avancer®
Simplified **IT** Security

WHY CONDUCT PENETRATION TESTING FOR ENSURING CYBERSECURITY?

Regular penetration testing is must for ensuring robust IT security and adhering to compliance.

Undertaking cyber security assessment is imperative for enterprises to implement pro-active strategies for identifying and addressing vulnerabilities in its IT ecosystem. Failure to safeguard data or prevent breaches may significantly damage the reputation of the company, along with causing financial loss and compliance issues
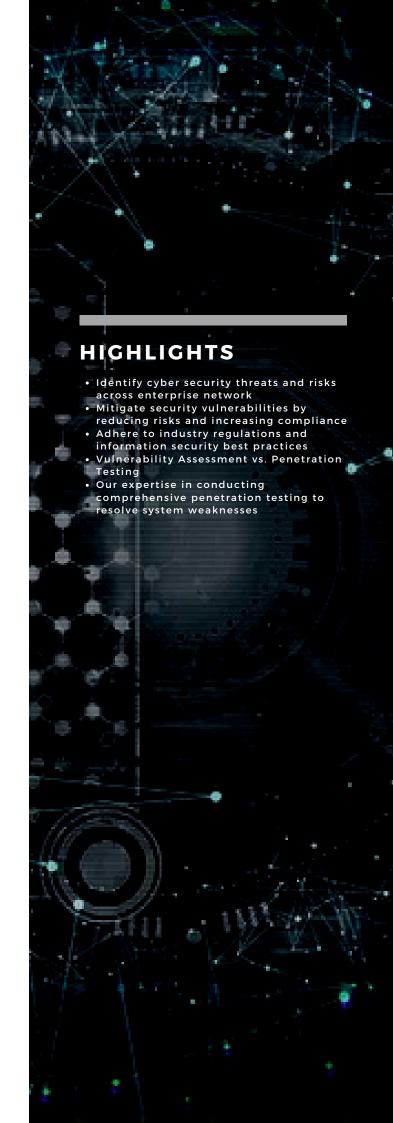
METHODS OF CYBER SECURITY ASSESSMENT

Prominently, vulnerability assessment and penetration testing are the two techniques used to find security weaknesses. While vulnerability assessment focuses on detecting any system shortcomings that might be susceptible to previously discovered viruses or malicious cyberattacks, penetration testing determines whether the security controls of an enterprise is robust enough to safeguard it from possible attacks.

Thus, penetration testing becomes a natural extension to vulnerability assessment for any organization planning to conduct cyber security assessment. Here's why?

LIMITED EFFICACY OF VULNERABILITY ASSESSMENT

In vulnerability assessment, past known IT security issues are documented, and the data from the system are compared with these issues to understand if the system is vulnerable to these known problems. Thereafter, remedial measures for the identified vulnerabilities are implemented. Such a type of assessment usually estimates the susceptibility of the system to identified vulnerabilities such as a known virus or Trojan attack, which could be restrictive in nature as it does not account for any future unknown weakness.

HIGHLIGHTS

- Identify cyber security threats and risks across enterprise network
- Mitigate security vulnerabilities by reducing risks and increasing compliance
- Adhere to industry regulations and information security best practices
- Vulnerability Assessment vs. Penetration Testing
- Our expertise in conducting comprehensive penetration testing to resolve system weaknesses

SOME OF THE LIMITATIONS OF VULNERABILITY ASSESSMENT ARE:

- Absence of tests for identifying social engineering attacks such as phishing, vishing, malware etc.
- Absence of live web application testing to detect errors or unexpected results from the app
- Absence of ability to implement pivoting technique for exploiting vulnerabilities to prevent future attacks

COMPREHENSIVE ASSESSMENT WITH PENETRATION TESTING

Designed to test a system, application, or network, penetration testing enables enterprises to identify vulnerabilities that could be potentially exploited by hackers or people with malicious intent. In this type of testing, experts gain access to an enterprise network and data in a similar manner as a hacker would.

Such a test is beneficial as it allows organizations to identify unknown network susceptibilities, and provide an opportunity to implement robust solutions for not only preventing future attacks, but also safeguarding critical information and managing regulatory compliance proactively.

SOME OF THE KEY BENEFITS OF PENETRATION TESTING ARE:

- Ability to identify critical IT infrastructure and assets at risk
- Mitigate or minimize security vulnerabilities proactively
- Schedule tests, manage assessments and business requirements as per threat environment
- Develop and implement highly customized remediation plan
- Monitor analysis of results and get detailed reports

Our Verdict: Although vulnerability assessments are comparatively less costly and quicker than penetration testing, it is only ideal for conducting source code reviews, configuration reviews and regular system checks, and might not be an optimal choice for maintaining a robust security protocol for unforeseen cyberattacks.

