Information Technology Auditing Report

2020

Assignment Report

P. D. R. P. Gunarathne

Bachelor of Science Special (Honors) In Information Technology
Specialized in Computer Systems and Network Engineering

Department of Computer Systems Engineering

Sri Lanka Institute of Information Technology
Sri Lanka

May 2020

IAA Mid-Assignment
2020

Assignment Report

Pahala Divakarage Ravindu Prabashwara Gunarathne

IT17029728

B.Sc. (Hons) Degree in Information Technology

Specializing in Computer Systems & Network Engineering

Department of Computer Systems Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

May 2020

Declaration

I declare that this is my own work and this report does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Name	Student ID	Signature
P. D. R. P. Gunarathne	IT17029728	

Supervised by: 8/05/2020

…………………………. ……………………..

Dr. Lakmal Rupasinghe Date of Submission

Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

IT - Information Technology

1. INTRODUCTION

The technology is spreading among the individuals and enterprises day by day. Technologies and communication play a major role in the business world. Information systems as an important tool for the organization in business. Information technology audit is examinees the internal control structure in an information system set up. Basically it means inspection of the IT infrastructure, operations and policies. It helpful to suggest improvements. An IT auditor is responsible for IT network. IT include identifying weaknesses in the IT system and responding to any found. They are using Information technology security tools to audit internal network. In this report we take a look a range of IT security auditing tools and how to improve organization IT security network through that tools. There are mapping tools used to identify systems, open ports and services. These can be used to check firewalls. It auditor is responsible for IT audit. He is responsible for analyzing and assessing a company’s technological infrastructure to ensure processes and systems run accurately and efficiently, An IT auditor also identifies any IT issues, related to security and risk management. IT auditors are responsible for communicating their findings to others in the organization. He is responsible for offering solutions to improve systems and also ensure security and compliance.

2. AUDITING TOOLS

There are many vulnerability assessment tools. They are belongs to two types. Commercial type and open source tools. This types of tools provide a severity categorization and output for reports.

2.1 Comparison of commercial and open source tools

Table 2.1-1: Comparison of commercial and open source tool

Commercial	Open Source
Nessus Professional (vulnerability assessment tool)	W3af (web application scanner)
ManageEngine AdAudit Plus(real-time auditing)	SQLMap (penetration testing tool)
Acunetix (network security auditing tool)	OpenVAS (servers and network devices) Nikto
Netwrix Auditor (network security auditing tool)	Nikto (web server scanner)

Figure 2.1-1: OpenVMS [1].

3. PROCESS OF WEBSITE AUDITING USING W3AF TOOL.

3.1 What is W3af tool?

W3af is a Web Application Attack and Audit Framework [2]. By using this tool, we can identify more than 200 kinds of web application vulnerabilities including SQL injection, Cross-Site Scripting and many others.

It comes with a graphical and console interface. You can use it easily. Because it's easy to understand interface.

3.2 Installing the W3af tool

Prerequisites

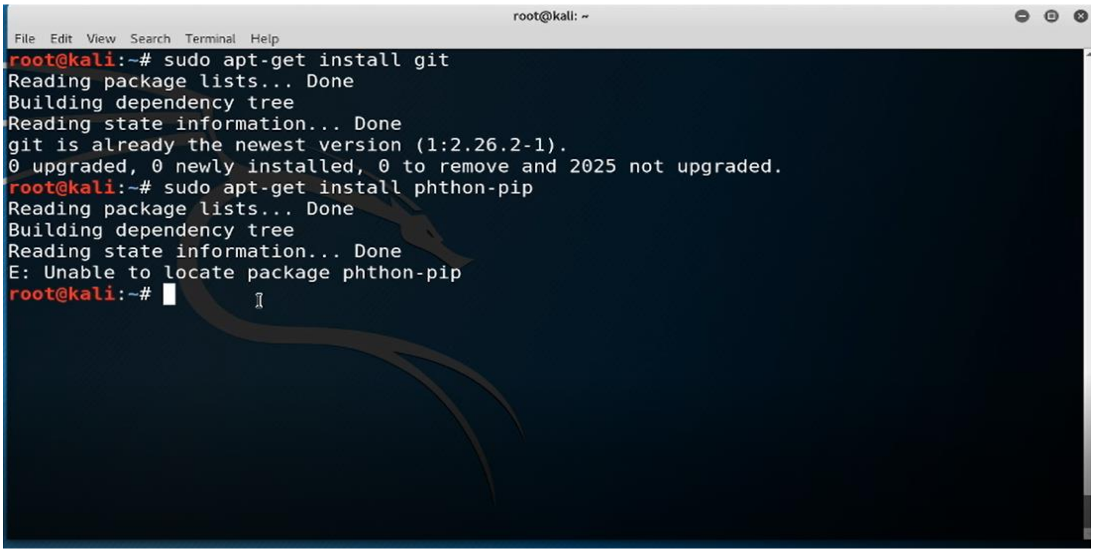
Before install the W3af tool we have to check the following software's are installed to our main Linux machine.

- Git client
- Python 2.7
- Pip version 1.1

If not we can use the bellow commands to install that software's.

1. Git client: sudo apt-get install git
2. Python 2.7, which is installed by default in most systems
3. Pip version 1.1: sudo apt-get install python-pip

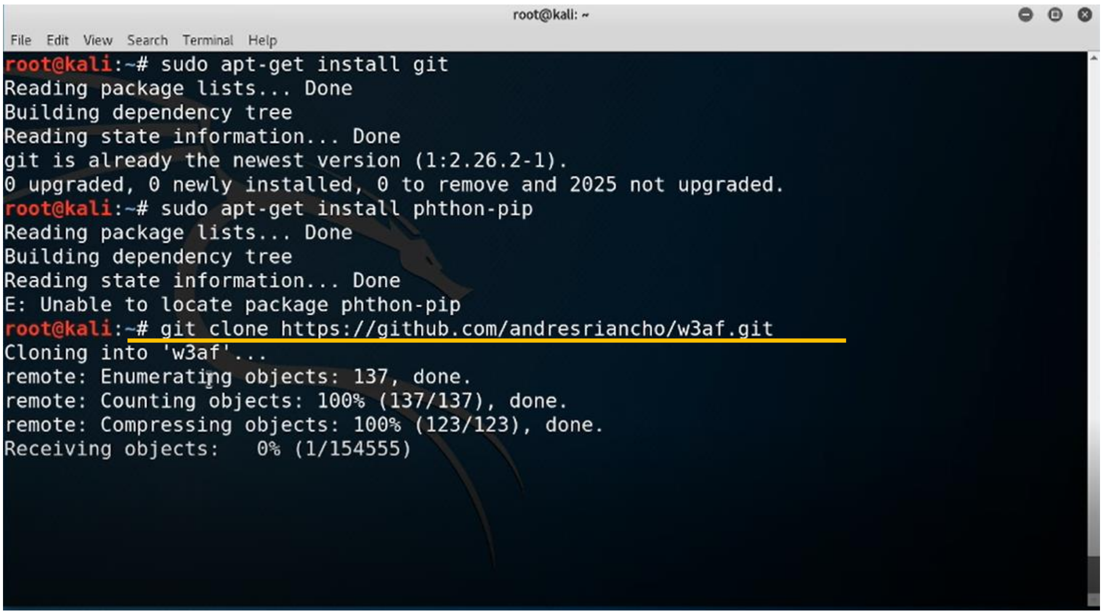
I have already installed to my Linux matching before.



```
root@kali:~# sudo apt-get install git
Reading package lists... Done
Building dependency tree
Reading state information... Done
git is already the newest version (1:2.26.2-1).
0 upgraded, 0 newly installed, 0 to remove and 2025 not upgraded.
root@kali:~# sudo apt-get install phthon-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package phthon-pip
root@kali:~#
```

