Penetration Test Summary

Qi Mao

4/28/20

Summary of Findings

This table is followed by a detailed breakdown outlining each category.

Vulnerabilities tallied by Risk rating			
Vulnerabilities	**High**	**Medium**	**Low**
Apache Tomcat Default Files		√	
Unencrypted Telnet Server		√	
mysql-dfsg-5.0-5.1 vulnerabilities	√		
Weak Debian OpenSSH Keys in ~/.ssh/authorized_keys	√		
samba vulnerability	√		
Bind Shell Backdoor Detection	√		
NFS Exported Share Information Disclosure	√		
VNC Server 'password' Password	√		
SMTP Service STARTTLS Plaintext Command Injection		√	
HTTP TRACE / TRACK Methods Allowed		√	

Apache Tomcat Default Files

- The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.

		Consequence Categories			
		Insignificant Consequences	Significant Consequences	Serious Accident	Major Accident
Likelihood Categories	Frequent				
	Probable				√
	Improbable				
	Very Improbable				

Unencrypted Telnet Server

- Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

		Consequence Categories			
		Insignificant Consequences	Significant Consequences	Serious Accident	Major Accident
Likelihood Categories	Frequent				
	Probable			√	
	Improbable				
	Very Improbable				

mysql-dfsg-5.0-5.1 vulnerabilities

- host is missing one or more security-related patches.

		Consequence Categories			
		Insignificant Consequences	Significant Consequences	Serious Accident	Major Accident
Likelihood Categories	Frequent				√
	Probable				
	Improbable				
	Very Improbable				

Weak Debian OpenSSH Keys in ~/.ssh/authorized_keys

- The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL. This problem does not only affect Debian since any user uploading a weak SSH key into the ~/.ssh/authorized_keys file will compromise the security of the remote system. An attacker could try a brute-force attack against the remote host and logon using these weak keys.

		Consequence Categories			
		Insignificant Consequences	Significant Consequences	Serious Accident	Major Accident
Likelihood Categories	Frequent				√
	Probable				
	Improbable				
	Very Improbable				

samba vulnerability

- Brian Gorenc discovered that Samba incorrectly calculated array bounds when handling remote procedure calls (RPC) over the network. A remote, unauthenticated attacker could exploit this to execute arbitrary code as the root user.

		Consequence Categories			
		Insignificant Consequences	Significant Consequences	Serious Accident	Major Accident
Likelihood Categories	Frequent				√
	Probable				
	Improbable				
	Very Improbable				

Bind Shell Backdoor Detection

- A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

		Consequence Categories			
		Insignificant Consequences	Significant Consequences	Serious Accident	Major Accident
Likelihood Categories	Frequent				√
	Probable				
	Improbable				
	Very Improbable				

NFS Exported Share Information Disclosure

- At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

		Consequence Categories			
		Insignificant Consequences	Significant Consequences	Serious Accident	Major Accident
Likelihood Categories	Frequent				√
	Probable				
	Improbable				
	Very Improbable				

VNC Server 'password' Password

- The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

		Consequence Categories			
		Insignificant Consequences	Significant Consequences	Serious Accident	Major Accident
Likelihood Categories	Frequent				√
	Probable				
	Improbable				
	Very Improbable				

SMTP Service STARTTLS Plaintext Command Injection

- The remote SMTP service contains a software flaw in its STARTTLS implementation that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase. Successful exploitation could allow an attacker to steal a victim's email or associated SASL (Simple Authentication and Security Layer) credentials.

		Consequence Categories			
		Insignificant Consequences	Significant Consequences	Serious Accident	Major Accident
Likelihood Categories	Frequent				
	Probable		√		
	Improbable				
	Very Improbable				

HTTP TRACE / TRACK Methods Allowed

- The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

		Consequence Categories			
		Insignificant Consequences	Significant Consequences	Serious Accident	Major Accident
Likelihood Categories	Frequent				
	Probable				
	Improbable		√		
	Very Improbable				

Risk Assessment Matrix

Vulnerabilities tallied by Risk rating			
Category	**High**	**Medium**	**Low**
configuration management	√		
patch management		√	
encryption	√		

recommendation to fix:

For configuration management

- Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.
- Disable the Telnet service and use SSH instead.
- Remove all the offending entries from ~/.ssh/authorized_keys.
- Verify if the remote host has been compromised and reinstall the system if necessary.
- Configure NFS on the remote host so that only authorized hosts can mount its remote shares.
- Disable TRACE and TRACK HTTP methods. Refer to the plugin output for more information.

For path management:

- Update the affected packages and install security-related patches.
- Update the affected samba package.

For encryption:

- Secure the VNC service with a strong password.

Comparative Analysis

I think this environment is very weak. The impact of most vulnerabilities is very serious and can be easily exploited. Also, the host's shell is listening on the remote port without any authentication. The host is most likely already compromised. From the previous table, we can find that the threat of most vulnerabilities is very serious, and more than half of the vulnerabilities can be directly used to exploit. The security posture rating of this environment is below the average.