

Seguridad de Sistemas

Clase 5: Análisis de vulnerabilidades

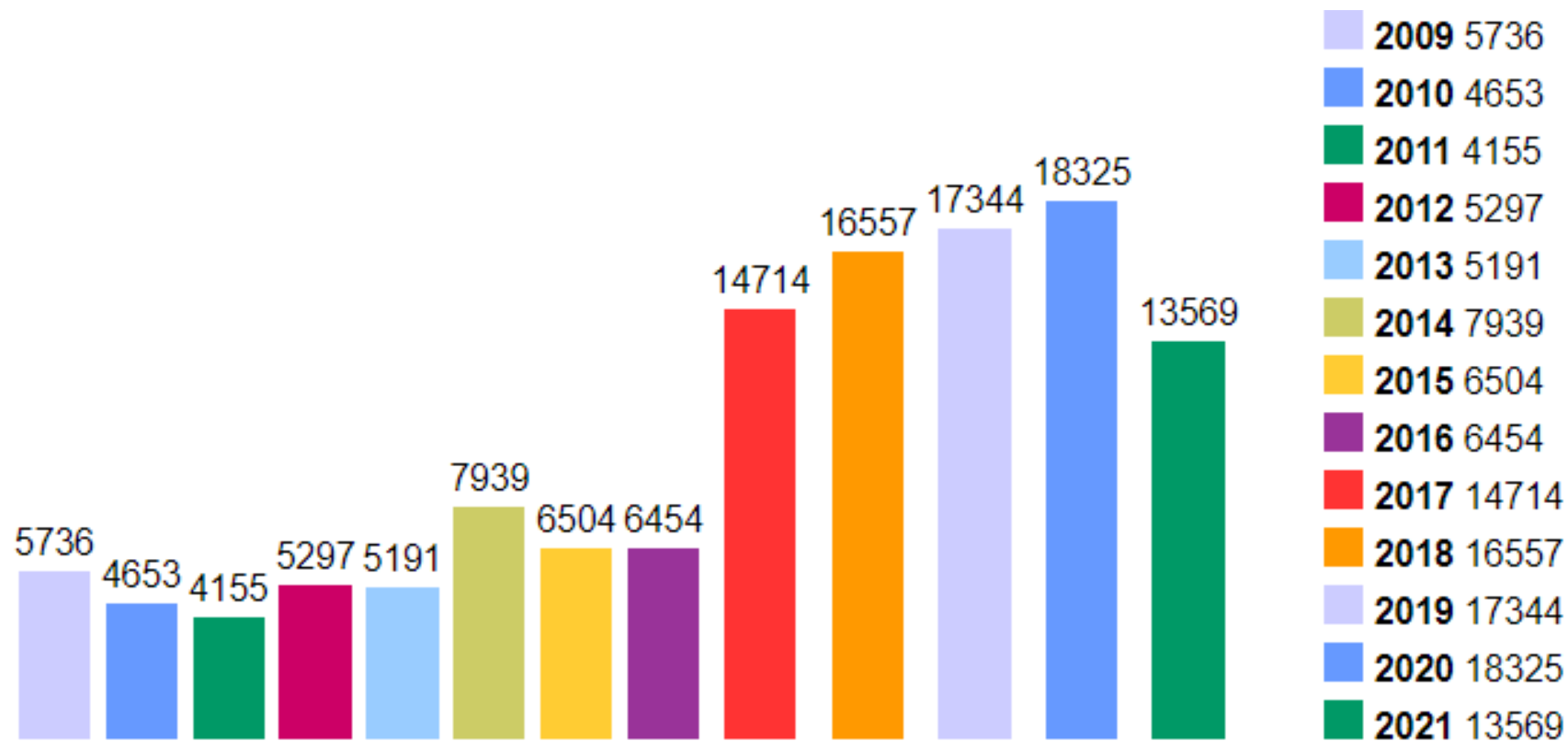
Contenidos

- Conocer la metodología de análisis de vulnerabilidades
- Conocer el ciclo de gestión de vulnerabilidades
- Conocer las principales herramientas utilizadas en el proceso de análisis de vulnerabilidades
- Conocer el formato de reporte y proceso de mitigación

Introducción

- Es un proceso mediante el cual la organización determina el nivel de exposición y la predisposición a la pérdida de un elemento o grupo de elementos ante una amenaza específica. Se valora (0) la más baja a (10) en el nivel más alto o pérdida total.
- El principal objetivo de este proceso es determinar el nivel de exposición que tienen los principales activos de la compañía, clasificar su nivel de riesgo y realizar el plan de mitigación o corrección de las vulnerabilidades encontradas.

