Security tools

Vulnerability scanner – an update

Luca Carbone – INFN MiB

sectools.org: top ten security tools

by popularity

- **Wireshark (1 up)** *sniffer*
- **Metasploit (3 up)** *exploit development/testing platform*
- **Nessus (2 down)** *vulnerability scanner*
- **Aircrack (17 up)** *suite of tools for 802.11a/b/g WEP and WPA cracking*
- **Snort (2 down)** *network intrusion detection and prevention system*
- **Cain and Abel (3 up)** *Windows-only password recovery tool*
- **Backtrack/Kali (25 up)** *Security/forensics tools collection on live CD*
- **Netcat (4 down)** *TCP/UDP transmitter/receiver*
- **tcpdump (1 down)** *sniffer*
- **John the ripper (stable)** *password cracker*

sectools.org: vuln scanners

by popularity

- **Nessus**
  - Latest release: 6.3.3 3/2015
- **OpenVAS**
  - Latest release: 8.0 4/2015
- **Core Impact** *(up to 30 k$/year...)*
  - Latest release: 2015 R1.1 7/2015
- **Nexpose**
  - Latest release: 6.0 10/2015 (weekly releases: 6.0.n)
- ...

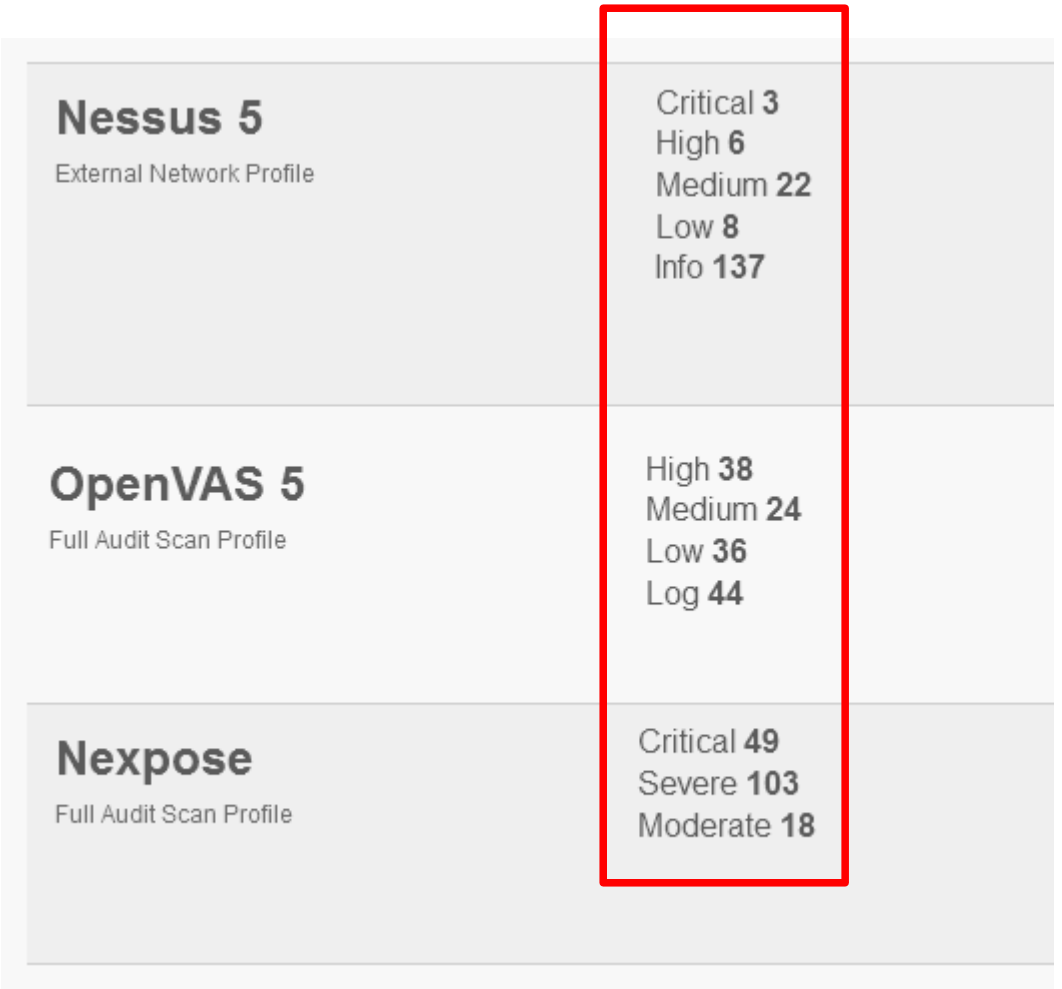
Nessus vs OpenVAS vs Nexpose

against M*etasploitable*

- Black-box test (2012: the one and only?) by *hackertarget.com* against a *Metasploitable Version 2* virtual host (*an intentionally vulnerable virtual machine designed for training, exploit testing, and general target practice*);
- Nessus *home feed* V5, OpenVAS V5 (Full scan profile, no external tools), Nexpose *community edition* V? (full audit profile)
- Default scan profiles; no credentials – external network services focused scan

Nessus vs OpenVAS vs Nexpose

great disorder under the Heavens, and the situation is excellent...



Nessus vs OpenVAS vs Nexpose *(vs Nmap/NSE)*

*analysing a specific sample of **15** security issues*

Security Issue	Nessus	OpenVAS	Nexpose	Nmap
FTP 21 Anonymous FTP Access	✓	✓	✓	✓
FTP 21 VsFTPd Smiley Face Backdoor	✓	✓		
FTP 2121 ProFTPD Vulnerabilities		✓		
SSH 22 Weak Host Keys	✓		✓	
PHP-CGI Query String Parameter Injection	✓	✓	✓	✓
CIFS Null Sessions	✓	✓	✓	✓
INGRESLOCK 1524 known backdoor drops to root shell				
NFS 2049 /* exported and writable		✓		
MYSQL 3306 weak auth (root with no password)	✓	✓	✓	✓
RMI REGISTRY 1099 Insecure Default Config				
DISTCCd 3632 distributed compiler				
POSTGRESQL 5432 weak auth (postgresql)				
VNC 5900 weak auth (password)			✓	
IRC 6667 Unreal IRCd Backdoor				✓
Tomcat 8180 weak auth (tomcat/tomcat)	✓		✓	✓

Nessus vs OpenVAS vs Nexpose

conclusions...?

- The results show *significant variation* in discovered security vulnerabilities by the different tools.
  - *tune the vulnerability scan profiles to suit your requirements (one size DOESN'T fit all);*
  - *run secondary tools* (nmap, a secondary vulnerability scanning solution and/or specialised tools);
  - perform detailed analysis of the results (beware of *false positives*).
- When running internal scans it is *probably* recommended to perform *credential supplied scanning – uncredentialed scanning* is by far less effective in discovering vulnerabilities.

