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

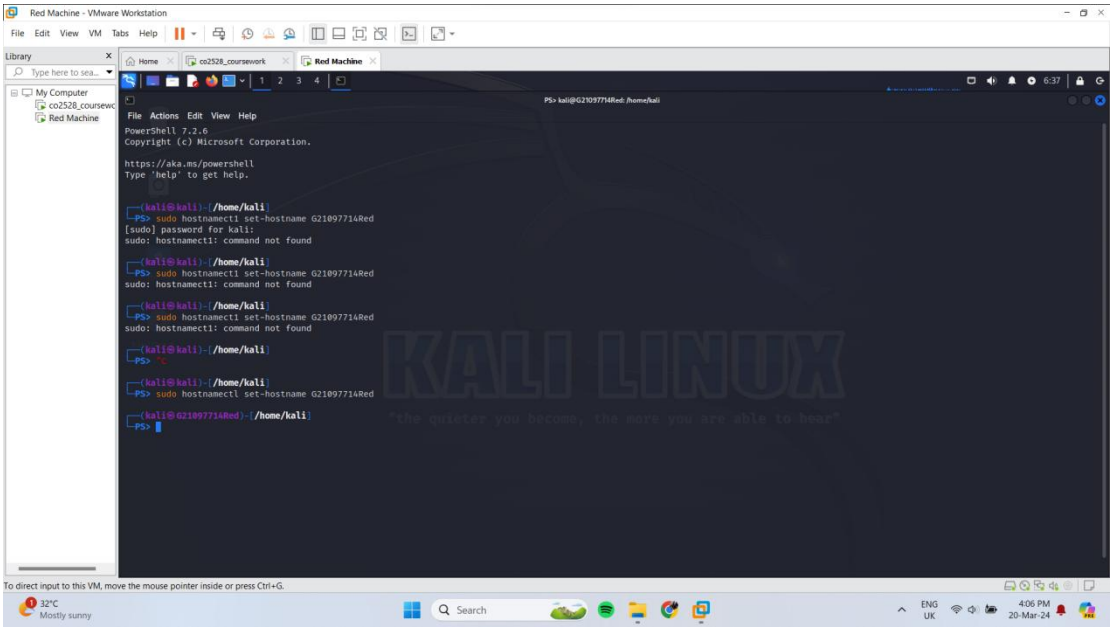
University of Central Lancashire
UCLan

CO2528 - Cyber Security - Capture the Flag

Task 1 – Setting up the 'Blue Computer'…

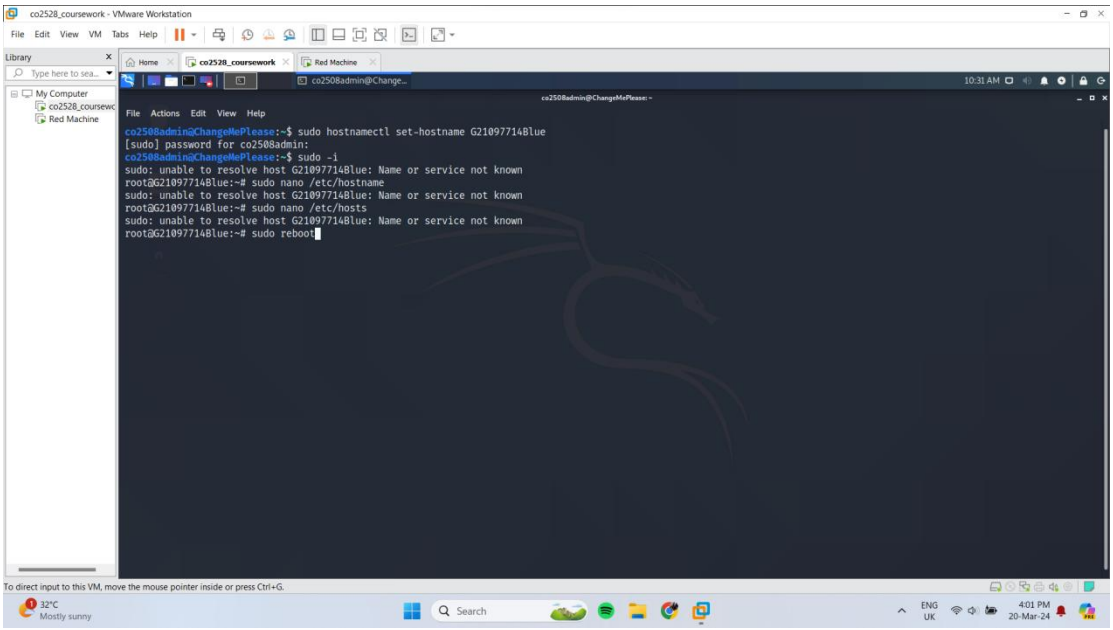
Changing the host name of the red computer.

- $ sudo hostnamectl set-hostname G21097714Red



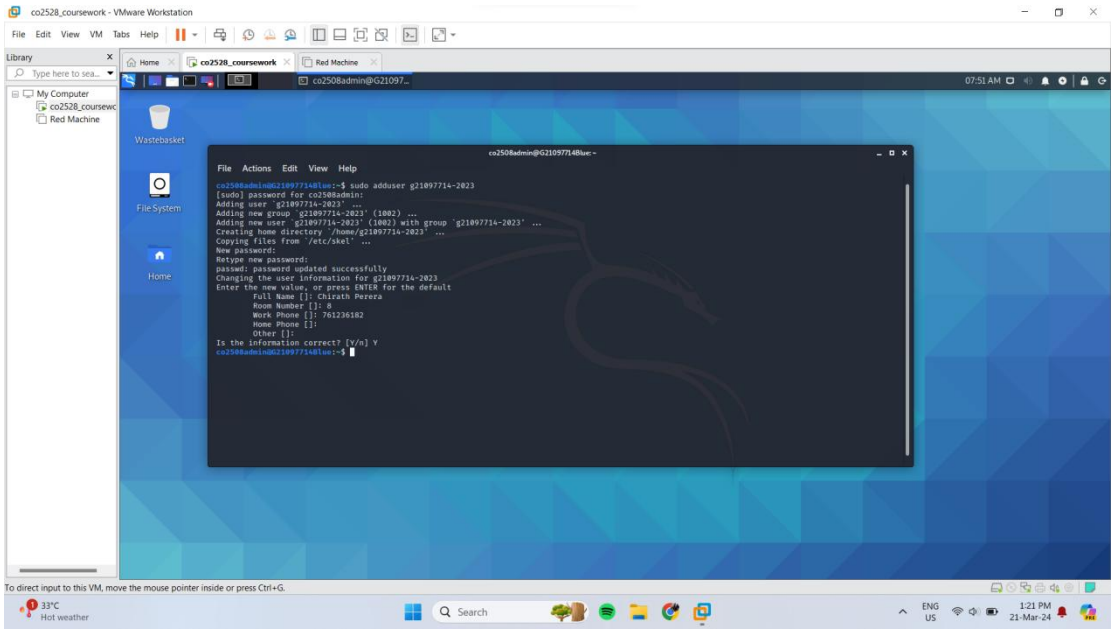
Changing the host name of the blue computer.

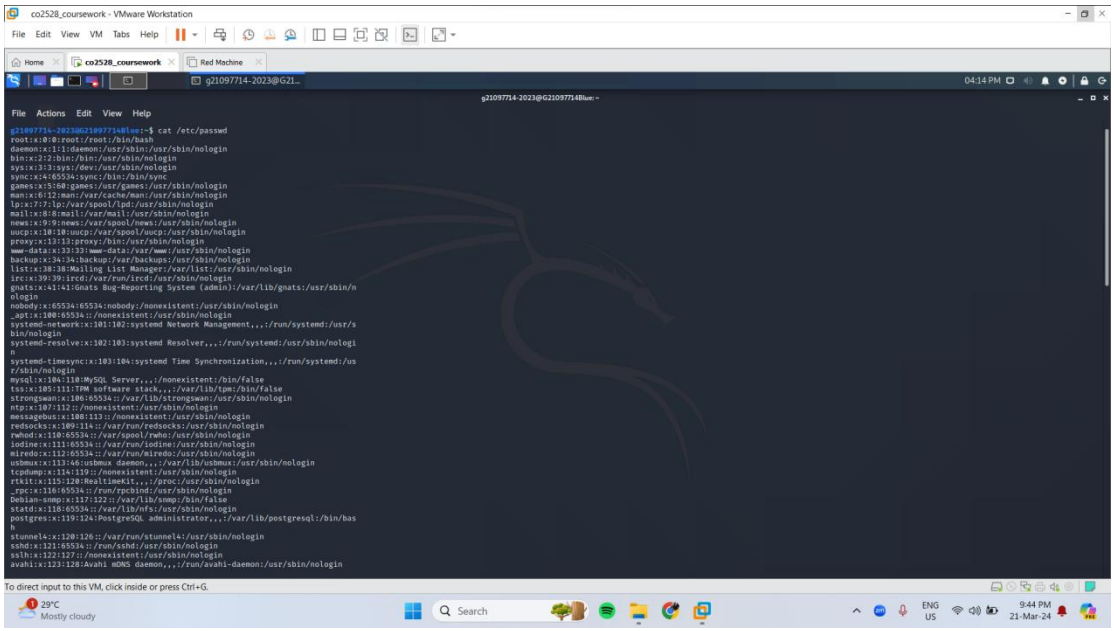
- $ sudo hostnamectl set-hostname G21097714Blue

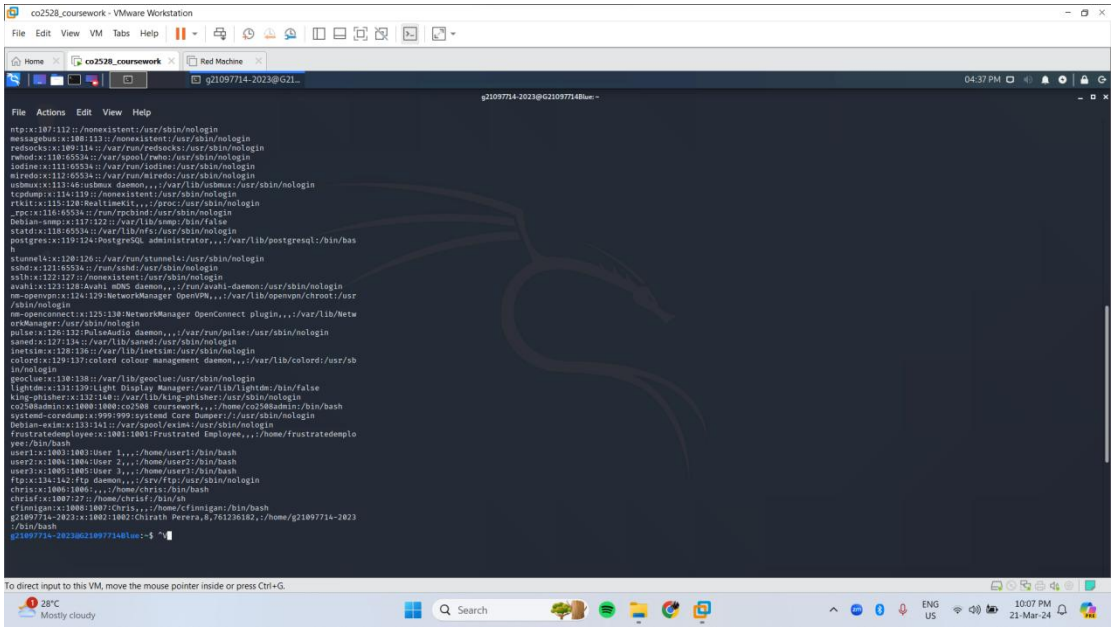


Creating a new user on the blue computer

- $ sudo adduser g21097714-2023

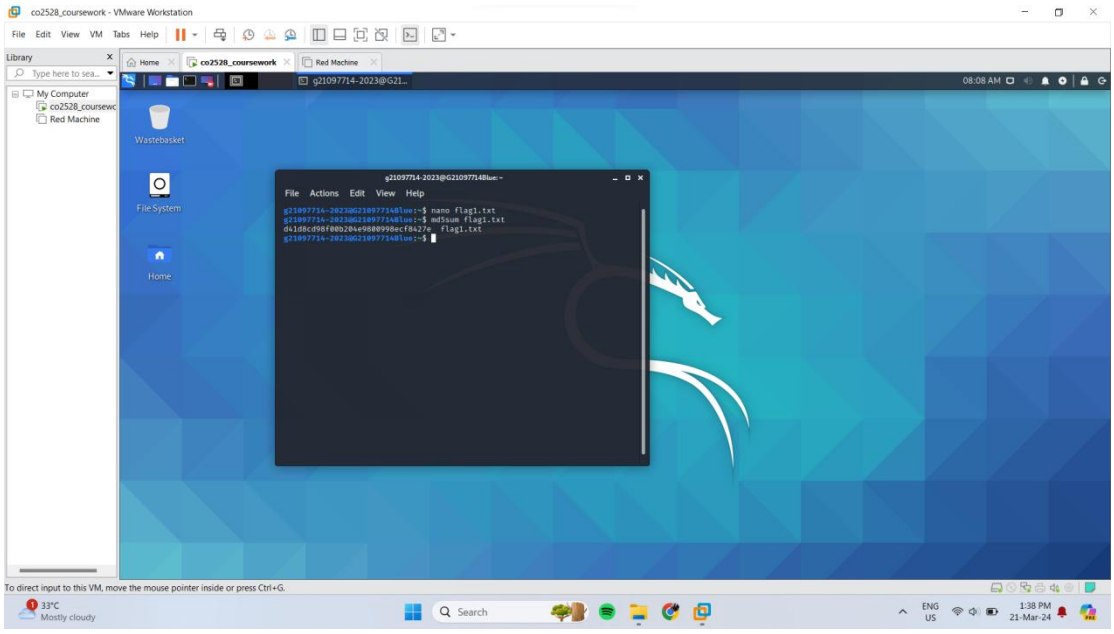






Setting up the blue team “flag”

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



Enable the firewall using the following command

- $ su - co2508admin

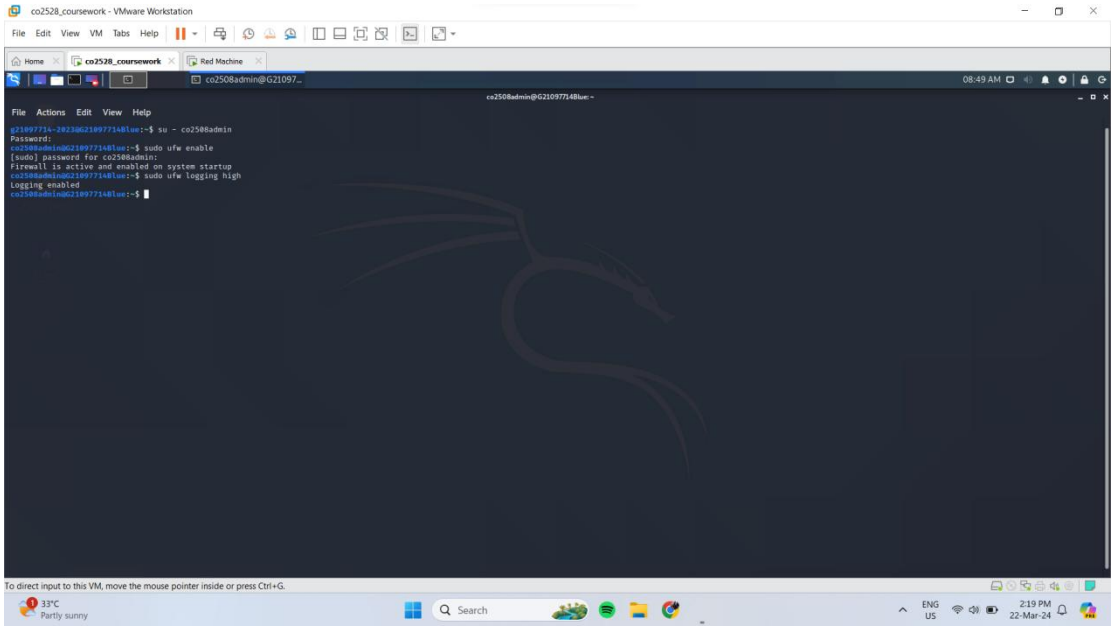
- used this to change the current user from g21097714-2023 to co2508admin

