GUIDE TO PENETRATION TESTING

HALOCK®
Purpose Driven Security

Contents

The Vulnerability Assessment Services practice within HALOCK offers comprehensive penetration testing services. A penetration test assesses your unique environment and evaluates its strengths and vulnerabilities as well as validates existing security practices and controls. Whether you are just now researching penetration testing or you have a regularly scheduled penetration testing program in place, there is a great deal of information and misinformation in the marketplace with regard to exactly what penetration testing is and what you should expect from a penetration testing company. In this guide, you will find comprehensive answers to typical questions surrounding penetration testing.

What is a penetration test?

A penetration test, also known as a "pen test" is a method for evaluating the effectiveness of an organization's security controls. Testing is performed under controlled conditions, simulating scenarios representative of what a real attacker would attempt. When gaps are identified in a security control, a penetration test goes beyond basic vulnerability scanning to determine how an attacker would escalate access to sensitive information assets, confidential information, personally identifiable information (PII), financial data, intellectual property or any other sensitive information. Penetration testing utilizes tools and techniques, guided by a disciplined and repeatable methodology, resulting in a report containing detailed findings and recommendations that allow an organization to implement counter measures and improve the security posture of the environment. These improvements ultimately reduce the likelihood an attacker could gain access.

How does a penetration test differ from an automated vulnerability scan?

Both penetration tests and automated vulnerability scans are useful tools for managing vulnerabilities. While these are different testing methods, they are complementary and both should be performed.

A ***vulnerability scan*** is an automated, low-cost method for testing common network and server vulnerabilities. This is sometimes referred to as an automated pen test. Many automated tools are available and most are easily configured by the end user to scan for published vulnerabilities on a scheduled basis. While an automated vulnerability scan is very efficient and cost-effective in identifying common vulnerabilities such as missing patches, service misconfigurations, and other known weaknesses, they are not as accurate in validating the accuracy of vulnerabilities nor do they fully determine the impact through exploitation. Automated scanners are more prone to reporting false positives (incorrectly reporting weaknesses) and false negatives (failing to identify vulnerabilities, especially those impacting web applications). Automated Vulnerability Scanning is mandated by the Payment Card Industry Data Security Standard (PCI DSS) as noted in requirement 11.2.

A ***penetration test*** focuses on the environment as a whole. In many ways, it picks up where the scanners leave off to provide a comprehensive analysis of the overall security posture. While scripts and tools are leveraged by a penetration tester, their use is largely limited to reconnaissance activities. The bulk of a penetration test is manual by nature. A penetration test identifies vulnerabilities scanners cannot, such as wireless flaws, web application vulnerabilities, and vulnerabilities not yet published. Further, pen testing includes attempts to safely exploit vulnerabilities, escalate privileges, and ultimately demonstrate how an attacker could gain access to sensitive information assets. Penetration testing frequently applies "test scenarios" specific to an organization as well. For example, a university may grant access to student workers, a hospital may leverage third party service providers, or a consultancy may have unique access rights for their engineers. Each of these scenarios would require different positioning of the penetration tester within the environment and requires adjustments to the methodology. Penetration Testing is also mandated by the PCI DSS as noted in requirement 11.3.

Penetration testing and automated vulnerability scans both serve a purpose and both types of testing belong in a comprehensive vulnerability assessment program. Automated vulnerability scanning should be scheduled to run on a frequent basis, ideally at least weekly, with penetration tests scheduled quarterly or when significant changes are planned to an environment.

What are the goals of a penetration test?

Goals vary greatly based on the scope of review. Generally speaking, the goal of a penetration test is to validate the effectiveness of security controls designed to protect the system or assets being protected.

Why should we have a penetration test performed?

Penetration testing should be performed for a variety of reasons. Some of the more common reasons why companies perform penetration tests include:

1. Most relevant regulatory standards require penetration tests are performed.
2. Penetration testing can identify vulnerabilities inadvertently introduced during changes to the environment, such as a major upgrade or system reconfiguration.
3. Penetration testing can be integrated into the QA process of the Software Development Life Cycle to prevent security bugs from entering into production systems.
4. Organizations, especially those acting as data custodians, are being required to

have testing performed by their customers. Penetration testing can demonstrate a commitment to security from a customer perspective and provide attestation that their assets or services are being managed securely.

5. Penetration testing is a common requirement for internal due diligence as part of ongoing efforts to manage threats, vulnerabilities, and risks to an organization. Results can be used as input into an on-going Risk Management process.
6. Penetration testing allows companies to assess the security controls of potential acquisition targets. Most organizations preparing to acquire an organization seek insights into the vulnerabilities they may introduce in doing so and plan for the costs they may be incurring to remediate.
7. To support a breach investigation, penetration testing may tell an organization where the other vulnerabilities may exist in order to have a comprehensive response to the incident.
8. Penetration testing allows companies to proactively assess for emerging or newly discovered vulnerabilities that were not known or have not yet been widely published.
9. Penetration testing serves as an aid to development teams who are writing new web applications. Many development lifecycles include penetration testing at key stages of the process. Correcting flaws are typically less costly the earlier in the development lifecycle that they are discovered. Additional testing prior to go-live on a production-ready build can identify any remaining issues that might require attention before loading users on the application.

