

Experiment 1: Reconnaissance and foot printing

-ESHAN SHENDE K027

Aim: To perform foot printing and reconnaissance for a given target of evaluation.

Learning Outcomes:

After completion of this experiment, student should be able to

1. Describe basic steps in hacking
2. Describe active and passive reconnaissance.
3. Use various tools and utilities for information gathering about target of evaluation.

Theory:

Steps in hacking: Figure 1 below indicates basic steps involved in hacking.



Figure 1: Basic Hacking Process

Reconnaissance refers to the preparatory phase where an attacker seeks to gather information about a target prior to launching an attack. Reconnaissance can be active or passive reconnaissance. *Passive reconnaissance* involves gathering information regarding a potential target without the targeted individual's or company's knowledge. *Active reconnaissance* involves probing the network to discover individual hosts, IP addresses, and services on the network. This usually involves more risk of detection than passive reconnaissance.

Scanning refers to the pre-attack phase when the attacker scans the network for specific information on the basis of information gathered during reconnaissance

Gaining access is the phase where the real hacking takes place. Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access.

Once a hacker has gained access, they want to keep that access for future exploitation and attacks.

Once hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action.

Footprinting is part of the preparatory pre-attack phase and involves accumulating data regarding a target's environment and architecture, usually for the purpose of finding ways to intrude into that environment. Footprinting can reveal system vulnerabilities and identify the ease with which they can be exploited. *Footprinting* is defined as the process of creating a blueprint or map of an organization's network and systems. Information gathering is also known as footprinting an organization. Footprinting begins by determining the target system, application, or physical location of the target. Once this information is known, specific information about the organization is gathered using nonintrusive methods.

Following tools and utilities can be used for information gathering

- *ping*
- *tracert*
- *nslookup*
- *whois*
- etc

Ping is a computer network administration utility used to test the reachability of a host on an IP network and to measure the round-trip time for messages sent from the originating host to a destination computer. Ping operates by sending ICMP *echo request* packets to the target host and waiting for an ICMP response. In the process it measures *round-trip time* and records any packet loss. The results of the test are printed in the form of a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times, and sometimes the standard deviation of the mean. Ping does not evaluate or compute the time to establish the connection; it only gives the mean round-trip times of an established connection with an open session.

Traceroute is a diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. The history of the route is recorded as the round-trip times of the packets received from each successive host (remote node) in the route (path); the sum of the mean times in each hop indicates the total time spent to establish the connection. Traceroute proceeds unless all (three) sent packets are lost more than twice, then the connection is lost and the route cannot be evaluated. Traceroute sends a sequence of three ICMP Echo Request packets addressed to a destination host. The time-to-live (TTL) value, also known as **hop limit**, is used in determining the intermediate routers being traversed towards the destination. Routers decrement packets' TTL value by 1 when routing and discard packets whose TTL value has reached zero, returning the ICMP error message ICMP Time Exceeded. Traceroute works by sending packets with gradually increasing TTL value, starting with TTL value of 1. The first router receives the packet, decrements the TTL value and drops the packet because it then has TTL value zero. The router sends an ICMP Time Exceeded message back to the source. The next set of packets are given a TTL value of 2, so the first router forwards the packets, but the second router drops them and replies with ICMP Time Exceeded. Proceeding in this way, traceroute uses the returned

ICMP Time Exceeded messages to build a list of routers that packets traverse, until the destination is reached and returns an ICMP Echo Reply message.

The timestamp values returned for each router along the path are the delay (latency) values, typically measured in milliseconds for each packet. On UNIX systems, such as FreeBSD or Linux, it is available as a `traceroute` command in a terminal. On Microsoft Windows, it is named **tracert**. For IPv6 the tool sometimes has the name **traceroute6** or **tracert6**.