Figure 3.2-1: Installing Prerequisites

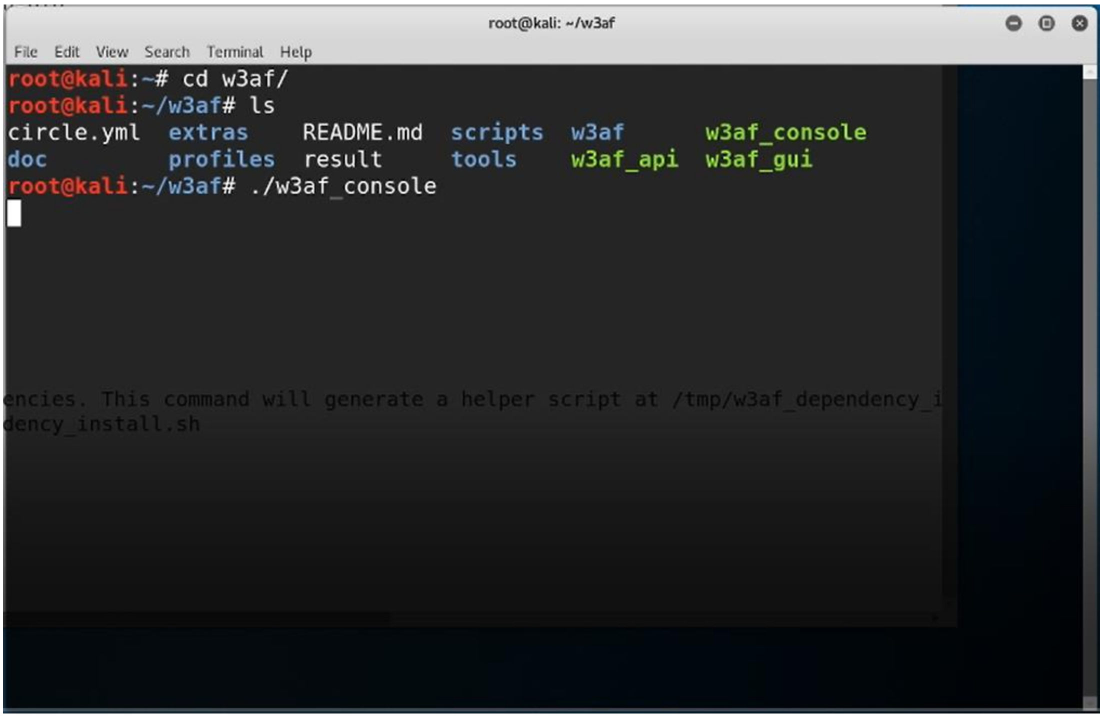
- Then we use git to download source code.



```
root@kali:~# sudo apt-get install git
Reading package lists... Done
Building dependency tree
Reading state information... Done
git is already the newest version (1:2.26.2-1).
0 upgraded, 0 newly installed, 0 to remove and 2025 not upgraded.
root@kali:~# sudo apt-get install phthon-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package phthon-pip
root@kali:~# git clone https://github.com/andresriancho/w3af.git
Cloning into 'w3af'...
remote: Enumerating objects: 137, done.
remote: Counting objects: 100% (137/137), done.
remote: Compressing objects: 100% (123/123), done.
Receiving objects:   0% (1/154555)
```

Figure 3.2-2: Downloading Source Code

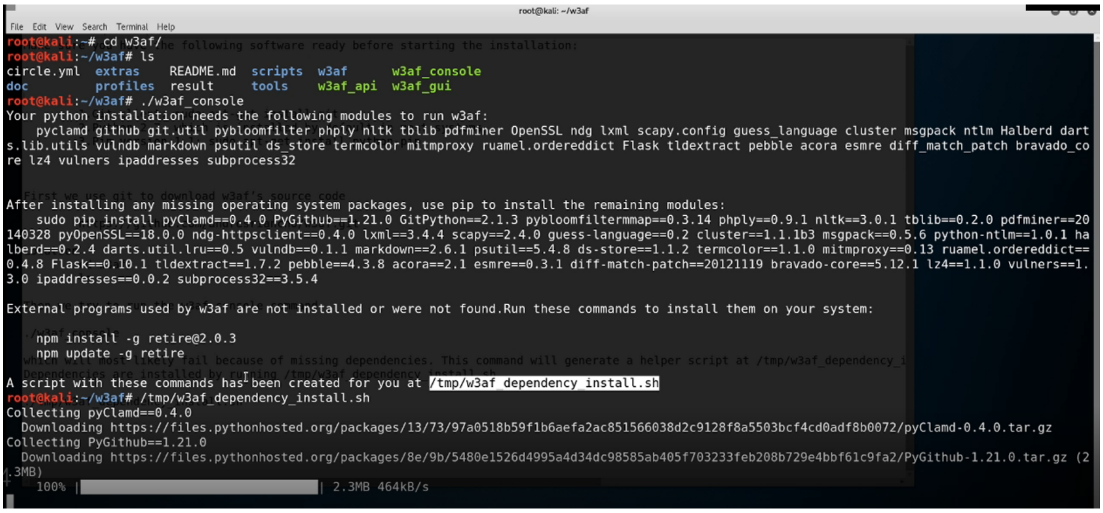
- Then we move to location where we install W3af tool and try to run the w3af_console.We use commands “cd w3af/” “./w3af_console”.



```
root@kali:~# cd w3af/
root@kali:~/w3af# ls
circle.yml  extras    README.md  scripts  w3af      w3af_console
doc         profiles  result     tools    w3af_api  w3af_gui
root@kali:~/w3af# ./w3af_console

encies. This command will generate a helper script at /tmp/w3af_dependency_i
dency_install.sh
```

