

Porque hackean las empresas ?



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

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.
- Bajaron la seguridad en las sedes principales porque los servidores están en la nube

Hacking en la nube Multicloud



Backup en la nube



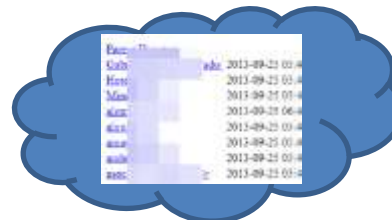
Office 365
Google Apps



Antivirus
Access Point /etc



Aplicativos propios



Aplicativos para ISO /
seguridad en el trabajo



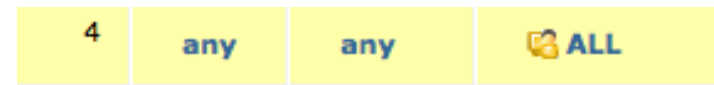
ERP / CRM /
Gestión Documental

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.



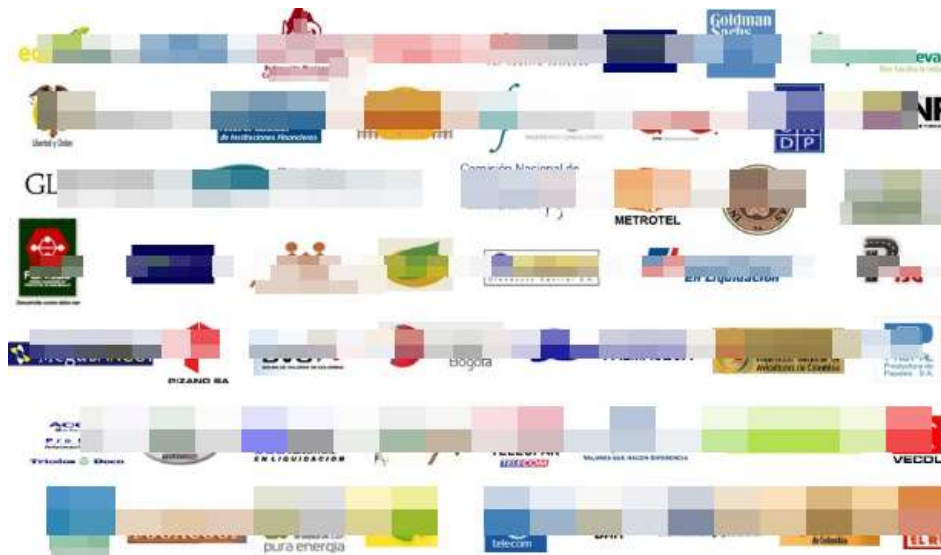
Hacking Proveedores



Hacking Proveedores



CASOS DE EXITO – NUESTROS CLIENTES



Hacking Proveedores

Google search results for [https://\[redacted\]web.com/ip/](https://[redacted]web.com/ip/). Results include a link to the same URL.

Secure | [https://\[redacted\]web.com/ip/](https://[redacted]web.com/ip/)

Index of /ip

Name	Last modified	Size	Description
Parent Directory			-
Gabo	2013-09-25 05:48		-
Hoteles	2013-09-25 05:48		-
Min	2013-09-25 05:48		-
alex	2013-09-25 06:48		-
alqu	2013-09-25 05:48		-
ama	2013-09-25 05:48		-
ande	2013-09-25 05:48		-
asoc	2013-09-25 05:48		-
boto	2015-11-05 10:25		-
canc	2018-04-05 05:44		-
cent	2013-09-25 01:18		-
cerra	2013-09-25 05:48		-
cocin	2013-09-25 01:18		-
cocin	2013-09-25 01:18		-
col-1	2013-09-25 05:48		-
colo	2013-09-25 01:18		-
com	2013-09-25 05:48		-
conc	2013-09-25 05:48		-
cone	2013-09-25 05:48		-
copy	2013-09-25 05:48		-
digit	2013-09-25 05:48		-
dind	2013-09-25 01:18		-
disc	2013-09-25 01:18		-

LISTADO QUE PERSONAL NO ADMITIDO DE

REFLECTORES
NOMBRE Y APELLIDO
LERMA FRA
PEREZ ALAI
VILLAREAL
RONCANCIC

TOPOLOGÍA.....

