

' or '1'=1 (4 / 130)

(+) Symbol indicator in raw packet (2 / 112)

/dev/kmem (5 / 69)

/etc/passwd (4 / 36)

/etc/password (1 / 217)

/etc/resolv.conf (3 / 87)

/etc/shadow (1 / 217)

/etc/shadow (4 / 37)

3-Way Handshake (Port Scanning) (2 / 90)

4 Levels - Identification (Attacks) (1 / 59)

AAR (Lessons Learned) (1 / 128)

Account Harvesting (4 / 84)

Account Harvesting Defense (4 / 87)

ACK Scan (2 / 94)

ACK Storm (3 / 69)

admin' union select passwd from users here username='admin';-- (4 / 131)

AFX Rootkit (5 / 7)

Aircrack-ng (2 / 64)

Alureon (5 / 78)

Alureon/TDL (TSAA / TDL1 / TDL2) (5 / 77)

Amplification Attack - EDNS Overview (4 / 151)

Amplification Attack - Overview (4 / 150)

Anti-Rootkit (Sophos) (5 / 81)

Application - Level Detection Logs (1 / 58)

Application-Level (Trojans / Backdoors) (5 / 9)

Application-Level Trojan Horse (5 / 7)

Applying Lessons (Lessons Learned) (1 / 129)

ARP (Passv / Active Scans) (3 / 46)

Archived Prior Webpage Versions (2 / 39)

ARP (3 / 47)

arp -a (Linux Tools) (1 / 256)

arp -a (Detect Session HiJacking) (3 / 75)

ARP Cache Poisoning (3 / 70)

arp -e (3 / 75)

ARPspooF (3 / 48)

ASEP (1 / 141)

ASLEAP (2 / 64)

Assessment of Event Impact (1 / 93)

at Command (1 / 73)

Attack Tool list (4 / 138)

Attacks (Trends) (2 / 4)

Attacks - General overview (2 / 9)

Attacks (Trends) (2 / 10)

Attacks (For Profit) (2 / 11)

Attacks (Defense - General) (2 / 13)

Autoruns (1 / 69)

autostart folders (1 / 70)

Avatar (5 / 76)

Backdoor (5 / 6)

Base64 (1 / 67)

base64 --decode (5 / 147)

Base64 Problem (5 / 146)

Beaconing (1 / 135)

Beast (3 / 62)

BeEF (4 / 112)

BF | %d seperation and overview (3 / 154)

BGP Hijacking (3 / 4)

BGP Hijacking (3 / 5)

[BIND \(3 / 87\)](#)

[BluePill \(5 / 71\)](#)

[BOK2 \(5 / 7\)](#)

[Boot Sector \(5 / 7\)](#)

[Bots \(Kernel-Mode Rootkit Types\) \(4 / 67\)](#)

[Bots \(Loadable Kernel Modules & Device Drivers\) \(4 / 68\)](#)

[Bots \(Altering Kernel Memory\) \(4 / 69\)](#)

[Bots \(Virtulizing Kernels to avoid Detection\) \(4 / 71\)](#)

[Bots \(Rooty\) \(4 / 73\)](#)

[Bots \(Kernel Rootkits - Altering System Call Tbl\) \(4 / 74\)](#)

[Bounds Checking \(3 / 141\)](#)

[Brute Force Attacks \(4 / 12\)](#)

[btmp \(5 / 93\)](#)

[Buffer Overflow \(General\) \(3 / 98\)](#)

[Buffer Overflow \(Registers EIP\) \(3 / 100\)](#)

[Buffer Overflow \(Procedure Pre-Amble\) \(3 / 101\)](#)

[Buffer Overflow \(Stack LIFO / Return Pointer\) \(3 / 102\)](#)

[Buffer Overflow \(Smashed Stack / RP\) \(3 / 103\)](#)

[Buffer Overflow \(Generating Overflow - Options\) \(3 / 104\)](#)

[Buffer Overflow \(3 step to locate possible candidate\) \(3 / 105\)](#)

[Buffer Overflow \(scan tools and known C function calls\) \(3 / 106\)](#)

[Buffer Overflow \(Detection Tools - Prevention\) \(3 / 107\)](#)

[Buffer Overflow \(finding overflow length - CRAM\) \(3 / 108\)](#)

[Buffer Overflow \(Bad Characters to avoid\) \(3 / 111\)](#)

[Buffer Overflow \(NOP Sleds\) \(3 / 113\)](#)

[Buffer Overflow \(NOP Generator - MSFConsole\) \(3 / 123\)](#)

[Buffer Overflow \(Defense\) \(3 / 126\)](#)

[Buffer Overflow \(Canaries\) \(3 / 128\)](#)

[Buffer Overflow \(User Input Validation\) \(3 / 129\)](#)

Index - Merged All-Terms (SANS 504-B)

Buffer Overflow (Code checking tools) (3 / 131)

Buffer Overflow (Protocol Parser Flaws) (3 / 135)

Building the IR Team (1 / 30)

Burp Suite (4 / 138)

Business Continuety Plan (1 / 10)

C2 (Botnets) (4 / 69)

C2 (Trojans) (5 / 15)

Cache Posioning (3 / 90)

Cache:www.counterhack.net (2 / 39)

Cain (LANMAN Hashes) (4 / 16)

Cain (LANMAN Brute Forcing) (4 / 18)

Cain (NT Hashes) (4 / 19)

Cain (Salt Impacts on Hashes) (4 / 20)

Cain (Rainbow Tbls) (4 / 22)

Cain (Tool Features) (4 / 24)

Cain (Pswd Cracking) (4 / 25)

Cain and Able (4 / 23)

CAM Table overflowing (3 / 79)

Canaries (3 / 128)

Center for Internet Security (CIS) (1 / 76)

Chain of Custody (1 / 96)

Chart (5 / 7)

Chkrootkit (5 / 80)

Classification of Incident (1 / 101)

client mode - overview / std 0,1,2 and err modes (3 / 8)

Code Checking Tools (3 / 131)

command - %x Writes memory to logs or screen depending on settings (3 / 164)

Command - Backgrounds metaterpreter session (3 / 122)

Command - CLI method for displaying startup list (1 / 70)

Command - Connect to SMB share as a different user (2 / 143)

Command - Data Transfer / moves a file from listener to client (3 / 12)

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

Command - Detect ADS on Win Vista + (5 / 115)

Command - Drops all outbound sessions to host (2 / 150)

Command - Drops inbound session to host (2 / 150)

Command - enums all users in domain and write to a txt file (2 / 145)

command - example xxs / sqli combo to extract hash of admin user (4 / 131)

Command - Extracts compressed files from a Tar Ball (1 / 240)

command - kills a running process (2 / 102)

Command - Launches windows Client for Networks (2 / 156)

Command - Launches windows services control panel (2 / 157)

Command - Linus establishing a SMB share to Windows Host (2 / 148)

command - Linux to display the current logged in user (1 / 215)

Command - Linux clear command history (1 / 211)

Command - Linux command to add a user (1 / 213)

Command - Linux displays all files associated with listening port (2 / 103)

Command - Linux displays ARP entries (1 / 256)

Command - Linux displays available drive space (1 / 261)

command - Linux displays details about the logged in user (1 / 215)

Command - Linux displays scheduled tasks (1 / 257)

command - Linux est interactive shell on remote host (3 / 15)

command - Linux flushes iptables settings from host (3 / 167)

Command - Linux kills the service running on specified PID (2 / 104)

Command - Linux Port Listener Listing (1 / 56)

command - Linux returns user names and passwords (4 / 35)

command - Linux runs shell without terminal window in background (3 / 16)

command - Linux sets adapter ipaddress for the session (3 / 173)

Command - Linux shell script for persistent listener (3 / 16)

Index - Merged All-Terms (SANS 504-B)

command - Linux shows ARP cache in Linux style (3 / 75)

Command - Linux shows listening ports (1 / 238)

command - Linux shows listening ports, PID, and program names (2 / 103)

