SEC617 – Wireless Penetration Testing & Ethical Hacking

Topics

WiFi Data Collection & Analysis
- Wireless Threats 617.1–2-32
- Sniffing 617.1–33-89
- Rogue AP Analysis 617.1–90-123
- Bridging the Airgap 617.1–124-152

WiFi Attack & Exploitation Techniques
- Hotspots 617.2–3-30
- WiFi Client 617.2–31-62
- WEP 617.2–63-83
- DoS 617.2–84-122
- WiFi Fuzzing 617.2–123-147

Enterprise WiFi, DECT & Zigbee Attacks
- WPA2 PSK 617.3–3-49
- WPA2 Enterprise 617.3–50-77
- DECT 617.3–78-105
- Zigbee 617.3–106-149

Bluetooth & SDR Attacks
- Bluetooth 617.4–3-49
- Bluetooth Low Energy 617.4–50-95
- SDR 617.4–96-132

RFID, Smart Cards & NFC Hacking
- RFID 617.5–3-67
- Smart Cards 617.5–68-115
- NFC 617.5–116-137

Capture the Flag 617.6–2-15

Categories

Summaries
- Bluetooth Attacks 617.4–47-48
- Bluetooth LE Attacks 617.4–94
- Bridging the Airgap 617.1–152
- DECT Attacks 617.3–104
- Denial-of-Service Attacks 617.2–120
- Exploiting WiFi Hotspots 617.2–30
- NFC Attacks 617.5–137
- RFID 617.5–14
  - Contactless Smart Card Attacks 617.5–113
  - Low-Frequency Attacks 617.5–66
  - Tracking & Privacy Attacks 617.5–32
- Rogue AP Analysis 617.1–121
- SDR 617.4–130
- Sniffing WiFi 617.1–87
- WEP Attacks 617.2–80
- WiFi Client Attacks 617.2–61
- WiFi Fuzzing for Bug Discovery 617.2–145
- Wireless Threat 617.1–31
- WPA2 Enterprise Attacks 617.3–76
- WPA2 PSK Attacks 617.3–48
- Zigbee Attacks 617.3–148

Tools
- Aircrack-ng 617.1–45
  617.2–73-74
  - Airdecap-ng 617.2–79
  - Aireplay-ng 617.2–21, 77, 101
  - Airgraph-ng 617.3–52
  - Airmon-ng 617.1–45
  - Airodump-ng 617.3–52
  - Airtun-ng 617.2–42
  - Hostapd-WPE 617.3–69-71
- AirMagnet Laptop Analyzer 617.1–105
- AirPcap 617.1–40
- Airport 617.1–43
- AirPWN 617.2–36-38
- Android Pcap Capture 617.1–53, 79-80
- Android WiFi Analyzer 617.1–107
- Aruba AirMonitor 617.1–110
- Asleap 617.3–72
- BLE Fuzzer 617.4–85
- BLE Scannner 617.4–39
- BLE Sniffer 617.4–67
- BLEAH 617.4–86
- BLEFuzz 617.4–86
- BLEReplay 617.4–79, 89
- BLESuite 617.4–79-80, 85
- BLESuiteCLI 617.4–80
- Blue Hydra 617.4–94
- BlueScannner 617.4–39
- Bluesnarfer 617.4–43
- Bluetooth Scannner 617.4–39
- Bluetooth Stack Smasher 617.4–46
- BlueZ Suite 617.4–74-75, 84-85
- BTCrack 617.4–27-28, 40
- BTScannner 617.4–39, 43
- Burp Suite 617.2–27
- Cain & Abel 617.1–40
- Cain Password Sniffer 617.2–50
- CarWhisperer 617.4–43
- Cookies Manager+ 617.2–26
- CoWPAtty 617.3–21-23
- Cpscam 617.2–17
- Crackle 617.4–71, 81
- CrowbarKC 617.1–148
- DECT CLI 617.3–92, 98
- DECT Decoder 617.3–97, 99-100
- DECTShark 617.3–93-94
- Dump1090 617.4–116
- Eaphammer 617.3–71
- Easy Flasher 617.5–51
- Ekahau HeatMapper 617.1–82
- Ferret 617.2–24
- File2Air 617.2–99-100, 104, 110
- G72X Decoder 617.3–97
- GISKismet 617.1–77
- GPSMap 617.1–83
- Hamster 617.2–24
- Hashcat 617.3–26-28

  - HCCAPX Format 617.3–26
- Hcitool 617.4–44-45
- Hostapd-WPE 617.3–69-71
- Hwk 617.2–95
- ICMPTX 617.2–12
- InSSIDer 617.1–105-106
- Iodine 617.2–12
- ISniff-GPS 617.2–44-46
- John the Ripper 617.3–73
- JRockets 617.2–115
- Kalibrate 617.4–122
- KillerBee 617.3–126-141
  - Arsenal 617.3–130
  - Attack Example 617.3–132, 134, 136
- KillerZee 617.3–144-147
- Kismapping 617.1–83-84
- Kismet 617.1–40, 53, 67-74
  - Aircrack-PTW Plugin 617.1–69
  - Channel Control 617.1–74
  - Features 617.1–68-69
  - Filtering 617.1–101-104
  - Oldcore 617.1–83
  - Postprocessing Analysis 617.1–85-86
  - Signal Quality 617.1–113
- LibPcap 617.1–43
- MDK3 617.2–102
- Metasploit 617.1–130
  617.2–22, 47
  - Meterpreter 617.1–130-132, 137, 141-143
    617.2–56-59
  - MsfVenom 617.1–130
- Mfcuk 617.5–85, 88-89
- Mfoc 617.5–85-87, 90-91
- Mifare Classic Tool 617.5–95-96
- MIFARE SmartHack 617.5–108, 111-112
- MS Message Analyzer (MMA) 617.1–42
- Multimon-ng 617.4–120
- MyKismap 617.1–83-84
- Netdisco 617.1–119
- NetMon 617.1–41-42, 137-138
- NetScout AirCheck G2 617.1–115
- Network Associates Sniffer 617.1–59
- Network Chemistry WSP-100 617.1–59
- NFC MFClassic 617.5–94-95
- NFC Smart Card Info 617.5–75
- NFC Tag Cloner 617.5–106
- NFC Tag Info 617.5–81, 101, 110
- NFC Tag Writer 617.5–124
- NFCProxy 617.5–77
- Nmap 617.1–99
  617.2–131
  - RogueAP (NSE Script) 617.1–99
- NRF Connect 617.4–76-78
- Nstx 617.2–12
- Obexftp 617.4–44-45
- PCSC-Lite 617.5–79-80
- Pickupline 617.2–17
- ProxBrute 617.5–50-52
- Proxmark 3 617.5–45-52
  - Data Decoding 617.5–63-64
  - Data Plot 617.5–58-61
- Pwnpass 617.5–74
- Re-DECTed 617.3–103
- Reaver 617.3–35-37
- Responder 617.4–101
- Rfcomm 617.4–44-45
- RFIDIOt 617.5–38-39
- RFProtect Mobile 617.1–105
- RTL Power & Heatmap 617.4–109, 112-114
- RTL-FM 617.4–120
- RTL_433 617.4–125
- RX-Tools 617.4–120
- Scapy 617.2–105, 131-139
  617.4–84
- SniffAir 617.3–60
- SpectrumSpy 617.4–107
- Squareless 617.5–75
- TagMo 617.5–131-132
- Tcpdump 617.1–37-38, 53, 55-58
  - Filters 617.1–58
  - Options 617.1–56
- Tshark 617.2–143
- Ulread 617.5–128
- UltraReset 617.5–105
- Ussp-Push 617.4–44-45
- Vapor Trail 617.4–101
- Vistumbler 617.1–105
- WiFiFoFum 617.1–107
- Wifite2 617.2–78
- WildPackets AiroPeek NX 617.1–59
- Windump 617.1–40
- WinPcap 617.1–40
- WirelessKeyView 617.1–134
  617.3–39
- Wireshark 617.1–40, 53, 59, 138
  617.3–95, 103, 141
  617.4–68
  - Filters 617.1–61-65
  - TCP Stream 617.2–25
- Zillow 617.2–19