AVANCER'S PENETRATION TESTING SOLUTION

Our penetration testing solution is custom-made as per an enterprise's requirements, security protocols, critical networks, systems and applications. Our specialists go beyond customary automated vulnerability scans and focus on undertaking advanced manual tests as well to ensure the elimination of any vulnerability or weakness in the security ecosystem. Furthermore, our experts provide detailed remediation steps to help secure these vulnerabilities in the systems and infrastructure, along with strengthening the security platforms for any possible future attacks.

Some of our customized penetration testing solutions include:

Penetration Test	Purpose	Benefit
Application testing	To test and prioritize critical and risk-based web or mobile applications for vulnerabilities and secure them with immediate effect	Access security vulnerabilities of applications that may lead to data breaches
Network testing	To identify network vulnerabilities such as unknown back doors, configuration errors or flaws in the system	Secure network and devices to prevent unauthorized access that may lead to financial losses or regulatory issues
Cloud testing	To mitigate security risks such as human error or system misconfiguration on cloud environment	Ensure seamless cloud migrations and secure data on cloud
Social engineering	To identify vulnerable devices or insecure endpoints, which are being targeted by cybercriminals through creative social engineering methods	Enable the system to identify threats such as malware and phishing attacks on real-time basis

OUR THREE-PRONGED STRATEGY

At Avancer, we follow three-pronged strategy to secure enterprises from potential threats.

Conducting penetration testing:

Advisors at Avancer implement strategic approach to conduct penetration testing and identify underlying vulnerabilities in the system, APIs, firmware, applications or through social engineering methods that could be potentially exploited by cybercriminals. Our service also includes assessing the system for compliance-related mapping.

Our experts undertake a systematic process:

- Undertake reconnaissance of the network, system or application that is being assessed
- Enumerate the vulnerabilities found in the IT ecosystem
- Exploit vulnerabilities in a controlled environment through penetration testing tools and other methods
- Gain access to data and other critical information through gap in security platform

Fixing system vulnerabilities:

Our experts help in fixing identified vulnerabilities and safeguard the data and system from being compromised by people with malicious intent.

Our experts implement detailed remediation solutions:

- Safeguard vulnerable system through robust identity and cybersecurity solutions
- Revoke privileges of compromised users to access sensitive information
- Prevent malicious insider from infiltrating the network

Providing proactive strategies:

We generate a comprehensive insights report, identifying potential future risks and its impact on the business, thereby, helping enterprises prioritize their future security investments.

Our experts provide result-based solutions:

- Comprehensive report on system vulnerabilities and other threat elements for immediate action
- Risk-based analysis of the target environment for possible future attacks
- Strategic long-term recommendations and solutions for robust IT infrastructure

WITH THE THREAT ENVIRONMENT EVOLVING CONSTANTLY, IT IS IMPERATIVE FOR ORGANIZATIONS TO CONDUCT PENETRATION TESTING AT LEAST ANNUALLY TO CREATE AN INCLUSIVE IT SECURITY FRAMEWORK.

WHY AVANCER?

We have more than a decade's experience in identity and cybersecurity and managing threat landscape. Our experts are at the forefront in identifying and addressing vulnerabilities in enterprise systems, networks and applications through our robust penetration testing service. Through our unparalleled expertise in understanding current and future threats, along with investigative techniques such as hacker behavior and advanced persistent threats (APTs), and proprietary assessment tools, we implement comprehensive incident response strategies.

We focus on helping enterprises undertake digital transformation seamlessly by creating effective security protocols in sync with the business goals of the enterprise.

WE CONDUCT ASSESSMENTS TO EXPOSE WEAKNESSES IN ENTERPRISE NETWORKS, APPLICATIONS AND RESOURCES, AND ALONG WITH PROVIDING ADVISORY AND RECOMMENDATIONS TO MINIMIZE RISKS, OUR EXPERTS ALSO HELP TO ADDRESS VULNERABILITIES BY IMPLEMENTING ROBUST IDENTITY AND CYBERSECURITY SOLUTIONS.

AVANCER'S EXPERTISE IN IAM

At Avancer, we understand that one of the compelling factors for organizations to bring in technical solutions is to adhere by existing compliances. However, there is so much more to technical solutions, and these add on benefits help in bringing efficiency, security and operational automation. We add an edge to solutions in Identity and Access Governance, IT Security and Big Data by closing any loopholes, and tailoring the solutions as per the needs of the business, industrial standards and regulatory considerations.

For more information on how we can make a difference in your organization, drop us a request here or directly contact our IT Security Leaders

RAJESH MITTAL, CTO| ARUN MEHTA, CEO | ABHA SHARMA, IT SECURITY EXPERT

Contact Us

Avancer Corporation

101 Interchange Plaza

Suite 201 Cranbury

NJ 08512, USA

Tel: +1 (609) 632-1285

Fax: +1 (877) 843-8594

Email: info@goavancer.com

Website: http://www.avancercorp.com/

To consult IAM Experts, click here.