Command - Linux to change to the user root (1 / 215)

Command - Linux used to list all running processes (1 / 125)

Command - Linux used to locate specific text (1 / 232)

Command - Linux used to set a users password (1 / 214)

Command - Listener Conversations w/ Binaries (1 / 55)

Command - listening ports (tcp/udp) (1 / 66)

command - Lists all running services (2 / 102)

command - Metasploit add a pivot point route stmt (3 / 122)

command - MSFConsole cmd displays info for requested exploit (3 / 175)

command - msfconsole cmd to extract the hashes from the remote host (3 / 184)

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

command - msfconsole displays all active sessions (3 / 181)

command - msfconsole displays the current user contexts ID (3 / 181)

command - msfconsole for remote shell access on host (3 / 185)

command - msfconsole searches for path to exploits that match search string (3 / 175)

Command - NetBIOS ofver TCP/IP (1 / 65)

Command - NetBIOS SMB listeners w/ owning process (1 / 66)

Command - open web console as background process (2 / 131)

Command - perfoms OS, Ver, script-scan, & tracert (2 / 108)

command - Perl cmd used to call a web site via cli (4 / 84)

Command - Port and Vuln scans w/ Netcat (3 / 13)

command - rekal memory analysis start-up (5 / 24)

Command - rpcclient sub-cmd displays SMB host OS version (2 / 164)

Command - Samba RPC client connection to Win Host (2 / 149)

command - searches for the case-insensitive string that follows in the target file (3 / 80)

Command - see page for code samples (4 / 172)

Index - Merged All-Terms (SANS 504-B)

Command - See Script on page (2 / 145)

command - sets a service start-up to disabled (2 / 102)

command - show PID, EXE, and DLLs in use (2 / 101)

Command - Shows Exe and associated DLLs of a process (1 / 66)

command - shows who has session on win host (2 / 150)

Command - SMB est a connection as current user (2 / 143)

Command - SMB Null User Session connection (2 / 143)

command - sqli to test for suseptibility (4 / 130)

command - starts msfconsole without the banner (3 / 180)

Command - state service (2 / 131)

Command - Stops Nessus Service (2 / 140)

Command - Sudo as Super User Root (1 / 154)

Command - Terminates outbound SMB share connection (2 / 150)

Command - Usage / purpose to show portstate reason (2 / 107)

Command - Used post net use to show all established host shares (2 / 144)

command - used to call a website via cli (4 / 84)

Command - used to display details of long files more managably (1 / 225)

Command - View file shares (1 / 65)

Command - View open Sessions (1 / 65)

Command - View the local host ARP cache for signs of session hijacking (3 / 75)

Command - Windows add user via cli and prompt to set pswd now (2 / 158)

Command - Windows cli for deleting a scheduled task (1 / 86)

Command - Windows cli for discovering schedule tasks (1 / 86)

Command - Windows CLI to set state of Win FW to off (1 / 91)

command - Windows dispalys ARP cache contents for signs of session hijack (3 / 75)

Command - Windows displays all local grp mbrs from CLI (1 / 71)

Command - Windows Displays all users from the cli (1 / 71)

command - Windows est interactive shell on remote host (3 / 15)

Command - Windows get system inventory using wmic cli (1 / 137)

Index - Merged All-Terms (SANS 504-B)

Command - Windows GUI Event log query of security events (1 / 188)

Command - Windows scheduled task cli (1 / 73)

Command - Windows scheduled tasks via CLI (1 / 73)

Command - Windows Services (1 / 68)

Command - Windows show service details (1 / 68)

Command - Windows stops a running service / listener (2 / 102)

Command - windows syntax for running tasks as an alternate user ID (1 / 89)

Command Injection Defense (4 / 92)

Command Injection General (4 / 89)

Command-line Invocation (Rekall DLLlist Output) (5 / 27)

Commands Listing (Netcat Switches) (3 / 10)

Common Capabilities (Appl-Level Trojans / Backdoors) (5 / 15)

Comparison (Telnet .vs Netcat) (3 / 14)

Connection Data (Beaconing Detection - Netflow) (1 / 135)

Containment (Definition of) (1 / 97)

Containment (Short-term 3 Sub-phases) (1 / 99)

Containment (Incident Categorization) (1 / 101)

Containment (Analysis w/o Alerting Intruder) (1 / 105)

Containment (Short-term Actions) (1 / 106)

Containment (Forensics Images) (1 / 109)

Containment (Imaging - Disk Dup) (1 / 110)

Containment (Long-Term General overview) (1 / 112)

Counting Processes in Windows (4 / 172)

Country Specific Laws (1 / 183)

Course Roadmap (504 Overall High Level) (1 / 9)

Covering Tracks (Hiding Files - Linux) (5 / 86)

Covering Tracks (Hiding Directories - Linux) (5 / 87)

Covering Tracks (Editing Log Files *Nix) (5 / 89)

Covering Tracks (Nix Shell History) (5 / 90)

Index - Merged All-Terms (SANS 504-B)

Covering Tracks (Auditing NIX Log Locations) (5 / 93)

Covering Tracks (Nix log editing) (5 / 94)

Covering Tracks (NTFS Alt Data Streams / ADS) (5 / 109)

Covering Tracks (Findingd ADS) (5 / 110)

Covering Tracks (Editing Windows Logs) (5 / 118)

Covering Tracks (Editing Windows logs / Physical Access) (5 / 119)

Covering Tracks (Editing Logs w/ Metasploit) (5 / 120)

Covering Tracks (Defense - Protecting logs) (5 / 121)

Covering Tracks (Defense - hashing logs for integrity) (5 / 122)

Covering Tracks (Tunneling - General overview) (5 / 124)

Covering Tracks (Reverse HTTP Shells) (5 / 126)

Covering Tracks (ICMP Tunneling) (5 / 128)

Covering Tracks (TCP/IP Header Tunneling) (5 / 131)

Covering Tracks (Covert_TCP Overview) (5 / 132)

Covering Tracks (Covert_TCP Modes) (5 / 133)

Covering Tracks (Covert_TCP Bounce Server) (5 / 134)

Covering Tracks (Covert_TCP Other Fields) (5 / 135)

Covering Tracks (General Types of Channels) (5 / 136)

Covering Tracks (Gcat via Gmail) (5 / 137)

Covering Tracks (Defense) (5 / 138)

Covering Tracks (Encrypted Covert Channels) (5 / 140)

Covering Tracks (VSAgent - General) (5 / 141)

Covering Tracks (Stego General) (5 / 151)

Covering Tracks (Hydan - General) (5 / 154)

Covering Tracks (Stego Detection) (5 / 158)

Covering Tracks (Stego Defense) (5 / 159)

Covert Channel Tools - Other (5 / 136)

Covert Channels - Encrypted Channels (5 / 140)

Covert Channels - Gcat (Gmail) (5 / 137)

Covert Channels - VSAgent - General (5 / 141)

Covert_TCP (General) (5 / 131)

Covert_TCP - Bounce Mode (5 / 134)

Covert_TCP - Client / Server (5 / 132)

Covert_TCP - Transmission (1 char @ time) (5 / 133)

CoWPAtty (2 / 65)

cpuhog (4 / 148)

Cracking Benchmarks (4 / 18)

Cracking Modes (4 / 38)

Cram Input Overview (3 / 108)

Creation Options (3 / 104)

Crime (3 / 62)

crontab (1 / 257)

Cryptcat (3 / 7)

Ctrl + z (3 / 122)

curl (4 / 84)

CyberCPR (1 / 104)

Data Sentinel (lonx) (5 / 82)

Decesion - Secrecy .vs Law Enforcement (1 / 22)

Declariation (1 / 102)

Default Live-Host Scan protocols Use (2 / 82)

Defense (BGP Hijacking) (3 / 5)

Defense (DDOS) (4 / 164)

Defense - Stego (5 / 159)

Defense - User Input Sanitization (3 / 129)

