Como Convertirte en un Profesional de la Seguridad Informática

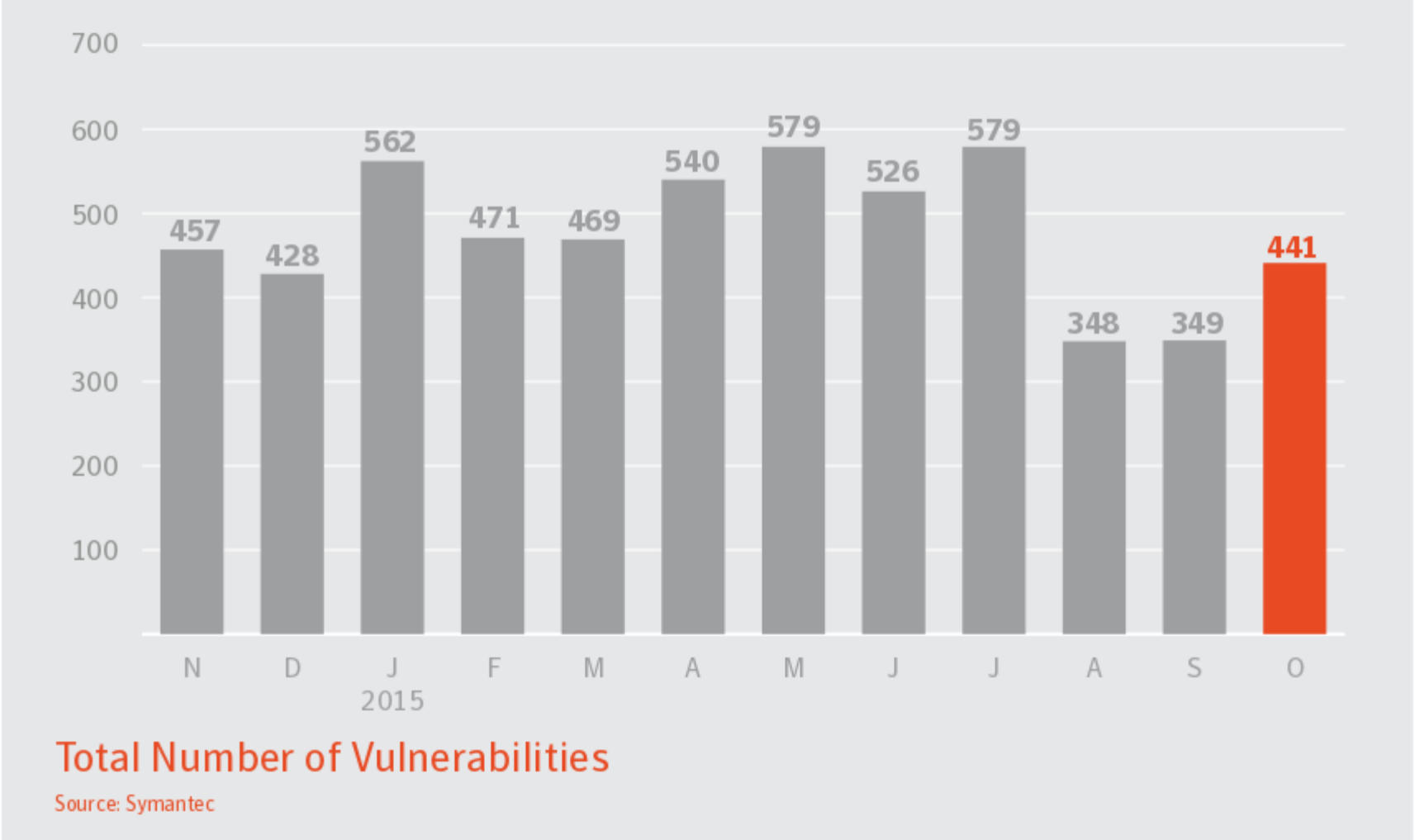
Fabian Martinez Portantier

- Consultor en Seguridad Informática
- Co-Fundador de Securetia (www.securetia.com)
- Instructor y Escritor sobre el tema
- Coordinador de la Carrera de Seguridad

