



XX 网服务器安全扫描报告

■文档编号

■密级

商业机密

■版本编号 V1.0

■日期

2011-06-13



©2017 绿盟科技

■ 版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属**绿盟科技**所有，受到有关产权及版权法保护。任何个人、机构未经**绿盟科技**的书面授权许可，不得以任何方式复制或引用本文的任何片断。

■ 版本变更记录

时间	版本	说明	修改人
2011-06-13	V1.0	文档创建	李贵鹏

■ 适用性声明

本文档是绿盟科技在 XX 有限公司（以下简称“XX 网”）网络安全服务中，对指定网络服务器进行安全扫描后提交的安全扫描报告，供相关人员参考。

目录

一、概述	1
1.1 扫描范围	1
1.2 扫描时间	3
1.3 扫描内容	4
二、扫描结果摘要	5
三、扫描结果分析	7
3.1 10.10.1.0 网段	7
3.1.1 风险分布	7
3.1.2 风险分类	8
3.1.3 主机风险等级列表	8
3.1.4 漏洞列表	8
3.1.5 脆弱应用帐号列表	8
3.1.6 安全建议	9
3.2 10.10.10.0 网段	错误!未定义书签。
3.2.1 风险分布	错误!未定义书签。
3.2.2 风险分类	错误!未定义书签。
3.2.3 主机风险等级列表	错误!未定义书签。
3.2.4 漏洞列表	错误!未定义书签。
3.2.5 脆弱应用帐号列表	错误!未定义书签。
3.2.6 安全建议	错误!未定义书签。
3.3 10.10.20.0 网段	错误!未定义书签。
3.3.1 风险分布	错误!未定义书签。
3.3.2 风险分类	错误!未定义书签。
3.3.3 主机风险等级列表	错误!未定义书签。
3.3.4 漏洞列表	错误!未定义书签。
3.3.5 脆弱应用帐号列表	错误!未定义书签。
3.3.6 安全建议	错误!未定义书签。
3.4 10.10.30.0 网段	错误!未定义书签。
3.4.1 风险分布	错误!未定义书签。
3.4.2 风险分类	错误!未定义书签。
3.4.3 主机风险等级列表	错误!未定义书签。
3.4.4 漏洞列表	错误!未定义书签。
3.4.5 脆弱应用帐号列表	错误!未定义书签。
3.4.6 安全建议	错误!未定义书签。
3.5 10.10.40.0 网段	错误!未定义书签。
3.5.1 风险分布	错误!未定义书签。
3.5.2 风险分类	错误!未定义书签。
3.5.3 主机风险等级列表	错误!未定义书签。

3.5.4 漏洞列表	错误!未定义书签。
3.5.5 脆弱应用帐号列表	错误!未定义书签。
3.5.6 安全建议	错误!未定义书签。
3.6 10.10.50.0 网段	错误!未定义书签。
3.6.1 风险分布	错误!未定义书签。
3.6.2 风险分类	错误!未定义书签。
3.6.3 主机风险等级列表	错误!未定义书签。
3.6.4 漏洞列表	错误!未定义书签。
3.6.5 脆弱应用帐号列表	错误!未定义书签。
3.6.6 安全建议	错误!未定义书签。
3.7 10.10.60.0 网段	错误!未定义书签。
3.7.1 风险分布	错误!未定义书签。
3.7.2 风险分类	错误!未定义书签。
3.7.3 主机风险等级列表	错误!未定义书签。
3.7.4 漏洞列表	错误!未定义书签。
3.7.5 脆弱应用帐号列表	错误!未定义书签。
3.7.6 安全建议	错误!未定义书签。
3.8 10.10.70.0 网段	错误!未定义书签。
3.8.1 风险分布	错误!未定义书签。
3.8.2 风险分类	错误!未定义书签。
3.8.3 主机风险等级列表	错误!未定义书签。
3.8.4 漏洞列表	错误!未定义书签。
3.8.5 脆弱应用帐号列表	错误!未定义书签。
3.8.6 安全建议	错误!未定义书签。
3.9 10.10.80.0 网段	错误!未定义书签。
3.9.1 风险分布	错误!未定义书签。
3.9.2 风险分类	错误!未定义书签。
3.9.3 主机风险等级列表	错误!未定义书签。
3.9.4 漏洞列表	错误!未定义书签。
3.9.5 脆弱应用帐号列表	错误!未定义书签。
3.9.6 安全建议	错误!未定义书签。
3.10 10.10.90.0 网段	错误!未定义书签。
3.10.1 风险分布	错误!未定义书签。
3.10.2 风险分类	错误!未定义书签。
3.10.3 主机风险等级列表	错误!未定义书签。
3.10.4 漏洞列表	错误!未定义书签。
3.10.5 脆弱应用帐号列表	错误!未定义书签。
3.10.6 安全建议	错误!未定义书签。
3.11 10.10.100.0 网段	错误!未定义书签。
3.11.1 风险分布	错误!未定义书签。
3.11.2 风险分类	错误!未定义书签。
3.11.3 主机风险等级列表	错误!未定义书签。

