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:

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

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):

- 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 Admininstrative 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.

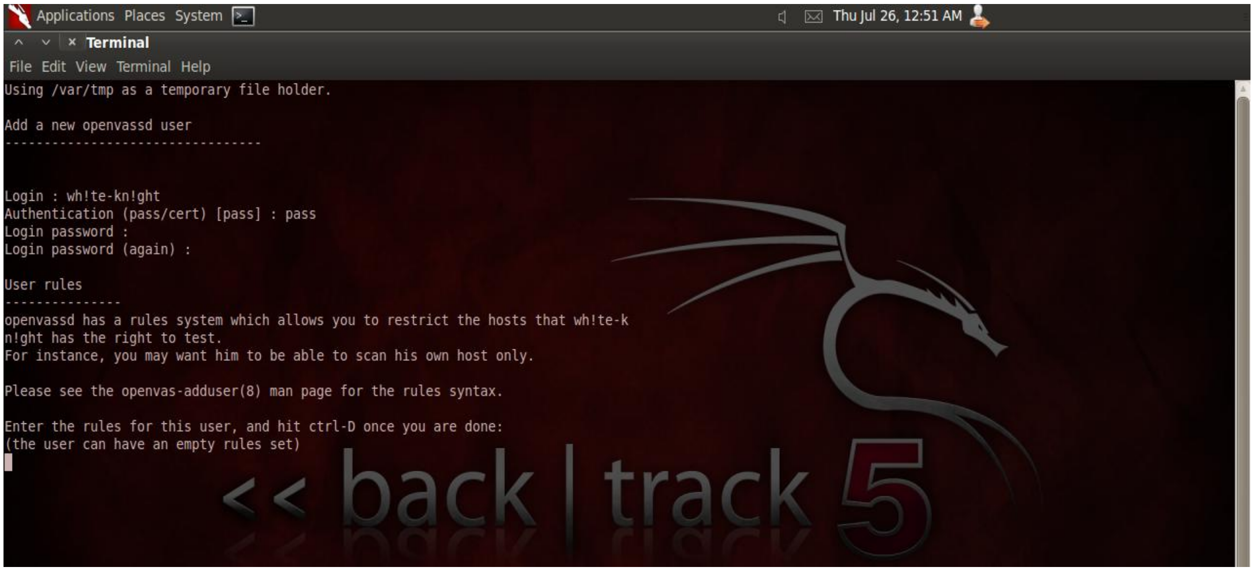
Steps to setup OpenVAS in Backtrack 5:

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.

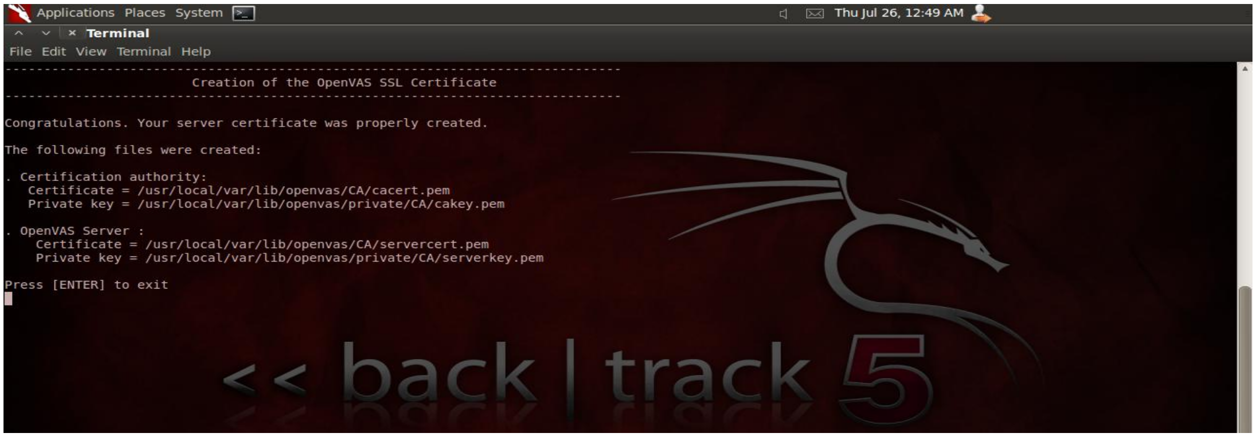
- Add a user to the OpenVAS using the option OpenVAS Adduser. Output is displayed in figure 1.



```
Using /var/tmp as a temporary file holder.

Add a new openvassd user
---------------------------------


Login : wh!te-kn!ght
Authentication (pass/cert) [pass] : pass
Login password :
Login password (again) :

User rules
---------------
openvassd has a rules system which allows you to restrict the hosts that wh!te-k
n!ght has the right to test.
For instance, you may want him to be able to scan his own host only.

Please see the openvas-adduser(8) man page for the rules syntax.

Enter the rules for this user, and hit ctrl-D once you are done:
(the user can have an empty rules set)
```

