

Vulnerability Assessment & Penetration Test Audit



Experienced Consultants

Ready to Solve your
Business Challenges

 Skillmine Technology Consulting Pvt. Ltd.

VA & PT

EXECUTIVE SUMMARY

1. The requirement to secure today's network services is no longer focused on securing the perimeter alone. 'Defence in depth' is the challenge organizations are facing. Additionally, the frequency and level of sophistication of attacks has grown spectacularly over the last couple of years, whilst at the same time, the level of skills and knowledge required to carry out these attacks has decreased.

2. In order to keep up with the risk of attacks, organisations need to utilise professional expertise to secure their infrastructure and applications. Skillmine offers services that help mitigating the risk of security breaches:

Vulnerability assessment: Assessment of the risks posed by security vulnerabilities in your systems

Infrastructure penetration testing: Penetration testing to simulate a hacker attack on your critical network infrastructure

Configuration review: Review of your servers configuration to determine weaknesses

3. Skillmine's work plan is aligned to your needs and operates proactively to identify threats in all external or internal access points and suggest clear remediation options. Our approach can be summarised as follows:

We establish the scope, so that you can control the effects of any possible test in time and space. We also agree upfront on escalation and incident management procedures in case tests yield a noticeable operational effect.

We document the type of attacks, the applications, the data and the potential weaknesses you are most concerned about. Our experience has shown that every company has its unique risk profile that drives the type, scope and level of hostility of our tests.

We determine and scan for the systems, network components, and wireless connection points visible from the attack points. Our experience has shown that this type of discovery generally leads to surprises that confirm the need of attack and penetration testing.

We conduct a wide range of vulnerability scans and simulated attacks using various methodologies and tools. All tests are bound by the agreed time-table and scope and by the Skillmine policy and service agreement. This ensures that the tests don't miss anything and yet do not harm your normal operations.

A combination of Internet based and inside-the-DMZ tests ensure complete coverage and allows you to understand the vulnerability level in case of faulty configuration or maintenance later on.

VA & PT

OUR VALUE PROPOSITION

1. Our services go beyond technical vulnerability assessments. We translate technical issues into profound business risks if any.
2. Our ability to act as advisor and partner to help you resolve vulnerabilities in a vendor-agnostic (but knowledgeable) way.
3. We deliver reports that are to-the-point, that answer the 'so-what?' questions and provide clear guidance on how to solve the issues at hand.
4. All penetration tests are performed by Skillmine professionals to limit your exposure and disclosure.
5. Our professionals arrive at their conclusions by using the same tools and techniques as rogue hackers, and by following a pragmatic and project-oriented approach to ensure predictability and consistency.
6. Selected hosts or networks are targeted carefully, to protect the integrity of critical systems, data and applications and keep any side-effect on other hosts to an absolute minimum.

VA & PT

OUR APPROACH

1. Skillmine assesses the vulnerabilities and undertakes penetration testing for our clients as a holistic and complete project to ensure that the best possible security assessment is undertaken and the same is followed up suggesting possible solutions to mitigate the same. We would also be in a position to assist the client in implementing these solutions to ensure that the business derives the maximum benefit from its trusted information systems.

2. We shall undertake the VAPT as a professional and comprehensive solution and could include:

Assist the client to prepare for the VAPT

The development of VAPT plans

The conduct of the VAPT and the analysis, documentation, and reporting of the results

Post-assessment follow-on activities.



3. Conducting a VAPT in today's complex environment of sophisticated information technology infrastructures and high-visibility, mission-critical applications can be difficult, challenging, and resource-intensive. However, success requires the cooperation and collaboration among all parties having a vested interest in the organisation's information security or privacy posture, including information system owners, common control providers, authorizing officials, chief information officers, senior information security officers etc. Establishing an appropriate set of expectations before, during, and after an assessment is paramount to achieving an acceptable outcome—that is, producing information necessary to help the authorizing official make a credible, risk-based decision on whether to place the information system into operation or continue its operation.

VA & PT

4. Thorough preparation by the organization is an important aspect of conducting effective VAPT. Preparatory activities address a range of issues relating to the cost, schedule, and performance of the assessment. We shall assist the client to prepare for the VAPT by including the following key activities:

Ensuring that appropriate policies covering the information security VAPT are in place and understood by all affected organizational elements

Ensuring that all steps in the RMF (Risk Management Framework) prior to the security or privacy control assessment step, have been successfully completed and received appropriate management oversight

Establishing the objective and scope of assessments (i.e., the purpose of the assessments and what is being assessed)

Notifying key people and departments of impending assessments and allocating necessary resources to carry out the assessments;

Establishing appropriate communication channels among relevant people and departments having an interest or stake in the assessments

Establishing time frames for completing the assessments and key milestone decision points required by the organization to effectively manage the assessments

Preparing documents (e.g., policies, procedures, plans, specifications, designs, records, administrator/operator manuals, information system documentation, interconnection agreements, previous assessment results, legal requirements)

Establishing a mechanism between the client and the assessment team to minimise ambiguities or misunderstandings about the implementation of security controls and weaknesses/deficiencies identified during the assessments.

5. Depending upon the client's needs. Skillmine would undertake the following steps in developing plans to assess the vulnerabilities within the client's information systems or inherited by those systems:

Determine which systems are to be included in assessments based upon the purpose and scope of the assessment.

Select the appropriate assessment procedures to be used.

Tailor the selected assessment procedures (e.g., select appropriate assessment methods and objects, assign depth and coverage attribute values)

Optimize the assessment procedures to reduce duplication of effort (e.g., sequencing and consolidating assessment procedures) and provide cost-effective assessment solutions; and

Finalize assessment plans and obtain the necessary approvals to execute the plans.

VA & PT

6. Based upon the approved execution plan Skillmine shall undertake the assessment as per the agreed upon schedule. Skillmine's findings are unbiased, factual reporting of what was found. For each finding, Skillmine shall indicate which parts of the information system are affected and describe how the system differs from the planned or expected state. The potential for compromises to confidentiality, integrity, and availability due to the findings are also noted in the security assessment report. This would reflect the lack of a specified protection and the exploitation that could occur as a result (i.e., workstation, dataset, root level access).
7. During all phases of reporting and analysis we shall constantly consult the Common Vulnerability Scoring System (CVSS) and work with your team to commonly assign a risk rating based on business risk, and provide a clear standards based approach to risk analysis.
8. The results of the assessment ultimately influence control implementations, the content of security plans and privacy plans, and the respective plans of action and milestones. Accordingly, Skillmine shall assist the client to understand the assessment report and facilitate the updating of the risk assessment document and with the concurrence of the client's management, identify the appropriate steps required to respond to those weaknesses and deficiencies identified during the assessment.
9. Follow up assessment to ensure that the identified vulnerabilities have been mitigated could also be undertaken as can regular periodic assessments. This shall ensure that the information systems provide the best value for the client's business processes.

VA & PT

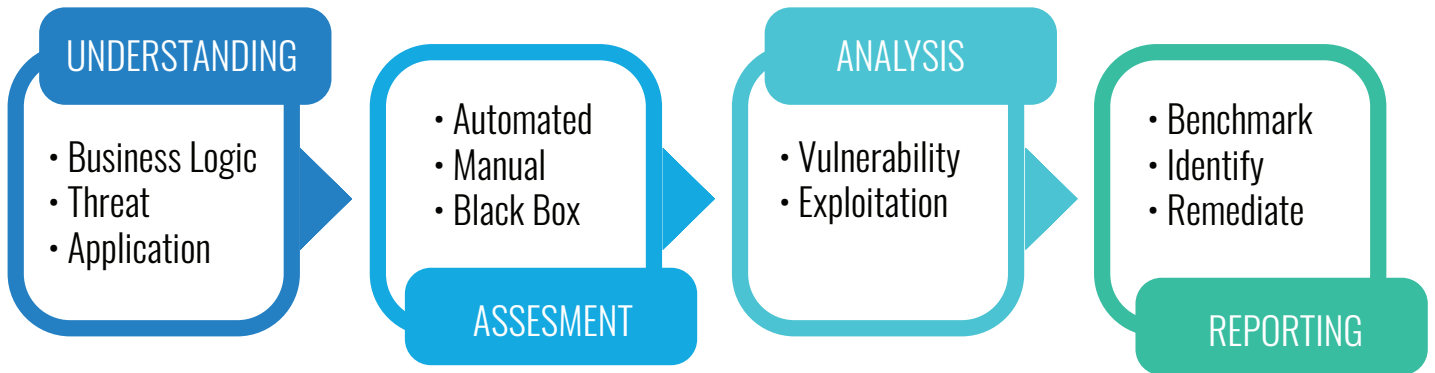
OUR METHODOLOGY

1. The Skillmine methodology for engagement is completely based upon the customer’s requirement and can be tailor-made to meet the client’s expectation. Prior to the beginning of the assessment, we will work with the client to develop a detailed and mutually agreeable assessment plan. The following methodology will be leveraged:

Application Penetration Testing (Black Box)

External Penetration Testing (Black Box)

2. Black Box Application Penetration testing:



We shall perform the vulnerability assessment and attempt exploitation of the client’s application in a controlled environment. We shall attempt to identify and exploit vulnerabilities present in the applications under scope as per the methodology brought out in the subsequent paragraphs.