*A **quantitative** evaluation of vulnerability scanning*
Holm, Sommestad, Almroth & Persson - 2011

- The purpose of this paper is to evaluate if automated vulnerability scanning accurately identifies vulnerabilities in computer networks and if this accuracy is contingent on the platforms used.
- Setup: 7 scanners against 28 Windows/Linux virtual hosts running several different network services (HTTP, HTTPS, SMTP, SSH, ...)

Property	AVDS	McAfee VM	Nessus	NeXpose	Patchlink scan	QualysGuard	SAINT
Software flaws	x	x	x	x	x	x	x
Configuration errors	x	x	x	x	x	x	x
All ports		x	x	x		x	x
Active scanning	x	x	x	x	x	x	x
Passive scanning							
Exploits				x			x
Authenticated scanning		x	x	x	x	x	x
Vulnerability signatures	6,000	22,000	41,000	53,000	500	6,000	40,000
Web application scans	x	x	x	x		x	

*A **quantitative** evaluation of vulnerability scanning*
results (1)

Overview of identified vulnerabilities

	Unauthenticated scan				Authenticated scan			
Scanner	High	Medium	Low	Potential	High	Medium	Low	Potential
AVDS	46	140	306		291	990	393	
McAfee VM	143	169	64		2,028	2,033	126	
Nessus	145	82	889		2,221	468	1,256	
NeXpose	180	391	106		1,073	969	126	
Patchlink scan	1	4	15		814	328	313	
QualysGuard	73	125	151	284	753	1,891	342	313
SAINT	81	60		223	114	65		257

*A **quantitative** evaluation of vulnerability scanning*
results (2)

Tool	Detection (%)	Detection (%) (Linux)	Detection (%) (Windows)
AVDS	6	0	11
McAfee VM	8	0	15
Nessus	20	4	33
NeXpose	24	22	30
Patchlink scan	0	0	0
QualysGuard	24	17	30
SAINT	36	43	30

Detection and false alarms rate for **unauthenticated** scan

Tool	False alarm (%)	False alarm (%) (Linux)	False alarm (%) (Windows)
AVDS	0	0	0
McAfee VM	3	0	3
Nessus	5	18	3
NeXpose	5	11	0
Patchlink scan	6	0	8
QualysGuard	13	15	11
SAINT	15	11	18

*A **quantitative** evaluation of vulnerability scanning*
results (3)

Tool	Detection (%)	Detection (%) (Linux)	Detection (%) (Windows)
AVDS	34	0	67
McAfee	36	0	70
Nessus	43	9	75
NeXpose	43	22	63
Patchlink scan	36	0	71
QualysGuard	55	17	92
SAINT	43	57	29

Detection and false alarms rate for **authenticated** scan

Tool	False alarm (%)	False alarm (%) (Linux)	False alarm (%) (Windows)
AVDS	0	0	0
McAfee	3	0	3
Nessus	5	18	3
NeXpose	5	11	0
Patchlink scan	6	0	8
QualysGuard	10	15	7
SAINT	13	6	18

*A **quantitative** evaluation of vulnerability scanning*
discussion

- **Unauthenticated scans**: (…) significant differences between how many issues the scanners managed to detect; (…) there is a statistical difference between the tools. The frequency of false alarm was fairly low, indicating that the tools often fail to assess actual vulnerabilities, but are reliable when they do. (…) Informally speaking, it seems that there is a strong connection between the detection rate and the rate of false alarms.
- **Authenticated scans**: (…) all confidence intervals regarding the authenticated scans and detection rate fully overlap. Thus, there is no reason to believe that the scanners perform statistically different when it comes to finding vulnerabilities using credential scans. (…); there is no statistical basis for saying that one tool performs better than the other
- Detection rate when doing both unauthenticated and authenticated scans are significantly higher on Windows hosts.

*A **quantitative** evaluation of vulnerability scanning*
conclusions

- (…) automated scanning, while useful, only find a subset (20-30%) of the vulnerabilities present in a network - accuracy can be improved (up to 40-50%) by giving scanners credentials to the scanned hosts.
- A combined scan using all the included tools yelds a mean of 80% detection rate for credentialed scans – this suggests thah a joint scan using several appliances and a *unified results database* (which is not that easy...) can be a potent solution when in need of highly accurate scans.

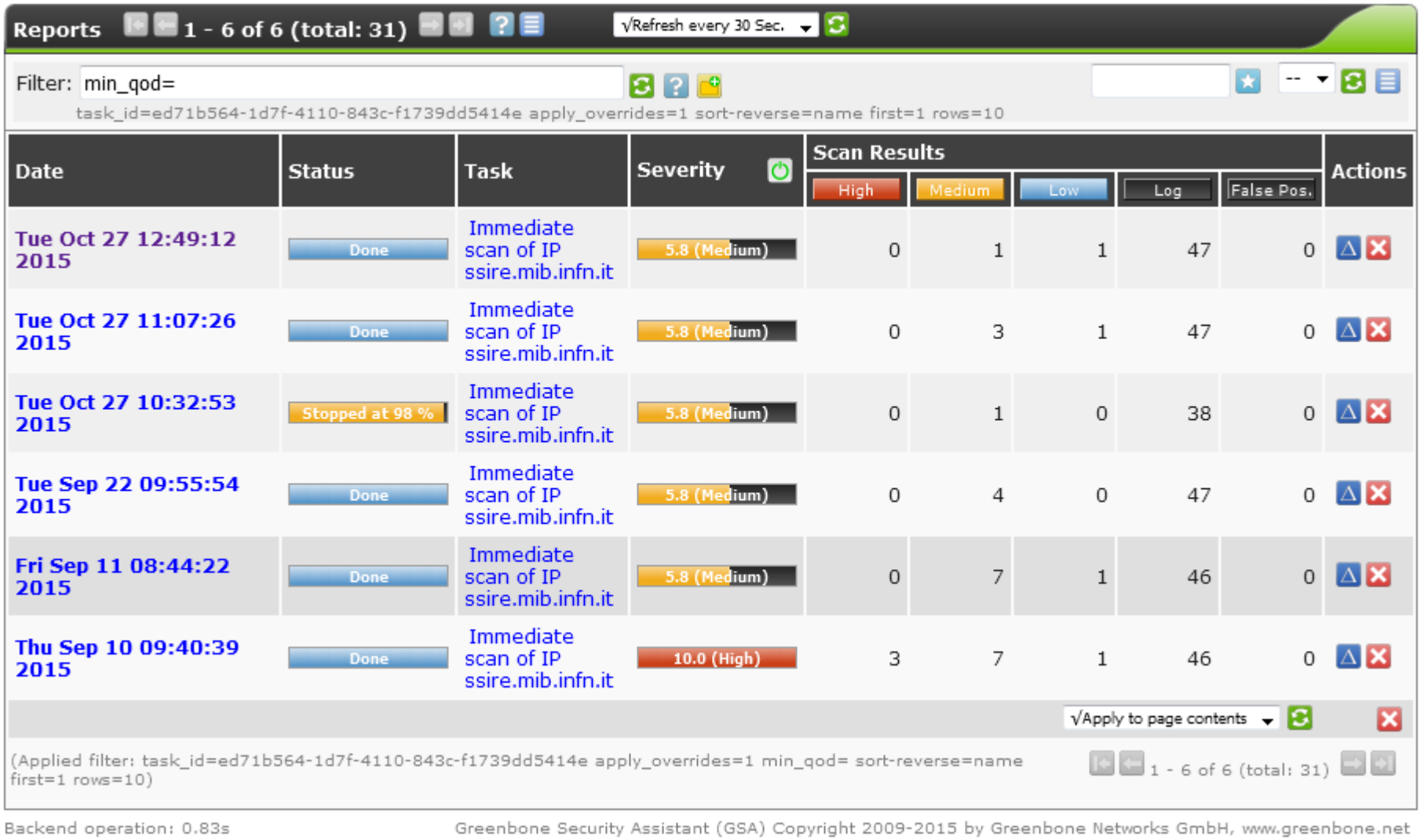
Scan type	Detection (%)	Detection (%) (Linux)	Detection (%) (Windows)
Authenticated	80	65	92
Unauthenticated	44	52	37

