

ESET®
**INTELLIGENCE
LABS**

Servicios
confiables,
Negocios
Seguros



ESET®
**INTELLIGENCE
LABS**

Servicios
confiables,
Negocios
Seguros



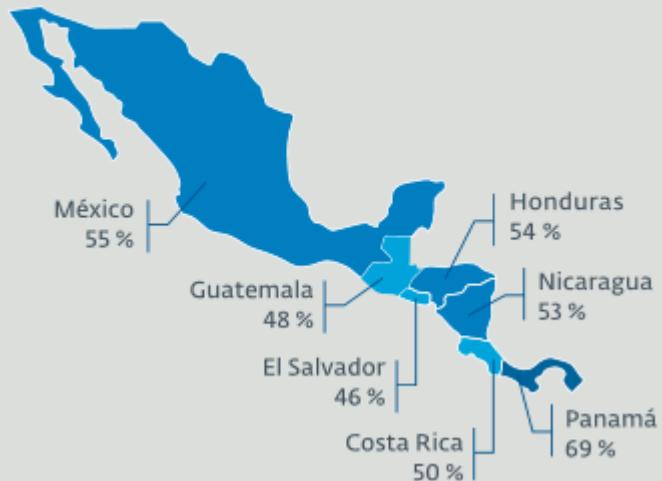
Presentación de servicios
profesionales





Situación en Latinoamérica

Porcentaje de empresas, por país, que sufrieron un incidente relacionado con acceso indebido a aplicaciones y/o bases de datos



Accesos indebidos

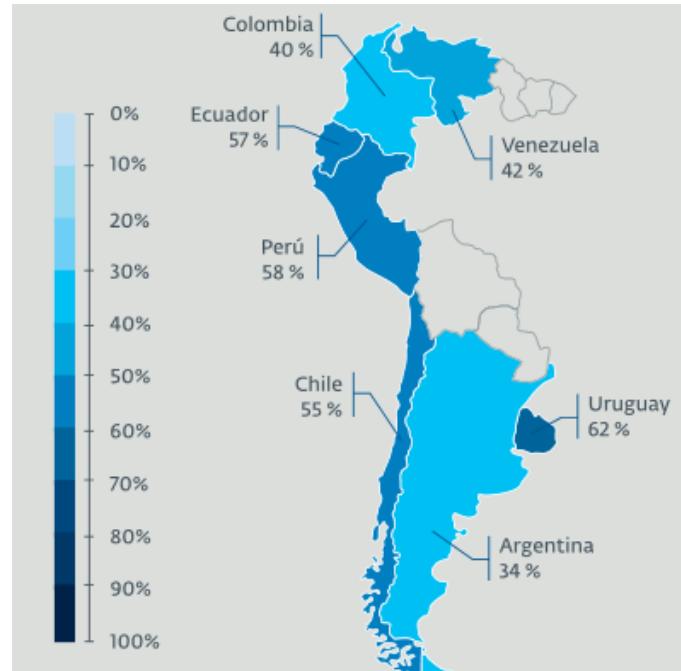


GRÁFICO 4 / Acceso indebido por país.



Preocupaciones en términos de seguridad

Preocupaciones relacionadas con la seguridad de la información en las empresas encuestadas en Latam,
clasificadas por tamaño de empresa

