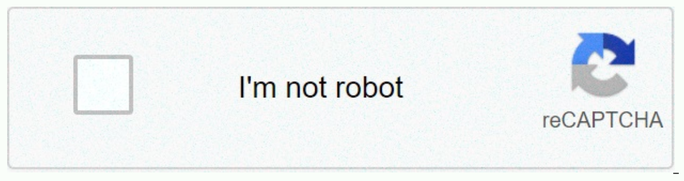

Continue

Penetration testing report example

Some organizations make a mistake by treating pencil tests as a tick exercise to meet only one compliance requirement before the next movement. This approach cannot be achieved by security improvement organisations, which must keep up with the latest threats – corrective measures are essential. In order to facilitate the healing process, all externally sourced pencil tests should provide codes of practice to achieve tangible security improvements. This blog outlines five things you should expect from a penetration test report. 1. A detailed overview of the security risks identified is, of course, the first thing to ensure that all vulnerabilities uncovered during the probationary period are covered in sufficient detail. In order to help all key stakeholders understand the test results, a good pencil test report usually contains an executive summary highlighting the main results. The report should subsequently describe the technical details and practical consequences of each vulnerability. The human-led penetration test reveals complex exposures that sit beneath the surface and are usually longed for by automated scanning tools. In the pen test report, you should wait for an explanation of where these deeper vulnerabilities are located, what assets are affected, how they were discovered and what the attacker could do if the vulnerabilities are not addressed. 2. Business impact assessment In order to help stakeholders understand the priority level of weaknesses identified, the pen-test reports should also include the potential impact of each issue on business. By default, many automated testing tools determine a certain numerical vulnerability scoring level that is often mapped to the Common Vulnerability Assessment System (CVSS). However, these scores are of limited value – they do not take into account which vulnerabilities are actively exploited in nature and how they relate to the specific risk profile of the organisation. In order to increase the value, the pencil test report should be prepared by a security expert, who may use a more complex assessment system that determines both the comparable score (critical/high/average/low) and the accompanying explanation of what this means for the company in question. For example, a critical vulnerability points to an issue that could lead to a complete compromise of an asset or network that can cause significant financial and reputational damage, such as an unauthenticated SQL injection error. Vulnerabilities with large, medium and low impacts cover all other issues that may affect confidentiality, integrity, or availability. Organisations should also expect to be informed of informational issues – any minor deviation from the best security that may pose a greater risk in the future, while at the same time causing minimal immediate risk. 3. An overview of operational difficulties A closely related factor affecting the risk assessment is Difficulty. Severity cannot be effectively analyzed without examining whether an attacker can actually exploit the vulnerability. The main advantage of penetration testing is that it goes beyond the scope of more basic security assessments, identifying not only vulnerabilities but also trying to exploit them. The typical operational scale of the report ranges from simple (where exploitation is trivial and requires basic resources and knowledge) to the difficulty (requiring experts' hacking and development skills, as well as considerable time and effort). The most advanced weaknesses can be determined by difficulties at the level of the state, the attacks of which can only be theoretical, which requires large resources to commit an attack. 4. Healing tips for identifying vulnerabilities are only half the battle – timely confirmation is also important, and buyers should look for a pen testing partner to provide detailed guidance on how to solve each problem as part of the reporting process. Healing is usually significantly different. Some issues require easy patches or updates and can be solved immediately. Others may require a reconfiguration or code rewrite from the development team, which sometimes requires assistance from a partner or vendor. Some problems may simply not have an accessible correction, which requires temporary infrastructure and process changes to mitigate risks. A good pen-test provider guides customers through this process and makes recommendations about what information needs to be provided to vendors and regulators and which organizations to use for help. Most of this information is provided in the test report, but critical vulnerabilities should be described if uncovered in order to minimise the potential risk. 5. Strategic recommendations In addition to the instructions for redress, the importance of strategic recommendations in the pen-test reports is often disregarded. Security should be seen as a journey, not a destination. Even the most comprehensive program assesses the state of security at only one point in time; with ever-evolving threats and attackers who are planning new ways of exploiting vulnerabilities on a daily basis, organisations cannot afford to think only in the short term. Starting with the expert opinion on the overall security position of the contracted organisation, a good pencil testing report will be submitted to advise on which areas to consider in the long term. This may include an assessment of existing security controls, feedback on working procedures and guidance on which future security investments should be prioritised. Why choose Redscan for your testing needs? As a multi-award winning CREST-approved penetration test service provider, Redscan is ideally positioned to meet your organization's security assessment

