金鸡滩"安全漏洞扫描"

评估报告



榆林信安关键信息基础设施安全保护中心

报告生成时间：2023-10-10

**目 录**

[1. 综述信息 3](#_Toc1856)

[1.1. 任务信息 3](#_Toc2104)

[1.2. 风险分布 4](#_Toc6440)

[1.2.1. 主机风险分布 4](#_Toc8769)

[1.2.2. 漏洞风险分布 4](#_Toc11496)

[1.3. 资产综述 5](#_Toc19987)

[1.3.1. 操作系统 5](#_Toc20064)

[2. 风险类别 5](#_Toc27769)

[2.1. 漏洞风险类别 5](#_Toc5596)

[2.1.1. 服务分类 5](#_Toc11415)

[2.1.2. 应用分类 6](#_Toc5611)

[2.1.3. 系统分类 8](#_Toc24274)

[2.1.4. 威胁分类 8](#_Toc3366)

[2.1.5. 时间分类 8](#_Toc24575)

[2.1.6. CVE年份分类 10](#_Toc9000)

[3. 主机信息 11](#_Toc26364)

[4. 漏洞信息 25](#_Toc29249)

[5. 参考标准 43](#_Toc4130)

[5.1. 单一漏洞风险等级评定标准 43](#_Toc27553)

[5.2. 主机风险等级评定标准 44](#_Toc7471)

[5.3. 网络风险等级评定标准 44](#_Toc21014)

[6. 安全建议 45](#_Toc21914)

# 综述信息

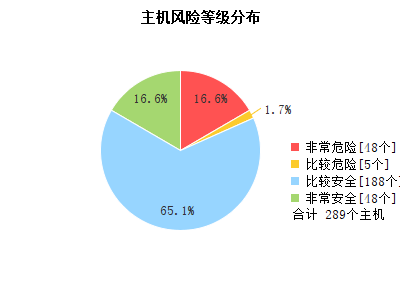
|  |
| --- |
| 本次评估范围内的11台有效主机及设备都已扫描完毕，安全漏洞扫描系统从如下几个方面进行分类统计：   1. 主机风险等级列表 2. 主机分布信息 3. 漏洞风险分类信息 4. 漏洞风险分布情况 5. 脆弱的帐号口令列表   网络的安全等级为非常危险，其中有7个设备的安全等级为非常危险。被评估网络的风险值为10。关于漏洞风险程度的分类规则以及主机风险分类规则，请参见《参考标准》。 |

## 任务信息

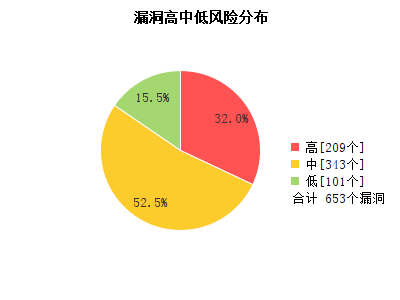
|  |  |
| --- | --- |
| 任务名称 | 金鸡滩漏洞扫描 |
| 网络风险值 | 10.0 |
| 任务类型 | 评估任务 |
| 存活主机 | 11 |
| 成功扫描主机 | 11 |
| 失败扫描主机 | 0 |
| 未扫描主机 | 0 |
| 系统版本信息 | V6.0R04F01SP06 |

## 风险分布

### 主机风险分布



### 漏洞风险分布



## 资产综述

### 操作系统

|  |  |  |
| --- | --- | --- |
| **操作系统** | **主机数量** | **比率** |
| windows | 6 | 55% |
| others | 3 | 27% |
| linux | 2 | 18% |
| 合计 | 11 | 100% |

