

Index - Tools By Keyword (SANS 504-B)

Absinth - SQLi Blind Injection Tool...(5 / 172)

aircrack-ng-CUDA (cracks WPA2 PSK w/ GPU)...(5 / 12)

Bing Dorking Tool // Bishop Fox BHDB...(1 / 166)

Bishop Fox Co // Google Dorks...(1 / 166)

Browser Exploitation Framework (BeEF)...(5 / 131)

Burp Suite - Web App Attack Proxy...(5 / 97)

CeWL - Spiders web pages and generates unique words as pswd list...(4 / 117)

Cipher /w...(1 / 46)

Cobalt Strike // Commercial Exploit Framework...(3 / 20)

Core Impact // Commercial Exploit Framework...(3 / 20)

Core Impact // Vuln Scanner capabilities...(2 / 154)

CUDA-Multiforcer (crack unsalted MD4/5, NT Hashes)...(5 / 12)

Dig - DNS Query Tool...(1 / 158)

dig -t AXFR // nix dns zone transfer cmd...(1 / 158)

Djohn (Distribted JtR cracking tool)...(4 / 11)

Dnetj (JtR Distributed cracking tool)...(5 / 11)

Dradis - Pentest team collaboration tool...(1 / 116)

emacs - GUI-based text editor in *nix instances...(99 / 99)

Enum // SMB User / Group Capture; spts anon and auth sessions...(2 / 159)

Etherpad - Pentest Collaboration Tool...(1 / 117)

ExifTool - Overview...(1 / 125)

Fiddler - Web App Attack Proxy...(5 / 97)

FOCA...(1 / 124)

Foundstone Scanning Service // Remote Vuln Scan Svc...(2 / 154)

FSDB // Foundstone Database...(1 / 166)

Google Dorking - File ext usage...(1 / 163)

Google Hacking Database...(1 / 164)

GPU MD5 (Crack Unsalted MD5)...(5 / 12)

Hashcat (CPU only -based cracking)...(5 / 13)

Index - Tools By Keyword (SANS 504-B)

Im2ntcrack - Metasploit framework tool to render pswd in correct case...(4 / 115)

Immunity Canvas // Commercial Exploit Framework...(3 / 20)

Jikto - Java-based variant of Nikto \\ performs internal XSS scans...(5 / 130)

John-MPI (JtR distributed cracking tool)...(5 / 11)

Kon-boot \\ Boot loader; alters kernel (win or nix); removes need for paswd entry (null)...(4 / 131)

Lair - Pentest Collaboration Tool...(1 / 117)

Linux / sudo su - //run command as root//...(1 / 54)

MagicTree - Team Pentest Collaboration Tool...(1 / 116)

Mallory - Web App Attack Proxy...(5 / 97)

MBSA // MS Baseline Sect Analyzer - Software Inventory tool...(3 / 14)

MediaWiki - Pentest Team Collaboration toom...(1 / 116)

Metasploit - Psexec w/ PTH \\ Module accepts hash or password...(5 / 70)

Metasploit Autopwn - Enumerates Client-side Programs...(3 / 13)

Metasploit Database - Pentest Collaboration Tool...(1 / 117)

Metasploit Framework Console Prompt...(1 / 51)

MetaSploit Pro // Vuln Scanner...(2 / 154)

Metasploit Shell Prompt...(1 / 51)

Microsoft Baseline Security Analyzer...(3 / 14)

msfencode // depercated msfconsole payload encoder...(3 / 103)

msfmap \\ optional module for port scanning from within MSF compromised host...(3 / 74)

msfvenom // msfconsole payload encoder...(3 / 103)

ncpa.cpl // Windows - Launches Networking Ctrl Pnl...(1 / 57)

Nessus Vulnerability Scanner - General...(2 / 130)

Netcat - General Overview...(2 / 170)

Netcat - Options...(2 / 171)

netcat - port scanner syntax...(2 / 174)

Netcat - Service-Is-Alive Heartbeat sytax...(2 / 176)

Netcat \\ piping std in/out syntax...(2 / 170)

Nikto - Web App Vuln Scanner (General)...(5 / 82)

Index - Tools By Keyword (SANS 504-B)

NLNZ - National Lib of New Zealand... (1 / 124)

nmap - Default scans top 1000 ports... (2 / 9)

nmap - general... (2 / 42)

nmap -p 0-65536 (scan all ports)... (2 / 9)

