1) Attacking from Kali to windows -

① start VM < kali
window

② VM → windows → cmd → ipconfig → Note it down

(for windows - ipconfig
kali - ifconfig)

③ VM → kali → cmd →

- sudo su
- password - kali
- type all commands.

(we hv to use IP of windows to execute all commands).

kali (attacker)
windows (victim)

2) phishing → attackers trick ppl into revealing sensitive info like password eg fake email to get password...

- to see installatⁿ of socialphish → refer manual.

① VM → kali → firefox / chrome → social phish. github (go on this site)

→ take url/code → paste it in kali (cmd) →

ⓐ cd socialphish
ⓑ ./socialphish.sh
ⓒ choose option ~~from~~ - Instagram (enter it's code)
ⓓ link generate (open link)
ⓔ enter fake email / Id . & Pass.

[Psudo su
[pass - kali } helps you to get in root folder. (you can use it after step ⓐ or ⓑ if error occur).

1) Attacking from Kali to windows -

① start VM < kali
window

② VM → windows → cmd → ipconfig → Note it down

(for windows - ipconfig
kali - ifconfig)

③ VM → Kali → ~~$~~ cmd →

- sudo su
- password - kali
- type all commands.
  (we hv to use IP of windows to execute all commands).

1- enter ipconfig in window(vm)
2- in kali command
promt enter-
1-sudo su
2-pass
3- all commands given
by pratyush

Kali Linux Commands

Attacking from kali (attacker) to windows (victim)

For ip address in kali terminal, the command is: ifconfig

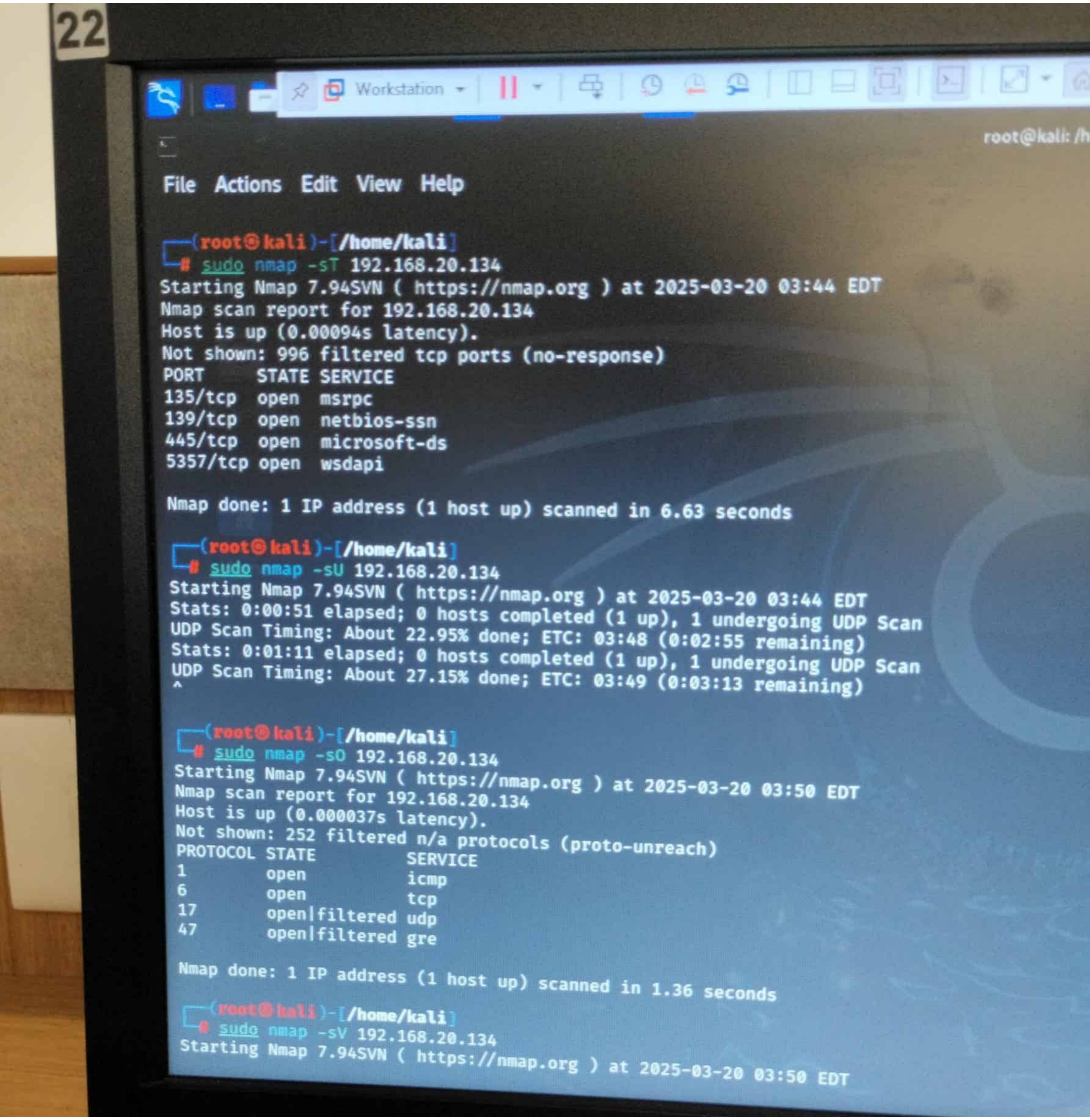
For ip address in windows, the command is: ipconfig

