

Como Convertirte en un Profesional de la Seguridad Informática

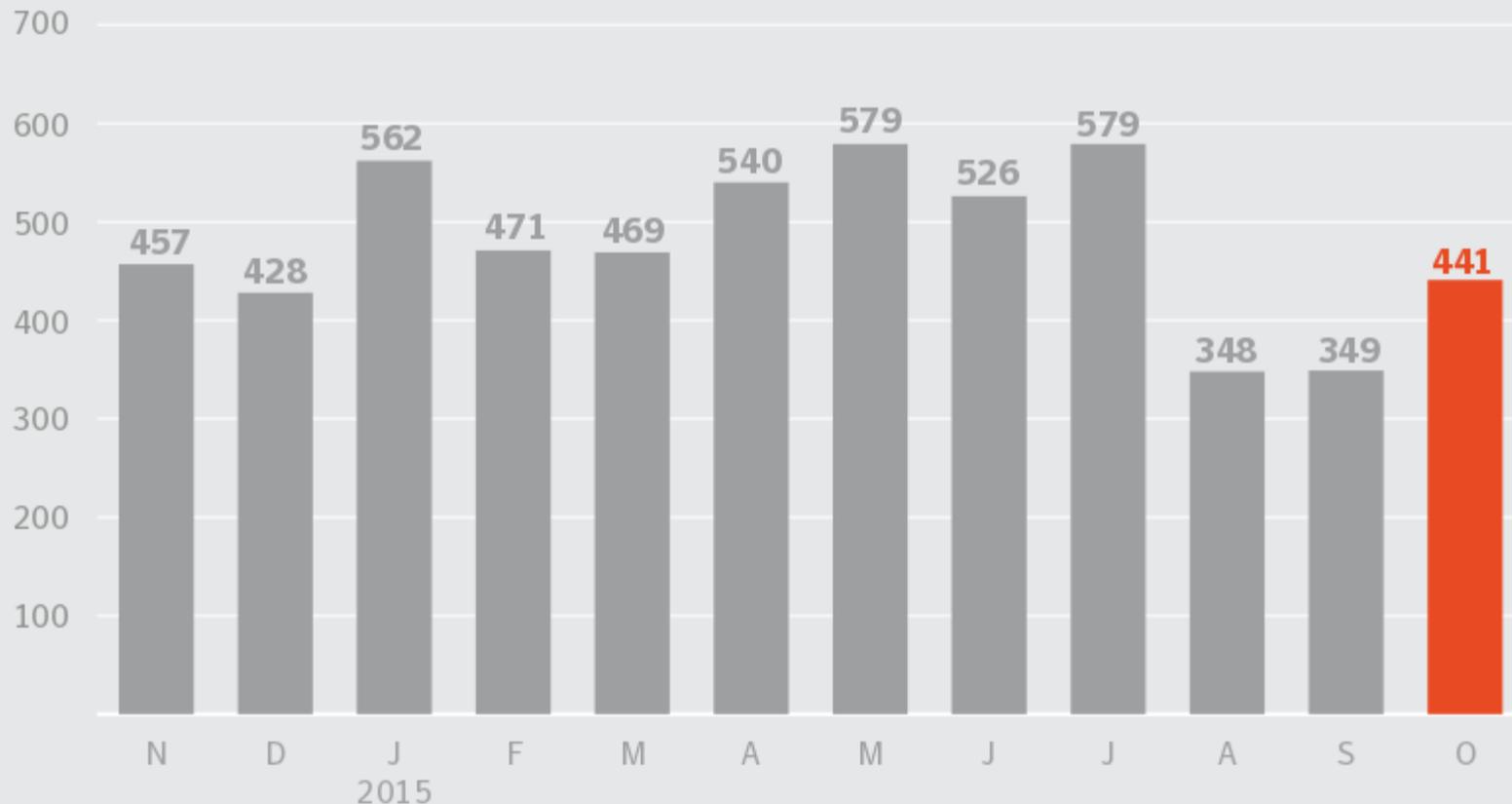
Fabian Martinez Portantier

- 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



Total Number of Vulnerabilities

Source: Symantec

Algunas estadísticas



Crypto-Ransomware Over Time

Source: Symantec

Algunas estadísticas

***“More secure software,
NOT more security software.”***

***(WhiteHat Security,
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	



Algunas estadísticas

7 de los 10 dispositivos IoT más utilizados contenían vulnerabilidades serias

(HP Internet of Things Research Study 2014)

