

Vulnerability Scanning



LinkedIn : <https://www.linkedin.com/in/mohamed-elsayaad>

GitHub : <https://github.com/0xDos>

Vulnerability Scanning Overview

- How Vulnerability Scanners Work

لازم اشتغل مع Manual مع Automated ؟

- Manual vs. Automated Scanning

لو شغال في Red Teaming ما ينفعش استخدم أي Automated Scanner لان الأولوية بتكون اني افضل علي network بدون ما اعمل أي انذار لل Security Team او أي Device المفروض انه ممكن يكشفهم سواء IDS او IPS او حتي Firewall لان معظم scanners بتتكشف بسهولة سواء الطريقة ال بتفحص بيها او حتي signature الخاصه بيها شكل packet الخاصه ب nmap مثلا وهيا بتتبع request ازاي

- Internet Scanning vs Internal Scanning

بعدا كذا قدام هاعرف ازاي اعدي firewall اني اغير شكل traffic وحجم الباكيت

- *Authenticated vs Unauthenticated Scanning*

Network Vulnerability Scanning

Network vulnerability scans go deeper than discovery scans.

a false positive report (crying wolf)

when the vulnerability scanner reports a vulnerability but there is no vulnerability.

a false negative report.

when the vulnerability scanner misses a vulnerability and fails to alert the administrator to the presence of a dangerous situation.

By default, network vulnerability scanners run **unauthenticated scans**.

Means scanner has no special privileges. (They test the target systems without having passwords or any root/ administrator privileges) , this limits the ability of the scanner to fully evaluate possible vulnerabilities.

To reduce false positive and false negative reports we should perform **authenticated scans** of systems.

كمان علشان احسن جوده Scanner عمله Update قبل ما أبتدي الشغل بتاعي علشان قاعده البيانات الخاصه به يكون وصلها اخر حاجه

Scanner أوقات كتيره بتطلعلي false positive و false negative علشان كذا دايما اراجع واتأكد من output بتاعها وبالتالي أتأكد انها ثغره ولا لا

The best tool for network vulnerability scan is **Nessus vulnerability scanner**

Scanner بيعمل حاجتين :

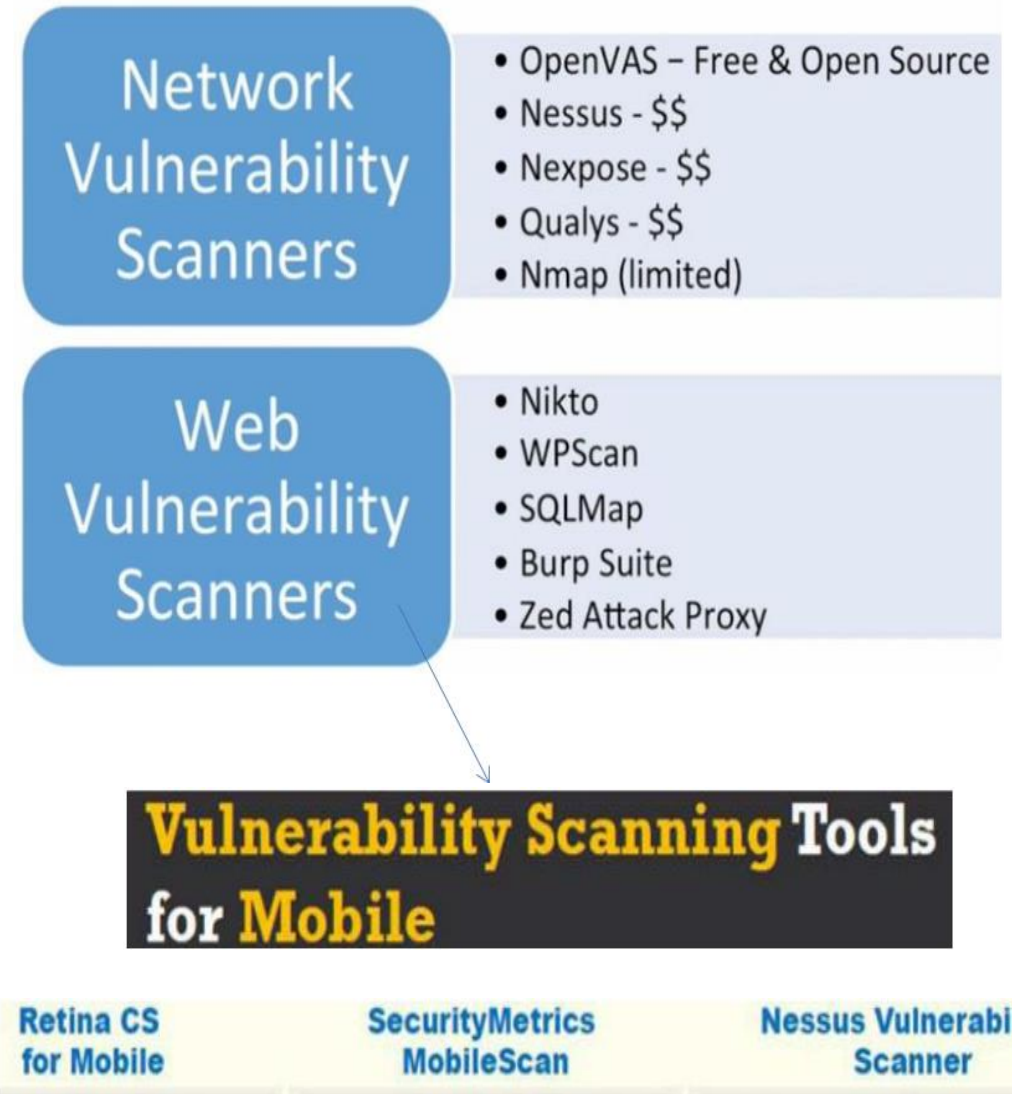
(1) **Misconfiguration** <<< يعني user, pass هما (admin,admin) يعني administrator وهو بيعمل اعدادات السيستم ينس يغير اعدادات default بتاعته ال هيا admin,admin

(2) **Bugs** <<< في service ال شغاله حاجه مثلا زي internal blues ودي ثغره موجوده في service بتاعت smb

Vulnerability Scanner Tools

Nessus , GFI LanGuard , **OpenVAS** , Retina CS , MBSA
Nsauditor network security Auditor . Nexpose . SAINT

Retina CS http://www.beyondtrust.com	OpenVAS http://www.openvas.org
Core Impact Professional http://www.coresecurity.com	Security Manager Plus http://www.manageengine.com
MBSA http://www.microsoft.com	Nexpose http://www.rapid7.com
Shadow Security Scanner http://www.safety-lab.com	SAINT http://www.saintcorporation.com
Nsauditor Network Security Auditor http://www.nsauditor.com	Security Auditor's Research Assistant (SARA) http://www-arc.com



Nessus® Vulnerability Scanner



Tenable Nessus

Nessus is one of the most popular vulnerability scanners, it has a number of policies that can be deployed across an enterprise network.

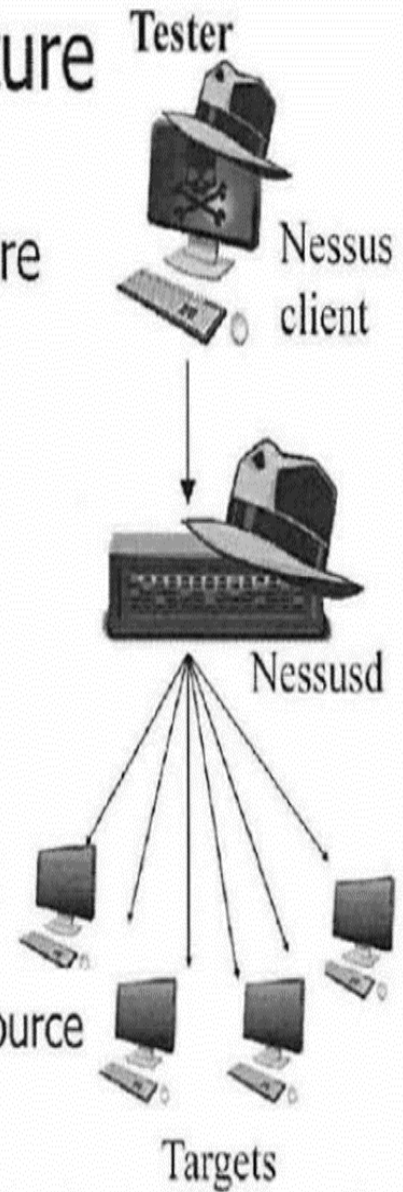
<https://www.tenable.com/products/nessus/select-your-operating-system>

