Task-2

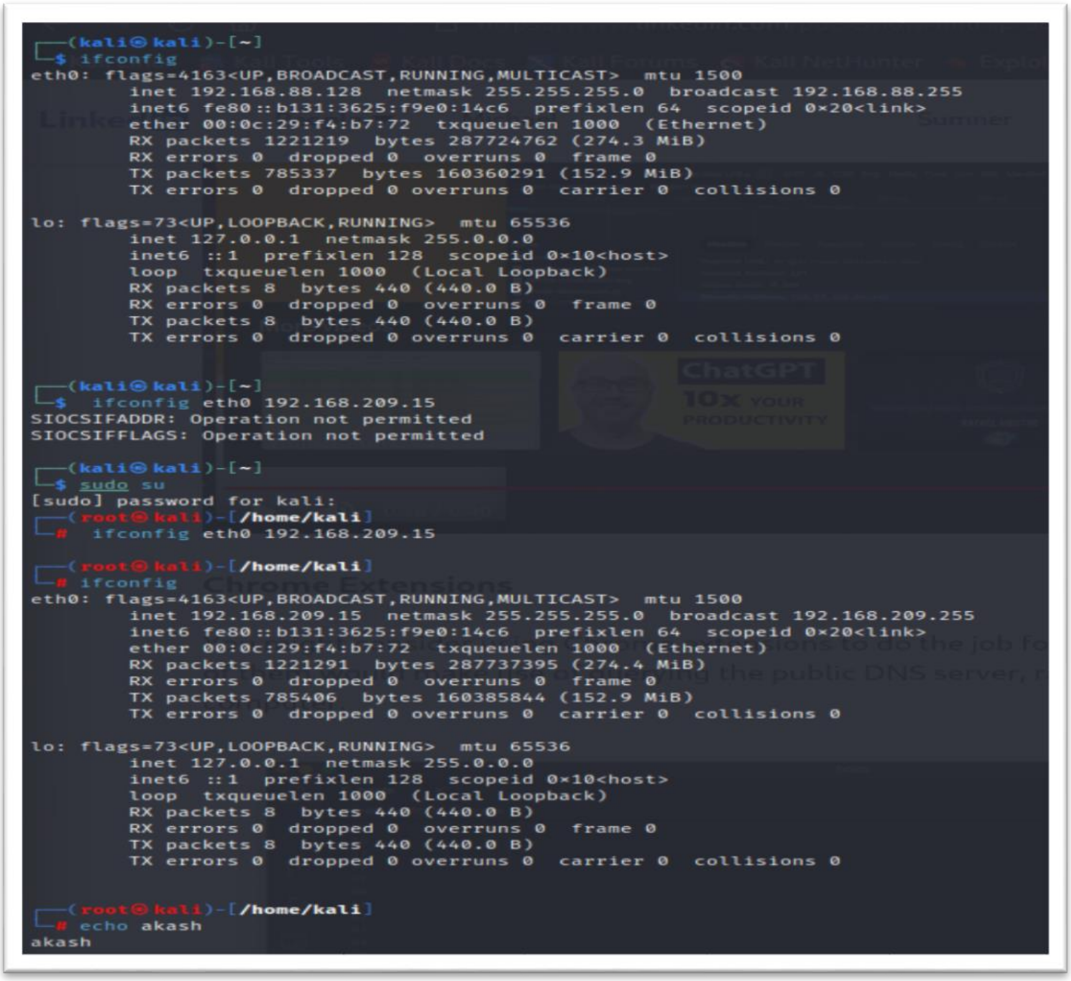
Name: akash gp

Date: 2/03/2023

1. Perform IP address spoofing

In IP spoofing, a hacker uses tools to modify the source address in the packet header to make the receiving computer system think the packet is from a trusted source, such as another computer on a legitimate network, and accept it. This occurs at the network level, so there are no external signs of tampering.

- $ ifconfig eth0 192.168.209.15
- $ ifconfig

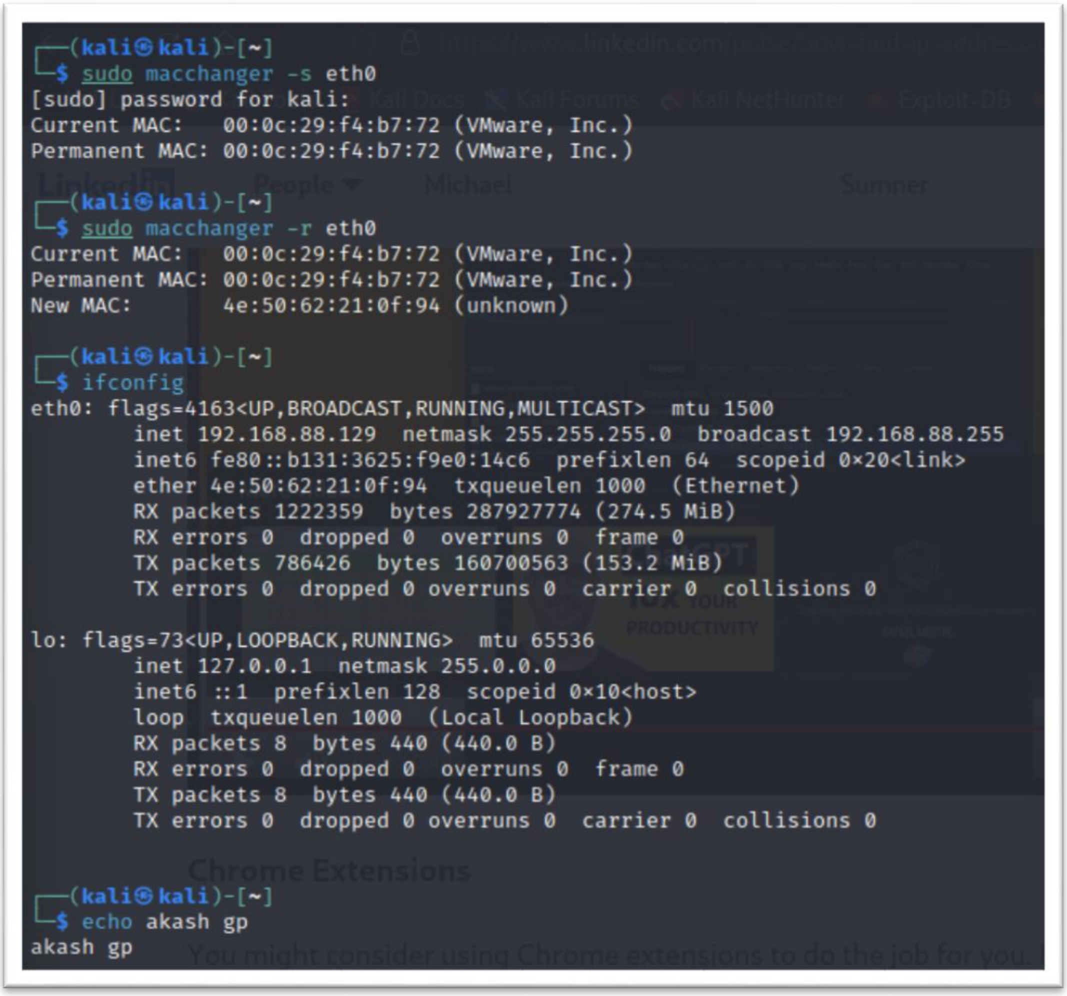


```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.88.128  netmask 255.255.255.0  broadcast 192.168.88.255
        inet6 fe80::b131:3625:f9e0:14c6  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:f4:b7:72  txqueuelen 1000  (Ethernet)
        RX packets 1221219  bytes 287724762 (274.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 785337  bytes 160360291 (152.9 MiB)
        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 8  bytes 440 (440.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 440 (440.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$  ifconfig eth0 192.168.209.15
SIOCSIFADDR: Operation not permitted
SIOCSIFFLAGS: Operation not permitted

┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─#  ifconfig eth0 192.168.209.15

┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.209.15  netmask 255.255.255.0  broadcast 192.168.209.255
        inet6 fe80::b131:3625:f9e0:14c6  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:f4:b7:72  txqueuelen 1000  (Ethernet)
        RX packets 1221291  bytes 287737395 (274.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 785406  bytes 160385844 (152.9 MiB)
        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 8  bytes 440 (440.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 440 (440.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[/home/kali]
└─# echo akash
akash
```

2.Perform MAC address spoofing

An attacker can mimic your MAC address and redirect data sent to your device to another and access your data. A MAC spoofing attack is when a hacker changes the MAC address of their device to match the MAC address of another on a network in order to gain unauthorized access or launch a Man- in-the-Middle attack.

