Penetration Testing Project

Keerthimol Veeralasseril Nadesan

Date: 06.08.2024

Table of Contents

Executive Summary

This project report outlines the results of a penetration testing exercise conducted on the Metasploitable2 virtual machine using Kali Linux. The primary objective of this project was to identify and assess potential vulnerabilities within the target system, focusing on both web and network vulnerabilities.

Scope of Work: The project was divided into two main parts:

- **Part A** involved scanning and identifying web and network vulnerabilities using tools like Nikto and OpenVAS

- **Part B** focused on detailed observations on the vulnerabilities and OWASP Top 10 categorizations of the vulnerabilities.

Methodology: The testing process involved setting up the necessary environment with Metasploitable2 and Kali Linux virtual machines. Scans were performed using tools like Nikto for web vulnerabilities and OpenVAS for network vulnerabilities. The IP addresses of the target machines were determined, and specific tools were used to detect, analyze, and exploit identified vulnerabilities.

Assumptions: The testing was conducted under controlled conditions using a vulnerable machine designed for educational purposes. It is assumed that the vulnerabilities found would be present in a real-world scenario on an unpatched system.

Resources: Key resources included the Metasploitable2 virtual machine, Kali Linux, Nikto for web vulnerability scanning, and OpenVAS for network vulnerability analysis.

Risk Rating: The vulnerabilities identified varied in severity. For instance, the clickjacking vulnerability was rated as medium risk due to its potential high impact, while the network vulnerabilities, such as the DistCC RCE and vsftpd backdoor, were rated as high risk due to their ease of exploitation and the potential for severe system compromise.

Strategic Recommendation: To mitigate the risks identified, it is recommended to implement security best practices, such as enabling proper HTTP headers like X-Frame-Options and Content Security Policy (CSP), securing network services with the latest patches, and continuously monitoring for vulnerabilities using advanced security tools. These steps will help in reducing the likelihood of successful attacks and protecting sensitive data from unauthorized access.

Part A – Summary of Scans and Findings

In this project, both web and network vulnerabilities were assessed using the Metasploitable2 virtual machine as the target. The analysis was divided into two parts:

Web Vulnerabilities

Using the Nikto web scanner, several web vulnerabilities were identified:

- **Clickjacking**: A medium-risk vulnerability where attackers can trick users into clicking on hidden elements, leading to unauthorized actions.

- **Directory Browsing**: The server allowed browsing of directories, exposing sensitive files that could be accessed by attackers.

Network Vulnerabilities

The focus then shifted to network vulnerabilities using the OpenVAS scanner:

- **DistCC Remote Code Execution (RCE)**: A high-risk vulnerability in the DistCC service that could allow attackers to execute arbitrary code on the server, potentially compromising the entire system.

- **vsftpd Backdoor**: Another high-risk vulnerability, where a backdoor in the vsftpd service enabled unauthorized remote access, posing a serious threat to system security.

Together, these findings underscore the importance of securing both web applications and network services. Proper mitigation strategies, including patching, disabling unnecessary services, and implementing security best practices, are crucial to protecting against these vulnerabilities.
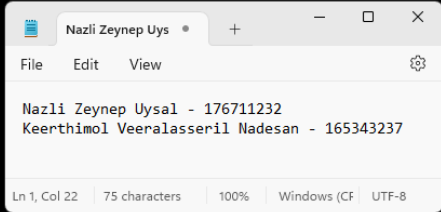
Preparing for the scan:

We conducted our penetration testing on Metasploitable2 machine using Kali Linux VM. First, found the IP address of Metasploitable 2 using the "ifconfig" command. The IP address was 192.168.214.128.

Figure 1 IP Address of Metasploitable2

We returned to our Kali machine and using Metasploitable's IP address we started our Nikto scan.

Nikto is an open source, command line web vulnerability scanner. Nikto already comes preinstalled in Kali Linux, so we used this tool to find the web vulnerabilities.

Figure 2 Nikto Scan of Metasploitable2

Part A Finding Details:

Web Vulnerability 1:

FD1.3.1. Finding Name

CWE-1021: Improper Restriction of Rendered UI Layers or Frames

FD1.3.2. Affected Resource

Apache/2.2.8 (Ubuntu) DAV/2 web server. Mutillidae web page in Metasploitable2.

FD1.3.3. Method of Finding

We found the Metasploitable2's IP address by using the "ifconfig" command and then we used Nikto web scanner to scan Metasploitable2 virtual machine.

FD1.3.4. Description

The description in the Nikto result revealed that "anti-clickjacking X-Frame-Options header is not present". The X-Frame-Options here is a HTTP response header is used to indicate whether a browser is allowed to render a page inside a frame or iframe. And clickjacking is a malicious technique where a web user is deceived into clicking something other than they believe that they are interacting with. This is done by the attacker by using transparent layers in the website UI.

In this vulnerability the web application does not restrict or incorrectly restrict frame objects or UI layers that belong to another application or domain, which can lead to user confusion about which interface the user is interacting with. This is a medium risk level vulnerability with a high impact. It has high impact because the user can click the dangerous object that could lead them into downloading a malicious payload.

```
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
```

Figure 3 Clickjacking Vulnerability found

FD1.3.5. Exploitation

We identified this vulnerability from the Nikto results. There are ways to test for clickjacking. One of the ways is by checking the frame restrictions. Other way is by creating a test web page and testing if the target site's link inserted in the inline frame in the HTML code can be loaded or not. If it loads into the frame, then the site is vulnerable to clickjacking attacks. Another way to test for clickjacking is by using Burp Suite.

1. Load the web page in the Burp Suite, Go to the Proxy HTTP history tab.
2. Right click on the request to test and click active scan.
3. Go to Burp dashboard and review the issue activity log to see if there are any "framable" responses.