3.11.4 漏洞列表	错误!未定义书签。
3.11.5 脆弱应用帐号列表	错误!未定义书签。
3.11.6 安全建议	错误!未定义书签。
3.12 10.10.200.0 网段	错误!未定义书签。
3.12.1 风险分布	错误!未定义书签。
3.12.2 风险分类	错误!未定义书签。
3.12.3 主机风险等级列表	错误!未定义书签。
3.12.4 漏洞列表	错误!未定义书签。
3.12.5 脆弱应用帐号列表	错误!未定义书签。
3.12.6 安全建议	错误!未定义书签。
附录 A 原始扫描数据	10
附录 B 参考标准	10
B.1 单一漏洞危险等级评定标准	10
B.2 主机风险等级评定标准	10
B.3 网络风险等级评定标准	11

表格索引

表 1.1 扫描范围列表.....	1
表 3.1 按服务类型高、中风险分布列表.....	8
表 3.2 主机风险等级列表.....	8
表 3.3 漏洞列表.....	8
表 3.4 安全建议列表.....	9
表 3.5 按服务类型高、中风险分布列表.....	错误!未定义书签。
表 3.6 主机风险等级列表.....	错误!未定义书签。
表 3.7 漏洞列表.....	错误!未定义书签。
表 3.8 应用程序脆弱性列表.....	错误!未定义书签。
表 3.9 安全建议列表.....	错误!未定义书签。
表 3.10 按服务类型高、中风险分布列表.....	错误!未定义书签。
表 3.11 主机风险等级列表.....	错误!未定义书签。
表 3.12 漏洞列表.....	错误!未定义书签。
表 3.13 安全建议列表.....	错误!未定义书签。
表 3.14 按服务类型高、中风险分布列表.....	错误!未定义书签。
表 3.15 主机风险等级列表.....	错误!未定义书签。
表 3.16 漏洞列表.....	错误!未定义书签。
表 3.17 安全建议列表.....	错误!未定义书签。
表 3.18 按服务类型高、中风险分布列表.....	错误!未定义书签。
表 3.19 主机风险等级列表.....	错误!未定义书签。
表 3.20 漏洞列表.....	错误!未定义书签。
表 3.21 安全建议列表.....	错误!未定义书签。
表 3.22 按服务类型高、中风险分布列表.....	错误!未定义书签。
表 3.23 主机风险等级列表.....	错误!未定义书签。
表 3.24 漏洞列表.....	错误!未定义书签。
表 3.25 安全建议列表.....	错误!未定义书签。
表 3.26 按服务类型高、中风险分布列表.....	错误!未定义书签。
表 3.27 主机风险等级列表.....	错误!未定义书签。

