

- Hackthone
 - Zphisher
 - Advance phishing tool
 - <https://github.com/Ignitetch/AdvPhishing>
 - **Nexphisher**
 - <https://kalilinuxtutorial.com/install-nexphisher-on-kali-linux/>
 - Wireshark
 - **Slowloris (DOS attack)**
-
- Hping3
 - Nmap

```
kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[satish@kali: ~] satish@kali: ~ Capturing from eth0 10:29 PM
satish@kali: ~
File Actions Edit View Help
root@kali:~/# hping3 -1 -c 6 -i 5 192.168.217.3
HPING 192.168.217.3 (eth0 192.168.217.3): icmp mode set,
 28 headers + 0 data bytes
len=46 ip=192.168.217.3 ttl=64 id=17102 icmp_seq=0 rtt=7
.3 ms
len=46 ip=192.168.217.3 ttl=64 id=17850 icmp_seq=1 rtt=1
005.1 ms
len=46 ip=192.168.217.3 ttl=64 id=18631 icmp_seq=2 rtt=1
004.0 ms
len=46 ip=192.168.217.3 ttl=64 id=19834 icmp_seq=3 rtt=1
```

```
File Actions Edit View Help  Statistics Telephony Wireless Tools Help
root@kali:~/# hping3 -1 --fast 192.168.217.3
```

No.	Time	Source	Destination	Protocol	Length	Info
1	5.187526101	PcsCompu_88:69:85	PcsCompu_28:63:0a	ARP	42	Who has 192.168.217.3? Tell 192.168.217.4
2	5.188992548	PcsCompu_28:63:0a	PcsCompu_88:69:85	ARP	66	192.168.217.3 is at 88:69:85:69:85:85
3	5.237017213	PcsCompu_88:69:85	PcsCompu_28:63:0a	ARP	66	Who has 192.168.217.4? Tell 192.168.217.3
4	5.237017213	PcsCompu_28:63:0a	PcsCompu_88:69:85	ARP	42	192.168.217.4 is at 88:69:85:69:85:85
11	30.000722635	192.168.217.4	192.168.217.3	ICMP	42	Echo (ping) request id=652269, seq=65, ttl=64 (reply in 12)
12	30.000722635	192.168.217.3	192.168.217.4	ICMP	66	Echo (ping) reply id=652269, seq=65, ttl=64 (request in 11)
13	35.010718957	192.168.217.4	192.168.217.3	ICMP	42	Echo (ping) request id=652269, seq=66, ttl=64 (reply in 34)
14	35.010718957	192.168.217.3	192.168.217.4	ICMP	66	Echo (ping) reply id=652269, seq=66, ttl=64 (request in 13)
15	35.072756472	PcsCompu_28:63:0a	PcsCompu_88:69:85	ARP	66	Who has 192.168.217.4? Tell 192.168.217.3
16	35.072756472	PcsCompu_88:69:85	PcsCompu_28:63:0a	ARP	42	192.168.217.4 is at 88:69:85:69:85:85
17	35.120029902	PcsCompu_88:69:85	PcsCompu_28:63:0a	ARP	42	Who has 192.168.217.3? Tell 192.168.217.4
18	35.120029902	PcsCompu_28:63:0a	PcsCompu_88:69:85	ARP	66	192.168.217.3 is at 88:69:85:69:85:85
19	35.010718957	192.168.217.4	192.168.217.3	ICMP	42	Echo (ping) request id=652269, seq=67, ttl=64 (reply in 30)
20	35.010718957	192.168.217.3	192.168.217.4	ICMP	66	Echo (ping) reply id=652269, seq=67, ttl=64 (request in 19)
21	35.020219475	192.168.217.4	192.168.217.3	ICMP	42	Echo (ping) request id=652269, seq=68, ttl=64 (reply in 37)
22	35.020219475	192.168.217.3	192.168.217.4	ICMP	66	Echo (ping) reply id=652269, seq=68, ttl=64 (request in 21)
23	35.020219475	192.168.217.4	192.168.217.3	ICMP	42	Echo (ping) request id=652269, seq=69, ttl=64 (reply in 34)
24	35.020219475	192.168.217.3	192.168.217.4	ICMP	66	Echo (ping) reply id=652269, seq=69, ttl=64 (request in 23)
25	35.020219475	192.168.217.4	192.168.217.3	ICMP	42	Echo (ping) request id=652269, seq=70, ttl=64 (reply in 30)
26	35.020219475	192.168.217.3	192.168.217.4	ICMP	66	Echo (ping) reply id=652269, seq=70, ttl=64 (request in 25)

```
File Machine View Input Devices Help
satish@kali: ~
satish@kali: ~
Capturing from eth0 10:31 PM

File Actions Edit View Help
root@kali:/# hping3 -1 --faster 192.168.217.3
QStandardPaths: XDG_RUNTIME_DIR not set, default
/tmp/runtime-root'
22:29:45.423 Main Warn QXcbConnection: XCB e
(BadWindow), sequence: 7146, resource id: 210624
r code: 40 (TranslateCoords), minor code: 0
22:30:39.259 Main Warn QXcbConnection: XCB e
(BadWindow), sequence: 9701, resource id: 210600
```

kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

satish@kali: ~ satish@kali: ~ Capturing from eth0 10:36 PM

satish@kali: ~

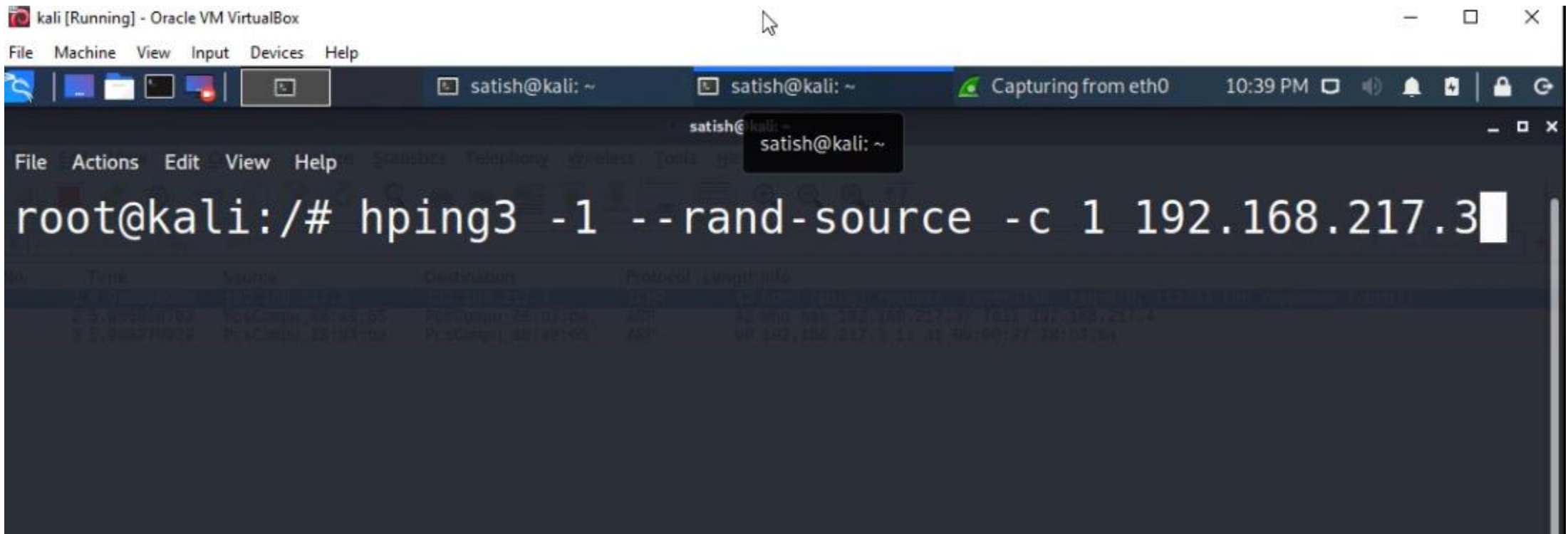
File Actions Edit View Help

```
root@kali:/# hping3 -1 -a 192.168.217.2 -c 1 192.168.217.3
```

StandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'

22:29:45.423 Main Warn QXcbConnection: XCB error: 3 (BadWindow), sequence: 7146, resource id: 21062442, major code: 40 (TranslateCoords), minor code: 0

22:30:39.259 Main Warn QXcbConnection: XCB error: 3 (BadWindow), sequence: 9701, resource id: 21069004, major code: 40 (TranslateCoords), minor code: 0





All Links



Search Links

CREATE

CREATE LINK



Links

☒ Date Created ☐ Top Performing

Filters

Tag



☐ Hidden Links Only

1 Result

Clicks all time

Show Chart

MAY 31

☐ Attacker - The Domain Name Attacker.com is Now For...

bit.ly/3x0bom6

0 clicks

Attacker - The Domain Name Attacker.com is Now For Sale.