If there are frameable responses the web page is vulnerable to clickjacking.

FD1.3.6. Impact

Attackers can trick users into performing actions that are masked and hidden form the user's view. Impact varies depending on the function of the hidden application. For example, the attacker can build a website with a "Free IPhone" button and the underneath it there would be a button that has a bank transfer action that sends money to the attacker's account. The user can be tricked into clicking the free IPhone button thinking that they are safe.

FD1.3.7. Likelihood

Likelihood depends on several factors including the security posture of the website and the awareness of the user. The likelihood on Apache 2.2.8 server is high because it lacks X-Frame-Options header. Implementing X-Frame-Options and CSP(content security policy) headers while using modern web development practices that have built in anti-clickjacking defense will decrease the likelihood of this attack.

FD1.3.8. Risk

Many of websites still do not implement X-Frame-Options or Content Security Policies so this makes them vulnerable. Clickjacking attacks are relatively easy to execute and there are tools for attackers to use. Since this attack includes user input, the risk rating depends on the level of awareness of the user as well. Most people lack tech literacy, and they click on unsafe links and buttons. This could lead to other situations such as victims losing money, data and other private information.

FD1.3.9. Recommendations to fix

Implementing X-Frame-Options and CSP with the frame-ancestors directive will fix the issue with this vulnerability. The Use of X-Frame-Options allows web developers to restrict the usage of overlays, frames or iFrames. Using this option the developer can indicate which domains can frame the content of the web page.

Another option is to use a "frame-breaker" script for each page that should not be framed. This is particularly helpful for legacy browsers that do not support X-Frame-Options. Unfortunately,

this option was bypassed by attackers because it does not account for multiple nested frames that can be presented to the user.

Web Vulnerability 2

FD1.3.1. Finding Name

CVE-2023-47612 / CWE-552: Files or Directories Accessible to External Parties

FD1.3.2. Affected Resource

/phpinfo.php on Metasploitable virtual machine.

FD1.3.3. Method of Finding

In the first step we found the IP address of Metasploitable virtual Machine using the command "ifconfig" and the IP address is 192.168.214.128. To find the we server vulnerabilities we used the web-server vulnerability scanner **Nikto**. Nikto is an open-source web vulnerability scanner. It can perform comprehensive security tests against web server and checks for over 6700 potentially dangerous files/programs, outdated versions of web server software. Nikto is preinstalled in KaliLinux VM.

The command used to scan the web server at the specified IP address is,
nikto -h 192.168.214.128

The web server vulnerability **CVE-2024-2052** was found in the nikto scan on Metasploitable VM.

FD1.3.4. Description

The description of the vulnerability **CVE-2024-2052** mentioned in nikto scanning is,

/phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.

The vulnerability **CVE-2024-2052** allows files or directories accessible to external users without permission. This vulnerability allows unauthorized attackers to exfiltrate and download sensitive files and logs without logging in. The hackers can do this by changing the URL to point to a different file location. This poses severe security risk by allowing unauthorized users to access sensitive information which leads to data breaches. Also, affect the integrity and confidentiality of the data.
The severity rating of the vulnerability is high since it leads to unauthorized access to sensitive information.

FD1.3.5. Exploitation

The vulnerability in '/phpinfo.php' was found in the nikto scan, indicating the accessibility of sensitive information. There are ways to exploit this vulnerability, one of the ways is,

- Access the file 'phpinfo.php' by navigating to the IP address of metasploitable through the web browser. For example,

'http://<metasplotable-ip>/phpinfo.php'

Check the if the page provides sensitive information regarding the server's PHP configuration, including system details and environment variables.

- Manipulate the URL to access the hidden files on the server to find the sensitive files which includes the password file.

For example,

http://<metasploitable-ip>/../../../../../etc/passwd to move out of the web folder and into the system folders.

If the server allows to download the sensitive files which contains the password it means that website is not secure and is vulnerable.

- Further exploitation is possible by accessing the different path to

to see if more data can be accessed or if other vulnerabilities can be exploited.

FD1.3.6. Impact

The impact of CVE 2024-2052 is severe because accessing the '/phpifo/php' leads to data breaches where sensitive information's such as logs, configuration files, or personal data can be accessed and stolen. The integrity of the data is compromised completely which lead to intellectual property theft. The hackers can further exploit other files by the changing the file location results in complete devastation of system.
The organizations may suffer reputational damage due to sensitive data exposure. Ultimately the data breach result in significant financial loss.

FD1.3.7. Likelihood

The likelihood of exploitation is High, as the vulnerability can be easily identified and exploited by attackers using simple URL manipulation techniques.

FD1.3.8. Risk

The risk associated with this vulnerability is High, according to NVD the severity rating is 7.5. As it allows unauthorized access to sensitive files and data, potentially leading to data breaches, intellectual property theft, and system compromise.

FD1.3.9. Recommendations to fix

To mitigate the vulnerability CVE 2024-2025, it is recommended to restrict access to sensitive files and directories using proper access controls and authentication mechanisms. Additionally, implementing secure file storage and serving mechanisms, such as using secure protocols like HTTPS and validating user input, can help prevent exploitation. Regular reviews and updates of security configurations, as well as patching vulnerabilities, are also crucial to prevent attacks. Furthermore, adopting secure coding practices, including input validation and output encoding, can prevent URL manipulation attacks. Finally, considering the implementation of a Web Application Firewall (WAF) can help detect and prevent URL manipulation attacks, providing an added layer of security.

Network Vulnerabilities

To find network vulnerabilities we decided to use the OpenVAS scan. To prepare for OpenVAS first we did the installation through the Kali Linux terminal.

