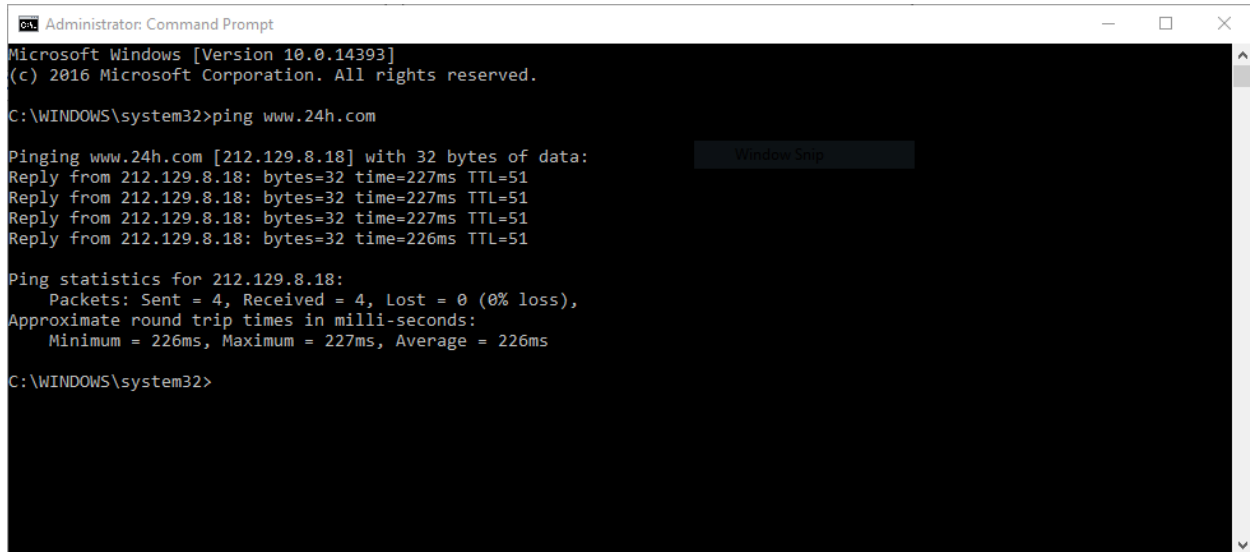
19.3. Lab 3: Basic Data Encrypting Using Advanced Encryption Package.....**Error! Bookmark not defined.**

19.4. Lab 6: Encrypting and Decrypting Data Using BCTextEncoder**Error! Bookmark not defined.**

Chương 2: CEH v8 Labs Module 02 Footprinting and Reconnaissance

2.1. Lab 1: Footprinting a Target Network Using the Ping Utility

Mở Command Prompt và tìm địa chỉ của trang web www.24h.com bằng cách sử dụng lệnh ping www.24h.com. Thấy được địa chỉ ip của trang web là: 212.129.8.18.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping www.24h.com

