Endpoint Vulnerability Scanning

California State Polytechnic University Pomona

Computer Science Department

CS 4630 Undergraduate Seminar Term Paper

Russell Rickards

13 May 2024

rdrickards@cpp.edu

ABSTRACT

Learning the importance and background of information security, specifically endpoint vulnerability scanning is essential to maintaining a safe and secure working environment.

1. OVERVIEW

Every day, endpoints of various companies are accessed by many users. Although most of the time the users are granted access and allowed on these endpoints, some have malicious intent. Companies must maintain secure endpoints to keep company information safe. This paper delves into various aspects of endpoint vulnerability scanning tools, encompassing web and endpoint vulnerability scanning, along with the differentiation between authenticated and unauthenticated scans. It explores the prioritization of vulnerabilities using Common Vulnerabilities and Exposures (CVE), the Common Vulnerability Scoring System (CVSS), and the vulnerability/risk formula.

2. ENDPOINT VULNERABILITY SCANNING TOOLS

a. What is Endpoint Vulnerability Scanning?

In summary, endpoint vulnerability scans are computer programs that are used to target weaknesses within various domains such as computers, networks, and applications. In order to properly secure an endpoint, annalists must cover every type of vulnerability point. This can be accomplished by using various endpoint vulnerability scanning tools. There are three categories under which all endpoint vulnerability scanning tools fall; website vulnerability scanning tools, endpoints vulnerability scanning tools, and authenticated / unauthenticated scanning tools. Throughout this paper, I will discuss how each of these tools operates and what they are used within real-world applications.

b. Website Vulnerability Scanning Tools

As the name implies, website vulnerability scanning tools specifically target the websites that an endpoint can access. On average, a single user with a machine (endpoint) accesses up to 130 websites per day. Taking into account how many people have access to an endpoint, the number of websites an endpoint accesses rises astronomically. It is important that all the website being accessed are secure before a user can get to it. Furthermore, because most websites are hosted on external-facing servers (servers that are accessible through the internet), it is very easy and likely that their servers may contain some form of malware. In order to catch any malicious intent, website vulnerability scanning tools look into the source code targeting coding vulnerabilities.

One reliable way of checking if a website is secure before an endpoint is allowed access to it is by scanning the security headers utilized with a website. In most cases, websites list the various security heads used. Depending on the company's specifications, an analyst is able to look for the specific security headers that are necessary within a website. If these headers are not found, the annalist is able to block the website before a user is able to access it.

```python
def check_security_headers(url):
    response = requests.get(url)

    vulnerabilities = 0

    # Check for security headers
    security_headers = ['Strict-Transport-Security', \
                        'Content-Security-Policy',\
                        'X-Content-Type-Options',\
                             'X-Frame-Options', \
                               'X-XSS-Protection']

    for header in security_headers:
        if header not in response.headers:
            print(f"Missing security header: {header}")
            vulnerabilities += 1

    return vulnerabilities
```

Figure 1. Security Header Scanner Method

Figure 1. Shows an example of how a security header scanner would be implemented in Python. In this example, the targeted security headers are:

- Strict Transport Security
- Content Security Policy
- X Content Type Options
- X Frame Options
- X XSS Protection

By specifying the security headers and comparing them with the source code, an annalist can compile the results necessary to determine if a website is safe for an endpoint to access.

Some popular website vulnerability scanning tools include

- Detectify
- Upuard
- Qualis

c. Endpoint Vulnerability Scanning Tools

Endpoint vulnerability scanning tools focus on securing and detecting weaknesses within the endpoint itself. An endpoint refers to any machine a user has access to, ie: a laptop, personal computer, tablet, or smartphone. Each of these endpoints can server as a form of access to private data and thus must be secure and free of weaknesses.

All endpoint vulnerability scanning tools rely on a plugin feed. A plugin feed for endpoint vulnerability scanning is like a library of specialized tools that help find weaknesses in computer systems. The plugin feeds are based on a database of publicly known vulnerabilities which is constantly updated. In order to better categorize vulnerabilities, each one is referenced by the Common Vulnerability and Exposures (CVEs). I will go more in-depth on CVEs later on in the paper but for now, CVEs give an internet standard rating for each vulnerability from 1 to 10, 1 being low and 10 being critical.

The most common way endpoint vulnerability scanning tools are implemented is by using scanning templates. The procedure in which an analyst uses a scanning template is as follows:

1. A non-compliant credential attempts to join the domain.
2. The analyst installs a scanning agent which is then linked to a manager. The manager can be a supervisor or an analyst themself.
3. The analyst or manager creates an agent scan that is not on the domain.

After the completion of these steps, the endpoint scanning is successfully installed within the endpoint which can then be monitored for weaknesses.

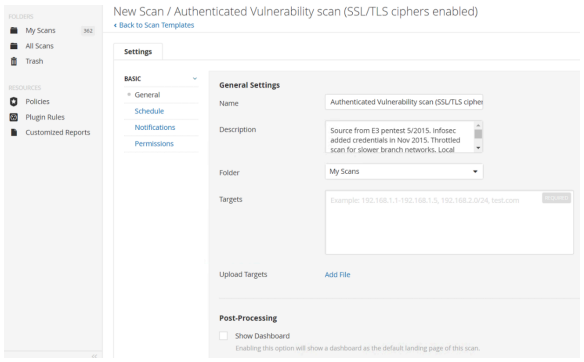

Figure 2. Nessus Scanner Template

In Figure 2., we can see an example of how a scanner template is utilized. In this specific example, analysts are able to name the scan, determining which endpoints within the domain they want targeted, and how often the scan should be run. Scans can

be set to run once or repeatedly. Templates can also be used to specify who is notified and who has access to change the created scan.

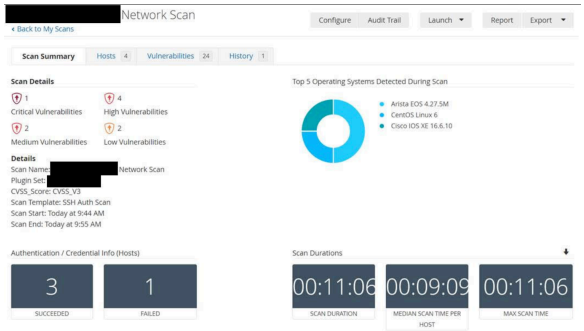

Figure 3. Endpoint Scan Results

After a scan is completed, it can give necessary information that can be used to determine the vulnerability of an endpoint. In Figure 3., we see that the example endpoint has many vulnerabilities varying in criticality.

With endpoint vulnerability scanning tools, analysts can create scans that can target an endpoint or multiple endpoints for that matter. By utilizing recurring scans, analysts get a visual representation of when an endpoint has been attacked.

Some popular endpoint vulnerability scanning tools include:

- Tenable Nessus Scanner
- RedCloak
- SumoLogic

d. Authenticated & Unauthenticated Scanning Tools

The last type of endpoint vulnerability scanning category is authenticated and unauthenticated scanning tools. These tools can be considered separate types but because they are so similarly defined it is easier to explain them together.

Authenticated scanning tools refer to any type of tool that is given access to the endpoint. In other words, the scan is a domain administrative account that is allowed access to anything specified. Authenticated scans are useful since they provide only true positives when a vulnerability is found. Because the scan is already given access to the endpoint and its applications, it avoids login errors which can throw a false positive. This makes it easier for analyst to see any vulnerabilities that are found within the endpoint.

In vice-versa, unauthenticated scans are not given any privileges or access to the endpoint. Although unauthenticated scans can produce false positives due to logging failure, there is still information that can be found useful. Unauthenticated scans are able to give analysts a threat actor's point of view. Much like the unauthenticated scan, most threat actors are trying to attack the endpoint without any access. Unauthenticated scans can show how vulnerable an endpoint is to outside forces.