Figure 4 OpenVAS setup

Then, we changed both of our Kali and Metasploitable 2 virtual machine's Network connection from NAT to Bridged. The IP was 172.16.21.121

Figure 5 IP Address of Metasploitable2 after bridging

Figure 6 IP address of Kali after bridging

After that, we started OpenVAS scan and logged into Greenbone. Using the task wizard, we entered the IP address of Metasploitable2 and started the scan.
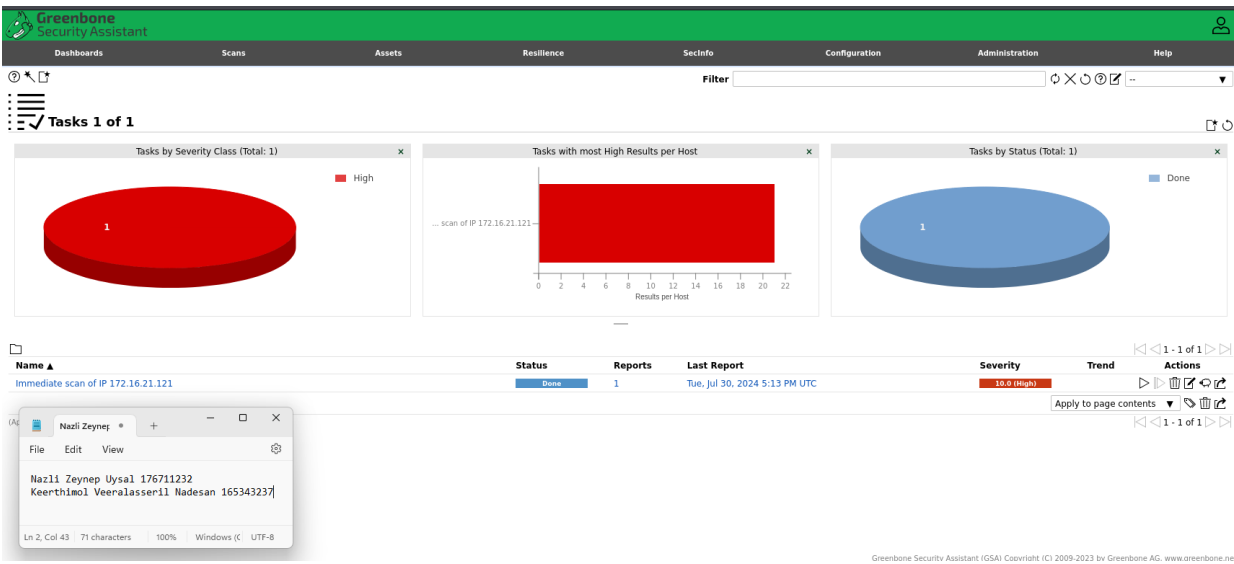
Figure 7 OpenVAS Task Completed
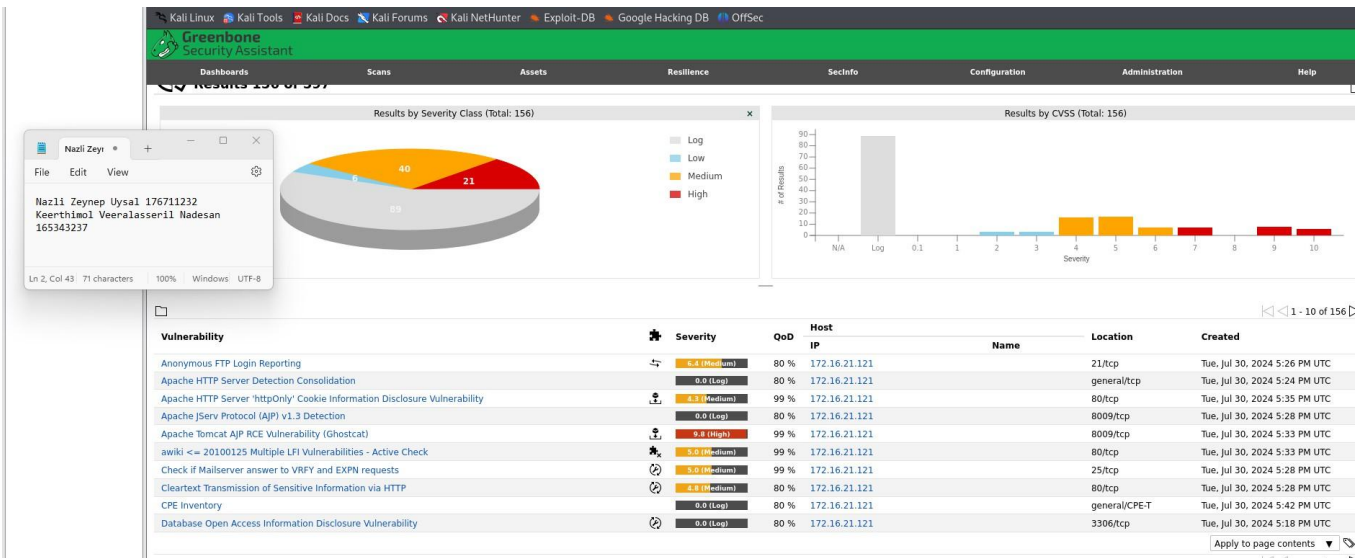
Figure 8 OpenVAS Results Page
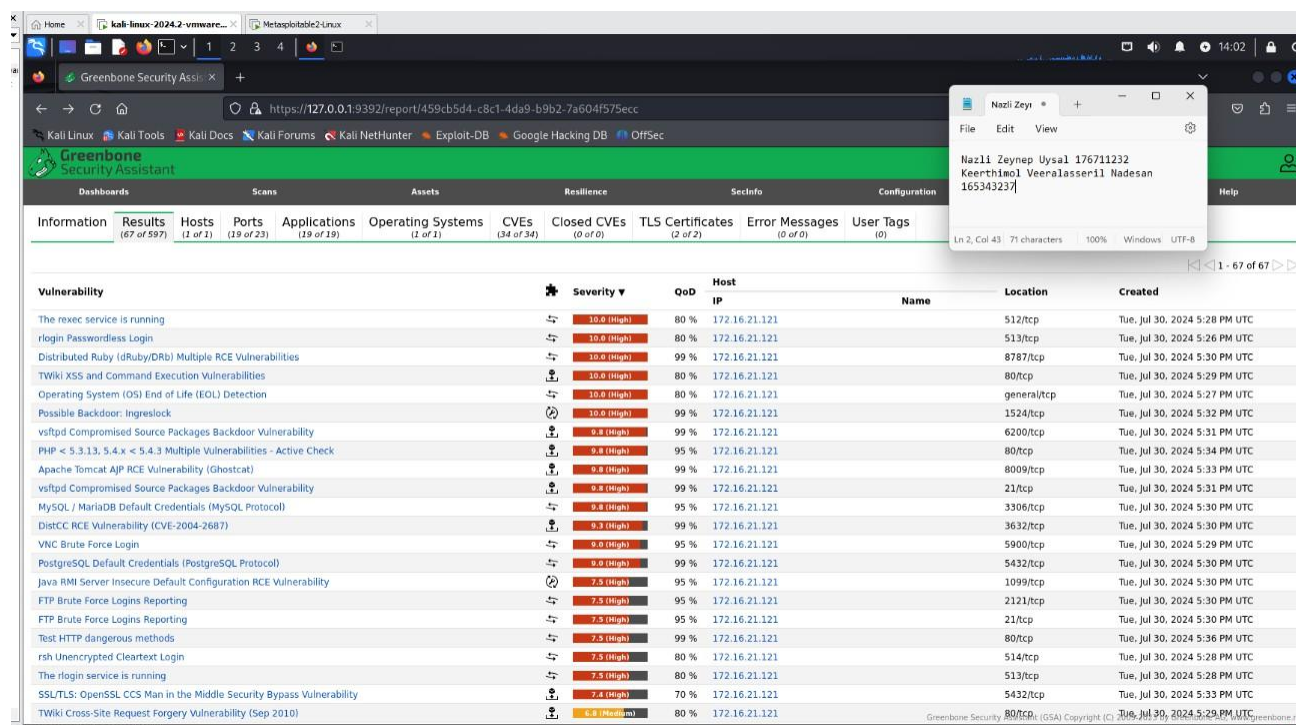
Figure 9 OpenVAS Results with the severity ratings