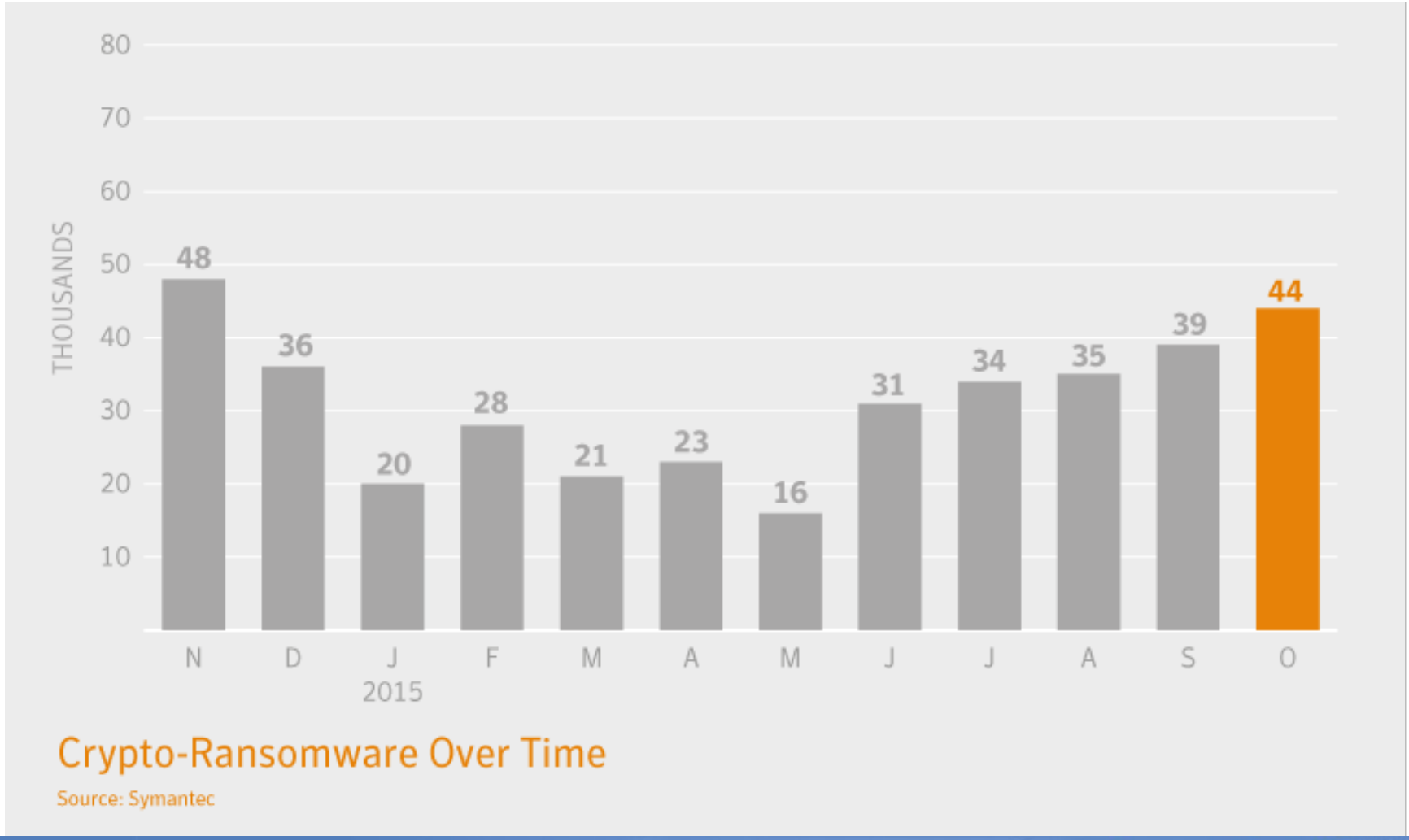
Objetivos

- Comprender el mercado de la seguridad
- Conocer algunas herramientas útiles
- Sacarnos dudas
- Divertirnos! :)