# 风险类别

## 漏洞风险类别

### 服务分类

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **服务** | **高风险** | **中风险** | **低风险** | **合计** |
| WWW | 36 | 13 | 5 | 54 |
| 系统补丁 | 6 | 1 | 0 | 7 |
| SSL/TLS | 1 | 7 | 7 | 15 |
| 远程管理 | 1 | 0 | 2 | 3 |
| DNS | 0 | 2 | 2 | 4 |
| 其他 | 0 | 2 | 2 | 4 |
| SMB | 0 | 0 | 7 | 7 |
| SSH | 0 | 0 | 3 | 3 |
| 数据库 | 0 | 0 | 2 | 2 |
| Kernel | 0 | 0 | 2 | 2 |
| LDAP | 0 | 0 | 2 | 2 |
| DCE/RPC | 0 | 0 | 1 | 1 |
| 合计 |  |  |  |  |

### 应用分类

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **应用** | **高风险** | **中风险** | **低风险** | **合计** |
| Apache | 21 | 4 | 0 | 25 |
| OpenSSL | 7 | 9 | 0 | 16 |
| PHP | 5 | 2 | 0 | 7 |
| Windows SMB | 4 | 1 | 6 | 11 |
| 其他 | 3 | 4 | 13 | 20 |
| SSL | 1 | 4 | 3 | 8 |
| IIS | 1 | 0 | 0 | 1 |
| Windows 补丁 | 1 | 0 | 0 | 1 |
| Windows RDP | 1 | 0 | 0 | 1 |
| BIND | 0 | 1 | 1 | 2 |
| 04WebServer | 0 | 0 | 4 | 4 |
| MS SQL Server | 0 | 0 | 2 | 2 |
| OpenLDAP | 0 | 0 | 2 | 2 |
| OpenSSH | 0 | 0 | 2 | 2 |
| Radmin | 0 | 0 | 1 | 1 |
| SSH | 0 | 0 | 1 | 1 |
| 合计 |  |  |  |  |

### 系统分类

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **系统** | **高风险** | **中风险** | **低风险** | **合计** |
| 系统无关 | 37 | 23 | 28 | 88 |
| Windows | 7 | 2 | 7 | 16 |
| 合计 |  |  |  |  |

### 威胁分类

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **威胁** | **高风险** | **中风险** | **低风险** | **合计** |
| 其他 | 42 | 19 | 7 | 68 |
| 远程执行命令 | 2 | 0 | 0 | 2 |
| 远程信息泄露 | 0 | 4 | 24 | 28 |
| 不必要的服务 | 0 | 1 | 4 | 5 |
| 远程拒绝服务 | 0 | 1 | 0 | 1 |
| 合计 |  |  |  |  |

### 时间分类

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **时间** | **高风险** | **中风险** | **低风险** | **合计** |
| 2022年 | 17 | 8 | 1 | 26 |
| 2021年 | 10 | 0 | 0 | 10 |
| 2023年 | 9 | 7 | 0 | 16 |
| 2017年 | 5 | 1 | 0 | 6 |
| 2015年 | 1 | 2 | 0 | 3 |
| 2016年 | 1 | 0 | 2 | 3 |
| 2018年 | 1 | 0 | 0 | 1 |
| 1999年 | 0 | 1 | 9 | 10 |
| 2024年 | 0 | 1 | 5 | 6 |
| 2003年 | 0 | 1 | 1 | 2 |
| 2013年 | 0 | 1 | 1 | 2 |
| 2004年 | 0 | 1 | 0 | 1 |
| 2006年 | 0 | 1 | 0 | 1 |
| 2011年 | 0 | 1 | 0 | 1 |
| 2001年 | 0 | 0 | 9 | 9 |
| 2000年 | 0 | 0 | 2 | 2 |
| 2005年 | 0 | 0 | 2 | 2 |
| 2008年 | 0 | 0 | 1 | 1 |
| 2010年 | 0 | 0 | 1 | 1 |
| 2019年 | 0 | 0 | 1 | 1 |
| 合计 |  |  |  |  |

