PENETRATION TESTING: ADVANCED METHODS FOR STRATEGIC RISK MANAGEMENT

PENETRATION TESTING:
ADVANCED METHODS FOR STRATEGIC RISK MANAGEMENT

What is Penetration Testing?

Penetration testing is an ethical hacking, legal threat, and bluff used for firms of all sizes, in all industries. This kind of risk monitoring has become an essential aspect of every security strategy. Pen tests are simulated attacks, on networks or on an entire IT framework, that reveal flaws in web browsers, connected devices, and operating systems. The aim is to identify and protect weaknesses before the systems come under attack or exploited by hackers. Considering the time and current stats, penetration testing is a critical step in data security management.

Penetration analysis is the method of simulating an intruder to find vulnerabilities in an IT network. Consider it as a reliability control for IT protection. It also ensures the safety of supply chains. As with most individuals, decision-makers likely think that quality assurance is both reasonable and important before releasing it into development. Not because they don't trust the developers but because it is mandatory to make sure that the program runs in their favor and has no functional difficulty.

While they utilize almost the same procedure, some ethical hackers prefer the word "security evaluation" to "penetration testing."

Penetration regulators are also known as "The Red Team." This refers to penetration testers, a phrase that dates back to the early days of security research in the army, whereas the "Blue Team" refers to the defense team. How does vulnerability assessment apply to finding vulnerabilities and threat detection? Penetration tests must be more than just a way to check a box: we can expect critical initial steps for improving cyber defense. Also, another point worth mentioning here is that weakness measurement is not the same as penetration testing.

Risk assessments produce a prioritized list of weaknesses, as well as recommendations, for how to address the vulnerability.

Common Phases of Penetration Testing

The first common step is planning: infrastructure and boundaries, inspecting ports, studying weaknesses, attack vectors, choosing the right devices, and so on. This process of white-box research also involves collecting data on the target business and its workers. Preparation is the most important and time-taking step in pen-testing, but indeed has its own value.

Throughout the attack process, testers attempt to compromise the target network by breaching the secure perimeter, gaining or escalating credentials, gaining access to data, and erasing traces.

The last step, the post-attack phase, entails evaluating possible harm and reporting on the penetration testing process' findings. The risk evaluation strategy is normally concluded with a report with all the necessary information:

- An overview of the method and techniques being used in testing
- A list of vulnerabilities
- Analysis of the threats these weaknesses may pose
- An evaluation of the potential business effect of the revealed risks

Benefits of Penetration Testing

- Identify the vulnerabilities
- Identify high-risk weaknesses, factors and pain points
- Final reporting of all identified vulnerabilities and specific advice

Possible Risks of Penetration Testing

- If not done with precautions, the servers can collapse and data could be corrupted
- The team performing pen testing needs to gather realistic data, otherwise the result could be meaningless
- You need to trust an outsider (Penetration Tester) with all your systems and data
- An attack can come uninvited anytime, so employees and leaders need to be stronger, and assessors need to be realistic towards the test results
- Pen testing needs to be performed with limitations of time and scope taken into consideration, otherwise unexpected costs could burden the project

How to Maximize Penetration Testing Results

1. Pen testing needs to be conducted by experts

Testing performed in-house is very tempting because of the cost and time effectiveness; however, unbiased results cannot be generated for several reasons:

- Low level of skills
- Conditions which are not realistic
- Likelihood that an attack cannot be executed

The benefit of hiring employees from third-party organizations is that they are experts with the command of their skills, and results generated by them would be unbiased and insightful. As part of cyber security planning, owners need to discuss the amount they can pay to expert organizations, and also document the previous results of pen testing so that there will be no compromises on the performance of new tasks.

2. Highest coverage of tests

Even if you've checked and protected everything, there's always the chance of being targeted. Hackers will find new ways to get through flaws in the operating system, hardware, or other applications. Low test coverage and incomplete testing only give the illusion of security. To prevent such cases, firms often perform high coverage in order to double-check security fixes applied after penetration testing.

3. Test arrangements shouldn't be rushed

Testers evaluate weaknesses, weaponize themselves, and plan test cases before the attack. However, outside of the research team, it can seem that none of that is occurring since no real evaluation is taking place. It's fine to inquire about the testing phase now and then, but don't push the process. Keep in mind that this is a lengthy procedure. The phase of black-box analysis will account for up to 89% of the overall projected cost.

4. Apply applicable penetration testing values

Each testing process necessitates a unique mindset. There are, however, internationally recognized and industry-accepted penetration testing guidelines. These specifications can be used to direct internal teams or to ensure that third-party providers follow them.

5. Stop the progress of processes when pen testing

Pen testing identifies vulnerabilities in the sense of a specific area. Changing accessible parameters or installing the latest software during the evaluation will jeopardize the outcome. To include new aspects of the program in the experimental context, it's better to conclude the planning process prior to the actual test.

6. Appraise the reliability of safety measures after the analysis

The team performing safety measures can clean up their traces by closing backdoors generated during the assessment, deleting exploitation scripts, temporary files, reversing configuration adjustment, and so on. Teams can, nevertheless, double-check the following:

- Safety flaws that were developed for research purposes have been patched
- Insecure passwords are updated
- Customer accounts for developers are removed

7. Don't overlook the importance of corrective actions

According to some sources, pen testing companies also make recommendations for threat mitigation. If the analysis is done infrequently or covers a broad range of activities, it is likely to reveal a huge number of vital risks, necessitating a significant amount of time and funds. Security teams can delay corrective actions or remediation, or can repair just the important problems to save money. Due to limited time to act on the findings of a penetration test, it might be better to begin with inner intrusion detection rather than a full-fledged penetration test.

Conclusion

Penetration testing is an advanced risk management strategy that lets companies securely explore, evolve, and grow. Threat evaluation is indeed a difficult but essential step in the process of risk management. It aids in the identification, assessment, and prioritization of a company's cybersecurity threats. Penetration monitoring, Red Team testing, and risk-based testing are only a few of the approaches for performing a threat measurement. On the other end, penetration testing cannot be overlooked in this procedure: it allows for a detailed appraisal of safety controls as well as the simulation of an actual assault on the secured business.

To learn more about Estes Group Services, please visit www.estesgrp.com.