1.0 Redes Internas Y Externas. 3
1.1 Introducción. 3
1.2 Redes. 3
1.2.1 Red Corporativa/Internet. 3
1.2.2 Protocolos. 5
1.2.2.1 Modelo OSI. 6
1.2.3 Enrutamiento. 8
1.2.4 Protocolos De Nivel Superior: HTTP y SMB. 8
1.2.5 Wireshark Analizando Trafico De Red. 9
1.2.5.1 ¿Desde Donde Ejecutar Wireshark? 9
1.2.5.2 Introducción A Wireshark. 9
1.2.5.3 Filtros En Wireshark. 13
1.3 Buscando hash en paquetes SMB. 15
1.3.1 Autenticación NTLMv2. 18
1.3.1 Taller Analizar Red 1. 24
1.4 Buscando en paquetes HTTP Y TCP. 25
1.4.1 Viendo La Información De Un Paquete. 26
1.4.1.1 Viendo Paquetes Imágenes De Tipo Byte. 29
1.4.2 Taller Analizar Red 2. 32
1.5 Detectando Ataques A Redes. 33
1.5.1 Ataques ARP. 33
1.5.1.1 Protocolo ARP. 33
1.5.1.2 En Que Consiste El Ataque ARP. 34
1.5.1.3 Como Detectarlo Con WiresHark. 34
1.5.2 IP Protocol Scan. 36
1.5.3 ICMP Barrido De Ping. 36
1.5.4 TCP Barrido De Ping. 37
1.5.5 UDP Barrido De Ping. 37
1.5.6 Resumen Tabla Detección De Descubrimiento De Host. 37
1.5.7 TCP SYN / Stealth Scan (Buscando Equipos Modo Silencioso). 38
1.5.8 TCP Connect() Scan (Buscando Puertos). 38
1.5.9 TCP Null Scan (Firewall). 39
1.5.10 TCP FIN Scan (Firewall). 39
1.5.11 Xmass Scan (Firewall). 40

1.5.12 UDP Port Scan. 40
1.5.13 Resumen Tabla Scaneos Detección De Puertos. 41
1.5.13 Ataque Vlan Hoping. 42
1.5.14 Unexplained Packet Loss. 42
1.5.15 Resumen Tabla De Ataques A Redes 42
1.5.16 Exfiltracion De Datos. 43
1.5.16.1 Exfiltracion Por HTTP. 43
1.5.16.2 Exfiltracion Por SMTP. 43
1.5.16.3 Exfiltracion Por DNS. 43
1.5.16.4 Exfiltracion Por ICMP 44
1.5.16.5 Exfiltracion Por IPV6. 44
1.5.17 Ataque A Redes Wireless. 46
1.5.17.1 Deautenticacion De Cliente. 46
1.5.17.2 Disociación De Cliente. 47
1.5.17.3 Fake AP Beacom Flood. 48
1.5.17.4 Autenticación Denegación De Servicio. 49
1.5.18 Resumen Tablas De Ataque A Redes Wireless. 50
1.5.19 Taller Analizar Red 3 50