|  |
| --- |
| **老男孩信息系统安全配置基线**  **H3C网络设备分册（初稿）** |
| **版本 V1.0** |

**二○一九年一月**

|  |  |  |  |
| --- | --- | --- | --- |
| ■版本变更记录 | | | |
| 时间 | 版本 | 说明 | 修改人 |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| 目录 |
| [一. 概述 4](#_Toc408348074)  [1.1适用范围 4](#_Toc408348075)  [1.2规范依据 4](#_Toc408348076)  [1.3实施策略 4](#_Toc408348077)  [二. 安全配置基线标准 6](#_Toc408348078)  [2.1身份鉴别 6](#_Toc408348079)  [2.1.1分配用户账号 6](#_Toc408348080)  [2.1.2配置密码复杂度 7](#_Toc408348081)  [2.1.3加密账号静态口令 8](#_Toc408348082)  [2.1.4删除无关帐号 8](#_Toc408348083)  [2.1.5设置访问级密码 9](#_Toc408348084)  [2.1.6启用远程认证授权 10](#_Toc408348085)  [2.2访问控制 11](#_Toc408348086)  [2.2.1防止地址欺骗 11](#_Toc408348087)  [2.3安全审计 12](#_Toc408348088)  [2.3.1启用远程日志 12](#_Toc408348089)  [2.3.2启用NTP服务 13](#_Toc408348090)  [2.4入侵防范 14](#_Toc408348091)  [2.4.1过滤已知攻击 14](#_Toc408348092)  [2.5网络设备防护 15](#_Toc408348093)  [2.5.1限制远程管理地址 15](#_Toc408348094)  [2.5.2启用SSH登录维护 16](#_Toc408348095)  [2.5.3启用登录失败处置 17](#_Toc408348096)  [2.5.4启用登录超时退出 18](#_Toc408348097)  [2.5.5禁用非必要网络服务 19](#_Toc408348098)  [2.5.6配置命令级别 19](#_Toc408348099)  [2.5.7更改SNMP默认Community串 20](#_Toc408348100)  [2.5.8限制SNMP服务主机 21](#_Toc408348101)  [2.6其他安全项 22](#_Toc408348102)  [2.6.1关闭未使用接口 22](#_Toc408348103)  [三. 评审与修订 22](#_Toc408348104) |

1. 概述
   1. 适用范围

本配置规范适用于老男孩的H3C网络设备，主要涉及H3C网络设备安全配置方面的基本要求，用于指导安全例行工作、新系统入网安全检查等场合。

在未特别说明的情况下，均适用于所有运行的H3C网络设备。

* 1. 规范依据

根据老男孩目前H3C网络设备的安全现状，综合参考各信息系统运维部门的意见，结合金融行业等级保护实施指引，制定适合于老男孩的基线配置规范。

主要参考依据如下：

* JR/T0071-2012《金融行业信息系统信息安全等级保护实施指引》（2012年7月发布）
  1. 实施策略

结合网络和信息系统建设情况，考虑安全配置项影响的范围，根据以往工作经验，提出如下安全项目实施策略：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **配置类别** | **安全基线项目名称** | **实施策略** |
| 1 | 身份鉴别 | 分配用户账号 | 必须实施 |
| 2 | 身份鉴别 | 配置密码复杂度 | 必须实施 |
| 3 | 身份鉴别 | 加密账号静态口令 | 必须实施 |
| 4 | 身份鉴别 | 删除无关帐号 | 按需实施 |
| 5 | 身份鉴别 | 设置访问级密码 | 按需实施 |
| 6 | 身份鉴别 | 启用远程认证授权 | 按需实施 |
| 7 | 访问控制 | 防止地址欺骗 | 按需实施 |
| 8 | 安全审计 | 启用远程日志 | 按需实施 |
| 9 | 安全审计 | 启用NTP服务 | 按需实施 |
| 10 | 入侵防范 | 过滤已知攻击 | 建议实施 |
| 11 | 网络设备防护 | 限制远程管理地址 | 必须实施 |
| 12 | 网络设备防护 | 启用SSH登录维护 | 必须实施 |
| 13 | 网络设备防护 | 启用登录失败处置 | 必须实施 |
| 14 | 网络设备防护 | 启用登录超时退出 | 必须实施 |
| 15 | 网络设备防护 | 禁用非必要网络服务 | 建议实施 |
| 16 | 网络设备防护 | 配置命令级别 | 按需实施 |
| 17 | 网络设备防护 | 更改SNMP默认Community串 | 按需实施 |
| 18 | 网络设备防护 | 限制SNMP服务主机 | 按需实施 |
| 19 | 其他安全项 | 关闭未使用接口 | 按需实施 |

