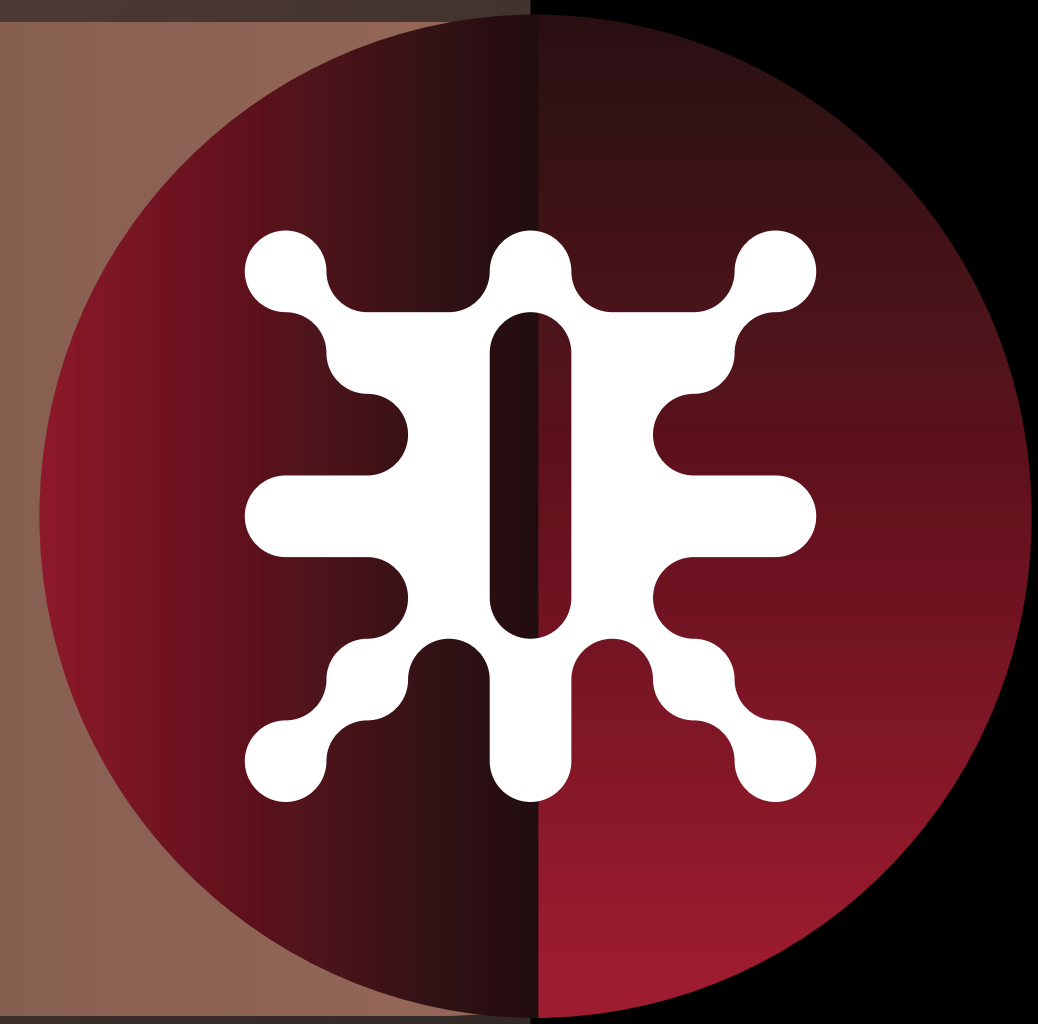


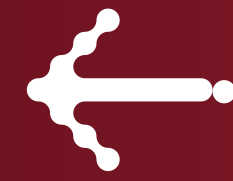
P E N E T R A T I O N T E S T

P E N T E S T



Penetration Test

service, abbreviated as pentest, is a method to measure the security level of a system or infrastructure that, as an attacker, examines the entire network and system to identify security gaps.



In recent years, many companies have added some features to existing applications or implemented new applications for the convenience of their customers and employees. For example, we can mention online access to banking services and the development of electronic communication methods for employees. On the other hand, many companies have realized the necessity of being on the Internet to attract potential customers and retain current customers.

When we talk about being on the Internet, the element of security becomes essential, especially security in the aspect of confidentiality and authenticity. Web servers, along with their helpful services, have also created a new set of vulnerabilities that should be taken seriously by computer system operators, especially web-based systems. Vulnerabilities are not limited to servers and may also exist in the design and implementation of applications.