- $ macchanger –s eth0
- $ ifconfig $ macchanger –r eth0
- $ ifconfig

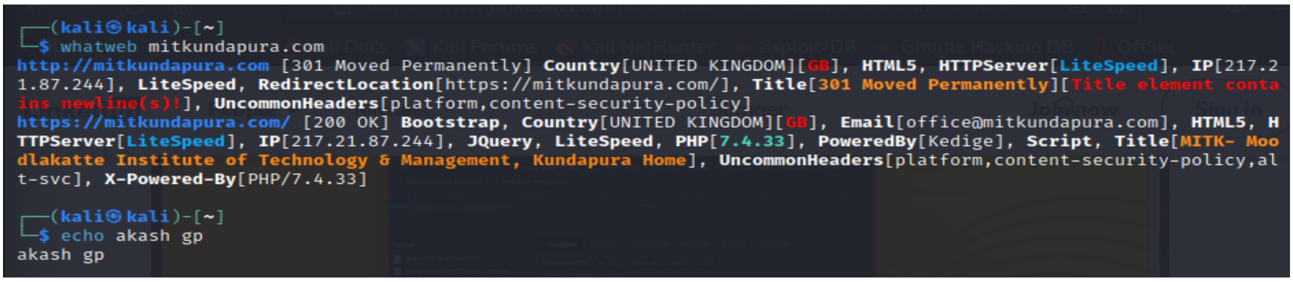


```
┌──(kali㉿kali)-[~]
└─$ sudo macchanger -s eth0
[sudo] password for kali:
Current MAC:   00:0c:29:f4:b7:72 (VMware, Inc.)
Permanent MAC: 00:0c:29:f4:b7:72 (VMware, Inc.)

┌──(kali㉿kali)-[~]
└─$ sudo macchanger -r eth0
Current MAC:   00:0c:29:f4:b7:72 (VMware, Inc.)
Permanent MAC: 00:0c:29:f4:b7:72 (VMware, Inc.)
New MAC:       4e:50:62:21:0f:94 (unknown)

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.88.129  netmask 255.255.255.0  broadcast 192.168.88.255
        inet6 fe80::b131:3625:f9e0:14c6  prefixlen 64  scopeid 0x20<link>
        ether 4e:50:62:21:0f:94  txqueuelen 1000  (Ethernet)
        RX packets 1222359  bytes 287927774 (274.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 786426  bytes 160700563 (153.2 MiB)
        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 8  bytes 440 (440.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 440 (440.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ echo akash gp
akash gp
```

3.Any 5 whatweb commands

Basic scanning: The most basic command to scan a website with WhatWeb is

- $ whatweb mitkundapura.com

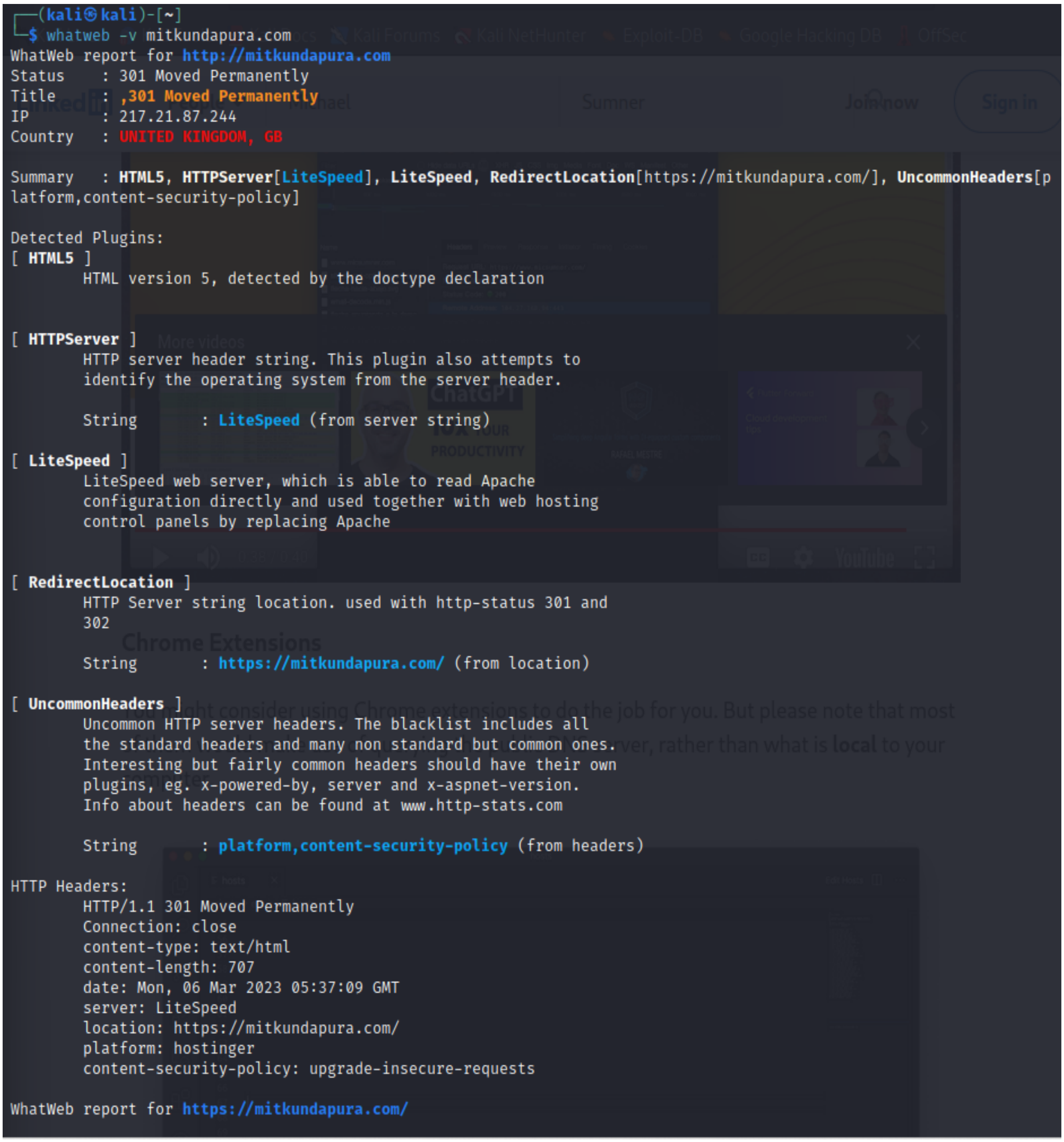


```
┌──(kali㉿kali)-[~]
└─$ whatweb mitkundapura.com
http://mitkundapura.com [301 Moved Permanently] Country[UNITED KINGDOM][GB], HTML5, HTTPServer[LiteSpeed], IP[217.2
1.87.244], LiteSpeed, RedirectLocation[https://mitkundapura.com/], Title[301 Moved Permanently][Title element conta
ins newline(s)!], UncommonHeaders[platform,content-security-policy]
https://mitkundapura.com/ [200 OK] Bootstrap, Country[UNITED KINGDOM][GB], Email[office@mitkundapura.com], HTML5, H
TTPServer[LiteSpeed], IP[217.21.87.244], JQuery, LiteSpeed, PHP[7.4.33], PoweredBy[Kedige], Script, Title[MITK- Moo
dlakatte Institute of Technology & Management, Kundapura Home], UncommonHeaders[platform,content-security-policy,al
t-svc], X-Powered-By[PHP/7.4.33]

┌──(kali㉿kali)-[~]
└─$ echo akash gp
akash gp
```

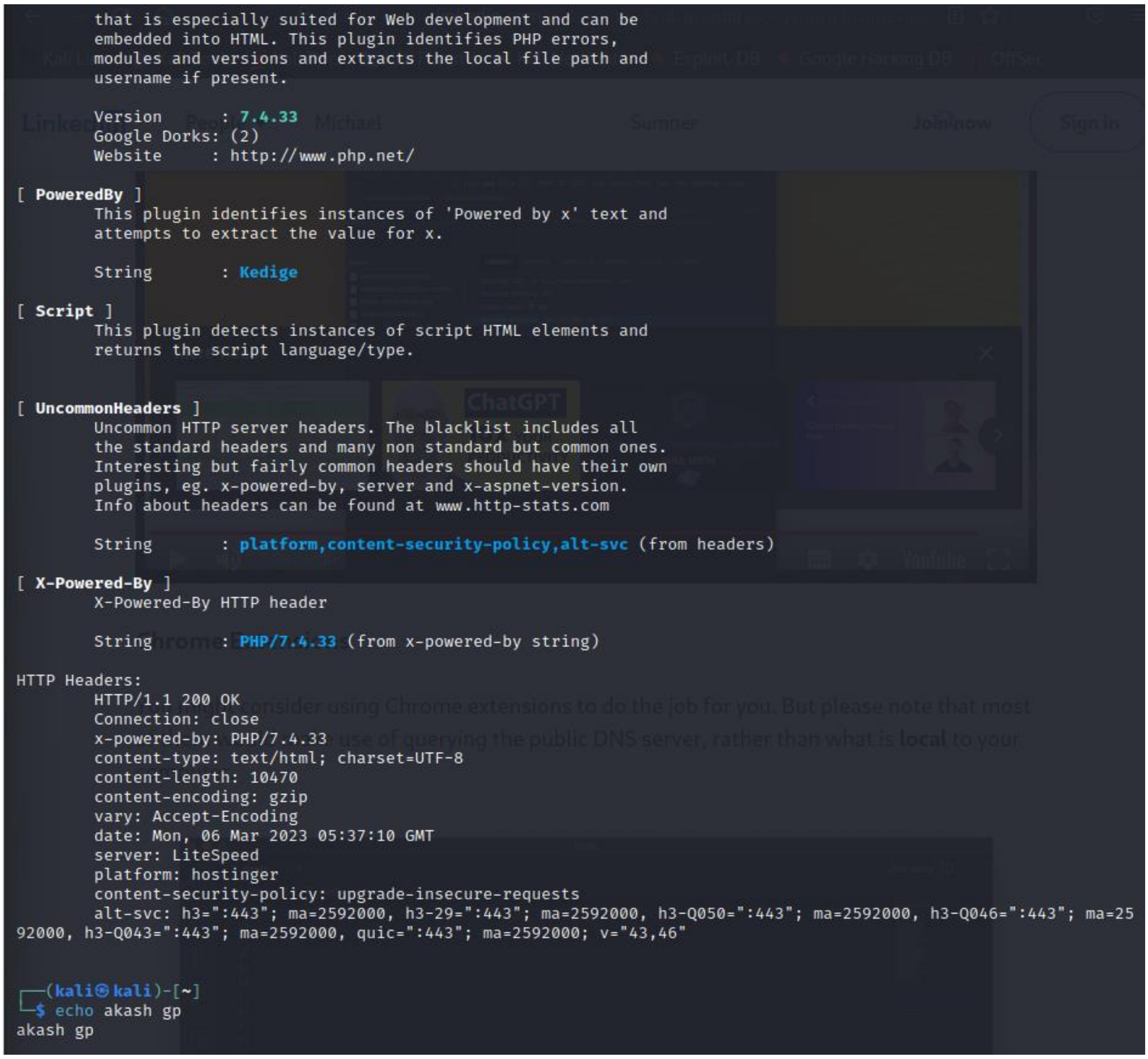
This will perform a default scan of the website and display the identified technologies.