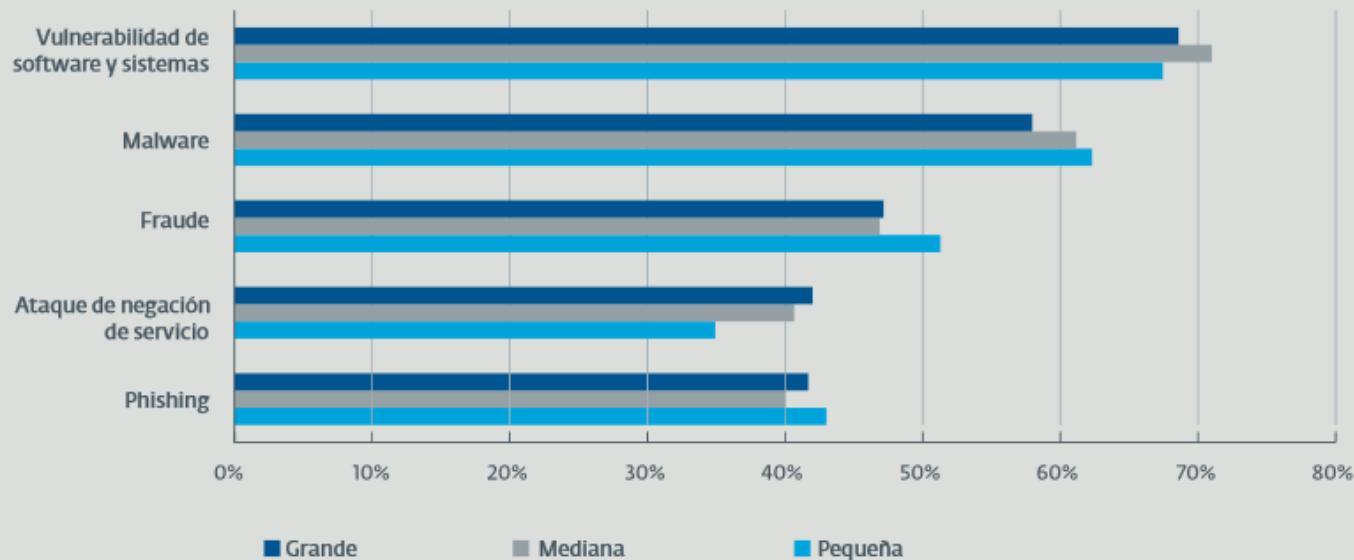


GRÁFICO 1 / Preocupaciones de la Seguridad de la Información de las empresas de acuerdo de su tamaño



Situación en Latinoamérica

Porcentaje de empresas, por país, que sufrieron un incidente relacionado con Explotación de Vulnerabilidades

