INFORME TECNICO DE SEGURIDAD CIBERNÉTICA DE OPERACIONES E INTELIGENCIA

Metrobank S.A.

Octubre, 2018

Tel: +1 609-651-4246
Tel: +507-836-5355

Info@glesec.com
www.glesec.com

CONFIDENCIAL

Tabla de contenido

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

Sobre este informe

Este informe es un complemento del Informe ejecutivo mensual de inteligencia y operaciones. El propósito de este documento es proporcionar información a nivel técnico y táctico, detalles y recomendaciones en la medida en que puedan resumirse. GLESEC procesa una gran cantidad de datos y no todos pueden presentarse en un formato de informe detallado. Para obtener más información, puede consultar los paneles de la GMP o, si es necesario, comuníquese con nosotros en los Centros de operaciones de GLESEC (GOC).

Confidencialidad

GLESEC considera la confidencialidad de la información de los clientes como un secreto comercial. La información bajo este contexto se clasifica como:

- Nombre e información de contacto del cliente
- Arquitectura del sistema, configuración, métodos de acceso y control de acceso
- Contenido de seguridad

Todo lo mencionado arriba es resguardado de manera segura de la misma forma como GLESEC resguarda su propia información confidencial.

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

Servicio Administrado de Vulnerabilidades (MSS-VM)

El Servicio Administrado de Vulnerabilidades (MSS-VM) permite a las organizaciones minimizar el riesgo de vulnerabilidades descubriendo rápidamente las debilidades, midiendo el riesgo potencial y la exposición, informando, proporcionando la información de remediación necesaria para mitigar esos riesgos de manera continua y facilitando la presentación de informes y el cumplimiento Con normativa y mejores prácticas.

Para este período y según el rango de direcciones proporcionadas por Metrobank S.A., el número total de hosts analizados es de 16, de los cuales en 11 de ellos se encontró al menos una vulnerabilidad. Estas vulnerabilidades se dividen en las siguientes severidades como se muestra en la siguiente tabla. Además, puede observar la puntuación de valor de riesgo de su organización según nuestras métricas, que ha aumentado en comparación con el mes pasado. La vulnerabilidad crítica en el host 190.34.183.131 continúa reportándose a su organización.

Total IP's Scanned	IP's Vulnerable
16	11

Risk Distribution				
Critical	High	Medium	Low	Total
1	5	35	20	61

According to the metrics:
RV= 0.273309426

The following values are to clarify RV:
RV=1 Points to every IP address in the infrastructure that are susceptible to attacks
RV=0 Points to no IP address in the infrastructure aret susceptible to attacks
RV=0.1 Point to 1/10 IP address in the infrastructure that are susceptible to attacks

Todas las vulnerabilidades encontradas en su organización pertenecen a las siguientes categorías:

Category	Critical	High	Low	Medium	Total
General	0	0	8	27	35
Misc.	0	1	9	6	16
Service detection	0	4	2	0	6
Windows	1	0	0	2	3
Web Servers	0	0	1	0	1

GLESEC www.glesec.com
USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

- General (57%).
- Misc (26%).
- Services Detection (10%).
- Windows (5%).
- Web Servers (2%).

Para detalles adicionales sobre estas vulnerabilidades se encontraron en Metrobank S.A, favor referirse a la sección de severidad del MSS-VM en la página 9.

Metrobank continúa presentando vulnerabilidades críticas (2%), altas (8%), medias (57%) y bajas (33%). Para este mes, el número total de vulnerabilidades disminuyó a 61.

Principales categorías que tienen más vulnerabilidades:

- General (57%) presenta en su mayoría vulnerabilidades de tipo SSL, como las suites de cifrado de fuerza media y el certificado SSL no confiable. Estos representan un nivel medio de severidad.

- Misc. (26%) presenta las principales vulnerabilidades de tipo: SSH Server CBC Mode Ciphers Habilitado, Logjam representa un bajo nivel de severidad y SSH soporta algoritmos débiles, SSL / TLS FREAK y DROWN, el Terminal Services no usa NLA y el nivel de cifrado es Medio o Bajo representa Un nivel de severidad media.
- Service Detection (10%) presenta principalmente el tipo de vulnerabilidad: la detección de los protocolos SSL versión 2 y 3 representa un alto nivel de severidad; y también presenta SSL Anonymous Cipher Suites Supported, que tiene un bajo nivel de severidad.

- Windows (5%) su principal vulnerabilidad es MS15-034: Una vulnerabilidad en HTTP.sys podría permitir la ejecución remota de código (3042553) (verificación sin credenciales) representa un nivel de riesgo crítico

- Web Servers (2%) presenta encabezado HTTP puede revelar dirección IP interna esta vulnerabilidad representa un nivel de resgo bajo.

De todos los tipos de vulnerabilidades mencionados anteriormente, los que se presentan con frecuencia son los paquetes de cifrado SSL de potencia media compatibles (15%) y el certificado SSL no se puede confiar (8%).

Entre las vulnerabilidades que presentan un nivel de gravedad crítica y alta tenemos:

- La vulnerabilidad de HTTP.sys permite la ejecución remota de código (3042553) (verificación sin credenciales). Existe una actualización de seguridad que se considera fundamental para todas las ediciones compatibles de Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1 y Windows Server 2012 R2. Esta vulnerabilidad se sigue presentando en el host 190.34.183.131.

- La vulnerabilidad de detección del protocolo SSL versiones 2 y 3 se considera de alta severidad y se presenta en los hosts 190.34.183.142, 190.34.183.149, 190.34.183.154 y 190.34.183.152.

Los 4 puertos considerados más vulnerables para este período fueron 443 (HTTPS), 3389 (RDP) y 22 (SSH) y 80 (HTTP). Esto se debe al hecho de que se encontraron muchas vulnerabilidades relacionadas con ellas y que la mayoría se clasifica en un nivel de gravedad medio, excepto en el puerto 80 que tiene un nivel de gravedad crítico.

A continuación, se muestran los hosts más vulnerables para estos puertos:

- 443 (HTTPS) La mayoría de los hosts son vulnerables por este puerto, entre ellos tenemos: 190.34.183.139, 190.34.183.142, 190.34.183.152, 190.34.183.154, 190.34.183.132, 190.34.183.91 y 190.34.183.90.

- 22 (SSH) Las vulnerabilidades presentadas por este puerto son: Algoritmos débiles SSH admitidos, Cifrados en modo CBC del servidor SSH habilitados y Algoritmos MAC débiles SSH habilitados. Los hosts afectados son 190.34.183.148 y 190.34.183.142.

- 3389 (RDP) Las vulnerabilidades que presenta este puerto son: Debilidad del hombre en el medio del Servidor de Protocolo de Escritorio Remoto de Microsoft Windows, Servicios de Terminal Server no solo para NLA, el Nivel de Cifrado de Servicios de Terminal Server es Medio o Bajo. El host afectado es 190.34.183.139.

- 80 (HTTP) El host que presenta vulnerabilidad por este puerto es

190.34.183.131 y es una vulnerabilidad crítica como se mencionó anteriormente "Vulnerabilidad de HTTP.sys Permitir la ejecución remota de código (3042553).

El puerto que aparece con mayor frecuencia como vulnerable es 443.

