VULNERABILITY ASSESMENT AND PENETRATION TESTING

By

Tanmoy Paul

ID: 181-15-10935

This Report Presented in Partial Fulfilment of the Requirements for the Degree of Bachelor of Computer science and Engineering (BSc in CSE).

Supervised By

Mr. Gazi Zahirul Islam

Assistant Professor

Department of CSE

Daffodil International University

Co-Supervised By

Md. Abbas Ali Khan

Lecturer

Department of CSE

Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

Dhaka, Bangladesh

4th January 2022

APPROVAL

This Project titled VULNERABILITY ASSESMENT AND PENETRATION TESTING submitted by Mr. Gazi Zahirul Islam and Md. Abbas Ali Khan to the department of computer science and engineering, Daffodil International University has been accepted as satisfactory for the partial fulfilment to the requirement for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 4th January 2022

BOARD OF EXAMINERS

______________________ **Chairman**

Dr. Md. Ismail Jabiullah

Professor

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Daffodil International University

Nzmoon **Internal Examiner**

____

Nazmun Nessa Moon (NNM)

Assistant Professor

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Daffodil International University

Aniruddha Rakshit

Internal Examiner

Aniruddha Rakshit (AR)

Senior Lecturer

Department of Computer Science and Engineering

Faculty of Science & Information Technology

Daffodil Interational University

External Examiner

Dr. Md Arshad Ali

Associate Professor

Department of Computer Science and Engineering

Hajee Mohammad Danesh Science and Technology University

DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Mr. Gazi Zahirul Islam, Assistant Professor Department of CSE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

Zahir

Mr. GaziZahirul Islam
Assistant Professor
Department of CSE
Daffodil International University

Submitted by:

Tanmoy.

Tanmoy Paul
ID: 181-15-10935
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

Firstly, I like to forward my regard to Almighty Allah for showing me the right path while attempting the duty.

The real sprit of achieving a destiny is through the path of eminence and solid discipline. I would have never achieved in finishing my job without the alliance, inspiration and assist issued to me by different personalities. This thesis report would not have been manageable without the assist and direction of **Md. GaziZahirul Islam, Assistant Professor**, Department of Computer Science and Engineering, Daffodil International University, under whose supervision I chose this topic.

I must grant with due respect the endless support and patience of my family members for finishing this internship.

ABSTRACT

Cyber threats increase exponentially in this day. To survive from these threats, we need to ensure strong defence from cyber-attacks. But the question is how can we measure this defence. By assessing the security, we can measure the security defence and ensure the security.

A cybersecurity assessment examines your security controls and how they stack up against known vulnerabilities. It’s similar to a cyber-risk assessment, a part of the risk management process, in that it incorporates threat-based approaches to evaluate cyber resilience. A complete security assessment includes a close look at the company’s overall security infrastructure.

In cyber security assessment, Vulnerability and Penetration Testing is most popular methods.

The primary objective of this internship training conduct vulnerability scan penetration test by using automated tools from Rapid7.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 01

INTRODUCTION

1.1INTRODUCTION:

Vulnerability assessment is process of documenting, discovering, and quantifying the current security, vulnerability found with a system. Vulnerability is necessary for the protection of IT resources. It finds out the vulnerability in a system which increase the security of the data.

Data is now very valuable to the whole world So we have to take many methods to save it. Vulnerability is one of them. With this we can find out the weak point of the vulnerabilities, and vulnerabilities are reported to cyber security, as a result hacker can't longer attack vulnerabilities in the system.

We find out the vulnerability of the system to make the system error free and find out all the faults in the system. So vulnerability is very important for data security and cyber security.

When the weak point is fixed, it is tested for penetration tasting. The penetration test is used to attack those vulnerability areas like hackers, to understand whether the cyber security has fixed that weak spot.

1.2MOTIVATION:

Cyber-attacks occur every day. To protect from those attack, we need to build flaw less infrastructure that's why we need to conduct VAPT based on compliance/ regulatory basis.

1.3 OBJECTIVE:

The Objective of this internship training is, how to scan vulnerability for a system? prioritization of vulnerabilities, provide remediation guidelines and reporting. And How to conduct penetration testing and exploit those vulnerabilities that we found in vulnerability scan in automated fashion by using a modern Vulnerability Assessment tool (Nexpose) and Penetration testing tool (Metasploit Pro) from Rapid7.

1.4 OUTCOME:

Evaluate the vulnerability of Router, Switch, Server, Endpoint device, and report to the organization to fix vulnerabilities to prevent future cyber-attack.

For penetration test, assess the organisation people, process and technology and evaluate their incident response process.

1.5 LAYOUT OF THE REPORT:

The report put on-

CHAPTER-01: INTRODUCTION

1.1) Introduction 1.2) Motivation 1.3) Objective 1.4) Outcome

CHAPTER-02: BACKGROUND

2.1) Why Vulnerability Assessment 2.2) Penetration Test

CHAPTER-03: Vulnerability Assessment

3.1) Vulnerability Assessment 3.2) Break down 4 four steps

CHAPTER-04: PENETRATION TESTING

4.1) Penetration Test 4.2) Penetration Test Steps

CHAPTER-05: VULNERABILITY ASSESSMENT PROCESS AND FIGURE

5.1) Vulnerability Assessment process

CHAPTER-06: PENETRATION TEST FIGURE

6.1) Penetration Test Figure

CHAPTER-07: FINDING AND CONCLUSION

7.1) Findings vulnerability **7**.2) Conclusion

CHAPTER 02

BACKGROUND

2.1 Why Vulnerability Assessment:

Data is now the most valuable asset in the whole world. For data save we used many types of data security. We used vulnerabilities to find out these data security errors and vulnerabilities.

So vulnerabilities are important cause hackers don't find vulnerabilities in the system so they can't to steal data.

If we don't apply Vulnerability Assessment, then there would be a lot of problem in the system, then hackers can easily hack any system and the stole any data.

2.2 Why Penetration Test:

When vulnerabilities assessment process is end then this process report is submitted to the management for correction.

When they correction all vulnerabilities in this report then we start penetration test. Penetration is, trying to break or bypass like a hacker.

By penetration test, we know that the weak point or vulnerability of the system how much has been corrected.

CHAPTER 03

VULNERABILITY ASSESSMENT

3.1 Vulnerability Assessment:

Vulnerability Assessment is find out any Router, Switch, Server, Endpoint device.

Vulnerability Assessment is four steps:

1. Identify vulnerabilities
2. Evaluate vulnerabilities
3. Treating vulnerabilities
4. Reporting vulnerabilities

1. Identify vulnerabilities:

The scan made 4 stage.

a) Pinging network accessible system or scanning by sending TCP/UDP packets.
b) Detected the open port of the scan systems.
c) Collect all data to the system and log in.
d) Connecting vulnerabilities to all data of the system, damage scanners are able to detect various system running on a network such as laptop, desktop, database, switch etc. Identification system are searched for various features, operating system, installed, file system structured, system configuration and much more.

   To perform this association, the vulnerability scanners will use a vulnerability database to list all known vulnerabilities.

   Vulnerabilities scanners are able to detect all system running to a network.

Correctly vulnerability scan is necessary for any system.

If any organization has very limited network bandwidth during work, then vulnerability sold be scanned at the end of the work.

2.Evaluate vulnerabilities:

After identify the vulnerabilities, it should be noted so that the identify vulnerability are evaluated.

Some example:

a) This vulnerability is how real or false it is.
b) Does anyone take advantage of this vulnerabilities?
c) How right it would be to use these vulnerability?
d) How weak it is?

Company must identify the vulnerability correctly and then evaluate them properly, so that the vulnerabilities are no longer there.

3.Treating Vulnerability:

There are different ways to treat vulnerabilities:

Remediation: Vulnerability are fixing or patching correctly or completely so that it is not exploited. This is often the possibility of the perfect treatment that the company try for.

Mitigation: A weakness reduces the chances of being exploited. This is requiring when an accurate fix is not available for marked vulnerabilities. This option should be used to buy a time to remedy a weakness for an organization.

4.Reporting Vulnerability:

Regular vulnerabilities assessment organization can understand the speed and efficiency of their vulnerability management programs over time. Vulnerabilities organization solution usually have totally different choice for commercialism and notice vulnerabilities scan knowledge with a spread of customizable report and dashboard.

At this end of all vulnerability scan, the report is thoroughly reviews. So that all the vulnerability in this report are well known and they organization or company can be fixed in the right way. So vulnerability report is very important for any company.

CHAPTER 04

Penetration Testing

4.1 Penetration Testing:

We know that, every day occurs cyber-attacks. Hackers are stealing many important data. So protect all the data of our company, they key is to check the penetration testing all the time.

Penetration testing is designed in such a way that our safety is assessed before an attacker. This tool simulates actual world attack situation towards find and exploit safety gaps that would result in taken records, compromised credentials, holding, in person specifiable info, private, protected health info, different damaging business result.

Utilizing security vulnerability, intrusion test help determines how to protect important data from future cyber attackers.

4.2Penetration Testing Step:

There are five key step:

1. Information gathering
2. Scanning
3. Gaining access
4. Maintaining access
5. Analysis

1. Information Gathering: The potential goal of collecting appropriate information must be met before any action can be taken by the penetration testing team. This time is important for attack planning and server placement as a platform for the completion of the appointment.

2. Scanning: Flowing resuscitation phase, a set of scan is performing on the goal to decode however their security system can counter many break makes an attempt. Invention of vulnerability open ports different parts of debilitation at interval a network structure will instruction however samples can continue by the planned attack.

3. Gaining Access: After collecting data, testers attack common application so that they can exploit existing vulnerabilities. Testers try to mimic the potential damage that can result from a vulnerability.

4.Maintain Access: The first target for this period is realize a state of continuous presence at intervals the target surroundings. As period development, a lot of knowledge is culled throughout the exploit system that permits the checker to imitative advanced preserving treats.

5.Analysis: Penetration testing result are then made into a report detailing,

a) The exact vulnerability that is exploited.
b) Subtle data that are accessed.
c) Quantity of time the pen sample is able to remain in the system undetected.

This information is analysis by security private to help configure.

CHAPTER 05

Vulnerability Assessment Process

5.1 Vulnerability Assessment Process:

For Vulnerability Assessment, we are using Nexpose from Rapid7. And we have selected target as a Linux server.

First, we login into Nexpose web console.

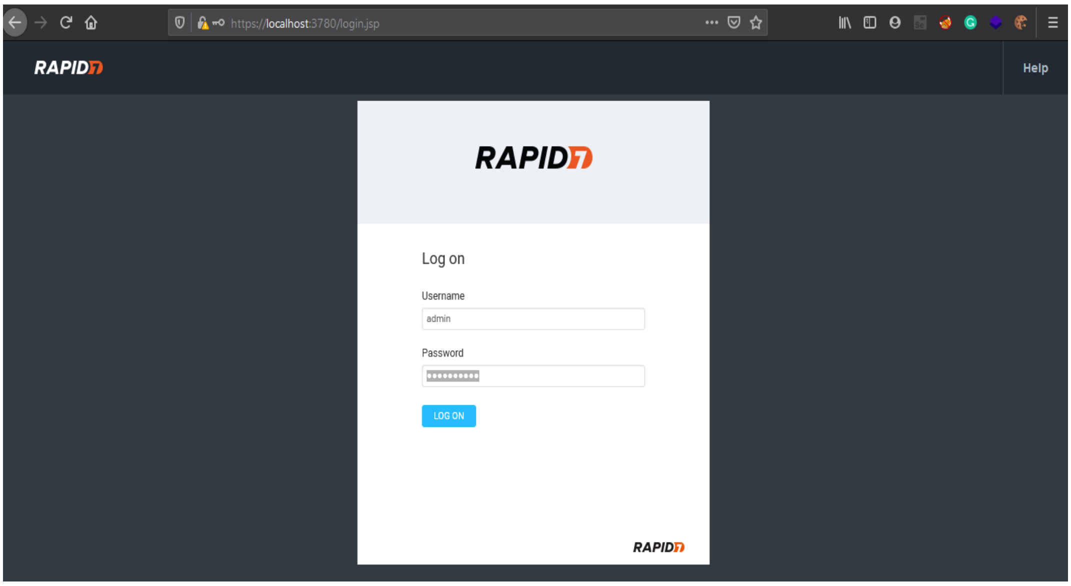
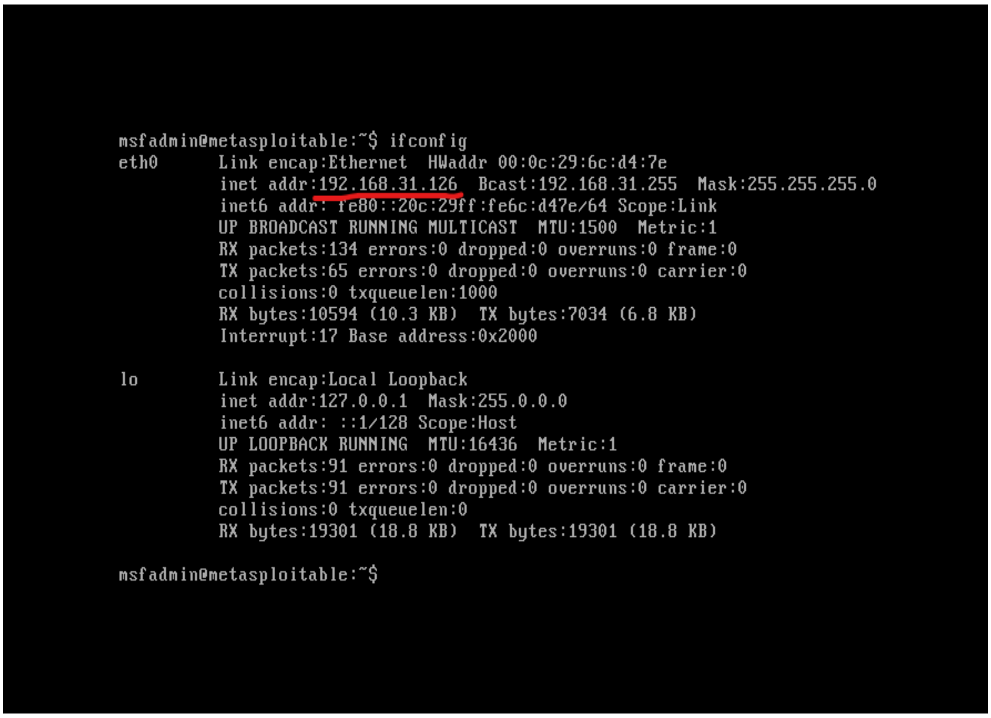


Figure 5.1 Login.