Network Vulnerability 2

FD1.3.1. Finding Name

CVE-2004-2687 / CWE-16: NVT: DistCC RCE Vulnerability

FD1.3.2. Affected Resource

DistCC Software

FD1.3.3. Method of Finding

We found the vulnerability through the OpenVAS scan results. Firstly, we bridged our connection and then run the OpenVAS system. We logged into GreenBone and entered the bridged IP address of the Metasploitable2 machine and started the scan.

FD1.3.4. Description

DistCC is a distributed compiler software which is used to speed up the compilation of programs by distributing the work across multiple machines. In metasploitable2 machine DistCC software

is prone to a remote code execution (RCE) vulnerability. If distcc 2.x is not configured, it allows an attacker to attack the port and gain remote access and the attacker to run the commands without any authorization.

DistCC usually runs under a non-privileged user account, this means that it does not give direct root access, but it only gives the privileges of the user that is running the DistCC service. Since this is a remote code execution vulnerability the attacker can gain remote access to the system and execute other commands. This access, combined with other exploits, can be used as a privilege escalation to further the attack on the system.

FD1.3.5. Exploitation

We identified this vulnerability from the OpenVAS results. OpenVAS revealed that vulnerability detection found that it was possible to execute the "id" command. The attacker can issue a nmap command to find the open ports on the machine and use mfsconsole to use the distcc payload.

1. Open msfconsole in the kali terminal.
2. Use command use exploit/unix/misc/distcc_exec
3. Using the options command set RPORT number
4. Set RHOST as metasploitable2 IP and LHOST kali IP.
5. Start the exploit using the "exploit"command.
6. Use "whoami" command to see that we have access the daemon user.

This allows attackers to get access to daemon which is a low privilege account that can later be used for privilege escalation with few extra steps.

FD1.3.6. Impact

The distcc CVE-2004-2687 vulnerability is a security flaw in the distcc distributed compiler, which allows remote attackers to execute arbitrary code on affected systems.

Impacts of this vulnerability could be:

- **Remote Code Execution**: The vulnerability enables attackers to execute malicious code on the distcc server, potentially leading to system compromise, data theft, and further attacks.

- **Denial of Service (DoS)**: Exploitation of this vulnerability can cause the distcc service to crash or become unresponsive, disrupting development workflows and build processes.

- **Lateral Movement**: In a distributed development environment, an attacker could potentially move laterally to other systems, compromising the entire network.

FD1.3.7. Likelihood

Since this is an old vulnerability that was discovered in 2004, the likelihood of exploitation is relatively low, but not impossible. A patch has been available for over 19 years, and most systems should have already applied it. Newer systems and development environments have robust security measures which makes the exploitation more difficult. Older systems or legacy environments might still be vulnerable if they haven't been updated or patched. Systems that are no longer maintained or have been forgotten might still be exploitable. If an attacker specifically targets a vulnerable system, the likelihood will increase.