Algunas estadísticas



Algunas estadísticas



Algunas estadísticas

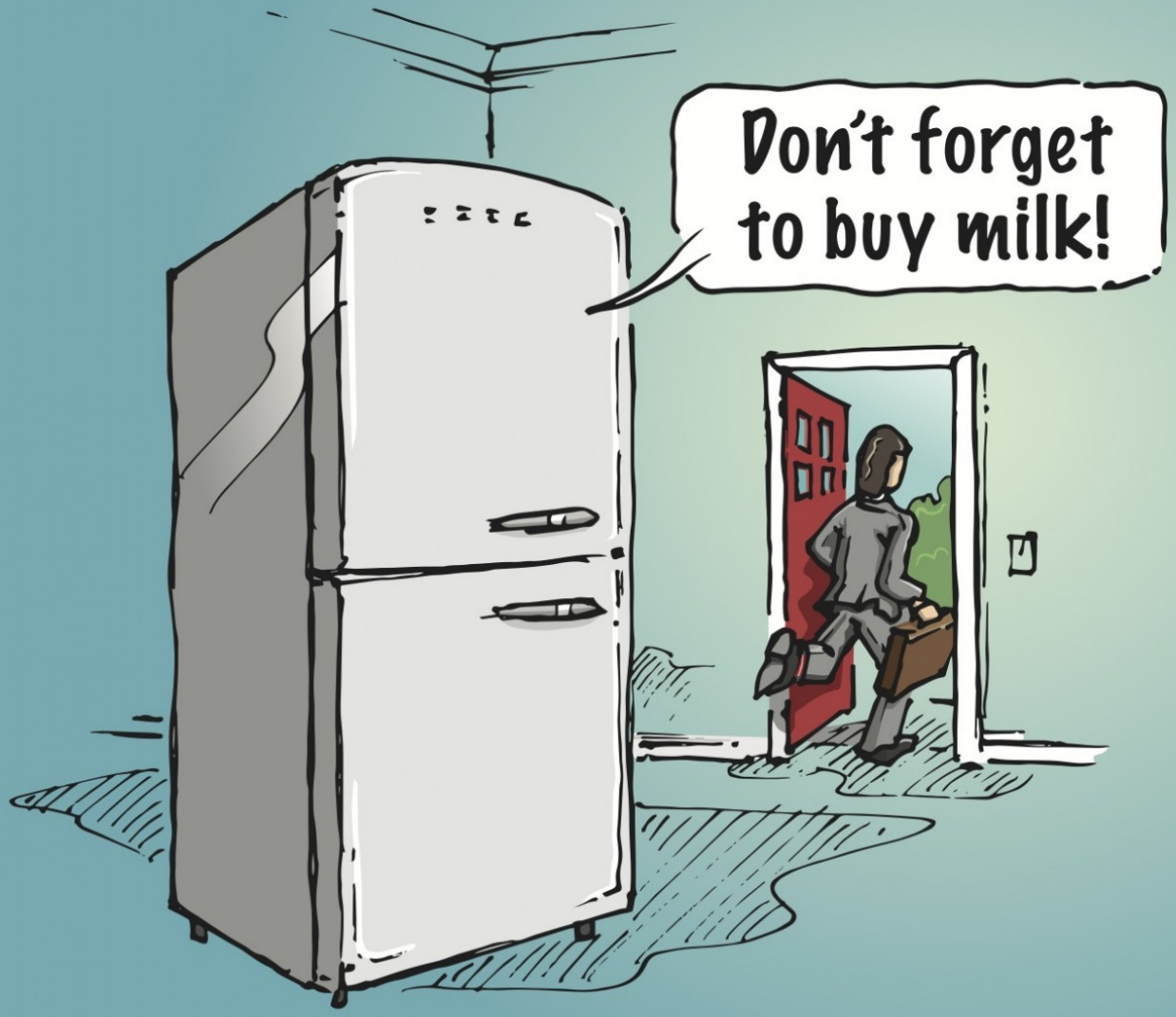
"More secure software,
NOT more security software."

(Website Security Statistics Report 2015)

Algunas estadísticas

Item	2014 Cost
1,000 Stolen Email Addresses	$0.50 to $10
Credit Card Details	$0.50 to $20
Scans of Real Passports	$1 to $2
Stolen Gaming Accounts	$10 to $15
Custom Malware	$12 to $3500
Value of Information Sold on Black Market	

Item	2014 Cost
1,000 Social Network Followers	$2 to $12
Stolen Cloud Accounts	$7 to $8
1 Million Verified Email Spam Mail-outs	$70 to $150
Registered and Activated Russian Mobile Phone SIM Card	$100
Value of Information Sold on Black Market	


Don't forget to buy milk!

Algunas estadísticas

7 de los 10 dispositivos IoT más utilizados contenían vulnerabilidades serias

(HP Internet of Things Research Study 2014)

THE FBI FEDERAL BUREAU OF INVESTIGATION

CONTACT US | ABOUT US | MOST WANTED | NEWS

Wanted by the FBI

Home • Most Wanted • Cyber's Most Wanted

Cyber's Most Wanted

Select the images of suspects to display more information.

EVGENIY MIKHAILOVICH BOGACHEV

NICOLAE POPESCU

ALEXSEY BELAN

JOSHUA SAMUEL AARON

VIET QUOC NGUYEN

CARLOS ENRIQUE

SUN KAILIANG

HUANG ZHENYU

WEN XINYU

WANG DONG

Algunas estadísticas

¿Está preparado para un ciberataque sofisticado?
NO → 52%

¿Están los ciberataques entre sus tres principales preocupaciones?
SI → 82%

¿Cree que faltan profesionales calificados?
SI → 86%

(2015 Global Cybersecurity Status Report – LATAM Data)

BBC | Ingresar | Menú

MUNDO

Noticias | América Latina | Internacional | Economía | Tecnología | Ciencia | Salud

Si quiere un empleo, luche contra el ciberterror

Sean Coughlan
BBC

6 abril 2014

Dice la sabiduría popular que no hay mal que por bien no venga. Y en la era de los ataques tecnológicos cada vez más frecuentes y generalizados, también hay un beneficio oculto tras el llamado ciberterrorismo.

