8/14/2021

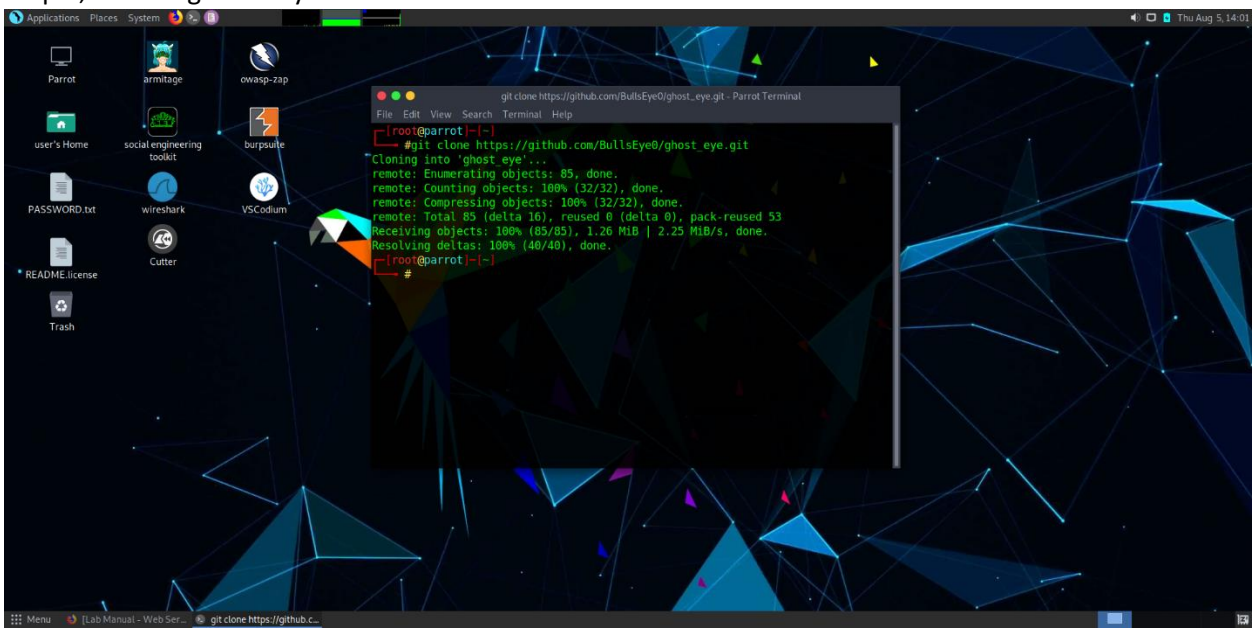
LAB ACTIVITIES

Table of Contents

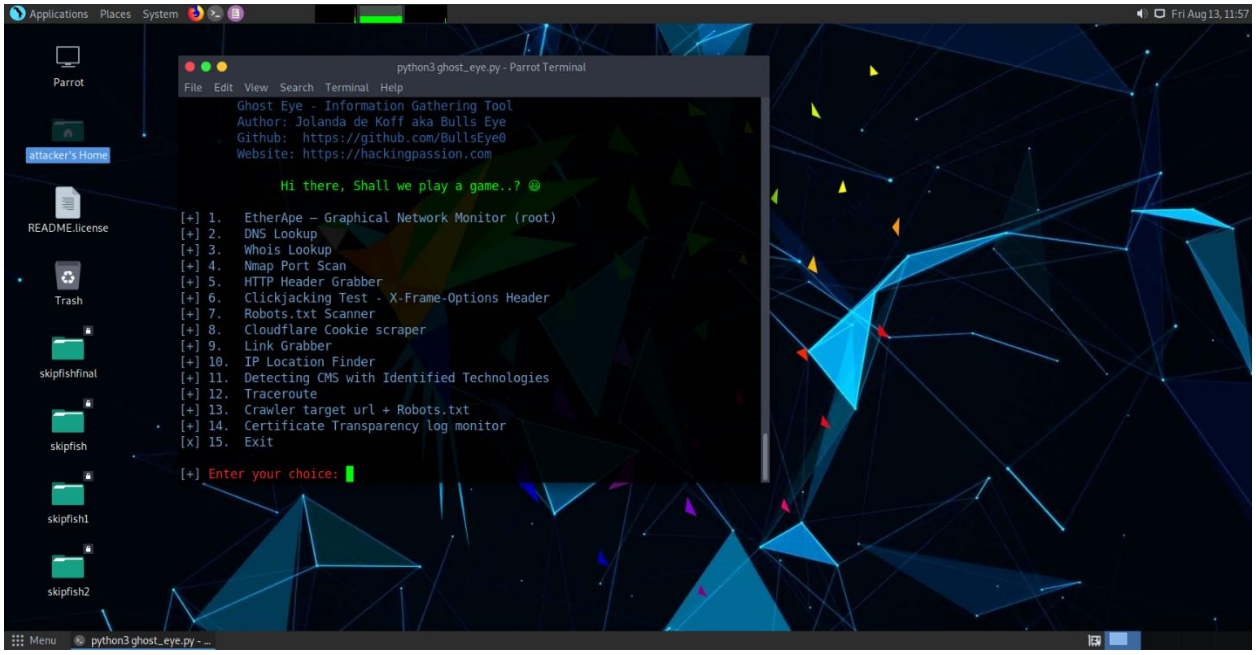
Task 1: Information gathering using GhostEye

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

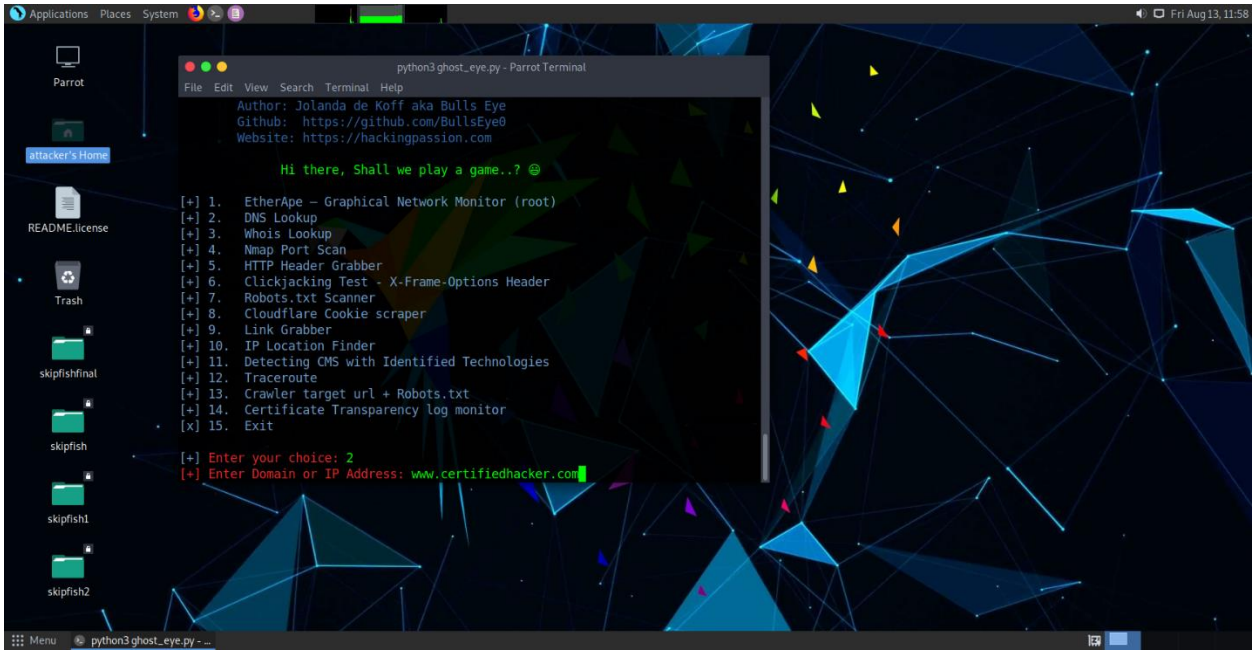


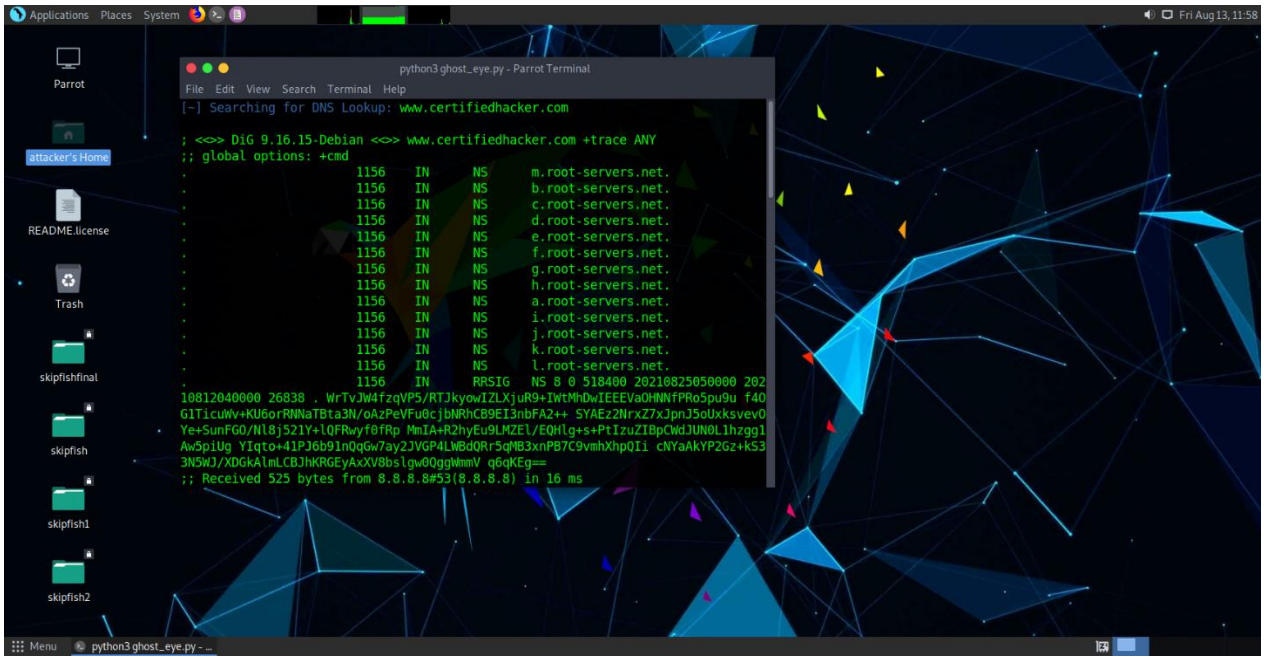
Step2: Do **sudo su and enter the ParrotOS password**. Then do **cd**. Use the command cd ghost_eye. Use the command **python3 ghost_eye.py** to start GhostEye

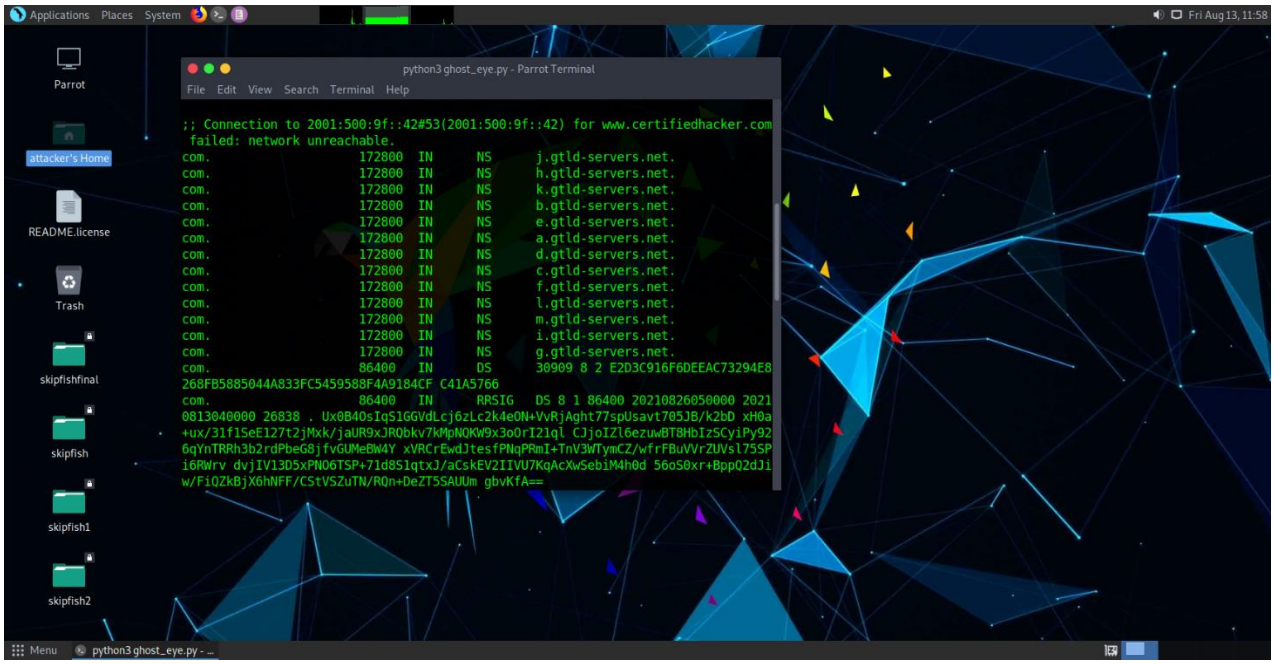


Step 3: from here it is mostly selecting the option and entering the target domain

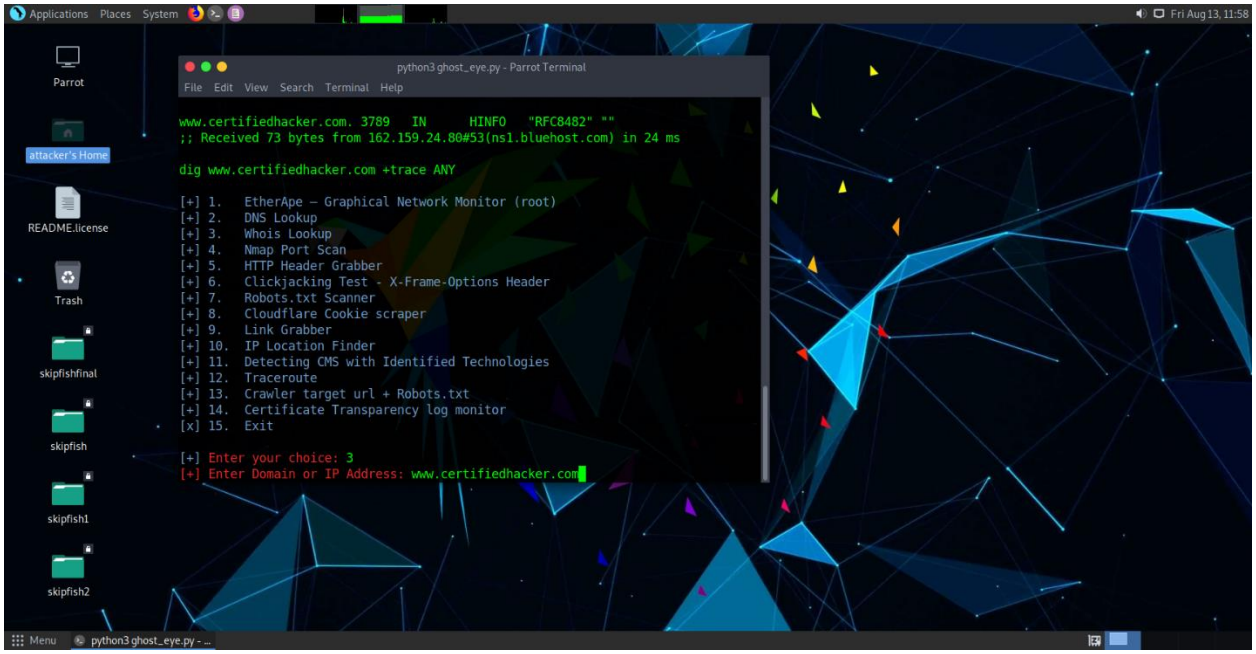
Step 4: Starting with DNS **Lookup**

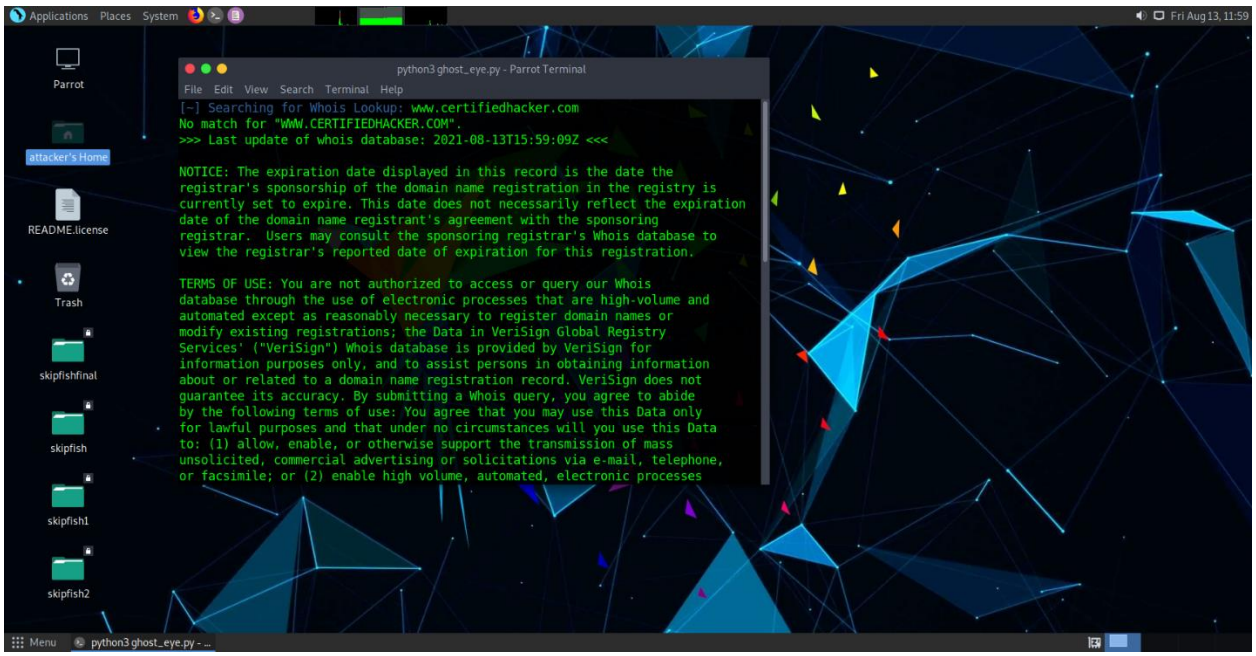



Applications Places System
Fri Aug 13, 11:58
Parrot
attacker's Home
README.license
Trash
skipfishfinal
skipfish
skipfish1
skipfish2
python3 ghost_eye.py - Parrot Terminal
File Edit View Search Terminal Help
[~] Searching for DNS Lookup: www.certifiedhacker.com
; <<>> DiG 9.16.15-Debian <<>> www.certifiedhacker.com +trace ANY
;; global options: +cmd
. 1156 IN NS m.root-servers.net.
. 1156 IN NS b.root-servers.net.
. 1156 IN NS c.root-servers.net.
. 1156 IN NS d.root-servers.net.
. 1156 IN NS e.root-servers.net.
. 1156 IN NS f.root-servers.net.
. 1156 IN NS g.root-servers.net.
. 1156 IN NS h.root-servers.net.
. 1156 IN NS a.root-servers.net.
. 1156 IN NS i.root-servers.net.
. 1156 IN NS j.root-servers.net.
. 1156 IN NS k.root-servers.net.
. 1156 IN NS l.root-servers.net.
. 1156 IN RRSIG NS 8 0 518400 20210825050000 202
10812040000 26838 . WrTvJW4fzqVP5/RTJkyowIZLXjuR9+IWtMhDwIEEEVaOHNNfPRo5pu9u f4O
G1TicuWv+KU6orRNNaTBta3N/oAzPeVFu0cjbNRhCB9EI3nbFA2++ SYAEz2NrxZ7xJpnJ5oUxksvevO
Ye+SunFGO/Nl8j521Y+lQFRwyf0fRp MmIA+R2hyEu9LMZEl/EQHlg+s+PtIzuZIBpCWdJUN0L1hzgg1
Aw5piUg YIqto+41PJ6b91nQqGw7ay2JVGP4LWBdQRr5qMB3xnPB7C9vmhXhpQIi cNYaAkYP2Gz+kS3
3N5WJ/XDGkAlmLCBJhKRGEyAxXV8bslgw0QggWmmV q6qKEg==
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 16 ms
Menu
python3 ghost_eye.py - ...

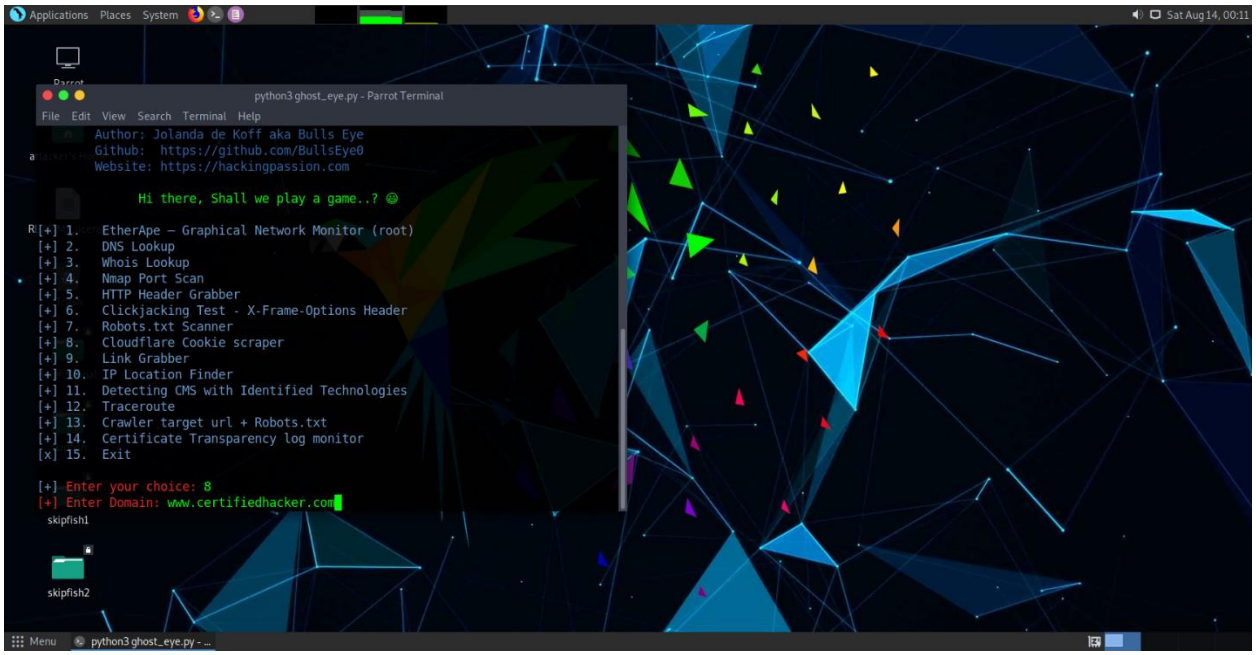

Applications Places System
Fri Aug 13, 11:58
Parrot
attacker's Home
README.license
Trash
skipfishfinal
skipfish
skipfish1
skipfish2
python3 ghost_eye.py - Parrot Terminal
File Edit View Search Terminal Help
;; Connection to 2001:500:9f::42#53(2001:500:9f::42) for www.certifiedhacker.com
failed: network unreachable.
com. 172800 IN NS j.gtld-servers.net.
com. 172800 IN NS h.gtld-servers.net.
com. 172800 IN NS k.gtld-servers.net.
com. 172800 IN NS b.gtld-servers.net.
com. 172800 IN NS e.gtld-servers.net.
com. 172800 IN NS a.gtld-servers.net.
com. 172800 IN NS d.gtld-servers.net.
com. 172800 IN NS c.gtld-servers.net.
com. 172800 IN NS f.gtld-servers.net.
com. 172800 IN NS l.gtld-servers.net.
com. 172800 IN NS m.gtld-servers.net.
com. 172800 IN NS i.gtld-servers.net.
com. 172800 IN NS g.gtld-servers.net.
com. 86400 IN DS 30909 8 2 E2D3C916F6DEEAC73294E8
268FB5885044A833FC5459588F4A9184CF C41A5766
com. 86400 IN RRSIG DS 8 1 86400 20210826050000 2021
0813040000 26838 . Ux0B4OsIqS1GGVdLcj6zLc2k4eON+VvRjAght77spUsavt705JB/k2bD xH0a
+ux/31f1SeE127t2jMxk/jaUR9xJRQbkv7kMpNQKW9x3oOrI21ql CJjoIZl6ezuwBT8HbIzSCyiPy9Z
6qYnTRRh3b2rdPbeG8jfvGUMeBW4Y xVRCrEwdJtesfPNqPRmI+TnV3WTymCZ/wfrFBuVVrZUVsl75SP
i6RWrv dvjIV13D5xPNO6TSP+71d8S1qtxJ/aCskEV2IIVU7KqAcXwSebiM4h0d 56oS0xr+BppQ2dJi
w/FiQZkBjX6hNFF/CStVSZuTN/RQn+DeZT5SAUUm gbvKfA==
Menu
python3 ghost_eye.py - ...

