GUIDE

Best Practices Guide: Vulnerability Assessments

A Straightforward Guide to Successful Vulnerability Assessments for Infrastructure and Applications

NOPSEC

nopsec.com | hello@nopsec.com

Table of Contents

Introduction

If you are new to vulnerability assessments or looking to refresh your knowledge, the information in this guide should help you to quickly understand the choices you have available. You will read advanced-level content created by IT Security engineers with hands-on experience in IT security and vulnerability assessments. This document will provide some insight as to why a vulnerability assessment is necessary and outline the process. By the end of this document you should understand the benefits of vulnerability assessments and be confident about the next steps to make your organization's IT infrastructure and applications more secure.

Enjoy!

Chapter 1: Introduction to Vulnerability Management

What is the Cause of IT Security Vulnerabilities?

Making information exchange available to customers and business partners, by definition, requires that companies have a connection to the outside world. Keeping the information secure from attackers becomes the challenge. There is a consistent stream of new security vulnerability discoveries due to flaws in software development, improper configuration of hardware and software applications, and the inevitable unintended errors made by IT users. With a significant number of applications and systems across your IT environment, keeping the information secure from attackers becomes the challenge. Maintaining and updating system operating systems and applications to eliminate vulnerabilities is critical, particularly for assets that are linked to personally identifiable customer information or sensitive corporate data.

Vulnerabilities generally fall into three categories: vendor, system, and user-originated. Vendor-originated vulnerabilities are programming mistakes in software that include insecure services or non-robust implementations of protocol standards. System-originated vulnerabilities include improper configuration of applications and lack of password protection policies. User-originated vulnerabilities result from falling prey to malware (Ie. Phishing emails), and not running anti-virus software.

It is important to identify the primary threat vectors your organization must worry about. Attackers will attempt to exploit any given vulnerability from the outside, such as exposed networks or web applications, or from the inside via internal networks, application flaws and malware. A serious concern is that once a single vulnerability from outside the organization is compromised, that system can be used as a springboard for additional attacks on the same network.

What is a Vulnerability Assessment?

A vulnerability assessment, also known as vulnerability testing, is the practice of detecting, classifying, prioritizing, and remediating security vulnerabilities in IT infrastructure and applications.

A vulnerability assessment is typically performed according to the following steps:

- Discover and inventory IT assets
- Assign importance to those resources
- Identify the vulnerabilities or potential threats to each resource
- Remediate or mitigate the most serious vulnerabilities for the most critical assets

A vulnerability assessment can be completed against your network, systems and applications using automated software. The tools provide a list of identified vulnerabilities sorted by asset, with vulnerabilities ranked by overall risk and recommendations for remediation. A vulnerability assessment should be part of a structured approach to addressing security vulnerabilities that may include implementing perimeter defenses such as firewalls, intrusion detection systems and anti-virus/malware scanning software. A Defense in Depth approach helps defend systems against any particular attack and addresses security vulnerabilities with multiple layers of protection.

Why is Vulnerability Assessment Important?

Regulatory compliance is a considerable driver for vulnerability assessments. In some industries certain types of data, and how the data is handled, is strictly regulated. Industry standards such as HIPAA, PCI, FISMA, Sarbanes-Oxley, and Gramm-Leach-Bliley all dictate how to secure different types of systems and the associated data. Regulators commonly require a documented security process, and a vulnerability assessment can serve that purpose. Even if you are not bound by any of these governmental regulations,

you still might want to use them as resources to help guide your own IT security practices. IT infrastructure changes over time, possibly opening it up to new vulnerabilities. New methods of compromising systems are continually invented, so constant vigilance is required.

What are the Objectives of a Vulnerability Assessment?

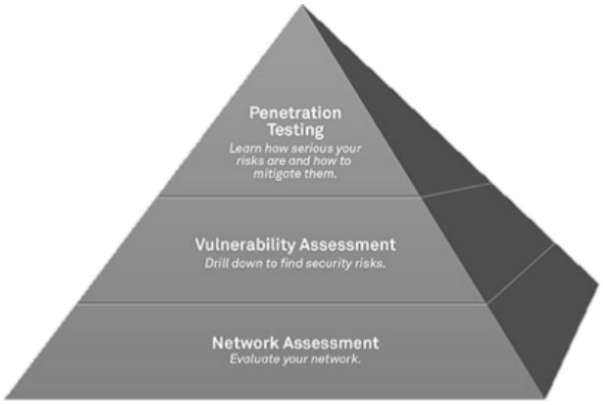
A vulnerability assessment should be a regular activity of every organization's security policy. The purpose of a vulnerability assessment is to find out what systems have holes and to take action in order to mitigate the risk. The objectives of a vulnerability assessment include:

- Documenting the state of security for audit and compliance with laws, regulations, and business policies.
- Understanding the overall security posture of your organization and identifying known security exposures before potential attackers do.
- Proactively tackling software configurations and patches to make the systems less susceptible to attack.
- Implementing practices that improve the management of IT security risks and developing staff expertise.

