Assess the vulnerability of an enterprise's applications and network

Provide a proactive mechanism for detecting vulnerabilities

Madhusudhan Rajappa

August 23, 2016

This tutorial describes effective ways of conducting vulnerability assessments of web applications and networks in any organization and illustrates how to proactively defend against cyber attacks using a combination of enterprise-grade and trustworthy vulnerability scanners such as Tenable Nessus Scanner and IBM Security AppScan Enterprise.

New systems, applications, and devices are becoming more interconnected everyday. In addition, social media and e-commerce buzz are adding more people to the online world, bringing with them a lot of sensitive business and personal data.

With these developments come the added risk of security vulnerabilities and the possibility of crucial and sensitive data that is exposed to cybercriminals.

One of the most important methods of protecting the IT infrastructure of any organization is to proactively identify and address the vulnerabilities present within the organization's applications and networks by performing vulnerability scans periodically.

The objective of this tutorial is to show an effective way of conducting a vulnerability assessment of the web applications and network of any organization. This tutorial also shows how to proactively defend the organization from cyber attacks by using a combination of enterprise-grade and trustworthy vulnerability scanners. The scanners that will be discussed in this tutorial are the Tenable™ Nessus® Scanner and the IBM AppScan® Enterprise. This tutorial also includes step-by-step instructions to implement a vulnerability assessment by using each of those scanners.

“This tutorial describes effective ways of conducting vulnerability assessments of web applications and networks in any organization and illustrates how to proactively defend against cyber attacks by using scanners such as Tenable Nessus Scanner and IBM Security AppScan Enterprise.”
What is vulnerability assessment?
Vulnerability assessment is the process of identifying, ranking, and reporting the vulnerabilities that are present in the IT infrastructure of an organization. Vulnerability assessment predominantly uses automated tools for scanning, with manual verifications of identified issues. The potential risks posed by the known vulnerabilities are ranked in accordance with NVD/CVSS base scores that use the CVSS calculator.

The vulnerability assessment approach
The following sections define the approaches that will help in performing vulnerability assessment efficiently and effectively.

Determine the target systems
In this stage, the vulnerability analyst has to make a list of IP addresses that are required to be scanned in the organization network. The list should contain IP addresses of all the systems and devices that are connected in the organization's network. The analyst should be aware of the network topology of the organization.

Determine the target applications
In this stage, the vulnerability analyst lists the web applications and services to be scanned. The analyst determines the type of web application server, web server, database, third-party components, and technologies (for example, Flash, AJAX, Java®, and JavaScript) out of which the applications are built. Also, the analyst has to obtain a test user account to log in to the application when configuring the scan in AppScan.

Vulnerability analysts should work with the application architect and gain complete knowledge about each application (for example, its logical flow and the different levels of access); this will help in accurately configuring the assessment scans.

Vulnerability scanning and reporting
For the successful completion of a vulnerability assessment, the vulnerability analyst keeps network teams and IT teams informed of all assessment activity, because vulnerability assessment can occasionally create huge bursts in network traffic when loading the target servers with requests. Also, the analyst obtains the unauthenticated pass-through for scanner IPs across the organization network and ensures the IPs are whitelisted in IPS/IDS. Otherwise, the scanner can trigger a malicious traffic alert, resulting in its IP being blocked and the sending of mass emails.

Using Tenable Nessus Professional Scanner
Why Tenable Nessus?
Nessus Professional is a widely used vulnerability scanner that discovers the vulnerabilities in an organization's networks. It also provides the CVSS Base Score along with the advisory. Nessus has a high-speed, accurate asset discovery engine that is capable of scanning operating systems, network devices, firewalls, hypervisors, databases, and middleware applications for vulnerabilities, threats, and compliance violations. Nessus can detect threats by viruses,
backdoors, malwares, botnet, and unknown processes. It also provides flexible reporting options: reports can be customized based on vulnerability type or hosts; they can create executive summaries or compare the scan results to highlight any changes; and reports can be published in XML, PDF, and HTML format.

**Configure a Nessus scan**

1. Log in to Nessus Professional. You will see the Scans / My Scans page. By default, all created scans are stored in the My Scans folder. It is best to create a new folder with an appropriate identifier before configuring a scan. You can create new folders by clicking the **New Folder** button on the left navigation area of the Scans / My Scans page. The following steps demonstrate how you can create and schedule the new scan.

2. Click **New Scan**.

3. At the next screen, select the scan template. I recommend that you use the **Basic Network Scan** template as it is the predefined scanner template that is best suited to scan internal or external hosts.

4. At the next screen, enter valid responses for the General section. Enter a name for scan identification, the scan description, the correct folder...
for the scan, and the valid target IP Address / IP Range / Hostname.

5. Once you complete updating the general details, click **Schedule** on the same page and enable the scan scheduling by clicking on the slide button. Then set the scan to launch monthly and enter the start day and time, the timezone, and the Repeat By value.
6. Click **Notifications**. Provide the email addresses of the persons who will receive the scan notifications.

7. Click **Discovery**. Select **Port scan (all ports)** as the Scan Type so that all 65536 ports of each system are scanned for vulnerability.

8. At the Assessment screen, select **Scan for all web vulnerabilities (complex)** as the Scan Type, so that any vulnerability that is related to the web application is also discovered. The scope is limited in using this scan type as we will focus more on using IBM Security AppScan Enterprise for web application security assessment.
Assess the vulnerability of an enterprise’s applications and network because it has more advanced scan configuration options that improve the assessment coverage.

