K•R•N•U•X Solutions

Porque hackean las empresas ?

Errores más comunes a nivel de seguridad en nuestra experiencia de ethical hacking

Por: Carlos Fernando Arismendy Ch. – Steven Zuluaga

Hacking en la nube

- Migran a soluciones en la nube sin tener un plan estructurado a nivel de seguridad.
- No se tiene conocimiento de la administración de la plataforma.
- El proveedor conoce la plataforma de la nube pero no tiene experiencia en seguridad.
- Integraciones de nube con servidores internos de la empresa, dejan todos los puertos abiertos por defecto.
- No implementan controles de seguridad en la nube, y por desconocimiento dejan configuraciones expuestas (SSH, RDP, administraciones Web, Etc.)
- Contraseñas débiles de usuarios y de administración de nube.
- Bajan la seguridad en las sedes principales porque los servidores están en la nube

Hacking en la nube Multicloud

Backup en la nube

Antivirus
Access Point /etc

Office 365
Google Apps

Aplicativos propios

ERP / CRM /
Gestión Documental

Aplicativos para ISO /
seguridad en el trabajo

Hacking en perímetro externo

- Firewalls desactualizados con bugs (CVE's) y puertos administración.
- Tienen Firewall, pero expuesto por Ej: RDP , SSH
- Módulos de seguridad desactivados.
- Sitios Web expuestos a internet pero no tienen WAF
- Nadie esta revisando las alertas ni los ataques

- Reglas mal configuradas ANY TO ANY
- Wifi corporativos y visitantes en la misma red.
- **Aplicativos Web vulnerables expuestos a internet**
- Proveedores que no conocen bien seguridad y realizan instalaciones por defecto.
- Personal interno administrando el firewall, crea y modifica reglas, a veces le funciona, pero expone la seguridad por desconocimiento.

4	any	any	ALL

Hacking en perímetro interno

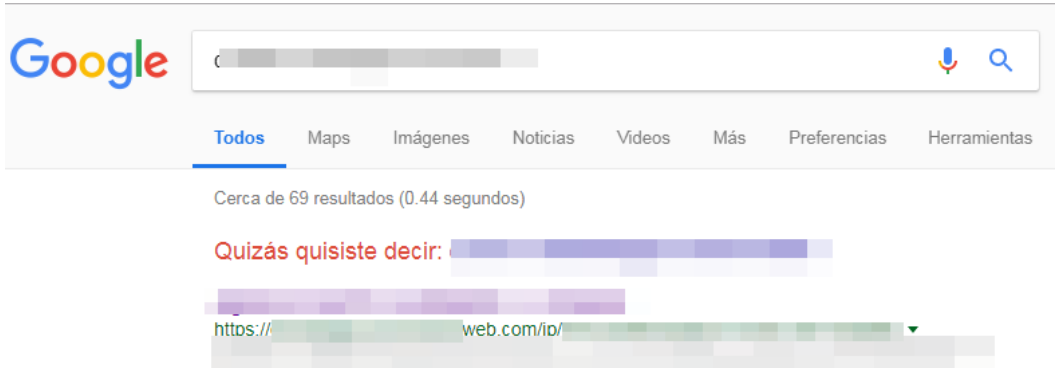
- Servidores llenos de vulnerabilidades críticas, y desactualizados .
- Servidores y aplicativos internos no están protegidos y se encuentran en la misma red.
- **Nadie revisa en los PC si tiene dispositivos de hardware extraños, como keyloggers, sniffers, video loggers etc.**
- Se comprometen servidores críticos haciendo pivoting de equipos de usuarios normales o servidores de baja importancia.
- Se subestima el conocimiento de los empleados.

