**Metasploitable2系统渗透测试报告**

|  |  |  |  |
| --- | --- | --- | --- |
| ■ 文档编号 | 2024 | ■ 密级 | 商业机密 |
| ■ 版本编号 | V1.0 | ■ 日期 | 2024-05-18 |

**2024网络攻防基础实践——任宇**

|  |
| --- |
| ■ 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，版权均属厦门大学信息学院网络攻防基础实践课程和**任宇**所有，受到有关产权及版权法保护。任何个人、机构未经厦门大学信息学院网络攻防基础实践课程和**任宇**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 |
| 2024年5月18日 | V1.0 | 创建报告 |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| ■ 适用性声明 |
| 本文档为网络攻防基础实践课程学生任宇（以下简称“网安—任宇”）实施渗透测试服务后提供的测试分析报告，适用于相关技术人员在对发现的漏洞进行安全修复时参考。 |

# 摘要

网络攻防基础实践课程学生任宇于2024年5月7日-2021年5月18日，对Metasploitable2系统进行了渗透测试工作，测试结果如下。

本次测试相关信息如下：

表1-1 渗透测试信息表

|  |  |  |  |
| --- | --- | --- | --- |
| 接入点 | 测试账号 | 测试时间 | 目标信息 |
| Kali | root | 2024年5月10日 | Metasploitable2 |
| Telnet（23端口） | msfadmin | 2024年5月10日 | 弱密码漏洞 |
| MySQL（3306端口） | root | 2024年5月10日 | 弱密码漏洞 |
| SSH（22端口） | root | 2024年5月10日 | 弱口令漏洞 |
| Tomcat（8180端口） | tomcat | 2024年5月10日 | 管理台默认口令漏洞 |
| PostgreSQL（5432端口） | postgres | 2024年5月10日 | 弱密码漏洞 |

详细安全问题汇总如下：

表1-2 问题汇总

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测试对象 | 问题等级 | 种类 | 数量 | 安全问题名称 |
| Metasploitable2 系统 | 严重问题 | 7种 | 7个 | 弱密码漏洞（Telnet、MySQL、PostgreSQL、VNC）  Vsftpd源码包后门漏洞  SSH弱口令漏洞  Samba MS-RPC Shell命令注入漏洞 |
| 中等问题 | 8种 | 8个 | NFS共享目录配置漏洞  UnrealIRCd后门漏洞  Java RMI SERVER命令执行漏洞  Ingreslock后门漏洞  PHP CGI参数注入执行漏洞  Tomcat管理台默认口令漏洞  Druby远程代码执行漏洞  Distcc后门漏洞 |
| 轻度问题 | 0种 | 0个 | - |
| 风险提示 | 1种 | 1个 | 多种服务配置不当导致系统易受攻击 |

# 服务概述

本次渗透测试工作是由网络攻防基础实践课程的学生任宇独立完成的。

任宇在2024年5月7日-2024年5月18日进行了渗透测试工作。在此期间，渗透测试小组利用部分前沿的攻击技术，使用成熟的黑客攻击手段，集合软件测试技术（标准）对指定网络、系统做入侵攻击测试，希望由此发现网站、应用系统中存在的安全漏洞和风险点。

## 2.1 测试流程

渗透测试服务流程定义为如下阶段。

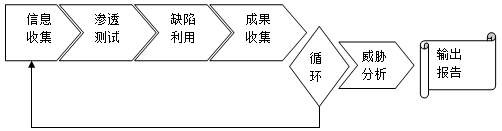


图2.1 渗透测试流程

信息收集：此阶段中，测试人员进行必要的信息收集，如 IP 地址、DNS 记录、软件版本信息、IP 段、Google中的公开信息等。

渗透测试：此阶段中，测试人员根据第一阶段获得的信息对网络、系统进行渗透测试。此阶段如果成功的话，可能获得普通权限。

缺陷利用：此阶段中，测试人员尝试由普通权限提升为管理员权限，获得对系统的完全控制权。在时间许可的情况下，必要时从第一阶段重新进行。

成果收集：此阶段中，测试人员对前期收集的各类弱点、漏洞等问题进行分类整理，集中展示。

威胁分析：此阶段中，测试人员对发现的上述问题进行威胁分类和分析其影响。

输出报告：此阶段中，测试人员根据测试和分析的结果编写直观的渗透测试服务报告。

## 2.2 风险管理及规避

为保障客户系统在渗透测试过程中稳定、安全的运转，我们将提供以下多种方式来进行风险规避。

**对象的选择**

为更大程度的避免风险的产生，渗透测试还可选择对备份系统进行测试。因为备份系统与在线系统所安装的应用和承载的数据差异较小，而其稳定性要求又比在线系统低，因此，选择对备份系统进行测试也是规避风险的一种常见方式。

