Rapid and Proactive Approach on Exploration of Database Vulnerabilities

A. Ramachandran
Department Of Computer Science And Engineering,
Anna University Of Technology,
Tiruchirappalli, Tamilnadu – 602 024. INDIA.
ramautpc@gmail.com

S. Ramachandran

Department Of Computer Science And Engineering,
Anna University Of Technology,
Tiruchirappalli, Tamilnadu – 602 024. INDIA.
ramachandran_engg@yahoo.com

Abstract **In today's complicated computing environment, managing data has become the primary concern of all industries. Information security is the greatest challenge and it has become essential to secure the enterprise system resources like the databases and the operating systems from the attacks of the unknown outsiders. Our approach plays a major role in detecting and managing vulnerabilities in complex computing systems. It allows enterprises to assess two primary tiers through a single interface as a vulnerability scanner tool which provides a secure system which is also compatible with the security compliance of the industry. It provides an overall view of the vulnerabilities in the database, by automatically scanning them with minimum overhead. It gives a detailed view of the risks involved and their corresponding ratings. Based on these priorities, an appropriate mitigation process can be implemented to ensure a secured system. The results show that our approach could effectively optimize the time and cost involved when compared to the existing systems.**

Index Terms: **software engineering, fault injection, attack injection, vulnerability assessment.**

I. Introduction

In today's complex computing environment, managing data has become the primary concern of all industries. Information security is the greatest challenge that confronts an enterprise today. Many organizations tend to implement client and network security solutions designed to protect workstations and network resources. This is because data is not just accessed by the company's employees but is open for access by its partners as well as its customers. Thus it becomes essential to secure enterprise system resources like the databases and the operating systems from the attacks of the unknown outsiders. ID Theft, data breaches, data exposure crimes are at an increasing rate in the recent days and are motivated by financial gains.

Administrative error, for example, is a primary cause of vulnerabilities that can be exploited by a novice hacker, whether an outsider or insider in the organization. Routine use of vulnerability assessment tools along with immediate response to problems identified will alleviate this risk. It follows, therefore, that routine vulnerability scanning should be a standard element of every organization's security policy. This vulnerability scanning has been designed to allow organizations to build up their crisis management capability. Its purpose is to help answer the question: "How secure is your organization's information?" This crucial question emerges over and over as one of the highest priorities in an organization.

This allows the organization to develop their crisis planning capability by:

a) Detailing the vulnerabilities of the organization

b) Developing response plans and procedures

c) Improving capability of crisis management teams

KNOW YOUR VULNERABILITY

A vulnerability scanner detects the flaws in the database. It is essential to know your enemy before you attack them. So, let's see what the common vulnerabilities threats are. Vulnerability is an error or weakness in a component that allows it to be attacked, resulting in unauthorized use of the item or in damage to it and components connected to it. In an information-technology network like the Internet, successful exploitation of vulnerabilities can result in operating-system damage, illegal release of information, data destruction, disruption of service, and a galaxy of other tribulations.

"As Internet-accessible systems are the most vulnerable to remote attackers, organizations should continue to evaluate those systems to identify, analyse, and fix vulnerabilities."

Some common vulnerability that is detected in a target systems are:

- Common Configuration Errors - Many systems have inadequate configuration settings, leaving various openings for an attacker to gain access.
- Default Configuration Weaknesses - Often many systems have very weak security settings, including default accounts and passwords.
- Well-known System Vulnerabilities - Every day, volumes of new security holes are discovered and published in a variety of locations on the Internet. Vendors try to keep up with the attack of newly discovered vulnerabilities by creating security patches. However, once the vulnerabilities are published, a flurry of attacks against un-patched systems is inevitable.

  Identifying such vulnerable areas is done by authorized technicians, who see a system from an attacker's perspective so it can be fixed or the risk of intrusion minimized. In that context, two tasks are to be addressed:
- First, to minimize an intruder's incentive by limiting the enticements that leads an intruder to probe a system.
- Second, to maintain a system so that it is less susceptible to actual intrusion and better prepared to recover from an attack.

AUDITING VULNERABILITY

Auditing is no longer a financial term but is associated with evaluation of the internal controls of the system. IT audit is concerned with determination of the risks that are likely to attack the target system and mitigate these risks. Protection of Information assets of an organization is served by IT auditing tools which reviews and evaluates the organization's data availability, confidentiality and integrity.

