Name: Ashriya

Date:2/3/2023

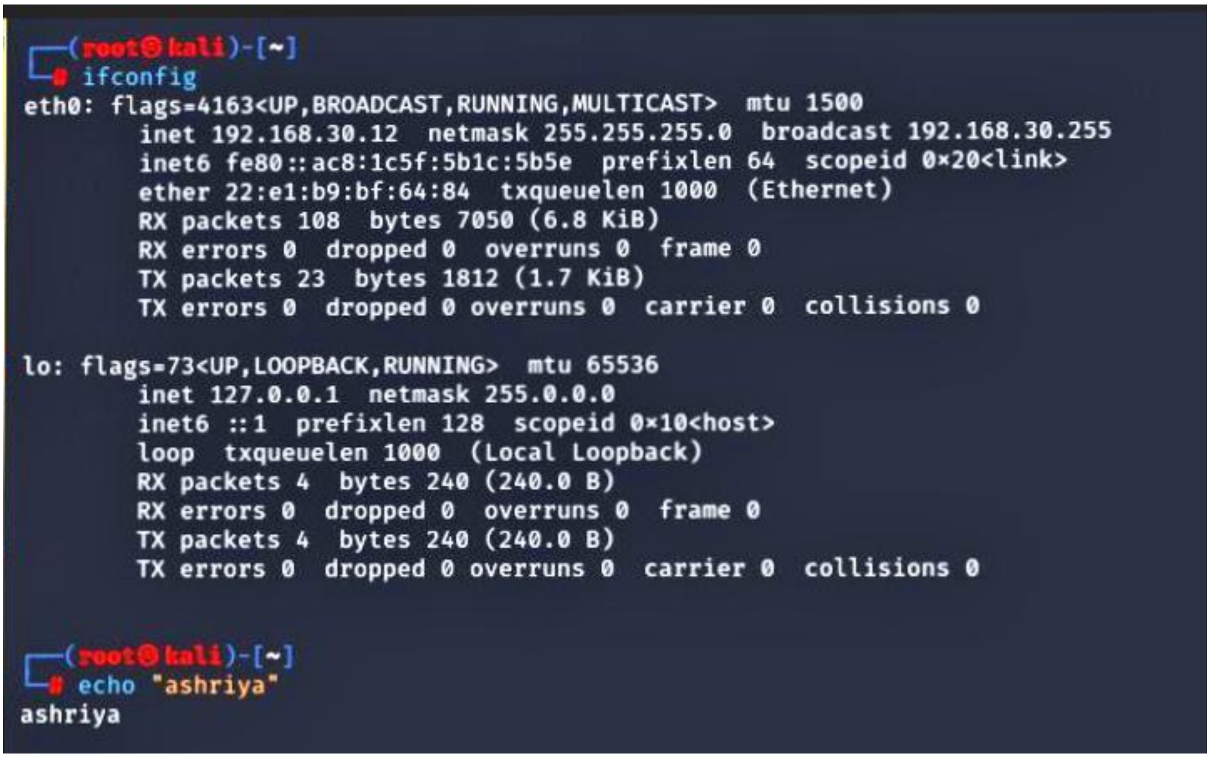
Task:2

1. Perform IP address spoofing

IP address spoofing is the act of falsifying the content in the Source IP header, usually with 6randomized numbers, either to mask the sender's identity or to launch a reflected DDoS attack, as described below.Name

Command:

```
$ ifconfig eth0 192.168.29.12
$ ifconfig
```



```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.30.12  netmask 255.255.255.0  broadcast 192.168.30.255
        inet6 fe80::ac8:1c5f:5b1c:5b5e  prefixlen 64  scopeid 0x20<link>
        ether 22:e1:b9:bf:64:84  txqueuelen 1000  (Ethernet)
        RX packets 108  bytes 7050 (6.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 1812 (1.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[~]
└─# echo "ashriya"
ashriya
```

2.MAC address spoofing

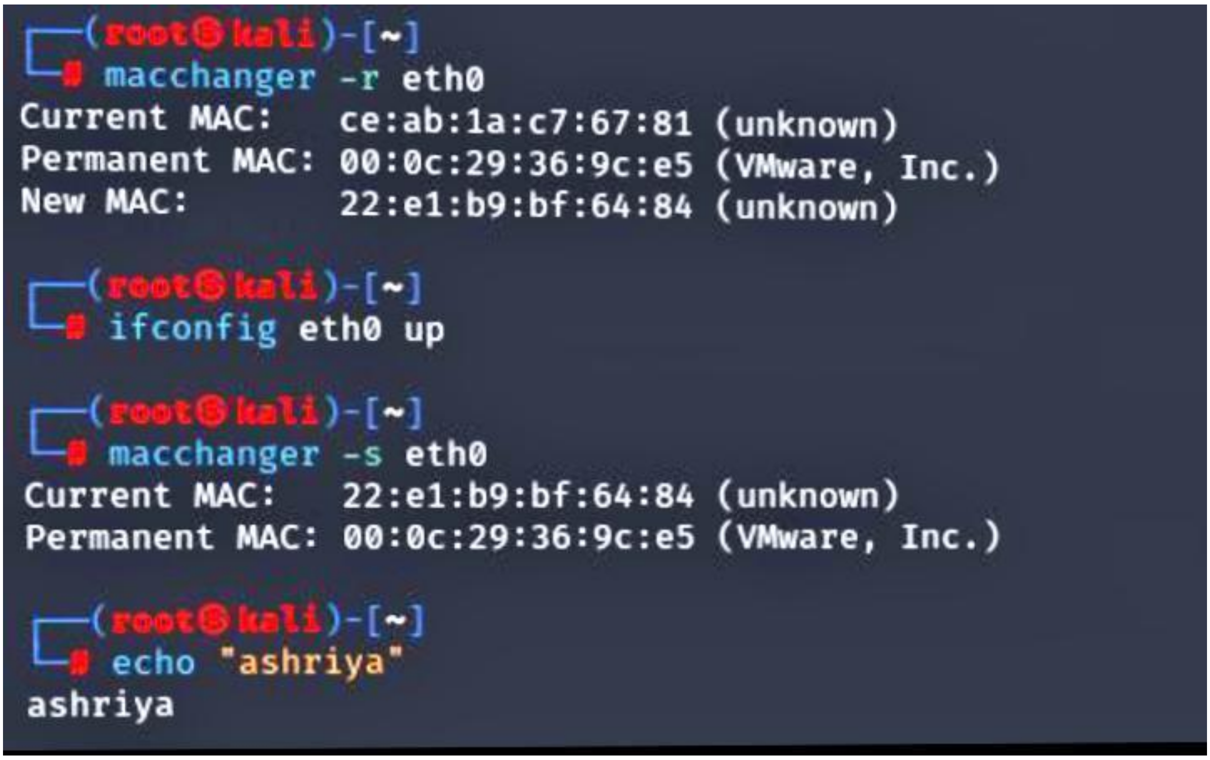
MAC Spoofing is a type of attack used to exploit flaws in the authentication mechanism implemented by wired and wireless networking hardware. In layman’s terms, MAC spoofing is when someone or something intercepts, manipulate or otherwise tampers with the control messages exchanged between a networked device and its unique MAC address.

Command:

$ macchanger -r eth0

$ ifconfig eth0 up

$ macchanger –s eth0



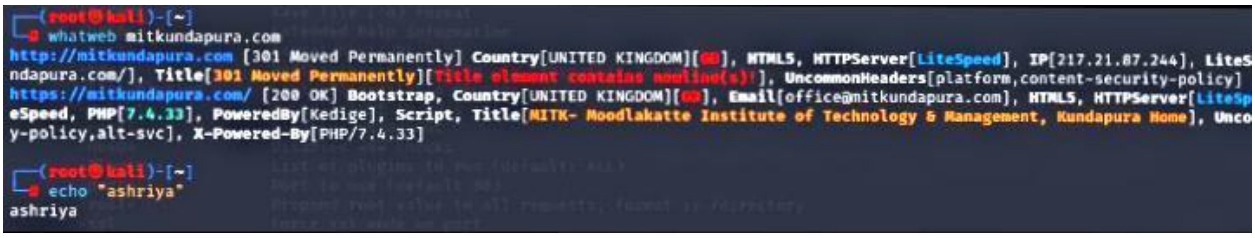
```
┌──(root㉿kali)-[~]
└─# macchanger -r eth0
Current MAC:   ce:ab:1a:c7:67:81 (unknown)
Permanent MAC: 00:0c:29:36:9c:e5 (VMware, Inc.)
New MAC:       22:e1:b9:bf:64:84 (unknown)

┌──(root㉿kali)-[~]
└─# ifconfig eth0 up

┌──(root㉿kali)-[~]
└─# macchanger -s eth0
Current MAC:   22:e1:b9:bf:64:84 (unknown)
Permanent MAC: 00:0c:29:36:9c:e5 (VMware, Inc.)

┌──(root㉿kali)-[~]
└─# echo "ashriya"
ashriya
```

3.Whatweb

The WhatWeb tool is used to identify different web technologies used by the website. It is included in Kali Linux, and it can be accessed by going to Applications | 03 – Web Application Analysis | Web Vulnerability scanners.