**时间的控制**

从时间安排上，测试人员将将尽量避免在数据高峰时进行测试，以此来减小测试工作对被测试系统带来的压力。另外，测试人员在每次测试前也将通过电话、邮件等方式告知相关人员，以防止测试过程中出现意外情况。

**技术手段**

XXXX的渗透测试人员都具有丰富的经验和技能，在每一步测试前都会预估可能带来的后果，对于可能产生影响的测试（如：溢出攻击）将被记录并跳过，并在随后与客户协商决定是否进行测试及测试方法。

**监控措施**

针对每一系统进行测试前，测试人员都会告知被测试系统管理员，并且在测试过程中会随时关注目标系统的负荷等信息，一旦出现任何异常，将会停止测试。

**工具使用**

在使用工具测试的过程中，测试人员会通过设置线程、插件数量等参数来减少其对系统的压力，同时还会去除任何可能对目标系统带来危害的插件，如：远程溢出攻击类插件、拒绝服务攻击类插件等等。

## 2.3 参考标准

为了保证此次渗透测试的先进性、完备性、规范性，渗透工程师任宇将参考下列国内、国际与渗透测试有关的标准进行工作。

**国内可参考的标准、指南或规范：**

* ISO/IEC 27001:2005信息技术-安全技术-信息系统规范与使用指南
* ISO/IEC 13335-1: 2004 信息技术-安全技术-信息技术安全管理指南
* ISO/IEC TR 15443-1: 2005 信息技术安全保障框架
* ISO/IEC PDTR 19791: 2004 信息技术 安全技术 运行系统安全评估
* GB/T 20984-2007信息安全技术 信息安全风险评估规范
* GB/T 19715.1-2005 信息技术-信息技术安全管理指南
* GB/T 19716-2005 信息技术-信息安全管理实用规则
* GB/T 18336-2001 信息技术-安全技术-信息技术安全性评估准则
* GB/T17859-1999 计算机信息系统安全保护等级划分准则
* GB/T 20984-2007信息安全技术 信息安全风险评估规范
* GB/T 20988-2007信息系统灾难恢复规范
* GB/Z 20986-2007信息安全事件分类分级指南

**国际可参考的标准、指南或规范：**

* 信息系统审计标准（ISACA）G3 利用计算机辅助审计技术
* 信息系统审计标准（ISACA）G7 应有的职业谨慎
* 信息系统审计标准（ISACA）G9 不正当行为的审计考虑
* 信息系统审计标准（ISACA）G18 信息系统管理
* 信息系统审计标准（ISACA）G19 不正当及非法行为
* 信息系统审计标准（ISACA）G33 对网络使用的总体考虑
* CESG (CHECK) IT Health Check方法
* OWASP OWASP\_Testing\_Guide\_v3
* OWASP OWASP\_Development\_Guide\_2005
* OWASP OWASP\_Top\_10\_2010\_Chinese\_V1.0
* OWASP OWASP\_Top\_10\_2013-Chinese-V1.2
* OWASP OWASP\_Top\_10\_2017\_RC1\_V1.0
* OSSTMM OSSTMM\_Web\_App\_Alpha
* Web应用安全委员会（WASC）WASC Threat Classification v2

## 2.4 预期结果

通过实施渗透测试服务，可对贵方的系统起到如下推进作用：

**明确安全隐患**

渗透测试是一个从空间到面再到点的过程，测试人员模拟黑客的入侵，从外部整体切入最终落至某个威胁点并加以利用，最终对整个网络产生威胁，以此明确整体系统中的安全隐患点。

**提高安全意识**

如上所述，任何的隐患在渗透测试服务中都可能造成“千里之堤溃于蚁穴”的效果，因此渗透测试服务可有效督促管理人员杜绝任何一处小的缺陷，从而降低整体风险。

**提高安全技能**

在测试人员与用户的交互过程中，可提升用户的技能。另外，通过专业的渗透测试报告，也能为用户提供当前流行安全问题的参考。

# 测试服务说明

## 3.1 测试对象与环境

本次渗透测试按着事先约定的测试范围展开测试工作，测试对象如下所示：

表3-1 测试对象

|  |  |  |
| --- | --- | --- |
| 测试对象 | 测试地址 | 应用版本 |
| Metasploitable2 |  |  |

表3-2 测试帐号

|  |  |  |  |
| --- | --- | --- | --- |
| 测试账号 | 账号 | 密码 | Ukey |
| 高权限 | msfadmin | \*\*\*\*\*\* | 无 |

