

# System Scan Report

Prepared for Hotel Dorsey



**Name:** Susan Reeves

**Team Number:** 4

**Student Number:** 4

## Introduction

Haverbrook Security Lab System Scan for Hotel Dorsey.

For this system scan we will be using Kali (10.4.4.50), a Linux distribution for penetration testing, to scan the company's Linux system (10.4.4.100), which is running network services and database applications. No exploitation will be done on the system and is acknowledged as being strictly unpermitted for this phase of the project. Our team will only be using the tools we have received permission to utilize from Hotel Dorsey to look for information regarding any critical vulnerabilities, banner messages, and application versions.

Our primary tools are Zenmap and OpenVAS. Zenmap is graphical user interface form the Linux nmap utility. It is primarily used for conducting port scanning but can also be used as a limited vulnerability scanner. For more detailed information regarding any potential vulnerabilities the Open Vulnerability Assessment System (OpenVAS) will be used. It is a powerful, dedicated vulnerability scanner. For each vulnerability identified, the report lists a summary, vulnerability detection result, impact, solution, affected software/OS, vulnerability insight, vulnerability detection method, product detection result, and references.

## Target

The first step in scanning the system is to look for open ports on the target machine. Ports are logical or virtual start and stop points on the network that route incoming and outgoing traffic in an organized and efficient way. Each port is associated with specific process or services. Ports are standardized across all network-connected devices, and each port is assigned a number. While IP addresses allow for messages and data to go to specific devices, ports allow for targeting specific services or applications within those devices. The Internet Assigned Numbers Authority (IANA) maintains a full list of port numbers and protocols assigned to them. Below is an Nmap scan performed on the target Linux machine (10.4.4.100)

with the Kali Linux attack machine (10.4.4.50) showing the open ports accepting TCP connections and the corresponding services associated with the port number.

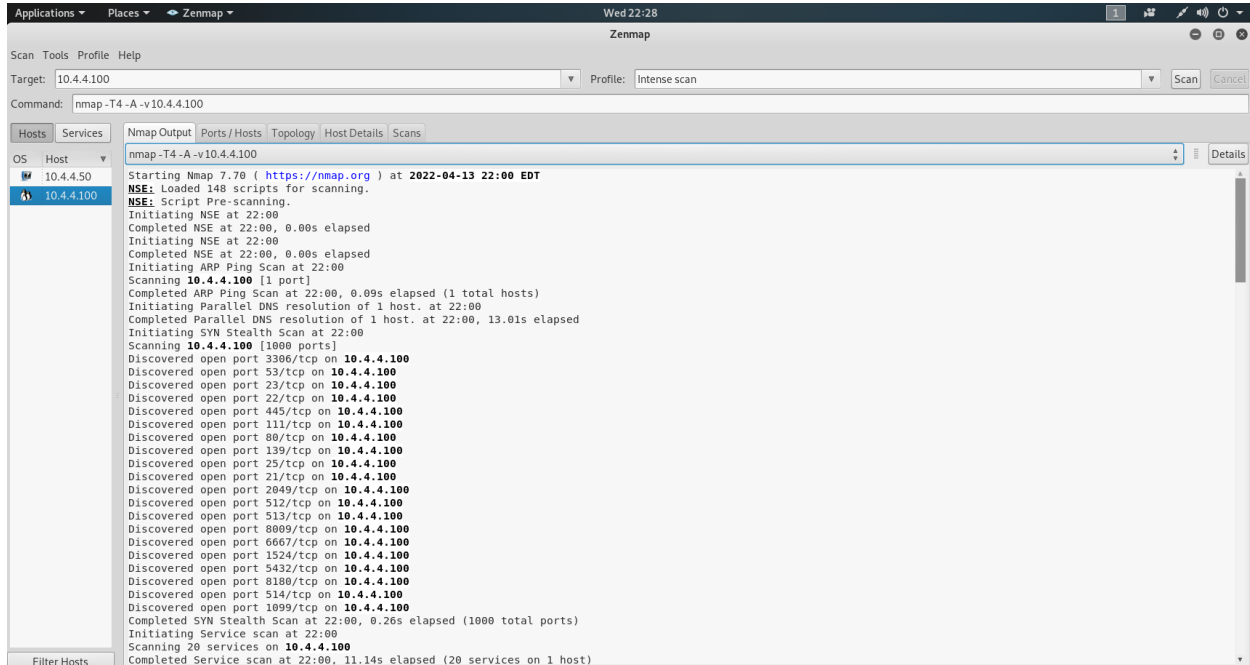
	Hostname	IP Address	MAC Address
<b>Target Machine</b>	Metasploitable2 Linux	10.4.4.100	00:0C:29:06:47:0E (VMware)
<b>Attack Machine</b>	Kali Linux	10.4.4.50	

