Vulnerability Scanning & Management

(An approach to managing the risk level of a vulnerability)

Ziad Khalil\textsuperscript{1}, Mohamed Elammari\textsuperscript{2}

\textsuperscript{1}Higher Academy, \textsuperscript{2}Rogue Wave Software

Ottawa, Canada

Abstract

Vulnerability scanners can reveal different vulnerabilities of a particular system, along with their respective risk levels. However, the veracity of the output is highly dependent on the tool used, as sometimes the estimated risks pertaining to different vulnerabilities do not reflect the reality, irrespective of whether a vulnerability is false positive or not.

The paper introduces a process that can be adopted to manage risks related to the vulnerabilities identified by vulnerability scanning, focusing on the risk rate only. The work presented is based on a manual approach to vulnerability management in order to assign the most reliable risk rates to each one.

Keywords: vulnerability scanning, vulnerability management.

Introduction

The ISO 27002 standard defines vulnerability as “A weakness of an asset or group of assets that can be exploited by one or more threats” [1].

In this context, vulnerability scanning can be understood as utilization of a computer program to identify vulnerabilities in networks, computer infrastructure or applications.
In line with the above, **vulnerability management** is the process in which vulnerabilities are identified and corresponding risks evaluated. This evaluation allows for the vulnerabilities to be addressed, thus removing the risk. Alternatively, the management of an organization may decide to formally accept the risk [2, 6].

In the aforementioned process, **vulnerability scanner** is an invaluable tool, as it facilitates scanning computers, computer systems, networks or applications for security vulnerabilities [7]. Common scanning tools include Security Profile Inspector (SPI), Internet Security Scanner (ISS), Security Analysis Tool for Auditing Networks (SATAN), Tiger, Sscan, Nmap, COPS, Tripwire [8-10], and Nessus Vulnerability scanner [3].

**Vulnerability Scanning**

This paper presents a typical vulnerability scanning process conducted on a target using Nessus Vulnerability scanner. This is one of the security activities constantly performed in an organization. As a part of this ongoing initiative, the security engineers conduct vulnerability scanning and use the results produced by the scanner to assess the identified vulnerabilities and corresponding risks. This formation is subsequently used to produce a report comprising the results yielded by the automatic scanner and their evaluation.

In some cases, the security engineers will go further and manually eliminate the false positive vulnerabilities. This data can be used as a proof of concept typically complementing exploitable tools such as Metasploit Framework [11, 12]. Similarly, more than one scanner can be used simultaneously, whereby comparison of their
respective results can yield valuable information regarding the likely risk rate of each vulnerability. However, even in such cases, the automatically generated vulnerabilities and their respective risks may not reflect those the organization recognizes, since each company has its own priorities and attitudes towards risks.

For example, using Nessus on one of the servers of a Telecom company to obtain vulnerability and risk results of that server produces the outcomes summarized in Figure 1.

![Figure 1. Nessus scan output.](image)

As can be seen from Figure 1, Nessus assesses one vulnerability as Critical, three as Medium and further three as Low. In this paper, the focus is on the vulnerability rated as Critical, along with two with Medium, and one with Low risk. The Critical vulnerability is illustrated in Figure 2.
Figure 2. Critical vulnerability based on a Nessus scan.

According to the scanner assessment, the Critical vulnerability identified on this particular server could be exploited by man-in-the-middle attack, indicating an internal risk. More specifically, this vulnerability is exploitable with Core Impact [Commercial Pentest framework] not shown in the figure.

The two medium vulnerabilities are illustrated in Figure 3 and Figure 4.

Figure 3. Unencrypted Telnet Server (Medium Risk Vulnerability)
Figure 4. DNS Server Spoofed Request Medium Risk Vulnerability.

One of the three vulnerabilities deemed to pose low risk is illustrated Figure 5.

Figure 5. X Display Manager Control (Low Risk Vulnerability)

Vulnerability Management

Discovering vulnerabilities is clearly important; however, this information is of little value if the associated risk to the business is not evaluated accurately.

This section describes an approach that can be adopted to estimate the severity of all of the risks identified by the scanning process, allowing the management to make an
informed decision regarding actions to be taken with respect to each of the risks. Clearly, having an effective and efficient risk rating system in place will save time and eliminate subjectivity in prioritizing actions to be taken.