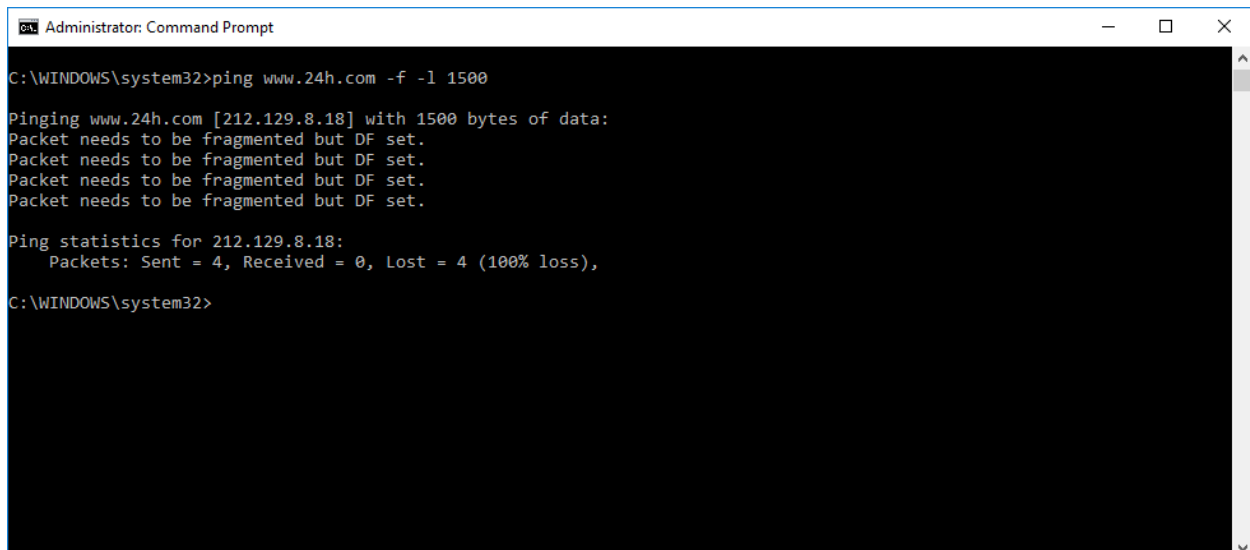
Pinging www.24h.com [212.129.8.18] with 32 bytes of data:
Reply from 212.129.8.18: bytes=32 time=227ms TTL=51
Reply from 212.129.8.18: bytes=32 time=227ms TTL=51
Reply from 212.129.8.18: bytes=32 time=227ms TTL=51
Reply from 212.129.8.18: bytes=32 time=226ms TTL=51

Ping statistics for 212.129.8.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 226ms, Maximum = 227ms, Average = 226ms

C:\WINDOWS\system32>
```

Tiếp theo, ta sẽ tìm kích thước khung hình lớn nhất trên mạng.

Nhập ping www.24h.com -f -l 1500.



```
Administrator: Command Prompt

C:\WINDOWS\system32>ping www.24h.com -f -l 1500

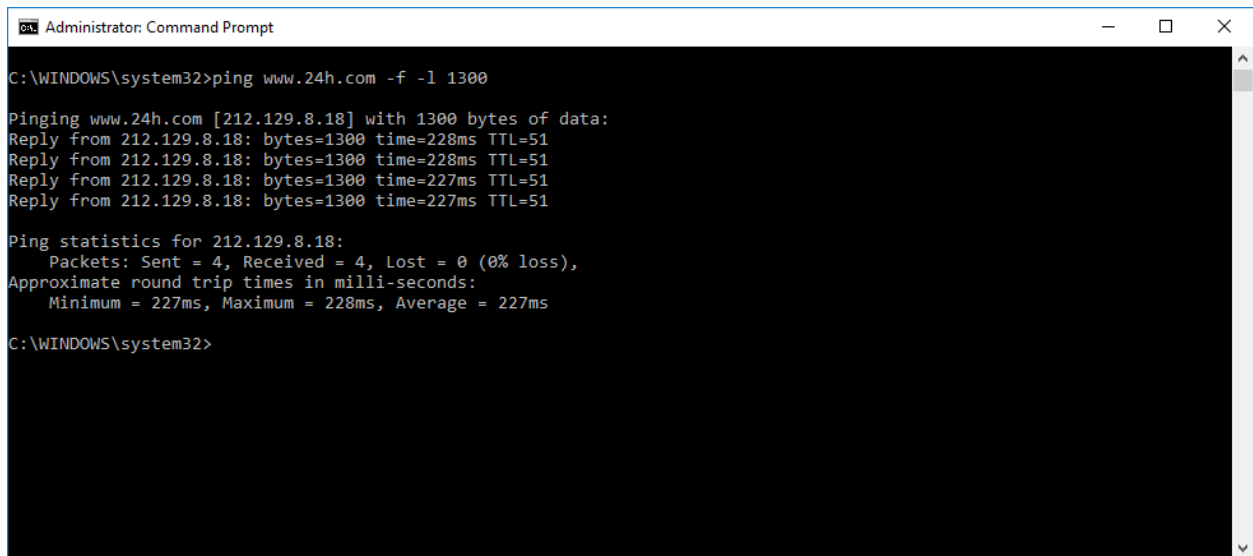
Pinging www.24h.com [212.129.8.18] with 1500 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 212.129.8.18:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\WINDOWS\system32>
```

Kết quả cho thấy khung hình quá lớn và cần được phân mảnh.

Nhập ping www.24h.com -f -l 1300 và xem kết quả.



