Windows 操作系统安全加固

1、IP 协议安全配置

1.1 IP 协议安全

启用 SYN 攻击保护

a. 指定触发SYN洪水攻击保护所必须超过的TCP连接请求数阈值为 5。

b. 指定处于 SYN_RCVD 状态的 TCP 连接数的阈值为 500。

c. 指定处于至少已发送一次重传的 SYN_RCVD 状态中的 TCP 连接数的阈值为 400。

操作步骤

打开 注册表编辑器，根据推荐值修改注册表键值。

Windows Server 2012

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect

推荐值：2

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen

推荐值：500

Windows Server 2008

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SynAttackProtect

推荐值：2

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpMaxPortsExhausted

推荐值：5

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpMaxHalfOpen

推荐值：500

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpMaxHalfOpenRetried

推荐值：400

2、文件权限

2.1 共享文件夹及访问权限

2.1.1 关闭默认共享

非域环境中，关闭Windows硬盘默认共享，例如C$，D$。

操作步骤

打开 注册表编辑器，根据推荐值修改注册表键值。

注意： Windows Server 2012 版本已默认关闭Windows硬盘默认共享，且没有该注册表键值。

HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer

推荐值： 0

2.1.2 共享文件夹授权访问

每个共享文件夹的共享权限，只允许授权的帐户拥有共享此文件夹的权限。

操作步骤

每个共享文件夹的共享权限仅限于业务需要，不要设置成为 Everyone。打开 控制面板 > 管理工具 > 计算机管理，在 共享文件夹 中，查看每个共享文件夹的共享权限。

3、服务安全

3.1 禁用 TCP/IP 上的 NetBIOS

禁用TCP/IP上的NetBIOS协议，可以关闭监听的 UDP 137（netbios-ns）、UDP 138（netbios-dgm）以及 TCP 139（netbios-ssn）端口。

操作步骤

在 计算机管理 > 服务和应用程序 > 服务 中禁用 TCP/IP NetBIOS Helper 服务。

在网络连接属性中，双击 Internet协议版本 4（TCP/IPv4），单击 高级。在 WINS 页签中，进行如下设置:

a. 禁用不必要的服务

b. 禁用不必要的服务，请参考:

服务名称	建议
DHCP Client	如果不使用动态IP地址，就禁用该服务
Background Intelligent Transfer Service	如果不启用自动更新，就禁用该服务
Computer Browser	禁用
Diagnostic Policy Service	手动
IP Helper	禁用。该服务用于转换IPv6 to IPv4
Print Spooler	如果不需要打印，就禁用该服务
Remote Registry	禁用。Remote Registry主要用于远程管理注册表
Server	如果不使用文件共享，就禁用该服务。禁用本服务将关闭默认共享，如ipc$、admin$和c$等
TCP/IP NetBIOS Helper	禁用
Windows Remote Management (WS-Management)	禁用
Windows Font Cache Service	禁用
WinHTTP Web Proxy Auto-Discovery Service	禁用
Windows Error Reporting Service	禁用

4、安全选项

4.1 启用安全选项

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 本地策略 > 安全选项 中，进行如下设置:

安全选项	配置内容
交互式登录: 试图登录的用户的消息标题	注意
交互式登录: 试图登录的用户的消息文本	内部系统只能因业务需要而使用，经由管理层授权。 管理层将随时监测此系统的使用。
Microsoft 网络服务器: 对通信进行数字签名(如果客户端允许)	启用
Microsoft 网络服务器: 对通信进行数字签名(始终)	启用
Microsoft 网络客户端: 对通信进行数字签名(如果服务器允许)	启用
Microsoft 网络客户端: 对通信进行数字签名(始终)	启用
网络安全: 基于 NTLM SSP 的(包括安全 RPC)服务器的最小会话安全	要求 NTLMv2 会话安全 要求 128 位加密
网络安全: 基于 NTLM SSP 的(包括安全 RPC)客户端的最小会话安全	要求 NTLMv2 会话安全 要求 128 位加密
网络安全: LAN 管理器身份验证级别	仅发送 NTLMv2 响应\拒绝 LM & NTLM
网络访问: 不允许 SAM 帐户的匿名枚举	启用（默认已启用）
网络访问: 不允许 SAM 帐户和共享的匿名枚举	启用
网络访问 : 可匿名访问的共享	清空（默认为空）
网络访问 : 可匿名访问的命名管道	清空（默认为空）
网络访问: 可远程访问的注册表路径	清空，不允许远程访问注册表
网络访问: 可远程访问的注册表路径和子路径	清空，不允许远程访问注册表

4.2 禁用未登录前关机

服务器默认是禁止在未登录系统前关机的。如果启用此设置，服务器安全性将会大大降低，给远程连接的黑客造成可乘之机，强烈建议禁用未登录前关机功能。

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 本地策略 > 安全选项中，禁用 关机：允许系统在未登录前关机 策略。

5、其他安全配置

5.1 防病毒管理

Windows系统需要安装防病毒软件。

操作步骤

安装企业级防病毒软件，并开启病毒库更新及实时防御功能。

5.2 设置屏幕保护密码和开启时间

设置从屏幕保护恢复时需要输入密码，并将屏幕保护自动开启时间设定为五分钟。

操作步骤

启用屏幕保护程序，设置等待时间为 5 分钟，并启用 在恢复时使用密码保护。

5.3 限制远程登录空闲断开时间

对于远程登录的帐户，设置不活动超过时间 15 分钟自动断开连接。

操作步骤

打开 控制面板 > 管理工具 > 本地安全策略，在 本地策略 > 安全选项中，设置 Microsoft网络服务器：暂停会话前所需的空闲时间数量 属性为 15 分钟。

5.4 操作系统补丁管理

安装最新的操作系统Hotfix补丁。安装补丁时，应先对服务器系统进行兼容性测试。

操作步骤

安装最新的操作系统Hotfix补丁。安装补丁时，应先对服务器系统进行兼容性测试。

注意：对于实际业务环境服务器，建议使用通知并自动下载更新，但由管理员选择是否安装更新，而不是使用自动安装更新，防止自动更新补丁对实际业务环境产生影响。