

Vulnerability Assessments



Overview

Introduction to Vulnerability Assessments



Testing Overview



Technical Cyber Security Alerts



Vulnerability Assessments Tools



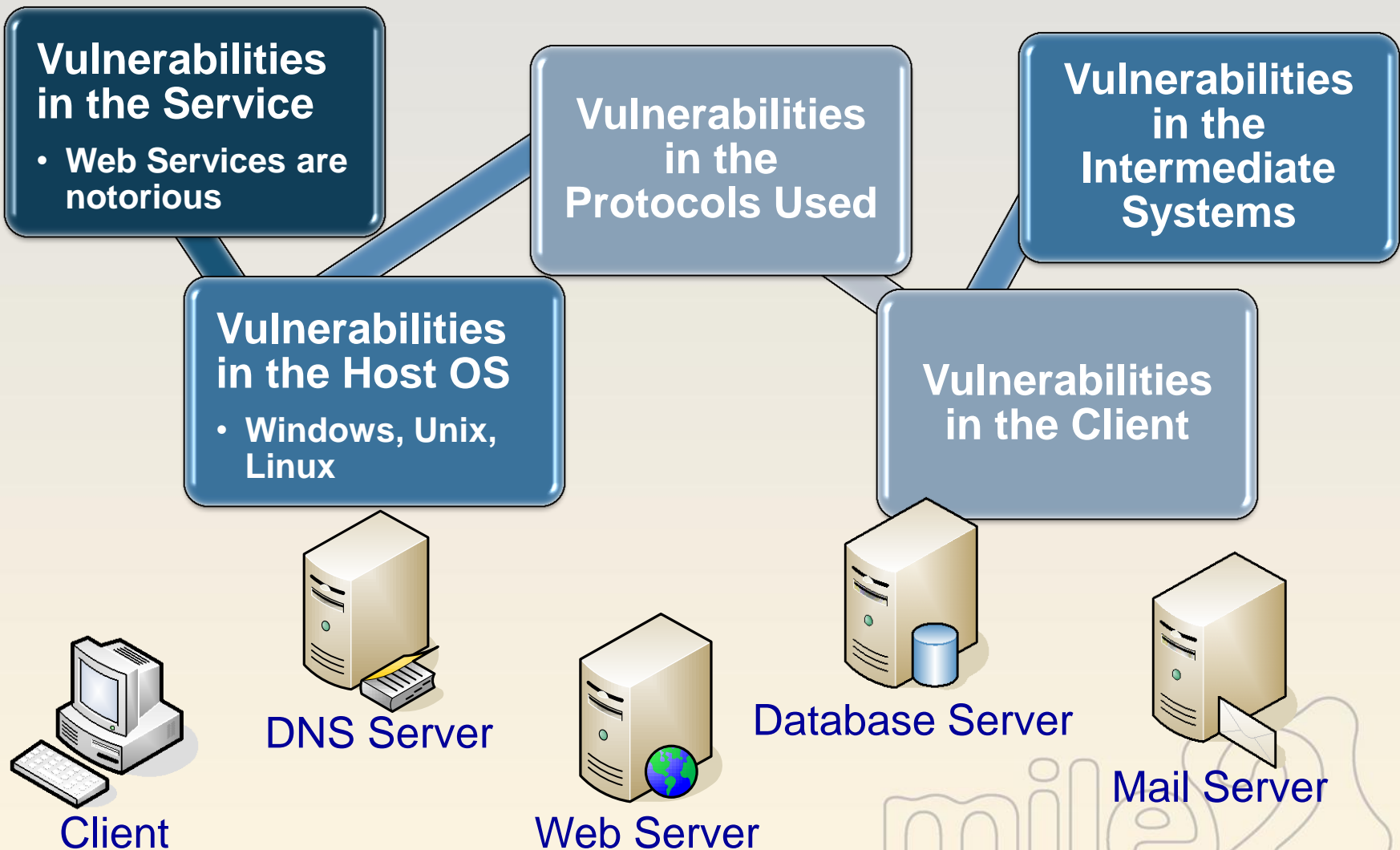
Dealing with the results



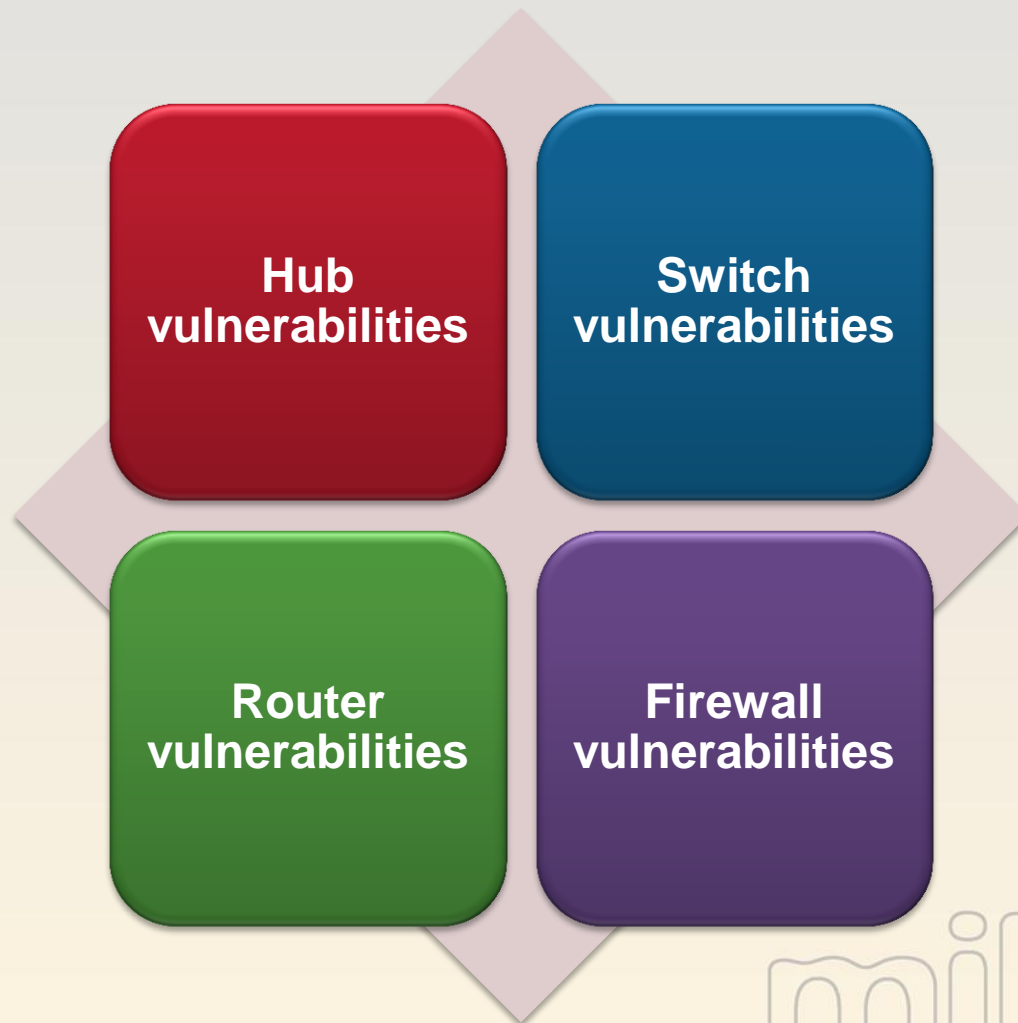
Patch Management



Vulnerabilities in Network Services



Vulnerabilities in Networks



The systematic examination of a system to identify those critical infrastructures or related components that may be at risk from an attack and the determination of appropriate procedures that can be implemented to reduce that risk.

[The] systematic examination of an information system (IS) or product to determine the adequacy of security measures. Identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. [INFOSEC-99]

Vulnerability Assessment Intro

**DON'T rely on Automated tools to do the Pen Test,
as these tools work within a frame work and you may get false results.**



**The Professional Pen Tester will focus on manual methods to confirm
whether the results in the vulnerability assessment report are positive or
negative.**



You can use these tools as a foundation when building your report.