Defense - Wb Proxies (1 / 170)

Defense (DNS Recon) (2 / 27)

Defense (Website Info Disclosure) (2 / 33)

Defense (War Dialing) (2 / 57)

Index - Merged All-Terms (SANS 504-B)

Defense (Wifi) (2 / 72)

Defense (Network Mapping) (2 / 85)

Defense (Port Scanning) (2 / 100)

Defense (IDS/IPS Evasion) (2 / 121)

Defense (Vulnerability Scanning) (2 / 129)

Defense (SMB Sessions) (2 / 151)

Defense (Session Hijack) (3 / 74)

Defense (DNS Cache Poisoning) (3 / 93)

Defense (Buffer Overflow) (3 / 126)

Defense (LANMAN Cracking) (4 / 31)

Defense (Pass-the-Hash) (4 / 53)

Defense (Worms & Bots) (4 / 75)

Defense (VM Attacks) (4 / 80)

Defense (System Logs) (5 / 121)

Defense - Covert Channels (5 / 138)

Defense - File Integrity Checks (5 / 82)

Defense - hashes of key files (5 / 60)

Defense - Kernel-Mode (5 / 79)

Defense - Log Cryptographic Integrity Checks (5 / 122)

Defense - Network Intel / Forensics (5 / 83)

Defense - Removing Search Results (2 / 44)

Defense - Robots.txt Honeypot directory triggers (2 / 44)

Defense - Software Spoofing (2 / 13)

Defense (Whois Recon) (2 / 22)

Defining Assets (1 / 180)

Incident (General) (1 / 11)

Event (General) (1 / 12)

Espionage (General) (1 / 158)

Unauthorized Use (General) (1 / 164)

Insider Threat (General) (1 / 172)

Intellectual Property (General) (1 / 179)

VMWare (General) (1 / 194)

War Dialer (General) (2 / 53)

Trojans and Backdoors (General) (5 / 6)

Scareware (General) (5 / 16)

Rootkit (General) (5 / 47)

DEP (3 / 127)

Detecting Stego Tool Usage (5 / 158)

df (1 / 261)

Dictionary Attacks (4 / 11)

Differences on Windows vs Linux for SAM Results (--format=nt) (4 / 48)

Dig @dns_svr target.tld -t AXFR (2 / 24)

Diggity (2 / 43)

dir /r /s c:\tmp (5 / 115)

Disaster Recovery (1 / 10)

Distribution (4 / 68)

DLL Injection / Hooking - Debug Right Requirement (5 / 54)

DLL Injection and API Hooking - General (5 / 54)

DLLlist pid - General (5 / 27)

DNS (IR Artifacts) (1 / 133)

DNS (Recon Defenses) (2 / 27)

DNS (General) (3 / 87)

DNS (Attacks) (3 / 88)

DNS (Cache Poisoning) (3 / 90)

DNS (Defenses) (3 / 93)

DNS (Split-Split DNS) (3 / 94)

DNS (DNSSEC) (3 / 95)

DNS (Amplification Attacks) (4 / 150)

DNS (Enhanced DNS / EDNS) (4 / 151)

DNS (Reflected Attacks) (4 / 159)

DNS Local Cache - Linux (3 / 87)

DNS Transfer (2 / 25)

Dnscat (3 / 7)

DNSCat2 (5 / 136)

DNSSEC (3 / 95)

dnsstuff.com (2 / 50)

DOS - Linux resource exhaustion technique (4 / 148)

DOS / DDOS (Categories) (4 / 146)

DOS / DDOS (Pulsing Zombie) (4 / 160)

DOS / DDOS (HTTP / SYN Flooding) (4 / 161)

DOS / DDOS (Defenses) (4 / 164)

Driftnet (3 / 53)

droidsheep (3 / 63)

Dsniff (General) (3 / 43)

Dsniff (Components) (3 / 44)

Dsniff (MITM) (3 / 54)

Dsniff (DNSSpoof) (3 / 55)

Dsniff (WebMITM) (3 / 57)

Dsniff (SSHMITM) (3 / 60)

Dump - Crack - Use (4 / 51)

Easy-Creds (2 / 67)

ECTF (1 / 25)

Editing Log Files - Linux (5 / 89)

Editing Log Files - Windows (Meterpreter) (5 / 120)

Editing Log Files - Windows (Physical Access Methods) (5 / 119)

Editing Logs - Windows Temp Event log files (5 / 118)

Editing Unix Logs (5 / 94)

Index - Merged All-Terms (SANS 504-B)

Editing Windows Logs - General (5 / 118)

EIP (3 / 100)

Electronic Crimes Task Force (1 / 25)

Emergency Communications Plan (1 / 33)

Enterprise IR IR Ingress/Egress Monitoring) (1 / 132)

Enterprise IR (DNS Monitoring) (1 / 133)

Enterprise IR (Web Proxy Monitoring) (1 / 134)

Enterprise IR (Netflow) (1 / 135)

Enterprise IR (SCCM - Detect Unpatched software) (1 / 138)

Enterprise IR (Powershell) (1 / 139)

Enum (2 / 144)

Enum Acct Details (2 / 166)

Enumerating Admin Groups (2 / 165)

Enumerating Server / Grp Mbrs (2 / 164)

Eradication (IR Step) (1 / 116)

Eradication (Restoring from BU) (1 / 117)

Eradication (Vuln Scan b4 RTP) (1 / 120)

Escape Techniques (4 / 78)

Espionage (General) (1 / 158)

Espionage (Determin Likely Targets) (1 / 159)

Espionage (Identifiy Perps) (1 / 160)

Espionage (Evidence Sources) (1 / 161)

etc/network/interfaces (1 / 234)

Ettercap (3 / 67)

Ettercap (3 / 71)

Evading IDS/IPS (2 / 110)

Event (1 / 12)

eventquery.vbs (1 / 74)

eventvwr.msc (1 / 74)

Evidence - Email (1 / 165)

Evilcore (5 / 7)

Evt2sys (5 / 121)

Exe32pack (5 / 19)

exploit (3 / 178)

exploit-db.com (1 / 153)

Extreme Hiding (5 / 74)

EyeWitness (2 / 98)

Fastdump (5 / 22)

Fast-Flux Explained (4 / 71)

Feature Set (4 / 24)

Fiddler (4 / 138)

Fields and sizes listing (2 / 91)

Fields and sizing (2 / 92)

fields within file (4 / 36)

fields within file (4 / 37)

File - hashed and salted password for each user (1 / 217)

File - Linux contains the users id, shells, and encr algo types used (1 / 217)

File - Location of linux network configuration settings (1 / 234)

File Types of interest (2 / 40)

filesnarf (3 / 51)

find (1 / 232)

Find Large Files (1 / 72)

Finding Hidden Streams (ADS) (5 / 110)

Firesheep (3 / 63)

Firmware (5 / 7)

FOCA (2 / 41)

Fontanini Rootkit (5 / 52)

For Profit Attacking (2 / 11)

For security Testing (4 / 14)

Forkbomb (4 / 148)

Format String Attacks (General) (3 / 140)

Format String Attacks (Common Errors) (3 / 141)

Format String Attacks (Defined Variables) (3 / 142)

Format String Attacks (Memory Manipulation) (3 / 149)

Format String Attacks (Seperating Code & Data) (3 / 154)

Format String Attacks (Defenses) (3 / 164)

Fragroute (2 / 120)

FU (5 / 7)

FU (5 / 69)

Function Overview (3 / 105)

FUto (5 / 7)

Gcat (5 / 137)

getuid (3 / 181)

Gnu Netcat (2 / 7)

Goal of (1 / 97)

Goals (1 / 116)

Google Dork Directives (2 / 37)

Google Rapid Response (1 / 39)

Goolge Maps to Recon Physical Sites (2 / 36)

Gratuitous overview (3 / 47)

grep -i (3 / 80)

GRR (1 / 39)

Hacker Defender (5 / 7)

Handlers List (1 / 15)