1. 安全配置基线标准
   1. 身份鉴别
      1. 分配用户账号

|  |  |
| --- | --- |
| **安全基线项目名称** | 分配用户账号（必须实施） |
| **安全基线编号** | 网络设备-H3C-配置-1 |
| **安全基线项说明** | 按照用户分配帐号，避免不同用户间共享帐号，避免用户帐号和设备间通信使用的帐号共享。 |
| **配置方法** | **1.参考配置操作**  使用display current-configuration配置查看命令，查看输出中username部分是否按照用户分配账号，根据输出询问管理员账户使用情况。  **2.补充说明**  无。 |
| **检查方法** | **1.判定条件**  查看输出中username部分，根据输出询问管理员账户使用情况；  **2.参考检测操作**  <H3C>display current-configuration  **3.补充说明**  无。 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：a）应对登录网络设备的用户进行身份鉴别；  7.1.2.7网络：网络设备防护（G3）：c）网络设备用户的标识应唯一。 |
| **备注** | 手工检查 |

* + 1. 配置密码复杂度

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置密码复杂度（必须实施） |
| **安全基线编号** | 网络设备-H3C-配置-2 |
| **安全基线项说明** | 对于采用静态口令认证技术的设备，口令长度至少8位，并包括数字、小写字母、大写字母和特殊符号四类中至少两类，且5次以内不得设置相同的口令，密码应至少每90天进行更换。 |
| **配置方法** | **1.参考配置操作**  user-interface aux 0 8  authentication-mode password  user privilege level 0  set authentication password cipher xxx  user-interface vty 0 4  authentication-mode password  //或authentication-mode scheme  user privilege level 0  set authentication password cipher xxx  **2.补充说明**  无。 |
| **检查方法** | **1.判定条件**  查看密码强度  **2.参考检测操作**  <H3C>display current-configuration  **3.补充说明**  无。 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：e）身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换。 |
| **备注** |  |

* + 1. 加密账号静态口令

|  |  |
| --- | --- |
| **安全基线项目名称** | 加密账号静态口令（必须实施） |
| **安全基线编号** | 网络设备-H3C-配置-3 |
| **安全基线项说明** | 静态口令必须使用不可逆加密算法加密，以密文形式存放。如使用enable secret配置enable密码，不使用enable password配置enable密码。 |
| **配置方法** | **1.参考配置操作**  user-interface aux 0 8  user privilege level 0  set authentication password cipher xxx  user-interface vty 0 4  user privilege level 0  set authentication password cipher xxx  super password level 1 cipher password1  super password level 2 cipher password2  super password level 3 cipher password3 |
| **检查方法** | **1.判定条件**  用户的加密口令在config文件中显示的密文。  **2.参考检测操作**  display current-configuration |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：g）当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；  7.1.2.7网络：网络设备防护（G3）：e）身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换。 |
| **备注** |  |

* + 1. 删除无关帐号

|  |  |
| --- | --- |
| **安全基线项目名称** | 删除无关帐号（按需实施） |
| **安全基线编号** | 网络设备-H3C-配置-4 |
| **安全基线项说明** | 应删除与设备运行、维护等工作无关的帐号。 |
| **配置方法** | **1.参考配置操作**  使用display current-configuration配置查看命令，查看输出中username部分,根据业务需要删除无关账号。  **2.补充说明**  无。 |
| **检查方法** | **1.判定条件**  查看输出中username部分是否有意义不明或测试类的账户  **2.参考检测操作**  <H3C>display current-configuration  **3.补充说明**  无。 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：a）应对登录网络设备的用户进行身份鉴别；  7.1.2.7网络：网络设备防护（G3）：c）网络设备用户的标识应唯一；  7.1.2.7网络：网络设备防护（G3）：n) 应定期检查并锁定或撤销网络设备中不必要的用户账号。 |
| **备注** | 需要手工检查，由管理员判断是否存在无关帐号 |

* + 1. 设置访问级密码

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置访问级密码（按需实施） |
| **安全基线编号** | 网络设备-H3C-配置-5 |
| **安全基线项说明** | 用户可以无条件切换到比当前低的用户级别，但是当使用AUX或VTY用户界面登录，并且从低级别往高级别切换时，需要输入级别切换密码（级别切换密码可以通过super password命令设置）。如果输入的密码错误或者没有配置级别切换密码，切换操作失败。因此，在进行切换操作前，请先配置级别切换密码。 |
| **配置方法** | **1.参考配置操作**  <Sysname> system-view [Sysname] super password level 1 cipher password1  [Sysname] super password level 2 cipher password2  [Sysname] super password level 3 cipher password3  **2.补充说明**  无。 |
| **检查方法** | **1.判定条件**  [Sysname] display current-configuration |
| **依据** | 7.1.2.7 网络：网络设备防护（G3）：a）应对登录网络设备的用户进行身份鉴别；  7.1.2.7 网络：网络设备防护（G3）：h）应实现设备特权用户的权限分离。 |
| **备注** |  |

* + 1. 启用远程认证授权

|  |  |
| --- | --- |
| **安全基线项目名称** | 启用远程认证授权（按需实施） |
| **安全基线编号** | 网络设备-H3C-配置-6 |
| **安全基线项说明** | 设备通过相关参数配置，与认证系统联动，满足帐号、口令和授权的强制要求。 |
| **配置方法** | **1.参考配置操作**  Router#configure terminal  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)#aaa new-model  Router(config)#aaa authentication login default group tacacs+  Router(config)#aaa authentication enable default group tacacs+  Router(config)#tacacs-server host 192.168.6.18  Router(config)#tacacs-server key Ir3@1yh8n#w9@swD  Router(config)#end  Router#  **2.补充操作说明**  与外部TACACS+ server 192.168.6.18联动，远程登录使用TACACS+ server验证 |
| **检查方法** | **1.判定条件**  帐号、口令配置，指定了认证系统  **2.检测操作**  使用show running-config命令，如下例：  router#show running-config  Building configuration...  Current configuration:  !  aaa new-model  aaa authentication login default group tacacs+  aaa authentication enable default group tacacs+  tacacs-server host 192.168.6.18  tacacs-server key Ir3@1yh8n#w9@swD  **3.补充说明**  无 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：a）应对登录网络设备的用户进行身份鉴别；  7.1.2.7网络：网络设备防护（G3）：c）网络设备用户的标识应唯一。 |
| **备注** |  |

* 1. 访问控制
     1. 防止地址欺骗

|  |  |
| --- | --- |
| **安全基线项目名称** | 防止地址欺骗（按需实施） |
| **安全基线编号** | 网络设备-H3C-配置-7 |
| **安全基线项说明** | 为了防止地址欺骗攻击，设备应配置URPF的安全特性。 |
| **配置方法** | **1.参考配置操作**  ip urpf strict acl <acl\_number>  或  [H3C]arp static 192.168.1.1 AAAA-AAAA-AAAA 2  [H3C]am user-bind mac-addr AAAA-AAAA-AAAA ip-addr 192.168.x.x  **2.补充说明**  无。 |
| **检查方法** | **1.参考检测操作**  display current-configuration  或  执行display am user-bind命令，查看接口是否有绑定列表输出。  **2.补充说明**  无。 |
| **依据** | 7.1.2.2网络：访问控制（G3）：f）重要网段应采取技术手段防止地址欺骗。 |
| **备注** |  |