As previously noted, a vulnerability that is critical to one organization may not be very important to another. Thus, when using the data provided by the scanner, it is useful to consider a basic framework that can be customized to meet the needs of the organization [4].

**Approach**

Risk analysis is a very diverse and complex field and there is no uniform approach. The methodology presented here is based on a widely accepted mathematical expression, which tend to be relatively simple, allowing organizations to calculate and prioritize risks quickly. However, further modifications can be applied if necessary.

Risk rating depends on many factors, some of which are discussed in the following section.

The main risk rating factors are:

1. Technical Impact (I)
2. Access Range (G)
3. Ease of Discover (EoD)
4. Ease of Exploit (EoE)

These can be used in the Risk Rating Formula:
The risk rating factors could be identified by many elements, for example:

3 = High, 2 = Medium, 1 = Low

**Ease with which vulnerabilities can be exploited:**

In terms of its exploitability, a vulnerability can be rated as Vulnerability on the wild (3), Commercial tools only (2), or Required skills (1).

If the exploit vulnerability is available in the wild and the vulnerability could be exploited by an automated tool, the severity of the EoE will be High and will be denoted by 3. If use of commercial tools is necessary to exploit a particular vulnerability, the risk severity will be rated as Medium (2), while Low (1) risk is assigned to a vulnerability that requires skills to be exploited.

**Ease with which vulnerabilities can be discovered:**

How easily a vulnerability can be discovered can also be rated, whereby Difficult (1), Medium (2), and Easy (3) are typically assigned.

**Access Range factors:**

Each vulnerability can also be evaluated based on its range as, for example, Remote (3), Local (2), or Authenticated (1).

If the vulnerability could accessed remotely then the severity is High (3), if the access is locally only, then the severity is Medium (2), and if the access requires authentication then the severity is Low (3).
**Technical Impact factors:**

A particular vulnerability can also be evaluated based on its technical impact, whereby Full Control (3), Denial of Service (2), and Info (1) are usually assigned.

If the vulnerability can be exploited to gain full access to the system, its severity is High (3), whereas if the impact will cause a denial of service, the severity will be deemed Medium (2). Finally, if exploiting a vulnerability would result in access to information only, the severity is Low (1).

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Element</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical Impact (I)</td>
<td>Full Control</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>DOS</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Info</td>
<td>1</td>
</tr>
<tr>
<td>Access Range (G)</td>
<td>Remote</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Local</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Authenticated</td>
<td>1</td>
</tr>
<tr>
<td>Ease of Exploit (EoE)</td>
<td>Wild</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Commercial</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Required Skills</td>
<td>1</td>
</tr>
<tr>
<td>Ease of Discover (EoD)</td>
<td>Easy</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Difficult</td>
<td>1</td>
</tr>
</tbody>
</table>

**Table 1. Values for Risk Factors**

Once a value is assigned to each factor in the formula noted above, it can be applied to each vulnerability to calculate the associated risk rate.
Note: In many extant studies, Likelihood is recognized as one of the main factors, which is here presented as EoD+EoE.

The Risk Rate Scale allows for classifying risks as Low, Medium or High, with corresponding values ranging from 2 to 6, as shown below.

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Risk Rate Scale</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 to &lt;3</td>
<td>LOW</td>
</tr>
<tr>
<td>3 to &lt;5</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>5 to 6</td>
<td>HIGH</td>
</tr>
</tbody>
</table>

Table 2. Risk Rate Scale

The risk level of the vulnerabilities identified during the scanning process will be calculated based on the formula presented earlier.

Risk Analysis

As the most important vulnerability, the one rated as Critical is discussed first.

SunSSH > CBC Plaintext Disclosure.

In order to assign a risk level to this vulnerability, the factors used in the formula will be evaluated against the vulnerability. Many resources will be used to help assign severity to the factors.

The impact of the above SSH vulnerability could lead to unauthorized access, unauthorized modification and disruption of service. Therefore, the severity of the technical impact is deemed High, i.e., I = 3
The Access Range of the vulnerability is Local [5], i.e., \( G = 2 \), while Ease of Discovery is considered easy, since the vulnerability could be identified by an automated tool, i.e., \( \text{EoD} = 3 \). However, as exploiting this vulnerability requires skills, \( \text{EoE} = 1 \).

From the rating presented above, the risk level of the vulnerability can be calculated as:

\[
R = \frac{I + G}{2} + \frac{\text{EoD} + \text{EoE}}{2}
\]

\[
R = \frac{3 + 2}{2} + \frac{3 + 1}{2}
\]

\[ R = 2.5 + 2 = 4.5 \]

Based on the previous classification, this risk level is **Medium**.

While Nessus rated this vulnerability as Critical, and many extant studies considered it as posing High Risk to the organization, here it is deemed only Medium Risk. However, as previously noted, this rating is based on a default configuration and the organization's situation will determine what this vulnerability's risk will be in practice.

**Unencrypted Telnet Server**

In this section, the first vulnerability deemed of Medium Risk is analyzed in detail. The remote Telnet server transmits traffic in cleartext, which can allow man-in-the-middle attacks, whereby company employees can eavesdrop on a Telnet session to obtain confidential information.
Given the above, the technical impact of this vulnerability is considered High (3), since the attacker can use the session data to take control of the system.

In addition, Access range is Local (2), while the Ease of Discovery is easy (3), since using a free tool could be used to gain access to the session.

Finally, the Ease of Exploit is rated as 3.

Thus, the Risk can be calculated as:

\[ R = \frac{3+2}{2} + \frac{3+3}{2} = 2.5 + 3 = 5.5 \]

Based on the previous classification, this corresponds to **High** Risk Level.

**DNS Server Spoofed Request Amplification DDoS.**

This section pertains to the other Medium vulnerability. Based on the Nessus report, "The remote DNS server answers to any request. The remote DNS server could be used in a distributed denial of service attack."

Thus, the Technical Impact is DOS (2).

The Access Range is Remote (3).

The Ease of Discovery is set at 2 and the Ease of Exploit is 1.

Given the data above, the Risk equals:

\[ R = \frac{2+3}{2} + \frac{2+1}{2} = 2.5 + 1.5 = 4 \]

Hence, the Risk is **Medium.**
X Display Manager Control Protocol (XDMCP) Detection

Finally, one of the Low vulnerabilities is discussed in this section. XDMCP allows a UNIX user to remotely obtain a graphical X11 login (and therefore act as a local user on the remote host).

The Technical Impact is thus 3, because attackers that gain the necessary credentials can obtain full access to the system.

The Access Range is Remote (1).

The Ease of Discovery is set at 2 and the Ease of Exploit is 1.

The Risk can thus be calculated as: \[ R = \frac{3+1}{2} + \frac{2+1}{2} = 2 + 1.5 = 3.5 \]

This value corresponds to Medium risk.

Justification for the Formula

As a proof of concept that can provide justification for the formula used above, another vulnerability scan was conducted against the same server using OpenVAS vulnerability scanner [13]. The scan results did not align with those produced by Nessus. However, in this work the focus is on the risk level only.

One of the vulnerabilities found by OpenVAS is X Display Manager Control Protocol (XDMCP). This vulnerability was rated by Nessus as Low Risk, while OpenVAS classified it as Medium Risk, as shown below.
Having the same vulnerability assigned a different risk rate could be confusing when it comes to managing and prioritizing risks. Thus, it is advisable that each organization adopts a customized formula appropriate to its level of risk aversion. This would allow those in the decision-making positions to focus on actions to be taken, while relying on a unified method to calculate the risks.

After assessing the severity of all identified risks, the organization can prioritize them and determine the course of action associated with each. As a general rule, the most severe risks should be mitigated first.

**Conclusion**

Vulnerability scanning is one of the most important activities in penetration testing, and can be accomplished easily by employing many of the commercially available vulnerability scanners. However, this reliance on automated tools may cause companies to overlook the importance of vulnerability management process. In this work, a simple method for calculating risks associated with vulnerabilities was presented, which can be adopted without any additional cost. Its simplicity will hopefully encourage a greater
number of companies to manage the vulnerabilities and their associated risks more proactively.

Having a customized risk rating methodology allows security administrators and penetration testers to identify and prioritize risks, in order to make decisions regarding the appropriate course of action regarding each risk (i.e., whether to fix, mitigate, transfer or accept those risks).

References


