secure auditor

Audit Report

Vulnerability categorization by machine in

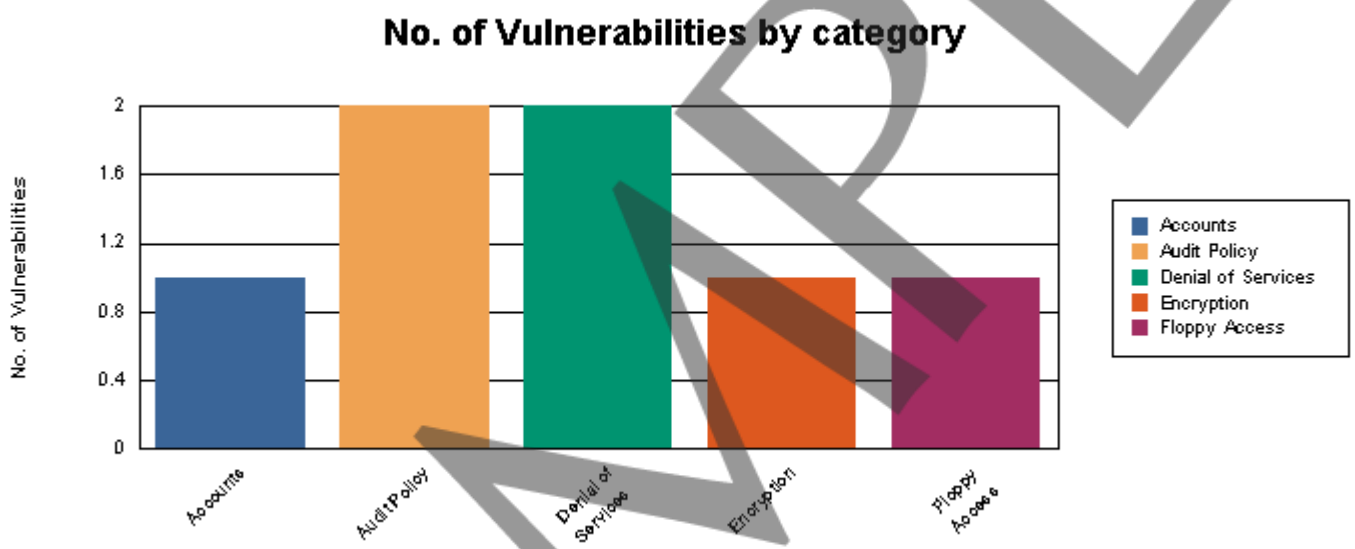
Report Generated Time: 10/13/2011 At 6:10:25PM

Audit Name: : WinAudit(Oct 13 2011 6:07PM)
Description: : Windows Audit Report
IP Count : 1
IPs: : 192.168.100.40

Vulnerability categorization by machine in Specified time

Report generated on 13-Oct-2011 at 6:10:25PM

Windows based machines are the weakest link in the enterprise security chain and a curious company takes care of every aspect of security. A security scan was performed on Windows based machine/s on your network. This report will give you a complete picture of the security pasture and designed to show a wide ranging description of vulnerabilities discovered in this audit. This report covers the maximum researched and checked information about a vulnerability including the aspect, ways and areas sensitive or unsafe which is usually adapted by attackers. It is recommended to take a thorough review of the vulnerabilities discovered.



Vulnerability categorization by machine in Specified time

Category	**Accounts**		
Audit Performed :	**WinAudit(Oct 13 2011 6:07PM)**	**Selected Profile:**	**TestWindows**
Machine IP	**192.168.100.40**	**Machine Port**	**139**

Risk Level :	Medium
Name	**Force UnLockLogon Not Enabled**

Description

ForceUnlockLogon controls whether a full login should be performed when a workstation is unlocked or a password is used with the screen saver. Normally Windows does not check whether the account has been locked out first. Without the ForceUnlockLogon enabled, the default unlocking behavior will still accept a valid password and unlock the screen saver, despite the account being locked out. Also without the ForceUnlockLogon enabled, a successful break-in by someone guessing or knowing your password will not register an event in the Security event log. For added protection, enable the ForceUnlockLogon option. Enabling the ForceUnlockLogon forces a log on instead of relying on the hash of the password that is stored in the Winlogon service.

2270	**Vulnerability/ies of type**	**Accounts**	
Category	**Audit Policy**		
Audit Performed :	**WinAudit(Oct 13 2011 6:07PM)**	**Selected Profile:**	**TestWindows**
Machine IP	**192.168.100.40**	**Machine Port**	**139**

Risk Level :	High
Name	**Audit Policy: Audit Logon Events Failure**

Description

If you audit for logon events - every time that a user logs on or off a computer - an event is generated in the security log of the computer where the logon attempt occurs. Also, when a user connects to a remote server, a logon event is generated in the security log of the remote server. Logon events are created when the logon session and token are created or destroyed respectively. Logon events can be useful to track attempts to logon interactively at servers or to investigate attacks launched from a particular computer.

Risk Level :	Low
Name	**Audit Policy: Audit privilege use Failure**

Description

The audit log "use of user rights" is not tracking Failure. Privilege auditing records when any user rights are granted to a user or process. These events appear in the Security Log. Without audit logs, you cannot track users who have gained unauthorized access. Auditing will enable detection if a potential intruder is launching an attack.This security setting determines whether to audit each instance of a user exercising a user right. Failure audits generate an audit entry when the exercise of a user right fails. Default: Audits are not generated for use of the following user rights, even if success audits or failure audits are specified for "Audit privilege use".

- Bypass traverse checking
- Debug programs
- Create a token object
- Replace process level token

Vulnerability categorization by machine in Specified time

- Generate security audits
- Back up files and directories
- Restore files and directories

2216	Vulnerability/ies of type	Audit Policy
Category	**Denial of Services**	
Audit Performed :	**WinAudit(Oct 13 2011 6:07PM)**	**Selected Profile:** **TestWindows**
Machine IP	**192.168.100.40**	**Machine Port** **139**

Risk Level : High

Name **Denial of Service Attacks: TCPMaxPortsExhausted**

Description

In a SYN flood attack, the attacker sends a continuous stream of SYN packets to a server, and the server leaves the half-open connections open until it is overwhelmed and no longer is able to respond to legitimate requests.Determines how many connection requests the system can refuse before TCP/IP initiates SYN flooding attack protection. The system must refuse all connection requests when its reserve of open connection ports runs out. This entry is used only when SYN flooding attack protection is enabled on this server, that is, the value of the SynAttackProtect entry is 1 and the value of the TcpMaxConnectResponseRetransmissions entry is at least 2).This entry establishes one of three configurable thresholds that, if exceeded, trigger TCP's SYN attack flooding protection feature. Because SYN flooding often consumes all reserved connection ports, TCP interprets an elevated number connection refusals and a depleted port reserve as a symptom of SYN flooding.

Risk Level : Medium

Name **NetBIOS: Netbios DoS Name Spoofing Not Ignored**

Description

NetBIOS is a protocol used by computers to access each other over a network. When you use Network Neighborhood you are making use of NetBIOS. The NetBIOS protocol is unauthenticated which means that each computer inherently trusts each other computer on the network. One computer can send a false message to another computer insisting that its name is not unique. In this situation the target computer may become unavailable to other computers on the network (or Internet). By setting this value to 'Enabled' the operating system ignores messages suggesting that its name is not unique.

2260	Vulnerability/ies of type	Denial of Services
Category	**Encryption**	
Audit Performed :	**WinAudit(Oct 13 2011 6:07PM)**	**Selected Profile:** **TestWindows**
Machine IP	**192.168.100.40**	**Machine Port** **139**

Risk Level : Medium

Name **Microsoft network server: Digitally sign communications (if client agrees)**

Description

This security setting determines whether the SMB server will negotiate SMB packet signing with clients that request it.The server message block (SMB) protocol provides the basis for Microsoft file and print sharing and many other networking operations, such as remote Windows administration. To prevent man-in-the-middle attacks that modify SMB packets in transit, the SMB protocol supports the digital signing of SMB packets. This

Vulnerability categorization by machine in Specified time

policy setting determines whether the SMB server will negotiate SMB packet signing when an SMB client requests it.

2369	**Vulnerability/ies of type Encryption**		
Category	**Floppy Access**		
Audit Performed :	**WinAudit(Oct 13 2011 6:07PM)**	**Selected Profile:**	**TestWindows**
Machine IP	**192.168.100.40**	**Machine Port**	**139**
Risk Level :	Medium		
Name	**Registry: Allocate floppies.**		

Description

By default, Windows allows any program to access files on floppy disks, possible leaving sensitive data exposed. In a highly secure environment, only the person interactively logged on should have access to the floppy drives, and not allow remote users access to the floppy drive at the same time. A floppy drive can be restricted (allocated) to an interactive user and not be shared by other users or programs on the system. This allows the interactive user to write sensitive information to the floppy drives without others seeing or modifying that data. When no one is logged on, the floppy drive can be accessed over the network.

2279	**Vulnerability/ies of type Floppy Access**
Total Vulnerabilities:	**7**