* 1. 安全审计
     1. 启用远程日志

|  |  |
| --- | --- |
| **安全基线项目名称** | 启用远程日志（按需实施） |
| **安全基线编号** | 网络设备-H3C-配置-8 |
| **安全基线项说明** | 设备应支持远程日志功能。所有设备日志均能通过远程日志功能传输到日志服务器。设备应支持至少一种通用的远程标准日志接口，如SYSLOG、FTP等。 |
| **配置方法** | **1.参考配置操作**  路由器侧配置：  [H3C]info-center enable  [H3C]info-center loghost 10.90.200.93facility local0 language English  [H3C]info-center source default channel loghost log level notifications  [H3C]display info-center  **2.补充操作说明**  如果使用SNMP记录日志配置如下：  [H3C]snmp-agent  [H3C]snmp-agent sys-info version all  [H3C]snmp-agent community read ahltnms  [H3C]snmp-agent community write ahltnms  [H3C]snmp-agent traps enable  [H3C]snmp-agent target-host trap address udp-domain 10.199.39.215 [H3C]params securityname trapcomm |
| **检查方法** | **1.判定条件**  是否正确配置了相应的日志服务器地址，日志服务器正确记录了日志信息。  **2.参考检测操作**  登录后执行display info-center命令，查看输出中：  information Center状态是否为“enabled”；  log host后面的主机名或IP指向日志服务器  通常记录日志数不为0。  **3.补充说明**  注意：锁定info-center关键字查看是否启用相关配置 |
| **依据** | 7.1.2.3网络：安全审计（G3）：a）审计记录应包括：应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；  7.1.2.3网络：安全审计（G3）：c）应能够根据记录数据进行分析，并生成审计报表；  7.1.2.3网络：安全审计（G3）：d）应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。 |
| **备注** | 根据应用场景的不同，如部署场景需开启此功能，则强制要求此项。建议核心设备必选，其它根据实际情况启用 |

* + 1. 启用NTP服务

|  |  |
| --- | --- |
| **安全基线项目名称** | 启用NTP服务（按需实施） |
| **安全基线编号** | 网络设备-H3C-配置-9 |
| **安全基线项说明** | 开启NTP服务，保证日志功能记录的时间的准确性。 |
| **配置方法** | **1.参考配置操作**  启用NTP认证：  [H3C]ntp-service authentication-keyid 1 authentication-mode md5 N`C55QK<`=/Q=^Q`MAF4<1!!  [H3C]ntp-service unicast-server 2.2.2.2 authentication-keyid 1 |
| **检查方法** | 使用display current-configuration命令，查看是有如下配置：ntp-service相关关键字。 |
| **依据** | 7.1.2.3网络：安全审计（G3）：b）审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；  7.1.2.7网络：网络设备防护（G3）：m) 应建立网络设备的时钟同步机制。 |
| **备注** | 请将配置方法中2.2.2.2替换为实际网络环境中的NTP服务器IP |

* 1. 入侵防范
     1. 过滤已知攻击

|  |  |
| --- | --- |
| **安全基线项目名称** | 过滤已知攻击（建议实施） |
| **安全基线编号** | 网络设备-H3C-配置-10 |
| **安全基线项说明** | 过滤已知攻击：在网络边界，设置安全访问控制，过滤掉已知安全攻击数据包，例如udp 1434端口（防止SQL slammer蠕虫）、tcp445,5800,5900（防止Della蠕虫）。 |
| **配置方法** | **1.参考配置操作**  常见的ACL控制列表如下：  Acl number 2000  ##用于控制Blaster蠕虫的传播  rule 1 deny tcp source any destion any destination eq 4444  rule 2 deny udp source any destion any destination eq 69  ##用于控制Blaster蠕虫的扫描和攻击  rule 3 deny tcp source any destion any destination eq 135  rule 4 deny udp source any destion any destination eq 135  rule 5 deny tcp source any destion any destination eq 139  rule 6 deny udp source any destion any destination eq 139  rule 7 deny tcp source any destion any destination eq 445  rule 8 deny udp source any destion any destination eq 445  rule 9 deny tcp source any destion any destination eq 593  rule 10 deny udp source any destion any destination eq 593  ##用于控制 Slammer 蠕虫的传播  rule 11 deny udp source any destion any destination eq 1434  ##用于控制震荡波的传播  rule 12 deny tcp source any destination any destination-port eq 5554  rule 13 deny tcp source any destination any destination-port eq 9995  rule 14 deny tcp source any destination any destination-port eq 9996  ##其他  rule 15 deny udp destination-port eq netbios-ns  rule 16 deny udp destination-port eq netbios-dgm |
| **检查方法** | 使用display current-configuration或display traffic policy命令，查看是有如安全配置方法中的相关控制列表存在。 |
| **依据** | 7.1.2.5网络：入侵防范（G3）：a）应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等；  7.1.2.5网络：入侵防范（G3）：b）当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。 |
| **备注** | 1. 屏蔽端口操作需要管理员测试是否会影响相关应用   如果网络边界存在防火墙或者IPS等硬件防护设备，可以利用防火墙白名单的规则进行防护，无需在路由器上面配置，此项为可选。 |