Commands

- `aircrack-ng` 617.2–74
  617.3–24
- `airdecap-ng` 617.2–79
  617.3–40
- `aireplay-ng` 617.2–77, 101
- `airgraph-ng` 617.3–52
- `airmon-ng` 617.1–45
  617.3–71
- `airodump-ng` 617.3–52
- `airport` 617.1–43, 145-146
- `airpwn` 617.2–38
- `airtun-ng` 617.2–42
- `amiitool` 617.5–131
- `asleap` 617.3–72

SEC617 – Wireless Penetration Testing & Ethical Hacking

bleah 617.4–87-88
blesuite-runner.py 617.4–80
bss 617.4–46
btcrack 617.4–28
btmon 617.4–70
cap2hccapx 617.3–27
cardselect.py 617.5–38
cowpatty 617.3–23, 25
crackle 617.4–82
dect-decoder.sh 617.3–100
dect_cli 617.3–92, 98
dectshark 617.3–93
dump1090 617.4–116
fdxbnum.py 617.5–39
file2air 617.2–100
gatttool 617.4–75
genpmk 617.3–25
getsystem 617.1–142
giskismet 617.1–75-77
gstrings 617.5–131
hashcat 617.3–27-28
hcitool 617.4–32, 37, 44, 75
heatmap.py 617.4–113
hostapd-wpe 617.3–71
hwk 617.2–95
idletime 617.1–137
ifconfig 617.1–44-46
    617.2–16
iwconfig 617.1–44-46
iw 617.1–44-46, 51-52
john 617.3–73
jrockets 617.2–115
kal 617.4–122
kismet 617.1–70
macshift 617.2–16
mdk3 617.2–102
mfcuk 617.5–89
mfoc 617.5–87, 90
mifare-ultralight-info 617.5–108
msfconsole 617.1–130
    617.2–57
    617.5–134
msfvenom 617.1–130
    617.2–56
msiexec 617.1–137
multimon-ng 617.4–120
ncpa.cpl 617.2–49
neighbor.sh 617.2–52-55, 57
netsh 617.1–96, 129, 133-135, 139-143
networksetup 617.1–150
nfc-emulate-tag 617.5–101
nfc-emulate-uid 617.5–102
nfc-list 617.5–100
nfc-mfclassic 617.5–94
nfc-mfdesfire-keysearch 617.5–112
nfc-mfultralightc 617.5–108
nfc-mfultralight 617.5–105, 617.5–124
nm2lp 617.1–138
nmap 617.1–99
nmcap 617.1–137
nmwifi 617.1–137
pcsc_scan 617.5–80
play 617.3–100
proxmark3 617.5–45-46, 56-57, 63-64, 97-98
reaver 617.3–36
rogueap 617.1–142
rtl_433 617.4–126-127
rtl_fm 617.4–120
rtl_power 617.4–113
scapy 617.2–132
sdptool 617.4–45
security 617.1–148
sniffair.py 617.3–60
sw_vers 617.1–147
tcpdump 617.1–37-38, 57
tshark 617.2–143
    617.4–32
ubertooth-btle 617.4–72, 82
ubertooth-lap 617.4–35, 37
ubertooth-uap 617.4–37
ulread 617.5–128
wifite2 617.2–78
winenum 617.1–141
wirelesskeyview 617.3–39
zbdsniff 617.3–133
zbdump 617.3–131
zbfind 617.3–137
zbgoodfind 617.3–140
zbid 617.3–131
zbreplay 617.3–135
zbstumbler 617.3–131
zwdump 617.3–147
zwreplay 617.3–147

Toolkit

ACG LAHF LF/HF Reader/Writer 617.5–37
ACR122U Smart Card Reader/Writer 617.1–25
    617.5–79-80, 86, 94, 100-102, 112, 128
Adafruit BLE Sniffer 617.4–66
AirSpy 617.4–107
AVR Dragon 617.3–128
AVR RZ Raven USB Stick 617.3–127
BladeRF 617.3–103
    617.4–105
Canakit 617.1–28
Ettus SDR 617.4–107
FTS4BT 617.4–28
HackRF 617.3–103
    617.4–104, 125, 127-128
I Love My Neighbors 617.1–29
    617.2–51-55, 57
  Services 617.2–54
Kali Linux 617.1–29
LimeSDR 617.4–84, 107
Linksys USBBT100 617.3–146
Panda USB Adapter 617.1–23-24

