Module 02: Ethical Hacking Fundamentals

Scenario

Ethical hacking involves the use of hacking tools, tricks, and techniques to identify vulnerabilities and ensure system security. It focuses on simulating the techniques used by attackers to verify the existence of exploitable vulnerabilities in a system's security. Ethical hackers perform security assessments for an organization with the permission of concerned authorities.

The labs in this module will give you real-time experience in understanding different phases of hacking cycle.

Objective

The objective of the lab is to extract information about the target organization that includes, but is not limited to:

- **Organization Information** Employee details, partner details, weblinks, web technologies, patents, trademarks, etc.
- **Network Information** Domains, sub-domains, network blocks, network topologies, trusted routers, firewalls, IP addresses of the reachable systems, the Whois record, DNS records, and other related information
- **System Information** Operating systems, web server OSes, user accounts and passwords, etc.

Overview of Ethical Hacking

Ethical hacking is the practice of employing computer and network skills in order to assist organizations in testing their network security for possible loopholes and vulnerabilities. White Hats (also known as security analysts or ethical hackers) are the individuals or experts who perform ethical hacking.

Nowadays, most organizations (such as private companies, universities, and government organizations) are hiring White Hats to assist them in enhancing their cybersecurity. They perform hacking in ethical ways, with the permission of the network or system owner and without the intention to cause harm. Ethical hackers report all vulnerabilities to the system and network owner for remediation, thereby increasing the security of an organization's information system.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to collect information about the target. Recommended labs that will assist you in learning various footprinting techniques include:

1. Perform passive footprinting to gather information about a target
    - Gather information using advanced google hacking techniques
    - Extract a company's data using Web Data Extractor
    - Perform whois lookup using DomainTools
2. Perform network scanning to identify live hosts, open ports and services and target OS in the network
    - Perform network tracerouting in Windows and Linux machines
    - Perform host discovery using Nmap
    - Perform port and service discovery using MegaPing
    - Perform OS discovery using Unicornscan
3. Perform enumeration on a system or network to extract usernames, machine names, network resources, shares, etc.
    - Perform NetBIOS enumeration using Windows Command-Line utilities
    - Perform NetBIOS enumeration using NetBIOS Enumerator

Lab 2-1: Perform Passive Footprinting to Gather Information About a Target

Lab Scenario

Passive footprinting involves gathering information about the target without direct interaction. It is mainly useful when the information gathering activities are not to be detected by the target. Performing passive footprinting is technically difficult, as active traffic is not sent to the target organization from a host or anonymous hosts or services over the Internet. We can only collect archived and stored information about the target using search engines, social networking sites, and so on.

Lab Objectives

- Gather Information using Advanced Google Hacking Techniques
- Extract a Company's Data using Web Data Extractor
- Perform Whois Lookup using DomainTools

Task 1: Gather Information using Advanced Google Hacking Techniques

Advanced Google hacking refers to the art of creating complex search engine queries by employing advanced Google operators to extract sensitive or hidden information about a target company from the Google search results. This can provide information about websites that are vulnerable to exploitation. Note: Here, we will consider EC-Council as a target organization.

Here, we will consider **EC-Council** as a target organization.

1. By default **Windows 10** machine selected, click Ctrl+Alt+Delete.

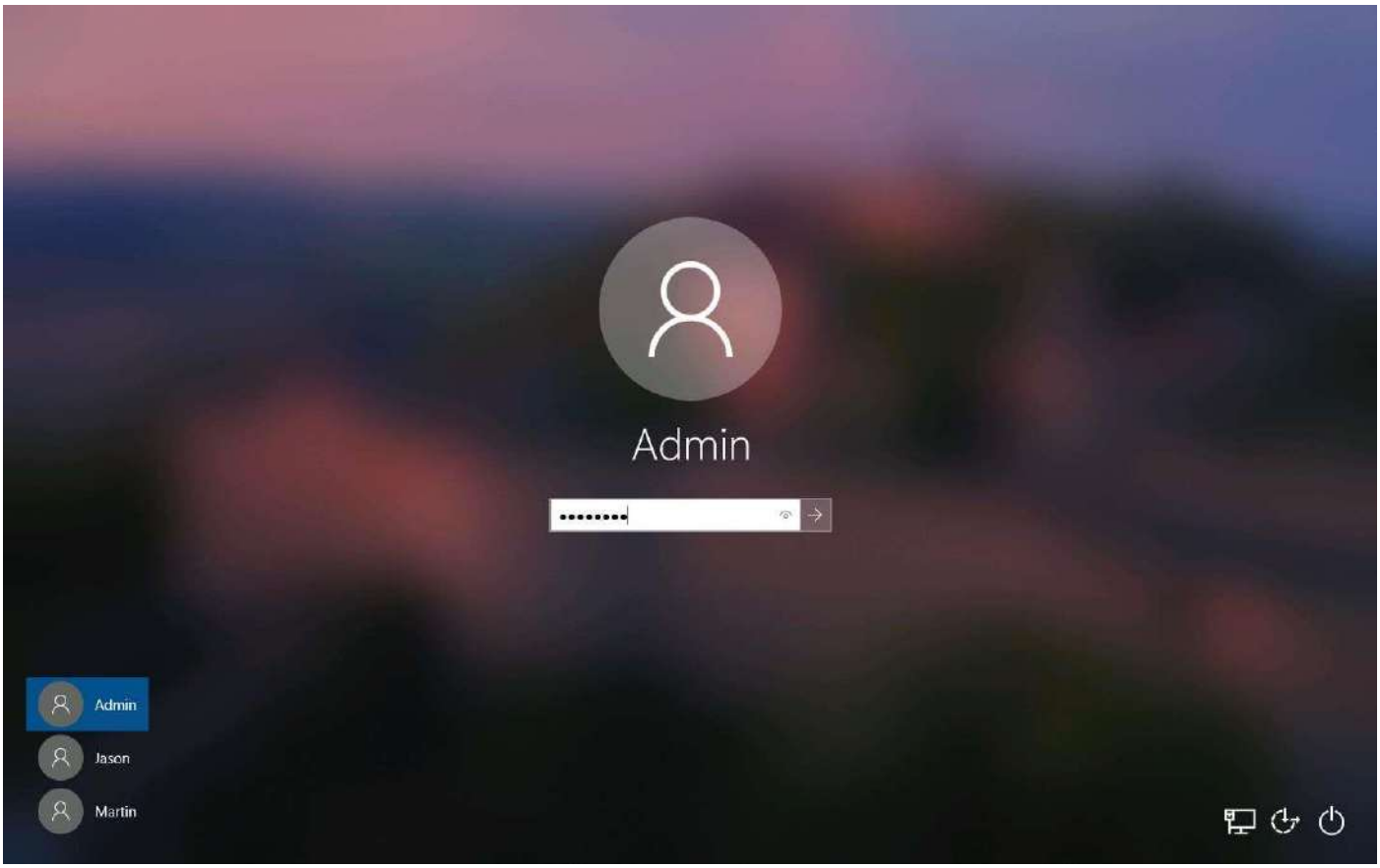
Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 10** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under Commands (**thunder** icon) menu.

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

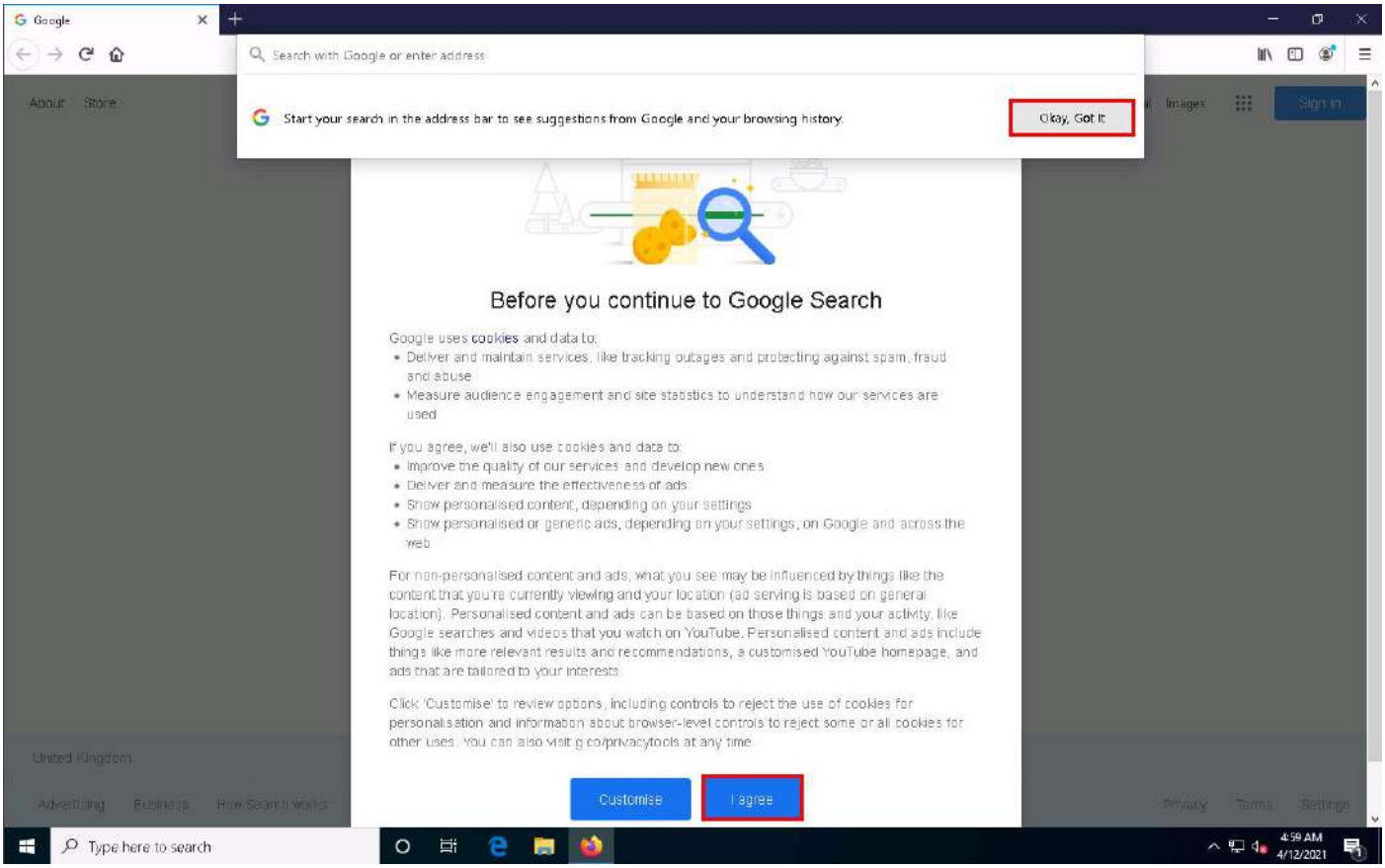
Alternatively, you can also click **Pa$$w0rd** under **Windows 10** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

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

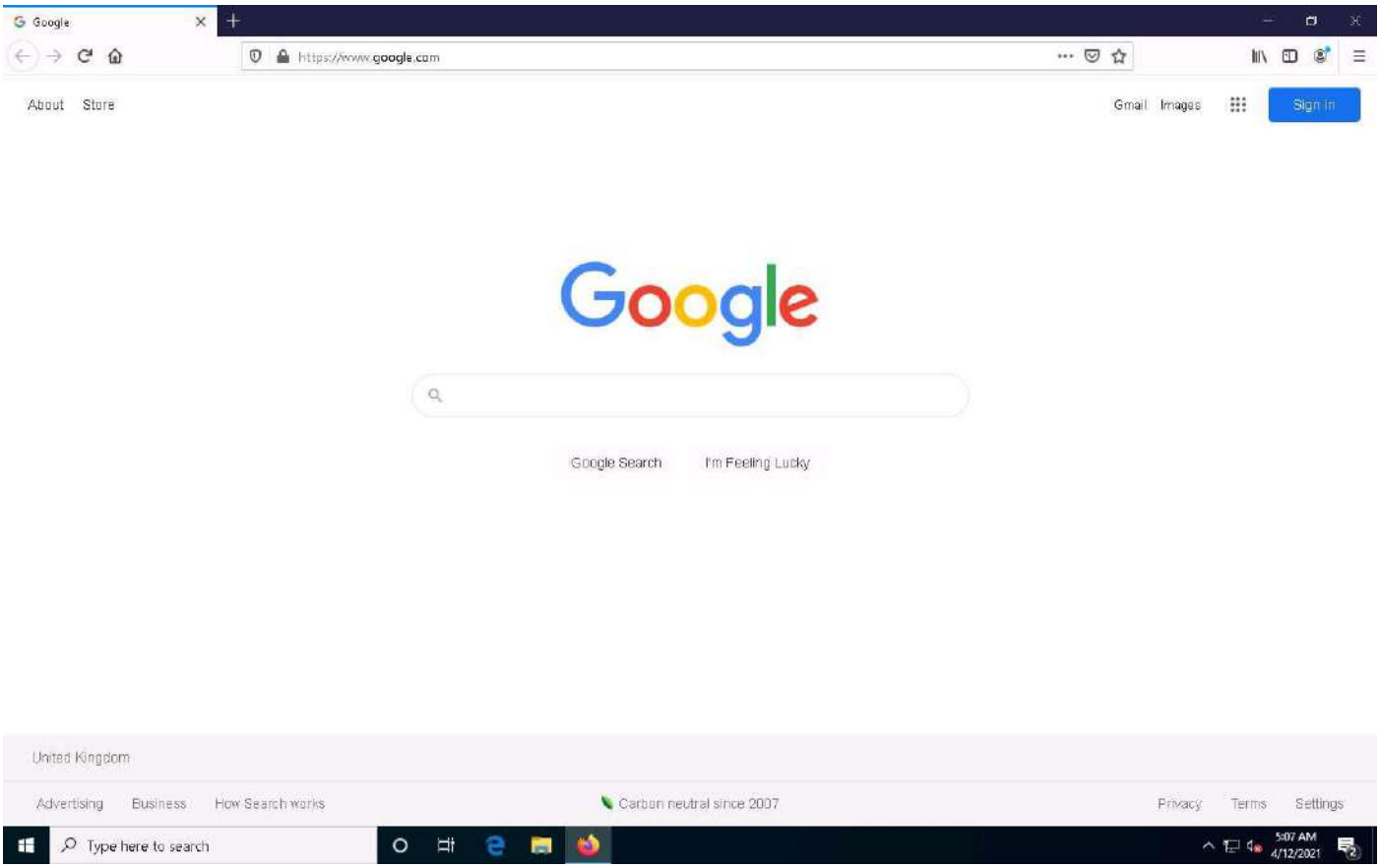


3. Launch any browser, in this lab we are using **Mozilla Firefox**. In the address bar of the browser place your mouse cursor and click https://www.google.com and press **Enter**.
    - If the **Default Browser** pop-up window appears, uncheck the **Always perform this check when starting Firefox** checkbox and click the **Not now** button.
    - If a **New in Firefox: Content Blocking** pop-up window appears, follow the step and click **Got it** to finish viewing the information.
4. If a notification appears at the top section of a browser window, click **Okay, Got it** and in **Before you continue to Google Search** wizard, click **I agree** button.

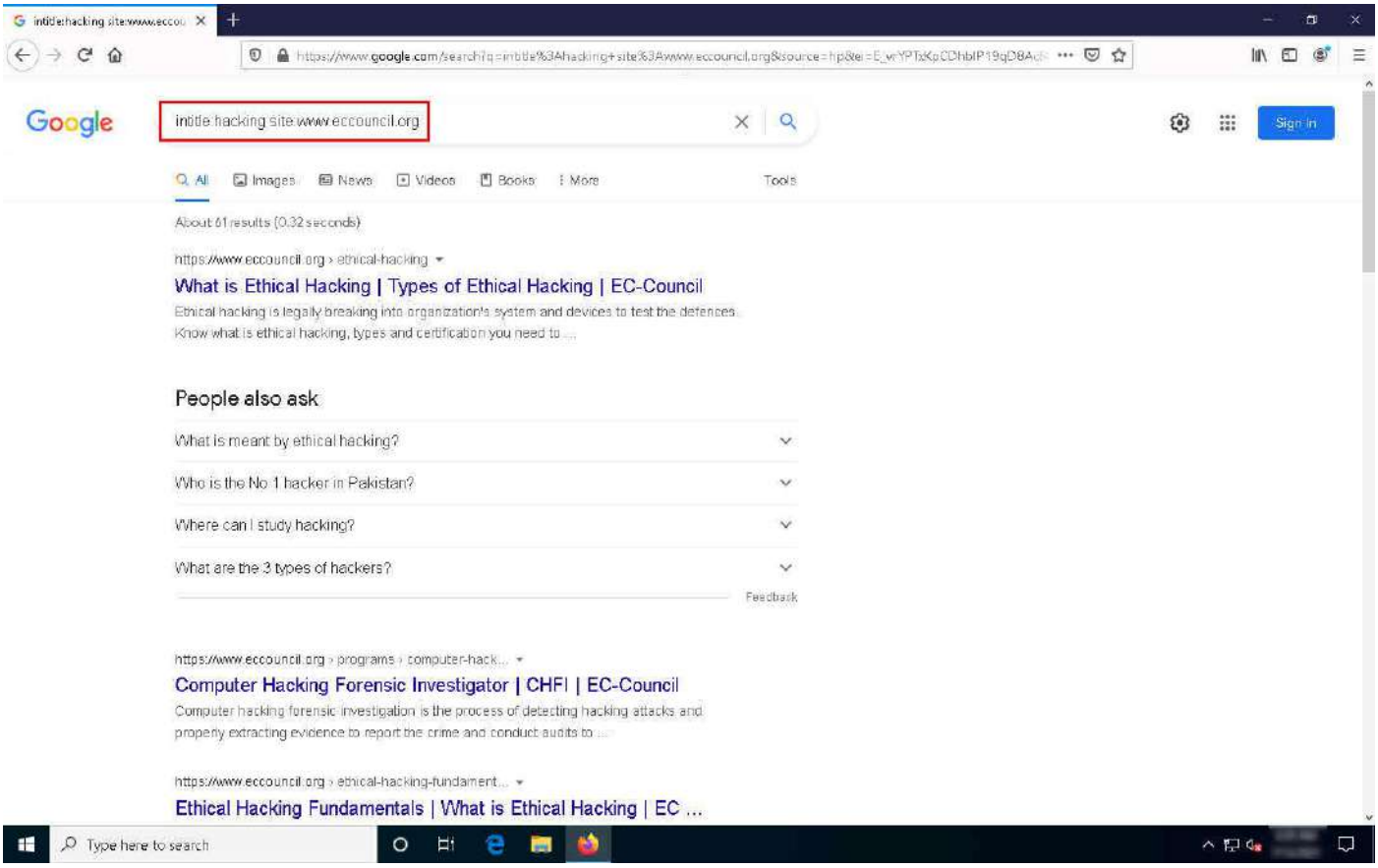


5. Once the **Google** search engine appears, you should see a search bar, as shown in the screenshot.

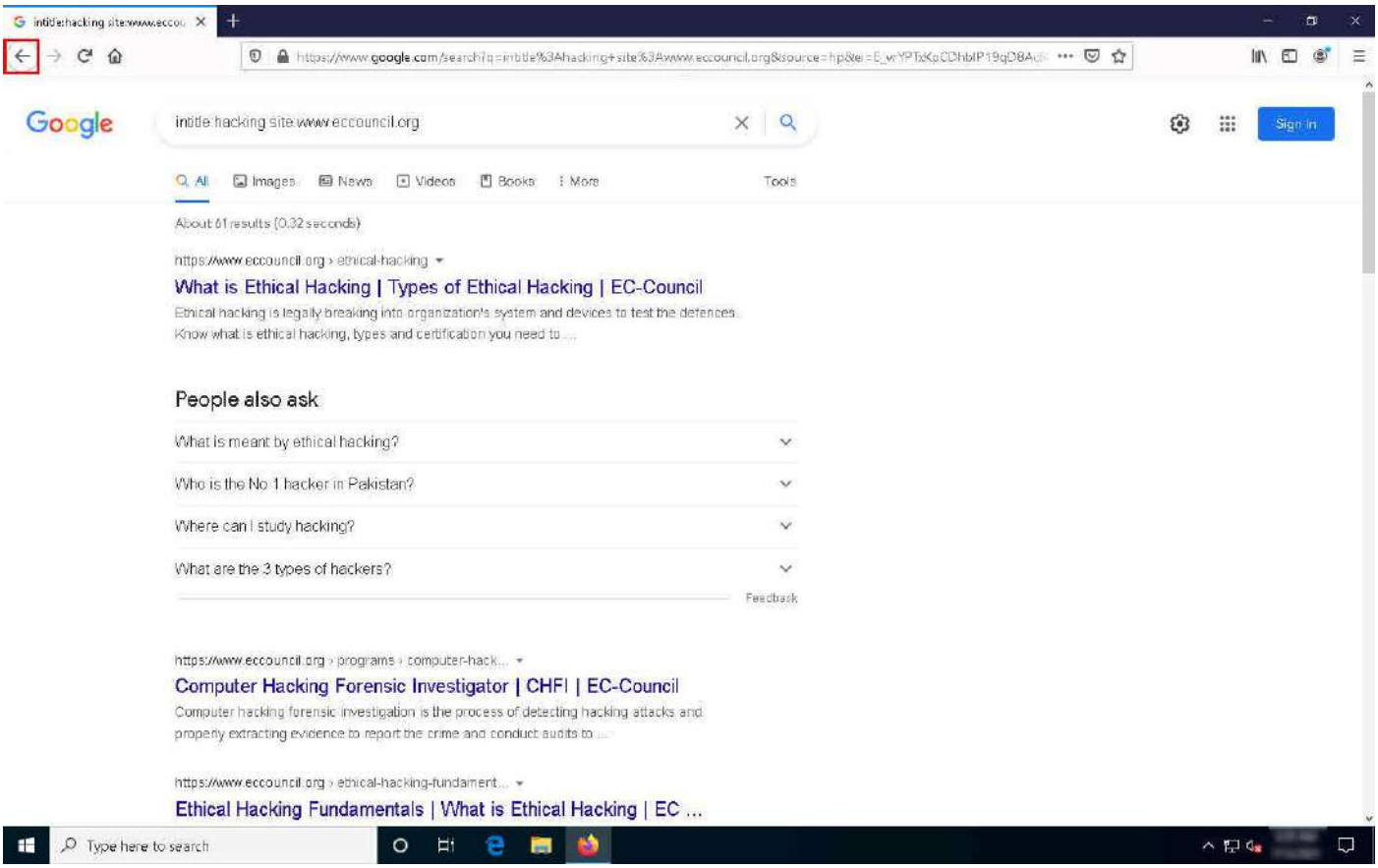
If any pop-up window appears at the top-right corner, click **No, thanks**.



6. Type **intitle:hacking site:www.eccouncil.org** and press **Enter**. This search command uses **intitle** and **site** Google advanced operators, which restrict results to pages on the **www.eccouncil.org** website that contain the term **hacking** in the title. An example is shown in the screenshot below.



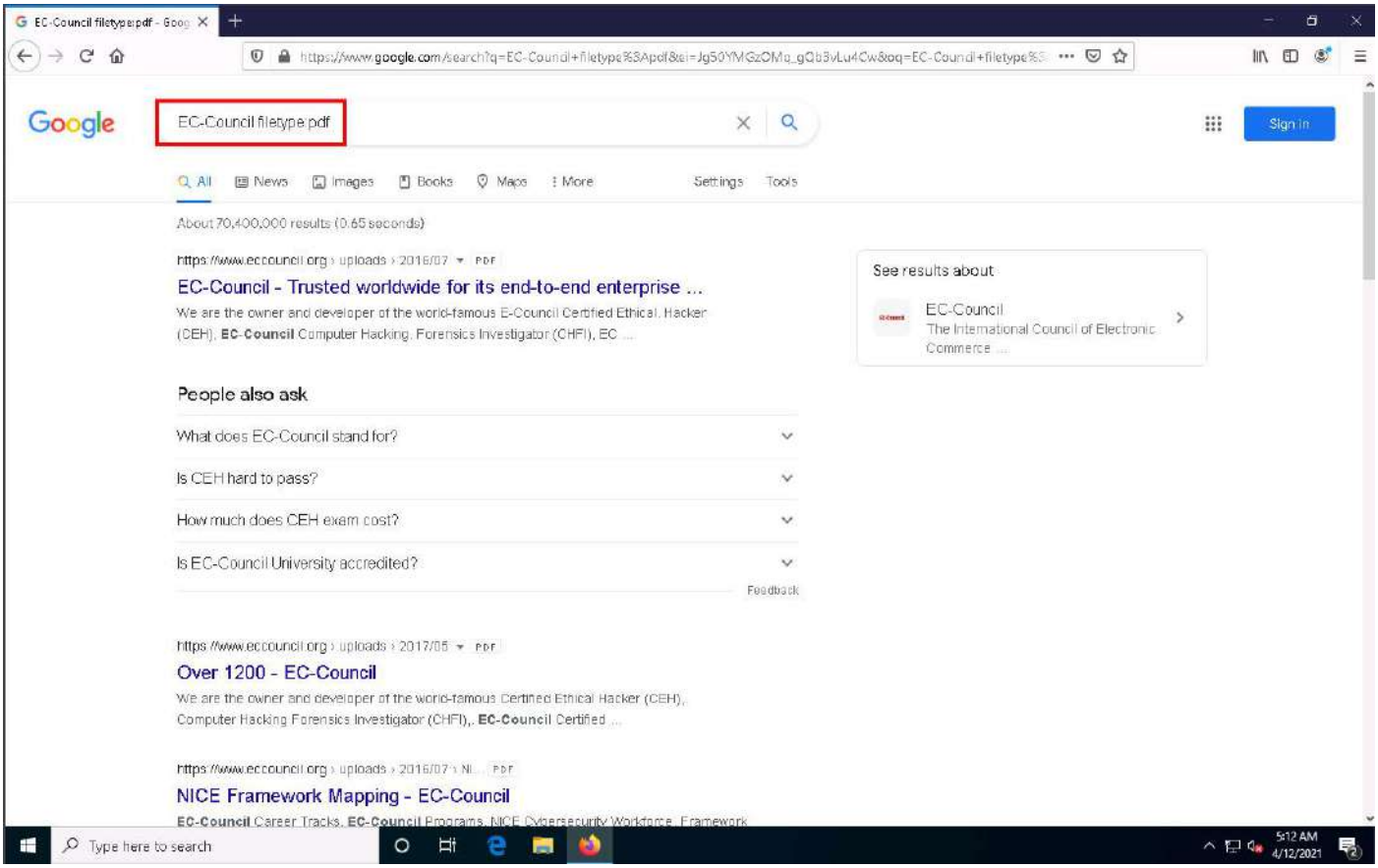
7. Now, click back icon present on the top-left corner of the browser window to navigate back to **https://www.google.com**.



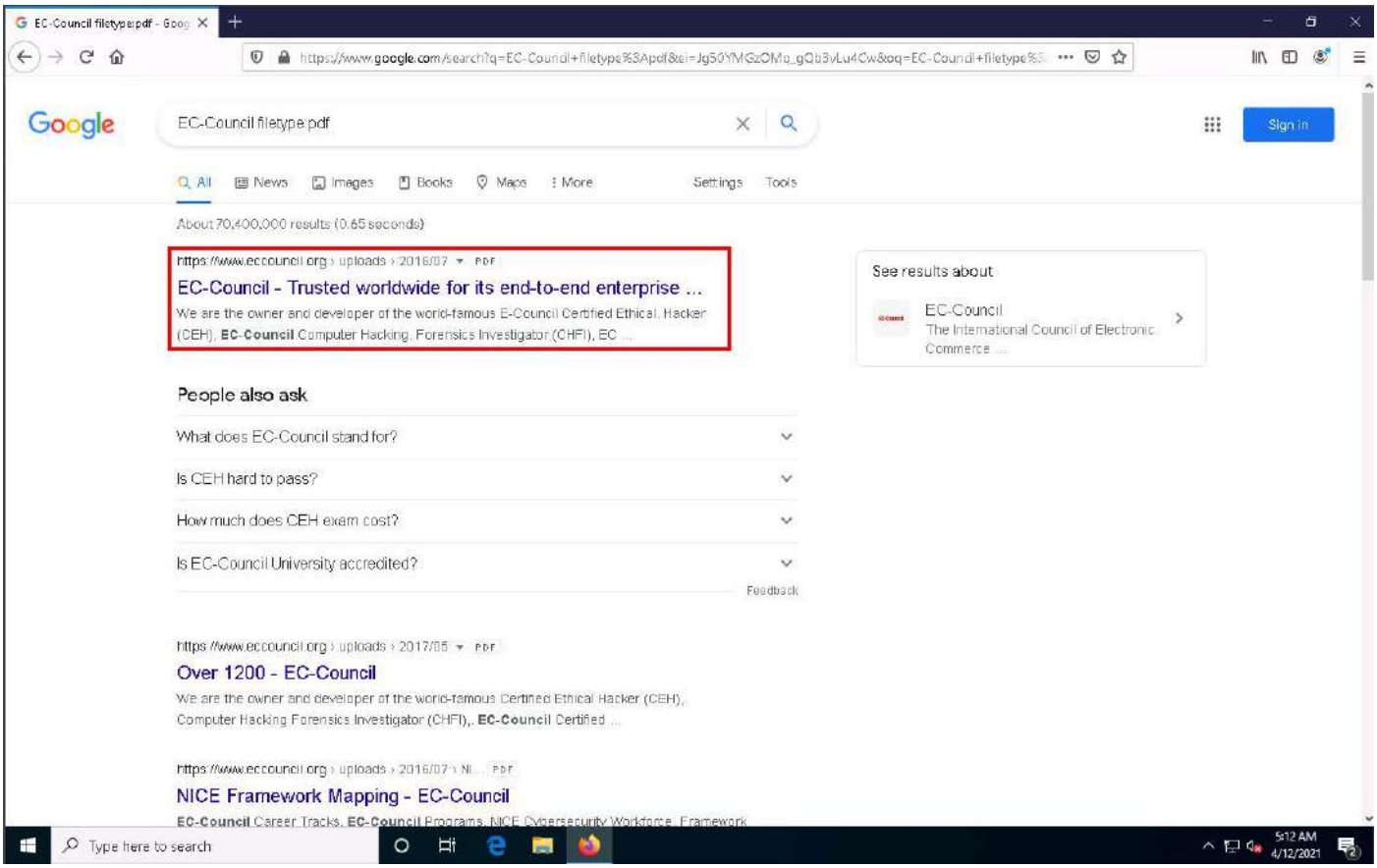
8. In the search bar, type the command **EC-Council filetype:pdf** and press **Enter** to search your results based on the file extension.

Here, the file type pdf is searched for the target organization EC-Council.

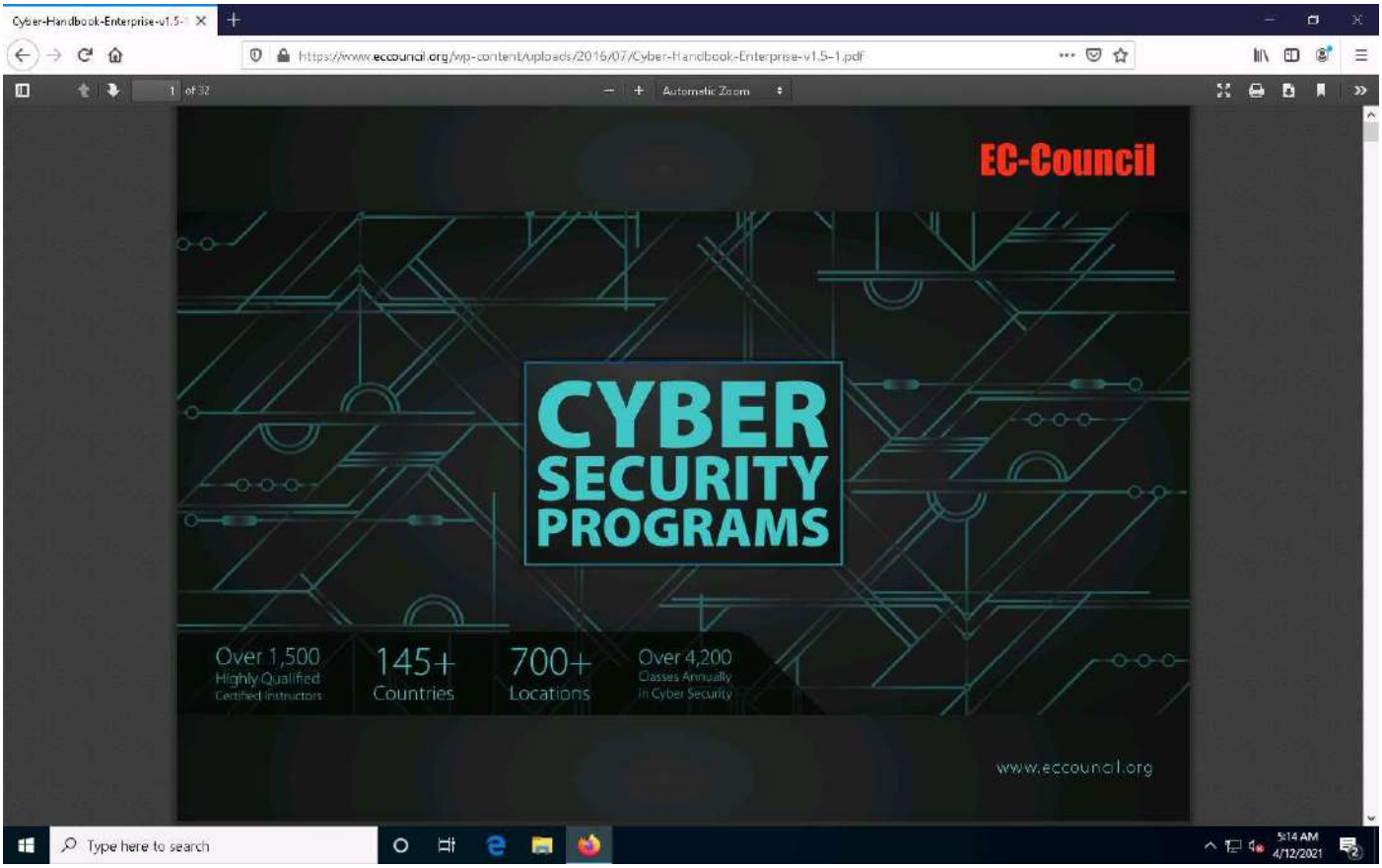
The result will be different in your lab environment.



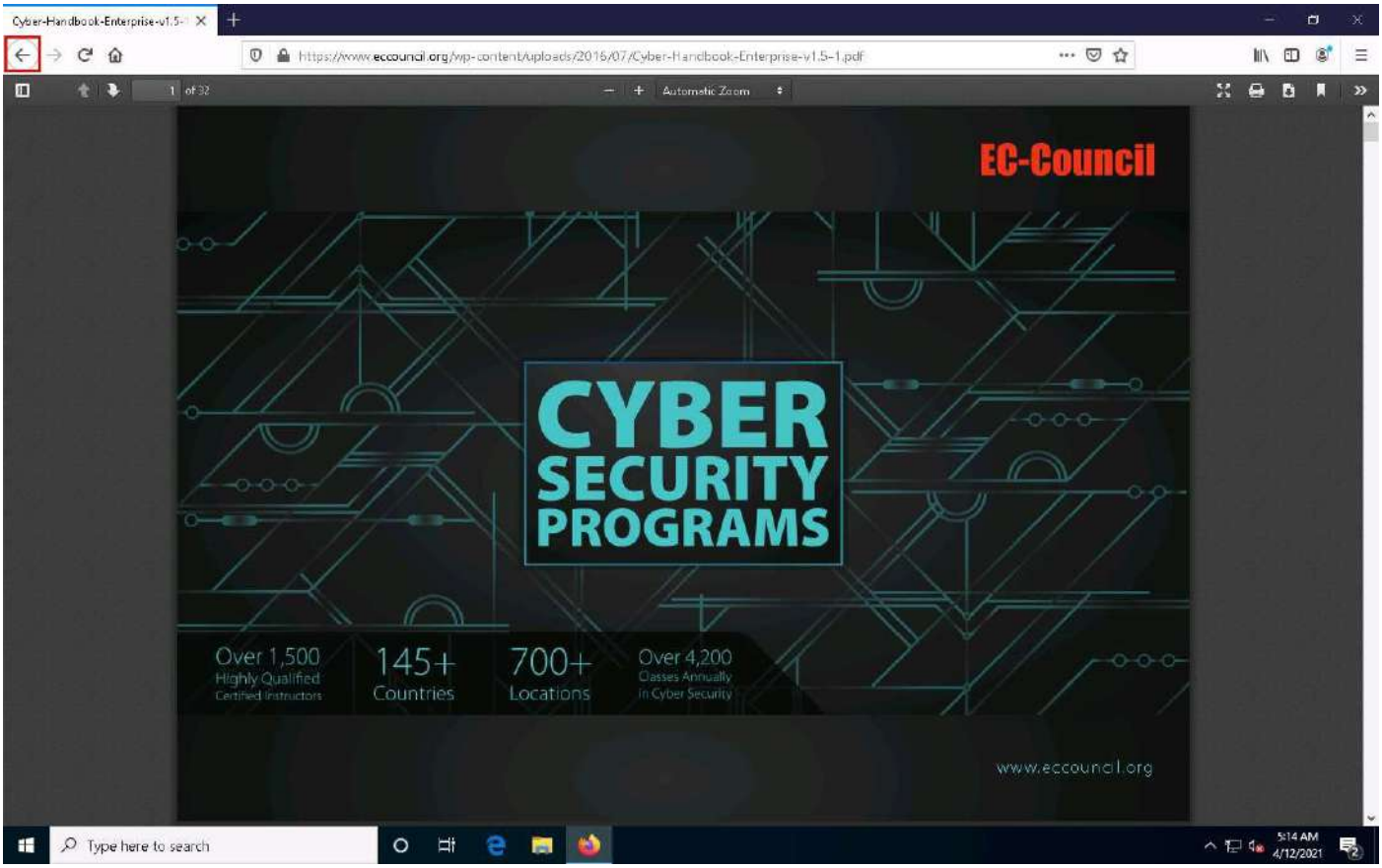
9. Now, click on any link from the results (here, first link) to view the pdf file.



10. The page appears displaying the PDF file, as shown in the screenshot.

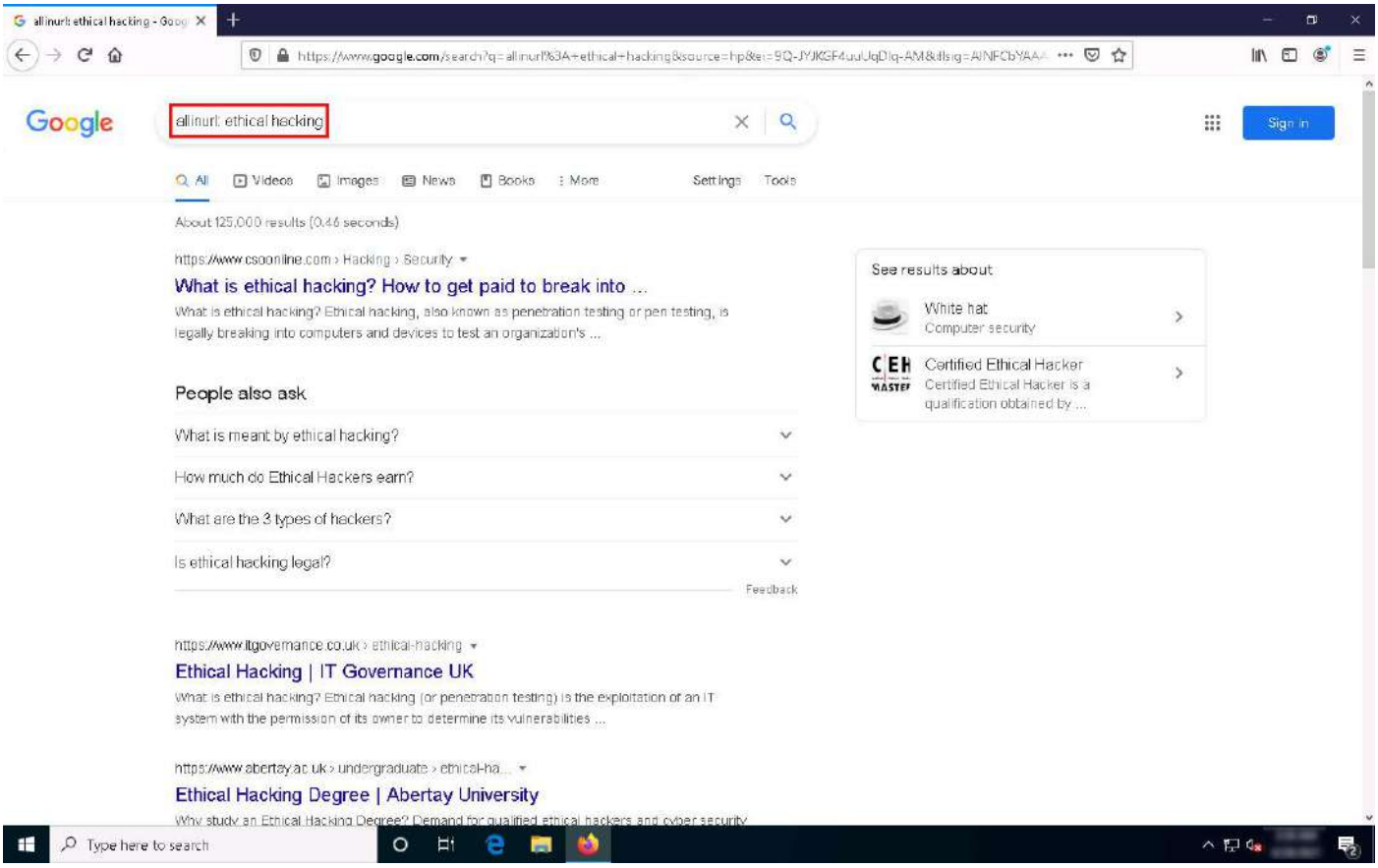


11. Now, click back icon present on the top-left corner of the browser window to navigate back to **https://www.google.com**.

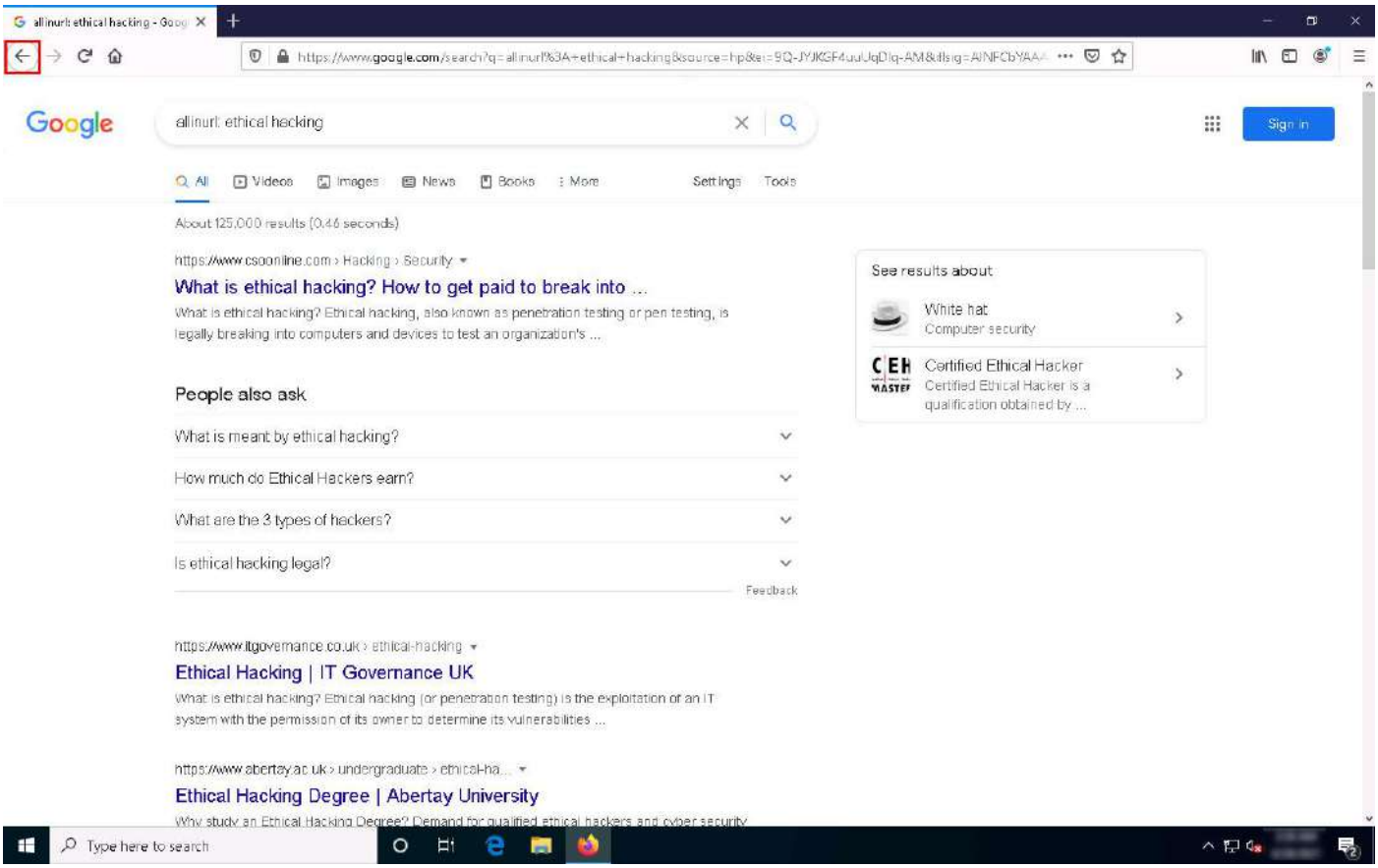


12. In the search bar, type the command **allinurl: ethical hacking** and press **Enter** to search your results contaning the word specified in the URL.

13. The page displays only pages containing the words “ethical” and “hacking” in the URL, as shown in the screenshot.

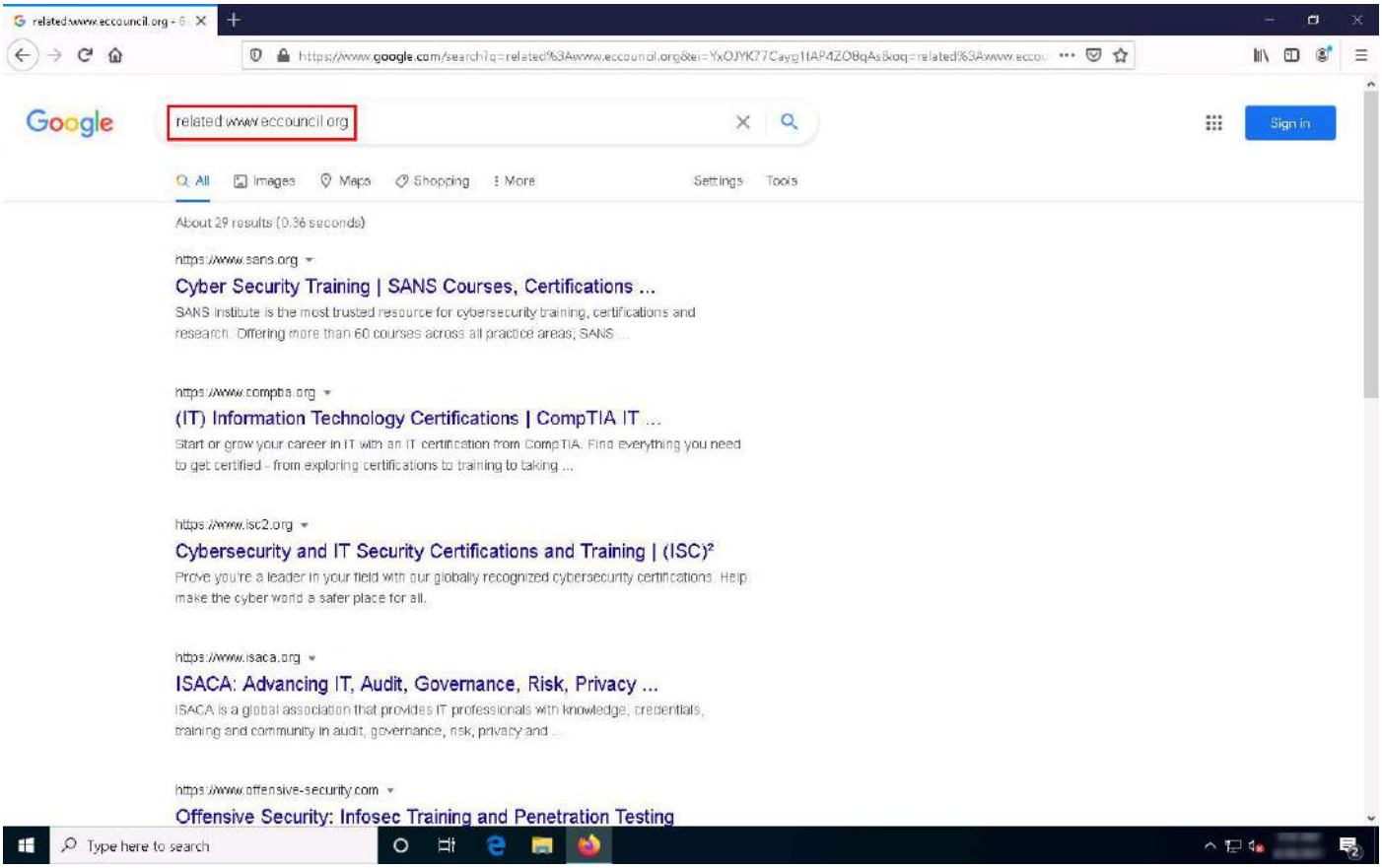


14. Now, click back icon present on the top-left corner of the browser window to navigate back to **https://www.google.com**.



15. In the search bar, type the command **related:www.eccouncil.org** and press **Enter** to search your results that are similar or related to the URL specified.

16. The page displays Google search engine results page with websites similar to eccouncil.org, as shown in the screenshot.



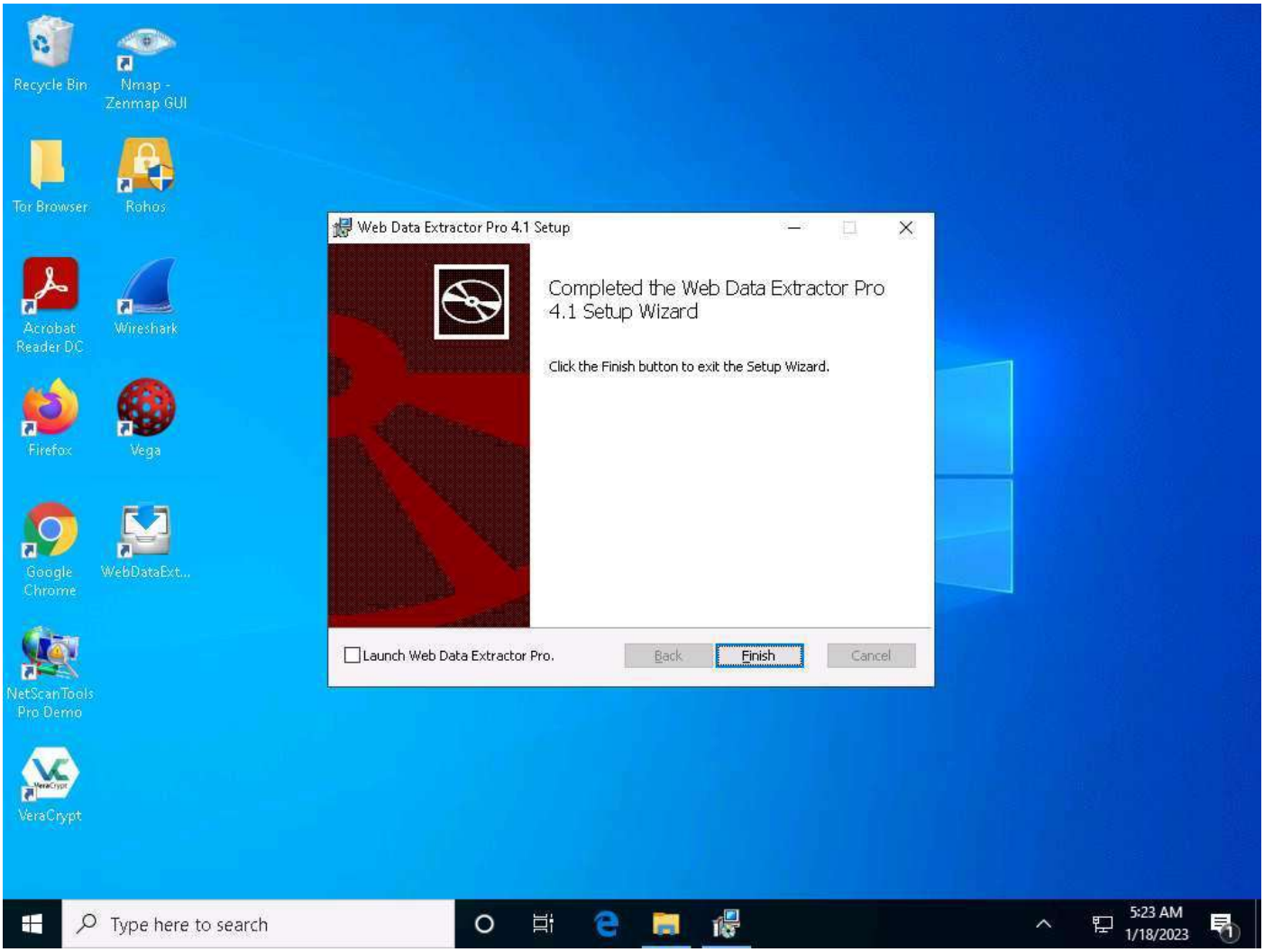
17. Apart from the aforementioned advanced Google operators, you can also use the following to perform an advanced search to gather more information about the target organization from publicly available sources.
    - **cache**: This operator allows you to view cached version of the web page. [cache:www.google.com]-Query returns the cached version of the website www.google.com
    - **inurl**: This operator restricts the results to pages containing the word specified in the URL [inurl: copy site:www.google.com]—Query returns only pages in Google site in which the URL has the word "copy"
    - **allintitle**: This operator restricts results to pages containing all the query terms specified in the title. [allintitle: detect malware]—Query returns only pages containing the words "detect" and "malware" in the title
    - **inanchor**: This operator restricts results to pages containing the query terms specified in the anchor text on links to the page. [Anti-virus inanchor:Norton]—Query returns only pages with anchor text on links to the pages containing the word "Norton" and the page containing the word "Anti-virus"
    - **allinanchor**: This operator restricts results to pages containing all query terms specified in the anchor text on links to the page. [allinanchor: best cloud service provider]—Query returns only pages in which the anchor text on links to the pages contain the words "best," "cloud," "service," and "provider"
    - **link**: This operator searches websites or pages that contain links to the specified website or page. [link:www.googleguide.com]—Finds pages that point to Google Guide's home page
    - **info**: This operator finds information for the specified web page. [info:gothotel.com]—Query provides information about the national hotel directory GotHotel.com home page
    - **location**: This operator finds information for a specific location. [location: 4 seasons restaurant]—Query give you results based around the term 4 seasons restaurant
18. This concludes the demonstration of gathering information using advanced Google hacking techniques. You can conduct a series of queries on your own by using these advanced Google operators and gather the relevant information about the target organization.
19. Close all open windows and document all the acquired information.

Task 2: Extract a Company's Data using Web Data Extractor

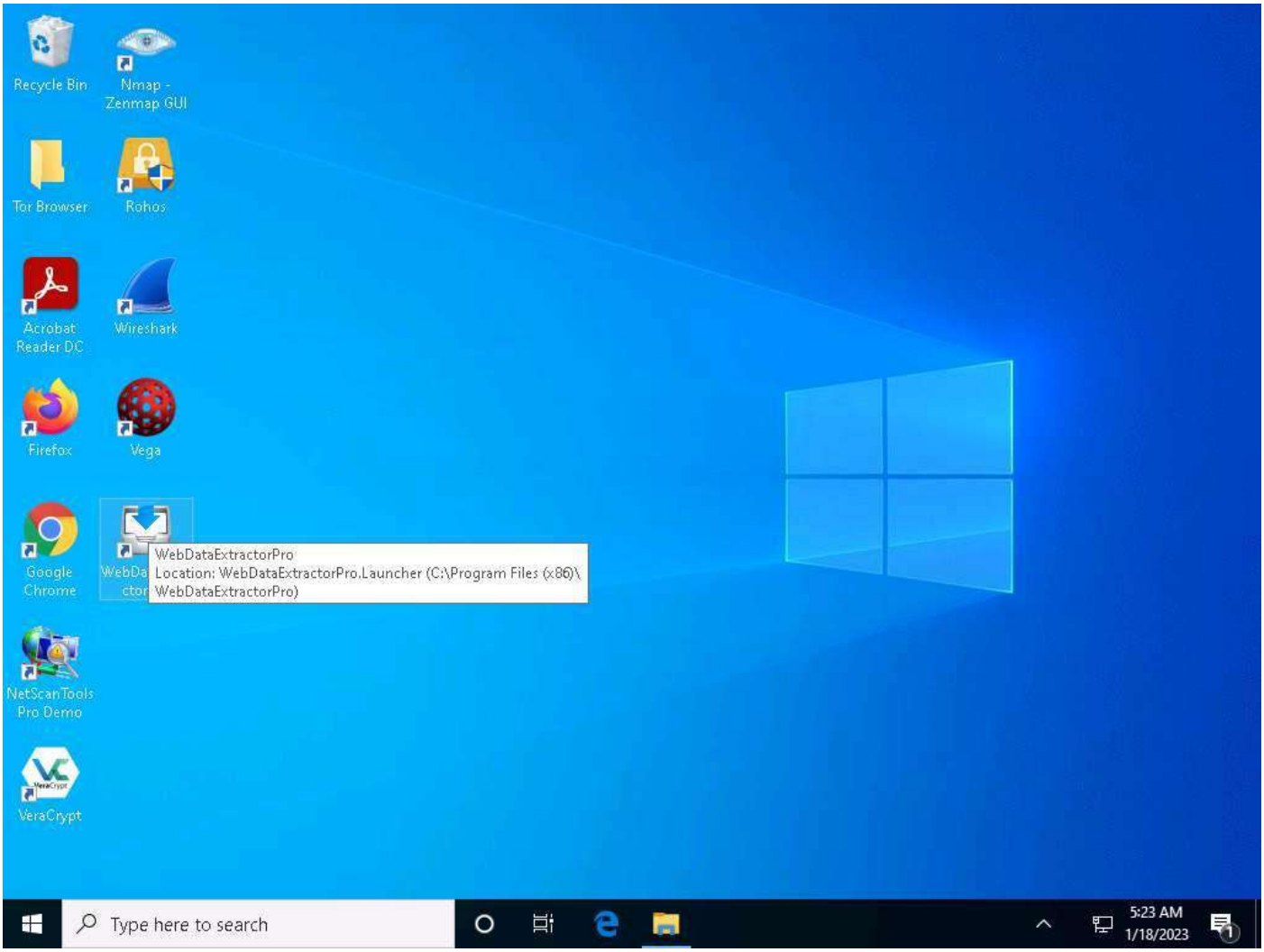
Web data extraction is the process of extracting data from web pages available on the company's website. A company's data such as contact details (email, phone, and fax), URLs, meta tags (title, description, keyword) for website promotion,directories, web research, etc. are important sources of information for an ethical hacker. Web spiders (also known as a web crawler or web robot) such as Web Data Extractor perform automated searches on the target website and extract specified information from the target website.

Here, we will gather the target company's data using the Web Data Extractor tool.

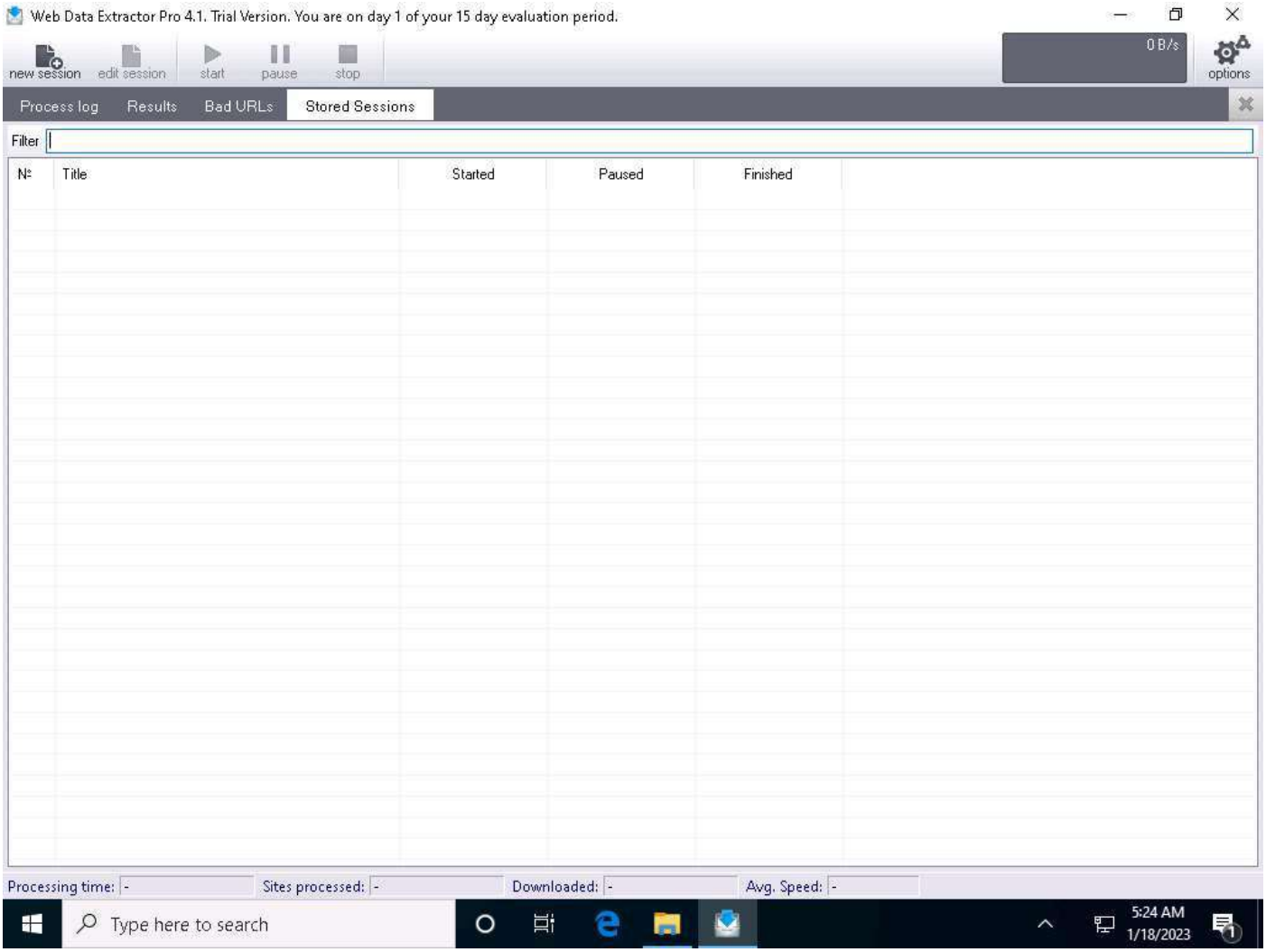
1. In the **Windows 10** machine, navigate to **D:\EHE-Tools\EHE Module 02 Ethical Hacking Fundamentals\Web Spiders\Web Data Extractor** and double-click **wdepro.exe**.
2. If the **User Account Control** pop-up appears, click **Yes**.
3. Follow the wizard steps to install Web Data Extractor Pro and click **Finish**.



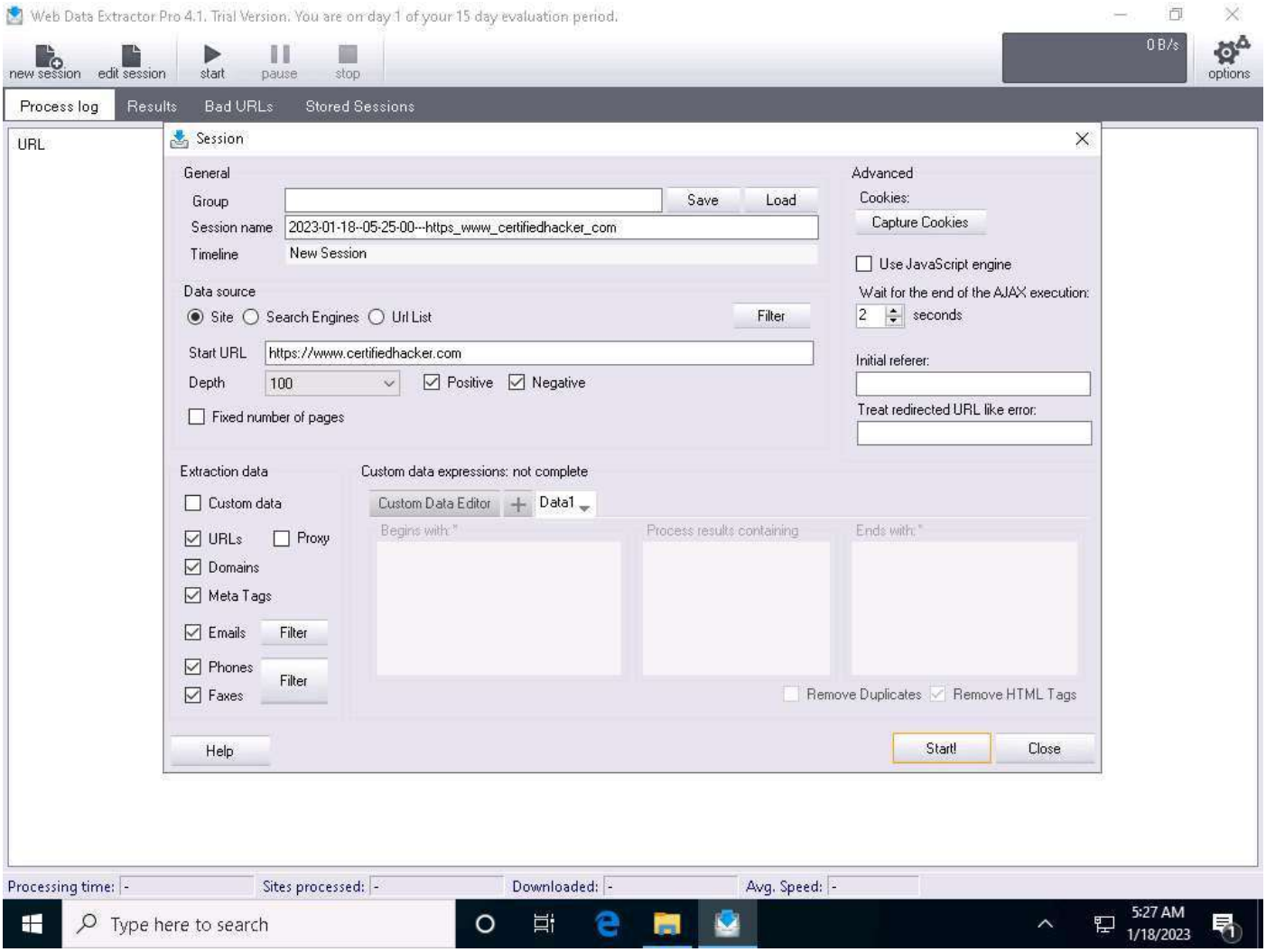
4. After installation, launch **Web Data Extractor Pro** from **Desktop**.



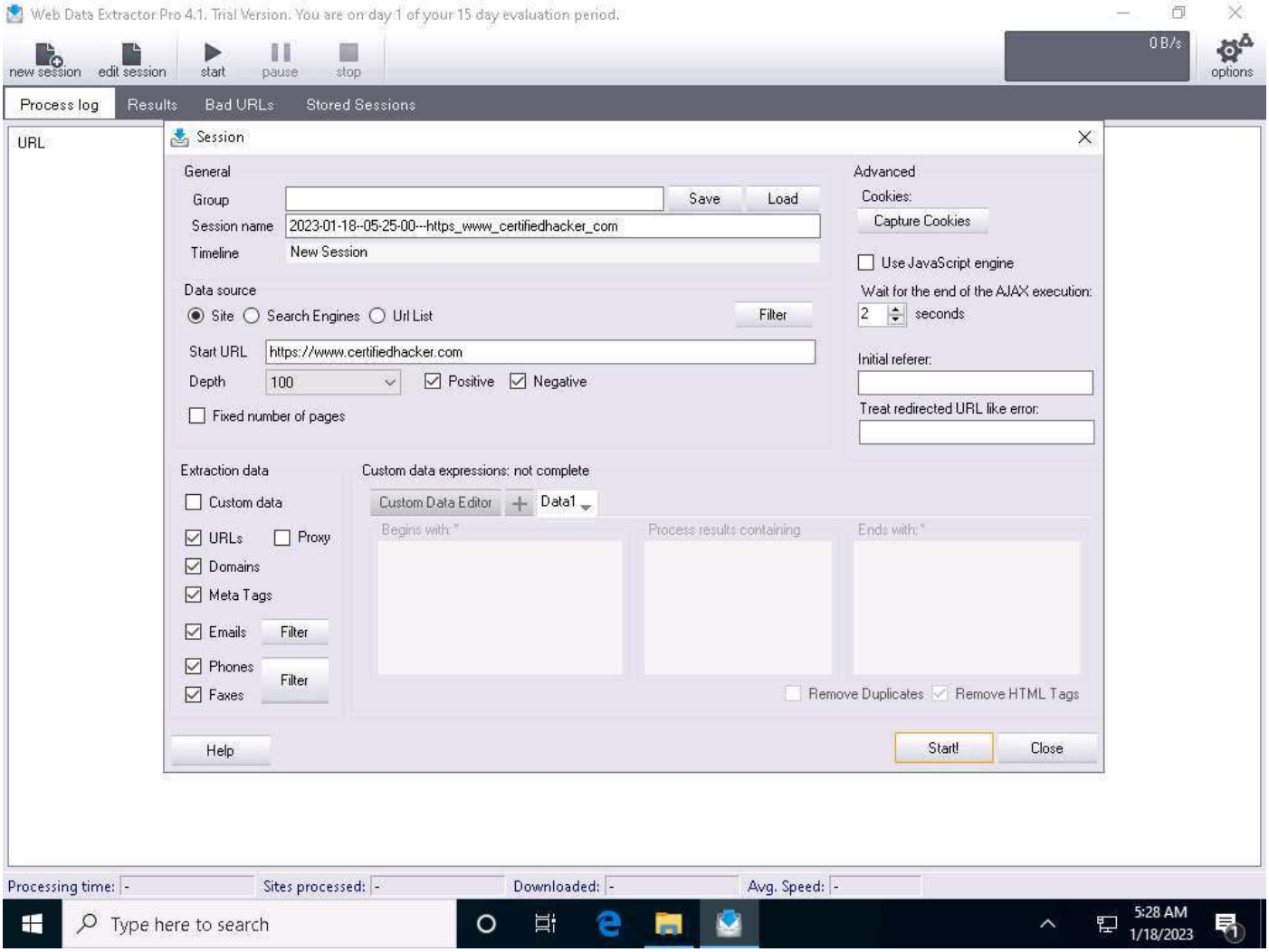
5. The **Web Data Extractor Pro** main window appears. Click **new session** to start a new session.



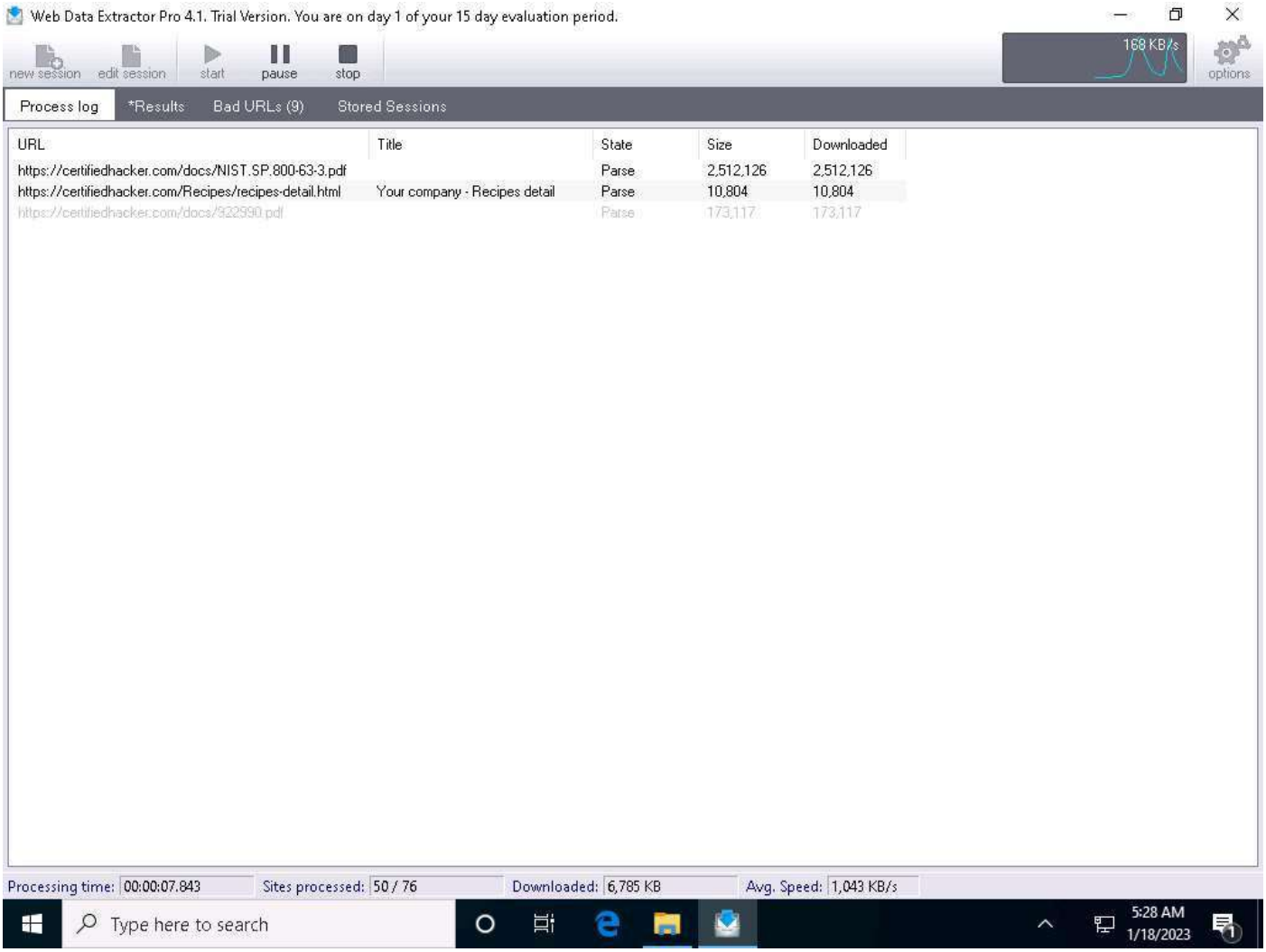
6. The **Session** window appears; type a URL (here, **https://www.certifiedhacker.com**) in the **Start URL** field. Check all the options, as shown in the screenshot.



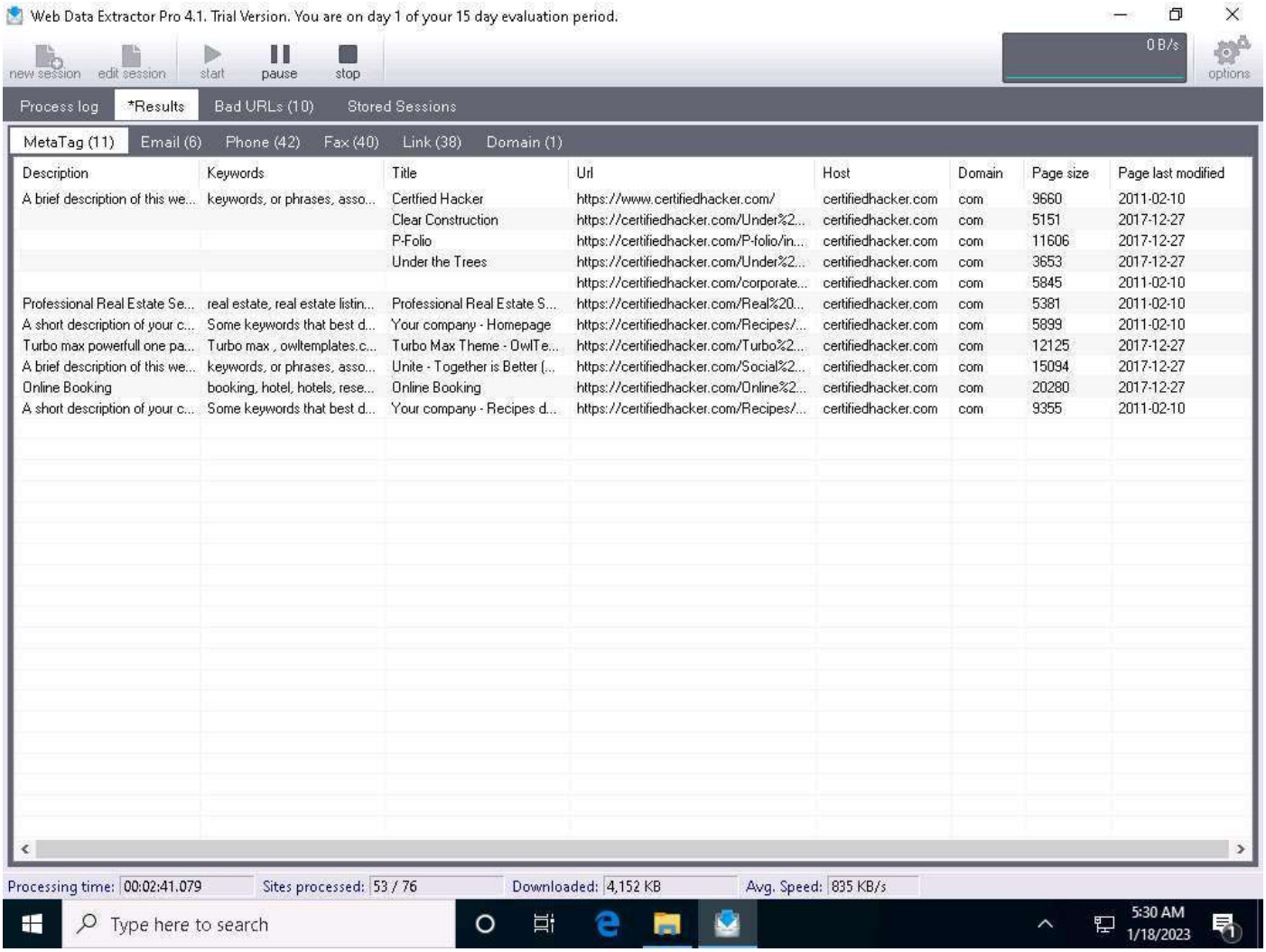
7. Click **Start** to initiate the data extraction.



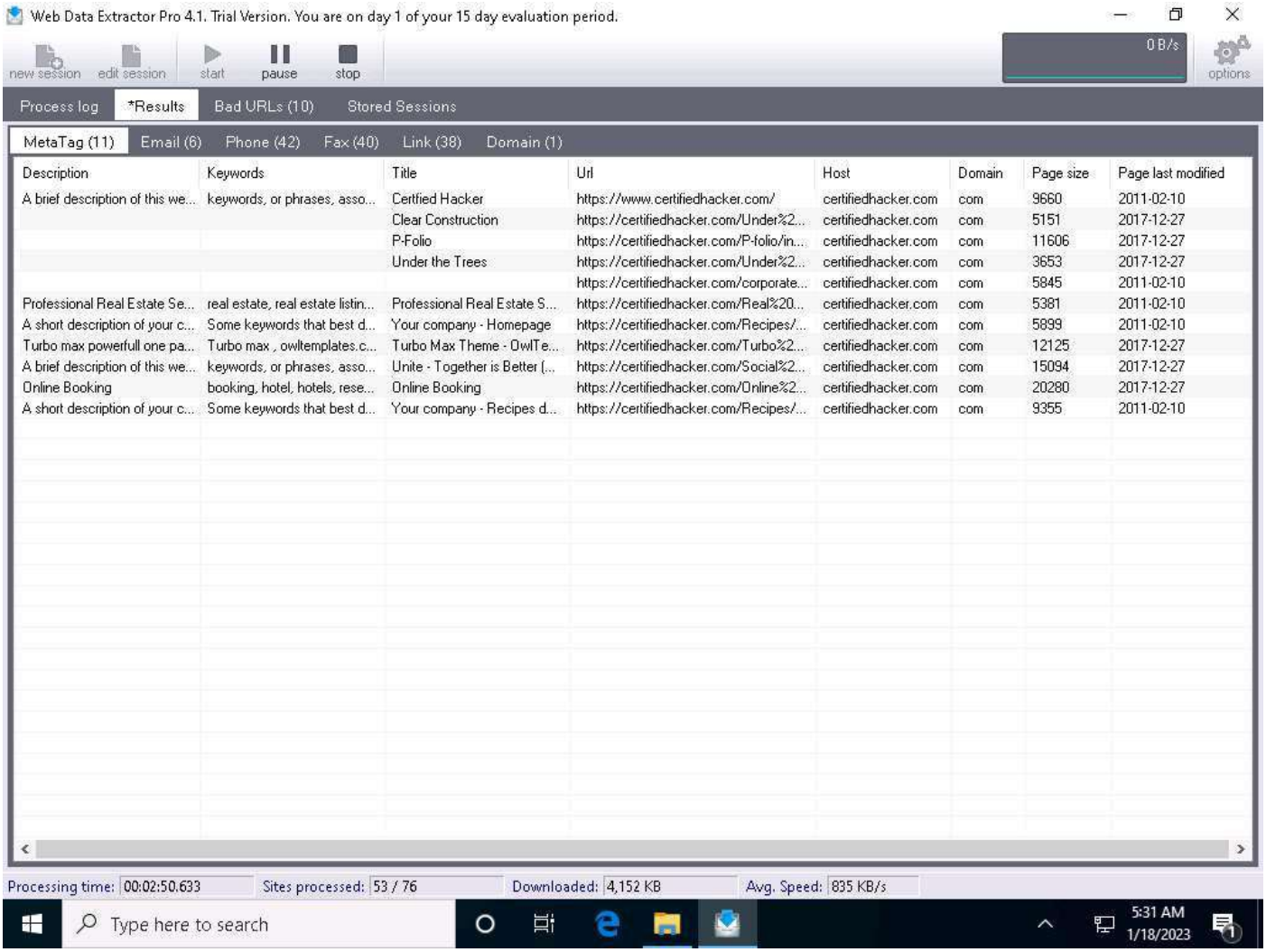
8. **Web Data Extractor Pro** will start collecting information (**Session**, **Meta tags**, **Emails**, **Phones**, **Faxes**, **Links**, and **Domains**).



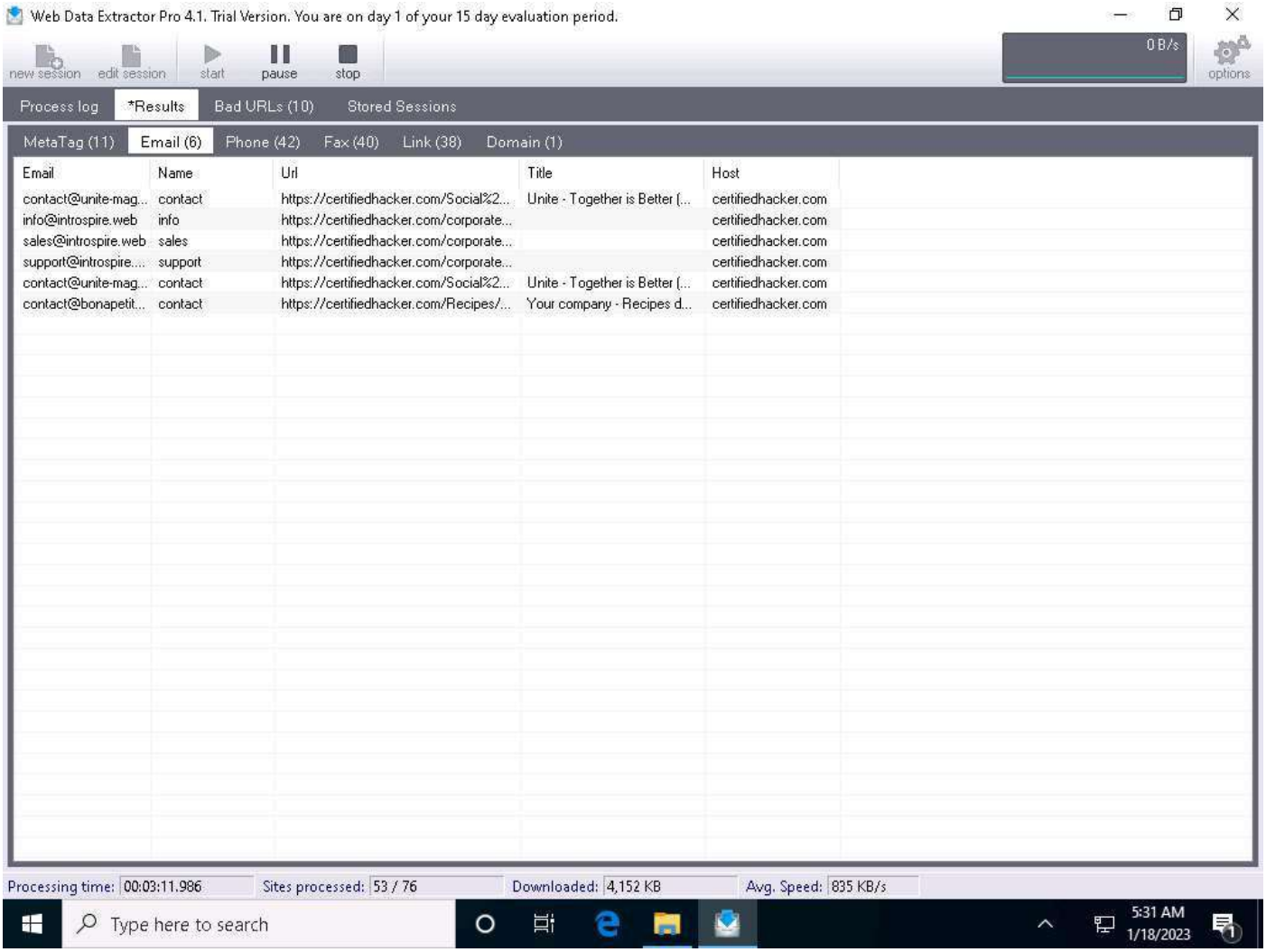
9. Click on **Results** tab to view the collected information about the website.



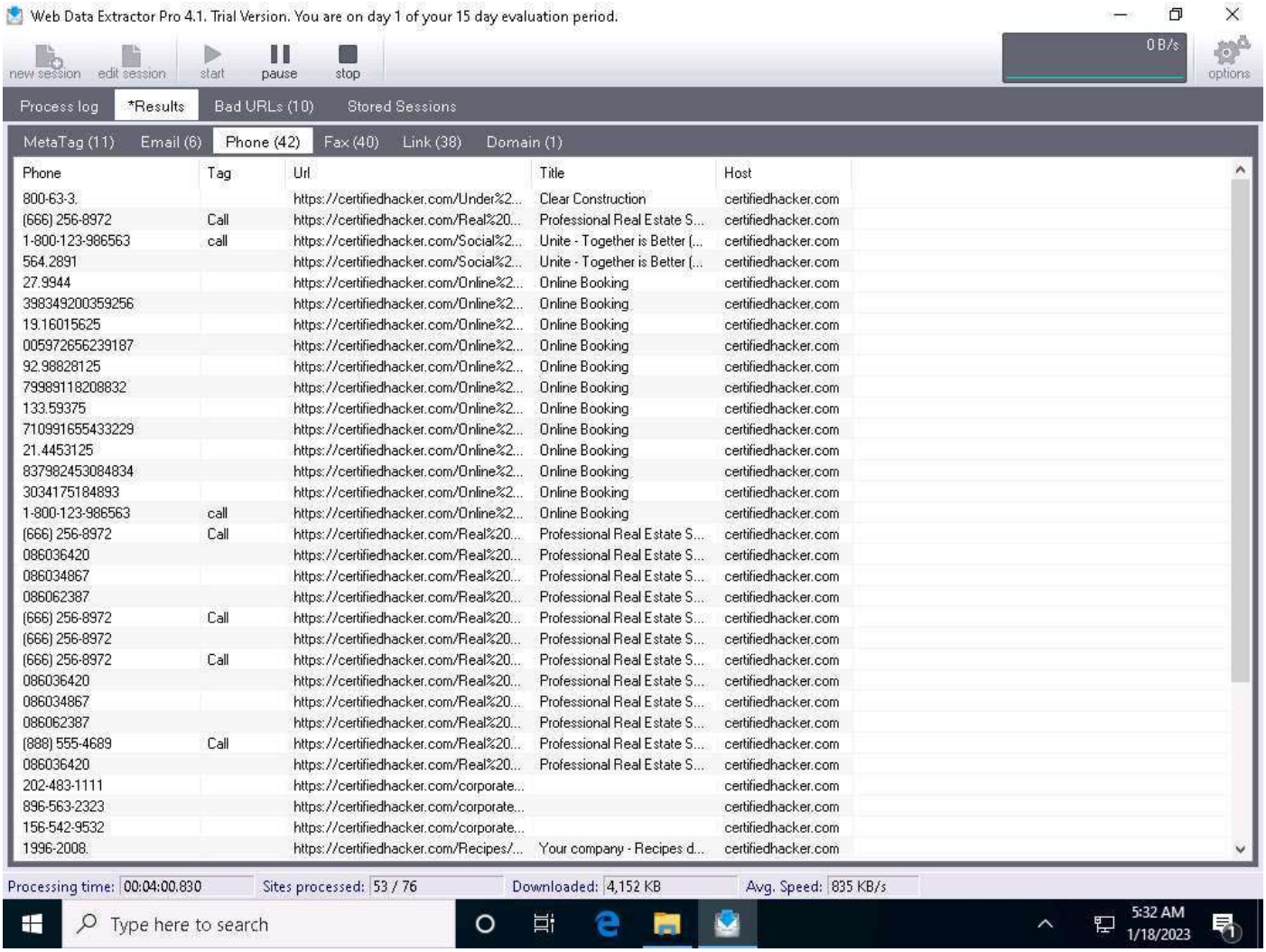
10. View the extracted information by clicking the tabs.
11. Select the **Meta tag** tab to view the URL, Title, Keywords, Description, Host, Domain, page size, etc.



12. Select the **Email** tab to view information related to emails such as Email address, Name, URL, Title, etc.



13. Select the **Phone** tab to view the Phone, Source, Tag, URL, etc.

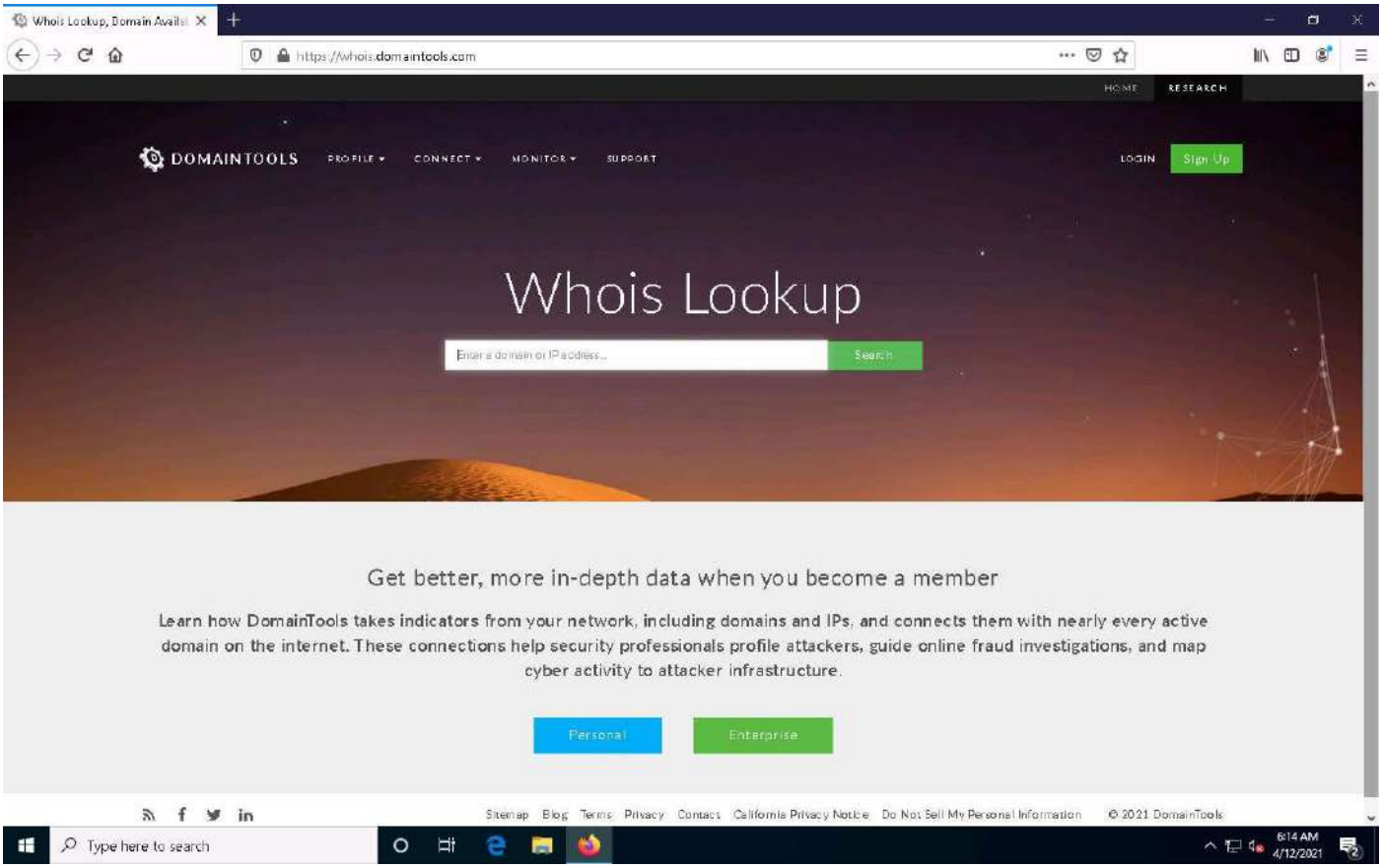


14. Check for more information under the **Fax**, **Link** and **Domain** tabs.
15. This concludes the demonstration of extracting a company's data using the Web Data Extractor Pro tool.
16. Close all open windows and document all the acquired information.

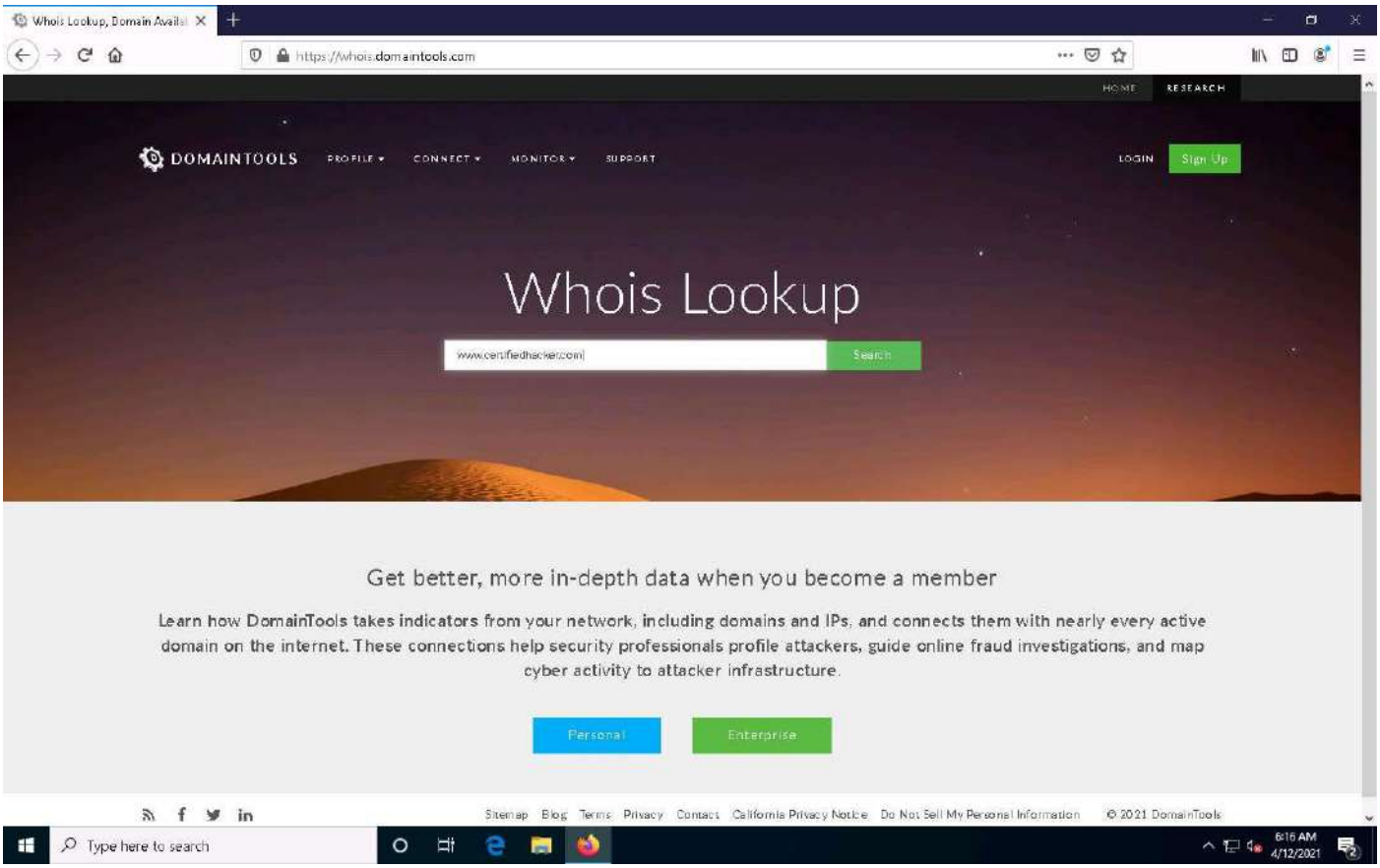
Task 3: Perform Whois Lookup using DomainTools

Whois is a query and response protocol used for querying databases that store the registered users or assignees of an Internet resource such as a domain name, an IP address block,or an autonomous system. This protocol listens to requests on port 43 (TCP). Regional Internet Registries (RIRs) maintain Whois databases, and contains the personal information of domain owners. For each resource, the Whois database provides text records with information about the resource itself and relevant information of assignees, registrants, and administrative information (creation and expiration dates). Here, we will gather target information by performing Whois lookup using DomainTools.

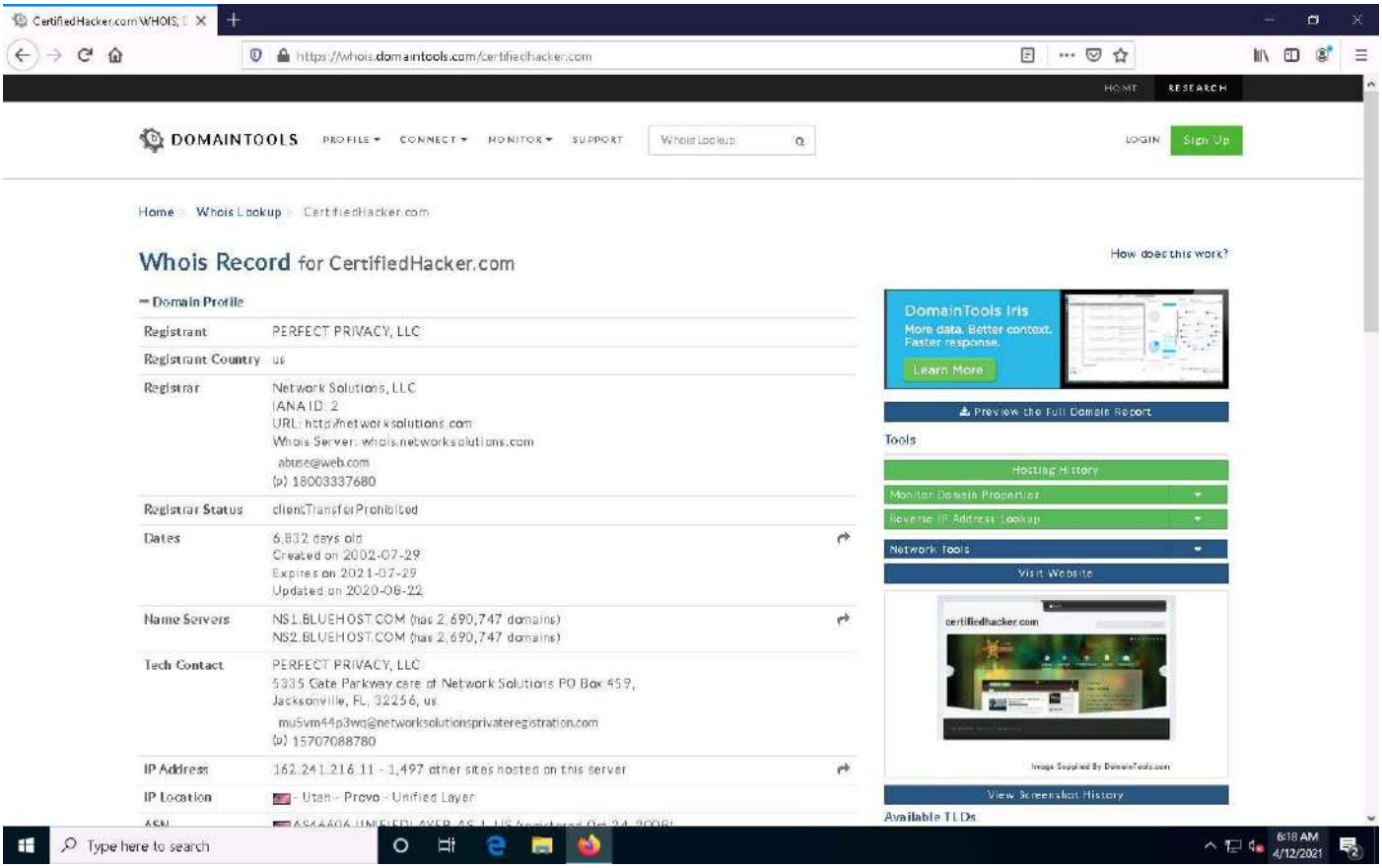
1. In the **Windows 10** machine, open any web browser (here, **Mozilla Firefox**). In the address bar of the browser place your mouse cursor, click http://whois.domaintools.com and press **Enter**. The Whois Lookup website appears, as shown in the screenshot.

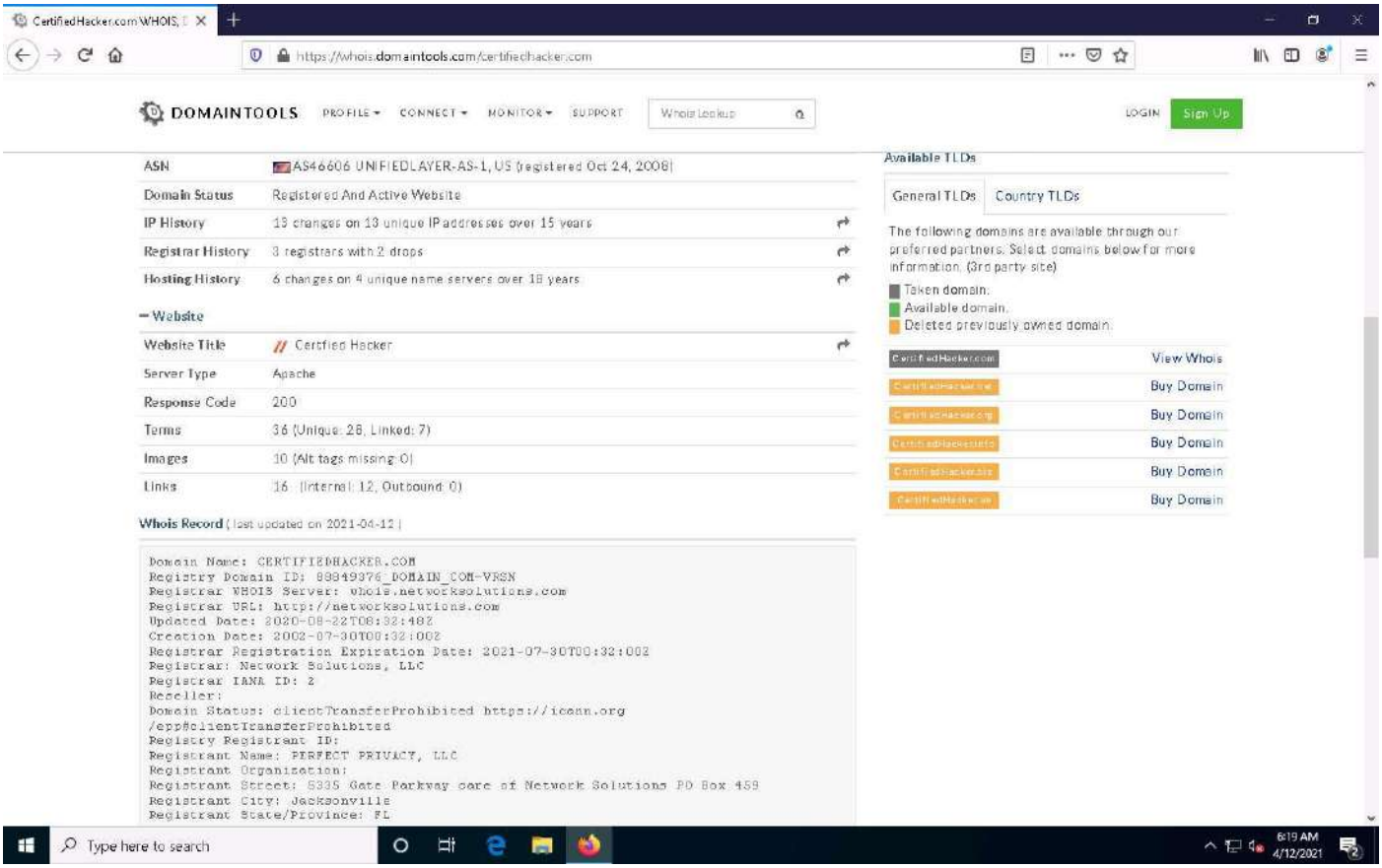


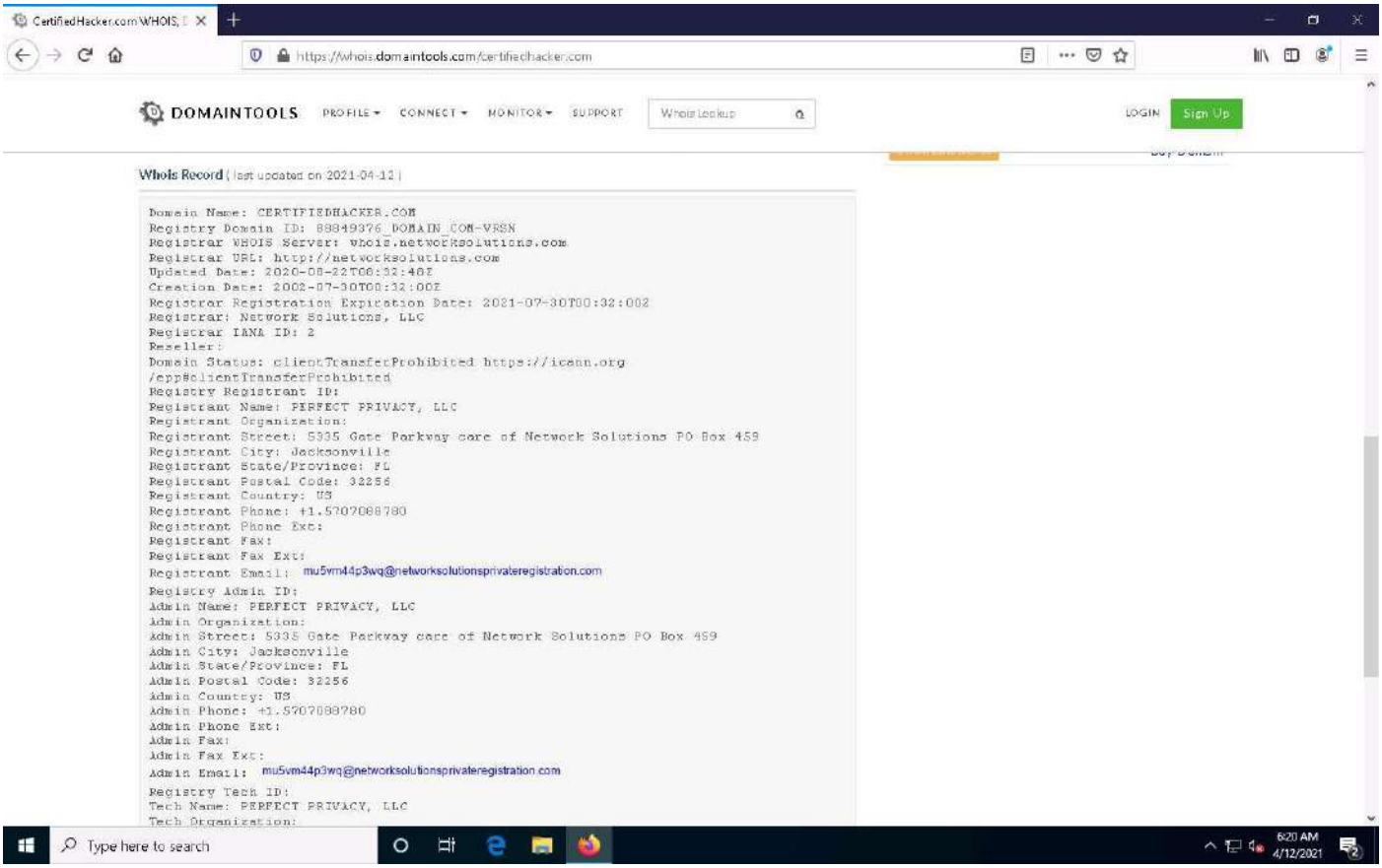
2. Now, in the **Enter a domain or IP address...** search bar, type **www.certifiedhacker.com** and click **Search**.



3. This search result reveals the details associated with the URL entered, **www.certifiedhacker.com**, which includes organizational details such as registration details, name servers, IP address, location, etc., as shown in the screenshots.


CertifiedHacker.com WHOIS,
https://whois.domaintools.com/certifiedhacker.com
HOME
RESEARCH
DOMAINTOOLS
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
LOGIN
Sign Up
Home
Whois Lookup
CertifiedHacker.com
Whois Record for CertifiedHacker.com
How does this work?
Domain Profile
Registrant
PERFECT PRIVACY, LLC
Registrant Country
us
Registrar
Network Solutions, LLC
IANA ID: 2
URL: http://networksolutions.com
Whois Server: whois.networksolutions.com
abuse@web.com
(p) 18003337680
Registrar Status
clientTransferProhibited
Dates
6,832 days old
Created on 2002-07-29
Expires on 2021-07-29
Updated on 2020-08-22
Name Servers
NS1.BLUEHOST.COM (has 2,690,747 domains)
NS2.BLUEHOST.COM (has 2,690,747 domains)
Tech Contact
PERFECT PRIVACY, LLC
5335 Gate Parkway care of Network Solutions PO Box 459,
Jacksonville, FL, 32256, us
mu5vm44p3wq@networksolutionsprivateregistration.com
(p) 15707088780
IP Address
162.241.216.11 - 1,497 other sites hosted on this server
IP Location
- Utah - Provo - Unified Layer
DomainTools Iris
More data. Better context.
Faster response.
Learn More
Preview the Full Domain Report
Tools
Hosting History
Monitor Domain Properties
Reverse IP Address Lookup
Network Tools
Visit Website
certifiedhacker.com
View Screenshot History
Available TLDs
Type here to search
6:18 AM
4/12/2021


CertifiedHacker.com WHOIS,
https://whois.domaintools.com/certifiedhacker.com
DOMAINTOOLS
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
LOGIN
Sign Up
ASN
AS46606 UNIFIEDLAYER-AS-1, US (registered Oct 24, 2008)
Domain Status
Registered And Active Website
IP History
13 changes on 13 unique IP addresses over 15 years
Registrar History
3 registrars with 2 drops
Hosting History
6 changes on 4 unique name servers over 18 years
Website
Website Title
// Certified Hacker
Server Type
Apache
Response Code
200
Terms
36 (Unique: 28, Linked: 7)
Images
10 (Alt tags missing: 0)
Links
16 (Internal: 12, Outbound: 0)
Whois Record (last updated on 2021-04-12)
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 89849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2020-08-22T08:32:48Z
Creation Date: 2002-07-30T00:32:00Z
Registrar Registration Expiration Date: 2021-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited https://icann.org
/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Registrant City: Jacksonville
Registrant State/Province: FL
Available TLDs
General TLDs
Country TLDs
The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)
Taken domain
Available domain
Deleted previously owned domain
CertifiedHacker.com
View Whois
Buy Domain
Buy Domain
Buy Domain
Buy Domain
Buy Domain
Type here to search
6:19 AM
4/12/2021



4. This concludes the demonstration of gathering information about a target organization by performing the Whois lookup using DomainTools.
5. Close all open windows and document all the acquired information.

Lab 2-2: Perform Network Scanning to Identify Live Hosts, Open Ports and Services and Target OS in the Network

Lab Scenario

Network scanning refers to a set of procedures used for identifying hosts, ports, and services in a network. Network scanning is also used for discovering active machines in a network and identifying the OS running on the target machine. It is one of the most important phases of intelligence gathering for an attacker, which enables him/her to create a profile of the target organization. In the process of scanning, the attacker tries to gather information, including the specific IP addresses that can be accessed over the network, the target's OS and system architecture, and the ports along with their respective services running on each computer.

Lab Objectives

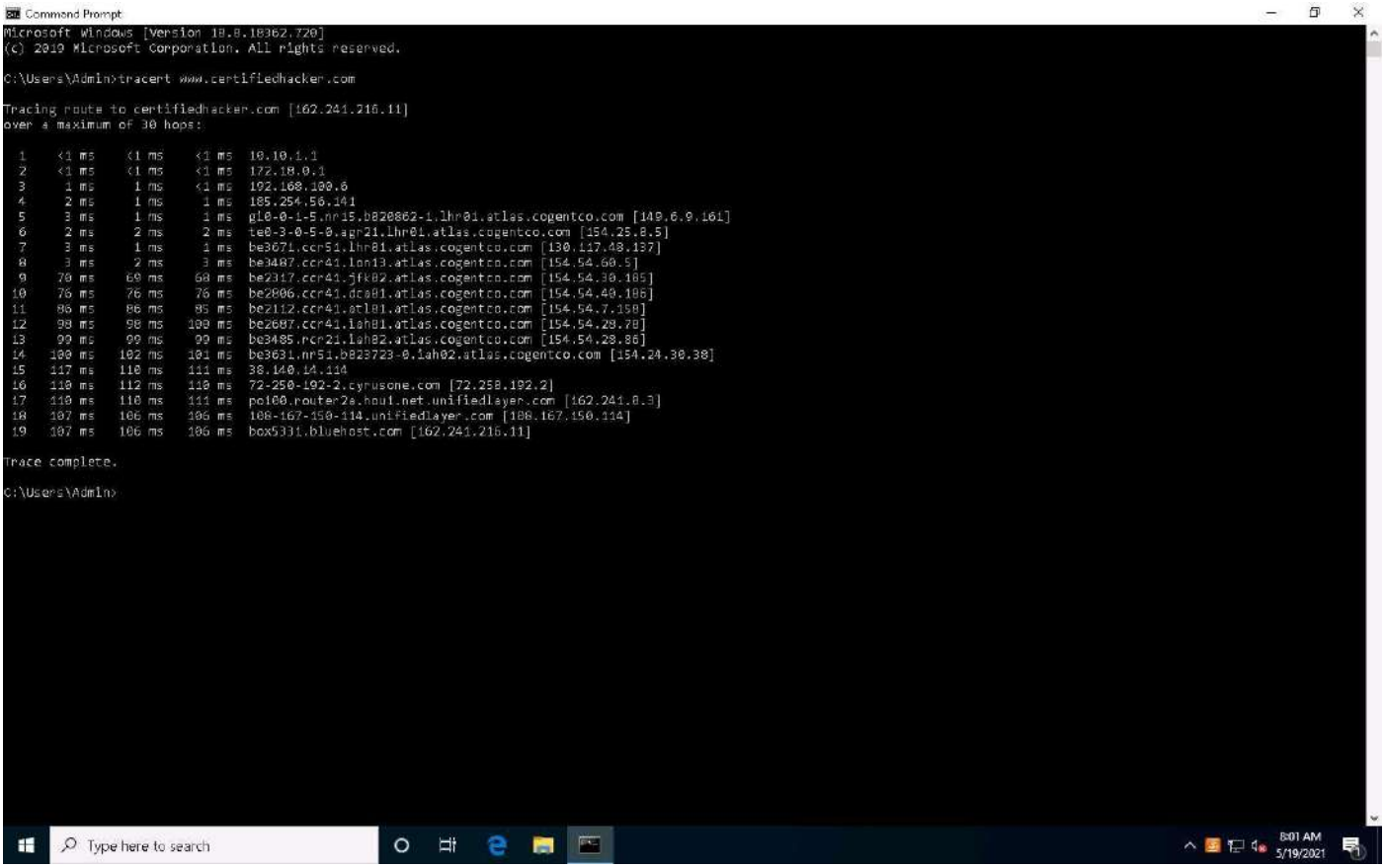
- Perform Network Tracerouting in Windows and Linux Machines
- Perform Host Discovery using Nmap
- Perform Port and Service Discovery using MegaPing
- Perform OS Discovery using Unicornscan

Task 1: Perform Network Tracerouting in Windows and Linux Machines

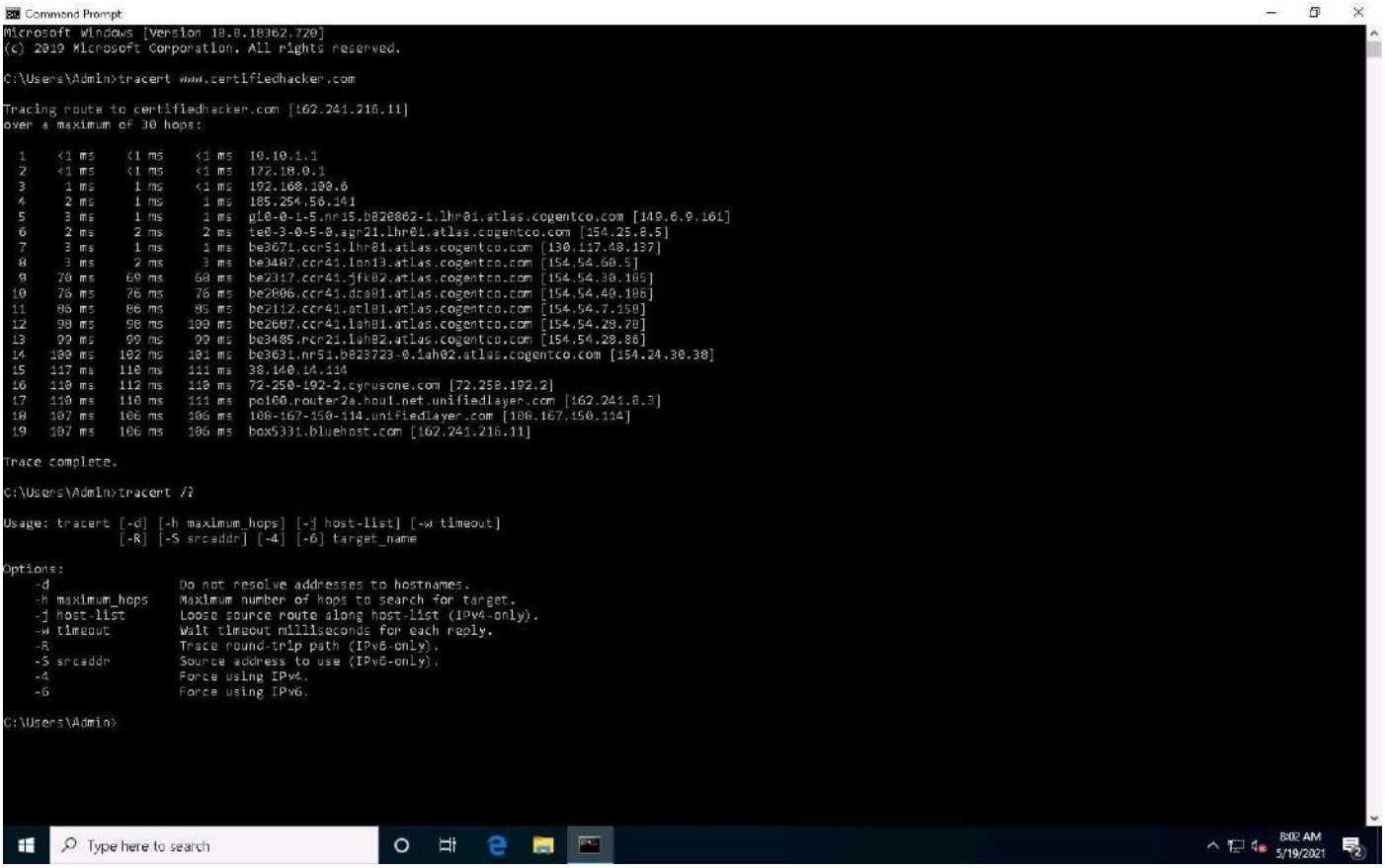
The route is the path that the network packet traverses between the source and destination. Network tracerouting is a process of identifying the path and hosts lying between the source and destination. Network tracerouting provides critical information such as the IP address of the hosts lying between the source and destination, which enables you to map the network topology of the organization. Traceroute can be used to extract information about network topology, trusted routers, firewall locations, etc.

Here, we will perform network tracerouting using both Windows and Linux machines.

1. In the **Windows 10** machine, open the **Command Prompt** window. Type **tracert www.certifiedhacker.com** and press **Enter** to view the hops that the packets made before reaching the destination.

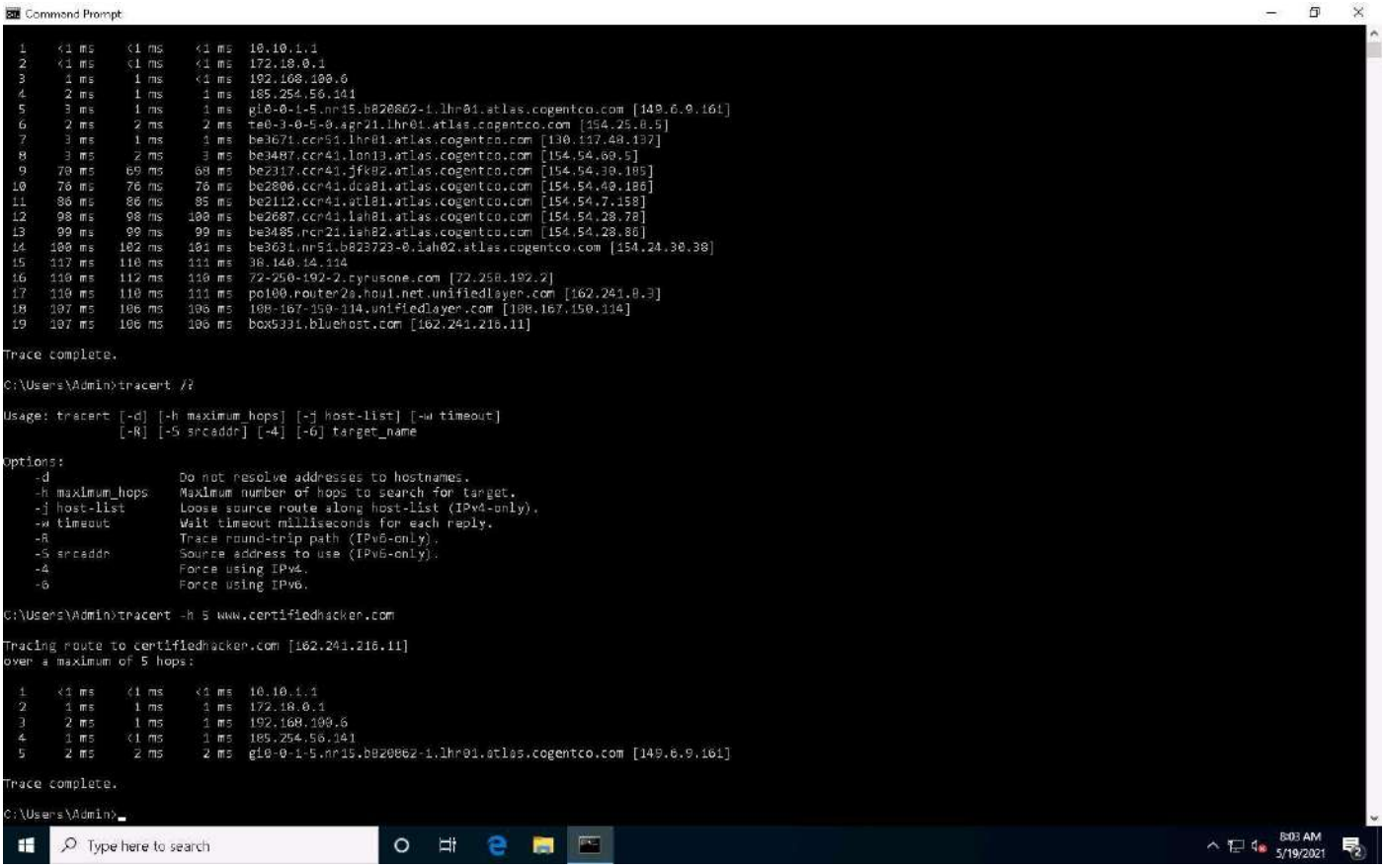


2. Type **tracert /?** and press **Enter** to show the different options for the command, as shown in the screenshot.

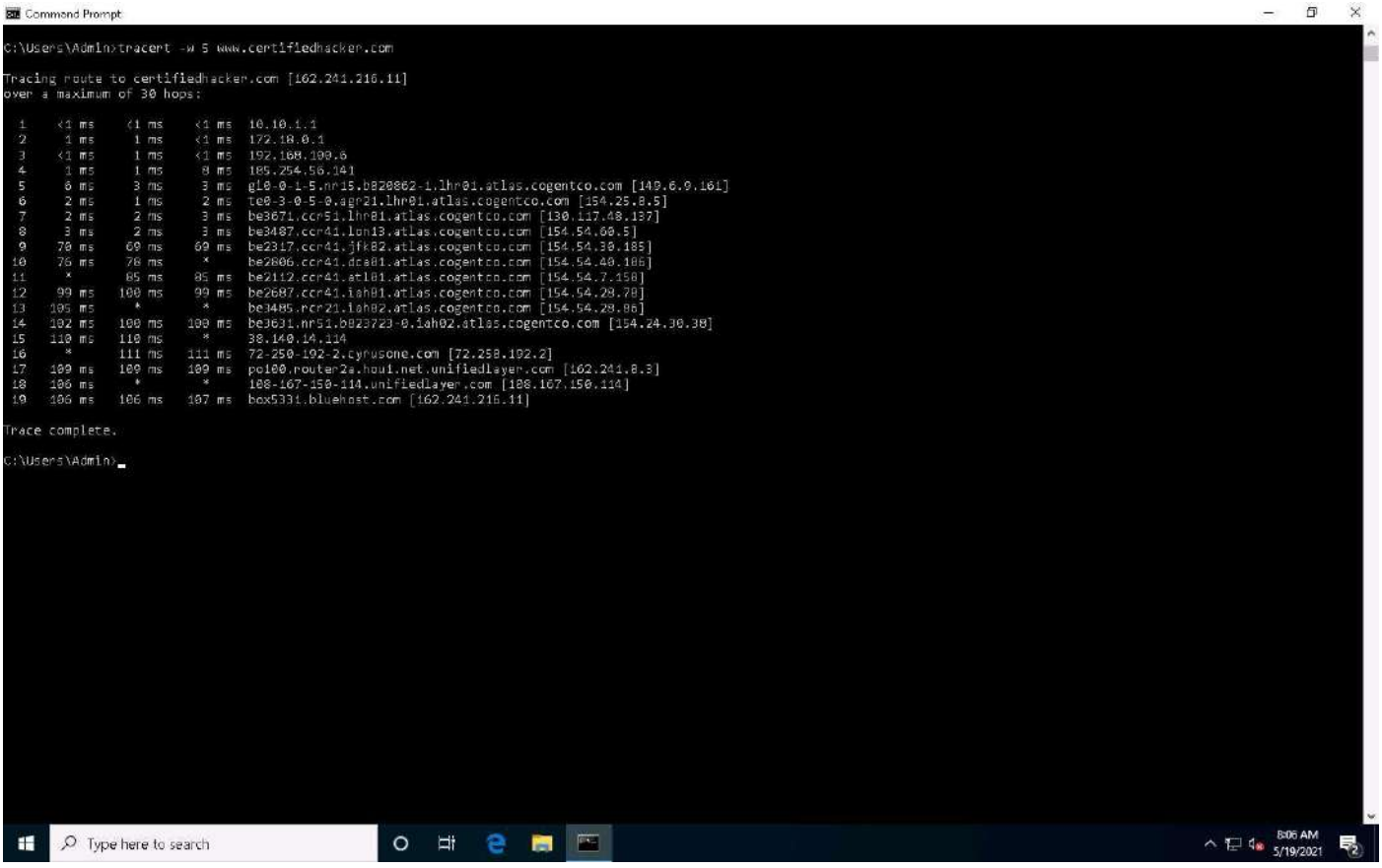


3. Type **tracert -h 5 www.certifiedhacker.com** and press **Enter** to perform the trace, but with only 5 maximum hops allowed.

4. The results are displayed, as shown in the screenshot.



5. Type **tracert -w 5 www.certifiedhacker.com** and press **Enter** to perform the trace, but with only 5 milliseconds wait time for each reply.



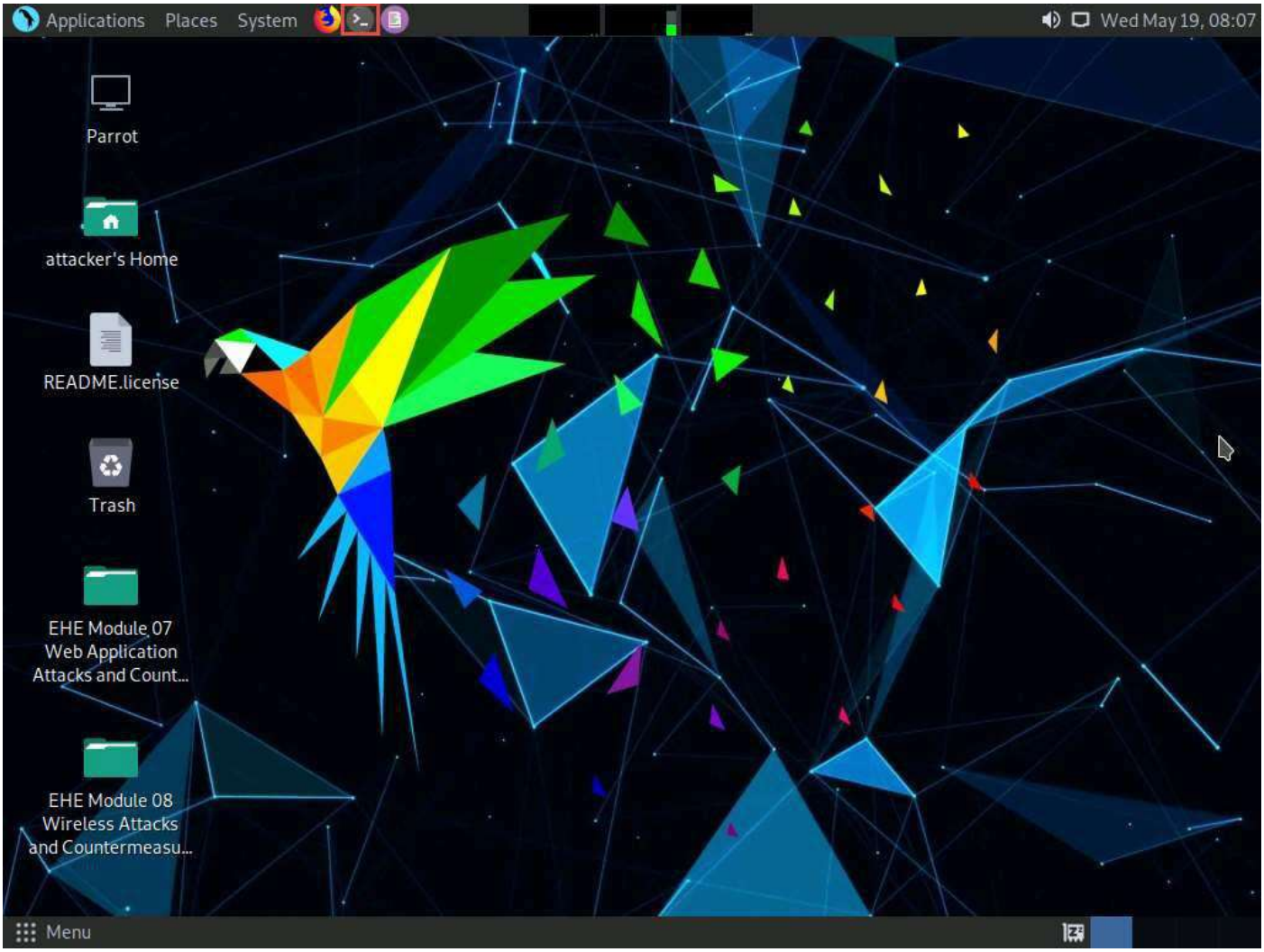
6. After viewing the result, close the command prompt window.
7. Now, click Parrot Security to switch to the **Parrot Security** machine.

8. 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.

If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

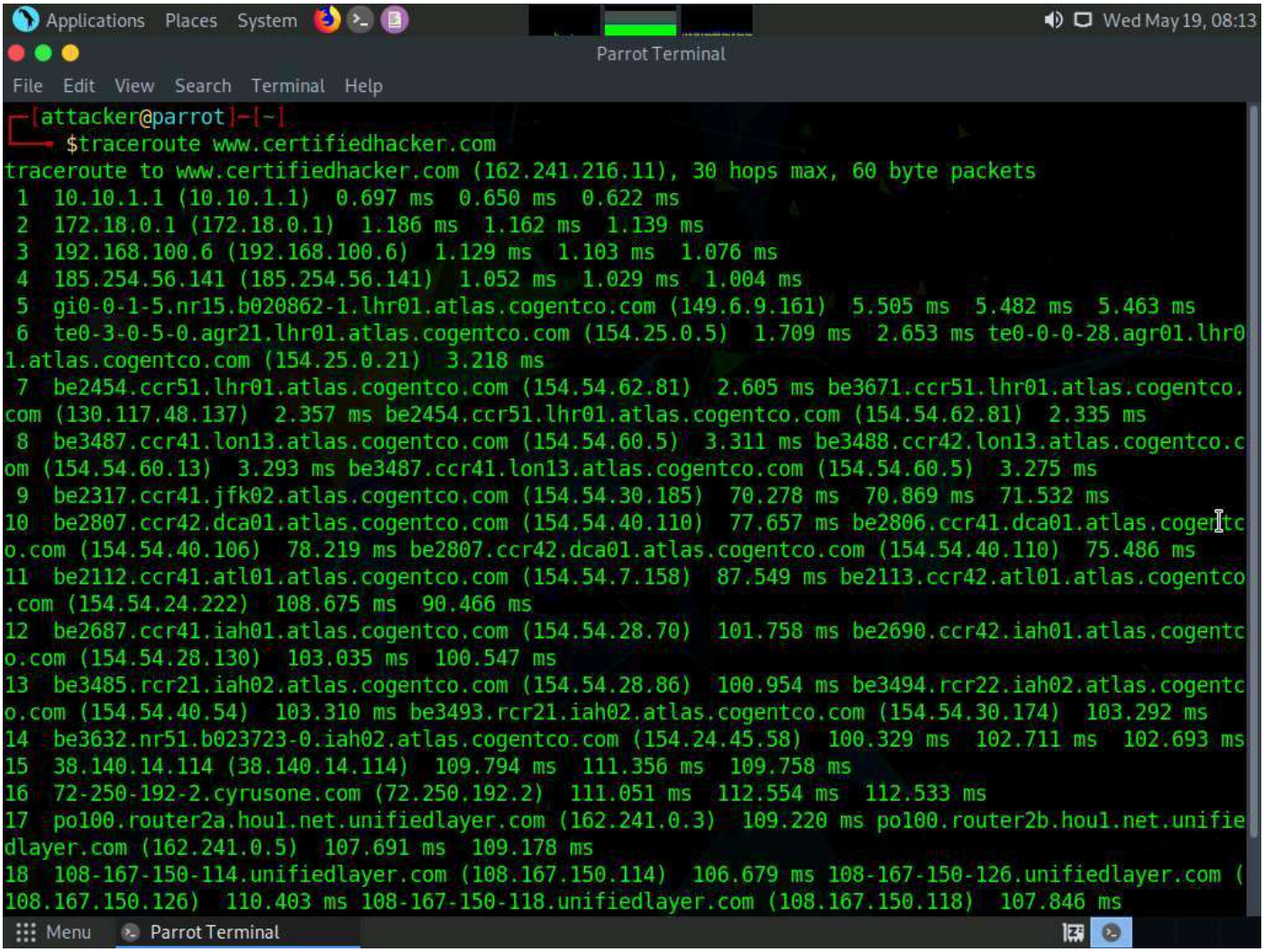
If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

9. Click the **MATE Terminal** icon at the top-left corner of the **Desktop** window to open a **Terminal** window.



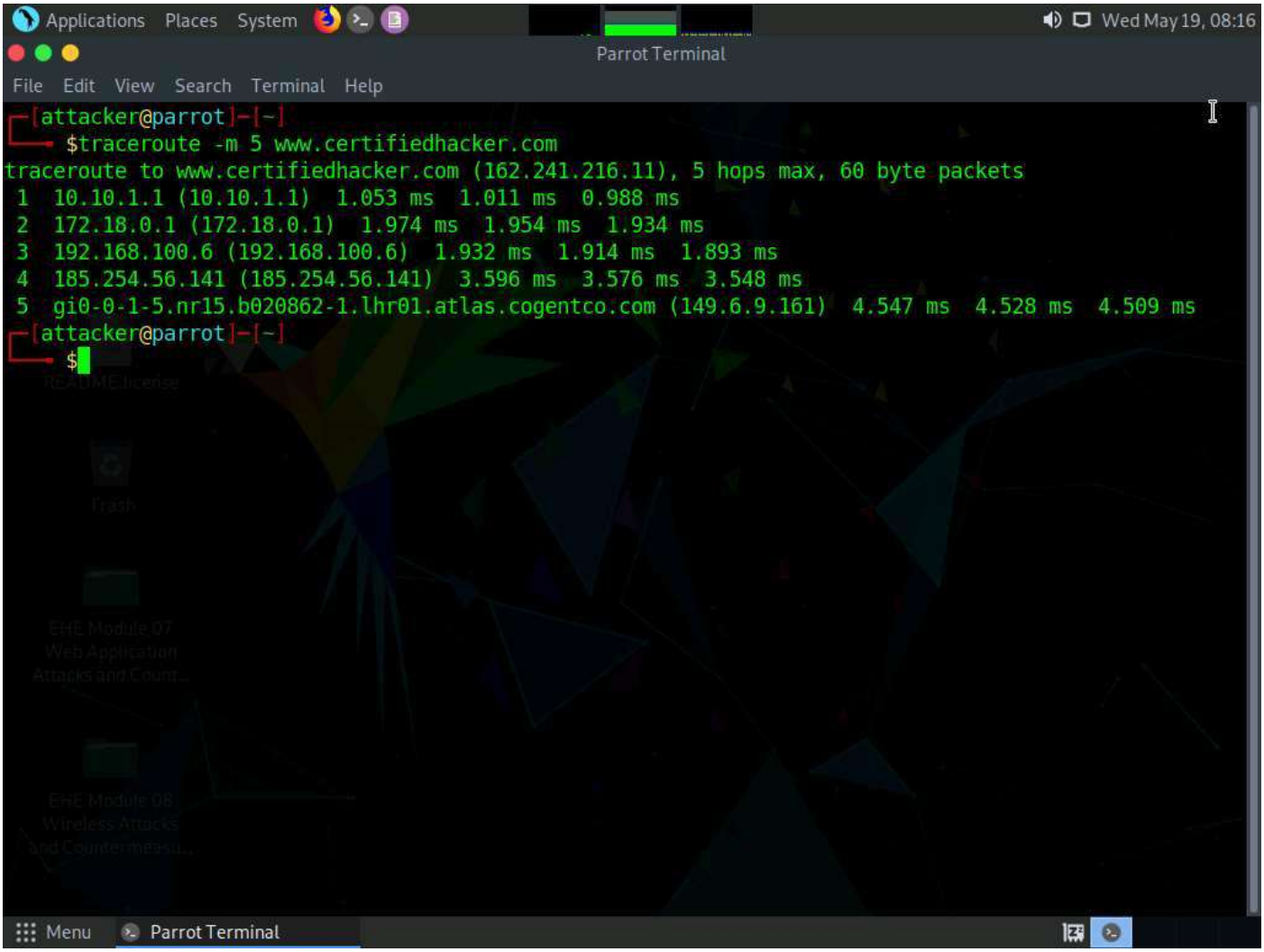
10. A **Parrot Terminal** window appears. In the terminal window, type **traceroute www.certifiedhacker.com** and press **Enter** to view the hops that the packets made before reaching the destination.

Since we have set up a simple network, you can find the direct hop from the source to the target destination. However, screenshots may vary depending on the target destination.



11. Now, type **traceroute -m 5 www.certifiedhacker.com** and press **Enter** to set the max number of hops as **5** for the packet to reach the destination.

Default value of hop count is 30.



12. This concludes the demonstration of performing network tracerouting using the Windows and Linux machines.
13. Close all open windows and document all acquired information.

Task 2: Perform Host Discovery using Nmap

Nmap is a utility used for network discovery, network administration, and security auditing. It is also used to perform tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Here, we will use Nmap to discover a list of live hosts in the target network. We can use Nmap to scan the active hosts in the target network using various host discovery techniques such as ARP ping scan, UDP ping scan, ICMP ECHO ping scan, ICMP ECHO ping sweep, etc.

Here, we will consider EC-Council as a target organization.

If you are already logged into the **Windows 10** machine, then skip to **Step#3**.

1. Click Windows 10 to switch to the **Windows 10** machine.

Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 10** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under Commands (**thunder** icon) menu.

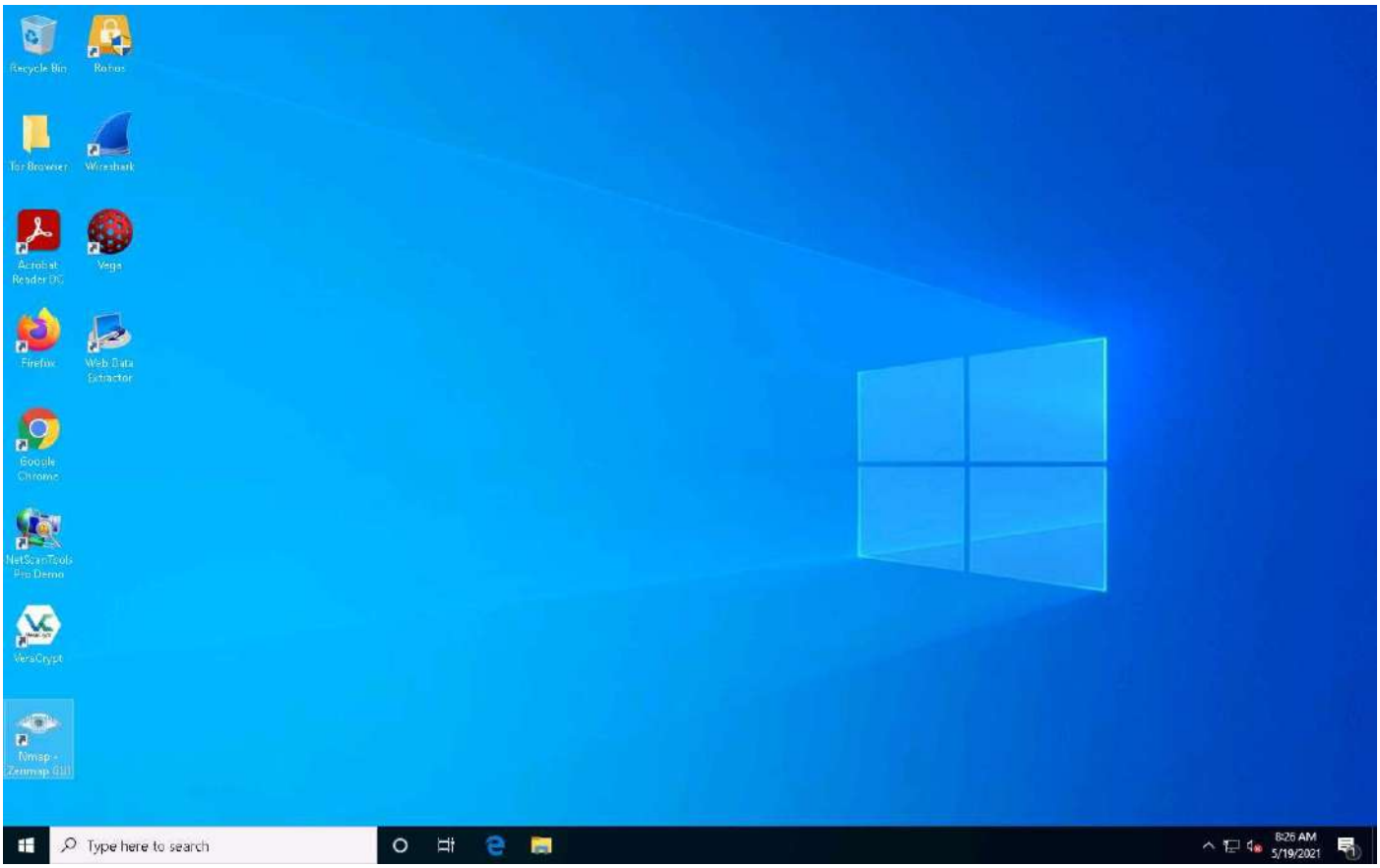
2. By default, **Admin** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.

Alternatively, you can also click **Pa$$w0rd** under **Windows 10** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

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

3. Navigate to the Desktop and double-click **Nmap - Zenmap GUI** shortcut.



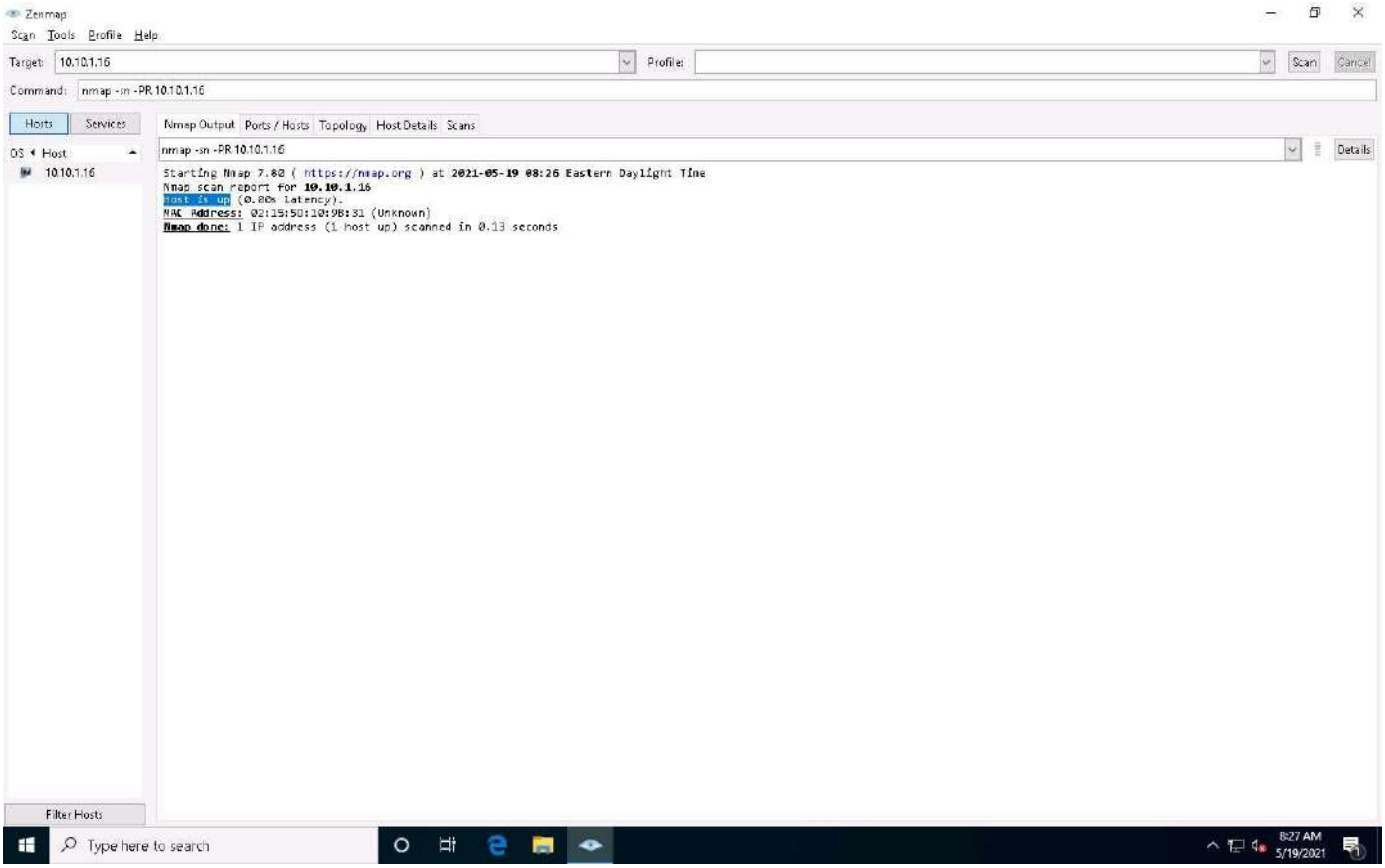
4. The **Nmap - Zenmap** GUI appears; in the **Command** field, type the command **nmap -sn -PR [Target IP Address]** (here, the target IP address is **10.10.1.16**) and click **Scan**.

-sn: disables port scan and **-PR**: performs ARP ping scan.

5. The scan results appear, indicating that the target **Host is up**, as shown in the screenshot.

In this lab, we are targeting the **Windows Server 2016** (**10.10.1.16**) machine.

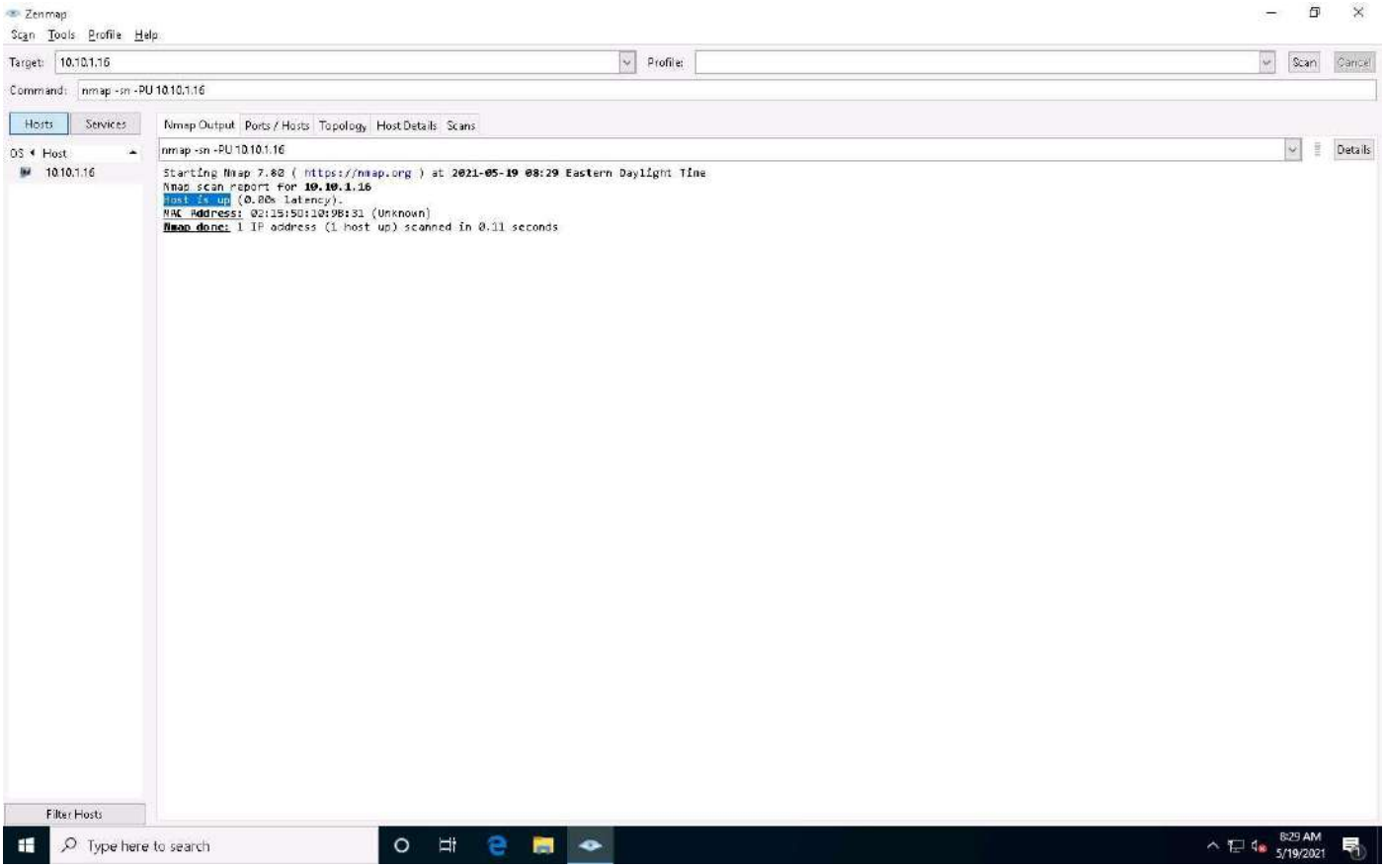
The ARP ping scan probes ARP request to target host; an ARP response means that the host is active.



6. In the **Command** field, type **nmap -sn -PU [Target IP Address]**, (here, the target IP address is **10.10.1.16**) and click **Scan**. The scan results appear, indicating the target **Host is up**, as shown in the screenshot.

-PU: performs the UDP ping scan.

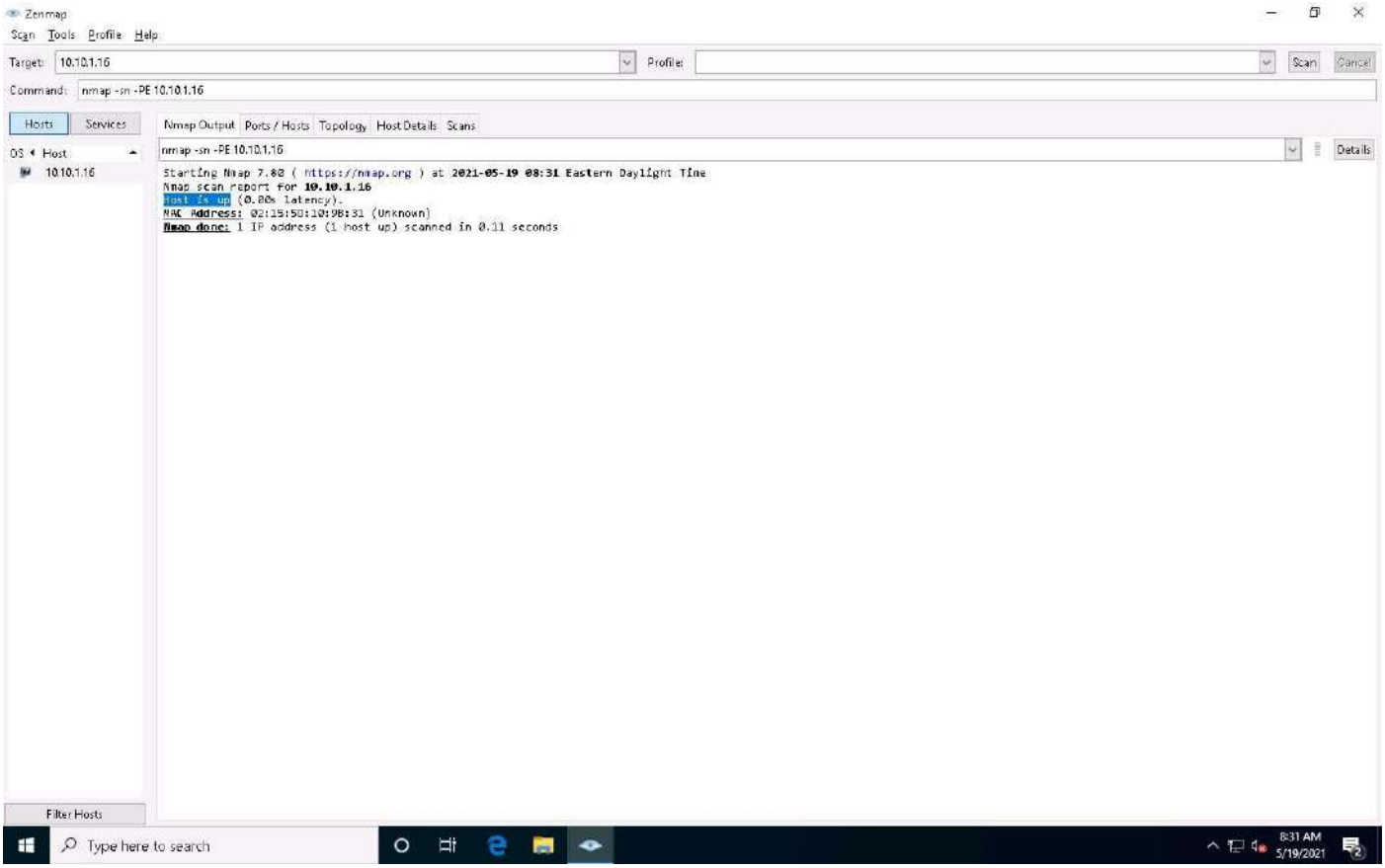
The UDP ping scan sends UDP packets to the target host; a UDP response means that the host is active. If the target host is offline or unreachable, various error messages such as “host/network unreachable” or “TTL exceeded” could be returned.



7. Now, we will perform the ICMP ECHO ping scan. In the **Command** field, type **nmap -sn -PE [Target IP Address]**, (here, the target IP address is **10.10.1.16**) and click **Scan**. The scan results appear, indicating that the target **Host is up**, as shown in the screenshot.

-PE: performs the ICMP ECHO ping scan.

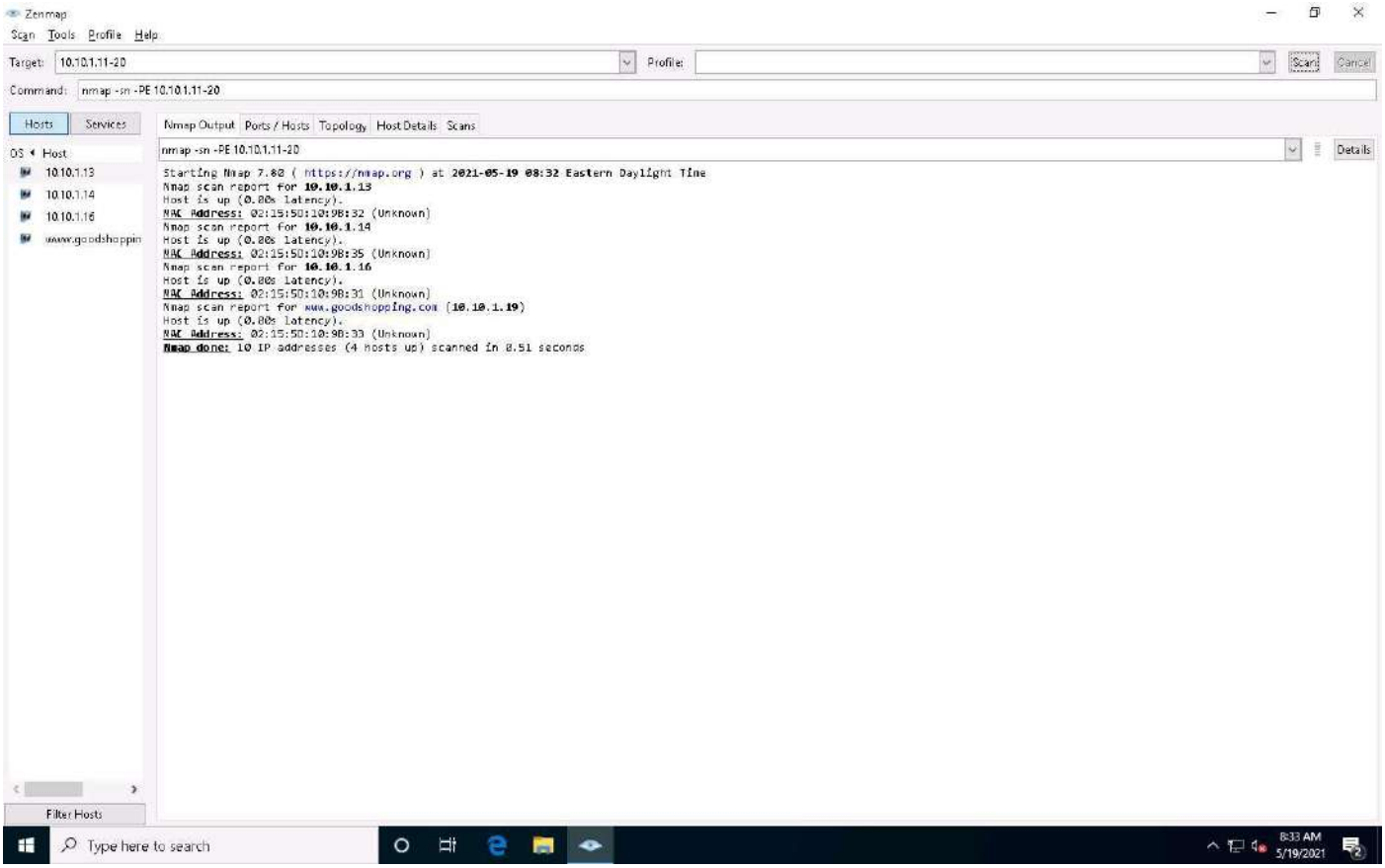
The ICMP ECHO ping scan involves sending ICMP ECHO requests to a host. If the target host is alive, it will return an ICMP ECHO reply. This scan is useful for locating active devices or determining if the ICMP is passing through a firewall.



8. Now, we will perform an ICMP ECHO ping sweep to discover live hosts from a range of target IP addresses. In the **Command** field, type **nmap -sn -PE [Target Range of IP Addresses]** (here, the target range of IP addresses is **10.10.1.11-20**) and click **Scan**. The scan results appear, indicating the target **Host is up**, as shown in the screenshot.

In this lab task, we are scanning **Windows Server 2019**, **Windows Server 2016**, **Parrot Security** and **Android** machines.

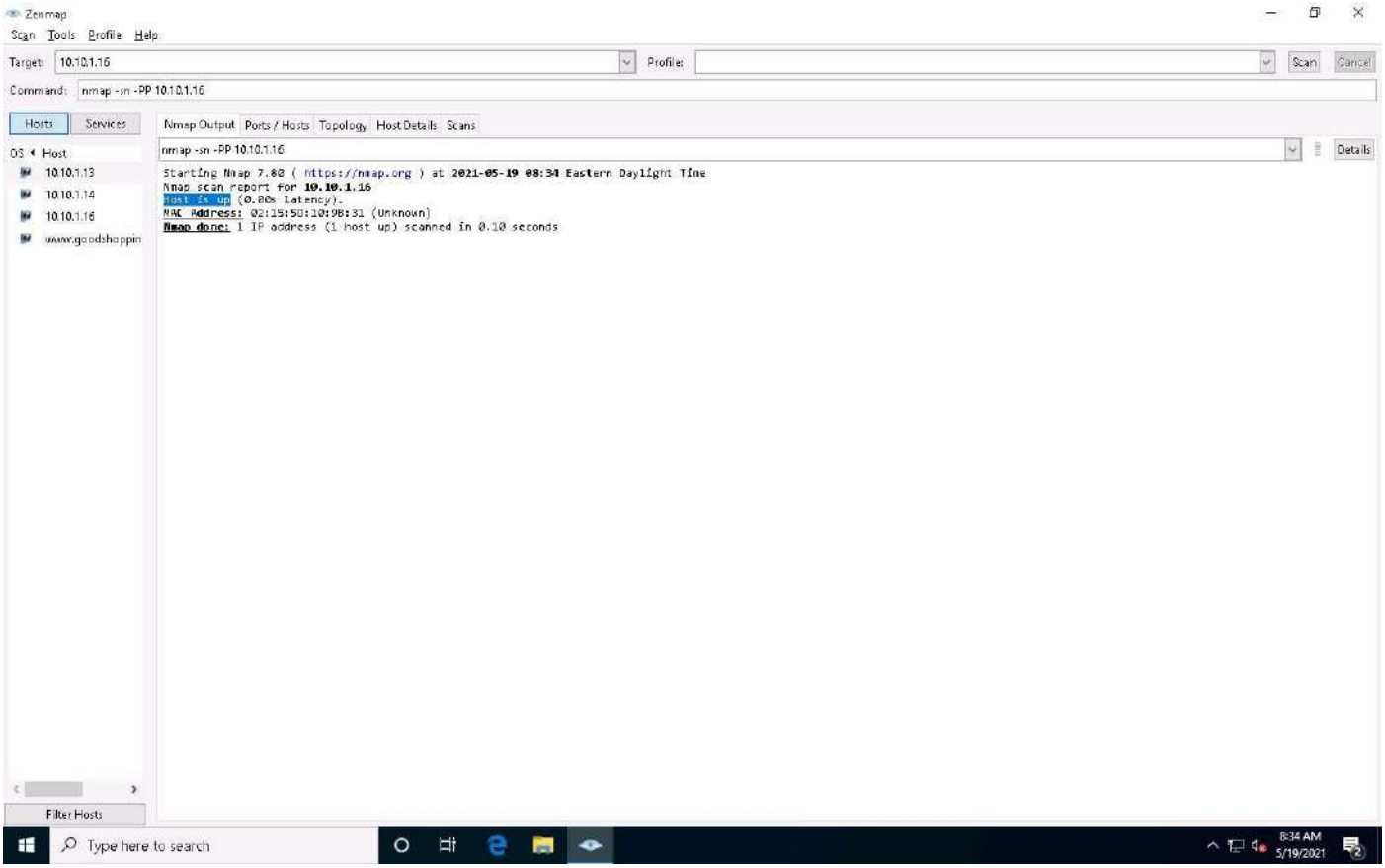
The ICMP ECHO ping sweep is used to determine the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts. If a host is alive, it will return an ICMP ECHO reply.



9. Now, we will perform the ICMP timestamp ping scan. In the **Command** field, type **nmap -sn -PP [Target IP Address]**, (here, the target IP address is **10.10.1.16**) and click **Scan**. The scan results appear, indicating that the target **Host is up**, as shown in the screenshot.

-PP: performs the ICMP timestamp ping scan.

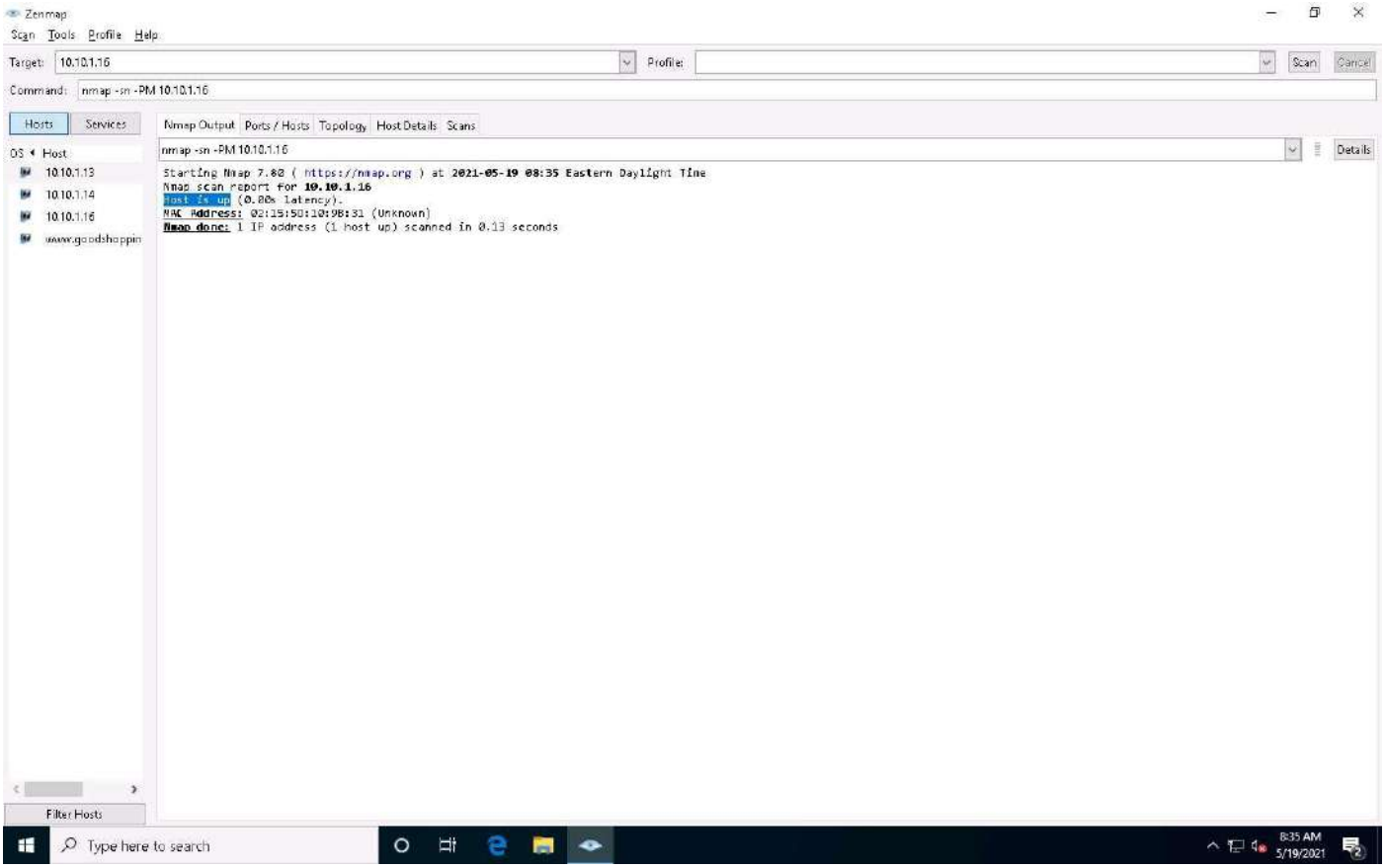
In ICMP timestamp ping scan the target machine responds with a timestamp reply to each timestamp query that is received. It is an optional and additional type of ICMP ping whereby a timestamp message can be queried to acquire the information related to the current time from the target host machine.



10. Now, we will perform the ICMP address mask ping scan. In the **Command** field, type **nmap -sn -PM [Target IP Address]**, (here, the target IP address is **10.10.1.16**) and click **Scan**. The scan results appear, indicating that the target **Host is up**, as shown in the screenshot.

-PM: performs the **ICMP timestamp ping scan**.

In ICMP address mask ping scan ICMP address mask query is sent to the target host to acquire information related to the subnet mask.This type of ping method is also effective in identifying the active hosts similarly to the ICMP timestamp ping, specifically when the administrator blocks the traditional ICMP Echo ping.



11. Apart from the aforementioned network scanning techniques, you can also use the following scanning techniques to perform a host discovery on a target network.

    - **ICMP Timestamp and Address Mask Ping Scan**: These techniques are alternatives for the traditional ICMP ECHO ping scan, which are used to determine whether the target host is live specifically when administrators block the ICMP ECHO pings.

Example –

ICMP timestamp ping scan

 # nmap -sn -PP [target IP address]

ICMP address mask ping scan

 # nmap -sn -PM [target IP address]

    - **TCP SYN Ping Scan**: This technique sends empty TCP SYN packets to the target host, ACK response means that the host is active.

 # nmap -sn -PS [target IP address]

    - **TCP ACK Ping Scan**: This technique sends empty TCP ACK packets to the target host; an RST response means that the host is active.

 # nmap -sn -PA [target IP address]

    - **IP Protocol Ping Scan**: This technique sends different probe packets of different IP protocols to the target host, any response from any probe indicates that a host is active.

 # nmap -sn -PO [target IP address]

12. This concludes the demonstration of discovering the target host(s) in the target network using various host discovery techniques.
13. Close all open windows and document all the acquired information.