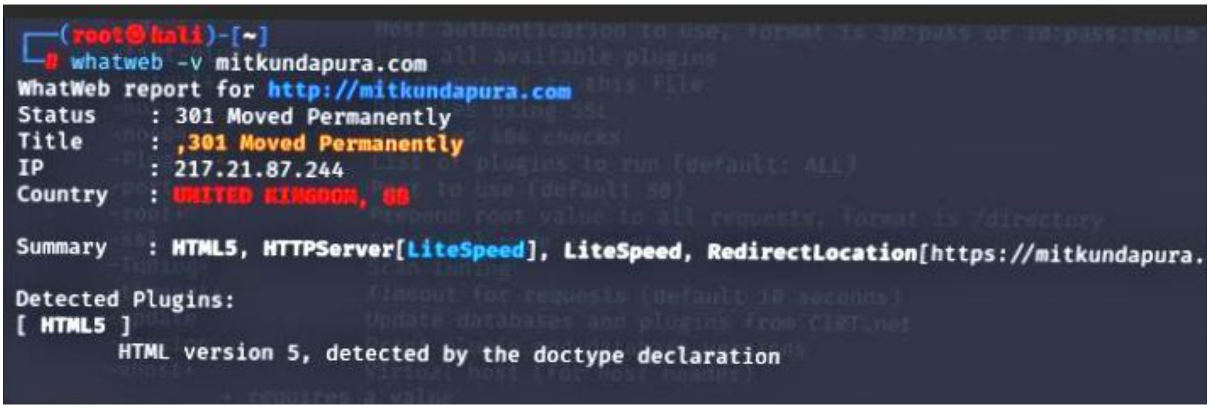
Command:

$ whatweb mitkundapura.com



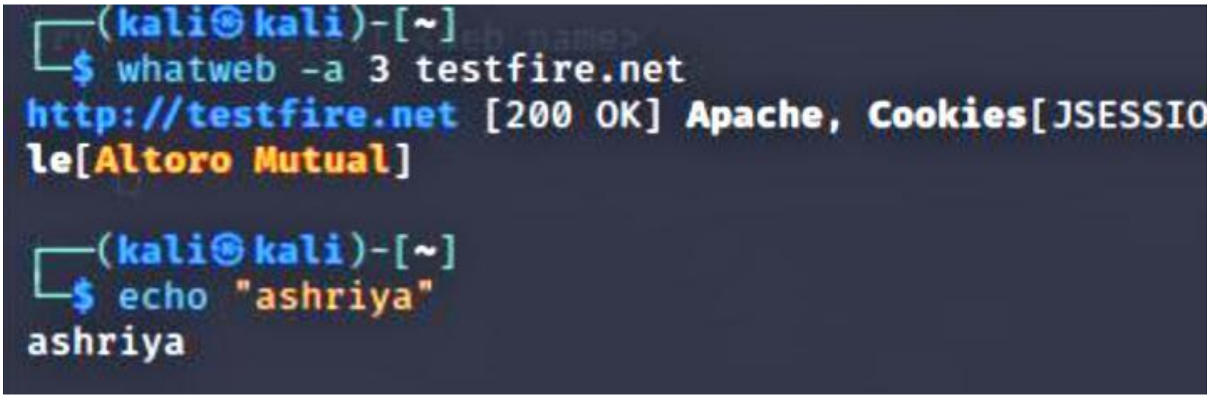
```
┌──(root㉿kali)-[~]
└─# whatweb mitkundapura.com
http://mitkundapura.com [301 Moved Permanently] Country[UNITED KINGDOM][GB], HTML5, HTTPServer[LiteSpeed], IP[217.21.87.244], LiteS
ndapura.com/], Title[301 Moved Permanently][Title element contains newline(s)!], UncommonHeaders[platform,content-security-policy]
https://mitkundapura.com/ [200 OK] Bootstrap, Country[UNITED KINGDOM][GB], Email[office@mitkundapura.com], HTML5, HTTPServer[LiteSp
eSpeed, PHP[7.4.33], PoweredBy[Kedige], Script, Title[MITK- Moodlakatte Institute of Technology & Management, Kundapura Home], Unco
y-policy,alt-svc], X-Powered-By[PHP/7.4.33]

┌──(root㉿kali)-[~]
└─# echo "ashriya"
ashriya
```

$ whatweb -v mitkundapura.com



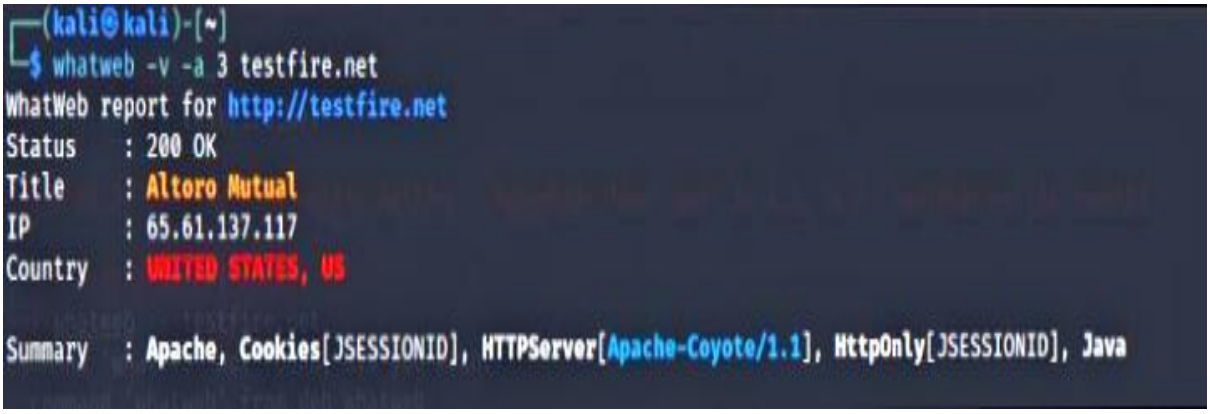
```
┌──(root㉿kali)-[~]
└─# whatweb -v mitkundapura.com
WhatWeb report for http://mitkundapura.com
Status    : 301 Moved Permanently
Title     : ,301 Moved Permanently
IP        : 217.21.87.244
Country   : UNITED KINGDOM, GB

Summary   : HTML5, HTTPServer[LiteSpeed], LiteSpeed, RedirectLocation[https://mitkundapura.

Detected Plugins:
[ HTML5 ]
        HTML version 5, detected by the doctype declaration
```

$ whatweb -a 3 testfire.net



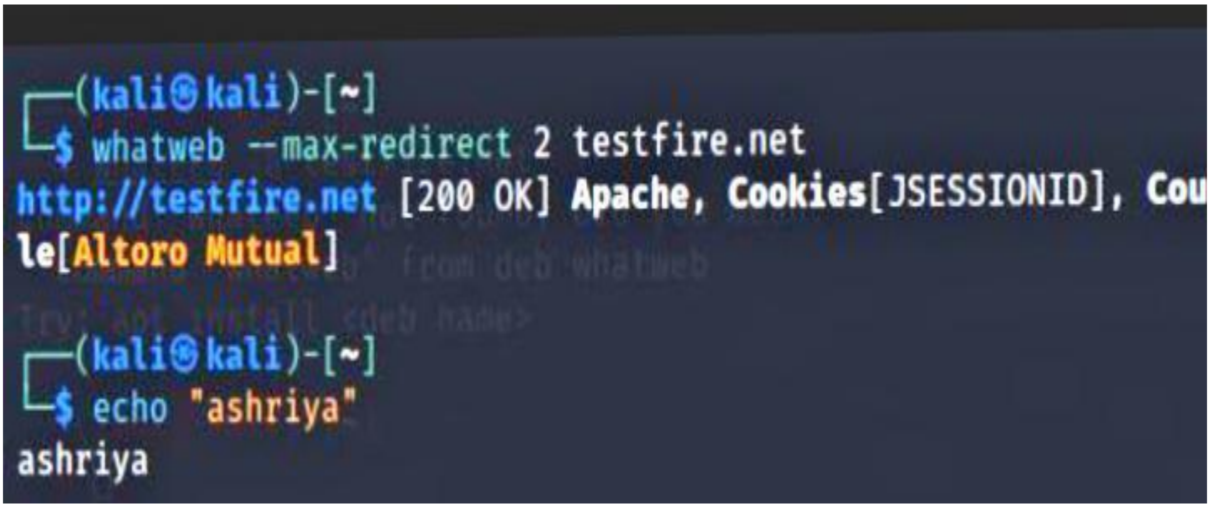
```
┌──(kali㉿kali)-[~]
└─$ whatweb -a 3 testfire.net
http://testfire.net [200 OK] Apache, Cookies[JSESSIO
le[Altoro Mutual]

┌──(kali㉿kali)-[~]
└─$ echo "ashriya"
ashriya
```

