

RMIT  
Classification:  
Trusted

## Practical Exercise Submission Template

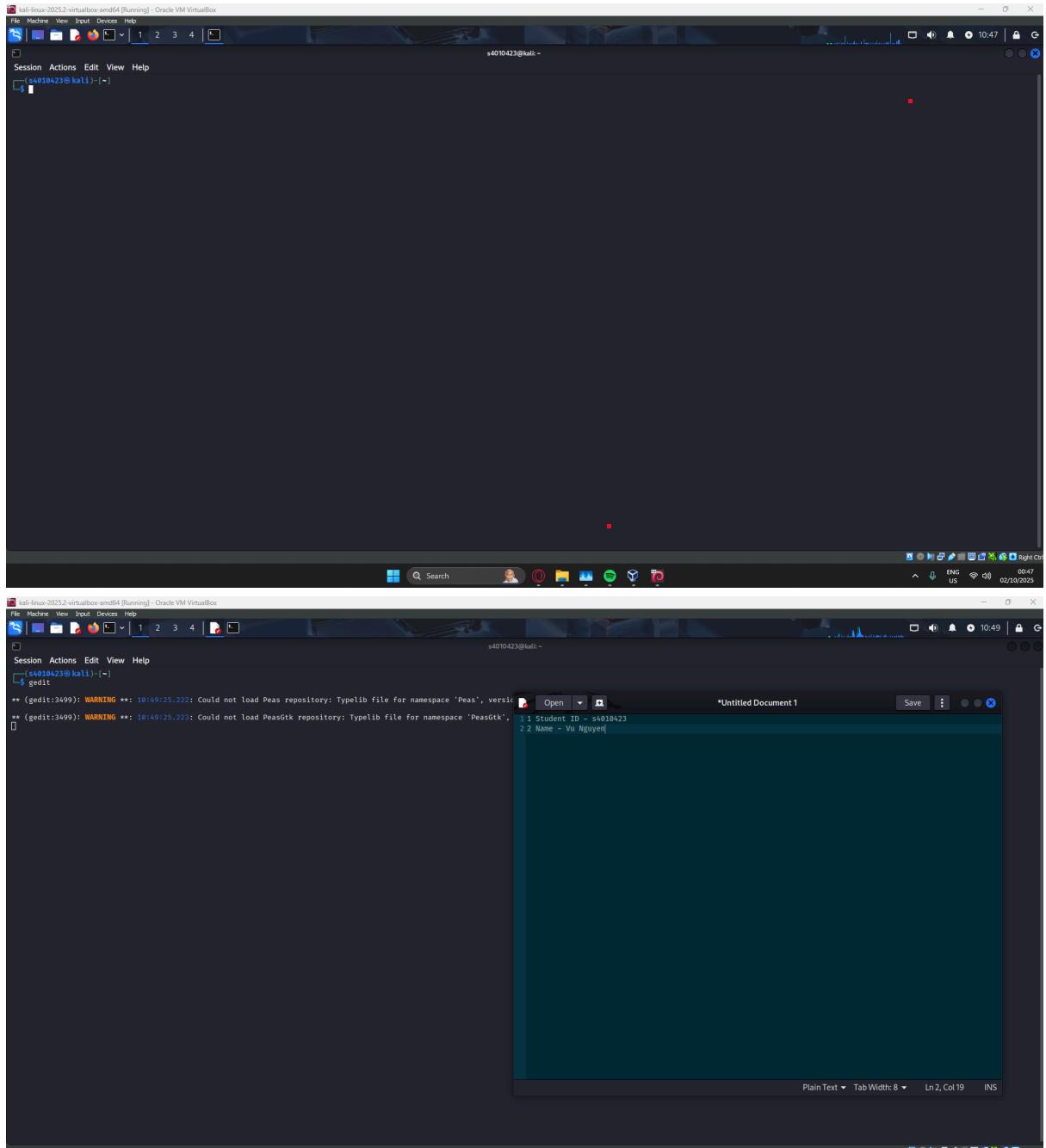
### Task 2a Practical Lab exercises

**STD ID: s4010423**

**Name: Vu Nguyen**

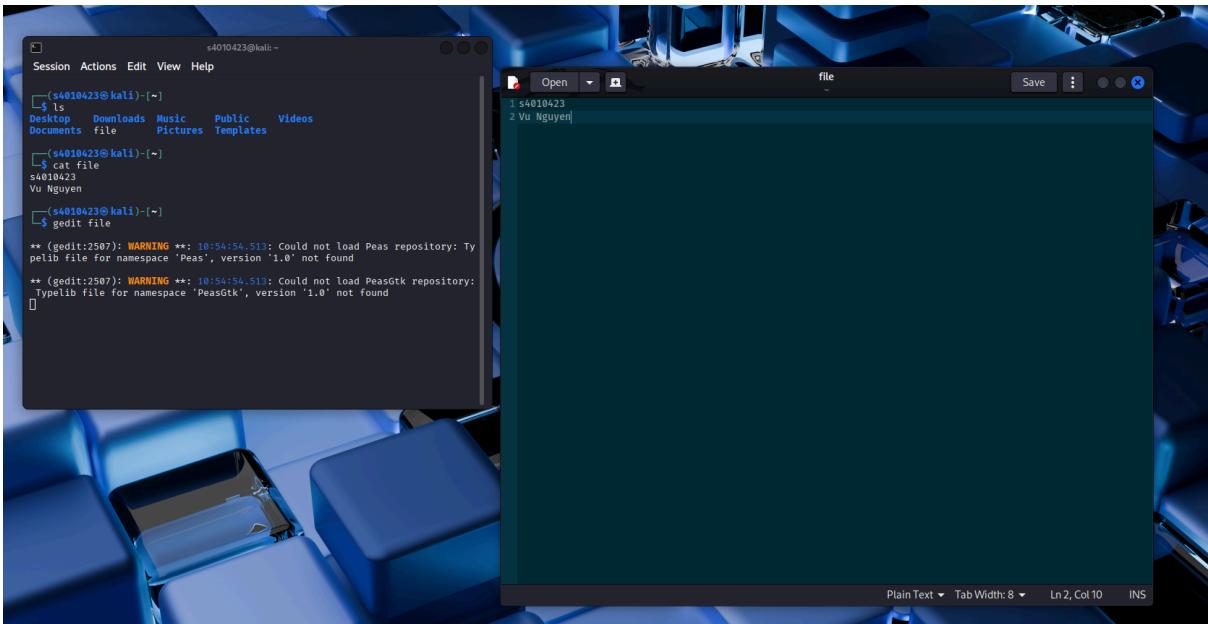
#### Task 1

- Successful Installation of Kali and Creation of user account with student ID**

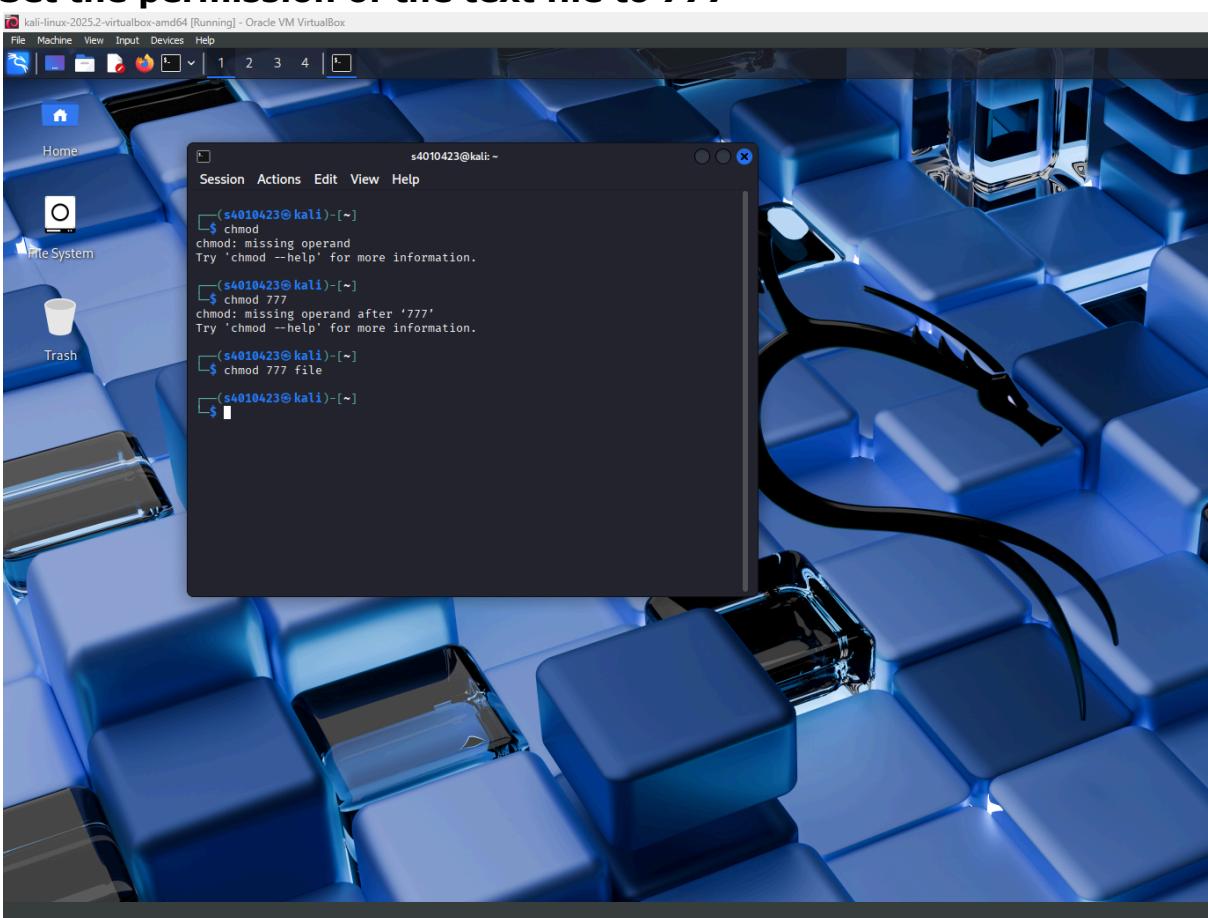


RMIT  
Classification:  
Trusted

- Successful creation of the text file inside the home folder



- Set the permission of the text file to 777



SMT  
Classification:  
Trusted

## Task 2

- Launching Recon-ng from personal account

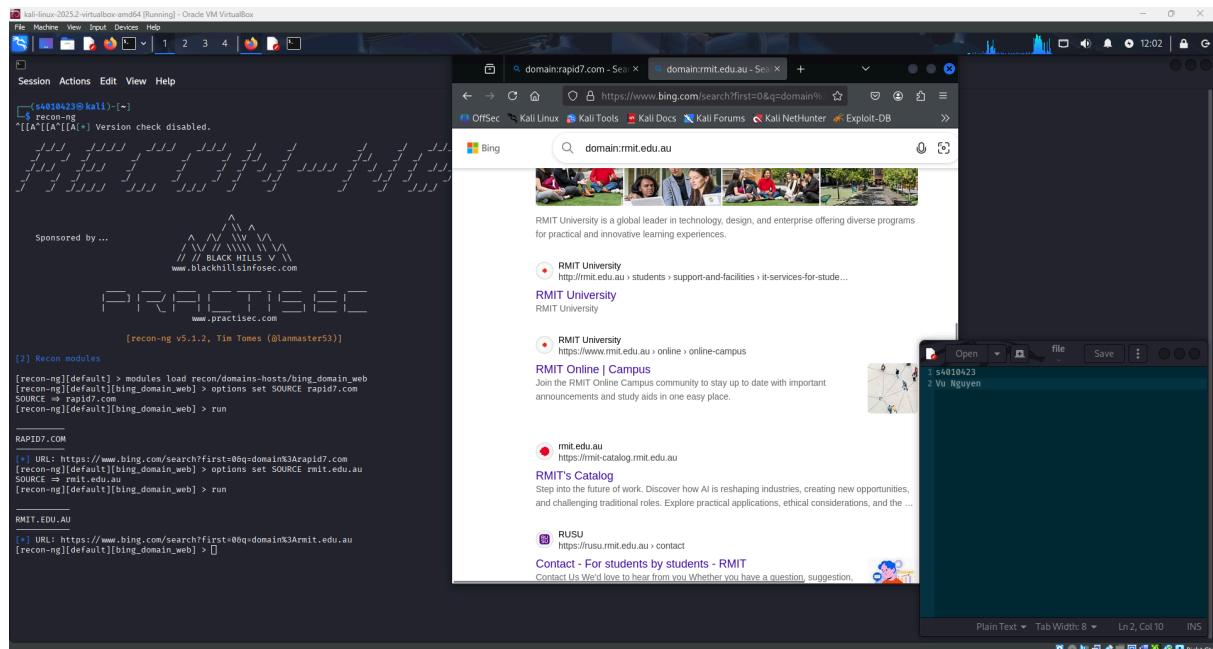
**Follow the Above sample template for the rest of the requirements**

- Install both `hackertarget` and `bings_domain_web` modules

RMIT  
Classification:  
Trusted

- Reconnaissance of RMIT's primary domain using both modules

```
[*] ali-foxx-2023-2-vxlab.rmit.edu.au [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
[+] Country: None  
[*] Host: cstrike240_vxlab.rmit.edu.au  
[*] Ip_Address: 131.170.250.240  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] Country: None  
[*] Host: cstrike241_vxlab.rmit.edu.au  
[*] Ip_Address: 131.170.250.241  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] Country: None  
[*] Host: cstrike242_vxlab.rmit.edu.au  
[*] Ip_Address: 131.170.250.242  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] Country: None  
[*] Host: cstrike243_vxlab.rmit.edu.au  
[*] Ip_Address: 131.170.250.243  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] Country: None  
[*] Host: cstrike244_vxlab.rmit.edu.au  
[*] Ip_Address: 131.170.250.244  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] Country: None  
[*] Host: cstrike245_vxlab.rmit.edu.au  
[*] Ip_Address: 131.170.250.245  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*] --  
  
SUMMARY  
[*] 500 total (500 new) hosts found.  
[recon-ng][default][hackertarget] > █
```