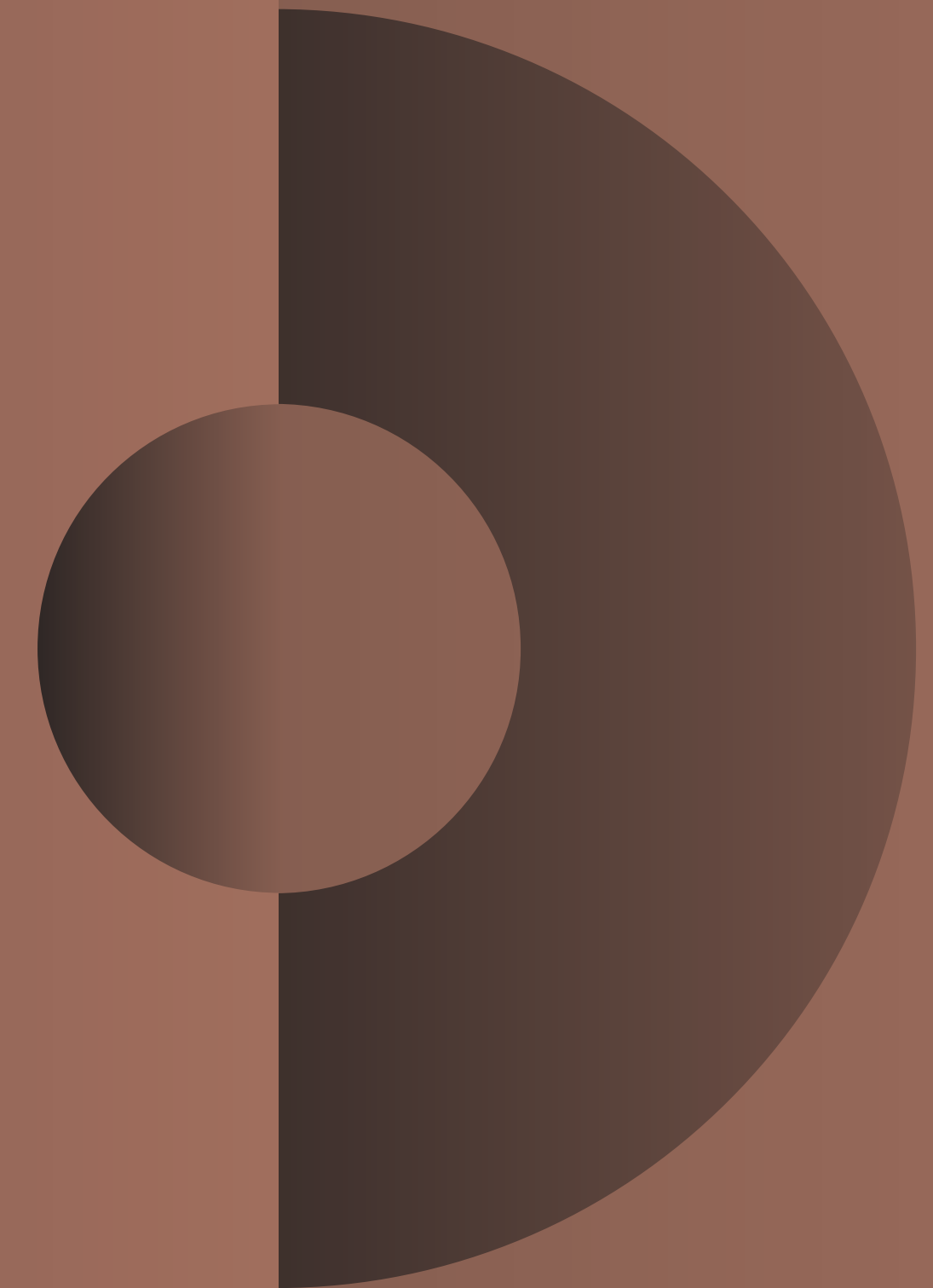
Many organizations use standard system development cycles and pay enough attention to the evaluation of the quality and security status of their system. On the one hand, some considerations from the developer's point of view may be repetitive work and be missed. On the other hand, since most of the organizations' focus has been on providing services as quickly as possible in the form of internet systems and correcting and improving the problems related to them, the necessary and sufficient focus to provide the security requirements of these systems has not been done.