Parani SENA UD-100 . . . . 617.1–24
. . . . 617.4–73
Pineapple Nano 617.2–48-49
PiPoint Raspberry Pi 617.1–28
Powered USB Hub 617.1–27
Proxmark 3 RDV2 . . . . 617.5–44-48
RTL-SDR 617.1–26
. . . . 617.3–103
  DVB-T Tuner 617.4–106
Stingray 617.4–121
SWAT 617.1–22
. . . . 617.3–69
Tastic RF Thief 617.5–53-54
Ubertooth One 617.4–35, 71-72, 81, 84, 104
Verizon MiFi 617.2–21
VIVOPay Credit Card Reader 617.5–73-75
Wave Bubble 617.2–90
YARD Stick One 617.3–146
. . . . 617.4–104

SEC617 – Wireless Penetration Testing & Ethical Hacking

A

- Access Code 617.4–33
- Access Control List 617.2–39, 617.3–124
- Account Lockout 617.3–59
- Account Monitoring 617.2–29
- ACK Frame 617.3–118
- ACL 617.4–15
- ACL → Access Control List
- Active Directory 617.2–60
- Active Discovery 617.1–105
- Ad-hoc Mode 617.1–35
- Adafruit Feather HUZZAH 617.5–53
- ADC 617.4–99
- Administrative Interface 617.2–11
- Adobe Flash Attack 617.2–53
- ADS-B 617.4–116
- Advertisement Packet Chaining 617.4–93
- AeroScout 617.5–7
- AES-CCM 617.4–57
- AES-CCM* 617.3–120, 142
- AES-CCMP 617.2–111, 617.3–7
- AES-GCM 617.3–46
- AFH → Frequency Hopping / Adaptive
- AID 617.5–109-111
- AID → Association IDentifier
- Aircraft Beacon 617.4–116
- AirDefense 617.1–105, 117
- AirMagnet 617.1–105, 117
- Airport Interface 617.1–144, 146
- AirTight 617.1–117
- Alarm System 617.4–126
- Amazon AWS 617.3–29
- Amiibo 617.5–128
  - Key Recovery 617.5–131-132
  - Security 617.5–130-132
- Amiiqo 617.5–132
- Amplifier 617.1–81
- AN10787 617.5–110
- Android Beam 617.5–125
- Android CyanogenMod 617.5–77
- Android Developer Mode 617.4–69
- Anomaly Analysis 617.5–39
- Anonymity Attack 617.1–14, 617.5–17
- Antivirus Bypass 617.1–130
- AP 617.2–5
  - Filter Bypass 617.2–41
  - Fingerprinting 617.1–98
  - Impersonation 617.2–21, 52
  - Spoofing 617.2–20
- Apple Bonjour 617.2–44
- Apple Pay 617.5–127
- ARP Poisoning 617.2–50
- ARP Replay 617.2–76
- ARP Table 617.1–110, 119
- ARP Unicast 617.2–44
- ARQN 617.4–14
- Aruba Networks 617.1–105, 117
- Ascom Voo:Doo 617.3–90
- Association Flood 617.2–94
- Association IDentifier 617.2–94
- Atmel T5557 617.5–42
- ATT 617.4–57-59
- Authentication Bypass 617.2–13, 17
- Authentication Credentials 617.2–6
- Authentication Flood 617.2–94
- Authentication Server 617.2–6

B

- Backdoor 617.1–92, 142
- Backoff Timer 617.3–33, 35
- Barker Code 617.4–33
- BCC 617.5–101
- BD_ADDR 617.4–13, 16, 20, 25, 30, 32, 36
- Beacon Chaining 617.4–92
- Beacon Flood 617.2–102
- Beacon Frame 617.2–104, 130, 617.3–118
  - Display Filter 617.1–64
- Beaconmaker 617.5–24
- Beamforming 617.1–49
- BER 617.4–33
- Berkeley Packet Filter (BPF) 617.1–55
- Biphase 617.5–62
- Block Cipher 617.2–68
- Bluesocket 617.2–10
- Bluetooth 617.1–17, 617.4–4-94
  - 5 617.4–91-93
  - Adapter 617.1–24, 617.4–63, 71, 73
  - Addressing 617.4–13
  - AMP 617.4–9, 53
  - Classic 617.4–6-8
    - Channels 617.4–7
    - Classes 617.4–8
    - Frequency 617.4–6
    - Pairing 617.4–24-26
    - Profiles 617.4–18
    - Security Modes 617.4–19
  - Device Assessment 617.4–43
  - Device Configuration 617.4–42
  - Dongle 617.4–34
  - EO Cipher 617.1–12
  - Low Energy 617.4–10, 51-54
    - Advantages 617.4–54
    - Beacon 617.5–23
    - Bonding Requirements 617.4–57
    - Channels 617.4–56
    - Differences with Classic 617.4–56-62
    - Pairing 617.4–57
    - Profiles 617.4–57-58, 62
  - Maximum #Slaves 617.4–14

- Monitoring (Insufficiency) 617.1–21
- PIN 617.4–20, 22, 24, 26
- Profiles 617.4–11-12
- Protocol Stack 617.4–11-12
- Range 617.4–8, 23, 54
- Security Enhancements 617.4–90
- Sniffer 617.4–28, 64
- Sniper Rifle 617.4–23
- Technology 617.4–4

BNEP 617.4–12, 18
BPF → Berkeley Packet Filter
Bridged Connection 617.2–49
Bridging the Airgap 617.1–126-151
- Concept 617.1–127
- Limitations 617.1–128
- Mac OS 617.1–144-150
- Windows 617.1–129-143

Brute Force 617.3–27, 32
617.4–36, 58, 60, 81
617.5–88
BSS 617.1–35, 617.4–46
BSSID Display Filter 617.1–64-65
BTBB 617.4–84
Bug Discovery 617.2–124
Bus Sniffing 617.3–140
617.5–112

C

CA 617.3–65-67
CALEA 617.5–17
Canakit 617.1–28
CAP Code 617.4–118-120
Captive Web Portal 617.2–6-7
Card Reader 617.5–79
CC2540 617.3–146
CCM* → AES-CCM*
CCMP 617.1–39
617.3–7, 41, 56
CDP → Cisco Discovery Protocol
Cellular Tower 617.4–105, 121
Certificate Validation 617.2–29
Challenge/Response 617.3–124
Channel Hopping 617.1–74
617.3–92
617.4–35, 56
ChopChop Attack 617.2–77
CIA 617.1–9
Circuit Hooks 617.3–139
Cisco Discovery Protocol 617.1–69, 111, 118
- Announcements 617.1–110, 118