http://www.atis.org/tg2k/_vulnerability_assessment.html

Testing Overview

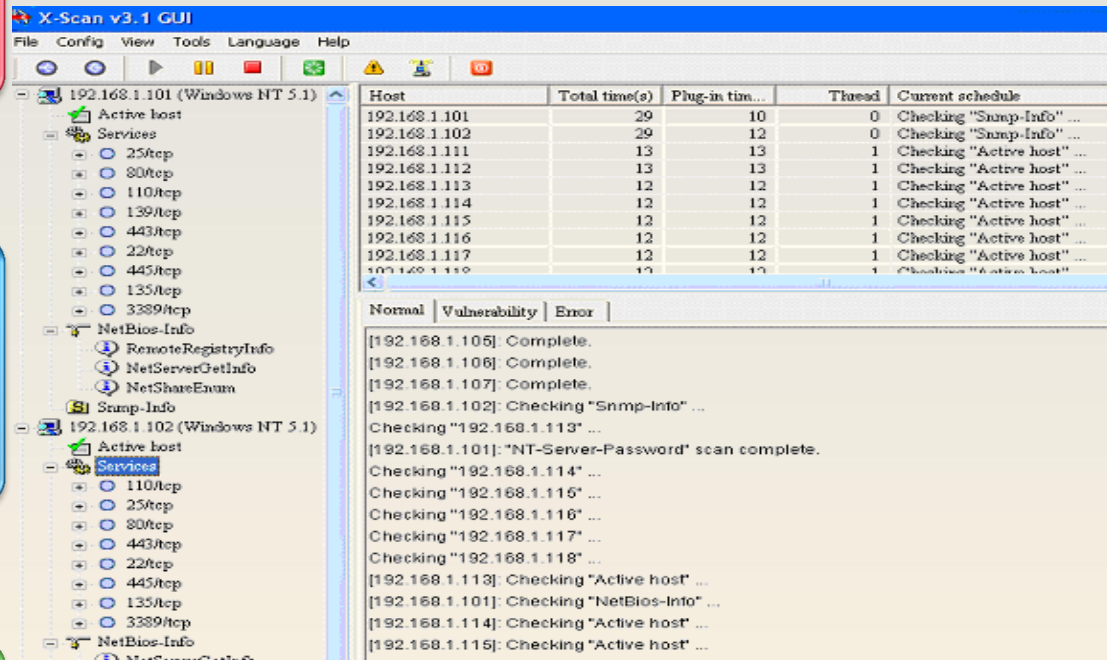
Most automated vulnerability assessment tools have a GUI front end.



You will start off with the target network or an individual specific URL or IP address of the target/s.



Once the assessment tool has generated the results report you will be required to further investigate and mitigate potential weaknesses by means of exploitation.



The U.S National Vulnerability Database (NVD)

<http://nvd.nist.gov/>



The screenshot shows the NVD homepage with a header banner featuring the DHS and NIST logos. The main content area includes a search bar, a 'Welcome to NVD!!' sidebar, and various search filters.

Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of Standards and Technology

National Vulnerability Database

a comprehensive cyber vulnerability resource

[Search CVE](#), [Download CVE](#), [Statistics](#), [CVSS](#), [Vendors](#), [Contact](#), [FAQ](#)

Welcome to NVD!!

NVD is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. It is based on and synchronized with the [CVE](#) vulnerability naming standard.

Search CVE Vulnerability Database ([Perform Advanced Search](#))

Keyword search:

Try a product or vendor name
Try a CVE standard vulnerability name or OVAL query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

Show only vulnerabilities that have the following associated resources:

- ☐ US-CERT [Technical Alerts](#)
- ☐ US-CERT [Vulnerability Notes](#)
- ☐ [OVAL](#) Queries

Vulnerability Research Sites

nvd.nist.gov/

secunia.com/historic_advisories/

cve.mitre.org

www.sans.org/top-cyber-security-risks/

oval.mitre.org/

www.securitywizardry.com/

www.dshield.org/

www.securityfocus.com/

secunia.com/

www.isecom.org/



Vulnerability Scanners

Nessus

- <http://www.nessus.org/>
Linux/Windows | Purchase/Free

SAINT

- <http://www.saintcorporation.com/>
Linux | Purchase

Retina

- <http://www.eeye.com/>
Windows | Purchase

Qualys

- <http://www.qualys.com/>
Windows | Purchase

GFI LANguard

- <http://www.gfi.com/languard/>
Windows | Purchase

MBSA

- <http://www.microsoft.com/mbsa>
Windows | Free



www.nessus.org/nessus/

Agentless Patch, Configuration, Content Auditing.