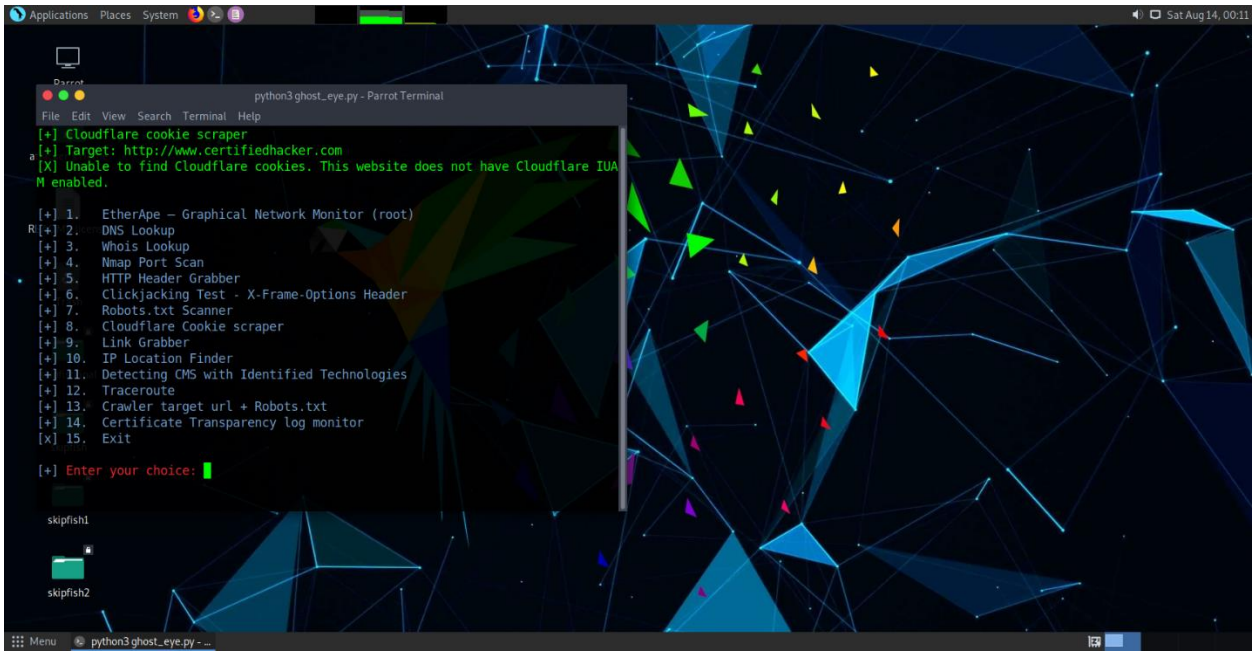
Step 5: Using **Whois Lookup**



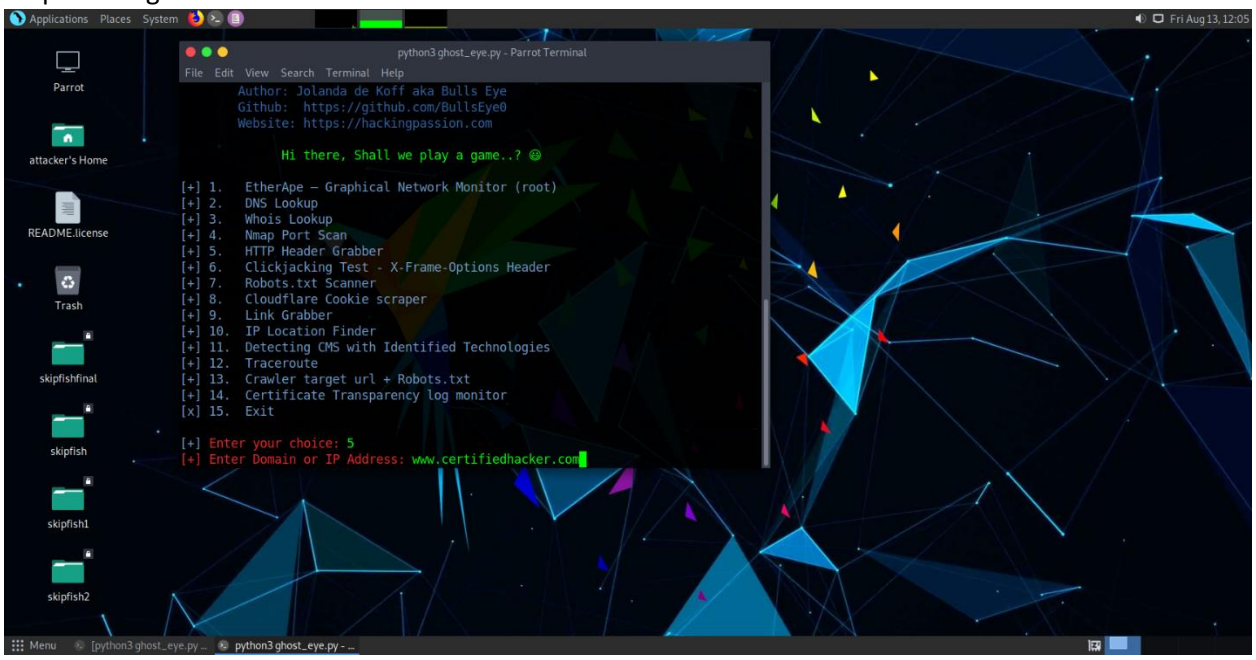


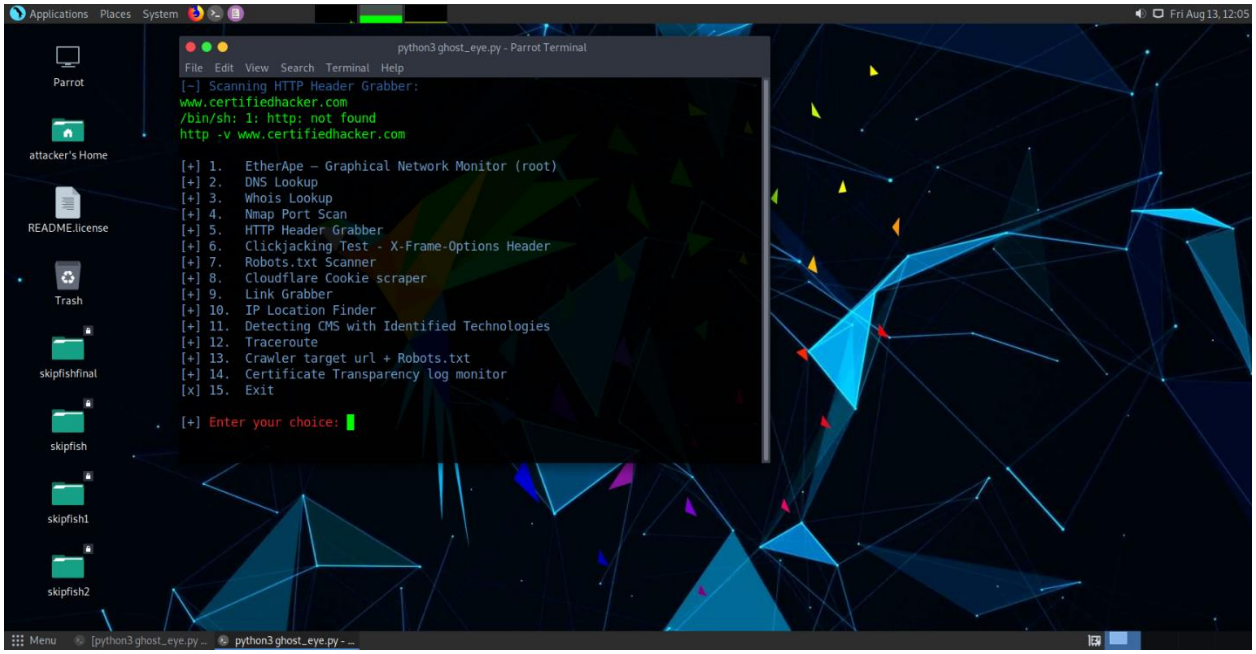
Step 6: Using CloudFlare Cookie Scraper



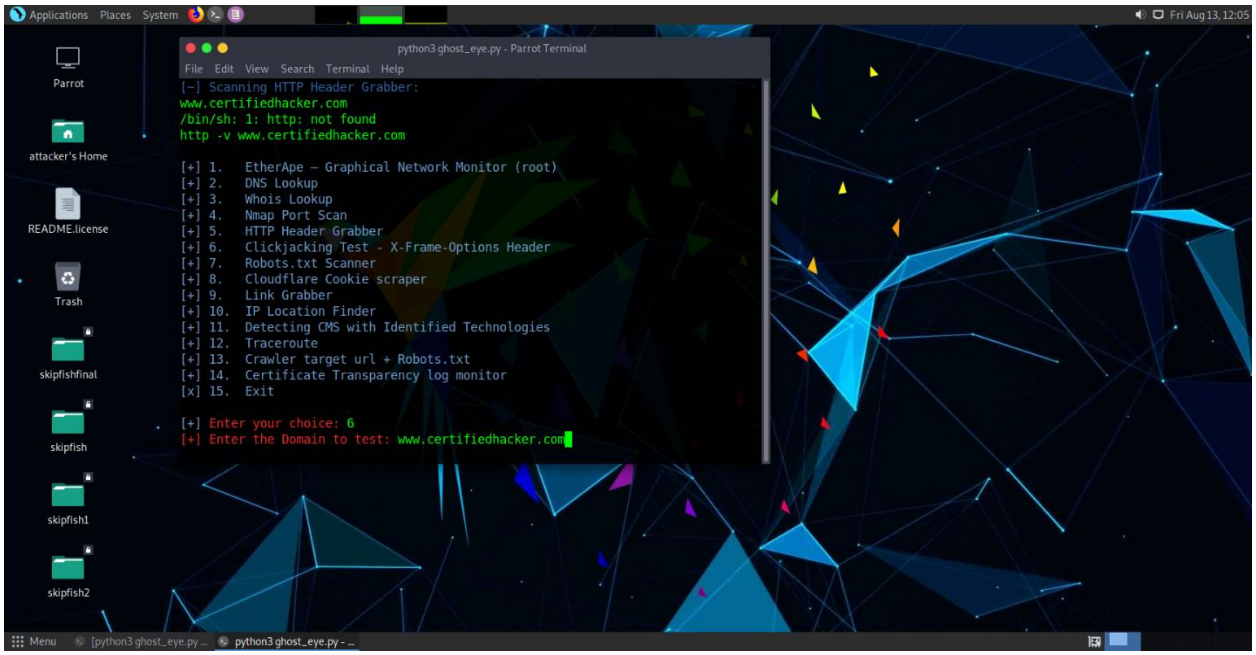


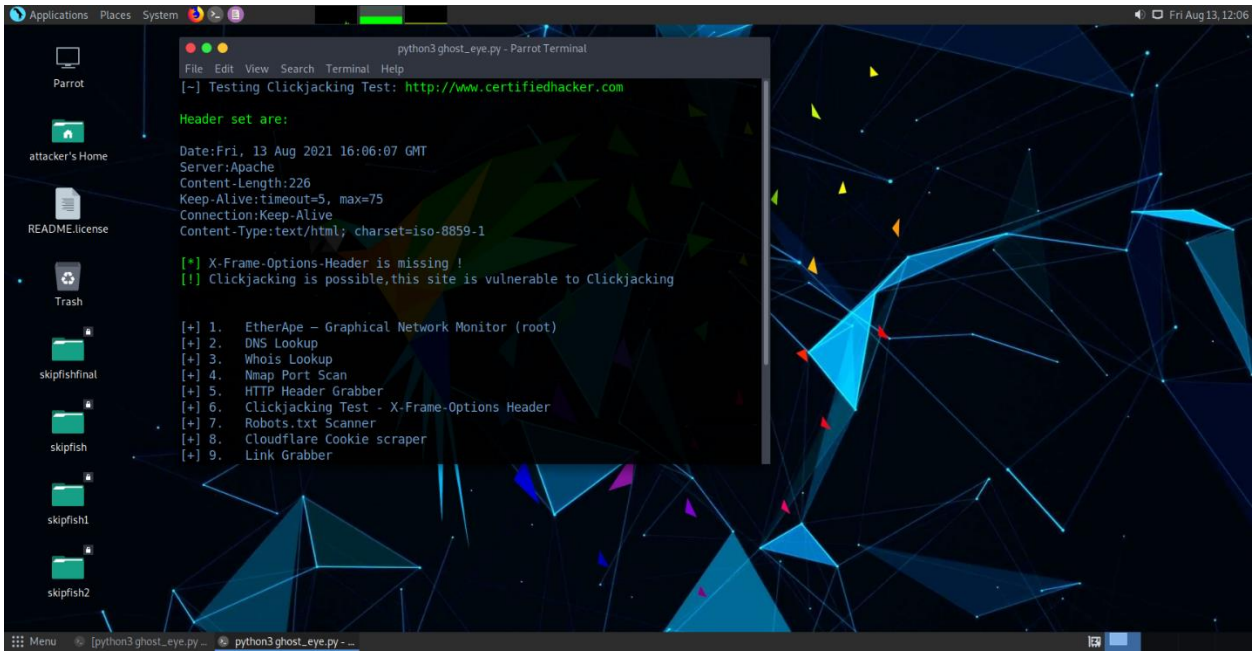
Step 7: Using HTTP Header Grabber



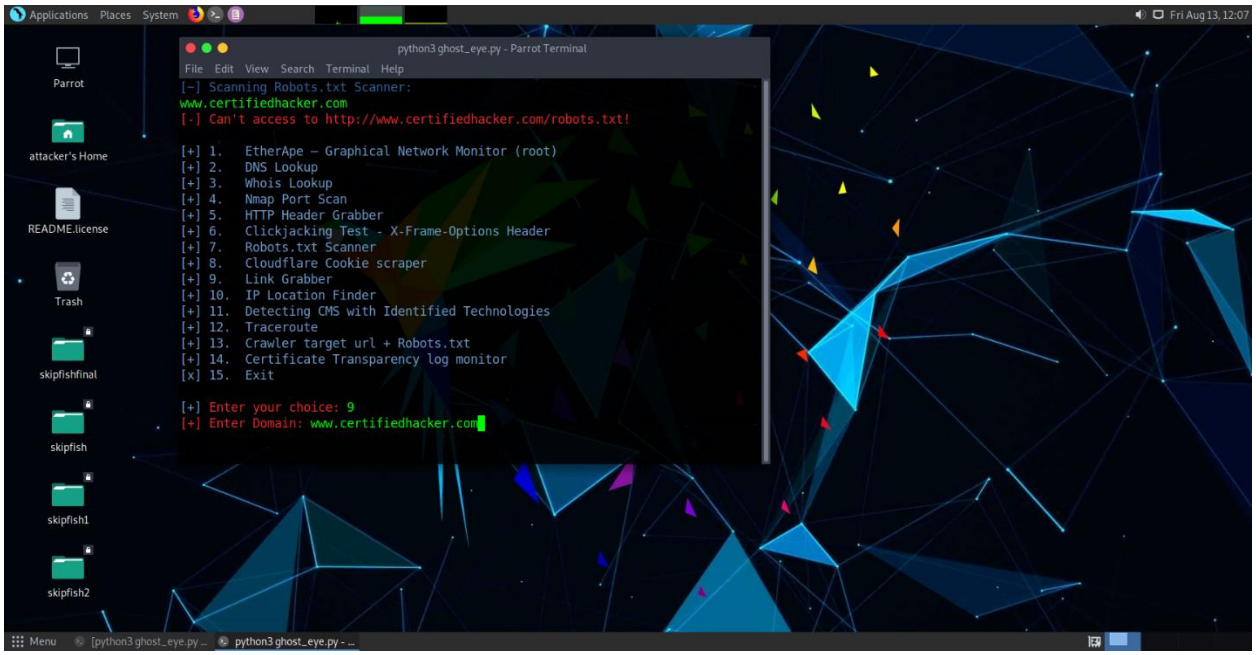


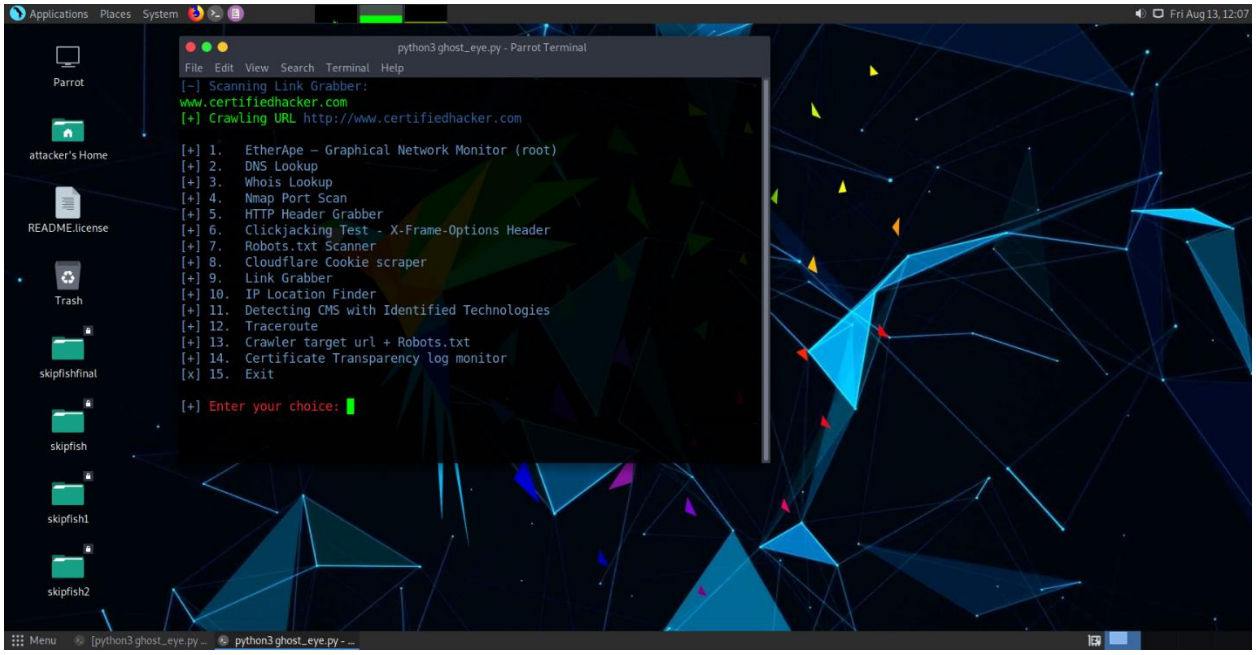
Step 8: Using Clickjacking



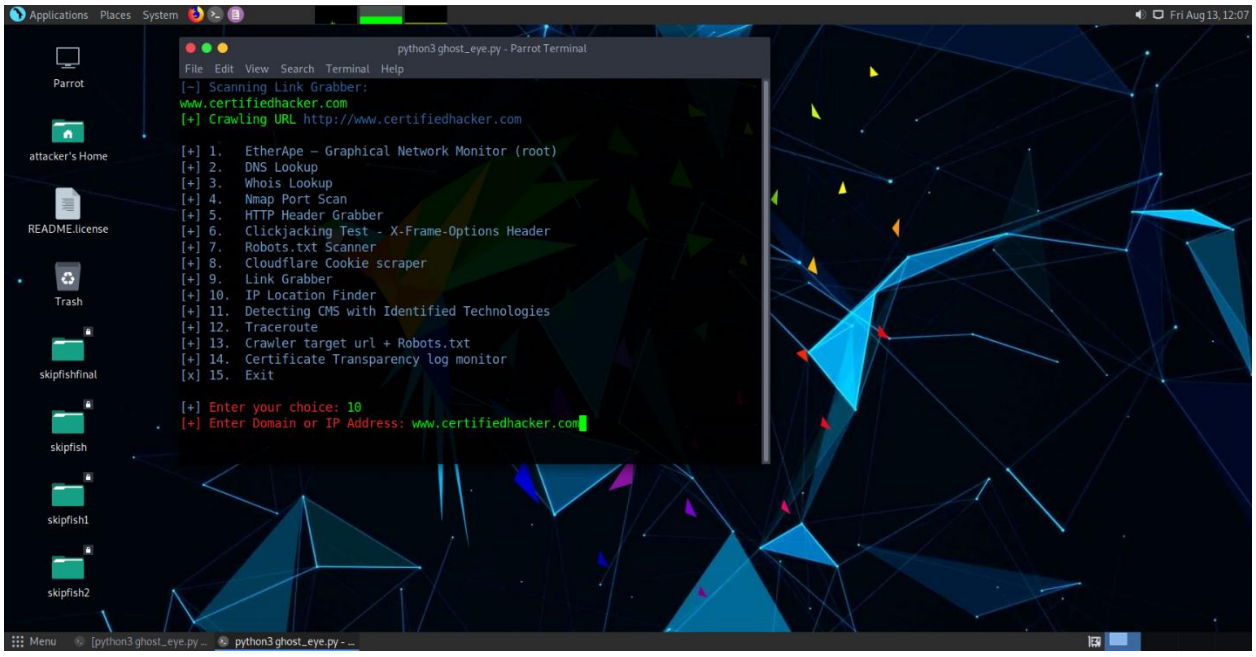


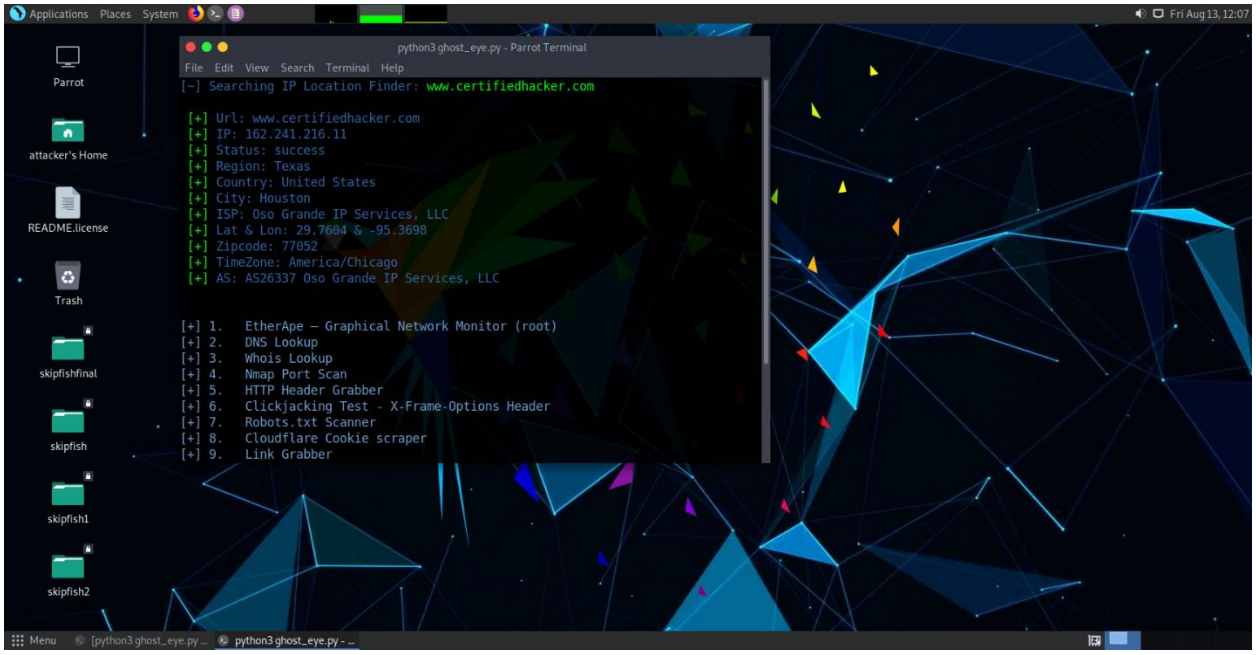
Step 9: Using Link grabber





Step 10: using IP Location finder

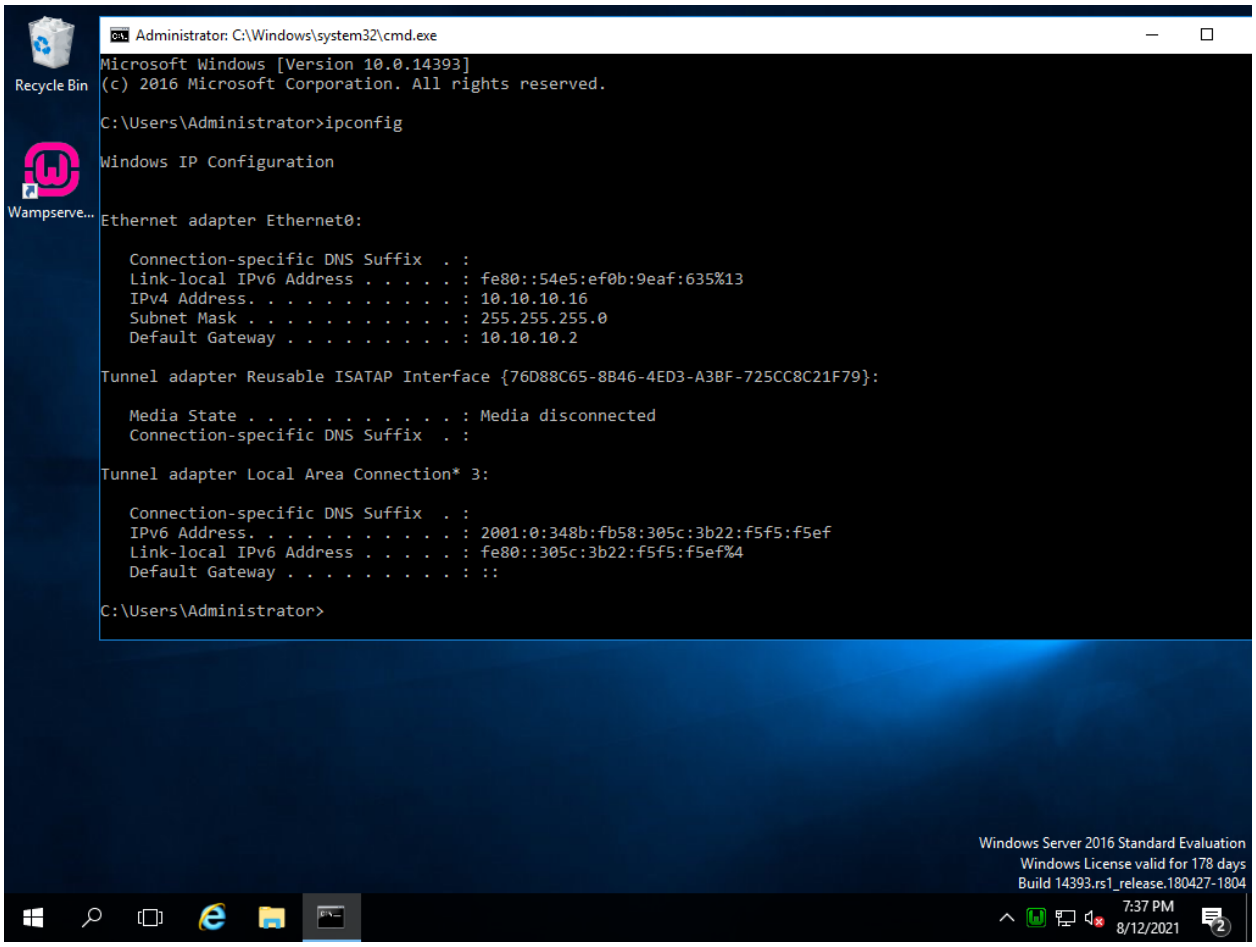




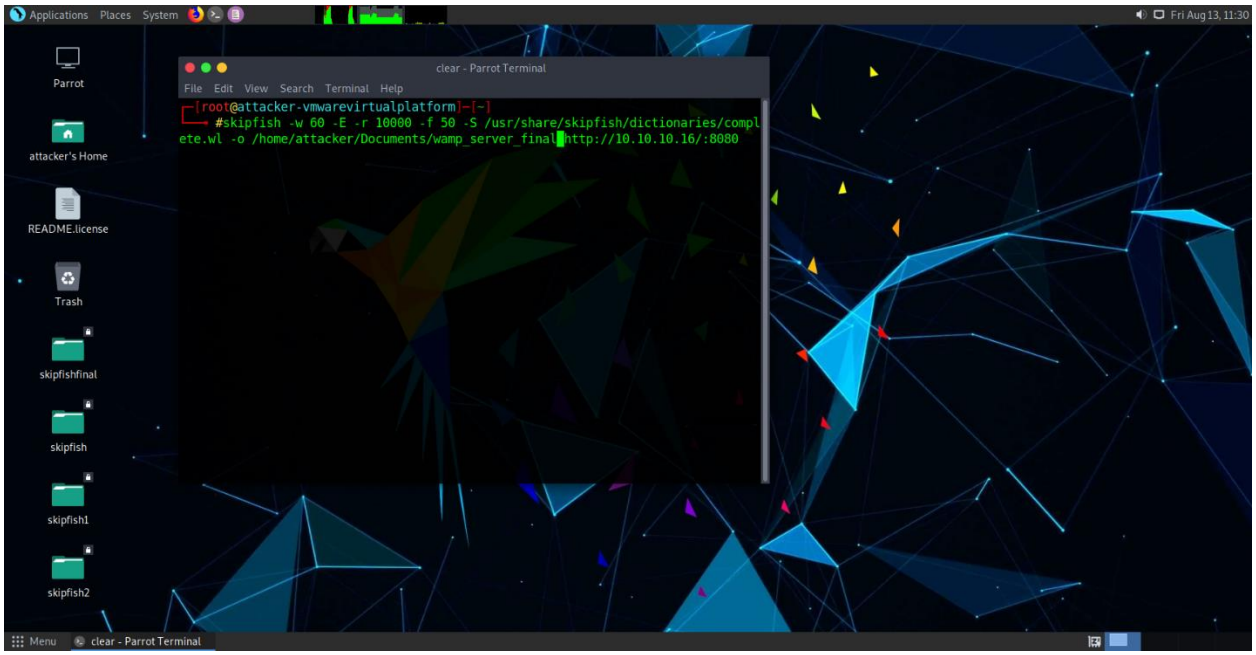