Se necesitan cada vez más "ciberpolicías" para protegernos de los ataques informáticos.

www.bbc.com/mundo/noticias/2014/04/140329_economia_empleo_ciberseguridad_ataques_finde_aa

Puestos en InfoSec

- Chief Information Security Officer (CISO)
- Security Manager
- Security Engineer
- Incident Responder
- Security Consultant
- Security Auditor
- Computer Forensics Expert
- Malware Analyst
- Security Specialist
- Penetration Tester
- Vulnerability Researcher

¿Qué se espera de los profesionales de la Seguridad Informática?

Criptografía

GNU/Linux

Redes

Ethical Hacking

Mobile

Windows

Web

Malware

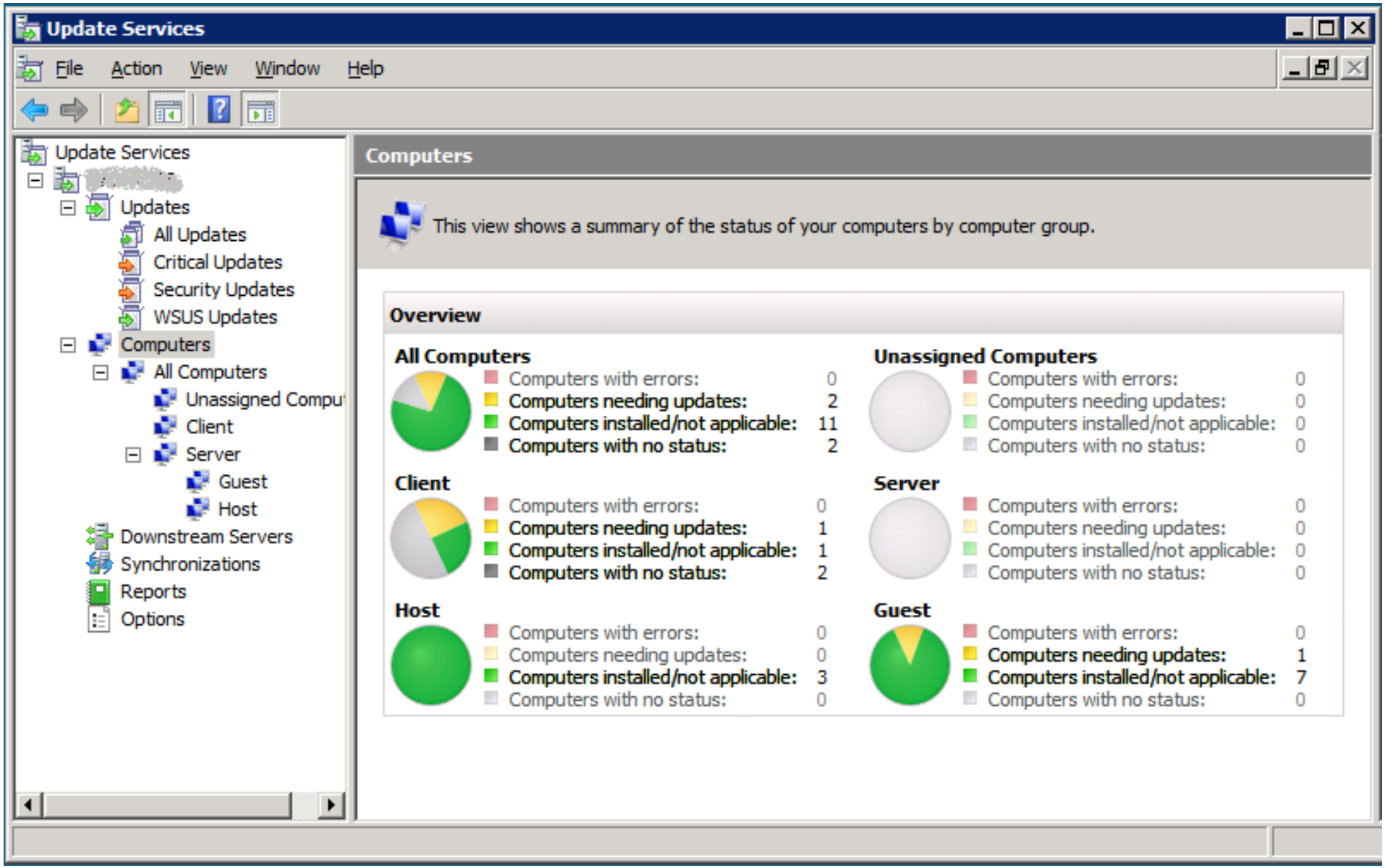
Nuestros Cursos

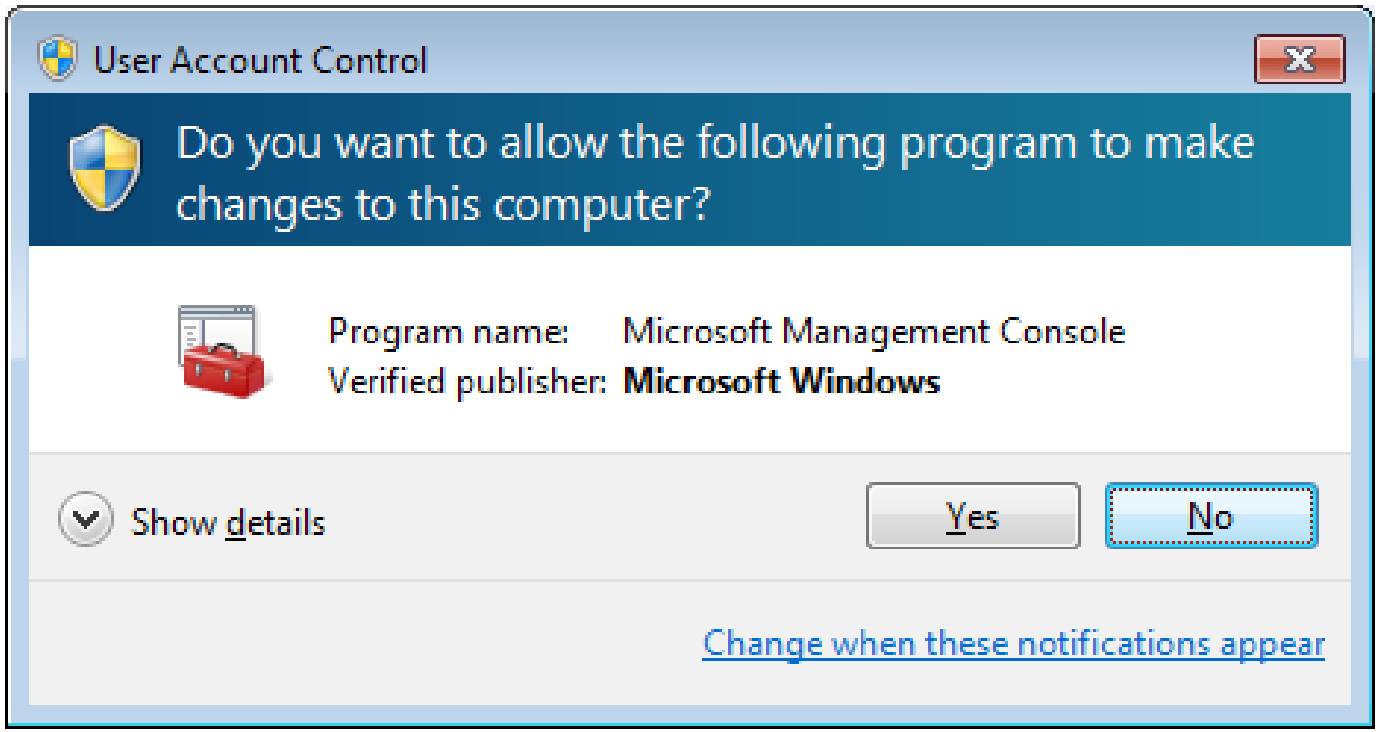
- Introducción a la Seguridad Informática
- Seguridad en Redes
- Seguridad Web
- Seguridad GNU/Linux
- Desarrollo Seguro
- Ethical Hacking
- Administración Android
- Ethical Hacking para Programadores
- Instalación y Configuración de Windows Server
- Google Hacking e Ingeniería Social
- Seguridad Física y Aspectos Legales