Handling Practices (1 / 173)

Hash Collisions (3 / 62)

hashdump (3 / 184)

hashdump .vs run hashdump (3 / 184)

Heap Definition (3 / 123)

Hidden File Directories - Unix / Linux (5 / 87)

Hiding Components (5 / 56)

Hiding Files - Unix / Linux (5 / 86)

Hiding Files - Windows (Alternate Data Streams // ADS) (5 / 109)

High Orbit Ion Cannon (HIOC) (4 / 163)

High Technology Crime Investigation Association (1 / 25)

history -c (1 / 211)

History of notable worms (4 / 56)

How they work (4 / 22)

How to avoid (3 / 61)

HTCIA (1 / 25)

Hybrid Attacks (4 / 13)

Hydan (5 / 152)

IANA (1 / 56)

ICMP Each Request Overview (2 / 82)

ICMP Tunneling - Ptnnel General Overview (5 / 128)

ICMP Tunnels - General (5 / 128)

id (1 / 215)

Identification (Monitoring for IR Events) (1 / 49)

Identification (OOB Comms) (1 / 52)

Identification (IR Detection Locations) (1 / 53)

Identification (IR App Level Locations) (1 / 58)

Identification (Notification by 3rd Party) (1 / 59)

Identification (IR Sheatsheets) (1 / 62)

Identification (Initial Assessment) (1 / 93)

Identification (Espionage) (1 / 160)

Identification (Insider Threat) (1 / 174)

IDP / IPS Evasion (2 / 121)

ifconfig eth0 IP/CIRD (3 / 173)

Import Attackers Cert (3 / 63)

Inception (4 / 29)

Incident (General) (1 / 11)

Incident (Containment) (1 / 102)

Incident Charactorization (1 / 101)

Incident Communications (1 / 52)

Incident Handling Guide (1 / 14)

Incident Handling Phases (1 / 17)

Incident Handling Plan (1 / 10)

Incident Handling Steps (1 / 14)

Incident Response (1 / 40)

Incident Response - Helpdesk Staff (1 / 38)

Incident Response Pre-authorized Actions (1 / 35)

Incident Response Team Encrypted Email Exchange (1 / 25)

Incident Response Team Organization (1 / 32)

Identification (1 / 50)

info exploitpath/exploit (3 / 175)

Infor Management (1 / 102)

Infragard (1 / 25)

Ingress / Egress (1 / 132)

Initial Analysis Steps (1 / 105)

Insider Threat (General) (1 / 172)

Insider Threat (Warning Banners) (1 / 173)

Insider Threat (Activity Identification) (1 / 174)

Insider Threat (Monitoring User) (1 / 175)

InSSIDER (2 / 61)

Intellectual Property (General) (1 / 179)

Index - Merged All-Terms (SANS 504-B)

Intellectual Property (Crown Jewels) (1 / 180)

Intellectual Property (Preparing a Defense) (1 / 181)

Internet Storm Center (1 / 15)

Invalid Checksum Bypass (2 / 116)

Invisible Secrets (5 / 152)

IP Fragmentation (Evading IDS/IPS) (2 / 110)

IP Fragmentation (The Frag Flag) (2 / 112)

IP Fragmentation (Frag Types) (2 / 114)

IP Fragmentation (Tiny Frag) (2 / 115)

IP Fragmentation (Invalid Checksum Frag) (2 / 116)

IP Fragmentation (Overlap Frag) (2 / 117)

IP Fragmentation (Frag Reassembly Challenges) (2 / 118)

IP Header (2 / 81)

ipconfig /displaydns (3 / 75)

iptables -F (3 / 167)

IR Handling Preparation (1 / 181)

ISP Coordination (1 / 106)

ISR-Evilgrade (2 / 12)

Issue Handling (1 / 22)

John the Ripper (General) (4 / 35)

John the Ripper (Cracking Modes) (4 / 38)

John the Ripper (Supported Encrypt Methods) (4 / 39)

John the Ripper (Win ver LANMAN Reassembly Switch) (4 / 48)

john.pot cracked passwd file store (4 / 39)

Jsteg (5 / 152)

Jump Bag Contents (1 / 40)

Kansa (1 / 141)

Karmetasploit (2 / 69)

Kbeast (5 / 7)

Kernel-Mode Root Kits (5 / 7)

Kernel File Alteration - General (5 / 70)

Kernel-Mode - 5 methods for Kernel Manipulation (5 / 67)

Kernel-Mode - Definition / Description (5 / 64)

Kernel-Mode - Linux Loadable Kernel Modules (LKM) (5 / 68)

Kernel-Mode - System Call Table Modification (5 / 66)

Kernel-Mode - Virtualization of System (5 / 71)

Kernel-Mode Linux Alter Kernel in Memory (5 / 69)

Kernel-Mode Rootkit - Windows Kernal Memory Map (5 / 69)

Kernel-Mode Rootkit Linux map of Kernel Memory (5 / 69)

Kernel-Mode Windows (Vista Mandatory Driver Signing) (5 / 68)

Kernel-Mode Windows Device Drivers (5 / 68)

Key Points (1 / 49)

kill PID (2 / 104)

KIS (5 / 7)

Kismet (2 / 63)

Kiwi Syslog (5 / 121)

Konboot (4 / 29)

Kon-boot (5 / 7)

LADS (5 / 110)

LANMAN Hashs (4 / 17)

lastlog (5 / 93)

LE - Acting as an Agency for (1 / 24)

LE - Exchanging PGP Keys (1 / 25)

LE - Interactions prior to an Incident (1 / 25)

LE - Optional Reasons to Notify (1 / 23)

LE - pre-incident Interaction (1 / 25)

LE - Preserving Files (1 / 96)

LE - Reason not to Notify (1 / 24)

LE - When you MUST notify (1 / 23)

Legal (1 / 183)

length .vs complexity (4 / 33)

less (1 / 225)

Leveraging a found modem (2 / 56)

LIFO (3 / 102)

Linkcat (3 / 7)

Linux Commands (5 / 102)

Listener = Attacker Host (3 / 30)

Listener Port (1 / 56)

LM Padding - AAD3B435B51404EE (null value for that portion) (4 / 28)

Logging (1 / 161)

Logs / Linux - Currently logged on; past; failed; logon history files (5 / 93)

Long Term Goals (1 / 112)

look-up sources (2 / 19)

Low Orbin Ion Cannon (IOC) (4 / 162)

Lrk6 (5 / 7)

ls .vs Echo for detection (5 / 59)

Isuf -i (1 / 56)

Isuf -i (1 / 238)

Isuf -p PID (2 / 103)

lusrmgr.msc (1 / 71)

Macof (3 / 48)

mailsnarf (3 / 51)

Maltego (General) (2 / 46)

Maltego (Transforms) (2 / 47)

Maltego (Defenses) (2 / 48)

Malware Layer (5 / 7)

Malware Layers (5 / 7)

Malware Microcode (5 / 7)

Management Support (1 / 29)

Masscan (2 / 97)

Maux (5 / 7)

md5deep (1 / 109)

md5sum (1 / 109)

Mdd (5 / 22)

Mebroim BIOS Rootkit (5 / 7)

Memory Analysis (5 / 22)

MemoryDD.Bat (5 / 22)

Memoryze (1 / 109)

Memoryze (5 / 22)

Metamorphic (4 / 66)

Metasploit (3 / 115)

Metasploit (3 / 119)

methods of attack (4 / 10)

MitM SSH v1 Overview (3 / 60)

Modules - General (5 / 23)

Monitoring (1 / 124)

Monitoring (1 / 175)

Morris Worm (4 / 55)

Most powerful tools in suite are.. (3 / 54)

MP3Stego (5 / 152)

msf | search (1 / 155)

msfconsole (3 / 184)

msfconsole -q (3 / 180)

msfelfscan (3 / 106)

Msgsnarf (3 / 51)

mspescan (3 / 106)

Msyslog (5 / 122)

Multi-exploit (4 / 58)

