One vulnerability to rule them all

Red Mage Testing

Security Assessment Findings Report

Business Confidential

7 April 2021
Project 1

Table of Contents

Confidentiality Statement

This report will contain confidential information. The purpose of the data exposed within if for demonstrating the exploits found during the test and will be used only for that purpose.

Disclaimer

The penetration test referenced in this document takes place between April and May 2021, the devices used during the course of this test have been returned to their previous state and all credentials have been destroyed.

Contact Information

Name	Tittle	Contact Information
Demo Company		
Rando Company	Senior Sec Manager	123-455-1254
Red Mage Testing		
Joseph Karpp	Pen Tester	555-555-5555

Executive Summary

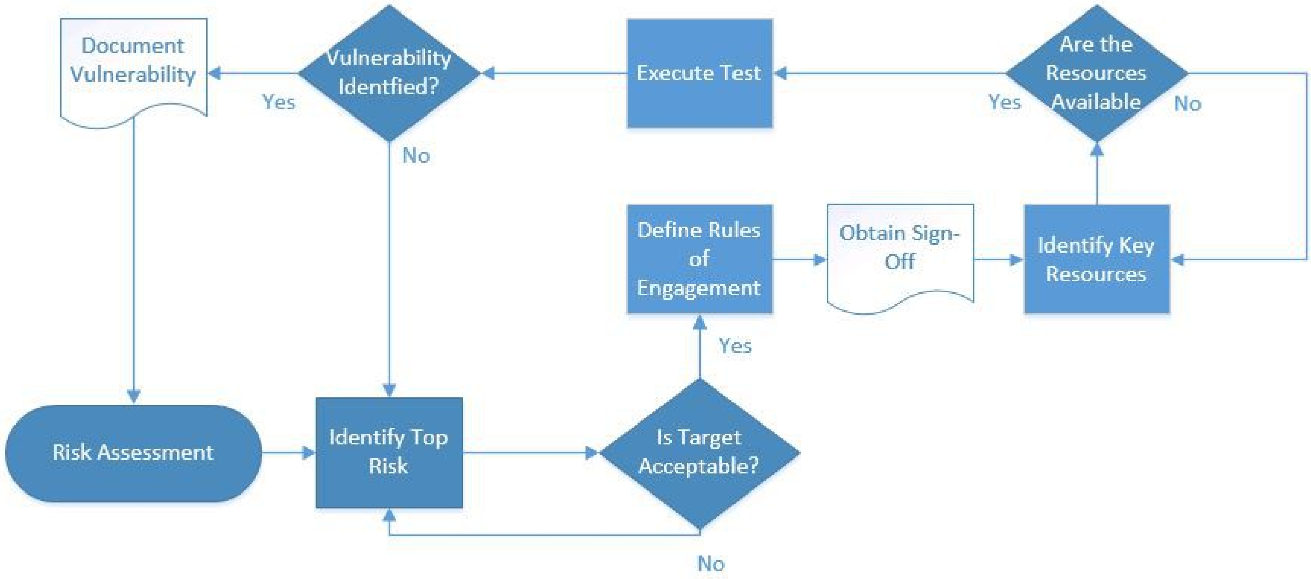
The Penetration test was completed on 11 May 2021, The following findings require immediate remediation and

Attack Summary

The following table describes how RMT gained internal network access, step by step

Step	Action	Recommendation
1	Exploited User Jamie	Increase Password security. Limit Admin rights to require password on Sudo usage.
2	Exploited MySQL database using Jamie user.	Increase sql database security to require password. Salt passwords in the database.
3	Exfultrated password files and cracked them	Was able to exploit SCP to retrieve hard copies of password files

Assessment Overview



Assessment Components

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A Red Mage engineer attempts to gather sensitive information through open source intelligence, including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The engineer also preforms scanning and enumeration to identify Vulnerabilities in hopes of exploitation.

Finding Severity Rating

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible
Moderate	4.0-6.9	Vulnerability exists but are not exploitable or require extra steps such as social engineering. It is advised o form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.0	Vulnerabilities are non-exploitable but would reduce an origination's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during test, strong controls, and additional documentation.

Scope

Assessment	Details
Baseline	Pen test completed to enable remediation of vulnerabilities

-Full scope information provided in “Full findings report”

Scope Exclusions

Unable to exploit main account of hosts to gain access.
Production servers must remain up. (No negative affects from pen test)

Client Allowances

None this will be a black box test.

