

572.4- Commercial Tools, Wireless, and Full-packet Hunting

SMTP4-23

Overview & history.....	4
M-acronyms	5
MUA, MSA, MTA, MX, MDA	5
Email message flow	6-8
Common ports.....	9
Basic transaction example.....	10-13
SMTP evolutions.....	14
MIME & Base64.....	15-17
MIME Example	16-17
Authentication	18-19
Overview & history.....	18
Examples	19
Encryption	20-21
Native TLS vs. STARTTLS	20
STARTTLS example	21
Unicode handling	22
Investigative relevance.....	23
Exfiltration.....	23

Network Miner25-35

Overview	25
Host profiling.....	29-30
Image & credential extraction.....	31-32
Use-cases.....	33
CapLoader for large PCAPs	34-35

Wireless Network Forensics40-82

Course scope	40
Attack surface.....	41
Modes	42-43
Master & Managed	42
Ad-Hoc & Monitor	43
Basic Service Set (BSS).....	44

Extended Service Set (ESS)	45-46
----------------------------------	-------

Legality	47
----------------	----

Tools	48-57
-------------	-------

Required tools.....	48
Alfa USB adapter	49
802.11 analysers	50-51
Wireshark	50
Kismet.....	50
NetSpot.....	50
tcpdump	50

inSSIDer.....	52-53
---------------	-------

Built-In macOS WiFi tools	54
---------------------------------	----

WiFi Controller software.....	55-57
-------------------------------	-------

802.11 Frame.....	58-66
-------------------	-------

Overview.....	58
---------------	----

Frame types	59
-------------------	----

Management frame subtype	60
--------------------------------	----

Service Set Identifier (SSID)	61-62
-------------------------------------	-------

Control frame subtype.....	63
----------------------------	----

Data frames	64
-------------------	----

Frame control fields (directionality)	65-66
---	-------

ToDS, FromDS	65-66
--------------------	-------

Sniffing.....	67-71
---------------	-------

Managed mode sniffing	67-68
-----------------------------	-------

RFMON sniffing – WPA2	69
-----------------------------	----

RFMON sniffing – No WPA/WEP	70-71
-----------------------------------	-------

Attacks.....	72-82
--------------	-------

Detection difficulties.....	72
-----------------------------	----

Main attacks overview	73
-----------------------------	----

WPA2 PSK attacks	74-75
------------------------	-------

DOS: RF overload	76
------------------------	----

DOS: Deauth & RTS/CTS attacks	77-78
-------------------------------------	-------

Spotting DOS.....	79
-------------------	----

Evil twin attack.....	80-81
-----------------------	-------

Attacker staged approach.....	82
-------------------------------	----

Automated tools & libraries84-102

Overview & categories	84
Popular libraries	85
libpcap/npcap	85
libnids.....	85
tcpflow	86-88
Overview	86
Object extraction.....	87-88
Scapy	89
Dshell.....	90-91
editcap.....	92
ngrep	93
tcpstat & tcpdstat.....	94-97
Overview	94-95
gnuplot visualization	96-97
ntopng	98-100
tcpextract	101-102

Arkime..... 106-129

Overview	107-108
Components (Capture, Elastic, Viewer).....	108
Architecture	109-110
Limitations.....	111
Processing PCAP files.....	112
Filtering/querying.....	113-115
Fields	113-114
Examples	115
Viewer walkthrough	116-125
Sessions & rows.....	116-117
Sessions inspection	118-119
Uncompress: Extracting files	120-121
Connections tab	122-123
Hunts tab.....	124-125
Native enrichment.....	126
WISE – other enrichments.....	127
Integrated CyberChef	128-129

SMTP 4-23

Overview & history 4

M-acronyms 5

MUA, MSA, MTA, MX, MDA 5

Email message flow 6-8

Common ports 9

Basic transaction example 10-13

SMTP evolutions 14

MIME & Base64 15-17

MIME Example 16-17

Authentication 18-19

Overview & history 18

Examples 19

Encryption 20-21

Native TLS vs. STARTTLS 20

STARTTLS example 21

Unicode handling 22

Investigative relevance 23

Exfiltration 23

Network Miner 25-35

Overview 25

Host profiling 29-30

Image & credential extraction 31-32

Use-cases 33

CapLoader for large PCAPs 34-35

Wireless Network Forensics 40-82

Course scope 40

Attack surface 41

Modes 42-43

Master & Managed 42

Ad-Hoc & Monitor 43

- Basic Service Set (BSS) 44
- Extended Service Set (ESS) 45-46
- Legality 47
- Tools 48-57
 - Required tools 48
 - Alfa USB adapter 49
 - 802.11 analysers 50-51
 - Wireshark* 50
 - Kismet* 50
 - NetSpot* 50
 - tcpdump* 50
 - inSSIDer 52-53
 - Built-In macOS WiFi tools 54
 - WiFi Controller software 55-57
 - 802.11 Frame 58-66
 - Overview 58
 - Frame types 59
 - Management frame subtype 60
 - Service Set Identifier (SSID) 61-62
 - Control frame subtype 63
 - Data frames 64
 - Frame control fields (directionality) 65-66
 - ToDS, FromDS* 65-66
 - Sniffing 67-71
 - Managed mode sniffing 67-68
 - RFMON sniffing – WPA2 69
 - RFMON sniffing – No WPA/WEP 70-71
 - Attacks 72-82
 - Detection difficulties 72
 - Main attacks overview 73
 - WPA2 PSK attacks 74-75
 - DOS: RF overload 76
 - DOS: Deauth & RTS/CTS attacks 77-78
 - Spotting DOS 79
 - Evil twin attack 80-81
 - Attacker staged approach 82

Automated tools & libraries 84-102

Overview & categories 84

Popular libraries 85

libpcap/npcap 85

libnids 85

tcpflow 86-88

Overview 86

Object extraction 87-88

Scapy 89

Dshell 90-91

editcap 92

ngrep 93

tcpstat & tcpdstat 94-97

Overview 94-95

gnuplot visualization 96-97

ntopng 98-100

tcpextract 101-102

Arkime 106-129

Overview 107-108

Components (Capture, Elastic, Viewer) 108

Architecture 109-110

Limitations 111

Processing PCAP files 112

Filtering/querying 113-115

Fields 113-114

Examples 115

Viewer walkthrough 116-125

Sessions & rows 116-117

Sessions inspection 118-119

Uncompress: Extracting files 120-121

Connections tab 122-123

Hunts tab 124-125

Native enrichment 126

WISE – other enrichments 127

Integrated CyberChef 128-129