表 3.28 漏洞列表.....	错误!未定义书签。
表 3.29 安全建议列表.....	错误!未定义书签。
表 3.30 按服务类型高、中风险分布列表.....	错误!未定义书签。
表 3.31 主机风险等级列表.....	错误!未定义书签。
表 3.32 漏洞列表.....	错误!未定义书签。
表 3.33 安全建议列表.....	错误!未定义书签。
表 3.34 按服务类型高、中风险分布列表.....	错误!未定义书签。
表 3.35 主机风险等级列表.....	错误!未定义书签。
表 3.36 漏洞列表.....	错误!未定义书签。
表 3.37 安全建议列表.....	错误!未定义书签。
表 3.38 按服务类型高、中风险分布列表.....	错误!未定义书签。
表 3.39 主机风险等级列表.....	错误!未定义书签。
表 3.40 漏洞列表.....	错误!未定义书签。
表 3.41 安全建议列表.....	错误!未定义书签。
表 3.42 按服务类型高、中风险分布列表.....	错误!未定义书签。
表 3.43 主机风险等级列表.....	错误!未定义书签。
表 3.44 漏洞列表.....	错误!未定义书签。
表 3.45 安全建议列表.....	错误!未定义书签。
表 3.46 按服务类型高、中风险分布列表.....	错误!未定义书签。
表 3.47 主机风险等级列表.....	错误!未定义书签。
表 3.48 漏洞列表.....	错误!未定义书签。
表 3.49 安全建议列表.....	错误!未定义书签。

插图索引

图 3.1 10.10.1.0 网段风险分布图.....	7
图 3.2 10.10.10.0 网段风险分布图.....	错误!未定义书签。
图 3.3 10.10.20.0 网段风险分布图.....	错误!未定义书签。
图 3.4 10.10.30.0 网段风险分布图.....	错误!未定义书签。
图 3.5 10.10.40.0 网段风险分布图.....	错误!未定义书签。
图 3.6 10.10.50.0 网段风险分布图.....	错误!未定义书签。
图 3.7 10.10.60.0 网段风险分布图.....	错误!未定义书签。
图 3.8 10.10.70.0 网段风险分布图.....	错误!未定义书签。
图 3.9 10.10.80.0 网段风险分布图.....	错误!未定义书签。
图 3.10 10.10.90.0 网段风险分布图.....	错误!未定义书签。
图 3.11 10.10.100.0 网段风险分布图.....	错误!未定义书签。
图 3.12 10.10.200.0 网段风险分布图.....	错误!未定义书签。

一. 概述

漏洞扫描主要是通过评估工具以远程扫描的方式对评估范围内的服务器和网络、安全设备进行安全扫描，通过远程的方式对被评估对象进行一系列的安全探测，以发现目标可能存在的安全隐患，是安全服务工作中发现信息系统脆弱性的主要技术手段之一。

通过漏洞扫描工作，可以详细的了解当前网络和系统中可能存在的潜在安全隐患，有效发现网络设备、操作系统和应用软件在用户账号、口令，安全漏洞，服务配置等方面存在的安全风险、漏洞和威胁，为进一步通过技术手段降低或解决发现的问题提供了参考依据和方法。

在 XX 网网络安全服务中，绿盟科技使用“极光”远程安全评估系统对 XX 网服务器进行了安全漏洞扫描，通过对扫描结果的分析，对发现的问题提供了建议解决方案，供系统管理员参考。

接下来将对扫描结果进行详细描述。

1.1 扫描范围

此次评估的范围为 XX 网服务器，IP 地址范围为 10.10.1.0、10.10.10.0、10.10.20.0、10.10.30.0、10.10.40.0、10.10.50.0、10.10.60.0、10.10.70.0、10.10.80.0、10.10.90.0、10.10.100.0、10.10.200.0 网段指定服务器。具体扫描范围如下表。

表 1.1 扫描范围列表

IP 地址段	IP 地址	负责人	Device
10.10.1.0	10.10.1.10	南园	f5
	10.10.1.253	蒋学军	entrust
10.10.10.0	10.10.10.105	南园	windows
	10.10.10.117	王冬杰	
	10.10.10.123	孙宝明	trackingapp01
	10.10.10.125	谢志胜	dhjms
	10.10.10.132	王冬杰	
	10.10.10.170	孙洪静	
	10.10.10.171	孙洪静	bgserver01
	10.10.10.176	孙洪静	bbs
	10.10.10.177	孙洪静	localhost