Download link:

https://www.tenable.com/downloads/nessus#download?utm_campaign=00000292&utm_promoter=tenable-dm&utm_medium=email&utm_content=confirmation&utm_source=nessus-trial

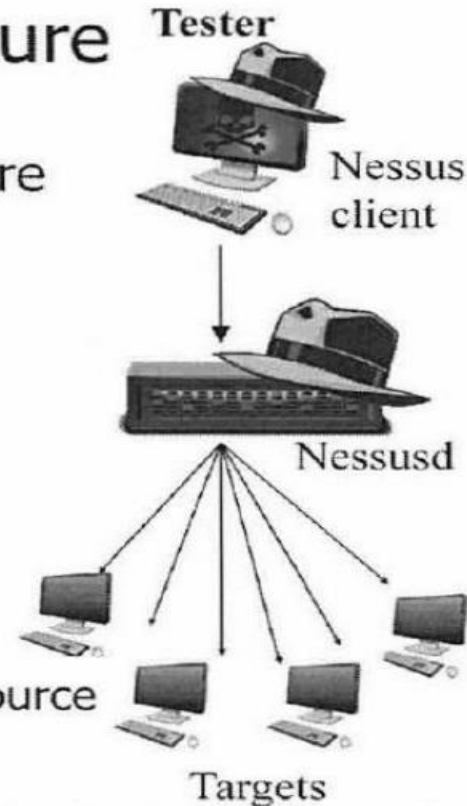
Nessus Architecture

- Nessus is a client-server architecture
 - Client: Browser-based
 - Server: nessusd
- Nessus 5 is the most widely used version today
 - OpenVAS is a free fork of Nessus 2
 - Includes new plugins but not as many as commercial Nessus does
 - Also, OpenVAS performance is about 50% slower than Nessus
 - Still, OpenVAS is useful, free, open-source



Nessus Architecture

- Nessus is a client-server architecture
 - Client: Browser-based
 - Server: nessusd
- Nessus 5 is the most widely used version today
 - OpenVAS is a free fork of Nessus 2
 - Includes new plugins but not as many as commercial Nessus does
 - Also, OpenVAS performance is about 50% slower than Nessus
 - Still, OpenVAS is useful, free, open-source



Many years ago, some open source developers created a fork of the last free, open source version of Nessus (version 2).

The result was **Open VAS**, a completely free vulnerability scanner.

Although new plugins are distributed with and for Open VAS, it is important to note that the commercial version of Nessus has more plug ins and is more than 50% faster than Open VAS.

Still, **Open VAS is a useful, free, open-source alternative**.

OpenVAS

```
root@kali:~# apt-get update
root@kali:~# apt-get dist-upgrade
root@kali:~# apt-get install openvas
root@kali:~# openvas-setup
```

User created with password 'c2a16828-a0de-40e5-bb60-1f0fd9104fca'. root@kali:~# **OpenVAS-start**

Point your browser to <https://127.0.0.1:9392>, accept the self signed SSL certificate and plugin the credentials for the admin user.

Default user is admin.


The admin password was generated during the setup phase

In case if you forget username or password , type in terminal:

```
openvasmd --user=admin --new-password=new_password
openvasmd --create-user NEWUSER
```

This opens the '**greenbone**' web interface for openvas and sign in.

To initiate a simple scan of an ip address or hostname, click the small **(tiny) purple icon** with the wand in it. This will take you to a screen with an input where you can perform a full fast scan of a host.

 **Greenbone**
Security Assistant

Logged in as Admin **admin** | Logout
Tue Nov 8 01:46:08 2016 UTC

Scan Management

Asset Management

SecInfo Management

Configuration

Extras

Administration

Help

Tasks (total: 0)      vNo auto-refresh Filter:   

apply_overrides=1 rows=10 first=1 sort=name

Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon  any time later on.