Task 2-3: Perform Port and Service Discovery using Mega Ping

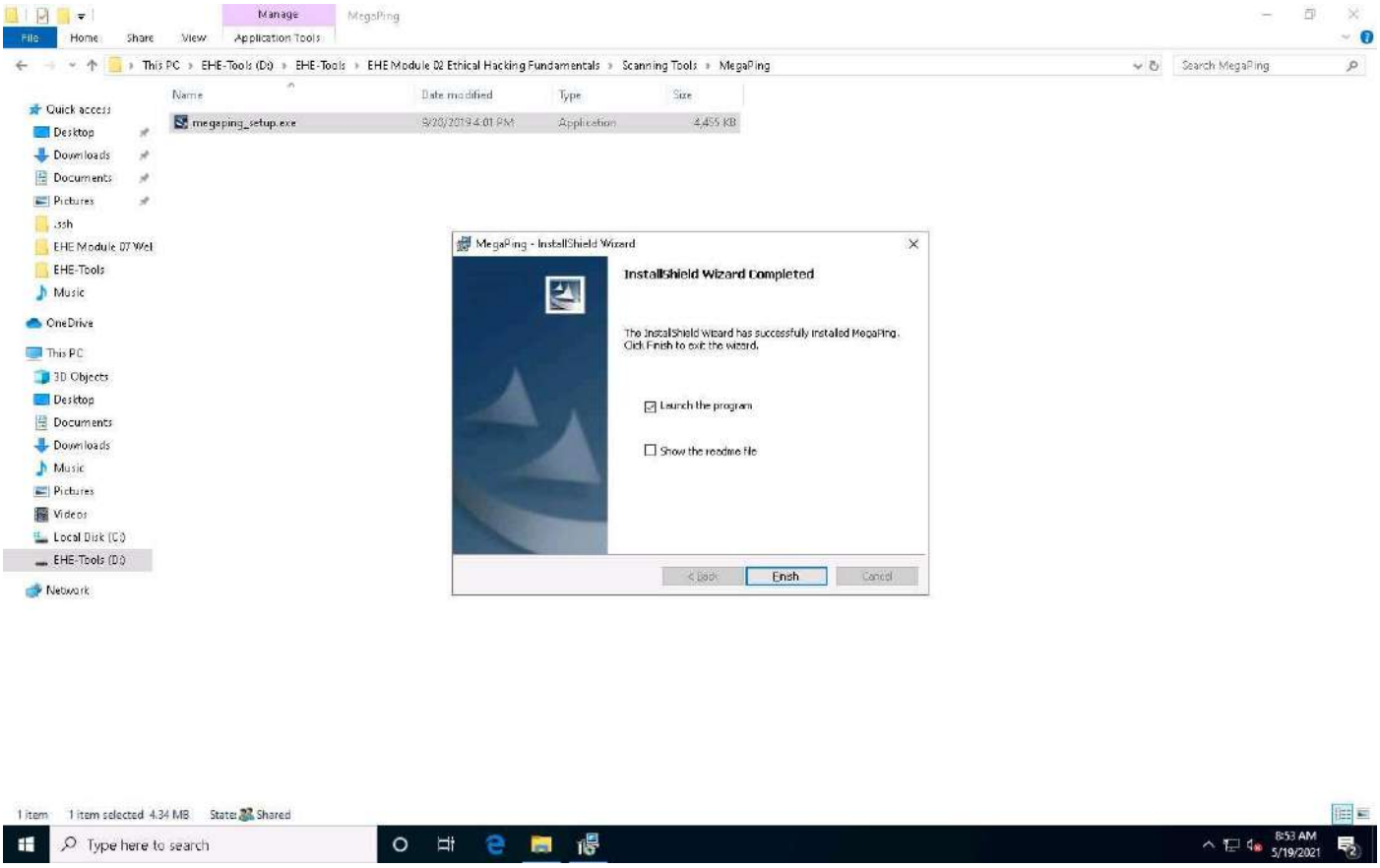
MegaPing is a toolkit that provides essential utilities for Information System specialists, system administrators, IT solution providers, and individuals. It is used to detect live hosts and open ports of the system in the network, and can scan your entire network and provide information such as open shared resources, open ports, services/drivers active on the computer, key registry entries, users and groups, trusted domains, printers, etc. You can also perform various network troubleshooting activities with the help of integrated network utilities such as DNS lookup name, DNS list hosts, Finger, host monitor, IP scanner, NetBIOS scanner, ping, port scanner, share scanner, traceroute, and Whois.

Here, we will use the MegaPing tool to scan for open ports and services running on the target range of IP addresses.

1. In the **Windows 10** machine, navigate to **D:\EHE-Tools\EHE Module 02 Ethical Hacking Fundamentals\Scanning Tools\MegaPing** and double-click **megaping_setup.exe**.

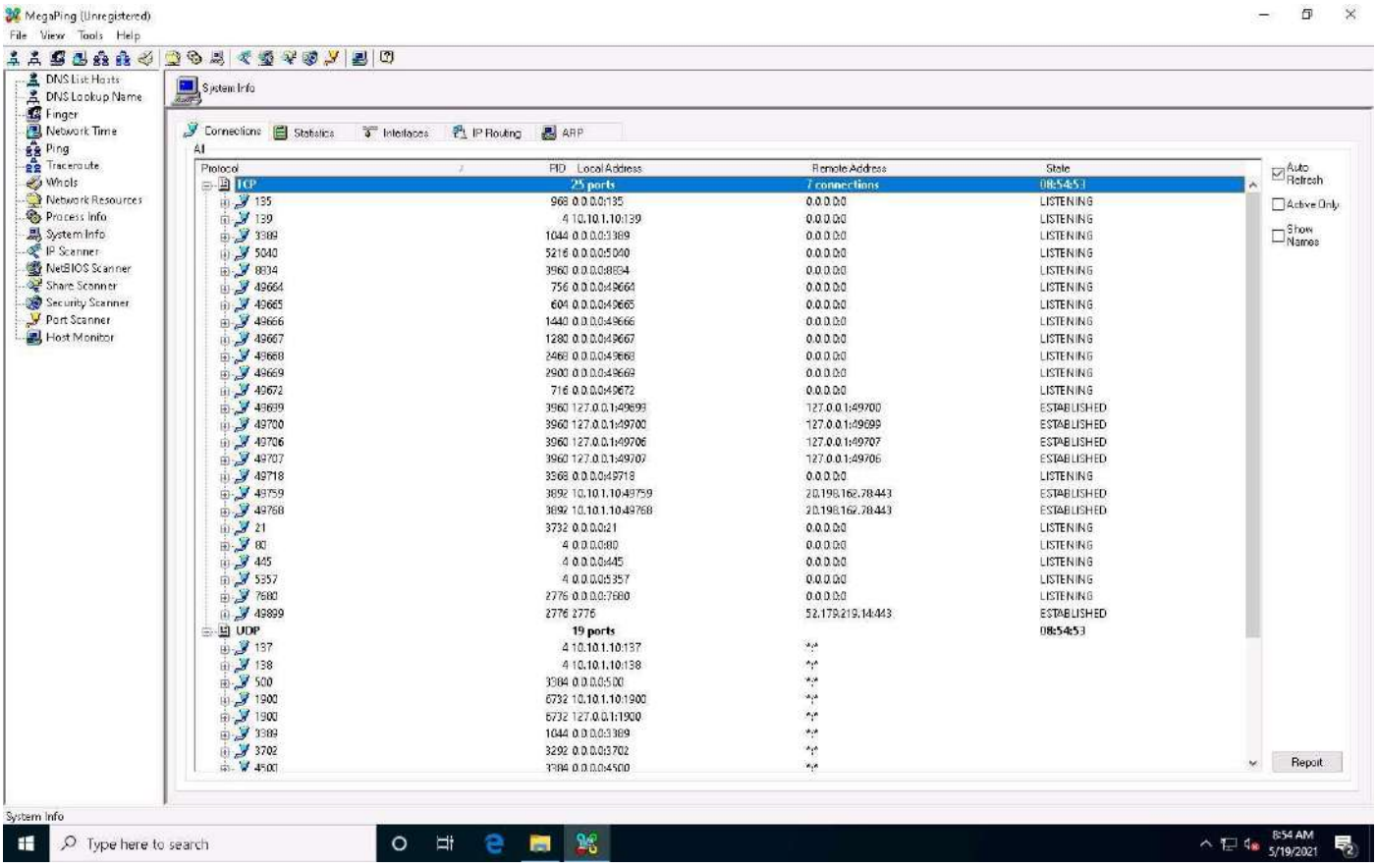
If a **User Account Control** pop-up appears, click **Yes**.

2. The **MegaPing - InstallShield Wizard** window appears; click **Next** and follow the wizard-driven installation steps to install **MegaPing**.
3. After the completion of the installation, click on the **Launch the program** checkbox and click **Finish**.

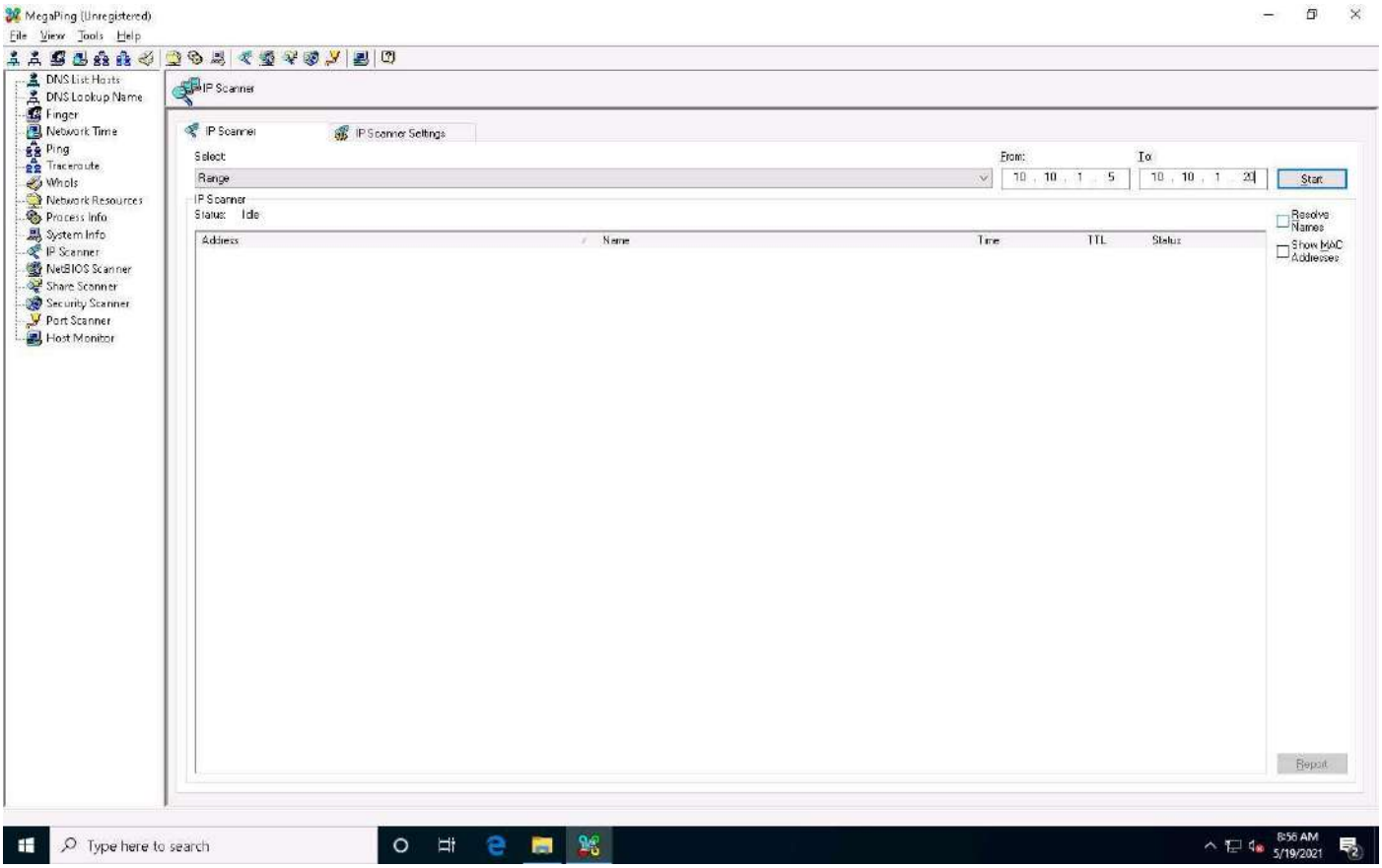


4. The **About MegaPing** window appears; click the **I Agree** button.

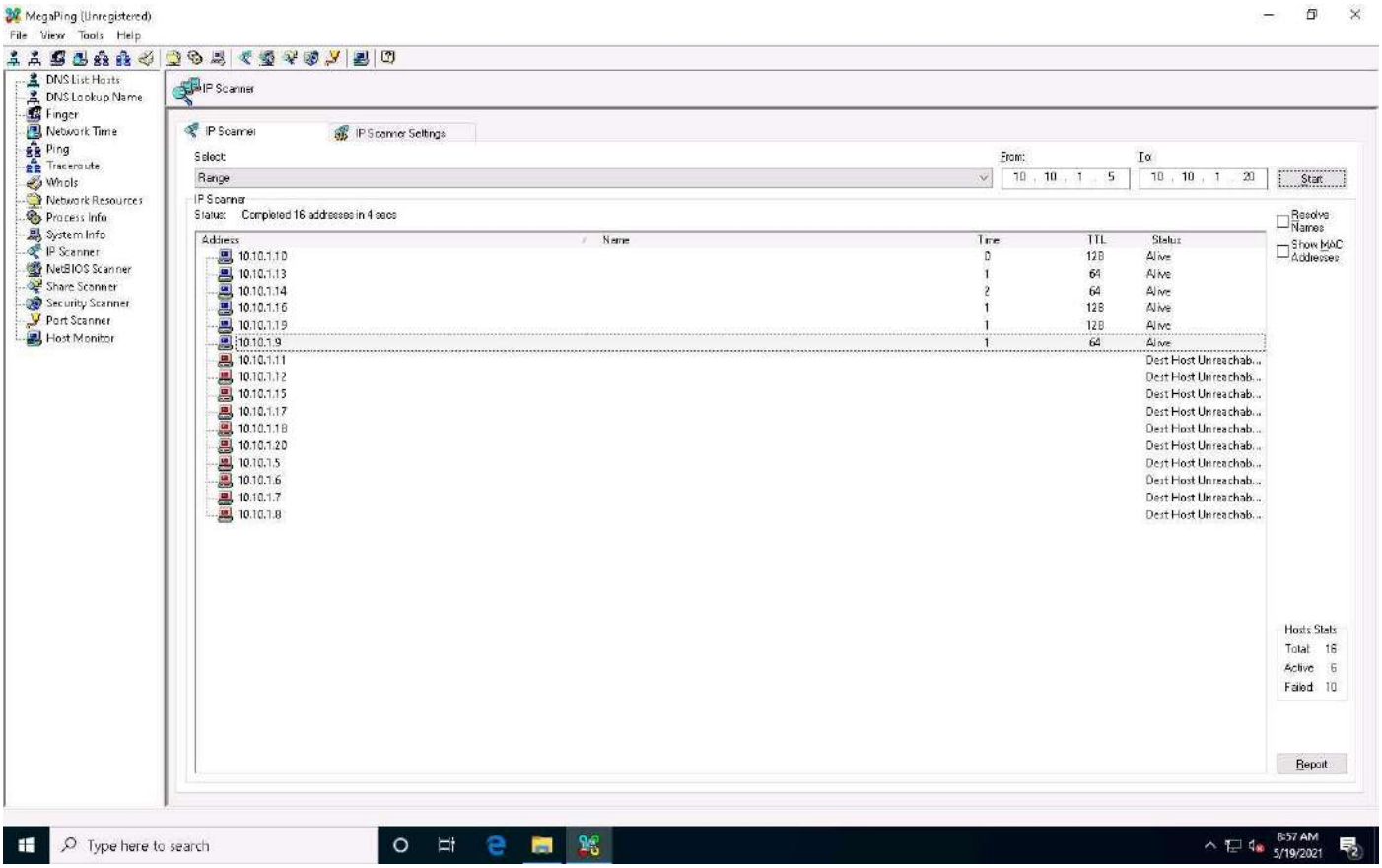
5. The **MegaPing (Unregistered)** GUI appears displaying the **System Info**, as shown in the screenshot.



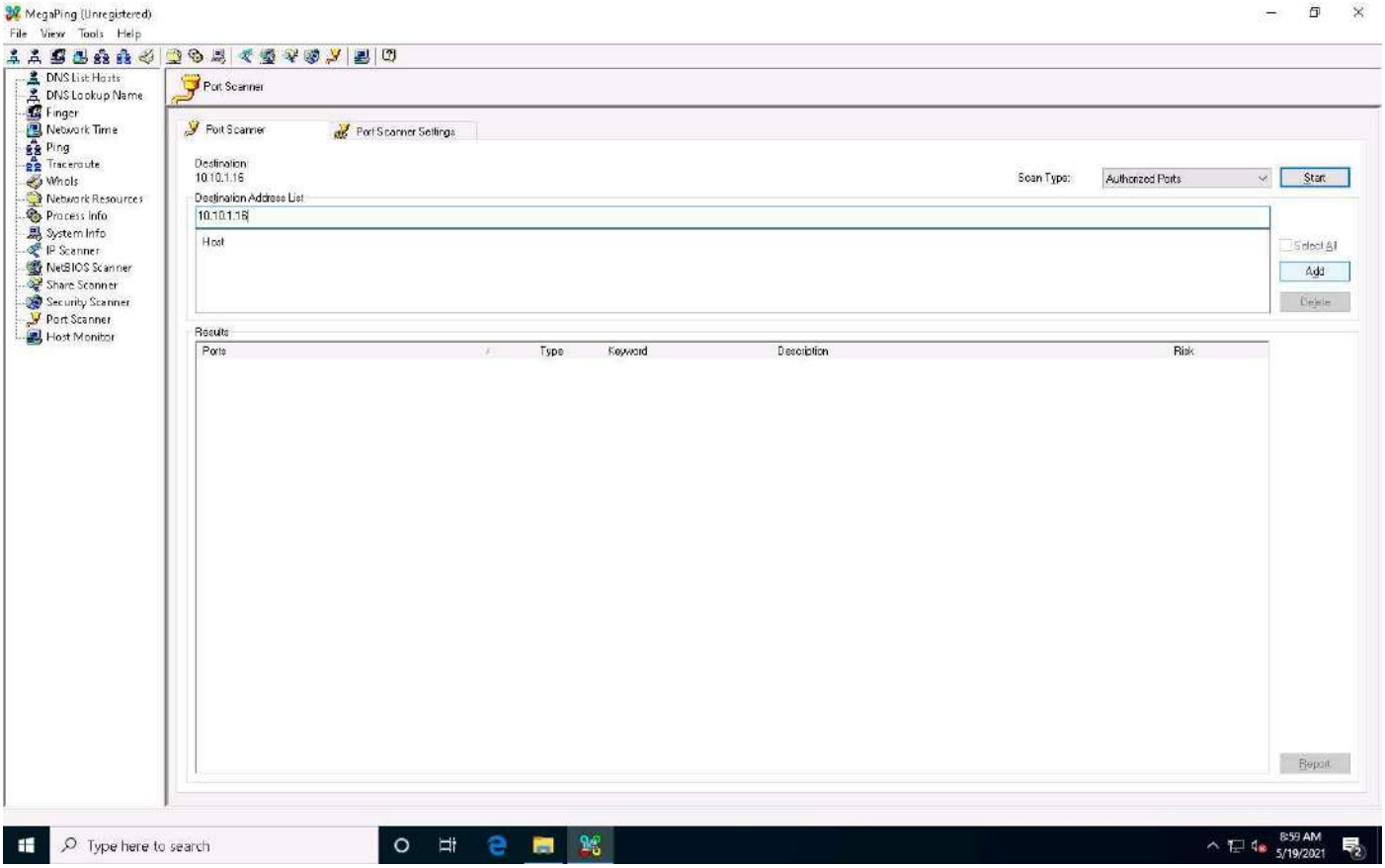
6. Select the **IP Scanner** option from the left pane. In the **IP Scanner** tab in the right-hand pane, enter the IP range in the **From** and **To** fields; in this lab, the IP range is **10.10.1.5** to **10.10.1.20**; then, click **Start**.



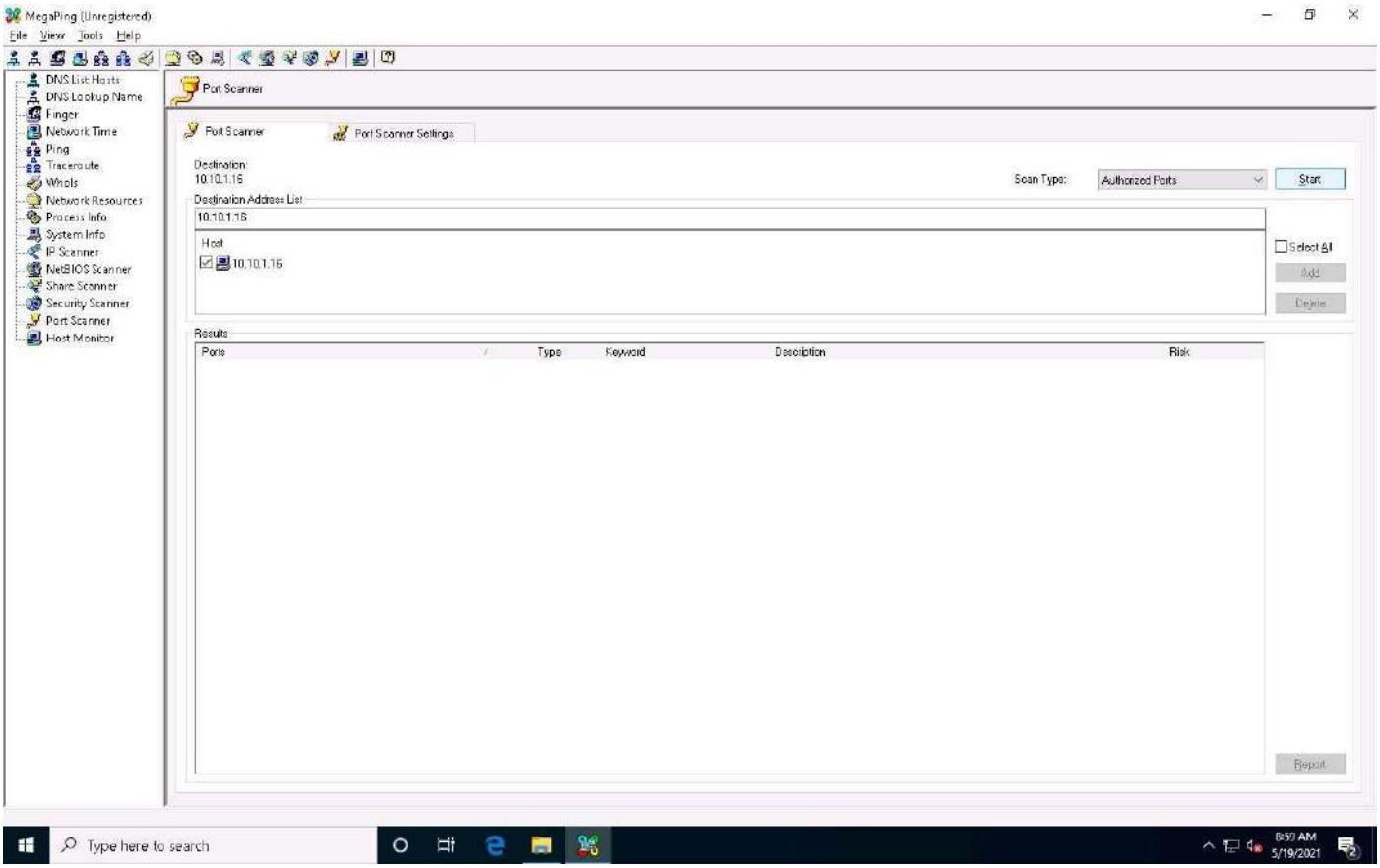
7. MegaPing lists all IP addresses under the specified target range with their TTL value, Status (dead or alive), and statistics of the dead and alive hosts, as shown in the screenshot.



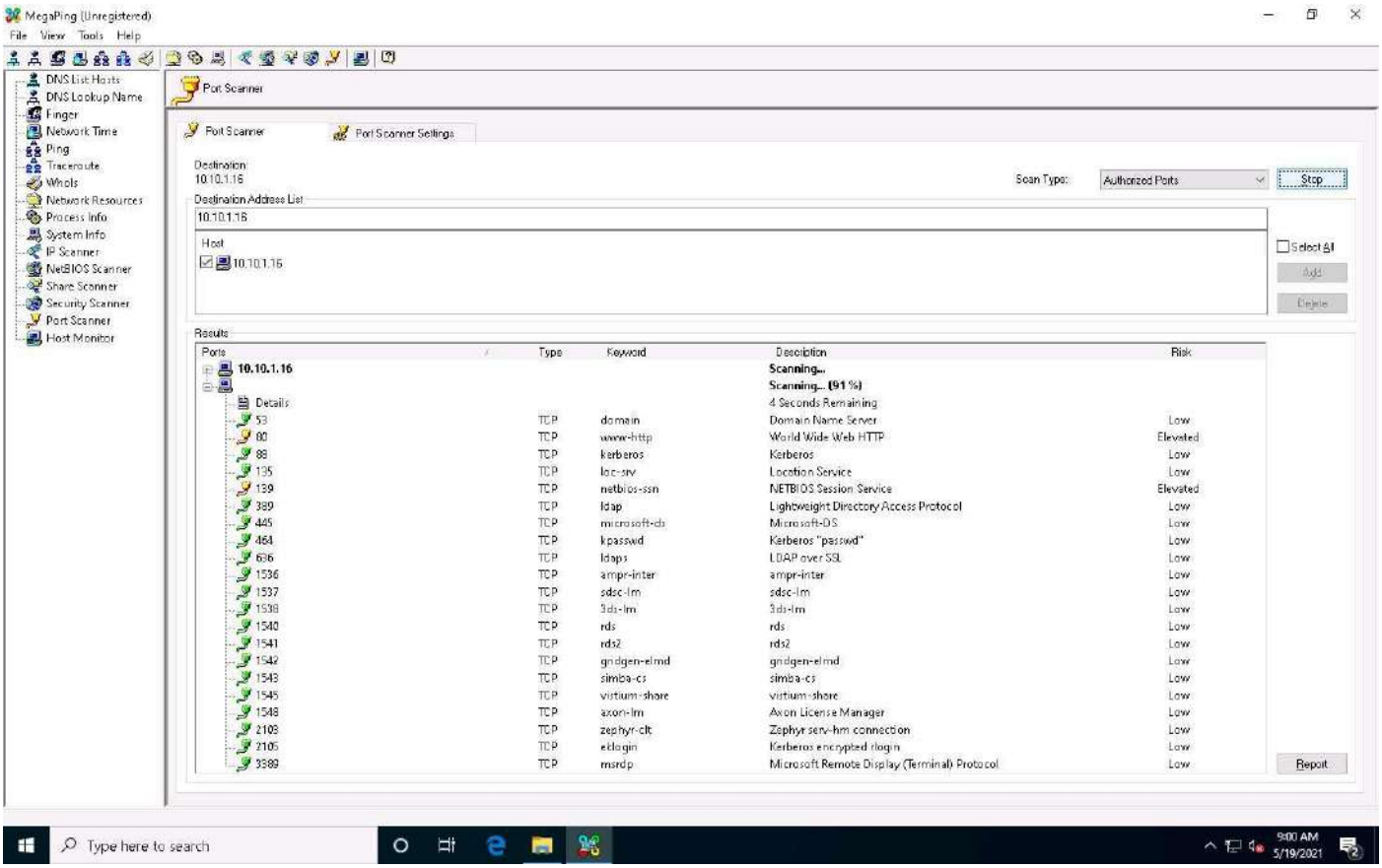
8. Select the **Port Scanner** option from the left-hand pane. In the **Port Scanner** tab in the right-hand pane, enter the IP address of the **Windows Server 2016** (**10.10.1.16**) machine into the **Destination Address List** field and click **Add**.



9. Select the **10.10.1.16** checkbox and click the **Start** button to start listening to the traffic on 10.10.1.16.



10. MegaPing lists the ports associated with **Windows Server 2016** (**10.10.1.16**), with detailed information on port number and type, service running on the port along with the description, and associated risk, as shown in the screenshot.



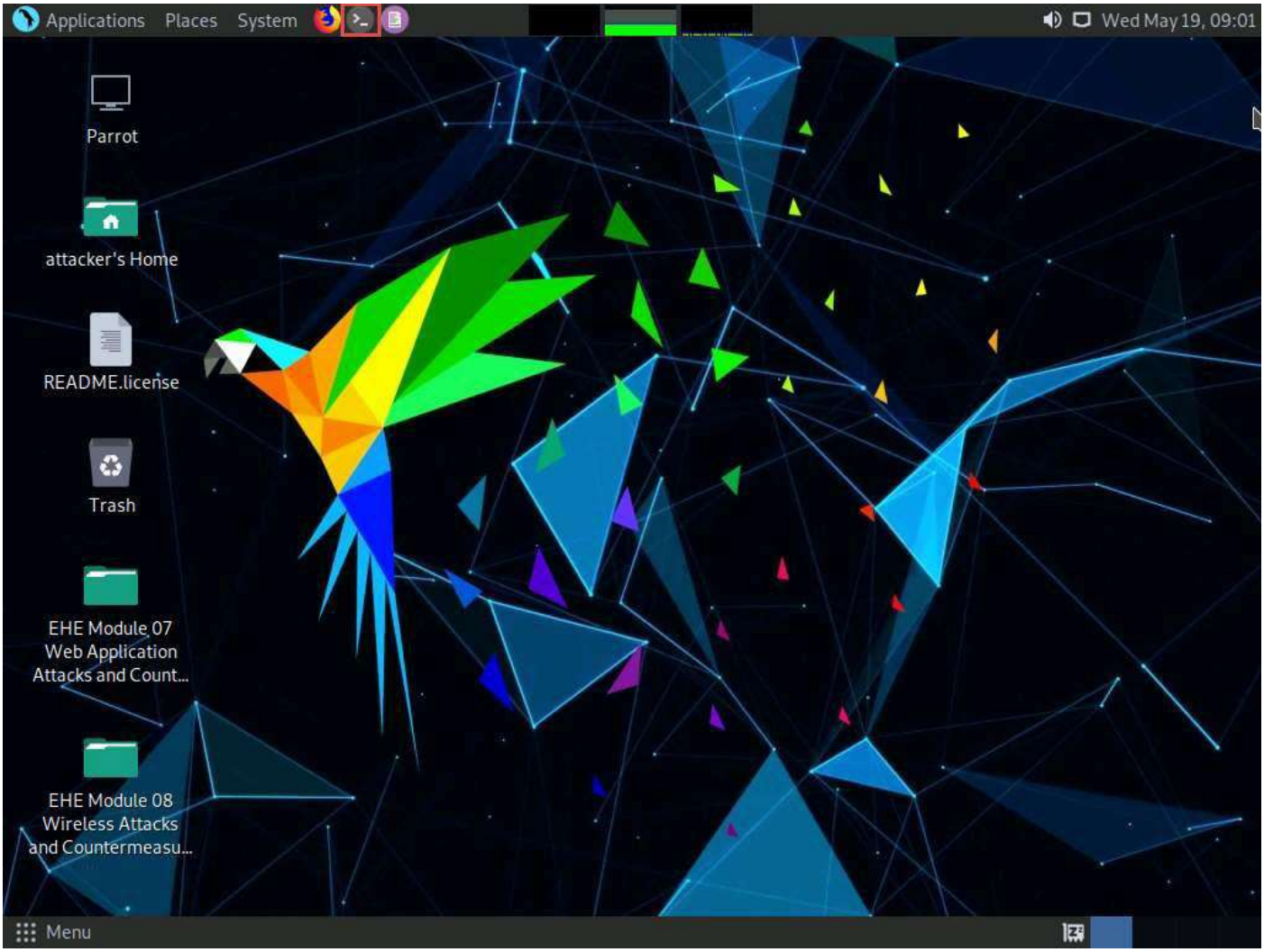
11. Similarly, you can perform port and service scanning on other target machines.
12. This concludes the demonstration of discovering open ports and services running on the target IP address using MegaPing.
13. Close all open windows and document all the acquired information.

Task 4: Perform OS Discovery using Unicornscan

Unicornscan is a Linux-based command line-oriented network information-gathering and reconnaissance tool. It is an asynchronous TCP and UDP port scanner and banner grabber that enables you to discover open ports, services, TTL values, etc. running on the target machine. In Unicornscan, the OS of the target machine can be identified by observing the TTL values in the acquired scan result.

Here, we will use the Unicornscan tool to perform OS discovery on the target system.

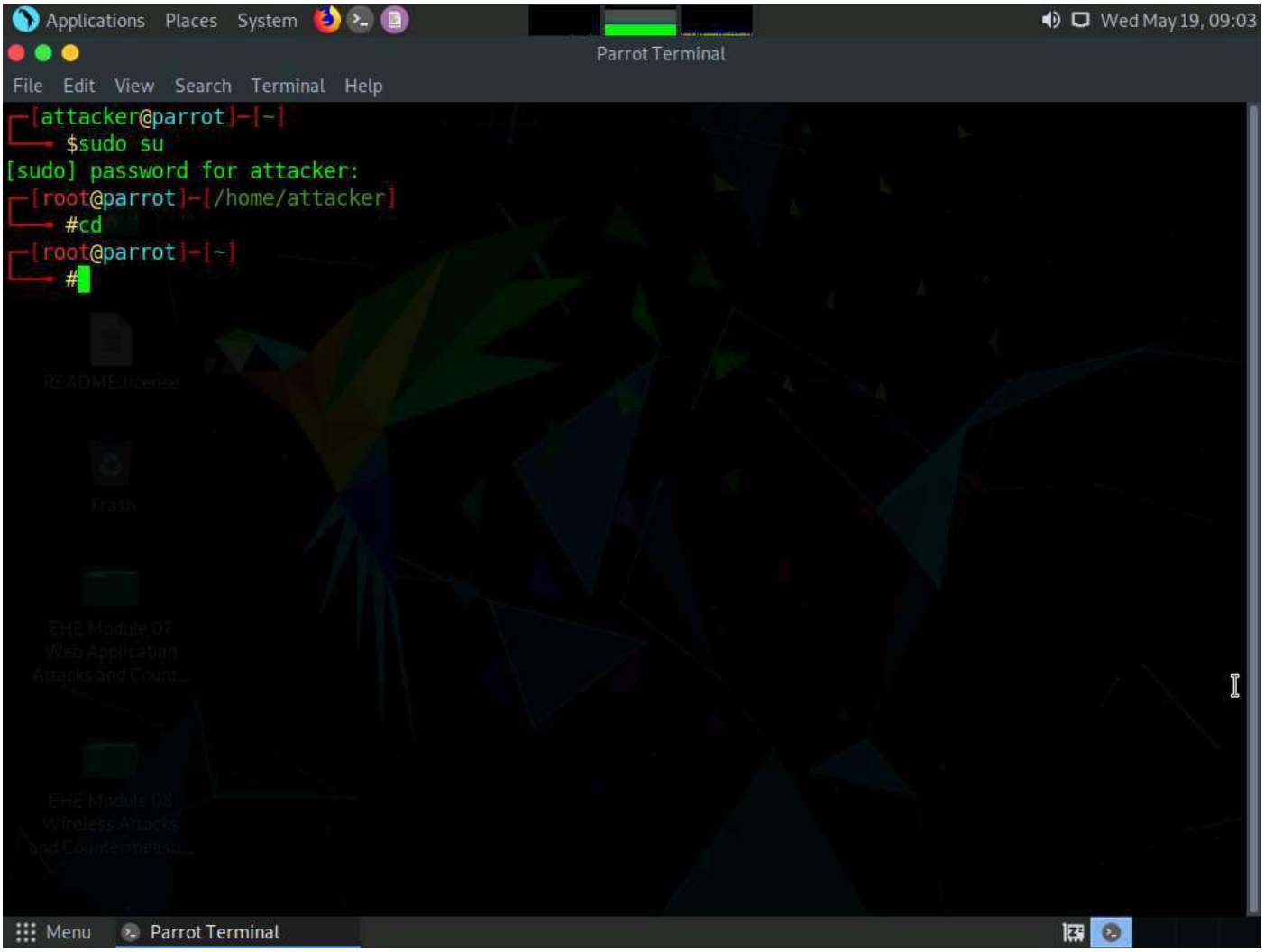
1. Click Parrot Security to switch to the **Parrot Security** machine.
2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.



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**.

The password that you type will not be visible.

5. Now, type **cd** and press **Enter** to jump to the root directory.

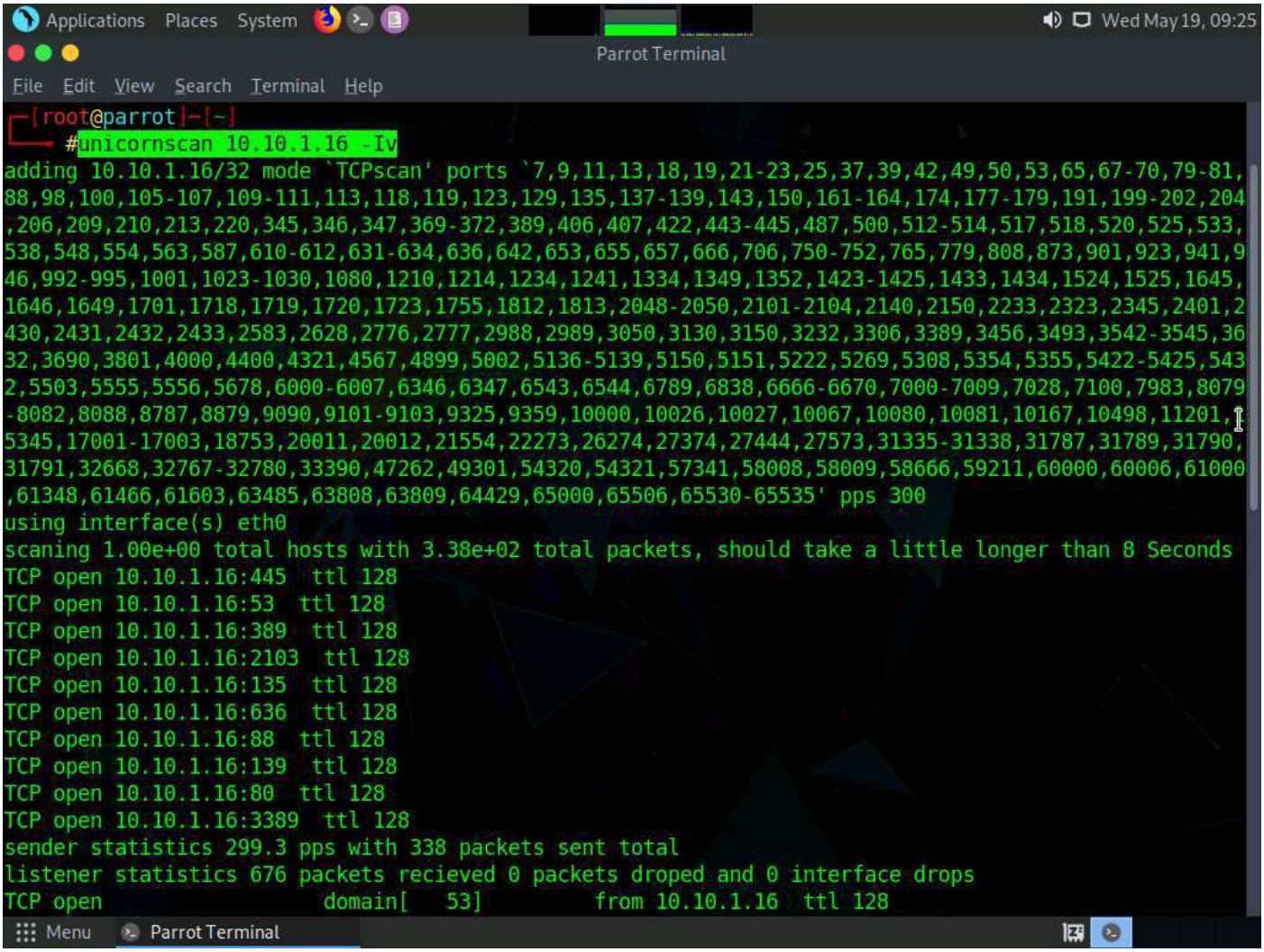


6. In the terminal window, type **unicornscan [Target IP Address] -Iv** (here, the target machine is **Windows Server 2016** [**10.10.1.16**]) and press **Enter**.

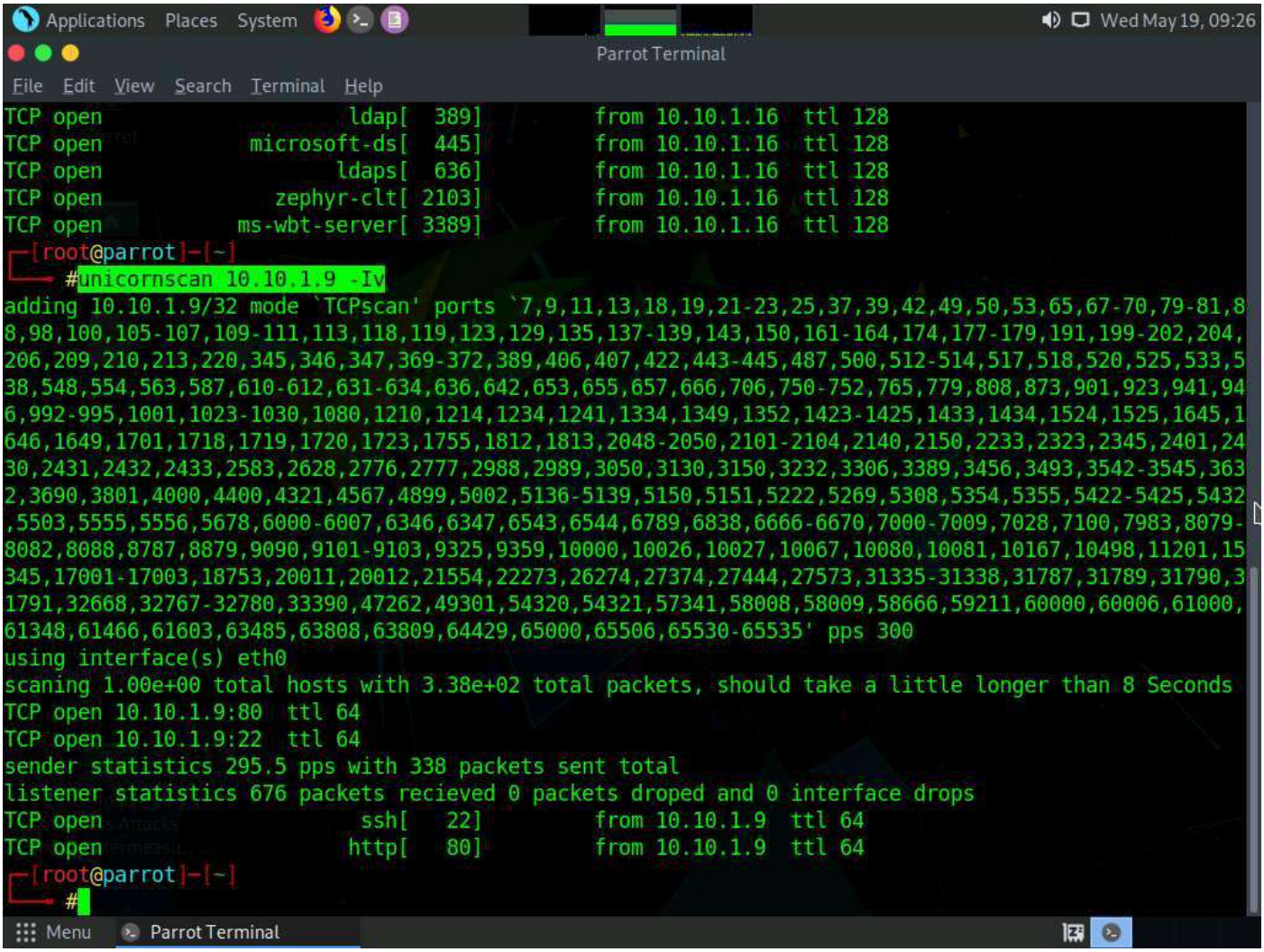
In this command, **-I** specifies an immediate mode and **v** specifies a verbose mode.

7. The scan results appear, displaying the open TCP ports along with the obtained TTL value of **128**. As shown in the screenshot, the **ttl** values acquired after the scan are **128**; hence, the OS is possibly Microsoft Windows (Windows 7/8/8.1/10 or Windows Server 2008/12/16).

Here, the target machine is **Windows Server 2016** (**10.10.1.16**).



8. In the **Parrot Terminal** window, type **unicornscan [Target IP Address] -Iv** (here, the target machine is **Ubuntu** [**10.10.1.9**]) and press **Enter**.
9. The scan results appear, displaying the open TCP ports along with a TTL value of **64**. As shown in the screenshot, the **ttl** values acquired after the scan are **64**; hence, the OS is possibly a Linux-based machine (Google Linux, Ubuntu, Parrot, or Kali).



10. This concludes the demonstration of discovering the OS of the target machine using Unicornscan.
11. Close all open windows and document all the acquired information.

Lab 2-3: Perform Enumeration on a System or Network to Extract Usernames, Machine Names, Network Resources, Shares, etc.

Lab Scenario

Enumeration creates an active connection with the system and performs directed queries to gain more information about the target. It extracts lists of computers, usernames, user groups, ports, OSes, machine names, network resources, and services using various techniques. Enumeration techniques are conducted in an intranet environment.

Lab Objectives

- Perform NetBIOS Enumeration using Windows Command-Line Utilities
- Perform NetBIOS Enumeration using NetBIOS Enumerator

Task 1: Perform NetBIOS Enumeration using Windows Command-Line Utilities

Nbtstat helps in troubleshooting NETBIOS name resolution problems. The nbtstat command removes and corrects preloaded entries using several case-sensitive switches. Nbtstat can be used to enumerate information such as NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local and remote computers, and the NetBIOS name cache.

Net use connects a computer to, or disconnects it from a shared resource. It also displays information about computer connections.

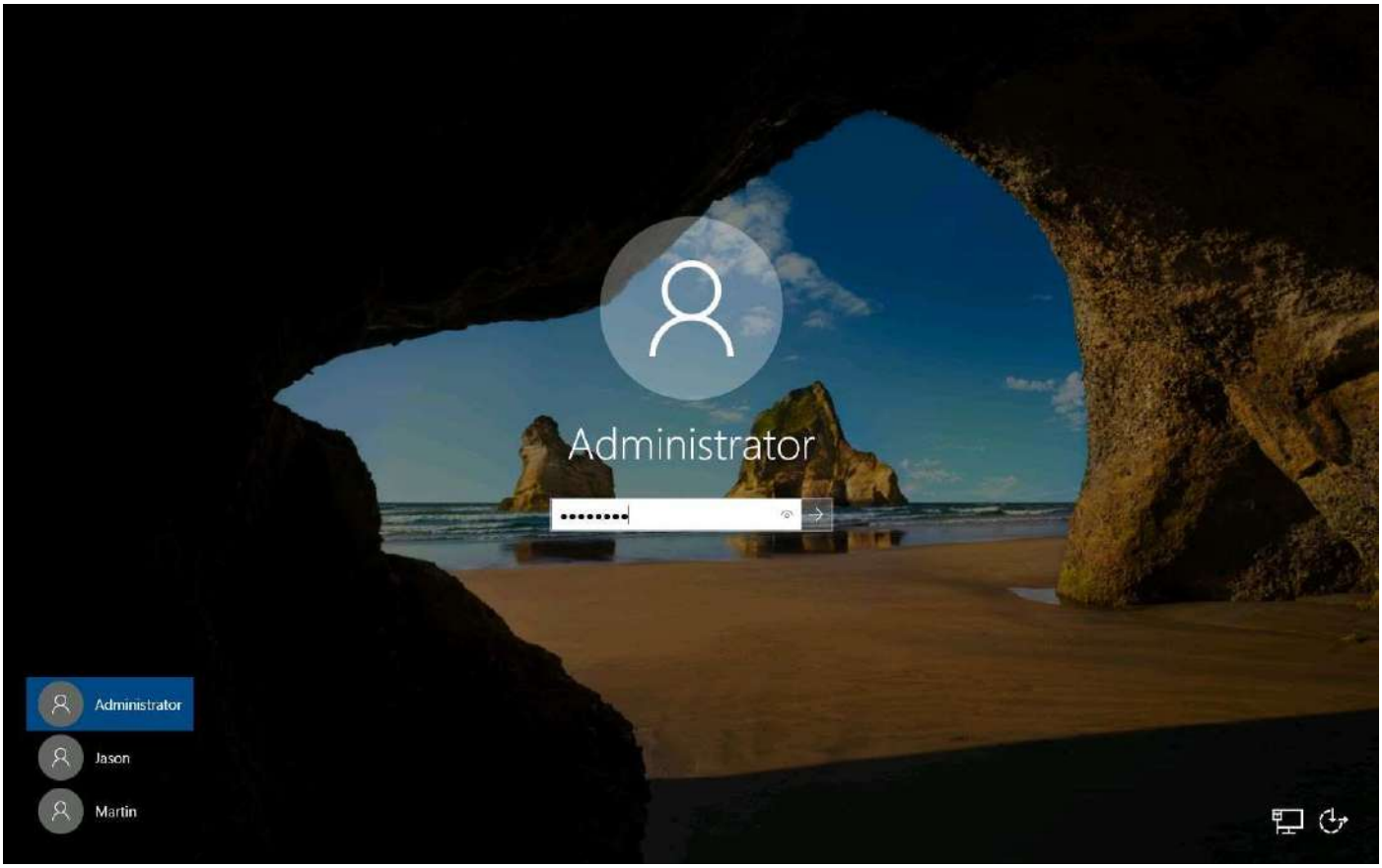
Here, we will use the Nbtstat and Net use Windows command-line utilities to perform NetBIOS enumeration on the target network.

We will use a **Windows Server 2019** (10.10.1.19) machine to target a **Windows 10** (10.10.1.10) machine.

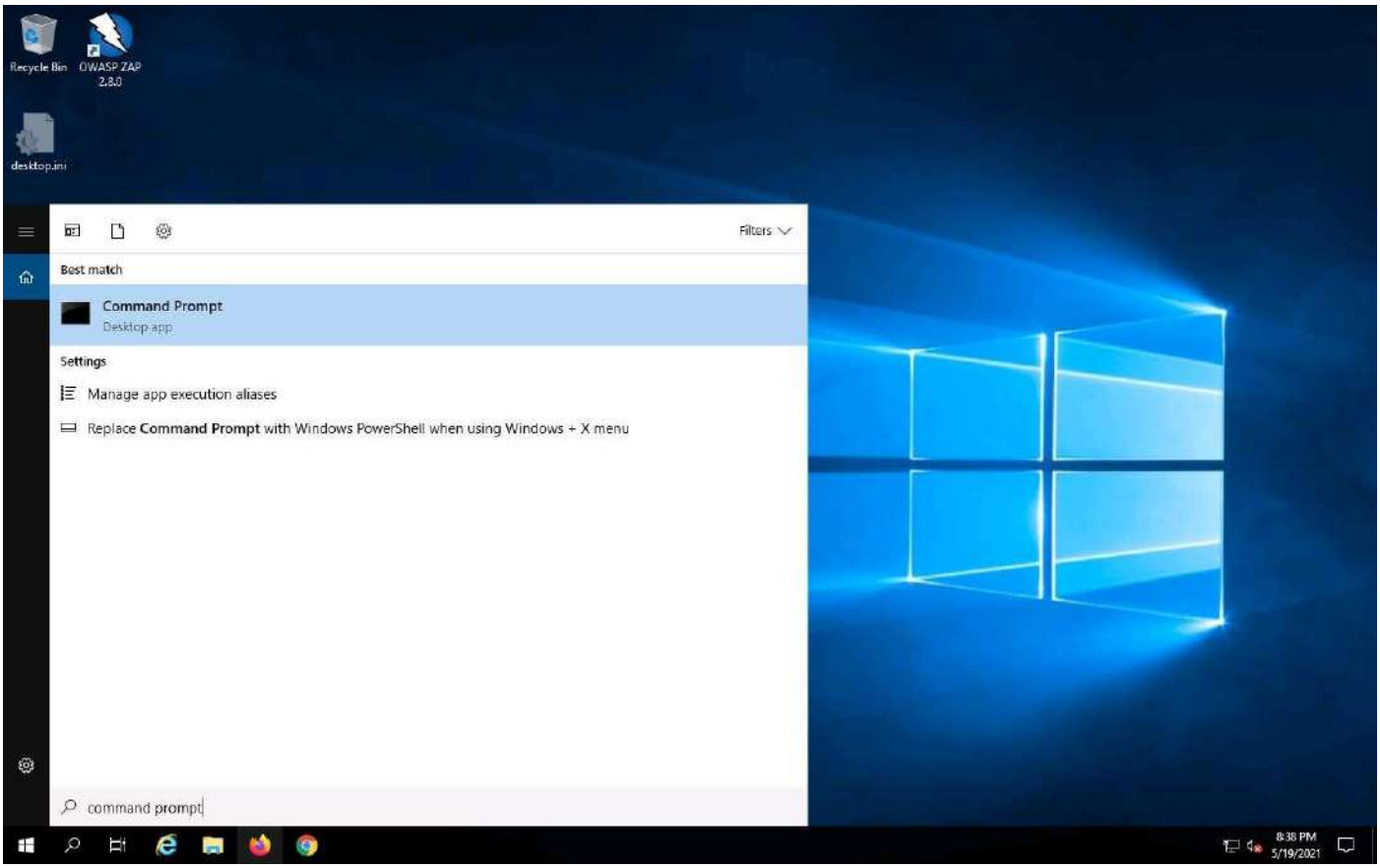
1. Click Windows Server 2019 to switch to the **Windows Server 2019** machine.
2. Click Ctrl+Alt+Delete to activate the machine. By default, **Administration** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.

Alternatively, you can also click **Pa$$w0rd** under **Windows Server 2019** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

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



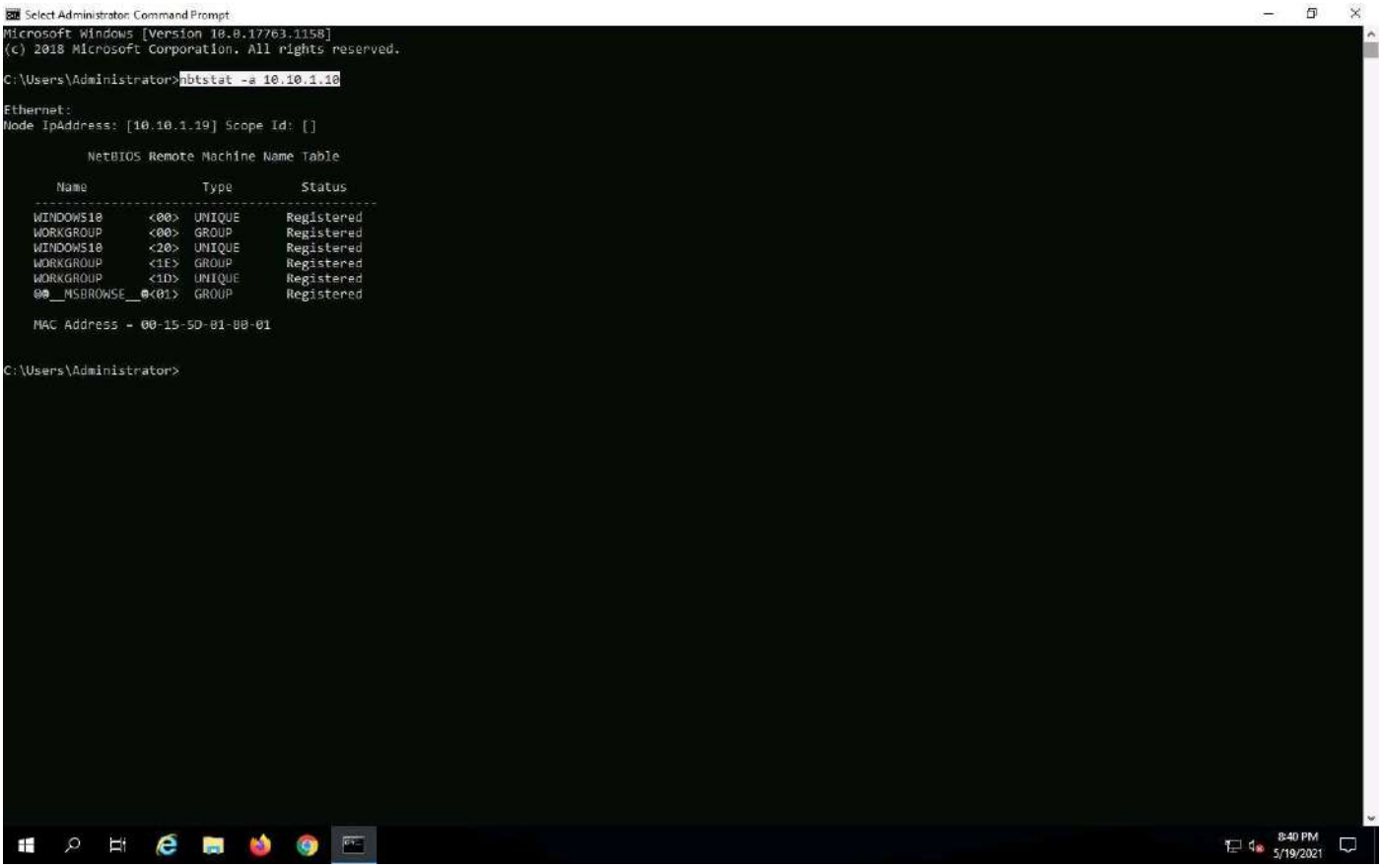
3. Open a **Command Prompt** window.



4. Type **nbtstat -a [IP address of the remote machine]** (in this example, the target IP address is **10.10.1.10**) and press **Enter**.

In this command, **-a** displays the NetBIOS name table of a remote computer.

5. The result appears, displaying the NetBIOS name table of a remote computer (in this case, the **WINDOWS10** machine), as shown in the screenshot.

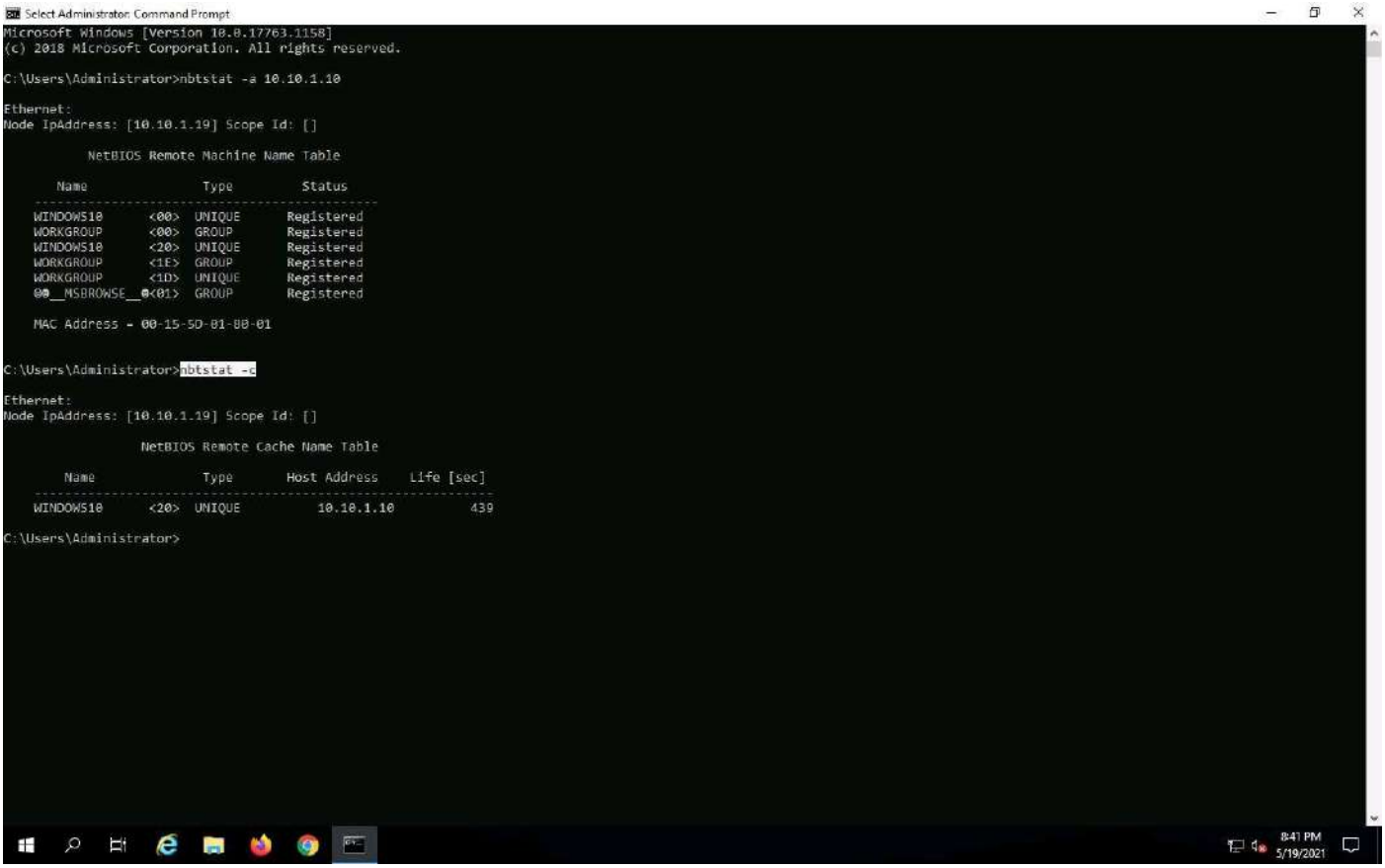


6. In the same **Command Prompt** window, type **nbtstat -c** and press **Enter**.

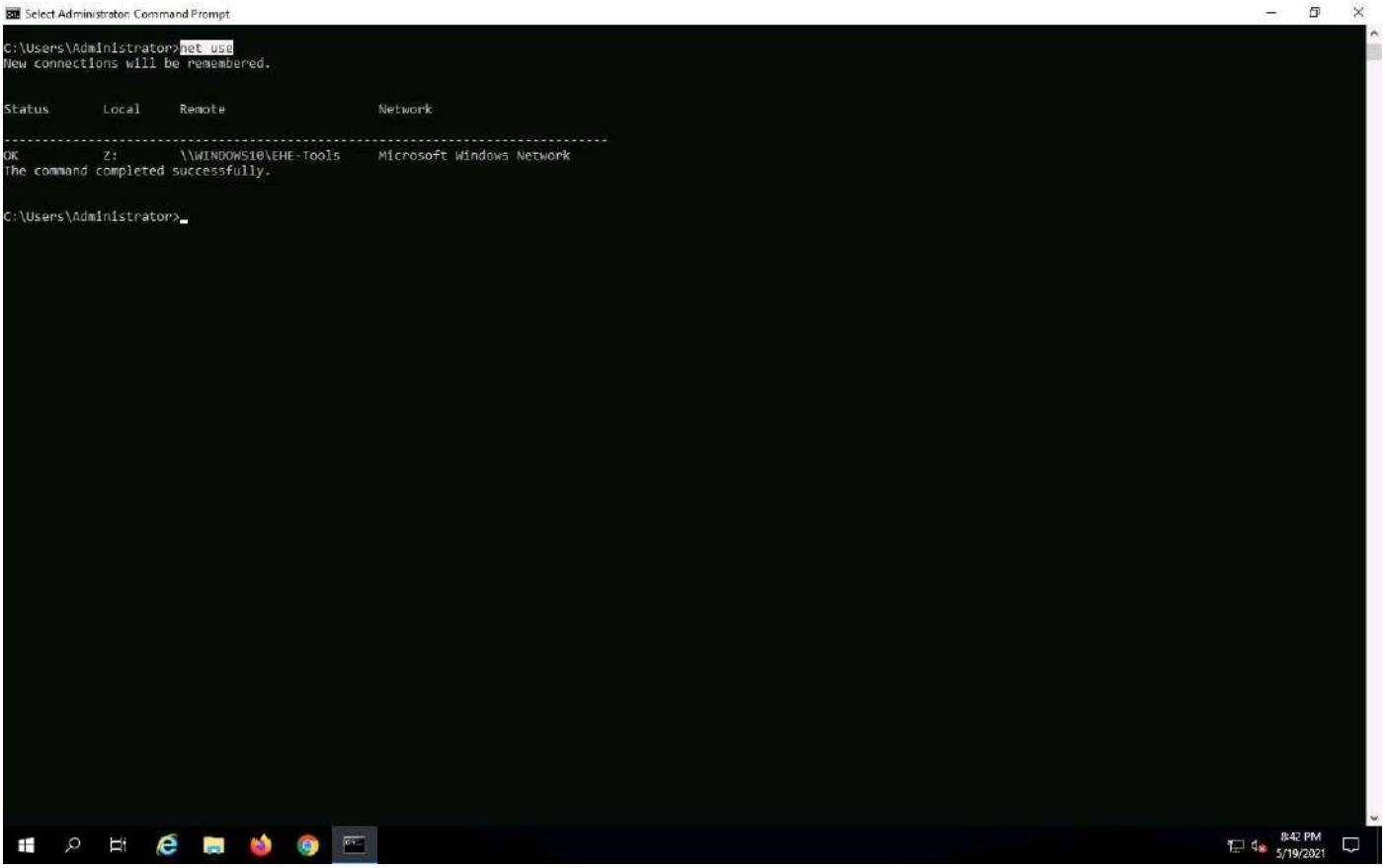
In this command, **-c** lists the contents of the NetBIOS name cache of the remote computer.

7. The result appears, displaying the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses.

It is possible to extract this information without creating a **null session** (an unauthenticated session).



8. Now, type **net use** and press **Enter**. The output displays information about the target such as connection status, shared folder/drive and network information, as shown in the screenshot.



9. This concludes the demonstration of performing NetBIOS enumeration using Windows command-line utilities such as Nbtstat and Net use.
10. Close all open windows and document all the acquired information.

Task 2: Perform NetBIOS Enumeration using NetBIOS Enumerator

NetBIOS Enumerator is a tool that enables the use of remote network support and several other techniques such as SMB (Server Message Block). It is used to enumerate details such as NetBIOS names, usernames, domain names, and MAC addresses for a given range of IP addresses.

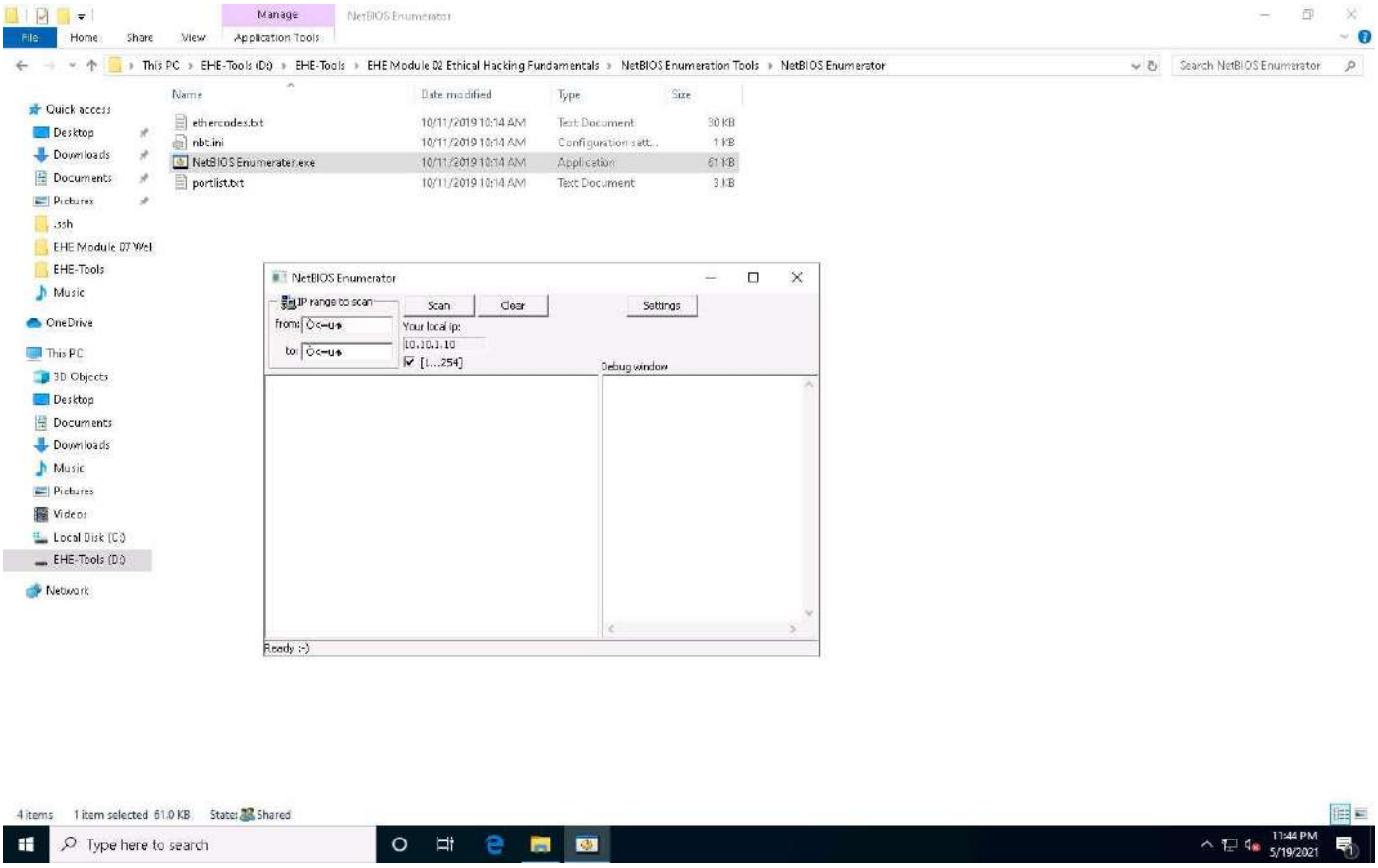
Here, we will use the NetBIOS Enumerator to perform NetBIOS enumeration on the target network.

We will use a **Windows 10** machine to target **Windows Server 2016** and **Windows Server 2019** machines.

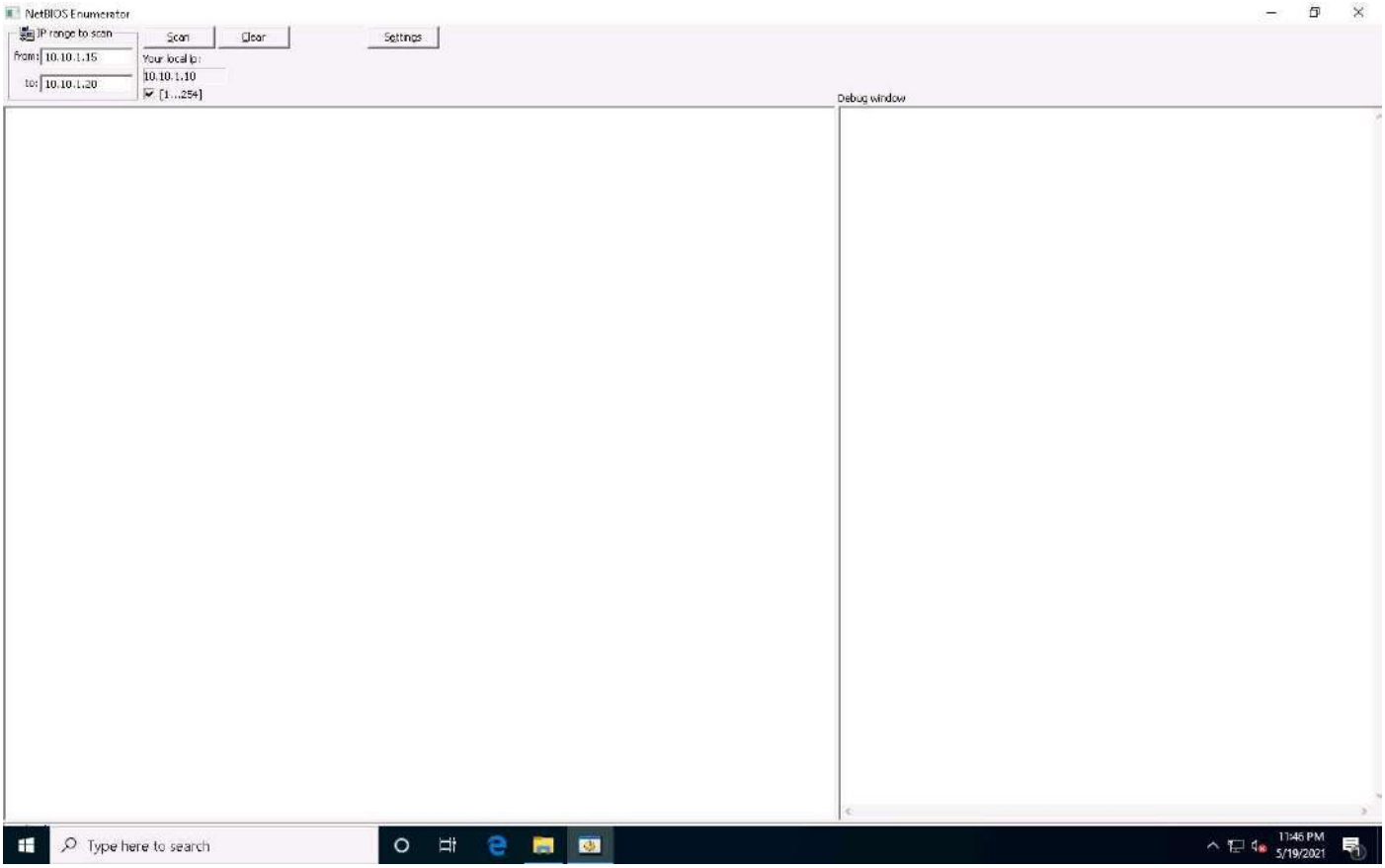
1. Click Windows 10 to switch to the **Windows 10** machine.
2. In the **Windows 10** machine, navigate to **D:\EHE-Tools\EHE Module 02 Ethical Hacking Fundamentals\NetBIOS Enumeration Tools\NetBIOS Enumerator** and double-click **NetBIOS Enumerater.exe**.

If the **Open - File Security Warning** pop-up appears, click Run.

3. The **NetBIOS Enumerator** main window appears, as shown in the screenshot.

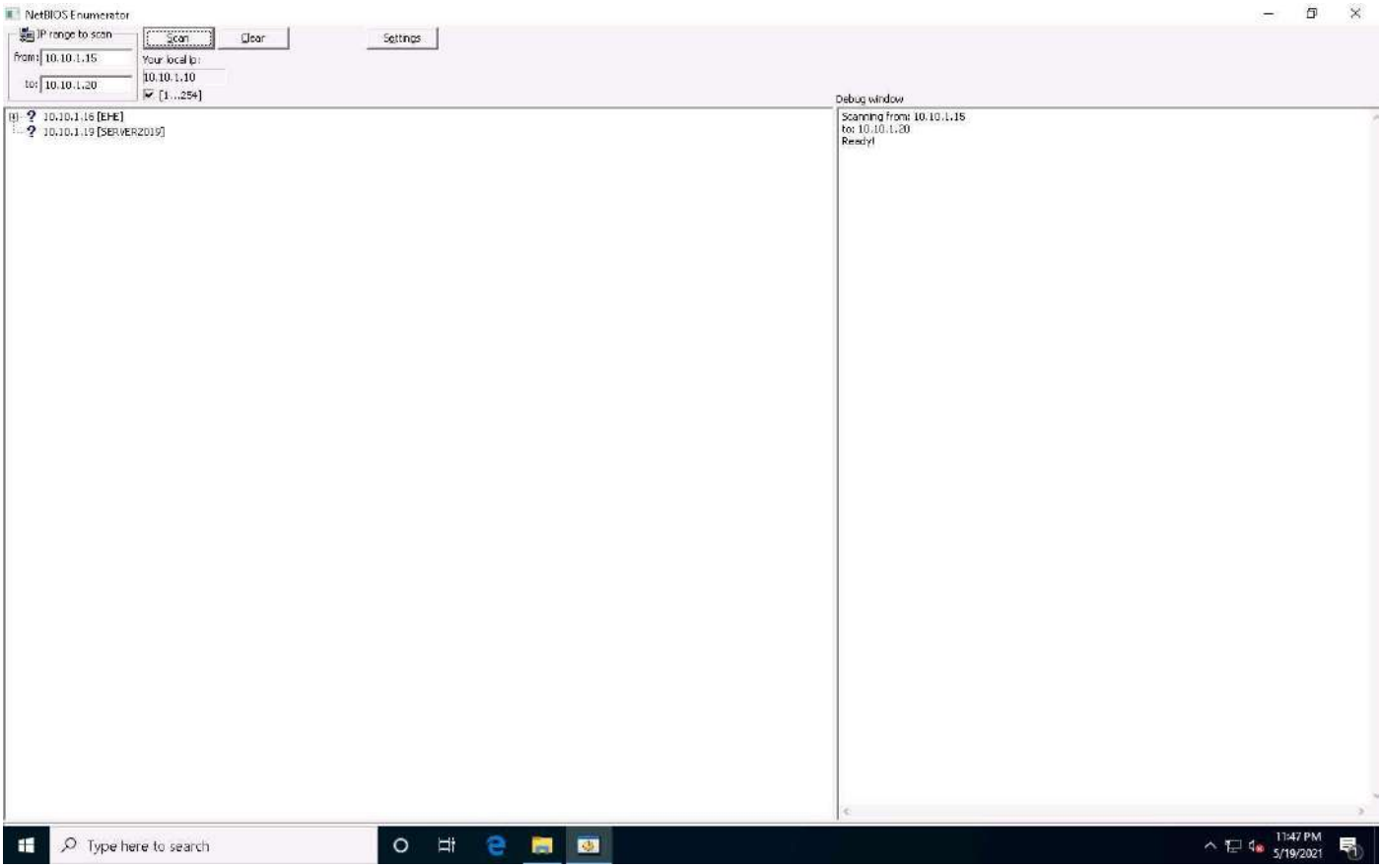


4. Under **IP range to scan**, enter an **IP range** in the **from** and **to** fields and click the **Scan** button to initiate the scan (In this example, we are targeting the IP range **10.10.1.15-10.10.1.20**).

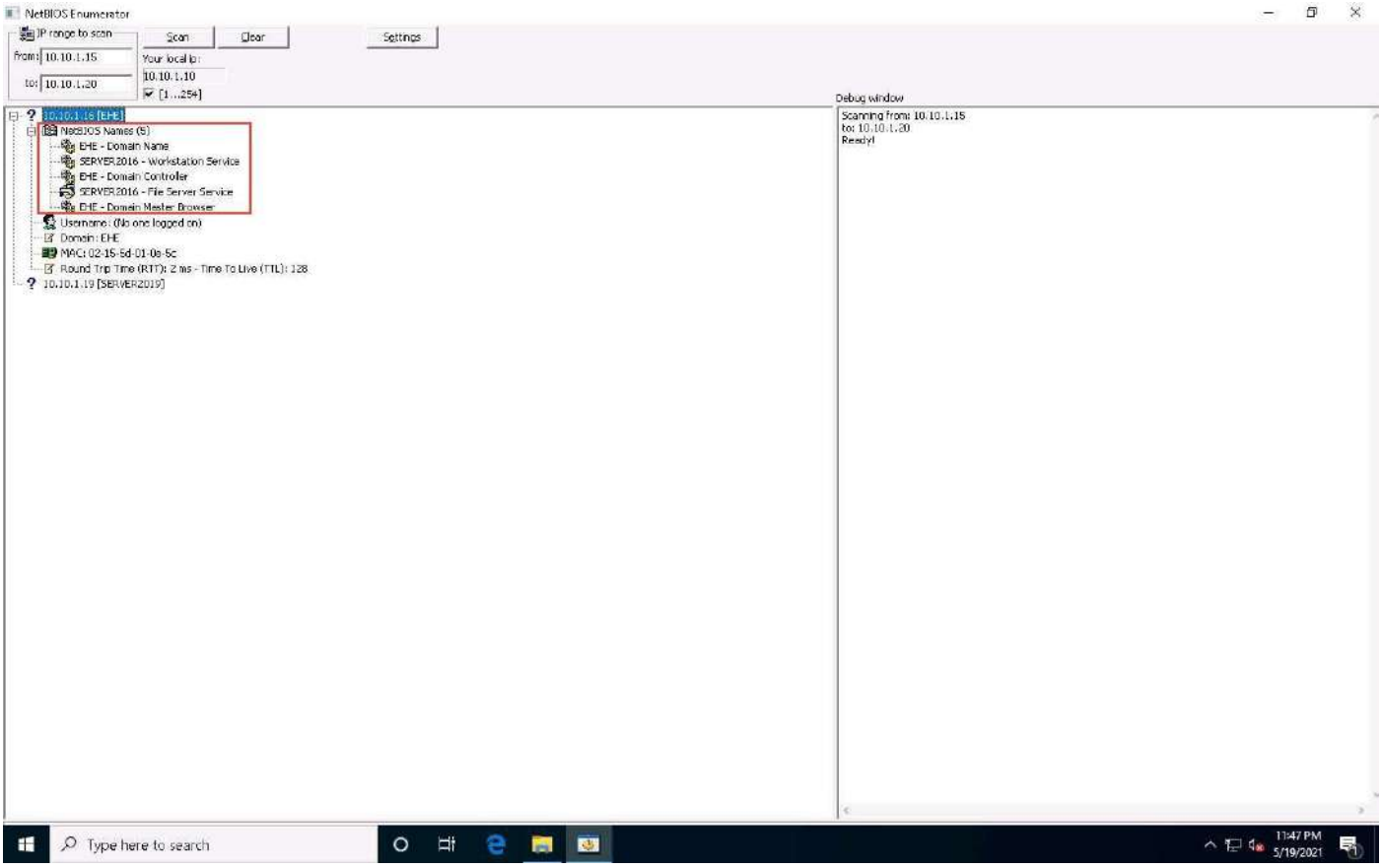


5. NetBIOS Enumerator scans for the provided IP address range. On completion, the scan results are displayed in the left pane, as shown in the screenshot.

6. The **Debug window** section in the right pane shows the scanning range of IP addresses and displays **Ready**! after the scan is finished.



7. Click on the expand icon (**+**) to the left of the **10.10.1.16** and **10.10.1.19** IP addresses in the left pane of the window. Then click on the expand icon (**+**) to the left of **NetBIOS Names** to display NetBIOS details of the target IP address, as shown in the screenshot.



8. This concludes the demonstration of performing NetBIOS enumeration using NetBIOS Enumerator. This enumerated NetBIOS information can be used to strategize an attack on the target.

9. Close all open windows and document all the acquired information.

Module 03: Information Security Threats and Vulnerability Assessment

Scenario

A threat is a potential occurrence of an undesirable event that can eventually damage and disrupt the operational and functional activities of an organization. Threat can be any type of entity or action performed on physical or intangible asset that can disrupt the security. The existence of threats may be accidental, intentional, or due to the impact of some other action. Attackers use cyber threats to infiltrate and steal data such as individual's personal information, financial information, and login credentials. They can also use the compromised system to perform malicious activities and launch further attacks. The criticality of a threat is based on how much damage it will cause, or how uncontrollable it is, or how complicated it is to identify the latest discovered threat incident in advance. Threats to data assets cause loss of confidentiality, integrity, or availability (CIA) of data. They also result in data loss, identity theft, cyber sabotage, and information disclosure.

The lab activities in this module provide first-hand experience with various techniques that attackers use to write and propagate malware. You will also learn how to effectively perform vulnerability assessment to determine security vulnerabilities in the target system or network.

Objective

The objective of the lab is to create malware and perform other tasks that include, but are not limited to:

- Create a Trojan and exploit a target machine
- Create a virus to infect the target machine
- Perform vulnerability assessment to identify security vulnerabilities in the target system or network

Overview of Threats

Following are various sources from which threats originate and can be broadly classified as natural threats, unintentional threats, and intentional threats.

- **Natural Threats**: Natural factors such as fires, floods, power failures, lightning, meteor, and earthquakes are potential threats to the assets of an organization. For example, these may cause severe physical damage to computer systems.
- **Unintentional Threats**: Unintentional threats are threats that exist due to the potential for unintentional errors occurring within the organization. Examples include insider-originating security breaches, negligence, operator errors, unskilled administrators, lazy or untrained employees, and accidents.
    - **Intentional Threats**: There are two sources of intentional threats.
    - **Internal Threats**: Most computer and Internet-related crimes are insiders or internal attacks. These threats are performed by insiders within the organization such as disgruntled or negligent employees and harm the organization intentionally or unintentionally. Most of these attacks are performed by privileged users of the network.
    - **External Threats**: External attacks are performed by exploiting vulnerabilities that already exist in the network, without the assistance of insider employees. Therefore, the potential to perform an external attack depends on the severity of the identified network weaknesses.

Lab Tasks

Ensure that the **Windows Defender Firewall is Turn off** on the machines you are using for the lab tasks in this module, as it blocks and deletes malware as soon as it is executed.

We can use numerous tools and techniques to gain access to the target network or machine. Recommended labs that will assist you in learning various malware attack and vulnerability assessment techniques include:

1. Create a Trojan to gain access to the target system
    - Create a Trojan server using Theef RAT trojan
    - Gain control over a victim machine using the njRAT RAT Trojan

2. Create a virus to infect the target system
    - Create a virus using the JPS Virus Maker Tool and infect the target system
3. Perform vulnerability assessment to identify security vulnerabilities in the target system or network
    - Perform vulnerability analysis using OpenVAS

Lab 3-1: Create a Trojan to Gain Access to the Target System

Lab Scenario

A Trojan is wrapped within or attached to a legitimate program, meaning that the program may have functionality that is not apparent to the user. Furthermore, attackers use victims as unwitting intermediaries to attack others. They can use a victim's computer to commit illegal DoS attacks.

A compromised system can affect other systems on the network. Systems that transmit authentication credentials such as passwords over shared networks in clear text or a trivially encrypted form are particularly vulnerable. If an intruder compromises a system on such a network, he or she may be able to record usernames and passwords or other sensitive information.

Additionally, a Trojan, depending on the actions it performs, may falsely implicate a remote system as the source of an attack by spoofing, thereby causing the remote system to incur a liability. Trojans enter the system by means such as email attachments, downloads, and instant messages.

The lab tasks in this exercise demonstrate how easily hackers can gain access to the target systems in the organization and create a covert communication channel for transferring sensitive data between the victim computer and the attacker.

Lab Objectives

- Create a Trojan Server using Theef RAT Trojan
- Gain Control over a Victim Machine using the njRAT RAT Trojan

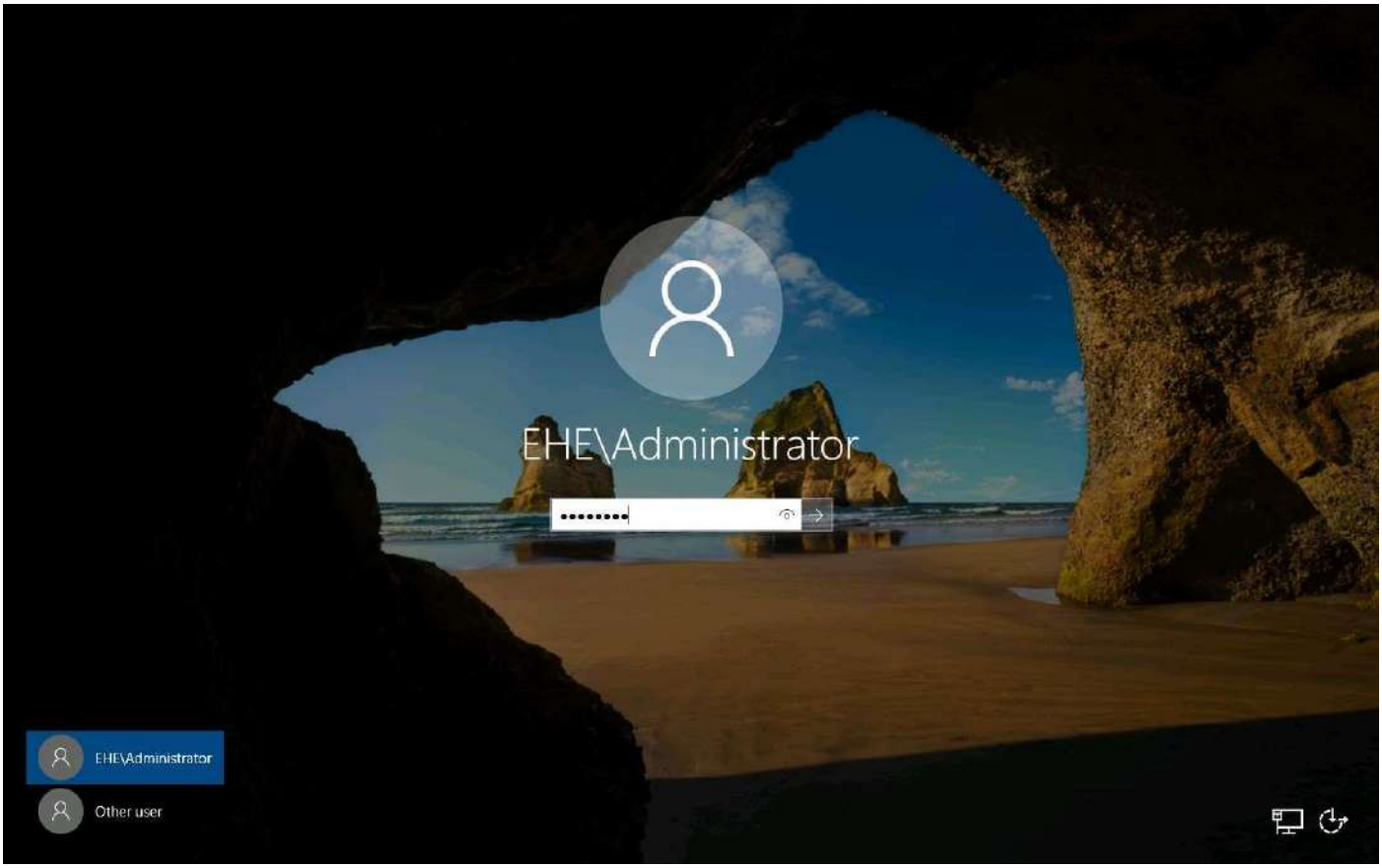
Task 1: Create a Trojan Server using Theef RAT Trojan

Attackers use Remote Access Trojans (RATs) to infect the target machine to gain administrative access. RATs help an attacker to remotely access the complete GUI and control the victim's computer without his/her awareness. They can perform screening and camera capture, code execution, keylogging, file access, password sniffing, registry management, and other tasks. The virus infects victims via phishing attacks and drive-by downloads and propagates through infected USB keys or networked drives. It can download and execute additional malware, execute shell commands, read and write registry keys, capture screenshots, log keystrokes, and spy on webcams.

Theef is a Remote Access Trojan written in Delphi. It allows remote attackers access to the system via port 9871. Theef is a Windows-based application for both client and server. The Theef server is a virus that you install on a target computer, and the Theef client is what you then use to control the virus.

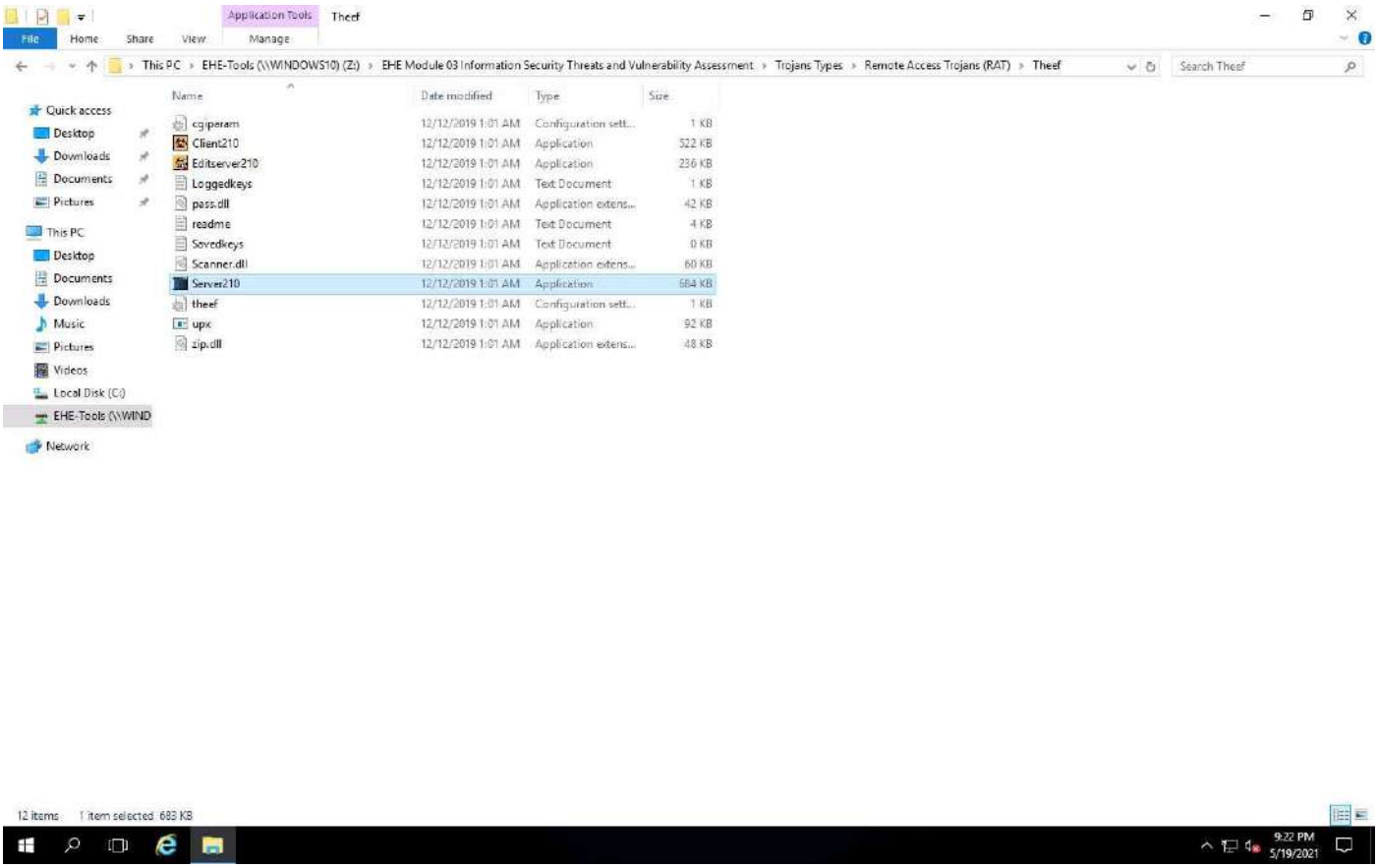
The versions of the created client or host, and the appearance of its website, may differ from that of this lab. However, the actual process of creating the server and the client is the same.

1. Generally, an attacker might send a server executable to the victim machine and entice the victim into running it. In this lab, for demonstration purposes, we are directly executing the file on the victim machine, **Windows Server 2016**.
2. Click Windows Server 2016 to switch to the **Windows Server 2016** machine. Click Ctrl+Alt+Delete to activate the machine, by default, **EHE\Administrator** account is selected, click Pa$$w0rd to enter the password and press **Enter**.



3. Navigate to **Z:\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\Theef** and double-click **Server210.exe** to run the Trojan on the victim machine.

If an **Open File - Security** Warning pop-up appears, click **Run**.



4. Now, click Windows 10 to switch to the **Windows 10** machine (as an attacker) click Ctrl+Alt+Delete.

Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 10** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under Commands (**thunder** icon) menu.

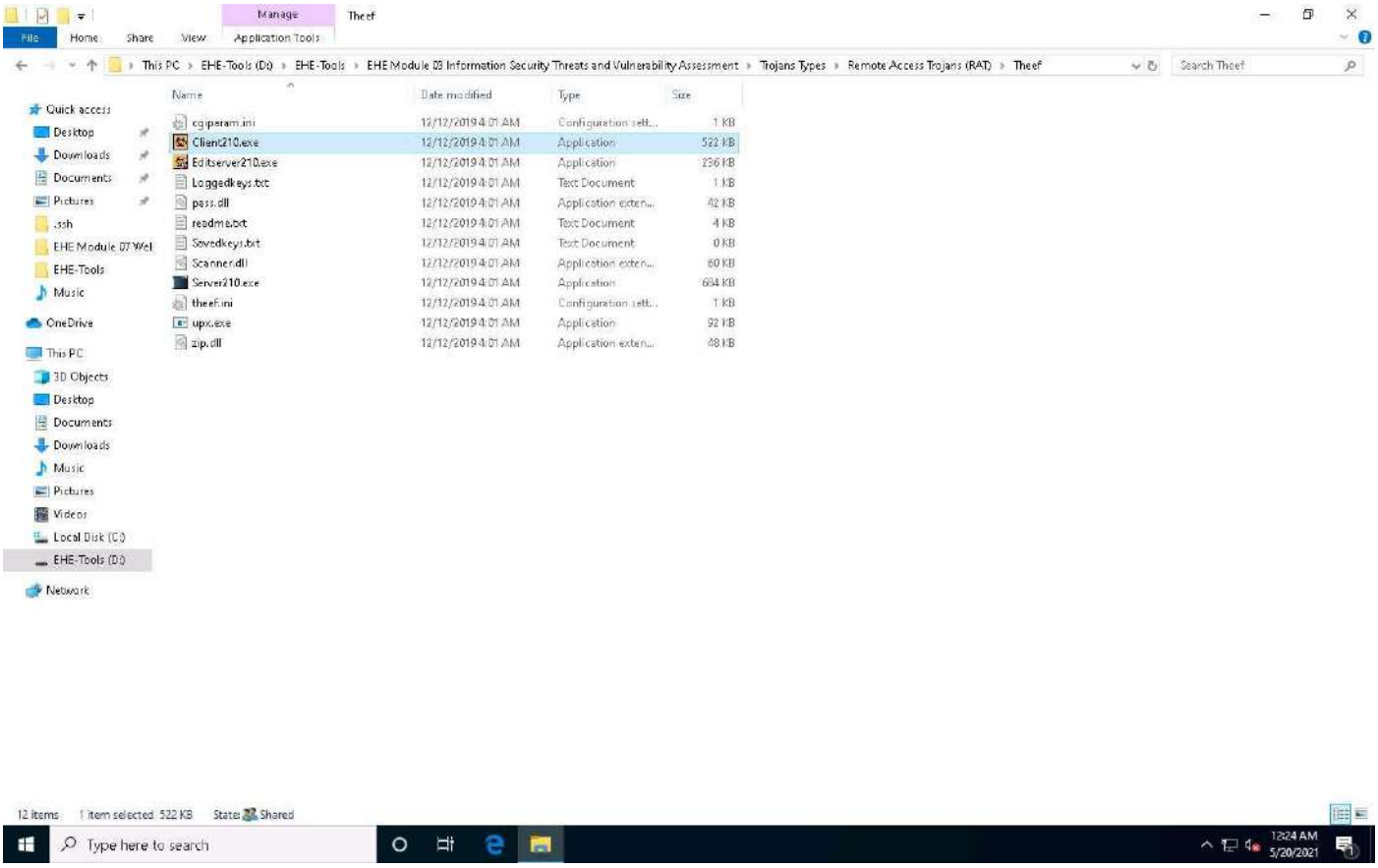
5. By default, **Admin** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.

Alternatively, you can also click **Pa$$w0rd** under **Windows 10** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

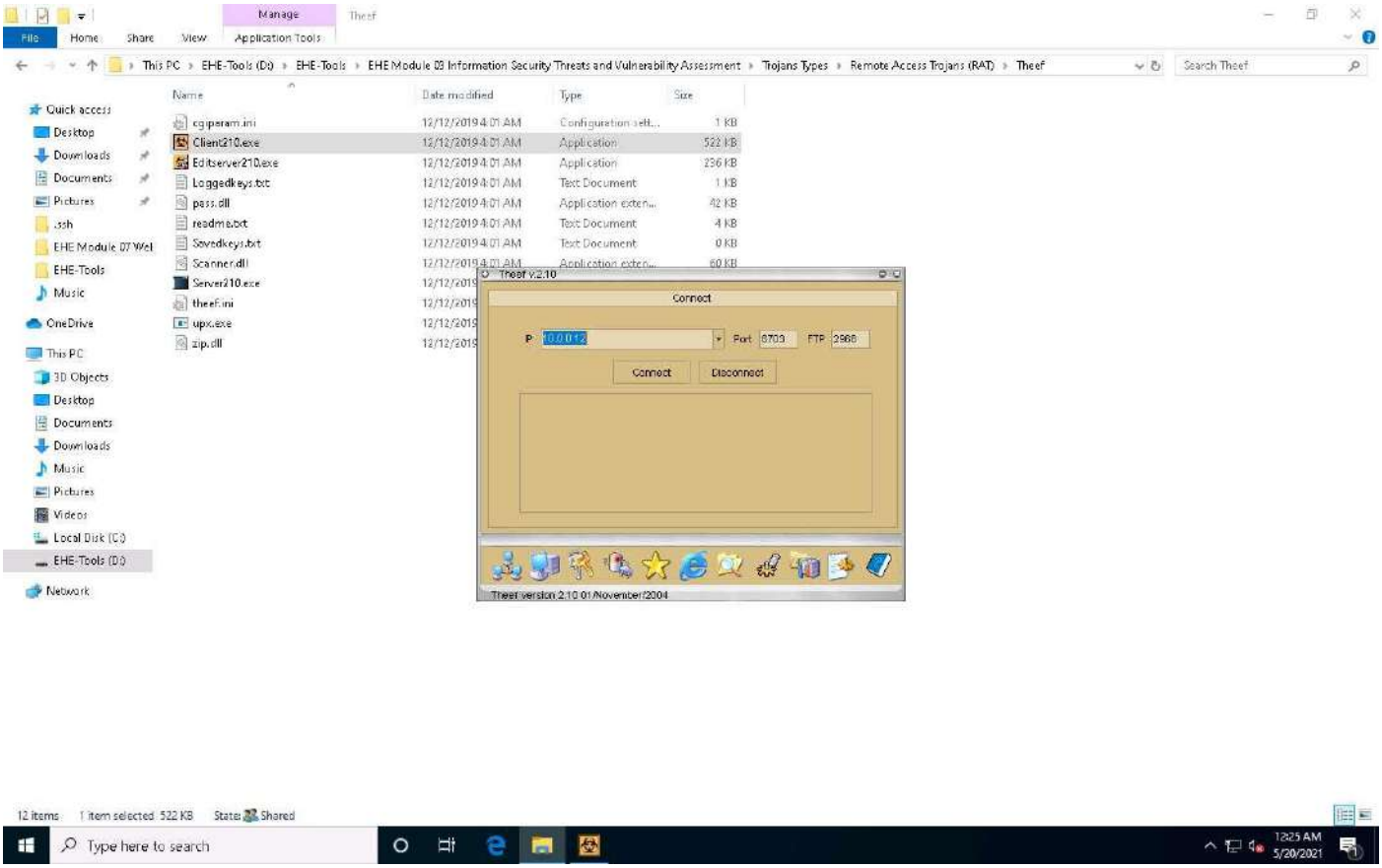
If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

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

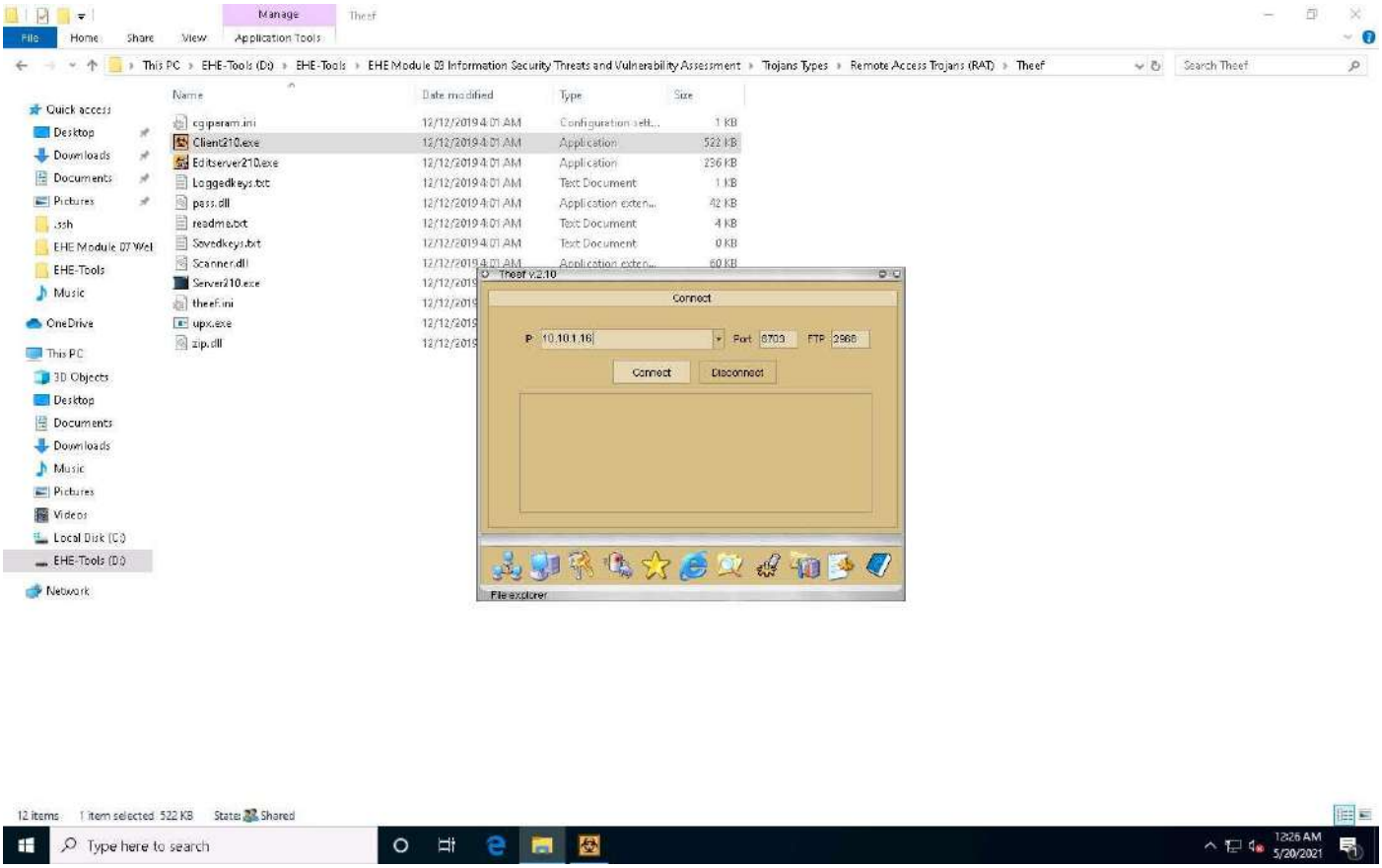
6. Navigate to **D:\EHE-Tools\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\Theef** and double-click **Client210.exe** to access the victim machine remotely.



7. The **Theef** main window appears, as shown in the screenshot.

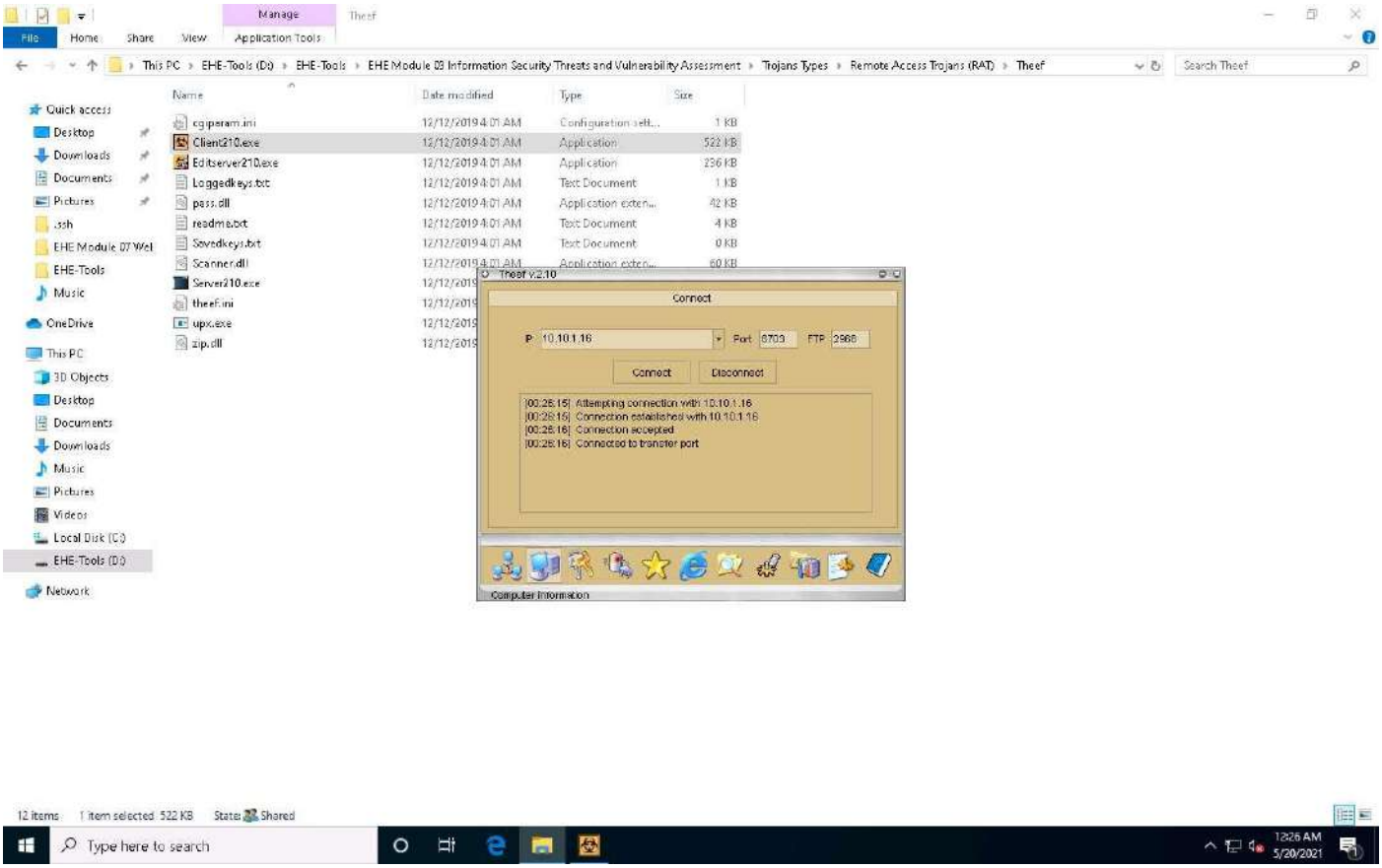


8. Enter the IP address of the target machine (here, **Windows Server 2016**) in the **IP** field (**10.10.1.16**), and leave the **Port** and **FTP** fields set to default; click **Connect**.



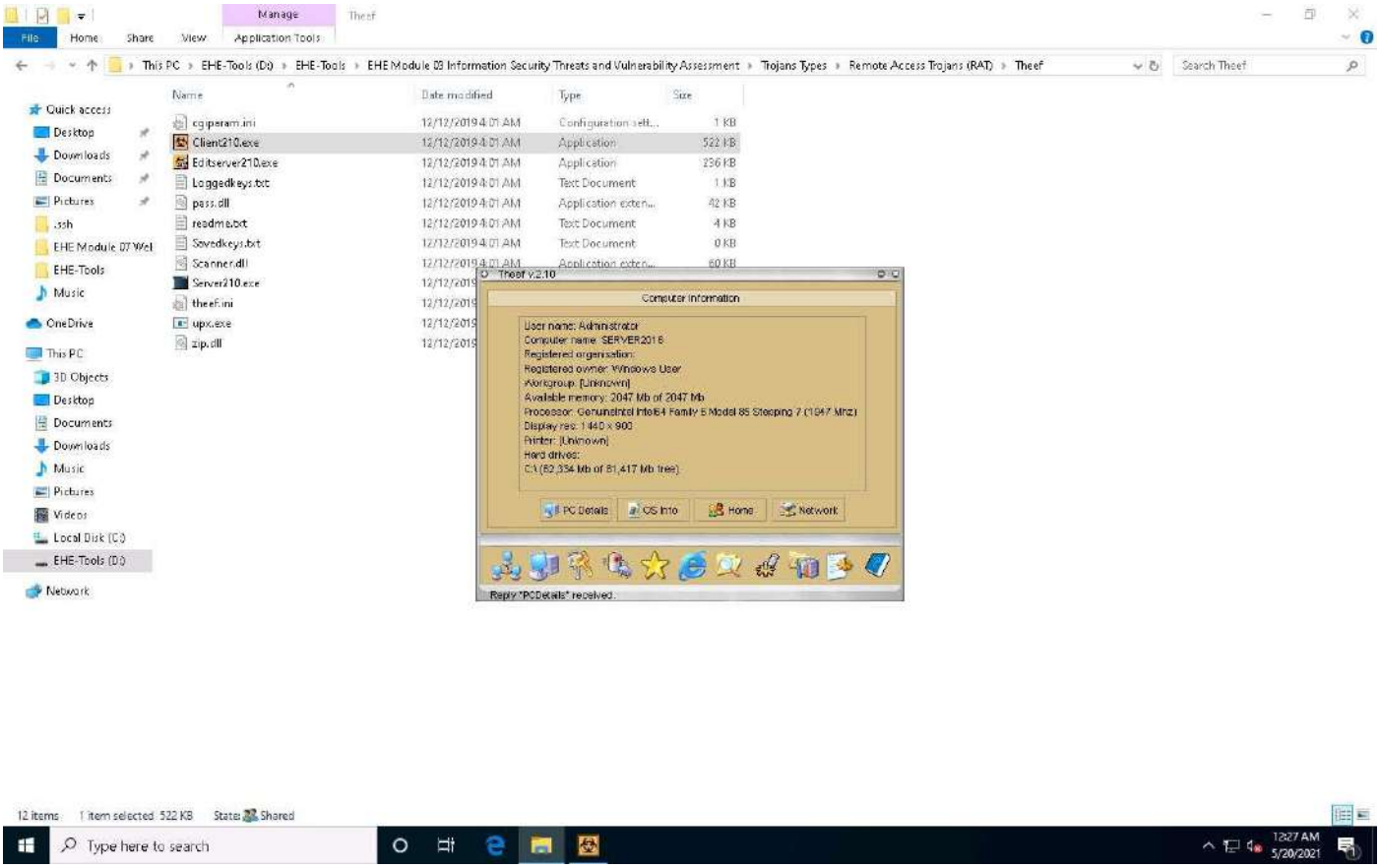
9. Now, from **Windows 10**, you have successfully established a remote connection with the **Windows Server 2016** machine.

10. To view the computer's information, click the **Computer Information** icon from the lower part of the window.

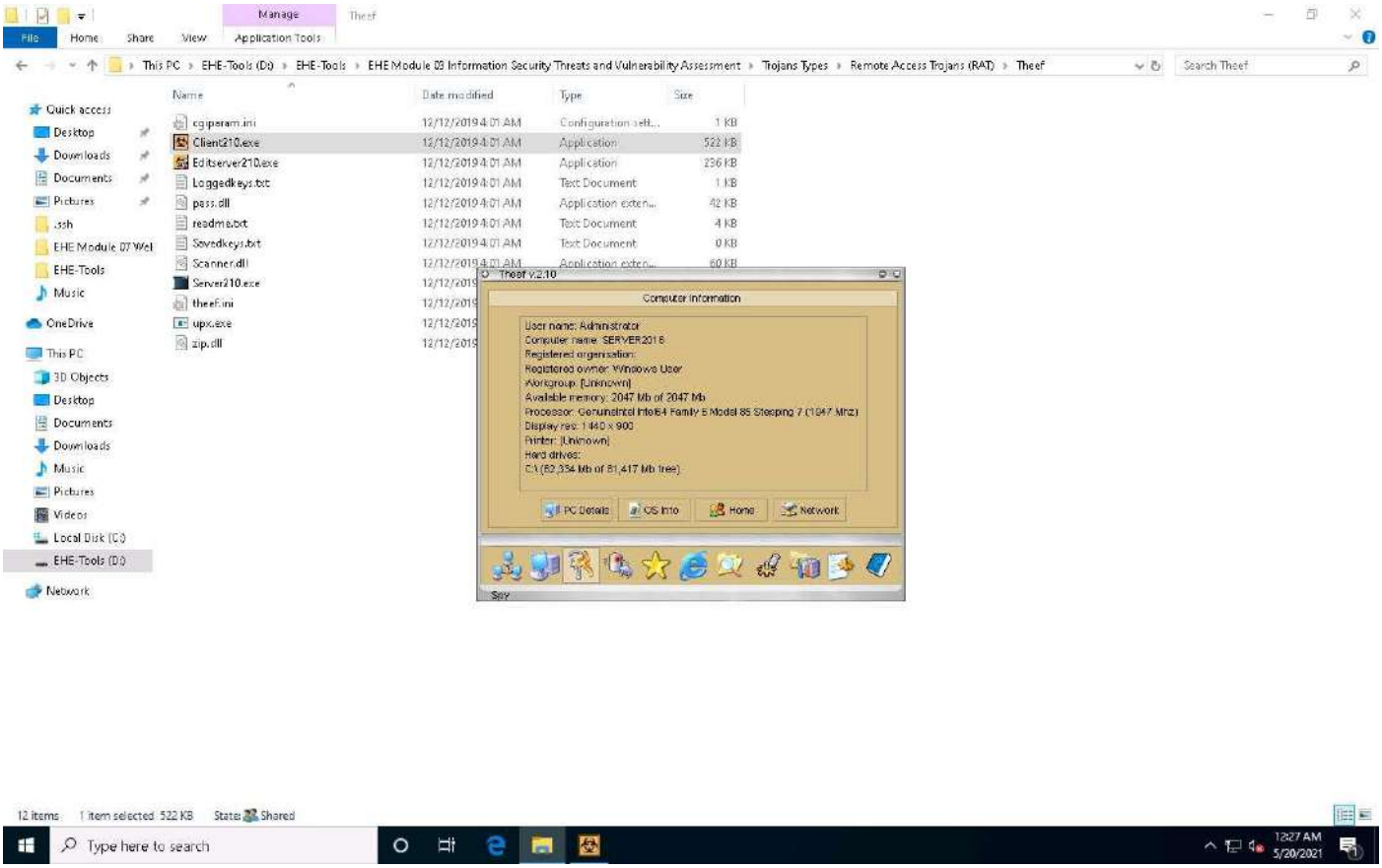


11. In **Computer Information**, you can view **PC Details**, **OS Info**, **Home**, and **Network** by clicking their respective buttons.

12. Here, for example, selecting **PC Details** reveals computer-related information.

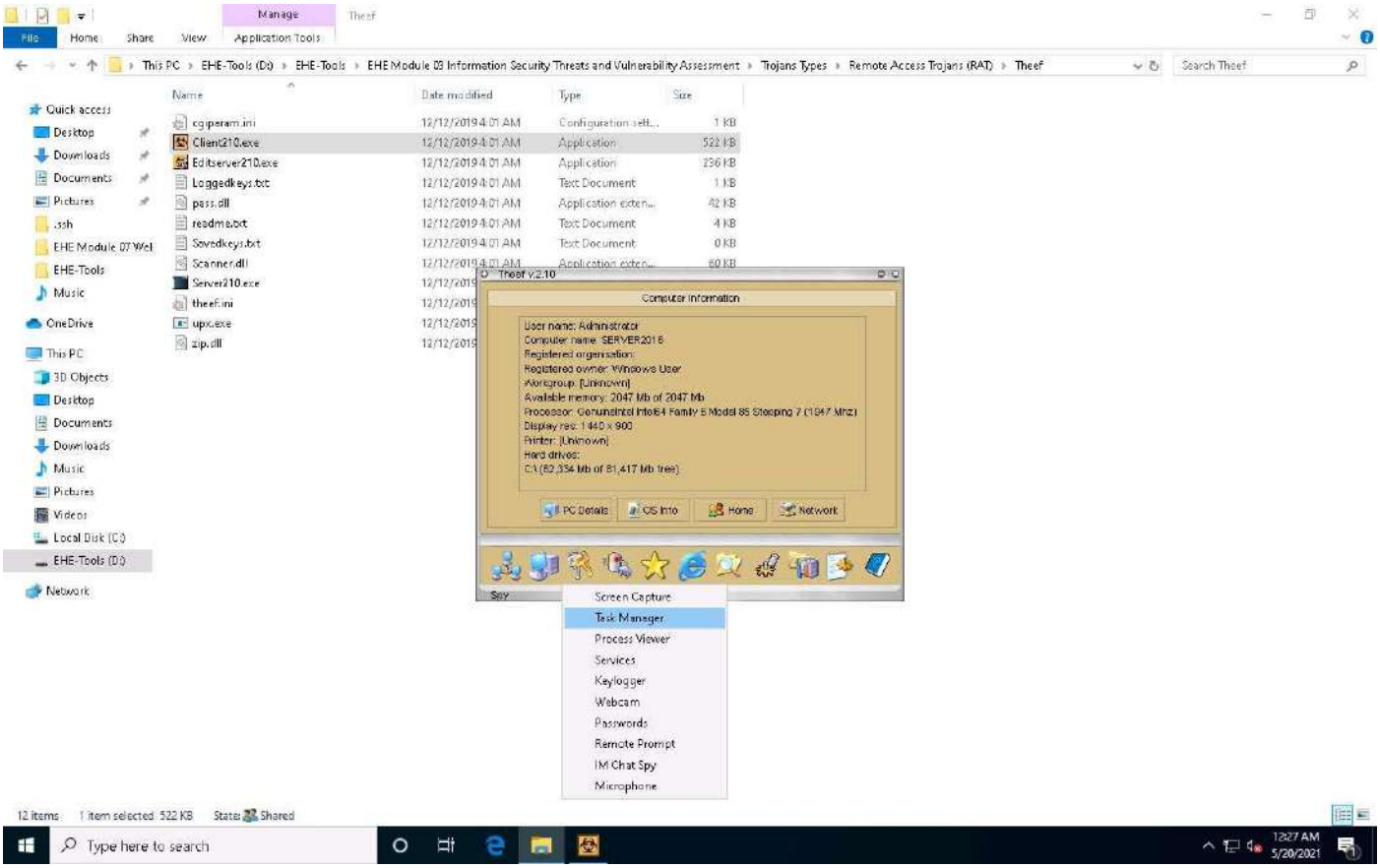


13. Click the **Spy** icon to perform various operations on the target machine.

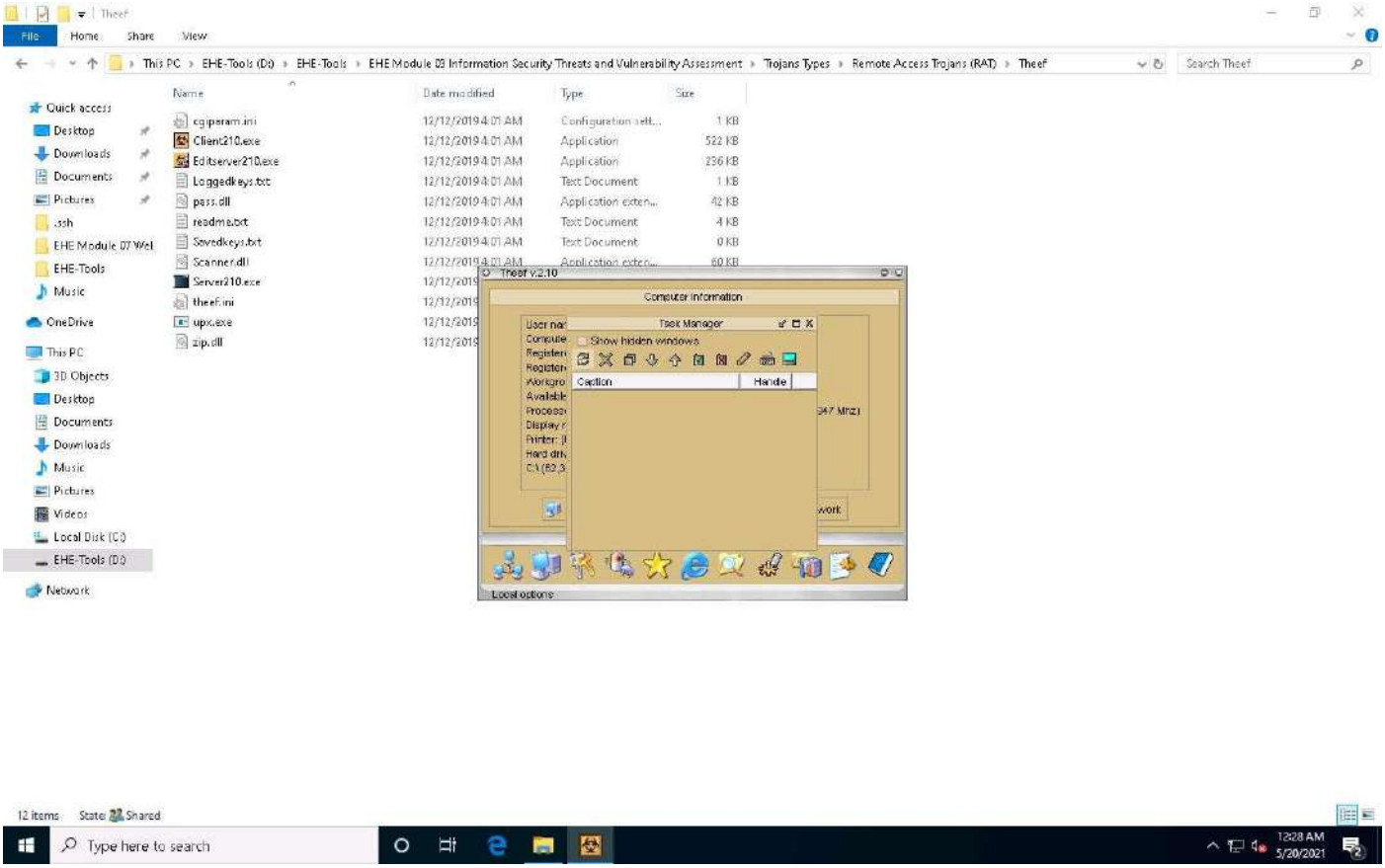


14. You can perform various operations such as capture screens, log keys, view processes, view the task manager, use the webcam, and use the microphone on the victim machine by selecting their respective options.

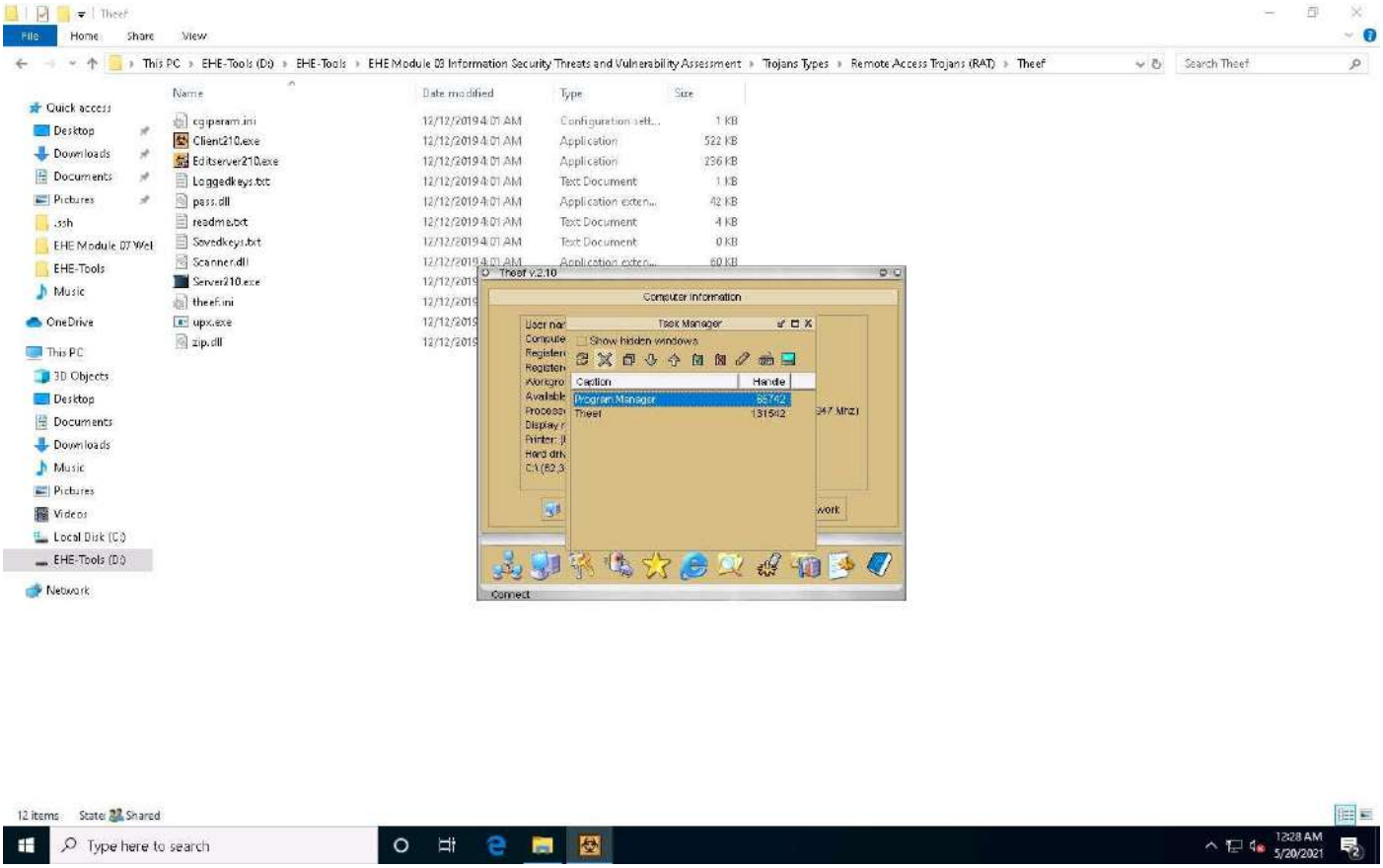
15. Here, for instance, selecting **Task Manager** views the tasks running on the target machine.



16. In the **Task Manager** window, click **Refresh** icon to obtain the list of running processes.



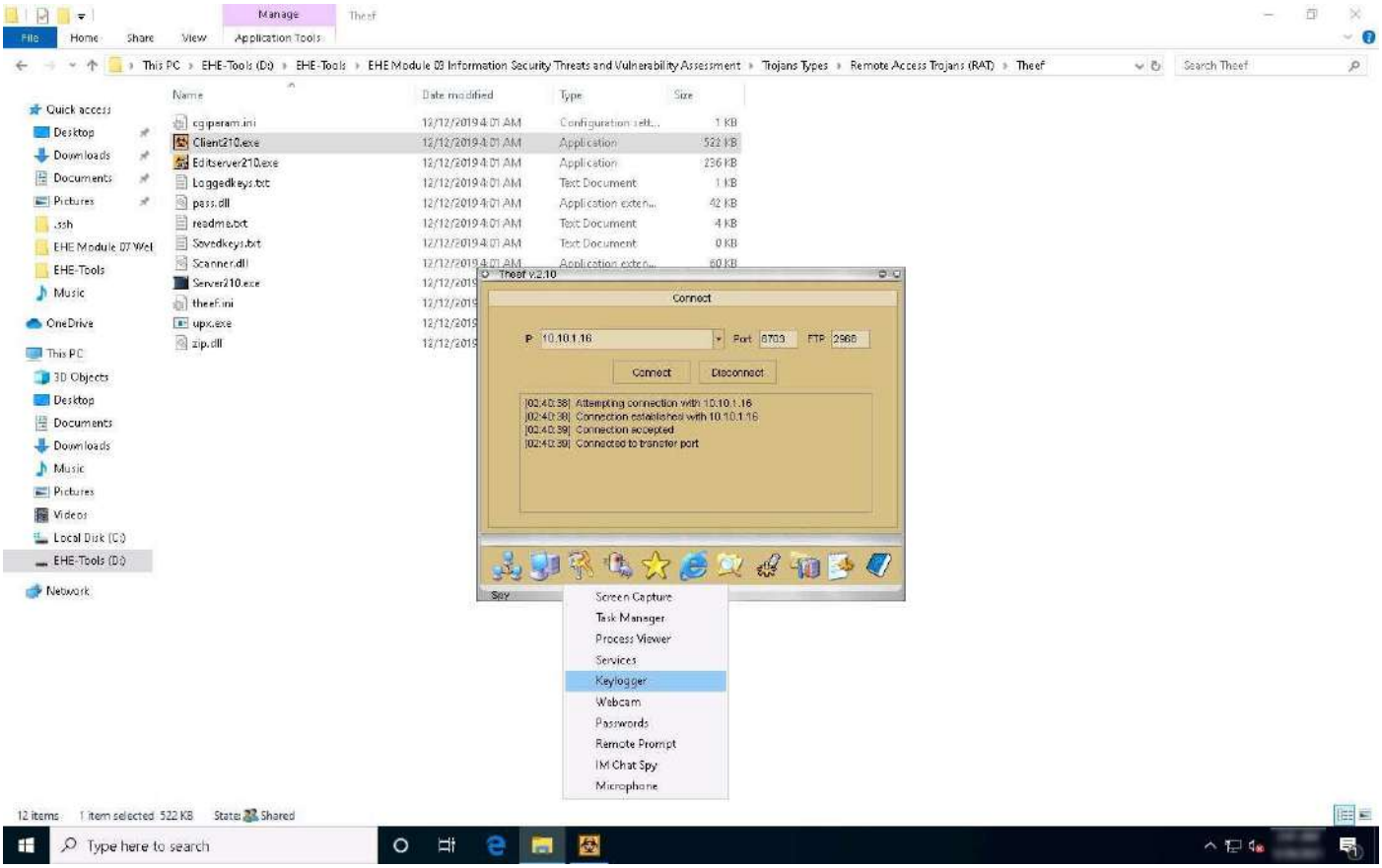
17. Select a process (task); click the **Close window** icon to end the task on the target machine.



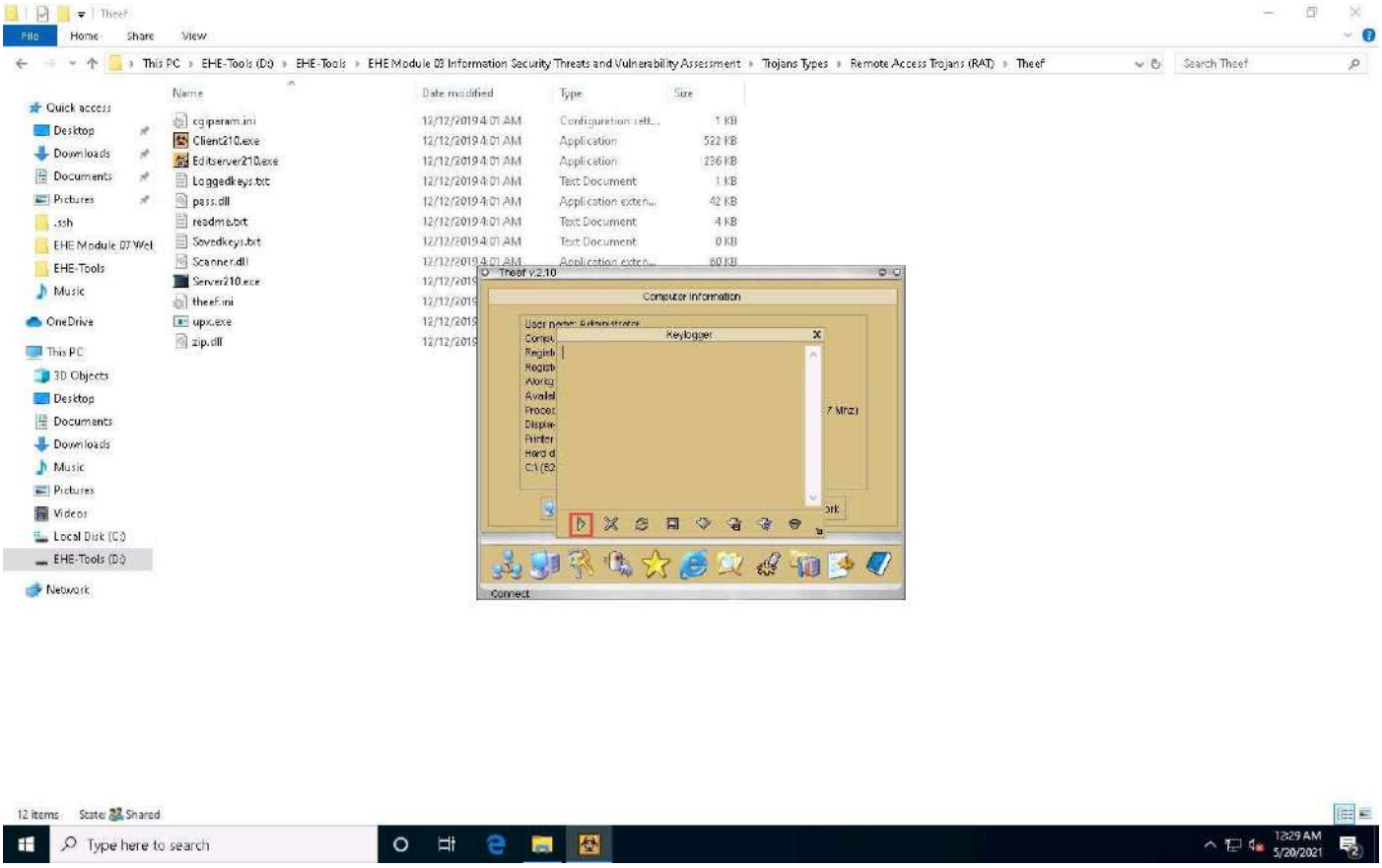
18. Close the **Task Manager** window.

The tasks running in the task manager may vary in your lab environment.

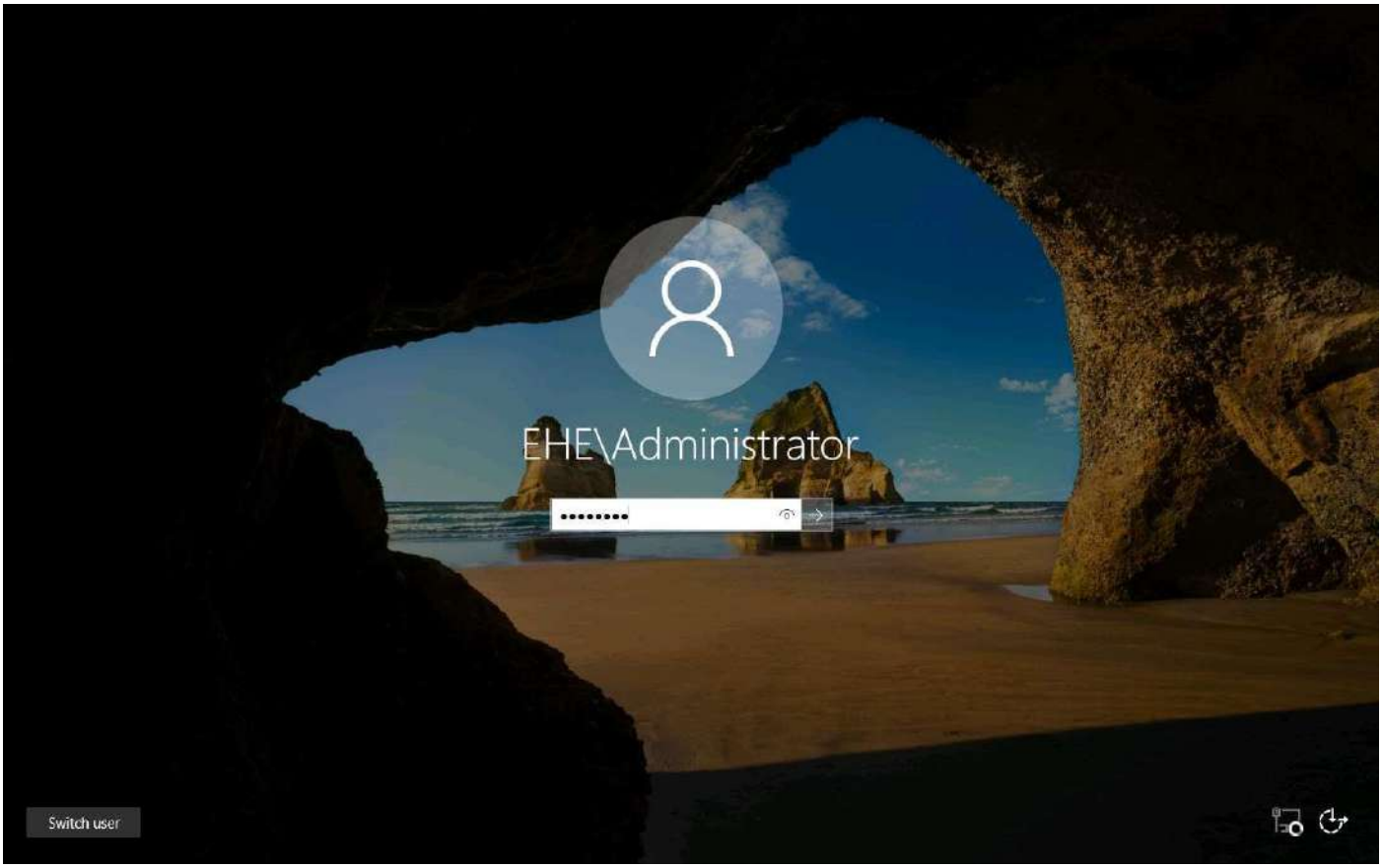
19. From the **Spy** menu, click **Keylogger** to record the keystrokes made on the victim machine.



20. The **Keylogger** pop-up appears; click the **Start** icon to read the keystrokes of the victim machine.

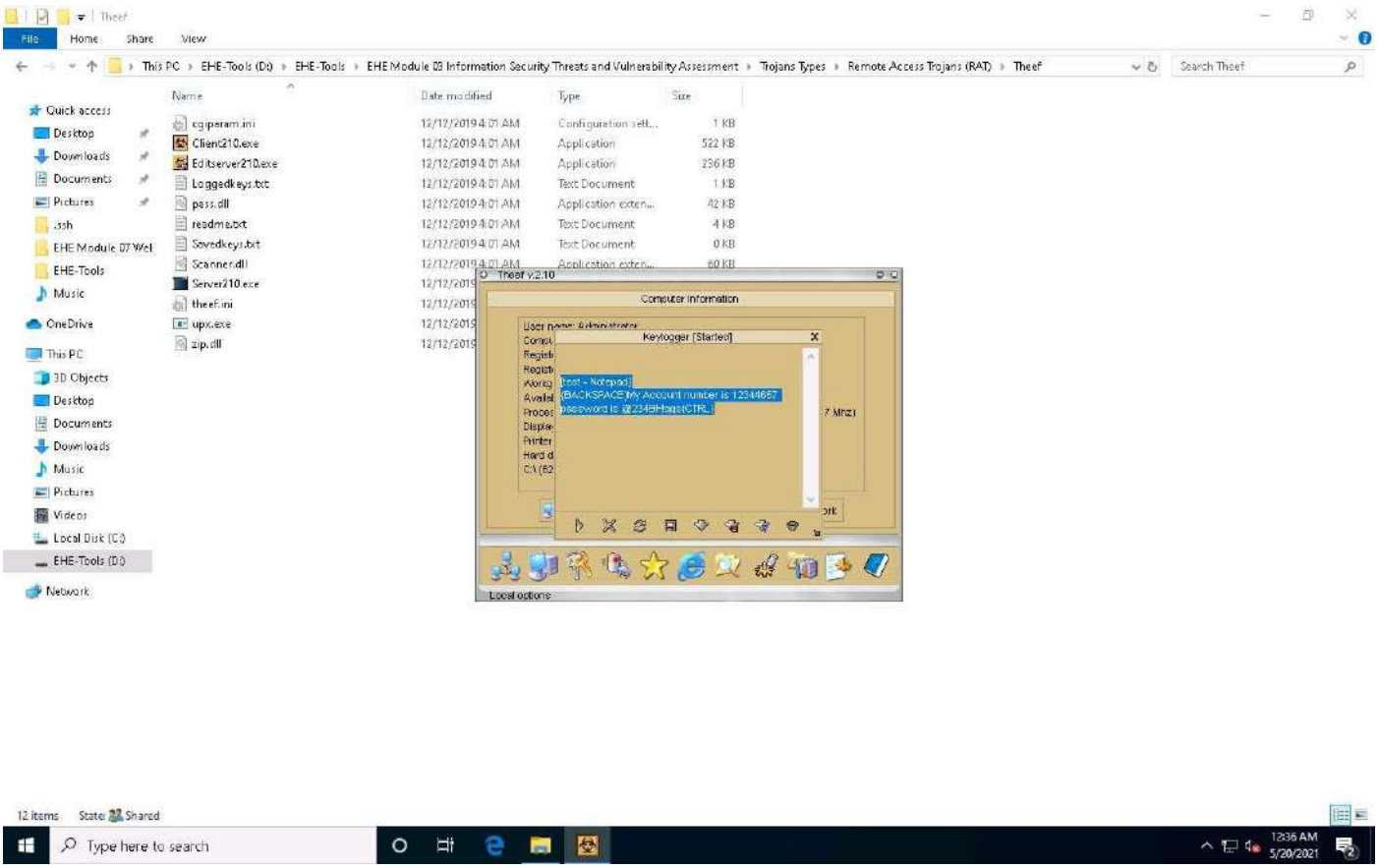


21. Click Windows Server 2016 to switch to the **Windows Server 2016** machine. Click Ctrl+Alt+Delete to activate the machine, by default, **EHE\Administrator** account is selected, click Pa$$w0rd to enter the password and press **Enter**.



22. Open a browser window and browse some websites or open a text document and type some sensitive information.

23. Click Windows 10 to switch back to the attacker machine (**Windows 10**) to view the recorded keystrokes of the victim machine in the **Theef** Keylogger window.



24. Close the Theef **Keylogger** window.

25. Similarly, you can access the details of the victim machine by clicking on the various icons.
26. Close all open windows on both the **Windows 10** and **Windows Server 2016** machines.

Task 2: Gain Control over a Victim Machine using the njRAT RAT Trojan

njRAT is a RAT with powerful data-stealing capabilities. In addition to logging keystrokes, it is capable of accessing a victim's camera, stealing credentials stored in browsers, uploading and downloading files, performing process and file manipulations, and viewing the victim's desktop.

This RAT can be used to control Botnets (networks of computers), allowing the attacker to update, uninstall, disconnect, restart, and close the RAT, and rename its campaign ID. The attacker can further create and configure the malware to spread through USB drives with the help of the Command and Control server software.

Here, we will use the njRAT Trojan to gain control over a victim machine.

The versions of the created client or host and appearance of the website may differ from what it is in this lab. However, the actual process of creating the server and the client is the same, as shown in this lab.

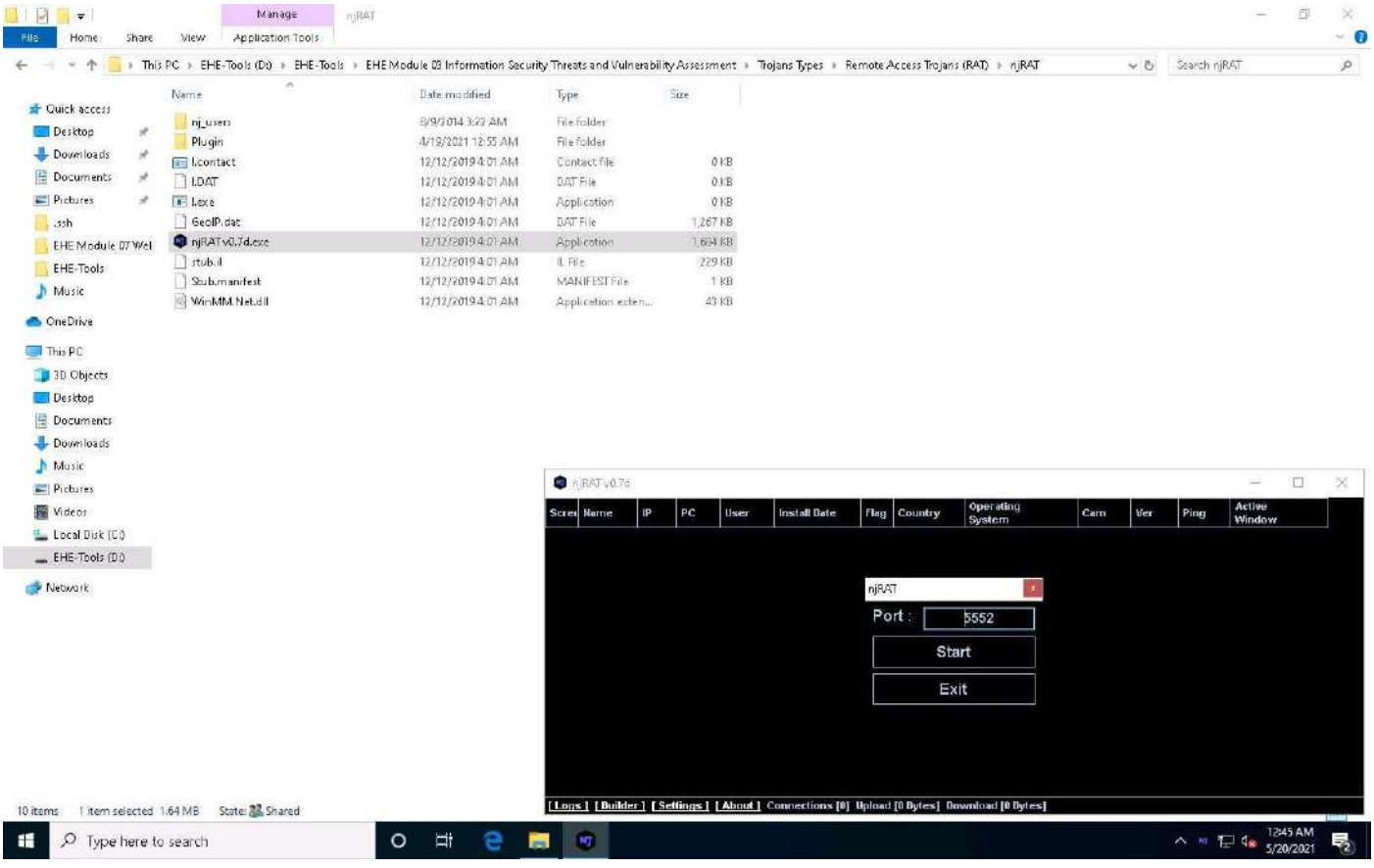
In this lab task, we will use the **Windows 10** (**10.10.1.10**) machine as the attacker machine and the **Windows Server 2016** (**10.10.1.16**) machine as the victim machine.

1. In the **Windows 10**, navigate to **D:\EHE-Tools\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\njRAT** and double-click **njRAT v0.7d.exe**.

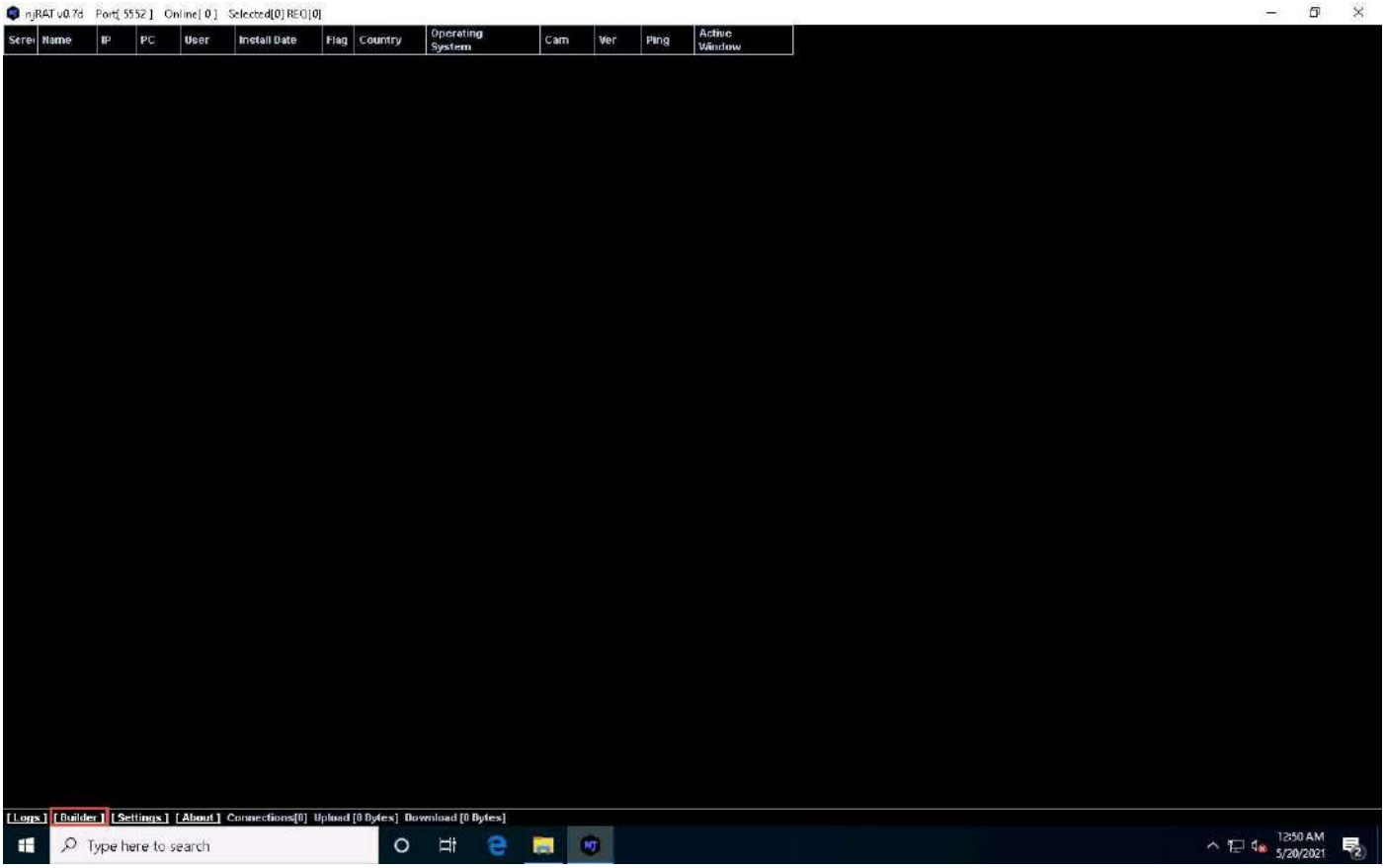
If a **User Account Control** window appears, click **Yes**.

If an **Open File - Security Warning** pop-up appears, click **Run**.

2. The **njRAT GUI** appears along with an njRAT pop-up, where you need to specify the port you want to use to interact with the victim machine. Enter the port number and click **Start**.
3. In this lab, the default port number **5552** has been chosen.

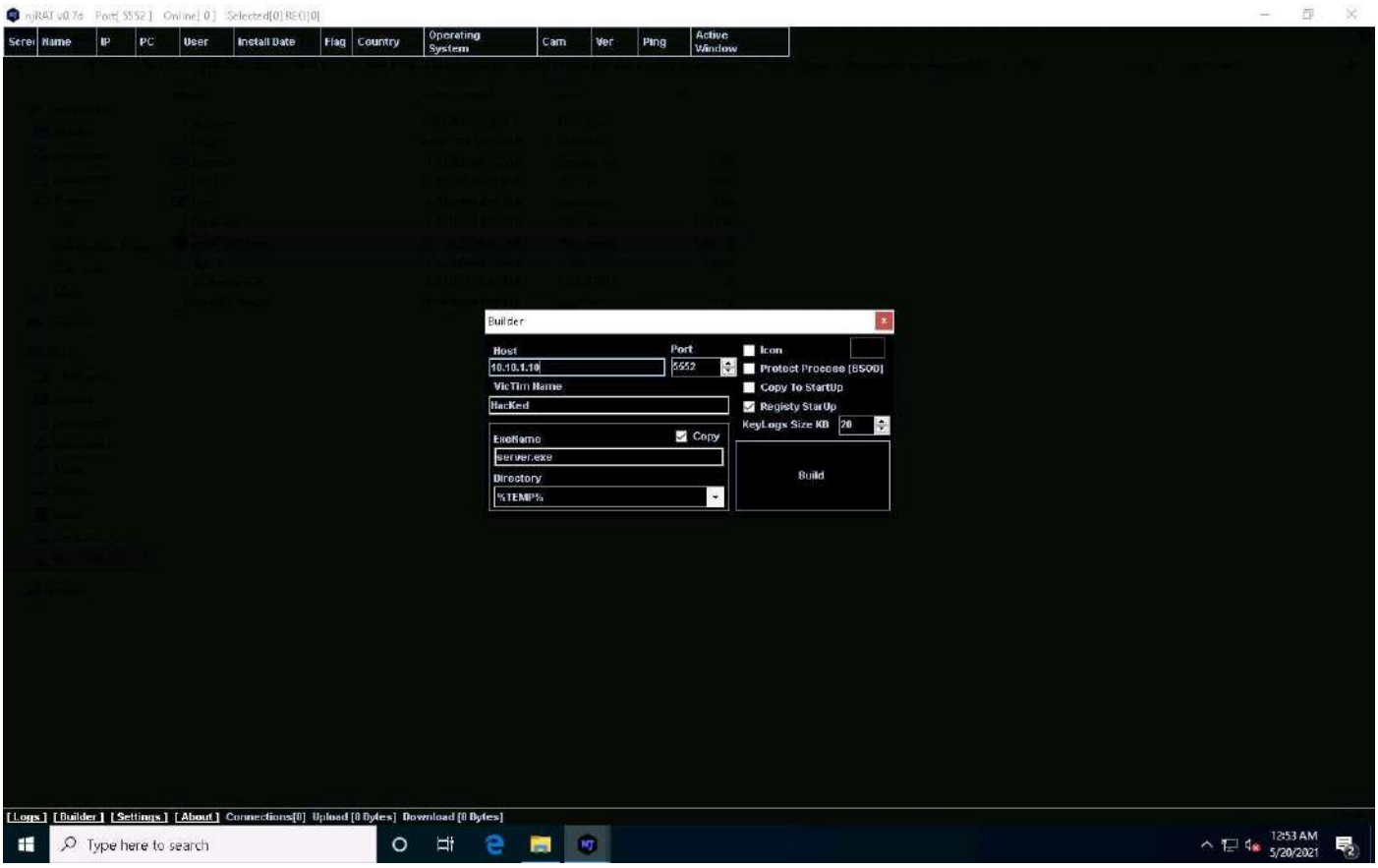


4. The njRAT GUI appears; click the **Builder** link located in the lower-left corner of the GUI to configure the exploit details.

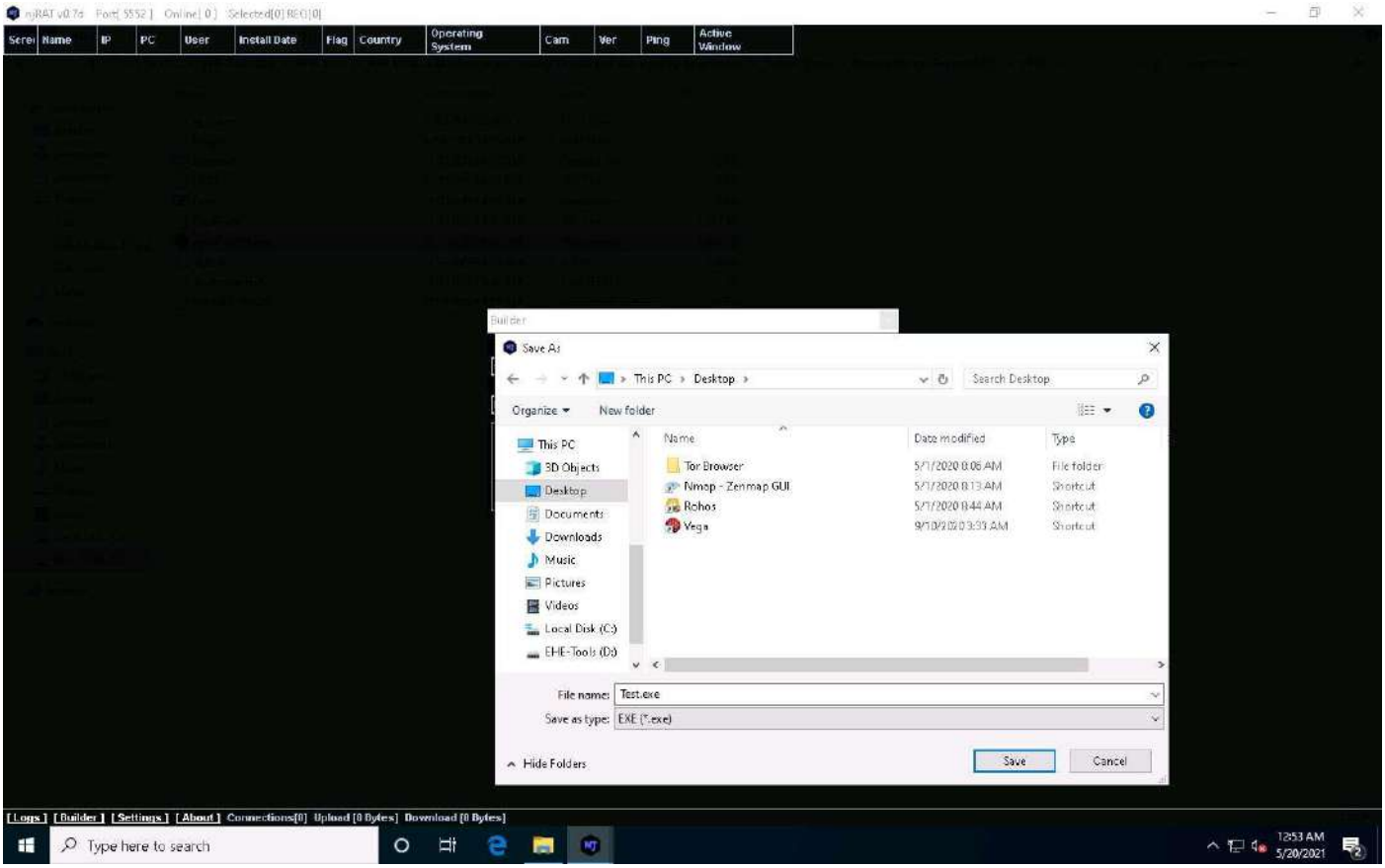


5. The **Builder** dialog-box appears; enter the IP address of the **Windows 10** (attacker machine) machine in the **Host** field, check the option **Registy StarUp**, leave the other settings to default, and click **Build**.

In this lab, the IP address of the **Windows 10** machine is **10.10.1.10**. This IP address might vary in your lab environment.



6. The **Save As** window appears; specify a location to store the server, rename it, and click **Save**.
7. In this lab, the destination location chosen is **Desktop**, and the file is named **Test.exe**.



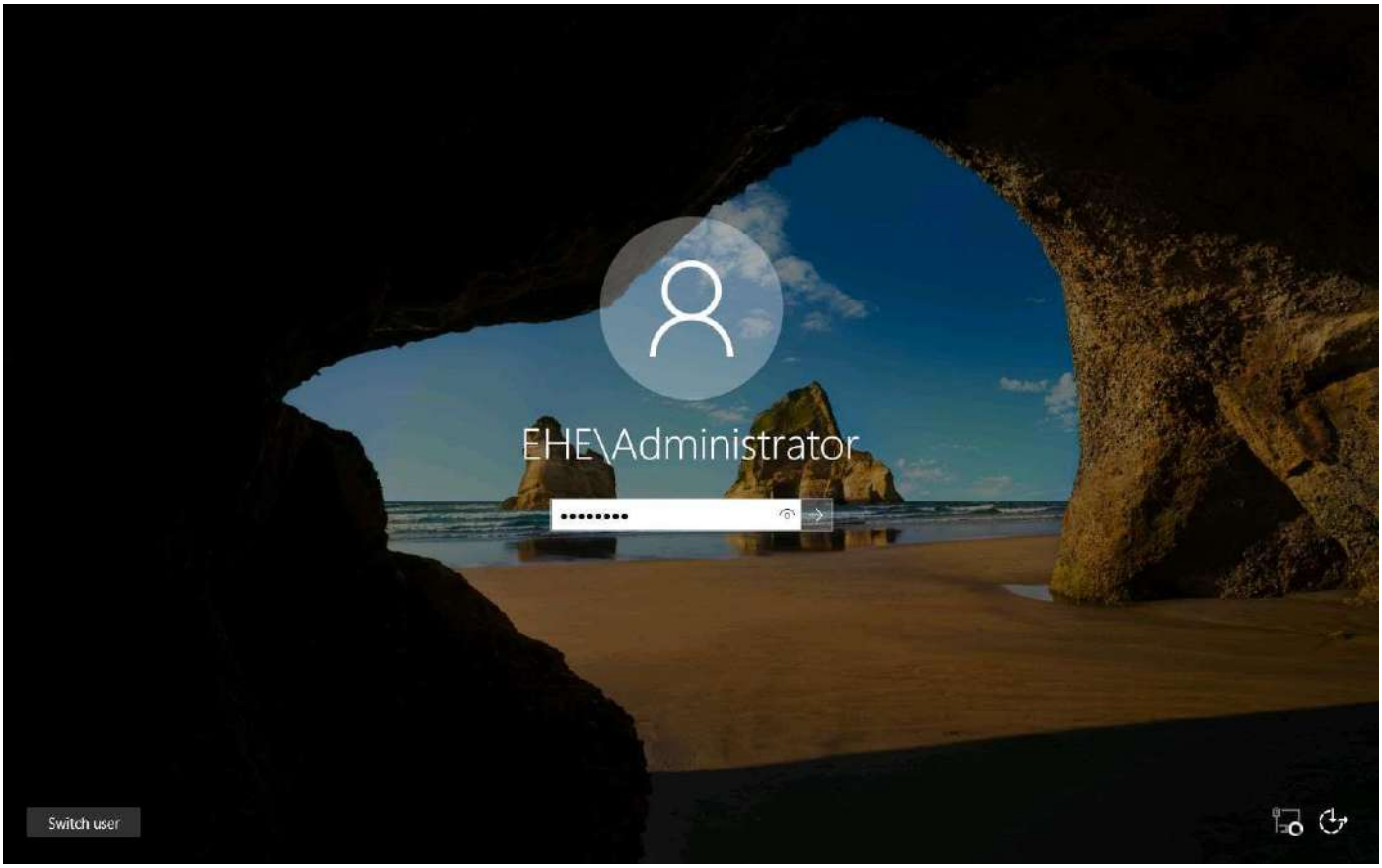
8. Once the server is created, the **DONE!** pop-up appears; click **OK**.
9. Now, use any technique to send this server to the intended target through email or any other source (in real-time, attackers send this server to the victim).

In this lab, we copied the **Test.exe** file to the shared network location (**EHE-Tools**) to share the file.

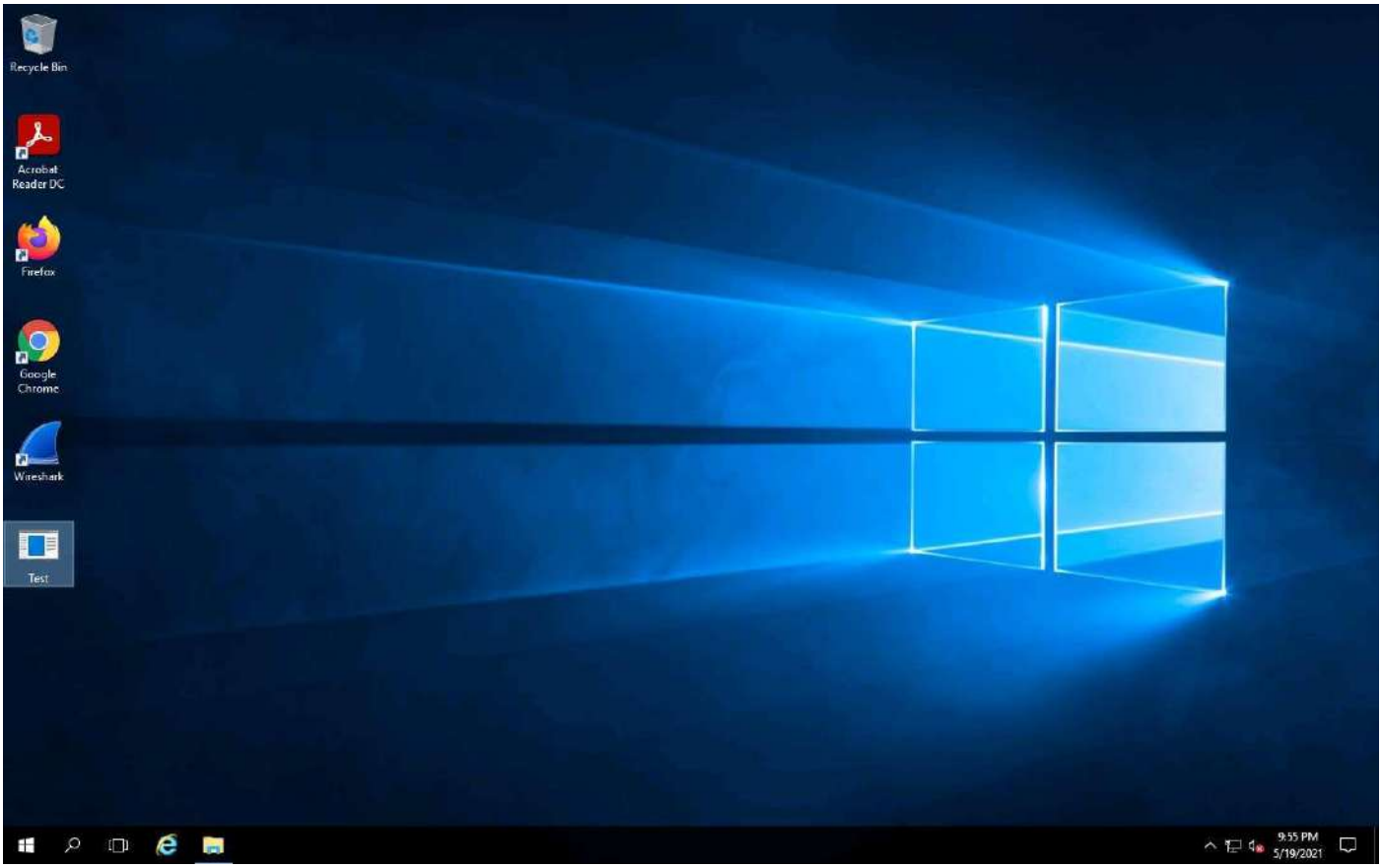
10. Click Windows Server 2016 to switch to the **Windows Server 2016** machine.

If you are already logged into the **Windows Server 2016** machine, then skip to **Step#12**.

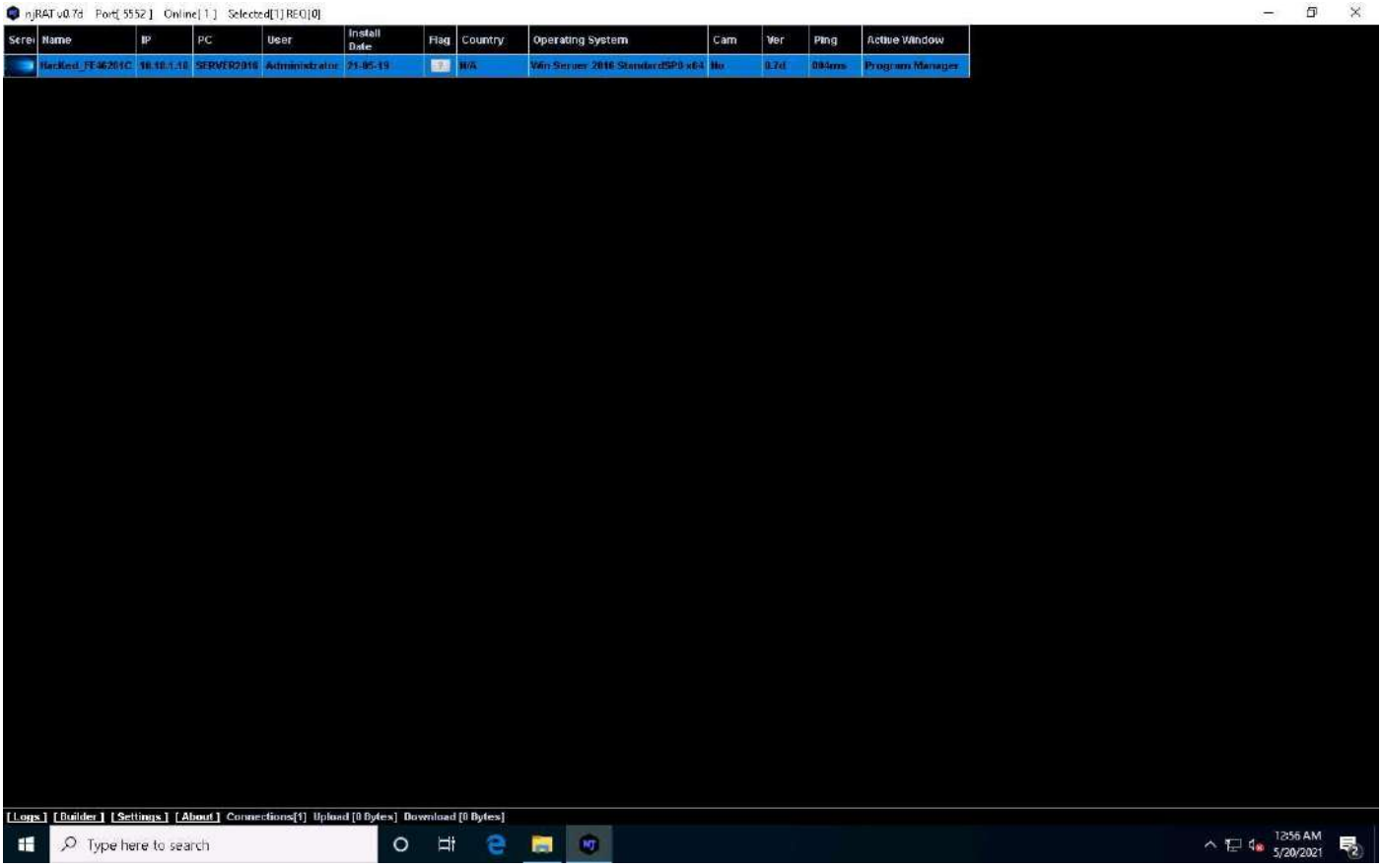
11. Click Ctrl+Alt+Delete to activate the machine, by default, **EHE\Administrator** account is selected, click Pa$$w0rd to enter the password and press **Enter**.