Understanding: This includes gathering information associated with the application and the related infrastructure from different sources. We shall understand the following

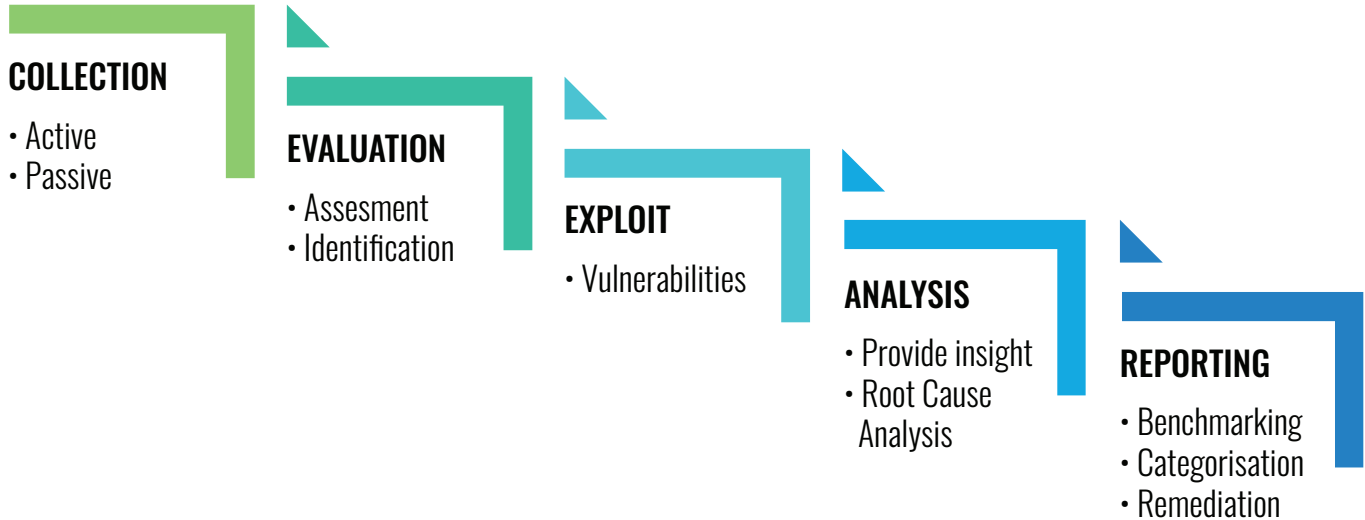
- Business Logic
- Application
- Associated Threats

Assessment: The application is assessed using automated tools and manual techniques in order to identify Vulnerabilities present. This assessment shall include automated and manual tools along with black box testing of the application.

Reporting: all discovered and exploited vulnerabilities would be aggregated in a technical report that thoroughly describes risk, root cause, description of vulnerability, remediation steps, and links to vendor information on the vulnerability. Furthermore, the vulnerabilities are assigned a root cause category and mapped against CVSS risk rankings and benchmarked across industries and our customer base. We shall also recommend specific remediation steps which shall be comprehensively communicated to our client.

VA & PT

3. Infrastructure Penetration testing.



We shall perform the vulnerability assessment and attempt exploitation of the client's IT infrastructure in a controlled environment. We shall attempt to identify and exploit vulnerabilities present in the infrastructure under scope as per the methodology brought out in the subsequent paragraphs.

Collection: We shall collect actively and/or passively the information regarding the client's infrastructure. This shall include public sources as well as through discussions with the client

Evaluation: The information collected would be assessed and vulnerabilities identified using commercially available tools.

Exploit: The identified vulnerabilities would be exploited. This stage requires active involvement of the client to allow / disallow the exploitation of the vulnerabilities. Care would be taken so as to ensure no disruption to the clients business.

Analysis: This involves bringing together the intellectual property of Skillmine Consultants experience, the commercial and non-commercial tool results, and the manual techniques. The discovered vulnerabilities are correlated so as to provide the client with a deep insight into the attack surface. Root cause analysis would also be undertaken to discover the reason for the existence of the vulnerability.

Reporting: All discovered vulnerabilities are reported in a comprehensive technical report. The report shall include a root cause categorisation and proposed remediation plans.

VA & PT

CUSTOMER ENGAGEMENT MANAGEMENT

Engagement management principles

Our project team will track and manage project timelines, milestones, deliverables, and budgets.

Project management will be essential to the ongoing success of the project, and our project team will rigorously track and manage the project timelines, milestones, deliverables, budgets, etc.

Quality Control

Quality control is integral to our project management methodology, and as such our activities and deliverables will be closely followed and reviewed to confirm that they comply with our professional delivery standards

Issue management

Skillmine has a process in place to identify issues and resolve them before they hurt the project. Our approach to issue management includes processes that will be used to identify, control, and resolve issues throughout the engagement.

