

## Index - Tools By Keyword (SANS 504-B)

Able | Rns in Background // for dumping target info...( 4 / 23 )

AFX Rootkit | User-Mode Rootkit...( 5 / 7 )

Aircrack-ng | WLAN wep cracking tool...( 2 / 64 )

Alureon/TDL (TSAA / TDL1 / TDL2) | Kernel-Mode Rootkit Windows Dev Drv Alters...( 5 / 77 )

Anti-Rootkit (Sophos) | Windows Rootkit Detector...( 5 / 81 )

ARPspooF | Manipulate IP to MAC mapping...( 3 / 48 )

ASLEAP | WLAN Dictionary Attacks on LEAP Authentication...( 2 / 64 )

Autoruns | Auto Start Entry Point viewer Microsoft...( 1 / 69 )

Avatar | Kernel-Mode Rootkit encrypt C2 / VM detect / drv bypass...( 5 / 76 )

Base64 | Coding and decoding...( 1 / 67 )

Beast | Javascript exploit using chosen plain-text to crack encrypted SSL traffic...( 3 / 62 )

BeEF | Browser exploitation tool, hooks victim browsers and attempt to exploit...( 4 / 112 )

BluePill | Kernel-Mode Rootkit Virtualization of system...( 5 / 71 )

BOK2 | Application Layer Trojan...( 5 / 7 )

Burp Suite | commercial / free used to fuzz website inputs...( 4 / 138 )

Cache:www.counterhack.net | Cached version of a web site...( 2 / 39 )

Chkrootkit | Linux Root Kit Type detection / Identification...( 5 / 80 )

Containment | Disk Duplicator...( 1 / 110 )

Containment | Forensic Image Options...( 1 / 109 )

Covert\_TCP | Covert Ch over tcp headers...( 5 / 131 )

CoWPAtty | WLAN pre-computer dictionary cracking tool for WPA/WPA2...( 2 / 65 )

cpu Hog | Local DOS Attack Tool //...( 4 / 148 )

cpuhog | DOS resource exhausting simulator...( 4 / 148 )

Crime | chosen plain-text exploit to crack encrypted SSL traffic...( 3 / 62 )

Cryptcat | Encrypted Ncat...( 3 / 7 )

CyberCPR | IR Tracking Tool w/Secure OOB Chat...( 1 / 104 )

Data Sentinel (Ionx) | File Integrity Checker...( 5 / 82 )

Dig @dns\_svr target.tld -t AXFR | Linux enumerates dns query results...( 2 / 24 )

Diggity | Suite of search tools (Google, Search, Bing, DLP,...)...( 2 / 43 )

## Index - Tools By Keyword (SANS 504-B)

DNS Transfer | nslookup set type=any ls-d...( 2 / 25 )

Dnscat | ports over DNS...( 3 / 7 )

DNSCat2 | Covert Ch trans via DNS...( 5 / 136 )

DNSSpoof | M-i-t-M Tool, does have to be on same LAN as target just btwn...( 3 / 56 )

dnsstuff.com | Web dns probing tool...( 2 / 50 )

Driftnet | commercial / monitors http for jpeg files and reassembles...( 3 / 53 )

droidsheep | android tool for web session hijacking...( 3 / 63 )

Dsniff | Linux / BSD / Win32 (unstable) - Ethernet and wlan network tool...( 3 / 43 )

Easy-Creds | WLAN Spoofs AP's / SSL MITM & strip / session hijacking...( 2 / 67 )

Enterprise IR | Kansa...( 1 / 139 )

Enterprise IR | SCCM...( 1 / 138 )

Enum | SMB Cli enums users, groups mbrs, pswd policies...( 2 / 144 )

Ettercap | Overview and options...( 3 / 71 )

Ettercap | Session theft across networks...( 3 / 67 )

eventquery.vbs | Windows vbscript query log events...( 1 / 74 )

eventvwr.msc | Windows launch event viewer via CLI...( 1 / 74 )

Evilcore | Boor Sector Root Kit...( 5 / 7 )

Evt2sys | Windows Syslog Server...( 5 / 121 )

Exe32pack | Wrapper...( 5 / 19 )

exploit-db.com | Site containing open source exploit scripts...( 1 / 153 )

EyeWitness | screenshots websites / VNC / RDP banners / trys known default creds...( 2 / 98 )

Fastdump | Memory Analysis...( 5 / 22 )

Fiddler | free allows for scripting stop points to check suseptibility...( 4 / 138 )

filesnarf | saves files captures from NFS to local host...( 3 / 51 )

Firesheep | web session hijacking...( 3 / 63 )

FOCA | Seaches for searches for MS Office files / extracts Metadata...( 2 / 41 )

Fontanini Rootkit | General...( 5 / 52 )

Fragroute | Requires FragRouter / hard for IPS venders to write sigs...( 2 / 120 )

FU | Kernal-mode Rootkit...( 5 / 7 )

## Index - Tools By Keyword (SANS 504-B)

FU | Kernel-Mode Memroy Map Alteration...( 5 / 69 )

FUTo | Kernal-mode Rootkit...( 5 / 7 )

Gcat | Covert Ch C2 (Gmail)...( 5 / 137 )

GHDB | Google Hacking Database - Recon...( 2 / 35 )

Gnu Netcat | summary...( 2 / 7 )

Google Rapid Response | Incident Response...( 1 / 39 )

GRR | Incident Response...( 1 / 39 )

Hacker Defender | User-Mode Rootkit...( 5 / 7 )

High Orbit Ion Cannon (HIOC) | DDOS tool...( 4 / 163 )

HTTP Flood | High Orbit Ion Cannon (HOIC)...( 4 / 163 )

HTTP Flood | Low Orbit Ion Cannon (LOIC)...( 4 / 162 )

Hydan | Stego hides data in win/nix exe's...( 5 / 152 )

ICMPCmd | Win Cmd.exe access over ICMP...( 5 / 128 )

ICMPShell | Tunnel payload in ICMP...( 5 / 128 )

Inception | extracts pswds from hosts with encript boot via firewire / thunderbolt...( 4 / 29 )

Input Validation | OWASP...( 4 / 82 )

InSSIDER | WLAN Discovery a/b/g/n...( 2 / 61 )

Invisible Secrets | Stego tool - Hides data in Banner Ads for websites...( 5 / 152 )

ISR-Evilgrade | Spoofs Automated Software Updates...( 2 / 12 )

Jsteg | Stego tool hides jpeg using DCT Coefficients...( 5 / 152 )

Kaminsky | DNS Cache Poison / Predict QueryID via brute force...( 3 / 90 )

Kansa | Autostart Point Entry (ASEP)...( 1 / 141 )

Karmetasploit | WLAN AP spoofing / POP, HTTP, Samba, DHCP spoofing...( 2 / 69 )

Kbeast | Kernal-mode Rootkit...( 5 / 7 )

KIS | Kernal-mode Rootkit...( 5 / 7 )

Kismet | WLAN scanner spts a,b,g,n,Zigbee...( 2 / 63 )

Kismet Wifi Sniffing War Driving | AP & Zigbee Passive Discovery...( 2 / 63 )

Kiwi Syslog | Windows Syslog Server...( 5 / 121 )

Konboot | cool boot password extraction tool...( 4 / 29 )

## Index - Tools By Keyword (SANS 504-B)

Kon-boot | Boot Sector Root Kit...( 5 / 7 )

LADS | Windows ADS Detection...( 5 / 110 )

Linkcat | Uses raw ether frames...( 3 / 7 )

Loki | Linux // Hides Payloads inside ICMP...( 5 / 128 )

Low Orbin Ion Cannon (IOC) | DDOS tool...( 4 / 162 )

Lrk6 | User-Mode Rootkit...( 5 / 7 )

lusmgr.msc | Launches User Mgr from CLI...( 1 / 71 )

Macof | Manupulate MAC to Phy Port Mapping...( 3 / 48 )

mailsnarf | saves email from captured pop / smtp sessions on local host...( 3 / 51 )

Maltego | Defenses...( 2 / 48 )

Maltego | Paterva's Automated Intel gathering suite...( 2 / 46 )

Maltego | Transforms Overview...( 2 / 47 )

Masscan | spilts send / receive part 3-way handshake, scans 1ks host per min...( 2 / 97 )

Maux | Firmware Rootkit (Ethernet and Video Cards)...( 5 / 7 )

md5deep | md5 hash of file...( 1 / 109 )

md5sum | Creates MD5 hash of file...( 1 / 109 )

Mdd | Memory Analysis...( 5 / 22 )

Mebroim BIOS Rootkit | Firmware Rootkit (Motherboards and BIO)...( 5 / 7 )

MemoryDD.Bat | Memory Analysis...( 5 / 22 )

Memoryze | Forensic Memort acqisition tool...( 1 / 109 )