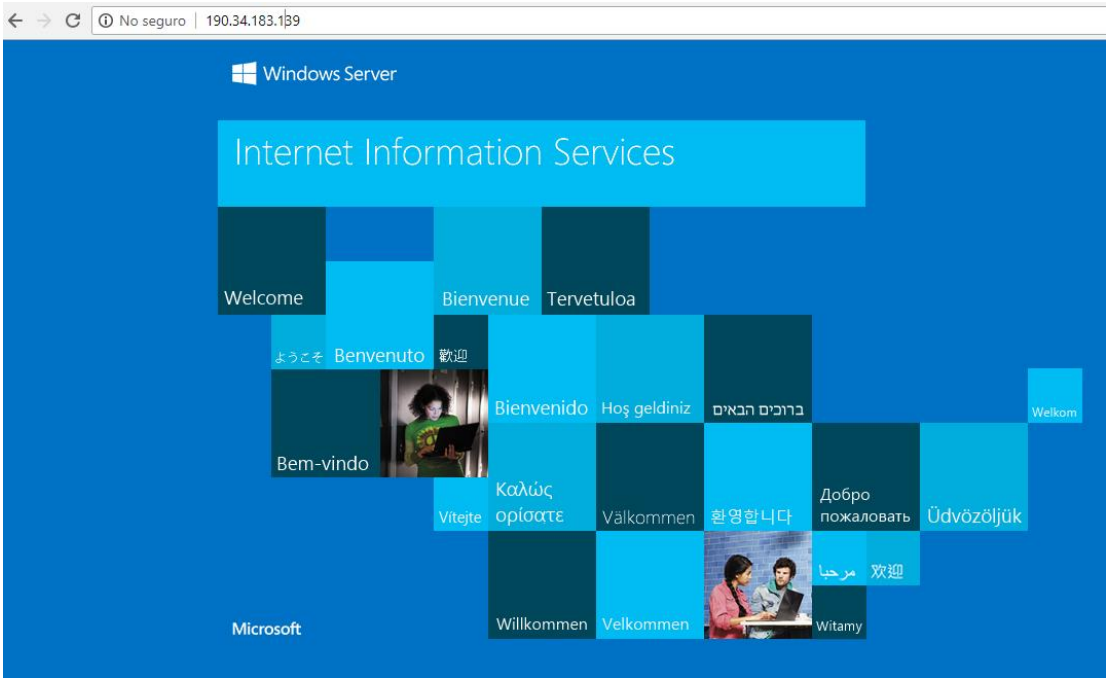
Los hosts más vulnerables son: 190.34.183.139, 190.34.183.142, 190.34.183.152 y 190.34.183.154; La mayoría son de severidad media y baja.

Descripción por Host

The remote host http://190.34.183.139/ Se ve afectada la acción de Fingerprinting.
Esta vulnerabilidad es conocida como OS Fingerprinting es una técnica que consiste en analizar las huellas dejadas por un sistema operativo en sus conexiones de red. Se basa en los tiempos de respuesta a los diferentes paquetes, para establecer una conexión en el protocolo TCP / IP, que es utilizado por los diferentes sistemas operativos. Recomendamos aplicar más seguridad a sus servidores.
Otra vulnerabilidad que presenta es: Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle. Esto se basa en el hecho de que una versión remota del Servidor de protocolo de escritorio remoto (Servicio de Terminal Server) es vulnerable a un ataque de hombre en el medio (MiTM). El cliente RDP no intenta validar la identidad del servidor al configurar el cifrado. Un atacante con la capacidad de interceptar el tráfico del servidor RDP puede establecer el cifrado con el cliente y el servidor sin ser detectado.

Adjuntamos la imagen del host vulnerable.

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355



El host remoto 190.34.183.131 (https://www.govimar.com.pa/) es afectado por la vulnerabilidad HTTP.sys podría permitir la ejecución remota de código (3042553), que afecta a los sistemas Windows (puertos 80/443); Recomendamos aplicar todas las actualizaciones de seguridad sugeridas por Windows, especialmente MS15-034 (KB 3042553), ya que todas resuelven las vulnerabilidades encontradas en este tipo de sistema. El mes anterior se presentó esta vulnerabilidad.

Vulnerabilidades por severidad

La siguiente sección describirá en detalle cada vulnerabilidad encontrada de acuerdo con su severidad.

Vulnerabilidades de severidad critica

MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution

Descripción
La versión de Windows que se ejecuta en el host remoto se ve afectada por una condición de desbordamiento de entero en la pila de protocolo HTTP (HTTP.sys) debido al análisis incorrecto de las solicitudes HTTP elaboradas.

Solución
Microsoft ha lanzado un conjunto de parches para Windows 7, 2008 R2, 8, 8.1, 2012 y 2012 R2.

Sistemas Afectados

80 / tcp / possible_wls	190.34.183.131
443 / tcp / possible_wls	190.34.183.131

Vulnerabilidades de riesgo Alto

SSL Version 2 and 3 Protocol Detection

Descripción
El servicio remoto acepta conexiones cifradas utilizando SSL 2.0 y / o SSL 3.0. Estas versiones de SSL se ven afectadas por varios defectos criptográficos.