OpenVAS versus Nexpose

a quick'n'dirty comparison

- Both scanners tested as VMs.
  - OpenVAS: Open Source (*the world's most advanced OS vulnerability scanner and manager*) - forked from the last free version of Nessus; plugins are written in NASL (nessus attack scripting language). Actively mantained (~ 1 release/year), latest version: 8 (4/2015)
  - Nexpose: aims to support the entire vulnerability management lifecycle, including discovery, detection, verification, risk classification, impact analysis, reporting and mitigation - integrates with Rapid7's *Metasploit* for vulnerability exploitation/validation. Free *Community Edition* fully functional but limited to 32 IP addresses. *Resource hungry* (8GB RAM required, 16 GB recommended - 4 GB RAM at least, otherwise scans abort with a *not enough memory* error), but quite fast (faster than OVAS, at least). Actively mantained (weekly updates), latest version: 6.0.0 (10/2015)

OpenVAS against ssire
1



Reports 1 - 6 of 6 (total: 31) √Refresh every 30 Sec.

Filter: min_qod=

task_id=ed71b564-1d7f-4110-843c-f1739dd5414e apply_overrides=1 sort-reverse=name first=1 rows=10

Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Tue Oct 27 12:49:12 2015	Done	Immediate scan of IP ssire.mib.infn.it	5.8 (Medium)	0	1	1	47	0	
Tue Oct 27 11:07:26 2015	Done	Immediate scan of IP ssire.mib.infn.it	5.8 (Medium)	0	3	1	47	0	
Tue Oct 27 10:32:53 2015	Stopped at 98 %	Immediate scan of IP ssire.mib.infn.it	5.8 (Medium)	0	1	0	38	0	
Tue Sep 22 09:55:54 2015	Done	Immediate scan of IP ssire.mib.infn.it	5.8 (Medium)	0	4	0	47	0	
Fri Sep 11 08:44:22 2015	Done	Immediate scan of IP ssire.mib.infn.it	5.8 (Medium)	0	7	1	46	0	
Thu Sep 10 09:40:39 2015	Done	Immediate scan of IP ssire.mib.infn.it	10.0 (High)	3	7	1	46	0	

√Apply to page contents

(Applied filter: task_id=ed71b564-1d7f-4110-843c-f1739dd5414e apply_overrides=1 min_qod= sort-reverse=name first=1 rows=10)

1 - 6 of 6 (total: 31)

Backend operation: 0.83s

Greenbone Security Assistant (GSA) Copyright 2009-2015 by Greenbone Networks GmbH, www.greenbone.net

OpenVAS against ssire
2

Report: Results 1 - 57 of 57 (total: 76) PDF Done

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base=

Vulnerability	Severity	QoD	Host	Location	Actions
Mail relaying (thorough test)	10.0 (High)	75%	193.206.156.10 (ssire.mib.infn.it)	25/tcp	
Mail relaying (thorough test)	10.0 (High)	75%	193.206.156.10 (ssire.mib.infn.it)	465/tcp	
Mail relaying (thorough test)	10.0 (High)	75%	193.206.156.10 (ssire.mib.infn.it)	587/tcp	
http TRACE XSS attack	5.8 (Medium)	75%	193.206.156.10 (ssire.mib.infn.it)	80/tcp	
http TRACE XSS attack	5.8 (Medium)	75%	193.206.156.10 (ssire.mib.infn.it)	443/tcp	
http TRACE XSS attack	5.8 (Medium)	75%	193.206.156.10 (ssire.mib.infn.it)	5000/tcp	
Apache /server-status accessible	5.0 (Medium)	75%	193.206.156.10 (ssire.mib.infn.it)	80/tcp	
Apache /server-info accessible	5.0 (Medium)	98%	193.206.156.10 (ssire.mib.infn.it)	80/tcp	
Apache /server-status accessible	5.0 (Medium)	75%	193.206.156.10 (ssire.mib.infn.it)	443/tcp	
Apache /server-info accessible	5.0 (Medium)	98%	193.206.156.10 (ssire.mib.infn.it)	443/tcp	
TCP timestamps	2.6 (Low)	75%	193.206.156.10 (ssire.mib.infn.it)	general/tcp	
OS fingerprinting	0.0 (Log)	75%	193.206.156.10 (ssire.mib.infn.it)	general/tcp	
DIRB (NASL wrapper)	0.0 (Log)	75%	193.206.156.10 (ssire.mib.infn.it)	general/tcp	
ICMP Timestamp Detection	0.0 (Log)	75%	193.206.156.10 (ssire.mib.infn.it)	general/icmp	
arachni (NASL wrapper)	0.0 (Log)	75%	193.206.156.10 (ssire.mib.infn.it)	general/tcp	
Nikto (NASL wrapper)	0.0 (Log)	75%	193.206.156.10 (ssire.mib.infn.it)	general/tcp	

OpenVAS QoD (new to 8.0)

describes the reliability of vulnerability detection

Overview on QoD values and types

QoD	QoD Type(s)	Description
100%	exploit	The detection happened via an exploit and therefore is fully verified.
99%	remote_vul	Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerability.
98%	remote_app	Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.
97%	package	Authenticated package-based checks for Linux(oid) systems.
97%	registry	Authenticated registry-based checks for Windows systems.
95%	remote_active	Remote active checks (code execution, traversal attack, sql injection etc.) where the response shows the likely presence of the vulnerable application or of the vulnerability. "Likely" means that only rare circumstances are possible where the detection would be wrong.
80%	remote_banner	Remote banner check of applications that offer patch level in version. Many proprietary products do so.
80%	executable_version	Authenticated executable version checks for Linux(oid) or Windows systems where applications offer patch level in version.
75%		This value was assigned to any pre-qod results during migration to OpenVAS-8 and is also assigned for results from NVTs that do not own a qod. However, some NVTs eventually might own this value for some reason.
70%	remote_analysis	Remote checks that do some analysis but which are not always fully reliable.
50%	remote_probe	Remote checks where intermediate systems such as firewalls might pretend correct detection so that it is actually not clear whether the application itself answered. This can happen for example for non-TLS connections.
30%	remote_banner_unreliable	Remote Banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches.
30%	executable_version_unreliable	Authenticated executable version checks for Linux(oid) systems where applications don't offer patch level in version identification.
1%	general_note	General note on potential vulnerability without finding any present application.

