What is Penetration Testing?

An Introduction for IT Managers
What Is Penetration Testing?

Penetration testing is the process of identifying security gaps in your IT infrastructure by mimicking an attacker. Think about it as quality assurance for your IT security.

Like most people, you probably think that quality assurance for software is both sensible and necessary before you roll out software into production. It’s sensible not because you don’t trust the software developers to do a good job, but because it’s good business practice to ensure that the code works as expected. It verifies that your production systems are secure.

Some penetration testers prefer the term “security assessment” over “penetration testing,” although they relate to the exact same process. Penetration testers are sometimes called the Red Team, a term that comes from the early days of penetration testing in the military, whereas the Blue Team is the defensive team.

If you wonder how penetration testing relates to port scanning and vulnerability management, you’re not alone. Although they are related, they are quite different:

- **Port scanning** identifies active services on hosts.
- **Vulnerability management** identifies potential vulnerabilities on systems based on the installed software version of the operating system or applications.
- **Penetration testing** involves trying to take control over the systems and obtain data.

The differences between the three are easier to understand if you think of your network as a house:

- **Port scanning** is like counting the doors and windows on the house.
- **Vulnerability management** is like walking around the house and lists all the doors, windows and locks that are reportedly insecure based on the vendor and model information.
- **Penetration testing** is like trying to break into the house by picking the weak locks and smashing a window.

Why Penetration Test?

People conduct penetration tests for a number of different reasons:

- **Prevent data breaches**: Since a penetration test is a benign way to simulate an attack on the network, you can learn whether and how you are exposed. It’s a fire drill to ensure you’re optimally prepared if there’s ever a real fire.

- **Check security controls**: You probably have a number of security measures in place in your network already, such as firewalls, encryption, DLP, and IDS/IPS. Penetration tests enable you to test if your defenses are working—both the systems and your teams.

- **Ensure the security of new applications**: When you roll out a new application, whether hosted by you or a SaaS provider, it makes sense to conduct a security assessment before the roll-out, especially if the applications handle sensitive data. Some example applications includes customer relationship management (CRM), marketing automation program (MAP), HR’s applicant tracking system, health insurance providers’ benefits management software, et cetera.
• Get a baseline on your security program: New CISOs often conduct a security assessment when they join a new company to obtain a gap analysis of the security program. This shows them how effective the organization is in dealing with cyber-attacks. These security assessments are sometimes conducted without the knowledge of the IT security team because it could otherwise influence the results.

• Compliance: Some regulations, such as PCI DSS, require penetration tests. Make sure you understand how the penetration test should be conducted to ensure that you will pass the audit.

How to conduct a Security Assessment: Typical steps

Every penetration tester has a slightly different method, and similarly each security assessment is different depending on the environment and goals. That said, this graphic illustrates the typical steps of a security assessment:

A typical penetration test goes through these stages:

1. **Goal:** Setting the objective of the security assessment.

2. **Reconnaissance:** Finding out as much as possible about the target company and the systems being audited. This occurs both online and offline.

3. **Discovery:** Port or vulnerability scanning of the IP ranges in question to learn more about the environment.

4. **Exploitation:** Using the knowledge of vulnerabilities and systems to exploit systems to gain access, either at the operating system or application level.

5. **Brute forcing:** Testing all systems for weak passwords and gaining access if they do.
6. **Social engineering**: Exploiting people through phishing emails, malicious USB sticks, phone conversations, and other methods to gain access to information and systems.

7. **Taking Control**: Accessing data on the machine, such as passwords, password hashes, screenshots, files, installing keyloggers, and taking over the screen control. Often this can open new doors to more exploitation, brute forcing, and social engineering.

8. **Pivoting**: Jumping to different network segments, providing the host has multiple network interfaces, such as some machines in the DMZ.

9. **Gathering Evidence**: Collecting screenshots, passwords hashes, files as proof that you got in.

10. **Reporting**: Generating a report about how the penetration tester was able to breach the network and the information they were able to access.

11. **Remediation**: Addressing the issues that enabled the penetration tester to enter the network. This is typically not done by the penetration tester but by other resources in the IT department.

### Setting the Scope of a Penetration Test

Asking a penetration tester simply to “try and break in” is not necessarily a good way to frame a penetration test. Before you start, ask yourself this question: What is the most important digital asset that your company needs to protect? If you are in retail, it may be the database that stores all of your customers’ credit card numbers. If you are a software vendor, it may be your source code. If you are a bank, it may be your online banking application. You get the idea.

Once you’ve identified your most precious asset, instruct the penetration tester to try to access those systems. This will make the engagement much more impactful and realistic, providing you with a real learning experience and a clear indicator of whether the penetration tester has achieved his or her goal.

If you are conducting a penetration test for compliance reasons, such as PCI DSS, then the goal should be to access the systems inside the PCI scope to extract cardholder data.

### External and Internal Security Assessments

Security assessments can be carried out from the perspective of an outsider who tries to attack the organization over the internet, or from the view of a malicious insider. These two approaches are called external and internal security assessments.

You should choose an external security assessment if you are worries about your organization getting attacked from the Internet. Most organizations start with an external penetration test.

An internal penetration test always assumes that you have internal network access. It can provide valuable insight if you are worried that a rogue employee could try to access data that they’re not authorized to view. However, its uses go much further: Internal penetration tests can also tell you how much damage an intruder could do if one of your
employees mistakenly opens an attachment on a phishing email, or how far a visitor to your site could get by plugging their laptop into the local network.

**Denial of Service Testing**

You may not only be worried about whether people can break into your network to steal information but also whether someone on the Internet could bring down your servers to disrupt your business. If you are running a large online retail store or an online banking site, a system outage could cost you millions.