Multi-Platform (4 / 59)

NASL Scripting Language (2 / 128)

nbtstat - S (1 / 65)

nc -l -p port -e /bin/sh (3 / 15)

nc -l -p port -e cmd.exe (3 / 15)

nc -l -p portnum < filename (3 / 12)

nc -v -w3 -z IP startport-endport (3 / 13)

Ncat (3 / 7)

ncpa.cpl (2 / 156)

Nessus (General) (2 / 125)

Nessus (General) (2 / 127)

Nessus (Plug-ins) (2 / 128)

Nessus - https://localhost:8834 & (2 / 131)

Nessus - sudo systemctl start nessusd (2 / 131)

Nessus - sudo systemctl stop nessusd (2 / 140)

net localgroup (1 / 71)

net session (1 / 65)

net session (2 / 150)

net session \\IP /del (2 / 150)

net start (1 / 68)

net use * /del (2 / 150)

net use \\IP (2 / 143)

net use \\IP "" /u:"" (2 / 143)

net use \\IP /del (2 / 150)

net use \\IP\SHARE\ password /u: username (2 / 143)

net user /domain >> users.txt (2 / 145)

net user username * /add (2 / 158)

net users (1 / 71)

net view (1 / 65)

net view \\IP (2 / 144)

Netcat (General) (3 / 7)

Netcat (Client Mode) (3 / 8)

netcat (Switches) (3 / 10)

Netcat (Use Cases) (3 / 11)

Netcat (Reverse Shell Shoveling) (3 / 30)

Netcat .vs. Telnet (3 / 14)

netcat -l -p 2222 (1 / 80)

Netcat Relays (3 / 19)

netsh advfirewall (1 / 91)

netstat -naob (1 / 55)

netstat -nap (1 / 238)

netstat -b (1 / 66)

Netstat Module (5 / 25)

netstat -na (1 / 66)

netstat -nao (1 / 66)

netstat -naob (2 / 101)

netstat -nap (2 / 103)

NetStumbler (2 / 61)

Network Mapping (2 / 82)

Network Mapping (2 / 85)

network-tools.com (2 / 50)

Niksun (3 / 53)

NIST (1 / 14)

Nmap (General) (2 / 80)

Nmap (No Ping Net Mapping) (2 / 82)

Nmap (Scan Types) (2 / 93)

Nmap (--reason Flag) (2 / 107)

Nmap -A IP (2 / 108)

Nmap --reason IP (2 / 107)

nohup ./listener.sh & (3 / 16)

NOPs (3 / 113)

Note Taking (1 / 27)

NT Hash general info (4 / 19)

NTLDR (5 / 70)

Obtaining (2 / 8)

Ollydbg (5 / 20)

Omnipeek (2 / 64)

Online tools / search engines (3 / 107)

OpenPuff (5 / 153)

OpenStego (5 / 153)

Original (SunOS 4.1x) & Platforms (5 / 48)

OS Fingerprinting (2 / 95)

OS supported (1 / 63)

OSI Layer Utiliation (3 / 45)

OSINT (Web General) (2 / 29)

OSINT (Web Defenses) (2 / 33)

OSINT (Search Engining Dorking) (2 / 35)

OSINT (Google Maps for Phy Recon) (2 / 36)

OSINT (Google Dorking) (2 / 37)

OSINT (using Cache and Wayback Machine) (2 / 39)

OSINT (Search Engine - Finding Files by type) (2 / 40)

OSINT (Web Defenses) (2 / 44)

OSSEC (5 / 82)

Other TCP Header Fields for Covert Transmission (5 / 135)

Out-of-Band Communications (1 / 52)

Overlap Attack (2 / 117)

Overview - bypasses ext svc scans (2 / 94)

Overview - Spoofing DNS Query (3 / 55)

Overview - Wireshark (3 / 42)

Overview of combined toolsets (4 / 23)

Overview of function (3 / 87)

Overview of Tool / Variants (3 / 7)

OWASP Overview (4 / 82)

Pass-the-Hash Attack (General Overview) (4 / 50)

Pass-the-Hash Attack (Tools for) (4 / 52)

Pass-the-Hash Attack (Defenses) (4 / 53)

passwd (1 / 214)

Password Cracking (Pswd Spraying) (4 / 7)

Password Cracking (Pswd Guessing) (4 / 6)

Password Cracking (Cracking Methods) (4 / 10)

Password Cracking (Dictionary Attacks) (4 / 11)

Password Cracking (Brute Force) (4 / 12)

Password Cracking (Hybrid) (4 / 13)

Password Cracking (for Purposes of Good) (4 / 14)

Password Cracking (Using CAIN) (4 / 25)

Password Cracking (Using Cain Overview) (4 / 28)

Password Cracking (Defenses) (4 / 31)

Password Cracking (Enforcing Complexity) (4 / 33)

Password Cracking (Pass-the-Hash) (4 / 51)

Password Spraying overview (3 / 7)

Payloads (3 / 119)

Peer Notification Policy (1 / 26)

People (1 / 20)

Permissions (2 / 8)

Index - Merged All-Terms (SANS 504-B)

Phase - Short Term Goals (1 / 106)

Phases (1 / 99)

Phrack 66 (5 / 7)

PICERL (1 / 14)

Pluggable Authentication Module (PAM) (4 / 41)

Poison Ivy (5 / 7)

Poison Ivy (5 / 14)

Policy (1 / 21)

Polymorphic (4 / 63)

Port Scan (NMAP Types) (2 / 93)

Port Scan (Defenses) (2 / 100)

Port Scanner (2 / 88)

Post Removal Steps (1 / 120)

Powerbleed (3 / 61)

Powershell Empire (2 / 147)

Preparation (Warning Banner) (1 / 21)

Preparation (When not to Notify LE) (1 / 24)

Preparation (Interfacing w/ LE) (1 / 25)

Preparation (Peer Nitification) (1 / 26)

Preparation (Notes and Documentatin) (1 / 27)

Preparation (Informing Mgt) (1 / 29)

Preparation (Building the IR Team) (1 / 30)

Preparation (IR Checklists) (1 / 31)

Preparation (IR Team Org) (1 / 32)

Preparation (IR Team OOB Comms) (1 / 33)

Preparation (Obtaining Systems Access) (1 / 35)

Preparation (Reporting and Opertions Space) (1 / 36)

Preparation (IR Team Training) (1 / 37)

Preparation (Relationships w/ external entities) (1 / 38)

Preparation (Personnel) (1 / 20)

Primary Incident Responder (1 / 50)

Problem Hex Charactors (5 / 146)

Process Explorer (1 / 76)

Process Monitor (1 / 76)

Protocol Analyzer (General) (3 / 41)

Protocol Analyzer (Wireshark) (3 / 42)

Protocol Analyzer (Using the OSI Model) (3 / 45)

Protocol Parsers (3 / 135)

ps (1 / 125)

PSLIST - General (5 / 26)

Ptunnel (5 / 128)

Public - When you MAY need to notify (1 / 23)

Pulsing Zombies (4 / 160)

PushPin (2 / 31)

pwdump (4 / 29)

py2exe (5 / 148)

pyInjector (5 / 148)

pyinstaller (5 / 148)

Qualys (2 / 124)

Query ID attacks (3 / 88)

QUICK (5 / 136)

Quote (2 / 14)

Rainbow Table (4 / 22)

Rainbow Tables (4 / 22)

Reassembly Handling (2 / 118)

Reconnaissance (2 / 16)

Recovery (Validate Ready for RTP) (1 / 122)

Recovery (When to Restore to Ops) (1 / 123)

Recovery (Post RTP Monitoring) (1 / 124)

Recovery (Monitoring new exploit attempts) (1 / 125)

Reflected Attack - Overview (4 / 159)

reg query (1 / 69)

regedit (1 / 84)

Registration Required Information (2 / 18)

Registry Keys Targeted Most Often (1 / 69)

rekal -f /file-location/memdumpfile.dd (5 / 24)

