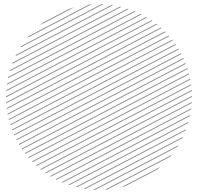
BEST PRACTICES
PENETRATION TESTING
GUIDE

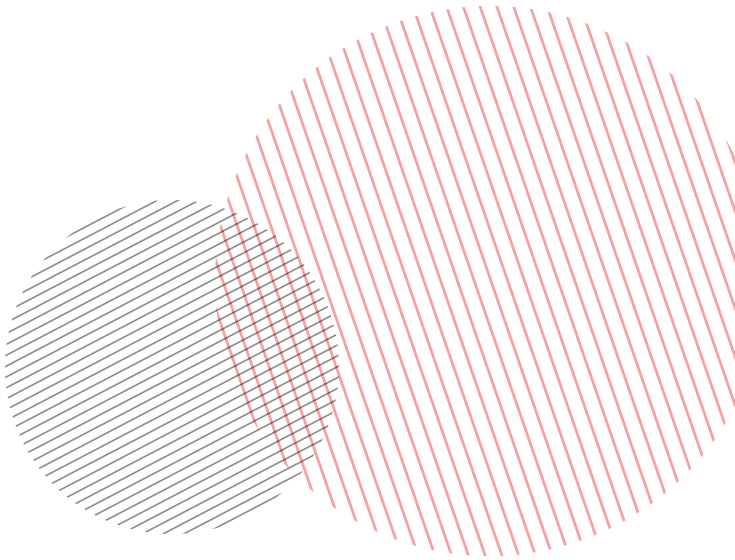
BEST PRACTICES GUIDE: PENETRATION TESTING

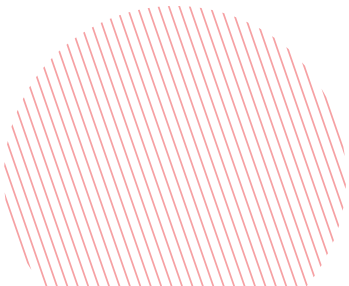
A straightforward guide to successful penetration testing for infrastructure and applications

If you are new to penetration testing or looking to refresh your knowledge, the information in this guide should help you to quickly understand the choices you have available. This guide was created by IT Security engineers with hands-on experience in performing and evaluating penetration testing services. By the end of this document you should understand the benefits of a penetration test and be confident about the next steps to make your organization's IT infrastructure and applications more secure.

Enjoy!







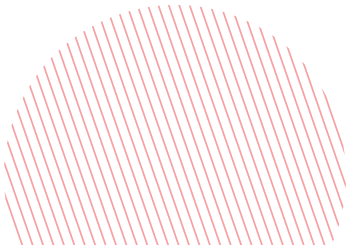
ABOUT NOPSEC UNIFIED VULNERABILITY RISK MANAGEMENT

NopSec was founded to pursue a vision: IT security and effective vulnerability management can be a business advantage.

NopSec is a cybersecurity technology company focused on helping businesses to proactively manage security vulnerability risks, make better security decisions, and effectively protect their IT environment from security breaches.

For many companies, keeping on top of IT security is a real tough job. Vulnerability discovery, analysis, and filtering processes can be lengthy, cumbersome, error prone and involve many manual tasks. Penetration testing is often the first step toward implementing an ongoing and proactive process to address vulnerability management.

Our flagship product, Unified VRM (Vulnerability Risk Management), is a cloud-based SaaS solution that enables vulnerability management for applications, infrastructure, and configurations that reside on premises and in the cloud. Unified VRM takes a holistic approach to finding, filtering, and fixing exploitable vulnerabilities. Our customers dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation. Streamlined reporting allows senior management to see progress being made against vulnerability risks on an ongoing basis. And our customers can help avoid potential financial losses and damage to their public reputation associated with a security breach.



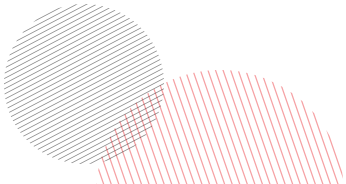


TABLE OF CONTENTS

BEST PRACTICES GUIDE PENETRATION TESTING

CHAPTER 1: INTRODUCTION TO PENETRATION TESTING

What is Penetration Testing?

Penetration testing is a critical component in an overall security strategy. The general definition is that penetration testing (sometimes referred to as pentesting) is a method of evaluating IT security by simulating an attack on computer systems, networks, or applications from external and internal threats. Trusted individuals actively attempt to exploit vulnerabilities and gain access to system resources without damaging or disrupting an organization's production services.

Why Perform Penetration Testing?

There are many reasons to conduct a penetration test. One obvious, and unfortunate, motivation for a penetration test is because you have been hacked and want to discover more about the exploitable vulnerabilities and threats to your systems. The outcome of a successful penetration test can reduce the risk of another hacker attack.

In some industries certain types of data and how the data is handled securely is strictly regulated. Examples of standards include the New York State Department of Financial Services Cybersecurity Regulations (23 NYCRR 500), Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and the Office of the Comptroller of the Currency (OCC) which supervises all national banks. Regulators commonly require a documented certification process, and penetration test results can serve that purpose. Often associated with regulated industries, if you are a product vendor your client may request that a penetration test be performed on their behalf.

The main objective of penetration testing is to determine IT security weaknesses. A penetration test can also be used to gauge an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents.

How is Penetration Testing Valuable?

Regardless of why you are performing a penetration test, the results can be valuable information for your organization. The adage, “any road looks good if you don't know where you're going” certainly holds true when it comes to an IT security strategy.

Your organization may be trying to address the challenges of the consumerization of IT and bring-your-own movements, the shift to cloud computing, and the need to protect the vast amount of data being generated on a continual basis. The business necessity of having Internet-facing applications means that there is no shortage of risks facing your IT infrastructure.

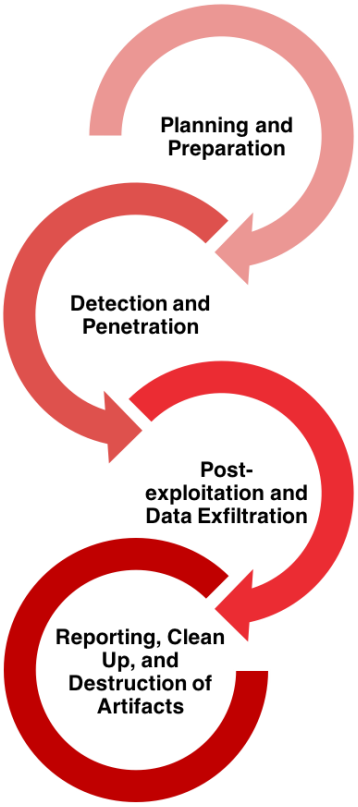
Penetration testing allows you to understand where you need to focus your attention by determining the feasibility of a particular set of attack vectors. A penetration test will identify high-risk vulnerabilities and may uncover vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software.

Penetration testing will determine if your organization is able to successfully detect and respond to hacker attacks. It will also help assess the magnitude of potential business and operational impacts should an attack occur. In addition to the benefits listed above, if you are in the role of protecting and maintaining infrastructure and applications for your company, penetration testing may provide the evidence to support increased investments in security personnel and technology.

Safeguarding your company's reputation, and your professional credibility, has proven to be one of the motivating factors for a proactive approach to IT security. Protecting sensitive internal data, sensitive customer data, and intellectual property is not just about peace of mind… it is a business imperative. Any publicity related to security concerns or breaches is bad for the reputation of a business and can also hurt the bottom line.

CHAPTER 2: PENETRATION TESTING METHODOLOGY

What are the Phases of Penetration Testing?



The process of penetration testing can be viewed as gathering information about the targets, identifying possible entry points, and attempting to exploit vulnerabilities. In order to make the penetration test a success, there are multiple phases that need to be completed including planning, the physical assessment, post-exploitation, and the reporting stage. Planning and Preparation Detection and Penetration Post-Exploitation and Data Exfiltration Reporting, Clean Up, and Destruction of Artifacts.

The first phase of a penetration test is planning and preparation which often includes a formal agreement that should specify the engagement team, the exact dates, times of the test, escalation path and other arrangements.

In the detection and penetration phase the penetration tester endeavors to attain a greater level of access to your information assets. When a potential entry point is identified, attempts are made to verify the validity of vulnerabilities by exploiting them.

During post-exploitation all possible exfiltration paths are documented. This allows you to identify where access has been achieved and the impact on sensitive data, configuration settings, communication channels, and relationships with other devices that can be used to gain further access to the network.

In the final phase you receive a report that contains detailed information on what vulnerabilities were found, samples of where they were found, what it means, and specifics on how to remediate the issues.

What Happens During the ‘Detection and Penetration’ Phase?

As introduced above, penetration testing has a number of steps. The initial work involves gathering information about the systems, networks, and applications. In some cases, you may provide this information in advance to the penetration testing provider. Otherwise, by severely limiting the information given, you can request a blind penetration test that simulates the actions and procedures of a real attacker.

During this phase a complete list of all accessible systems and their respective services is gathered, obtaining as much information about your Internet facing assets as possible. With the reconnaissance work completed, the focus now transitions to identifying vulnerabilities in systems and applications.

This phase typically utilizes many tools that may be available in the public domain and are used by hackers. The exact intrusion techniques employed depend on the type of penetration test being performed (see 'What should you test?' below). Attempts are made to fully compromise the systems and once the active intrusion begins, targets are likely to be alerted to suspicious activity. The methods used during this phase are tightly controlled by the penetration testing agreement and activities are extensively logged. Any information or data obtained during the penetration testing will be treated as confidential and will be returned or destroyed accordingly after the tests.

What Should You Test?

Any part of your IT infrastructure and applications can be tested. One common implementation is external penetration testing, which addresses assets such as networks and web applications that are reachable from the Internet. Wireless penetration testing and mobile application penetration testing are becoming increasing prevalent in the industry and may be a consideration for your organization.

Some areas that you might not have previously considered threats are new attack vectors for hackers. PBX & VOIP systems and social engineering, where attacks implemented through human interaction and manipulation can be appropriate targets for penetration testing. Remember, once a hacker has access to your internal network it can be challenging to contain their activities.

Some of the most common vulnerabilities tend to be design flaws, configuration errors, and software bugs. These get introduced during development and implementation, generally by accident and, once identified by host security configuration penetration testing, can usually be quickly resolved.

Penetration testing providers typically offer a wide range of services and the scope of tests can be designed to meet your specific needs to manage risk and become compliant with industry and governmental regulations.

What Does a Penetration Test Report Include?

Penetration testing reports usually have a number of target audiences within your organization, so the report will often have a hierarchical structure with a corresponding level of details. You should expect to receive a report with an executive summary and an in-depth technical review upon completion of a penetration test. This document show the services provided, the methodology utilized, as well as testing results and recommendations. In addition to highlighting security vulnerabilities, it will provide guidance on remediation with a focus on how to mitigate risks.

The executive summary will recap the scope of the penetration testing, provide an overall risk posture and describe general findings. The intended audience will be those who are in charge of the oversight of the IT security program as well as any members of your organization which may be impacted by the confirmed threats. It is common for the technical report to include a threat level from low to critical, vulnerability rating, analysis of the issue, and the impact on the information asset in the event that the vulnerability is exploited. The threat level is determined by a combination factors including ease of access, level of access gained, difficulty of discovering the vulnerability and exploiting it, and the value of the asset to your organization. NopSec uses a DREAD Score scoring system which includes well-documented test results that provide robust insight using the following factors: Damage + Reproducibility + Exploitability + Affected Users + Discoverability.

And of course, the penetration testing report would not be complete without documented recommendations to secure any high-risk systems and detailed technical information on how to mitigate the vulnerabilities. You should be able to understand the tasks needed to resolve the risks identified and how much effort may be required to implement the recommended fix.