Cisco Systems 617.1–103
Clear To Send 617.2–106-110
Client Isolation 617.2–9
CloneMyKey 617.5–93
Cloning 617.5–12, 35, 39, 64-65, 70, 90-91, 94-96, 106
- Attack 617.5–45-47

Clothing Tag 617.5–31
CloudShark Uploader 617.1–80
CNSA 617.3–46
Coded LE 617.4–92
Com-on-Air 617.3–90
Combination Key 617.4–25
Command Frame 617.3–118
Commercial Mode 617.3–122
Common Name 617.3–62
Compatibility Mode 617.2–111
Contact Sensor 617.4–126
Control Frame 617.1–38, 50
617.2–66
Controller 617.2–5-7
- Vulnerabilities 617.2–10

Cookie 617.2–24-27
Cox WiFi 617.2–7-8
- Network Access 617.2–9

CRAPTO1 617.5–85
CRC32 617.2–66, 70
CRYPTO1 617.5–83, 88, 99, 107
- Weaknesses 617.5–85

CryptUnprotectedData() 617.3–39
CSMA/CA 617.2–106
CTS → Clear To Send
CVC 617.5–72, 76
CVV2 617.5–72
Cyanogen 617.5–77

D

DAC 617.4–17, 99
DarkSide Attack 617.5–88
Data Disclosure 617.5–12
Data Frame 617.1–38, 50
617.3–118
Data Injection 617.5–12
Data Integrity 617.3–5
Data Recovery 617.5–91
Data Sampling 617.5–57
Datasheet 617.5–62
DCK 617.3–88, 101
Deauthenticate Attack 617.1–10
617.2–21
617.4–83
Deauthenticate Frame 617.1–109
617.2–96, 101
Deauthentication Flood 617.2–96, 100, 102-103
DECT 617.1–12, 15
617.2–65
617.3–80-104
- Architecture 617.3–83-85
- Attack 617.3–96, 101
  - HW 617.3–90
- Audio Eavesdropping 617.3–96-100
- Frequency 617.3–84
- Interoperability 617.3–81
- MAC Layer 617.3–85
- Network Scanning 617.3–92-95

- PHY Layer 617.3–84
- Range 617.3–80
- Security 617.3–86-88
- Standard Cipher 617.1–15
  617.3–101

Default Password 617.3–27
Defensive Measures 617.2–28-29, 60, 119
617.3–47, 74-75
617.4–40-43
Denial-of-Service 617.1–9, 109
617.2–21, 84-118
617.3–59
617.4–73
- Impact 617.2–84
- Range 617.2–116
- Response Plan 617.2–119
- Targets 617.2–88
- Types 617.2–87

DES 617.5–107
Design Weakness 617.1–10
Device Provisioning Protocol 617.3–45
DFS → Dynamic Frequency Selection
Dial-Up 617.4–18
DIAMETER 617.1–30
Dictionary Attack 617.1–147-148
617.3–19, 21, 31
Diffie-Hellman 617.3–45
Directional Antenna 617.4–23
Directional Transmit 617.1–49
Directory Browsing 617.2–11
Disassociation Flood 617.2–96, 102-103
Discoverable Mode 617.4–16
DLP 617.4–101
DNS 617.2–9
- Tunneling 617.2–12

Domain Settings 617.1–52
DPP → Device Provisioning Protocol
Dragon 617.3–128
Driver Software Weakness 617.1–10
DSAA 617.3–87
DSC 617.4–126
DSC → DECT Standard Cipher
DSSS 617.2–117
617.3–115
Dwell 617.1–74
Dynamic Frequency Selction (DFS) 617.1–52

E

E0 617.4–21
E21 617.4–25-26
E22 617.4–25
EAP 617.1–66
617.2–32
- -MS-CHAP 617.1–12
  617.3–55, 65, 71
  - Cracking 617.3–72-73
- -PEAP 617.1–66

EAPOL 617.1–66
617.3–12, 56, 58
ECC 617.3–46, 125
ECDH 617.4–57
EDR 617.4–6
Ellisys Bluetooth Explorer 617.4–64-65
EMV 617.5–71-73
- Reader 617.5–73-75
- Token 617.5–127

Encryption Dumb-down Attack 617.3–101
ESP8266 617.5–53
ESSID 617.1–77
Estimote 617.5–24
ETC 617.5–18
Ethernet-Compatibility Mode 617.1–35-36
ETSI 617.3–80
Excel 617.1–86
EZ-Pass 617.5–7, 18, 29
- Tracking 617.5–19-21

EZon 617.5–99-102
- UID Analysis 617.5–99

F

Fake DNS 617.2–22
False Positive 617.1–100
617.4–35
FasTrak 617.5–18
FCCH 617.4–122
FCS 617.3–119
FEC 617.4–92-93
FFD 617.3–116
FFT 617.4–110
FH → Frequency Hopping
FHSS 617.3–109
617.4–6
Firewall 617.2–5
FLC 617.3–112
FLEX 617.4–118
Floor Plan 617.1–82
FP 617.3–83
- Impersonation 617.3–101

FPGA 617.4–99
Frequency Detection 617.5–56
Frequency Hopping 617.4–16-17
- Adaptive 617.4–6, 93

Friendly Rogue 617.1–92, 97
From-DS Bit 617.2–40-41
Fuzzing 617.2–124-144
617.4–73, 84-88
- Plan of Attack 617.2–141
- Targets 617.2–130
- Traffic Recording 617.2–142-143
- When ? 617.2–144

G

GAP 617.3–87-88
GATT 617.4–57-59, 61

- Discovery 617.4–84, 86

- GCMP 617.3–41
- Geiger Counter 617.1–107, 114
- GFSK 617.4–54
- GNU Radio 617.1–26
  - 617.3–101
  - 617.4–128
  - Companion 617.4–124, 128
- GoodFET 617.3–138-140
- Google Earth 617.1–75, 84
- Google Maps 617.2–44
- Google Wallet 617.5–126, 133
- GPS 617.1–68, 77, 83-84
- GQRX 617.1–26
  - 617.4–109-112
- Greengate DA099 .... 617.3–90
- Group Policy 617.2–28, 60
- Guestbox 617.2–11