Task 2: Web Server Reconnaissance Skipfish

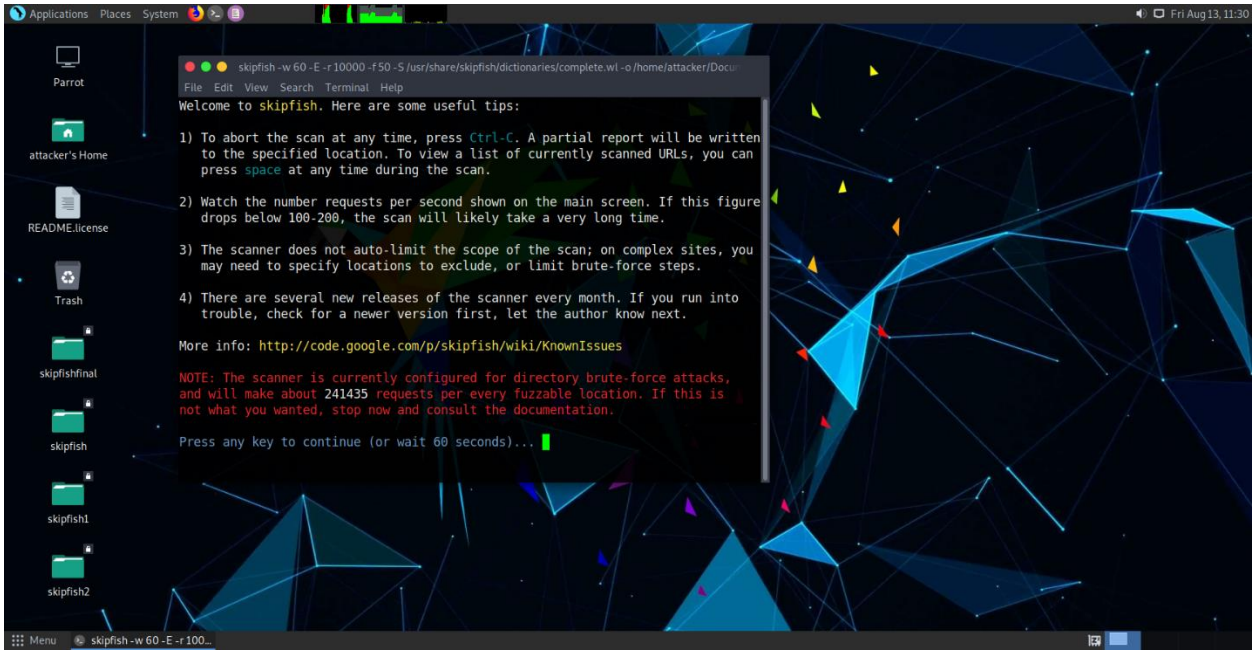
Skipfish is a web reconnaissance tool used to find information about a web server. It uses 2 methods to do this: dictionary and recursive crawl probing. With the help of a specific wordlist, Skipfish will conduct a brute forcing attack on the web server and log all the details obtained from that process. 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

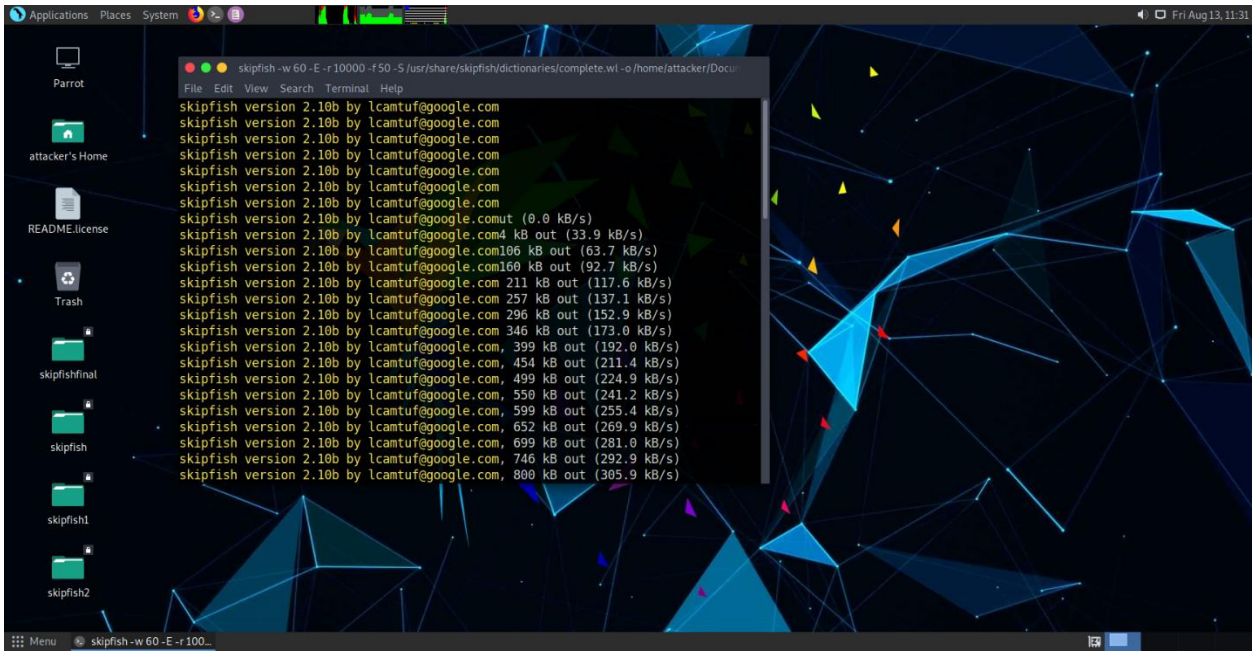


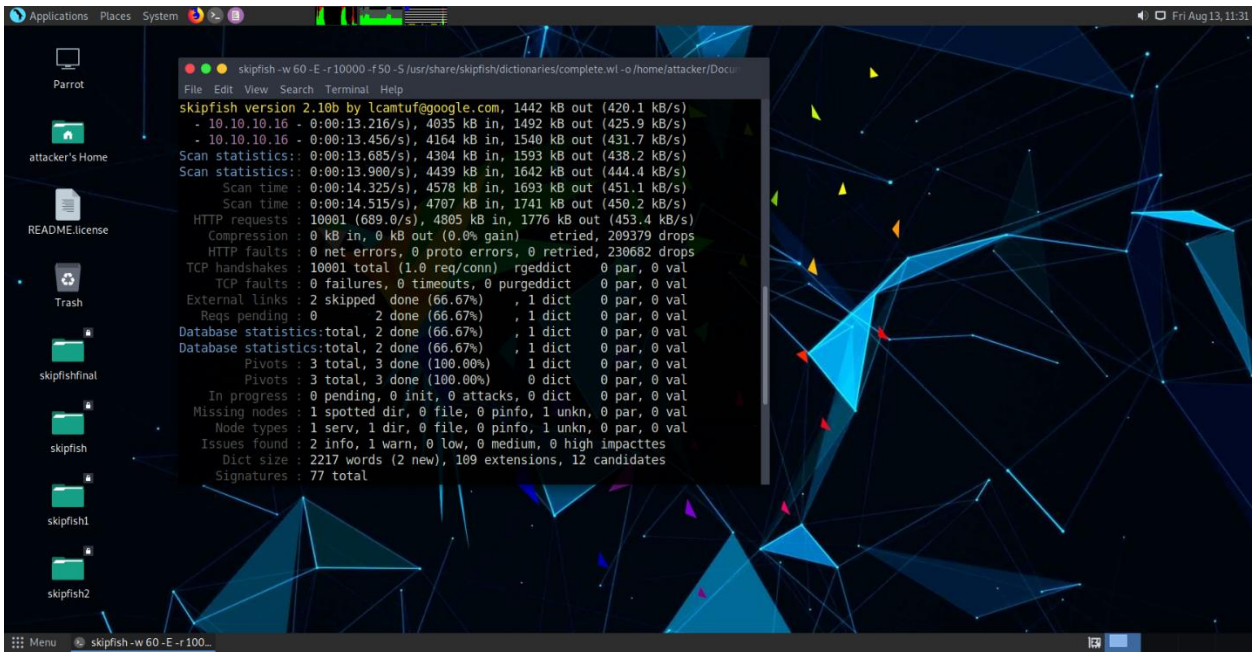
Step 2: Starting Skipfish in ParrotOS

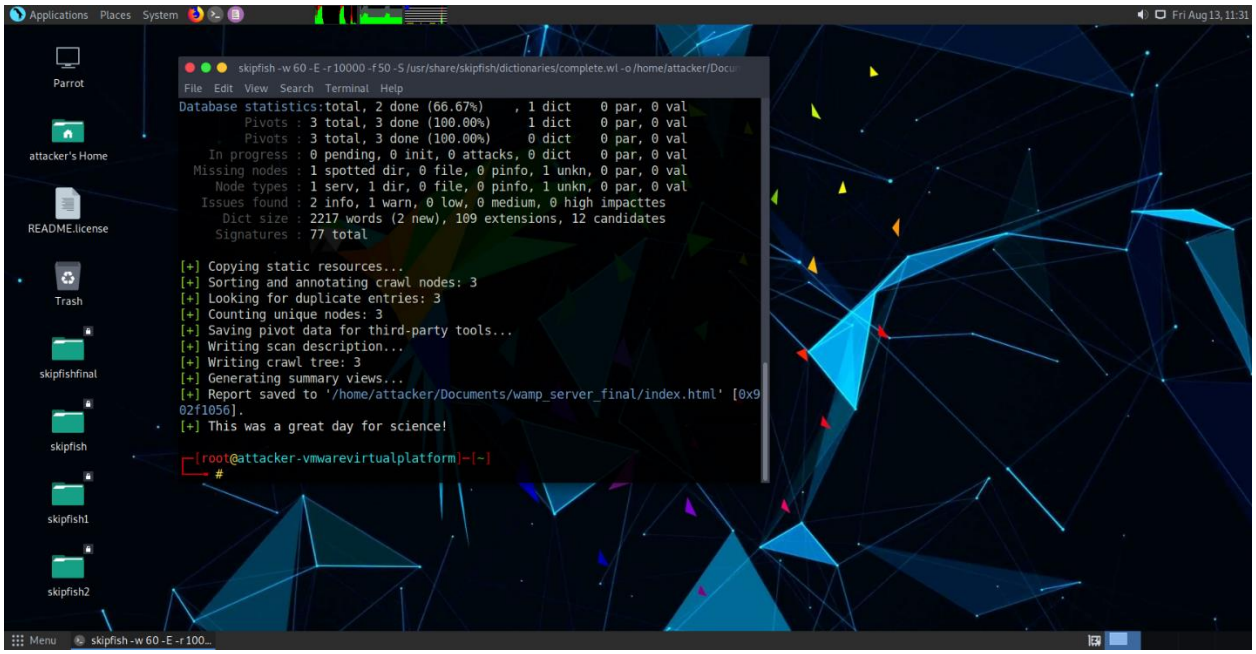




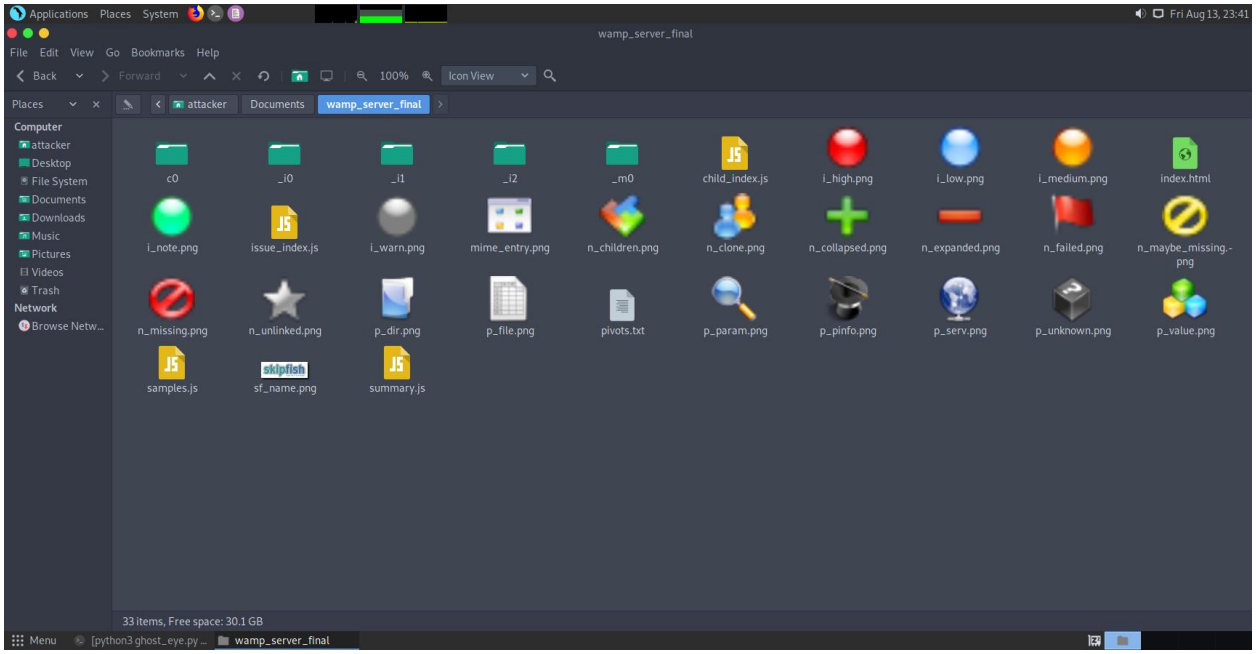
Ste 3: Skipfish Results on ParrotOS Terminal