### CVE年份分类

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CVE年份** | **高风险** | **中风险** | **低风险** | **合计** |
| CVE-2022 | 19 | 8 | 0 | 27 |
| CVE-2021 | 10 | 1 | 0 | 11 |
| CVE-2023 | 6 | 5 | 0 | 11 |
| CVE-2017 | 5 | 1 | 0 | 6 |
| CVE-2006 | 1 | 1 | 0 | 2 |
| CVE-2015 | 1 | 1 | 0 | 2 |
| CVE-2016 | 1 | 0 | 0 | 1 |
| CVE-2018 | 1 | 0 | 0 | 1 |
| Others | 0 | 4 | 28 | 32 |
| CVE-2024 | 0 | 1 | 1 | 2 |
| CVE-2004 | 0 | 1 | 0 | 1 |
| CVE-2011 | 0 | 1 | 0 | 1 |
| CVE-2013 | 0 | 1 | 0 | 1 |
| CVE-1999 | 0 | 0 | 5 | 5 |
| CVE-2008 | 0 | 0 | 1 | 1 |
| 合计 |  |  |  |  |

# 主机信息

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **IP地址** | **主机名** | **操作系统** | **高** | **中** | **低** | **主机风险值** |
| 192.168.10.18 | WIN-OD0CJ4AND8G | Windows 8.1 or Windows Server 2012 R2 | 72 | 34 | 21 | 10 |
| 192.168.10.10 | WIN-56QRLEO40BV | Windows 8 or Windows Server 2012 | 3 | 3 | 17 | 10 |
| 192.168.10.7 | WIN-9O7PBMRGC14 | Windows Server 2012 R2 Standard 9600 | 6 | 1 | 11 | 8.4 |
| 192.168.10.3 |  | linux:linux\_kernel | 1 | 1 | 11 | 7.6 |
| 192.168.10.2 |  | linux:linux\_kernel | 1 | 1 | 11 | 7.6 |
| 192.168.10.17 | WIN-MB4BNTU55PU | Windows 8.1 or Windows Server 2012 R2 | 1 | 0 | 6 | 7 |
| 192.168.10.6 | WIN-UGTN846CAA7 | microsoft:windows | 1 | 2 | 13 | 7 |
| 192.168.10.1 |  | Comware 7.1.064 | 0 | 2 | 14 | 5.1 |
| 192.168.10.14 |  |  | 0 | 0 | 1 | 2.1 |
| 192.168.10.9 | DESKTOP-EPBJFLB | Windows 10, Version 1809 or Windows Server 2019, Version 1809 | 0 | 0 | 4 | 2.1 |
| 192.168.10.8 |  |  | 0 | 0 | 1 | 0 |