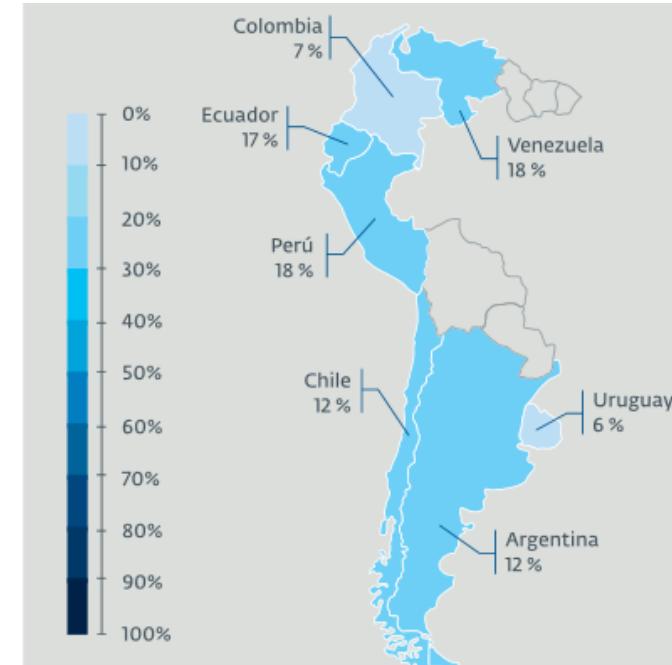
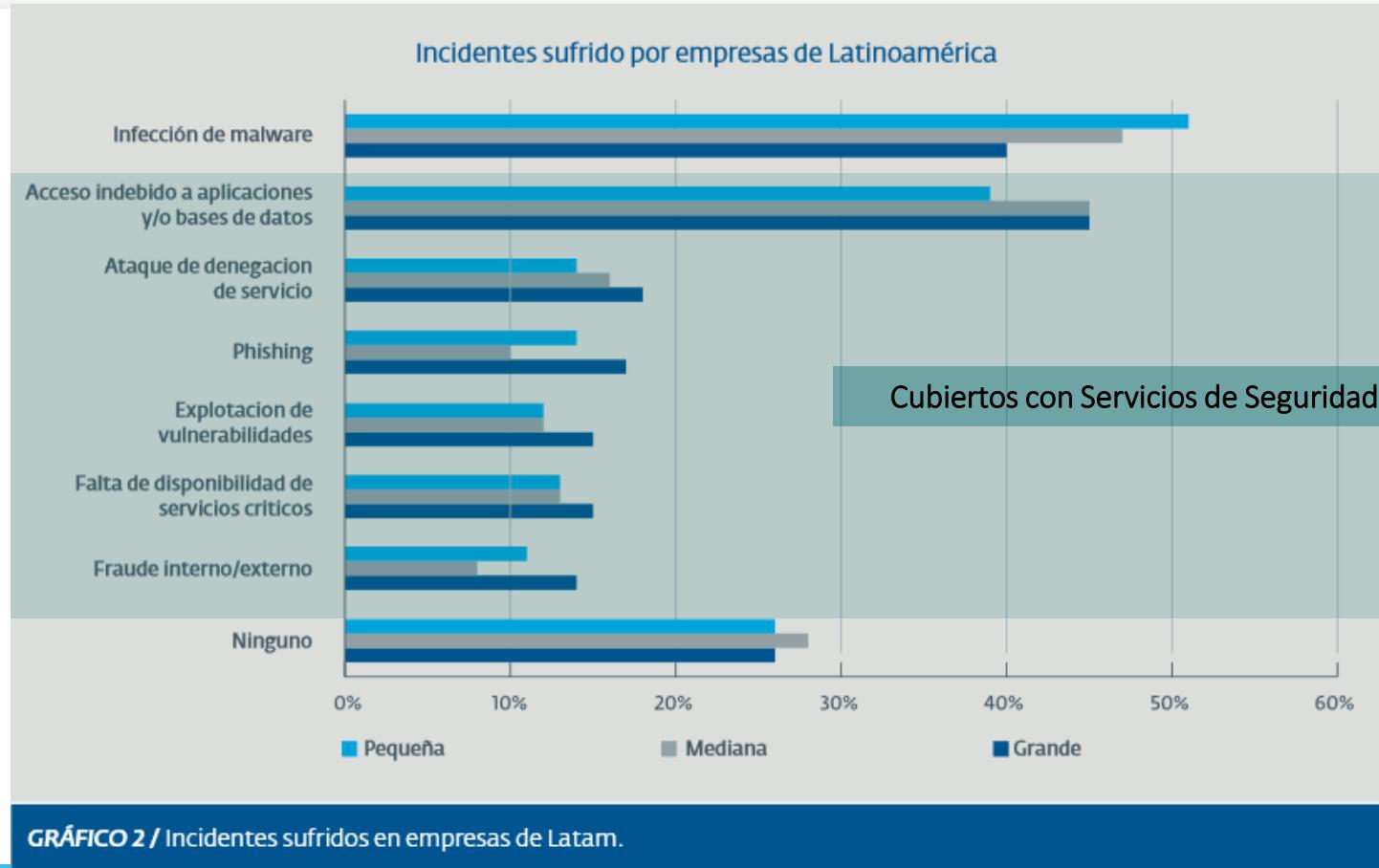


GRÁFICO 5 / Explotación de vulnerabilidades por país.

