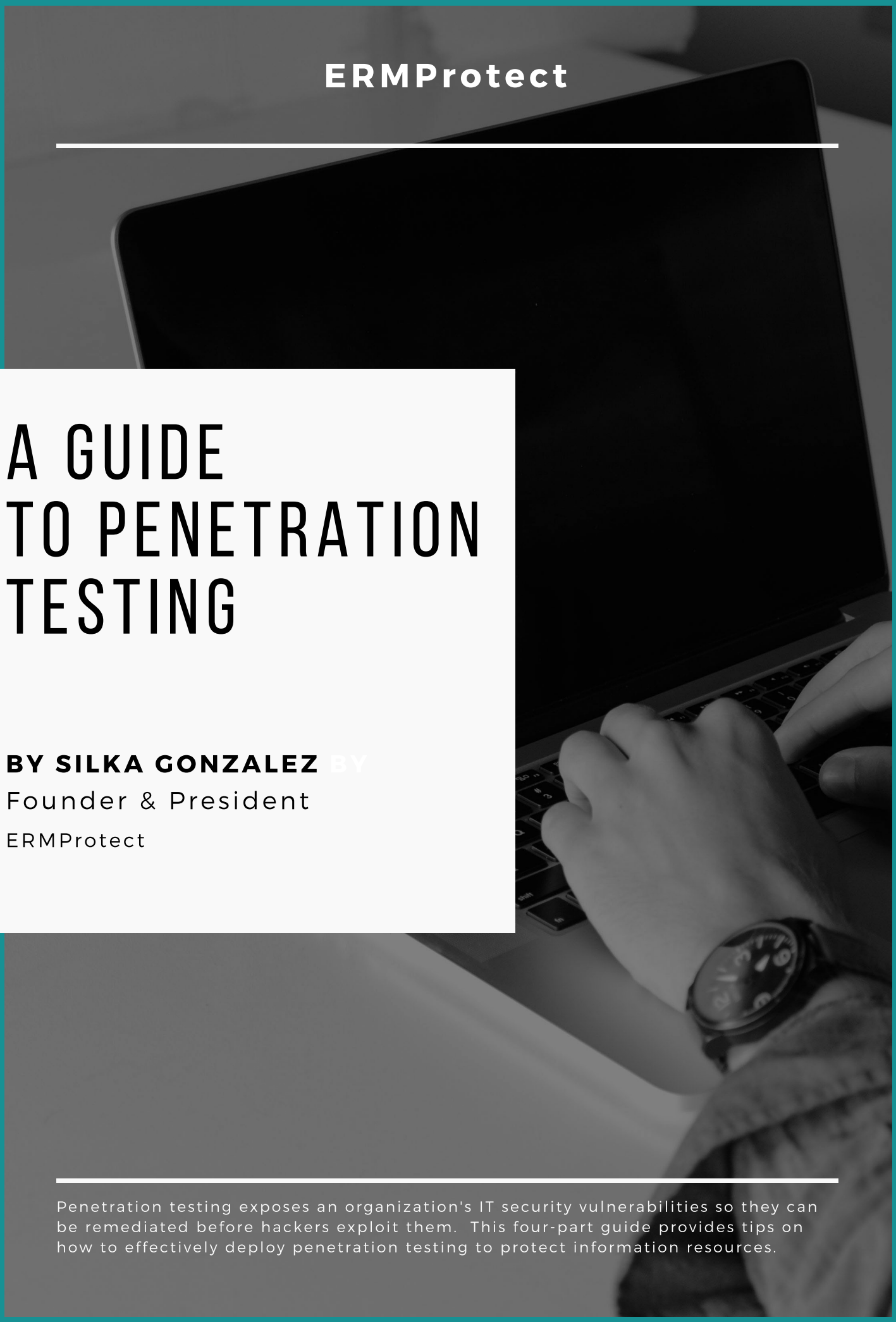
ERMProtect



A GUIDE TO PENETRATION TESTING

BY SILKA GONZALEZ BY
Founder & President
ERMProtect

Penetration testing exposes an organization's IT security vulnerabilities so they can be remediated before hackers exploit them. This four-part guide provides tips on how to effectively deploy penetration testing to protect information resources.

HOW ETHICAL HACKERS HELP ORGANIZATIONS IDENTIFY THEIR CYBER VULNERABILITIES

To know your enemy, you must become your enemy. – Sun Tzu

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.

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 a hacker attacked, what method would they use? What time would they attack? What entry point would they use? Cyber experts answer these questions by hacking organizations,then revealing how they got inside and recommending fixes to exploited loopholes.

Penetration Testing Phases

While the methodology of penetration testing differs for every ethical hacker, there are, broadly, five phases:

1. Planning
2. Reconnaissance
3. Intrusion
4. Reporting
5. Re-testing

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

Next, in the reconnaissance stage, the ethical hacker gathers as much data and intelligence as possible about the target before launching any attacks. The collected data

include IP addresses, domain details, mail servers, network topology, systems, applications, people etc.

During the intrusion state, 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 "attacker" actively looks for openings into the information resource in order to exploit and compromise it.

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 them to secure the information resource.