# 漏洞信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 HTTP.sys远程代码执行漏洞(MS15-034)(CVE-2015-1635)【原理扫描】 | 1/11 | 9% | 1 |
| 2 | Apache HTTP Server 缓冲区错误漏洞(CVE-2022-23943) | 1/11 | 9% | 2 |
| 3 | Apache HTTP Server 缓冲区错误漏洞(CVE-2021-39275) | 1/11 | 9% | 2 |
| 4 | Apache HTTP Server 环境问题漏洞(CVE-2022-22720) | 1/11 | 9% | 2 |
| 5 | OpenSSL 安全特征问题漏洞(CVE-2022-2068) | 1/11 | 9% | 2 |
| 6 | Apache HTTP Server 环境问题漏洞(CVE-2023-25690) | 1/11 | 9% | 2 |
| 7 | OpenSSL 操作系统命令注入漏洞(CVE-2022-1292) | 1/11 | 9% | 2 |
| 8 | Apache HTTP Server缓冲区溢出漏洞(CVE-2021-44790) | 1/11 | 9% | 2 |
| 9 | Apache HTTP Server 授权问题漏洞(CVE-2022-31813) | 1/11 | 9% | 2 |
| 10 | Apache HTTP Server 缓冲区错误漏洞(CVE-2022-28615) | 1/11 | 9% | 2 |
| 11 | Apache HTTP Server 输入验证错误漏洞(CVE-2022-22721) | 1/11 | 9% | 2 |
| 12 | Apache HTTP Server 安全漏洞(CVE-2022-36760) | 1/11 | 9% | 2 |
| 13 | Apache HTTP Server 代码问题漏洞(CVE-2021-40438) | 1/11 | 9% | 2 |
| 14 | PHP 安全漏洞(CVE-2022-31626) | 1/11 | 9% | 2 |
| 15 | PHP远程命令执行漏洞(CVE-2022-31626) | 1/11 | 9% | 2 |
| 16 | Apache HTTP Server SSRF漏洞(CVE-2021-44224) | 1/11 | 9% | 2 |
| 17 | PHP 安全漏洞(CVE-2022-31625) | 1/11 | 9% | 2 |
| 18 | Microsoft Windows SMB 远程代码执行漏洞(CVE-2017-0148)(MS17-010)【原理扫描】 | 1/11 | 9% | 1 |
| 19 | PHP远程命令执行漏洞(CVE-2022-31625) | 1/11 | 9% | 2 |
| 20 | Microsoft Windows SMB 远程代码执行漏洞(CVE-2017-0145)(MS17-010)【原理扫描】 | 1/11 | 9% | 1 |
| 21 | Microsoft Windows SMB 远程代码执行漏洞(CVE-2017-0146)(MS17-010)【原理扫描】 | 1/11 | 9% | 1 |
| 22 | Microsoft Windows SMB 远程代码执行漏洞(CVE-2017-0143)(MS17-010)【原理扫描】 | 1/11 | 9% | 1 |
| 23 | Microsoft Windows SMB 远程代码执行漏洞(CVE-2017-0144)(MS17-010)【原理扫描】 | 1/11 | 9% | 1 |
| 24 | SSL/TLS协议信息泄露漏洞(CVE-2016-2183)【原理扫描】【可验证】 | 2/11 | 18% | 2 |
| 25 | Apache HTTP Server 格式化字符串错误漏洞(CVE-2021-32785) | 1/11 | 9% | 2 |
| 26 | Perth Dropbear 授权问题漏洞(CVE-2021-36369) | 2/11 | 18% | 2 |
| 27 | OpenSSL 拒绝服务漏洞(CVE-2023-0464) | 1/11 | 9% | 2 |
| 28 | Apache HTTP Server 环境问题漏洞(CVE-2023-27522) | 1/11 | 9% | 2 |
| 29 | OpenSSL 安全漏洞（CVE-2022-4450） | 1/11 | 9% | 2 |
| 30 | OpenSSL 安全漏洞（CVE-2023-0215） | 1/11 | 9% | 2 |
| 31 | Apache HTTP Server 缓冲区错误漏洞(CVE-2022-30556) | 1/11 | 9% | 2 |
| 32 | Apache HTTP Server 缓冲区错误漏洞(CVE-2023-31122) | 1/11 | 9% | 2 |
| 33 | Apache HTTP Server 缓冲区错误漏洞(CVE-2006-20001) | 1/11 | 9% | 2 |
| 34 | Apache HTTP Server 输入验证错误漏洞(CVE-2022-29404) | 1/11 | 9% | 2 |