* 1. 网络设备防护
     1. 限制远程管理地址

|  |  |
| --- | --- |
| **安全基线项目名称** | 限制管理员远程登录（必须实施） |
| **安全基线编号** | 网络设备-H3C-配置-11 |
| **安全基线项说明** | 系统远程管理服务TELNET、SSH默认可以接受任何地址的连接，出于安全考虑，应该只允许特定地址访问。 |
| **配置方法** | **1.参考配置操作**  只允许特定地址访问：  [H3C]acl 2000  [H3C-acl-basic-2000]rule permit ip source 10.0.0.1 0  [H3C]user-interface vty 0 4  [H3C-ui-vty0-4]acl 2000 inbound  **2.补充说明**  无。 |
| **检查方法** | **1.判定条件**  通过设定acl，成功过滤非法的访问。  **2.参考检测操作**  使用dis cur命令，输出中查看是否有rule permit字段。  **3.补充说明**  无。 |
| **依据** | 7.1.2.7 网络：网络设备防护（G3）：a）应对登录网络设备的用户进行身份鉴别；  7.1.2.7 网络：网络设备防护（G3）：b）应对网络设备的管理员登录地址进行限制。 |
| **备注** |  |

* + 1. 启用SSH登录维护

|  |  |
| --- | --- |
| **安全基线项目名称** | 启用SSH登录维护（必须实施） |
| **安全基线编号** | 网络设备-H3C-配置-12 |
| **安全基线项说明** | 对于使用IP协议进行远程维护的设备，设备应配置使用SSH等加密协议，关闭TELNET协议。 |
| **配置方法** | **1.参考配置操作**  # 设置用户界面VTY 0 到VTY 4 支持SSH 协议。 <Sysname> system-view [Sysname] user-interface vty 0 4 [Sysname-ui-vty0-4] authentication-mode scheme [Sysname-ui-vty0-4] protocol inbound ssh  **2.补充说明**  无。 |
| **检查方法** | **1.参考检测操作**  <H3C>display current-configuration  **2.补充说明**  无。 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：g）当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。 |
| **备注** |  |

* + 1. 启用登录失败处置

|  |  |
| --- | --- |
| **安全基线项目名称** | 启用登录失败处置（必须实施） |
| **安全基线编号** | 网络设备-H3C-配置-13 |
| **安全基线项说明** | 设置登录失败策略，在30秒钟以内对网络设备连续错误登录5次，账号锁定10分钟。 |
| **配置方法** | 1.参考配置操作   * Console登录连接超时：   [H3C]user-interface con 0  [H3C-ui-console0]idle-timeout 5 0   * 远程登录连接超时：   [H3C]user-interface vty 0 4  [H3C-ui-vty0-4]idle-timeout 5 02.补充说明 |
| **检查方法** | 每种登录方式均设置了timeout值。用display current-configuration命令，如下例：  //下为console登录限制超时时间为5分钟  user-interface con 0  idle-timeout 5 0  //下为telent/SSH登录限制超时时间为5分钟  user-interface vty 0 4  idle-timeout 5 0 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：f）应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。 |
| **备注** |  |

* + 1. 启用登录超时退出

|  |  |
| --- | --- |
| **安全基线项目名称** | 启用登录超时退出（必须实施） |
| **安全基线编号** | 网络设备-H3C-配置-14 |
| **安全基线项说明** | 配置定时帐户自动登出，登出后用户需再次登录才能进入系统，设置超时时间为5分钟。 |
| **配置方法** | **1.参考配置操作**  设置超时时间为5分钟  <Sysname> system-view  [Sysname] user-interface console 0  //Or user-interface aux 0 8  [Sysname-ui-console0] idle-timeout 5 0  **2.补充说明**  无。 |
| **检查方法** | **1.判定条件**  在超出设定时间后，用户自动登出设备。  **2.参考检测操作**  display current-configuration configuration user-interface  **3.补充说明**  无。 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：f）应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。 |
| **备注** |  |