	10.10.10.199	刘文涛	
	10.10.10.21	谢志胜	localhost
	10.10.10.247	南园	monitor01
	10.10.10.249	南园	log
	10.10.10.250	南园	windows
	10.10.10.31	谢志胜	api
	10.10.10.32	王冬杰	
	10.10.10.40	刘文涛	
	10.10.10.41	刘文涛	dbtmp01
	10.10.10.43	刘文涛	
	10.10.10.45	刘文涛	slavedb
	10.10.10.46	刘文涛	etl-dbrac1
	10.10.10.47	刘文涛	etl-dbrac2
	10.10.10.48	刘文涛	streamdb2
	10.10.10.52	南园	Memcache03
	10.10.10.64	南园	image64
	10.10.10.69	南园	localhost
	10.10.10.77	孙洪静	encode01
	10.10.10.95	刘文涛	showdb
	10.10.10.96	刘文涛	adstdby
	10.10.10.98	刘文涛	logdb
	10.10.10.99	刘文涛	showdb01
10.10.20.0	10.10.20.101	谢志胜	nginx
	10.10.20.121	谢志胜	手机
10.10.30.0	10.10.30.101	谢志胜	agent
	10.10.30.11	谢志胜	seller01
	10.10.30.31	谢志胜	product
10.10.40.0	10.10.40.11	南园	windows
	10.10.40.12	谢志胜	job
	10.10.40.14	谢志胜	email
	10.10.40.21	谢志胜	jms
	10.10.40.31	谢志胜	spiderjob01
	10.10.40.53	孙宝明	dstorage03
	10.10.40.61	孙宝明	squid01
	10.10.40.71	孙宝明	hadoop01
	10.10.40.72	王冬杰	expjob
	10.10.40.73	王冬杰	expsrv01
	10.10.40.75	王冬杰	expweb01
	10.10.40.81	孙宝明	hadoop02

	10.10.40.91	王冬杰	memcached01
10.10.50.0	10.10.50.150	王冬杰	searchwebserver00
	10.10.50.20	王冬杰	indexserver00
	10.10.50.202	王冬杰	fenliesearchserver01
	10.10.50.222	王冬杰	The12th
	10.10.50.224	王冬杰	localhost
	10.10.50.45	王冬杰	memcached05
	10.10.50.50	王冬杰	ctrlserver00
	10.10.50.60	王冬杰	searchserver00
	10.10.50.83	王冬杰	sortserver03
10.10.60.0	10.10.60.240	王冬杰	searchtmp01
	10.10.60.60	王冬杰	sellerseo01
10.10.70.0	10.10.70.102	孙洪静	dhport02
10.10.80.0	10.10.80.101	南园	windows
	10.10.80.11	孙洪静	blog01
10.10.90.0	10.10.90.10	南园	upload01
	10.10.90.100	南园	localhost
	10.10.90.111	南园	vm
	10.10.90.20	南园	imgcache01
	10.10.90.30	南园	image01
	10.10.90.43	南园	qietu04
	10.10.90.50	南园	缓存服务器
10.10.100.0	10.10.100.11	刘文涛	
	10.10.100.12	刘文涛	
	10.10.100.13	刘文涛	
	10.10.100.91	刘文涛	
	10.10.100.92	刘文涛	
	10.10.100.93	刘文涛	
	10.10.100.94	刘文涛	
	10.10.100.97	刘文涛	
10.10.200.0	10.10.200.5	南园	

1.2 扫描时间

本次漏洞扫描工作开始时间为 XX 年 XX 月 XX 日，结束时间为 XX 年 XX 月 XX 日。

1.3 扫描内容

- ◆ 对扫描范围内的系统、服务进行信息获取；
- ◆ 对扫描范围内的系统、服务的风险进行评估分类；
- ◆ 对扫描范围内的系统、服务的主机漏洞进行评估；
- ◆ 对扫描范围内的系统、服务的账号进行评估；
- ◆ 对扫描范围内的系统、服务的脆弱应用账号进行评估；
- ◆ 对扫描范围内的系统、服务的软件漏洞进和配置进行评估；
- ◆ 提供系统以及应用软件安全漏洞修补建议；
- ◆ 提供主机风险列表以及漏洞列表；
- ◆ 提供应用脆弱性帐号列表；
- ◆ 提供部分管理制度建议

