

Table of Contents

Chapter 1 - Nmap overview & networking basics.....	6
What is Nmap?.....	7
OSI model.....	8
MAC address.....	10
TCP/IP suite of protocols.....	12
IP address.....	12
Private IP addresses.....	14
Transmission Control Protocol (TCP).....	15
User Datagram Protocol (UDP).....	16
TCP and UDP ports.....	17
IPv4 header.....	19
Chapter 2 - Nmap installation.....	22
Install Nmap on Windows.....	23
Install Nmap on Linux.....	25
Install Kali Linux.....	26
Chapter 3 - Nmap basics.....	37
Start Nmap.....	38
Determine service version.....	39
Specify port ranges.....	40
Specify IP address range.....	42
Discover if a host is online.....	43
Discover hosts with a TCP SYN ping scan.....	43
Disable ping sweep.....	44
Determine operating system.....	44
Chapter 4 - Zenmap.....	48
What is Zenmap?.....	49
Example Zenmap scan.....	50

Interpret scan results.....	52
Chapter 5 - Advanced usage.....	59
Packet trace.....	60
Timing options.....	60
The reason flag.....	62
Adjust delay between probes.....	63
Save Nmap's output.....	63
UDP scan.....	65
Port states.....	65