Nmap 7.70 Nmap scan report for 10.4.4.50		
PORT	SERVICE	FUNCTION
<b>21</b>	File Transfer Protocol (FTP)	File Transfer. Method for transferring files. Access to files can be protected by requiring usernames and passwords. This service allows for dissimilar operating systems to exchange files.
<b>22</b>	Secure Shell (SSH)	Network Management. SSH allows for secure interactive control of remote systems by using RSA public key cryptography for both connection and authentication. It is more secure than Telnet, a similar network management protocol.
<b>23</b>	Remote Terminal Emulation (Telnet)	Network Management. Telnet allows a computer to remotely access another system in the network. Was once widely used for remote management tasks but is rarely used anymore.
<b>25</b>	Simple Mail Transfer Protocol (SMTP)	Email. Protocol used to route email through the internet. It is used between mail servers, all email clients to send mail, and by some email client programs, like Microsoft Outlook, to receive mail from an exchange server.
<b>53</b>	Domain Name System (DNS)	Network Service. DNS is a distributed system service throughout the internet that provides address and name resolution.
<b>80</b>	Hypertext Transfer Protocol (HTTP)	Web Service. An information requesting and responding protocol. Internet browsers and servers use HTTP to exchange files over the internet.
<b>111</b>	rpcbind	Linux utility. Maps universal addresses to Remote Procedure Call (RPC) programs.
<b>139</b>	netbios-ssn	NETBIOS Session Service. Windows machines and other systems running Server Message Blocks (Samba) (SMB) use this service to make TCP connections that form "NetBIOS Sessions" to allow for file sharing.
<b>445</b>	microsoft-ds	Microsoft Directory Services. Replaces the original Windows NetBIOS trio of ports (137-139). It is the preferred port for Windows file sharing.
<b>512</b>	exec	Remote Process Execution. Protocol used to run a program on a remote server as if it was being run on the local machine.
<b>513</b>	login	Remote login via Telnet. An older service for remote administration that was used by Linux machines. Because of security concerns this service has been replaced by slogin and the ssh.
<b>514</b>	shell	Remote Shell. A legacy service that allows for remote connection and control of a server.
<b>1099</b>	rmiregistry	RMI Registry. Houses a directory of available services between Java Virtual Machines.

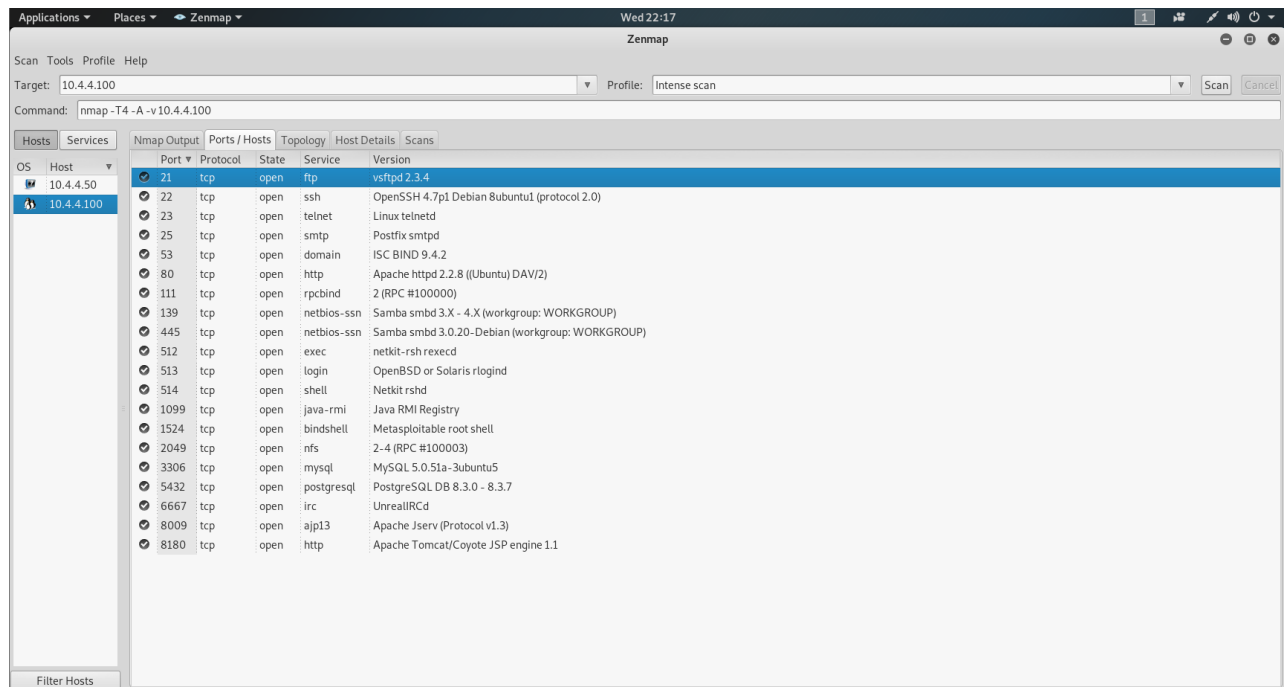
1524	ingreslock	Database Application. Service used to lock parts of an Ingres database.
2049	nfs	Network File System. Allows for remote file system access.
3306	mysql	Database Application. MySQL database server connections. Used to connect with MySQL clients and utilities.
5432	postgresql	PostgreSQL Database Application. PostgreSQL is an open-source object-relational database system that uses and expands upon the SQL language.
6667	irc	Internet Relay Chat. A teleconferencing system that uses a server to provide connections so that clients can communicate with each other via text.
8009	ajp13	Apache JServ Protocol. An enhanced and optimized version of the HTTP protocol that allows the Apache web server to talk to Tomcat for pure Java applications.
8180	unknown	services are "unknown" because they are not listed in <code>nmap's services</code> file, nmap uses that to map port numbers to services.