Memoryze | Memory Analysis...( 5 / 22 )

MP3Stego | Stego tool hides data in Mpeg files...( 5 / 152 )

msf | search | Metasploit...( 1 / 155 )

msfelfscan | Metasploit tool searchs Linux binaries for buffer overflow potential...( 3 / 106 )

Msgsnarf | captures IM msg and saves to local host...( 3 / 51 )

mspedescan | Metasploit tool searchs Windows binaries for buffer overflow potential...( 3 / 106 )

Msyslog | Windows Syslog Integrity Checker...( 5 / 122 )

Ncat | budled with nmap / spt SSL / mulit connections / NAT-bypass...( 3 / 7 )

Nessus | Dangerous Plug-ins...( 2 / 127 )

## Index - Tools By Keyword (SANS 504-B)

Nessus | Vuln Scanner / most popular / client-server architecture / plug-ins...( 2 / 125 )

netcat -l -p 2222 | establish a listener...( 1 / 80 )

NetStumbler | WLAN Discovery a/b/g nets...( 2 / 61 )

network-tools.com | web hosts tools launched from a 3rd party for recon...( 2 / 50 )

Niksun | commercial / reassembles entire http session from captures traffic...( 3 / 53 )

NMAP | Default Protocols for sweep...( 2 / 82 )

Ollydbg | Unpacker...( 5 / 20 )

Omnipeek | WLAN Sniffer commercial tool; formerly airopEEK...( 2 / 64 )

OpenPuff | Stego multi-pswd spt / multi-rnd encrypt / images,audio,Vid,flash...( 5 / 153 )

OpenStego | Stego Embeds data and digital watermarks into images...( 5 / 153 )

OSSEC | File Integrity Checker...( 5 / 82 )

Phrack 66 | Firmware Rootkit (Vmware and Awd BIOS)...( 5 / 7 )

PingChat | Win Chage over ICMP Program...( 5 / 128 )

Poison Ivy | Application Layer Trojan...( 5 / 7 )

Poison Ivy | Trojan Application-Level...( 5 / 14 )

Powerbleed | uses malformed Heartbleed requests to extract server keys from memory...( 3 / 61 )

Process Explorer | Windows Systemals Displays running processes...( 1 / 76 )

Process Monitor | Windows Systemals...( 1 / 76 )

Ptunnel | ICMP Tunneling Tool (via Echo / Reply packets)...( 5 / 128 )

PushPin | Linux Part of Recon-ng, provides social media geo-location...( 2 / 31 )

pwdump | for dumping pswds from hosts...( 4 / 29 )

py2exe | Converts python into exe...( 5 / 148 )

pyInjector | Converts Python Scripts into Exe...( 5 / 148 )

pyinstaller | Converts python into exe...( 5 / 148 )

Qualys | Vuln Scanner / Best for PCI Compliance scans...( 2 / 124 )

QUICK | Covert trans via multiplex UDP streams...( 5 / 136 )

reg query | cli query of a specified registry key...( 1 / 69 )

regedit | Windows GUI registry editor...( 1 / 84 )

Rekall | Memory Analysis...( 5 / 22 )

## Index - Tools By Keyword (SANS 504-B)

Remux | Scans via multiple open Proxies, Python tool, bypasses tor blocks...( 2 / 99 )

Rootcheck - OSSEC | Linux Rootkit Detection (Only Actively Maintained)...( 5 / 80 )

Rootkit Detective | Windows Rootkit Detection...( 5 / 81 )

Rootkit Hunter | Linux Rootkit Detection...( 5 / 80 )

Rootkit Revealer (PSTOOLS) | Windows Rootkit Detection...( 5 / 81 )

Rooty | Kernel-Mode Rootkit Linux LKM & Drvr Spt...( 5 / 73 )

RTIR | Real Time Incident Response...( 1 / 103 )

SANS Investigative Forensics Toolkit (SIFT) | Incident Response...( 1 / 43 )

Scheduled Tasks | Windows GUI...( 1 / 73 )

SCTP | Covert Ch trans via multi-streaming w/ c2...( 5 / 136 )

secpol.msc | Windows GUI for editing local security policy...( 1 / 88 )

Security Onion | Rootkit Detection / C2 Communications...( 5 / 83 )

services.msc | Windows GUI launch from cli...( 1 / 68 )

shodan | Web hosted probe and OSINT results...( 2 / 50 )

SilentEye | Stego encrypts data into Jpg, BMP, and Wav...( 5 / 153 )

SL4NT | Windows Syslog Server...( 5 / 121 )

S-Mail | Stego tool hides data in exe/dll files...( 5 / 152 )

Snare Agent / Log Server | Windows System agent and server - commercial...( 5 / 121 )

Socat | relays across data ch / Spts SSL and Raw IP...( 3 / 7 )

SSLStrip | rewrites url's back to client to replace HTTPS w/ HTTP in all links...( 3 / 64 )

Stash | Stego Tool hides data in variety of formats...( 5 / 152 )

StegExpose | Stego // Java// detects w/i lossless img format /< Sig Bit (LSB)...( 5 / 158 )

Sub7 | Application Layer Trojan...( 5 / 7 )

Subterfuge | Web MITM tool for: session hijack / SSL strip / VPN Ch Blocking...( 3 / 73 )

Subvert | Kernel-Mode Rootkit Virtualization...( 5 / 71 )

Super User Control Kit (SUCKit) | Kernel-Mode Rootkit Memory Alteration...( 5 / 69 )

SuperUser Control Kit | Kernal-mode Rootkit...( 5 / 7 )

Tamperdata | firefox plugin for manipulating http request prior to returning response...( 4 / 136 )

tasklist | Windows running tasks and processes...( 1 / 67 )

## Index - Tools By Keyword (SANS 504-B)

tasklist /svc | Windows running tasks...( 1 / 68 )

tcpkill | sends resets to kill tcp connects / forces new session auth...( 3 / 50 )

tcpnice | injusts packets w/ sml window sizes to slow packet rates on fast conn...( 3 / 50 )

TCPView | Windows Systemals TCP/UDP Port Listeners...( 1 / 76 )

TFN | DDOS Tool...( 4 / 157 )

THChydra | overview...( 4 / 8 )

Themida | Wrapper...( 5 / 19 )

traceroute.com | web hosted trace routing / validates route from 3rd party source...( 2 / 50 )

Tribe Flood Network (TFN) | DDOS...( 4 / 157 )

Tribe Flood Network (TFN) / TFN2000 | DDOS Tool / resource exhaustion...( 4 / 157 )

Tripwire | File Integrity Checker...( 5 / 82 )

TTYsnoop | Session Hijacking for terminal and VPN...( 3 / 67 )

TTYSpy | terminal and VPN session theft...( 3 / 67 )

UPX | Wrapper...( 5 / 19 )

URLSnarf | captures url's from http traffic...( 3 / 51 )

Vbootkit 2.0 | Boot Sector Rootkit...( 5 / 7 )

vmlinuz | Kernel-Mode File Alteration...( 5 / 70 )

VNC | General...( 5 / 11 )

Volatility | Forensic Image acqisition...( 1 / 109 )

Volatility Framework | Memory Analysis (Python)...( 5 / 22 )

VSAgent | Covert Channels VIEWSTATE...( 5 / 141 )

w3af | Free used to assess for attack suseptibility...( 4 / 138 )

WAF | Web Application Proxy / requires tuning to be effective...( 4 / 142 )

WarVOX | spoofs caller id, MP3 of results, break into VoIP and Cell VM boxes...( 2 / 54 )

Wayback Machine | Cached prior versions of websites...( 2 / 39 )

Web-Based Recon | Web hosted recon scanner tools...( 2 / 50 )

Webspy | sends dsniif-ed url's to attackers browser in realtime...( 3 / 53 )

WEPCrack | WLAN intercepts and Cracks WEP keys...( 2 / 64 )

Win32dd | Memory Analysis...( 5 / 22 )

## Index - Tools By Keyword (SANS 504-B)

Windows Credential Editor (WCE) | Windows for pass the hash and pass the token...( 4 / 52 )

Windows Firewall Settings | Show Configuration...( 1 / 66 )

Windows Management Instruction CLI | Show Process list...( 1 / 67 )

Winpmem | Memory Analysis (most Popular)...( 5 / 22 )

WinVNC | General...( 5 / 13 )

wmic | Show Process list...( 1 / 67 )

Xplico | reassembles files, videos, and images / scales to multiple hosts...( 3 / 52 )

Yoda | Wrapper...( 5 / 19 )

ZAP | Free OWASP tool for checking for info leak, XXS, SQLi, etc.....( 4 / 139 )

ZenMap | General / GUI for Nmap...( 2 / 80 )

Zenmap | Overview...( 2 / 84 )