$ whatweb -v -a 3 testfire.net



```
┌──(kali㉿kali)-[~]
└─$ whatweb -v -a 3 testfire.net
WhatWeb report for http://testfire.net
Status    : 200 OK
Title     : Altoro Mutual
IP        : 65.61.137.117
Country   : UNITED STATES, US

Summary   : Apache, Cookies[JSESSIONID], HTTPServer[Apache-Coyote/1.1], HttpOnly[JSESSIONID], Java
```

$ whatweb –max-redirect 2 tesfire.net



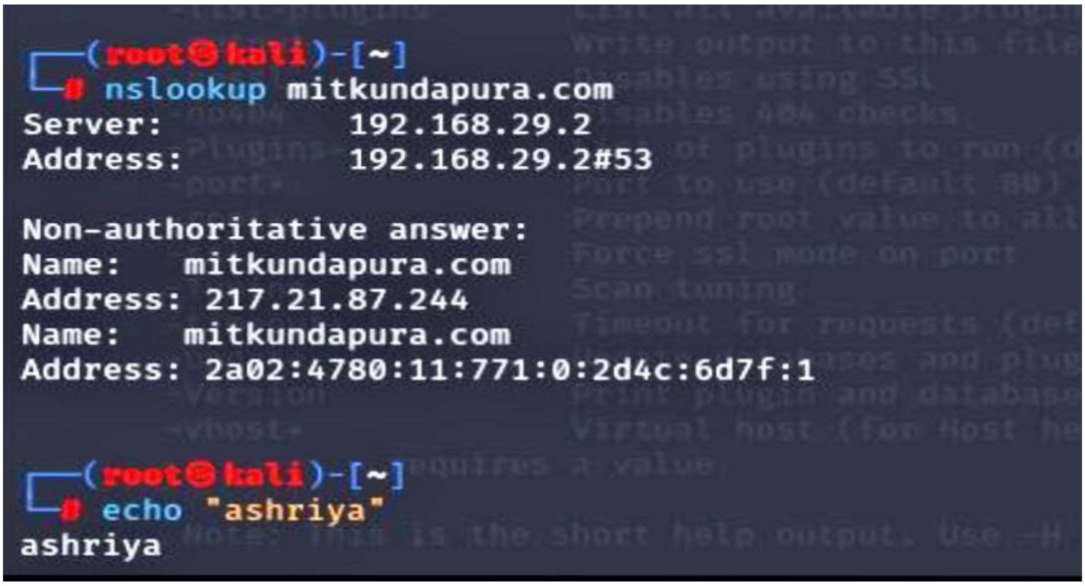
```
┌──(kali㉿kali)-[~]
└─$ whatweb --max-redirect 2 testfire.net
http://testfire.net [200 OK] Apache, Cookies[JSESSIONID], Cou
le[Altoro Mutual]

┌──(kali㉿kali)-[~]
└─$ echo "ashriya"
ashriya
```

4.Nslookup

Nslookup is the name of a program that lets an Internet server administrator or any computer user enter a host name and find out the corresponding IP address or domain name system (DNS) record. The user can also enter a command for it to do a reverse DNS lookup and find the host name for an IP address that is specified.

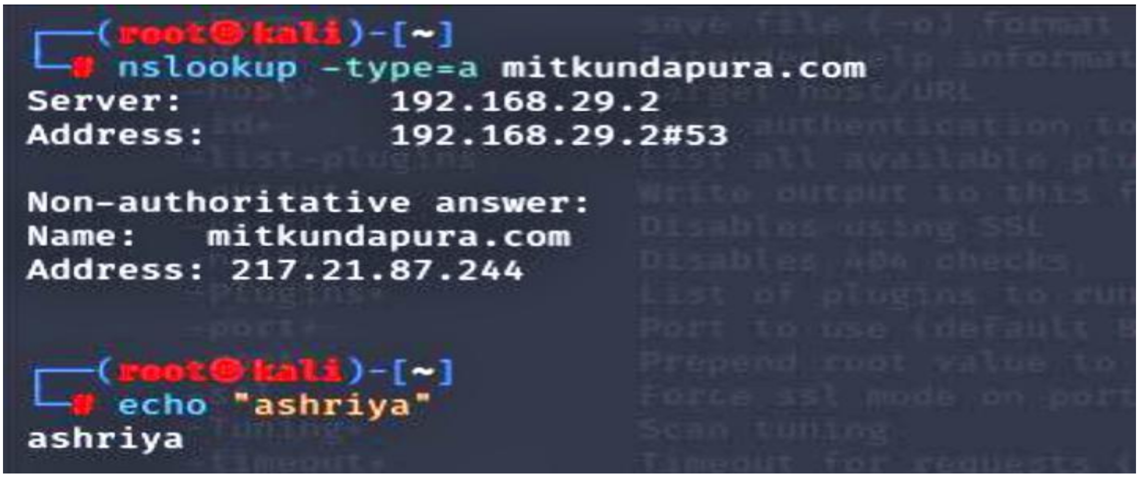
Command:

$ nslookup mitkundapura.com



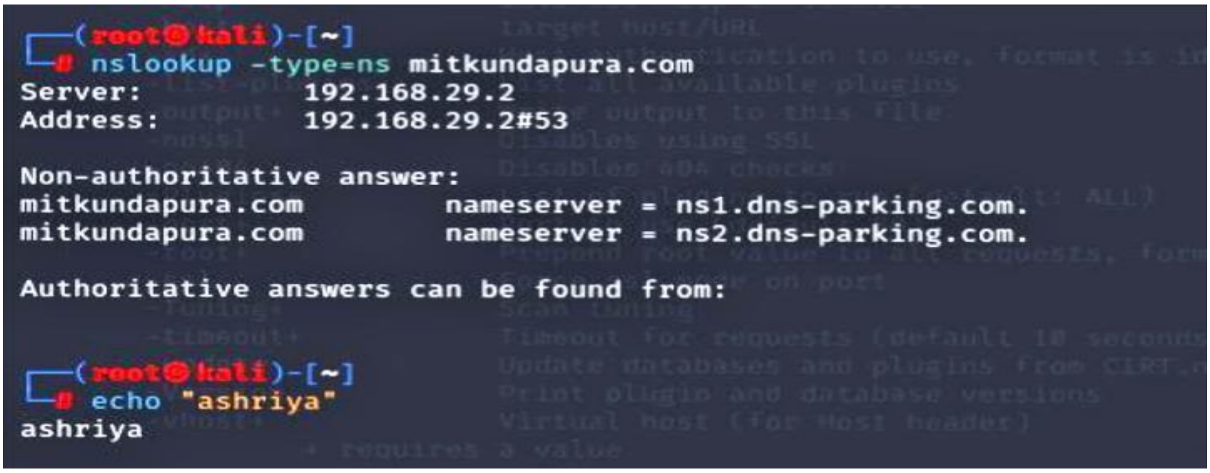
```
┌──(root㉿kali)-[~]
└─# nslookup mitkundapura.com
Server:         192.168.29.2
Address:        192.168.29.2#53

Non-authoritative answer:
Name:   mitkundapura.com
Address: 217.21.87.244
Name:   mitkundapura.com
Address: 2a02:4780:11:771:0:2d4c:6d7f:1

┌──(root㉿kali)-[~]
└─# echo "ashriya"
ashriya
```