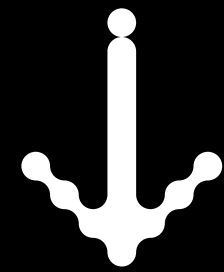


Security assessment and penetration testing are done in the organization for the following reasons:

- Finding security holes in the systems before others find them
- Hackers use any security hole and situation to penetrate. This test examines the security from the hacker's point of view, then according to the results, identifies the security weaknesses and fixes them to prevent attacks
- Providing reports of security problems and vulnerabilities to the organization manager
- Checking of security settings
- Training the network and security experts of the organization to provide the ability to respond to attacks

Today, it is more important to conduct a security assessment of the network, services, and products that are supposed to be provided in public spaces such as the Internet. Lack of attention to adequate and accurate assessment causes widespread financial and informational abuses by profit-seeking people and hackers from the weak points of electronic services.





Introducing Spara's penetration test service

Spara has created a comprehensive, efficient, and agile framework for assessing and testing network penetration and applications by using the advantages of standards in network security, software, and penetration testing. This team carefully assesses the security and identifies the vulnerabilities of the network and application and uses the obtained information to perform the penetration test and achieve the desired goals. This procedure, along with the use of the specialized knowledge of the expert of the security assessment and Penetration Test team, as well as the extensive cost of developing specific tools in this field, leads to the maximum identification of security vulnerabilities.

Differences between Penetration Test and Red Team service

During the implementation of the security assessment and penetration test on the systems/networks of an organization, with a comprehensive analysis, the maximum possible vulnerabilities in an organization's information technology system/infrastructure are identified and the solution to solve each of them is introduced separately. On the other hand, by simulating a variety of attack scenarios, the Red Team will check the quality and effectiveness of the security measures implemented and the organization's defense strategies, and the implementation of security assessment and the penetration test is one of the most important measures.

In this regard, due to the broad scope of the implementation of the Red Team, it was not possible to identify all the vulnerabilities of the systems, and mainly some of the macro examples of vulnerabilities and weaknesses of the organization's defense solutions of the organization's systems/information technology infrastructure are identified and mentioned. In other words, the scope of focus during security assessment and penetration test will include comprehensive assessment and identification of all system vulnerabilities one by one, and based on the type of access created and the agreement made, it can apply at all access levels from the black box to the white box and even source code analysis. The result of the security assessment and penetration test will significantly increase the resilience level of the system/network against cyberattacks. Ultimately, the Red team and Penetration Test are both complementary and play a vital role in keeping an organization secure against complex cyber threats.



Services provided by Spara Penetration Test team



Security assessment and penetration test of web systems

Today, with the expansion of Internet access, the use of remote services to facilitate and expedite service processes has increased. These are usually done in the form of web-based systems. Whereas these systems receive information from users to provide services, and given that these systems are often available to all; therefore they can potentially be considered a source of threats such as disclosure and misuse of information.

By adopting the OWASP standard methods in the security assessment and penetration test of applications, as well as its many years of experience in this field, Spara has collected test cases. The exact implementation of these cases, along with the use of the special tools of the penetration test team of Spara, will accurately evaluate the state of the application in terms of security.

Security assessment and web penetration test

With the expansion of web-based systems, integrating these systems to reduce the costs of development, setup, and deployment led to the development and formation of web services technology. Considering the provision of various services by web services and their interaction with databases, they can potentially be considered as a source of threats such as disclosure and misuse of information.

Based on OWASP standard methods and relying on exploit writing knowledge, the ability to identify zero-day bugs, the experience of experts, and using licensed specialized tools, Spara company can evaluate web services based on SOAP, RESTful, etc. technologies.

Security assessment and penetration test of mobile applications

Due to the widespread use of mobile phones, tablets, etc., which can run mobile applications, the security of mobile applications should be given more attention. The architecture of most mobile applications consists of a client and a server. In addition to the vulnerabilities that threaten web-based applications, mobile clients are also vulnerable to being lost or stolen and secondary malware on the device. Therefore, the security of the client installed on the user's device has become very important. The security assessment and Penetration Test team of Spara uses a set of powerful tools in the security assessment of mobile applications and services, which will provide complete coverage in the static assessment of program code and dynamic and server-side assessment. Also, due to the membership of some members of the security assessment group in the global working group for the preparation of methods for evaluating mobile applications (MSTG OWASP), they will always be familiar with the latest tools and evaluation methods.

In addition to the previous cases, according to the knowledge and work experience of the relevant team, this group has succeeded in developing more than 14 special tools for security assessment and mobile penetration testing.





Security assessment and penetration test of desktop applications

The development and use of applications that can be installed and run on a personal computer to accelerate and manage workflows have spread in organizations. These applications usually contain some or all of the important information about organizations and are also often based on client-server architecture. Lack of security in these applications, in addition to the risk of information disclosure, due to installation and execution on in-house computers, can potentially, in the least case, threaten the user's computer and in the most severe case, the entire network of the organization and even other related networks.

