

绿盟科技"远程安全评估系统"安全 评估报告

报表生成时间 2024-06-21 13:44:56

目录

1 综述信息	1
1.1 任务信息	1
1.2 风险分布	2
1.3 资产综述	2
2 风险类别	3
2.1 漏洞风险类别	3
3 主机信息	5
3.1 主机风险等级列表	5
4 漏洞信息	6
4.1 漏洞分布	6
5 脆弱帐号	8
5.1 系统脆弱帐号	8
5.2 应用程序脆弱帐号	9
6 参考标准	10
6.1 单一漏洞风险等级评定标准	11
6.2 主机风险等级评定标准	12
6.3 网络风险等级评定标准	13
6.4 安全建议	13

1 综述信息

本次评估范围内的1台有效主机及设备都已扫描完毕，远程安全评估系统从如下几个方面进行分类统计：

- 主机风险等级列表
- 主机分布信息
- 漏洞风险分类信息
- 漏洞风险分布情况
- 脆弱的帐号口令列表

网络的安全等级为 **▲非常危险**。其中有1个设备的安全等级为非常危险。被评估网络的风险值为10.0。关于漏洞风险程度的分类规则以及主机风险分类规则，请参见《参考标准》。

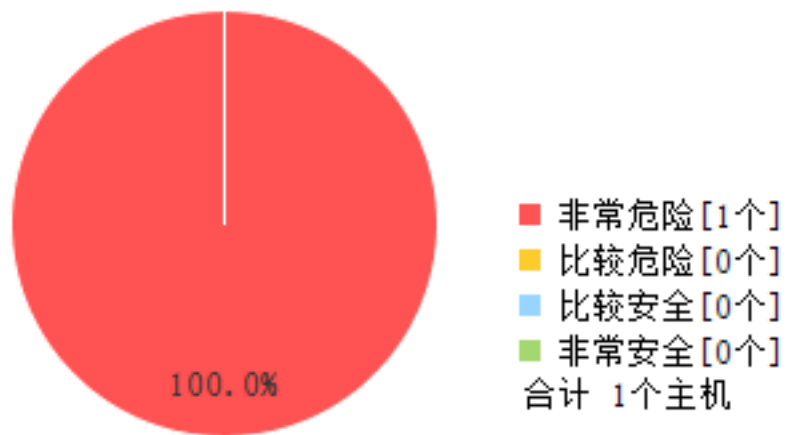
1.1 任务信息

任务名称	扫描【192.168.4.22】
配置核查模板	
网络风险值	10.0
任务类型	评估任务
存活主机	1
成功扫描主机	0
失败扫描主机	1
未扫描主机	0
开始时间	2024-06-21 13:41:40
结束时间	2024-06-21 13:42:54
系统版本信息	V6.0R04F03SP04

1.2 风险分布

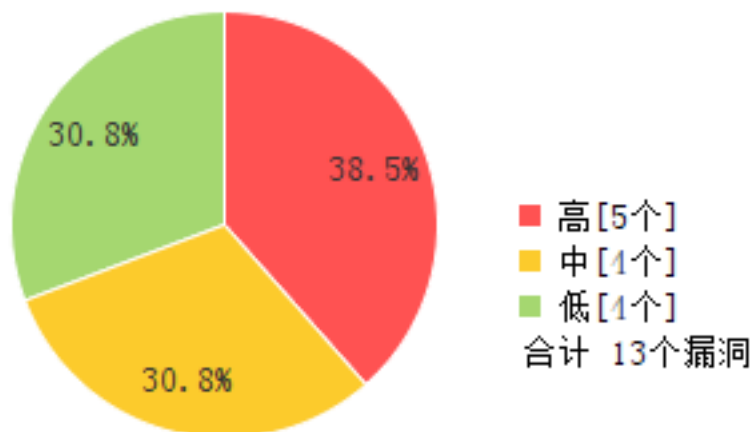
1.2.1 主机风险分布

主机风险等级分布



1.2.2 漏洞风险分布

漏洞高中低风险分布



1.3 资产综述

1.3.1 操作系统

操作系统	主机数量	比率
------	------	----

linux	1	100%
合计	1	100%

2 风险类别

2.1 漏洞风险类别

2.1.1 服务分类

服务	高风险	中风险	低风险	总计
SSH	3	3	3	9
其他	2	1	0	3
Kernel	0	0	1	1
合计	5	4	4	13

2.1.2 应用分类

应用	高风险	中风险	低风险	总计
OpenSSH	5	4	2	11
其他	0	0	1	1
SSH	0	0	1	1
合计	5	4	4	13

2.1.3 系统分类

系统	高风险	中风险	低风险	总计
系统无关	5	2	4	11
UNIX通用	0	2	0	2
合计	5	4	4	13

2.1.4 威胁分类

威胁	高风险	中风险	低风险	总计
其他	5	4	2	11
远程信息泄露	0	0	2	2
合计	5	4	4	13

2.1.5 时间分类


时间	高风险	中风险	低风险	总计
2023年	3	3	0	6
2021年	2	0	1	3
2016年	0	1	1	2
1999年	0	0	2	2
合计	5	4	4	13

2.1.6 CVE年份分类

CVE年份	高风险	中风险	低风险	总计
CVE-2023	3	3	0	6
CVE-2021	2	0	1	3
CVE-2016	0	1	0	1
CVE-1999	0	0	2	2
Others	0	0	1	1
合计	5	4	4	13

