

572.5- Encryption, Protocol Reversing, OPSEC and Intel

Encoding, encryption & SSL.....4-40

Encoding.....4-7

Overview.....4

Base64.....5-7

Encryption.....8-21

Overview.....8

Strength.....9-10

Symmetric key encryption.....11-13

Overview.....11

Stream vs. block cipher modes.....12-13

Synchronous vs. self-synchronous.....12-13

Asymmetric key encryption.....14-15

Basic SSL/TLS process.....16-17

Perfect Forward Secrecy (PFS).....18

Diffie-Hellman exchange.....19-21

SSL/TLS.....22-33

HTTPS.....22

TLS handshake details.....23-30

Client Hello.....23

JA3 fingerprint.....24

Server Hello.....25

JA3S fingerprint.....26-27

Certificate exchange.....28-30

HTTPS data transferred problem.....31

HTTP vs. HTTPS.....32-33

Analytic mitigation.....34-40

NetFlow & DNS correlation.....34-35

Certificate metadata.....36

Wireshark decryption.....37-40

Example.....37-38

Requirements.....39

PFS.....40

MITM.....45-61

Overview.....45

ARP Spoofing.....46-47

Port stealing (CAM table manipulation).....48

UDP first response wins.....49-51

Common attack themes.....52

Other MITM attacks.....52

Open-source MITM tools.....53-54

Bettercap & dsniff.....53

Yersinia.....54

Investigative use.....55-58

Proxy, NSM, IDS/DLP.....55-56

Commercial solutions.....57-58

TLS inspection limitations.....59-60

Analytics on encrypted data.....61

Protocol Reversing.....63-86

Overview.....63

Protocol attributes.....64

How to approach.....65

Compromised websites.....67-72

Overview.....67

IPHONE8.5 example.....68-72

Request.....68

Response.....69

More responses.....70

Downloaded file.....71

Summary.....72

Common protocol backdoors.....73-77

Overview.....73

Cookie example.....74-77

Request.....74-75

Request (decoded).....76-77

Mixed protocol analysis.....78-81

Overview.....78

No space example.....79-81

Request headers.....79

Request body (binary data).....80

Decoded Windows shell	81
Binary protocol analysis	82-86
Overview	82
GHOST RAT example	83-68
gh0st_header	83
Encoded message.....	84
Decompressed payload	85
Partially decoded	86
OPSEC & Intel	91-111
Overview	91-92
Research OPSEC	93-98
DNS lookup on bad domains	93
OSINT	94-95
IR: The attacker is watching	96
IR: Premature blocking.....	97-98
LAN Scope	99-102
DHCP/DNS traffic.....	99-101
MDNS/UPNP/Bonjour	99-101
Other traffic	102
Research risk mitigations	103-105
Third party lookups	103
VPN/TOR	103
Air gapped	103-104
Separate IR network.....	105
Separate platforms.....	105
Guarding intel from attackers	106-107
Responsible sharing (ISACs & ISAOs).....	106-107
Traffic Light Protocol (TLP)	110
Community resources	111

Encoding, encryption & SSL 4-40

Encoding 4-7

Overview 4

Base64 5-7

Encryption 8-21

Overview 8

Strength 9-10

Symmetric key encryption 11-13

Overview 11

Stream vs. block cipher modes 12-13

Synchronous vs. self-synchronous 12-13

Asymmetric key encryption 14-15

Basic SSL/TLS process 16-17

Perfect Forward Secrecy (PFS) 18

Diffie-Hellman exchange 19-21

SSL/TLS 22-33

HTTPS 22

TLS handshake details 23-30

Client Hello 23

JA3 fingerprint 24

Server Hello 25

JA3S fingerprint 26-27

Certificate exchange 28-30

HTTPS data transferred problem 31

HTTP vs. HTTPS 32-33

Analytic mitigation 34-40

NetFlow & DNS correlation 34-35

Certificate metadata 36

Wireshark decryption 37-40

Example 37-38

Requirements 39

PFS 40

MITM 45-61

Overview 45

ARP Spoofing 46-47

Port stealing (CAM table manipulation)

48

UDP first response wins 49-51

Common attack themes 52

Other MITM attacks 52

Open-source MITM tools 53-54

Bettercap & dsniff 53

Yersinia 54

Investigative use 55-58

Proxy, NSM, IDS/DLP 55-56

Commercial solutions 57-58

TLS inspection limitations 59-60

Analytics on encrypted data 61

Protocol Reversing 63-86

Overview 63

Protocol attributes 64

How to approach 65

Compromised websites 67-

Overview 67

IPHONE8.5 example 68-72

Request 68

Response 69

More responses 70

Downloaded file 71

Summary 72

Common protocol backdoors 73-77

Overview 73

Cookie example 74-77

Request 74-75

Request (decoded) 76-77

Mixed protocol analysis 78-81

Overview 78

No space example 79-81

Request headers 79

Request body (binary data) 80

Decoded Windows shell 81

Binary protocol analysis 82-86

Overview 82

GH0ST RAT example 83-68

gh0st_header 83

Encoded message 84

Decompressed payload 85

Partially decoded 86

OPSEC & Intel 91-111

Overview 91-92

Research OPSEC 93-98

DNS lookup on bad domains 93

OSINT 94-95

IR: The attacker is watching 96

IR: Premature blocking 97-98

LAN Scope 99-102

DHCP/DNS traffic 99-101

MDNS/UPNP/Bonjour 99-101

Other traffic 102

Research risk mitigations 103-105

Third party lookups 103

VPN/TOR 103

Air gapped 103-104

Separate IR network 105

Separate platforms 105

Guarding intel from attackers 106-107

Responsible sharing (ISACs & ISAOs) 106-107

Traffic Light Protocol (TLP) 110

Community resources 111