Then enter these commands in kali terminal:

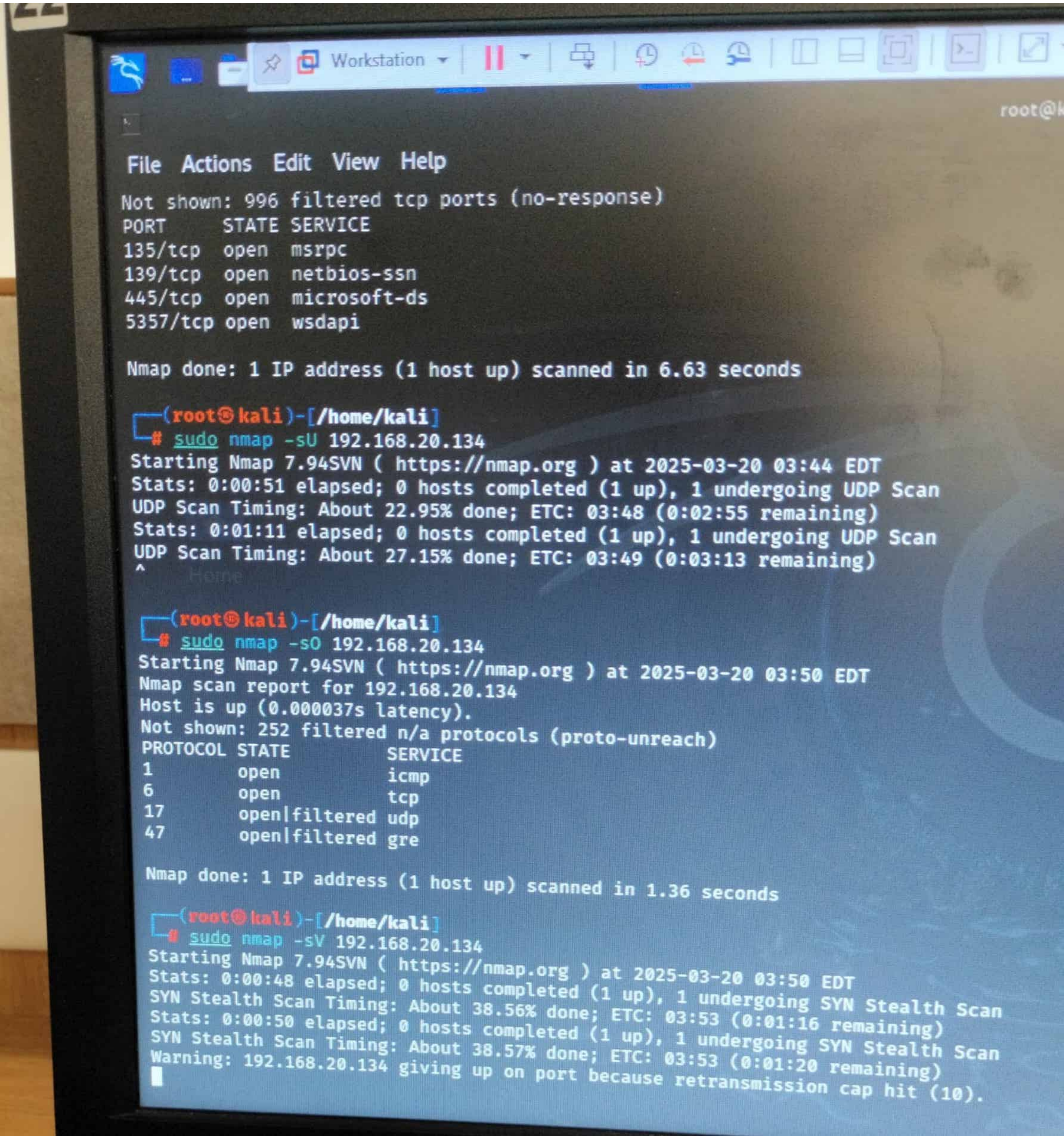
For root user: sudo su

Nmap commands:

1) nmap -sS <your-ip> - for performing stealth scan
2) nmap -sT <your-ip> - scans for tcp protocols
3) init 0 – turns off the entire kali terminal
4) nmap -O <your-ip> - for os detection
5) nmap -sU <your-ip> - scans for udp protocols
6) nmap -sV <your-ip> - for service version detection
7) nmap -sP <your-ip> - for ping scan



```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sT 192.168.20.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-20 03:44 EDT
Nmap scan report for 192.168.20.134
Host is up (0.00094s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 6.63 seconds

┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sU 192.168.20.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-20 03:44 EDT
Stats: 0:00:51 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 22.95% done; ETC: 03:48 (0:02:55 remaining)
Stats: 0:01:11 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 27.15% done; ETC: 03:49 (0:03:13 remaining)
^

┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sO 192.168.20.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-20 03:50 EDT
Nmap scan report for 192.168.20.134
Host is up (0.000037s latency).
Not shown: 252 filtered n/a protocols (proto-unreach)
PROTOCOL STATE         SERVICE
1        open          icmp
6        open          tcp
17       open|filtered udp
47       open|filtered gre

Nmap done: 1 IP address (1 host up) scanned in 1.36 seconds

┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sV 192.168.20.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-20 03:50 EDT
```