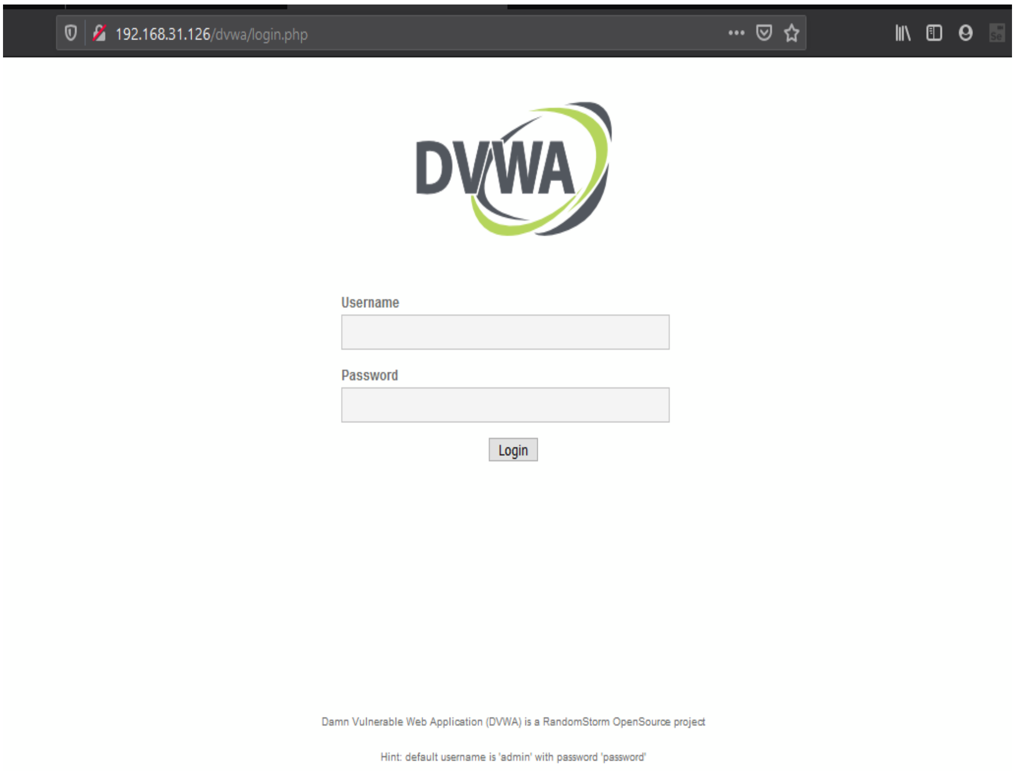
Target ip: Our target is Linux Ubuntu server and ip address 192.168.31.126



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:6c:d4:7e
          inet addr:192.168.31.126  Bcast:192.168.31.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6c:d47e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:134 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10594 (10.3 KB)  TX bytes:7034 (6.8 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```

Figure5.2 target ip

Target server:



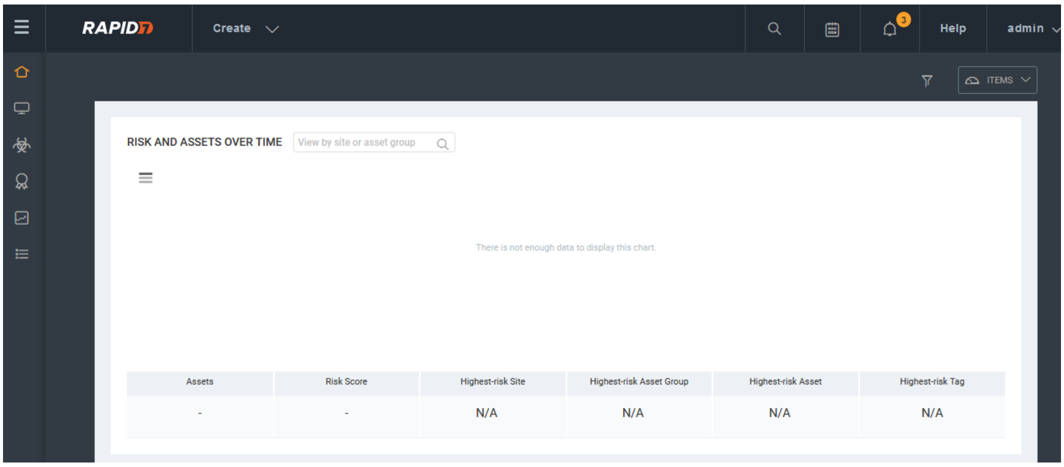
192.168.31.126/dvwa/login.php

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

Figure 5.3 Target server has also a web service

Dashbord: When we login in correct email and password then we can see dashbord.



RISK AND ASSETS OVER TIME

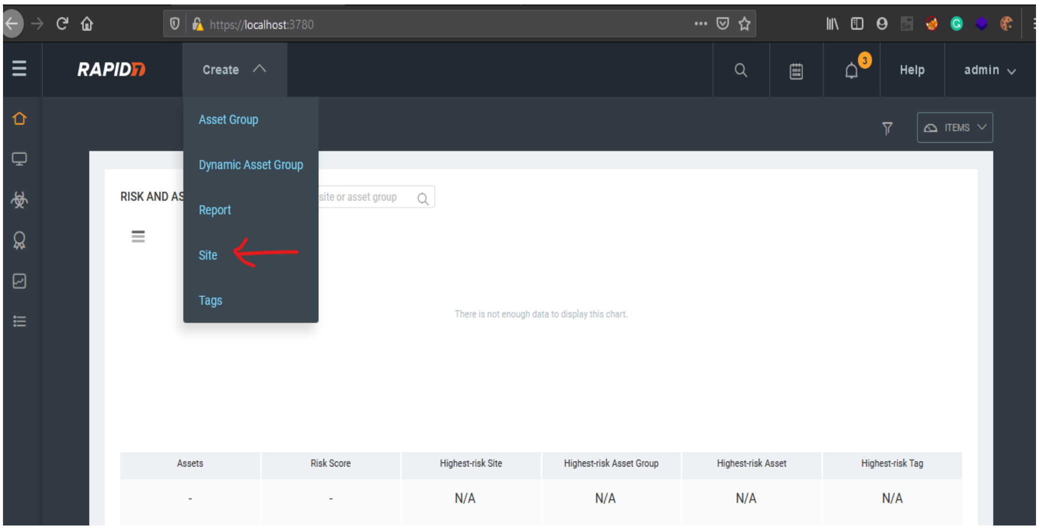
View by site or asset group

There is not enough data to display this chart.

Assets	Risk Score	Highest-risk Site	Highest-risk Asset Group	Highest-risk Asset	Highest-risk Tag
-	-	N/A	N/A	N/A	N/A

Figure 5.4 Nexpose Dashboard

Create site: There are many option such as asset group, dynamic asset group, report, site, tags. At first we need to create a site. For conduct a vulnerability scan, first we need to create a site. To do this we have clicked create and click site.



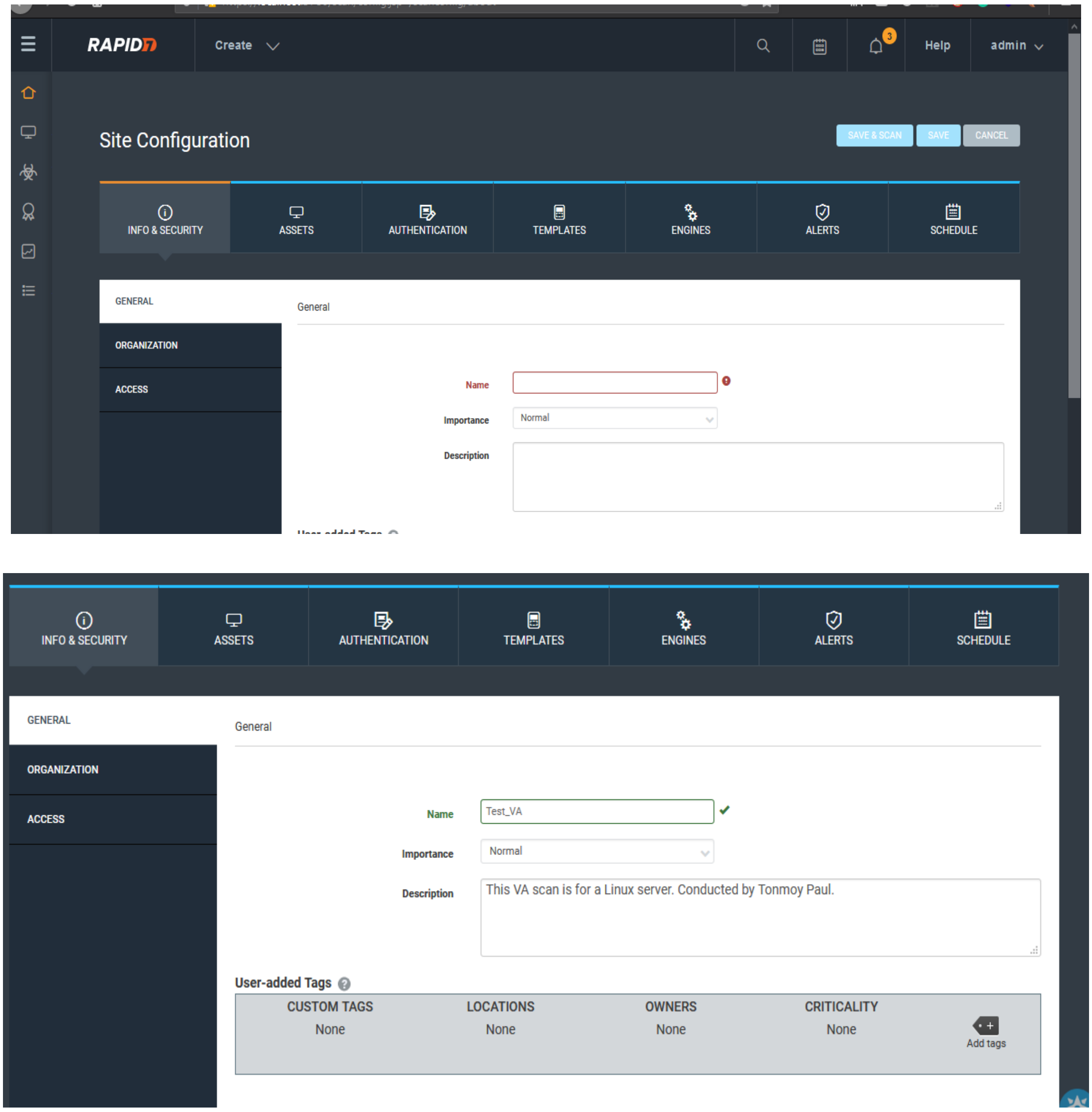
site or asset group

There is not enough data to display this chart.

Assets	Risk Score	Highest-risk Site	Highest-risk Asset Group	Highest-risk Asset	Highest-risk Tag
-	-	N/A	N/A	N/A	N/A

Figure 5.5 clicked create site

Set name and other information: Here we set name and write some information to the description box.