## Zenmap Scan

The default landing page for the Zenmap results is the “Nmap Output” tab. Depending on the type of scan performed there will be range of actions taken by the nmap tool to scan the system. Every action will be detailed here. For this scan, 148 NSE’s were loaded and performed on the system. It is a dense amount of information. The other tabs, shown below, make sorting the most important information more easily, but reviewing the nmap output is going to give the most detailed information.



The “Ports/Hosts” tab in Zenmap will show the open ports on the system, which protocol it is using (TCP or UDP), the service running on the port, and the service version.



As mentioned above, this tab will give an overview of the ports, services, and versions, but in the nmap output there will be necessary details for accessing the security of the system. One example of many is the FTP Service. The “Ports/Hosts” tab shows limited information.

Nmap Output		Ports / Hosts		Topology	Host Details	Scans
	Port ▼	Protocol	State	Service	Version	
	21	tcp	open	ftp	vsftpd 2.3.4	

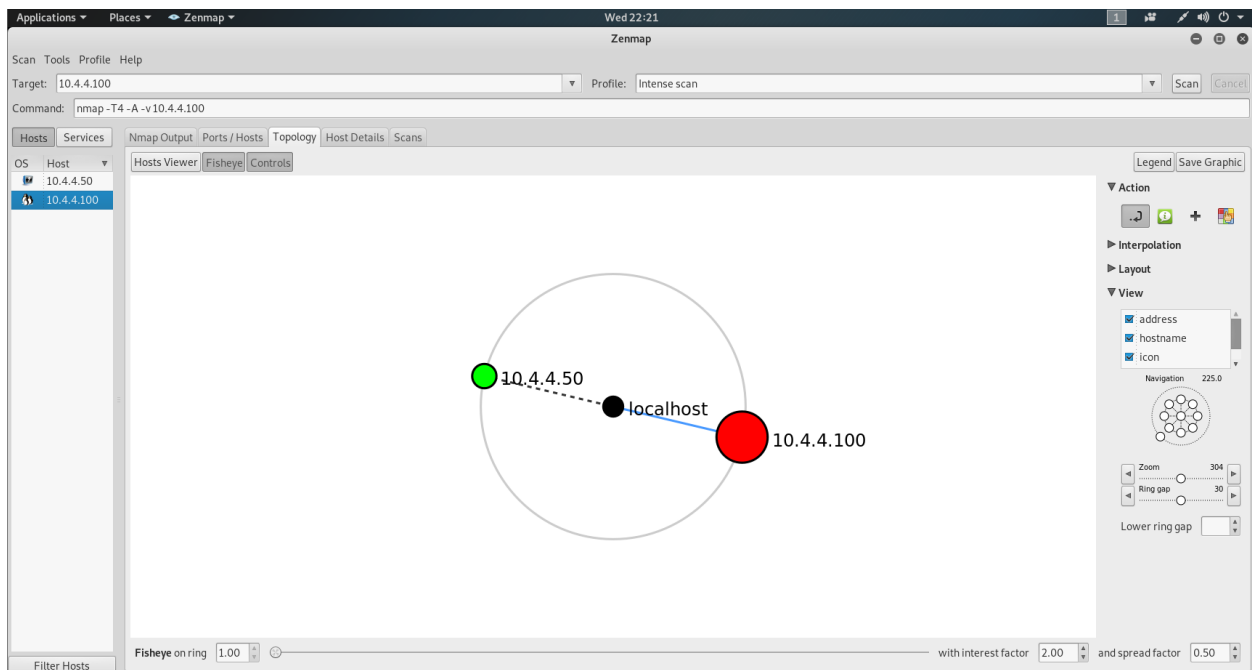