VIERNES 24 DE JULIO DEL 2015 | 13:03

Chrysler retira 1,5 millones de autos tras hackeo de su jeep

La empresa decidió retirar diversos modelos de sus vehículos con el fin de actualizar sus sistemas informáticos

 Compartir

8

 Twittear

0

 G+1

0

 Compartir

2

 Pinit

0

 0





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%

**(ISACA 2015 Global Cybersecurity
Status Report - LATAM Data)**

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

Héctor Alonso: "Un número uno en ciberseguridad ya cuesta tanto como uno de ventas"

El presidente de Level 3 para América latina advierte sobre el crecimiento de los ataques informáticos; dice que hay que superar la antinomia público-privado en el desarrollo de las telecomunicaciones cuya incidencia en el PBI crece

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

Windows

Mobile

Web

Malware

Nuestros Cursos

Introducción a la
Seguridad Informática

Seguridad en
Redes

Seguridad
Web

Seguridad
GNU/Linux

Desarrollo
Seguro

Ethical Hacking

Administración
Android

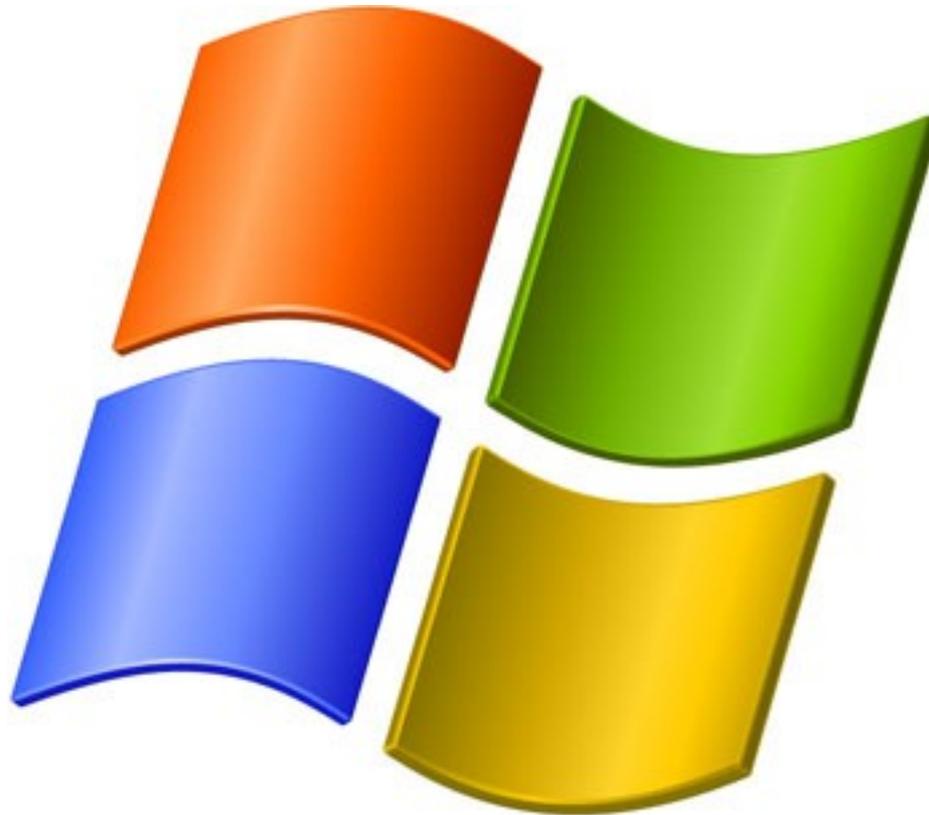
Ethical Hacking
para Programadores

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*

The screenshot displays the Windows Update Services console. The left-hand pane shows a tree view with 'Update Services' expanded to 'Computers'. The right-hand pane, titled 'Computers', provides a summary of the status of computers by group. It includes an 'Overview' section with six pie charts and their corresponding data tables.

Computers

This view shows a summary of the status of your computers by computer group.

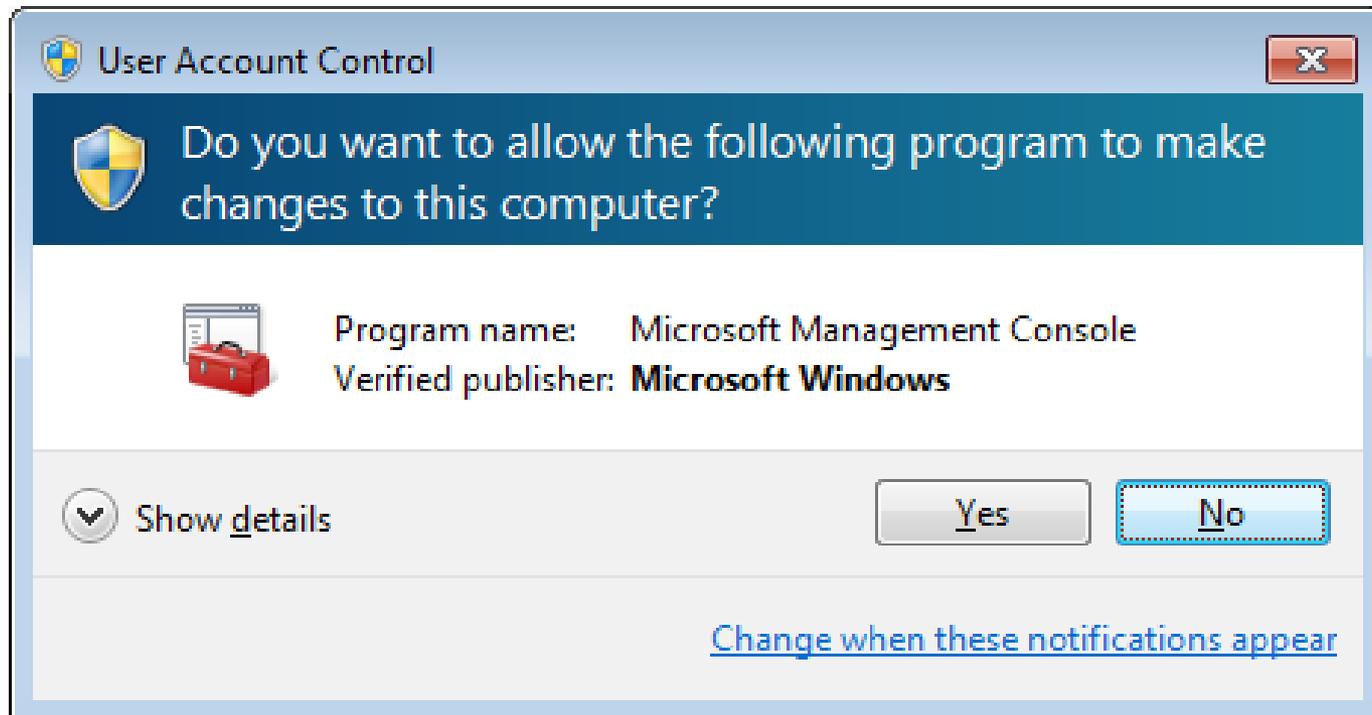
Overview

Group	Computers with errors	Computers needing updates	Computers installed/not applicable	Computers with no status
All Computers	0	2	11	2
Unassigned Computers	0	0	0	0
Client	0	1	1	2
Server	0	0	0	0
Host	0	0	3	0
Guest	0	1	7	0

Seguridad Windows

La Importancia de los Parches

**Video:
MS08-067**





The screenshot shows the Windows Control Panel window for BitLocker Drive Encryption. The title bar reads "All Control Panel I... BitLocker Drive Encryption". The address bar contains "Search Control Panel". The main content area is titled "Control Panel Home" and features a heading: "Help protect your files and folders by encrypting your drives". Below this, a paragraph explains that BitLocker Drive Encryption helps prevent unauthorized access to files on the drives shown. A link asks "What should I know about BitLocker Drive Encryption before I turn it on?".