May 31, 8:54 AM by DrSniper

bit.ly/3x0bom6

Copy

Destination: https://attacker.com/

Add tags

0

TOTAL CLICKS

bit.ly



ENTER LONG URL

https://attacker.com



UTM Parameters (Optional)

UTMs can help you track web traffic in analytics tools. [Learn more](#)

SOURCE

e.g. google, newsletter

MEDIUM

e.g. cpc, banner, email

CAMPAIGN

e.g. spring_sale



If you use UTMs, be sure to



[Upgrade for bulk imports](#)

- Ngrok.io

File Edit Selection Find View Goto Tools Project Preferences Help

◀ ▶ https://example.com/?r=attacker.com •

1 https://example.com/?r=attacker.com

- IDN Homograph attack

Homograph Examples			
Sn	Fake Name	Original Name	Remark
1	techchip	techchip	
2	paypal	paypal	
3	google	google	
4	techchip	techchip	
5	facebook	facebook	
6	apple	apple	
7	rnicrosoft	microsoft	
8	clog	dog	



Hey there!

This may or may not be the site you are looking for! This site demonstration of a flaw in the way unicode domains are handled **browser isn't affected.**

[Read the blog post for the full details](#)

Hey there!

Apple

Apple Inc. (US) <https://www.apple.com>



Mac

iPad

iPhone

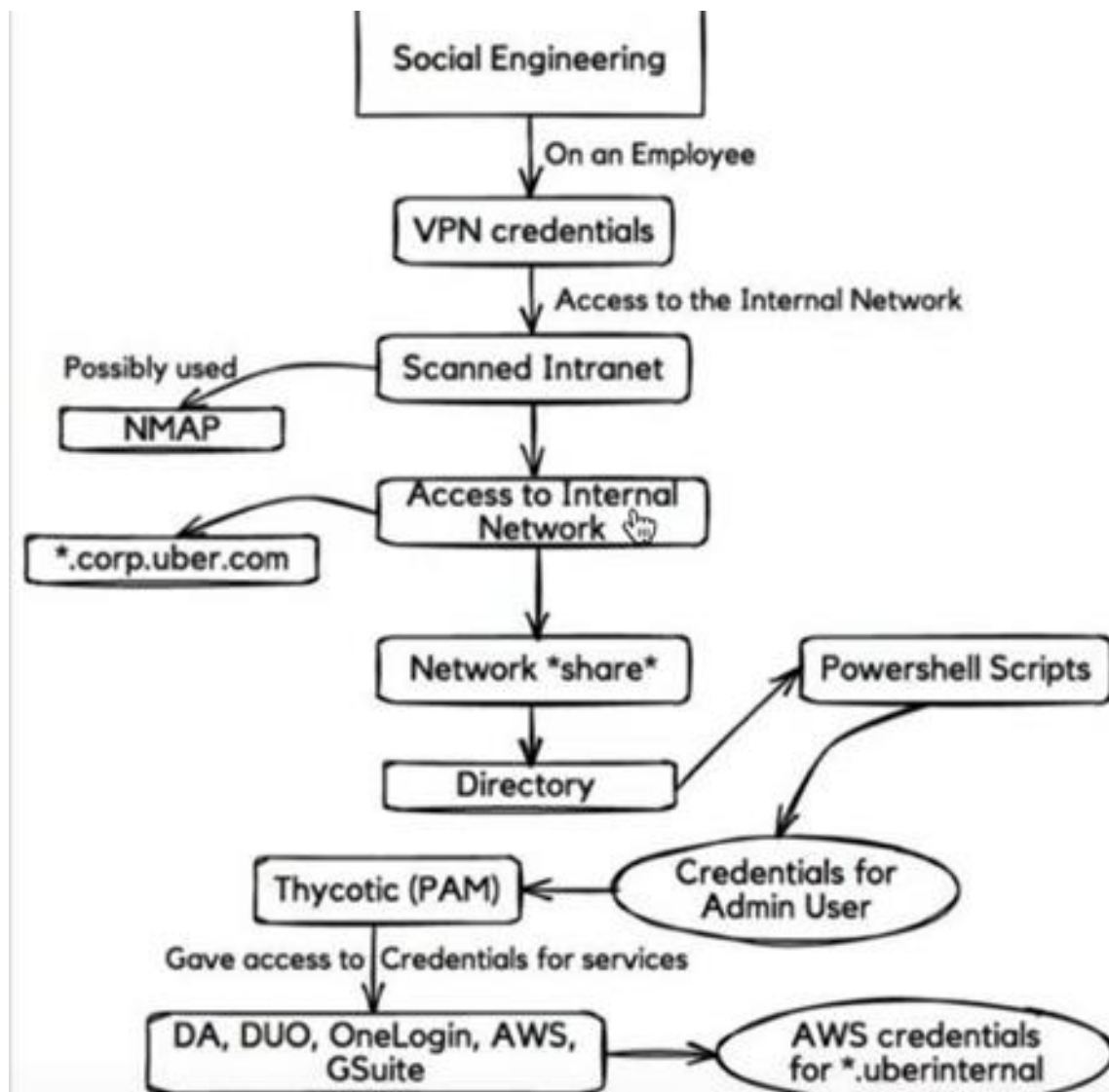
Watch

TV

Special Edition

(PR

- Homograph generator
- Uber attack case study

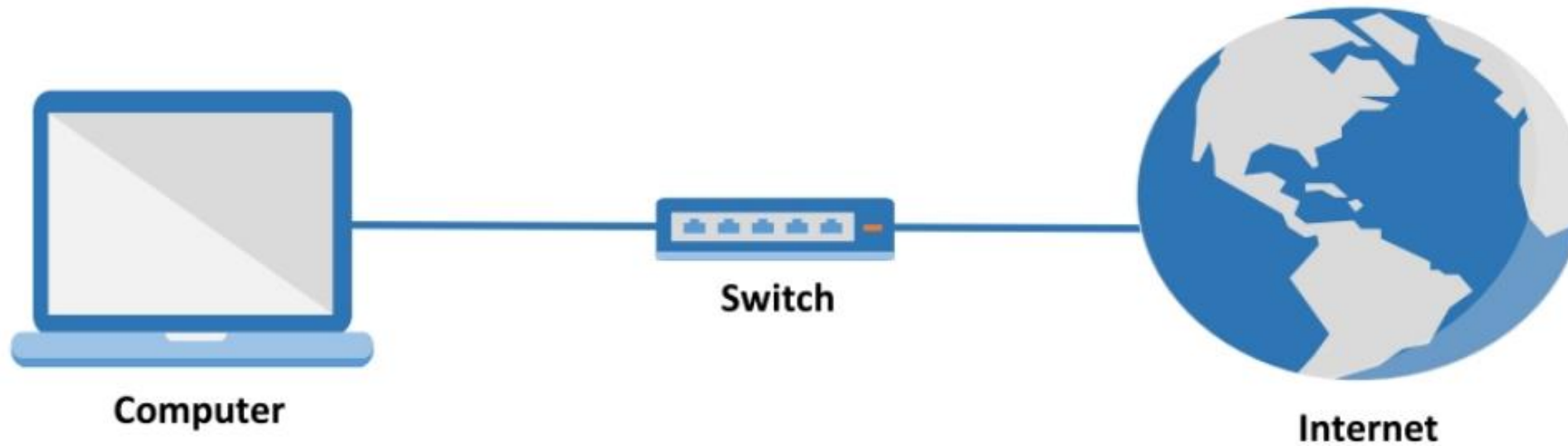


- Lab manual browser security

Website : www.bing.com	4