OpenVAS against ssire 3

Report: Results 1 - 39 of 39 (total: 58) PDF 98 %

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base=

Vulnerability	Severity	QoD	Host	Location	Actions
http TRACE XSS attack	5.8 (Medium)	75%	193.206.156.10	5000/tcp	
TCP timestamps	2.6 (Low)	75%	193.206.156.10	general/tcp	
OS fingerprinting	0.0 (Log)	75%	193.206.156.10	general/tcp	
DIRB (NASL wrapper)	0.0 (Log)	75%	193.206.156.10	general/tcp	
ICMP Timestamp Detection	0.0 (Log)	75%	193.206.156.10	general/icmp	
arachni (NASL wrapper)	0.0 (Log)	75%	193.206.156.10	general/tcp	
Nikto (NASL wrapper)	0.0 (Log)	75%	193.206.156.10	general/tcp	
Traceroute	0.0 (Log)	75%	193.206.156.10	general/tcp	
SSH Protocol Versions Supported	0.0 (Log)	75%	193.206.156.10	22/tcp	
SSH Server type and version	0.0 (Log)	75%	193.206.156.10	22/tcp	
Services	0.0 (Log)	75%	193.206.156.10	22/tcp	
SMTP Server type and version	0.0 (Log)	75%	193.206.156.10	25/tcp	
SMTP STARTTLS Detection	0.0 (Log)	75%	193.206.156.10	25/tcp	
Services	0.0 (Log)	75%	193.206.156.10	25/tcp	
HTTP Server type and version	0.0 (Log)	75%	193.206.156.10	80/tcp	
Services	0.0 (Log)	75%	193.206.156.10	80/tcp	

OpenVAS against ssire
4

```
net.ipv4.tcp_timestamps = 0
```

Report: Results 1 - 39 of 39 (total: 58) PDF Stopped

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base=

Vulnerability	Severity	QoD	Host	Location	Actions
http TRACE XSS attack	5.8 (Medium)	75%	193.206.156.10 (ssire.mib.infn.it)	5000/tcp	
OS fingerprinting	0.0 (Log)	75%	193.206.156.10 (ssire.mib.infn.it)	general/tcp	

index.html empty

Report: Results 1 - 51 of 51 (total: 70) PDF Done

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base=

Vulnerability	Severity	QoD	Host	Location	Actions
http TRACE XSS attack	5.8 (Medium)	75%	193.206.156.10 (ssire.mib.infn.it)	5000/tcp	
Apache Web Server ETag Header Information Disclosure Weakness	4.3 (Medium)	75%	193.206.156.10 (ssire.mib.infn.it)	80/tcp	
Apache Web Server ETag Header Information Disclosure Weakness	4.3 (Medium)	75%	193.206.156.10 (ssire.mib.infn.it)	443/tcp	
TCP timestamps	2.6 (Low)	75%	193.206.156.10 (ssire.mib.infn.it)	general/tcp	
OS fingerprinting	0.0 (Log)	75%	193.206.156.10 (ssire.mib.infn.it)	general/tcp	

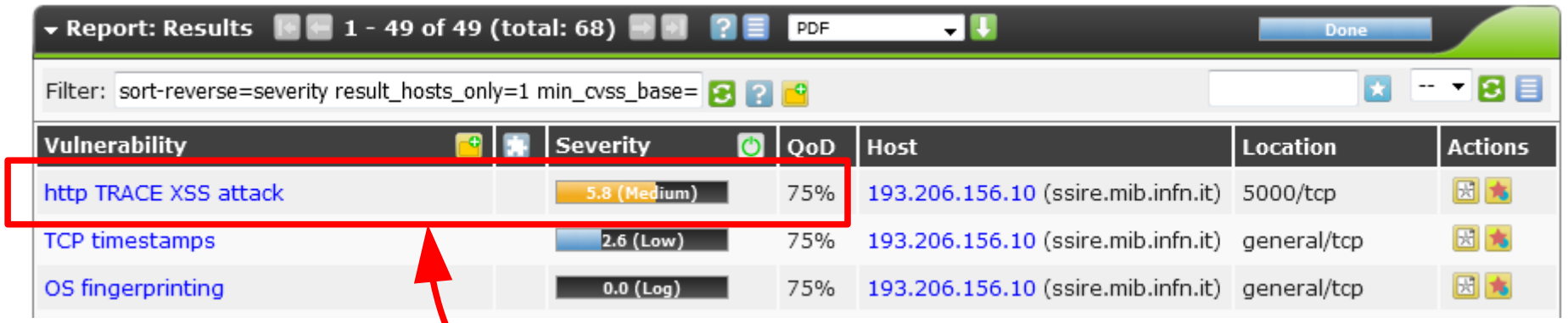
OpenVAS against ssire

5

index.html empty

in httpd.conf:

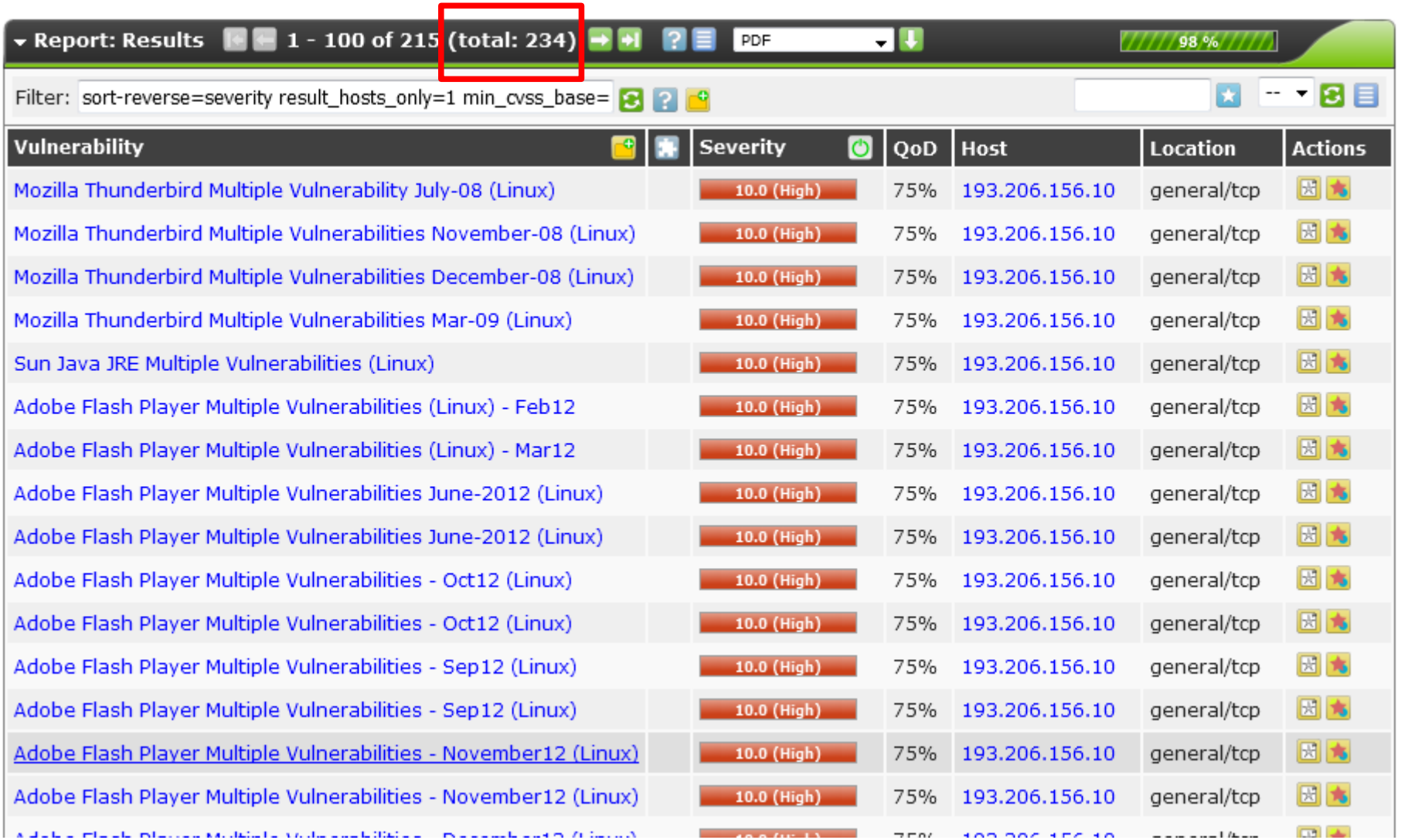
- `Header unset Etag`
- `FileETag none`



OMD (open monitoring distribution) http server

OpenVAS against ssire

6 – auth scan (!!!)



Report: Results 1 - 100 of 215 (total: 234) PDF 98 %

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base=

Vulnerability	Severity	QoD	Host	Location	Actions
Mozilla Thunderbird Multiple Vulnerability July-08 (Linux)	10.0 (High)	75%	193.206.156.10	general/tcp	
Mozilla Thunderbird Multiple Vulnerabilities November-08 (Linux)	10.0 (High)	75%	193.206.156.10	general/tcp	
Mozilla Thunderbird Multiple Vulnerabilities December-08 (Linux)	10.0 (High)	75%	193.206.156.10	general/tcp	
Mozilla Thunderbird Multiple Vulnerabilities Mar-09 (Linux)	10.0 (High)	75%	193.206.156.10	general/tcp	
Sun Java JRE Multiple Vulnerabilities (Linux)	10.0 (High)	75%	193.206.156.10	general/tcp	
Adobe Flash Player Multiple Vulnerabilities (Linux) - Feb12	10.0 (High)	75%	193.206.156.10	general/tcp	
Adobe Flash Player Multiple Vulnerabilities (Linux) - Mar12	10.0 (High)	75%	193.206.156.10	general/tcp	
Adobe Flash Player Multiple Vulnerabilities June-2012 (Linux)	10.0 (High)	75%	193.206.156.10	general/tcp	
Adobe Flash Player Multiple Vulnerabilities June-2012 (Linux)	10.0 (High)	75%	193.206.156.10	general/tcp	
Adobe Flash Player Multiple Vulnerabilities - Oct12 (Linux)	10.0 (High)	75%	193.206.156.10	general/tcp	
Adobe Flash Player Multiple Vulnerabilities - Oct12 (Linux)	10.0 (High)	75%	193.206.156.10	general/tcp	
Adobe Flash Player Multiple Vulnerabilities - Sep12 (Linux)	10.0 (High)	75%	193.206.156.10	general/tcp	
Adobe Flash Player Multiple Vulnerabilities - Sep12 (Linux)	10.0 (High)	75%	193.206.156.10	general/tcp	
Adobe Flash Player Multiple Vulnerabilities - November12 (Linux)	10.0 (High)	75%	193.206.156.10	general/tcp	
Adobe Flash Player Multiple Vulnerabilities - November12 (Linux)	10.0 (High)	75%	193.206.156.10	general/tcp	

Qualys SSL server test against ssire

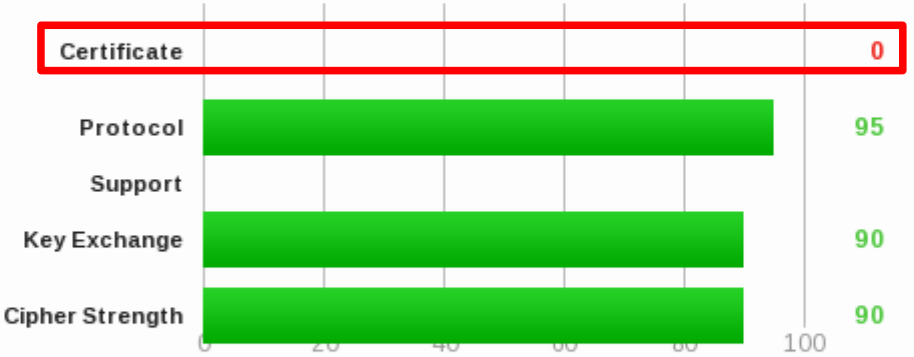
SSL Report: ssire.mib.infn.it (2001:760:4211:0:0:0:0:100)

Assessed on: Wed, 28 Oct 2015 11:23:38 UTC | **HIDDEN** | Clear cache

Scan Another »

Summary

Overall Rating



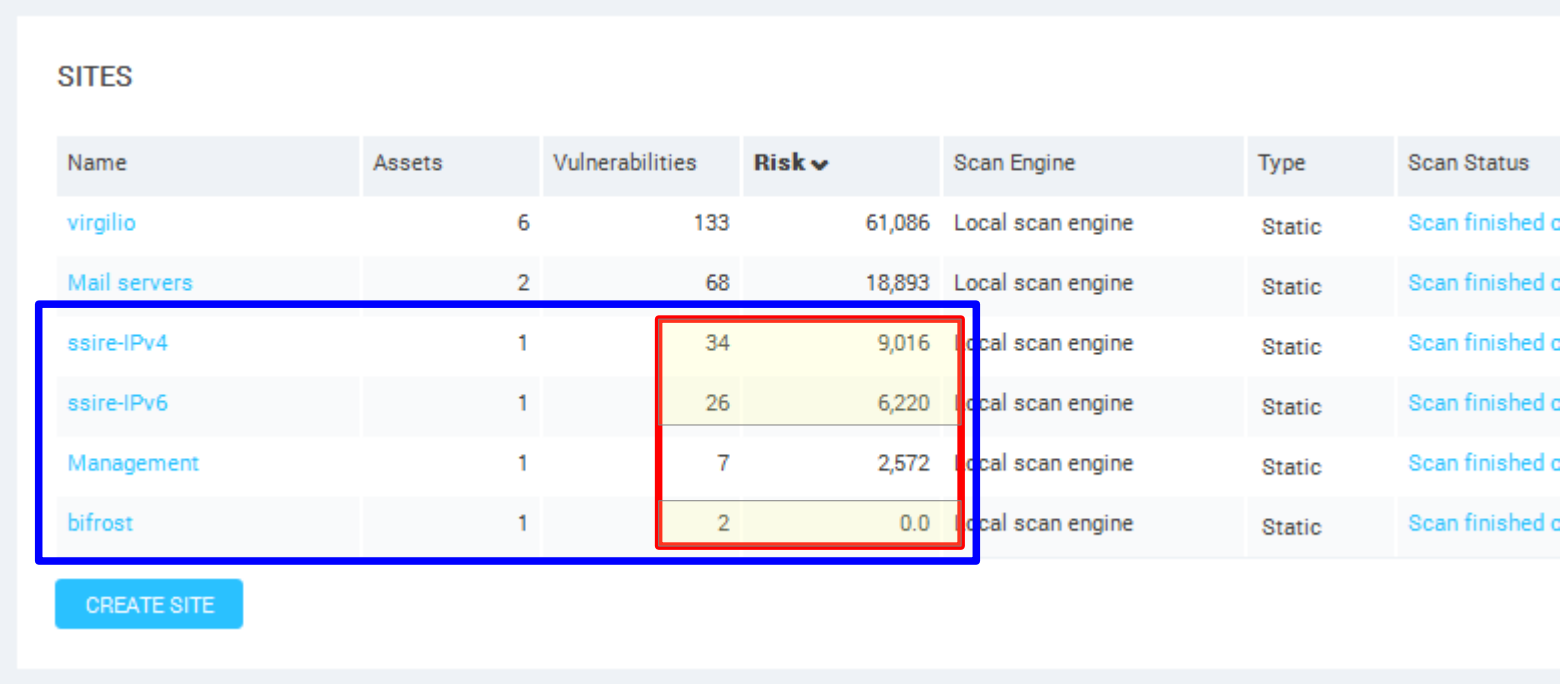
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server's certificate is not trusted, see below for details.

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

Nexpose against ssire

1 – unauth scan



SITES

Name	Assets	Vulnerabilities	Risk	Scan Engine	Type	Scan Status
virgilio	6	133	61,086	Local scan engine	Static	Scan finished c
Mail servers	2	68	18,893	Local scan engine	Static	Scan finished c
ssire-IPv4	1	34	9,016	cal scan engine	Static	Scan finished c
ssire-IPv6	1	26	6,220	cal scan engine	Static	Scan finished c
Management	1	7	2,572	cal scan engine	Static	Scan finished c
bifrost	1	2	0.0	cal scan engine	Static	Scan finished c

CREATE SITE

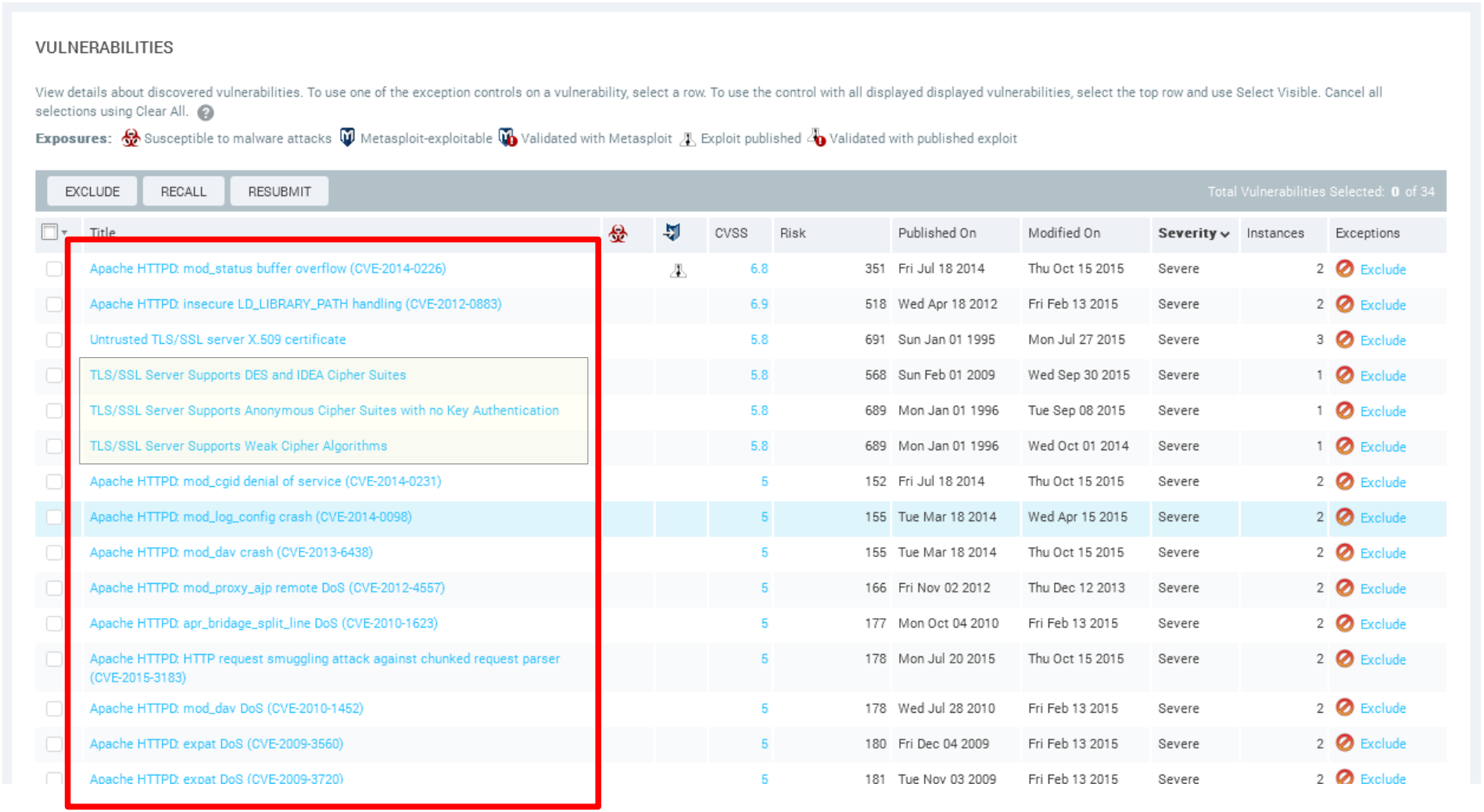
Nexpose against ssire
2 – unauth scan

SERVICES

Service Name	Product	Port ▲	Protocol	Vulnerabilities	Users	Groups
SMTP	Sendmail	25	TCP	1	0	0
HTTP	HTTPD 2.2.15	80	TCP	25	0	0
portmapper		111	UDP	0	0	0
portmapper		111	TCP	0	0	0
HTTPS	HTTPD 2.2.15	443	TCP	27	0	0
SMTPS		465	TCP	5	0	0
SMTP	Sendmail	587	TCP	1	0	0
UPnP-HTTPU		5000	TCP	1	0	0
status		40402	TCP	0	0	0
status		40586	UDP	0	0	0

Nexpose against ssire

3 – unauth scan



VULNERABILITIES

View details about discovered vulnerabilities. To use one of the exception controls on a vulnerability, select a row. To use the control with all displayed displayed vulnerabilities, select the top row and use Select Visible. Cancel all selections using Clear All.

Exposures: Susceptible to malware attacks | Metasploit-exploitable | Validated with Metasploit | Exploit published | Validated with published exploit

EXCLUDE | RECALL | RESUBMIT — Total Vulnerabilities Selected: 0 of 34

Title	CVSS	Risk	Published On	Modified On	Severity	Instances	Exceptions
Apache HTTPD: mod_status buffer overflow (CVE-2014-0226)	6.8	351	Fri Jul 18 2014	Thu Oct 15 2015	Severe	2	Exclude
Apache HTTPD: insecure LD_LIBRARY_PATH handling (CVE-2012-0883)	6.9	518	Wed Apr 18 2012	Fri Feb 13 2015	Severe	2	Exclude
Untrusted TLS/SSL server X.509 certificate	5.8	691	Sun Jan 01 1995	Mon Jul 27 2015	Severe	3	Exclude
TLS/SSL Server Supports DES and IDEA Cipher Suites	5.8	568	Sun Feb 01 2009	Wed Sep 30 2015	Severe	1	Exclude
TLS/SSL Server Supports Anonymous Cipher Suites with no Key Authentication	5.8	689	Mon Jan 01 1996	Tue Sep 08 2015	Severe	1	Exclude
TLS/SSL Server Supports Weak Cipher Algorithms	5.8	689	Mon Jan 01 1996	Wed Oct 01 2014	Severe	1	Exclude
Apache HTTPD: mod_cgid denial of service (CVE-2014-0231)	5	152	Fri Jul 18 2014	Thu Oct 15 2015	Severe	2	Exclude
Apache HTTPD: mod_log_config crash (CVE-2014-0098)	5	155	Tue Mar 18 2014	Wed Apr 15 2015	Severe	2	Exclude
Apache HTTPD: mod_dav crash (CVE-2013-6438)	5	155	Tue Mar 18 2014	Thu Oct 15 2015	Severe	2	Exclude
Apache HTTPD: mod_proxy_ajp remote DoS (CVE-2012-4557)	5	166	Fri Nov 02 2012	Thu Dec 12 2013	Severe	2	Exclude
Apache HTTPD: apr_bridage_split_line DoS (CVE-2010-1623)	5	177	Mon Oct 04 2010	Fri Feb 13 2015	Severe	2	Exclude
Apache HTTPD: HTTP request smuggling attack against chunked request parser (CVE-2015-3183)	5	178	Mon Jul 20 2015	Thu Oct 15 2015	Severe	2	Exclude
Apache HTTPD: mod_dav DoS (CVE-2010-1452)	5	178	Wed Jul 28 2010	Fri Feb 13 2015	Severe	2	Exclude
Apache HTTPD: expat DoS (CVE-2009-3560)	5	180	Fri Dec 04 2009	Fri Feb 13 2015	Severe	2	Exclude
Apache HTTPD: expat DoS (CVE-2009-3720)	5	181	Tue Nov 03 2009	Fri Feb 13 2015	Severe	2	Exclude

Nexpose against ssire

4 – auth scan

Scan Type	Started	Assets	Vulnerabilities	Duration	Completed
Manual	11/3/2015 11:42 AM	1	21	6 minutes	11/3/2015 11:49 AM
Manual	11/3/2015 11:26 AM	1	27	7 minutes	11/3/2015 11:33 AM
Manual	11/3/2015 11:07 AM	1	35	5 minutes	11/3/2015 11:12 AM

SITES

Name	Assets	Vulnerabilities	Risk	Type	Scan Status
virgilio	6	133	61,093	Static	Scan finishe
Mail servers	2	68	18,896	Static	Scan finishe
ssire-IPv4	1	21	9,140	Static	Scan finishe
ssire-IPv6	1	26	6,222	Static	Scan finishe
Management	1	7	2,573	Static	Scan finishe
bifrost	1	2	0.0	Static	Scan finishe

CREATE SITE

Nexpose against ssire
5 – auth scan

CESA-2015:1012: thunderbird security update

CESA-2015:1471: bind security update

CESA-2015:1513: bind security update

CESA-2015:1623: kernel security and bug fix update

Apache HTTPD: insecure LD_LIBRARY_PATH handling (CVE-2012-0883)

CESA-2015:1482: libuser security update

Untrusted TLS/SSL server X.509 certificate

TLS/SSL Server Supports Weak Cipher Algorithms

TLS/SSL Server Supports Anonymous Cipher Suites with no Key Authentication

TLS/SSL Server Supports DES and IDEA Cipher Suites

CESA-2015:0797: xorg-x11-server security update

Apache HTTPD: HTTP request smuggling attack against chunked request parser (CVE-2015-318

TLS/SSL Server Supports Cipher Block Chaining (CBC) Ciphers

CESA-2015:1210: abrt security update

CESA-2015:1185: bind security update

TLS/SSL Server Supports The Use of Static Key Ciphers

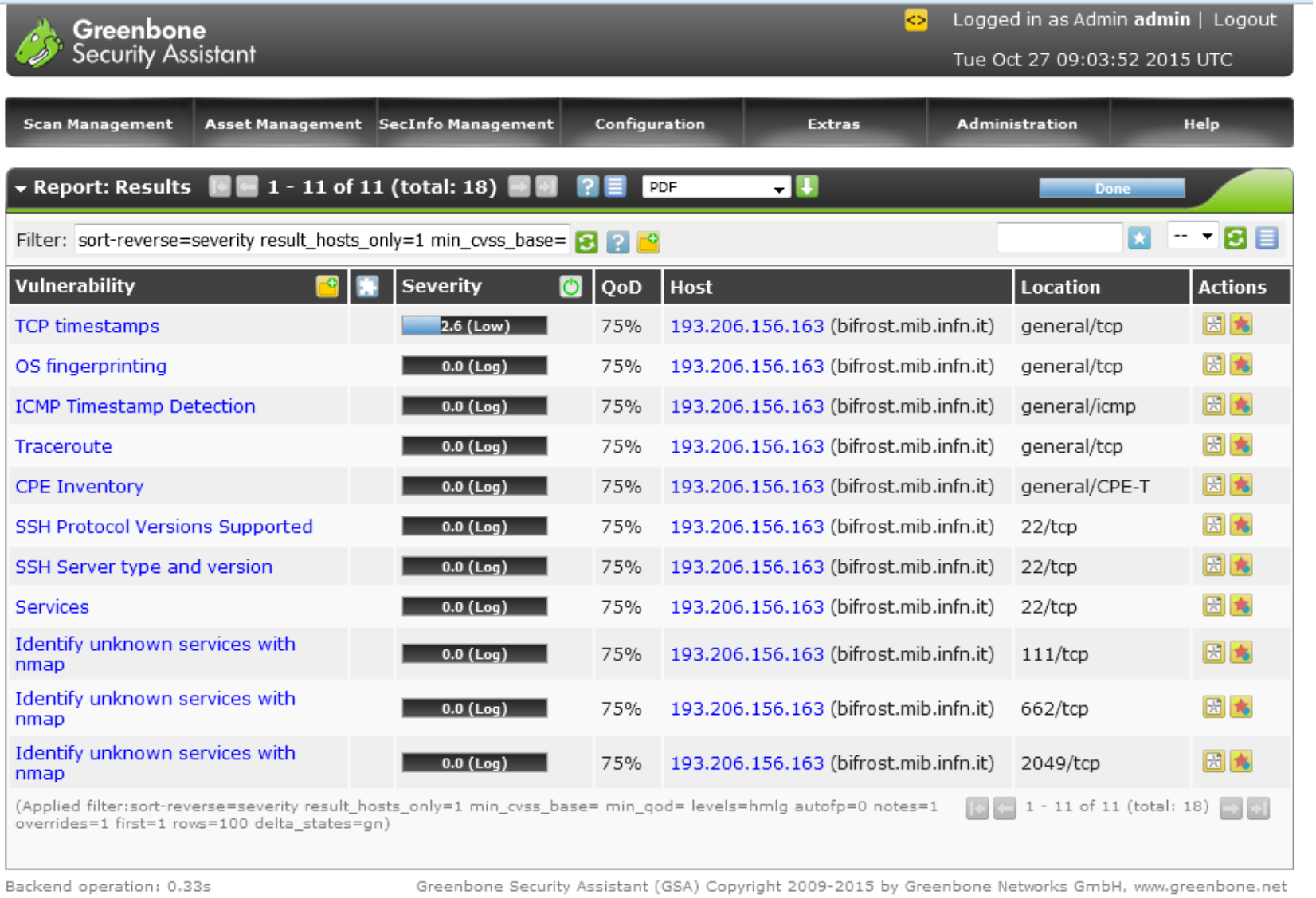
TCP timestamp response

VULNERABILITIES

Vulnerability	Severity	Instances
CESA-2013:1476: firefox security update	Critical	1
CESA-2015:1207: firefox security update	Critical	1
CESA-2015:1455: thunderbird security update	Critical	1
CESA-2015:1229: java-1.7.0-openjdk security update	Critical	1
CESA-2015:1526: java-1.6.0-openjdk security update	Critical	1
CESA-2015:1586: firefox security update	Critical	1
CESA-2015:1012: thunderbird security update	Critical	1
CESA-2015:1623: kernel security and bug fix update	Critical	1
Apache HTTPD: insecure LD_LIBRARY_PATH handling (	Severe	2
Untrusted TLS/SSL server X.509 certificate	Severe	3
TLS/SSL Server Supports Anonymous Cipher Suites w	Severe	1
TLS/SSL Server Supports Weak Cipher Algorithms	Severe	1
TLS/SSL Server Supports DES and IDEA Cipher Suites	Severe	1
CESA-2015:0797: xorg-x11-server security update	Severe	1
Apache HTTPD: HTTP request smuggling attack agains	Severe	2
TLS/SSL Server Supports Cipher Block Chaining (CBC)	Severe	2
TLS/SSL Server Supports The Use of Static Key Ciphe	Moderate	1
TCP timestamp response	Moderate	1
UDP IP ID Zero	Moderate	1
ICMP timestamp response	Moderate	1
UPnP SSDP Traffic Amplification	Moderate	1

Showing 1 to 21 of 21 Rows per page: 100 1 of 1

OpenVAS against bifrost



Nexpose against bifrost

bifrost | View all sites
Full audit without Web Spider | View all scans

				RISK SCORE	USER-ADDED TAGS		
ADDRESSES		OS	Linux 2.6.32				
HARDWARE	B8:AC:6F:85:4E:81	CPE	cpe:/o:linux:linux_kernel:2.6.32	ORIGINAL 0.0	CUSTOM TAGS None	OWNERS None	Add tags
ALIASES	bifrost.mib.infn.it	HOST TYPE	Unknown				
SITE	bifrost	LAST SCAN	Oct 29, 2015 2:43:10 PM (1 minute ago)	CONTEXT-DRIVEN 0.0	LOCATIONS None	CRITICALITY None	
SEE ASSET PAGE							

VULNERABILITIES

Vulnerability	Severity	Instances
UDP IP ID Zero	Moderate	1

SERVICES

Service Name	Product	Port	Protocol	Vulnerabilities	Users	Groups
SSH	OpenSSH 5.3	22	TCP	0	0	0
portmapper		111	UDP	0	0	0
portmapper		111	TCP	0	0	0
status		662	UDP	0	0	0
status		662	TCP	0	0	0
OpenVPN		1194	UDP	0	0	0

Conclusions

There are more things in heaven and earth, Horatio,
Than are dreamt of in your philosophy.

- Vulnerability detection & assessment ***IS NOT*** an exact science...;
- 100% trust in the response of a single tool ***IS*** a bad idea;
- It seems that running *at least two tools* is not only recommended, but *mandatory;* running one credentialed scan is recommended:
  - say: *unauth OpenVAS* & *nmap w/NSE* from outside your network; *auth Nexpose* from inside your network (against critical or exposed nodes, at least)

References

- sectools.org
- nmap.org
- hackertarget.com
- A quantitative evaluation of vulnerability scanning

  Holm, Sommestad, Almroth, Persson

  Information Management & Computer Security, Vol.19 No.4, 2011
- Performance of automated network vulnerability scanning at remediating security issues

  Holm

  Computers & Security 31 (2012)

NSE - Nmap Scripting Engine

poodle!

weak ciphers!