Vulnerability Report of LAN

Aida Gaston, Leila King, Zoe Medina & Randall Seymore

Professor Burke

CYBR 502- Cybersecurity Network Defense

Shiley-Marcos School of Engineering (SMSE), University of San Diego

Introduction

Vulnerabilities are weaknesses that cyber criminals can take advantage of to gain access to a computer system. Because of this, our team was tasked with running an vulnerabilities scan on our network to find any exploits that need to be patched. Our network consists of a firewall with strict rules on which IP addresses can access the LAN and on what ports, vulnerable machines such as OWASP and Metasploitable that are sitting within the LAN, Security Onion which is responsible for monitoring and logging intrusions into the LAN, and a Kali Linux virtual machine which hosted the vulnerability scanner. We used OpenVAS, a free open-source vulnerability scanner, to perform a scan on our local area network. Because the scanner was on the Kali Linux machine within the LAN, we didn't need to make any changes to the network. We located somewhere around 230 vulnerabilities across the Metasploitable, OWASP, and Security Onion virtual machines. No vulnerabilities could be found on the firewall or Kali Linux. This paper will discuss the top ten vulnerabilities that have the most significant impact on the system and how they should be remedied.

OWASP - High (CVSS: 10.0) NVT: Apache Tomcat Manager/Host Manager/Server Status Default/Hardcoded Credentials (HTTP)

This vulnerability, found on our Owasp Virtual Machine (VM), is a high rated vulnerability that requires immediate attention. The Tomcat Manager is a web application that runs inside of a Tomcat server. This application allows for the creation and deletion of virtual machines hosted on the server. The vulnerability exists because the default Admin credentials were not changed. This is extremely dangerous to the system because if left as is, an attacker could access the Apache Tomcat Manager application as an Admin and upload and execute arbitrary code. Arbitrary code execution is a form of hacking. In this instance a hacker could create a backdoor, could collect sensitive data such as password files, or misconfigure/delete virtual machines (Pittamand3tx,2022).

Luckily however, the remediation for this vulnerability is very simple. Change the Admin account's default password to a much more complex password or delete the default Admin account altogether.

Owasp - High (CVSS: 9.8) NVT: Joomla < 3.8.12 Multiple Vulnerabilities

The Common Vulnerabilities and Exposures (CVE) classifies vulnerabilities to determine the threat level of each vulnerability. In NVT Joomla <3.8.12, an issue was discovered where inadequate checks in the InputFilter class could be used to bypass the upload filter for specially prepared PHAR files. Input validation attacks may utilize a variety of input formats, including code scripts and commands ("Input Validation Attacks | Bugcrowd," n.d.). PHAR files which are PHP archives, are considered to be executable files. PHAR (PHP Archive) files simplify the distribution of applications and libraries by compressing many PHP code files and other resources into a single archive file. For example, PHAR files are used to support bzip2 and gzip compression. Additionally, with archive checksums, PHP applications can be deployed and run from a single file (Beaver, n.d.).

Cross site scripting (XSS) is a vulnerability that depends on unsanitized user input. In this case, the malicious script input into the application is not sent to the database server but instead echoed back to the user's browser and executed. In many cases, an attacker will impersonate a user to gain access to the application by stealing the user's cookies. Less common XSS attacks use JavaScript to redirect users to another page that closely resembles the original page, also known as a phishing attack ("Input Filtering," n.d.). In this scenario, there is bad code that is out of date. In this case, we want to remediate it rather than just leaving them unresolved. The solution would be to patch the system. We can set up automated patches so that this won't occur again in the future. One powerful tool that can be used to combat cross scripting is web application firewall (WAF); this application would protect against XSS.

If an attacker does cross site scripting, the execution could occur automatically when the webpage loads or the user hovers over particular fields or hyperlinks. Some consequences include crashing the browser, capturing the user's keystrokes, and again gaining access to the cookie information to compromise the user's account. In addition, users can be tricked into entering credentials on a phony form, giving the attacker full access to their accounts. ("What Is Cross Site Scripting (XSS) and How Does It Work? | Synopsys," n.d.). The solution to this vulnerability would be to update the system. This can be achieved through a manual update or setting up an automated system to keep it up to date.

