



secure auditor

Audit Report

Vulnerability Details and Their Solutions

Report Generated Time: 10/13/2011 At 6:08:09PM

Audit Name: : WinAudit(Oct 13 2011 6:07PM)

Description: : Windows Audit Report

IP Count : 1

IP(s): : 192.168.100.40

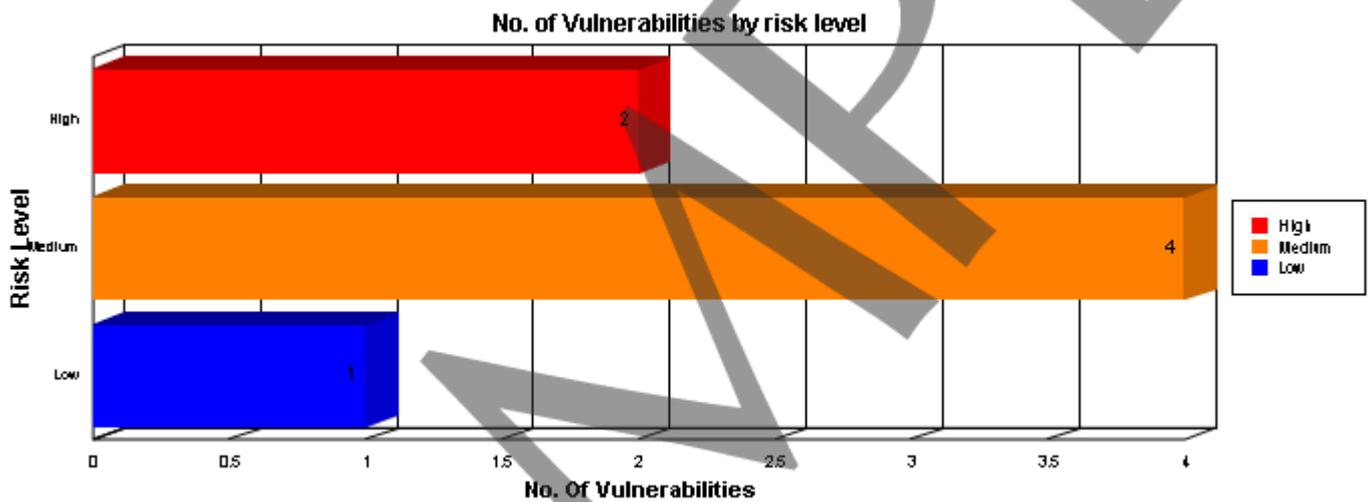




Vulnerability Details and Their Solutions

Report generated on 13-Oct-2011 At 6:08:09PM

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 details and their solutions

Summary Information :

Machine : 192.168.100.40		Selected Profile: TestWindows
Risk Level	Number of Vulnerabilities	Percentage
High	2	28.57%
Medium	4	57.14%
Low	1	14.29%
Vulnerabilities on 192.168.100.40	7	100.00%
Total Vulnerabilities:	7	100.00%

SAMPLE



Vulnerability details and their solutions

Machine	192.168.100.40
Risk Level	High
Selected Profile: TestWindows	

Vulnerability: **Audit Policy: Audit Logon Events Failure**

Vulnerability's Occurrence::	1	Machine	192.168.100.40	Port:	139
Risk Level	High	Product Name	Windows	Vendor	Microsoft
Versions	Windows 2000 or Above	Test Type Name	Audit		

Vulnerability Information:

Category Name Audit Policy

Overview: The purpose of auditing is to record certain type of actions to a log, for system administrators to review and detect unauthorized activity. Audit logs helps a lot while performing forensics. This particular event prevents from the potential threat of Random attempts to hack an account. By creating this log every bad attempt to log into an account will be maintained in the log and will help administrators in performing either forensics or monitor suspicious activities.

Vulnerability References:

References <http://technet2.microsoft.com/windowsserver/en/library/e104c96f-e243-41c5-aaea-d046555a079d1033.mspx?mfr=true>
 BREAK <http://www.rippletech.com/PDF/New/SOX/Auditing%20Best%20Practices.pdf>

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.

Solution

For Windows XP:

1. Go to Start > Control Panel > Administrative Tools > Local Security Policy > Local Policies
2. In Local Policies select 'Audit Policy'
3. In the right Pane double click 'Audit account logon events'
4. A dialogue box will appear
5. Check the 'Failure' box and Click OK.

For Windows 2000/NT:

1. Go to 'Start > Settings > Control Panel > Administrative Tools > Local Security Policy > Local Policies > Audit Policy'.
2. Double click on "Audit account logon events" and under the "Audit these attempts" local policy setting,
3. Check the "Failure" box Click OK.