requirements. Our team of ethical hacking experts deeply understands how the attackers operate, and we leverage that knowledge organisations to mitigate cyber risk. After each penetration test, we provide clear and detailed reports that include comprehensive threat analysis, actionable advice, and full post-test care to help you improve your cybersecurity position in a tangible and lasting way. Get a Pen Test Quote Today Read More: Vote For Redscan in Cybersecurity Excellence Awards! The 10 ways to strengthen your organization's cybersecurity 2020 Redscan-listed finalist at the FStech Awards 2020 Penetration Testing may consist of a variety of activities designed to simulate real-world attack scenarios against corporate IT and physical security checks. The ultimate goal of the penetration test is to validate vulnerabilities detected during the scanning phase and to intelligence other attack vectors. Modern attackers face sophisticated security checks and smaller offensive surfaces; this has led to a shift in the approach of attacking the company. Simple attacks have evolved into elaborate campaigns for intelligence, data collection, phishing, fraud, theft, and social engineering to evade these advanced tools. In this model report, our experts share their approach to protecting companies from their advanced cyber attacks. Finally, you have the knowledge you need to read, write and perform a successful penetration test. You'll also better understand what to expect from your security vendor when you present these results. Penetration test reports are very important and will give you a structured detailed overview of the pen test after completion of your involvement. However, often this critical documentation lacks the basic aspects that should be included, and customers begin to question the practical value of their assessments-and-rightly. The report is everything. While there are many nice things that can be included in the report, Rhino Security Labs has identified four features that make each pentest report outstanding. The executive summary is a high-level overview of both risk and business impact in plain English. The aim is to be short and clear. This should be something that non-technical readers can review and get an overview of the security issues highlighted in the report. While IT staff may need all the technical details, managers do not need to understand this technology. They need to understand business risk, something good executive summary to communicate effectively. It is imperative that business leaders understand what is at stake in order to make informed decisions about their companies, and an executive summary is essential to achieving that understanding. Visual communication can also be useful in getting complex points throughout clearly. You can find graphs, charts, and similar visuals in the summary data provided here. Most reports use a rating system to measure risk, but rarely take the time to explain the risk. The Client's IT department must effective decisions on how best to address vulnerabilities. To do that, they need the approval of the people upstairs. Just to claim that something is dangerous is not a properly conveyed risk. For example, if a critical vulnerability is found that allows file uploads to a health portal, there are two ways to report it: 1 – technically accurate – the Company X web application does not restrict user upload by file type, creating a vulnerability that allows an attacker to run arbitrary code remotely and elevate their permissions in the application. 2 – Both accurate and contextualized – Enterprise X Web Application does not restrict user upload by file type, creating a vulnerability that allows an attacker to run arbitrary code remotely and elevate their privilege in the application. In this case, the attacker would be able to view the health data of each user and act as an administrator of the application. The second is more weight, which shows not only the technical aspects, but also the impact on business. The most valuable reports are those who speak to all members of the audience in a language they understand – especially those in leadership positions. For example, if your team finds that the Customer Health Management Web Portal allows users to upload a profile picture but doesn't prevent them from uploading arbitrary code instead, there are essentially two ways to report it: risk can be divided into two pieces: probability and potential impact. The probability is standard in most evaluation reports. Of course, the likelihood of exploitation is not enough to determine the risk, albeit important. You do not rank a deeply rooted remote code execution lower than the email address developer apparently exists in the HTML script. This is because the former would be much more influential to the customer. If you think you're seeing a topic here, you're not wrong. The evaluation report is not intended solely for IT staff. Leaders need to see how vulnerability that anyone could have directly affected their organization specifically. An important part of the excellent report is to take into account both the likelihood of exploitation and the potential impact on the overall risk. Most penetration test reports include a general high-level description of how to solve these problems; but these general catch-all instructions are often missing when it comes to the unique context of the customer's needs. If a client has a vulnerable service running on a Web server on which they depend, the fix should offer more than a complete disabling of the service. Of course, it's important to let the client know that filtering SQL injections is a simple method or configure a firewall to block certain attacks. This means that the quality of the pentest report gives you several improvement options that are detailed enough to prepare the client's IT team for a quick fix. internal staff already know how to re-improve all vulnerabilities, significantly reduces the value of the penetration test. The penetration test itself is not the reason customers are looking for security assessments. The assessment report and the customer support are. That is why we put so much attention and effort into reporting. Details such as a literal description, the correct methodology, vulnerability description and other factors are also important; the implementation of these four concepts is also a recipe for an excellent report. If you didn't have these items at the last time your organization was involved, or you're simply not happy with the documentation, contact us for a quote or check our own sample reports. Reports.