Penetration Testing Versus Vulnerability Assessments?

Both penetration tests and vulnerability assessments are valuable tools that can benefit any security program. While the two are often used interchangeably, the methodology differs dramatically. A vulnerability assessment generally begins with a scan of systems using automated tools that reduce the effort and costs associated with repetitive and time-consuming tasks. A penetration test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious hacker. The analysis of systems for any technical misconfigurations or vulnerabilities is carried out from the

perspective of a potential attacker, and will involve active exploitation of security vulnerabilities. Any security issues that are found will be presented together with an explanation of their impact and recommendations for remediation.



Chapter 2: Stages of a Vulnerability Assessment

Discovery and Inventory of Assets

The first step in a vulnerability assessment is to understand the scope of networks and systems. The initial work is comprised of gathering information about the systems, networks, and applications. Nmap is a popular tool that can be used to determine the layout of a network, host systems and open ports on those systems. This typically involves directing a vulnerability scanner at a range of IP addresses for domains and sub-networks or, in the case of a web application, a specific web address (URL). The vulnerability scan generates a complete list of all accessible systems and their respective services, obtaining as much information about your assets as possible. The vulnerability scan will inventory hardware, software applications, services and configurations. The scan can also identify rogue systems and devices that are connected to the network without authorization.

Risk Classification of Assets

The next step in a vulnerability assessment is to complete a prioritization or classification of information assets based on business risk. Not all data has the same level of sensitivity, nor do the assets on which the data reside. You may want to rank assets by the attributes of confidentiality, integrity, and availability. Primarily you will need to prioritize sensitive internal information (e.g., business plans, strategic initiatives, etc.), and regulated information (e.g., employee information, customer data, classified information, etc.)

A classification scheme helps your organization rank information assets based on the amount of harm that would be caused if the information was disclosed or altered.

Vulnerability Detection

The vulnerability scanner that was used during the discovery phase actively probes IT assets and applications for weaknesses. Known information security vulnerabilities that are found on the systems are reported. There are many options for scanning tools and most use a vulnerability database of known risks including The Common Vulnerability Scoring System (CVSS) and Common Vulnerabilities and Exposures (CVE). (See more information under 'Vulnerability Classification and Prioritization' below)

A vulnerability scan can be conducted both with or without network and system credentials. The more comprehensive the scan, the longer it will take to complete. One way to increase performance is through the use of multiple scanners on the network, which can report back to one system that aggregates the results. The sophistication and accuracy of vulnerability scanning software is generally comprehensive, however, errors can occur in the form of false positives. A false positive is a vulnerability that has been identified by the scanner but does not exist. Uncovering and removing these "phantom" vulnerabilities is a vital task for any vulnerability assessment provider.

What to Scan?

You will want the vulnerability scan to be comprehensive. Everything that is connected to your company's network should be scanned. For any network that is attached to the Internet, as well as networks that can be penetrated through weak Internet facing security controls, focus areas include DNS servers, FTP servers, intrusion detection systems, routers and switches, HTTP/HTTPS servers, VPN servers, load balancers, firewalls, and mail servers.
Web applications should include web servers, application code, and databases with focus on application logic built into the website susceptible to SQL injection, Blind SQL injection and client side attacks, such as Cross Site Scripting.

Other areas to consider are wireless access points, PBX and VOIP systems, and client devices such as desktop, laptop computers and even mobile devices.

Vulnerability Classification and Prioritization

Not all vulnerabilities are created equal. The Common Vulnerability Scoring System (CVSS) and Common Vulnerabilities and Exposures (CVE) are government and industry efforts for communicating the characteristics and impacts of IT vulnerabilities.

Vulnerability scanners categorize and rank vulnerabilities based on technical and business risks. The objective is to identify the issues that could impact the most critical systems or data, so you know what to fix first. The generally held categorization includes: Critical, High, Moderate/Medium, and Low. The severity level indicates the security risk of the vulnerability and the difficult of exploiting the vulnerability. The theory is that the more severe the vulnerability rating, the more at risk your organization is to attack. If there is a known exploit, the likelihood of an attack is much higher. In other cases, it often depends

on both the technical risk as well as the business importance of the asset on which the vulnerability resides.