Rekall (General Overview) (5 / 22)

Rekall (Modules) (5 / 23)

Rekall (Netstat) (5 / 25)

Rekall (PSList) (5 / 26)

Rekall (DllList) (5 / 27)

Removing ADS (5 / 109)

Remux (2 / 99)

Report (Final from Lessons Learned) (1 / 127)

Return Pointer (3 / 102)

Return to Normal Ops (1 / 123)

Reverse HTTP Shells - General (5 / 126)

RIR - Regional Sources (2 / 20)

Rise of Hacktivism (2 / 10)

Risky Functions for exploit (3 / 106)

root .vs Usr privledges (2 / 107)

Rootcheck - OSSEC (5 / 80)

Rootkit (First Detected) (5 / 48)

Rootkit (DLL Inject / API Hooking) (5 / 54)

Rootkit (Hiding Files) (5 / 56)

Rootkit (Defenses) (5 / 59)

Rootkit (Defenses - Hashes) (5 / 60)

Index - Merged All-Terms (SANS 504-B)

Rootkit (System Call Table) (5 / 64)

Rootkit (Kernel Mode Hiding Files) (5 / 66)

Rootkit (5 Kernal Mode Types) (5 / 67)

Rootkit (Kernel Mode LKM) (5 / 68)

Rootkit (Kernel Mode Memory Altering) (5 / 69)

Rootkit (Kernel Mode HD Altering) (5 / 70)

Rootkit (Kernel Mode VM host) (5 / 71)

Rootkit (Extreme Hiding) (5 / 74)

Rootkit (Defenses - Hardwning Host) (5 / 79)

Rootkit (Defenses File Integrity Chk) (5 / 82)

Rootkit (C2 Comms Monitoring) (5 / 83)

Rootkit Detective (5 / 81)

Rootkit Hunter (5 / 80)

Rootkit Kernel-Mode Windows Protection (5 / 70)

Rootkit Revealer (PSTOOLS) (5 / 81)

Rootkit (Definition) (5 / 47)

Rootkit (User-Mode Root Components) (5 / 50)

Rootkit (User-Mode Rooted Processes) (5 / 51)

RootKit (Debug Mode Requirement) (5 / 54)

Rooty (5 / 73)

route add pivotIP 255.255.255.255 sessionID (3 / 122)

rpcclient (2 / 149)

rpcclient -U username IP (2 / 149)

RTIR (1 / 103)

runas (1 / 89)

Salting Hashes (4 / 20)

SANS Investigative Forensics Toolkit (SIFT) (1 / 43)

sc config servicename start= disabled (2 / 102)

sc query (1 / 68)

sc query (2 / 102)

sc stop servicename (2 / 102)

Scan Types / Use Cases (2 / 93)

Scareware (5 / 16)

Scheduled Tasks (1 / 73)

schtasks (1 / 73)

schtasks /delete (1 / 86)

schtasks | more (1 / 86)

Scripting - Windows CLI For Loop (1 / 72)

SCTP (5 / 136)

Search Engine usage (2 / 35)

search type:exploit exploitinfo_or_cve# (3 / 175)

secpol.msc (1 / 88)

Security Onion (5 / 83)

Sending App Appropriate Data Caveats (2 / 93)

Services (2 / 104)

services.msc (1 / 68)

services.msc (2 / 157)

Session Hijacking (General) (3 / 67)

Session Hijacking (ACK Storms) (3 / 69)

Session Hijacking (ARP Cache Poisoning) (3 / 70)

Session Hijacking (Defenses) (3 / 74)

Session Hijacking (Flooding CAM Tbl) (3 / 79)

Session State - General (4 / 135)

sessions -l (3 / 181)

Sexually Explicit Content (1 / 169)

shell (3 / 185)

Shell Code Inersion (3 / 111)

Shell History (5 / 90)

shell redirect < & > symbol usage (3 / 10)

shodan (2 / 50)

Shoveling Shells (3 / 17)

SilentEye (5 / 153)

Six Steps (1 / 17)

SL4NT (5 / 121)

S-Mail (5 / 152)

Smashed Stack (3 / 103)

SMB (Defense - Windows Registry Keys) (2 / 151)

SMB (Enum Servers and Groups) (2 / 164)

SMB (Enum Admin Grp / Mbrs) (2 / 165)

SMB (Enum Admin Acct Details) (2 / 166)

SMB (Layer 7 Protocol) (2 / 142)

SMB Password Spraying (2 / 145)

smbclient (2 / 148)

smbclient -L IP -U username -p 445 (2 / 148)

Snare Agent / Log Server (5 / 121)

Socat (3 / 7)

Split-Split (3 / 94)

Spoofing SSL / SSH Targets (3 / 57)

SQLi - Defense (4 / 101)

SQLi - examples (4 / 96)

SQLi - Extracting Database Structure Example (4 / 100)

SQLi - Testing tools (4 / 95)

SQLi General (4 / 94)

srvinfo (2 / 164)

SSL Certificate Warning (Dodging Client Warnings) (3 / 61)

SSL Certificate Warning (Hash Collisions) (3 / 62)

SSL Certificate Warning (Compromising Client Browsers) (3 / 63)

SSLStrip (3 / 64)

Stack Definition (3 / 123)

Stash (5 / 152)

Steganography - General (5 / 151)

Steganography Tools (5 / 152)

StegExpose (5 / 158)

Stego - Detecting Methods (5 / 158)

Stego - Hydan | General Info (5 / 154)

Steps for identifying Reoccurring Intrusions (1 / 125)

su - (1 / 154)

Sub7 (5 / 7)

Sub-routing Pre-Amble (3 / 101)

Subterfuge (3 / 73)

Subvert (5 / 71)

sudo su - (1 / 215)

Suite Component Listing (3 / 44)

Super User Control Kit (SUCKit) (5 / 69)

SuperUser Control Kit (5 / 7)

supporting Tools for technique (4 / 52)

SYN and HTTP Flooding (4 / 161)

System Build Checklist (1 / 31)

System Hardening Template (1 / 76)

System Memory Map (5 / 69)

Tamperdata (4 / 136)

tar xvf (1 / 240)

Targeting (1 / 159)

tasklist (1 / 67)

tasklist /svc (1 / 68)

TCP Header (2 / 91)

Index - Merged All-Terms (SANS 504-B)

TCP/IP Header Hiding (5 / 131)

tcpkill (3 / 50)

tcpnice (3 / 50)

TCPView (1 / 76)

Team Training (1 / 37)

Term - Linux Bad logon attempts /var/log/btmp (5 / 93)

Term - Linux currently logged on users /var/run/utmp (5 / 93)

Term - Linux Logon History (last logon) /var/log/lastlog (5 / 93)

Term - Linux past logged on users /var/log/wtmp (5 / 93)

Terms - Linux Multiple (whoami, uname, tar,mv,wget, etc..) (5 / 102)

THChydra (4 / 8)

The Hacker Manafesto (2 / 14)

Themida (5 / 19)

Tiny Frag (2 / 115)

tool - android tool for web session hijacking (3 / 63)

Tool - Application Layer Trojan (5 / 7)

Tool - Auto Start Entry Point viewer Microsoft (1 / 69)

Tool - Autostart Point Entry (ASEP) (1 / 141)

Tool - Boor Sector Root Kit (5 / 7)

Tool - Boot Sector Root Kit (5 / 7)

Tool - Boot Sector Rootkit (5 / 7)

Tool - Browser exploitation tool, hooks victim browsers and attempt to exploit (4 / 112)

Tool - budled with nmap / spt SSL / mulit connections / NAT-bypass (3 / 7)

Tool - Cached prior versions of websites (2 / 39)

Tool - Cached version of a web site (2 / 39)

tool - captures IM msg and saves to local host (3 / 51)

Tool - captures url's from http traffic (3 / 51)

Tool - chosen plain-text exploit to crack encrypted SSL traffic (3 / 62)

Tool - cli query of a specified registry key (1 / 69)