Solución
Consulte la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0.
Utilice TLS 1.1 (con conjuntos de cifrado aprobados) o superior en su lugar.

Sistemas afectados
443 / tcp / possible_wls 190.34.183.139, 190.34.183.149, 190.34.183.154, 190.34.183.152, 190.34.183.142

Vulnerabilidades de severidad media

SSL Medium Strength Cipher Suites Supported

Descripción
El host remoto admite el uso de cifrados SSL que ofrecen cifrado de intensidad media. GLESEC considera la fuerza media como cualquier cifrado que usa longitudes de clave de al menos 64 bits y menos de 112 bits, o bien que utiliza el conjunto de cifrado 3DES.

Solución
Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados de

resistencia media

Sistemas Afectados
9443 / tcp / possible_wls 190.34.183.139
8089 / tcp / possible_wls 190.34.183.139
443 / tcp / possible_wls 190.34.183.132, 190.34.183.139, 190.34.183.142, 190.34.183.149, 190.34.183.152, 190.34.183.154, 190.34.183.90, 190.34.183.91

SSL Certificate Cannot Be Trusted

Descripción
El certificado X.509 del servidor no es confiable

Solución
Genere certificados de confianza.

Sistemas Afectados
25 / tcp / smtp 190.34.183.148
443 / tcp / possible_wls 190.34.183.142
443 / tcp / possible_wls 190.34.183.90, 190.34.183.91, 190.34.183.132

SSL Certificate Signed Using Weak Hashing Algorithm

Descripción
El servicio remoto utiliza una cadena de certificados SSL que se ha firmado con un algoritmo de hashing criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques de colisión. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, permitiendo que un atacante se haga pasar por el servicio afectado.

Tenga en cuenta que este complemento informa de todas las cadenas de certificados SSL firmadas con SHA-1 que caducan después del 1 de enero de 2017 como vulnerables.

Sistemas Afectados
443 / tcp / possible_wls 190.34.183.132, 190.34.183.142, 190.34.183.90,

190.34.183.91

SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability(POODLE)

Descripción
El host remoto se ve afectado por una vulnerabilidad de divulgación de información de man-in-the-middle (MitM) conocida como POODLE. La vulnerabilidad se debe a la forma en que SSL 3.0 maneja los bytes de relleno al descifrar mensajes encriptados usando cifrados de bloque en el modo de encadenamiento de bloques de cifrado (CBC).

Solución
SSLv3.

Sistemas Afectados
443 / tcp / possible_wls 190.34.183.142, 190.34.183.149

SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Descripción
El host remoto admite conjuntos de cifrado EXPORT_RSA con claves menores o iguales a 512 bits. Un atacante puede factorizar un módulo RSA de 512 bits en un corto período de tiempo.

Sistemas Afectados
- 190.34.183.154
- 190.34.183.152
- 190.34.183.139

Vulnerabilidades de severidad baja

SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Descripción
El host remoto admite el uso de RC4 en una o más suites de cifrado.
El cifrado RC4 tiene fallas en su generación de un flujo de bytes pseudoaleatorios,

por lo que se introduce una amplia variedad de pequeños sesgos en el flujo, lo que disminuye su aleatoriedad.

Solución
Reconfigure la aplicación afectada, si es posible, para evitar el uso de cifrados RC4. Considere el uso de TLS 1.2 con las suites AES-GCM sujetas a soporte de navegador y servidor web.

Sistemas Afectados
443 / tcp / possible_wls190.34.183.139,190.34.183.142,190.34.183.149, 190.34.183.152, 190.34.183.154

SSH Server CBC Mode Ciphers Enabled

Description
El servidor SSH está configurado para admitir el cifrado de Cipher Block Chaining (CBC).

Sistemas Afectados
190.34.183.142

SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Descripción
El host remoto permite conexiones SSL / TLS con uno o más módulos Diffie-Hellman menores o iguales a 1024 bits.