The page is divided into two sections: "BitLocker Drive Encryption - Hard Disk Drives" and "BitLocker Drive Encryption - BitLocker To Go".

BitLocker Drive Encryption - Hard Disk Drives

Drive	Status	Actions
C:	On	Turn Off BitLocker , Suspend Protection , Manage BitLocker
HP_TOOLS (Z:)	Off	Turn On BitLocker

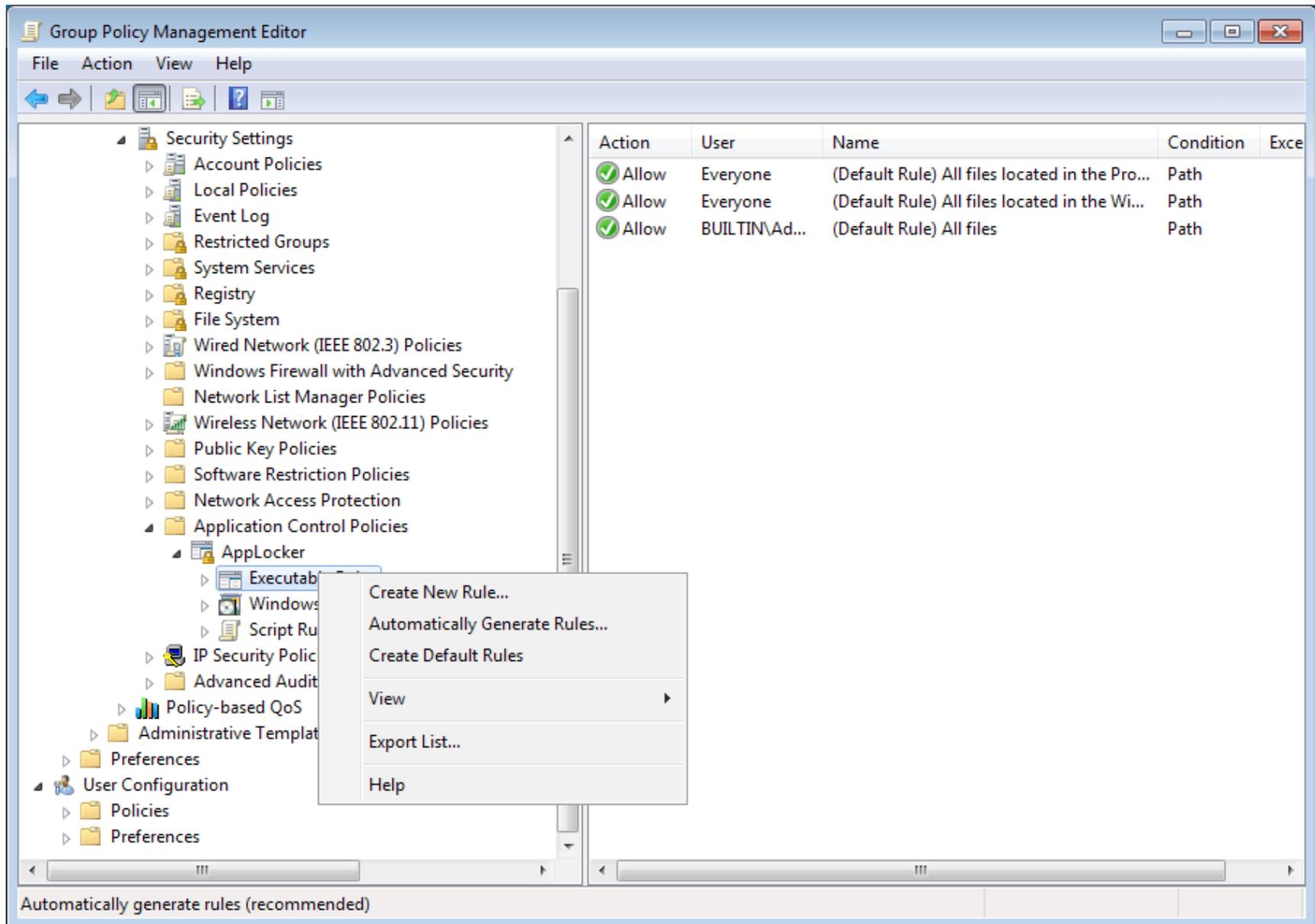
BitLocker Drive Encryption - BitLocker To Go

