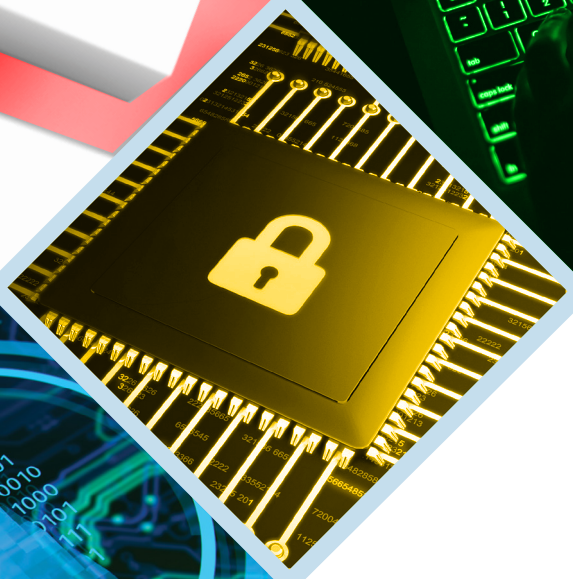
ERMProtect
Cybersecurity Solutions



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 simulates real-world cyberattacks to evaluate the security of systems and information resources. Security consultants adopt a hacker's mindset, asking: How would attackers strike? When? Through which entry point? They launch controlled attacks to uncover vulnerabilities, document how they gained access, and provide actionable recommendations to strengthen defenses.

Why is Penetration Testing Needed?

Hackers have the advantage of surprise, stealth, and persistence. They can choose to retreat and strike again at will. Organizations, on the other hand, must defend against attacks from any direction, at any time.

Penetration testing, though, offers organizations a way to prepare and fight back. Rather than waiting for a breach, they engage in **adversary simulation** to identify vulnerabilities and measure resilience. By emulating hacker tactics, penetration tests reveal weaknesses in technical infrastructure and provide actionable insights to strengthen security before an actual attack occurs.

© 2026 ERMProtect. All rights reserved.

305-447-6750 | info@ermprotect.com

What are Phases of Penetration Testing?

Penetration testing methodologies may differ, but there are typically five phases that ensure the testing is robust, thorough, methodical, and effective.

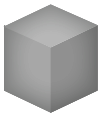
1 The Pre-engagement & Scoping Phase

The planning stage involves agreeing on the scope and method of testing. In some scenarios, ethical hackers are provided with advanced information about IT security systems while in others, they are told absolutely nothing.

There are three approaches:

The "white box/full-knowledge" penetration test is where the tester is given all information about the information resource being attacked. These tests may be more comprehensive and unearth more vulnerabilities since the "attacker" has so much advanced information about the target.

The "black box/zero-knowledge" penetration test is exactly the reverse – the tester is given no information about the information resource being attacked. These tests offer a more "real world" scenario in which the malicious hacker has no advanced knowledge about the organization's technical infrastructure.



The "grey box/partial knowledge" penetration test is a middle ground in which the tester is given some information. These tests are often the best route to take since malicious hackers are bound to have gathered at least some information about their target.

2 The Reconnaissance Phase

In the reconnaissance stage, the ethical hacker gathers as much data and intelligence as possible about the target before launching attacks. Data collected may include IP addresses, domain details, mail servers, network topology, applications, people etc.

3 The Intrusion/Exploitation Phase

During the intrusion stage, the ethical hacker performs active scans and probes to break into the information resource, whether that be a network, a file, or a cloud service. The goal is to exploit vulnerabilities and demonstrate real-world impact, such as obtaining administrative access to a sensitive interface.

4 The Reporting Phase

When complete, the results of the penetration test are compiled into a report with detailed information about specific vulnerabilities and detailed instructions on how to remediate. The reports include "Risk Scoring" (like CVSS - Common Vulnerability Scoring System) showing a prioritized list of vulnerabilities based on the danger they pose.