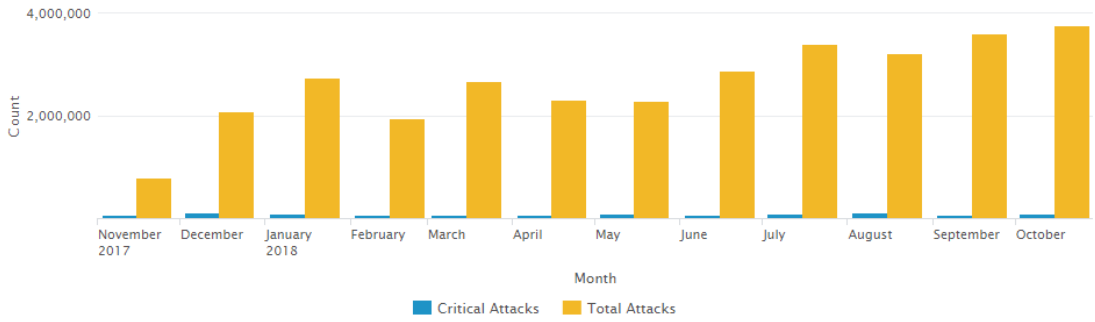
Solución
Reconfigure el servicio para usar un único módulo Diffie-Hellman de 2048 bits o más.

Sistemas Afectados
443 / tcp / possible_wls190.34.183.154, 190.34.183.152, 190.34.183.139

AMENAZAS

GLESEC utiliza sus MSS-APS, MSS-EPS, MSS-SIEM, MSS-EIR y MSS-UTM para determinar actividad de inteligencia de amenazas.

Las Amenazas tal como fueron reportadas por MSS-APS, MSS-EPS, MSS-SIEM, MSS-EIR, MSS-UTM para este mes son ataques de reconocimiento (escaneos de puertos).



Basándonos en la información recolectada por las contramedidas de seguridad durante este periodo, 3,759,359 ataques hacia Metrobank S.A.; 80,179 de los cuales fueron considerados "críticos". Pudimos observar un aumento en actividad de ataques con respecto al mes de Septiembre (Ataques totales: 3,596,487) de un 5% aproximadamente y un aumento en ataques críticos con relación al mes de Septiembre (Ataques críticos: 51,427) de alrededor de un 56%. El ataque crítico que ocurrió con más frecuencia este mes fue Network Flood IPv4 UDP (82%) y pertenece a la categoría Behavorial-DoS.

Éstos son algunos de los ataques bloqueados y el nivel de severidad que representan:

- Network Flood IPv4 UDP, SIP-Scanner-SIPVicious y Denied Access debido a una solicitud maliciosa se consideran con un alto nivel de severidad.
- TCP Scan (horizontal), TCP Scan, UDP Scan (horizontal), Ping Sweep y TCP Scan (vertical) se consideran con un nivel de severidad media.
- Threat List, Link Protocol, se consideran con un nivel de gravedad bajo.

Tiene una gravedad "informativa" de tipo Anomaly-SSL-renegotiation-Cli que

pertenece a la categoría de intrusiones en el host 190.34.183.154 hasta el puerto 443.

Entre los ataques frecuentes y bloqueados por semana tenemos: TCP Scan (horizontal), TCP Scan, threat list, Network Flood IPv4 UDP, UDP Scan (horizontal), SIP-Scanner-SIPVicious, Ping Sweep.
Todo esto fue detenido por las contramedidas de seguridad gestionadas por GLESEC.

La duración que presenta la mayoría de los ataques son:

- Menos de un minuto se generan a partir de las categorías de Anti-Scanning, Behavioral-DoS and HttpFlood.
- De uno a cinco minutos se generan a partir de las categorias de Anti-Scanning, Cracking Protection y Behavioral-DoS

Las 5 fuentes más frecuentes de ataques provienen de los siguientes países: Federación de Rusia (31.5%), Panamá (21.7%), Ucrania (12.3%), Estados Unidos (10.9%) y Holanda (7.2); Estos están destinados principalmente a los puertos: 8545 está destinado a exploraciones con mucha frecuencia; si no es necesario dejarlo abierto, sería recomendable cerrarlo o filtrarlo del tráfico del exterior, 3389 (RDP: Remote Desktop Protocol) y el puerto de acceso web (8080).