Vulnerabilidades por año

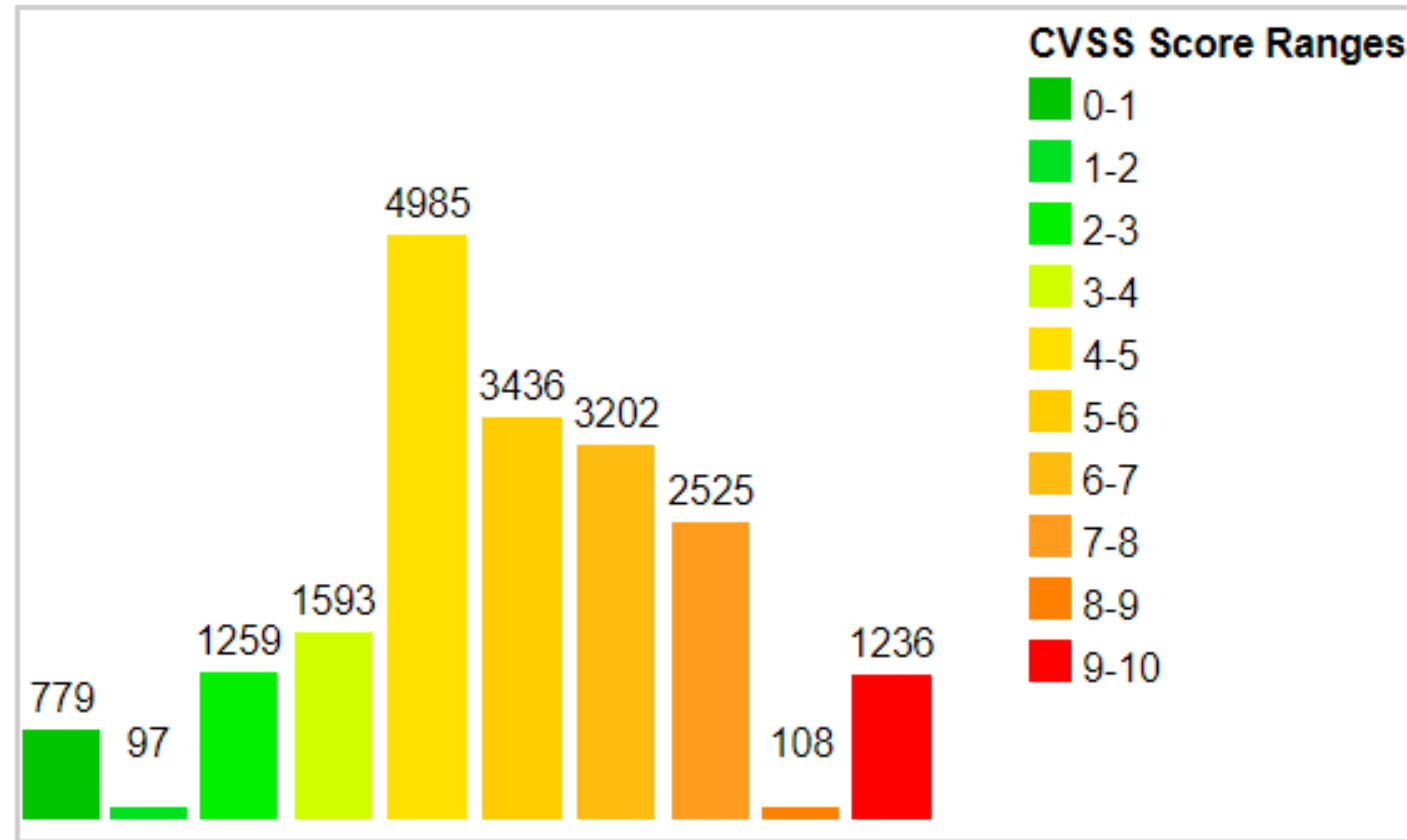


Análisis de vulnerabilidades

- Vulnerabilidades: como toda aplicación de software, el S. O. esta sujeto a tener vulnerabilidades y dado que está expuesto a la red en la mayoría de los casos, esto hace que mayor su grado de exposición.
- Una vulnerabilidad corresponde a una falla o debilidad del Sistema Operativo que permite a algún atacante afectar a algún atributo de la información
- Las vulnerabilidades de un Sistema Operativo están publicadas por su fabricante con su respectiva solución, sin embargo existen sitios en los cuales también se publican éstas.

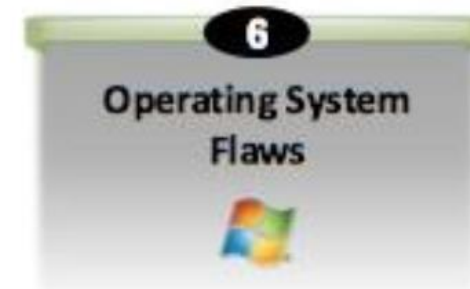
Distribución de vulnerabilidades

Vulnerability Distribution By CVSS Scores



Fuente: CVE 2021

Causas de vulnerabilidades



Ranking de vulnerabilidades

	Vendor Name	Number of Products	Number of Vulnerabilities	#Vulnerabilities/#Products
1	Microsoft	626	7970	13
2	Oracle	860	7759	9
3	Google	119	6405	54
4	Debian	106	5244	49
5	IBM	1297	5228	4
6	Apple	136	5040	37
7	Cisco	5039	4063	1
8	Redhat	397	3945	10
9	Canonical	48	3025	63
10	Linux	23	2732	119

Proceso de análisis de vulnerabilidades

- Análisis de vulnerabilidades (Vulnerability Assessment): es el proceso en el cual se identifican y clasifican las vulnerabilidades de un sistema informático.
- Para esto existen dos formas:
 - Reconocimiento: a través de la información que se tiene del sistema (Ej: versión del SO) se pueden buscar las vulnerabilidades asociadas
 - Scanning: a través de herramientas especializadas, que cuentan con bases de datos de vulnerabilidades, se realiza una revisión al sistema destino y se obtiene un reporte con el detalle correspondiente.

Análisis de vulnerabilidades

- Scanning de vulnerabilidades:
 - La herramienta mas utilizada para esta función es Nessus de Tenable, esta disponible para Windows y Linux y tiene una licencia pagada y una licencia gratuita (Home)
 - <https://www.tenable.com/products/nessus-home>
- Operación de Nessus:
 - Nessus realiza un mapeo de todos los puertos que están abiertos en el servidor destino
 - A continuación envía los plugin o firmas de trafico que tiene configurados a los puertos disponibles
 - Luego recibe la respuesta del servidor para validar si la vulnerabilidad existe
 - Luego compara el resultado con su base de dato interna para validar la clasificación de las vulnerabilidades encontradas



USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Ciclo de gestión de vulnerabilidades





USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Baseline

- Uno de los principales referentes para obtener información sobre hardening de Sistemas o Servidores es CIS Security
- <https://www.cisecurity.org/cis-benchmarks/>
- En esta sitio existen guías con recomendaciones para realizar configuraciones seguras de los mas diversos Sistemas Operativos y aplicaciones utilizadas en los sistemas informáticos.
- Además estas guías se actualizan permanentemente.





USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Ciclo de gestión de vulnerabilidades

- Descubrimiento: en esta etapa se detallan todos los activos que formaran parte del análisis y se realiza el scanning
- Priorización: en esta etapa se define cuales son los activos mas críticos para el negocio
- Evaluación: se realiza en función de la criticidad de los activos y el nivel de riesgo de las vulnerabilidades
- Reporte: corresponde a la medición del nivel de riesgo encontrado en su conjunto en función de alguna base predeterminada (política)
- Remediación: en esta etapa se aplican los controles en función del análisis anterior (orden de prioridad)
- Verificación: se realiza una nueva medición para validar que las vulnerabilidades fueron mitigadas.



USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Tipos de análisis de vulnerabilidades

- **Basado en productos:**
 - Las empresas compran soluciones de análisis de vulnerabilidades y las operan localmente con la frecuencia requerida y luego realizan las labores de mitigación. Tiene el costo de las herramientas y las HH involucradas.
- **Basado en servicios:**
 - Las empresas contratan un servicio en el cual un proveedor, en forma periódica realiza análisis de vulnerabilidades sobre un parque de servidores definido. Solo tiene el costo del servicio.



USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Clasificación de vulnerabilidades

- Proceso en el cual se les asigna una puntuación a cada vulnerabilidad (ranking), existen diferentes criterios para realizar esta clasificación.
- Clasificación CVE (CVSS): utiliza varios parámetros para realizar la calificación de puntaje, entre ellos:
 - Como afecta la vulnerabilidad a los atributos de la información (CIA)
 - La facilidad de explotación o complejidad de acceso
 - Si se requiere o no autenticación para explotar la vulnerabilidad
 - Los daños específicos que podría causar una vez explotada, tales como DoS, control remoto, ejecución de comandos, etc.
 - Si permite o no tomar control del objetivo



UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level
1	CVE-2016-1715	189		DoS +Priv Mem. Corr.	2016-01-12	2016-01-21	5.5	None
<p>The swin.sys kernel driver in McAfee Application Control (MAC) 6.1.0 before build 706, 6.1.1 before build 404, 6.1.2 before build 449, 6.1.3 before build 450, 6.1.4 before build 451, 6.1.5 before build 452, 6.1.6 before build 453, 6.1.7 before build 454, 6.1.8 before build 455, 6.1.9 before build 456, 6.1.10 before build 457, 6.1.11 before build 458, 6.1.12 before build 459, 6.1.13 before build 460, 6.1.14 before build 461, 6.1.15 before build 462, 6.1.16 before build 463, 6.1.17 before build 464, 6.1.18 before build 465, 6.1.19 before build 466, 6.1.20 before build 467, 6.1.21 before build 468, 6.1.22 before build 469, 6.1.23 before build 470, 6.1.24 before build 471, 6.1.25 before build 472, 6.1.26 before build 473, 6.1.27 before build 474, 6.1.28 before build 475, 6.1.29 before build 476, 6.1.30 before build 477, 6.1.31 before build 478, 6.1.32 before build 479, 6.1.33 before build 480, 6.1.34 before build 481, 6.1.35 before build 482, 6.1.36 before build 483, 6.1.37 before build 484, 6.1.38 before build 485, 6.1.39 before build 486, 6.1.40 before build 487, 6.1.41 before build 488, 6.1.42 before build 489, 6.1.43 before build 490, 6.1.44 before build 491, 6.1.45 before build 492, 6.1.46 before build 493, 6.1.47 before build 494, 6.1.48 before build 495, 6.1.49 before build 496, 6.1.50 before build 497, 6.1.51 before build 498, 6.1.52 before build 499, 6.1.53 before build 500, 6.1.54 before build 501, 6.1.55 before build 502, 6.1.56 before build 503, 6.1.57 before build 504, 6.1.58 before build 505, 6.1.59 before build 506, 6.1.60 before build 507, 6.1.61 before build 508, 6.1.62 before build 509, 6.1.63 before build 510, 6.1.64 before build 511, 6.1.65 before build 512, 6.1.66 before build 513, 6.1.67 before build 514, 6.1.68 before build 515, 6.1.69 before build 516, 6.1.70 before build 517, 6.1.71 before build 518, 6.1.72 before build 519, 6.1.73 before build 520, 6.1.74 before build 521, 6.1.75 before build 522, 6.1.76 before build 523, 6.1.77 before build 524, 6.1.78 before build 525, 6.1.79 before build 526, 6.1.80 before build 527, 6.1.81 before build 528, 6.1.82 before build 529, 6.1.83 before build 530, 6.1.84 before build 531, 6.1.85 before build 532, 6.1.86 before build 533, 6.1.87 before build 534, 6.1.88 before build 535, 6.1.89 before build 536, 6.1.90 before build 537, 6.1.91 before build 538, 6.1.92 before build 539, 6.1.93 before build 540, 6.1.94 before build 541, 6.1.95 before build 542, 6.1.96 before build 543, 6.1.97 before build 544, 6.1.98 before build 545, 6.1.99 before build 546, 6.1.100 before build 547, 6.1.101 before build 548, 6.1.102 before build 549, 6.1.103 before build 550, 6.1.104 before build 551, 6.1.105 before build 552, 6.1.106 before build 553, 6.1.107 before build 554, 6.1.108 before build 555, 6.1.109 before build 556, 6.1.110 before build 557, 6.1.111 before build 558, 6.1.112 before build 559, 6.1.113 before build 560, 6.1.114 before build 561, 6.1.115 before build 562, 6.1.116 before build 563, 6.1.117 before build 564, 6.1.118 before build 565, 6.1.119 before build 566, 6.1.120 before build 567, 6.1.121 before build 568, 6.1.122 before build 569, 6.1.123 before build 570, 6.1.124 before build 571, 6.1.125 before build 572, 6.1.126 before build 573, 6.1.127 before build 574, 6.1.128 before build 575, 6.1.129 before build 576, 6.1.130 before build 577, 6.1.131 before build 578, 6.1.132 before build 579, 6.1.133 before build 580, 6.1.134 before build 581, 6.1.135 before build 582, 6.1.136 before build 583, 6.1.137 before build 584, 6.1.138 before build 585, 6.1.139 before build 586, 6.1.140 before build 587, 6.1.141 before build 588, 6.1.142 before build 589, 6.1.143 before build 590, 6.1.144 before build 591, 6.1.145 before build 592, 6.1.146 before build 593, 6.1.147 before build 594, 6.1.148 before build 595, 6.1.149 before build 596, 6.1.150 before build 597, 6.1.151 before build 598, 6.1.152 before build 599, 6.1.153 before build 600, 6.1.154 before build 601, 6.1.155 before build 602, 6.1.156 before build 603, 6.1.157 before build 604, 6.1.158 before build 605, 6.1.159 before build 606, 6.1.160 before build 607, 6.1.161 before build 608, 6.1.162 before build 609, 6.1.163 before build 610, 6.1.164 before build 611, 6.1.165 before build 612, 6.1.166 before build 613, 6.1.167 before build 614, 6.1.168 before build 615, 6.1.169 before build 616, 6.1.170 before build 617, 6.1.171 before build 618, 6.1.172 before build 619, 6.1.173 before build 620, 6.1.174 before build 621, 6.1.175 before build 622, 6.1.176 before build 623, 6.1.177 before build 624, 6.1.178 before build 625, 6.1.179 before build 626, 6.1.180 before build 627, 6.1.181 before build 628, 6.1.182 before build 629, 6.1.183 before build 630, 6.1.184 before build 631, 6.1.185 before build 632, 6.1.186 before build 633, 6.1.187 before build 634, 6.1.188 before build 635, 6.1.189 before build 636, 6.1.190 before build 637, 6.1.191 before build 638, 6.1.192 before build 639, 6.1.193 before build 640, 6.1.194 before build 641, 6.1.195 before build 642, 6.1.196 before build 643, 6.1.197 before build 644, 6.1.198 before build 645, 6.1.199 before build 646, 6.1.200 before build 647, 6.1.201 before build 648, 6.1.202 before build 649, 6.1.203 before build 650, 6.1.204 before build 651, 6.1.205 before build 652, 6.1.206 before build 653, 6.1.207 before build 654, 6.1.208 before build 655, 6.1.209 before build 656, 6.1.210 before build 657, 6.1.211 before build 658, 6.1.212 before build 659, 6.1.213 before build 660, 6.1.214 before build 661, 6.1.215 before build 662, 6.1.216 before build 663, 6.1.217 before build 664, 6.1.218 before build 665, 6.1.219 before build 666, 6.1.220 before build 667, 6.1.221 before build 668, 6.1.222 before build 669, 6.1.223 before build 670, 6.1.224 before build 671, 6.1.225 before build 672, 6.1.226 before build 673, 6.1.227 before build 674, 6.1.228 before build 675, 6.1.229 before build 676, 6.1.230 before build 677, 6.1.231 before build 678, 6.1.232 before build 679, 6.1.233 before build 680, 6.1.234 before build 681, 6.1.235 before build 682, 6.1.236 before build 683, 6.1.237 before build 684, 6.1.238 before build 685, 6.1.239 before build 686, 6.1.240 before build 687, 6.1.241 before build 688, 6.1.242 before build 689, 6.1.243 before build 690, 6.1.244 before build 691, 6.1.245 before build 692, 6.1.246 before build 693, 6.1.247 before build 694, 6.1.248 before build 695, 6.1.249 before build 696, 6.1.250 before build 697, 6.1.251 before build 698, 6.1.252 before build 699, 6.1.253 before build 700, 6.1.254 before build 701, 6.1.255 before build 702, 6.1.256 before build 703, 6.1.257 before build 704, 6.1.258 before build 705, 6.1.259 before build 706, 6.1.260 before build 707, 6.1.261 before build 708, 6.1.262 before build 709, 6.1.263 before build 710, 6.1.264 before build 711, 6.1.265 before build 712</p>								



USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Ejemplo de clasificación CVSS

– CVSS Scores & Vulnerability Types

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the res
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfi
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service Execute Code Memory corruption
CWE ID	399

– CVSS Scores & Vulnerability Types

CVSS Score	6.8
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the atta
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions n
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	94



USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Clasificación según Nessus

- En este caso se utiliza un código de colores para la clasificación de las vulnerabilidades en 5 niveles
- Ejemplo de clasificación de vulnerabilidades según Nessus de Tenable:

critical	MS08-067: Microsoft Windows Server Service Crafted RPC	Windows	1
critical	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code	Windows	1
high	MS02-045: Microsoft Windows SMB Protocol	Windows	1
high	MS06-035: Vulnerability in Server Service Could Allow Remote...	Windows	1
medium	Microsoft Windows SMB NULL Session Authentication	Windows	1
medium	MS05-007: Vulnerability in Windows Could Allow Information D...	Windows	1
medium	SMB Signing Disabled	Misc.	1
low	Multiple Ethernet Driver Frame Padding Information Disclosur...	Misc.	1



USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Clasificación de vulnerabilidades

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

TABLE 5.1: CVSS v3.0 ratings



USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Clasificación de vulnerabilidades

- Clasificación de vulnerabilidades según Microsoft: existe un sitio donde se publican las vulnerabilidades reportadas:
- <https://portal.msrc.microsoft.com/en-us/security-guidance/summary>
- Este sitio clasifica las vulnerabilidades en tres niveles,
 - Crítica
 - Importante
 - Moderada
- principalmente en función del daño que podría causar si es explotada.



USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Clasificación de vulnerabilidades

Fecha ▼	Número de boletín	Número de KB	Título	Clasificación del boletín
08/03/2016	MS16-036	3144756	Security Update for Adobe Flash Player	Crítica
08/03/2016	MS16-035	3141780	Security Update for .NET Framework to Address Security Feature Bypass	Importante
08/03/2016	MS16-034	3143145	Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege	Importante
08/03/2016	MS16-033	3143142	Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege	Importante
08/03/2016	MS16-032	3143141	Security Update for Secondary Logon to Address Elevation of Privilege	Importante
08/03/2016	MS16-031	3140410	Security Update for Microsoft Windows to Address Elevation of Privilege	Importante
08/03/2016	MS16-030	3143136	Security Update for Windows OLE to Address Remote Code Execution	Importante
08/03/2016	MS16-029	3141806	Security Update for Microsoft Office to Address Remote Code Execution	Importante
08/03/2016	MS16-028	3143081	Security Update for Microsoft Windows PDF Library to Address Remote Code Execution	Crítica
08/03/2016	MS16-027	3143146	Security Update for Windows Media to Address Remote Code Execution	Crítica



USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Calculadora de NVD

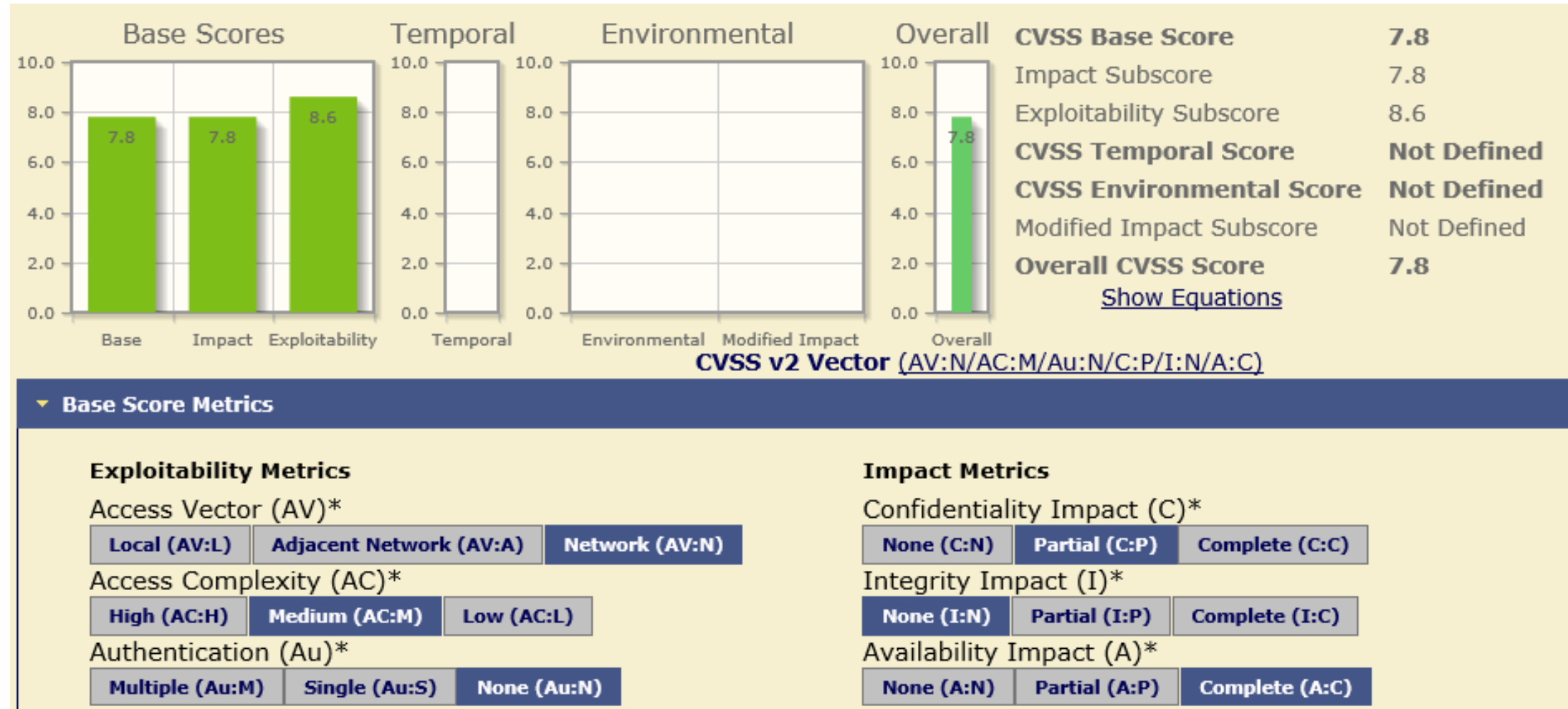
- NIST propone una metodología para clasificar las vulnerabilidades según varios parámetros, en el sitio:
- <https://nvd.nist.gov/cvss.cfm?calculator&version=2>
- Los principales factores a considerar son:
- Facilidad de explotación
 - Acceso
 - Complejidad
 - Autenticación
- Impacto
 - Confidencialidad
 - Integridad
 - Disponibilidad



USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Calculadora de NVD



Herramientas de análisis de vulnerabilidades

- **Características de una buena herramienta de vulnerabilidades**
- Debe tener una gran base de datos con plugin de vulnerabilidades conocidas
- Soportar múltiples plataformas y sistemas operativos
- Tener una alta precisión en la búsqueda de vulnerabilidades
- Actualización automática
- Generación de reportes amigables
- Programación de análisis

Sitios de búsqueda de vulnerabilidades

- CVE
- <https://cve.mitre.org/data/downloads/index.html>
- Security Focus
- <https://www.securityfocus.com/>
- Vulnerability Lab
- <https://www.vulnerability-lab.com/>

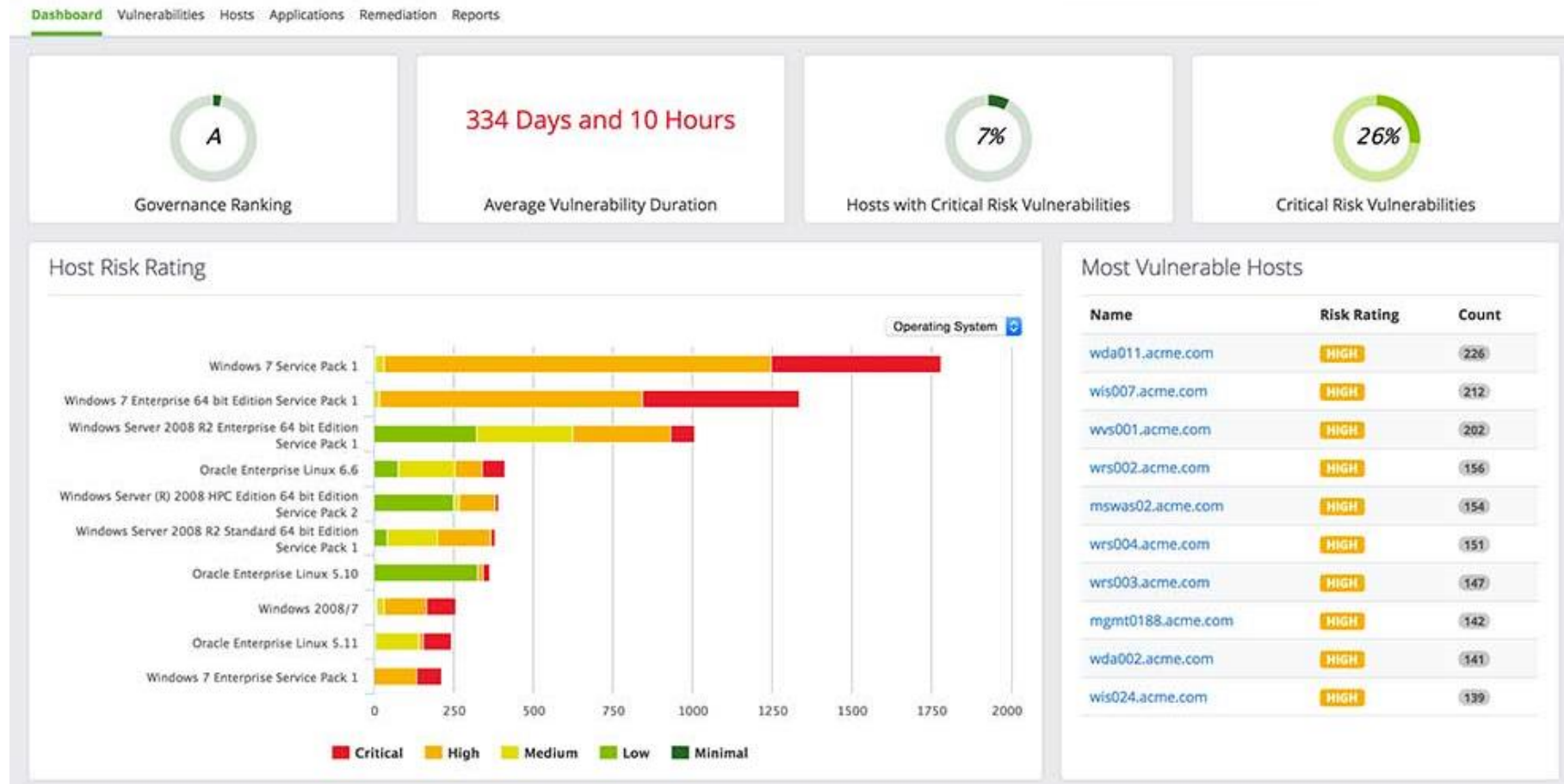


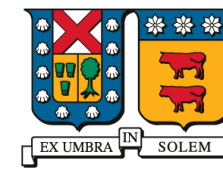
USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Herramientas

- Qualys vulnerability management



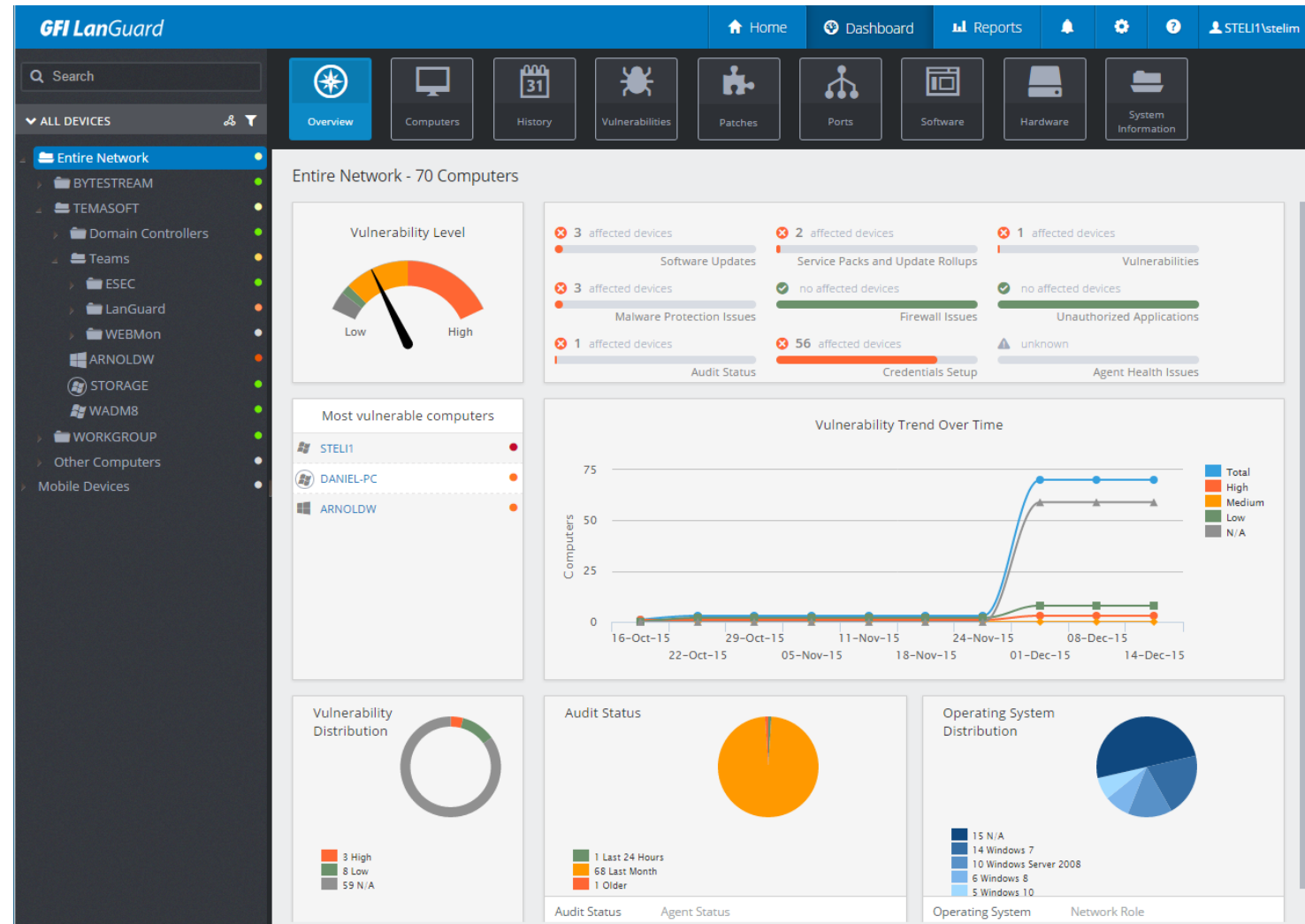


USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Herramientas

- GFI LanGuard





USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Herramientas

- Nikto

```
# nikto -h 10.0.2.81
- Nikto v2.1.6

+ Target IP: 10.0.2.81
+ Target Hostname: 10.0.2.81
+ Target Port: 80
+ Start Time: 2021-09-23 14:55:02 (GMT-4)

+ Server: Apache/2.4.7 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a dif
+ OSVDB-3268: /: Directory indexing found.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /.: Directory indexing found.
+ /.: Appending '/./' to a directory allows indexing
+ OSVDB-3268: //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ OSVDB-3268: /%2e/: Directory indexing found.
+ OSVDB-576: /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. http://www.securityfo
```

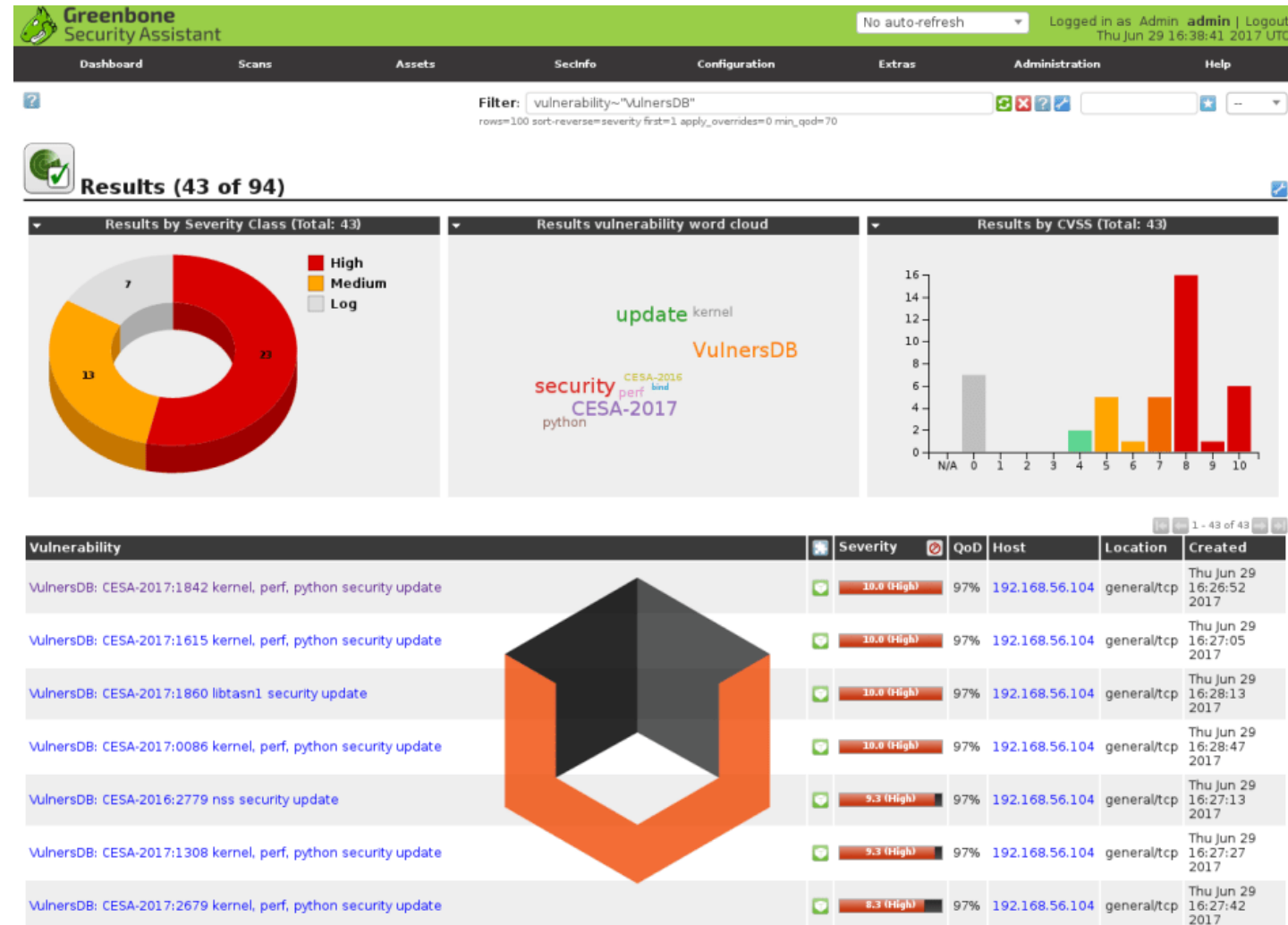


USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Herramientas

- OpenVAS



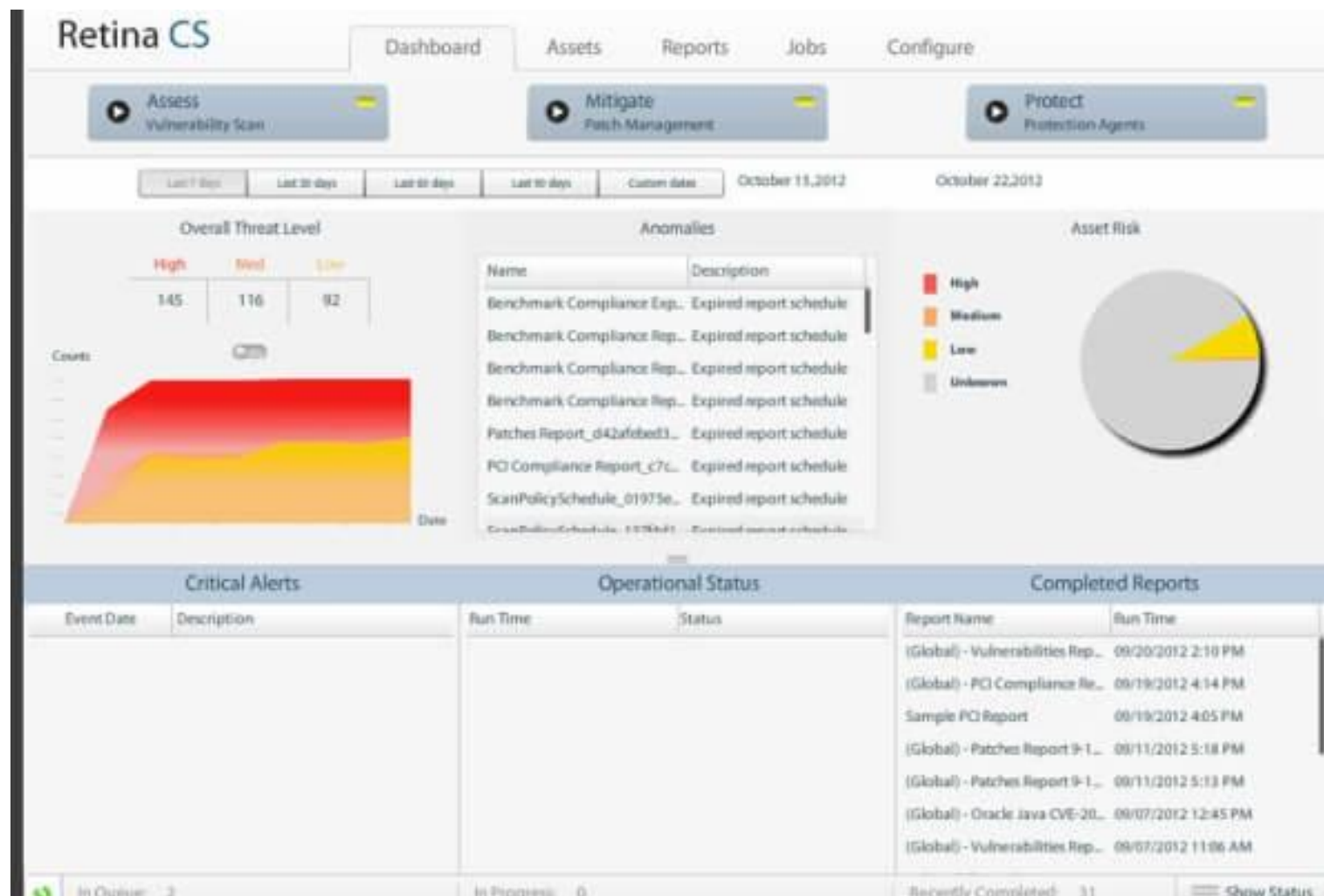


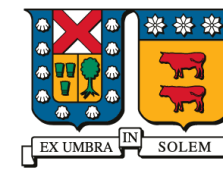
USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Herramientas

