Cheat Sheet

Common Commands and Methodologies

RECON

Before starting the lab, do a full scan to find low hanging fruit. “At this stage, using tools such as nmap/arp-scan/netdiscover would be useful to see all the machines in the subnet which we would have access to, then start port scanning for key services (DNS, FTP, HTTP/HTTPS, NetBIOS, SSH/rDesktop/VNC)” -g0tm1lk (i think)

Also open up this checklist for enumeration, its pretty good! github.com/theonlykernel/enumeration/wiki ### Autorecon Before doing anything probably start an autorecon scan. It gives a ton of info and can be pretty useful. It also sets up folders nicely for the rest of the pentest.

Nmap Scanning

Start with a quick-ish nmap scan, then after run a more intense scan in the background.
First Scan:

```
$ sudo nmap -sV -v -sC -oA 10.11.1.72-top1000 10.11.1.72
```

Full TCP scan:

```
$ sudo nmap -sV -sT -p- -v -oA 10.11.1.72-tcp 10.11.1.72
```

Full UDP scan (because g0tm1lk said “Don’t forget about UDP (*cough* because we haven’t *cough*)”:

```
$ sudo nmap -sV -sU -p- -v -oA 10.11.1.72-udp 10.11.1.72
```

After you scan ALL the ports, you can run the original nmap command but on the list of open ports. `nmap 10.11.1.72 -p 22,25,80,110,111,119,2049,4555 -sV -sC -v -oA foundports-aggressive`

The correct way to domb this is probably unicorn scan to get open ports, then nmap aggressive scan on all the open unicorn ports. This can be done with onetwopunch, but I should write my own script to do this maybe.

DNS

dns and revrese dns lookup and zone transfer:
reverse dns lookup bruteforce:

```
for ip in $(seq 50 100); do host 38.100.193.$ip; done | grep -v "not found"
```

dns lookup bruteforce:

```
for ip in $(cat usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt); do host $ip.megacorpone
```

find name server:

```
host -t ns megacorpone.com | cut -d " " -f 4
ns1.megacorpone.com.
ns2.megacorpone.com.
ns3.megacorpone.com.
```

zone transfer:

```
host -l <domain name> <dns server address>
host -l megacorpone.com ns1.megacorpone.com
```

Vulnerability scanning

You should also run specific tools/nmap scripts based on what ports are open. Autorecon does some of this, and it also gives you recommendations on tools to run. If you want to do it 100% manually, take a look at the service-scans-default.toml file that comes with autorecon. It bascially tells you what to run based on what services are being run on each port (even though it does this automatically, scripts can make mistakes, so if you are stuck try double checking.)

smb

nfs

smtp

snmp

web app nitko is a general vuln scanner:
`nikto -host=http://www.megacorpone.com -maxtime=30s`

Dirbuster is a gui app that bruteforces directories. Run with dirbusters medium wordlist and it should be fine.

Check ssl cert.

SSl server test: https://www.ssllabs.com/ssltest/

Post Explotation Enumeration

Linucks post enumeration save all passwords and hashes (/etc/shadow, /etc/passwd), ssh public key fingerprints, etc. Check connections to other machines in the network `netstat -antup` (you may also see sql running with this, if it is connect to it and read the database info, it could have some interesting stuff!), check all home folders `ls -lahR /home`, check if xorg ix running `pgrep -l x` and if so, then we can check browser loot like passwords history and cookies (i know almost as a fact that some cookie passwords are reused, such as on the box that is friends with alice supposedly) etc. Also save privesc script outputs to my local machine. Find pgpkeys, ssh keys, backups and passwords:
`find / \( -name ".ssh" -o -name ".gnupg" -o -name "*.bak" \)`
`find / -name password*` https://github.com/mubix/post-exploitation/wiki/Linux-Post-Exploitation-Command-List#collecting_info

Winblows https://github.com/emilyanncr/Windows-Post-Exploitation

Other Useful Stuff:

Spawn tty shell:
`$python -c 'import pty; pty.spawn("/bin/bash")'`

Payloads: PayloadsAllTheThings
Reverse Shells: PenTestMonkey