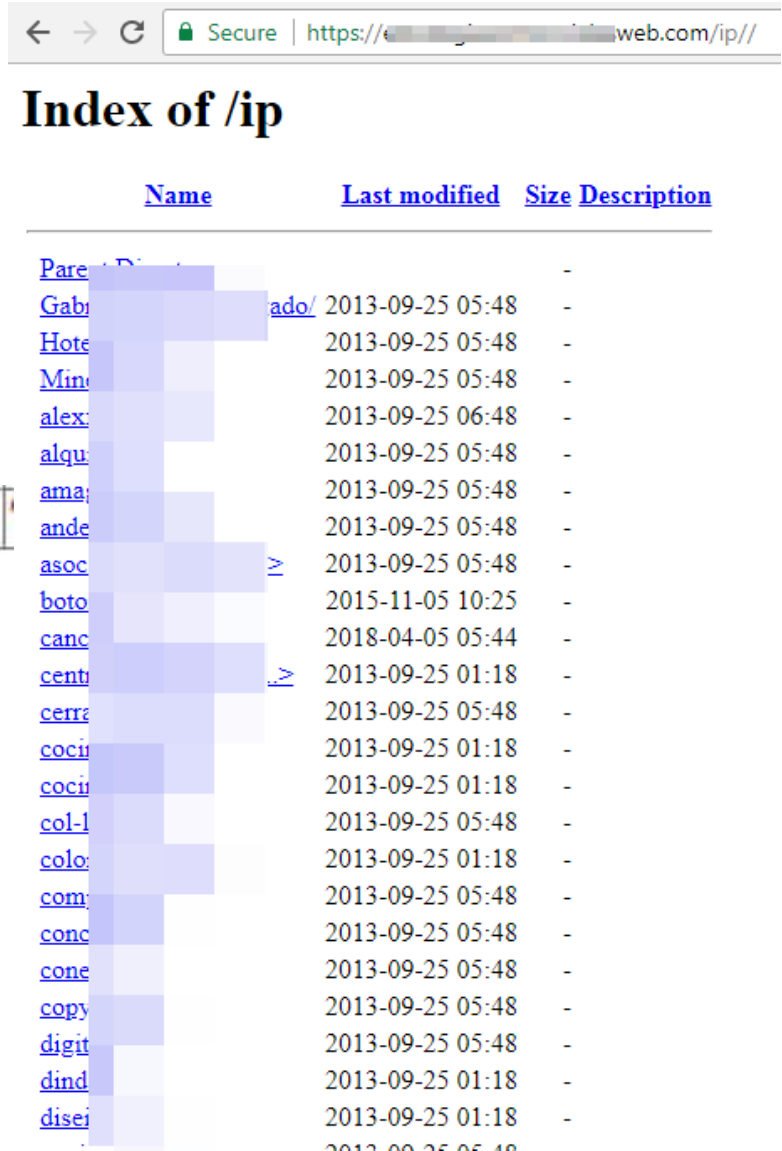
Hacking Proveedores

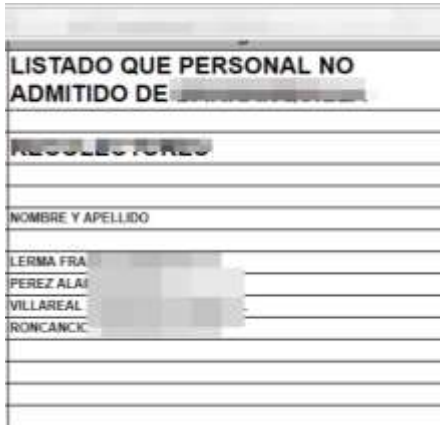
Hacking Proveedores

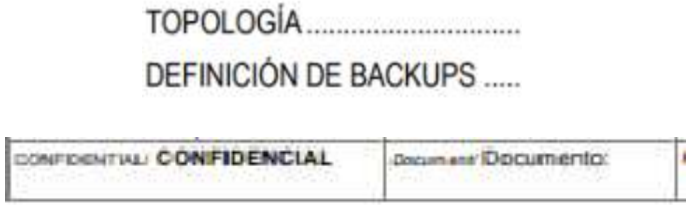