Explotación de vulnerabilidades

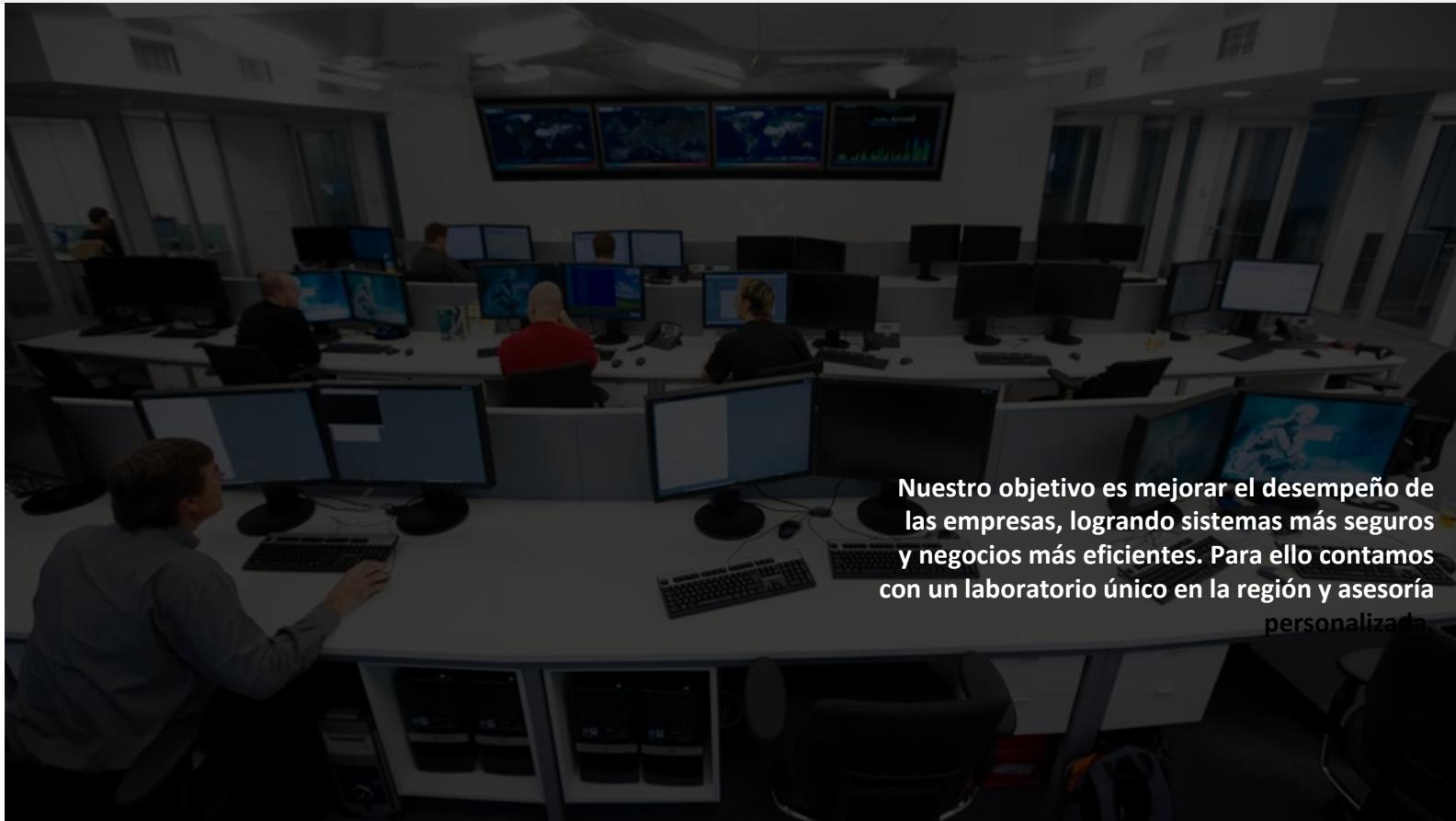


¿Qué incidentes sufrieron las empresas?





ESET Intelligence Labs





¿Por qué servicios de seguridad?

- ▶ Conocer el nivel de seguridad dentro de la organización.
- ▶ Conocer el nivel de seguridad hacia fuera de la organización.
- ▶ Cumplir normativas y regulaciones sobre seguridad de la información.
- ▶ Implementar y mejorar el proceso de “Gestión de Riesgos”.

Vulnerability Assessment

Interno
Externo

Alcance del servicio

- ▶ Localizar vulnerabilidades en una etapa temprana (antes que un atacante).
- ▶ Relevar superficies de ataque
- ▶ Informe sobre el estado actual de los servicios analizados.