OWASP - High (CVSS 9.8) NVT: Joomla! Core LDAP Information Disclosure Vulnerability Nov17

This vulnerability was found on our OWASP virtual machine and is due to an inadequate escaping in the LDAP authentication plugin. In this vulnerability, Joomla is prone to an information disclosure vulnerability, in which a successful exploitation of the issue would allow remote attackers to disclose usernames and passwords. Information disclosure attacks utilize vulnerabilities to acquire sensitive system specific information that can allow the attacker to compromise the system ("IBM Documentation," n.d.). An attack using this specific vulnerability can be initiated remotely, and no form of authentication is required to successfully exploit this vulnerability ("JOOMLA CMS UP TO 3.7.X LDAP AUTHENTICATION PASSWORD LDAP INJECTION," 2017). This exploit is rated very high as a vulnerability because it is incredibly easy to initiate, as no physical access or authorization keys are required. If an attacker was able to use this exploit, they would gain access to the username and password for Joomla and would be able to steal a plethora of valuable information or even download further malware into the system.

To fix this vulnerability, the appropriate updates should be made to Joomla. Our scans have shown that the software patch should be in Joomla version 3.8.2 or later. Updating this software will require the user to check for updates on their device, or in some cases, manually download and insert the patched software. Keeping software up to date and patched is an easy and incredibly powerful way to ensure your information is kept secure. According to the Cybersecurity and Infrastructure Security Agency (CISA), patches are “software and operating system (OS) updates that address security vulnerabilities within a program or product” and are released by the companies whenever they are aware of a potential exploit for their system (“Understanding Patches and Software Updates | CISA,” 2023).

Security Onion - High (CVSS 9.8) NVT: CentOS: Security Advisory for httpd

This vulnerability was found on our Security Onion virtual machine and is due to the remote host missing an update for the ‘httpd’ package(s). The “httpd” packages provide the Apache HTTP server, a web server. In this vulnerability, errors encountered during the discarding of a request body lead to HTTP request smuggling. The affected software is CentOS 7. HTTP request smuggling occurs when an “attacker sends both headers in a single request,” which can cause either front-end or back-end servers to incorrectly interpret the request and pass a malicious HTTP query (McKeever, n.d.). Attackers exploit this vulnerability to maneuver around security measures to gain access to sensitive data, bypass firewalls, and even set up a cross-scripting attack (McKeever, n.d.). An attacker can even hijack a user’s session.

To fix this vulnerability, the “httpd” package(s) for CentOS 7 need to be updated. To do so, the users will need to download the appropriate package(s) from the CentOS website and download them onto their machine. As with many of the vulnerabilities listed in this paper, software updates with security patches are usually an incredibly powerful way of ensuring that known vulnerabilities are not exploited onto your user system or network.

Metasploitable - High (CVSS 9.3) NVT: DistCC RCE Vulnerability

This vulnerability was found on our Metasploitable virtual machine and is due to a misconfiguration. Our scan found that DistCC was prone to a remote code vulnerability. In this case, DistCC is not configured to restrict access to the server port, which allows attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks. DistCC, by default, trusts its clients completely, which could allow a malicious client to execute arbitrary commands on the server.

Remote code execution (RCE) vulnerabilities allows attackers to “remotely execute commands to place malware or other malicious code on your computer or network” (CrowdStrike, 2023). Unlike a phishing or XSS attack, RCE exploits does not require user input from the victim and can compromise data without physical access, which is why RCE vulnerabilities are considered critical to fix promptly (CrowdStrike, 2023). Once the attacker gains access to your system to execute malicious code, they are able to use that to install an endless amount of damage to the network. For instance, an attacker can inject ransomware into the network to hold data hostage until the victim pays the fee to unlock or decrypt their data.

To fix this vulnerability, it is recommended to update DistCC to add the applicable security patches. Immediately updating this software will ensure that the user’s network is secure. To install the appropriate software version, the user will need to install the update from the DistCC GitHub repository.

OWASP - High (CVSS 8.8) NVT: Tiki Wiki CMS Groupware < 17.2 SQL Injection

This vulnerability was found on our OWASP virtual machine and is due to a potential SQL Injection via the tiki-user_tasks.php show_history parameter. OpenVAS found this vulnerability due to a shared database of known vulnerabilities. These databases are collections of information from multiple sources of security companies and professionals about different vulnerabilities in hardware and software. In this case, OpenVAS found that version 1.9.5 of Tiki Wiki is susceptible to SQL Injections from the CVE database of known vulnerabilities. It is important to keep vulnerability scanners such as OpenVAS up to date with these databases so that it can detect these types of exploits.

A SQL Injection is an attack where a hacker inserts SQL code into a query input to retrieve information or bypass credentials. For example, an attacker could enter a generic "admin–" username into the user box. Because of the "--" at the end of admin, it doesn't matter what the attacker puts in the password box. Since the SQL code reads "--" as a comment, the password check of the query condition is commented out and ignored. In this case, a search parameter to show a user's history is vulnerable to a SQL Injection. This means an attacker could craft a SQL input to display information from the database besides the user history by commenting out the given search conditions and inserting their own.

To fix this vulnerability, it is recommended to update the Tiki Wiki version to at least 17.2 where the developers have already patched the exploit. Patching a SQL Injection vulnerability would consist of creating better input sanitation so that any SQL code will be rejected by the system before being put into the query. Furthermore, it is important to always keep software and packages up to date to fix known vulnerabilities.

Security Onion - High (CVSS: 7.8): NVT: CentOS: Security Advisory for polkit

This vulnerability was found on our Security Onion virtual machine and is due to the virtual machine missing an update for the "polkit" package. OpenVAS detected this vulnerability from a CVE database of known vulnerabilities. In this case, the "polkit" version installed on the system, "polkit-0.112-26.e17," is known to be susceptible to privilege escalation.

Privilege Escalation occurs when a hacker is able to gain admin or root access in a system from a non-privileged account. With privileged access, a hacker would be able to access any information in the system or compromise the system so that it can no longer be used. In this case, the "polkit" version installed on Security Onion has an exploit due to a mishandled return error that can create a new user with sudo privileges from a non-privileged account. A hacker would need to run a specifically crafted "dbus-send" command requesting to create this new user and add them to the sudo group. If the hacker is able to kill the command at the moment when the "polkit" service is asking for a UID, the "dbus-daemon" hits an error since it no longer sees a UID and returns 0. However, the "polkit" service reads 0 as the UID of a root user and proceeds with creating a new sudo user. The process can be repeated to set a password for the new sudo user and then the hacker will have full access to an account with root privileges.

To fix this vulnerability, it is recommended that at least version "polkit-0.112-26.e17_9.1" of the "polkit" package is installed onto Security Onion. The developers patched the exploit in this version so that new users can no longer be created in this way. Patching this exploit would consist of handling the return error in a way that doesn't conflict with how “polkit” reads UID 0 or have “polkit” notice when the process is killed so that it doesn’t continue with the command.

Metasploitable - High (CVSS: 7.5) NVT: FTP Brute Force Logins Reporting

A hacking method that relies on trial and error to break security measures like encryption keys, login credentials, and passwords is known as brute force. It is a tactical method for breaking into an account without permission. Hackers often use bots or scripts to attack the login pages of various websites and online apps, but these attacks can also be used for other malicious purposes. In attempts to gain access forcefully, the hacker will enter different combinations of usernames and passwords until they finally succeed.

It is possible to remotely log into a File Transfer Protocol (FTP). The ability to send files from a client (a user on another machine) to your server is made possible by FTP. It was possible to login into this server as the credentials were weak. This vulnerability's real reporting occurs in this VT since the VT "FTP Brute Force Logins" may experience a timeout. The resolution to this issue is to change the password immediately to mitigate the vulnerability. This would be done manually. The configurations that need to change include implementing access controls that are stricter and better authentication protocols. It is recommended that users utilize passphrases instead of basic passwords. Setting rate limits is a way to minimize traffic overall. In other words, you can configure resources so that there are only a limited number of failed user attempts within a given time period (Crane, 2021). Also, two factor authentication and having software updated as needed would help against a brute force attack.

Metasploitable - High (CVSS: 7.5) NVT: Test HTTP dangerous methods

This vulnerability was found on our Metasploitable virtual machine and is due to a misconfigured web server that allows for the use of HTTP methods “PUT” and “DELETE” by a remote client. OpenVAS found this vulnerability on the web server by creating HTTP packets with the “PUT” and “DELETE” methods. The “PUT” packet was sent to the web server with a test file in the data section. OpenVAS knew that the “PUT” method worked because it received an “HTTP OK” response that stated the file was successfully created. The “DELETE” packet contained the name of the previously placed test file. OpenVAS also received a successful response from the web server that the file had been deleted.

The presence of this vulnerability allows for malicious actors to put executable code onto the web server or delete files of valuable data. A common example of this would be uploading scripts to create a backdoor. Once the backdoor is established, an attacker can use it for a variety of reasons, such as stealing information, installing malware, and taking control of the server. For example, an attacker could create a file or payload with the .PHP extension that contains a script to create a reverse shell. The attacker could then use the “PUT” method to place the payload onto the web server and set up a netcat to listen for when the .PHP file is executed. The reverse shell will give the attacker access to the web server directories and, depending on other security measures in place, could proceed to escalate privilege.

In order to fix this vulnerability, security professionals should restrict access to these HTTP methods. They should only be enabled on the web server if they are absolutely necessary for a crucial service to run. If not, it is best practice to disable these methods all together to enforce the principle of least privilege.

Metasploitable - High (CVSS: 7.4) NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

CVE-2014-0224 was reported as a vulnerability existing on our Metasploitable virtual machine. This vulnerability allows a man-the-middle attacker to be able to intercept OpenSSL communications between a client and a server. Successful exploitation would allow the attacker to intercept sensitive information or hijack the session altogether.

Successful exploitation of this vulnerability can be achieved by an attacker waiting for a new TLS connection followed by the ClientHello / ServerHello handshake to take place. The attacker then would issue a ChangeCipherSec (CCS) in both directions, which would cause the OpenSSL code to use a zero-length pre-master secret key. Doing so creates Session Keys derived from the zero-length pre-master key. This then allows the hacker to renegotiate the handshake parameters and grants them the capability of decrypting or modifying all packets in transit (Sidhpurwala, 2014).

OpenSSL has since patched this vulnerability by changing how it handles the zero length master keys. In fact, OpenSSL no longer accepts the use of zero length master keys at all. CCS packets are also no longer able to be received before the master key is sent. This patch has remediated the vulnerability, so it is recommended that both the client and server upgrade to the latest OpenSSL versions to avoid exploitation (Sidhpurwala, 2014).

Conclusion

Throughout this white paper we have reported on ten of the nearly two hundred and thirty vulnerabilities identified in an OpenVAS scan of our network. For each vulnerability that we chose to report on we provided a description of the vulnerability, how it could be successfully exploited, the impact of the exploit, and how to properly remediate the vulnerability. As you can see, unresolved vulnerabilities can leave your network, your data, and your reputation at risk. Flaw remediation is vital to a system's health and should never be taken lightly nor put off.

References

Backhouse, K. (2021, June 10). *Privilege escalation with polkit: How to get root on linux with a seven-year-old bug*. The GitHub Blog. Retrieved April 10, 2023, from https://github.blog/2021-06-10-privilege-escalation-polkit-root-on-linux-with-bug/

Beaver, G. (n.d.). PHAR File Extension - What is .phar and how to open? - ReviverSoft. Retrieved from https://www.reviversoft.com/en/file-extensions/phar

Brute force attacks : FTP Brute Force Logins Reporting. (n.d.). Retrieved from http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.108718

Chandel, R. (2018, October 10). *Multiple ways to exploiting put method*. Hacking Articles. Retrieved April 10, 2023, from https://www.hackingarticles.in/multiple-ways-to-exploiting-put-method/

Crane, C. (2021, August 10). *15 Brute Force Attack Prevention Techniques You Should Know*. The SSL Store. Retrieved from https://www.thesslstore.com/blog/15-brute-force-attack-prevention-techniques-you-should-know/

CrowdStrike. (2023, March 6). What is Remote Code Execution (RCE)? | CrowdStrike. Retrieved from https://www.crowdstrike.com/cybersecurity-101/remote-code-execution-rce/

IBM Documentation. (n.d.). Retrieved from https://www.ibm.com/docs/en/snips/4.6.0?topic=categories-information-disclosure-attacks

Input Filtering. (n.d.). Retrieved from https://www.dnnsoftware.com/wiki/input-filtering

What Is Cross Site Scripting (XSS) and How Does It Work? | Synopsys. (n.d.). Retrieved from https://www.synopsys.com/glossary/what-is-cross-site-scripting.html

Input Validation Attacks | Bugcrowd. (n.d.). Retrieved from https://www.bugcrowd.com/glossary/input-validation-attacks/

JOOMLA CMS UP TO 3.7.X LDAP AUTHENTICATION PASSWORD LDAP INJECTION. (2017, September 21). Retrieved from https://vuldb.com/?id.106906

McKeever, G. (n.d.). What Is HTTP Request Smuggling? | Attack Examples | Imperva. Retrieved from https://www.imperva.com/learn/application-security/http-request-smuggling/

Pittamand3tx (2022, August 26). *What isArbitrary Code Execution?* Geeksforgeeks.org. Retrieve from https://www.geeksforgeeks.org/what-is-arbitrary-code-execution/

Sidhpurwala, H. (2014,June5). *OpenSSL MITM CCSinjection attack (CVE-2014-0224)*.Redhat.com. Retrieved from https://www.redhat.com/en/blog/openssl-mitm-ccs-injection-attack-cve-2014-0224

Understanding Patches and Software Updates | CISA. (2023, February 23). Retrieved from https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates

What is SQL injection? tutorial & examples: Web security academy. What is SQL Injection? Tutorial & Examples | Web Security Academy. (n.d.). Retrieved April 10, 2023, from https://portswigger.net/web-security/sql-injection