```
Administrator: Command Prompt
C:\WINDOWS\system32>ping www.24h.com -f -l 1300

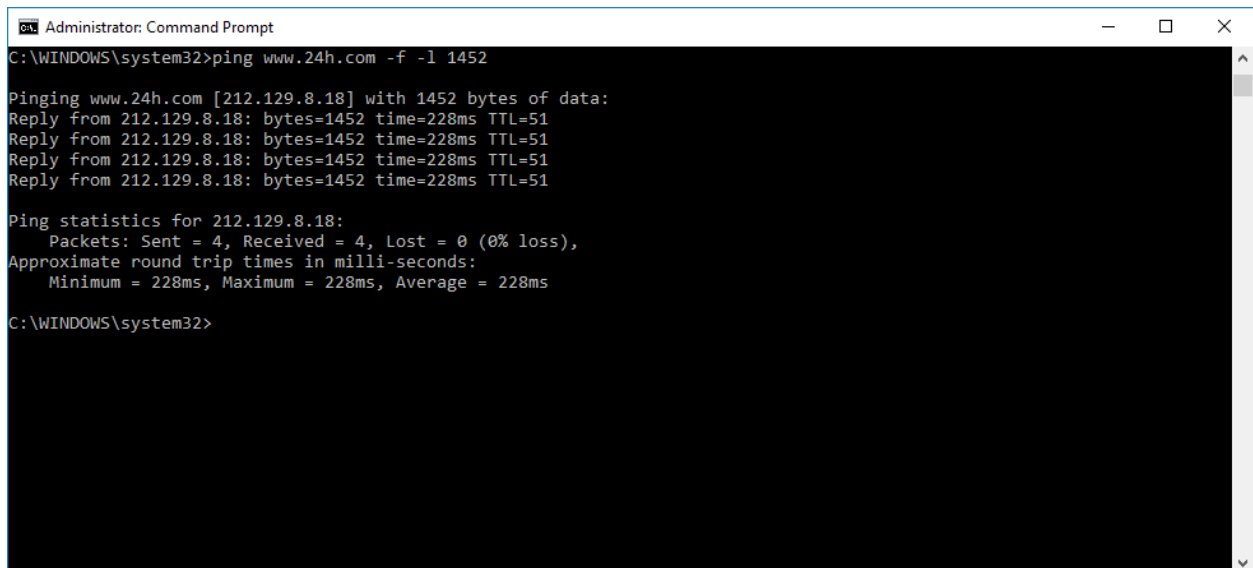
Pinging www.24h.com [212.129.8.18] with 1300 bytes of data:
Reply from 212.129.8.18: bytes=1300 time=228ms TTL=51
Reply from 212.129.8.18: bytes=1300 time=228ms TTL=51
Reply from 212.129.8.18: bytes=1300 time=227ms TTL=51
Reply from 212.129.8.18: bytes=1300 time=227ms TTL=51

Ping statistics for 212.129.8.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 227ms, Maximum = 228ms, Average = 227ms

C:\WINDOWS\system32>
```

Qua 2 lệnh ping trên, cho thấy kích thước tối đa của gói là ít hơn 1500 byte và lớn hơn 1300 byte.

Bây giờ, hãy thử các giá trị khác nhau cho đến khi bạn tìm thấy kích thước khung hình tối đa (trong trường hợp này là -f -l 1452).