Vulnerability audit ensures that the data is free from risk and is in par with the IT security standards. This is achieved by developing a system by means of audit and compliance with security standards. With rapid growth in both the number and sophistication of cyber attacks, it has become imperative that cyber defenders be equipped with highly effective tools that identify security vulnerabilities before they are exploited.

Vulnerability can be defined as a set of conditions which if true, can leave a system open for intrusion, unauthorized access, denied availability of services running on the system or in any way violate the security policies of the system [2]. While breaches happen at every corner of an enterprise network, often the security of the end hosts is the most brittle line of defence. A breach of security occurs when a stated organizational policy or legal requirement regarding information security, has been contravened. The only way for a business to protect its most critical data from both outside hackers and unscrupulous insiders is to ensure that the database is properly configured, patched, and locked down. Our approach is to find security holes and configuration problems in the database, and then present the user with a report detailing the issues found and recommended fixes.

Our identification of missing patches, weak passwords, and insecure configuration settings is the main purpose for using this proactive approach. It can be configured to perform configuration policy compliance scans (Health

Insurance Portability and Accountability Act (HIPAA)), automatically determining if applications are configured properly, and calling out exactly which settings violate the policy.

The proposed architecture has the following advantages over the conventional design. Our proactive approach plays a major role in detecting and managing vulnerabilities in complex computing systems. It allows enterprises to assess two primary tiers through a single interface as a vulnerability scanner tool which provides a secure system which is also compatible with the security compliance (like Common Vulnerabilities and Exposures (CVE), HIPAA, etc.) of the industry.

It provides an overall view of the vulnerabilities in the OS and database, by automatically scanning them with minimum overhead. It gives a detailed view of the risks involved and their corresponding ratings. Based on these priorities, an appropriate mitigation process can be implemented to ensure a secured system. The results show that our tool could effectively optimize the time and cost involved when compared to the existing systems. This architecture also supports other high level security analysis on the data collected from all the hosts on the network. Our research is conducted within the context of the Multi-host, multi-stage. Vulnerability Analysis enterprise-level security analyzer that can automatically compute all possible multi-step, multi-host attack paths in an enterprise network based on security vulnerabilities discovered on end hosts

Our goal is to design architecture for host-based security scanning, which enables more efficient and flexible usage of external knowledge in enterprise network security management, and supports a range of enterprise-level security analysis based on information provided by host-based security scanning.

II. LITERATURE REVIEW

With the rapid development of more complex systems, the chance of introduction of errors, faults and failures increases in many stages of software development life-cycle [8]. This class of system failures is commonly termed as software vulnerabilities. These security vulnerabilities violate security policies and can cause the system to be compromised leading to loss of information [9]. Vulnerabilities can be introduced in a host system in different ways; via errors in the code of installed software, mis-configurations of the software settings that leave systems less secure than they should be (improperly secured accounts, running of unneeded services, etc.) [10].

Vulnerability analysis, also known as vulnerability assessment, is a process that defines, identifies, and classifies the vulnerabilities (security holes) in a computer, network, or communications infrastructure [11]. Vulnerability analysis can be used to predict the effectiveness of the proposed countermeasures and evaluate them after they are put into use. Vulnerability analysis begins with gathering, defining and classifying network or system resources. The resources can be classified according to their level of importance in the network. Next comes the identification of potential threats to those resources. This stage of identification of threats can be performed by probing the network or system to discover potential weak points.

A vulnerability assessment tool (or scanner) can be defined as a utility that can be used to test the capability of a systems or networks security and discover their points of weakness [2]. These tools themselves do not provide any kind of security or protection to the system, rather they gather and report information, which can be used to instate a different tool, policy or mechanism to secure the system. Vulnerability assessment tools can be broadly classified into network based and host based analysers as described in the following Sections 2.1 and 2.2 respectively.

2.1 NETWORK BASED ANALYZERS

Network based vulnerability assessment gathers information of the system and services attached to the network and identify weakness and vulnerabilities exploitable in the network. These vulnerabilities could be related to services, such as HTTP, FTP and SMTP protocol, running on the given network. A network-based scanning assessment may also detect extremely critical vulnerabilities such as mis-configured firewalls or vulnerable web servers in a De-Militarized Zone (DMZ), which could provide a security hole to an intruder, allowing them to compromise an organizations security [4].

Network assessment tools gather information and may also have network mapping and port scanning abilities. Typical network based scanner architecture is shown in Fig 1.

In addition it also has an interactive console, which helps the administrator to schedule vulnerability assessments on different targets on the network. Furthermore the scanning engine is the main component of the network based scanner. It performs the assessment as instructed by the interactive console by sending specially constructed packets for the test. Results repository is the final component, which holds the entire scan results received and is also used for report generation for the system administrators [12]. The strengths of network based scanners lie in the fields described below:

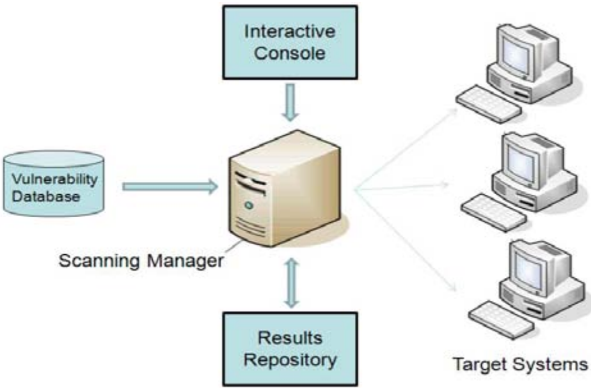


Fig 1: Architecture of a typical Network-Based Analyzer

However network-based scanners also have the following demerits:-

1. A network-based scanner does not have direct access to the target's file system. Thus, it is not able to check for file permission.
2. Another problem which network based scanners face is their inability to scan targets behind a firewall. Complicated measures have been taken to let scanners get to these target systems.
3. Network based scanners may also face the problem of network congestion due to a lot to-and-fro data transfer.

2.2 HOST-BASED ANALYZERS

Host based analyzers also scan the system for vulnerabilities like the network scanners, however they are able to scan much more due to the fact that they have a service/agent residing on the target system. They can easily identify system-level vulnerabilities such as file permissions, user account properties and registry settings. A typical host-based architecture is shown in Fig 2. The host-based analyzer is installed on a network by first installing a scanning manager on the network.

Agents are then installed on all the target systems to be scanned. The working of these agents is controlled by the manager. In some systems, there may be a separate user console to interact with the scanning manager, which is merged with the manager otherwise. When the manager wants to initiate a scan, it sends the necessary information like scanning policy to the agent on the host. The scanning policy consists of the different vulnerability checks. The agent on the host scans accordingly and reports back the results of the scan. As new vulnerabilities are discovered frequently the security definitions have to be regularly updated on each agent.

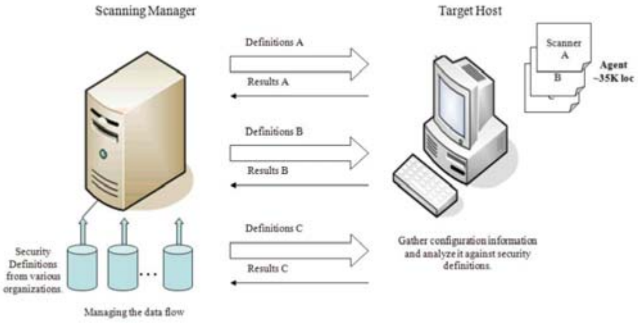


Fig 2: Architecture of Conventional Host-Based Analyzer.

The main strength of host-based scanners lies in the fact that they have direct access to configuration details and services of the target system. However, host-based scanners do not come without weaknesses.

They are described below:-

1. The scanning agents have to be installed on new systems and updated regularly on the old ones to keep the assessment fool-proof.
2. System administrators are reluctant to install unknown agents on the production systems.
3. Agents residing on the target host utilize its resources, sometimes interfering in the normal functioning of the host.
4. As the enterprise network increases in size, managing and updating agents on all the hosts becomes an issue.

2.3 ATTACK INJECTION METHODOLOGY

A penetration test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious hacker (Fig 3). The process involves an active analysis of the system for any weaknesses, technical flaws or vulnerabilities. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution [1].

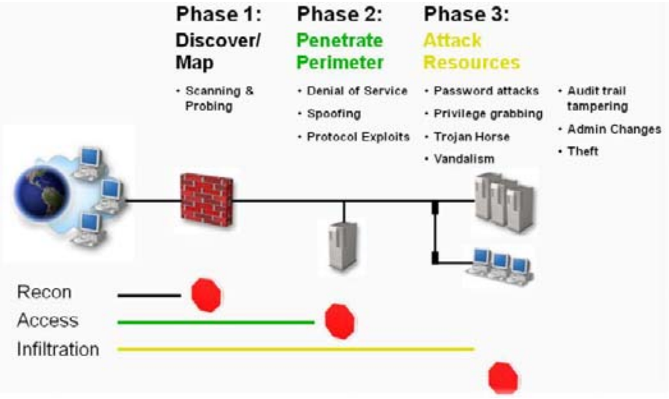


Fig 3: Penetration test

Target system is attacked automatically by using attack generation algorithm. Discovery of vulnerabilities in server applications is based on the behaviour of malicious adversaries. Generate several attacks against a target network server, while observing its execution. This monitoring information is later Analyzed to determine if the server executed correctly, or on the other hand, if it exhibited any suspicious behaviour suggesting the presence of vulnerability. An attack Injection Methodology architecture is shown in Fig 4.

In the Existing system attack injection methodology has been used which is not suitable for online computation system example ATM, Banking etc). It has become critical for organizations to add database-specific attacks injection to their existing security infrastructure.

Since all online system are incorporated with special user profile mechanism they never allow to inject the attacks (ie When we enter wrong user credential more than 3 time the corresponding account get locked automatically based on predefined profile settings

Benefits of Penetration Testing

A successful penetration test provides indisputable evidence of the problem as well as a star ting point for prioritizing remediation. Penetration testing focuses on high-sever vulnerabilities and there are no false positives.

Drawbacks of Penetration Testing

Penetration testing focuses on vulnerabilities that allow command execution. Most command-execution vulnerabilities are buffer over flows, which inherently run the risk of crashing computers or services. However, automated penetration tests schedule the exploits from least to most dangerous. Another drawback is false negatives because buffer over flow exploits require precision within varying memory states. In addition, penetration testing only detects vulnerabilities which lead to penetration; this excludes cross-site scripting, denial of service, information gathering, etc.

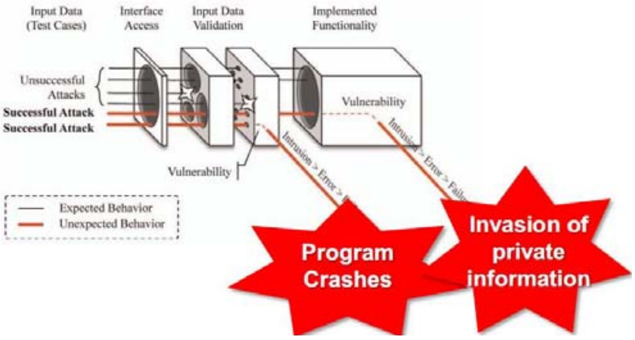


Fig 4: Attack Injection Methodology

III. PROPOSED SYSTEM

RAPID AND PROACTIVE VULNERABILITIES SCANNING (RPVS) is analogous to NAC (Network Admission Control) commonly implemented at the Network Router level to identify and quarantine new hardware systems, till they are thoroughly scanned for vulnerabilities.

Our proactive approach plays a major role in detecting and managing vulnerabilities in complex computing systems. It allows enterprises to assess two primary tiers through a single interface as a vulnerability scanner tool which provides a secure system which is also compatible with the security compliance (like CVE, HIPAA, etc.) of the industry.

When the term "Vulnerability assessment" is used in the context of vulnerability scanners it means "the process" of finding known vulnerabilities in a network. This process identifies vulnerabilities so they can be eliminated before exploited by malicious software or hackers. In most cases the vulnerabilities are known and can therefore be found. The vulnerabilities that constitute threats in a network include software defects, unnecessary services, mis-configurations and unsecured accounts [2]. Proposed architecture is shown in Fig 5.

The vulnerability scanner works with a proactive approach, it finds vulnerabilities, hopefully, before they have been used. There is however a possibility that a, to the public, unknown vulnerability is present in the system. A program that takes advantage of an unknown vulnerability is called a "Zero day exploit". A Zero day exploit is unknown to security professionals which mean that information about the exploit is not publicly available [5].

Our proactive approach provides an overall view of the vulnerabilities in the OS and database, by automatically scanning them with minimum overhead. It gives a detailed view of the risks involved and their corresponding ratings. Based on these priorities, an appropriate mitigation process can be implemented to ensure a secured system. The results show that our tool could effectively optimize the time and cost involved when compared to the existing systems.

The only way for a business to protect its most critical data from both outside hackers and unscrupulous insiders is to ensure that the database is properly configured, patched, and locked down. Our approach is to find security holes and configuration problems in the database, and then present the user with a report detailing the issues found and recommended fixes. Our identification of missing patches, weak passwords, and insecure configuration settings is the main purpose for using this proactive approach.

A vulnerability scanner can assess a variety of vulnerabilities across information systems (including computers, network systems, operating systems, and software applications) that may have originated from a vendor, system administration activities, or general day-to-day user activities:

Architecture Description

It is a comprehensive vulnerability scanning methodology. It allows enterprises to assess two primary tiers through a single interface. They are: Operating System and Database. RPVS similarly, will detect new Oracle database instances, in the domain (range of IP addresses of an enterprise), seamlessly, quarantines it, and also scans for instance, user, data, schema, and OS vulnerabilities. Our Approach is based on the premise that your data base, may have very critical/confidential data like SSN, Credit Card info, etc., and so the schema/metadata have to be checked before allowing users access to it, to prevent malicious users accessing confidential data. The main areas in which the computing system's functions in order to secure the system are:

- Scanning of ports,
- Identification of vulnerabilities,
- Generation of reports and
- Validation of the state of security of the information technology infrastructure.

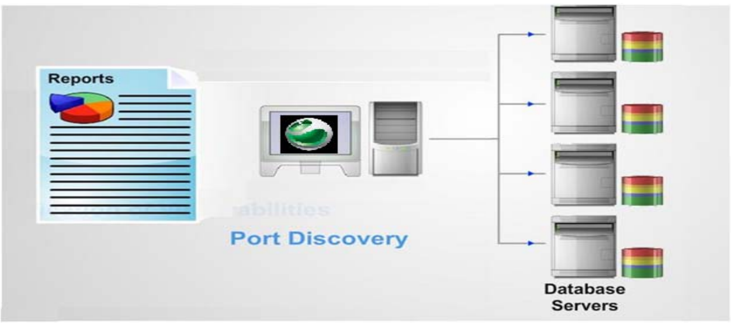


Fig 5: Proposed System

IV. DISCUSSION

This chapter begins with shedding some light on the security knowledge base which is a very significant part of the architecture as shown in Fig 6. RPVS is a comprehensive enterprise Vulnerability Scanner Tool. It functions to track risk assessment of Oracle databases. It performs port discovery of hosts and application, identification of your Oracle database vulnerabilities, generation of reports.

RPVS runs on any desktop machine, and collects data from ORACLE Database Server that may be installed in any operating systems (LINUX, WINDOWS, AIX, etc.). It serves as an agent-less tool. The security vulnerabilities are listed, and the data from the system for each of these vulnerabilities is taken, and risk evaluation is done. In general, a vulnerability scanner is made up of four main modules, namely, a Scan Engine, a Scan Database, a Report Module and a User Interface.

- Parallelized and concurrent operations to support fast vulnerability assessment in large enterprises.
- Agent-less installation and data transmission on target nodes.
- Encryption of reports for secure transmission.
- Database assessment can be carried out in any of the operating systems products.

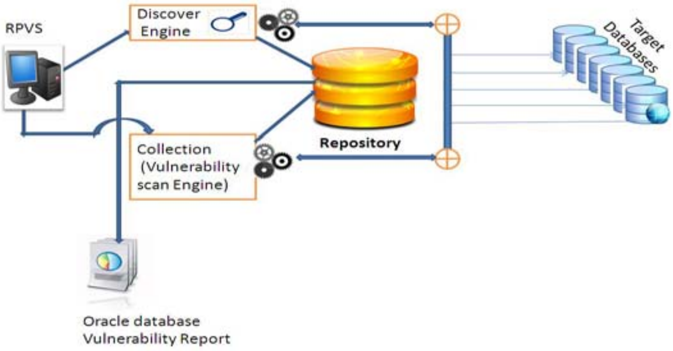

RPVS
Discover Engine
Collection (Vulnerability scan Engine)
Repository
Target Databases
Oracle database Vulnerability Report

Fig 6: RPVS System Modules

4.1 DISCOVERY

An essential part of any compliance and database vulnerability management program is a clear knowledge of the assets requiring protection. The RPVS Discovery and Assessment Server (DAS) offers automated network-based database discovery. The discovery results include detailed information about the specific platforms and RDBMS, which combined with data classification and vulnerability assessment and mitigation enabled risk management that maps sensitive data with vulnerability risks. Database discovery also helps with asset management and is an important first step for ensuring that rogue database servers do not exist on the network. Identification of IT assets, such as hosts and databases on your network by specifying IP Addresses and Ports is done by RPVS using the auto-scan feature that scans all the IP Addresses for servers in the enterprise up to n Oracle databases assets, even the host which does not have Oracle. OracleTNSCtrl is used to query the TNS listener for various informations, like the Oracle lsnrctl utility.

Discovers servers within your infrastructure

1. Detects unknown hosts and machines
2. Consolidates management of hosts and databases
3. Auto-scan all the IP Addresses for servers in the enterprise
4. It can scan all the Operating System and Database in each system
5. Scans even the host which does not have Oracle
6. Can scan the IP addresses for any oracle instances started

4.2 DATA COLLECTION

Automatically identifies new oracle instances, Scans the Oracle database instance for all vulnerabilities. The Scan Engine executes security checks according to its installed plug-ins, Identifying system information and vulnerabilities. It can scan more than one host at a time and compares the results against known vulnerabilities. The Scan Database stores vulnerability information, scan results, and other data used by scanner. The number of available plug-ins and the updating frequency of plug-ins will vary depending on the corresponding vendor.

Database Vulnerability Scanner is a part of database security assessment tool (RPVS) based on deep analysis of database typical security vulnerabilities and the popular attack techniques. DB Scan can scan potential vulnerabilities and discover Information like Oracle Authentication, Oracle Authorization, Oracle Network security and Oracle system integrity using Database server V$ views. It performs more than 100 security checks across databases including checks for SQL Injection and buffer overflow vulnerabilities, more than 200 database tables are checked for the presence of password information, deprecated functions, etc. The tool also detects weak, shared, and default passwords, changed database objects, altered data including modifications of privilege and user tables.

The User Interface allows the administrator to operate the scanner. By using Graphical User Interface (GUI). Most vulnerability scanners are characterized by their modular structure as explained above. However, there are also primitive scanners that are basically sets of scripts code exploits producing simple plain-text files as scanning results. Updates to these primitive scanners are infrequent and require manual intervention.

It has features designed to help you to secure your applications and the network,

1. Easy to use - Auto Scanning and Zero Configuration
2. Instant reporting of compliance to standards, with rating of risks, etc.,
3. Support Oracle Database Vulnerability Scanning
4. Secured Repository
5. In-depth agent-less Audit
6. Exact rating of the vulnerability

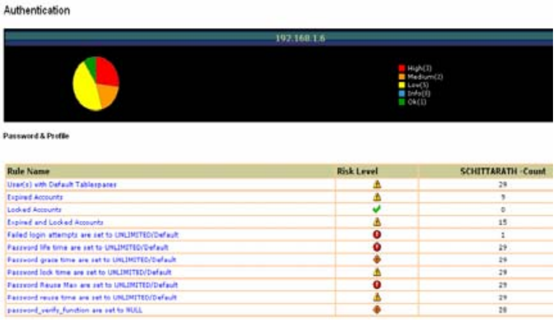
4.3 REPORT GENERATION

The Report Module provides different levels of reports on the scan results, such as detailed technical reports with suggested remedies for system administrators, summary reports for security managers, and high-level graph and trend reports for executives. This report gives graphical representations and the information about the vulnerabilities in database for two different configurations. Risk level identify is to monitor the database vulnerabilities. RPVS perfectly identifies and reports the software vulnerabilities, and configuration problems in the production databases. Most of the industry security regulations require periodic reports to be filed, online and in printed format. Reports can be generated in html.

- Oracle Authentication
- Oracle Authorization
- Oracle System Integrity
- Oracle Network Security

ORACLE AUTHENTICATION

Database authentication by the Oracle database requires use of a password. Oracle stores account passwords in encrypted format within the database. The table that stores the passwords is restricted from direct access by any database account. Fig 7 represents the check list of oracle authentication.



Authentication

192.168.1.6

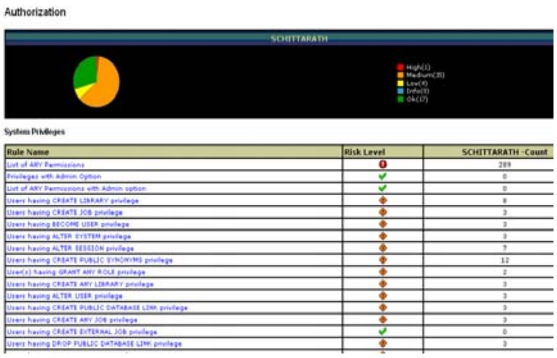
Password & Profile

Rule Name	Risk Level	SCHITTARATH -Count
User(s) with Default Tablespaces	⚠	29
Expired Accounts	⚠	9
Locked Accounts	✓	0
Expired and Locked Accounts	⚠	15
Failed login attempts are set to UNLIMITED/Default	●	1
Password life time are set to UNLIMITED/Default	●	29
Password grace time are set to UNLIMITED/Default	◆	29
Password lock time are set to UNLIMITED/Default	⚠	29
Password Reuse Max are set to UNLIMITED/Default	●	29
Password reuse time are set to UNLIMITED/Default	⚠	29
password_verify_function are set to NULL	◆	28

Fig 7: Oracle Authentication

ORACLE AUTHORIZATION

The access system enables you to protect your resources with policy domains and policies that specify who is authorized to use the resources and who is not allowed to use them, and under what conditions. Fig 8 represents the check list of oracle authorization.



Authorization

SCHITTARATH

🟥 High(1)
🟧 Medium(35)
🟨 Low(4)
🟦 Info(0)
🟩 Ok(17)

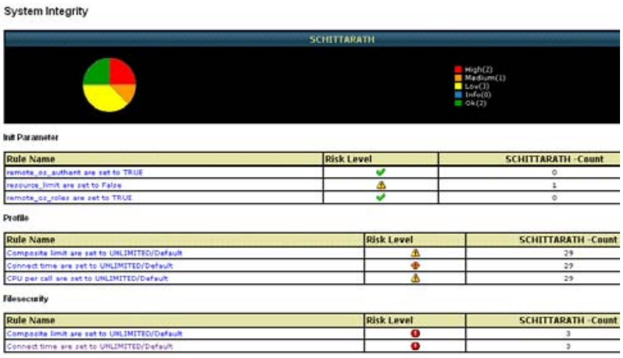
System Privileges

Rule Name	Risk Level	SCHITTARATH -Count
List of ANY Permissions	!	289
Privileges with Admin Option	✓	0
List of ANY Permissions with Admin option	✓	0
Users having CREATE LIBRARY privilege	◆	8
Users having CREATE JOB privilege	◆	3
Users having BECOME USER privilege	◆	3
Users having ALTER SYSTEM privilege	◆	3
Users having ALTER SESSION privilege	◆	7
Users having CREATE PUBLIC SYNONYMS privilege	◆	12
User(s) having GRANT ANY ROLE privilege	◆	2
Users having CREATE ANY LIBRARY privilege	◆	3
Users having ALTER USER privilege	◆	3
Users having CREATE PUBLIC DATABASE LINK privilege	◆	3
Users having CREATE ANY JOB privilege	◆	3
Users having CREATE EXTERNAL JOB privilege	✓	0
Users having DROP PUBLIC DATABASE LINK privilege	◆	3

Fig 8: Oracle Authorization

ORACLE SYSTEM INTEGRITY

Proper security and system management helps to protect system hardware, software, application and data from unauthorized access and improper modification and contributes to secure operation of database systems. Fig 9 represents the check list of Oracle System Integrity.



System Integrity

SCHITTARATH

🟥 High(2)
🟧 Medium(1)
🟨 Low(3)
🟦 Info(0)
🟩 Ok(2)

Init Parameter

Rule Name	Risk Level	SCHITTARATH -Count
remote_os_authent are set to TRUE	✓	0
resource_limit are set to False	⚠	1
remote_os_roles are set to TRUE	✓	0

Profile

Rule Name	Risk Level	SCHITTARATH -Count
Composite limit are set to UNLIMITED/Default	⚠	29
Connect time are set to UNLIMITED/Default	◆	29
CPU per call are set to UNLIMITED/Default	⚠	29