二. 扫描结果摘要

本次安全扫描服务的工作内容包括：

- 1、确认资产的有效性，找到未标示的主机 **10.10.10.40、10.10.10.43、10.10.90.50**，并确认其状态；
- 2、对 10.10.1.0、10.10.10.0、10.10.20.0、10.10.30.0、10.10.40.0、10.10.50.0、10.10.60.0、10.10.70.0、10.10.80.0、10.10.90.0、10.10.100.0、10.10.200.0 网段指定服务器进行了扫描；
- 3、对服务器主机状态，风险状态，主要安全问题进行分析；
- 4、通过发掘服务器中存在的安全隐患（系统隐患、配置缺陷），以便能根据这些检测信息修补漏洞缺陷，为维护服务器的健康稳定，提供相应的安全建议；

本次安全扫描服务结果：

- 1、本次对 10.10.1.0 网段指定主机安全扫描发现有计算机所安装的应用软件存在已知漏洞，**OpenSSH S/Key 远程信息泄露漏洞、OpenSSH 复制块远程拒绝服务漏洞、OpenSSH GSSAPI 信号处理程序内存两次释放漏洞**等。
- 2、本次对 10.10.10.0 网段指定主机安全扫描发现有计算机所安装的应用软件存在已知漏洞，**Apache 配置漏洞 1 个、Mysql 配置漏洞 13 个、nginx 漏洞 2 个、Oracle 漏洞和配置漏洞共 10 个、PHP 应用漏洞 7 个**等。
- 3、本次对 10.10.20.0 网段指定主机安全扫描发现所安装的应用软件存在已知漏洞，**OpenSSH S/Key 远程信息泄露漏洞、OpenSSH 复制块远程拒绝服务漏洞、OpenSSH GSSAPI 信号处理程序内存两次释放漏洞、OpenSSL 多个拒绝服务和无效证书验证漏洞、OpenSSL kssk_keytab_is_available()远程拒绝服务出漏洞**等。
- 4、本次对 10.10.30.0 网段指定主机安全扫描发现所安装的应用软件存在已知漏洞，**OpenSSH S/Key 远程信息泄露漏洞、OpenSSH 复制块远程拒绝服务漏洞、OpenSSH GSSAPI 信号处理程序内存两次释放漏洞**等。
- 5、本次对 10.10.40.0 网段指定主机安全扫描发现有计算机存在缺失 windows 安全更新存在 **Microsoft Windows Server 服务远程缓冲区溢出漏洞(MS06-040/KB921883)、Microsoft Windows Server 驱动内存信息泄露漏洞(MS06-035/KB917159)、Microsoft Windows Server 驱动 Mailslot 远程堆溢出漏洞(MS06-035/KB917159)**，

所安装的应用软件存在已知漏洞，**PostgreSQL 数据库空密码漏洞、OpenSSH S/Key 远程信息泄露漏洞、OpenSSH 复制块远程拒绝服务漏洞、OpenSSH GSSAPI 信号处理程序内存两次释放漏洞**等。

- 6、本次对 10.10.50.0 网段指定主机安全扫描发现有计算机所安装的应用软件存在已知漏洞，**Caucho Resin viewfile 远程文件及路径泄露漏洞、OpenSSH S/Key 远程信息泄露漏洞、OpenSSH 复制块远程拒绝服务漏洞、OpenSSH GSSAPI 信号处理程序内存两次释放漏洞**等。
- 7、本次对 10.10.60.0 网段指定主机安全扫描发现有计算机所安装的应用软件存在已知漏洞，**OpenSSH S/Key 远程信息泄露漏洞、OpenSSH 复制块远程拒绝服务漏洞、OpenSSH GSSAPI 信号处理程序内存两次释放漏洞**等。
- 8、本次对 10.10.70.0 网段指定主机安全扫描发现有计算机所安装的应用软件存在已知漏洞，**OpenSSH S/Key 远程信息泄露漏洞、OpenSSH 复制块远程拒绝服务漏洞、OpenSSH GSSAPI 信号处理程序内存两次释放漏洞**等。
- 9、本次对 10.10.80.0 网段指定主机全扫描发现有计算机存在缺失 windows 安全更新存在 **Windows Server 服务 RPC 请求缓冲区溢出漏洞(MS08-067)[精确扫描]**，所安装的应用软件存在已知漏洞，**OpenSSH S/Key 远程信息泄露漏洞、OpenSSH 复制块远程拒绝服务漏洞、OpenSSH GSSAPI 信号处理程序内存两次释放漏洞**等。
- 10、本次对 10.10.90.0 网段指定主机全扫描发现有计算机所安装的应用软件存在已知漏洞，**OpenSSH S/Key 远程信息泄露漏洞、OpenSSH 复制块远程拒绝服务漏洞、OpenSSH GSSAPI 信号处理程序内存两次释放漏洞**等。
- 11、本次对 10.10.100.0 网段指定主机全扫描发现有计算机所安装的应用软件存在已知漏洞，**OpenSSH S/Key 远程信息泄露漏洞、OpenSSH 复制块远程拒绝服务漏洞、OpenSSH GSSAPI 信号处理程序内存两次释放漏洞**等。
- 12、本次对 10.10.200.0 网段指定主机全扫描发现有计算机所安装的应用软件存在已知漏洞，**OpenSSH S/Key 远程信息泄露漏洞、OpenSSH 复制块远程拒绝服务漏洞、OpenSSH GSSAPI 信号处理程序内存两次释放漏洞**等。

三. 扫描结果分析

本次对 XX 网服务器进行扫描，按照 10.10.1.0、10.10.10.0、10.10.20.0、10.10.30.0、10.10.40.0、10.10.50.0、10.10.60.0、10.10.70.0、10.10.80.0、10.10.90.0、10.10.100.0、10.10.200.0 网段对以下指定 81 台设备进行了扫描，下面将对扫描结果进行详细分析。

3.1 10.10.1.0 网段

本次扫描中共发现 2 台有效设备，其中 1 台设备处于“比较危险”状态，1 台主机处于“比较安全”状态。

下面将对扫描结果进行详细分析。

3.1.1 风险分布

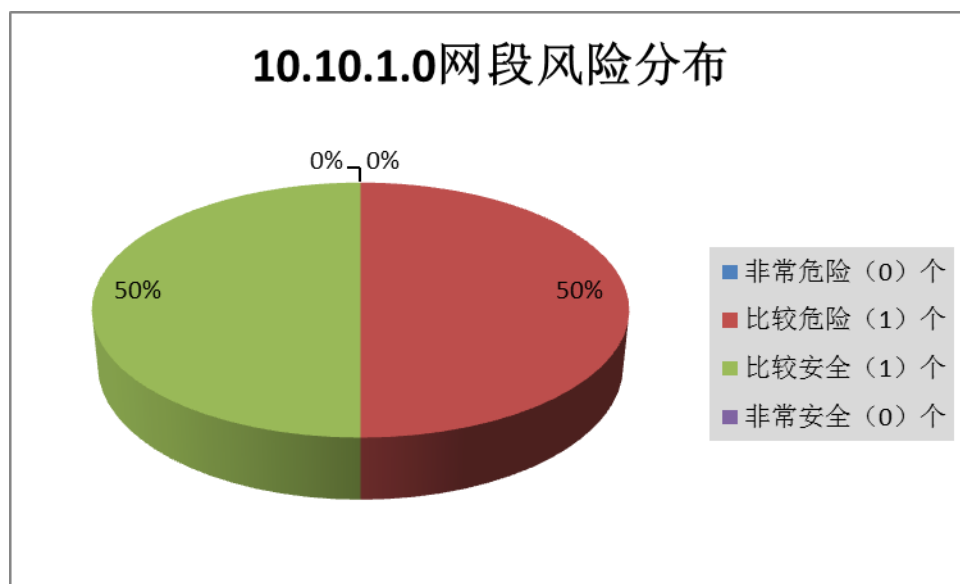


图 3.1 10.10.1.0 网段风险分布图

由风险分布图可以看出比较危险设备占设备总数的 50%。需要引起关注。

3.1.2 风险分类

从如下风险分类表中可以看出，SSH 存在的中风险漏洞较多，其余服务均为低风险漏洞。其中 SSH 高、中风险漏洞 4 个，占漏洞总数的 50%。

表 3.1 按服务类型高、中风险分布列表

分类名	高风险	中风险	低风险	总计
SSH	0	3	3	6
WWW	0	0	7	7
Kernel	0	0	1	1
数据库	0	0	1	1

3.1.3 主机风险等级列表





下表是主机风险等级列表，主机风险等级分为四个等级，分别为  非常危险， 比较危险， 比较安全， 非常安全（具体评分依据参看附录 B）。

表 3.2 主机风险等级列表

IP 地址	主机名	操作系统	风险等级
10.10.1.253		Unix/Linux	比较危险
10.10.1.10		Unix/Linux	比较安全

3.1.4 漏洞列表

漏洞列表描述了安全扫描中发现的各主机的安全漏洞，主要问题是

表 3.3 漏洞列表

影响 IP	漏洞名称
10.10.1.10	OpenSSH S/Key 远程信息泄露漏洞
10.10.1.253	OpenSSH S/Key 远程信息泄露漏洞
	OpenSSH 复制块远程拒绝服务漏洞
	OpenSSH GSSAPI 信号处理程序内存两次释放漏洞

3.1.5 脆弱应用帐号列表

在本次扫描中未发现 windows 系统、Linux 系统和应用程序存在脆弱账号问题。

3.1.6 安全建议

根据扫描结果和漏洞的风险等级，以及操作的难易程度和对系统的影响，绿盟科技建议优先处理系统和应用程序问题，修复系统漏洞，然后在充分测试的前提下修复应用程序的漏洞。提供以下建议供 XX 网相关人员参考。

表 3.4 安全建议列表

序号	漏洞描述	安全建议
1	OpenSSH S/Key 远程信息泄露漏洞	升级补丁以修复这个安全问题，请到厂商的主页下载： ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/
2	OpenSSH 复制块远程拒绝服务漏洞	如果您不能立刻安装补丁或者升级，建议您采取以下措施以降低威胁： 临时解决方法： * 停止使用 SSH 协议 1，改用 SSH 协议 2
