Government Polytechnic College Udupi

Name: Pooja

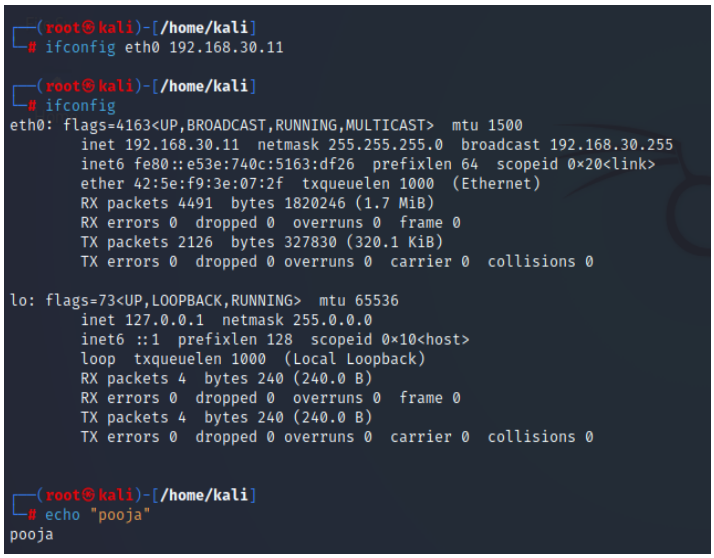
Register no: 145CS20010

Task report: 2

1)Perform IP address spoofing

Ip spoofing is a technique used to change the source ip address in an IP packet. This can be used to hide the true source of the traffic, or to make it appear as if it is coming from a different location. Ip spoofing can be used for malicious purposes, such as DDoS attacks, or simply to make it more difficult to track down the source of a problem.

Command :ifconfig eth0 <ip address>



2) perform Mac address spoofing

MAC changer is an utility that makes the maniputation of MAC addresses of network interface easier. MAC addresses are unique identifiers on networks, they only need to be, unique they can be changed on most network hardware.

Command: execute macchanger with an option -s and an argument eth0.

```
# macchanger -s eth0
```

- **Use ifconfig command to turn off your network interface**

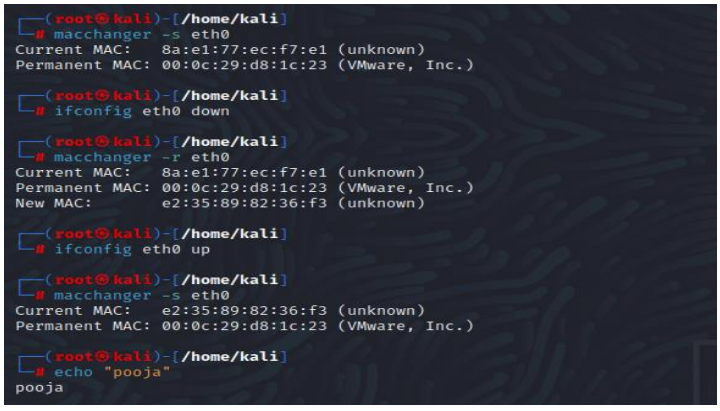
```
# ifconfig eth0 down.
```

- **change network card's hardware MAC address to some random hexadecimal numbers**:

```
# macchanger -r eth0
```

- **network interface up and display your new MAC address:**

```
# ifconfig eth0 down
# macchanger -s eth0
```



3)Whatweb

Whatweb identifies websites. It recognises web technologies including content management system, blogging platforms, JavaScript libraries and embedded devices. Whatweb has over 900 plugins, each to recognise something different. It also identifies version numbers, email address, account id and more.

