Kaeyln security inc

Michele G. (CyberSecurity expert)

Kaelyn Security INC

www.kaelynsecinc.com Gkae@kaesec.net

Penetration Testing Report for target machine “Metasploitable 2”

Table of Contents

Introduction

Metasploitable2 is a purposely vulnerable virtual machine designed for security testing, specifically for penetration testing and vulnerability assessment. It's a freely available open-source project that provides a simulated environment with intentionally exploitable vulnerabilities. This environment allows cybersecurity professionals, researchers, and students to practice and hone their skills in identifying, exploiting, and securing systems against various common security threats. Metasploitable2 includes a range of vulnerabilities found in real-world systems, making it a valuable tool for learning about cybersecurity principles and techniques in a safe and controlled setting.

After setting up Metasploitable2, conducting the security test took approximately two hours. During this time, various scanning and exploitation tools were employed to assess the vulnerabilities present in the system. The testing process involved identifying weaknesses such as outdated software versions, misconfigured services, default credentials, and known exploits.

Additionally, it's essential to note that the vulnerabilities found during the security assessment of Metasploitable2 are valid as of May 8th, the day when the scan was conducted.

Identified Vulnerabilities

The vulnerabilities listed below are arranged in order of severity, with the most critical issues appearing first. This prioritization helps focus attention on addressing the most pressing security concerns promptly. By addressing high-severity vulnerabilities first, organizations can mitigate the most significant risks to their systems and data, thereby enhancing overall security posture and resilience against potential cyber threats.

VNC Server 'password' Password (Critical)

CVSS V3.0 score: 10.0

The VNC server on the remote host is secured with a weak password, specifically 'password'. This vulnerability allows a malicious actor to authenticate using this weak password. An attacker could exploit this remotely and without authentication, potentially gaining control of the system. To mitigate this risk, it's crucial to secure the VNC service with a strong, hard-to-guess password.

Suggested solution:

Change the password and secure the VNC service with a stronger password.

UnrealIRCd Backdoor Detection (Critical)

CVSS V3.0 score: 10.0

The remote IRC server is a version of UnrealIRCd with a malicious backdoor that allows an attacker to execute arbitrary code on the affected host.

Suggested solution:

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

Useful links:

https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor/

https://seclists.org/fulldisclosure/2010/Jun/277

NFS Exported Share Information Disclosure (Critical)

CVSS V3.0 score: 10.0

It is possible to access NFS shares on the remote host, an attacker may be able to leverage this to read (and possibly write) files on remote host.

Suggested solution:

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Debian OpenSSH/OpenSSL Package Random Number Generator weakness (SSL check) (Critical)

CVSS V3.0 score: 10.0

The remote SSL certificate uses a weak key.

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Suggested solution:

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (Critical)

CVSS V3.0 score: 10.0

The remote SSH host keys are weak.

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

Suggested solution:

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Useful links:

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

Unix Operating System Unsupported Version Detection (Critical)

CVSS V3.0 score: 10.0

The operating system running on the remote host is no longer supported.

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Suggested solution:

Upgrade to a version of the Unix operating system that is currently supported.

Apache Tomcat SEoL (<= 5.5.x) (Critical)

CVSS V3.0 score: 10.0

According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Suggested solution:

Upgrade to a version of Apache Tomcat that is currently supported.

Useful links:

https://tomcat.apache.org/tomcat-55-eol.html

SSL Version 2 and 3 Protocol Detection (Critical)

CVSS V3.0 score: 9.8

The remote service encrypts traffic using a protocol with known weaknesses.

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Suggested solution:

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.2 (with approved cipher suites) or higher instead.

Useful links:

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf

https://www.openssl.org/~bodo/ssl-poodle.pdf

https://www.imperialviolet.org/2014/10/14/poodle.html

Bind Shell Backdoor Detection (Critical)

CVSS V3.0 score: 9.8

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.

Suggested solution:

Verify if the remote host has been compromised, and reinstall the system if necessary.

Another solution could be to kill the process and to remove it from the host machine

Apache Tomcat AJP Connector Request Injection (Ghostcat) (Critical)

CVSS V3.0 score: 9.8

There is a vulnerable AJP connector listening on the remote host.

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Suggested solution:

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

Useful links:

https://access.redhat.com/security/cve/CVE-2020-1745

https://access.redhat.com/solutions/4851251

In conclusion, the vulnerability assessment conducted on the Metasploitable2 machine revealed several significant vulnerabilities that could be exploited by malicious attackers to compromise the system. Through in-depth analysis of the identified vulnerabilities, solutions and countermeasures have been proposed to mitigate the security risks. However, it is important to emphasize that cybersecurity is a continuous and evolving process, therefore it is advisable to implement constant monitoring and regular updates to ensure effective protection against current and future threats.

Signature

Michele G