Figure 3.2-3: Running Console

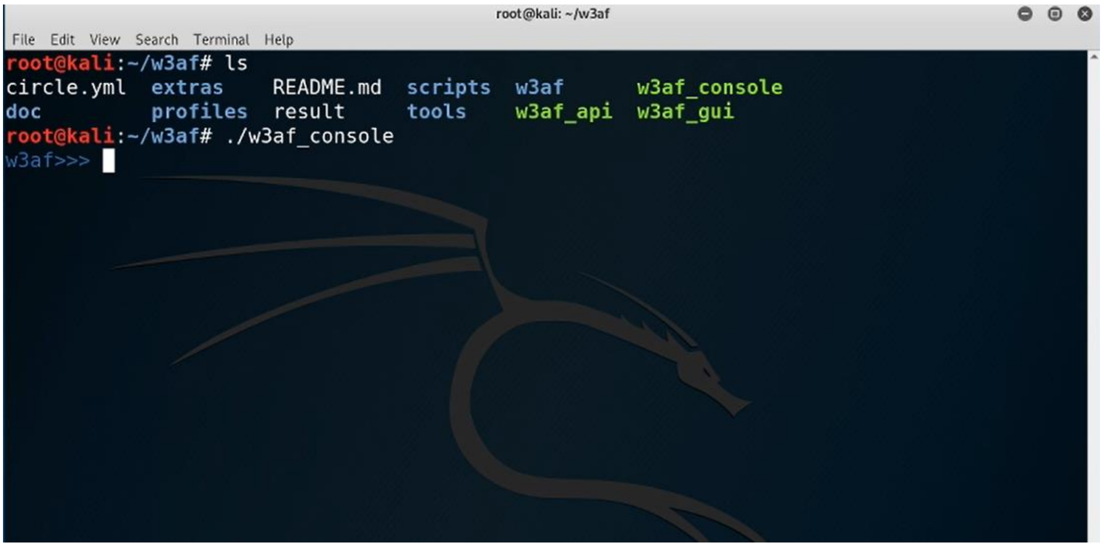
We can install dependencies by running "/tmp/w3af_dependency_install.sh" command.



```
root@kali:~# cd w3af/
root@kali:~/w3af# ls
circle.yml  extras    README.md  scripts  w3af      w3af_console
doc         profiles  result     tools    w3af_api  w3af_gui
root@kali:~/w3af# ./w3af_console
Your python installation needs the following modules to run w3af:
    pyclamd github git.util pybloomfilter phply nltk tblib pdfminer OpenSSL ndg lxml scapy.config guess_language cluster msgpack ntlm Halberd dart
s.lib.utils vulndb markdown psutil ds_store termcolor mitmproxy ruamel.ordereddict Flask tldextract pebble acora esmre diff_match_patch bravado_co
re lz4 vulners ipaddresses subprocess32


After installing any missing operating system packages, use pip to install the remaining modules:
    sudo pip install pyClamd==0.4.0 PyGithub==1.21.0 GitPython==2.1.3 pybloomfiltermmap==0.3.14 phply==0.9.1 nltk==3.0.1 tblib==0.2.0 pdfminer==20
140328 pyOpenSSL==18.0.0 ndg-httpsclient==0.4.0 lxml==3.4.4 scapy==2.4.0 guess-language==0.2 cluster==1.1.1b3 msgpack==0.5.6 python-ntlm==1.0.1 ha
lberd==0.2.4 darts.util.lru==0.5 vulndb==0.1.1 markdown==2.6.1 psutil==5.4.8 ds-store==1.1.2 termcolor==1.1.0 mitmproxy==0.13 ruamel.ordereddict==
0.4.8 Flask==0.10.1 tldextract==1.7.2 pebble==4.3.8 acora==2.1 esmre==0.3.1 diff-match-patch==20121119 bravado-core==5.12.1 lz4==1.1.0 vulners==1.
3.0 ipaddresses==0.0.2 subprocess32==3.5.4

External programs used by w3af are not installed or were not found.Run these commands to install them on your system:

    npm install -g retire@2.0.3
    npm update -g retire

A script with these commands has been created for you at /tmp/w3af_dependency_install.sh
root@kali:~/w3af# /tmp/w3af_dependency_install.sh
Collecting pyClamd==0.4.0
  Downloading https://files.pythonhosted.org/packages/13/73/97a0518b59f1b6aefa2ac851566038d2c9128f8a5503bcf4cd0adf8b0072/pyClamd-0.4.0.tar.gz
Collecting PyGithub==1.21.0
  Downloading https://files.pythonhosted.org/packages/8e/9b/5480e1526d4995a4d34dc98585ab405f703233feb208b729e4bbf61c9fa2/PyGithub-1.21.0.tar.gz (2
.3MB)
    100% |████████████████████████████████| 2.3MB 464kB/s
```

Figure 3.2-4: Installing Dependencies

- Running the console again and go to W3af prompt.

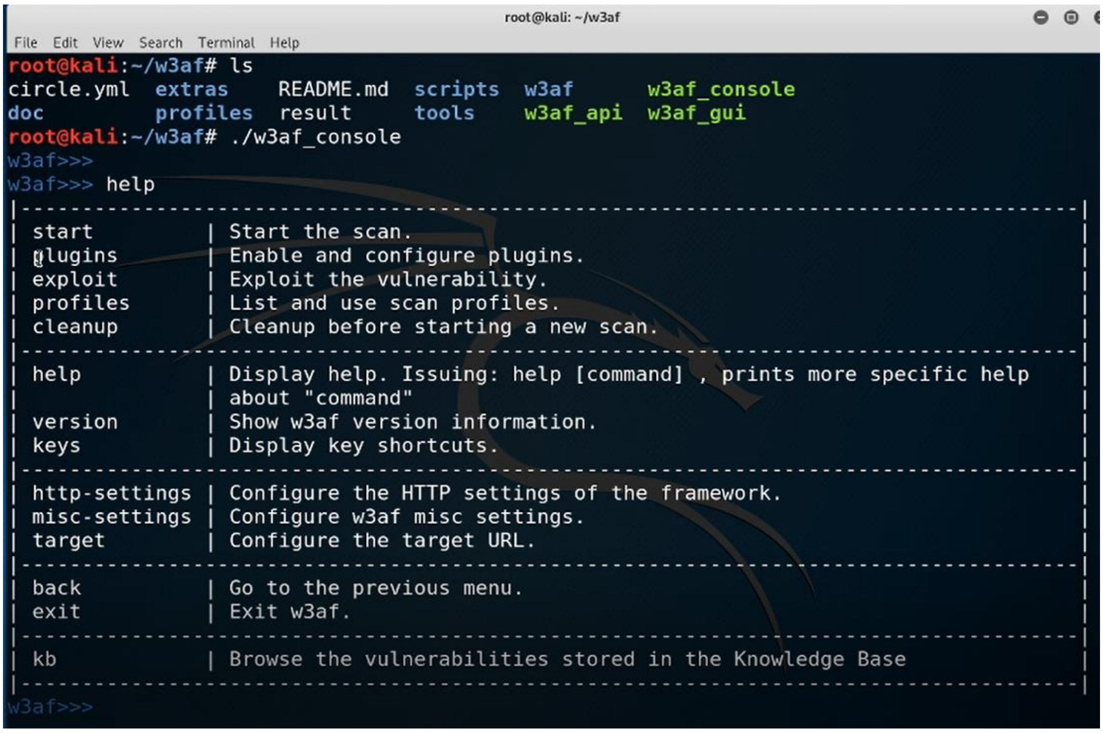


```
root@kali:~/w3af# ls
circle.yml  extras    README.md  scripts  w3af      w3af_console
doc         profiles  result     tools    w3af_api  w3af_gui
root@kali:~/w3af# ./w3af_console
w3af>>> 
```

Figure 3.2-5: W3af Prompt

3.3 Using the W3af tool for Web Page vulnerability scanning.

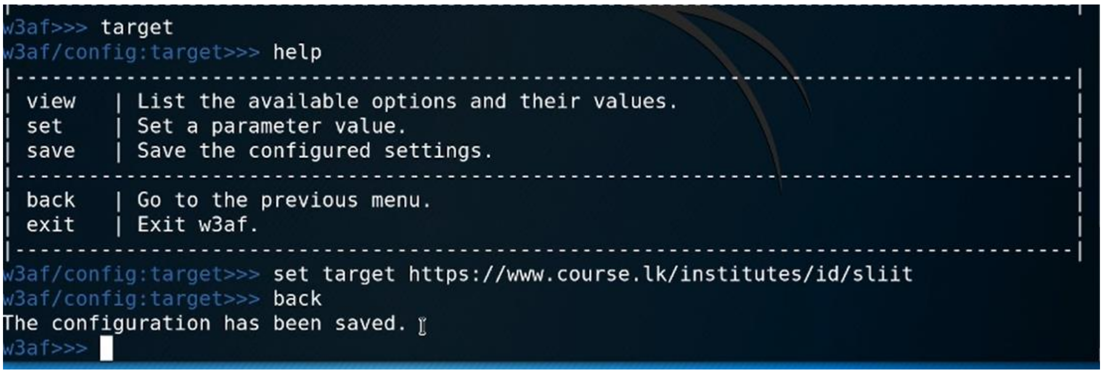
- Understanding the tool and the commands by using “help” command.



```
root@kali:~/w3af# ls
circle.yml  extras    README.md  scripts  w3af      w3af_console
doc         profiles  result     tools    w3af_api  w3af_gui
root@kali:~/w3af# ./w3af_console
w3af>>>
w3af>>> help
|----------------------------------------------------------------------------------|
| start         | Start the scan.                                                  |
| plugins       | Enable and configure plugins.                                    |
| exploit       | Exploit the vulnerability.                                       |
| profiles      | List and use scan profiles.                                      |
| cleanup       | Cleanup before starting a new scan.                              |
|----------------------------------------------------------------------------------|
| help          | Display help. Issuing: help [command] , prints more specific help |
|               | about "command"                                                  |
| version       | Show w3af version information.                                    |
| keys          | Display key shortcuts.                                           |
|----------------------------------------------------------------------------------|
| http-settings | Configure the HTTP settings of the framework.                    |
| misc-settings | Configure w3af misc settings.                                    |
| target        | Configure the target URL.                                        |
|----------------------------------------------------------------------------------|
| back          | Go to the previous menu.                                         |
| exit          | Exit w3af.                                                       |
|----------------------------------------------------------------------------------|
| kb            | Browse the vulnerabilities stored in the Knowledge Base          |
|----------------------------------------------------------------------------------|
w3af>>>
```