<u>Verbose scanning</u>: If you want more detailed information about the website, you can use the verbose flag (-v)

- $ whatweb -v [website URL] This will perform a more thorough scan a



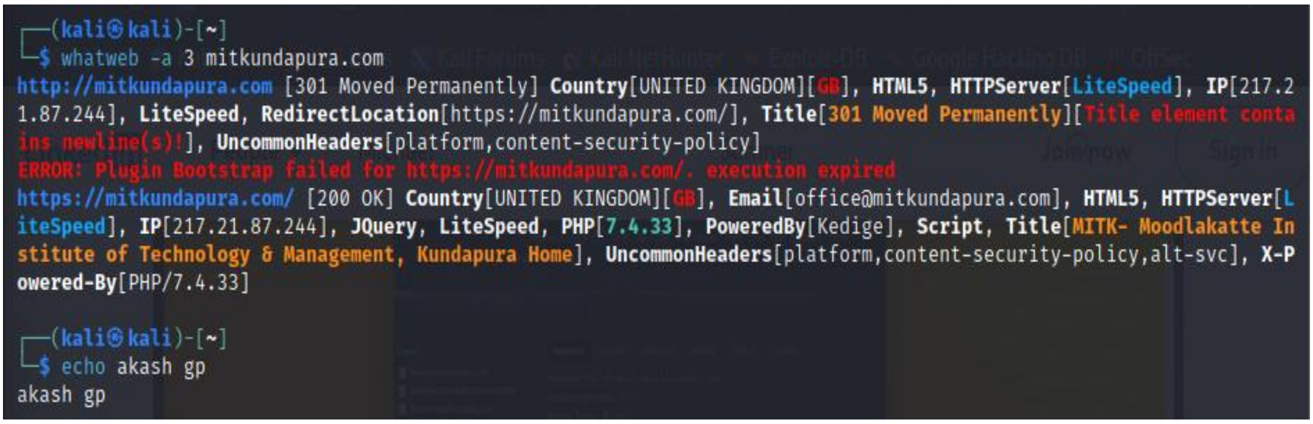
```
┌──(kali㉿kali)-[~]
└─$ whatweb -v mitkundapura.com
WhatWeb report for http://mitkundapura.com
Status    : 301 Moved Permanently
Title     : ,301 Moved Permanently
IP        : 217.21.87.244
Country   : UNITED KINGDOM, GB

Summary   : HTML5, HTTPServer[LiteSpeed], LiteSpeed, RedirectLocation[https://mitkundapura.com/], UncommonHeaders[p
latform,content-security-policy]

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


[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : LiteSpeed (from server string)

[ LiteSpeed ]
        LiteSpeed web server, which is able to read Apache
        configuration directly and used together with web hosting
        control panels by replacing Apache


[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : https://mitkundapura.com/ (from location)

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : platform,content-security-policy (from headers)

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Connection: close
        content-type: text/html
        content-length: 707
        date: Mon, 06 Mar 2023 05:37:09 GMT
        server: LiteSpeed
        location: https://mitkundapura.com/
        platform: hostinger
        content-security-policy: upgrade-insecure-requests

WhatWeb report for https://mitkundapura.com/
```



```
          that is especially suited for Web development and can be
          embedded into HTML. This plugin identifies PHP errors,
          modules and versions and extracts the local file path and
          username if present.

          Version      : 7.4.33
          Google Dorks: (2)
          Website      : http://www.php.net/

[ PoweredBy ]
          This plugin identifies instances of 'Powered by x' text and
          attempts to extract the value for x.

          String       : Kedige

[ Script ]
          This plugin detects instances of script HTML elements and
          returns the script language/type.


[ UncommonHeaders ]
          Uncommon HTTP server headers. The blacklist includes all
          the standard headers and many non standard but common ones.
          Interesting but fairly common headers should have their own
          plugins, eg. x-powered-by, server and x-aspnet-version.
          Info about headers can be found at www.http-stats.com

          String       : platform,content-security-policy,alt-svc (from headers)

[ X-Powered-By ]
          X-Powered-By HTTP header

          String       : PHP/7.4.33 (from x-powered-by string)

HTTP Headers:
          HTTP/1.1 200 OK
          Connection: close
          x-powered-by: PHP/7.4.33
          content-type: text/html; charset=UTF-8
          content-length: 10470
          content-encoding: gzip
          vary: Accept-Encoding
          date: Mon, 06 Mar 2023 05:37:10 GMT
          server: LiteSpeed
          platform: hostinger
          content-security-policy: upgrade-insecure-requests
          alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=25
92000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"


┌──(kali㉿kali)-[~]
└─$ echo akash gp
akash gp
```

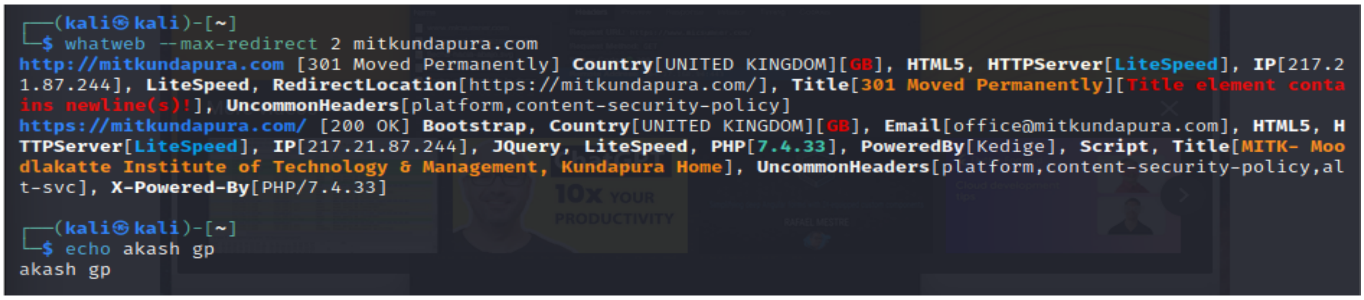
This will perform a more thorough scan and provide additional details, such as HTTP headers and server information.

$ whatweb –a 3 mitkundapura.com



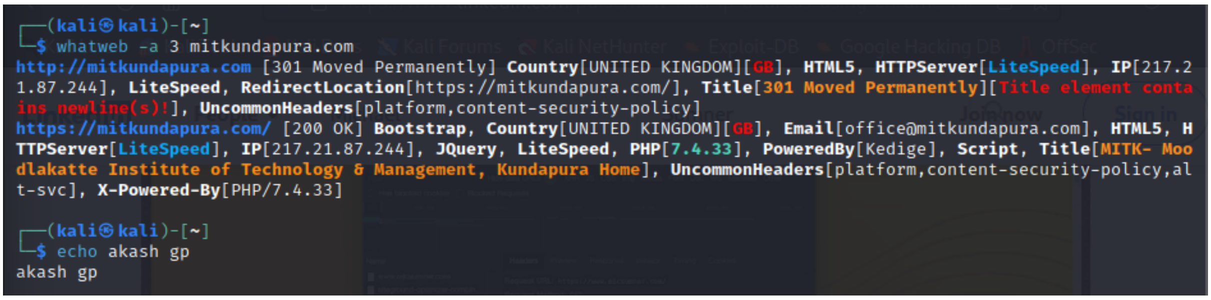
```
┌──(kali㉿kali)-[~]
└─$ whatweb -a 3 mitkundapura.com
http://mitkundapura.com [301 Moved Permanently] Country[UNITED KINGDOM][GB], HTML5, HTTPServer[LiteSpeed], IP[217.2
1.87.244], LiteSpeed, RedirectLocation[https://mitkundapura.com/], Title[301 Moved Permanently][Title element conta
ins newline(s)!], UncommonHeaders[platform,content-security-policy]
ERROR: Plugin Bootstrap failed for https://mitkundapura.com/. execution expired
https://mitkundapura.com/ [200 OK] Country[UNITED KINGDOM][GB], Email[office@mitkundapura.com], HTML5, HTTPServer[L
iteSpeed], IP[217.21.87.244], JQuery, LiteSpeed, PHP[7.4.33], PoweredBy[Kedige], Script, Title[MITK- Moodlakatte In
stitute of Technology & Management, Kundapura Home], UncommonHeaders[platform,content-security-policy,alt-svc], X-P
owered-By[PHP/7.4.33]

┌──(kali㉿kali)-[~]
└─$ echo akash gp
akash gp
```

$ whatweb --max –redirect 2 mitkundapura.com



```
┌──(kali㉿kali)-[~]
└─$ whatweb --max-redirect 2 mitkundapura.com
http://mitkundapura.com [301 Moved Permanently] Country[UNITED KINGDOM][GB], HTML5, HTTPServer[LiteSpeed], IP[217.2
1.87.244], LiteSpeed, RedirectLocation[https://mitkundapura.com/], Title[301 Moved Permanently][Title element conta
ins newline(s)!], UncommonHeaders[platform,content-security-policy]
https://mitkundapura.com/ [200 OK] Bootstrap, Country[UNITED KINGDOM][GB], Email[office@mitkundapura.com], HTML5, H
TTPServer[LiteSpeed], IP[217.21.87.244], JQuery, LiteSpeed, PHP[7.4.33], PoweredBy[Kedige], Script, Title[MITK- Moo
dlakatte Institute of Technology & Management, Kundapura Home], UncommonHeaders[platform,content-security-policy,al
t-svc], X-Powered-By[PHP/7.4.33]

┌──(kali㉿kali)-[~]
└─$ echo akash gp
akash gp
```