WHOIS FOOTPRINTING	6
Website : www.whois.net	7
Website : www.who.is	8
Website : www.godaddy.com	10
Tool : Smartwhois.....	11
NETWORK FOOTPRINTING	14
Website : www.whatismyipaddress.com	16
Website : www.technicalinfo.net	18
Website : www.network-tools.com	22
Tool : ping	23
Tool : IP2country	25
Tool : Path Analyzer Pro.....	26
Tool : VisualRoute	28
Tool : Sam Spade	29
WEBSITE FOOTPRINTING	31
Website : www.netcraft.com	32

Website : www.spokeo.com	57
Website : www.pipl.com	59
EMAIL FOOTPRINTING	60
Website : www.ip2location.com	61
Website : www.whatismyipaddress.com	63
Website : www.whoreadme.com	65
Tool : EmailTrackerPro	68
GOOGLE HACKING	70
Website : www.exploit-db.com	71
Website : www.shodan.io	73
Tool : Google Hacks	76
IP SCANNER.....	77
Tool : Angry IP Scanner	78
Tool : Ping Manager	80
Tool: Advanced IP Scanner.....	82
Tool : MyLanViewer Network/IP Scanner	83
PORT SCANNER.....	85
Tool : Superscan	86
Tool : Advanced Port Scanner	88
VULNERABILITY SCANNER.....	89
Tool : Zenmap (NMAP - GUI).....	90
Tool : Shadow Security Scanner.....	93
Tool : Retina.....	96
WEB APPLICATION SCANNER.....	98
Tool : Acunetix.....	99
EXPLOITS.....	104
Website : www.securityfocus.com	105
Web Sever Hacking.....	107
Router Hacking	110
Internet Explorer Hacking	112
Web Application Hacking Through XSS	114
Web Application Hacking Through SQL Injection	116