H

- Hack RF Jawbreaker 617.4–104
- Hashing 617.3–5
- HCCAP Format 617.3–27
- HCE 617.5–126
- HCI 617.4–11, 59
  - Snooping 617.4–69
- Headset 617.4–18, 38
- Heatmap 617.1–82
- HEC 617.4–14
- HF 617.5–70, 79
- HID MaxiProx 617.5–53
- HID Proxcard 617.1–12, 18
- HID ProxCard II 617.5–40-55
  - Clonability 617.5–46
  - ID Numbers 617.5–49
- Hidden Node Problem 617.2–106-107
- High Security Model 617.3–122
- High Throughput 617.1–146
- High-Gain Antenna 617.1–81
- HMAC 617.3–6
  - -MD5 .... 617.3–12-13
  - -SHA1 .... 617.3–9, 11-13
- Home ID 617.3–144
- Hopping Pattern 617.4–7
- Hopping Speed 617.4–17
- Host IPS 617.2–28
- Hostapd 617.3–52, 69
- Hotspot 617.2–5, 617.1–13
  - Architecture 617.2–5-6
  - Components 617.2–5-6
  - Impersonation 617.2–22
  - Injection 617.2–34-35
- HT → High Throughput ....
- HT20 .... 617.1–48
- HT40 .... 617.1–48
- HTTP Filter 617.2–6
- HTTP Vulnerability 617.2–23
- Hunter Killer Attack 617.2–103

I

- I-Love-My-Neighbors 617.1–29
  - 617.2–51
- I-Pass 617.5–18
- IBeacon 617.5–22-29
  - Application 617.5–26-28
  - Localization 617.5–25
- IBSS 617.1–35
  - Rogue 617.1–94-95
- IC 617.4–10
- ICMP 617.2–9
  - Echo 617.2–12-14
  - Tunneling 617.2–12
  - Unreachable 617.2–13
- ICV → Integrity Check Value ....
- IDS 617.4–101
- IEEE 802.11 .... 617.1–38-39
  - 617.4–14, 32
  - a 617.1–47
  - ac 617.1–47, 49, 51
  - b 617.1–47
    - 617.3–115
    - 617.4–23
  - e 617.2–113
  - g 617.1–47
  - i 617.1–39
    - 617.2–113, 117
    - 617.3–41
  - n 617.1–47-48, 146
    - 617.2–111, 115
  - p 617.5–18
  - r 617.3–41
  - w 617.2–103, 117
  - Expert Analysis 617.1–68
  - Raw Frames 617.1–39
    - Not Encrypted 617.1–60
- IEEE 802.15.4 .... 617.2–65
  - 617.3–108, 124, 126, 134, 140
- IEEE 802.1X Authentication 617.2–5, 29, 98
  - 617.3–7, 38, 47, 56
- IEEE 802.3 .... 617.1–37
  - 617.4–14
- IHV 617.1–41
- ILMN → I-Love-My-Neighbors ....
- IMEI 617.4–121
- Imposter AP 617.2–52
- IMSI 617.4–121
  - Catcher Detector 617.4–121-122
- Information Disclosure 617.1–8
  - 617.2–18
- Infrastructure Rogue 617.1–97
- Initialization Vector 617.2–65, 68-69, 71
- Inquiry Mode 617.4–16, 35
- Integrity Check Value 617.2–66, 70-71, 75
- Interoperability 617.1–68

- IOS ... 617.1–119
- IPoDNS ... 617.2–12
- IPoICMP ... 617.2–12
- IPSec ... 617.2–29
  - Gateway ... 617.2–39
- ISO 14443 ... 617.1–25, 617.5–71, 82, 118
  - UID Format ... 617.5–99
- IV → Initialization Vector ...
- IV Collision Attack ... 617.3–56, 142
- IV Reuse ... 617.3–142

J

- JTAG ... 617.3–138
- Just Works ... 617.4–57-58, 60, 73, 82

K

- Kali ... 617.1–29, 51
- Karma Attack ... 617.2–47
- Karmetasploit Attack → Karma Attack ...
- Keepalive Ping ... 617.1–93
- KEK → Key Encryption Key ...
- Kerberos ... 617.1–30
- Kernel Panic ... 617.1–27
- Key Derivation ... 617.5–130
- Key Diversification ... 617.5–92-93
- Key Encryption Key ... 617.3–12, 58
- Key Guessing Attack ... 617.5–86, 111
- Key Recovery Attack ... 617.1–16
  ... 617.5–88-90, 131-132
- Key Reuse Attack ... 617.2–65, 111
- Key Rotation ... 617.3–132, 136
- Key Sniffer ... 617.3–133
- Key Stream ... 617.2–69
- Keychain Attack ... 617.1–147-149
- Keyhole Markup Language ... 617.1–75, 84
- Keysy ... 617.5–46
- Kickstarter ... 617.4–104
- KML → Keyhole Markup Language ...
- Know Your System ... 617.1–27
- Kontakt ... 617.5–24
- KRACK ... 617.3–41-44
- KYS → Know Your System ...

L

- L2 Encryption ... 617.2–34
- L2CAP ... 617.4–11, 45-46, 59
- LAP ... 617.4–13, 34-37
- Law Enforcement ... 617.1–115
- LDAP ... 617.2–6
- LE1M ... 617.4–92
- LE2M ... 617.4–92
- LEAP (Cisco) ... 617.1–12
  ... 617.3–72
- Least Privilege ... 617.4–42
- LibNFC ... 617.1–28
  ... 617.5–101, 105, 108
- LibPCAP ... 617.1–53-54, 144
  - Format ... 617.1–43, 138
    ... 617.3–27
- Link Key ... 617.4–25
- Linksys ... 617.1–119
- LMP ... 617.4–11
  - Exchange ... 617.4–15
- Location Tracking ... 617.4–121
  ... 617.5–17
- Logout URL ... 617.2–17
- Long-Range Attack ... 617.2–116
- LSFR ... 617.3–88
  ... 617.4–21
- LT ... 617.4–14
- LT_ADDR ... 617.4–14
- LTK ... 617.4–57, 82