In the “Nmap Output” tab the nmap scan report gives details on the above in addition to the FTP server status and, critically, the fact that the control connection and data connections are both in plain text. The report includes the same level of details for each open port and service. However, it does not alert you to the vulnerabilities nor does it include most known vulnerabilities regarding port services. Zenmap does have vulnerability scanning capabilities, but they are limited. It’s main use for network mapping and port scanning and not vulnerability assessment and management.

```

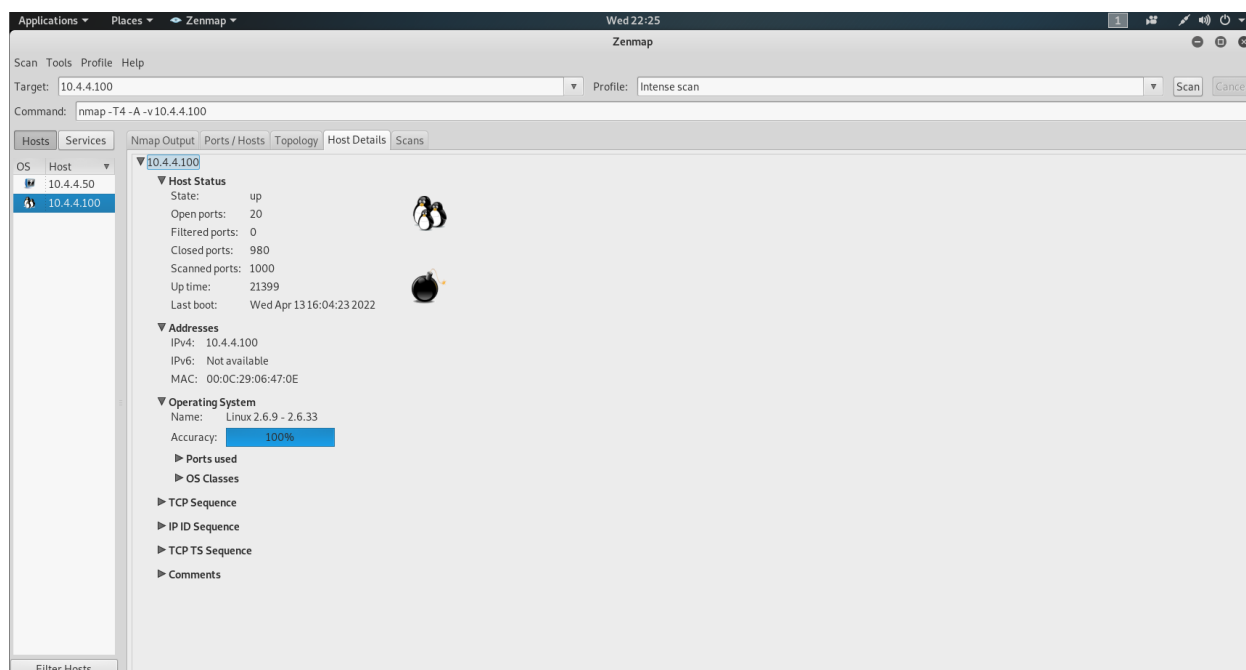
Nmap scan report for 10.4.4.100
Host is up (0.00099s latency).
Not shown: 980 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|   STAT:
|   FTP server status:
|       Connected to 10.4.4.50
|       Logged in as ftp
|       TYPE: ASCII
|       No session bandwidth limit
|       Session timeout in seconds is 300
|       Control connection is plain text
|       Data connections will be plain text
|       vsFTPd 2.3.4 - secure, fast, stable
|_End of status

```

The “Topology” tab gives a graphical map of the network determined by the nmap scan. Here, it shows the connection between the two machines being used in this system scan, The Kali Linux attack machine (10.4.4.50) and the Metasploitable2 Linux target machine (10.4.4.100).