Finally, post-remediation, the team re-tests the findings to validate that gaps and vulnerabilities were fixed.

Types of Penetration Tests

There are different approaches to performing a penetration test. The white box penetration test is where the tester is given all information about the information resource being attacked. The black box penetration test is exactly the reverse – the tester is given no information about the information resource being attacked.

The grey box penetration test is a "middle ground" wherein the tester is given some information.

There are also various types of penetration tests that can be performed:

- Network Penetration Testing
- Web Application Penetration Testing
- Social Engineering Testing
- Wireless Network Penetration Testing
- Mobile Application Penetration Testing
- Regulatory Compliance Penetration Testing
- Application Penetration Testing
- Cloud Infrastructure Penetration Testing
- ICS/SCADA Penetration Testing
- PCI Penetration Testing
- Physical Site Penetration Testing
- IoT Penetration Testing

This is a generic list. 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.

UNDERSTANDING THE TYPES OF PEN TESTS

Different kinds of penetration tests work in different ways. The needs and goals vary from organization to organization depending on factors such as infrastructure, industry vertical, risk, supply chain ecosystem, and more.

Let's dive in to the details:

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.

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.

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.

Wireless Network Penetration Test

Life without "Wi-Fi" is almost unimaginable today. 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.

Regulatory Compliance Penetration Testing

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.

Cloud Infrastructure Penetration Testing

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 Testing

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.

PCI Penetration Testing

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.

Physical Site Penetration Testing

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.

IoT Penetration Testing

The Internet of Things is the network of devices such as vehicles and home appliances that contain 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.

HOW TO PLAN AND MANAGE VULNERABILITY TESTING FOR MAXIMUM GAIN

Penetration testing is one of the best ways to assess cybersecurity defenses, identifying weaknesses and poorly protected entry routes so organizations can fix the chinks in their armor. But managing these penetration tests is a process that organizations need to get right in order to best reap its benefits. The most significant questions to address are:

(1) How to select the right cybersecurity experts to perform the penetration tests?
(2) How to manage the penetration test from start to finish?

Key Considerations to Pick a Team

Selecting the right team to perform the penetration tests is a critical piece of the puzzle and is arguably the 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 and/or candidates keep the following tips in mind:

- Evaluate the credentials, experience, and expertise of the external vendor as a company but also perform the same evaluation of each member of the penetration testing team. Be sure each team member has experience in a wide range of industry verticals as well as organizations of all sizes.

- Penetration testers are certainly going to get access to your confidential data so check how the vendor keeps 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 it will 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 and evaluate if the reports are clear, easy to understand, and include risk-prioritized recommendations. A good penetration testing report will typically include:
  - An executive summary highlighting the organization's overall security posture;
  - A technical section describing the 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.

- Make sure your vendor offers re-test options to validate your remediation efforts. Retesting is critical in a continuous penetration testing process.

Regulatory expertise is critical

Another key consideration for organizations performing penetration tests is regulatory compliance. 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 following the rules.

Most importantly, the team should be able to view regulatory requirements in light of business impact and profitability, so your organization can grow and prosper. ◆

SHORE UP HUMAN VULNERABILITIES, NOT JUST TECHNICAL ONES, TO PREVENT DATA BREACHES

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, remediate and, remember to address the human vulnerabilities exposed by testing.

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 during non-production hours to avoid adverse impacts. A good vendor should already know after looking at the organization's network diagram, 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 by a specific, accountable individual, along with a specific timeline on when the vulnerability will be remediated.

Address human vulnerabilities

While penetration testing is a great tool, if an organization doesn't follow up to deal with the human, as well as technical vulnerabilities, exposed by penetration testing, hackers will still find their way in.

Employees are your first line of defense and it's imperative that they

be cyber-aware. Organizations invest in state-of-the art security technologies only for an employee to inadvertently bypass all the protections in place and cause a data breach. Technology alone will not solve the issue.

To illustrate the problem:

- 50 percent of Internet users receive at least one phishing email per day.
- Nearly 75 percent of Internet users would download a potentially malicious file because they lack the "cyber-savviness" they need to spot dangers online.
- More than 50 percent of enterprise data breaches are caused by negligent employees, contractors and third-party vendors.

It should be no surprise then, that some of the biggest data breaches known to date were caused by phishing attacks or social engineering. For example, the data of 145 million eBay customers was comprised when a hacker used a phishing attack to steal employee credentials. And the data of 80 million Anthem customers was exposed by a social engineering attack.

Despite these sobering statistics, only 45 percent of organizations provide employees with mandatory security awareness training. Nearly all the training occurs when an employee joins an organization and is not repeated – a sign that organizations are doing the bare minimum in terms of cybersecurity awareness training.

So, at the conclusion of your testing, the next step should be to develop a Security Awareness Training Program that teaches employees how to recognize and avoid hacker lures. Don't make the mistake of addressing only the technical issues unveiled by penetration testing. Instead, develop engaging, monthly and measurable training that makes employees "street smart" when it comes to recognizing new tricks and techniques that hackers will employ.

Final Words

To see examples of Cyber Security Awareness Training modules, please visit our website at ermprotect.com or our YouTube channel. For more information about penetration testing, visit our Services page or Blog.

◆