Seguridad Windows

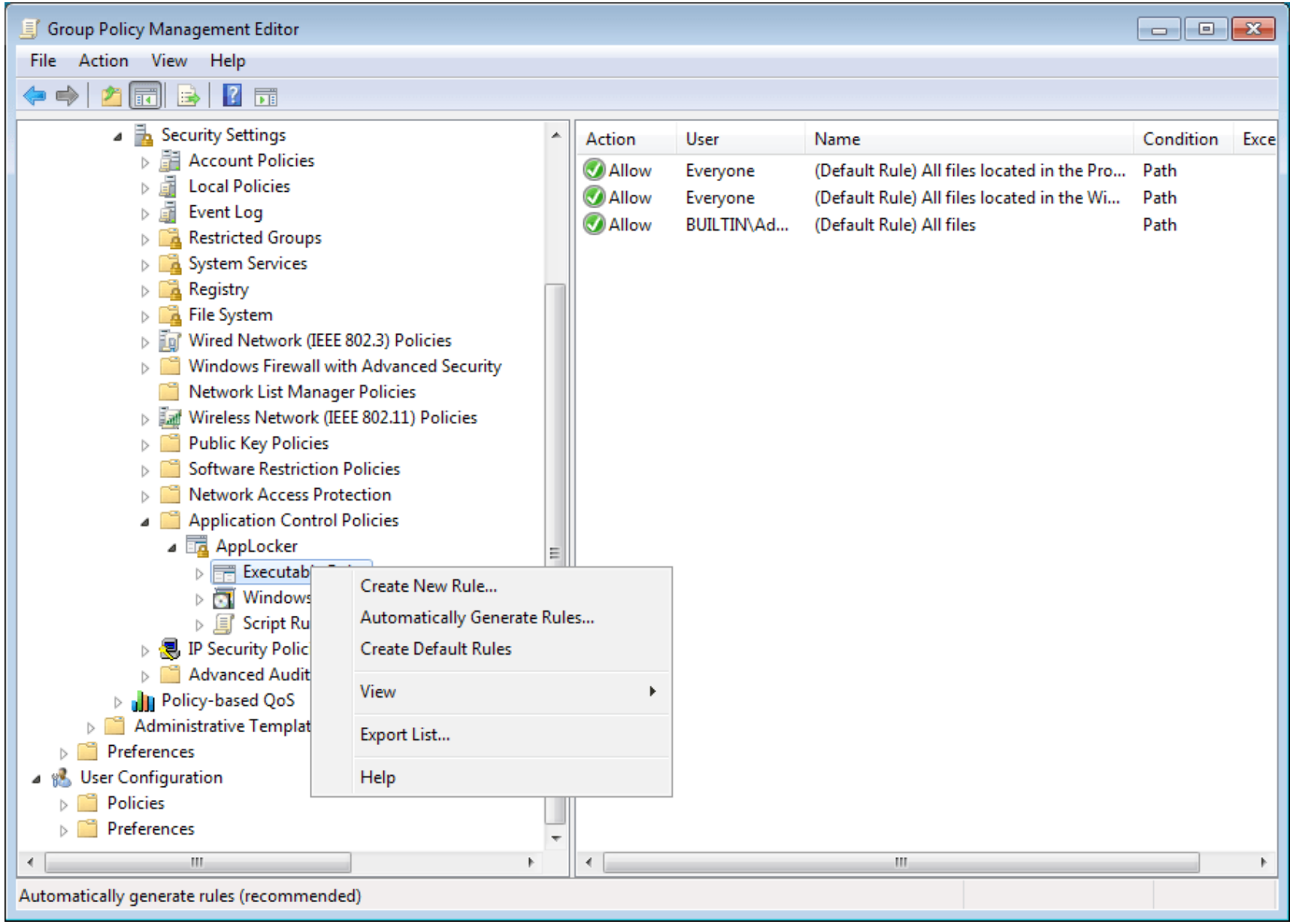
Seguridad Windows

- *Windows Server Update Services*
- *User Account Control (UAC)*
- *BitLocker*
- *AppLocker*
- *Baseline Security Analyzer*


Update Services
File Action View Window Help
Update Services
[redacted]
Updates
All Updates
Critical Updates
Security Updates
WSUS Updates
Computers
All Computers
Unassigned Compu
Client
Server
Guest
Host
Downstream Servers
Synchronizations
Reports
Options
Computers
This view shows a summary of the status of your computers by computer group.
Overview
All Computers
Computers with errors: 0
Computers needing updates: 2
Computers installed/not applicable: 11
Computers with no status: 2
Unassigned Computers
Computers with errors: 0
Computers needing updates: 0
Computers installed/not applicable: 0
Computers with no status: 0
Client
Computers with errors: 0
Computers needing updates: 1
Computers installed/not applicable: 1
Computers with no status: 2
Server
Computers with errors: 0
Computers needing updates: 0
Computers installed/not applicable: 0
Computers with no status: 0
Host
Computers with errors: 0
Computers needing updates: 0
Computers installed/not applicable: 3
Computers with no status: 0
Guest
Computers with errors: 0
Computers needing updates: 1
Computers installed/not applicable: 7
Computers with no status: 0