```
Administrator: Command Prompt
C:\WINDOWS\system32>ping www.24h.com -f -l 1452

Pinging www.24h.com [212.129.8.18] with 1452 bytes of data:
Reply from 212.129.8.18: bytes=1452 time=228ms TTL=51
Reply from 212.129.8.18: bytes=1452 time=228ms TTL=51
Reply from 212.129.8.18: bytes=1452 time=228ms TTL=51
Reply from 212.129.8.18: bytes=1452 time=228ms TTL=51

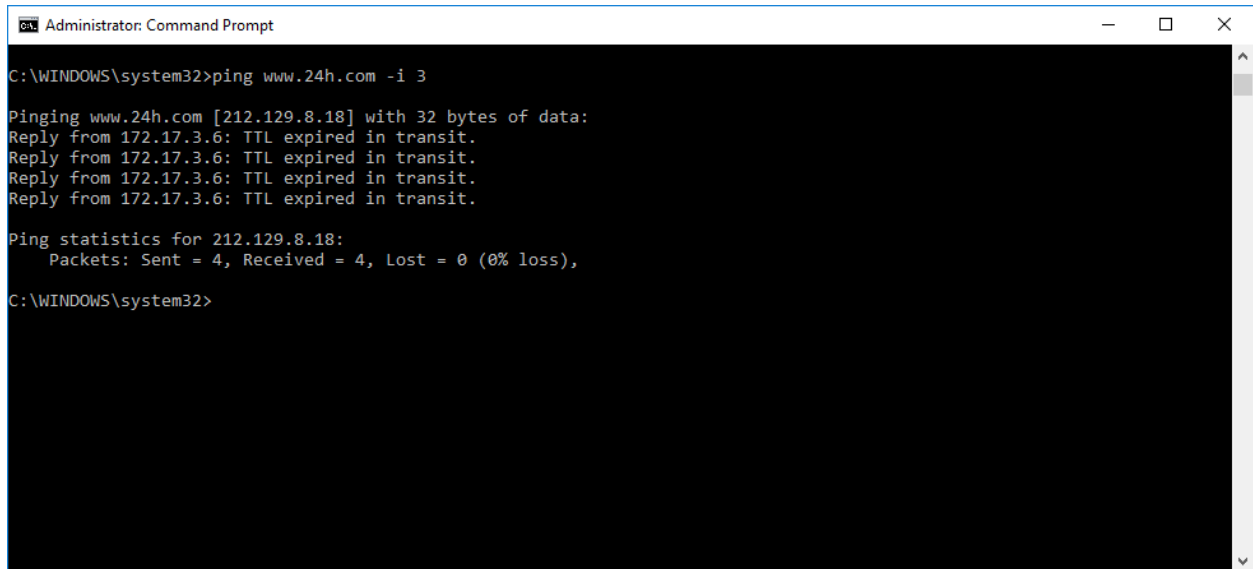
Ping statistics for 212.129.8.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 228ms, Maximum = 228ms, Average = 228ms

C:\WINDOWS\system32>
```

Lưu ý: Các kích thước khung hình khác nhau tùy thuộc vào mạng.

Bây giờ tìm hiểu những sẽ xảy ra khi TTL (Time to Live) hết hạn. Mỗi khung hình trên mạng đều có TTL xác định. Nếu TTL bằng không, router loại bỏ gói đó. Cơ chế này giúp ngăn chặn mất gói tin.

Nhập ping www.24h.com -i 3.



```
Administrator: Command Prompt
C:\WINDOWS\system32>ping www.24h.com -i 3

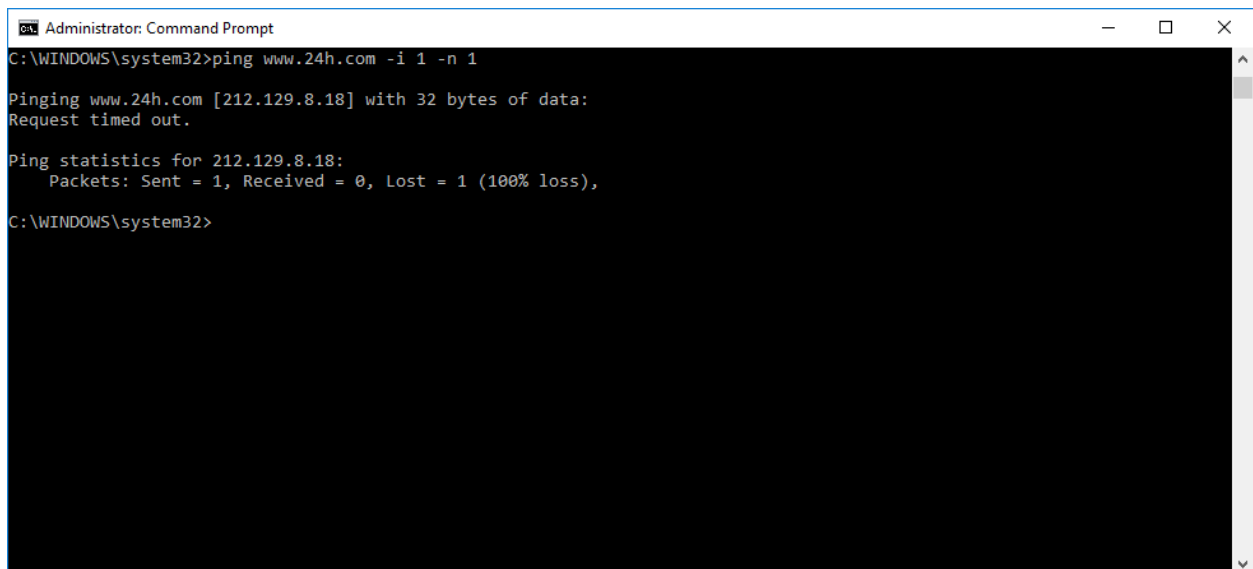
Pinging www.24h.com [212.129.8.18] with 32 bytes of data:
Reply from 172.17.3.6: TTL expired in transit.
Reply from 172.17.3.6: TTL expired in transit.
Reply from 172.17.3.6: TTL expired in transit.
Reply from 172.17.3.6: TTL expired in transit.

Ping statistics for 212.129.8.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\WINDOWS\system32>
```

Nhận được kết quả từ địa chỉ ip khác là Reply from 115.200.79.1: TTL expired in transit, điều này có nghĩa là router đã loại bỏ các khung hình, bởi vì nó đã hết hạn TTL.

Gõ ping www.24h.com -i 1 -n 1 và xem kết quả.