$nslookup -type=a mitkundapura.com



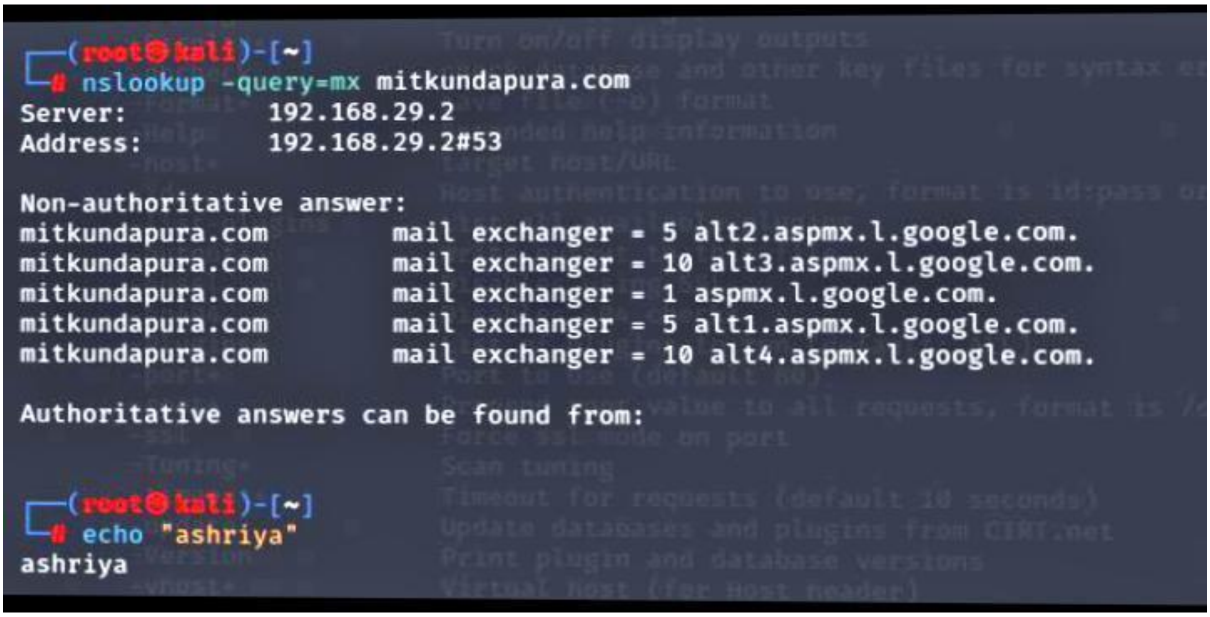
```
┌──(root㉿kali)-[~]
└─# nslookup -type=a mitkundapura.com
Server:         192.168.29.2
Address:        192.168.29.2#53

Non-authoritative answer:
Name:   mitkundapura.com
Address: 217.21.87.244

┌──(root㉿kali)-[~]
└─# echo "ashriya"
ashriya
```

$ nslookup -type=ns mitkundapura.com



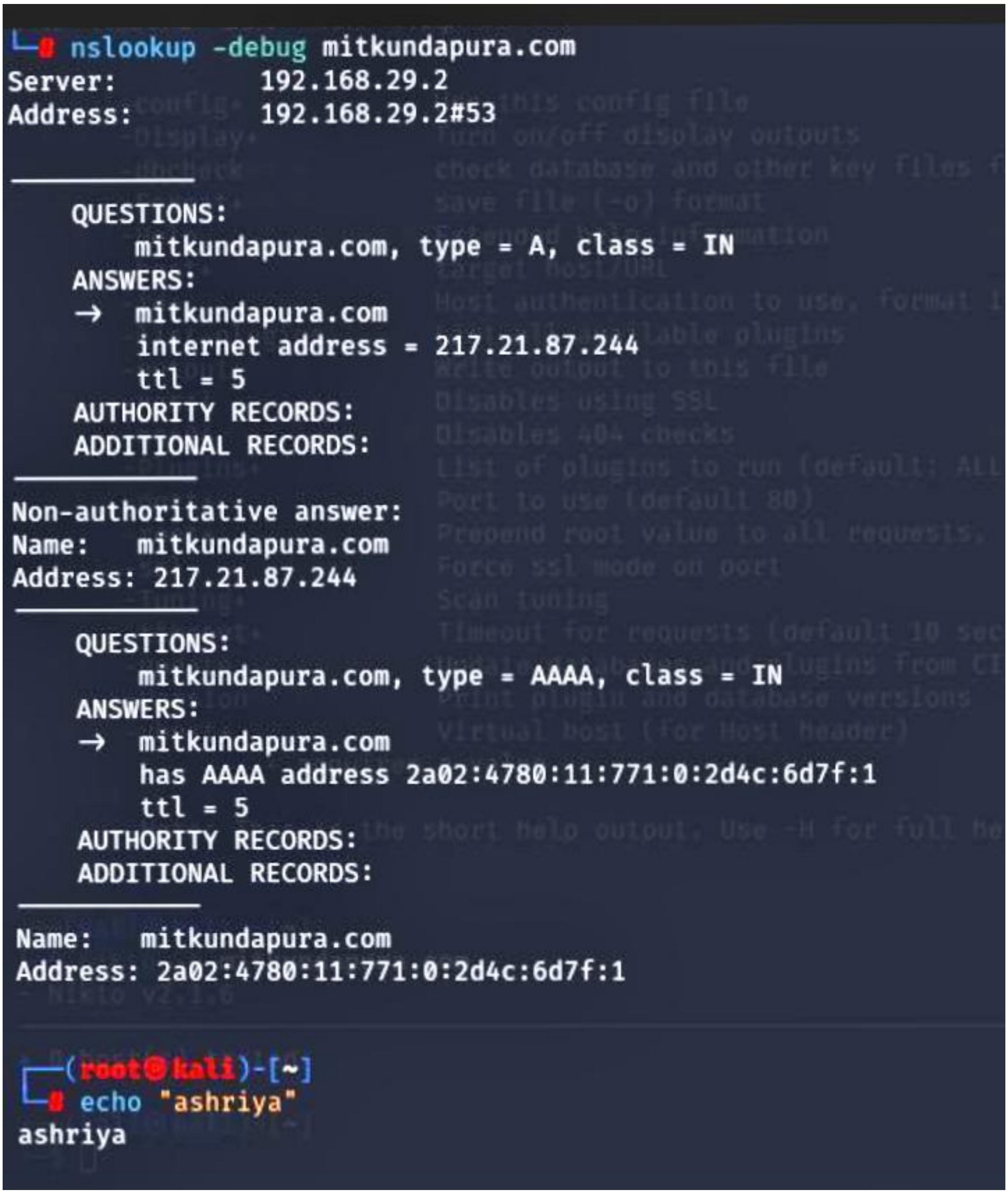
```
┌──(root㉿kali)-[~]
└─# nslookup -type=ns mitkundapura.com
Server:         192.168.29.2
Address:        192.168.29.2#53

Non-authoritative answer:
mitkundapura.com        nameserver = ns1.dns-parking.com.
mitkundapura.com        nameserver = ns2.dns-parking.com.

Authoritative answers can be found from:

┌──(root㉿kali)-[~]
└─# echo "ashriya"
ashriya
```

$nslookup -query=mx mitkundapura.com



```
┌──(root㉿kali)-[~]
└─# nslookup -query=mx mitkundapura.com
Server:         192.168.29.2
Address:        192.168.29.2#53

Non-authoritative answer:
mitkundapura.com        mail exchanger = 5 alt2.aspmx.l.google.com.
mitkundapura.com        mail exchanger = 10 alt3.aspmx.l.google.com.
mitkundapura.com        mail exchanger = 1 aspmx.l.google.com.
mitkundapura.com        mail exchanger = 5 alt1.aspmx.l.google.com.
mitkundapura.com        mail exchanger = 10 alt4.aspmx.l.google.com.

Authoritative answers can be found from:

┌──(root㉿kali)-[~]
└─# echo "ashriya"
ashriya
```

