

Chapter 4: Address Resolution Protocol (ARP)	
4.1. Introduction	84
4.2. ARP	84-87
4.3. ARP For Reconnaissance	87-88
4.4. ARP Vulnerabilities	89
4.5. ARP Poisoning Attack	90-97
Chapter 5: Domain Name System (DNS)	
5.1. Introduction	98
5.2. What Is DNS?	98-99
5.3. What Is Domain Name?	99-100
5.4. How DNS Works	101-102
5.5. Local Hostname Resolution	102-104
5.6. Roles Of DNS	104-105
5.7. Zone Files	106
5.8. DNS Records	106-110
5.9. Checking DNS Queries & Responses	110-116
5.10. DNS Vulnerabilities	
Chapter 6: Server Message Block (SMB)	
6.1. Introduction	117
6.2. What Is SMB?	117-118
6.3. LM Authentication System	118
6.4. NTLM	118-119
6.5. Kerberos	119-120
6.6. SMB Vulnerabilities	120-121
6.7. Samba & File Sharing	121-128
Chapter 7: SMTP	
7.1. Introduction	129
7.2. What Is SMTP?	129-131
7.3. How SMTP Works	131-132
7.4. Vulnerabilities Of SMTP	132
7.5. User Enumeration On SMTP	133-137
Chapter 8: SNMP	
8.1. Introduction	138
8.2. What Is SNMP?	138-139
8.3. Attacking SNMP	139-145

မာတိကာ	
ခေါင်းစဉ်	အကြောင်းအရာ
Chapter 1: TCP/IP	
1.1. Introduction	9
1.2. What is Network?	9-12
1.3. IP Addresses	12-15
1.4. IP Ranges	15-19
1.5. DHCP	19-20
1.6. NAT	20-21
1.7. Port	22-23
1.8. Protocol	24
1.9. Internet Protocol	24-26
1.10. Transmission Control Protocol	26-29
1.11. TCP Three-way Handshake	29-31
1.12. OSI Model	31-37
1.13. OSI Layers & Attacks	37-39
Chapter 2: Subnetting & CIDR Notation	
2.1. Introduction	40
2.2. What is Subnetting	41-42
2.3. Subnet Masks	42-43
2.3. Practical Subnetting	43-45
2.4. Block Size	45
2.5. CIDR Notation	46-47
2.6. Wildcard Mask	48
2.7. CIDR Table	49
2.8. Private & Special IPv4 Addresses	49
2.9. All IP Addresses For All Classes	50
2.10. Bogon IP Address	50
Chapter 3: Network Analysis	
3.1. Introduction	51
3.2. What is Network Analysis?	51-52
3.3. Hackers Vs Network Administrators	52-53
3.4. Network Sniffers	53-54
3.5. Promiscuous Mode	55
3.6. TCP Dump	55-61
3.7. Wireshark	61-67
3.8. Practical Analysis With Captured Pcap	68-83

Chapter 9: HTTP	
9.1. Introduction	146-147
9.2. HTTP/3	147-148
9.3. HTTP Requests & Responses	148-149
9.4. HTTP Methods (Or) HTTP Verbs	150-154
9.5. HTTP Headers	155-156
9.6. HTTP Cookies	157
9.7. HTTP Status Codes	157-161
9.8. HTTPS	161
Chapter 10: WiFi Networks	
10.1. Introduction	162
10.2. IEEE 802.11	162-163
10.3. IEEE 802.11 Security Protocols	163-164
10.4. What Is Forward Secrecy	165
10.5. Needs For WiFi Hacking	166-167
10.6. Adapters For WiFi Hacking	167-170
10.7. Knowing Wireless Interfaces	170-173
10.8. WiFi Frames	173-174
10.9. Hacking WiFi	175-179
10.10. Evil Twin Attacks	179-185
10.11. PMKID Attack	186-192
Chapter 11: Bluetooth Networks	
11.1. Introduction	193
11.2. What Is Bluetooth?	193-194
11.3. Bluetooth's Pairing Systems	194-195
11.4. Security Modes For Bluetooth Devices	195-196
11.5. What Is Bluetooth Hacking?	1196
11.6. Bluejacking	196-198
11.7. Bluesnarfing	198-199
11.8. Bluebugging	199-202
11.9. Blueborne Attack (CVE-2017-0785)	202-205
11.10. KNOB Attack (CVE-2019-9506)	206-208
11.11. BIAS Attak (CVE-2020-0022)	208-210
11.12. Other Attacks, CVEs & Exploit Frameworks	211
Chapter 12: Automobile Networks	
12.1. Introduction	212
12.2. Automobile Networks Architecture	213-214
12.3. Controller Area Network (CAN)	214-217
12.4. OnBoard Diagnostic (OBD) - II Connector	217-222
12.5. CAN Utilities	223
12.5. Studying With Virtual CAN Network	224
12.6. CAN Simulators	225-229

12.8. Testing CAN Utilities	229-232
12.9. Key Fob Hacking	232-240
Chapter 13: SCADA/ICS Networks	
13.1. Introduction	241-243
13.2. ICS Communication Protocols	243-249
13.3. Testing Modbus	249-253
Chapter 14: Radio Frequency Networks	
14.1. Introduction	254
14.2. Security Concerns In Radio Frequency Communications	254-256
14.3. Hardware Devices	256-261
14.4. What Is SDR?	261-263
14.5. Testing Aircraft Communication	263-265
References:	267