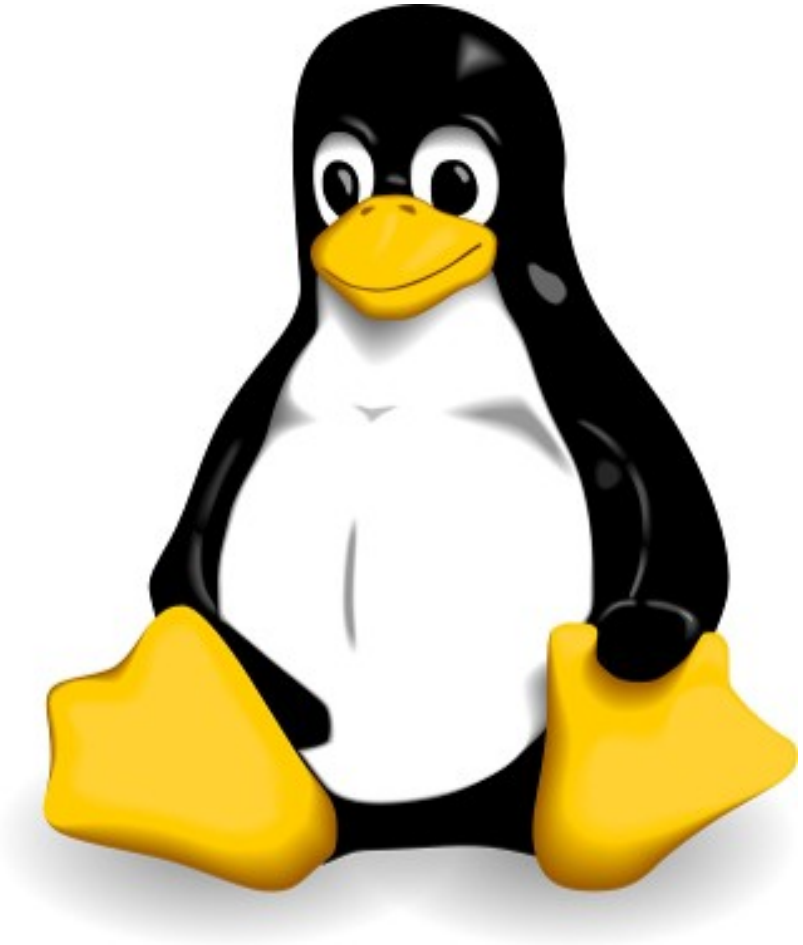

User Account Control
Do you want to allow the following program to make changes to this computer?
Program name: Microsoft Management Console
Verified publisher: Microsoft Windows
Show details
Yes
No
Change when these notifications appear


« All Control Panel I... ▸ BitLocker Drive Encryption
Search Control Panel
Control Panel Home
Help protect your files and folders by encrypting your drives
BitLocker Drive Encryption helps prevent unauthorized access to any files stored on the drives shown below. You are able to use the computer normally, but unauthorized users cannot read or use your files.
What should I know about BitLocker Drive Encryption before I turn it on?
BitLocker Drive Encryption - Hard Disk Drives
C:
On
Turn Off BitLocker
Suspend Protection
Manage BitLocker
HP_TOOLS (Z:)
Off
Turn On BitLocker
BitLocker Drive Encryption - BitLocker To Go
D:
Off
Turn On BitLocker
See also
TPM Administration
Disk Management
Read our privacy statement online


Group Policy Management Editor
File Action View Help
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
AppLocker
Create New Rule...
Automatically Generate Rules...
Create Default Rules
View
Export List...
Help
IP Security Polic
Advanced Audit
Policy-based QoS
Administrative Templat
Preferences
User Configuration
Policies
Preferences
Action User Name Condition Exce
Allow Everyone (Default Rule) All files located in the Pro... Path
Allow Everyone (Default Rule) All files located in the Wi... Path
Allow BUILTIN\Ad... (Default Rule) All files Path
Automatically generate rules (recommended)


Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft
Report Details for WORKGROUP - WIN-AQ5MBV0BQQ5 (2014-09-18 16:20:27)
Computer name: WORKGROUP\WIN-AQ5MBV0BQQ5
IP address: 192.168.128.129
Security report name: WORKGROUP - WIN-AQ5MBV0BQQ5 (2014-9-18 下午 04-20)
Scan date: 2014/9/18 下午 04:20
Scanned with MBSA version: 2.3.2208.0
Catalog synchronization date:
Security update catalog: Microsoft Update
Security Update Scan Results
Score
Issue
Result
Developer Tools, Runtimes, and Redistributables Security Updates
2 security updates are missing.
What was scanned
Result details
How to correct this
SQL Server Security Updates
1 security updates are missing.
What was scanned
Result details
How to correct this
Windows Security Updates
15 security updates are missing. 2 service packs or update rollups are missing.
What was scanned
Result details
How to correct this

Seguridad GNU/Linux



Seguridad GNU/Linux

Lynis (www.rootkit.nl)

```
[+] Software: PHP
------------------------------------
  - Checking PHP...                              [ FOUND ]
    - Checking PHP disabled functions...         [ NONE ]
    - Checking register_globals option...        [ WARNING ]
    - Checking expose_php option...              [ ON ]
    - Checking enable_dl option...               [ OFF ]
    - Checking allow_url_fopen option...         [ ON ]
    - Checking allow_url_include option...       [ OFF ]
```

Seguridad Web

Seguridad Web

Están totalmente expuestas
(Muchas accesibles desde internet)

Usan muchas tecnologías diferentes
(JavaScript, SQL, HTTP, PHP, Java, etc)

OWASP Top 10 2013

A1- Inyección	A2 – Pérdida de Autenticación y Gestión de Sesiones	A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	A4 – Referencia Directa Insegura a Objetos	A5 – Configuración de Seguridad Incorrecta
A6 – Exposición de datos sensibles	A7 – Ausencia de Control de Acceso a Funciones	A8 - Falsificación de Peticiones en Sitios Cruzados (CSRF)	A9 – Utilización de componentes con vulnerabilidades conocidas	A10 – Redirecciones y reenvios no validados