Figure 3.3-1: Help

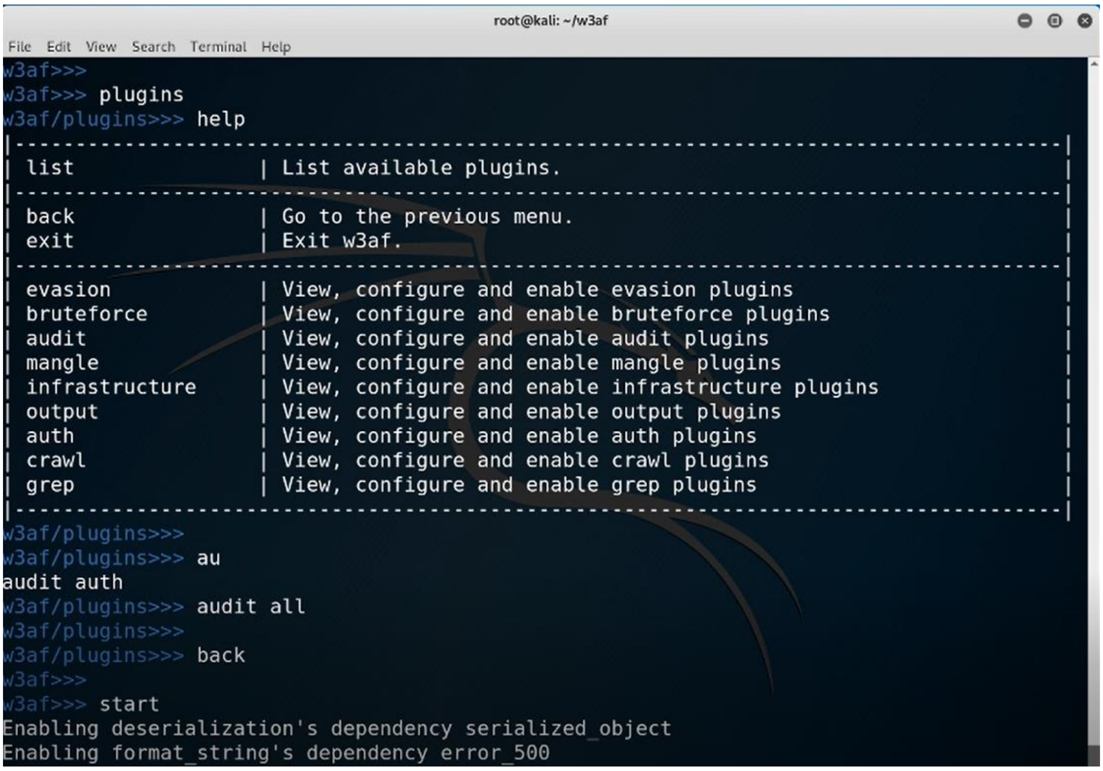
- Using a target command to set a URL target.
- We can use “set target https://www.sliitacademy.lk/” to set a target.
- After that we have to type “back” command and save the target.



```
w3af>>> target
w3af/config:target>>> help
|------------------------------------------------------------------------------------|
| view    | List the available options and their values.                             |
| set     | Set a parameter value.                                                   |
| save    | Save the configured settings.                                            |
|------------------------------------------------------------------------------------|
| back    | Go to the previous menu.                                                 |
| exit    | Exit w3af.                                                               |
|------------------------------------------------------------------------------------|
w3af/config:target>>> set target https://www.course.lk/institutes/id/sliit
w3af/config:target>>> back
The configuration has been saved.
w3af>>>
```

Figure 3.3-2:Setting Up the Target URL

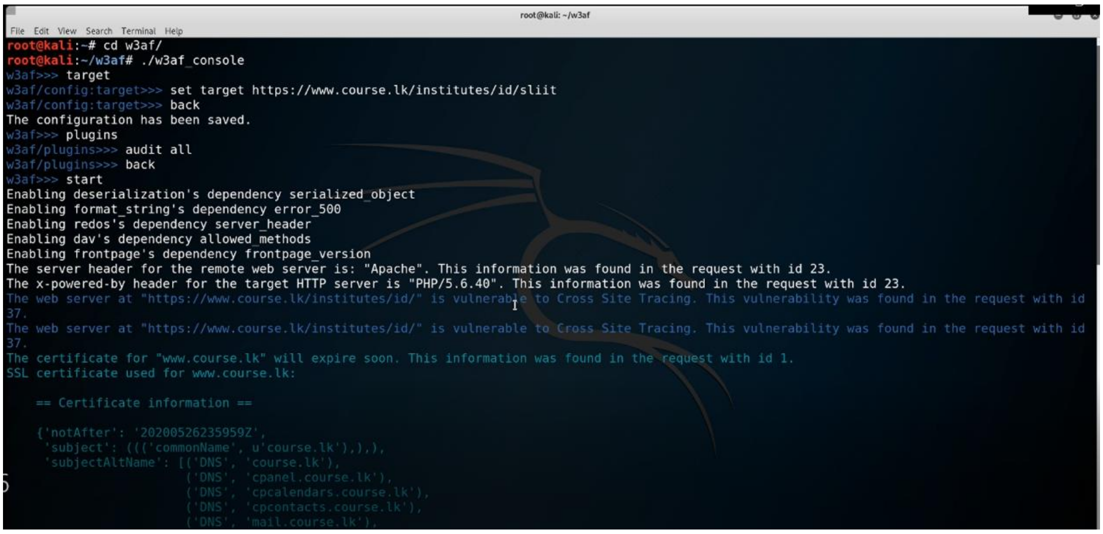
- Save and we use “plugins” command to make suitable plugins we want.
- After that we can start the vulnerability scanning by using “start” command.



```
w3af>>>
w3af>>> plugins
w3af/plugins>>> help
|------------------------------------------------------------------------------------|
| list                   | List available plugins.                                   |
|------------------------------------------------------------------------------------|
| back                   | Go to the previous menu.                                  |
| exit                   | Exit w3af.                                                |
|------------------------------------------------------------------------------------|
| evasion                | View, configure and enable evasion plugins                |
| bruteforce             | View, configure and enable bruteforce plugins             |
| audit                  | View, configure and enable audit plugins                  |
| mangle                 | View, configure and enable mangle plugins                 |
| infrastructure         | View, configure and enable infrastructure plugins         |
| output                 | View, configure and enable output plugins                 |
| auth                   | View, configure and enable auth plugins                   |
| crawl                  | View, configure and enable crawl plugins                  |
| grep                   | View, configure and enable grep plugins                   |
|------------------------------------------------------------------------------------|
w3af/plugins>>>
w3af/plugins>>> au
audit auth
w3af/plugins>>> audit all
w3af/plugins>>>
w3af/plugins>>> back
w3af>>>
w3af>>> start
Enabling deserialization's dependency serialized_object
Enabling format_string's dependency error_500
```