$nslookup -debug mitkundapura.com



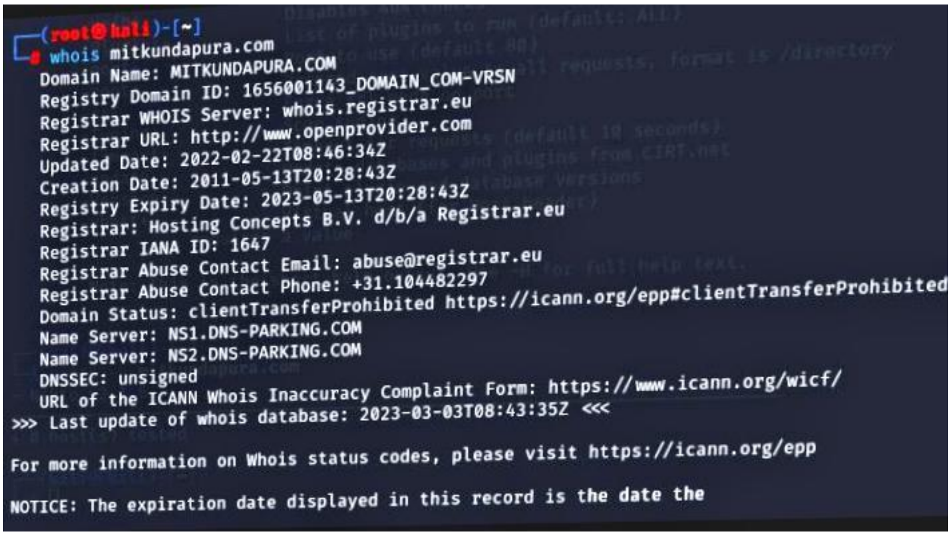
```
└─# nslookup -debug mitkundapura.com
Server:         192.168.29.2
Address:        192.168.29.2#53

------------
    QUESTIONS:
        mitkundapura.com, type = A, class = IN
    ANSWERS:
    ->  mitkundapura.com
        internet address = 217.21.87.244
        ttl = 5
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Non-authoritative answer:
Name:   mitkundapura.com
Address: 217.21.87.244
------------
    QUESTIONS:
        mitkundapura.com, type = AAAA, class = IN
    ANSWERS:
    ->  mitkundapura.com
        has AAAA address 2a02:4780:11:771:0:2d4c:6d7f:1
        ttl = 5
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Name:   mitkundapura.com
Address: 2a02:4780:11:771:0:2d4c:6d7f:1


┌──(root㉿kali)-[~]
└─# echo "ashriya"
ashriya
```

5.Whois

Whois is a widely used Internet record listing that identifies who owns a domain and how to get in contact with them. The Internet Corporation for Assigned Names and Numbers (ICANN) regulates domain name registration and ownership.

Commands:

$ whois mitkundapura.com



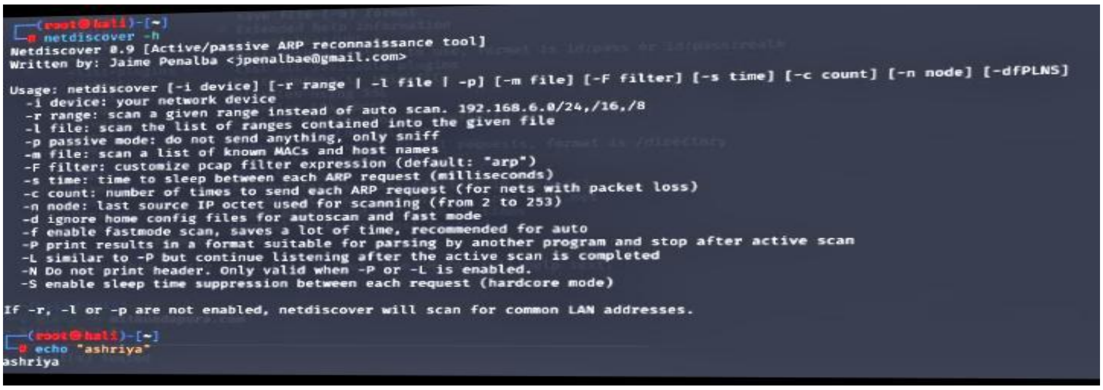
```
┌──(root㉿kali)-[~]
└─# whois mitkundapura.com
   Domain Name: MITKUNDAPURA.COM
   Registry Domain ID: 1656001143_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrar.eu
   Registrar URL: http://www.openprovider.com
   Updated Date: 2022-02-22T08:46:34Z
   Creation Date: 2011-05-13T20:28:43Z
   Registry Expiry Date: 2023-05-13T20:28:43Z
   Registrar: Hosting Concepts B.V. d/b/a Registrar.eu
   Registrar IANA ID: 1647
   Registrar Abuse Contact Email: abuse@registrar.eu
   Registrar Abuse Contact Phone: +31.104482297
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1.DNS-PARKING.COM
   Name Server: NS2.DNS-PARKING.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-03-03T08:43:35Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
```

6. Netdiscover

Netdiscover is an active/passive address reconnaissance tool, mainly developed for those wireless networks without dhcp server, when you are wardriving. It can be also used on hub/switched networks.

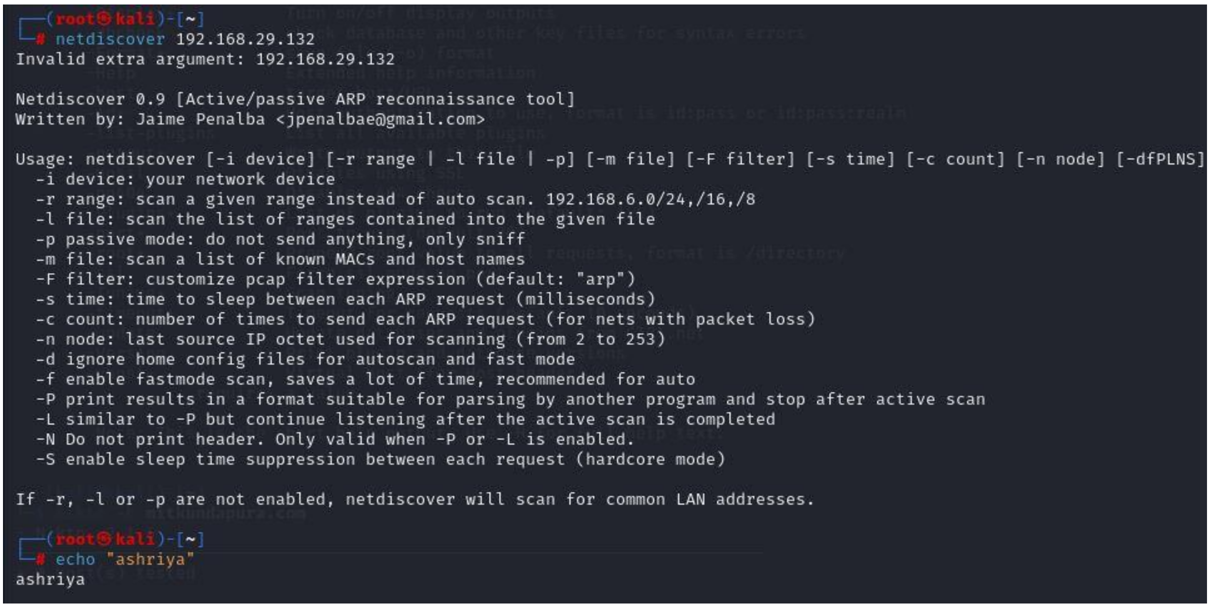
Command:

$ netdiscover –h



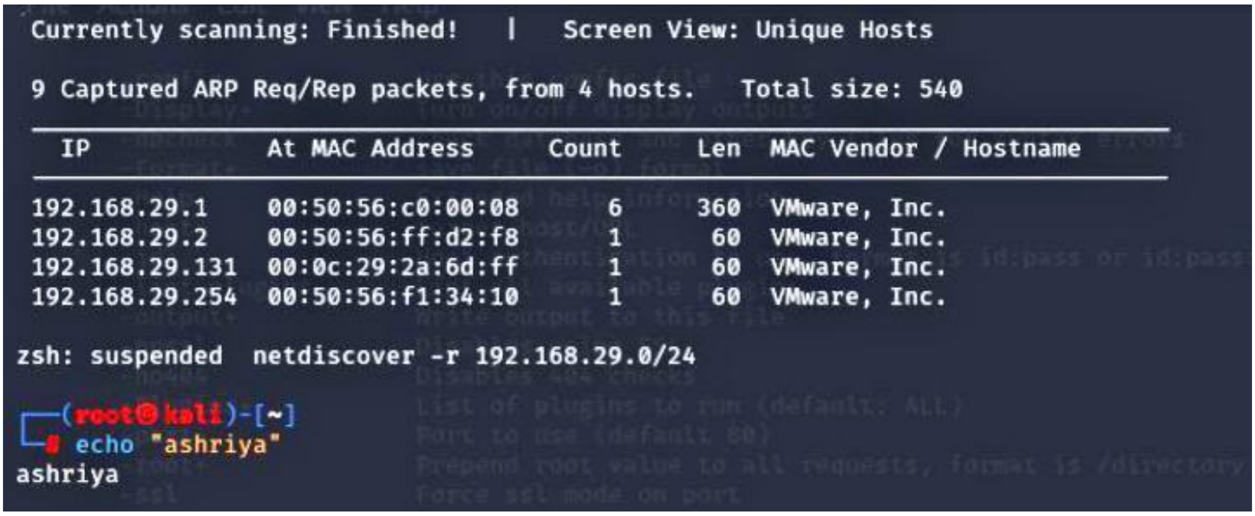
```
┌──(root㉿kali)-[~]
└─# netdiscover -h
Netdiscover 0.9 [Active/passive ARP reconnaissance tool]
Written by: Jaime Penalba <jpenalbae@gmail.com>

Usage: netdiscover [-i device] [-r range | -l file | -p] [-m file] [-F filter] [-s time] [-c count] [-n node] [-dfPLNS]
  -i device: your network device
  -r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8
  -l file: scan the list of ranges contained into the given file
  -p passive mode: do not send anything, only sniff
  -m file: scan a list of known MACs and host names
  -F filter: customize pcap filter expression (default: "arp")
  -s time: time to sleep between each ARP request (milliseconds)
  -c count: number of times to send each ARP request (for nets with packet loss)
  -n node: last source IP octet used for scanning (from 2 to 253)
  -d ignore home config files for autoscan and fast mode
  -f enable fastmode scan, saves a lot of time, recommended for auto
  -P print results in a format suitable for parsing by another program and stop after active scan
  -L similar to -P but continue listening after the active scan is completed
  -N Do not print header. Only valid when -P or -L is enabled.
  -S enable sleep time suppression between each request (hardcore mode)

If -r, -l or -p are not enabled, netdiscover will scan for common LAN addresses.

┌──(root㉿kali)-[~]
└─# echo "ashriya"
ashriya
```