- $ sudo ufw enable

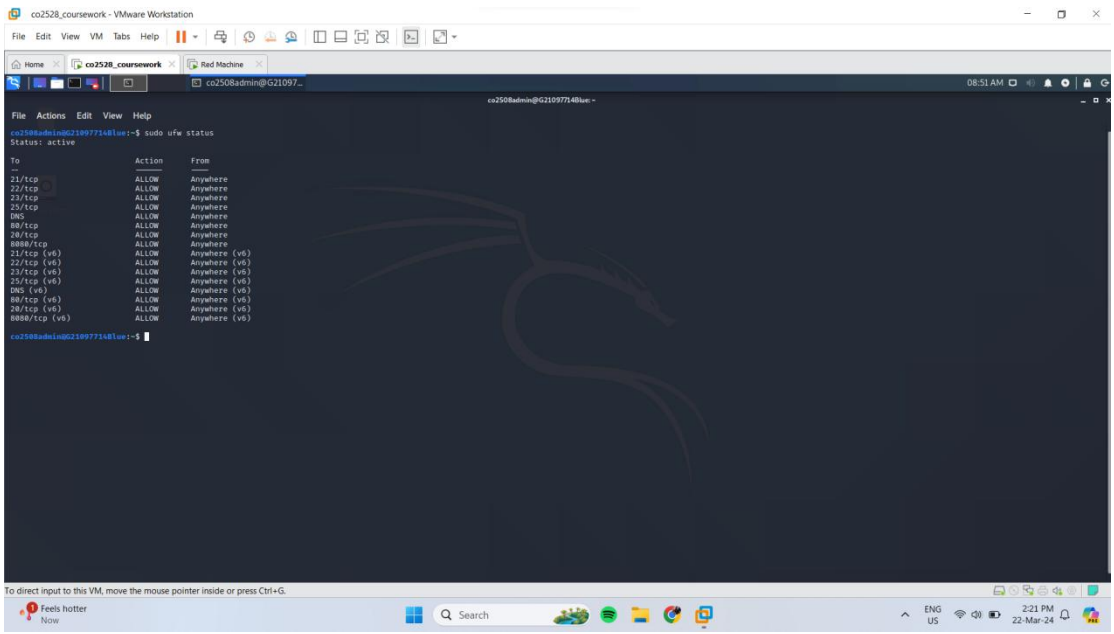
- firewall activated

- $ sudo ufw logging high

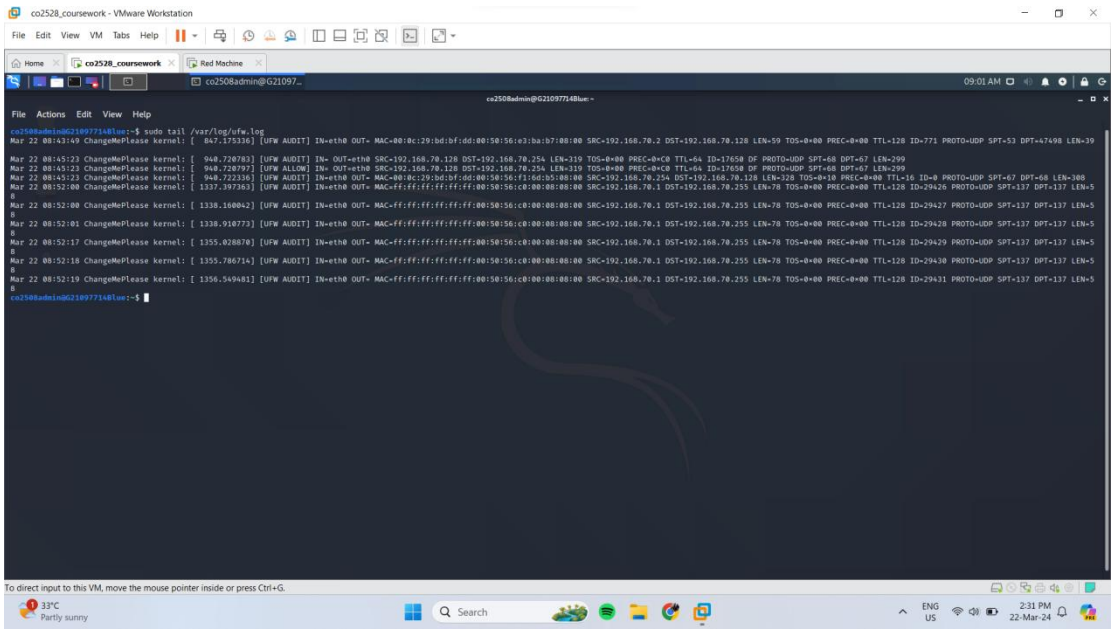
- set the logging to high



- $ sudo ufw status



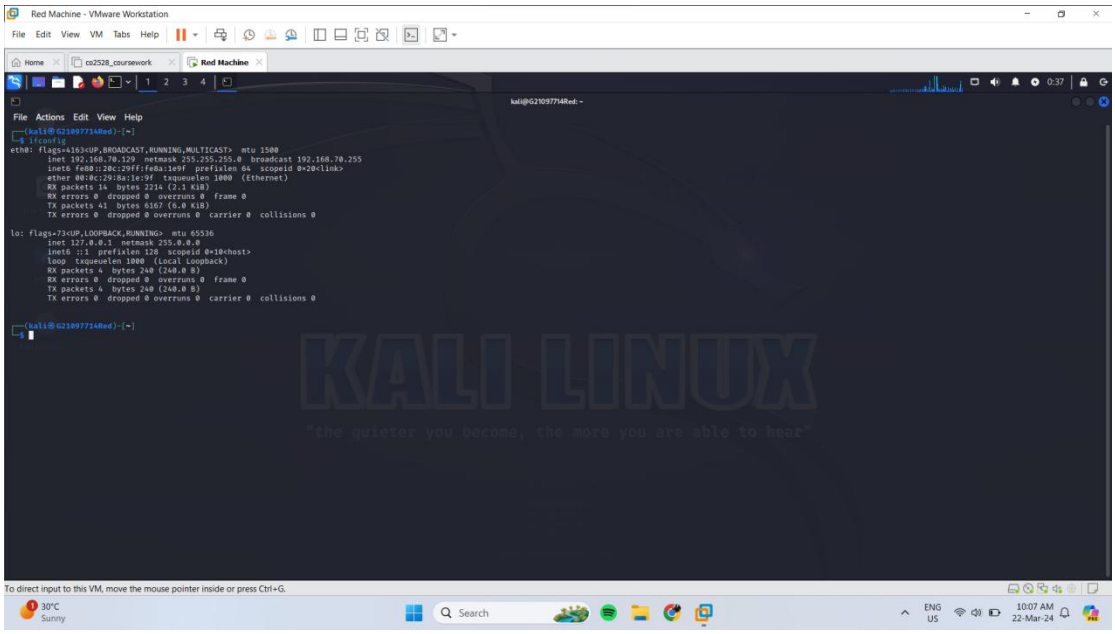
- $ sudo tail /var/log/ufw.log



Task 2 - Performing Initial Reconnaissance

Identifying the IP addresses of both computers

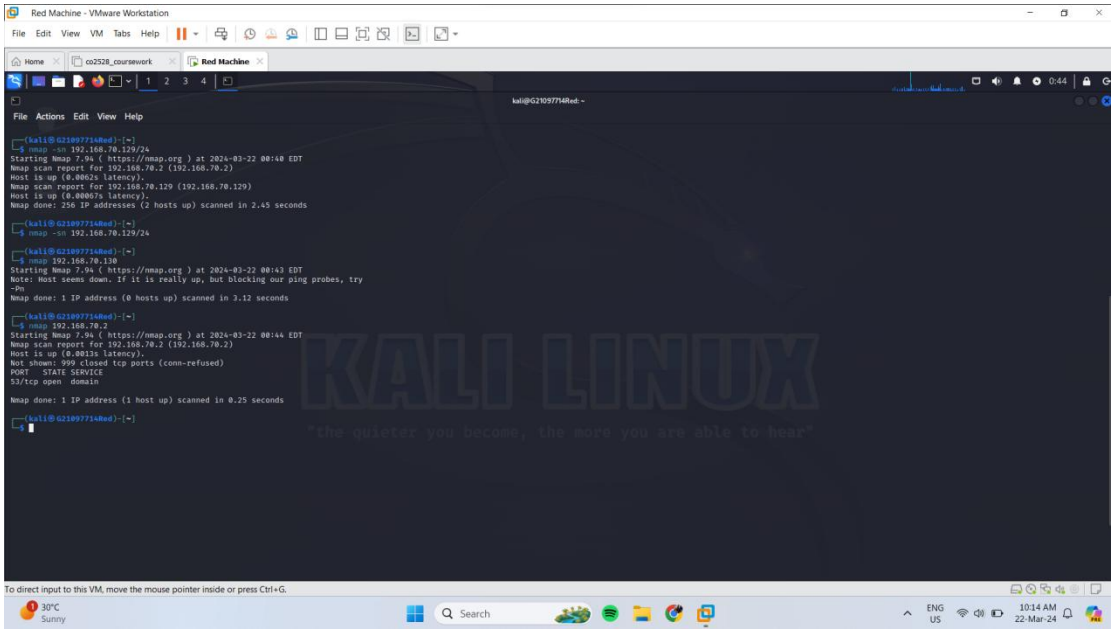
- $ ifconfig



Team Computer	IP Address
Red Team	192.168.70.129
Blue Team	192.168.70.130

Using nmap to find the available IP address

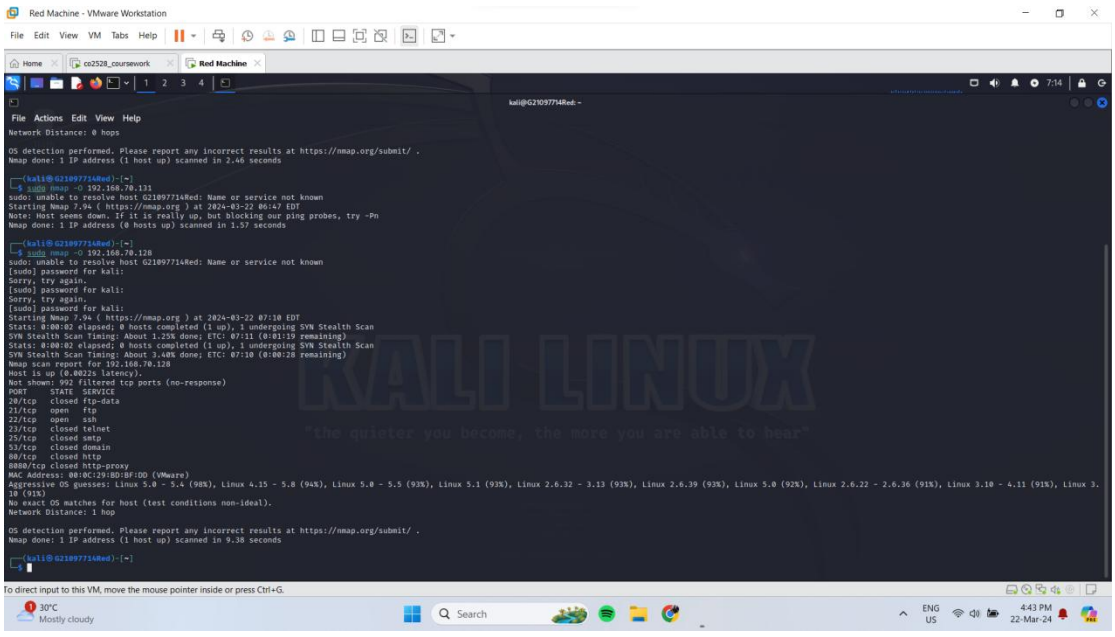
- $ nmap -sn 192.168.70.129/24



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

Operating system fingerprinting

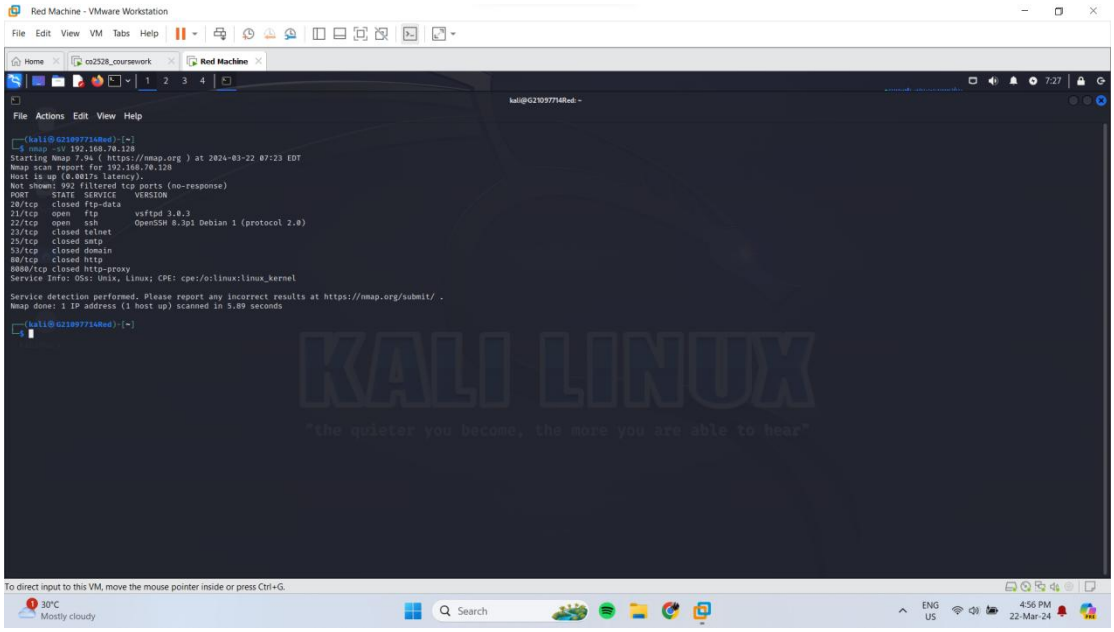
- $ sudo nmap -O 192.168.70.129



Computer	Operating System
Blue Team	Linux 5.0 - 5.4

Identify any daemons/services running

- $ nmap -sV 192.168.70.128

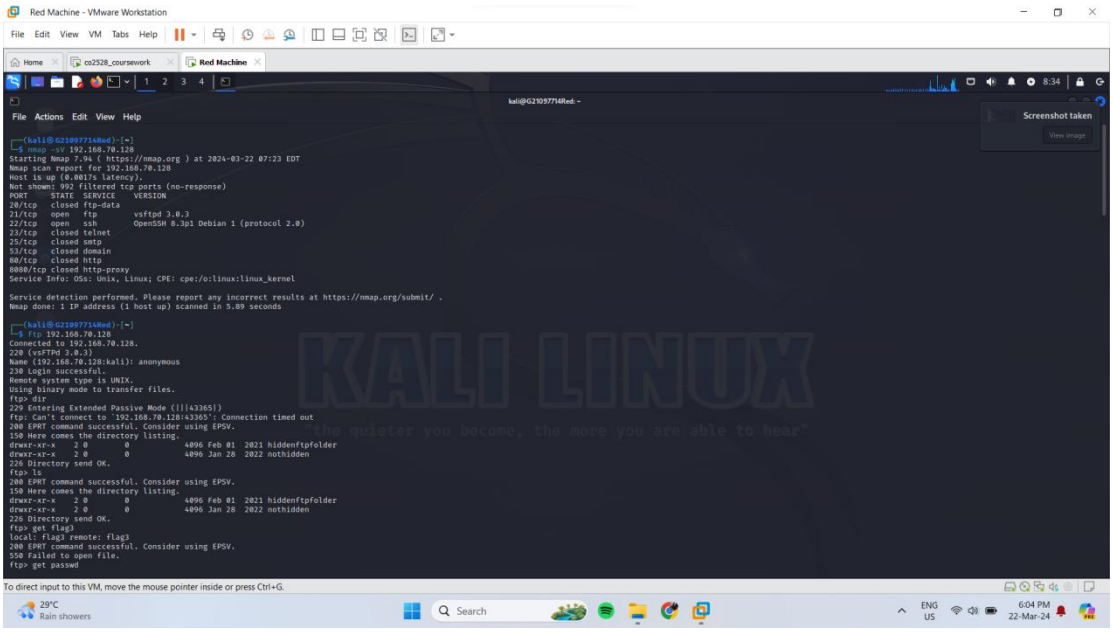


Service	Port Number	Description
ftp-data	20/tcp	Closed port – running closed ftp-data
ftp	21/tcp	Open port – running open ftp
ssh	22/tcp	Open port – running open ssh
telnet	23/tcp	Closed port – running closed telnet
smtp	25/tcp	Closed port – running closed smtp
domain	53/tcp	Closed port – running closed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