Screenshot - Example of penetration testing report

consistent level of quality, regardless of the network size. Based on the results of the penetration assessment, NopSec identified five (5) critical, four (4) high, and three (3) moderate risk vulnerabilities. NopSec determined that a motivated adversary positioned on the [redacted] network could compromise the Windows domain supporting a majority of the internal nodes. NopSec identified numerous systemic weaknesses that could be exploited to grant unauthorized access to sensitive resources including the presence of weak passwords, shared resources accessible without credentials, default credentials, and system misconfigurations.

Note: No critical system can be considered acceptably protected unless network segments and critical hosts / servers are constantly monitored for signs of abuse and intrusion attempts; all hosts, servers and routers are constantly kept up-to-date with the latest software security patches and end users are properly educated on acceptable behavior in the use of computing resources.

Overall, NopSec was able to achieve the goals of the assessment and gain unauthorized access to protected resources. There were a number of critical and high risk findings identified during the assessment including the following:

Finding Name	DREAD Score
Vulnerable to MS17-010	50
Vulnerable to Web Proxy Auto-discovery Protocol Man-in-the-Middle	50
NULL Session on Domain Controller	46
Vulnerable to Mimikatz Credential Harvesting	42
Vulnerable to Pass-the-Hash	42
Outdated Windows Version	38
Default Credentials	36
Path Traversal	35

You Have the Penetration Test Report… Now What?

Upon completion of the penetration testing and receipt of a formal report, you may need some help determining next steps. If the reason for your penetration test was to fulfill regulatory compliance, you may be done. However, armed with this vulnerability information the prudent action would be to fix the issues. You should request a full debrief from the penetration testing provider. NopSec provides an Executive Readout and Remediation Assistance as part of its penetration testing services. During this process you can get clarification about critical and high level vulnerabilities along with guidance on remediation. It might also be advisable to schedule a follow-up re-test at a later date to ensure that your remediation efforts have been successful. NopSec offers complimentary re-tests to validate remediation steps along with Positive Control Validation.

CHAPTER 3: PENETRATION TESTING RECOMMENDATIONS

How Should You Prepare for Penetration Testing?

You should have a clear reason and objective for penetration testing. In most cases, the objective of a penetration test is to demonstrate that exploitable vulnerabilities exist within your organization's infrastructure and applications. You should ensure that the appropriate internal staff is involved. You should agree upon what to do with the results and outcome of the penetration testing report. It is vital that normal business and everyday operations of your organization will not be disrupted during the duration of the penetration testing. You may encounter conflicts between the need to ensure that everything is tested and the need to avoid taxing your systems during periods of heavy and critical use. As such, penetration tests may need to be run at particular times of day.

What Determines the Cost and Time for Penetration Testing?

The truthful answer to this question is, it depends. Generally the cost and how long the penetration testing will take to complete is dependent on the size and complexity of the IT environment and the rigor with which the testing is performed. Detection, penetration, and exploitation of vulnerabilities can be time consuming. A small IT footprint can be completed in a few days. If your environment is large or complex, penetration testing may take several weeks.

What are the Limitations of Penetration Testing?

There are many security problems that penetration testing will not be able to identify. A penetration test can only identify those problems that it is designed to look for. If a particular system, service or application is not tested, then there will be no information about its security or insecurity.

Bear in mind that a penetration test does not last forever either. A penetration testing report is no more than a snapshot of your organization's IT security at a single moment in time. If any changes are made to the infrastructure or applications, there is the possibility that a new vulnerability has been exposed.

How Should You Select a Penetration Testing Provider?

As with all important buying decisions, you need to choose your penetration testing provider wisely. You want to ensure your organization's valuable assets are safeguarded by a reputable and trusted provider.

You should consider asking the penetration testing provider for a list of references from organizations with a similar profile to yours. You may also ask the vendor for examples of similar projects they have undertaken in the past. There are common accreditations in the IT security industry and you can ask to confirm the credentials and experience of the individuals who will oversee penetration testing services for your company.

Get started with NopSec Penetration Testing

Contact us to schedule an initial consultation
at **(646) 502-7900**
or
email **hello@nopsec.com**