General

Name: Test_VA

Importance: Normal

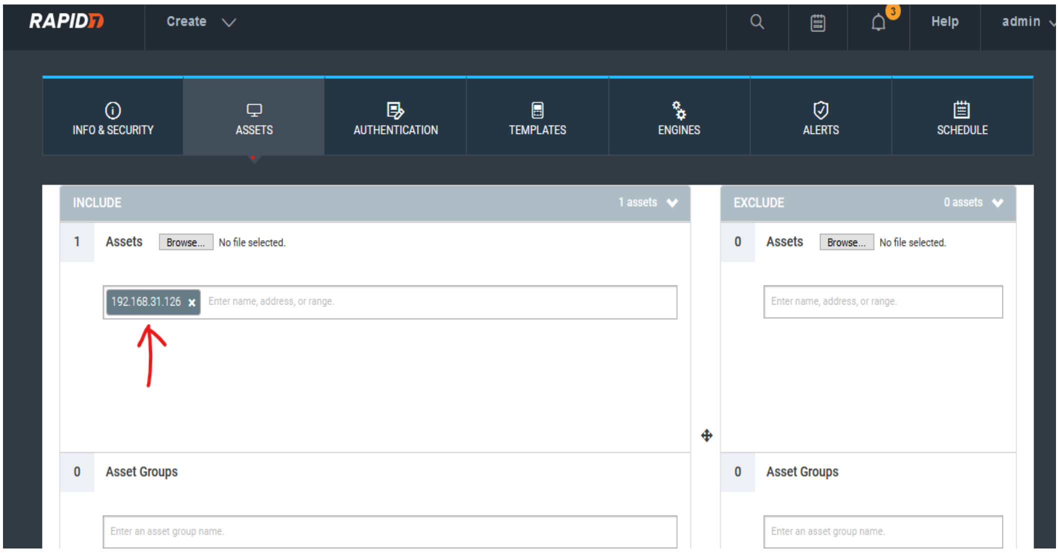
Description: This VA scan is for a Linux server. Conducted by Tonmoy Paul.

User-added Tags

CUSTOM TAGS	LOCATIONS	OWNERS	CRITICALITY
None	None	None	None

Figure 5.6Set name and other information

Asset section: From Asset section, we have set our target IP.



INCLUDE 1 assets

1 Assets No file selected.

192.168.31.126 ×

0 Asset Groups

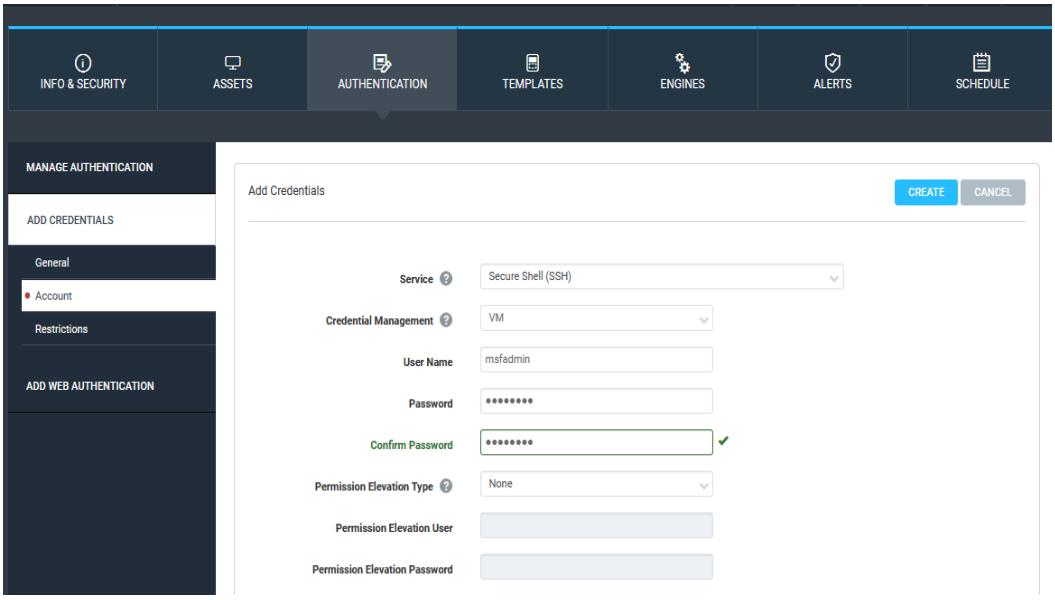
EXCLUDE 0 assets

0 Assets No file selected.

0 Asset Groups

Figure 5.7 Asset section

Authentication: Vulnerability scanning can done by two methods, for white box scan we have set authentication for our target. Here we have set SSH authentication.

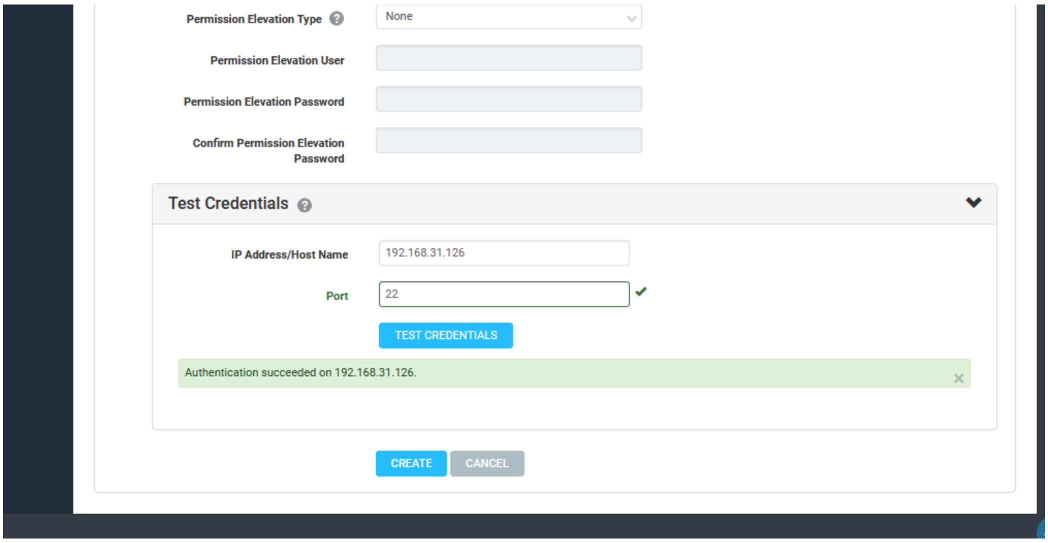


Add Credentials

Service	Secure Shell (SSH)
Credential Management	VM
User Name	msfadmin
Password	••••••••
Confirm Password	•••••••• ✓
Permission Elevation Type	None
Permission Elevation User	
Permission Elevation Password	

Figure 5.8 authentication.

Authentication is verified checked: As we can see our authentication is verified.



Permission Elevation Type: None

Permission Elevation User:

Permission Elevation Password:

Confirm Permission Elevation Password:

Test Credentials

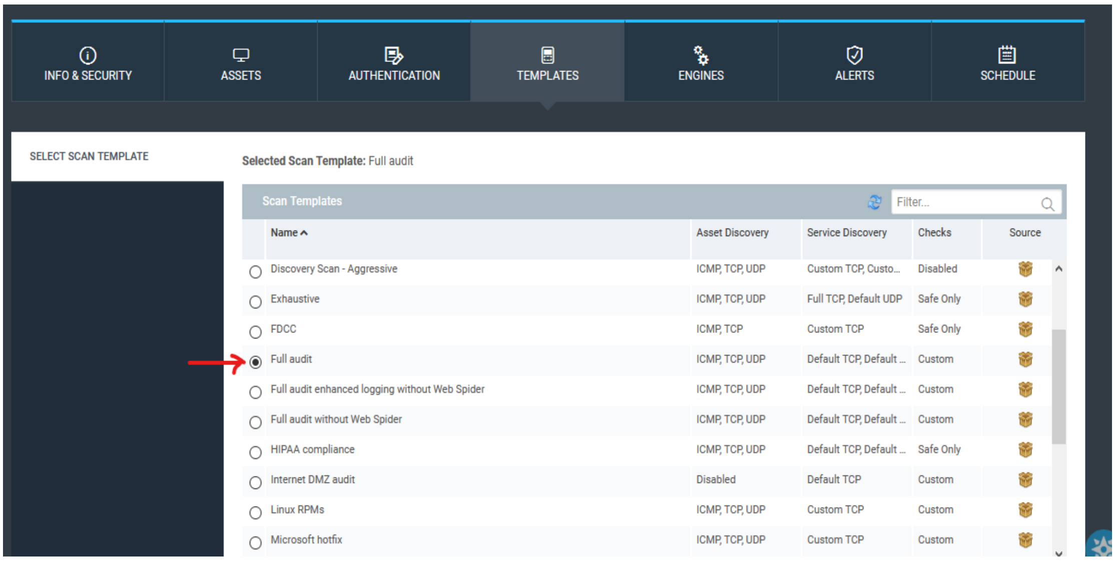
IP Address/Host Name: 192.168.31.126

Port: 22 ✓

Authentication succeeded on 192.168.31.126.

Figure 5.9 Authentication verified.

Scan templates: In automated vulnerability scanner, there is various kinds of scan templates available. We select full audit for details scan. Cause full audit scan give a fulfil report.



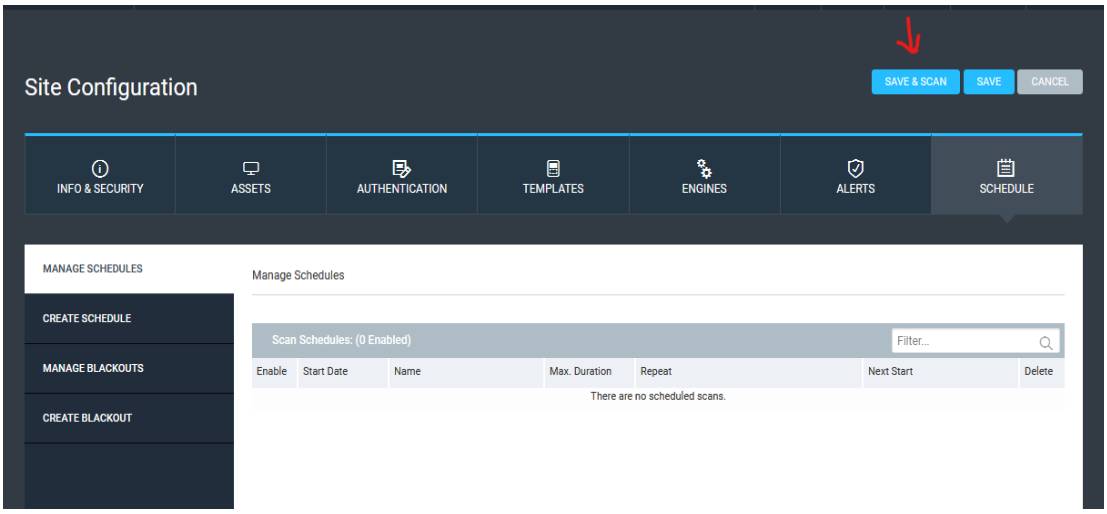
Selected Scan Template: Full audit

Scan Templates

	Name ^	Asset Discovery	Service Discovery	Checks	Source
○	Discovery Scan - Aggressive	ICMP, TCP, UDP	Custom TCP, Custo...	Disabled	
○	Exhaustive	ICMP, TCP, UDP	Full TCP, Default UDP	Safe Only	
○	FDCC	ICMP, TCP	Custom TCP	Safe Only	
●	Full audit	ICMP, TCP, UDP	Default TCP, Default ...	Custom	
○	Full audit enhanced logging without Web Spider	ICMP, TCP, UDP	Default TCP, Default ...	Custom	
○	Full audit without Web Spider	ICMP, TCP, UDP	Default TCP, Default ...	Custom	
○	HIPAA compliance	ICMP, TCP, UDP	Default TCP, Default ...	Safe Only	
○	Internet DMZ audit	Disabled	Default TCP	Custom	
○	Linux RPMs	ICMP, TCP, UDP	Custom TCP	Custom	
○	Microsoft hotfix	ICMP, TCP, UDP	Custom TCP	Custom	

Figure 5.10 Scan templates

Save and scan: After select the scan template, there is others option such as alert and schedule. But we didn't use any of them. And finally click save and scan.



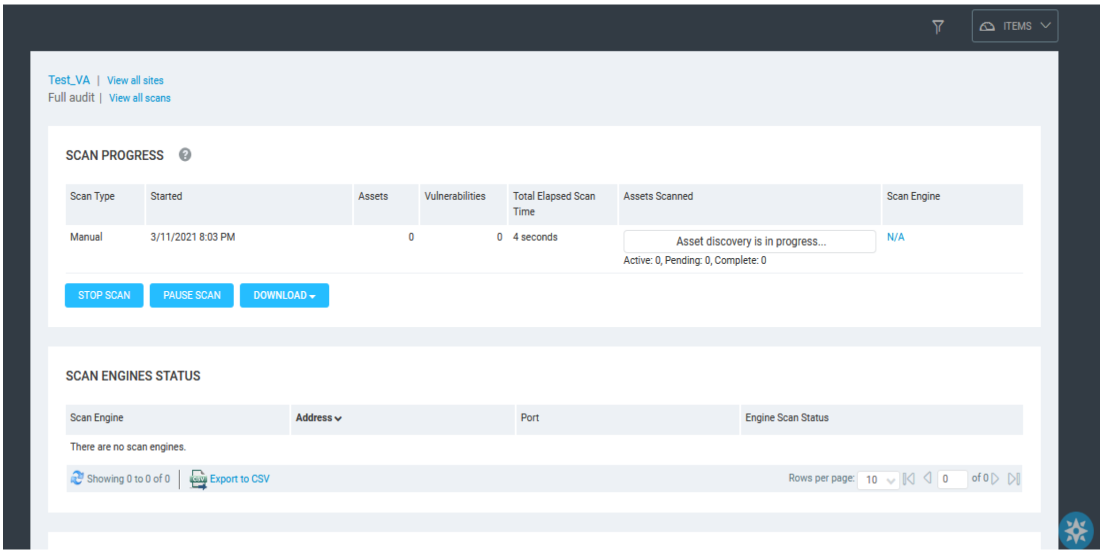
Manage Schedules

Scan Schedules: (0 Enabled)

Enable	Start Date	Name	Max. Duration	Repeat	Next Start	Delete
There are no scheduled scans.						

Figure 5.11 save and scan.

Scan time: Full scan took around 20 minutes.



SCAN PROGRESS

Scan Type	Started	Assets	Vulnerabilities	Total Elapsed Scan Time	Assets Scanned	Scan Engine
Manual	3/11/2021 8:03 PM	0	0	4 seconds	Asset discovery is in progress... Active: 0, Pending: 0, Complete: 0	N/A

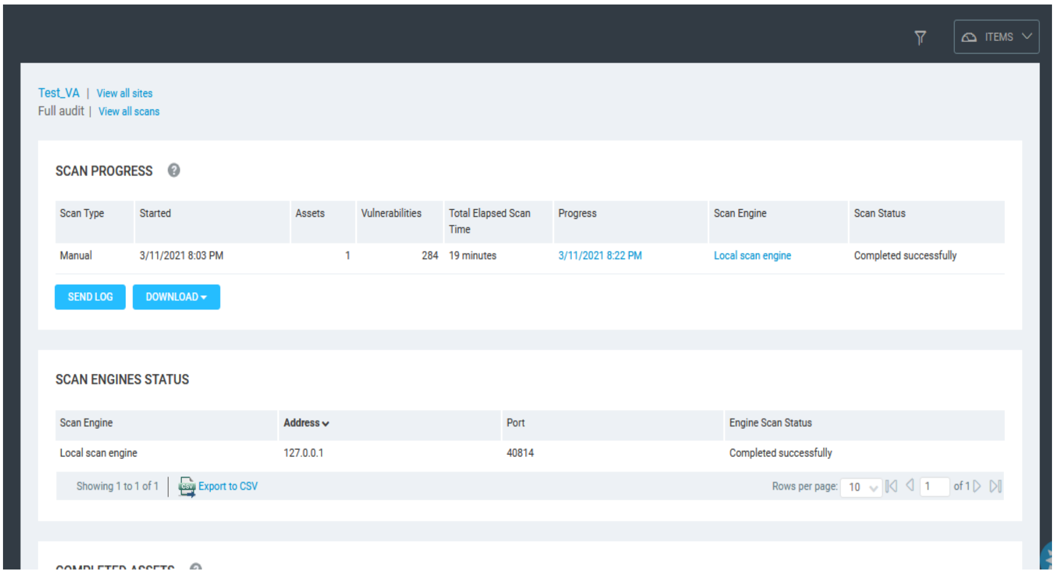
SCAN ENGINES STATUS

Scan Engine	Address	Port	Engine Scan Status
There are no scan engines.			

Showing 0 to 0 of 0 | Export to CSV   Rows per page: 10   0 of 0

Figure 5.12 Scan time

Scan process finished: When scan had finished, the status shows Completed Successfully.



Test_VA | View all sites
Full audit | View all scans

SCAN PROGRESS

Scan Type	Started	Assets	Vulnerabilities	Total Elapsed Scan Time	Progress	Scan Engine	Scan Status
Manual	3/11/2021 8:03 PM	1	284	19 minutes	3/11/2021 8:22 PM	Local scan engine	Completed successfully

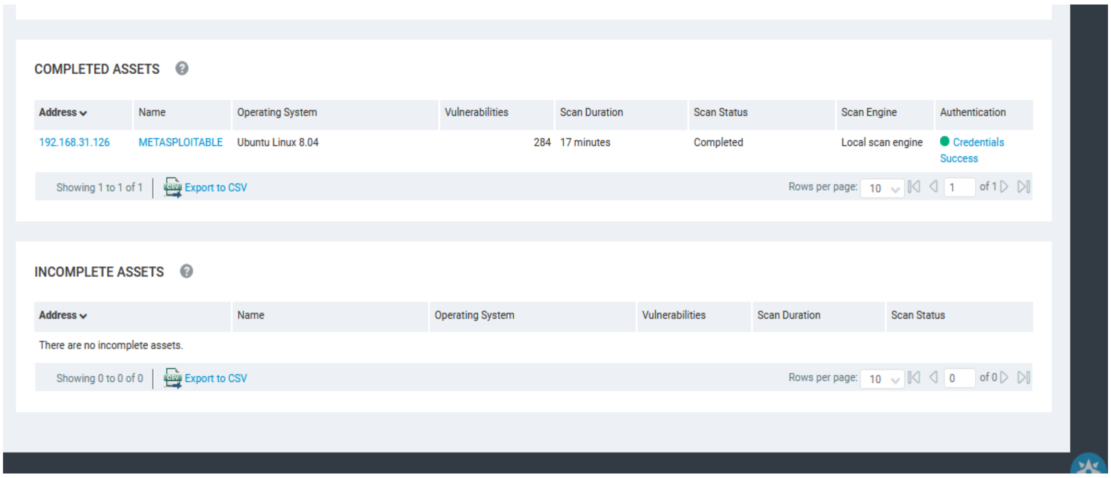
SCAN ENGINES STATUS

Scan Engine	Address	Port	Engine Scan Status
Local scan engine	127.0.0.1	40814	Completed successfully

Showing 1 to 1 of 1 | Export to CSV   Rows per page: 10 1 of 1

Figure 5.13 Scan process finished

Completed assets: Success scan show the assets ip.



COMPLETED ASSETS

Address	Name	Operating System	Vulnerabilities	Scan Duration	Scan Status	Scan Engine	Authentication
192.168.31.126	METASPLOITABLE	Ubuntu Linux 8.04	284	17 minutes	Completed	Local scan engine	● Credentials Success

Showing 1 to 1 of 1 | Export to CSV   Rows per page: 10 1 of 1

INCOMPLETE ASSETS

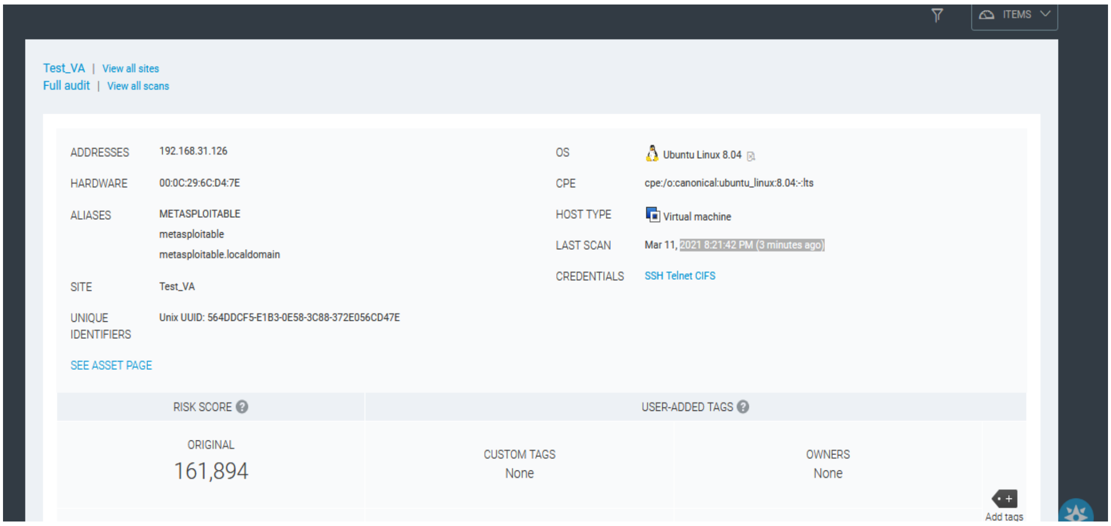
Address	Name	Operating System	Vulnerabilities	Scan Duration	Scan Status

There are no incomplete assets.

Showing 0 to 0 of 0 | Export to CSV   Rows per page: 10 0 of 0

Figure 5.14 Completed assets

Details info: For details we clicked the ip, and we can see details info about the target. Such as hostname, OS, etc.



Test_VA | View all sites
Full audit | View all scans

ADDRESSES	192.168.31.126	OS	Ubuntu Linux 8.04
HARDWARE	00:0C:29:6C:D4:7E	CPE	cpe:/o:canonical:ubuntu_linux:8.04:-:lts
ALIASES	METASPLOITABLE metasploitable metasploitable.localdomain	HOST TYPE	Virtual machine
		LAST SCAN	Mar 11, 2021 8:21:42 PM (3 minutes ago)
		CREDENTIALS	SSH Telnet CIFS
SITE	Test_VA		
UNIQUE IDENTIFIERS	Unix UUID: 564DDCF5-E1B3-0E58-3C88-372E056CD47E		

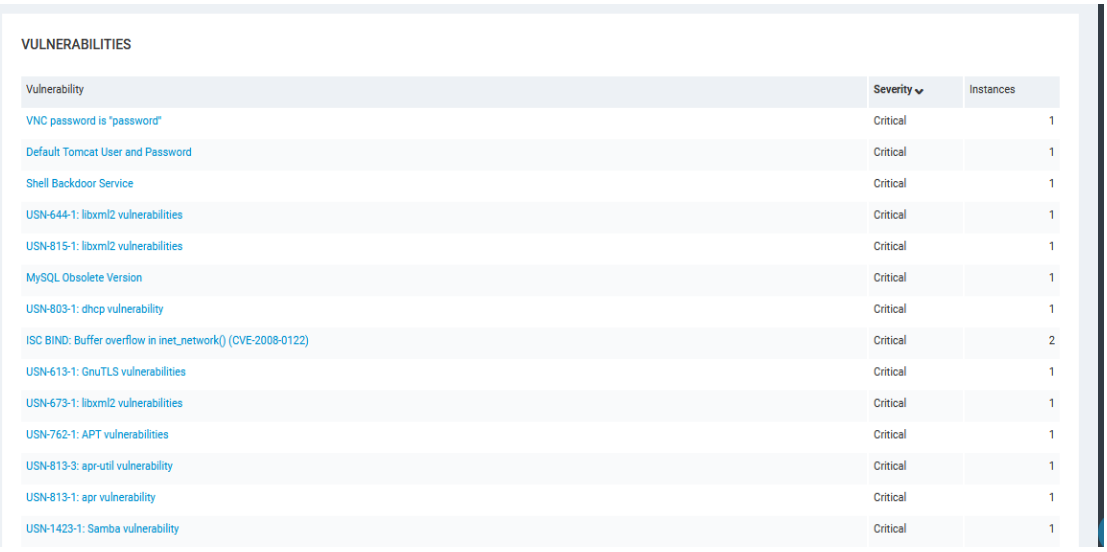
SEE ASSET PAGE

RISK SCORE	USER-ADDED TAGS	
ORIGINAL 161,894	CUSTOM TAGS None	OWNERS None

Figure 5.15 Details info.

Found vulnerability: We have found 250 + vulnerability.

.

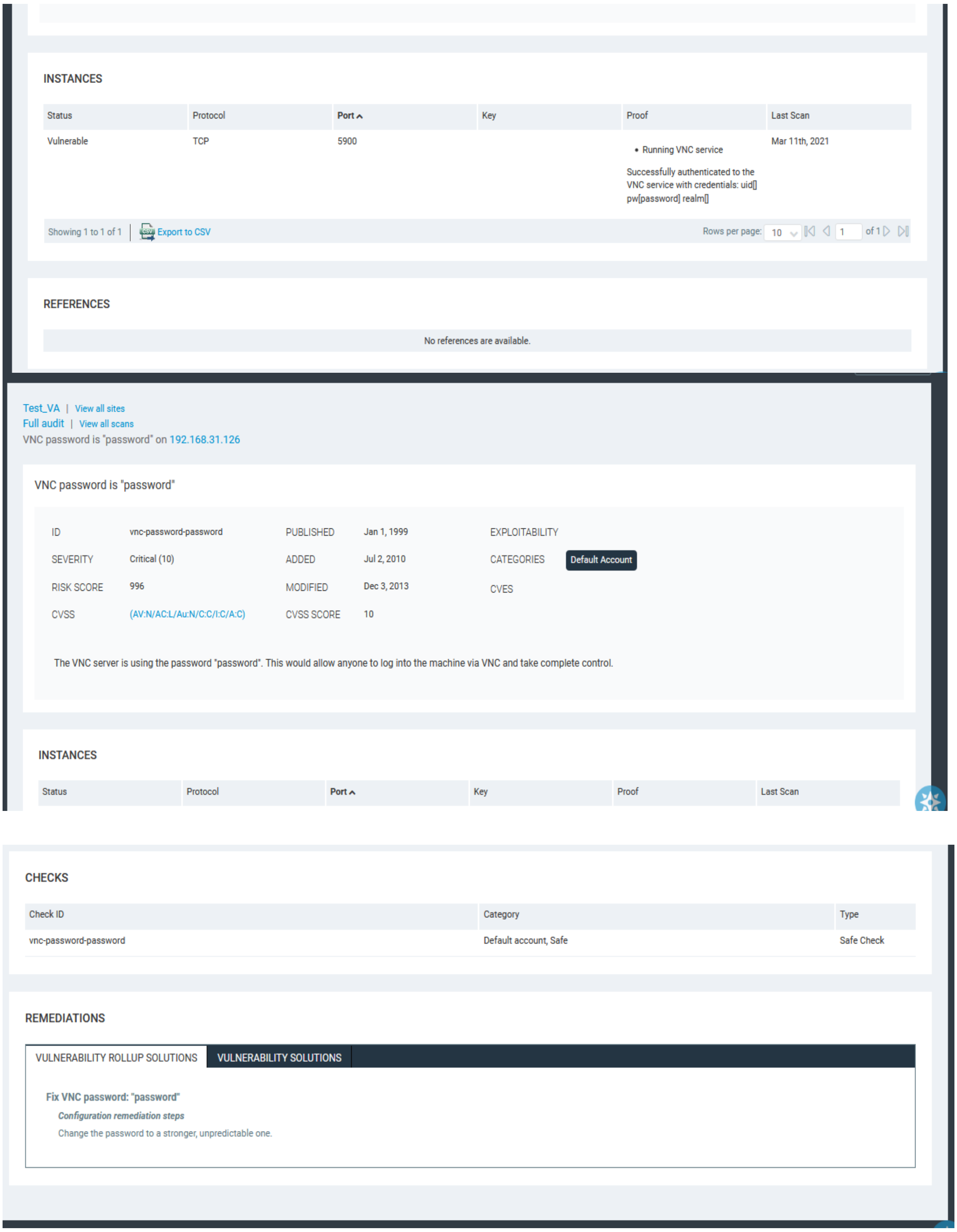


VULNERABILITIES

Vulnerability	Severity	Instances
VNC password is "password"	Critical	1
Default Tomcat User and Password	Critical	1
Shell Backdoor Service	Critical	1
USN-644-1: libxml2 vulnerabilities	Critical	1
USN-815-1: libxml2 vulnerabilities	Critical	1
MySQL Obsolete Version	Critical	1
USN-803-1: dhcp vulnerability	Critical	1
ISC BIND: Buffer overflow in inet_network() (CVE-2008-0122)	Critical	2
USN-613-1: GnuTLS vulnerabilities	Critical	1
USN-673-1: libxml2 vulnerabilities	Critical	1
USN-762-1: APT vulnerabilities	Critical	1
USN-813-3: apr-util vulnerability	Critical	1
USN-813-1: apr vulnerability	Critical	1
USN-1423-1: Samba vulnerability	Critical	1

Figure 5.16 found vulnerability

Details: If we click any, the details has shown also remediation.



INSTANCES

Status	Protocol	Port ^	Key	Proof	Last Scan
Vulnerable	TCP	5900		• Running VNC service Successfully authenticated to the VNC service with credentials: uid[] pw[password] realm[]	Mar 11th, 2021

Showing 1 to 1 of 1 | Export to CSV Rows per page: 10 1 of 1

REFERENCES

No references are available.

Test_VA | View all sites
Full audit | View all scans
VNC password is "password" on 192.168.31.126

VNC password is "password"

ID	vnc-password-password	PUBLISHED	Jan 1, 1999	EXPLOITABILITY	
SEVERITY	Critical (10)	ADDED	Jul 2, 2010	CATEGORIES	Default Account
RISK SCORE	996	MODIFIED	Dec 3, 2013	CVES	
CVSS	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	CVSS SCORE	10		

The VNC server is using the password "password". This would allow anyone to log into the machine via VNC and take complete control.

INSTANCES

Status	Protocol	Port ^	Key	Proof	Last Scan

CHECKS

Check ID	Category	Type
vnc-password-password	Default account, Safe	Safe Check

REMEDIATIONS

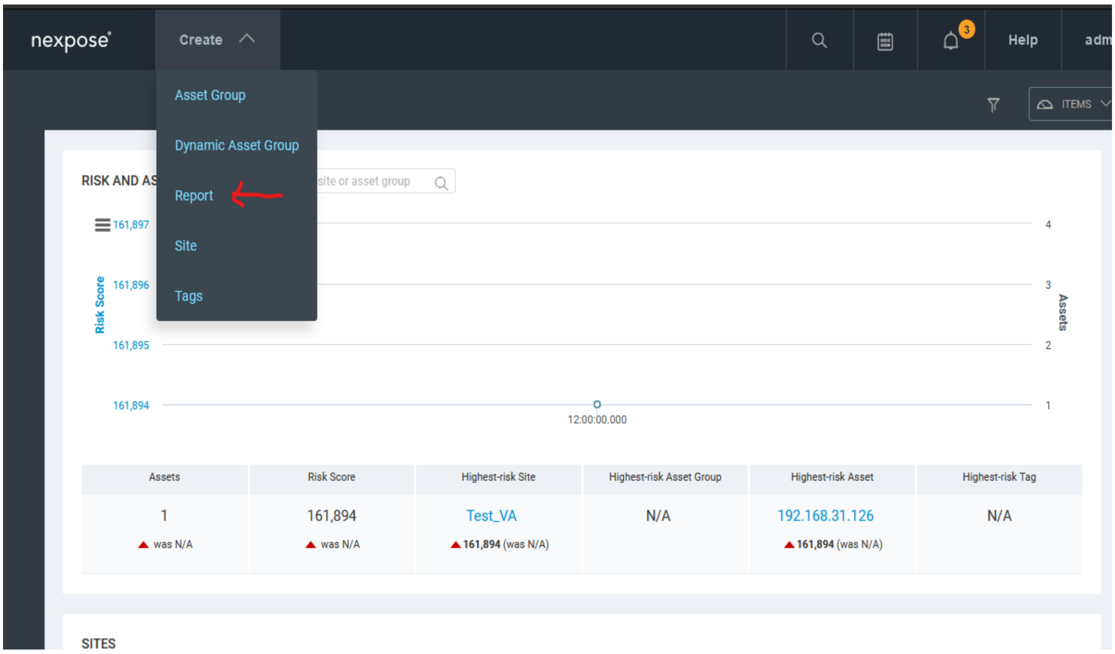
Fix VNC password: "password"

Configuration remediation steps

Change the password to a stronger, unpredictable one.

Figure 5.17 details

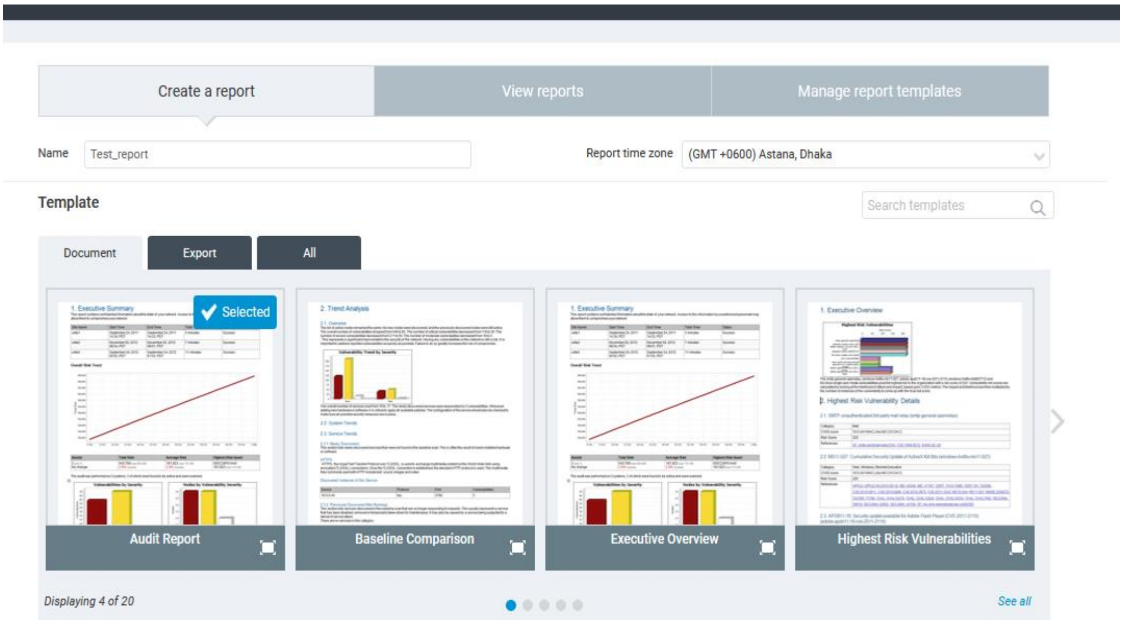
Create Report: After scanning, we have generated a standard report called audit report. To generate the report click, create and Report.



Assets	Risk Score	Highest-risk Site	Highest-risk Asset Group	Highest-risk Asset	Highest-risk Tag
1 ▲ was N/A	161,894 ▲ was N/A	Test_VA ▲ 161,894 (was N/A)	N/A	192.168.31.126 ▲ 161,894 (was N/A)	N/A

Figure 5.18 create Report.

Select audit report: There are various types of report template we have selected Audit report.

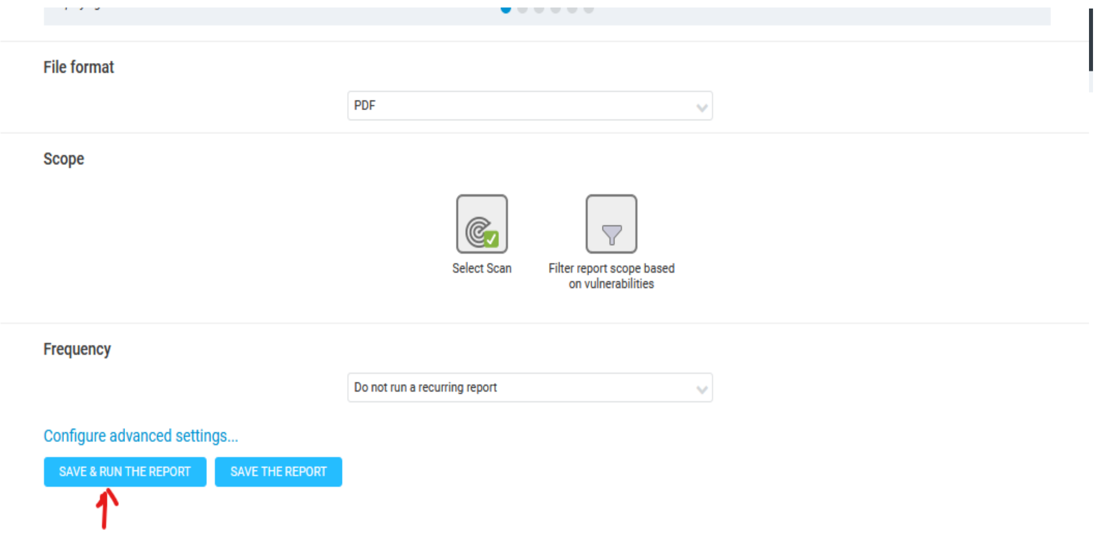


Name: Test_report

Report time zone: (GMT +0600) Astana, Dhaka

Figure 5.19 selected Audit report

Generate report: Then we have selected pdf format and click generate the report.



File format

PDF

Scope

Select Scan
Filter report scope based on vulnerabilities

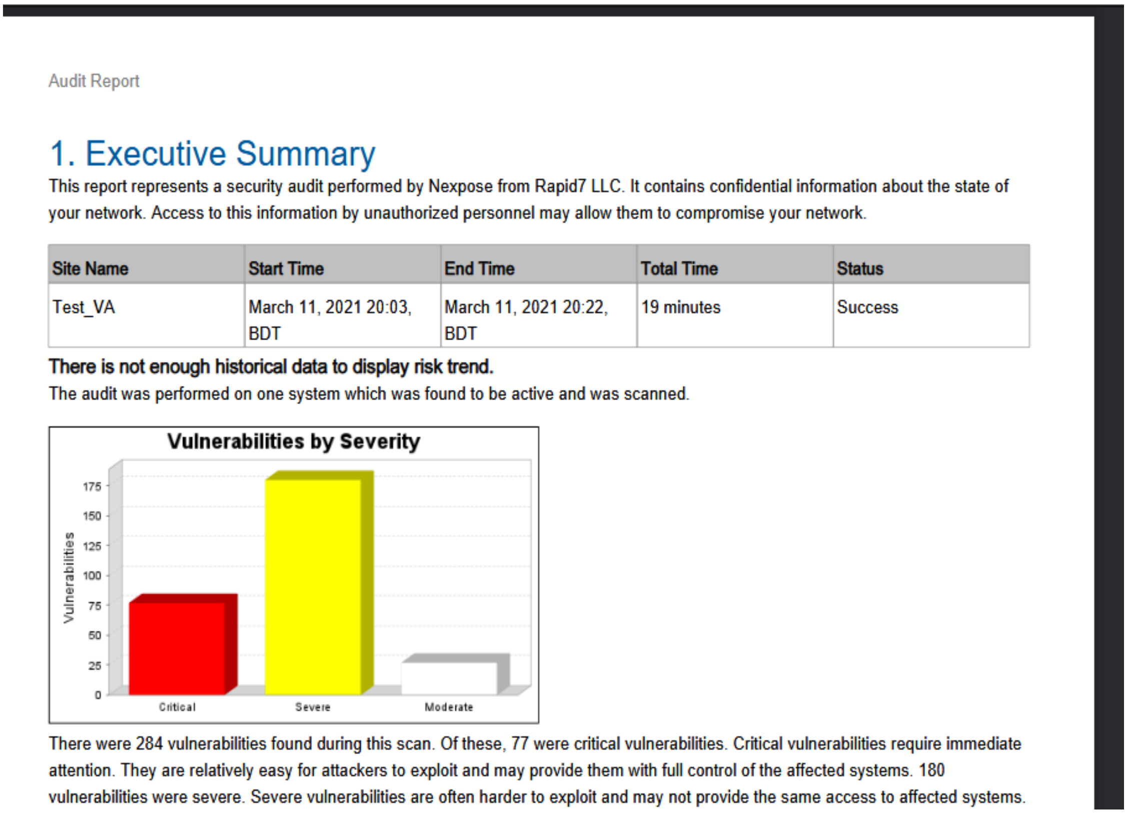
Frequency

Do not run a recurring report

Configure advanced settings...
SAVE & RUN THE REPORT
SAVE THE REPORT

Figure 5.20 generate report.

Successfully generate report: The report has generated.



Audit Report

1. Executive Summary

This report represents a security audit performed by Nexpose from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

Site Name	Start Time	End Time	Total Time	Status
Test_VA	March 11, 2021 20:03, BDT	March 11, 2021 20:22, BDT	19 minutes	Success

There is not enough historical data to display risk trend.

The audit was performed on one system which was found to be active and was scanned.

There were 284 vulnerabilities found during this scan. Of these, 77 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 180 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems.

Figure 5.21 Successfully generate report

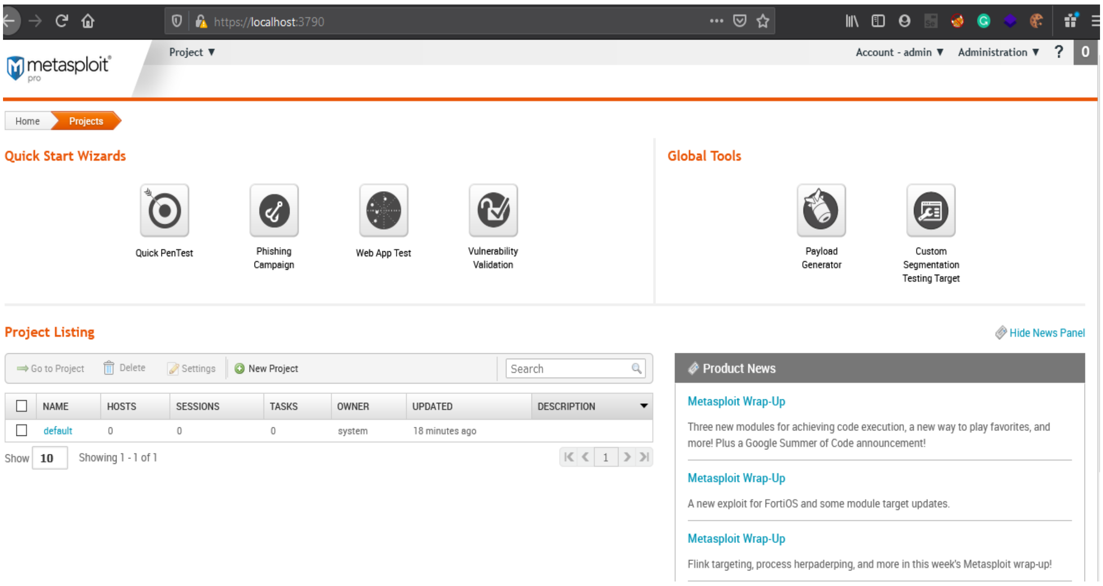
CHAPTER 06

Penetration Test Process

6.1 Penetration Test Process:

For Penetration Testing, we have selected same server as we used for VA. We have found 250+ vulnerabilities the VA scan. Now we trying to penetrate those vulnerabilities using Metasploit Pro form Rapid7.

Login: First we have logged into Metasploit pro web console.



☐	NAME	HOSTS	SESSIONS	TASKS	OWNER	UPDATED	DESCRIPTION
☐	default	0	0	0	system	18 minutes ago	

Show 10 Showing 1 - 1 of 1

Product News

Metasploit Wrap-Up

Three new modules for achieving code execution, a new way to play favorites, and more! Plus a Google Summer of Code announcement!

Metasploit Wrap-Up

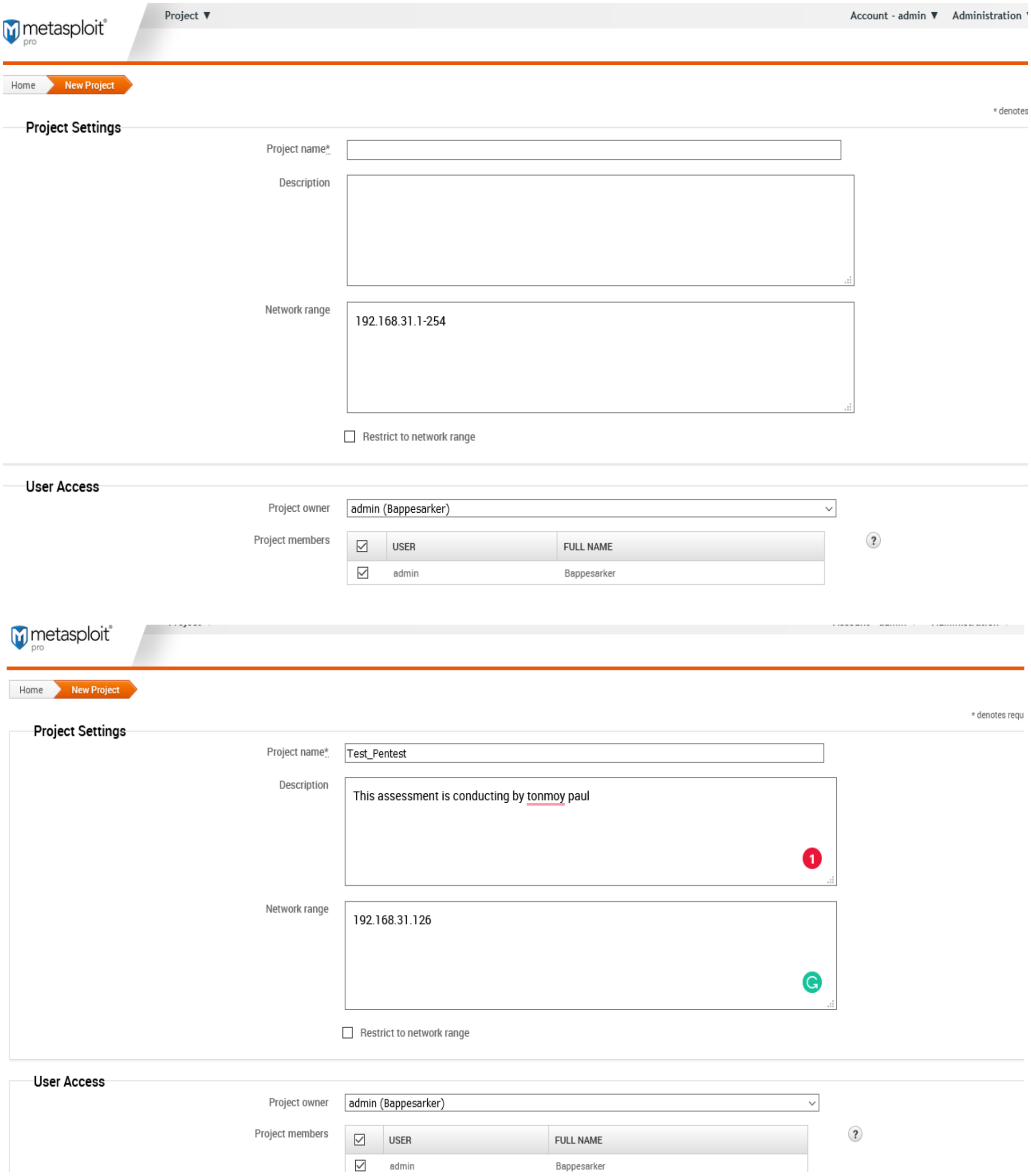
A new exploit for FortiOS and some module target updates.

Metasploit Wrap-Up

Flink targeting, process herpaderping, and more in this week's Metasploit wrap-up!

Figure 6.1 Login

Fill up details: We have create a project and set a name and details and set the target ip.



Project Settings

Project name*

Description

Network range: 192.168.31.1-254

☐ Restrict to network range

User Access

Project owner: admin (Bappesarker)

☑	USER	FULL NAME
☑	admin	Bappesarker

Project Settings

Project name*: Test_Pentest

Description: This assessment is conducting by tonmoy paul

Network range: 192.168.31.126

☐ Restrict to network range

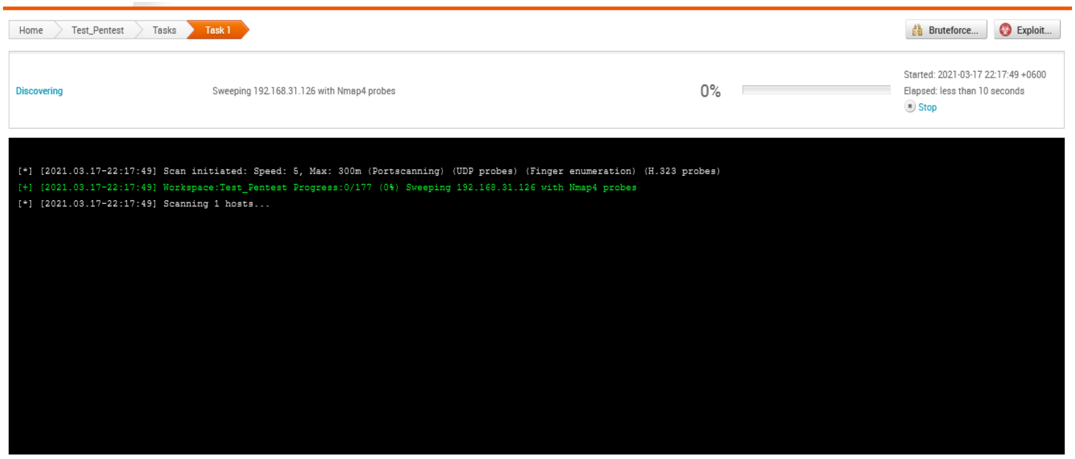
User Access

Project owner: admin (Bappesarker)

☑	USER	FULL NAME
☑	admin	Bappesarker

Figure 6.2 Fill up details.

Import the vulnerabilities: After crating the project, we import the vulnerabilities from Nexpose. Because these two solutions are integrated.



Discovering

Sweeping 192.168.31.126 with Nmap4 probes

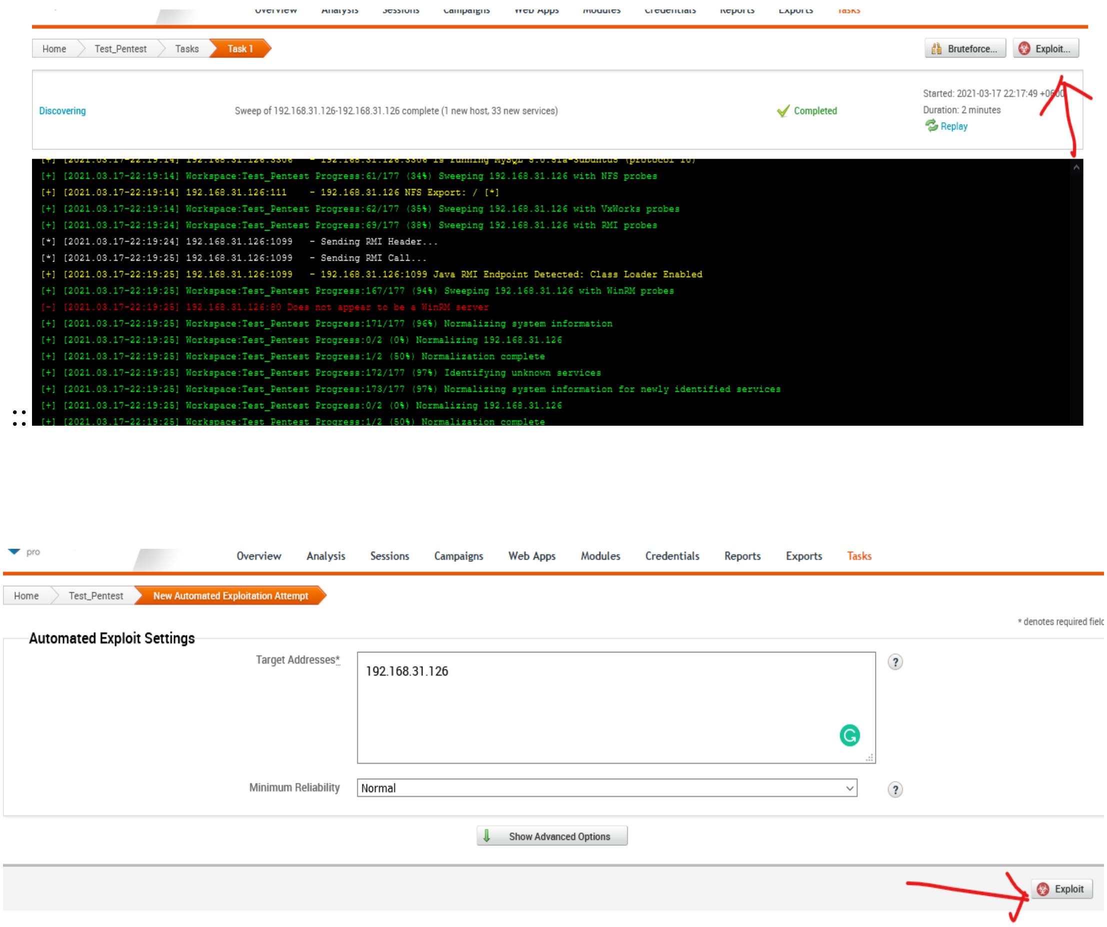
0%

Started: 2021-03-17 22:17:49 +0600
Elapsed: less than 10 seconds
Stop

```
[*] [2021.03.17-22:17:49] Scan initiated: Speed: 5, Max: 300m (Portscanning) (UDP probes) (Finger enumeration) (H.323 probes)
[+] [2021.03.17-22:17:49] Workspace:Test_Pentest Progress:0/177 (0%) Sweeping 192.168.31.126 with Nmap4 probes
[*] [2021.03.17-22:17:49] Scanning 1 hosts...
```

Figure 6.3 import the vulnerabilities.

Exploit: After Imported the scan data, we have runed Exploit for penetrating the target.



Discovering   Sweep of 192.168.31.126-192.168.31.126 complete (1 new host, 33 new services)   ✓ Completed

Started: 2021-03-17 22:17:49 +0600
Duration: 2 minutes

```
[+] [2021.03.17-22:19:14] 192.168.31.126:3306   - 192.168.31.126:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)
[+] [2021.03.17-22:19:14] Workspace:Test_Pentest Progress:61/177 (34%) Sweeping 192.168.31.126 with NFS probes
[+] [2021.03.17-22:19:14] 192.168.31.126:111    - 192.168.31.126 NFS Export: / [*]
[+] [2021.03.17-22:19:14] Workspace:Test_Pentest Progress:62/177 (35%) Sweeping 192.168.31.126 with VxWorks probes
[+] [2021.03.17-22:19:24] Workspace:Test_Pentest Progress:69/177 (38%) Sweeping 192.168.31.126 with RMI probes
[*] [2021.03.17-22:19:24] 192.168.31.126:1099   - Sending RMI Header...
[*] [2021.03.17-22:19:25] 192.168.31.126:1099   - Sending RMI Call...
[+] [2021.03.17-22:19:25] 192.168.31.126:1099   - 192.168.31.126:1099 Java RMI Endpoint Detected: Class Loader Enabled
[+] [2021.03.17-22:19:25] Workspace:Test_Pentest Progress:167/177 (94%) Sweeping 192.168.31.126 with WinRM probes
[-] [2021.03.17-22:19:25] 192.168.31.126:80 Does not appear to be a WinRM server
[+] [2021.03.17-22:19:25] Workspace:Test_Pentest Progress:171/177 (96%) Normalizing system information
[+] [2021.03.17-22:19:25] Workspace:Test_Pentest Progress:0/2 (0%) Normalizing 192.168.31.126
[+] [2021.03.17-22:19:25] Workspace:Test_Pentest Progress:1/2 (50%) Normalization complete
[+] [2021.03.17-22:19:25] Workspace:Test_Pentest Progress:172/177 (97%) Identifying unknown services
[+] [2021.03.17-22:19:25] Workspace:Test_Pentest Progress:173/177 (97%) Normalizing system information for newly identified services
[+] [2021.03.17-22:19:25] Workspace:Test_Pentest Progress:0/2 (0%) Normalizing 192.168.31.126
[+] [2021.03.17-22:19:25] Workspace:Test_Pentest Progress:1/2 (50%) Normalization complete
```

* denotes required field

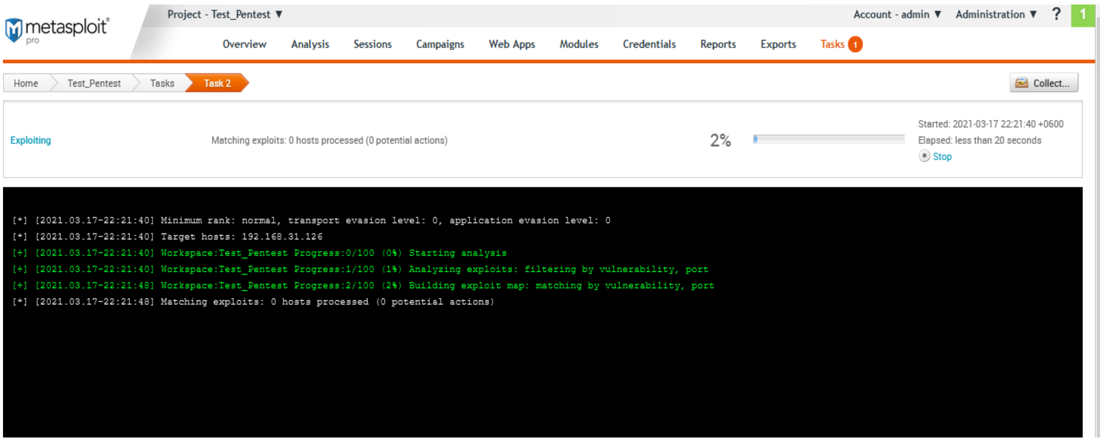
Automated Exploit Settings

Target Addresses*: 192.168.31.126

Minimum Reliability: Normal

Figure 6.4 Exploit

Exploit process:



Exploiting

Matching exploits: 0 hosts processed (0 potential actions)

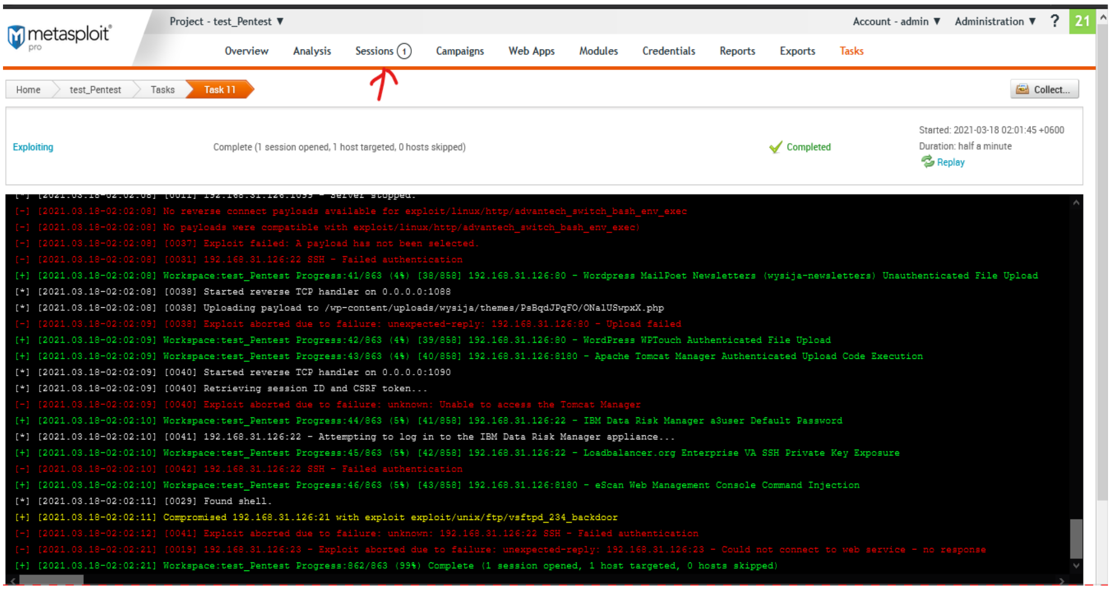
2%

Started: 2021-03-17 22:21:40 +0600
Elapsed: less than 20 seconds

```
[*] [2021.03.17-22:21:40] Minimum rank: normal, transport evasion level: 0, application evasion level: 0
[*] [2021.03.17-22:21:40] Target hosts: 192.168.31.126
[+] [2021.03.17-22:21:40] Workspace:Test_Pentest Progress:0/100 (0%) Starting analysis
[+] [2021.03.17-22:21:40] Workspace:Test_Pentest Progress:1/100 (1%) Analyzing exploits: filtering by vulnerability, port
[+] [2021.03.17-22:21:48] Workspace:Test_Pentest Progress:2/100 (2%) Building exploit map: matching by vulnerability, port
[*] [2021.03.17-22:21:48] Matching exploits: 0 hosts processed (0 potential actions)
```

Figure 6.5 After clicking the Exploit

Session: After completed the Exploitation process we have found 1 session has created.



Exploiting

Complete (1 session opened, 1 host targeted, 0 hosts skipped)

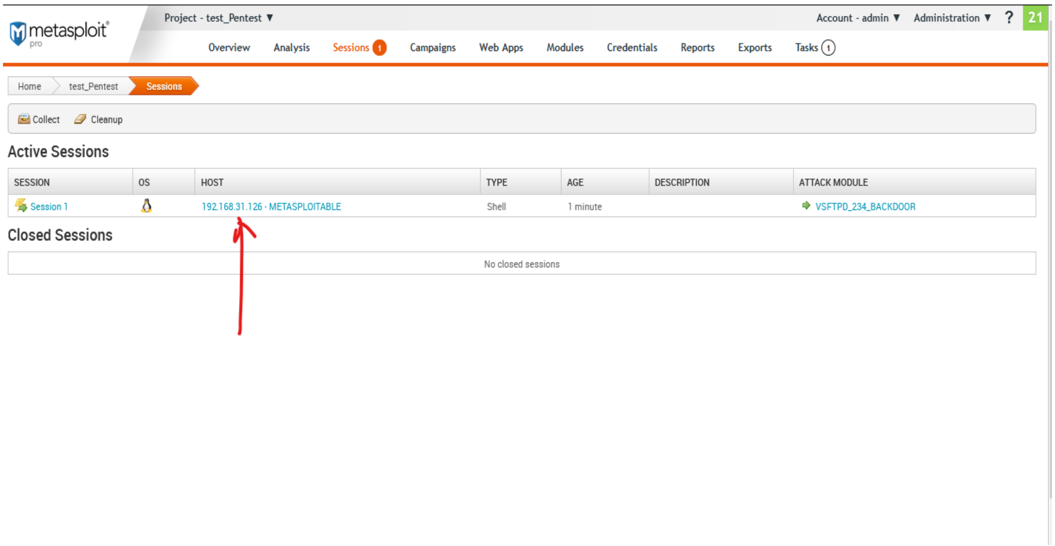
✓ Completed

Started: 2021-03-18 02:01:45 +0600
Duration: half a minute

```
[*] [2021.03.18-02:02:08] [0011] 192.168.31.126:1055 - Server stopped.
[-] [2021.03.18-02:02:08] No reverse connect payloads available for exploit/linux/http/advantech_switch_bash_env_exec
[-] [2021.03.18-02:02:08] No payloads were compatible with exploit/linux/http/advantech_switch_bash_env_exec)
[-] [2021.03.18-02:02:08] [0037] Exploit failed: A payload has not been selected.
[-] [2021.03.18-02:02:08] [0031] 192.168.31.126:22 SSH - Failed authentication
[+] [2021.03.18-02:02:08] Workspace:test_Pentest Progress:41/863 (4%) [38/858] 192.168.31.126:80 - Wordpress MailPoet Newsletters (wysija-newsletters) Unauthenticated File Upload
[*] [2021.03.18-02:02:08] [0038] Started reverse TCP handler on 0.0.0.0:1088
[*] [2021.03.18-02:02:08] [0038] Uploading payload to /wp-content/uploads/wysija/themes/PsBqdJPqFO/ONalUSwpxX.php
[-] [2021.03.18-02:02:09] [0038] Exploit aborted due to failure: unexpected-reply: 192.168.31.126:80 - Upload failed
[+] [2021.03.18-02:02:09] Workspace:test_Pentest Progress:42/863 (4%) [39/858] 192.168.31.126:80 - WordPress WPTouch Authenticated File Upload
[+] [2021.03.18-02:02:09] Workspace:test_Pentest Progress:43/863 (4%) [40/858] 192.168.31.126:8180 - Apache Tomcat Manager Authenticated Upload Code Execution
[*] [2021.03.18-02:02:09] [0040] Started reverse TCP handler on 0.0.0.0:1090
[*] [2021.03.18-02:02:09] [0040] Retrieving session ID and CSRF token...
[-] [2021.03.18-02:02:09] [0040] Exploit aborted due to failure: unknown: Unable to access the Tomcat Manager
[+] [2021.03.18-02:02:10] Workspace:test_Pentest Progress:44/863 (5%) [41/858] 192.168.31.126:22 - IBM Data Risk Manager a3user Default Password
[*] [2021.03.18-02:02:10] [0041] 192.168.31.126:22 - Attempting to log in to the IBM Data Risk Manager appliance...
[+] [2021.03.18-02:02:10] Workspace:test_Pentest Progress:45/863 (5%) [42/858] 192.168.31.126:22 - Loadbalancer.org Enterprise VA SSH Private Key Exposure
[-] [2021.03.18-02:02:10] [0042] 192.168.31.126:22 SSH - Failed authentication
[+] [2021.03.18-02:02:10] Workspace:test_Pentest Progress:46/863 (5%) [43/858] 192.168.31.126:8180 - eScan Web Management Console Command Injection
[*] [2021.03.18-02:02:11] [0029] Found shell.
[+] [2021.03.18-02:02:11] Compromised 192.168.31.126:21 with exploit exploit/unix/ftp/vsftpd_234_backdoor
[-] [2021.03.18-02:02:12] [0041] Exploit aborted due to failure: unknown: 192.168.31.126:22 SSH - Failed authentication
[-] [2021.03.18-02:02:21] [0019] 192.168.31.126:23 - Exploit aborted due to failure: unexpected-reply: 192.168.31.126:23 - Could not connect to web service - no response
[+] [2021.03.18-02:02:21] Workspace:test_Pentest Progress:862/863 (99%) Complete (1 session opened, 1 host targeted, 0 hosts skipped)
```

Figure 6.6 session.

Target: When we have clicked the session we saw that a session has opened from target.



Active Sessions

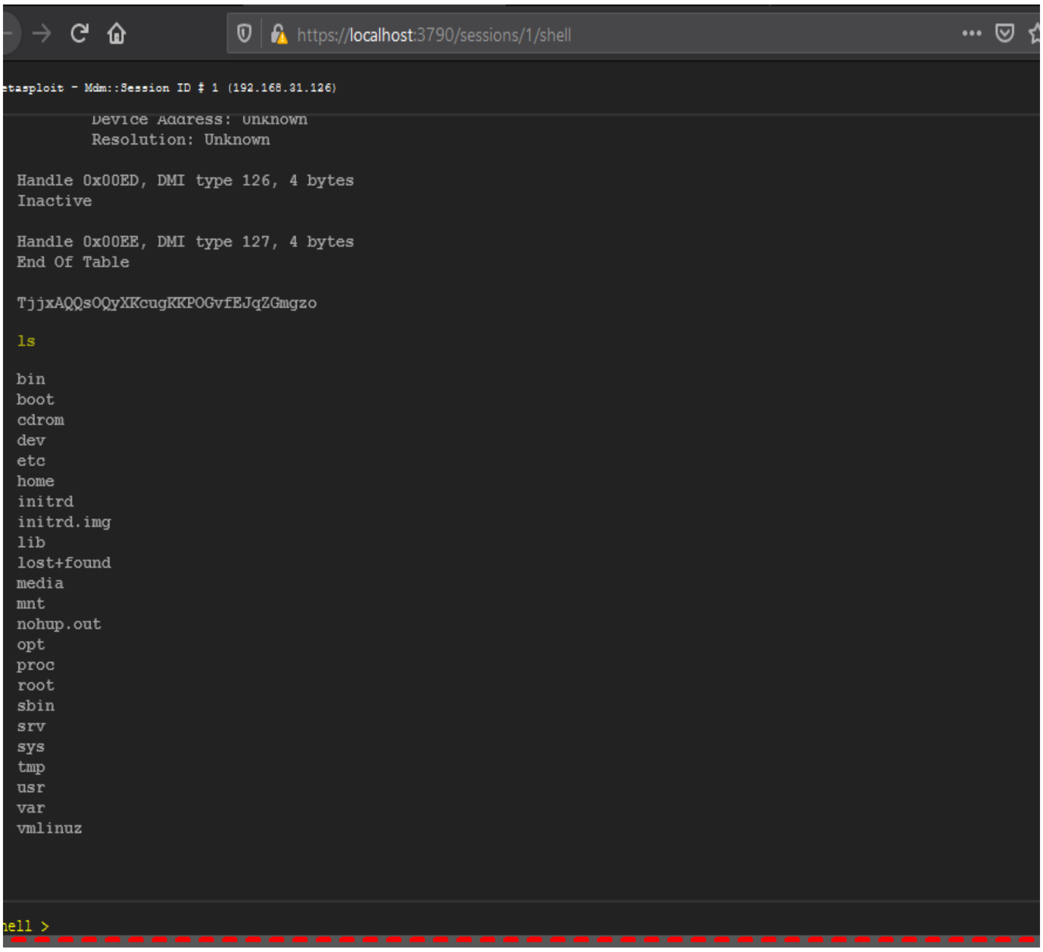
SESSION	OS	HOST	TYPE	AGE	DESCRIPTION	ATTACK MODULE
Session 1	🐧	192.168.31.126 - METASPLOITABLE	Shell	1 minute		VSFTPD_234_BACKDOOR

Closed Sessions

No closed sessions

Figure 6.7 target.

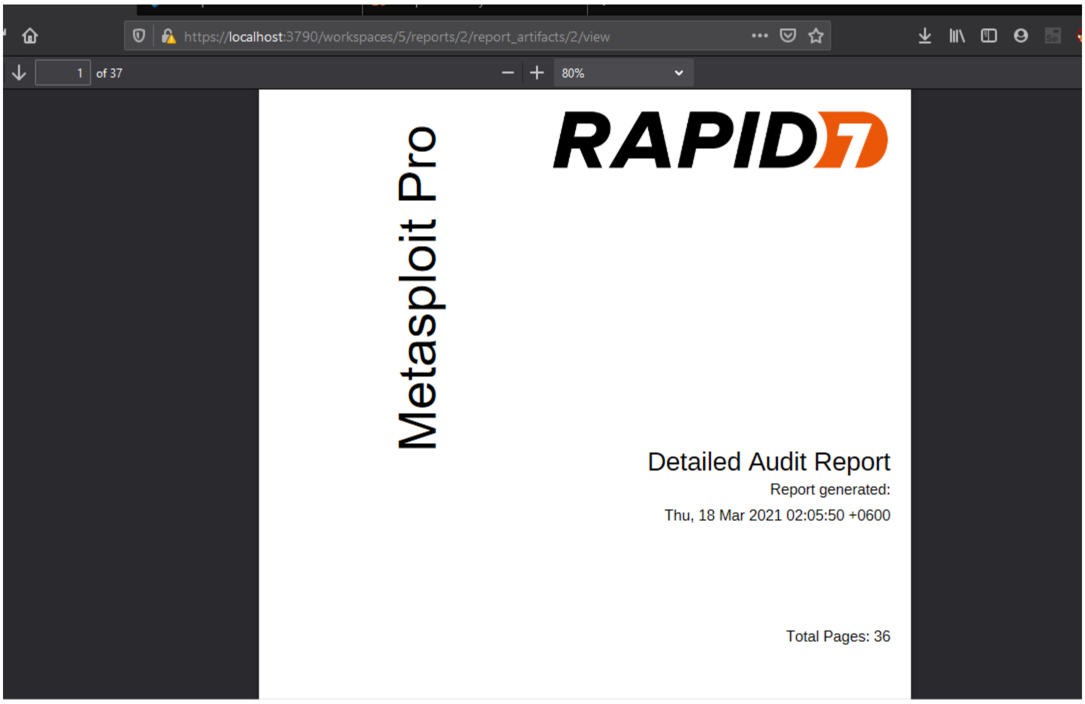
Successfully access: We have successfully gained access into that system. And run command as an administrator.



```
etasploit - Mdm::Session ID # 1 (192.168.31.126)
        Device Address: Unknown
        Resolution: Unknown

Handle 0x00ED, DMI type 126, 4 bytes
Inactive

Handle 0x00EE, DMI type 127, 4 bytes
End Of Table

TjjxAQQsOQyXKcugKKPOGvfEJqZGmgzo

ls

bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz


ell >
```

Figure 6.8successfully access

Report: we have generated a standard penetration testing report.


https://localhost:3790/workspaces/5/reports/2/report_artifacts/2/view
1
of 37
80%
RAPID7

Metasploit Pro

Detailed Audit Report

Report generated:

Thu, 18 Mar 2021 02:05:50 +0600

Total Pages: 36

.

Figure 6.9 report

CHAPTER 07

Findings

7.1 Findings

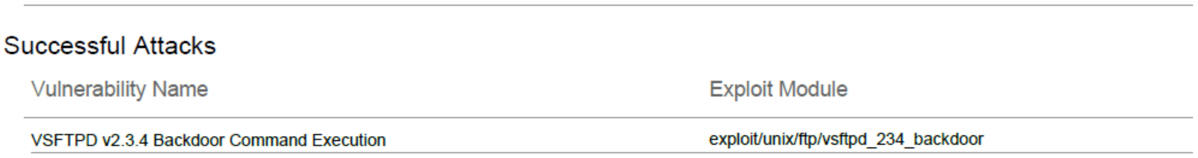
We have successfully completed both Vulnerability Assessment and Penetration Test regarding a Linux Ubuntu server. Here is executive findings that I have provided.

Vulnerability Assessment:

We have found 284 total vulnerabilities. Apart from that 77 were critical, 180 were severe and 27 were low. And we found vulnerable service as DNS, FTP, HTTP, NFS.

Penetration Test:

We Have success fully attack using VSFTTPD v2.3.4 command execution vulnerability using *exploit/unix/ftp/vsftpd_234_backdoor*



Successful Attacks

Vulnerability Name	Exploit Module
VSFTPD v2.3.4 Backdoor Command Execution	exploit/unix/ftp/vsftpd_234_backdoor

7.2 Conclusion:

Vulnerability Assessment and Penetration Testing is a great method for Infrastructure IT security Assessment. To ensure organization IT security we need to conduct VAPT as per organization security policy. In this training I understand the concept behind vulnerability assessment and penetration test.

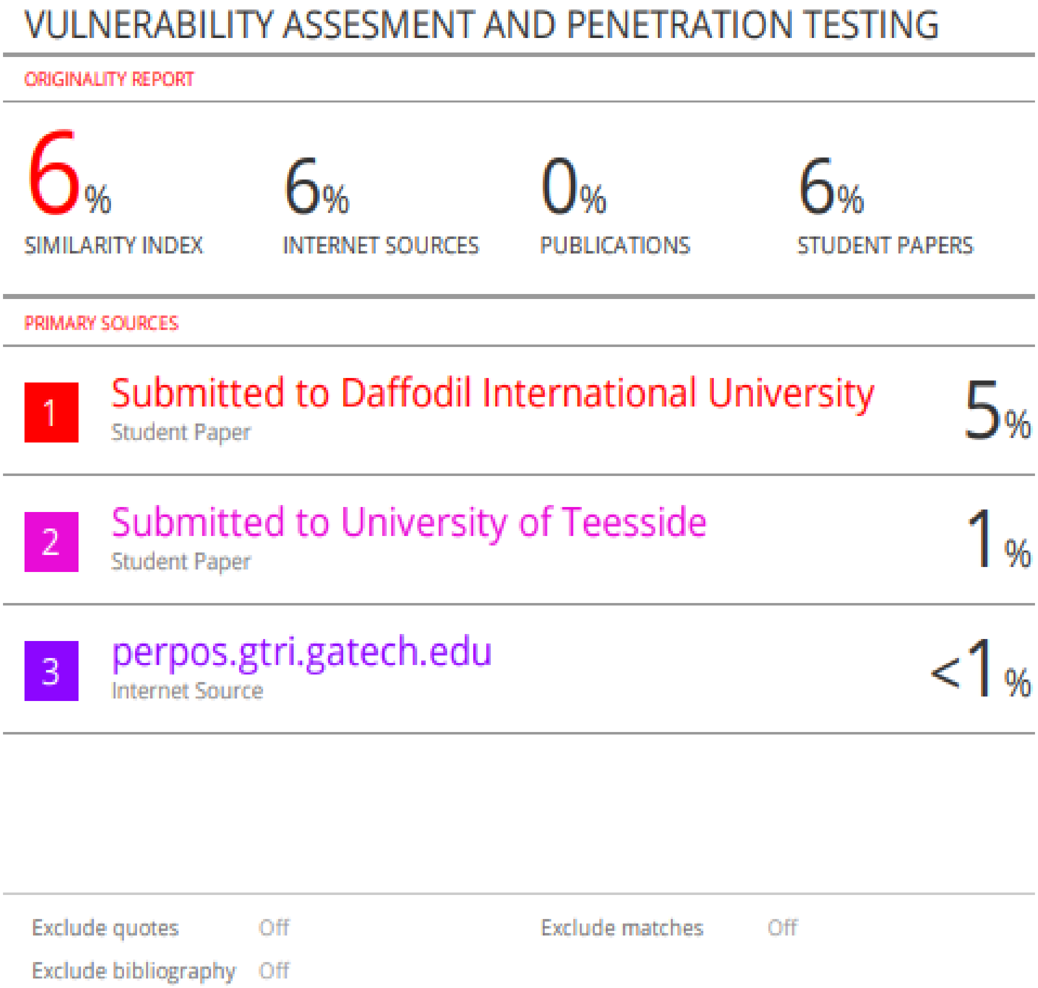
And I have learned how to conduct vulnerability assessment and penetration test using automated enterprise tools from Rapid7.

References

[1] rapid7, “rapid7,” [Online]. Available: <<https://www.rapid7.com/services/security-consulting/penetration-testing-services/>>. [Accessed 6 may 2021].

[2] trustaira, “trustaira,” [Online]. Available: <<https://trustaira.com/#>>. [Accessed 2 may 2021].

[3] tutorials point, “tutorials point,” tutorials point web site, [Online]. Available: <<https://www.tutorialspoint.com/penetration_testing/index.htm>>. [Accessed 15 jun 2021].



VULNERABILITY ASSESMENT AND PENETRATION TESTING

ORIGINALITY REPORT

6%	6%	0%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Daffodil International University Student Paper	5%
2	Submitted to University of Teesside Student Paper	1%
3	perpos.gtri.gatech.edu Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		