测试过程中，XXXX测试小组使用过多个IP地址开展的分析工作，地址如下：

表3-3 测试IP

|  |  |  |  |
| --- | --- | --- | --- |
| IP地址 | IP地址 | IP地址 | IP地址 |
| 192.168.232.164 |  |  |  |

在此通知相关人员在对受测试的目标站点服务器、相应的网络入侵检测系统进行安全监控和日志分析时，排除以上IP地址产生的任何违规信息，以保证分析结果的准确有效。

## 3.2 测试时间与人员

本次渗透测试按着事先约定的测试时间开展，如下所示：

测试时间

|  |  |  |  |
| --- | --- | --- | --- |
| 测试工作时间段 | | | |
| 起始时间 | 2024年5月7日 | 结束时间 | 2024年5月18日 |

本次测试小组参与渗透测试人员，如下所示：

测试人员

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 参测人员名单 | | | | | |
| 姓名 | 任宇 | 所属部门 | 厦门大学信息学院网络攻防基础实践课程 | 联系方式 | QQ：2497585385 |

## 3.3 工具及相关资源

本次渗透测试使用部分工具如下：

测试工具：Nmap

|  |  |
| --- | --- |
| 工具名称 | Nmap |
| 工具用途 | 端口扫描，服务识别，操作系统指纹识别 |
| 相关信息 | http://nmap.org/ |

测试工具：MetasploitFramework

|  |  |
| --- | --- |
| 工具名称 | Metasploit Framework |
| 工具用途 | 漏洞扫描与利用，安全研究与开发，渗透测试 |
| 相关信息 | https://www.metasploit.com/ |

在具体的测试和分析过程中，测试小组主要在Kali平台上，使用Nmap和Metasploit Framework对指定的测试对象进行了分析、校验和测试。因此，漏洞分析检测到的部分安全问题可能与特定的操作系统、软件版本有具体关系。提醒后期实施漏洞修复工作的人员特别注意其中的差异。

# 测试结果与建议

## 漏洞01：

|  |  |
| --- | --- |
| 漏洞地址 | Telnet（23端口） |
| 漏洞描述 | Telnet服务使用弱密码 |
| 漏洞等级 | 严重 |
| 漏洞详情 | Telnet服务的用户名和密码均为默认的msfadmin，攻击者可以轻松获取系统访问权限。 |
| 整改建议 | 禁用Telnet服务，或者更改默认用户名和密码为强密码。 |

## 漏洞02：

|  |  |
| --- | --- |
| 漏洞地址： | MySQL（3306端口） |
| 漏洞描述： | MySQL服务使用弱密码 |
| 漏洞等级 | 严重 |
| 漏洞详情 | MySQL服务的root用户没有设置密码，攻击者可以直接访问数据库，获取敏感信息。 |
| 整改建议： | 设置强密码，并限制外部访问MySQL服务。 |

## 漏洞03：

|  |  |
| --- | --- |
| 漏洞地址 | PostgreSQL（5432端口） |
| 漏洞描述 | PostgreSQL服务使用弱密码 |
| 漏洞等级 | 严重 |
| 漏洞详情 | PostgreSQL服务的postgres用户没有设置密码，攻击者可以直接访问数据库。 |
| 整改建议 | 设置强密码，并限制外部访问PostgreSQL服务。 |

## 漏洞04：

|  |  |
| --- | --- |
| 漏洞地址 | VNC（5900端口） |
| 漏洞描述 | VNC服务使用弱密码 |
| 漏洞等级 | 严重 |
| 漏洞详情 | VNC服务的密码为默认的password，攻击者可以轻松获得远程桌面控制权。 |
| 整改建议 | 更改默认密码为强密码，并限制VNC服务的外部访问。 |

## 漏洞05：

|  |  |
| --- | --- |
| 漏洞地址 | Vsftpd（21端口） |
| 漏洞描述 | Vsftpd源码包后门漏洞 |
| 漏洞等级 | 严重 |
| 漏洞详情 | 在特定版本的vsftpd服务器中被植入恶意代码，当用户名以“:)”结尾时，服务器会在6200端口监听并执行任意代码。 |
| 整改建议 | 更新Vsftpd至最新版本，确保未使用受影响版本。 |

## 漏洞06：

|  |  |
| --- | --- |
| 漏洞地址 | SSH（22端口） |
| 漏洞描述 | SSH服务使用弱口令 |
| 漏洞等级 | 严重 |
| 漏洞详情 | SSH服务的root用户使用弱密码，攻击者可以通过暴力破解获取系统访问权限。 |
| 整改建议 | 设置强密码，禁用root用户的SSH登录，启用基于密钥的身份验证。 |

## 漏洞07：

|  |  |
| --- | --- |
| 漏洞地址 | Samba（139端口） |
| 漏洞描述 | Samba MS-RPC Shell命令注入漏洞 |
| 漏洞等级 | 严重 |
| 漏洞详情 | Samba服务的MS-RPC接口存在命令注入漏洞，攻击者可以通过恶意输入在/bin/sh中执行任意命令。 |
| 整改建议 | 更新Samba至最新版本，并严格配置smb.conf文件。 |

## 漏洞08：

|  |  |
| --- | --- |
| 漏洞地址 | NFS（2049端口） |
| 漏洞描述 | NFS共享目录配置漏洞 |
| 漏洞等级 | 中等 |
| 漏洞详情 | NFS服务配置不当，允许远程用户写入/root/.ssh/authorized\_keys文件，实现无密码SSH登录。 |
| 整改建议 | 重新配置NFS服务，限制共享目录的写入权限，并移除不必要的共享目录。 |

## 漏洞09：

|  |  |
| --- | --- |
| 漏洞地址 | UnrealIRCd（6667端口） |
| 漏洞描述 | UnrealIRCd后门漏洞 |
| 漏洞等级 | 中等 |
| 漏洞详情 | 在2009年11月至2010年6月间分布于某些镜像站点的UnrealIRCd中包含恶意代码，允许远程攻击者执行任意代码。 |
| 整改建议 | 更新UnrealIRCd至最新版本，确保未使用受影响版本。 |

## 漏洞10：

|  |  |
| --- | --- |
| 漏洞地址 | Java RMI（1099端口） |
| 漏洞描述 | Java RMI SERVER命令执行漏洞 |
| 漏洞等级 | 中等 |
| 漏洞详情 | Java RMI Server的RMI注册表和RMI激活服务的默认配置存在漏洞，攻击者可以利用漏洞执行任意代码。 |
| 整改建议 | 重新配置RMI服务，限制访问，并使用安全的RMI配置。 |

## 漏洞11：

|  |  |
| --- | --- |
| 漏洞地址 | Ingreslock（1524端口） |
| 漏洞描述 | Ingreslock后门漏洞 |
| 漏洞等级 | 中等 |
| 漏洞详情 | Ingreslock后门程序运行在1524端口，允许攻击者通过该端口直接获得root权限。 |
| 整改建议 | 关闭Ingreslock服务，或者限制访问该端口。 |

## 漏洞12：

|  |  |
| --- | --- |
| 漏洞地址 | PHP CGI（80端口） |
| 漏洞描述 | PHP CGI参数注入执行漏洞 |
| 漏洞等级 | 中等 |
| 漏洞详情 | PHP CGI脚本未正确处理请求参数，允许远程攻击者在请求参数中插入执行命令。 |
| 整改建议 | 更新PHP至最新版本，并确保CGI脚本正确处理请求参数。 |

## 漏洞13：

|  |  |
| --- | --- |
| 漏洞地址 | Tomcat（8180端口） |
| 漏洞描述 | Tomcat管理台默认口令漏洞 |
| 漏洞等级 | 中等 |
| 漏洞详情 | Tomcat管理台安装后未及时修改默认管理账户和密码，攻击者可以部署任意web应用。 |
| 整改建议 | 修改默认管理账户和密码为强密码，并限制管理台的外部访问。 |

## 漏洞14：

|  |  |
| --- | --- |
| 漏洞地址 | Druby（任意端口） |
| 漏洞描述 | Druby远程代码执行漏洞 |
| 漏洞等级 | 中等 |
| 漏洞详情 | Druby配置不当会被滥用执行命令，但在MSF未找到对应渗透模块。 |
| 整改建议 | 重新配置Druby服务，限制外部访问，并使用安全的Druby配置。 |