DEFINICIÓN DE BACKUPS

CONFIDENTIAL CONFIDENCIAL Document Documento

Atentamente,

SECRETARÍA

Not secure | [redacted]

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/7.0.59

The Apache Software Foundation
http://www.apache.org/

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:
[Security Considerations HOW-TO](#)
[Manager Application HOW-TO](#)
[Clustering/Session Replication HOW-TO](#)

Server Status
Manager App
Host Manager

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

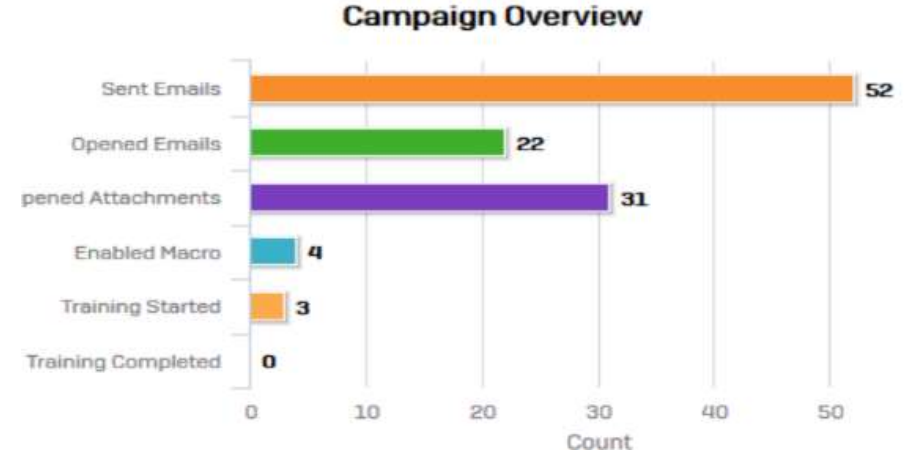
MAPA DE PROCESOS

MATRICES SEGURIDAD Y SALUD EN EL TRABAJO y AMBIENTAL

MAPA DE PROCESOS

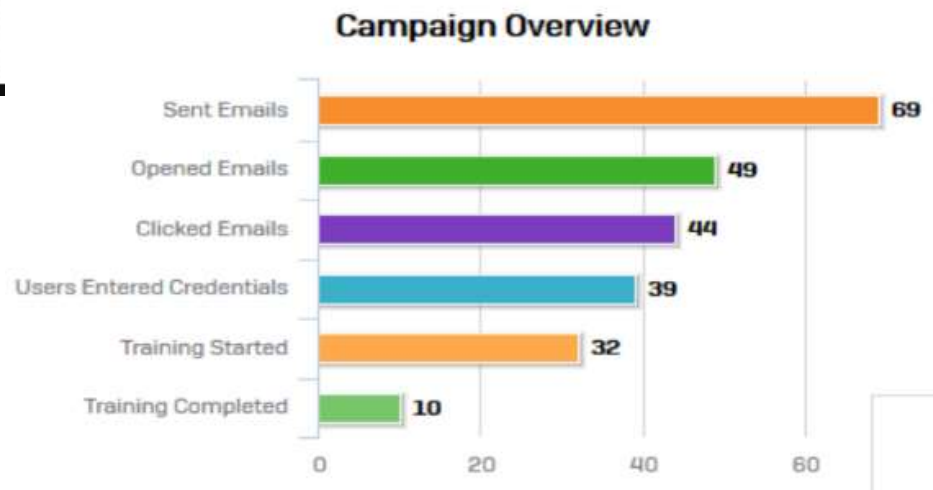
MATRICES SEGURIDAD Y SALUD EN EL TRABAJO y AMBIENTAL

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.**