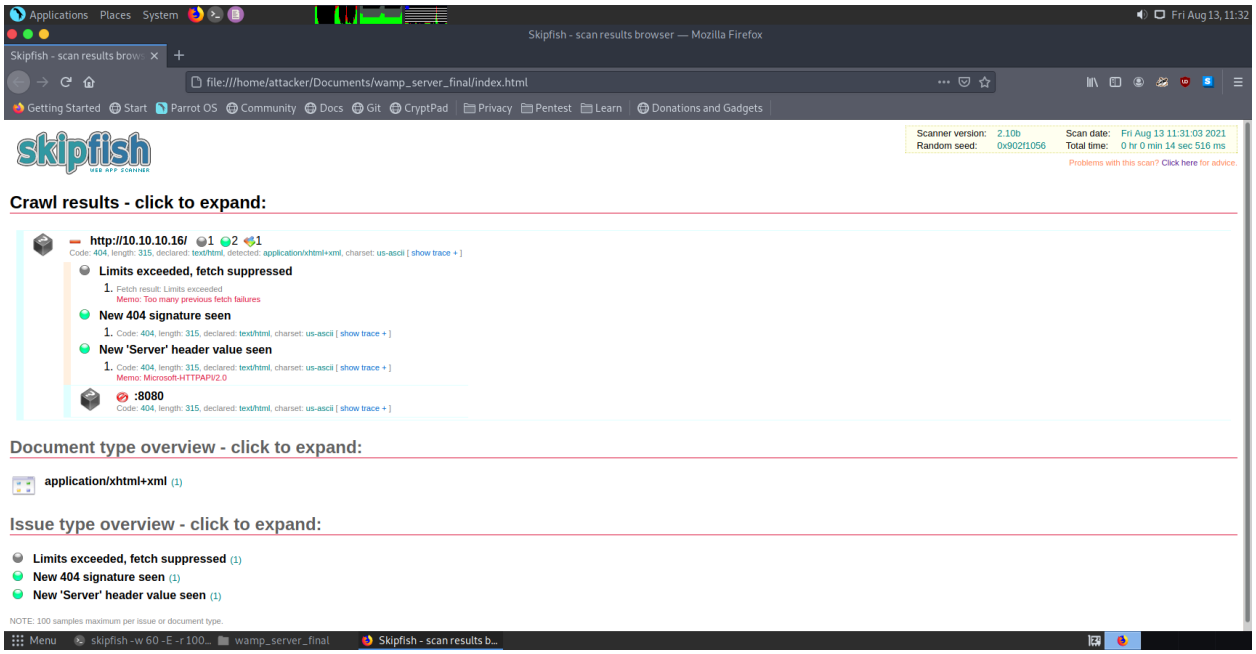


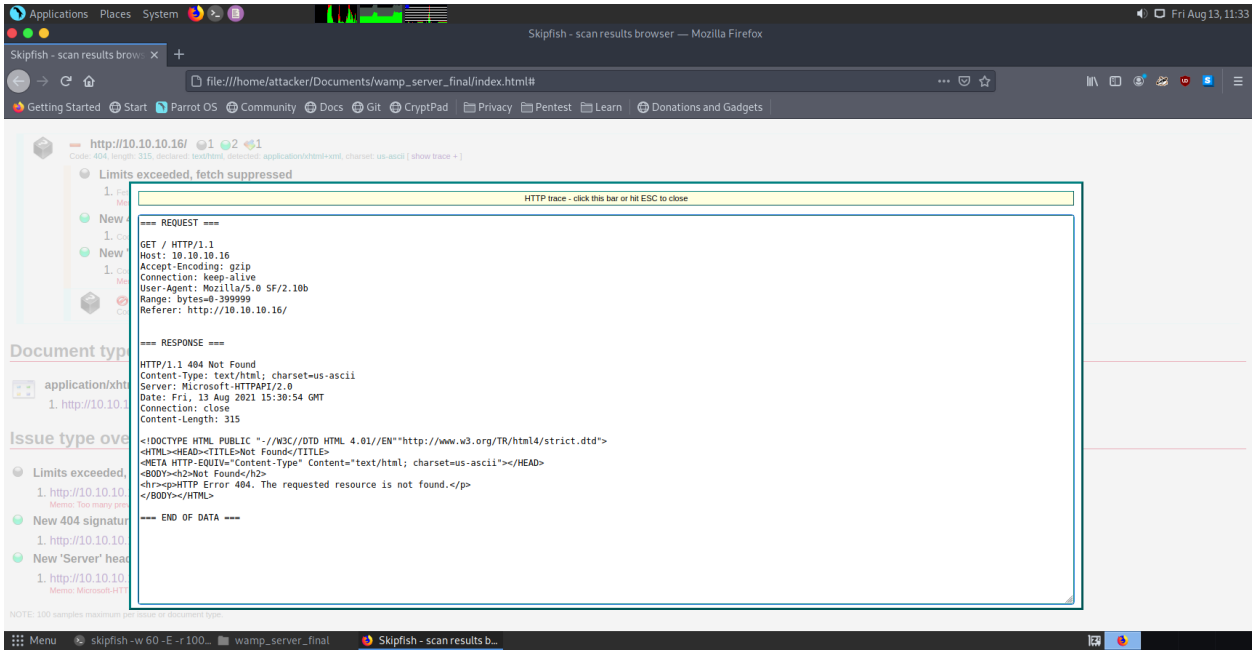


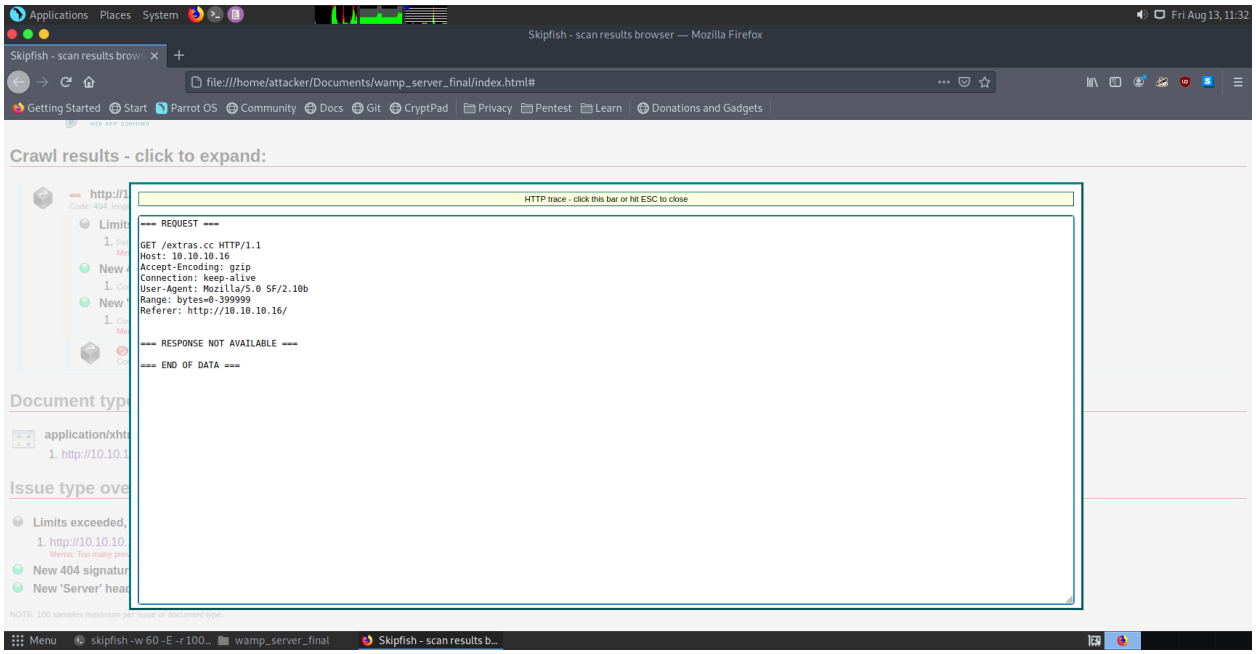


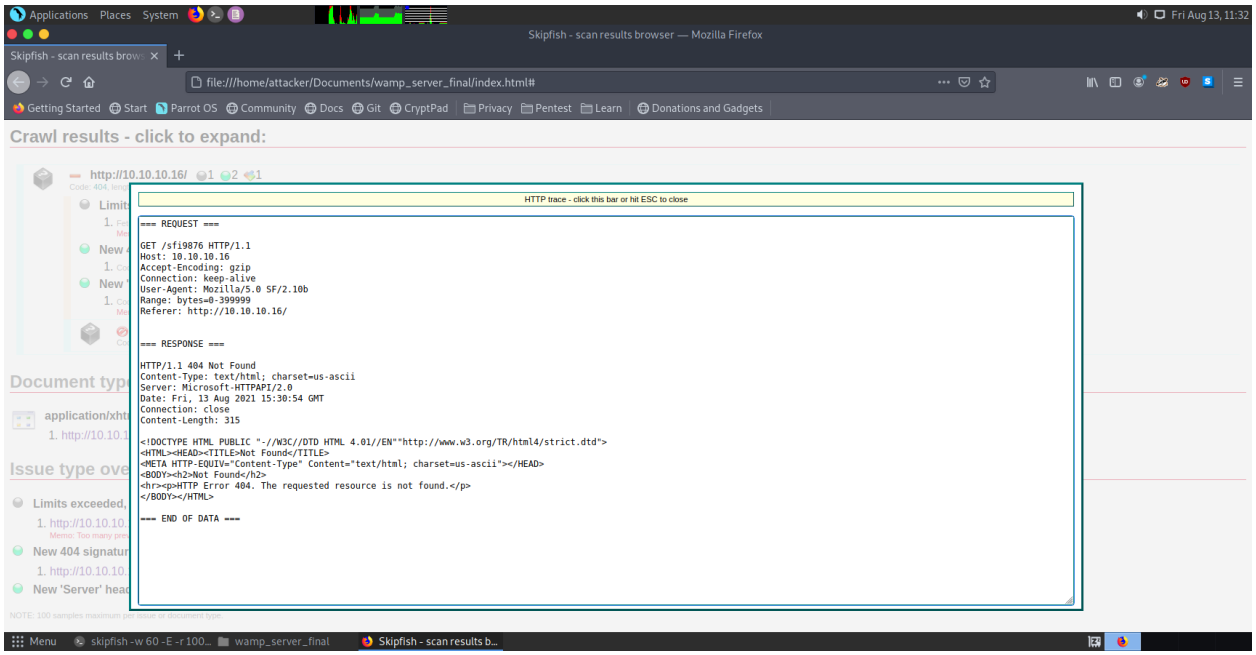
Step 4: Looking at Skipfish results in browser by accessing the Index.html file generated as output in the Documents folder inside wamp_server_final folder

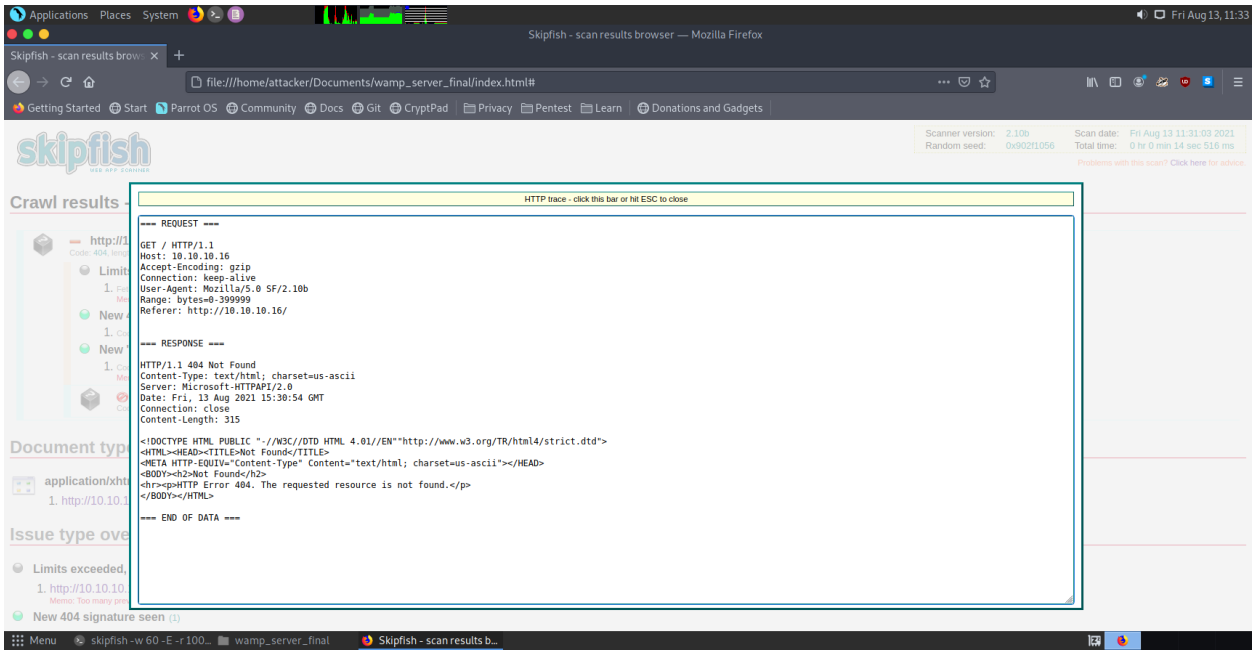



Applications Places System
Fri Aug 13, 11:32
Skipfish - scan results browser — Mozilla Firefox
file:///home/attacker/Documents/wamp_server_final/index.html
Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn Donations and Gadgets
skipfish
Scanner version: 2.10b
Random seed: 0x902f1056
Scan date: Fri Aug 13 11:31:03 2021
Total time: 0 hr 0 min 14 sec 516 ms
Problems with this scan? Click here for advice.
Crawl results - click to expand:
http://10.10.10.16/ 1 2 1
Code: 404, length: 315, declared: text/html, detected: application/xhtml+xml, 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...


Applications Places System
Fri Aug 13, 11:33
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 "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr> HTTP Error 404. The requested resource is not found.
</BODY></HTML>
=== END OF DATA ===
Menu
skipfish -w 60 -E -r 100...
wamp_server_final
Skipfish - scan results b...


Applications Places System
Fri Aug 13, 11:32
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
Crawl results - click to expand:
HTTP trace - click this bar or hit ESC to close
=== REQUEST ===
GET /extras.cc 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 NOT AVAILABLE ===
=== END OF DATA ===
Menu
skipfish -w 60 -E -r 100...
wamp_server_final
Skipfish - scan results b...


Applications Places System
Fri Aug 13, 11:32
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
Crawl results - click to expand:
http://10.10.10.16/
HTTP trace - click this bar or hit ESC to close
=== REQUEST ===
GET /sfi9876 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 "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>Not Found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
<BODY><h2>Not Found</h2>
<hr> HTTP Error 404. The requested resource is not found.
</BODY></HTML>
=== END OF DATA ===
Menu
skipfish -w 60 -E -r 100...
wamp_server_final
Skipfish - scan results b...

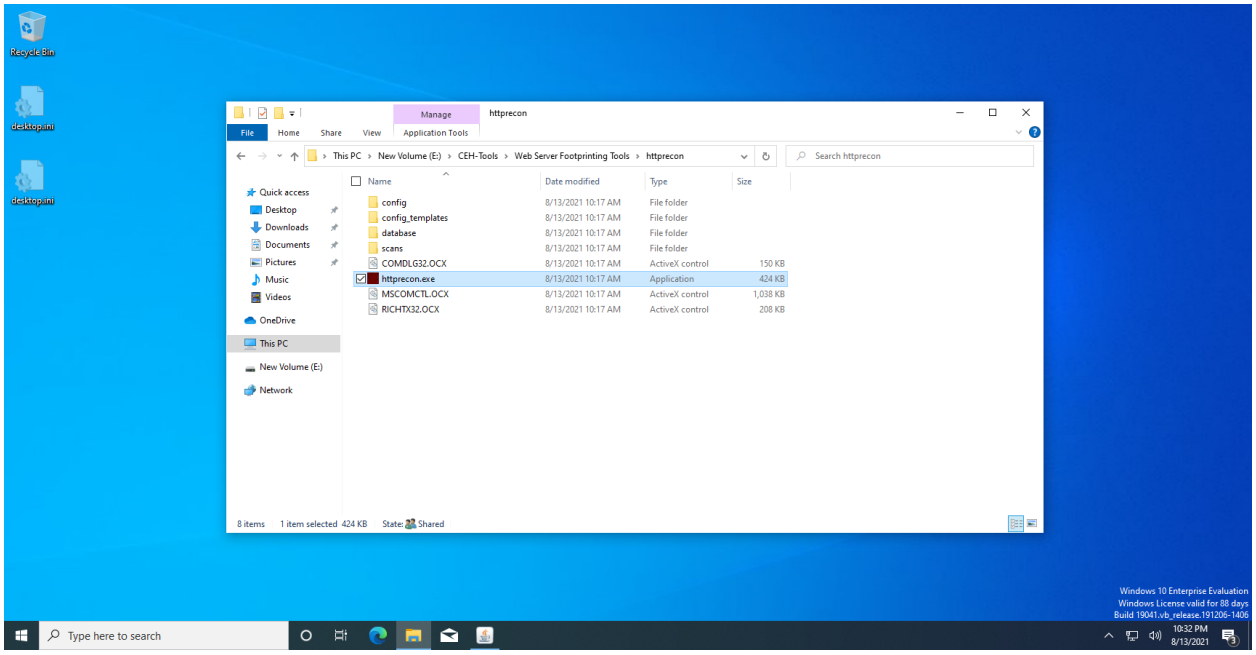


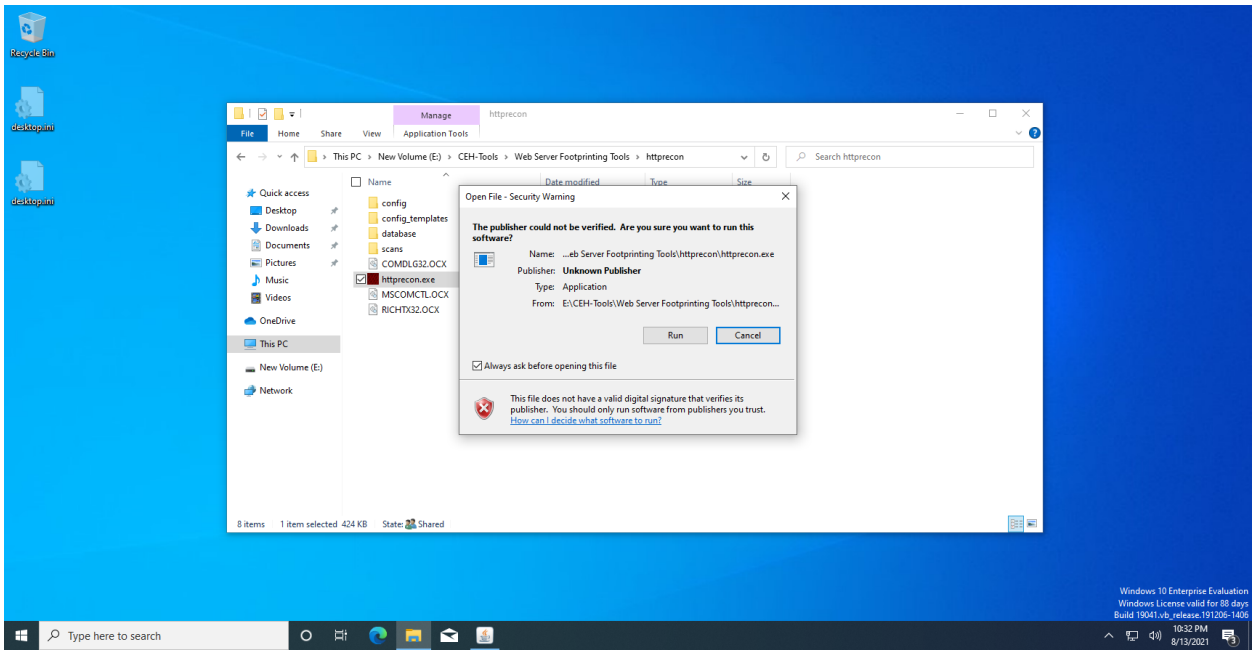
The end goal of Skipfish is to show the attacker of all the defensive measure in place to help better optimize the attack to have better penetration and greater impact. On the defensive side, this tool will help the cyber security team have a better understanding of vulnerabilities and ways they can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

Task 3: Web Server footprinting using HTTPRecon tool

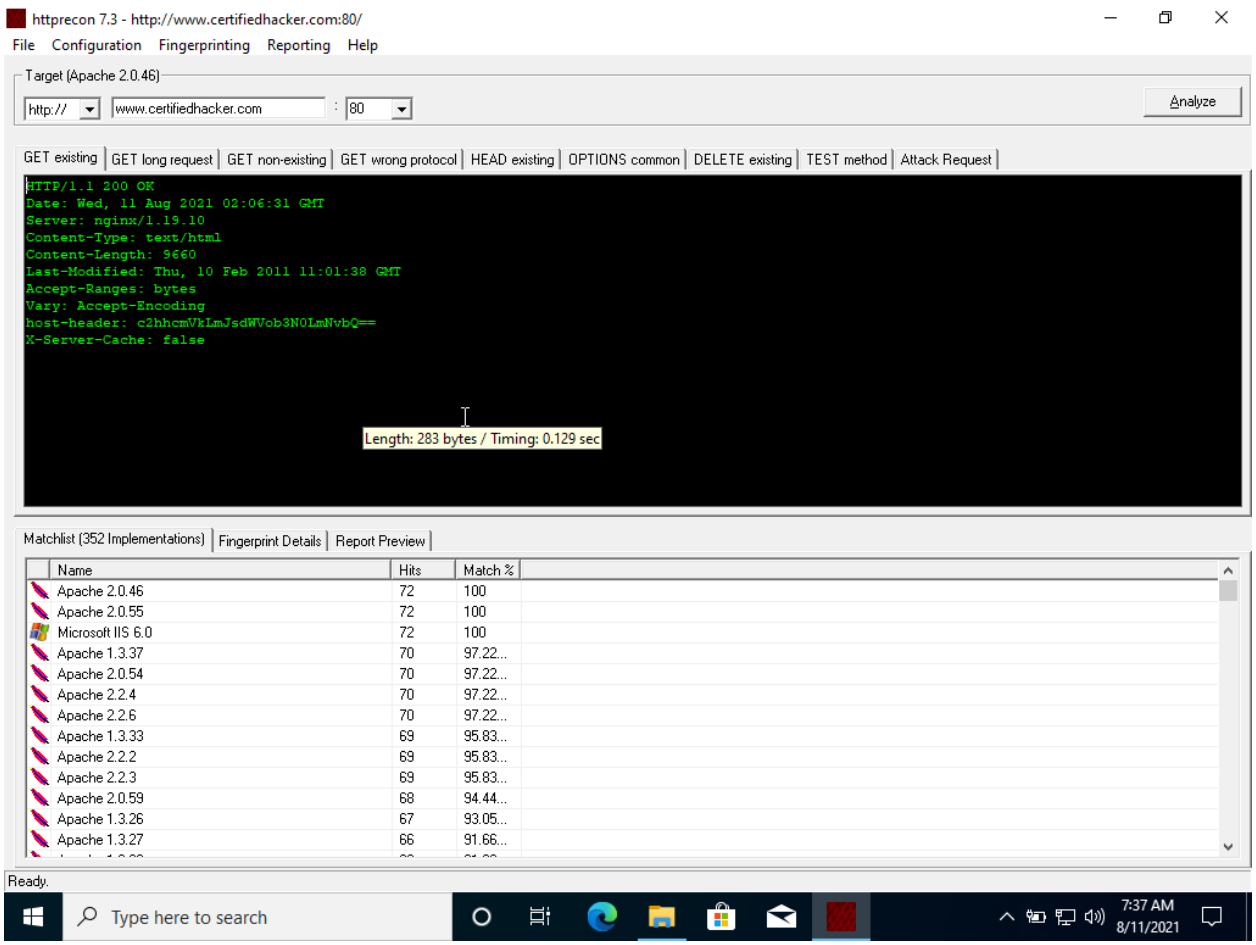
HTTPRecon is as its name suggests a http reconnaissance tool for Windows. It is a fingerprinting tool with advanced functionalities. The purpose of this tool is to find as accurate as possible httpd implementations on a website or webserver

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

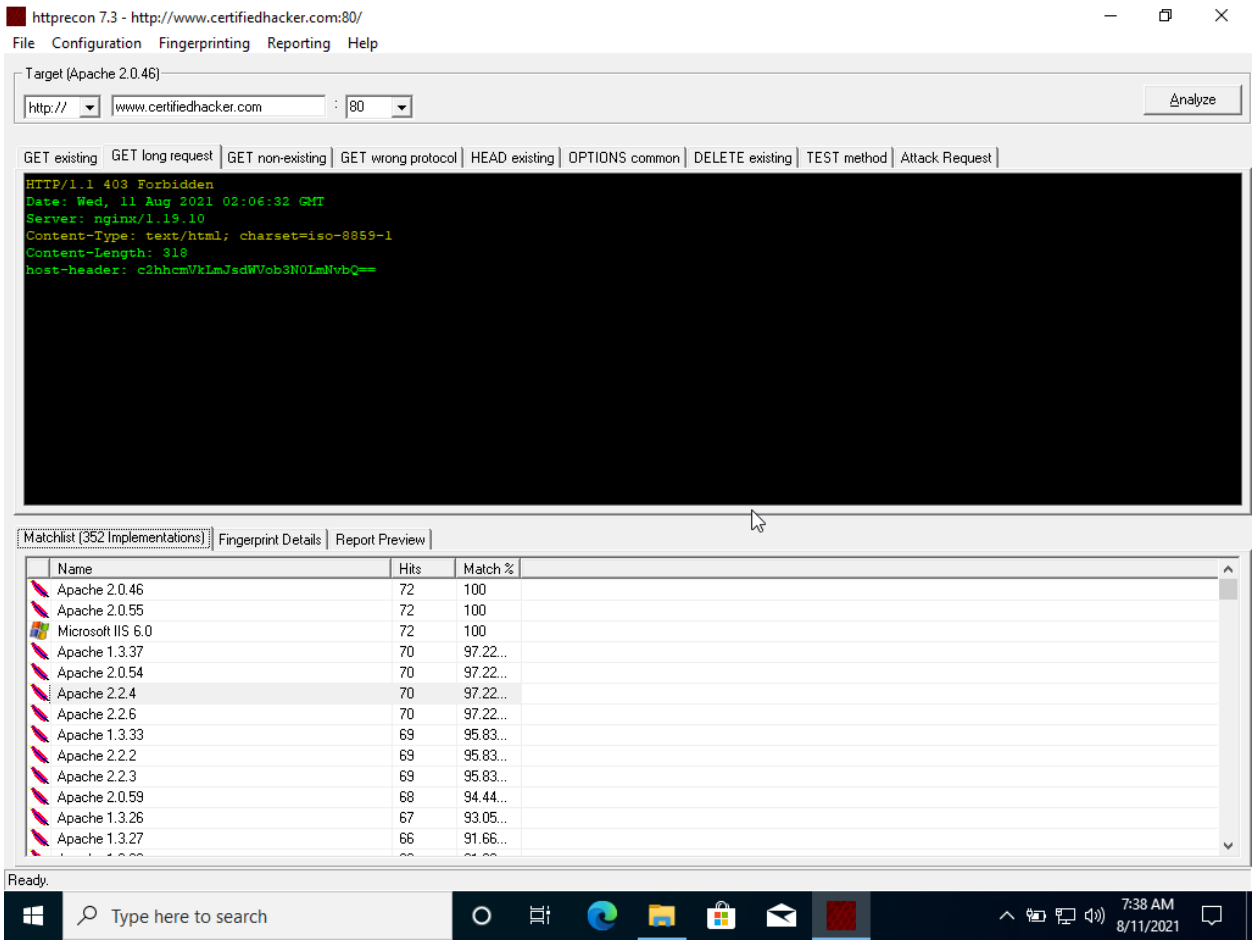




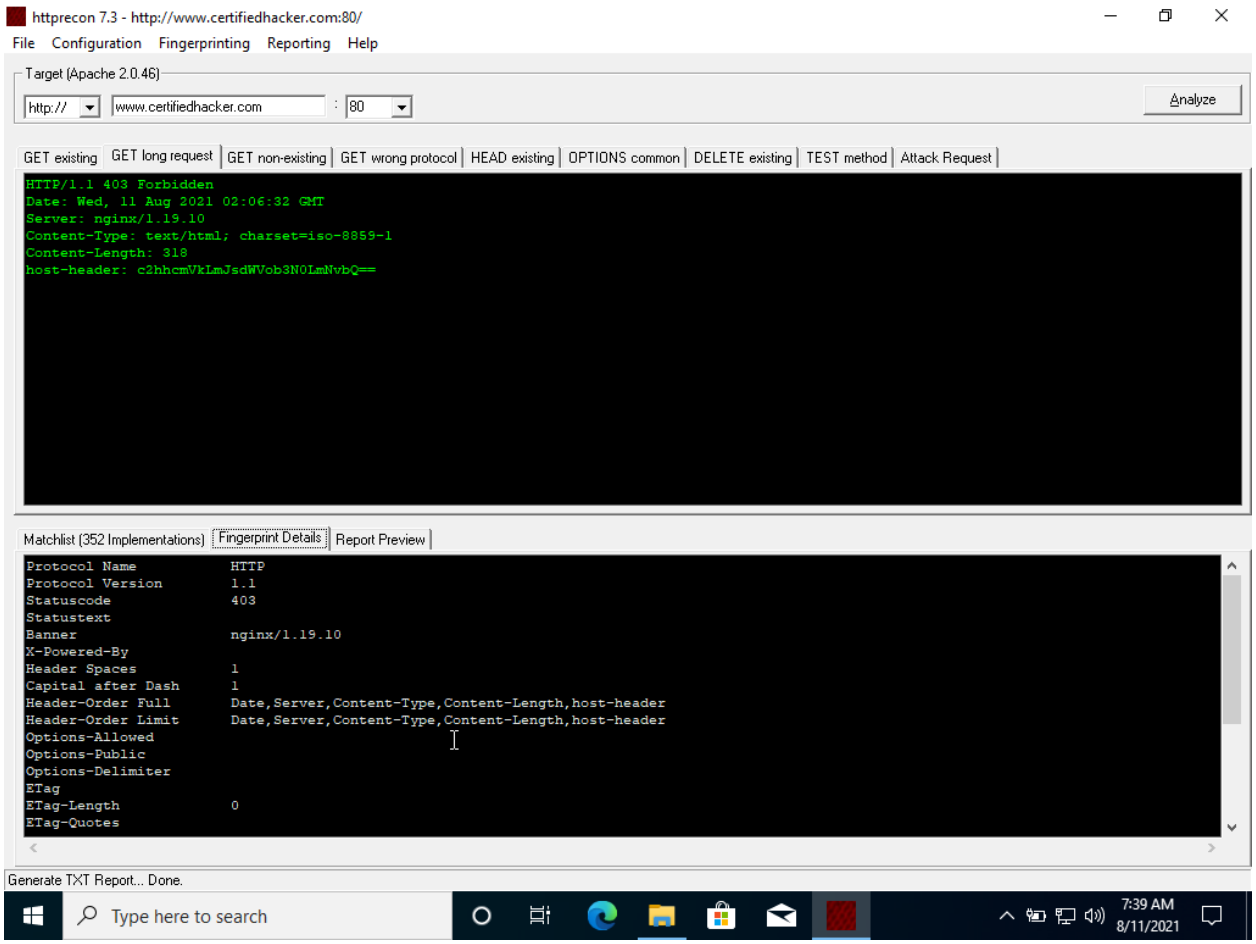
Step 2: Analyzing **www.certifiedhacker.com** at port 80 to GET existing details about the connection