Based on common checklists and relying on exploit writing knowledge and expert experiences, and using specialized tools, Spara can evaluate desktop applications based on different programming languages and frameworks.

Security assessment and penetration test of network and equipment

The role of computer networks in managing, executing, and monitoring work processes and information sharing in the organization, is very important and necessary. Regardless of the size and type of services, the stability and especially the security of the computer network of any organization is very important. Lack of security in any computer network, in addition to the threat of disclosing information in the organization's business process cycle, can jeopardize the stability of services and cause service disruptions.

Based on OSSTMM, ISSAF, and PTES standards, relying on exploit writing knowledge, and expert experiences, Spara can evaluate local and wireless computer networks based on Windows, Linux, and other related devices such as Switch, Router, and Firewall.



Benefits of implementing Spara penetration test service

- Identifying the maximum vulnerabilities of the organization's IT systems/infrastructure
- Getting solutions to fix vulnerabilities and increase cyber resilience against advanced attacks
- Rechecking and ensuring that previously identified vulnerabilities are resolved
- Checking security settings
- Training the network and security experts of the organization to provide the ability to respond to attacks

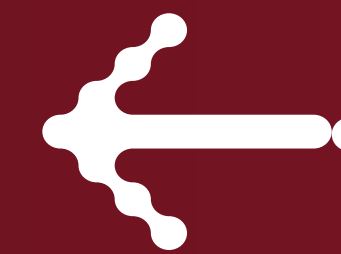
The competitive advantage of the Spara penetration test service

- Technical and specialized assessment to identify weaknesses and vulnerabilities using manual and automated techniques
- A specialized and accurate evaluation by first-rate experts, in addition to benefiting from the ability to identify system vulnerabilities with the exclusive tools of Spara Security Company
- Implementation of optimal methods and maximum identification of system vulnerabilities
- Providing complete security assessment services in web, web service, mobile, desktop, network, security equipment, etc
- Providing technical solutions for all identified vulnerabilities
- The possibility of developing and preparing different scenarios to increase the depth of penetration and perform attacks
- Significant increase in security maturity level and secure programming knowledge in organizations' development teams



Penetration Test is suitable for which businesses?

One of the most important ways to increase security and identify security weaknesses in the organization is the comprehensive implementation of security assessment and penetration tests on the organization's information technology systems/infrastructure. In this regard, using the penetration test service of Spara can be suitable for all companies, government departments, private and organizations.





About Spara

Today cyber risks are a critical threat to all organizations worldwide. In the past, organizations tried to provide their cyber security only by using the security equipment and software available in the market. But today, cyberattacks have a very complex structure, so it is no longer possible to deal with them using traditional methods. Therefore, to deal with advanced cyber threats, organizations need to use advanced detection and prevention systems to identify them in the shortest possible time in case of cyber penetration.

In this regard, “Spara” company and a group of the best cyber security experts in the country have produced new products, diverse services, and comprehensive cyber security solutions. “PAM”, “EMS” and “EDR” are the most important products of Spara. Spara’s security services and solutions also include a wide range of security services such as “Security Operations Center”, “Penetration Test”, “Threat Hunting”, “Red Team”, “Governance, Risk Management, and Compliance”, “Incident Response”, “Consulting” and “Training”.



We have been trusted by:



بانک پاساگاد



بانک تجارت



فنا
زیرساخت



فناپ تلکام
FARNAP TELECOM



فناپ تک
FANAP TECH



بانک آینده
AYANDEH BANK



ریاست جمهوری
معاونت علمی و فناوری



ساییا



MIDHCO



پست بانک ایران



هاده اول



شاتل
SHATEL



شرکت سیرده گذاری مرکز
اوراق بهادار و تسویه وجوه (سپا)



شوکا



شرکت فناوری اطلاعات ناواکو



پایگاه اطلاع رسانی پشتیبانی پاد



شرکت نرم افزاری دانش آریین قشم



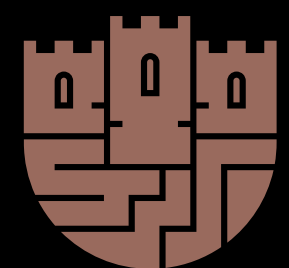
سازمان فناوری اطلاعات ایران



نماوا
NAMAVA



ایرانسل
MTN



سپارا
SPARA



+98(0)21-22275003



info@spara.ir



www.spara.ir