FD1.3.8. Risk

The DisCC vulnerability is a significant risk to older systems, including the potential for code execution, denial of service, and lateral movement. If exploited, attackers can execute arbitrary code on the distcc server, leading to system compromise, data theft, and further attacks on connected systems. Also, exploitation can cause the distcc service to crash or become unresponsive, disrupting workflows and processes.

FD1.3.9. Recommendations to fix

As a recommendation to fix, it is important to update distcc to the latest version, which includes patches for this vulnerability. If updating is not available, consider disabling distcc until a secure version can be implemented. Also, implement firewalls and access controls to restrict access to the distcc service and limit network exposure.

Network Vulnerability 2

FD1.3.1. Finding Name

CVE-2011-2523: vsftpd Compromised Source Packages Backdoor Vulnerability

FD1.3.2. Affected Resource

vsftpd 2.3.4 source package is affected in Metasploitable 2 VM.

FD1.3.3. Method of Finding

The network vulnerability CVE-2011-2523 was found using the openVas on Metasploitable VM.

FD1.3.4. Description

The CVE-2011-2523 is a critical security vulnerability affected in vsftpd 2.3.4. The vsftpd 2.3.4 is a File Transfer Protocol (FTP) server software. This backdoor vulnerability opens a shell on port 6200/tcp allows unauthorized access to the affected systems. The unauthorized attackers can execute arbitrary commands with root privileges. Logging in the systems without authentication leads to the full compromise of the system. The backdoor vulnerability in vsftpd 2.3.4 was found in the version downloaded between June 30, 2011, and July 3, 2011.

FD1.3.5. Exploitation

The version of the Vsftpd service running on the target system can be identified using the nmap. The command to find the version of the FTP service running on port 6200 is,

nmap -sV -p6200 <metasploitable IP>

Once the version of vsftpd is identified we find the vulnerability details in NVD database.

In this case the vsftpd 2.3.4 vulnerability opened a backdoor shell which allows unauthorized root privileges.

The steps to exploit the vsftpd 2.3.4 vulnerability using Metasploitable 2 in Kali Linux is as follows,

1. Login to the Metasploitable VM using the default credentials.

2. Find the IP address of Metasploitable using the command, ifconfig.

3. Open the Metasploit tool using the command 'msfconsole' to exploit the Vsftpd version.

4. Search for the vsftpd version in the msfconsole using the command,

search vsftpd 2.3.4

After searching it will show the backdoor related to this version of vsftpd which can be exploited to compromise the target machine.

5. Select the exploit path using the command,

use <path of exploit>

6. To set the port of vsftpd we use, 'set RPORT 6200' and to set the ip address of the target metasploitable machine we use, 'set RHOSTS <metasploitable ip>'

7. After setting the port and target ip address exploit the backdoor using the command 'exploit' and use "whoami" command to see the root access.

By conducting the exploitation steps we will gain the root access and successfully exploited the Vsftpd 2.3.4.

FD1.3.6. Impact

The impact of the CVE-2011-2523 vulnerability is severe, allowing unauthorized attackers to gain access to the affected system without authentication and execute arbitrary commands with root privileges. The affected source package of Vsftpd also contains a backdoor which opens a shell on port 6200/tcp. This enables them to fully compromise the system, steal sensitive data, install malware, modify system configurations, and disrupt system operations. The vulnerability also allows for lateral movement, enabling attackers to potentially exploit other vulnerable systems within the network. The ease of exploitation, wide impact, and high privileges granted by this vulnerability make its severity critical, emphasizing the need to patch or update vsftpd to a secure version to prevent exploitation and protect against potential attacks.

FD1.3.7. Likelihood

The likelihood of exploitation of the CVE-2011-2523 vulnerability is high. This is due to the ease of exploitation, which requires only basic skills and publicly available tools and techniques, making it an attractive target for attackers. Additionally, the vulnerable version of vsftpd (2.3.4) was widely downloaded and potentially used in many organizations, increasing the number of potential targets. The vulnerability's ability to grant attackers root privileges further increases the likelihood of exploitation, as it offers a high level of control over compromised systems.

FD1.3.8. Risk

The risk associated with this vulnerability is critical, according to NVD the severity rating is 9.8. It poses a significant threat to organizations due to the potential for unauthorized access, data breaches and system compromise. Its ease of exploitation and wide exposure raise significantly the chance of an attack, as it leads to further gain over systems and steal sensitive data. Once they access the vulnerability in Vsftpd they can move laterally within the systems exploiting other vulnerable systems leads to a severe data breach. The critical risk level demands immediate attention and action.

FD1.3.9. Recommendations to fix

To mitigate the critical risk associated with CVE-2011-2523 we strongly recommend immediately updating vsftpd to a secure version 2.3.5 or later to patch the vulnerability. Ensure a robust patch management process is in place to promptly address future vulnerabilities. Segment networks to limit lateral movement in case of a breach. Implement strict access controls including firewalls and intrusion detection/prevention systems. Continuously monitor systems for suspicious activity and signs of exploitation. Develop and regularly test an incident response plan to ensure readiness in case of a breach. Regular security audits should be performed to identify and address potential vulnerabilities. By implementing these recommendations

organizations can effectively mitigate the risk associated with CVE-2011-2523 and enhance their overall cybersecurity posture.

Network Vulnerability 3:

FD1.3.1. Finding Name

CVE-2014-0224/CWE-326: SSL/TLS:OpenSSL CCS Man in the Middle Security Bypass Vulnerability

FD1.3.2. Affected Resource

The affected resource of OpenSSL which includes, all versions prior to 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h. The details regarding the versions of OpenSSL are affected by CVE-2014-0224 was found in Metasploitable 2 VM.