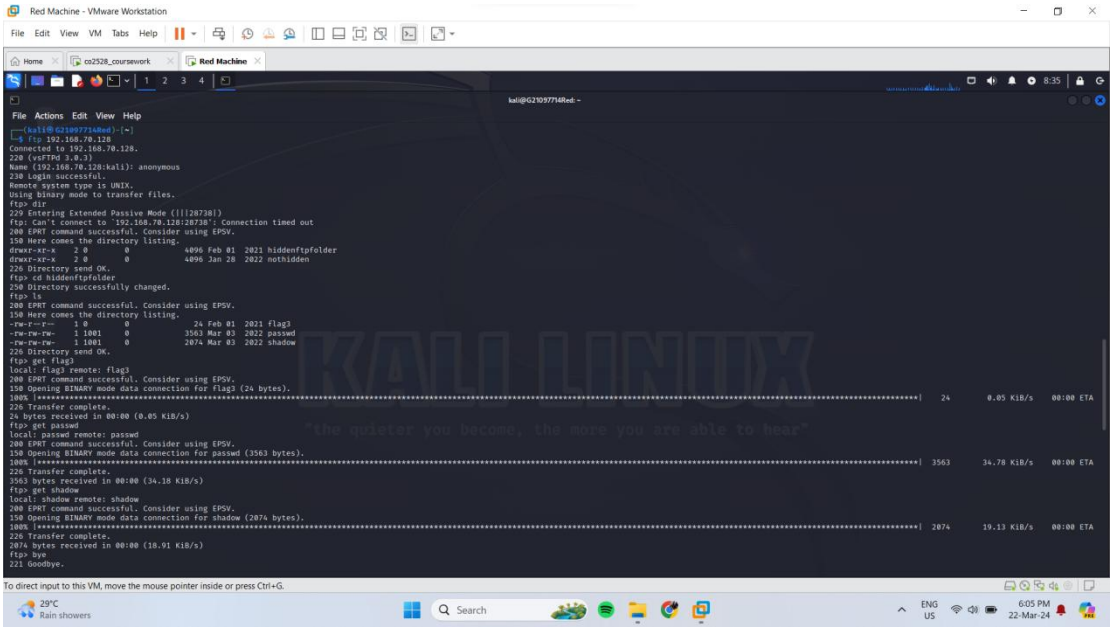
Task 3 - Insider Sabotage

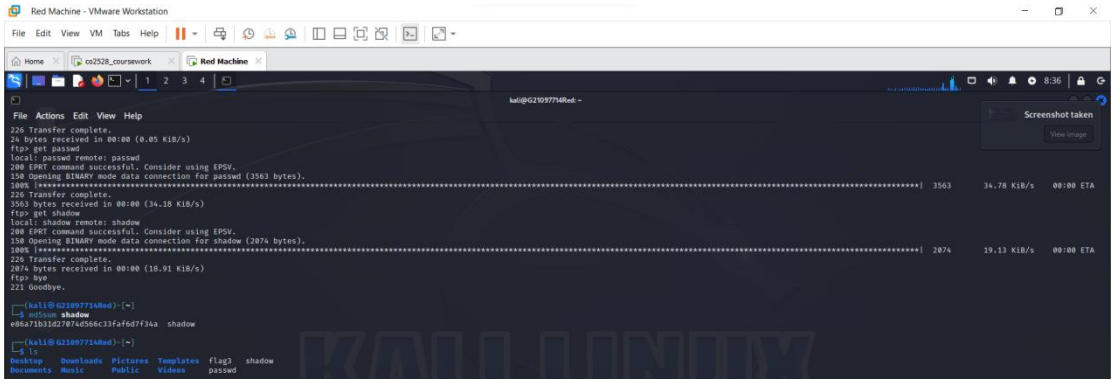
Exploiting the vulnerability and obtaining the files

- $ nmap -sV 192.168.70.128



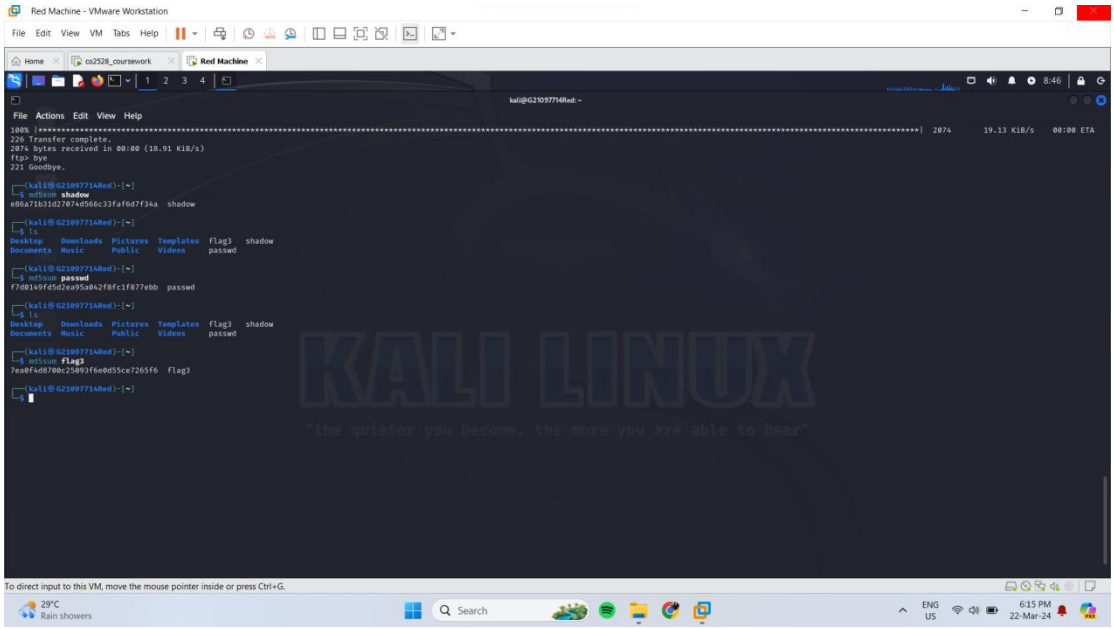
- $ ftp 192.168.70.128

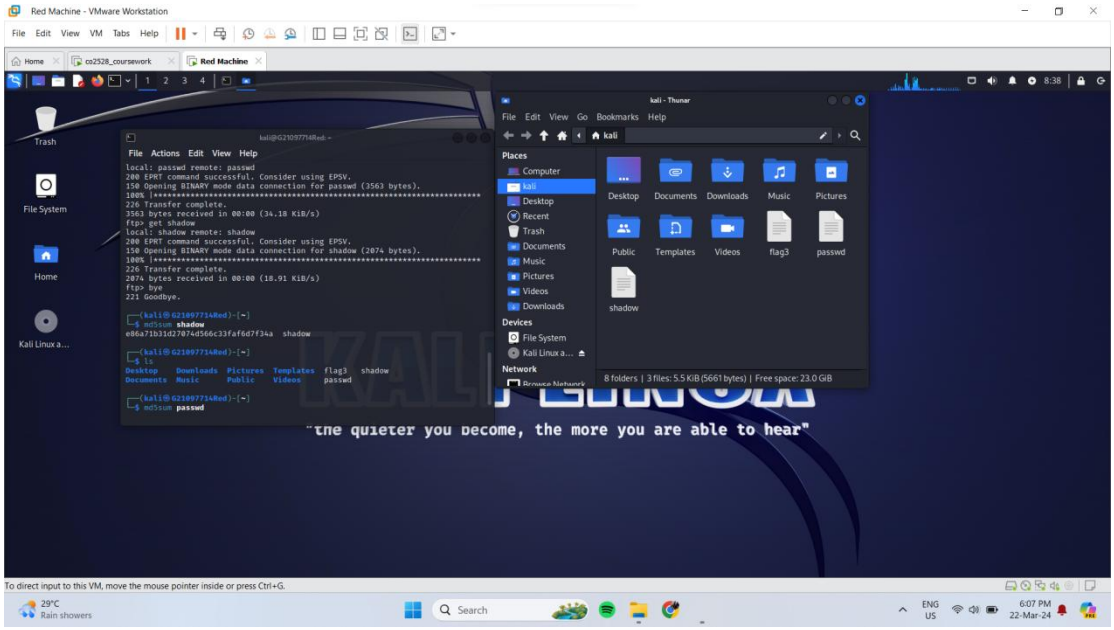




- $ md5sum filename

To get the md5 values for each file

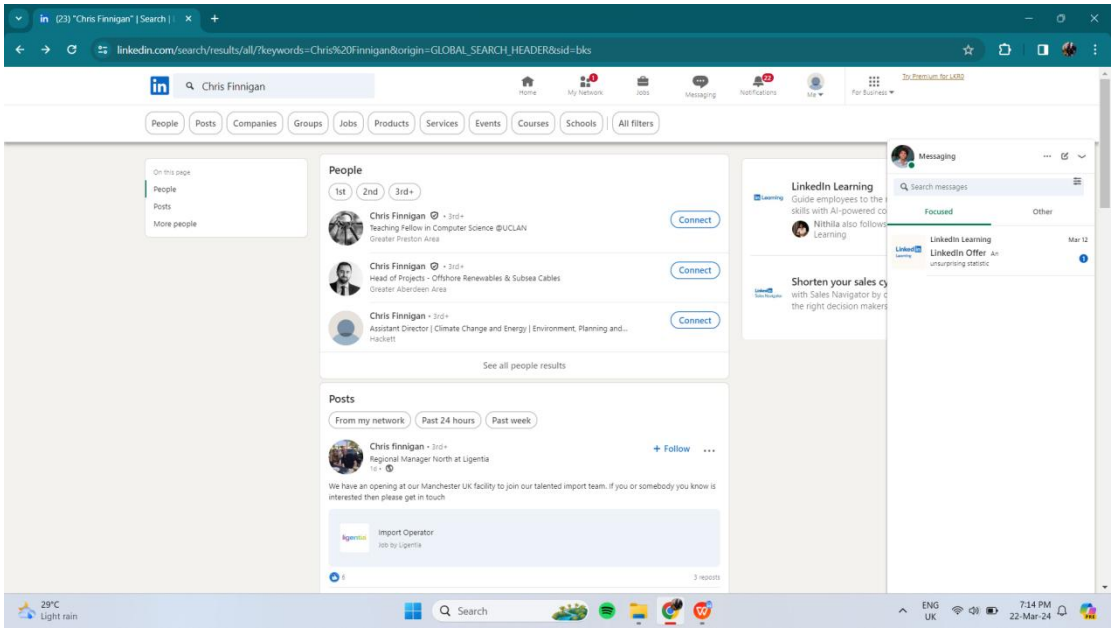


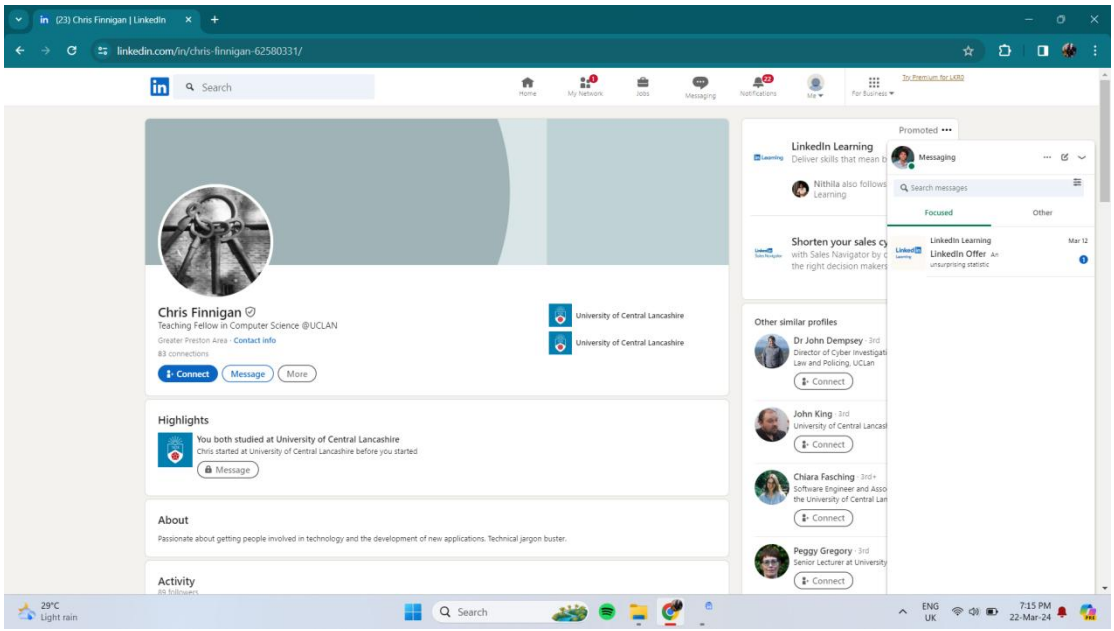


file name	MD5
hiddenftpfolder – flag3	7ea0f4d8700c25093f6e0d55ce7265f6
hiddenftpfolder - passwd	f7d0149fd5d2ea95a042f8fc1f877ebb
hiddenftpfolder - shadow	e86a71b31d27074d566c33faf6d7f34a

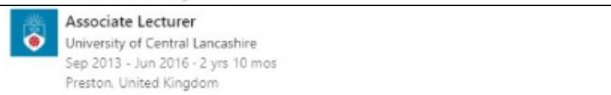
Task 4 – OSINT (Open-Source Intelligence Investigation)

Performing an open-source intelligence investigation on Chris Finnigan.