FOOTPRINTING THROUGH SEARCH ENGINES



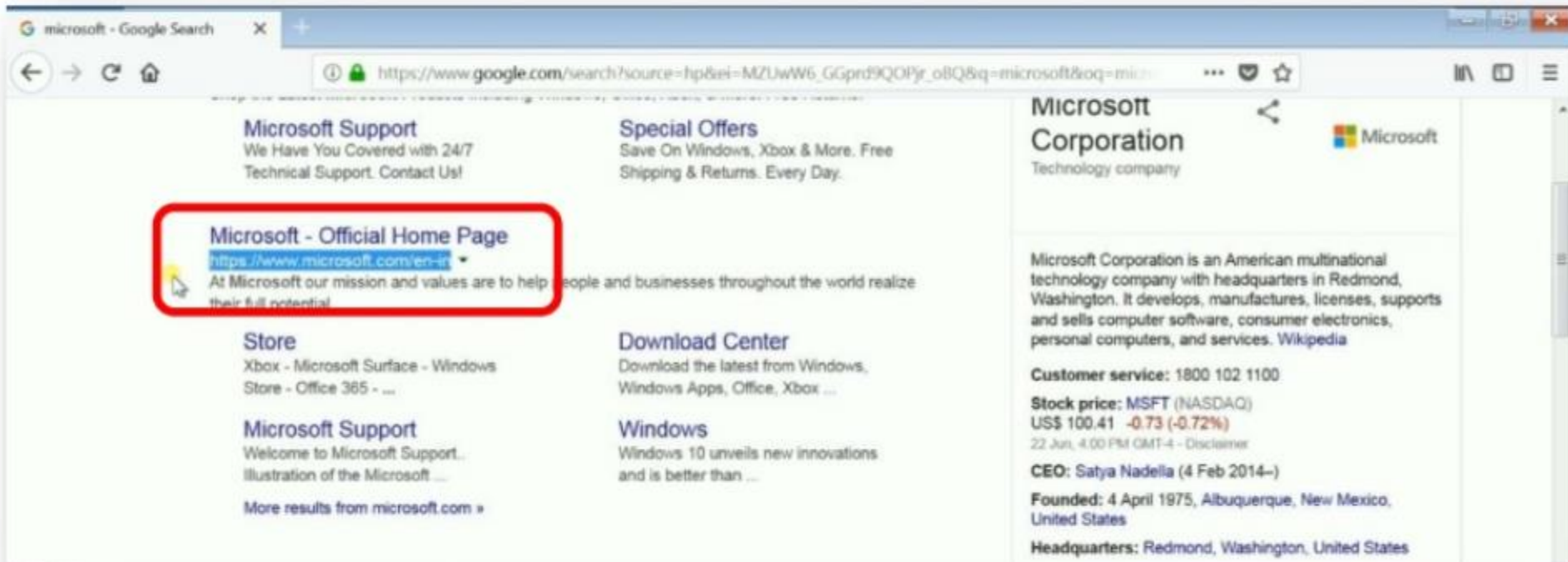
Pre-requisite:

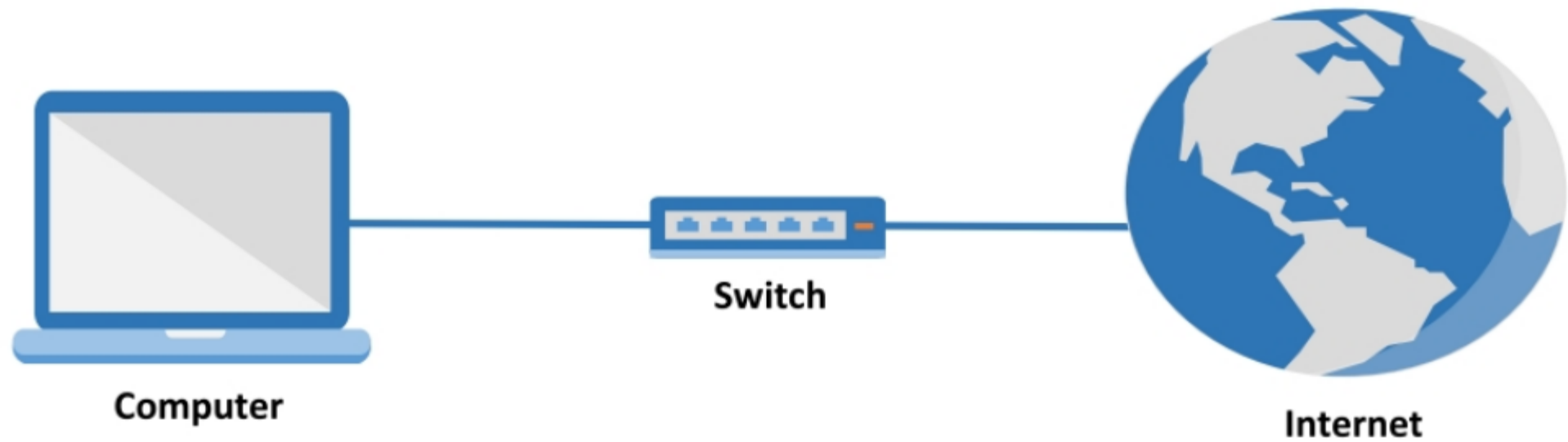
- Computer installed with OS
- Internet Connection (Broadband, Dial-up)

Footprinting – Search Engines Websites

- www.google.com
- www.bing.com

- We get the organization's website URL in the search result which gives us the domain name used by the organization.



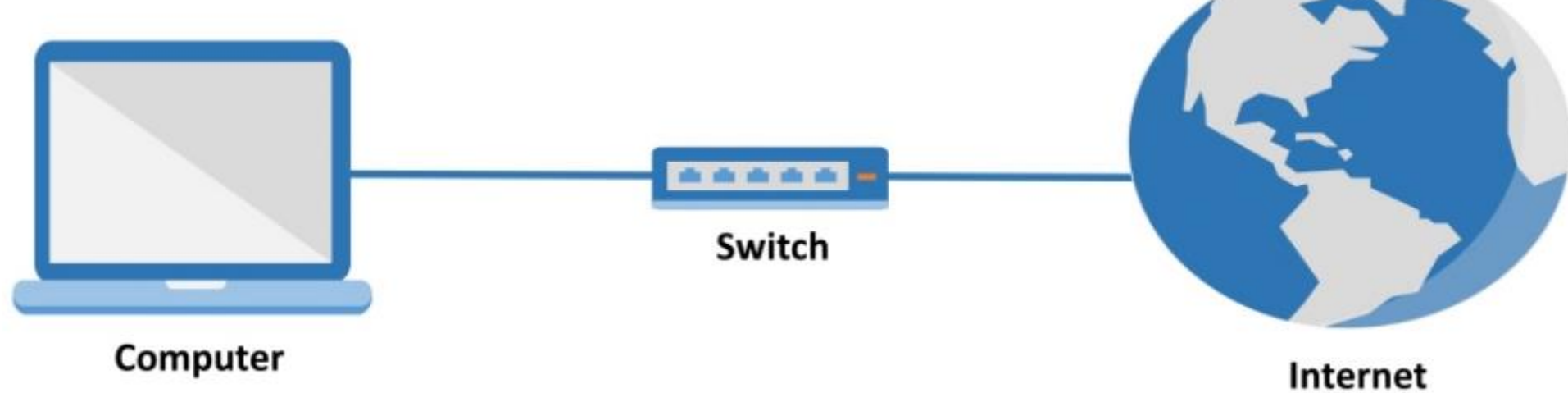


Pre-requisite:

- Computer installed with OS
- Internet Connection (Broadband, Dial-up)

Footprinting – Whois Websites

- www.whois.net
- www.who.is
- www.godaddy.com



Pre-requisite:

- Computer installed with OS
- Internet Connection (Broadband, Dial-up)

Network Footprinting – Websites

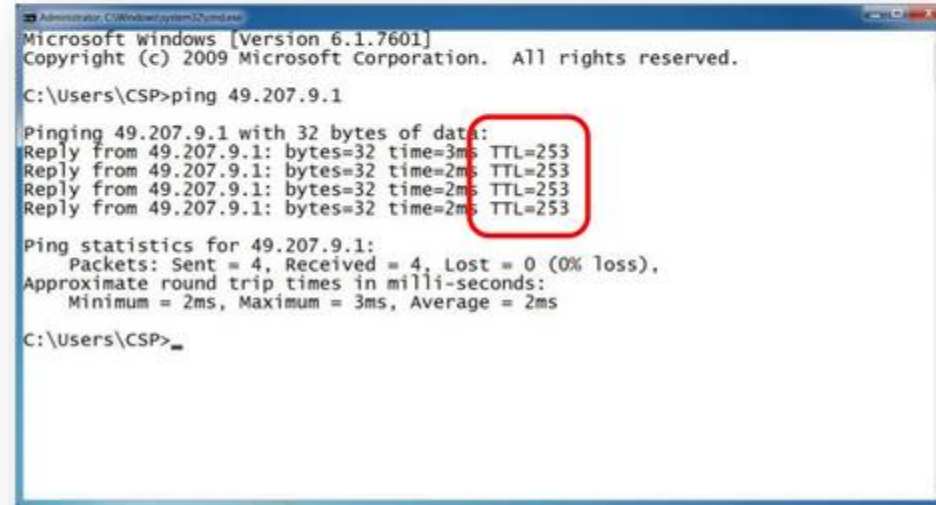
- www.whatismyipaddress.com
- www.technicalinfo.net
- www.network-tools.com

Network Footprinting – Tools

Tool : ping

Ping command can be used to check connectivity or availability of a host in the network. Ping also helps us find the kind of system that we are communicating to. Ping uses ICMP protocol.

- If the TTL value for a ping reply is between 226 and 255, it is a network device like a router or switch.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

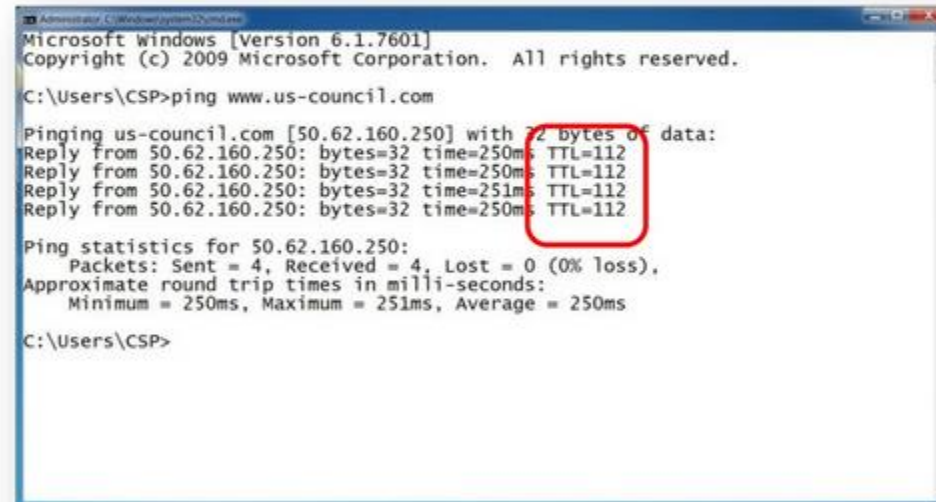
C:\Users\CSP>ping 49.207.9.1

Pinging 49.207.9.1 with 32 bytes of data:
Reply from 49.207.9.1: bytes=32 time=3ms TTL=253
Reply from 49.207.9.1: bytes=32 time=2ms TTL=253
Reply from 49.207.9.1: bytes=32 time=2ms TTL=253
Reply from 49.207.9.1: bytes=32 time=2ms TTL=253

Ping statistics for 49.207.9.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\CSP>
```

- If the TTL value for a ping reply is between 99 and 128, it is a windows host.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

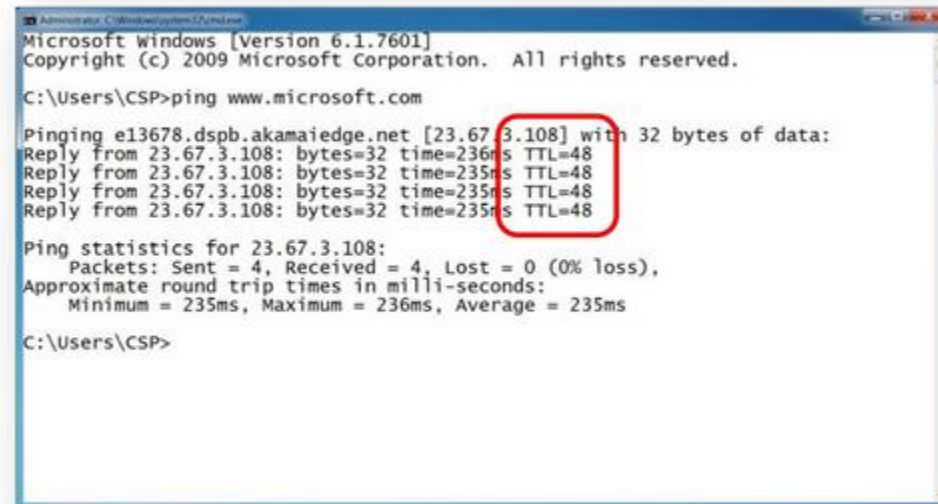
C:\Users\CSP>ping www.us-council.com

Pinging us-council.com [50.62.160.250] with 32 bytes of data:
Reply from 50.62.160.250: bytes=32 time=250ms TTL=112
Reply from 50.62.160.250: bytes=32 time=250ms TTL=112
Reply from 50.62.160.250: bytes=32 time=251ms TTL=112
Reply from 50.62.160.250: bytes=32 time=250ms TTL=112

Ping statistics for 50.62.160.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 250ms, Maximum = 251ms, Average = 250ms

C:\Users\CSP>
```