Penetration Testing

Interno
Externo

Alcance del servicio

- ▶ Análisis más extensivo que Vulnerability Assessment.
- ▶ Evalúa la explotación de la vulnerabilidad.
- ▶ Verifica los niveles de intrusión a los que se expone un sistema.



Ransomware Prevention

Alcance del servicio

▶ Por medio de la ejecución de diferentes evaluaciones de seguridad, permite identificar y prevenir que una organización se vea afectada por este tipo de ataque.

Se incluyen tanto auditorias del tipo Penetration test, Red, Web, como evaluaciones que revelan el nivel de concientización de los usuarios.



Web Penetration Testing

Externo

Alcance del servicio

- ▶ De similares características que un Penetration Test pero orientado a web.
- ▶ Evalúa la explotación de las vulnerabilidades web.
- ▶ Verifica los niveles de intrusión a los que se expone un sistema.



Mobile Penetration Test

Interno
Externo

Alcance del servicio

- ▶ Análisis que se enfoca en evaluar aplicaciones móviles.
- ▶ Puede llevarse a cabo tanto desde un punto de vista interno como externo.
- ▶ ¿Para qué?
Para conocer el estado de la seguridad de la aplicación móvil de la organización.



Social Engineering Testing

Externo

Alcance del servicio

- ▶ Evaluar el grado de concientización de los usuarios de la organización en seguridad de la información.
- ▶ Entender si los usuarios están exponiendo a riesgos externos a la organización.
- ▶ Disparar acciones necesarias en materia de capacitación interna en seguridad de la información



Gap Analysis

Alcance del servicio

- ▶ Evalúa el riesgo de la existencia de fuga de información.
- ▶ Entrevistas por parte de un consultor con actores claves en la empresa.
- ▶ Analiza la existencia de políticas de seguridad y la funcionalidad de las mismas.
- ▶ Verifica el grado de cumplimiento de seguridad de una organización con respecto a una determinada normativa.



WIFI Penetration Test

Interno

Alcance del servicio

- ▶ Evaluar el nivel de seguridad de las redes inalámbricas.
- ▶ Comprender si un atacante, sin acceso a la red WIFI corporativa, podría conectarse de todas formas.
- ▶ Detectar configuraciones débiles que implican riesgos para la red corporativa o bien a los usuarios de la misma.



Continuous Security Assessment

Externo

Alcance del servicio

- ▶ Localizar debilidades y vulnerabilidades en una etapa temprana (antes que un atacante).
- ▶ Para constituir un ciclo de revisión y mejora para la seguridad.
- ▶ Dar seguimiento a la aplicación de parches y corrección de vulnerabilidades en la organización.
- ▶ Para contar con indicadores de gestión en la materia.



Etapas de un Penetration Test



Reconocimiento

Etapa de reconocimiento de sistemas

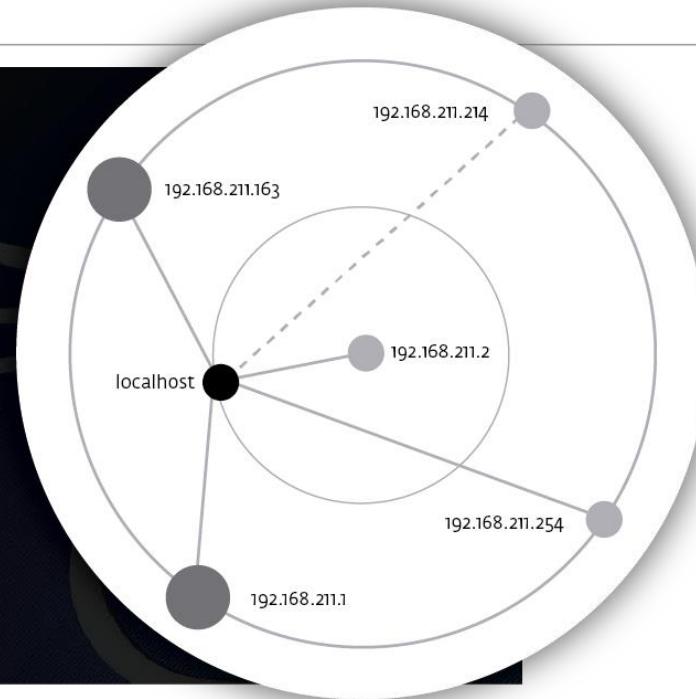




Reconocimiento

Detección de puertos y servicios

```
root@kali:~# nmap -sS -sV 192.168.211.163 -p1-65535
Starting Nmap 7.01 ( https://nmap.org ) at 2016-05-09 13:40 EDT
Nmap scan report for 192.168.211.163
Host is up (0.00015s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smptd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  shell        Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd    distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6007/tcp  open  X11         (access denied)
```



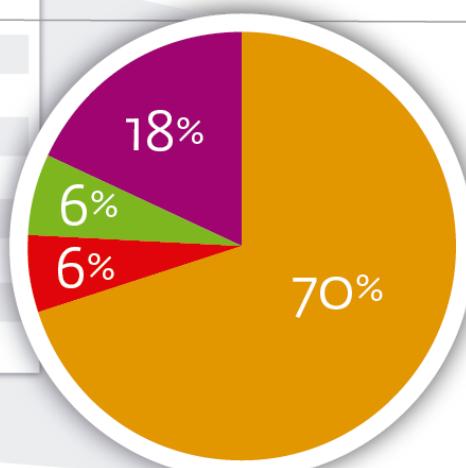


Análisis de Vulnerabilidades

Identificación de Vulnerabilidades unificadas por nombre

RIESGO	NOMBRE	ESTADO
CRITICAL	PHP Remote File Inclusion	Explotado
CRITICAL	Remote File Execution	Explotado
CRITICAL	Remote Command Execution	Explotado
HIGH	Microsoft Windows SMB Shares Unprivileged Access	Potencial
MEDIUM	SSL Certificate Expiry	Verificado
MEDIUM	SSL Version 2 and 3 Protocol Detection	Verificado
MEDIUM	SSL Weak Cipher Suites Supported	Verificado
MEDIUM	NFS Shares World Readable	Verificado
MEDIUM	SSL Medium Strength Cipher Suites Supported	Verificado

Total de vulnerabilidades



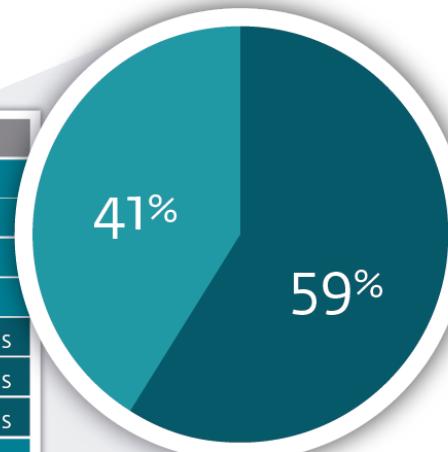


Analisis de Vulnerabilidades

Identificación de Vulnerabilidades unificadas por Tipo de Solución

RIESGO	NOMBRE	ESTADO
CRITICAL	PHP Remote File Inclusion	Configuración
CRITICAL	Remote File Execution	Configuración
CRITICAL	Remote Command Execution	Configuración
HIGH	Microsoft Windows SMB Shares Unprivileged Access	Configuración
MEDIUM	SSL Certificate Expiry	Problemas Criptográficos
MEDIUM	SSL Version 2 and 3 Protocol Detection	Problemas Criptográficos
MEDIUM	SSL Weak Cipher Suites Supported	Problemas Criptográficos
MEDIUM	NFS Shares World Readable	Configuración
MEDIUM	SSL Medium Strength Cipher Suites Supported	Problemas Criptográficos

Total de vulnerabilidades
por tipo de Fix





Explotación

Explicación de cada Vulnerabilidad. Riesgo e impacto

(CRITICAL) PHP Remote File Inclusion

Riesgo e impacto:

La vulnerabilidad de inclusión de archivo remota le permite a un atacante subir contenido malicioso al equipo. Mediante esta técnica puede utilizar el servidor afectado para alojar malware, phishing, exploit packs entre otros.