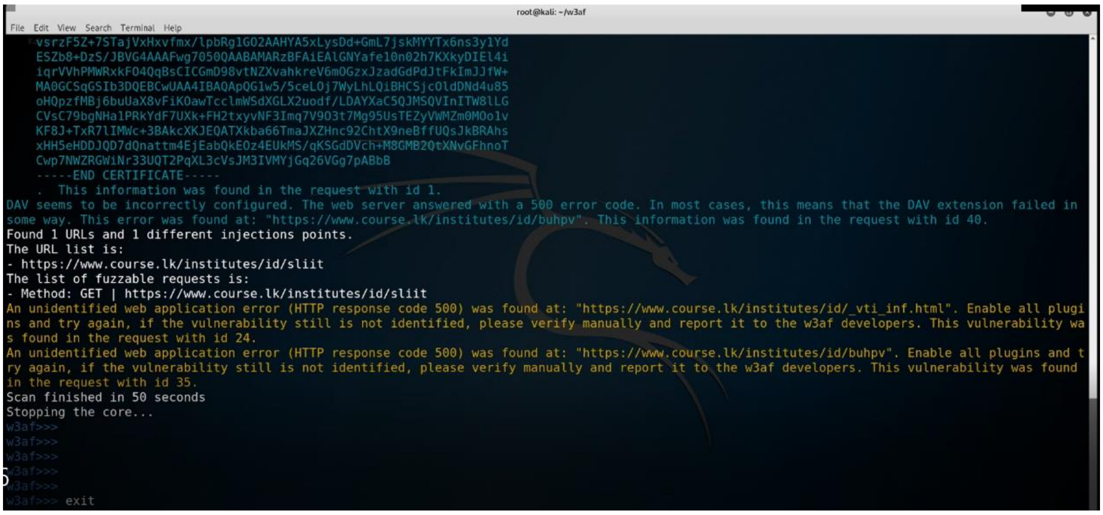
Figure 3.3-3: Start the Scan

- Vulnerability scanning report.
- We can see the blue color lines and many more information.
- They are the vulnerabilities we found using this web URL.



```
root@kali:~# cd w3af/
root@kali:~/w3af# ./w3af_console
w3af>>> target
w3af/config:target>>> set target https://www.course.lk/institutes/id/sliit
w3af/config:target>>> back
The configuration has been saved.
w3af>>> plugins
w3af/plugins>>> audit all
w3af/plugins>>> back
w3af>>> start
Enabling deserialization's dependency serialized_object
Enabling format_string's dependency error_500
Enabling redos's dependency server_header
Enabling dav's dependency allowed_methods
Enabling frontpage's dependency frontpage_version
The server header for the remote web server is: "Apache". This information was found in the request with id 23.
The x-powered-by header for the target HTTP server is "PHP/5.6.40". This information was found in the request with id 23.
The web server at "https://www.course.lk/institutes/id/" is vulnerable to Cross Site Tracing. This vulnerability was found in the request with id
37.
The web server at "https://www.course.lk/institutes/id/" is vulnerable to Cross Site Tracing. This vulnerability was found in the request with id
37.
The certificate for "www.course.lk" will expire soon. This information was found in the request with id 1.
SSL certificate used for www.course.lk:

    == Certificate information ==

    {'notAfter': '20200526235959Z',
     'subject': ((('commonName', u'course.lk'),),),
     'subjectAltName': [('DNS', 'course.lk'),
                        ('DNS', 'cpanel.course.lk'),
                        ('DNS', 'cpcalendars.course.lk'),
                        ('DNS', 'cpcontacts.course.lk'),
                        ('DNS', 'mail.course.lk'),
```

Figure 3.3-4:Vulnerability Report



```
    vsrzF5Z+7STajVxHxvfmx/lpbRg1GO2AAHYA5xLysDd+GmL7jskMYYTx6ns3y1Yd
    ESZb8+DzS/JBVG4AAAFwg7050QAABAMARzBFAiEAlGNYafe10n02h7KXkyDIEl4i
    iqrVVhPMWRxkF04QqBsCICGmD98vtNZXvahkreV6m0GzxJzadGdPdJtFkImJJfW+
    MA0GCSqGSIb3DQEBCwUAA4IBAQApQG1w5/5ceL0j7WyLhLQiBHCSjc0ldDNd4u85
    oHQpzfMBj6buUaX8vFiKOawTcclmWSdXGLX2uodf/LDAYXaC5QJMSQVInITW8lLG
    CVsC79bgNHa1PRkYdF7UXk+FH2txyvNF3Imq7V903t7Mg95UsTEZyVWMZm0MOo1v
    KF8J+TxR7lIMWc+3BAkcXKJEQATXkba66TmaJXZHnc92ChtX9neBffUQsJkBRAhs
    xHH5eHDDJQD7dQnattm4EjEabQkEOz4EUkMS/qKSGdDVch+M8GMB2QtXNvGFhnoT
    Cwp7NWZRGWiNr33UQT2PqXL3cVsJM3IVMYjGq26VGg7pABbB
    -----END CERTIFICATE-----
    .  This information was found in the request with id 1.
DAV seems to be incorrectly configured. The web server answered with a 500 error code. In most cases, this means that the DAV extension failed in
some way. This error was found at: "https://www.course.lk/institutes/id/buhpv". This information was found in the request with id 40.
Found 1 URLs and 1 different injections points.
The URL list is:
- https://www.course.lk/institutes/id/sliit
The list of fuzzable requests is:
- Method: GET | https://www.course.lk/institutes/id/sliit
An unidentified web application error (HTTP response code 500) was found at: "https://www.course.lk/institutes/id/_vti_inf.html". Enable all plugi
ns and try again, if the vulnerability still is not identified, please verify manually and report it to the w3af developers. This vulnerability wa
s found in the request with id 24.
An unidentified web application error (HTTP response code 500) was found at: "https://www.course.lk/institutes/id/buhpv". Enable all plugins and t
ry again, if the vulnerability still is not identified, please verify manually and report it to the w3af developers. This vulnerability was found
in the request with id 35.
Scan finished in 50 seconds
Stopping the core...
w3af>>>
w3af>>>
w3af>>>
w3af>>>
w3af>>>
w3af>>> exit
```

Figure 3.3-5: Vulnerability Report

4. VULNERABILITY SCANNING METASPLOIT VIRTUAL MACHINE USING OPENVAS SCANNING TOOL.

4.1 What is OpenVAS tool?

OpenVAS - Open Vulnerability Assessment Scanner. OpenVAS is an open-source vulnerability scanning software aimed at Linux environments that offers authenticated and unauthenticated testing [3]. OpenVAS is constantly updated to detect the latest vulnerabilities with the Greenbone Network Vulnerability Tests public feed, which includes over 50,000 different vulnerabilities [3].

4.2 Using OpenVAS Vulnerability Scanner.

- Setup the GCE

  Now we have to go to the bellow link and download the OpenVAS iso file.

  Download: https://dl.greenbone.net/download/VM/gsm-ce-6.0.7.iso
- Create new virtual machining using VirtualBox.
- OpenVas dashboard. (We can log in to it by using OpenVas IP address)

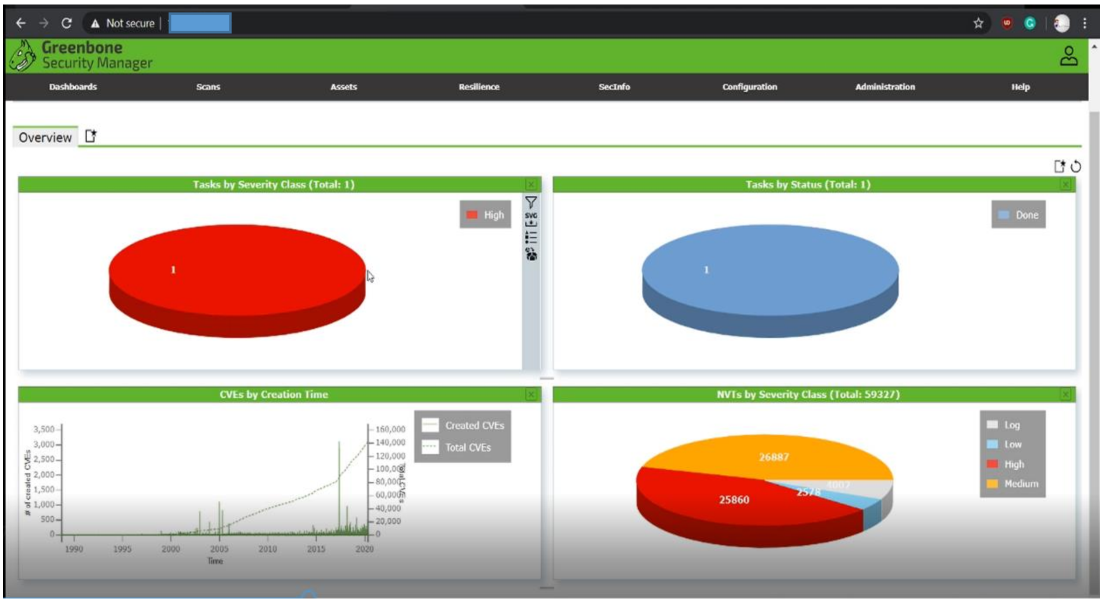
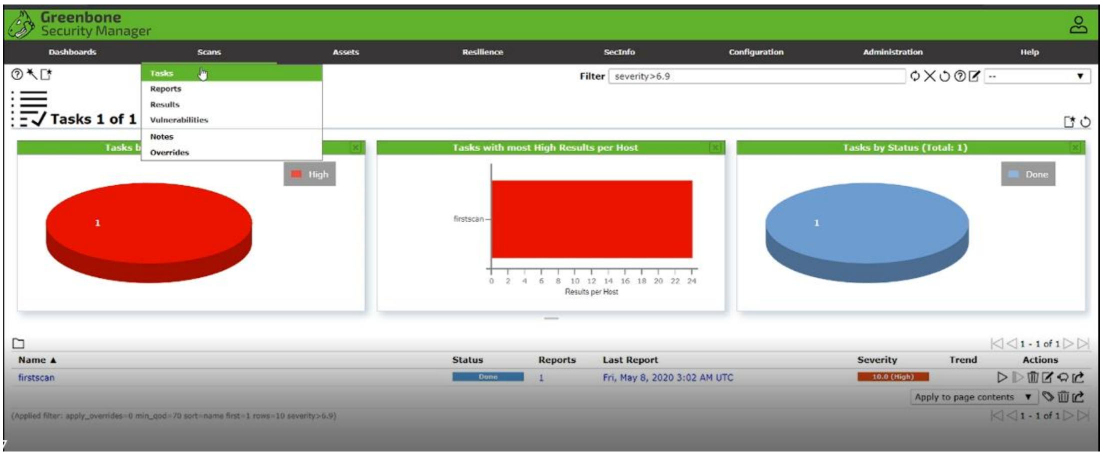


Figure 4.2-1:Dashboard

- To start a new scan we have to select the "Scan" tab and then we have to choose the "task" and hit enter.



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
firstscan	Done	1	Fri, May 8, 2020 3:02 AM UTC	10.0 (High)		

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10 severity>6.9)

Figure 4.2-2: New Task

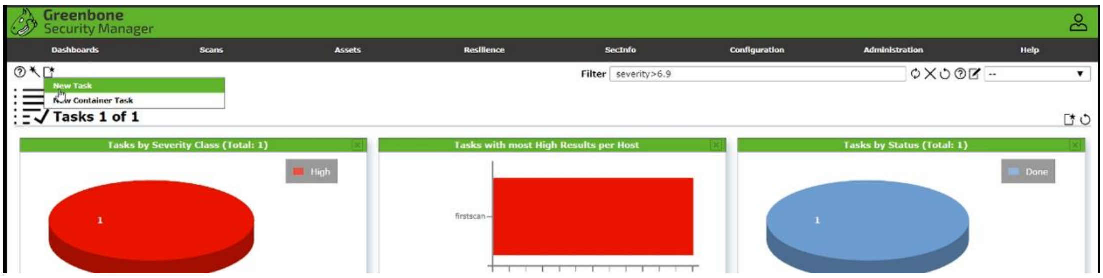
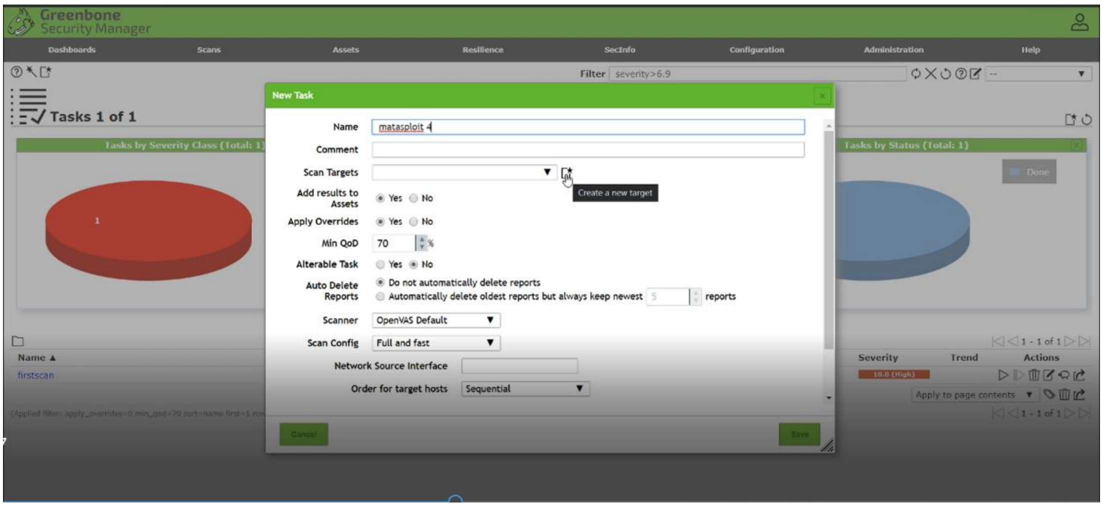


Figure 4.2-3: Select the New Task

- Now we can see the New Task window and in there we have to give the suitable name for our scan and we have to create the new target.



Name: matasploit 4

Comment:

Scan Targets:

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

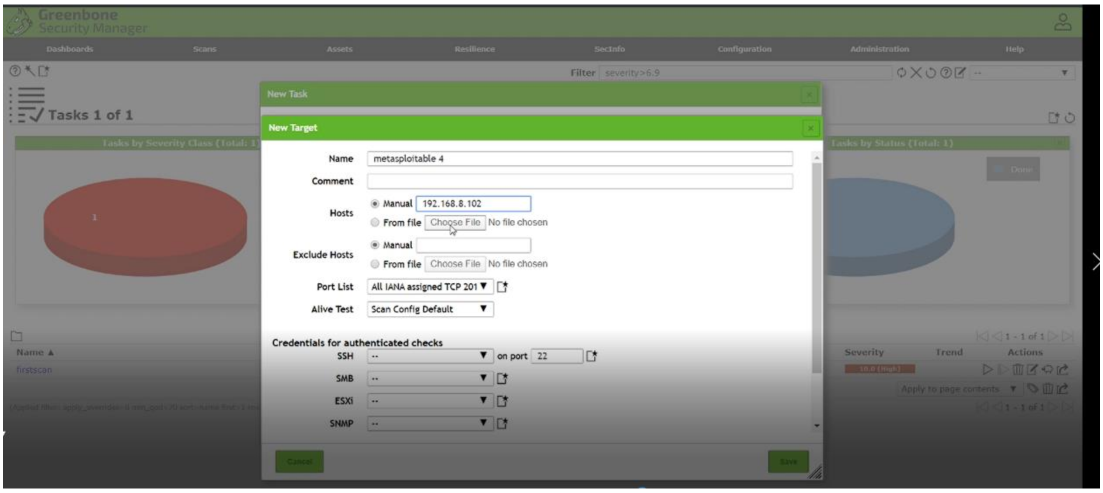
Scan Config: Full and fast

Network Source Interface:

Order for target hosts: Sequential

Figure 4.2-4: New Task Window

- In new target we have to give the suitable name for the new target and we have to give the IP address of our metasploit machine as the host.



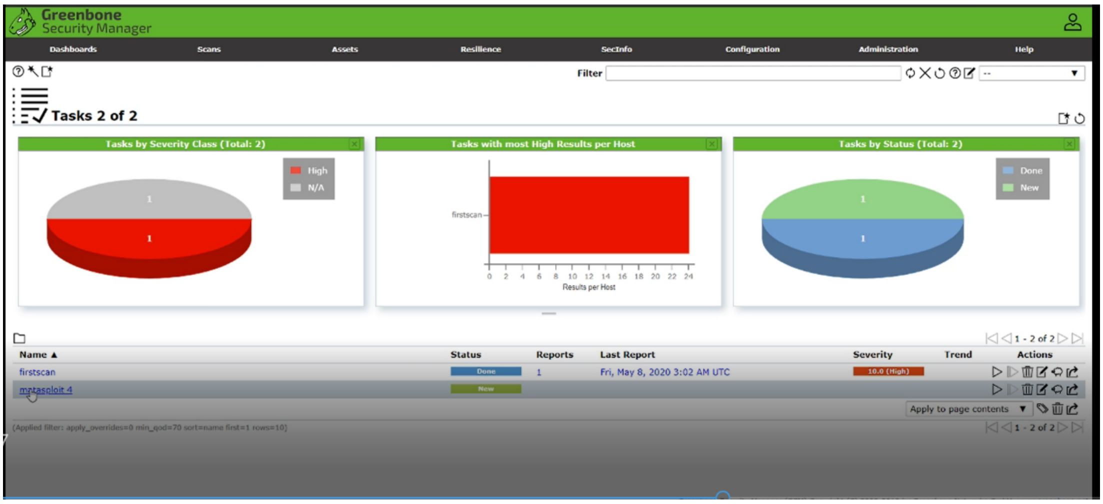
Name	metasploitable 4
Comment	
Hosts	● Manual 192.168.8.102 ○ From file Choose File No file chosen
Exclude Hosts	● Manual ○ From file Choose File No file chosen
Port List	All IANA assigned TCP 201 ▼
Alive Test	Scan Config Default ▼

Credentials for authenticated checks

SSH	-- ▼ on port 22
SMB	-- ▼
ESXi	-- ▼
SNMP	-- ▼

Figure 4.2-5: New Target

- Then we can save the details and we can see the new scan in our dashboard under the name tab.

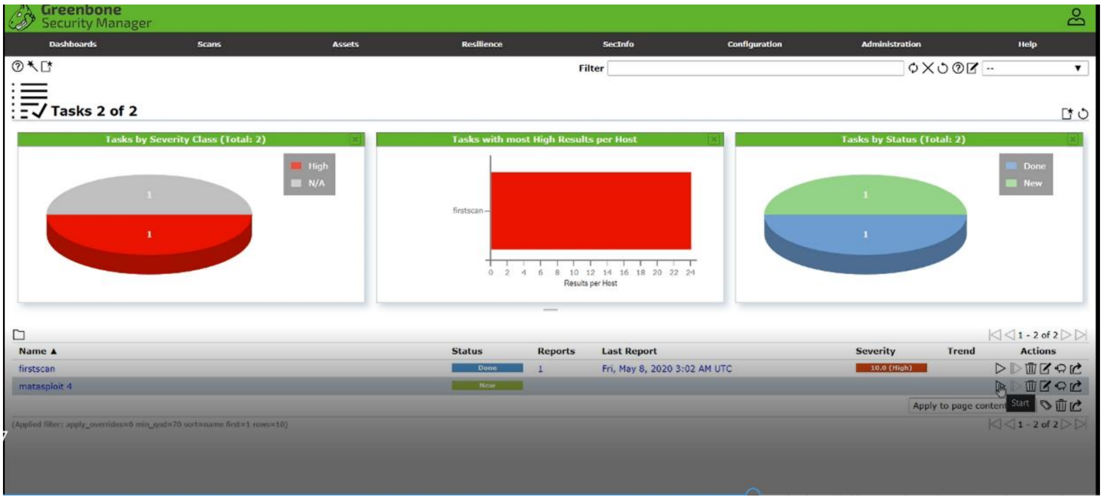


Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
firstscan	Done	1	Fri, May 8, 2020 3:02 AM UTC	10.0 (High)		
metasploit 4	New					

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Figure 4.2-6: Newly Created Scan

- We can start the scan by clicking “Start” button.

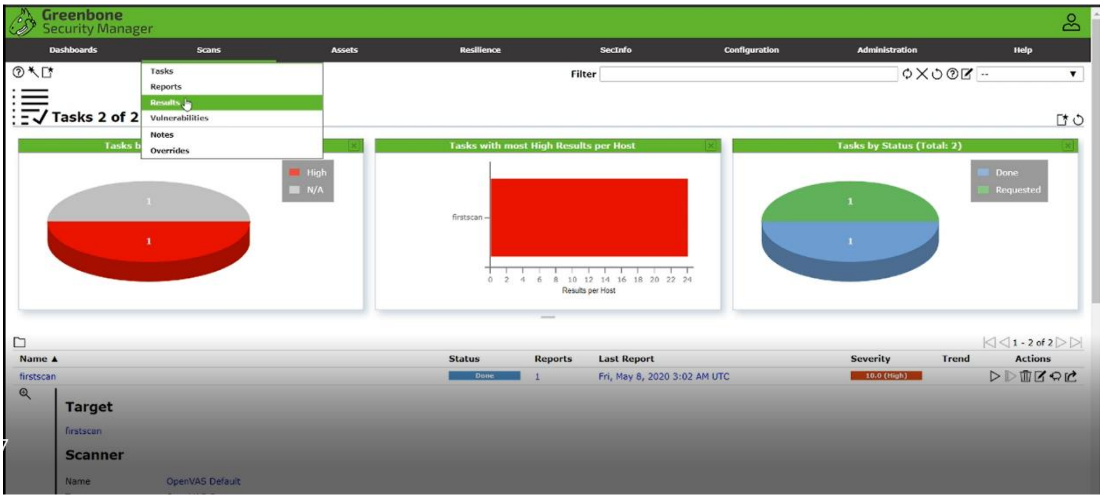


Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
firstscan	Done	1	Fri, May 8, 2020 3:02 AM UTC	10.0 (High)		
matasploit 4	New					

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Figure 4.2-7: Start the Vulnerability Scan

- After the scan finish we can see the result by going to Scan tab and then click the “result” button.