FD1.3.3. Method of Finding

The vulnerability CVE-2014-0224 was found during the OpenVas scan. OpenVAS identified the OpenSSL CCS Man-in-the-Middle Security Bypass Vulnerability (CVE-2014-0224) due to the presence of an affected OpenSSL version.

FD1.3.4. Description

A critical security vulnerability CVE-2014-0224 in OpenSSL versions allows man-in-the-middle attackers to bypass SSL/TLS encryption and hijack sessions or obtain sensitive information. The vulnerability arises from improper processing of ChangeCipherSpec (CCS) messages, enabling attackers to trigger the use of a zero-length master key, effectively disabling encryption.

FD1.3.5. Exploitation

1. Preconditions:

- Both the client and server must be running a vulnerable version of OpenSSL.
- The attacker must be able to intercept and modify the network traffic between the client and the server.

2. Setup:

- **Network Interception:** The attacker needs to be in a position where they can intercept communication between the client and the server.

3. Manipulation of the Handshake:

- **Intercept the Handshake:** The attacker intercepts the handshake process between the client and the server.
- **Inject CCS Message:** The attacker injects a CCS (ChangeCipherSpec) message at the right moment during the handshake process.
- **Force Use of Weak Keys:** By injecting the CCS message early, the attacker can force both the client and server to use weak keys, which are more predictable and thus easier to break.

4. Establishing a MITM Position:

- **Alter Traffic:** With the weak keys in place, the attacker can now decrypt and potentially alter the communication between the client and server.
- **Relaying Traffic:** The attacker relays the traffic between the client and server, decrypting and possibly modifying it on the fly.

FD1.3.6. Impact

The OpenSSL CCS Injection Vulnerability has severe impacts on the security and integrity of encrypted communications. It allows attackers to hijack SSL/TLS sessions and steal sensitive information such as login credentials and personal data. The vulnerability effectively disables encryption by using a zero-length master key allowing attackers to eavesdrop on encrypted communications and modify or inject data. It can also be used to exploit trust relationships between systems enabling man-in-the-middle attacks and lateral movement within a network. The lateral movement in the network will leads to further data breaches.

FD1.3.7. Likelihood

The likelihood of exploitation of the OpenSSL CCS Man in the Middle Security Bypass Vulnerability (CVE-2014-0224) is considered Medium to High due to its wide impact, ease of exploitation, and high severity, allowing attackers to intercept and modify sensitive information. Although a patch has been available since 2014, some systems may still be vulnerable due to lack of updates or maintenance, and modern security measures can detect and prevent exploitation attempts, making it essential to ensure systems are up-to-date and patched to prevent potential attacks.

FD1.3.8. Risk

This vulnerability poses a significant risk to organizations, as it allows attackers to intercept and modify sensitive information, including encrypted data and authentication credentials, potentially leading to unauthorized access, data tampering, and eavesdropping. This vulnerability can compromise the confidentiality and integrity of sensitive information, leading to financial loss, reputational damage, and legal consequences, making it essential to address this vulnerability promptly and ensure that all systems are updated with the latest security patches.

FD1.3.9. Recommendations to fix

To address this vulnerability, it is recommended to update OpenSSL to version 1.0.1h or later, which includes the necessary security patches. Additionally, organizations should ensure that all applications and systems using OpenSSL are updated and patched and consider implementing additional security measures such as TLS protocol verification, certificate pinning, and perfect forward secrecy to further mitigate the risk of man-in-the-middle attacks. Regular security audits and vulnerability scans should also be performed to identify and address any potential security weaknesses.

Part B – Observation Summary

OWASP Top 10 2021 Mapping:

A01:2021 – Broken Access Control	**CWE-552:** Files or Directories Accessible to External Parties, phpinfo.php
A02:2021 – Cryptographic Failures	**CWE-326:** SSL/TLS:OpenSSL CCS Man in the Middle Security Bypass Vulnerability
A03:2021 – Injection	**CWE-78:** vsftpd Compromised Source Packages Backdoor Vulnerability
A04:2021 – Insecure Design	**CWE-1021:** Improper Restriction of Rendered UI Layers or Frames. X-Frames-Header misconfigured.
A05:2021 – Security Misconfiguration	CWE-16: DistCC RCE Vulnerability

Observation List

Metasploitable 2

Observation ID	Description	Inherent Risk
MS2-1	Improper Restriction of Rendered UI Layers or Frames "anti-clickjacking X-Frame-Options header is not present".	Medium
MS2-2	Files or Directories Accessible to External Parties: A vulnerability in /phpinfo.php allowing unauthorized access to sensitive files and directories, leading to data breaches, intellectual property theft, and system compromise.	High
MS2-3	DistCC RCE Vulnerability: If distcc 2.x is not configured, it allows an attacker to attack the port and gain remote access and the attacker to run the commands without any authorization.	High
MS2-4	vsftpd Compromised Source Packages Backdoor Vulnerability: critical vulnerability in vsftpd 2.3.4 that opens a backdoor shell on port 6200/tcp, allowing unauthorized access and execution of commands with root privileges.	High
MS2-5	SSL/TLS:OpenSSL CCS Man in the Middle Security Bypass Vulnerability: allows man-in-the-middle attackers to bypass SSL/TLS encryption and hijack sessions or obtain sensitive information.	High

Metasploitable 2

Observation ID: MS2-1

Title: CWE-1021: Improper Restriction of Rendered UI Layers or Frames

Affected asset: Frames in Mutillidae web page in Metasploitable2.