CASOS DE EXITO – NUESTROS CLIENTES

Hacking Proveedores





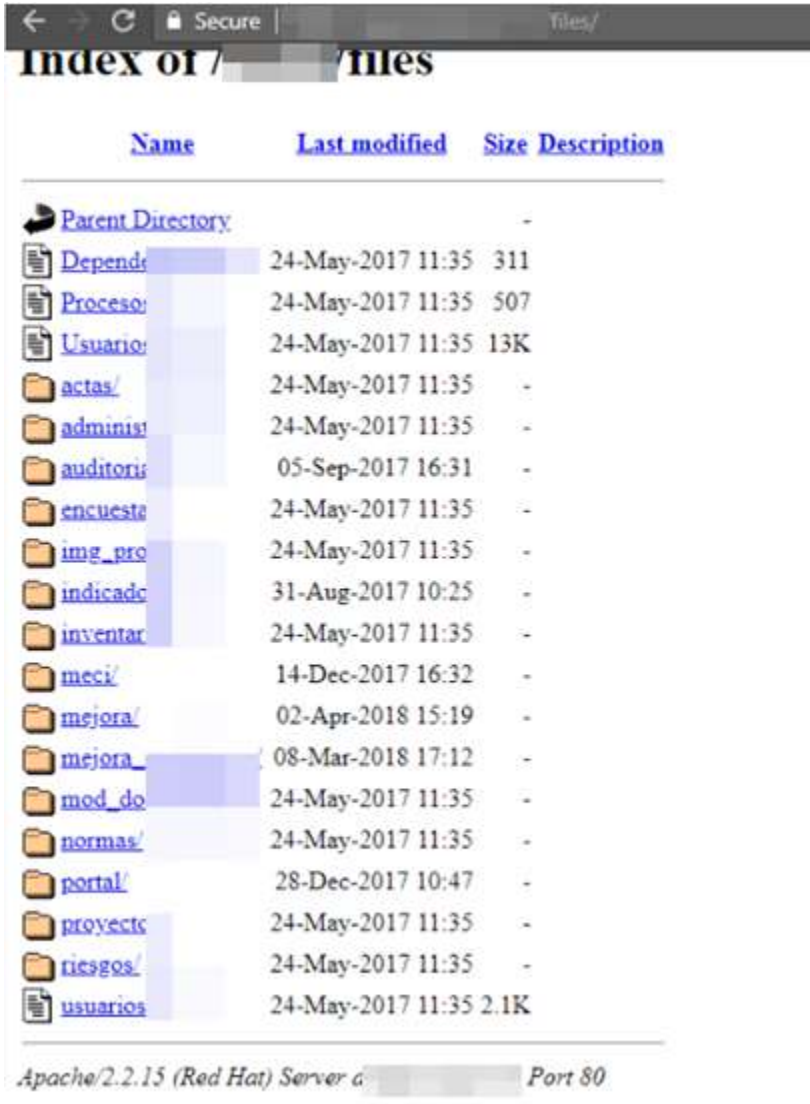




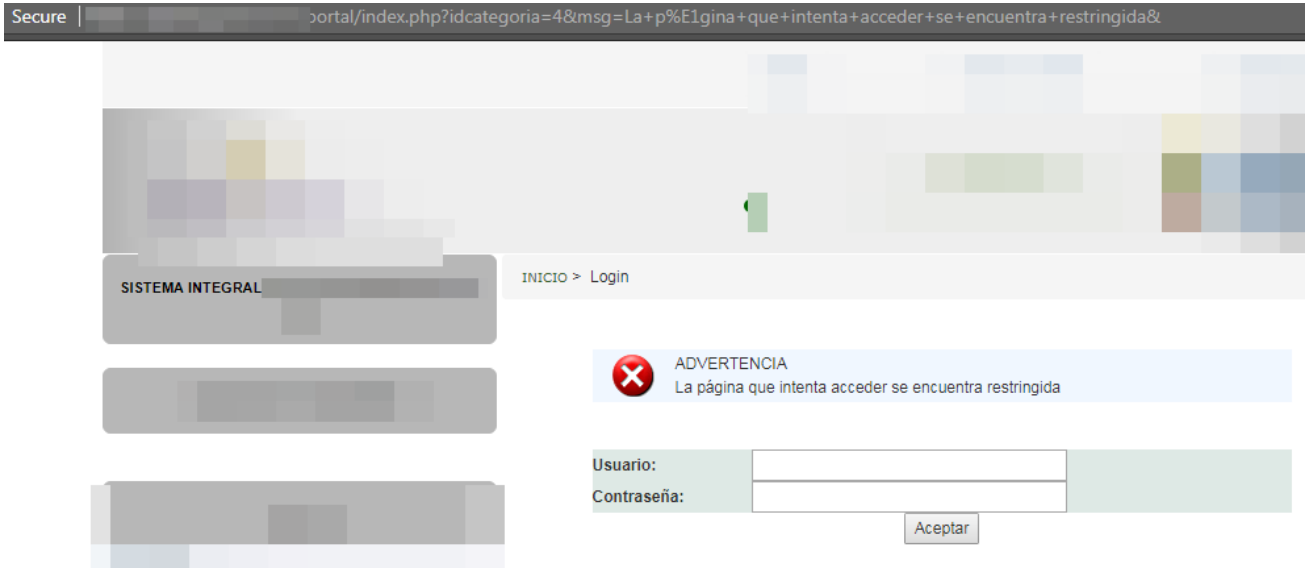
Hacking Proveedores