- Retina CS



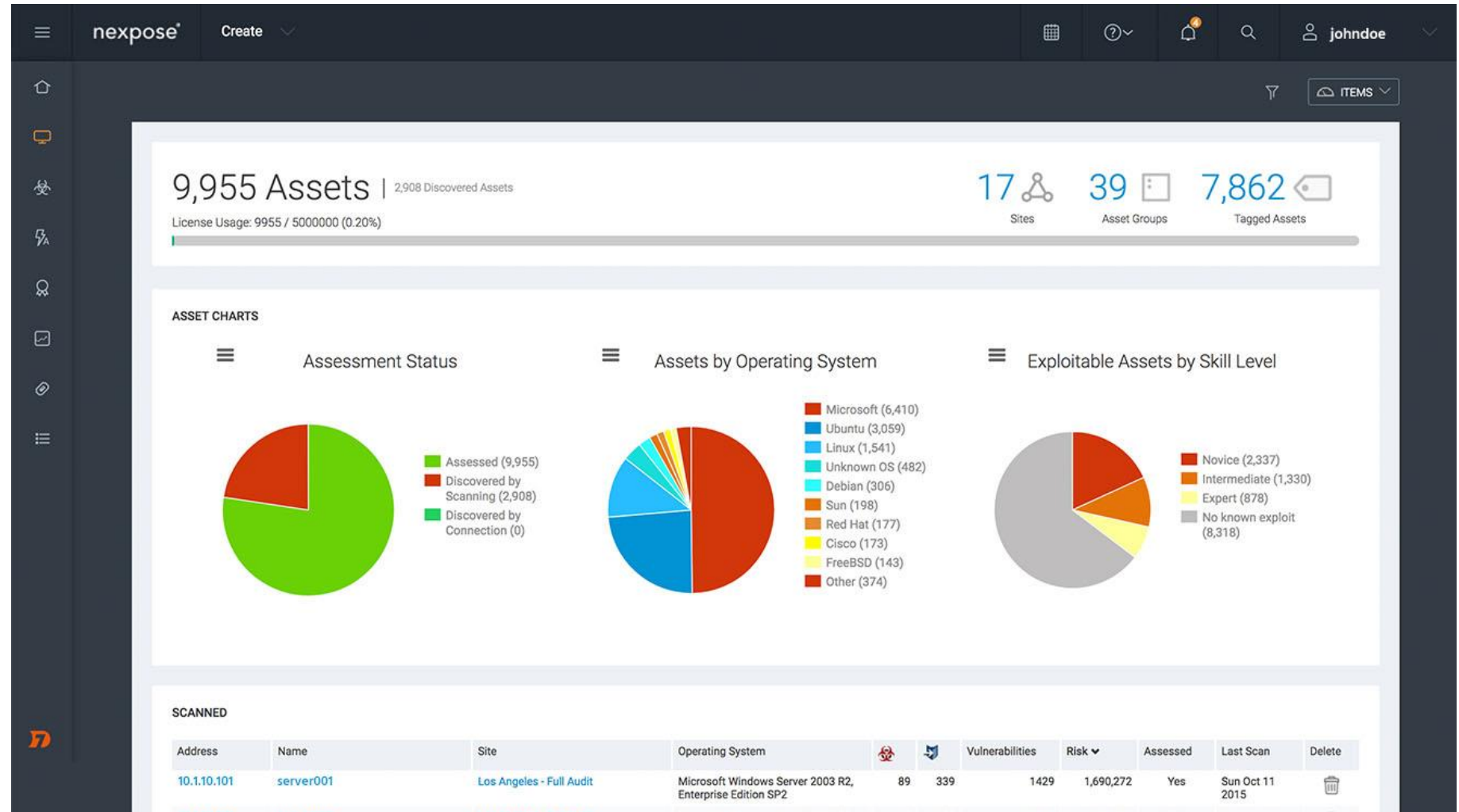


USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Herramientas

- Nexpose





USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Herramientas

- MBSA

Microsoft Baseline Security Analyzer 2.1

Microsoft
Baseline Security Analyzer

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Local Account Password Test	Some user accounts (2 of 6) have blank or simple passwords, or could not be analyzed. What was scanned Result details How to correct this
	Administrators	More than 2 Administrators were found on this computer. What was scanned Result details How to correct this
	Password Expiration	Some user accounts (3 of 6) have non-expiring passwords. What was scanned Result details How to correct this
	Automatic Updates	Automatic Updates are managed through Group Policy on this computer. What was scanned
	Incomplete Updates	No incomplete software update installations were found. What was scanned
	Windows Firewall	Windows Firewall is disabled and has exceptions configured. What was scanned Result details How to correct this
	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
	Autologon	Autologon is not configured on this computer. What was scanned
	Guest Account	The Guest account is disabled on this computer. What was scanned
	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned

Additional System Information

Score	Issue	Result
	Auditing	Logon Success and Logon Failure auditing are both enabled. What was scanned
	Services	Some potentially unnecessary services are installed. What was scanned Result details How to correct this
	Shares	2 share(s) are present on your computer. What was scanned Result details How to correct this
	Windows Version	Computer is running Microsoft Windows XP. What was scanned



USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Herramientas

- AVDS





USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Detección con script

- NMAP

```
root@kali:~# nmap --script-args=unsafe=1 --script smb-check-vulns.nse -p445 192.168.1.121

Starting Nmap 6.46 ( http://nmap.org ) at 2014-11-21 16:42 MST
Nmap scan report for 192.168.1.121
Host is up (0.0027s latency).
PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:18:6B:DB (VMware)

Host script results:
| smb-check-vulns:
|   MS08-067: VULNERABLE
|   Conficker: Likely CLEAN
|   SMBv2 DoS (CVE-2009-3103): NOT VULNERABLE
|   MS06-025: NOT VULNERABLE
|_  MS07-029: NO SERVICE (the Dns Server RPC service is inactive)

Nmap done: 1 IP address (1 host up) scanned in 18.74 seconds
```



USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Mitigación

- Ejemplo de un reporte de mitigación de Nessus

Description
<p>The remote version of Windows contains a flaw in the Server Message Block (SMB) implementation that could allow an attacker to execute arbitrary code on the remote host.</p> <p>An attacker does not need to be authenticated to exploit this flaw.</p>
Solution
<p>Microsoft has released a set of patches for Windows 2000, XP and 2003 :</p> <p>http://technet.microsoft.com/en-us/security/bulletin/ms05-027</p>
Plugin Information
<p>Plugin ID: 18483</p> <p>Plugin Version: \$Revision: 1.32 \$</p> <p>Plugin Type: local</p> <p>Plugin Publication Date: 2005/06/14</p> <p>Plugin Last Modification Date: 2013/02/01</p>



USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Mitigación

- Ejemplo de reporte de mitigación

Software description

- openssl - Secure Socket Layer (SSL) cryptographic library and tools

Details

Anton Johansson discovered that OpenSSL incorrectly handled certain invalid TLS handshakes. A remote attacker could use this issue to cause OpenSSL to crash, resulting in a denial of service. ([CVE-2013-4353](#))

Ron Barber discovered that OpenSSL used an incorrect data structure to obtain a version number. A remote attacker could use this issue to cause OpenSSL to crash, resulting in a denial of service. ([CVE-2013-6449](#))

Dmitry Sobinov discovered that OpenSSL incorrectly handled certain DTLS retransmissions. A remote attacker could use this issue to cause OpenSSL to crash, resulting in a denial of service. ([CVE-2013-6450](#))

This update also disables the default use of the RdRand feature of certain Intel CPUs as the sole source of entropy.

Update instructions

The problem can be corrected by updating your system to the following package version:

Ubuntu 13.10:

[libssl1.0.0](#) [1.0.1e-3ubuntu1.1](#)

Ubuntu 13.04:

[libssl1.0.0](#) [1.0.1c-4ubuntu8.2](#)



USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Reporte de vulnerabilidades

- Resumen Ejecutivo
- Sistemas vulnerables
- Descripción de la vulnerabilidad
- Clasificación de Riesgo
- Mitigación
- Sistemas afectados
- Referencias
- Recomendaciones





USM









UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Reporte de vulnerabilidades

Filter by:

All (57) Level 5 (1) Level 4 (4) Level 3 (30) Level 2 (20) Level 1 (2) Info (44)

Search for Title, Category, CVE ID or QID

All Scan Results		1 - 25 of 101
	Shellshock Apache Injection	<div><div></div><div></div><div></div><div></div><div></div></div>
	OpenSSL Multiple Remote Security Vulnerabilities	<div><div></div><div></div><div></div><div></div><div></div></div>
	PhpMyAdmin Multiple Vulnerabilities (PMASA-2011-9, PMA...	<div><div></div><div></div><div></div><div></div><div></div></div>
	PhpMyAdmin Multiple Vulnerabilities (PMASA-2011-9, PMA...	<div><div></div><div></div><div></div><div></div><div></div></div>
	PhpMyAdmin Multiple Vulnerabilities (PMASA-2011-9, PMA...	<div><div></div><div></div><div></div><div></div><div></div></div>
	Web Server Vulnerable to Cross Site Scripting	<div><div></div><div></div><div></div><div></div><div></div></div>
	HTTP TRACE / TRACK Methods Enabled	<div><div></div><div></div><div></div><div></div><div></div></div>
	"test-cgi" CGI Vulnerability	<div><div></div><div></div><div></div><div></div><div></div></div>

Shellshock Apache Injection

QID: 150134

CVE Base: 10

Port: -

CVSS Temporal: 8.5

Category: Web
Application

CVE ID: [CVE-2014-6271](#), [CVE-2014-7169](#)

Threat:

ShellShock vulnerability allows an attacker to execute arbitrary commands by leveraging the fact that environment variables can be created with specially crafted values before calling Bash shell. For e.g. Injecting () {test;} ; echo; /bin/cat /etc/passwd in HTTP header injection reveals /etc/passwd file contents in the response.

Impact:

Environmental variables with an arbitrary name can contain any nefarious function which can potentially lead to network exploitation. The vulnerability is critical since any application hosted on web server using mod_cgi/mod_cgid module of Apache HTTP Server or code that calls the bash shell is vulnerable.



USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Resumen

- Análisis de vulnerabilidades
- Ciclo de gestión de vulnerabilidades
- Clasificación de vulnerabilidades
 - CVSS
- Herramientas de análisis de vulnerabilidades
- Mitigación de vulnerabilidades
- Reporte





USM

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA