

Name:Prasheela

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 randomized numbers, either to mask the sender's identity or to launch a reflected DDoS attack, as described below.

Command:

```
$ ifconfig eth0 192.168.29.12
```

```
$ ifconfig
```

```
(root@kali)-[~]
# ifconfig eth0 192.168.30.13

(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.30.13 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 "prasheela"
prasheela
```

2. MAC address spoofing

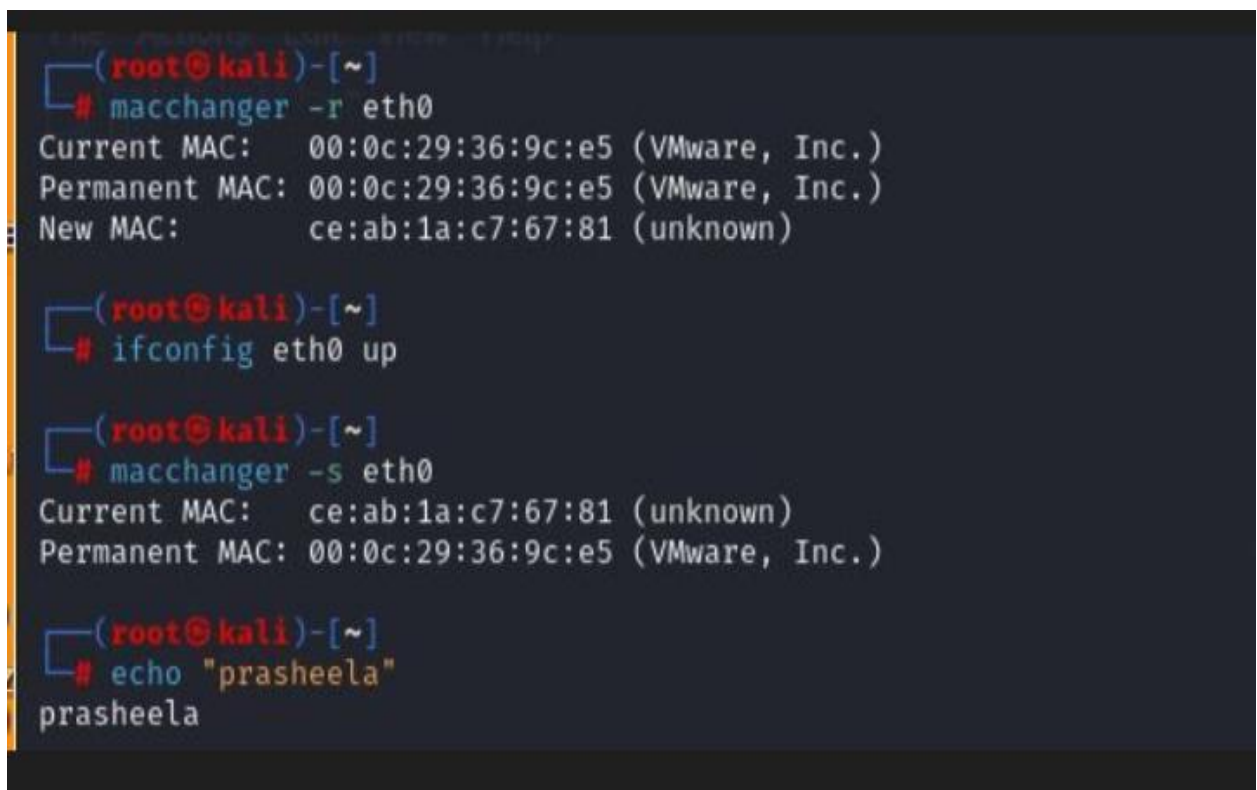
MAC Spoofing is a type of attack used to exploit flaws in the authentication mechanism implemented by wired and wireless networking hardware. In layman's terms, MAC spoofing is when someone or something intercepts, manipulate or otherwise tampers with the control messages exchanged between a networked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

Command:

```
$ macchanger -r eth0
```

```
$ ifconfig eth0 up
```

```
$ macchanger -s eth0
```