M

- MAC
  - Attack ... 617.2–88, 93
  - Filtering ... 617.3–124
  - Impersonation ... 617.2–16
- Malformed MP4 ... 617.5–134
- Malicious Rogue ... 617.1–92-93
- Man-in-the-Middle ... 617.1–29
  ... 617.2–50
  ... 617.3–13, 43, 124
  ... 617.4–58, 105, 121
- Managed Mode ... 617.1–35, 37
- Management Frame ... 617.1–38-39, 50
  ... 617.2–66, 102-103
  - Protection ... 617.2–103
- Manchester ... 617.5–62
- Manual Tag Analysis ... 617.5–55
- Marshmallow ... 617.5–134
- Mask Attack ... 617.3–26-27
- Master Mode ... 617.1–35
- McDonald's ... 617.5–123
- MDNS ... 617.2–44
- Medium Attack ... 617.1–9
- Medium Reservation Attack ... 617.2–109
- Message Integrity Check ... 617.1–10
  ... 617.2–103
  ... 617.3–121
  - Key ... 617.3–12
- Meterpreter Commands ... 617.2–58
- MFP → Management Frame Protection ...
- MIC → Message Integrity Check ...
- Michael Countermeasures ... 617.2–115
- Michael Key ... 617.3–12
- Michael MIC ... 617.2–115
- Micheal Protocol ... 617.1–10
- MIFARE ... 617.1–12, 25, 617.5–82
  - Classic ... 617.5–83-98
    - 1K/4K ... 617.5–84

    Attack 617.5–97
    Cloning 617.5–94-96
    Memory Structure 617.5–84
  DESFire 617.5–109
    Enumeration 617.5–110
    EV1 617.5–109
    EV2 617.5–109
  Dump 617.5–91, 105
  Ultralight 617.5–103-107, 129
    C 617.5–107
  Writable Cards 617.5–93
MiFi 617.3–52
MIMO 617.1–48
Misconfigured Equipment 617.1–92
MMI 617.3–123
MO 617.5–127
Mobile Operator (MO) 617.1–13
Mobility 617.1–7
Monitor Mode 617.1–35-36, 38
  Android 617.1–78
  Linux 617.1–44-46
  Mac OS 617.1–43
  Windows 617.1–40-42
MS-CHAP → EAP-MS-CHAP
MTBF 617.4–107
MTU 617.4–92
MU-MIMO 617.1–49
Multi-SSID Impersonation 617.2–47-48
Multiple-Transmitter 617.1–49
Mutual Authentication 617.3–124
  617.4–26, 123

N

NAP 617.4–13, 36
NAT 617.1–151
NAV → Network Allocator Vector
NDEF 617.5–119, 136
  Header 617.5–120
  Writing 617.5–124
NDIS 617.1–41, 96, 129, 142
Nested Authentication Attack 617.5–85-86, 90
NetBIOS Advertisements 617.1–110
NetShair Nano 617.1–11
Network Allocator Vector 617.2–108-109
Network Impersonation 617.2–43, 47-48, 51
Network Monitoring 617.4–101
Network Radius 617.3–120
Network Tracking 617.2–44
NFC 617.1–18
  617.4–53
  Common Attacks 617.5–133
  Controller 617.5–126-127
  Data Exchange Format 617.5–119
  Frequency 617.5–6
  Infrastructure Attacks 617.5–136
  Proxy Attack 617.5–76-77
  Technology 617.5–117
    UID Record Writing 617.5–124
    Versus RFID 617.5–11
    Versus Smart Card 617.5–118
    Writing 617.5–124
NfcPy 617.5–124
Nintendo 617.5–131
NJDOT
    Tracking 617.5–20
Nmap Scripting Engine 617.1–99
No Wireless Policy 617.1–11
Non-Discoverable Device 617.4–30, 35-36, 38, 42
Non-Persistent Attack 617.2–87
Nonce 617.3–14, 41
NPP 617.5–125, 136
NRF51822 617.4–66
NSE → Nmap Scripting Engine
NTAG215 617.5–128, 132
    Security 617.5–129
NYSDOT
    Tracking 617.5–20-21

O

OBEX 617.4–12, 18, 45
Obj-C 617.5–26
Off-by-One Enumeration 617.4–31-32
On-The-Go 617.1–78
OOB 617.3–30
  617.4–58
Open Authentication 617.2–34
Open Network Impersonation 617.2–21
OpenBTS 617.4–105
OpenCL 617.3–26
OpenLTE 617.4–105
Opportunistic Wireless Encryption 617.3–45
Oracle Traffic Display Filter 617.1–64
Organizational Policy 617.1–92
OS Fingerprinting 617.1–99
Osmo-fl2k 617.4–103
OTA → Over-the-Air
OTG → On-The-Go
OTP 617.5–103-104, 107, 129
OUI 617.4–13
Over-the-Air 617.3–130, 132-133
OWE → Opportunistic Wireless Encryption

P

Packet Capture 617.1–50
Packet Crafting 617.2–131
Packet Injection 617.2–99
Pairing Authentication Attack 617.4–27
Pairwise Key Expansion 617.3–10
Pairwise Master Key 617.3–8-10, 42-43, 56
Pairwise Transient Key 617.3–8-13, 56, 58
    Mapping 617.3–12
PAN ID 617.3–116, 118