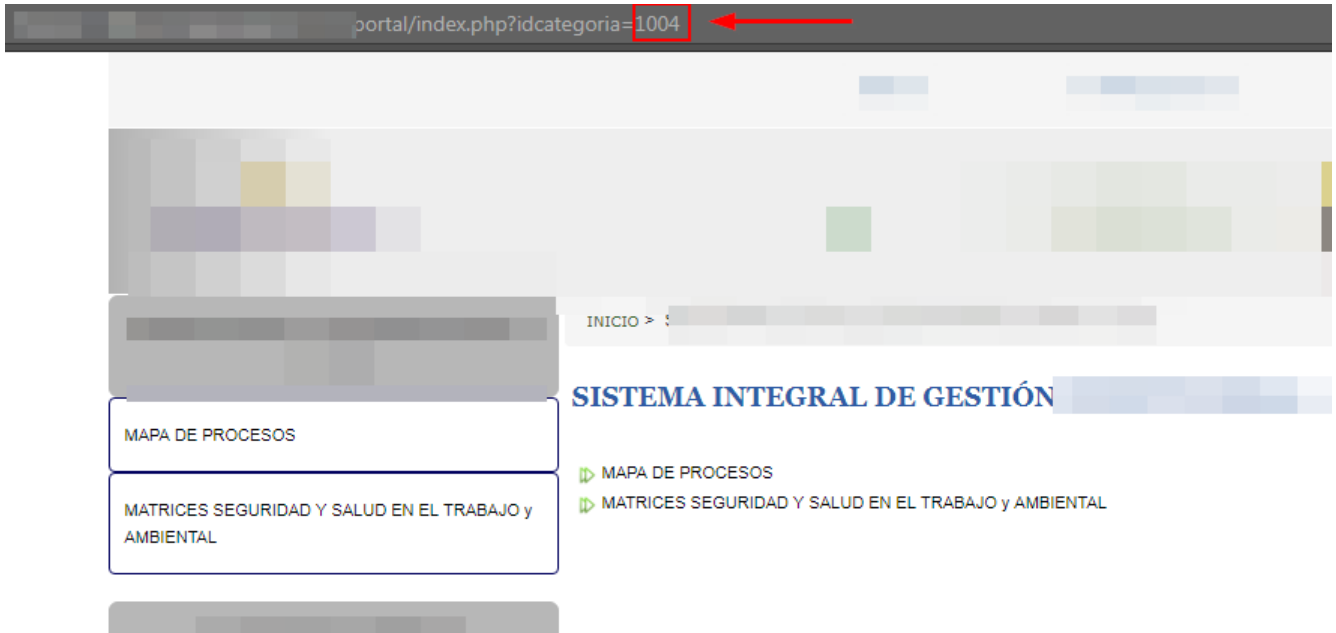

```
SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
SET time_zone = "+00:00";


/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;
```