Nmap-services // File containing (Ranking most popular ports in order)... (2 / 51)

nslookup - General Usage... (1 / 155)

nslookup - usage... (1 / 156)

ntdsxtract - parses nthashes from ntds.dit... (4 / 148)

ocl Hashcat... (5 / 13)

oclHashcat (cpu/GPU-based password cracking)... (5 / 13)

Odysseus / Telemachus - Web App Attack Proxy... (5 / 97)

OpenVAS // Free Fork of Nessus 2... (2 / 131)

P0f2 - Passive OS Fingerprinting tool... (2 / 71)

Password Attacks \\ Cain - General... (5 / 25)

Patchlink Scanner // Vuln Scanner... (2 / 154)

Powershell Command Prompt... (1 / 51)

Precomp - Rainbow Tbl Generator from Ophcrack... (5 / 55)

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)

Rapid 7 - Metasploit Pro // Commercial Exploit Framework... (3 / 20)

Rapid 7 NeXopse // Vuln Scanner... (2 / 154)

Recon-ng overview... (1 / 170)

Retina // Vuln Scanner... (2 / 154)

rtgen - Rainbow Tbl Generator... (5 / 55)

Saint // Vuln Scanner... (2 / 154)

ScanRand - Hyperfast Port Scanner... (2 / 13)

Scapy - Functions... (2 / 86)

Scapy - Launching options... (2 / 84)

Index - Tools By Keyword (SANS 504-B)

Scapy - Packet Crafting...(2 / 87)

Scapy - Packet Crafting // General...(2 / 84)

Search Diggity - Gui...(1 / 168)

Search Diggity Suite...(1 / 167)

ServifyThis \\ wraps a service w/ api call to notify Win sever start successful...(4 / 60)

shg - Rainbow Tbl Generator (SMB Hash Generator)...(5 / 55)

Shread -n...(1 / 46)

Sid2User // Windows to enum users accts on host...(2 / 157)

Sid2User - Takes win SID and queries host for usr name...(2 / 161)

Skip Tracing Framework - Recon tool list...(1 / 119)

SQLmap - SQLi tool to discover and exploit vulns...(5 / 163)

Strings...(1 / 124)

Strings - Tool Overview...(1 / 126)

Systemals Strings - Locates Unicode & ASCII strings...(1 / 126)

tcpdump - CLI packet sniffer / Linux & Windows port...(2 / 15)

tcpdump - Legacy tool captures first 68 bytes by default...(2 / 17)

THC-Hydra \\ Bruteforce password guessing tool...(4 / 133)

Traceroute - Linux // discover route packet takes...(2 / 23)

traceroute ICMP Filter response // * (Exceeded in Transit)...(2 / 23)

Tracert // Windows...(2 / 23)

tracert -6 // Windows IPv6...(2 / 23)

Trouceroute -6 // Linux IPv6 version...(2 / 23)

User2sid // Windows tool to enum users...(2 / 157)

User2sid // uses LookupAccountname API to convert usr name to a SID...(2 / 161)

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)

Veil-Evasion // Exploit Encoder...(3 / 105)

Vmware Guest Settings - Cntl + D...(1 / 58)

Index - Tools By Keyword (SANS 504-B)

Volumn Shadow Copy Service (VSS) \\ used to grab ntdt.dit from domain...(4 / 161)

w3af - Web App Attack Proxy...(5 / 97)

Webscarab - Web App Attack Proxy...(5 / 97)

Whois - General...(1 / 142)

Whois - gooktools.com...(1 / 142)

Whois - Internic.net...(1 / 142)

Whois - Whois.net...(1 / 142)

Wikto - .Net Web Vuln Scanner (port of Nikto)...(5 / 83)

Windows CMD Elevated - Cntl-Shift-Enter...(1 / 52)

Windows CMD Prompt...(1 / 51)

Windows Credential Editor (WCE) - PTH Tool...(5 / 69)

Windows Shell Elevated Privs...(1 / 52)

Windump - port of tcpdump...(2 / 16)

Winfingerprint // GUI and CLI tool for enum sessions,user, & groups...(2 / 162)

Wireshark - Consistent String and Buffer Overflow Attacks...(2 / 19)

ZAP - Web App Attack Proxy...(5 / 97)

Zed Attack Proxy (ZAP) \\ OWASP Nontransparent Proxy and Web Scanner...(5 / 92)

Zmap: IPv4 Single port scanner...(2 / 13)