

|  |  |
| --- | --- |
| 文档编号 | AH-{user-acronym}-{date-month}{date-day} |
| 版本编号 | V1.0 |
| 密级 | 受控 |
| 日期 | {date-start} |

|  |
| --- |
| {user-name}  主机扫描报告 |

|  |
| --- |
| **©2021安恒信息** |
| **版权所有，未经授权，严禁复制、编辑和传播** |

* 适用性声明

本文档仅适用于杭州安恒信息技术股份有限公司（以下简称“安恒信息”）在{user-name}（以下简称“{user-name}”）开展主机扫描时的状况。主机扫描结束之后，因内部环境或不可预知的国内国际政治、经济、法律等社会环境的变化，可能会影响文档的有效性。再者，任何控制系统都存在固有的局限性，错误、违反内部控制的情况仍然有可能发生及不被发现。

* 版权声明

本文中的所有信息均为{user-name}（以下简称“{user-name}”）内部信息，务请妥善保管，未经{user-name}和安恒信息明确作出的书面许可，不得为任何目的、以任何形式或手段（包括电子、机械、复印、录音或其他形式）对本文档的任何部分进行复制、存储、引入检索系统或者传播。

* 版本变更记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本号** | **拟制／修改日期** | **拟制／修改人** | **修改记录** | **批准人** |
| V0.1 | 2020-04-27 | 张韵 | 创建文档，添加样式库 | 韦国文 |
| V0.2 | 2020-07-30 | 甘雁南、苏启波 | 添加样式库、修改图注 | 韦国文 |
| V0.3 | 2020-09-08 | 甘雁南 | 修改格式和字体 | 韦国文 |
| V0.4 | 2020-10-23 | 王琦 | 修改格式 | 韦国文 |
| V1.0 | 2021-01-25 | 甄杰 | 修改格式和样式库 | 韦国文 |

目录

[一. 概述 3](#_Toc69344326)

[1.1 项目目标 3](#_Toc69344327)

[1.2 测试依据 3](#_Toc69344328)

[1.3 项目收益 3](#_Toc69344329)

[二. 实施范围 4](#_Toc69344330)

[三. 风险规避与处理措施 4](#_Toc69344331)

[3.1 风险规避措施 4](#_Toc69344332)

[3.1.1 系统备份与恢复 4](#_Toc69344333)

[3.1.2 风险与应对 4](#_Toc69344334)

[3.2 风险处理措施 4](#_Toc69344335)

[四. 检测结果与建议 5](#_Toc69344336)

1. 概述
   1. 项目目标

根据{user-name}的安全性需求，授权杭州安恒信息技术股份有限公司（以下简称“安恒信息”）对其进行主机扫描测试；并根据本次扫描过程中所发现的系统脆弱点提供改进方案，以指导{user-name}开展安全整改、完善安全策略，降低安全风险，使{user-name}的安全保障能力符合国家的相关政策法规和自身业务的安全需求。

* 1. 测试依据

项目所依据及参考的标准：

《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）

《信息技术 安全技术 信息技术安全性评估准则》（GB/T 18336-2015）

《信息系统安全保障评估框架》（GB/T 20274-2006）

《OWASP测试指南V4.0》（2014）

《开源安全测试方法手册（OSSTMM）3》（2010）

《PTES渗透测试执行标准》（2011）

* 1. 项目收益

从攻击者的角度进行测试将有助于发现并识别出一些隐性存在的安全漏洞和风险点。

从客户收益的角度来说，可以对信息系统的安全性得到较深的感性认知，有助于后续的安全建设，对设备的版本、典型的可利用漏洞可以进行全面的排查，同时也可以用于验证经过安全保护后的网络是否真实的达到了预定安全目标、遵循了安全策略。

1. 实施范围

经过与{user-name}协商确定，将主机扫描的时间安排为{date-start}，主机扫描限定于以下对象：

|  |  |  |
| --- | --- | --- |
| 序号 | 测试对象 | 对象名称 |

1. 风险规避与处理措施
   1. 风险规避措施
      1. 系统备份与恢复

为防止在加固过程中出现的异常情况，所有被加固系统均应在被加固之前进行完整的系统备份,以便在系统发生灾难后及时恢复。

操作系统类：对系统的配置、用户目录和重要文件进行备份。例如：注册表、sam文件、/etc中的配置文件。并应该确保备份的自身安全。

数据库系统类：对数据库系统进行数据转储，并妥善保护好备份数据。同时对数据库系统的配置信息和用户信息进行备份。

网络应用系统类：对网络应用服务系统及其配置、用户信息、数据库等进行备份。

网络设备类：对网络设备的配置文件进行备份。

* + 1. 风险与应对

加固时间尽量安排在业务量不大的时段。在加固过程中如果出现被加固系统没有响应的情况，应立即停止加固工作，与配合人员一起分析情况，在确定原因后，并正确恢复系统，采取必要的预防措施后，才可以继续进行。

* 1. 风险处理措施

对信息系统安全加固过程中发现的风险，其处理方式一般有以下处理方式：

* 避免：指通过不继续进行可能产生风险的活动来避免风险。这种方式是最佳的解决方式，但实施的前提是要具有可行性，需要结合具体的实际情况在分析后决定。
* 转移：是指将相关的风险借助合同、保险以及合伙，合资等方式全部或部分转移给第三方，但这种转移一般只能降低部分经济损失或转移部分责任，不能降低安全本身的风险。
* 降低：通过采取相应的风险控制措施、安全机制来切实降低风险，减少发生的机率可能性，这也是采用最多的一种方式之一。
* 接受：在风险降低或转移后，可能还有剩余的风险，完全的零风险最理论和实践中都是不可能的，而且降低风险的成本会随着风险的降低而增大，通常考虑的尺度是让风险的处理成本与该项处理活动保持一种可接受的平衡。

1. 检测结果与建议

经过此次检测，{conclusion-result}