Server works as a daemon at back end and client is used as a front end.

Test and discovery of known security vulnerabilities published in the security communities.

Nessus vulnerability scanner is designed to identify all the latest vulnerabilities with solutions for known security problems, before a hacker takes advantage of vulnerabilities.



<http://www.nessus.org>

Nessus Report

Nessus : Untitled

File Help

TENABLE

NESSUS 3

Scan

Report

Report:

08/08/12 11:28:45 PM - Default scan policy

Delete

Export...

192.168.2.149

general/tcp

general/icmp

general/udp

domain (53/tcp)

domain (53/udp)

kerberos (88/tcp)

ntp (123/udp)

http (80/tcp)

netbios-ssn (139/tcp)

ldap (389/tcp)

microsoft-ds (445/tcp)

kpasswd (464/tcp)

epmap (135/tcp)

netbios-ns (137/udp)

http-rpc-epmap (593/tcp)

ldaps (636/tcp)

cap (1026/tcp)

unknown (1046/tcp)

unknown (1038/tcp)

blackjack (1025/tcp)

msft-gc-ssl (3269/tcp)

msft-gc (3268/tcp)

Filter...

LDAP allows null bases

Synopsis :

It is possible to disclose LDAP information.

Description :

Improperly configured LDAP servers will allow the directory BASE to be set to NULL. This allows information to be culled without any prior knowledge of the directory structure. Coupled with a NULL BIND, an anonymous user can query your LDAP server using a tool such as 'LdapMiner'

Solution:

Disable NULL BASE queries on your LDAP server

Risk factor :

Medium / CVSS Base Score : 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Nessus ID : [10722](#)

Disconnect

Lets you exploit vulnerabilities found by the scanner with the integrated penetration testing tool, SAINTexploit™.

Shows you how to fix the vulnerabilities and where to begin remediation efforts —with the exploitable vulnerabilities.

Correlates CVE , CVSS, the presence of exploits, and more. Checks for PCI security compliance.

Allows you to design and generate vulnerability assessment reports quickly and easily.

Shows you if your network security is improving over time by using the trend analysis report.