For Windows Server 2003

1. Within the Group Policy Object Editor Go to Computer Configuration > Windows Settings > Local Policies > Audit Policy
2. Double click on "Audit account logon events" and under the "Audit these attempts" local policy setting,
3. Check the "Failure" box Click OK.

Vulnerability Specifications: :

[ObjectName] = AuditCategoryLogon
 [Failure] = 0
 [NoAuditing] = 1

Vulnerability details and their solutions

Vulnerability: Denial of Service Attacks: TCPMaxPortsExhausted

Vulnerability's Occurrence::	1	Machine	192.168.100.40	Port:	139
Risk Level	High	Product Name	Windows	Vendor	Microsoft
Versions	Windows 2000 or Above	Test Type Name	Audit		

Vulnerability Information:

Category Name Denial of Services

Overview: Denial of Service attacks are difficult to defend against. One approach is to harden the TCP/IP stack on a Windows 2000 server or workstation to help prevent DoS attacks. By default, the TCP/IP stack is configured to handle normal traffic and to be robust under normal working conditions. If a Windows 2000 server or workstation is going to be exposed to the Internet, the TCP/IP stack should be reconfigured to handle the various TCP/IP protocol attacks. The TcpMaxPortsExhausted registry entry defines the number of dropped SYN requests, after which the protection against SYN attacks starts to operate.

Vulnerability References:

References <http://msdn2.microsoft.com/en-us/library/aa302363.aspx>

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.

Solution

- Go to 'Start | Run' and enter "Regedit".
- From the Registry Editor navigate to the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
- Create new DWORD value, or modify the existing value, called "TCPMaxPortsExhausted" and set it 5.

Note: Restart Windows for the change to take effect.

Disclaimer: Modifying the registry can cause serious problems that may require you to reinstall your operating system. We cannot guarantee that problems resulting from modifications to the registry can be solved. Use the information provided at your own risk.

Vulnerability Specifications: :

HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\TCPMaxPortsExhausted (Key does not exists)



Vulnerability details and their solutions

Risk Level Medium **Selected Profile:** TestWindows

Vulnerability: Force UnlockLogon Not Enabled

Vulnerability's Occurrence:: 1 **Machine** 192.168.100.40 **Port:** 139

Risk Level Medium **Product Name** Windows **Vendor** Microsoft

Versions Windows 2000 or Above **Test Type Name** Audit

Vulnerability Information:

Category Name Accounts

Overview: When a user logs on to a computer, the Winlogon Service stores a hash of the user's password for future unlock attempts. When the user attempts to unlock the workstation, this stored copy of the password is verified. If the password entered at the unlock dialog request and stored hash match, the workstation is unlocked. If the password entered does not match the stored hash, the workstation attempts to logon (authenticate the password). If the logon process succeeds, the local hash is updated with the new password. If the logon process is unsuccessful, the unlock process is also unsuccessful.

Vulnerability References:

References <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q188700>

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.

Solution

For WIN2K

Change The Force Loggoff Setting.

- a. Go to 'Start | Settings | Control Panel | Administrative Tools | Local Security Policy | Local Policies | Security Options .
- b. Double click on the "Automatically logoff users when logon time expires (Local) " object in the right-hand details pane to open the corresponding Security Policy Setting dialog window.
- c. Set the local policy setting to Enabled.

For WINXP And Above

Change The Force Loggoff Setting.

- a. Go to 'Start | Settings | Control Panel | Administrative Tools | Local Security Policy | Local Policies | Security Options .
- b. Double click on the "Network Security: Force logoff when logon time expires" object in the right-hand details pane to open the corresponding Security Policy Setting dialog window.
- c. Set the local policy setting to Enabled.

Vulnerability Specifications: :

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ForceUnlockLogon = 0



Vulnerability details and their solutions

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

Vulnerability's Occurrence::	1	Machine	192.168.100.40	Port:	139
Risk Level	Medium	Product Name	Windows	Vendor	Microsoft
Versions	Windows 2000 or Above	Test Type Name	Audit		

Vulnerability Information:

Category Name Encryption

Overview: Determines if the SMB server performs SMB packet signing.

Vulnerability References:

References <http://technet2.microsoft.com/WindowsServer/en/Library/9842e709-0583-4367-8618-ee7edaf8d2f61033.msp>

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

Solution

- a. Go to 'Start | Settings | Control Panel | Administrative Tools | Local Security Policy | Local Policies | Security Options'.
 - b. Double click on Security Option "Microsoft network server: Digitally sign communications (if client agrees)".
 - c. Set the local security policy to Enabled.
- Note: Restart Windows for the change to take effect.

Vulnerability Specifications: :

HKLM\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature = 0



Vulnerability details and their solutions

Vulnerability: NetBIOS: Netbios DoS Name Spoofing Not Ignored

Vulnerability's Occurrence::	1	Machine	192.168.100.40	Port:	139
Risk Level	Medium	Product Name	Windows	Vendor	Microsoft
Versions	Windows 2000 or Above	Test Type Name	Audit		

Vulnerability Information:

Category Name Denial of Services

Overview: This vulnerability results because the NetBIOS over TCP/IP (NBT) protocols specified in RFCs 1001 and 1002 are unauthenticated and allow machines on a network to help manage their peers. The protocols are correctly implemented in Windows NT 4.0 and Windows 2000, but, by design, they are vulnerable to misuse and spoofing. This could allow any machine on a network to spoof a WINS server and send a name conflict or name release datagram to another machine, thereby causing the machine to abandon its name and be unresponsive to requests for service.

Vulnerability References:

References <http://support.microsoft.com/default.aspx?scid=kb;en-us;324270>
<http://www.tcpiq.com/tcplQ/DenialOfServiceAttack/>

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.

Solution

- a. Go to 'Start | Run' and enter "Regedit".
- b. From the Registry Editor navigate to the registry key HKLM\System\CurrentControlSet\Services\Netbt\Parameters
- c. Create new DWORD value, or modify the existing value, called "NoNameReleaseOnDemand" and set it 1.

Note: Restart Windows for the change to take effect.

Disclaimer: Modifying the registry can cause serious problems that may require you to reinstall your operating system. We cannot guarantee that problems resulting from modifications to the registry can be solved. Use the information provided at your own risk.

Vulnerability Specifications :

HKLM\System\CurrentControlSet\Services\Netbt\Parameters\NoNameReleaseOnDemand (Key does not exists)

Vulnerability details and their solutions

Vulnerability: Registry: Allocate floppies.

Vulnerability's Occurrence::	1	Machine	192.168.100.40	Port:	139
Risk Level	Medium	Product Name	Windows	Vendor	Microsoft
Versions	Windows 2000 or Above	Test Type Name	Audit		

Vulnerability Information:

Category Name Floppy Access

Overview: A Windows NT system does not restrict access to floppy disk drive. This policy determines whether a Floppy is accessible to both local and remote users simultaneously. If this policy is enabled, it allows only the interactively logged – on user to access removable Floppy media. If this policy is enabled and no one is logged on interactively, the Floppy drive can be accessed over the network

Vulnerability References:

References <http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/regentry/58527.msp?mfr=true>

Description

By default, Windows allows any program to access files on floppy disks, possibly 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.

Solution

- Go to 'Start | Run' and enter "Regedit".
- From the Registry Editor navigate to the registry key HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
- Create new REG_SZ value, or modify the existing value, called "AllocateFloppies" and set it to 1.

Note: Restart Windows for the change to take effect.

Disclaimer: Modifying the registry can cause serious problems that may require you to reinstall your operating system. We cannot guarantee that problems resulting from modifications to the registry can be solved. Use the information provided at your own risk.

Or

- Go to 'Start | Settings | Control Panel | Administrative Tools | Local Security Policy | Local Policies | Security Options'.
- Double click on Security Option "Devices: Restrict floppy access to locally logged-on users only".
- Set the local policy setting to Enabled.

Vulnerability Specifications :

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies = 0



Vulnerability details and their solutions

Risk Level **Low** **Selected Profile:** TestWindows

Vulnerability: **Audit Policy: Audit privilege use Failure**

Vulnerability's Occurrence:: 1 **Machine** 192.168.100.40 **Port:** 139

Risk Level Low **Product Name** Windows **Vendor** Microsoft

Versions Windows 2000 or Above **Test Type Name** Audit

Vulnerability Information:

Category Name Audit Policy

Overview: Determines whether to audit each instance of a user exercising a user right. If you define this policy setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Failure audits generate an audit entry when the exercise of a user right fails.

Vulnerability References:

References <http://technet2.microsoft.com/windowsserver/en/library/ee2f85ac-e3fb-4a24-b133-8c7dfc5cee81033.aspx?mfr=true>

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

Solution

- a. Go to 'Start | Settings | Control Panel | Administrative Tools | Local Security Policy | Local Policies | Audit Policy'.
- b. Double click on "Audit privilege use" and under the "Audit these attempts" local policy setting,
- c. Check the "Failure" box Click OK.

Vulnerability Specifications:

[ObjectName] = AuditCategoryPrivilegeUse
 [Failure] = 0
 [NoAuditing] = 1