Command: whatweb <url>

whatweb mitkundapura.com

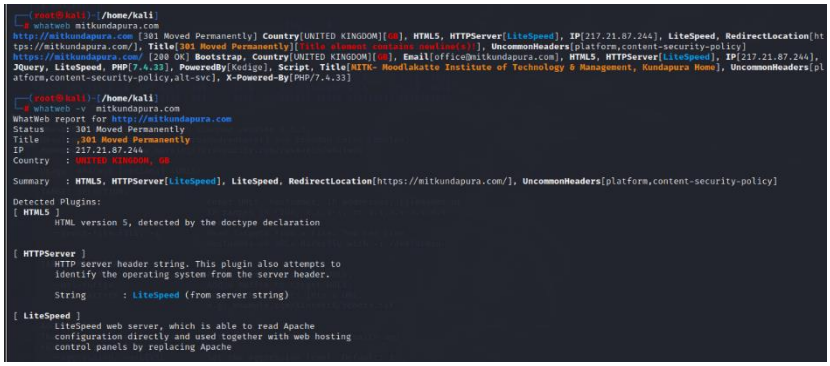
To give a more verbose Output

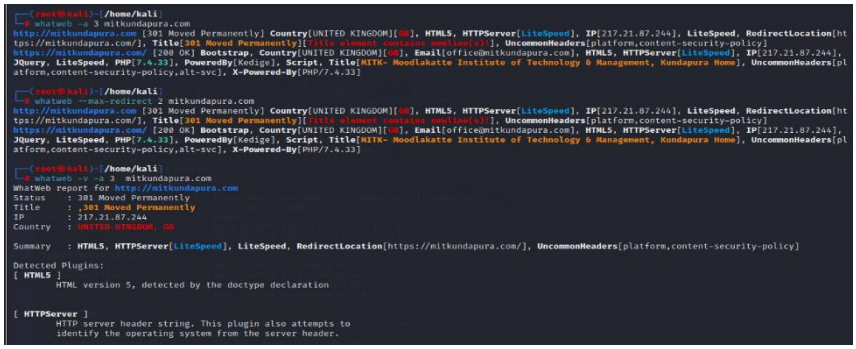
Whatweb -v mitkundapura.com

whatweb -a 3 mitkundapura.com

whatweb --max-redirect 2 mitkundapura.com

whatweb -v -a 3 mitkundapura.com





4)nslookup

Nslookup (stands for “Name Server Lookup”) is a useful command for getting information from DNS server. It is a network administration tool for querying the DNS to obtain domain name or IP address mapping or any other specific DNS record. It also used to troubleshoot DNS-related problems.

Command: nslookup followed by the domain name will display the "A Record" (IP address) of the domain.

nslookup google.com

- **SOA record provides the authoritative information about the domain, e-mail, the serial numbers etc…**

  # nslookup -type==soa google.com

- **NS (name server) it will output the name serves which are associated with given domains.**

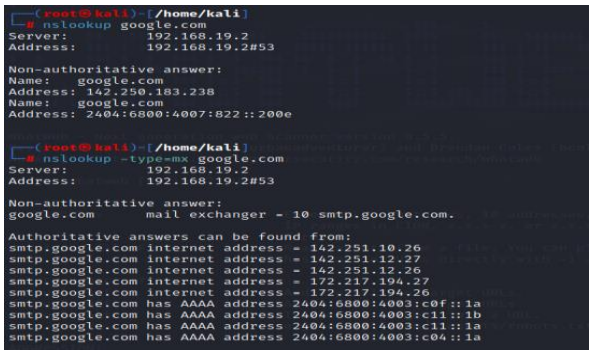
  # nslookup -type=ns google.com

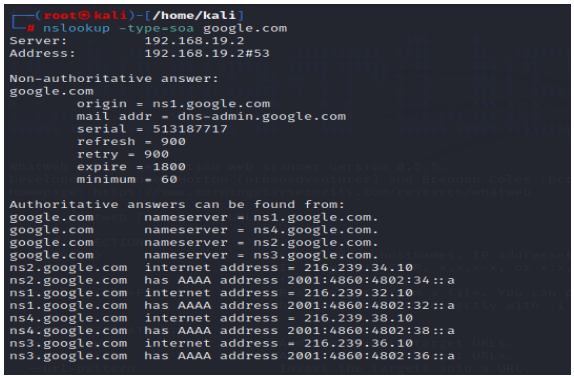
- **MX (mail exchange) record maps a domain name to list of mail exchange servers for that domain.**

  # nslookup -type=mx google.com

- **To view information useful for debugging, use the debug option**

  # nslookup -debug google.com





```
┌──(root㉿kali)-[/home/kali]
└─# nslookup -type=ns google.com
Server:         192.168.19.2
Address:        192.168.19.2#53

Non-authoritative answer:
google.com      nameserver = ns1.google.com.
google.com      nameserver = ns4.google.com.
google.com      nameserver = ns2.google.com.
google.com      nameserver = ns3.google.com.

Authoritative answers can be found from:
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  has AAAA address 2001:4860:4802:38::a
ns2.google.com  internet address = 216.239.34.10
ns2.google.com  has AAAA address 2001:4860:4802:34::a
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  has AAAA address 2001:4860:4802:36::a


┌──(root㉿kali)-[/home/kali]
└─# nslookup -debug google.com
Server:         192.168.19.2
Address:        192.168.19.2#53

------------
    QUESTIONS:
        google.com, type = A, class = IN
    ANSWERS:
    ->  google.com
        internet address = 142.250.183.238
        ttl = 5
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Non-authoritative answer:
Name:   google.com
Address: 142.250.183.238
------------
    QUESTIONS:
        google.com, type = AAAA, class = IN
    ANSWERS:
    ->  google.com
        has AAAA address 2404:6800:4007:822::200e
        ttl = 5
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Name:   google.com
Address: 2404:6800:4007:822::200e


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

5) Whois

The whois command displays information about a website's record. You may get all the information about a website regarding its registration and owner's information.

Syntax: whois<website name>

Command : # whois mitkundapura.com