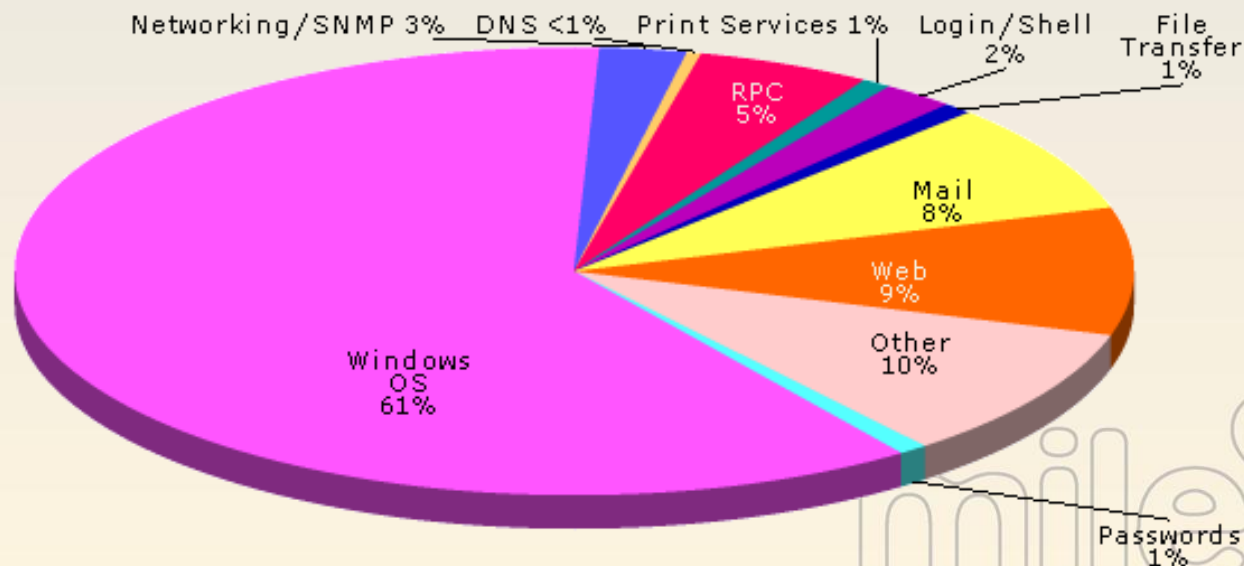
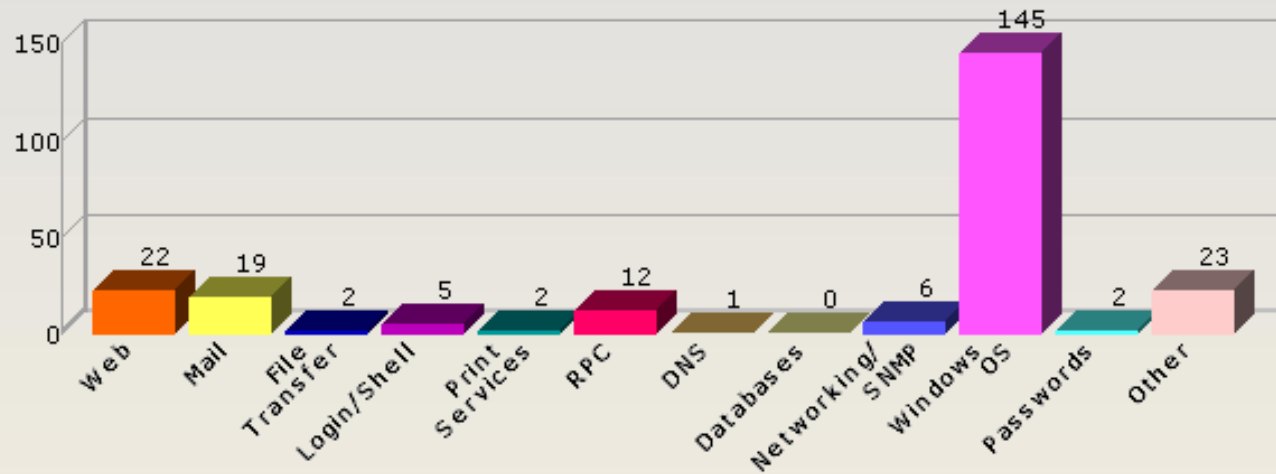
Gives cross references, which can be automatically correlated in reports: CVE, IAVA, OSVDB, BID, CVSS 2.0 (PCI requirement), and SANS/FBI Top 20.

Gives you the option to store the vulnerability data locally or remotely.

Provides automatic updates at least every two weeks or sooner for a critical vulnerability announcement.

Lets you manage and schedule scans across large enterprises with the SAINTmanager™ remote management console.

SAINT – Sample Report



Tool: Retina



<http://www.eeye.com/html/index.html>

Retina® Network Security Scanner, recognized as the industry standard for vulnerability assessment, identifies known network security vulnerabilities and assists in prioritizing threats for remediation.




Featuring fast, accurate, and non-intrusive scanning, users are able to secure their networks against even the most recent of discovered vulnerabilities.



- <http://www.qualys.com/products/overview/>

[Home](#)
[Map](#)
[Scan](#)
[Report](#)
[Remediation](#)
[Preferences](#)
[Support](#)
[Help](#)
[Logout](#)



PERIMETER SCANNING

QualysGuard's external scanners provide fast and efficient perimeter scanning for vulnerabilities in the Qualys vulnerability KnowledgeBase – the industry's largest and most up-to-date database of vulnerability checks. An average of 25 new signature updates are delivered each week, giving users the ability to scan for the latest threats. QualysGuard scans lead the industry in accuracy, delivering 99.997% precision and a false positive rate of less than 0.003%. Even with the comprehensive and accurate scanning, the impact on your network load is minimal due to the inference-based scanning engine that intelligently runs only tests applicable to each host.