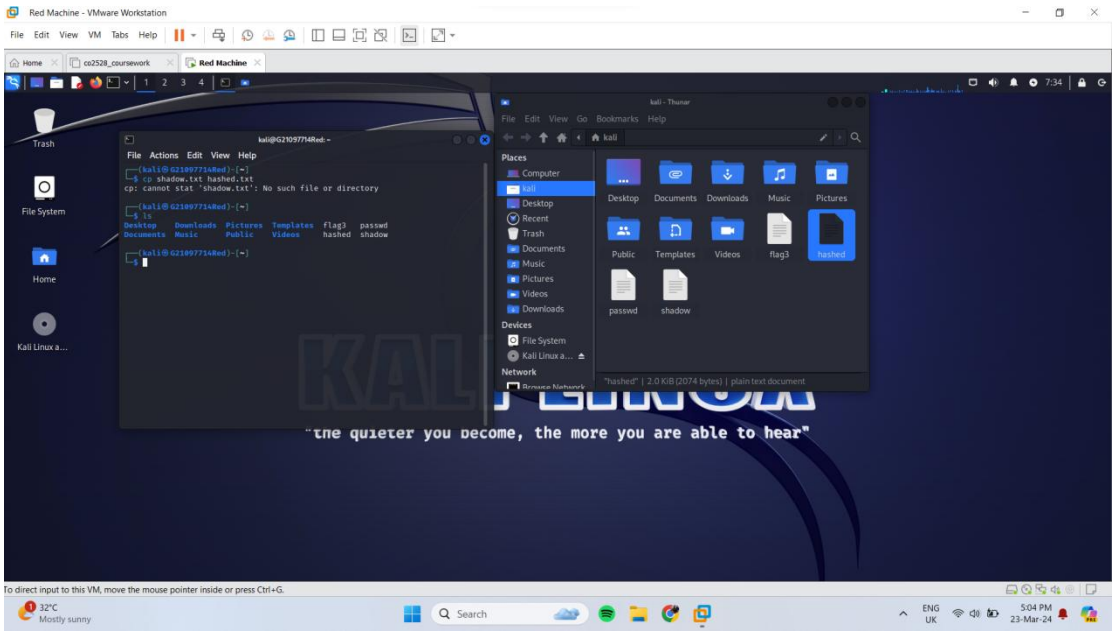
Generate a dictionary to attack the computer.

Pass Phrase	Justification
LisTechnical	
AssociateLecture	
LisTechnicianCoordinator	
AssociateLecturer	
SeniorTechnician	
LecturerUclan	
FellowUclan	
TechnicianUclan	
CoordinatorUclan	
TeachingLancashire	
FellowLancashire	
LecturerLancashire	
TechnicianLancashire	
CoordinatorLancashire	
FellowUniversity	
ChrisFinnigan	
ExperienceExperience	
UniversityCentral	
LancashireTeaching	
FellowAssociate	
LecturerLIS	

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

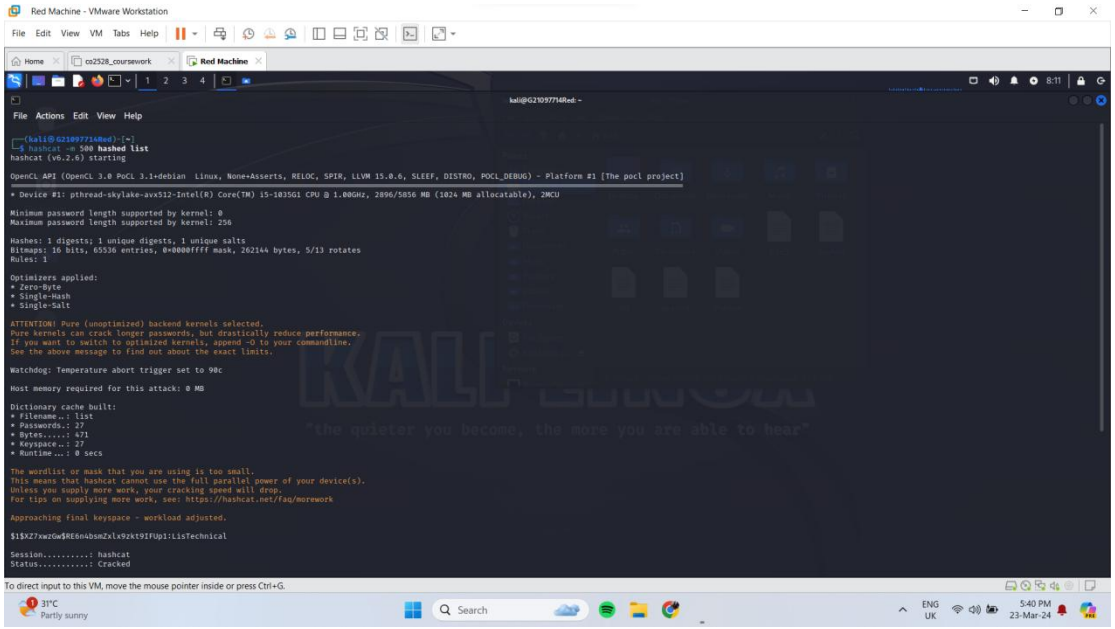
Task 5 – Cracking Passwords

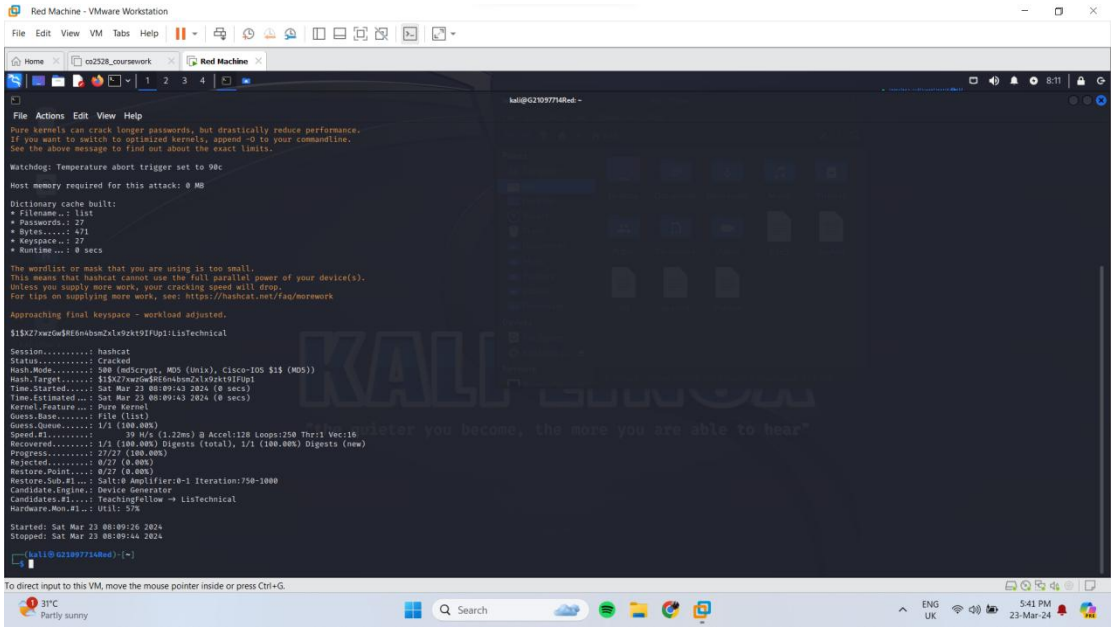
Manually copy pasted from shadow file to hashed file