Figure1. Adding a user to OpenVAS

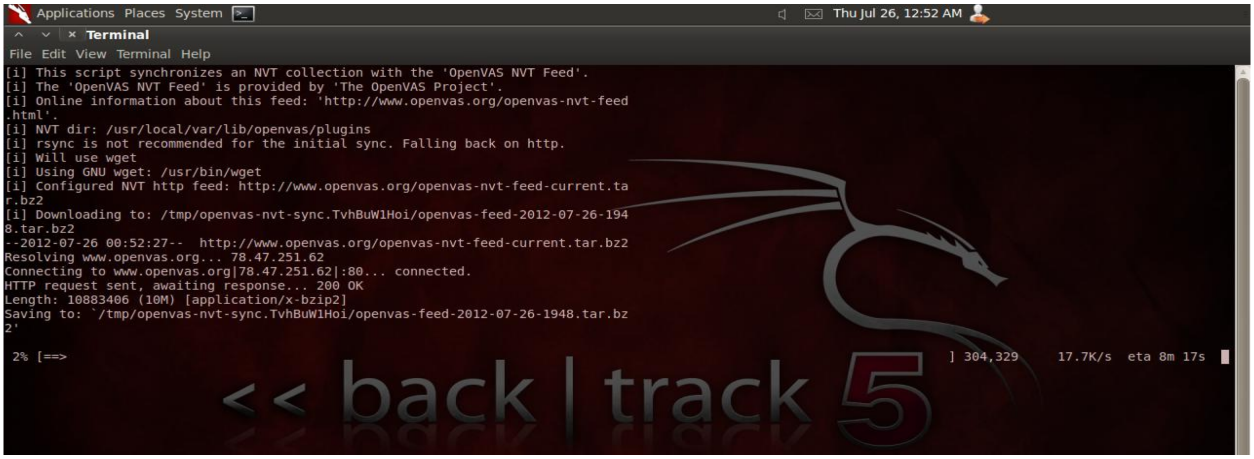
- Create the certificate using the option OpenVAS Mkcert Certificate creation is demonstrated in figure 2.



```
-------------------------------------------------------------------------------
                        Creation of the OpenVAS SSL Certificate
-------------------------------------------------------------------------------

Congratulations. Your server certificate was properly created.

The following files were created:

. Certification authority:
   Certificate = /usr/local/var/lib/openvas/CA/cacert.pem
   Private key = /usr/local/var/lib/openvas/private/CA/cakey.pem

. OpenVAS Server :
    Certificate = /usr/local/var/lib/openvas/CA/servercert.pem
    Private key = /usr/local/var/lib/openvas/private/CA/serverkey.pem

Press [ENTER] to exit
```

Figure 2. Certficate created

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



```
[i] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'.
[i] The 'OpenVAS NVT Feed' is provided by 'The OpenVAS Project'.
[i] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed
.html'.
[i] NVT dir: /usr/local/var/lib/openvas/plugins
[i] rsync is not recommended for the initial sync. Falling back on http.
[i] Will use wget
[i] Using GNU wget: /usr/bin/wget
[i] Configured NVT http feed: http://www.openvas.org/openvas-nvt-feed-current.ta
r.bz2
[i] Downloading to: /tmp/openvas-nvt-sync.TvhBuW1Hoi/openvas-feed-2012-07-26-194
8.tar.bz2
--2012-07-26 00:52:27--  http://www.openvas.org/openvas-nvt-feed-current.tar.bz2
Resolving www.openvas.org... 78.47.251.62
Connecting to www.openvas.org|78.47.251.62|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10883406 (10M) [application/x-bzip2]
Saving to: `/tmp/openvas-nvt-sync.TvhBuW1Hoi/openvas-feed-2012-07-26-1948.tar.bz
2'

 2% [==>                                                                                          ] 304,329     17.7K/s  eta 8m 17s
```