If you want help creating new scan tasks but also more options, you can select "Advanced Task Wizard" from the wizard selection menu at the top of this window where it currently says "Task Wizard" marked with a small arrow.

For more detailed information on functionality, please try the integrated help system. It is always available as a context sensitive link as icon .



Quick start: Immediately scan an IP address
IP address or hostname:

For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

When creating the Target and Task I will use the default Port List, Alert, OpenVAS Scan Config, Credentials, OpenVAS Scanner and Slave configured in "My Settings".

By clicking the New Task icon  you can also create a new Task yourself. However, you will need a Target first, which you can create by going to the Targets page found in the Configuration menu using the New icon there.

Backend operation: 0.22s

Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

There are loads of menus in the greenbone web ui:

Scan management

The most important entry in this menu is 'New Task' – you can start complex scans from this screen.

Asset Management

Currently contains a single item: Hosts

This is where the list of accumulated hosts from all your scans appear.

Sec Info Management

Contains a few items, each representing the vulnerability databases that openvas knows about

Configuration

Various configuration options, targets and scan configurations

Extras

Configuration of the web Gui it self

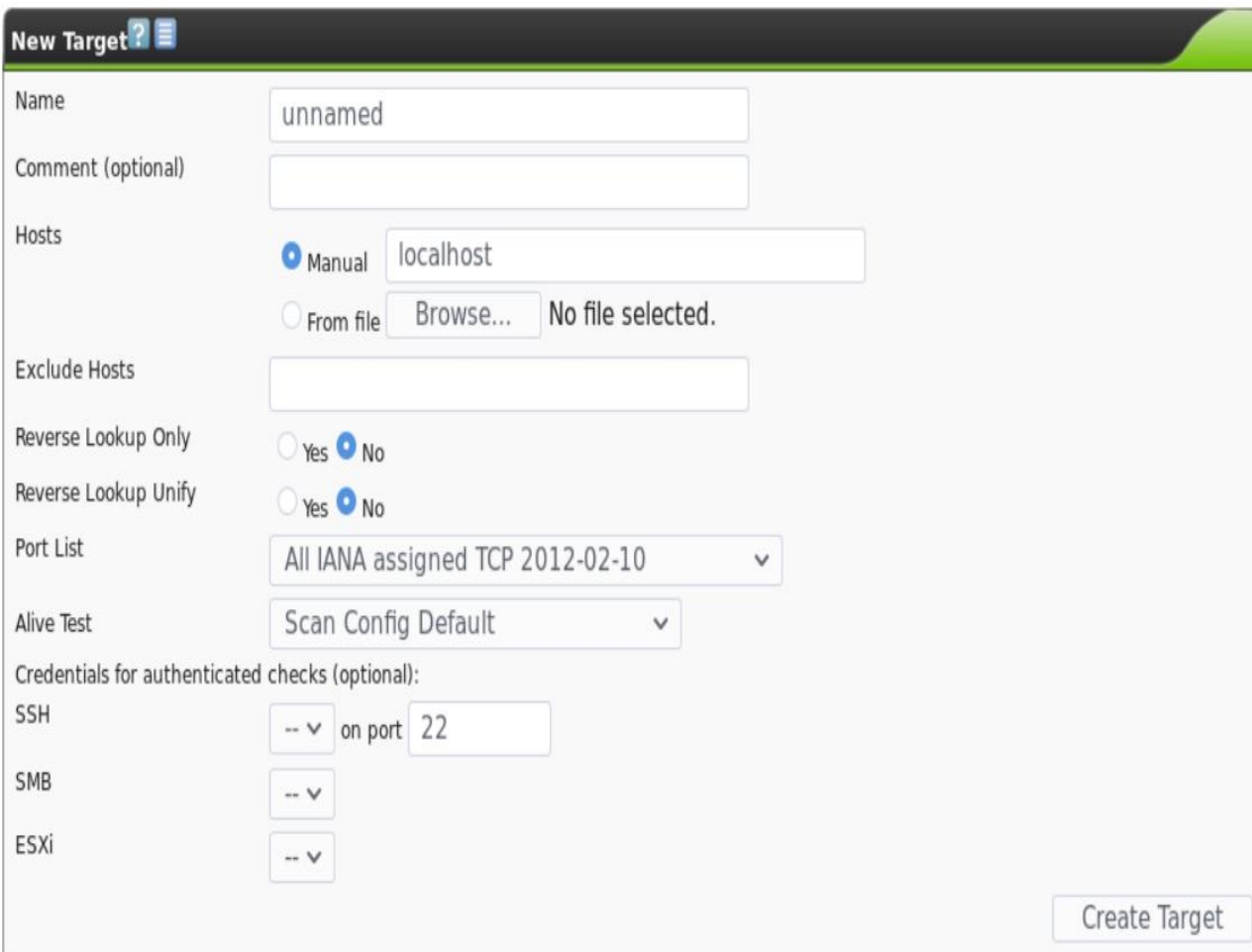
Administration

User management, Feed synchronization, update, etc

