The Complete Guide to Penetration Testing

ERMProtect
Cybersecurity Solutions

What is Penetration Testing?

["To know your enemy, you must become your enemy"– Sun Tzu]

A penetration test emulates methods used by real-world hackers to assess the security measures protecting a computer system or information resource. The process involves cyber experts - called ethical hackers - getting into the mindset of a hacker and launching attacks to identify an organization's likely vulnerabilities.

They contemplate: If hackers attacked, what method would they use? What time would they attack?
What entry point would they use? Cyber experts simulate these attacks, identify how they got inside and recommend fixes to exploited vulnerabilities.

Why is Penetration Testing Needed?

Hackers, as an adversary, are quite a handful for organizations. They have the elements of surprise and stealth, and they can simply choose to retreat and attack again at will. Organizations, on the other hand, have none of these luxuries. They're effectively left to defend a fortress against any type of attack, from any direction, at any time.

But organizations do have a way to prepare and fight back. It's called penetration testing. The goal of penetration testing is to assess the security measures protecting an information resource by emulating the methods used by real-world hackers. As a result, organizations can discover weaknesses in technical infrastructure and measure their resistance to hacker attacks.

Different Ways to Aproach Penetration Testing

Before beginning a pen test assessment, choose from one of these types:

White Box	*A white box penetration test is where the tester is given all information about the information resource being attacked.* **Benefit:** *A white box penetration test may be more comprehensive and unearth more vulnerabilities since the "attacker" has so much advance information about the target.*
Black Box	*A black box penetration test is exactly the reverse – the tester is given no information about the information resource being attacked.* **Benefit:** *A black box penetration test may offer a more "real world" scenario wherein the malicious hacker has no advance knowledge about the organization's technical infrastructure.*
Grey Box	*A grey box penetration test is a middle ground wherein the tester is given some information* **Benefit:** *A grey box penetration test is often the best route to take since malicious hackers are bound to have gathered at least some information about their target.*

The Five Penetration Testing Phases

The methodology of penetration testing differs for every ethical hacker, but there are typically five phases. These phases ensure the penetration testing is robust, thorough, methodical and effective.

The Different Types of Pen Tests

Network Penetration Test

A Network Penetration Test, as the name suggests, involves simulated hack attacks directed at the network of the organization being tested.

The External Network Penetration Test simulates real-life hacker attacks at a network level, in a scenario where the hacker is located outside the organization and its internal network.

The Internal Network Penetration Test, on the other hand, simulates real-life hacker attacks at a network level, in a scenario where the hacker is located inside the organization, connected to its internal network.

Both tests provide insights into how well protected the organization's networks and information resources are from malicious hackers.

Web Application Penetration Test

A web application is an application program that can be accessed through a web server such as online banking, e-commerce websites, and so on. Because these online portals enable a significant number of transactions of highly sensitive information and are typically globally accessible on the Internet, they are a high-value targets for attackers. By conducting Web Application Penetration Tests, organizations can significantly shore up defenses.

This test also includes testing of web services, which are vulnerable because they often interface with other IT solutions to meet business objectives. They are often the most neglected part of the application system because organizations think they are safer than the rest since they cannot be directly accessed through a browser or discovered openly. In fact, web services provide direct and easy access to hackers.

Cloud Infrastructure Penetration Test

Tests of cloud infrastructure identify vulnerabilities, misconfigurations, and implementation flaws. There are several ways in which a Cloud Infrastructure Penetration Test can be performed such as testing publicly available systems or privately held systems hosted within a cloud environment. All tests are performed after obtaining prior approval from the cloud service provider.

ICS/SCADA Penetration Test

ICS/SCADA Penetration Tests target the Industrial Control Systems (ICS) or the Supervisory Control and Data Acquisition (SCADA) systems within an organization. The tests are fully aligned with the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) requirements. These penetration tests require highly specialized skills and specific experience in testing ICS infrastructures.