Scan

[Launch Scan](#)
[Saved Scans](#)
[Running Scans](#)

<input type="checkbox"/>	View	Asset Group	IPs			
<input type="checkbox"/>		All	10.10.10.1-10.10.10.200, 64.41.134...	203	Edwin Hansen (Manager)	
<input type="checkbox"/>		Corporate	10.10.10.8-10.10.10.96, 64.41.134.6...	90	Edwin Hansen (Manager)	
<input checked="" type="checkbox"/>		Critical Servers	64.41.134.59-64.41.134.61	3	Oleg Kragen (Unit Manager)	
<input type="checkbox"/>		London	10.10.10.1-10.10.10.7	7	Edwin Hansen (Manager)	
<input type="checkbox"/>		New York	10.10.10.156-10.10.10.200, 64.41.13...	48	Edwin Hansen (Manager)	
<input type="checkbox"/>		Qualys Domain		0	Edwin Hansen (Manager)	
<input type="checkbox"/>		Training Lab	10.10.10.156-10.10.10.200, 64.41.13...	48	Steve Sorensen (Scanner)	

☐ Show only my groups



Tool: LANguard

LANguard Network Security Scanner

- Perform a network security audit Smart Reporting
- Complete patch management solution

LANguard Network Security Scanner features

- Report includes: service pack level of the machine, open shares, open ports, services/applications active on the computer, key registry entries, weak passwords, users and groups
- Shuts down unnecessary ports, closes shares, installing service packs and hot fixes, detects potential Trojans installed on users' workstations
- GFI LANguard N.S.S. identifies well-known services (such as www/FTP/telnet/SMTP) and also supports "banner grabbing", that is, it queries the port for an application name

www.gfi.com/lannetscan/

Microsoft Baseline Security Analyzer (MBSA) is an easy-to-use tool designed for the IT professional that helps small- and medium-sized businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance.

Users who primarily have:



- Windows 2000+ SP3 and later
- Office XP+ and later
- Exchange 2000+ and later
- SQL Server 2000 SP4+
- Other products supported by Microsoft Update in their environment should switch to MBSA 2.0 today.

<http://www.microsoft.com/mbsa>

MBSA Scan Report



Baseline Security Analyzer

Microsoft Baseline Security Analyzer

- Welcome
- Pick a computer to scan
- Pick multiple computers to scan
- Pick a security report to view
- View a security report**

See Also

- Microsoft Baseline Security Analyzer Help
- About Microsoft Baseline Security Analyzer
- Microsoft Security Web site

Actions

-  [Print](#)
-  [Copy](#)

View security report

Sort Order: [Score \(worst first\)](#)

Security Update Scan Results

Score	Issue	Result
	Windows Security Updates	9 security updates are missing, are out of date, or could not be confirmed. What was scanned Result details How to correct this
	Office Security Updates	2 security updates are missing. What was scanned Result details How to correct this
	IIS Security Updates	1 critical security updates are missing. What was scanned Result details How to correct this
	Windows Media Player Security Updates	1 security updates are out-of-date. What was scanned Result details How to correct this
	MDAC Security Updates	1 security updates are out-of-date. What was scanned Result details How to correct this
	MSXML Security Updates	2 security updates are out-of-date. What was scanned Result details How to correct this

Windows Scan Results

Vulnerabilities

Score	Issue	Result
	Internet Connection Firewall	1 of 2 network connections either do not have Internet Connection Firewall. What was scanned Result details How to correct this
	Local Account Password Test	No user accounts have simple passwords. What was scanned Result details
	Automatic	Updates are automatically downloaded and installed on this computer.

Dealing with Assessment Results

Many security companies will simply use the results from the automated vulnerability assessment tools in a Penetration Test Report and charge in the region of \$25K for this.



Whereas the Professional Penetration Testing teams will take the results and actually attempt to **PENETRATE** the vulnerability results from the scans, confirming whether the systems are exploitable using hacker methods.



Be sure to stay within the Penetration Testing Scope of work (Boundaries)



Written authorization to exploit such systems is imperative and the client may specify that certain systems are out of bounds, as far as exploitation is concerned.



Shavlik HFNetChkPro™

Powerful, intuitive patch management. Manage updates with ease. With its intuitive interface, you're in complete control!

Built on the industry standard HFNetChk™ scanning engine used by Microsoft in its popular Microsoft Baseline Security Analyzer (MBSA). Both HFNetChk™ and MBSA were developed by Shavlik Technologies. Used worldwide by corporations including Microsoft, educational institutions, government agencies, and others to assure proper security patch management.

<http://www.shavlik.com/hfnetchkpro.aspx>

Other Patch Management Options



Update Expert

www.lyonware.co.uk/Update-Expert.htm

Windows Server Update Services

www.microsoft.com/msus/



GFI LANguard

www.gfi.com

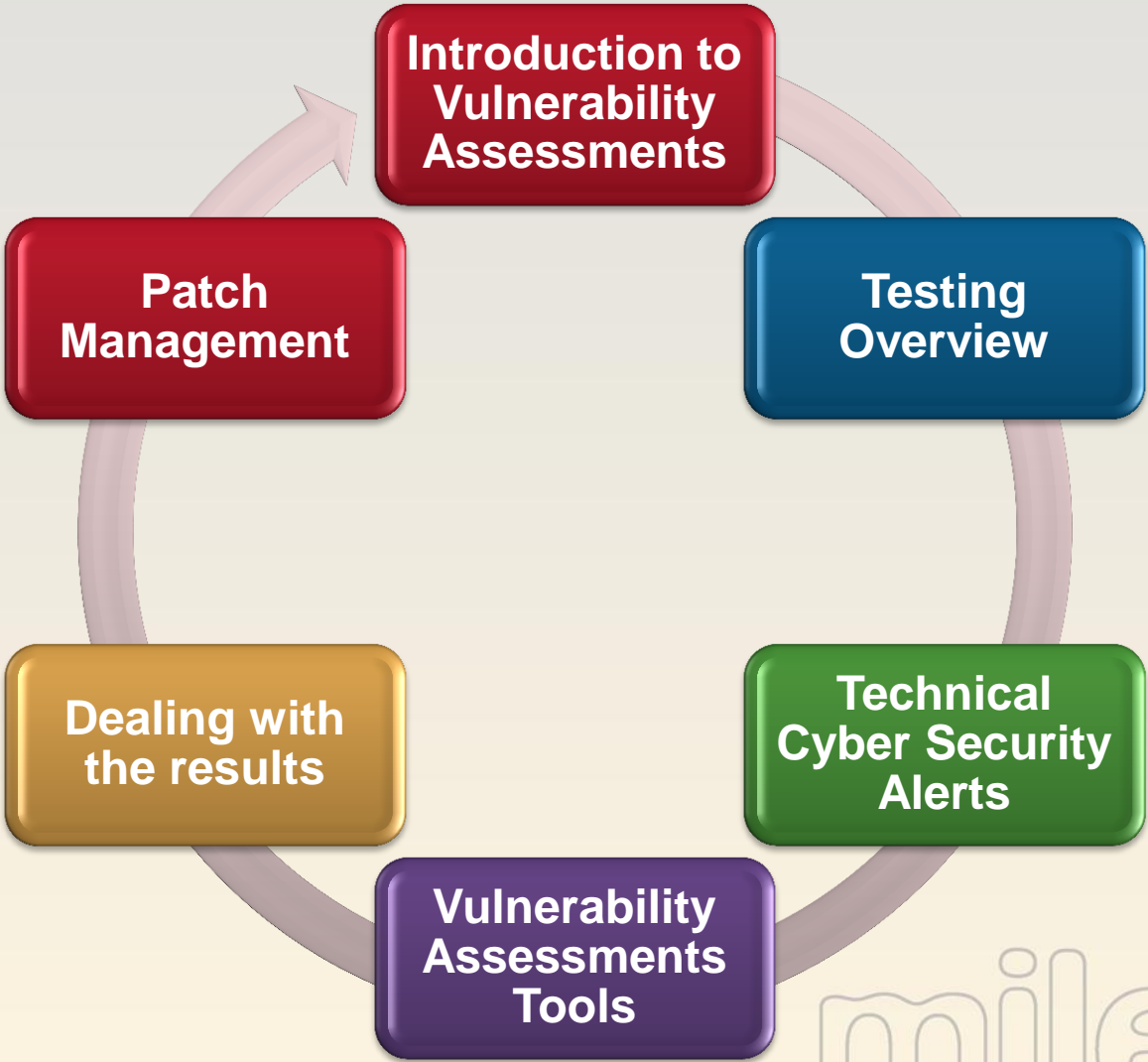


Kaseya

www.kaseya.com



Review



Module 6 Lab Vulnerability Assessment