```
┌──(root㉿kali)-[/home/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: 2023-03-03T09:44:29Z <<<

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
```

```
; 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.


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

6) Nikto

Nikto is an open-source command- line vulnerability scanner that scans web servers for potentially dangerous files, outdated versions, server configuration files and other problems. It is popular, easy-to-use, and very powerful pen testing tool.

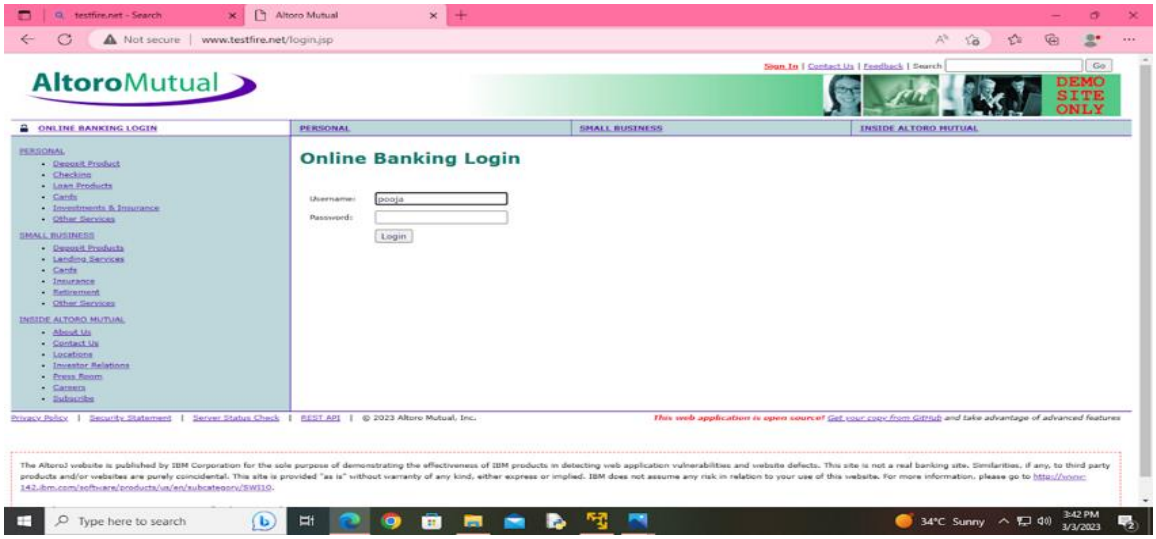
Syntax: nikto -h <website name>

Command: # nikto -h mitkundapura.com

```
┌──(kali㉿kali)-[~]
└─$ nikto -h mitkundapura.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          217.21.87.244
+ Target Hostname:    mitkundapura.com
+ Target Port:        80
+ Start Time:         2023-03-02 23:46:11 (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 of 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:  20 error(s) and 5 item(s) reported on remote host
+ End Time:           2023-03-02 23:46:47 (GMT-5) (36 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

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

7) Crypto configuration flaw

A cryptographic failure is a critical web application security vulnerability that exposes sensitive application data on a weak or non-existent cryptographic algorithm. Those can be passwords, patient health records, business secrets, credit card information, email addresses, or other personal user information.



8) Netdiscover

Netdiscover is a simple ARP scanner that can be used to scan for live hosts in a network. It can scan for multiple subnets also. It simply produces the output in a live display(ncurse). This can be used in the first phases of a pentest where you have access to a network. Netdiscover is a simple initial-recon tool that can be very handy.

Command: **To view the usage options.**

```
# netdiscover -h
```

- **use following command to check the IP Address:**

```
# ifconfig
```

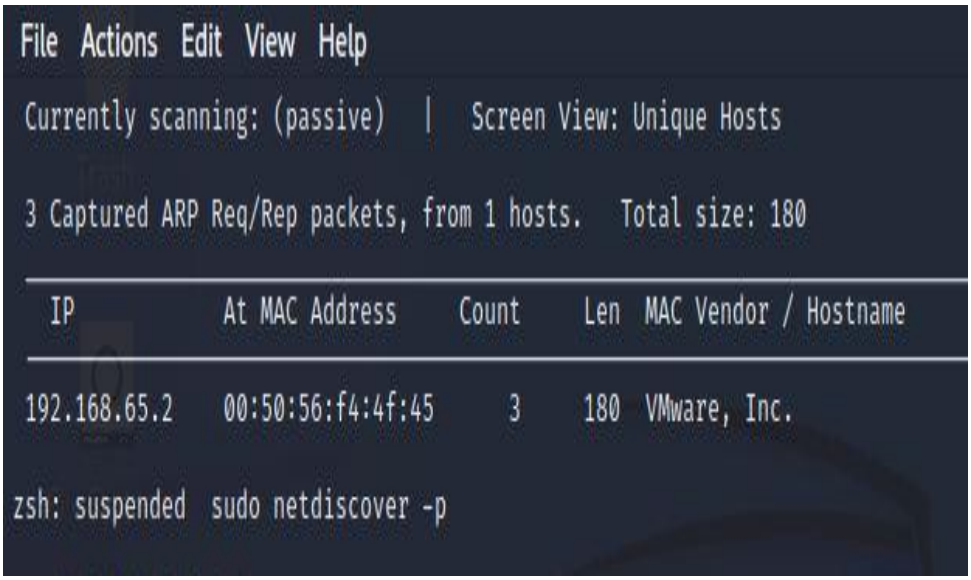
- **We can scan a specific range with -r option**

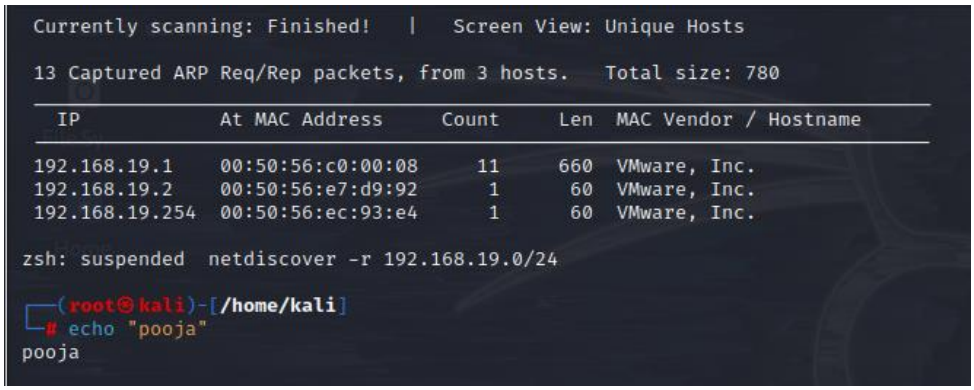
netdiscover -r 192.168.19.0/24

```
┌──(root㉿kali)-[/home/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)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.19.132  netmask 255.255.255.0  broadcast 192.168.19.255
        inet6 fe80::e53e:740c:5163:df26  prefixlen 64  scopeid 0x20<link>
        ether 42:5e:f9:3e:07:2f  txqueuelen 1000  (Ethernet)
        RX packets 8493  bytes 3321127 (3.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4342  bytes 571067 (557.6 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)-[/home/kali]
└─# netdiscover 192.168.19.132
Invalid extra argument: 192.168.19.132

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)
```

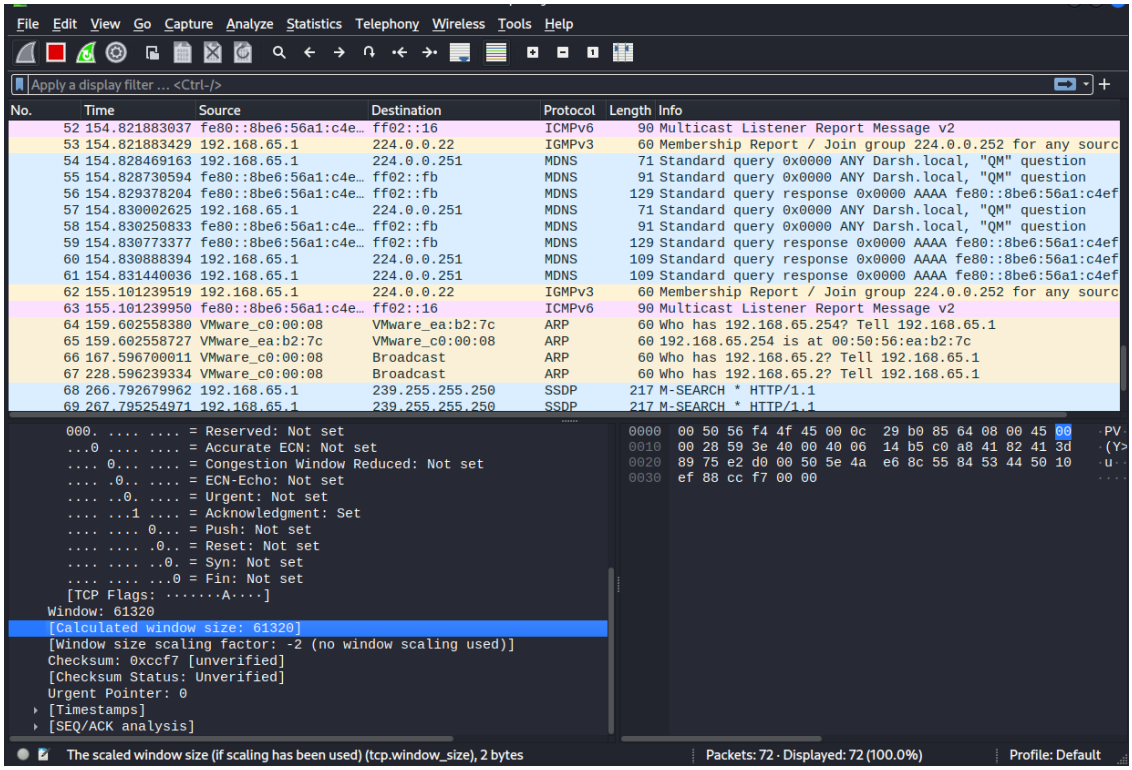
```
Currently scanning: 172.19.249.0/16   |   Screen View: Unique Hosts

10 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 600

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname

192.168.65.1    00:50:56:c0:00:08      2     120  VMware, Inc.
192.168.65.2    00:50:56:f4:4f:45      6     360  VMware, Inc.
192.168.65.254  00:50:56:ea:b2:7c      2     120  VMware, Inc.

zsh: suspended  sudo netdiscover -d -i eth0
```





9) Find data packet using wireshark

Wireshark is a network “sniffer” a tool that captures and analyse packets off wire. Wireshark is an open source network protocol analyzer that helps us to see what is happening inside a network when we try to communicate with other networks.

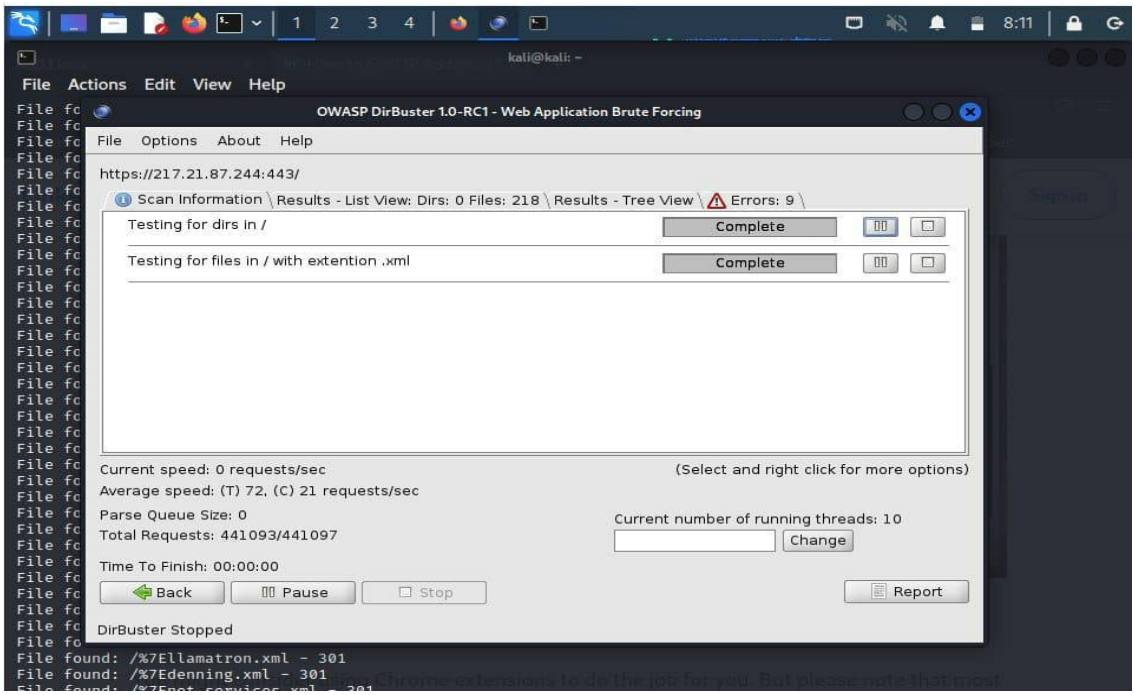


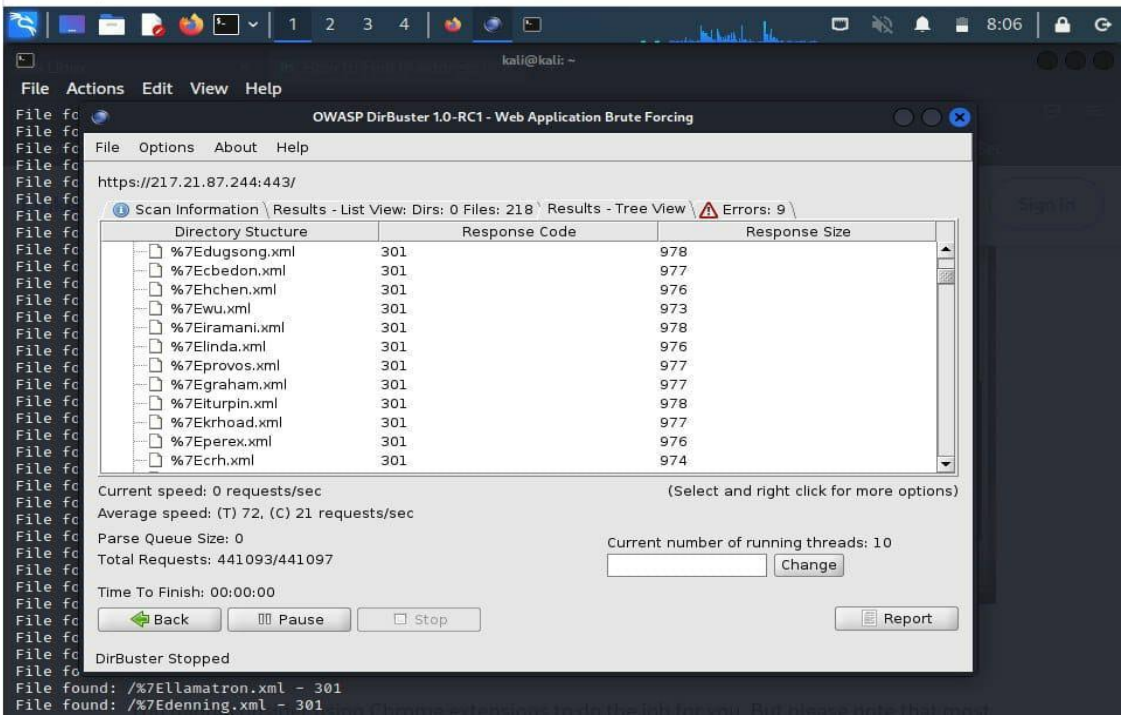
10) Find XML pages in website using Dirbuster

DirBuster is a multi threaded java application designed to brute force directories and files names on web/application servers.

Dirbuster is used once you have scanned an IP address and found any vulnerabilities. DirBuster will help you map out the application. Building a directory of the target site is useful in finding as many potential points of entry to the target.

For a developer, DirBuster can help you to increase the security of your application by finding content on the web server or within the application that is not required (or shouldn't even be public) or by helping developers understand that by simply not linking to a page does not mean it can not be accessed.


kali@kali: ~
File Actions Edit View Help
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
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
Total Requests: 441093/441097
Current number of running threads: 10
Change
Time To Finish: 00:00:00
Back
Pause
Stop
Report
DirBuster Stopped
File found: /%7Ellamatron.xml - 301
File found: /%7Edenning.xml - 301


kali@kali: ~
File Actions Edit View Help
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
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
Total Requests: 441093/441097
Current number of running threads: 10
Change
Time To Finish: 00:00:00
Back
Pause
Stop
Report
DirBuster Stopped
File found: /%7Ellamatron.xml - 301
File found: /%7Edenning.xml - 301