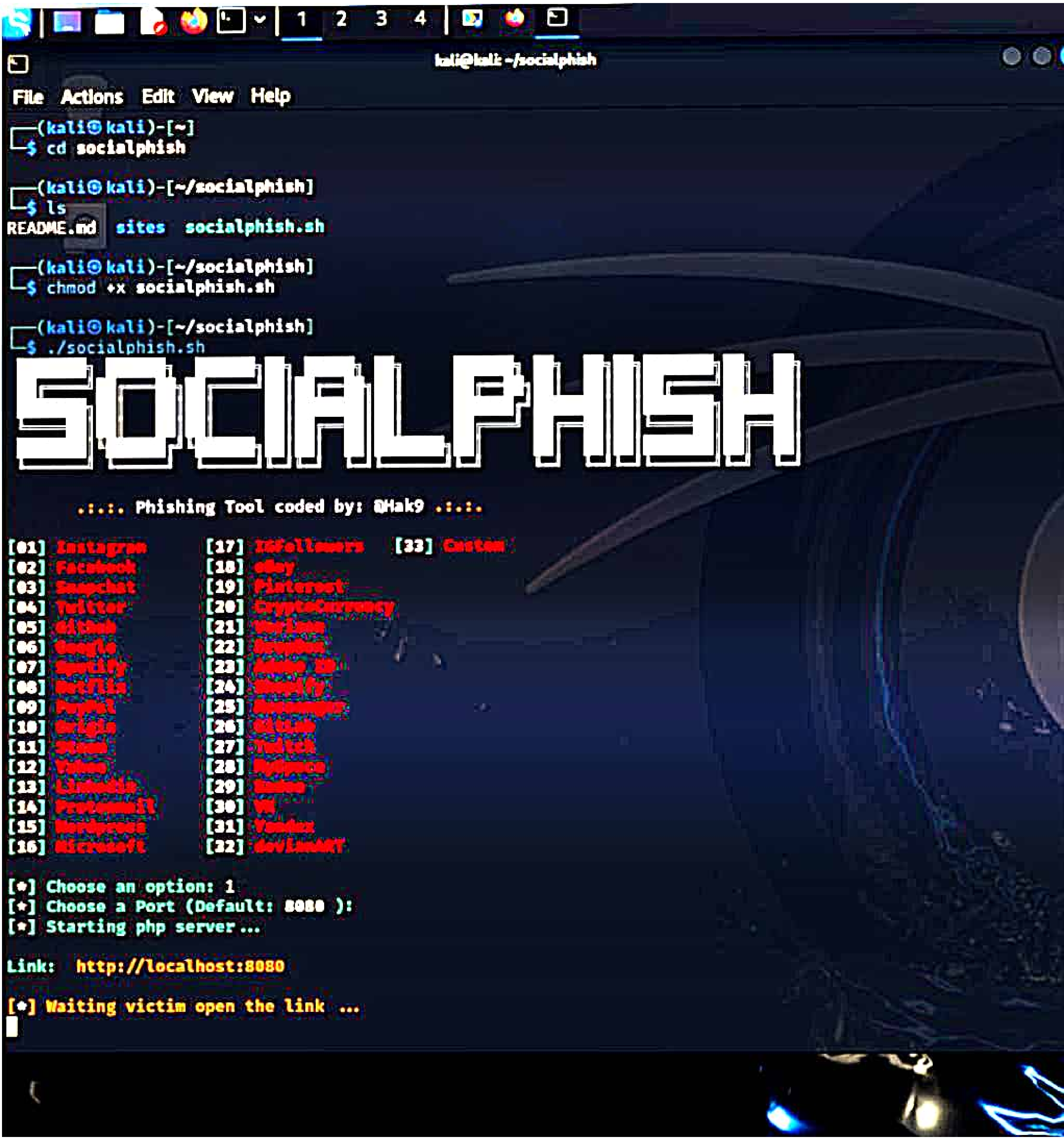
```
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 6.63 seconds

┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sU 192.168.20.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-20 03:44 EDT
Stats: 0:00:51 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 22.95% done; ETC: 03:48 (0:02:55 remaining)
Stats: 0:01:11 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 27.15% done; ETC: 03:49 (0:03:13 remaining)
^

┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sO 192.168.20.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-20 03:50 EDT
Nmap scan report for 192.168.20.134
Host is up (0.000037s latency).
Not shown: 252 filtered n/a protocols (proto-unreach)
PROTOCOL STATE         SERVICE
1        open          icmp
6        open          tcp
17       open|filtered udp
47       open|filtered gre

Nmap done: 1 IP address (1 host up) scanned in 1.36 seconds

┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sV 192.168.20.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-20 03:50 EDT
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 38.56% done; ETC: 03:53 (0:01:16 remaining)
Stats: 0:00:50 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 38.57% done; ETC: 03:53 (0:01:20 remaining)
Warning: 192.168.20.134 giving up on port because retransmission cap hit (10).
█
```

2) phishing → attackers trick ppl into revealing sensitive info like password eg fake email to get password...

- to see installat^{n} of socialphish → refer manual.