The “Host Details” tab details the Host Status (up or down, number of open ports, number of closed ports, the total number of scanned ports, the up time, and date and time of the last boot), Addresses (IPv4, IPv6, and MAC address), and the Operating System.

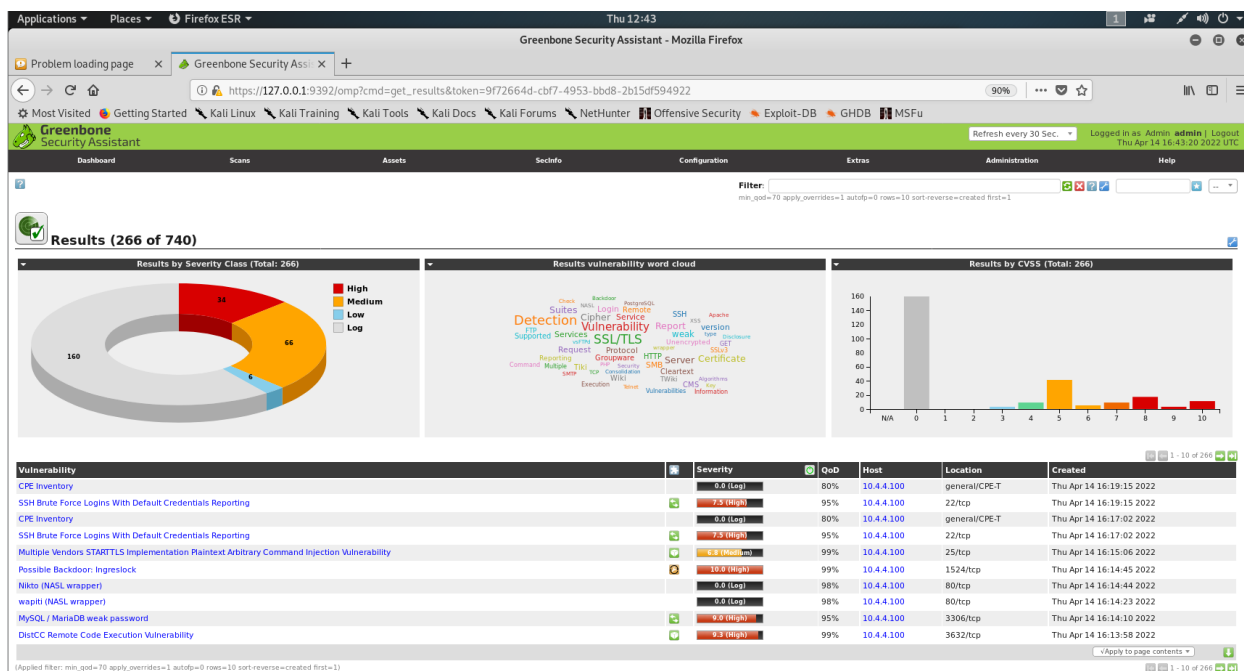


The report does not give any information about potential vulnerabilities explicitly. However, after determining ports, services, and versions consulting known vulnerability repositories can give information about potential vulnerabilities generally associated with the ports and services. Below you will find a table with potential vulnerabilities.

PORT	SERVICE	FUNCTION	POTENTIAL VULNERABILITIES
21	File Transfer Protocol (FTP)	File Transfer. Method for transferring files. Access to files is protected can be protected by requiring usernames and passwords. This service allows for dissimilar operating systems to exchange files.	<i><b>Insecure Protocol:</b> The FTP protocol does <u>not</u> use encryption. All data, including usernames, passwords, and files are sent across the network in clear text.</i>
23	Remote Terminal Emulation (Telnet)	Network Management. Telnet allows a computer to remotely access another system in the network.	Was once widely used for remote management tasks but is rarely used anymore, because it does not use encryption. SSH is a secure alternative to Telnet.
80	Hypertext Transfer Protocol (HTTP)	Web Service. An information requesting and responding protocol. Internet browsers and servers use HTTP to exchange files over the internet.	
512	exec	Remote Process Execution. Protocol used to run a program	<i><b>Insecure Protocol:</b> This service does <u>not</u> encrypt data. Usernames</i>