the "New Task" icon is represented by a star.

If you only have one IP address, you can use the quick start to immediately start up a scan for that IP address, as shown in the bottom right hand corner of the home page.

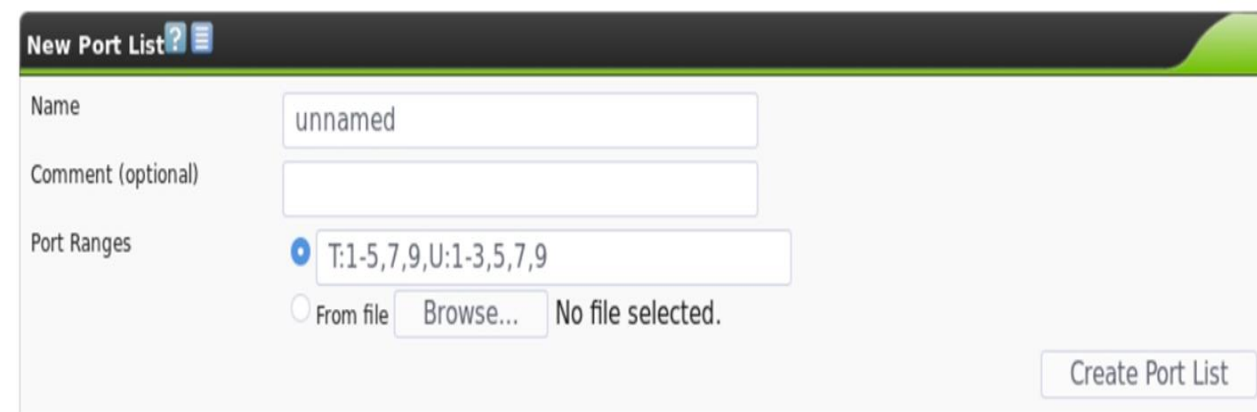
To configure a list of hosts instead of just one, navigate to the "Configuration" tab in the site header, then select Configuration -> Targets. This will take you to the Targets page where you can configure scan targets.



The 'New Target' form in OpenVAS includes the following fields and options:

- Name:** A text input field containing 'unnamed'.
- Comment (optional):** An empty text input field.
- Hosts:** A section with two radio buttons: 'Manual' (selected) and 'From file'. The 'Manual' option has a text input field containing 'localhost'. The 'From file' option has a 'Browse...' button and the text 'No file selected.'
- Exclude Hosts:** An empty text input field.
- Reverse Lookup Only:** Radio buttons for 'Yes' and 'No', with 'No' selected.
- Reverse Lookup Unify:** Radio buttons for 'Yes' and 'No', with 'No' selected.
- Port List:** A dropdown menu showing 'All IANA assigned TCP 2012-02-10'.
- Alive Test:** A dropdown menu showing 'Scan Config Default'.
- Credentials for authenticated checks (optional):** A section with three rows: 'SSH' (dropdown with '--' and 'on port' followed by input '22'), 'SMB' (dropdown with '--'), and 'ESXi' (dropdown with '--').
- Create Target:** A button at the bottom right.

To add a new custom list of ports that OpenVAS will scan, navigate to the "Port Lists" page by going to Configuration -> Port Lists.