3 主机信息

3.1 主机风险等级列表













IP地址	主机名	操作系统	高	中	低	主机风险值
 192.168.4.22		Linux 4.15 - 5.6	5	4	4	10.0

3.2 扫描失败主机列表

IP地址	失败原因
192.168.4.22	登陆失败: 连接被拒绝

4 漏洞信息

4.1 漏洞分布

序号	漏洞名称	影响主机个数	影响主机百分比	出现次数
1	 OpenSSH 安全漏洞(CVE-2023-38408)	1/1	100%	1
2	 OpenSSH 安全漏洞(CVE-2023-28531)	1/1	100%	1
3	 OpenSSH 安全漏洞(CVE-2021-28041)	1/1	100%	1
4	 OpenSSH 安全漏洞(CVE-2021-41617)	1/1	100%	1
5	 OpenSSH 安全漏洞(CVE-2023-51767)	1/1	100%	1
6	 OpenSSH 安全漏洞(CVE-2023-51385)	1/1	100%	1
7	 OpenSSH 安全漏洞(CVE-2023-48795)	1/1	100%	1
8	 OpenSSH 安全漏洞(CVE-2023-51384)	1/1	100%	1
9	 OpenSSH 安全漏洞(CVE-2016-20012)	1/1	100%	1
10	 OpenSSH 授权问题漏洞(CVE-2021-36368)	1/1	100%	1
11	 ICMP timestamp请求响应漏洞	1/1	100%	1
12	 SSH版本信息可被获取	1/1	100%	1
13	 探测到SSH服务器支持的算法	1/1	100%	1
合计				13

5 脆弱帐号

5.1 系统脆弱帐号




IP地址	用户名	密码	描述
------	-----	----	----

5.2 应用程序脆弱帐号

IP地址	用户名	密码	应用类型
------	-----	----	------

6 参考标准

6.1 单一漏洞风险等级评定标准

危险程度	危险值区域	危险程度说明
 高	$7 \leq \text{漏洞风险值} \leq 10$	攻击者可以远程执行任意命令或者代码，或对系统进行远程拒绝服务攻击。
 中	$4 \leq \text{漏洞风险值} < 7$	攻击者可以远程创建、修改、删除文件或数据，或对普通服务进行拒绝服务攻击。
 低	$0 \leq \text{漏洞风险值} < 4$	攻击者可以获取某些系统、服务的信息，或读取系统文件和数据。

说明：

漏洞的风险值兼容CVSS评分标准。

6.2 主机风险等级评定标准

主机风险等级	主机风险值区域
 非常危险	$7.0 \leq \text{主机风险值} \leq 10.0$
 比较危险	$5.0 \leq \text{主机风险值} < 7.0$
 比较安全	$2.0 \leq \text{主机风险值} < 5.0$
 非常安全	$0.0 \leq \text{主机风险值} < 2.0$

说明：

1. 按照远程安全评估系统的主机风险评估模型计算主机风险值。根据得到的主机风险值参考“主机风险等级评定标准”标识主机风险等级。
2. 将主机风险等级按照风险值的高低进行排序，得到非常危险、比较危险、比较安全、非常安全四种主机风险等级。
3. 用户可以根据自己的需要修订主机风险等级中的主机风险值范围。

6.3 网络风险等级评定标准

网络风险等级	网络风险值区域
 非常危险	$8.0 \leq \text{网络风险值} \leq 10.0$
 比较危险	$5.0 \leq \text{网络风险值} < 8.0$
 比较安全	$1.0 \leq \text{网络风险值} < 5.0$
 非常安全	$0.0 \leq \text{网络风险值} < 1.0$

说明：

1. 按照远程安全评估系统的网络风险评估模型计算该网络风险值。根据得到的网络风险值参考“网络风险等级评定标准”标识网络风险等级。
2. 将网络风险等级按照风险值的高低进行排序，得到非常危险、比较危险、比较安全、非常安全四种网络风险等级。
3. 用户可以根据自己的需要修订网络风险等级中的网络风险值范围。

6.4 安全建议

据市场研究公司Gartner研究报告称"实施漏洞管理的企业会避免近90%的攻击"。可以看出，及时的漏洞修补可以在一定程度上防止病毒、攻击者的威胁。

远程安全评估系统建议对存在漏洞的主机参考附件中提出的解决方案进行漏洞修补、安全增强。

- 建议所有 Windows 系统使用"Windows Update"进行更新。
- 对于大量终端用户而言，可以采用 WSUS 进行自动补丁更新，也可以采用补丁分发系统及时对终端用户进行补丁更新。
- 对于存在弱口令的系统，需在加强使用者安全意识的前提下，督促其修改密码，或者使用策略来强制限制密码长度和复杂性。
- 对于存在弱口令或是空口令的服务，在一些关键服务上，应加强口令强度，同时需使用加密传输方式，对于一些可关闭的服务来说，建议关闭该服务以达到安全目的。
- 对于UNIX系统订阅厂商的安全公告，与厂商技术人员确认后进行漏洞修补、补丁安装、停止服务等。
- 由于其他原因不能及时安装补丁的系统，考虑在网络边界、路由器、防火墙上设置严格的访问控制策略，以保证网络的动态安全。
- 建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的严重漏洞，攻与防的循环，伴随每个主流操作系统、应用服务的生命周期。
- 建议采用远程安全评估系统定期对网络进行评估，真正做到未雨绸缪。