		on a remote server as if it was being run on the local machine.	<i>and passwords can be viewed with a packet sniffer.</i>
513	login	Remote login via Telnet. An older service for remote administration that was used by Linux machines.	Because of security concerns this service has been replaced by slogin and the ssh.
514	shell	Remote Shell. A legacy service that allows for remote connection and control of a server.	<i><b>Insecure Protocol:</b> Does not provide encryption or require passwords. A secure alternative is Secure Shell (SSH).</i>
1524	ingreslock	Database. Service used to lock parts of an Ingres database.  Ingres is an open-source relational database management system (DBMS) used by enterprises and government applications.	Trojans use this port as a backdoor into a system. By connecting to this port an attacker gains access to a machine and is logged in with all the same rights as the user in which the service is running.
3306	mysql	MySQL database server connections. Used to connect with MySQL clients and utilities.	<i><b>Insecure Protocol:</b> In general, do not leave this port open because it is vulnerable to attack. A more secure method of connecting to a database remotely is with A SSH tunnel. If the port must be used restrict which IP addresses that can access it.</i>
6667	irc	Internet Relay Chat. A teleconferencing system that uses a server to provide connections so that clients can communicate with each other via text.	A plaintext protocol, anyone with access to the network traffic can read the data flowing over IRC. For more security, run IRC while encrypted with TSL/SSL.  IRC commonly used for communication by botnets.
8009	ajp13	Apache JServ Protocol. An enhanced and optimized version of the HTTP protocol that allows the Apache web server to talk to Tomcat for pure Java applications.	CVE-2020-1938 'Ghostcat'
8180	unknown		

Results overview of the OpenVAS full and fast scan on Linux target machine (10.4.4.100) performed by the Kali Linux attack machine (10.4.4.50). Appendix I contains the full scan results produced by OpenVAS.



The OpenVAS scan found 53 vulnerabilities on the Linux target machine (10.4.4.100); 17 potentially high severity, 33 potentially medium severity, and 3 potentially low severity. When available solutions for each are included in the report. These are most often mitigations, but there are some workarounds as well.

... (continued) ...

Service (Port)	Threat Level
6200/tcp	High
512/tcp	High
1524/tcp	High
21/tcp	High
3632/tcp	High
3306/tcp	High
22/tcp	High
80/tcp	High
514/tcp	High
8787/tcp	High

... (continues) ...

Service (Port)	Threat Level
513/tcp	High
5432/tcp	High
general/tcp	High
21/tcp	Medium
22/tcp	Medium
80/tcp	Medium
23/tcp	Medium
445/tcp	Medium
25/tcp	Medium
5432/tcp	Medium
22/tcp	Low
80/tcp	Low
general/tcp	Low



**Port 21/TCP  
File Transfer  
Protocol ( FTP)**

**High (CVSS: 7.5)**

**NVT: vsftpd Compromised Source Packages Backdoor Vulnerability**

<b>Summary</b>	vsftpd is prone to a backdoor vulnerability.
<b>Vulnerability Detection Result</b>	Vulnerability was detected according to the Vulnerability Detection Method.
<b>Impact</b>	Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.
<b>Solution</b>	Solution type: VendorFix The repaired package can be downloaded from the referenced link. Please validate the package with its signature.
<b>Aected Software/OS</b>	The vsftpd 2.3.4 source package is affected.
<b>Vulnerability Detection Method</b>	Details: vsftpd Compromised Source Packages Backdoor Vulnerability