Index - Merged All-Terms (SANS 504-B)

Tool - Coding and decoding (1 / 67)

tool - commercial / free used to fuzz website inputs (4 / 138)

tool - commercial / monitors http for jpeg files and reassembles (3 / 53)

tool - commercial / reassembles entire http session from captures traffic (3 / 53)

Tool - Converts python into exe (5 / 148)

Tool - Converts Python Scripts into Exe (5 / 148)

tool - cool boot password extraction tool (4 / 29)

Tool - Covert Ch C2 (Gmail) (5 / 137)

Tool - Covert Ch over tcp headers (5 / 131)

Tool - Covert Ch trans via DNS (5 / 136)

Tool - Covert Ch trans via multi-streaming w/ c2 (5 / 136)

Tool - Covert Channels VIEWSTATE (5 / 141)

Tool - Covert trans via multiplex UDP streams (5 / 136)

Tool - Creates MD5 hash of file (1 / 109)

Tool - Dangerous Plug-ins (2 / 127)

Tool - DDOS tool (4 / 162)

tool - DDOS tool (4 / 163)

Tool - DDOS Tool / resource exhaustion (4 / 157)

Tool - Defense (2 / 48)

Tool - Disk Duplicator (1 / 110)

tool - DOS resource exhausting simulator (4 / 148)

Tool - Encrypted Ncat (3 / 7)

Tool - establish a listener (1 / 80)

Tool - extracts pslds from hosts with encrpt boot via firewire / thunderbolt (4 / 29)

Tool - File Integrity Checker (5 / 82)

tool - firefox plugin for manipulating http request prior to returning response (4 / 136)

Tool - Firmware Rootkit (Ethernet and Video Cards) (5 / 7)

Tool - Firmware Rootkit (Motherboards and BIO) (5 / 7)

Tool - Firmware Rootkit (Vmware and Awd BIOS) (5 / 7)

Index - Merged All-Terms (SANS 504-B)

Tool - for dumping pswds from hosts (4 / 29)

Tool - Forensic Image acquisition (1 / 109)

Tool - Forensic Image Options (1 / 109)

Tool - Forensic Memort acquisition tool (1 / 109)

tool - free allows for scripting stop points to check suseptibility (4 / 138)

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

tool - Free used to assess for attack suseptibility (4 / 138)

Tool - General (5 / 11)

Tool - General (5 / 13)

Tool - General (5 / 52)

Tool - General / GUI for Nmap (2 / 80)

Tool - ICMP Tunneling Tool (via Echo / Reply packets) (5 / 128)

Tool - Incident Response (1 / 39)

Tool - Incident Response (1 / 43)

tool - injusts packets w/ sml window sizes to slow packet rates on fast conn (3 / 50)

Tool - IR Tracking Tool w/Secure OOB Chat (1 / 104)

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

Tool - Kansa (1 / 139)

Tool - Kernal-mode Rootkit (5 / 7)

Tool - Kernel-Mode File Alteration (5 / 70)

Tool - Kernel-Mode Memroy Map Alteration (5 / 69)

Tool - Kernel-Mode Rootkit encrypt C2 / VM detect / drvr bypass (5 / 76)

Tool - Kernel-Mode Rootkit Linux LKM & Drvr Spt (5 / 73)

Tool - Kernel-Mode Rootkit Memory Alteration (5 / 69)

Tool - Kernel-Mode Rootkit Virtualiztion (5 / 71)

Tool - Kernel-Mode Rootkit Virtulization of system (5 / 71)

Tool - Kernel-Mode Rootkit Windows Dev Drv Alters (5 / 77)

Tool - Launches User Mgr from CLI (1 / 71)

Tool - Linux / BSD / Win32 (unstable) - Ethernet and wlan network tool (3 / 43)

Index - Merged All-Terms (SANS 504-B)

Tool - Linux enumerates dns query results (2 / 24)

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

Tool - Linux Root Kit Type detection / Identification (5 / 80)

Tool - Linux Rootkit Detection (5 / 80)

Tool - Linux Rootkit Detection (Only Actively Maintained) (5 / 80)

Tool - Manipulate IP to MAC mapping (3 / 48)

Tool - Manipulate MAC to Phy Port Mapping (3 / 48)

Tool - md5 hash of file (1 / 109)

Tool - Memory Analysis (5 / 22)

tool - Memory Analysis (most Popular) (5 / 22)

tool - Memory Analysis (Python) (5 / 22)

Tool - Metasploit (1 / 155)

tool - Metasploit tool searches Linux binaries for buffer overflow potential (3 / 106)

tool - Metasploit tool searches Windows binaries for buffer overflow potential (3 / 106)

Tool - nslookup set type=any ls-d (2 / 25)

Tool - Overview (2 / 84)

Tool - overview (4 / 8)

Tool - Overview and options (3 / 71)

Tool - Paterva's Automated Intel gathering suite (2 / 46)

Tool - ports over DNS (3 / 7)

Tool - Real Time Incident Response (1 / 103)

tool - reassembles files, videos, and images / scales to multiple hosts (3 / 52)

Tool - relays across data ch / Spts SSL and Raw IP (3 / 7)

Tool - Requires FragRouter / hard for IPS vendors to write sigs (2 / 120)

tool - rewrites url's back to client to replace HTTPS w/ HTTP in all links (3 / 64)

Tool - Rootkit Detection / C2 Communications (5 / 83)

tool - saves email from captured pop / smtp sessions on local host (3 / 51)

tool - saves files captures from NFS to local host (3 / 51)

Tool - Scans via multiple open Proxies, Python tool, bypasses tor blocks (2 / 99)

Index - Merged All-Terms (SANS 504-B)

Tool - SCCM (1 / 138)

Tool - screenshots websites / VNC / RDP banners / trys known default creds (2 / 98)

Tool - Seaches for searches for MS Office files / extracts Metadata (2 / 41)

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

Tool - sends resets to kill tcp connects / forces new session auth (3 / 50)

Tool - Session Hijacking for terminal and VPN (3 / 67)

Tool - Session theft across networks (3 / 67)

Tool - Show Configuration (1 / 66)

Tool - Show Process list (1 / 67)

Tool - Site containing open source exploit scripts (1 / 153)

Tool - SMB Cli enums users, groups mbrs, pswd policies (2 / 144)

Tool - splits send / receive part 3-way handshake, scans 1ks host per min (2 / 97)

Tool - Spoofs Automated Software Updates (2 / 12)

Tool - spoofs caller id, MP3 of results, break into VoIP and Cell VM boxes (2 / 54)

Tool - Stego Embeds data and digital watermarks into images (5 / 153)

Tool - Stego encrypts data into Jpg, BMP, and Wav (5 / 153)

Tool - Stego hides data in win/nix exe's (5 / 152)

Tool - Stego Java-based detects in lossless img formats)Least Significant Bit) LSB (5 / 158)

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

Tool - Stego tool - Hides data in Banner Ads for websites (5 / 152)

Tool - Stego tool hides data in exe/dll files (5 / 152)

Tool - Stego tool hides data in Mpeg files (5 / 152)

Tool - Stego Tool hides data in variety of formats (5 / 152)

Tool - Stego tool hides jpeg using DCT Coefficients (5 / 152)

Tool - Suite of search tools (Google, Search, Bing, DLP,...) (2 / 43)

Tool - summary (2 / 7)

Tool - terminal and VPN session theft (3 / 67)

Tool - Transforms Overview (2 / 47)

Tool - Trojan Application-Level (5 / 14)

Tool - Unpacker (5 / 20)

Tool - User-Mode Rootkit (5 / 7)

Tool - uses malformed Heartbleed requests to extract server keys from memory (3 / 61)

Tool - Uses raw ether frames (3 / 7)

Tool - Vuln Scanner / Best for PCI Compliance scans (2 / 124)

Tool - Vuln Scanner / most popular / client-server architecture / plug-ins (2 / 125)

tool - Web Application Proxy / requires tuning to be effective (4 / 142)