| 35 | Apache HTTP Server 输入验证错误漏洞(CVE-2022-26377) | 1/11 | 9% | 2 |
| 36 | Apache HTTP Server 输入验证错误漏洞(CVE-2022-22719) | 1/11 | 9% | 2 |
| 37 | Apache HTTP Server越界读取漏洞(CVE-2021-36160) | 1/11 | 9% | 2 |
| 38 | OpenSSL 安全漏洞(CVE-2022-0778) | 1/11 | 9% | 2 |
| 39 | Apache HTTP Server HTTP请求走私漏洞(CVE-2021-33193) | 1/11 | 9% | 2 |
| 40 | Apache HTTP Server空指针解引用漏洞(CVE-2021-34798) | 1/11 | 9% | 2 |
| 41 | OpenSSL 安全漏洞（CVE-2023-0286） | 1/11 | 9% | 2 |
| 42 | PHP 缓冲区错误漏洞(CVE-2022-31630) | 1/11 | 9% | 2 |
| 43 | Microsoft Windows CredSSP 远程执行代码漏洞(CVE-2018-0886)【原理扫描】 | 5/11 | 45% | 5 |
| 44 | PHP 安全漏洞(CVE-2021-21703) | 1/11 | 9% | 2 |
| 45 | 检测到目标SSL证书已过期【原理扫描】【可验证】 | 3/11 | 27% | 3 |
| 46 | PHP 安全漏洞(CVE-2022-31629) | 1/11 | 9% | 2 |
| 47 | Microsoft Windows SMB 信息泄漏漏洞(CVE-2017-0147)(MS17-010)【原理扫描】 | 1/11 | 9% | 1 |
| 48 | SSL/TLS RC4 信息泄露漏洞(CVE-2013-2566)【原理扫描】【可验证】 | 1/11 | 9% | 1 |
| 49 | Apache HTTP Server 资源管理错误漏洞(CVE-2023-45802) | 1/11 | 9% | 2 |
| 50 | OpenSSL 安全漏洞(CVE-2022-4304) | 1/11 | 9% | 2 |
| 51 | OpenSSL 加密问题漏洞(CVE-2021-4160) | 1/11 | 9% | 2 |
| 52 | 远端WWW服务支持TRACE请求 | 1/11 | 9% | 1 |
| 53 | PHP 安全漏洞(CVE-2022-31628) | 1/11 | 9% | 2 |
| 54 | OpenSSL 安全漏洞(CVE-2024-0727) | 1/11 | 9% | 2 |
| 55 | Apache HTTP Server 注入漏洞(CVE-2022-37436) | 1/11 | 9% | 2 |
| 56 | OpenSSL 安全漏洞(CVE-2023-5678) | 1/11 | 9% | 2 |
| 57 | OpenSSL 安全漏洞(CVE-2023-3817) | 1/11 | 9% | 2 |
| 58 | OpenSSL 证书校验不当漏洞(CVE-2023-0466) | 1/11 | 9% | 2 |
| 59 | OpenSSL 证书校验不当漏洞(CVE-2023-0465) | 1/11 | 9% | 2 |
| 60 | OpenSSL 安全漏洞（CVE-2022-2097） | 1/11 | 9% | 2 |
| 61 | Apache HTTP Server 缓冲区错误漏洞(CVE-2022-28330) | 1/11 | 9% | 2 |
| 62 | Apache HTTP Server 缓冲区错误漏洞(CVE-2022-28614) | 1/11 | 9% | 2 |
| 63 | 伪来源IP地址的DNS远程攻击漏洞(CVE-2006-0987)【原理扫描】 | 1/11 | 9% | 1 |
| 64 | 远端DNS服务允许递归查询 | 1/11 | 9% | 1 |
| 65 | 服务器支持 TLS Client-initiated 重协商攻击(CVE-2011-1473)【原理扫描】 | 1/11 | 9% | 1 |
| 66 | SSL/TLS 受诫礼(BAR-MITZVAH)攻击漏洞(CVE-2015-2808)【原理扫描】【可验证】 | 1/11 | 9% | 1 |
| 67 | SSL证书使用了弱hash算法【原理扫描】 | 2/11 | 18% | 2 |
| 68 | PHP 安全漏洞（CVE-2022-45307） | 1/11 | 9% | 2 |
| 69 | SSL/TLS 服务器瞬时 Diffie-Hellman 公共密钥过弱【原理扫描】 | 2/11 | 18% | 2 |
| 70 | pprof调试信息泄露漏洞【原理扫描】 | 3/11 | 27% | 3 |
| 71 | 使用了自签名证书【原理扫描】 | 5/11 | 45% | 5 |
| 72 | 获取SSL 证书中的hostname【原理扫描】 | 5/11 | 45% | 5 |
| 73 | SSL 证书链不完整【原理扫描】 | 5/11 | 45% | 5 |
| 74 | SSL 证书无法受到信任【原理扫描】 | 5/11 | 45% | 5 |