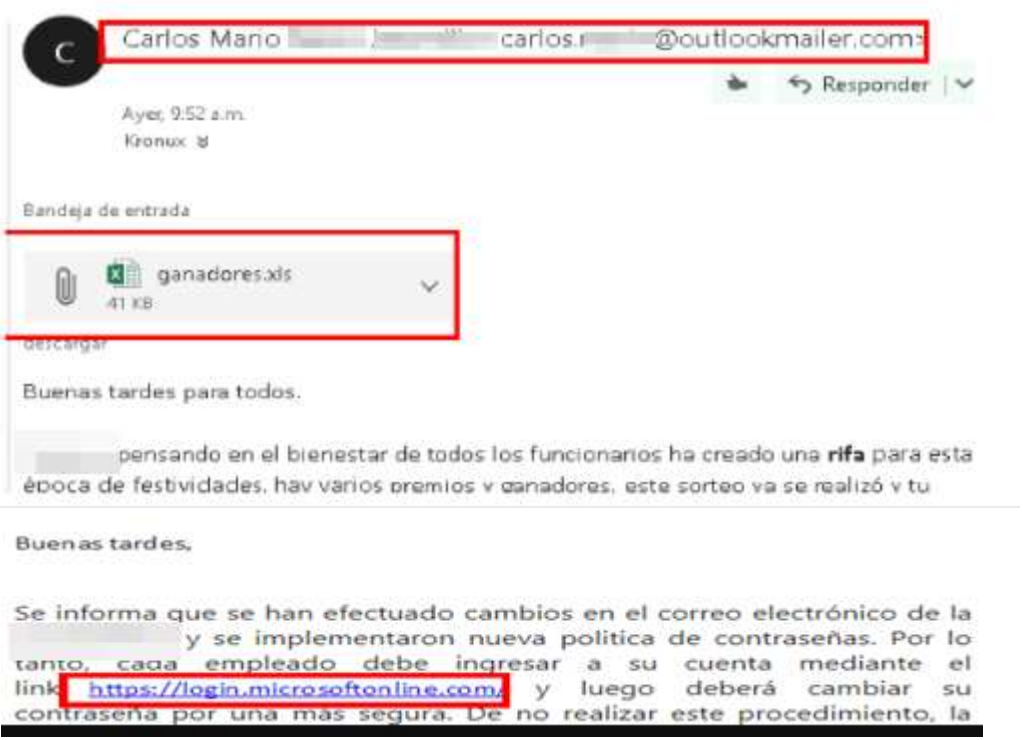


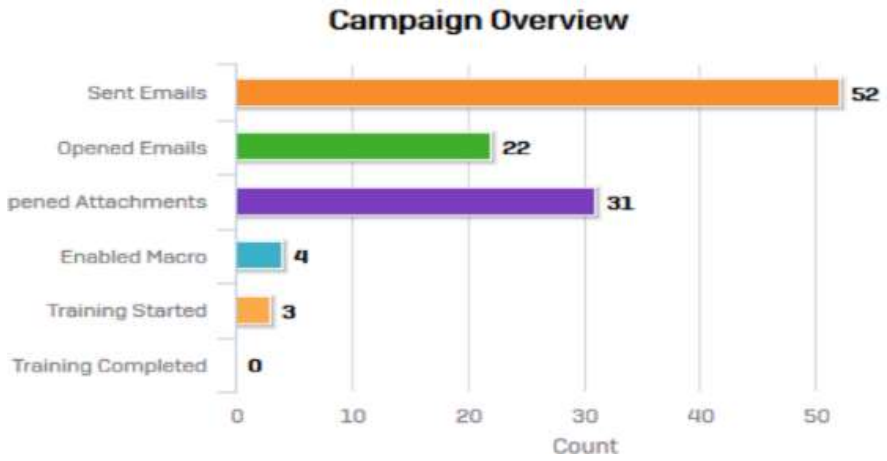
Hacking Proveedores

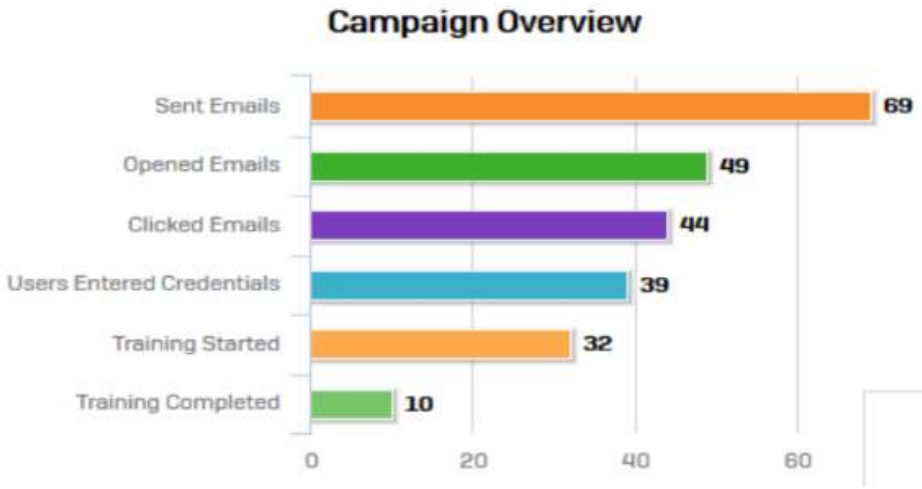




Phishing Proveedores / usuarios







Hacking IP's expuestas escritorio remoto

TOTAL RESULTS

12,077

TOP COUNTRIES

Colombia	12,077

TOP CITIES

Bogota	3,350
Medellin	2,517
Cali	275
Pereira	268
Bucaramanga	216

TOP ORGANIZATIONS

Telmex Colombia S.A.	4,107
UNE	2,719
ETB	1,465
Movistar Colombia	1,425
Ifx Networks Colombia	200

K•R N•U•X Solutions

DEMO

- **EXPLOTACION DESDE UN MOVIL A UN EQUIPO WINDOWS.**
- **AUTOMATIZACION PARA HACER ATAQUES MASIVOS.**