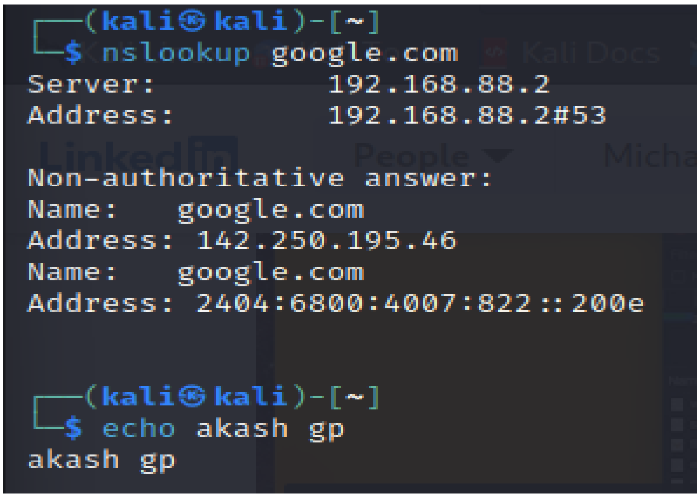
$ whatweb –a 3 mitkundapura.com



```
┌──(kali㉿kali)-[~]
└─$ whatweb -a 3 mitkundapura.com
http://mitkundapura.com [301 Moved Permanently] Country[UNITED KINGDOM][GB], HTML5, HTTPServer[LiteSpeed], IP[217.2
1.87.244], LiteSpeed, RedirectLocation[https://mitkundapura.com/], Title[301 Moved Permanently][Title element conta
ins newline(s)!], UncommonHeaders[platform,content-security-policy]
https://mitkundapura.com/ [200 OK] Bootstrap, Country[UNITED KINGDOM][GB], Email[office@mitkundapura.com], HTML5, H
TTPServer[LiteSpeed], IP[217.21.87.244], JQuery, LiteSpeed, PHP[7.4.33], PoweredBy[Kedige], Script, Title[MITK- Moo
dlakatte Institute of Technology & Management, Kundapura Home], UncommonHeaders[platform,content-security-policy,al
t-svc], X-Powered-By[PHP/7.4.33]

┌──(kali㉿kali)-[~]
└─$ echo akash gp
akash gp
```

4.Any 5 nslookup commands

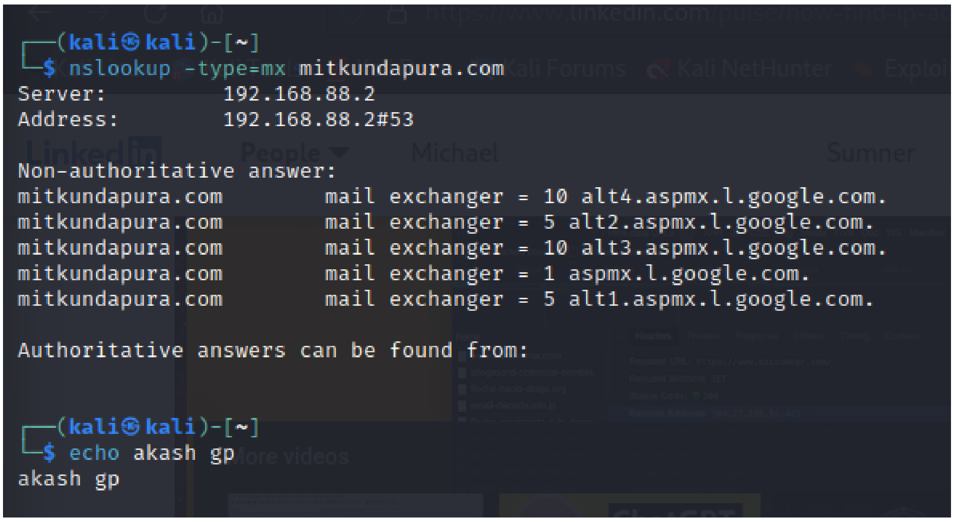
- $ nslookup google.com



```
┌──(kali㉿kali)-[~]
└─$ nslookup google.com
Server:         192.168.88.2
Address:        192.168.88.2#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.195.46
Name:   google.com
Address: 2404:6800:4007:822::200e


┌──(kali㉿kali)-[~]
└─$ echo akash gp
akash gp
```

- $ nslookup -type=mx example.com

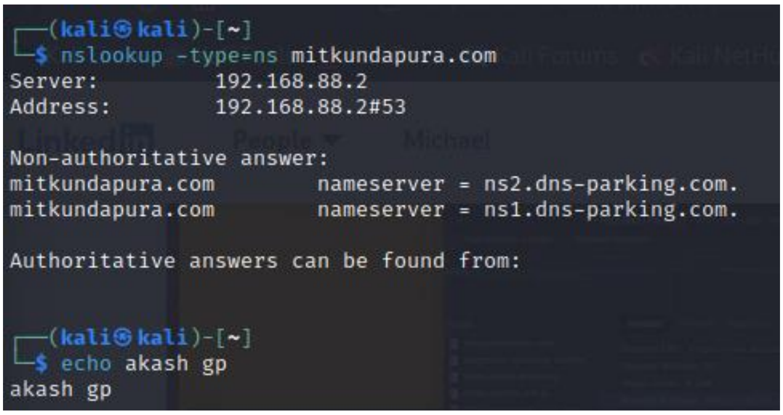
This command will perform a DNS lookup for the mail exchange (MX) records associated with the domain name “mitkundapura.com”.



```
┌──(kali㉿kali)-[~]
└─$ nslookup -type=mx mitkundapura.com
Server:         192.168.88.2
Address:        192.168.88.2#53

Non-authoritative answer:
mitkundapura.com        mail exchanger = 10 alt4.aspmx.l.google.com.
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.

Authoritative answers can be found from:


┌──(kali㉿kali)-[~]
└─$ echo akash gp
akash gp
```

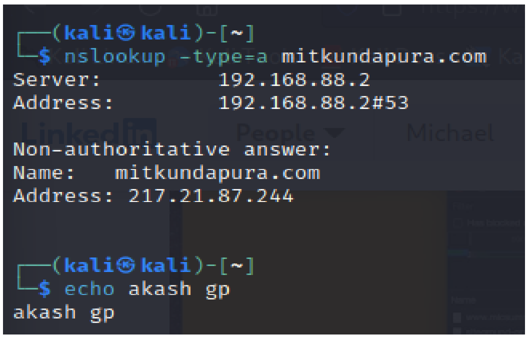
$ nslookup -type=ns mitkundapura.com

This command will perform a DNS lookup for the name server (NS) records associated with the domain name “mitkundapura.com”



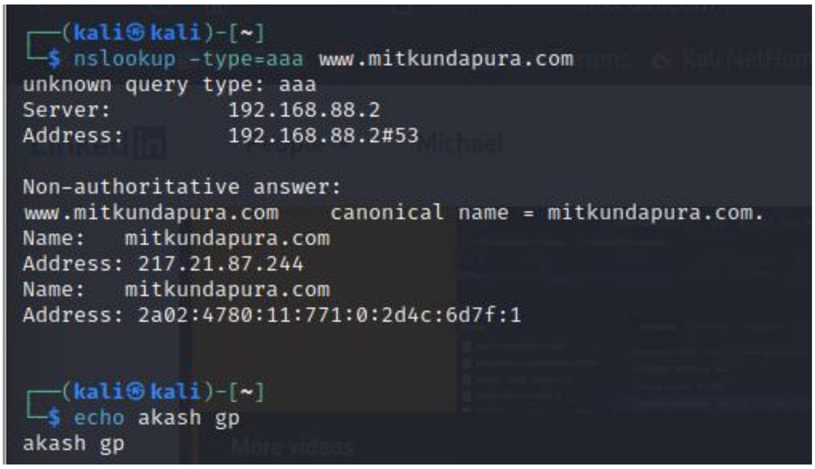
```
┌──(kali㉿kali)-[~]
└─$ nslookup -type=ns mitkundapura.com
Server:         192.168.88.2
Address:        192.168.88.2#53

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

Authoritative answers can be found from:


┌──(kali㉿kali)-[~]
└─$ echo akash gp
akash gp
```

$ nslookup -type=a www.mitkundapura.com This command will perform a DNS lookup for the IPv4 address associated with the subdomain www.mitkundapura.com.



```
┌──(kali㉿kali)-[~]
└─$ nslookup -type=a mitkundapura.com
Server:         192.168.88.2
Address:        192.168.88.2#53

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


┌──(kali㉿kali)-[~]
└─$ echo akash gp
akash gp
```

$ nslookup -type=aaa www.mitkundapura.com This command will perform a DNS lookup for the IPv6 address associated with the subdomain www.mitkundapura.com