* + 1. 禁用非必要网络服务

|  |  |
| --- | --- |
| **安全基线项目名称** | 禁用非必要网络服务（建议实施） |
| **安全基线编号** | 网络设备-H3C-配置-15 |
| **安全基线项说明** | 关闭网络设备不必要的服务，比如FTP、TFTP、HTTP服务等。 |
| **配置方法** | **1.参考配置操作**  undo ftp server  undo http server enable  **2.补充说明**  无。 |
| **检查方法** | **1.判定条件**  不能访问设备的ftp和http等服务。  **2.参考检测操作**  display current-configuration  **3.补充说明**  无。 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：k）对网络设备系统自带的的服务端口进行梳理，关掉不必要的系统服务端口，并建立相应的端口开放审批制度。 |
| **备注** | 根据应用场景的不同，如部署场景需开启此功能，则强制要求此项。 |

* + 1. 配置命令级别

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置命令级别（按需实施） |
| **安全基线编号** | 网络设备-H3C-配置-16 |
| **安全基线项说明** | 交换机命令级别共分为访问、监控、系统、管理4个级别，分别对应标识0、1、2、3，配置登录默认级别为访问级（0-VISIT）。 |
| **配置方法** | **1.参考配置操作**  user-interface aux 0 8  authentication-mode password  user privilege level 0  set authentication password cipher xxx  user-interface vty 0 4  authentication-mode password  user privilege level 0  set authentication password cipher xxx  **2.补充说明**  无。 |
| **检查方法** | **1.判定条件**  用配置中没有的用户名去登录，结果是不能登录  **2.参考检测操作**  <H3C>display current-configuration  **3.补充说明**  无。 |
| **依据** | 7.1.2.7 网络：网络设备防护（G3）：a）应对登录网络设备的用户进行身份鉴别；  7.1.2.7 网络：网络设备防护（G3）：h）应实现设备特权用户的权限分离。 |
| **备注** | 手工检查 |

* + 1. 更改SNMP默认Community串

|  |  |
| --- | --- |
| **安全基线项目名称** | 更改SNMP默认Community串（按需实施） |
| **安全基线编号** | 网络设备-H3C-配置-17 |
| **安全基线项说明** | 系统应修改SNMP的Community默认通行字，通行字应符合口令强度要求。 |
| **配置方法** | **1.参考配置操作**  snmp-agent community read xxx  snmp-agent community write xxxx  **2.补充说明**  无。 |
| **检查方法** | **1.判定条件**  系统成功修改SNMP的Community为用户定义口令，非常规private或者public，并且符合口令强度要求。  **2.参考检测操作**  display current-configuration  **3.补充说明**  无。 |
| **依据** | 7.1.2.7网络：网络设备防护（G3）：g）当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； |
| **备注** |  |

* + 1. 限制SNMP服务主机

|  |  |
| --- | --- |
| **安全基线项目名称** | 限制SNMP服务主机（按需实施） |
| **安全基线编号** | 网络设备-H3C-配置-18 |
| **安全基线项说明** | 设置SNMP访问安全限制，只允许特定主机通过SNMP访问网络设备。 |
| **配置方法** | **1.参考配置操作**  snmp-agent community read XXXX01 acl 2000  **2.补充说明**  无。 |
| **检查方法** | **1.判定条件**  通过设定acl来成功过滤特定的源才能进行访问。  **2.参考检测操作**  display current-configuration  **3.补充说明**  无。 |
| **依据** | 7.1.2.2网络：网络设备防护（G3）：b）应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级； |
| **备注** |  |

* 1. 其他安全项
     1. 关闭未使用接口

|  |  |
| --- | --- |
| **安全基线项目名称** | 关闭未使用接口（按需实施） |
| **安全基线编号** | 网络设备-H3C-配置-19 |
| **安全基线项说明** | 关闭未使用的接口。 |
| **配置方法** | **1.参考配置操作**  [HW-Ethernet3/0/0]shutdown  **2.补充说明**  无。 |
| **检查方法** | **1.判定条件**  未使用端口状态为admin down。  **2.参考检测操作**  Display interface  **2.补充说明**  无。 |
| **依据** |  |
| **备注** |  |

1. 评审与修订

本标准由老男孩定期进行审查，根据审视结果修订标准，并颁发执行。