The 'New Port List' form in OpenVAS includes the following fields and options:

- Name:** A text input field containing 'unnamed'.
- Comment (optional):** An empty text input field.
- Port Ranges:** A section with two radio buttons: 'Manual' (selected) and 'From file'. The 'Manual' option has a text input field containing 'T:1-5,7,9,U:1-3,5,7,9'. The 'From file' option has a 'Browse...' button and the text 'No file selected.'
- Create Port List:** A button at the bottom right.

click scan
click the star (new task)
click actions play

Greenbone Security Assistant

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Tasks (0 of 0)

Tasks by Severity Class

New Task

Name: metasploitable scan

Comment:

Scan Targets: metasploitable

Alerts:

Schedule: --

Add results to Assets: ☒ yes ☐ no

Apply Overrides: ☒ yes ☐ no

Min QoD: 70 %

Alterable Task: ☐ yes ☒ no

Auto Delete Reports: ☒ Do not automatically delete reports

☐ Automatically delete oldest reports but always keep newest 5 reports

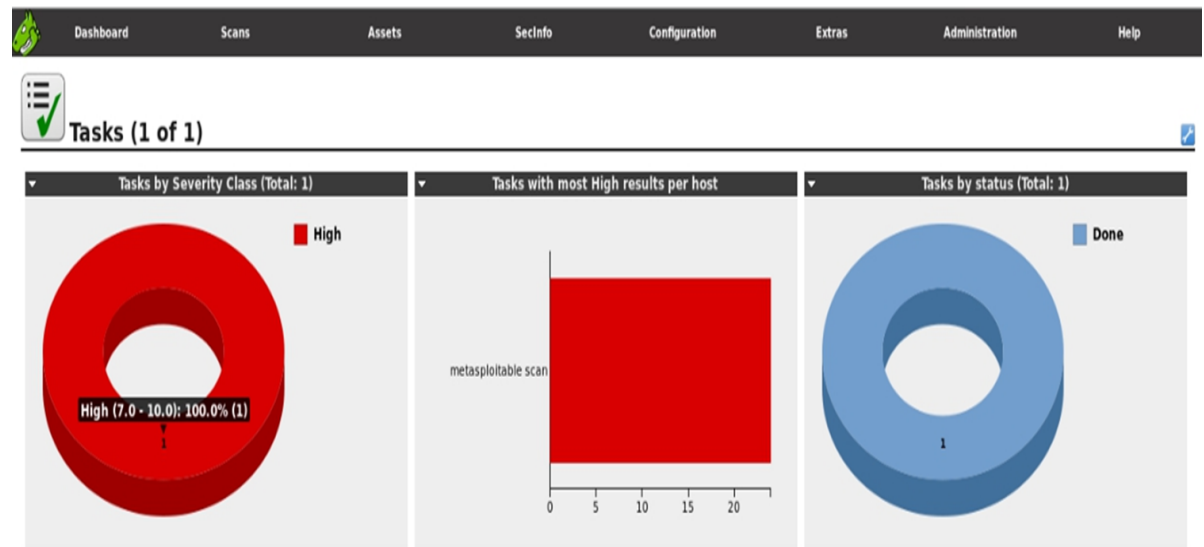
Scanner: OpenVAS Default

Create

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
metasploitable scan	Requested	0 (1)				

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
metasploitable scan	1 %	0 (1)				

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
metasploitable scan	84 %	0 (1)				



Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
metasploitable scan	Done	1 (1)	Oct 20 2017	10.0 (High)		

when finish check the info shown to you

min_qod=70 apply_overrides=1 autofp=0 rows=10 sort-reverse=created first=1



Results (140 of 356)

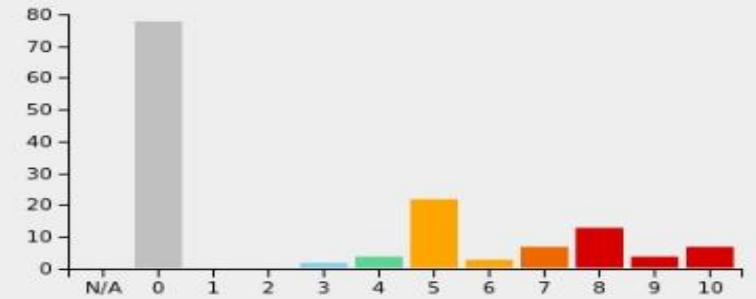
Results by Severity Class (Total: 140)



Results vulnerability word cloud



Results by CVSS (Total: 140)



Vulnerability		Severity	QoD	Host	Location	Created
SSH Brute Force Logins With Default Credentials Reporting		9.0 (High)	95%	192.168.226.129	22/tcp	Fri Oct 20 03:51:12 2017
CPE Inventory		0.0 (Log)	80%	192.168.226.129	general/CPE-T	Fri Oct 20 03:51:12 2017
OS End Of Life Detection		10.0 (High)	80%	192.168.226.129	general/tcp	Fri Oct 20 03:51:12 2017
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	99%	192.168.226.129	6200/tcp	Fri Oct 20 03:50:35 2017
vsftpd Compromised Source Packages Backdoor Vulnerability		7.5 (High)	99%	192.168.226.129	21/tcp	Fri Oct 20 03:50:35 2017
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities		10.0 (High)	99%	192.168.226.129	8787/tcp	Fri Oct 20 03:49:50 2017
Check for Backdoor in UnrealIRCd		7.5 (High)	70%	192.168.226.129	6667/tcp	Fri Oct 20 03:49:49 2017
PostgreSQL weak password		9.0 (High)	99%	192.168.226.129	5432/tcp	Fri Oct 20 03:49:34 2017
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.		7.5 (High)	95%	192.168.226.129	80/tcp	Fri Oct 20 03:49:17 2017
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability		4.3 (Medium)	99%	192.168.226.129	80/tcp	Fri Oct 20 03:49:05 2017


vApply to page contents

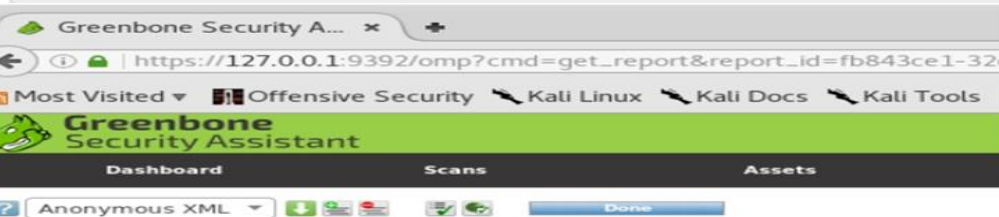
(Applied filter: min_qod=70 apply_overrides=1 autofp=0 rows=10 sort-reverse=created first=1)

when finish click scans results then go to reports and click date

ID: 47dac7d0-4106-4c90-bb09-071ea0b5c054
Created: Fri Oct 20 03:51:12 2017
Modified: Fri Oct 20 03:51:12 2017
Owner: admin

Result: OS End Of Life Detection

Vulnerability	Severity	QoD	Host	Location	Actions
OS End Of Life Detection	10.0 (High)	80%	192.168.226.129	general/tcp	 
Summary OS End Of Life Detection The Operating System on the remote host has reached the end of life and should not be used anymore					
Vulnerability Detection Result The "Ubuntu" Operating System on the remote host has reached the end of life. CPE: cpe:/o:canonical:ubuntu_linux:8.04 Installed version, build or SP: 8.04 EOL date: 2013-05-09 EOL info: https://wiki.ubuntu.com/Releases					
Vulnerability Detection Method Details: OS End Of Life Detection (OID: 1.3.6.1.4.1.25623.1.0.103674) Version used: \$Revision: 7633 \$					



Report: Results (62 of 356)

Vulnerability
Check for rexecd Service
TWiki XSS and Command Execution Vulnerabilities
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability
Possible Backdoor: Ingreslock
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities
OS End Of Life Detection
DistCC Remote Code Execution Vulnerability
VNC Brute Force Login
PostgreSQL weak password
SSH Brute Force Logins With Default Credentials Reporting
DistCC Detection
phpinfo() output accessible
phpMyAdmin Code Injection and XSS Vulnerability

click download by choose green arrow , choose html or pdf format