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
firstscan	Done	1	Fri, May 8, 2020 3:02 AM UTC	10.0 (High)		

Target

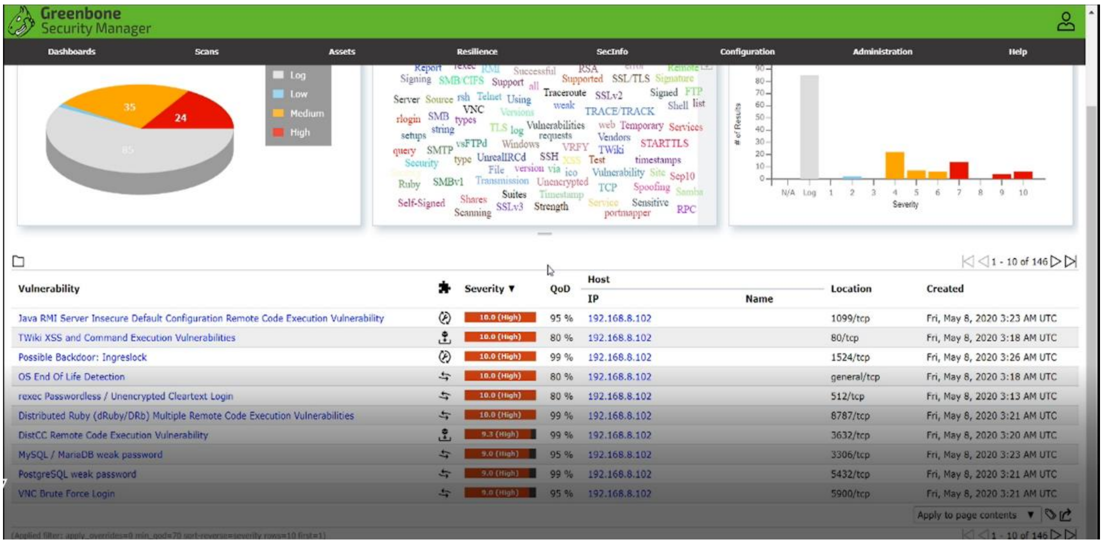
firstscan

Scanner

Name OpenVAS Default

Figure 4.2-8: Viewing the Result

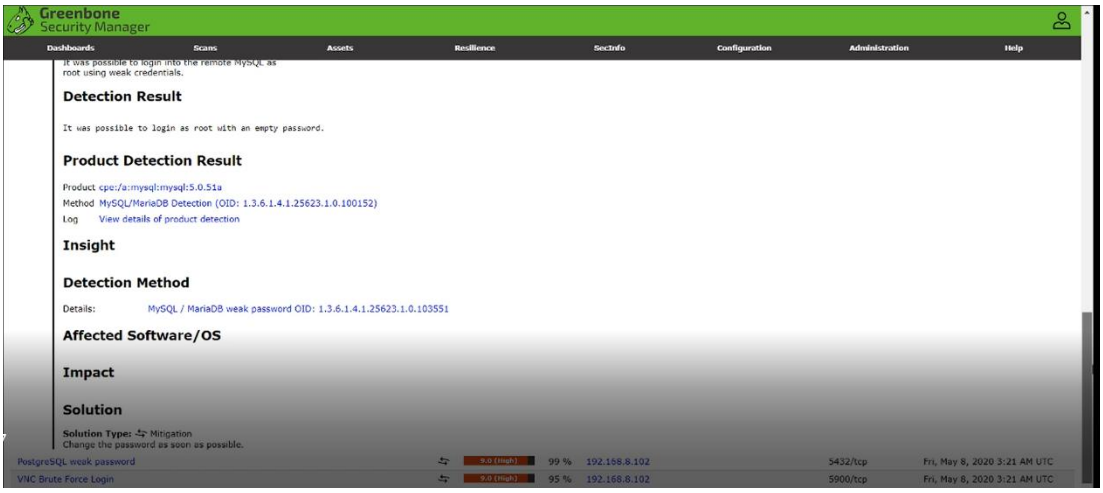
- Vulnerability report



Vulnerability		Severity ▼	QoD	Host IP	Host Name	Location	Created
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability		10.0 (High)	95 %	192.168.8.102		1099/tcp	Fri, May 8, 2020 3:23 AM UTC
TWiki XSS and Command Execution Vulnerabilities		10.0 (High)	80 %	192.168.8.102		80/tcp	Fri, May 8, 2020 3:18 AM UTC
Possible Backdoor: Ingreslock		10.0 (High)	99 %	192.168.8.102		1524/tcp	Fri, May 8, 2020 3:26 AM UTC
OS End Of Life Detection		10.0 (High)	80 %	192.168.8.102		general/tcp	Fri, May 8, 2020 3:18 AM UTC
rexec Passwordless / Unencrypted Cleartext Login		10.0 (High)	80 %	192.168.8.102		512/tcp	Fri, May 8, 2020 3:13 AM UTC
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities		10.0 (High)	99 %	192.168.8.102		8787/tcp	Fri, May 8, 2020 3:21 AM UTC
DistCC Remote Code Execution Vulnerability		9.3 (High)	99 %	192.168.8.102		3632/tcp	Fri, May 8, 2020 3:20 AM UTC
MySQL / MariaDB weak password		9.0 (High)	95 %	192.168.8.102		3306/tcp	Fri, May 8, 2020 3:23 AM UTC
PostgreSQL weak password		9.0 (High)	99 %	192.168.8.102		5432/tcp	Fri, May 8, 2020 3:21 AM UTC
VNC Brute Force Login		9.0 (High)	95 %	192.168.8.102		5900/tcp	Fri, May 8, 2020 3:21 AM UTC

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

- It generate a full report of vulnerability and we can see the information like summary, detection result, impact to our system and how to mitigate the vulnerability.



It was possible to login into the remote MySQL as root using weak credentials.

Detection Result

It was possible to login as root with an empty password.

Product Detection Result

Product cpe:/a:mysql:mysql:5.0.51a
Method MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)
Log View details of product detection

Insight

Detection Method

Details: MySQL / MariaDB weak password OID: 1.3.6.1.4.1.25623.1.0.103551

Affected Software/OS

Impact

Solution

Solution Type: Mitigation
Change the password as soon as possible.

PostgreSQL weak password		9.0 (High)	99 %	192.168.8.102	5432/tcp	Fri, May 8, 2020 3:21 AM UTC
VNC Brute Force Login		9.0 (High)	95 %	192.168.8.102	5900/tcp	Fri, May 8, 2020 3:21 AM UTC

Figure 4.2-9: Information and Solution

5. IEEE REFERENCING

[1] "Green Leaf Background - Unlimited Download. cleanpng.com.," [Online]. Available: https://www.cleanpng.com/png-openvas-vulnerability-management-installation-comp-3123117/download-png.html.

[2] "Open Source Web Application Security Scanner," [Online]. Available: http://w3af.org/. [Accessed 20 Aprial 2020].

[3] "11 Best Network Security Auditing Tools - Full reviews with Free Trial Links," 27 April 2020. [Online]. Available: https://www.comparitech.com/net-admin/network-security-auditing-tools/. [Accessed 5 May 2020].