La mayoría de los ataques parecen ser de reconocimiento (escaneo) duraron menos de un minuto y seguidamente de 1 a cinco minutos. Alrededor de un 94% de los ataques de este mes fueron provenientes de escaneos que pueden considerarse reconocimiento y se utiliza como planeación para futuros ataques. Los ataques que consumen la mayor cantidad de ancho de banda son los ataques de Behavorial-DoS, Anti-Scanning, Access, Anomalies and Intrusions.

En este periodo hubo un bajo porcentaje de ataques en las categorías:

- Cracking Protection (Web Scan) a las direcciones IP 190.34.183.139, 190.34.183.149, 190.34.183.81, 190.34.183.148 y 190.34.183.153.
- HttpFlood (Http Page Flood Attack) a las direcciones IP 190.34.183.154,

190.34.183.149, 190.34.183.152, 190.34.183.131 y 190.34.183.132.

El Dispositivo DefensePro y AppWall protege todos estos ataques dirigidos a la red y en el nivel del servidor dirigido a números de puerto conocidos: 23 (Telnet), 3389 (RDP), 8545 (JSON-RPC), 8080 and 81(HTTP-Alternative), 4500(IPSec NAT Traversal), 80 (HTTP), 22(SSH) y 5060 (SIP) en orden de frecuencia para este periodo.

Las 5 principales IP de origen (locales o públicas).

- 190.34.192.73
- 190.34.192.31
- 122.228.10.50
- 91.217.254.167
- 201.225.225.225

Los tipos de ataques más frecuentes fueron TCP Scan y TCP Scan (Horizontal).
La primera y segunda dirección IP fueron los principales atacantes y provienen de Panamá, la tercera dirección IP proviene de China, la cuarta dirección proviene de Ucrania y la última proviene de Panamá también.

Correlación entre el MSS-APS y el MSS-VME
En la siguiente tabla, describiremos qué hosts son los objetivos más frecuentes y si estos ataques atacan vulnerabilidades específicas en estos hosts.

Destino de ataques (MSS-APS/APFW)	Número de ataques	Vulnerabilidades presentes (MSS-VME)
190.34.183.135	139,595	None
190.34.183.132	25,393	• El certificado SSL no es confiable • Certificado SSL firmado usando un algoritmo de hash débil • Admite suites de cifrado de resistencia media SSL
190.34.183.158	18,028	None

190.34.183.137	6,151	None
190.34.183.149	4,031	• Soporta protocolo SSL versión 2 y 3 • Divulgación de información de Microsoft Exchange • SSL DROWN Attack • Vulnerabilidad de SSL POODLE • Vulnerabilidad de SSL Bar Mitzvah • Admite suites de cifrado SSL de fuerza media

Análisis:

- La mayoría de los ataques en host 190.34.183.132 fueron network Flood usando el protocolo UDP, estos ataques no apuntan a ninguna vulnerabilidad específica. Sin embargo, el resto de los ataques apuntaron a múltiples puertos, entre ellos el puerto 80 (HTTP) y 443 (HTTPS), las vulnerabilidades en este host se pueden aprovechar a través del puerto 443. haciendo que las comunicaciones sean interceptadas o descifradas por un actor malicioso.

- La mayoría de los ataques en host 190.34.183.149 se dividen entre Web Scan, violación de protocolo de enlace TCP y TCP Scan (vertical).
  El web scan se refiere a una táctica utilizada para recopilar información sobre el servidor, las herramientas automatizadas se utilizan para enviar diferentes tipos de solicitudes HTTP y analizar las respuestas que obtiene. Estos ataques apuntan a los puertos 80 y 443 y muchas de las vulnerabilidades presentes en este host pueden ser explotadas a través de estos puertos.
  Los protocolos TCP se refieren al tráfico caído debido a una coincidencia con una ACL.
  TCP Scan (Vertical) se refiere a la práctica de escanear múltiples puertos en un solo host, esta práctica se usa como una táctica de reconocimiento para identificar los puntos débiles en los hosts.

USA-ARGENTINA-PANAMA
México-Perú-Brasil- Chile

Tel: +1 609-651-4246
Tel: +507-836-5355

Info@glesec.com
www.glesec.com