Denial of service (DOS) testing should be carried out with ultimate care because the DOS modules are designed to bring services down. You should either try them out on a development system or choose to conduct the tests during times when a successful DOS attack would have minimal impact on your business.

**How to Safely Conduct Penetration Tests**

In the same way that you wouldn’t let just anyone work on your servers, you should ensure that the person carrying out a penetration test on your systems is qualified to do so. If you hire an external penetration tester, ask for references. If you are asking an internal resource to conduct a penetration test, you should ensure this individual has sufficient experience or received training.

Exploits talk to systems in a way that was never intended by the developers. However, many exploits are perfectly safe to use on a production system. The penetration testing software Metasploit automatically chooses only tested, safe exploits by default to avoid any issues with your production environment.

Some organizations restrict the penetration test to development systems that mimic the production systems. This is especially common when the production system is unstable or the risks of running an active penetration test are very high, such as conducting a security assessment on a nuclear power station. At the same time, this approach has some drawbacks. The production system will in most cases be slightly different from the development system, and these differences may be critical.

Especially when conducting an external security assessment, it can make sense to pull out all the stops from an engagement, because only then will a test reveal the true risks an organization faces every day from attacks over the internet.

**In-House and Outsourced Security Assessments**

Whether you want to do your security assessments in-house or outsource them depends on a number of factors. The first one is the size of your organization. Do you have enough work to employ a penetration tester full-time? If not, do you have a security professional who can take this task on as a part-time job? Given the right tools, such as Metasploit Pro, security professionals can quickly and easily get up to speed to conduct security assessments on your network.

Outsourcing may be the right decision if you only have one penetration test to carry out each year that wouldn’t justify the cost of a tool and the training for a particular individual. It may also be the right choice if you want a truly independent assessment of your network’s security. It may be a good idea to switch your external penetration tester once a year to get a fresh pair of eyes on the network. This doesn’t mean that you’ll have to switch companies, just that you’ll ask for a different consultant for the next engagement.

Some companies decide to run a hybrid model: They conduct monthly or quarterly penetration tests using a junior in-house resource to identify the low-hanging fruit, such as unpatched systems and weak passwords. It makes
sense to do this more often as these issues also carry a higher risk of a data breach. In addition, once a year these organizations call in a specialized penetration tester to go deeper into the systems to identify the more advanced security issues.

Compliance may also factor into your decision. PCI DSS requirement 11.3 requires an annual security assessment. You can either outsource it or do it internally; if you choose an internal security assessment, the penetration tester must be able to prove expertise in this area (e.g., training certification) and must be organizationally separate from the people managing the network that is being assessed.

How to select a penetration tester

Whether you’re looking to hire an internal penetration tester or a consultant, you should ensure that the person is well trained and highly trustworthy. For penetration testing consultants, you should ask for references and buy services from a reputable firm. For internal resources, conduct a background check and ask for references. Training may or may not be a good indicator of someone’s skills since many of the best people in this fast-moving industry are self-taught.

As part of their engagement, penetration testers may get access to data that they would ordinarily not be authorized to see, including intellectual property, credit card numbers, and human resources records. This is why trustworthiness is so important. However, this should not put you off from hiring a penetration tester because the alternative is worse: If you do not identify and fix the security issues on your network by hiring someone who is on your side, your most sensitive data will likely be accessed by someone who is not.
What is Metasploit?

Metasploit is the leading software used by penetration testers around the world. A collaboration between the open source community and Rapid7, Metasploit software helps security and IT professionals identify security issues, verify vulnerability mitigations, and manage expert-driven security assessments, providing true security risk intelligence. Capabilities include smart exploitation, password auditing, web application scanning, and social engineering. Teams can collaborate in Metasploit and present their findings in consolidated reports.

Metasploit editions range from a free edition to professional enterprise editions, all based on the Metasploit Framework, an open source software development kit with the world’s largest, public collection of quality-assured exploits. To learn more about Metasploit or for a free trial, visit www.rapid7.com/metasploit.

Additional Metasploit Use Cases

Apart from security assessments, Metasploit can also be used for other purposes:

- **Vulnerability Verification**: If you are using a vulnerability scanner, you may be overwhelmed by the number of vulnerabilities reported on your network. Usually restrained by tight resources, most IT teams don’t have the time to fix all of them. Metasploit enables IT teams to verify whether a vulnerability is posing a real risk or whether it can be disregarded. This greatly reduces the time for remediation and increases the overall security posture of your organization.

- **Password Auditing**: Most people know they should use strong passwords, yet a surprising number of data breaches involve issues with passwords, such as weak passwords or passwords shared across trust zones and accounts. Metasploit enables you to audit the passwords used on your network across a large number of services, not just for Windows accounts.

- **Measuring Security Awareness**: Phishing attacks can compromise the security of entire organizations. One effective countermeasure is security awareness training. With Metasploit’s social engineering module, organizations can send out phishing campaigns to their users to report metrics on user security awareness.

About Rapid7

Rapid7 is a leading provider of IT security risk management software. Its integrated vulnerability management and penetration testing products, Nexpose and Metasploit, and mobile risk management solution, Mobilisafe, enable defenders to gain contextual visibility and manage the risk associated with the IT environment, users and threats relevant to their organization. Rapid7’s simple and innovative solutions are used by more than 2,000 enterprises and government agencies in more than 65 countries, while the Company’s free products are downloaded more than one million times per year and enhanced by more than 175,000 members of its open source security community. Rapid7 has been recognized as one of the fastest growing security companies by Inc. Magazine and as a “Top Place to Work” by the Boston Globe. Its products are top rated by Gartner®, Forrester® and SC Magazine. The Company is backed by Bain Capital and Technology Crossover Ventures. For more information about Rapid7, please visit http://www.rapid7.com.