

Table of Contents

Module 1: Cyber Security in Networks.....	1
Network Security Fundamentals.....	5
Principles of Network Security.....	7
Security Terminologies.....	9
Security Components.....	11
Security Policies.....	13
Security Procedures.....	15
Physical Security.....	17
Securing Devices.....	20
Securing Applications.....	23
OS Updates.....	24
Advanced TCP/IP.....	25
Communication Protocols in Depth.....	26
Network Layers Attacks.....	28
The Process of DHCP and APIPA.....	30
Cryptograpy.....	32
Encryption Algorithms.....	33
Cryptography Tools.....	34
Heartbleed and Poodlebleed.....	35
Public Key Infrastructure (PKI).....	37
Encrypting Services.....	39
Packet Structure and Analysis.....	41
Capture and Identify IP Datagrams.....	42
Capture and Identify ICMP Messages.....	44
Capture and Identify TCP Headers.....	46
Capture and Identify UDP Headers.....	48
Error Detection and Error Handling.....	49
Packet Fragmentation.....	50
Module 2: Advanced Network Awareness.....	51
Analyzing The Network.....	53
Preforming Web-Screenshots using NMAP.....	54
Detecting Service Changes using Shodan CLI.....	55
Launching NSE to Detect Possible vulnerabilities.....	57
The Methodology of Finding Hosts in the Network.....	58
Capturing Fake MAC and IP Addresses.....	60



Spying the Local network using Driftnet and Urlsnarf	62
Hunting for Rootkits with windbg.....	64
Analysis of Leaked Network Security Information.....	66
The OSINT Framework	67
Social Engineering	70
Using The-Harvester to Find Exposed Private Emails.....	72
Private Domain Hunting using Amass	74
The WHO-IS and Dmitry Tools.....	75
Phishing Attacks	76
DNS Poisoning.....	77
Network Security Threats	80
Virus	81
Malware.....	82
Trojans	84
Worm	85
Spyware.....	86
Payloads.....	87
Buffer Overflows	88
Module 4: Hardening the Network	90
Routing and Network Components Hardening	91
Static ARP and DHCP Entry to Prevent Poisoning.....	92
Firewall Components	94
Proxy Server	95
Counter-measuring attacks	97
Designing and Configuring an IDS	100
Constructing Honeypots.....	102
Session Hijacking Counter-Measures	104
Detecting Active Sniffing.....	106
SMB Hardening against Enumerations.....	108
Identifying Log Tampering.....	109
Working with VPNs.....	110
VPN Fundamentals.....	111
IP Security Protocols.....	114
Design and Architecture.....	116
VPN Security.....	118
Configure your VPN.....	120



Module 4: Linux and Windows Hardening	121
Securing Linux.....	122
Key Concepts Linux	123
Administration and Security	125
Linux Network Files	127
Linux Network Process	130
Key Linux Network Commands	132
Hardening Linux	133
Network File System and Linux	136
Network Information Service and Linux	137
Securing Windows.....	140
Windows Fundamental Security	141
Windows NT Resource Security.....	143
Windows Infrastructure.....	145
Windows Authentication.....	147
Windows User and Group Security	148