5 The Remediation & Validation Phase

Finally, in post-remediation, the team re-tests the findings to confirm vulnerabilities have been fixed and ensure no new gaps were introduced during remediation.

© 2026 ERMProtect. All rights reserved.

305-447-6750 | info@ermprotect.com

What are Types of Pen Tests?

Network Penetration Test

A Network Penetration Test simulates cyberattacks targeting an organization's network to identify vulnerabilities. An External Network Test emulates attacks from outside the organization, assessing how well external defenses protect against unauthorized access. An Internal Network Test simulates attacks from within the organization, evaluating risks posed by insiders or compromised internal systems. Both tests provide critical insights into the strength of network security and help organizations safeguard sensitive information.

Web Application & API Penetration Test

Web applications, such as online banking and e-commerce, are prime targets because they process sensitive transactions and are globally accessible. A Web Application Penetration Test identifies and fixes vulnerabilities before exploitation. It also includes API security testing, as APIs often provide direct access to critical systems and are frequently overlooked, making them a high-risk entry point. (API security involves protecting the integrity, confidentiality, and availability of application programming interfaces (APIs) by managing authentication, authorization, and data encryption to prevent unauthorized access and breaches.)

Cloud Infrastructure Penetration Test

Cloud infrastructure tests uncover vulnerabilities, misconfigurations, and implementation flaws in the cloud environment. A Cloud Infrastructure Penetration Test can target publicly accessible systems or private systems. Tests require prior approval from the provider, though major platforms like AWS and Azure generally permit most security assessments without notification if their policies and guidelines are followed.

ICS/SCADA & Operational Technology (OT) Penetration Test

ICS/SCADA Penetration Tests assess Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) environments. Industrial Control Systems are specialized, integrated hardware and software configurations that monitor and automate industrial processes such as manufacturing, energy, and water treatment. These penetration tests align with the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards and focus on airgap validation, determining if attackers can pivot from corporate IT to control networks. They require specialized expertise and deep experience in ICS security testing.

Social Engineering Test

Social engineering attacks trick users into installing malware or revealing sensitive information. These tests gauge how well employees protect organizational data. Ethical hackers may send phishing emails, impersonate technical support, or use AI-generated voice/video calls posing as management to see if employees click through and expose critical information.

© 2026 ERMProtect. All rights reserved.

305-447-6750 | info@ermprotect.com

PCI Penetration Test

PCI DSS 4.0.1, a security standard designed to protect credit card data, requires organizations to conduct comprehensive infrastructure penetration tests. These ongoing and periodic tests align with specific PCI DSS requirements, helping organizations maintain compliance and protect cardholder data.

Mobile Application Penetration Test

Mobile applications are integral to daily life, but they also create new attack vectors. A Mobile Application Penetration Test allows organizations to assess their mobile application infrastructure (specifically the Android and iOS ecosystem and backend security).

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 regulations, such as GLBA, HIPAA, GDPR, and others, require ongoing penetration tests of systems storing sensitive data. Regulatory Compliance Penetration Tests are tailored to meet specific requirements of each applicable law, helping organizations achieve and maintain compliance.

IoT Penetration Test

The Internet of Things is the network of devices (such as vehicles and home appliances) that contain electronics, software and sensors allowing them to connect, interact and exchange data. Ethical hackers identify vulnerabilities within IoT infrastructures that could potentially have consequences.

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 brings new products to market, there are more things to test. Anything that is connected to your organization's network can be hacked, compromised, and leveraged to gain more unauthorized access in your organization.

AI/ML Penetration Test

Many organizations now integrate AI into their business processes. Unlike traditional software, AI is non-deterministic, so the same input could fetch different outputs. Penetration testing of AI systems involves testing the AI logic to manipulate its safety guardrails and manipulating the input data to train AI into giving malicious output to see if any sensitive information can be leaked.

© 2026 ERMProtect. All rights reserved.

305-447-6750 | info@ermprotect.com

How to Pick a Penetration Testing Company

Penetration testing is one of the best ways to assess cybersecurity defenses, but it is crucial to get it right to 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
- **A commitment** to re-test

Key Considerations to Pick a Pen Test Team

Selecting the right team is critical to the success of your penetration testing program. If co-sourcing, include at least two external cybersecurity experts to provide independent perspectives and avoid blind spots.

When selecting external vendors and/or candidates keep the following tips in mind:

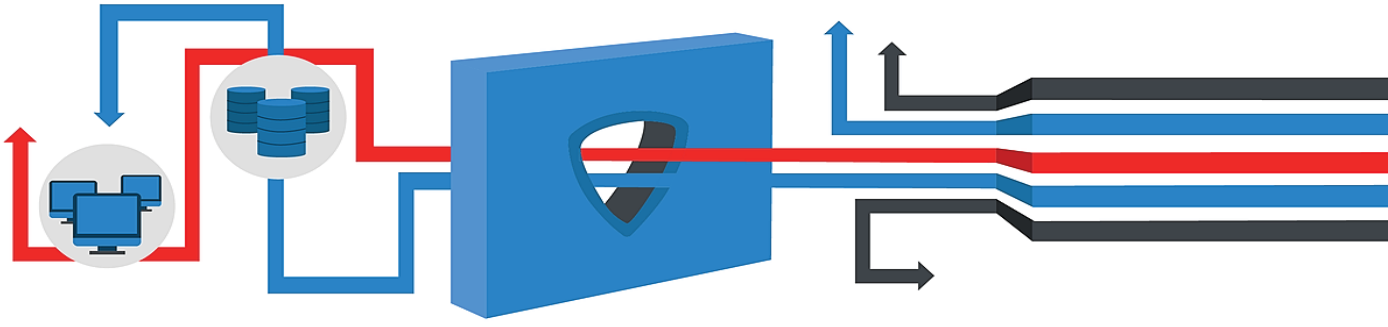
- **Evaluate** both the vendor and individual team members. Each tester should have experience across diverse industries and organizations of varying sizes.
- **Understand** how testers will protect your data during and after the engagement. Define how confidential data will be transmitted, stored, and destroyed.
- **Review the methodology** to ensure it follows industry best practices and includes both automated and manual techniques.
- **Review sample reports** for clarity and actionable insights. A strong report typically includes:
  - **Executive summary** of overall security posture
  - **Technical details** of testing activities
  - **Risk-prioritized findings and recommendations**
  - **Appendices** with real outputs, screenshots, and exploit evidence

Ensure the vendor offers re-testing to validate remediation efforts — an essential step in continuous testing.

The Importance of Regulatory Expertise

Your penetration testing team must have an encyclopedic knowledge of cybersecurity regulatory requirements and should be able to accurately interpret regulatory requirements in the context of a penetration testing project. Importantly, the team should be able to view regulatory requirements with the lens of business impact and profitability.

The penetration testing team should also perform targeted social engineering tests tailored to the specific risk and compliance considerations of the organization. Non-compliance can lead to severe fines from regulatory bodies and credit card brands after a breach.



© 2026 ERMProtect. All rights reserved.

305-447-6750 | info@ermprotect.com

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

Technical best practices for penetration testing:

- **Use Advanced Techniques:** Tests should be rigorous and leverage the latest attack methods. Hackers won't hold back, so neither should you.
- **Include All Connected Systems:** If it can connect to your network, it's in scope.
- **Avoid Operational Disruption:** Vendors should review network diagrams to ensure tests don't impact critical operations.
- **Engage Incident Response:** Monitor tests in real time to simulate a live attack scenario.
- **Prioritize Remediation:** Assign each vulnerability to an accountable owner with a clear timeline. Faster closure of critical attack paths equals greater resilience — the ultimate goal of penetration testing.