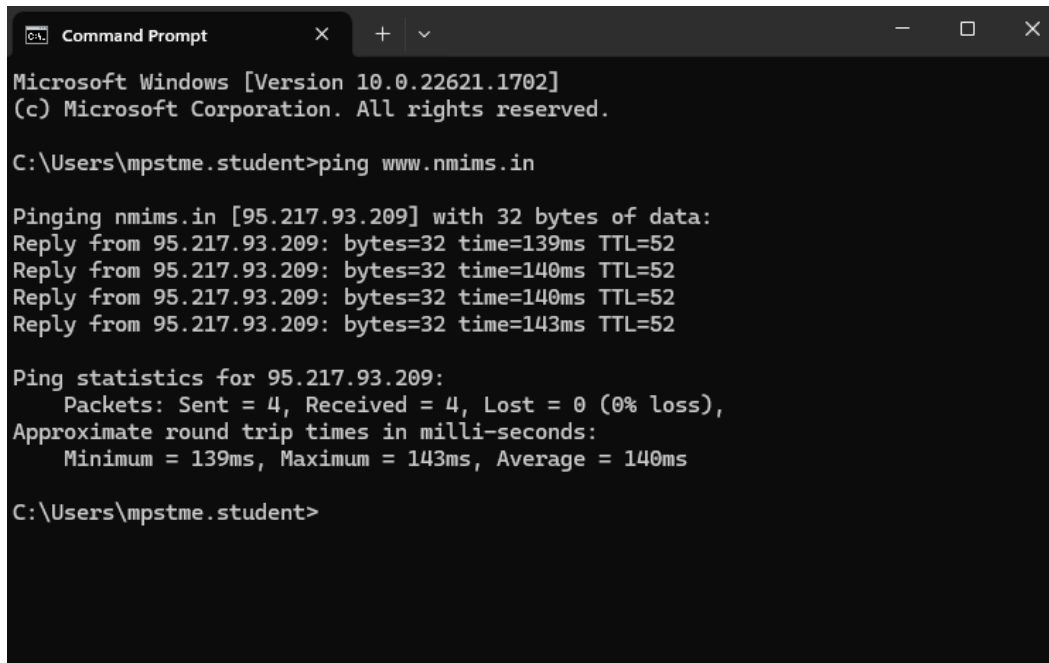
nslookup is a network administration command-line tool available for many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record. nslookup operates in interactive or non-interactive mode. When used interactively by invoking it without arguments or when the first argument is - (minus sign) and the second argument is a host name or Internet address of a name server, the user issues parameter configurations or requests when presented with the nslookup prompt (>). When no arguments are given, then the command queries the default server. The - (minus sign) invokes subcommands which are specified on the command line and should precede nslookup commands. In non-interactive mode, i.e. when the first argument is a name or Internet address of the host being searched, parameters and the query are specified as command line arguments in the invocation of the program. The non interactive mode searches the information for a specified host using the default name server.

WHOIS is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format.

Procedure:

Task 1: Finding IP address

1. On command prompt, read online help for ping using ping /?
2. Use *ping* to find the IP address of the target. Note the IP address and RTT.



```
Command Prompt
Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Users\mpstme.student>ping www.nmims.in

Pinging nmims.in [95.217.93.209] with 32 bytes of data:
Reply from 95.217.93.209: bytes=32 time=139ms TTL=52
Reply from 95.217.93.209: bytes=32 time=140ms TTL=52
Reply from 95.217.93.209: bytes=32 time=140ms TTL=52
Reply from 95.217.93.209: bytes=32 time=143ms TTL=52

Ping statistics for 95.217.93.209:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 139ms, Maximum = 143ms, Average = 140ms

C:\Users\mpstme.student>
```

Task 2: Finding maximum Frame Size

1. Use the command ping with -f and -l options as shown in figure 1 below.

```
C:\Users\mpstme.student>ping www.nmims.in -f -l 1500

Pinging nmims.in [95.217.93.209] 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 95.217.93.209:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\mpstme.student>
```

```
C:\Windows\system32\cmd.exe

-j host-list      Loose source route along host-list (IPv4-only).
-k host-list      Strict source route along host-list (IPv4-only).
-w timeout        Timeout in milliseconds to wait for each reply.
-R               Use routing header to test reverse route also (IPv6-only).
-S srcaddr        Source address to use.
-4               Force using IPv4.
-6               Force using IPv6.

C:\Users\pintu.shah>ping www.nmims.edu -f -l 1500

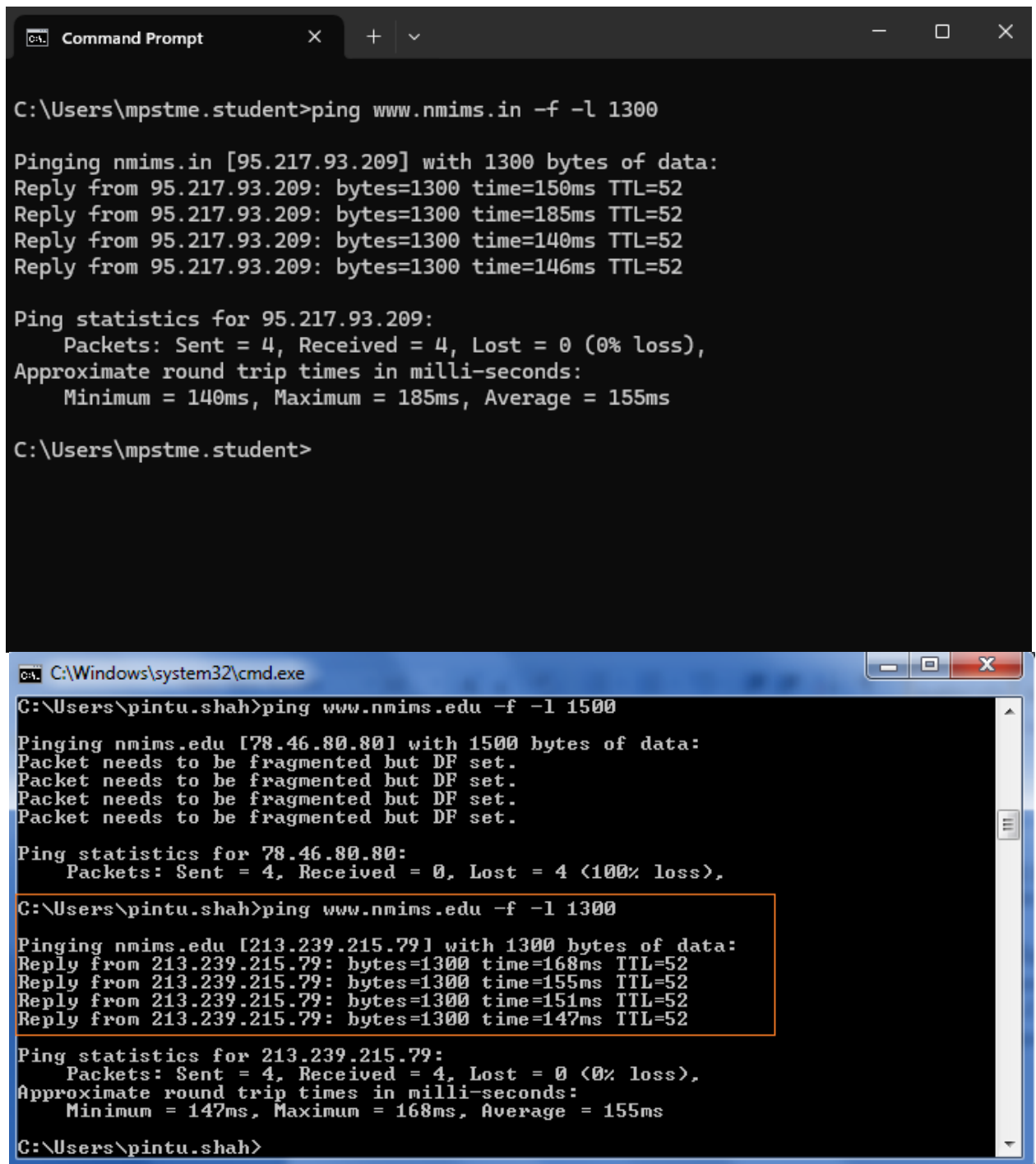
Pinging nmims.edu [78.46.80.80] with 1500 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 78.46.80.80:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\pintu.shah>
```