- ① VM → kali → firefox/chrome → social phish.github (go on this site) → take url/code → paste it in kali (cmd) →
  - ⓐ cd socialphish
  - ⓑ ./socialphish.sh
  - ⓒ choose option ~~from~~ - Instagram (enter it's code)
  - ⓓ link generate (open link)
  - ⓔ enter fake email/Id . & Pass.

[Psudo su
[pass - kali } helps you to get in root folder. (you can use it after step ⓐ or ⓑ if error occur).



```
┌──(kali㉿kali)-[~]
└─$ cd socialphish

┌──(kali㉿kali)-[~/socialphish]
└─$ ls
README.md  sites  socialphish.sh

┌──(kali㉿kali)-[~/socialphish]
└─$ chmod +x socialphish.sh

┌──(kali㉿kali)-[~/socialphish]
└─$ ./socialphish.sh
SOCIALPHISH

      .:.:. Phishing Tool coded by: @Hak9 .:.:.

[01] Instagram        [17] IGFollowers   [33] Custom
[02] Facebook         [18] eBay
[03] Snapchat         [19] Pinterest
[04] Twitter          [20] CryptoCurrency
[05] Github           [21] Verizon
[06] Google           [22] DropBox
[07] Spotify          [23] Adobe ID
[08] Netflix          [24] Shopify
[09] PayPal           [25] Messenger
[10] Origin           [26] GitLab
[11] Steam            [27] Twitch
[12] Yahoo            [28] MySpace
[13] Linkedin         [29] Badoo
[14] Protonmail       [30] VK
[15] Wordpress        [31] Yandex
[16] Microsoft        [32] devianART

[*] Choose an option: 1
[*] Choose a Port (Default: 8080 ):
[*] Starting php server...

Link:  http://localhost:8080

[*] Waiting victim open the link ...
```

3) DDOS -

① open Metaspoitable — Username & password : msfadmin

② ifconfig – to get ip address (Note it down).

③ outside vmware → chrome → slowloris (github) →
copy the code/url:

④ open kali → cmd → ① git clone <urlcode>
② cd slowloris
② python3 slowloris.py <ip of meta>

⑤ vm → windows / kali → chrome → enter<ip of meta>

you can see → site will not load .

4) keylogger - (see manual for pitures)

① setting → virus & Threat protect^n → Turn of all protect^n.

② browser (outside vm) → spyrix.app → download (free one) {spyrix free logger}
→ go to download →
install (sfk-setup) which we install →

③ more info → run anyway.

④ select language → email → email & pass → next →

⑤ Brower → spyrix.com → my account →
Login with Same email & pass →
Select screenshot tab to see recent screenshots.

Now you will be able to monitor victim's Device.

5) zap -(do from manual)

- instead of juice-shop link u can use "testphp" also.

① open zap → cut comment box → Automated scan → paste url of test php → attack → Alerts (vulnerabilities) → Generate report.

* disable - antivirus / firewall

6) MBSA (from manual)

① disable antivirus / firewall

② open MBSA → scan a computer → computer name (dropdown to automatically get hostname) → start scan → report generated

