Windows Vulnerability Assessment

Nowadays every enterprise, be it small or large, depends on information technology (IT) for some or most of its operations, and with IT comes information security. Most of the small and medium scale enterprises (SMEs) and sometimes large enterprises are unaware of the issue of information security and hence often ignore it. The budget (if) allocated for the purpose of implementing cyber security is usually too scarce to get a thorough penetration test and/or security compliance done. This negligence often leads to a security breach and ultimately costs more in the form of data loss and incident handling costs. It is always better to follow a proactive strategy than a reactive one in the field of cyber security.

In this article we are going to discuss the Windows vulnerability assessment utilizing some free and easy to use tools. The tools have been chosen intentionally that anyone with basic technical understanding can use them, so that the Administrator of even a small enterprise can utilize them to generate results and take appropriate action.

Before discussing vulnerability assessment and the tools in detail, here are few terminologies that need to be discussed:

Vulnerability: Vulnerability can be understood as a weakness or flaw in the application which allows an attacker to cause undesirable operations or gain unauthorized access. Presence of vulnerability poses a threat to the user of the application as it might lead to data compromise. Example: Buffer Overflow

Threat: An event or action that might prejudice security. A threat can also be described as a potential violation of security. Example: A Virus

Attack: Any action that attempts to violate the security of a system. Example: Brute Force

Exploit: A command sequence or data chunk whose aim is to take advantage of a flaw or vulnerability in an application. Example: MS 12-020 RDP exploit

Now we understand the basics, so let’s move forward. Vulnerability assessment in terms of cyber security can be understood as the process of Identifying, Enumerating and Ranking the vulnerabilities present in a system or network in order to patch them. It is concerned with the security of the resource and its environment and is a proactive approach.

Typical assessment steps:
- Classifying system resources
- Allocating enumerable value to the classified resources
- Detecting possible threats (vulnerabilities) to each resource
- Eliminating the vulnerabilities on priority basis

Often people, even in IT industry, confuse vulnerability assessment with penetration testing. Here are the differences between the two:

<table>
<thead>
<tr>
<th>Vulnerability Assessment</th>
<th>Penetration Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aim is to find out all potential vulnerabilities.</td>
<td>Aim is to identify and exploit the vulnerabilities.</td>
</tr>
<tr>
<td>It provides an overview of the existing flaws.</td>
<td>It demonstrates the impact of the flaw.</td>
</tr>
<tr>
<td>Might present false positives regarding the vulnerabilities. It does not validate them.</td>
<td>Exploiting the vulnerabilities removes the chance of a false positive.</td>
</tr>
<tr>
<td>It is difficult to check if the security measures (IPS, IDS, firewall etc.) can be bypassed or not.</td>
<td>Simulating the attack determines if the security measures can be bypassed or not.</td>
</tr>
</tbody>
</table>

Windows operating systems are some of the most used as well as exploited OS around the world. The ease of deployment and usage has not only made them popular among the common people but also a soft target for the attackers. Here we are going to discuss some tools which can be utilized to easily perform Windows vulnerability assessment so that the flaws are identified at the right time by the right people to avoid security breaches.

Open Vulnerability Assessment System: Initially named as GNessUs, OpenVAS is a powerful vulnerability scanning and management framework. It was forked from the popular vulnerability scanner Nessus after it went proprietary in 2005 (initially it was free and open source).

OpenVAS is based on client-server architecture over SSL. The architecture is explained below (source: [http://www.openvas.org/software.html](http://www.openvas.org/software.html)):

- OpenVAS Scanner: At the core of the architecture is the OpenVAS scanner which executes the Network Vulnerability Tests (NVTs). The NVTs are regularly updated with the NVT feed.
- OpenVAS Manager: It provides the service of combining the vulnerability scanning with vulnerability management. The manager makes it possible to implement various clients for consistent behavior. It also controls a SQL database for central storage.
- Greenbone Security Assistant: GSA provides a browser based interface for the application.
• Greenbone Security Desktop: GSD provides a desktop client.

• OpenVAS CLI: A simple command line interface.

• OpenVAS Administrator: It is a full service daemon whose task is user and feed management.

The protocols implemented in OpenVAS are:

• OpenVAS Transfer Protocol (OTP)

• OpenVAS Management Protocol (OMP)

• OpenVAS Administrative Protocol (OAP)

Feature overview of OpenVAS:

OpenVAS Scanner
• Many target hosts are scanned concurrently
• OpenVAS Transfer Protocol (OTP)
• SSL support for OTP (always)
• WMI support (optional)

OpenVAS Manager
• OpenVAS Management Protocol (OMP)
• SQL Database (SQLite) for configurations and scan results
• SSL support for OMP (always)
• Many concurrent scans tasks (many OpenVAS Scanners)
• Notes management for scan results
• False Positive management for scan results
• Scheduled scans
• Flexible escalators upon status of a scan task
• Stop, Pause and Resume of scan tasks
• Master-Slave Mode to control many instances from a central one
• Reports Format Plugin Framework with various plugins for: XML, HTML, LateX, etc.

OpenVAS Administrator
• OpenVAS Administration Protocol (OAP)
• SSL support for OAP (always)
• All OAP commands also as command line parameters
• User Management
• Feed status view
• Feed synchronization
Greenbone Security Assistant (GSA)
- Client for OMP and OAP
- HTTP and HTTPS
- Web server on its own (micro-httpd), thus no extra web server required
- Integrated online help system

Greenbone Security Desktop (GSD)
- Client for OMP
- Qt-based
- Runs on Windows, Linux, etc.
- Support of Internationalization (English, German, French...)

OpenVAS CLI
- Client for OMP
- Runs on Windows, Linux, etc.

OpenVAS comes pre-installed on the Backtrack 5 under:

Backtrack ➔ Vulnerability Assessment ➔ Vulnerability Scanners.

Steps to setup OpenVAS in Backtrack 5:

OpenVAS provides a utility to check the setup of the application, it can be fired up using the following command under the directory /pentest/misc/openvas

# ./openvas-check-setup

This command checks and provides advisories on the issues related to the setup.

- Add a user to the OpenVAS using the option OpenVAS Adduser. Output is displayed in figure 1.
Figure 1. Adding a user to OpenVAS

- Create the certificate using the option OpenVAS Mkcert Certificate creation is demonstrated in figure 2.

Figure 2. Certificate created

- Synchronize the NVTs using the option OpenVAS NVT sync. NVT sync. process is shown in figure 3.
Figure 3. NVT sync.

- Start the scanner through option Start OpenVAS Scanner. The output of the function and the following steps are shown in figure 4.

- Create the client cert using the command:
  
  ```
  # openvas-mkcert-client –n om –i
  ```

- Rebuild the database by running the command:

  ```
  # openvasmd –rebuild
  ```

- Create an administrative user using the command:

  ```
  # openvasd –c `add_user` –n AdminNameHere –r Admin
  ```

- Start OpenVas Manager

  ```
  # openvasmd –p 9390 –a 127.0.0.1
  ```

- Start OpenVAS Administrator

  ```
  # openvasad –p 9393 –a 127.0.0.1
  ```
• Start Greenbone Security Assistant

```bash
# gsad --http-only --listen=127.0.0.1 --p 9392
```

• Access the Greenbone Security Assistant interface to start the assessment using a web browser with address 127.0.0.1:9390. Figure 5 shows the GSA interface.

Microsoft Baseline Security Analyzer (MBSA) is a software tool provided by Microsoft to assess the security state of a Windows machine. MBSA looks for missing security patches and security
misconfigurations to find out the basic security issues the machine might be facing. MBSA not only looks out for OS based issues but also for some the widely deployed Microsoft services and applications such as Windows IIS, SQL server, Internet Explorer (IE), MS office. Figure 6 shows the MBSA interface.

Figure 6. MBSA interface

MBSA provides two interfaces to use the application, the graphical interface can be accessed by the Mbsa.exe and the command line interface can be accessed through the Mbsacli.exe. Although both the interfaces perform the same function, the command line interface provides some advanced technical options for better administration. The advantage of using the graphical interface is that it displays the result immediately after the process of scanning. After completing the process of scanning a single computer or multiple computers, MBSA provides a list of security recommendations that can easily be implemented by the administrator to elevate the security level of the machine. Figure 7 displays the result of a MBSA scan.

Figure 7. MBSA scan result
(source: http://en.wikipedia.org/wiki/Microsoft_Baseline_Security_Analyzer)
Secunia PSI: Although Microsoft Baseline Security Analyzer (MBSA) can be used to check for missing updates for the Windows OS and services, what about the third party applications? Even if the release of a new version of an application is known, it is often ignored, so this is where Secunia Personal Software Inspector comes in. Secunia PSI is a free application for security scanning. It checks out which applications need to be updated and is also capable of automating the process of updating. The application can run in the background and identify the programs that need updating, and download the appropriate patch and install it, without much user interaction. If it is not capable of updating the application itself, it notifies the user about it and also provides some instructions that can be helpful in the process. Figure 8 shows the output of Secunia PSI for a windows machine.

![Secunia PSI scan result](image)

Figure 8. Secunia PSI scan result

Secunia PSI performs its functionality by examining the files on the computer and extracting software vendor specific metadata. This collected data is further sent to Secunia’s server for determination of the applications installed on the machine and provides the report of the security updates which are missing from the system. By allowing scanning for all the updates through one interface and automating the process of updating, it substantially reduces the effort required for keeping the system updated and increases the security level. Figure 9 displays the Secunia PSI interface after updating the specific application.
Protector Plus- Windows Vulnerability Scanner: Protector Plus-WVS is a utility developed by Proland Software that is capable of detecting the vulnerabilities present in a Windows environment. It scans a machine for vulnerabilities and displays the result in the form of a list. Along with the vulnerabilities it also provides the rating of the vulnerabilities and a link to the appropriate Microsoft patch (Microsoft Security Bulletin). It is a simple program which requires no installation and executes by simply double-clicking the Winvulscan.exe. Along with displaying the result list it also creates a log file named as Protector_Plus_Windows_Vulnerability_Scan.htm in the folder where the .exe is. The result of the Protector Plus WVS is shown in figure 10.
Windows Sysinternals: Windows Sysinternals is actually not a vulnerability scanner, but it is capable of assisting users with its various functionalities. It is a collection of utilities which can help to manage, diagnose, troubleshoot and monitor a Windows machine. The utilities of Sysinternals have been bundled together into a single suite, the Sysinternals suite. The list of the tools in the suite is:

AccessChk | DiskView | PortMon | RegDelNull
AccessEnum | Disk Usage | ProcDump | RegJump
AdExplorer | (DU) | Process | RootkitRevealer
AdInsight | EFSDump | Explorer | SDelete
AdRestore | FindLinks | Process Monitor | ShareEnum
Autologon | Handle | PsExec | ShellRunas
Autoruns | Hex2dec | PsFile | SigCheck
BgInfo | Junction | PsGetSid | Streams
CacheSet | LDMDump | PsInfo | Strings
ClockRes | ListDLLs | PsKill | Sync
Contig | LiveKd | PsList | TCPView
Coreinfo | LoadOrder | PsLoggedOn | VMMAP
Ctrl2Cap | LogonSessions | PsLogList | VolumeID
DebugView | MoveFile | PsPasswd | Whols
Desktops | NTFSInfo | PsService | WinObj
Disk2vhd | PageDefrag | PsShutdown | ZoomIt
DiskExt | PendMoves | PsSuspend | RAMMap
DiskMon | PipeList | |

The utilities provided in the Sysinternals suite are small yet quite useful. The utilities such as Process Explorer, RAMMAP, and Autoruns are very advanced and provide functionalities which are not even provided by various commercial applications. Although these utilities do not provide any vulnerability detection, yet they can be very helpful in detection of various security threats/attacks and daily troubleshooting.

Conclusion

Vulnerability assessment as described above helps to substantially reduce the risk of a security breach. It should not be taken as a substitute to other security practices such as penetration testing, malware scanning, IPS/IDS implementation, log analysis etc., but should be practiced as a complementary process. As it does not require special training in the information security domain and can be accomplished by anyone with a basic understanding of computers, it must be in the priority list of any enterprise which desires to keep its data safe.