By utilizing authenticated scans and unauthenticated in tandem, analysts can cover all points of view of an endpoint. With authenticated scans, any vulnerabilities from the inside of an endpoint can be found, while with unauthenticated scans, all vulnerabilities that can be exploited by external forces can be found.

3. VULNERABILITIES & THEIR PRIORITIES

a. Current Vulnerability Analysis

There are many vulnerabilities that have been found within endpoints. In order to prioritize which vulnerability an analyst should focus on, each vulnerability is categorized using three points:

- Common Vulnerabilities & Exposures
- Common Vulnerability Scoring System
- Risk Equation

Each of these points relies on various factors to determine how critical a vulnerability is to a company, this giving an analyst a way of prioritization.

b. Common Vulnerabilities & Exposures

Common Vulnerabilities and Exposures (CVEs) represent public disclosed security flaws within software systems [5], each assigned a unique ID number for easy reference, such as the format CVE-YYYY-NNNN.

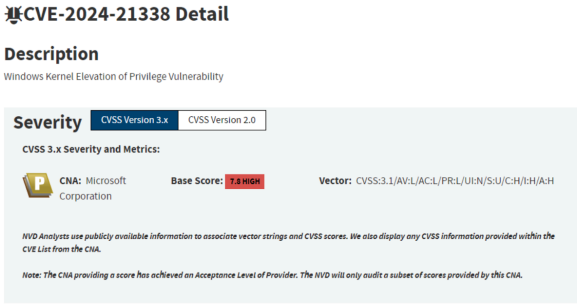

Figure 4. CVE Representation

All of the CVEs ever recorded can be found on the following website: https://nvd.nist.gov/ [6]. In Figure 4., we see an example of a CVE along with the CVSS rating. These identifiers allow for efficient communication and tracking of vulnerabilities across various platforms and organizations. The National Vulnerability Database (NVD), hosted by the National Institute of Standards and Technology (NIST), serves as a central repository for CVEs, providing detailed information about each vulnerability, including its severity, impact, and potential mitigations. CVEs are frequently referenced by plug-in feeds utilized by vulnerability scanning tools and security products. These feeds are constantly updated to include the latest CVE entries, ensuring that organizations have access to up-to-date information about known security weaknesses. Due to their widespread adoption and recognition, CVEs have become an internet standard for identifying and addressing security vulnerabilities, playing a crucial role in cybersecurity risk management and mitigation efforts.

c. Common Vulnerability Scoring System

The Common Vulnerability Scoring System (CVSS) is a standardized framework for evaluating and ranking reported vulnerabilities based on their severity and potential impact on systems and networks. With its latest version, CVSS 3.1, vulnerabilities are assigned a score ranging from 0 to 10, with 10 representing the most severe impact. CVSS provides a structured approach to assessing vulnerabilities, considering factors such as Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, Confidentiality, Integrity, and Availability.

The first five metrics—Attack Vector, Attack Complexity, Privileges Required, User Interaction, and Scope—determine the exploitability of a vulnerability. Attack Vector assesses how remote an attacker can exploit the vulnerability, while Attack Complexity measures the level of difficulty in exploiting it. Privileges Required evaluates the level of access an attacker needs to exploit the vulnerability, and User Interaction considers whether user interaction is required for the exploit to succeed. Scope assesses whether the vulnerability impacts resources beyond its immediate scope.

Figure 5.

The last three metrics:

- Confidentiality
- Integrity
- Availability

form the CIA triad as seen in Figure 5., representing the core principles of

information security [2]. Confidentiality refers to the protection of sensitive data from unauthorized access or disclosure. Integrity ensures that data remains accurate and unchanged, protecting it from unauthorized modifications or tampering. Availability ensures that systems and resources are accessible and usable when needed, guarding against disruptions or denial of service attacks.

For example, a vulnerability with a high Confidentiality score may involve a flaw in a web application that allows attackers to access sensitive user data, compromising the privacy of individuals. A vulnerability with a high Integrity score could be a software bug that enables attackers to modify critical system files, leading to unauthorized changes and potential system compromise. A vulnerability with a high Availability score might involve a denial-of-service vulnerability in a network service, rendering it inaccessible to legitimate users and disrupting normal operations. By considering these factors, CVSS provides organizations with a standardized and repeatable method for assessing and prioritizing vulnerabilities based on their potential impact on the CIA triad.

d. Vulnerability / Risk Formula

Currently, the way that analysts categorize and score a vulnerability is by giving it a score using the vulnerability/risk formula.

$$\text{Risk}(R) = \text{Likelihood}(L) \times \text{Impact}(I)$$

This formula takes into account how likely the vulnerability is executed and multiples it by how much of an impact it would have on the company if the vulnerability were to be exploited. Although this formula does surface. I believe multiple other factors can be taken into consideration when calculating the risk of a vulnerability.

$$\text{Risk}(R) = \text{Criticality}(C) [\text{Likelihood}(L) \times \text{Vulnerability Scores (CVSS)}] \times \text{Impact}(I)$$

It is important to note that the new equation still takes into account the likelihood and impact much like the current equation, however, with the addition of Criticality and the CVSS score we get a more tailor-made risk formula. With this updated formula we take into account many more factors while also consulting the CVSS score.

We will now cover each of the parts of the equation and how they are useful when considering a risk score.

Criticality refers to the significance of a particular event, situation, or system failure within an enterprise, directly impacting the company's operations. It is often quantified by multiplying the probability of an event occurring by its severity, yielding a score typically ranging from 0 to 1, where higher scores indicate greater criticality. An example of a criticality table can be seen in Figure 6.

Figure 6. Criticality Table

By assessing criticality, organizations can prioritize resources and interventions to address high-impact risks effectively and mitigate potential harm to the business.

Likelihood represents a statistical measure of the probability of an event occurring, often assessed through methods such as historical data analysis or predictive modeling. In cybersecurity, likelihood is commonly analyzed using techniques like attack trees, which map out potential paths attackers may take to exploit vulnerabilities and estimate the probability of each path's success. Likelihood scores typically range from 0 to 1, with higher scores indicating a higher probability of the event occurring. By understanding likelihood, organizations can better anticipate and prepare for potential security threats, enabling proactive risk management and mitigation strategies.

Impact refers to the consequences or effects of a risk event, encompassing various outcomes such as financial loss, operational disruptions, reputational damage, and regulatory penalties. It is quantified using a score ranging from 0 to 1, where higher scores indicate greater severity or significance of the impact. By assessing impact, organizations can prioritize risk responses and allocate resources to mitigate potential harm and minimize the adverse effects of risk events on their objectives and stakeholders.

By taking all of these factors into consideration, an analyst can get a better understanding of a vulnerability and how much risk it entails specifically to their company.

As an example, we will calculate the risk of failed logging attempts using both the current risk equation and the new risk equation. First, we will define the base values.

- Likelihood(0-1): 0.7
- Impact(0-1): 0.2
- Criticality(0-1): 0.3
- CVSS(0-10): 7.5

Remember that the CVSS score is standard publicly available information. As for the other factors, they are all determined by the analyst and company. Using the current risk formula, R=LI, the risk score of failed login attempts is 0.14. Using the new formula, R=C(L[CVSS])I, we get 0.315.

According to these results, we get similar answers that fall in the low-risk category. Each category score can be seen in Figure 7.