Drive	Status	Actions
D:	Off	Turn On BitLocker

See also

- [TPM Administration](#)
- [Disk Management](#)
- [Read our privacy statement online](#)

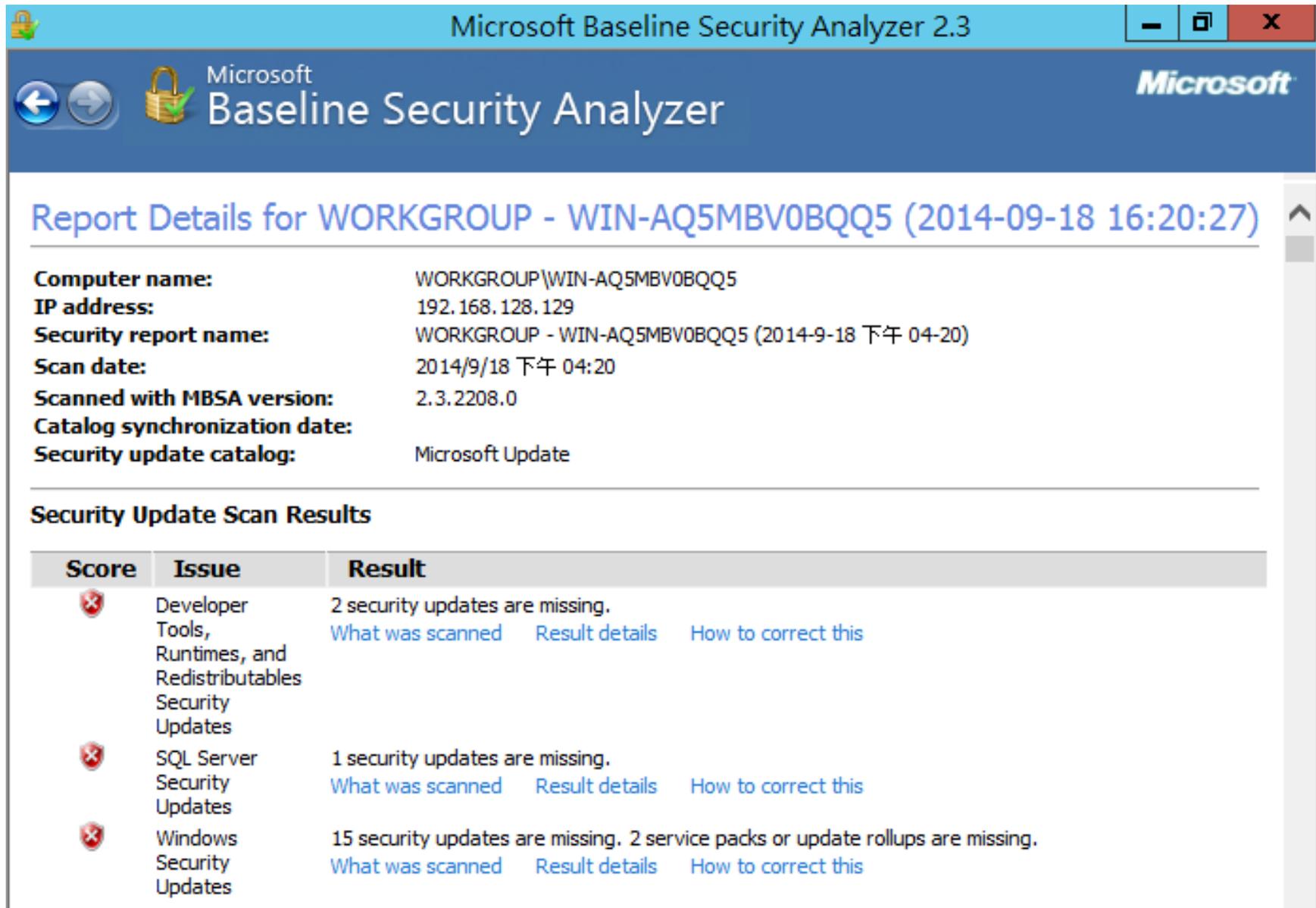
Como Convertirte en un Profesional de la Seguridad Informática



The screenshot shows the Group Policy Management Editor window. The left pane displays a tree view of policy categories, with 'AppLocker' expanded under 'Application Control Policies'. The right pane shows a table of existing rules. A context menu is open over the 'AppLocker' folder, listing options such as 'Create New Rule...', 'Automatically Generate Rules...', and 'Create Default Rules'.

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)



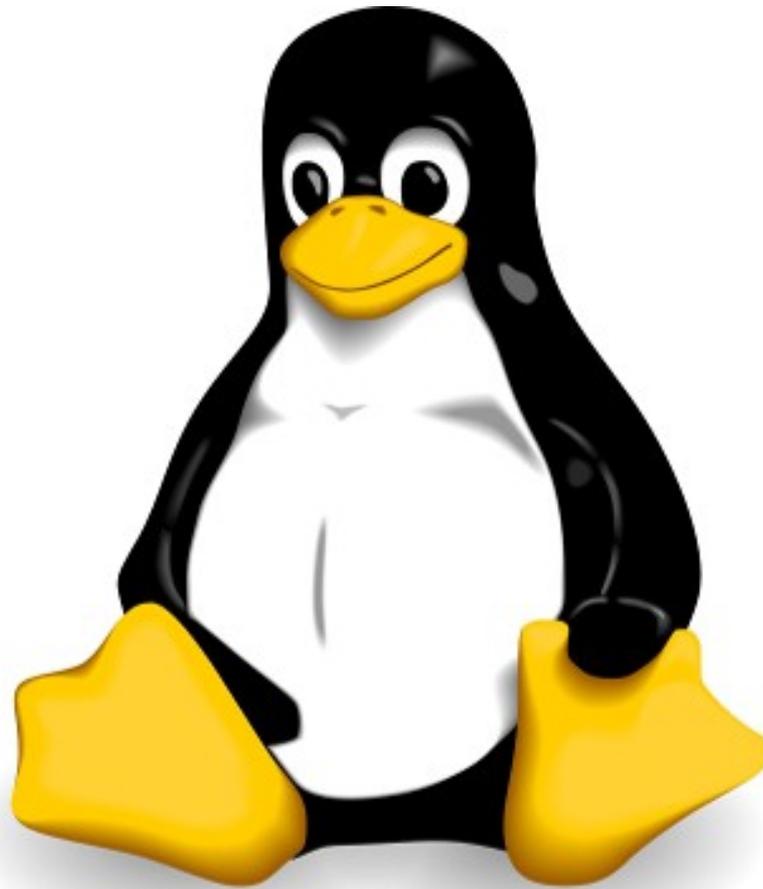
The screenshot displays the Microsoft Baseline Security Analyzer 2.3 interface. The title bar shows the application name and standard window controls. The main header includes the Microsoft logo and the application name. Below the header, the report title is "Report Details for WORKGROUP - WIN-AQ5MBV0BQQ5 (2014-09-18 16:20:27)". The report details section lists the following information:

- 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:** (blank)
- Security update catalog:** Microsoft Update

The "Security Update Scan Results" section is presented in a table with three columns: Score, Issue, and Result.

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 reenvíos no validados

OWASP Top 10 2013

***“10 Vulnerabilidades No Requieren
10 Medidas de Seguridad”***

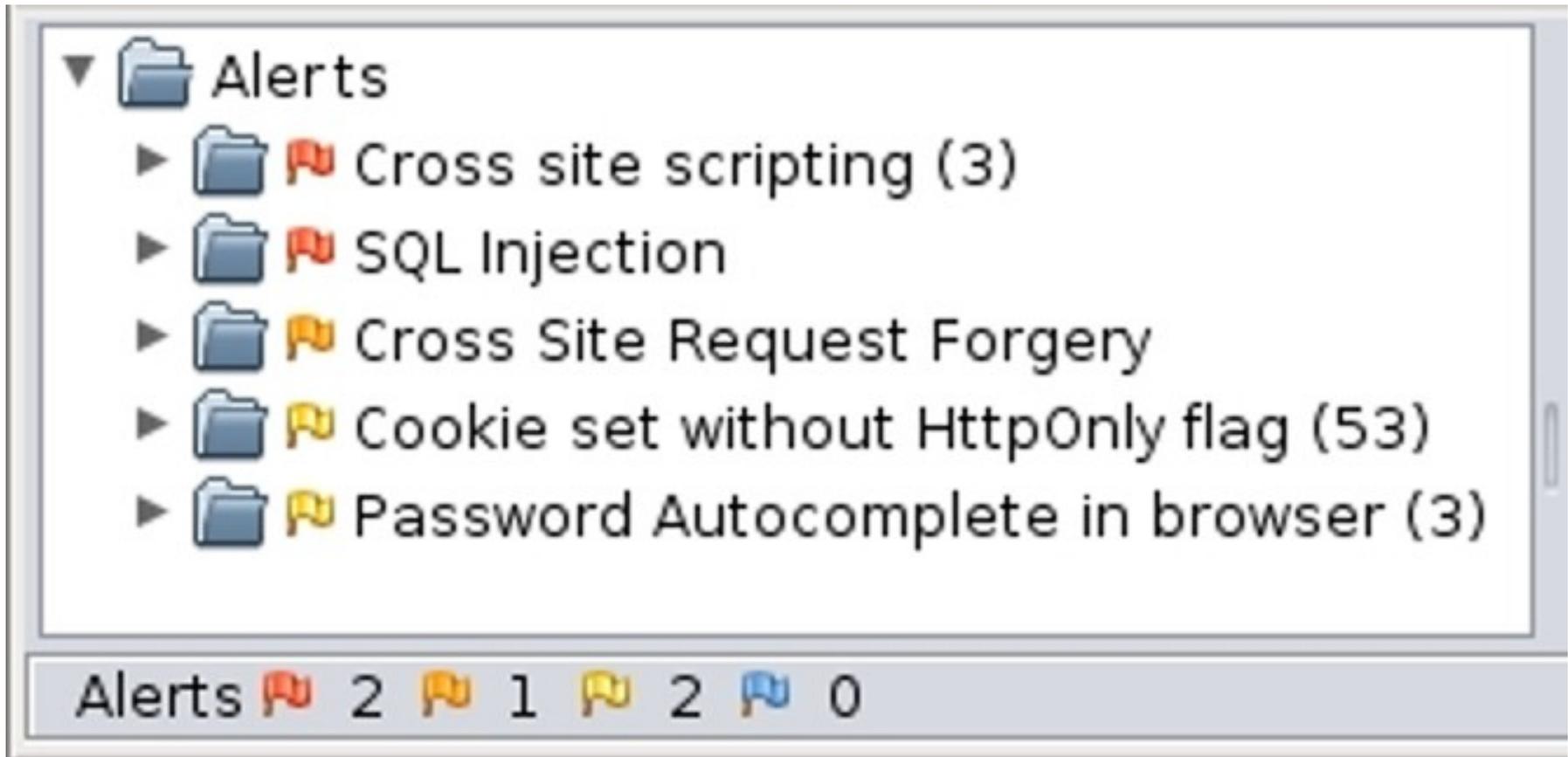
***(Validar Datos y Acciones Mitigan 7 de
las 10 Vulnerabilidades)***

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)



Seguridad Web

SQL Injection

Video:

SQL Injection con Payloads Comunes

Ethical Hacking



Ethical Hacking

***¿Qué tan difícil es penetrar
en un sistema?***

***Video:
Adobe Embedded Exe***

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

Todas las marcas y logos utilizados en la presentación son propiedad de sus respectivos propietarios