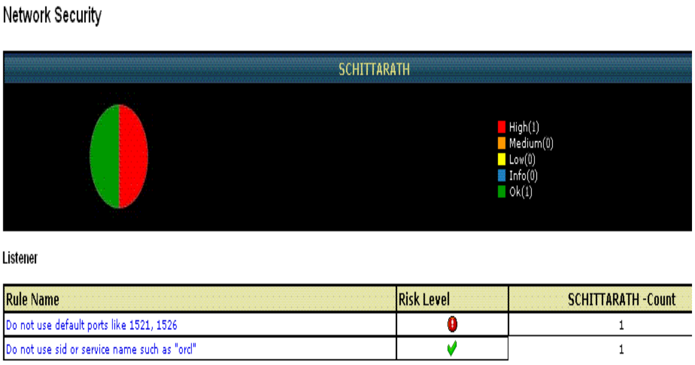
Filesecurity

Rule Name	Risk Level	SCHITTARATH -Count
Composite limit are set to UNLIMITED/Default	!	3
Connect time are set to UNLIMITED/Default	!	3

Fig 9: Oracle System Integrity

ORACLE NETWORK SECURITY

When a database connection is requested via the network to a database server [7], the client will provide an individual account name and authentication credentials to access the database. The database account name and any password transmission from a client to a database server over a network will be encrypted. Protecting the network and its traffic from inappropriate access or modification is the essence of network security. You should consider all paths the data travels, and assess the threats on each path and node. Then, take steps to lessen or eliminate those threats and the consequences of a security breach. In addition, monitor and audit to detect either increased threat levels or penetration attempts [6]. Fig 10 represents the check list of Oracle Network Security.



Network Security

SCHITTARATH

🟥 High(1)
🟧 Medium(0)
🟨 Low(0)
🟦 Info(0)
🟩 Ok(1)

Listener

Rule Name	Risk Level	SCHITTARATH -Count
Do not use default ports like 1521, 1526	!	1
Do not use sid or service name such as "orcl"	✓	1

Fig 10: Oracle Network Security

4.4 APPLICATIONS OF RPVS

As a vulnerability scanner tool provides you a secure system which is compatible with the security standards of the industry. RPVS is an easy to use, customizable, and lightweight tool which provides an overall view of the vulnerabilities in the database by automatically scanning them with minimum overhead. It is also compatible with the Security Compliances. It gives a detailed view of the risks and their corresponding ratings based on these priorities appropriating mitigation process can be implemented to ensure a secured system. This method protects enterprise data and users against unprotected enterprise data perform penetration testing and other atomic checks for much critical vulnerability.

V. CONCLUSIONS

In reality, there are often existing computer networks and external Internet connections. This situation introduces a significant number of known vulnerabilities. The tendency is to squander scarce resources on the most prominent vulnerabilities rather than investing the effort on the vulnerabilities that pose the greatest risk to the enterprise. The complexity of modern enterprises, their reliance on technology, and the heightened interconnectivity among organizations are rapidly evolving developments that create widespread opportunities for theft, fraud, and other forms of exploitation by offenders both outside and inside an organization. Internal and external perpetrators can exploit traditional vulnerabilities in seconds. As detailed in this paper, it is envisioned that using the vulnerability scanner aids on a regular basis, along with immediate response to problems identified will alleviate these risks. Routine vulnerability scanning, therefore, should be a standard element of every organization's security policy [10].

REFERENCES

[1] http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5374427.
[2] https://hercules.citadel.com/docs/301VulGuide.pdf,Pagevisited 051104.
[3] http://www.bitpipe.com/tlist/Vulnerability-Assessments.html
[4] http://documents.iss.net/whitepapers/nva.pdf.
[5] http://en.wikipedia.org/wiki/Zero-day_exploit, page visited 061203.
[6] www.databasesecurity.com/dbsec/database-stig-v7r1.pdf.
[7] www.integrigy.com/.../Integrigy_Oracle_Listener_TNS_Security.pdf.
[8] B.Marick, The craft of software testing, Prentice Hall.1995.
[9] I.V.Krsul, Software Vulnerability Analysis, PhD thesis, Purdue University,1998.
[10] www.symantec.com/connect/articles/vulnerability-assessment-survey. Search security,
[11] http://searchsecurity.techtarget.com/sDefinition/0, , sid14_gci1176511, 00.html
[12] R. Fussell, Vulnerability Assessment: Network based versus host based, Technical report, SANS Institute, 2002.