What should we expect from the penetration testing process?

As mentioned earlier, penetration testing is an extremely disciplined process. A penetration testing company should keep all stakeholders well-informed through every key stage of the process. As a company seeking penetration testing services, you should expect the following (at a minimum):

- A well-coordinated, planned, documented and communicated approach to know what is happening and when
- A disciplined, repeatable approach should be followed
- The approach should be customized to suit the unique environment of the business
- A clearly defined initiation process, planning process, coordinated testing and a collaborative delivery process to ensure accurate results and a clear understanding of remediation

Is testing disruptive to our environment? Will our systems go down?

If the test is not properly planned and coordinated, there is significant risk of disruption. This is why it is imperative that the planning is done properly, and comprehensively, to identify potential risks for disruption and adjust the approach accordingly. This planning should be conducted well in advance of any testing start date in order to ensure adequate time for communication to project stakeholders. The communication and monitoring should continue throughout the testing schedule.

How often should we do a penetration test?

It depends. A variety of factors should be thought-through when considering the frequency to conduct penetration tests. When determining what is appropriate include considerations such as:

- How frequently the environment changes: Tests are often timed to correlate with changes as they near a production ready state.
- How large the environment is: Larger environments are frequently tested in phases to level the testing effort, remediation activities, and load placed on the environment.
- Budgetary factors: Testing should be scoped to focus on the most critical assets according to a timeline that is supported by the allocation of security budgets.

Remember that the frequency of the testing needs to be adjusted to meet the unique needs of the organization; and it's important that those needs are understood and incorporated into the testing approach from the beginning.

Testing too infrequently allows for a window that increases an organization's exposure. On the other hand, if testing is done too frequently, there is inadequate time to remediate before testing resumes. Therefore it is important to strike a balance.

Companies that recognize the importance of penetration testing will implement testing on a recurring basis. Recurring pen testing programs allow the schedule to be more adaptable and is better suited to take these factors into consideration. Recurring pen testing programs also allow companies to spread the tests out over a longer horizon and increase frequency to narrow the window for exposure.

How is the scope defined for a penetration test?

Collaboratively. The scope should always be customized to suit the unique nature of the business. A variety of considerations, both internal and external to an organization, impact and guide the scope of a penetration test:

- The nature of the business and types of products/services offered
- Compliance requirements and deadlines
- Geographic considerations
- Organizational structure
- The organization's strategic plans
- Customer expectations, especially when an organization acts as a custodian of that customer's data
- The value of the company's assets
- Redundancy in the environment that may impact sampling thresholds
- Network segmentation and connectivity
- The age of different components of the environment
- Recent or planned changes to the environment

All of these factors need to be discussed and understood to make sure that the scope is appropriate and to ensure that the testing is focused in the areas of the environment that warrant it.

What qualifications should the penetration testing team possess?

When a penetration testing provider is hired, the hiring company should expect that every penetration test team includes a dedicated project manager, a skilled and experienced test team, resource coordinator(s), and a point of escalation. The test team should include individuals with in-depth experience across multiple technologies including client platforms, server infrastructures, web application development, and IP networking. The individuals on the team should hold valid certifications relevant to their role such as Project Management Professional (PMP), Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP) or equivalent credentials. When a penetration test is being performed to comply with a regulatory requirement, additional experience or certification is required to ensure the approach is appropriate and the results are presented in the correct context. For example, a penetration test performed to validate compliance with the Payment Card Industry Data Security Standard (PCI DSS) requirement 11.3 is best delivered by individuals with PCI QSA and PCI PA-QSA credentials. Many skilled penetration testers also typically possess other technology certifications to demonstrate their knowledge and proficiency.

The deliverable should clearly document the scope and boundaries of the engagement as well as the dates the testing was performed.

What documentation should I expect to receive when the testing is complete?

Once the penetration test is completed, the hiring company should receive a report or deliverable detailing all of the findings, recommendations, and supporting evidence. The deliverable should clearly document the scope and boundaries of the engagement as well as the dates the testing was performed. Additionally, all detailed findings should be included in their technical format as well as summarized for non-technical audiences. The report should include:

- Detailed recommendations for improvements that clearly document observed vulnerabilities
- A discussion of the potential business impacts from identified vulnerabilities
- Specific instructions for remediating, including instructional references where appropriate
- Supporting evidence and examples
- A step-by-step and screen-by-screen walkthrough demonstrating any exploits to allow an organization to understand and reproduce the scenario
- Executive and summary reports for non-technical audiences

Oftentimes, a separate deliverable is needed that is suitable for consumption by third parties seeking attestation that a penetration test was performed. A qualified penetration test provider prepares these documents as part of the process when requested by an organization. All deliverables should be of high quality and reviewed with the customer to validate accuracy and ensure recommendations are well understood.