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: 9660
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



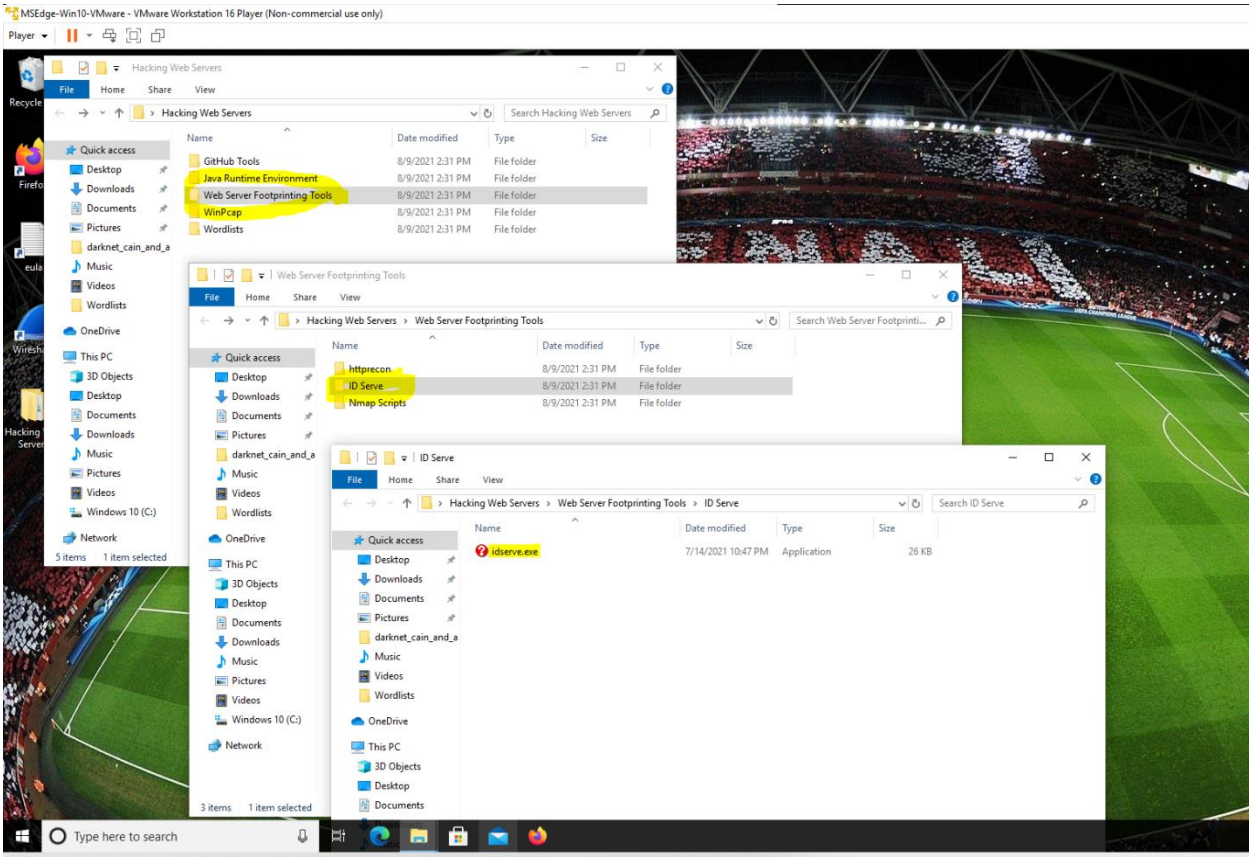
Step 4: Using the Fingerprinting Details tab at the bottom to see the protocols being used and its service versions



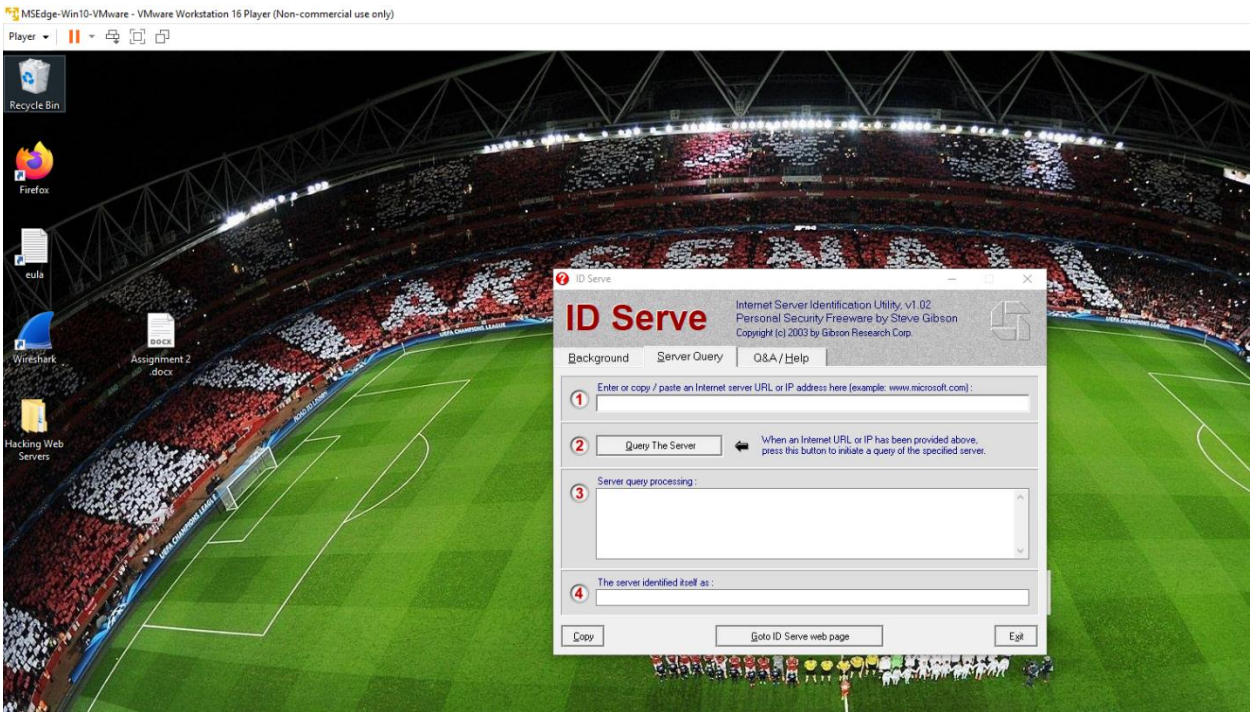
Task 4: Footprint a Web Server using ID Serve

Step 1: Open Windows10 VM.

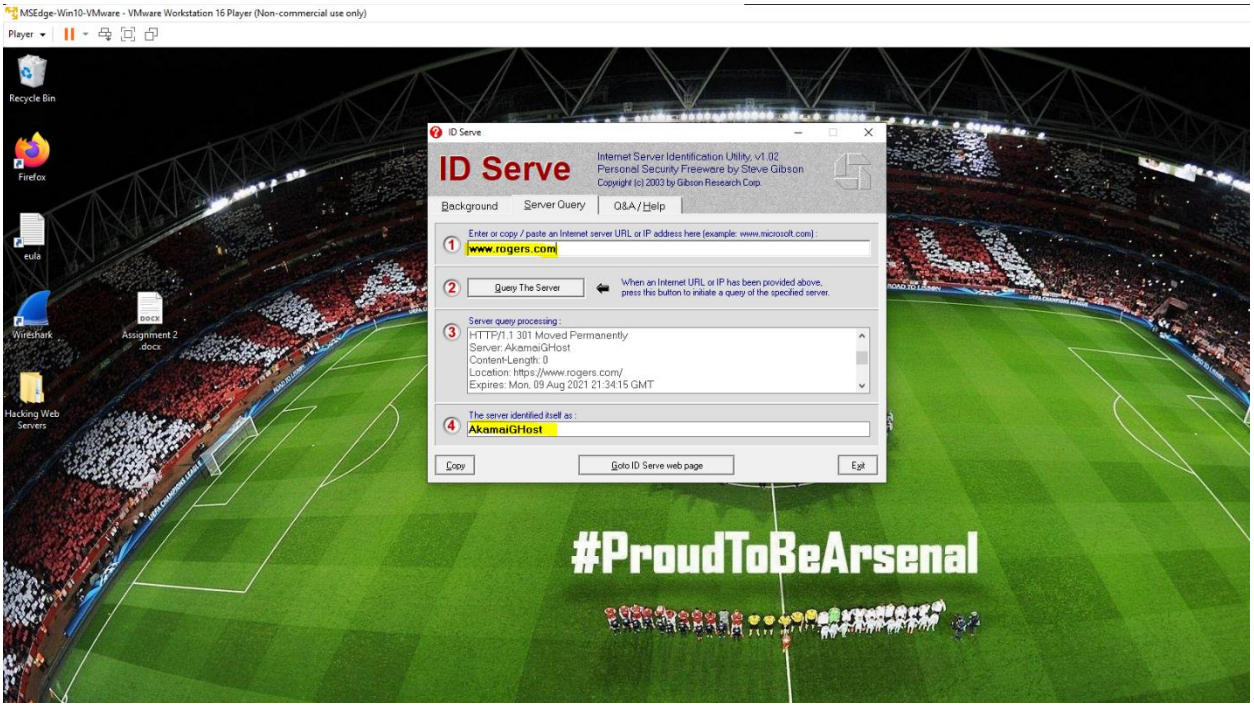
Step 2: Navigate to **Hacking Web Servers->Web Server Footprinting Tools->ID Serve.** Open idserve.exe.



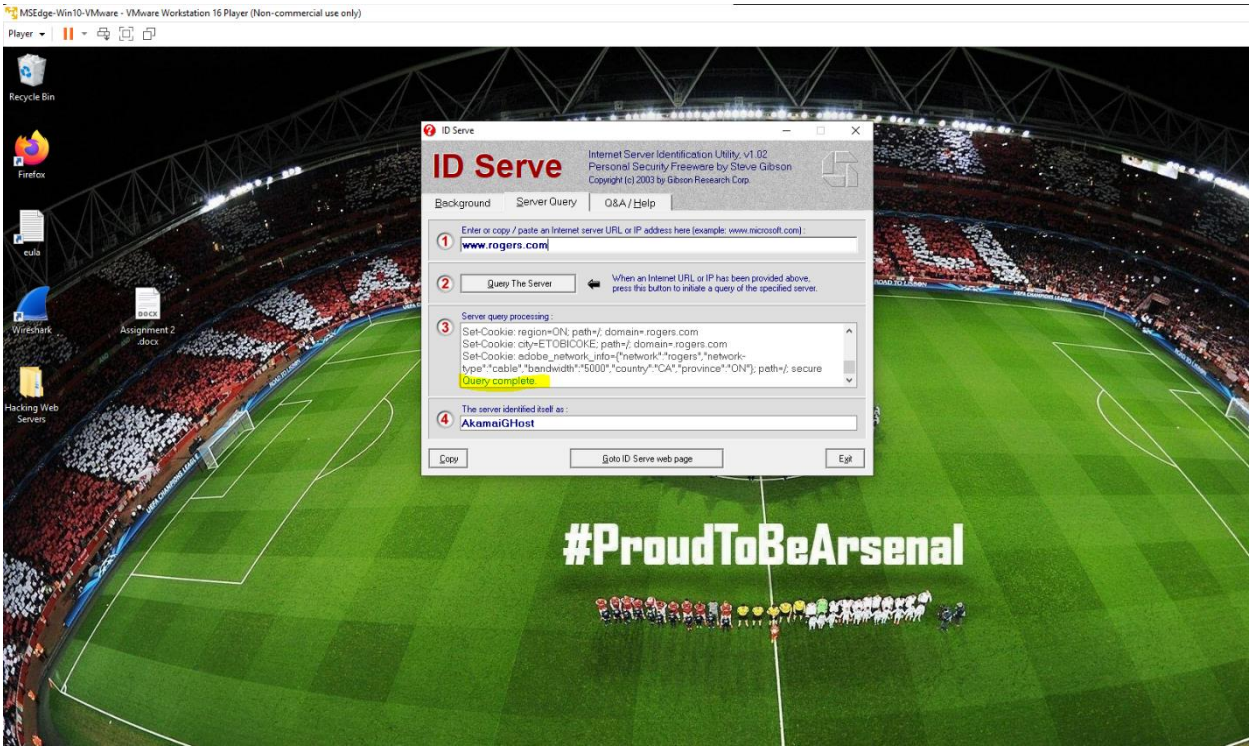
Step 3: The below mentioned ID Serve tab will open up.



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.



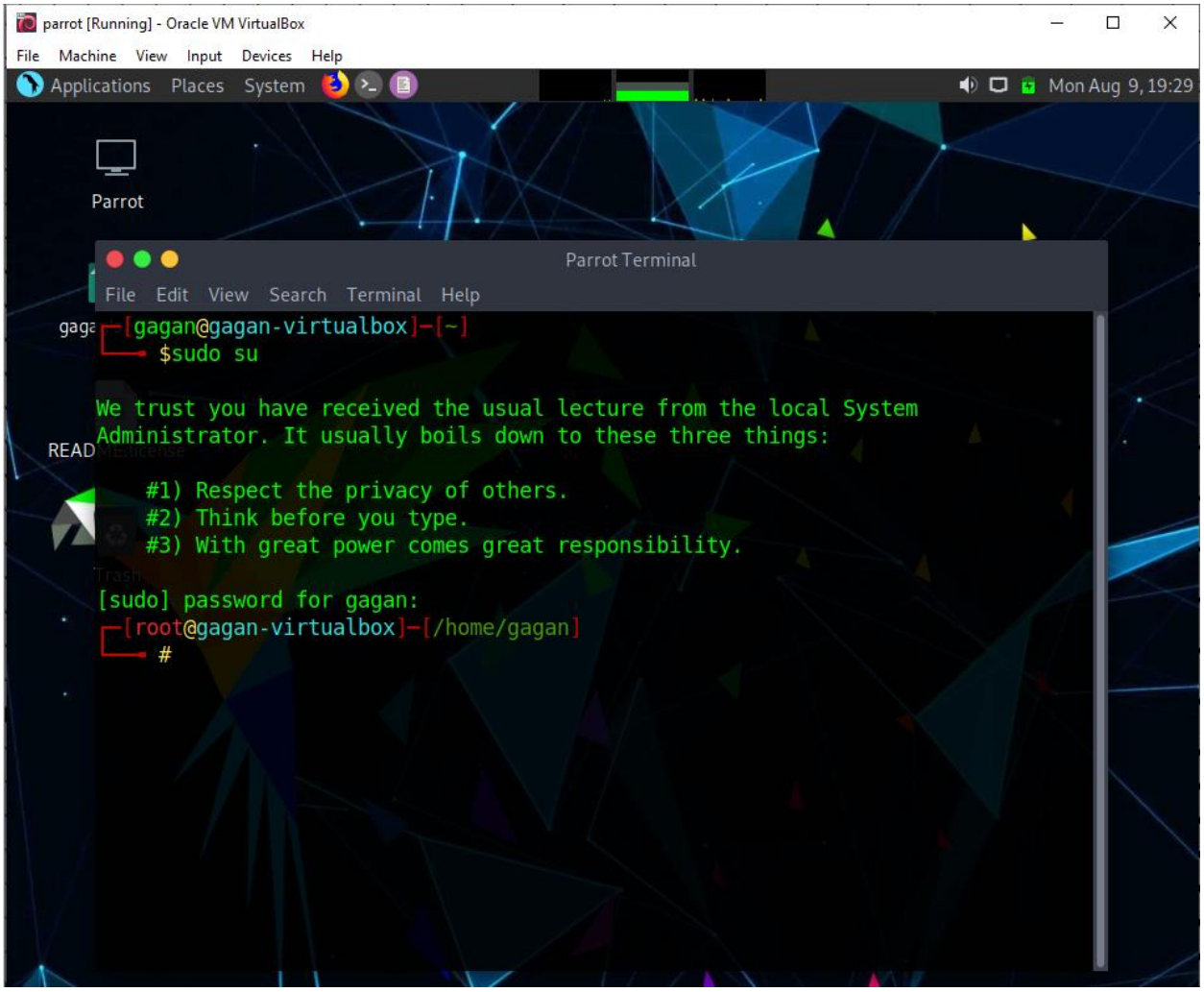
Step 5: The server type discovered is listed below after completing the query.


MSEdge-Win10-VMware - VMware Workstation 16 Player (Non-commercial use only)
Player
Recycle Bin
Firefox
eula
Wireshark
Assignment 2 .docx
Hacking Web Servers
ID Serve
ID Serve
Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.
Background
Server Query
Q&A / Help
Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com) :
www.rogers.com
Query The Server
When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server.
Server query processing :
Set-Cookie: region=ON; path=/; domain=.rogers.com
Set-Cookie: city=ETOBICOKE; path=/; domain=.rogers.com
Set-Cookie: edobe_network_info={"network":"rogers","network-type":"cable","bandwidth":"5000","country":"CA","province":"ON"}; path=/; secure
Query complete.
The server identified itself as :
AkamaiGHost
Copy
Goto ID Serve web page
Exit
#ProudToBeArsenal

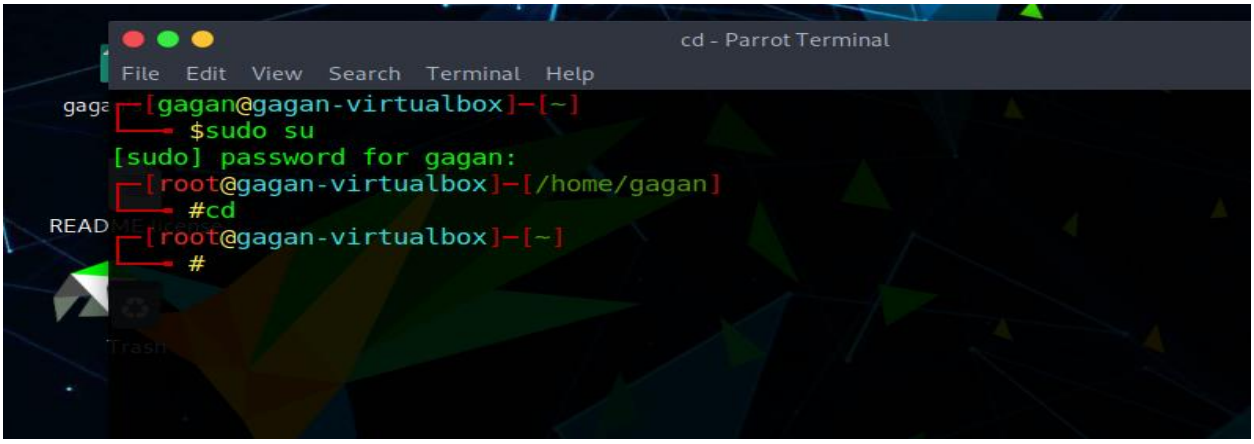
Task 5: Footprinting a Web Server using Netcat and Telnet

Step 1: Open the Parrot VM.

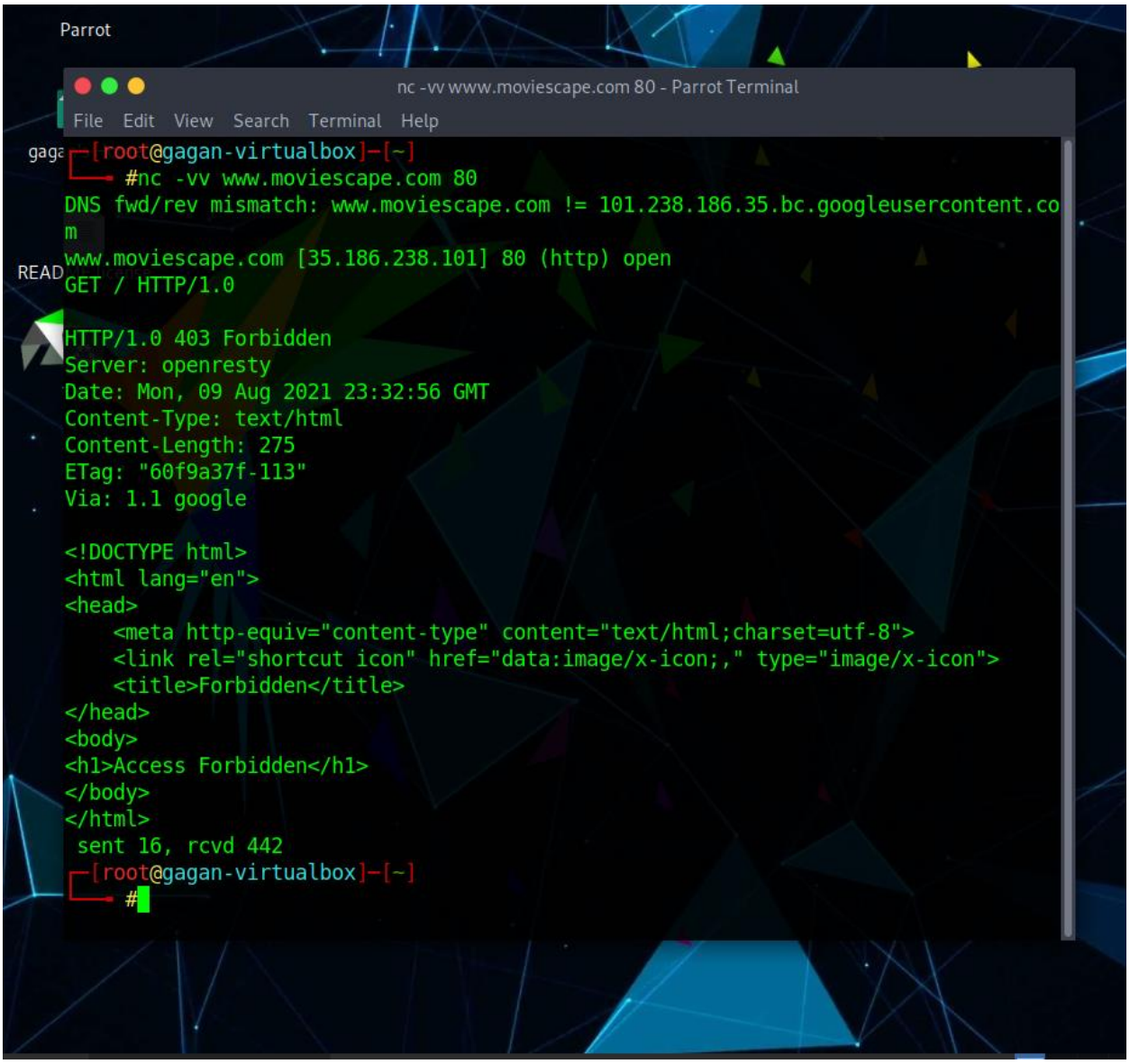
Step 2: Open Terminal and run command **sudo su** to get root privileges.



