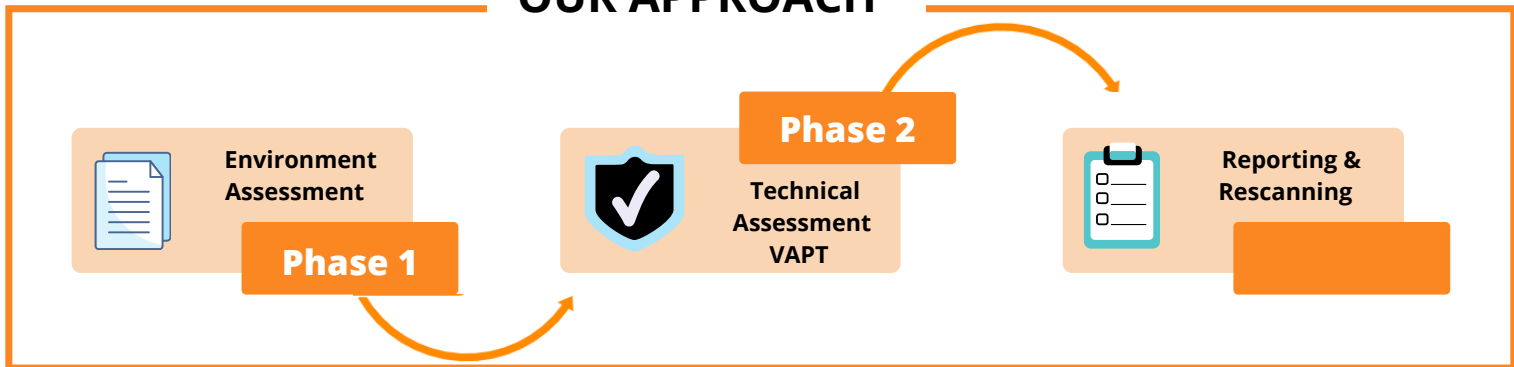


# Technical Security Risk Assessment (VAPT)

## About Us

CyberSRC® Consultancy LLP is a globally recognized award-winning and ISO 27001 certified organization. Established in January 2018, CyberSRC Consultancy offers the full gambit of cybersecurity services Data Governance & Protection, IT Audit & Assurance, Compliance Management, Vulnerability Management, January 2018, since then having traction with industry leaders and helping resolve complex problems in domains of Cyber Security, Data Governance & Protection, IT Audit & Assurance, and Compliance Management. We have challenged the bygone technological and business outlook toward security domains. Our society is more technologically reliant than ever before and there is no sign that this trend will slow down. With the ever-changing and dynamic cyberspace, our goal is to assist organizations globally- MSMEs, SMEs, Enterprises enhance their capabilities & effectiveness in Cyber Security, Minimize enterprise & IT Risks, Manage Security Operations &, to achieve Regulatory Compliances.

## OUR APPROACH



### Phase 1 Environment Assessment

In this phase our Cyber Security experts understand the IT landscape and scope of work in an organization. We do environment assessment and collate the information such as Network Architecture, Application Architecture, and other IT infrastructure related information. We provide project plan with time and effort estimate for end to end testing and remediation of the projects. Post approval & authorization from management we move to next phase.

### Phase 2 Technical Assessment- VAPT

This phase includes through testing of the in-scope IT landscape, this is done in many ways like manual testing, automated testing or simulating red team exercises.

## **Automated Methods:**

We use commercial and open source tools to evaluate vulnerabilities in systems, and evaluate the vulnerabilities in the system for false positive or false negative based on our knowledge and understanding of known vulnerabilities. We provide risk ratings based on severity and ease of exploitation of the vulnerabilities.

## **Manual Method:**

We use manual techniques to enumerate the systems, networks, and applications. By checking the application or system functionality and behavior closely when given different inputs or malformed requests and closely monitor the effect on the applications.

## **Red Team Exercises:**

Here we will execute our red team attacks on the organization to expose the company's sensitive information for preventing any breach in the organization.

## **Threat Modelling:**

Our goal here will be to analyze the product and create a threat model of the product for mitigating any security threat in the pre-production phase. We also test for post-exploitation if required so as to know how much loss a malicious attacker can cause. Based on these observations we provide comprehensive reports based on scenarios in which the system is vulnerable to hackers.

## **Mobile Pen-testing:**

Our goal here is to analyze all aspects of the mobile application and initiate attacks against those features to check whether it will cause any security failure or not by performing static and dynamic testing on these applications.