$ netdiscover 192.168.29.132



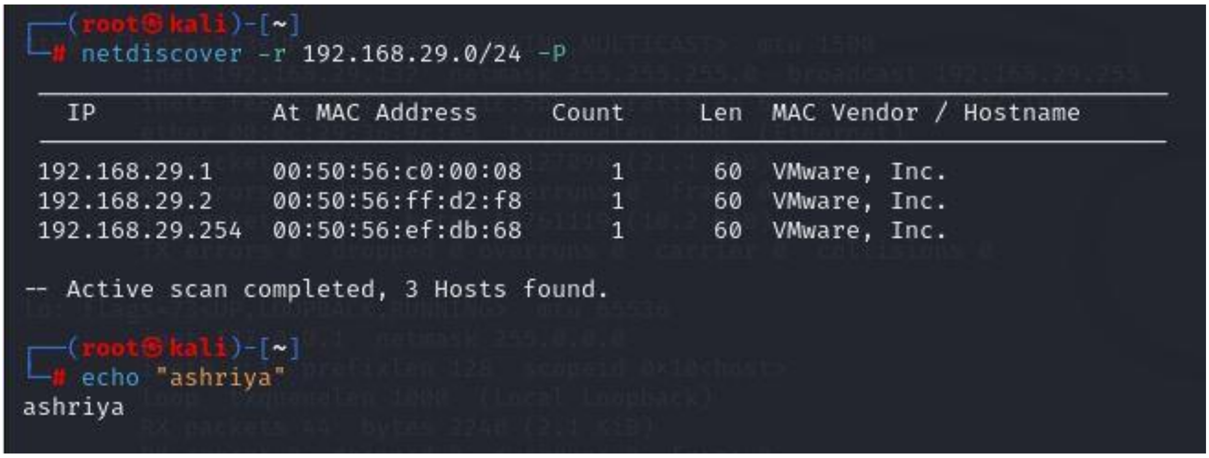
```
┌──(root㉿kali)-[~]
└─# netdiscover 192.168.29.132
Invalid extra argument: 192.168.29.132

Netdiscover 0.9 [Active/passive ARP reconnaissance tool]
Written by: Jaime Penalba <jpenalbae@gmail.com>

Usage: netdiscover [-i device] [-r range | -l file | -p] [-m file] [-F filter] [-s time] [-c count] [-n node] [-dfPLNS]
  -i device: your network device
  -r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8
  -l file: scan the list of ranges contained into the given file
  -p passive mode: do not send anything, only sniff
  -m file: scan a list of known MACs and host names
  -F filter: customize pcap filter expression (default: "arp")
  -s time: time to sleep between each ARP request (milliseconds)
  -c count: number of times to send each ARP request (for nets with packet loss)
  -n node: last source IP octet used for scanning (from 2 to 253)
  -d ignore home config files for autoscan and fast mode
  -f enable fastmode scan, saves a lot of time, recommended for auto
  -P print results in a format suitable for parsing by another program and stop after active scan
  -L similar to -P but continue listening after the active scan is completed
  -N Do not print header. Only valid when -P or -L is enabled.
  -S enable sleep time suppression between each request (hardcore mode)

If -r, -l or -p are not enabled, netdiscover will scan for common LAN addresses.

┌──(root㉿kali)-[~]
└─# echo "ashriya"
ashriya
```

$ netdiscover -r 192.168.29.0/24



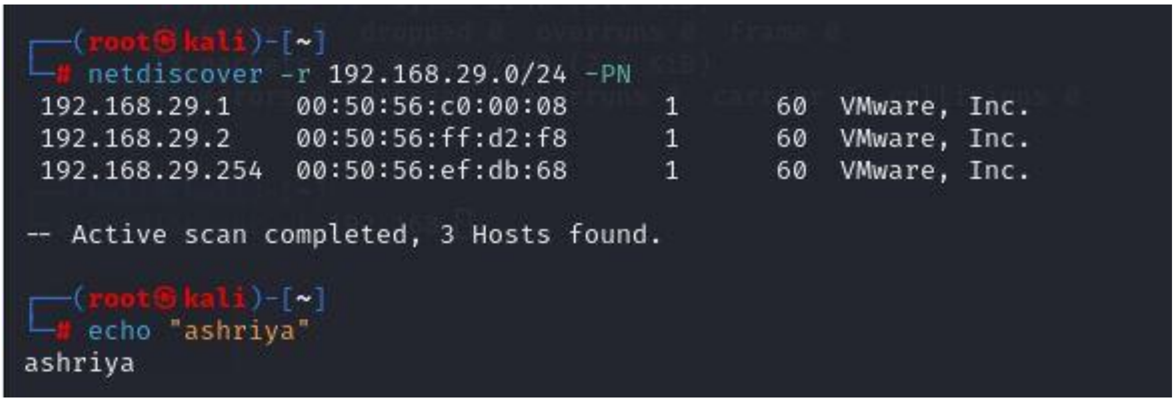
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 9 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 540
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.29.1    00:50:56:c0:00:08      6     360  VMware, Inc.
 192.168.29.2    00:50:56:ff:d2:f8      1      60  VMware, Inc.
 192.168.29.131  00:0c:29:2a:6d:ff      1      60  VMware, Inc.
 192.168.29.254  00:50:56:f1:34:10      1      60  VMware, Inc.

zsh: suspended  netdiscover -r 192.168.29.0/24

┌──(root㉿kali)-[~]
└─# echo "ashriya"
ashriya
```

$ netdiscover –r 192.168.29.0/24 –P



```
┌──(root㉿kali)-[~]
└─# netdiscover -r 192.168.29.0/24 -P
 ____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 ____________________________________________________________________________

 192.168.29.1    00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.29.2    00:50:56:ff:d2:f8      1      60  VMware, Inc.
 192.168.29.254  00:50:56:ef:db:68      1      60  VMware, Inc.

-- Active scan completed, 3 Hosts found.