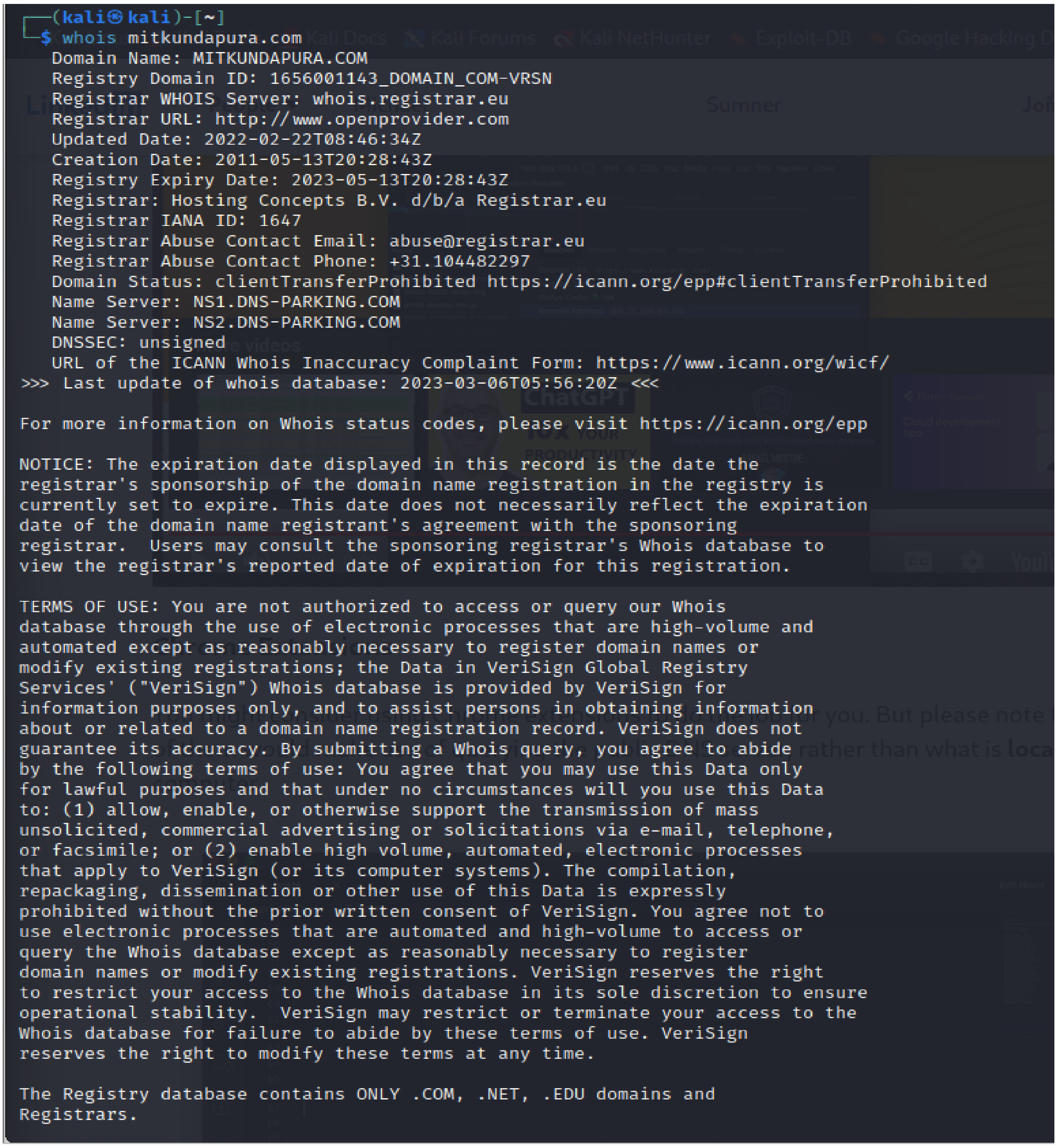
```
┌──(kali㉿kali)-[~]
└─$ nslookup -type=aaa www.mitkundapura.com
unknown query type: aaa
Server:         192.168.88.2
Address:        192.168.88.2#53

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

┌──(kali㉿kali)-[~]
└─$ echo akash gp
akash gp
```

5.whois Commands

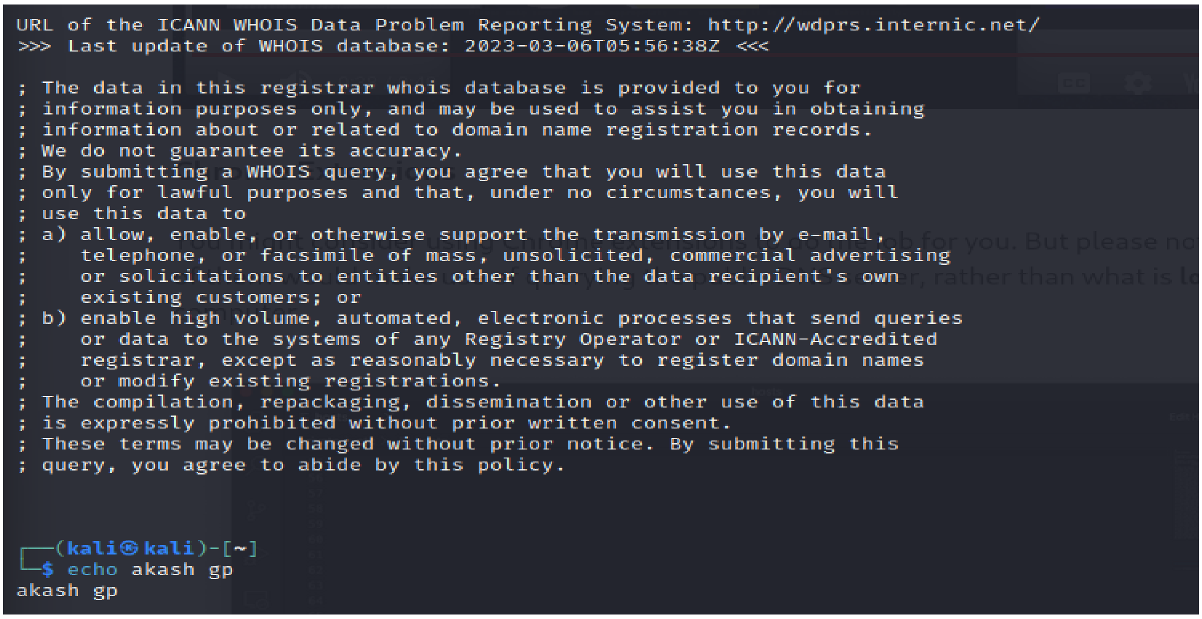
The whois command is a protocol used to look up information about domain names, IP addresses, and other network-related information. Here are some common WHOIS commands:

- $ whois mitkundapura.com

This command will display information about the domain name, such as the name of the registrant, the name servers, and the date of registration



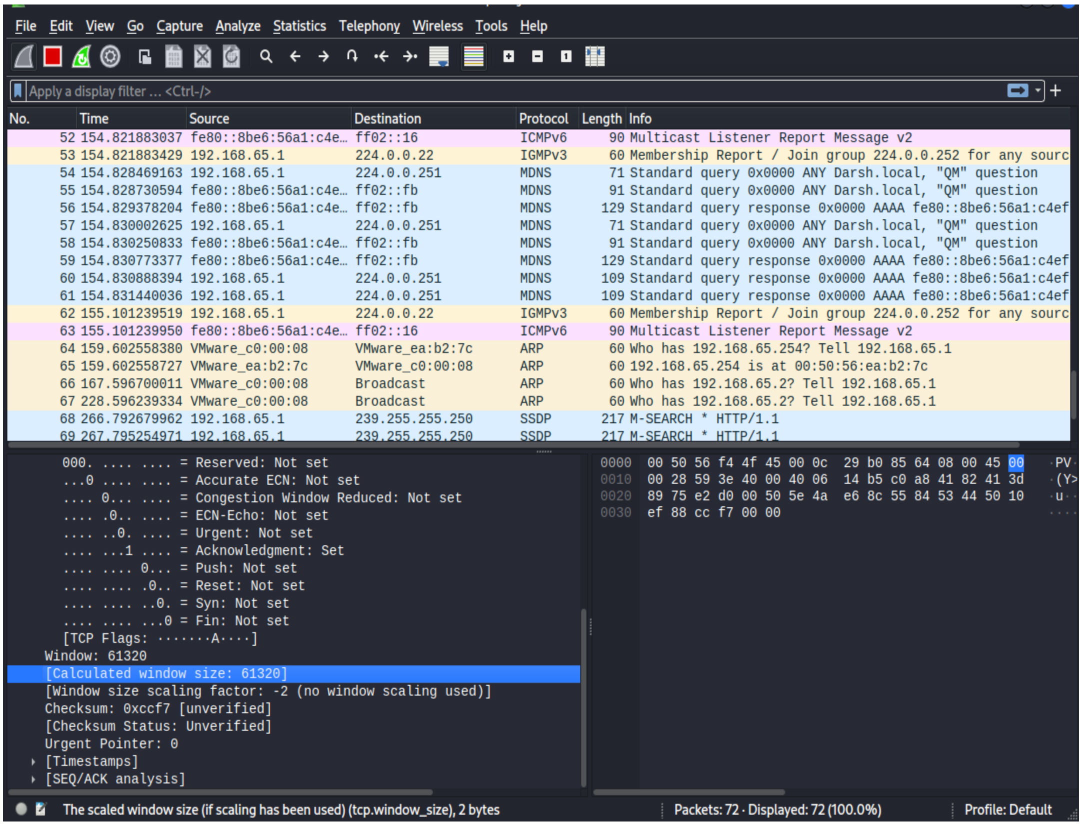
```
┌──(kali㉿kali)-[~]
└─$ whois mitkundapura.com
   Domain Name: MITKUNDAPURA.COM
   Registry Domain ID: 1656001143_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrar.eu
   Registrar URL: http://www.openprovider.com
   Updated Date: 2022-02-22T08:46:34Z
   Creation Date: 2011-05-13T20:28:43Z
   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: 2023-03-06T05:56:20Z <<<

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
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
```



```
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-03-06T05:56:38Z <<<

; The data in this registrar whois database is provided to you for
; information purposes only, and may be used to assist you in obtaining
; information about or related to domain name registration records.
; We do not guarantee its accuracy.
; By submitting a WHOIS query, you agree that you will use this data
; only for lawful purposes and that, under no circumstances, you will
; use this data to
; a) allow, enable, or otherwise support the transmission by e-mail,
;    telephone, or facsimile of mass, unsolicited, commercial advertising
;    or solicitations to entities other than the data recipient's own
;    existing customers; or
; b) enable high volume, automated, electronic processes that send queries
;    or data to the systems of any Registry Operator or ICANN-Accredited
;    registrar, except as reasonably necessary to register domain names
;    or modify existing registrations.
; The compilation, repackaging, dissemination or other use of this data
; is expressly prohibited without prior written consent.
; These terms may be changed without prior notice. By submitting this
; query, you agree to abide by this policy.


┌──(kali㉿kali)-[~]
└─$ echo akash gp
akash gp
```

6.Data packet using wireshark:

Wireshark is an open source packet analyser, which is used for education, analysis, software development, communication protocol development and network troubleshooting. Wireshark is a network protocol analyzer, or an application that captures packets from a network connection.



No.	Time	Source	Destination	Protocol	Length	Info
52	154.821883037	fe80::8be6:56a1:c4e…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
53	154.821883429	192.168.65.1	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sourc
54	154.828469163	192.168.65.1	224.0.0.251	MDNS	71	Standard query 0x0000 ANY Darsh.local, "QM" question
55	154.828730594	fe80::8be6:56a1:c4e…	ff02::fb	MDNS	91	Standard query 0x0000 ANY Darsh.local, "QM" question
56	154.829378204	fe80::8be6:56a1:c4e…	ff02::fb	MDNS	129	Standard query response 0x0000 AAAA fe80::8be6:56a1:c4ef
57	154.830002625	192.168.65.1	224.0.0.251	MDNS	71	Standard query 0x0000 ANY Darsh.local, "QM" question
58	154.830250833	fe80::8be6:56a1:c4e…	ff02::fb	MDNS	91	Standard query 0x0000 ANY Darsh.local, "QM" question
59	154.830773377	fe80::8be6:56a1:c4e…	ff02::fb	MDNS	129	Standard query response 0x0000 AAAA fe80::8be6:56a1:c4ef
60	154.830888394	192.168.65.1	224.0.0.251	MDNS	109	Standard query response 0x0000 AAAA fe80::8be6:56a1:c4ef
61	154.831440036	192.168.65.1	224.0.0.251	MDNS	109	Standard query response 0x0000 AAAA fe80::8be6:56a1:c4ef
62	155.101239519	192.168.65.1	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sourc
63	155.101239950	fe80::8be6:56a1:c4e…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
64	159.602558380	VMware_c0:00:08	VMware_ea:b2:7c	ARP	60	Who has 192.168.65.254? Tell 192.168.65.1
65	159.602558727	VMware_ea:b2:7c	VMware_c0:00:08	ARP	60	192.168.65.254 is at 00:50:56:ea:b2:7c
66	167.596700011	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.65.2? Tell 192.168.65.1
67	228.596239334	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.65.2? Tell 192.168.65.1
68	266.792679962	192.168.65.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
69	267.795254971	192.168.65.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

```
    000. .... .... = Reserved: Not set
    ...0 .... .... = Accurate ECN: Not set
    .... 0... .... = Congestion Window Reduced: Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·······A····]
  Window: 61320
  [Calculated window size: 61320]
  [Window size scaling factor: -2 (no window scaling used)]
  Checksum: 0xccf7 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
› [Timestamps]
› [SEQ/ACK analysis]
```

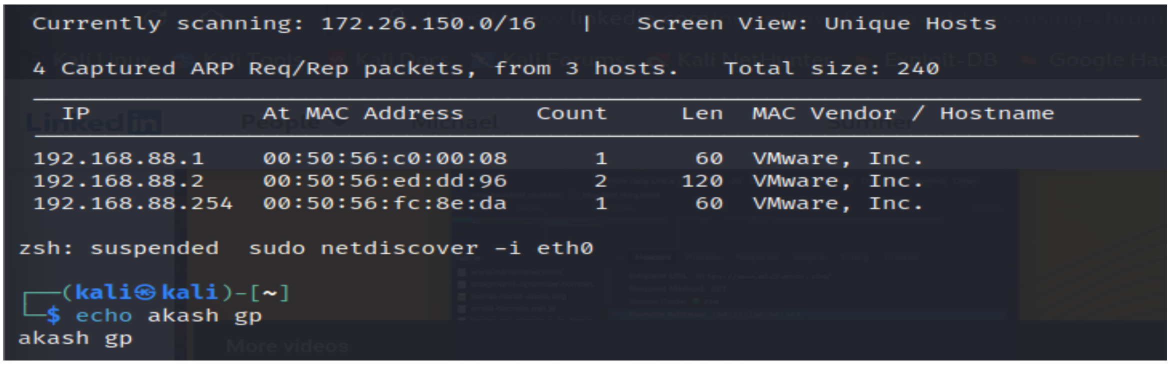
```
0000  00 50 56 f4 4f 45 00 0c  29 b0 85 64 08 00 45 00   ·PV·
0010  00 28 59 3e 40 00 40 06  14 b5 c0 a8 41 82 41 3d   ·(Y>
0020  89 75 e2 d0 00 50 5e 4a  e6 8c 55 84 53 44 50 10   ·u··
0030  ef 88 cc f7 00 00                                  ····
```

The scaled window size (if scaling has been used) (tcp.window_size), 2 bytes   Packets: 72 · Displayed: 72 (100.0%)   Profile: Default

7.Any 5 netdiscover command

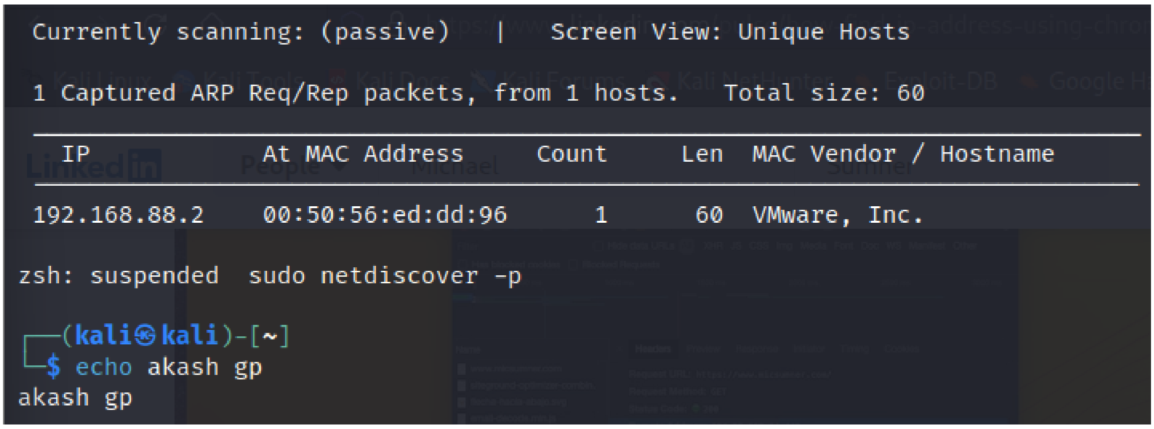
Netdiscover is a network scanning tool used for discovering hosts and gathering information about them on a local network. Here are some of the basic commands:

- $ netdiscover -i eth0



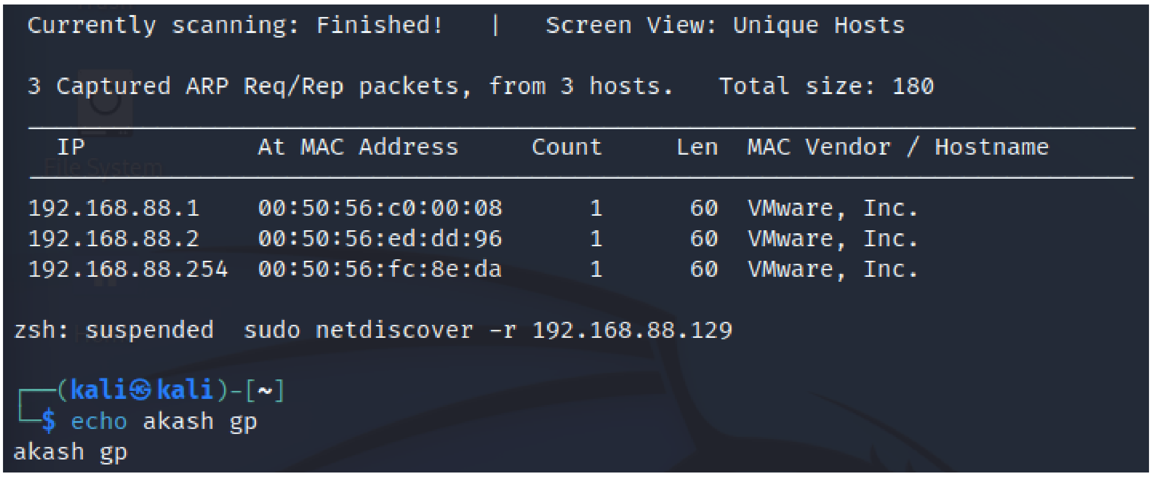
```
 Currently scanning: 172.26.150.0/16   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.88.1    00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.88.2    00:50:56:ed:dd:96      2     120  VMware, Inc.
 192.168.88.254  00:50:56:fc:8e:da      1      60  VMware, Inc.

zsh: suspended  sudo netdiscover -i eth0

┌──(kali㉿kali)-[~]
└─$ echo akash gp
akash gp
```

- $ netdiscover -p



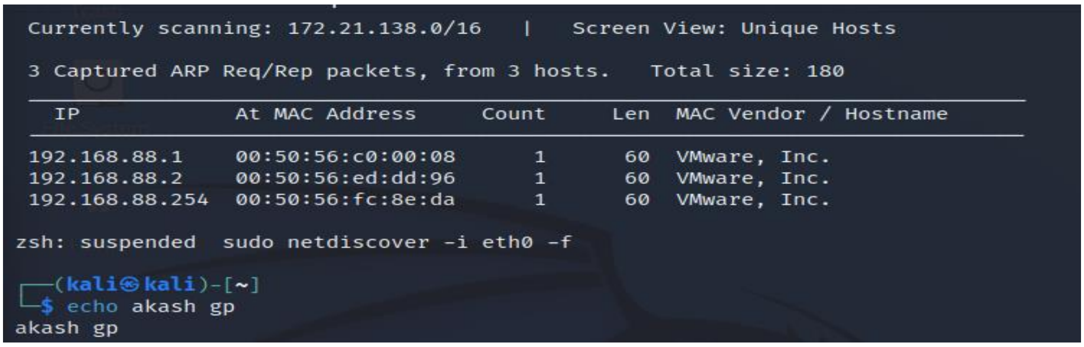
```
 Currently scanning: (passive)   |   Screen View: Unique Hosts

 1 Captured ARP Req/Rep packets, from 1 hosts.   Total size: 60
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.88.2    00:50:56:ed:dd:96      1      60  VMware, Inc.

zsh: suspended  sudo netdiscover -p

┌──(kali㉿kali)-[~]
└─$ echo akash gp
akash gp
```

- $ netdiscover -r 192.168.0.15



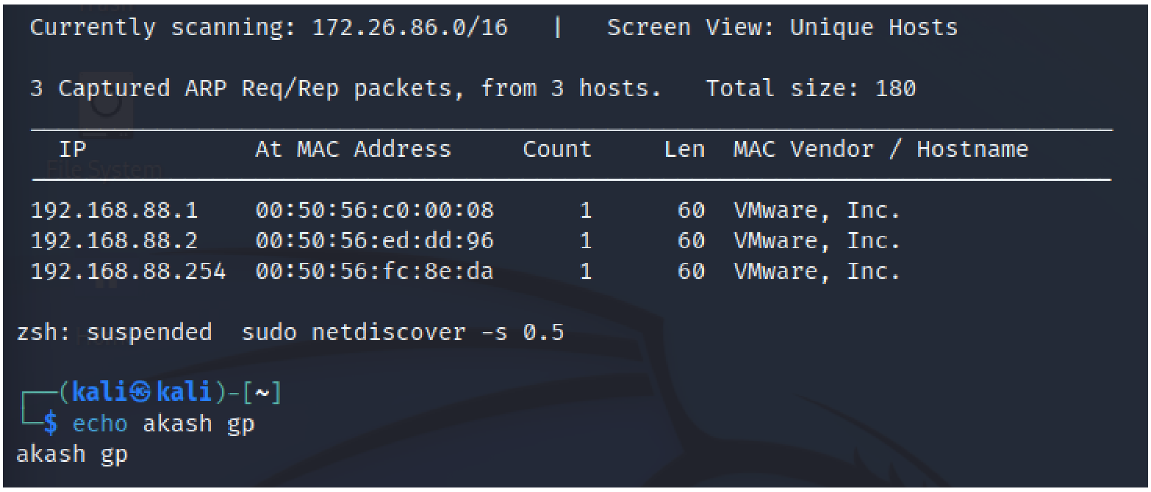
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.88.1    00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.88.2    00:50:56:ed:dd:96      1      60  VMware, Inc.
 192.168.88.254  00:50:56:fc:8e:da      1      60  VMware, Inc.

zsh: suspended  sudo netdiscover -r 192.168.88.129

┌──(kali㉿kali)-[~]
└─$ echo akash gp
akash gp
```

- $ netdiscover -i eth0 -f



```
 Currently scanning: 172.21.138.0/16   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.88.1    00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.88.2    00:50:56:ed:dd:96      1      60  VMware, Inc.
 192.168.88.254  00:50:56:fc:8e:da      1      60  VMware, Inc.

zsh: suspended  sudo netdiscover -i eth0 -f

┌──(kali㉿kali)-[~]
└─$ echo akash gp
akash gp
```

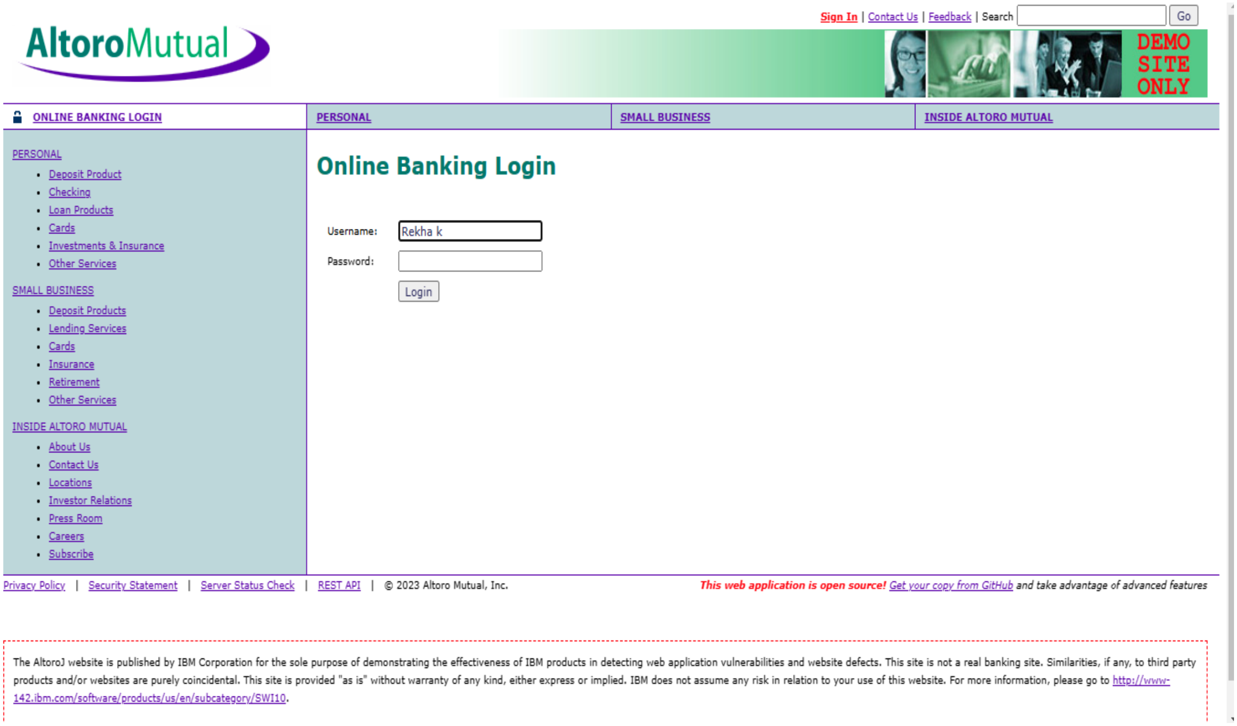
- $ netdiscover –s 0.5



```
Currently scanning: 172.26.86.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 ____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 ____________________________________________________________________________

192.168.88.1    00:50:56:c0:00:08      1       60  VMware, Inc.
192.168.88.2    00:50:56:ed:dd:96      1       60  VMware, Inc.
192.168.88.254  00:50:56:fc:8e:da      1       60  VMware, Inc.