Figure 1: finding maximum frame size

2. The display **Packet needs to be fragmented but DF** set means that the frame is too large to be on the network and needs to be fragmented. Since we used -f switch with the ping command, the packet was not sent, and the ping command returned this error.
3. Try using size of 1300 as shown in figure 2.



The image contains two screenshots of Windows Command Prompt windows. The top window, titled 'Command Prompt', shows a user running a ping command to 'www.nmims.in' with a packet size of 1300 bytes. The output shows four successful replies with varying round-trip times (150ms, 185ms, 140ms, 146ms) and a TTL of 52. Ping statistics indicate 0% loss. The bottom window, titled 'C:\Windows\system32\cmd.exe', shows a user running a ping command to 'www.nmims.edu' with a packet size of 1500 bytes. The output shows four failed replies with the message 'Packet needs to be fragmented but DF set.' and a 100% loss. Below this, the user runs the same command with a packet size of 1300 bytes, which shows four successful replies with round-trip times (168ms, 155ms, 151ms, 147ms) and a TTL of 52. Ping statistics indicate 0% loss. A yellow rectangular box highlights the successful ping results for the 1300-byte packet size in the bottom window.

```
C:\Users\mpstme.student>ping www.nmims.in -f -l 1300

Pinging nmims.in [95.217.93.209] with 1300 bytes of data:
Reply from 95.217.93.209: bytes=1300 time=150ms TTL=52
Reply from 95.217.93.209: bytes=1300 time=185ms TTL=52
Reply from 95.217.93.209: bytes=1300 time=140ms TTL=52
Reply from 95.217.93.209: bytes=1300 time=146ms TTL=52

Ping statistics for 95.217.93.209:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 140ms, Maximum = 185ms, Average = 155ms

C:\Users\mpstme.student>
```

```
C:\Users\pintu.shah>ping www.nmims.edu -f -l 1500

Pinging nmims.edu [78.46.80.80] 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 78.46.80.80:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\pintu.shah>ping www.nmims.edu -f -l 1300

Pinging nmims.edu [213.239.215.79] with 1300 bytes of data:
Reply from 213.239.215.79: bytes=1300 time=168ms TTL=52
Reply from 213.239.215.79: bytes=1300 time=155ms TTL=52
Reply from 213.239.215.79: bytes=1300 time=151ms TTL=52
Reply from 213.239.215.79: bytes=1300 time=147ms TTL=52

Ping statistics for 213.239.215.79:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 147ms, Maximum = 168ms, Average = 155ms

C:\Users\pintu.shah>
```

Figure 2: ping using size of 1300 bytes

4. Since ping is successful, we can see that the maximum packet size is less than 1500 bytes and more than 1300 bytes
5. Try with different sizes to find maximum frame size. Note the maximum size.

```
Command Prompt
C:\Users\mpstme.student>ping www.nmims.in -f -l 1472

Pinging nmims.in [95.217.93.209] with 1472 bytes of data:
Reply from 95.217.93.209: bytes=1472 time=180ms TTL=52
Reply from 95.217.93.209: bytes=1472 time=228ms TTL=52
Reply from 95.217.93.209: bytes=1472 time=155ms TTL=52
Reply from 95.217.93.209: bytes=1472 time=159ms TTL=52

Ping statistics for 95.217.93.209:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 155ms, Maximum = 228ms, Average = 180ms

C:\Users\mpstme.student>ping www.nmims.in -f -l 1473

Pinging nmims.in [95.217.93.209] with 1473 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 95.217.93.209:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\mpstme.student>
```

Packet Size : 1472

Task 3: Trace route to the target using tracert

1. Execute command tracert www.nmims.edu from command prompt.
2. Analyze the output
3. Note the number of hops required to reach the destination.

