

Tabla de Contenido

Introducción	1
1. Antecedentes	7
1.1. Estudios Sobre IPv4	7
1.1.1. SSL Observatory	7
1.1.2. Internet Census	8
1.1.3. SHODAN	9
1.2. Escáner de Puertos	10
1.2.1. ZMap	10
1.2.2. Masscan	11
1.2.3. Comparación	12
1.3. Nuevos Estudios Sobre IPv4	13
1.3.1. Certificados HTTPS	13
1.3.2. Vulnerabilidad: Heartbleed	15
1.4. Censys	16
2. Monitoreo Activo	18
2.1. Metodología	18
2.1.1. Detección de Puertos	19
2.1.2. Escáner de Protocolos	19
2.1.3. Procesamiento de Metadatos	19
2.1.4. Análisis y Agregación	19
2.2. Restricciones	20
2.3. ¿Qué IP Escaneamos?	20
2.3.1. Atlas RIPE	20
2.3.2. Geo-IP	21
2.3.3. Top Level Domain	21
2.3.4. Conclusiones	22
2.4. Equipamiento y Conexión de Red	23
2.4.1. Equipo	23
2.4.2. Conexión a Internet	23
2.4.3. Seguridad	25
2.5. Elección del Escáner de Puertos	26
3. Protocolos	27
3.1. ¿Qué Protocolos Estudiar?	27

3.2.	Tipos de Consultas	28
3.2.1.	Consulta Estado del Puerto	28
3.2.2.	Consulta Estándar	29
3.2.3.	Consulta de Opciones Limitadas o Forzadas	29
3.2.4.	Consulta Maliciosa	30
3.2.5.	Resumen	30
3.3.	Protocolos Estudiados	31
3.3.1.	SSL/TLS	31
3.3.2.	HTTP	35
3.3.3.	HTTPS	37
3.3.4.	Email	38
3.3.5.	Bases de Datos	42
3.3.6.	Otros Protocolos	43
4.	Sistema de Escaneo	45
4.1.	Escáner de Protocolos	45
4.1.1.	Requisitos	45
4.1.2.	Método de Consultas	47
4.1.3.	Implementación	49
4.1.4.	Extensión	51
4.1.5.	Rendimiento	53
4.2.	Procesamiento de Metadatos	55
4.2.1.	Requisitos	55
4.2.2.	Implementación	56
4.3.	Análisis y Visualización	58
5.	Análisis de datos	61
5.1.	Descripción del Dataset	61
5.2.	Análisis de los Protocolos	62
5.2.1.	Puertos Abiertos	62
5.2.2.	HTTP	63
5.2.3.	Certificados	72
5.2.4.	E-mails	80
5.2.5.	SSH	83
5.3.	Métrica de Seguridad	84
5.3.1.	Metodología	85
5.3.2.	HTTP	85
5.3.3.	HTTPS Certificados	88
5.4.	Otros	91
5.4.1.	Redes Mal Configuradas	92
5.4.2.	Servicios Expuestos	92
	Conclusión	96
	Bibliografía	99
	Anexo A. Terminología	103

Anexo B. Datos	104
B.1. Cipher Suites	104
B.2. Análisis de Datos	108
B.2.1. HTTP	108
B.2.2. Cipher Suites	117

Índice de Tablas

1.	Descripción de las características del dataset creado a partir de la información recolectada a lo largo del trabajo de tesis.	6
1.1.	Comparación entre Nmap y ZMap	11
1.2.	Comparación entre ZMap y Masscan	13
2.1.	IPs asignadas a Chile.	22
3.1.	Resumen de la información que es posible recabar con las distintas consultas.	31
3.2.	Puertos escaneados asociados a botnets.	44
5.1.	Descripción de las características del dataset creado a partir de la información recolectada a lo largo del trabajo de tesis.	61
5.2.	Equipos agrupados por Sistema Autónomo, presentes en el escaneo del 15 de agosto y no el 22 de agosto.	66
5.3.	Equipos agrupados por Sistema Autónomo, presentes en el escaneo del 12 de septiembre y no el 5 de septiembre.	66
5.4.	Top-10 Sistemas Autónomos detectados en un escaneo al puerto 80. Escaneo del 17/10/2016	66
5.5.	Equipos con CentOS agrupados por AS, presentes en el escaneo del 18 de abril y no el 11 de abril.	69
5.6.	Equipos con CentOS agrupados por AS, presentes en el escaneo del 25 de abril y no el 2 de mayo.	70
5.7.	Equipos con Nginx agrupados por AS, presentes en el escaneo del 18 de abril y no el 11 de mayo.	71
5.8.	Equipos con Nginx agrupados por AS, presentes en el escaneo del 25 de abril y no el 2 de mayo.	71
5.9.	Sistema operativo utilizado por los equipos que proveen el servicio de POP3. (Total de equipos: 11555)	81
5.10.	Versión de mail server utilizado por los equipos que proveen el servicio de POP3. (Total de equipos: 11555)	82
5.11.	Sistema operativo utilizado por los equipos que proveen el servicio de POP3. (Total de equipos: 28963)	82
5.12.	Versión de mail server utilizado por los equipos que proveen el servicio de SMTP. (Total de equipos: 28963)	82
5.13.	Sistema operativo utilizado por los equipos que proveen el servicio de IMAP. (Total de equipos: 10994)	83