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:

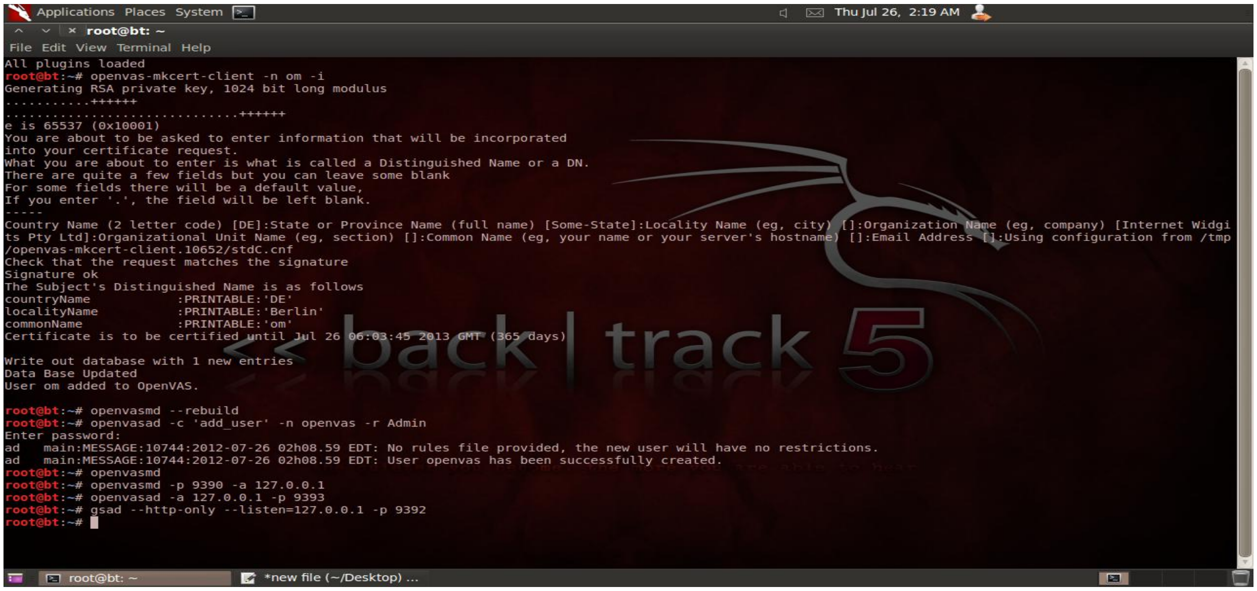
  # openvasd –c 'add_user' –n AdminNameHere –r Admin