Vulnerability Remediation

Fixing security issues and reducing your company's risk of a security breach is the core of vulnerability management. You should prioritize remediation of the most critical issues as quickly as possible. Most vulnerability scanners will provide guidance on remediation including links to recommended patches and workarounds from the vendors.

There are a number of areas that may need to be addressed: Operating systems on servers and workstations, infrastructure services such as email and DNS, web applications and databases as well as desktop productivity applications. One approach is for IT security analysts and IT operations to use a ticketing system to track progress of fixing critical vulnerabilities. This system ensures that fixes are addressed in a standardized way in a timely manner. If there are a large number of vulnerabilities, it may be useful to assign a project owner who has the authority to design a configuration management process to implement the necessary patches.

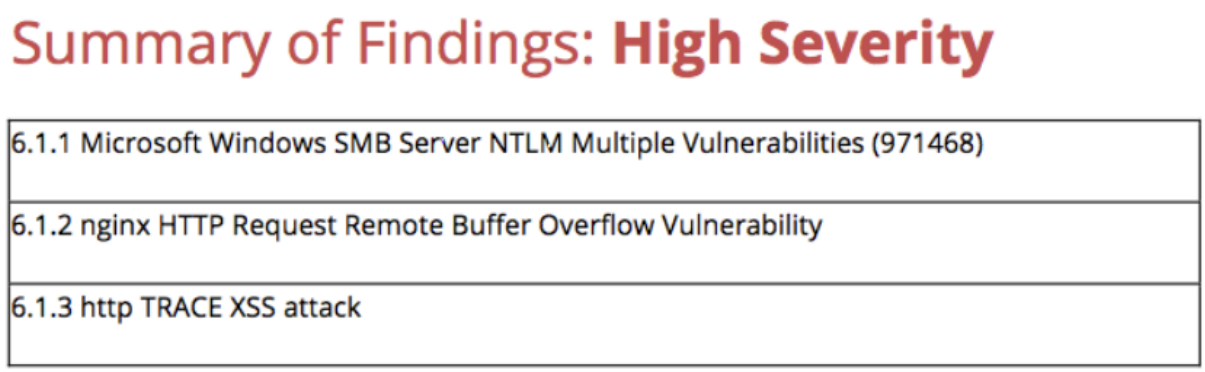
Reporting

Reports are used to document the data found during the previous phases of vulnerability management and provide a view appropriate for different audiences. Different reports are generally made available from templates targeting the specific audience. Some reports are targeted for auditors and industry regulators. Other formats help confirm compliance with internal operating policies. 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. An executive summary will recap the overall risk posture and describe general findings.

Common components in a vulnerability management report include:

- Assets covered in the detection phase
- Graphs and/or charts depicting overall risk status
- Prioritized listing of vulnerabilities ranked by risk rating
- Trending of vulnerabilities from discovery and remediation perspectives
- Trouble-ticket status
- Technical information about unresolved vulnerabilities

A vulnerability 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 issues and how much effort may be required to implement the recommended fix.



Chapter 3: Vulnerability Assessment Recommendations

How Can You Prepare for a Vulnerability Assessment?

The key to the successful completion of a vulnerability assessment is in the preparation and planning. Vulnerability assessments are normally contracted out to security companies, who have experience in conducting the efforts and can minimize the risk of

disruption. It is vital that the everyday operations of your organization will not be interrupted, particularly during the vulnerability scanning procedure.

Before starting a vulnerability assessment, it is important to ensure that the underlying policies are in place to facilitate the process. For example, defining the scope of activities to be covered as well as clearly defining each individual's roles and responsibilities in the discovery, analysis and remediation phases of the vulnerability assessment. There also should be an established method to track issues and distribute the findings to the system owners for resolution.

What Determines the Cost of Vulnerability Management?

There are multiple options for how you can complete a vulnerability assessment such as running the software yourself, or contracting the work out to a specialized IT security vendor. Vulnerability assessment providers have different pricing models. In most cases, the cost is directly related to the size, complexity and the number of assets being checked for vulnerabilities. The cost of a vulnerability assessment is dependent on:

- Scope: Size and complexity of the IT environment.
- Methodology: Rigor with which the testing is performed. The tools employed, specifically the vulnerability scanners, need to be based on a proven and regularly updated scanning engine.
- Qualifications: Expertise of the vendor providing the services. Is a specialized security firm delivering the vulnerability assessment with qualified and accredited practitioners?

Is There an Established Methodology for a Vulnerability Assessment?

When conducting a vulnerability assessment, the tool set being used should be very similar to those that are currently being employed by cyber attackers. There are a number of established methodologies for completing a vulnerability assessment.

The Open Source Security Testing Methodology Manual, also known as the OSSTMM, is a peer-reviewed manual of security testing and analysis.

The Open Information System Security Group (OISSG) Information Systems Security Assessment Framework is a peer-reviewed framework that categorizes information system security assessment into various domains, and details specific evaluation or testing criteria for each of these domains.

The National Institute of Standards and Technology (NIST) released a Special Publication 800-115 Technical Guide on Information Security Testing and Assessment.

The Open Web Application Security Project (OWASP), specifically the OWASP Top 10 is a document covering web application security and the most critical web application security flaws.

How Should You Select a Vulnerability Assessment Provider?

Your choice needs to incorporate your budget and resource considerations. Because you are protecting your organization's most valuable assets from security breaches, you will want to select a vendor that balances a solid track record of performance.

You should seek out a provider that understands the unique needs of your IT environment and has the flexibility to deliver a customized solution. With efficient and effective remediation being the end goal, having a provider that integrates well with your existing security and management tools should be a strong consideration.

You should consider asking the vulnerability management 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 the vulnerability management services for your company.

Chapter 4: Vulnerability Assessment Best Practices

There are fundamentals that can help increase the odds of a successful vulnerability assessment. Below is a condensed list of learning based on the experience gleaned from conducting vulnerability assessments:

1. *Identify and Understand Your Business Processes*

   To get the most out of a vulnerability assessment, you need to deeply understand the systems in your IT environment that are critical and sensitive in terms of compliance, customer privacy, and competitive position. This extends to

mission-critical processes as much as software development environments that are inherently less secure than production environments. Having an effective asset management system and knowing the ever-changing landscape should be a priority. There is an adage in IT security that, "you cannot protect what you cannot see".

2. *Determine What Safeguards are Already in Place*

As noted in the first chapter, a vulnerability assessment should be part of a structured approach to addressing security vulnerabilities that includes existing security and business continuity measures you have already put in place. These safeguards may include firewalls, intrusion detection and prevention systems (IDPS), virtual private networks (VPNs), data loss prevention (DLP), encryption and internal policies. Understand the key capabilities of these protections, and which vulnerabilities they address most effectively.

3. *Apply Business Context to Scanner Results*

Your scanner may produce an enormous quantity of vulnerabilities with severity ratings. However, since vulnerability scores are based on technical objective measures, it's important to evaluate and prioritize the results from a business context. It can be helpful to partner with a company that is well versed in all aspects of security and threat assessment. Your results need to be analyzed to determine which vulnerabilities should be targeted first and most aggressively. There is a law of diminishing returns when it comes to remediation efforts for low risk vulnerabilities.

4. *Remediate in the Most Efficient Way Possible*

Your vulnerability assessment report may recommend software patches and upgrades to address security holes. If available, use an automated patching solution that tests patches to ensure compatibility before deployment. Moreover, track the remediation process from initiation all the way through the process to validate that the fix has been applied correctly.

5. *Remain Vigilant and Continually Improve*

Performing a vulnerability assessment can provide an accurate "point-in-time" representation of your organization's security posture. Cyber attacks frequently take advantage of the weakest links in your infrastructure and applications, and frequently those weak links can be found at branch offices or among mobile laptops and other unpatched devices.

The only way to really minimize the overall risk is to incorporate the vulnerability assessment into a continual security process. Organizations with a mature security approach provide recommendations back to configuration management to build and deploy more secure standard IT asset configurations. In some cases, they require new hardware and applications to be analyzed for vulnerabilities before they can be added or authenticated to the network. You can also educate non-security staff members about the importance of strong passwords, not falling prey to social-engineering attacks, and not opening email attachments from people they do not know. It is advisable to increase both the frequency and coverage of vulnerability scanning and follow a structured process for swift remediation.

Find out how NopSec's Unified VRM can help you think like a hacker and stay ahead of the trends. Visit www.nopsec.com or email hello@nopsec.com for additional information or to request a demo.

About NopSec

NopSec operates with one mission: to help people make better decisions to reduce security risks. Our team is passionate about building technology to help customers simplify their work, manage security vulnerability risks effectively, and empower them to make more informed decisions. Our software-as-a-service approach to vulnerability risk management offers an intelligent solution to dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation.

NopSec helps security professionals simplify their work, effectively manage and prioritize vulnerabilities, and make better informed decisions.

NopSec's Unified VRM is an innovative threat and vulnerability management solution that addresses the need for better prioritization and remediation of security vulnerabilities in a single platform.

NopSec Inc. • www.nopsec.com • info@nopsec.com