| 75 | 获取目标SSL证书过期时间【原理扫描】【可验证】 | 2/11 | 18% | 2 |
| 76 | OpenSSL 安全漏洞(CVE-2024-2511) | 1/11 | 9% | 2 |
| 77 | DNS 服务缓存远程信息披露窥探漏洞 | 1/11 | 9% | 1 |
| 78 | OpenSSH CBC模式信息泄露漏洞(CVE-2008-5161)【原理扫描】【可验证】 | 1/11 | 9% | 1 |
| 79 | ICMP timestamp请求响应漏洞 | 5/11 | 45% | 5 |
| 80 | ICMP网络掩码请求响应漏洞 | 1/11 | 9% | 1 |
| 81 | 可通过NetBIOS名字服务端口远程获取系统信息 | 4/11 | 36% | 4 |
| 82 | 可通过空会话访问远程主机 | 1/11 | 9% | 1 |
| 83 | 服务器服务正在运行 | 2/11 | 18% | 2 |
| 84 | Microsoft SQL Server远程版本信息泄漏 | 5/11 | 45% | 5 |
| 85 | 检测到目标主机开放着445/TCP，同时139/TCP关闭 | 3/11 | 27% | 3 |
| 86 | 检测到远端CIS服务正在运行中 | 1/11 | 9% | 1 |
| 87 | 远端VMWARE SERVER服务正在运行 | 1/11 | 9% | 1 |
| 88 | 服务器允许SSL会话恢复【原理扫描】 | 2/11 | 18% | 2 |
| 89 | 检测到目标主机加密通信支持的SSL加密算法【原理扫描】【可验证】 | 4/11 | 36% | 8 |
| 90 | LDAP服务器允许NULL BASE特性 | 1/11 | 9% | 1 |
| 91 | 工作站服务正在运行 | 5/11 | 45% | 5 |
| 92 | 可以获取远端Native Lan Manager版本 | 1/11 | 9% | 1 |
| 93 | 检测到远端LDAP服务正在运行中 | 1/11 | 9% | 1 |
| 94 | 嵌入式web服务器探测 | 2/11 | 18% | 2 |
| 95 | SSH版本信息可被获取 | 3/11 | 27% | 3 |
| 96 | 远程主机计算机名检测 | 4/11 | 36% | 5 |
| 97 | 远程桌面服务(RDS)协议探测 | 6/11 | 55% | 6 |
| 98 | 可通过HTTP获取远端WWW服务信息 | 6/11 | 55% | 8 |
| 99 | 探测到服务器支持的SSL加密协议【原理扫描】【可验证】 | 4/11 | 36% | 4 |
| 100 | 远端HSTS服务运行中 | 2/11 | 18% | 2 |
| 101 | 检测到远端DNS服务正在运行中 | 1/11 | 9% | 2 |
| 102 | 可通过HTTPS获取远端WWW服务信息 | 2/11 | 18% | 2 |
| 103 | Microsoft SQL Server数据库服务正在运行 | 5/11 | 45% | 5 |
| 104 | 探测到SSH服务器支持的算法 | 1/11 | 9% | 1 |
| **合计** | | | | 239 |

# 参考标准

## 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，或进对系统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。

## 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. 按照安全漏洞扫描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。

## 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. 按照安全漏洞扫描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。

# 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。

安全漏洞扫描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。

1. 建议所有Windows系统使用"Windows Update"进行更新。
2. 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。
3. 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。
4. 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。
5. 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。
6. 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。
7. 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。
8. 建议采用安全漏洞扫描系统定期对网络进行评估，真正做到未雨绸缪。