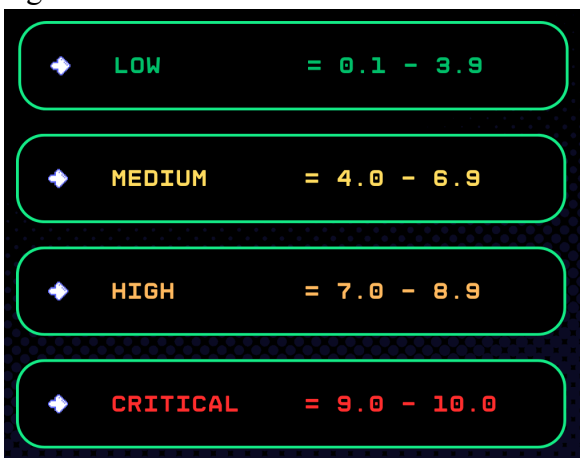

Figure 7. Criticality Scoring System

While both formulas yield identical conclusions, the updated equation facilitates tailoring the risk score to align more closely with the company's specific needs, while also incorporating the CVSS. This enhancement notably increases the efficiency and depth of vulnerability analysis, streamlining the process while providing richer insights.

4. CONCLUSION

In conclusion, endpoint vulnerability scanning tools play a crucial role in identifying and addressing security weaknesses within computer systems, networks, and applications. These tools encompass various categories, including website vulnerability scanning tools, endpoint vulnerability scanning tools, and authenticated/unauthenticated scanning tools, each serving specific purposes in vulnerability detection and mitigation. By leveraging standardized frameworks such as the Common Vulnerability Scoring System

(CVSS) and incorporating factors like criticality, likelihood, and impact, analysts can prioritize vulnerabilities effectively and tailor risk assessments to align with the company's specific needs.

The integration of these factors enhances the depth and efficiency of vulnerability analysis, enabling organizations to proactively manage security risks and safeguard their assets and operations effectively. Moreover, the new risk formula, which incorporates criticality and CVSS scores alongside likelihood and impact, offers a significant improvement over the current formula. By considering a broader range of factors and consulting the standardized CVSS scores, the new formula provides a more comprehensive and tailored approach to risk assessment. This enhancement allows analysts to better understand the specific risk profile of vulnerabilities, leading to more informed decision-making and resource allocation. Overall, the new formula enhances the effectiveness of vulnerability analysis, streamlining the process while providing richer insights and enabling organizations to stay ahead of evolving security threats.

REFERENCES

[2] National Institute of Standards and Technology (NIST). "Common Vulnerability Scoring System (CVSS)." [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss

[3] SANS Institute. "What is CVSS?" [Online]. Available: https://www.sans.org/blog/what-is-cvss/

[4] Microsoft Security Response Center (MSRC). "CVE-2024-21338." [Online]. Available: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21338

[1] ISACA. "An Enhanced Risk Formula for Software Security Vulnerabilities." [Online]. Available: https://www.isaca.org/resources/isaca-journal/past-issues/2014/an-enhanced-risk-formula-for-software-security-vulnerabilities#:~:text=An%20enhanced%20risk%20formula%2C%20Risk,rating%20for%20software%20security%20vulnerabilitieS

[5] Red Hat. "What is CVE?" [Online]. Available: https://www.redhat.com/en/topics/security/what-is-cve

[6] National Institute of Standards and Technology (NIST). "National Vulnerability Database (NVD)." [Online]. Available: https://nvd.nist.gov/

[7] CVE. "CVE Program: About the CVE Program," [Online]. Available: https://www.cve.org/About/Process

[8] FIRST. "Common Vulnerability Scoring System Version 3.1: Specification Document," [Online]. Available: https://www.first.org/cvss/specification-document#:~:text=CVSS%20is%20composed%20of%20four,impact%20across%20different%20deployed%20environments.

[9] Quest. "15 common endpoint security risks organizations need to address," [Online]. Available: https://blog.quest.com/15-common-endpoint-security-risks-organizations-need-to-address/

[10] TechTarget. "Confidentiality, integrity and availability (CIA)," [Online]. Available: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA