CS631 Final Project
Risk Identification and Assessment

Akanksha Singh, Roll No. :21111005
Gajender Sharma, Roll No. : 21111028
Gargi Sarkar, Roll No. : 21111263
Manu Shukla, Roll No. : 21111040
Shiv Kumar Yadav, Roll No. :21111057

November 2021

Contents

1 Introduction

Organizations in both the public and private sectors rely on information technology and information systems, specifically industrial control systems, networks, and telecommunication system etc, to successfully carry out their business functions and missions. The information system is under attack from a variety of sources. Threats can severely impact an organization's operation and mission by exploiting both unknown and known vulnerabilities to breach confidentiality, integrity, and availability. As a result, continuous risk assessment is required to achieve a stable state.

2 Goal

Risk assessment is done to identify relevant threats to organization , to identify external and internal vulnerabilities, measurement of impact(harm) that may occur given the potential for threats exploiting vulnerabilities and the likelihood that the harm will occur and finally to determine the risk. Our goal here is to query the national vulnerability database and find vulnerabilities, the user will enter information about the system and the threats related to the system and accordingly it will display the vulnerabilities. Based on those vulnerabilities and certain threats, to let the user to assess the system's risk (less ambiguous)

3 Definitions

3.1 Vulnerability

A vulnerability is a weakness present in a system that a threat source could exploit. Vulnerabilities are identified in the information system and can be found in organizational governance structure caused by a lack of effective risk management strategies. Vulnerabilities can also be found in external relationships, for example, supply chain, telecommunication providers. The vulnerability could also be based on predisposing conditions like natural calamities, outdated technologies consisting of end of service devices, Etc.

3.2 Threat

Any circumstance or event that has the potential to negatively impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification, or denial of service is considered a threat. Additionally, the likelihood that a threat source will be successful in exploiting a specific information system vulnerability.

3.3 Risk Assessment

Risk assessment is the process of determining the likelihood of threats being used against the vulnerabilities present in a system component and drawing conclusions about the resulting impact when a successful compromise occurs. Finally, it provides a foundation for developing policies and selecting cost-effective techniques for putting those policies into action in order to protect the system from cyber attacks. We will be following the first 7 steps of NIST methodology for conducting risk management [1].

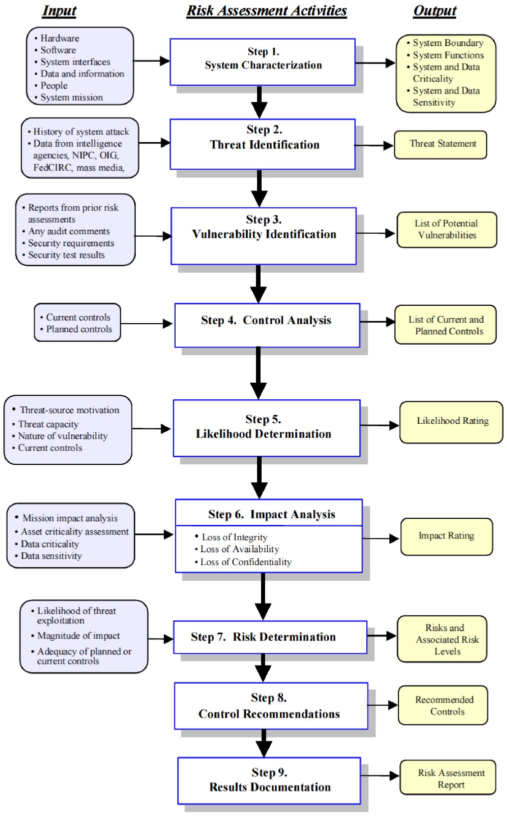

Input
Risk Assessment Activities
Output
• Hardware • Software • System interfaces • Data and information • People • System mission
Step 1. System Characterization
• System Boundary • System Functions • System and Data Criticality • System and Data Sensitivity
• History of system attack • Data from intelligence agencies, NIPC, OIG, FedCIRC, mass media,
Step 2. Threat Identification
Threat Statement
• Reports from prior risk assessments • Any audit comments • Security requirements • Security test results
Step 3. Vulnerability Identification
List of Potential Vulnerabilities
• Current controls • Planned controls
Step 4. Control Analysis
List of Current and Planned Controls
• Threat-source motivation • Threat capacity • Nature of vulnerability • Current controls
Step 5. Likelihood Determination
Likelihood Rating
• Mission impact analysis • Asset criticality assessment • Data criticality • Data sensitivity
Step 6. Impact Analysis
• Loss of Integrity • Loss of Availability • Loss of Confidentiality
Impact Rating
• Likelihood of threat exploitation • Magnitude of impact • Adequacy of planned or current controls
Step 7. Risk Determination
Risks and Associated Risk Levels
Step 8. Control Recommendations
Recommended Controls
Step 9. Results Documentation
Risk Assessment Report

Figure 3-1. Risk Assessment Methodology Flowchart

Figure 1: NIST-Risk Assessment Methodology Flowchart showing different steps,input and output of this steps

4 Methodology and Work Done

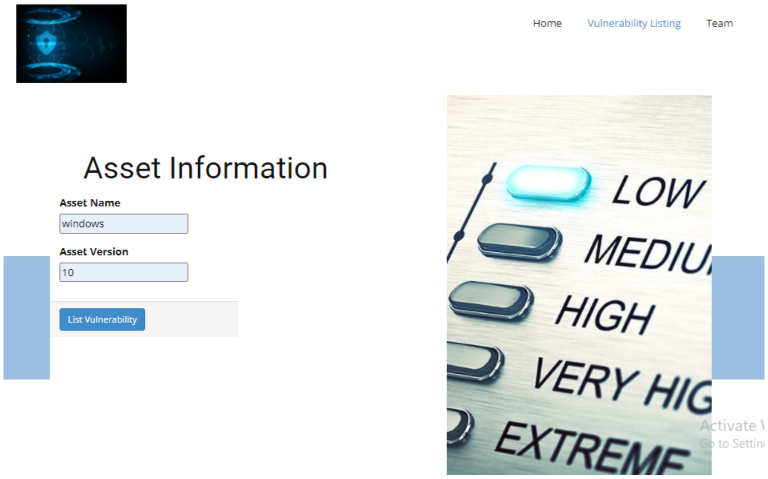
In this section we will discuss the methods we used and the work we did to carry out our risk assessment. We have created a webapp using Django to implement our idea, the details of which will be covered in the subsections.

4.1 NIST-NVD API

In order to identify vulnerabilities of an asset, we have created an API that would exploit NIST's National Vulnerability Database(NVD). Since there are thousands of vulnerabilities for a single asset, we have decided to sort the recent vulnerabilities in the descending order of Base Score. The Base Score reflects the severity of a vulnerability according to its intrinsic characteristics, which are constant over time and assume the reasonable worst-case impact across different deployed environments. From the sorted list of vulnerabilities, we take the top 5 for the user as this seemed feasible for creating the matrix.

4.2 Collecting data related to System Characterization

The first step is to gather information about system components, such as the list of hardware models, their versions, software, patch levels, running operating system details, firmware, and so on.



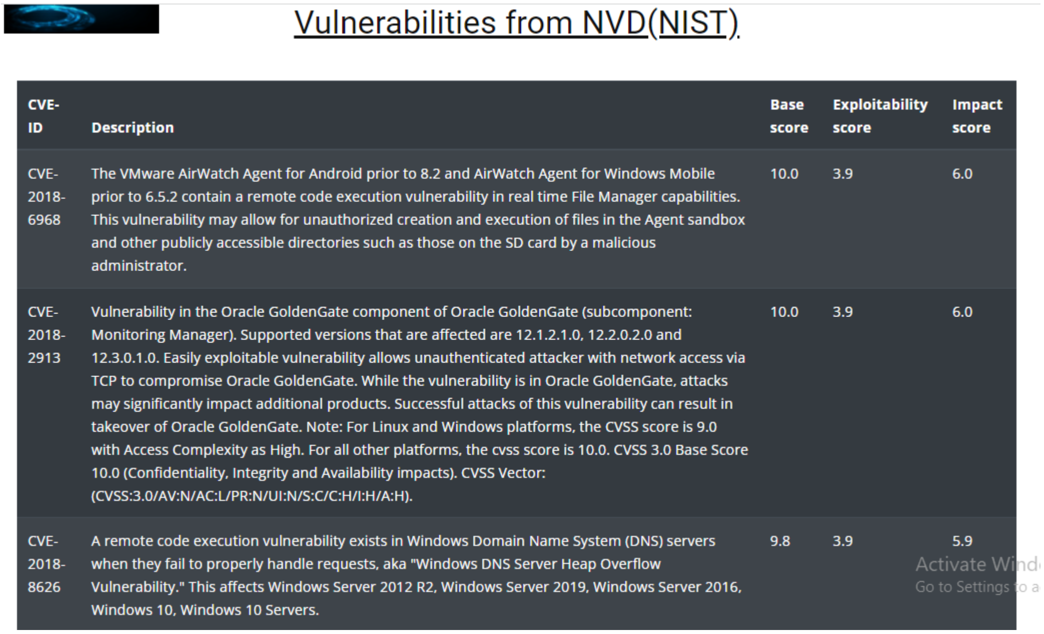
Asset Information

Asset Name: windows

Asset Version: 10

4.3 Vulnerability Identification

We send the collected information to our API to receive the top 5 recent vulnerabilities of it present in NIST-NVD. We list those vulnerabilities to the user along with their Description, Base Score, Exploitability Score and Impact Score.

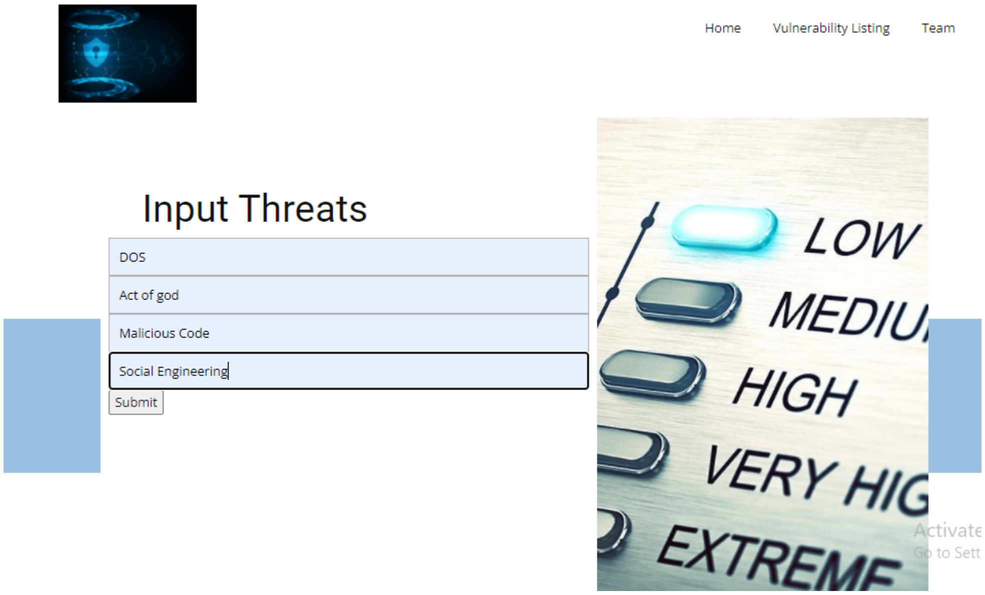


Vulnerabilities from NVD(NIST)

CVE-ID	Description	Base score	Exploitability score	Impact score
CVE-2018-6968	The VMware AirWatch Agent for Android prior to 8.2 and AirWatch Agent for Windows Mobile prior to 6.5.2 contain a remote code execution vulnerability in real time File Manager capabilities. This vulnerability may allow for unauthorized creation and execution of files in the Agent sandbox and other publicly accessible directories such as those on the SD card by a malicious administrator.	10.0	3.9	6.0
CVE-2018-2913	Vulnerability in the Oracle GoldenGate component of Oracle GoldenGate (subcomponent: Monitoring Manager). Supported versions that are affected are 12.1.2.1.0, 12.2.0.2.0 and 12.3.0.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle GoldenGate. While the vulnerability is in Oracle GoldenGate, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle GoldenGate. Note: For Linux and Windows platforms, the CVSS score is 9.0 with Access Complexity as High. For all other platforms, the cvss score is 10.0. CVSS 3.0 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	10.0	3.9	6.0
CVE-2018-8626	A remote code execution vulnerability exists in Windows Domain Name System (DNS) servers when they fail to properly handle requests, aka "Windows DNS Server Heap Overflow Vulnerability." This affects Windows Server 2012 R2, Windows Server 2019, Windows Server 2016, Windows 10, Windows 10 Servers.	9.8	3.9	5.9

4.4 Threat Identification Process

The user will now have to provide the possible threats that he expects on the system and we perform our analysis of the likelihood of each threat on each vulnerability.



Input Threats

DOS

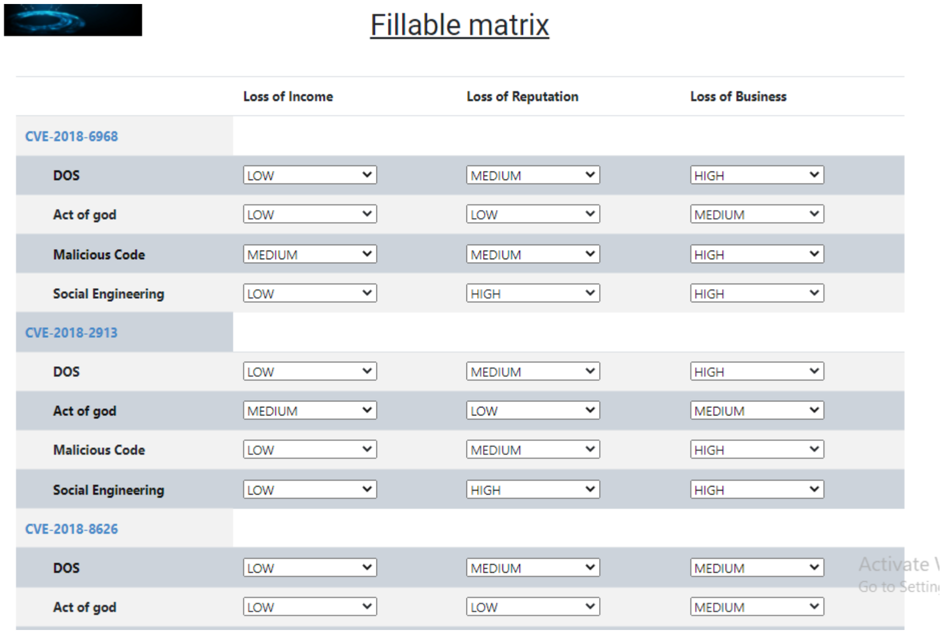
Act of god

Malicious Code

Social Engineering

4.5 Likelihood Determination

Likelihood is the weighted risk factor. It is calculated based on the probability that when a threat is given, how much it is capable of exploiting a given vulnerability. Likelihood is occurrence is estimated basically based on historical data, adversary capability , intent and to whom the adversary is targeting or state of the organization. There are three step to determine the overall likelihood of threat events. First of all assessing the likelihood that the threat events will be initiated, then assessing the likelihood that the threat events once initiated , how much it will affect asses, individuals, or the nation, finally assessment of the overall likelihood as a combination of likelihood of occurrence and likelihood of resulting adverse impact. Likelihood indicates about the possibilities of a threat exploiting existing vulnerabilities in a system and if the exploitation becomes successful what will be the amount of loss to face. if the system is already patched against certain vulnerabilities , then for some threats possibility of exploiting those certain vulnerabilities comes up with very low likelihood. on other hand if a threat is exploiting certain vulnerabilities which are still present in the system , the likelihood goes up accordingly. Likelihood is not usually numerically computed but computed qualitatively. It depends on the amount of vulnerabilities present , the characteristic of the vulnerabilities , the exposure related to insider and outsider threat, number of attachment point with the external world, the present equipment safety level, awareness of the employees,what is the nature of target and whats the current threat landscape of that.

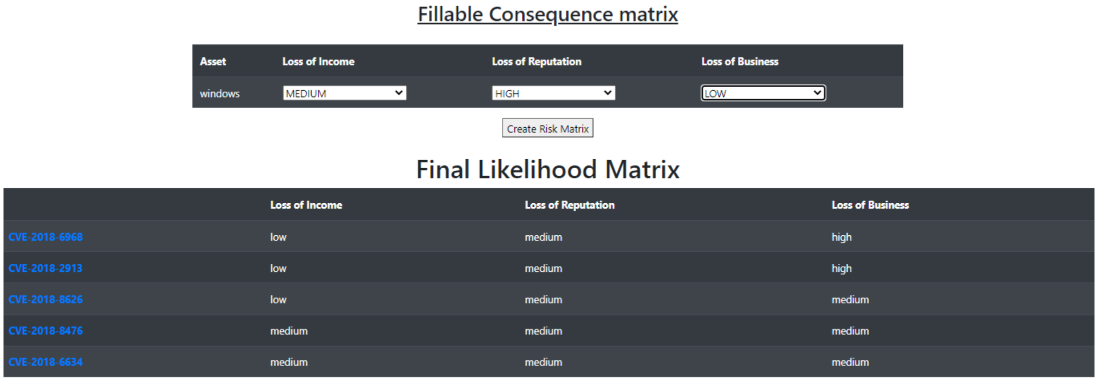


Fillable matrix

	Loss of Income	Loss of Reputation	Loss of Business
CVE-2018-6968			
DOS	LOW	MEDIUM	HIGH
Act of god	LOW	LOW	MEDIUM
Malicious Code	MEDIUM	MEDIUM	HIGH
Social Engineering	LOW	HIGH	HIGH
CVE-2018-2913			
DOS	LOW	MEDIUM	HIGH
Act of god	MEDIUM	LOW	MEDIUM
Malicious Code	LOW	MEDIUM	HIGH
Social Engineering	LOW	HIGH	HIGH
CVE-2018-8626			
DOS	LOW	MEDIUM	MEDIUM
Act of god	LOW	LOW	MEDIUM

4.6 Impact Analysis

Impact is the magnitude of harm that is caused when a successful attack happened. The consequences include breaching the confidentiality i.e disclosure of information, integrity i,e unauthorized modification or destruction of information and availability of system . Impact may vary to different organization and hence its mostly predefined from strategic policies and planning . If a particular vulnerability got exploited , what and how it would jeopardise the mission of the organization. After impact analysis we will be getting an impact rating(another matrix)



Fillable Consequence matrix

Asset	Loss of Income	Loss of Reputation	Loss of Business
windows	MEDIUM	HIGH	LOW

Final Likelihood Matrix

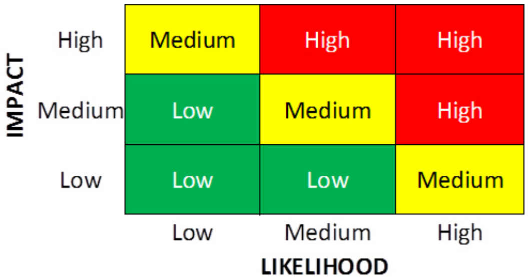
	Loss of Income	Loss of Reputation	Loss of Business
CVE-2018-6968	low	medium	high
CVE-2018-2913	low	medium	high
CVE-2018-8626	low	medium	medium
CVE-2018-8476	medium	medium	medium
CVE-2018-6634	medium	medium	medium

4.7 Risk Determination

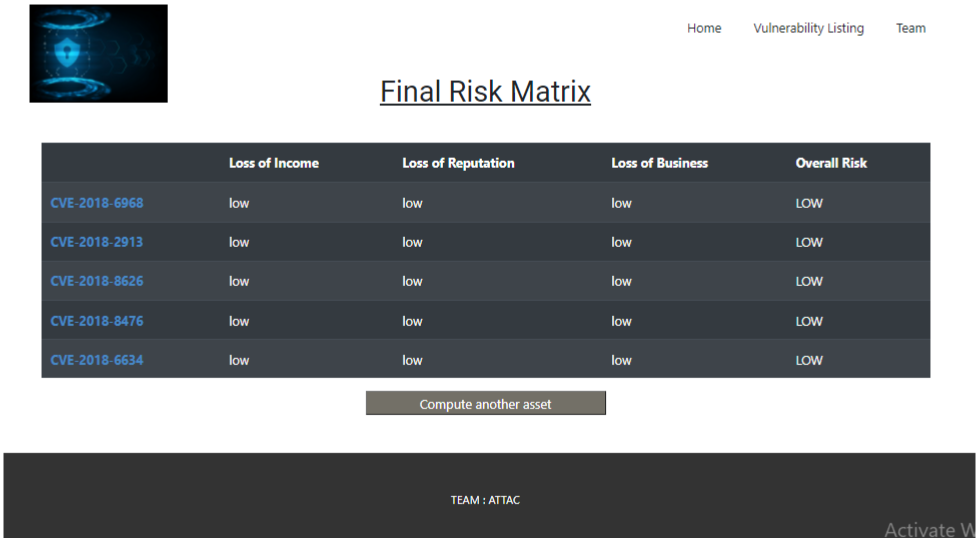
The classical risk equation for risk assessment is given by :

$$risk = threat * vulnerability * consequence$$
$$risk = likelihood * consequence$$

Basically risk is a function of the adverse impacts that would arise if the events got exploited. in information security the risks arise from loss of confidentiality, data integrity,or data availability which leads to potential adverse impacts on mission, function, reputation,image etc i.e on the organizational operations, assets etc.The overall risk is determined using the matrix given below.



IMPACT				
	High	Medium	High	High
	Medium	Low	Medium	High
	Low	Low	Low	Medium
		Low	Medium	High
			LIKELIHOOD	



Final Risk Matrix

	Loss of Income	Loss of Reputation	Loss of Business	Overall Risk
CVE-2018-6968	low	low	low	LOW
CVE-2018-2913	low	low	low	LOW
CVE-2018-8626	low	low	low	LOW
CVE-2018-8476	low	low	low	LOW
CVE-2018-6634	low	low	low	LOW

TEAM : ATTAC

4.7.1 Acceptable level of risk in a system

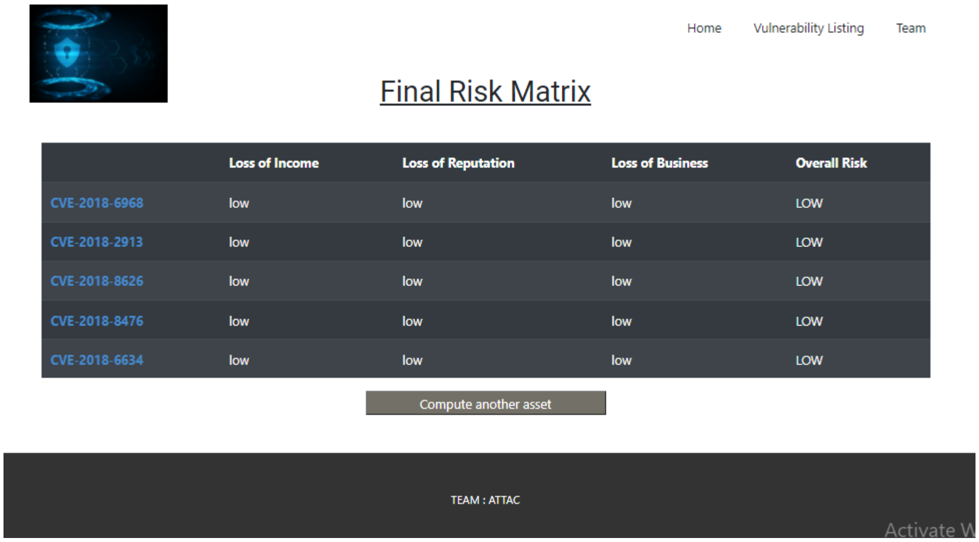
A thing is safe if its risks are judged to be acceptable. A risk is acceptable when it falls below some arbitrary defined probability . The term " acceptable risk" describes the likelihood of an event whose probability of occurrence is small, and the consequences are low , but the benefits are so great that the organization is willing to be subjected to the risk that the event might occur.

if the recomputable risk after doing counter measure is not below acceptable risk , then we have to do more mitigation . We identify the gap between current system risk level and the initial requirements by the organisation, create action plan and add additional control points to control the risk and bring it in acceptable range.

5 Results

The risk assessment matrix presents the possibility of an attack occurring in an industry. It is quantitative estimation of the particular vulnerability exploited by various threat to the industry across the world. It is qualitative estimation of the the particular consequences that a particular company might have to face in case the attack takes place.

The risk assessment matrix brings in light the several vulnerabilities associated with a asset and the severity of the harm that an attack exploiting that vulnerability will have over the companies social and economic aspects. The matrix gives the security team the priority of the vulnerabilities present(based on impact), so that the company can deploy resources in an efficient way to guard from the most juicy vulnerabilities. As it estimates the possibility and impact of explaitation of all vulnerabilities present it also provides an assurance about the level of security that the company has from the cyber physical attacks against them.



Final Risk Matrix

	Loss of Income	Loss of Reputation	Loss of Business	Overall Risk
CVE-2018-6968	low	low	low	LOW
CVE-2018-2913	low	low	low	LOW
CVE-2018-8626	low	low	low	LOW
CVE-2018-8476	low	low	low	LOW
CVE-2018-6634	low	low	low	LOW

6 Conclusion

The project gave an understanding of the importance of risk assessment for a company. The assets are identified and the vulnerabilities present in them are fetched from the NVD database. The database provides several ways to fetch the vulnerabilities like based on year of found, version, particular CVE-id, etc..

The project allowed us to appreciate the huge vulnerability database maintained centrally and the efforts that the people in industry are taking to minimise the possibility of cyber attacks by overcoming the listed vulnerabilities. The community is creating awareness about the possibility of exploiting the loop holes. The NVD api provides a way to integrate this database with projects.

The security team of company can then identify the possibility of the attacks listed for happening in their industry and also the corresponding likelihood of the attack.

7 Future Goal

Although the proposed project works perfectly for an asset, there is still much scope for improvement. We want to extend our work to do complete risk analysis for complex OT(ICS, Scada, DCS) systems. We want to allow the user to include complex network diagrams and assets(independent and interconnected/dependent) and then perform a risk assessment for the entire system.

8 Acknowledgement

This project and its associated report would not have been possible without the exceptional support and guidance of our prof. Sandeep k. Shukla. We would like to express our heartfelt appreciation and gratitude to him. We'd also like to thank our TA, Venkata Sai Charan Putrevu, for guiding us through the journey.

References

[1] Nist special publication 800-30,guide for conducting risk assessments.