- If the TTL value for a ping reply is between 35 and 64, it is a unix/linux host.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\CSP>ping www.microsoft.com

Pinging e13678.dspb.akamaiedge.net [23.67.3.108] with 32 bytes of data:
Reply from 23.67.3.108: bytes=32 time=236ms TTL=48
Reply from 23.67.3.108: bytes=32 time=235ms TTL=48
Reply from 23.67.3.108: bytes=32 time=235ms TTL=48
Reply from 23.67.3.108: bytes=32 time=235ms TTL=48

Ping statistics for 23.67.3.108:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 235ms, Maximum = 236ms, Average = 235ms

C:\Users\CSP>
```

The screenshot shows a Windows command prompt window with a blue title bar. The text inside shows the execution of a ping command to www.microsoft.com. The output displays four successful replies from IP address 23.67.3.108, each with a TTL of 48. A red circle highlights the TTL values in the four reply lines. Below the replies, the ping statistics are shown, indicating 4 packets sent and received with 0% loss, and round trip times ranging from 235ms to 236ms.

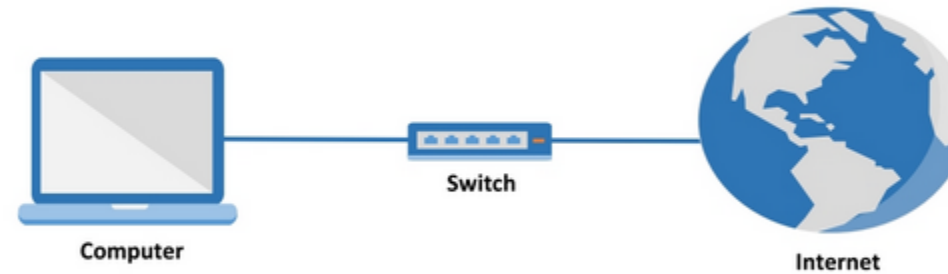
Tool : IP2country

IP2country is a small application that takes an IP or host and tells you in which country the IP is located.

- Start the **IP2country** application and give the IP address. It will tell you in which country the IP is located.



WEBSITE FOOTPRINTING



Pre-requisite:

- Computer installed with OS
- Internet Connection (Broadband, Dial-up)

Website Footprinting – Websites

- www.netcraft.com
- www.builtwith.com
- www.archive.org

Website Footprinting – Tools

- ID Serv

Website : www.netcraft.com

Netcraft.com provides web server and web hosting analysis, including web server and operating system detection. Depending on the queried server's operating system, their service is able to monitor uptimes, etc. for determining the reliability of a web hosting provider.

- Access www.netcraft.com from any web browser.



- Type the URL of the webserver whose information is to be found.



- It will display website details like website title, website description, keywords, site rank, etc.

Background

Site title	Microsoft - Official Home Page	Date first seen	August 1995
Site rank	1158	Primary language	English
Description	At Microsoft our mission and values are to help people and businesses throughout the world realise their full potential.		
Keywords	Not Present		
Netcraft Risk Rating [FAQ]	0/10		

- It will display IP address of the website, domain registrar details, owner of the domain name, website hosting company and country details.

Network

Site	http://www.microsoft.com	Netblock Owner	Akamai International, BV
Domain	microsoft.com	Nameserver	ns1.mft.net
IP address	23.200.101.224	DNS admin	martha@microsoft.com
IPv6 address	2a02:2400:71:20e::0:0:3f6e	Reverse DNS	a23-200-101-224.deploy.static.akamaitechnologies.com
Domain registrar	markmonitor.com	Nameserver organisation	whois.markmonitor.com
Organisation	Microsoft Corporation, One Microsoft Way, Redmond, 98052, United States	Hosting company	Akamai Technologies
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	unknown
Hosting country	NL	Latest Performance	Performance Graph

- It will also display hosting history details like different IP address / operating system used.

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.198.83.104	Linux	unknown	24-Jun-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.44.105.131	Linux	unknown	22-Jun-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.4.211.190	Linux	unknown	19-Jun-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.103.201.26	Linux	unknown	12-Jun-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.133.197	Linux	unknown	12-Jun-2018
Akamai	88.221.58.244	Linux	unknown	1-Jun-2018
Akamai	84.33.169.149	Linux	unknown	26-May-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.133.187	Linux	unknown	26-May-2018
Akamai	88.221.58.244	Linux	unknown	19-May-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.44.105.131	Linux	unknown	12-May-2018