Tool - Web dns probing tool (2 / 50)

Tool - Web hosted probe and OSINT results (2 / 50)

Tool - Web hosted recon scanner tools (2 / 50)

Tool - web hosted trace routing / validates route from 3rd party source (2 / 50)

Tool - web hosts tools launched from a 3rd party for recon (2 / 50)

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

Tool - web session hijacking (3 / 63)

Tool - Windows ADS Detection (5 / 110)

tool - Windows for pass the hash and pass the token (4 / 52)

Tool - Windows GUI (1 / 73)

Tool - Windows GUI for editing local security policy (1 / 88)

Tool - Windows GUI launch from cli (1 / 68)

Tool - Windows GUI registry editor (1 / 84)

Tool - Windows launch event viewer via CLI (1 / 74)

Tool - Windows Rootkit Detection (5 / 81)

Tool - Windows Rootkit Detector (5 / 81)

Tool - Windows running tasks (1 / 68)

Tool - Windows running tasks and processes (1 / 67)

Tool - Windows Syslog Integrity Checker (5 / 122)

Tool - Windows Syslog Server (5 / 121)

Tool - Windows System agent and server - commercial (5 / 121)

Tool - Windows Systemals (1 / 76)

Index - Merged All-Terms (SANS 504-B)

Tool - Windows Systemals Displays running processes (1 / 76)

Tool - Windows Systemals TCP/UDP Port Listeners (1 / 76)

Tool - Windows vbscript query log events (1 / 74)

Tool - WLAN AP spoofing / POP, HTTP, Samba, DHCP spoofing (2 / 69)

Tool - WLAN Dictionary Attacks on LEAP Authentication (2 / 64)

Tool - WLAN Discovery a/b/g nets (2 / 61)

Tool - WLAN Discovery a/b/g/n (2 / 61)

Tool - WLAN intercepts and Cracks WEP keys (2 / 64)

Tool - WLAN pre-computer dictionary cracking tool for WPA/WPA2 (2 / 65)

Tool - WLAN scanner spts a,b,g,n,Zigbee (2 / 63)

Tool - WLAN Sniffer commercial tool; formerly airopeek (2 / 64)

Tool - WLAN Spoofs AP's / SSL MITM & strip / session hijacking (2 / 67)

Tool - WLAN wep cracking tool (2 / 64)

Tool - Wrapper (5 / 19)

Tool- Kernel-Mode Rootkit Virtulization of System (5 / 71)

Traceroute (2 / 83)

traceroute.com (2 / 50)

Tribe Flood Network (TFN) / TFN2000 (4 / 157)

Tripwire (5 / 82)

Trojan Horse (5 / 6)

Trojans (5 / 9)

TTYsnoop (3 / 67)

TTYSpy (3 / 67)

Tunneling Protocols - General (5 / 124)

Types (2 / 114)

types of attackers (2 / 16)

Types of Attacks (4 / 146)

UDP Header (2 / 92)

Unauthorized Use (Definition) (1 / 164)

Index - Merged All-Terms (SANS 504-B)

Unauthorized Use (Artifacts -emails) (1 / 165)

Unauthorized Use (Artifacts -web) (1 / 168)

Unauthorized Use (Sexually Explicit Sites) (1 / 169)

Unauthorized Use (Artifacts Web Proxy) (1 / 170)

Underground Trends (2 / 9)

Unpacker (5 / 20)

unshadow pswd.txt shadow.txt > combined.txt (4 / 35)

Unusual Activities - searching for intruders (1 / 62)

Update Authentication (3 / 95)

UPX (5 / 19)

URLSnarf (3 / 51)

Use cases (3 / 11)

useradd (1 / 213)

User-Mode - Defense (5 / 59)

User-Mode - Linux Commonly Hidden / Filtered Component Outputs (5 / 51)

User-Mode - Linux Commonly Rooted Components (5 / 50)

User-Mode Root Kits (5 / 7)

utmp (5 / 93)

Validation (1 / 122)

variable Definitions (3 / 142)

Vbootkit 2.0 (5 / 7)

Vitriol (5 / 71)

VM Attacks (General) (4 / 77)

VM Attacks (VM Sandboxing Detection) (4 / 78)

VM Attacks (Defenses) (4 / 80)

vmlinuz (5 / 70)

VMWare (1 / 194)

VNC (5 / 11)

Volatility (1 / 109)

Volatility Framework (5 / 22)

VPN (1 / 26)

VSAgent (5 / 141)

Vulnerability Scanner (General) (2 / 123)

Vulnerability Scanner (Tools) (2 / 124)

Vulnerability Scanner (Defenses) (2 / 129)

w3af (4 / 138)

WAF (4 / 142)

War Dialing (Overview) (2 / 53)

War Dialing (Testing for Risk) (2 / 56)

War Dialing (Defense) (2 / 57)

War Room (1 / 36)

Warhop/Flash Spread Vector Metric (4 / 62)

Warning Banner (1 / 21)

Warning Banner (1 / 26)

WarVOX (2 / 54)

Wayback Machine (2 / 39)

Web Access (1 / 168)

Web App Attacks (OWASP Overview) (4 / 82)

Web App Attacks (Acct Harvesting) (4 / 84)

Web App Attacks (Defenses) (4 / 87)

Web App Attacks (Cmd Injection Overview) (4 / 89)

Web App Attacks (Cmd Injection Defenses) (4 / 92)

Web App Attacks (SQL Injection General) (4 / 94)

Web App Attacks (SQL Injection Overview) (4 / 95)

Web App Attacks (SQLi Mapping) (4 / 96)

Web App Attacks (SQLi Common Stmts) (4 / 100)

Web App Attacks (SQLi Defenses) (4 / 101)

Web App Attacks (XSS Overview) (4 / 104)

Web App Attacks (XSS Defenses) (4 / 116)

Web App Attacks (Session State Attacks) (4 / 135)

Web App Attacks (Tools) (4 / 138)

Web Proxies (1 / 134)

Web-Based Recon (2 / 50)

Website public info sources (2 / 29)

Webspy (3 / 53)

WEPCrack (2 / 64)

wevent qe security (1 / 188)

wget (4 / 84)

Where it occurs (1 / 53)

while [1]; do echo "Started"; nc -l -p port -e /bin/sh; done (3 / 16)

whoami (1 / 215)

Whois Lookups (Results) (2 / 18)

Whois Lookups (Methods to) (2 / 19)

Whois Lookups (RIR by Reigon) (2 / 20)

Whois Lookups (Defenses) (2 / 22)

Win32dd (5 / 22)

Windows - Registry (1 / 69)

Windows - suspect locations (1 / 70)

Windows Cheat Sheets (1 / 63)

Windows Credential Editor (WCE) (4 / 52)

Windows Firewall Settings (1 / 66)

Windows Management Instruction CLI (1 / 67)

Windows Versions (2 / 164)

Winpmem (5 / 22)

WinVNC (5 / 13)

WLAN War Driving (General) (2 / 60)

WLAN War Driving (Tools) (2 / 61)

WLAN War Driving (Defenses) (2 / 72)

wmic (1 / 67)

wmic - startup (1 / 70)

wmic /node (1 / 137)

wmic pid delete (2 / 102)

Worm (General) (4 / 55)

Worm (History of relivant ones) (4 / 56)

Worm (Multi-Exploit) (4 / 58)

Worm (Mulit-Platform) (4 / 59)

Worm (0-Day) (4 / 60)

Worm (Warhol/Flash Spread Technique) (4 / 62)

Worm (Polymorphic) (4 / 63)

Worm (Metaporhic) (4 / 66)

Wrappers (5 / 18)

wtmp (5 / 93)

Xplico (3 / 52)

XXS - Defense (4 / 116)

XXS - General (4 / 104)

Yoda (5 / 19)

ZAP (4 / 139)

ZenMap (2 / 80)

Zenmap (2 / 84)

Zero-day Usage (4 / 60)