How do we verify vulnerabilities have been remediated?

Validating that vulnerabilities have been remediated can be performed using a variety of methods, either in-house or through external independent verification testing. Some organizations prefer to track remediation in-house and possess the resources to independently validate successful remediation, however most seek independent validation and should have a remediation verification test performed. This is why it is critical that a penetration test be performed in a repeatable manner. Of equal importance is that the individual validating remediation is not the same individual that performed the remediation. Checking one's own work is not as reliable as having an independent individual check that person's work.

How do we prepare for a penetration test?

In general, there is no need for any special preparation with respect to how security controls are managed on a day-to-day basis. Remember that a penetration test is a point in time review of the environment. The test is going to assess the security posture at that particular point in time. If patches are deployed every Wednesday, for example, there is no need to change this behavior to accommodate the penetration test itself. If the results of the penetration test determine this process requires attention, then that would be the appropriate time to adjust.

An organization should expect to participate in preparation activities related to planning the penetration test itself to ensure the test can be performed under controlled conditions. Some preparation related to positioning the tester may also be needed, specifically when testing is being performed onsite.

The hiring company should be prepared to participate in the planning and coordination activities and be ready to have documentation available that details the in-scope IP ranges for testing when web application pen testing is being performed. Also be ready to prepare test environments and to support test scenarios defined in the scope. During internal onsite penetration tests, oftentimes visitor access badges are required for the penetration testers. Otherwise, there is not much else that is needed to be done prior to the test.

We have our website hosted with a third party. Should we test it?

Maybe. The first thing to do is to find out if the third party is already having a reputable penetration test provider review the website. If so, due diligence is needed to validate the scope is appropriate, review the methodology, and understand if any key findings were observed. An organization should confirm when it was last tested, when it will next be tested, and if there are any security vulnerabilities that were determined to be tolerable by the hosting provider.

If the third party is not testing the site, or if the testing being performed is not adequate, then yes, the site needs to be tested. Obtain the third party's permission, as they should be involved in planning, to ensure that the site is tested safely and coordinated appropriately. If the third party won't allow testing, one should strongly consider obtaining a "right to audit" clause in their contract or locate another hosting provider that accommodates the need for ongoing vulnerability management, including penetration testing.

Should we fix all of the vulnerabilities that are reported?

No, but this is not a blanket rule. You should evaluate all of the vulnerabilities using a risk-based model first. Each vulnerability should be evaluated for business impact and probability of being exploited to ultimately assign a risk rating. Companies should have risk criteria defined in order to determine thresholds for remediation. Vulnerabilities above the threshold should be remediated or appropriately compensated for in order to bring them within tolerable risk levels. Vulnerabilities that are within an acceptable threshold may not require remediation and instead may simply be monitored over time in case the risk level changes. The penetration test deliverables should contribute to this process. In certain compliance situations, specific vulnerabilities may be viewed as compliance gaps; and those gaps typically are either remediated or compensating controls are put in place when remediation is not possible.

What are typical costs for a penetration test?

The cost for penetration testing varies greatly. A number of factors are used to determine pricing including, but not limited to the scope of the project, the size of the environment, the quantity of systems, and the frequency of testing. It is critical to have a detailed scoping meeting to produce a very clear understanding of the needs, and develop a statement of work prior to engaging any penetration test. Ideally a penetration test should be performed on a fixed-fee basis to eliminate any unexpected costs or unplanned expenditures. The quoted fee should include all labor and required testing tools. Statements of work that only provide estimates of the work effort should not be entertained.

How much time is needed to perform a typical penetration test?

Adequate time should be reserved in advance of testing for planning activities. Additional time should be allocated after testing for report development and subsequent review meetings including remediation discussions. The entire effort varies greatly based on the size and complexity of the penetration test. The larger or more complex the environment is, the more effort is required. The duration of the test, however, is very controllable. The duration of the test should be compressed to ensure a good, representative view of the environment at a given point in time. Generally speaking, four to six weeks is a good estimate for the duration of the entire engagement from planning through final delivery. The actual test itself typically varies from one to two weeks depending on the size of the environment. It is very rare for a test to take longer than two weeks and when an environment is large, a larger pen test team should be assigned to keep the test window to one to two weeks max. For larger or more complex environments, testing may be broken into phases.

Can we do our own penetration testing?