Total hops : 15

```
Command Prompt
tracert www.nmims.edu

Tracing route to www.nmims.edu [95.217.93.209]
over a maximum of 30 hops:

  1  <1 ms  <1 ms  <1 ms  10.125.145.1
  2   1 ms   2 ms  11 ms  10.125.138.1
  3   1 ms  <1 ms  <1 ms  mumbaicampus.svkm.ac.in [10.0.1.9]
  4   2 ms   2 ms   2 ms  115.242.5.145
  5   *      *      *      Request timed out.
  6   4 ms   4 ms  10 ms  103.198.140.60
  7  122 ms  122 ms  123 ms  103.198.140.81
  8  121 ms  119 ms  118 ms  ae15-0.fra20.core-backbone.com [5.56.20.229]
  9  133 ms  133 ms  135 ms  ae1-2081.sth10.core-backbone.com [80.255.14.194]

 10  139 ms  139 ms  148 ms  core-backbone.hetzner.com [80.255.15.126]
 11  146 ms  146 ms  145 ms  core53.sto.hetzner.com [213.239.252.73]
 12  139 ms  139 ms  140 ms  core31.hel1.hetzner.com [213.239.254.61]
 13  138 ms  138 ms  137 ms  ex9k2.dc2.hel1.hetzner.com [213.239.224.142]
 14  144 ms  144 ms  144 ms  nmedu.privatelabelhosts.com [95.216.243.20]
 15  147 ms  140 ms  139 ms  vps2.nmims.edu [95.217.93.209]

Trace complete.
```


Task 4: Using nslookup to find domain related information

1. Execute nslookup from command prompt in interactive mode.
2. Collect and note following information using nslookup.
 - a. Authoritative server
 - b. Non authoritative server
 - c. CNAME
 - d. Mail server information

```
Command Prompt

C:\Users\mpstme.student>nslookup www.google.com
Server: MUMDC-PRIM.SVKMGRP.COM
Address: 192.168.2.51

Non-authoritative answer:
Name: www.google.com
Addresses: 2404:6800:4009:827::2004
           142.250.192.4

C:\Users\mpstme.student>
```

```
Command Prompt

C:\Users\mpstme.student>nslookup www.nmims.edu
Server: MUMDC-PRIM.SVKMGRP.COM
Address: 192.168.2.51

Name: www.nmims.edu
Address: 95.217.93.209

C:\Users\mpstme.student>
```

Task 5: Analyzing domain and IP address queries using whois

1. Use whois utility available at www.dnsstuff.com.
2. Collect and note following information related to do domain
 - a. Registrant of domain NMIMS
 - b. Date of registration of domain 14-1-1998
 - c. Date of expiry of domain 31-7-25
 - d. Name servers ns.awareindia.com
 - e. Administrative contact details Pankaj Jaiswal
 - f. Technical contact details Pankaj Jaiswal

nmims.edu

whois information

Whois

RDAP

DNS Records

Diagnostics

cache expires in 29 days, 4 hours, 19 minutes and 23 seconds

Registrar Info

Name	Educause
Whois Server	whois.educause.net
Referral URL	http://www.educause.edu/edudomain
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Important Dates

Expires On	2025-07-31
Registered On	1998-01-14
Updated On	2022-07-15

Name Servers

ns.awareindia.com	185.136.96.15
ns1.awareindia.com	185.136.97.15

Similar Domains

nmims-assignment.com | nmims-assignments.com | nmims-assignments.xyz | nmims-bankonit.com | nmims-corporate.org | nmims-intuito.org | nmims-mpit.ac.in | nmims-paragana.com | nmims-perf.org | nmims-retail.com | nmims-solved-assignment.com | nmims.ac.in | nmims.co | nmims.college | nmims.com | nmims.digital | nmims.edu | nmims.edu.in | nmims.education | nmims.eu |

Registrar Data

[Make Private Now](#)

We will display stored WHOIS data for up to 30 days.

This Registry database contains ONLY .EDU domains.
The data in the EDUCAUSE Whois database is provided
by EDUCAUSE for information purposes in order to
assist in the process of obtaining information about
or related to .edu domain registration records.

The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: <http://whois.educause.edu>

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail. The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.