Panda 617.1–23, 83
Parani Sena 617.1–24
Passive Listening 617.1–8
Passphrase Minimal Length 617.3–47
Password Cracking 617.3–26
Password Spraying Attack 617.3–59-60
Payload 617.2–56
PBC 617.3–30
PBKDF2 617.3–9, 22
PCB 617.3–127
PCD 617.5–10-11, 41, 79
  Emulation 617.5–98
PCI 617.3–38
PCR800 617.4–126
PEAP → Protected Extensible Auth Protocol
Perfect Forward Secrecy 617.3–45
Peripheral Devices 617.4–6
Persistent Attack 617.2–87
Personal Firewall 617.2–28
PFS → Perfect Forward Secrecy
Phishing Campaign 617.4–120
Physical Layer
  Control 617.1–51-52
Physical Medium Attack 617.2–88-89
PICC 617.5–10-11, 41, 79
  Reconnaissance 617.5–78
Piconet 617.4–16-17
PIN 617.4–20, 22, 24, 26
PIN Attack 617.3–33, 35
  617.4–27, 29, 81-83
PIN Length 617.4–40
Ping 617.2–13
PiPoint 617.1–28
PKI 617.3–125
PLC → Programmable Logic Controller
PMK → Pairwise Master Key
PN532 Chipset 617.1–25
PNL → Preferred Network List
POCSAG 617.4–118, 128
PoE 617.5–7
Policy 617.4–39
  Establishment 617.4–40-41
POLP 617.4–42
PoS 617.5–126
Post-Exploitation 617.1–141
PP 617.3–83
Pre-Shared Key 617.2–69, 71, 75
  617.3–8-9
Preamble 617.4–33
Precomputation Attack 617.3–25
Preferred Network 617.1–14
  List 617.1–150
    617.2–43-44
    617.3–52
PRF 617.3–10
PRGA 617.2–69, 71
  617.4–21
Prism2 Test Mode Jamming Attack 617.2–119
Privacy 617.1–14
  617.2–44
  617.4–121
  617.5–17, 22, 29, 31
  Attack 617.5–12
Privacy Bit 617.1–64
Privilege Escalation 617.1–142
Probe Request 617.2–43-44, 47, 98, 128
  617.4–32
Profile Information 617.1–134
Programmable Logic Controller 617.2–90
Protected Extensible Auth Protocol 617.3–53-55
  Authentication Attack 617.3–59, 68
  Transaction 617.3–53-55
  Weakness 617.3–62
  Windows Properties 617.3–63, 74
Protocol Analyzer 617.3–140
Protocol Dissector 617.1–66
Protocol Fuzzing → Fuzzing
Protocol Manipulation 617.2–131
Protocol Weakness 617.1–12
Proxy 617.2–52
Pseudorandom Data Stream 617.2–69
PSK 617.5–62
PSK → Pre-Shared Key
PSPF → Publicly Secure Packet Forwarding
PSTN 617.3–83
PTK → Pairwise Transient Key
PTW Attack 617.2–73
Publicly Secure Packet Forwarding 617.2–39-41
  Bypass Attack 617.2–42

Q

QoS 617.2–113
  617.4–11

R

Race Condition 617.2–34
RADIUS 617.1–66
  617.2–6
  617.3–53, 55, 68-69
  Server Validation 617.3–61-62
Ralink 617.1–23
Range Mapping 617.1–81
Raspberry Pi 617.4–101
Raven 617.3–127
RC4 617.2–66, 68, 71
  617.4–21
RCE 617.5–134
Ready To Send 617.2–106-110
Real-Time Location System 617.1–82
Receiver 617.5–5
Red Team Tip 617.4–120
Regulatory Domain Settings → Domain Settings
Rekeying 617.2–111

Relay Attack 617.5–13, 133
Replay Attack 617.2–65, 111
  617.3–41, 130, 134-135
  617.4–25, 123-124
  617.5–12
Replay Protection 617.3–121, 134
Residential Mode 617.3–122
Resource Starvation Attack 617.2–94
Reverse Shell 617.1–130
RF Barriers 617.2–119
RF Jamming 617.2–90-91, 119
  Legality 617.2–91
RFcat 617.3–146
RFCOMM 617.4–12, 18, 45, 59
RFD 617.3–116
RFID 617.1–12, 18
  617.5–5-113
  Attack Surface 617.5–12
  Frequencies 617.5–6
  Improper Use 617.5–104, 107
  LF Tag 617.5–35
  Tag 617.5–5
    Active 617.5–7
    Passive 617.5–8-9
    Semi-Passive 617.5–8
  Technology 617.5–5
  Versus NFC 617.5–11
RFMON → Monitor Mode
RFPI 617.3–83
Roaming 617.2–20
  617.3–41
Rogue Aircraft 617.4–117
Rogue AP 617.3–43, 75
  617.4–121
  Analysis 617.1–100
  Identification 617.1–69
  Localization 617.1–112-119
Rogue Cellular Tower 617.4–122
Rogue RADIUS 617.3–63
Rogue Threats 617.1–11
  Types 617.1–92
Routing Filter 617.2–39
Routing Loop 617.3–120
Roximity 617.5–24
RP-SMA 617.1–23-24
RSN 617.2–130
RSSI 617.3–83
RT2800USB Driver 617.1–23
RT5372 Chipset (Ralink) 617.1–23
RTD 617.5–120
RTL-SDR 617.1–26
  617.4–101, 120, 125
RTL8187 617.1–78
RTL8812AU 617.1–51
RTLS → Real-Time Location System
RTS → Ready To Send
Runtime Errors 617.2–11
RZUSB 617.3–127-128

S

SAE → Simultaneous Authentication of Equals
SAFER+ 617.4–20, 25
Salt 617.3–25
Scapy 617.2–105, 131-139
  617.4–84
  Useful Functions 617.2–135-139
SCO 617.4–15
Scope 617.1–128, 151
  617.2–47, 141
SDP 617.4–44
SDR 617.1–19
  617.4–98-129
  Block Diagram 617.4–99
  In PenTest 617.4–102
  Platform 617.4–103
  Selection 617.4–108
  Threat 617.4–101
  Visualization 617.4–109-114
SDR# 617.1–26
  617.4–109, 112
SE 617.5–126-127
Security Through Obscurity 617.3–86
Selective Transmission 617.1–49
Self-Signed Certificate 617.3–69
Sensitive Information Storage 617.4–40
Sensor Network Analyzer 617.3–130
SEP 617.3–125
SEQN 617.4–14
Sequential Customer Number 617.2–11
Service Theft 617.2–12-13
Session Hijacking 617.2–15
Shared Key 617.2–68
Shikata Ga Nai 617.2–56
Short-Range Attack 617.2–116
Sidejacking 617.2–24-27
Siemens APOGEE 617.3–112
SIG 617.4–5, 21, 53
Signal Analysis 617.1–112-113
Signal Strength Capture 617.1–83
Signal-to-Noise Ratio 617.1–112-114
  617.4–93
Simultaneous Authentication of Equals 617.3–45
Site Mirroring 617.2–22
SKKE 617.3–123
Smart Card 617.1–12
  617.5–9-10, 70, 119
  Reader/Writer 617.1–25
  Versus NFC 617.5–118
Smart Energy 617.3–125
SNA → Sensor Network Analyzer
Snap Length 617.1–56
SNEP 617.5–125
Sniffing 617.1–8
  617.2–131
  Modes 617.1–35
SNR → Signal-to-Noise Ratio
SOC 617.4–10, 31