OWASP Top 10 2013

"10 Vulnerabilidades No Requieren 10 Medidas de Seguridad"

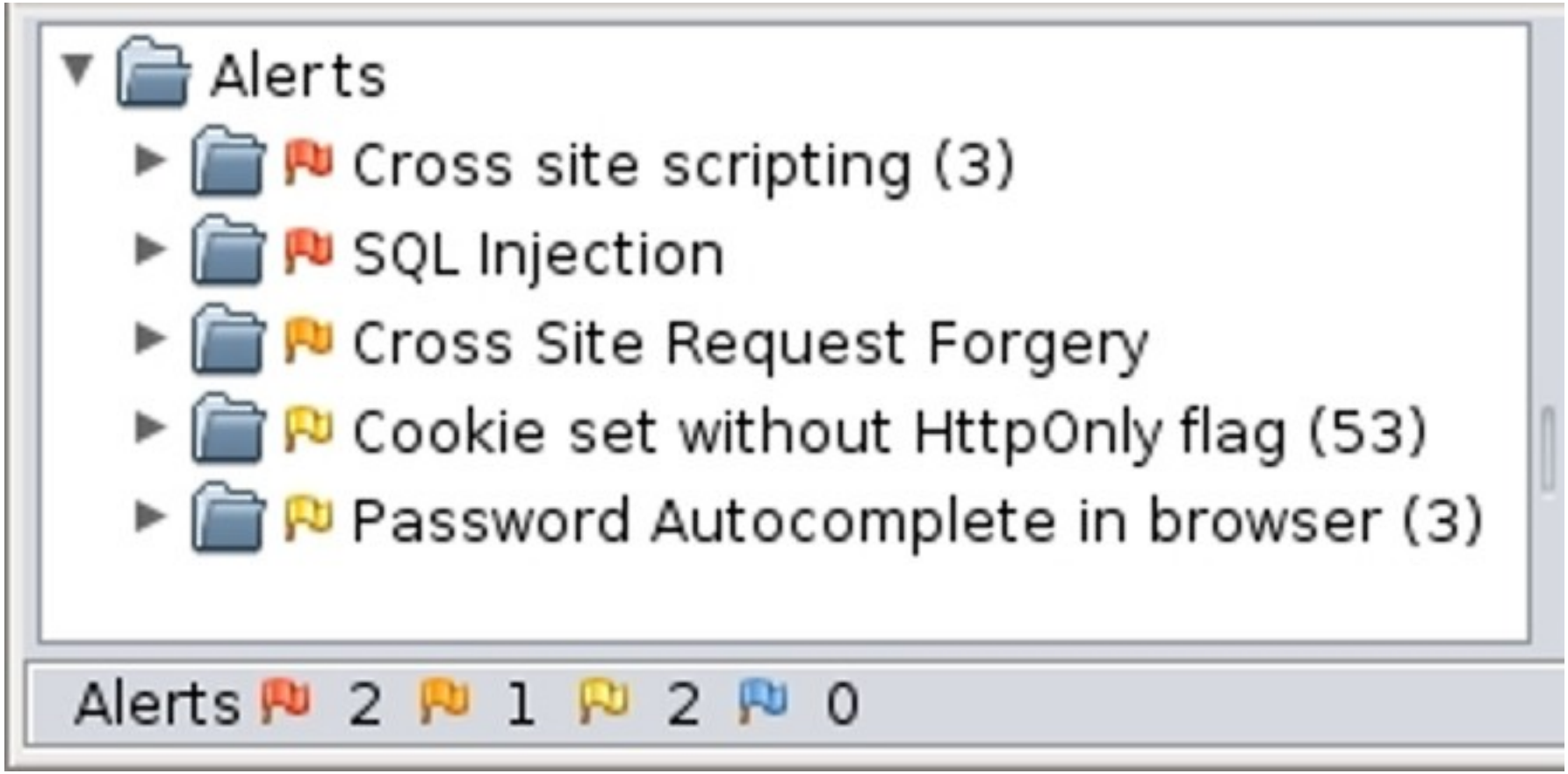
(Validar Datos y Acciones Mitigan 7 de las 10 Vulnerabilidades)

Validación de Datos en PHP

```
if(filter_var($email, FILTER_VALIDATE_EMAIL))
{
   echo “OK”;
}
else
{
   echo “ERROR”;
}
```

Seguridad Web

Zed Attack Proxy (www.owasp.org)



Ethical Hacking

Ethical Hacking

¿Qué tan difícil es penetrar en un sistema?

(Video)

Ethical Hacking

Herramienta Recomendada:

Metasploit

(www.metasploit.com)

¿Preguntas?

MUCHAS GRACIAS!

Fabian Martinez Portantier
Coordinador Carrera Seguridad Informática

seguridadinformatica@educacionit.com
www.educacionit.com

Argentina, Capital Federal
(54) (011) 4328-0457