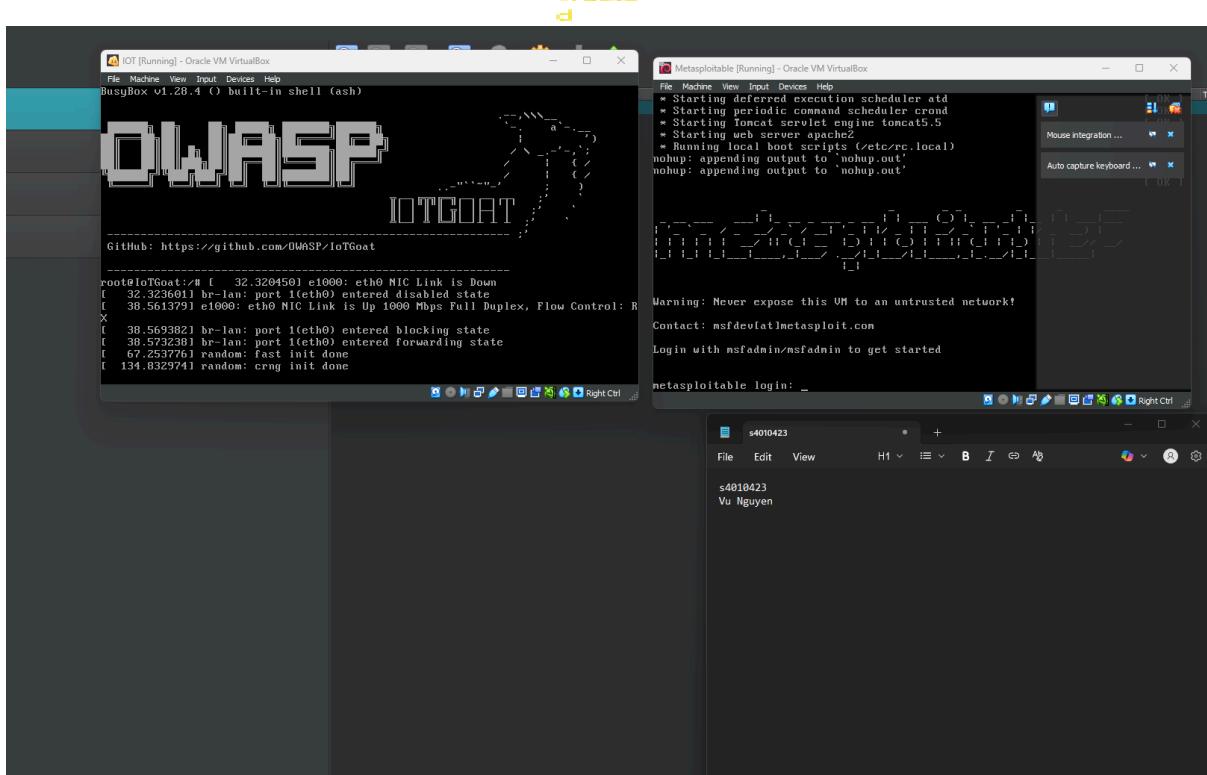


- Reconnaissance of another domain using both tools

The screenshot shows two Kali Linux desktop environments. The top window is a terminal session titled 'kali-linux-2023.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox'. It displays a list of hosts found by the 'recon-ng' tool, including their country, hostnames, IP addresses, and regions. The bottom window is a web browser titled 'domain:rapid7.com - Search | +'. It shows search results for 'domain:rapid7.com' on Bing, including links to Rapid7's login page, About page, and Cybersecurity Services. A status bar at the bottom right indicates 'Plain Text Tab Width: 8 Ln 2, Col 10'.

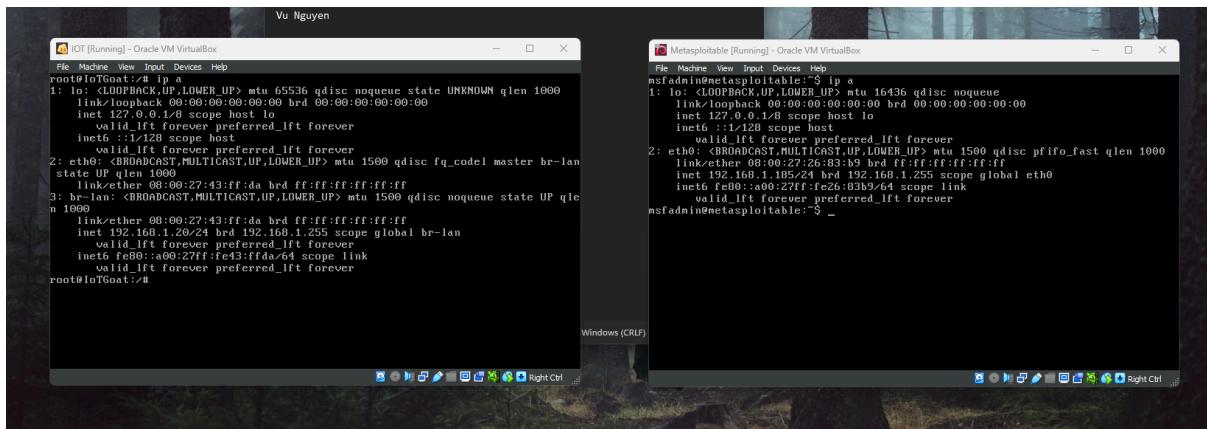
### **Task 3:**

- Installation of Metasploit and IoTGoat Virtual machines

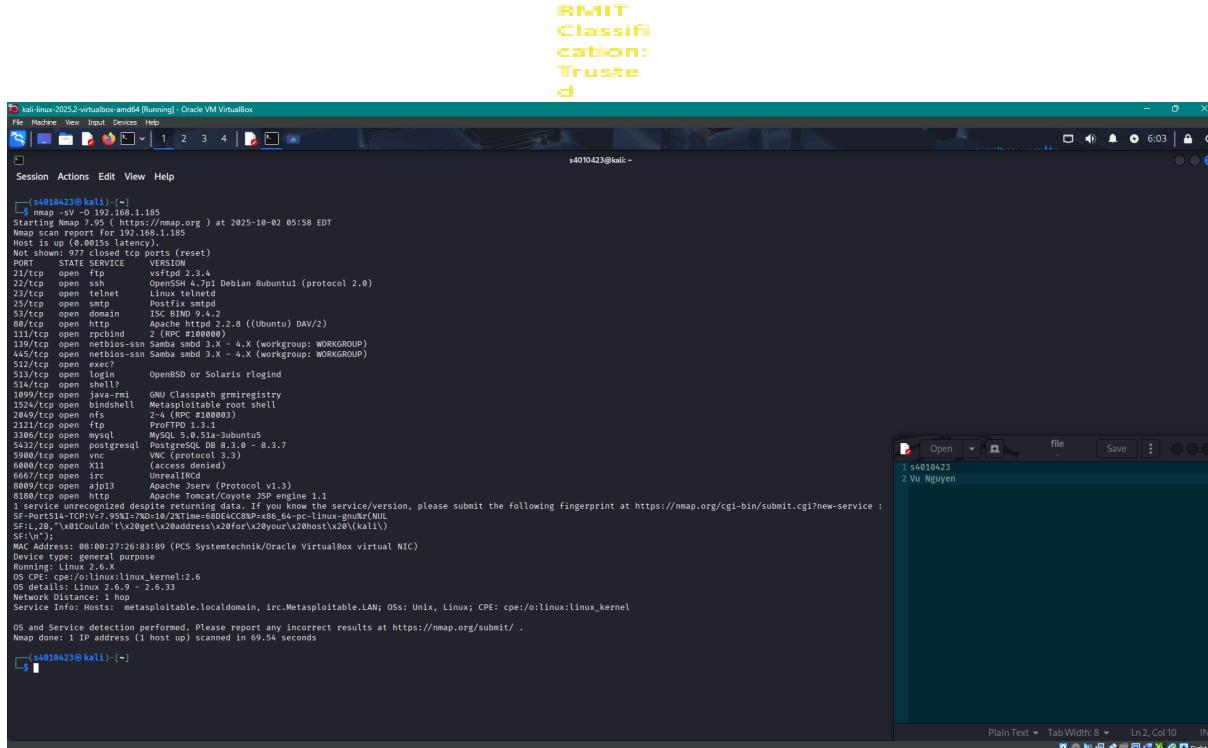


The above screenshot shows that I have successfully installed both virtual machines.

## Follow the Above sample template for the rest of the requirements

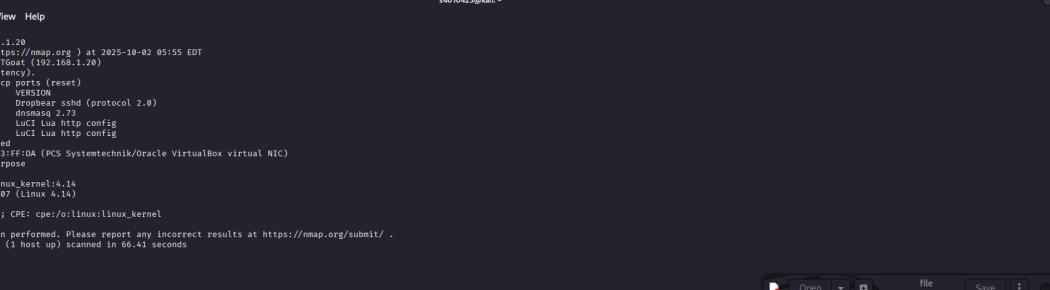


- Port scanning results for MetaSploit Virtual machine



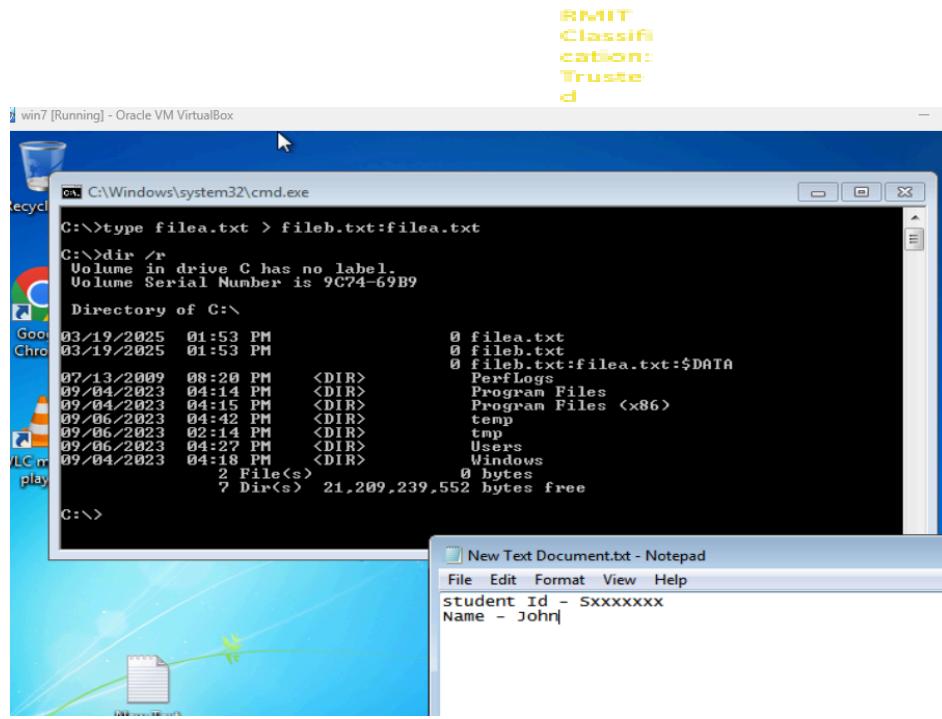
- Port scanning results for IoTGoat Virtual machine

```
 kali-nmap-2025.2-vm-1.vmdk [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
[ ]  
Session Actions Edit View Help  
[+] s4010423@kali: ~  
└─ $ nmap -sv -oN nmap.txt -p 1-2000 192.168.1.20  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-02 05:55 EDT  
Nmap scan report for 192.168.1.20  
Host is up (0.00094s latency).  
Not shown: 995 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh     OpenSSH 8.0p1, OpenSSL 1.1.1l 2020-02-23  
53/tcp    open  domain  dnsmasq 2.73  
80/tcp    open  http    LuCI  Lua http config  
443/tcp   open  https   LuCI  Lua http config  
5800/tcp  open  tcpwrapped  
MAC Address: 08:00:27:43:FF:DA (PC Systemtechnik/Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Linux 4.14  
OS CPE: cpe:/o:linux:linux_kernel:4.14  
OS details: OpenWrt 19.07 (Linux 4.14)  
Network Distance: 1 hop  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
Nmap done: 1 IP address (1 host up) scanned in 86.41 seconds  
[+] s4010423@kali: ~
```



#### **Task 4:**

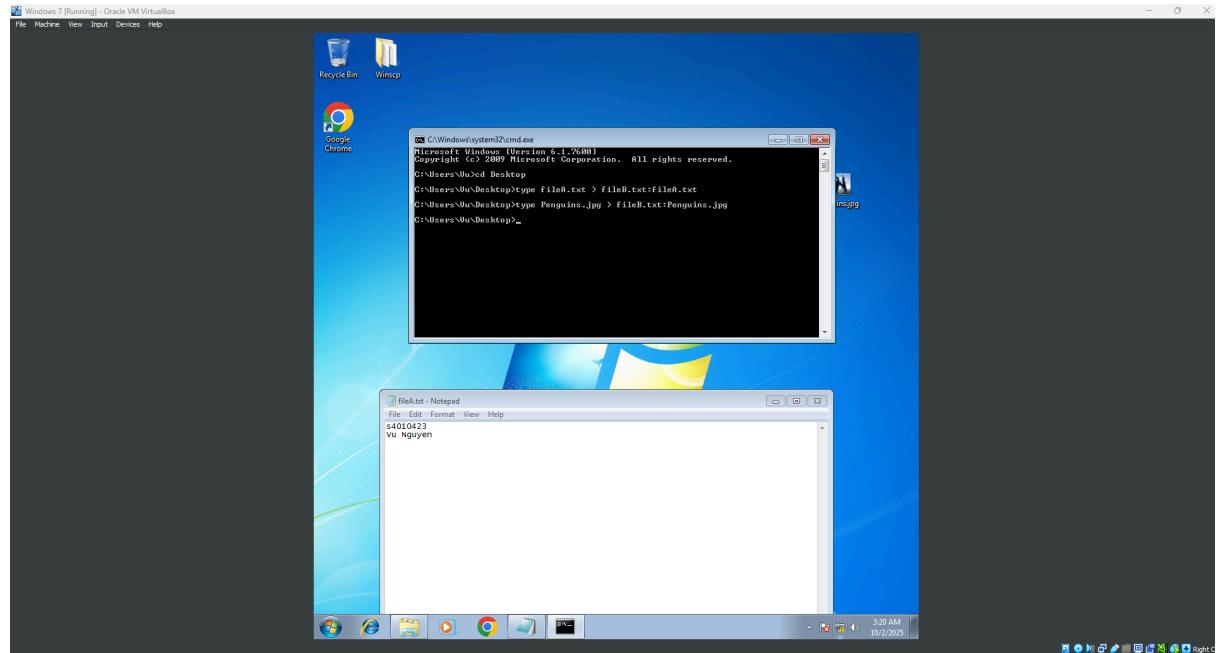
- **Command execution of hiding a textfile in the ADS of another textfile**

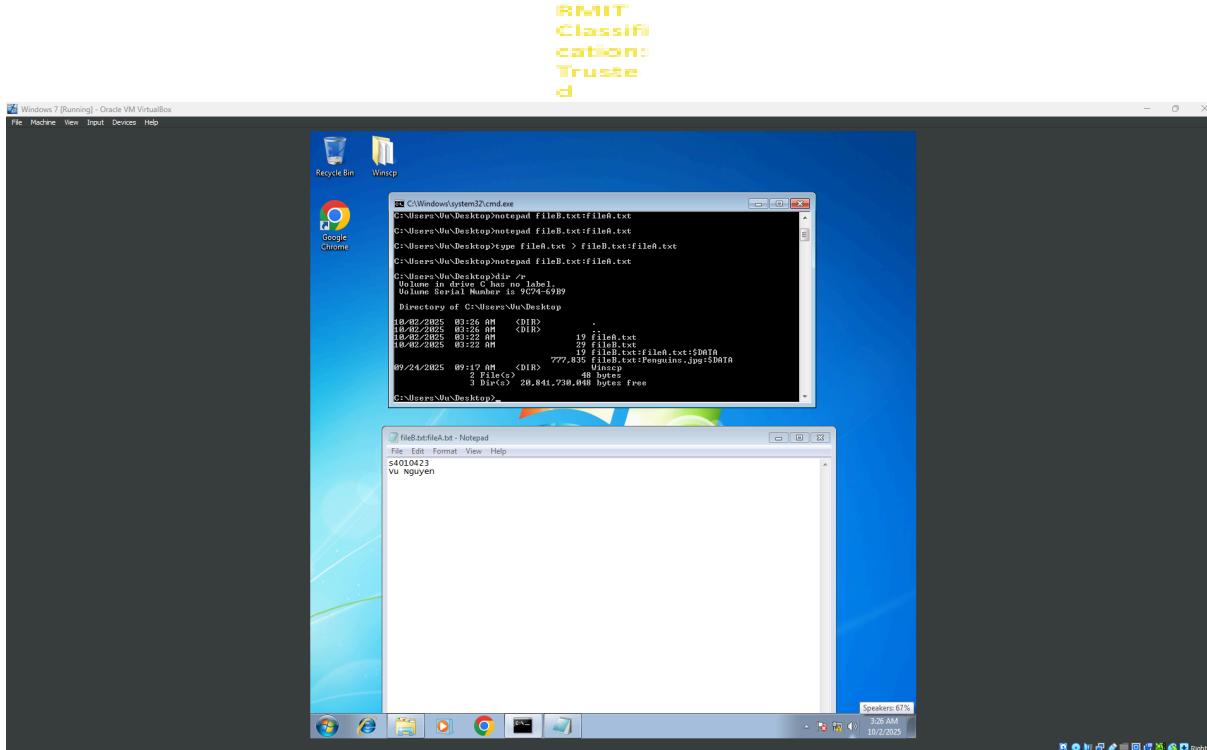


The above screenshot shows that filea has been successfully hidden in the ADS of fileb.