Performing a dictionary attack

- $ hashcat -m 500 hashed list

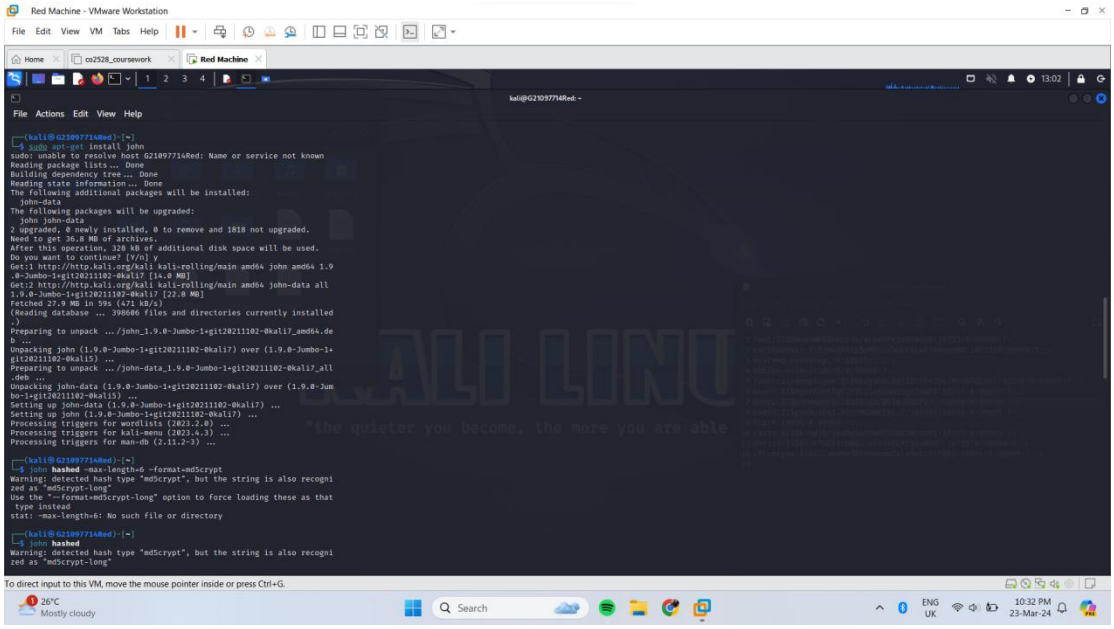




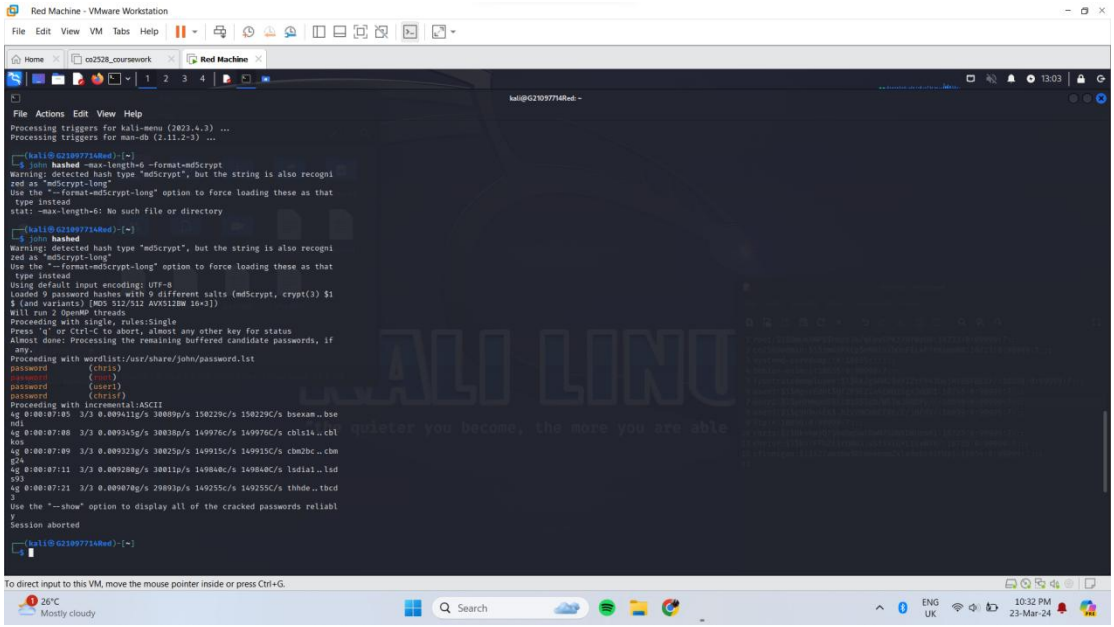
Performing a brute force attack

- $ sudo apt-get install john

To install john the ripper/ upgrade it

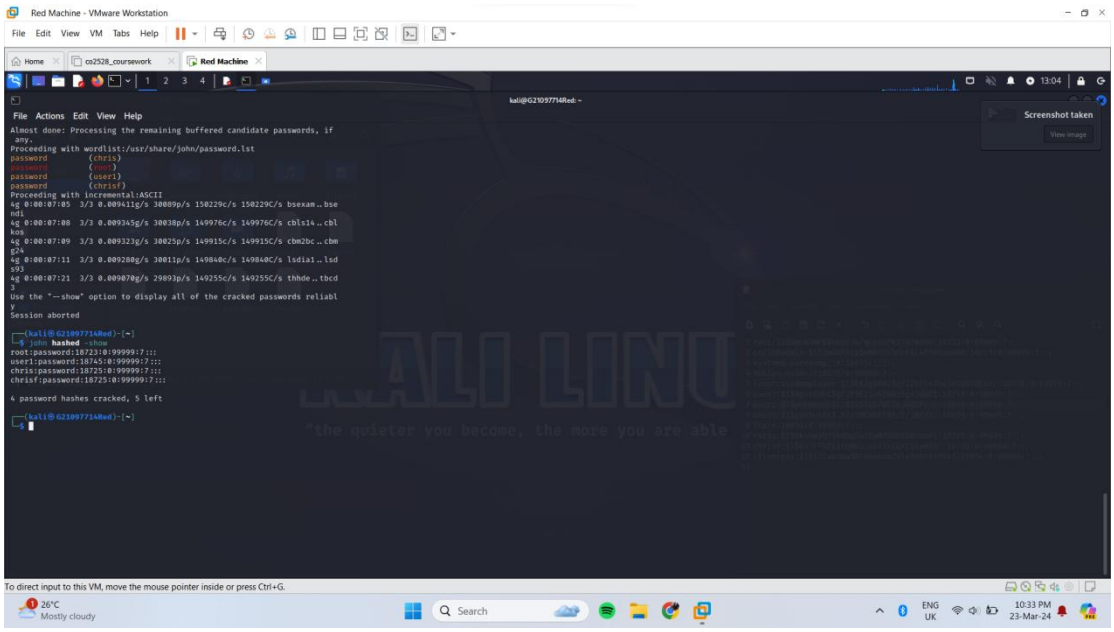


- $ john filename –max-length=6 –format=md5crypt
- $ john filename



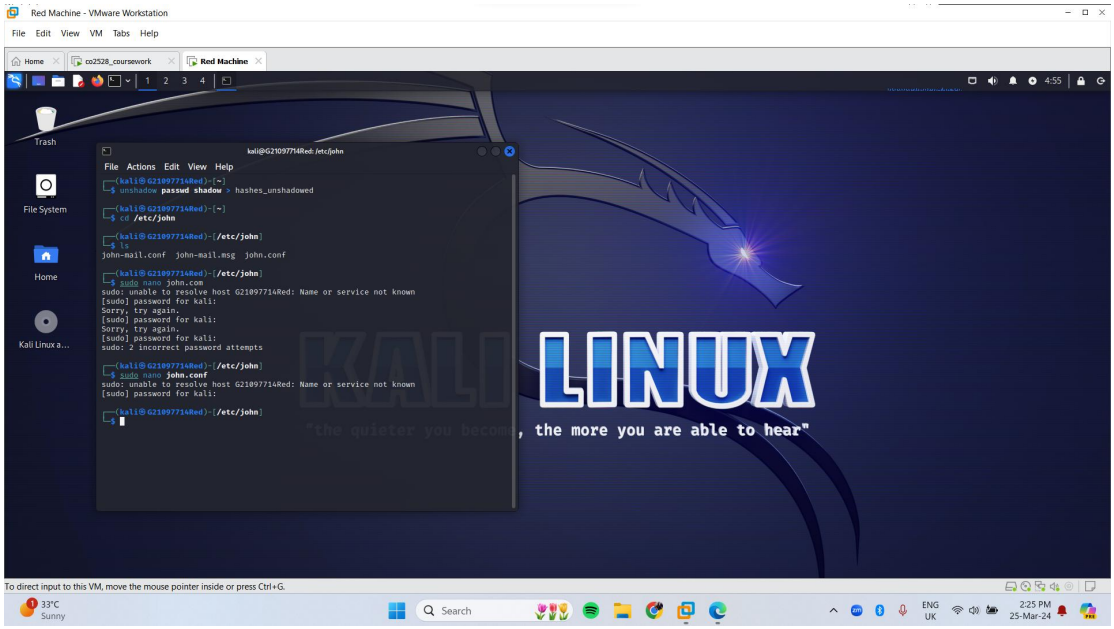
- $ john hashed show

To show the passwords that has been decoded

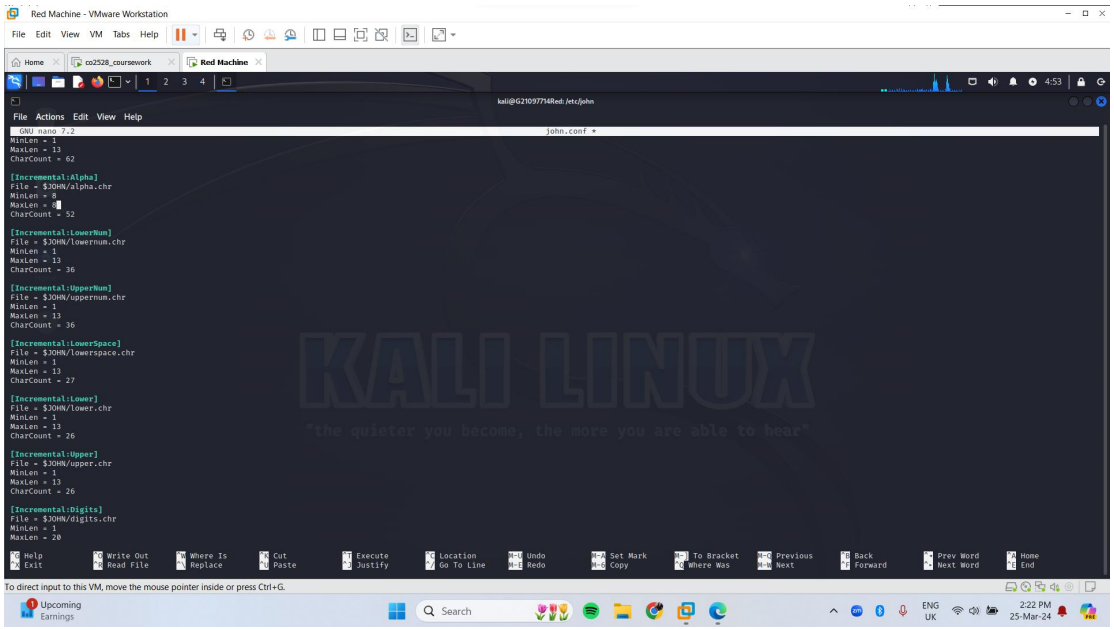


User ID	Password
User1	*password*
chris	*password*
root	*password*
chrisf	*password*

Brute force attack using john the ripper

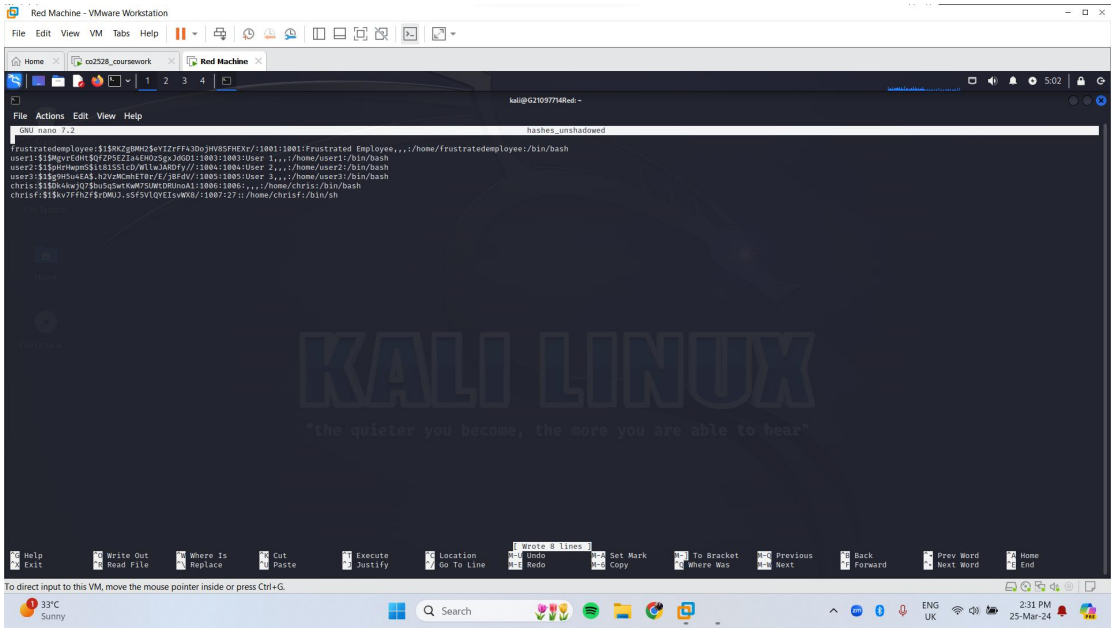


Here I change the value of incremental Alpha - MinLen and MaxLen to 8

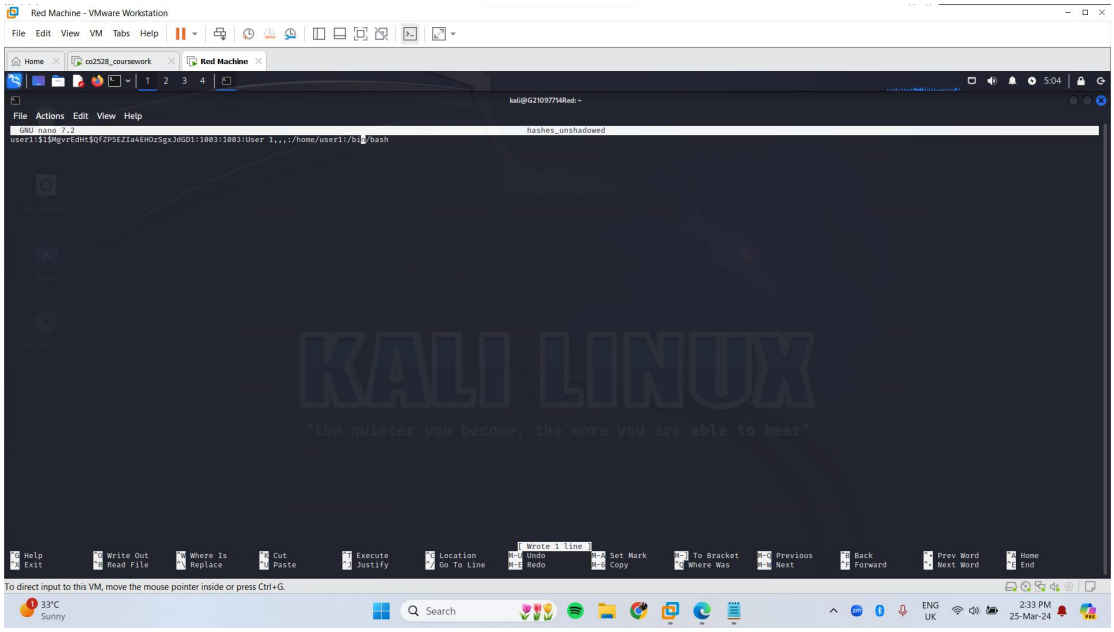


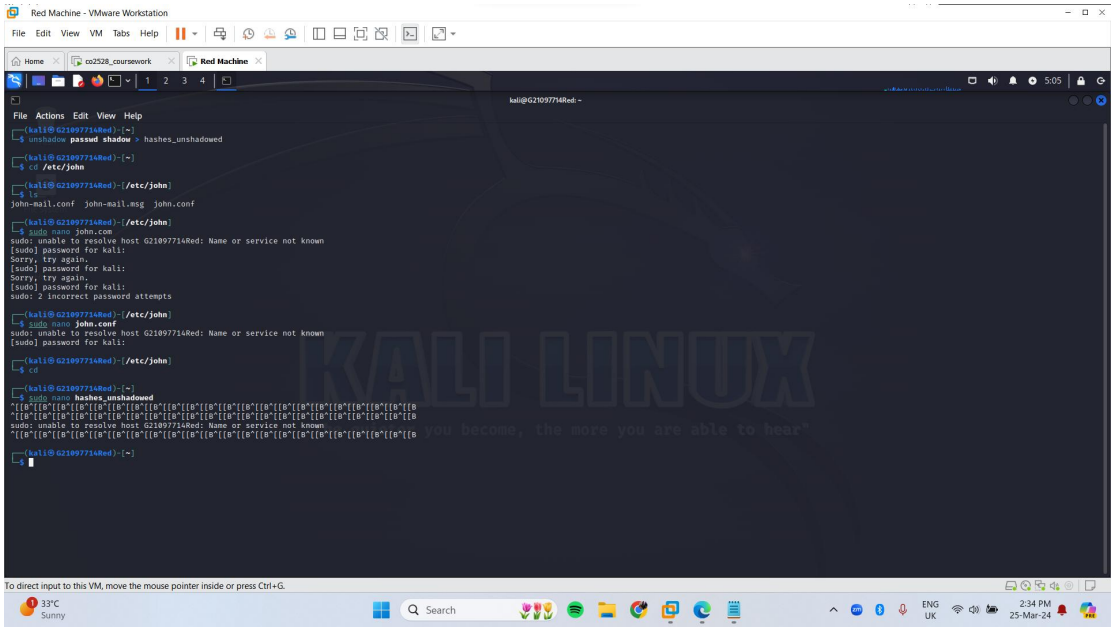
Filtered out the user hashes

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

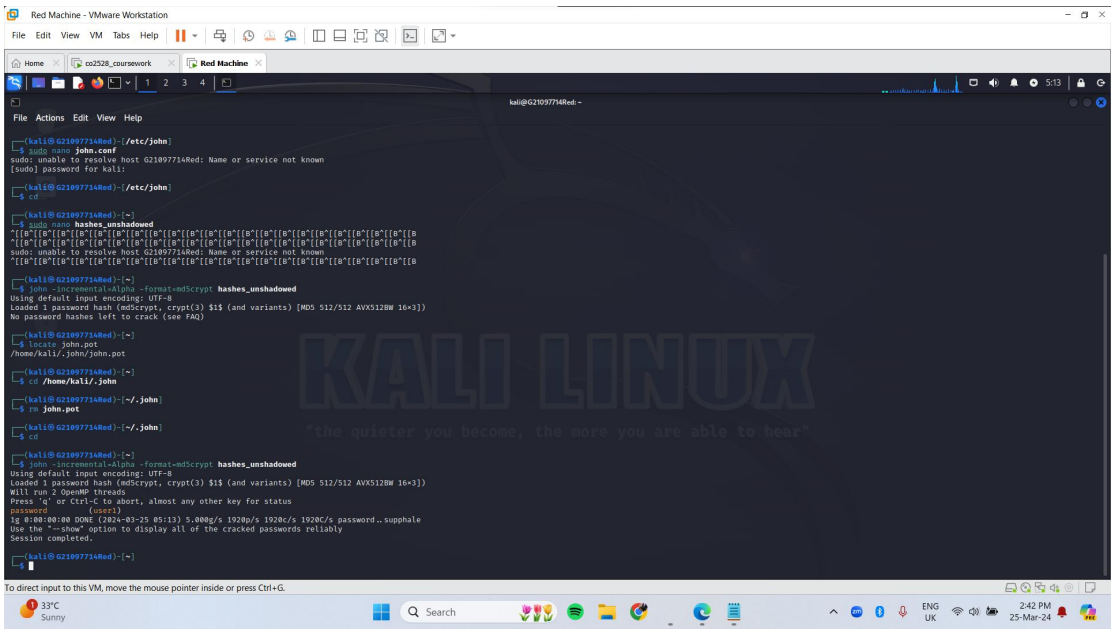


Attacking the weakest passwords first - user1





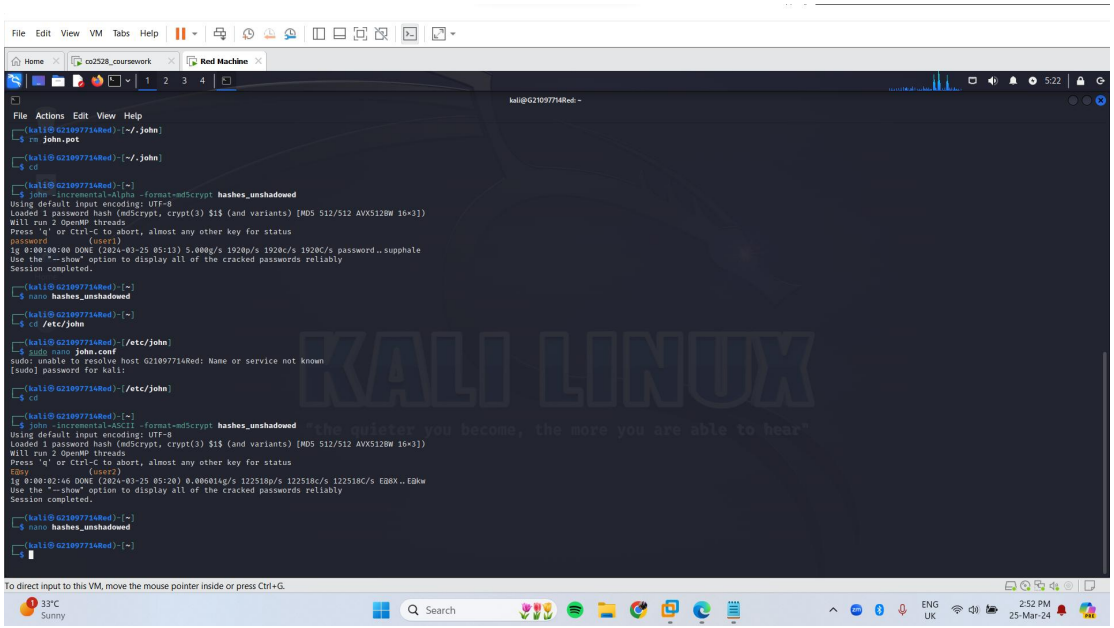
- $ john -incremental=Alpha -format=md5crypt hashes_unshadowed



