ESET®
INTELLIGENCE
LABS

Servicios confiables, Negocios Seguros

ESET®
INTELLIGENCE
LABS

Servicios confiables, Negocios Seguros

Presentación de servicios profesionales

Situación en Latinoamérica

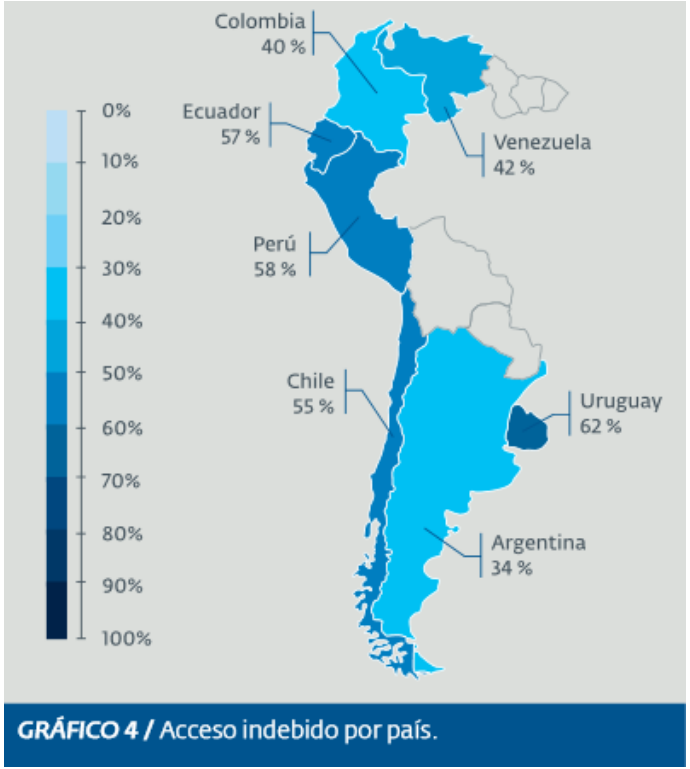


GRÁFICO 4 / Acceso indebido por país.