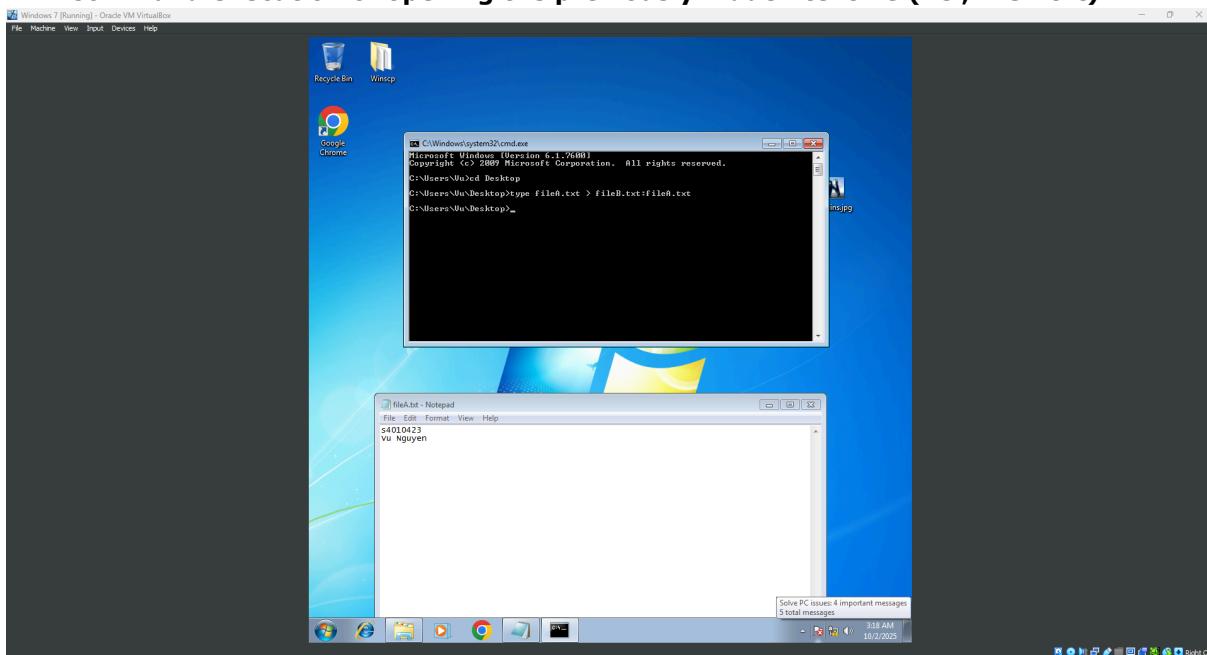
## Follow the Above sample template for the rest of the requirements

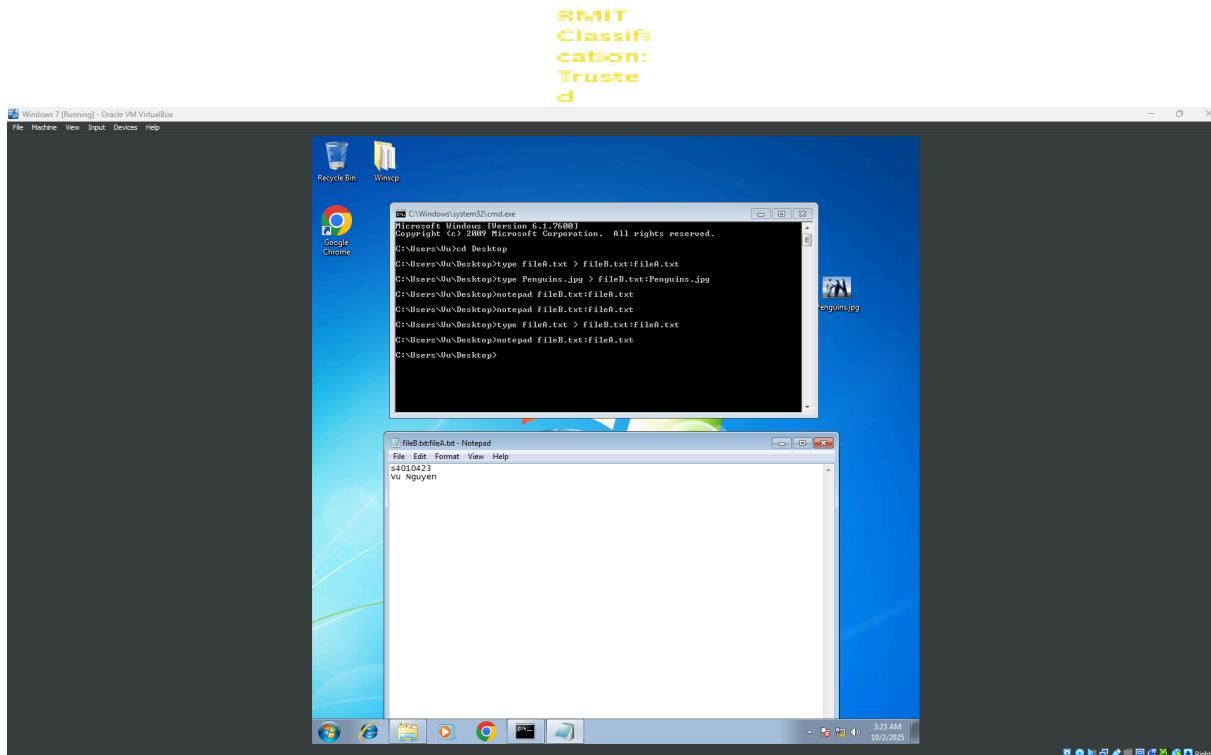
- **Command execution of hiding an image file (image.jpeg) in the ADS of the previously used text file (fileB.txt)**





- **Command execution of opening the previously hidden textfile (i.e., fileA.txt)**





- Command execution of opening the previously hidden image file (i.e., image.jpeg)

