

Porque hackean las empresas ?



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

Hacking en la nube Multicloud



Backup en la nube



Office 365
Google Apps



Antivirus
Access Point /etc



Aplicativos propios



Aplicativos para ISO /
seguridad en el trabajo



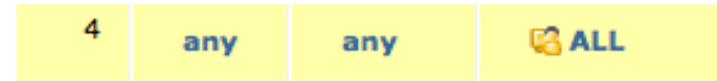
ERP / CRM /
Gestión Documental

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.



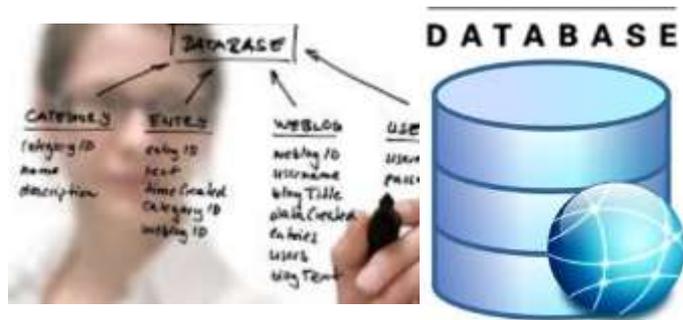
Hacking en perímetro interno



- 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

Red Hat Enterprise Linux Test Page

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, that sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf/serveicon.conf`.

You are free to use the image below on web sites powered by the Apache HTTP Server.



```
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 */;
```



Acceso	No. Radicado	Tipo Documento	Dependencia	Entidad	Tipo Entidad	Tipo Expediente	Nombre Expediente
	00000105	Expediente	CAF	PLA CO	AUC- FID- PLA		AUDITORIA
	00000103	Expediente	CAF	AC- IN- ME	AUC- FID-		A. FISCAL Y FINANCIERA
	00000023	Expediente	CAF	MU	AUC- EVA- FIN		
	00000023	Expediente	CAF	POI- VAI- ME	AUC- EVA- FIN		AU- DO

Index of /files/

Name Last modified Size Description

Name	Last modified	Size	Description
Parent Directory		-	
Depend	24-May-2017 11:35	311	
Proceso	24-May-2017 11:35	507	
Usuario	24-May-2017 11:35	13K	
actas/	24-May-2017 11:35	-	
adminis	24-May-2017 11:35	-	
auditori	05-Sep-2017 16:31	-	
encuesta	24-May-2017 11:35	-	
img_pro	24-May-2017 11:35	-	
indicad	31-Aug-2017 10:25	-	
inventar	24-May-2017 11:35	-	
meci/	14-Dec-2017 16:32	-	
mejora/	02-Apr-2018 15:19	-	
mejora_	08-Mar-2018 17:12	-	
mod_do	24-May-2017 11:35	-	
normas/	24-May-2017 11:35	-	
portal/	28-Dec-2017 10:47	-	
proyecto	24-May-2017 11:35	-	
riesgos/	24-May-2017 11:35	-	
usuarios	24-May-2017 11:35	2.1K	

Hacking Proveedores

Secure | portal/index.php?idcategoria=4&msg=La+p%E1gina+que+intenta+acceder+se+encuentra+restringida&

SISTEMA INTEGRAL

INICIO > Login

ADVERTENCIA
La página que intenta acceder se encuentra restringida

Usuario:

Contraseña:

Aceptar

portal/index.php?idcategoria=1004

INICIO > SISTEMA INTEGRAL DE GESTIÓN

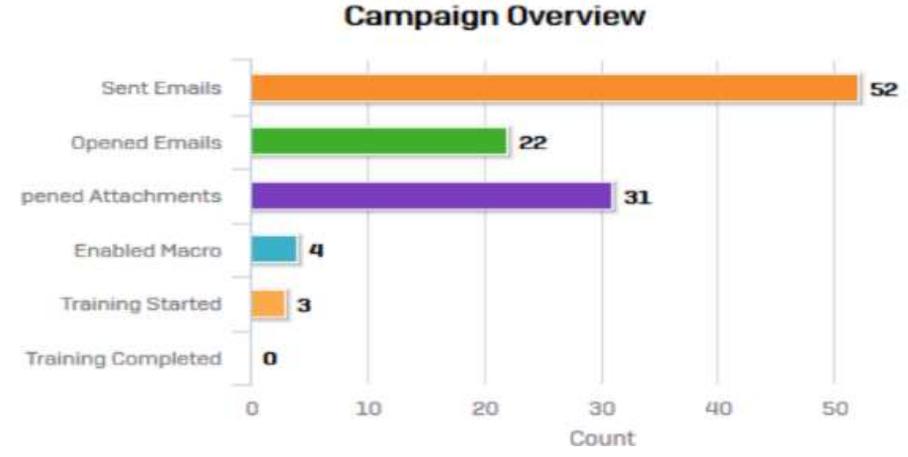
MAPA DE PROCESOS

MATRICES SEGURIDAD Y SALUD EN EL TRABAJO y AMBIENTAL

MAPA DE PROCESOS

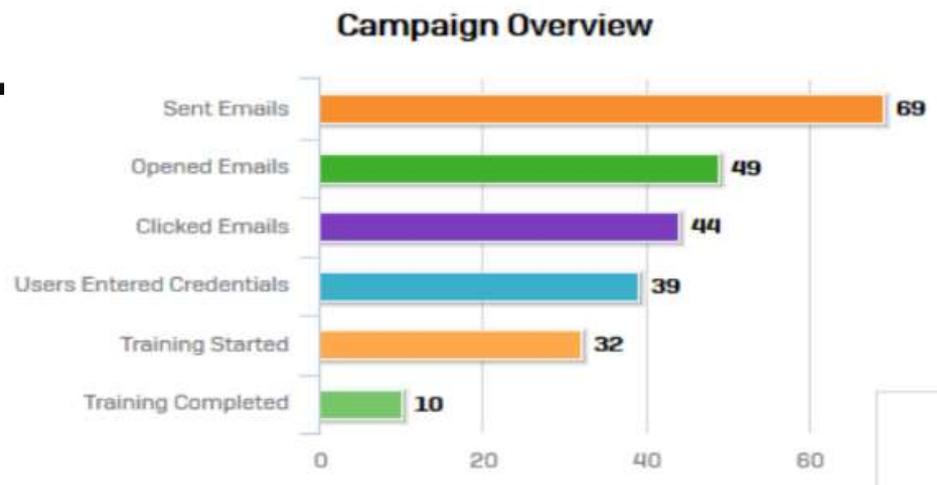
MATRICES SEGURIDAD Y SALUD EN EL TRABAJO y AMBIENTAL

Phishing Proveedores / usuarios



Buenas tardes,

Se informa que se han efectuado cambios en el correo electrónico de la ... y se implementaron nueva politica de contraseñas. Por lo tanto, cada empleado debe ingresar a su cuenta mediante el link <https://login.microsoftonline.com> y luego deberá cambiar su contraseña por una más segura. De no realizar este procedimiento, la



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



DEMO

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