Social Engineering Tests Human Vulnerabilities

In cybersecurity, the human element is often considered the "weakest link." Even with the latest cybersecurity defenses in place, your organization could be at risk if just one employee reveals sensitive company 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 manipulative techniques hackers use to trick employees into unknowingly breaching an organization's cyber defenses. These assessments help organizations identify human vulnerabilities. The insights gained drive targeted training to strengthen cybersecurity awareness and address specific weaknesses. Customized Security Awareness Training delivers maximum ROI by focusing on individual gaps rather than using a one-size-fits-all approach.

How Social Engineering Testing Helps

After ethical hackers deploy common forms of attacks on employees, organizations 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 others to "piggyback" into secure premises would be a prime candidate for physical security awareness training.

© 2026 ERMProtect. All rights reserved.

305-447-6750 | info@ermprotect.com

Types of Social Engineering Attacks

Here are some common types of social engineering attacks / tests:

Phishing: Attackers use email, social media, messaging, or SMS to trick victims into revealing sensitive data or clicking malicious links. Modern phishing leverages AI for hyper-personalized, error-free messages and thread hijacking, where attackers reply within real email conversations to appear legitimate.

Vishing: Voice-based attacks where callers spoof identities (e.g., IRS) and pressure victims for payment or credentials. AI voice cloning now enables attackers to mimic executives with just seconds of audio, bypassing security and authorizing fraudulent actions.

Spear Phishing: Highly targeted attacks using detailed research to impersonate trusted contacts, often for wire transfers or credential theft.

QR Code Phishing: Malicious links replaced with QR codes in emails or posters, tricking users into scanning with personal devices lacking corporate security.

Smishing: SMS-based phishing that delivers malicious links via text, leading to malware downloads or credential theft.

Digital & Physical Baiting: Attackers plant infected USBs or CDs in workplaces or offer fake "free" AI tools and premium reports online. Once accessed, malware or infostealers compromise systems.

Tailgating: Exploiting human helpfulness, attackers follow authorized personnel into secure areas by pretending to have forgotten their access card.

Effective Security Awareness Training

Penetration testing is a great tool, but if an organization does not address the human, as well as technical, vulnerabilities exposed by penetration testing, hackers may still be successful. Because employees are an organization's first line of defense, it is imperative that they be cyber-aware.

The Human Factor in Data Breaches

Major data breaches show clearly that cyberattacks can bring any business to a halt. A better approach to cybersecurity awareness training could significantly reduce these incidents.

While most organizations offer training, results often fall short because many non-technical employees don't see cybersecurity as part of their role. This perception is reinforced when companies treat Security Awareness Training as a compliance checkbox, delivering generic, annual sessions instead of meaningful, ongoing education.

© 2026 ERMProtect. All rights reserved.

305-447-6750 | info@ermprotect.com

Key Elements of an Effective Security Awareness Training Program

- **Analyze the organization's current program** by reviewing resources, compliance coverage, and alignment with industry best practices.
- **Develop a security awareness program** that strengthens security culture. Leadership should reinforce that cybersecurity is critical to business success.
- **Ensure that the content** of a Security Awareness Training program is diverse, engaging, and to-the-point. Keep training interactive and role specific.
- **Use a combination of training methods**, such as engaging videos, animations, games and interactive content. Add competitive elements and ensure mobile-friendly access.
- **Maintain and regularly update your program** at least annually or after major technical/operational changes. Cyber threats evolve quickly.
- **Measure the effectiveness** of your cybersecurity awareness training program on an ongoing basis beyond completion rates. Track metrics like mean time to report suspicious events, resilience ratio (employees reporting simulations), and reoccurrence rate (repeat errors by individuals/departments).

© 2026 ERMProtect. All rights reserved.

305-447-6750 | info@ermprotect.com

ERMProtect
Cybersecurity Solutions

800 S. Douglas Rd. Suite 940
Coral Gables, FL 33134

305-447-6750

info@ermprotect.com

ermprotect.com

Proven Protection.
Peace of Mind.