A terminal window on a Kali Linux system showing the process of MAC address spoofing. The user is at the root prompt. They run 'macchanger -r eth0', which shows the current MAC as 00:0c:29:36:9c:e5 (VMware, Inc.) and the new MAC as ce:ab:1a:c7:67:81 (unknown). Then they run 'ifconfig eth0 up'. Next, they run 'macchanger -s eth0', which shows the current MAC as ce:ab:1a:c7:67:81 (unknown) and the permanent MAC as 00:0c:29:36:9c:e5 (VMware, Inc.). Finally, they run 'echo "prasheela"', which outputs 'prasheela'.

```
(root@kali)-[~]  
# macchanger -r eth0  
Current MAC: 00:0c:29:36:9c:e5 (VMware, Inc.)  
Permanent MAC: 00:0c:29:36:9c:e5 (VMware, Inc.)  
New MAC: ce:ab:1a:c7:67:81 (unknown)  
  
(root@kali)-[~]  
# ifconfig eth0 up  
  
(root@kali)-[~]  
# macchanger -s eth0  
Current MAC: ce:ab:1a:c7:67:81 (unknown)  
Permanent MAC: 00:0c:29:36:9c:e5 (VMware, Inc.)  
  
(root@kali)-[~]  
# echo "prasheela"  
prasheela
```

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], LiteSpeed, RedirectLocation[https://mitkundapura.com/], Title[301 Moved Permanently][This domain contains no links], UncommonHeaders[platform,content-security-policy]  
https://mitkundapura.com/ [200 OK] Bootstrap, Country[UNITED KINGDOM][GB], Email[office@mitkundapura.com], HTML5, HTTPServer[LiteSpeed], IP[217.21.87.244], JQuery, LiteSpeed, PHP[7.4.33], PoweredBy[Kodiga], Script, Title[RITH- Noodlalattu Institute of Technology & Management, Kundapura Home], UncommonHeaders[platform,content-security-policy,all-svc], X-Powered-By[PHP/7.4.33]  
  
(root@kali) ~  
$ echo "prashwela"  
prashwela
```

\$ 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.com/]  
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[JSESSIONID], Country[UNITED STATES][U
le[Altoro Mutual]

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

\$ 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 "prasheela"
prasheela
```

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 "prasheela"
prasheela
```

```
$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 "prasheela"
prasheela
```

\$ 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:

# nslookup mitkundapura.com
Nikto v2.1.6

(root@kali)-[~]
# echo "prasheela"
prasheela
```

\$ 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 = 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.
mitkundapura.com    mail exchanger = 10 alt3.aspmx.l.google.com.

Authoritative answers can be found from:

# nslookup mitkundapura.com

(root@kali)-[~]
# echo "prasheela"
prasheela
```


\$nslookup -debug mitkundapura.com

```
(root@kali)-[~]
# 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 "prasheela"
```

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 <jpenalba@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 "prasheela"
prasheela
```

\$ 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 <jpenalba@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 "prasheela"
prasheela
```

\$ netdiscover -r 192.168.29.0/24

```
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240



| 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.          |
| 192.168.29.131 | 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 "prasheela"
prasheela
```

\$ netdiscover -r 192.168.29.0/24 -P

```
(root@kali)-[~]
# netdiscover -r 192.168.29.0/24 -P
-- Active scan completed, 3 Hosts found.



| 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.          |



(root@kali)-[~]
# echo "prasheela"
prasheela
```

\$ netdiscover -r 192.168.1.0/24 -PN

```
(root@kali)-[~]
# netdiscover -r 192.168.29.0/24 -PN
-- Active scan completed, 3 Hosts found.



| 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.          |



(root@kali)-[~]
# echo "prasheela"
prasheela
```

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 mitkundapura.com

```
(root@kali)-[~]
# nikto -h mitkundapura.com
- Nikto v2.1.6

+ Target IP: 217.21.87.244
+ Target Hostname: mitkundapura.com
+ Target Port: 80
+ Start Time: 2023-03-03 10:59:03 (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
+ 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 of the
+ 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: 7630
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 5 item(s) reported on remote host
+ End Time: 2023-03-03 10:59:36 (GMT-5) (33 seconds)

+ 1 host(s) tested

(root@kali)-[~]
# echo "prasheela"
prasheela
```

8. Crypto 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.

Altoro Mutual

[Sign In](#) | [Contact Us](#) | [Feedback](#) | [Search](#)

ONLINE BANKING LOGIN | **PERSONAL** | **SMALL BUSINESS** | **INSIDE ALTORO MUTUAL**

PERSONAL

- [Deposit Products](#)
- [Checking](#)
- [Loan Products](#)
- [Cards](#)
- [Investments & Insurance](#)
- [Other Services](#)

SMALL BUSINESS

- [Deposit Products](#)
- [Lending Services](#)
- [Cards](#)
- [Insurance](#)
- [Referrals](#)
- [Other Services](#)

INSIDE ALTORO MUTUAL

- [About Us](#)
- [Contact Us](#)
- [Locations](#)
- [Investor Relations](#)
- [Press Room](#)
- [Careers](#)
- [Subscribe](#)

Online Banking Login

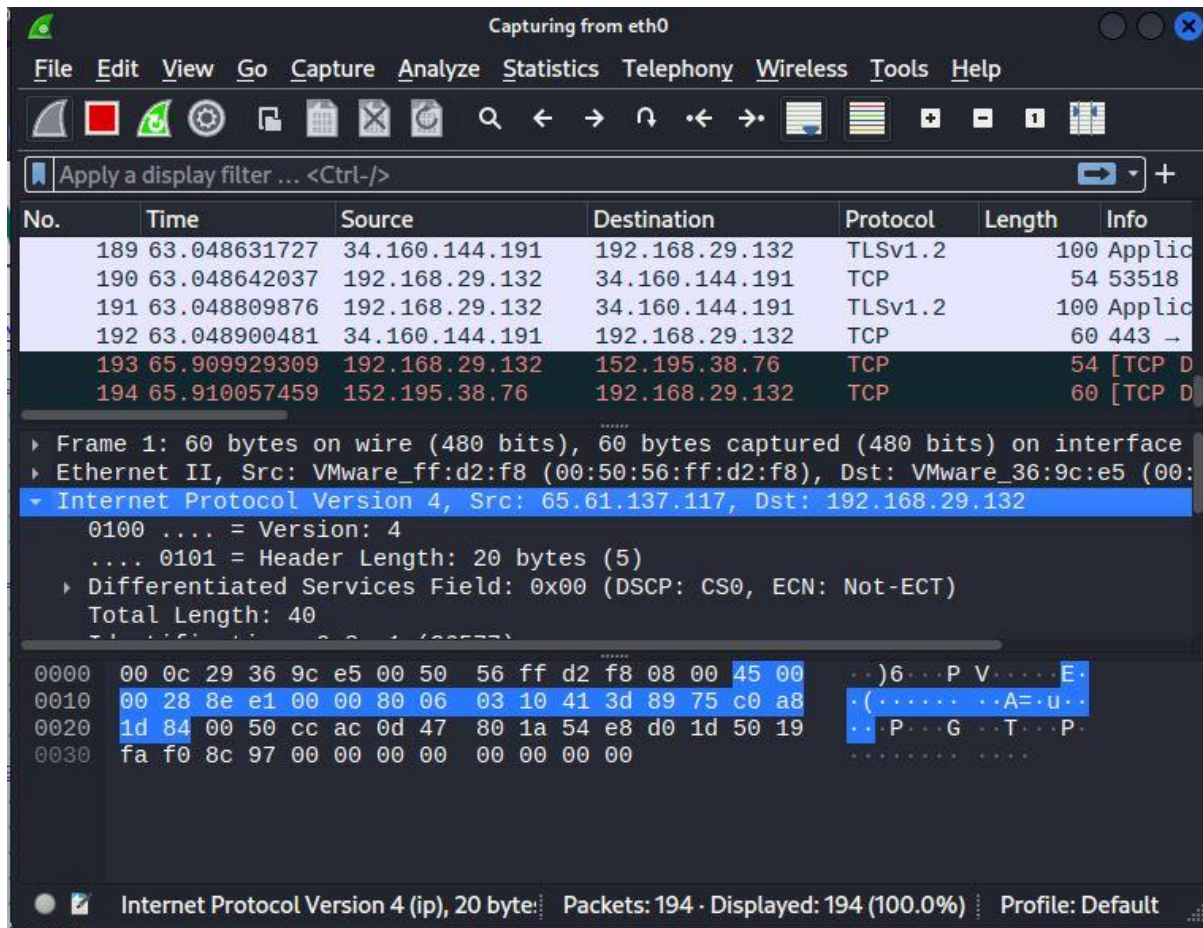
Username:

Password:

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2023 Altoro Mutual, Inc. **This web application is open source! Get your copy from GitHub and take advantage of advanced features.**

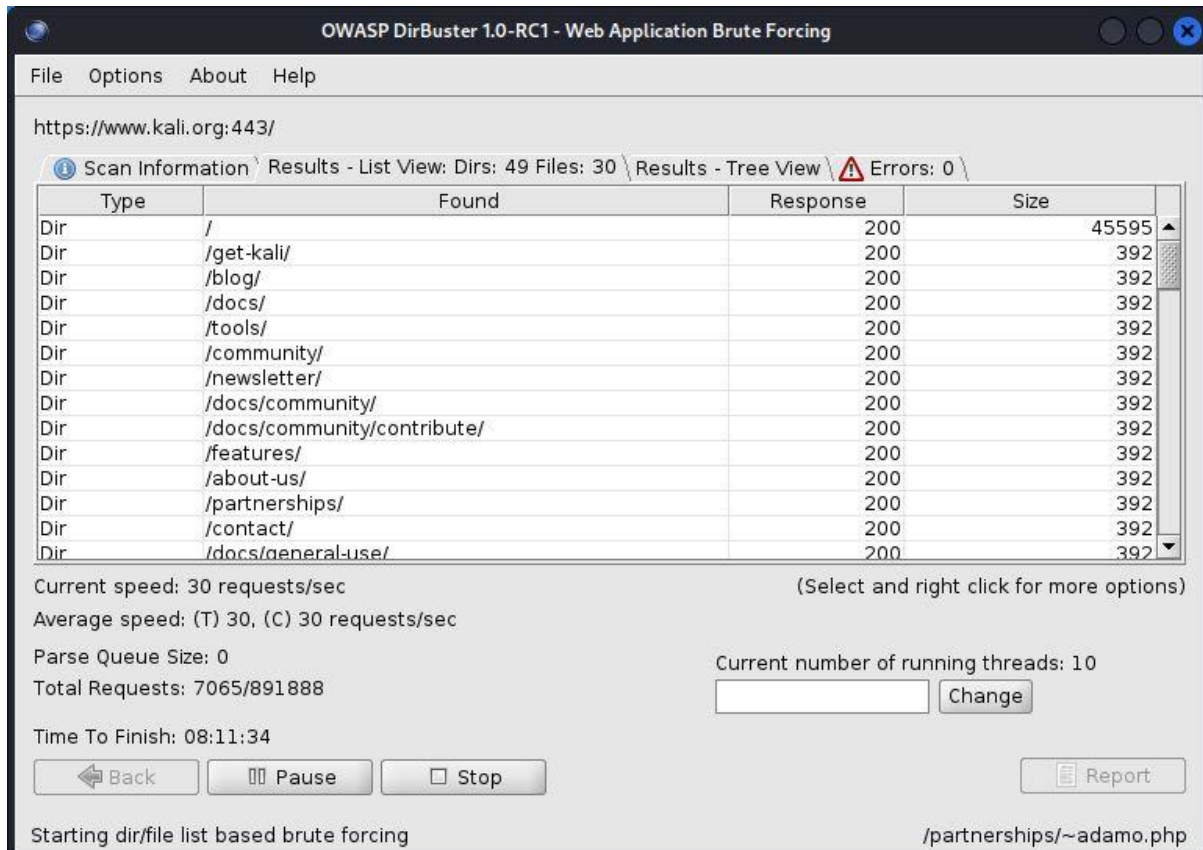
9. Find data packet using Wireshark

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.



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.



The screenshot shows the OWASP DirBuster 1.0-RC1 application window. The title bar reads "OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing". The menu bar includes "File", "Options", "About", and "Help". The address bar shows "https://www.kali.org:443/". Below the address bar, there are tabs for "Scan Information", "Results - List View: Dirs: 49 Files: 30", "Results - Tree View", and "Errors: 0". The main display area shows a table of scan results:

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

Below the table, the following statistics are displayed:

- Current speed: 30 requests/sec
- Average speed: (T) 30, (C) 30 requests/sec
- Parse Queue Size: 0
- Total Requests: 7065/891888
- Time To Finish: 08:11:34
- Current number of running threads: 10

At the bottom, there are buttons for "Back", "Pause", "Stop", and "Report". The status bar at the bottom left says "Starting dir/file list based brute forcing" and the bottom right shows the current path: "/partnerships/~adamo.php".