En este caso se utilizó la manipulación de formularios para subir imágenes mediante un proxy web para saltar medidas de seguridad como las...

CVSS Score

10,0

CWE

98

Existe exploit público

No se requiere

Sistemas Afectados

192.168.211.163

Estado

Explotado

Explotación

Evidencia

The screenshot shows a Linux metasploitable environment with several open windows:

- Vulnerability: File Upload**: A browser window showing a file upload form with a selected file "192.168.211.183/dvwa/vulnerabilities/upload".
- Vulnerability: File Upload**: Another browser window showing a file upload form with a selected file "192.168.211.183/dvwa/vulnerabilities/upload".
- File manager**: A terminal window displaying a file listing of the root directory. A red box highlights the directory structure from .. to /vmlinuz.
- File manager**: A terminal window showing the root directory (indicated by a red box).

A red arrow points from the text "Directorio Raíz /" at the bottom left to the root directory entry in the file manager terminal.

Name	Size	Modify	Owner/Group	Permissions	Actions
[..]	dir	2012-05-20 14:36:12	root/root	drwxr-xr-x	R T
[bin]	dir	2012-05-13 23:35:33	root/root	drwxr-xr-x	R T
[boot]	dir	2012-05-13 23:36:28	root/root	drwxr-xr-x	R T
[cdrom]	link	2010-03-16 18:55:51	root/root	drwxr-xr-x	R T
[dev]	dir	2016-05-04 16:59:31	root/root	drwxr-xr-x	R T
[etc]	dir	2016-05-09 23:27:50	root/root	drwxr-xr-x	R T
[home]	dir	2010-04-16 02:16:02	root/root	drwxr-xr-x	R T
[initrd]	dir	2010-03-16 18:57:40	root/root	drwxr-xr-x	R T
[lib]	dir	2012-05-13 23:35:22	root/root	drwxr-xr-x	R T
[lost+found]	dir	2010-03-16 18:55:15	root/root	drwxr-xr-x	R T
[media]	dir	2010-03-16 18:55:52	root/root	drwxr-xr-x	R T
[mnt]	dir	2010-04-28 16:16:56	root/root	drwxr-xr-x	R T
[opt]	dir	2010-03-16 18:57:39	root/root	drwxr-xr-x	R T
[proc]	dir	2016-05-04 16:59:04	root/root	dr-xr-xr-x	R T
[root]	dir	2016-05-09 09:19:14	root/root	drwxr-xr-x	R T
[sbin]	dir	2012-05-13 21:54:53	root/root	drwxr-xr-x	R T
[srv]	dir	2010-03-16 18:57:38	root/root	drwxr-xr-x	R T
[sys]	dir	2016-05-04 16:59:05	root/root	drwxr-xr-x	R T
[tmp]	dir	2016-05-09 18:58:56	root/root	drwxrwxrwt	R T
[usr]	dir	2010-04-28 00:06:37	root/root	drwxr-xr-x	R T
[var]	dir	2012-05-20 17:30:19	root/root	drwxr-xr-x	R T
[intrd.img]	7.56 MB	2012-05-13 23:35:56	root/root	-rw-r--r--	R T FED
[nohup.out]	12.73 KB	2016-05-09 09:19:14	root/root	-rw-----	R T FED
[vmlinuz]	1.90 MB	2008-04-10 12:55:41	root/root	-rw-r--r--	R T FED

Change dir: / >> Read file: >>
Make dir: (Not writable) >> Make file: (Not writable) >>



Reportes / Conclusiones

ESET®
**INTELLIGENCE
LABS**

Durante esta etapa se elaboran los entregables.
Reporte ejecutivo y Reporte técnico que explican en detalle el nivel de riesgo y la postura de seguridad de la organización, al mismo tiempo que proveen al cliente un detalle exhaustivo sobre las tareas de remediación necesarias para mitigar los problemas detectados.



¡Muchas gracias!