┌──(root㉿kali)-[~]
└─# echo "ashriya"
ashriya
```

$ netdiscover –r 192.168.29.0/24 –PN



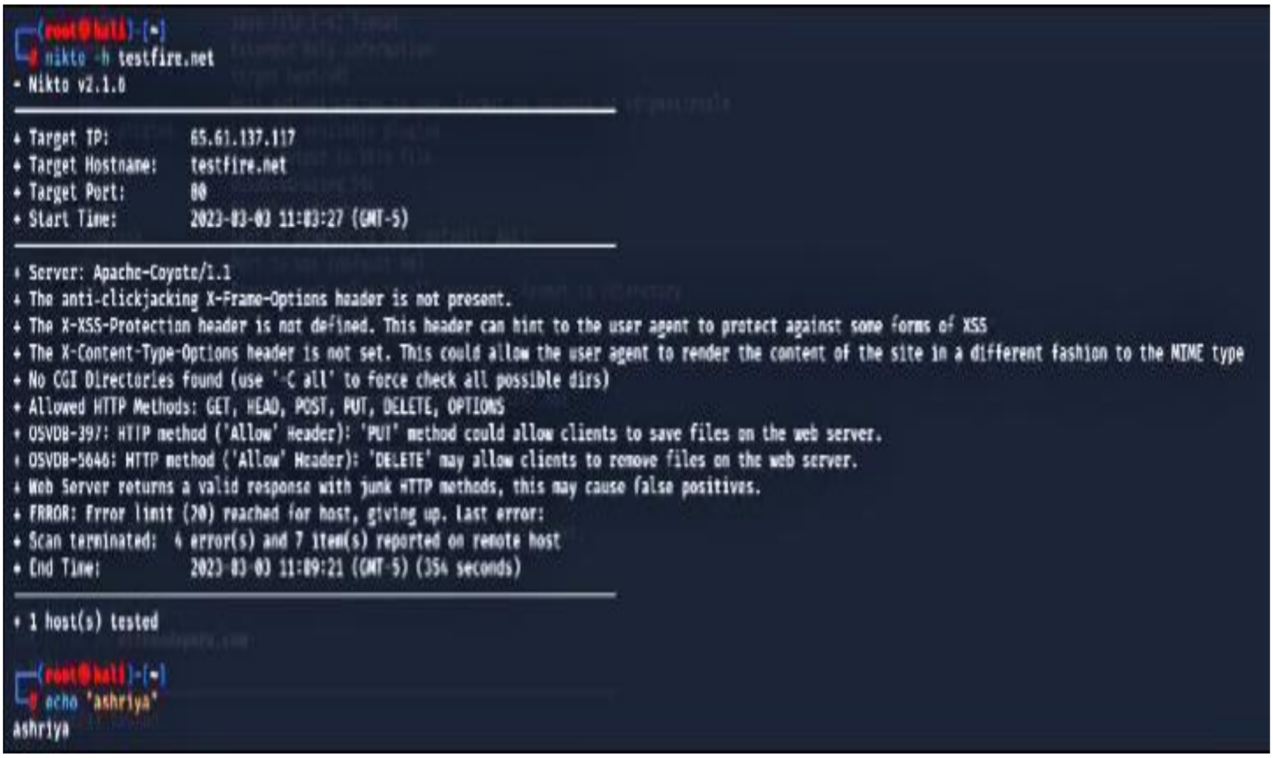
```
┌──(root㉿kali)-[~]
└─# netdiscover -r 192.168.29.0/24 -PN
 192.168.29.1    00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.29.2    00:50:56:ff:d2:f8      1      60  VMware, Inc.
 192.168.29.254  00:50:56:ef:db:68      1      60  VMware, Inc.

-- Active scan completed, 3 Hosts found.

┌──(root㉿kali)-[~]
└─# echo "ashriya"
ashriya
```

7.Nikto

Nikto is an Open Source software written in Perl language that is used to scan a web-server for the vulnerability that can be exploited and can compromise the server. It can also check for outdated version details of 1200 server and can detect problems with specific version details of over 200 servers.

Command:

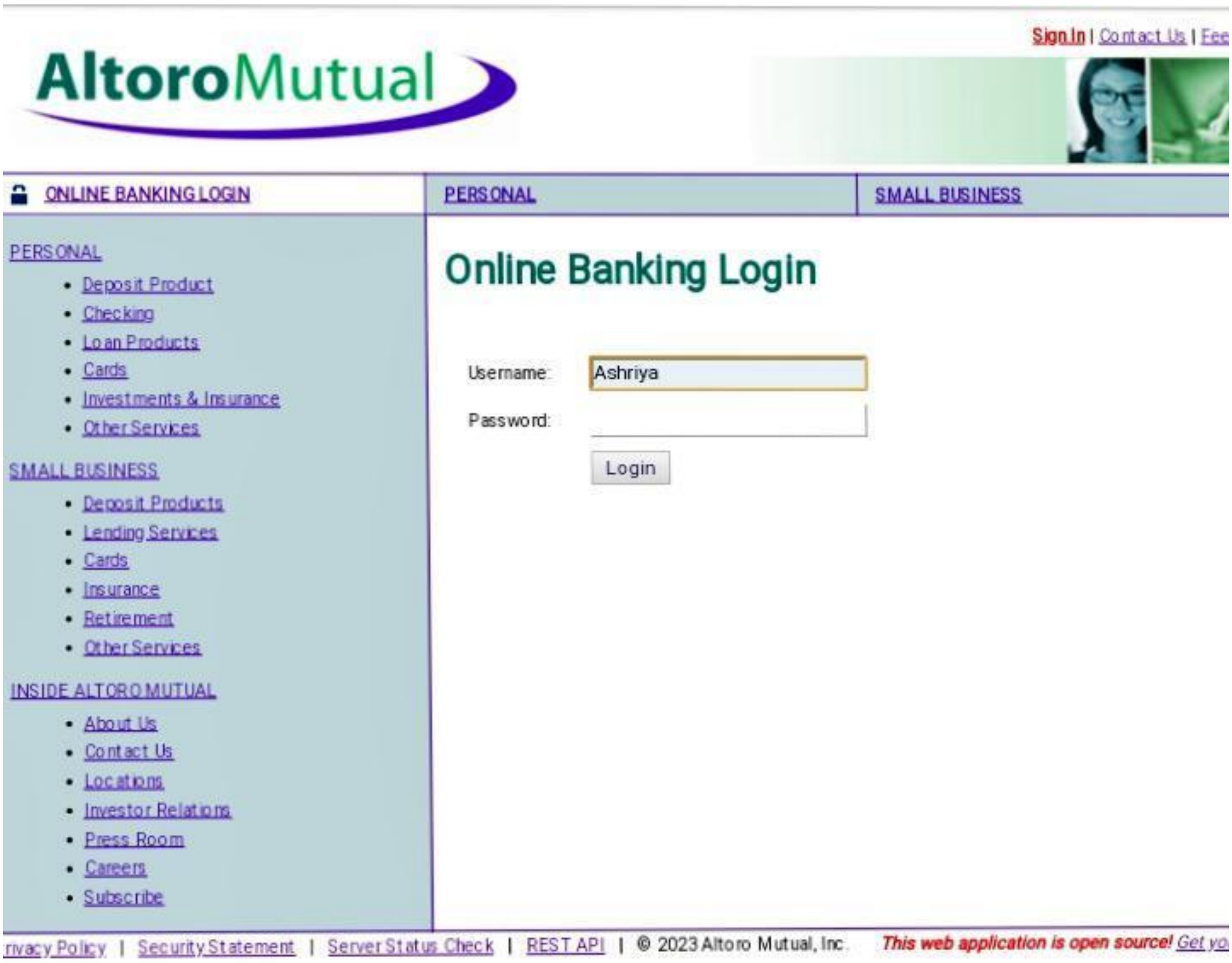
$ nikto -h testfire.net