3	OpenSSH GSSAPI 信号处理程序内存两次释放漏洞	OpenSSL 漏洞是根据版本判断的，建议访问 Apache 官方网站下载最新版本；

附录A 原始扫描数据



指定扫描主机_2011-06-09.zip





附录B 参考标准

B.1 单一漏洞危险等级评定标准

危险程度	危险值区域	危险程度说明
高	$8 \leq \text{漏洞风险值} \leq 10$	攻击者可以远程执行任意命令或者代码，或进行远程拒绝服务攻击。
中	$5 \leq \text{漏洞风险值} < 8$	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	$1 \leq \text{漏洞风险值} < 5$	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。

分值	评估标准
1	可远程获取 OS、应用版本信息。
2	开放了不必要或危险的服务，可远程获取系统敏感信息。
3	可远程进行受限的文件、数据读取。
4	可远程进行重要或不受限文件、数据读取。
5	可远程进行受限文件、数据修改。
6	可远程进行受限重要文件、数据修改。
7	可远程进行不受限的重要文件、数据修改，或对普通服务进行拒绝服务攻击。
8	可远程以普通用户身份执行命令或进行系统、网络级的拒绝服务攻击。
9	可远程以管理用户身份执行命令（受限、不太容易利用）。
10	可远程以管理用户身份执行命令（不受限、容易利用）。

B.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	$7 \leq \text{主机风险值} \leq 10$
 比较危险	$5 \leq \text{主机风险值} < 7$
 比较安全	$2 \leq \text{主机风险值} < 5$
 非常安全	$0 \leq \text{主机风险值} < 2$

1.将主机的漏洞按照分数的高低排序，依据漏洞的分数将漏洞威胁划分为高、中、低三个类别。

2.按照 绿盟科技 风险评估模型计算得到风险值。

注：高、中和低漏洞威胁的定义参见《单一漏洞威胁等级评定标准》

B.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	$8 \leq \text{主机风险值} \leq 10$
 比较危险	$5 \leq \text{主机风险值} < 8$
 比较安全	$1 \leq \text{主机风险值} < 5$
 非常安全	$0 \leq \text{主机风险值} < 1$

网络风险等级是网络中所有主机威胁分值的加权平均和。

1 对网络中的所有主机按照威胁分值进行高低排序，依据主机的威胁分值将主机风险划分为高、中、低三个类别。

2.按照 绿盟科技 风险评估模型计算得到风险值。

其中：

非常危险的主机定义为高风险；比较危险的主机定义为中风险；比较安全和非常安全的主机定义为低风险。