```
Administrator: Command Prompt
C:\WINDOWS\system32>ping www.24h.com -i 1 -n 1

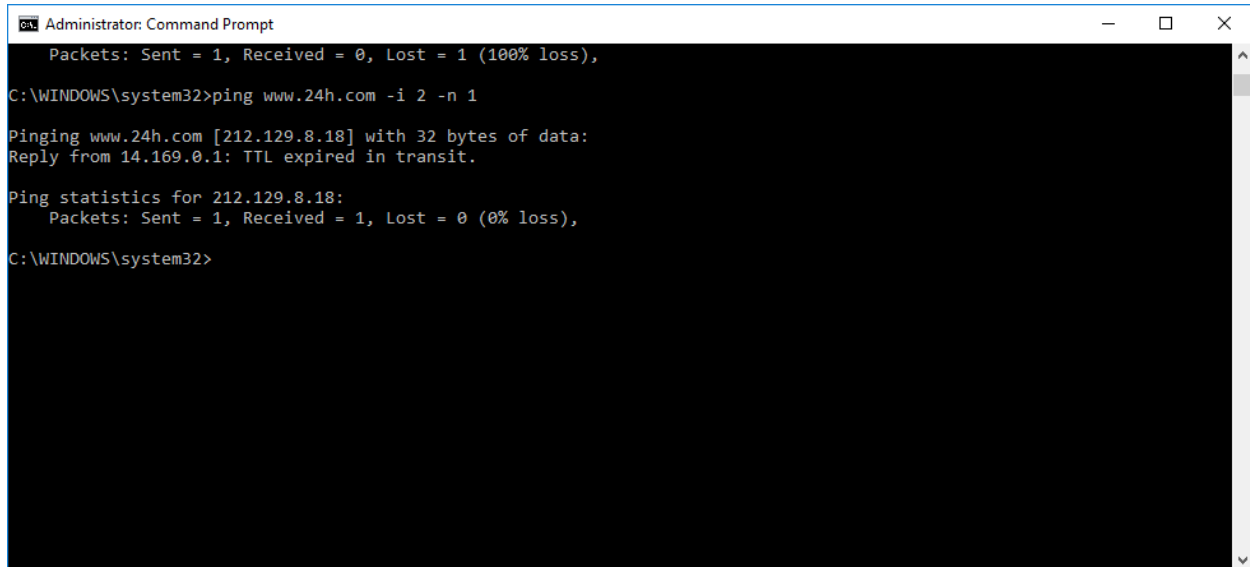
Pinging www.24h.com [212.129.8.18] with 32 bytes of data:
Request timed out.

Ping statistics for 212.129.8.18:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

C:\WINDOWS\system32>
```

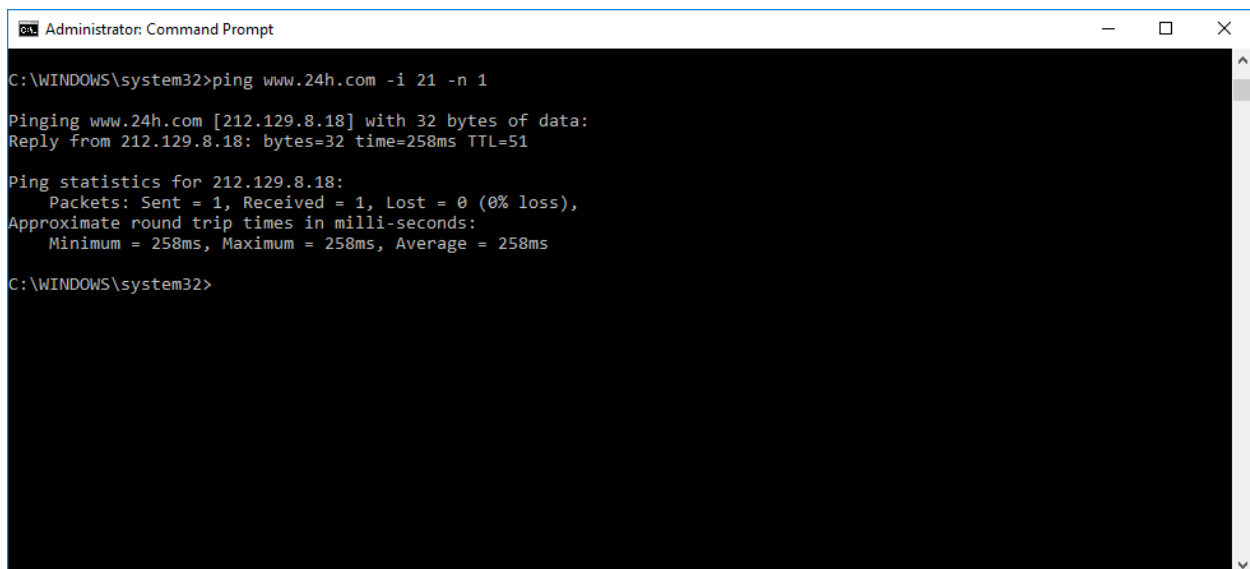

Lệnh -n 1 dùng để xuất 1 dòng kết quả duy nhất, thay vì nhận được 4 dòng kết quả như trên Windows hoặc ping mãi mãi trên Linux.

Gõ ping www.24h.com -i 2 -n 1 và xem kết quả.



