

Topics

Port

3128 (Squid)	1–29
53 (DNS)	2–51
80 (HTTP)	2–4

A

AAAA	2–49
Accepted Content	2–12
Acquisition	1–109
Apache	1–26, 2–37
mod_forensics	2–40

B

Basic Authentication	2–12
Berkeley Packet Filter (BPF)	1–68
Primitives	1–74–76
Blue Coat	1–26
BPF → Berkeley Packet Filter	

C

Cached Data	1–24
Calamaris	1–33
Challenges and Opportunities	1–134
Cloud	1–140
CNAME	2–49, 2–56
Collection	
Capture	1–131
Design	1–129
Homegrown	1–128
Plan	1–123–124
Compromise Discovery	1–17
CONNECT	2–9
Content Transaction Logs	1–24
Cookie	2–12
COPY	2–9
CryptoLocker	2–67

D

Data Reduction	1–77
date	1–35
DELETE	2–9
DGAs → Domain Name Generation Algorithms	2–00
DNS	2–49
Basics	2–51
Compression	2–52
Fast-Flux (detection)	2–64
Fast-Flux (double)	2–62
Fast-Flux (simple)	2–60
Internationalization	2–72
IR	2–57

Query Logging	2–57
Rebinding	2–68
Scenario	2–54
DNS-over-*	
Mitigations	2–71
DNS-over-HTTPS (DoH)	2–69–70
DNS-over-TLS (DoT)	2–69
DoH → DNS-over-HTTPS	2–00
Domain Name Generation Algorithms (DGAs)	2–65
DoT → DNS-over-TLS	2–00
Dwell time	1–17

E

Elastic Stack	2–120
Encryption	1–137
Endace	1–127
Endianness	1–70
ETL → Windows Analytical Event Logging	2–00
Event Aggregation	2–110

F

Forcepoint	1–26
fprobe	1–120

G

GET	2–9
Google Analytics	2–23

H

HEAD	2–9
Hostname	2–12
_hstc	2–25
HTTP	2–3
Forensics value	2–5
Headers	2–12
History	2–4
Protocol History	2–6
Request/Response	2–7
HTTP Logs	2–36
Analysis	2–44
Investigation Value	2–46
HTTP Profiling	2–33
HTTP/2	2–27–29
HubSpot	2–23

I

IDS → Intrusion Detection System	2–00
IIS	2–37
CEntralized Binary Logging	2–43
Log	2–42
Internet Protocol Flow Information eXport (IPFIX)	1–114
Intrusion Detection System (IDS)	2–74

Intrusion Prevention System (IPS) 2-74
IPFIX → Internet Protocol Flow Information eXport .
IPS → Intrusion Prevention System 2-00

J

jq 2-81
 select 2-83

K

Keep-Alive 2-19
Kibana 2-124-127

L

LiveAction LiveCapture 1-127
LOCK 2-9
Log
 Aggregation 2-117
 Innovation 2-115
 Real-Time 2-113
 Shortfalls 2-112
Logs 1-115
 External Sources 1-122
 Infrastructure Sources 1-121

M

Malware
 Network 1-143
MKCOL 2-9
MOVE 2-9
MX 2-49

N

Named-based hosting 2-12
NAT → Network Address Translation
NCSA 2-38
NetFlow 1-114, 1-120
Network Address Translation (NAT) 1-135
Network Architecture Optimization 1-139
Network Forensics 1-11
Network Packet 1-70
Network Security Monitoring (NSM) 2-74
NGINX 1-26
NIKSEN NetDetector 1-127
nprobe 1-120
NS 2-49
NSM → Network Security Monitoring 2-00
NULL 2-49
NXDOMAIN 2-49

O

Open-source vs. Commercial 1-27
OPTIONS 2-9

P

PassiveDNS 2-57, 2-59
pcap 1-113
 File format 1-70
pcapng 1-72
Phased C2 2-68
pmacct 1-120
Port Mirroring 1-117
POST 2-9
PROPFIND 2-9
PROPPATCH 2-9
Proxy 1-24
 Cache Extraction 1-53
 Investigation Process 1-38
 Logs 1-37
 Reverse 1-24
PTR 2-49
Punycode 2-72
PUT 2-9

Q

Query string 1-30

R

Referer 2-12, 1-31
Request (HTTP) 2-8-9
Response (HTTP) 2-15-18
 Code 2-16
 Fields 2-21
 Headers 2-19
RSA NetWitness 1-127

S

Separator bytes 1-56
Server String 2-19
Snaplen 1-70
SOF-ELK 2-128
 HTTPD 2-139-141
 Inputs 2-128
 Summary 2-132
 Syslog 2-134-138
SPAN Port 1-116
Squid 1-26, 1-28
 Cache 1-54-58
 Configuration File 1-29
 Custom Format 1-31
 Logs 1-30
 Raw logs 1-34
SquidView 1-33
SRV 2-49
SSHFP 2-49
SSL/TLS Interception 1-29

Storage Area Network	1-142
strings	1-58
Switches	1-116
Symantec ProxySG	1-26
Syslog	2-96
Configuration	2-102
Content	2-99
Parameters	2-100
Server	2-98

T

Taps	1-118
tcpdump	1-73
Examples	1-79
Options	1-73, 1-78
tcpdump	1-68
Timestamp	1-35-36
TRACE	2-9
tshark	1-69, 1-100
Options	1-101
Tunnel	1-138
TXT	2-49

U

UNLOCK	2-9
Urchin	2-23
User-Agent	2-12, 1-31
__utma	2-23
__utmb	2-23
__utmz	2-23

V

Voice Over IP	1-142
---------------------	-------

VPN	1-138
-----------	-------

W

W3C Extended Format	2-39
WebDav	2-9
Windows Analytical Event Logging (ETL)	2-57
Windows Event Collector	2-108
Windows Event Forwarding	2-102
Wireless	1-140
Wireshark	1-69
!=	1-94
Column Display	1-86
Decode As	1-99
Display Filters	1-88-93
Display Filters (color)	1-94
FollowTCP	1-97
Interface	1-81, 1-84
Name Resolution	1-84
Time Display	1-86
Traffic Capture	1-99

X

X-Forwarded-For	2-12
-----------------------	------

Z

Zeek	2-75
Community ID	2-86
JSON	2-79
Log files	2-77
Policy	2-90
Scripting	2-85
Signature	2-85
Zscaler	1-26