

Table of Contents

Networking	4
IP Address	4
IP Components.....	5
Default Gateway	5
Data Communications	7
LAN – Local Area Network	8
WAN – Wide area Network.....	8
Protocol.....	8
The OSI Model	9
Analyzing Packets Using Wireshark and Tshark	11
Wireshark.....	11
Tcpdump	14
Types of communications	16
TShark	18
Packet Data (-x and -V and -P)	21
Capturing Packets	21
Capture filters	22
Display Filters.....	22
Exporting Data	22
Filtering Live Capture.....	23
Fetch Filters (-f).....	23
File Extraction	23
Automation	23
Windows Firewall.....	24
Rules Based.....	24
Policy Based Firewalls.....	25
Next Generation Firewall (NGFW).....	26
Benefits of Next-Generation Firewalls	27
Linux Firewall	27
IP Tables	27
Checking Current IP Tables Status	28
Defining Chain Rules	28
Dropping All Other Traffic.....	29
Deleting Rules.....	29
Persisting Changes	29
IDS & IPS	29
Differences Between IDS & IPS	29
Network-Based IDS (NIDS)	31
Host-Based IDS (HIDS)	33



Introduction to pfSense	35
What is pfSense?.....	35
Interface Naming Terminology.....	35
Installation and Configuration	36
Configuring the Machine	37
Introduction to Snort IDS	51
Uses of Snort Rules	51
Configuring Snort and Detecting Attacks	52
Introduction to Scapy	57
Using Scapy Modules.....	58
Packet Analysis & Traffic Malware Analysis.....	61
The Digital Investigation Process	64
Forensics - Basic Principles.....	64
The Investigation Process	64
Windows OS.....	64
FTK Imager.....	64
AppData	65
EFS Encryption	65
NTFS File System	66
Volatility Framework.....	70
Requirements.....	70
Command Syntax	70
Investigation Process.....	70
Image Identification	71
Process and DLLs	71
Networking Modules.....	73
Working with Registry	75
Additional Information Gathering.....	77
Monitoring the Systems.....	79
Attacks from Inside the Network	79
Types of Attacks:.....	79
Intercept Packets from Router with Arpspoof	81
Performing the Password Attack:	86
Attacks from Outside the Network.....	87
Denial of Service	88
Phishing Attack	90



Types of Phishing Attacks	90
---------------------------------	----