Social Engineering Test

Social engineering attacks try to dupe computer users into installing malicious programs on their machines or divulging sensitive information. These tests help organizations understand how well their employees are equipped to protect organizational information and resources. Ethical hackers may send fake emails from management, masquerade as a technical support employee, or engage in other phishing schemes to see if employees click through, and accidentally expose the organization's sensitive data.

PCI Penetration Test

Payment Card Industry Data Security Standard (PCI DSS) requirements mandate that organizations perform comprehensive and detailed infrastructure penetration tests of several types. These tests help organizations attain compliance with PCI requirements by performing ongoing and periodic PCI Penetration Tests that are designed to align with each specific PCI DSS requirement that organizations need to comply with.

Mobile Application Penetration Test

Mobile applications ("apps") have become a crucial part of our lives. We use them for banking, ecommerce, messaging, maps, email and scores of other things. Unfortunately, they also provide additional entry routes to hackers. A Mobile Application Penetration Test allows organizations to assess their mobile application infrastructure.

Physical Site Penetration Test

Testing the physical defenses of an organization helps ensure that data can't be exploited via gaps in physical controls and security. Investigators test whether individuals can gain physical access to the organization's sensitive information and storage areas.

Regulatory Compliance Penetration Test

Many organizations are regulated by data laws such as GLBA, HIPAA, GDPR, HITECH, FACTA, FERPA, BSA, and so on. Most regulations directly or indirectly require organizations to perform ongoing and periodic penetration tests of the technical infrastructure that houses sensitive information. Regulatory Compliance Penetration Tests help organizations achieve compliance objectives by performing penetration tests completely tailored to the specific requirements of the applicable regulations.

IoT Penetration Test

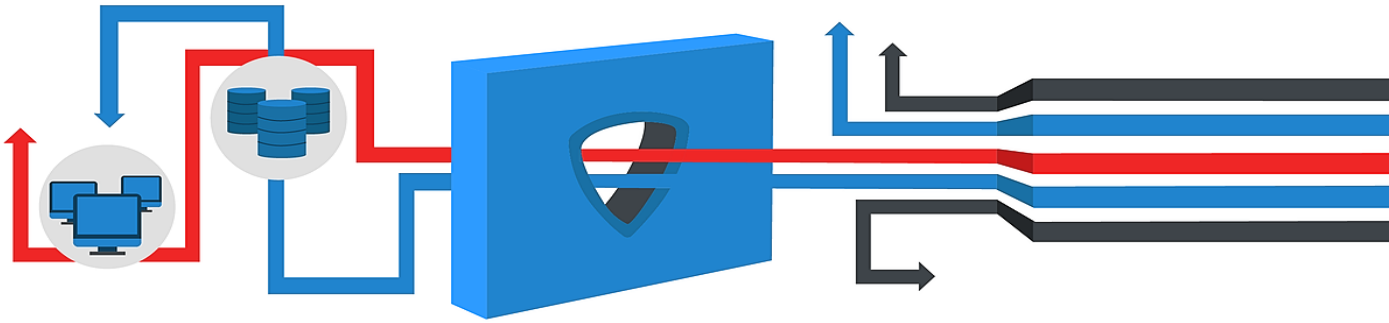
The Internet of Things is the network of devices such as vehicles and home appliances containing electronics, software and sensors that allow these things to connect, interact and exchange data. Ethical hackers identify vulnerabilities within IoT infrastructures that could potentially lead to a data breach – or worse.

Wireless Network Penetration Test

A Wireless Network Penetration Test simulates attacks on an organization's wireless network in a scenario where the hacker is within the range of the wireless network.

New Technology Test

As technology continues to churn out new gadgets and gizmos, there are more things to test. Remember, anything that is connected to your organization's network can exchange information with it. And if it can exchange information, it can be hacked, compromised, and leveraged to gain more unauthorized access in your organization.



How to Pick a Penetration Testing Company

Penetration testing is one of the best ways to assess cybersecurity defenses. But managing these penetration tests is a process that you need to get right in order to best reap its benefits. It is important to select a team with:

- **Deep experience in your specific industry**
- **A plan to keep your data secure during testing**
- **Methodologies based on industry best practices**
- **Sample reports for your review**

Key Considerations to Pick a Pen Test Team

Selecting the right team to perform penetration tests is a main determinant of the success or failure of your endeavor. If you're planning to co-source the penetration test, make sure that you include at least two external cybersecurity experts on the penetration testing team. An independent, external opinion is vital to help you avoid blind spots.

When selecting external vendors keep the following tips in mind:

Evaluate the credentials, experience, and expertise of the external vendor as a company but also evaluate each member of the penetration testing team. Each team member should have experience in a wide range of industry verticals and organizations of all sizes.

Understand how penetration testers will keep your data secure during and after the test. Identify and agree upon how confidential data will be transmitted, where will it be stored, and when and how will it be destroyed.

Review the methodology that will be used by your vendor. The methodology needs to be based on industry best practices and must include both automated and manual test methods.

Ask your vendor for sample reports. Evaluate if the reports are clear, easy to understand, and include risk-prioritized recommendations.

Ensure your vendor offers re-test options to validate your remediation efforts. Re-testing is critical in continuous penetration testing process.

A good penetration testing report will typically include:

- An executive summary highlighting the organization's overall security posture.
- A technical section describing activities performed to identify vulnerabilities in the target systems.
- A list of findings and recommendations.
- Appendices showing real test outputs, exploitations, screenshots, and other data related to vulnerabilities detected.

The importance of regulatory expertise

The team of cybersecurity experts that supports your penetration testing efforts must have an encyclopedic knowledge of cybersecurity regulatory requirements.

The team should be able to clearly and accurately interpret those regulatory requirements in the context of the penetration testing project. The penetration testing team should perform very targeted social engineering tests tailored to the specific risk situations and compliance considerations of the organization.

Keep in mind: Companies that are breached can pay high fines to regulatory bodies and credit card brands if it is discovered that they weren't compliant.

How to Get the Most Value Out of Pen Testing

After you've selected the right team to conduct your penetration testing, half the battle is won. The other half? You must ensure rigorous testing and remediation.

Tips for testing success

On the technical side of things, to get the most out of penetration testing be sure:

- Tests are intense, hardcore, and utilize the latest and greatest attack techniques. Hit yourself with everything you've got. Don't hold back. Remember, hackers won't hold back either.
- New technologies and IT infrastructure elements are in the scope of your penetration tests. The rule of thumb is – if it can connect to your network, it's in scope.
- Penetration tests are performed in a manner that avoids adverse impacts. A good vendor will have reviewed the organization's network diagram in advance to understand what types and bursts of attacks the infrastructure can withstand without killing operations.
- Your incident response team conducts monitoring during tests. That way, the incident response team gains an almost real-world live hack attack experience.
- Once the penetration tests are complete, remediation of the vulnerabilities identified is crucial. Make sure you diligently allocate each identified vulnerability to be remediated to a specific, accountable individual, along with a specific timeline on when the vulnerability will be remediated.

Social Engineering Tests Human Vulnerabilities

In cybersecurity, the human element is often known as the "weakest link." Your organization could have the latest, state-of-the-art cybersecurity defenses in place, but it would all count for nothing if just one employee is coerced into revealing sensitive organizational information. Social engineering assessments test weaknesses in human nature. They are critically important because employees are the first line of defense against cyberattacks.

What is Social Engineering?

Social engineering assessments emulate the coercion and manipulative techniques hackers use to trick employees into unwittingly breaching an organization's cyber defenses. The assessments help organizations identify human vulnerabilities so they can be remediated through training and improvement in the level of cybersecurity awareness among employees.

The training addresses specific weaknesses so organizations can shore up defenses. Customized Security Awareness Training generates maximum ROI by focusing on areas where each employee is weak rather than relying on a one-size-fits-all approach.

How Social Engineering Testing Helps

After ethical hackers deploy common forms of attacks on employees, organizations should follow up with Security Awareness Training that educates employees, so they are less likely to fall victim to a hacker.

For example, an employee who is prone to clicking potentially malicious links in emails can be provided with customized phishing awareness training. An employee who often allows other folks to "piggyback" into secure premises would be a prime candidate for physical security awareness training.