Accesos indebidos

Preocupaciones en términos de seguridad

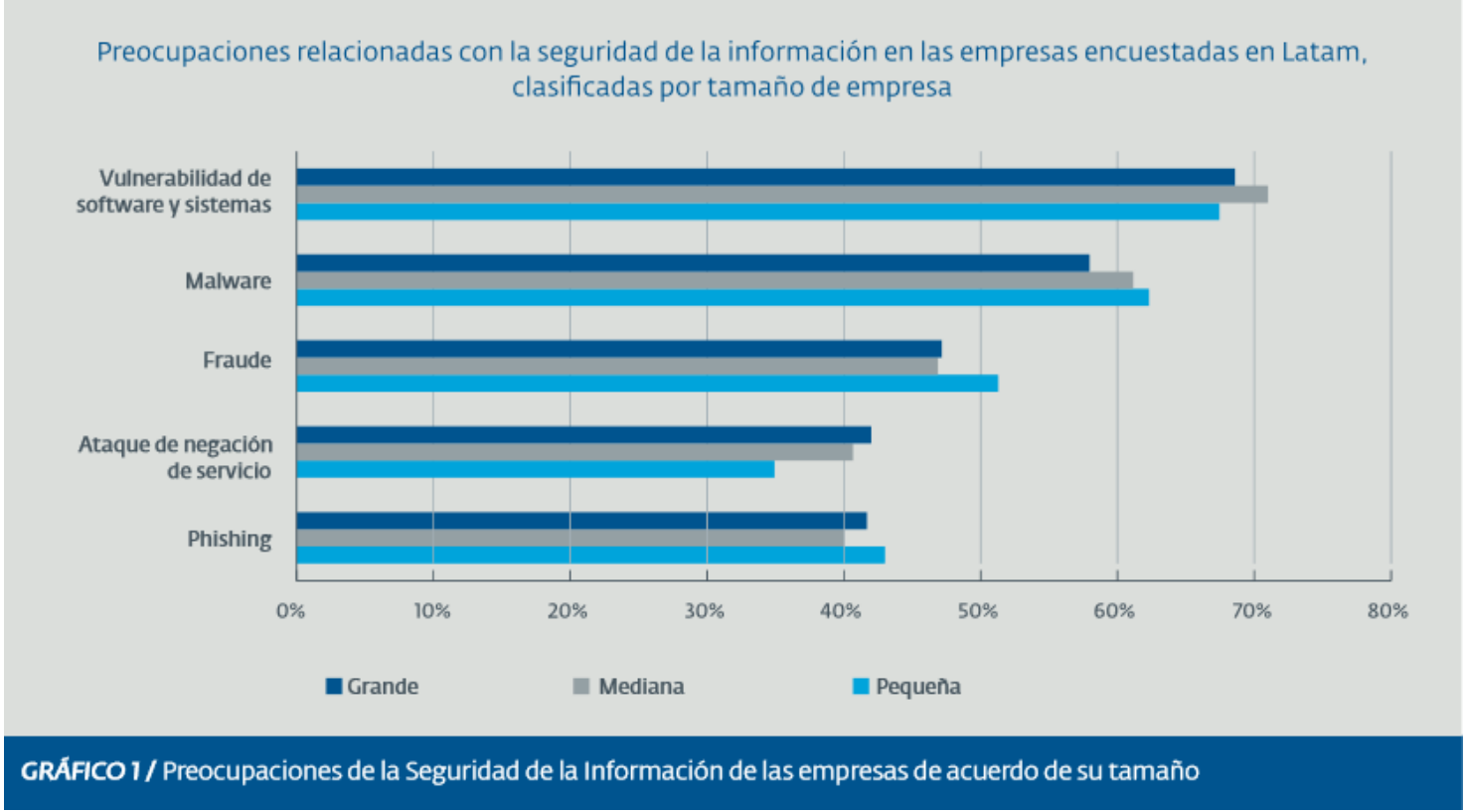


GRÁFICO 1 / Preocupaciones de la Seguridad de la Información de las empresas de acuerdo de su tamaño

Situación en Latinoamérica

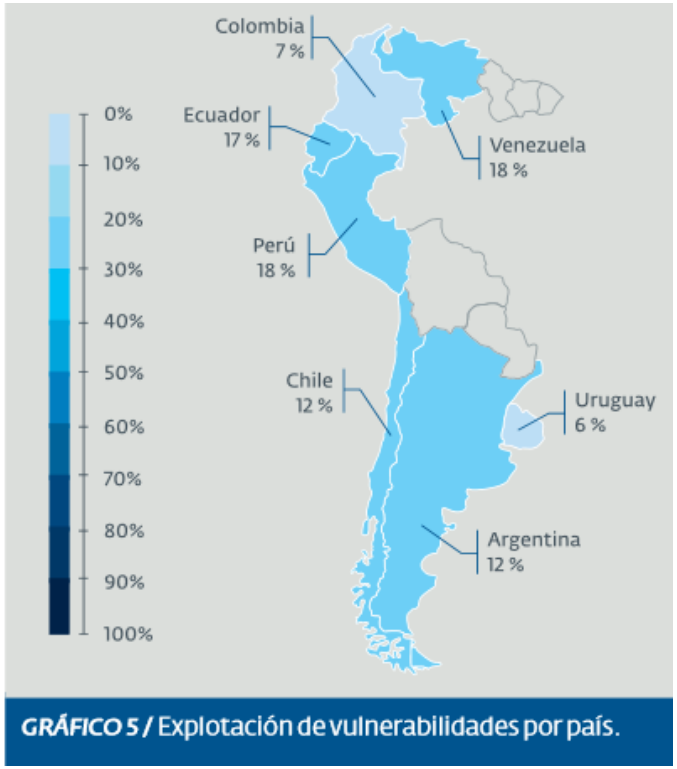


GRÁFICO 5 / Explotación de vulnerabilidades por país.

Explotación de vulnerabilidades

¿Qué incidentes sufrieron las empresas?