- Start OpenVas Manager

  # openvasmd –p 9390 –a 127.0.0.1

- Start OpenVAS Administrator

  # openvasad –p 9393 –a 127.0.0.1



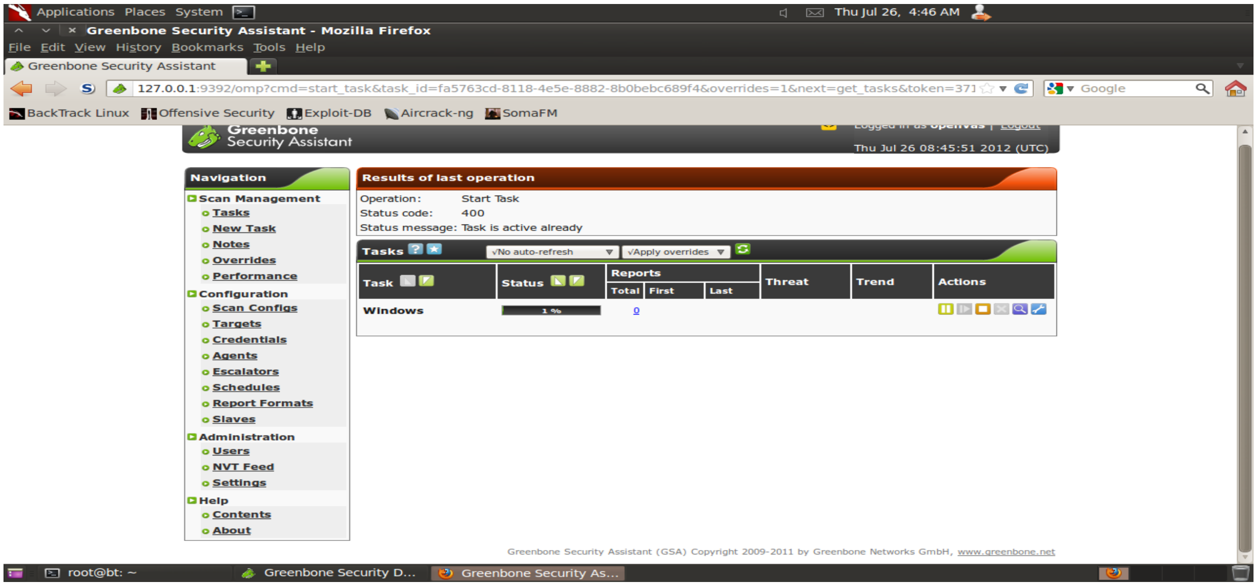
```
All plugins loaded
root@bt:~# openvas-mkcert-client -n om -i
Generating RSA private key, 1024 bit long modulus
...........++++++
..............................++++++
e is 65537 (0x10001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [DE]:State or Province Name (full name) [Some-State]:Locality Name (eg, city) []:Organization Name (eg, company) [Internet Widgi
ts Pty Ltd]:Organizational Unit Name (eg, section) []:Common Name (eg, your name or your server's hostname) []:Email Address []:Using configuration from /tmp
/openvas-mkcert-client.10652/stdC.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'DE'
localityName          :PRINTABLE:'Berlin'
commonName            :PRINTABLE:'om'
Certificate is to be certified until Jul 26 06:03:45 2013 GMT (365 days)

Write out database with 1 new entries
Data Base Updated
User om added to OpenVAS.

root@bt:~# openvasmd --rebuild
root@bt:~# openvasad -c 'add_user' -n openvas -r Admin
Enter password:
ad   main:MESSAGE:10744:2012-07-26 02h08.59 EDT: No rules file provided, the new user will have no restrictions.
ad   main:MESSAGE:10744:2012-07-26 02h08.59 EDT: User openvas has been successfully created.
root@bt:~# openvasmd
root@bt:~# openvasmd -p 9390 -a 127.0.0.1
root@bt:~# openvasad -a 127.0.0.1 -p 9393
root@bt:~# gsad --http-only --listen=127.0.0.1 -p 9392
root@bt:~#
```

Figure 4. OpenVAS Setup

- Start Greenbone Security Assistant

  # 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.



Applications Places System
Thu Jul 26, 4:46 AM
Greenbone Security Assistant - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Greenbone Security Assistant
127.0.0.1:9392/omp?cmd=start_task&task_id=fa5763cd-8118-4e5e-8882-8b0bebc689f4&overrides=1&next=get_tasks&token=371
Google
BackTrack Linux
Offensive Security
Exploit-DB
Aircrack-ng
SomaFM
Greenbone Security Assistant
Logged in as openvas | Logout
Thu Jul 26 08:45:51 2012 (UTC)
Navigation
Scan Management
Tasks
New Task
Notes
Overrides
Performance
Configuration
Scan Configs
Targets
Credentials
Agents
Escalators
Schedules
Report Formats
Slaves
Administration
Users
NVT Feed
Settings
Help
Contents
About

Results of last operation

Operation: Start Task
Status code: 400
Status message: Task is active already

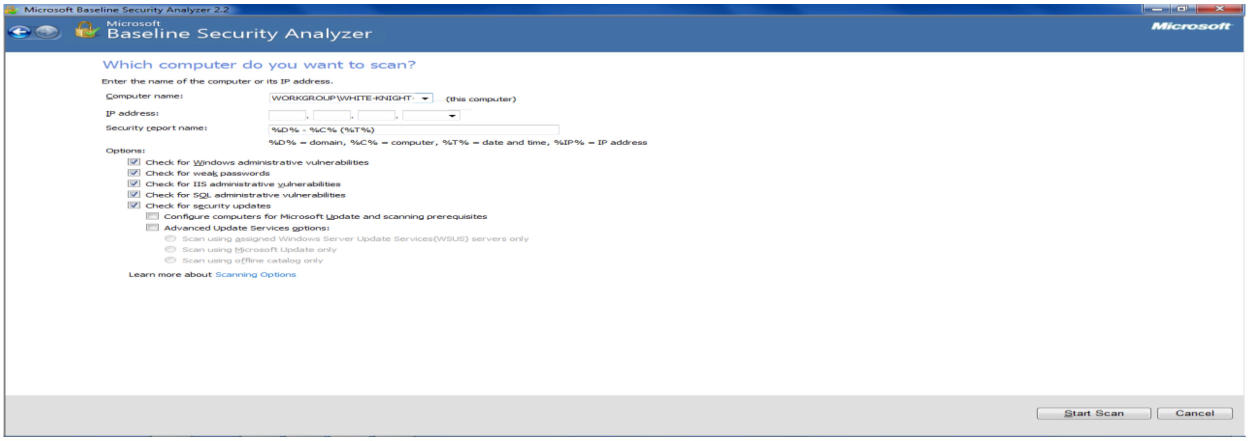
Tasks √No auto-refresh √Apply overrides

Task	Status	Reports			Threat	Trend	Actions
		Total	First	Last			
Windows	1 %	0					

Greenbone Security Assistant (GSA) Copyright 2009-2011 by Greenbone Networks GmbH, www.greenbone.net
root@bt: ~
Greenbone Security D...
Greenbone Security As...

Figure 5. 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.


Microsoft Baseline Security Analyzer 2.2
Microsoft
Baseline Security Analyzer
Microsoft

Which computer do you want to scan?

Enter the name of the computer or its IP address.

Computer name: WORKGROUP\WHITE-KNIGHT (this computer)

IP address: . . .

Security report name: %D% - %C% (%T%)

%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

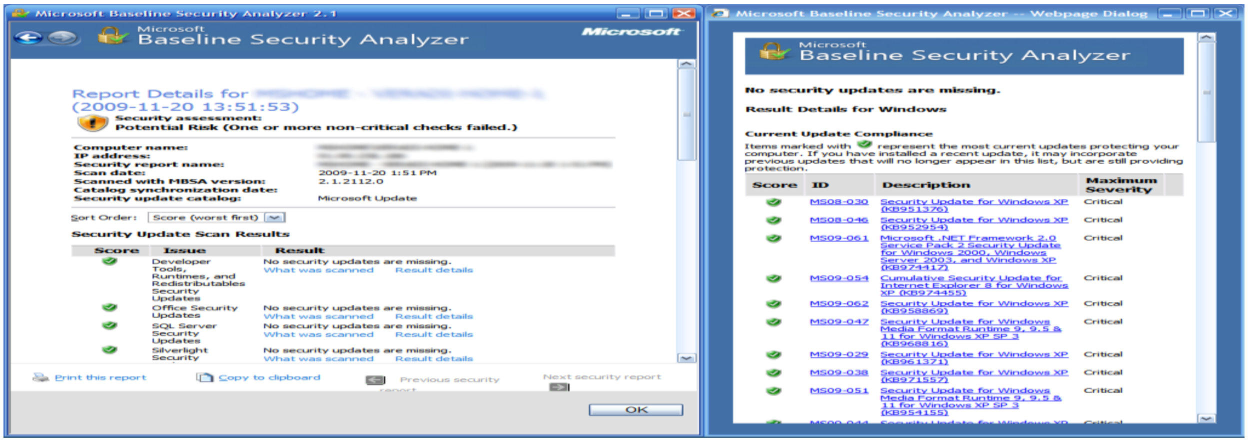
Options:

- ☑ Check for Windows administrative vulnerabilities
- ☑ Check for weak passwords
- ☑ Check for IIS administrative vulnerabilities
- ☑ Check for SQL administrative vulnerabilities
- ☑ Check for security updates
  - □ Configure computers for Microsoft Update and scanning prerequisites
  - □ Advanced Update Services options:
    - ○ Scan using assigned Windows Server Update Services(WSUS) servers only
    - ○ Scan using Microsoft Update only
    - ○ Scan using offline catalog only

Learn more about Scanning Options

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.