**Port 22/tcp  
Secure Shell (SSH)**

**High (CVSS: 7.5)**

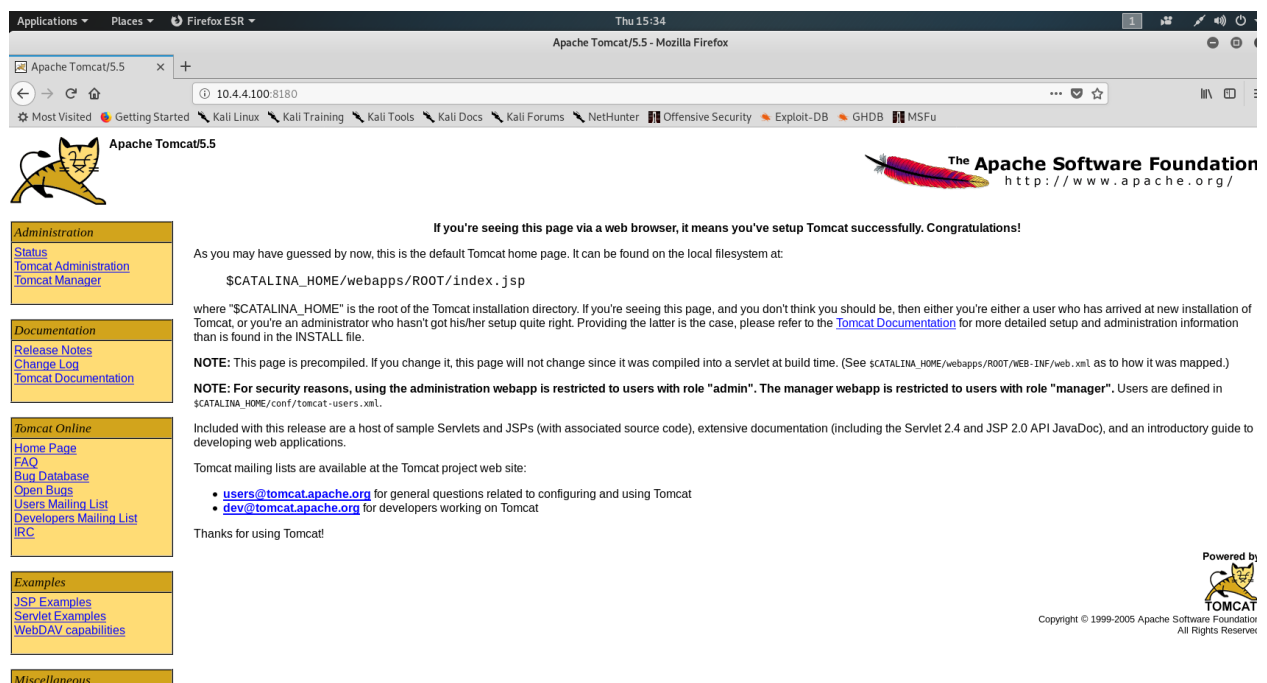
**NVT: SSH Brute Force Logins With Default Credentials Reporting**

<b>Summary</b>	It was possible to login into the remote SSH server using default credentials. As the NVT 'SSH Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such a timeout is reported.
<b>Vulnerability Detection Result</b>	It was possible to login with the following credentials <User>:<Password> msfadmin:msfadmin user:user
<b>Solution</b>	Solution type: Mitigation Change the password as soon as possible.
<b>Vulnerability Detection Method</b>	Try to login with a number of known default credentials via the SSH protocol. Details: SSH Brute Force Logins With Default Credentials Reporting OID:1.3.6.1.4.1.25623.1.0.103239 Version used: \$Revision: 13568 \$

The two tables above detail two of the most critical vulnerabilities on the Linux target machine found during the OpenVAS scan. The first is on Port 21/TCP running the File Transfer Protocol service (FTP) that is used for transferring and accessing files across systems. The OpenVAS scan found that there is a backdoor associated with the system's service version, vsftpd 2.3.4. Backdoors allow threat agents to perform actions on the affected system compromising the confidentiality and integrity of all data associated with the application. The second is on Port 22/TCP running the Secure Shell service (SSH). The scanner was able to login into the remote SSH server using widely known default credentials. The password should be changed as soon as possible to mitigate this vulnerability.

## Open Socket

The initial port scan performed by Zenmap revealed that port 8180 is running an unknown service. The OpenVAS scan was able to identify the service running – Apache Tomcat server. With that limited information a manual connection was made to the IP and 8180 port by opening a browser and enter the IP address followed by a colon and the port number – 10.4.4.100:8180. The browser shows a connection to the Apache Tomcat web server. Tomcat is an open-source web server used to run Java Servlets and Java Server Pages (JSP).





Applications ▾ Places ▾ Firefox ESR ▾ Thu 15:34 Apache Tomcat/5.5 - Mozilla Firefox

Apache Tomcat/5.5 x +

10.4.4.100:8180

Most Visited Getting Started Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFu

 Apache Tomcat/5.5  The Apache Software Foundation <http://www.apache.org/>

**Administration**

- Status
- Tomcat Administration
- Tomcat Manager

**Documentation**

- Release Notes
- Change Log
- Tomcat Documentation

**Tomcat Online**

- Home Page
- FAQ
- Bug Database
- Open Bugs
- Users Mailing List
- Developers Mailing List
- IRC

**Examples**

- JSP Examples
- Servlet Examples
- WebDAV capabilities

**Miscellaneous**

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

`$CATALINA_HOME/webapps/ROOT/Index.jsp`

where "\$CATALINA\_HOME" is the root of the Tomcat installation directory. If you're seeing this page, and you don't think you should be, then either you're either a user who has arrived at new installation of Tomcat, or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, please refer to the [Tomcat Documentation](#) for more detailed setup and administration information than is found in the INSTALL file.