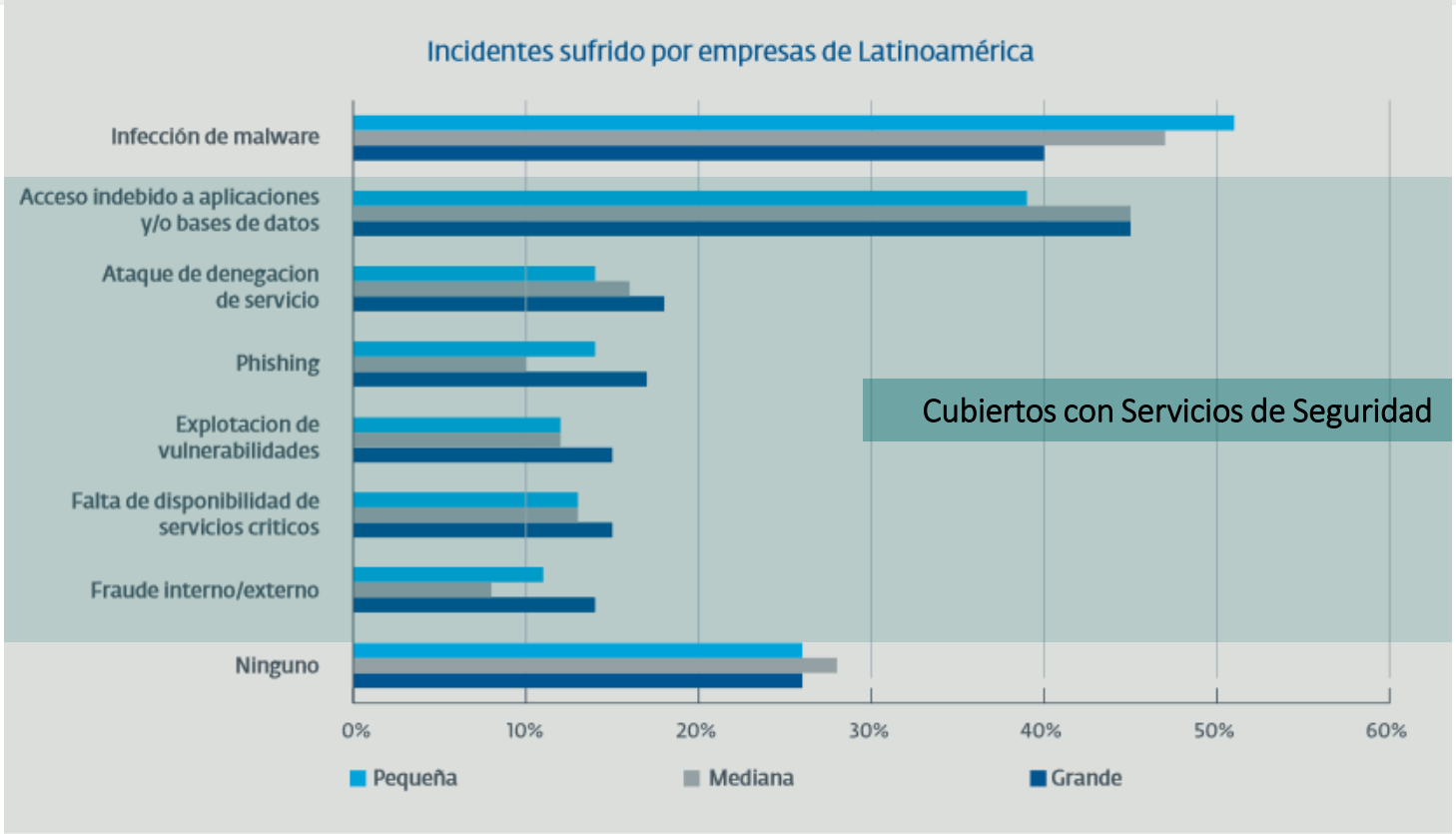
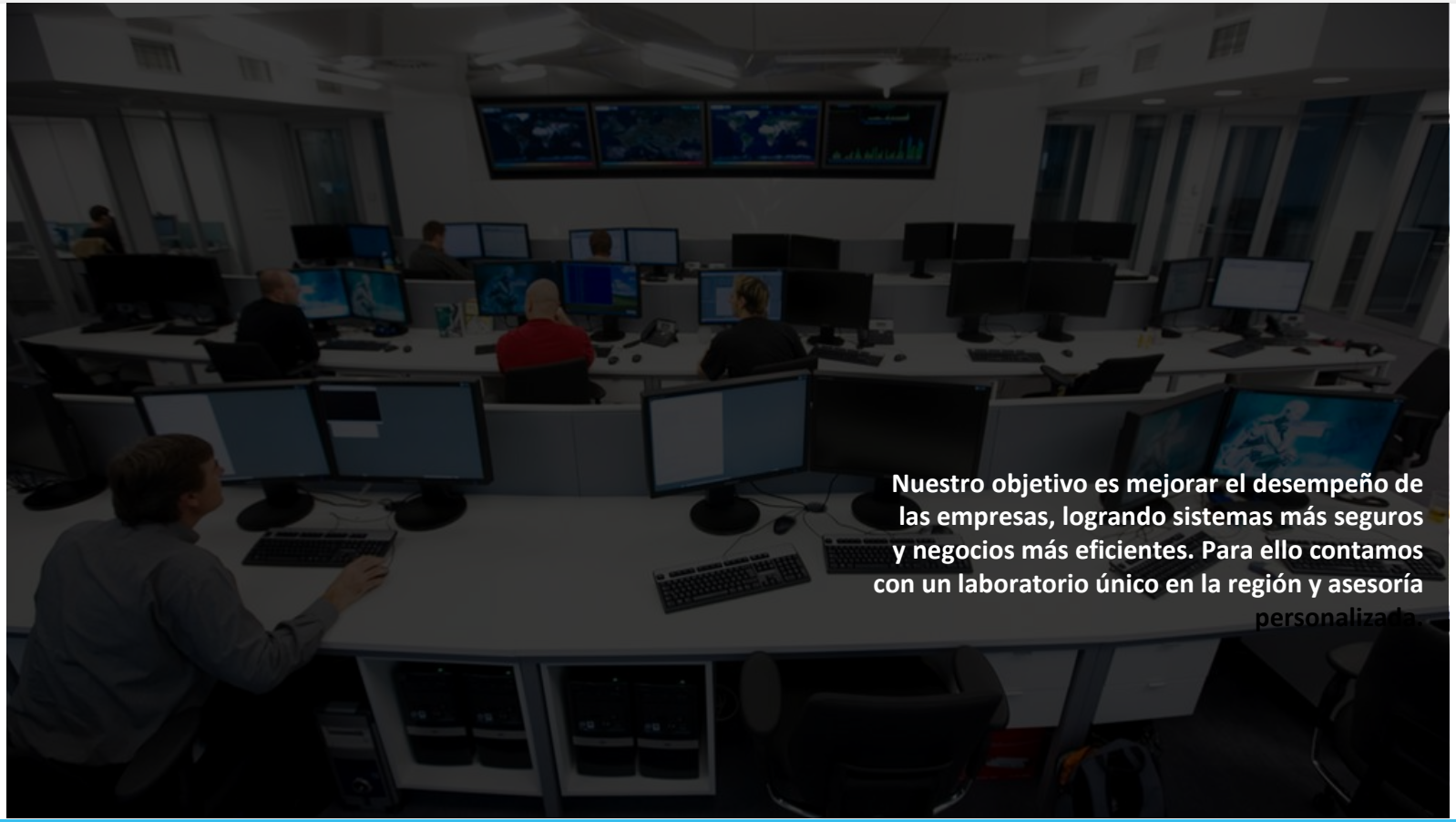


GRÁFICO 2 / Incidentes sufridos en empresas de Latam.

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 Vulnerabilty 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 que?**

  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

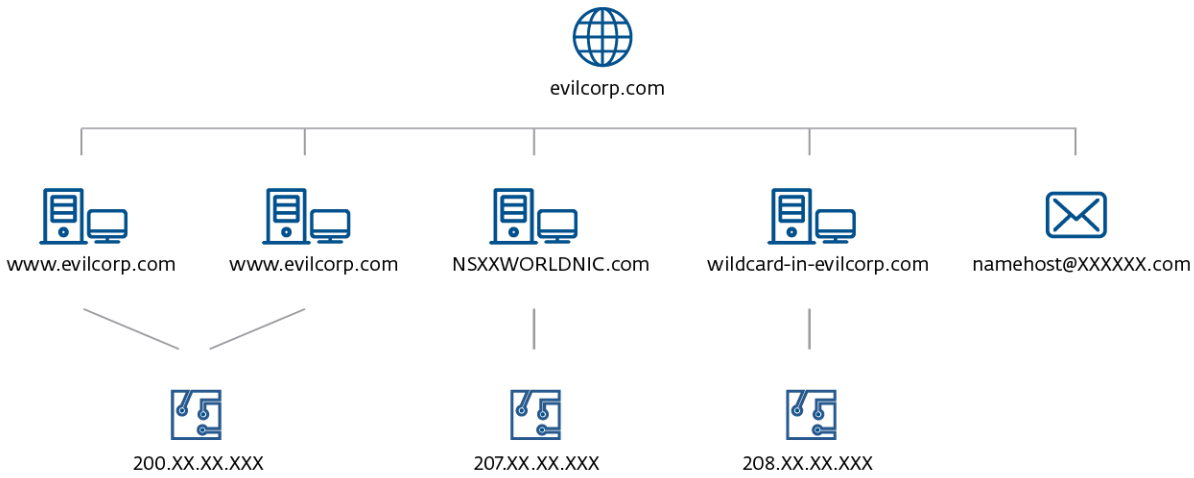
Alcance del servicio

- 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

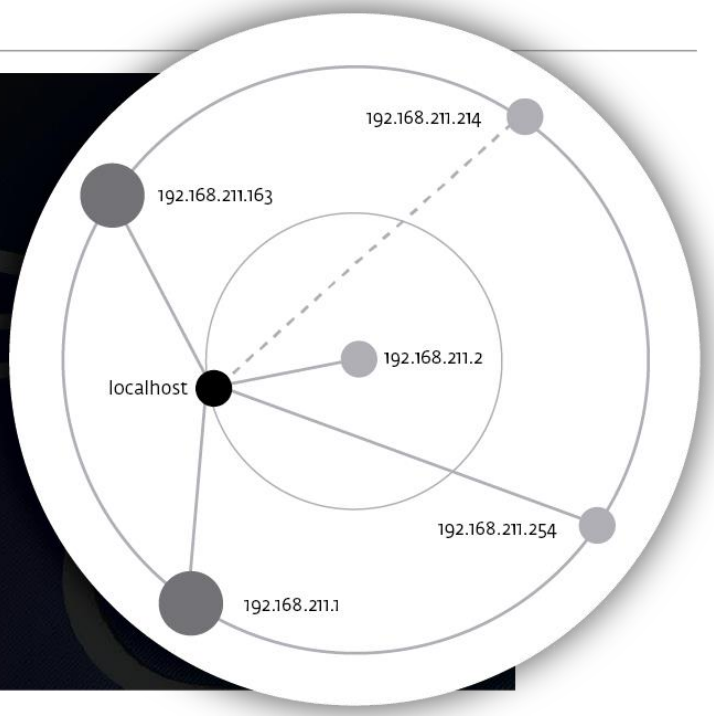
Etapa de reconocimiento de sistemas



Reconocimiento

Detección de puertos y servicios

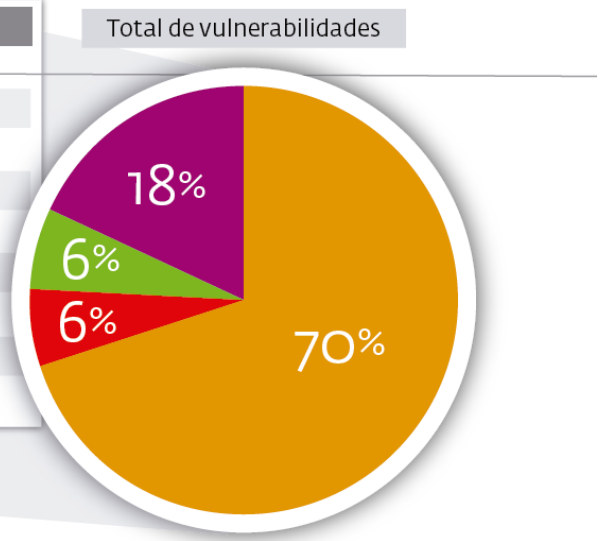
```
root@kali:~# nmap -sS -sV 192.168.211.163 -p1-65535

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 smtpd
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)
```



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

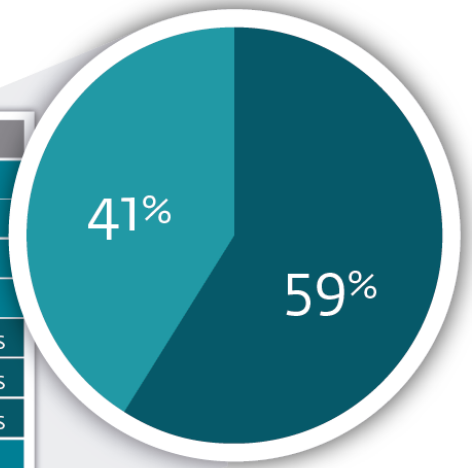


Analisis de Vulnerabilidades

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:

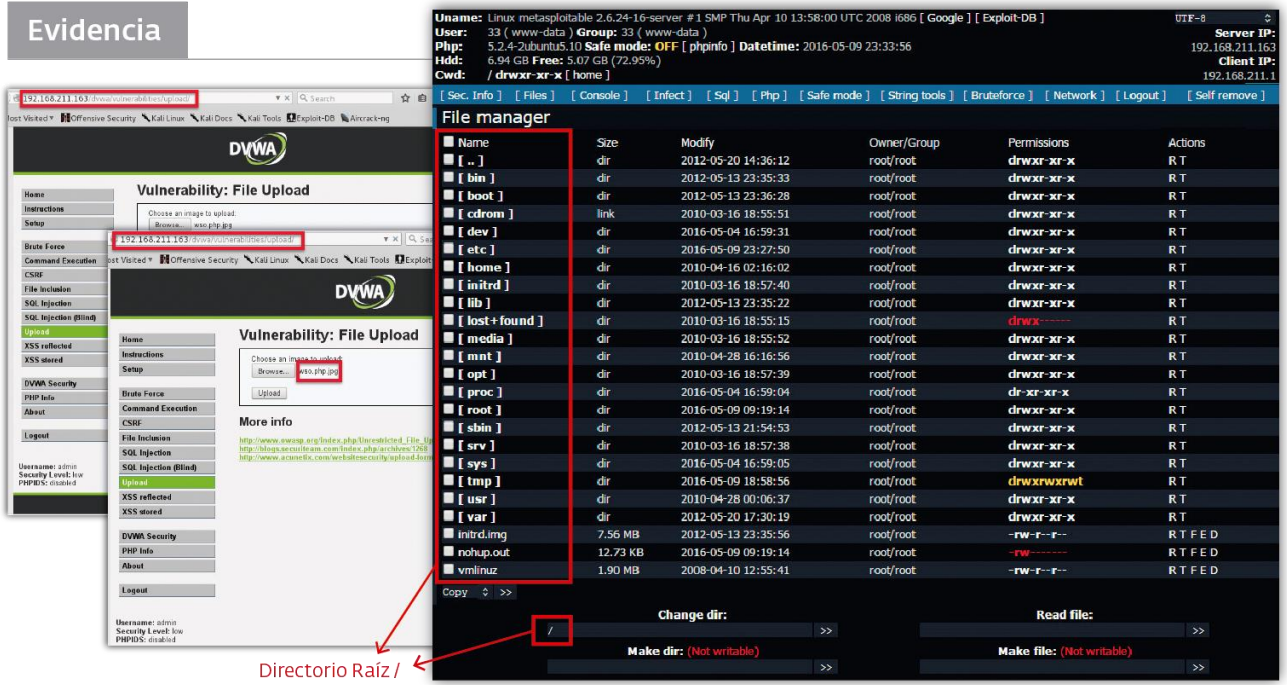
La vulnerabilidad de inclusión de archivo remota le permite a un atacante subir contenido malicioso al equipo. Mediante esta técnica puede utilizar el servidor afectado para alojar malware, phishing, exploit packs entre otros.

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

CVSS Score	CWE	Existe exploit público	Sistemas Afectados	Estado
10,0	98	No se requiere	192.168.211.163	Explotado

Explotación

Evidencia



Reportes / Conclusiones

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!