Stakeholder communications

Our clients will have constant access to our management in order to be able to escalate any issues.

VA & PT

PROPOSED TEAM STRUCTURE

Roles and responsibilities

The table below provides a high-level summary of the roles and responsibilities for our team as well as our client’s roles and responsibilities.

Proposed Team Role	Key Responsibilities
Client Stake Holder	Serves as the project sponsor and highest point of escalation for strategic and tactical direction of the project
Skillmine Advisor	Provides quality assurance oversight and risk management. Acts as a conduit to Skillmine leadership as necessary
Skillmine Project Manager	<p>Monitors and provides feedback regarding project direction, project management effectiveness and project status.</p> <p>Makes strategic-level decisions and resolves issues in a timely manner.</p> <p>Provides quality assurance oversight and assists in risk management.</p> <p>Manages Technical resources and provides local on-site testing.</p>
Client Project Manager	<p>Responsible for working with the Skillmine Project Manager to confirm that people and resources are available for the project team to conduct the work</p> <p>Attends all status meetings and help in issue resolution</p>
Skillmine Remote Consultants	<p>Responsible for working with the Skillmine Project Manager to confirm that people and resources are available for the project team to conduct the work</p> <p>Provides advanced technical testing capability for all security assessments</p>

VA & PT

PROPOSED DELIVERABLES

We appreciate the importance of providing our clients with a comprehensive and inclusive report as part of a successful engagement. The link between the IT risks and the associated business risk would be clearly articulated in our reports. We have in depth capabilities to provide our clients with tailor made reports as per the client requirement. All our reports shall consist of the following:

Overall risk classification. Each vulnerability or risk identified would be labelled as a finding and categorised as a **High-Risk, Medium-Risk, or Low-Risk**. In addition, each supplemental testing note is labelled as an Issue. These terms are defined below:

High Risk:

These findings identify conditions that could directly result in the compromise or unauthorized access of a network, system, application or information.

Medium Risk:

These findings identify conditions that do not immediately or directly result in the compromise or unauthorized access of a network, system, application or information, but do provide a capability or information that could, in combination with other capabilities or information, result in the compromise or unauthorized access of a network, system, application or information.

Low Risk:

These findings identify conditions that do not immediately or directly result in the compromise of a network, system, application, or information, but do provide information that could be used in combination with other information to gain insight into how to compromise or gain unauthorized access to a network, system, application or information. Low risk findings may also demonstrate an incomplete approach to or application of security measures within the environment

In addition each issue identified is described with the finding, the impact of the issue, how easy it would be for an attacker to exploit the issue and a recommendation. Each security issue is rated based on a number of factors, each of these are described in the following sections.

Issue Finding. The issue finding describes what configuration setting we identified that potentially poses a security threat. In addition to the finding details, any relevant background information is also described.

Issue Impact. The impact section describes what an attacker could gain from exploiting the security issue. The impact of an issue is often defined by other configuration settings that could heighten the issue or partially mitigate it. The impact is rated depending on the significance of the security threat.

VA & PT

IMPACT

Critical

These issues can pose a very significant security threat. The issues that have a critical impact are typically those that would allow an attacker to gain full administrative access to the device.

High

These issues pose a significant threat to security, but have some limitations on the extent to which they can be abused.

Medium

These issues have significant limitations on the direct impact they can cause.

Low

These issues represent a low level security threat.

Issue ease. Each identified issue shall be correlated to the knowledge, skill and physical access that would be required of an attacker in order to exploit it. The ease will describe if open source or commercially available tools are required for an attacker to exploit an issue. Additionally, the ease will note where an extended period of time is required to exploit the issue, such as cracking weak encryption ciphers.


Trivial	The issue requires little-to-no knowledge on behalf of an attacker and can be exploited using standard operating system tools.
Easy	The issue requires some knowledge for an attacker to exploit, which could be performed using standard operating system tools or tools downloaded from the Internet.
Moderate	The issue requires specific knowledge on behalf of an attacker and could be exploited using a combination of operating system tools or publicly available tools downloaded from the Internet.
Challenge	A security issue that falls into this category would require significant effort and knowledge on behalf of the attacker. The attacker may require specific physical access to resources or to the network infrastructure in order to successfully exploit it. Furthermore, a combination of attacks may be required.
N/A	The issue is not directly exploitable.

Thank you

Our Values

- Think & Care about Customer's Investment
- Predictable Delivery Every Time since First Time
- Passionate about Desired Outcome

info@skill-mine.com
orders@skill-mine.com



Private and Confidential - If you are not an intended recipient of this document. Please immediately delete this document from your computer or any other electronic device if you are using an electronic copy and/or please immediately trash this document if you are using a printed copy. © Skillmine Technology Consulting Pty Ltd