```
┌──(root㉿kali)-[~]
└─# nikto -h testfire.net
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          65.61.137.117
+ Target Hostname:    testfire.net
+ Target Port:        80
+ Start Time:         2023-03-03 11:03:27 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated:  4 error(s) and 7 item(s) reported on remote host
+ End Time:           2023-03-03 11:09:21 (GMT-5) (354 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(root㉿kali)-[~]
└─# echo 'ashriya'
ashriya
```

8.Cryto configuration flaw

Cryptographic failures are where attackers often target sensitive data, such as passwords, credit card numbers, and personal information, when you do not properly protect them. This is the root cause of sensitive data exposure.



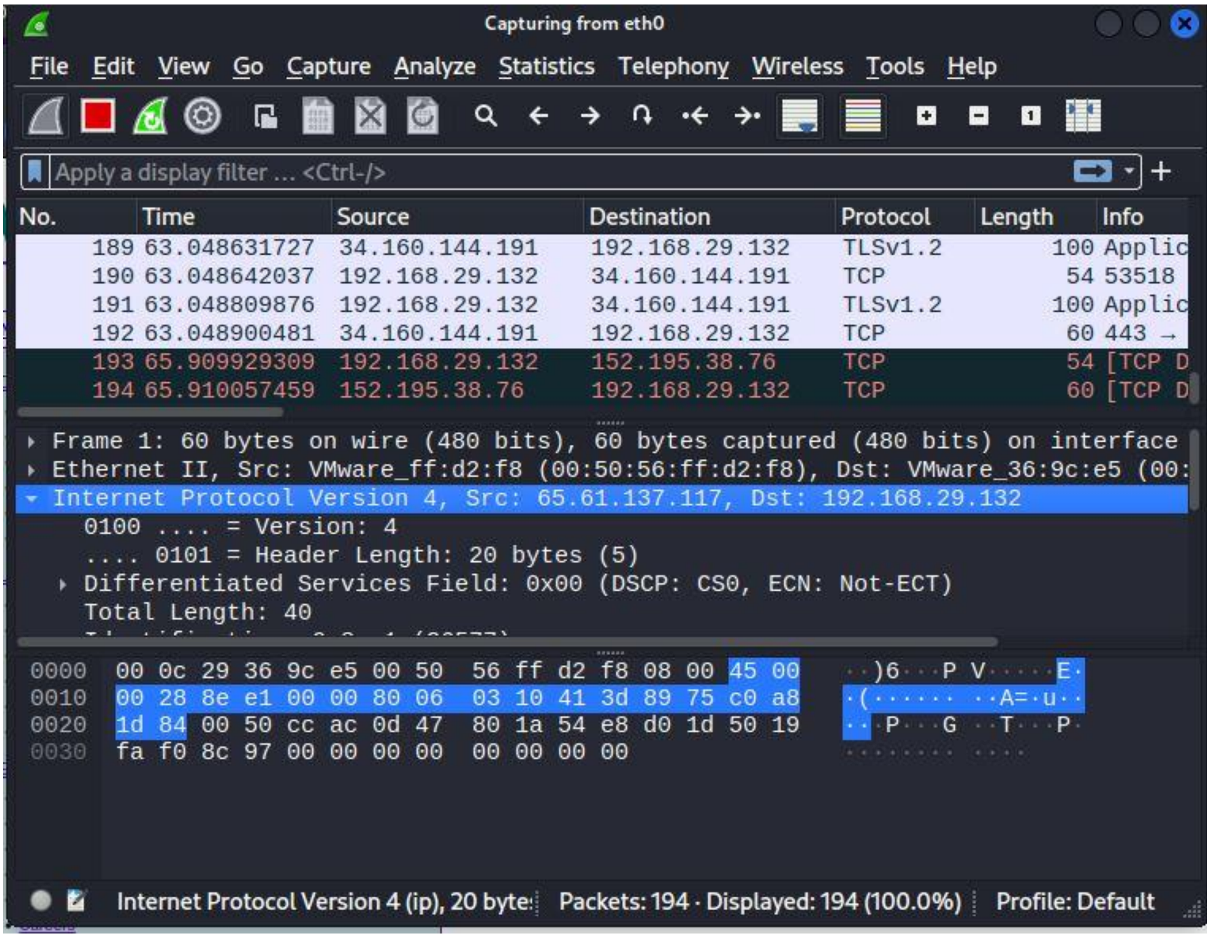
Online Banking Login

Username: Ashriya

Password:

9. Find data packet using wireshark

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network. Wireshark is the most often-used packet sniffer in the world.



No.	Time	Source	Destination	Protocol	Length	Info
189	63.048631727	34.160.144.191	192.168.29.132	TLSv1.2	100	Applic
190	63.048642037	192.168.29.132	34.160.144.191	TCP	54	53518
191	63.048809876	192.168.29.132	34.160.144.191	TLSv1.2	100	Applic
192	63.048900481	34.160.144.191	192.168.29.132	TCP	60	443 →
193	65.909929309	192.168.29.132	152.195.38.76	TCP	54	[TCP D
194	65.910057459	152.195.38.76	192.168.29.132	TCP	60	[TCP D

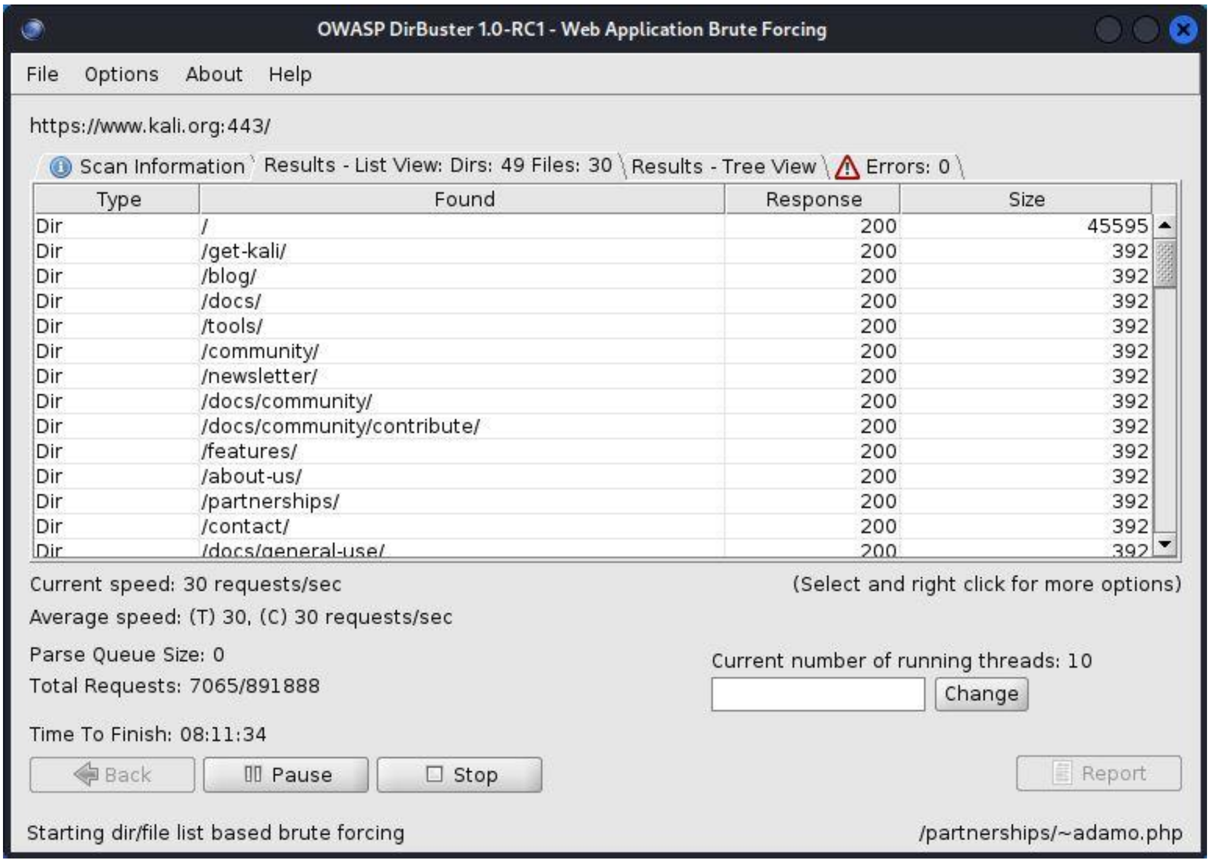
```
› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface
› Ethernet II, Src: VMware_ff:d2:f8 (00:50:56:ff:d2:f8), Dst: VMware_36:9c:e5 (00:
⌄ Internet Protocol Version 4, Src: 65.61.137.117, Dst: 192.168.29.132
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
```

```
0000   00 0c 29 36 9c e5 00 50  56 ff d2 f8 08 00 45 00   ··)6···P V·····E·
0010   00 28 8e e1 00 00 80 06  03 10 41 3d 89 75 c0 a8   ·(······ ··A=·u··
0020   1d 84 00 50 cc ac 0d 47  80 1a 54 e8 d0 1d 50 19   ··P···G ··T···P·
0030   fa f0 8c 97 00 00 00 00  00 00 00 00               ········ ····
```

Internet Protocol Version 4 (ip), 20 byte: | Packets: 194 · Displayed: 194 (100.0%) | Profile: Default

10. Find Xml pages in website using dirbuster

DirBuster is a multi threaded java application designed to brute force directories and files names on web/application servers. Often is the case now of what looks like a web server in a state of default installation is actually not, and has pages and applications hidden within.



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help
Scan Information
Results - List View: Dirs: 49 Files: 30
Results - Tree View
Errors: 0
Back
Pause
Stop
Change
Report

https://www.kali.org:443/

Type	Found	Response	Size
Dir	/	200	45595
Dir	/get-kali/	200	392
Dir	/blog/	200	392
Dir	/docs/	200	392
Dir	/tools/	200	392
Dir	/community/	200	392
Dir	/newsletter/	200	392
Dir	/docs/community/	200	392
Dir	/docs/community/contribute/	200	392
Dir	/features/	200	392
Dir	/about-us/	200	392
Dir	/partnerships/	200	392
Dir	/contact/	200	392
Dir	/docs/general-use/	200	392

Current speed: 30 requests/sec

(Select and right click for more options)

Average speed: (T) 30, (C) 30 requests/sec

Parse Queue Size: 0

Current number of running threads: 10

Total Requests: 7065/891888

Time To Finish: 08:11:34

Starting dir/file list based brute forcing

/partnerships/~adamo.php