## 漏洞15：

|  |  |
| --- | --- |
| 漏洞地址 | Distcc（3623端口） |
| 漏洞描述 | Distcc后门漏洞 |
| 漏洞等级 | 中等 |
| 漏洞详情 | Distcc用于分布式编译，如果配置不严格，容易被滥用执行任意命令。 |
| 整改建议 | 重新配置Distcc服务，限制外部访问，并移除不必要的服务。 |

# 致谢

在本次远程渗透测试过程中，厦门大学网络攻防安全基础课程渗透测试小组感谢相关机构人员和在渗透测试过程中进行沟通、协调的相关部门和人员的大力配合，使得我们的工作能够顺利完成。

附录A 安全等级评定

|  |  |
| --- | --- |
| 安全等级 | 资源内容描述 |
| 远程不安全系统  （符合任何一个条件） | 存在一个或一个以上严重的安全问题，可直接导致系统受到破坏；  与其他非安全系统连接，同时存在相互信任关系（或帐号互通）的主机；  发现已经被人入侵且留下远程后门的主机；  存在3个以上中等安全问题的主机；  与其他非安全系统在一个共享网络中，同时远程维护明文传输口令；  完全不能抵抗小规模的拒绝服务攻击 |
| 远程一般安全系统  （符合任何一个条件） | 存在一个或一个以上中等安全问题的主机；  开放过多服务，同时可能被利用来进行拒绝服务的主机；  与其他非安全系统直接连接，但暂时不存在直接信任(或帐号互通)关系；  远程维护通过明文的方式传递信息；  存在三个以上轻度安全问题的主机；  只能抵御最低级的拒绝服务攻击； |
| 远程安全系统  （符合全部条件） | 最多存在1-2个轻度安全问题；  远程维护方式安全；  与不安全或一般安全系统相对独立；  能抵挡一定规模的拒绝服务攻击。 |

附录B 风险程度分级

风险值计算方式说明如下：

漏洞风险值=F×Y×I

影响范围系数F

大（3）：能够获取大量数据、敏感数据或影响大量用户。

中（2）：能够获取部分数据、一般敏感数据或影响部分用户

小（1）：能够获取少量数据、非敏感数据或影响少量用户

漏洞系数Y

权限获取类（20）:可获取服务器权限的漏洞

数据获取类（8）：可导致结构化数据批量获取的漏洞

非法访问类（6）：以非正常方式访问资源的漏洞

业务缺陷类（5）：业务逻辑不完善导致的漏洞

暴力破解类（4）：与登录或认证凭据相关的暴力破解

客户端攻击类（3）：攻击其他客户端的漏洞

信息泄露类（3）：泄漏敏感的技术类信息及非结构化数据的漏洞

辅助攻击类（1）：单独存在不能形成攻击，但可以增加其他攻击手段效果的漏洞

其中权限获取类、暴力破解类、辅助攻击类影响范围系数F固定为1。

系统重要性系数I

核心应用系统（4）：主站、网银、商城等盈利站点

普通应用系统（2）：客服、OA等辅助类站点

边缘应用系统（1）：单一功能、单一接口类站点

风险程度的分级方式说明如下：

严重：风险值>18，直接导致系统被入侵或数据被破坏，一旦发生，就是严重的安全事件。建议紧急修复。

中等：6 ≤风险值≤18可能导致重要信息的泄漏、系统拒绝服务或有较高可能导致系统被入侵控制。

轻度：风险值小于6敏感信息泄漏或存在轻微安全问题，一般不会产生严重的安全事件。

附录C WASC威胁分类

WASC是一个非营利组织，WASC支持商业安全技术的合理使用。主要目标是研究协助解决Web软体安全之标准、工具与技术文件，长期致力于协助政府或企业了解并改善网页应用程式与网页服务的安全性。

WASC威胁分类主要内容如下：

|  |  |
| --- | --- |
| 认证和授权类 | 命令执行类 |
| 暴力攻击 | LDAP注入 |
| 认证不充分 | SSI注入 |
| 会话定置 | SQL注入 |
| 会话期限不充分 | Xpath注入 |
| 凭证/会话预测 | 操作系统命令 |
| 授权不充分 | 格式字符串攻击 |
| 逻辑攻击类 | 缓冲区溢出 |
| 功能滥用 | 信息泄漏类 |
| 拒绝服务 | 可预测资源定位 |
| 客户端攻击类 | 路径遍历 |
| 跨站点脚本编制 | 目录索引 |
| 内容电子欺骗 | 信息泄露 |