zsh: suspended  sudo netdiscover -s 0.5

┌──(kali㉿kali)-[~]
└─$ echo akash gp
akash gp
```

8.CryptoConfiguration Flaw:

CryptoConfiguration typically refers to the configuration of cryptographic protocols and algorithms used to protect sensitive data and communications.A flaw is context could refers to a weakness or vulnarabilty in the configuration that could that could potentially be exploited by the attackers.



Online Banking Login

Username: Rekha k

Password:

© 2023 Altoro Mutual, Inc.

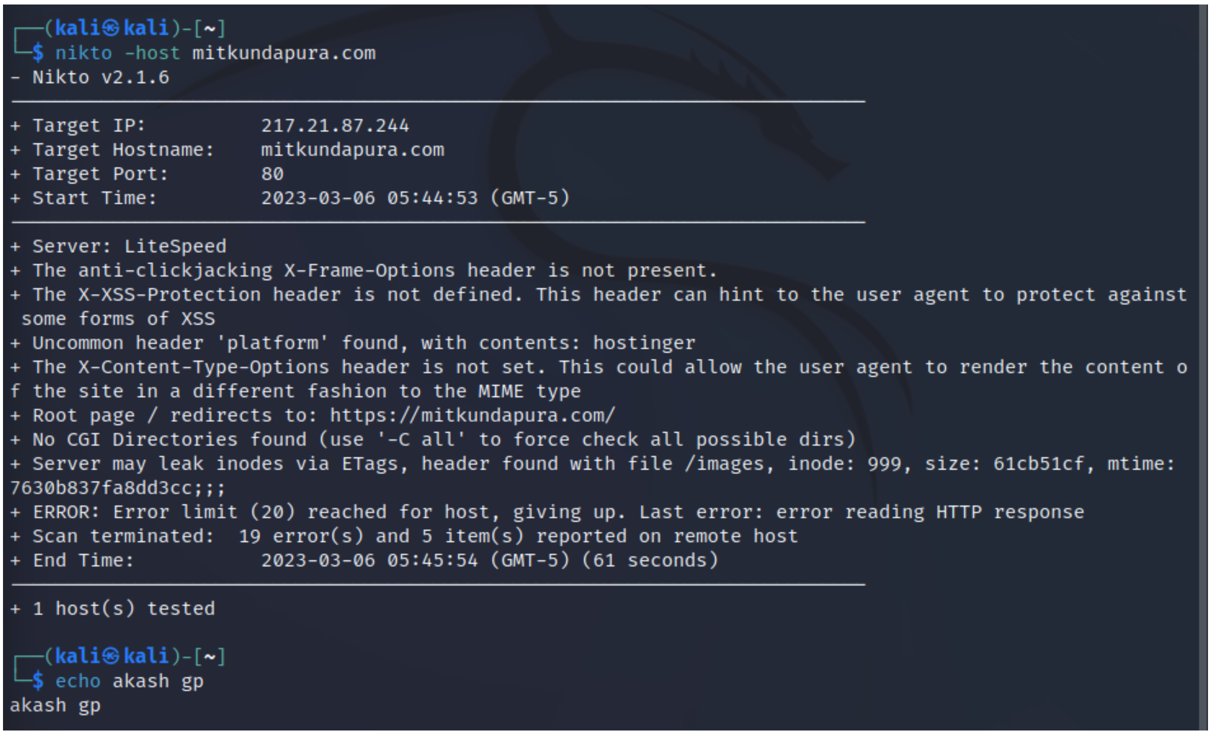
This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

9.Nikto commands:

Nikto is a popular web server scanner that can help you identify potential vulnerabilities on a web server. Here are some common Nikto commands

- $ nikto -host kali.org

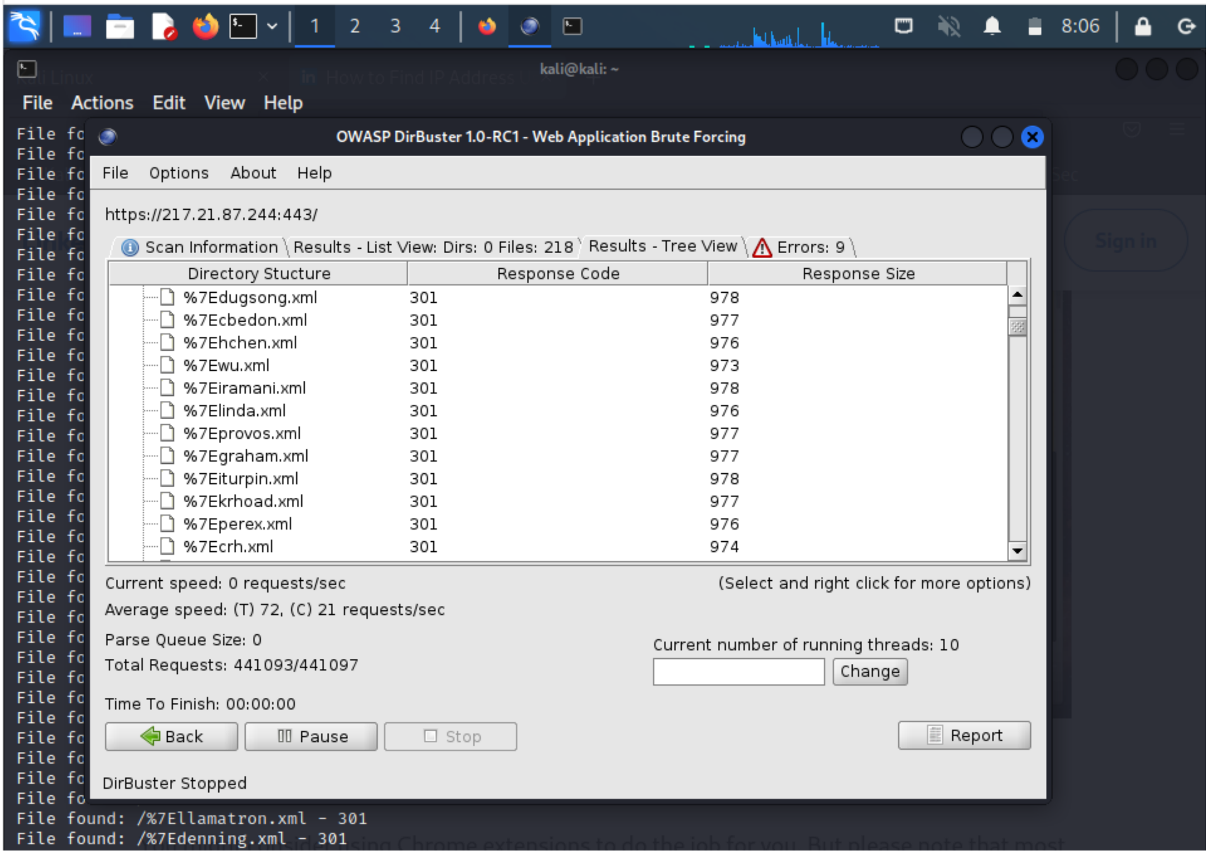


```
┌──(kali㉿kali)-[~]
└─$ nikto -host mitkundapura.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          217.21.87.244
+ Target Hostname:    mitkundapura.com
+ Target Port:        80
+ Start Time:         2023-03-06 05:44:53 (GMT-5)
---------------------------------------------------------------------------
+ Server: LiteSpeed
+ 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
+ Uncommon header 'platform' found, with contents: hostinger
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content o
f the site in a different fashion to the MIME type
+ Root page / redirects to: https://mitkundapura.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /images, inode: 999, size: 61cb51cf, mtime:
7630b837fa8dd3cc;;;
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated:  19 error(s) and 5 item(s) reported on remote host
+ End Time:           2023-03-06 05:45:54 (GMT-5) (61 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~]
└─$ echo akash gp
akash gp
```

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.

DirBuster is a tool created to discover, by brute force, the existing files and directories in a web server. We will use it in this recipe to search for a specific list of files and directories.



https://217.21.87.244:443/

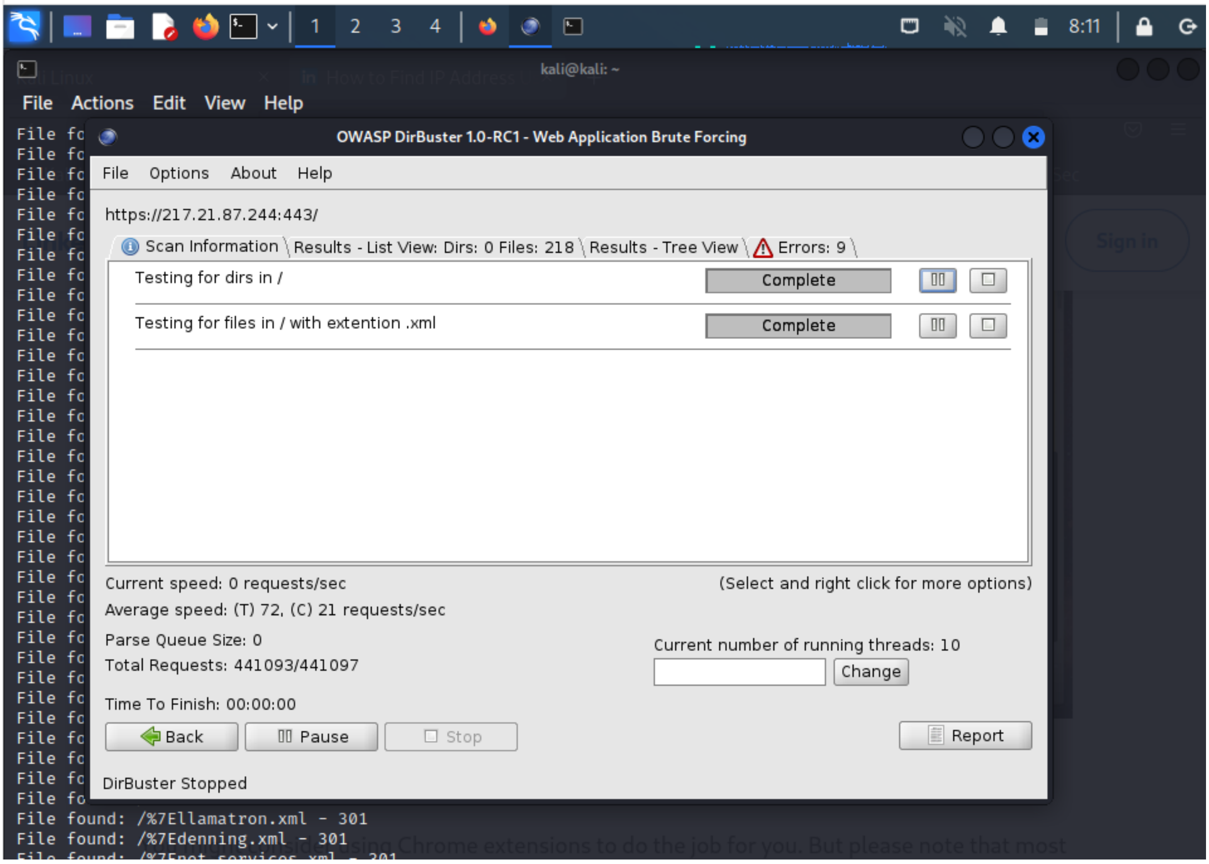
Scan Information \ Results - List View: Dirs: 0 Files: 218 \ Results - Tree View \ Errors: 9 \

Directory Stucture	Response Code	Response Size
%7Edugsong.xml	301	978
%7Ecbedon.xml	301	977
%7Ehchen.xml	301	976
%7Ewu.xml	301	973
%7Eiramani.xml	301	978
%7Elinda.xml	301	976
%7Eprovos.xml	301	977
%7Egraham.xml	301	977
%7Eiturpin.xml	301	978
%7Ekrhoad.xml	301	977
%7Eperex.xml	301	976
%7Ecrh.xml	301	974

Current speed: 0 requests/sec
(Select and right click for more options)
Average speed: (T) 72, (C) 21 requests/sec
Parse Queue Size: 0
Current number of running threads: 10
Total Requests: 441093/441097
Time To Finish: 00:00:00

DirBuster Stopped

```
File found: /%7Ellamatron.xml - 301
File found: /%7Edenning.xml - 301
```



https://217.21.87.244:443/

Scan Information \ Results - List View: Dirs: 0 Files: 218 \ Results - Tree View \ Errors: 9 \

Testing for dirs in / Complete

Testing for files in / with extention .xml Complete

Current speed: 0 requests/sec
(Select and right click for more options)
Average speed: (T) 72, (C) 21 requests/sec
Parse Queue Size: 0
Current number of running threads: 10
Total Requests: 441093/441097
Time To Finish: 00:00:00

DirBuster Stopped

```
File found: /%7Ellamatron.xml - 301
File found: /%7Edenning.xml - 301
File found: /%7Enet_services.xml - 301
```