绿盟科技"远程安全评估系统"安全评估报告

报表生成时间 2021-07-16 17:48:52

目录

1 综述信息

本次评估范围内的3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
- 配置风险分类信息
- 漏洞风险分布情况
- 配置信息合规情况
- 脆弱的帐号口令列表

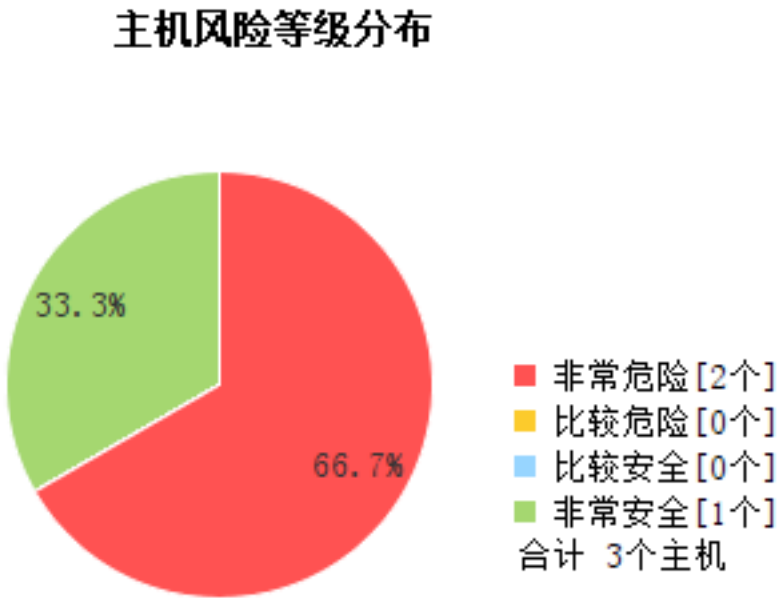
网络的安全等级为非常危险。 其中有2个设备的安全等级为非常危险。被评估网络的风险值为10.0。关于漏洞风险程度的分类规则以及主机风险分类规则，请参见《参考标准》。

1.1 任务信息

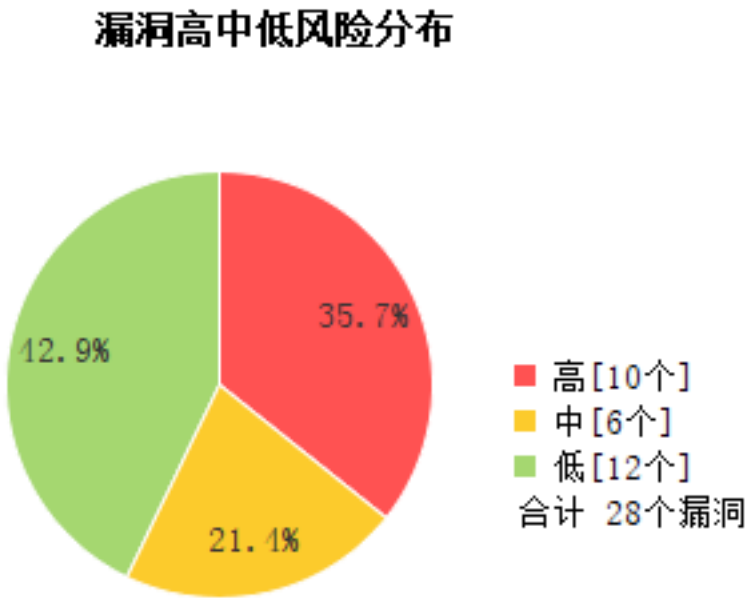
任务名称	扫描【10.61.15.12;10.61.15.25;10.61.15...】
网络风险值	10.0
任务类型	评估任务
存活主机	3
成功扫描主机	3
失败扫描主机	0
未扫描主机	0
开始时间	2021-07-16 17:43:08
结束时间	2021-07-16 17:48:09
系统版本信息	V6.0R04F00SP04

1.2 风险分布

1.2.1 主机风险分布



1.2.2 漏洞风险分布



1.3 资产综述

1.3.1 操作系统

操作系统	主机数量	比率

windows	2	67%
others	1	33%
合计	3	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
WWW	4	2	1	7
SSH	2	2	3	7
系统补丁	2	0	0	2
SSL/TLS	1	2	1	4
远程管理	1	0	3	4
数据库	0	0	2	2
DCE/RPC	0	0	1	1
其他	0	0	1	1
合计	**10**	**6**	**12**	**28**

2.1.2 应用分类

应用	高风险	中风险	低风险	总计
Nginx	4	2	0	6
Windows RDP	3	0	0	3
OpenSSH	2	2	2	6
SSL	1	2	1	4
其他	0	0	3	3
MS SQL Server	0	0	2	2
Terminal Server	0	0	2	2
RPC	0	0	1	1
SSH	0	0	1	1
合计	**10**	**6**	**12**	**28**

2.1.3 系统分类

系统	高风险	中风险	低风险	总计
系统无关	7	6	7	20
Windows	3	0	5	8
合计	**10**	**6**	**12**	**28**

2.1.4 威胁分类

威胁	高风险	中风险	低风险	总计

其他	7	5	1	13
远程执行命令	3	0	0	3
远程信息泄露	0	1	10	11
不必要的服务	0	0	1	1
合计	**10**	**6**	**12**	**28**