Domain Name: NMIMS.EDU

Registrant:

Narsee Monjee Institute of Management
Juhu Vile Parle Development
Scheme Vile Parle (West)
Mumbai, Maharashtra 400 058
India

Administrative Contact:

Pankaj Jainwal
Dotcom Service India Pvt. Ltd.
101/102 Tirupati Udyog Premises Opp Petrol Pump
I.B.Patel Road Goregaon East
Mumbai, Maharashtra 400063
India
+91.2226855700
uhs@actarhonoridindia.com

Technical Contact:

Pankaj Jainwal
Dotcom Service India Pvt. Ltd.
101/102 Tirupati Udyog Premises Opp Petrol Pump
I.B.Patel Road Goregaon East
Mumbai, Maharashtra 400063
India
+91.2226855700
uhs@actarhonoridindia.com

Name Servers:

NS.AWAREINDIA.COM
NS1.AWAREINDIA.COM

Domain record activated: 14-Jan-1998

Domain record last updated: 15-Jul-2022

Domain expires: 31-Jul-2025

Information Updated: 2025-01-07 07:50:07.595467+00

Whois IP 115.242.5.145

Updated 1 second ago

```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '115.240.0.0 - 115.247.255.255'

% Abuse contact for '115.240.0.0 - 115.247.255.255' is 'ip.abuse@ril.com'

inetnum:        115.240.0.0 - 115.247.255.255
netname:        RELIANCEJIO-IN
descr:          Reliance Jio Infocomm Limited
country:        IN
org:            ORG-RJIL1-AP
admin-c:        RJIL1-AP
tech-c:         RJIL1-AP
abuse-c:        AR1022-AP
status:         ALLOCATED PORTABLE
remarks:        -----
remarks:        To report network abuse, please contact mnt-irt
remarks:        For troubleshooting, please contact tech-c and admin-c
remarks:        Report invalid contact via www.apnic.net/invalidcontact
remarks:        -----
mnt-by:         APNIC-HM
mnt-lower:      MAINT-IN-RELIANCEJIO
mnt-routes:     MAINT-IN-RELIANCEJIO
mnt-irt:        IRT-RELIANCEJIO-IN
last-modified:  2020-08-19T13:07:29Z
source:         APNIC

irt:            IRT-RELIANCEJIO-IN
address:        Reliance JIO INFOCOMM LTD GHANSOLI INDIA
e-mail:         ip.abuse@ril.com
abuse-mailbox:  ip.abuse@ril.com
admin-c:        IBSP1-AP
tech-c:         IBSP1-AP
auth:          # Filtered
remarks:        ip.abuse@ril.com was validated on 2024-12-28
mnt-by:        MAINT-IN-RELIANCEJIO
last-modified:  2024-12-28T12:49:10Z
```

1. Open google.com
intitle:

Example: `intitle:login` → Finds pages with "login" in the title.

Searches for all specified keywords in the page title.

inurl:

Example: `inurl:admin` → Finds URLs containing "admin".

Searches for all specified keywords in the URL.

cache:

Example: `cache:example.com` → Shows the cached version of `example.com`.

The screenshot shows a web browser window with a Google search for 'inurl:password filetype:xls'. The search results list several links, including 'password Acqui BED', 'password form', and 'Forgot Password - Google Groups'. The right side of the image displays an Excel spreadsheet titled 'Default Password List'. The spreadsheet contains a table with columns: Manufacturer, Product, Revision, Protocol, User ID, Password, Access, comment, Validated, and LastMod. The table lists various network devices and their default credentials, such as CoreBuilder, HPwARC, LANtivity, and UniSwitch.

Search Results:

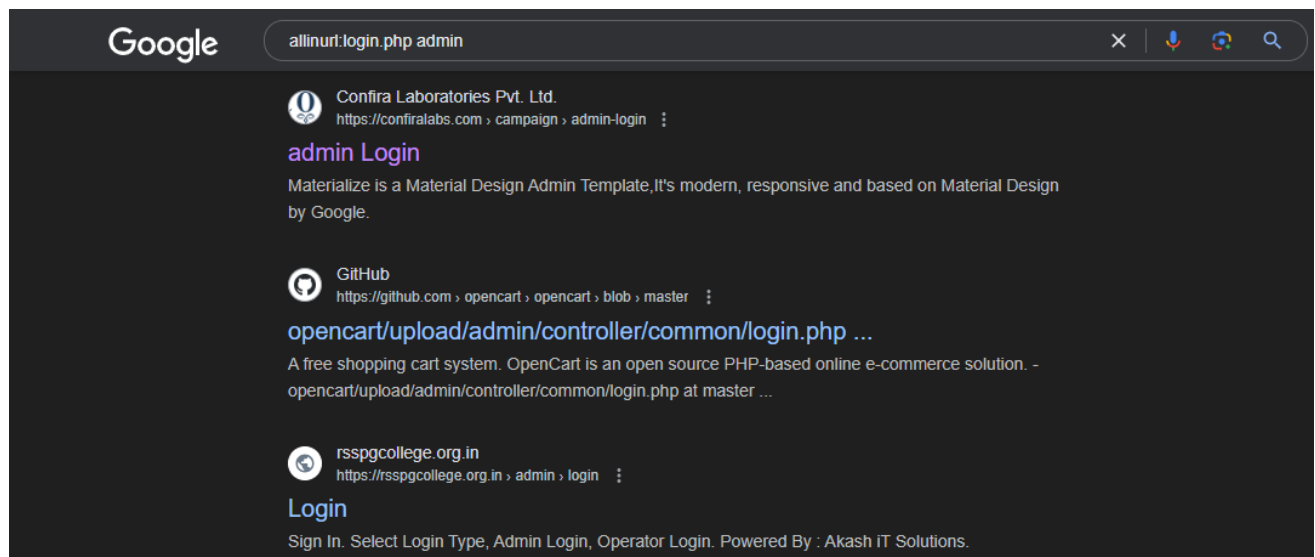
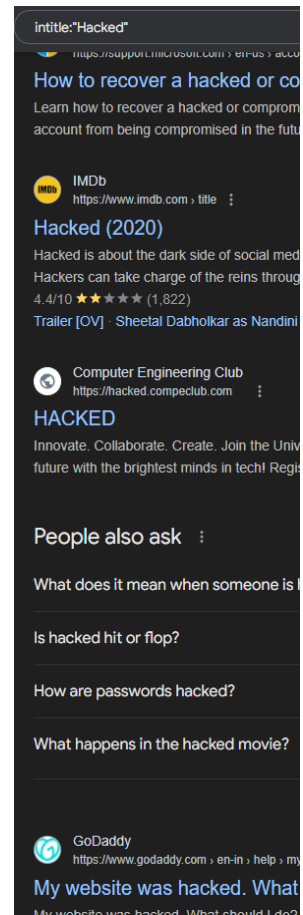
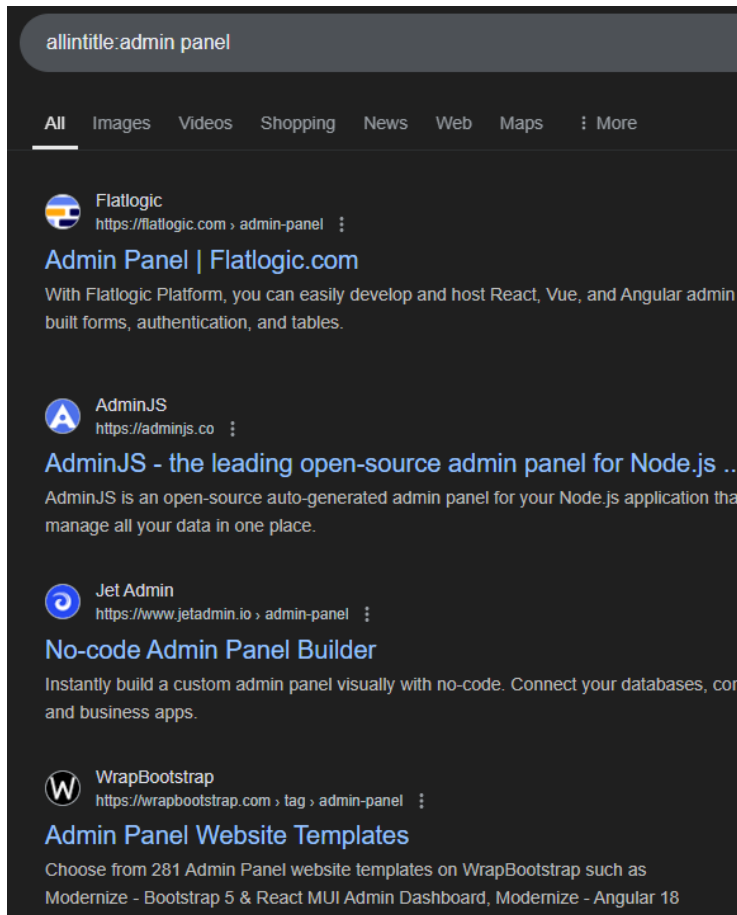
- scrt cg
https://www.scrt.cg.gov.in/pdf/BED2017-18 [XLS]
- password Acqui BED
- OrGrid.com
https://forum.acgrid.com/t/1112764-password-f [XLS]
- password form
- Google
https://googlegroups.com/group/metro/attach [XLS]
- Forgot Password - Google Groups
- UMass Boston
https://password.umb.edu/academics/pdf/AC... [XLS]
- Academic Program Change Approval Form
- straxo.com
https://www.straxo.com/excel/password [XLS]
- Sheet1 - Excel Password Remover
- Andrea Dekker
https://andradekker.com/uploads/2011/03 [XLS]
- Credit Cards & Money Accounts
- protecus.de
https://board.protecus.de/download/t21760... [XLS]
- Default Password List - Protecus Security Forum
- University of Nebraska
https://engineering.unl.edu/employee-resources [XLS]

Excel Spreadsheet: Default Password List

Stand: 14.05.2006 - Quelle: http://www.phenoelit.de/pldpl.html

	Manufacturer	Product	Revision	Protocol	User ID	Password	Access	comment	Validated	Created	LastMod
3	3COM	CoreBuilder	500/2500 7000/6000/3	Telnet	debug	synnet			No	10-01-2002	2005-13-7
4	3COM	CoreBuilder	500/2500	Telnet	tech	tech			No	10-01-2002	2005-13-7
5	3COM	HPwARC	v4.1.x	Telnet	admin	(none)			No	10-01-2002	2005-13-7
6	3COM	LANtivity	2500	Telnet	debug	synnet			No	10-01-2002	2005-13-7
7	3COM	LANtivity	2500	Telnet	tech	tech			No	10-01-2002	2005-13-7
8	3COM	LANtivity	2500	Telnet	tech	tech			No	10-01-2002	2005-13-7
9	3COM	UniSwitch	2000/2700	Telnet	tech	tech			No	10-01-2002	2005-13-7
10	3COM	NetBuilder		SNMP		ANYCOM	snmp-read		No	10-01-2002	2005-13-7
11	3COM	NetBuilder		SNMP		ILLMI	snmp-read		No	10-01-2002	2005-13-7
12	3COM	NetBuilder		Multi	admin	(none)	Admin		No	10-01-2002	2005-13-7
13	3COM	Connect ISDN Routers	5x0	Telnet	n/a	PASSWORD	Admin		No	10-01-2002	2005-13-7
14	3COM	SuperStack II Switch	2200	Telnet	debug	synnet			No	10-01-2002	2005-13-7
15	3COM	SuperStack II Switch	2700	Telnet	tech	tech			No	10-01-2002	2005-13-7
16	3COM	OfficeConnect 812 ADSL		Multi	adminmt	adminmt	Admin		No	10-01-2002	2005-13-7

3. Similarly explore google dorks like intitle, allinurl, cache, allintitle etc.



Review questions:

1. **How does tracer (trace route) find the route that the trace packets are (probably) using?**

Tracer uses ICMP Echo Request packets to map the path from the source to the destination. It starts by setting the TTL (Time-To-Live) field in the packet header to 1. As the packet traverses the network, each router decrements the TTL by 1. When TTL reaches 0 at an intermediate router, the router discards the packet and sends an ICMP Time Exceeded message back to the source. Tracer increases TTL incrementally for subsequent packets, recording each hop (router) until the destination replies with an ICMP Echo Reply. The times recorded for these responses provide insights into network latency and routing paths.

2. **We saw before:**

- a. **Request timed out**
- b. **Packet needs to be fragmented but DF set**
- c. **Reply from XXX.XXX.XXX.XXX: TTL expired in transit**

What ICMP type and code are used for the ICMP Echo request?

Explanation of Specific ICMP Messages:

- **Request timed out:**
This message indicates no ICMP response was received within the timeout period. It could happen if the target host is unreachable, intermediate routers drop packets, or a firewall blocks ICMP traffic.
- **Packet needs to be fragmented but DF set:**
This occurs when the packet size exceeds the Maximum Transmission Unit (MTU) of the network, and the DF (Don't Fragment) flag prevents the packet from being split into smaller fragments. Adjusting the packet size can resolve this error.
- **TTL expired in transit:**
Routers discard packets when their TTL reaches zero, and an ICMP Time Exceeded message is sent back to the source. This mechanism prevents packets from endlessly circulating in the network.

What ICMP type and code are used for the ICMP Echo request

- **Type 8 (Echo Request):** Used to initiate a ping operation or tracer.
- **Code 0:** Specifies no additional information about the request.

3. Analyze and determine each of the following DNS resource records:

- SOA
- NS
- A
- AAAA
- PTR
- CNAME
- MX
- SRV

SOA (Start of Authority) Record

The SOA record is the cornerstone of a DNS zone file, providing critical information about the domain's administration and functioning. It specifies which server is the authoritative source for the domain's DNS records and includes the administrator's contact email. The SOA also contains important timing parameters: the serial number, which is updated whenever the zone file changes, and intervals for refreshing, retrying, and expiring zone data. These parameters dictate how secondary (slave) DNS servers synchronize with the primary (master) server, ensuring data consistency and proper functioning across the network.

NS (Name Server) Record

NS records define the DNS servers responsible for a domain or subdomain, enabling proper resolution of domain names into IP addresses. Each domain can have multiple NS records to provide redundancy and enhance reliability. These records delegate authority over the domain, directing queries to the specified servers. For example, if a domain has NS records pointing to ns1.example.com and ns2.example.com, DNS queries for that domain will be resolved using these servers, ensuring that the domain remains accessible even if one server is down.

A (Address) Record

A records are the most commonly used DNS records, mapping a domain name to an IPv4 address. This translation allows users to access websites using human-readable names instead of numerical IP addresses. A single domain can have multiple A records, enabling load balancing by distributing traffic across multiple servers. For instance, if a website uses multiple servers for scalability, its A records will direct traffic to different IP addresses, ensuring smoother performance and high availability.

AAAA (IPv6 Address) Record

AAAA records perform the same function as A records but for IPv6 addresses. With the increasing adoption of IPv6 due to the exhaustion of IPv4 addresses, these records are becoming more important. They map domain names to 128-bit IPv6 addresses, supporting a vastly larger pool of IP addresses compared to

IPv4. This is crucial for future-proofing internet infrastructure, enabling devices and services to communicate seamlessly in a growing digital landscape.

PTR (Pointer) Record

PTR records are used for reverse DNS lookups, which are the opposite of regular DNS queries. Instead of translating a domain name into an IP address, PTR records map an IP address back to a domain name. They are primarily used for verification purposes, such as email server validation, where the server's identity is confirmed by ensuring its IP address maps back to the expected domain. These records are stored in special reverse lookup zones, such as in-addr.arpa for IPv4 and ip6.arpa for IPv6.