Microsoft Baseline Security Analyzer 2.1
Microsoft
Baseline Security Analyzer
Microsoft

Report Details for [redacted] (2009-11-20 13:51:53)

Security assessment:
Potential Risk (One or more non-critical checks failed.)

Computer name:	[redacted]
IP address:	[redacted]
Security report name:	[redacted]
Scan date:	2009-11-20 1:51 PM
Scanned with MBSA version:	2.1.2112.0
Catalog synchronization date:	
Security update catalog:	Microsoft Update

Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
✓	Developer Tools, Runtimes, and Redistributables Security Updates	No security updates are missing. What was scanned Result details
✓	Office Security Updates	No security updates are missing. What was scanned Result details
✓	SQL Server Security Updates	No security updates are missing. What was scanned Result details
✓	Silverlight Security	No security updates are missing. What was scanned Result details

No security updates are missing.

Result Details for Windows

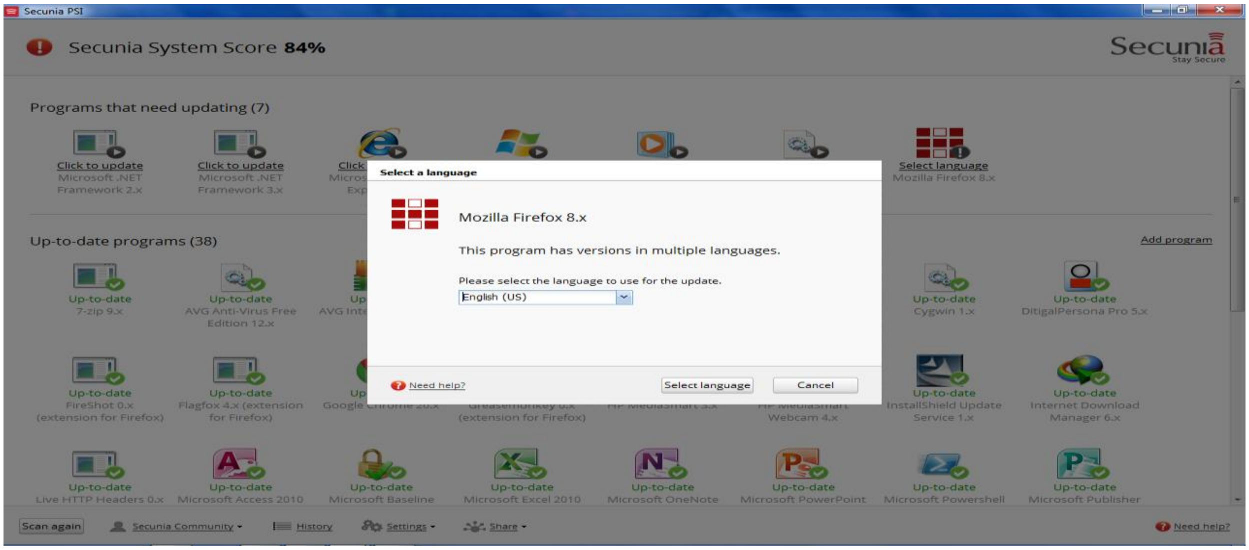
Current Update Compliance

Items marked with ✓ represent the most current updates protecting your computer. If you have installed a recent update, it may incorporate previous updates that will no longer appear in this list, but are still providing protection.

Score	ID	Description	Maximum Severity
✓	MS08-030	Security Update for Windows XP (KB951376)	Critical
✓	MS08-046	Security Update for Windows XP (KB952954)	Critical
✓	MS09-061	Microsoft .NET Framework 2.0 Service Pack 2 Security Update for Windows 2000, Windows Server 2003, and Windows XP (KB974417)	Critical
✓	MS09-054	Cumulative Security Update for Internet Explorer 8 for Windows XP (KB974455)	Critical
✓	MS09-062	Security Update for Windows XP (KB958869)	Critical
✓	MS09-047	Security Update for Windows Media Format Runtime 9, 9.5 & 11 for Windows XP SP 3 (KB968816)	Critical
✓	MS09-029	Security Update for Windows XP (KB961371)	Critical
✓	MS09-038	Security Update for Windows XP (KB971557)	Critical
✓	MS09-051	Security Update for Windows Media Format Runtime 9, 9.5 & 11 for Windows XP SP 3 (KB954155)	Critical
✓	MS09-044	Security Update for Windows XP	Critical

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 System Score **84%**

Select a language

Mozilla Firefox 8.x

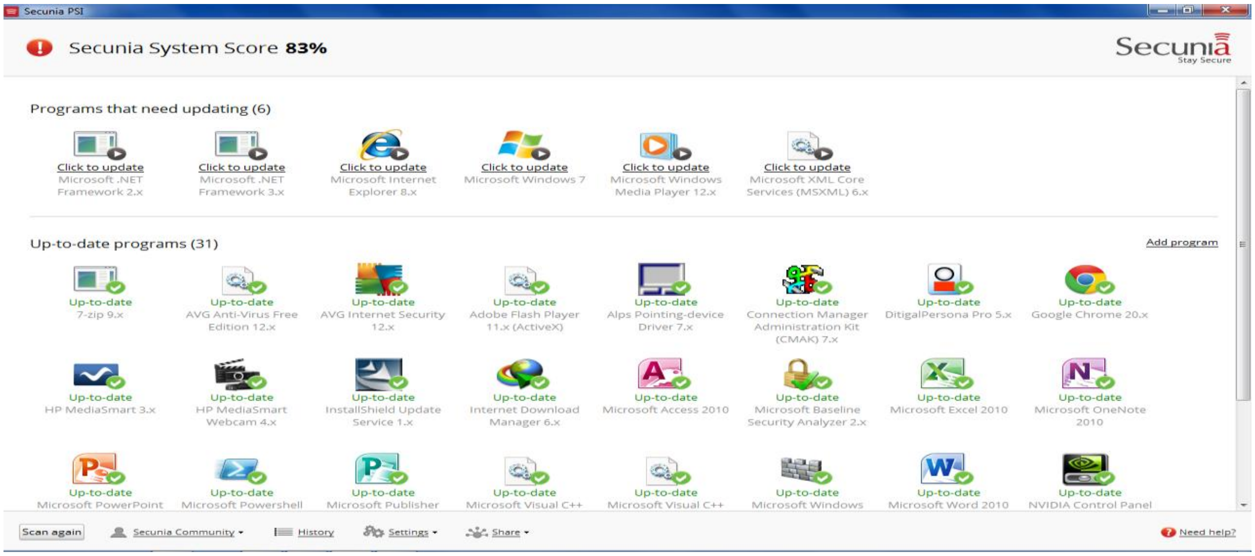
This program has versions in multiple languages.

Please select the language to use for the update.

English (US)

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.



Secunia PSI

Secunia System Score **83%**

Programs that need updating (6)

Click to update
Microsoft .NET Framework 2.x

Click to update
Microsoft .NET Framework 3.x

Click to update
Microsoft Internet Explorer 8.x

Click to update
Microsoft Windows 7

Click to update
Microsoft Windows Media Player 12.x

Click to update
Microsoft XML Core Services (MSXML) 6.x

Up-to-date programs (31)

Up-to-date
7-zip 9.x

Up-to-date
AVG Anti-Virus Free Edition 12.x

Up-to-date
AVG Internet Security 12.x

Up-to-date
Adobe Flash Player 11.x (ActiveX)