```
Administrator: Command Prompt
Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
C:\WINDOWS\system32>ping www.24h.com -i 2 -n 1
Pinging www.24h.com [212.129.8.18] with 32 bytes of data:
Reply from 14.169.0.1: TTL expired in transit.
Ping statistics for 212.129.8.18:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
C:\WINDOWS\system32>
```

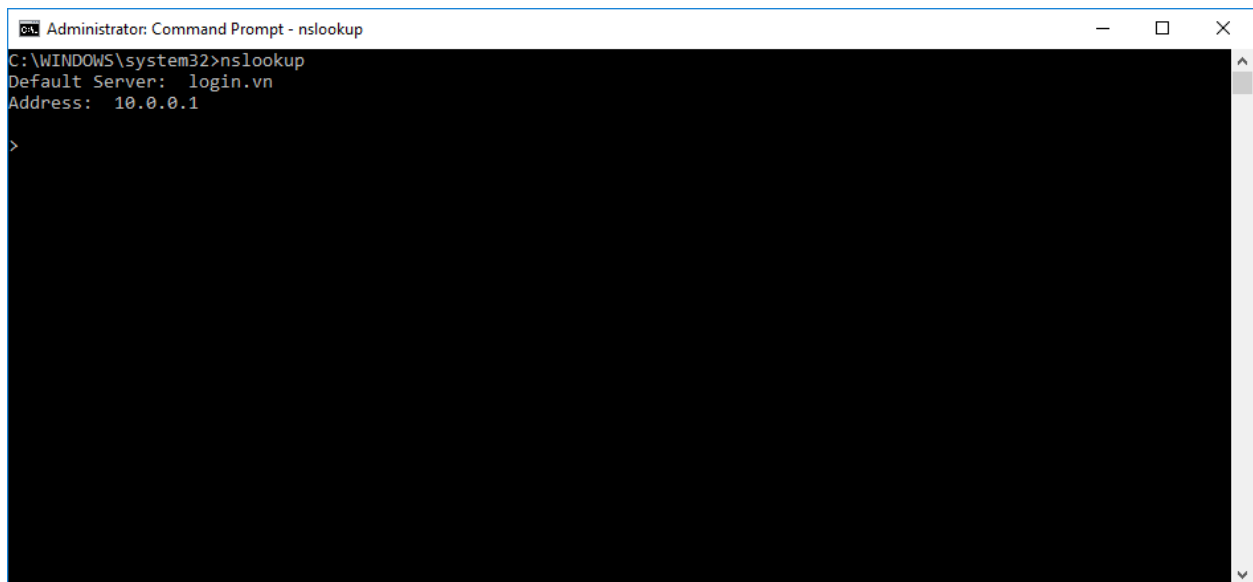
Lặp lại các bước trên cho đến khi bạn được địa chỉ ip cho www.24h.com (trong trường hợp này là -i 21) là xong.



```
Administrator: Command Prompt
C:\WINDOWS\system32>ping www.24h.com -i 21 -n 1
Pinging www.24h.com [212.129.8.18] with 32 bytes of data:
Reply from 212.129.8.18: bytes=32 time=258ms TTL=51
Ping statistics for 212.129.8.18:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 258ms, Maximum = 258ms, Average = 258ms
C:\WINDOWS\system32>
```

2.2. Lab 2: Footprinting a Target Network Using the nslookup Tool

Mở command prompt, nhập nslookup và Enter.



```
Administrator: Command Prompt - nslookup
C:\WINDOWS\system32>nslookup
Default Server: login.vn
Address: 10.0.0.1
>
```

Kết quả DNS server name: 10.0.0.1

Tiếp theo nhập help và xem kết quả.