Security Strengths

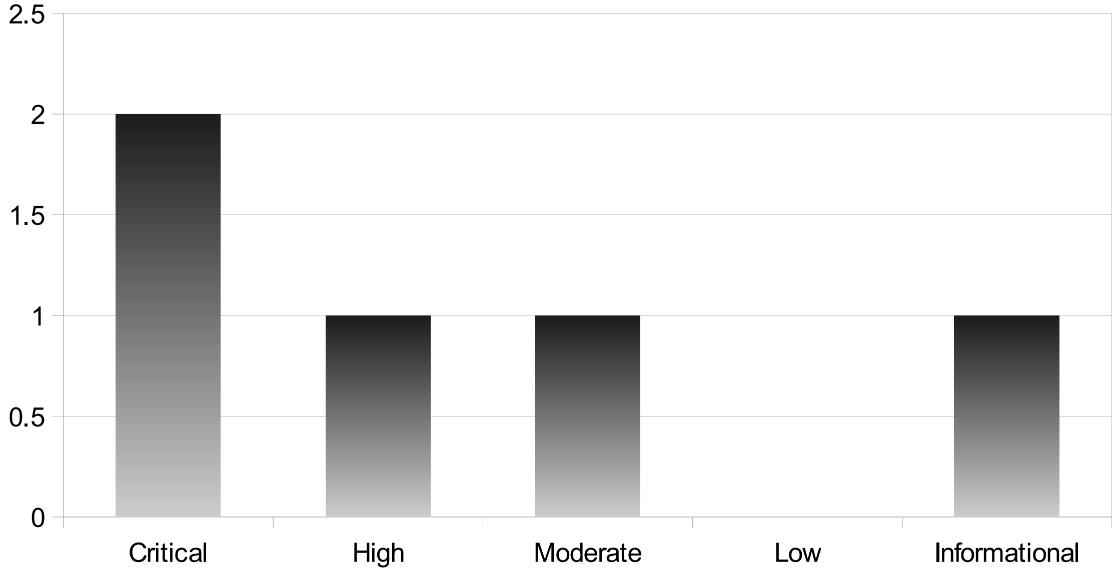
The company exposed there host for the purpose of demonstration. They store passwords in hashed format leaving no plan text passwords stored locally.

Security Weaknesses

The OS was designed with many flaws. The test was conducted exposing several weak ports on services that do not require external access. After exploiting the services the tester was able to create an account with admin rights that required no password to execute privileged commands. After creating this normal looking rogue account the tester was able to exfultrate data to a machine and crack other accounts PII. This is within the scope of the test but these exploits could be used to steal other data as well.

Vulnerabilities by Impact

The following chat illustrates the vulnerabilities found by impact.



External Penetration Test Findings

Tables showing test findings

Critical	
Description	Exploited Jamie User
Impact	Was able to gain access to a privileged user
System	Metasploitable
References	1C
CVSS Score	10

Critical	
Description	Exploited Database
Impact	Exposed passwords in the mysql data base for user accounts and other PII
System	Metasploitable
References	2C
CVSS Score	10

High	
Description	Exposed Ports
Impact	Many ports of non-required sevices exposed.
System	Metasploitable
References	1H
CVSS Score	7.5

Moderate	
Description	No expiration on passwords
Impact	There is currently no password expiration policy that would ensure users reset their passwords regularly.
System	Metasploitable
References	1M
CVSS Score	5

Informational	
Description	OS is designed to be exploited
Impact	The Pen test was conducted on a know weak distrbution of an OS
System	Metasploitable
References	1I
CVSS Score	5

Exploitation Proof of Concept

The providing of findings IE compromised accounts. Also will include statements about what the comprised accounts were used for.

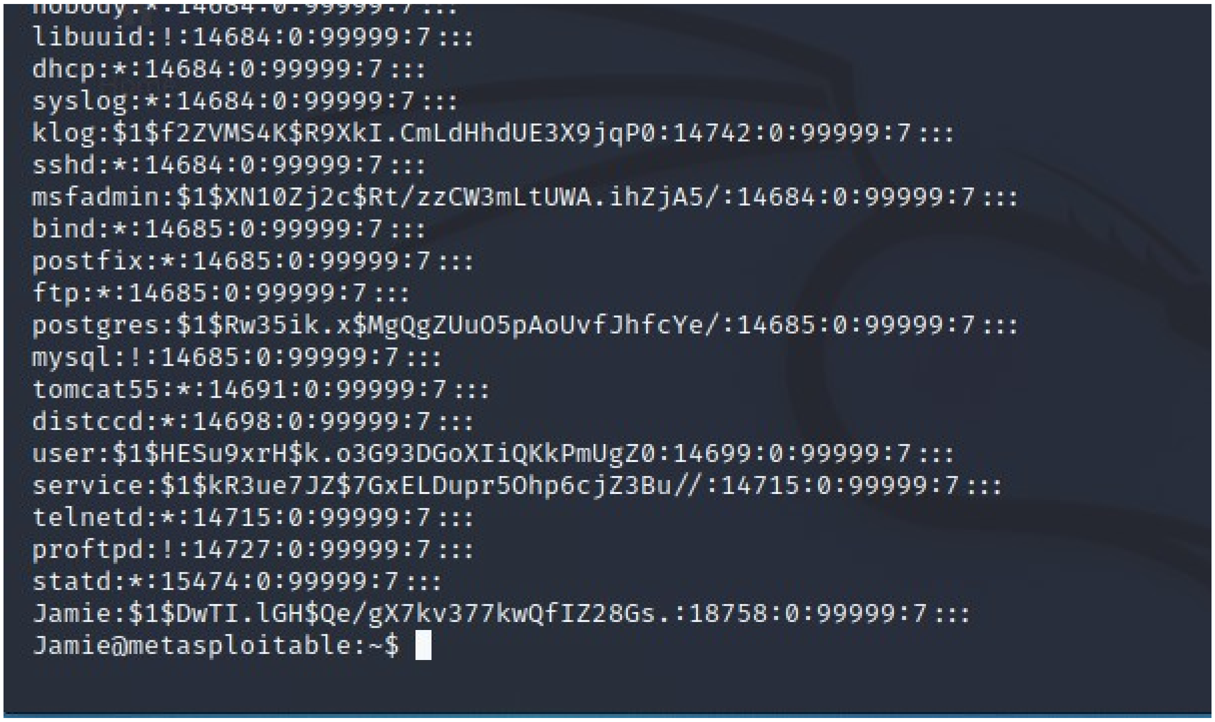
Username	Password
Jamie	1234

Remediation

The below table is for listing suggested fixes and who will be implementing them.

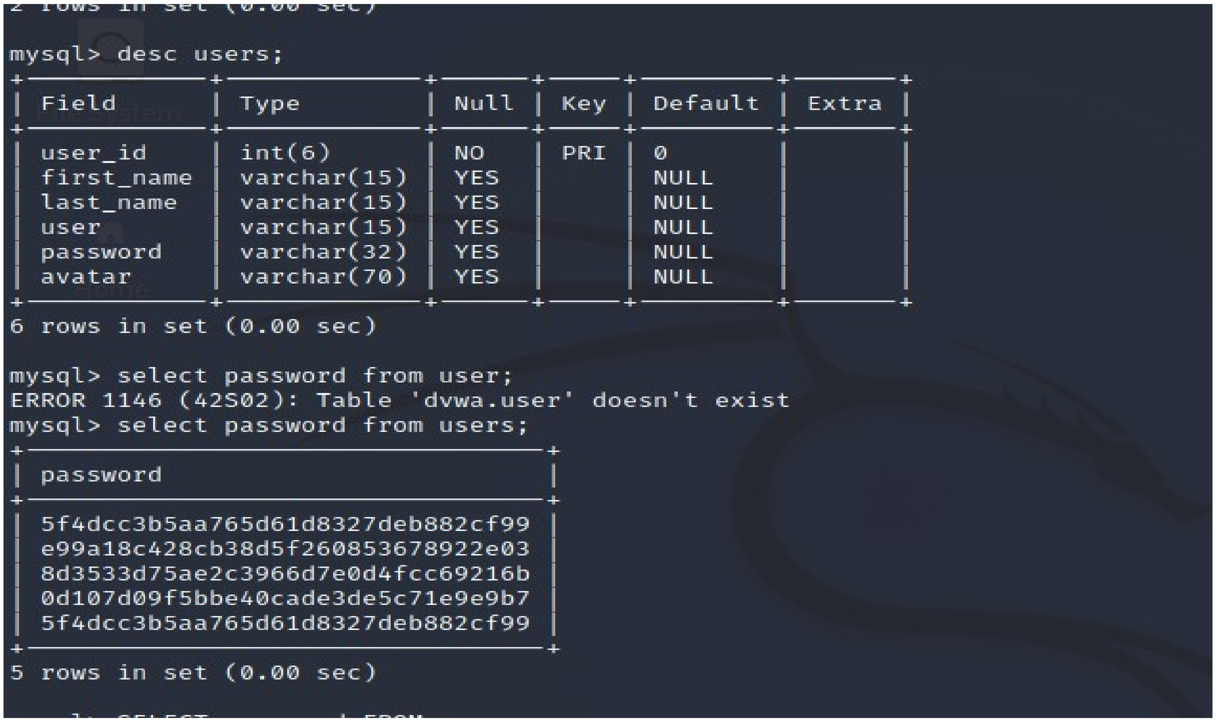
Who	IT department
Vector	Improve Password Security
Action	Will limit the potential to compromise the system

1C



```
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
Jamie:$1$DwTI.lGH$Qe/gX7kv377kwQfIZ28Gs.:18758:0:99999:7:::
Jamie@metasploitable:~$
```

2C

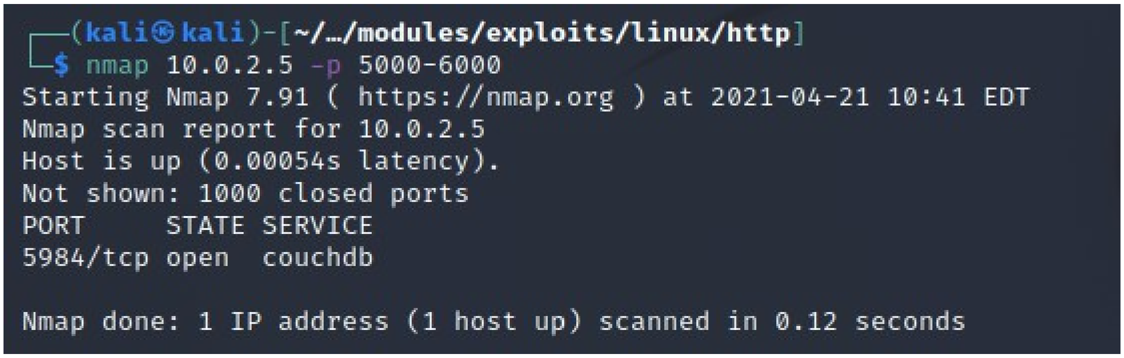


```
2 rows in set (0.00 sec)

mysql> desc users;
+------------+-------------+------+-----+---------+-------+
| Field      | Type        | Null | Key | Default | Extra |
+------------+-------------+------+-----+---------+-------+
| user_id    | int(6)      | NO   | PRI | 0       |       |
| first_name | varchar(15) | YES  |     | NULL    |       |
| last_name  | varchar(15) | YES  |     | NULL    |       |
| user       | varchar(15) | YES  |     | NULL    |       |
| password   | varchar(32) | YES  |     | NULL    |       |
| avatar     | varchar(70) | YES  |     | NULL    |       |
+------------+-------------+------+-----+---------+-------+
6 rows in set (0.00 sec)

mysql> select password from user;
ERROR 1146 (42S02): Table 'dvwa.user' doesn't exist
mysql> select password from users;
+----------------------------------+
| password                         |
+----------------------------------+
| 5f4dcc3b5aa765d61d8327deb882cf99 |
| e99a18c428cb38d5f260853678922e03 |
| 8d3533d75ae2c3966d7e0d4fcc69216b |
| 0d107d09f5bbe40cade3de5c71e9e9b7 |
| 5f4dcc3b5aa765d61d8327deb882cf99 |
+----------------------------------+
5 rows in set (0.00 sec)
```

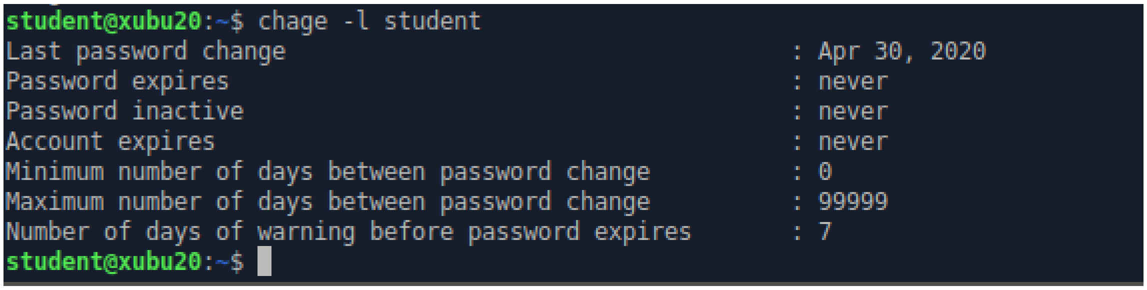
1H



```
┌──(kali㉿kali)-[~/…/modules/exploits/linux/http]
└─$ nmap 10.0.2.5 -p 5000-6000
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-21 10:41 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00054s latency).
Not shown: 1000 closed ports
PORT     STATE SERVICE
5984/tcp open  couchdb

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

1M



```
student@xubu20:~$ chage -l student
Last password change                                    : Apr 30, 2020
Password expires                                        : never
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 99999
Number of days of warning before password expires       : 7
student@xubu20:~$ 
```