**NOTE:** This page is precompiled. If you change it, this page will not change since it was compiled into a servlet at build time. (See `$CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml` as to how it was mapped.)


**NOTE:** For security reasons, using the administration webapp is restricted to users with role "admin". The manager webapp is restricted to users with role "manager". Users are defined in `$CATALINA_HOME/conf/tomcat-users.xml`.

Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web applications.

Tomcat mailing lists are available at the Tomcat project web site:

- [users@tomcat.apache.org](mailto:users@tomcat.apache.org) for general questions related to configuring and using Tomcat
- [dev@tomcat.apache.org](mailto:dev@tomcat.apache.org) for developers working on Tomcat

Thanks for using Tomcat!

Powered by  TOMCAT

Copyright © 1999-2005 Apache Software Foundation All Rights Reserved

```

Applications ▾ Places ▾ Terminal ▾ Thu 15:43
root@kali: ~
File Edit View Search Terminal Help

msf5 > search tomcat

Matching Modules
=====
#  Name                                     Disclosure Date Rank Check Description
-  -
0  auxiliary/admin/http/tomcat_administration  normal Yes Tomcat Administration Tool
Default Access
1  auxiliary/admin/http/tomcat_utf8_traversal  2009-01-09 normal Yes Tomcat UTF-8 Directory Traversal Vulnerability
2  auxiliary/admin/http/trendmicro_dlp_traversal  2009-01-09 normal Yes TrendMicro Data Loss Prevention 5.5 Directory Traversal
3  auxiliary/dos/http/apache_commons_fileupload_dos  2014-02-06 normal No Apache Commons FileUpload and Apache Tomcat DoS
4  auxiliary/dos/http/apache_tomcat_transfer_encoding  2010-07-09 normal No Apache Tomcat Transfer-Encoding Information Disclosure and DoS
5  auxiliary/dos/http/hashcollision_dos  2011-12-28 normal No HashTable Collisions
6  auxiliary/scanner/http/tomcat_enum  normal Yes Apache Tomcat User Enumeration
7  auxiliary/scanner/http/tomcat_mgr_login  normal Yes Tomcat Application Manager Login Utility
8  exploit/linux/http/cisco_prime_inf_rce  2018-10-04 excellent Yes Cisco Prime Infrastructure Unauthenticated Remote Code Execution
9  exploit/multi/http/struts2_namespace_ognl  2018-08-22 excellent Yes Apache Struts 2 Namespace Redirect OGNL Injection
10 exploit/multi/http/struts2_namespace_ognl  2014-02-06 normal No Apache Struts 2 Namespace Redirect OGNL Injection

```

The Metasploit Framework offers several tools for penetration testing. It is advised that if there are corresponding modules present in the Metasploit Framework Console, msfconsole, that there easily accessible exploits available for even the most inexperienced hackers to exploit your system. A search in the msfconsole reveal that there 19 exploitation modules available for the Apache Tomcat web server ranging in potential severity from high to low. The ease of use and availability of these modules are a pressing security issue that needs to be addressed.

## Recommendations

An amendment to the existing contract between Haverbrook Security Lab and Hotel Dorsey to perform a full penetration test of systems is highly recommended. The only true way to know which vulnerabilities are in a network is to have them exploited. Vulnerability scanners look for the potential for threat. This means that there are false positives returned quite often. Exploits will reveal which vulnerabilities exist. This will require a team of penetration testers to effectively and efficiently complete. Haverbrook Security Lab will be able to assess and improve the security posture for your organization. There are many critical vulnerabilities on just this one system. If the security posture isn't thoroughly analyzed, tested, and improved Hotel Dorsey may encounter ransomware attacks, consumer information data leaks that will damage the business reputation and trust between Hotel Dorsey and past/present/future clients.

## References

[1] "Chapter 4. Port Scanning Overview | Nmap Network Scanning," *nmap.org*.  
<https://nmap.org/book/port-scanning.html>

[2] "Chapter 5. Port Scanning Techniques and Algorithms | Nmap Network Scanning," *nmap.org*.  
<https://nmap.org/book/scan-methods.html>.

[3] "Chapter 15. Nmap Reference Guide | Nmap Network Scanning," *Nmap.org*, 2020.  
<https://nmap.org/book/man.html#man-description>

[4] "The Ultimate Guide to Vulnerability Scanning," *www.intruder.io*.  
<https://www.intruder.io/guides/the-ultimate-guide-to-vulnerability-scanning>