Up-to-date
Alps Pointing-device Driver 7.x

Up-to-date
Connection Manager Administration Kit (CMAK) 7.x

Up-to-date
DitigalPersona Pro 5.x

Up-to-date
Google Chrome 20.x

Up-to-date
HP MediaSmart 3.x

Up-to-date
HP MediaSmart Webcam 4.x

Up-to-date
InstallShield Update Service 1.x

Up-to-date
Internet Download Manager 6.x

Up-to-date
Microsoft Access 2010

Up-to-date
Microsoft Baseline Security Analyzer 2.x

Up-to-date
Microsoft Excel 2010

Up-to-date
Microsoft OneNote 2010

Up-to-date
Microsoft PowerPoint

Up-to-date
Microsoft Powershell

Up-to-date
Microsoft Publisher

Up-to-date
Microsoft Visual C++

Up-to-date
Microsoft Visual C++

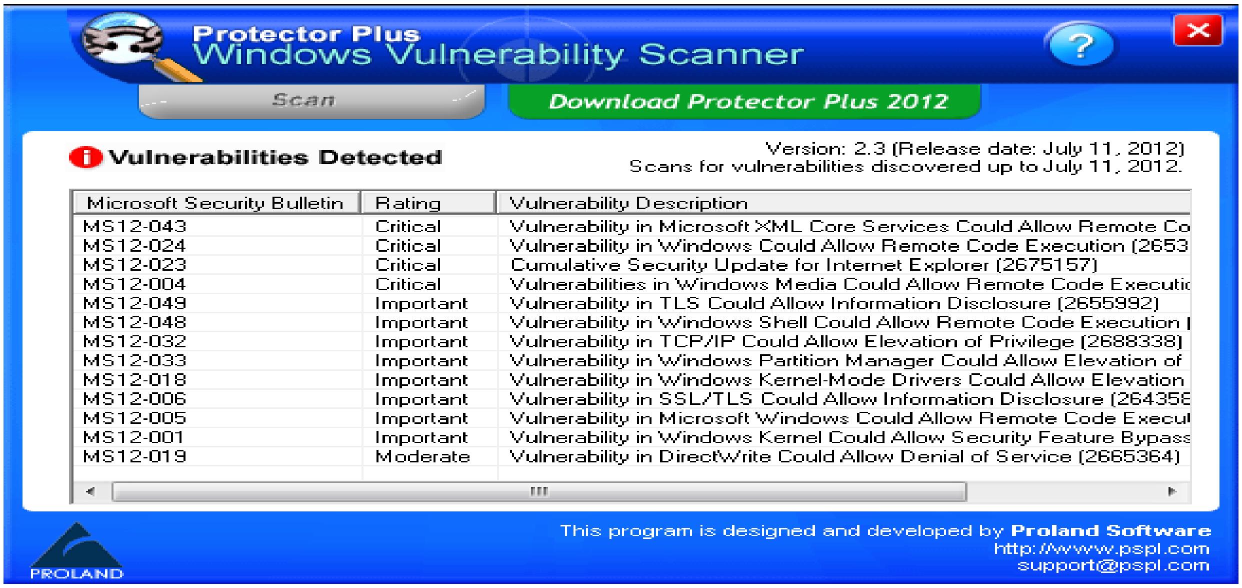
Up-to-date
Microsoft Windows

Up-to-date
Microsoft Word 2010

Up-to-date
NVIDIA Control Panel

Figure 9. Secunia PSI output

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.



Vulnerabilities Detected

Version: 2.3 (Release date: July 11, 2012)
Scans for vulnerabilities discovered up to July 11, 2012.

Microsoft Security Bulletin	Rating	Vulnerability Description
MS12-043	Critical	Vulnerability in Microsoft XML Core Services Could Allow Remote Co
MS12-024	Critical	Vulnerability in Windows Could Allow Remote Code Execution (2653
MS12-023	Critical	Cumulative Security Update for Internet Explorer (2675157)
MS12-004	Critical	Vulnerabilities in Windows Media Could Allow Remote Code Executic
MS12-049	Important	Vulnerability in TLS Could Allow Information Disclosure (2655992)
MS12-048	Important	Vulnerability in Windows Shell Could Allow Remote Code Execution (
MS12-032	Important	Vulnerability in TCP/IP Could Allow Elevation of Privilege (2688338)
MS12-033	Important	Vulnerability in Windows Partition Manager Could Allow Elevation of
MS12-018	Important	Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation
MS12-006	Important	Vulnerability in SSL/TLS Could Allow Information Disclosure (264358
MS12-005	Important	Vulnerability in Microsoft Windows Could Allow Remote Code Execut
MS12-001	Important	Vulnerability in Windows Kernel Could Allow Security Feature Bypass
MS12-019	Moderate	Vulnerability in DirectWrite Could Allow Denial of Service (2665364)

This program is designed and developed by **Proland Software**
http://www.pspl.com
support@pspl.com

Figure 10. Protector Plus WVS result

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

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.