Soft AP 617.1–98, 142
617.3–52
Software Install 617.2–54
Software Update 617.2–54
Sony FeliCa 617.1–25
SparkFun 617.3–139
Spoofed AP 617.2–96
Spoofed Beacon Frame 617.2–104
Spoofed Provider 617.2–20
Spoofed Response 617.2–34
SQLite 617.1–75, 77
- ESSID 617.1–77
- WEP Encryption 617.1–75
Squid 617.2–52, 57
SRES 617.4–47
SSID Information Element 617.2–128
STA-STA Attack 617.2–39
Standard Security Model 617.3–122
STK 617.4–57
Stolen Device 617.3–38
Stream Cipher 617.2–68
617.3–88, 142
617.5–83
Stress Test 617.2–95
Strong Authentication 617.2–32
Strong Encryption 617.2–32
Strong Passphrase 617.3–47
SunPass 617.5–18
Supplicant Behavior 617.3–64-67
- Android 617.3–67
- IOS 617.3–66
- Windows 617.3–64-65
SWAT 617.1–22
Synchronization Word 617.4–33-34

T

Tag Emulation 617.5–101
TC 617.3–116
TDD 617.4–7, 14
Team deDECTed 617.3–89
Telemetry 617.5–8
Temporal Key Integrity Protocol → TKIP
THGR810 617.4–126
Third-Party Stack 617.3–142
Three-Legged Stool 617.1–9
Throttling 617.3–35
Time Period 617.5–58
TJX 617.1–20
TK 617.4–57, 82
- Recovery 617.4–82
TKIP 617.1–10
617.2–65, 111-115
617.3–7, 12, 41, 56
- 4-Way Handshake 617.3–57
- Replay Attacks 617.2–112, 114-115
- Sequence Counter 617.2–112
TLS 617.3–54
- Tunnel 617.3–55, 58
TNF 617.5–119-121
- Well-Known 617.5–121
To-DS Bit 617.2–40
Toolkit 617.1–22
Tortoise and Hare 617.4–17
Transmit and Pray 617.2–106
Transponder 617.5–5
Triangulation 617.1–116-117, 119
TSC → TKIP Sequence Counter
TTL 617.3–120
TxBF 617.1–49

U

UAK 617.3–87-88
- Recovery 617.3–101
UAP 617.4–13-14
- Discovery 617.4–36
UID 617.5–100-101, 130
- Impersonation 617.5–102
Ultra Mobile PC 617.1–114
UMPC → Ultra Mobile PC
Unauthenticated Services 617.2–9
Unauthorized Access 617.1–7
Unauthorized Network 617.1–7
Unicast ARP 617.2–44
Unintended Rogue 617.1–92, 94
Untrusted Certificate 617.3–68
USB
- Timing Issue 617.1–28
User Paradigm 617.1–7

V

VLAN 617.2–5, 39
VNC 617.1–137
VoIP 617.3–83
VPN 617.1–151
617.2–28
Vulnerability Discovery 617.2–126

W

Wardriving 617.1–67, 100
617.4–39, 94
Warwalking 617.1–100-108
- Tools 617.1–105
Waterfall 617.4–114
WAVE 617.5–18
Weak Protocols 617.2–18
Weakest Link 617.2–32
Weather Sensor 617.4–126
WEP 617.1–12, 134, 149
617.2–65-66
617.3–134
- Advanced Analysis 617.1–69
- Cracking 617.1–137
- Decryption 617.2–72

- Display Filter 617.1–64
- Encryption 617.2–71
  - Coverage 617.2–66
- Failures 617.2–75
- Key Recovery 617.2–74
- Passive Cracking 617.1–69

WEP Bit 617.1–64

WIDS → WLAN IDS ....

Wiegand Protocol 617.5–41, 43

WiFi
- Management Information 617.1–39

WiFi Blackout 617.2–116

WiFi Protected Access → WPA(2) ....

WiFi Protected Setup 617.3–30-37, 47
- Detection 617.3–34
- PIN Authentication 617.3–32

WiGLE 617.4–9

WikiBeacon 617.5–32

Windows Bridging 617.1–95

Windows Connect Now 617.3–32

Windows Hosted Network 617.1–96

Windows ICS 617.2–49

Windows Native WiFi 617.3–63

Windows WiFi Connection Creation 617.1–139

Windows Wireless Data Collection 617.1–141

Wired-Side Analysis 617.1–98-99

Wireless Card Firmware Weakness 617.1–10

Wireless Discovery 617.1–135

Wireless-Side Analysis 617.1–100-120

WLAN IDS 617.1–68, 108
.... 617.2–60, 102, 119
.... 617.3–75
- Sensors 617.1–108
- Triangulation 617.1–117

WLAN IPS 617.1–109
.... 617.2–102

WPA2 .... 617.2–29
.... 617.3–7-47
- -Enterprise 617.3–38, 53, 56
  - Key Distribution 617.3–57
- -PSK 617.1–96, 134, 149
  .... 617.3–7, 16, 38, 136
  - Beacon 617.3–17-18
  - Key Recovery Attack 617.1–137
  - Passphrase 617.3–19
  - PMK Derivation 617.3–9, 25
  - PSK Selection 617.3–20
  - PTK Derivation 617.3–10-11
  - Securization 617.3–47
- 4-Way Handshake 617.3–13-15, 41

WPA3 .... 617.3–45-46

WPS → WiFi Protected Setup ....

Writable Cards 617.5–93

X

XMPP 617.1–30

XOR 617.2–67

Y

YDI 617.2–116

Z

Z-Wave 617.1–12
.... 617.3–144-145
- Frequencies 617.3–144

ZC 617.3–116

ZED 617.3–116

Zigbee 617.1–12, 16
.... 617.2–65
.... 617.3–108-148
.... 617.4–53
- 4-Way Handshake 617.3–123
- Background 617.3–115
- Bridging 617.3–118
- Capture Decryption 617.3–141
- Frequency 617.3–115
  .... 617.5–6
- Key Provisioning 617.3–123, 142
- MAC Layer 617.3–118-119
- NWK Layer 617.3–120
- PHY Layer 617.3–117
- PRO 617.3–116, 121, 123
- Router Bridging 617.3–118
- Security 617.3–125
  - Modes 617.3–122
- Thoughts 617.3–142
- Topologies 617.3–117

ZR 617.3–116