7) wireshark

① open wireshark →

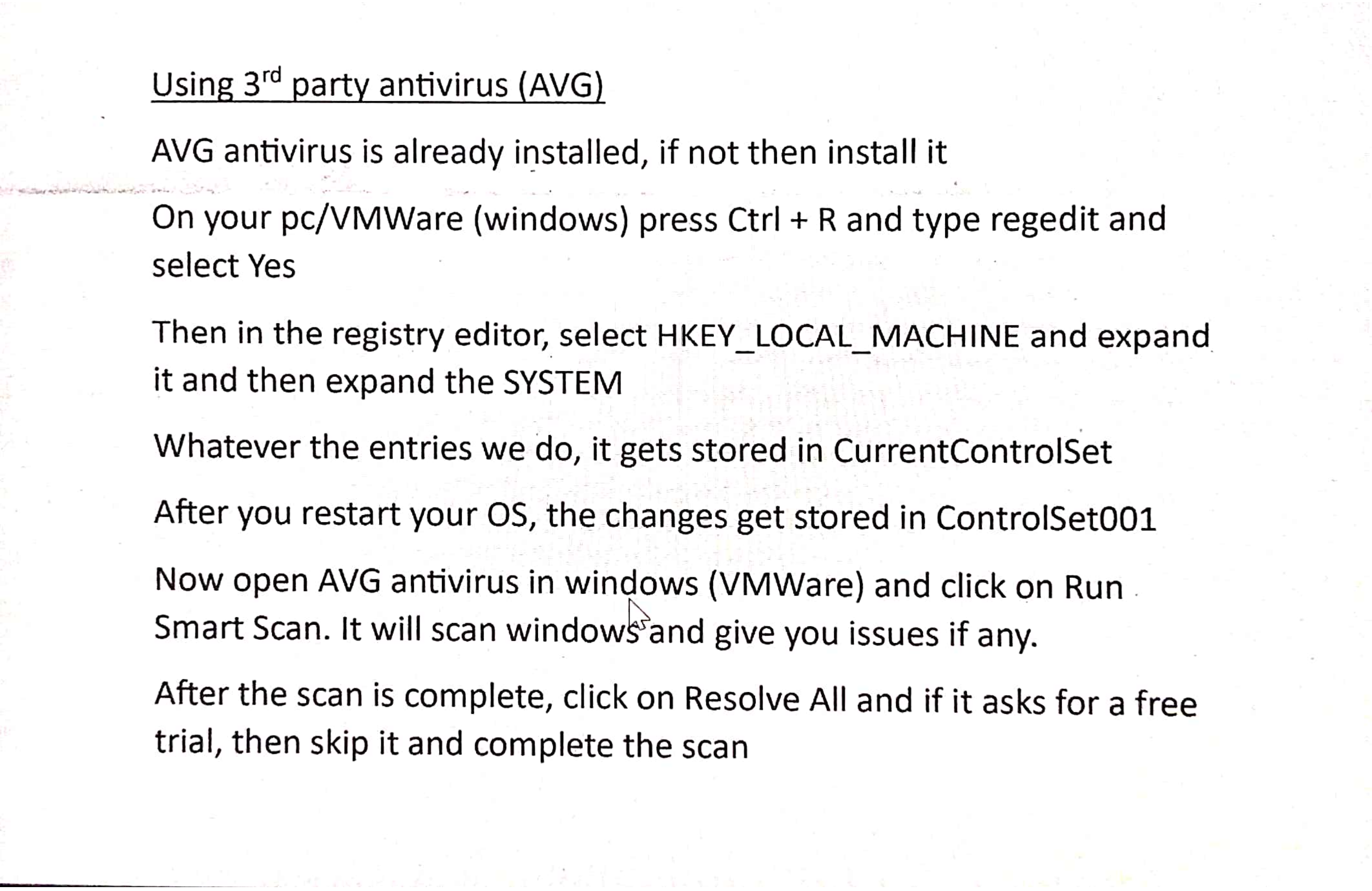
② double click on wifi

③ "testphp site" → username - test → login
pass - test

④ search "http" in filter → in wireshark.

⑤ double click on → userinfo.php.

⑥ search your username + pass i.e. test in it (scroll down)



Using 3rd party antivirus (AVG)

AVG antivirus is already installed, if not then install it

On your pc/VMWare (windows) press Ctrl + R and type regedit and select Yes

Then in the registry editor, select HKEY_LOCAL_MACHINE and expand it and then expand the SYSTEM

Whatever the entries we do, it gets stored in CurrentControlSet

After you restart your OS, the changes get stored in ControlSet001

Now open AVG antivirus in windows (VMWare) and click on Run Smart Scan. It will scan windows and give you issues if any.

After the scan is complete, click on Resolve All and if it asks for a free trial, then skip it and complete the scan

Check if your password is secure or not

1) Go to this site: security.org

Enter any password to see how secure it is

2) Go to this site: nordpass

Enter any password to see how secure it is