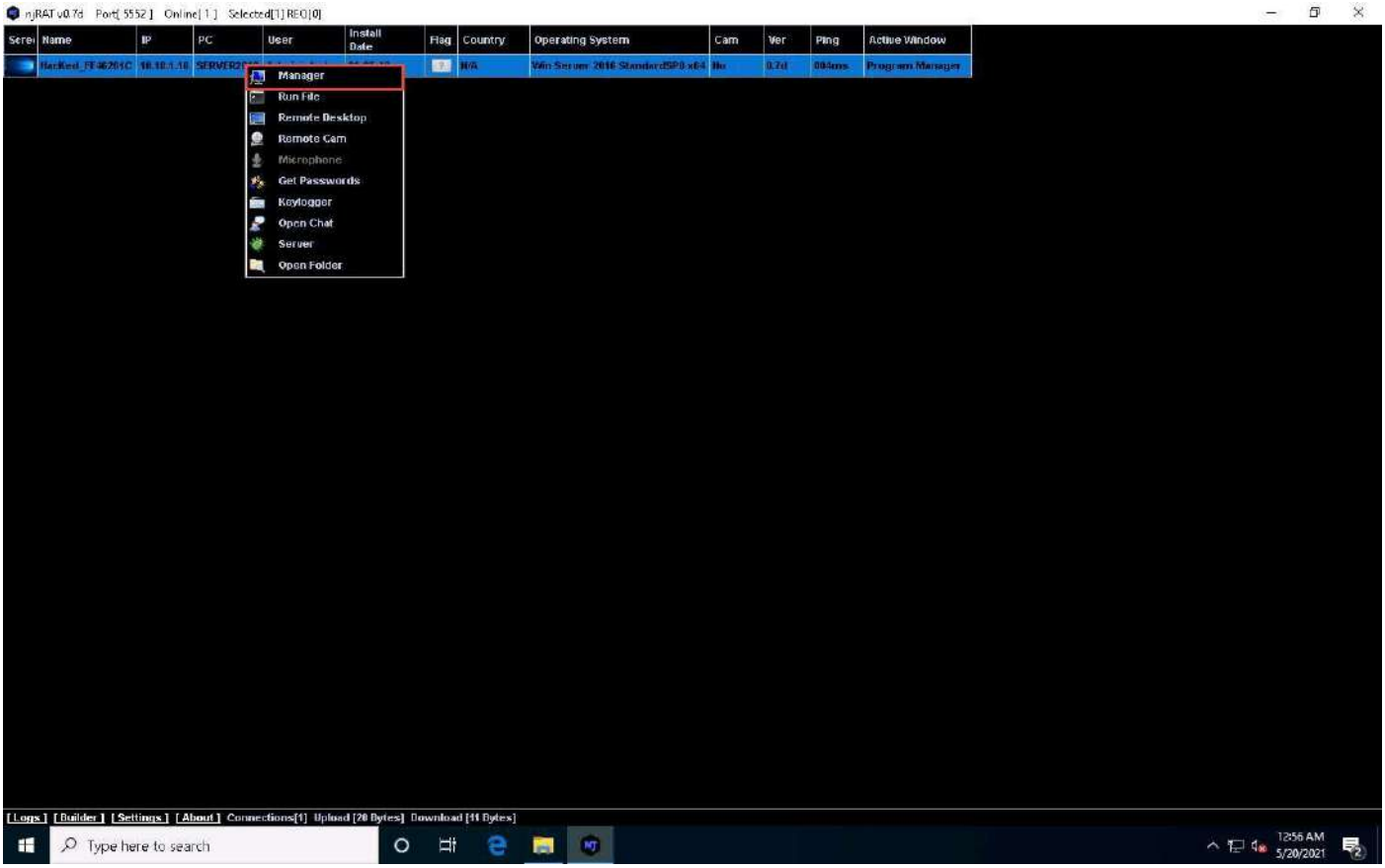
12. Navigate to the shared network location (**EHE-Tools**), and then **Copy** and **Paste** the executable file (**Test.exe**) onto the **Desktop** of **Windows Server 2016**.
13. Here, you are acting both as an **attacker** who logs into the **Windows 10** machine to create a malicious server, and as a **victim** who logs into the **Windows Server 2016** machine and downloads the server.
14. Double-click the server (**Test.exe**) to run this malicious executable.



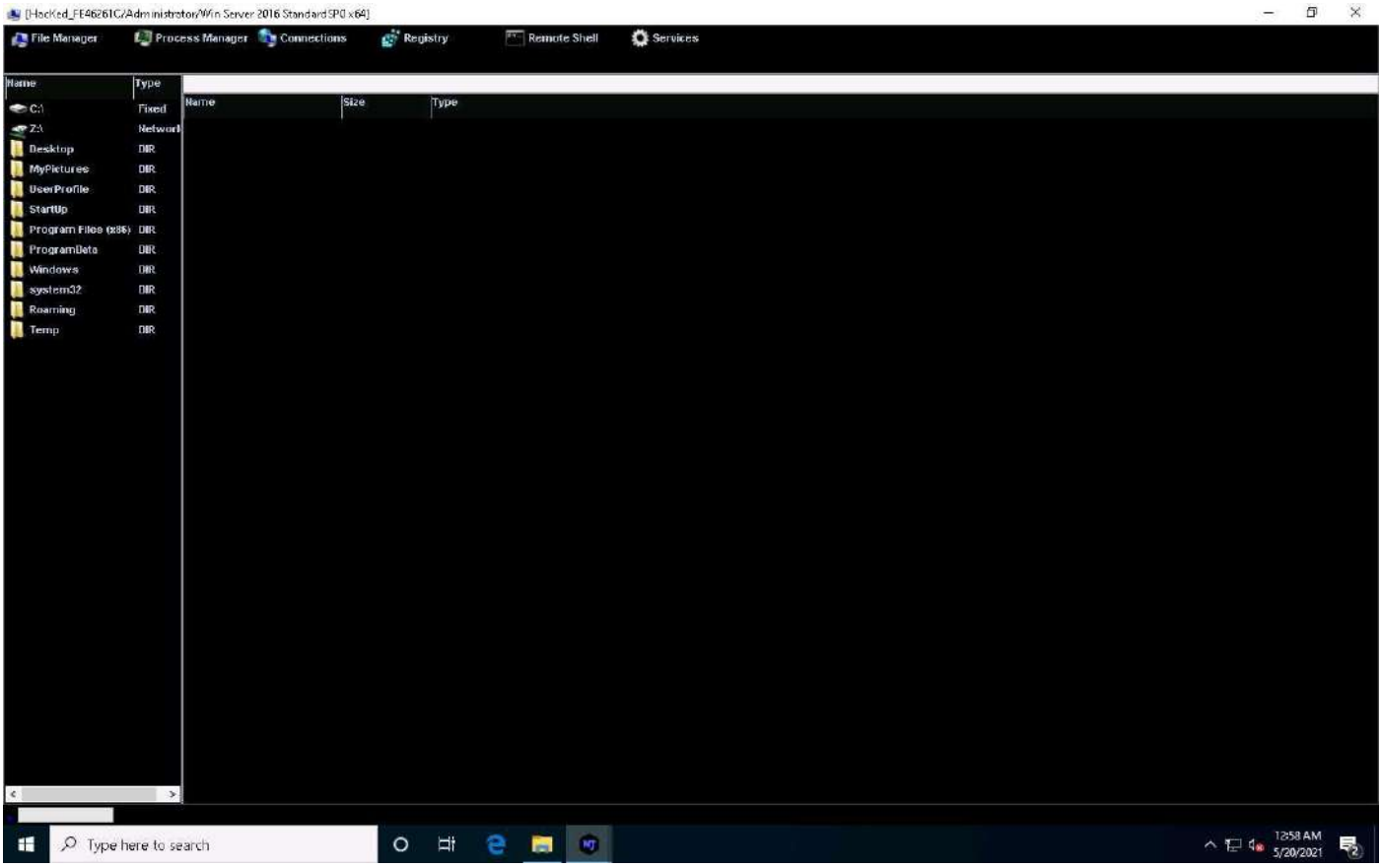
15. Click Windows 10 to switch back to the **Windows 10** machine. As soon as the victim (here, you) double-clicks the server, the executable starts running and the njRAT client (njRAT GUI) running in **Windows 10** establishes a persistent connection with the victim machine, as shown in the screenshot.



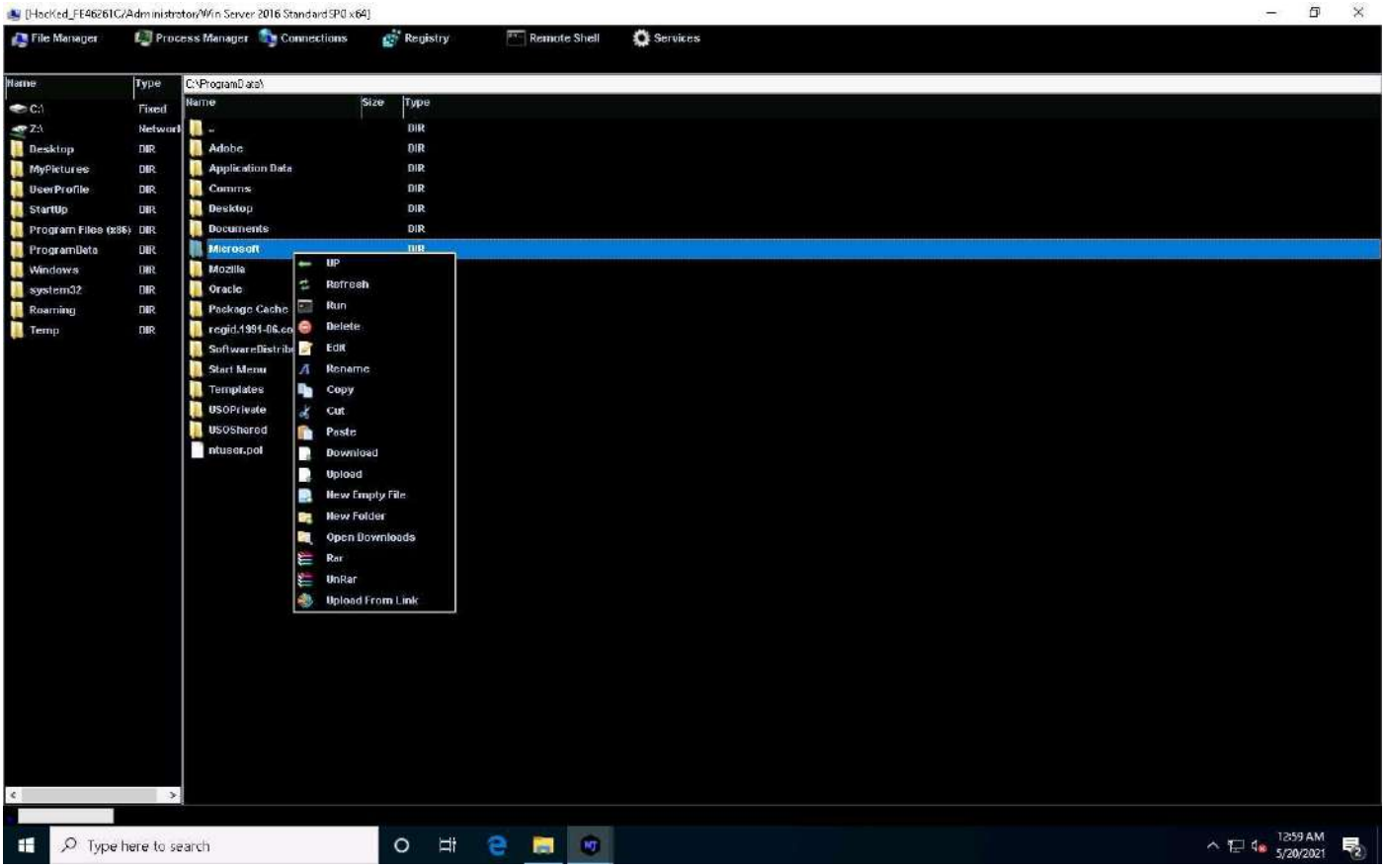
16. Unless the attacker working on the **Windows 10** machine disconnects the server on their own, the victim machine remains under their control.
17. The GUI displays the machine's basic details such as the IP address, User name, and Type of Operating system.
18. Right-click on the detected victim name and click **Manager**.



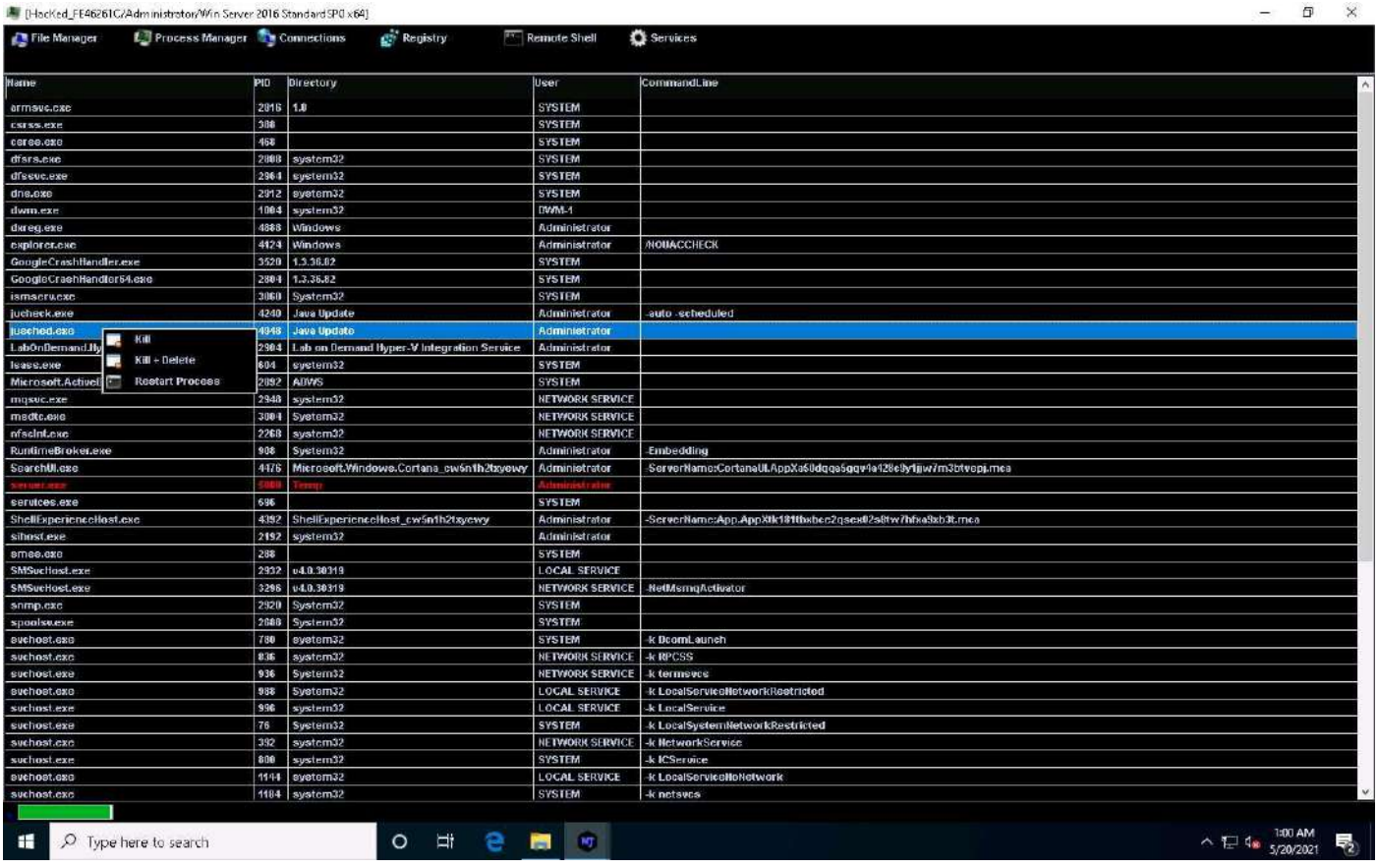
19. The **Manager** window appears with **File Manager** selected by default.



20. Double-click any directory in the left pane (here, **ProgramData**); all its associated files and directories are displayed in the right pane. You can right-click a selected directory and manipulate it using the contextual options.



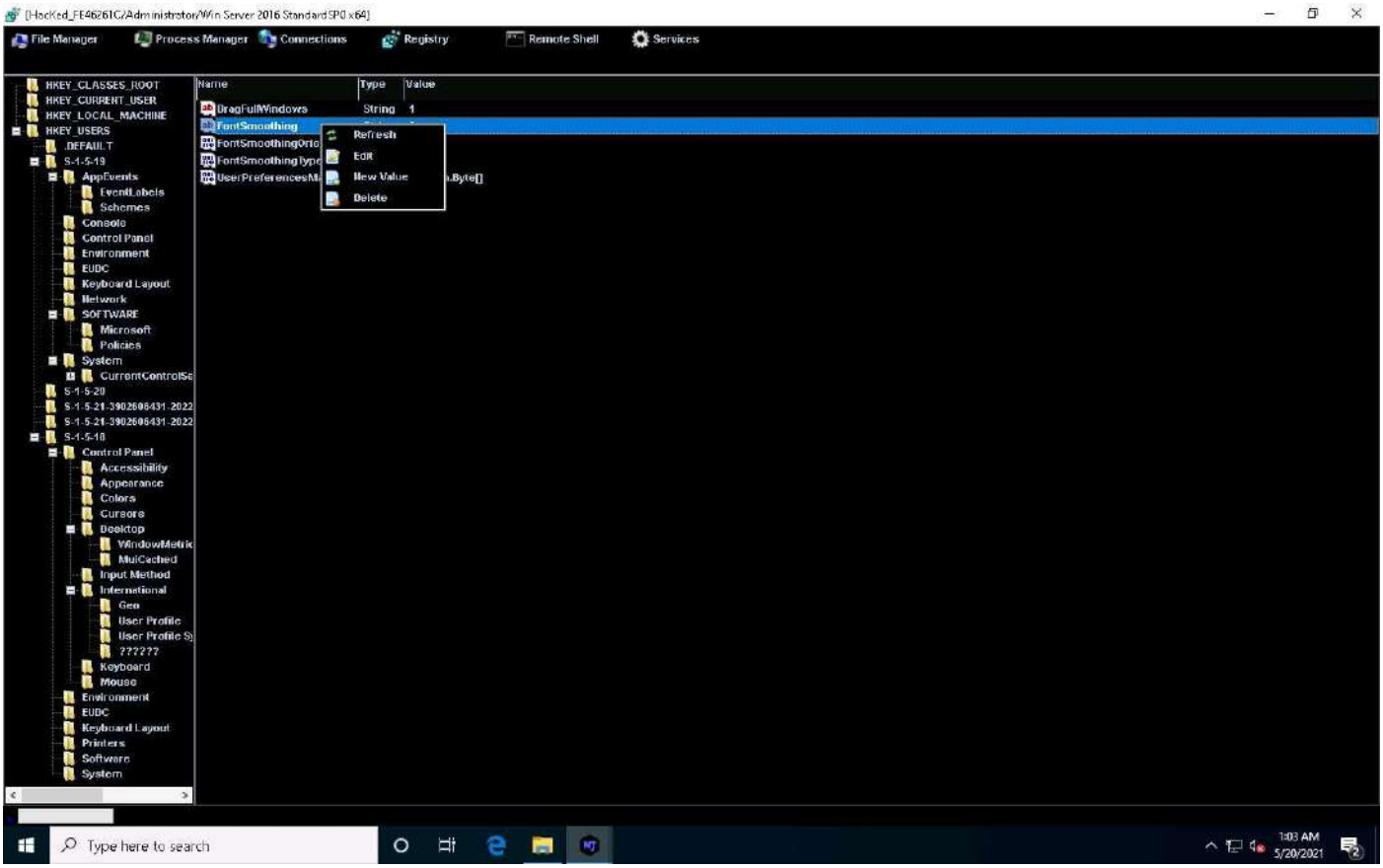
21. Click on **Process Manager**. You will be redirected to the Process Manager, where you can right-click on a selected process and perform actions such as **Kill**, **Delete**, and **Restart**.



22. Click on **Connections**, select a specific connection, right-click on it, and click **Kill Connection**. This kills the connection between two machines communicating through a particular port.

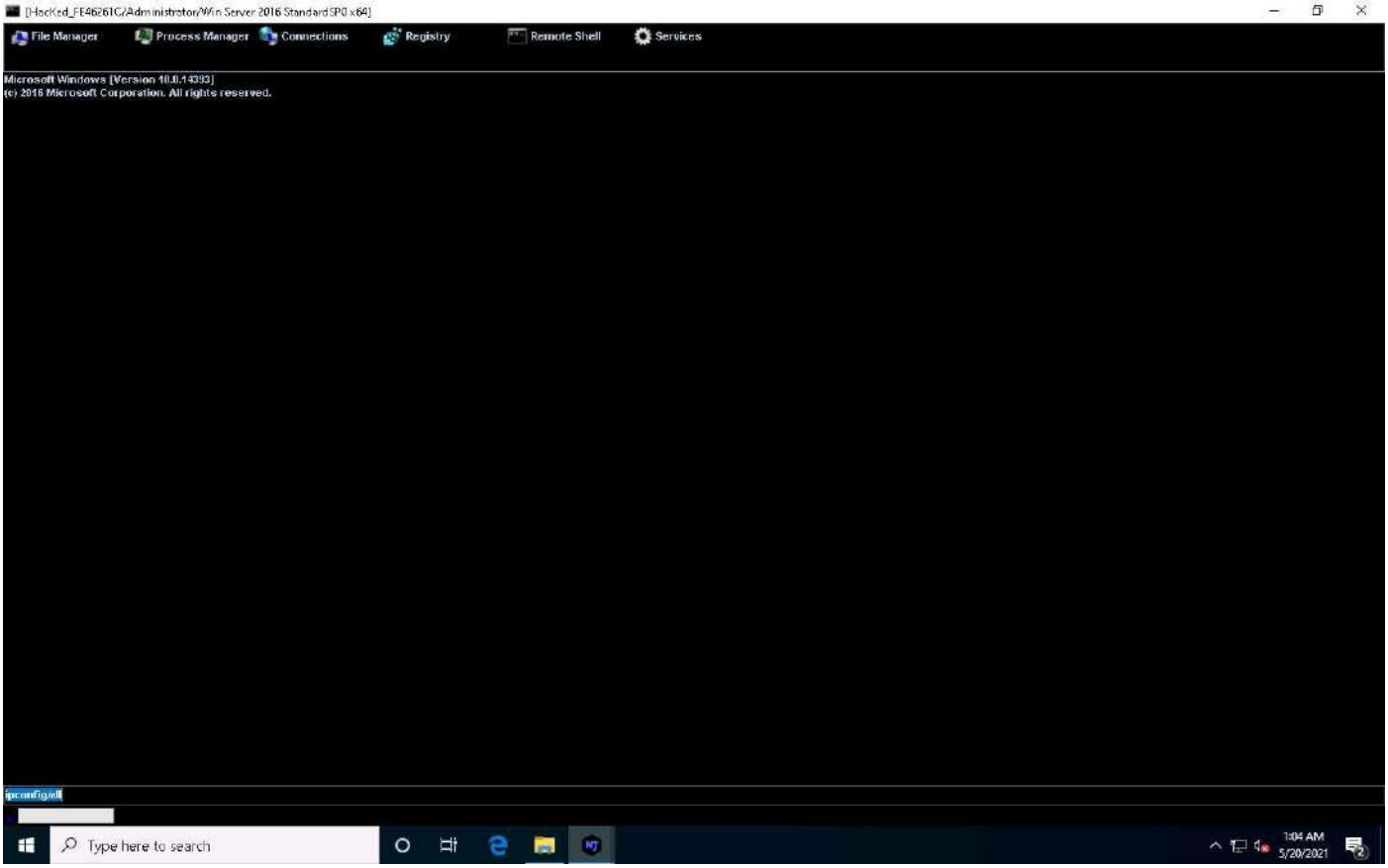
23. Click on **Registry**, choose a registry directory from the left pane, and right-click on its associated registry files.

24. A few options appear for the files; you can use these to manipulate them.

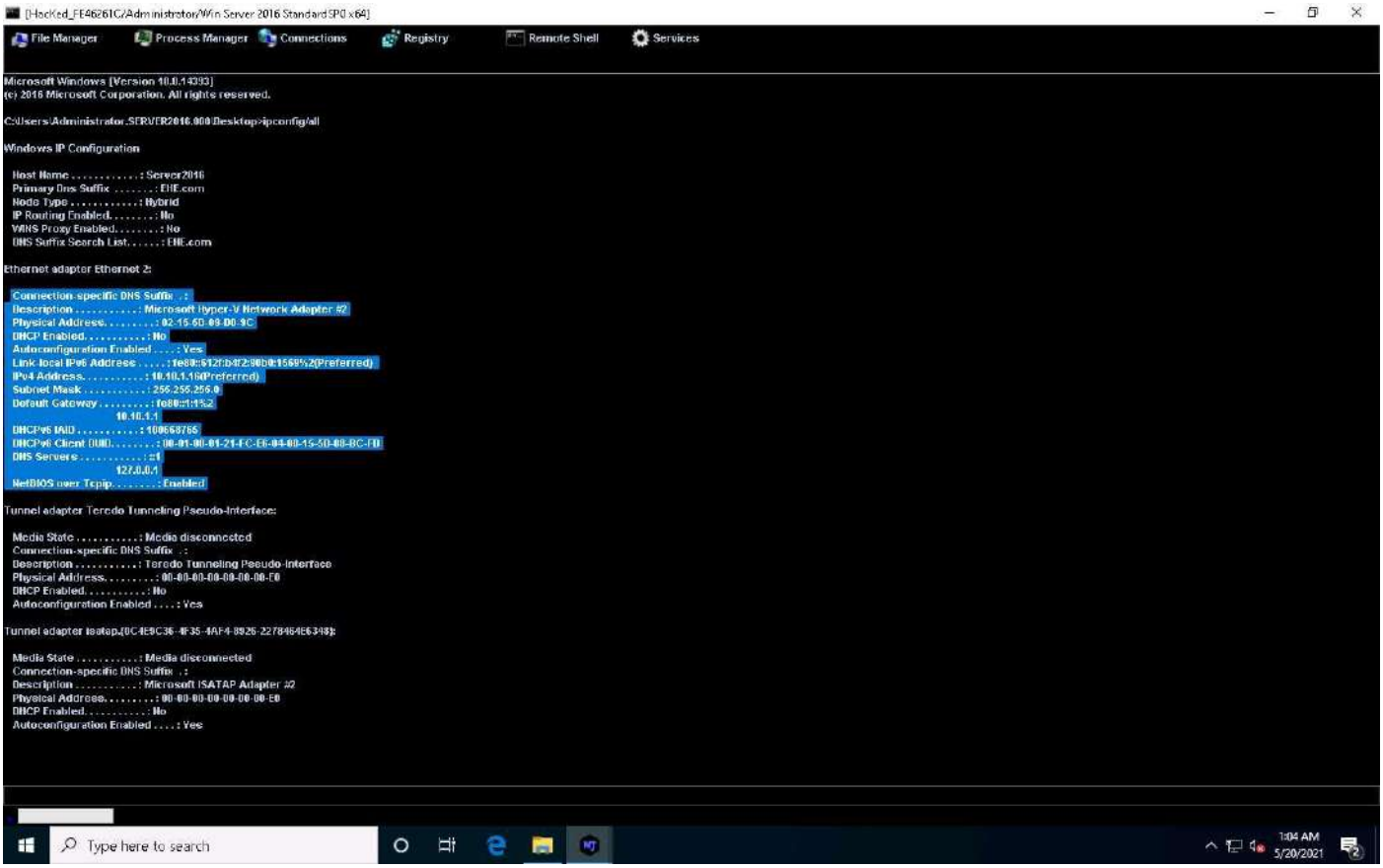


25. Click **Remote Shell**. This launches a remote command prompt for the victim machine (**Windows Server 2016**).

26. Type the command **ipconfig/all** and press **Enter**.



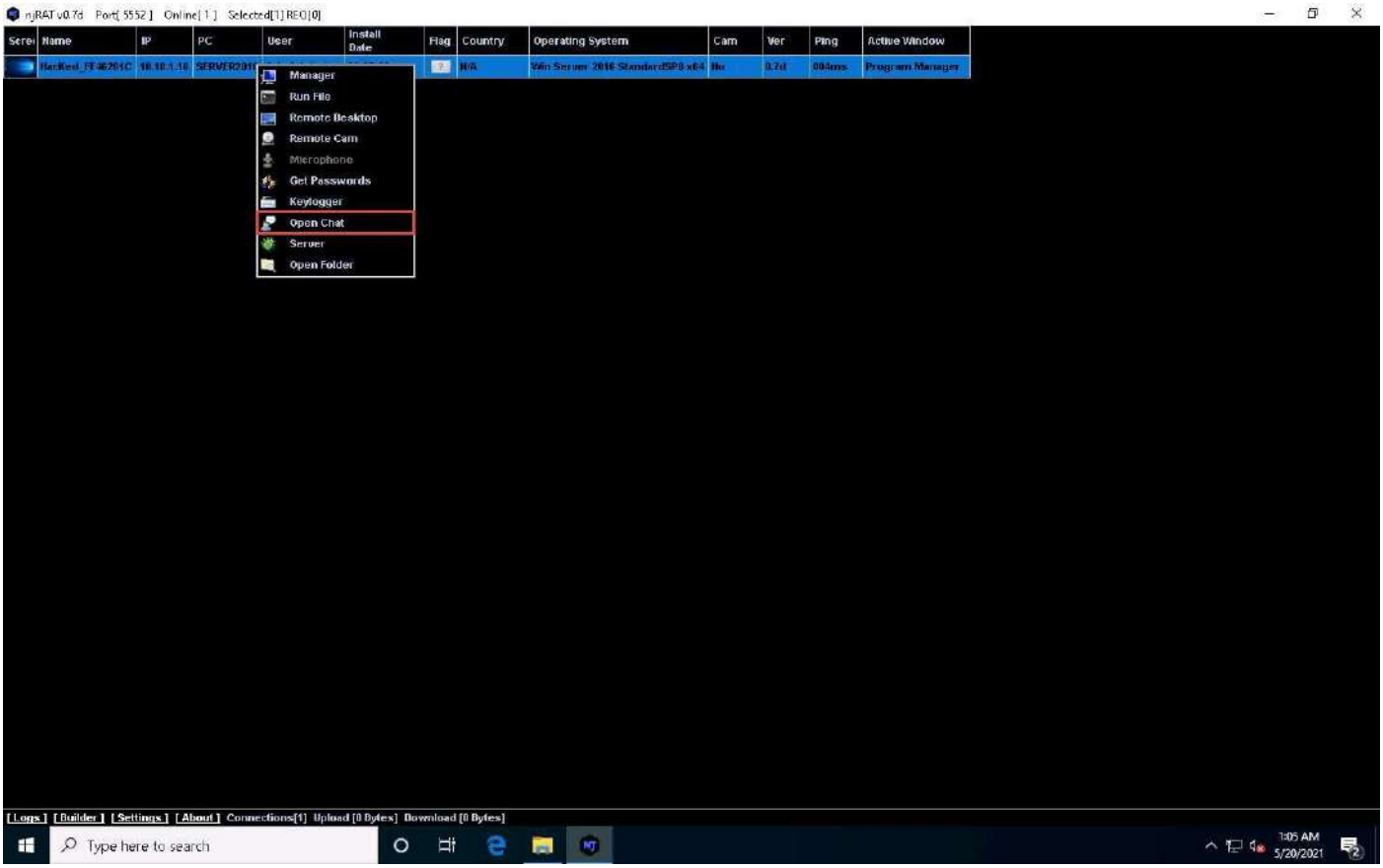
27. This displays all interfaces related to the victim machine, as shown in the screenshot.



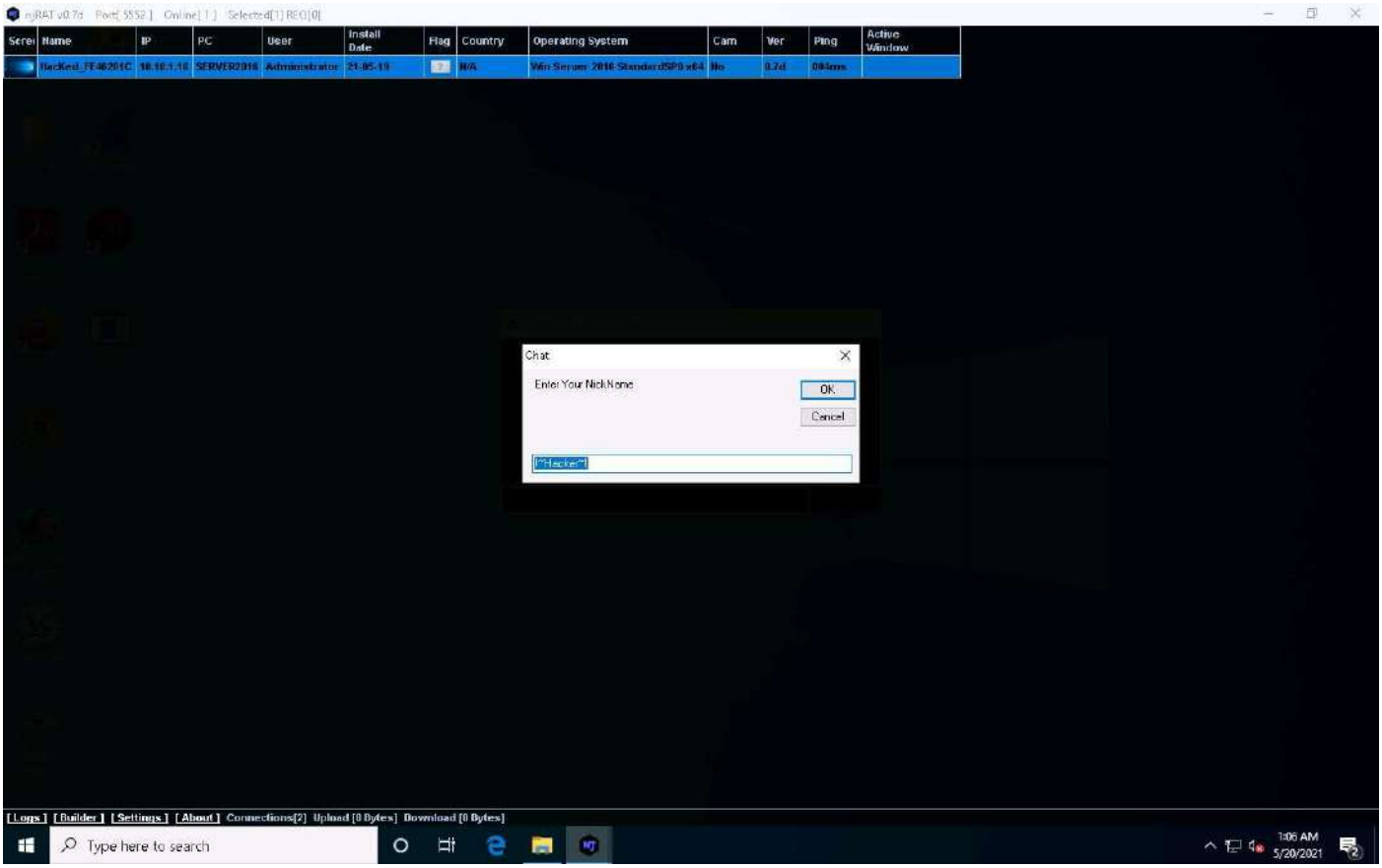
28. Similarly, you can issue all other commands that can be executed in the command prompt of the victim machine.
29. In the same way, click **Services**. You will be able to view all services running on the victim machine. In this section, you can use options to **start**, **pause**, or **stop** a service.
30. Close the **Manager** window.

If a **njRAT v0.7d** pop-up appears click on **Continue**.

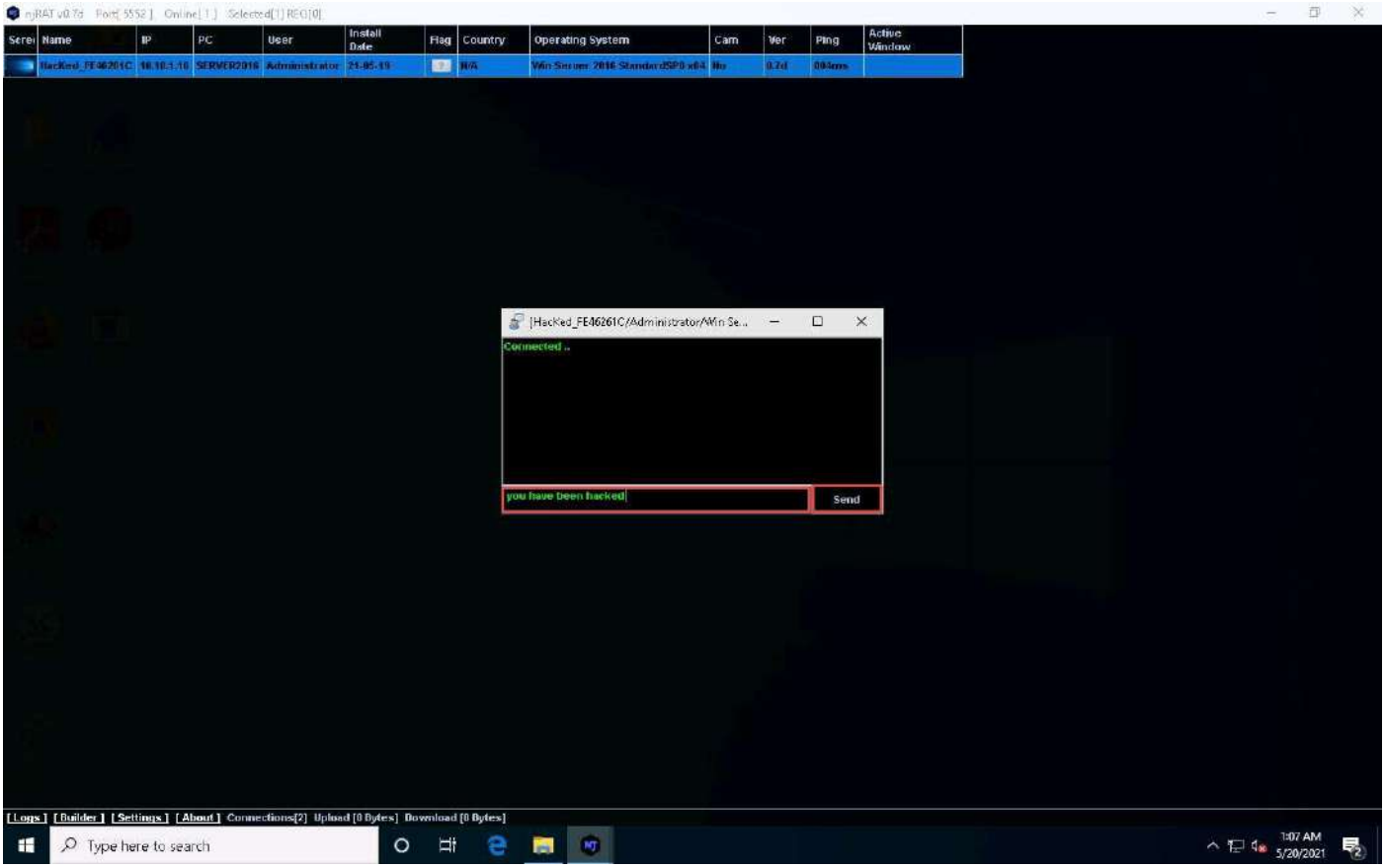
31. Right-click on the victim name, and click **Open Chat**.



32. A **Chat** pop-up appears; enter a nickname (here, **Hacker**) and click **OK**.

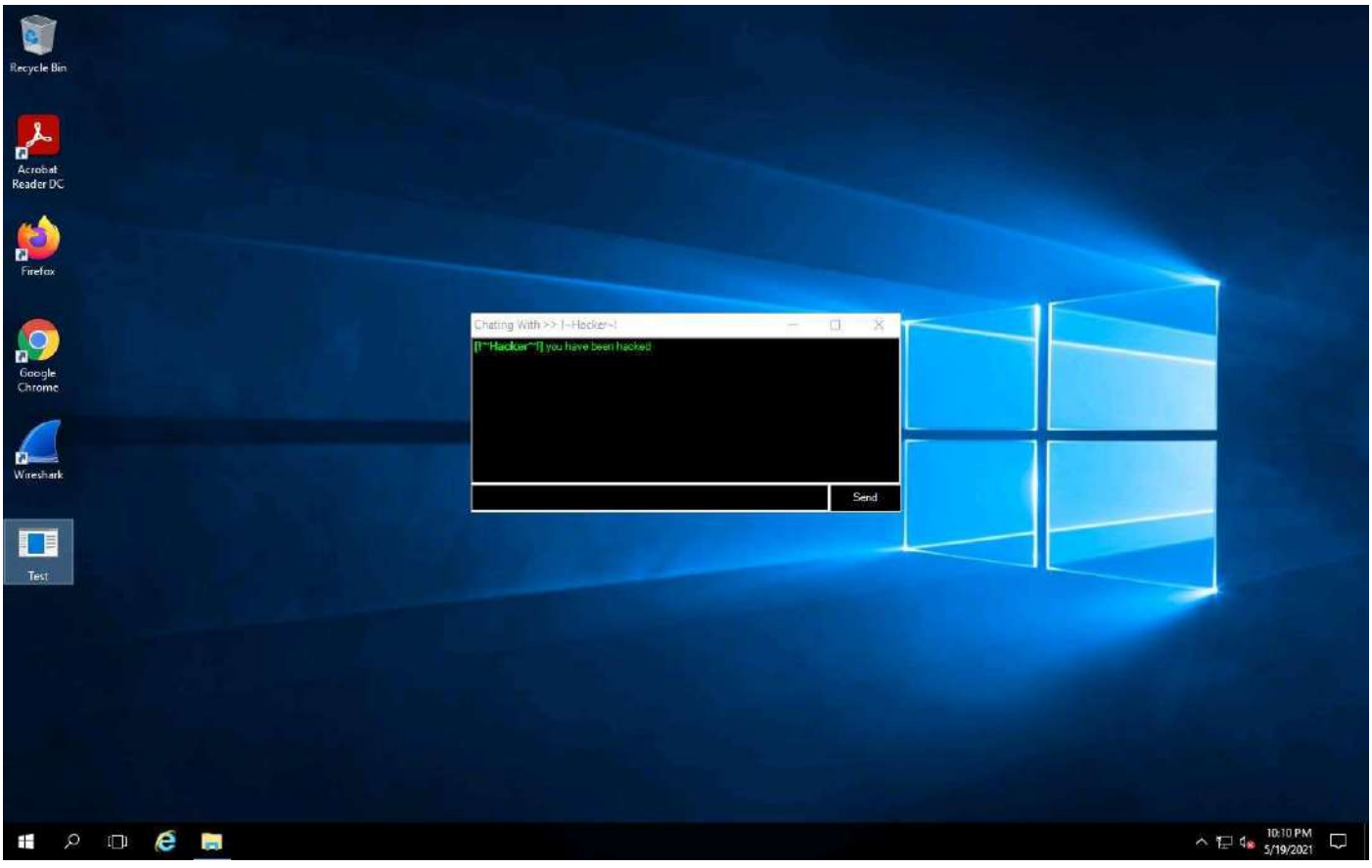


33. A chat box appears; type a message, and then click **Send**.



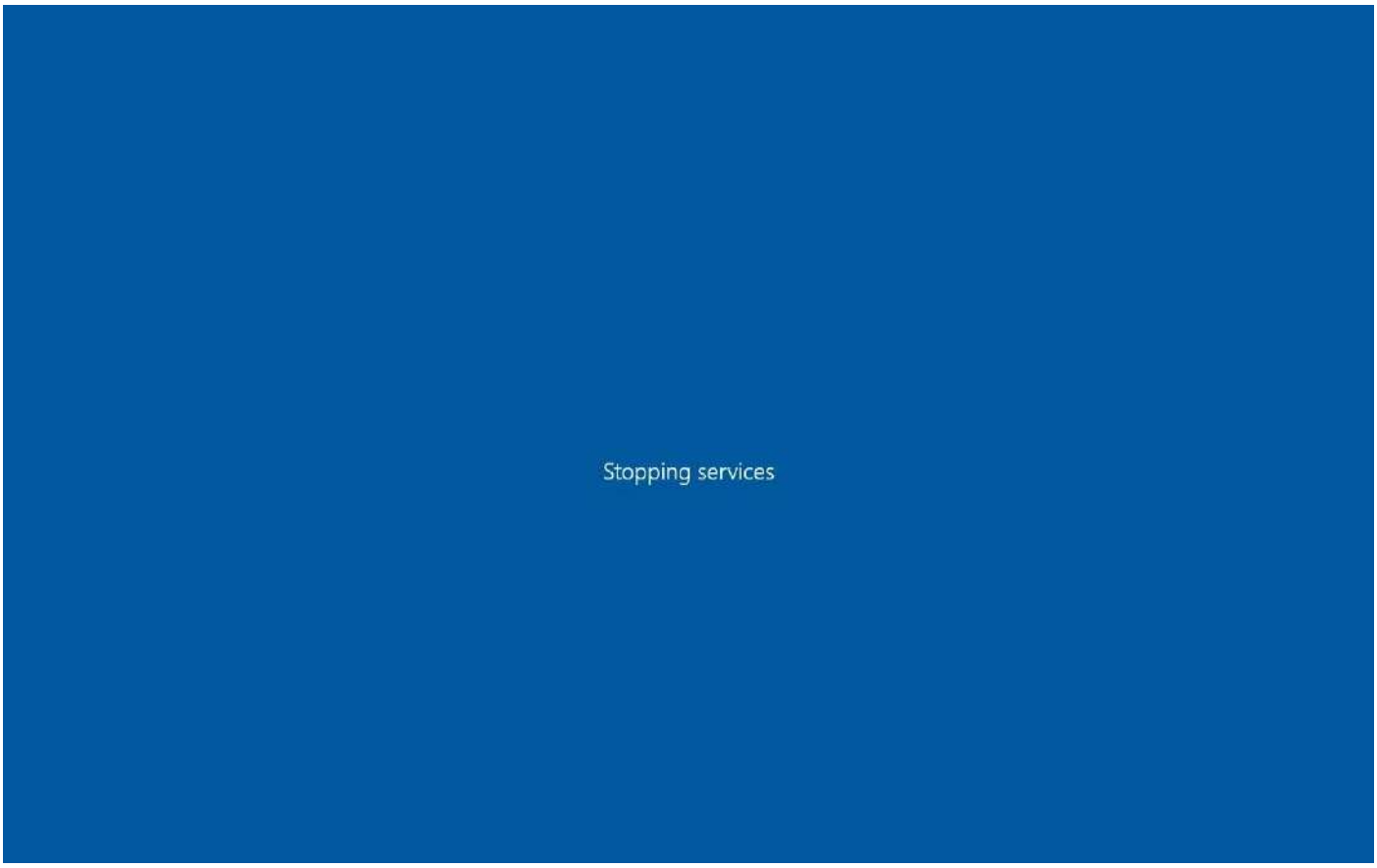
34. In real-time, as soon as the attacker sends the message, a pop-up appears on the victim's screen (**Windows Server 2016**), as demonstrated in the screenshot.

35. Click Windows Server 2016 to switch to the **Windows Server 2016** machine, you can observe the message from the hacker appears on the screen.

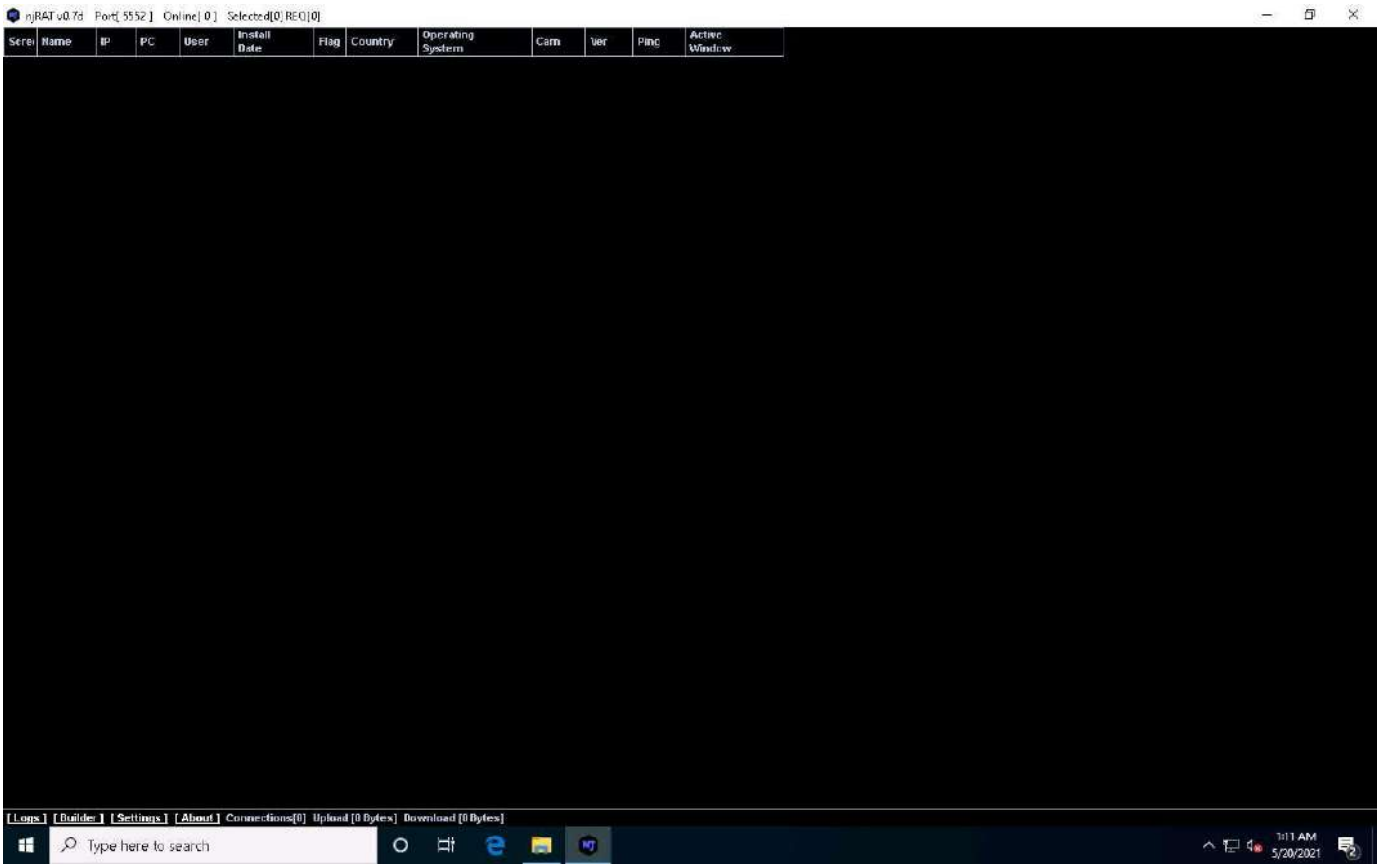


36. Seeing this, the victim becomes alert and attempts to close the chatbox. Irrespective of what the victim does, the chatbox remains for open as long as the attacker uses it.

37. Surprised by the behavior, the victim (you) attempts to break the connection by restarting the machine. As soon as this happens, njRAT loses its connection with **Windows Server 2016**, as the machine is shut down in the process of restarting.

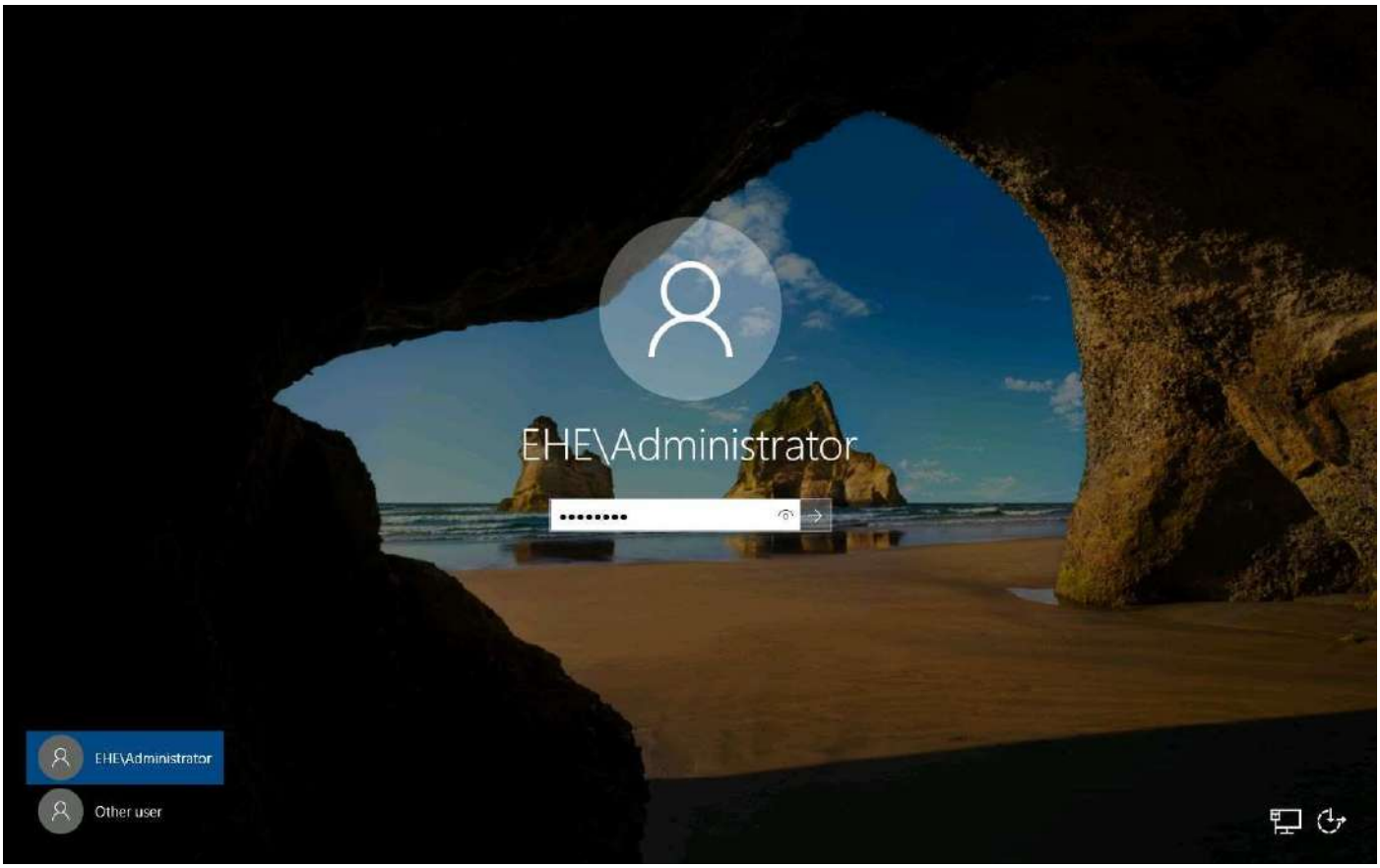


38. Click Windows 10 to switch back to the attacker machine (**Windows 10**); you can see that the connection with the victim machine is lost.



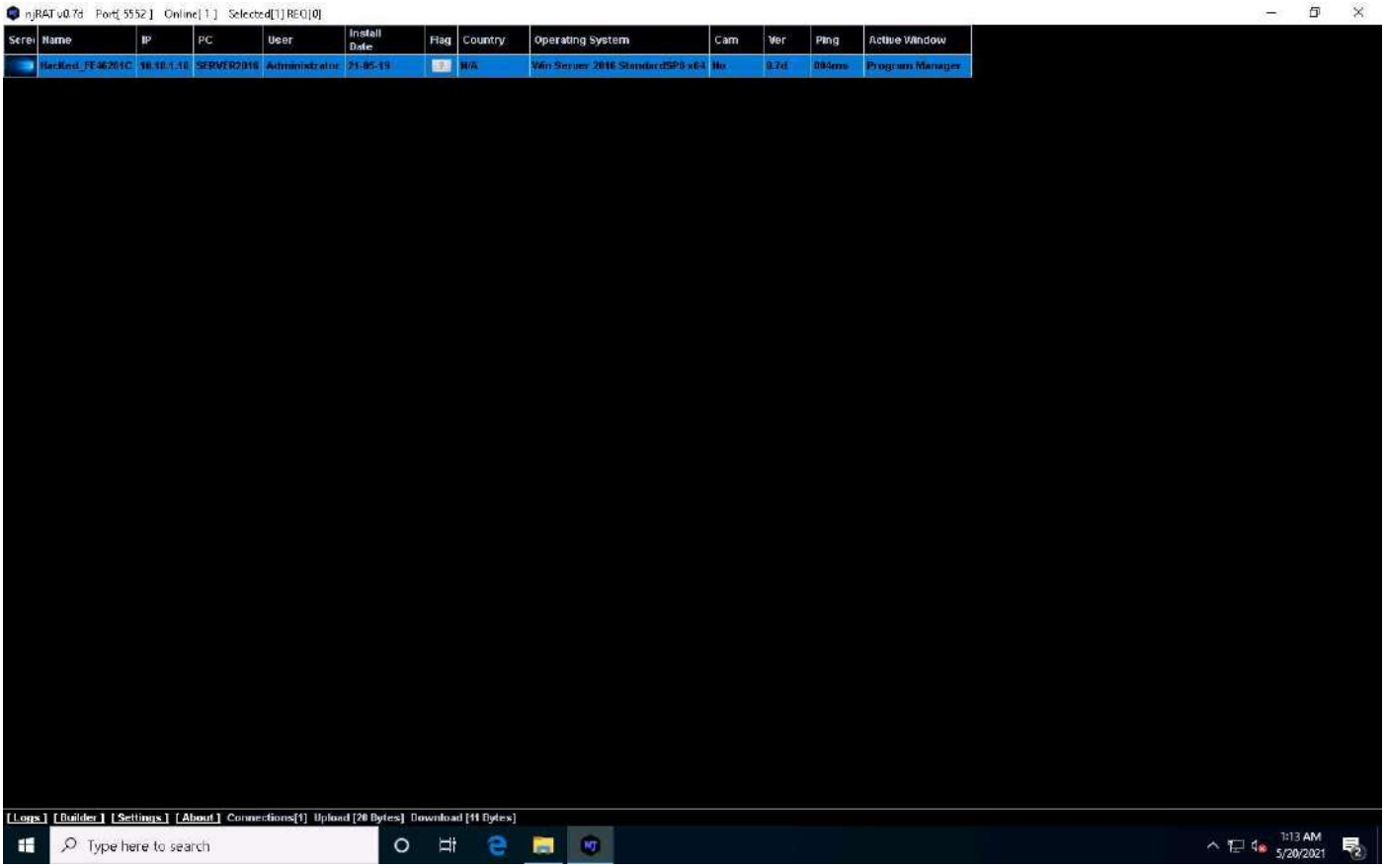
39. However, as soon as the victim logs in to their machine, the njRAT client automatically establishes a connection with the victim, as shown in the screenshot.

40. Click Windows Server 2016 to switch to the victim machine (**Windows Server 2016**). Click Ctrl+Alt+Delete to activate the machine, by default, **EHE\Administrator** account is selected, click Pa$$w0rd to enter the password and press **Enter**.



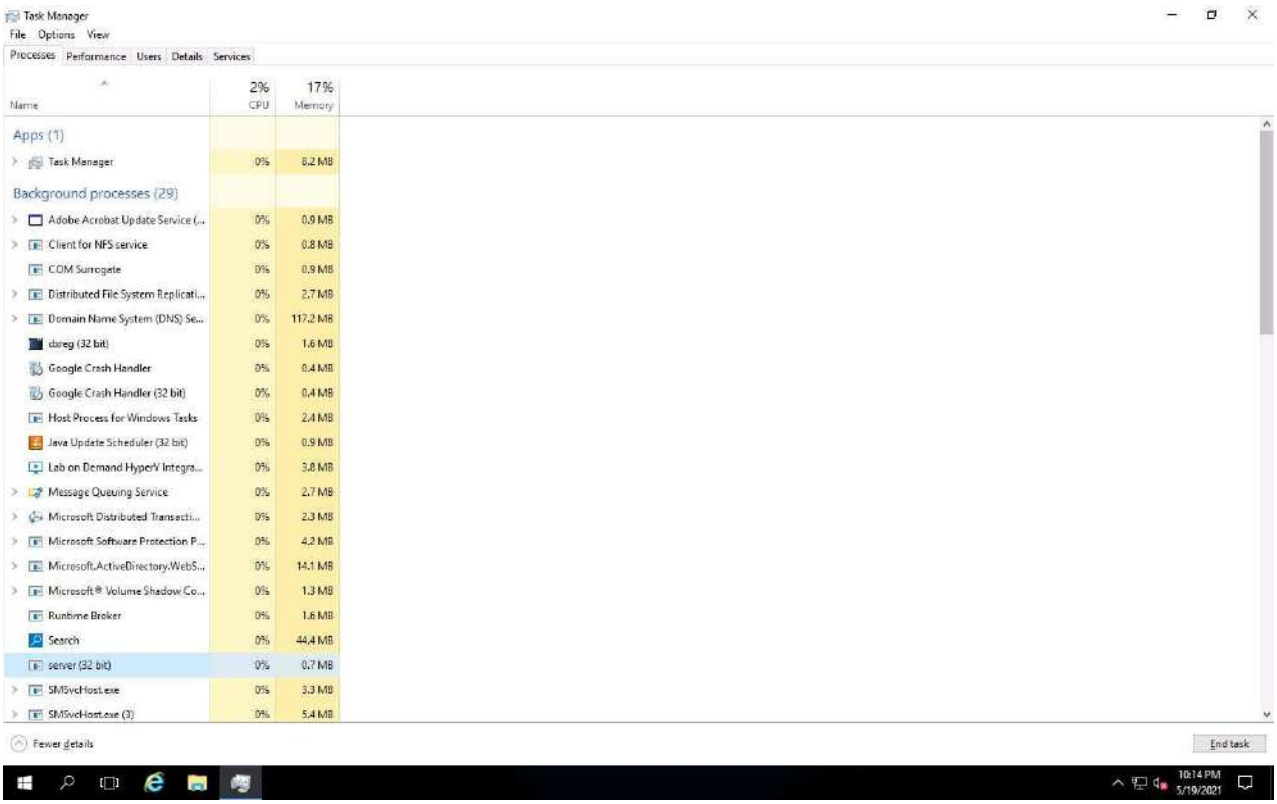
41. Click Windows 10 to switch back to the attacker machine (**Windows 10**); you can see that the connection has been re-established with the victim machine.

It might take some time to establish a connection with the victim.



42. The attacker, as usual, makes use of the connection to access the victim machine remotely and perform malicious activity.

43. On completion of this lab, click Windows Server 2016 to switch to the **Windows Server 2016** machine, launch **Task Manager**, look for the **server.exe (32 bit)** process, and click **End task**.



44. This concludes the demonstration of how to create a Trojan using njRAT Trojan to gain control over a victim machine.

45. Close all open windows.

Lab 3-2: Create a Virus to Infect the Target System

Lab Scenario

Viruses are the scourges of modern computing. Computer viruses have the potential to wreak havoc on both business and personal computers. The lifetime of a virus depends on its ability to reproduce. Therefore, attackers design every virus code in such a manner that the virus replicates itself n number of times, where n is a number specified by the attacker.

Virus reproduces its own code while enclosing other executables, and spreads throughout the computer. Viruses can spread the infection by damaging files in a file system. Some viruses reside in the memory and may infect programs through the boot sector. A virus can also be in an encrypted form.

Lab Objectives

- Create a Virus using the JPS Virus Maker Tool and Infect the Target System

Task 1: Create a Virus using the JPS Virus Maker Tool and Infect the Target System

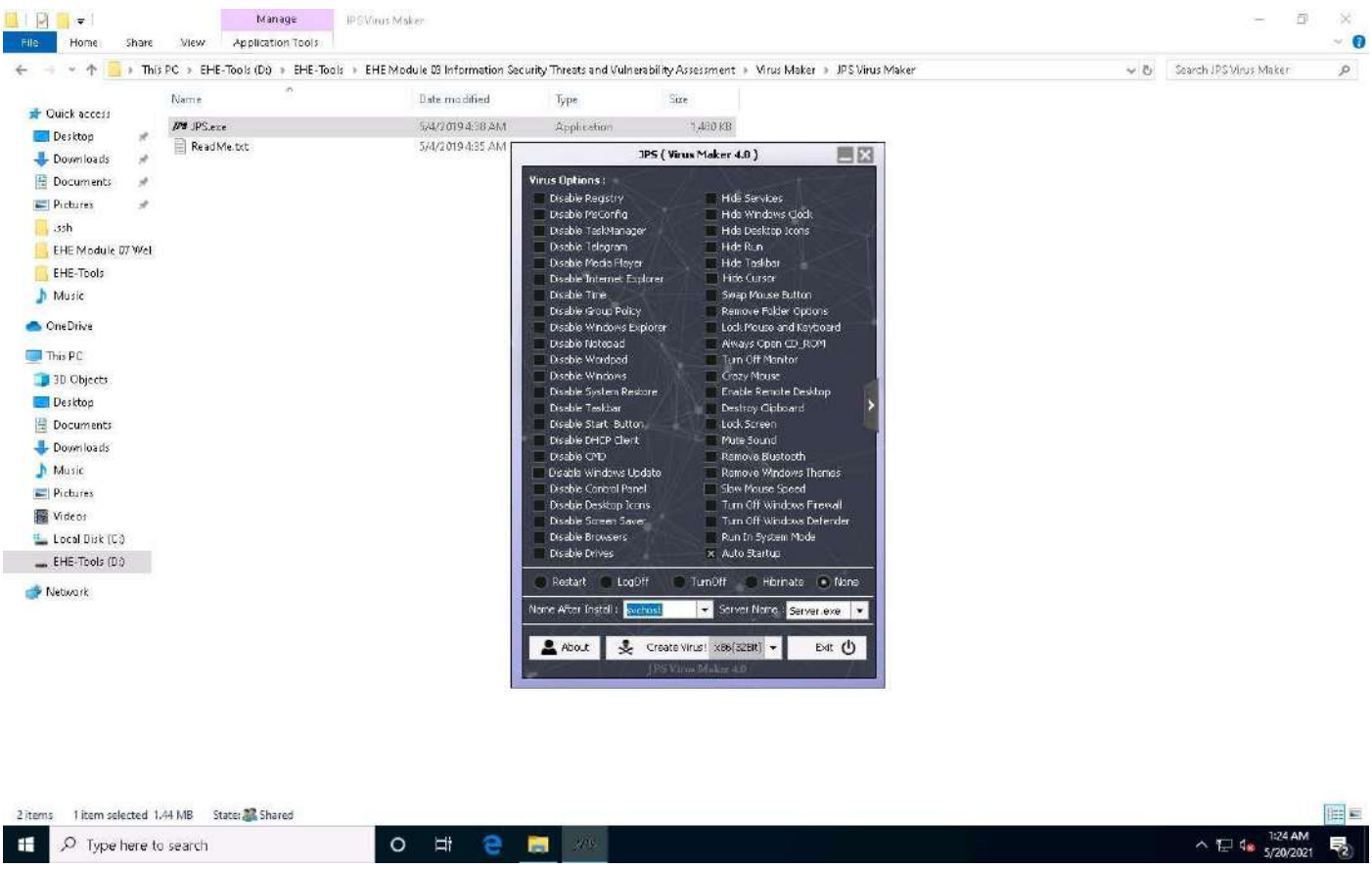
The JPS Virus Maker tool is used to create its own customized virus. This tool has many options for building that can be used to create a virus. Some of the tool's features are auto-start, shutdown, disable security center, lock mouse and keyboard, destroy protected storage, and terminate windows. We can use the JPS Virus Maker Tool as a proof of concept to audit perimeter security controls in an organization.

After performing this task, we will end and re-launch the lab as **Windows Server 2019** machine will be infected by the virus.

1. Click Windows 10 to switch to the **Windows 10** machine, navigate to **D:\EHE-Tools\EHE Module 03 Information Security Threats and Vulnerability Assessment\Virus Maker\JPS Virus Maker** and double-click **JPS.exe**.

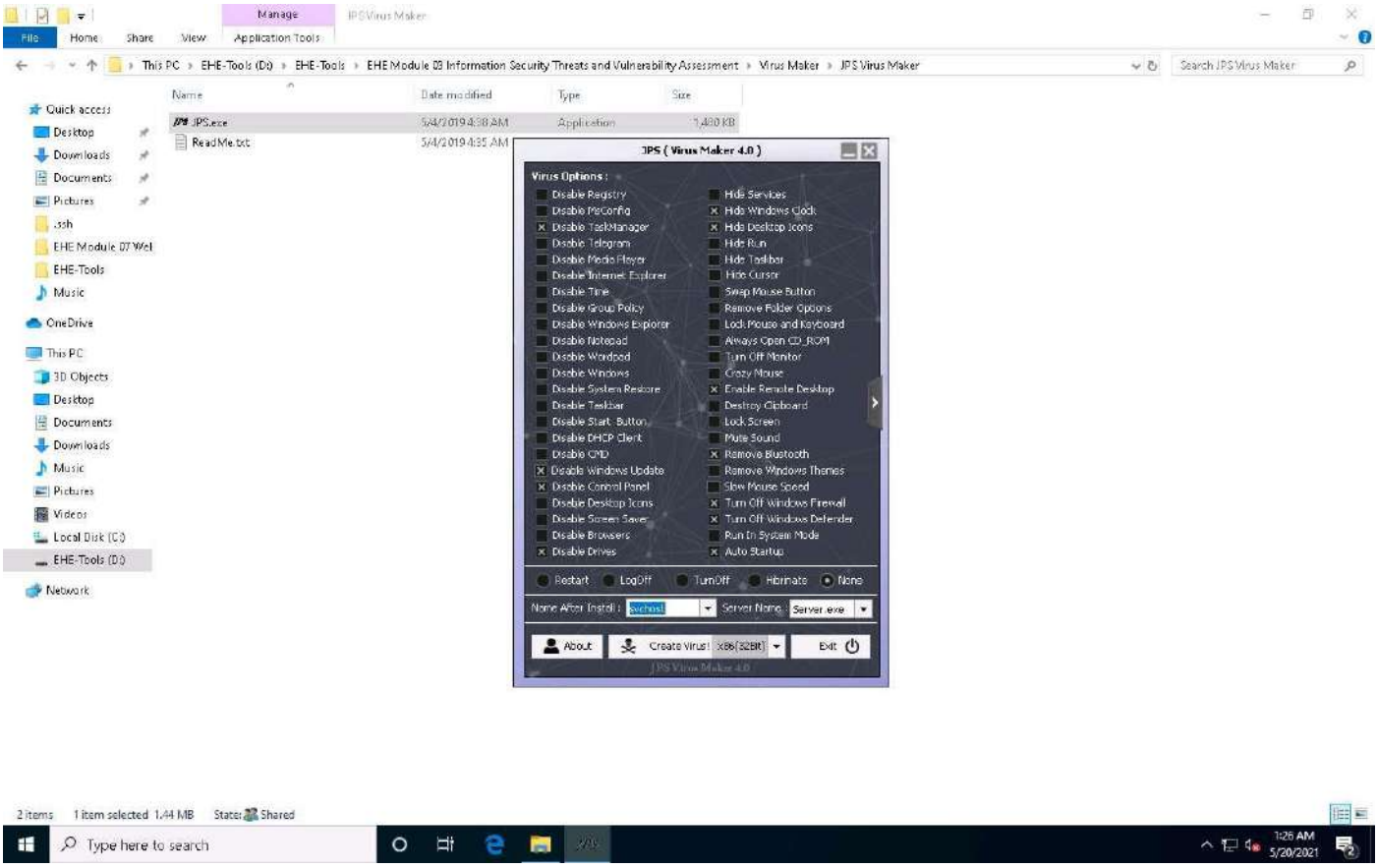
If an **Open File - Security** Warning pop-up appears, click **Run**.

2. The **JPS (Virus Maker 4.0)** window appears; tick the **Auto Startup** checkbox.



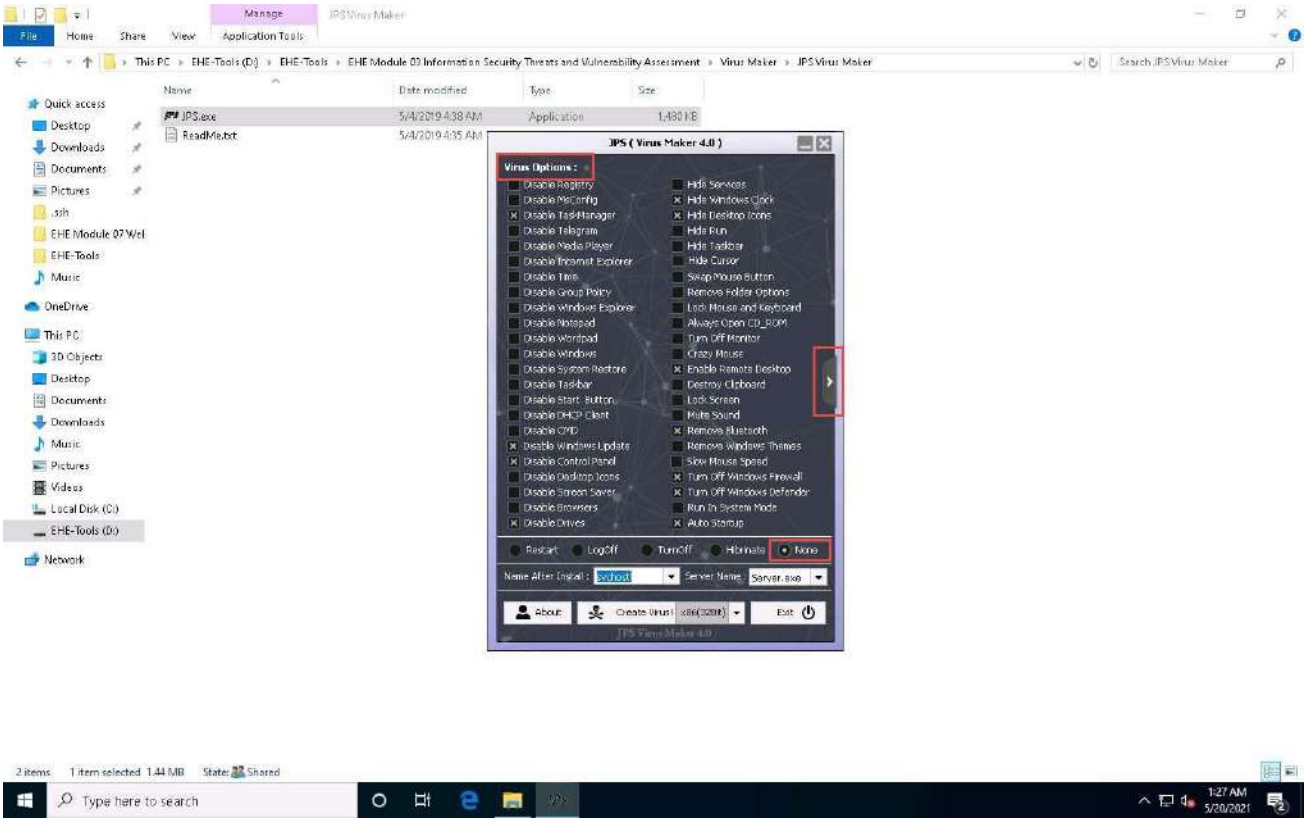
3. The window displays various features and options that can be chosen while creating a virus file.
4. From the **Virus Options**, check the options that you want to embed in a new virus file.

5. In this lab, the options embedded in the virus file are **Disable TaskManager**, **Disable Windows Update**, **Disable Control Panel**, **Disable Drives**, **Hide Windows Clock**, **Hide Desktop Icons**, **Enable Remote Desktop**, **Remove Bluetooth**, **Turn Off Windows Firewall**, **Turn Off Windows Defender**, and **Auto Startup**.

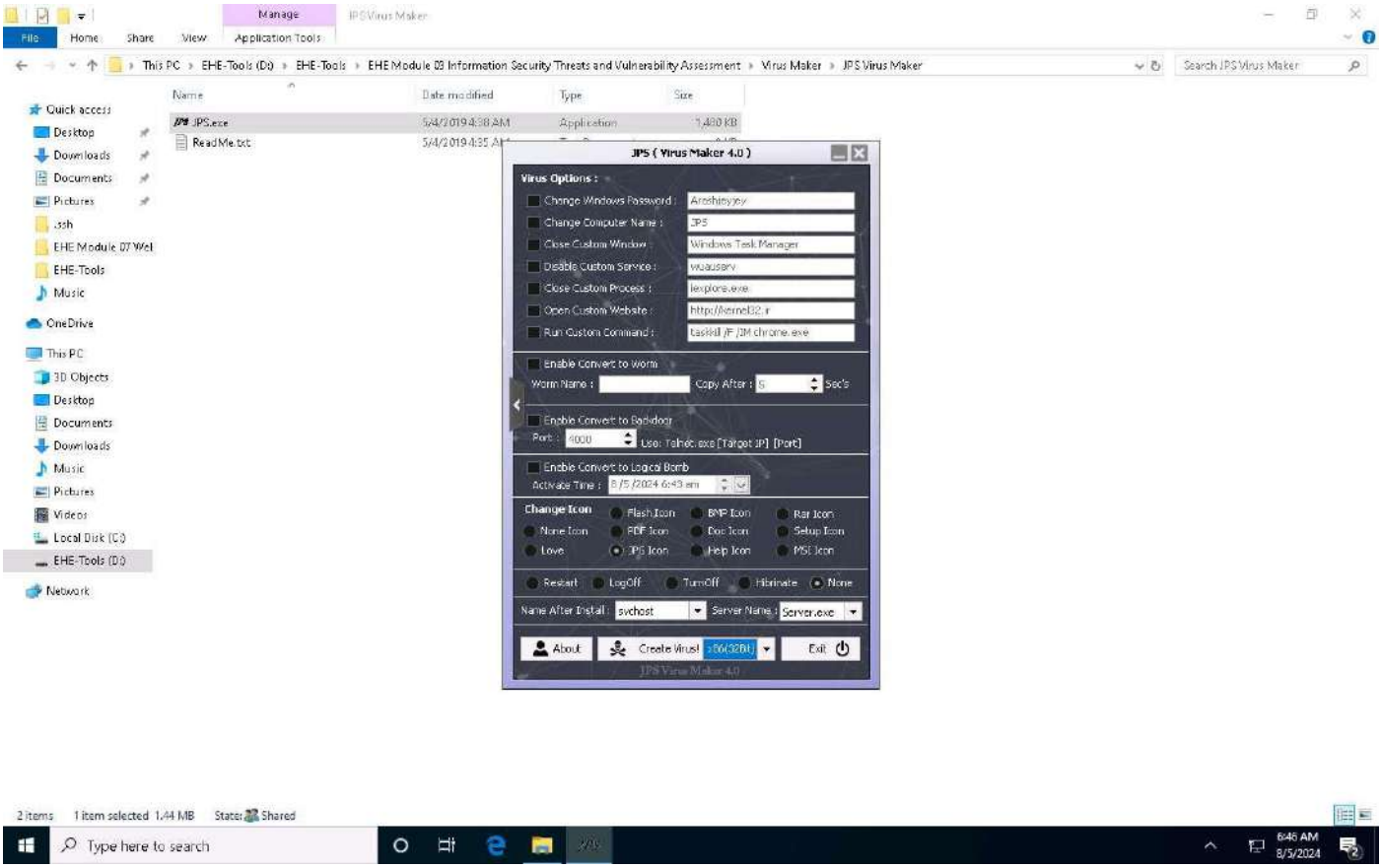


6. Ensure that the **None** radio button is selected to specify the trigger event when the virus should start attacking the system after its creation.

7. Now, before clicking on **Create Virus!**, click the right arrow icon from the right-hand pane of the window to configure the virus options.



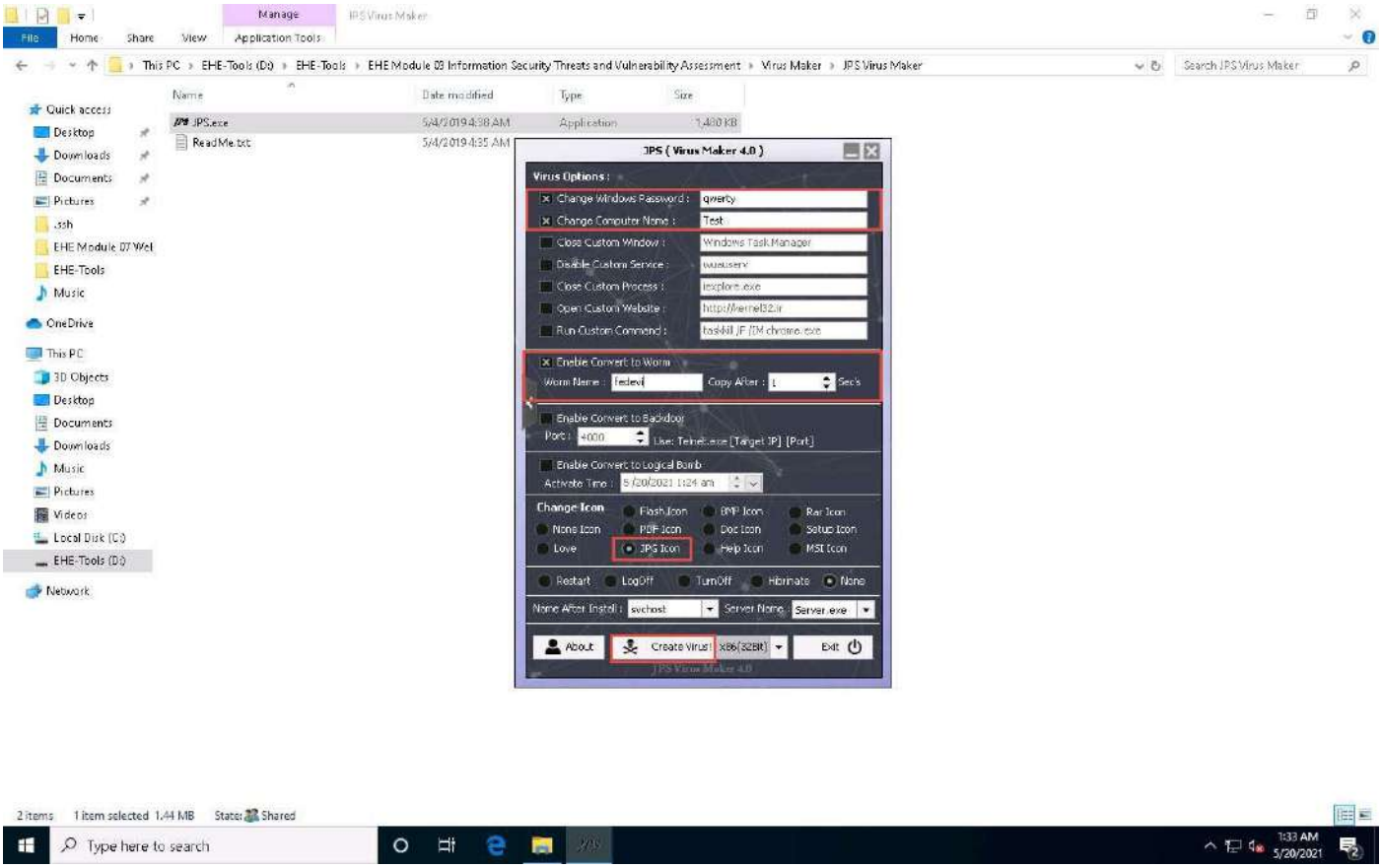
8. A **Virus Options** window appears, as shown in the screenshot.



9. Check the **Change Windows Password** option, and enter a password (here, **qwerty**) in the text field. Check the **Change Computer Name** option, and type **Test** in the text field.

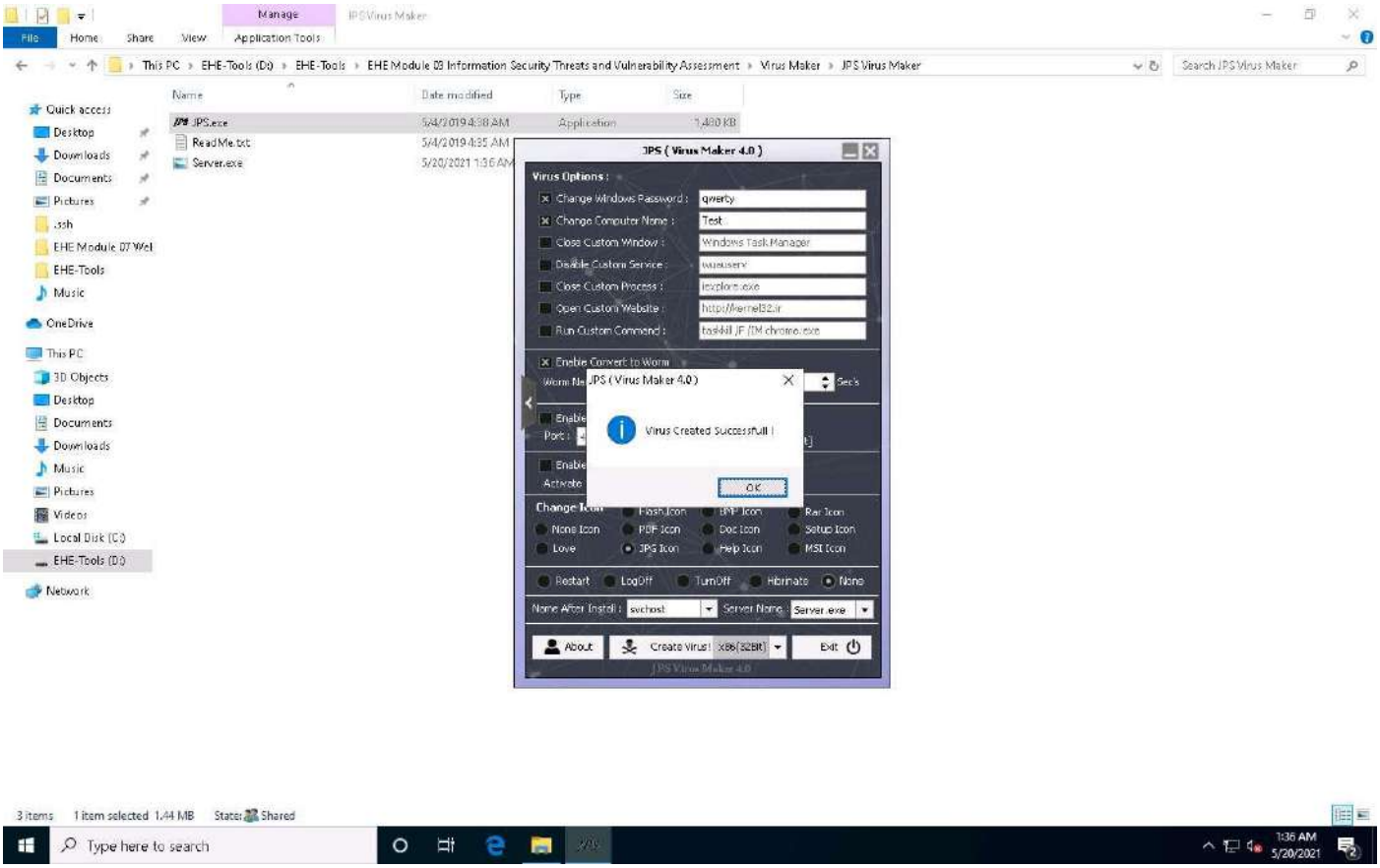
10. You can even configure the virus to convert to a worm. To do this, check the **Enable Convert to Worm** checkbox, and provide a **Worm Name** (here, **fedevi**). For the worm to self-replicate after a particular time, specify the time in seconds (here, **1 second**) in the **Copy After** field.

11. Ensure that the **JPG Icon** radio button is selected under the **Change Icon** section. Ensure that the **None** radio button is selected in the lower part of the window.



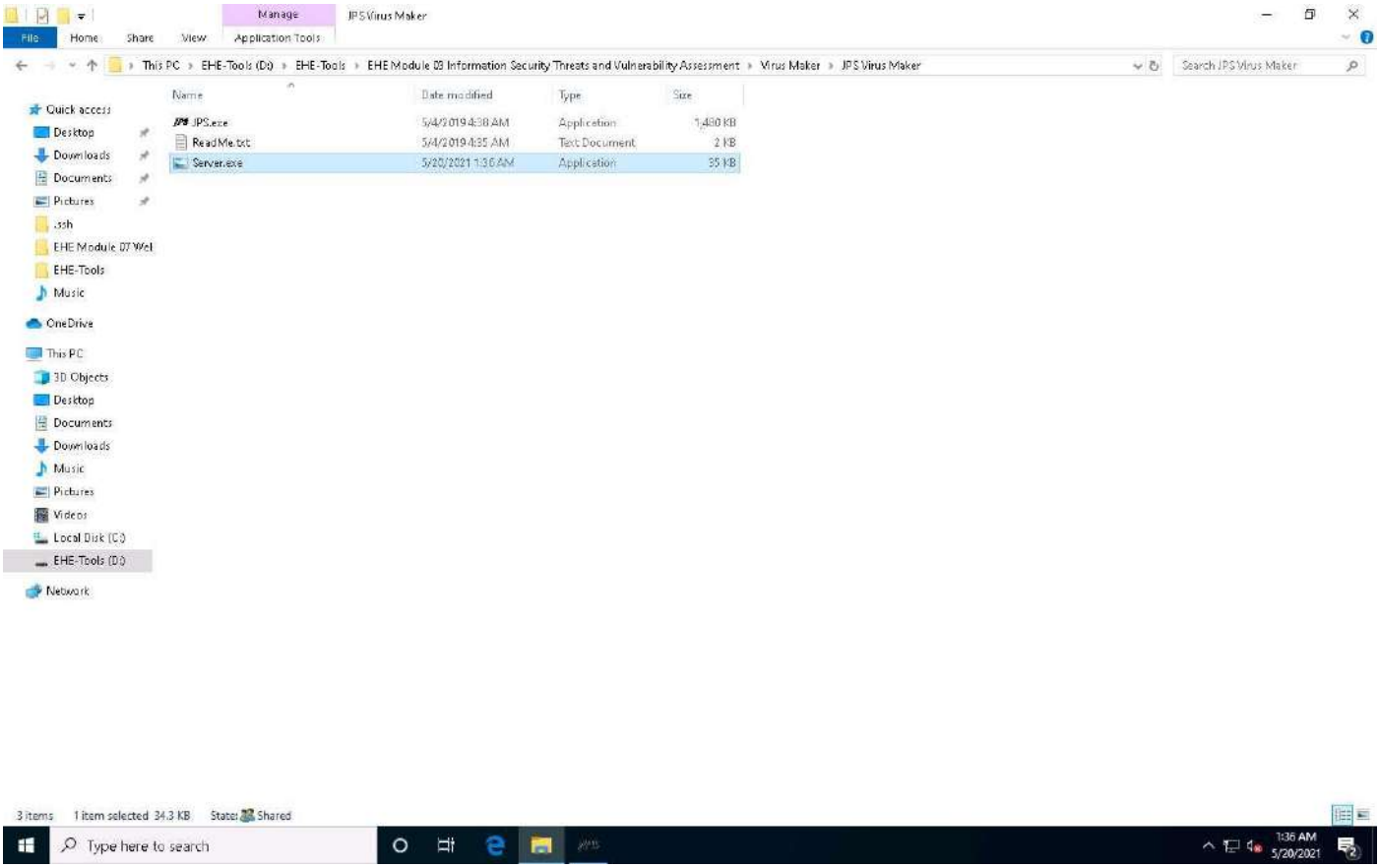
12. After completing your selection of options, click the drop-down icon next to the **Create Virus!** button and select **x86(32Bit)**; click **Create Virus!**

13. A **Virus Created Successful!** pop-up appears; click **OK**.



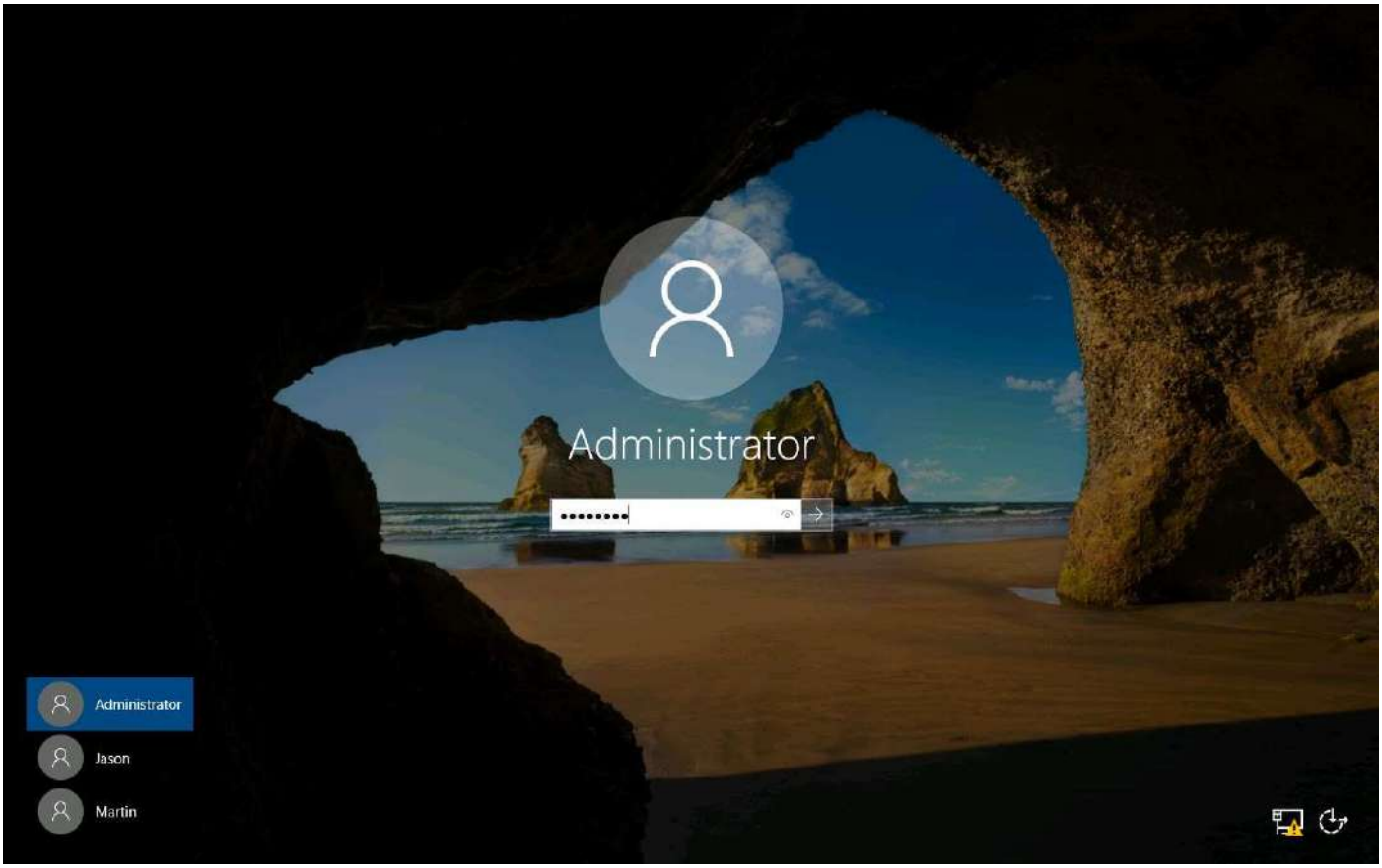
14. The newly created virus (server) is placed automatically in the **folder** where jps.exe is located, but with the name **Server.exe**. Navigate to **D:\EHE-Tools\EHE Module 03 Information Security Threats and Vulnerability**

Assessment\Virus Maker\JPS Virus Maker and observe that the newly created virus with the name **Server.exe** is available at the specified location.

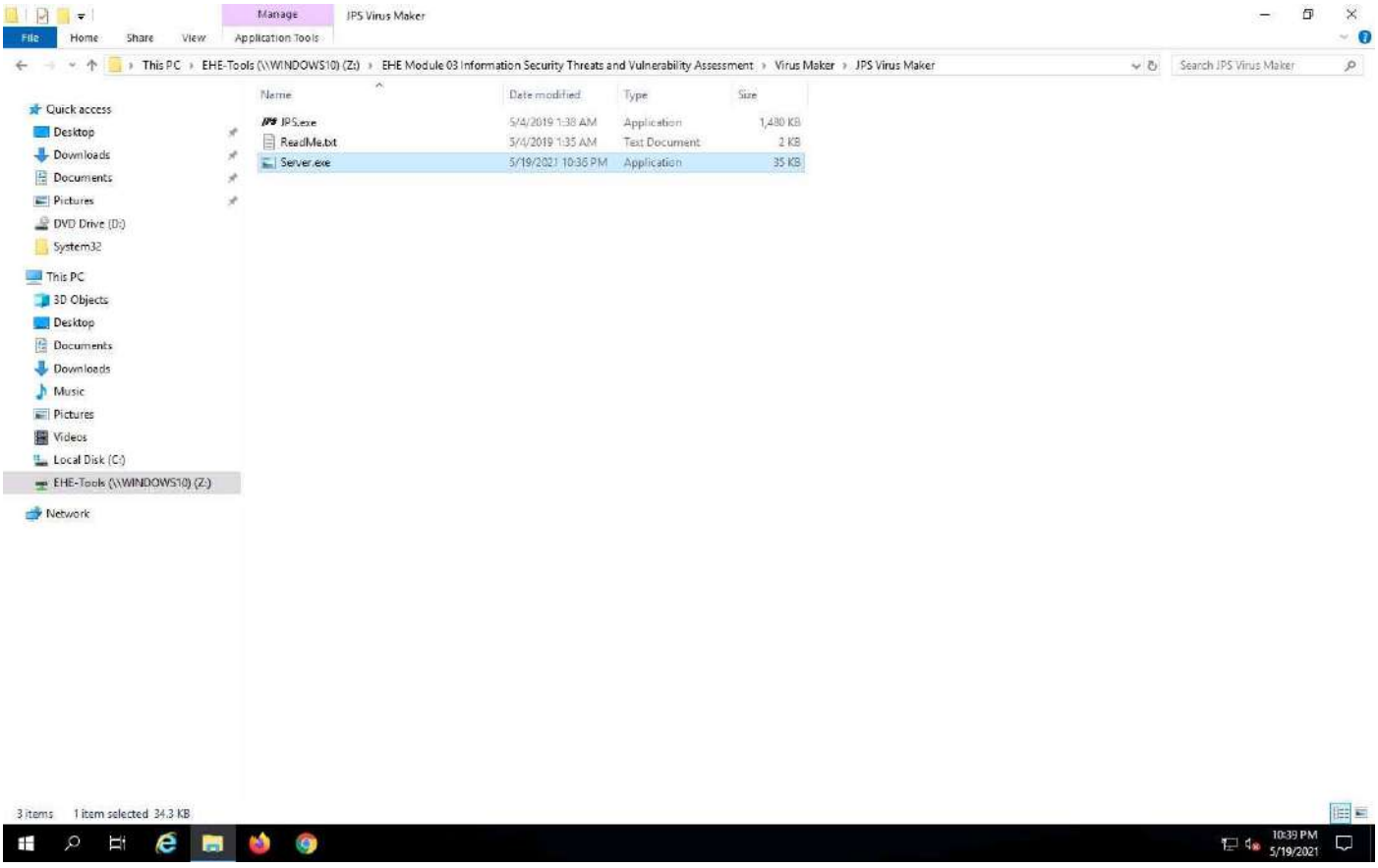


15. Now, pack this virus with a binder or virus packager and send it to the victim machine through email, chat, a mapped network drive, or other method.
16. In this task, we are using a mapped network drive to share the virus file to the victim machine. Assume that you are a victim and that you have received this file.
17. Click Windows Server 2019 to switch to the **Windows Server 2019** machine. Click Ctrl+Alt+Delete to activate the machine, by default, **Administrator** account is selected, click Pa$$w0rd to enter the password and press **Enter**.

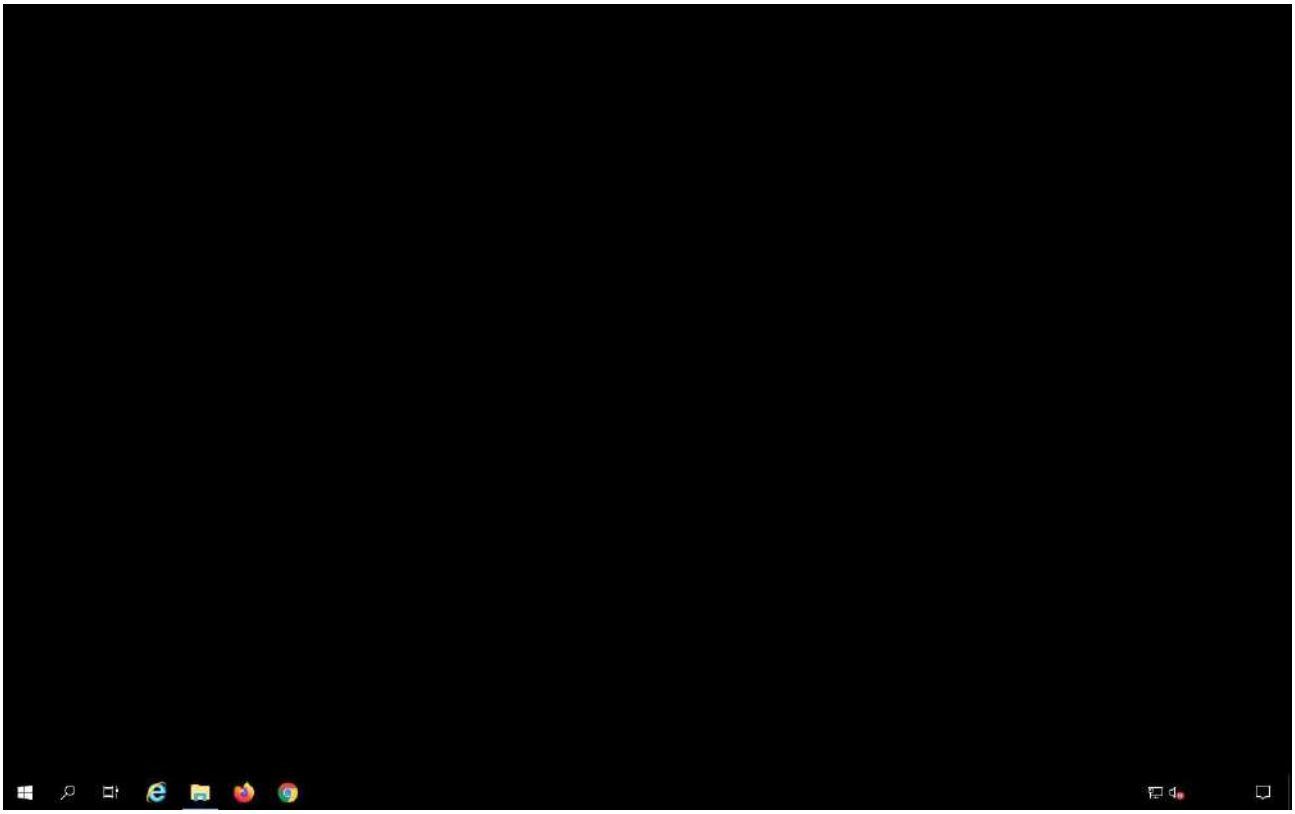
Here, we are logging into the machine as a victim.



18. Navigate to **Z:\EHE Module 03 Information Security Threats and Vulnerability Assessment\Virus Maker\JPS Virus Maker** and double-click **Server.exe** file to execute the virus.

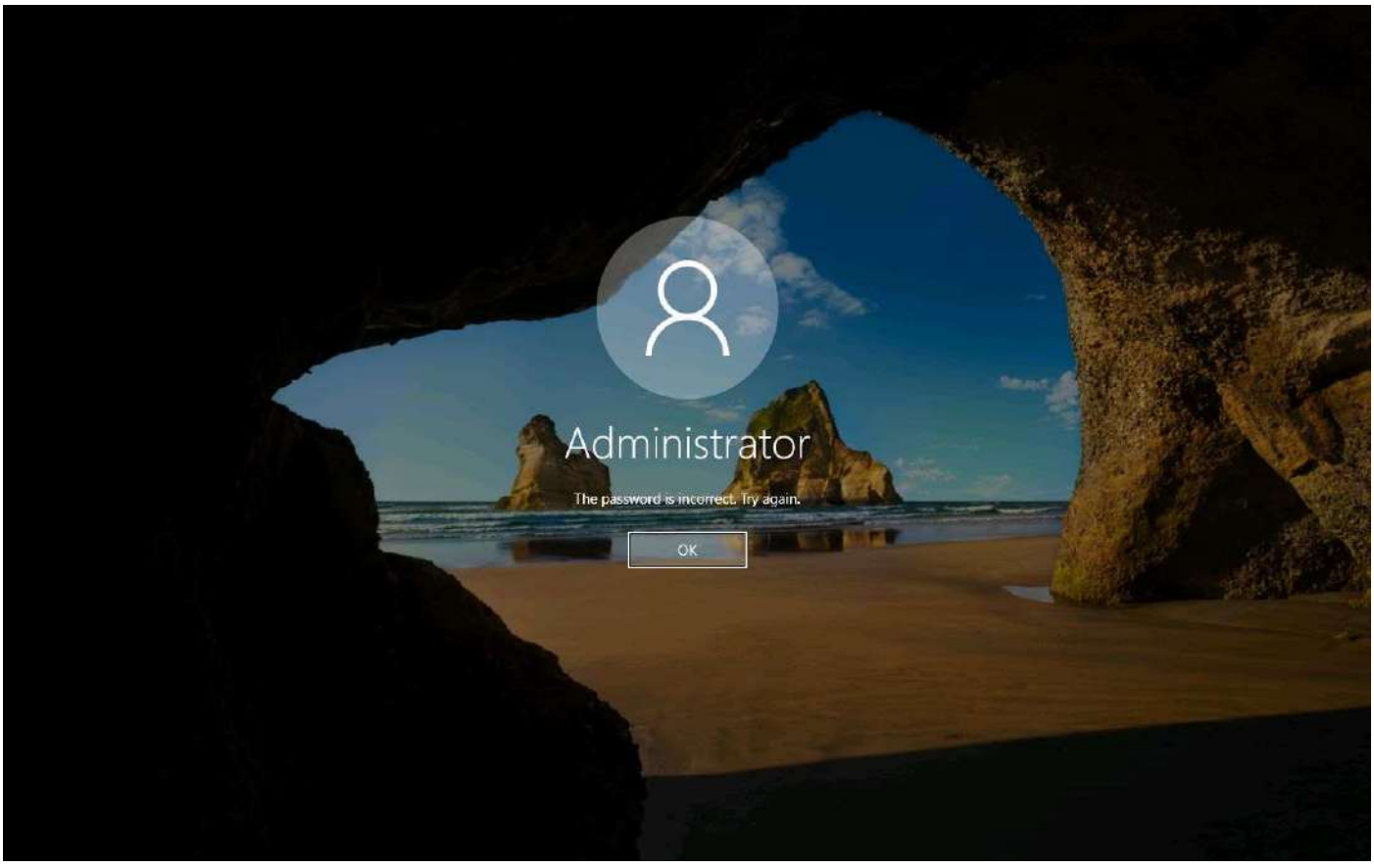


19. Once you have executed the virus, the **Desktop** screen goes blank, indicating that the virus has infected the system, as shown in the screenshot.

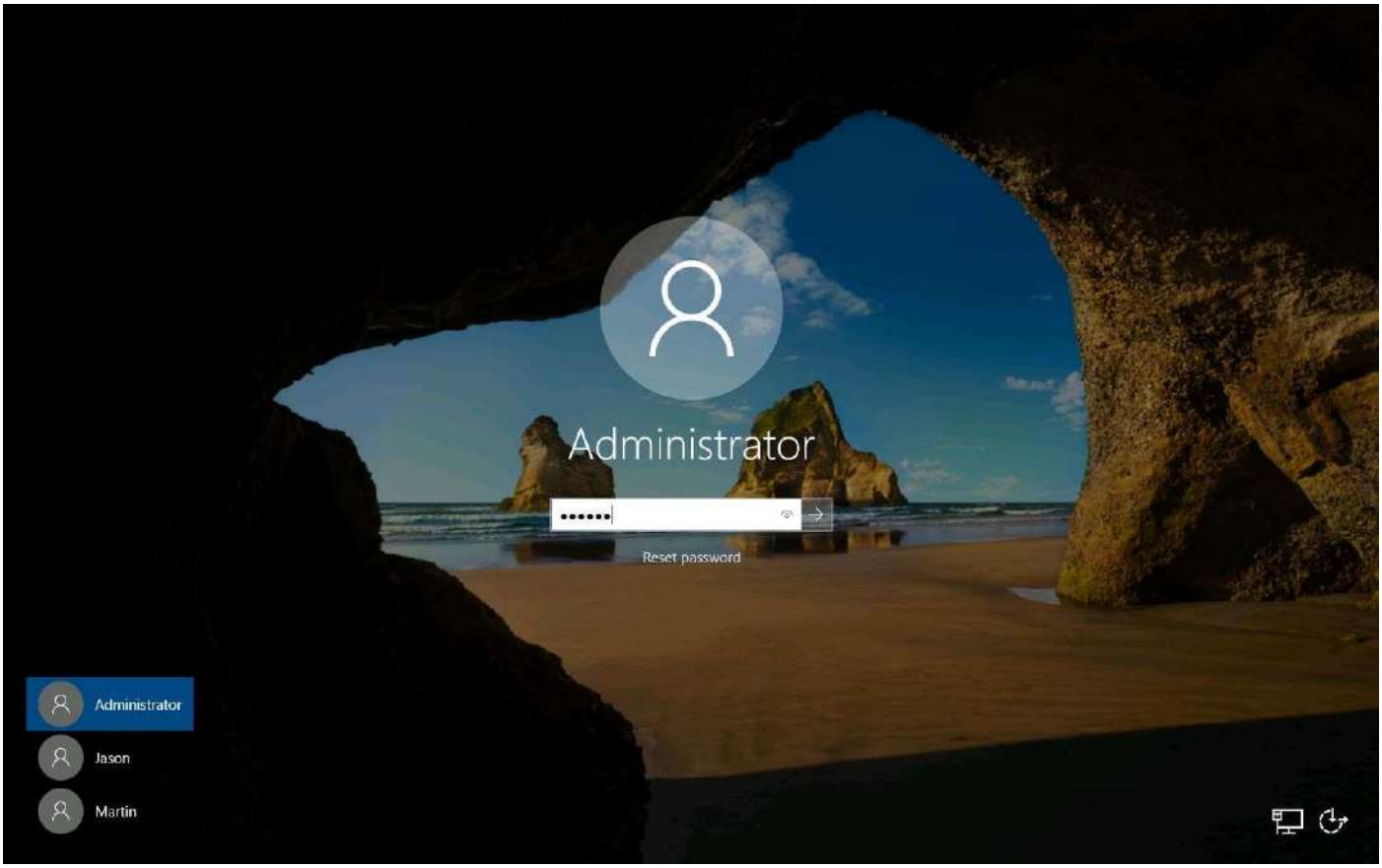


20. Surprised by the system behavior, the victim (you) attempts to fix the machine by restarting it. Once the machine has rebooted, try to log in to the machine with the provided **Username** and **Password**. You should receive the error message "The password is incorrect. Try again."

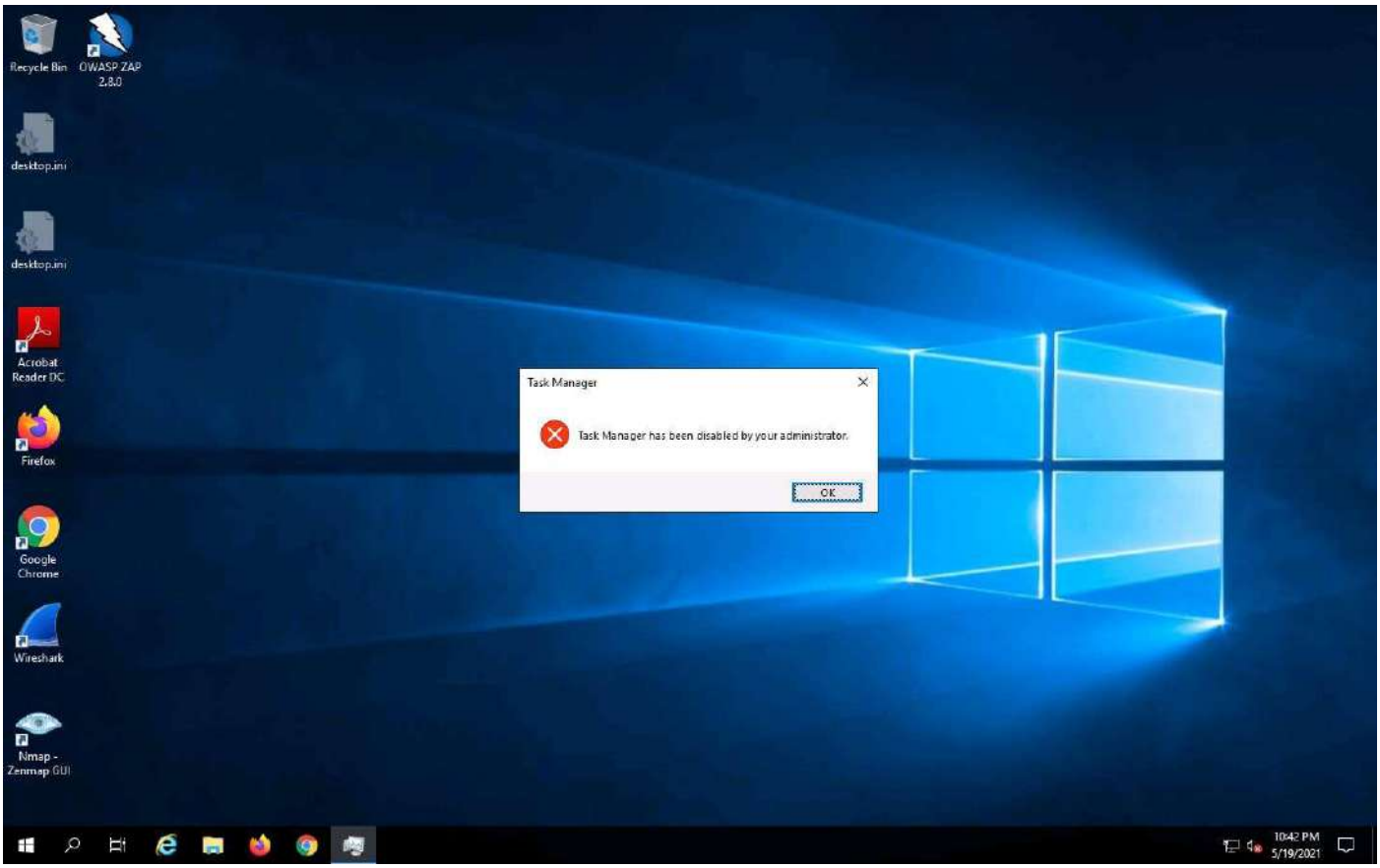
21. Click Ctrl+Alt+Delete to activate the machine, by default, **Administrator** account is selected, click Pa$$w0rd to enter the password and press **Enter**.



22. Now, login with the password that you provided at the time of virus creation (i.e., **qwerty**). You should log in to the machine with the new password.



23. Now, try to open **Task Manager**; observe that an opening error pop-up appears, and then click **OK**.



24. You will get a similar error for all the applications that are disabled by the virus.
25. This is how attackers infect a system with viruses. Now, before going to the next task, **End** the lab and re-launch it to reset the machines.

Lab 3-3: Perform Vulnerability Assessment to Identify Security Vulnerabilities in the Target System or Network

Lab Scenario

The information gathered in the previous labs might not be sufficient to reveal potential vulnerabilities of the target: there could be more information available that may help in finding loopholes. As an ethical hacker, you should look for as much information as possible using all available tools. This lab will demonstrate other information that you can extract from the target using various vulnerability assessment tools.

Lab Objectives

- Perform Vulnerability Analysis using OpenVAS

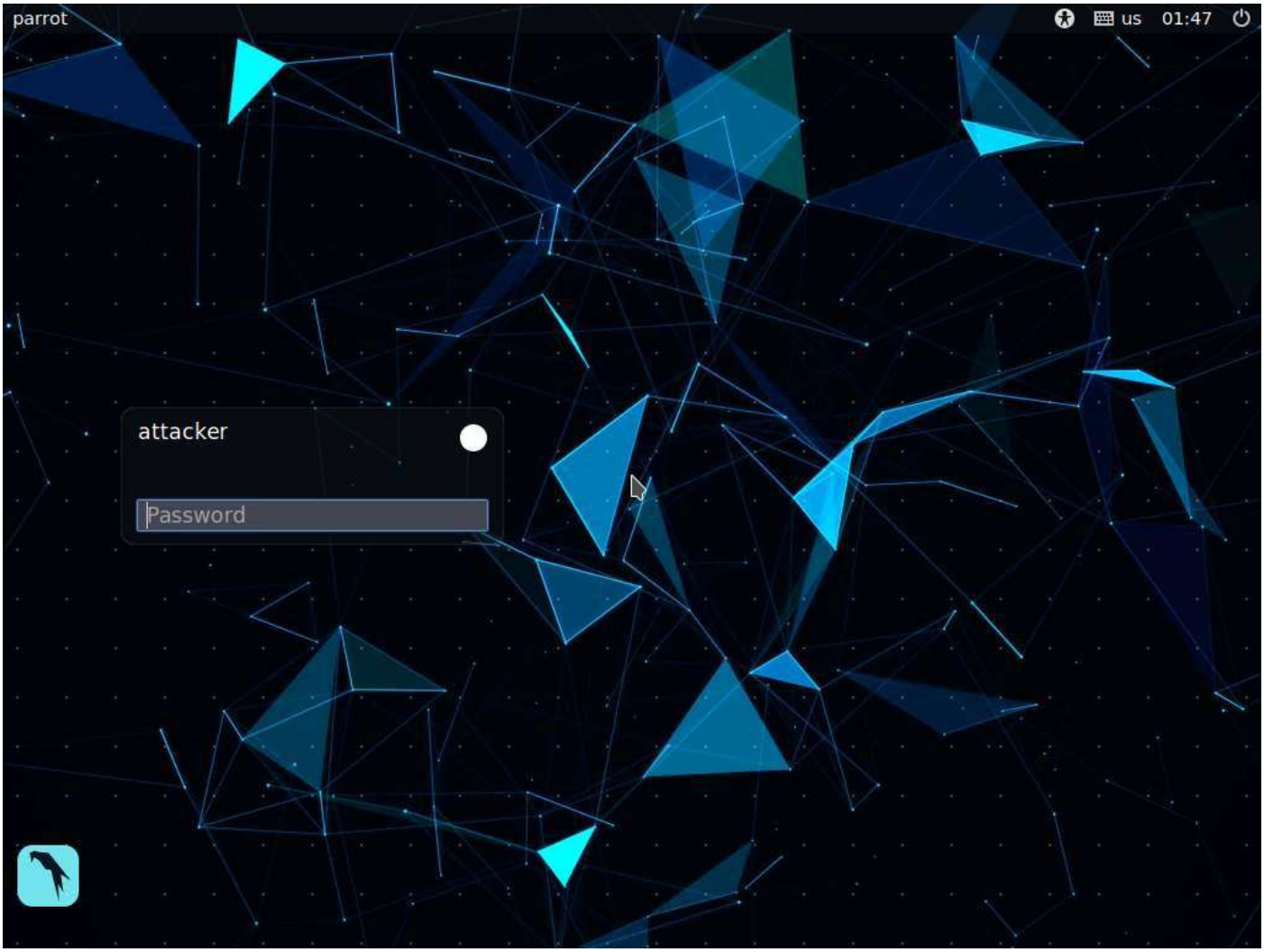
Task 1: Perform Vulnerability Analysis using OpenVAS

OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. Its capabilities include unauthenticated testing, authenticated testing, various high level and low-level Internet and industrial protocols, performance tuning for large-scale scans, and a powerful internal programming language to implement any vulnerability test. The actual security scanner is accompanied with a regularly updated feed of Network Vulnerability Tests (NVTs)—over 50,000 in total.

Here, we will perform a vulnerability analysis using OpenVAS.

In this task, we will use the **Parrot Security (10.10.1.13)** machine as a host machine and the **Windows Server 2016 (10.10.1.16)** machine as a target machine.

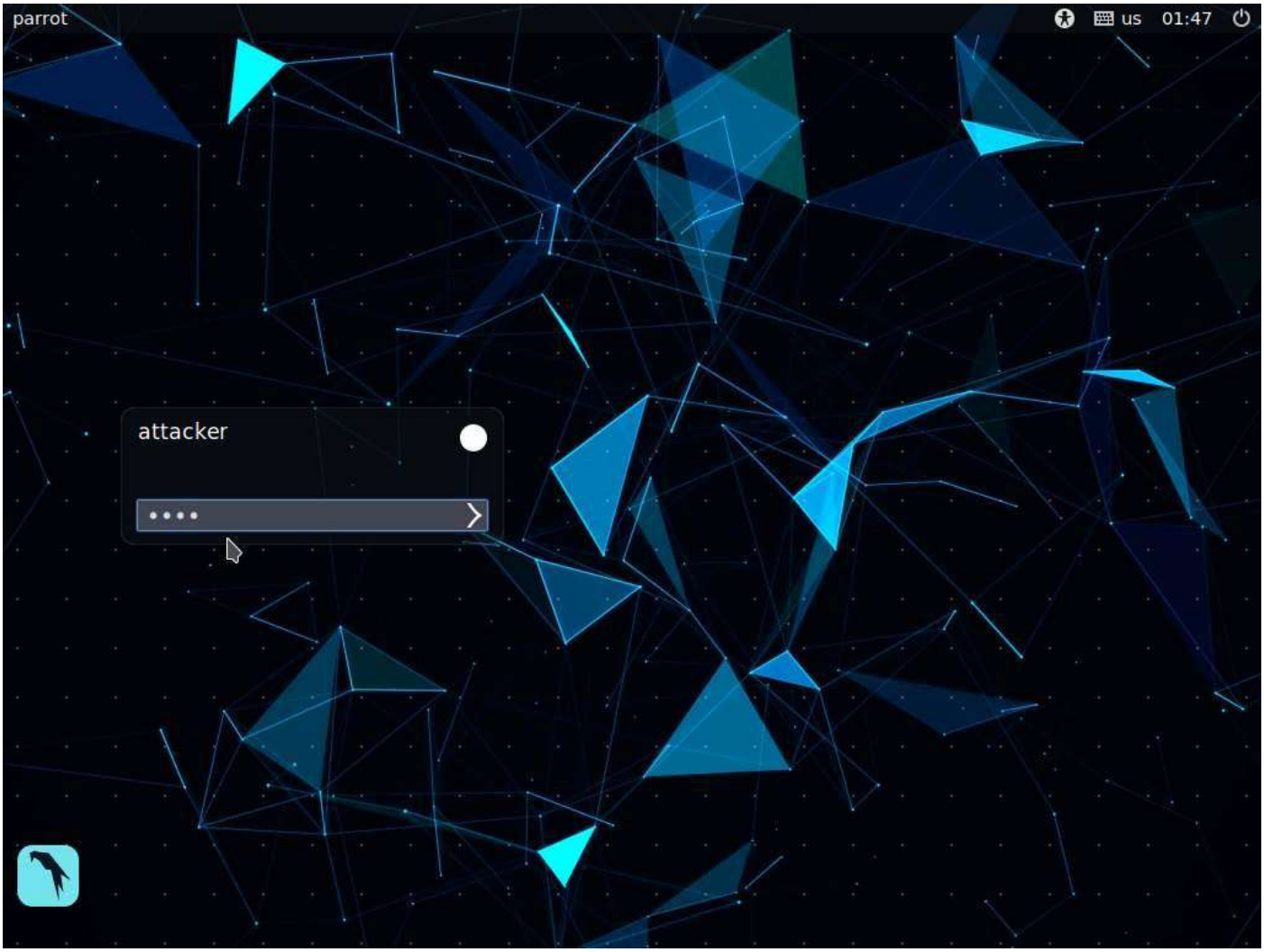
1. Click on Parrot Security to switch to the **Parrot Security** machine.



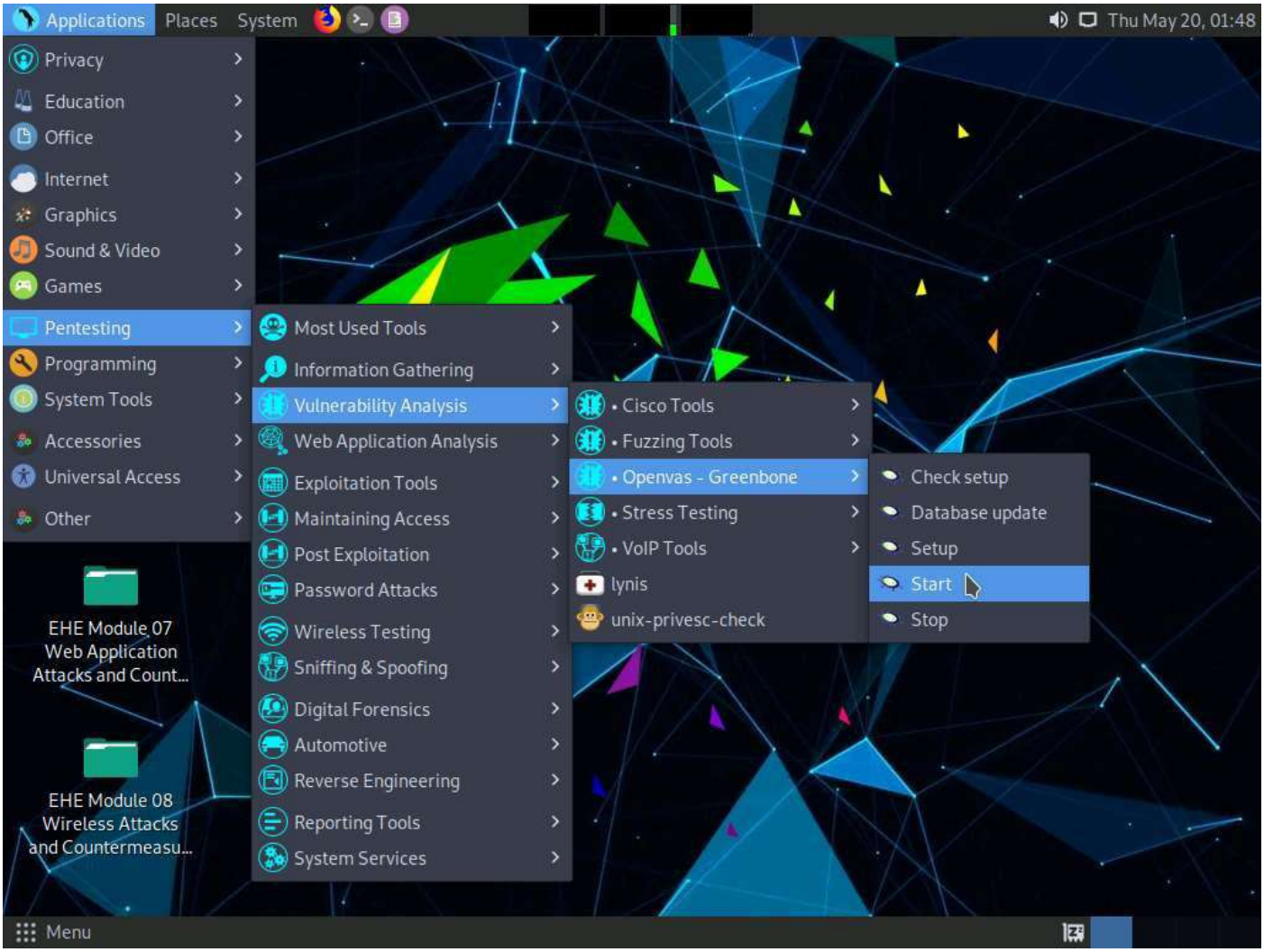
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

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

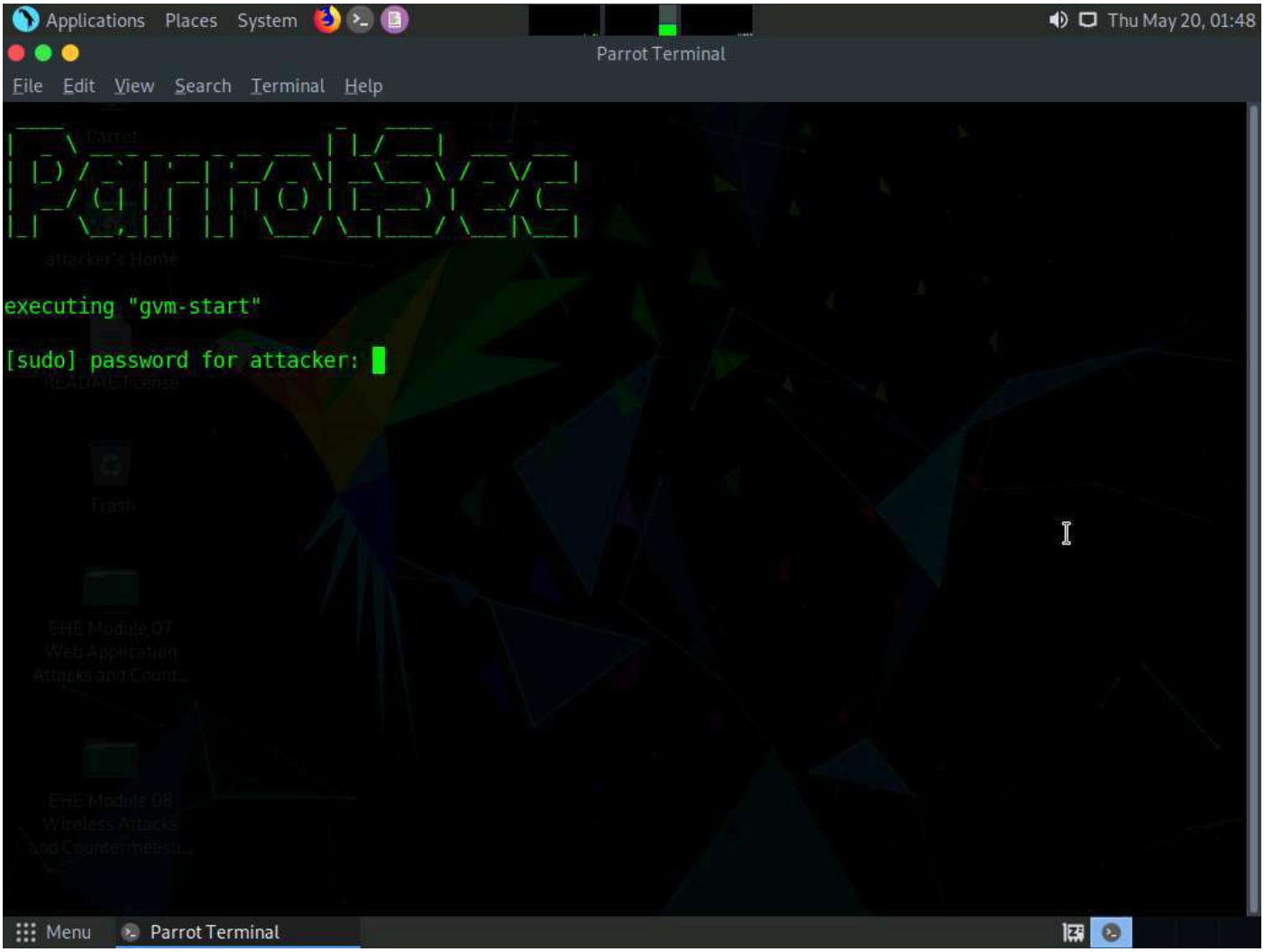


3. Click **Applications** at the top of the **Desktop** window and navigate to **Pentesting** --> **Vulnerability Analysis** --> **Openvas - Greenbone** --> **Start** to launch OpenVAS tool.

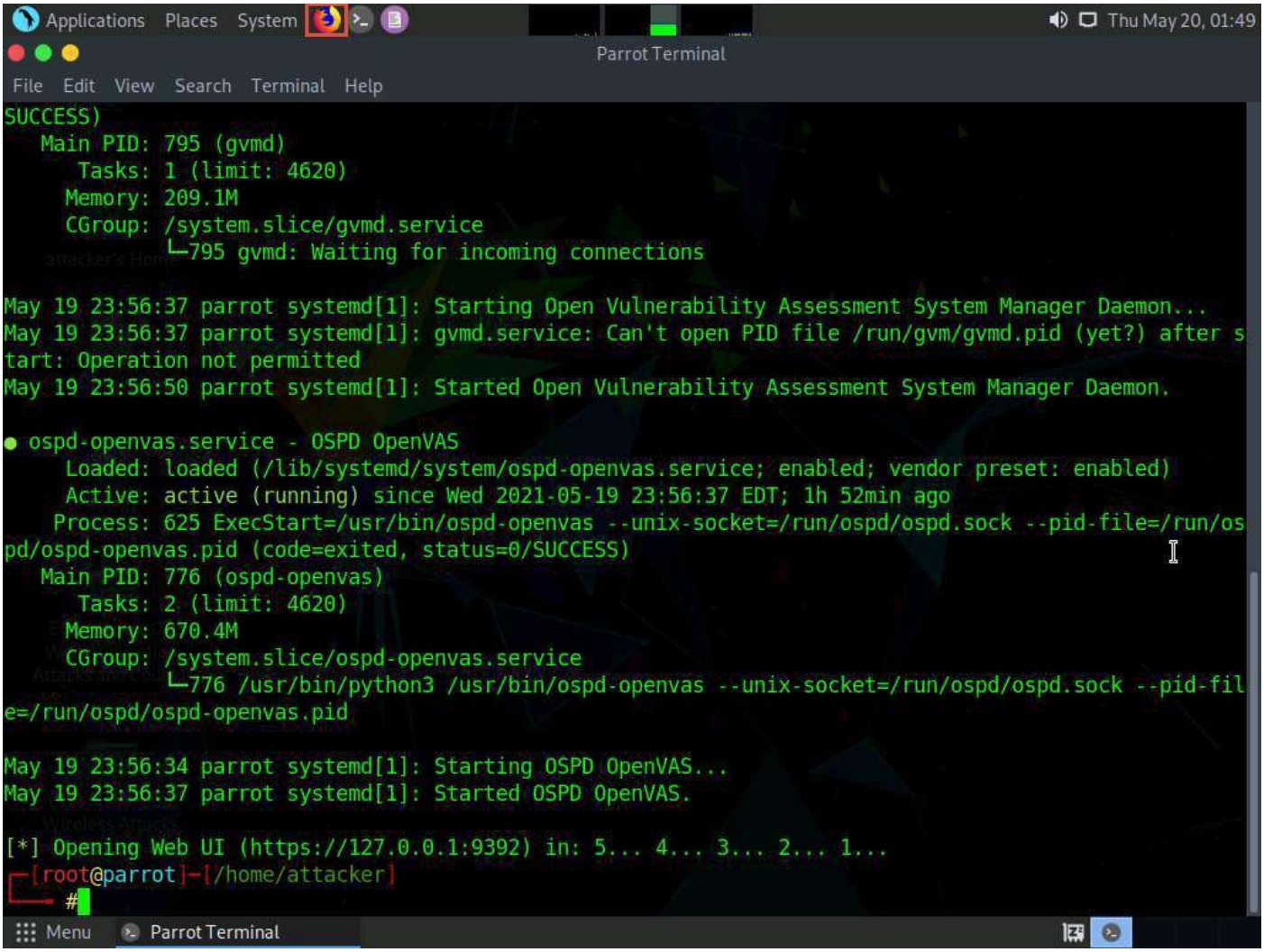


4. A terminal window appears, in the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. OpenVAS initializes.

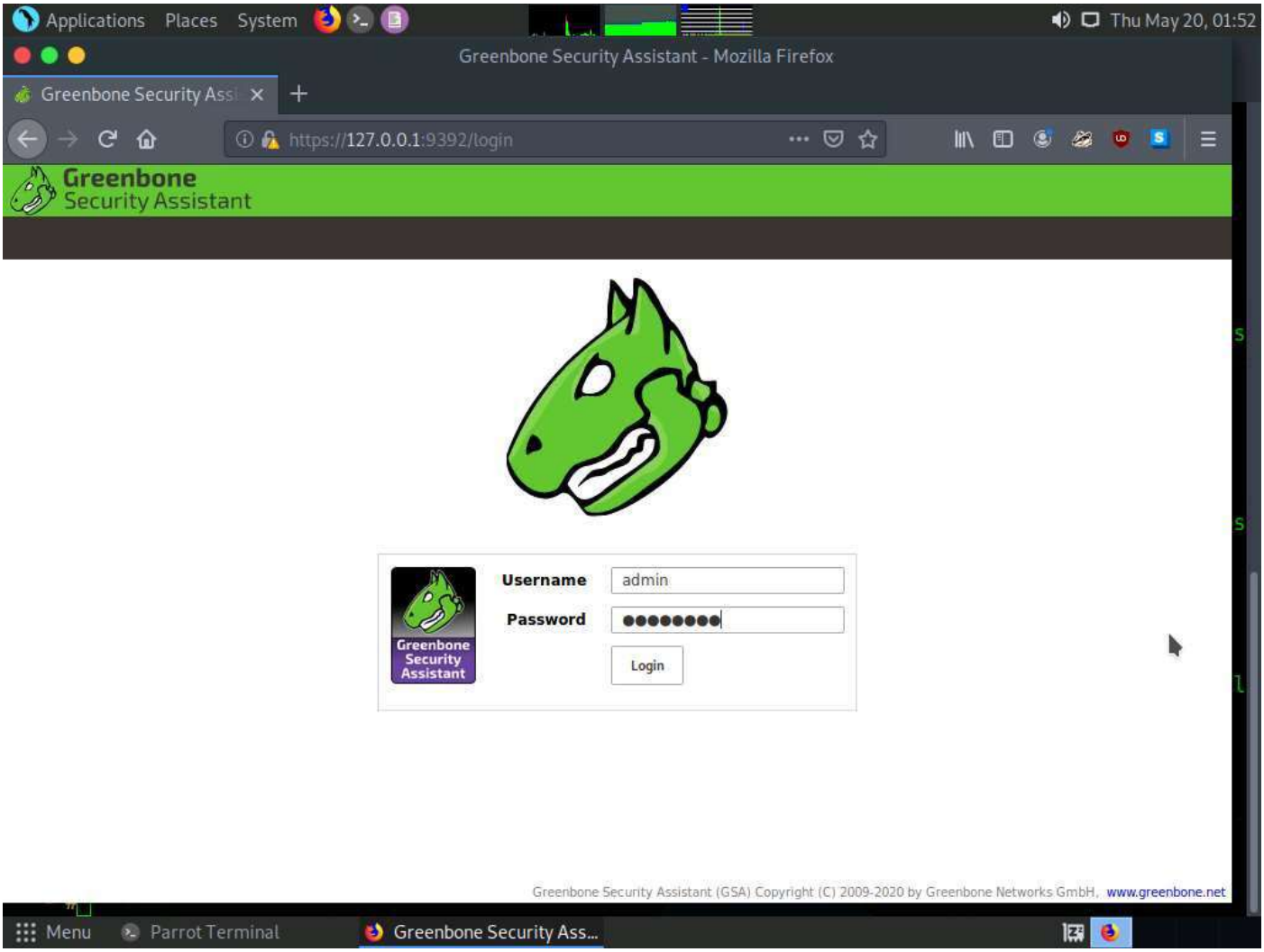
The password that you type will not be visible.



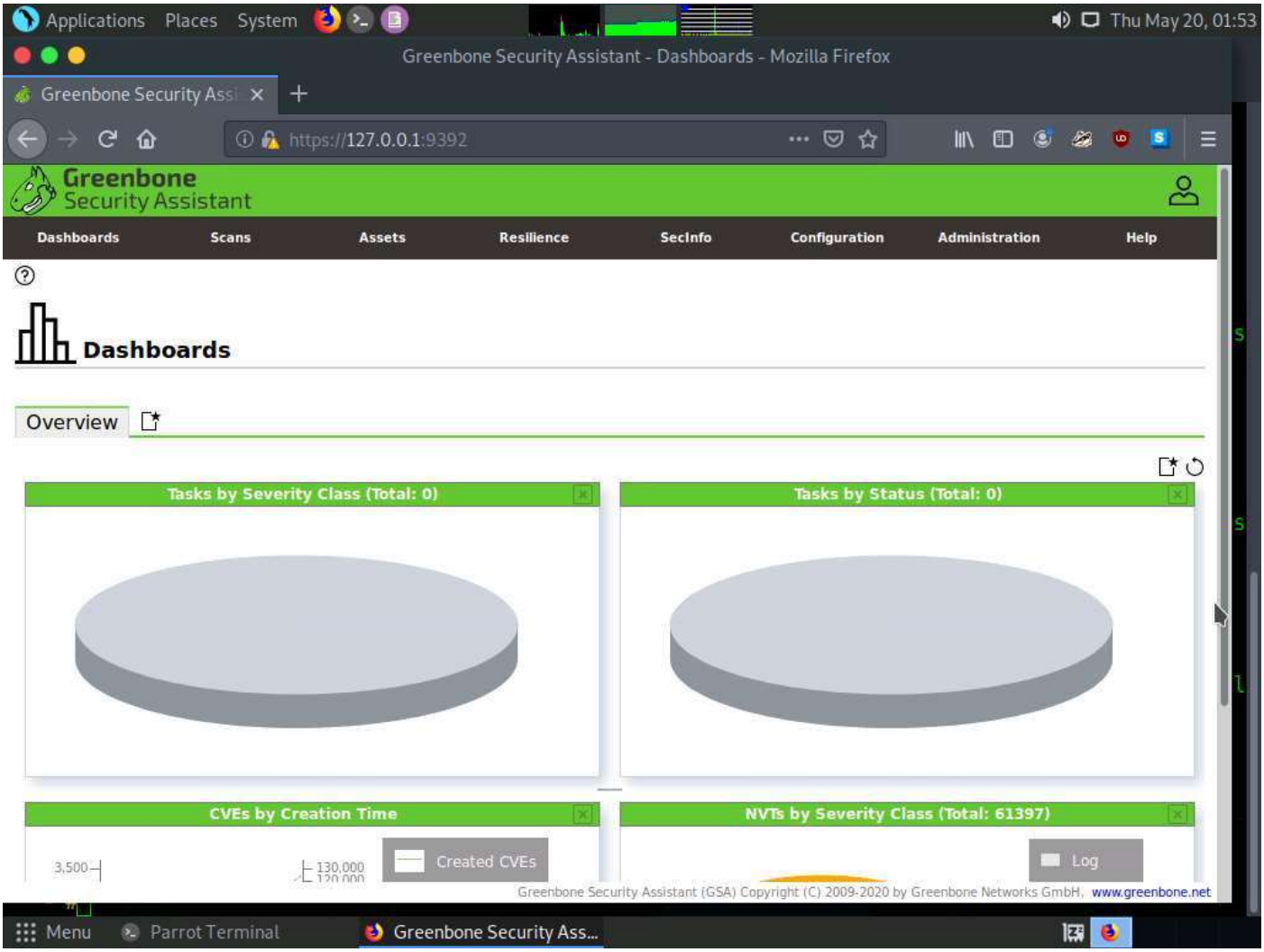
5. After the tool initializes, click **Firefox** icon from the top-section of the **Desktop**.



6. The **Firefox** browser appears, in the address bar, type **https://127.0.0.1:9392** and press **Enter**.
7. OpenVAS login page appears, log in with **Username** and **Password** as **admin** and **password** and click the **Login** button.

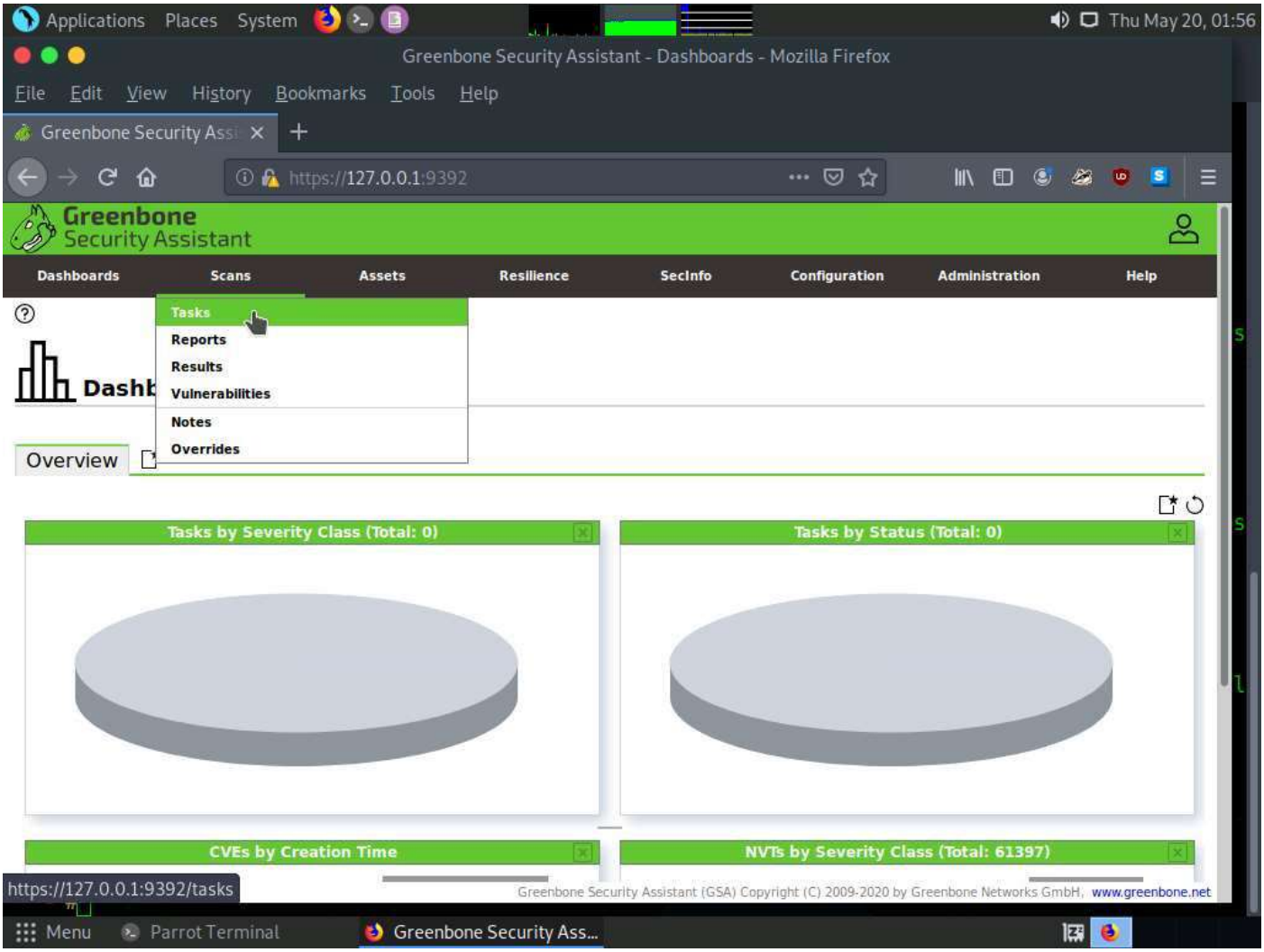


8. **OpenVAS Dashboards** appears, as shown in the screenshot.

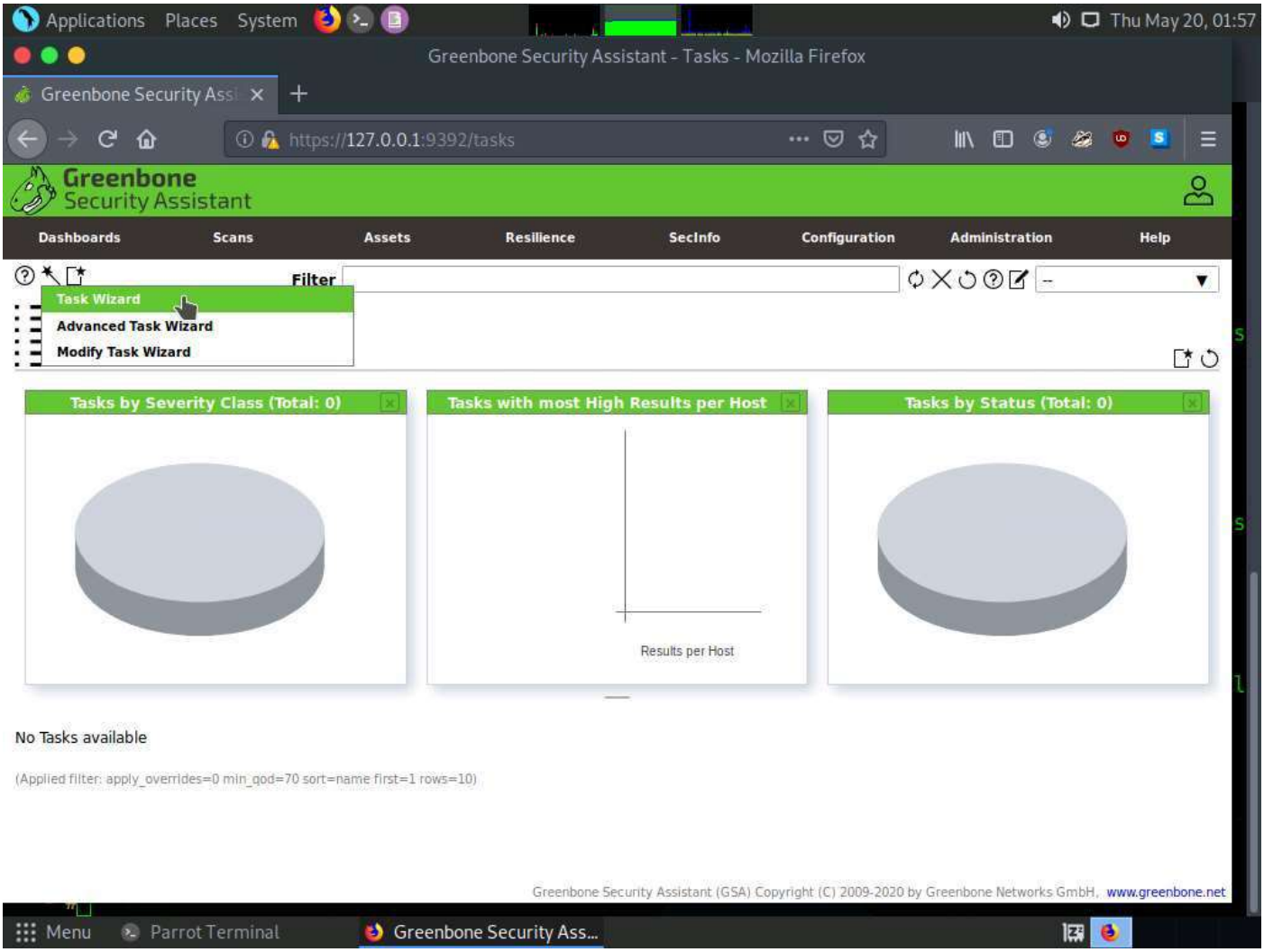


9. Navigate to **Scans --> Tasks** from the **Menu** bar.

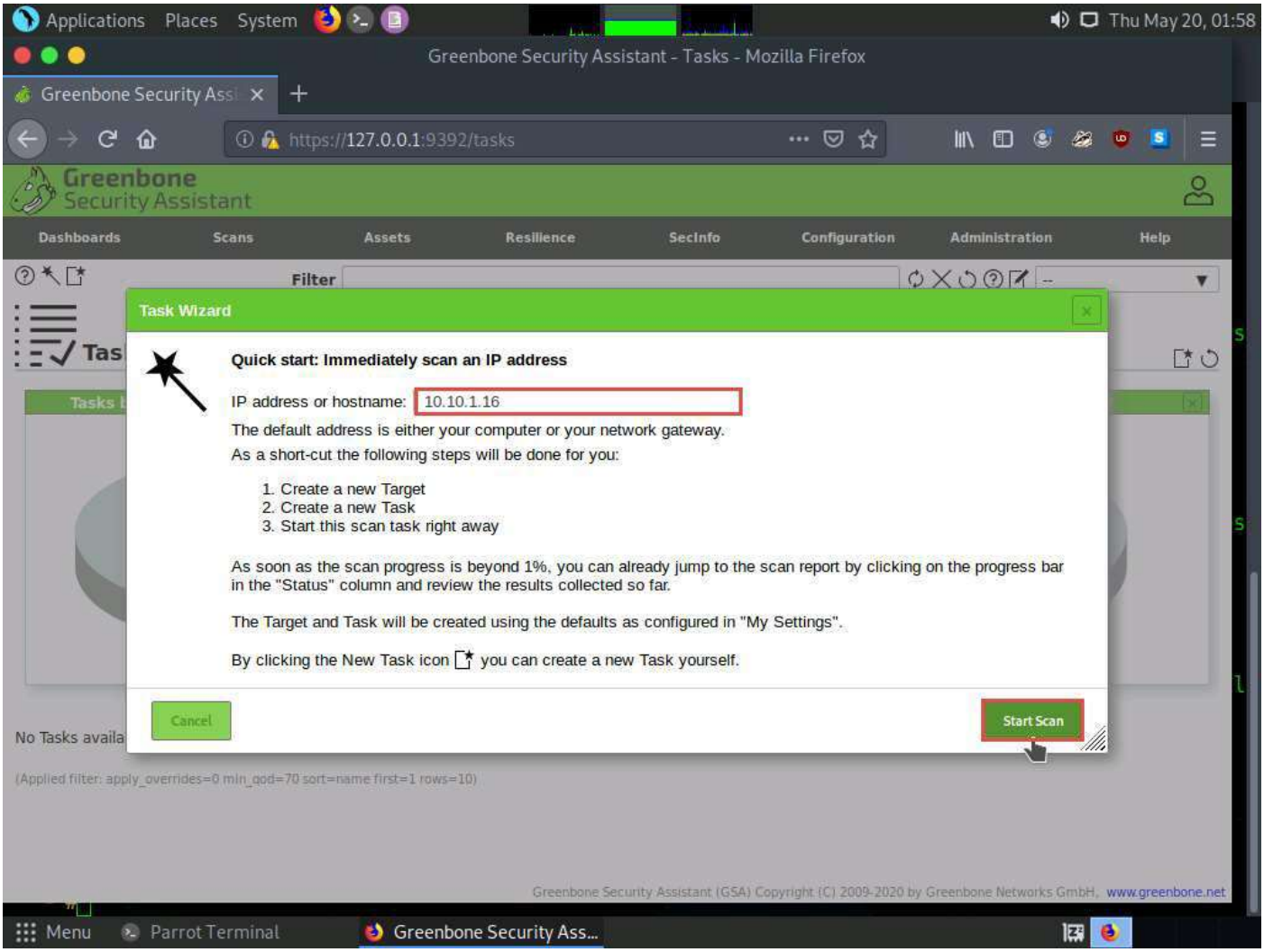
If a **Welcome to the scan management!** pop-up appears, close it.



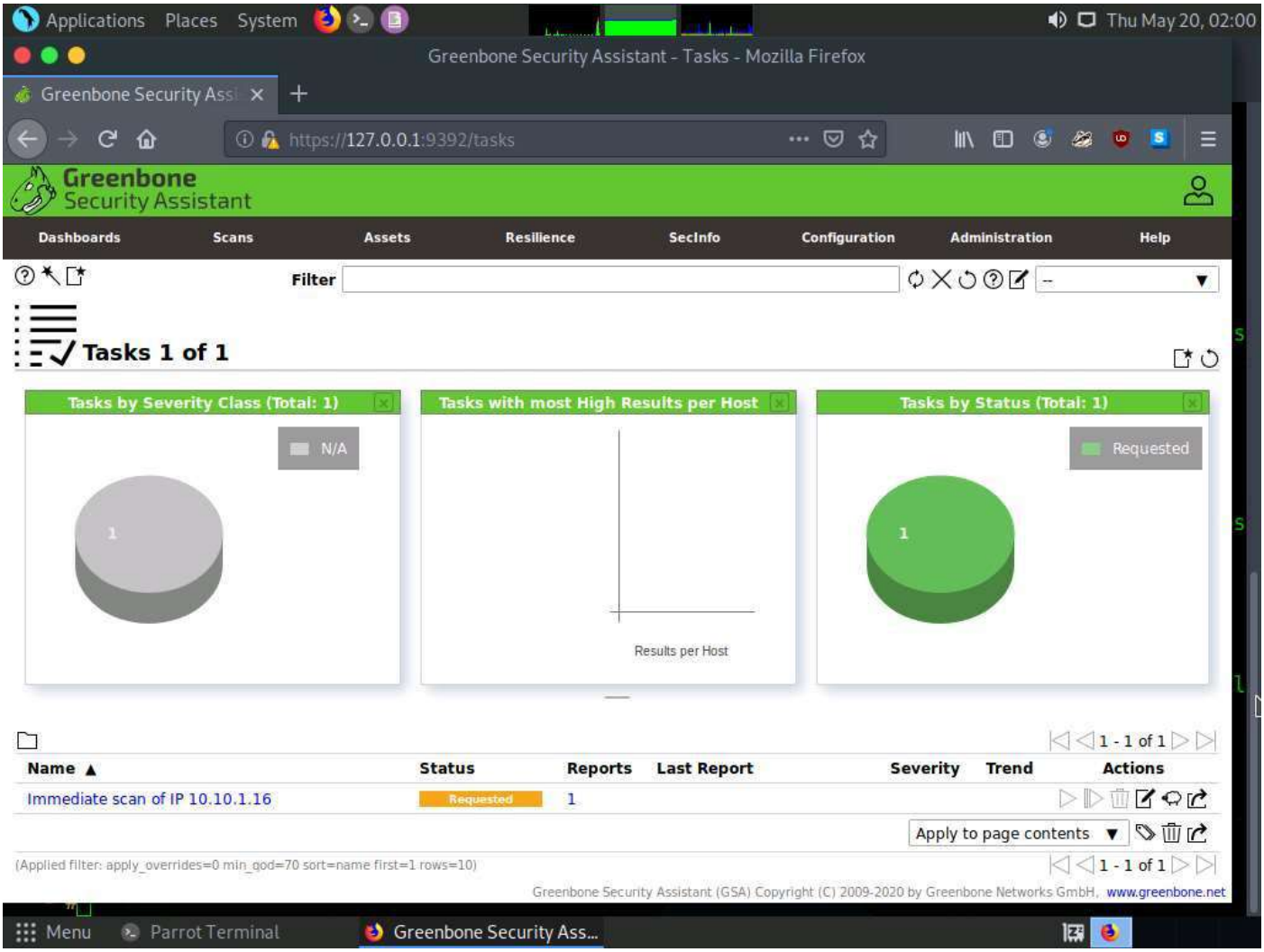
10. Hover over wand icon and click the **Task Wizard** option.



11. The **Task Wizard** window appears; enter the target IP address in the **IP address or hostname** field (here, the target system is **Windows Server 2016 [10.10.1.16])** and click the **Start Scan** button.

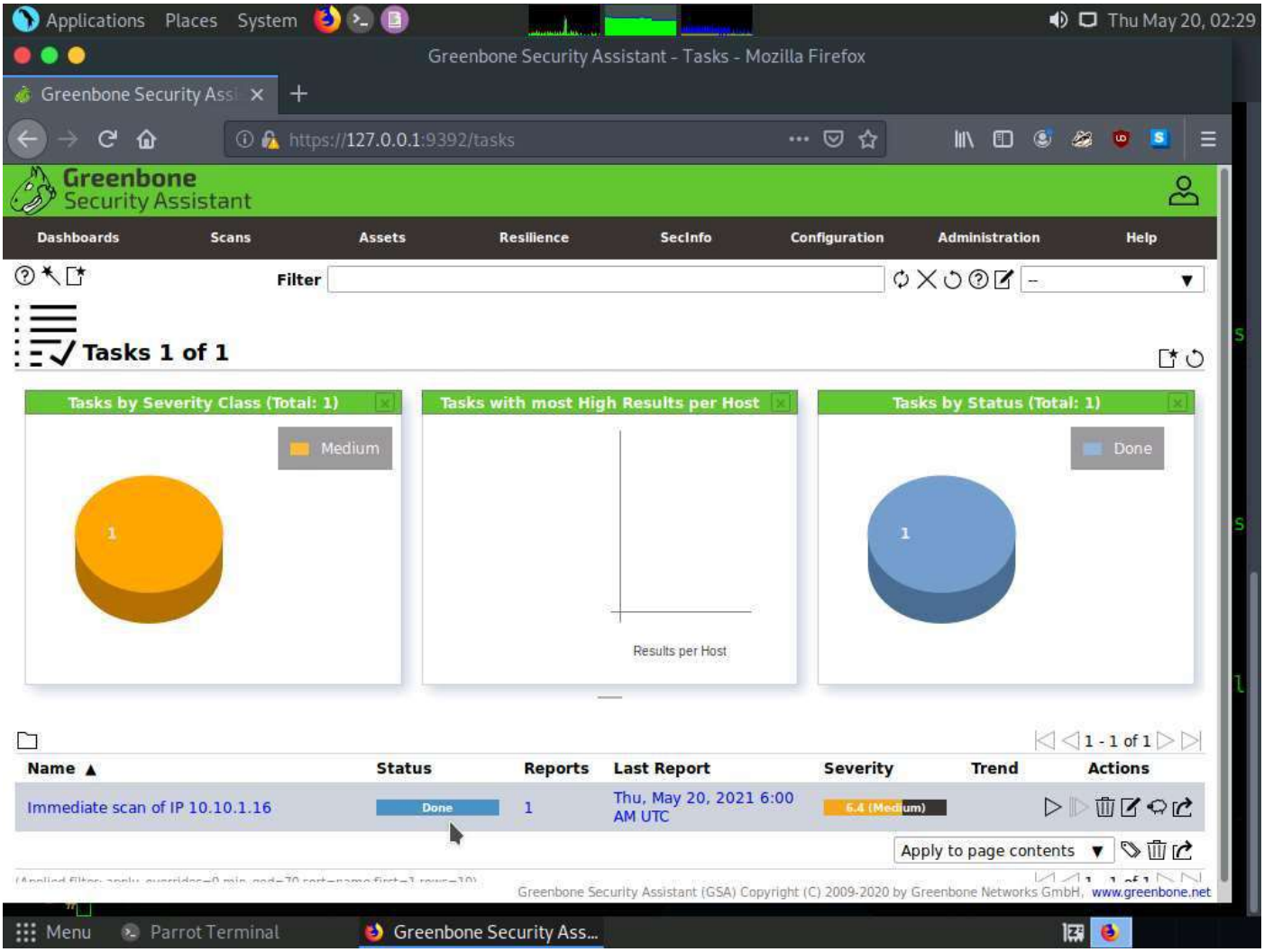


12. The task appears under the **Tasks** section; OpenVAS starts scanning the target IP address.



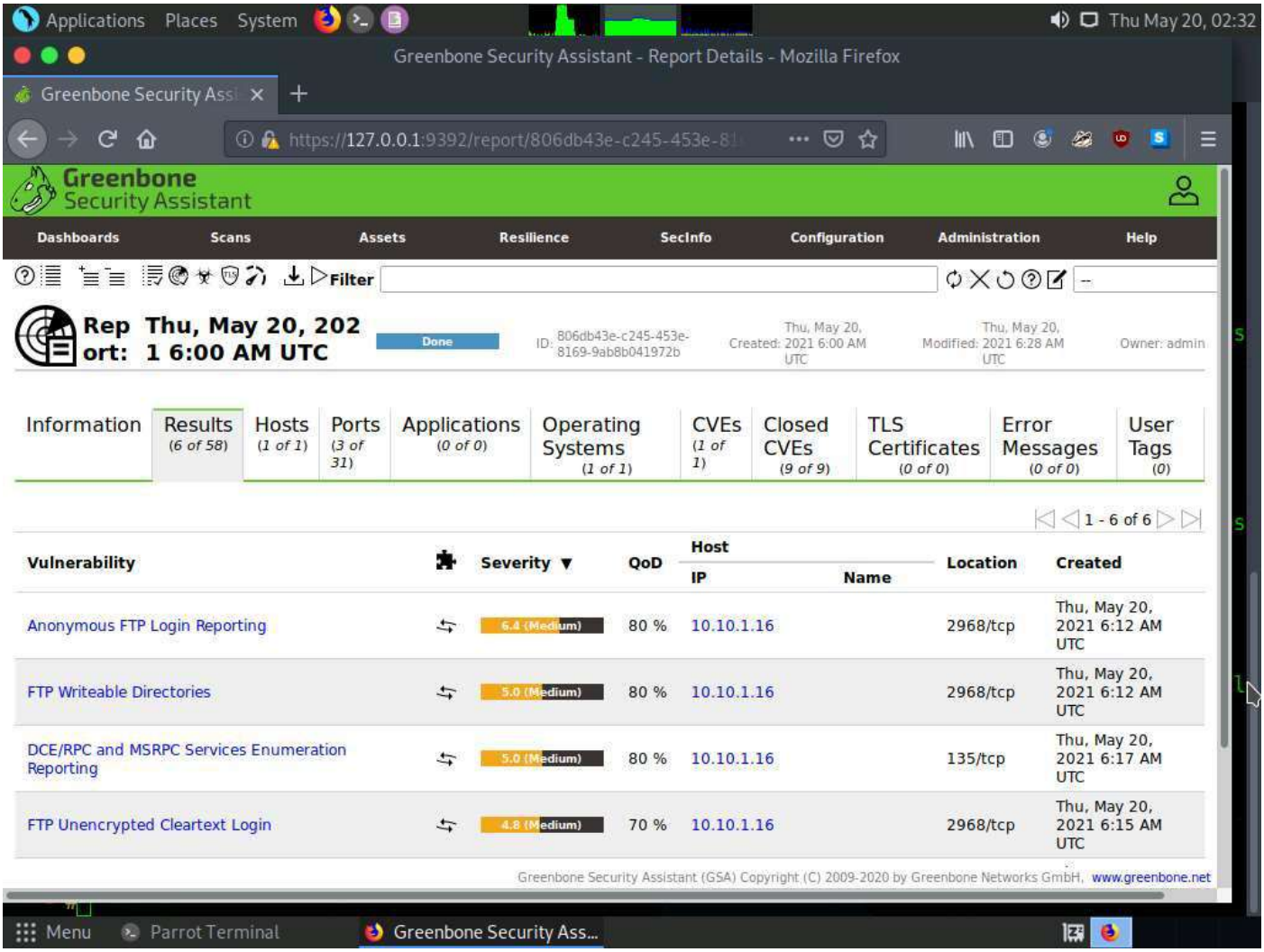
13. Wait for the **Status** to change from **Requested** to **Done**. Once it is completed, click the **Done** button under the **Status** column to view the vulnerabilities found in the target system.

If you are logged out of the session then login again using credentials **admin/password**.



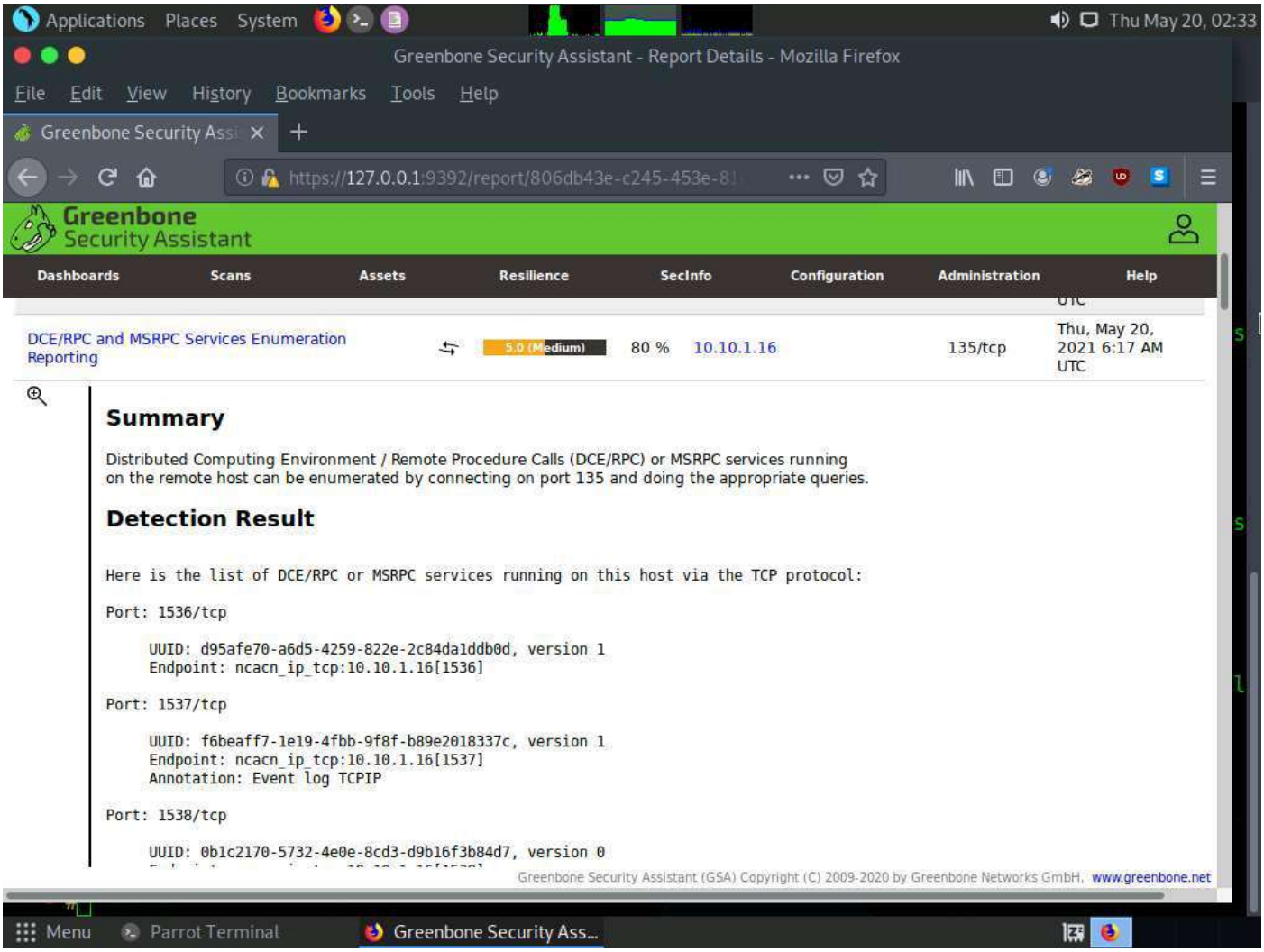
14. **Report: Information** appears, click **Results** tab to view the discovered vulnerabilities along with their severity and port numbers on which they are running.

The number of vulnerabilities discovered might vary in your lab environment.



15. Click on any vulnerability under the **Vulnerability** column (here, **DCE/RPC and MSRPC Services Enumeration Reporting** to view its detailed information.

16. Detailed information regarding selected vulnerability appears, as shown in the screenshot.



17. Similarly, you can click other discovered vulnerabilities under the **Report: Results** section to view detailed information regarding the vulnerabilities in the target system.
18. This concludes the demonstration performing vulnerabilities analysis using OpenVAS.
19. Close all open windows and document all the acquired information.

Module 06: Network Level Attacks and Countermeasures

Scenario

Attackers use various attack strategies to compromise the security of a network, potentially causing disruption, damage, and loss to organizations and individuals. Therefore, it is important for security professionals to have an understanding of these attack strategies, because such an understanding is essential for protecting the network from various attacks.

The labs in this module provide real-time experience in performing various network level attacks on the target organization.

Objective

The objective of the lab is to perform network level attacks and other tasks that include, but are not limited to:

- Sniff the network
- Analyse incoming and outgoing packets for any attacks
- Perform DoS attack, DDoS attack and session hijacking
- Secure the network from attacks

Overview of Network Level Attacks

Attackers compromise the security of networks using various techniques such as MAC flooding, ARP poisoning, ARP spoofing, DoS and DDoS attacks, and session hijacking. This allows attackers to capture data packets containing sensitive information such as passwords, account information, syslog traffic, router configuration, DNS traffic, email traffic, web traffic, chat sessions, and FTP passwords.

Using a DoS attack, attackers flood a victim's system with nonlegitimate service requests or traffic to overload its resources and make the system unresponsive, leading to the unavailability of the victim's website or at least significantly reducing the victim's system or network performance.

Further, attackers use session hijacking to take over a valid Transmission Control Protocol (TCP) communication session between two computers and sniff all the traffic from established TCP sessions to perform identity theft, information theft, fraud, etc.

Lab Tasks

We will use numerous tools and techniques to perform network level attacks. Recommended labs that assist in learning various network level attacks techniques include:

1. Perform MAC flooding to compromise the security of network switches
    - Perform MAC flooding using macof
2. Perform ARP poisoning to divert all communication between two machines
    - Perform ARP poisoning using arpspoof
3. Detect ARP attacks using ARP spoofing detection tools to ensure data privacy
    - Detect ARP poisoning in a switch-based network
4. Perform DoS and DDoS attacks using various techniques on a target host to prevents access to system resources for legitimate users
    - Perform a DoS attack on a target host using hping3
    - Perform a DDoS attack using HOIC
5. Detect and protect against DDoS attack
    - Detect and protect against DDoS attack using Anti DDoS Guardian
6. Perform session hijacking to seize control of a valid TCP communication session between two computers
    - Hijack a session using Zed Attack Proxy (ZAP)
7. Detect session hijacking attempts using manual method
    - Detect session hijacking using Wireshark

Lab 6-1: Perform MAC Flooding to Compromise the Security of Network Switches

Lab Scenario

The first step is to perform active sniffing on the target network using various active sniffing techniques such as MAC flooding, DHCP starvation, ARP poisoning, or MITM. In active sniffing, the switched Ethernet does not transmit information to all systems connected through the LAN as it does in a hub-based network.

In active sniffing, ARP traffic is actively injected into a LAN to sniff around a switched network and capture its traffic. A packet sniffer can obtain all the information visible on the network and records it for future review. Ethical hacker can see all the information in the packet, including data that should remain hidden.

Lab Objectives

- Perform MAC Flooding using macof

Task 1: Perform MAC Flooding using macof

MAC flooding is a technique used to compromise the security of network switches that connect network segments or network devices. Attackers use the MAC flooding technique to force a switch to act as a hub, so they can easily sniff the traffic.

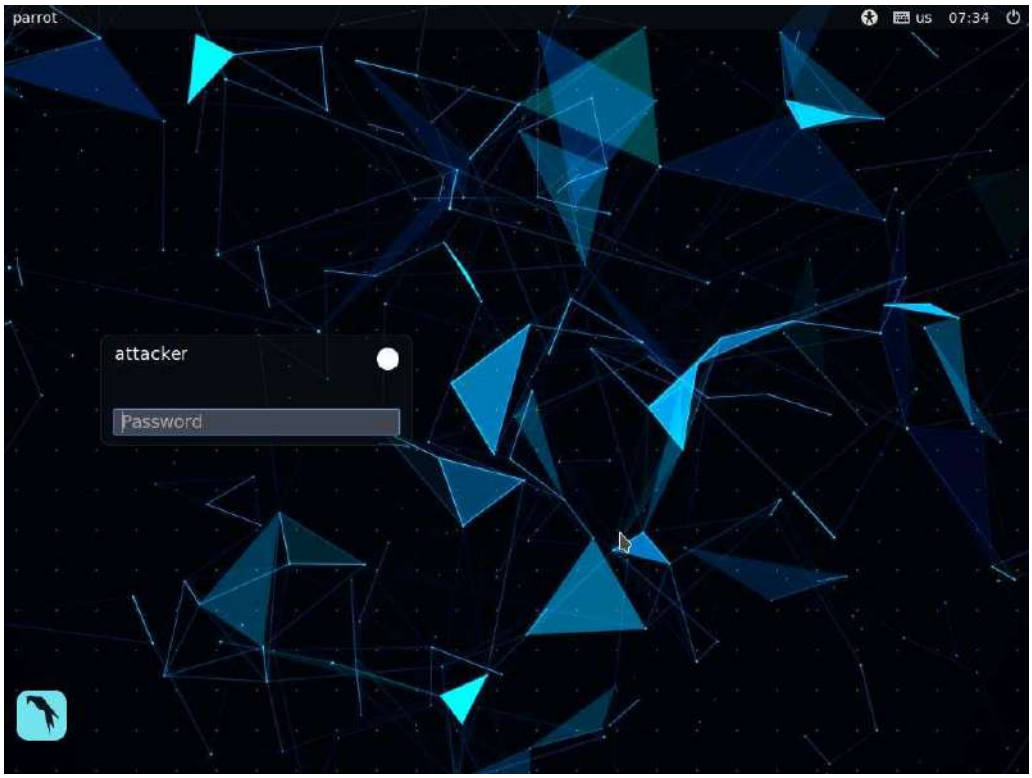
macof is a Unix and Linux tool that is a part of the dsniff collection. It floods the local network with random MAC addresses and IP addresses, causing some switches to fail and open in repeating mode, thereby facilitating sniffing. This tool floods

the switch's CAM tables (131,000 per minute) by sending forged MAC entries. When the MAC table fills up, the switch converts to a hub-like operation where an attacker can monitor the data being broadcast.

Here, we will use the macof tool to perform MAC flooding.

For demonstration purposes, we are using only one target machine (namely, **Windows 10**). However, you can use multiple machines connected to the same network. Macof will send the packets with random MAC addresses and IP addresses to all active machines in the local network.

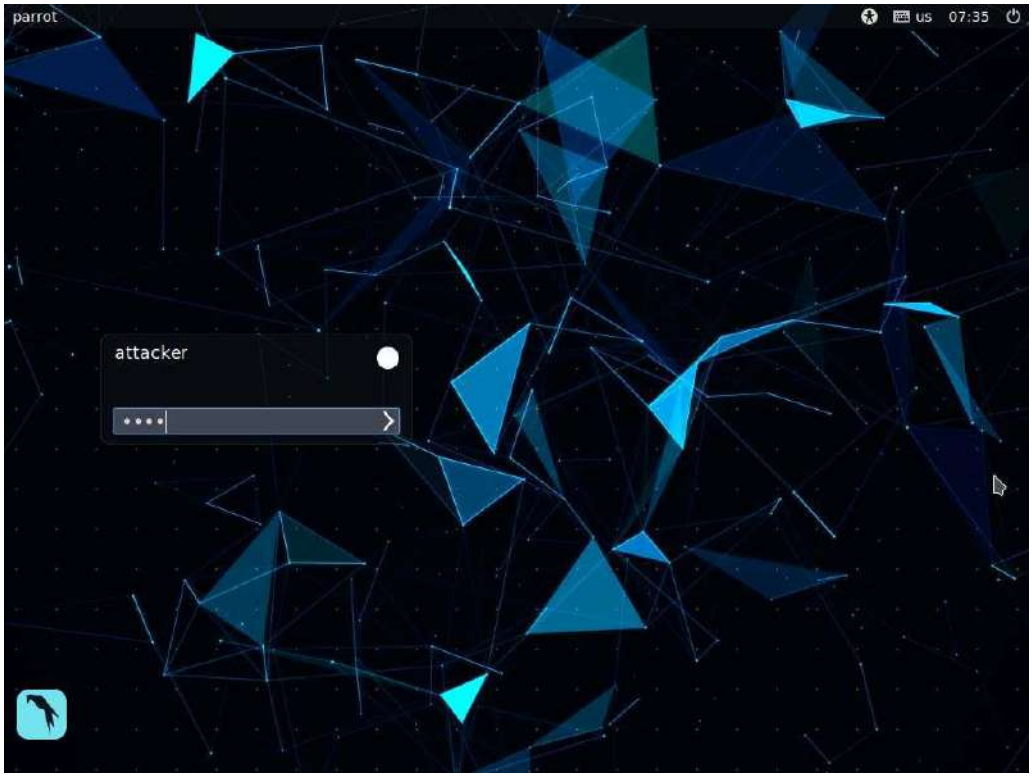
1. Click Parrot Security to switch to the **Parrot Security** machine.



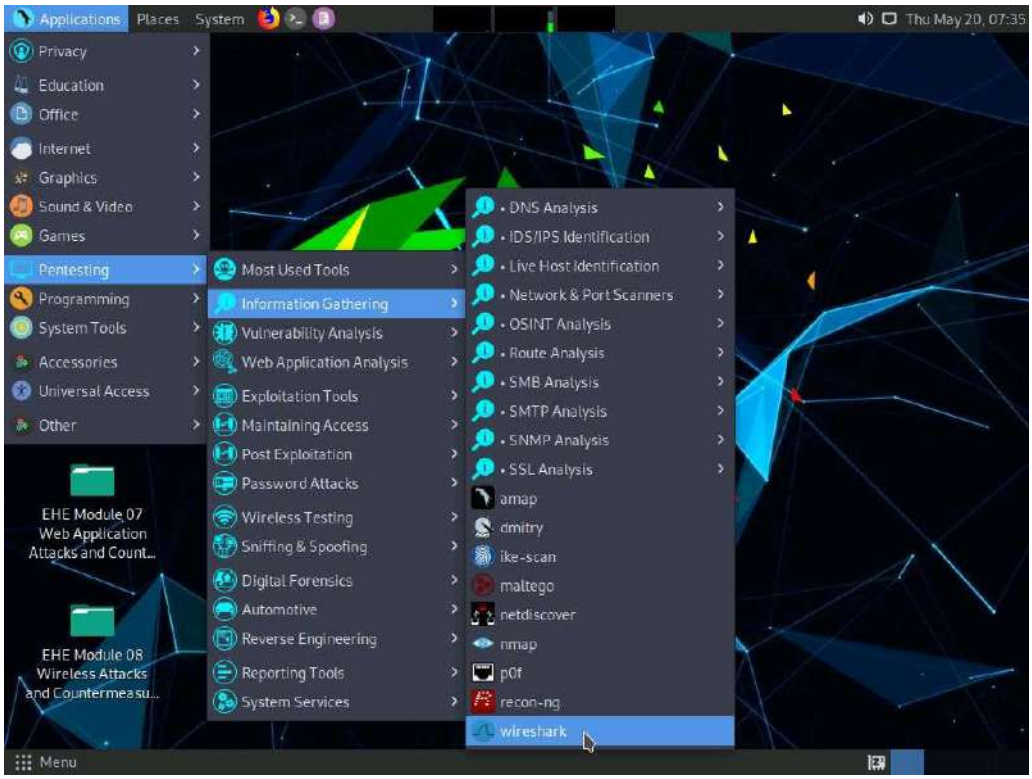
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

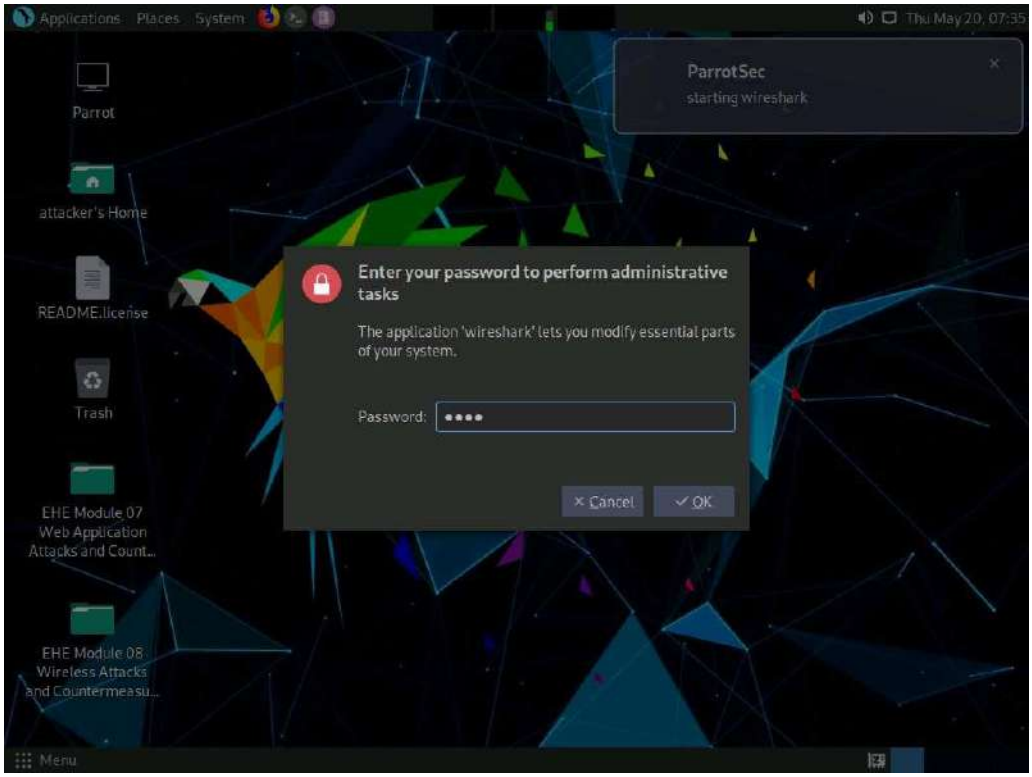
If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.



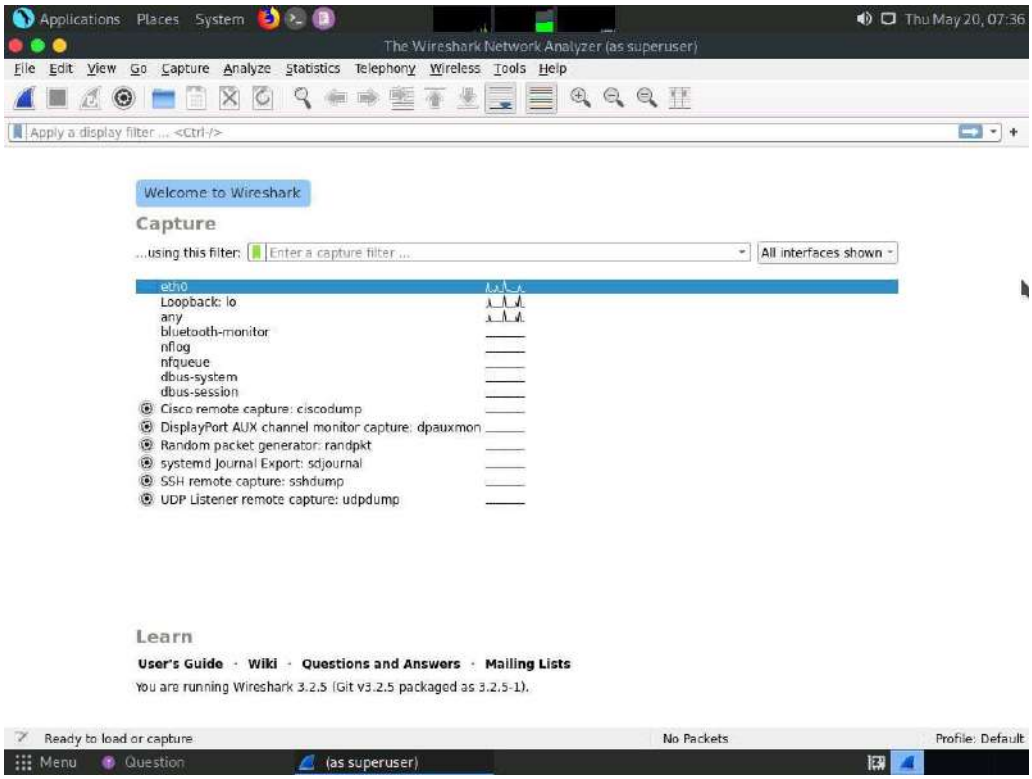
3. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Information Gathering** --> **wireshark**.



4. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

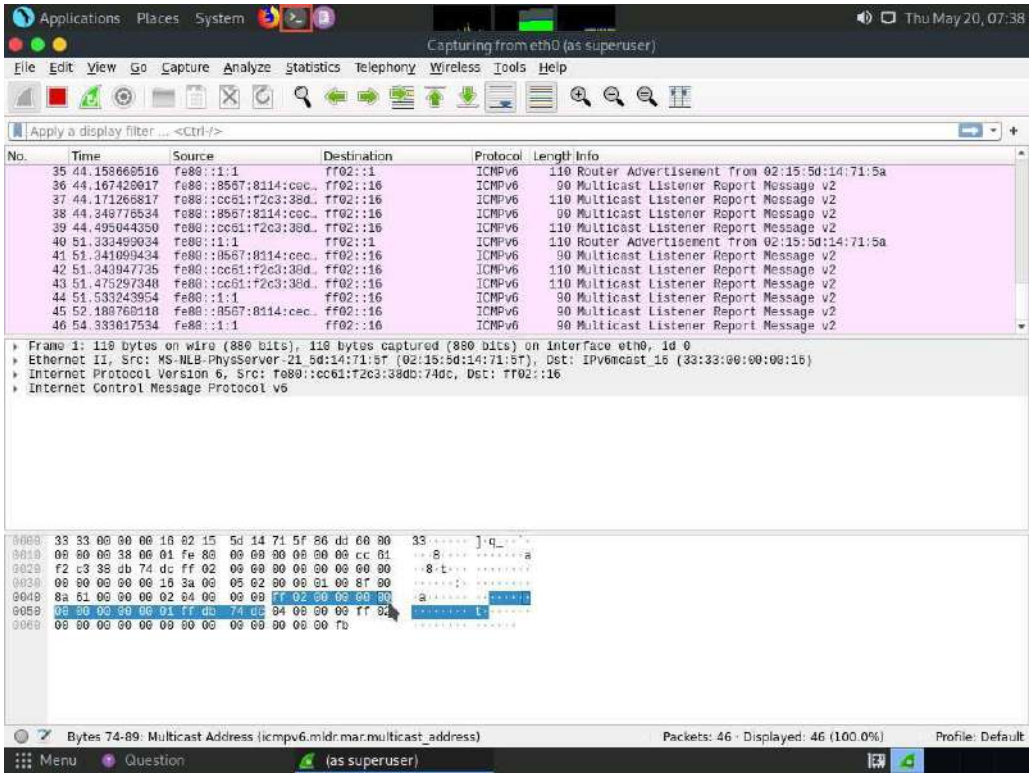


5. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.



6. Leave the **Wireshark** application running.

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

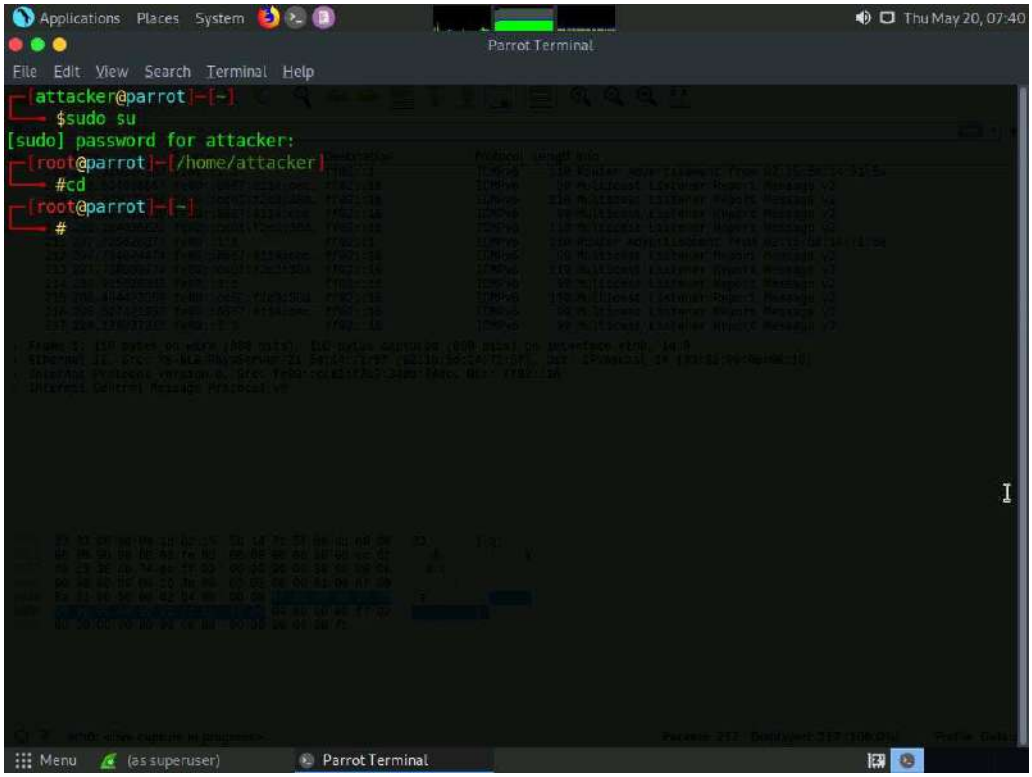


8. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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

The password that you type will not be visible.

10. Now, type **cd** and press **Enter** to jump to the root directory.

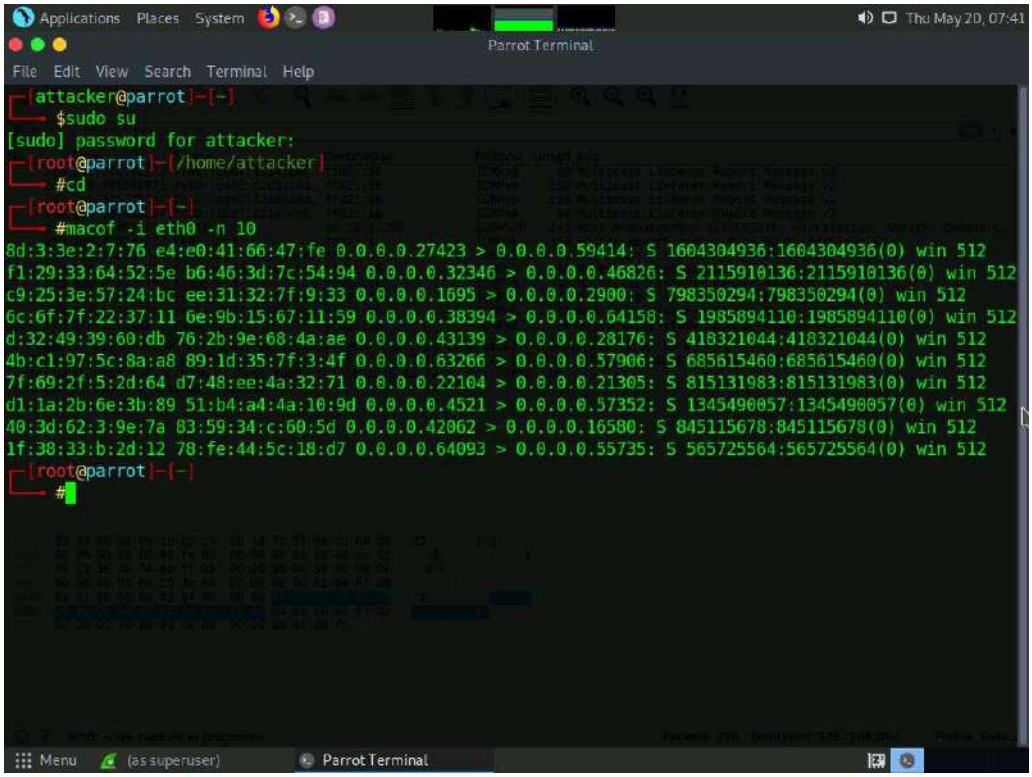


11. The **Parrot Terminal** window appears; type **macof -i eth0 -n 10** and press **Enter**.

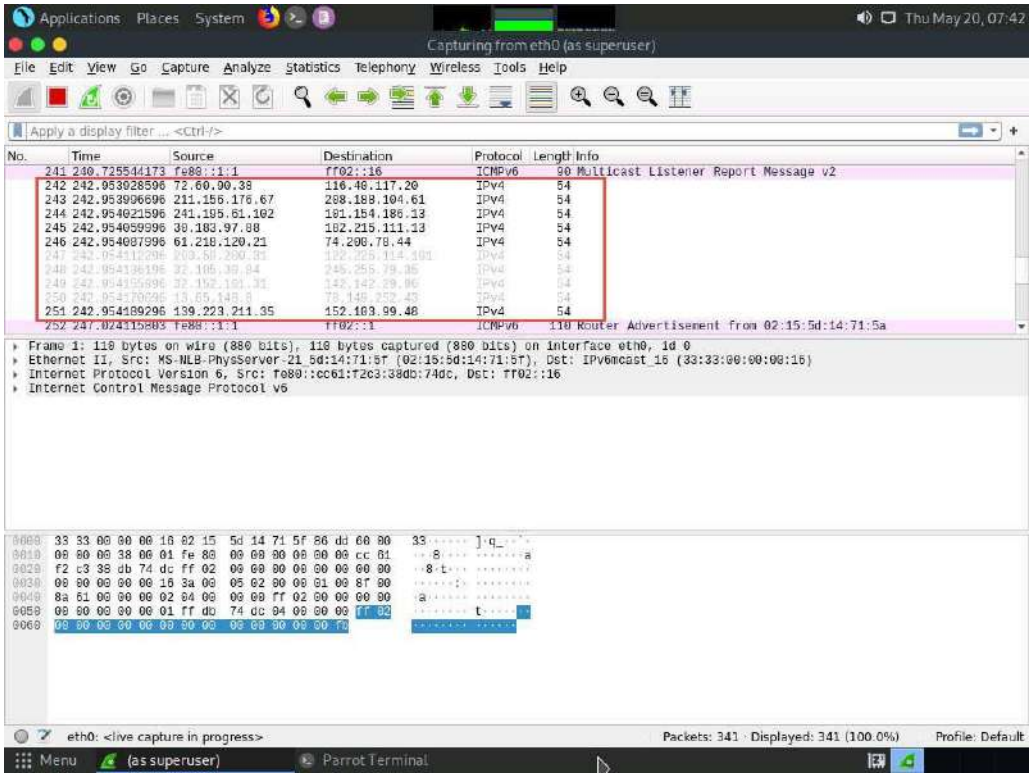
-i: specifies the interface and **-n**: specifies the number of packets to be sent (here, **10**).

You can also target a single system by issuing the command **macof -i eth0 -d [Target IP Address]** (**-d**: Specifies the destination IP address).

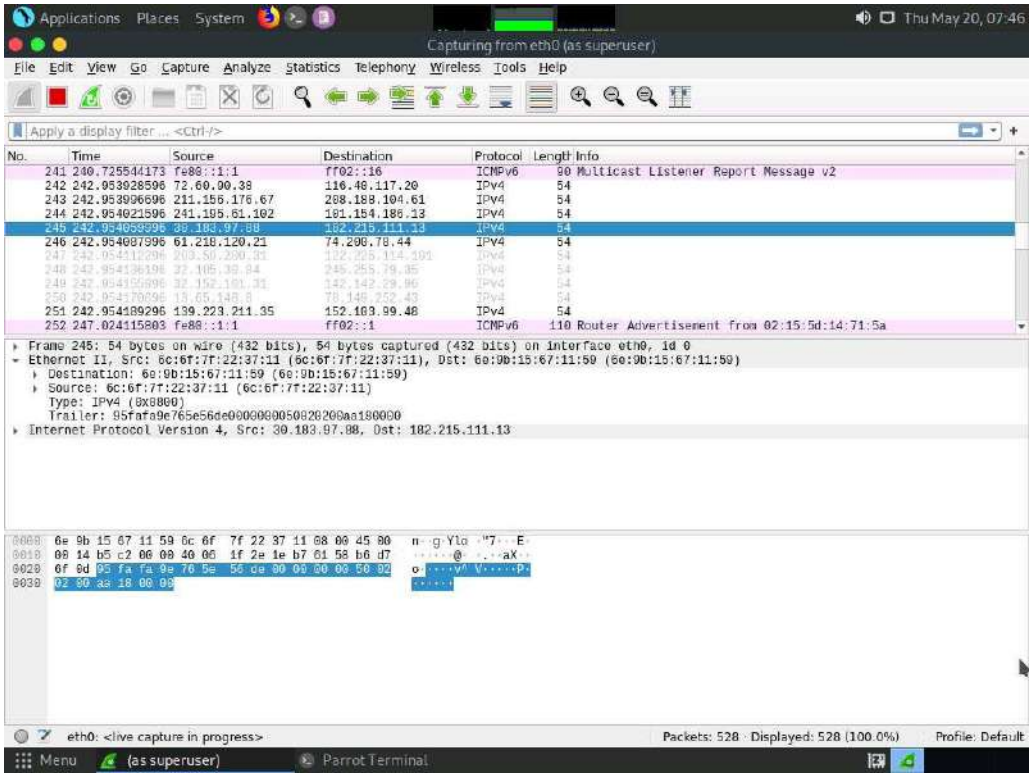
12. This command will start flooding the CAM table with random MAC addresses, as shown in the screenshot.



13. Switch to the **Wireshark** window and observe the **IPv4** packets from random IP addresses, as shown in the screenshot.



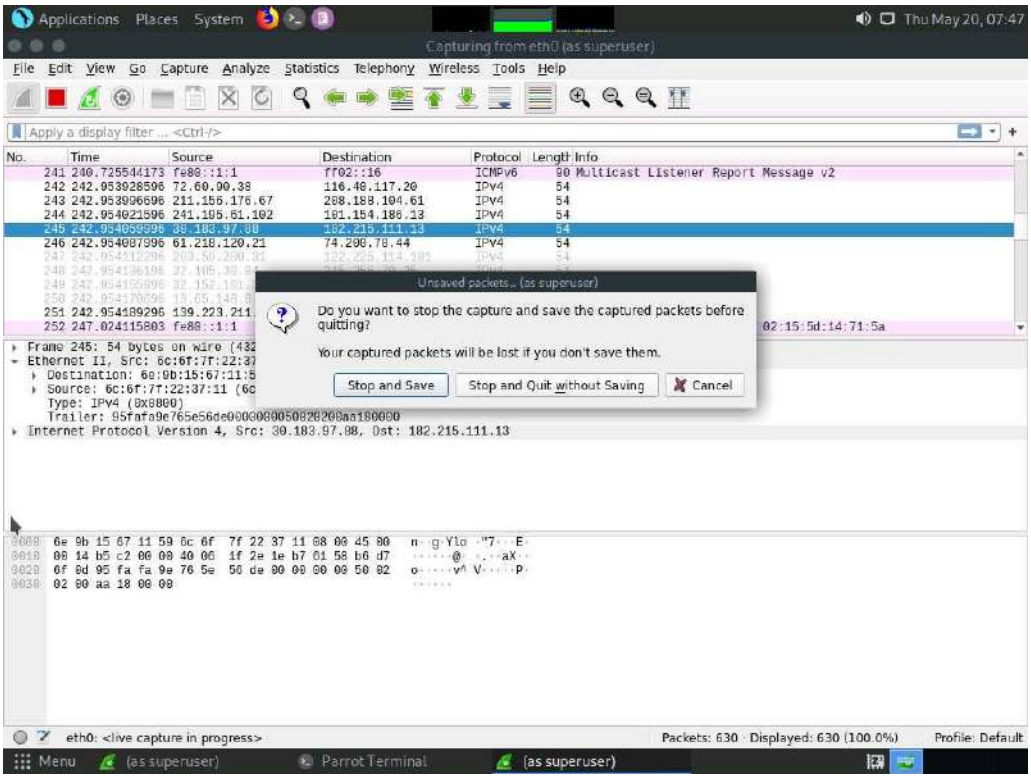
14. Click on any captured **IPv4** packet and expand the **Ethernet II** node in the packet details section. Information regarding the source and destination MAC addresses is displayed, as shown in the screenshot.



15. Similarly, you can switch to a different machine to see the same packets that were captured by Wireshark in the **Parrot Security** machine.

16. Macof sends the packets with random MAC and IP addresses to all active machines in the local network. If you are using multiple targets, you will observe the same packets on all target machines.

17. Close the **Wireshark** window. If an **Unsaved packets**... pop-up appears, click **Stop and Quit without Saving** to close the Wireshark application.



18. This concludes the demonstration of how to perform MAC flooding using macof.

19. Close all open windows and document all the acquired information.

Lab 2: Perform ARP Poisoning to Divert all Communication Between Two Machines

Lab Scenario

ARP poisoning technique generally used by attackers to perform sniffing on a target network. Using this method, an attacker can steal sensitive information, prevent network and web access, and perform DoS and MITM attacks using sniffing.

Lab Objectives

- Perform ARP Poisoning using arpspoof

Task 1: Perform ARP Poisoning using arpspoof

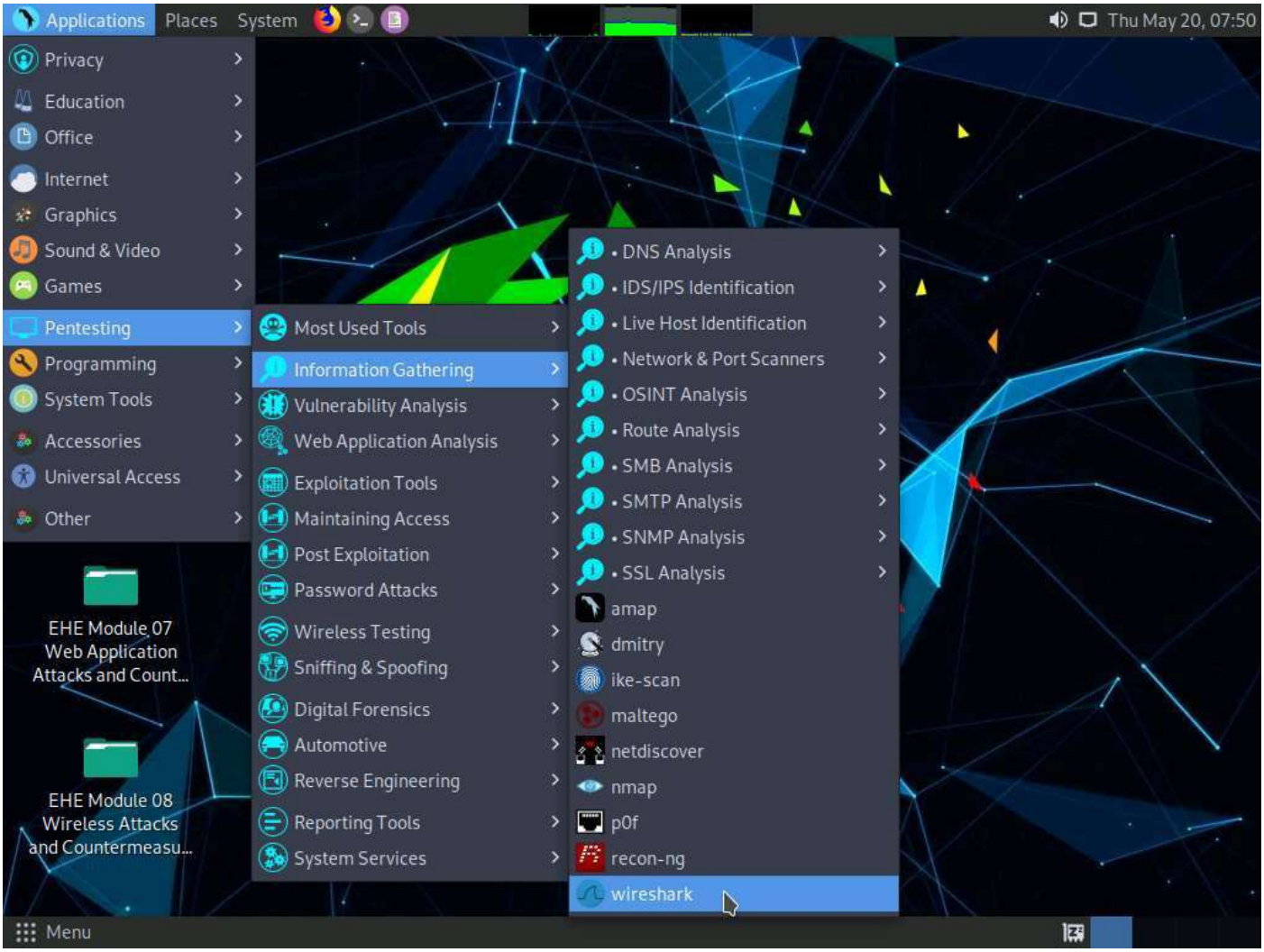
ARP spoofing is a method of attacking an Ethernet LAN. ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the destination computer (target) sends the frames to the attacker's computer, where the attacker can modify them before sending them to the source machine (User A) in an MITM attack.

arpspoof redirects packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies. This is an extremely effective way of sniffing traffic on a switch.

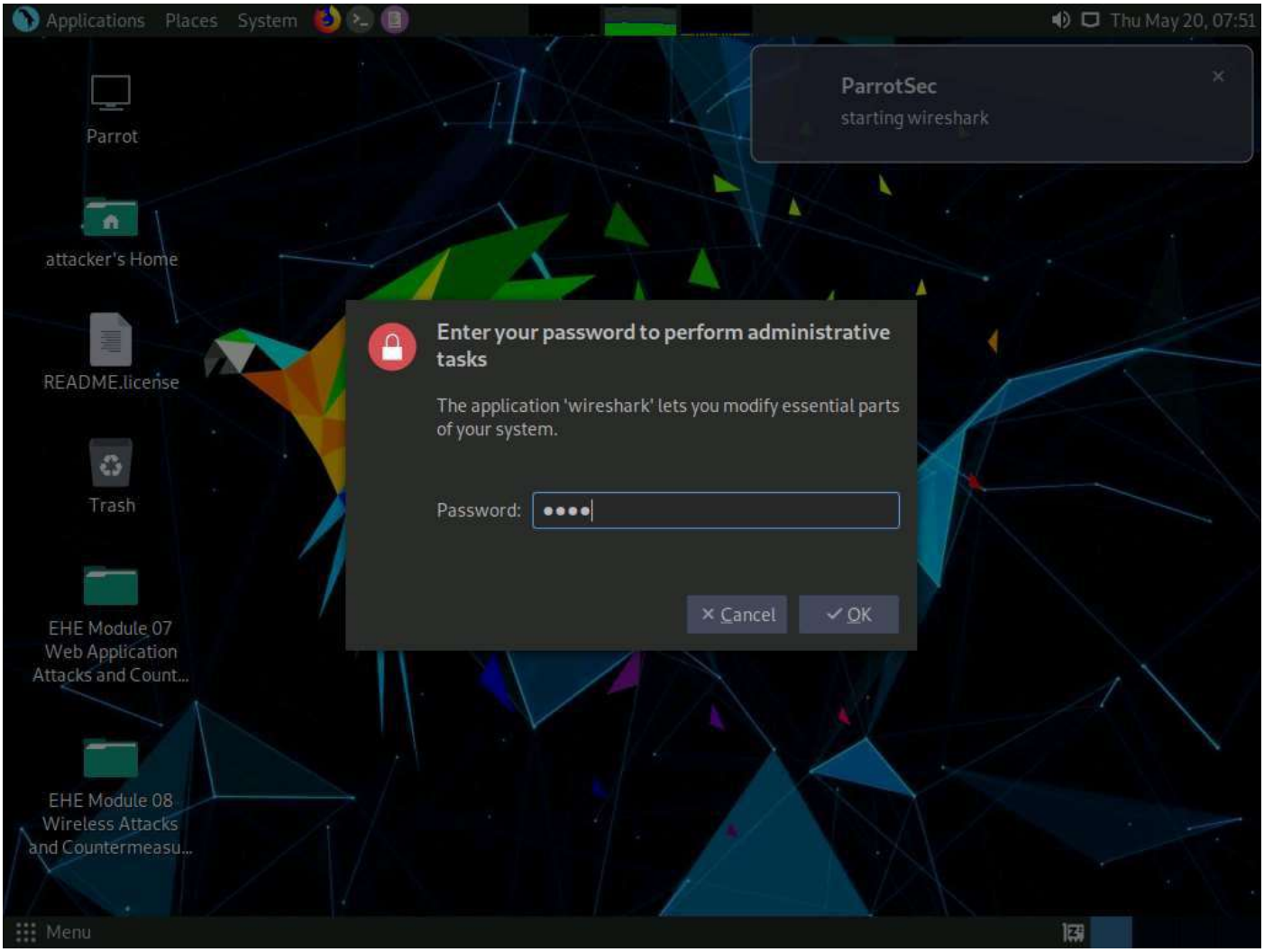
Here, we will use the arpspoof tool to perform ARP poisoning.

In this lab, we will use the **Parrot Security (10.10.1.13)** machine as the host system and the **Windows 10 (10.10.1.10)** machine as the target system.

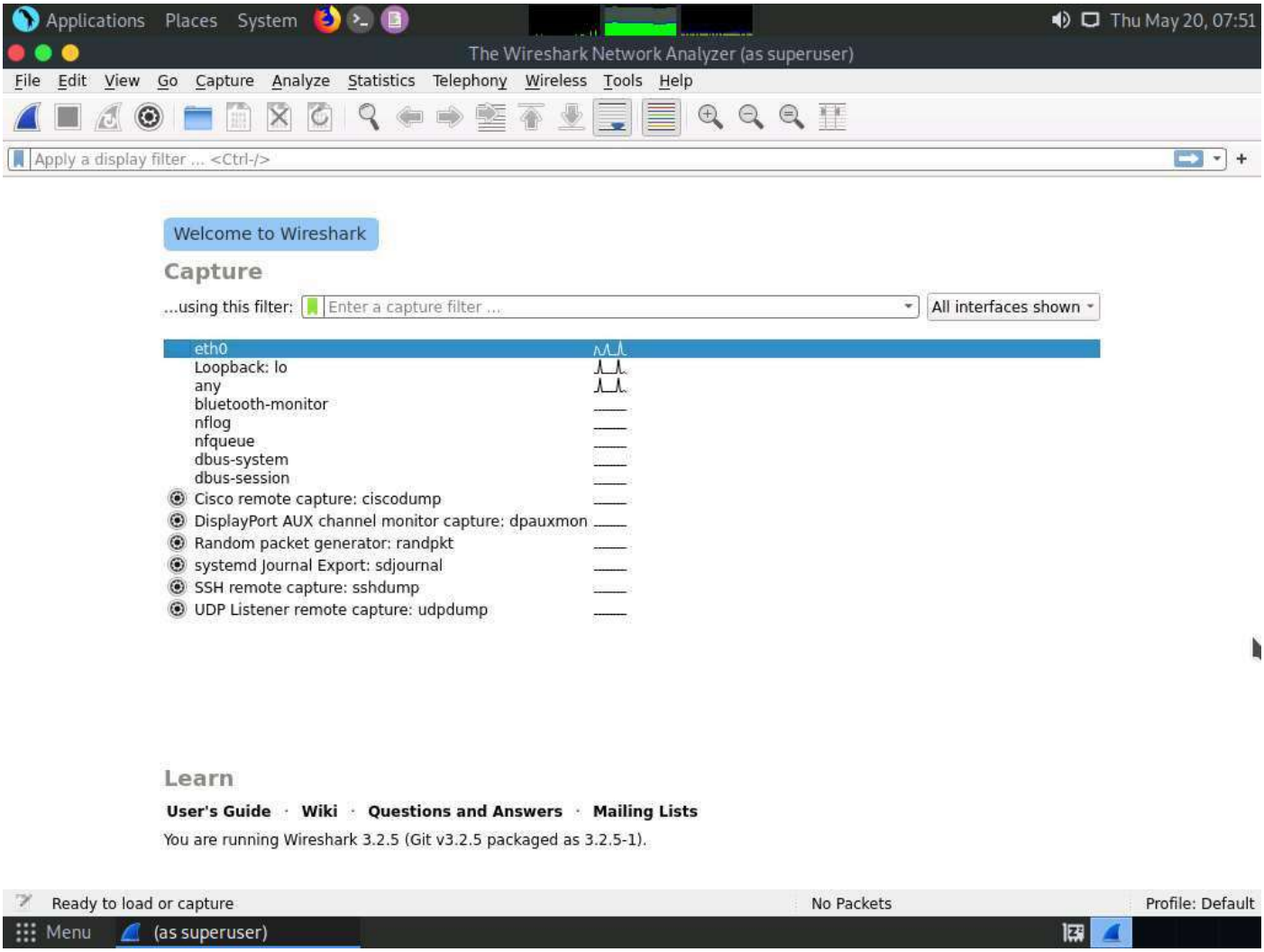
1. On the **Parrot Security** machine; click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Information Gathering** --> **wireshark**.



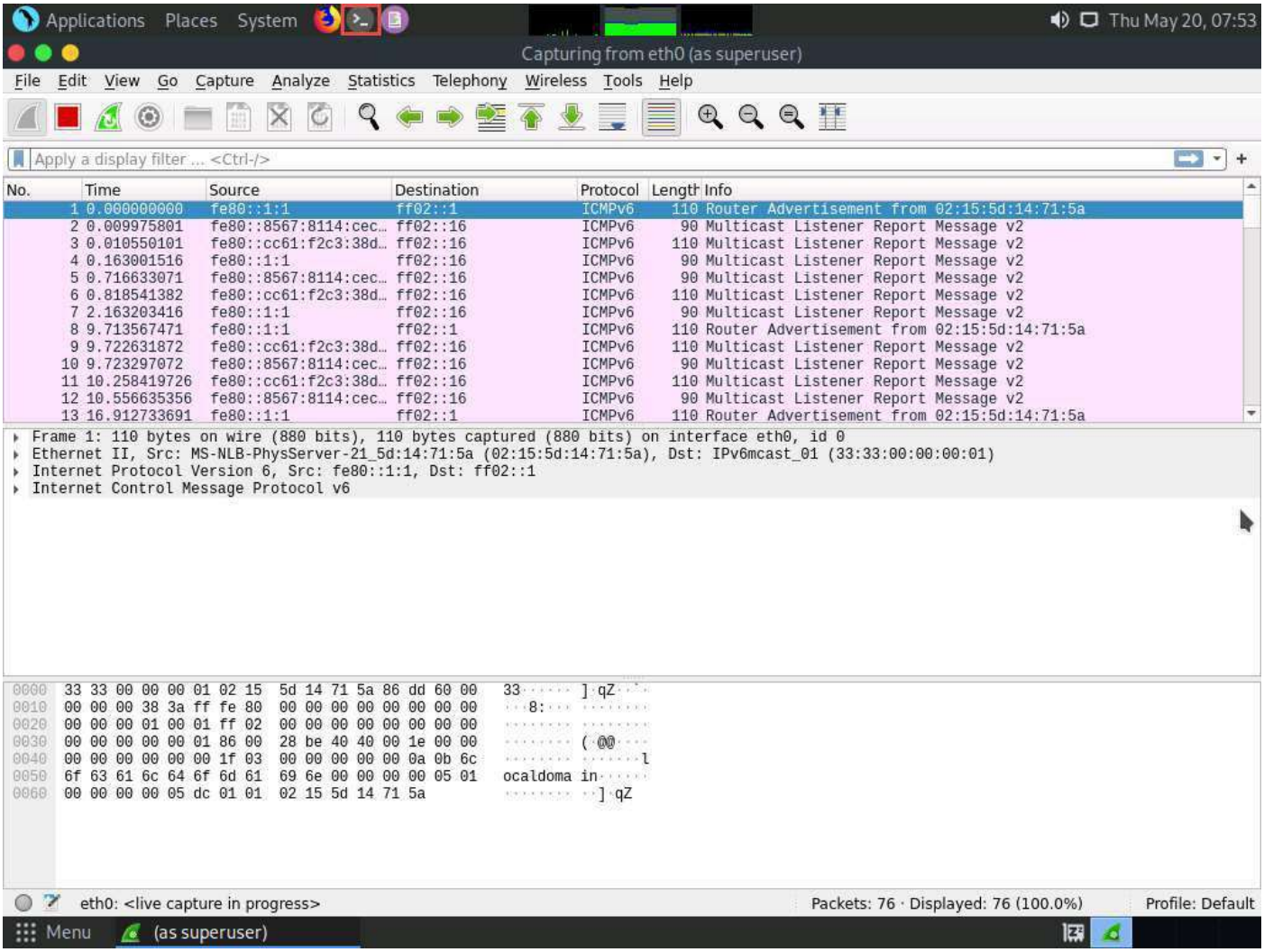
2. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.



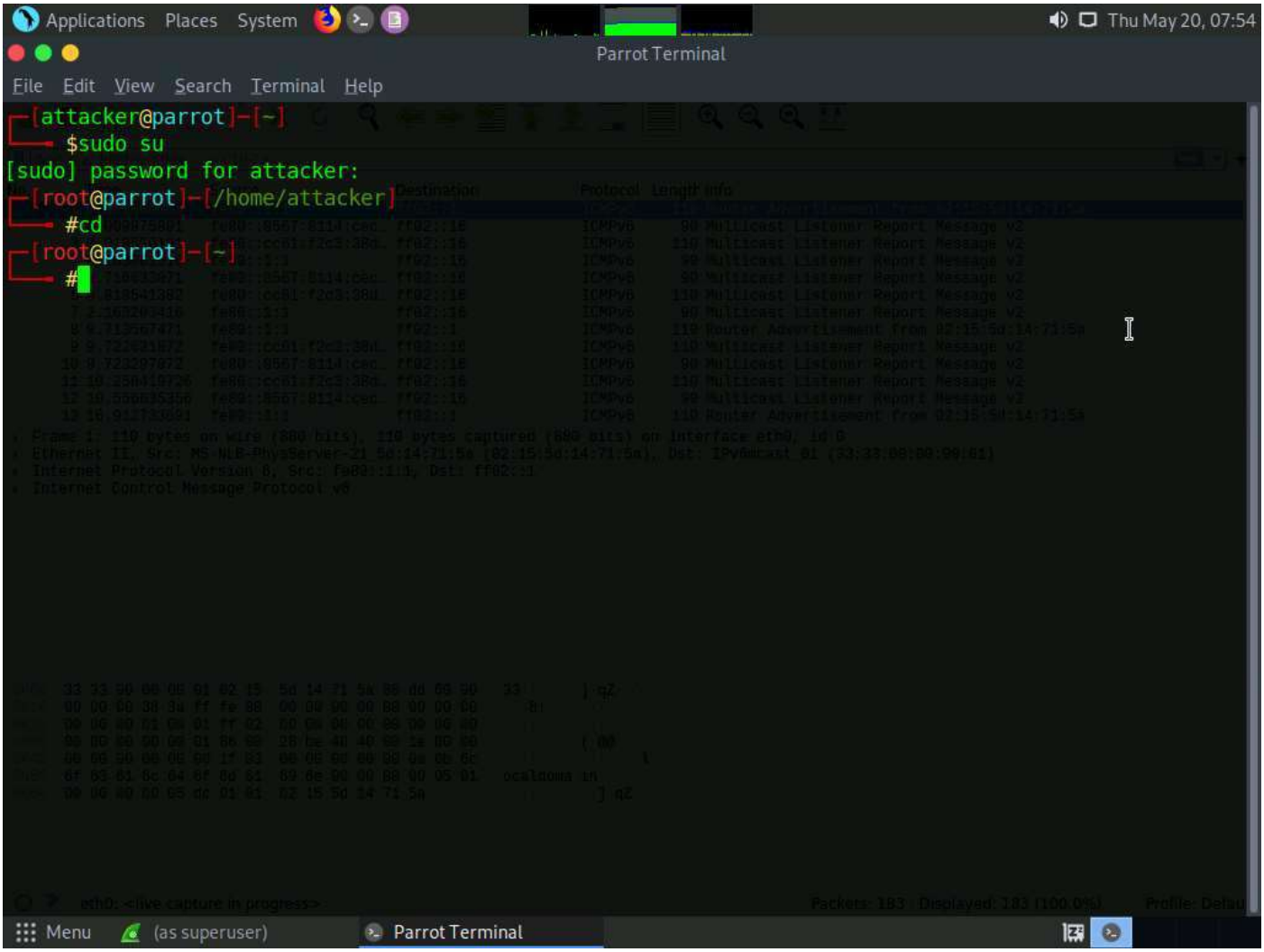
3. The **Wireshark Network Analyzer** window appears; double-click the available ethernet or interface (here, **eth0**) to start the packet capture, as shown in the screenshot.



4. Leave the **Wireshark** application running.
5. Now, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



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



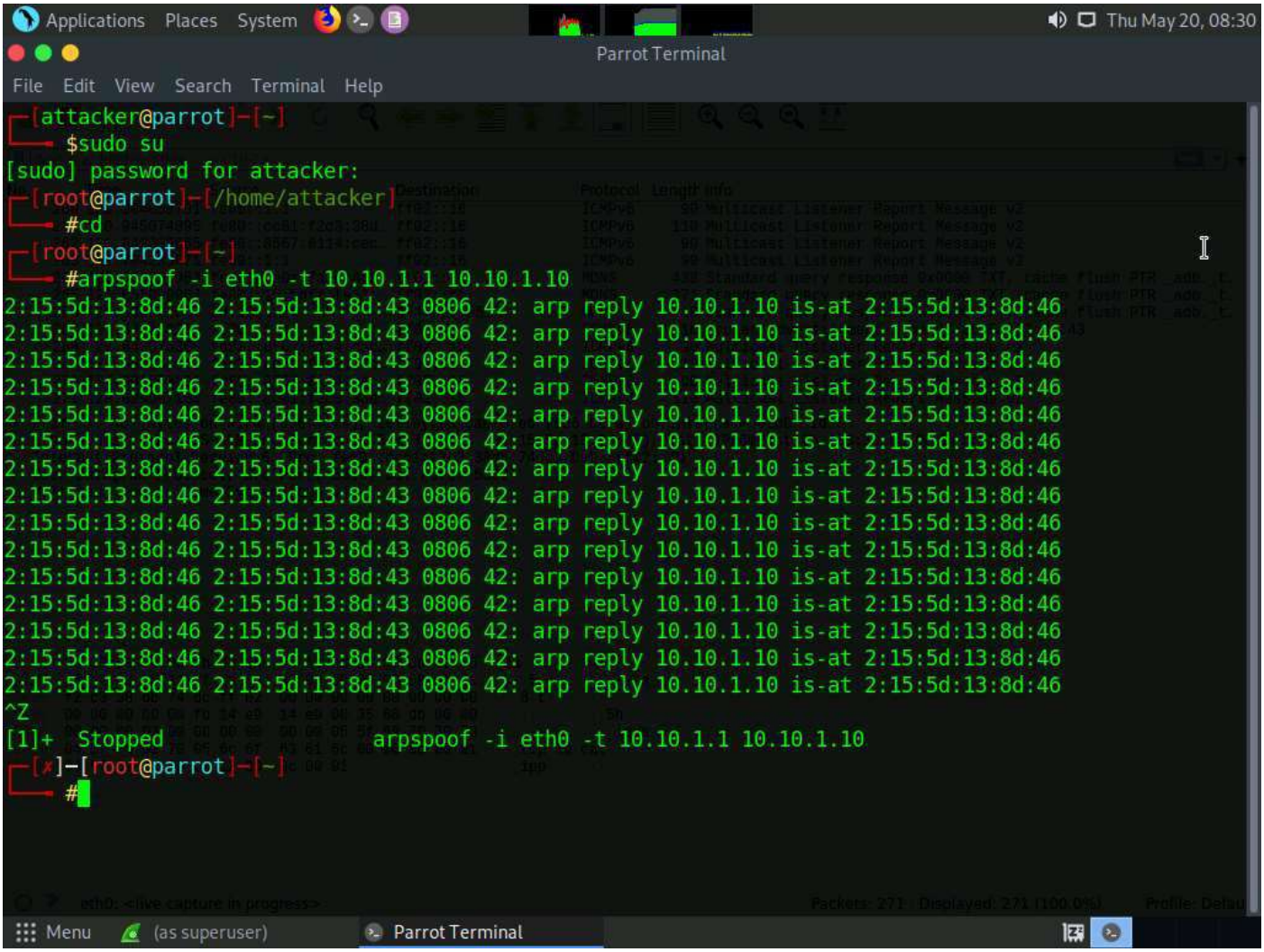
9. In the **Parrot Terminal** window, type **arpspoof -i eth0 -t 10.10.1.1 10.10.1.10** and press **Enter**.

(Here, **10.10.1.10** is IP address of the target system [**Windows 10**], and **10.10.1.1** is IP address of the access point or gateway)

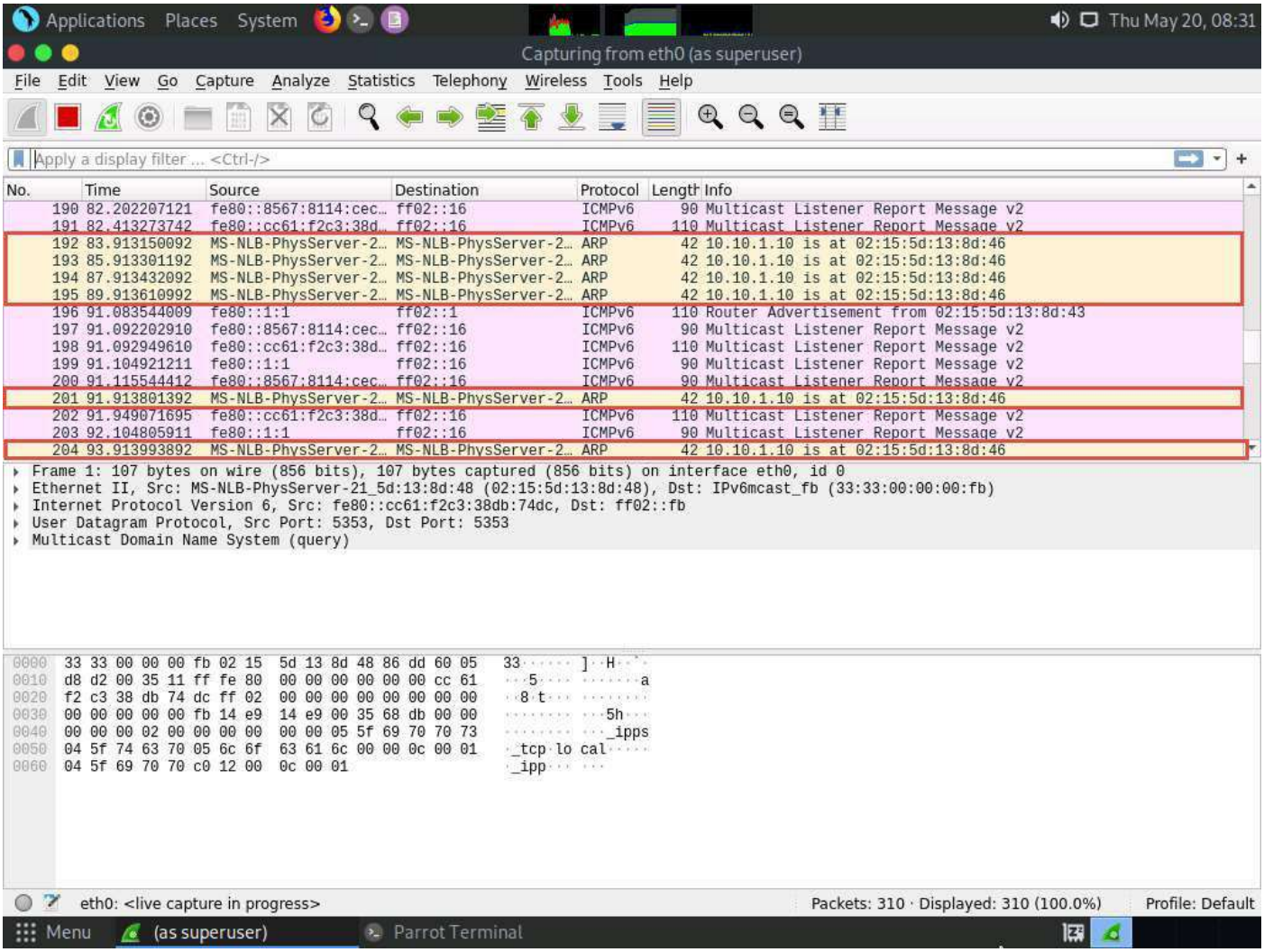
-i: specifies network interface and **-t**: specifies target IP address.

10. Issuing the above command informs the access point that the target system (**10.10.1.10**) has our MAC address (the MAC address of host machine (**Parrot Security**)). In other words, we are informing the access point that we are the target system.

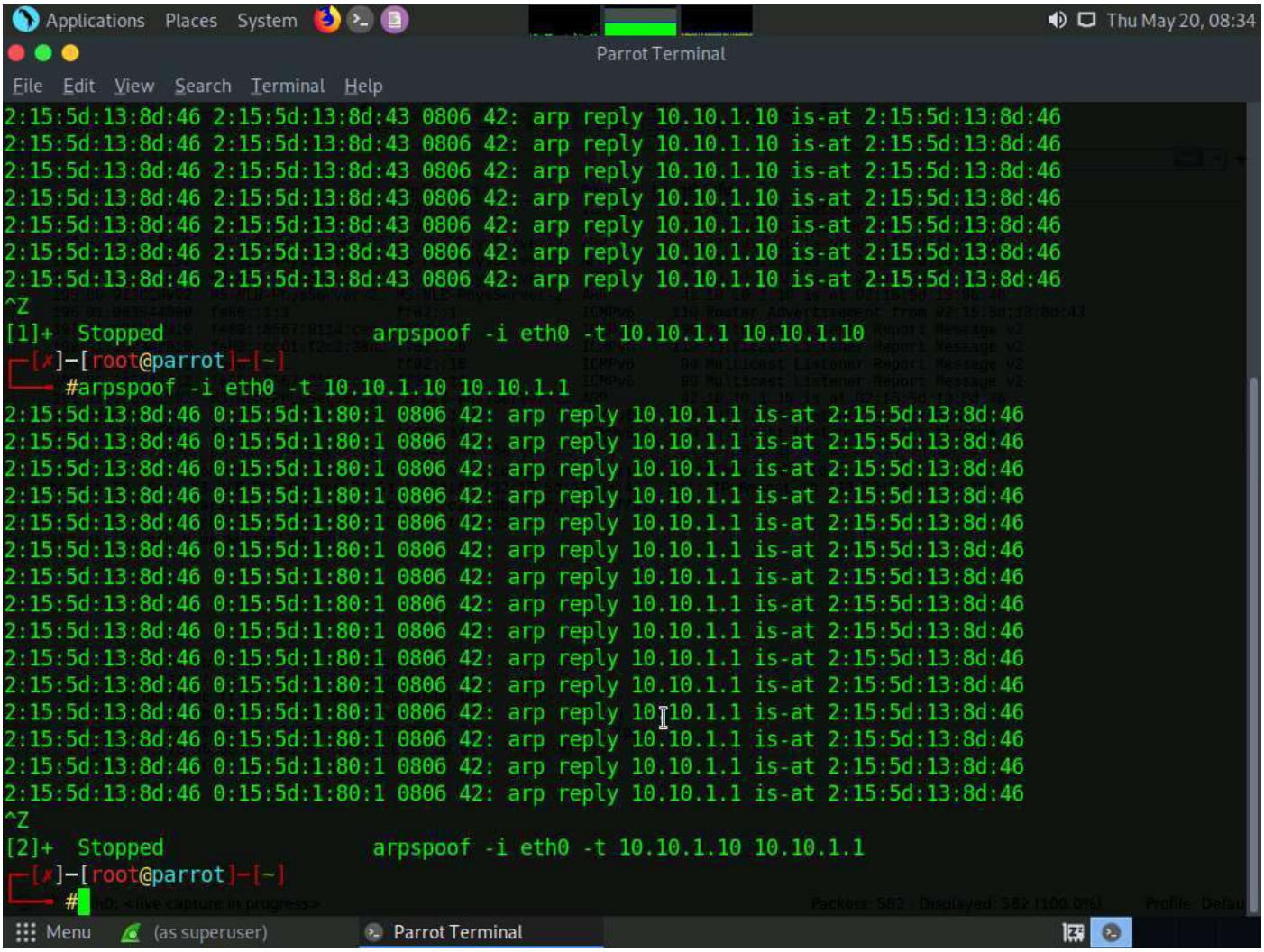
11. After sending a few packets, press **CTRL + Z** to stop sending the **ARP** packets.



12. Switch to the **Wireshark** window and you can observe the captured **ARP** packets, as shown in the screenshot.



13. Switch back to the terminal window where arpspoof was running. Type **arpspoof -i eth0 -t 10.10.1.10 10.10.1.1** and press **Enter**.
14. Through the above command, the host system informs the target system (**10.10.1.10**) that it is the access point (**10.10.1.1**).
15. After sending a few packets, press **CTRL + Z** to stop sending the **ARP** packets.



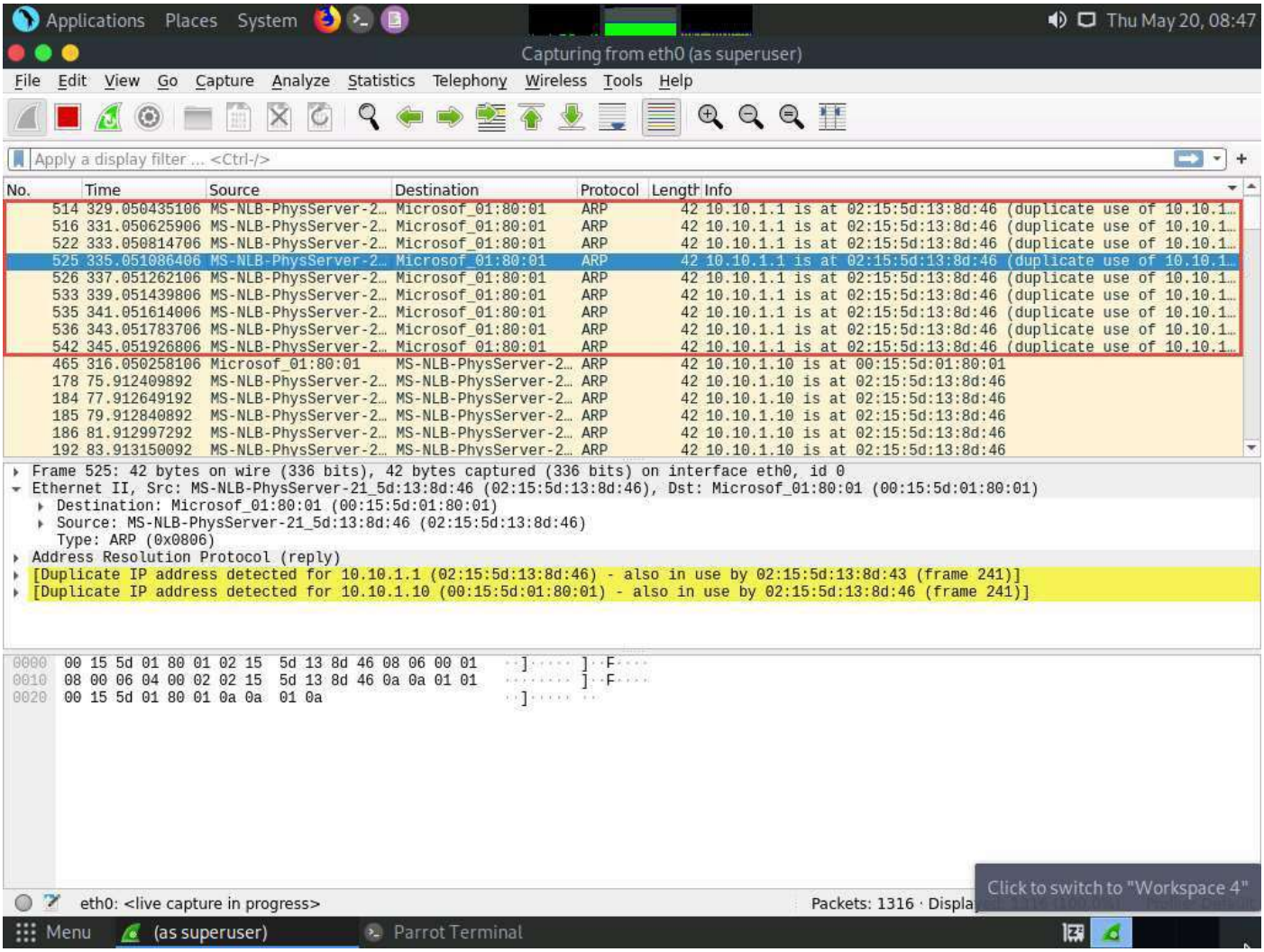
16. In **Wireshark**, you can observe the ARP packets with an alert warning "**duplicate use of 10.10.1.10 detected!**"

17. Click on any ARP packet and expand the **Ethernet II** node in the packet details section. As shown in the screenshot, you can observe the MAC addresses of IP addresses **10.10.1.1** and **10.10.1.10**.

Here, the MAC address of the host system (**Parrot Security**) is **02:15:5d:13:8d:46**.

Note: The results might differ in your lab environment.

18. Using arpspoof, we assigned the MAC address of the host system to the target system (**Windows 10**) and access point. Therefore, the alert warning of a duplicate use of **10.10.1.10** is displayed.



You can navigate to the **Windows 10** machine and see the IP addresses and their corresponding MAC addresses. You will observe that the MAC addresses of IP addresses **10.10.1.1** and **10.10.1.13** are the same, indicating the occurrence of an ARP poisoning attack, where 10.10.1.13 is the **Parrot Security** machine and 10.10.1.1 is the access point.

...less

19. This concludes the demonstration of how to perform ARP poisoning using arpspoof.
20. Close all open windows and document all the acquired information.

Lab 3: Detect ARP Attacks using ARP Spoofing Detection Tools to Ensure Data Privacy

Lab Scenario

Network sniffing involves using sniffer tools that enable the real-time monitoring and analysis of data packets flowing over computer networks. These network sniffers can be detected by using various techniques such as:

- **Ping Method**: Identifies if a system on the network is running in promiscuous mode
- **DNS Method**: Identifies sniffers in the network by analyzing the increase in network traffic
- **ARP Method**: Sends a non-broadcast ARP to all nodes in the network; a node on the network running in promiscuous mode will cache the local ARP address

We should be able to detect network sniffing in the network. A sniffer on a network only captures data and runs in promiscuous mode, so it is not easy to detect. Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety. The sniffer leaves no trace, since it does not transmit data. Therefore, to detect sniffing attempts, you must use the network sniffing detection technique and tool discussed in this lab.

Lab Objectives

- Detect ARP Poisoning in a Switch-Based Network

Task 1: Detect ARP Poisoning in a Switch-Based Network

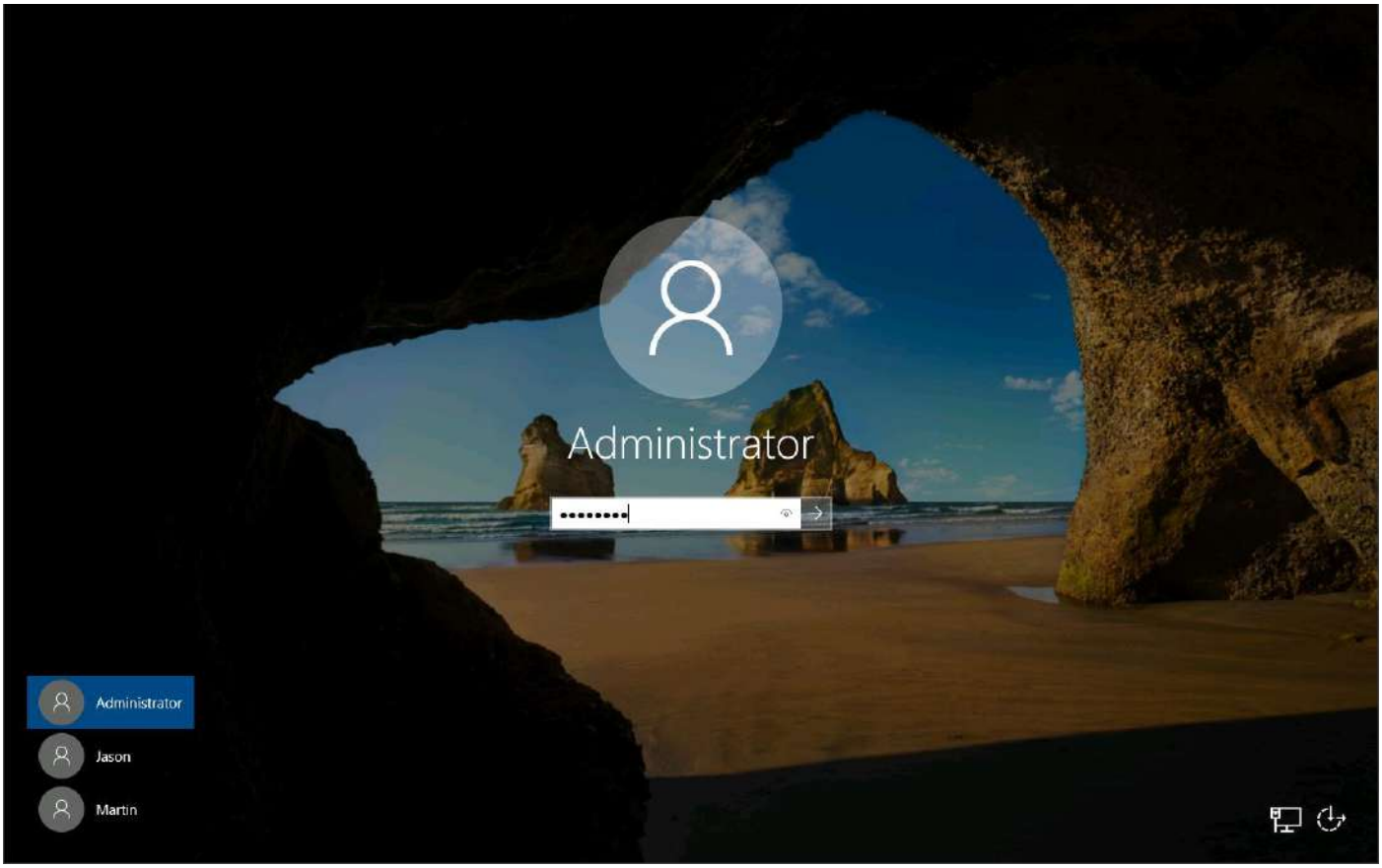
ARP poisoning involves forging many ARP request and reply packets to overload a switch. ARP cache poisoning is the method of attacking a LAN network by updating the target computer's ARP cache with both forged ARP request and reply packets designed to change the Layer 2 Ethernet MAC address (that of the network card) to one that the attacker can monitor. Attackers use ARP poisoning to sniff on the target network. Attackers can thus steal sensitive information, prevent network and web access, and perform DoS and MITM attacks.

We must assess the organization or target of evaluation for ARP poisoning vulnerabilities.

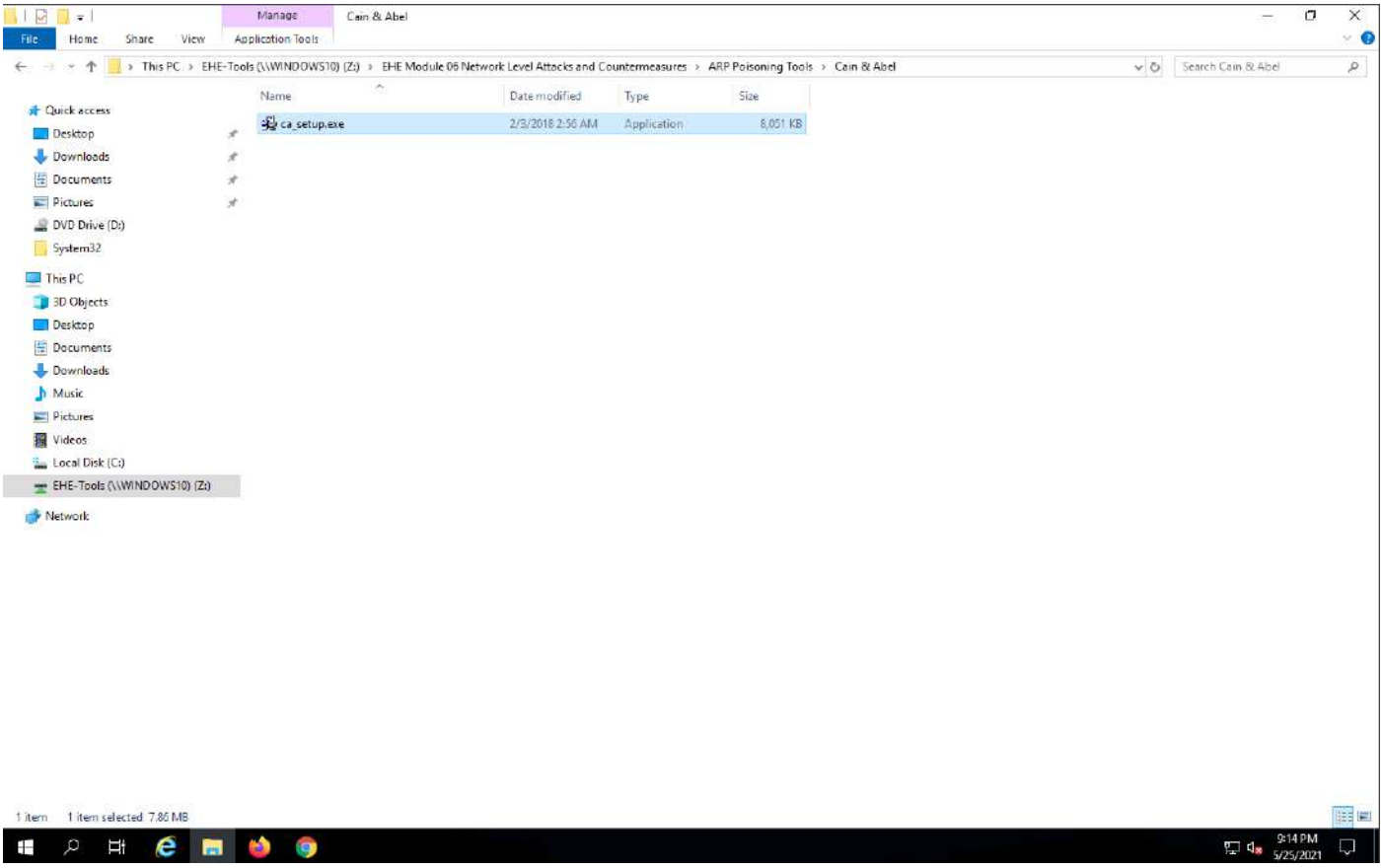
Here, we will detect ARP poisoning in a switch-based network.

In this task, we will use the **Windows Server 2019** machine as the host machine to perform ARP poisoning, and will sniff traffic flowing between the **Windows 10** and **Parrot Security** machines. Further, we will use the same machine (**Windows Server 2019**) to detect ARP poisoning.

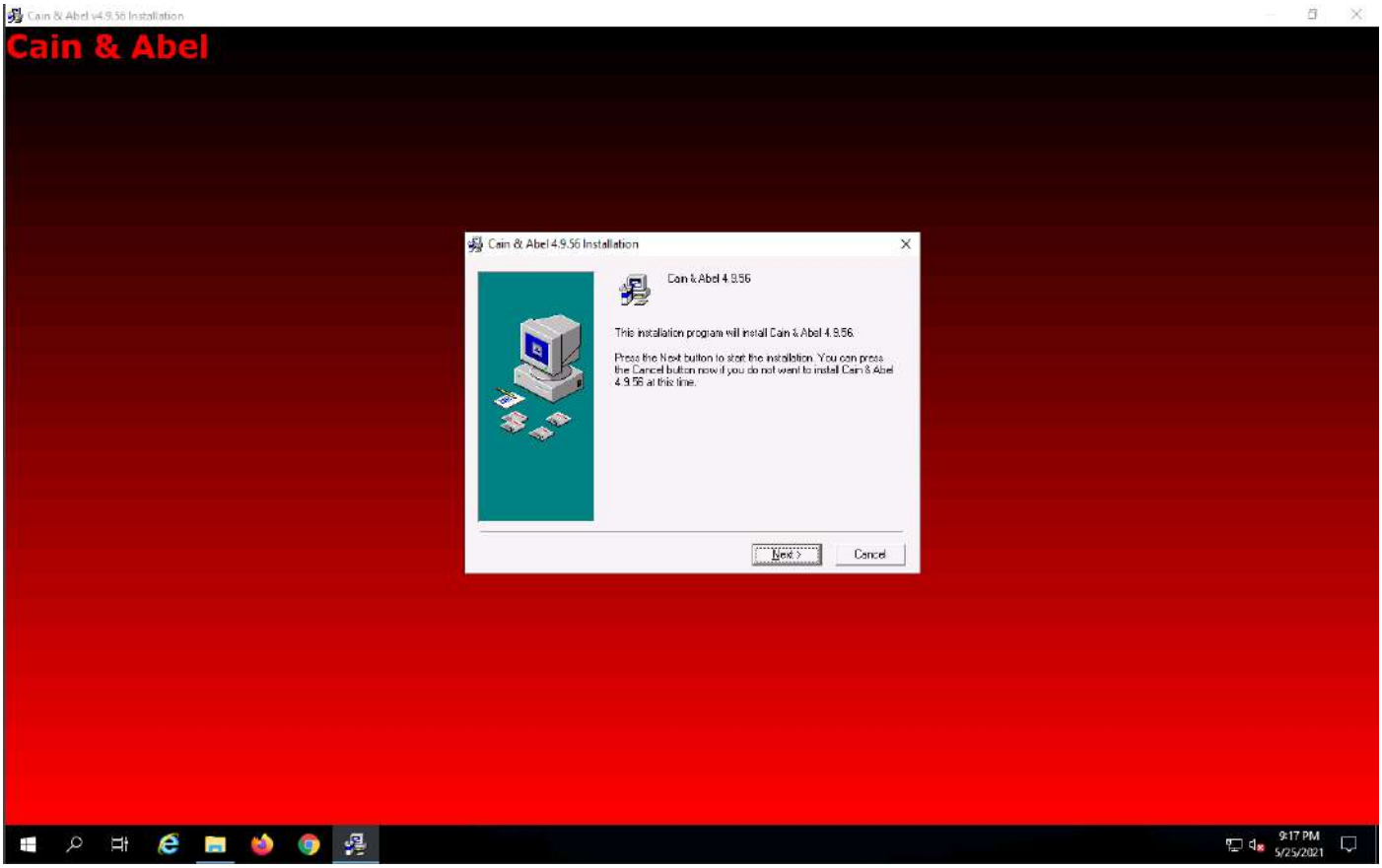
1. Click Windows Server 2019 to switch to the **Windows Server 2019** machine.
2. Click Ctrl+Alt+Delete to activate the machine, by default, **Administrator** account is selected, click Pa$$w0rd to enter the password and press **Enter**.



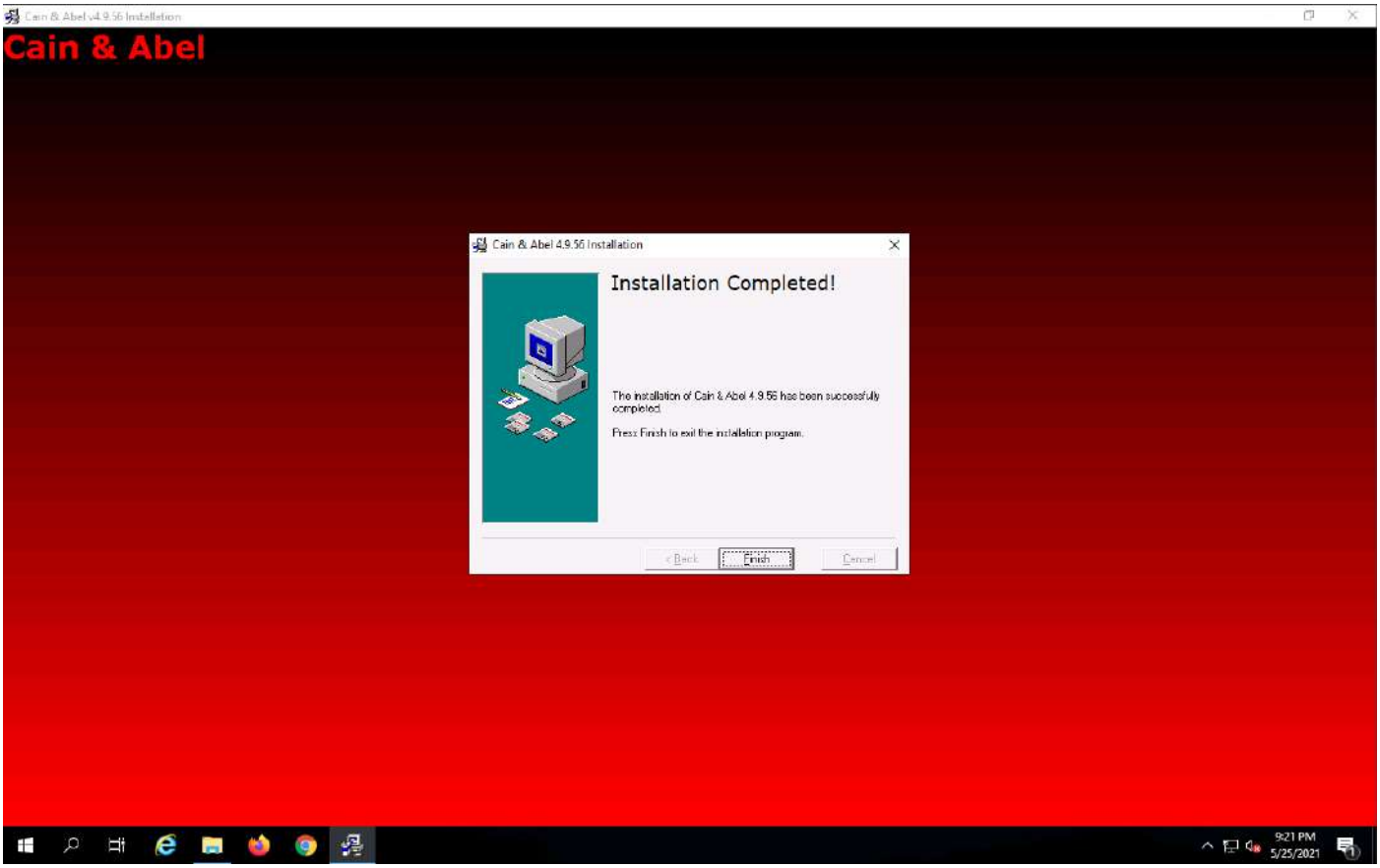
3. Navigate to **Z:\EHE Module 06 Network Level Attacks and Countermeasures\ARP Poisoning Tools\Cain & Abel** and double-click **ca_setup.exe**.



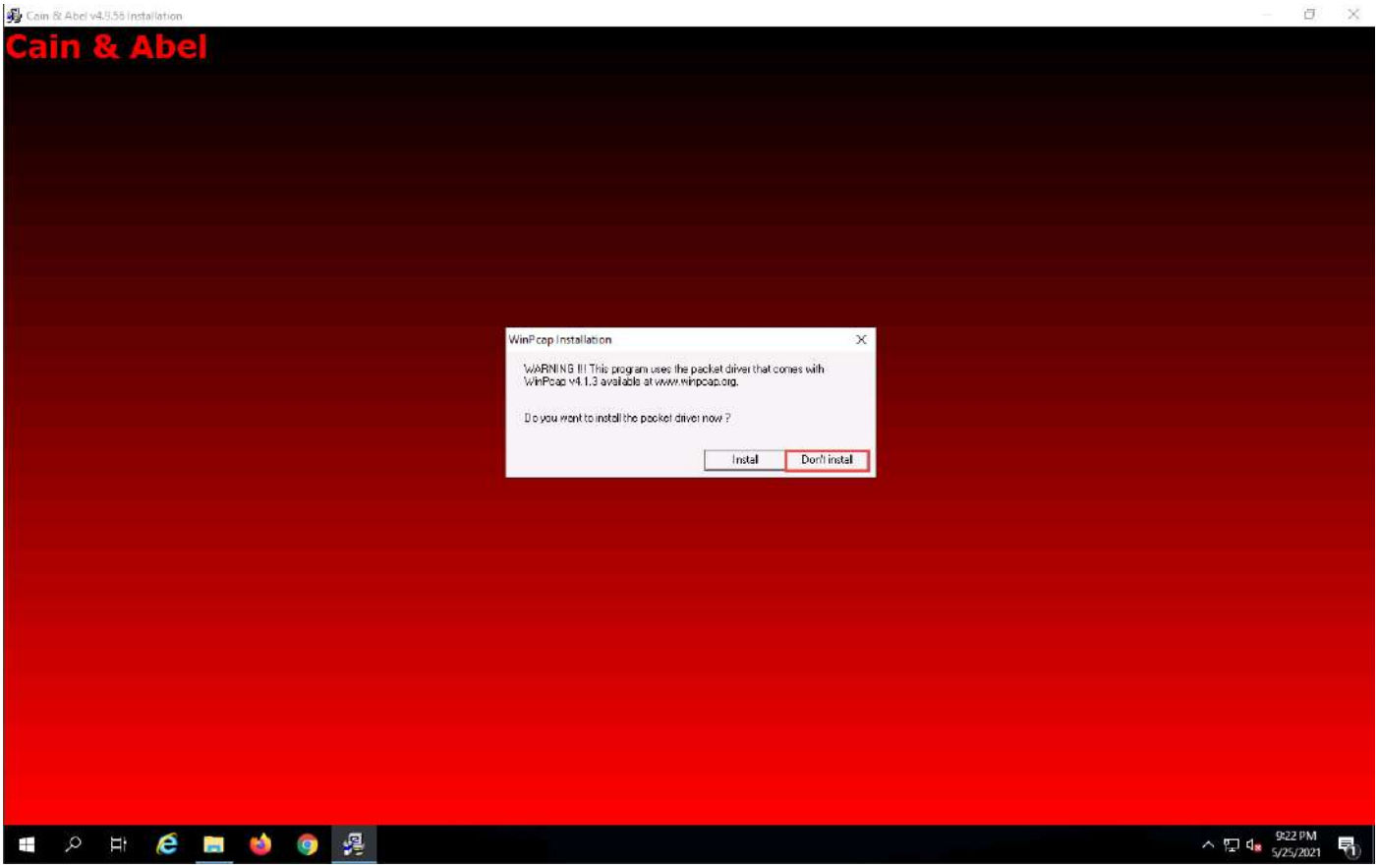
4. Cain & Abel initializes, and the **Cain & Abel Installation** window appears; click the **Next** button.



5. Follow the wizard-driven installation steps to install Cain & Abel.
6. After completing the installation, the **Installation Completed!** message appears; click **Finish**.

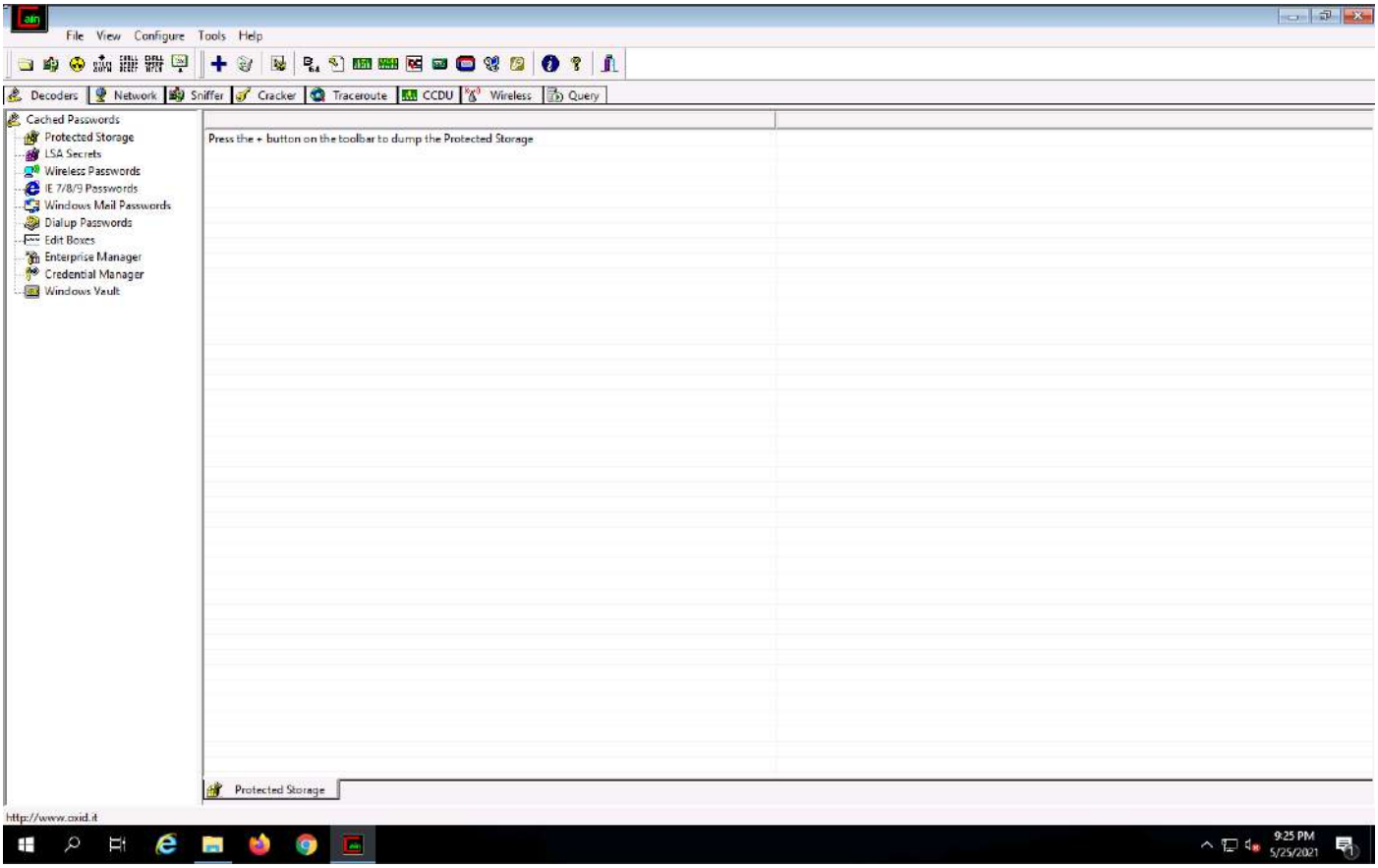


7. The **WinPcap Installation** pop-up appears; click **Don't install**, as you already installed it during the lab setup.

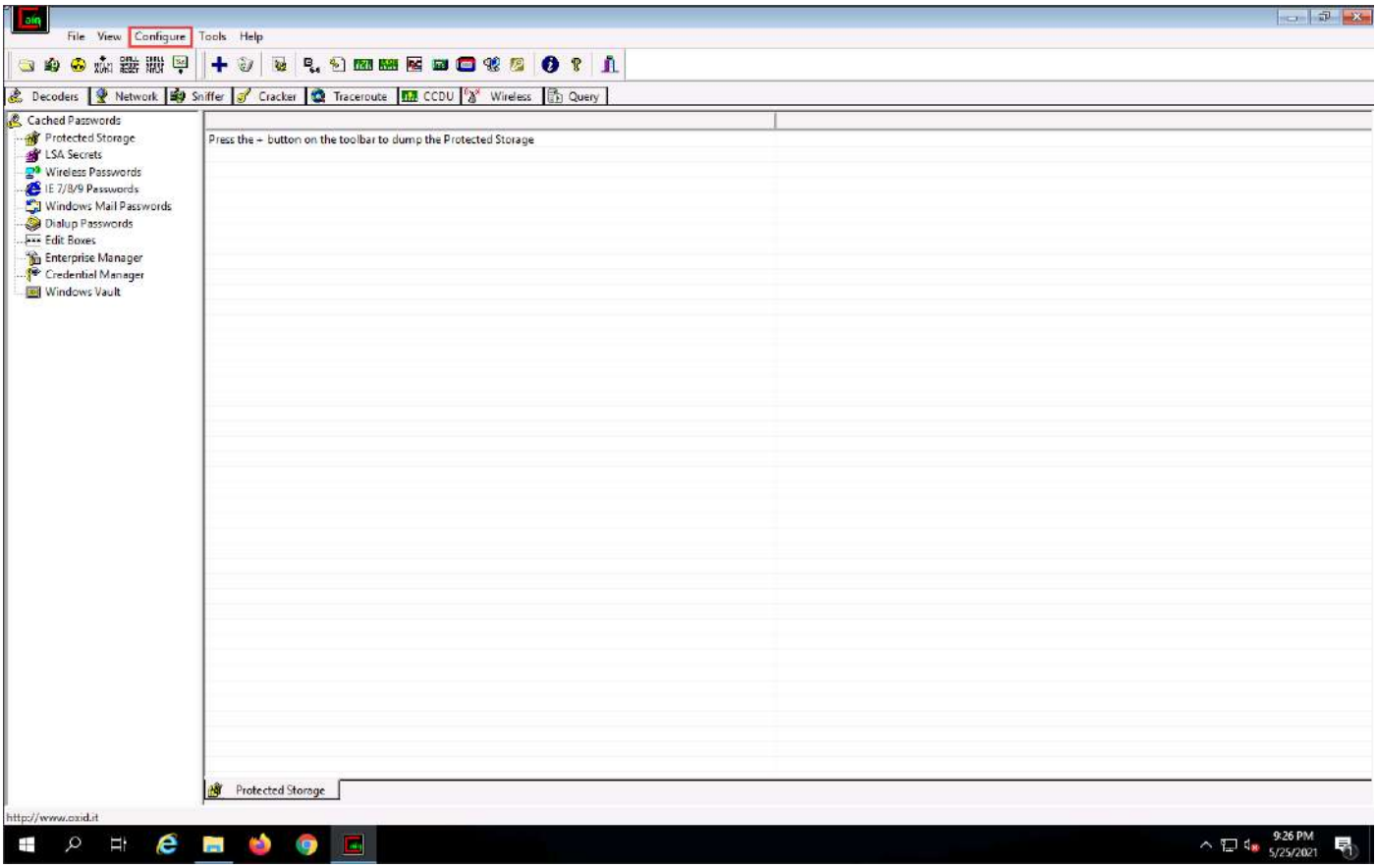


8. Now, double-click the **Cain** icon on **Desktop** to launch **Cain & Abel**.

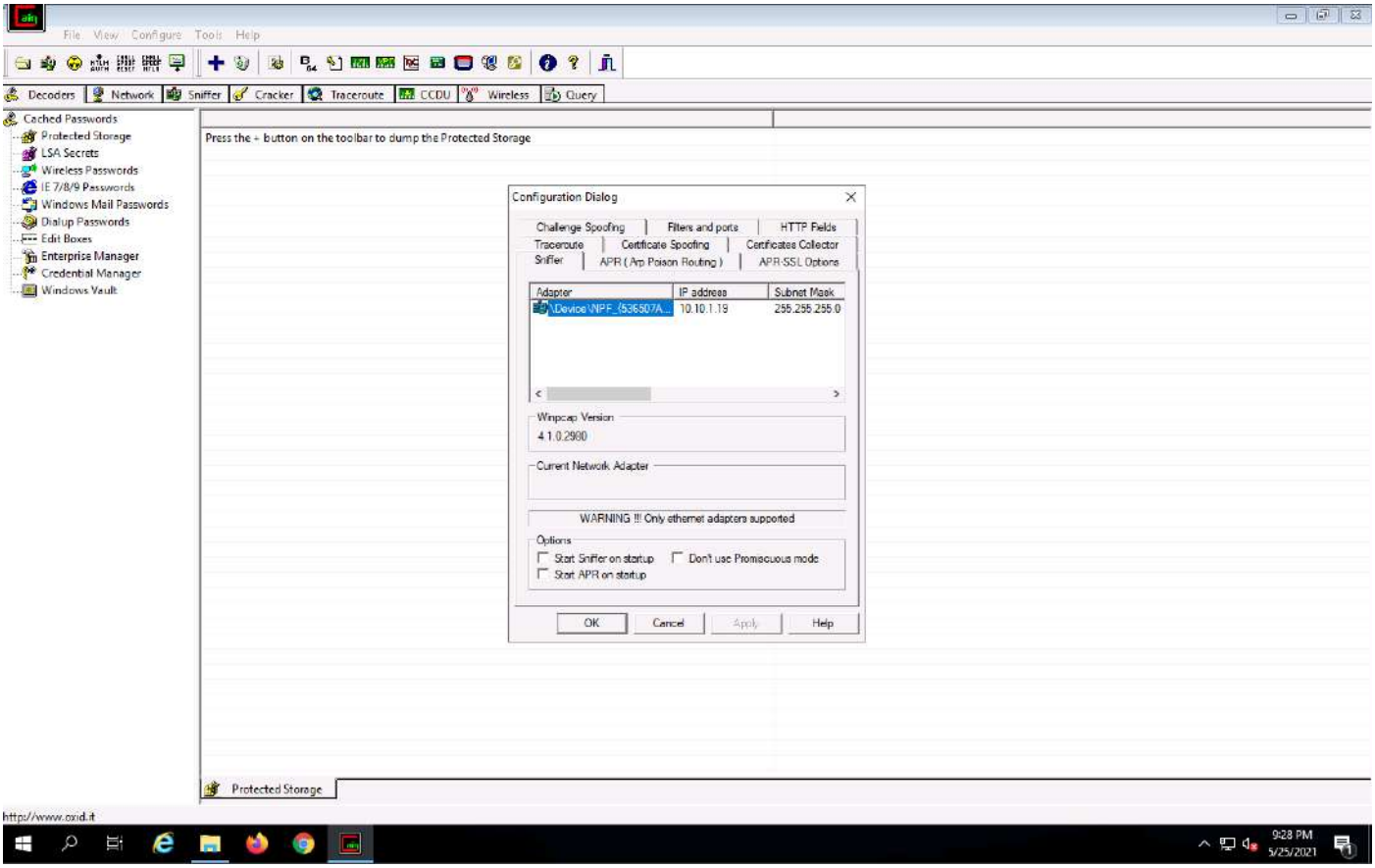
9. The **Cain & Abel** main window appears, as shown in the screenshot.



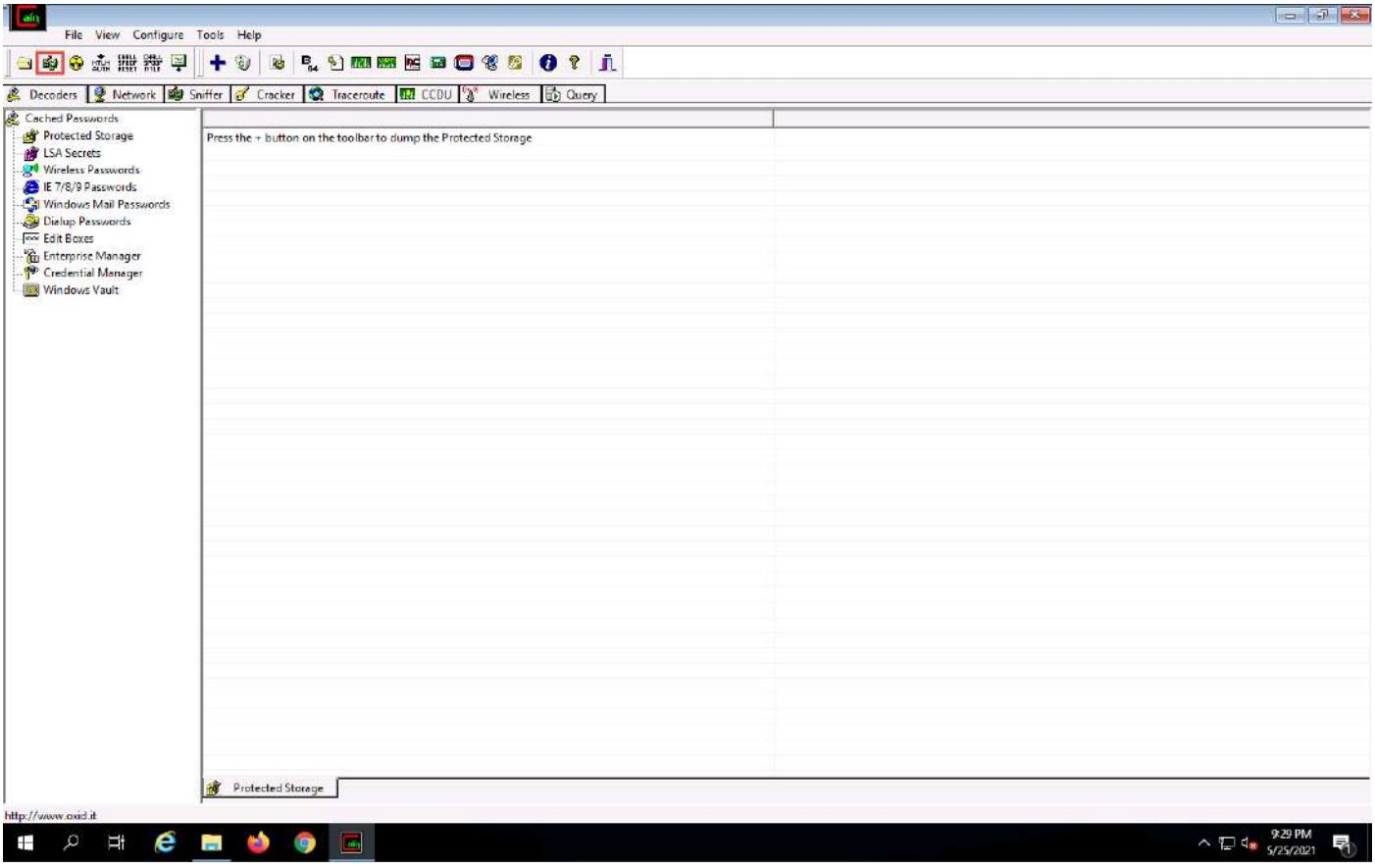
10. Click **Configure** from the menu bar to configure an ethernet card.



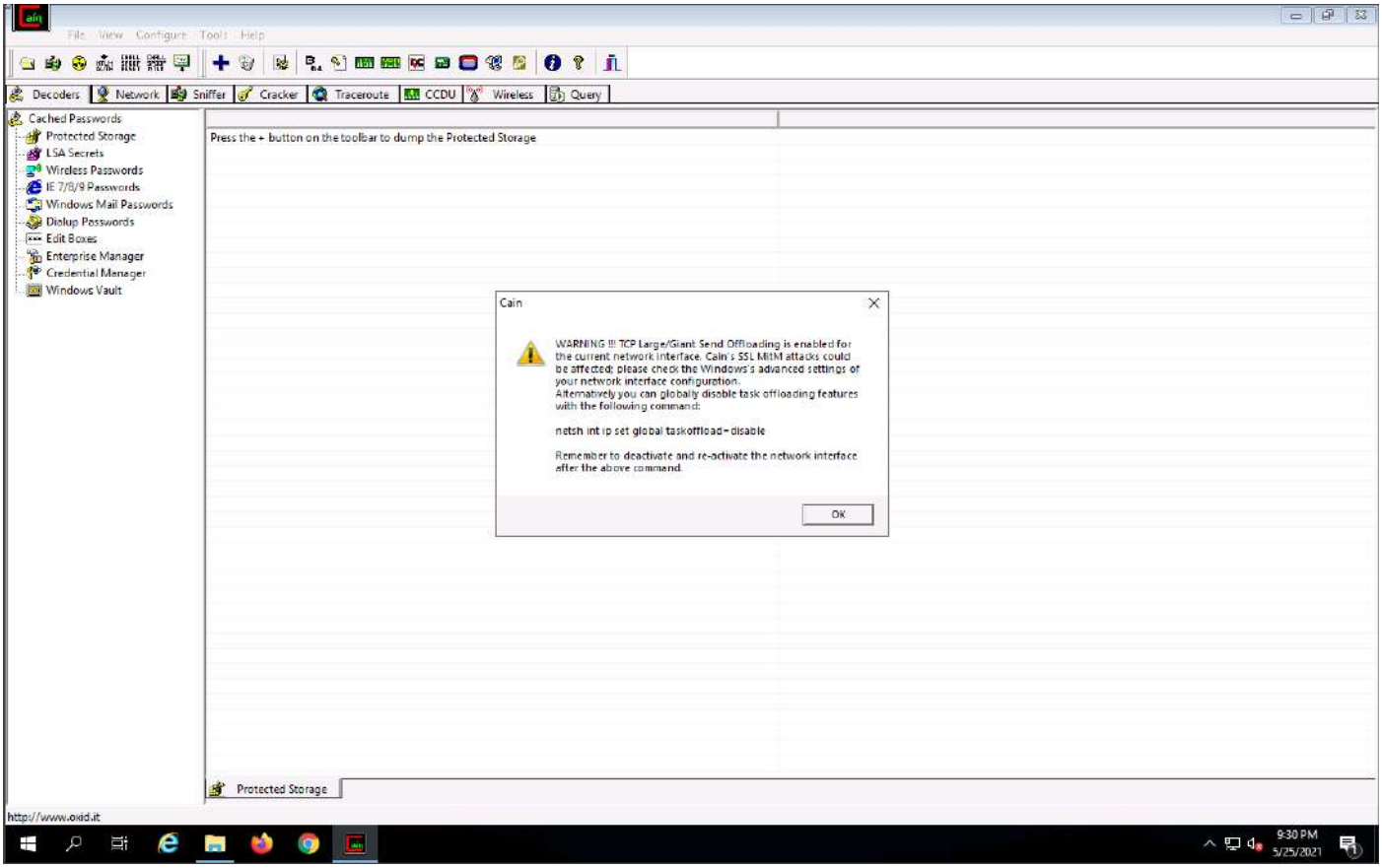
11. The **Configuration Dialog** window appears. The **Sniffer** tab is selected by default. Ensure that the **Adapter** associated with the **IP address** of the machine is selected and click **OK**.



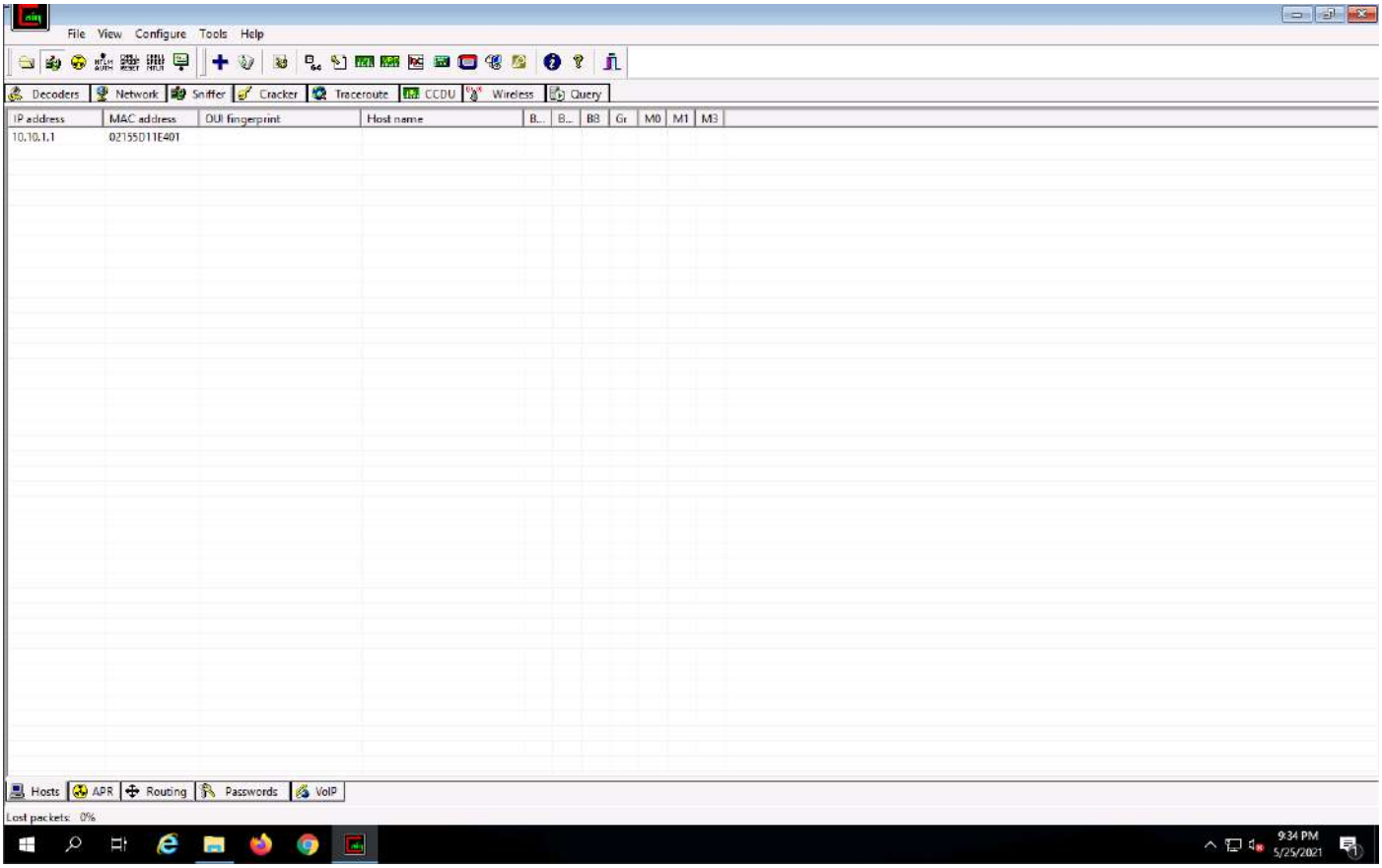
12. Click the **Start/Stop Sniffer** icon on the toolbar to begin sniffing.



13. The **Cain** pop-up appears with a **Warning** message, click **OK**.

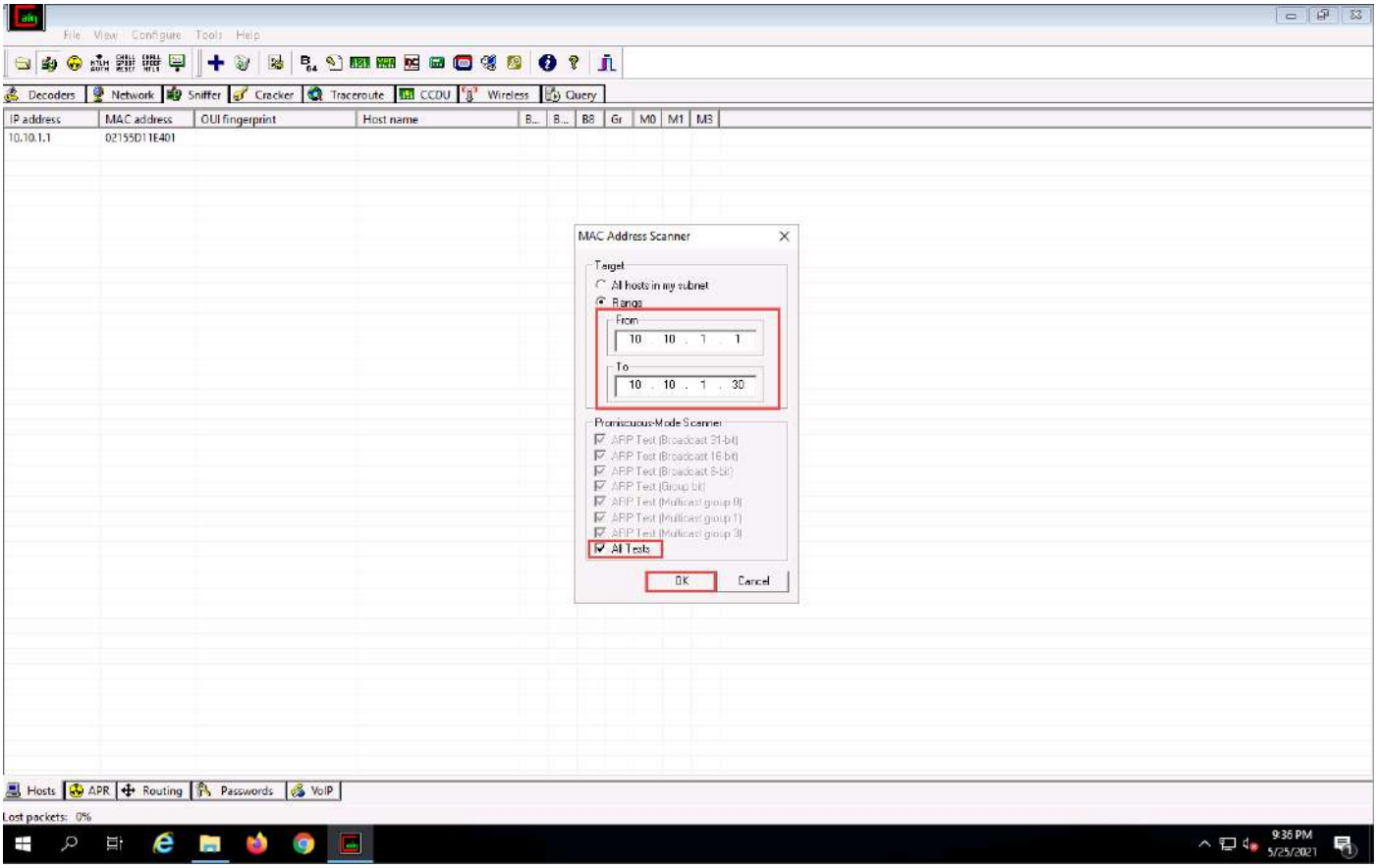


14. Now, click the **Sniffer** tab.

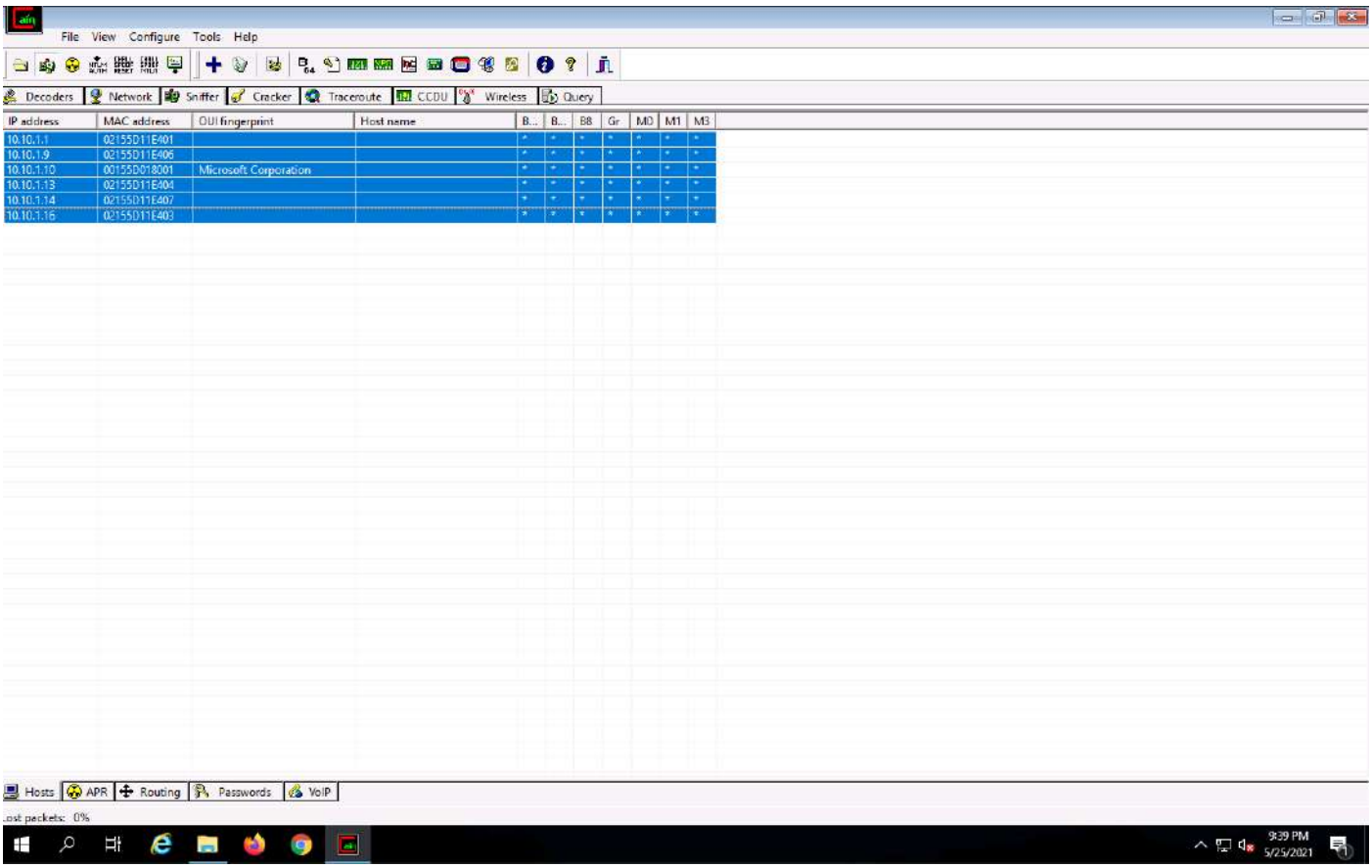


15. Click the plus (**+**) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.

16. The **MAC Address Scanner** window appears. Check the **Range** radio button and specify the IP address range as **10.10.1.1-10.10.1.30**. Select the **All Tests** checkbox; then, click **OK**.

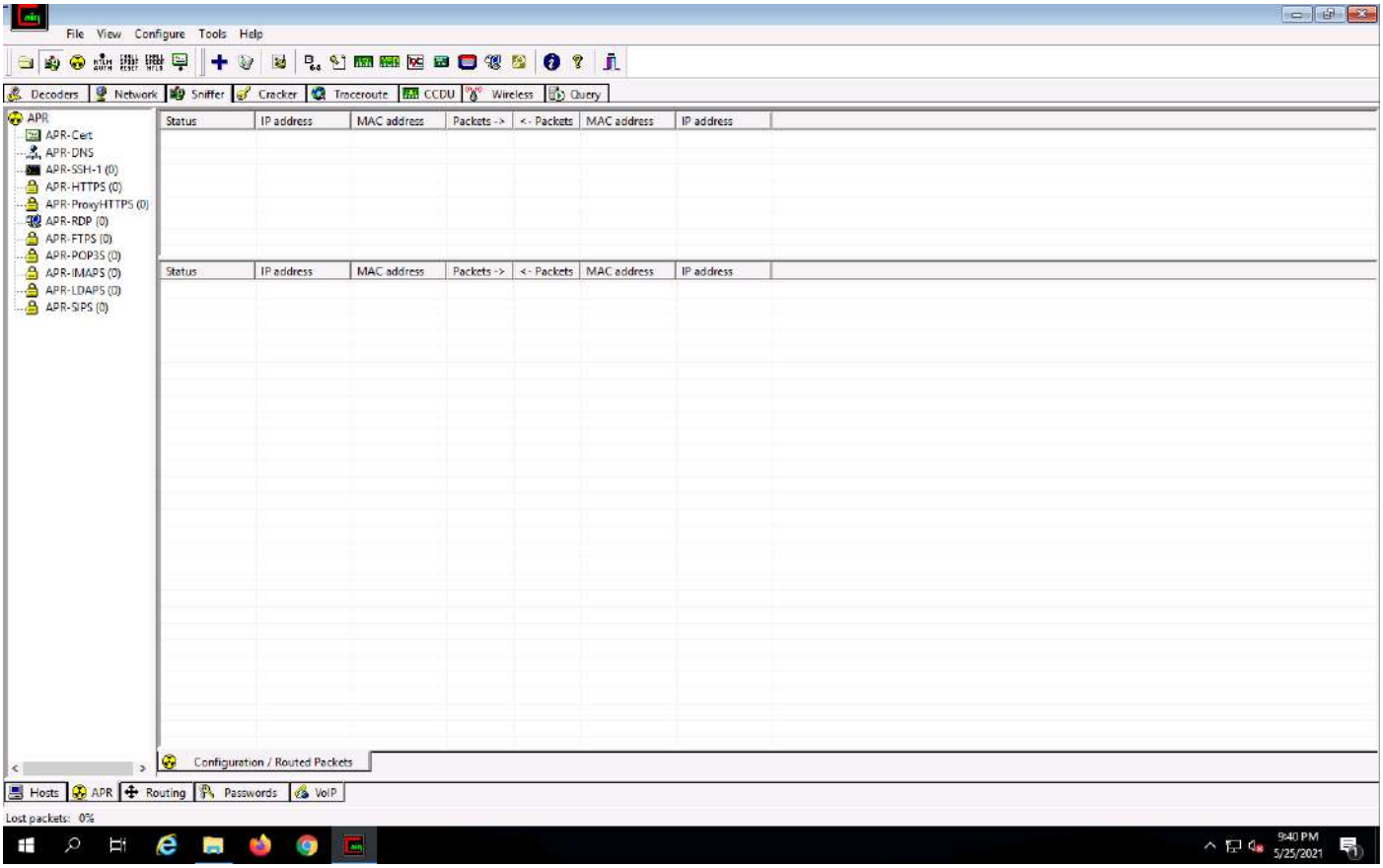


17. Cain & Abel starts scanning for MAC addresses and lists all those found.
18. After the completion of the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.

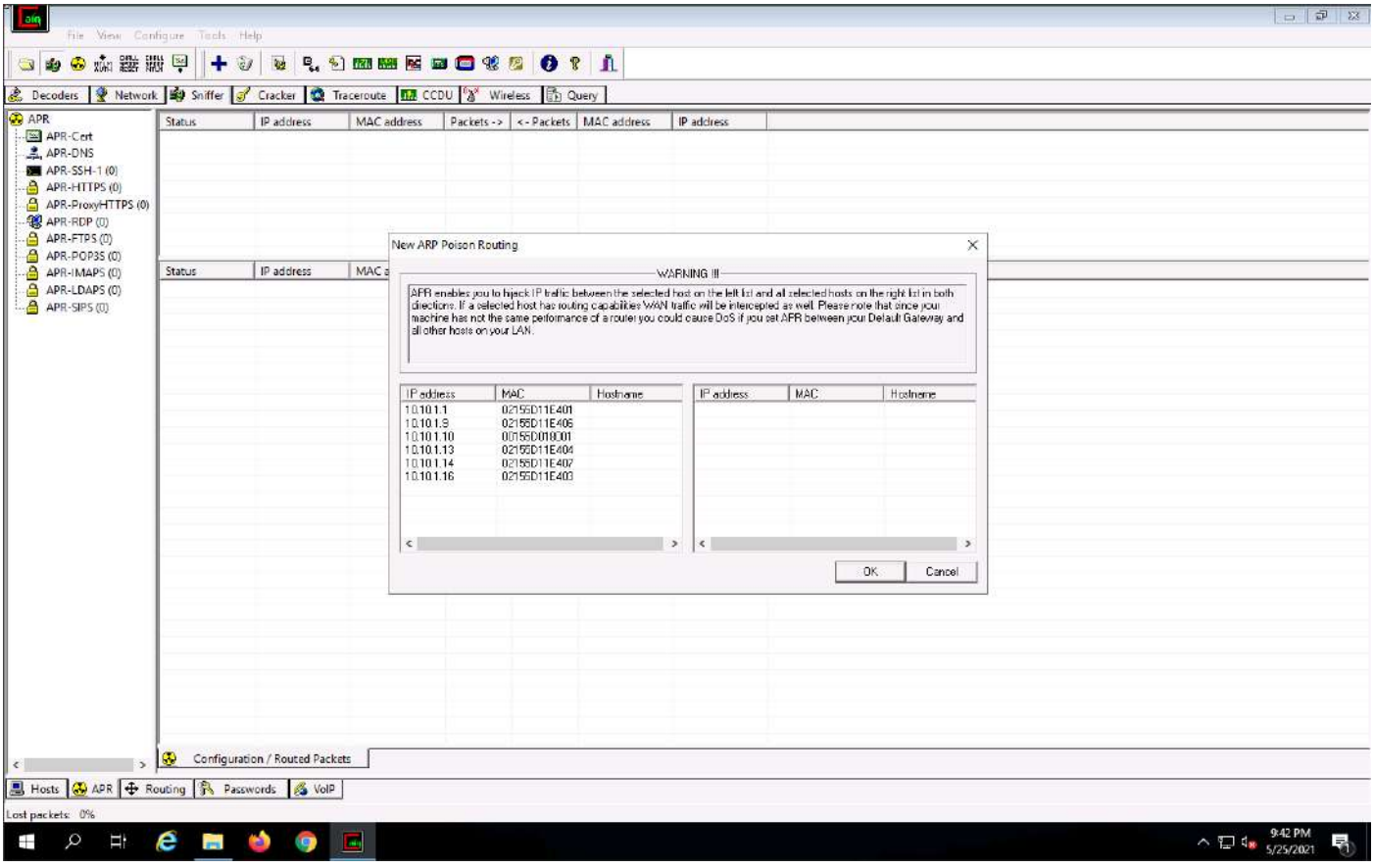


19. Now, click the **APR** tab at the bottom of the window.

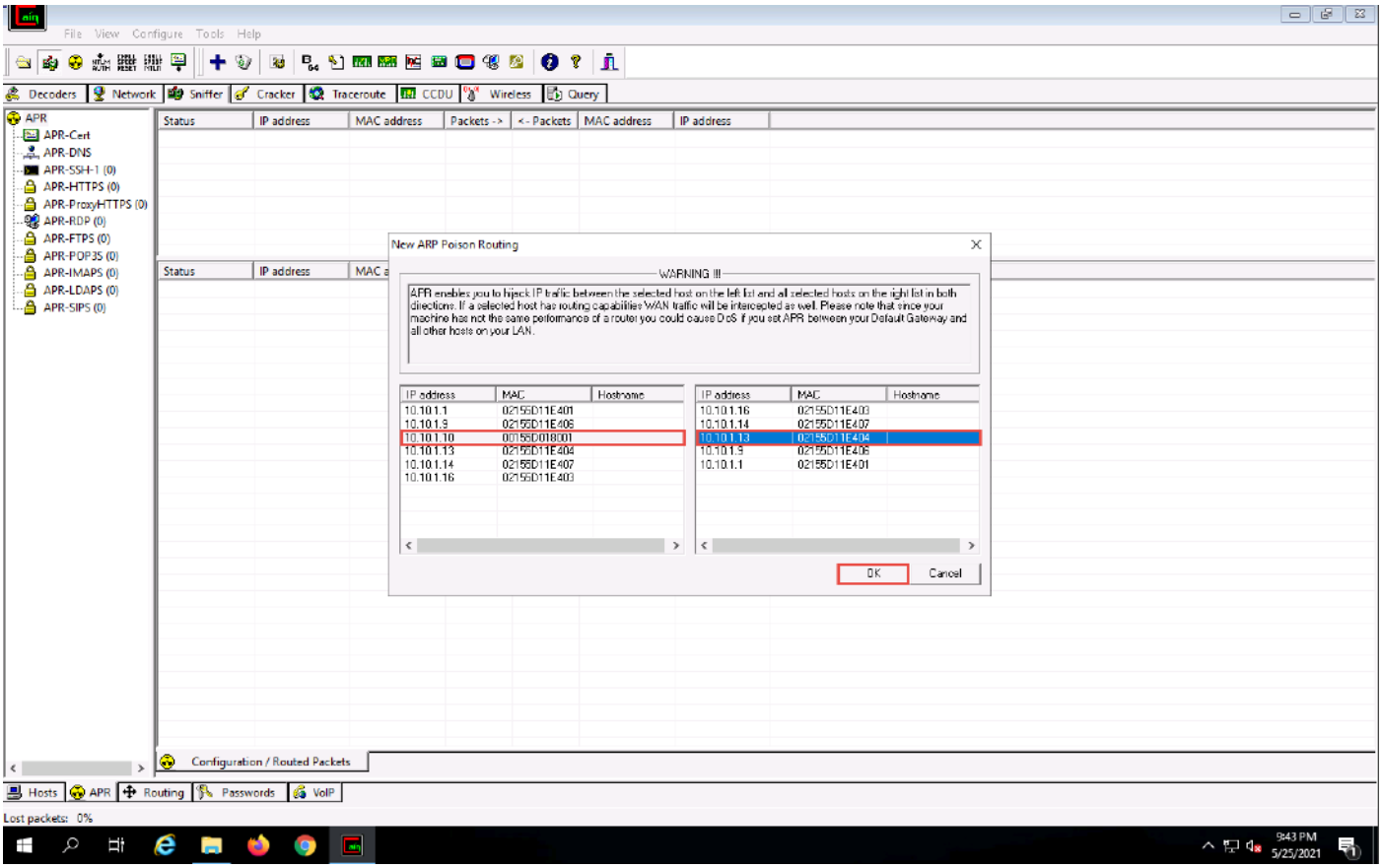
20. APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (**+**) icon.



21. Click the plus (**+**) icon; a **New ARP Poison Routing** window appears; from which we can add IPs to listen to traffic.

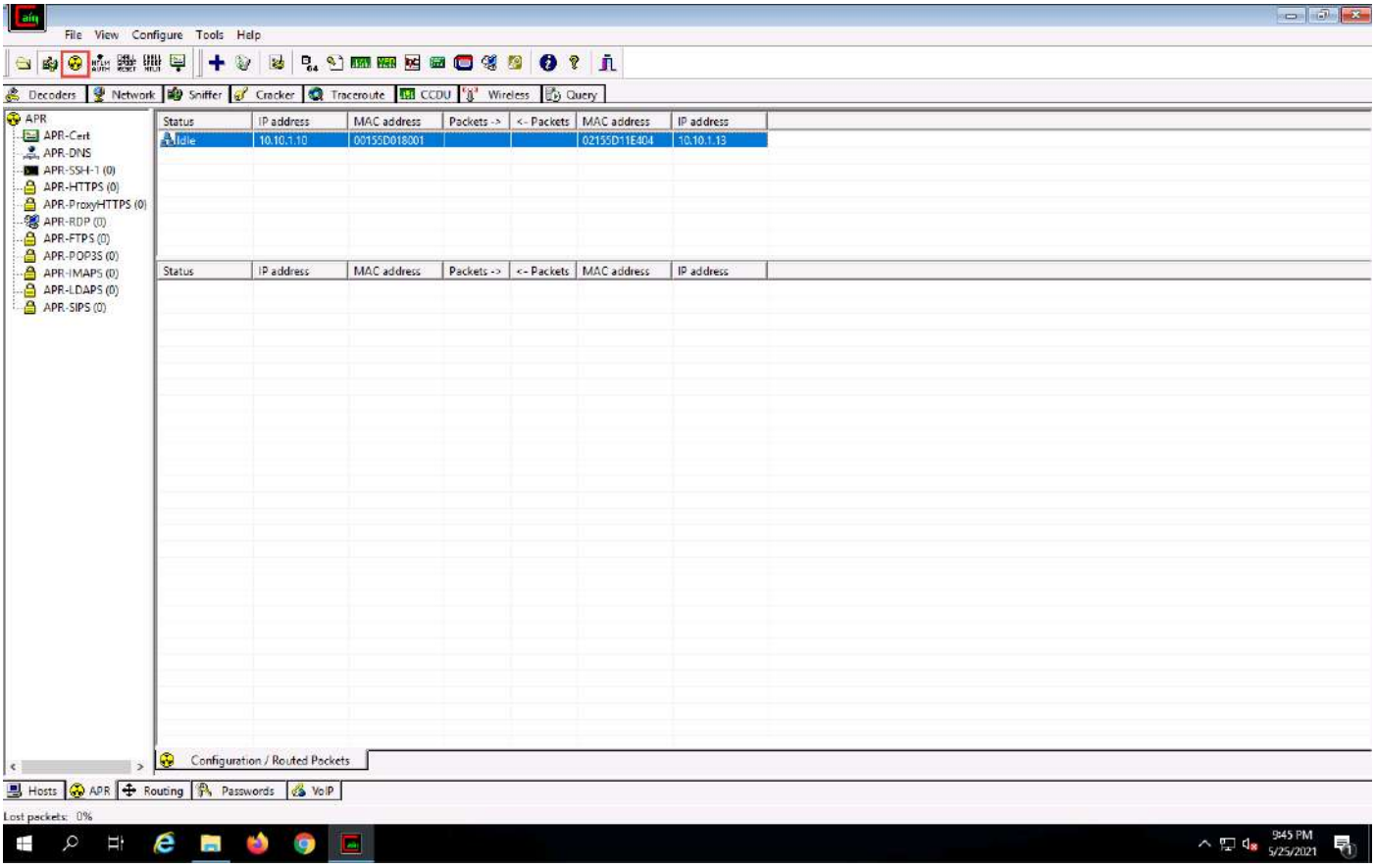


22. To monitor the traffic between two systems (here, **Windows 10** and **Parrot Security**), from the left-hand pane, click to select **10.10.1.10** (**Windows 10**) and from the right-hand pane, click **10.10.1.13** (**Parrot Security**); click **OK**. By doing so, you are setting Cain to perform ARP poisoning between the first and second targets.

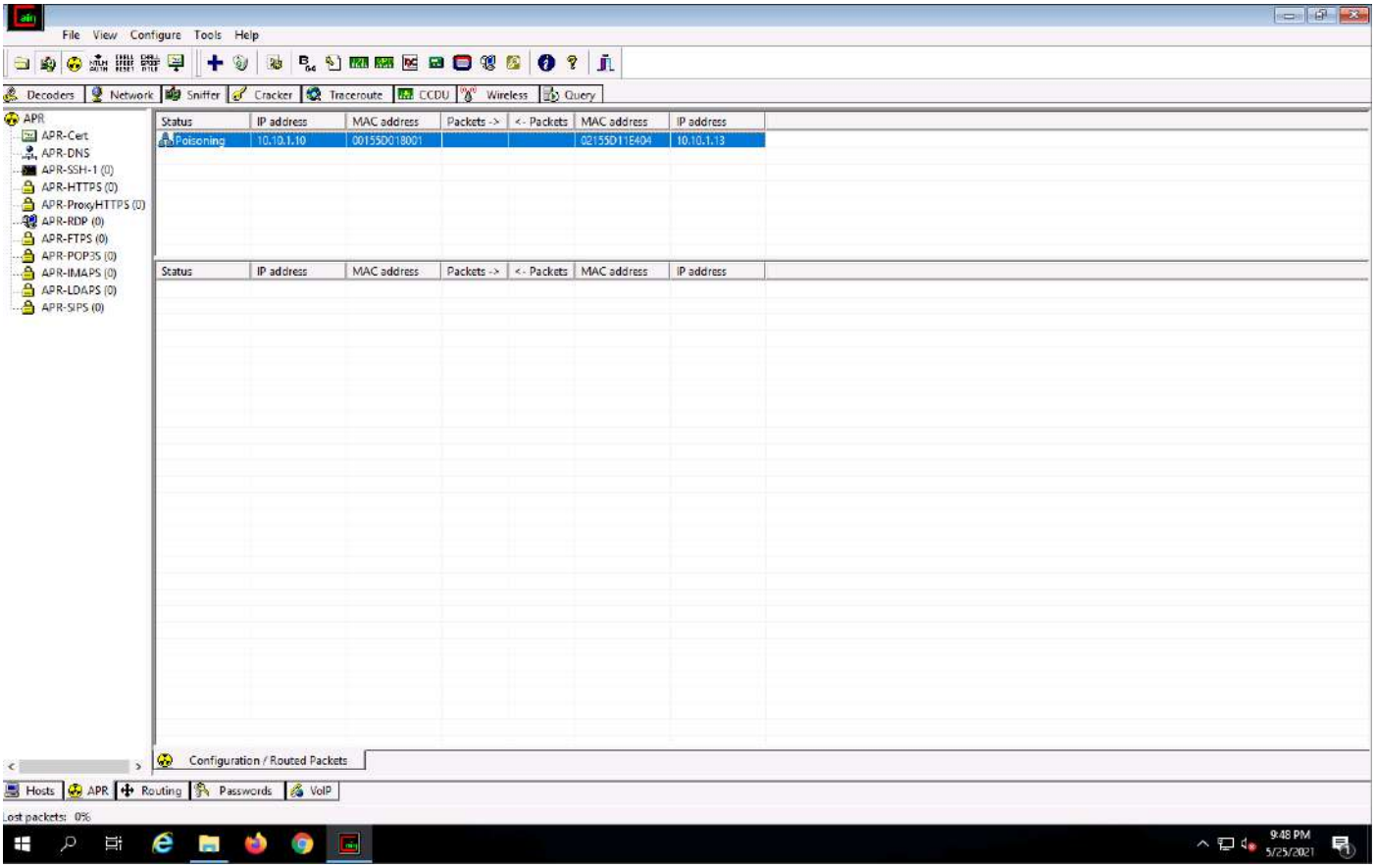


23. Click to select the created target IP address scan that is displayed in the **Configuration / Routed Packets** tab.

24. Click on the **Start/Stop** APR icon to start capturing ARP packets.



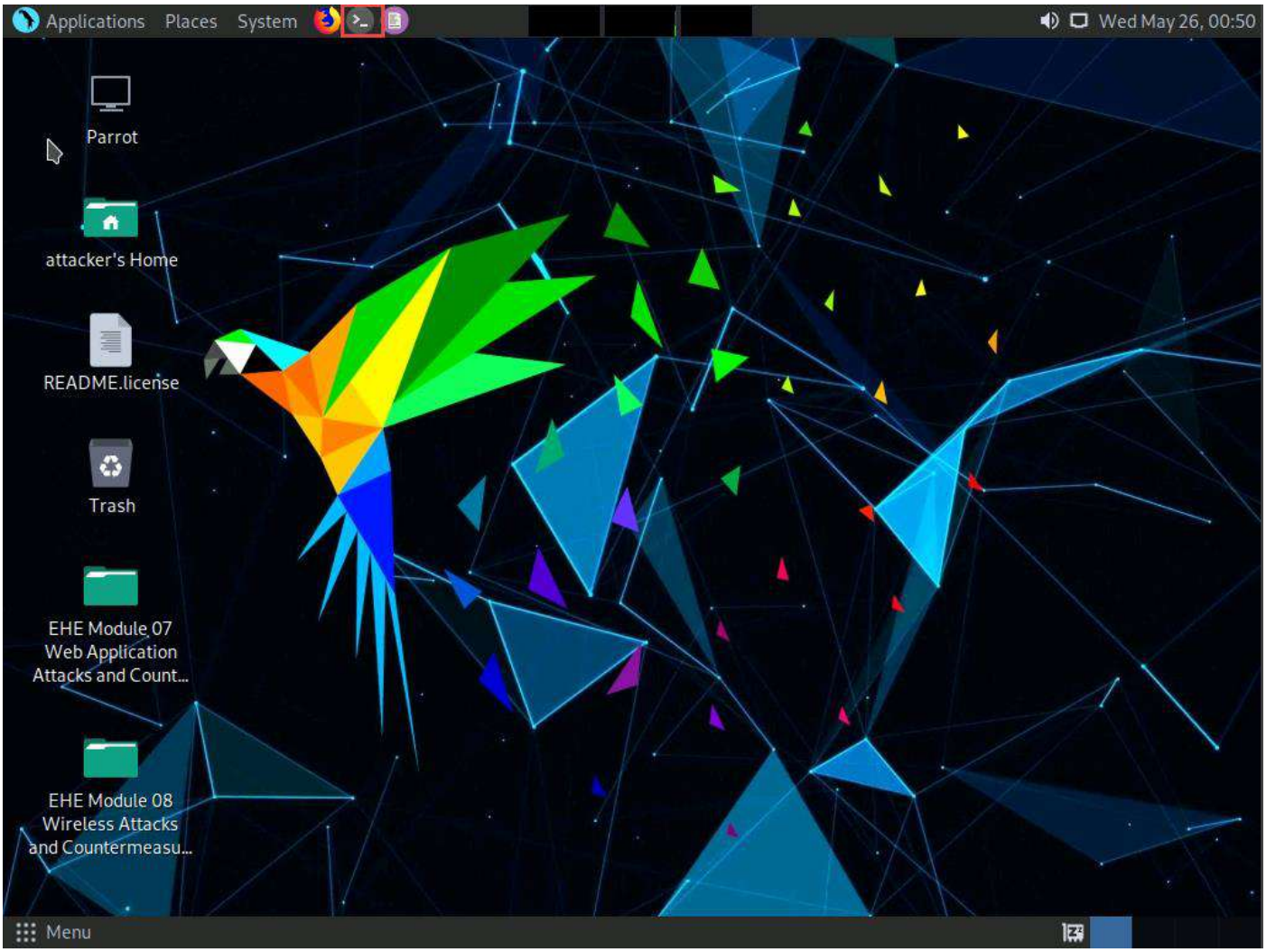
25. After clicking on the **Start/Stop** APR icon, Cain & Abel starts ARP poisoning and the status of the scan changes to **Poisoning**, as shown in the screenshot.



26. Cain & Abel intercepts the traffic traversing between these two machines.

27. To generate traffic between the machines, you need to ping one target machine using the other.

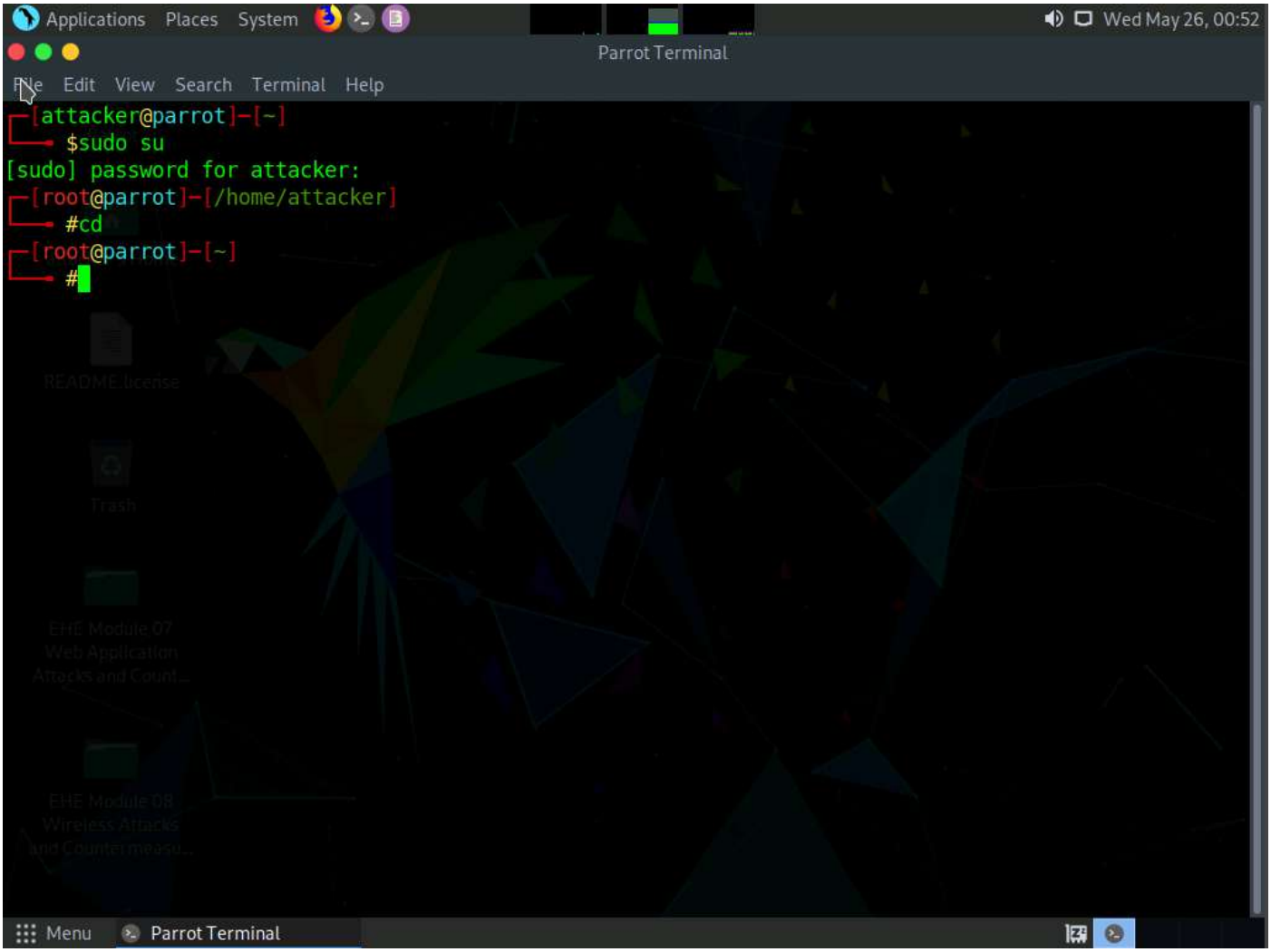
28. Click Parrot Security to switch to the **Parrot Security** machine.
29. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



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

The password that you type will not be visible.

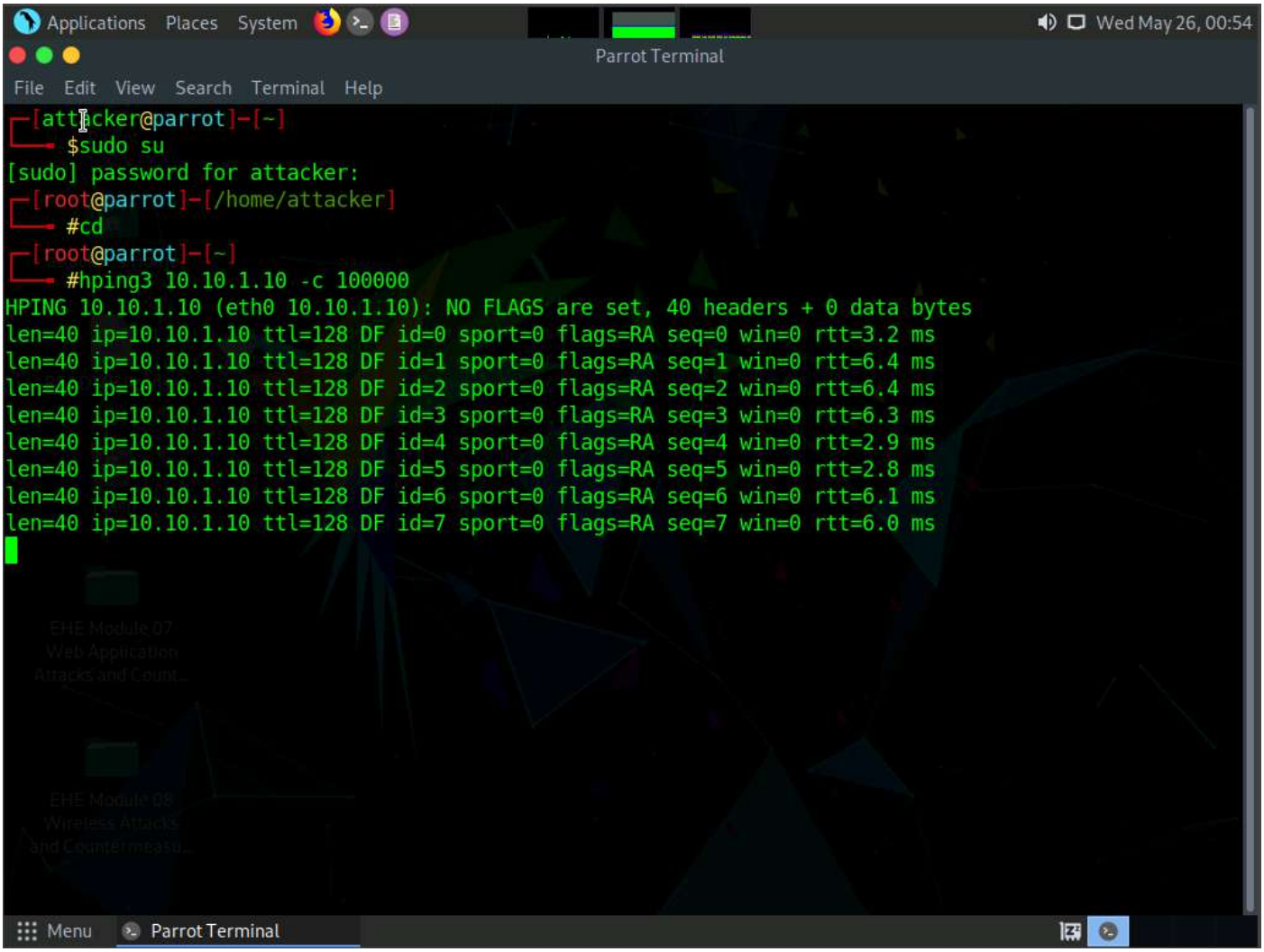
32. Now, type **cd** and press **Enter** to jump to the root directory.



33. In the terminal window, type **hping3 [Target IP Address] -c 100000** (here, target IP address is **10.10.1.10 [Windows 10]**) and press **Enter**.

-c: specifies the packet count.

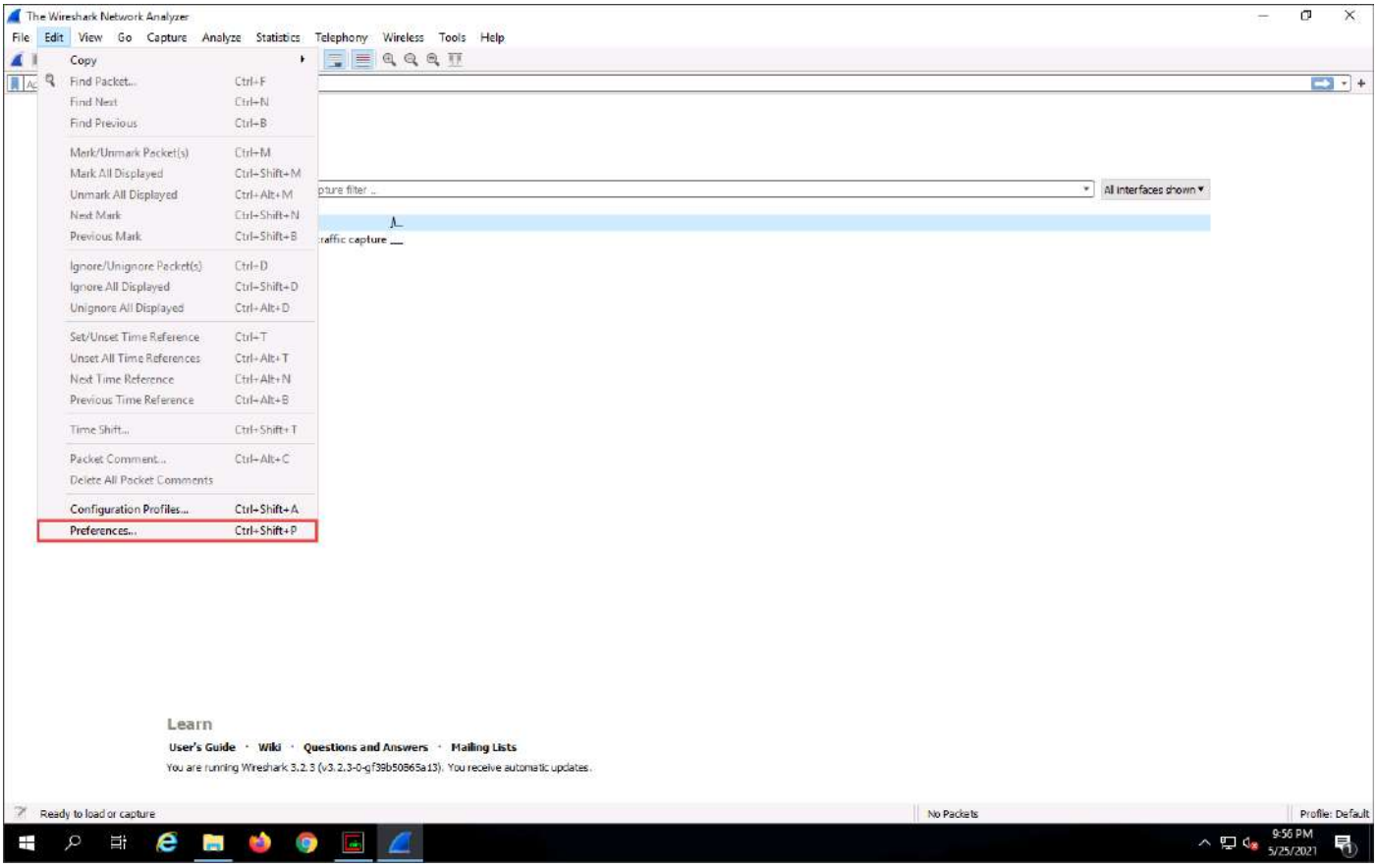
34. This command will start pinging the target machine (**Windows 10**) with 100,000 packets.



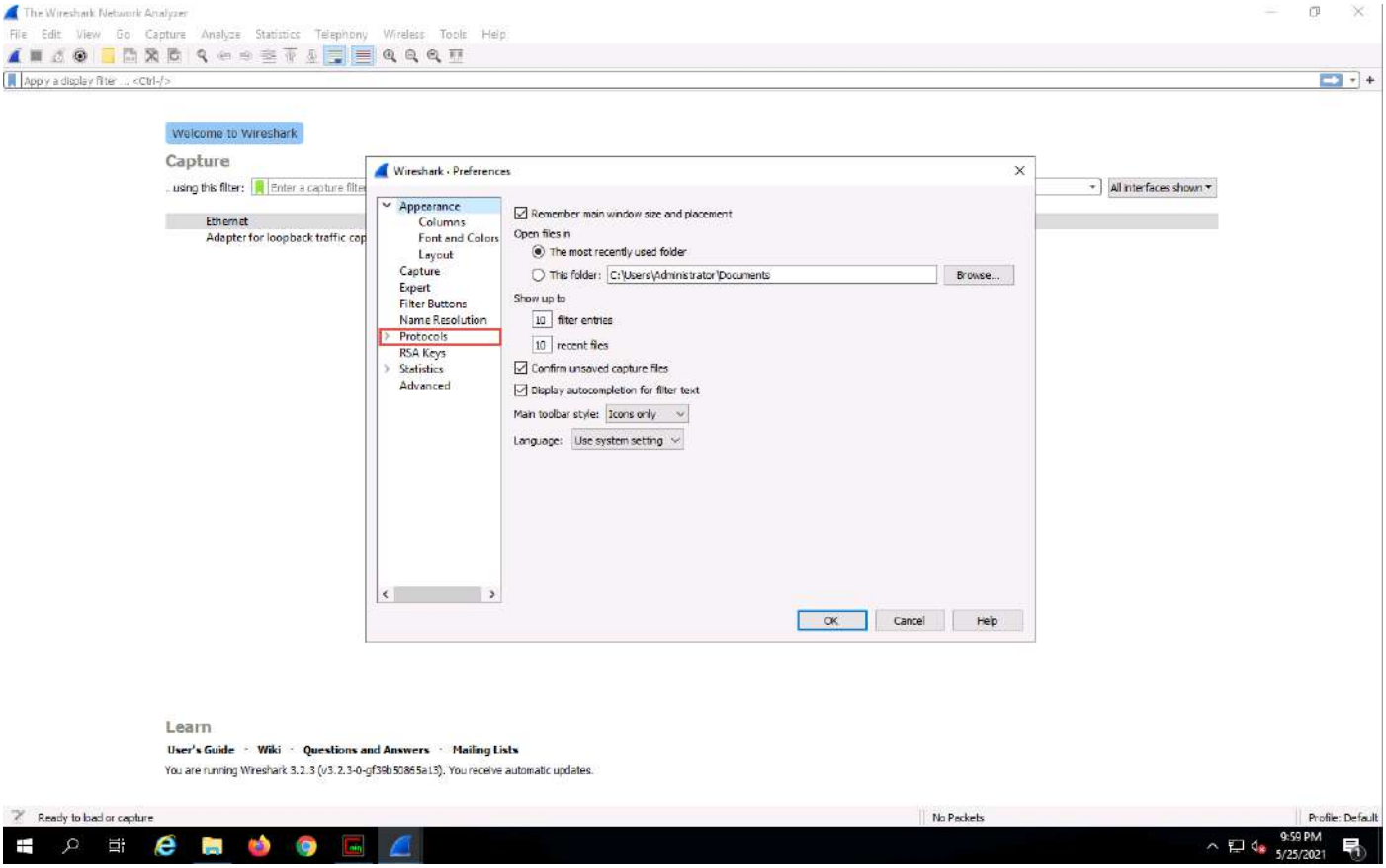
35. Leave the command running and immediately click Windows Server 2019 to switch to the **Windows Server 2019** machine.

36. Navigate to the **Desktop** and double-click **Wireshark** shortcut to launch it.

37. The **Wireshark Network Analyzer** window appears; click **Edit** in the menu bar and select **Preferences...**.

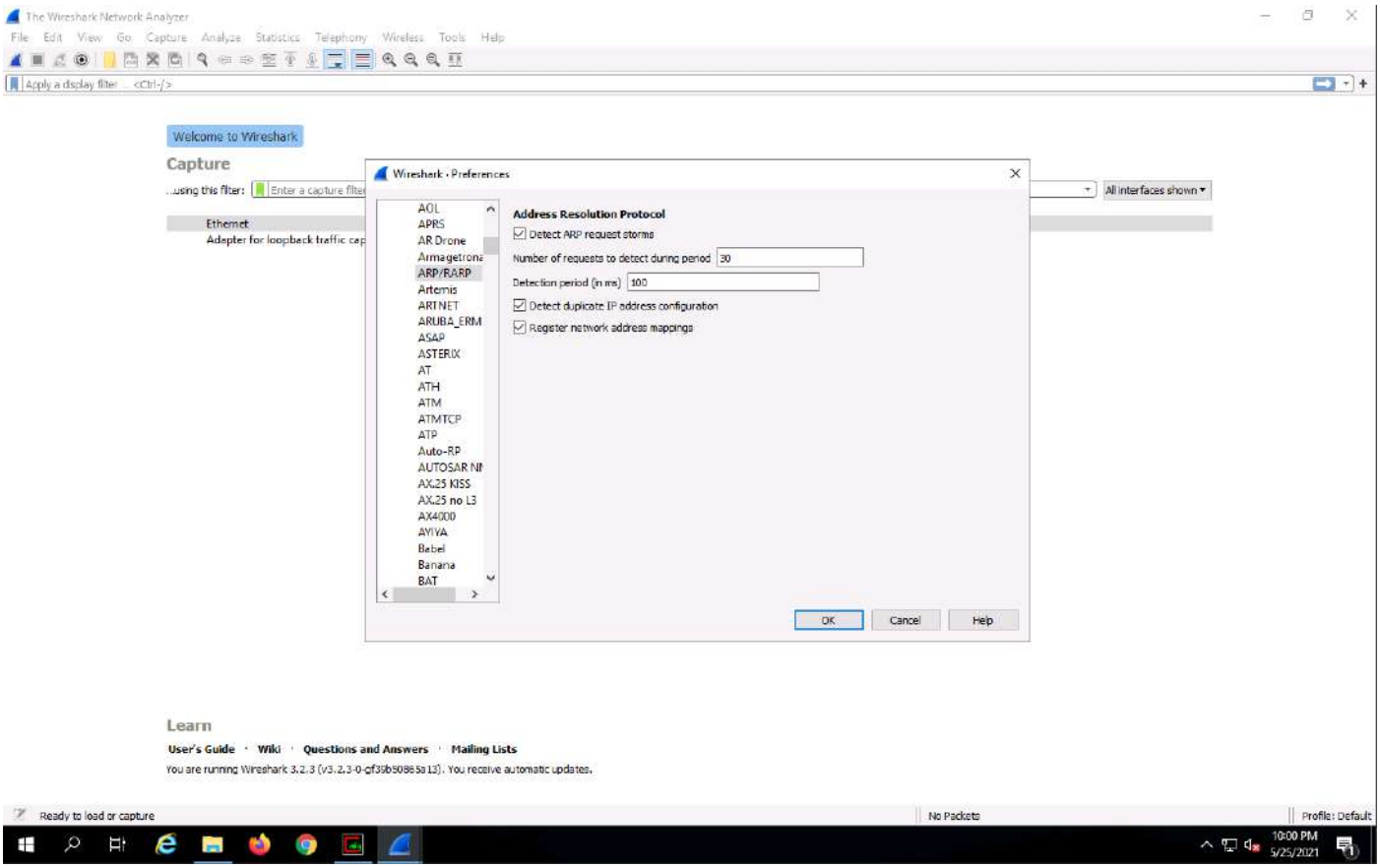


38. The **Wireshark . Preferences** window appears; expand the **Protocols** node.

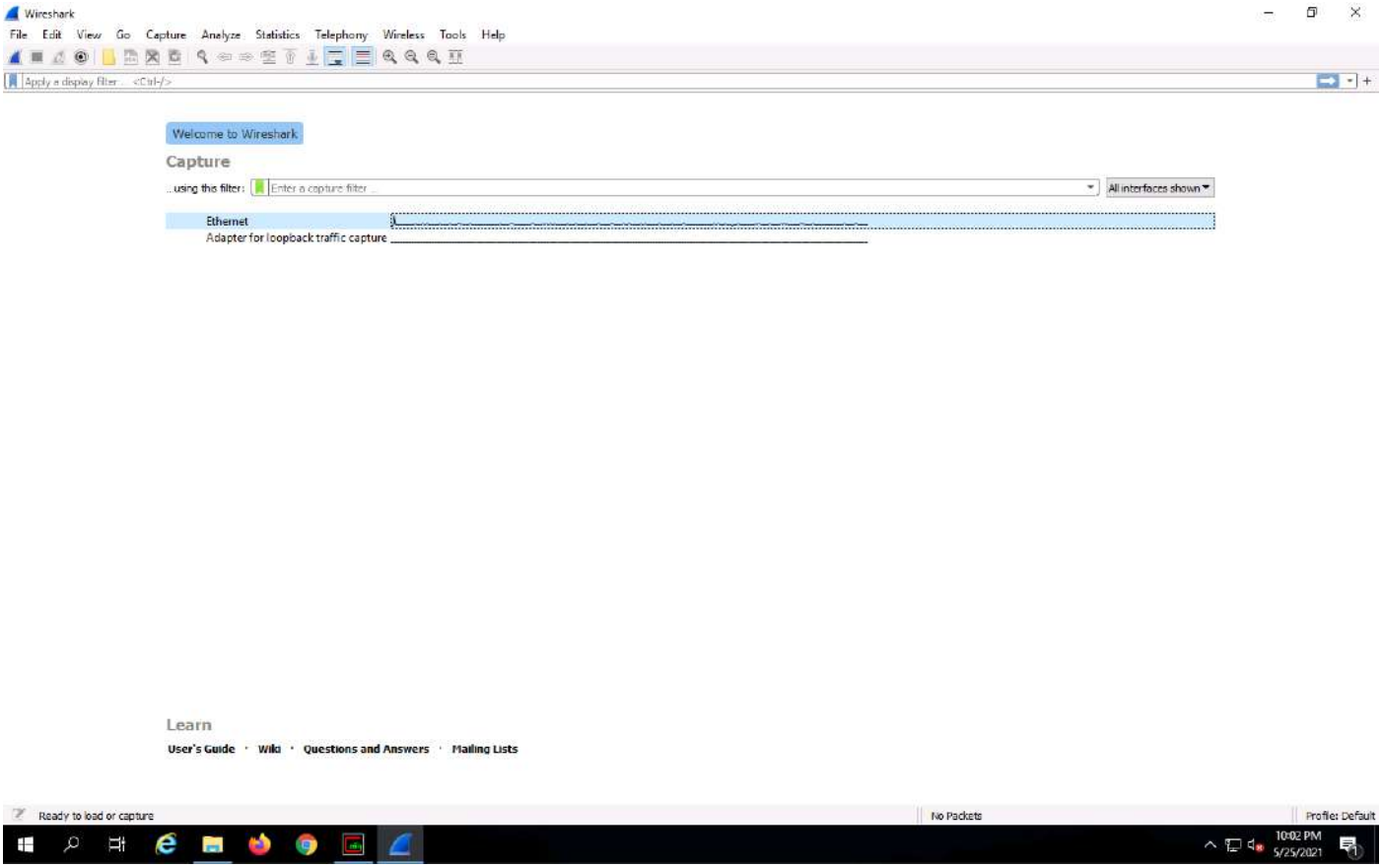


39. Scroll-down in the **Protocols** node and select the **ARP/RARP** option.

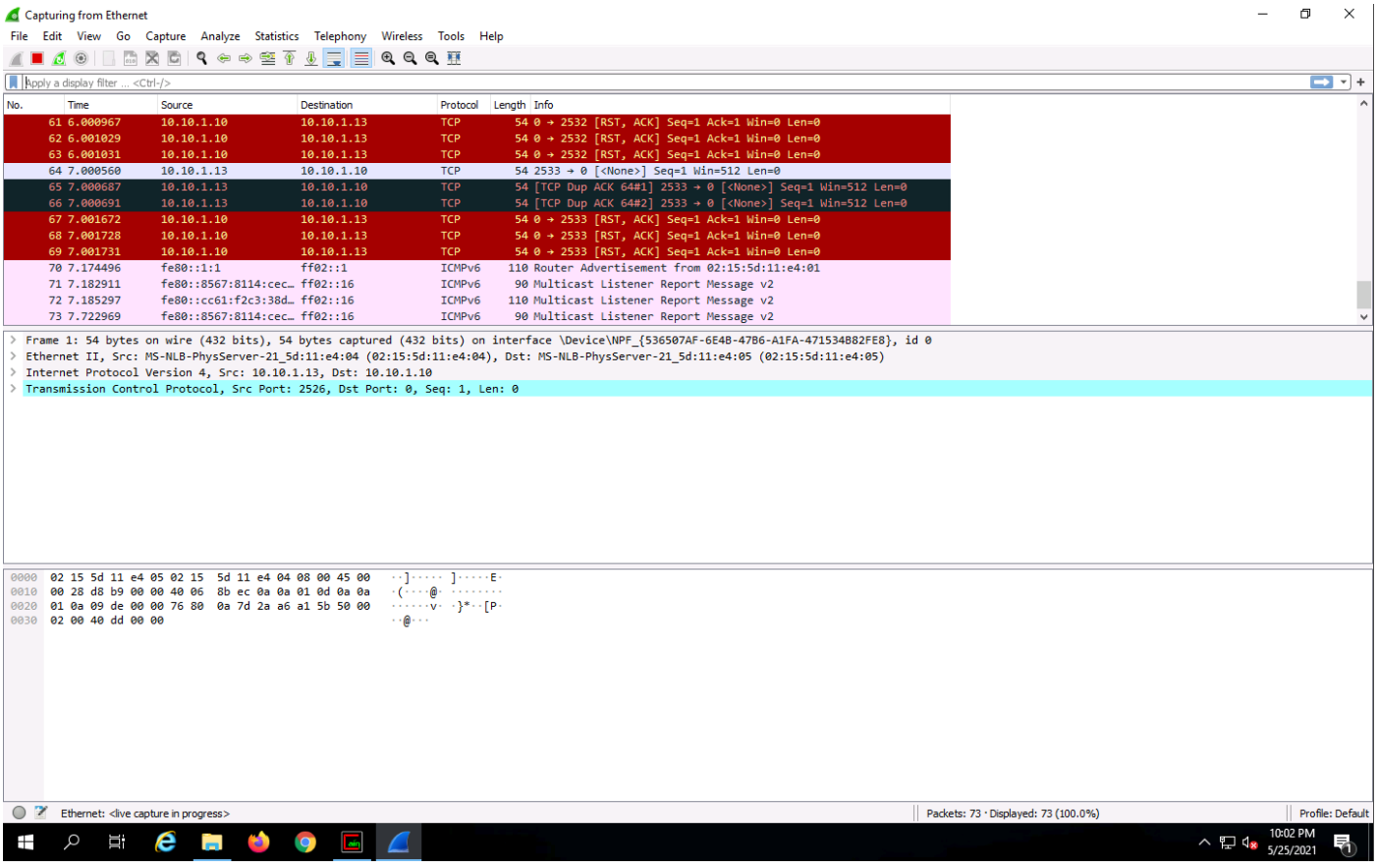
40. From the right-hand pane, click the **Detect ARP request storms** checkbox and ensure that the **Detect duplicate IP address configuration** checkbox is checked; click **OK**.



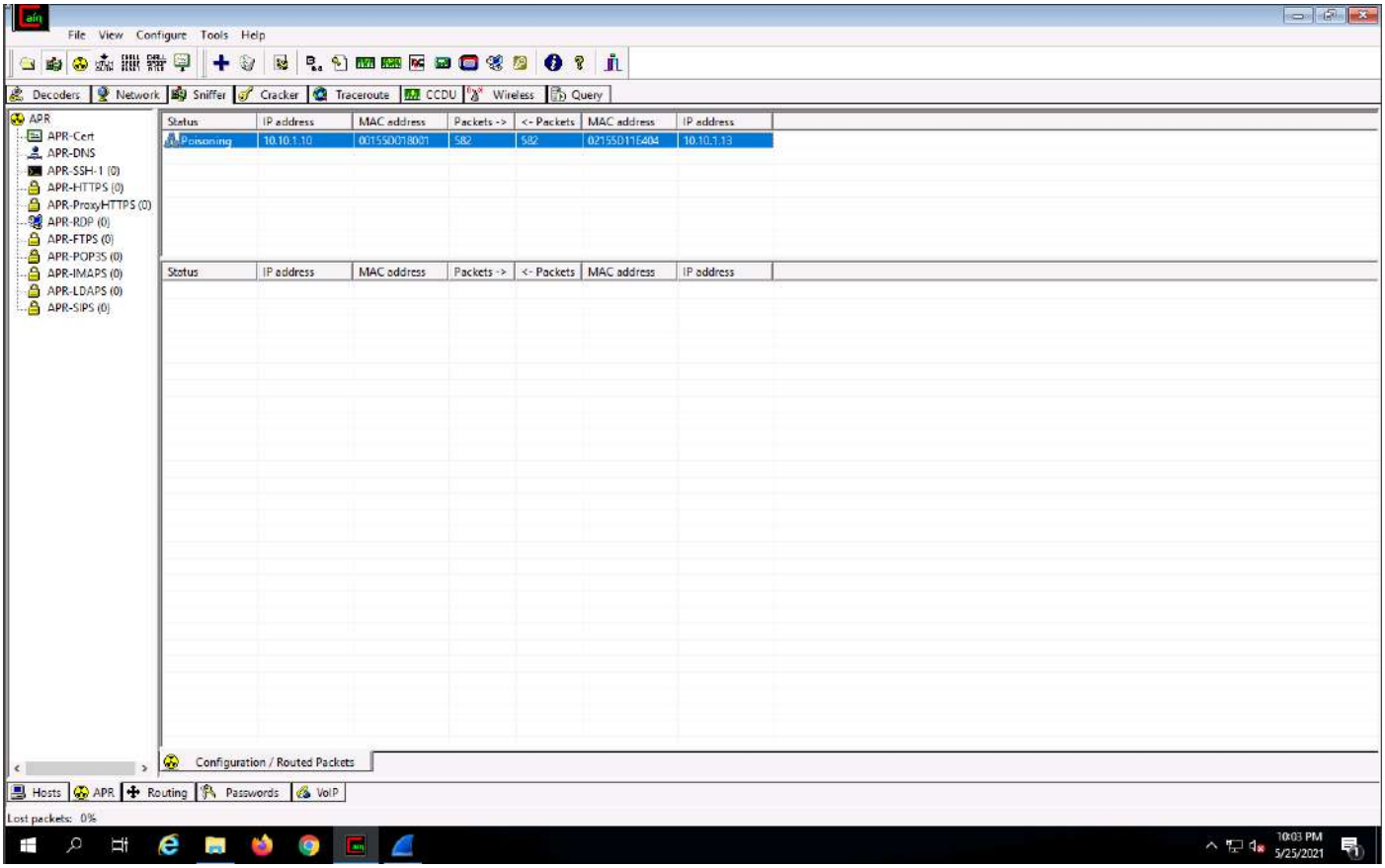
41. Now, double-click on the adapter associated with your network (here, **Ethernet**) to start capturing the network packets.