Description: The description in the Nikto result revealed that "anti-clickjacking X-Frame-Options header is not present". The X-Frame-Options here is a HTTP response header is used to indicate whether a browser is allowed to render a page inside a frame or iframe. And clickjacking is a malicious technique where a web user is deceived into clicking something other than they believe that they are interacting with. This is done by the attacker by using transparent layers in the website UI.

A way to test for clickjacking is by using Burp Suite.

1. Load the web page in the Burp Suite, Go to the Proxy HTTP history tab.
2. Right click on the request to test and click active scan.
3. Go to Burp dashboard and review the issue activity log to see if there are any "framable" responses.

If there are frameable responses the web page is vulnerable to clickjacking.

Impact: Attackers can trick users into performing actions that are masked and hidden form the user's view. Impact varies depending on the function of the hidden application. For example, the attacker can build a website with a "Free IPhone" button and the underneath it there would be a button that has a bank transfer action that sends money to the attacker's account.

Recommendation: Implementing X-Frame-Options and CSP with the frame-ancestors directive will fix the issue with this vulnerability. The Use of X-Frame-Options allows web developers to restrict the usage of overlays, frames or iFrames. Using this option the developer can indicate which domains can frame the content of the web page.

Observation ID: MS2-2

Title: CVE-2024-2052 / CWE-552: Files or Directories Accessible to External Parties

Affected asset: http://192.168.214.128/phpinfo.php

Description: This vulnerability is associated with the presence of a phpinfo.php file on the Metasploitable virtual machine, which exposes sensitive server information. The file reveals extensive details about the server's PHP configuration, including environment variables, system information, and potentially sensitive data.

Steps to Launch the Attack:

1. Identified Metasploitable VM's IP address: 192.168.214.128

2. Scanned web server using Nikto: nikto -h 192.168.214.128

3. Accessed vulnerable file: http://192.168.214.128/phpinfo.php

4. Exploited via URL manipulation: http://192.168.214.128/../../../../../etc/passwd to access sensitive files

5. Manipulated URL to access sensitive information, including system details and environment variables

6. Demonstrated ability to retrieve sensitive files, including password files, without authentication.

Impact: The vulnerability poses a severe security risk as it allows unauthorized access to sensitive files on the server. Attackers can exfiltrate critical data such as configuration files and environment variables, leading to data breaches, intellectual property theft, and potential further exploitation of the server. The exposure of such sensitive information can compromise the integrity and confidentiality of the system, leading to significant reputational and financial damage to the organization.

Recommendation: Restrict access to sensitive files, such as removing or limiting access to phpinfo.php, and ensure proper access controls and authentication mechanisms are in place. Implement secure file storage and serving mechanisms, like HTTPS, and validate user input to prevent URL manipulation. Regular security audits should be conducted to review and update security configurations, and promptly patch vulnerabilities. Adopting secure coding practices, including input validation and output encoding, can prevent similar vulnerabilities. Additionally, consider implementing a Web Application Firewall (WAF) to detect and prevent unauthorized access attempts and URL manipulation attacks.

Observation ID: MS2-3

Title: CVE-2004-2687 / CWE-16: NVT: DistCC RCE Vulnerability

Affected asset: 172.16.21.121 [TCP/3632]

Description: In metasploitable2 machine DistCC software is prone to a remote code execution (RCE) vulnerability. If distcc 2.x is not configured, it allows an attacker to attack the port and gain remote access and the attacker to run the commands without any authorization.

Impact: Remote Code Execution: The vulnerability enables attackers to execute malicious code on the distcc server, potentially leading to system compromise, data theft, and further attacks. Denial of Service (DoS): Exploitation of this vulnerability can cause the distcc service to crash or become unresponsive, disrupting development workflows and build processes. Lateral Movement: In a distributed development environment, an attacker could potentially move laterally to other systems, compromising the entire network.

Recommendation: As a recommendation to fix, it is important to update distcc to the latest version, which includes patches for this vulnerability. If updating is not available, consider disabling distcc until a secure version can be implemented. Also, implement firewalls and access controls to restrict access to the distcc service and limit network exposure.

Observation ID: MS2-4

Title: CVE-2011-2523 / CWE-78 : vsftpd Compromised Source Packages Backdoor Vulnerability

Affected asset: 192.168.214.128 [TCP/6200]

Description: This vulnerability affects the vsftpd 2.3.4 software running on the Metasploitable 2 virtual machine. CVE-2011-2523 is a critical backdoor vulnerability that was introduced in the vsftpd 2.3.4 source package. When exploited, this vulnerability allows attackers to gain unauthorized root access to the affected system by opening a shell on port 6200/tcp. This backdoor allows attackers to execute arbitrary commands with root privileges, leading to a complete system compromise.

Steps to Launch the Attack

1. Identify the IP Address:
   Use ifconfig on the Metasploitable VM to find the IP address, which is 192.168.214.128.

2. Verify vsftpd Version:
   Run nmap -sV -p6200 192.168.214.128 to confirm vsftpd 2.3.4 is running on port 6200/tcp.

3. Exploit the Vulnerability:
   a. Open Metasploit with msfconsole.
   b. Search for the exploit using search vsftpd 2.3.4.
   c. Select the module with use exploit/unix/ftp/vsftpd_234_backdoor.
   d. Set the target IP and port using set RHOSTS 192.168.214.128 and set RPORT 6200.

e. Launch the exploit with exploit.

f. Confirm root access with whoami, which should return "root".

Impact: The impact of this vulnerability is critical, as it allows attackers to gain root access to the affected system without authentication. With root privileges, attackers can execute arbitrary commands, steal sensitive data, install malware, and modify system configurations. The vulnerability also facilitates lateral movement within the network, allowing attackers to compromise other systems. This can result in extensive data breaches, operational disruption, and severe financial and reputational damage to the organization.