5.14. Versión de mail server utilizado por los equipos que proveen el servicio de IMAP. (Total de equipos: 10994)	83
5.15. Implementación del servidor SSH utilizado por los equipos que proveen el servicio de SSH. (Total de equipos: 25486)	84
5.16. Versiones de OpenSSH utilizadas por los equipos chilenos.	84
5.17. Versiones de Dropbear utilizadas por los equipos chilenos.	84
5.18. Sistemas autónomos correspondientes a los equipos con el protocolo SSH implementado.	85
5.19. Tabla de puntajes según la vulnerabilidad detectada.	85
5.20. Puntaje asignado a la presencia del campo server en el header	86
5.21. Puntaje asignado a la presencia del campo www-authenticate en el header	86
5.22. Puntaje asignado a la presencia del campo x-powered-by en el header	87
5.23. Evaluación de seguridad HTTP de los 10 ASN más grandes en Chile.	88
5.24. Puntaje asignado a la validez del certificado.	88
5.25. Puntaje asignado a la mayor versión de <i>SSL/TLS</i> soportada.	89
5.26. Limite al puntaje de equipos que soporten protocolos <i>SSL/TLS</i> inseguros.	89
5.27. Puntaje asignado según el algoritmo de hash utilizado.	90
5.28. Puntaje asignado al largo de la clave.	90
5.29. Evaluación de seguridad de los certificados de los 10 ASN más grandes en Chile.	91

Índice de Ilustraciones

1.	Usuarios de Internet en el mundo	2
2.	Cronología de vulnerabilidades de TLS/SSL	3
1.1.	Dispositivos en Carna Botnet	9
1.2.	Generación aleatoria de direcciones IP	13
1.3.	Tasa de parchado en el protocolo HTTPS	16
1.4.	Reemplazo de certificados en equipos vulnerables	16
2.1.	Metodología de Monitoreo Activo.	19
2.2.	Comparación de la precisión de MaxMind	21
2.3.	Conexión a Internet vía STI	24
2.4.	Conexión a Internet vía FCFM	24
2.5.	Número de conexiones activas, en el firewall del STI.	25
2.6.	Conexiones admitidas por el servidor de escaneo.	26
3.1.	Consulta DNS estándar.	31
3.2.	Obtención de Certificados.	33
3.3.	Conexión completa de HTTP.	37
3.4.	Conexión completa de HTTPS.	38
3.5.	Conexión completa SMTP.	40
3.6.	Conexión completa IMAP y POP.	41
3.7.	Error en login a PostgreSQL	43
4.1.	Método de Consultas: Realización de una consulta por equipo en la ejecución del programa.	48
4.2.	Método de Consultas: Realización de múltiples consultas por equipo en la ejecución del programa.	49
4.3.	Comparación de los métodos de consultas.	50
4.4.	Arquitectura del Escáner de Protocolos.	51
4.5.	Diagrama UML del módulo Reader.	52
4.6.	Diagrama UML de la interfaz Writable.	53
4.7.	Diagrama UML de la interfaz FileWriter.	53
4.8.	Diagrama UML de los datos recopilado por HTTP	53
4.9.	Rendimiento de Mercury en los protocolos HTTP y TLS.	54
4.10.	Arquitectura de implementada en Slurp.	57
4.11.	Vista del protocolo HTTP en www.osr.cl.	59
4.12.	Visualización de los sistemas operativos usados en el protocolo HTTP en www.osr.cl.	59

4.13. Visualización de toda la información obtenida sobre el equipo 192.80.24.4 en www.osr.cl.	60
5.1. Correlación de los puertos abiertos en cada IP detectados por ZMap	63
5.2. Número de equipos, con un puerto específico abierto.	64
5.3. Equipos detectados con el puerto 80 abierto (ZMap) y que sirven el protocolo HTTP correctamente (Mercury)	65
5.4. Campos del header utilizados por los servidores web. Aproximadamente 140.000 equipos por escaneo. (Escaneo del 17/10/2016)	67
5.5. Sistema Operativo utilizado por los equipos detectados con el puerto 80 abier- to. Aproximadamente 140.000 equipos por escaneo.	69
5.6. Servidor web utilizado por los equipos detectados con el puerto 80 abierto. Aproximadamente 140.000 equipos por escaneo.	71
5.7. Servidor web utilizado por los equipos detectados con el puerto 80 abierto. Aproximadamente 140.000 equipos por escaneo.	72
5.8. Validez de los certificados recopilados. Aproximadamente 55.000 equipos por escaneo.	74
5.9. Errores de validación de los certificados recopilados. Aproximadamente 55.000 equipos por escaneo.	74
5.10. Versión de TLS utilizada por el servidor, cuando el cliente soporta todas las versiones existentes del protocolo. Aproximadamente 55.000 equipos por escaneo.	76
5.11. Versión de TLS soportadas por los servidores.	77
5.12. Algoritmo de Hashing utilizado en el firmado de los certificados. Aproxima- damente 55.000 equipos por escaneo.	77
5.13. Tamaño en bits de la clave RSA utilizada por los certificados. Aproximada- mente 55.000 equipos por escaneo.	78
5.14. Equipos afectados con Heartblead. Aproximadamente 55.000 equipos por es- caneo.	80
5.15. Equipos que soportan cipher suites vulnerables a LogJam y Freak. Aproxima- damente 55.000 equipos por escaneo.	81
5.16. Evaluación de seguridad HTTP de los países sudamericanos	87
5.17. Evaluación de seguridad de los Certificados utilizados en los países sudameri- canos.	91
5.18. Login de cámaras expuestas a Internet.	93
5.19. Login de router wifi expuestas a Internet.	94
5.20. Login de impresoras expuestas a Internet.	94
5.21. Login del sistema de climatización de la Clínica Dávila expuesto a Internet. .	95
B.1. Equipos detectados por ZMap y Mercury en el puerto 443	108
B.2. Sistemas Operativos mayormente utilizados en los equipos detectados con el puerto 443 abierto	109
B.3. Servidores web más utilizados en los equipos detectados con el puerto 443 abierto	109
B.4. Tipos de dispositivos detectados con el puerto 443 abierto	110
B.5. Campos más utilizados en el Header de los equipos detectados con el puerto 443 abierto	110
B.6. Equipos detectados por ZMap y Mercury en el puerto 8000	111

B.7. Sistemas Operativos mayormente utilizados en los equipos detectados con el puerto 8000 abierto	111
B.8. Servidores web más utilizados en los equipos detectados con el puerto 8000 abierto	112
B.9. Tipos de dispositivos detectados con el puerto 8000 abierto	112
B.10. Campos más utilizados en el Header de los equipos detectados con el puerto 8000 abierto	113
B.11. Equipos detectados por ZMap y Mercury en el puerto 8080	113
B.12. Sistemas Operativos mayormente utilizados en los equipos detectados con el puerto 8080 abierto	114
B.13. Servidores web más utilizados en los equipos detectados con el puerto 8080 abierto	114
B.14. Tipos de dispositivos detectados con el puerto 8080 abierto	115
B.15. Campos más utilizados en el Header de los equipos detectados con el puerto 8080 abierto	116
B.16. Null Ciphers soportadas por los servidores.	117
B.17. Anonymous Null Ciphers soportadas por los servidores.	118
B.18. Anonymous DH Ciphers soportadas por los servidores.	119
B.19. Export 40 Ciphers soportadas por los servidores.	120
B.20. Low Ciphers soportadas por los servidores.	121
B.21. Medium Ciphers soportadas por los servidores.	122
B.22. 3DES Ciphers soportadas por los servidores.	123
B.23. High Ciphers soportadas por los servidores.	124