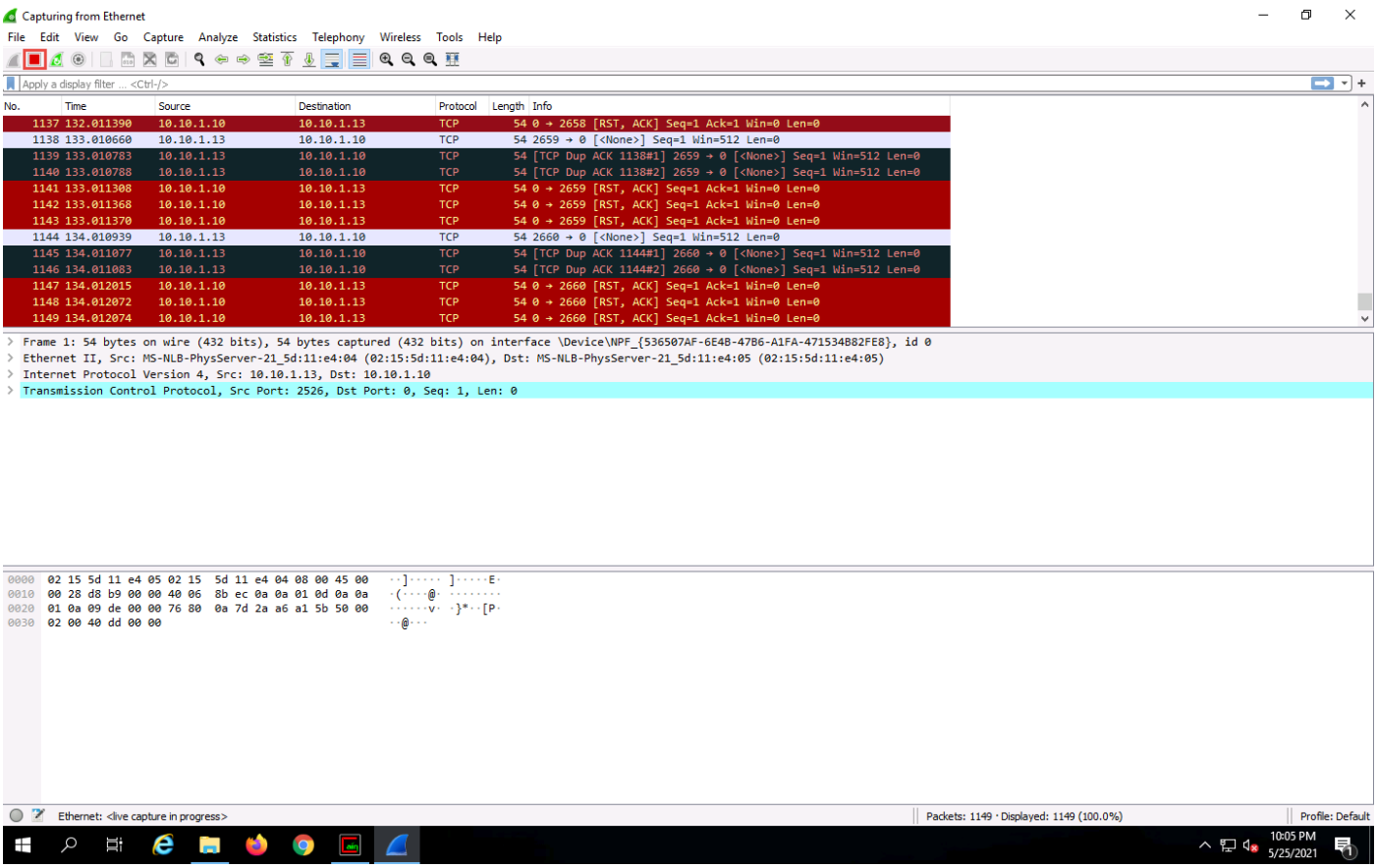
42. **Wireshark** begins to capture the traffic between the two machines, as shown in the screenshot.



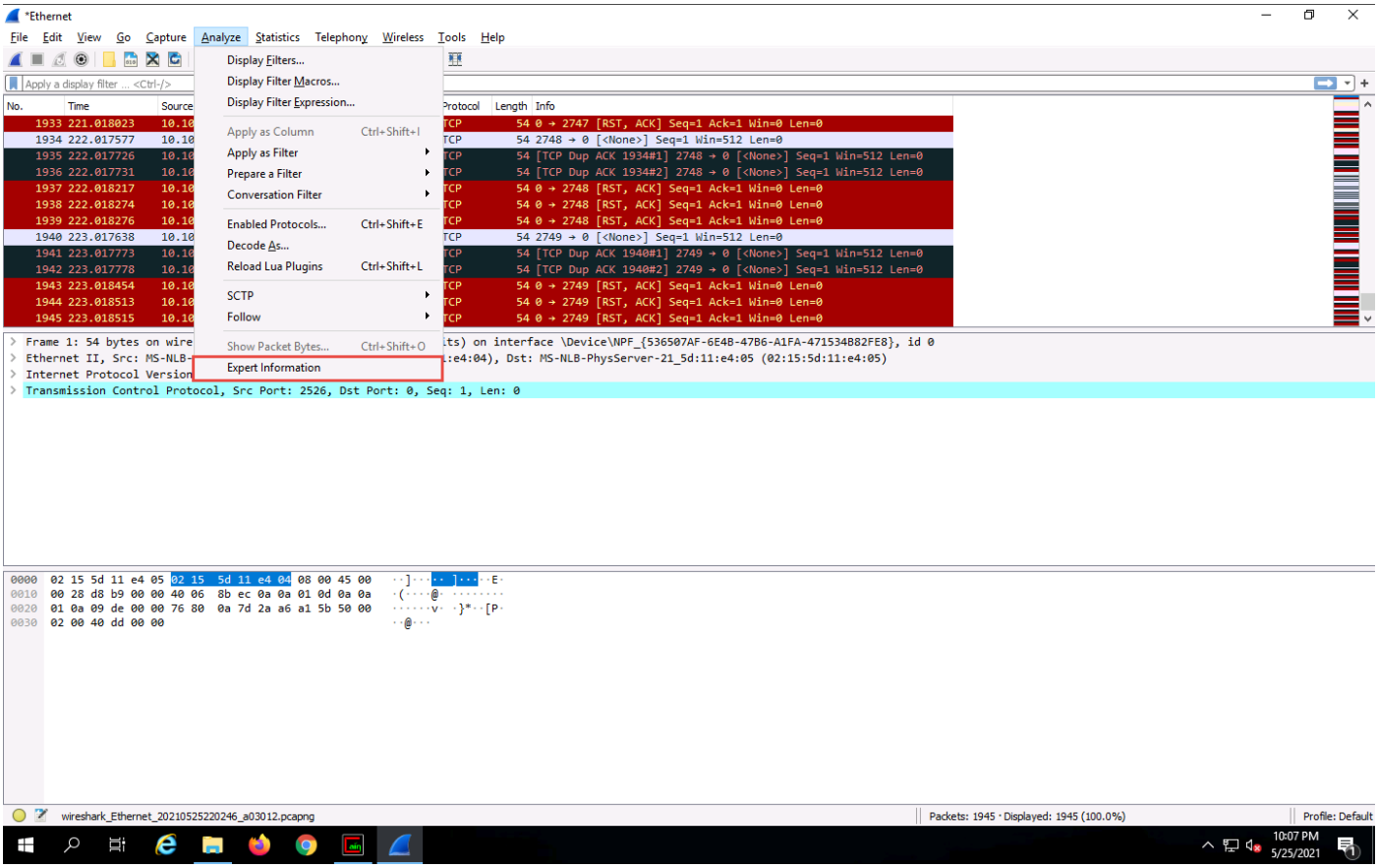
43. Switch to the **Cain & Abel** window to observe the packets flowing between the two machines.



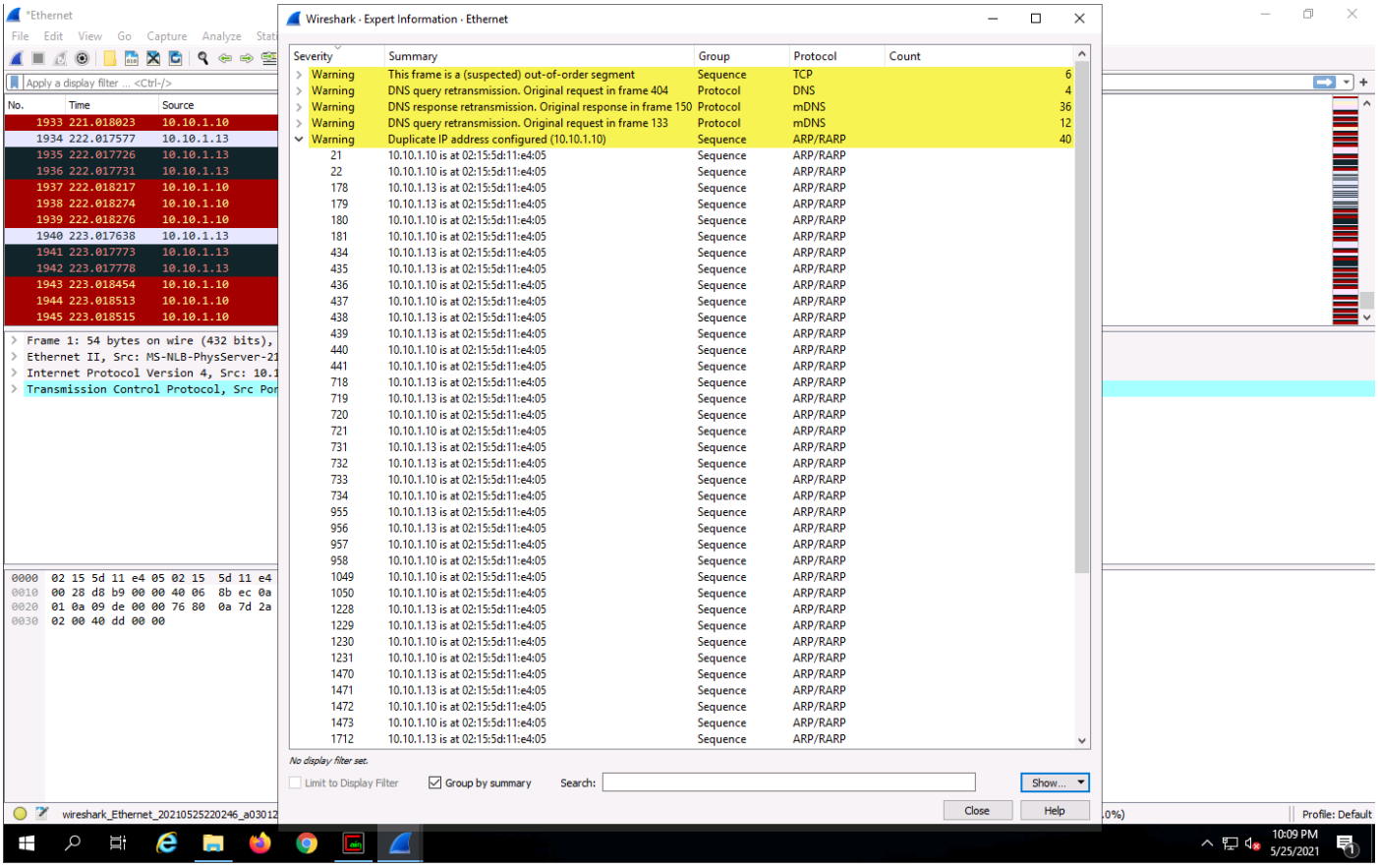
44. Now, switch to **Wireshark** and click the **Stop capturing packets** icon to stop the packet capturing.



45. Click **Analyze** from the menu bar and select **Expert Information** from the drop-down options.

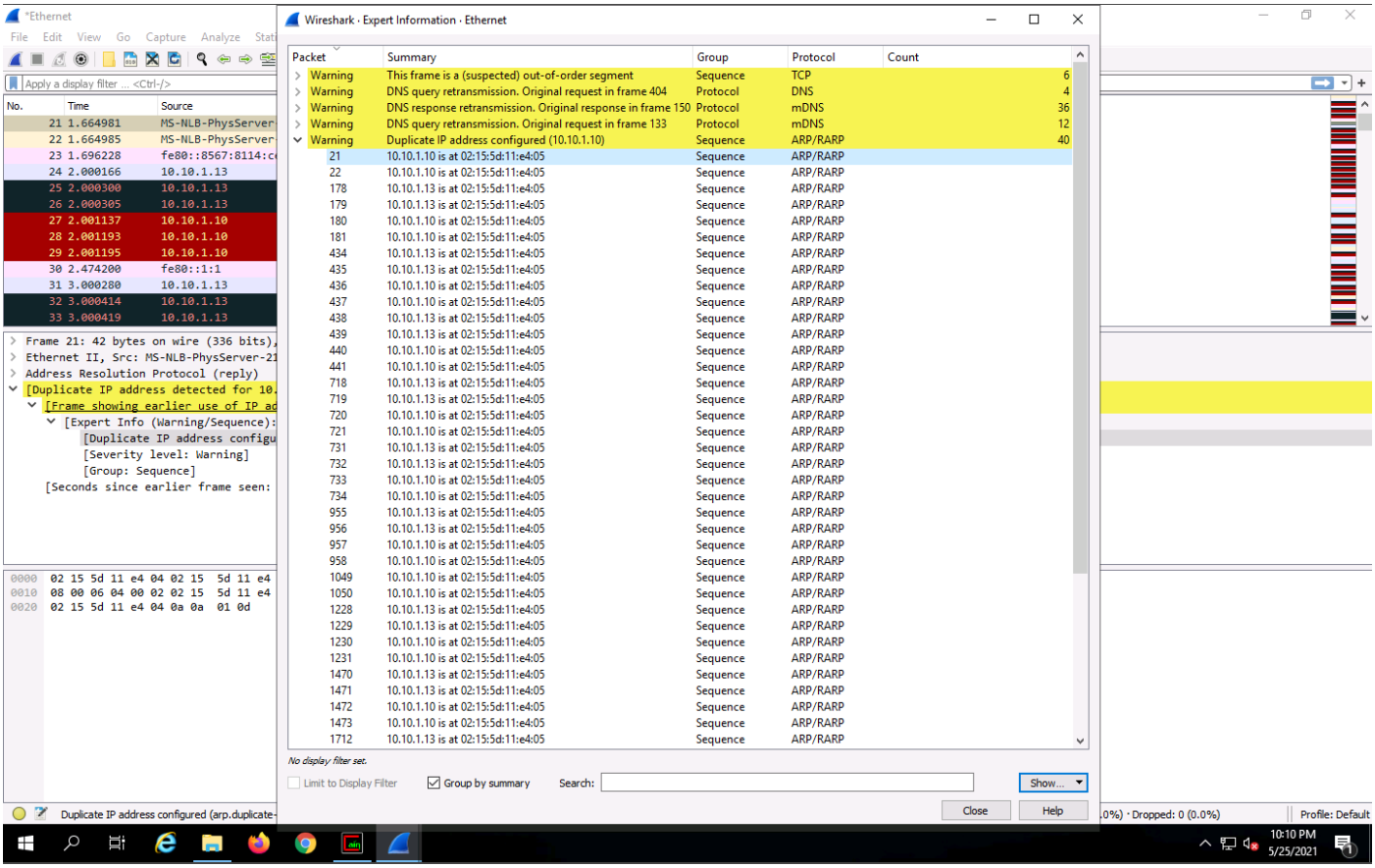


46. The **Wireshark . Expert Information** window appears; click to expand the **Warning** node labeled **Duplicate IP address configured (10.10.1.10)**, running on the **ARP/RARP** protocol.



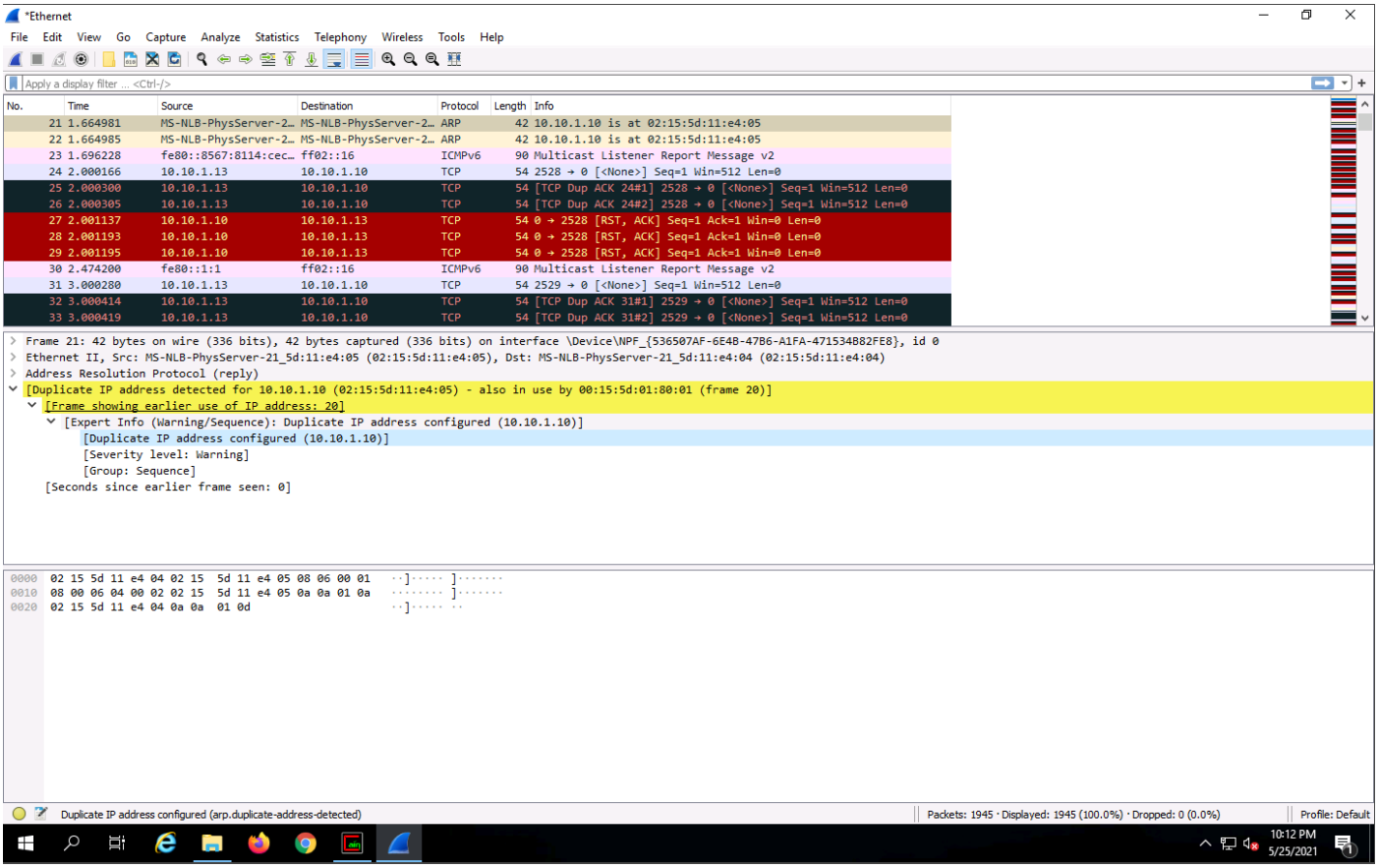
47. Arrange the **Wireshark . Expert Information** window above the **Wireshark** window so that you can view the packet number and the **Packet details** section.

48. In the **Wireshark . Expert Information** window, click any packet (here, **21**).



49. On selecting the packet number, **Wireshark** highlights the packet, and its associated information is displayed under the packet details section. Close the **Wireshark . Expert Information** window.

50. The warnings highlighted in yellow indicate that duplicate IP addresses have been detected at one MAC address, as shown in the screenshot.



ARP spoofing succeeds by changing the IP address of the attacker's computer to the IP address of the target computer. A forged ARP request and reply packet find a place in the target ARP cache in this process. As the ARP reply has been forged, the destination computer (target) sends frames to the attacker's computer, where the attacker can modify the frames before sending them to the source machine (User A) in an MITM attack. At this point, the attacker can launch a DoS attack by associating a non-existent MAC address with the IP address of the gateway or may passively sniff the traffic, and then forward it to the target destination.

51. This concludes the demonstration of detecting ARP poisoning in a switch-based network.
52. Close all open windows and document all the acquired information.

Lab 4: Perform DoS and DDoS Attacks using Various Techniques on a Target Host to Prevents Access to System Resources for Legitimate Users

Lab Scenario

DoS and DDoS attacks have become popular, because of the easy accessibility of exploit plans and the negligible amount of brainwork required while executing them. These attacks can be very dangerous, because they can quickly consume the largest hosts on the Internet, rendering them useless. The impact of these attacks includes loss of goodwill, disabled networks, financial loss, and disabled organizations.

In a DDoS attack, many applications pound the target browser or network with fake exterior requests that make the system, network, browser, or site slow, useless, and disabled or unavailable.

The attacker initiates the DDoS attack by sending a command to the zombie agents. These zombie agents send a connection request to a large number of reflector systems with the spoofed IP address of the victim. The reflector systems see these requests as coming from the victim's machine instead of as zombie agents, because of the spoofing of the source IP address. Hence, they send the requested information (response to connection request) to the victim. The victim's machine is flooded with unsolicited responses from several reflector computers at once. This may reduce performance or may even cause the victim's machine to shut down completely.

In this lab, you will gain hands-on experience in auditing network resources against DoS and DDoS attacks.

Lab Objectives

- Perform a DoS Attack on a Target Host using hping3
- Perform a DDoS Attack using HOIC

Task 1: Perform a DoS Attack on a Target Host using hping3

hping3 is a command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols.

It performs network security auditing, firewall testing, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, and other functions.

Here, we will use the hping3 tool to perform DoS attacks such as SYN flooding, Ping of Death (PoD) attacks, and UDP application layer flood attacks on a target host.

1. Click Windows 10 to switch to the **Windows 10** machine, click Ctrl+Alt+Delete.

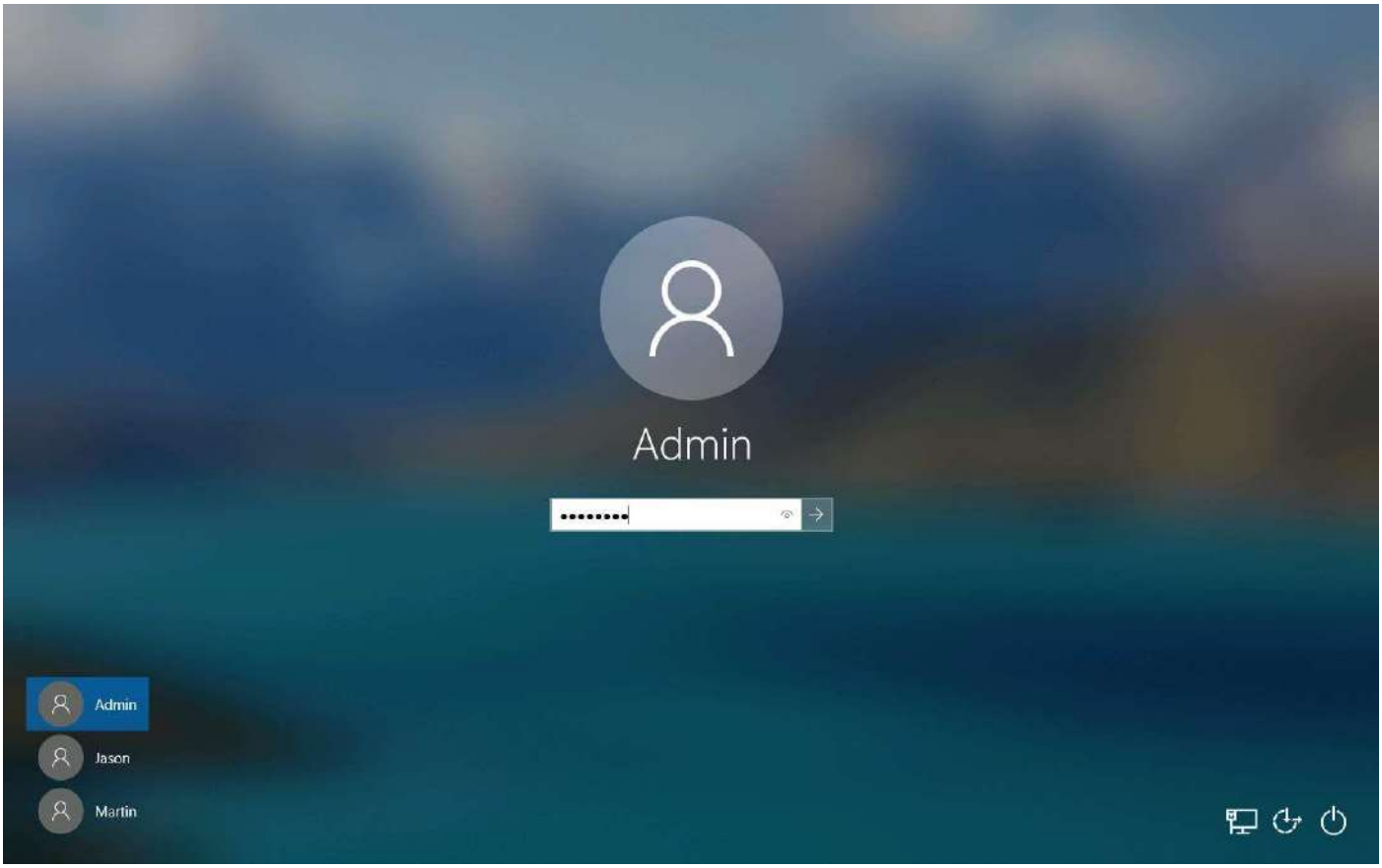
Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 10** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under Commands (**thunder** icon) menu.

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

Alternatively, you can also click **Pa$$w0rd** under **Windows 10** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

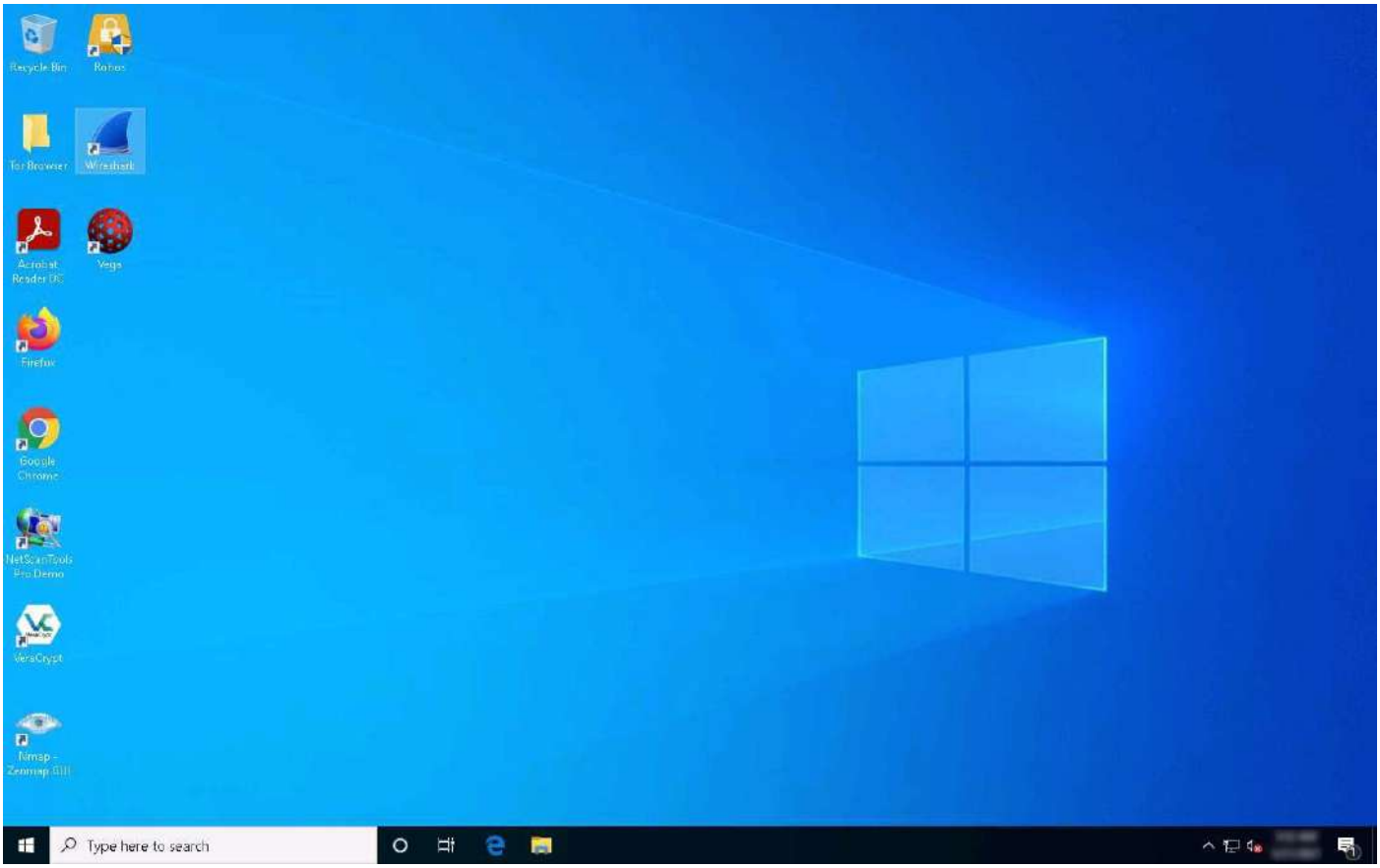
If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

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



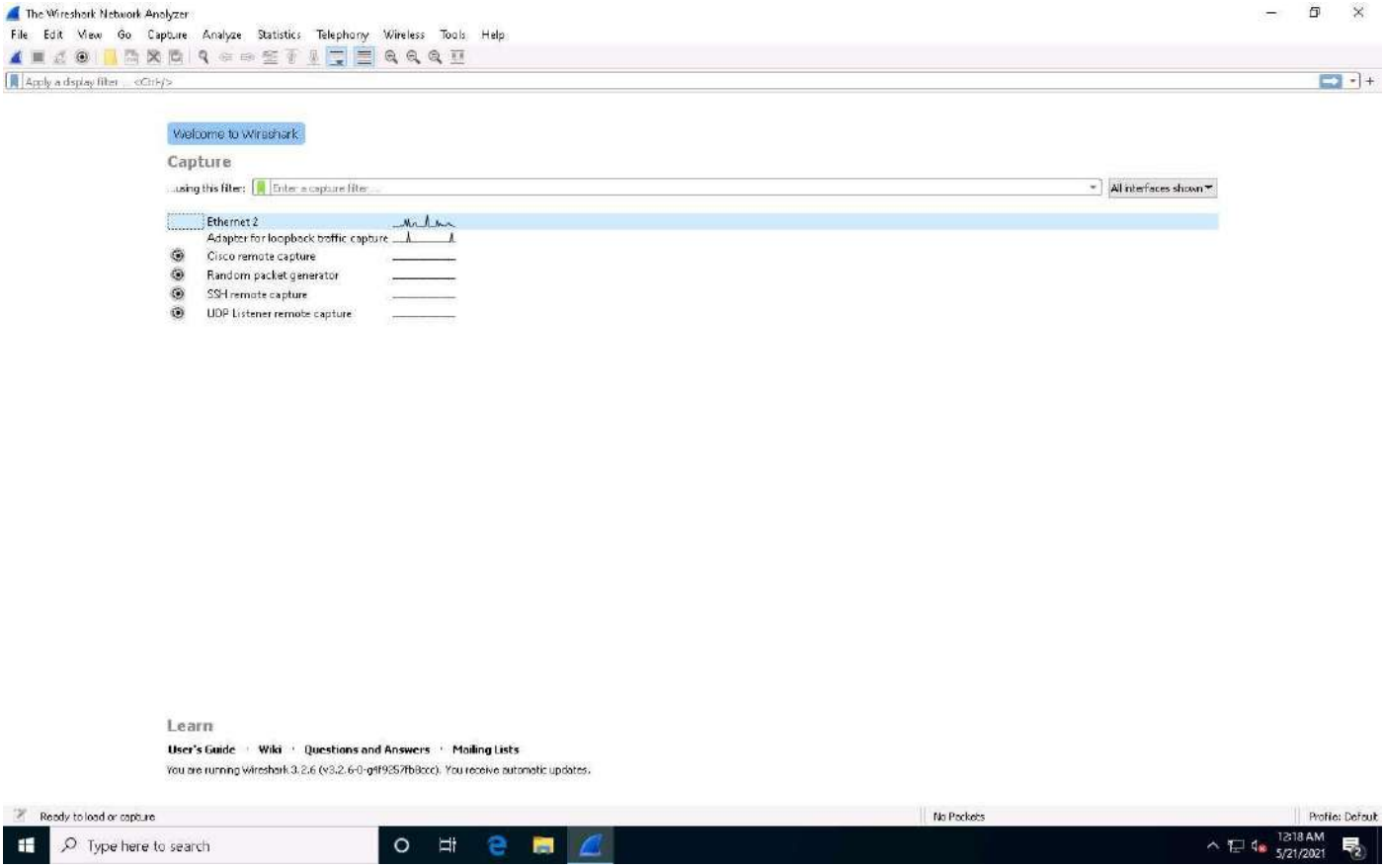
3. Double-click **Wireshark** shortcut present on the **Desktop**.

If **Software Update** popup appears click on **Remind me later**.

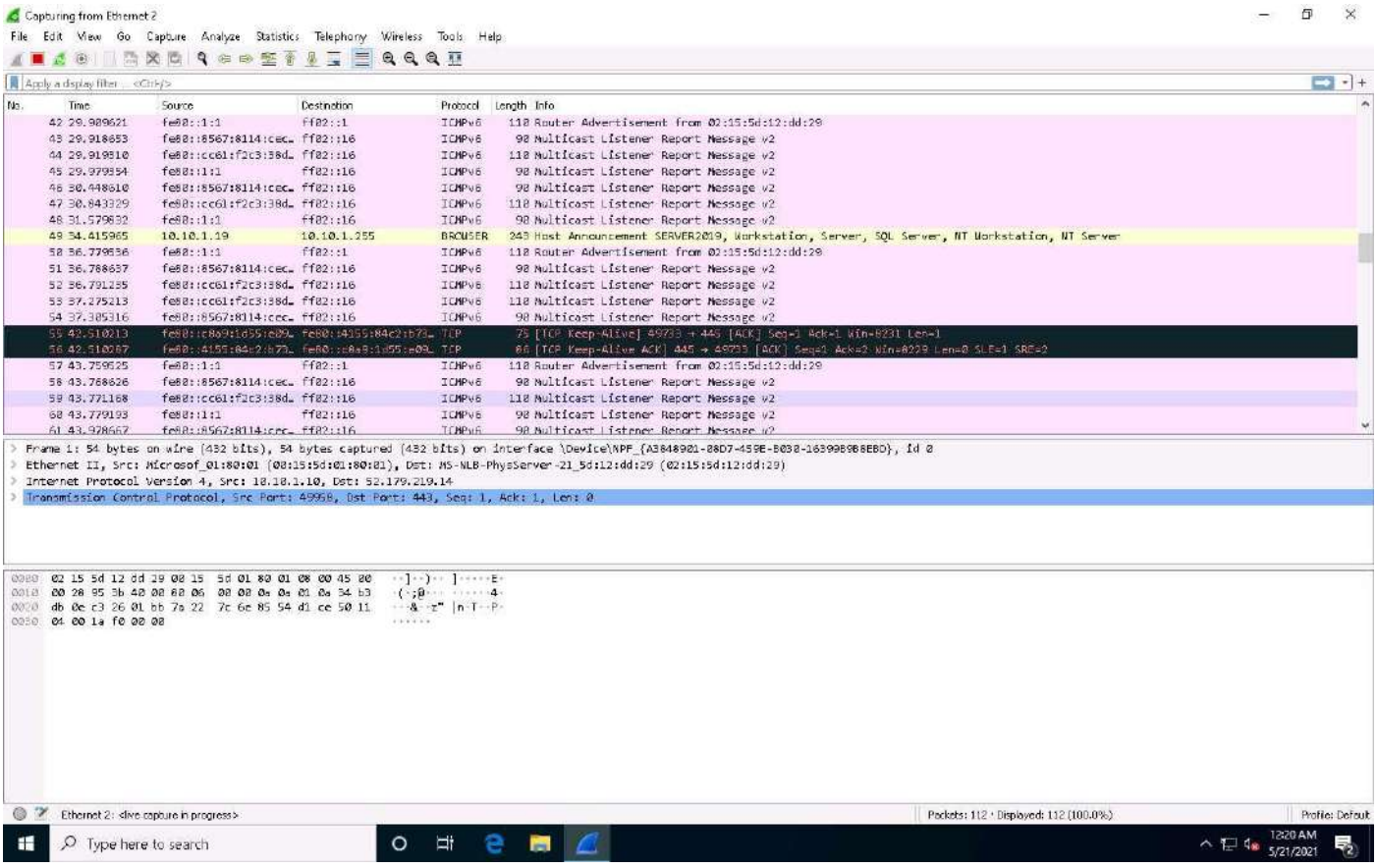


4. **The Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet 2**) to start capturing the network traffic.

Note: The primary network interface might vary in your lab environment.

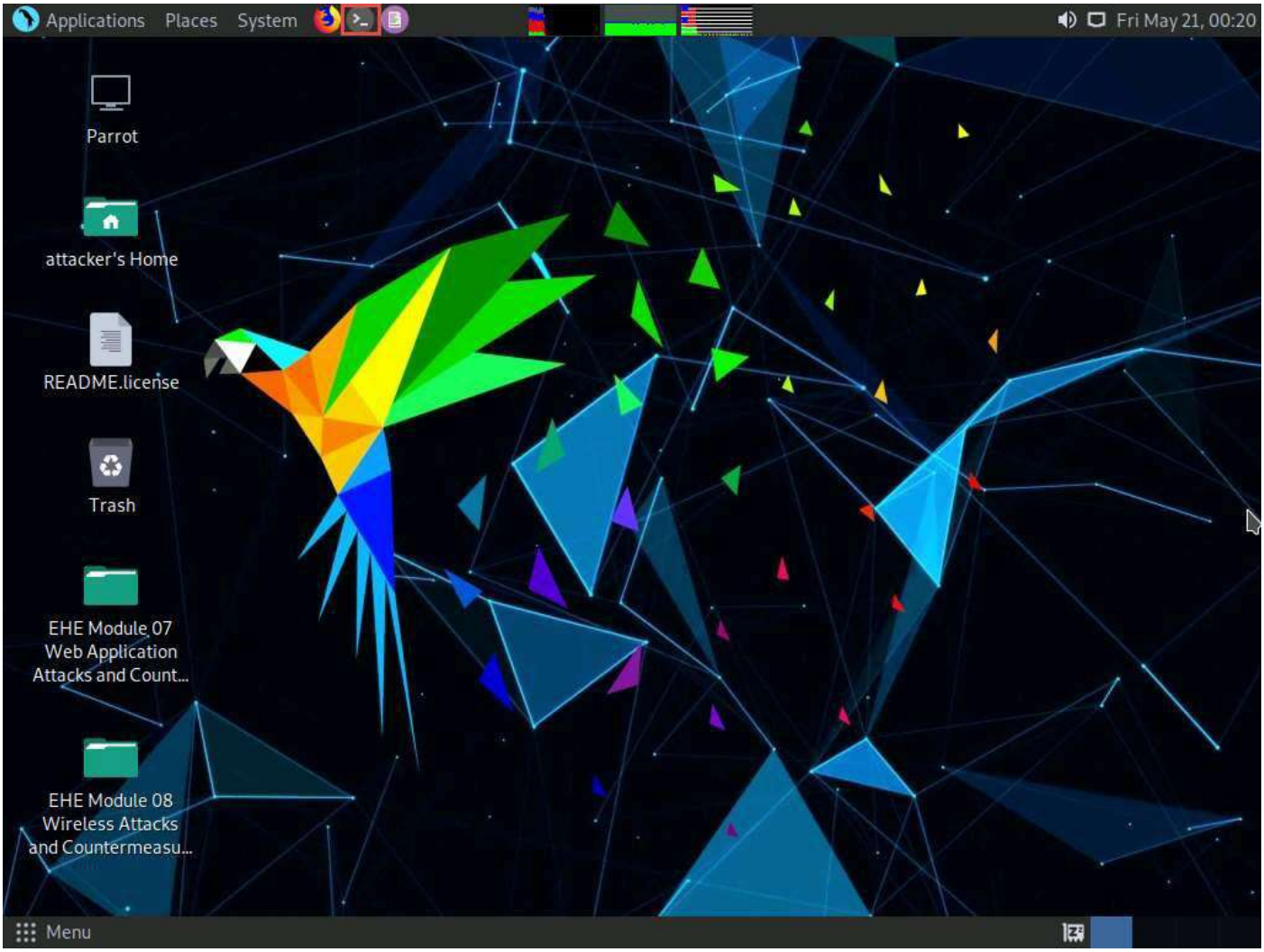


5. **Wireshark** starts capturing the packets; leave it running.



6. Click Parrot Security to switch to the **Parrot Security** machine.

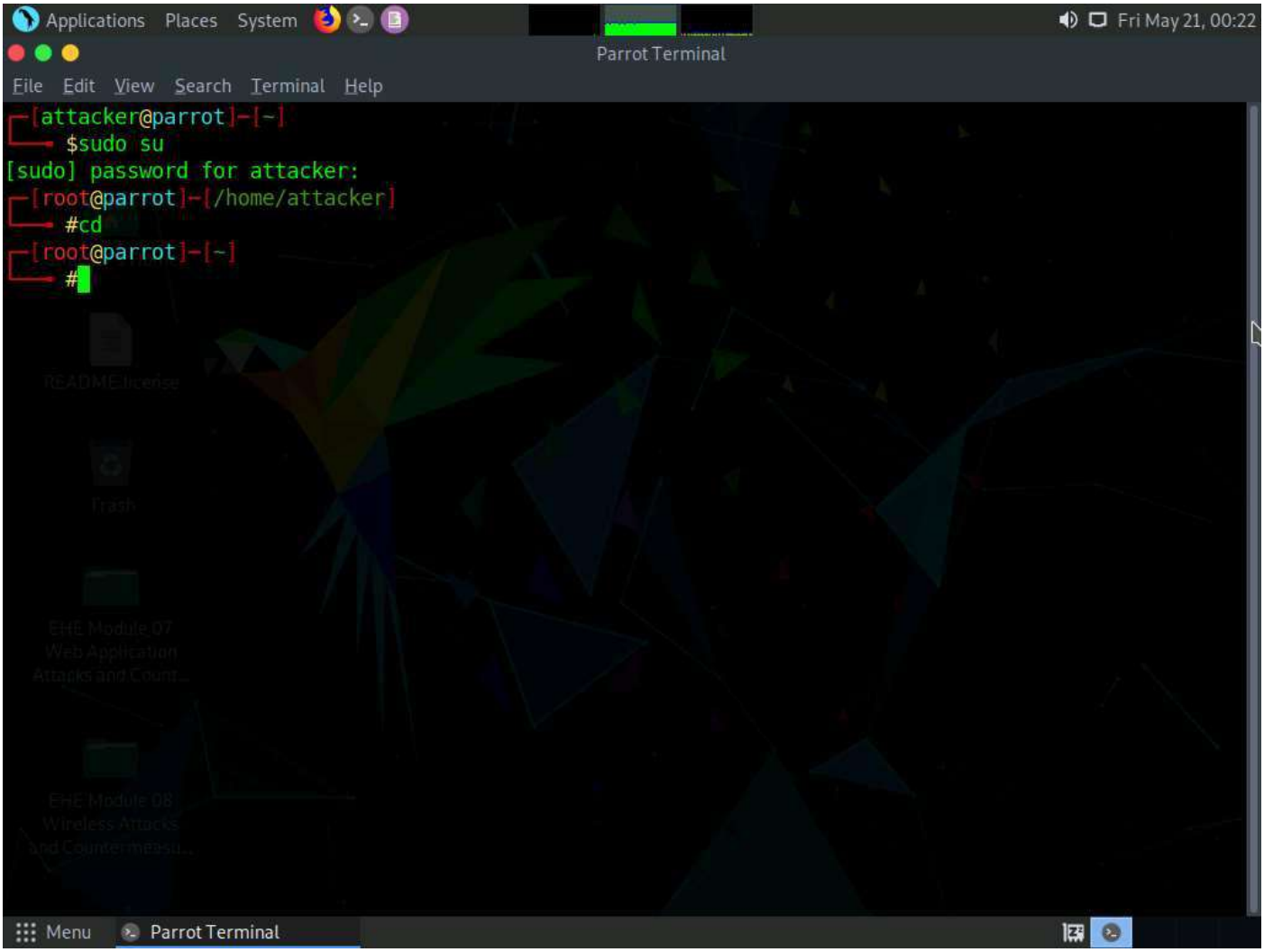
7. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



8. The **terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
9. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

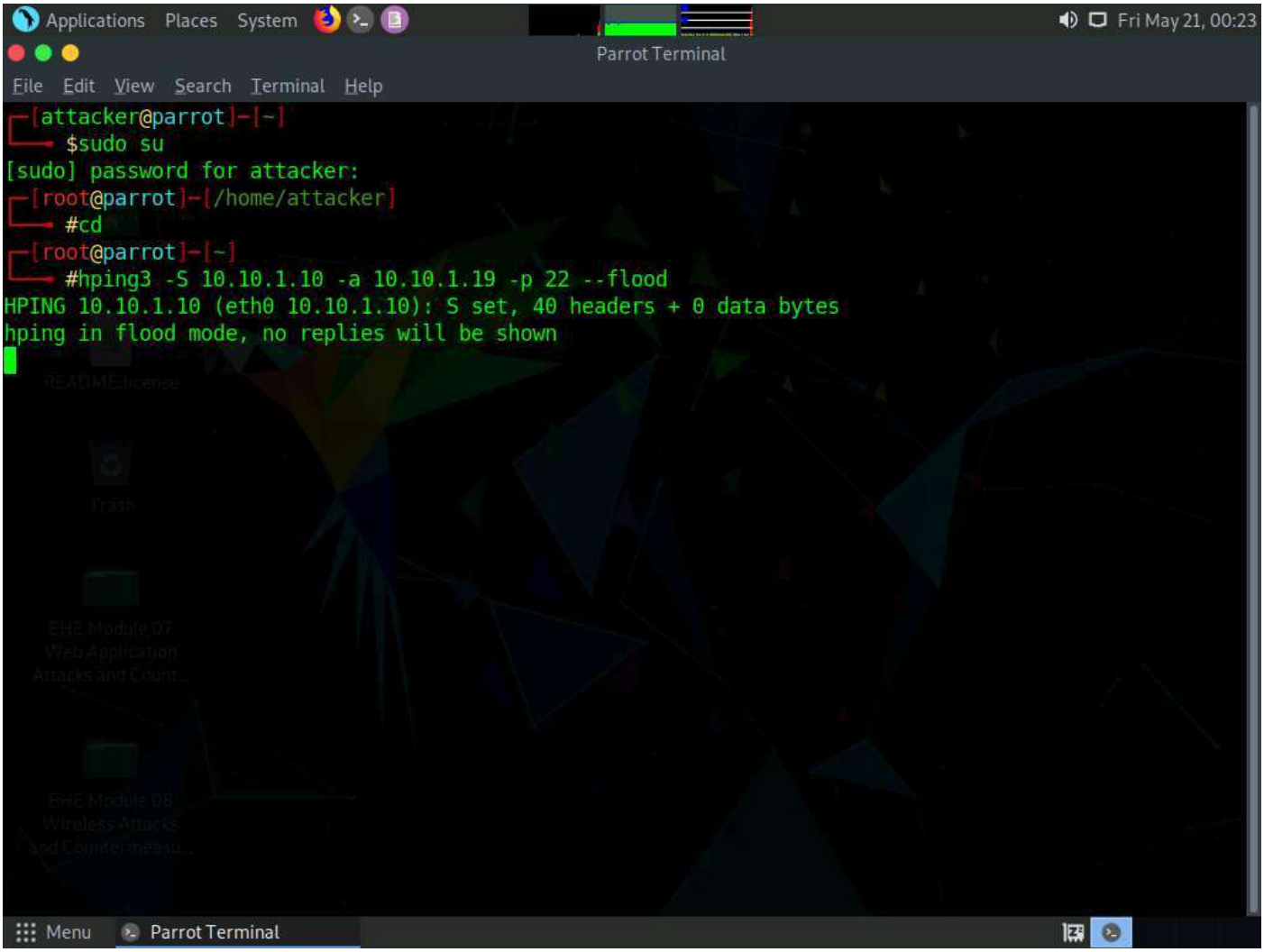
10. Now, type **cd** and press **Enter** to jump to the root directory.



11. In the **terminal** window, type **hping3 -S (Target IP Address) -a (Spoofable IP Address) -p 22 --flood** and press **Enter**.

Here, the target IP address is **10.10.1.10 [Windows 10]**, and the spoofable IP address is **10.10.1.19 [Windows Server 2019]**

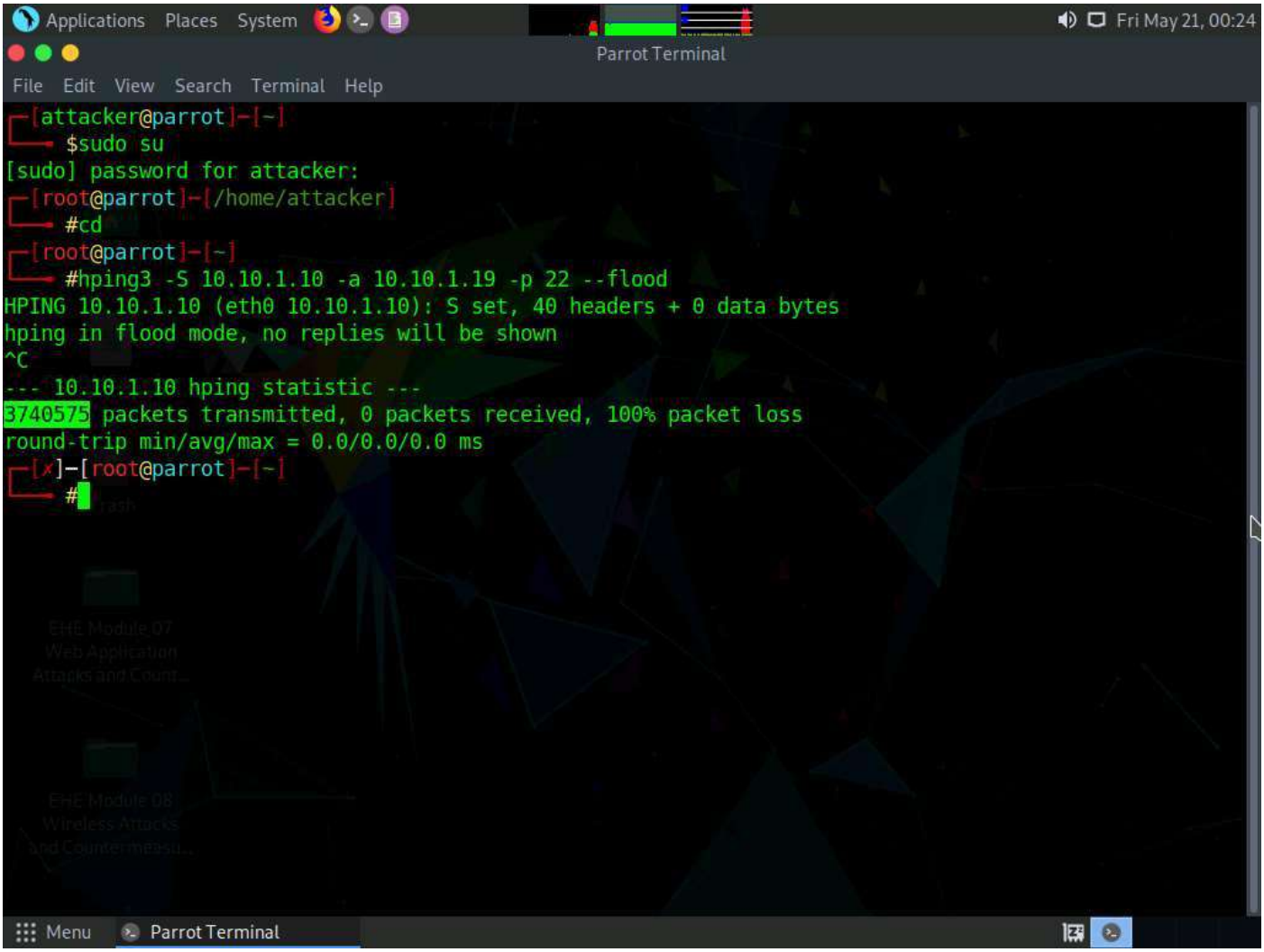
-S: sets the SYN flag; **-a**: spoofs the IP address; **-p**: specifies the destination port; and **--flood**: sends a huge number of packets.



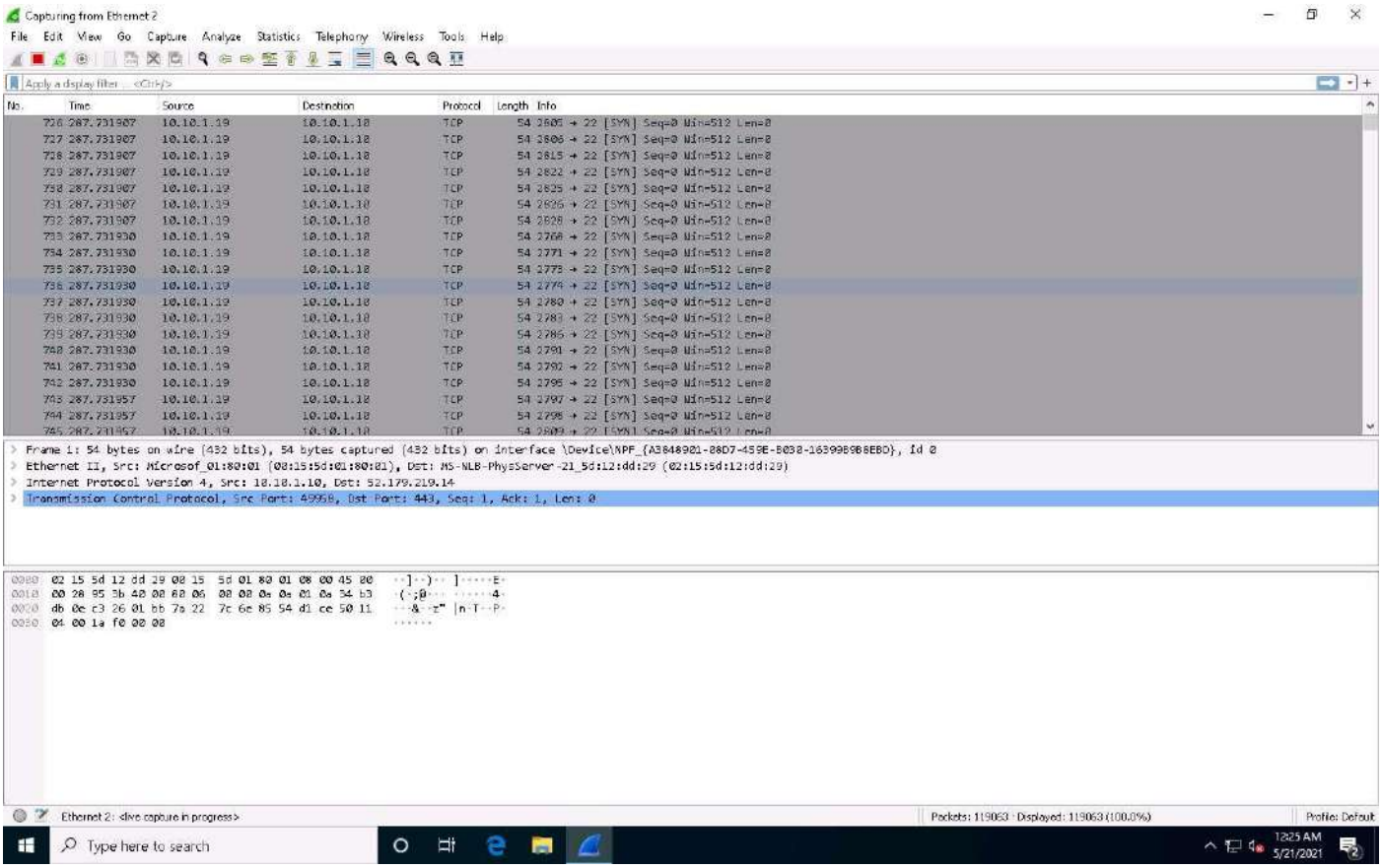
12. This command initiates the SYN flooding attack on the **Windows 10** machine. After a few seconds, press **Ctrl+C** to stop the SYN flooding of the target machine.

If you send the SYN packets for a long period, then the target system may crash.

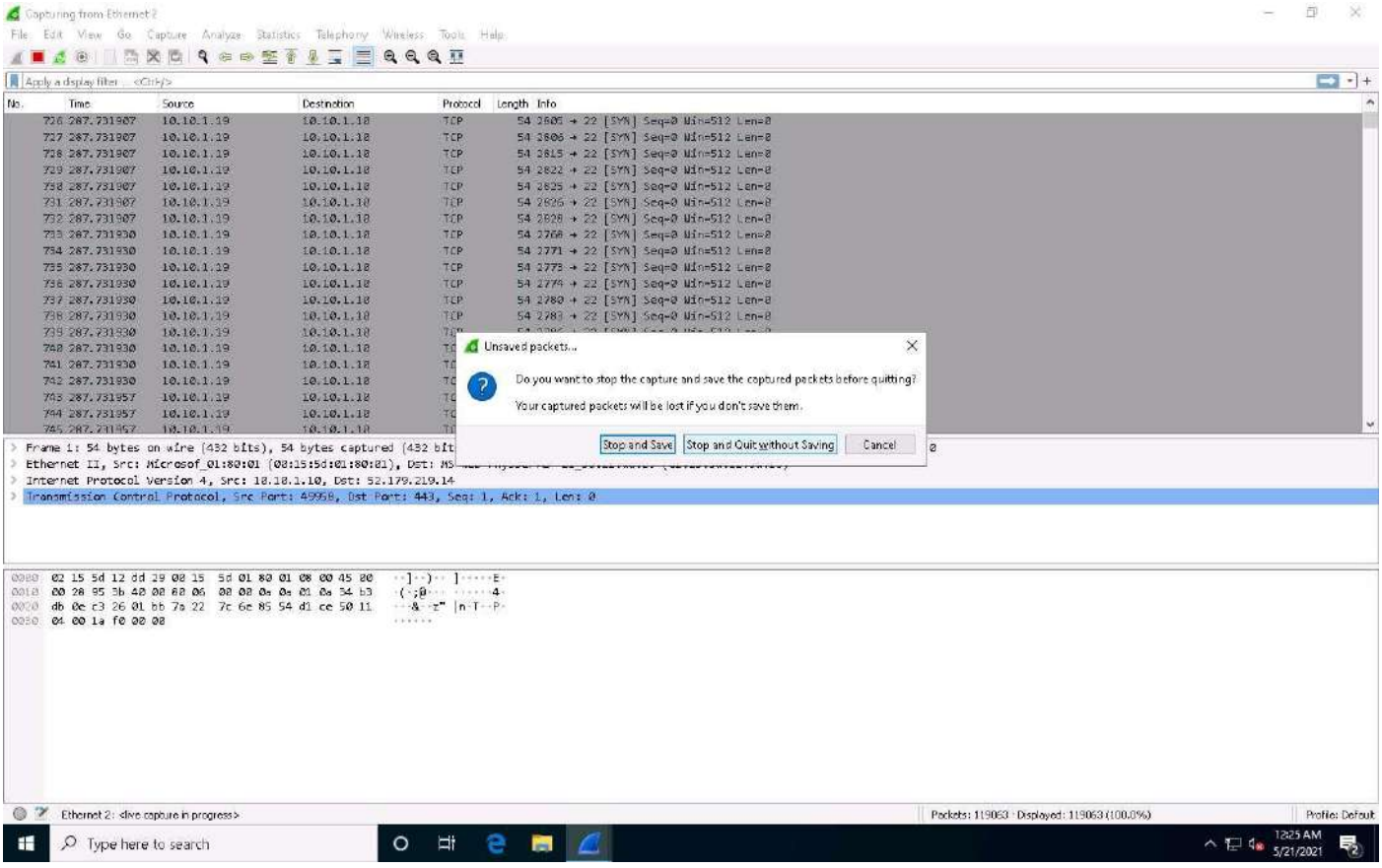
13. Observe how, in very little time, the huge number of packets are sent to the target machine.



14. **hping3** floods the victim machine by sending bulk **SYN packets** and **overloading** the victim's resources.
15. Click Windows 10 to switch to the **Windows 10** machine and observe the TCP-SYN packets captured by **Wireshark**.

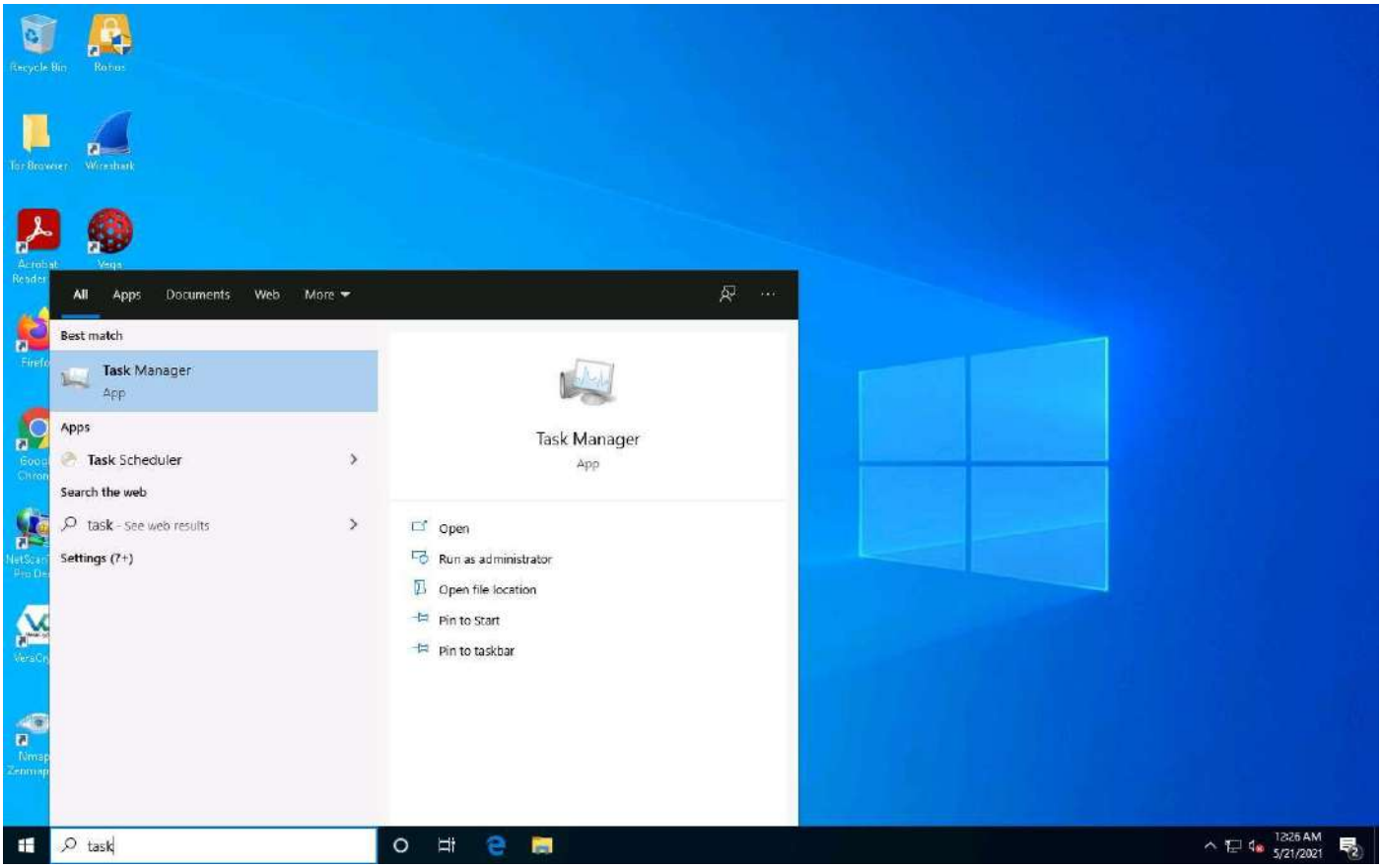


16. Close the **Wireshark** main window. If an **Unsaved packets...** pop-up appears, click **Stop and Quit without Saving**.

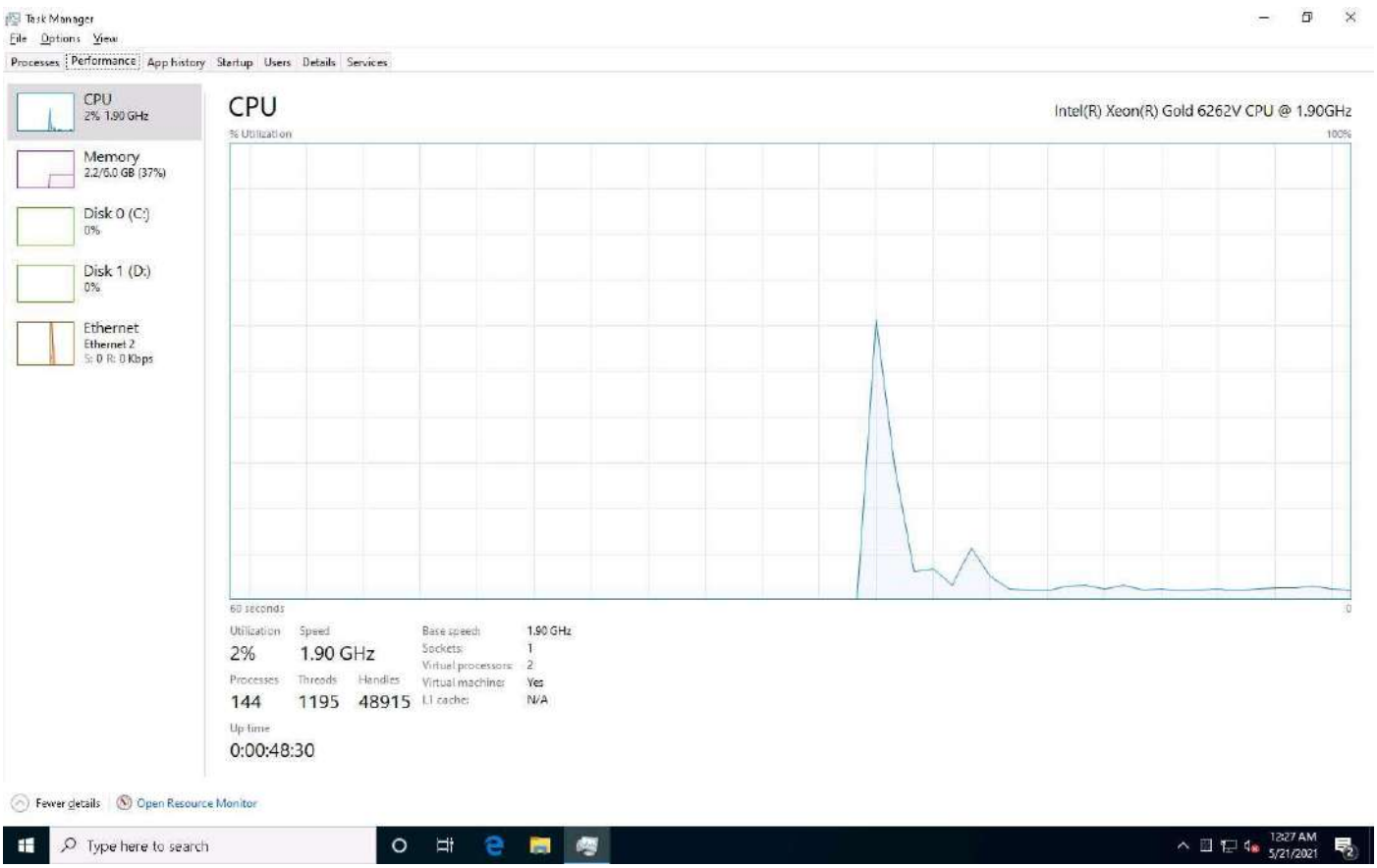


17. Now, we shall perform a PoD attack on the target system.

18. Click the **Type here to search** field present at the bottom of **Desktop**, and type **task**. Click **Task Manager** from the results.

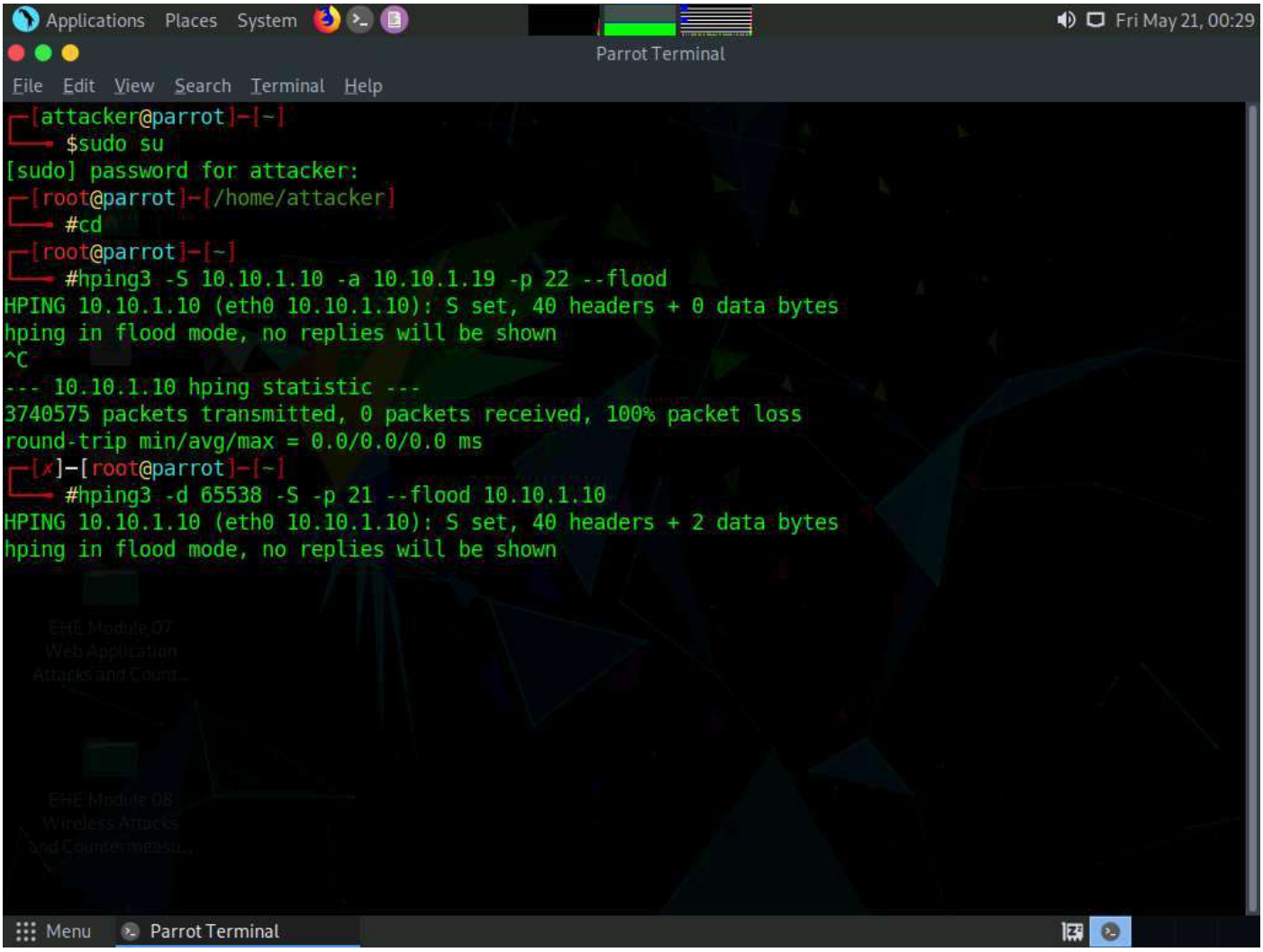


19. **Task Manager** window appears, click **More details** and by default **Processes** tab will appear, navigate to the **Performance** tab, as shown in the screenshot.



20. Now, click Parrot Security to switch to the **Parrot Security** machine. In the **Terminal** window, type **hping3 -d 65538 -S -p 21 --flood (Target IP Address)** (here, the target IP address is **10.10.1.10 [Windows 10]**) and press **Enter**.

-d: specifies data size; **-S**: sets the SYN flag; **-p**: specifies the destination port; and **--flood**: sends a huge number of packets.



21. This command initiates the PoD attack on the **Windows 10** machine.

In a PoD attack, the attacker tries to crash, freeze, or destabilize the targeted system or service by sending malformed or oversized packets using a simple ping command.

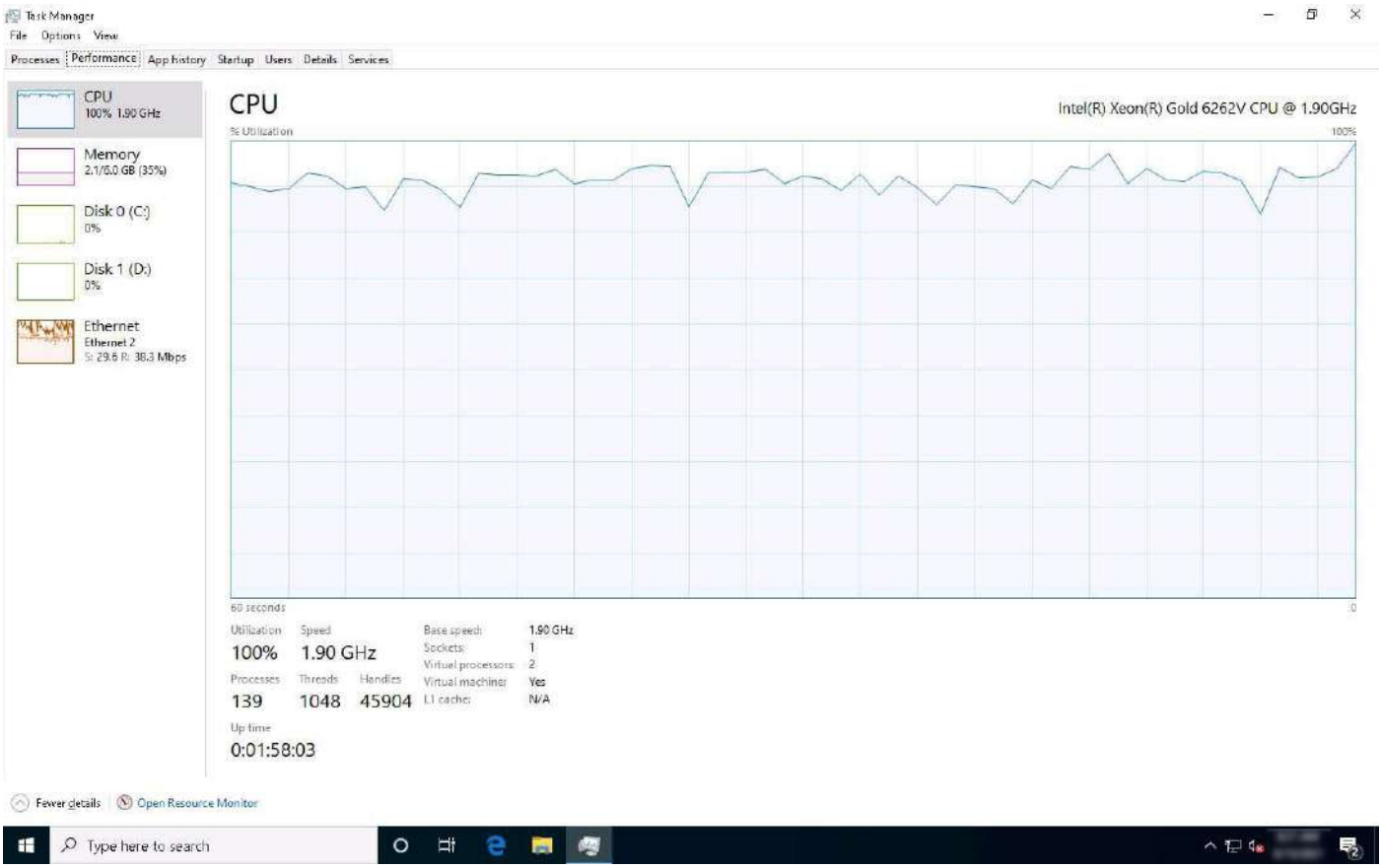
For example, the attacker sends a packet that has a size of 65,538 bytes to the target web server. This packet size exceeds the size limit prescribed by RFC 791 IP, which is 65,535 bytes. The receiving system's reassembly process might cause the system to crash.

22. **hping3** floods the victim machine by sending bulk packets, and thereby overloading the victim's resources.
23. Click Windows 10 to switch to the **Windows 10** machine
24. In the **Task Manager**, observe the **Performance** tab to view the performance of various system components (**CPU, Memory, Disk, Ethernet**).

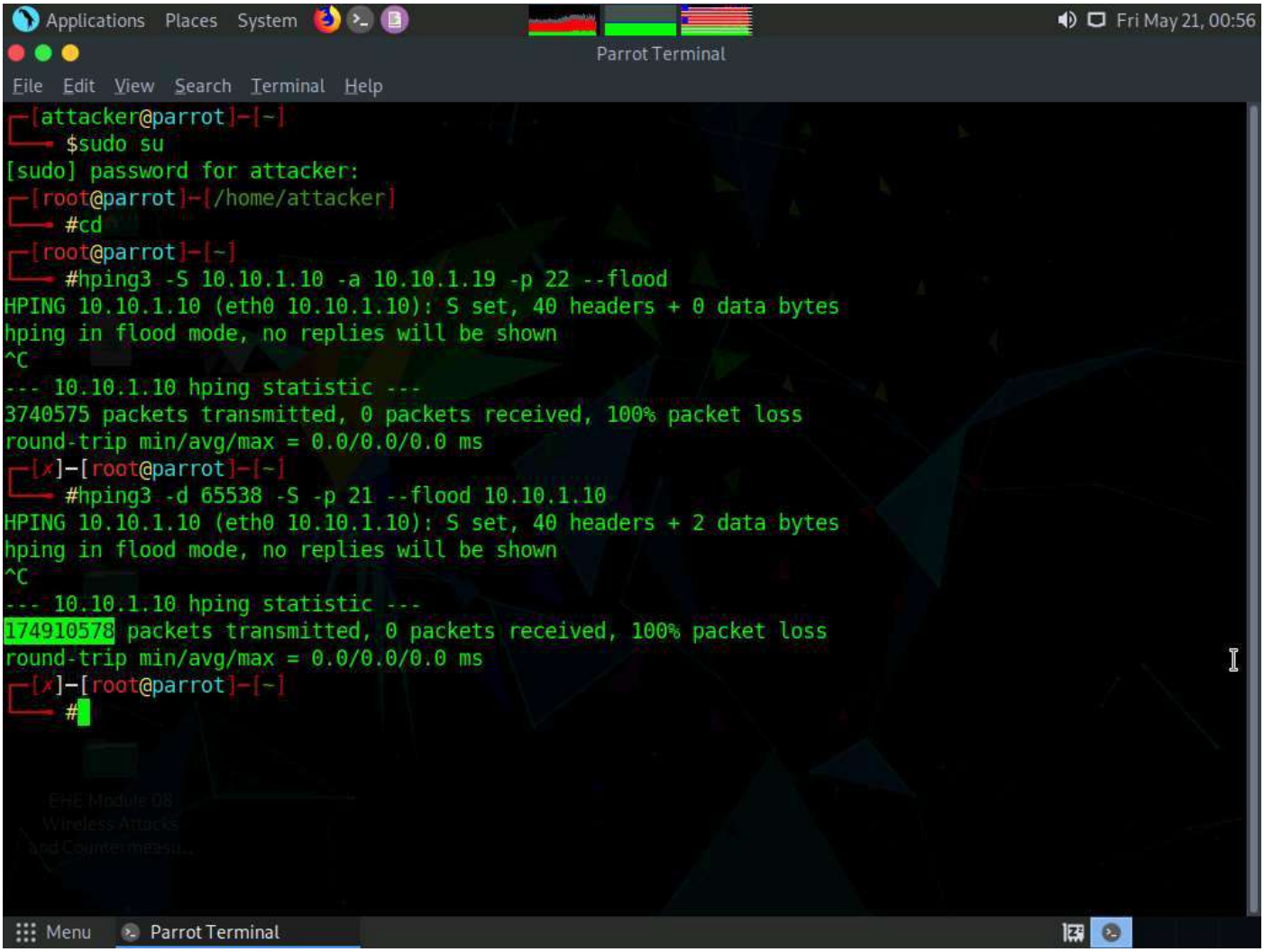
Wait for a while for the CPU utilization to reach to its maximum value (100%).

25. Under the **Performance** tab, by default, the **CPU** performance is displayed in the right-hand pane. Observe that the CPU **Utilization** percentage is **100%**, indicating a DoS attack on the system.
26. Observe the degradation in the performance of the system, which might result in the system crashing.

The results might differ in your lab environment.



27. Click Parrot Security to switch to the **Parrot Security** machine. In the **Terminal** window, press **Ctrl+C** to terminate the PoD attack using hping3.



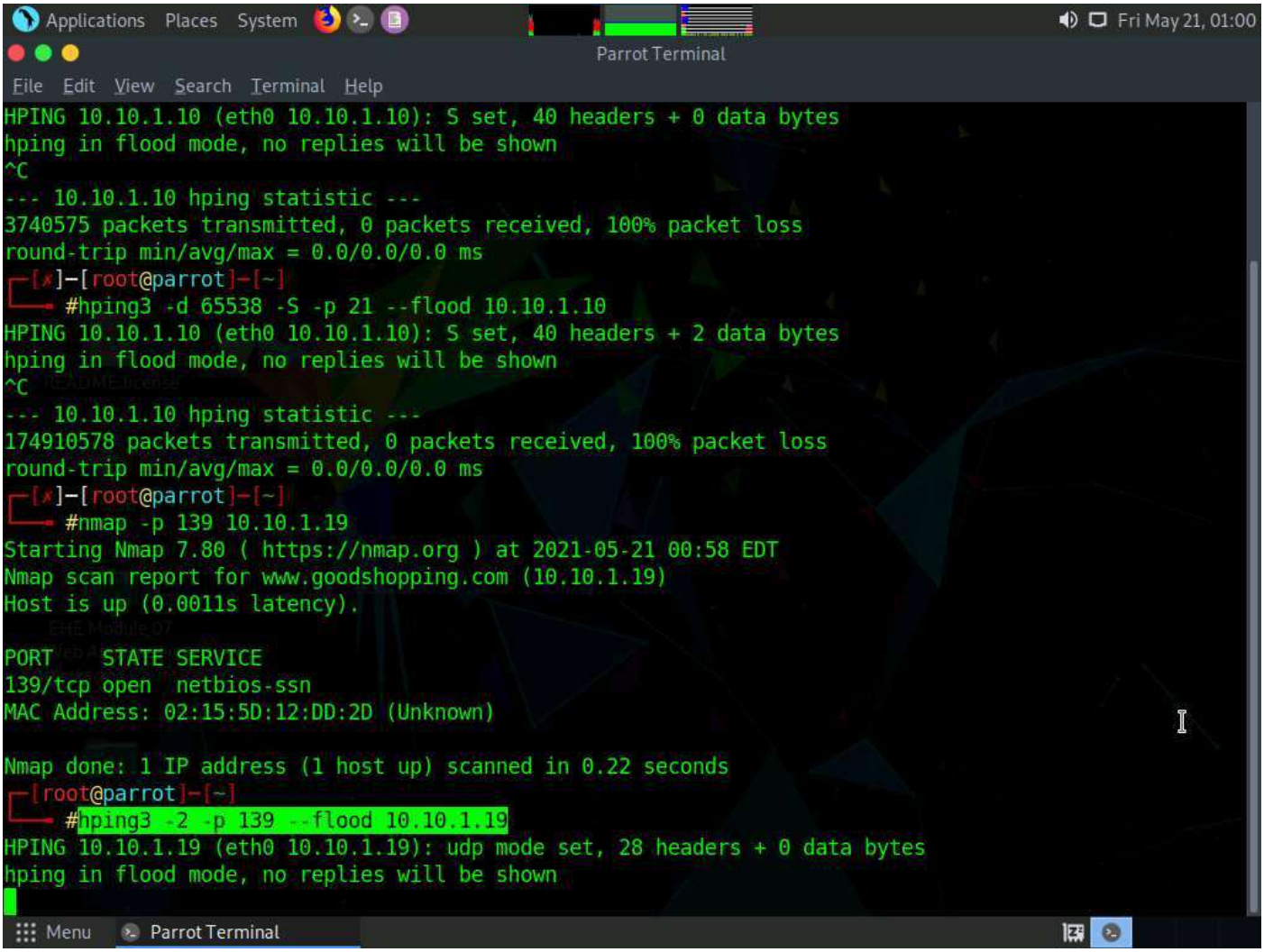
28. Now, we shall perform a UDP application layer flood attack on the **Windows Server 2019** machine using NetBIOS port 139. To do so, first, determine whether NetBIOS port 139 is open or not.

29. In the terminal window, type **nmap -p 139 (Target IP Address)** (here, the target IP address is **10.10.1.19 [Windows Server 2019]**) and press **Enter**.

Here, we will use NetBIOS port 139 to perform a UDP application layer flood attack.

30. Now, type **hping3 -2 -p 139 --flood (Target IP Address)** (here, the target IP address is **10.10.1.19 [Windows Server 2019]**) and press **Enter**.

-2: specifies the UDP mode; **-p**: specifies the destination port; and **--flood**: sends a huge number of packets.

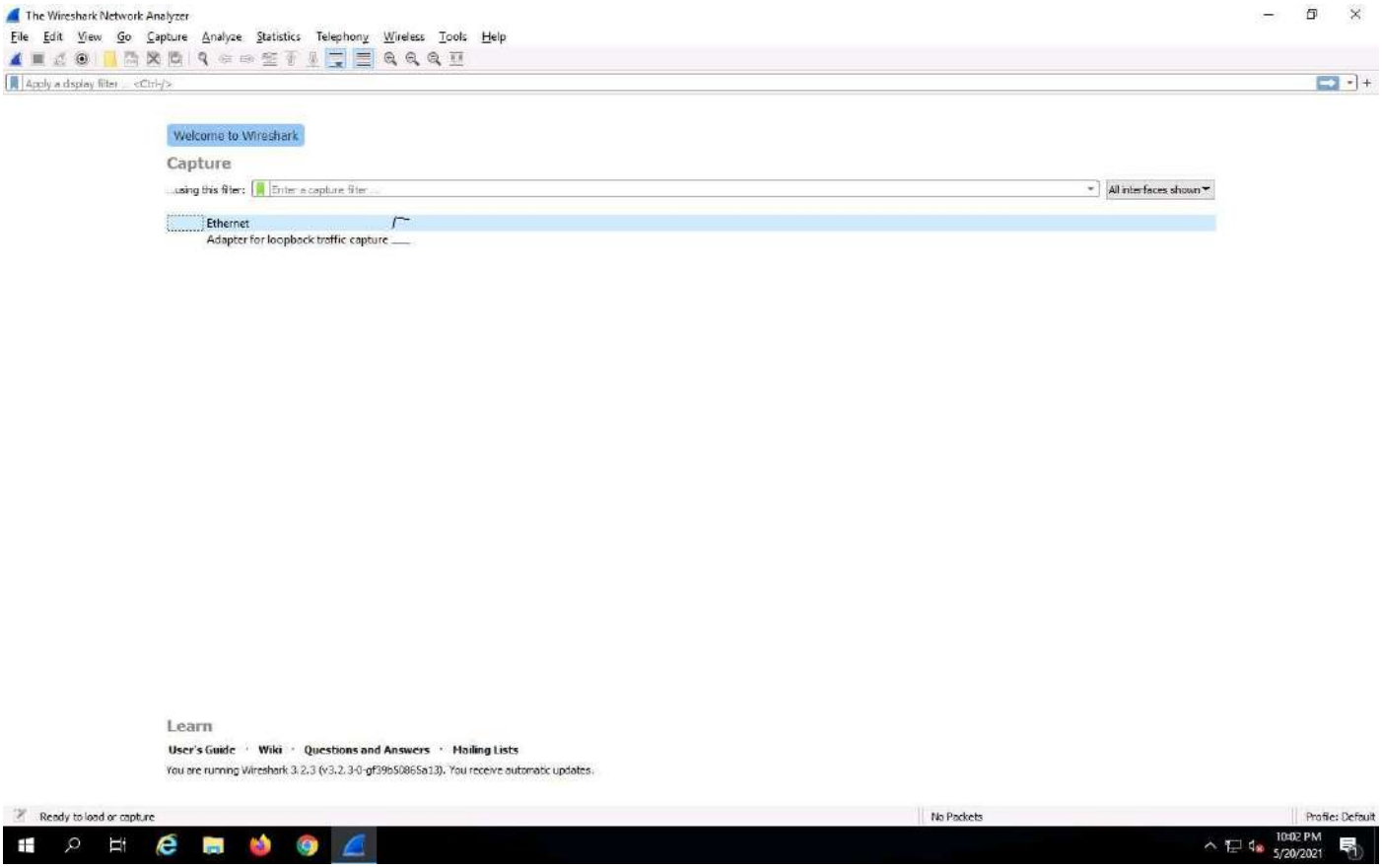


31. Click Windows Server 2019 to switch to the **Windows Server 2019** machine,
32. Double-click **Wireshark** shortcut present on the **Desktop**.

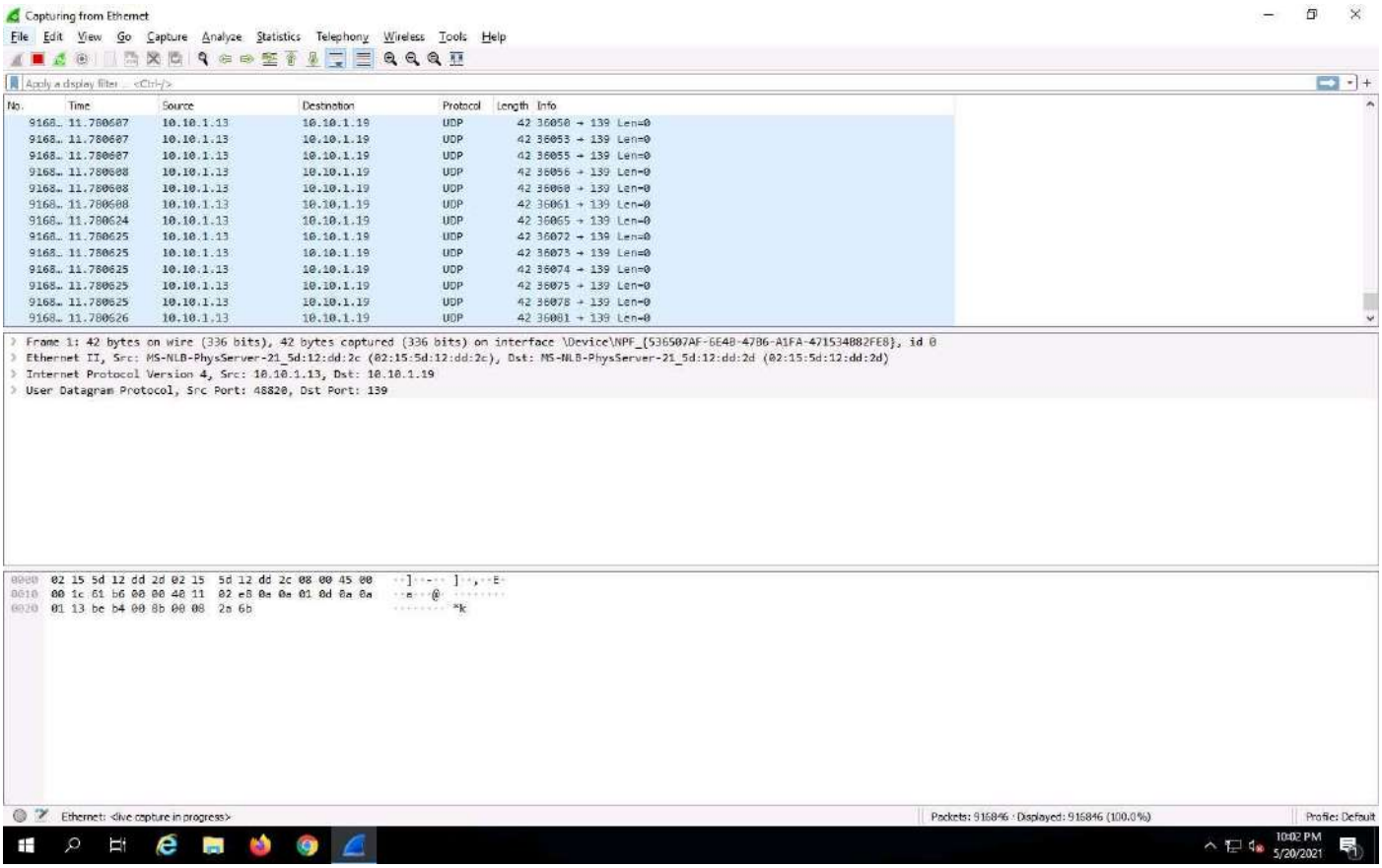
You might experience degradation in the **Window Server 2019** machine's performance.

33. **The Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.

The network interface might differ in your lab environment.



34. **Wireshark** displays the network's flow of traffic. Here, observe the huge number of **UDP** packets coming from the **Source** IP address **10.10.1.13** via port **139**.

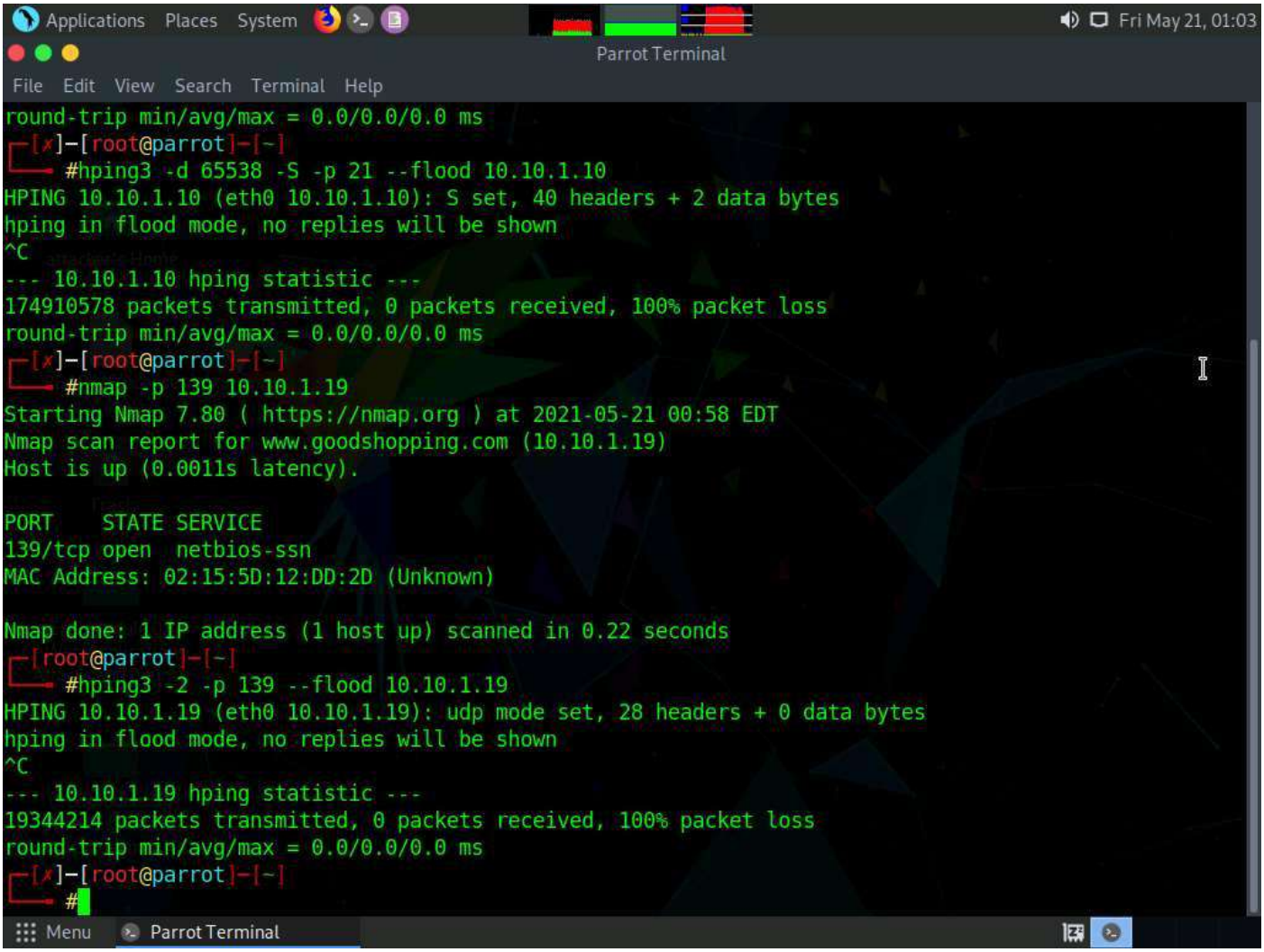


35. Click Parrot Security to switch to the **Parrot Security** machine. In the **Terminal** window, press **Ctrl+C** to terminate the DoS attack.

Here, we have used NetBIOS port 139 to perform a UDP application layer flood attack. Similarly, you can employ other application layer protocols to perform a UDP application layer flood attack on a target network.

Some of the UDP based application layer protocols that attackers can employ to flood target networks include:

- **CharGEN** (Port 19)
- **SNMPv2** (Port 161)
- **QOTD** (Port 17)
- **RPC** (Port 135)
- **SSDP** (Port 1900)
- **CLDAP** (Port 389)
- **TFTP** (Port 69)
- **NetBIOS** (Port 137,138,139)
- **NTP** (Port 123)
- **Quake Network Protocol** (Port 26000)
- **VoIP** (Port 5060)



36. This concludes the demonstration of how to perform DoS attacks (SYN flooding, PoD attacks, and UDP Application Layer Flood Attacks) on a target host using hping3.
37. Close all open windows and document all the acquired information.

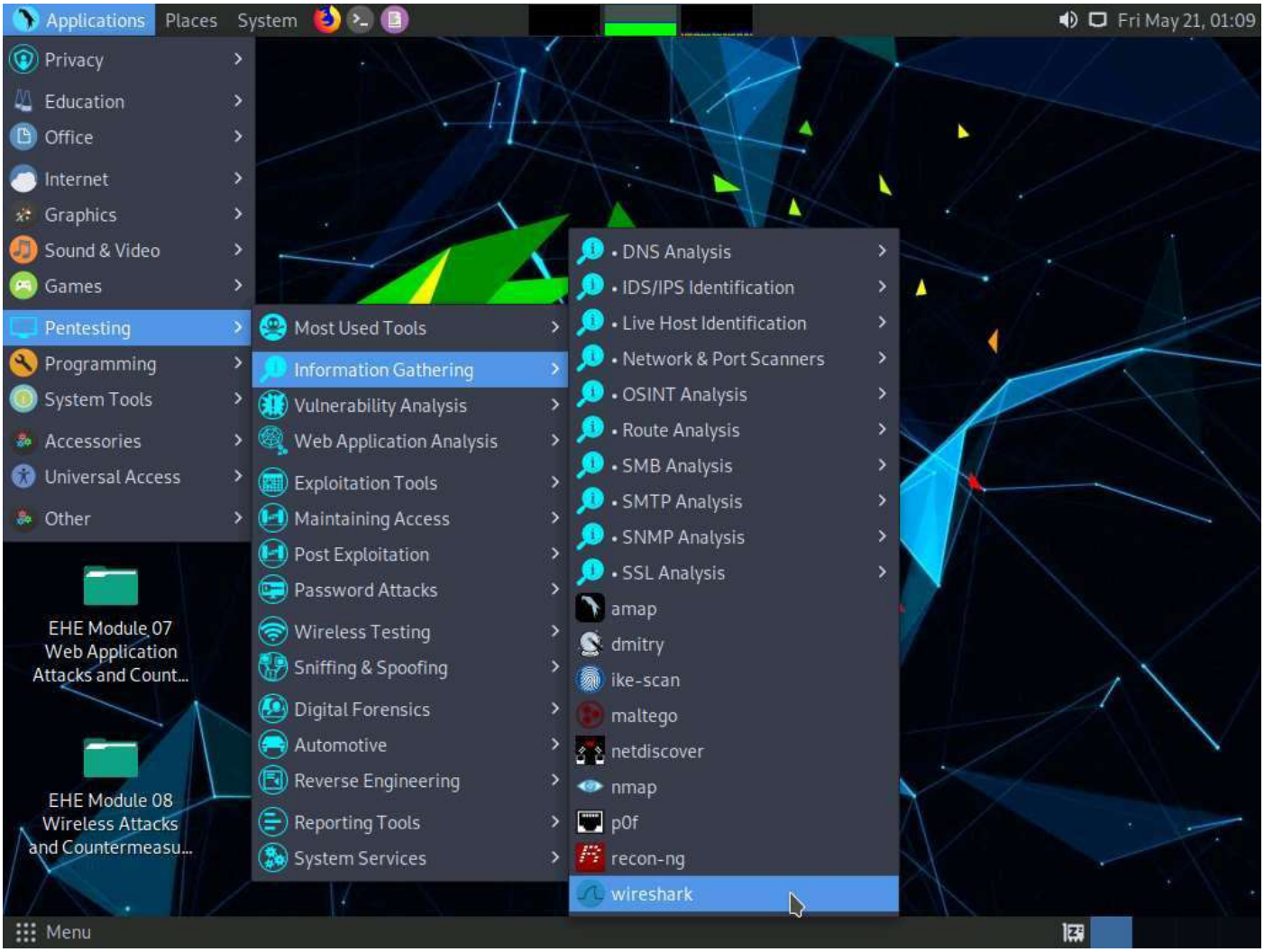
Task 2: Perform a DDoS Attack using HOIC

HOIC (High Orbit Ion Cannon) is a network stress and DoS/DDoS attack application. This tool is written in the BASIC language. It is designed to attack up to 256 target URLs simultaneously. It sends HTTP, POST, and GET requests to a computer that uses lulz inspired GUIs. It offers a high-speed multi-threaded HTTP Flood; a built-in scripting system allows the deployment of "boosters," which are scripts designed to thwart DDoS countermeasures and increase DoS output.

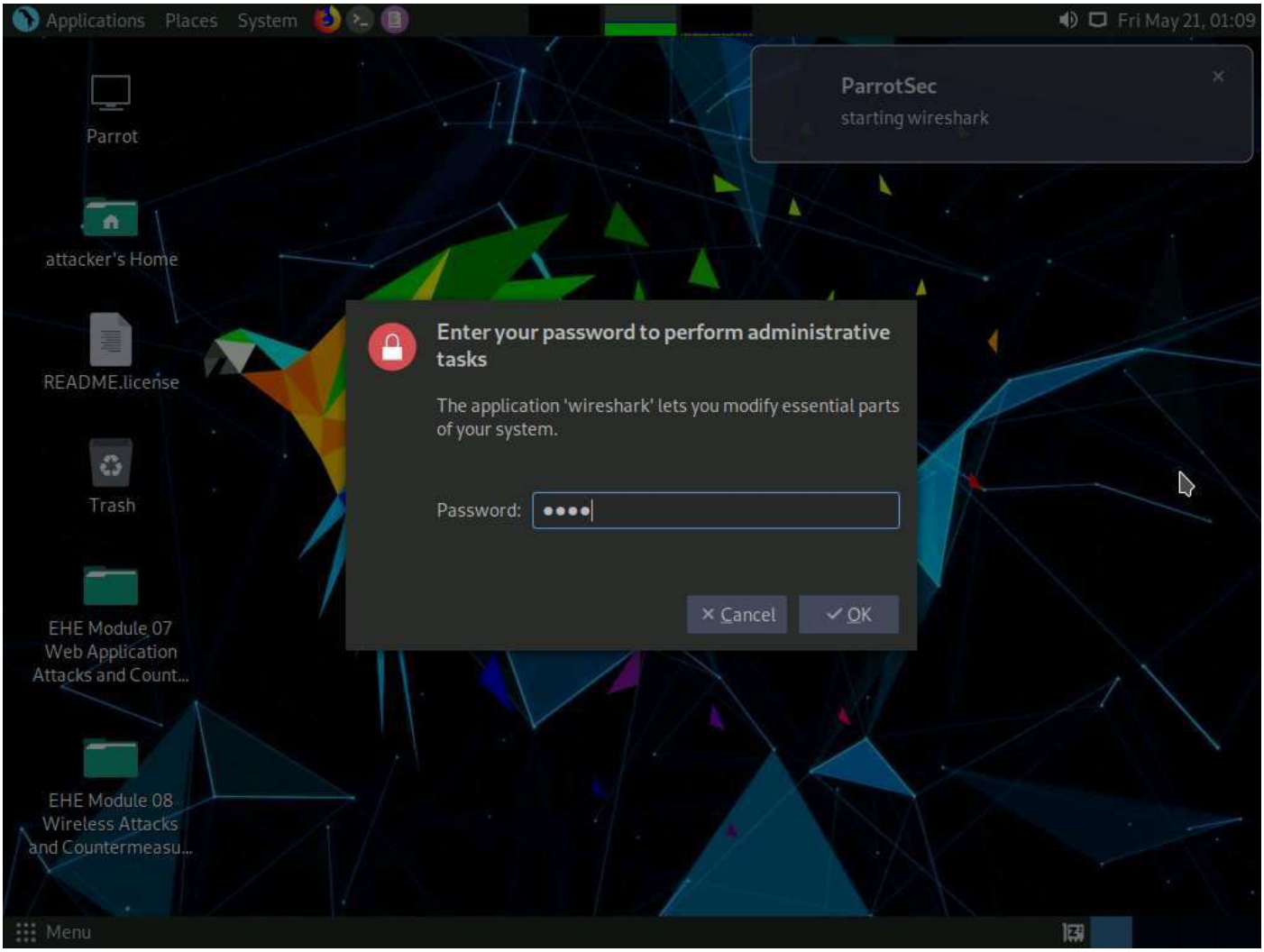
Here, we will use the HOIC tool to perform a DDoS attack on the target machine.

In this task, we will use the **Windows 10**, **Windows Server 2019** and **Windows Server 2016** machines to launch a DDoS attack on the **Parrot Security** machine.

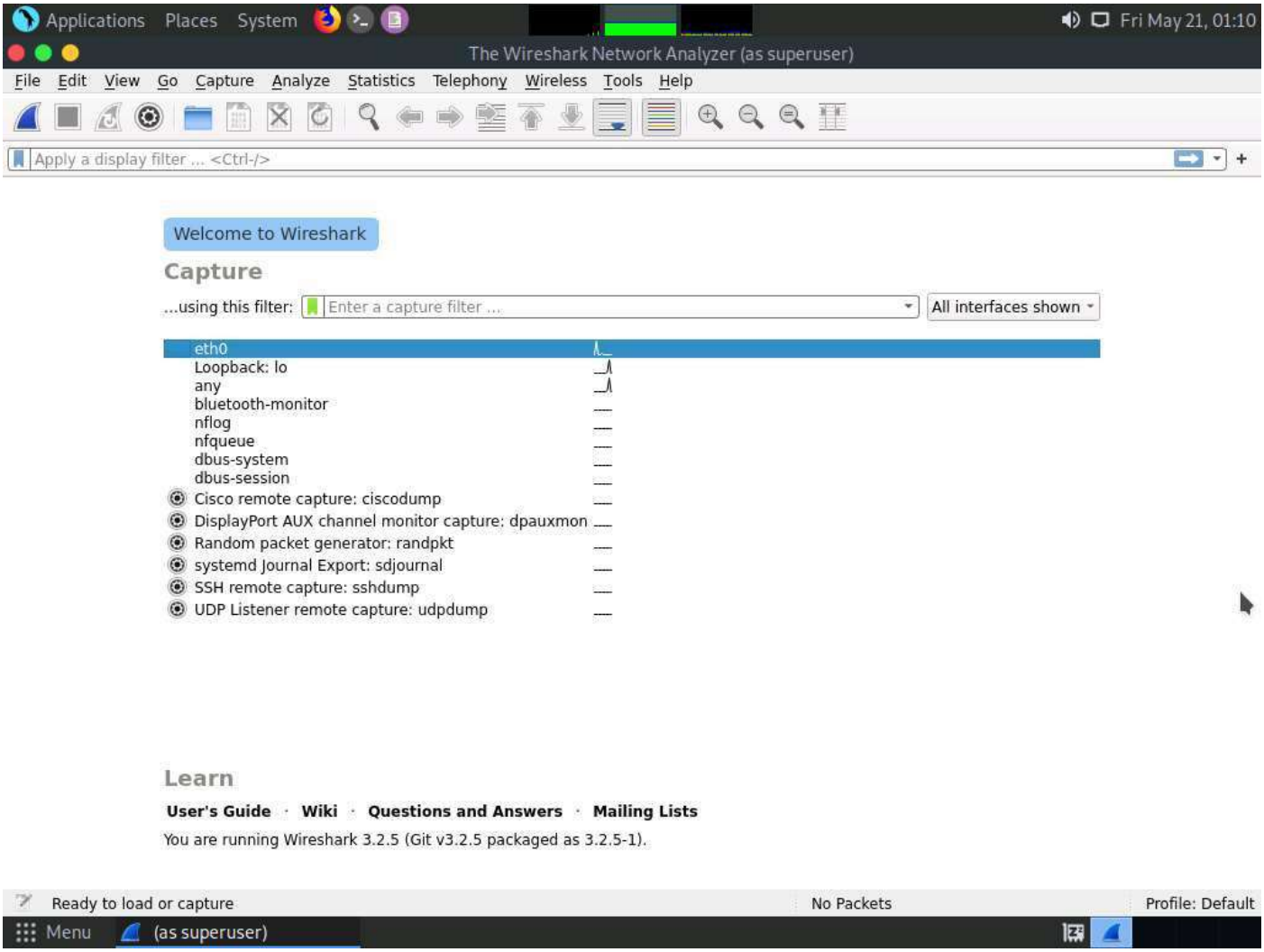
1. Click Parrot Security switch to the **Parrot Security** machine. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting** --> **Information Gathering** --> **wireshark**.



2. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

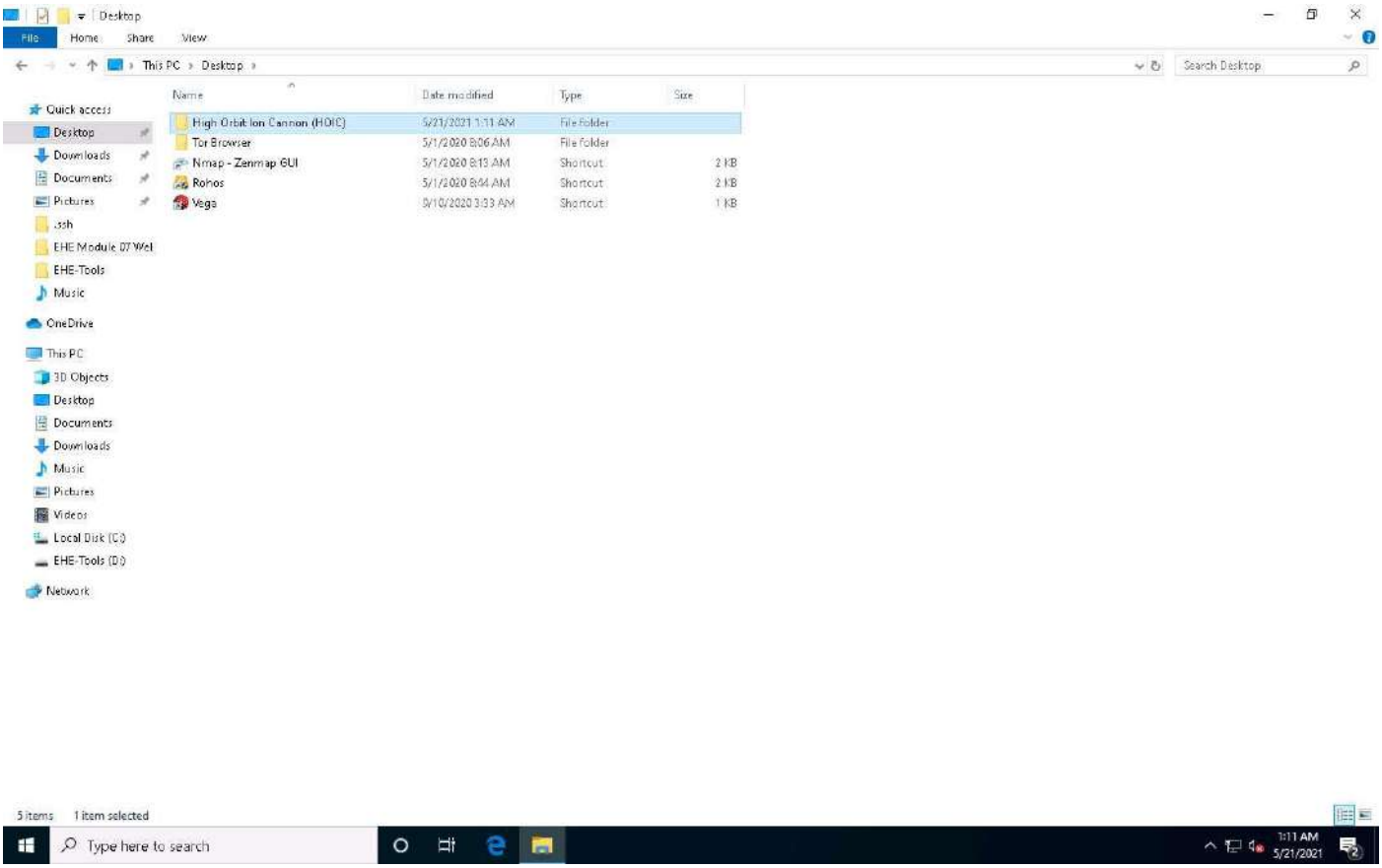


3. The **Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing the network traffic.



4. Click Windows 10 to switch to the **Windows 10** machine.
5. Navigate to **D:\EHE-Tools\EHE Module 06 Network Level Attacks and Countermeasures\DoS and DDoS Attack Tools** and copy the **High Orbit Ion Cannon (HOIC)** folder to **Desktop**.

To perform the DDoS attack, run this tool from various machines at once. If you run the tool directly from the shared drive in the machines one at a time, errors might occur. To avoid errors, copy the folder **High Orbit Ion Cannon (HOIC)** individually to each machine's **Desktop**, and then run the tool.

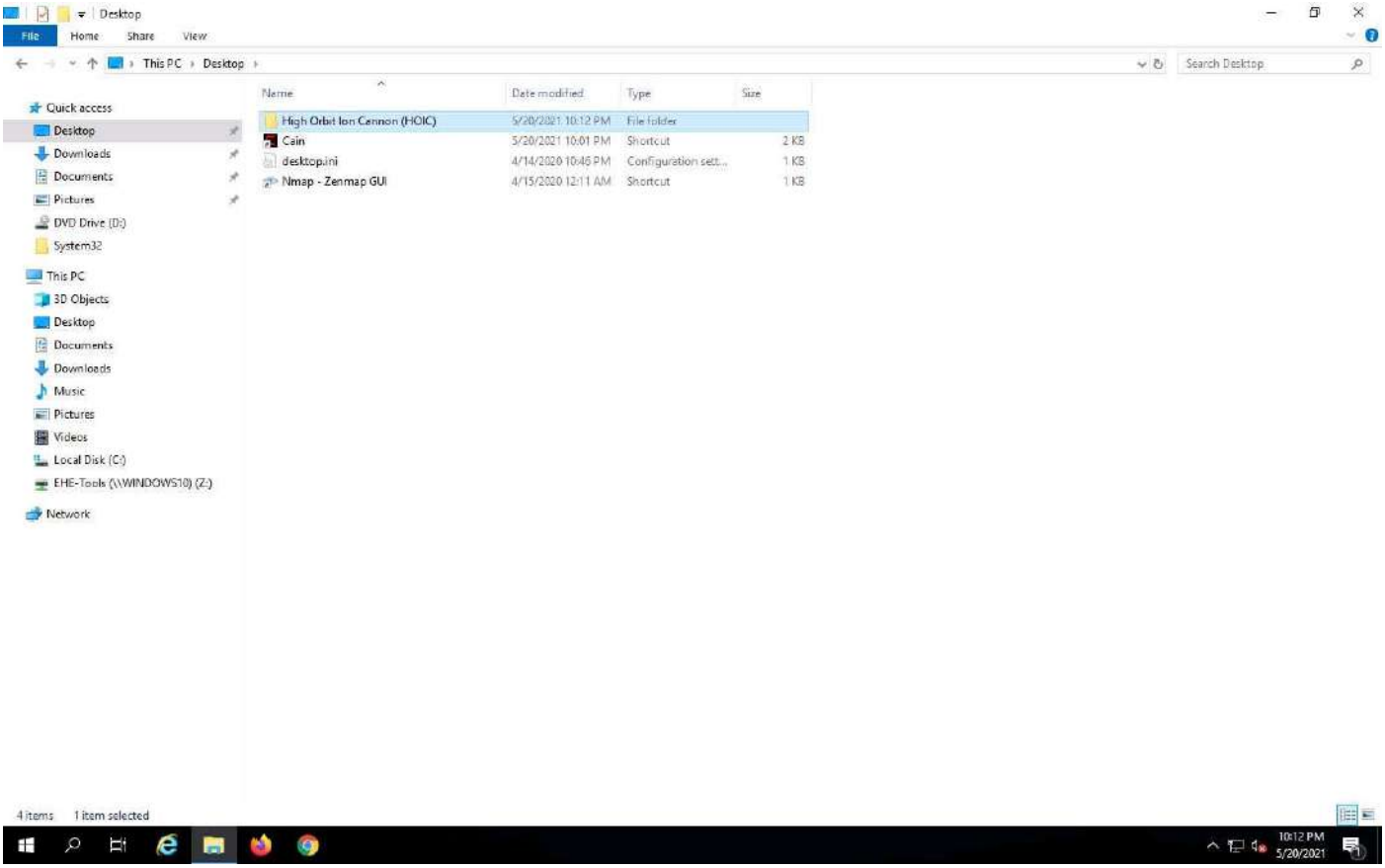


6. Similarly, follow the previous step (**Step #5**) on the **Windows Server 2019** (click Windows Server 2019 to switch to the **Windows Server 2019**) and **Windows Server 2016** (click Windows Server 2016 to switch to the **Windows Server 2016**) machines.

In **Windows Server 2019**, click Ctrl+Alt+Delete to activate the machine, by default, **Administrator** profile is selected, click Pa$$w0rd to enter the password and press **Enter** to log in.

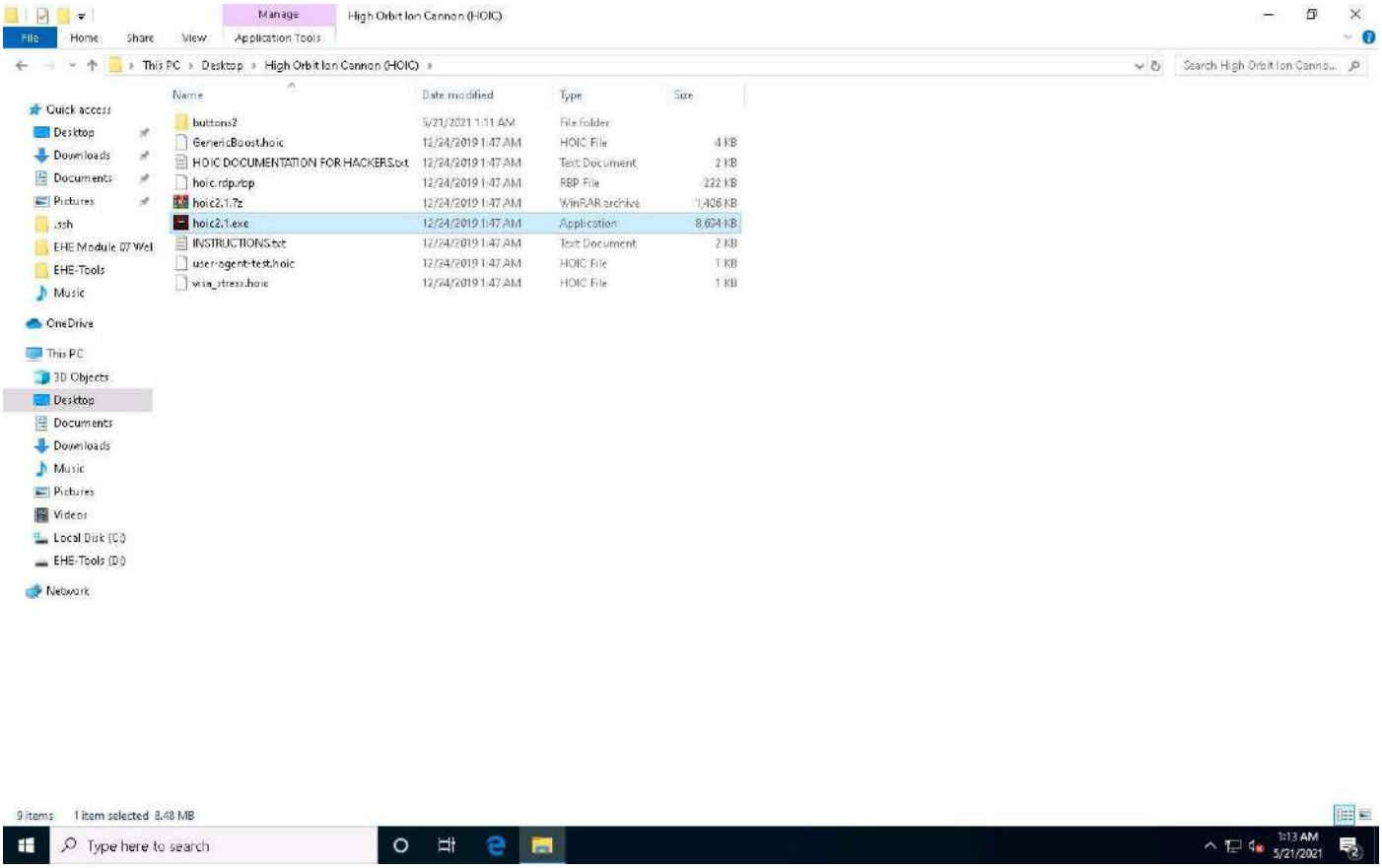
In **Windows Server 2016**, click Ctrl+Alt+Delete to activate the machine, by default, **EHE\Administrator** profile is selected, click Pa$$w0rd to enter the password and press **Enter** to log in.

On the **Windows Server 2019** and **Windows Server 2016** machines, the **High Orbit Ion Cannon (HOIC)** folder is located at **Z:\EHE Module 06 Network Level Attacks and Countermeasures\DoS and DDoS Attack Tools.**

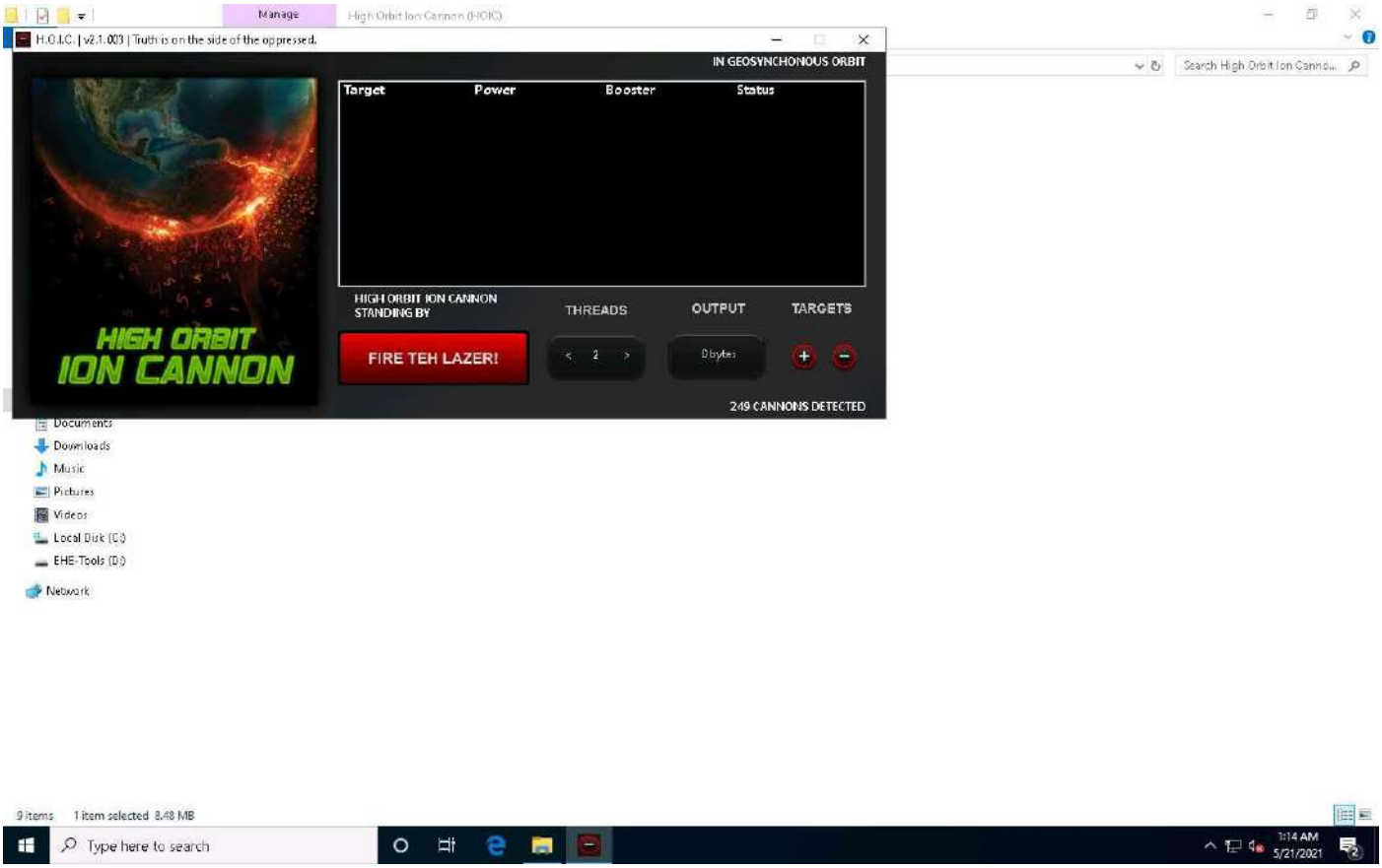


7. Now, click Windows 10 to switch to the **Window 10** machine and navigate to **Desktop**. Open the **High Orbit Ion Cannon (HOIC)** folder and double-click **hoic2.1.exe**.

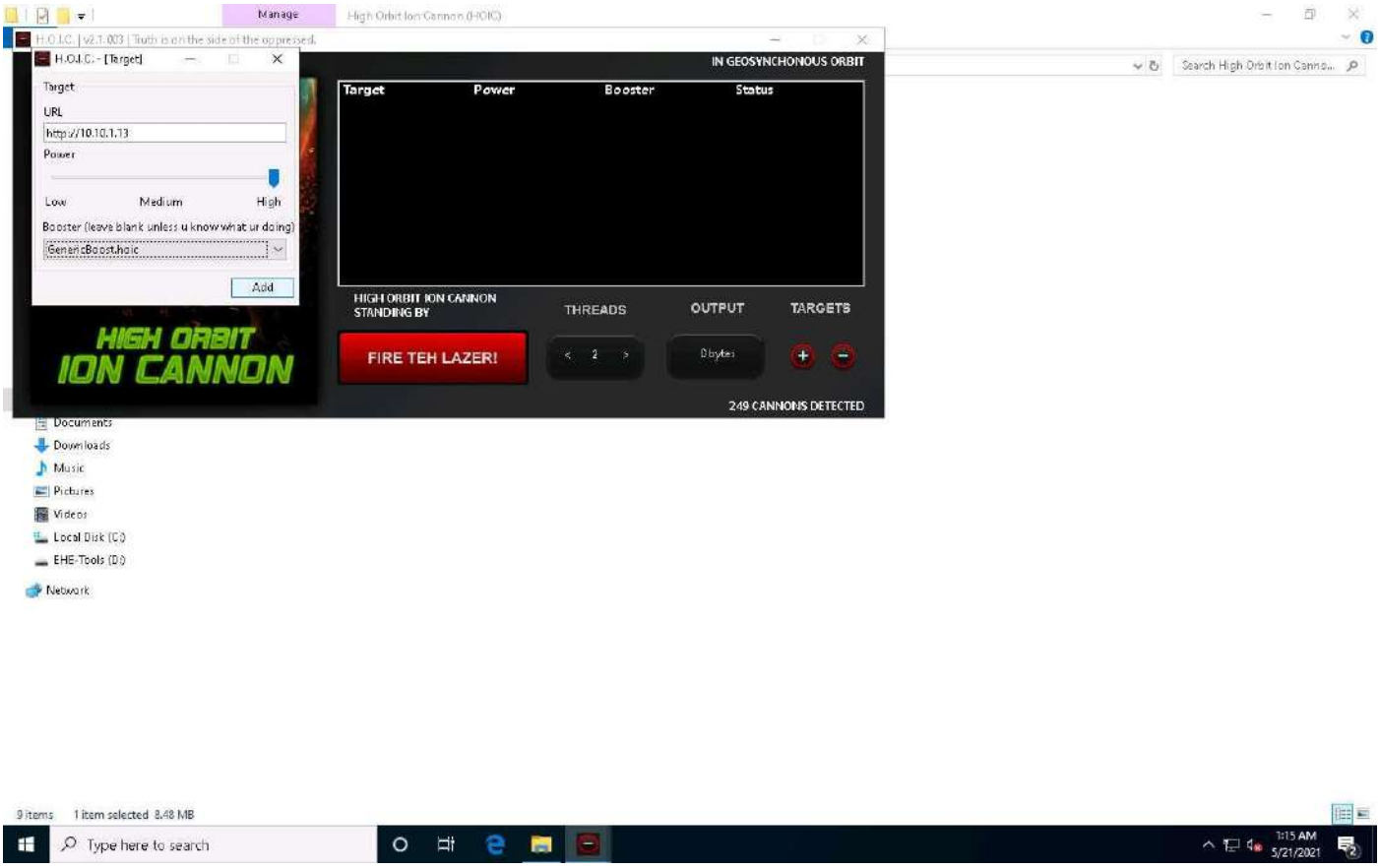
If an **Open File - Security Warning** pop-up appears, click **Run**.



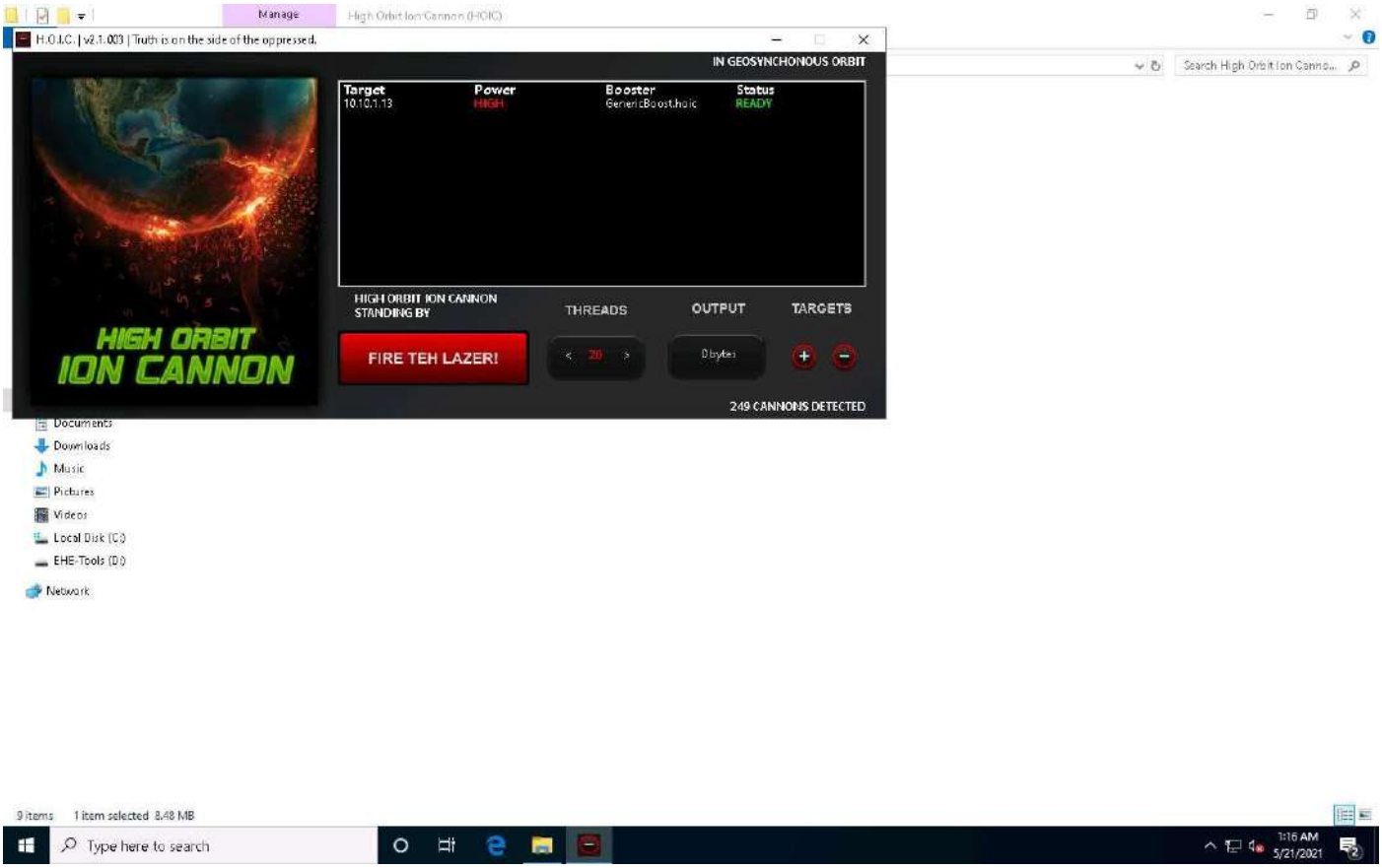
8. The **HOIC** GUI main window appears; click the "**+**" button below the **TARGETS** section.



9. The **HOIC - [Target]** pop-up appears. Type the target URL such as **http://[Target IP Address]** (here, the target IP address is **10.10.1.13 [Parrot Security]**) in the **URL** field. Slide the **Power** bar to **High**. Under the **Booster** section, select **GenericBoost.hoic** from the drop-down list, and click **Add**.



10. Set the **THREADS** value to **20** by clicking the **>** button until the value is reached.

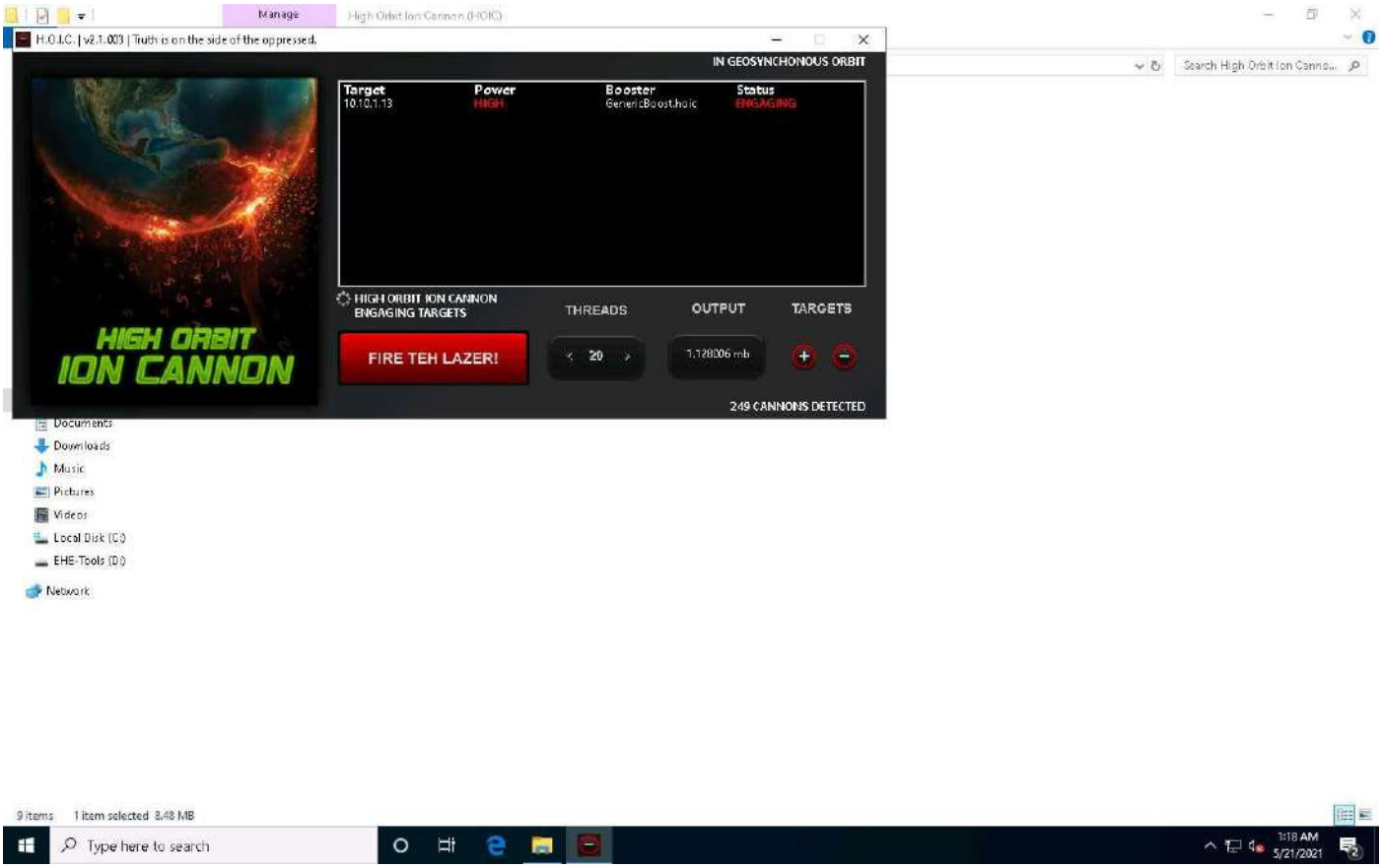


11. Now, switch to the **Windows Server 2019** (click Windows Server 2019 to switch to the **Windows Server 2019**) and **Windows Server 2016** (click Windows Server 2016 to switch to the **Windows Server 2016**) machines and follow **Steps 7-10** to configure HOIC.
12. Once **HOIC** is configured on all machines, switch to each machine (**Windows 10**, **Windows Server 2019**, and **Windows Server 2016**) and click the **FIRE TEH LAZER!** button to initiate the DDoS attack on the target the **Parrot Security** machine.

To switch to the **Windows 10**, click Windows 10

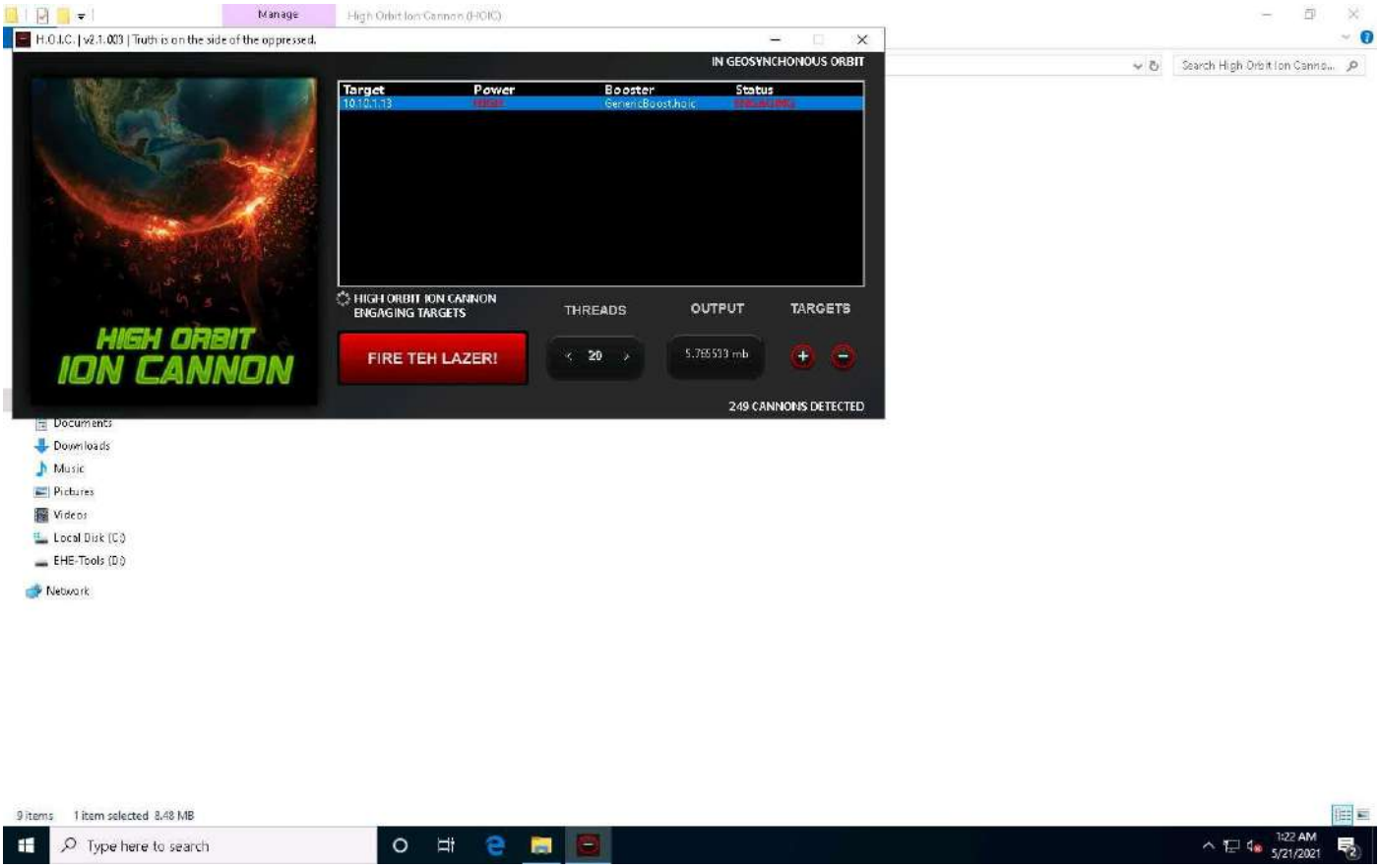
To switch to the **Windows Server 2019**, click Windows Server 2019.

To switch to the **Windows Server 2016**, click Windows Server 2016.



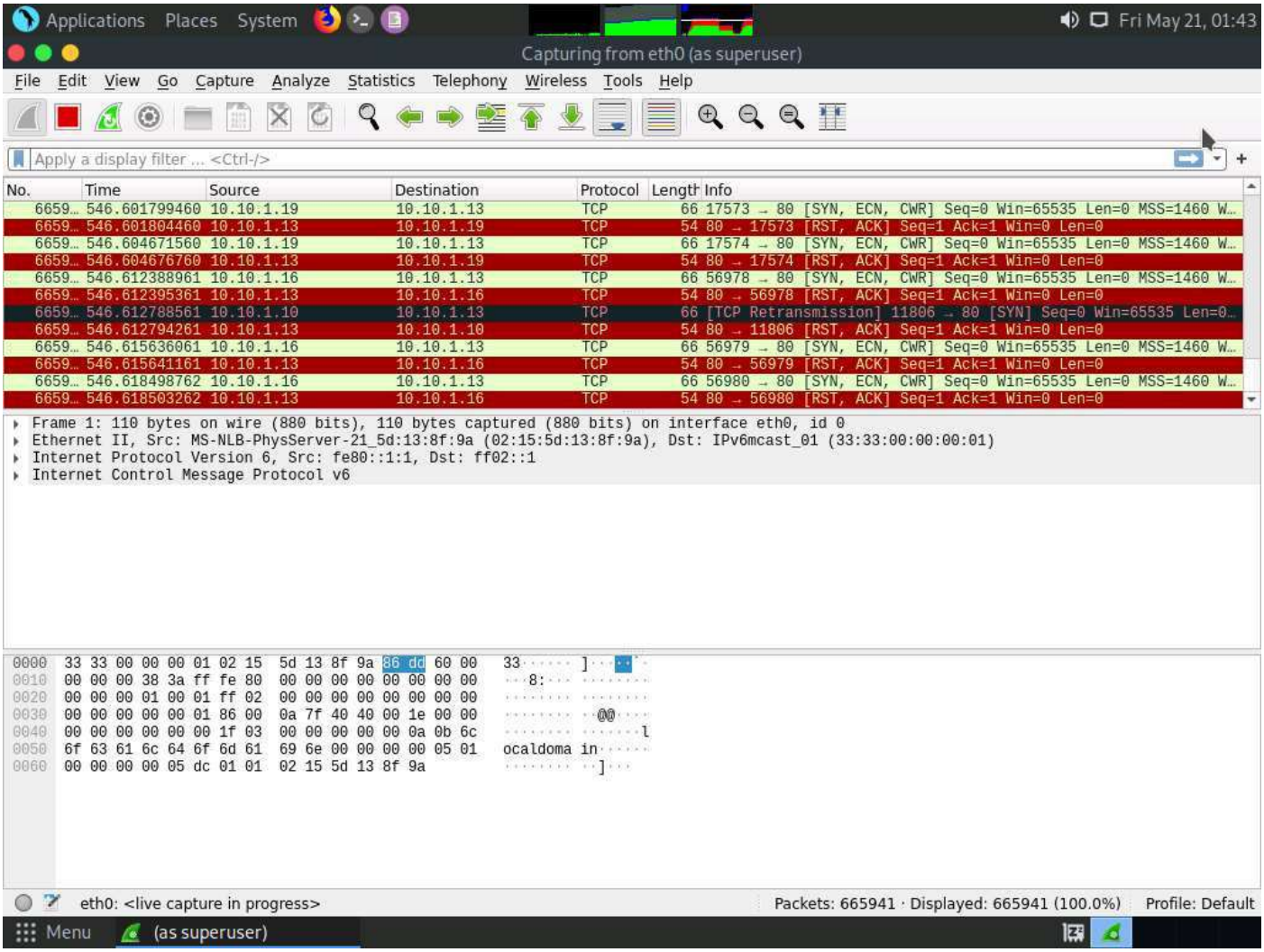
13. Observe that the **Status** changes from **READY** to **ENGAGING**, as shown in the screenshot.

If **HOIC** window closes relaunch it and configure it again.



14. Click Parrot Security switch to the **Parrot Security** machine.

15. Observe that **Wireshark** starts capturing a large volume of packets, which means that the machine is experiencing a huge number of incoming packets. These packets are coming from the **Windows 10, Windows Server 2019**, and **Windows Server 2016** machines.



16. You can observe that the performance of the machine is slightly affected and that its response is slowing down.

17. In this lab, only three machines are used to demonstrate the flooding of a single machine. If there are a large number of machines performing flooding, then the target machine's (here, **Parrot Security**) resources are completely consumed, and the machine is overwhelmed.

In real-time, a group of hackers operating hundreds or thousands of machines configure this tool on their machines, communicate with each other through IRCs, and simulate the DDoS attack by flooding a target machine or website at the same time. The target is overwhelmed and stops responding to user requests or starts dropping packets coming from legitimate users. The larger the number of attacker machines, the higher the impact of the attack on the target machine or website.

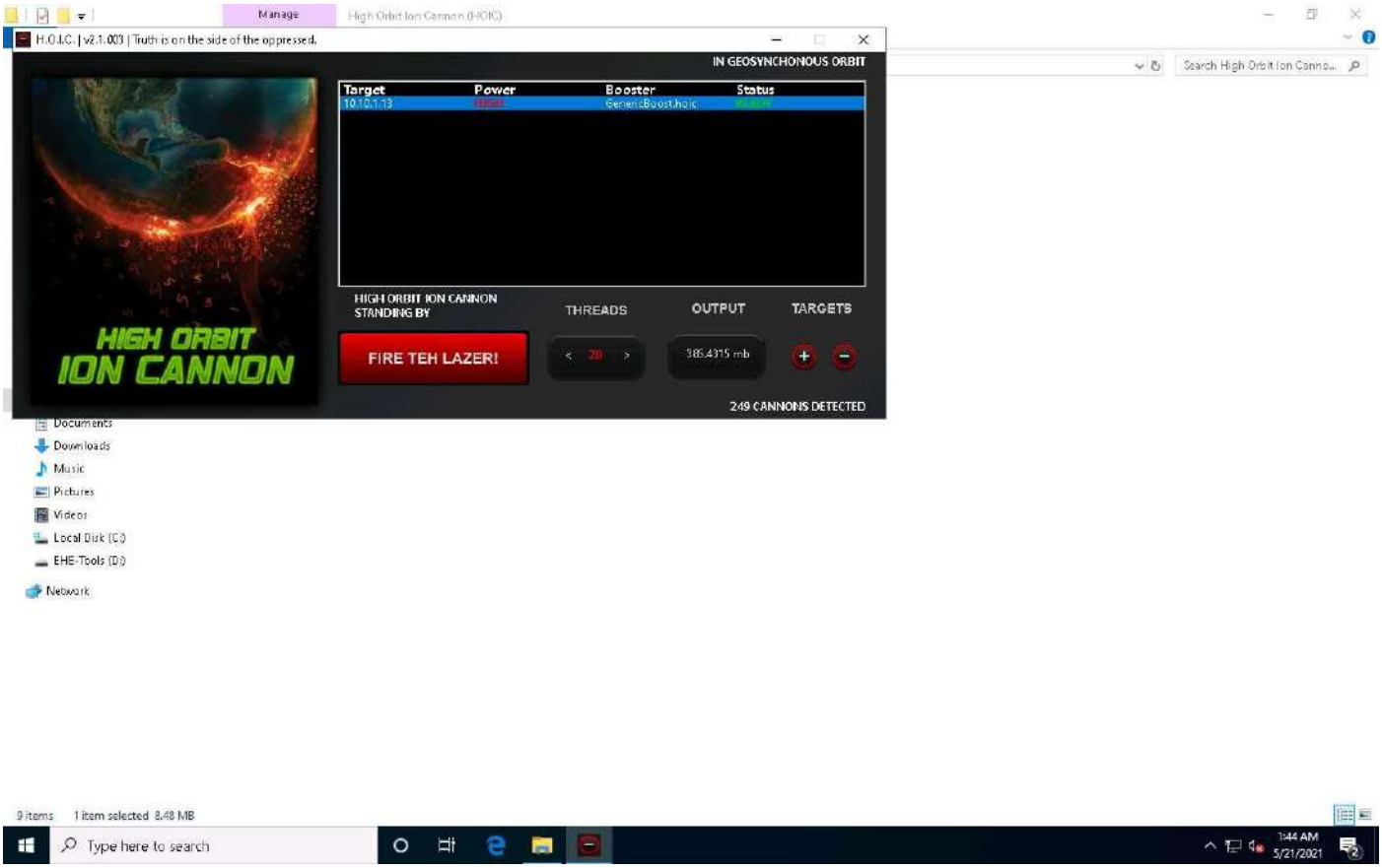
18. On completion of the task, click **FIRE TEH LAZER!** again, and then close the HOIC window on all the attacker machines. Also, close the **Wireshark** window on the **Parrot Security** machine.

To switch to the **Windows 10**, click Windows 10

To switch to the **Windows Server 2019**, click Windows Server 2019.

To switch to the **Windows Server 2016**, click Windows Server 2016.

To switch to **Parrot Security** machine click Parrot Security



19. This concludes the demonstration of how to perform a DDoS attack using HOIC.
20. Close all open windows and document all the acquired information.

Lab 5: Detect and Protect Against DDoS Attack

Lab Scenario

DoS/DDoS attacks are one of the foremost security threats on the Internet; thus, there is a greater necessity for solutions to mitigate these attacks. Early detection techniques help to prevent DoS and DDoS attacks. Detecting such attacks is a tricky job. A DoS and DDoS attack traffic detector needs to distinguish between genuine and bogus data packets, which is not always possible; the techniques employed for this purpose are not perfect. There is always a chance of confusion between traffic generated by a legitimate network user and traffic generated by a DoS or DDoS attack. One problem in filtering bogus from legitimate traffic is the volume of traffic. It is impossible to scan each data packet to ensure security from a DoS or DDoS attack. All the detection techniques used today define an attack as an abnormal and noticeable deviation in network traffic statistics and characteristics. These techniques involve the statistical analysis of deviations to categorize malicious and genuine traffic.

We must use various DoS and DDoS attack detection techniques to prevent the systems in the network from being damaged.

This lab provides hands-on experience in detecting DoS and DDoS attacks using various detection techniques.

Lab Objectives

- Detect and protect against DDoS attacks using Anti DDoS Guardian

Task 1: Detect and Protect Against DDoS Attack using Anti DDoS Guardian

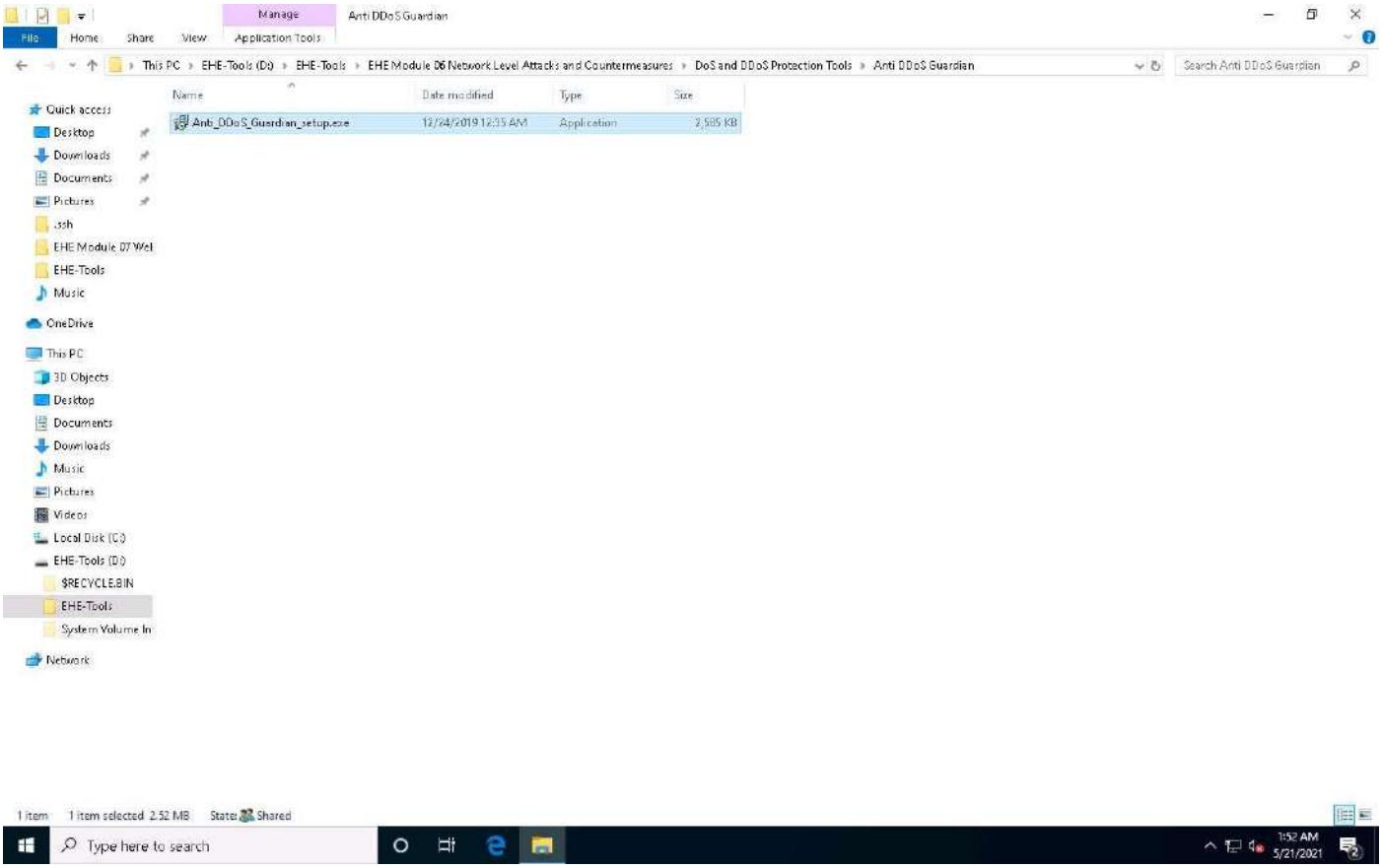
Anti DDoS Guardian is a DDoS attack protection tool. It protects IIS servers, Apache serves, game servers, Camfrog servers, mail servers, FTP servers, VOIP PBX, and SIP servers and other systems. Anti DDoS Guardian monitors each incoming and outgoing packet in Real-Time. It displays the local address, remote address, and other information of each network flow. Anti DDoS Guardian limits network flow number, client bandwidth, client concurrent TCP connection number, and TCP connection rate. It also limits the UDP bandwidth, UDP connection rate, and UDP packet rate.

Here, we will detect and protect against a DDoS attack using Anti DDoS Guardian.

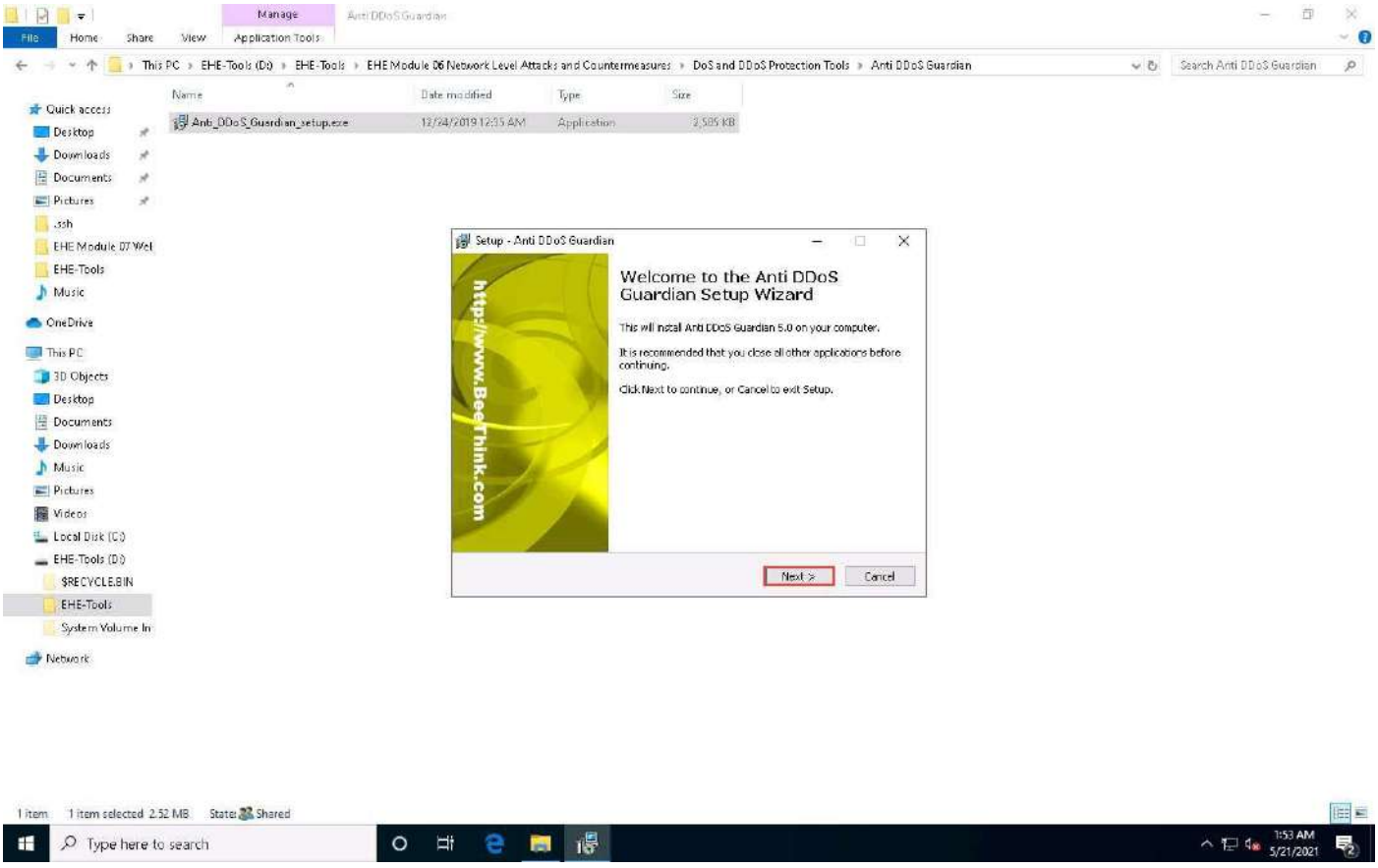
In this task, we will use the **Windows Server 2019** and **Windows Server 2016** machines to perform a DDoS attack on the target system, **Windows 10**.

1. On the **Windows 10** machine, navigate to **D:\EHE-Tools\EHE Module 06 Network Level Attacks and Countermeasures\DoS and DDoS Protection Tools\Anti DDoS Guardian** and double click **Anti_DDoS_Guardian_setup.exe.**

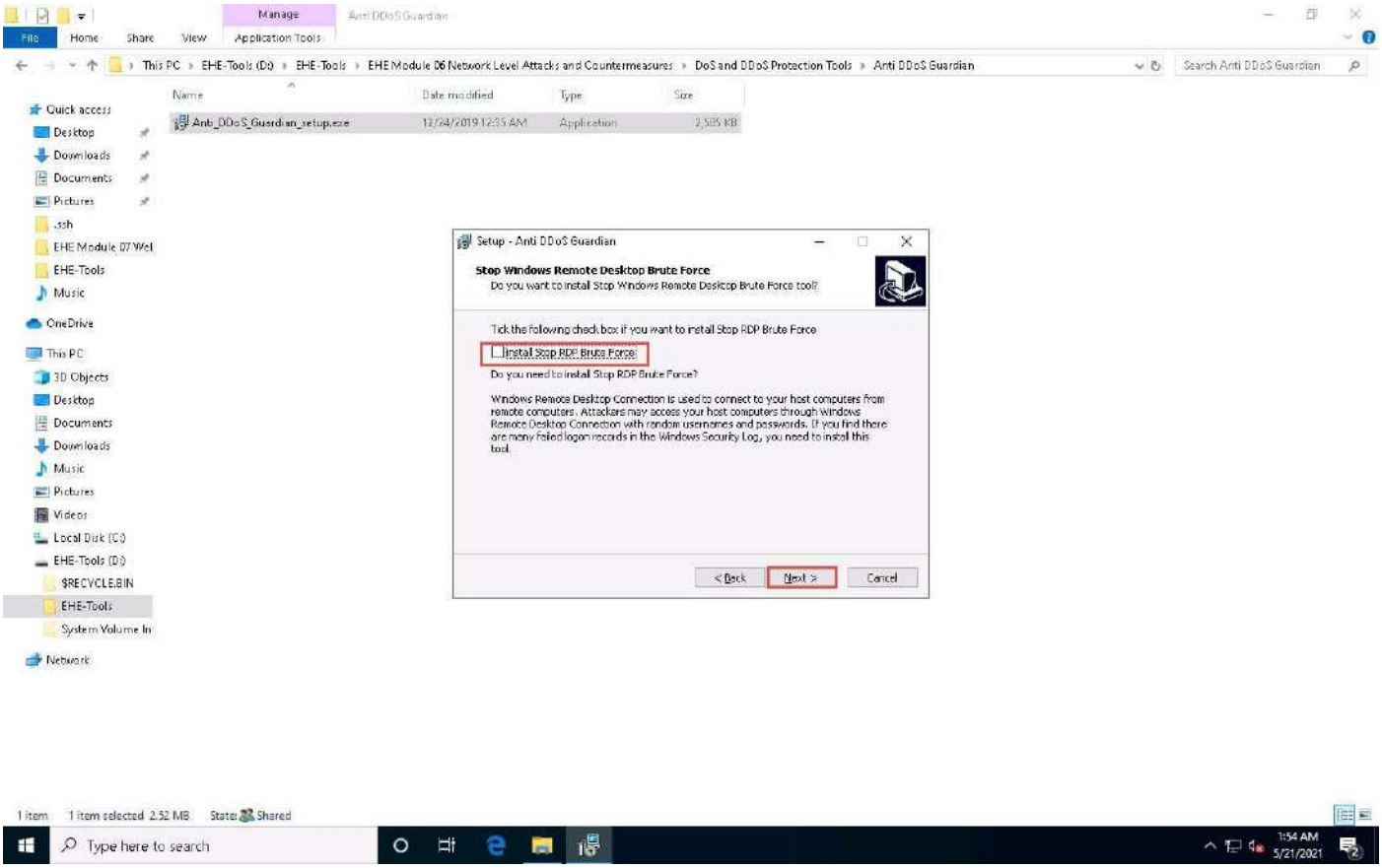
If a **User Account Control** pop-up appears, click **Yes**.



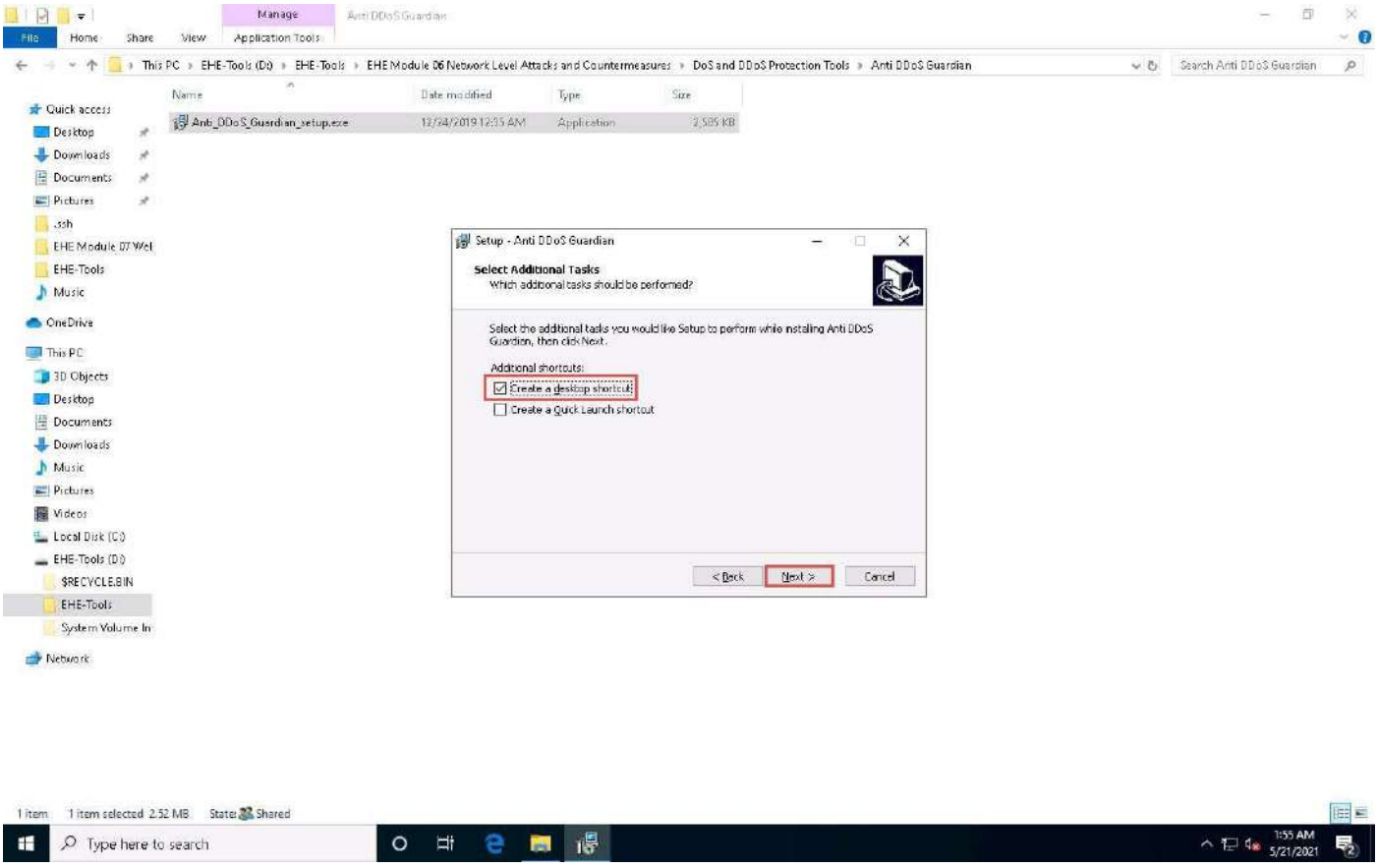
2. The **Setup - Anti DDoS Guardian window** appears; click **Next**. Follow the wizard-driven installation steps to install the application.



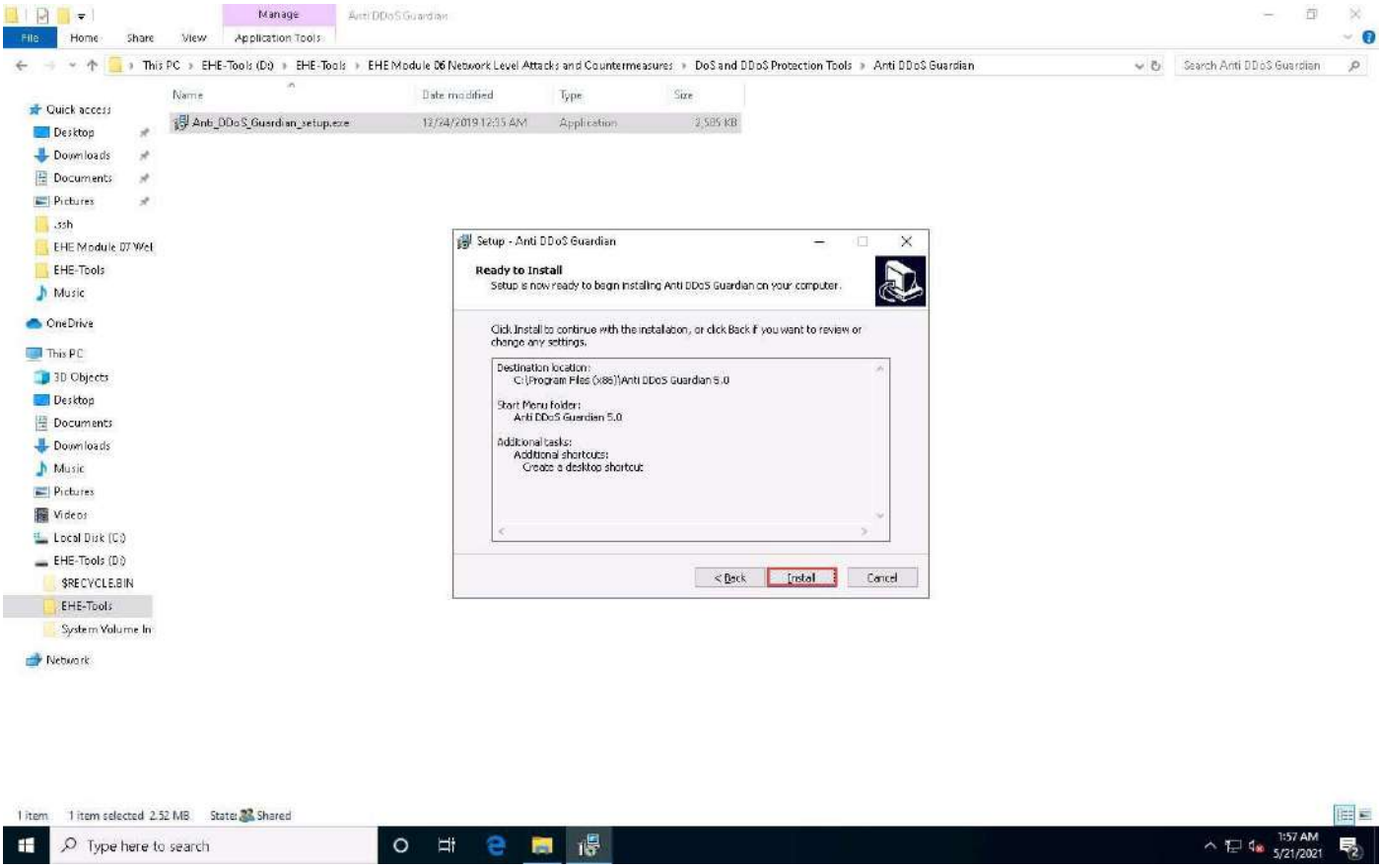
3. In the **Stop Windows Remote Desktop Brute Force** wizard, uncheck the **install Stop RDP Brute Force** option, and click **Next**.



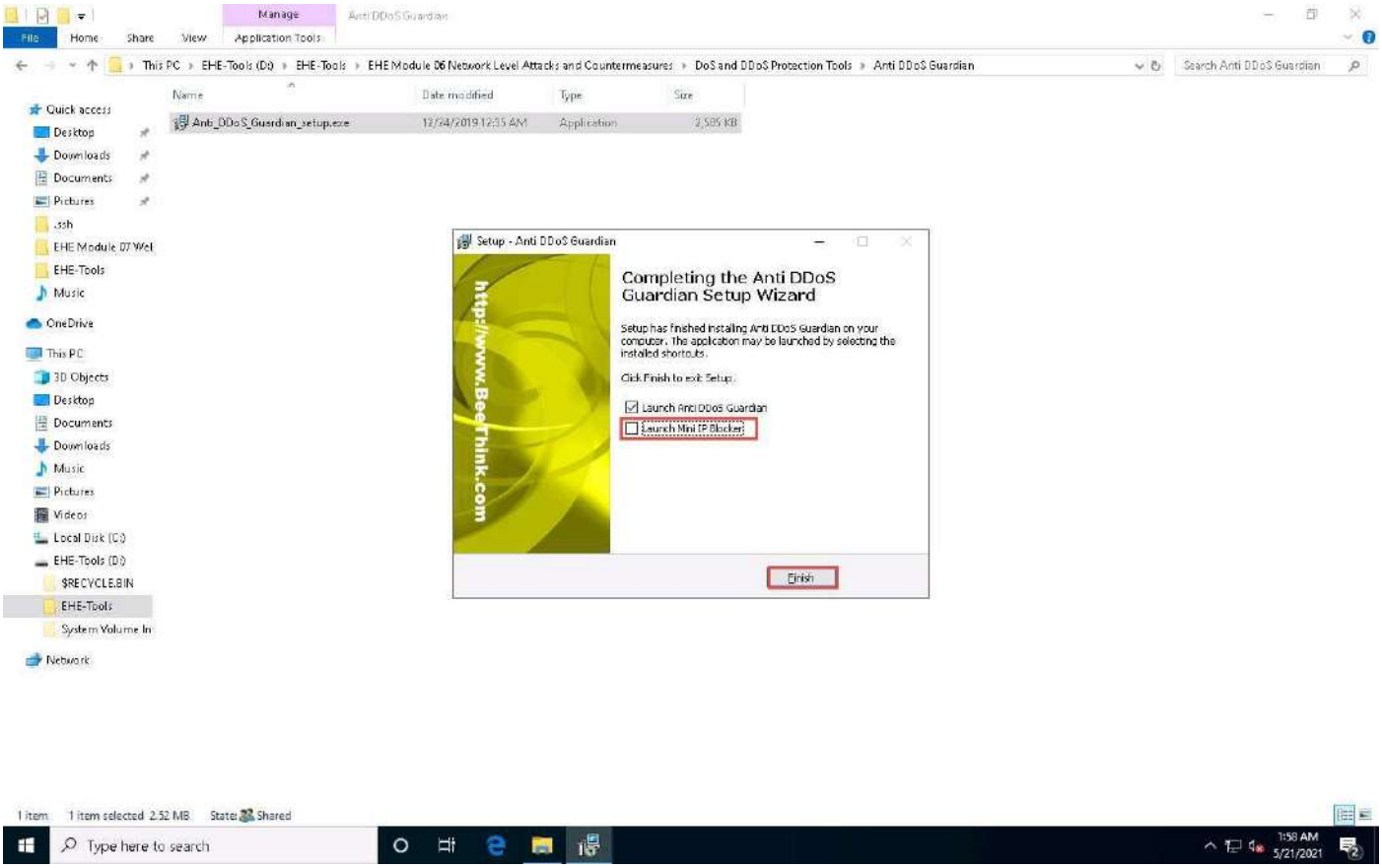
4. The **Select Additional Tasks** wizard appears; check the **Create a desktop shortcut** option, and click **Next**.



5. The **Ready to Install** wizard appears; click **Install**.

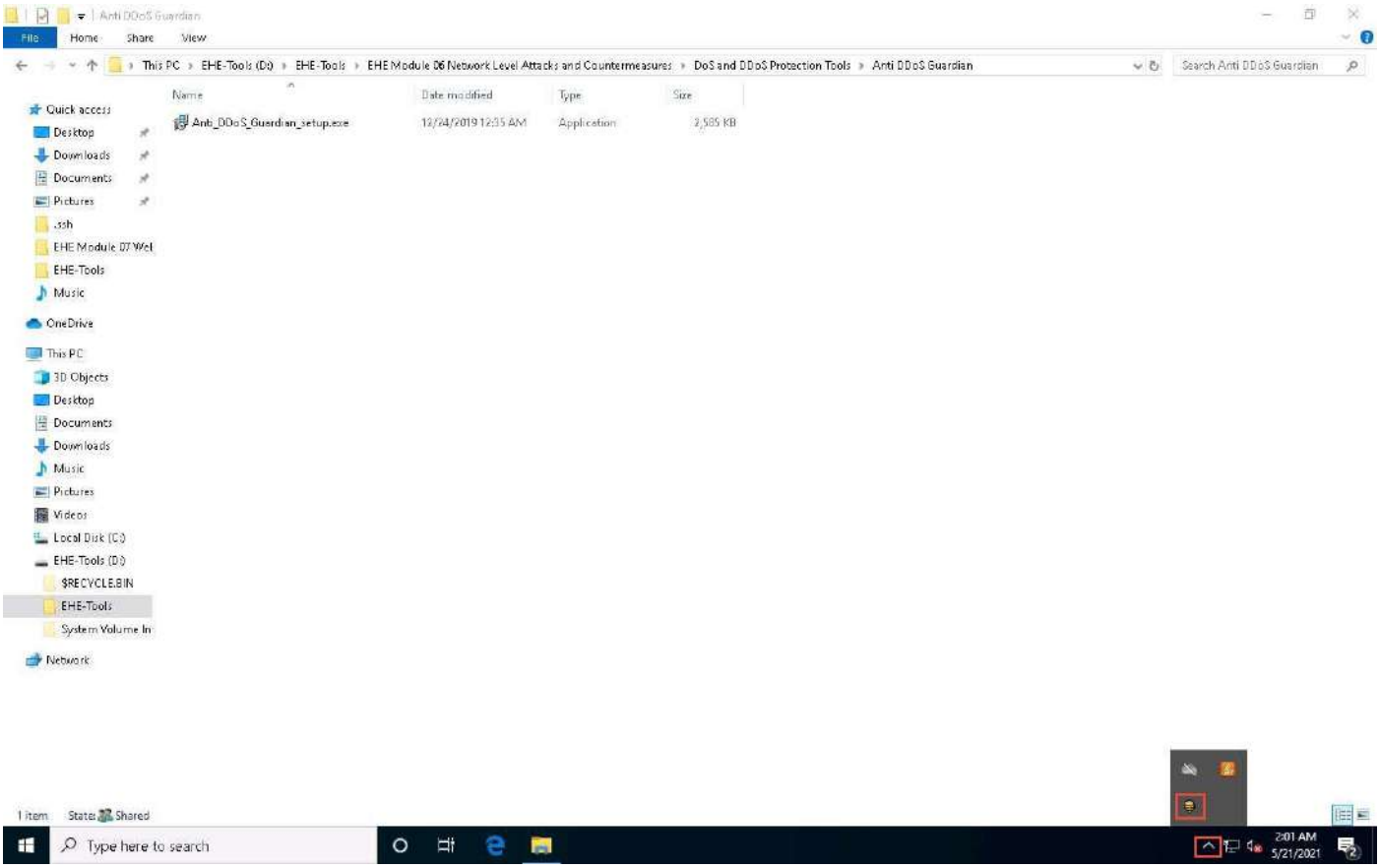


6. The **Completing the Anti DDoS Guardian Setup Wizard** window appears; uncheck the **Launch Mini IP Blocker** option and click **Finish**.

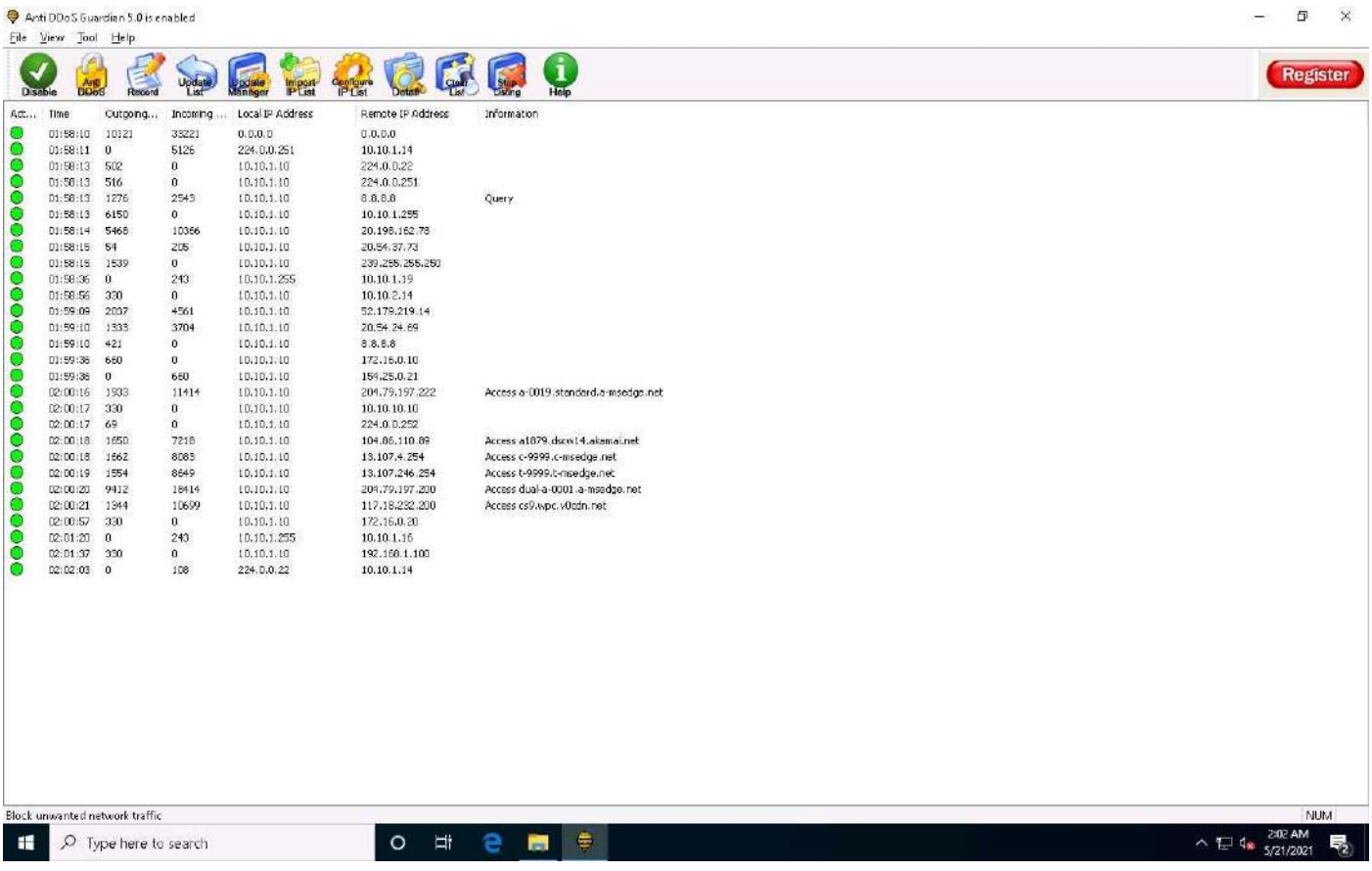


7. The **Anti-DDoS Wizard** window appears; click **Continue** in all the wizard steps, leaving all the default settings. In the last window, click **Finish**.

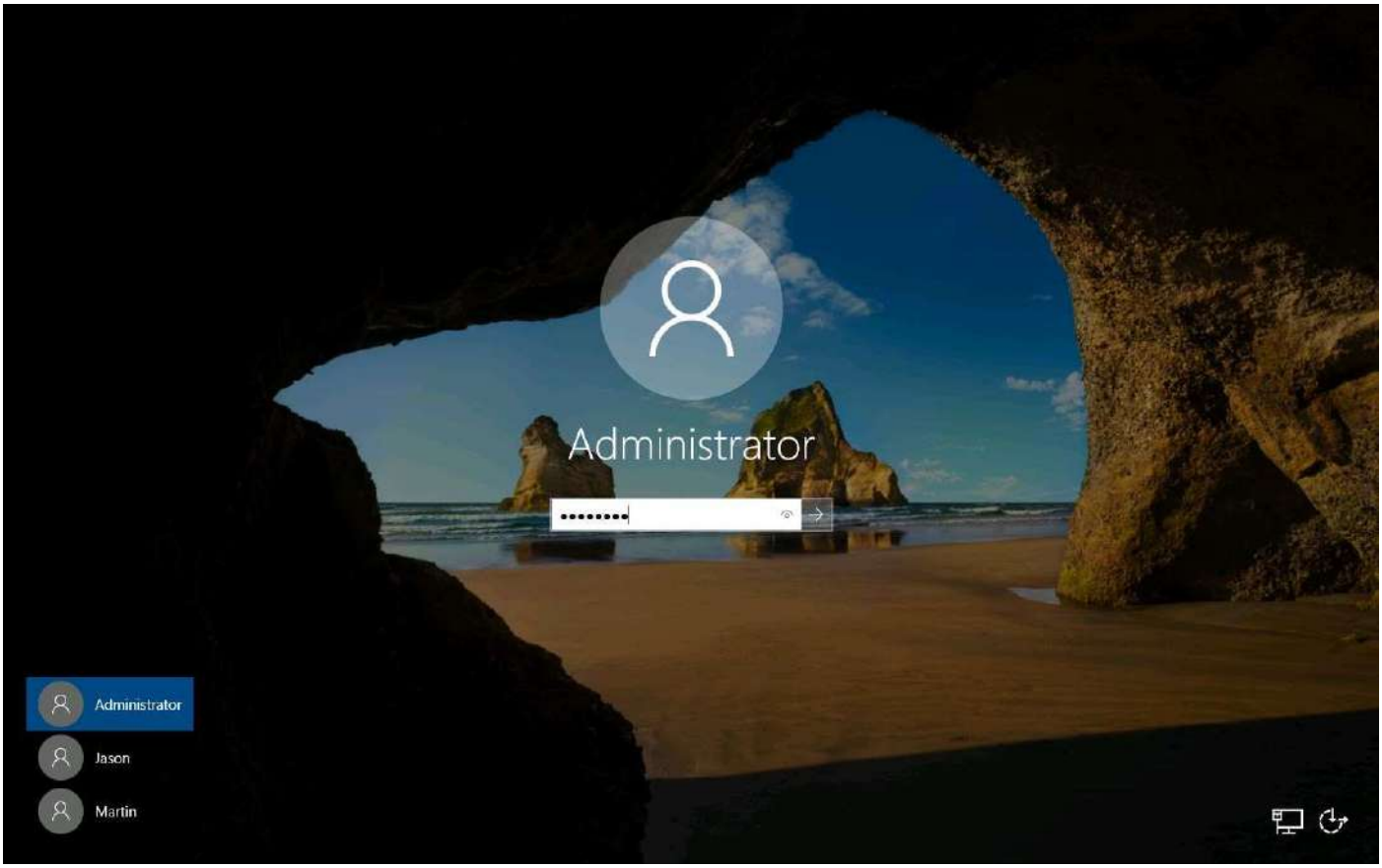
8. Click **Show hidden icons** from the bottom-right corner of **Desktop** and click the **Anti DDoS Guardian** icon.



9. The **Anti DDoS Guardian** window appears, displaying information about incoming and outgoing traffic, as shown in the screenshot.

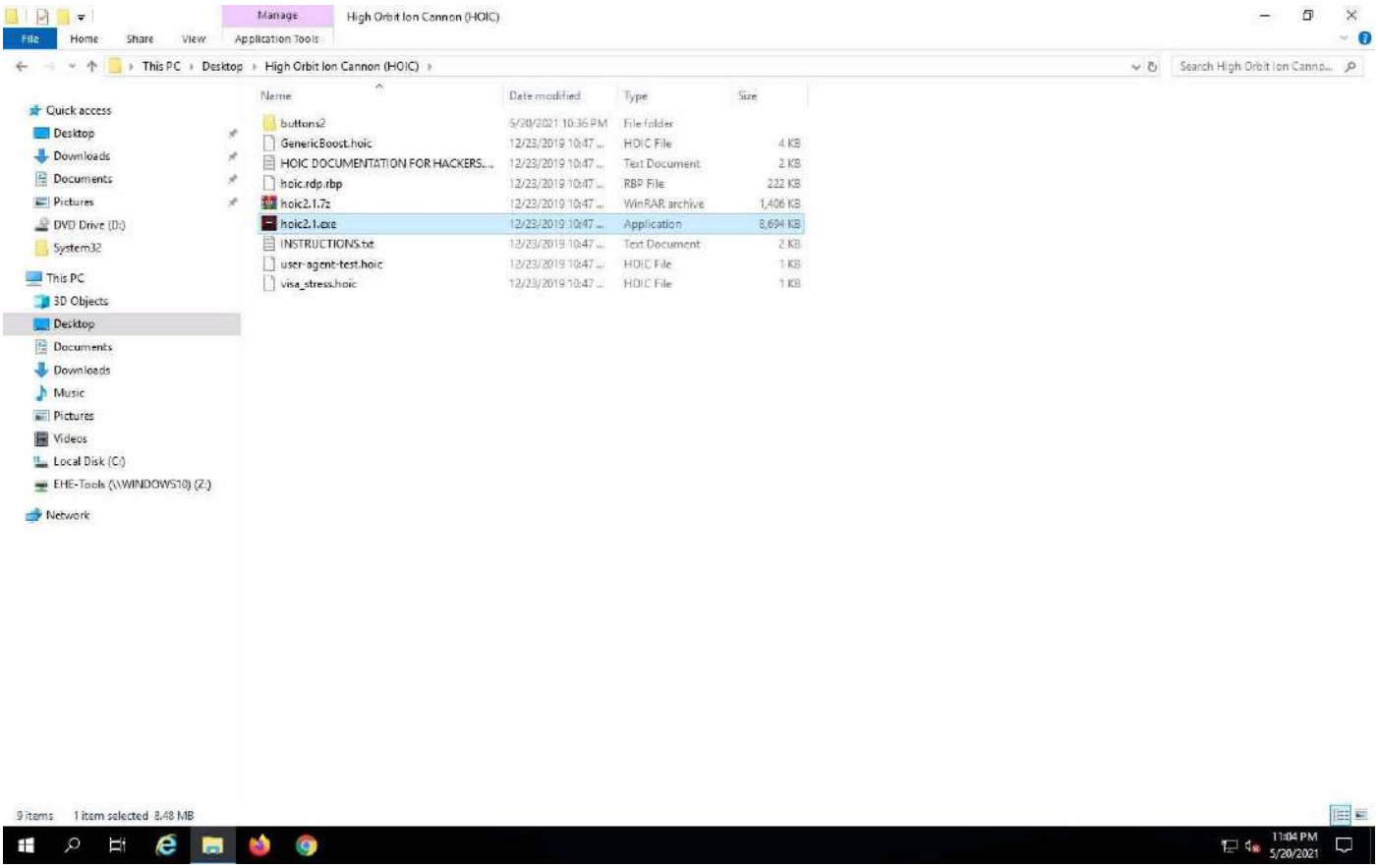


10. Now, click Windows Server 2019 to switch to the **Windows Server 2019** and click Ctrl+Alt+Delete to activate the machine. By default, **Administrator** profile is selected, click Pa$$w0rd to enter the password and press **Enter** to log in.

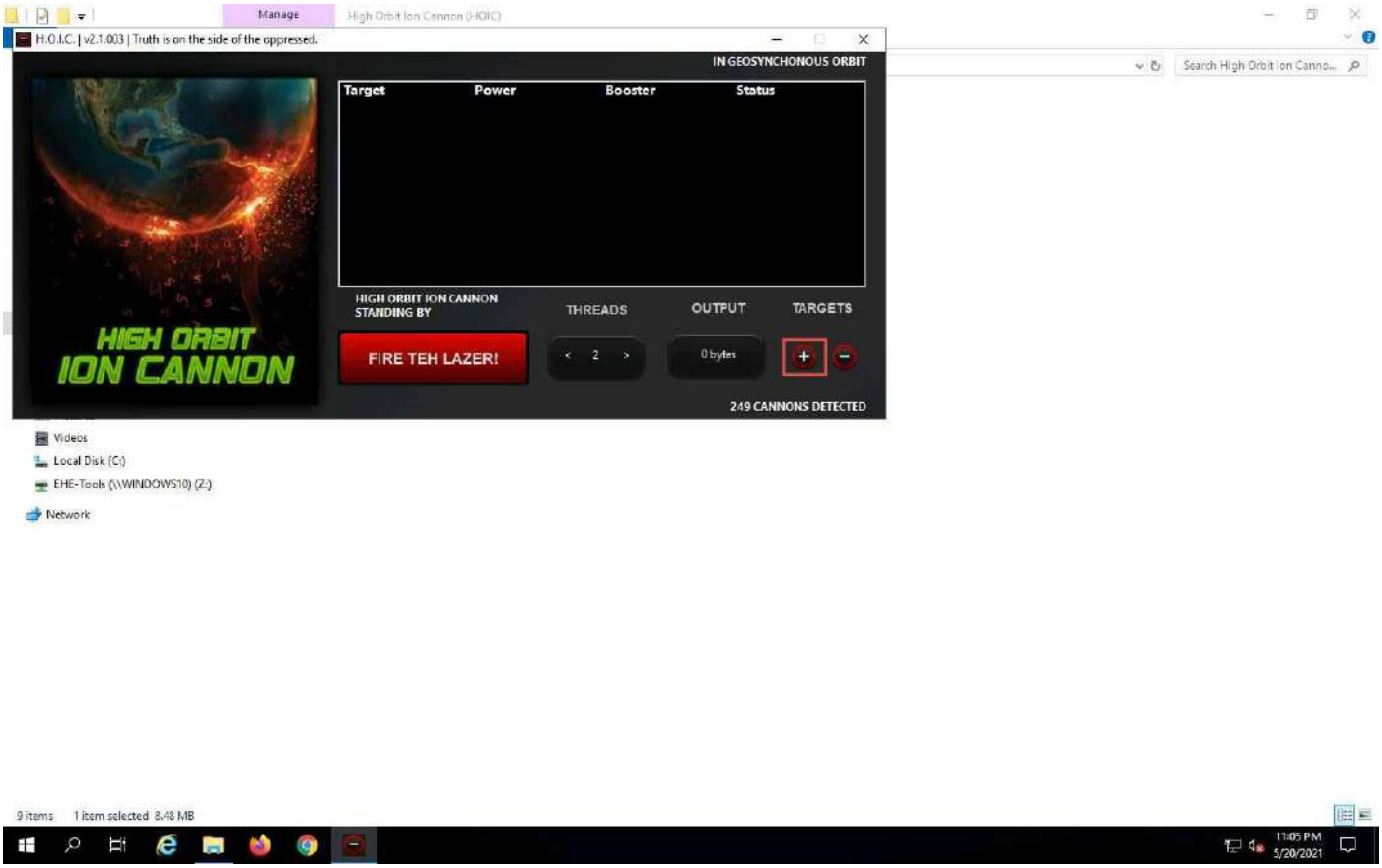


11. Navigate to **Desktop**, open the **High Orbit Ion Cannon (HOIC)** folder, and double-click **hoic2.1.exe**.

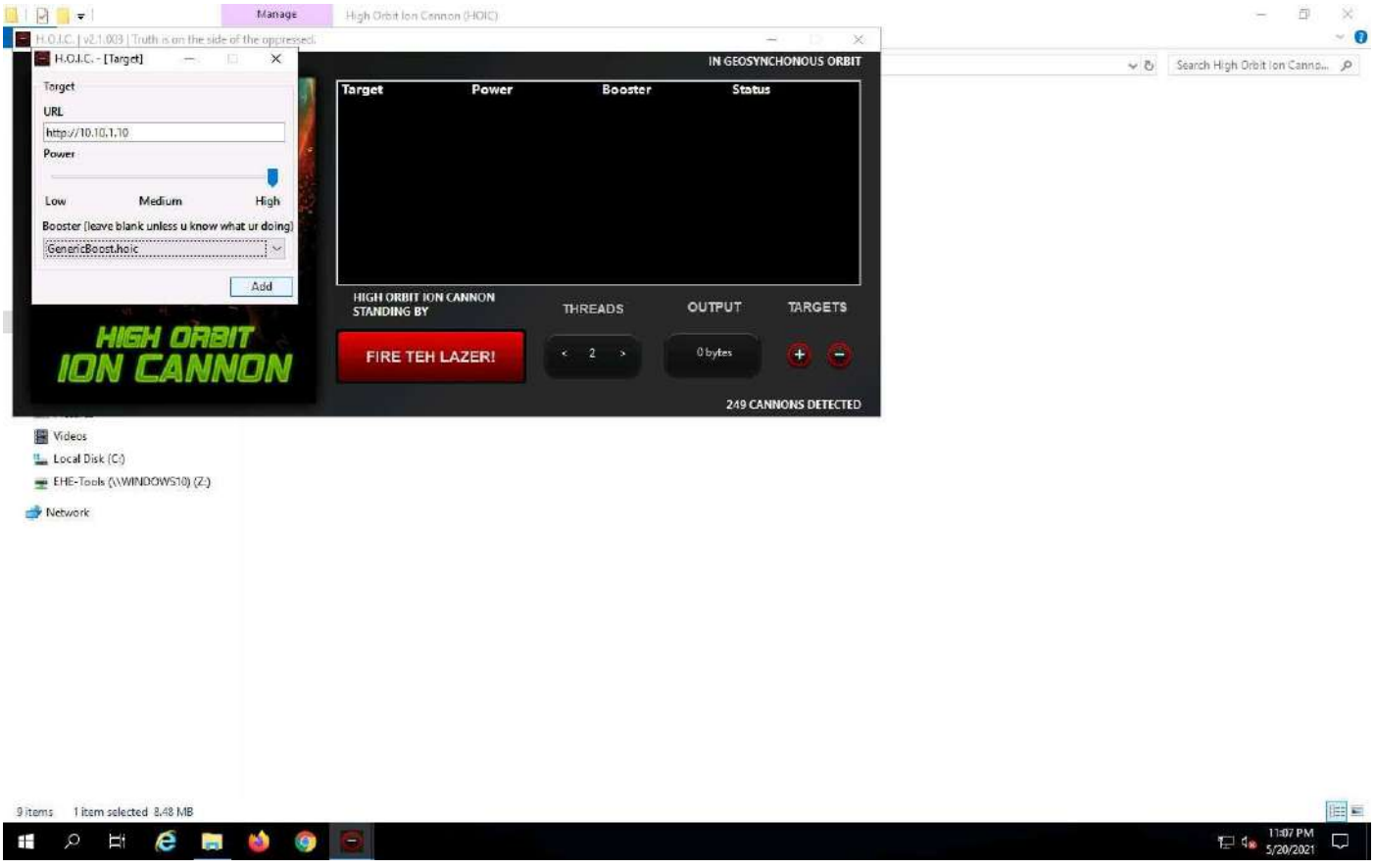
If an **Open File - Security Warning** pop-up appears, click **Run**.



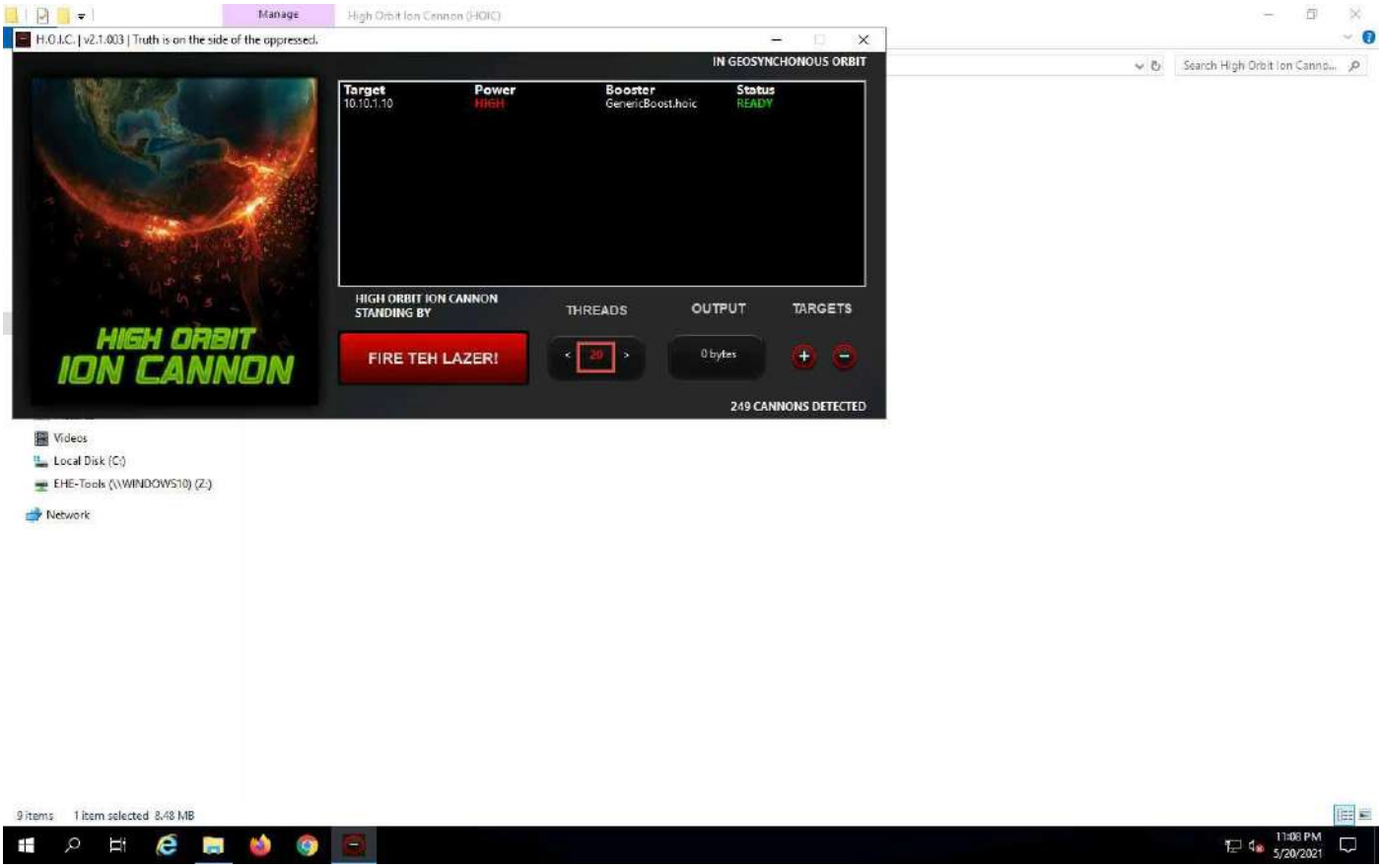
12. The **HOIC** GUI main window appears. Click the "**+**" button below the **TARGETS** section.



13. The **HOIC - [Target]** pop-up appears. Type the target URL such as **http://[Target IP Address]** (here, the target IP address is **10.10.1.10 [Windows 10]**) in the **URL** field. Slide the **Power** bar to **High**. Under the **Booster** section, select **GenericBoost.hoic** from the drop-down list and click **Add**.



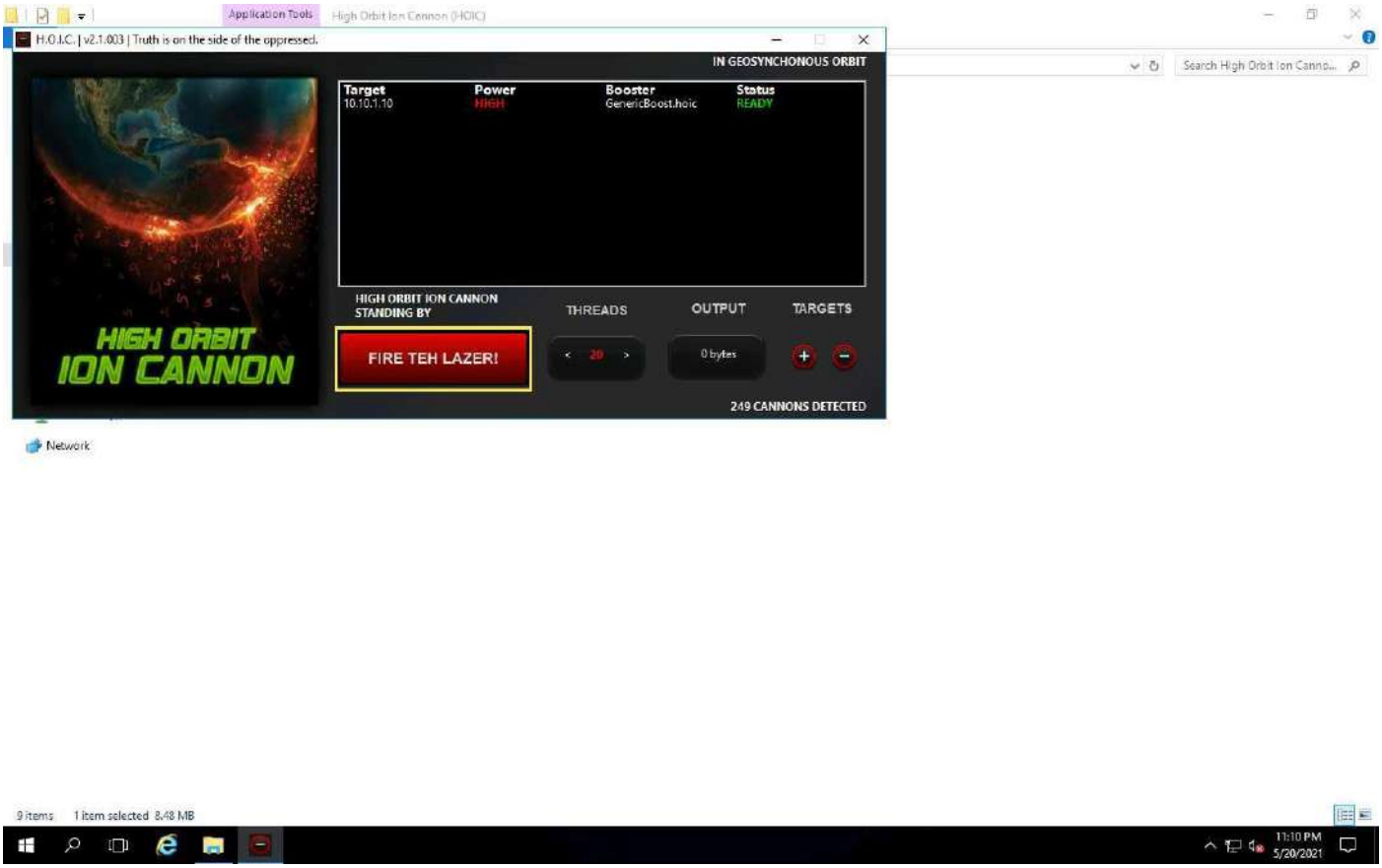
14. Set the **THREADS** value to **20** by clicking the **>** button until the value is reached.



15. Now, click Windows Server 2016 to switch to **Windows Server 2016** and click Ctrl+Alt+Delete to activate the machine. By default, **EHE\Administrator** profile is selected, click Pa$$w0rd to enter the password and press **Enter** to log in. Follow **Steps 11 - 14** to launch and configure HOIC.
16. Once **HOIC** is configured on both machines, switch to each machine (**Windows Server 2019** and **Windows Server 2016**) and click the **FIRE TEH LAZER!** button to initiate the DDoS attack on the target **Windows 10** machine.

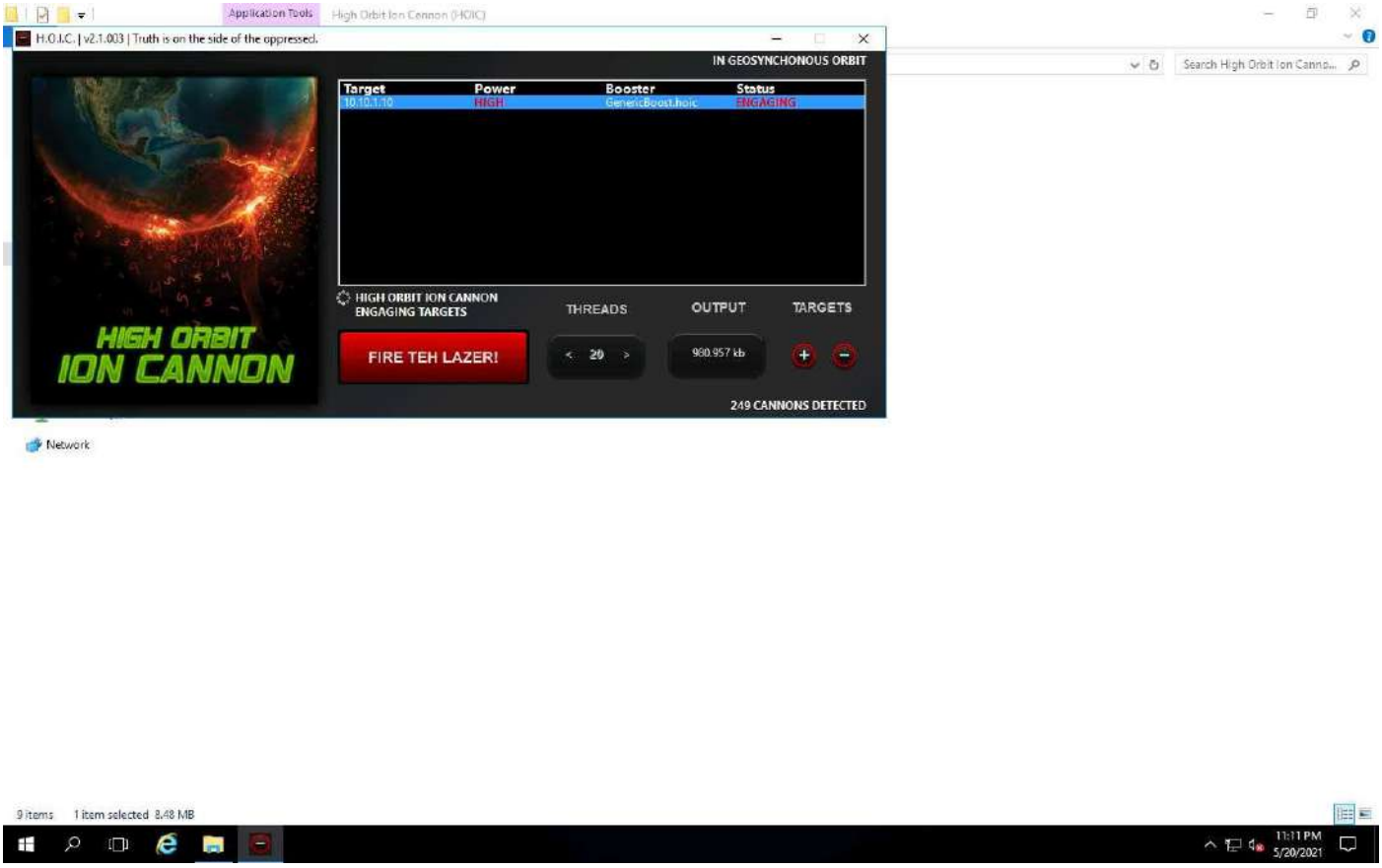
To switch to the **Windows Server 2019**, click Windows Server 2019.

To switch to the **Windows Server 2016**, click Windows Server 2016.



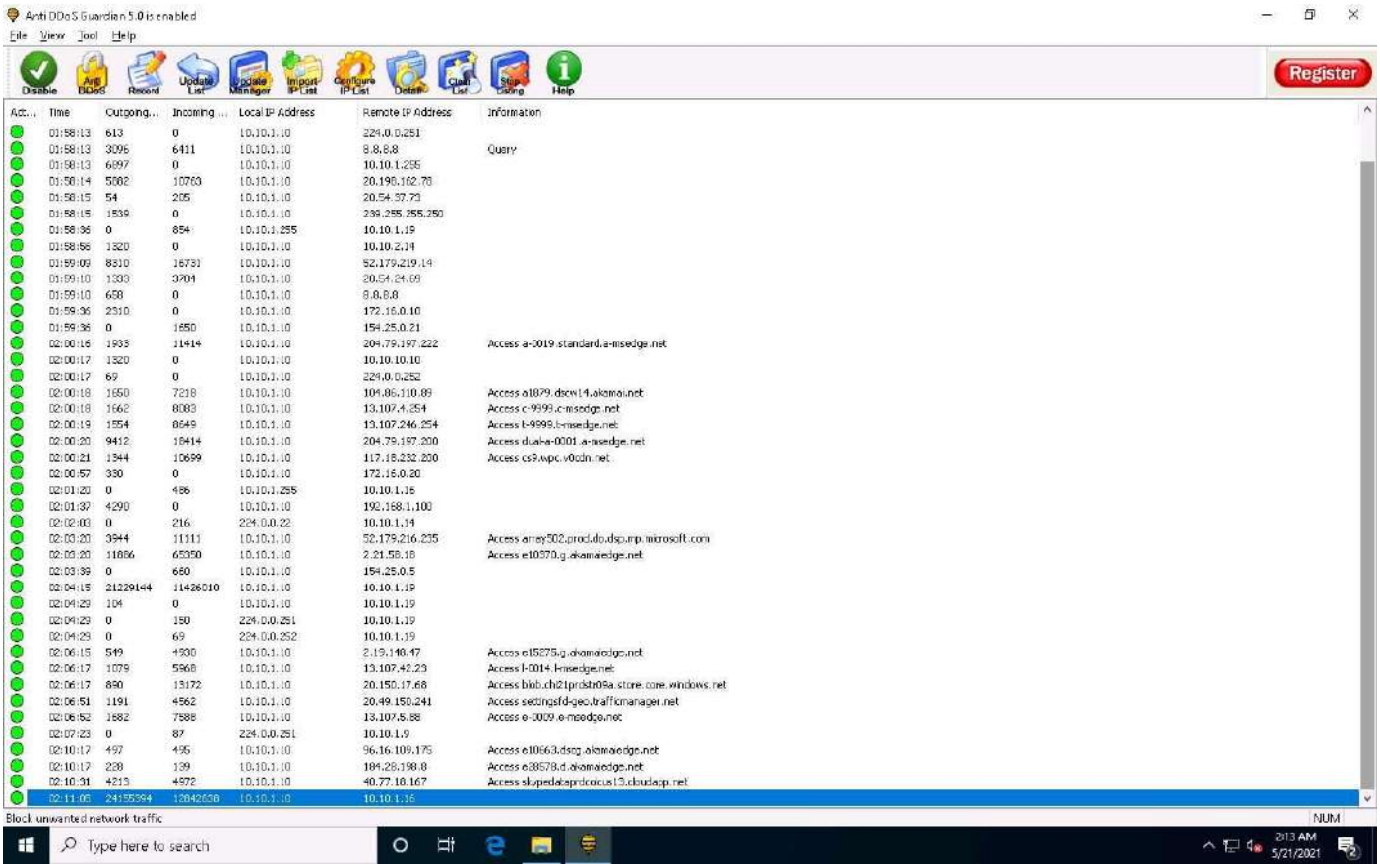
17. Observe that the **Status** changes from **READY** to **ENGAGING**, as shown in the screenshot.

If **HOIC** window closes relaunch it and configure it again.



18. Click Windows 10 to switch back to the **Windows 10** machine and observe the packets captured by **Anti DDoS Guardian**.

19. Observe the huge number of packets coming from the host machines (**10.10.1.19 [Windows Server 2019**] and **10.10.1.16 [Windows Server 2016]**).



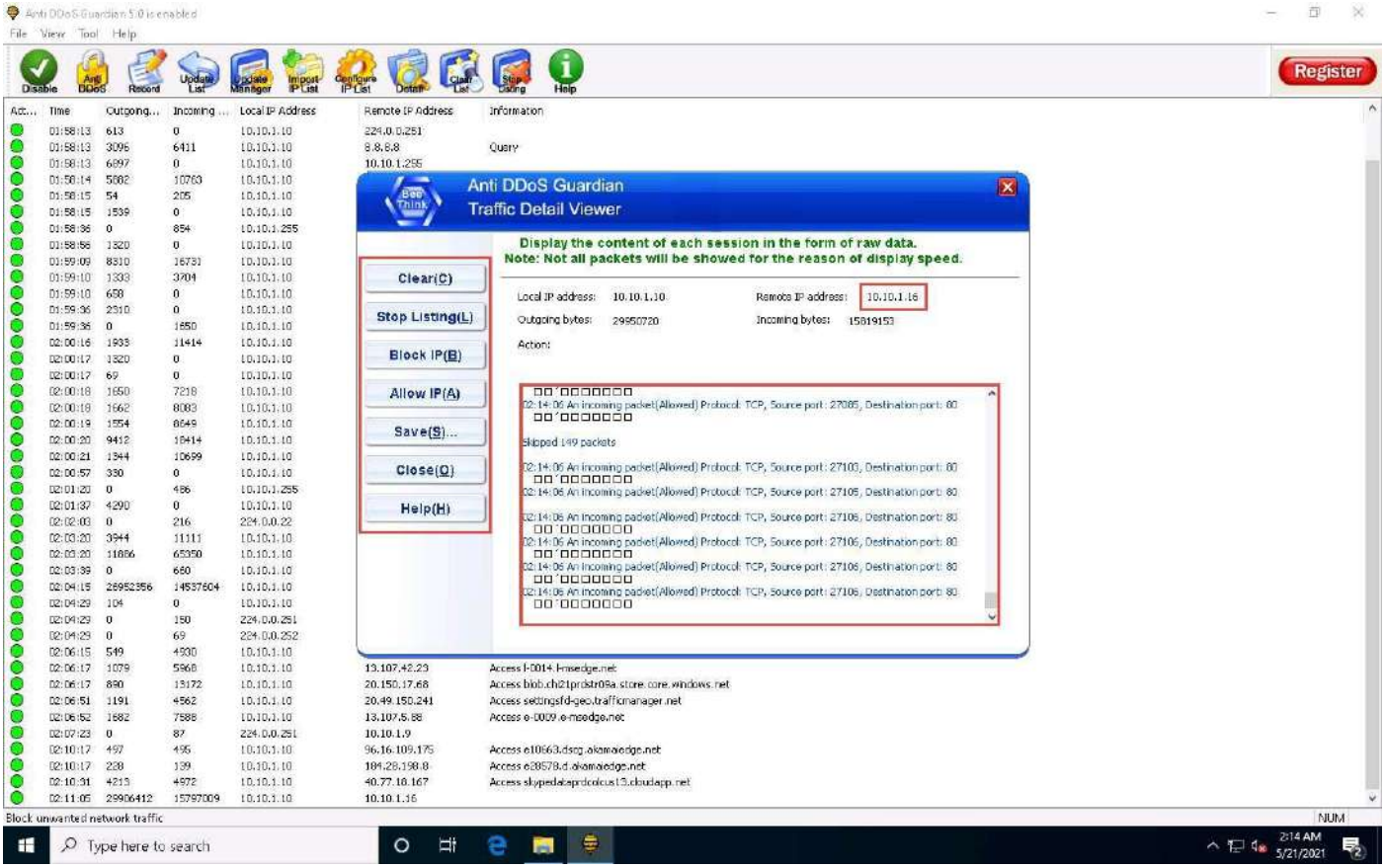
20. Double-click any of the sessions **10.10.1.19** or **10.10.1.16**.

Here, we have selected 10.10.1.16. You can select either of them.

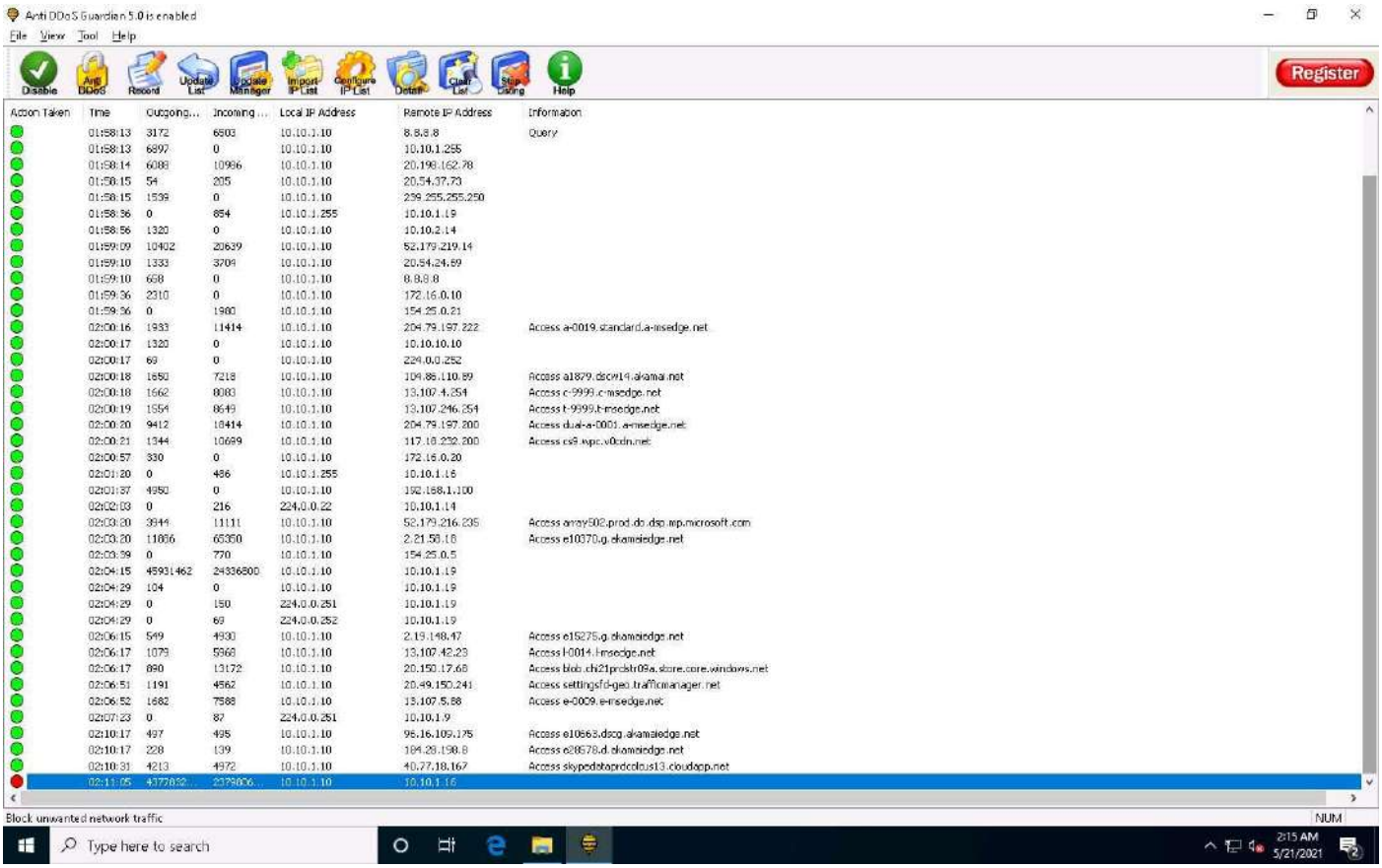
21. The **Anti DDoS Guardian Traffic Detail Viewer** window appears, displaying the content of the selected session in the form of raw data. You can observe the high number of incoming bytes from **Remote IP address 10.10.1.16**, as shown in the screenshot.

22. You can use various options from the left-hand pane such as **Clear**, **Stop Listing**, **Block IP**, and **Allow IP**. Using the Block IP option blocks the IP address sending the huge number of packets.

23. In the **Traffic Detail Viewer** window, click **Block IP** option from the left pane.



24. Observe that the blocked IP session turns red in the **Action Taken** column.



25. Similarly, you can **Block IP** the address of the **10.10.1.19** session.

26. On completion of the task, click **FIRE TEH LAZER!** again, and then close the HOIC window on all attacker machines (**Windows Server 2019** and **Windows Server 2016**).

To switch to the **Windows Server 2019**, click Windows Server 2019.

To switch to the **Windows Server 2016**, click Windows Server 2016.

27. This concludes the demonstration of how to detect and protect against a DDoS attack using Anti DDoS Guardian.
28. Close all open windows and document all the acquired information.
29. In **Windows 10**, navigate to **Control Panel** --> **Programs** --> **Programs and Features** and uninstall **Anti DDoS Guardian**.

Lab 6: Perform Session Hijacking to Seize Control of a Valid TCP Communication Session Between Two Computers

Lab Scenario

Session hijacking allows an attacker to take over an active session by bypassing the authentication process. It involves stealing or guessing a victim's valid session ID, which the server uses to identify authenticated users, and using it to establish a connection with the server. The server responds to the attacker's requests as though it were communicating with an authenticated user, after which the attacker is able to perform any action on that system.

Attackers can use session hijacking to launch various kinds of attacks such as man-in-the-middle (MITM) and Denial-of-Service (DoS) attacks. A MITM attack occurs when an attacker places himself/herself between the authorized client and the server to intercept information flowing in either direction. A DoS attack happens when attackers sniff sensitive information and use it to make host or network resource unavailable to users, usually by flooding the target with requests until the system is overloaded.

We must possess the required knowledge to hijack sessions in order to test the systems in the target network.

The labs in this exercise demonstrate how to hijack an active session between two endpoints.

Lab Objectives

- Hijack a session using Zed Attack Proxy (ZAP)

Task 1: Hijack a Session using Zed Attack Proxy (ZAP)

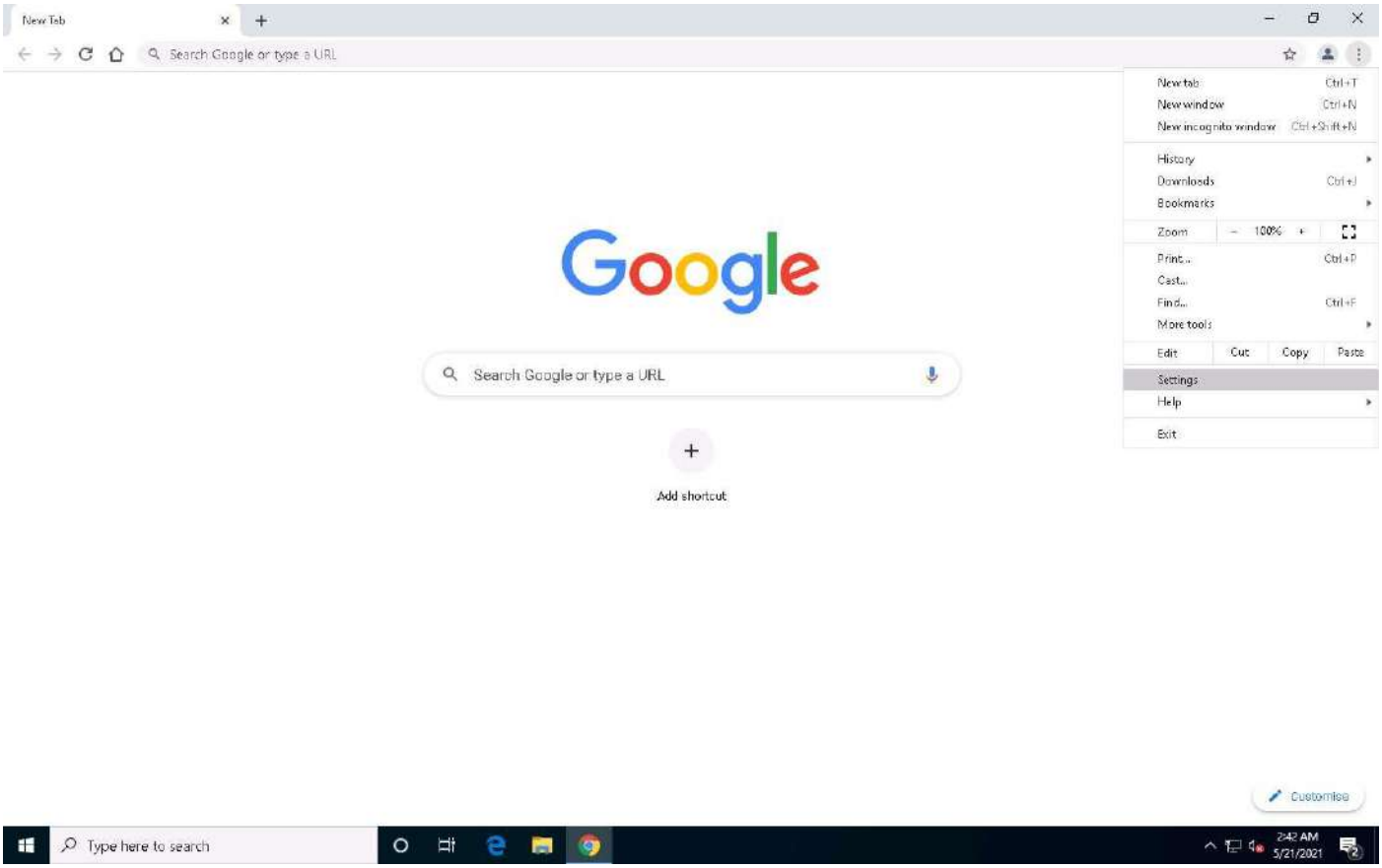
Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. It is designed to be used by people with a wide range of security experience, and as such is ideal for developers and functional testers who are new to penetration testing.

ZAP allows you to see all the requests you make to a web app and all the responses you receive from it. Among other things, it allows you to see AJAX calls that may not otherwise be outright visible. You can also set breakpoints, which allow you to change the requests and responses in real-time.

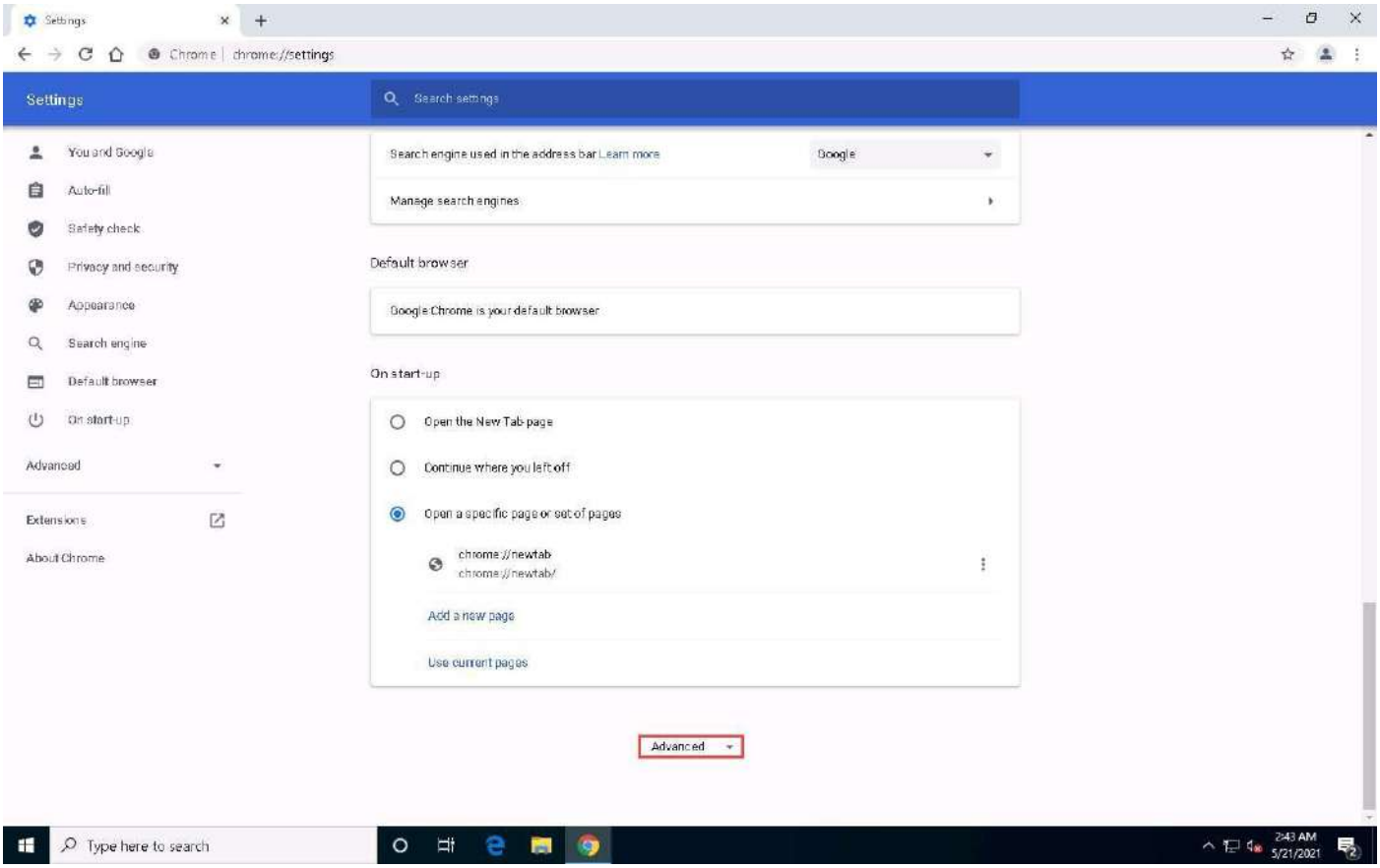
Here, we will hijack a session using ZAP. You will learn how to intercept the traffic of victims' machines with a proxy and how to view all the requests and responses from them.

Before starting this task, we need to configure the proxy settings in the victim's machine, which in this lab will be the **Windows 10** machine.

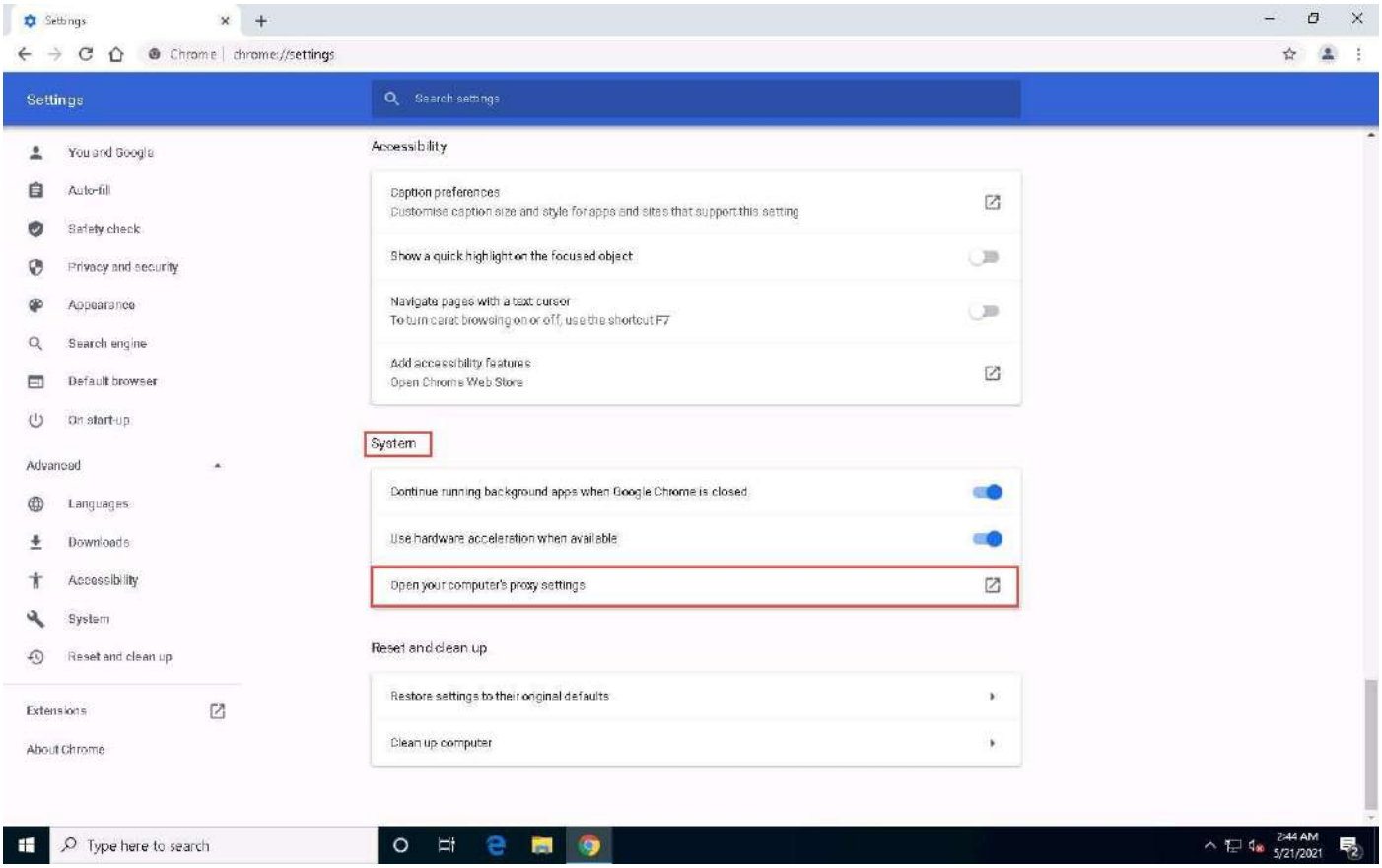
1. In **Windows 10** machine, open any web browser (here, **Google Chrome**), click the **Customize and control Google Chrome** icon, and select **Settings** from the context menu.



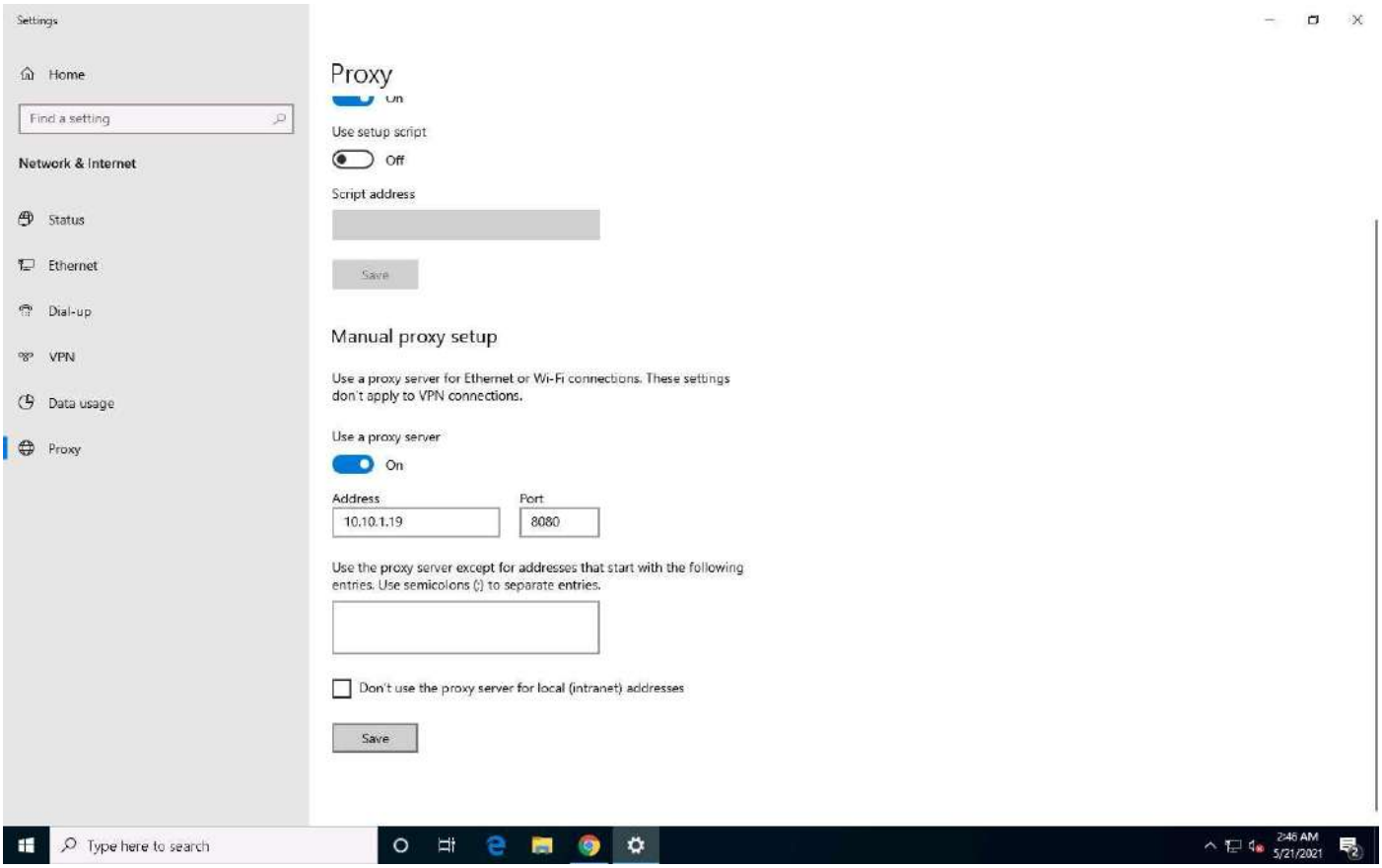
2. On the **Settings** page, scroll down and click the **Advanced** option in the browser.



3. Scroll down to the **System** section and click **Open your computer's proxy settings** to configure a proxy.

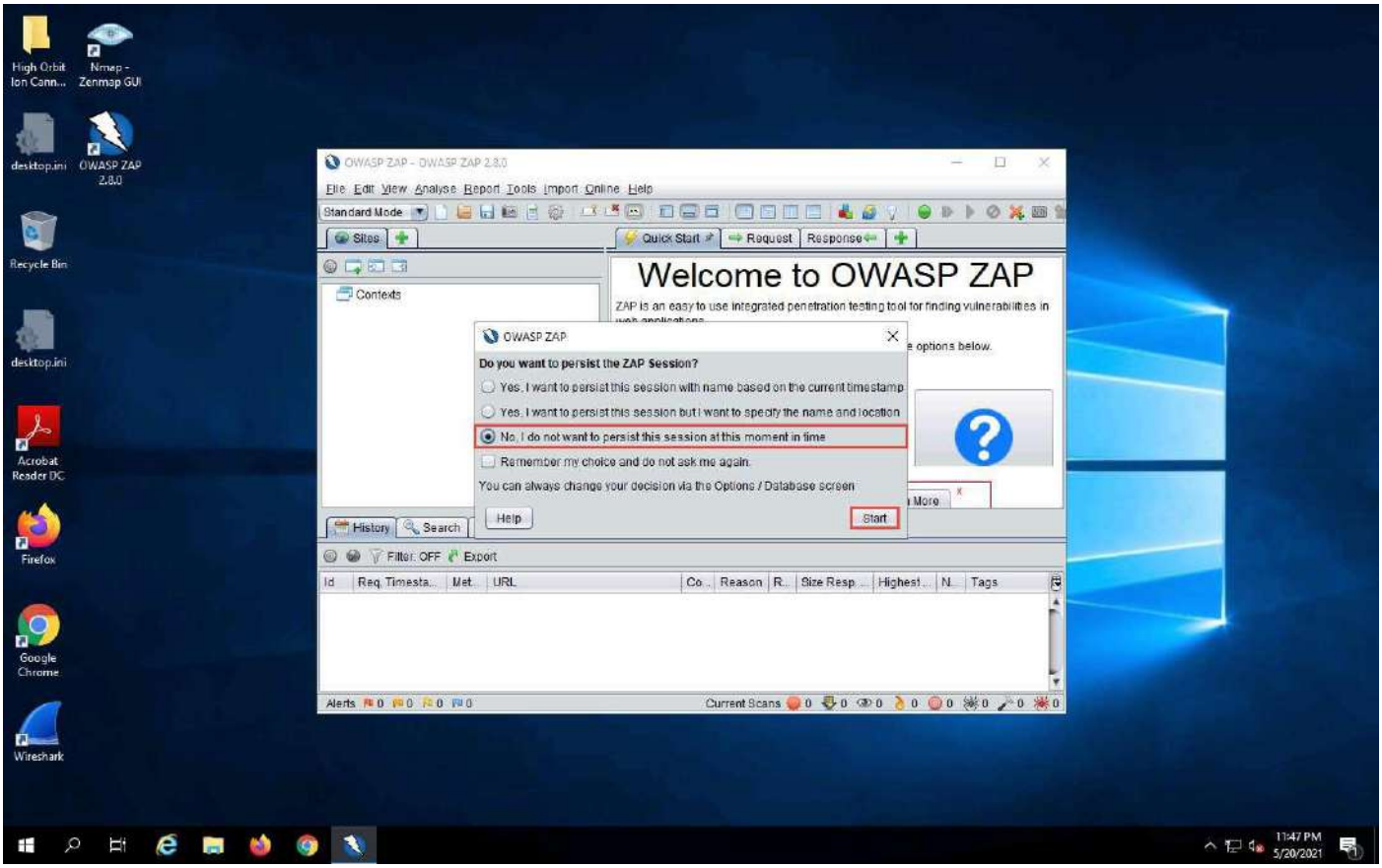


4. A **Settings** window opens, with the **Proxy** settings in the right pane.
5. Under the **Manual proxy setup** section, make the following changes:
    - Under the **Use a proxy server** option, click the **Off** button to switch it **On**.
    - In the **Address** field, type **10.10.1.19** (the IP address of the attacker's machine).
    - In the **Port** field, type **8080**.
    - Click **Save**.



6. After saving, close the **Settings** and **Browser** windows. You have now configured the proxy settings of the victim's machine.
7. Click Windows Server 2019 to switch to the **Windows Server 2019** machine.
8. Double-click the **OWASP ZAP** shortcut on **Desktop** to launch the application.

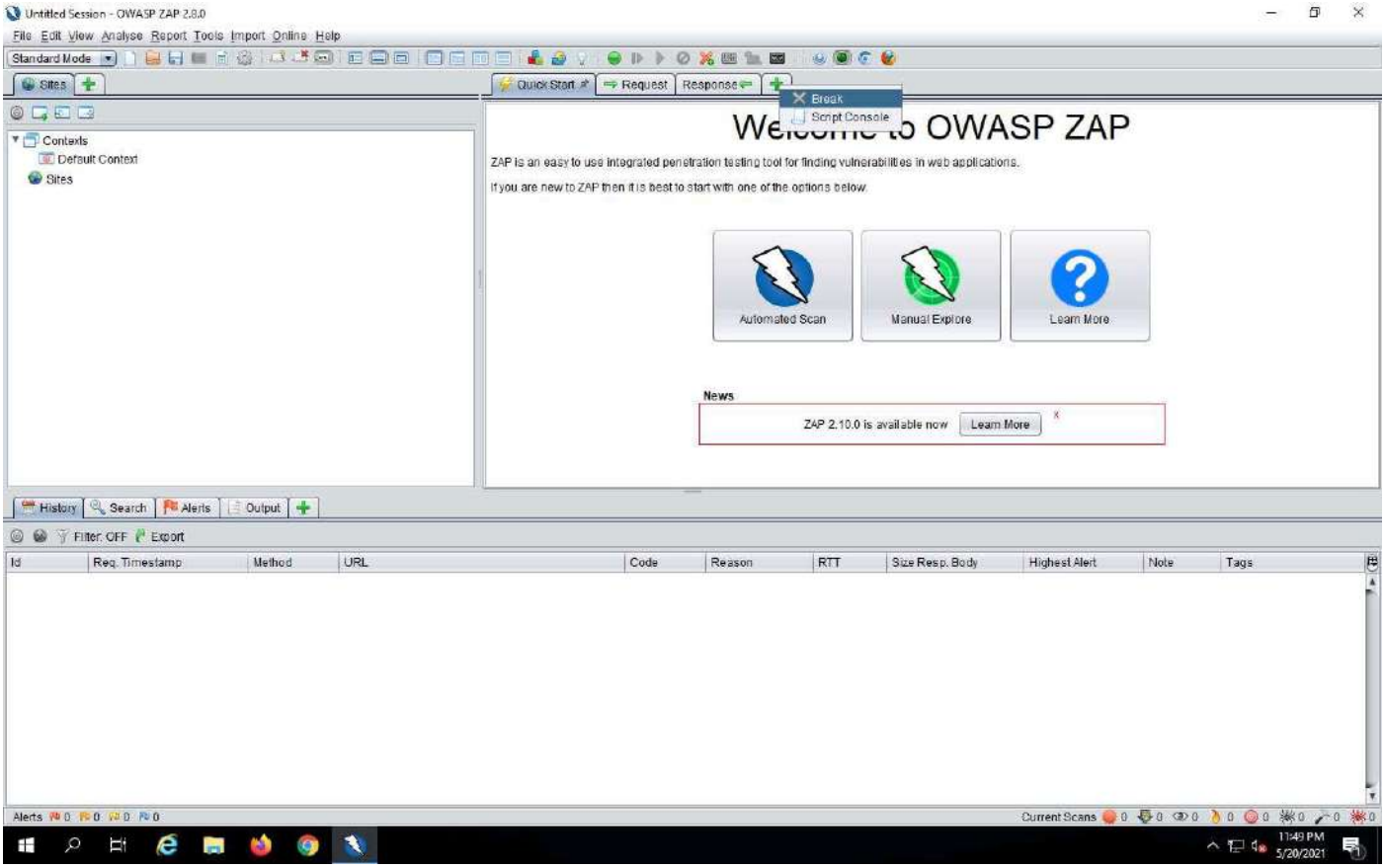
9. **OWASP ZAP** initialized and a prompt that reads **Do you want to persist the ZAP Session?** appears. Select the **No, I do not want to persist this session at this moment in time** radio button and click **Start**.



10. The **OWASP ZAP** main window appears. Click on the "**+**" icon in the right pane and select **Break** from the options.

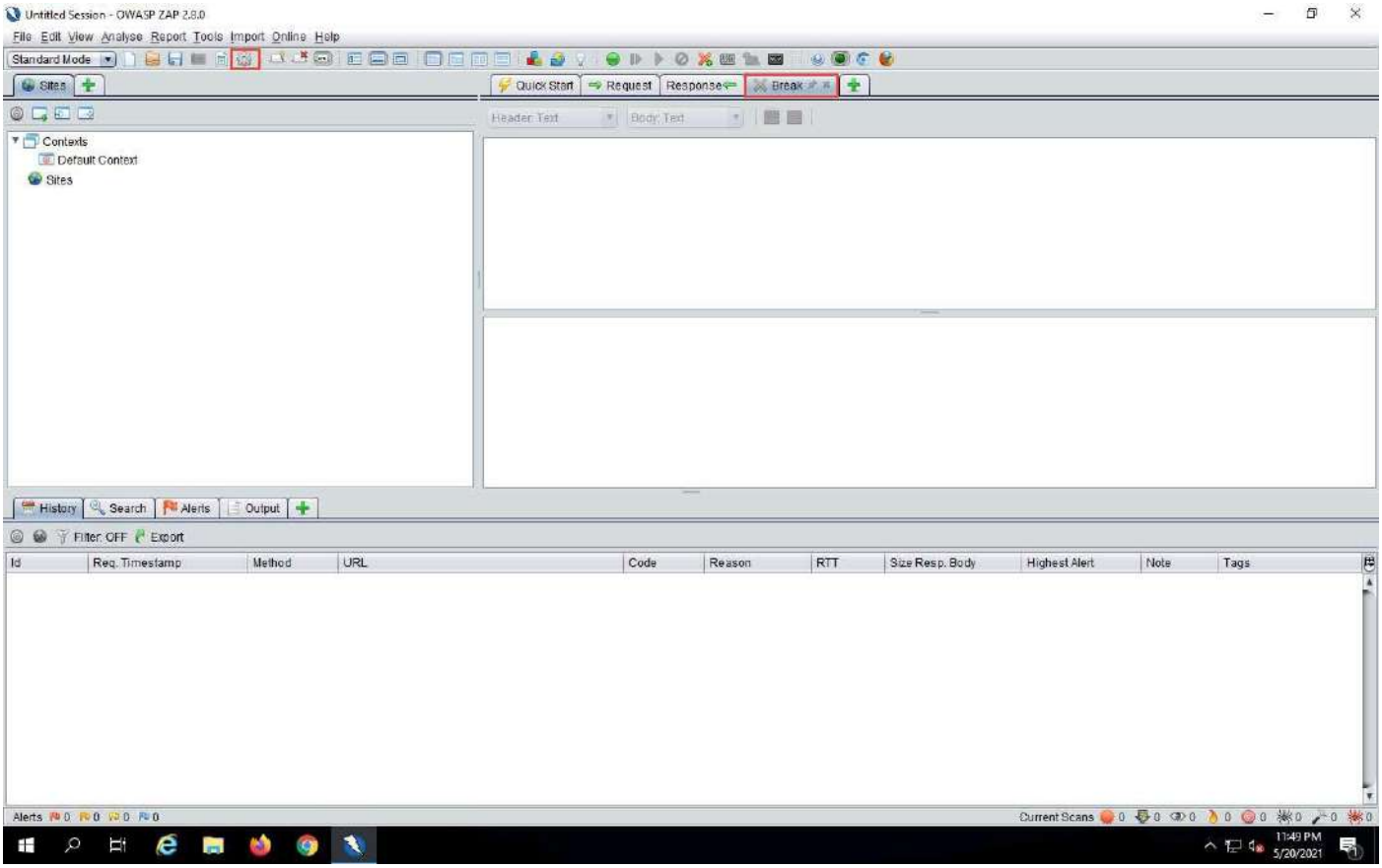
The **Break** tab allows you to modify a response or request when ZAP has caught it. It also allows you to modify certain elements that you cannot modify through your browser, including:

- The header
- Hidden fields
- Disabled fields
- Fields that use JavaScript to filter out illegal characters

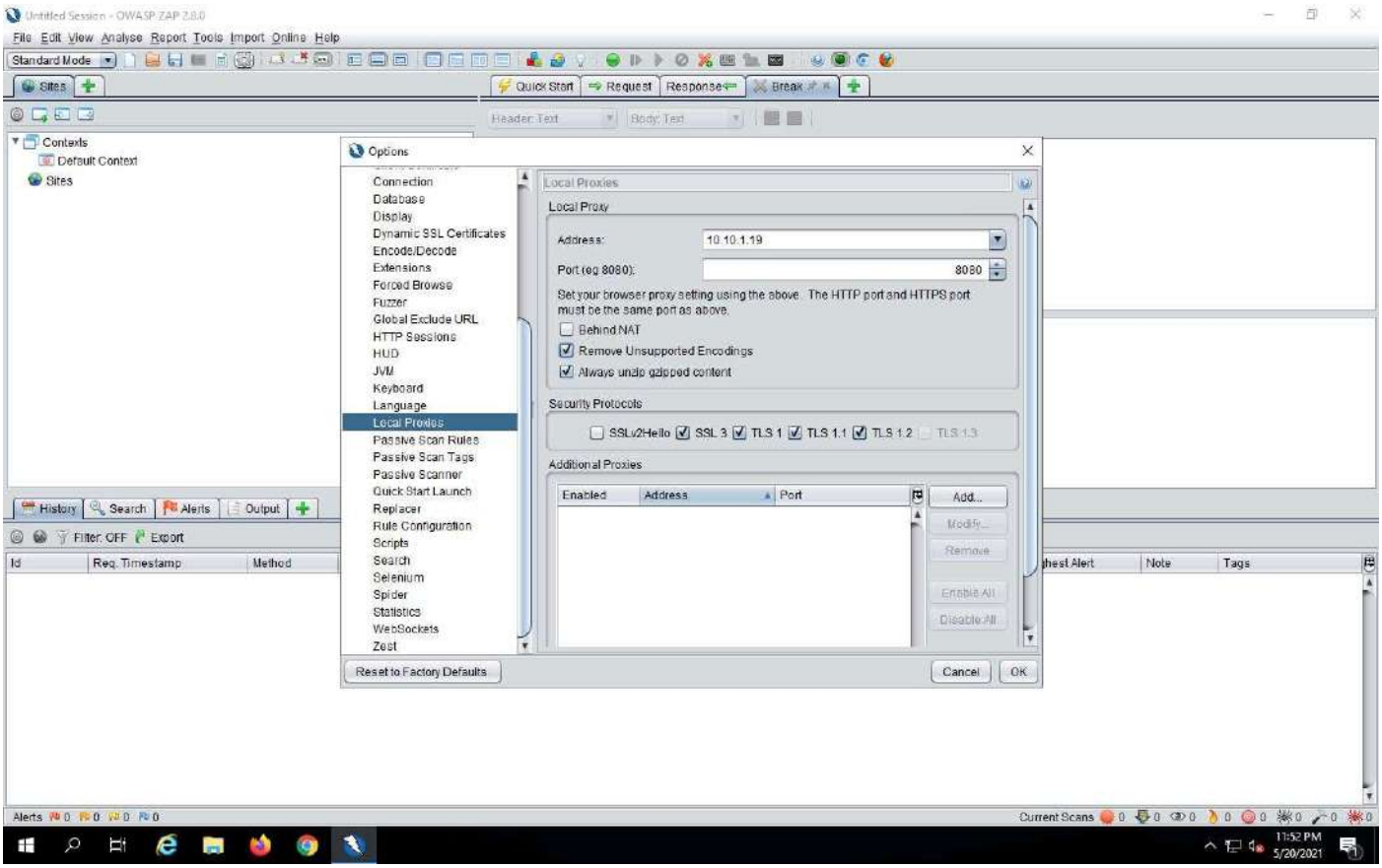


11. The **Break** tab is added to your **OWASP ZAP** window.

12. To configure ZAP as a proxy, click the **Settings** icon from the toolbar.

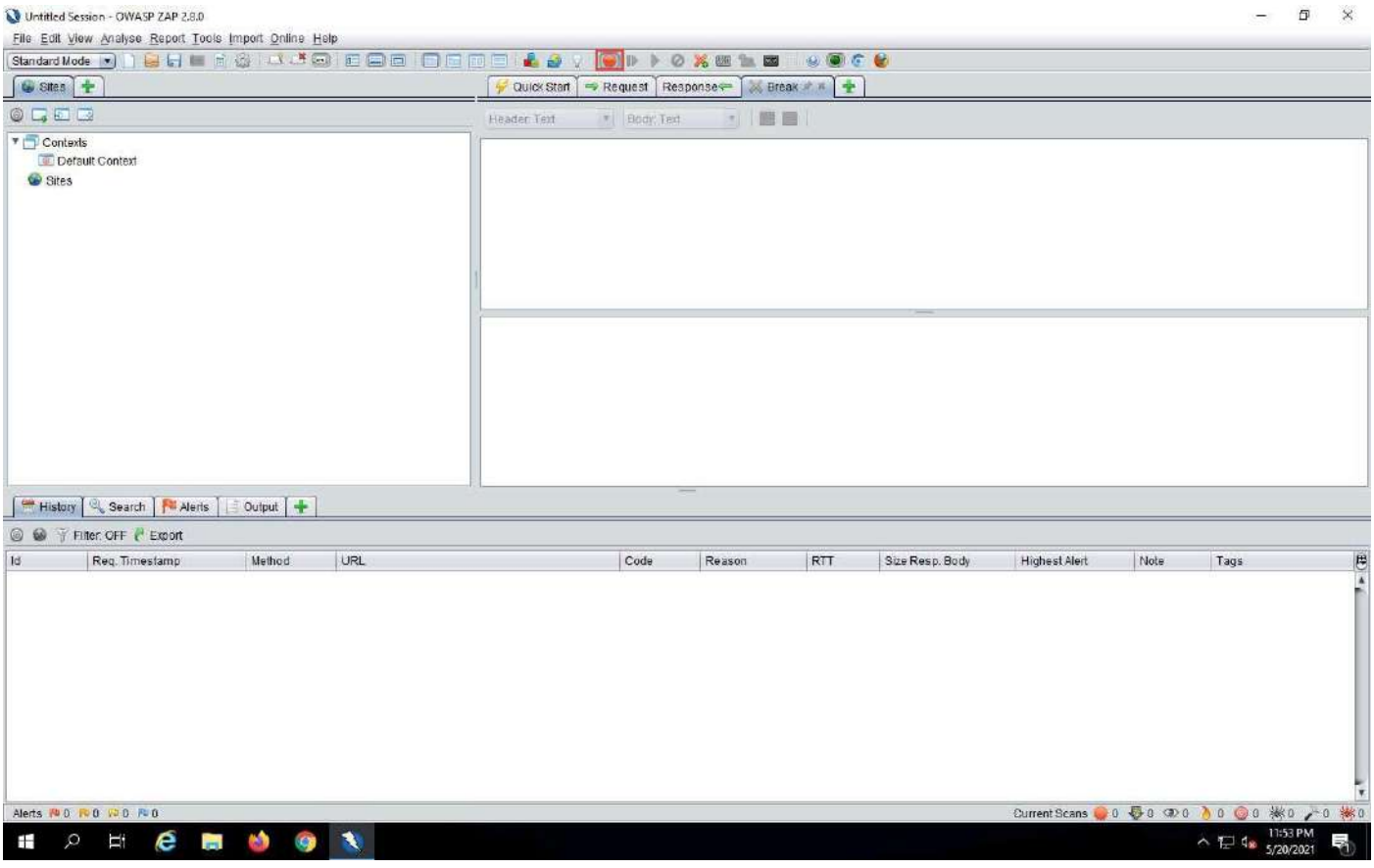


13. In the **Options** window, click **Local Proxies** in the left pane. In the right pane, under the **Local Proxy** section, type **10.10.1.19** (the IP address of the **Windows Server 2019** machine) in the **Address** field and set the **Port** value to the default, **8080**; click **OK**.

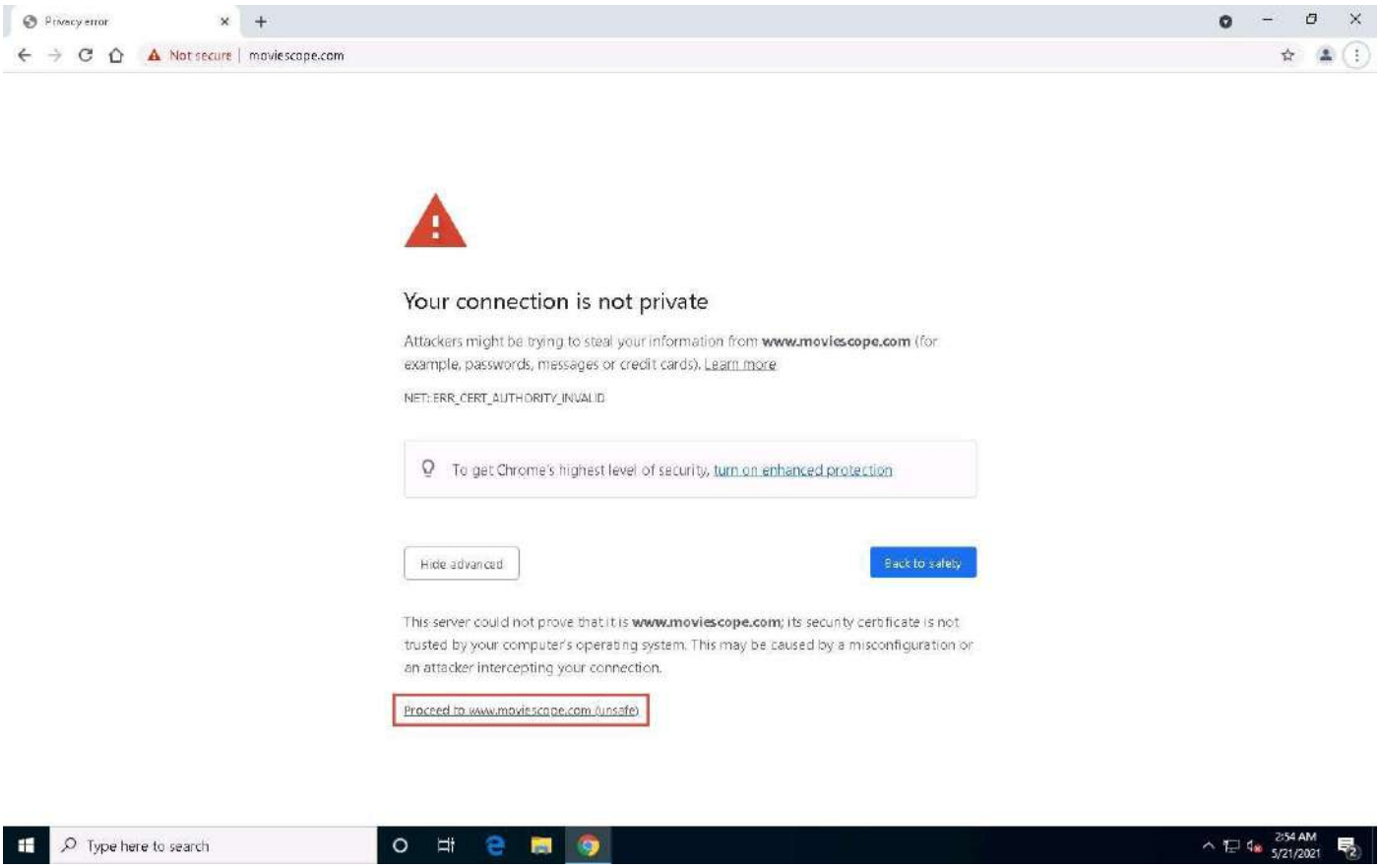


14. Click the **Set break on all requests and responses** icon on the main ZAP toolbar. This button sets and unsets a global breakpoint that will trap and display the next response or request from the victim's machine in the **Break** tab.

The **Set break on all requests and responses** icon turns automatically from green to red.

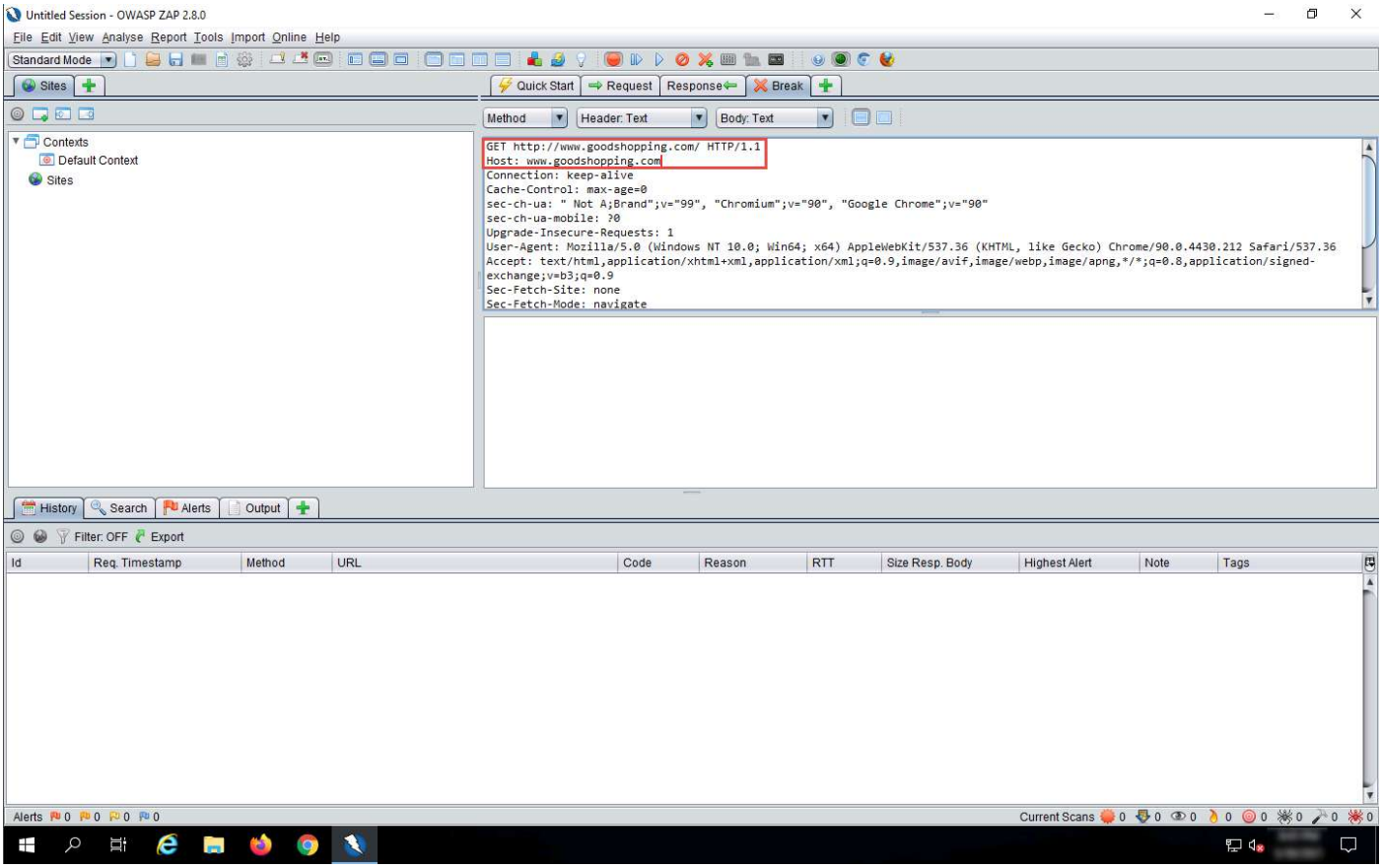


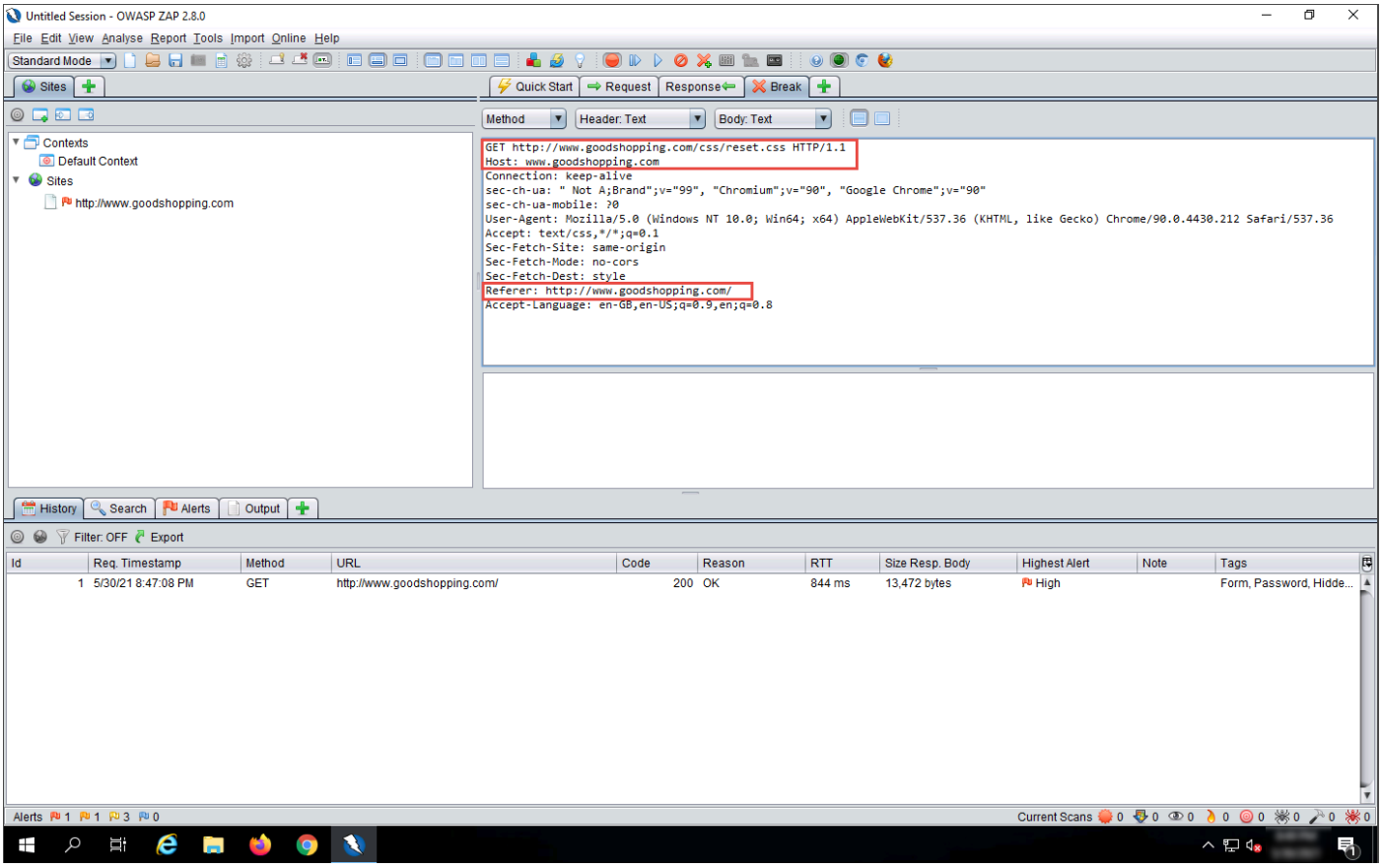
15. Now, click Windows 10 to switch back to the victim's machine (**Windows 10**) and launch the same browser in which you configured the proxy settings. In this lab, we have configured the **Google Chrome** browser.
16. Place your mouse cursor in the address bar, click www.moviescope.com and press **Enter**.
17. A message appears, stating that **Your connection is not private**. Click the **Advanced** button.
18. On the next page, click **Proceed to www.moviescope.com (unsafe)** to open the website.



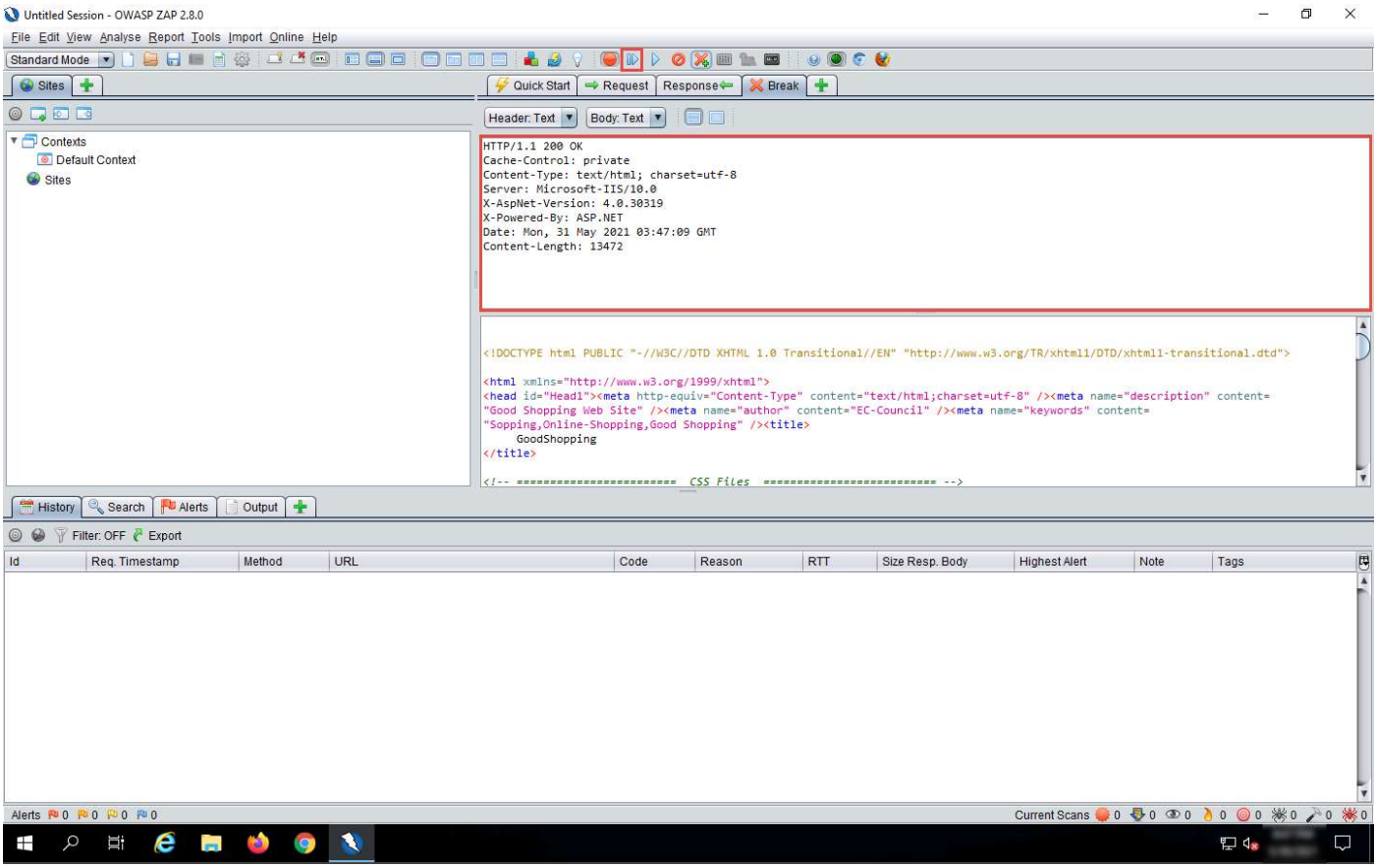
19. Now, click Windows Server 2019 to switch back to the attacker machine (**Windows Server 2019**) and observe that **OWASP ZAP** has begun to capture the requests of the victim's machine.
20. In Steps **16-18**, we visited **www.moviescope.com** in the victim's browser. A **HTTP response** appears in the **Break** tab.
21. Modify **www.moviescope.com** to **www.goodshopping.com** in all the captured GET requests. Once you have modified the GET requests, click the **Submit and step to next request or response** icon on the toolbar to forward the traffic to the victim's machine.

If you find any URL starting with **https**, modify it to **http**.





22. A **HTTP response** appears; click the **Submit and step to next request or response** icon on the toolbar.



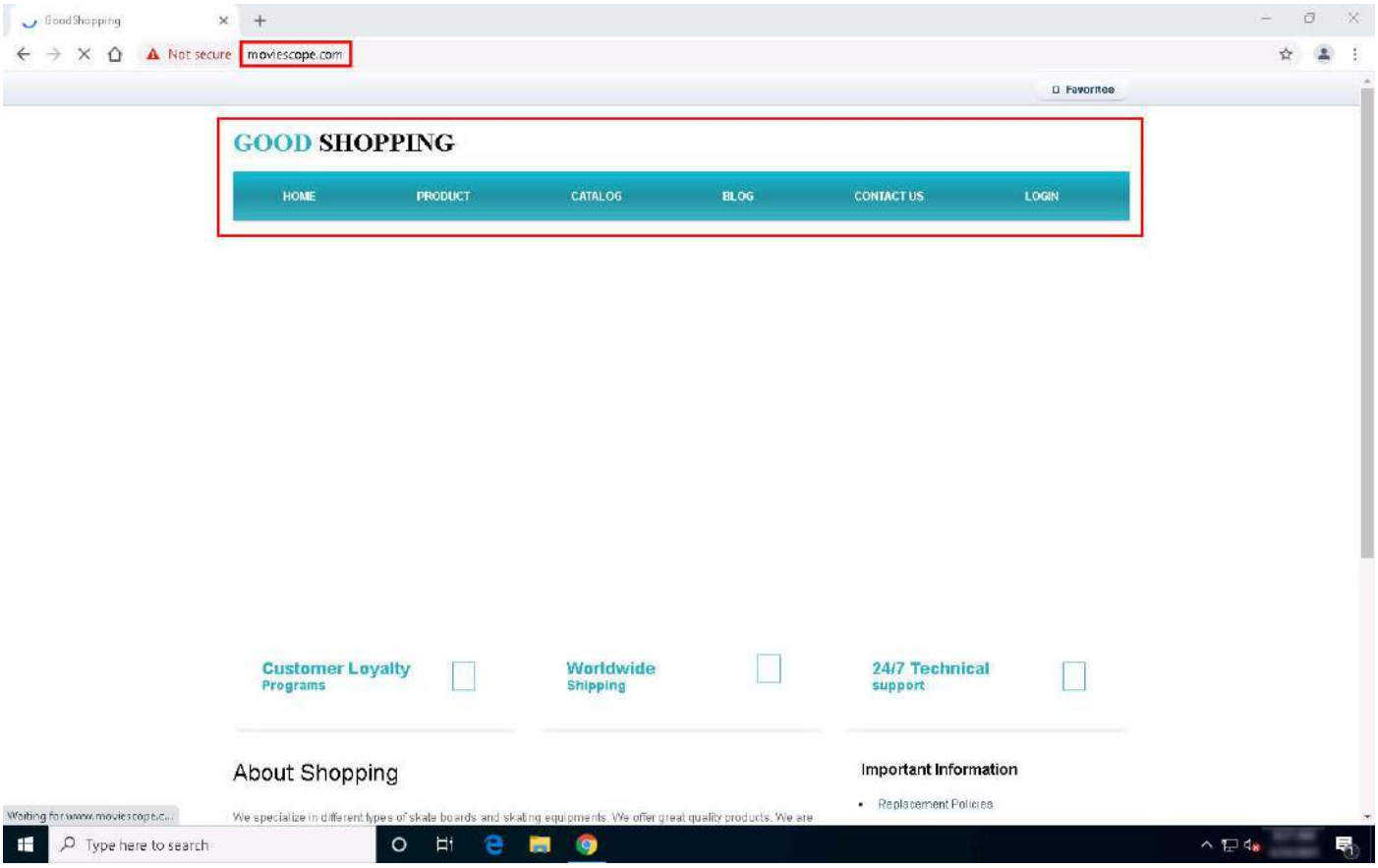
23. Modify every **HTTP** request captured by **OWASP ZAP** until you see the **www.goodshopping.com** page in the victim's machine.

You will need to switch back and forth from the victim's machine to see the browser status while you do this.

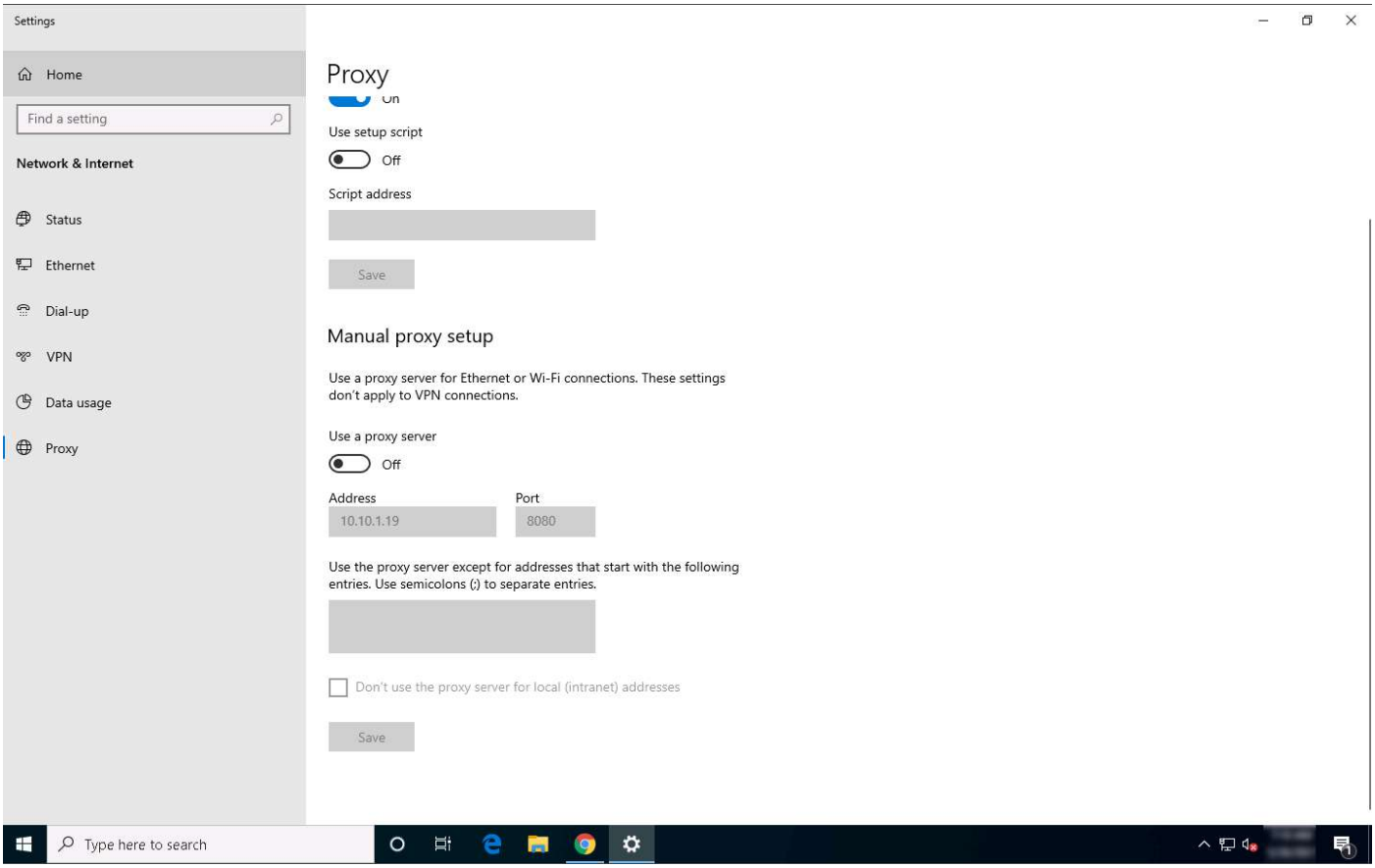
24. Now, click on Windows 10 to switch to the victim's machine (**Windows 10**); the browser displays the website that the attacker wants the victim's machine to see (in this example, **www.goodshopping.com**).

It takes multiple iterations to open the Good Shopping site in the victim's machine.

25. The victim has navigated to **www.moviescope.com**, but now sees **www.goodshopping.com**; while the address bar displays **www.moviescope.com**, the window displays **www.goodshopping.com**.



26. Now, we shall change the proxy settings back to the default settings. To do so, perform **Steps 1-3** again.
27. In the **Settings** window, under the **Manual proxy setup** section in the right pane, click the **On** button to toggle it back to **Off**, as shown in the screenshot.



28. This concludes the demonstration of performing session hijacking using ZAP.
29. Close all open windows and document all the acquired information.

Lab 7: Detect Session Hijacking Attempts using Manual Method

Lab Scenario

Session hijacking is very dangerous; it places the victim at risk of identity theft, fraud, and loss of sensitive information. All networks that use TCP/IP are vulnerable to different types of hijacking attacks. Moreover, these kinds of attacks are very difficult to detect, and often go unnoticed unless the attacker causes severe damage. However, following best practices can protect against session hijacking attacks.

It is very important that you have the required knowledge to detect session hijacking attacks and protect your organization's system against them. Fortunately, there are various tools available that can help you to detect session hijacking attacks such as packet sniffers, IDSs, and SIEMs.

Lab Objectives

- Detect Session Hijacking using Wireshark

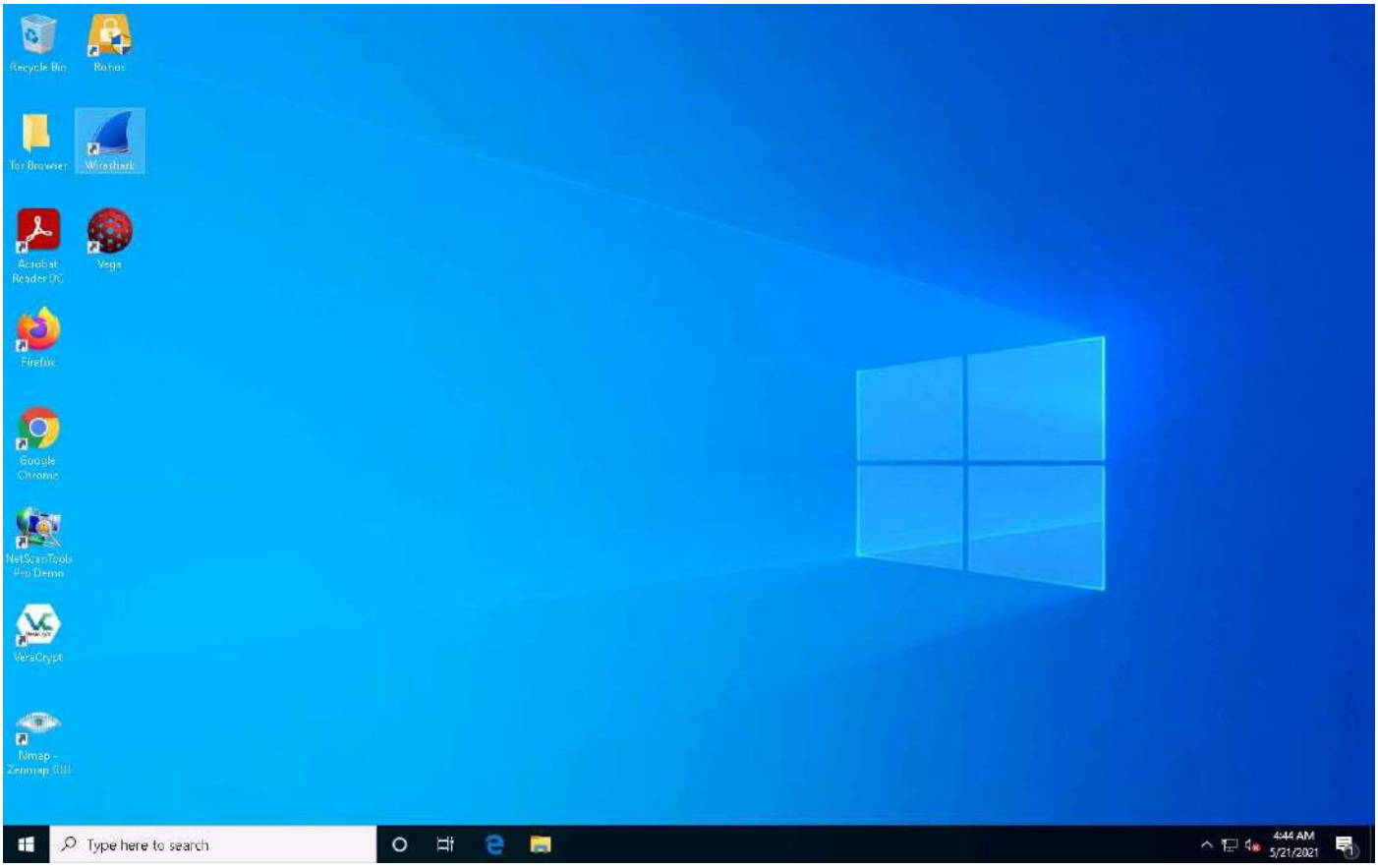
Task 1: Detect Session Hijacking using Wireshark

Wireshark allows you to capture and interactively browse the traffic running on a network. The tool uses WinPcap to capture packets, and so is only able to capture packets on networks that are supported by WinPcap. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks. Security professionals can use Wireshark to monitor and detect session hijacking attempts.

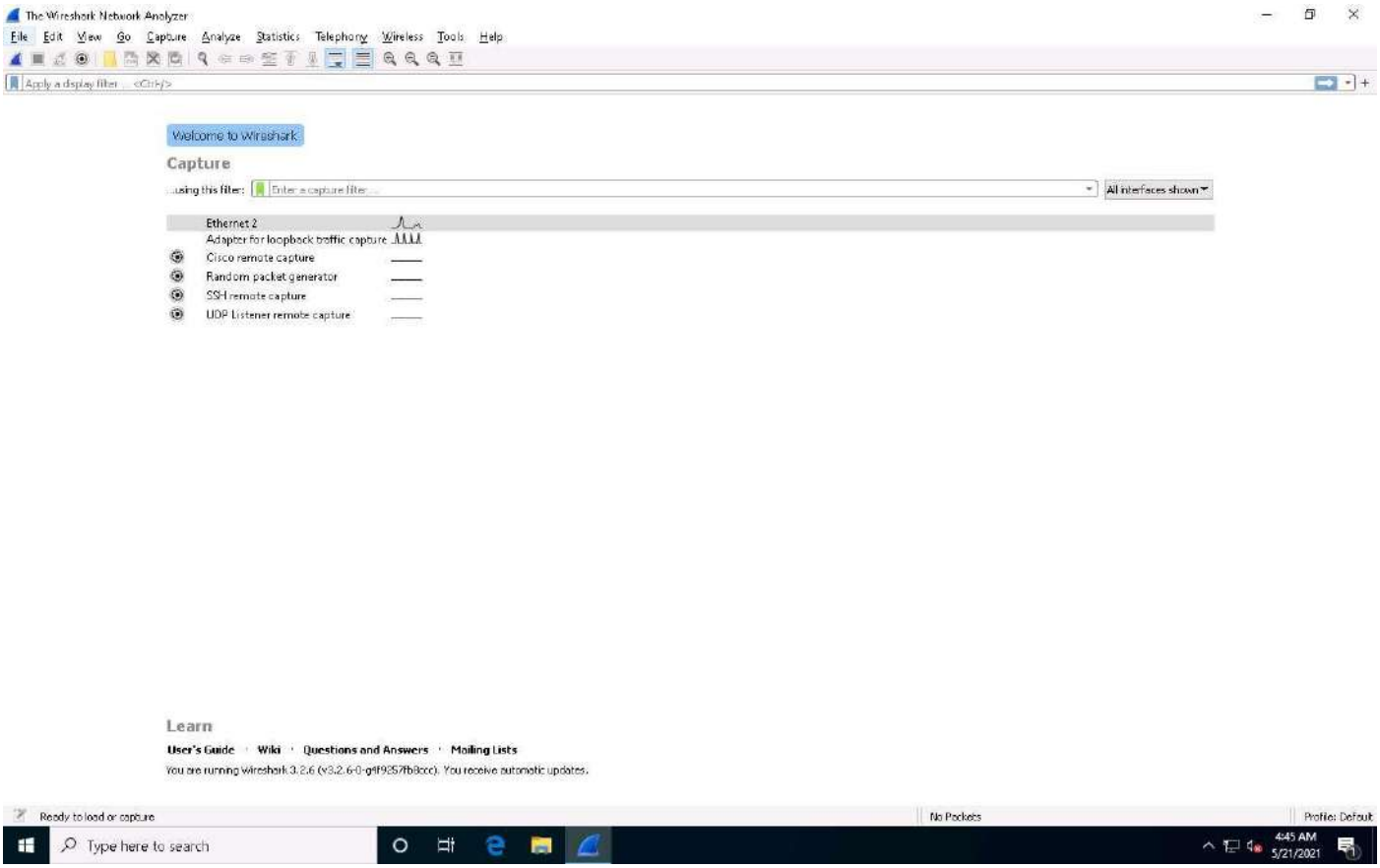
Here, we will use the Wireshark tool to detect session hijacking attacks manually on the target system.

We will use the **Parrot Security** (**10.10.1.13**) machine to carry out a session hijacking attack on the **Windows 10** (**10.10.1.10**) machine.

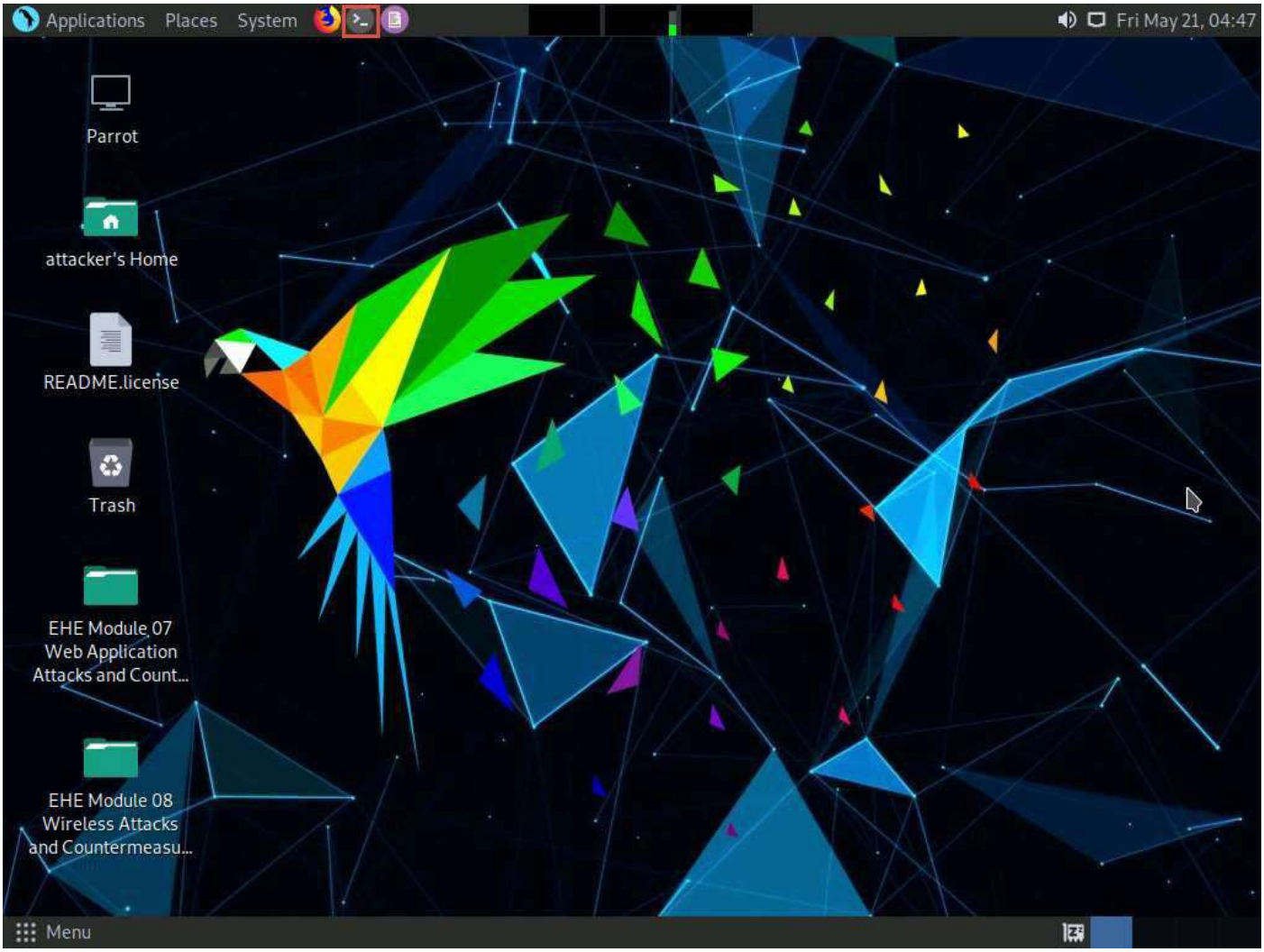
1. Click Windows 10 to switch to the **Windows 10** machine. In the **Desktop**, double-click **Wireshark** shortcut.



2. **The Wireshark Network Analyzer** window opens. Double-click the primary network interface (in this case, **Ethernet 2**) to start capturing network traffic.



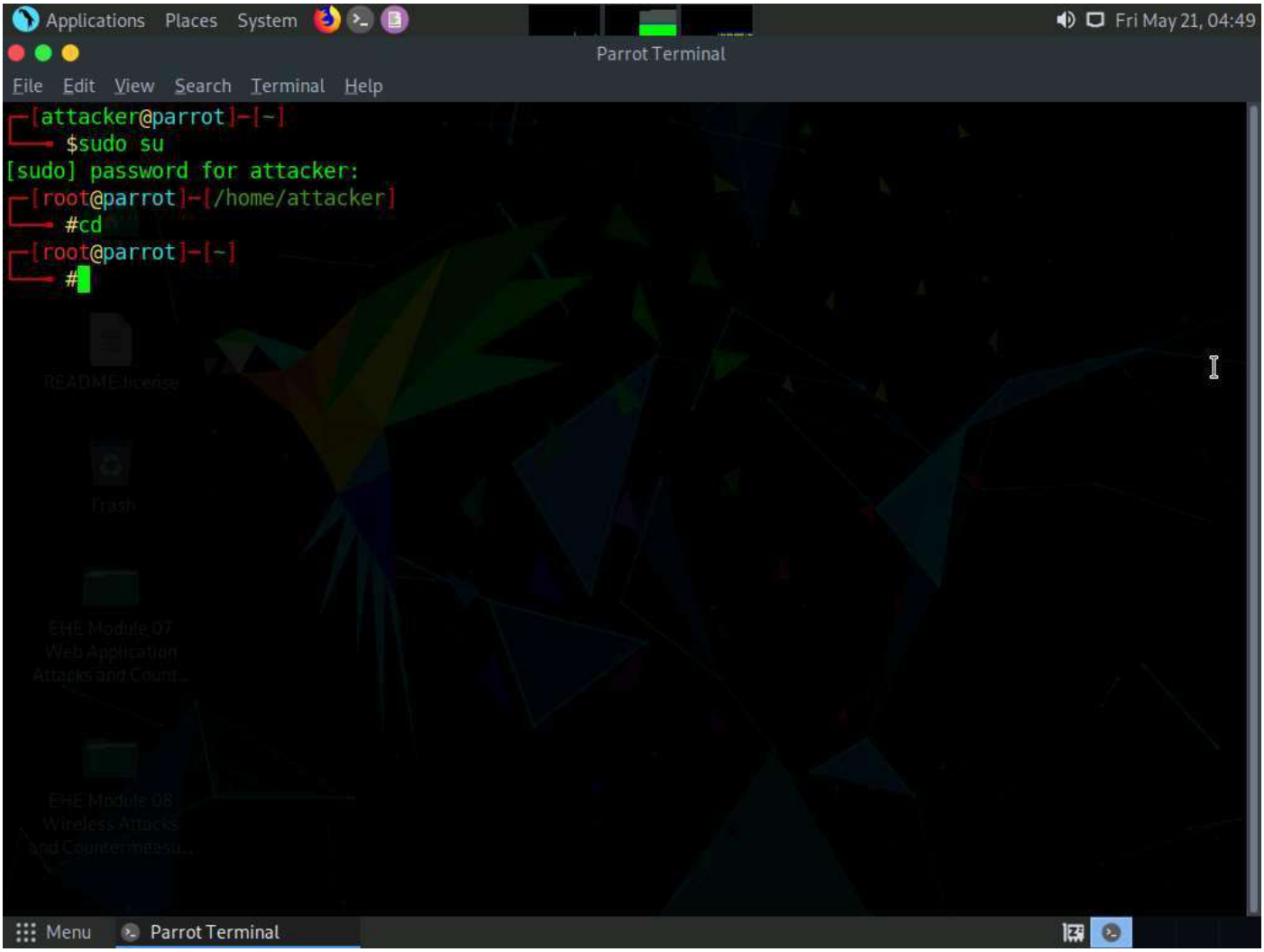
3. **Wireshark** starts capturing network traffic. Leave it running.
4. Now, we shall launch a session hijacking attack on the target machine (**Windows 10**) using **bettercap**.
5. Click Parrot Security to switch to the **Parrot Security** machine.
6. Click the **MATE Terminal** icon at the top of 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**.

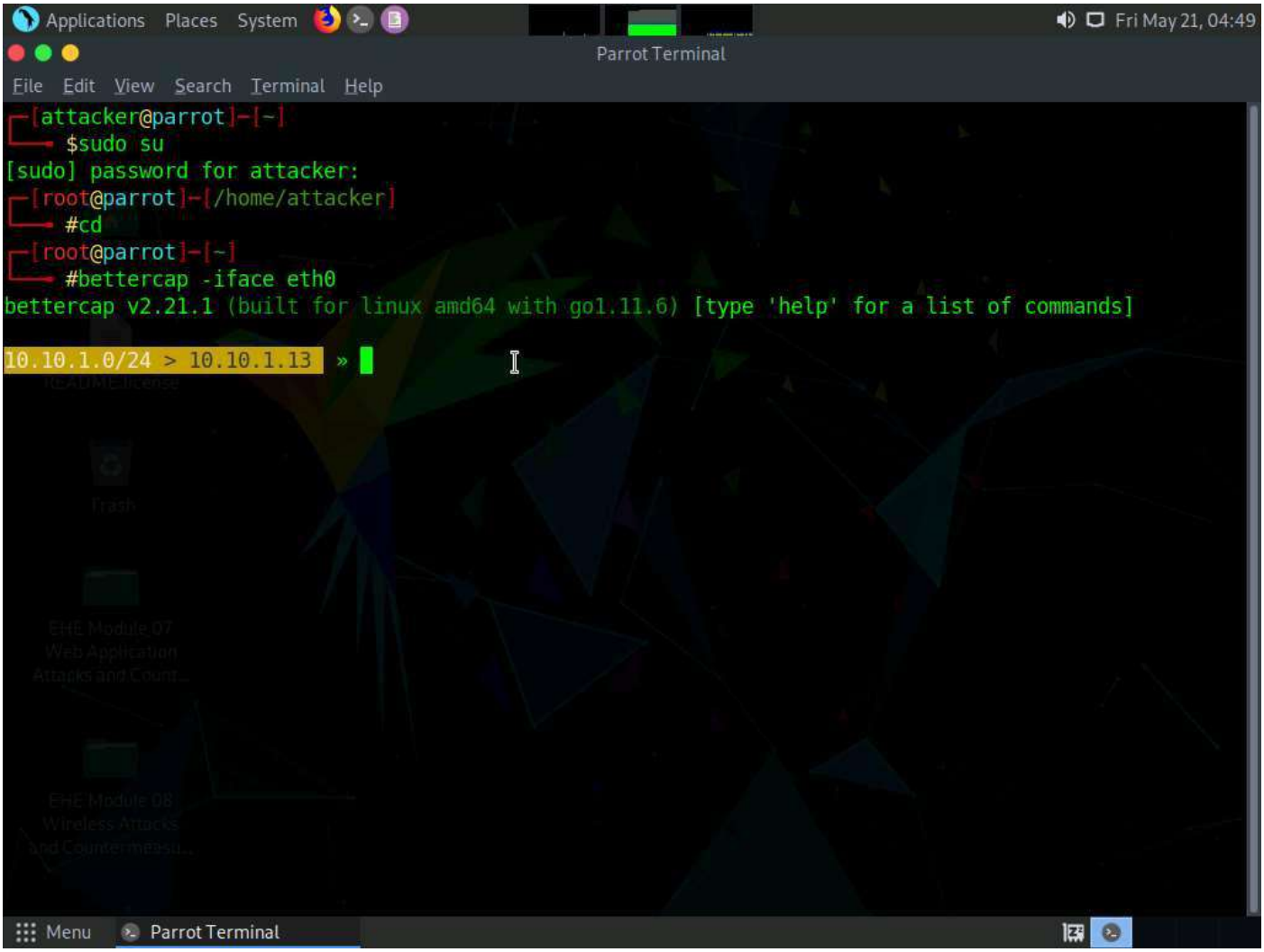
The password that you type will not be visible.

9. Now, type **cd** and press **Enter** to jump to the root directory.



10. In the terminal window, type **bettercap -iface eth0** and press **Enter** to set the network interface.

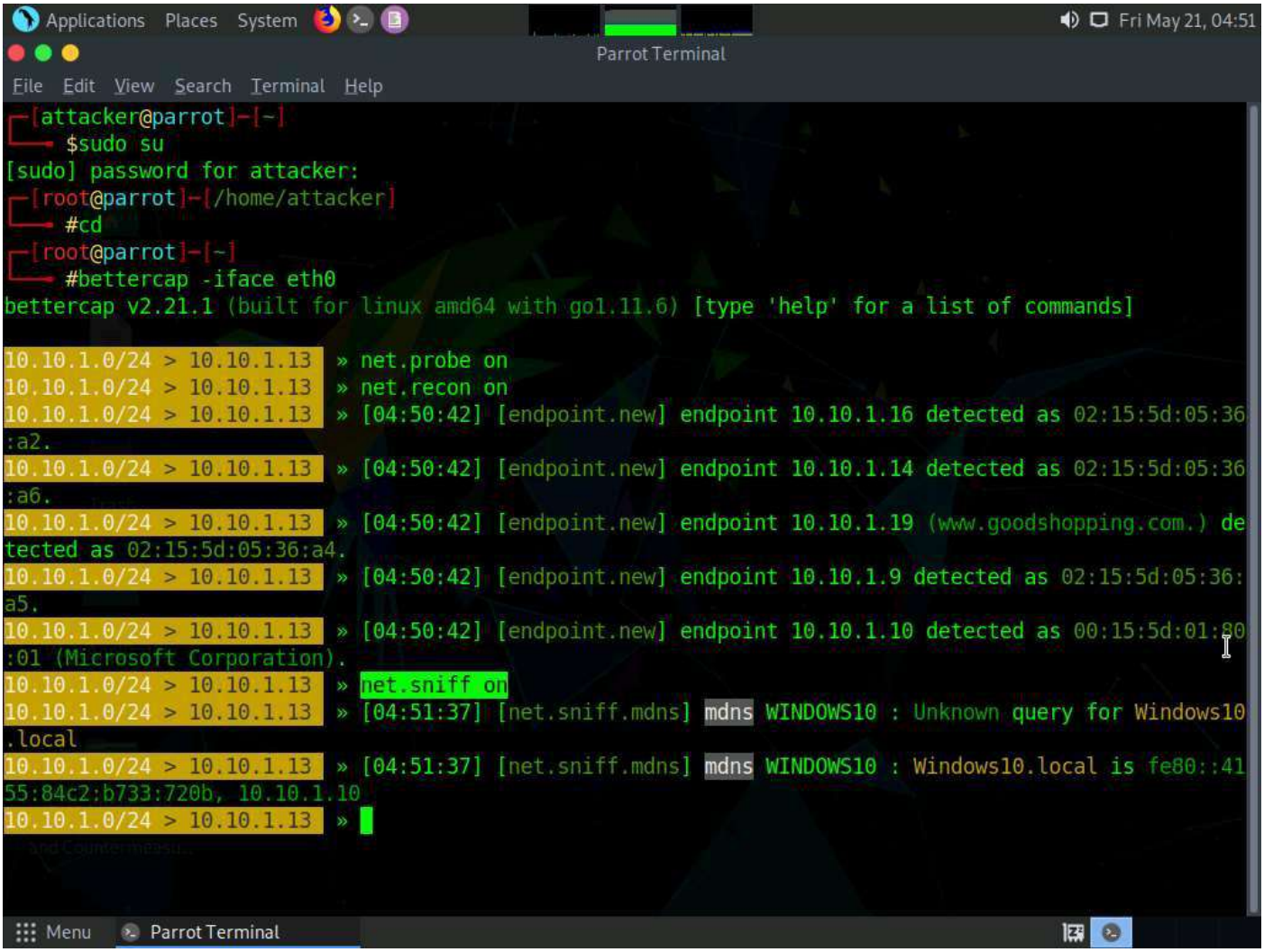
-iface: specifies the interface to bind to (in this example, **eth0**).



11. Type **net.probe on** and press **Enter**. This module will send different types of probe packets to each IP in the current subnet for the **net.recon** module to detect them.
12. Type **net.recon on** and press **Enter**. This module is responsible for periodically reading the system ARP table to detect new hosts on the network.

The net.recon module displays the detected active IP addresses in the network. In real-time, this module will start sniffing network packets.

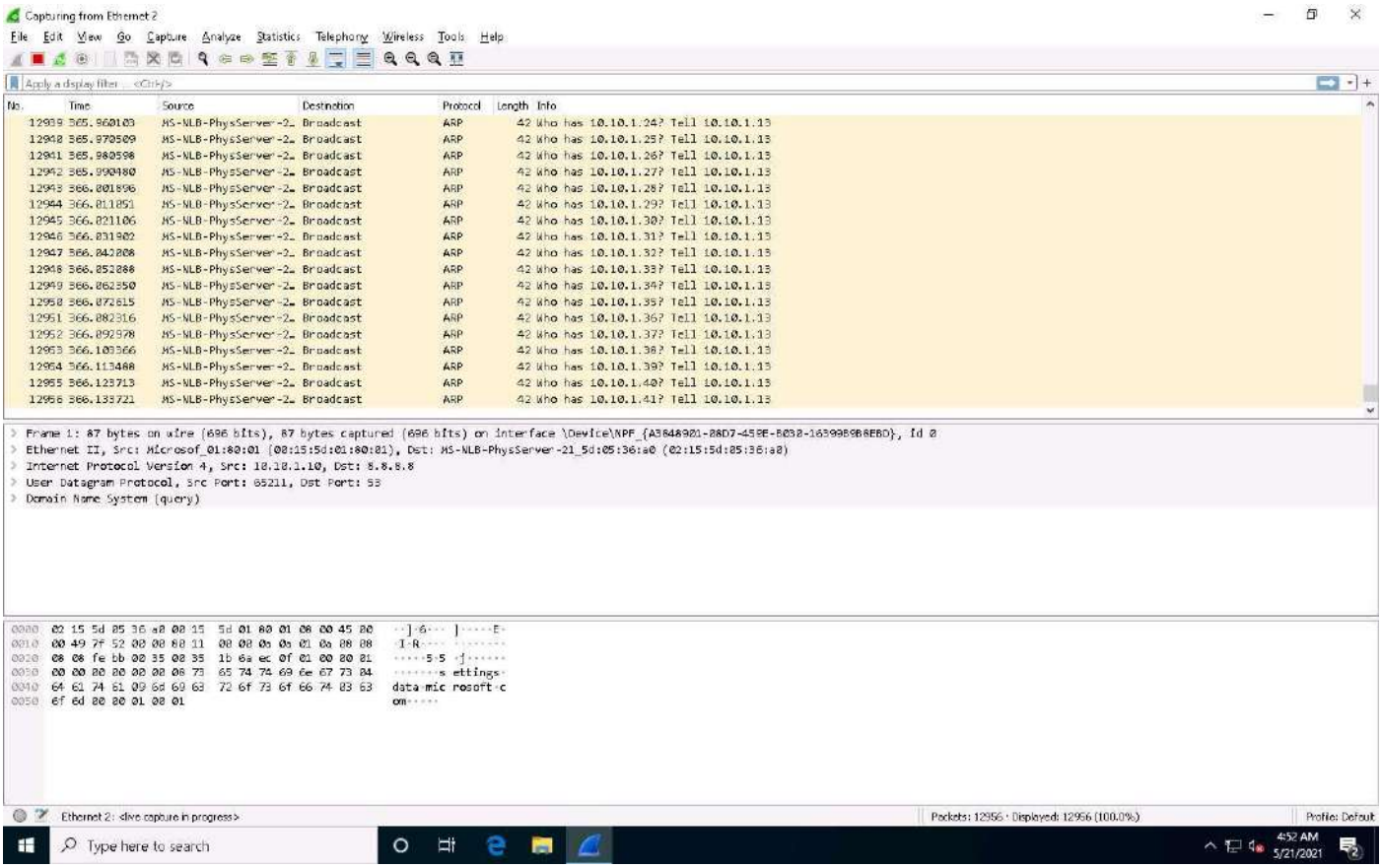
13. Type **net.sniff on** and press **Enter**. This module is responsible for performing sniffing on the network.
14. You can observe that bettercap starts sniffing network traffic on different machines in the network, as shown in the screenshot.



15. Click Windows 10 to switch back to the **Windows 10** machine and observe the huge number of **ARP packets** captured by the **Wireshark**, as shown in the screenshot.

bettercap sends several ARP broadcast requests to the hosts (or potentially active hosts). A high number of ARP requests indicates that the system at **10.10.1.13** (the attacker's system in this task) is acting as a client for all the IP addresses in the subnet, which means that all the packets from the victim node (in this case, **10.10.1.10**) will first go to the host system (**10.10.1.13**), and then the gateway. Similarly, any packet destined for the victim node is first forwarded from the gateway to the host system, and then from the host system to the victim node.

more...



16. This concludes the demonstration of how to detect a session hijacking attack using Wireshark.
17. Close all open windows and document all the acquired information.

Module 07: Web Application Attacks and Countermeasures

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.

A web application is a software application running on a web browser that allows a web user to submit data to and retrieve it from a database over the Internet or within an intranet. Web applications have helped to make web pages dynamic as they allow users to communicate with servers using server-side scripts. They allow users to perform specific tasks such as searching, sending emails, connecting with friends, online shopping, and tracking and tracing.

Objective

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

- Footprint a web server using various information-gathering tools and inbuilt commands
- Crack remote passwords
- Exploiting parameter tampering vulnerability
- Performing a SQL injection attack on a MSSQL database
- Extracting basic SQL injection flaws and vulnerabilities
- Detecting SQL injection vulnerabilities

Overview of Web Application

Web applications provide an interface between end-users and web servers through a set of web pages generated at the server end or that contain script code to be executed dynamically in a client's Web browser.

Web applications run on web browsers and use a group of server-side scripts (such as ASP and PHP) and client-side scripts (such as HTML and JavaScript) to execute the application. The working of a web application depends on its architecture, which includes the hardware and software that performs tasks such as reading the request, searching, gathering, and displaying the required data.

Lab Tasks

We will use numerous tools and techniques to hack a target web application. Recommended labs that will assist you in learning various web application attack techniques include:

1. Perform a web server attack to crack FTP credentials
    a. Crack FTP credentials using a dictionary attack
2. Perform a web application attack to compromise the security of web applications to steal sensitive information
    a. Perform parameter tampering using Burp Suite
3. Perform SQL injection attacks on a target web application to manipulate the backend database
    a. Perform an SQL injection attack against MSSQL to extract databases using sqlmap
4. Detect SQL injection vulnerabilities using SQL injection detection tools
    a. Detect SQL injection vulnerabilities using DSSS

Lab 7-1: Perform a Web Server Attack to Crack FTP Credentials

Lab Scenario

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.

We 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

Task 1: Crack FTP Credentials using a Dictionary Attack

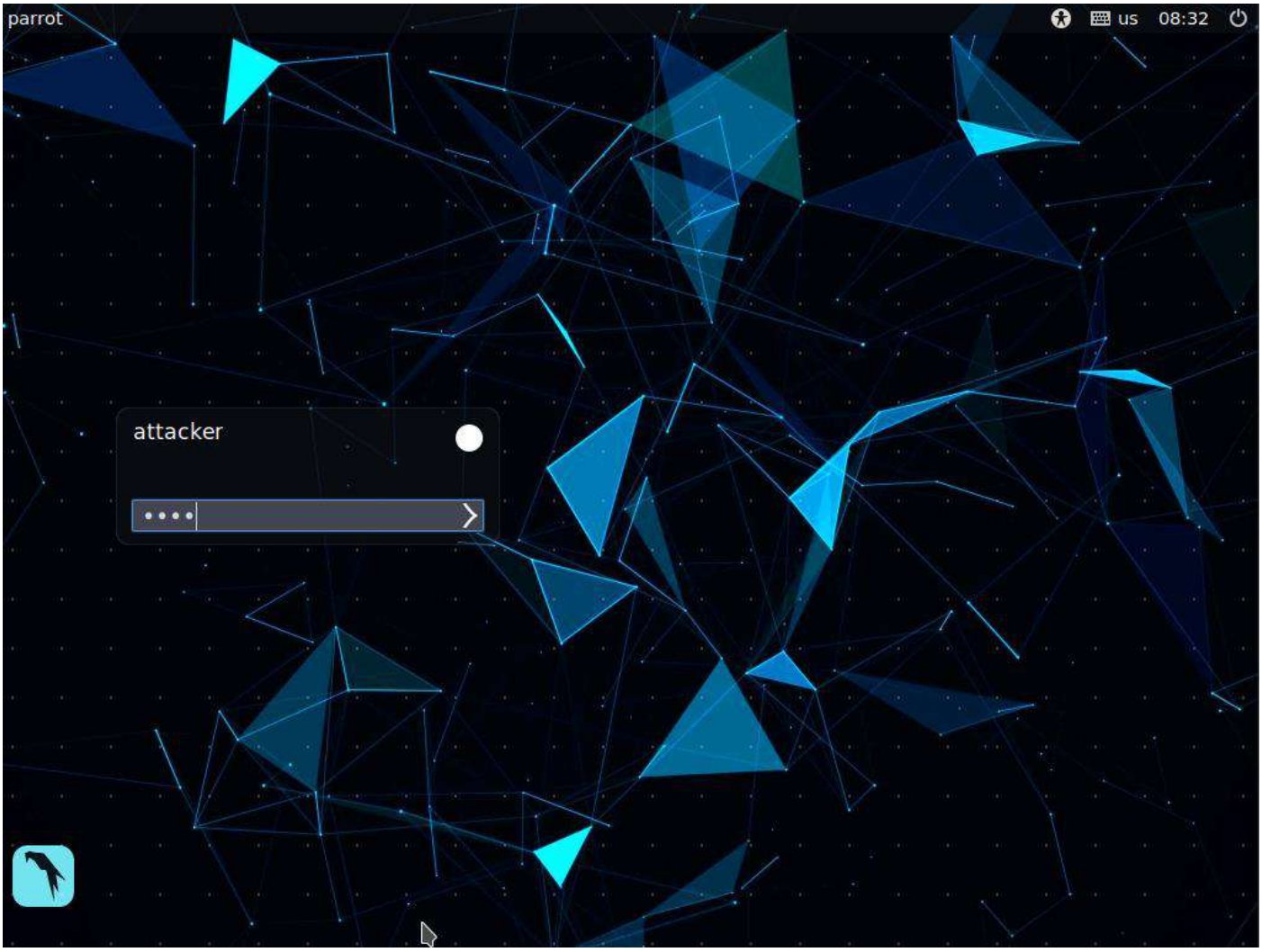
A dictionary or wordlist contains thousands of words that are used by password cracking tools to break into a password-protected system. An attacker may either manually crack a password by guessing it or use automated tools and techniques such as the dictionary method. Most password cracking techniques 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 Parrot Security to switch to the **Parrot Security** machine.
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.

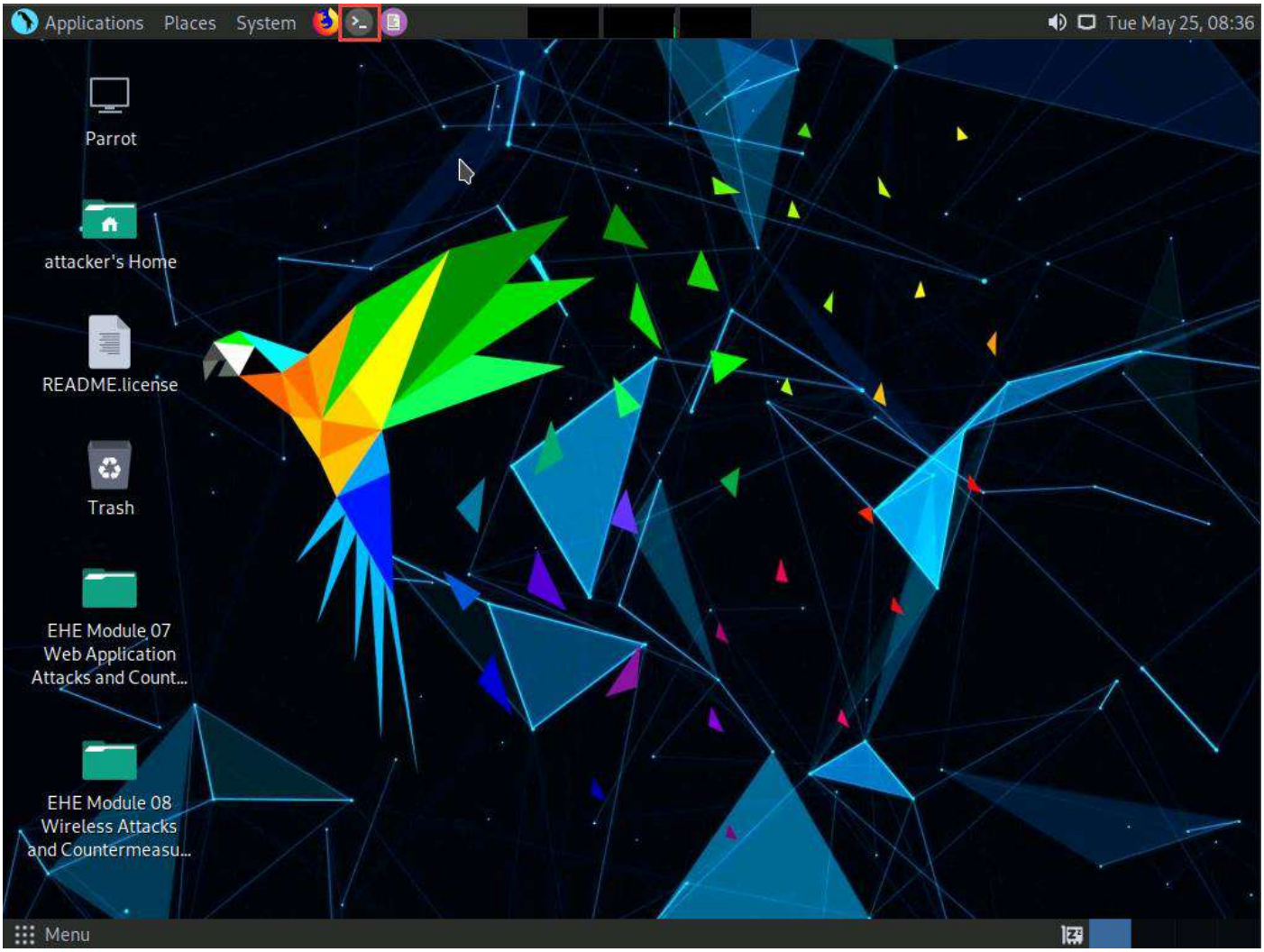
If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

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



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

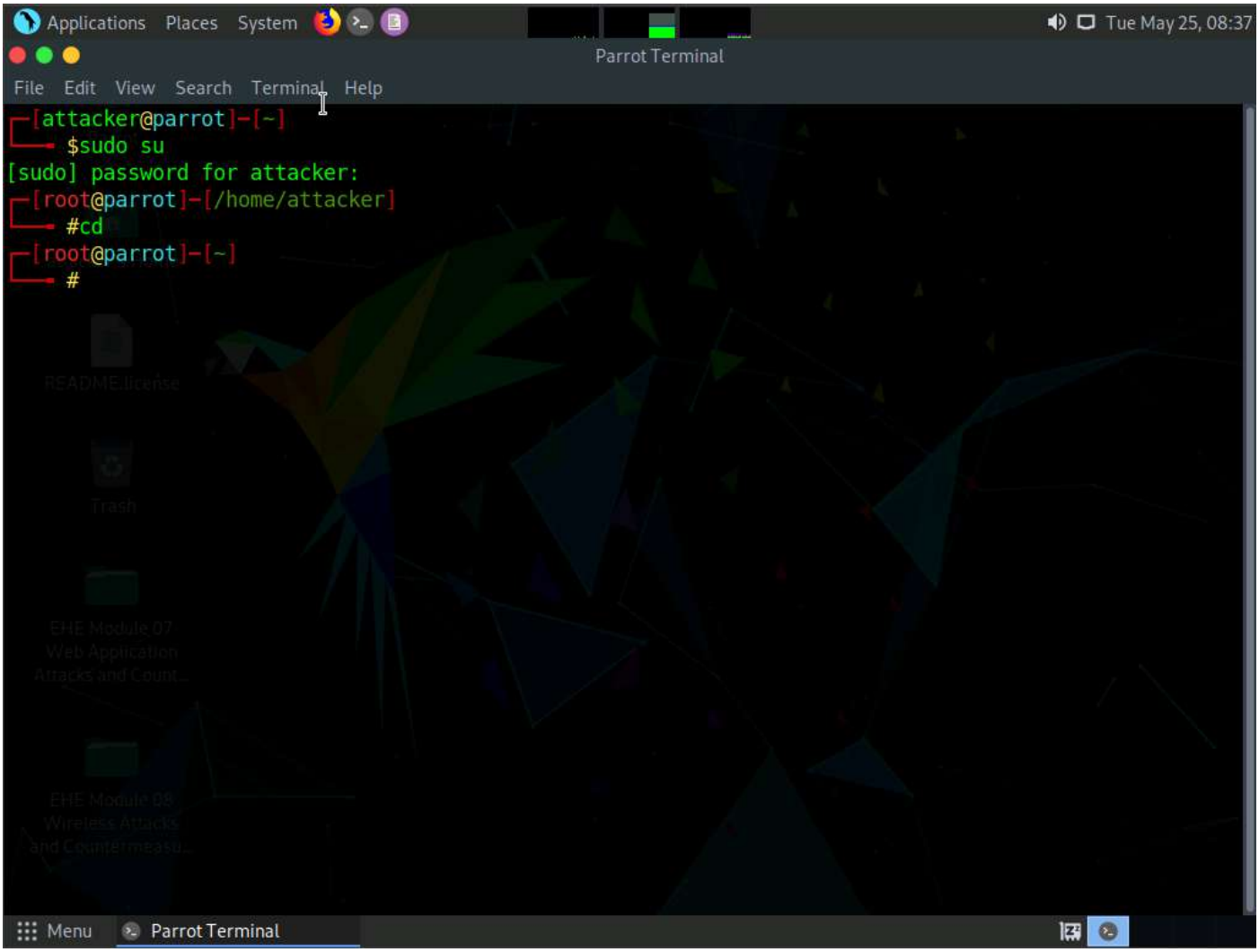
3. Assume that you are an attacker, and you have observed that the FTP service is running on the **Windows 10** machine.
4. Perform an **Nmap scan** on the target machine (**Windows 10**) to check if the FTP port is open.
5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



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

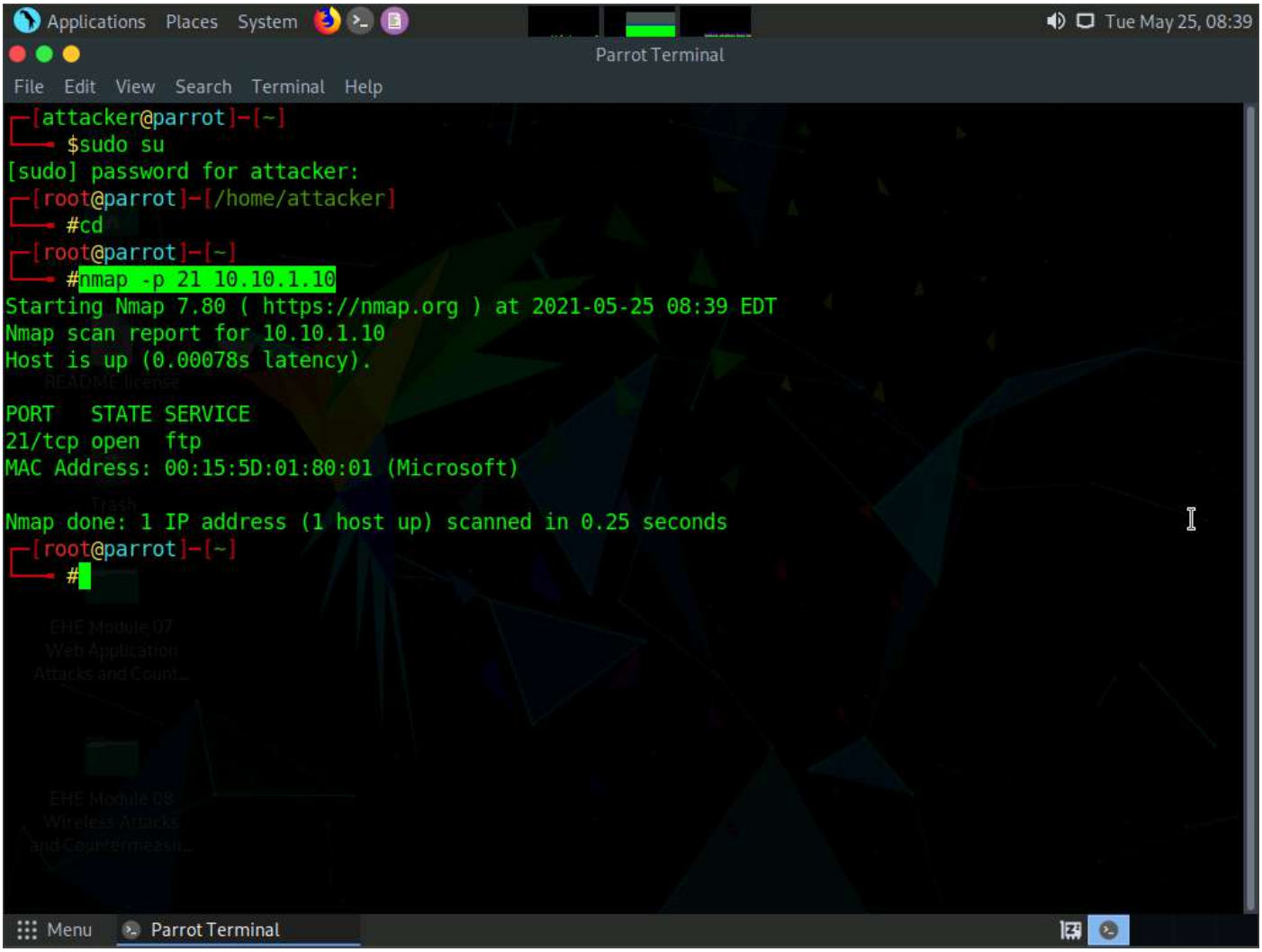
The password that you type will not be visible.

8. Now, type **cd** and press **Enter** to jump to the root directory.

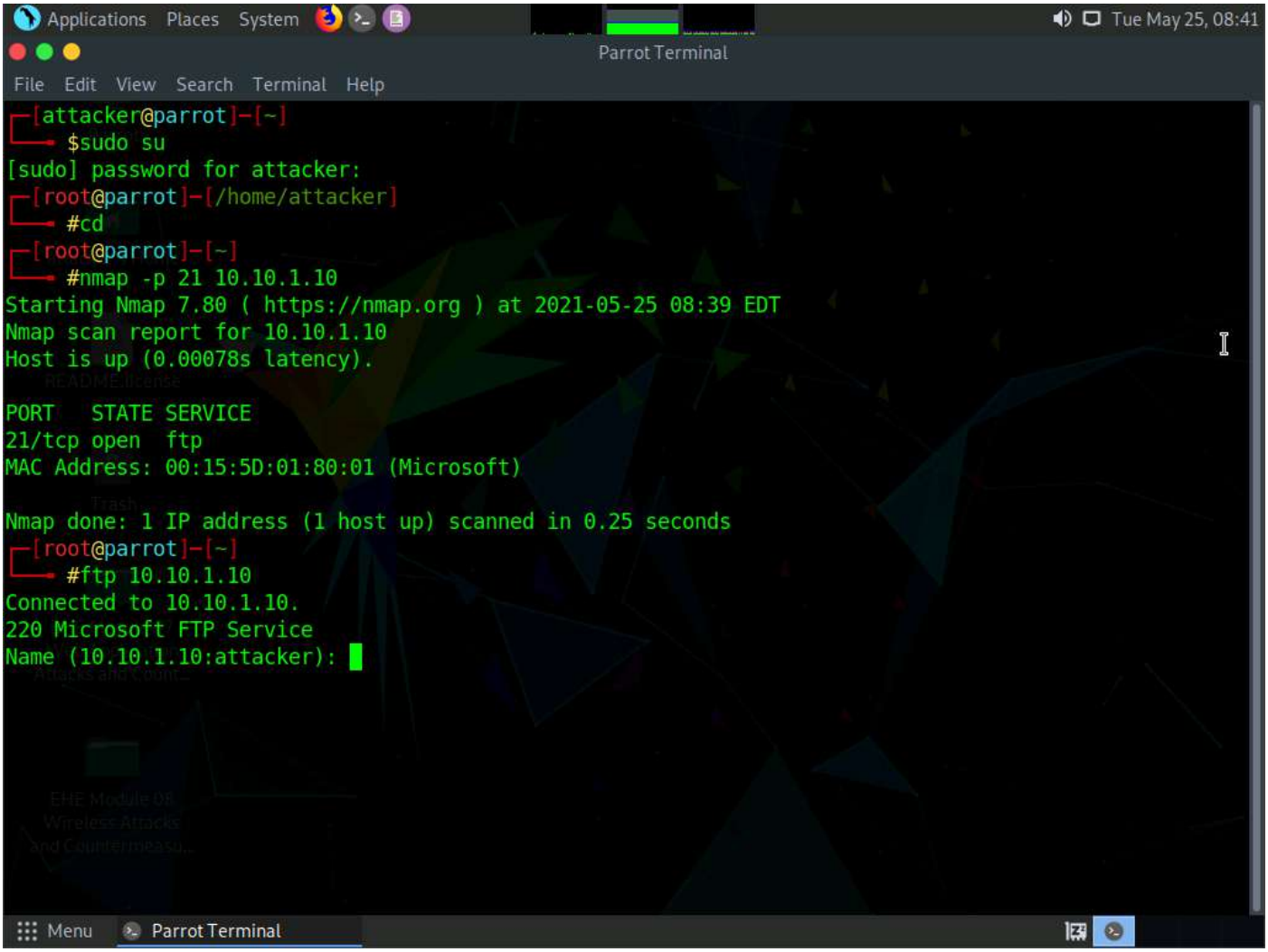


9. In the terminal window, type **nmap -p 21 [IP Address of Windows 10]**, and press **Enter**.

In this lab, the IP address of **Windows 10** is **10.10.1.10**.



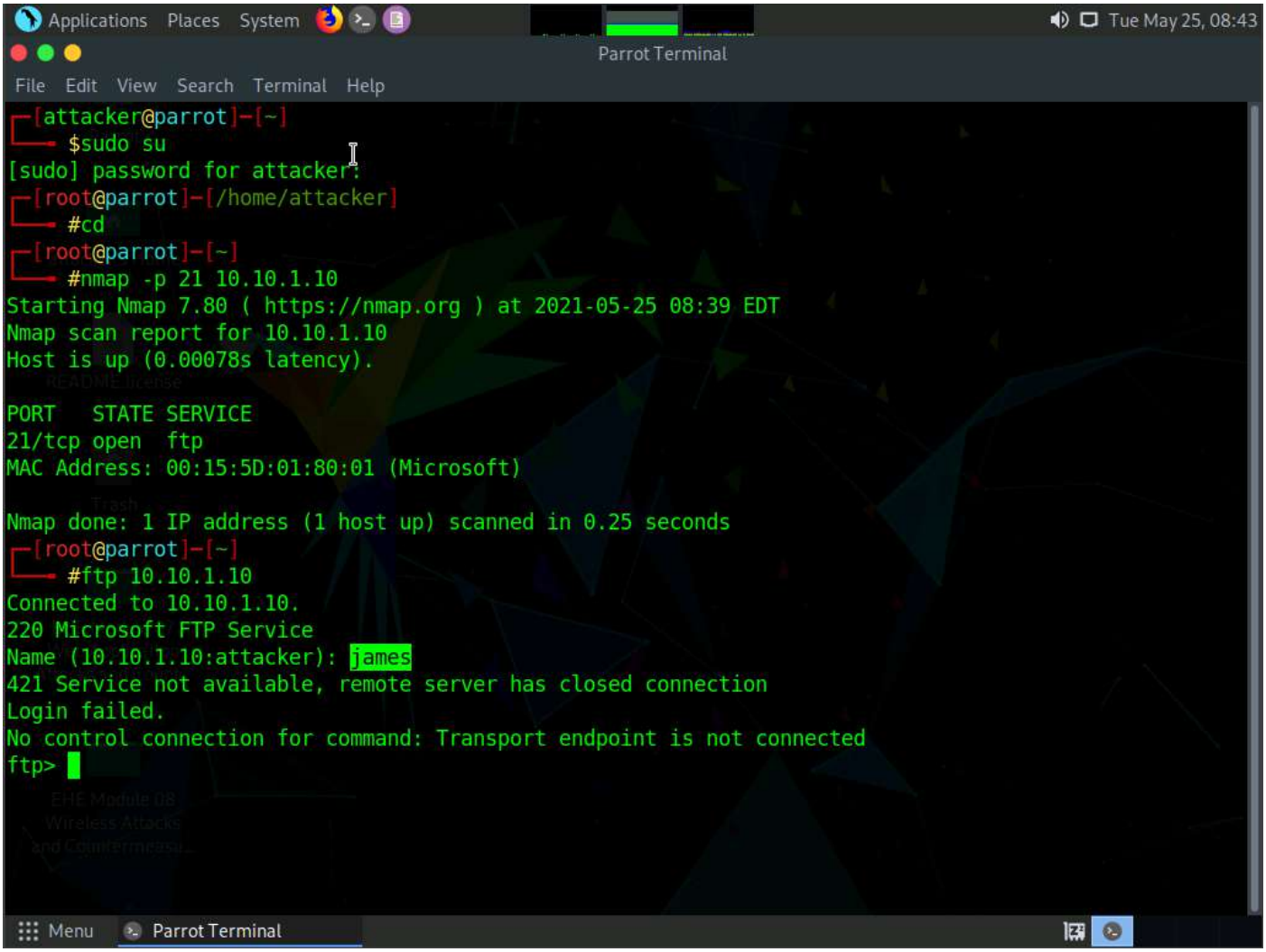
10. Observe that **port 21** is open in **Windows 10**.
11. Check if an FTP server is hosted on the **Windows 10** machine.
12. Type **ftp [IP Address of Windows 10]** and press **Enter**. You will be prompted to enter user credentials. The need for credentials implies that an FTP server is hosted on the machine.



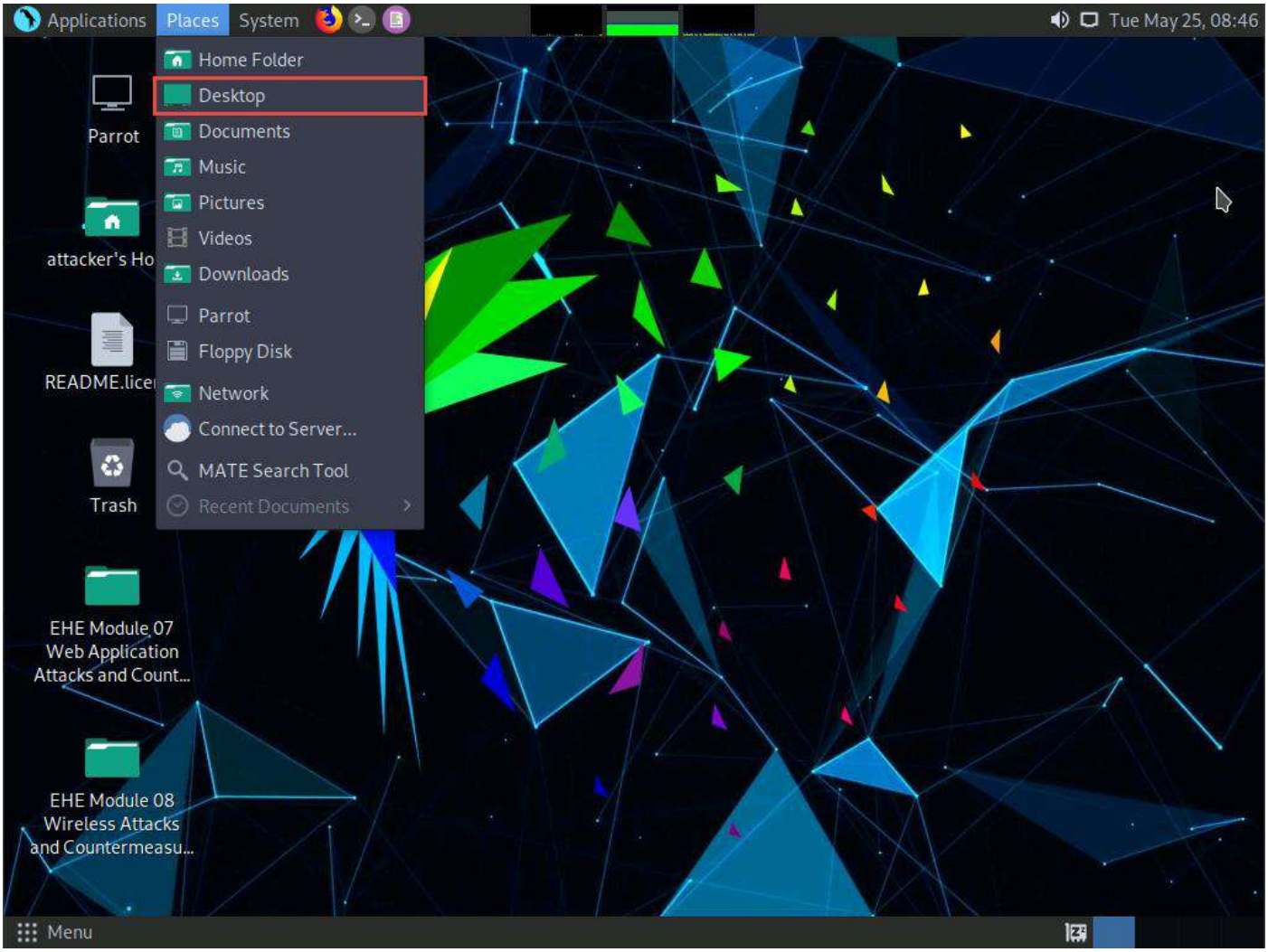
13. Try entering random usernames and passwords in an attempt to gain FTP access.

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

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

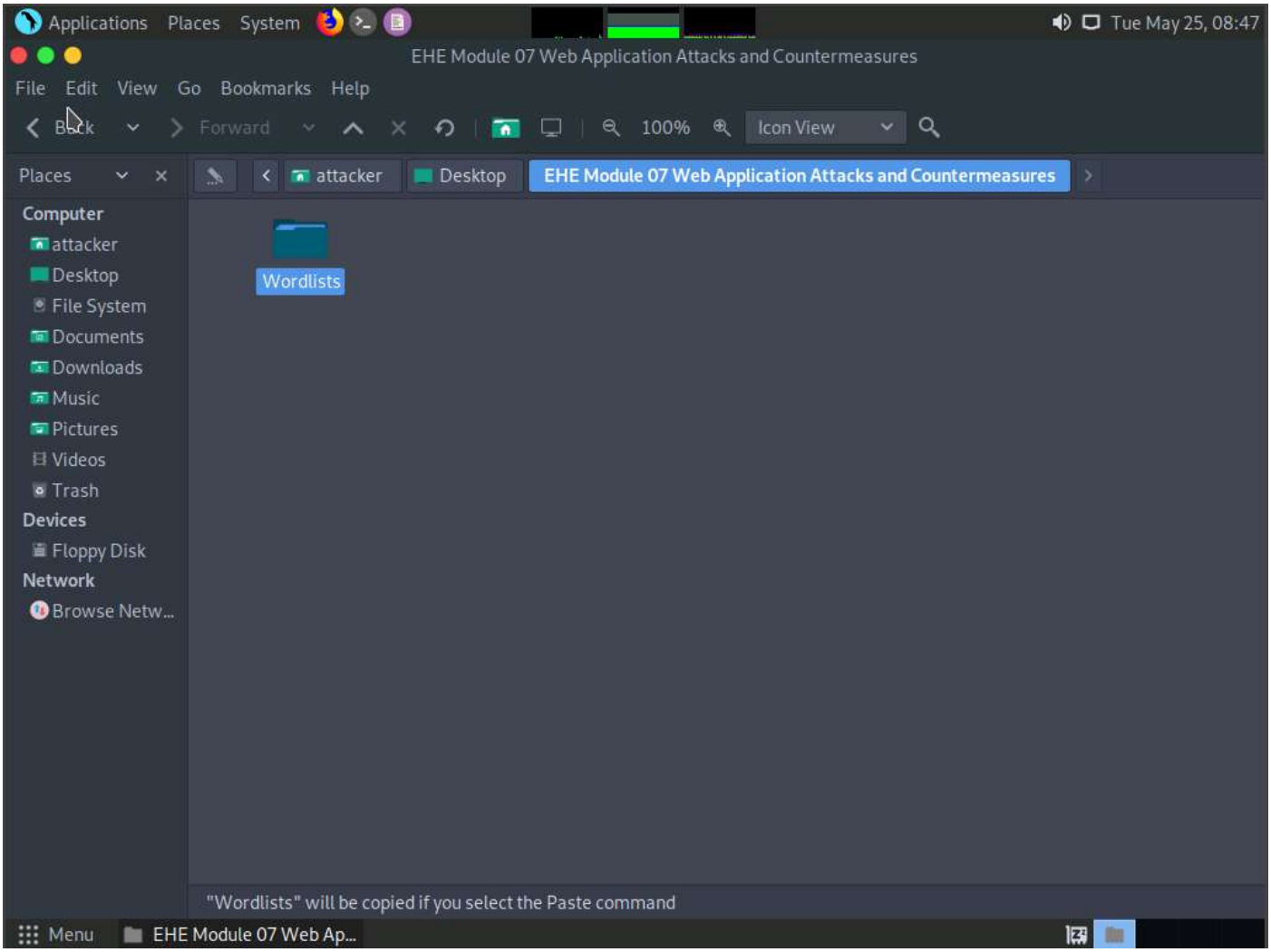


15. Now, to attempt to gain access to the FTP server, perform a dictionary attack using the THC Hydra tool.
16. Click **Places** from the top-section of the **Desktop** and click **Desktop** from the drop-down options.



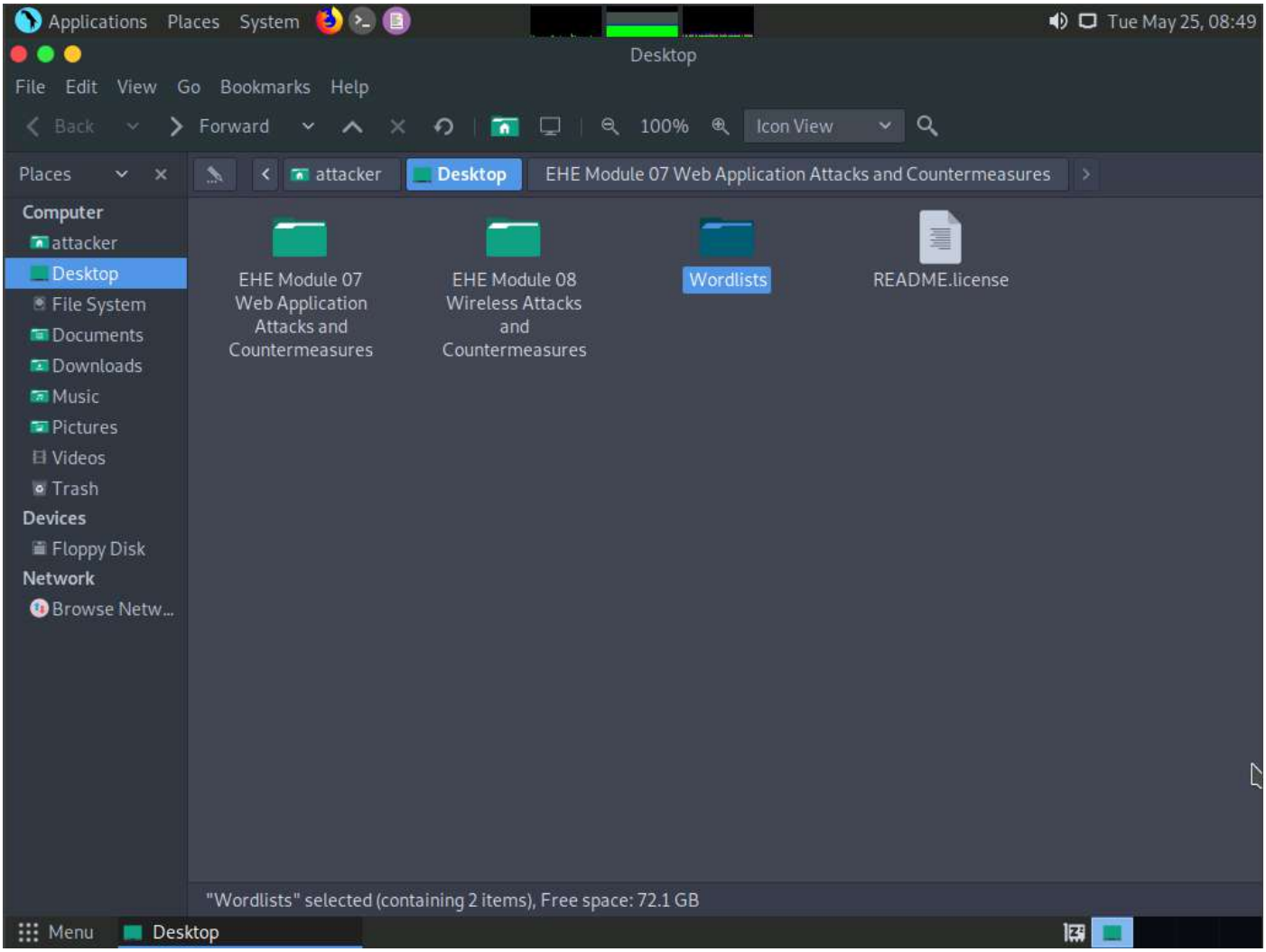
17. Navigate to **EHE Module 07 Web Application Attacks and Countermeasures** folder and copy **Wordlists** folder.

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

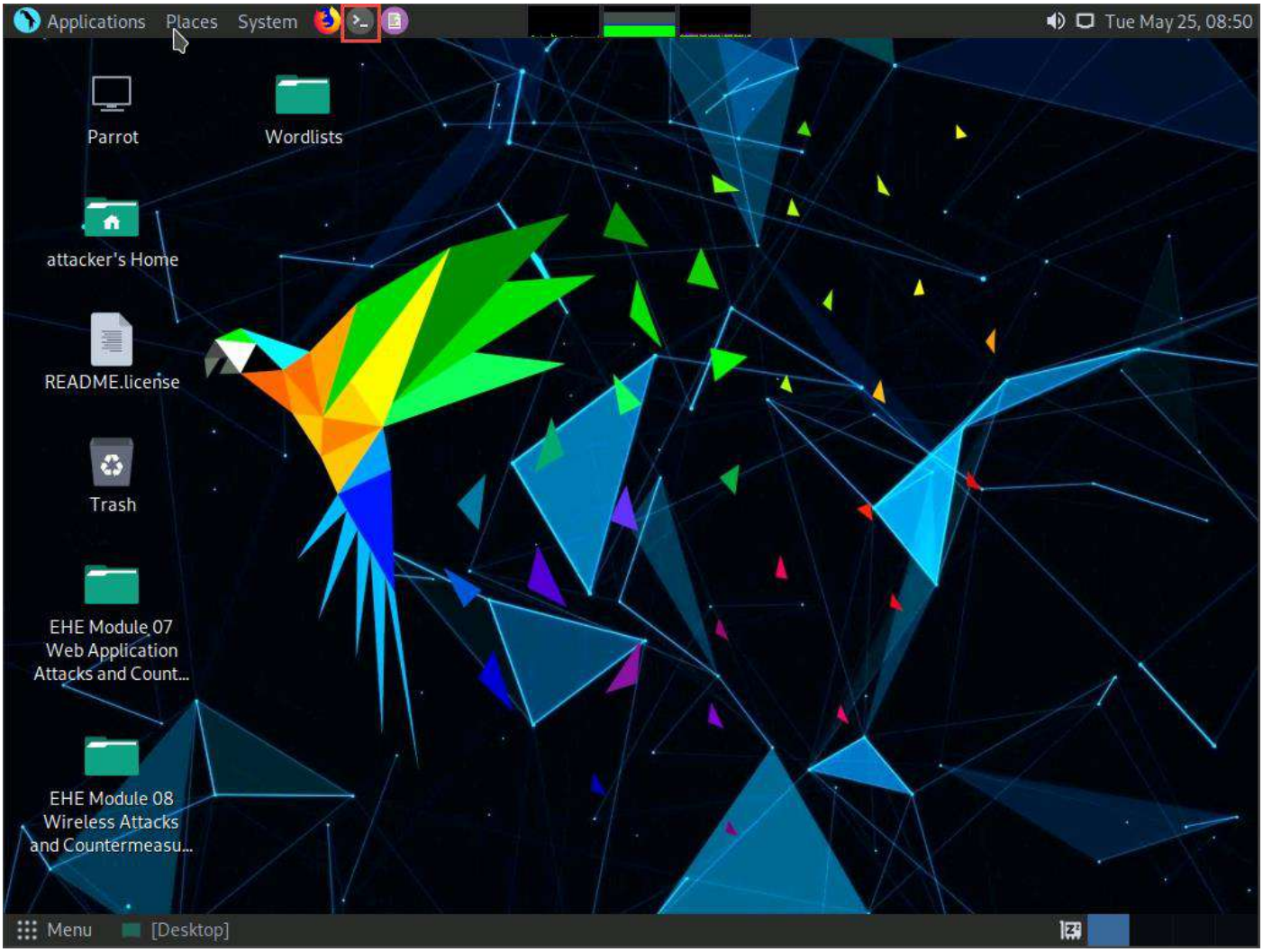


18. Paste the copied folder (**Wordlists**) on the **Desktop**. Close the window

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



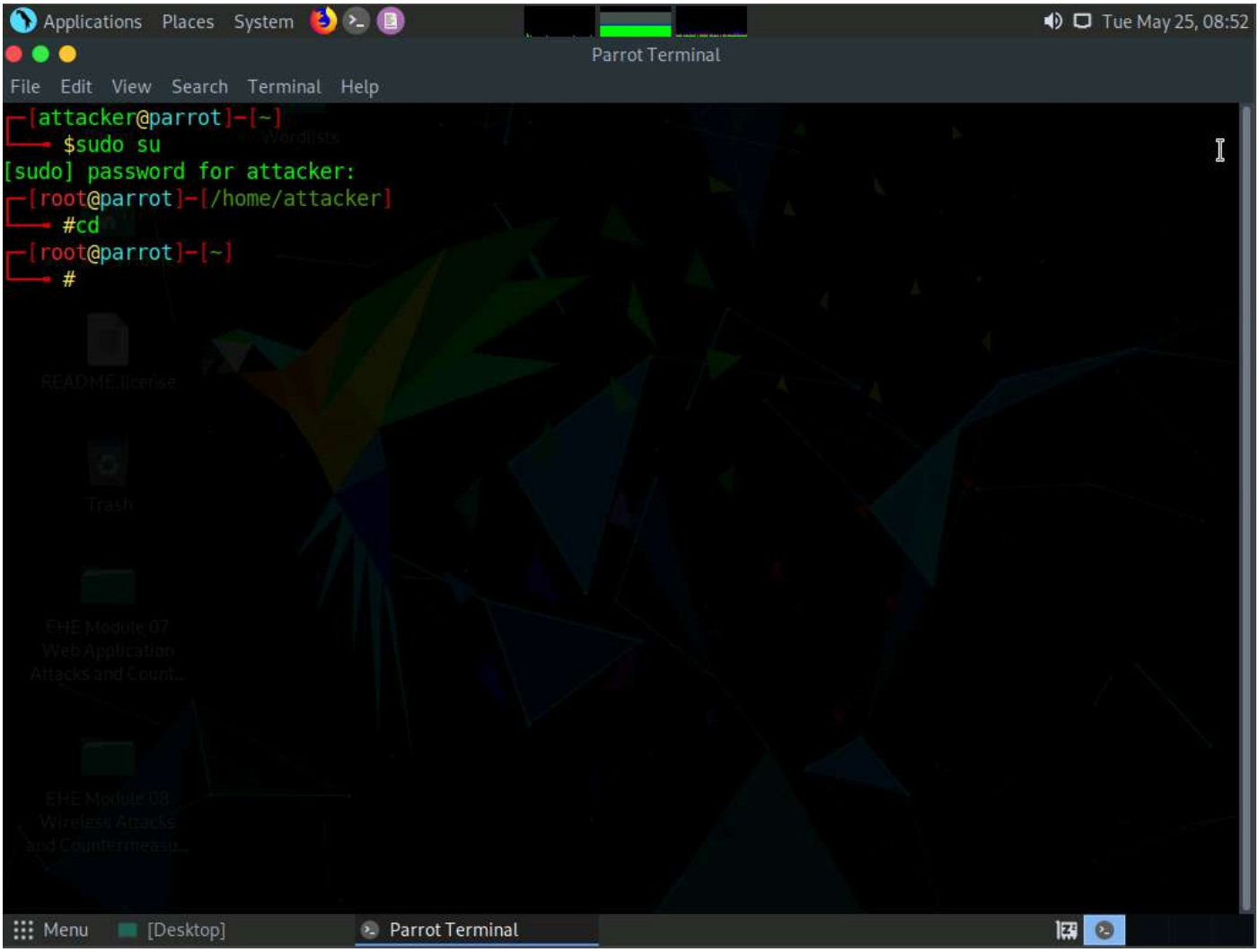
19. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



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

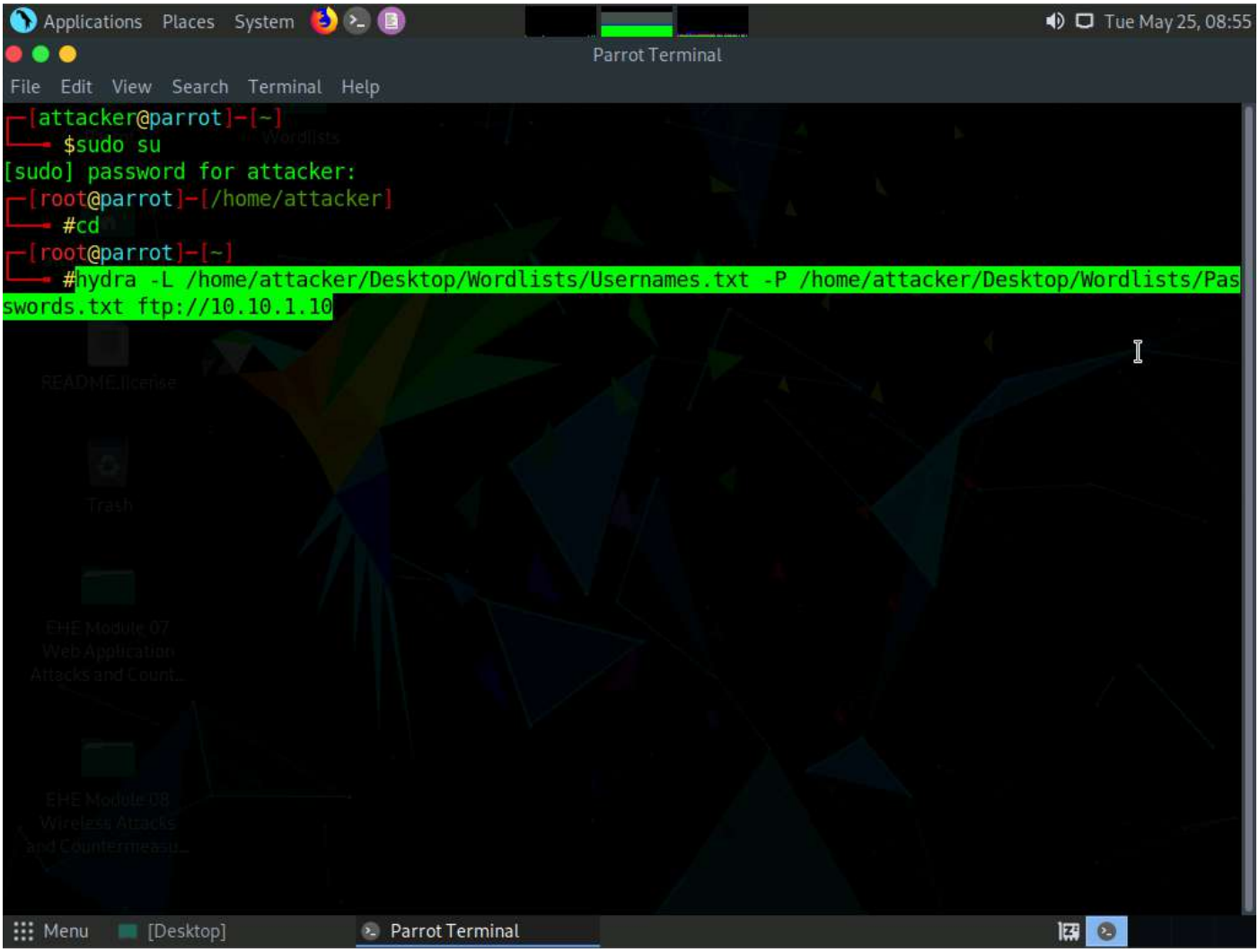
The password that you type will not be visible.

22. Now, type **cd** and press **Enter** to jump to the root directory.



23. 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 10]** and press **Enter**.

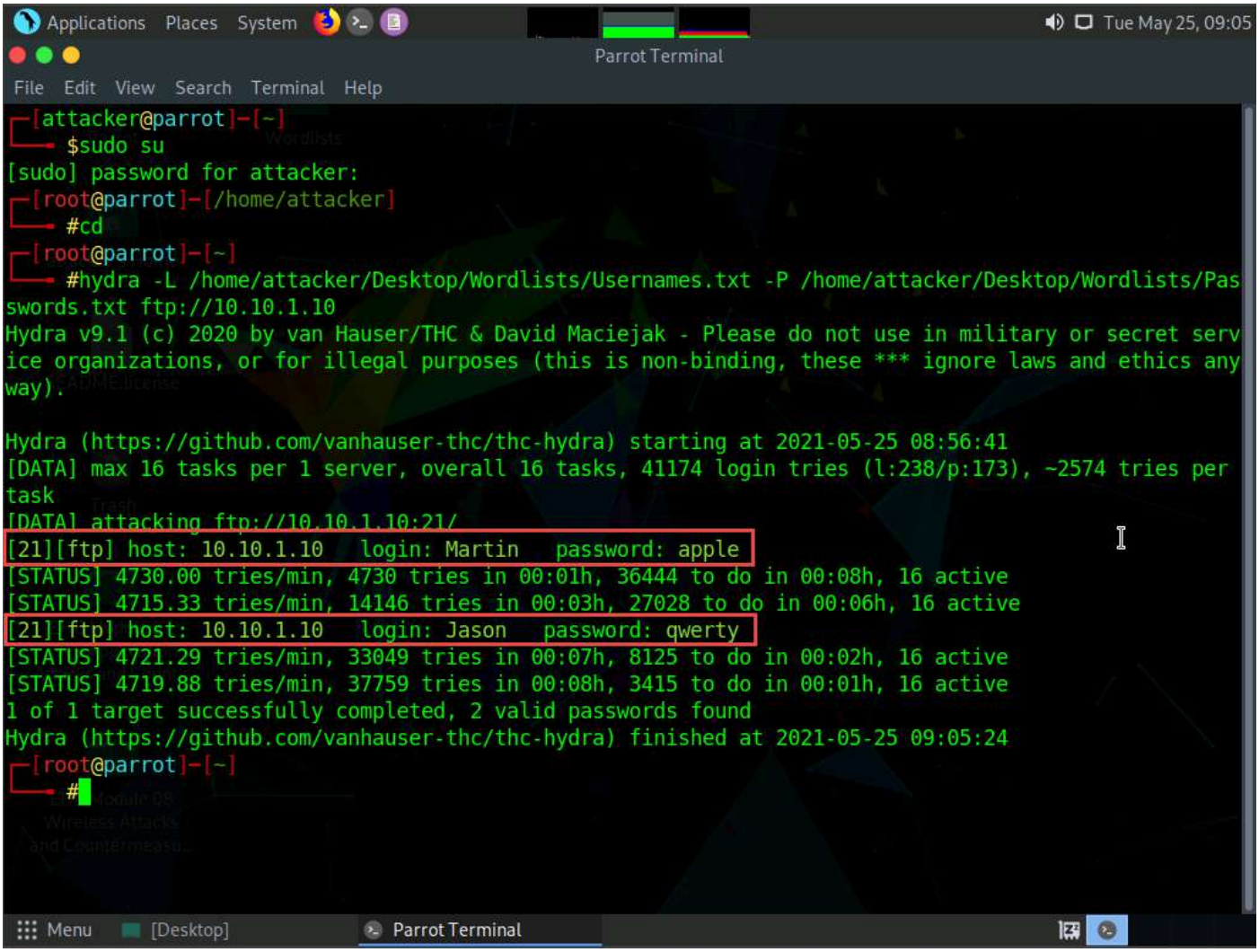
The IP address of **Windows 10** in this lab exercise is **10.10.1.10**. This IP address might vary in your lab environment.



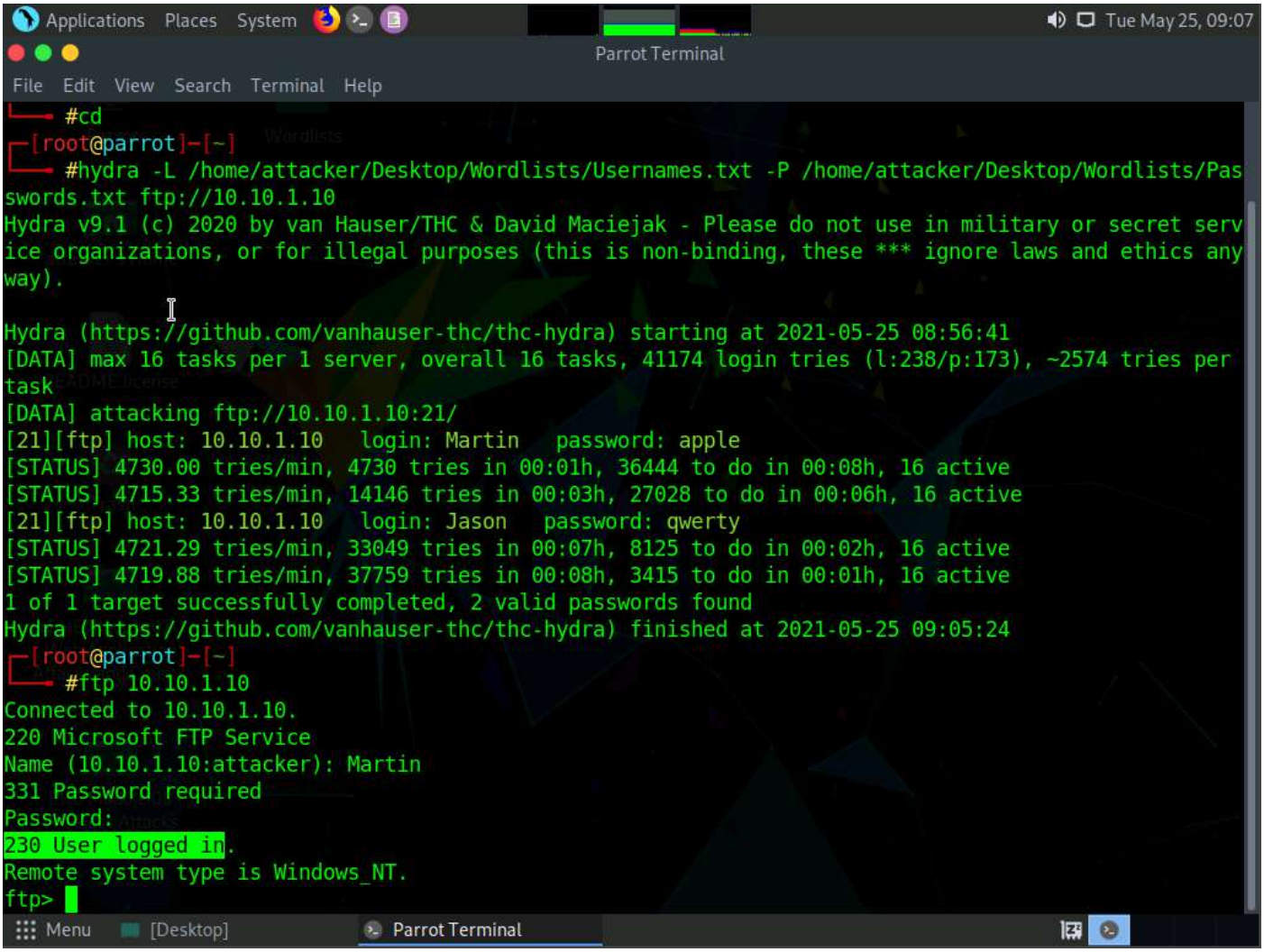
24. Hydra tries various combinations of usernames and passwords (present in the **Usernames.txt** and **Passwords.txt** files) on the FTP server and outputs cracked usernames and passwords, as shown in the screenshot.

This might take some time to complete.

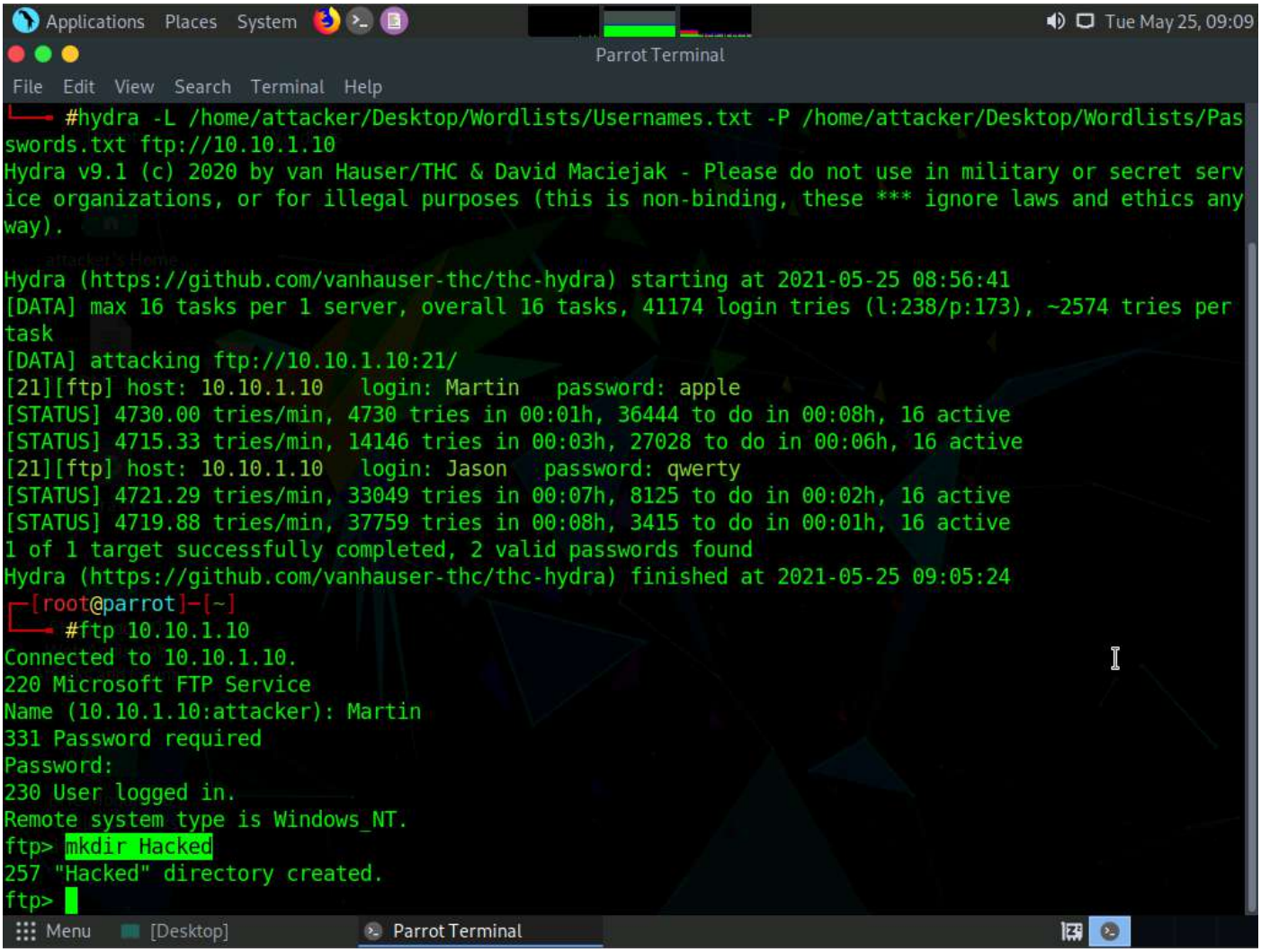
25. On completion of the password cracking, the **cracked credentials** appear, as shown in the screenshot.



26. 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.
27. In the terminal window, type **ftp [IP Address of Windows 10]**, and press **Enter**.
28. Enter Martin's user credentials (**Martin** and **apple**) to check whether you can successfully log in to the server.
29. On entering the credentials, you will successfully be able to log in to the server. An ftp terminal appears, as shown in the screenshot.



30. Now you can remotely access the FTP server hosted on the **Windows 10** machine.
31. Type **mkdir Hacked** and press **Enter** to remotely create a directory named **Hacked** on the **Windows 10** machine through the ftp terminal.



32. Click Windows 10 to switch to the **Windows 10** machine, click Ctrl+Alt+Delete.

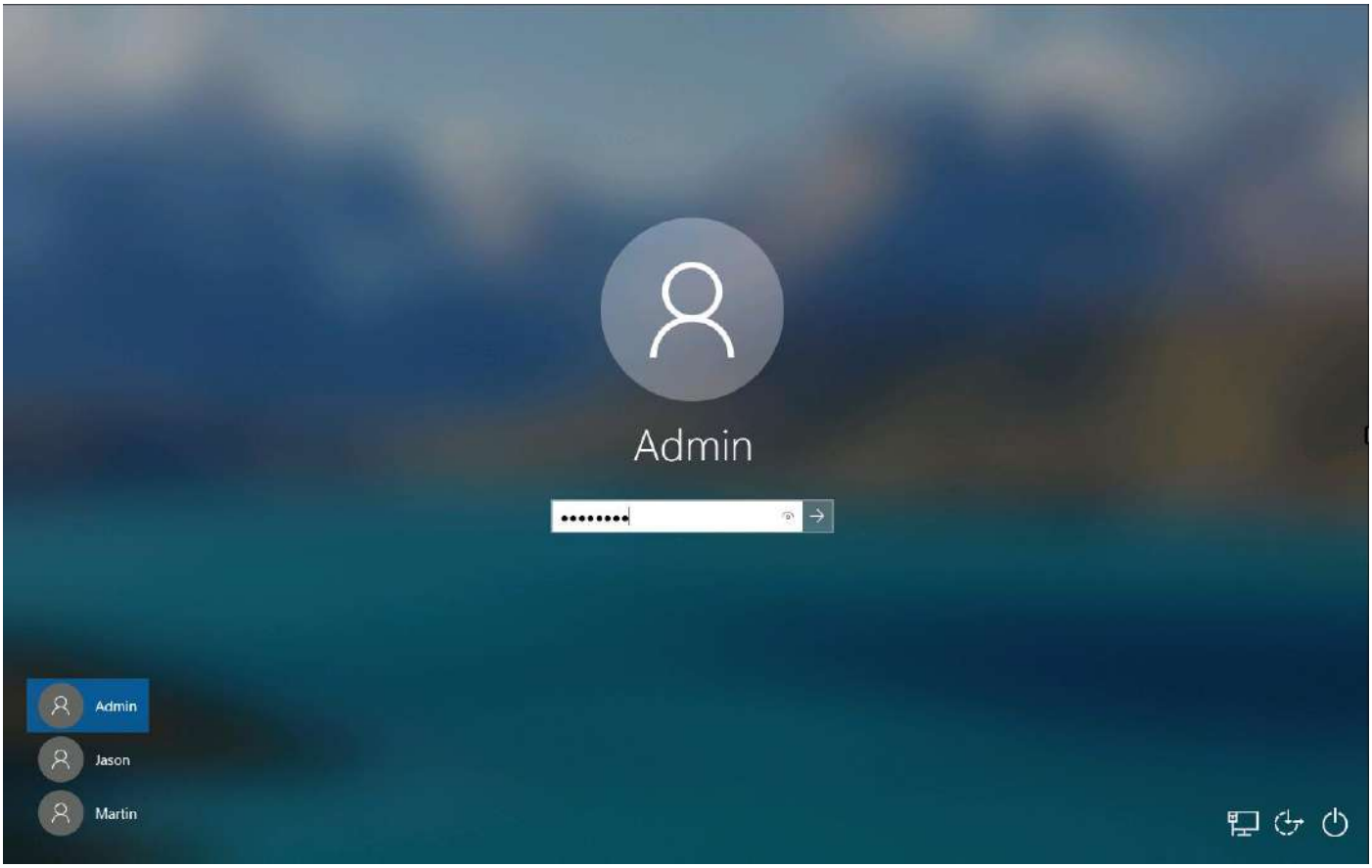
Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 10** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under Commands (**thunder** icon) menu.

33. By default, **Admin** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.

Alternatively, you can also click **Pa$$w0rd** under **Windows 10** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

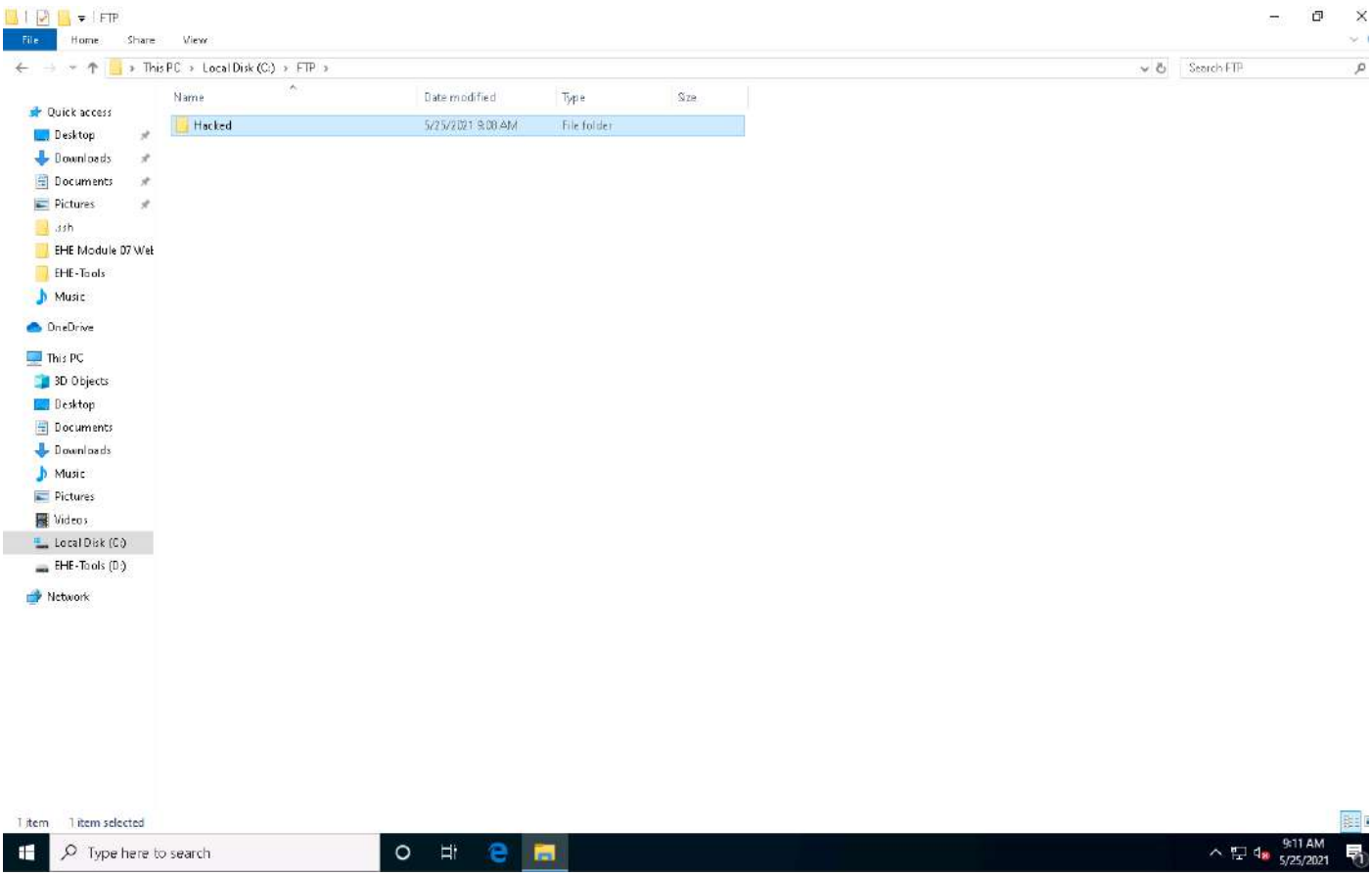
If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

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



34. Navigate to **C:\FTP**.

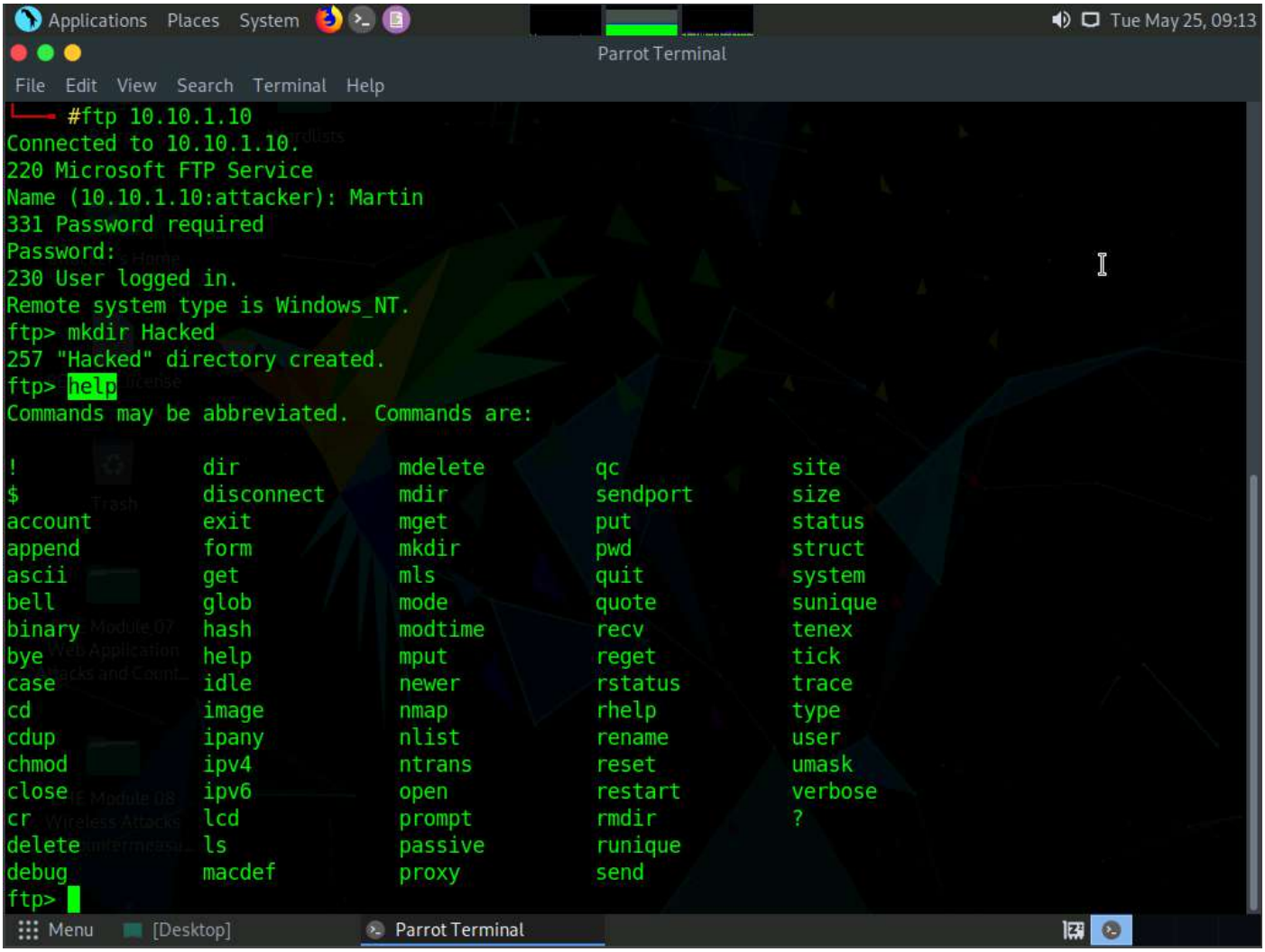
35. View the directory named **Hacked**, as shown in the screenshot:



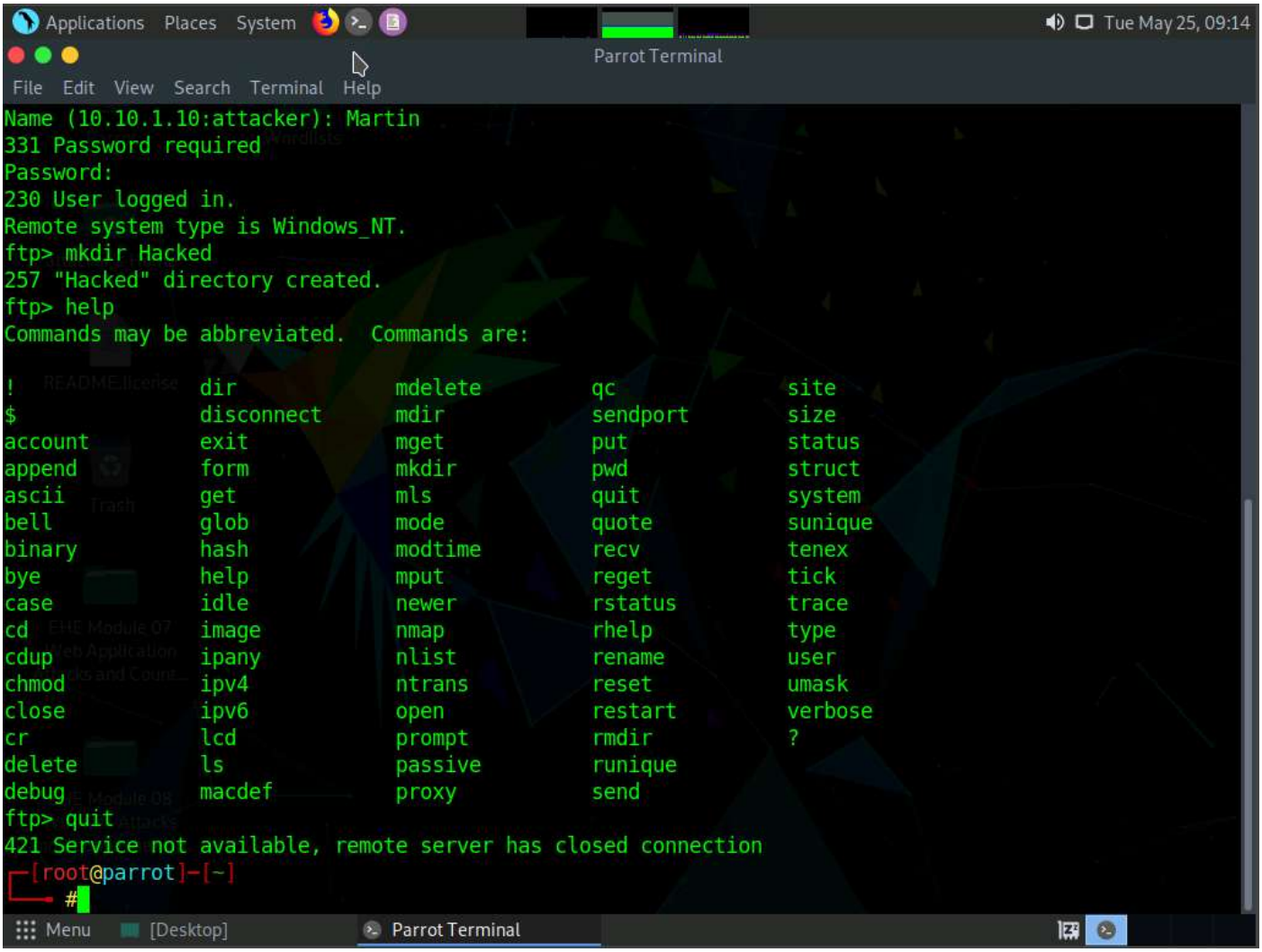
36. You have successfully gained remote access to the **FTP server** by obtaining the appropriate credentials.

37. Click Parrot Security to switch back to the **Parrot Security** machine.

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



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



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

41. Close all open windows on both the **Parrot Security** and **Windows 10** machines.

Lab 7-2: Perform a Web Application Attack to Compromise the Security of Web Applications to Steal Sensitive Information

Lab Scenario

Attackers perform web application attacks with certain goals in mind. These goals may be either technical or non-technical. For example, attackers may breach the security of the web application and steal sensitive information for financial gain or for curiosity's sake. To hack the web app, first, the attacker analyzes it to determine its vulnerable areas. Next, they attempt to reduce the "attack surface." Even if the target web application only has a single vulnerability, attackers will try to compromise its security by launching an appropriate attack. They try various application-level attacks such as injection, XSS, broken authentication, broken access control, security misconfiguration, and insecure deserialization to compromise the security of web applications to commit fraud or steal sensitive information.

We must test their company's web application against various attacks and other vulnerabilities. They must find various ways to extend the security test and analyze web applications, for which they employ multiple testing techniques. This will help in predicting the effectiveness of additional security measures in strengthening and protecting web applications in the organization.

The task in this lab will assist in performing attacks on web applications using various techniques and tools.

Lab Objectives

- Perform Parameter Tampering using Burp Suite

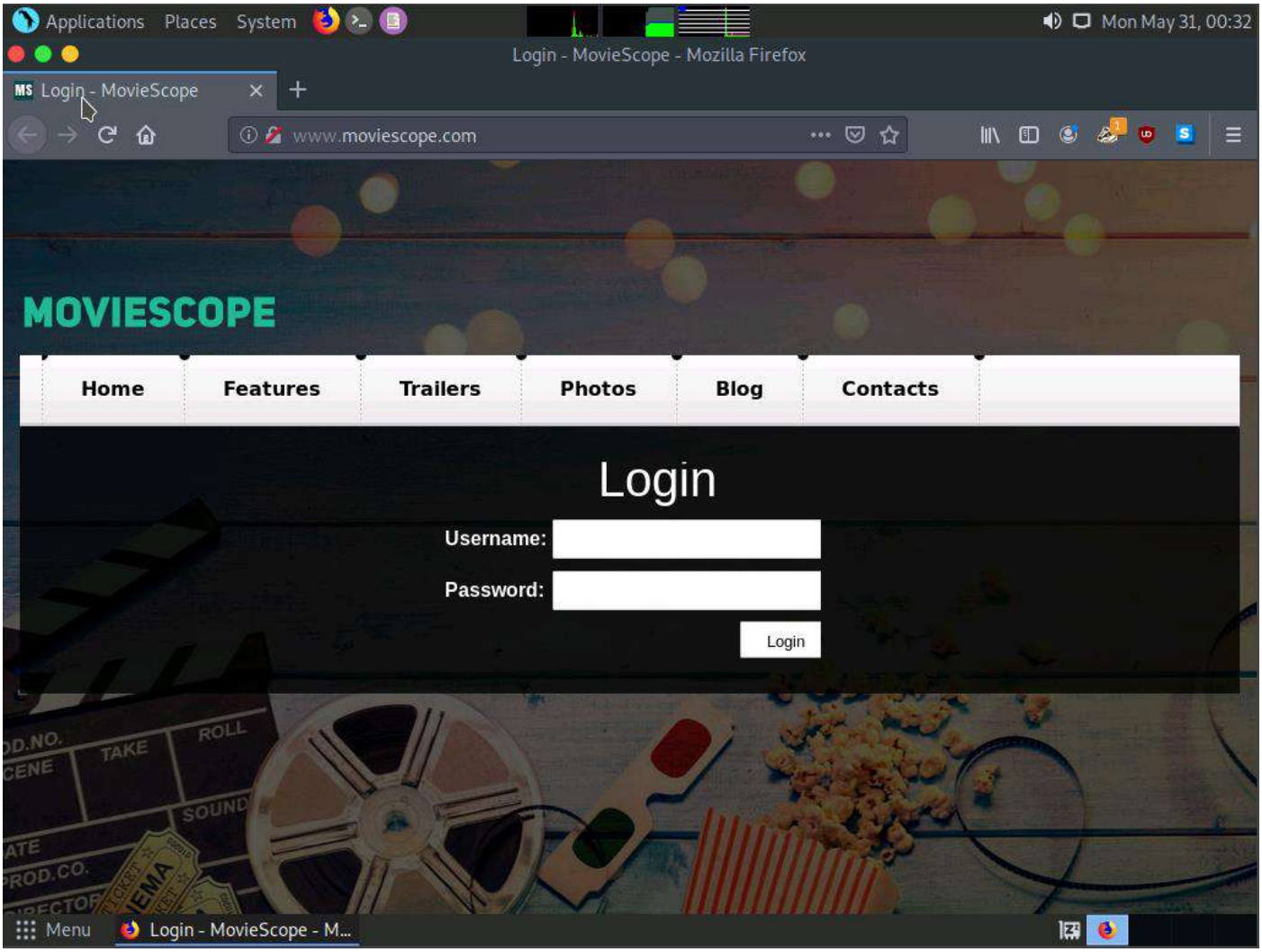
Task 1: Perform Parameter Tampering using Burp Suite

A web parameter tampering attack involves the manipulation of parameters exchanged between the client and server to modify application data such as user credentials and permissions, price, and quantity of products.

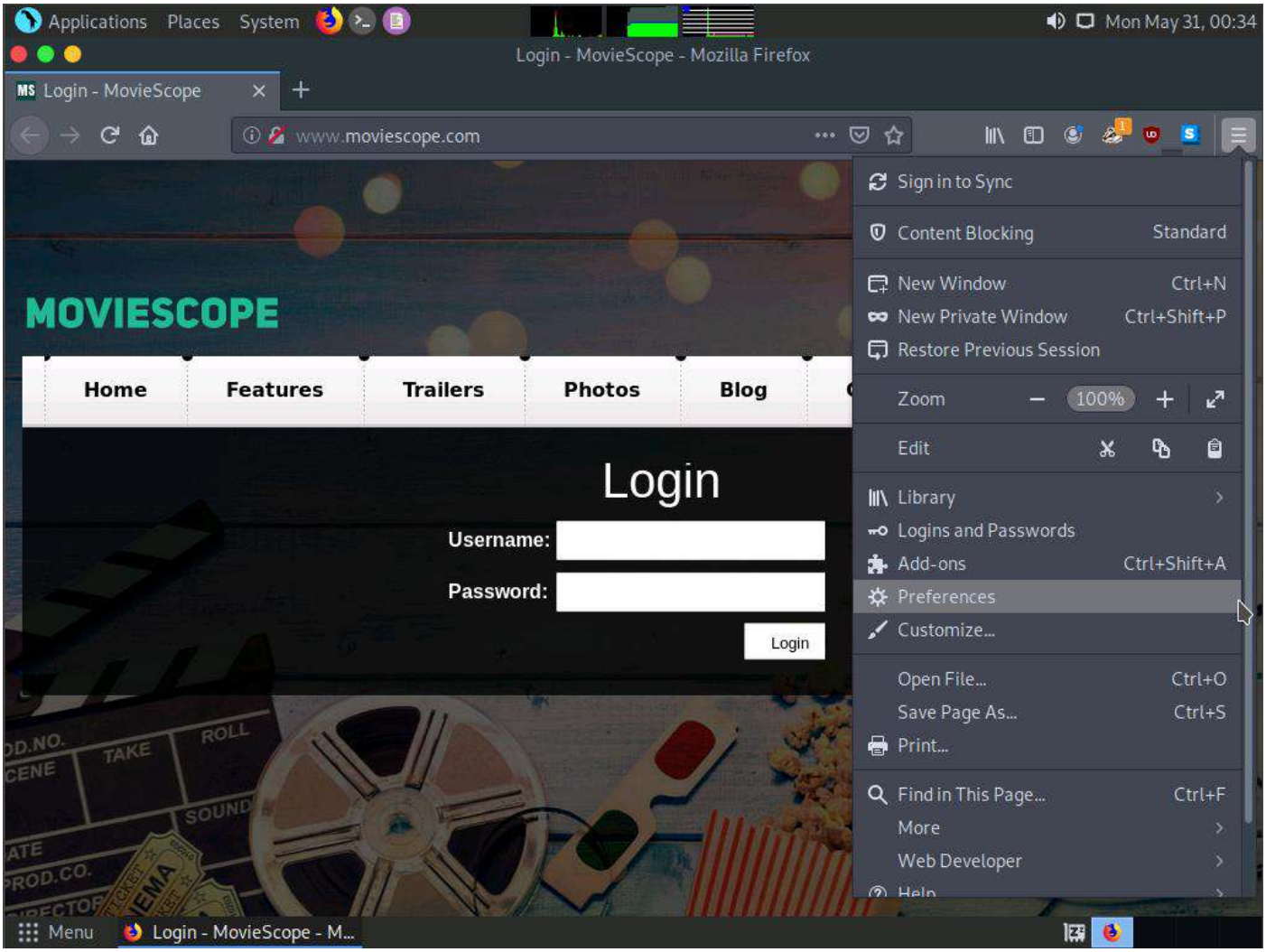
Here, we will use the Burp Suite tool to perform parameter tampering.

In this task, the target website (**www.moviescope.com**) is hosted by the victim machine, **Windows Server 2019**. Here, the host machine is the **Parrot Security** machine.

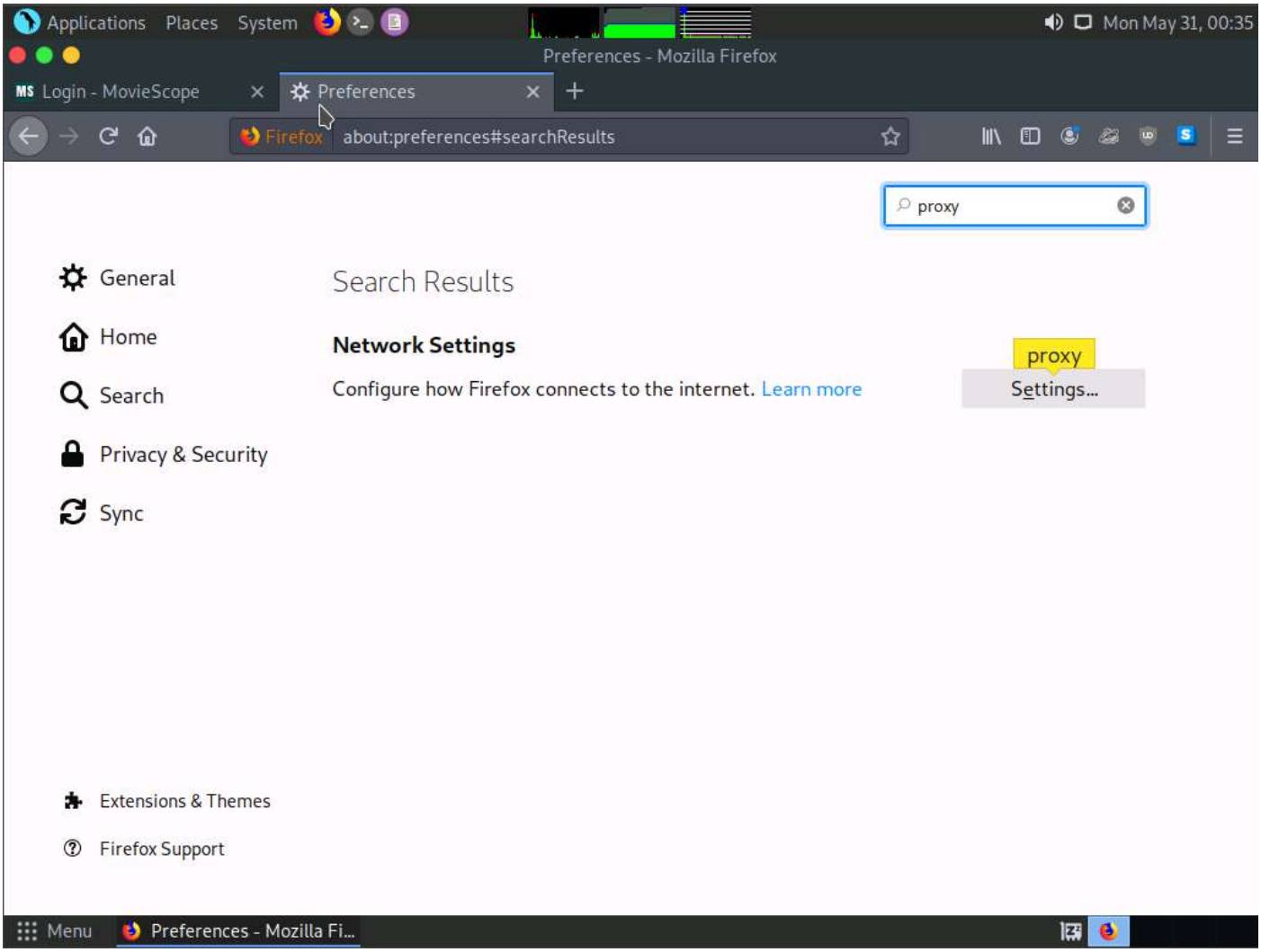
1. In **Parrot Security** machine click the **Firefox** icon from the top section of **Desktop** to launch the **Mozilla Firefox** browser.
2. The **Mozilla Firefox** window appears; type **http://www.moviescope.com** into the address bar and press **Enter**.



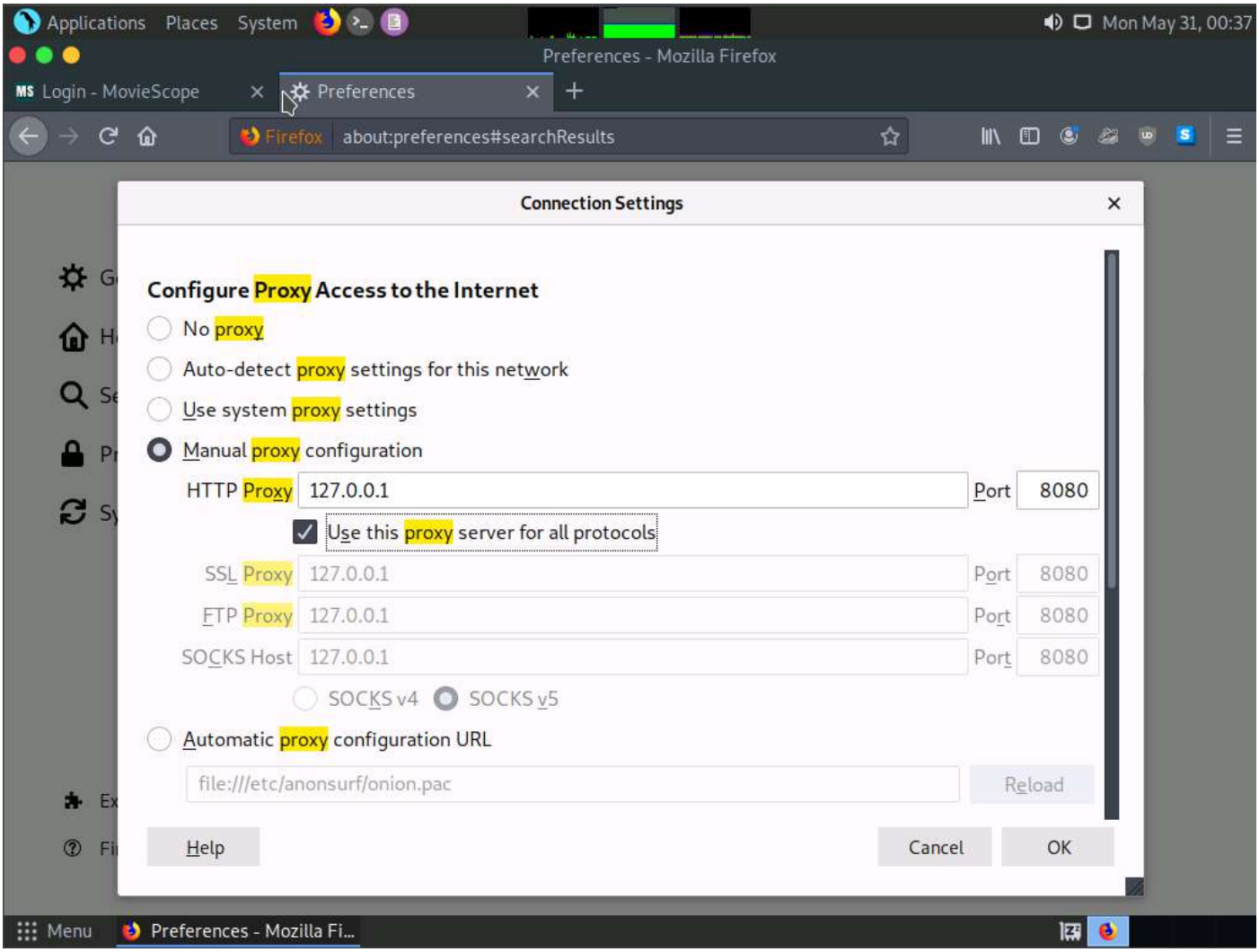
3. Now, set up a **Burp Suite** proxy by first configuring the proxy settings of the browser.
4. In the **Mozilla Firefox** browser, click the **Open menu** icon in the right corner of the menu bar and select **Preferences** from the list.



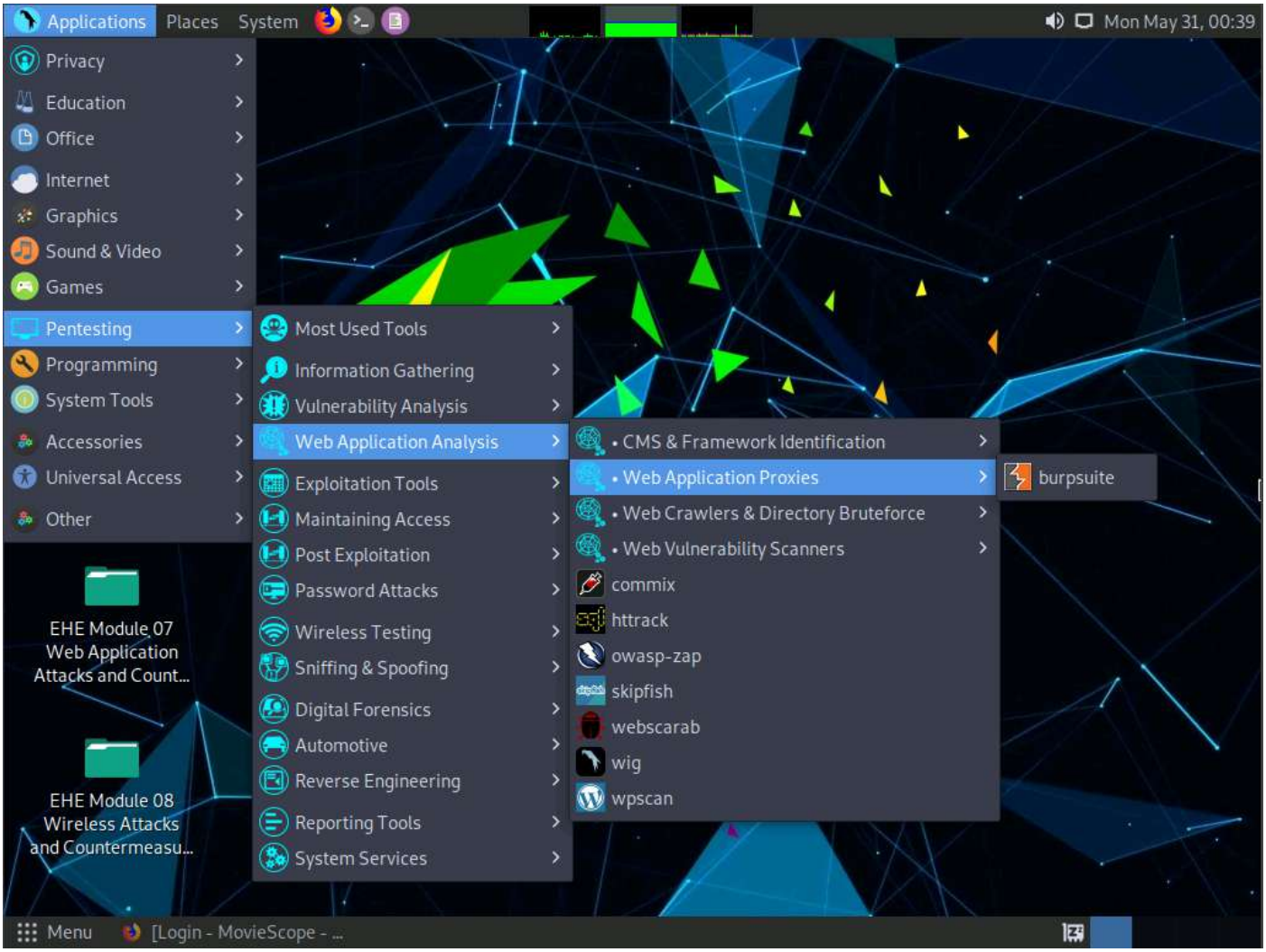
5. The **General** settings tab appears. In the **Find in Preferences** search bar, type **proxy**, and press **Enter**.
6. The **Search Results** appear. Click the **Settings** button under the **Network Settings** option.



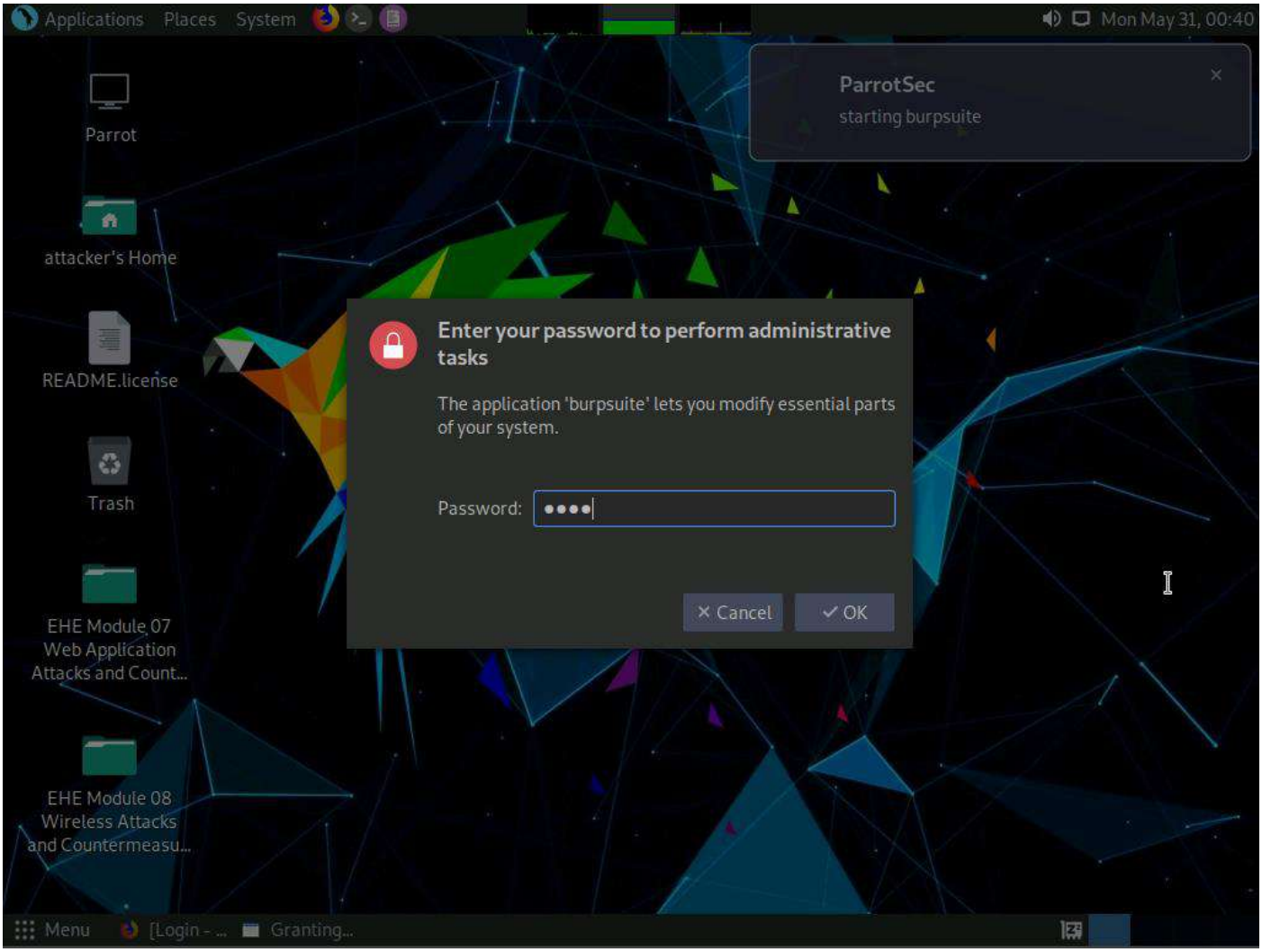
7. A **Connection Settings** window appears. Select the **Manual proxy configuration** radio button and specify the HTTP Proxy as **127.0.0.1** and the Port as **8080**. Tick the **Use this proxy server for all protocols** checkbox and click **OK**. Close the Preferences tab and minimize the browser window.



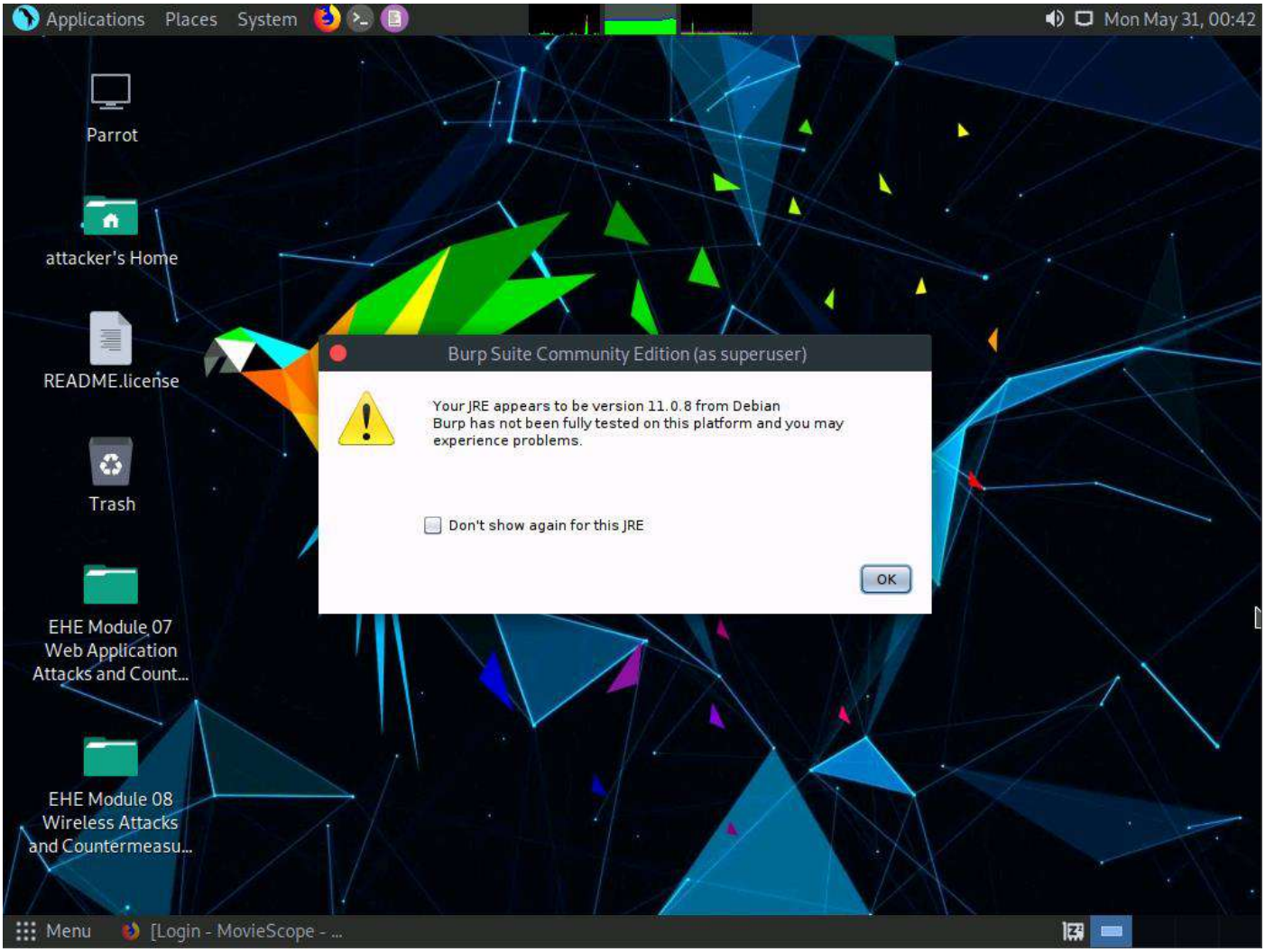
8. Click the **Applications** menu form the top left corner of **Desktop**, and navigate to **Pentesting** --> **Web Application Analysis** --> **Web Application Proxies** --> **burpsuite** to launch the **Burp Suite** application.



9. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.



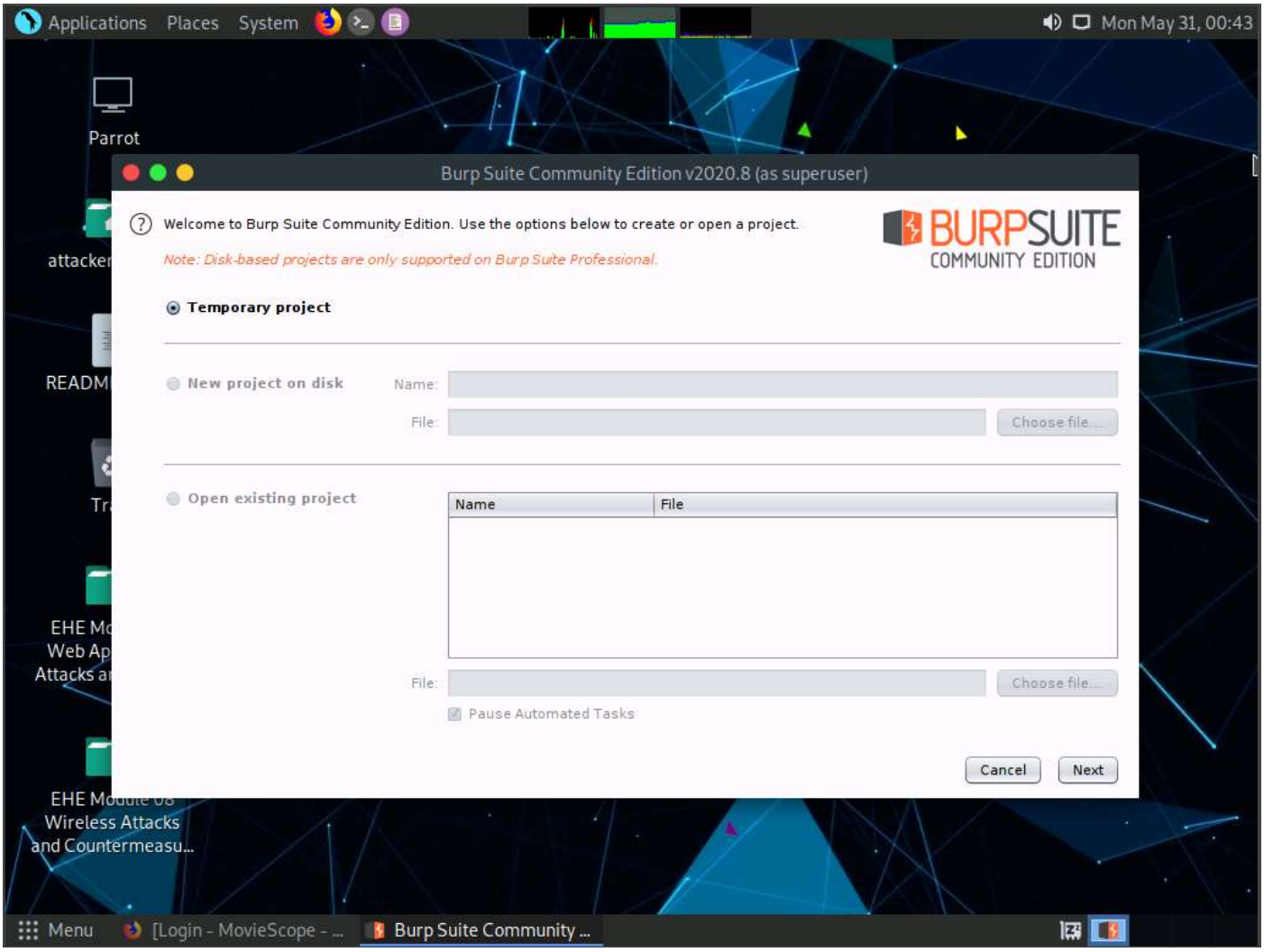
10. In the next **Burp Suite Community Edition** notification, click **OK**.



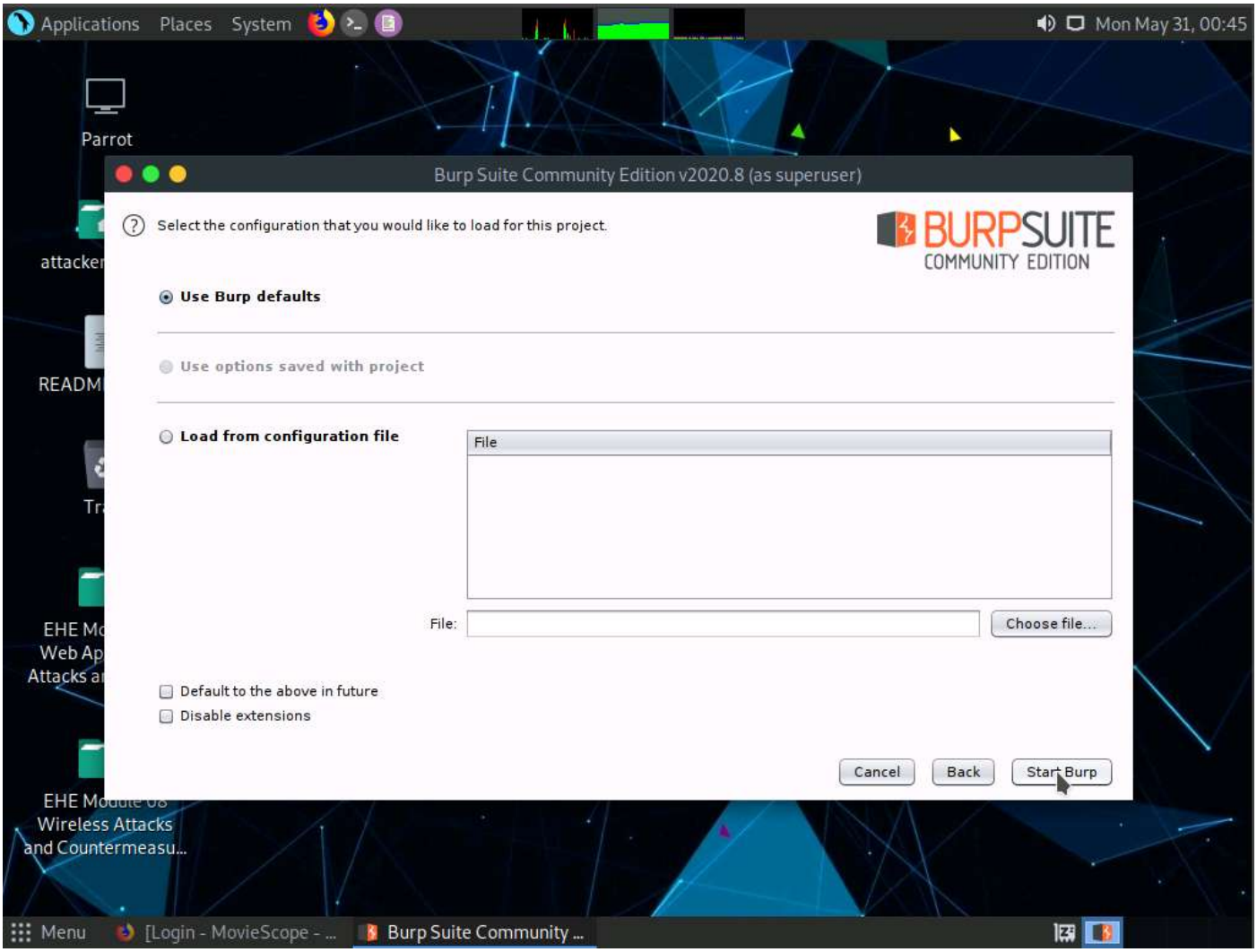
If Terms and Conditions window appears click on **I Accept**

11. **Burp Suite** initializes. If a **Burp Suite Community Edition** notification saying **An update is available** appears, click **Close**.
12. The **Burp Suite** main window appears; ensure that the **Temporary project** radio button is selected and click the **Next** button, as shown in the screenshot.

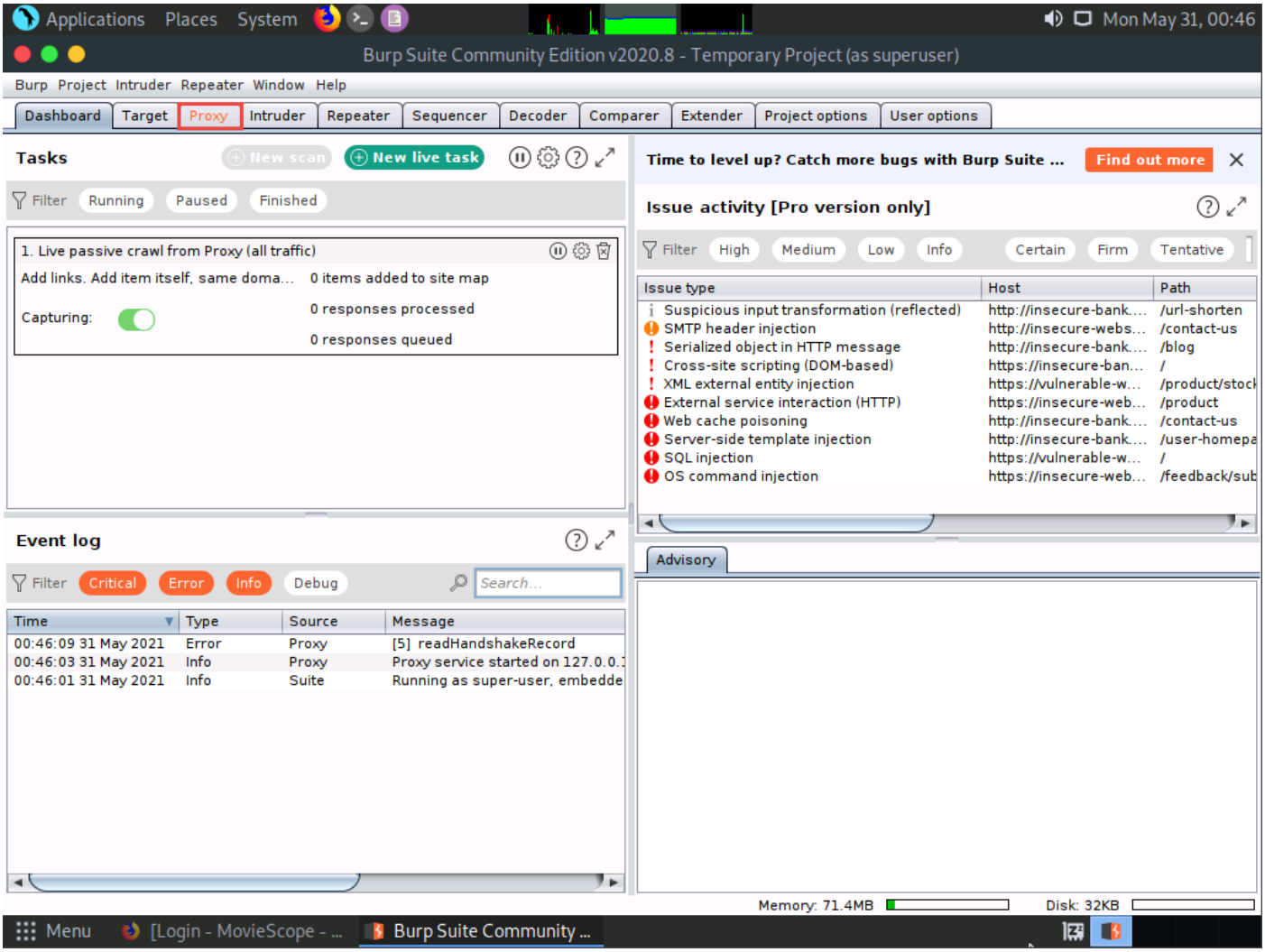
If an update window appears, click **Close**.



13. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.

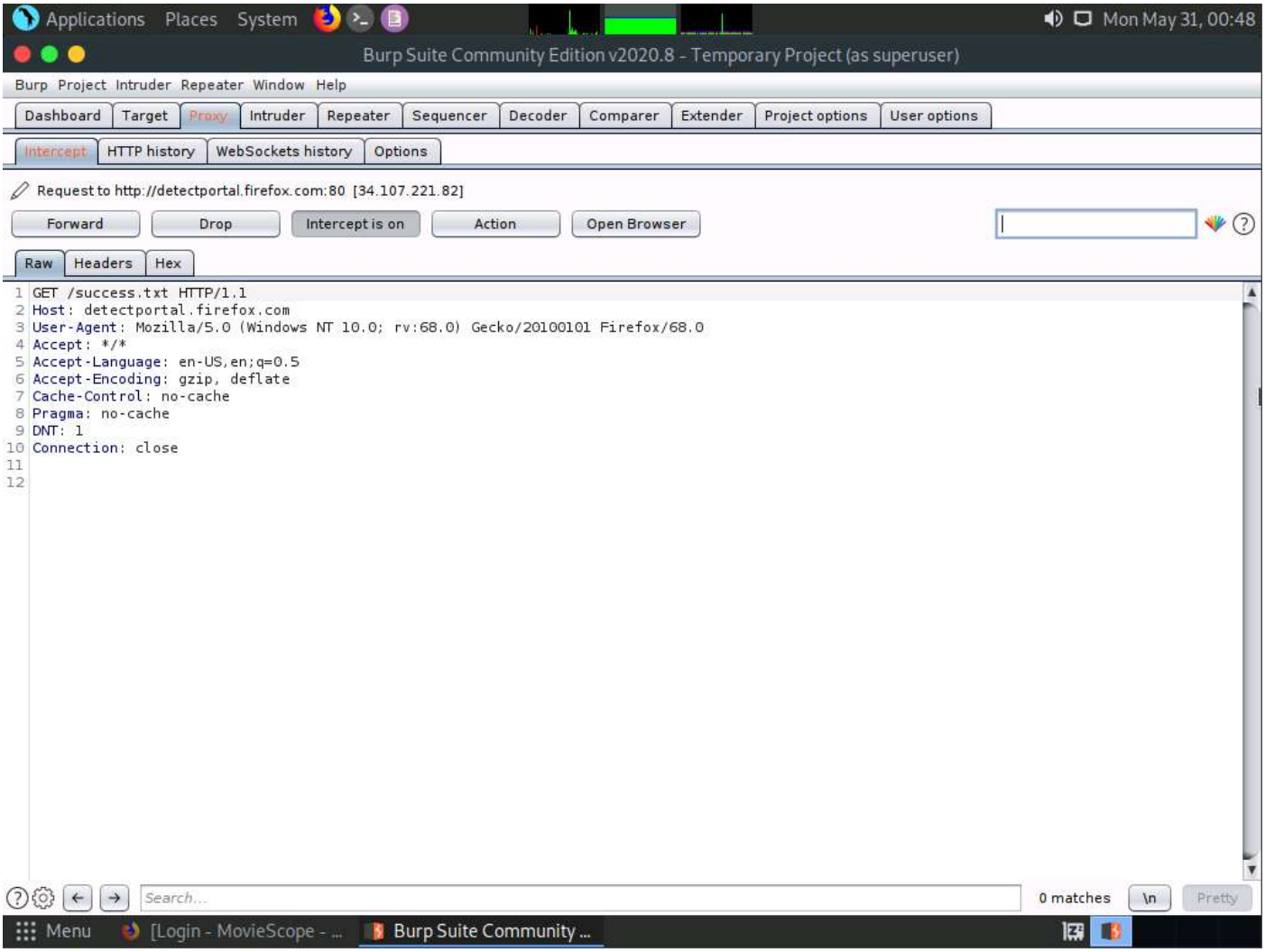


14. The **Burp Suite** main window appears; click the **Proxy** tab from the available options in the top section of the window.



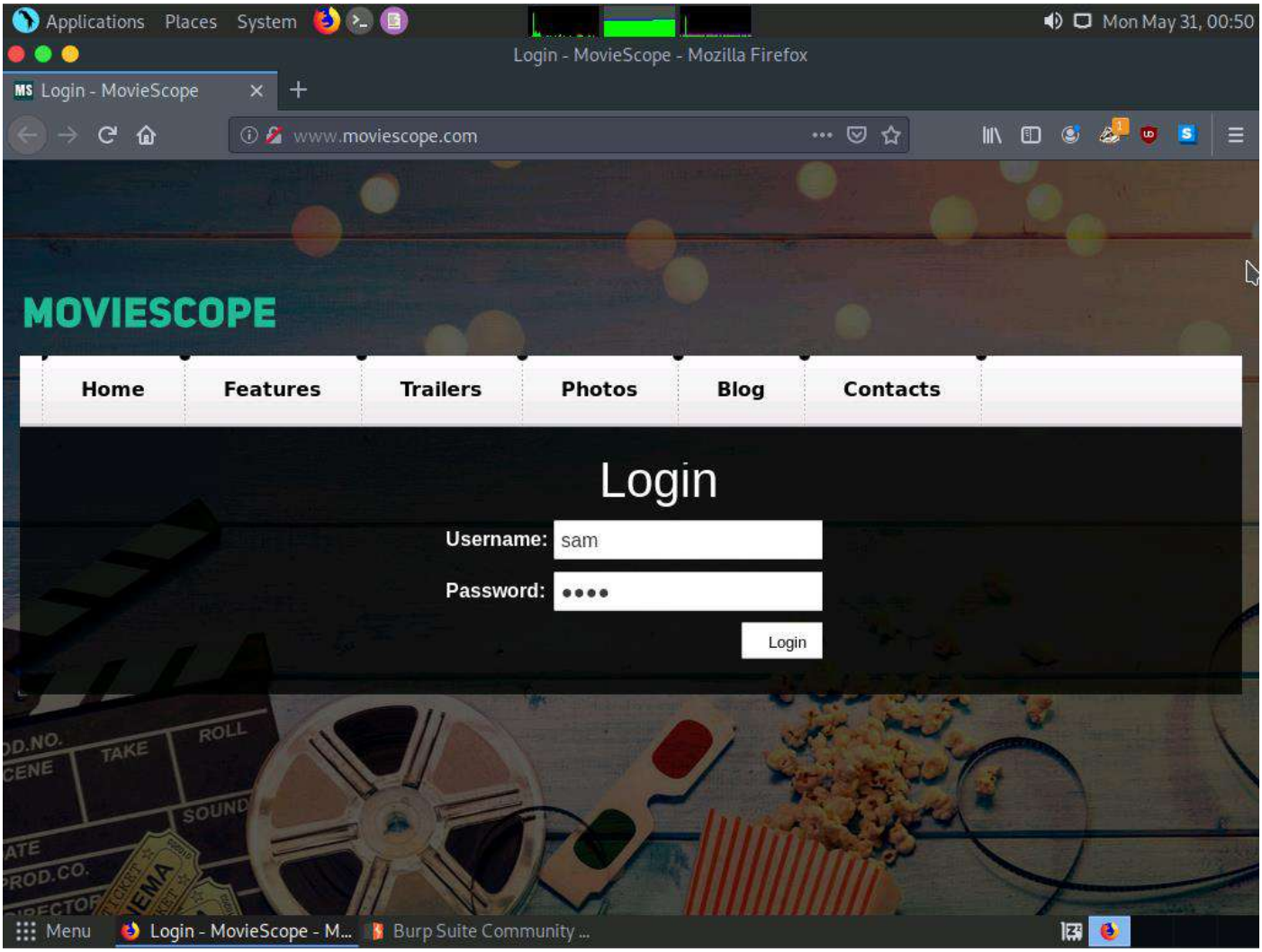
15. In the **Proxy** settings, by default, the **Intercept** tab opens-up. Observe that by default, the interception is active as the button says **Intercept is on**. Leave it running.

Turn the interception on if it is off.



16. Switch back to the browser window, and on the login page of the target website (**www.moviescope.com**), enter the credentials **sam** and **test**. Click the **Login** button.

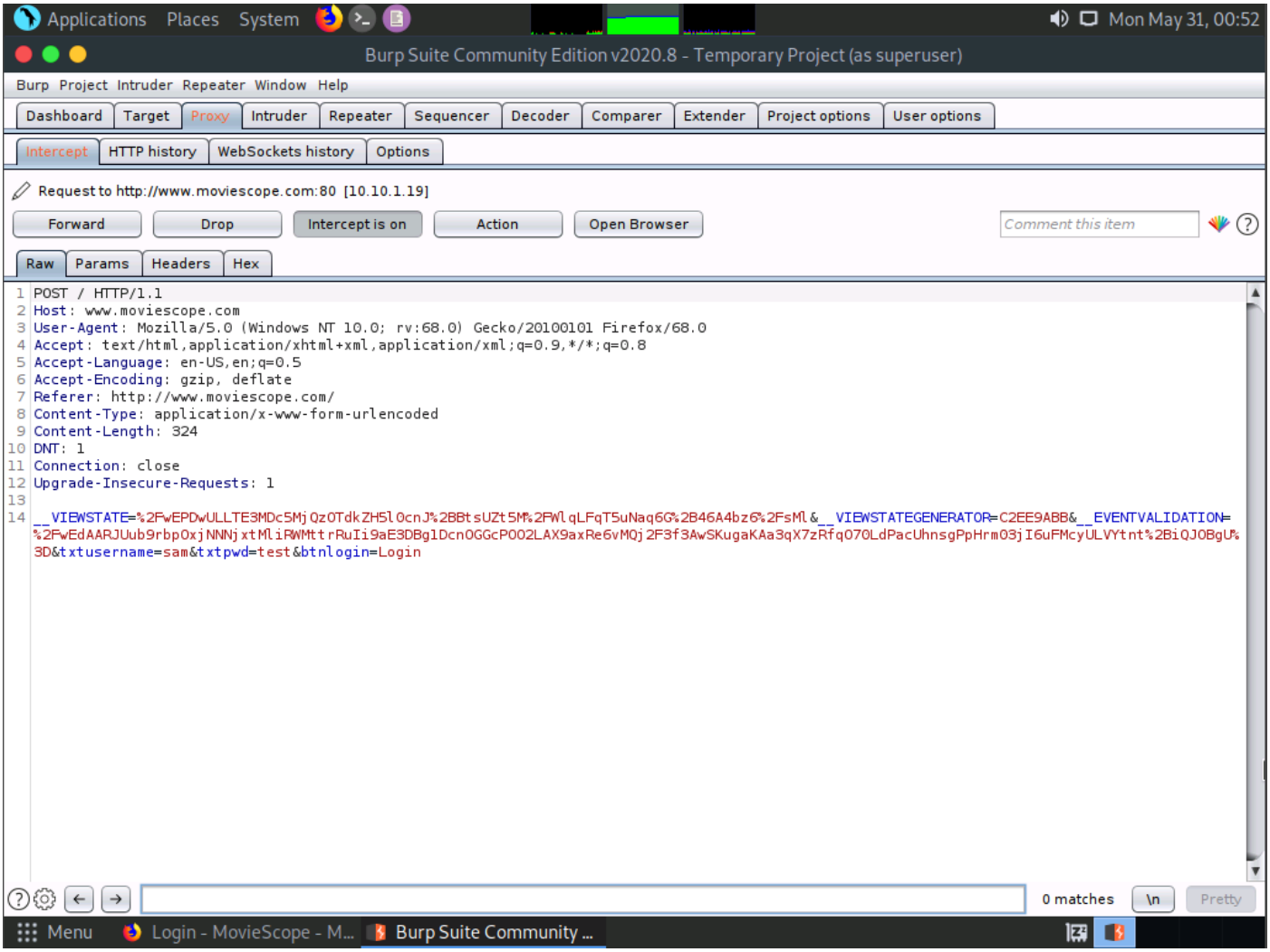
Here, we are logging in as a registered user on the website.



17. Switch back to the **Burp Suite** window and observe that the HTTP request was intercepted by the application.

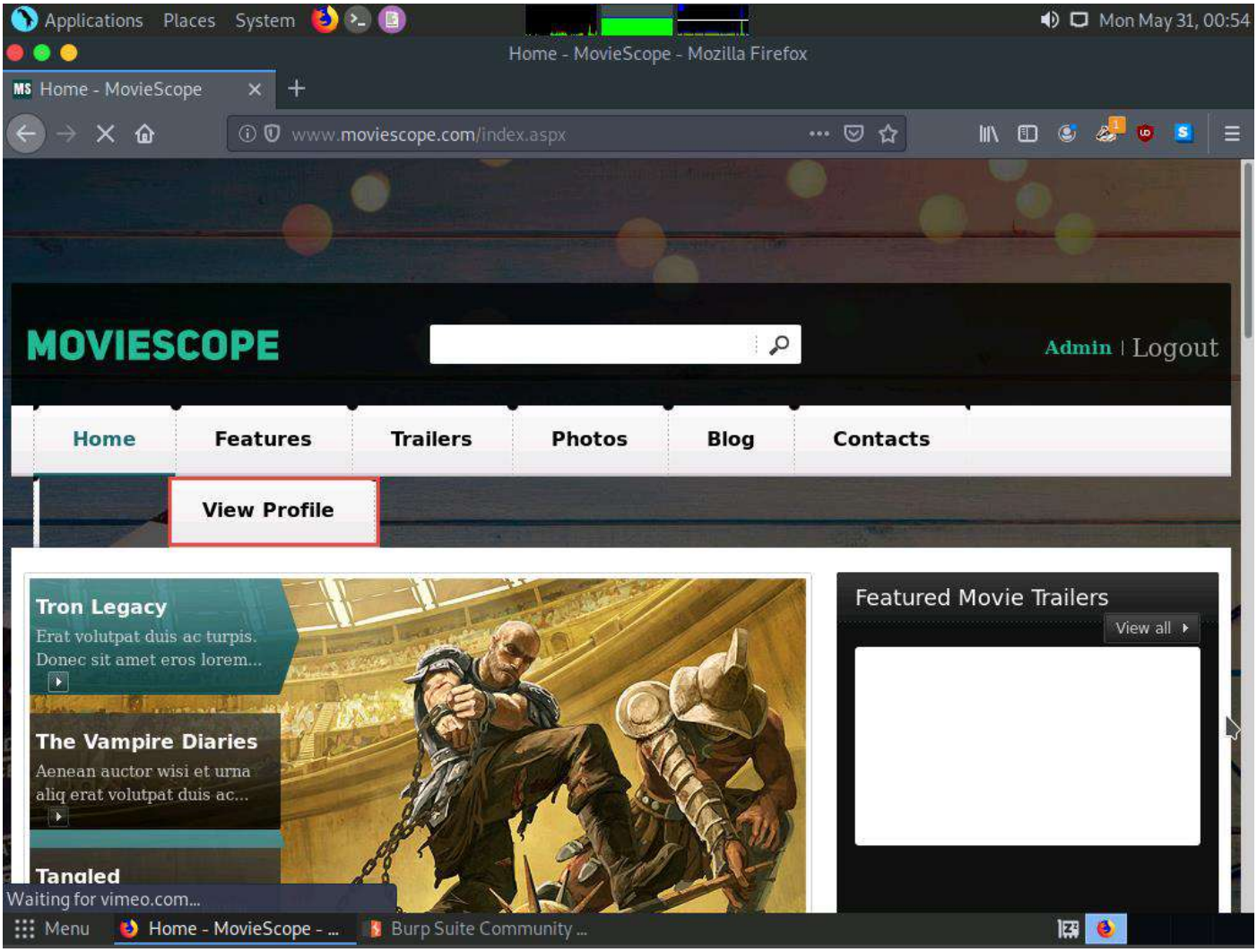
You can observe that the entered login credentials were intercepted by the Burp Suite.

18. Now, keep clicking the **Forward** button until you are logged into the user account.



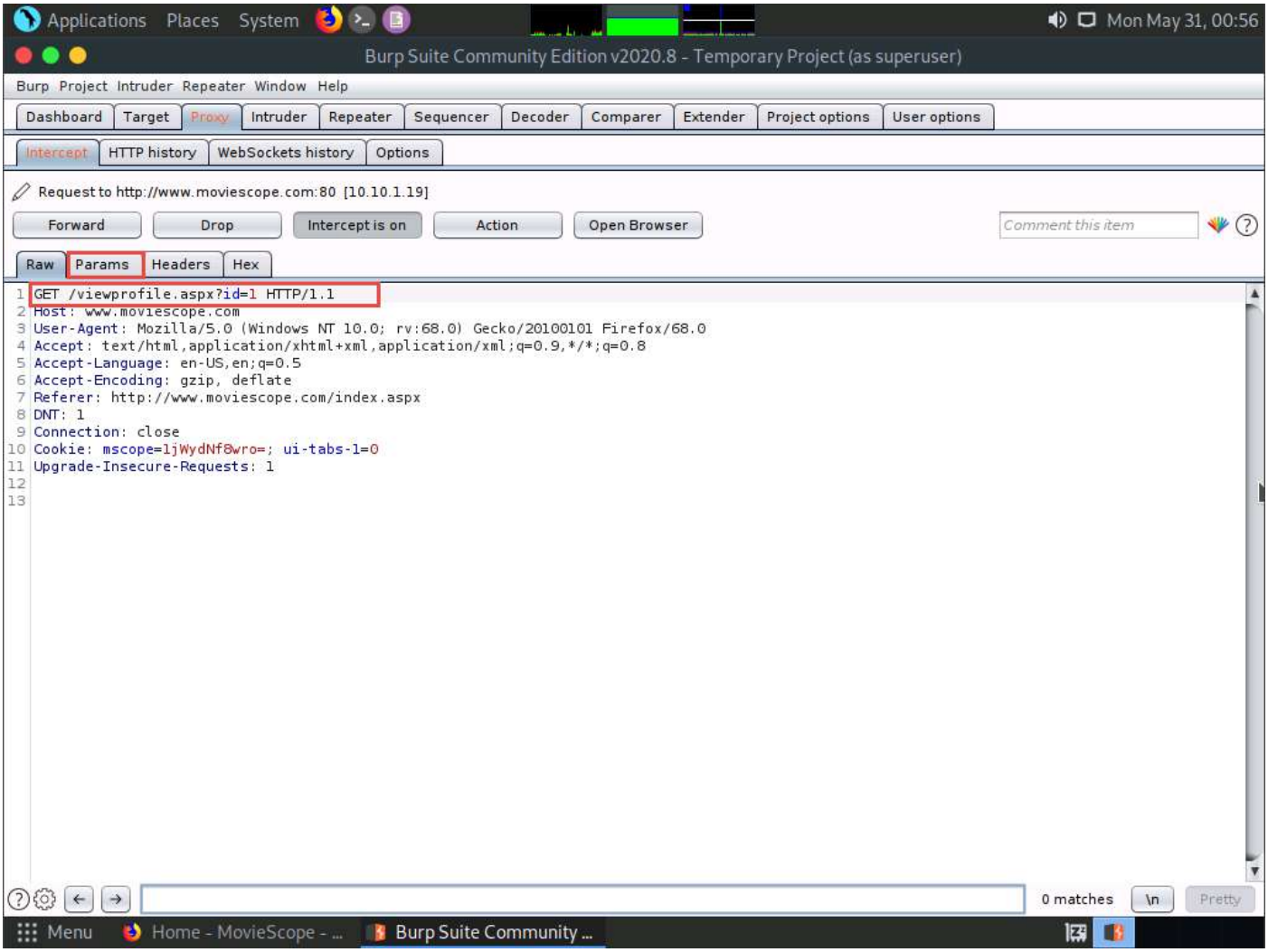
19. Switch to the browser, and observe that you are now logged into the user account, as shown in the screenshot.

20. Now, click the **View Profile** tab from the menu bar to view the user information.



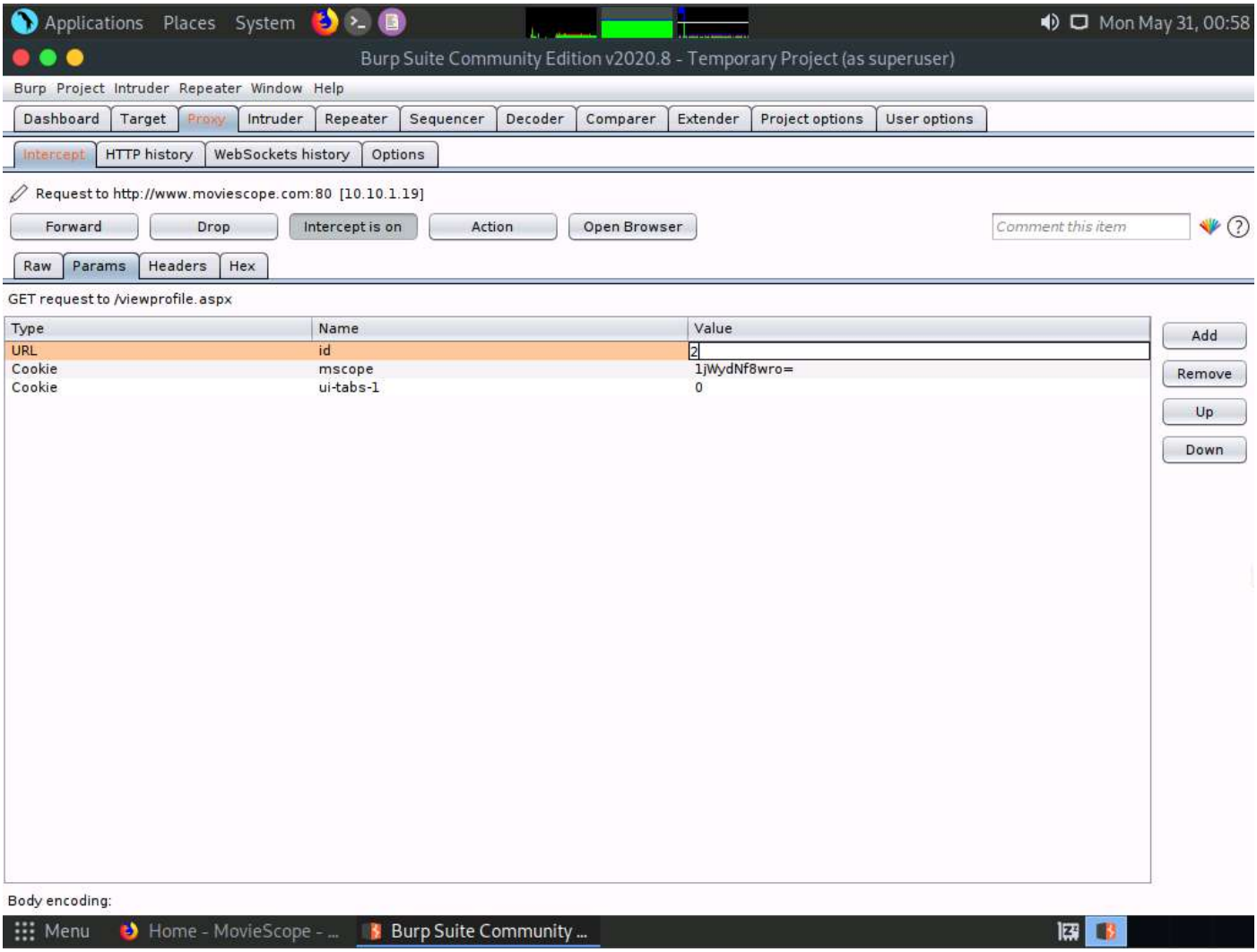
21. After clicking the **View Profile** tab, switch back to the **Burp Suite** window and keep clicking the **Forward** button until you get the HTTP request, as shown in the screenshot.

22. Now, navigate to the **Params** tab under the **Intercept** tab to view the captured parameters.

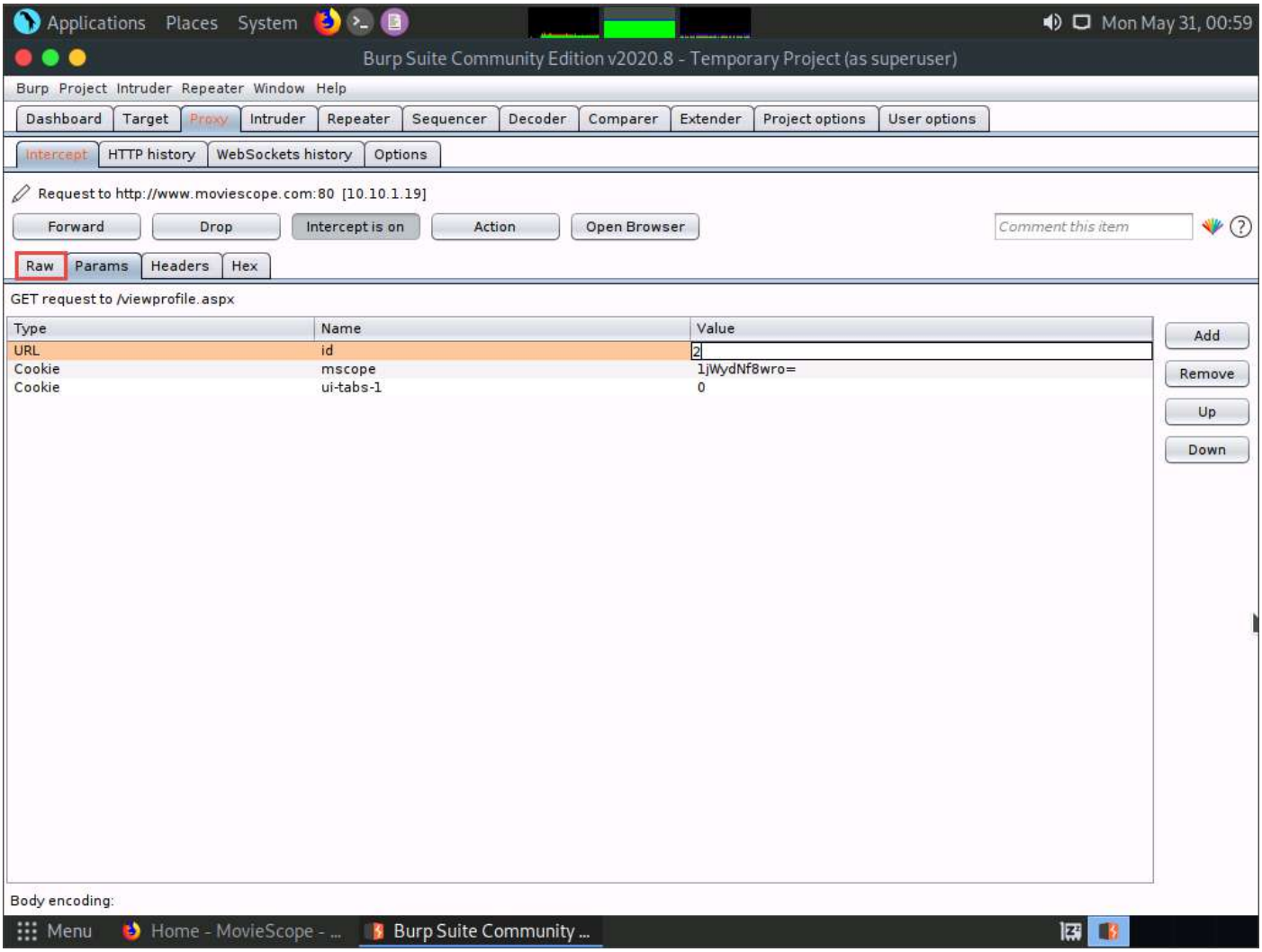


23. Under the **Params** tab, observe a table with captured values such as **URL** and **Cookie**.

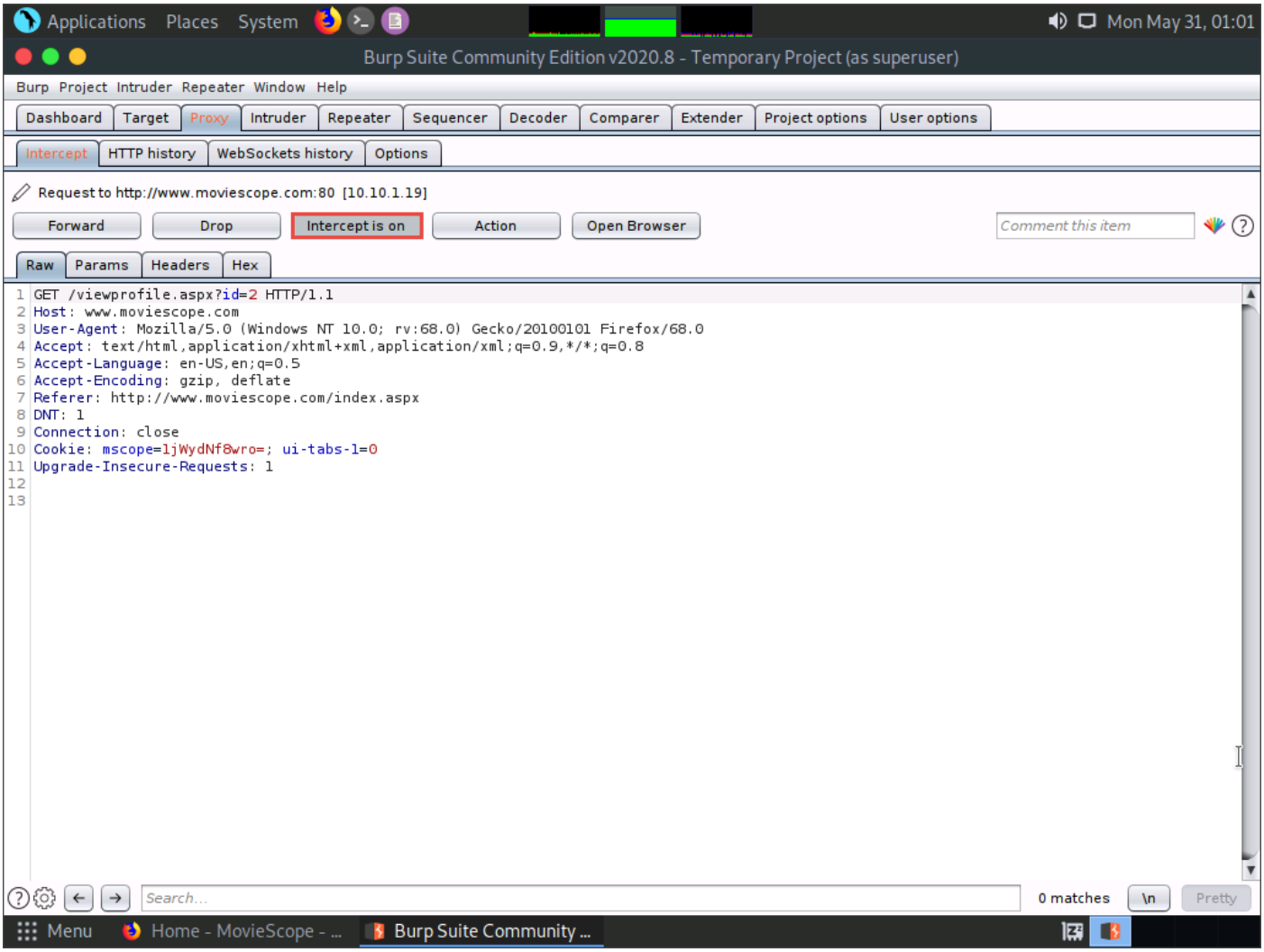
24. In the **URL** type with the name **id**, double-click the **Value** column to change it from **1** to **2**, as shown in the screenshot.



25. After changing the value, navigate back to the **Raw** tab.

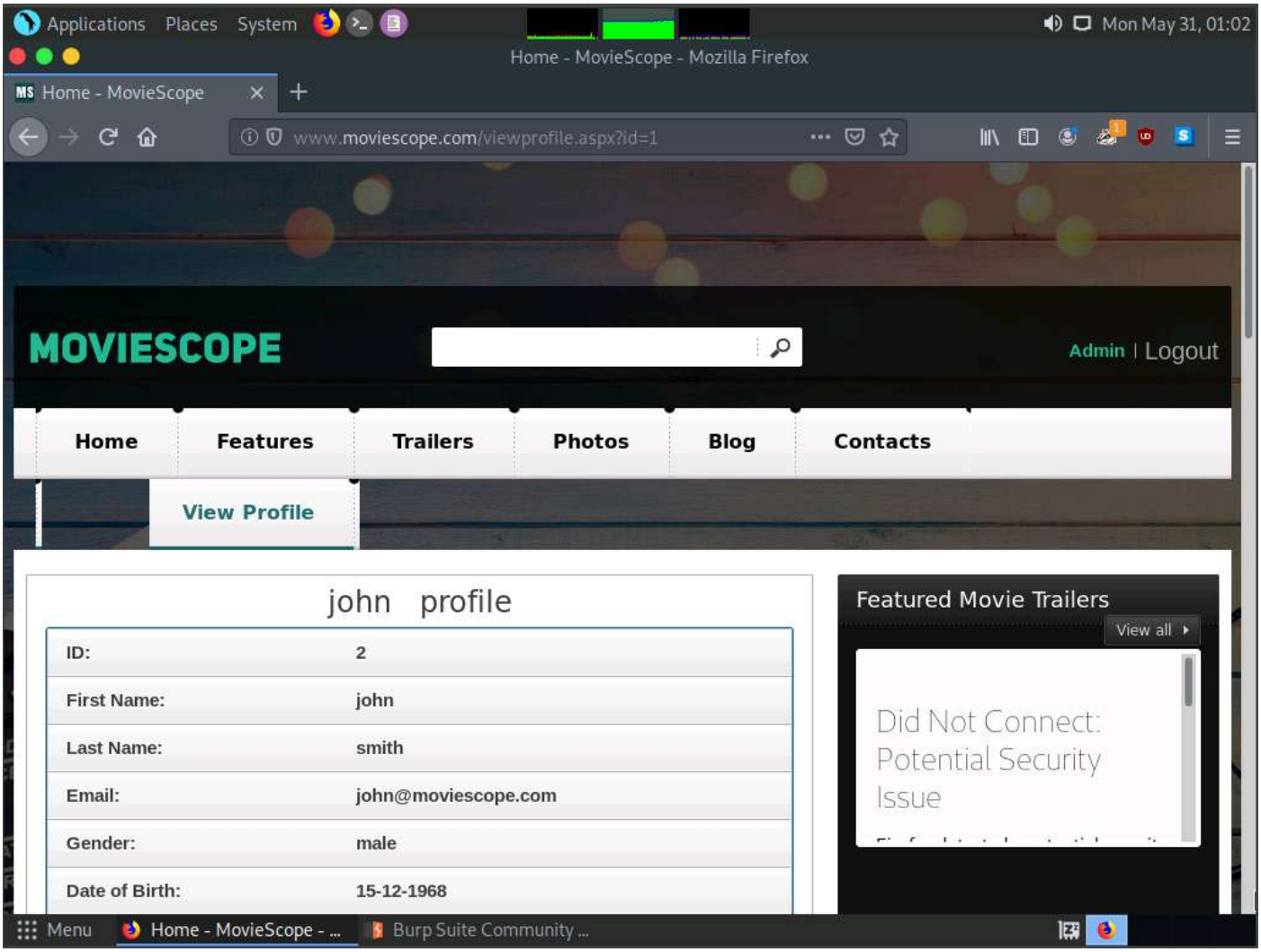


26. In the **Raw** tab, click the **Intercept is on** button to turn off the interception.



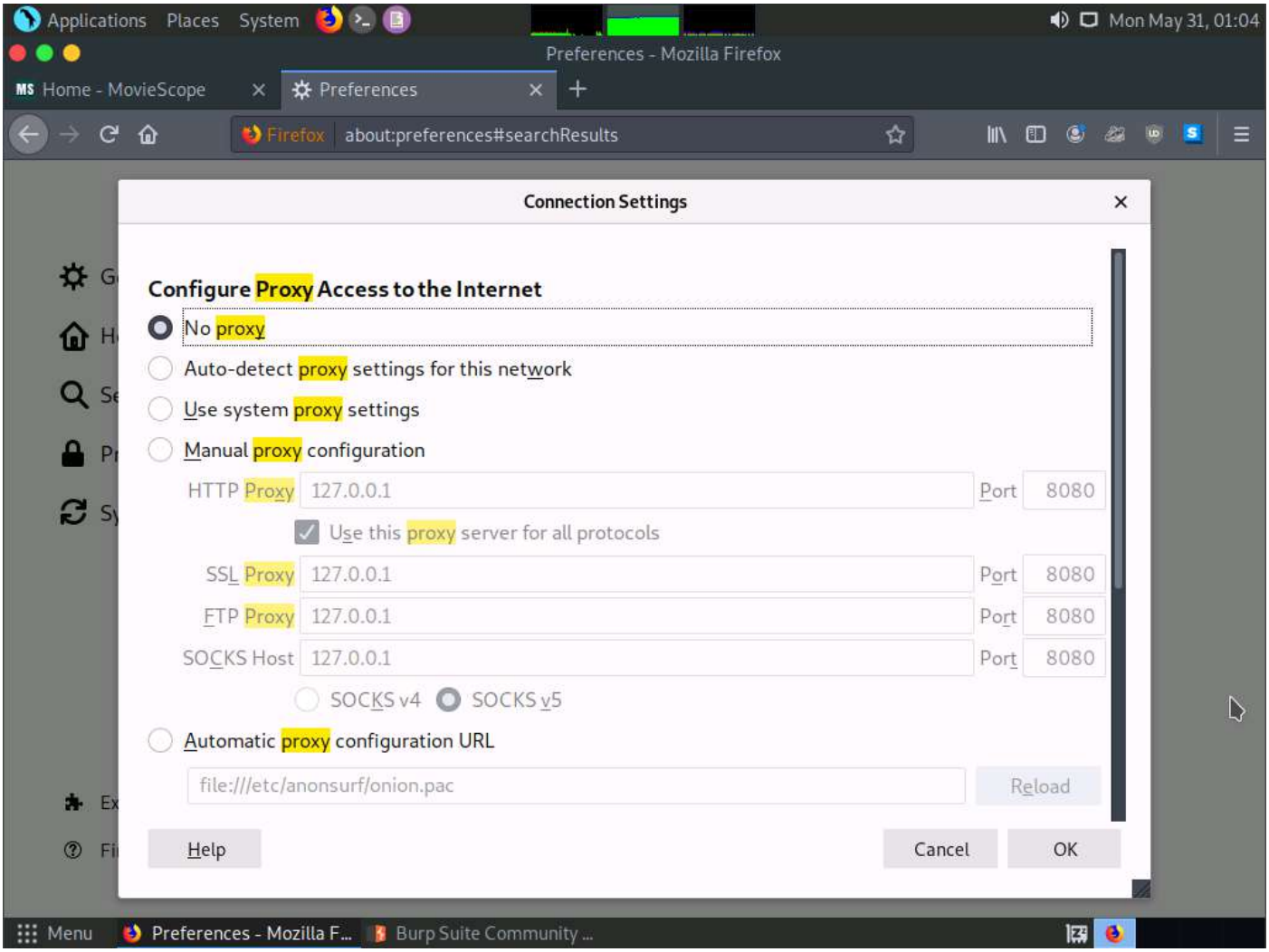
27. After switching off the interception, navigate back to the browser window and observe that the user account associated with **ID=2** appears with the name **John**, as shown in the screenshot.

Although we logged in using sam as a username with ID=1, using Burp Suite, we successfully tampered with the ID parameter to obtain information about other user accounts.



28. Similarly, you can edit the **id** parameter in Burp Suite with any random numeric value to view information about other user accounts.

29. Switch to the browser window and perform Steps **4-6**. Remove the browser proxy set up in **Step 7**, by selecting the **No proxy** radio-button in the Connection Settings window and click **OK**. Close the tab.



30. This concludes the demonstration of how to perform parameter tampering using Burp Suite.
31. Close all open windows and document all the acquired information.

Lab 7-3: Perform SQL Injection Attacks on a Target Web Application to Manipulate the Backend Database

Lab Scenario

SQL injection is an alarming issue for all database-driven websites. An attack can be attempted on any normal website or software package based on how it is used and how it processes user-supplied data. SQL injection attacks are performed on SQL databases with weak codes that do not adequately filter, use strong typing, or correctly execute user input. This vulnerability can be used by attackers to execute database queries to collect sensitive information, modify database entries, or attach malicious code, resulting in total compromise of the most sensitive data.

In order to assess the systems in your target network, you should test relevant web applications for various vulnerabilities and flaws, and then exploit those vulnerabilities to perform SQL injection attacks.

Lab Objectives

- Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap

Task 1: Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap

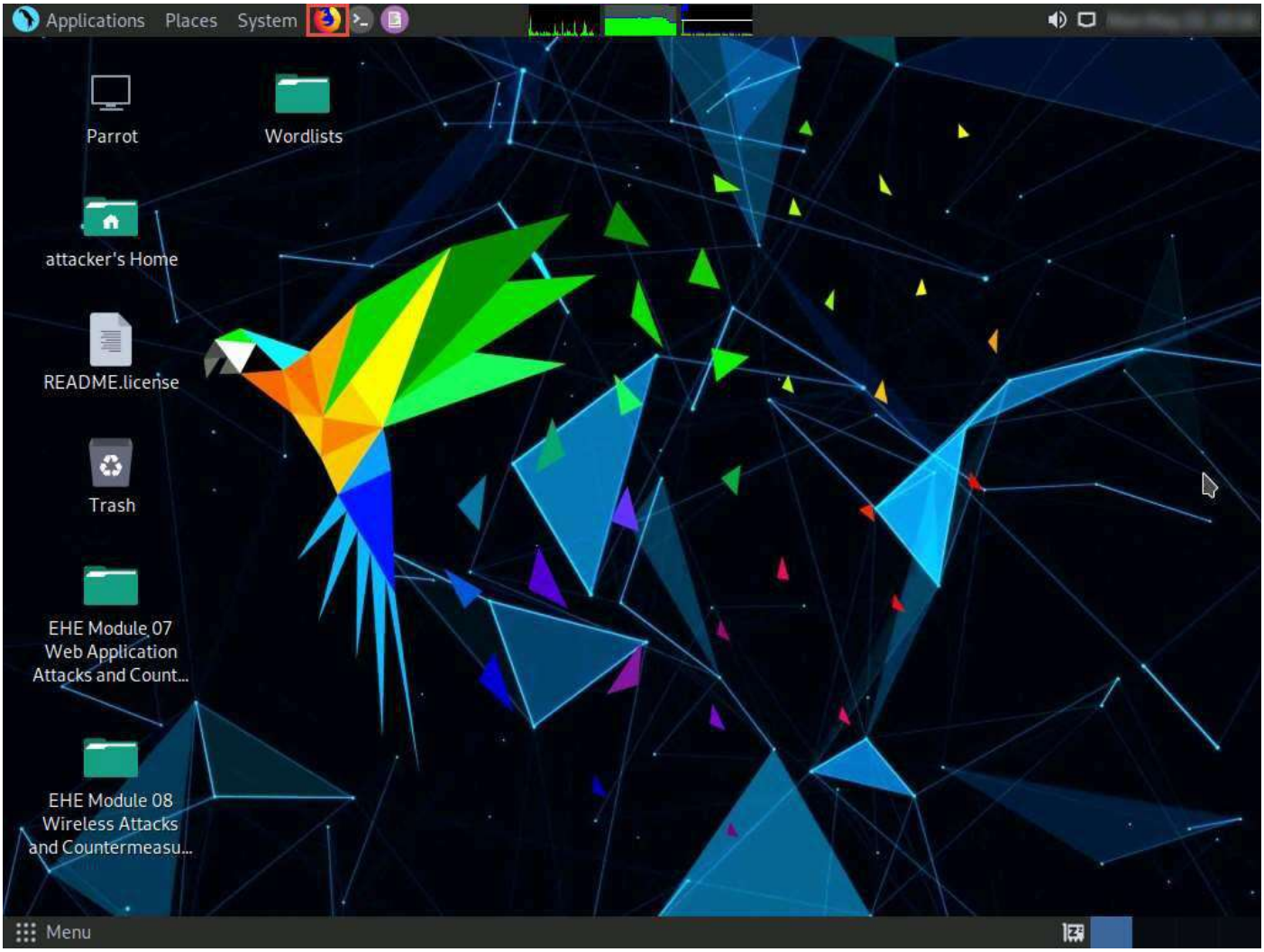
sqlmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features, and a broad range of switches—from database fingerprinting and data fetching from the database to accessing the underlying file system and executing commands on the OS via out-of-band connections.

You can use sqlmap to perform SQL injection on a target website using various techniques, including Boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries, and out-of-band SQL injection.

In this task, we will use sqlmap to perform SQL injection attack against MSSQL to extract databases.

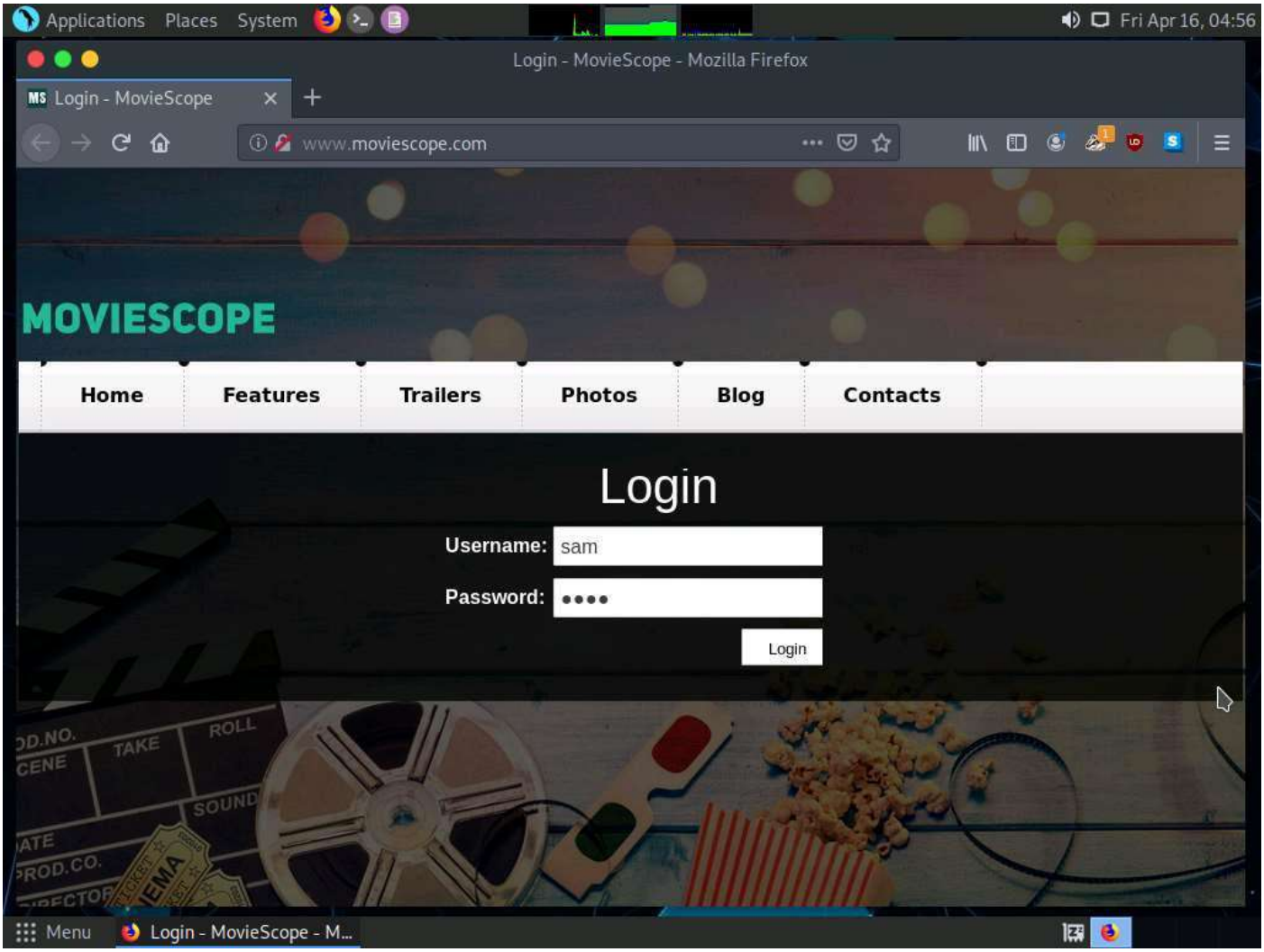
In this lab, you will pretend that you are a registered user on the **http://www.moviescope.com** website, and you want to crack the passwords of the other users from the website's database.

1. In **Parrot Security** machine, click the **Mozilla Firefox** icon from the menu bar in the top-left corner of **Desktop** to launch the web browser.

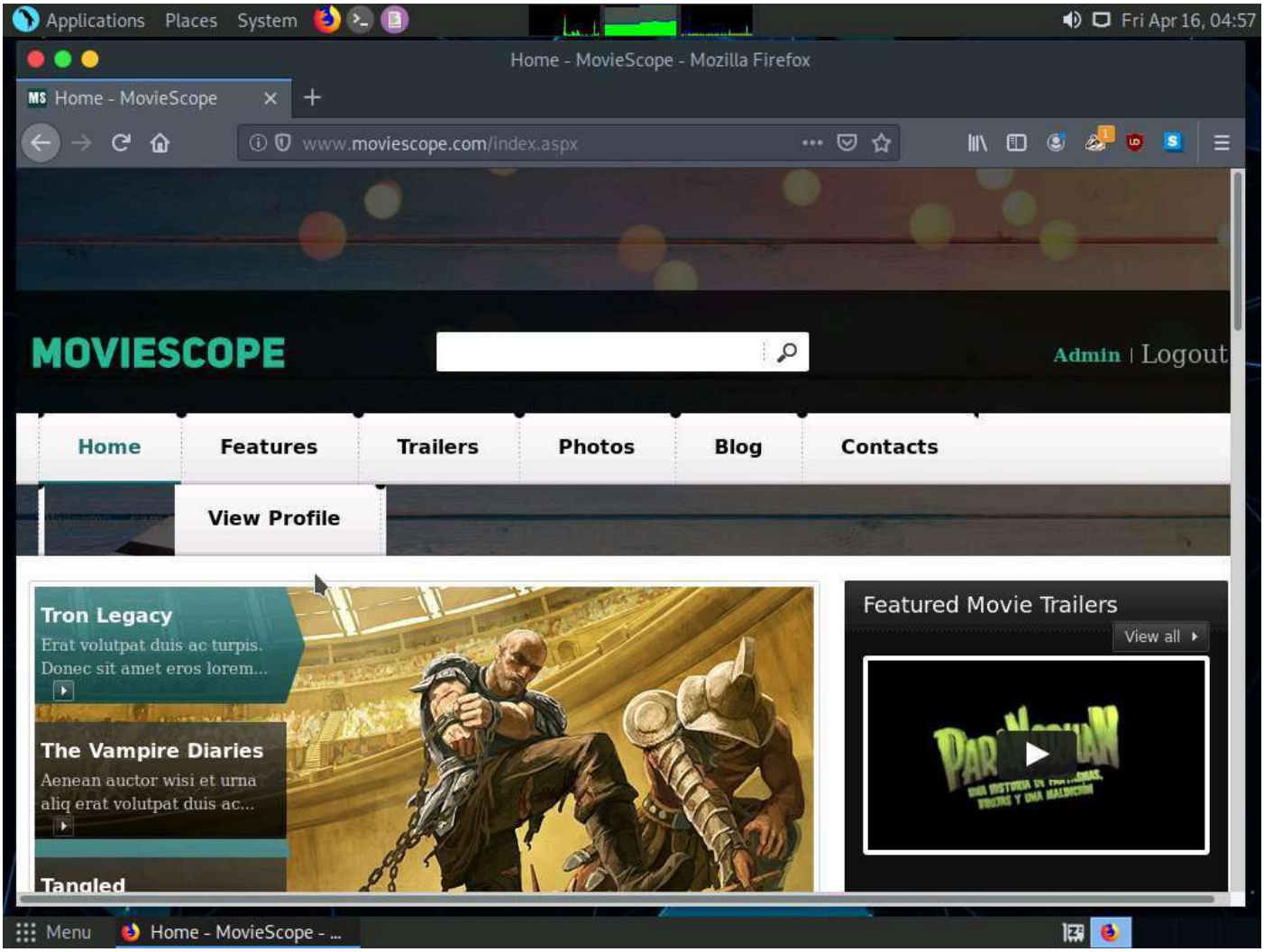


2. Type **http://www.moviescope.com/** and press **Enter**. A **Login** page loads; enter the **Username** and **Password** as **sam** and **test**, respectively. Click the **Login** button.

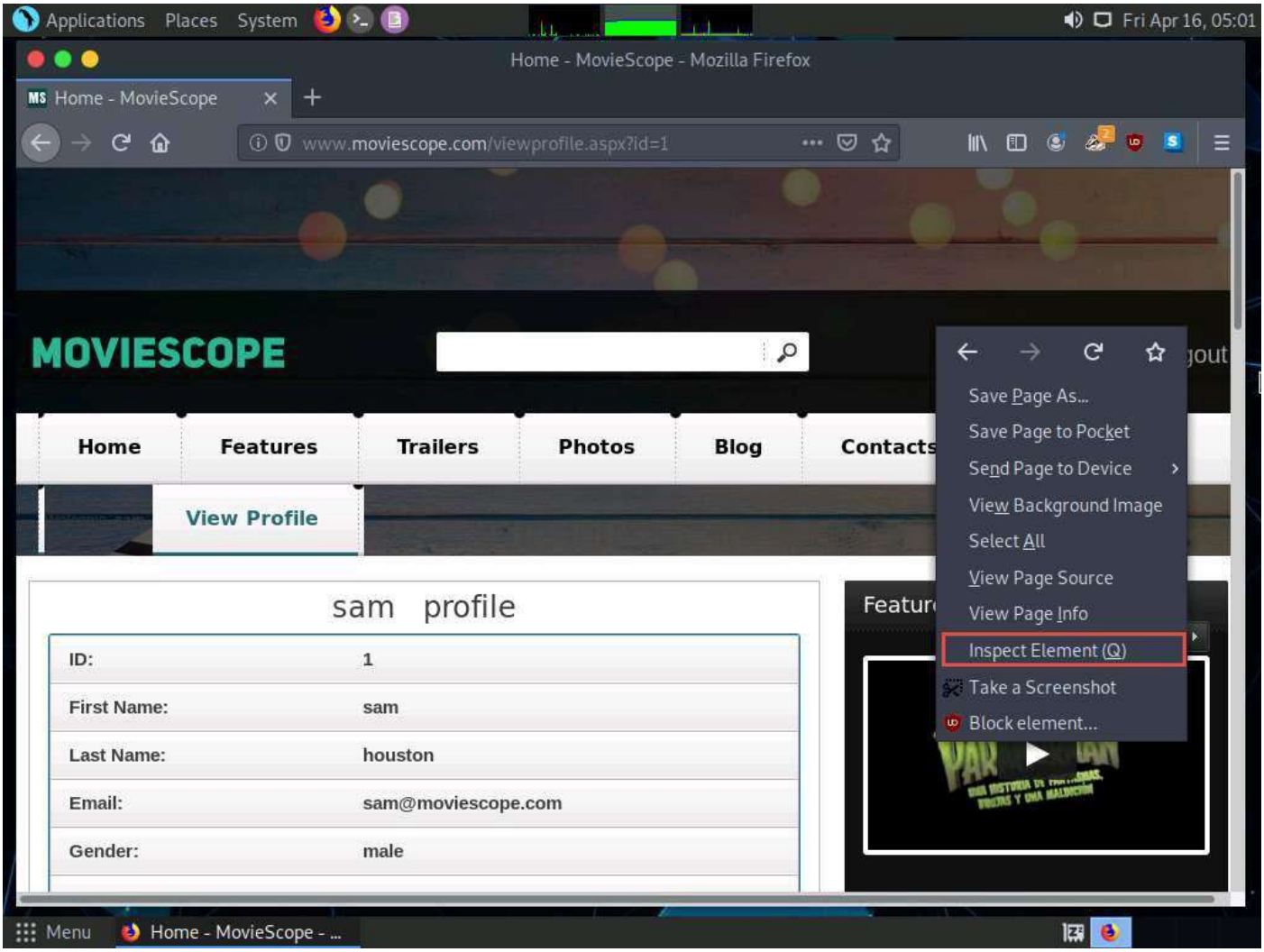
If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**.



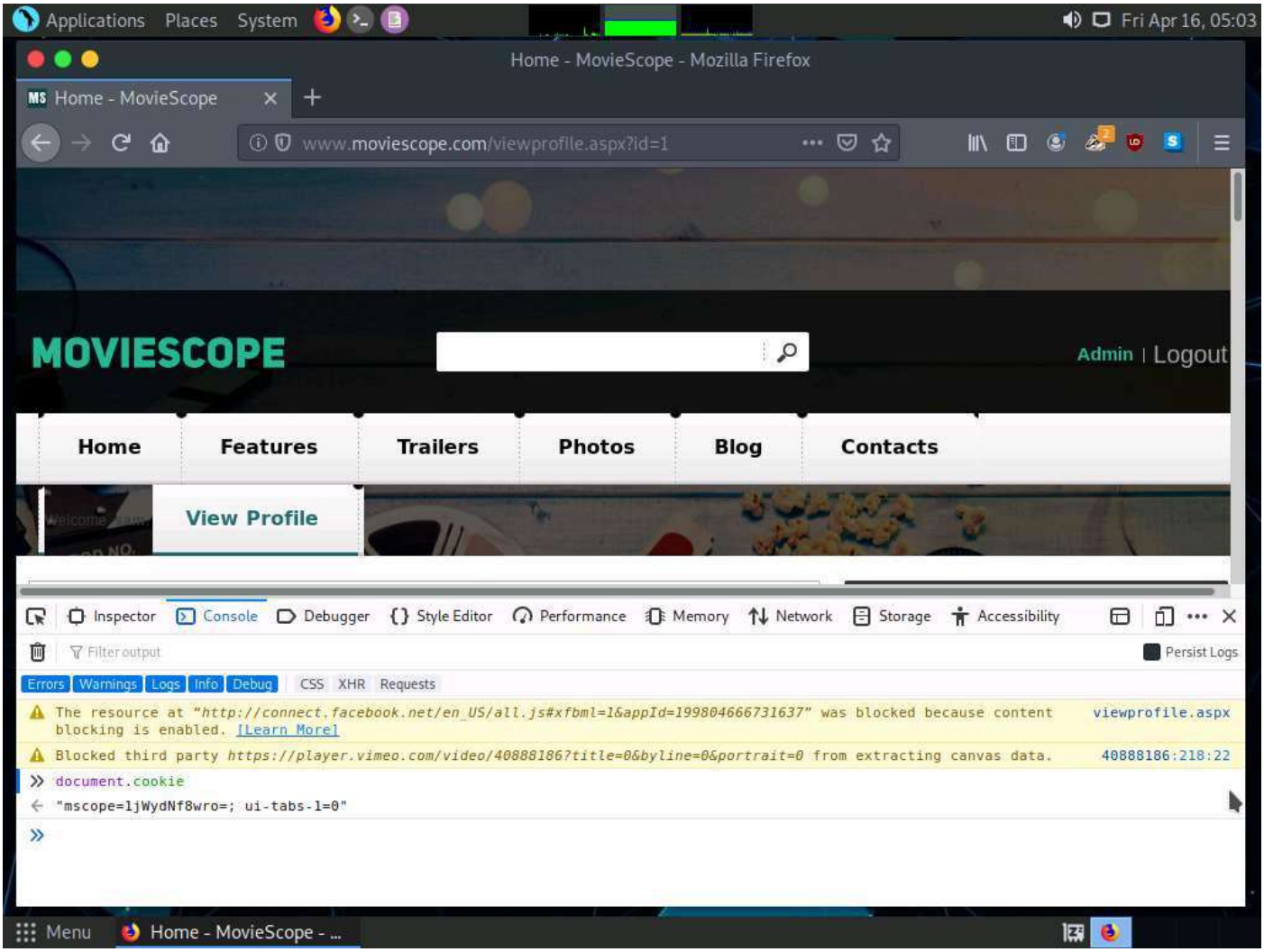
3. Once you are logged into the website, click the **View Profile** tab on the menu bar and, when the page has loaded, make a note of the URL in the address bar of the browser.



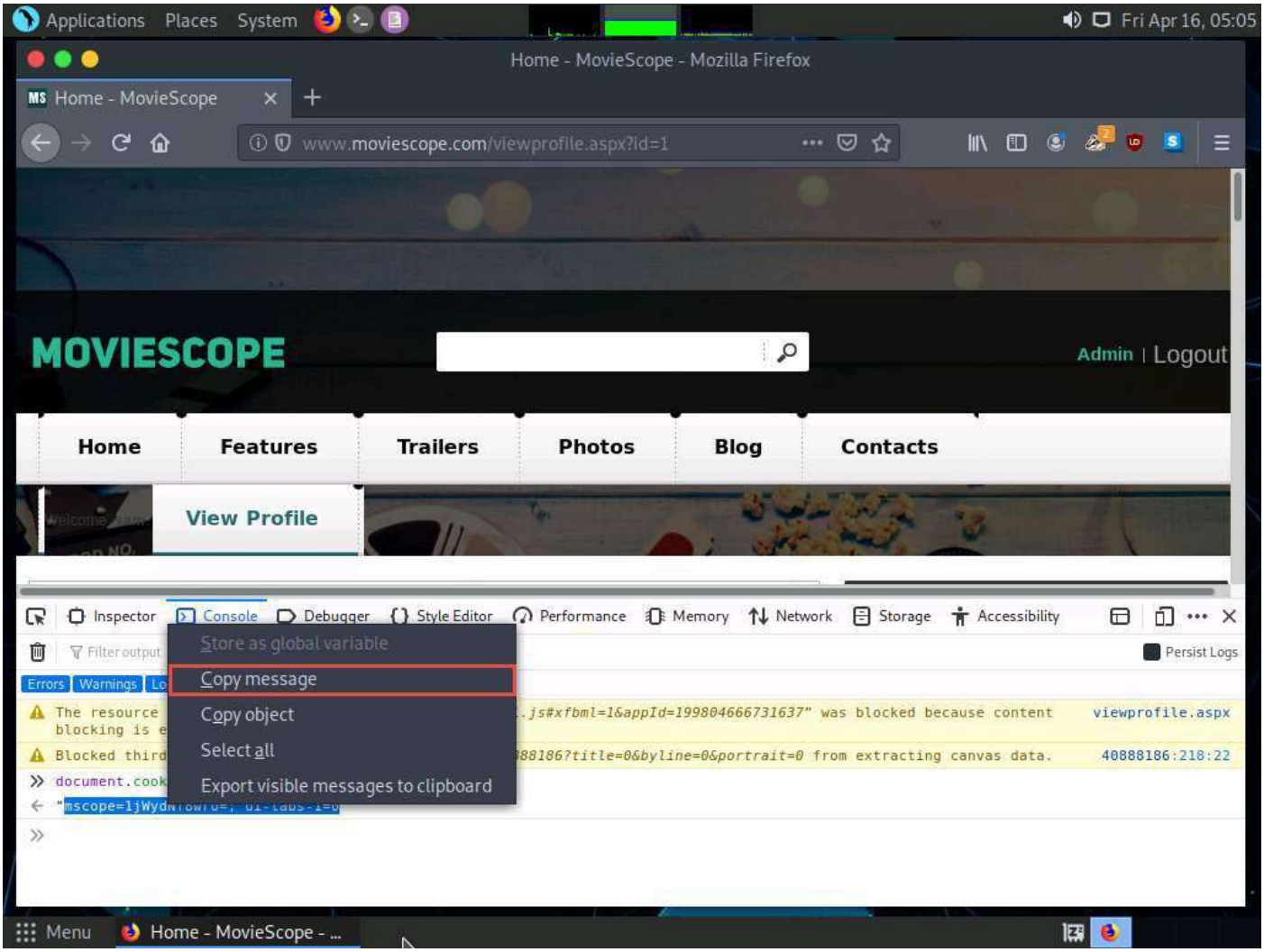
4. Right-click anywhere on the webpage and click **Inspect Element (Q)** from the context menu, as shown in the screenshot.



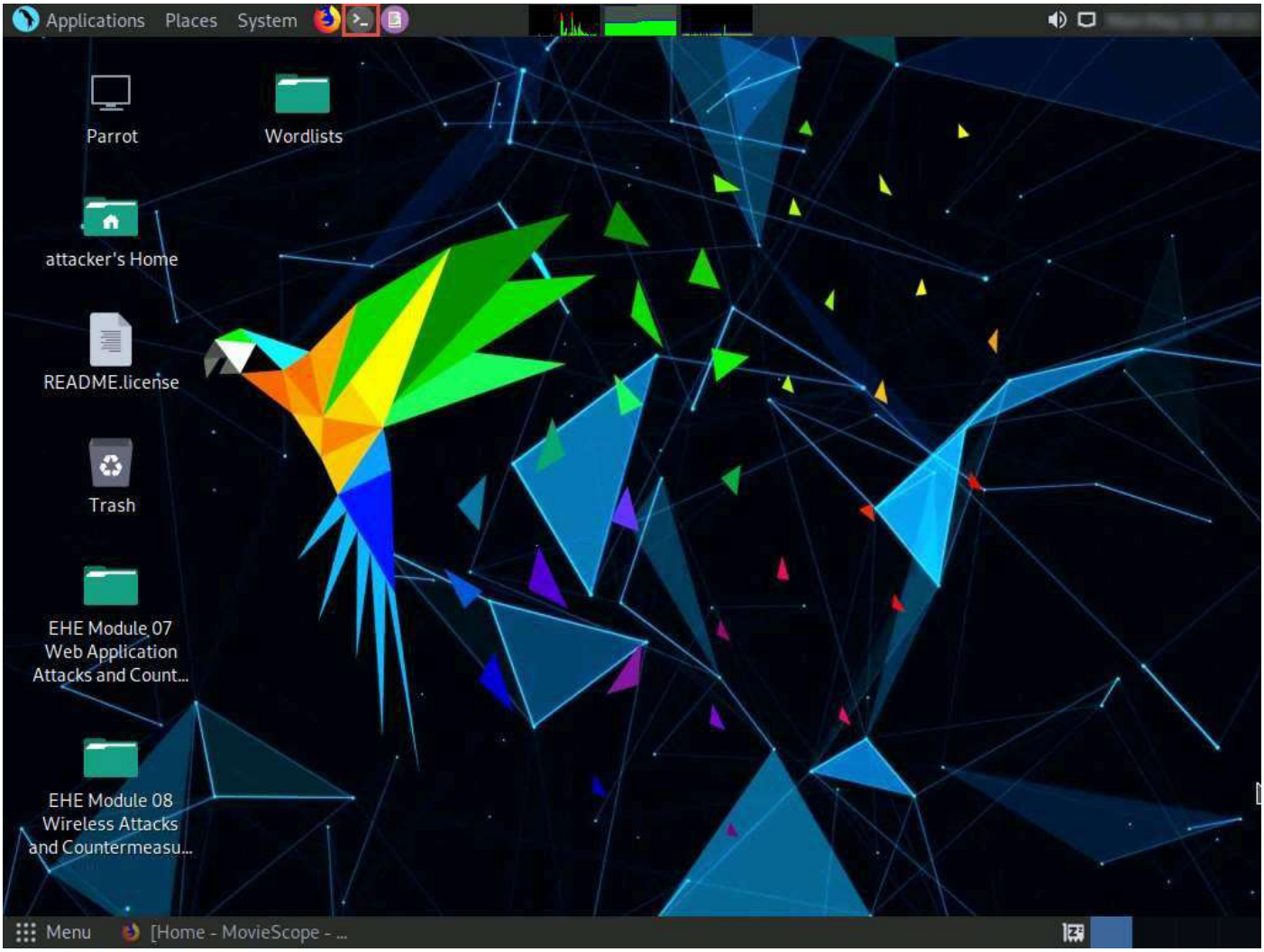
5. The **Developer Tools** frame appears in the lower section of the browser window. Click the **Console** tab, type **document.cookie** in the lower-left corner of the browser, and press **Enter**.



6. Select the cookie value, then right-click and copy it by clicking on **Copy message**, as shown in the screenshot. Minimize the web browser.



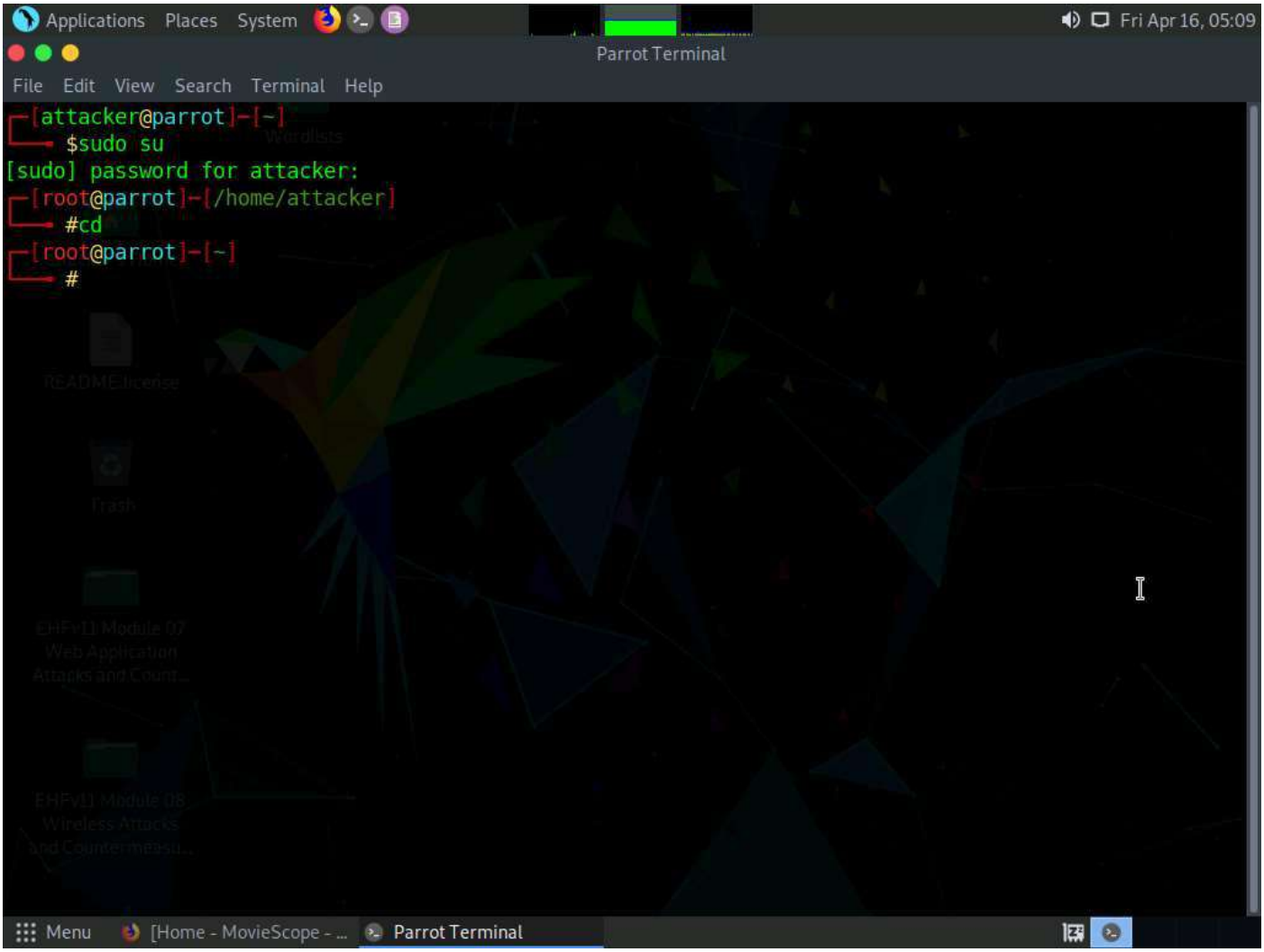
7. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Parrot Terminal** window.



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

The password that you type will not be visible.

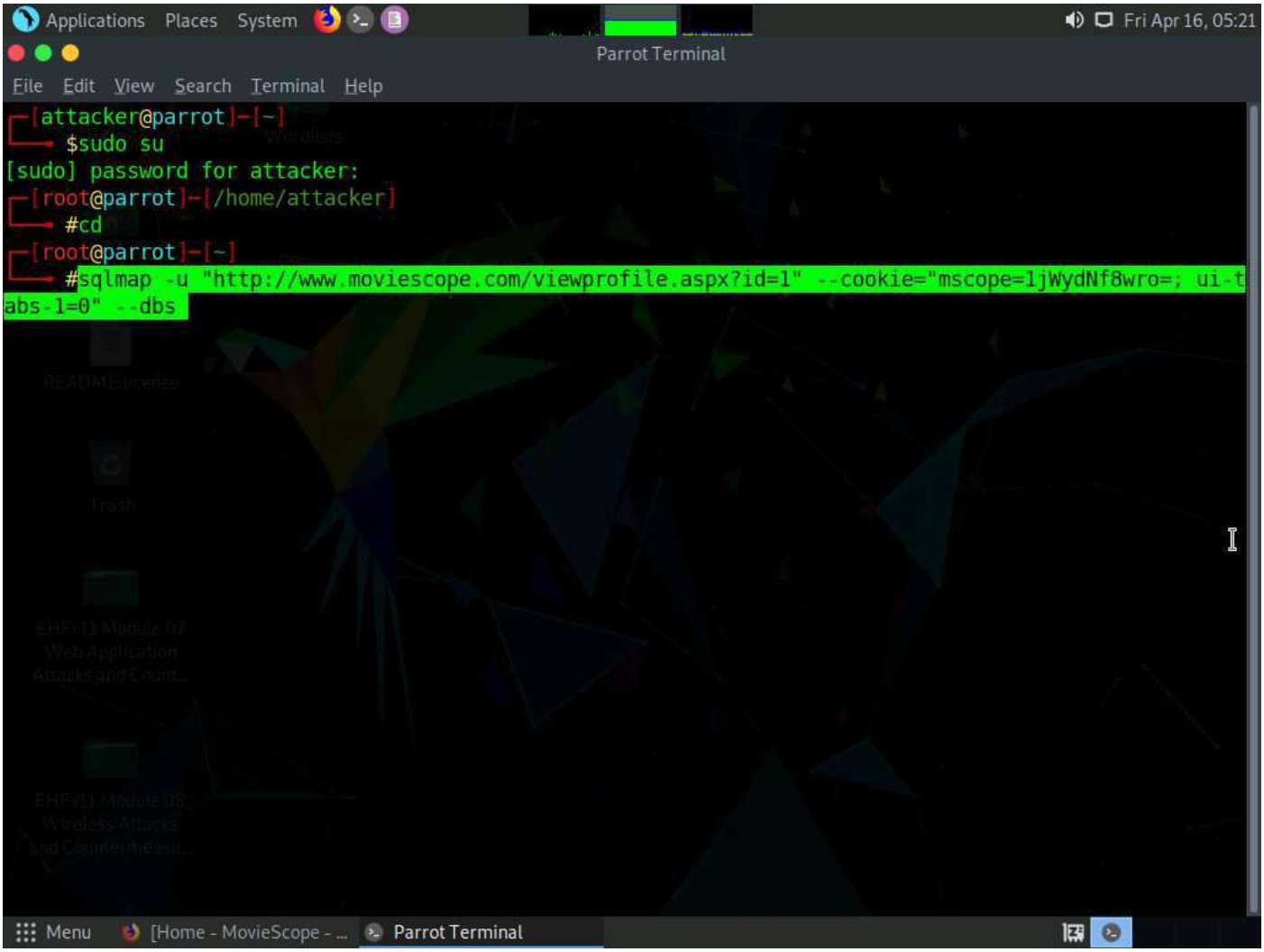
10. Now, type **cd** and press **Enter** to jump to the root directory.



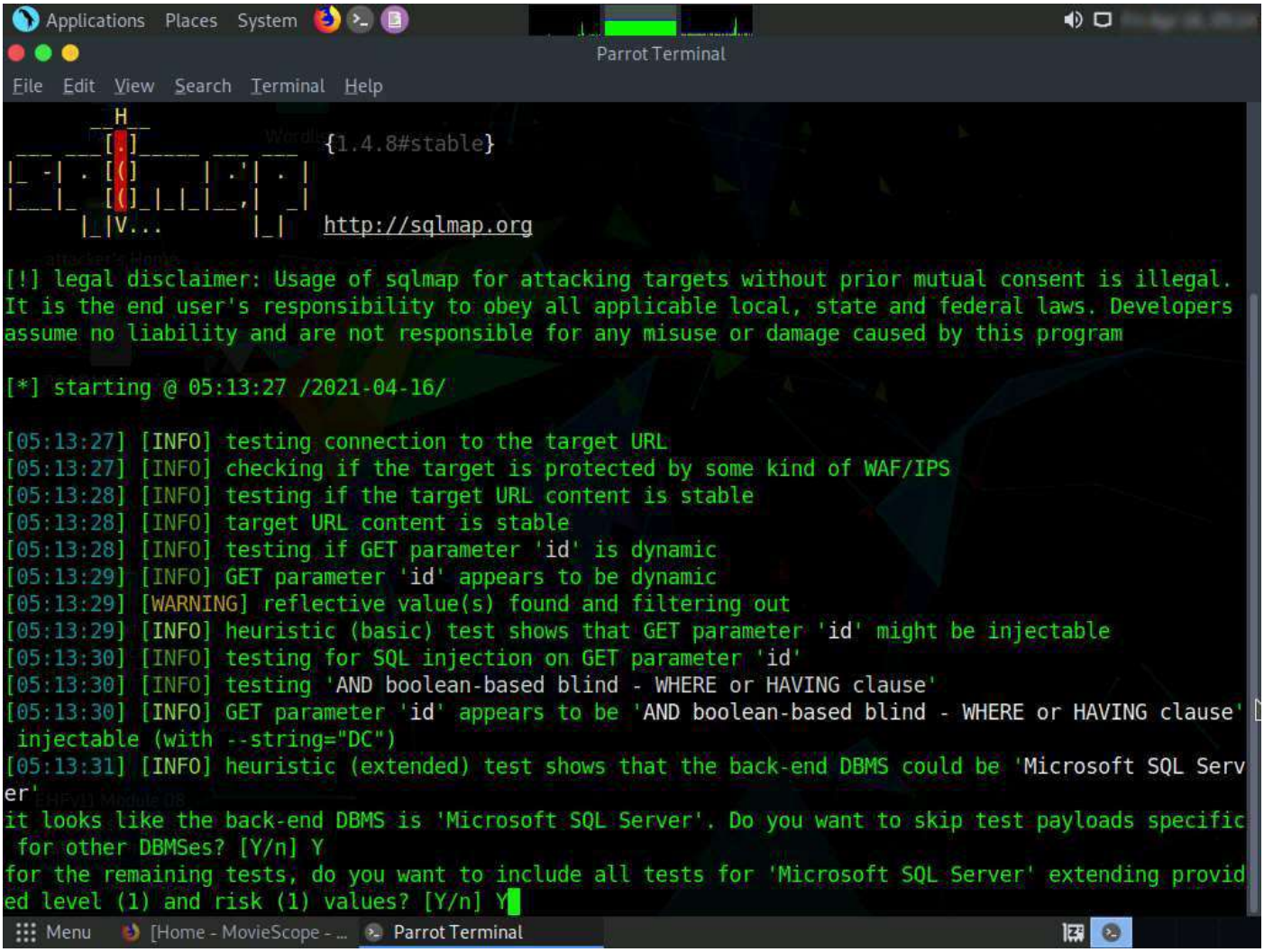
11. In the **Parrot Terminal** window, type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value that you copied in Step 6]" --dbs** and press **Enter**.

In this query, **-u** specifies the target URL (the one you noted down in Step 4), **--cookie** specifies the HTTP cookie header value, and **--dbs** enumerates DBMS databases.

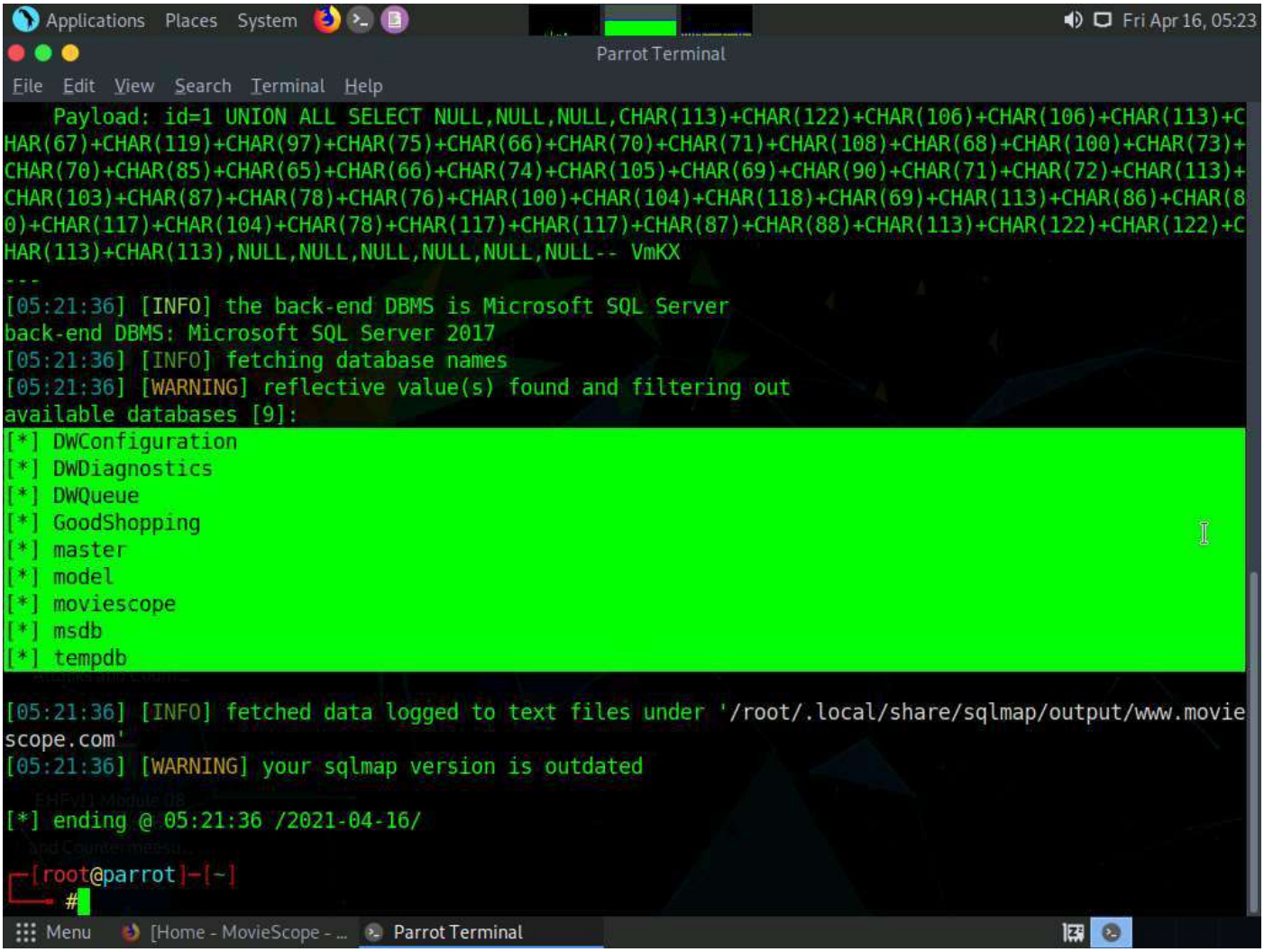
12. The above query causes sqlmap to enforce various injection techniques on the name parameter of the URL in an attempt to extract the database information of the **MovieScope** website.



13. If the message **Do you want to skip test payloads specific for other DBMSes? [Y/n]** appears, type **Y** and press **Enter**.
14. If the message **for the remaining tests, do you want to include all tests for 'Microsoft SQL Server' extending provided level (1) and risk (1) values? [Y/n]** appears, type **Y** and press **Enter**.
15. Similarly, if any other message appears, type **Y** and press **Enter** to continue.



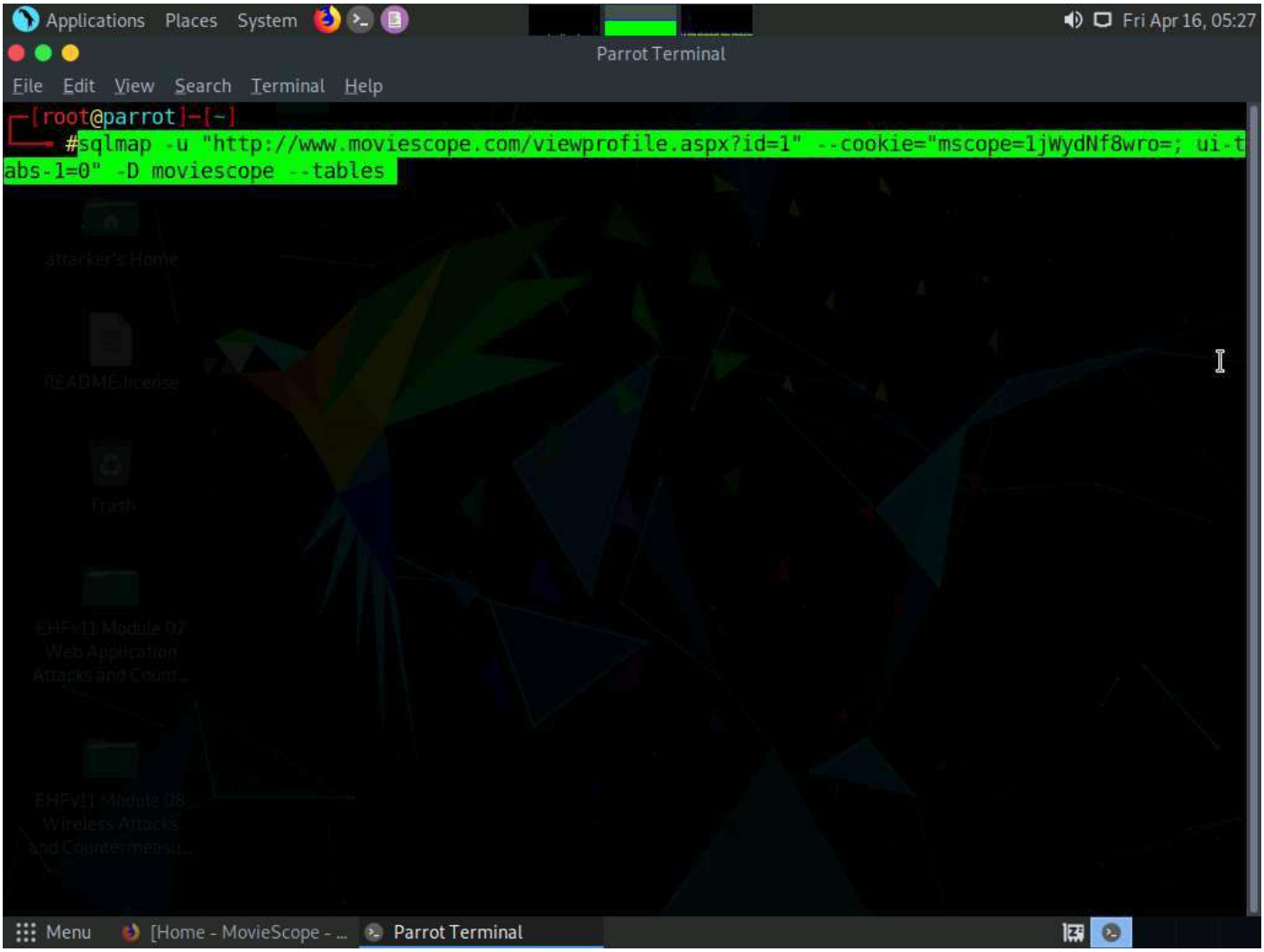
16. sqlmap retrieves the databases present in the MSSQL server. It also displays information about the web server OS, web application technology, and the backend DBMS, as shown in the screenshot.



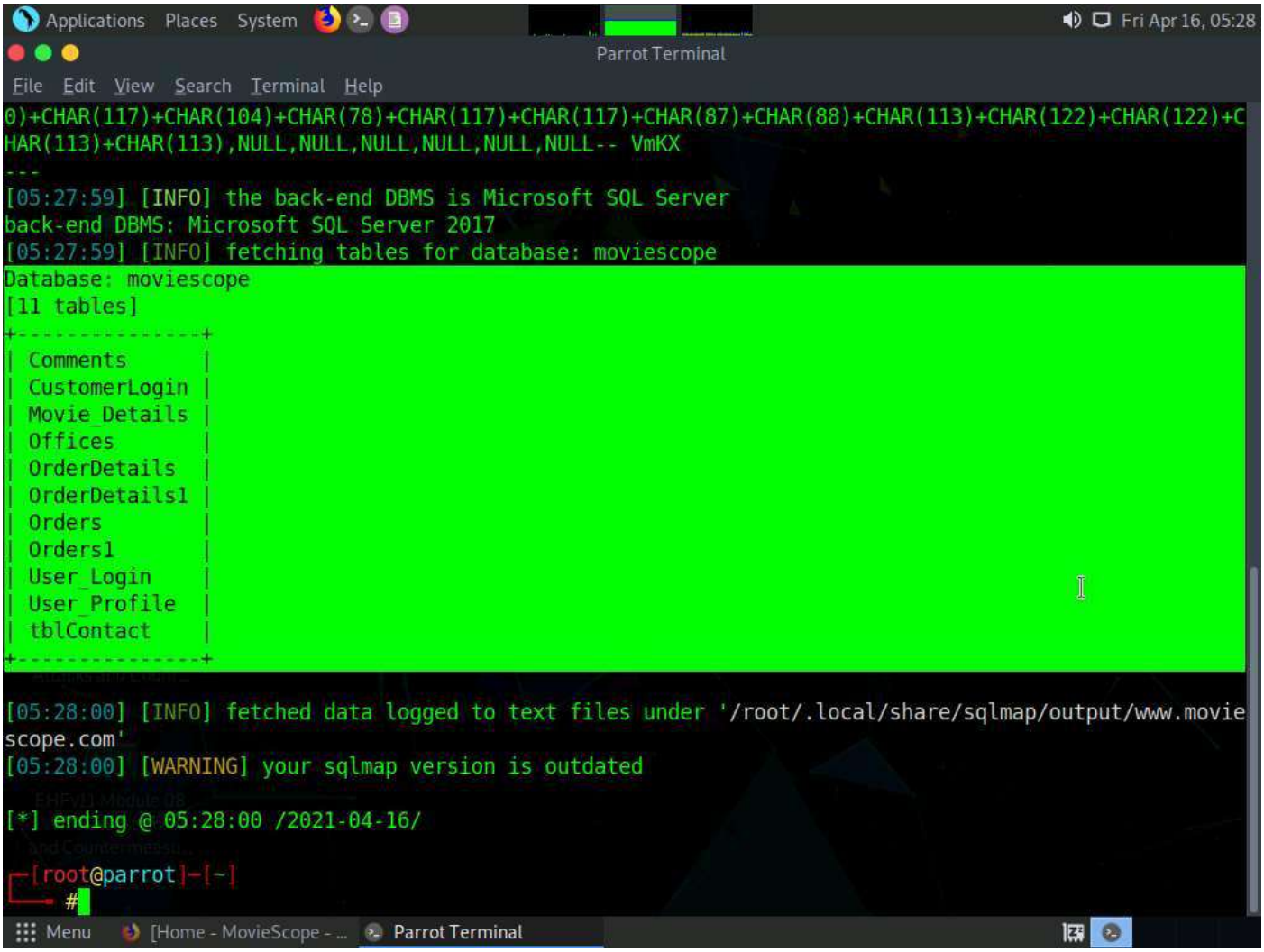
17. Now, you need to choose a database and use sqlmap to retrieve the tables in the database. In this lab, we are going to determine the tables associated with the database **moviescope**.
18. Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 6]" -D moviescope --tables** and press **Enter**.

In this query, **-D** specifies the DBMS database to enumerate and **--tables** enumerates DBMS database tables.

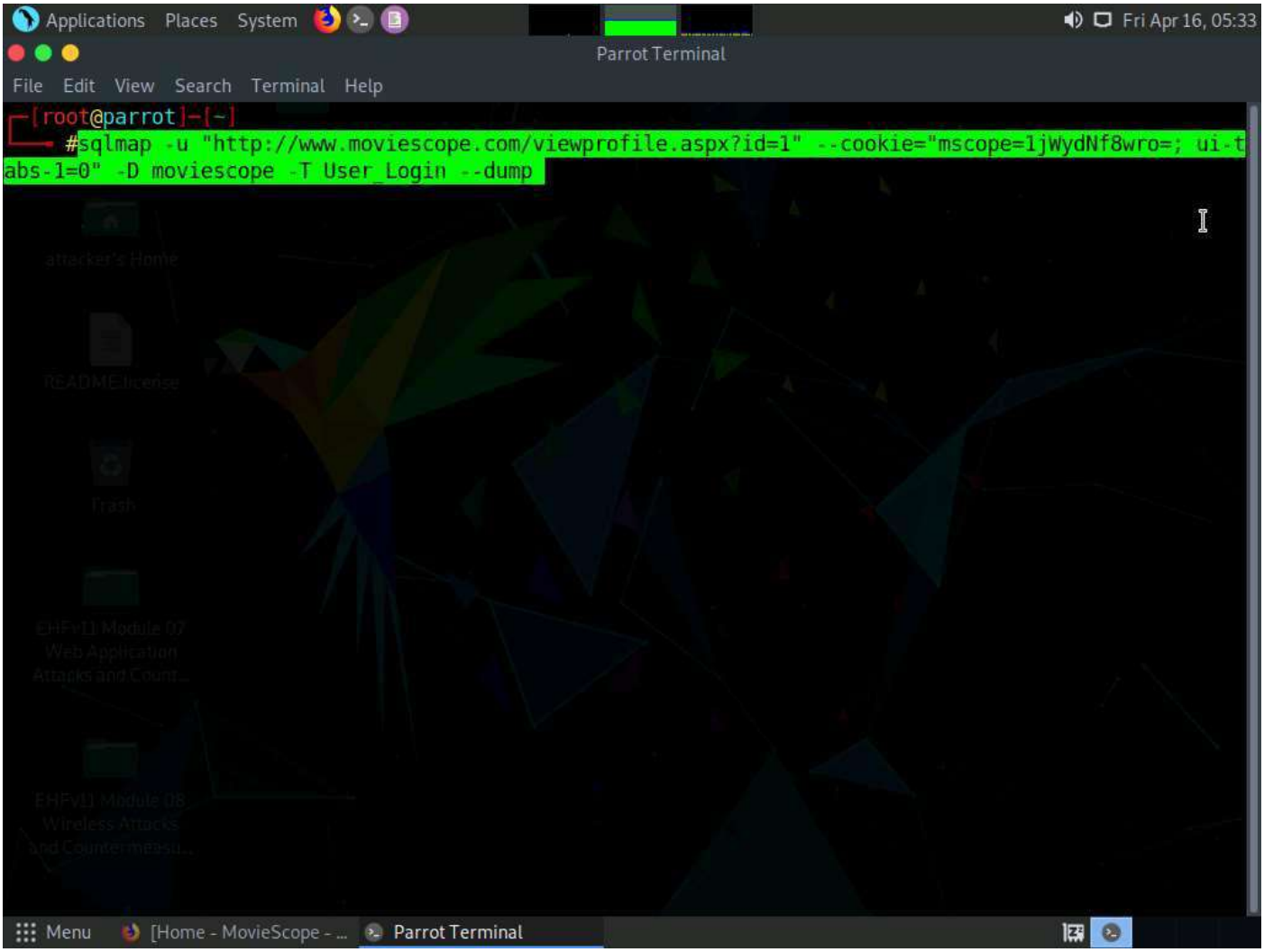
19. The above query causes sqlmap to scan the **moviescope** database for tables located in the database.



20. sqlmap retrieves the table contents of the moviescope database and displays them, as shown in screenshot.

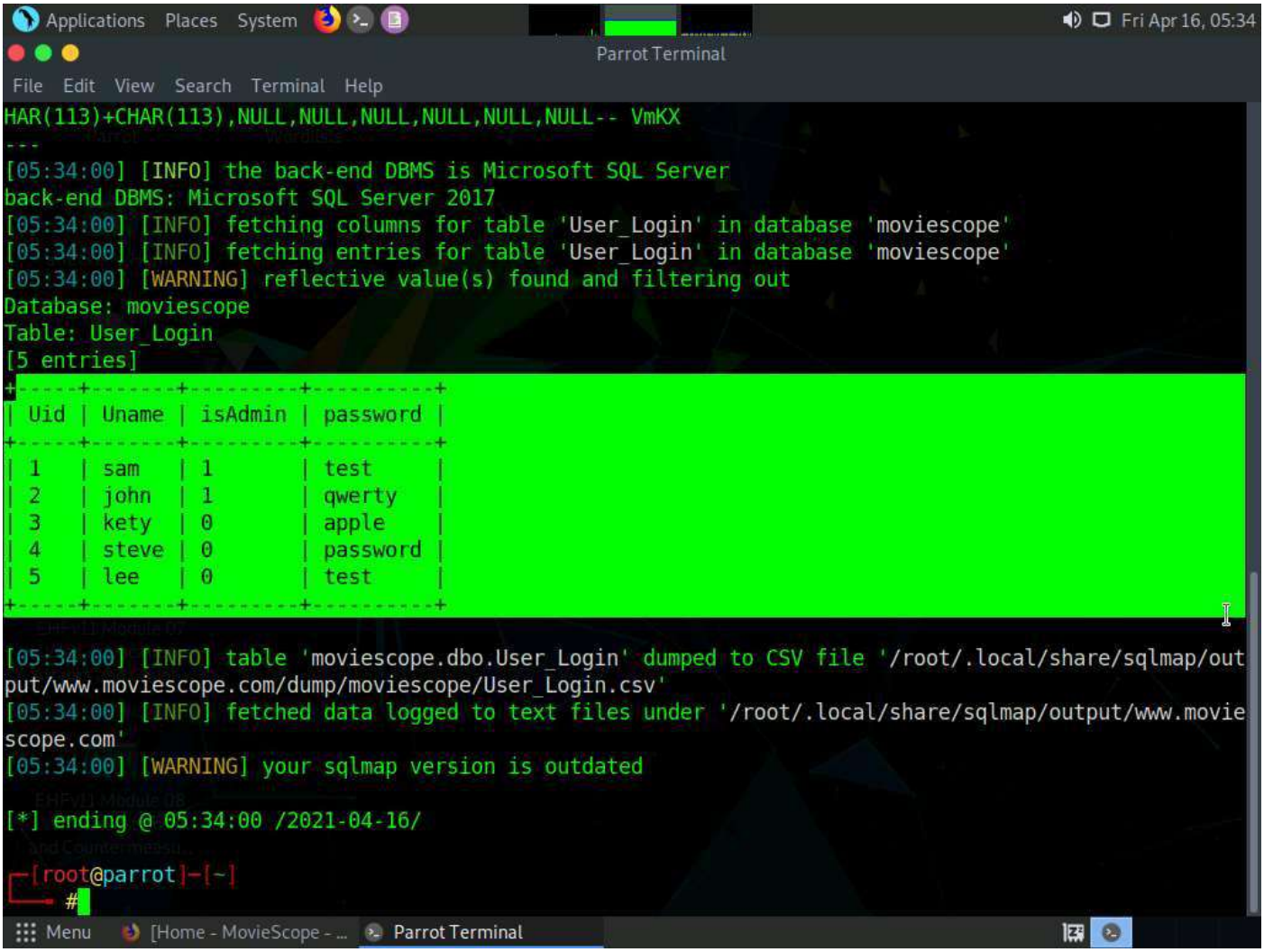


21. Now, you need to retrieve the table content of the column **User_Login**.
22. Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 6]" -D moviescope -T User_Login --dump** and press **Enter** to dump all the **User_Login** table content.

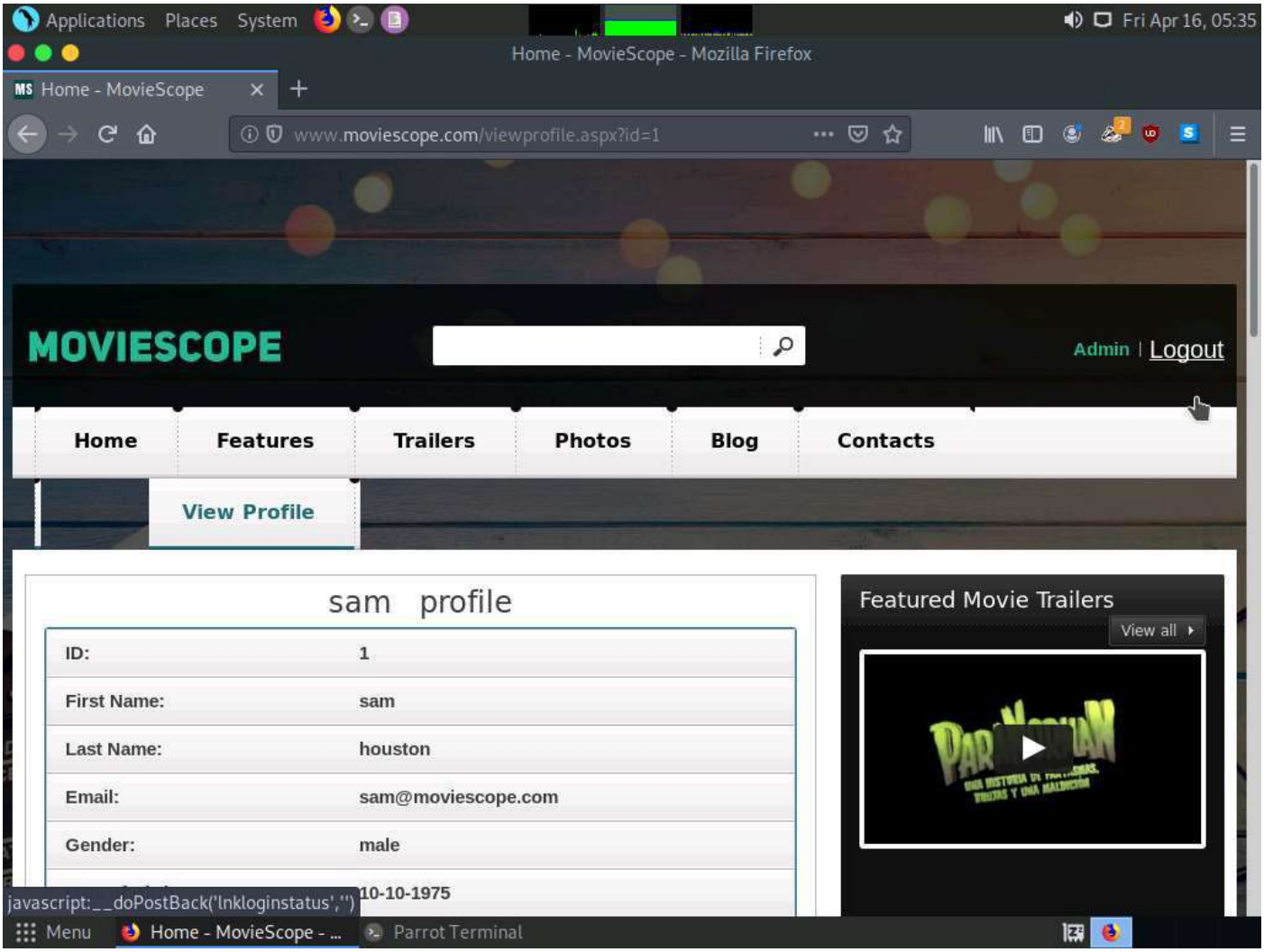


23. sqlmap retrieves the complete **User_Login** table data from the database moviescope, containing all users' usernames under the **Uname** column and passwords under the **password** column, as shown in screenshot.

24. You will see that under the **password** column, the passwords are shown in plain text form.

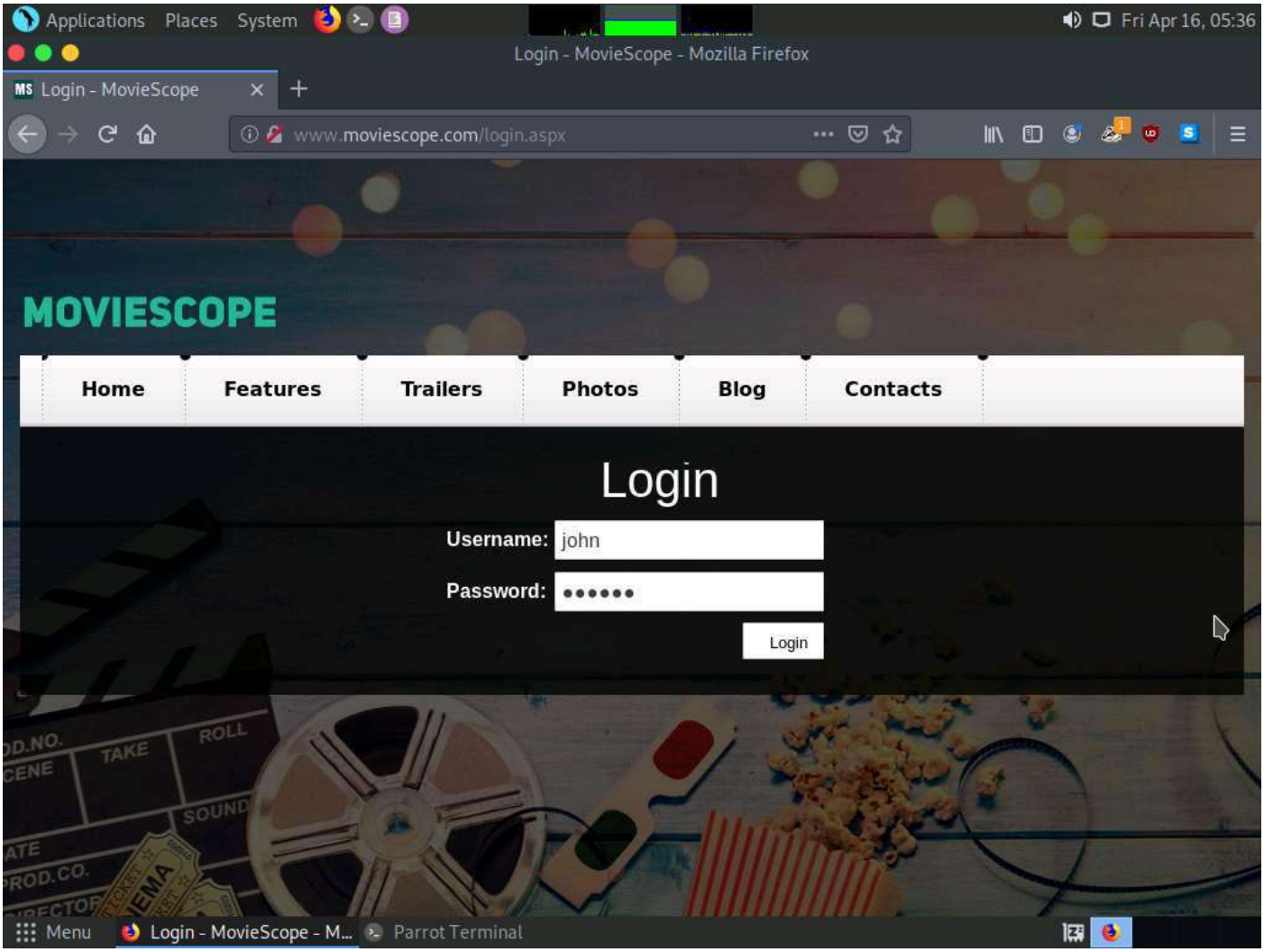


25. To verify if the login details are valid, you should try to log in with the extracted login details of any of the users. To do so, switch back to the web browser, close the **Developer Tools** console, and click **Logout** to start a new session on the site.

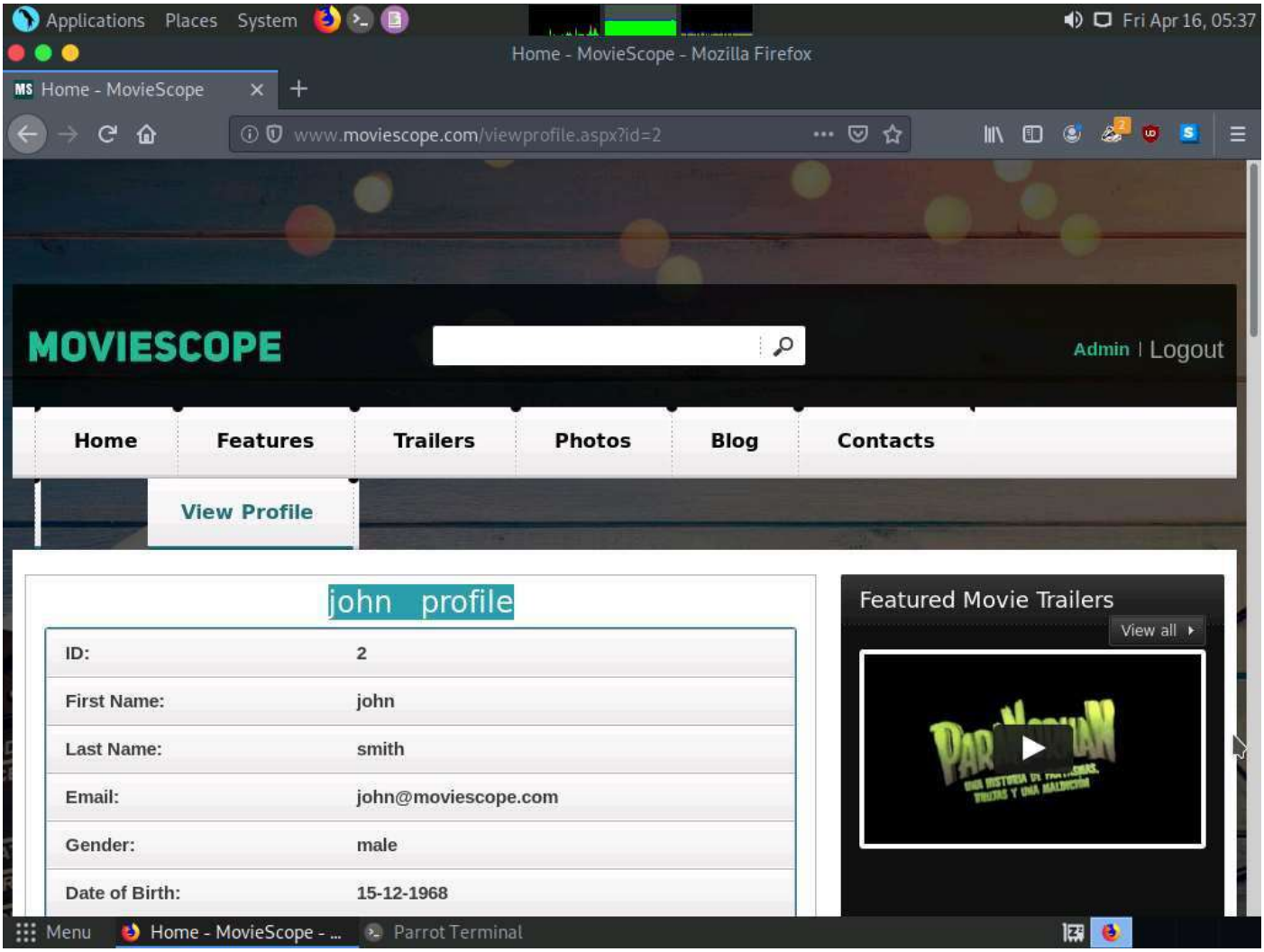


26. The **Login** page appears; log in into the website using the retrieved credentials **john/qwerty**.

If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**.

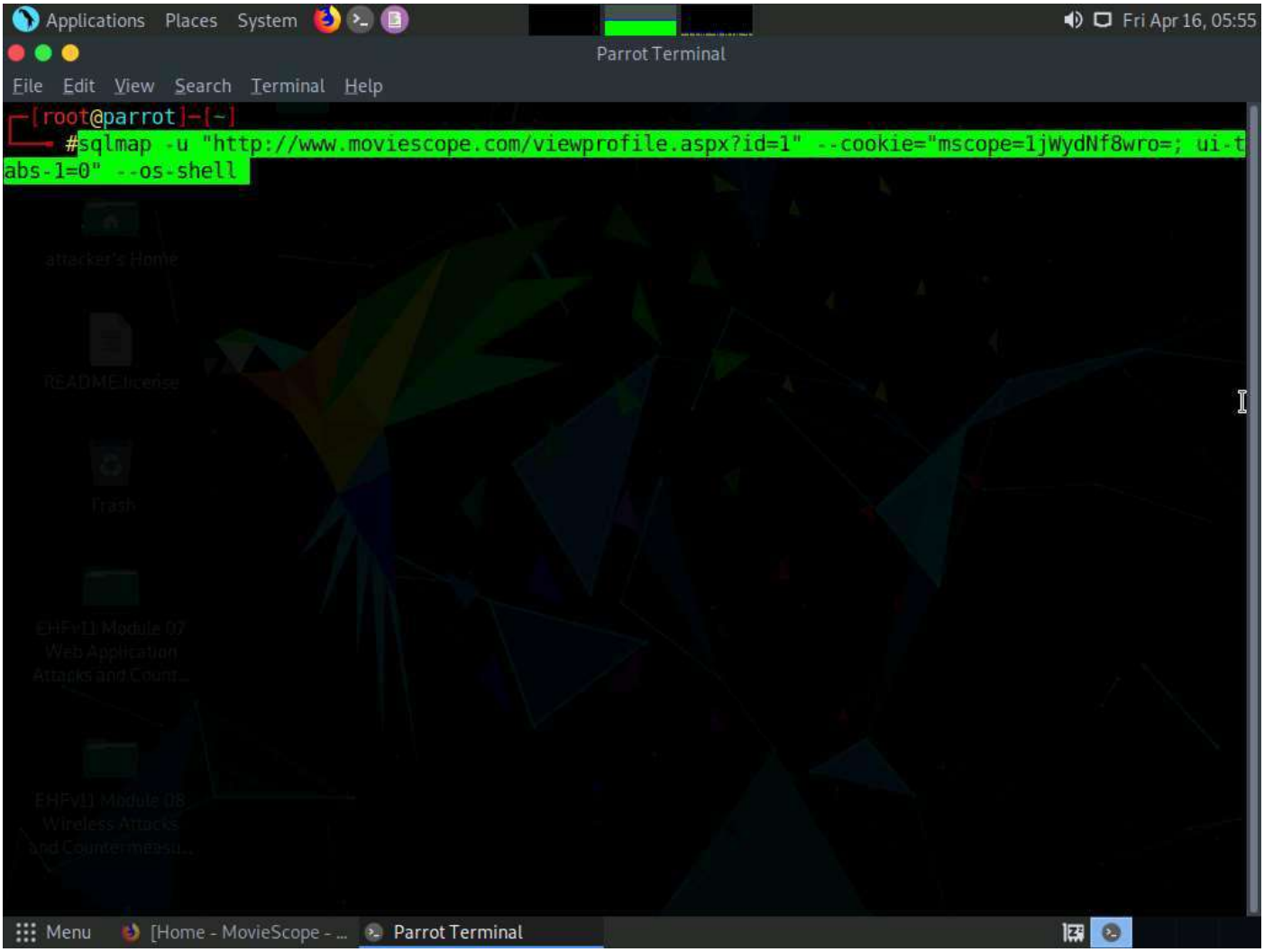


27. You will observe that you have successfully logged into the MovieScope website with john's account, as shown in the screenshot.

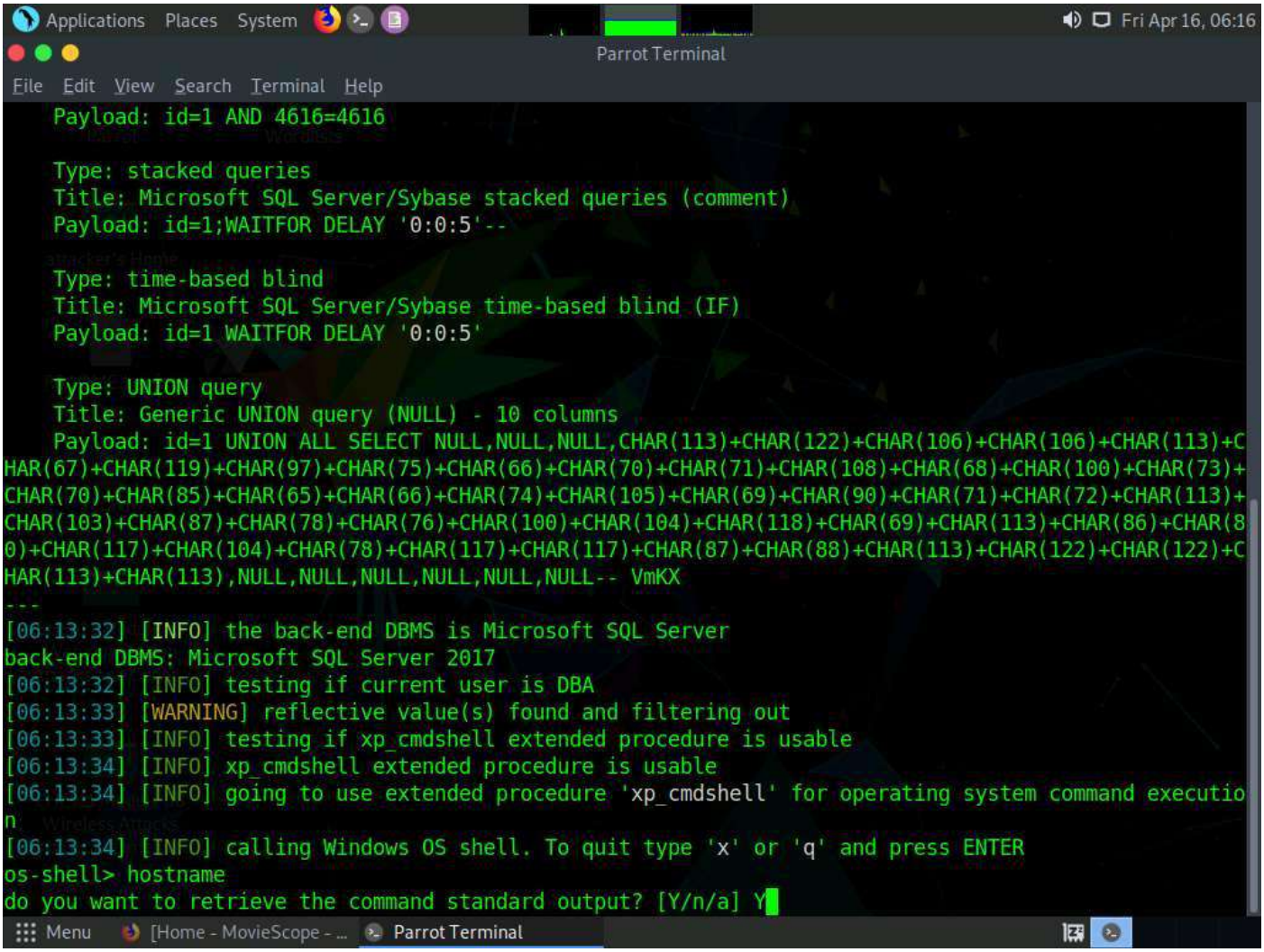


28. Now, switch back to the **Parrot Terminal window**. Type **sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 6]" --os-shell** and press **Enter**.

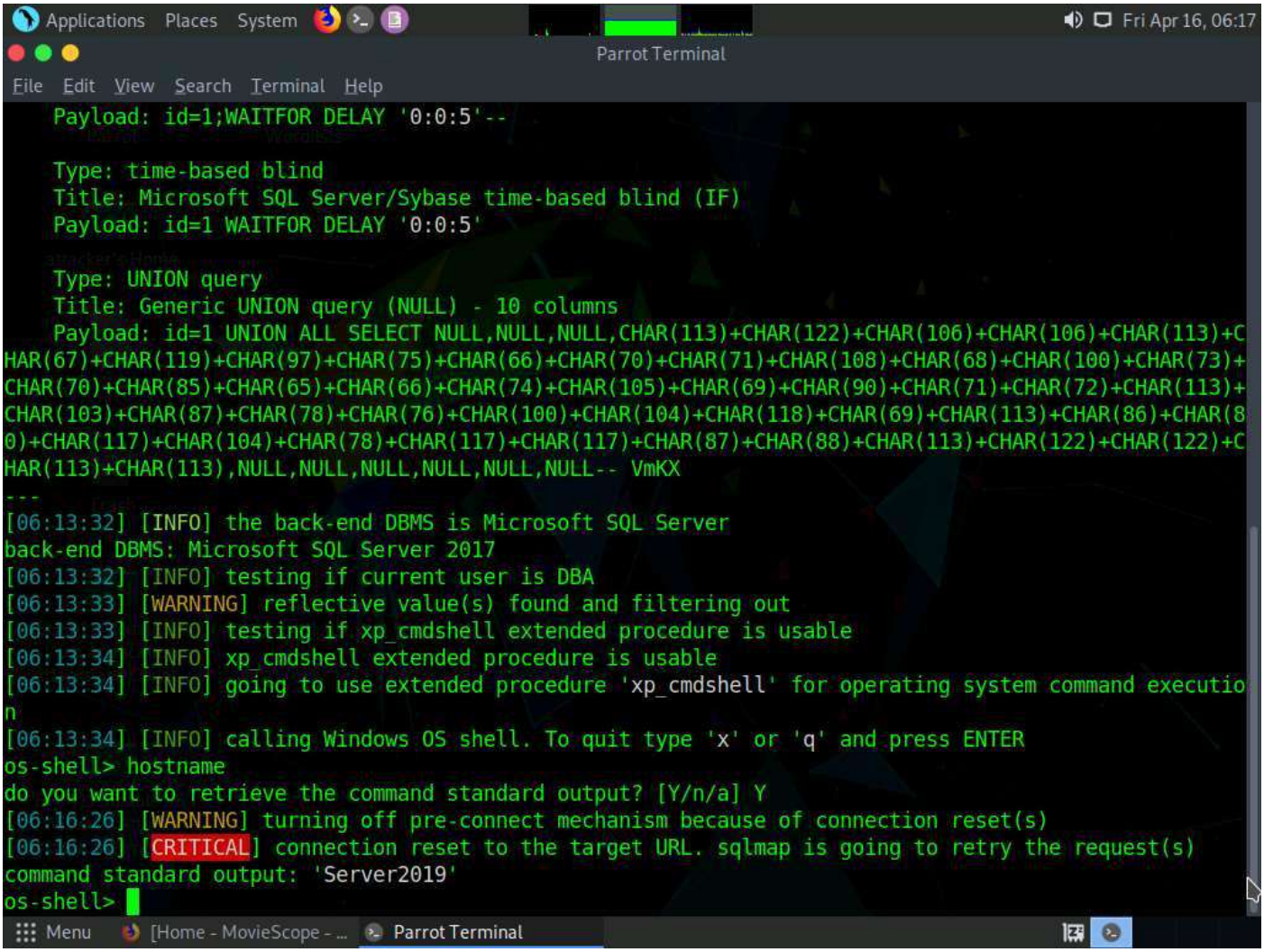
In this query, **--os-shell** is the prompt for an interactive OS shell.



29. If the message **do you want sqlmap to try to optimize value(s) for DBMS delay responses** appears, type **Y** and press **Enter** to continue.
30. Once sqlmap acquires the permission to optimize the machine, it will provide you with the OS shell. Type **hostname** and press **Enter** to find the machine name where the site is running.
31. If the message **do you want to retrieve the command standard output?** appears, type **Y** and press **Enter**.

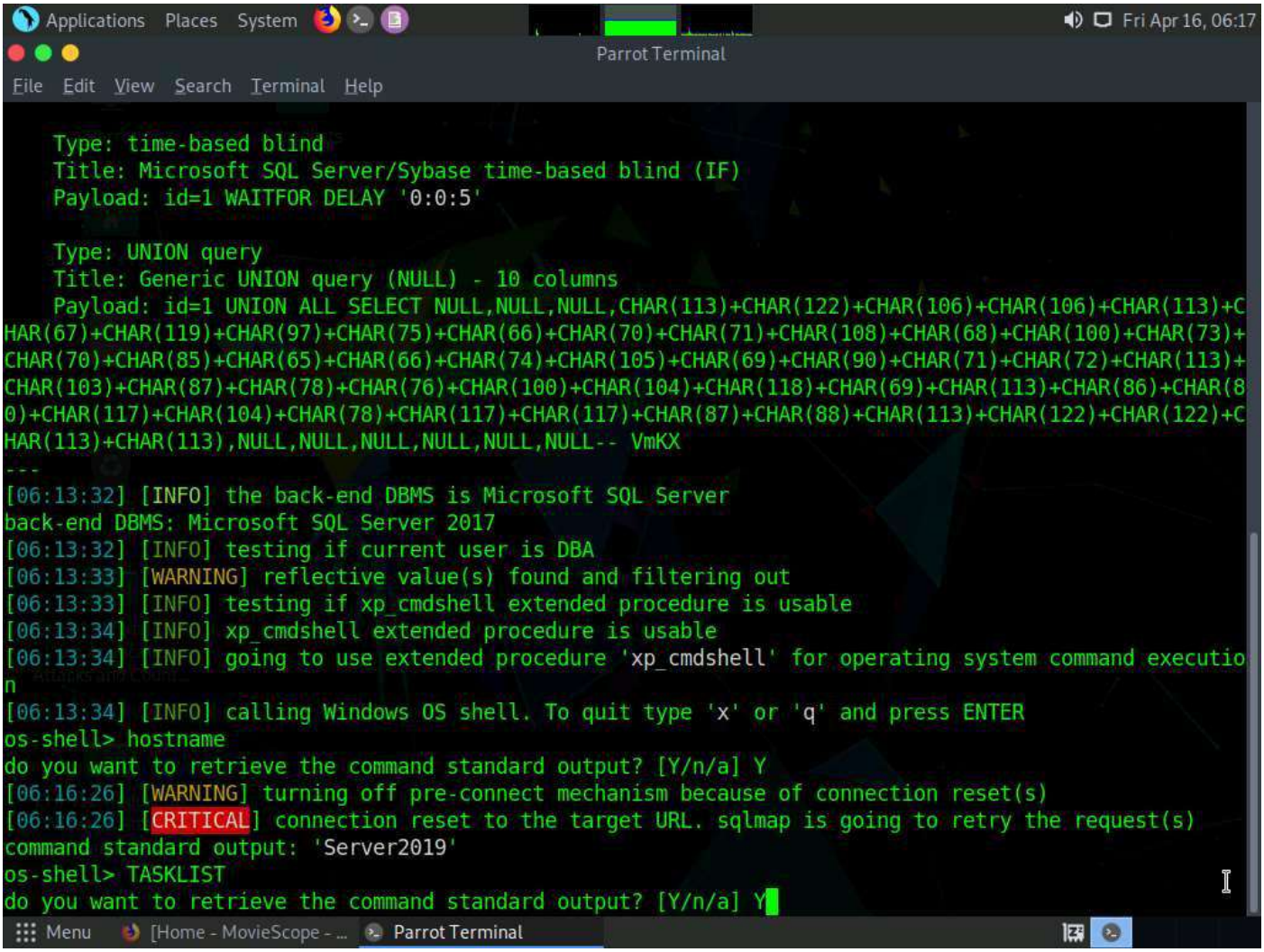


32. sqlmap will retrieve the hostname of the machine on which the target web application is running, as shown in the screenshot.

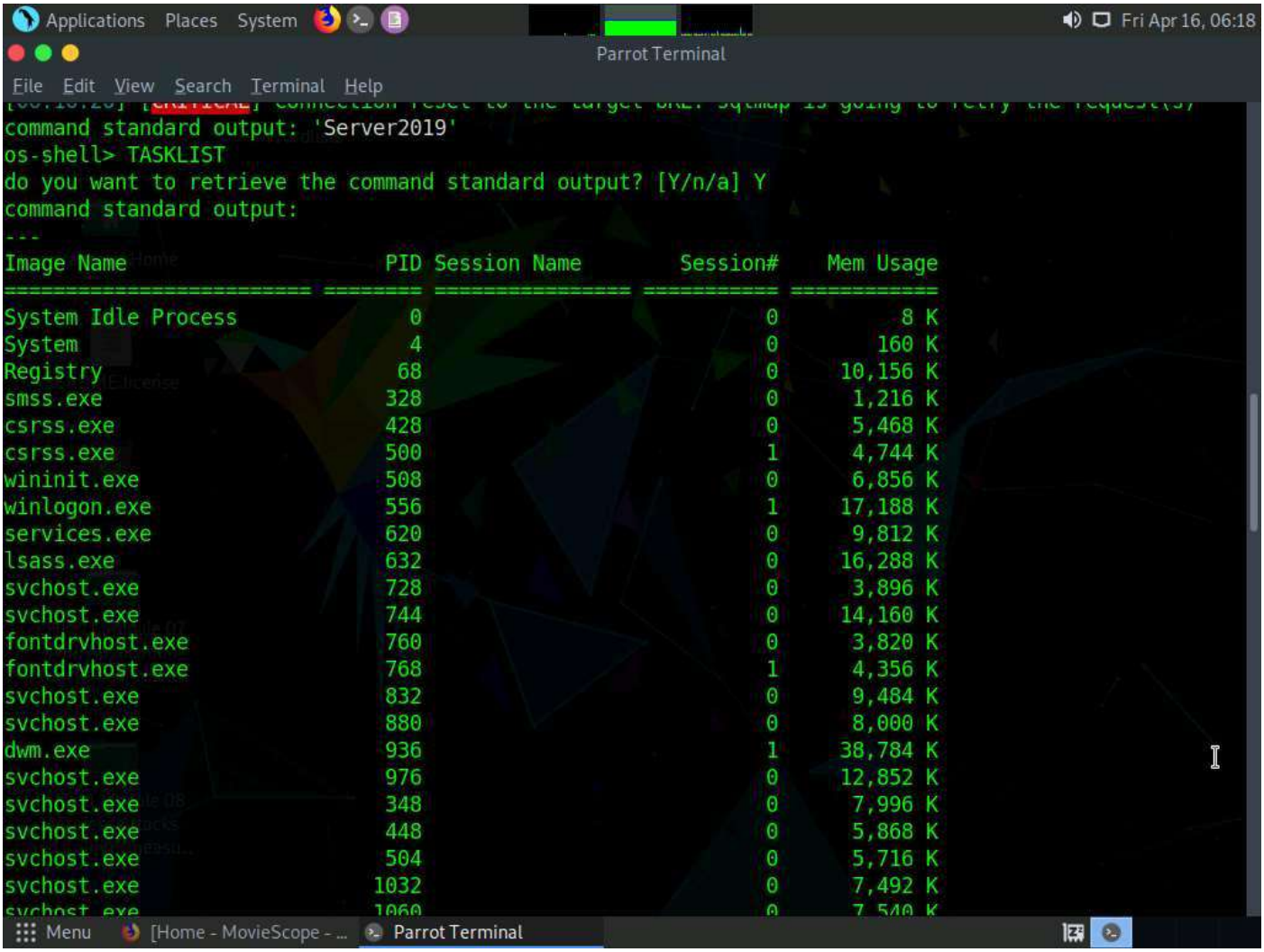


33. Type **TASKLIST** and press **Enter** to view a list of tasks that are currently running on the target system.

If the message **do you want to retrieve the command standard output?** appears, type **Y** and press **Enter**.



34. The above command retrieves the tasks and displays them under the **command standard output** section, as shown in the screenshots below.



35. Following the same process, you can use various other commands to obtain further detailed information about the target machine.

To view the available commands under the OS shell, type **help** and press **Enter**.

36. This concludes the demonstration of how to launch a SQL injection attack against MSSQL to extract databases using sqlmap.
37. Close all open windows and document all the acquired information.

Lab 7-4: Detect SQL Injection Vulnerabilities using SQL Injection Detection Tools

Lab Scenario

By now, you will be familiar with various types of SQL injection attacks and their possible impact. To recap, the different kinds of SQL injection attacks include authentication bypass, information disclosure, compromised data integrity, compromised availability of data and remote code execution (which allows identity spoofing), damage to existing data, and the execution of system-level commands to cause a denial of service from the application.

You must test your organization's web applications and services against SQL injection and other vulnerabilities, using various approaches and multiple techniques to ensure that your assessments, and the applications and services themselves, are robust.

In the previous lab, you learned how to use SQL injection attacks on the MSSQL server database to test for website vulnerabilities.

In this lab, you will learn how to test for SQL injection vulnerabilities using various other SQL injection detection tools.

Lab Objectives

- Detect SQL Injection Vulnerabilities using DSSS

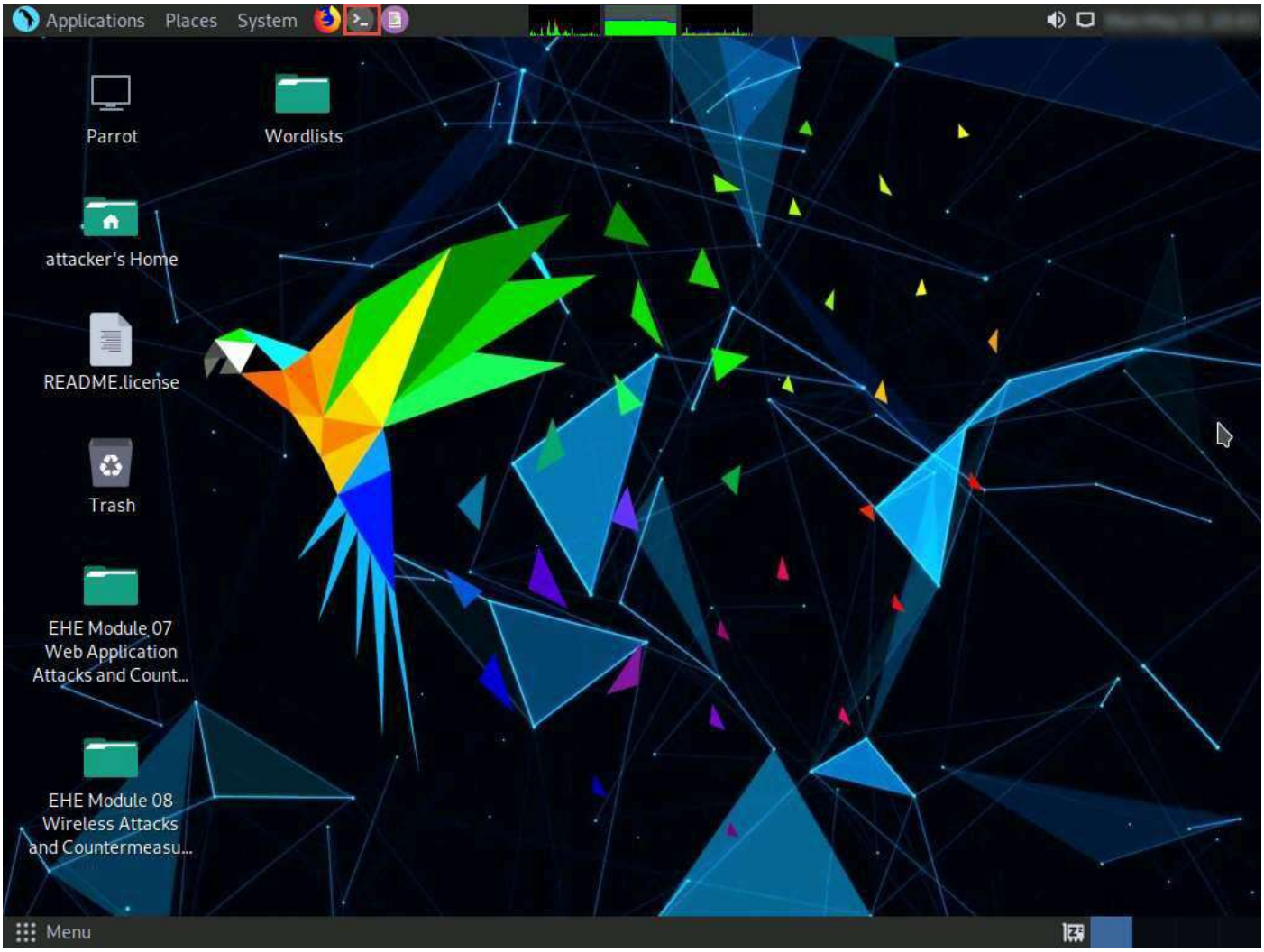
Task 1: Detect SQL Injection Vulnerabilities using DSSS

Damn Small SQLi Scanner (DSSS) is a fully functional SQL injection vulnerability scanner that supports GET and POST parameters. DSSS scans web applications for various SQL injection vulnerabilities.

Here, we will use DSSS to detect SQL injection vulnerabilities in a web application.

We will scan the **www.moviescope.com** website that is hosted on the **Windows Server 2019** machine.

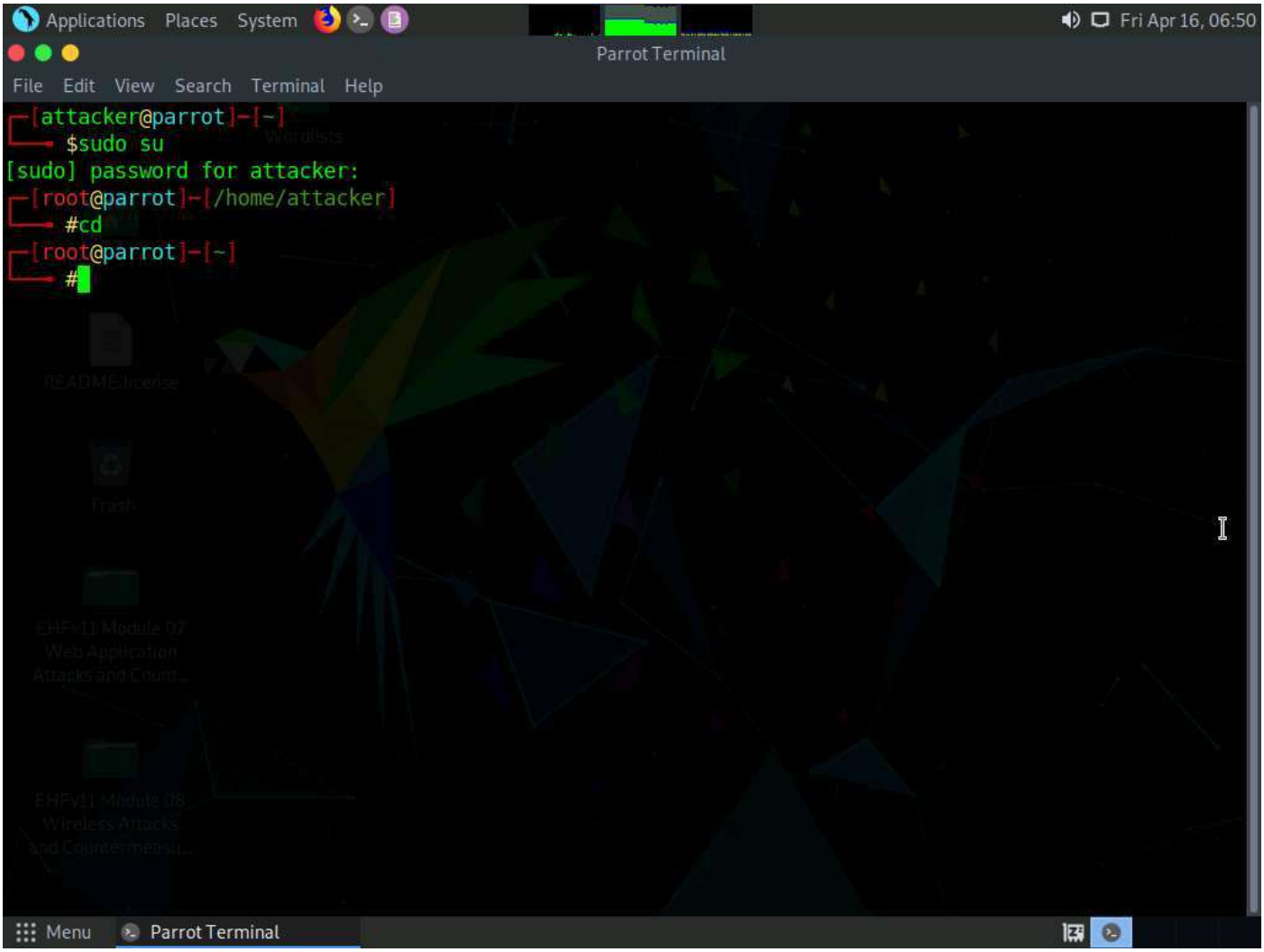
1. On the **Parrot Security** machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Parrot Terminal** window.



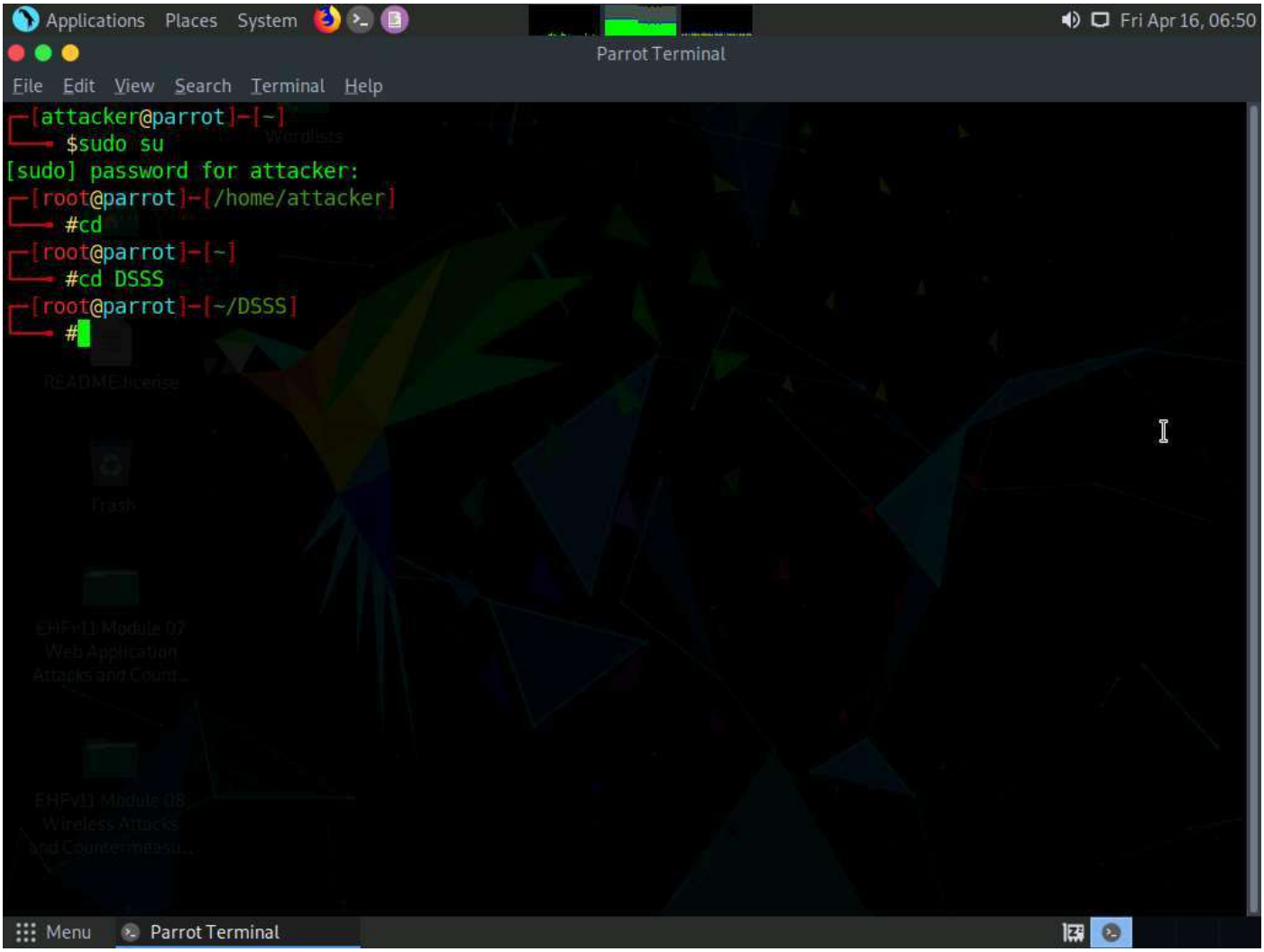
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

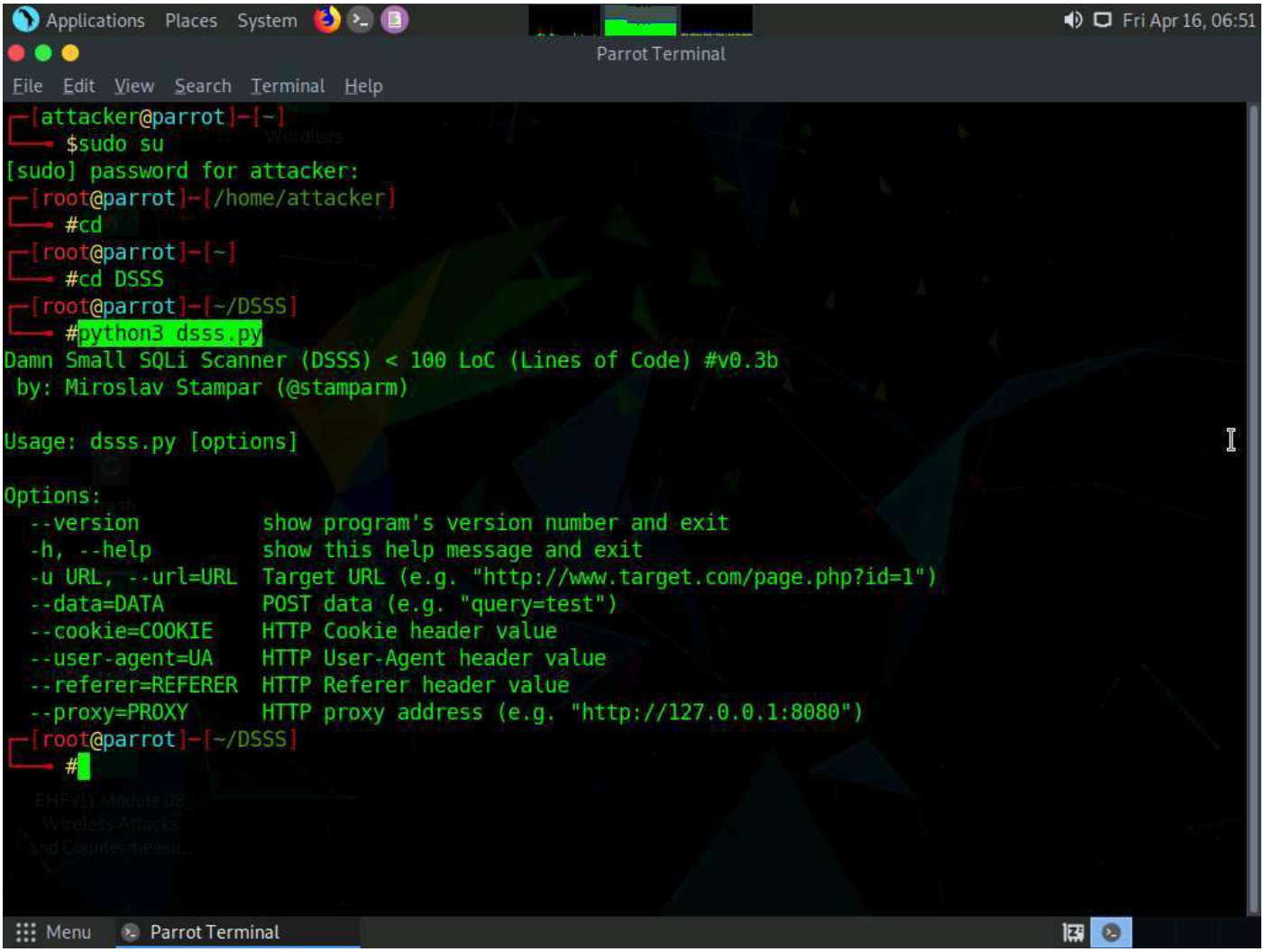
4. Now, type **cd** and press **Enter** to jump to the root directory.



5. In the **MATE Terminal** type **cd DSSS** and press **Enter** to navigate to the DSSS folder which is alredy downloaded.

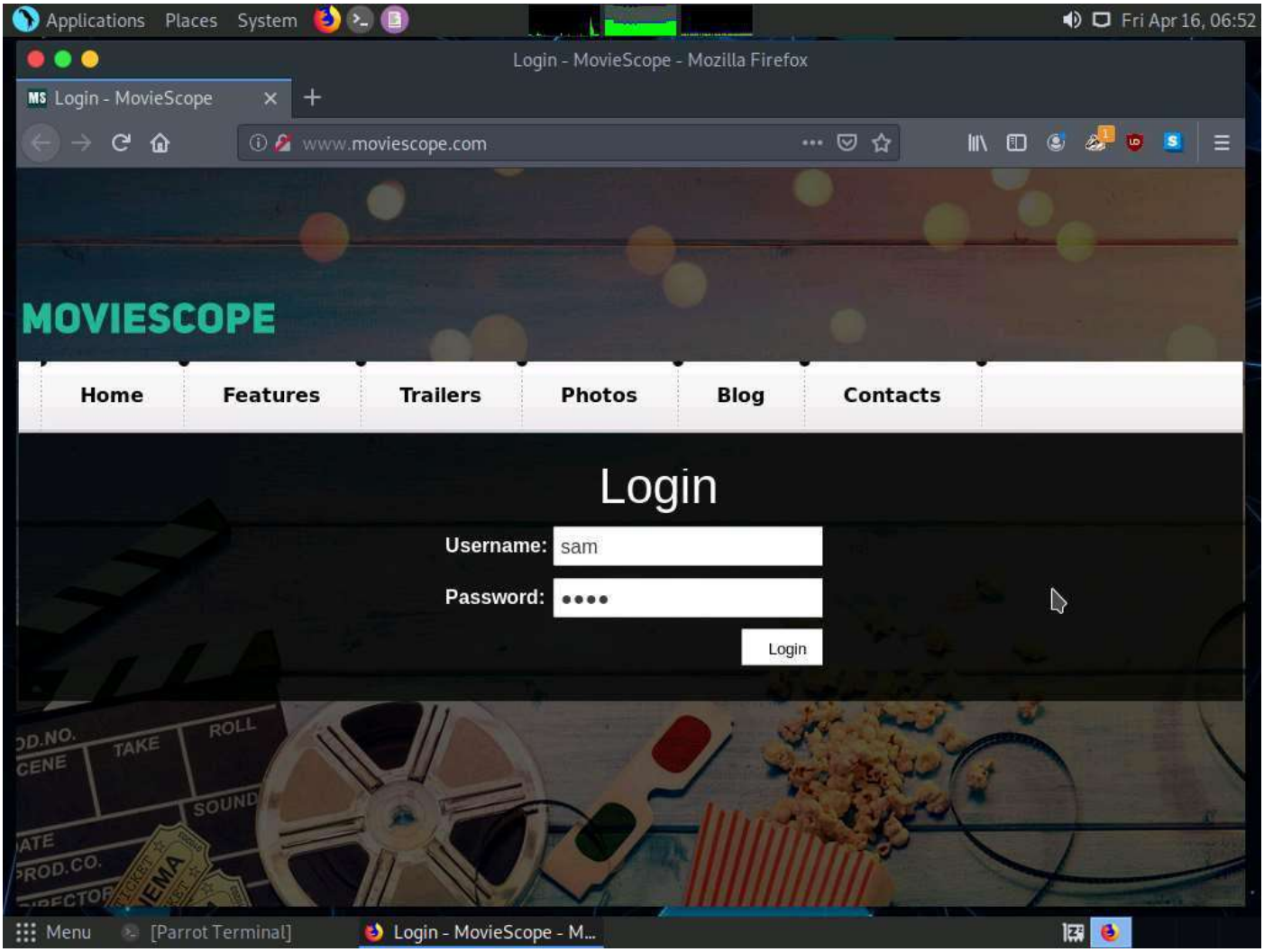


6. In the terminal window, type **python3 dsss.py** and press **Enter** to view a list of available options in the DSSS application, as shown in the screenshot.



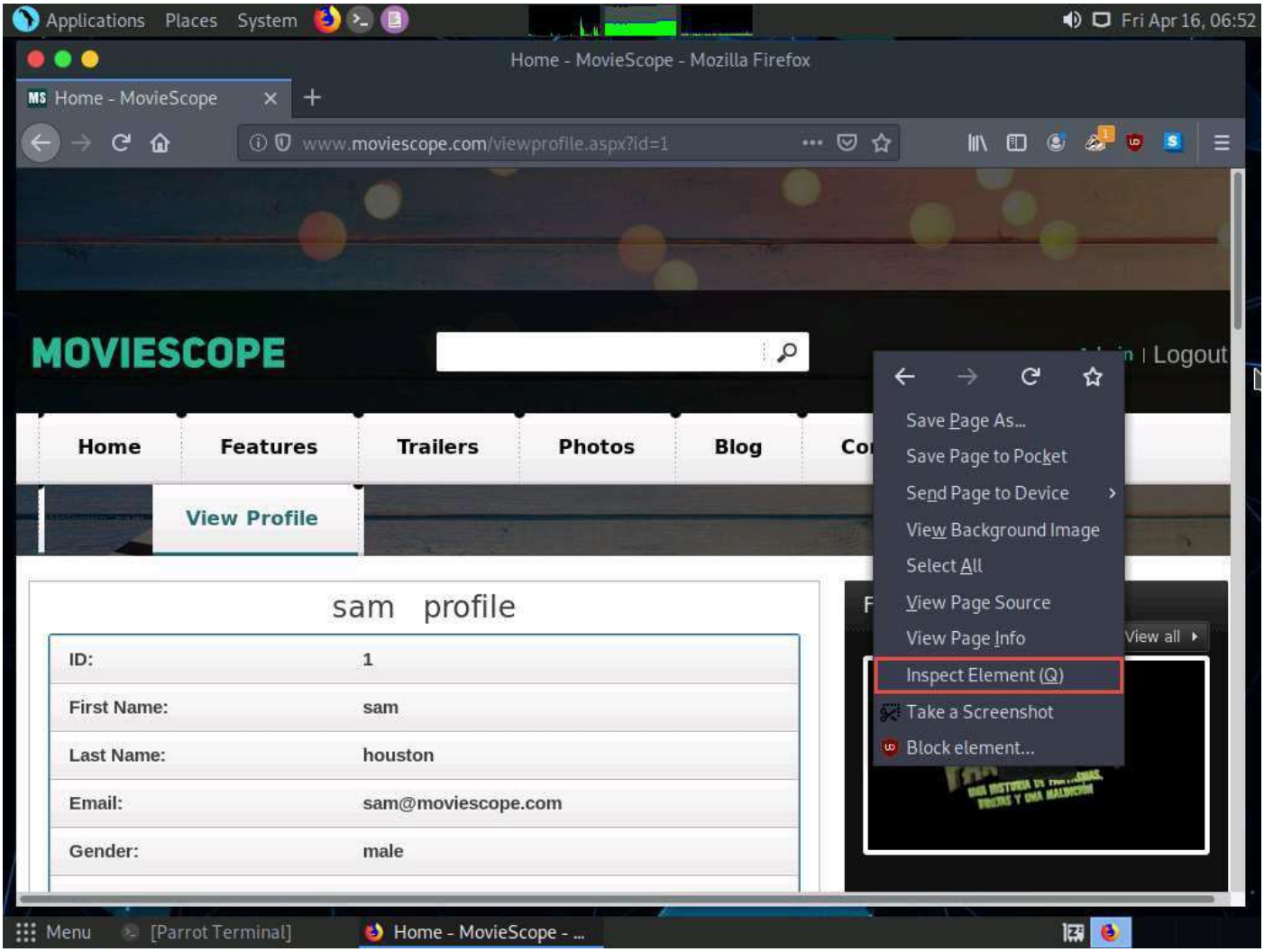
7. Now, minimize the **Terminal** window and click on the **Firefox** icon in the top section of **Desktop** to launch Firefox.
8. In the **Mozilla Firefox** window, type **http://www.moviescope.com/** in the address bar and press **Enter**. A **Login** page loads; enter the **Username** and **Password** as **sam** and **test**, respectively. Click the **Login** button.

If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**.

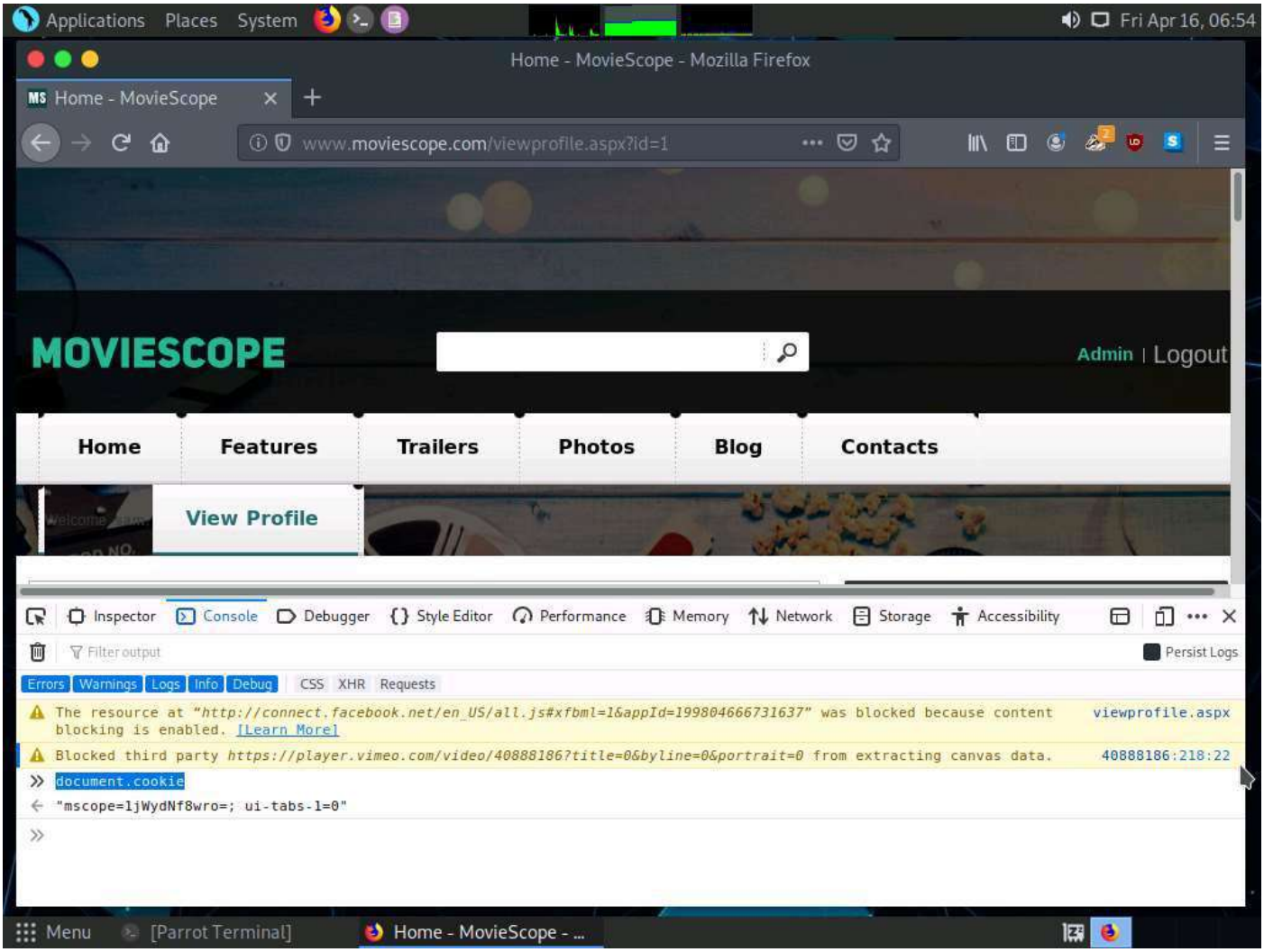


9. Once you are logged into the website, click the **View Profile** tab from the menu bar; and when the page has loaded, make a note of the URL in the address bar of the browser.

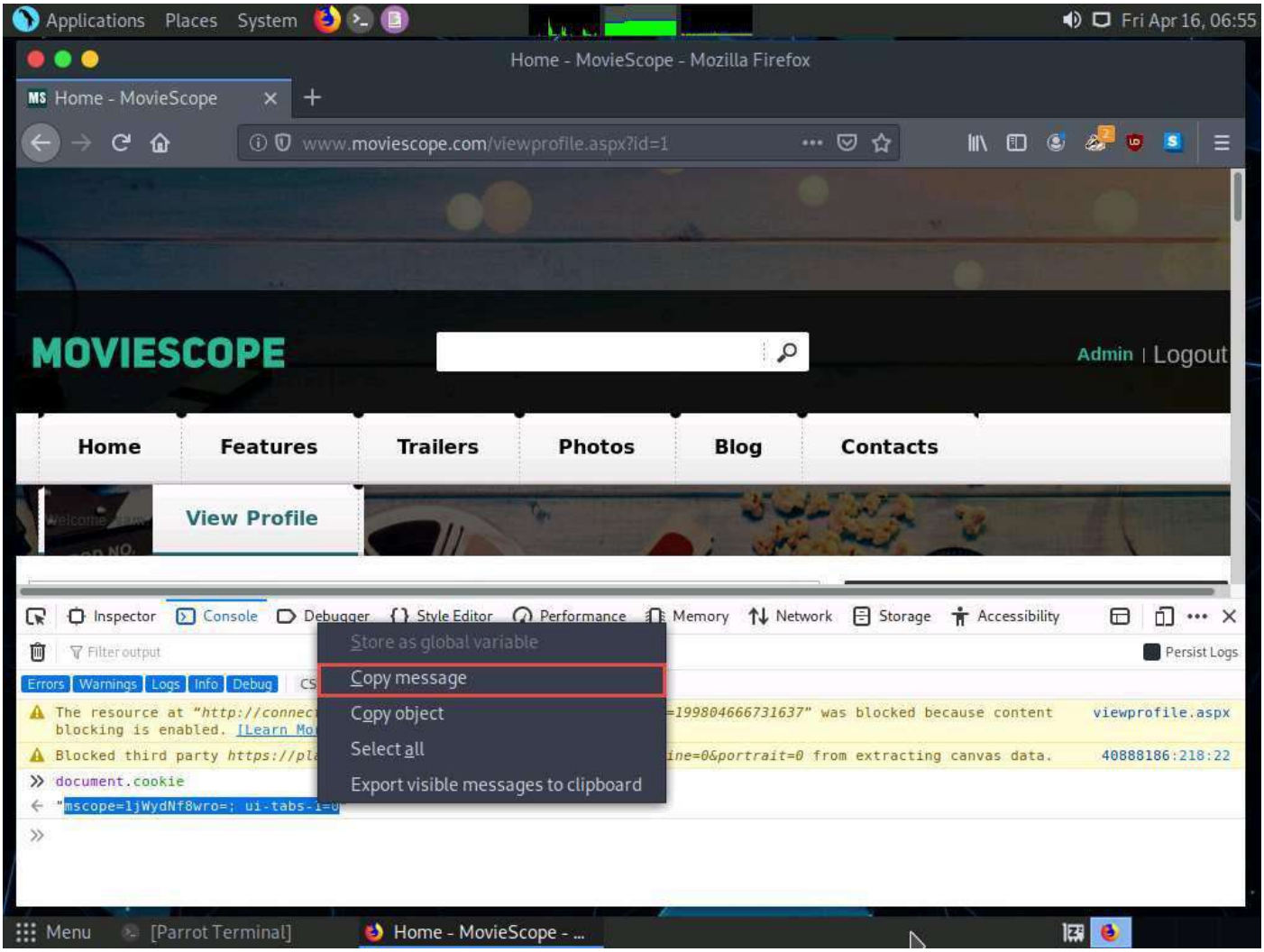
10. Right-click anywhere on the webpage and click **Inspect Element (Q)** from the context menu, as shown in the screenshot.



11. The **Developer Tools** frame appears in the lower section of the browser window. Click the **Console** tab, type **document.cookie** in the lower-left corner of the browser, and press **Enter**.

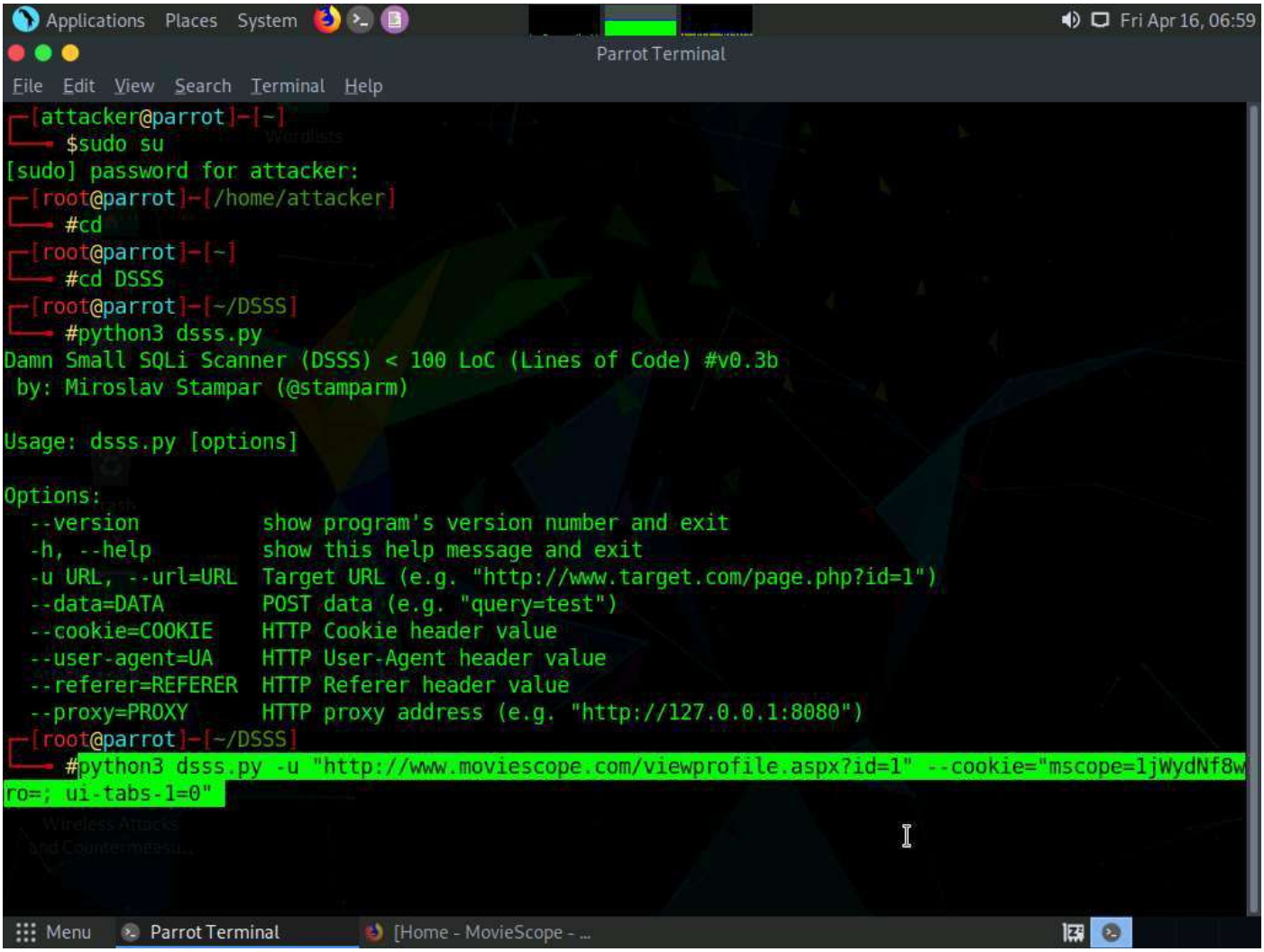


12. Select the cookie value, then right-click and copy it by clicking on **Copy message**, as shown in the screenshot. Minimize the web browser.

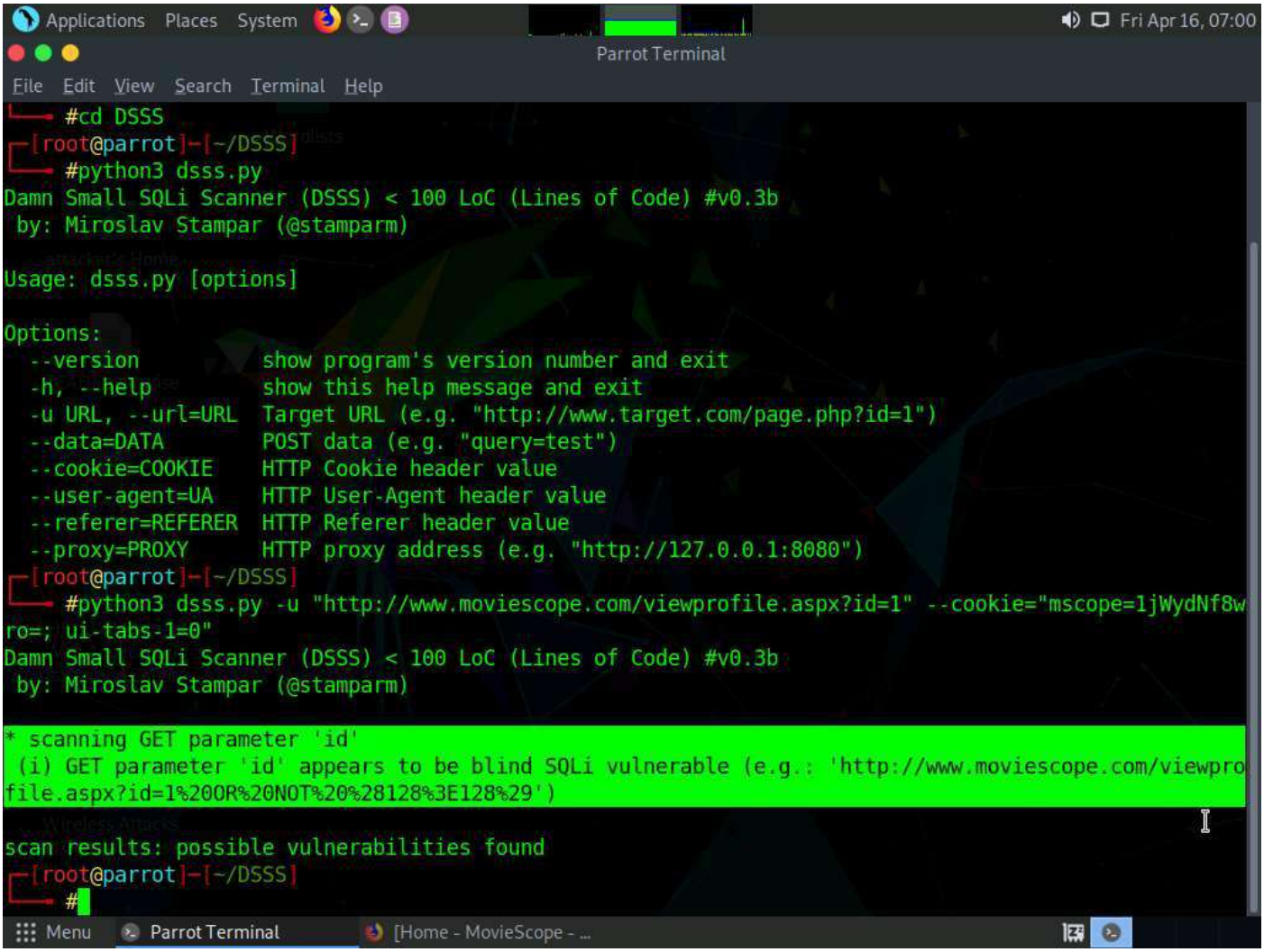


13. Switch to a terminal window and type **python3 dsss.py -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 12]"** and press Enter.

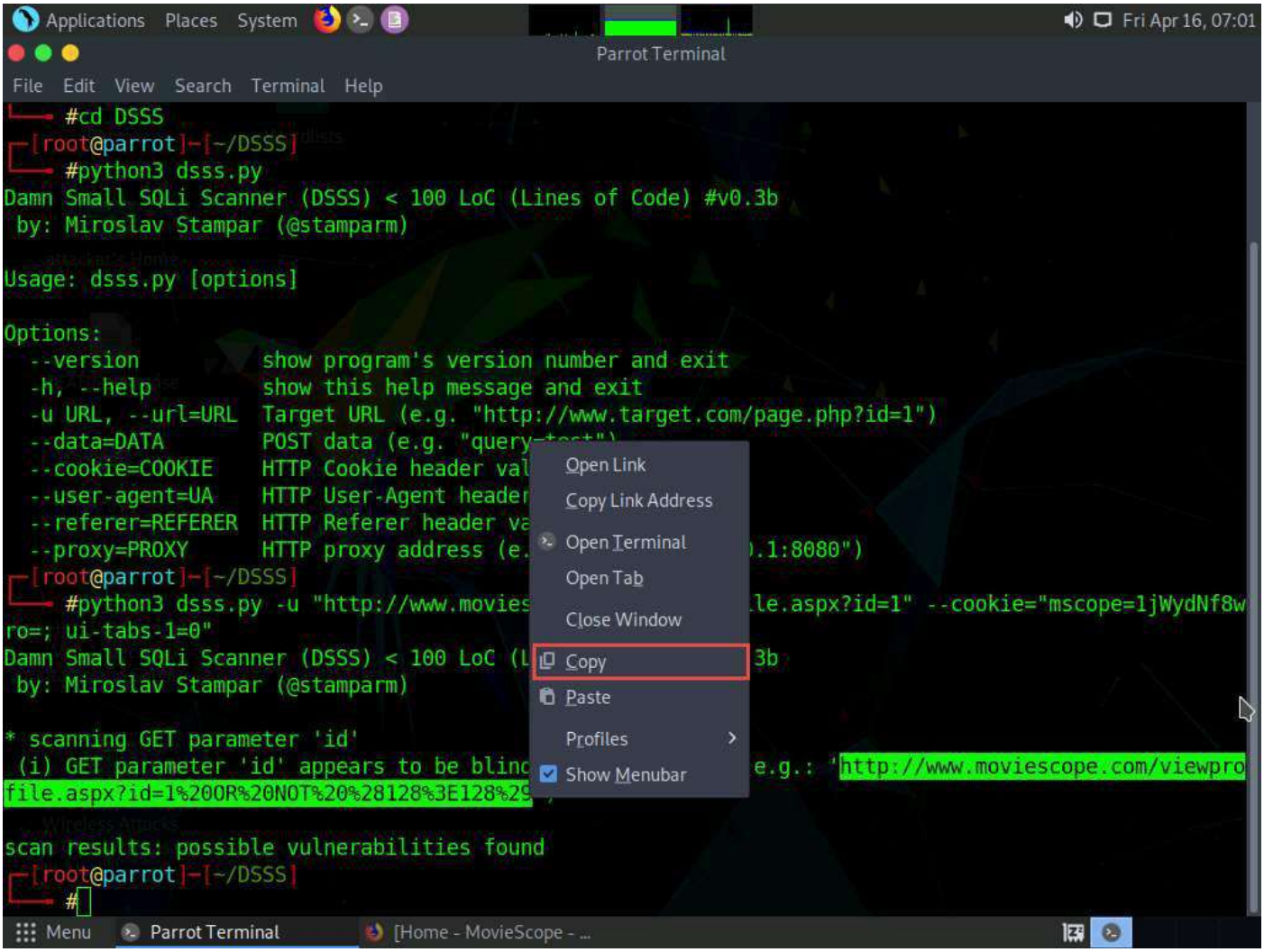
In this command, **-u** specifies the target URL and **--cookie** specifies the HTTP cookie header value.



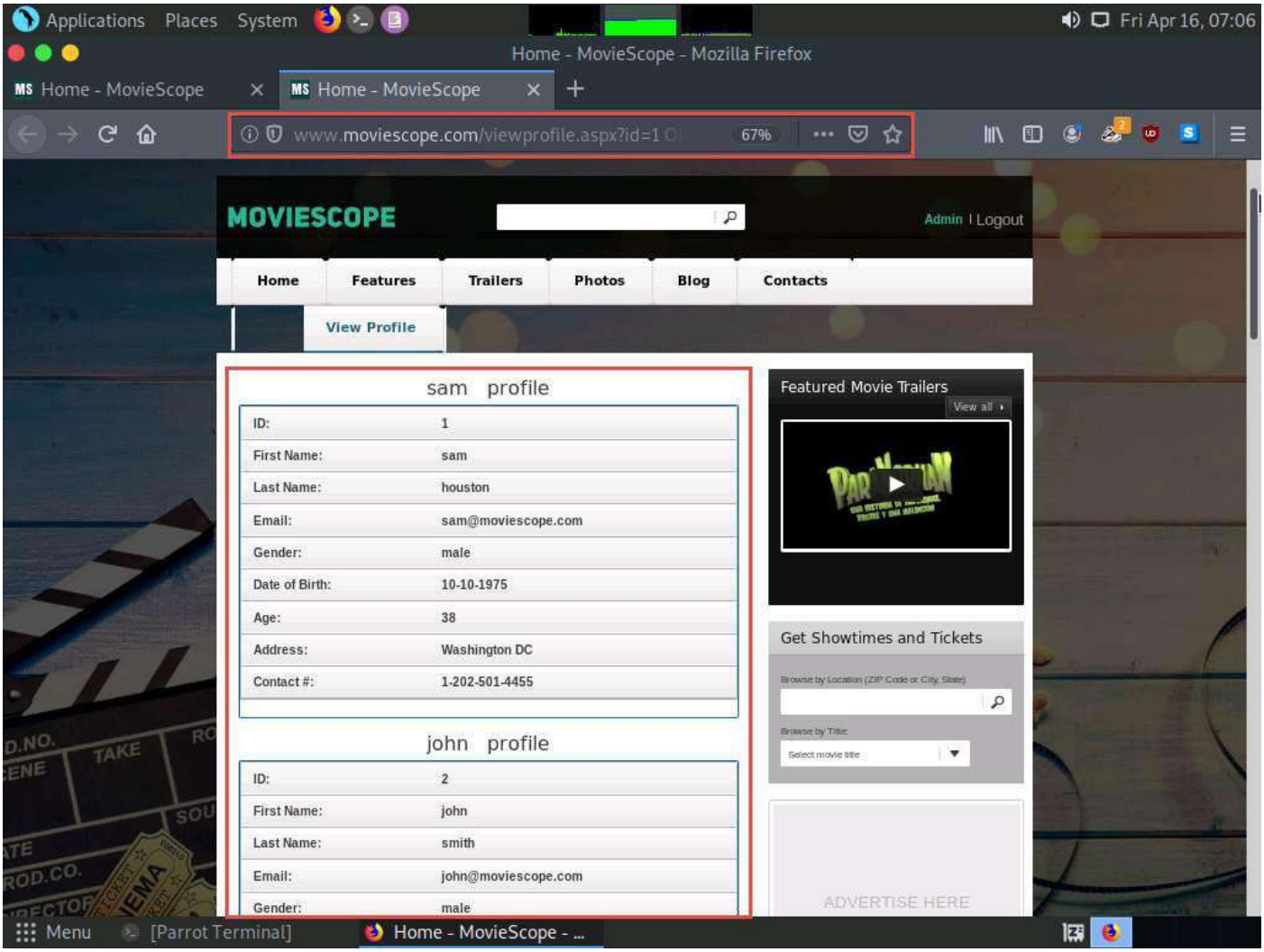
14. The above command causes DSSS to scan the target website for SQL injection vulnerabilities.
15. The result appears, showing that the target website (**www.moviescope.com**) is vulnerable to blind SQL injection attacks. The vulnerable link is also displayed, as shown in the screenshot.



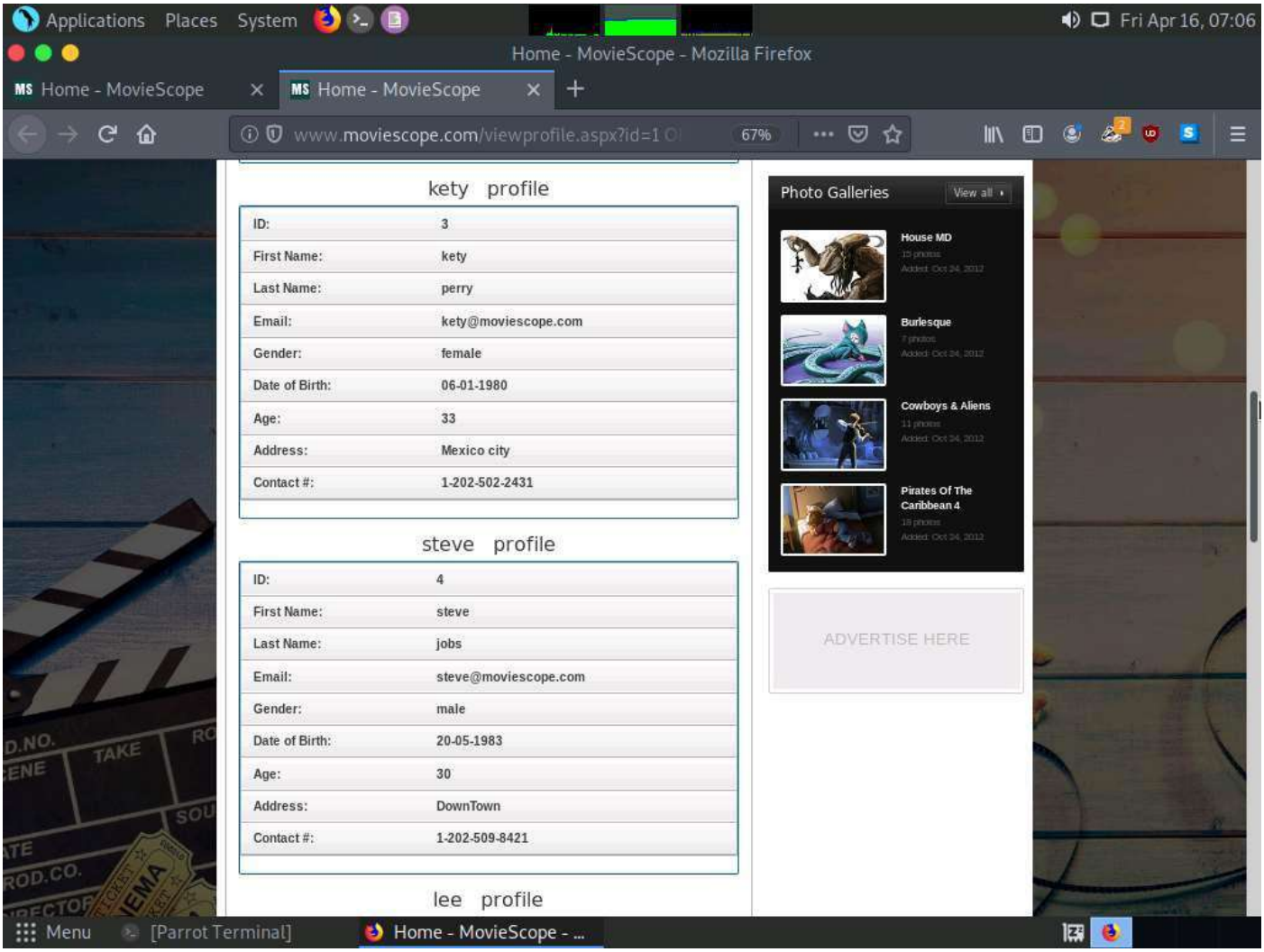
16. Highlight the vulnerable website link, right-click it, and, from the options, click **Copy**.

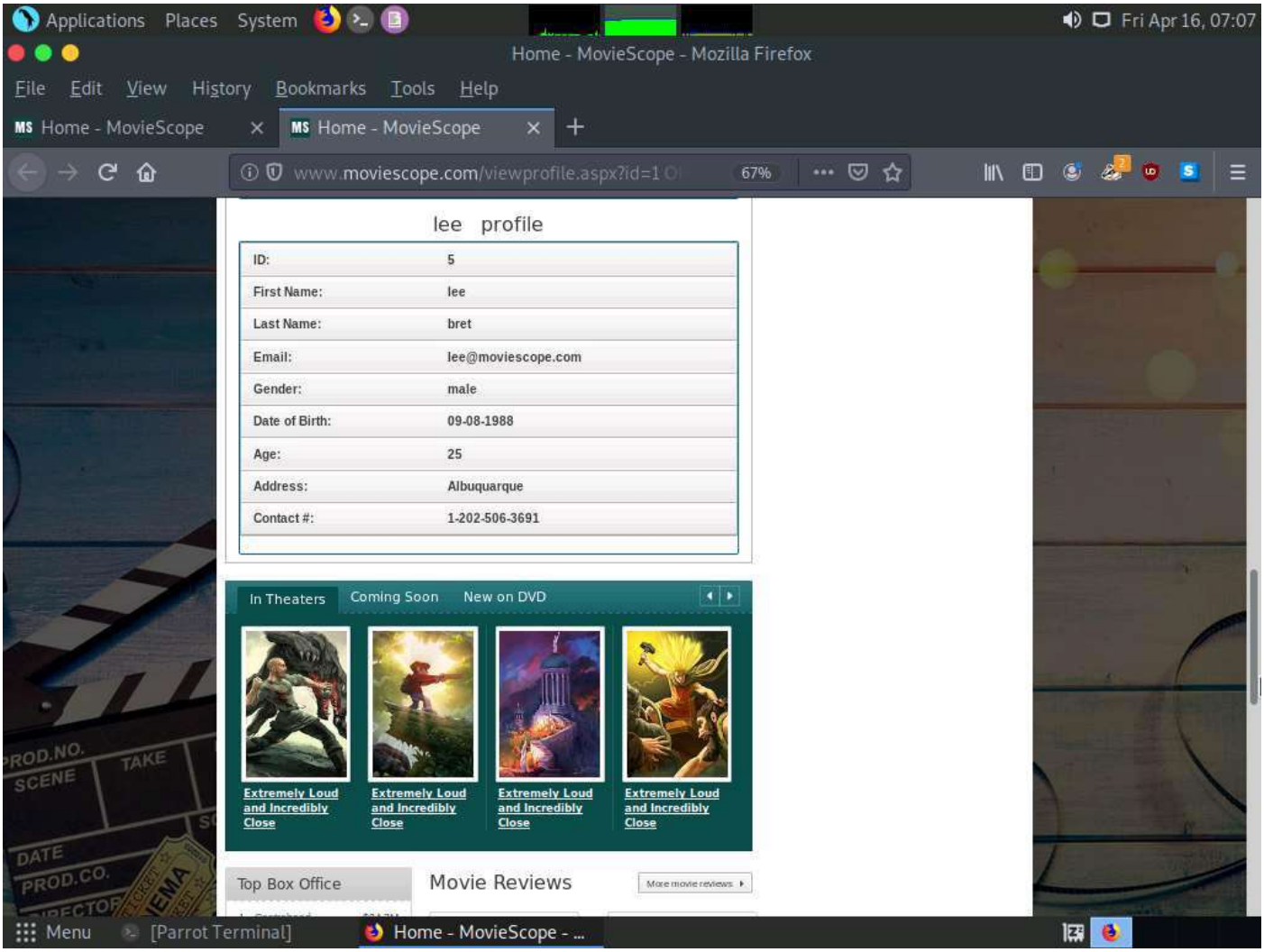


17. Switch to **Mozilla Firefox**; in a new tab, paste the copied link in the address bar and press **Enter**.
18. You will observe that information regarding available user accounts appears under the **View Profile** tab.



19. Scroll down to view the user account information for all users.


Applications Places System
Fri Apr 16, 07:06
Home - MovieScope - Mozilla Firefox
Home - MovieScope
Home - MovieScope
www.moviescope.com/viewprofile.aspx?id=1
67%
kety profile
ID: 3
First Name: kety
Last Name: perry
Email: kety@moviescope.com
Gender: female
Date of Birth: 06-01-1980
Age: 33
Address: Mexico city
Contact #: 1-202-502-2431
steve profile
ID: 4
First Name: steve
Last Name: jobs
Email: steve@moviescope.com
Gender: male
Date of Birth: 20-05-1983
Age: 30
Address: DownTown
Contact #: 1-202-509-8421
lee profile
Photo Galleries
View all
House MD
Burlesque
Cowboys & Aliens
Pirates Of The Caribbean 4
ADVERTISE HERE
Menu
[Parrot Terminal]
Home - MovieScope - ...



In real life, attackers use blind SQL injection to access or destroy sensitive data. Attackers can steal data by asking a series of true or false questions through SQL statements. The results of the injection are not visible to the attacker. This type of attack can become time-intensive, because the database must generate a new statement for each newly recovered bit.

20. This concludes the demonstration of how to detect SQL injection vulnerabilities using DSSS.
21. Close all open windows and document all the acquired information.

Module 08: Wireless Attacks and Countermeasures

Scenario

Wireless networking is revolutionizing the way people work and play. A wireless local area network (WLAN) is an unbounded data communication system, based on the IEEE 802.11 standard, which uses radio frequency technology to communicate with devices and obtain data. This network frees the user from complicated and multiple wired connections. With the need for a physical connection or cable removed, individuals are able to use networks in new ways, and data has become ever more portable and accessible.

Although wireless networking technology is becoming increasingly popular, because of its convenience, it has many security issues, some of which do not exist in wired networks. By nature, wirelessly transferred data packets are airborne and available to anyone with the ability to intercept and decode them. For example, several reports have demonstrated the weaknesses in the Wired Equivalent Privacy (WEP) security algorithm, specified in the 802.11x standard, which is designed to encrypt wireless data.

You must have sound knowledge of wireless concepts, wireless encryption, and related threats in order to protect your company's wireless network from unauthorized access and attacks. You should determine critical sources, risks, or vulnerabilities associated with your organization's wireless network, and then check whether the current security system is able to protect the network against all possible attacks.

Objective

The objective of the lab is to protect the target wireless network from unauthorized access. To do so, you will perform various tasks that include, but are not limited to:

- Wi-Fi Packet Analysis
- Crack WEP and WPA2 Wi-Fi networks

Overview of Wireless Networking

In wireless networks, communication takes place through radio wave transmission, which usually takes place at the physical layer of the network structure. Thanks to the wireless communication revolution, fundamental changes to data networking and telecommunication are taking place. This means that you will need to know and understand several types of wireless networks. These include:

- **Extension to a wired network**: A wired network is extended by the introduction of access points between the wired network and wireless devices
- **Multiple access points**: Multiple access points connect computers wirelessly
- **LAN-to-LAN wireless network**: All hardware APs have the ability to interconnect with other hardware access points
- **3G/4G hotspot**: A mobile device shares its cellular data wirelessly with Wi-Fi-enabled devices such as MP3 players, notebooks, tablets, cameras, PDAs, and netbooks

Lab Tasks

We will use numerous tools and techniques to hack target wireless networks. The recommended labs that will assist you in learning various wireless network hacking techniques include:

1. Perform Wi-Fi packet analysis
    - Wi-Fi packet analysis using Wireshark
2. Perform wireless attacks to crack wireless encryption
    - Crack a WEP network using Aircrack-ng
    - Crack a WPA2 network using Aircrack-ng

Lab 8-1: Perform Wi-Fi Packet Analysis

Lab Scenario

Our first step in hacking wireless networks is to capture and analyze the traffic of the target wireless network.

This wireless traffic analysis will help you to determine the weaknesses and vulnerable devices in the target network. In the process, you will determine the network's broadcasted SSID, the presence of multiple access points, the possibility of recovering SSIDs, the authentication method used, WLAN encryption algorithms, etc.

The labs in this exercise demonstrate how to use various tools and techniques to capture and analyze the traffic of the target wireless network.

Lab Objectives

- Wi-Fi Packet Analysis using Wireshark

Task 1: Wi-Fi Packet Analysis using Wireshark

Wireshark is a network protocol sniffer and analyzer. It lets you capture and interactively browse the traffic running on a target network. Wireshark can read live data from Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), and 802.11 wireless LAN. Npcap is a library that is integrated with Wireshark for complete WLAN traffic analysis, visualization, drill-down, and reporting. Wireshark can be used in monitor mode to capture wireless traffic. It is able to capture a vast number of management, control, data frames, etc. and further analyze the Radiotap header fields to gather critical information such as protocols and encryption techniques used, length of the frames, MAC addresses, etc.

Here, we will use Wireshark to analyze captured Wi-Fi packets.

In order to capture wireless traffic, a wireless adapter is required and using an adapter in the iLabs environment is not possible, therefore, in this lab, we are using a sample capture file (**WEPcrack-01.cap**) to analyze wireless packets.

1. By default, **Windows 10** machine selected, click Ctrl+Alt+Delete.

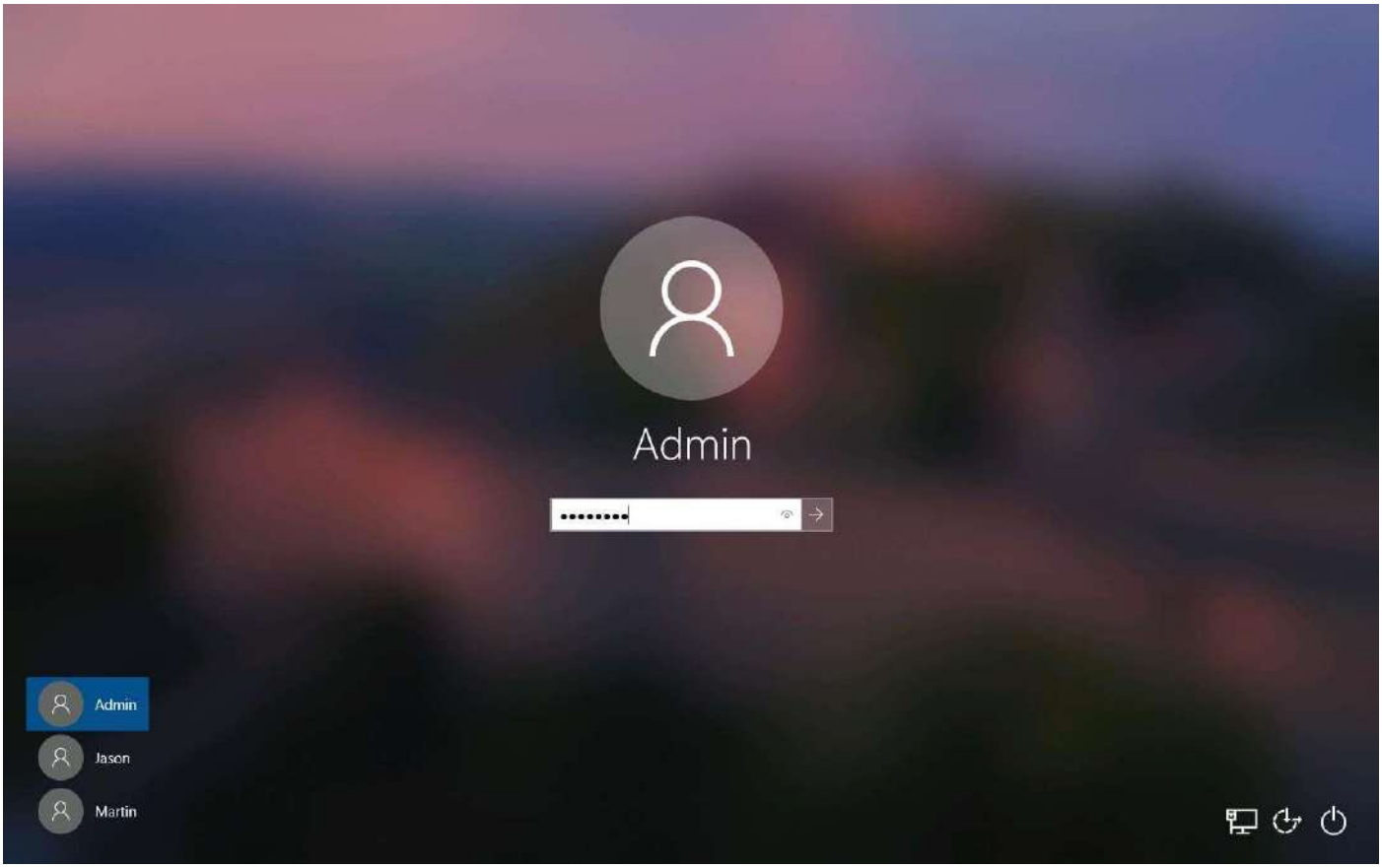
Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 10** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under Commands (**thunder** icon) menu.

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

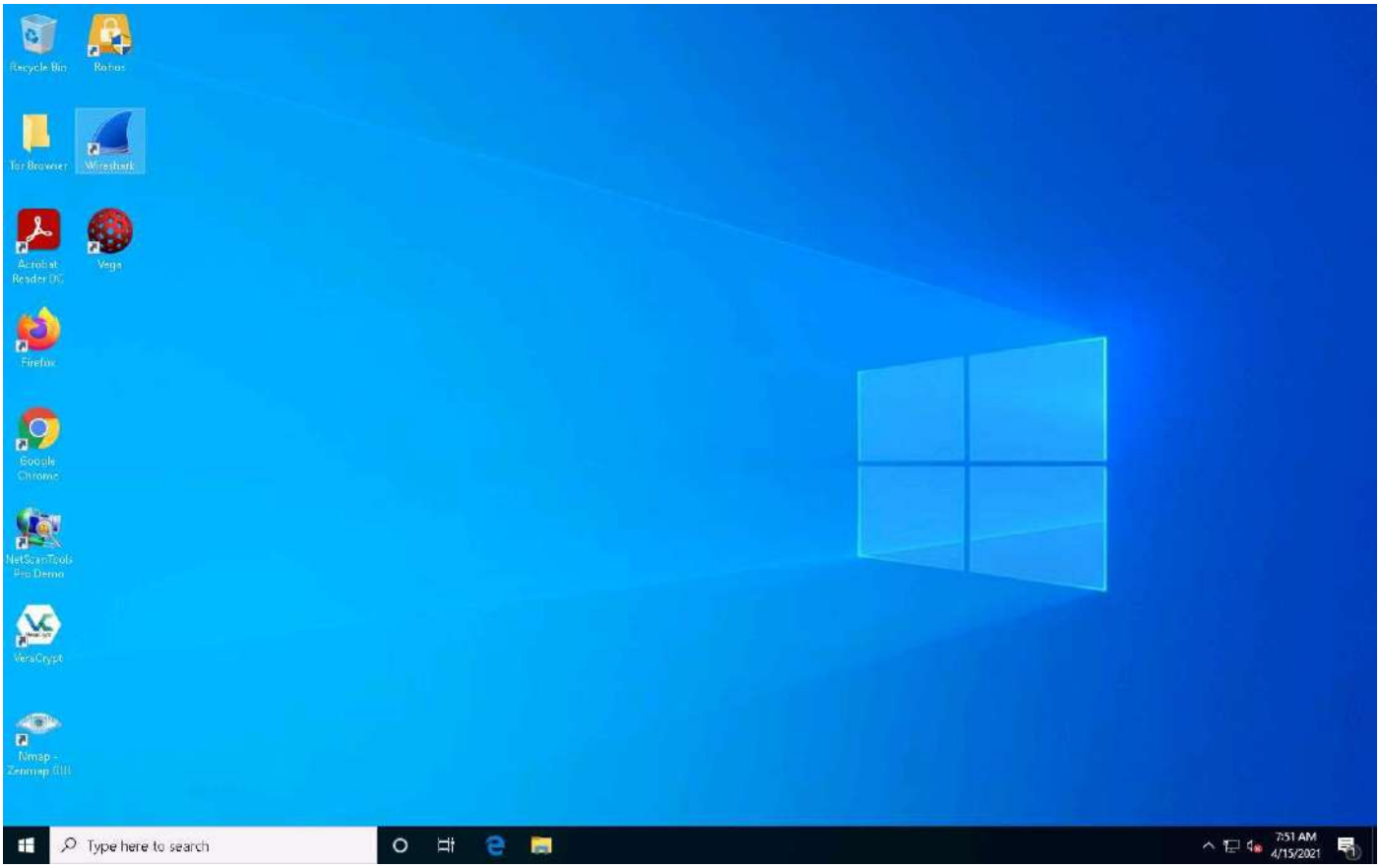
Alternatively, you can also click **Pa$$w0rd** under **Windows 10** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

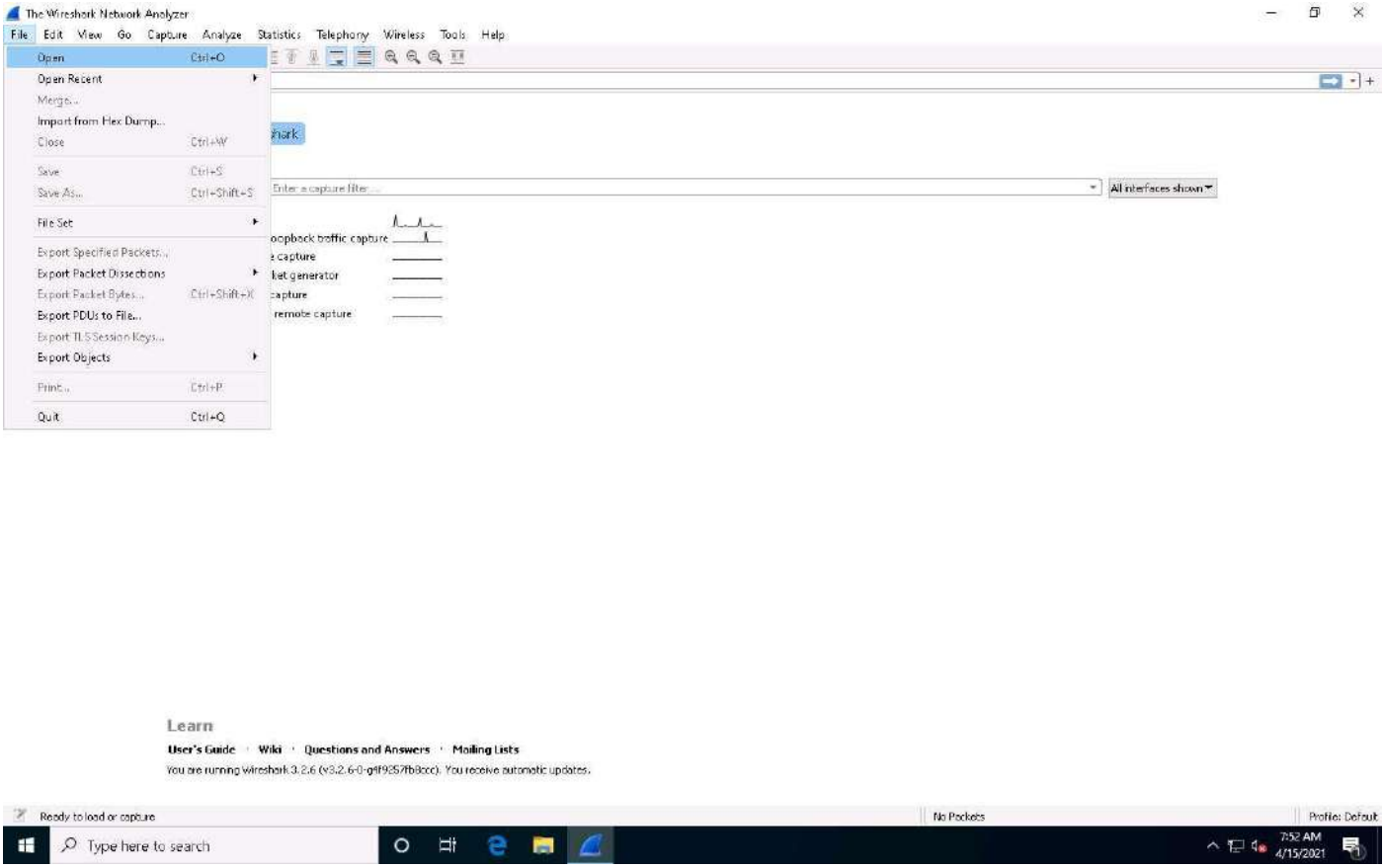
If **Networks** screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



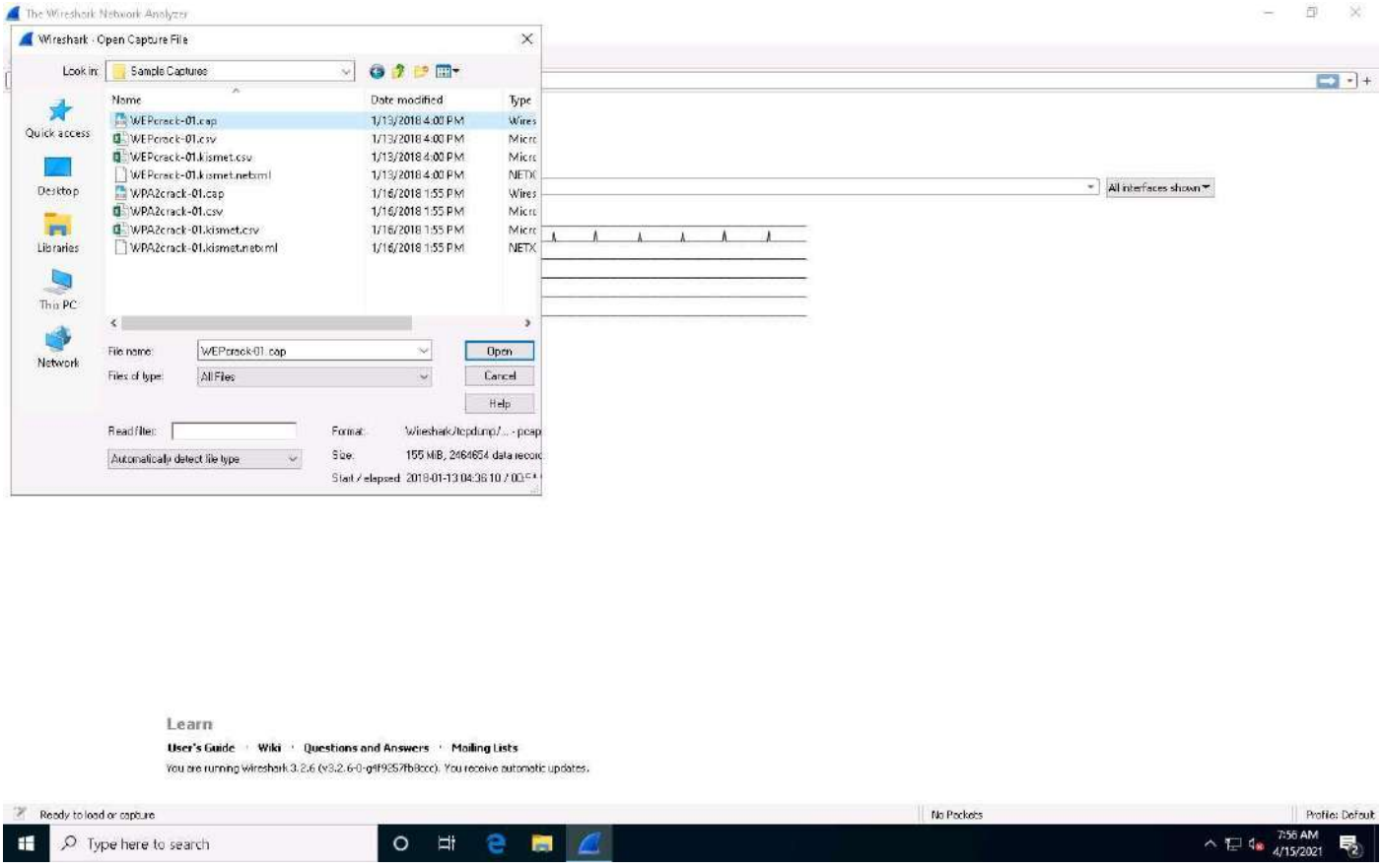
3. In the **Desktop**, double-click **Wireshark** shortcut.



4. The **Wireshark Network Analyzer** window appears.
5. In the menu bar, click **File** and click **Open** option from the drop-down list.



6. **Wireshark: Open Capture File** window appears, navigate to **D:\EHE-Tools\EHE Module 08 Wireless Attacks and Countermeasures\Sample Captures**, select **WEPcrack-01.cap** and click **Open**.



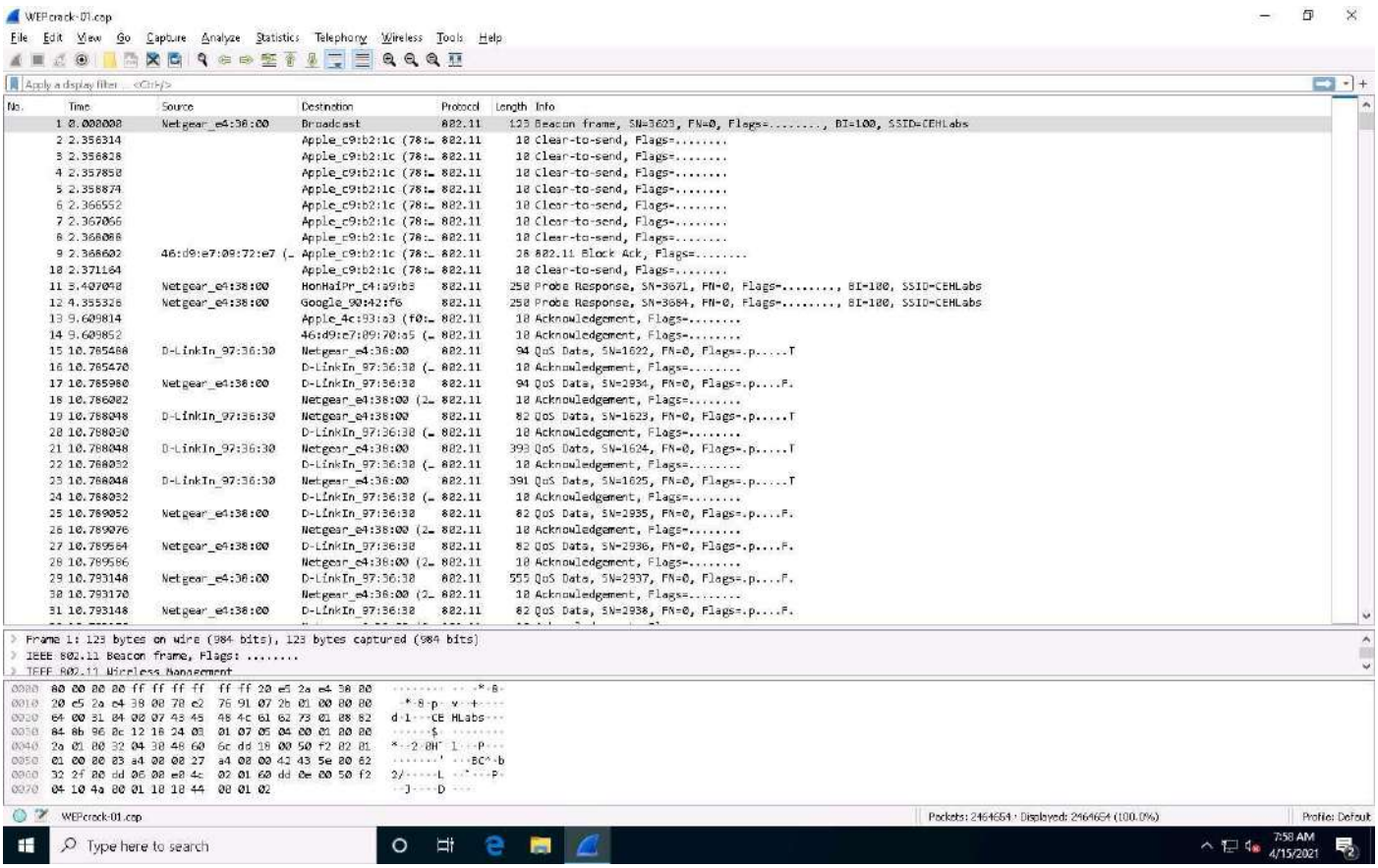
7. The **WEPcrack-01.cap** file opens in **Wireshark** window showing you the details of the packet for analysis. Here you can see the wireless packets captured which were otherwise masked to look like **ethernet** traffic.

Here 802.11 protocol indicates wireless packets.

You can access the saved packet capture file anytime, and by issuing packet filtering commands in the **Filter** field, you can narrow down the packet search in an attempt to find packets containing sensible information.

In real time, attackers enforce packet capture and packet filtering techniques to capture packets containing passwords (only for websites implemented on HTTP channel), perform attacks such as session hijacking, and so on.

Similarly, you can also analyze the **WPA2crack-01.cap** file for WPA packets.



8. This concludes the demonstration of how to analyze Wi-Fi packets using Wireshark.
9. Close all open windows and document all the acquired information.

Lab 8-2: Perform Wireless Attacks to Crack Wireless Encryption

Lab Scenario

You must have the required knowledge to perform wireless attacks in order to test the target network's security infrastructure.

After performing the discovery, mapping, and analysis of the target wireless network, you have gathered enough information to launch an attack. You should now carry out various types of attacks on the target network, including Wi-Fi encryption cracking (WEP, WPA, and WPA2), fragmentation, MAC spoofing, DoS, and ARP poisoning attacks.

WEP encryption is used for wireless networks, but it has several exploitable vulnerabilities. When seeking to protect a wireless network, the first step is always to change your SSID from the default before you actually connect the wireless router to the access point. Moreover, if an SSID broadcast is not disabled on an access point, ensure that you do not use a DHCP server, which would automatically assign IP addresses to wireless clients. This is because war-driving tools can easily detect your internal IP address.

You must test its wireless security, exploit WEP flaws, and crack the network's access point keys.

The labs in this exercise demonstrate how to perform wireless attacks using various hacking tools and techniques.

Lab Objectives

- Crack a WEP Network using Aircrack-ng
- Crack a WPA2 Network using Aircrack-ng

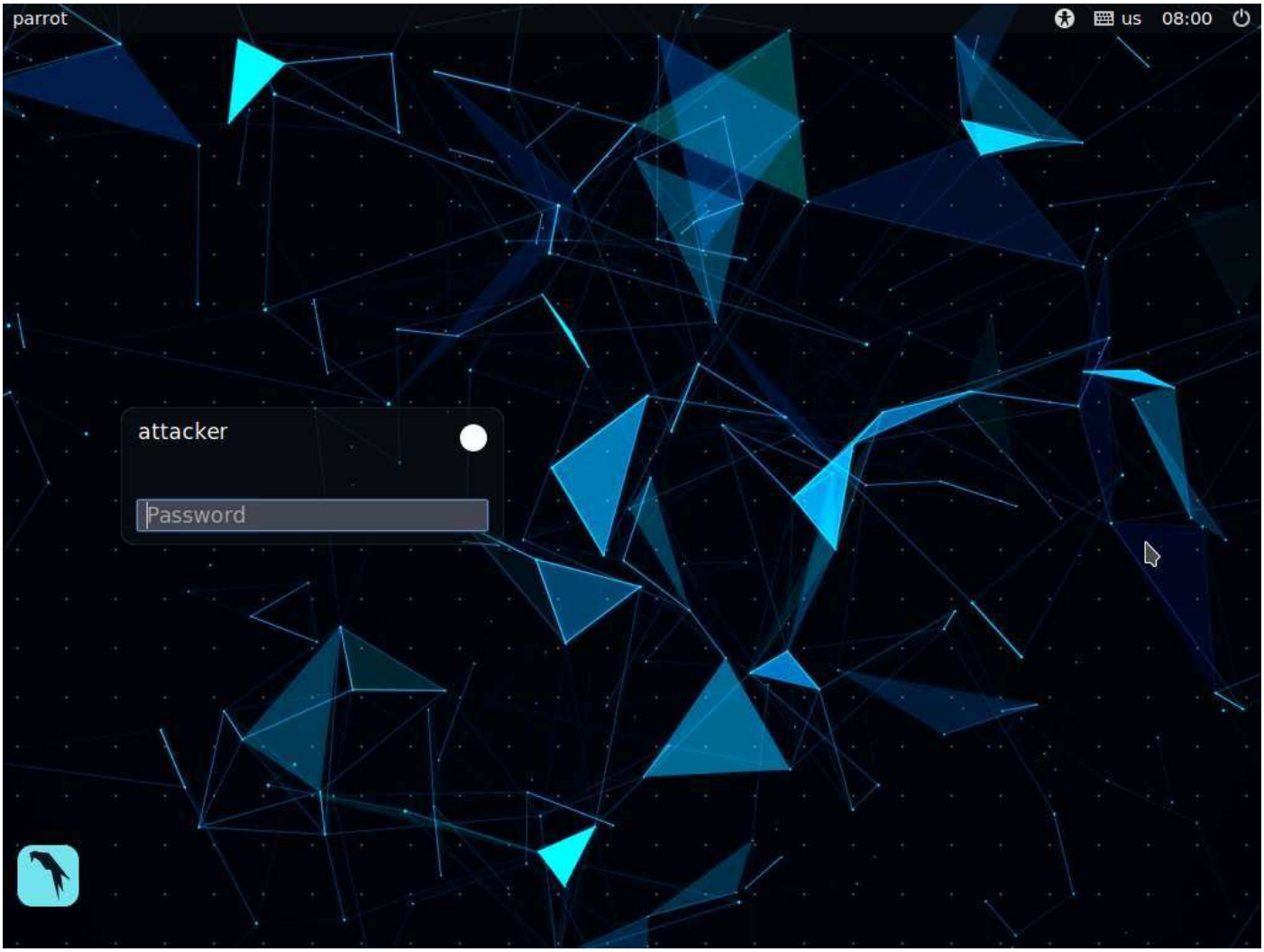
Task 1: Crack a WEP Network using Aircrack-ng

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP, and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. The program runs on both Linux and Windows.

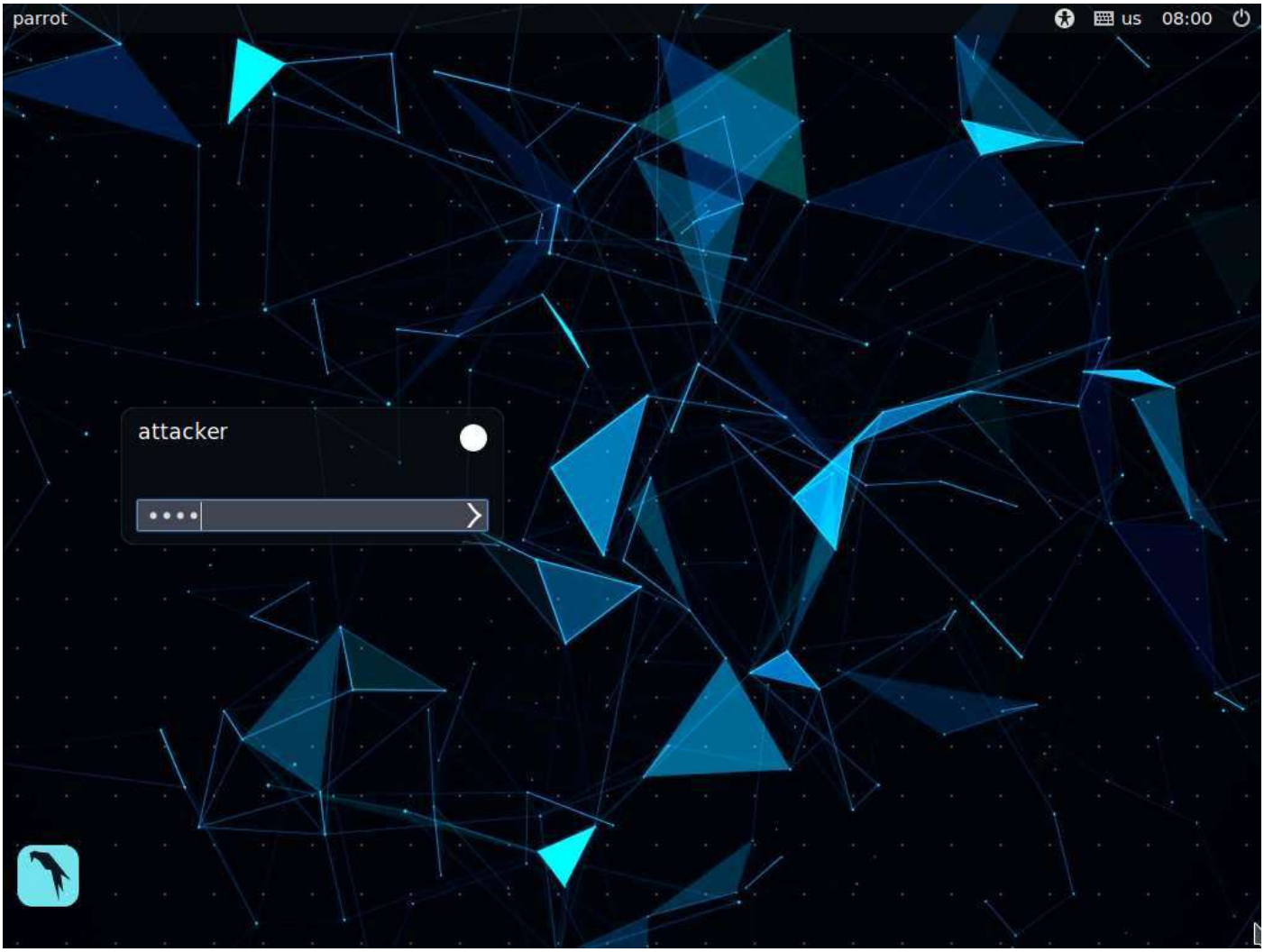
In this task, we will use the Aircrack-ng suite to crack the WEP encryption of a network.

In order to capture wireless traffic, a wireless adapter is required and using an adapter in the iLabs environment is not possible, therefore, in this lab, we are using a sample capture file (**WEPcrack-01.cap**) to crack WEP key.

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

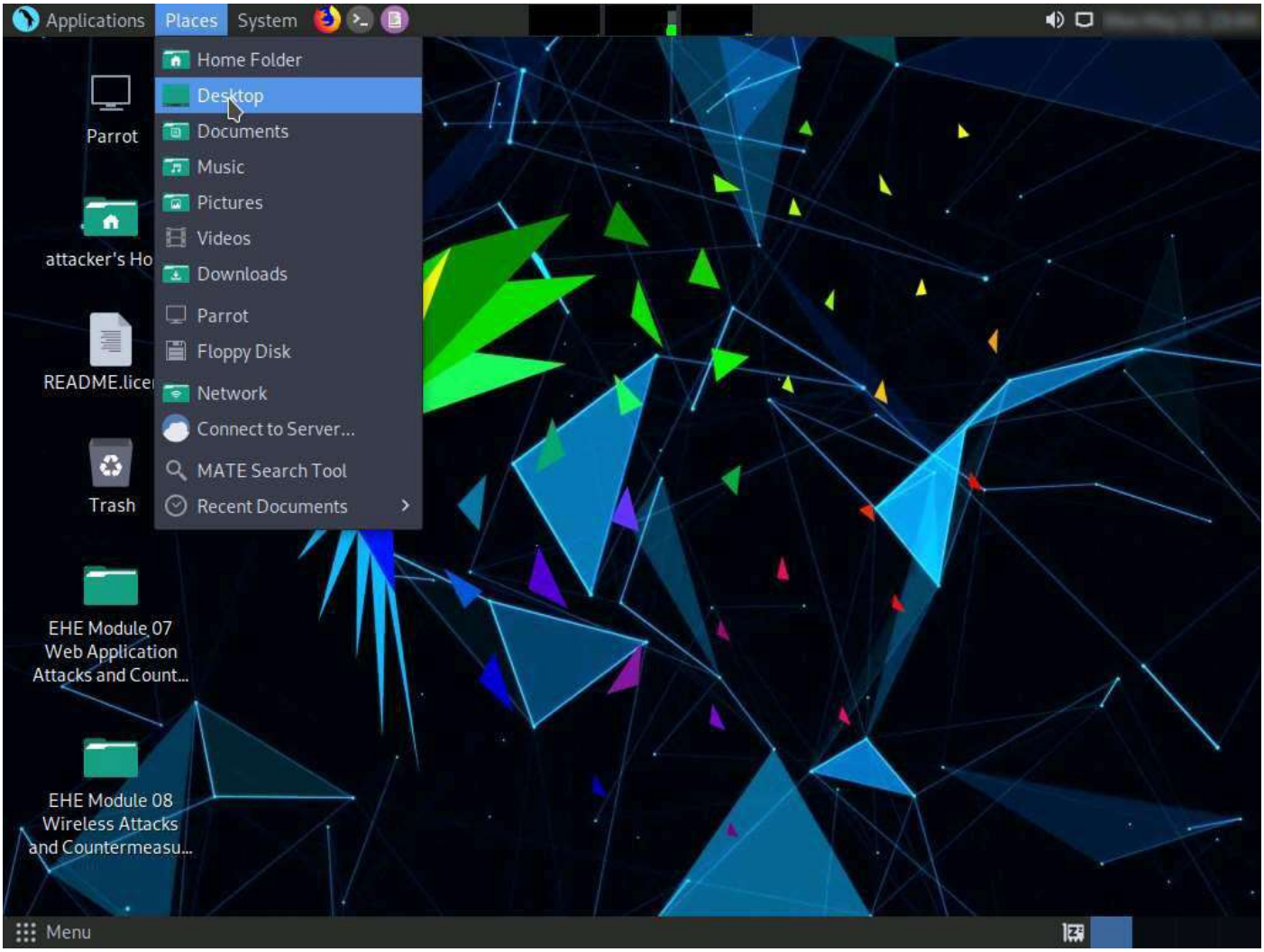


2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.



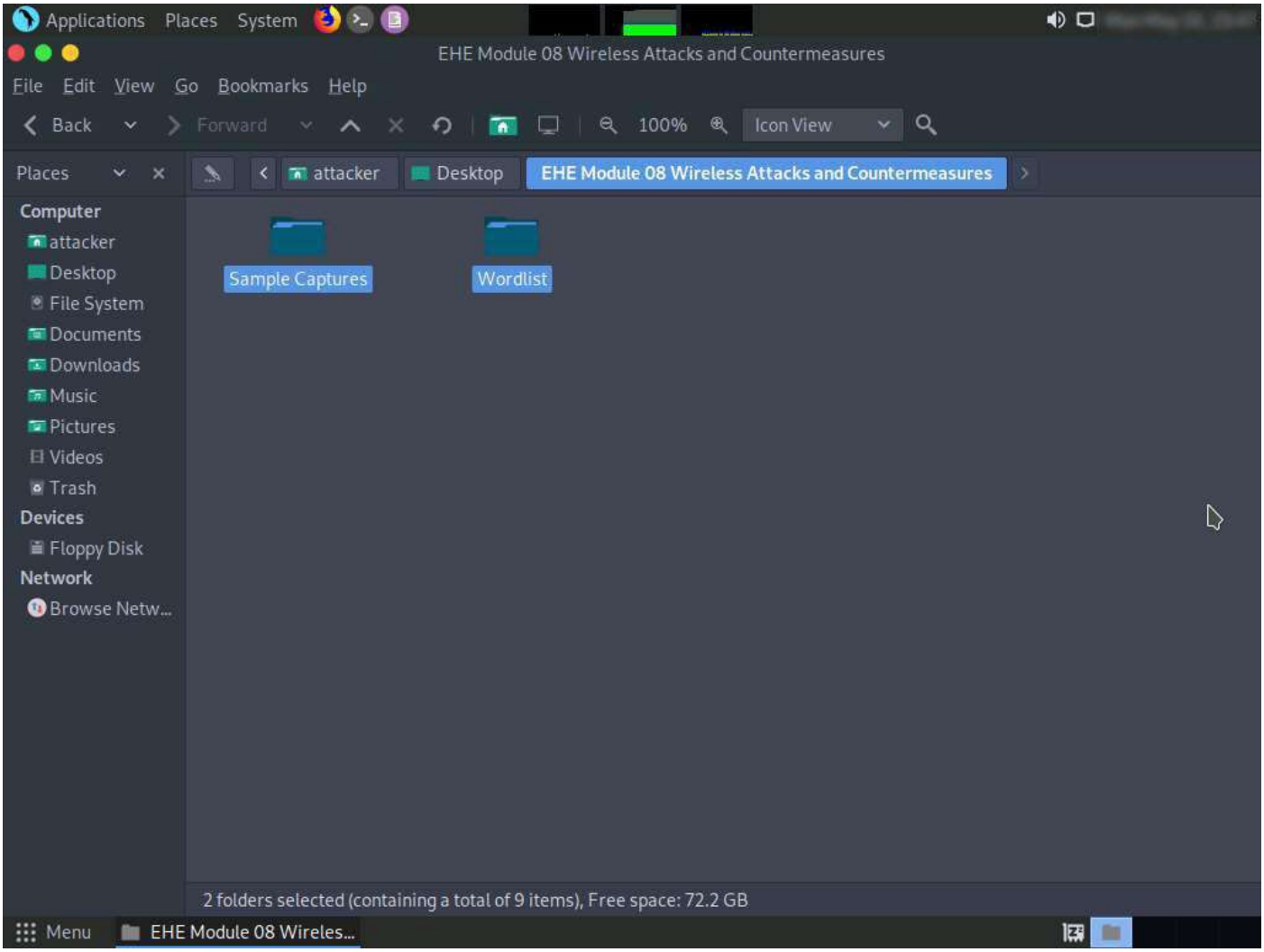
3. Navigate to the **Places** in the top-section of the window and click **Desktop** from the drop-down list.

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

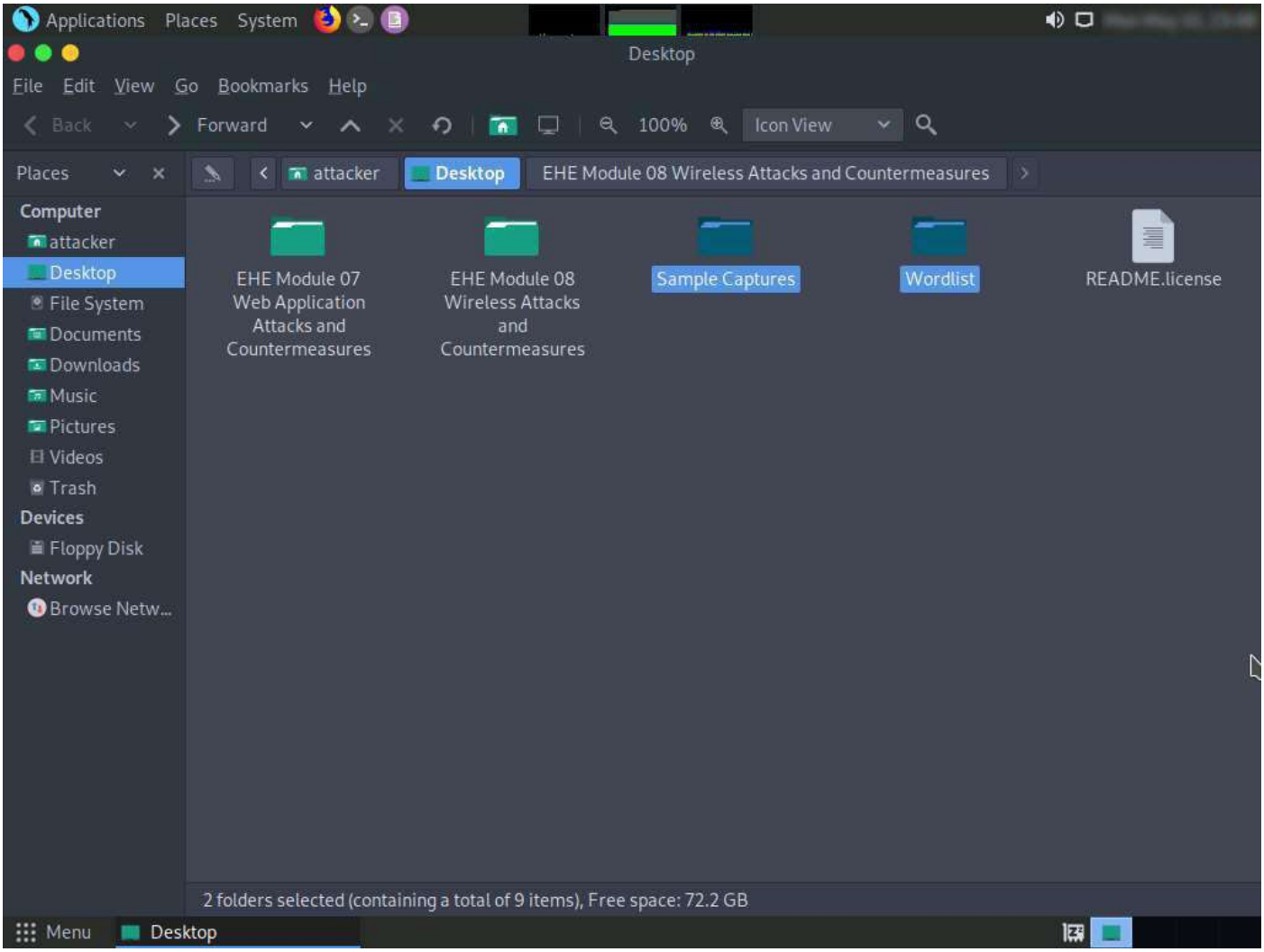


4. The **Desktop** window appears, navigate to the **EHE Module 08 Wireless Attacks and Countermeasures** folder and copy **Sample Captures** and **Wordlist** folders.

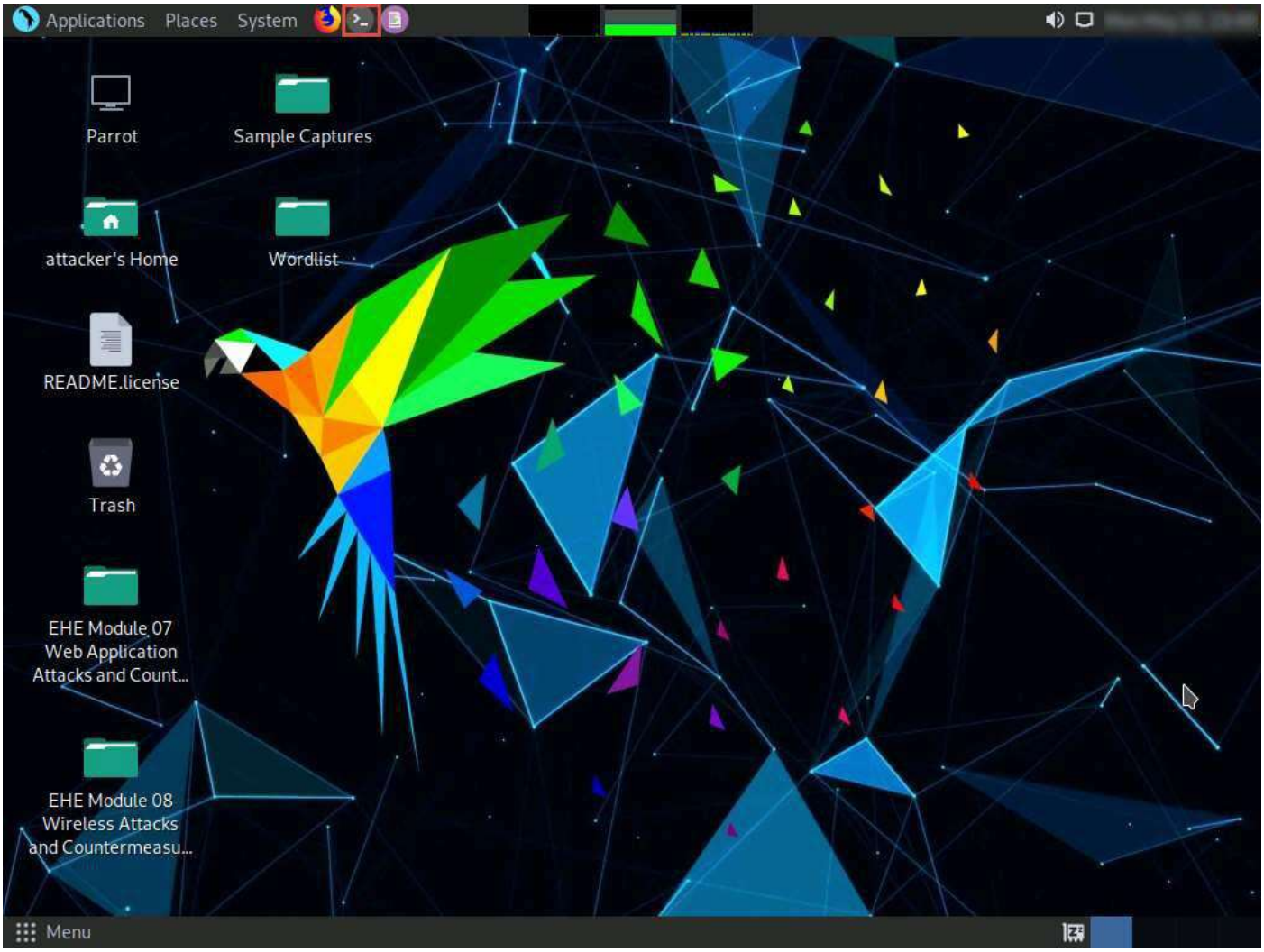
To copy the folders, firstly select both the folders and then press **Ctrl+C**.



5. Now, navigate to the **Desktop** and press **Ctrl+V** to paste the copied folders (**Sample Captures** and **Wordlist**). Close the **Desktop** window.



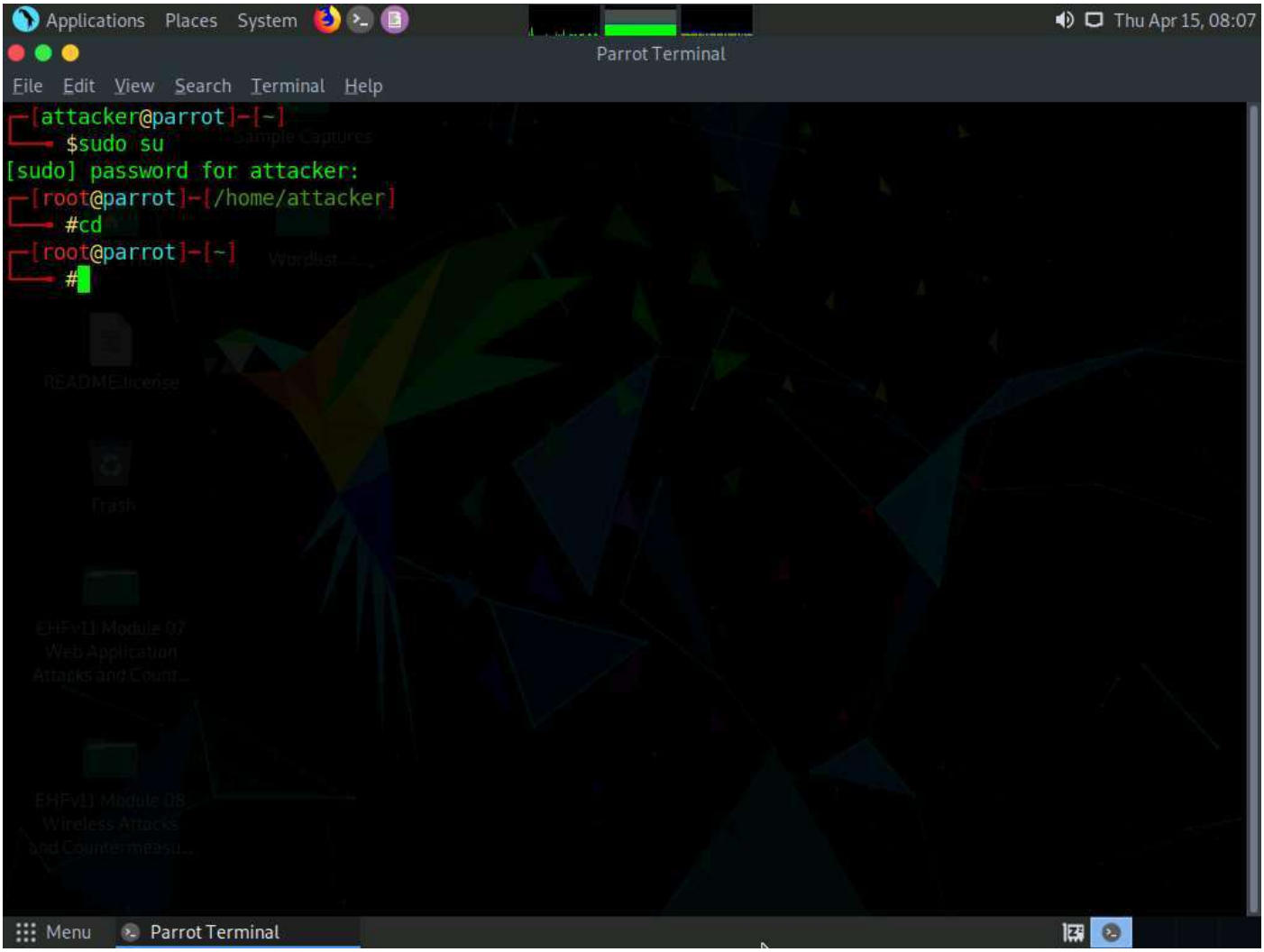
6. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



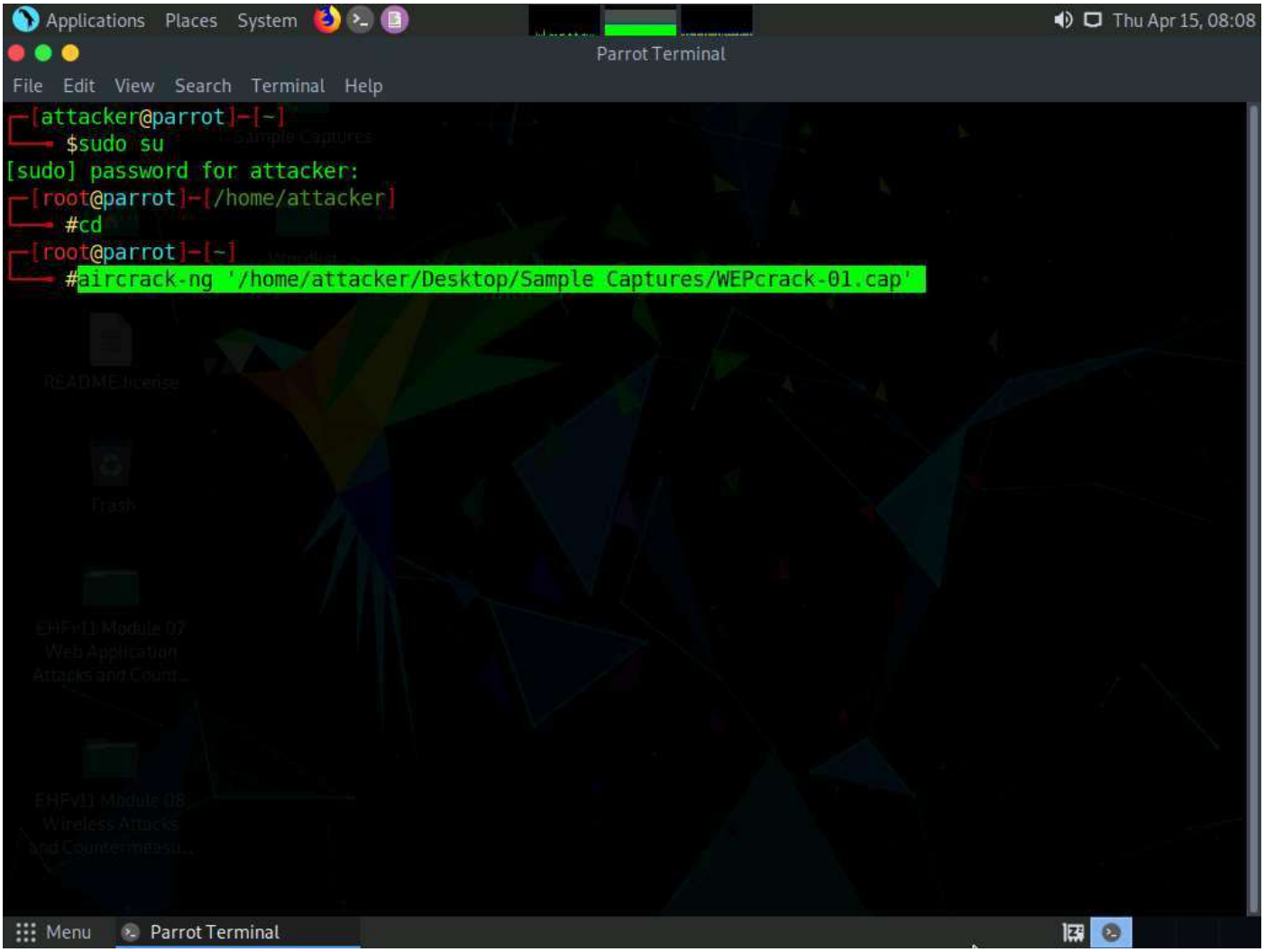
7. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
8. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

9. Now, type **cd** and press **Enter** to jump to the root directory.

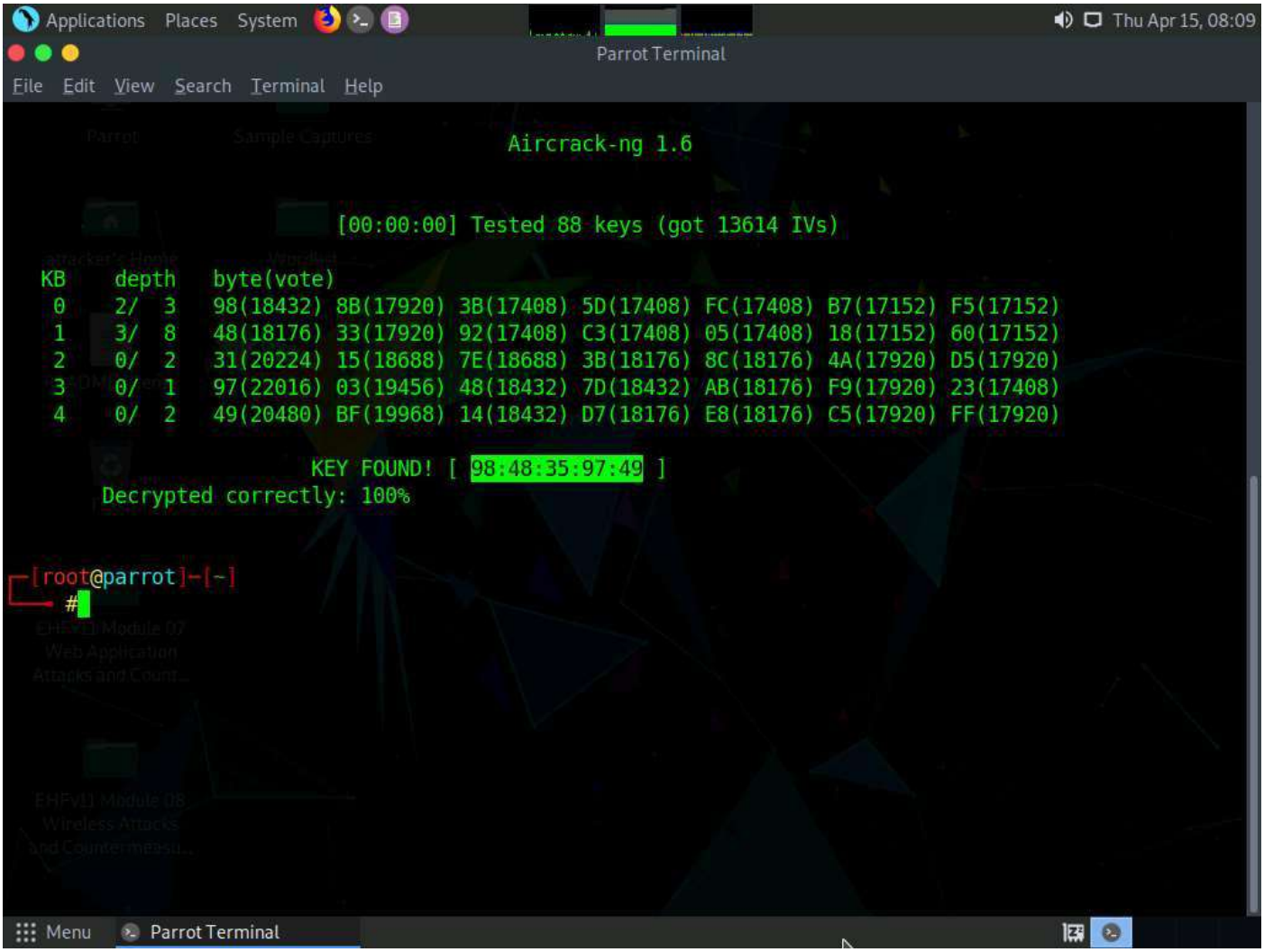


10. In the **Parrot Terminal** window, type **aircrack-ng '/home/attacker/Desktop/Sample Captures/WEPcrack-01.cap'** and press **Enter**.



11. By issuing the above command **aircrack-ng** will crack the WEP key of the access point, as shown in the screenshot.

In real-life attacks, attackers will use this key to connect to the access point and joint the target network. Once they enter the target network, they can use scanning tools to scan for open devices, perform a vulnerability analysis, and then start exploiting any vulnerabilities they find.



12. This concludes the demonstration of how to crack a WEP network using Aircrack-ng.
13. Close all open windows and document all the acquired information.

Task 2: Crack a WPA2 Network using Aircrack-ng

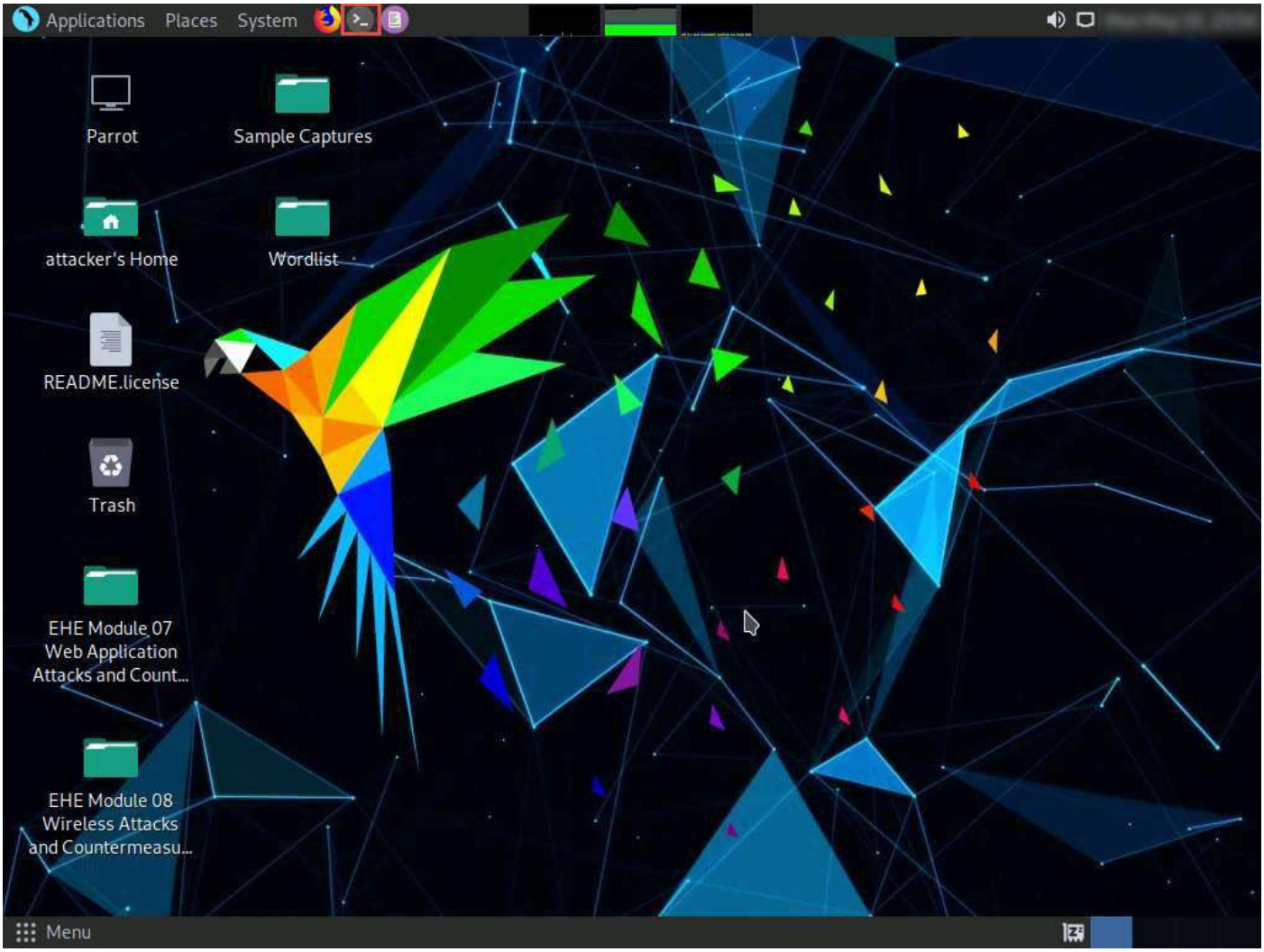
WPA2 is an upgrade to WPA; it includes mandatory support for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), an AES-based encryption protocol with strong security. WPA2 has two modes of operation: WPA2-Personal and WPA2-Enterprise. Despite being stronger than both WEP and WPA, the WPA2 encryption method can also be cracked using various techniques and tools.

In this task, we will use the Aircrack-ng suite to crack a WPA2 network.

In order to capture wireless traffic, a wireless adapter is required and using an adapter in the iLabs environment is not possible, therefore, in this lab, we are using a sample capture file (**WPA2crack-01.cap**) to crack WPA key.

Ensure that **Sample Captures** and **Wordlist** folders are present at the location **home/attacker/Desktop** which we copied in the previous task. If not, then navigate to the **EHE Module 08 Wireless Attacks and Countermeasures** folder on the **Desktop**, copy the **Sample Captures** and **Wordlist** folders and paste them at the location **home/attacker/Desktop**.

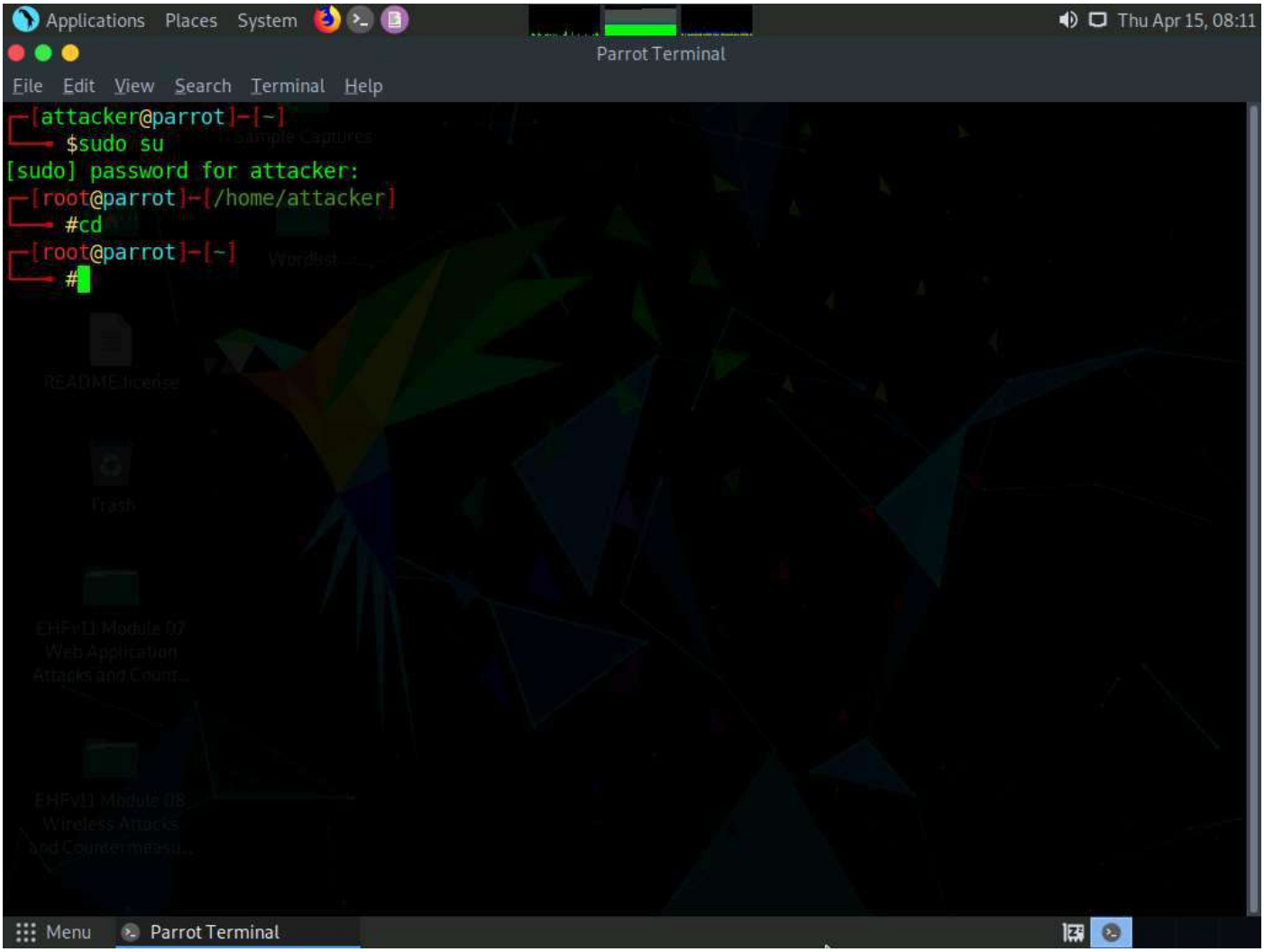
1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



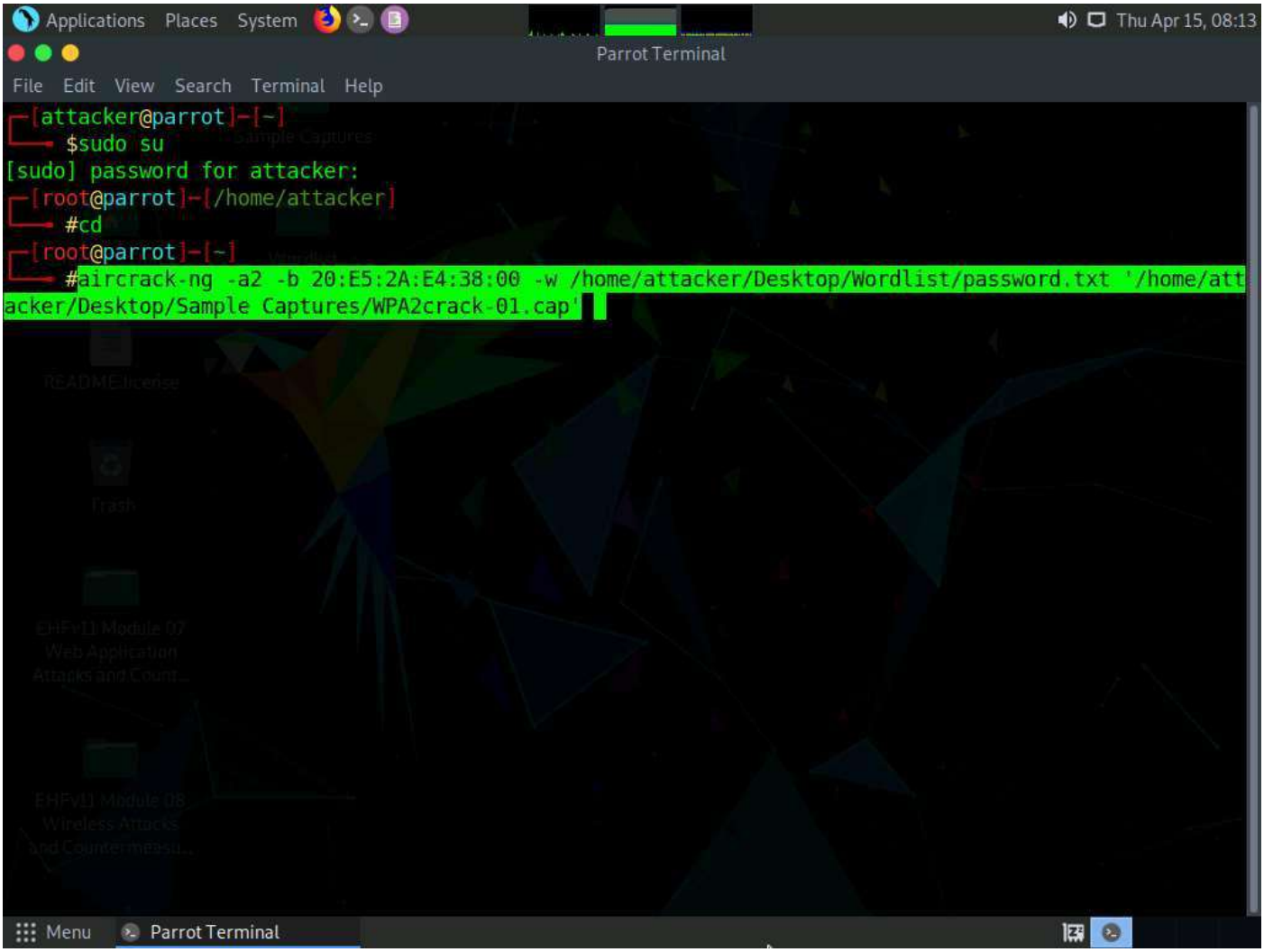
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

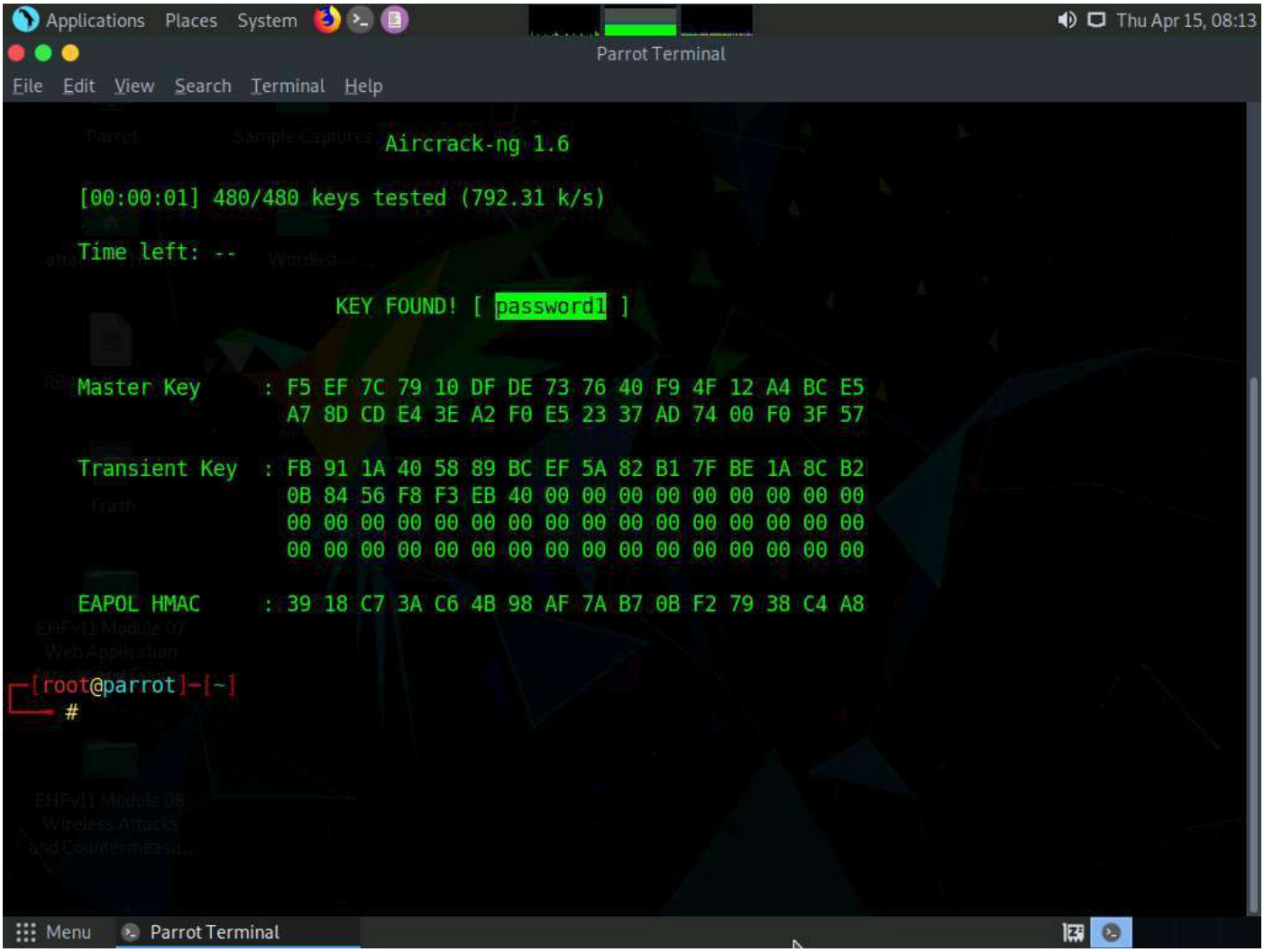


5. In the **Parrot Terminal** window, type **aircrack-ng -a2 -b [Target BSSID] -w /home/attacker/Desktop/Wordlist/password.txt '/home/attacker/Desktop/Sample Captures/WPA2crack-01.cap'** and press **Enter**. Here, the BSSID of the target is **20:E5:2A:E4:38:00**.
    - **-a** is the technique used to crack the handshake, **2**=WPA technique.
    - **-b** refers to bssid; replace with the BSSID of the target router.
    - **-w** stands for wordlist; provide the path to a wordlist.



6. The result appears, showing the WPA handshake packet captured with airodump-ng. The target access point's password is cracked and displayed in plain text next to the message **KEY FOUND!**, as shown in the screenshot.

If the password is complex, aircrack-ng will take a long time to crack it.



7. This concludes the demonstration of how to crack a WPA2 network using Aircrack-ng.
8. Close all open windows and document all the acquired information.