Recommendation: Upgrade vsftpd to version 2.3.5 or later to patch the vulnerability and implement a robust patch management process to ensure timely updates of all software. Additionally, segment networks to limit lateral movement in the event of a breach and apply strict access controls, including the use of firewalls and intrusion detection/prevention systems. Continuously monitor systems for suspicious activity and signs of exploitation and develop and regularly test an incident response plan to ensure readiness in case of a security breach. Finally, conduct regular security audits to identify and address potential vulnerabilities in the system.

Observation ID: MS2-5

Title: CVE-2014-0224/CWE-326: SSL/TLS:OpenSSL CCS Man in the Middle Security Bypass Vulnerability
Affected asset: 172.16.21.121 [TCP/5432]

Description: A critical security vulnerability CVE-2014-0224 in OpenSSL versions allows man-in-the-middle attackers to bypass SSL/TLS encryption and hijack sessions or obtain sensitive information. The vulnerability arises from improper processing of ChangeCipherSpec (CCS) messages, enabling attackers to trigger the use of a zero-length master key, effectively disabling encryption.

SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability   7.4 (High)   70 %   172.16.21.121   5432/tcp

Summary

OpenSSL is prone to security-bypass vulnerability.

Detection Result

Vulnerability was detected according to the Detection Method.

Insight

OpenSSL does not properly restrict processing of ChangeCipherSpec
messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in
certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive
information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.

Detection Method

Send two SSL ChangeCipherSpec request and check the response.
Details: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability OID: 1.3.6.1.4.1.25623.1.0.105042
Version used: 2023-07-26T05:05:09Z

Affected Software/OS

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h.

Impact

Successfully exploiting this issue may allow attackers to obtain
sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks.

Solution

Solution Type: Vendorfix
Updates are available. Please see the references for more information.

References

CVE   CVE-2014-0224

Nazli Zeynep

File   Edit   View

Nazli Zeynep Uysal 176711232
Keerthimol Veeralasseril Nadesan 165343237

Ln 2, Col 43   71 characters   100%   Windows (C   UTF-8

Impact: It allows attackers to hijack SSL/TLS sessions and steal sensitive information such as login credentials and personal data. The vulnerability effectively disables encryption by using a zero-length master key allowing attackers to eavesdrop on encrypted communications and modify or inject data. It can also be used to exploit trust relationships between systems enabling man-in-the-middle attacks and lateral movement within a network. The lateral movement in the network will leads to further data breaches.

Recommendation: It is recommended to update OpenSSL to version 1.0.1h or later, which includes the necessary security patches. Additionally, organizations should ensure that all applications and systems using OpenSSL are updated and patched and consider implementing additional security measures such as TLS protocol verification, certificate pinning, and perfect forward secrecy to further mitigate the risk of man-in-the-middle attacks. Regular security audits and vulnerability scans should also be performed to identify and address any potential security weaknesses.

Appendix

Appendix A: Tools and Technologies Used

- Kali Linux: A Debian-derived Linux distribution designed for digital forensics and penetration testing.

- Metasploitable2: A purposely vulnerable Linux virtual machine used for testing security tools and demonstrating vulnerabilities.

- Nikto: An open-source web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files and programs.

- OpenVAS: An open-source vulnerability scanning tool that provides detailed information about network vulnerabilities and potential points of exploitation.

- nmap: A network scanning tool used to discover hosts and services on a computer network by sending packets and analyzing the responses.

- msfconsole (Metasploit Framework): A powerful tool for developing and executing exploit code against a remote target machine.

Appendix B: Vulnerability Findings

1. Web Vulnerabilities (Nikto)

  - Clickjacking: A vulnerability where a user is tricked into clicking on something different from what the user perceives, often leading to unauthorized actions.

  - Directory Browsing: The ability to view directories on the web server, which can lead to exposure of sensitive files and data.

2. Network Vulnerabilities (OpenVAS)

  - DistCC RCE (Remote Code Execution): A vulnerability in the DistCC service allowing attackers to execute arbitrary code on the server.

  - vsftpd Backdoor: A vulnerability in the vsftpd service that allows unauthorized remote access to the system.

Appendix D: Risk Rating Criteria

- Low Risk: Minor vulnerabilities that do not pose immediate threats but should be addressed.

- Medium Risk: Vulnerabilities that could be exploited under certain conditions, potentially leading to data exposure or service disruption.

- High Risk: Serious vulnerabilities that are easy to exploit and can lead to significant data breaches, unauthorized access, or system compromise.

Appendix E: Glossary of Terms

- RCE (Remote Code Execution): The ability of an attacker to execute arbitrary commands on a remote machine.

- CSP (Content Security Policy): A security feature that helps prevent various types of attacks, including cross-site scripting (XSS) and data injection attacks.

- X-Frame-Options: An HTTP response header used to prevent clickjacking attacks by specifying whether a browser should be allowed to render a page in a frame, iframe, or object.

This appendix serves as a comprehensive reference to the tools, techniques, and findings documented in this penetration testing project report.

References

1. NIST. "NVD - Vulnerabilities." *Nist.gov*, 2019, nvd.nist.gov/vuln.

2. Singh, Mandeep, et al. "Penetration Testing on Metasploitable 2." *International Journal of Engineering and Computer Science*, vol. 9, no. 05, 10 May 2020, pp. 25014–25022, https://doi.org/10.18535/ijecs/v9i05.4476.

3. OWASP. "OWASP Top 10: 2021." OWASP, 2021, owasp.org/Top10/.

4. "CWE - Common Weakness Enumeration." Cwe.mitre.org, cwe.mitre.org/.