## **Web Pen-testing:**

Our goal here is to analyze and attack all the functions of the websites to give an accurate security image of the websites where it will show which functions, webpages, or technology used is vulnerable in nature.

## **Infrastructure Pen-testing:**

We conduct assessments of infrastructure for every possible flaw that could impact the security of the IT infrastructure. We assess IT infrastructures such as Servers (Windows, LINUX/ UNIX), Laptops/Desktops, Operating systems, Databases, and another infrastructure components.

## **Phase 3**

## **Reporting & Rescanning**

This phase we evaluate all the findings on basis of severity, impact, ease of exploitation and categorize the findings or vulnerabilities into Risk ratings of High, Medium, Low with explanations, proof of concepts, and remediation recommendations. Post fixes from the organization we conduct a revalidation test for findings /issues.

# NETWORK SECURITY



## Common vulnerabilities found in testing

- Malwares
- Misconfigurations
- Unpatched software

## OUR APPROACH

There are a variety of methodologies used when it comes to effective penetration testing. Some or all of these methodologies may be used depending upon the network system type.



### BLACK BOX

A penetration test that is black box is conducted without the knowledge of any information related to the technical aspects of a network. This type of test requires penetration testers to conduct comprehensive network exploration in an effort to determine the best way to organize a simulated attack. It is a simulation of a more realistic exploit on a network. This method is used by businesses that want to stay on top of what hackers are capable of doing within a very short period of time.



### WHITE BOX

A White Box penetration testing occurs when network professionals have gathered all data and information associated with a network and its architecture. This type of pen test is more like an audit and provides a comprehensive approach to security testing. This form of pen testing is used by businesses that want to ensure every single aspect of their network is as secure as possible.



### GREY BOX

This approach to penetration testing is performed according to internal information for a network including technical documents, user privilege credentials, and more. Based on the internal information collected, a highly sophisticated network attack can be launched to determine what can happen when hackers gain access to sensitive information. Grey Box pen tests are a common approach that provides detailed security testing that takes place over a shorter period of time than the more involved process of White Box pen tests. These are the main methodologies used in penetration testing. Other network monitoring tests such as intrusion detection, packet sniffing, and other methods are also often deployed to determine the status of network security.



# WEB APPLICATION SECURITY

## Common vulnerabilities found in Web Applications

- SQL Injections
- Cross Site Scripting Attacks
- Misconfigurations
- File inclusions
- File Upload

## OUR APPROACH

### VULNERABILITY SCANNING

Powered by both automation and manual testing, vulnerability scanning is used to identify the loopholes and vulnerability signatures present in the application. It is used to gain an understanding of the baseline of security risks.

### GRAY BOX ASSESSMENT


The final category of testing is called white-box testing, which allows the security consultant to have completely open access to applications and systems. This allows consultants to view source code and be granted high-level privilege accounts to the network. The purpose of white-box testing is to identify potential weaknesses in various areas such as logical vulnerabilities, potential security exposures, security misconfigurations, poorly written development code, and lack-of-defensive measures.

### WHITE BOX ASSESSMENT

Comparatively, a black-box tester begins the engagement from a strict external viewpoint attempting to get in, while the grey-box tester has already been granted some internal access and knowledge that may come in the form of lower-level credentials, application logic flow charts, or network infrastructure maps.

### BLACK BOX ASSESSMENT

In a black-box engagement, the consultant does not have access to any internal information and is not granted internal access to the client's applications or network. This type of testing is the most realistic, but also requires a great deal of time and has the greatest potential to overlook a vulnerability that exists within the internal part of the network or application.



# CLOUD APPLICATION SECURITY

## Our Approach

### Cloud Instance Hardening

This adds an extra layer of security to your instance/ server and protects it from outside attacks. It checks the policies used, configurations of the instance.

### Testing Applications Hosted on Cloud

Testing the cloud infrastructure for any unused open ports, vulnerable services running and unpatched software.

### Configuration Review of Cloud Console

Testing the cloud console for any misconfigurations such as the created user accounts and their permissions, implemented ACL, etc. This is more of a configuration review verifying standards policies have been implemented while creating accounts. We can identify different techniques to perform privilege escalation.

### Testing Applications Hosted on Cloud

Consider your web application hosted on a VPS or dedicated server and later moved to the cloud platform in which only your developed web application is considered in the scope.

### Testing Internal Applications Hosted on Cloud

This type of cloud assessment is performed where in the cloud system cannot be accessed externally and is private which has firewall to prevent direct access and can only be accessed by a bastion host.

## Common vulnerabilities found in Cloud Applications

- Multi Tenancy Attacks
- Privilege Escalation
- SQL injection
- Request Forgery



# MOBILE APPLICATION SECURITY

## Common vulnerabilities found in Mobile Applications

- Storing sensitive data in an insecure way
- Implementing poor authentication and authorization checks
- Using weak encryption and encoding methods
- Transmitting sensitive data over the internet without HTTPS

## Our Approach



### GREY-BOX TESTING

This one is the most common approach in security testing. With it, some information (like the credentials) is provided, but the rest is to be discovered by the tester.



### BLACK-BOX TESTING

With this approach, the tester has no prior knowledge of the app, which allows them to behave like user (or hacker) and exploit the publicly available info.



### WHITE-BOX TESTING

This method implies that the tester knows the app's ins and outs and has access to the source code and various documentation. White-box testing allows for faster testing and more sophisticated test cases.



## DYNAMIC ANALYSIS

It is the process of analyzing an application while executing the app in a controlled environment. The dynamic analysis will monitor network traffic and other communications to catch malicious activity. With a powerful dynamic analyzer, applications that attempt to connect out to unknown or malicious sites, or send SMS messages without authorization will be flagged as malicious and consequently be reported as threats.



## STATIC ANALYSIS

Static analysis is the process of analyzing an application without actually executing the application. Static analysis will review the code of an application to find known or suspicious function calls or permissions that deem malicious.

# RED TEAM EXERCISES

Red team assessments are similar to penetration tests but take the approach of “by any means necessary” to gain access to an organization’s private networks or sensitive data. Red team exercises are done to simulate a realistic cyber-attack by using the methods and techniques that have been recently used in real-world attacks against businesses. These attacks do not aim to take down the target systems but to compromise the gaps between good design, intentions, implementation, and maintenance of target systems in a manner that allows the attacker to circumvent security protocols to achieve the malicious objective, leading to the compromise of the network, and stealing sensitive data. In a real-world incident scenario, this would include business disruption and financial losses.

## Our Approach

The first objective of a red team exercise is to identify any physical, hardware, software, and human vulnerabilities that affect the security of your business. Compared to vulnerability assessments and penetration tests, where the goal is to identify vulnerabilities within a given environment, red team exercises are focused on identifying and exploiting multiple vulnerabilities across multiple environments, including trying to gain physical access to specific locations owned by the business.

The second objective of a red team exercise is to obtain a realistic understanding of the risks that your business can face. As the scope of what can be tested is increased, more vulnerabilities and risks will be revealed. Red team exercises focus on multiple security aspects that can affect a business, including procedures for guiding visitors around a facility, training used to prepare employees for cyber incidents, and the equipment and their setup used for physically securing a facility.

The final objective of a red team exercise is to help address and fix all identified security weaknesses. Once the risks that affect a manufacturer or business have been identified, a report from the red team will include how the vulnerability was exploited and what changes should be made to prevent the vulnerability from being exploited again.



# THREAT MODELLING



Threat modeling is a method of optimizing network security by locating vulnerabilities, identifying objectives, and developing countermeasures to either prevent or mitigate the effects of cyber-attacks against the system.

## Our Approach

Threat modeling consists of defining an enterprise's assets, identifying what function each application serves in the grand scheme, and assembling a security profile for each application. The process continues with identifying and prioritizing potential threats, then documenting both the harmful events and what actions to take to resolve them.

## DIGITAL INFRASTRUCTURE (AI, IOT, ML, BLOCKCHAIN)

We assess your digital environment for security risk such as IoT implementation (Firmware and application), AI/ML-based applications, Blockchain-based applications and review the security parameters and functionality that can impact the security posture of applications/infrastructure.

We conduct code review, manual penetration testing, automate testing (tool based).







Simplifying Cyber Risk Management..



+91 8800377255, 0120-4160448



[info@cybersrcc.com](mailto:info@cybersrcc.com)



[www.cybersrcc.com](http://www.cybersrcc.com)



**Head Office:** Unit 605, 6th Floor, World Trade Tower, Sector 16, Noida (UP)- 201301

**Other Office:**

**London (UK):** Kemp House 152-160 City Road, London, UK (EC1V 2NX)