It depends. Assigning internal resources may be a viable approach in certain situations. If the business is considering performing in-house penetration testing, the following should be considered first:

- The penetration testers on staff should be experienced, trained, and familiar with a variety of technologies.
- The penetration test team should have a different reporting structure than engineering or implementation teams. Separation between those managing the environment and those testing the environment is crucial. No one, no matter how skilled, can objectively test their own work.
- Some regulatory bodies have independence requirements that may require organizational changes or additional layers of oversight before they view the test as truly independent. These considerations should be explored to determine if they apply.
- A repository of commercial and open source tools should be obtained and updated regularly. As the costs for these tools can be significant, this should be included as part of the decision to avoid unexpected costs.
- On-staff experienced project management capabilities are needed, especially in larger organizations where coordinating with various business units is needed prior to the test beginning.
- Continued training and ongoing monitoring of newly discovered vulnerabilities and threats is necessary.
- Staying current and up-to-date with testing methodologies, planning and deliverable artifacts is also necessary.
- Penetration testers should have access to a dedicated test lab for developing and testing exploits prior to their use in a production environment.

If these assets are available to an organization or the cost to obtain and maintain them is lower than leveraging a third party, it may be more cost-effective to perform penetration testing in house. More often than not, it is far more cost-effective to leverage a third party that is already equipped for penetration testing.

My customer wants to see the results of our penetration test. Should I share the results with outside parties?

It is not a good idea to send results outside of your company. A penetration test report contains extremely sensitive information that is highly confidential and should only be made available to trusted internal resources on a "need-to-know" basis. Sharing detailed reports with external individuals is not recommended. Once the report is shared with an external party, control over its distribution is difficult to guarantee. A penetration test report can be a roadmap to an organization's vulnerabilities and should not be distributed outside unless absolutely necessary.

A penetration tester should provide a summary version of the report that details scope, approach, qualifications and categorical results. This summary report is more appropriate for an organization to share. It is common to include summary remediation plans if applicable but ultimately, the third party needs to receive documentation that gives them comfort that there is a mature, ongoing testing program that is proactively assessing the environment, and that key findings are being appropriately addressed. Providing the external party specific test details could present a significant security risk. A summary deliverable can be provided to third parties that provides insight into the testing without revealing sensitive details.

Nonetheless, some customers will still require that they see the full results. If this is a request an organization wishes to accommodate, the customer should be invited onsite and given a printed copy of the detail for onsite review only.

What is the difference between "Ethical Hacking" and other types of hackers and testing I've heard about?

It depends on who you ask and you shouldn't put a lot of stock into these terms since no industry accepted standard for these terms exist. For example, the approach of the test may be referred to as "Ethical Hacking" (implying legitimacy of the approach), "Black Box Testing" (implying a covert, unassisted, test), "White box Testing" (implying an assisted, non-covert test), or any variety of shades of gray along the way.

These are terms cleverly used for marketing purposes and should not be considered when forming a basis of the qualifications of the test team. When selecting a team to perform the test, the company should focus on the credentials of all team members on the project, their experience, peer references from those that have worked with them, and ultimately that their approach and methodology is industry accepted. These characteristics are what matters to ensure a test is performed safely, comprehensively, and can be relied on.

In the ever-changing world of cyber-security, new terms and names are continually being invented to describe a penetration test. Our recommendation is to call a "penetration test" by what it is...a "penetration test."

NEED MORE INFORMATION?

PENETRATION TESTING

How Do You Know If Your Systems Are Secure?

Penetration Testing (Pen testing) demonstrates what a malicious individual could accomplish in your environment and measures the effectiveness of existing security controls. Test findings include detailed recommendations that allow organizations to proactively implement countermeasures to prevent real world exploitation of identified vulnerabilities.

Penetration Tests are performed from a variety of perspectives to assess common entry points into the environment, including:

HAVE QUESTIONS?

Ask our Pen Testing team and see how HALOCK can help you.

Visit ***www.halock.com/pentest*** for more information about our Vulnerability Assessment Services as well as other ways HALOCK can help you.

PURPOSE DRIVEN SECURITY

Organized crime, state sponsored cyber teams, and hacktivists all have different aims, however, the one common theme that unites them is the unauthorized access and use of computer systems to fulfill their mission.

There is no silver bullet to protect assets from these threats. A paradigm shift is required to reduce risk to organizations. HALOCK Security Labs has pioneered a new security model to meet these cyber threats. At the foundation of this new model is a service philosophy called Purpose Driven Security® which helps define the right amount of security to protect critical assets; not too much, not too little. The philosophy can best be summarized as measured and preemptive risk management.

It is measured in that not all security controls should be implemented and only to a certain degree depending on the calculated risk being treated. It is preemptive in that organizations have an obligation to perform proactive due care to reduce liability for shareholders, clients, partners, employees, and the greater good as appropriate. Together this dual emphasis enables organizations to utilize a limited security budget and maximize protection of critical information assets.