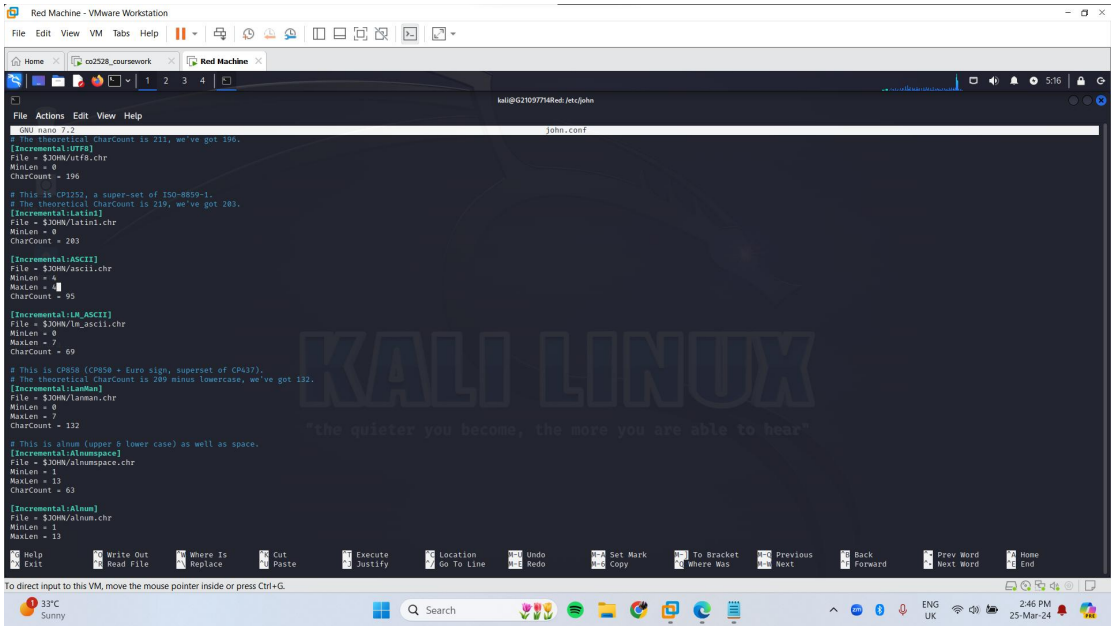
Attack the 2nd weakest passwords

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



Changed Incremental ASCII MinLen & MaxLen to 4



Attack the stronger passwords next

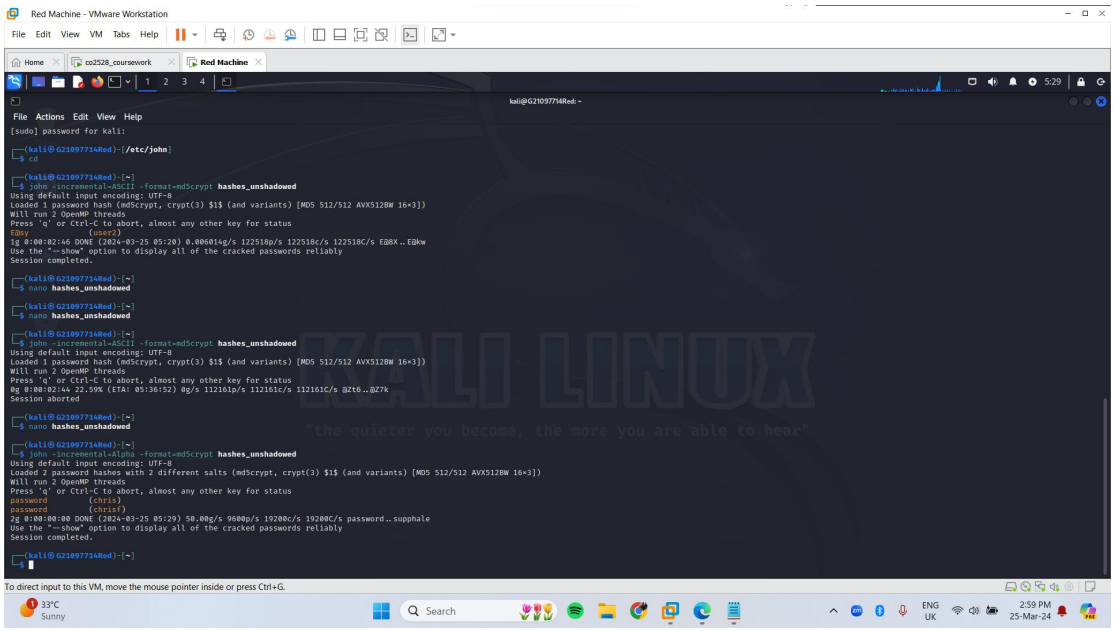
Used the same command for user 3 and fustratedemployee but erased user2 from hashes_unshadowed and pasted both user3 and fustratedemployee

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

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

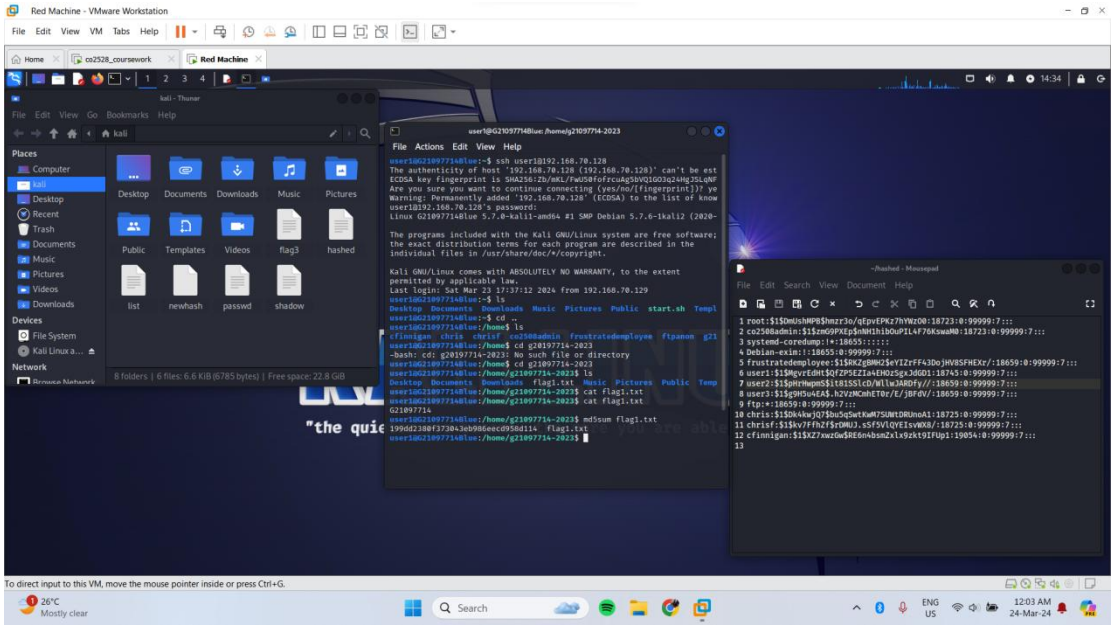
Used the same command for chris and chrisf, erased user3 from hashes_unshadowed and pasted chirs and chrisf both together

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



Task 6 – Capture the Flag

- $ ssh user1@192.168.70.128



- $ ls

To check if flag1.txt can be accessed

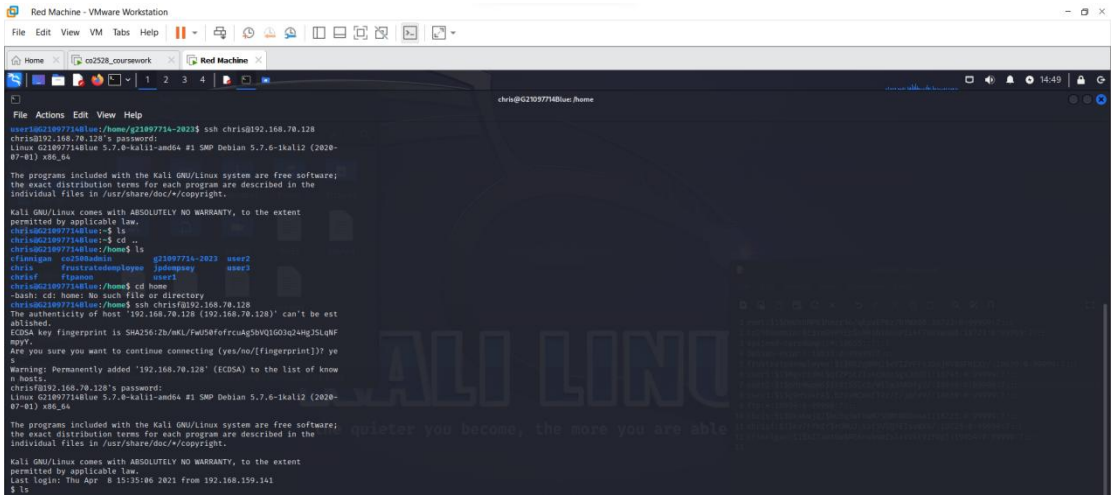
- $ cat flag1.txt
-
- $ md5sum flag1.txt

To get the md5 value for this file

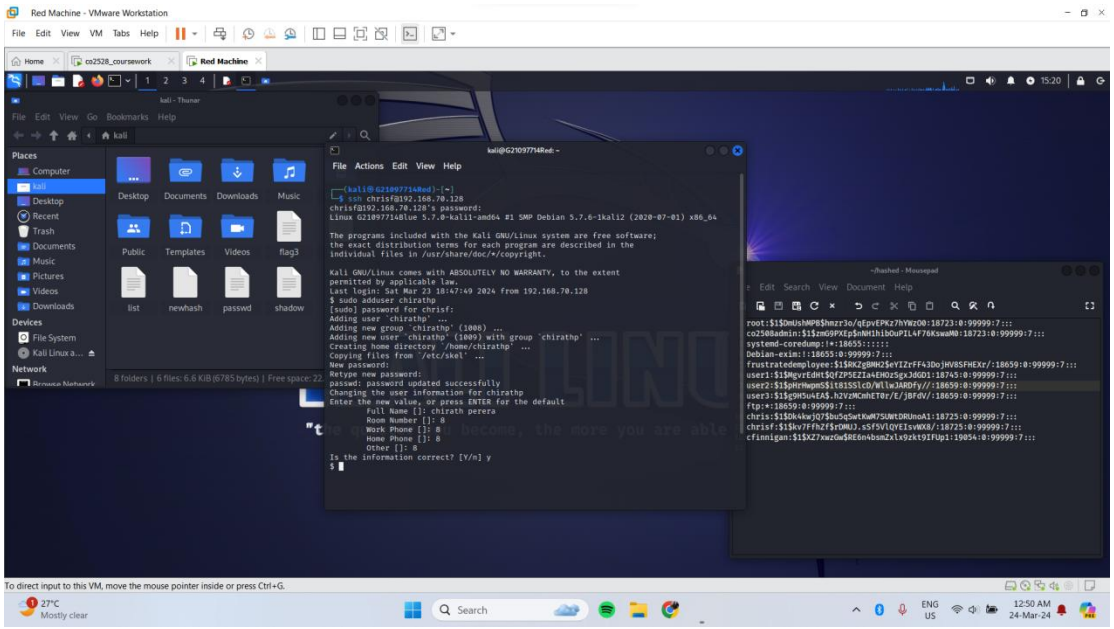
Task 7 - Backdoor Creation

Trying each UserID from task 5, part 2

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



Creating a backdoor

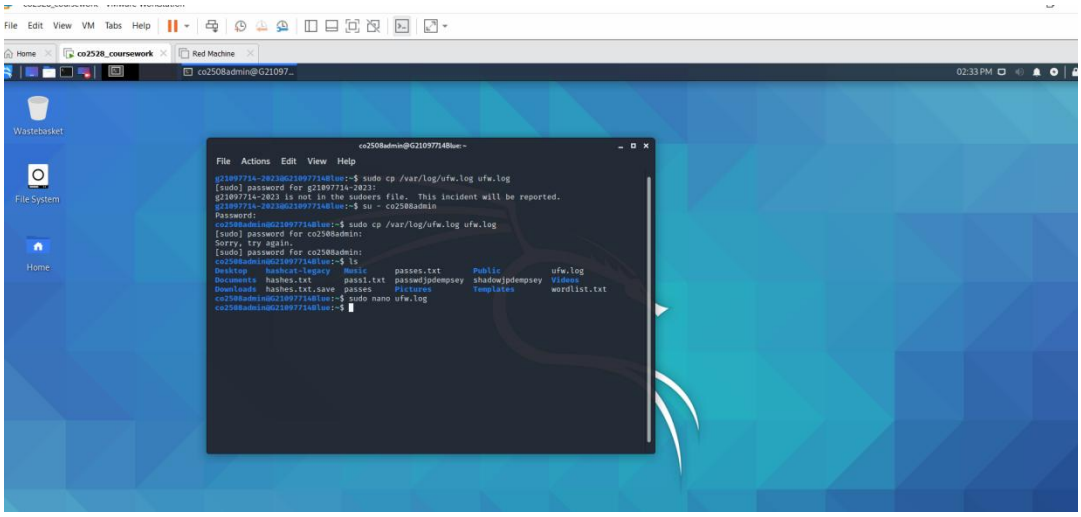


Task 8 – Defending

Analyse the firewall log files

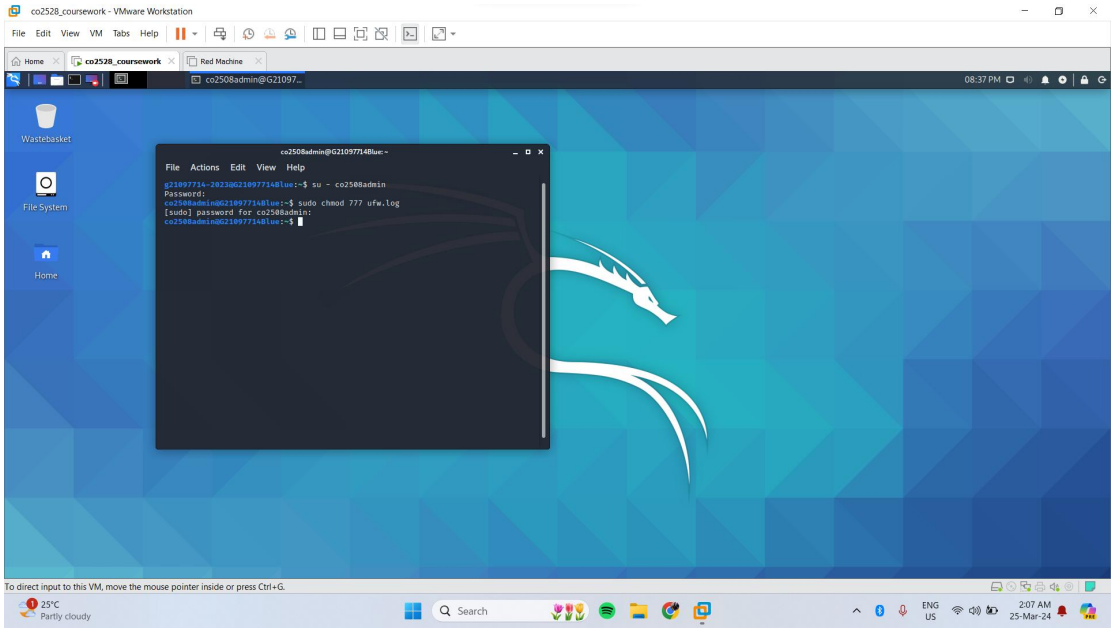
- $ sudo cp /var/log/ufw.log ufw.log

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

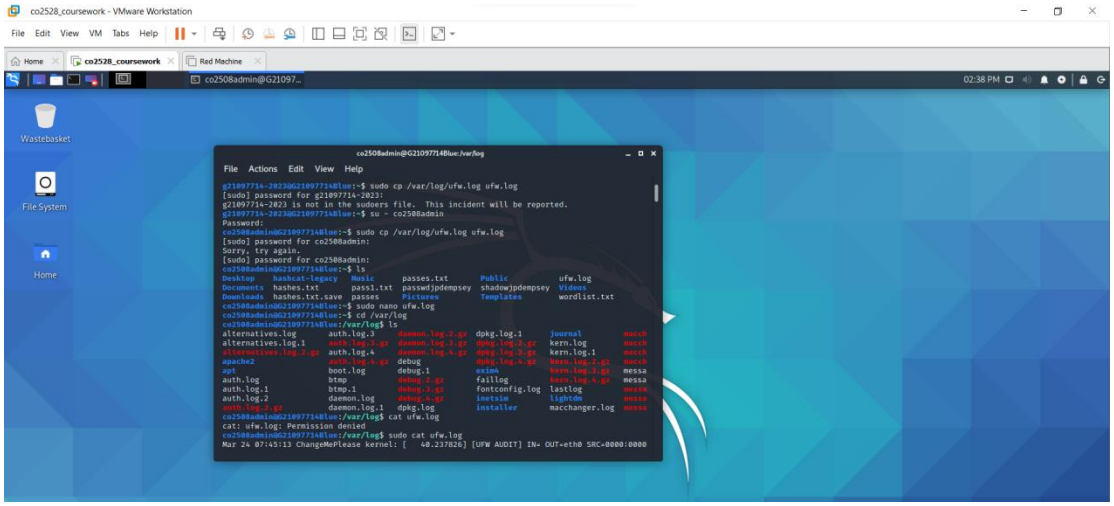
Getting the copy of the log file.