CNAME (Canonical Name) Record

CNAME records allow one domain to act as an alias for another domain. This is useful for redirecting traffic or managing multiple domain names that point to the same resource. For instance, a company might use `www.example.com` as an alias for `example.com`. The CNAME record ensures that all queries to the alias are resolved to the target domain's IP address. However, CNAME records cannot coexist with other records for the same domain, which is a limitation that must be considered during configuration.

MX (Mail Exchange) Record

MX records direct email traffic by specifying the mail servers responsible for receiving emails for a domain. Each MX record includes a priority value, with lower numbers indicating higher priority. This allows email systems to try servers in order of priority, ensuring that messages are delivered even if a preferred server is unavailable. For example, if a domain has two MX records with priorities 10 and 20, email systems will first attempt to deliver messages to the server with priority 10 and use the second server only as a fallback.

SRV (Service) Record

SRV records are used to specify the location of servers providing specific services, such as SIP (used in VoIP) or LDAP (used for directory services). These records include detailed parameters such as the service name, protocol (TCP or UDP), priority, weight (for load balancing), port, and target server. For example, a VoIP service might have an SRV record indicating the hostname and port of the server handling calls. This flexibility makes SRV records ideal for complex setups where multiple servers provide similar services.

4. Evaluate the difference between an authoritative and non-authoritative answer.

- **Authoritative Answer:**

- This type of DNS response is provided by a DNS server that has direct authority over the queried domain.
- These servers store the original DNS records created and managed by the domain owner.
- For example, if you query "example.com" and the authoritative server for that domain responds, the data is guaranteed to be accurate and up-to-date.
- Authoritative servers are part of the DNS hierarchy, including root servers, top-level domain (TLD) servers (e.g., .com, .org), and the domain's own DNS servers.

- **Non-Authoritative Answer:**

- This response comes from a caching or recursive DNS server that has retrieved and temporarily stored the DNS data from an authoritative server.
- It is useful for efficiency, as it reduces the need to query authoritative servers repeatedly for the same domain.
- However, if the cached record has not been updated after changes to the authoritative records, it may lead to stale or outdated information.
- For example, when you perform a DNS lookup, your ISP's DNS server might provide a non-authoritative answer based on previously cached data.

PTO

5. Determine when you will receive request time out in nslookup?

A request timeout happens when nslookup does not receive a response within a specified time limit. Common reasons include:

- 1. Slow or Unresponsive DNS Server:**
 - The DNS server may be overloaded, down, or experiencing network issues.
- 2. Nonexistent or Expired Domain:**
 - If the queried domain name is invalid, expired, or not registered, the DNS server cannot resolve it, leading to a timeout.
- 3. Network Connectivity Problems:**
 - Firewalls or network configurations may block the DNS query, preventing communication with the DNS server.
- 4. Incorrect DNS Settings:**
 - If the client system's DNS configuration points to an invalid or unreachable DNS server, nslookup cannot receive a response.

6. Why do you get Connection timed out or Connection failed errors when using whois?

WHOIS errors occur due to several potential issues:

- 1. Unreachable or Overloaded WHOIS Server:**
 - WHOIS servers may be temporarily unavailable due to maintenance, high traffic, or server-side issues.
- 2. Network Restrictions (e.g., Firewalls):**
 - Certain networks or ISPs block WHOIS queries as a security measure, preventing access to the data.
- 3. Misconfigured Client or Server Settings:**
 - An incorrect WHOIS client configuration or a server not responding on the expected port can lead to failures.
- 4. Domain Lacks a WHOIS Record:**
 - Newly created domains may not yet have WHOIS information available. Similarly, queries for invalid domains or IP blocks may return errors.

7. What do you understand by Google dorks?

Google dorks are advanced search operators that use Google's indexing power to uncover specific, often sensitive, information. These queries are used in cybersecurity for reconnaissance, penetration testing, and identifying vulnerabilities in systems. They can also inadvertently expose misconfigurations or leaked data.

Key operators include:

1. **intitle:**
 - Searches for specific keywords in the HTML title of web pages.
 - Example: `intitle:login` identifies pages with "login" in their title, often leading to login portals.
2. **allintitle:**
 - Searches for multiple keywords in the page title.
 - Example: `allintitle:admin panel` finds pages with both "admin" and "panel" in the title.
3. **inurl:**
 - Locates pages with specific words in their URL.
 - Example: `inurl:admin` finds URLs containing "admin," often leading to administrative sections of websites.
4. **allinurl:**
 - Searches for multiple keywords in the URL.
 - Example: `allinurl:login admin` finds URLs containing both "login" and "admin."
5. **filetype:**
 - Filters results by specific file types.
 - Example: `filetype:pdf` finds PDF files. Queries like `filetype:xls inurl:password` can reveal spreadsheets with sensitive data.
6. **cache:**
 - Displays Google's cached version of a webpage, showing its state when last indexed.
 - Example: `cache:example.com` retrieves the snapshot of `example.com`.

Significance of Google Dorks

- Google dorks allow cybersecurity professionals to uncover misconfigured systems, weak security practices, or inadvertently exposed sensitive information.
- Malicious attackers can also use these techniques to identify vulnerabilities, such as exposed login portals, sensitive files, and improperly secured directories.
- Proper system configuration and regular security audits are essential to mitigate risks arising from such queries.

