

Índice

Capítulo V

Análisis	13
1. Periodo de Prueba	13
2. Puertos y Servicios: Carácter y Personalidad	14
NMAP: Mapeador de Puertos & Servicios	15
Conversando Bien de Cerca	15
Método nativo desde Windows	15
Método nativo y gráfico desde Windows	19
Herramienta gráfica de terceros desde Windows	20
Exportar para Transformar en Adornos	24
Guardar y clasificar al estilo Carpe-Sano	28
Método nativo desde Linux	29
NMAP se Une a la Cercana Conversación	32
Negociación a 3 Bandas	33
NMAP y el Decorado de su Salida	35
Manteniendo una Prudente Distancia	38
3. Preliminares: Configuración Técnicas Sniffing	38
La Colección de Pines de los Certificados en Móviles	39
HTTP Strict Transport Security	40
HPKP HTTP Public Key Pinning	40
VideoMetraje	41
Editor de vídeo	43
Insertando un cronómetro	43
Técnica - Sniffing en el Propio Dispositivo	44
Técnica - Test Access Port	48
Windows	48
Linux	49
Técnica - Machine-in-the-Middle	51
Windows	51
Linux	52
Linux & Wi-Fi & Bridge	53
Windows & Wi-Fi & Bridge	56
Técnica - HotSpot: El Punto “Caliente”	58
“Punto Rápido” en Windows	58
“Punto Lento pero Seguro” en Windows	59
Modo Gráfico en Linux	60

Técnica - Port Mirroring: Los Espejos del Switch.....	62
Técnica - Bluetooth: La suciedad de entre los Azules Dientes	63
Teléfonos Pixel de Google.....	64
Resto de Terminales Android.....	69
Técnica - F12 – DevTools	71
Técnica - PROXY Explicito.....	72
Genera tu propio CA.....	73
Convirtiendo en formato base64.....	74
Instalación de certificado: WINDOWS	75
Instalación de certificado: KALI LINUX	76
Instalación de certificado: ANDROID.....	77
Instalación de certificado: FIREFOX	80
Configuración de servidor Proxy: WINDOWS	81
Configuración de servidor Proxy: KALI LINUX	82
Configuración de servidor Proxy: ANDROID.....	83
Configuración de servidor Proxy: FIREFOX	84
Importando el CA personalizado en Burp	85
Arrancando Burp	87
Dejando escapar a TLS.....	88
Técnica - PROXY Implícito.....	89
4. La Confianza da Datos.....	91
Análisis con Wireshark	93
Sacar la mejor Tajada.....	93
Buscar un Protocolo en un Océano.....	96
Conversaciones Públicas	97
Varios Aliados para un mismo Objetivo	106
El Laberinto de los Certificados	107
¿Quién es Quién?.....	112
El Alma del Host que no supo Encontrar la Luz	119
El Consumo de Tiempo de los Hosts marcado por un Reloj	120
Gráficos de Entrada y Salida en Wireshark	123
Perfilando a Wireshark para Adaptarse a otros Climas.....	127
Bluetooth y los Débiles Dientes [Low Energy].....	132
Análisis con DevTools	140
Extremidades de las DevTools.....	141
Revelando el Escondite de los HOSTS	150
El árbol Genealógico de los Iniciadores	153
Congelación de las Peticiones	153
Análisis con Burp Suite [Community Edition]	154
Extremidades de Burp Suite	154
Errores que delatan a HOSTS.....	156
Orientándose con el Mapa del Sitio.....	158

Extracto de Peticiones.....	159
Regreso al Futuro con Libre/Open Office	160
Guía de Primeros Auxilios para Mitmproxy	163
Orden en la Sala de Mitmproxy.....	165
Filtrado de Peticiones	166
Poner el Trabajo a Salvo	167

Capítulo VI

Cebolla Cibernética169

1. Conservando una Allium Cepa169

SIEMpre en Alerta.....	170
Visibilidad de Host: Host Intrusion Detection System [HIDS].....	171
Visibilidad de Red: Network Intrusion Detection System [NIDS].....	172

2. Trituradora de Archivos de Captura [PCAP]s173

Security Onion	173
Estructura.....	174
Eval-uando en un Hipervisor	176
Diagrama Arquitectónico.....	176
Requisitos Software	178
Requisitos Hardware.....	179
Instalando VirtualBox	180
Crear la VM [Máquina Virtual]	180
Configurar la VM [Máquina Virtual].....	182
Pelando la Cebolla	184
Pochando la Cebolla	193
Los PCAPs (se) Importan	200
Prevenir Problemas “Digietales”.....	204
[Alerts] Alertas.....	204
[Dashboards] Paneles de Control.....	205
[Dashboards] Muestreo/Filtrado de un PCAP en particular	207
[Alerts] Detalle de las Alertas Medias	210
[Cases] Creación de un Nuevo Caso/Incidente	212
[Hunt] Buscando posibles Daños.....	214
[PCAP] Desenmascarando el Archivo.....	215
[CyberChef] Pasando a Cocina.....	216
[Hunt] Importando Eventos en Relación al Caso	219
[Dashboards] Perspectiva de Todos los Ficheros	220
[Cases] Segunda/o Análisis/Revisión	220
[Hunt] Segundas Opiniones en Análisis	224
[VirusTotal] Análisis del Hash de un Archivo	225
[Alerts] Otras Alertas de la misma “Familia”	226

[Cases] Explorando la Segunda Alerta	227
[Hunt] Con Intención de Enviarse a Análisis Detallado	229
[PCAP] Esclareciendo la Sospecha	229
[Dashboards] Re-Confirmar la Auto-Firma	230
3. Datos de Buen Ver	232
Extracción de la Tormenta, Dejando hueco a la Lluvia	233
Protocolos Reunidos.....	237
Hosts con Nombres y Apellidos.....	242
SobreNombres de los Hosts	246
Nombres Sujetos a Certificados	247
Las Mentiras Tarde o Temprano se Descubren	249
Invirtiendo Tiempo para crear un Reloj de Hosts	252
MapaMundi de las Conexiones.....	255
4. Haciendo Pasar por el Aro a Todos los Dispositivos.....	256
Convenio de Nombres para asignación a los Dispositivos: HostNames.....	257
Direccionamiento IP como Identificador Vital.....	258
DHCP: Gestor de Reserva de “Mesas” para las IP	260
De WiFi a WiFi y Instalo AP para Conectarte	261
Balizas de Estado: SysLog.....	265
Configuración HIDS en Security Onion	265
SysLog en Windows 10	267
SysLog en DSM 7 (de Synology).....	271
Viendo Resultado de los Testeos en Security Onion	273
Encasillando a sus Puertos	274
Configuración del Mirroring en Switch	277
5. Día D (Dis-Positivo)	278
Escenario de Juego.....	278
Revisión de IP's Asignadas	280
IP's Vampíricas.....	283
Alertad@s.....	285
Alerta Roja.....	286
Relojes Europeos	288
Alerta Amarilla	295
Alertas Inofensivas	298
Intrusas Perpetuas: IP en Rango no estipulado	298
Comunicación Lateral entre sin-Vergüenzas.....	302
El Atracador de Certificados	302
Perdona... ¿Como te llamas?.....	307
Mi Nombre es... ¡Encantado/a!.....	310
Do you Speak “My Language”?	311
ICMP No es Solo ping	311
Tráfico HTTP por Senderos Desconocidos.....	313

HTTP sin Identidad.....	315
IP Vistiendo a la 6a Moda	317
Llamando a los Vecinos de la 6a sin Importar la Hora	317
Los Múltiples usos de ICMP en IPv6	319
La Afán por Saber los Nombres de los Vecinos de la 6a	320
Puertos Residuales en IPv6.....	321
Secretos entre los Vecinos de la 6a	322
ICMP versión 6 en Unicast.....	322
Desesperación por Tener una IPv6 Alquilada.....	323
DNS sin Nuestro Permiso	323
Broadcasters en Puertos Creativos/Originales [Classic IP]	325
El Espía del Registro del Sistema [SysLog]	329
Errores Seguros, pero con Mala Salud	330
Advertencias ¡No las Ignore!	331
Resto de “Suc_i_esos”	331
Malas Prácticas detectadas por Dr. Zeek.....	331
Certificados que se toman la Justicia por su Cuenta.....	333
Comunicación Común con el Exterior.....	334
HTTP: Viajando sin Protecciones.....	334
HTTPS: Viajando en Secreto.....	338
HTTPS: Exposición del Rostro	338
HTTPS: Ocultación del Rostro.....	339
En busca de Extraños en el Extranjero	340
Países Visitados: Viaje a la Vuelta al Mundo	343
Devorador/a de Bits.....	344

Índice alfabético347

Índice de imágenes355

Otros libros publicados.....369