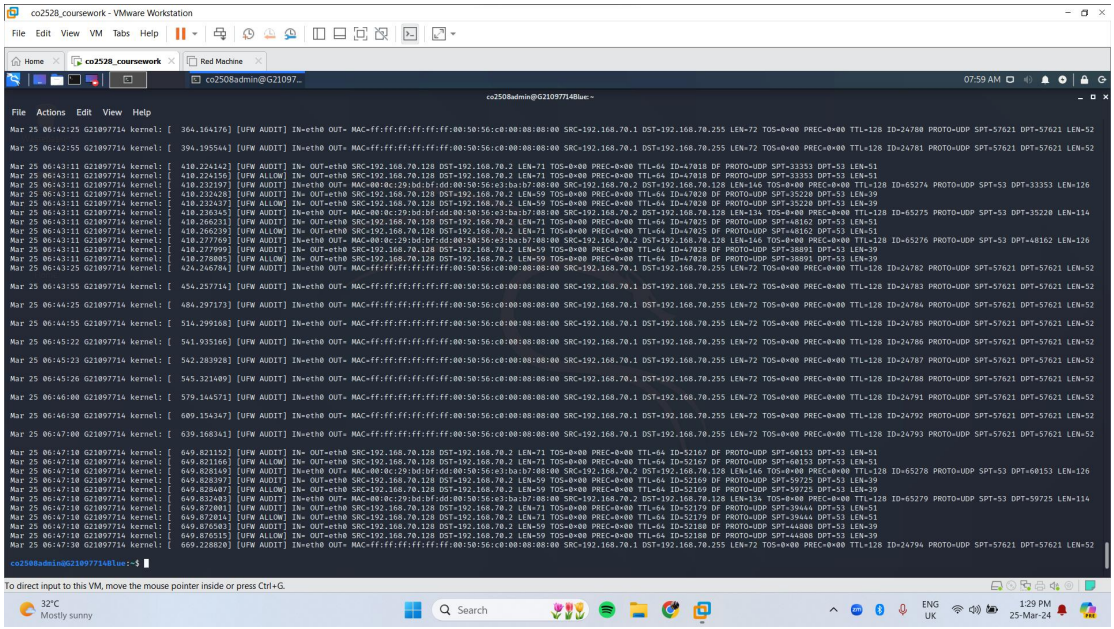
- $ ls
- $ sudo nano ufw.log
- $ cd /var/log

To go inside var log

- $ ls
- $ sudo cat ufw.log

Used to output the contents of the ufw.log


co2528_coursework - VMware Workstation
File Edit View VM Tabs Help
Home
co2528_coursework
Red Machine
co2508admin@G21097...
02:38 PM
Wastebasket
File System
Home
co2508admin@G21097714Blue:/var/log
File Actions Edit View Help
g21097714-2023@G21097714Blue:~$ sudo cp /var/log/ufw.log ufw.log
[sudo] password for g21097714-2023:
g21097714-2023 is not in the sudoers file. This incident will be reported.
g21097714-2023@G21097714Blue:~$ su - co2508admin
Password:
co2508admin@G21097714Blue:~$ sudo cp /var/log/ufw.log ufw.log
[sudo] password for co2508admin:
Sorry, try again.
[sudo] password for co2508admin:
co2508admin@G21097714Blue:~$ ls
Desktop hashcat-legacy Music passes.txt Public ufw.log
Documents hashes.txt pass1.txt passwdjpdempsey shadowjpdempsey Videos
Downloads hashes.txt.save passes Pictures Templates wordlist.txt
co2508admin@G21097714Blue:~$ sudo nano ufw.log
co2508admin@G21097714Blue:~$ cd /var/log
co2508admin@G21097714Blue:/var/log$ ls
alternatives.log auth.log.3 daemon.log.2.gz dpkg.log.1 journal macch
alternatives.log.1 auth.log.3.gz daemon.log.3.gz dpkg.log.2.gz kern.log macch
alternatives.log.2.gz auth.log.4 daemon.log.4.gz dpkg.log.3.gz kern.log.1 macch
apache2 auth.log.4.gz debug dpkg.log.4.gz kern.log.2.gz macch
apt boot.log debug.1 exim4 kern.log.3.gz messa
auth.log btmp debug.2.gz faillog kern.log.4.gz messa
auth.log.1 btmp.1 debug.3.gz fontconfig.log lastlog messa
auth.log.2 daemon.log debug.4.gz inetsim lightdm messa
auth.log.3.gz daemon.log.1 dpkg.log installer macchanger.log messa
co2508admin@G21097714Blue:/var/log$ cat ufw.log
cat: ufw.log: Permission denied
co2508admin@G21097714Blue:/var/log$ sudo cat ufw.log
Mar 24 07:45:13 ChangeMePlease kernel: [40.237826] [UFW AUDIT] IN= OUT=eth0 SRC=0000:0000


co2528_coursework - VMware Workstation
File Edit View VM Tabs Help
Home
co2528_coursework
Red Machine
co2508admin@G21097...
07:59 AM
co2508admin@G21097714Blue: ~
File Actions Edit View Help
Mar 25 06:42:25 G21097714 kernel: [364.164176] [UFW AUDIT] IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:50:56:c0:00:08:08:00 SRC=192.168.70.1 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=24780 PROTO=UDP SPT=57621 DPT=57621 LEN=52
Mar 25 06:42:55 G21097714 kernel: [394.195544] [UFW AUDIT] IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:50:56:c0:00:08:08:00 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 06:43:11 G21097714 kernel: [410.224142] [UFW AUDIT] IN= OUT=eth0 SRC=192.168.70.128 DST=192.168.70.2 LEN=71 TOS=0x00 PREC=0x00 TTL=64 ID=47018 DF PROTO=UDP SPT=33353 DPT=53 LEN=51
Mar 25 06:43:11 G21097714 kernel: [410.224156] [UFW ALLOW] IN= OUT=eth0 SRC=192.168.70.128 DST=192.168.70.2 LEN=71 TOS=0x00 PREC=0x00 TTL=64 ID=47018 DF PROTO=UDP SPT=33353 DPT=53 LEN=51
Mar 25 06:43:11 G21097714 kernel: [410.232197] [UFW AUDIT] IN=eth0 OUT= MAC=00:0c:29:bd:bf:dd:00:50:56:e3:ba:b7:08:00 SRC=192.168.70.2 DST=192.168.70.128 LEN=146 TOS=0x00 PREC=0x00 TTL=128 ID=65274 PROTO=UDP SPT=53 DPT=33353 LEN=126
Mar 25 06:43:11 G21097714 kernel: [410.232428] [UFW AUDIT] IN= OUT=eth0 SRC=192.168.70.128 DST=192.168.70.2 LEN=59 TOS=0x00 PREC=0x00 TTL=64 ID=47020 DF PROTO=UDP SPT=35220 DPT=53 LEN=39
Mar 25 06:43:11 G21097714 kernel: [410.232437] [UFW ALLOW] IN= OUT=eth0 SRC=192.168.70.128 DST=192.168.70.2 LEN=59 TOS=0x00 PREC=0x00 TTL=64 ID=47020 DF PROTO=UDP SPT=35220 DPT=53 LEN=39
Mar 25 06:43:11 G21097714 kernel: [410.236345] [UFW AUDIT] IN=eth0 OUT= MAC=00:0c:29:bd:bf:dd:00:50:56:e3:ba:b7:08:00 SRC=192.168.70.2 DST=192.168.70.128 LEN=134 TOS=0x00 PREC=0x00 TTL=128 ID=65275 PROTO=UDP SPT=53 DPT=35220 LEN=114
Mar 25 06:43:11 G21097714 kernel: [410.266231] [UFW AUDIT] IN= OUT=eth0 SRC=192.168.70.128 DST=192.168.70.2 LEN=71 TOS=0x00 PREC=0x00 TTL=64 ID=47025 DF PROTO=UDP SPT=48162 DPT=53 LEN=51
Mar 25 06:43:11 G21097714 kernel: [410.266239] [UFW ALLOW] IN= OUT=eth0 SRC=192.168.70.128 DST=192.168.70.2 LEN=71 TOS=0x00 PREC=0x00 TTL=64 ID=47025 DF PROTO=UDP SPT=48162 DPT=53 LEN=51
Mar 25 06:43:11 G21097714 kernel: [410.277769] [UFW AUDIT] IN=eth0 OUT= MAC=00:0c:29:bd:bf:dd:00:50:56:e3:ba:b7:08:00 SRC=192.168.70.2 DST=192.168.70.128 LEN=146 TOS=0x00 PREC=0x00 TTL=128 ID=65276 PROTO=UDP SPT=53 DPT=48162 LEN=126
Mar 25 06:43:11 G21097714 kernel: [410.277999] [UFW AUDIT] IN= OUT=eth0 SRC=192.168.70.128 DST=192.168.70.2 LEN=59 TOS=0x00 PREC=0x00 TTL=64 ID=47028 DF PROTO=UDP SPT=38891 DPT=53 LEN=39
Mar 25 06:43:11 G21097714 kernel: [410.278005] [UFW ALLOW] IN= OUT=eth0 SRC=192.168.70.128 DST=192.168.70.2 LEN=59 TOS=0x00 PREC=0x00 TTL=64 ID=47028 DF PROTO=UDP SPT=38891 DPT=53 LEN=39
Mar 25 06:43:25 G21097714 kernel: [424.246784] [UFW AUDIT] IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:50:56:c0:00:08:08:00 SRC=192.168.70.1 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 06:43:55 G21097714 kernel: [454.257714] [UFW AUDIT] IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:50:56:c0:00:08:08:00 SRC=192.168.70.1 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 G21097714 kernel: [484.297173] [UFW AUDIT] IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:50:56:c0:00:08:08:00 SRC=192.168.70.1 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 06:44:55 G21097714 kernel: [514.299168] [UFW AUDIT] IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:50:56:c0:00:08:08:00 SRC=192.168.70.1 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 G21097714 kernel: [541.935166] [UFW AUDIT] IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:50:56:c0:00:08:08:00 SRC=192.168.70.1 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=24786 PROTO=UDP SPT=57621 DPT=57621 LEN=52
Mar 25 06:45:23 G21097714 kernel: [542.283928] [UFW AUDIT] IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:50:56:c0:00:08:08:00 SRC=192.168.70.1 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=24787 PROTO=UDP SPT=57621 DPT=57621 LEN=52
Mar 25 06:45:26 G21097714 kernel: [545.321409] [UFW AUDIT] IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:50:56:c0:00:08:08:00 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 06:46:00 G21097714 kernel: [579.144571] [UFW AUDIT] IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:50:56:c0:00:08:08:00 SRC=192.168.70.1 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=24791 PROTO=UDP SPT=57621 DPT=57621 LEN=52
Mar 25 06:46:30 G21097714 kernel: [609.154347] [UFW AUDIT] IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:50:56:c0:00:08:08:00 SRC=192.168.70.1 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=24792 PROTO=UDP SPT=57621 DPT=57621 LEN=52
Mar 25 06:47:00 G21097714 kernel: [639.168341] [UFW AUDIT] IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:50:56:c0:00:08:08:00 SRC=192.168.70.1 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=24793 PROTO=UDP SPT=57621 DPT=57621 LEN=52
Mar 25 06:47:10 G21097714 kernel: [649.821152] [UFW AUDIT] IN= OUT=eth0 SRC=192.168.70.128 DST=192.168.70.2 LEN=71 TOS=0x00 PREC=0x00 TTL=64 ID=52167 DF PROTO=UDP SPT=60153 DPT=53 LEN=51
Mar 25 06:47:10 G21097714 kernel: [649.821166] [UFW ALLOW] IN= OUT=eth0 SRC=192.168.70.128 DST=192.168.70.2 LEN=71 TOS=0x00 PREC=0x00 TTL=64 ID=52167 DF PROTO=UDP SPT=60153 DPT=53 LEN=51
Mar 25 06:47:10 G21097714 kernel: [649.828149] [UFW AUDIT] IN=eth0 OUT= MAC=00:0c:29:bd:bf:dd:00:50:56:e3:ba:b7:08:00 SRC=192.168.70.2 DST=192.168.70.128 LEN=146 TOS=0x00 PREC=0x00 TTL=128 ID=65278 PROTO=UDP SPT=53 DPT=60153 LEN=126
Mar 25 06:47:10 G21097714 kernel: [649.828397] [UFW AUDIT] IN= OUT=eth0 SRC=192.168.70.128 DST=192.168.70.2 LEN=59 TOS=0x00 PREC=0x00 TTL=64 ID=52169 DF PROTO=UDP SPT=59725 DPT=53 LEN=39
Mar 25 06:47:10 G21097714 kernel: [649.828407] [UFW ALLOW] IN= OUT=eth0 SRC=192.168.70.128 DST=192.168.70.2 LEN=59 TOS=0x00 PREC=0x00 TTL=64 ID=52169 DF PROTO=UDP SPT=59725 DPT=53 LEN=39
Mar 25 06:47:10 G21097714 kernel: [649.832403] [UFW AUDIT] IN=eth0 OUT= MAC=00:0c:29:bd:bf:dd:00:50:56:e3:ba:b7:08:00 SRC=192.168.70.2 DST=192.168.70.128 LEN=134 TOS=0x00 PREC=0x00 TTL=128 ID=65279 PROTO=UDP SPT=53 DPT=59725 LEN=114
Mar 25 06:47:10 G21097714 kernel: [649.872001] [UFW AUDIT] IN= OUT=eth0 SRC=192.168.70.128 DST=192.168.70.2 LEN=71 TOS=0x00 PREC=0x00 TTL=64 ID=52179 DF PROTO=UDP SPT=39444 DPT=53 LEN=51
Mar 25 06:47:10 G21097714 kernel: [649.872014] [UFW ALLOW] IN= OUT=eth0 SRC=192.168.70.128 DST=192.168.70.2 LEN=71 TOS=0x00 PREC=0x00 TTL=64 ID=52179 DF PROTO=UDP SPT=39444 DPT=53 LEN=51
Mar 25 06:47:10 G21097714 kernel: [649.876503] [UFW AUDIT] IN= OUT=eth0 SRC=192.168.70.128 DST=192.168.70.2 LEN=59 TOS=0x00 PREC=0x00 TTL=64 ID=52180 DF PROTO=UDP SPT=44808 DPT=53 LEN=39
Mar 25 06:47:10 G21097714 kernel: [649.876515] [UFW ALLOW] IN= OUT=eth0 SRC=192.168.70.128 DST=192.168.70.2 LEN=59 TOS=0x00 PREC=0x00 TTL=64 ID=52180 DF PROTO=UDP SPT=44808 DPT=53 LEN=39
Mar 25 06:47:30 G21097714 kernel: [669.228820] [UFW AUDIT] IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:50:56:c0:00:08:08:00 SRC=192.168.70.1 DST=192.168.70.255 LEN=72 TOS=0x00 PREC=0x00 TTL=128 ID=24794 PROTO=UDP SPT=57621 DPT=57621 LEN=52
co2508admin@G21097714Blue:~$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
32°C
Mostly sunny
Search
ENG
UK
1:29 PM
25-Mar-24

Analyse the system log files.