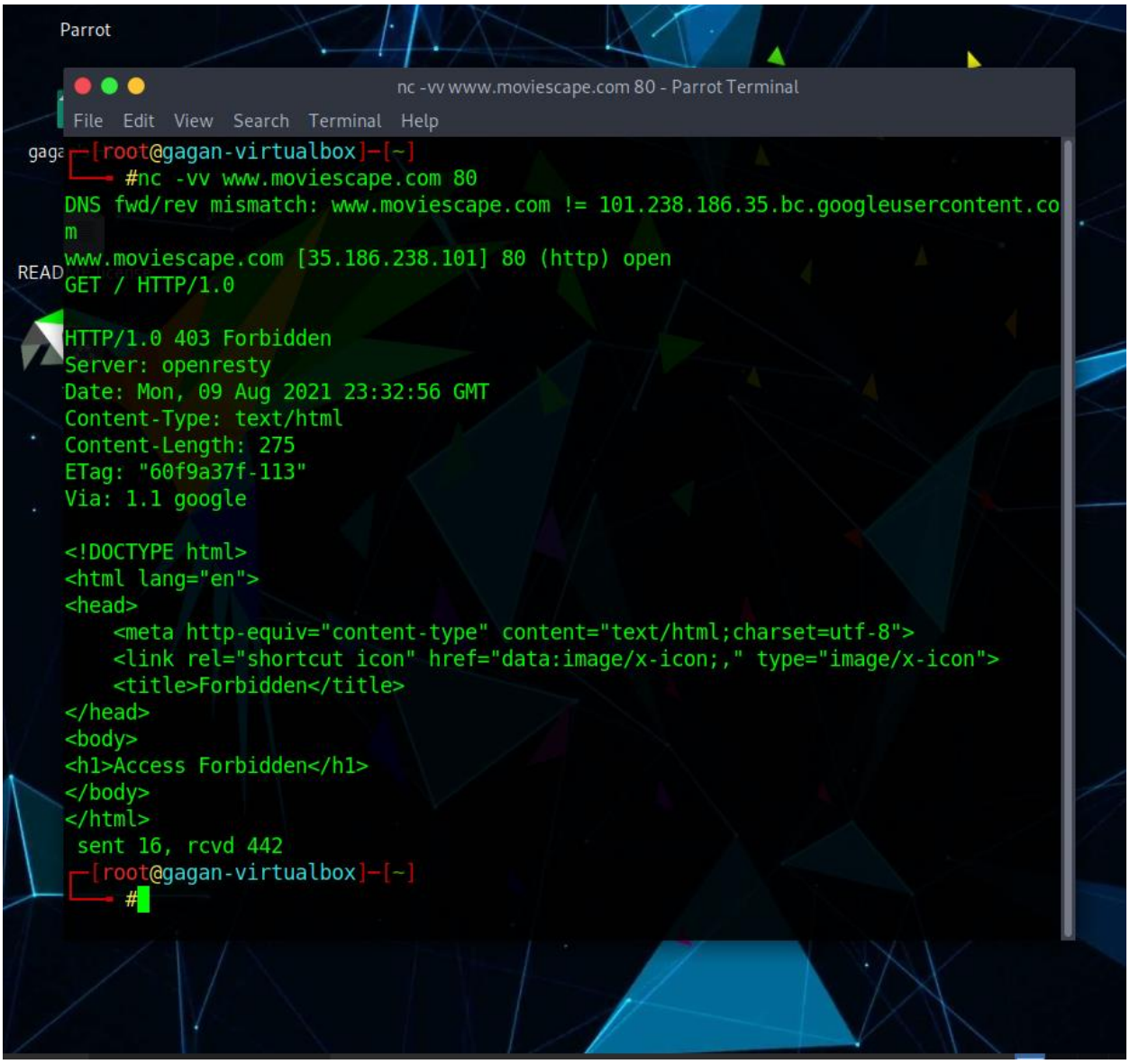
Step 3: Type cd and enter to jump to root directly.



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.

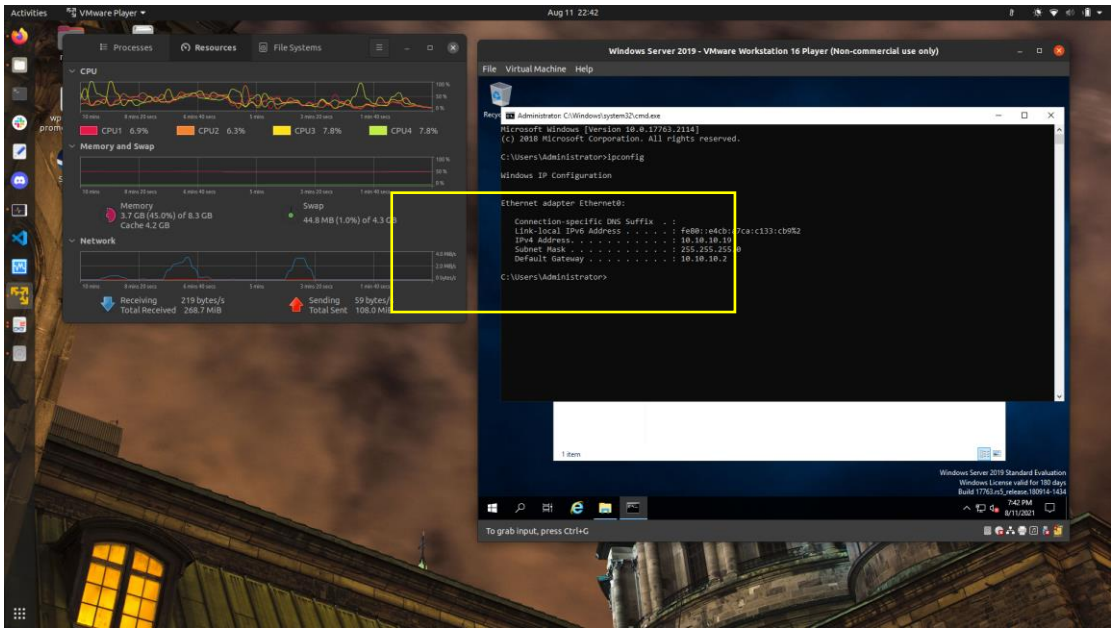


Step 5: This time, enter the command **telnet** www.moviescape.com and press enter. After hitting enter type **GET / HTTP/1.0** and press enter twice.

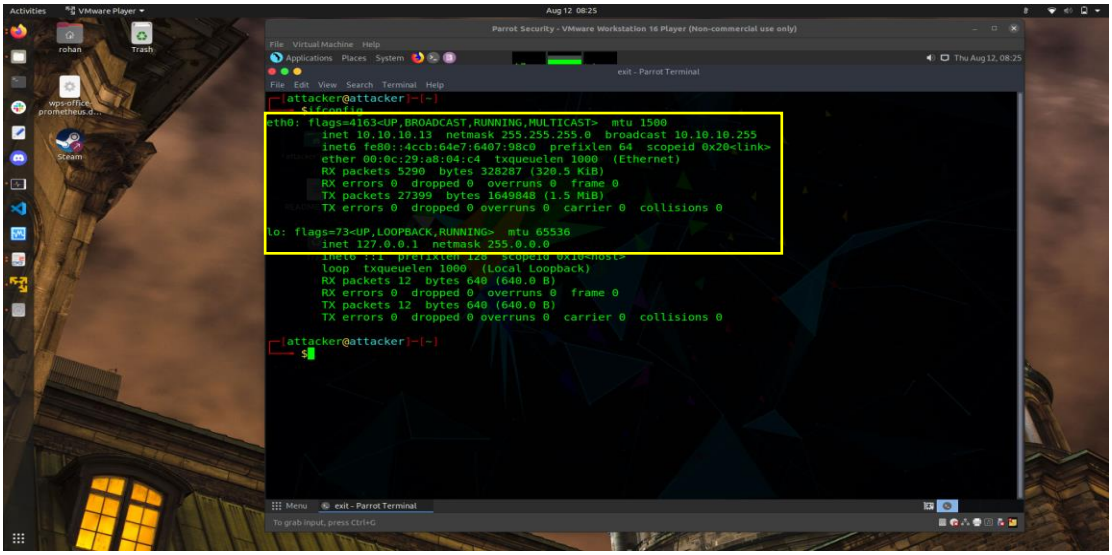


Task 6: Enumerate Web Server Information using Nmap Scripting Engine (NSE)

- Starting both VMs
- Windows Server 19 IP Address

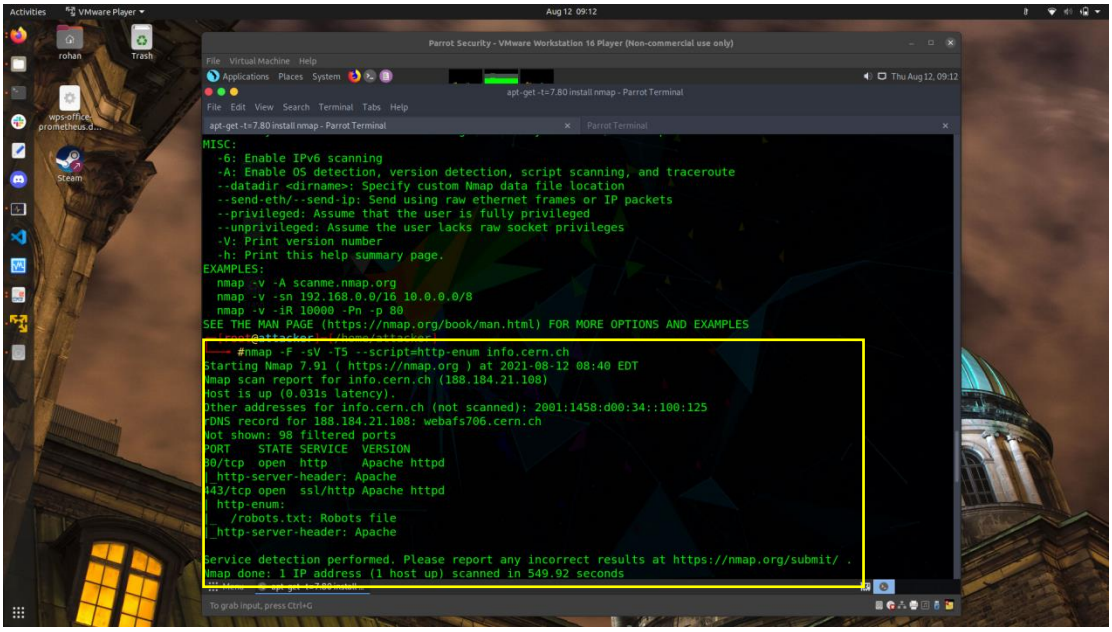


- Parrot IP address

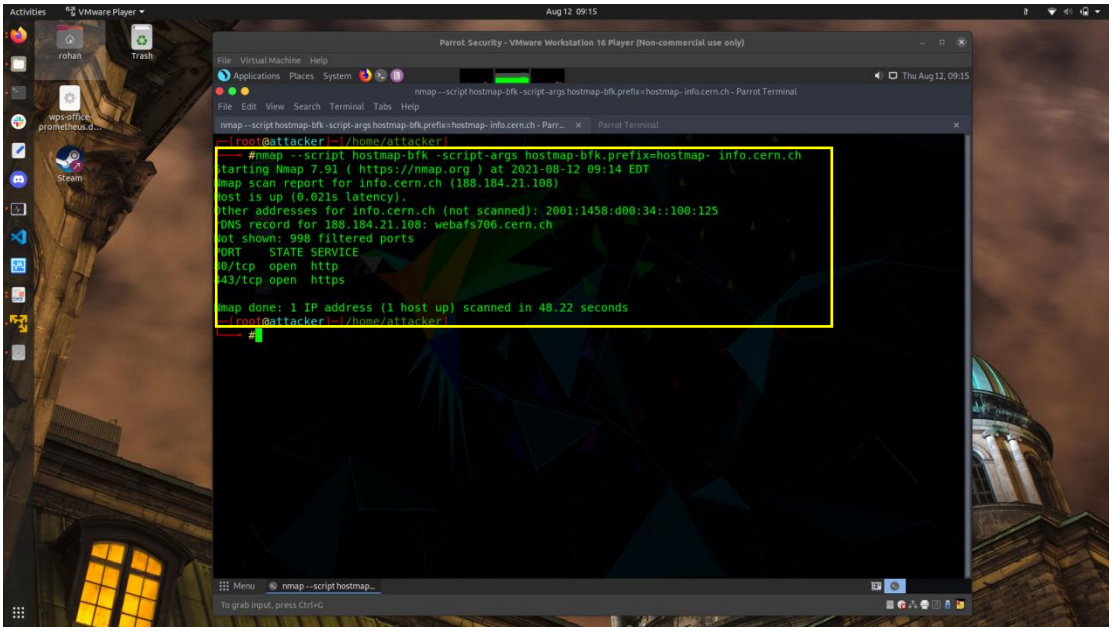


- Target Domain: http://info.cern.ch

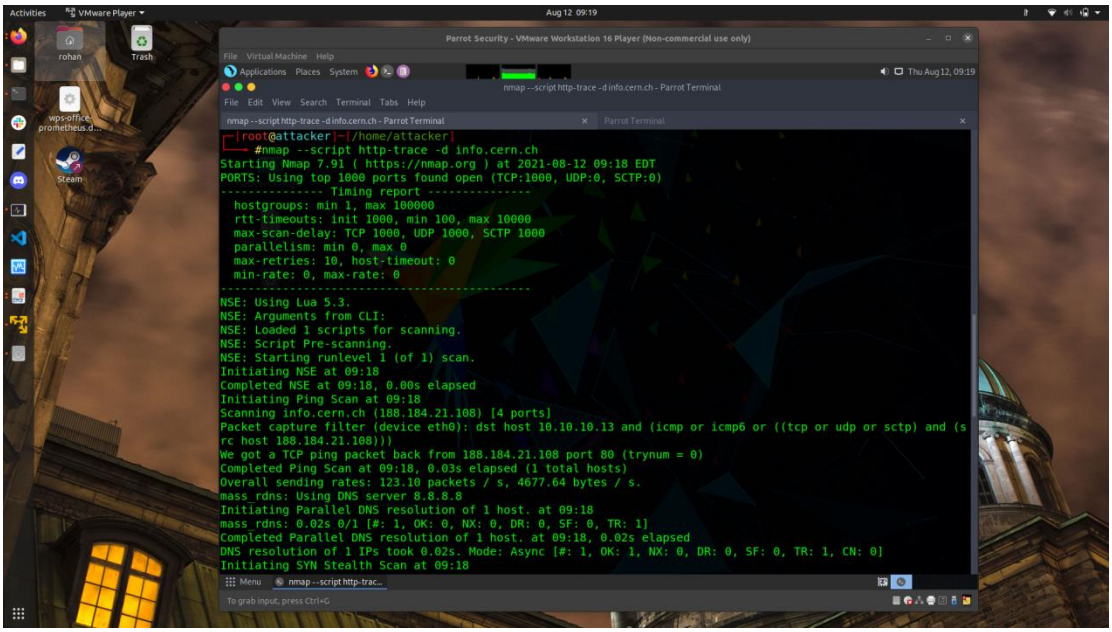
- Step 1: Run Nmap command on Parrot with http-enum script to enumerate the target.

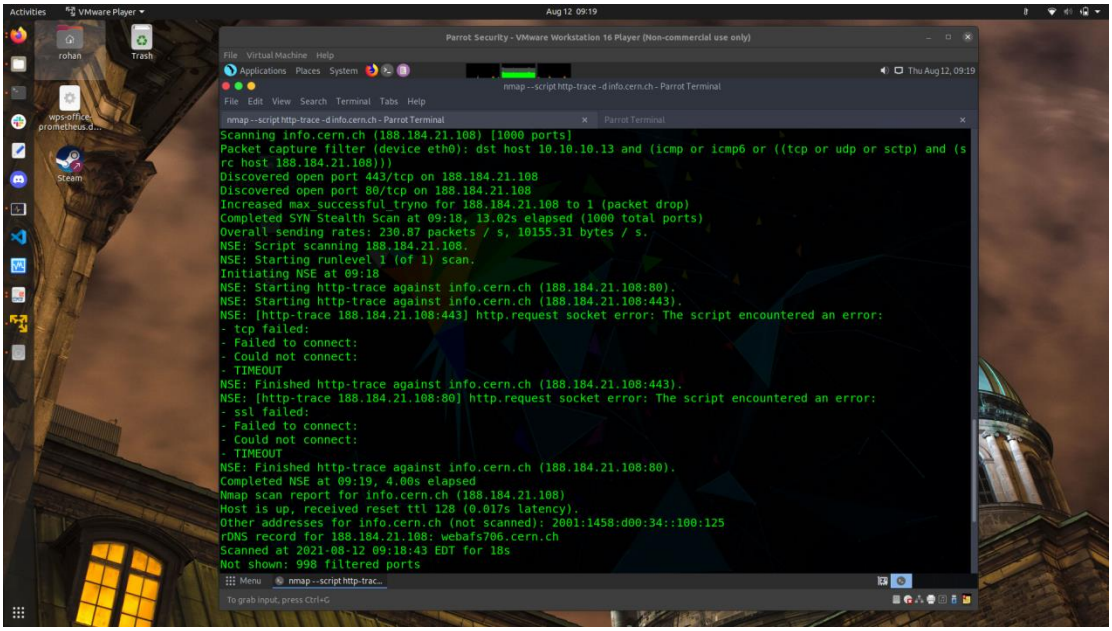


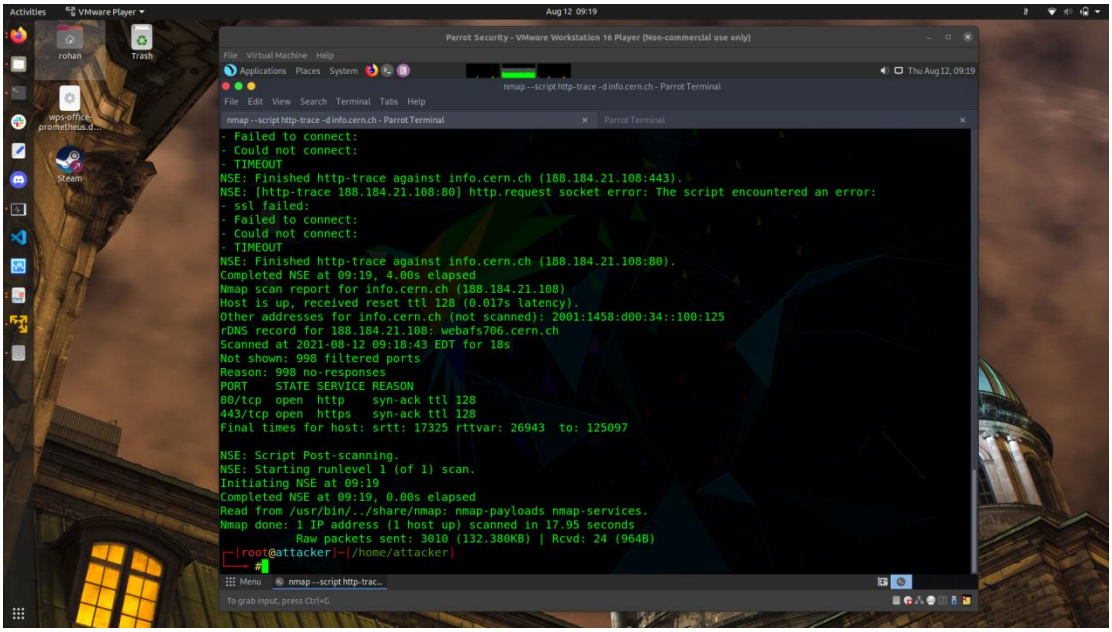
- Step 2: Discover hostname and resolve target domains



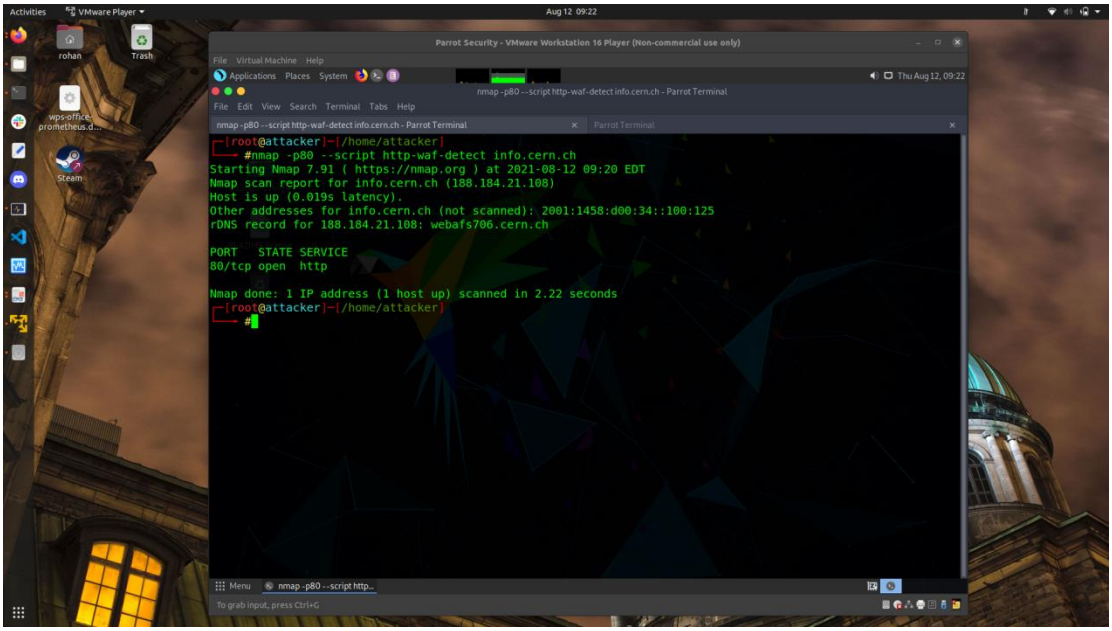
- Step 3: Run HTTP trace on the target domain







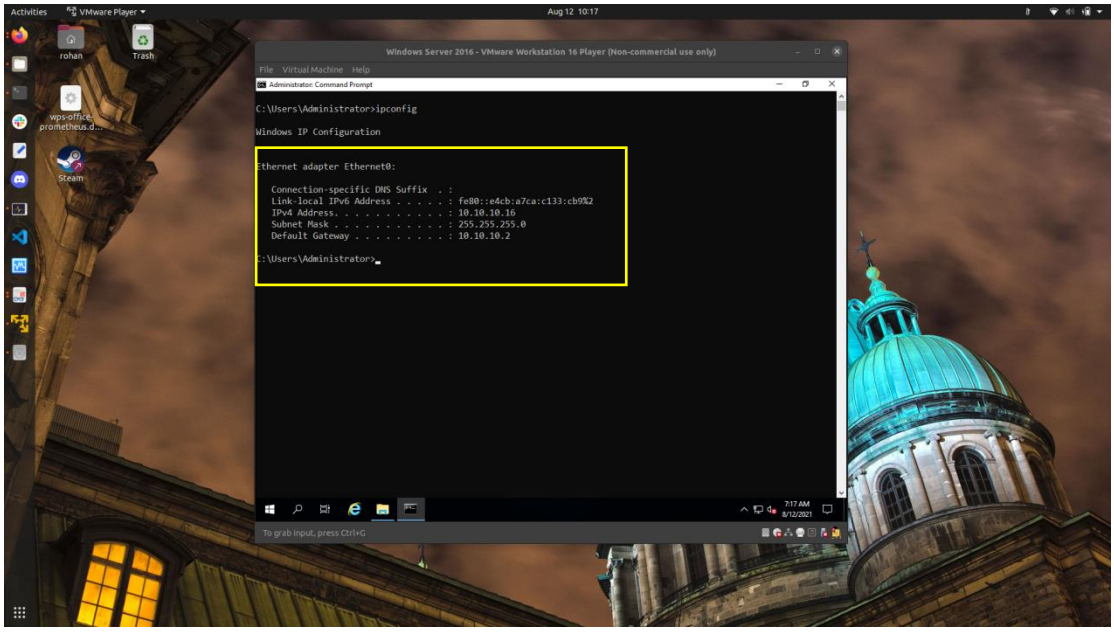
- Step 4: Check for Web Application Firewall, to identify IDS and IPS as well.