9. Retain the default preset options that were provided in the Report and Advanced link. Then save the scan by clicking Save. You will see the following screen capture image.

Now the scan is scheduled to run every month at the specified date and time. The History tab inside each scan job gives the status of the scan run at the specified duration.

**Reporting**

Once the scan is triggered and completed, you can view the vulnerability highlights by clicking Scan and then Vulnerabilities.
You can export the report in PDF, HTML, CSV, Nessus, and NessusDB formats.

For further analysis of the result, you can export the result in .nessus format, import it in Metasploit, and perform a manual analysis by using relevant Metasploit exploit modules. These reports should be shared with server administrators and network security teams so that they can take the necessary actions to address the vulnerability by patching, upgrading, and so on.

**Vulnerability assessment using IBM Security AppScan Enterprise**

**Why IBM Security AppScan Enterprise?**

IBM Security AppScan Enterprise Edition (AppScan) is a web application security assessment tool, used industry wide, that offers advanced application security testing and risk management with a platform that drives governance, collaboration, and security intelligence throughout an application's lifecycle. AppScan helps to discover vulnerabilities by utilizing a comprehensive set of security test policies. Its powerful dashboard classifies and prioritizes application assets based on business impact and identifies high-risk areas, permitting organizations to maximize their remediation efforts.
Configure an IBM Security AppScan Enterprise scan

The basic steps to configure web application scans in IBM Security AppScan Enterprise are in the following steps. For detailed coverage of scan configuration, please see my article "AppScan Enterprise scan configuration best practices."

1. Log in to IBM Security AppScan Enterprise. On the Scan tab, click on the + button to create a new scan job.
2. At the next screen, select Content Scan Job. Provide a valid name for Test and then click Create.
3. Provide the correct starting URL(s) of the test application in AppScan Enterprise. This is usually the front page of your application. Under "What To Scan," mark the checkbox In starting domains, only scan links in and below the directory of each starting URL if links only in and below directories need to be scanned in the starting URL. Leave that box unchecked if the links above the directory in the starting URL also need to be scanned. If there are domains outside the starting URLs with content that needs to be scanned (for example, if link http://www.example.com changes to http://www.support.example.com
4. As a best practice, I suggest manual explores be used to navigate through the web application to add pages that need user interaction, such as form fills, and pages that may be missed by an automatic scan. Examples of the latter include such pages as those that use Web 2.0 features that use AJAX, pages that require specific inputs, or those with embedded JavaScript or links found in Flash components. You may record manual explore data (and recorded login data) in any of three different ways:
   • With the manual explore browser plugin.
   • With the AppScan manual explore tool.
   • With AppScan Standard Edition (via the embedded browser or external browsers or by using AppScan as a proxy directly).

In addition, note the following:
   • If you select the AppScan manual explore tool or AppScan Standard for manual explores, you can save the results of your explore (or recorded login). This can save you time later if you need to modify your explore to accommodate changes to your scan configuration or to create a similar scan job.
   • Prior to manual explores (or recording logins), it is a good idea to clear any pre-existing cookies from your web browser.
   • During the manual explore (or login recording) process, make sure that all other browser windows are closed.
   • Clean up manual explores (and recorded logins) by removing any extraneous URLs or domains before running the scan. You can remove URLs and domains by selecting the checkbox next to the item and pressing the Delete button (marked with an x).
   • If your application requires that the pages be accessed in a particular sequence, this may be configured as a multi-step operation. However, multi-step operations can add significant work to the scan job and should be as small as possible to limit their impact.
   • You can find remaining pages that require additional manual exploring by using the “Pages with Unfilled Forms” report after your scan job completes.
5. At the next screen, configure Login Management. With the exception of applications that use only HTTP Basic or Digest authentication, "Recorded" logins are usually the best choice.

6. You can improve performance and the accuracy of the results by configuring the environment definition: for example, by entering the Web Server type, Application Server type, Database type, and so on.

7. In addition to using manual explore, configure a test with automatic explore, which will perform spidering and locate pages that might have been missed in the manual explore. This will enable greater scan coverage. The best coverage of an application
will result from a scan with extensive manual exploration and is allowed to spider.

8. Click **Schedule**. Enable the scan scheduling by selecting the checkbox **Run automatically as per the schedule below**. Then set the scan to launch monthly.

---

**Reporting**

Once the scan is complete, the report can be obtained from the **Report Pack** link from the dashboard, under the respective scan job. The report can be exported in spreadsheet, CSV, XML,
and PDF formats. Share these reports with the software development team so that they can work on fixing the reported application vulnerabilities.

Conclusion

An organization's applications and network are the main targets of an attacker. The solutions that are described in this article provide a proactive mechanism for detecting vulnerabilities so that IT teams can fix or take measures before an attacker exploits those vulnerabilities. Using AppScan and Nessus for vulnerability assessment enables an organization to project a high level of security posture of its hosted network and systems and web applications.

To improve security levels further, the organization could choose to perform penetration testing and ethical hacking of their IT infrastructure. For guides to these processes, see the Open Source Security Testing Methodology Manual or the Testing Guide of the Open Web Application Security Project (OWASP).
Related topics

- IBM AppScan Enterprise
- Tenable Nessus Professional Scanner
- CVSS calculator
- Metasploit