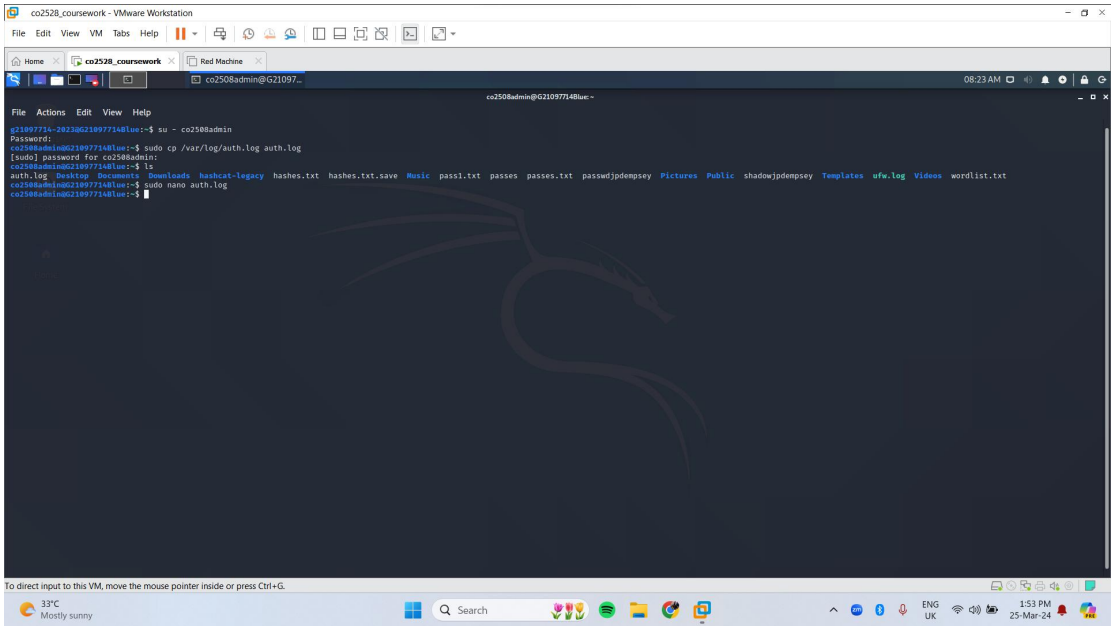
- $ su - co2508admin

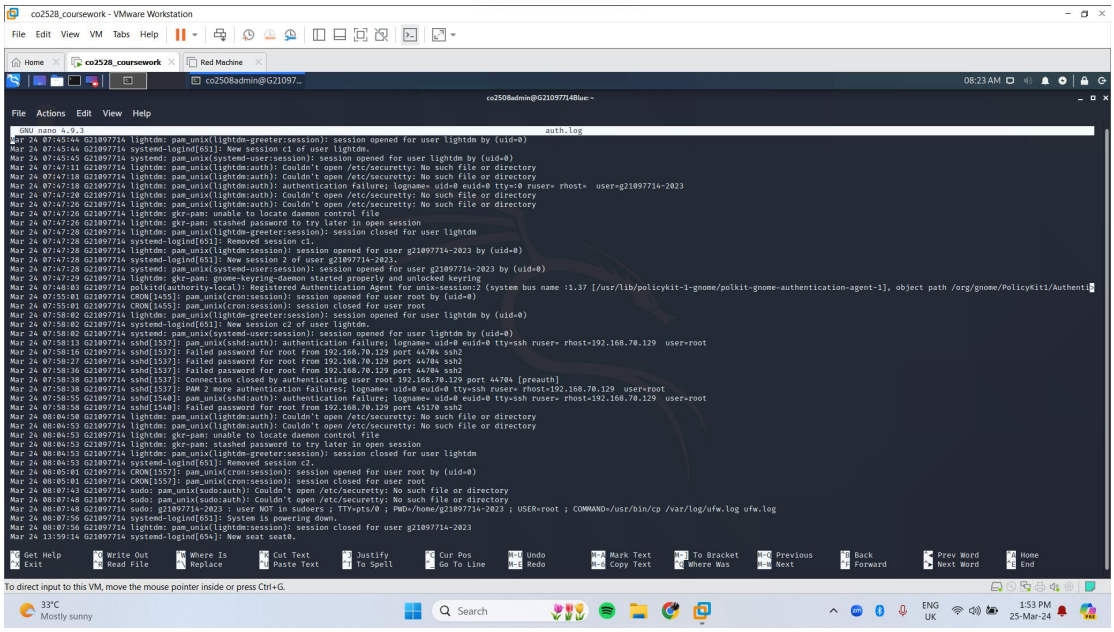
To go into the sudoers file

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

Getting the copy of the log file.

- $ ls
- $ sudo nano auth.log



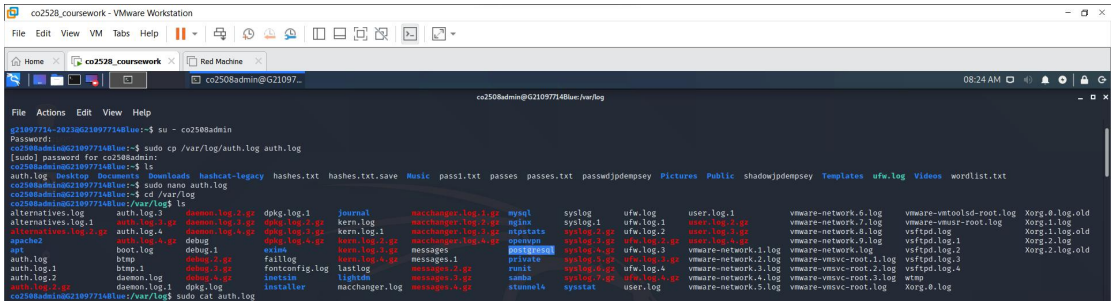


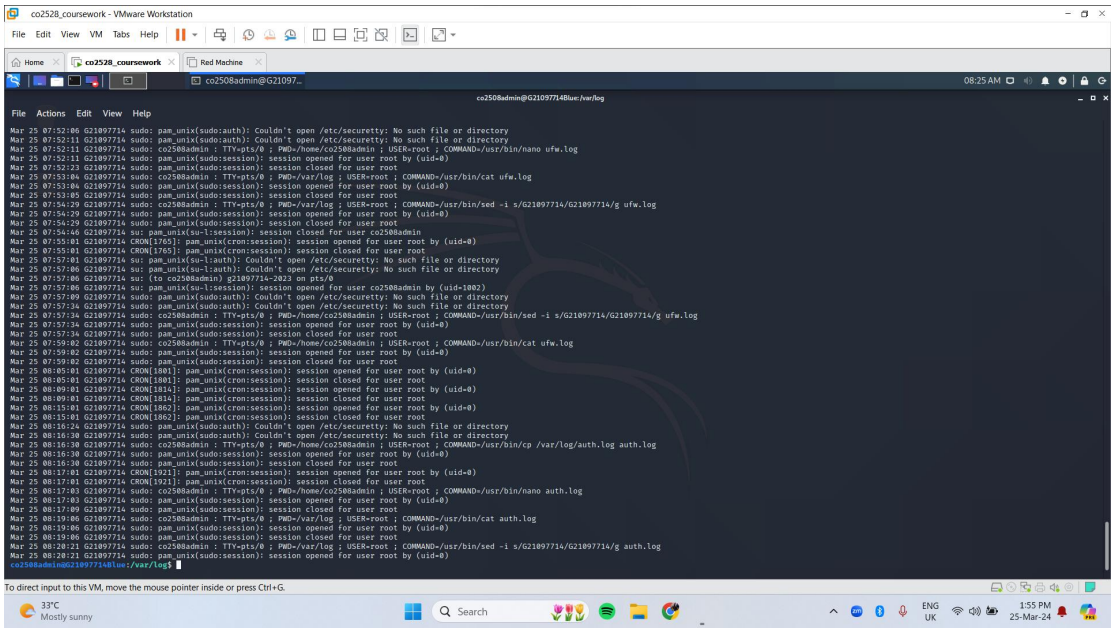
- $ cd /var/log

To go inside var log

- $ ls
- $ sudo cat auth.log

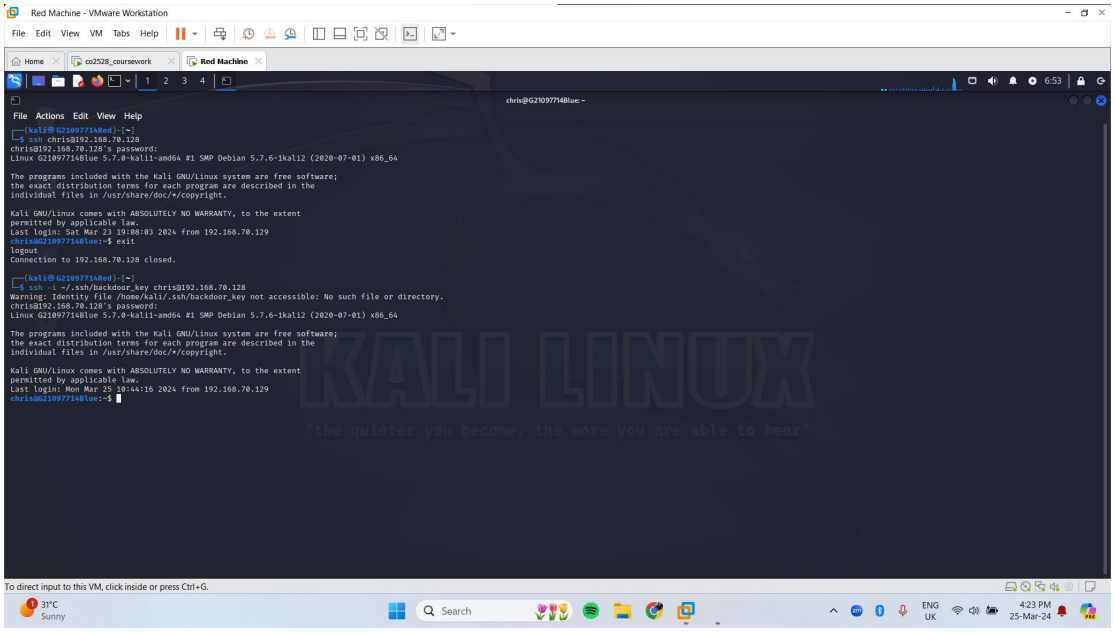
Used to output the contents of the ufw.log

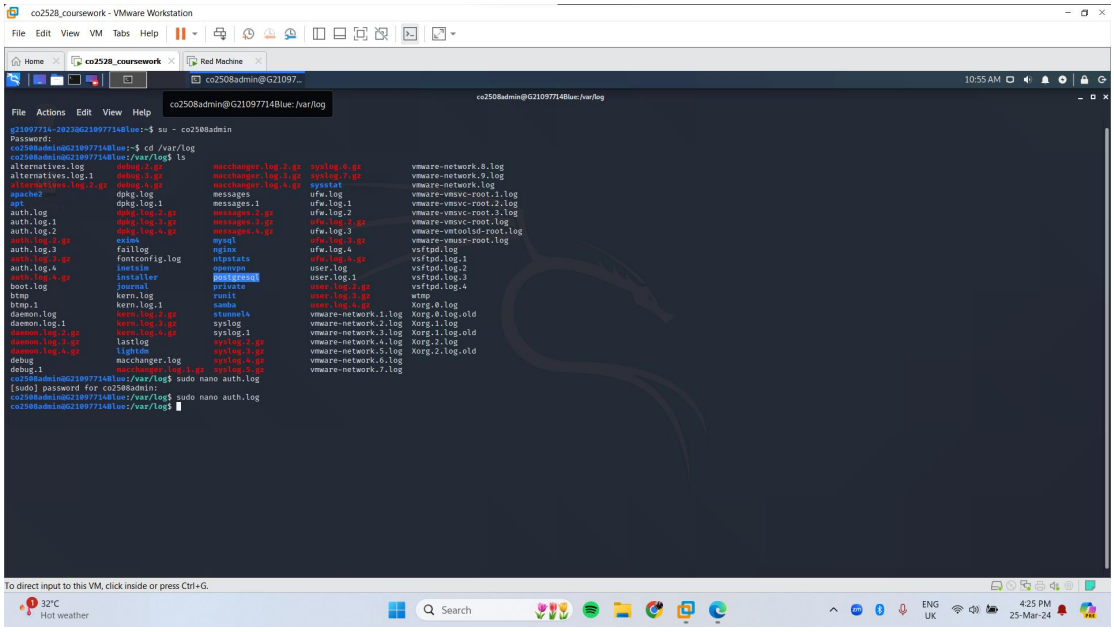




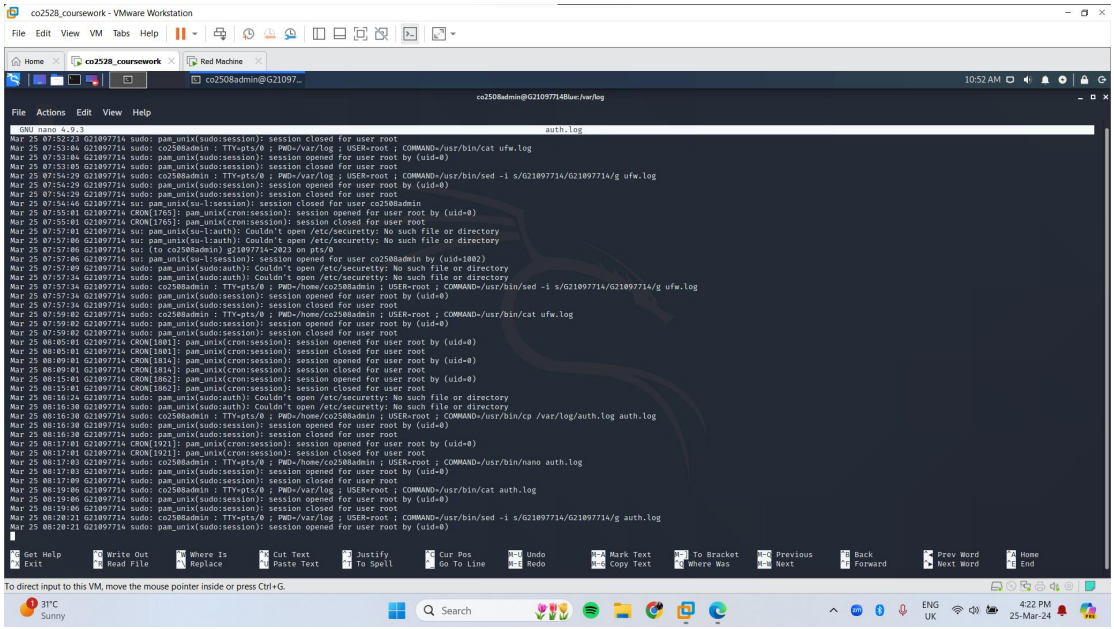
Identify in the system logs (if possible) where the red team have created a backdoor.

- $ ssh -I ~/.ssh/backdoor_key chris@192.168.70.128





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



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?			
Were the commands described?			3
Was the OS finger printing done correctly?			
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