Types of Social Engineering Attacks

The techniques that can be used in a social engineering assessment are only limited by imagination and creativity.

Here are some common types of social engineering attacks:

Phishing

Phishing is when attackers use emails, social media, instant messaging, or SMS to trick victims into divulging sensitive information or clicking on malicious links. Phishing emails are crafted to create a sense of urgency to get the victim to act.

Vishing

Vishing is a social engineering attack that tricks victims into divulging personal or sensitive information over the phone. Attackers will typically spoof their caller ID to make it appear calls are coming from a legitimate source, such as the IRS. The attacker then threatens adverse action if the victim doesn't provide a payment and key in credit card details.

Spear Phishing

Spear phishing attacks target a specific person, business, or organization. The cybercriminals research their targets and then craft tailored attacks to trick victims into thinking they are receiving, for example, a legitimate wire request from a colleague or client. The tailoring and customization involved in spear phishing brings higher success rates for attackers.

Smishing

That's short for "SMS phishing" – a social engineering attack that hackers use to target victims on their phones via SMS. This technique is essentially phishing but carried out over text (SMS) messages. Just like email phishing scams, the SMS will typically have a malicious link that, when clicked, downloads malware onto the device or leads the victim to a page that attempts to steal her/his credentials.

Baiting

In this technique, attackers use "bait" to lure victims. The bait could be USB pen drives, CDs, DVDs, and so on. First, the attacker gains access to the victims' workplace to place the bait in strategic locations where a victim is most likely to fall for it. For instance, the attacker may leave on a cafeteria table a CD that says "Layoffs – Employee List." A curious employee who comes across the CD would likely insert the CD in a computer, allowing malware on the CD to spread into the organization's technical infrastructure.

Tailgating

In tailgating, an attacker tries to enter a secure area that requires an access card. The attacker typically waits for someone with an authorized access card to come along and then manipulates the person into believing that s/he mistakenly left her/his access card inside. The person with the access card might then help the attacker gain unauthorized access to a secure area. With tailgating, attackers try to exploit the helpfulness in human nature.

Effective Security Awareness Training

Penetration testing is a great tool. But if an organization doesn't follow up to address the human - as well as technical - vulnerabilities exposed by penetration testing, hackers will still find their way in. Remember: Employees are an organization's first line of defense against cyberattacks. It it's imperative that they be cyber-aware.

Looking back at the massive data breaches of the past, it is clear that cyberattacks are disruptions that can bring even the biggest and best businesses to a standstill. It would be fair to say that a number of these data breaches could have been avoided or minimized, if there was a better or different approach to cybersecurity awareness training.

While most organizations provide cybersecurity awareness training to employees, the results and outcomes are sometimes far from desirable. Most employees do not view cybersecurity as part of their job. Organization's perpetuate this perception when they treat Security Awareness Training as just another box to be checked off on a compliance checklist via annual training.

Key Elements of an Effective Security Awareness Training Program

Analyze the organization's current program by observing the level of resources and support available to the program, the regulatory compliance requirements that are covered, and whether the program incorporates industry best practices and standards.

- Develop a security awareness program that strives to change the behaviors of individuals, which, in turn, bolsters the security culture. Top management must regularly reinforce the message to employees that cybersecurity is at the core of the organization's success.

Ensure that the content of a Security Awareness Training program is diverse, engaging, and to-the-point. Remember that you're trying to reach, not preach.

Use a combination of training methods, such as engaging videos, animations, games and interactive content.

Consider adding a competitive element into the mix.

Maintain and regularly update your program because awareness is a continuous process. A number of hacker techniques and protection methods in use today will be obsolete a year from now, if not sooner. Update your cybersecurity awareness training program at least once a year or whenever there is a significant technical or operational change at your organization.

Measure the effectiveness of your cybersecurity awareness training program on an ongoing basis. Gather key performance metrics and indicators to gauge the effectiveness of the program and incorporate lessons learned to update it.

Visit: https://ermprotect.com/security-awareness-training

ermprotect.com | info@ermprotect.com | 305.447.6750