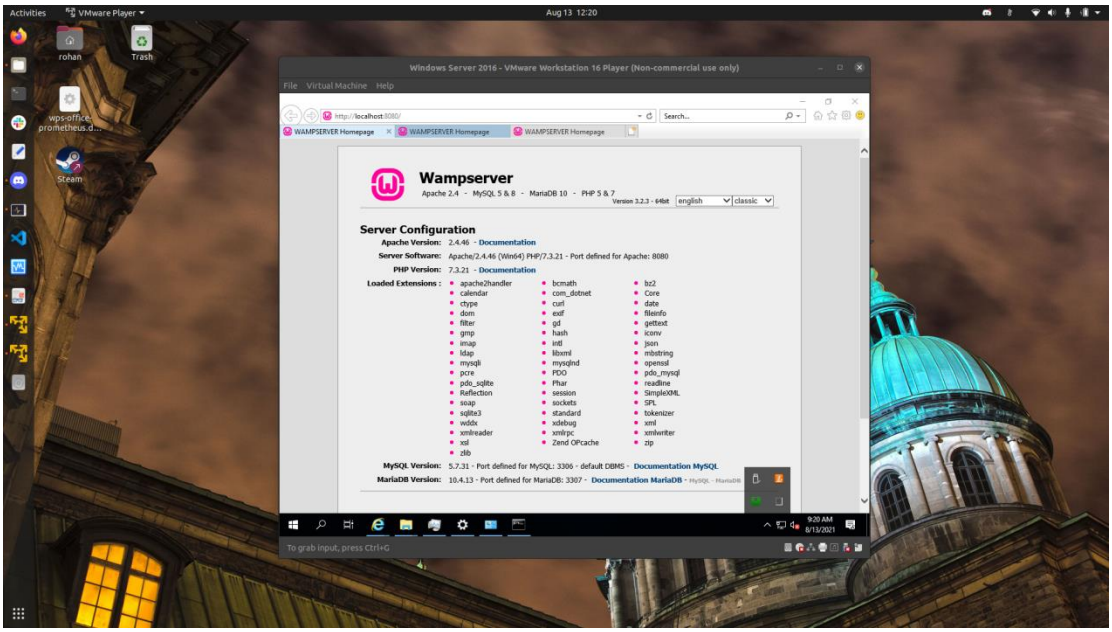
- No WAF detected by above script.

Task 7: Uniscan Web Server Fingerprinting in Parrot Security

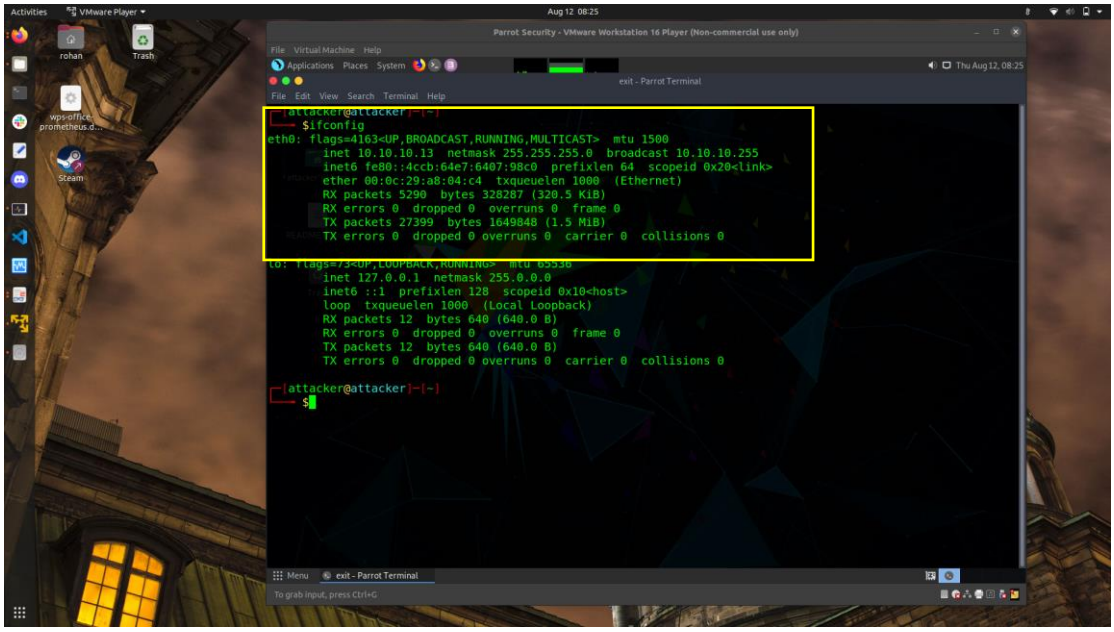
- Step 1: Starting both VMs
- Windows Server 16 IP Address



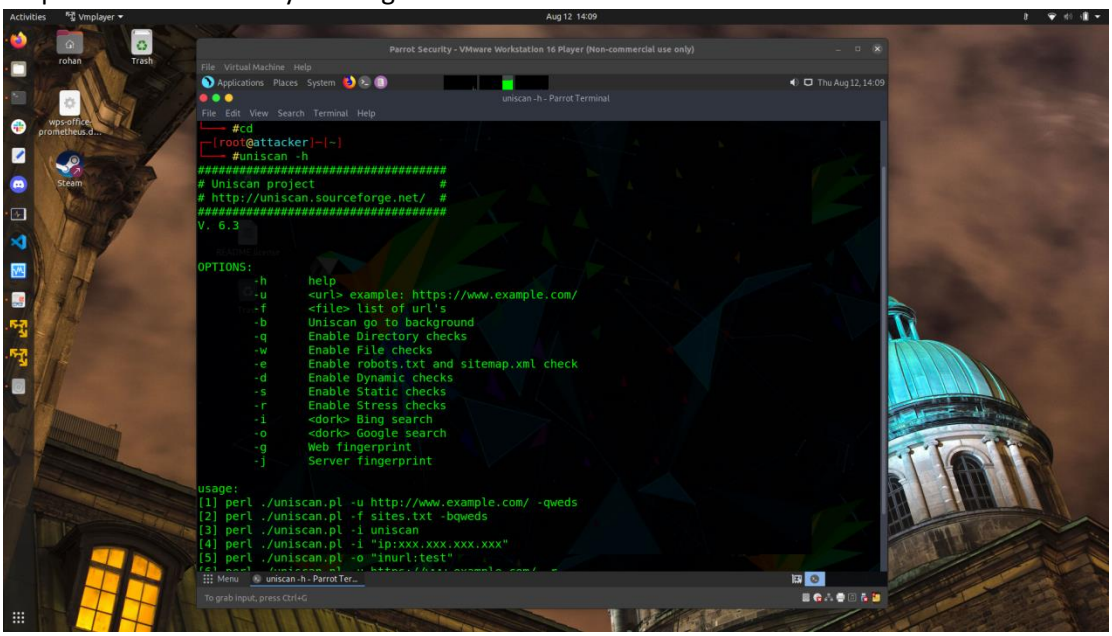
- WAMP server running on Windows Server



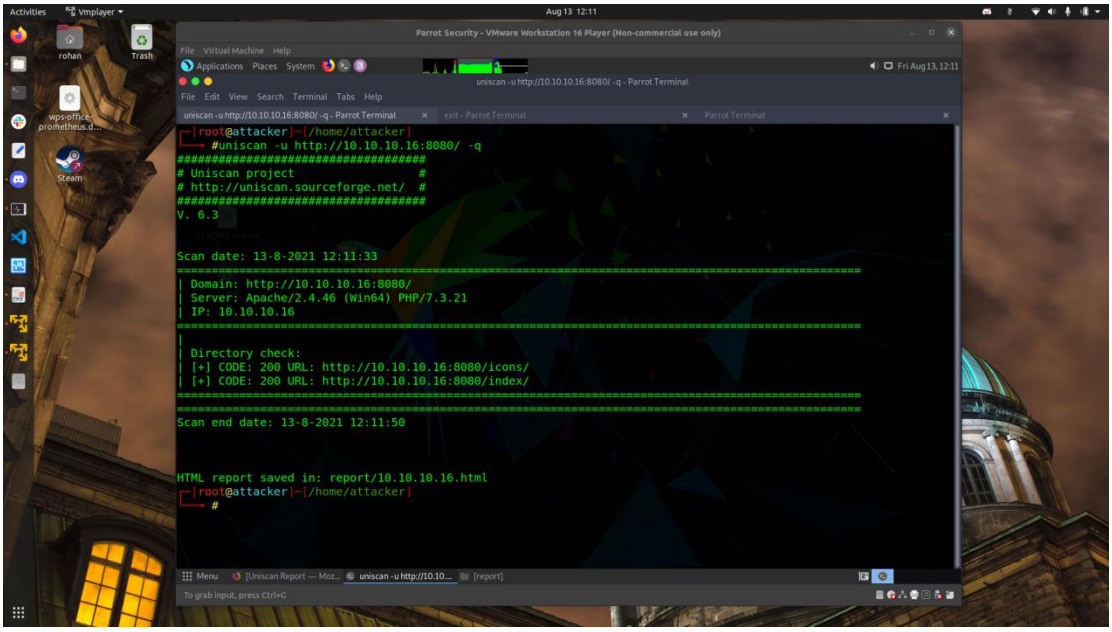
- Parrot IP address



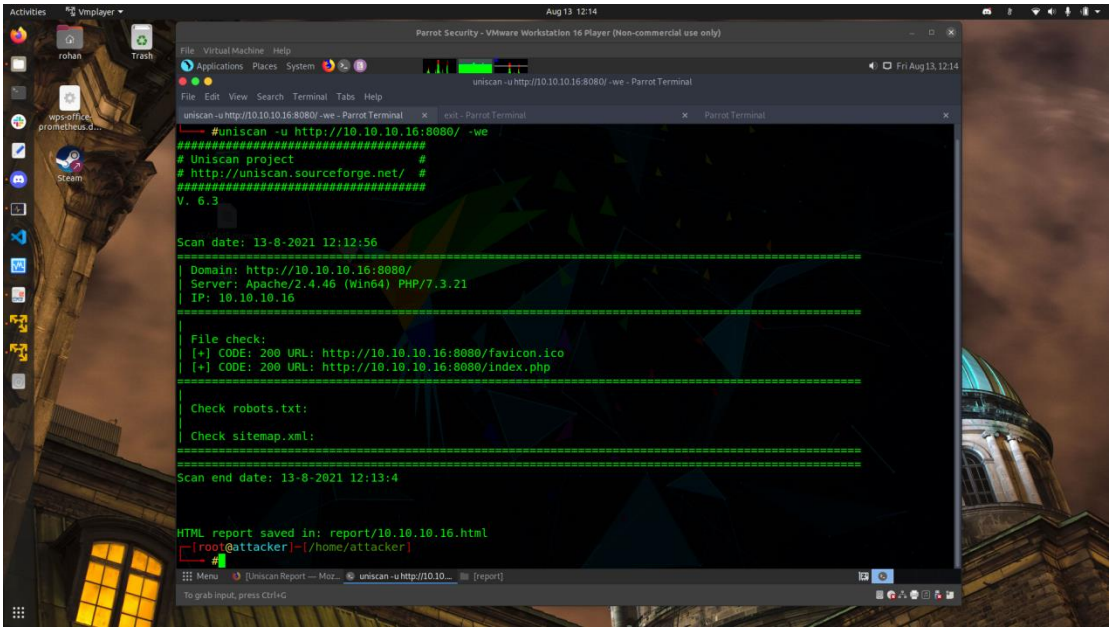
- Step 2: Check uniscan by running *uniscan -h* command



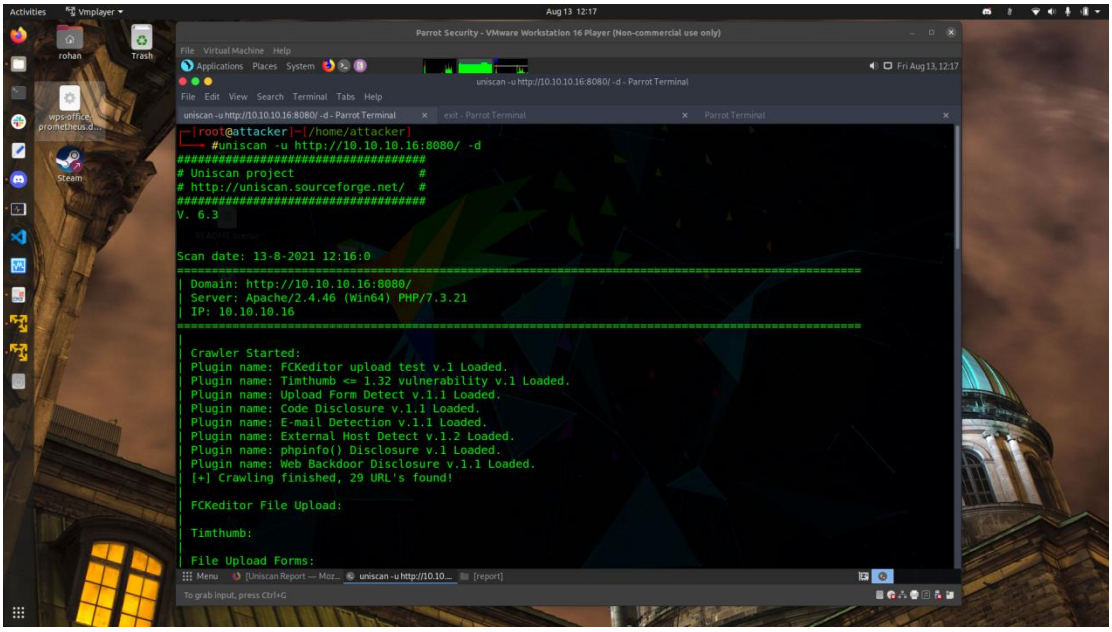
- Step 3: Perform a directory scan on Windows IP (10.10.10.16) on 8080 port.

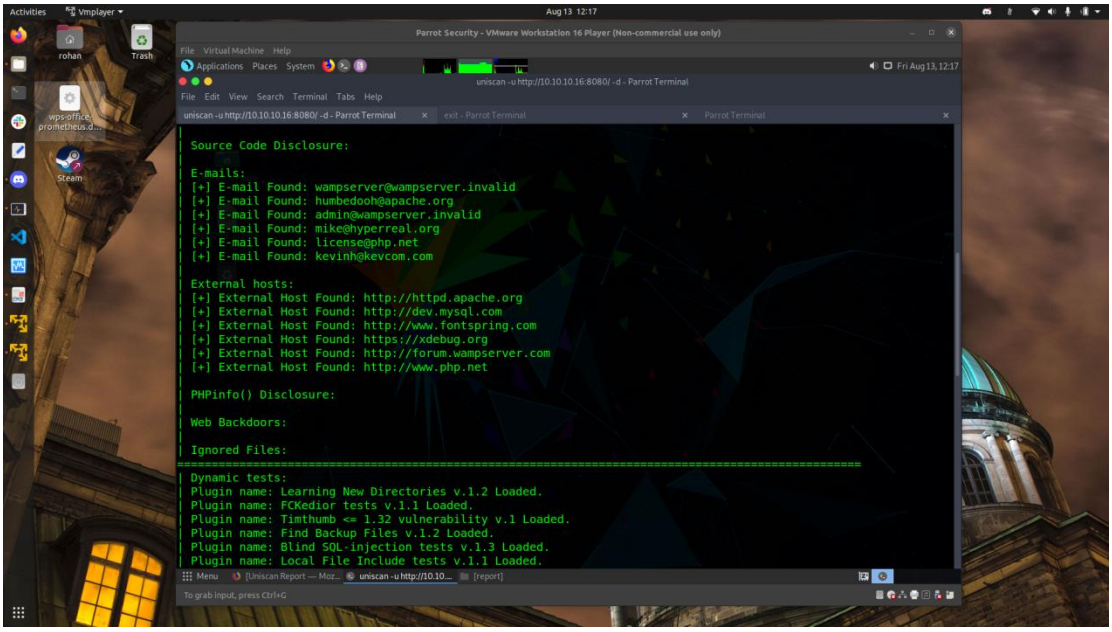


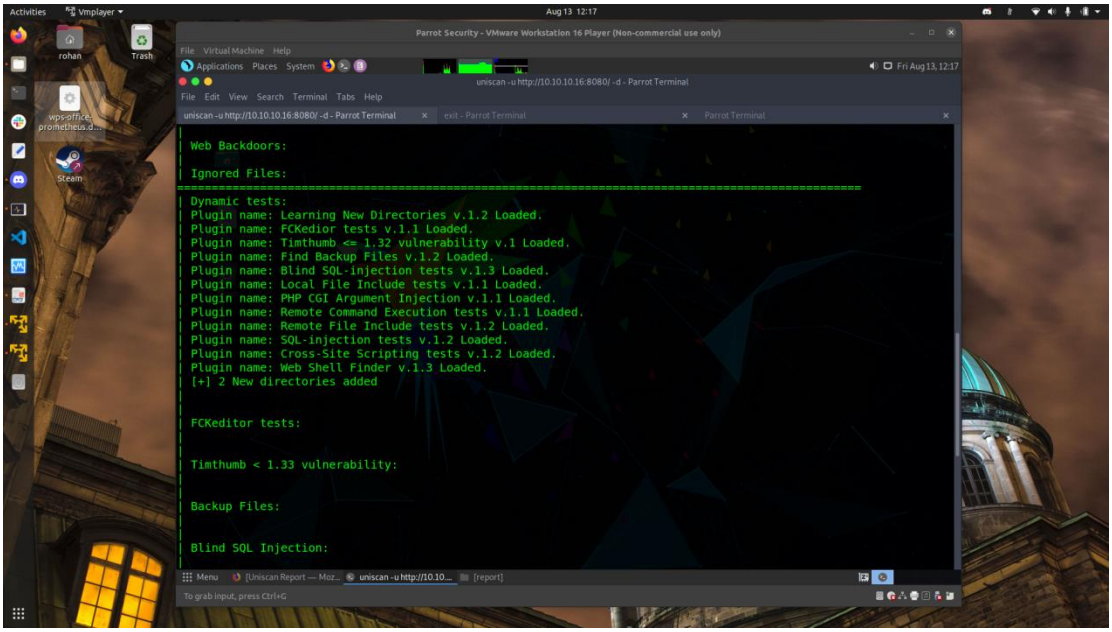
- Step 4: Run filecheck on web server (for robots.txt and sitemap.xml file)

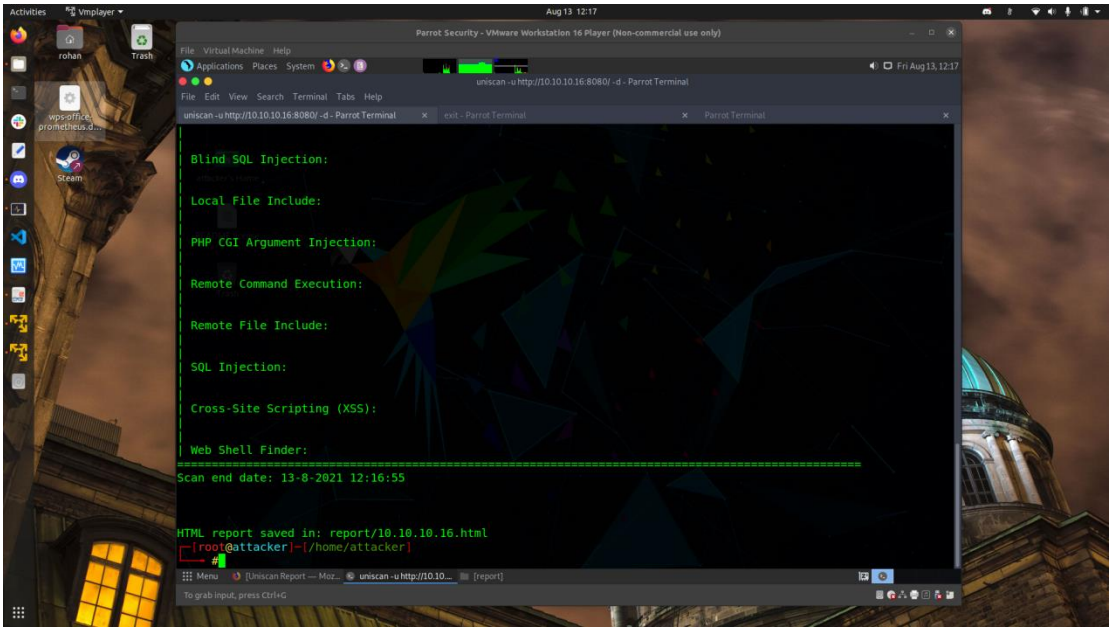


- Step 5: Perform dynamic testing on Web Server

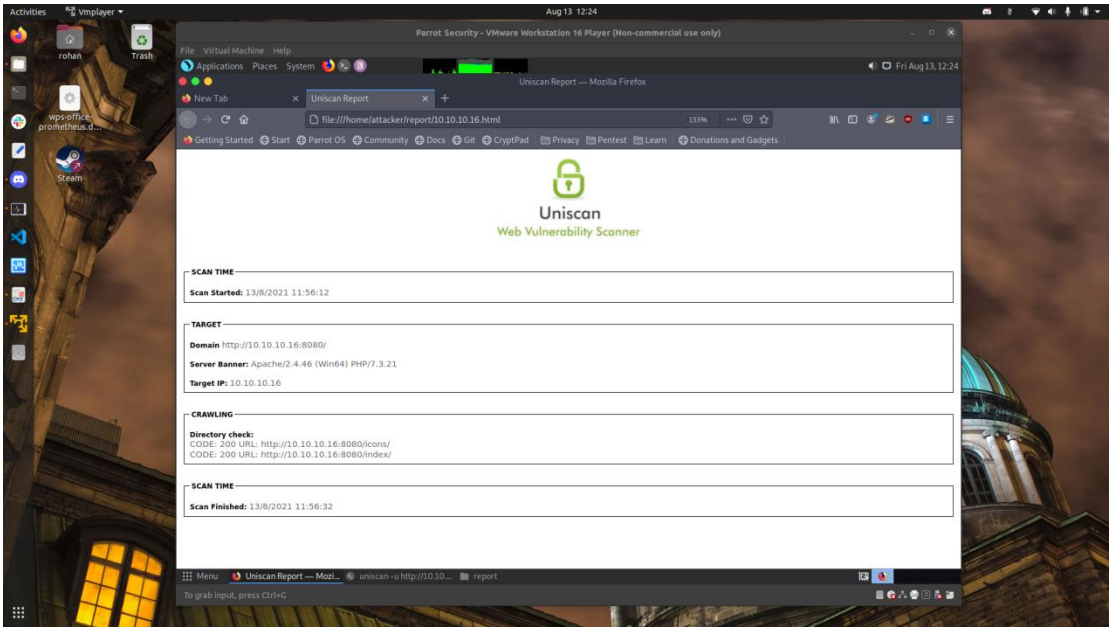


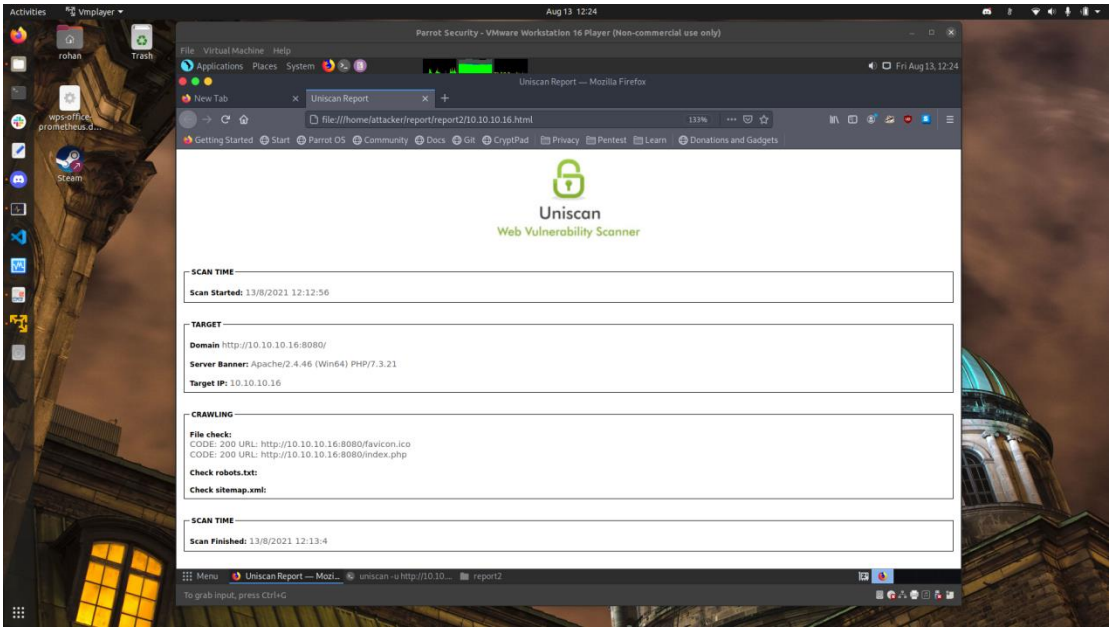


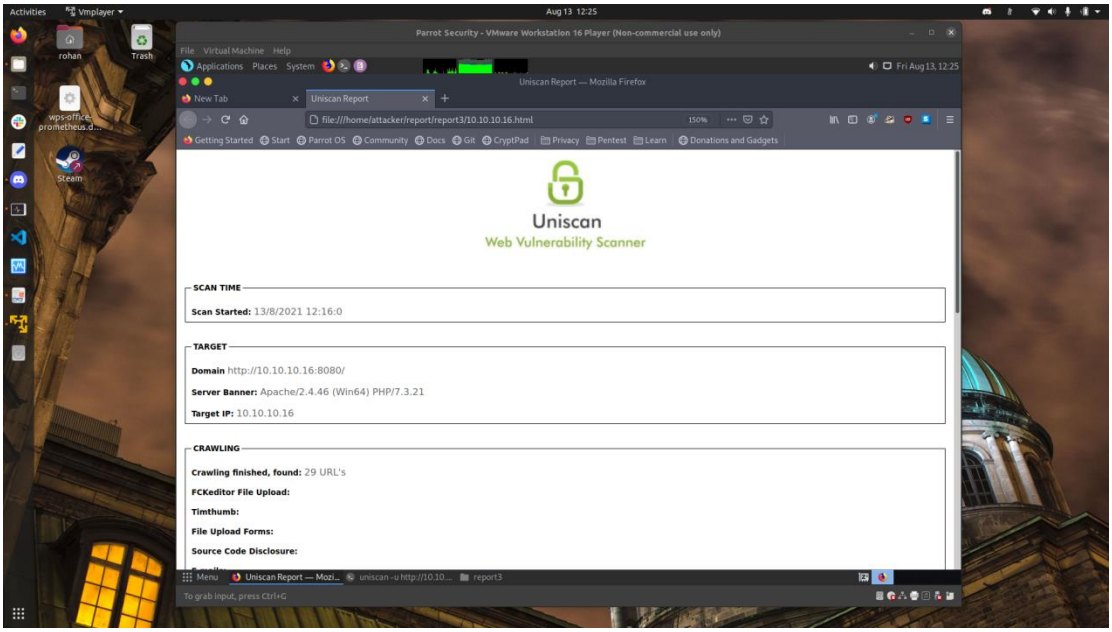

Activities
Vmplayer
Aug 13 12:17
Parrot Security - VMware Workstation 16 Player (Non-commercial use only)
File Virtual Machine Help
Applications Places System
Fri Aug 13, 12:17
uniscan -u http://10.10.10.16:8080/ -d - Parrot Terminal
File Edit View Search Terminal Tabs Help
uniscan -u http://10.10.10.16:8080/ -d - Parrot Terminal
exit - Parrot Terminal
Parrot Terminal
Web Backdoors:
Ignored Files:
Dynamic tests:
Plugin name: Learning New Directories v.1.2 Loaded.
Plugin name: FCKedior 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:
Menu
[Uniscan Report — Moz...
uniscan -u http://10.10...
[report]
To grab input, press Ctrl+G
rohan
Trash
wps-office_prometheus.d...
Steam

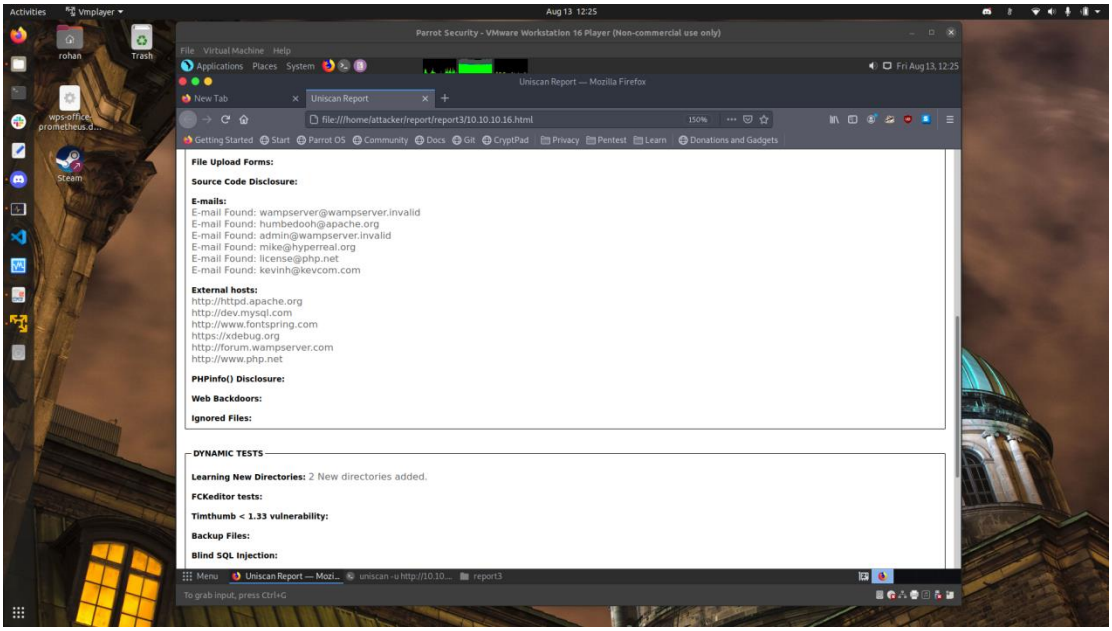

Activities
Vmplayer
Aug 13 12:17
Parrot Security - VMware Workstation 16 Player (Non-commercial use only)
File Virtual Machine Help
Applications Places System
Fri Aug 13, 12:17
uniscan -u http://10.10.10.16:8080/ -d - Parrot Terminal
File Edit View Search Terminal Tabs Help
uniscan -u http://10.10.10.16:8080/ -d - Parrot Terminal
exit - Parrot Terminal
Parrot Terminal
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]
#
Menu
[Uniscan Report — Moz...
uniscan -u http://10.10...
[report]
To grab input, press Ctrl+G
rohan
Trash
wps-office_prometheus.d...
Steam

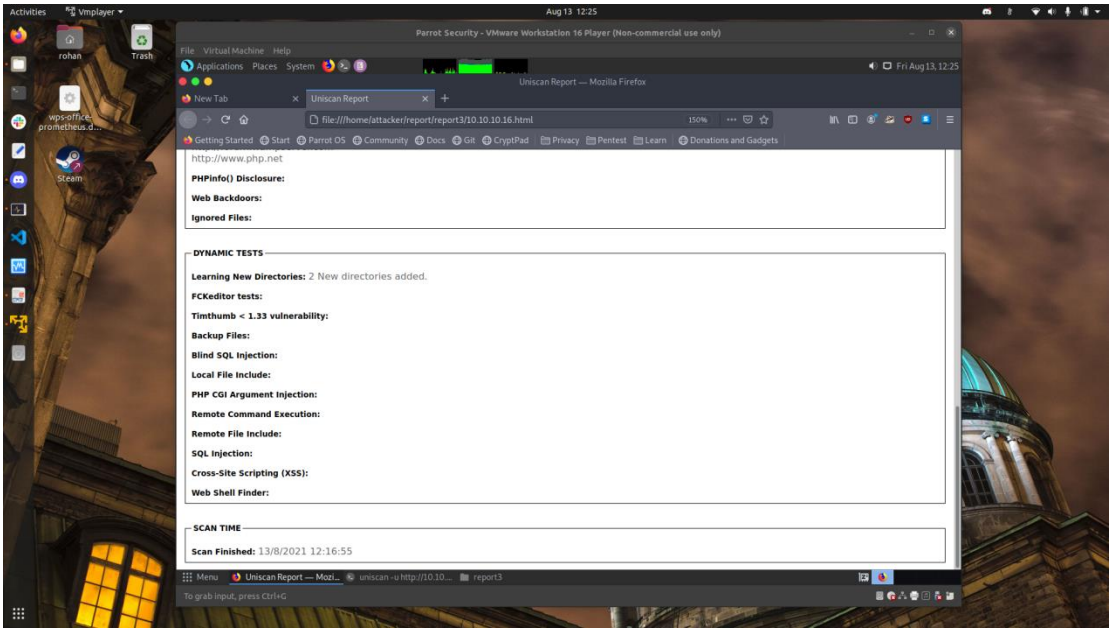
- Step 6: View report





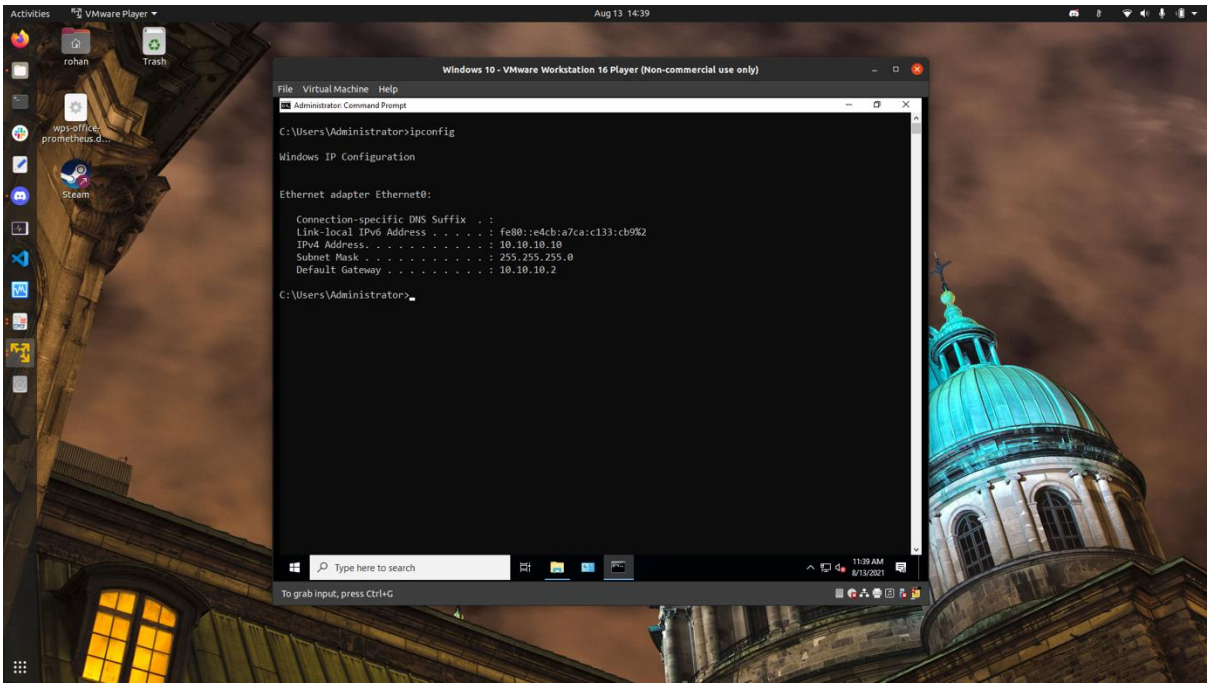

Uniscan
Web Vulnerability Scanner
SCAN TIME
Scan Started: 13/8/2021 12:16:0
TARGET
Domain http://10.10.10.16:8080/
Server Banner: Apache/2.4.46 (Win64) PHP/7.3.21
Target IP: 10.10.10.16
CRAWLING
Crawling finished, found: 29 URL's
FCKeditor File Upload:
Timthumb:
File Upload Forms:
Source Code Disclosure:


File Upload Forms:
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: kevinh@kevcom.com
External hosts:
http://httpd.apache.org
http://dev.mysql.com
http://www.fontspring.com
https://xdebug.org
http://forum.wampserver.com
http://www.php.net
PHPinfo() Disclosure:
Web Backdoors:
Ignored Files:
DYNAMIC TESTS
Learning New Directories: 2 New directories added.
FCKeditor tests:
Timthumb < 1.33 vulnerability:
Backup Files:
Blind SQL Injection:

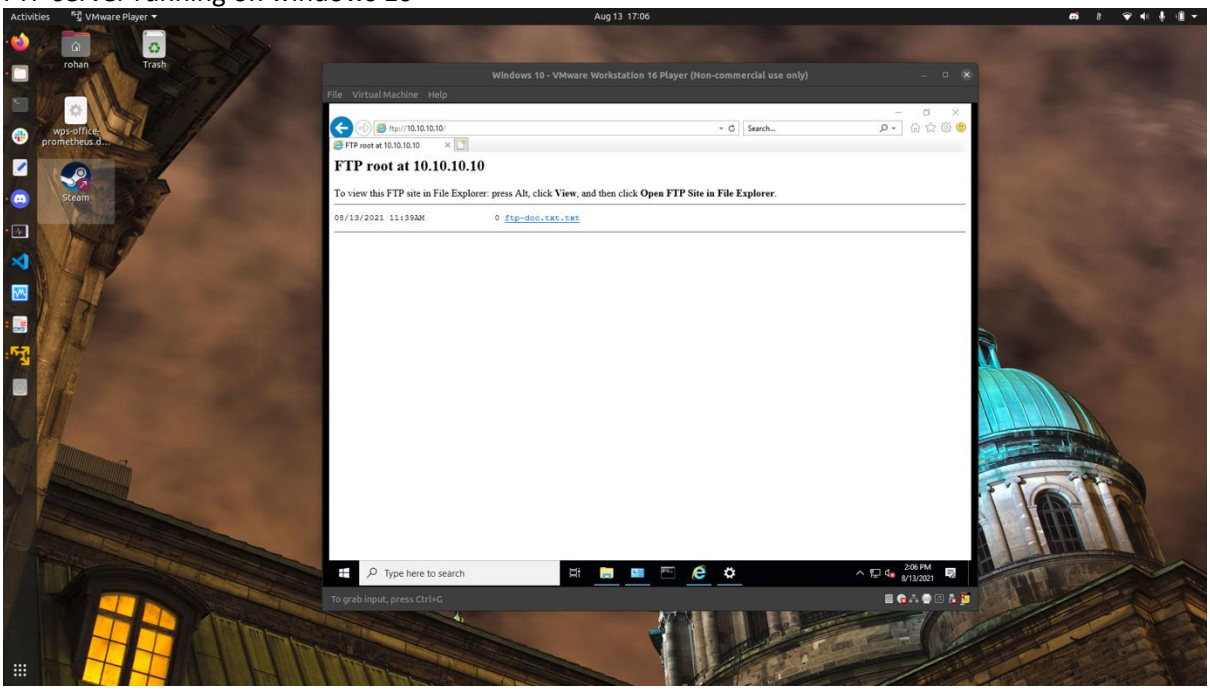

Activities
Vmplayer
Aug 13 12:25
Parrot Security - VMware Workstation 16 Player (Non-commercial use only)
File Virtual Machine Help
Applications Places System
Fri Aug 13, 12:25
Uniscan Report — Mozilla Firefox
New Tab
Uniscan Report
file:///home/attacker/report/report3/10.10.10.16.html
150%
Getting Started Start Parrot OS Community Docs Git CryptPad Privacy Pentest Learn Donations and Gadgets
http://www.php.net
PHPinfo() Disclosure:
Web Backdoors:
Ignored Files:
DYNAMIC TESTS
Learning New Directories: 2 New directories added.
FCKeditor tests:
Timthumb < 1.33 vulnerability:
Backup Files:
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 TIME
Scan Finished: 13/8/2021 12:16:55
Menu
Uniscan Report — Mozi...
uniscan -u http://10.10...
report3
To grab input, press Ctrl+G
rohan
Trash
wps-office-prometheus.d...
Steam

Lab 2: 1.1Crack FTP credentials using a Dictionary Attack

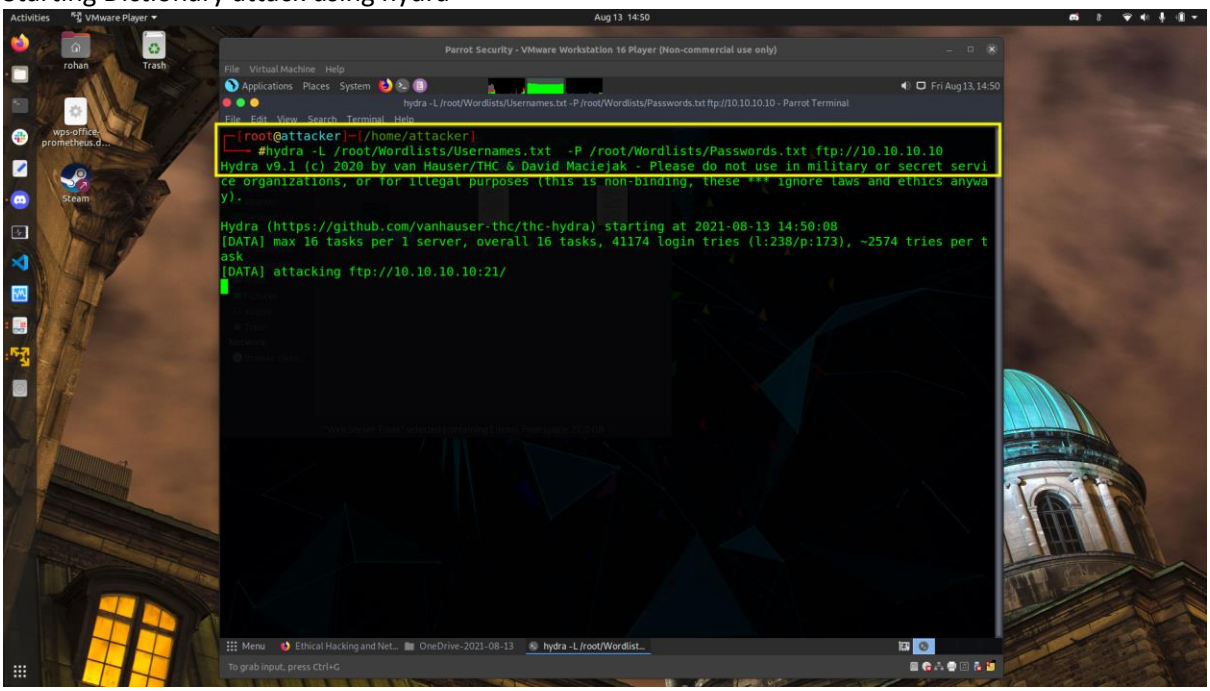
- Windows virtual machine IP



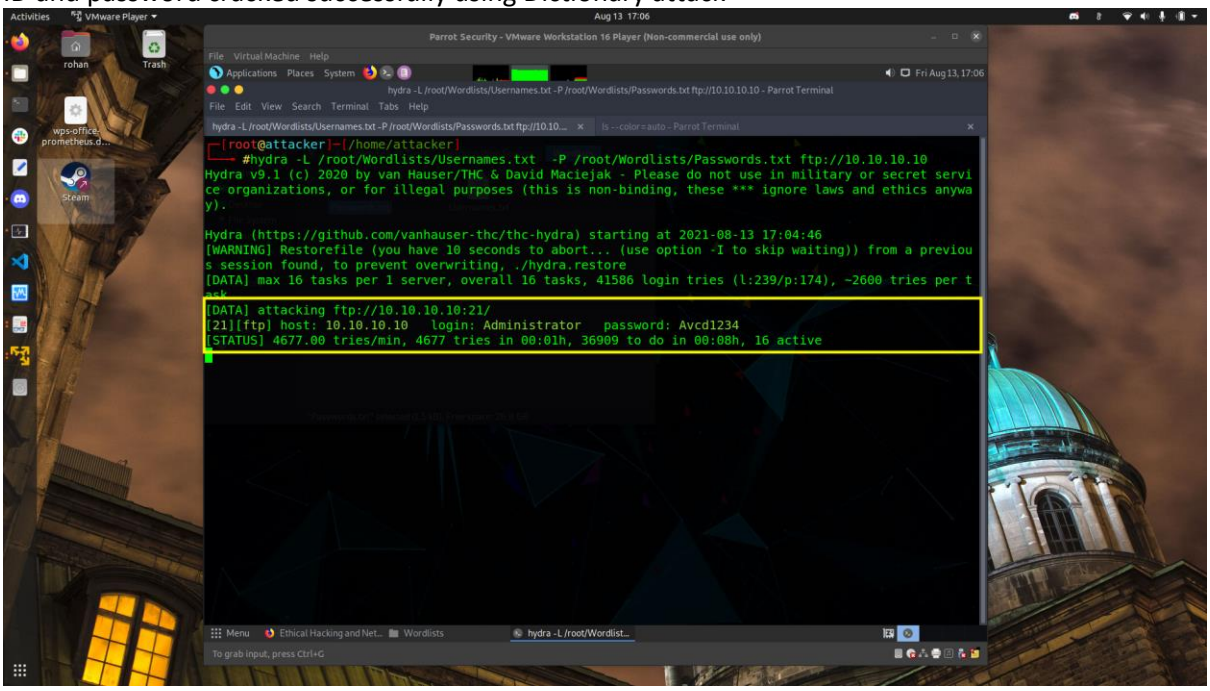
- FTP server running on windows 10



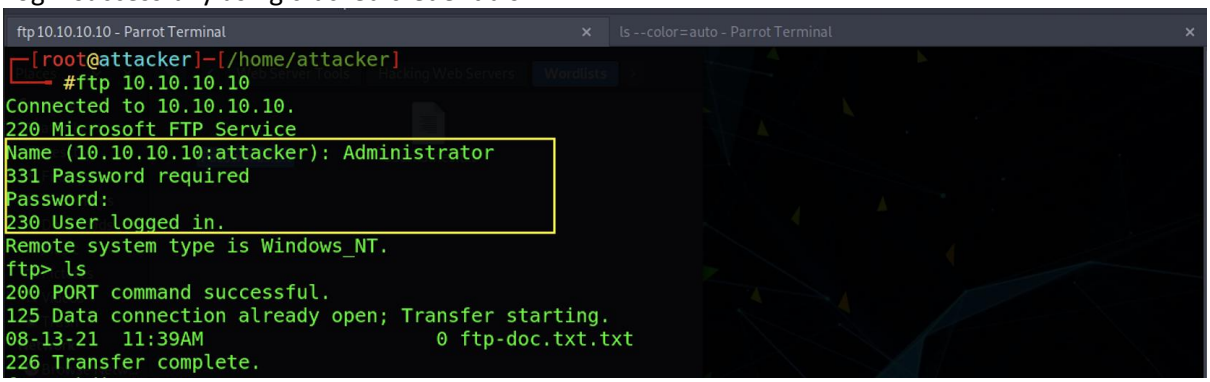
- Starting Dictionary attack using hydra



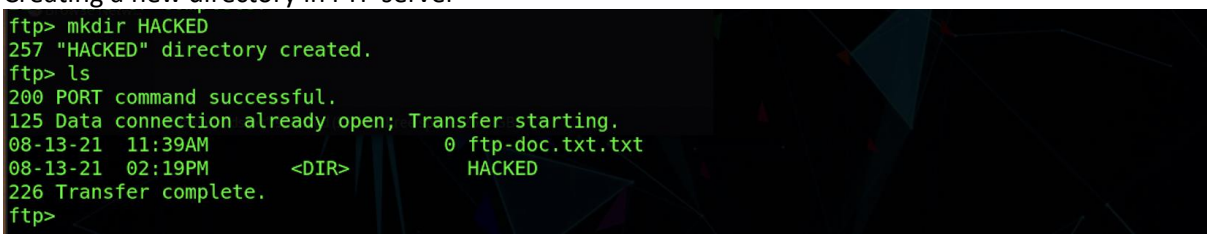
- ID and password cracked successfully using Dictionary attack



- Login successfully using cracked credentials



- Creating a new directory in FTP server



- New Directory created on FTP server by attacker