2.1.5 时间分类

时间	高风险	中风险	低风险	总计
2018年	3	2	0	5
2019年	3	1	1	5
2016年	1	0	1	2
2012年	1	0	0	1
2020年	1	0	0	1
2021年	1	0	0	1
2013年	0	1	0	1
2015年	0	1	0	1
2017年	0	1	0	1
2001年	0	0	5	5
1999年	0	0	4	4
2008年	0	0	1	1
合计	**10**	**6**	**12**	**28**

2.1.6 CVE年份分类

CVE年份	高风险	中风险	低风险	总计
CVE-2018	3	2	0	5
CVE-2019	3	1	0	4
CVE-2012	1	0	0	1
CVE-2016	1	0	0	1
CVE-2020	1	0	0	1
CVE-2021	1	0	0	1
CVE-2013	0	1	0	1
CVE-2015	0	1	0	1
CVE-2017	0	1	0	1
Others	0	0	8	8
CVE-1999	0	0	3	3
CVE-2008	0	0	1	1
合计	**10**	**6**	**12**	**28**

2.2 配置风险类别

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
10.61.15.12		Windows	4	2	8	10.0
10.61.15.25		Actiontec MI424WR-GEN3I WAP	6	4	4	8.1
10.61.15.6		Windows	0	0	5	1.0

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	Microsoft Windows 远程桌面服务远程执行代码漏洞(CVE-2019-0708)【原理扫描】	1/3	33%	1
2	Microsoft Windows RDP 远程代码执行漏洞(CVE-2012-0002)(MS12-020)【原理扫描】	1/3	33%	1
3	OpenSSH 命令注入漏洞(CVE-2020-15778)	1/3	33%	1
4	nginx 安全漏洞（CVE-2018-16844）	1/3	33%	1
5	nginx 安全漏洞（CVE-2018-16843）	1/3	33%	1
6	SSL/TLS协议信息泄露漏洞(CVE-2016-2183)【原理扫描】	1/3	33%	1
7	nginx 安全漏洞(CVE-2019-9513)	1/3	33%	1
8	nginx 安全漏洞(CVE-2019-9511)	1/3	33%	1
9	OpenSSH 安全漏洞(CVE-2021-28041)	1/3	33%	1
10	Microsoft Windows CredSSP 远程执行代码漏洞(CVE-2018-0886)【原理扫描】	1/3	33%	1
11	nginx 安全漏洞(CVE-2019-9516)	1/3	33%	1
12	nginx 安全漏洞（CVE-2018-16845）	1/3	33%	1
13	SSL/TLS RC4 信息泄露漏洞(CVE-2013-2566)【原理扫描】	1/3	33%	1
14	OpenSSH 用户枚举漏洞(CVE-2018-15919)	1/3	33%	1
15	OpenSSH 安全漏洞(CVE-2017-15906)	1/3	33%	1
16	SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)【原理扫描】	1/3	33%	1
17	OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)【原理扫描】	1/3	33%	1
18	Microsoft SQL Server远程版本信息泄漏	1/3	33%	1
19	检测到目标主机加密通信支持的SSL加密算法【原理扫描】	1/3	33%	1
20	允许Traceroute探测	3/3	100%	3
21	Windows终端服务器通信加密级别检查	1/3	33%	1
22	DCE/RPC服务枚举漏洞	2/3	67%	2
23	检测到目标主机上运行着Windows终端服务	1/3	33%	1

24	SSH版本信息可被获取	1/3	33%	1
25	远程桌面服务(RDS)协议探测	1/3	33%	1
26	Microsoft SQL Server数据库服务正在运行	1/3	33%	1
27	可通过HTTP获取远端WWW服务信息	2/3	67%	3
28	探测到SSH服务器支持的算法	1/3	33%	1
合计				**33**

5 配置信息

5.1 不合规配置信息

6 脆弱帐号

6.1 系统脆弱帐号

IP地址	用户名	密码	描述

6.2 应用程序脆弱帐号

IP地址	用户名	密码	应用类型

7 参考标准

7.1 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 <= 漏洞风险值 <=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 <= 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 <= 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。

7.2 单一配置检查项风险等级评定标准

危险程度	危险值区域	危险程度说明
高	7 <= 检查项风险值 <=10	不当的配置导致攻击者可以通过其他方式获得管理员权限、或者只有管理员权限才能加固的配置。
中	4 <= 检查项风险值 < 7	不当的配置导致攻击者可以对主机进行破坏或者收集主机的信息、或者遭受攻击后，重要事件没有记录。
低	0 <= 检查项风险值 < 4	不当地配置对主机安全不会造成太大的影响。

7.3 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 <= 主机风险值 <= 10.0
比较危险	5.0 <= 主机风险值 < 7.0
比较安全	2.0 <= 主机风险值 < 5.0
非常安全	0.0 <= 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。

7.4 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 <= 网络风险值 <= 10.0
比较危险	5.0 <= 网络风险值 < 8.0
比较安全	1.0 <= 网络风险值 < 5.0
非常安全	0.0 <= 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。

7.5 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。

远程安全评估系统建议对存在不合规检查项的主机参考对应的检查点详情中提出的调整方案和标准值进行修正。