信息系统密码应用的渗透测试与隐患点分析

廖旭亮 李建**

南宁学院信息工程学院，南宁，530200

摘 要 针对网络信息系统等级保护、密码应用基本要求，利用开源项目 CMS 搭建模拟的信息系统，使用 Nmap、Dirsearch 等渗试测试工具对搭建的信息系统进行攻击，根据收集到的信息系统薄弱点进行安全测试，最终获得服务器控制权限。结合信息系统密码应用基本要求分析渗透测试的攻击过程以及最终成果，阐明该虚拟系统的设计缺陷，对于密码应用不规范之处进行优化处置并给出相应的修复建议，完成漏洞的修补工作。

关键字 信息系统，密码应用，渗透测试，隐患点分析

Penetration Testing and Weak Point Analysis of the Password Application in Information System

Liao Xuliang Li Jian

School of Information Engineering
Nanning University
Nanning 530200, China
992959839@qq.com

Abstract—Aiming at the basic requirements of network information system level protection and password application, the open source project CMS was used to build a simulated information system. Then, the Nmap, Dirsearch and other penetration test tools were used to attack the built information system, the security tests is performed according to the collected weak points of the information system, and finally the server control authority was obtained. Combined with the basic requirements of information system password application, the attack process and final results of penetration test were analyzed, and the design defects of the virtual system were clarified. Finally, we optimized the places where the password application is not standardized and give corresponding repair suggestions to complete the repair of vulnerabilities.

Key words— Information system, Password application, Penetration testing, Weak point analysis

1 引 言

随着 5G 通信技术的快速发展，移动互联网已经完全渗透到人们的生活当中，无论在基础的衣、食、住、行方面，还是在教育、金融、航空航天等尖端领域都发挥着无以伦比的作用。但是互联网给人类带来了巨大便利的同时，也带来了前所未有的安全挑战。电信诈骗、勒索病毒、隐私泄露等威胁如影随形。

在现代社会中，信息系统数量众多，每一个系统或多或少存在着安全隐患，如弱口令、备份文件泄露、配置文件泄露、调试页面未关闭等，这些漏洞可被“黑客”利用，从而导致其窃取服务器的控制权限，从而威胁整个内网安全[1]。

数据是信息系统承载的最宝贵的战略资源，若数据安全得不到保障，整个信息系统就失去了存在的价值，因此数据安全的重要性无与伦比。将密码应用于信息系统中的数据传递、数据显示、数据存储等方面，将有效地保护该“战略资源”，使其更加稳定、更加安全[2]。为此，我国先后颁布了《中华人民共和国密码法》和 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》等法律法规和技术标准，旨在规范密码应用和管理，促进密码事业发展，保障网络与信息安全，提升密码工作科学化、规范化、法治化水平。国家密码管理局副局长刘平曾表示:“密码就像网络空间的 DNA，是构筑网络信息系统免疫体系和网络信任体系的基石，直接关系国家政治安全、经济安全、国防安全和信息安全，是保护党和国家根本利益的战略性资源，是国之重器。”因此，如何检测信息系统密码应用的能力和水平，是摆在政府、产业界、学术界一个重要的研究课题。

从密码学与应用密码学来看，美国等发达国家起步早，具备先发优势，其制定的密码应用标准和算法至今仍有理论先进性[3]。我国密码学领域起步较晚，

★**基金资助**：本文得到南宁学院教学质量与教学改革工程项目（《网络安全》核心课程）(2022BKHXK09)资助助。
★★ **通讯作者**：李建，教授，943667593@qq.com

但正逐步赶上甚至超越。SM1、SM2、SM3、SM4、SM7、SM9 是国家密码局认定的国产密码算法，其中，SM2、SM3、SM4、SM9 算法已 ISO/IEC 国际标准。

渗透测试方面，国外（以美国为例）的渗透测试起步早，已有很多机构对信息系统提供渗透测试服务，有较健全的工作准则，如 ISECOM 安全编写的开源安全测试方法 OSSTMM，美国国家标准和技术研究所公布的安全测试指导准则 SP800-115，他们都给出了关于渗透测试的方法及其流程[4]。除相关标准之外还设有许多优秀的开源项目，如 OWASP（The Open Web Application Security Project）项目，以供从业者或爱好者学习，并且设立应急响应平台以及众测机制，平台有着完善的奖励机制，当“白帽子”提交漏洞之后，平台会给予相应奖励，其中 Hackerone 最为人所知。国内渗透测试方面稍弱于美国，起步晚，大众的网络安全认识较为薄弱，大部分开发人员对系统安全加固的了解不够深刻，就很容易造成系统漏洞，一旦被黑客利用损失就无从估量了。自 2016 年《网络安全法》颁布之后，国家要求关键信息基础设施的运营者“制定网络安全事件应急预案，并定期进行演练”（护网行动），护网行动的出现加大了重要事业单位、国企、民企对网络安全的重视，也是我国网络安全史上的一个重要里程碑。

本文拟搭建基于密码技术的网络服务平台，模拟信息系统密码应用安全测评任务，运用 Kali Linux、Nmap、Dirsearch、Wireshark、Metasploit 等渗透系统或工具对信息系统模型进行安全性检测[5]，发现密码应用方面存在的薄弱环节，评估信息系统存在的安全风险，采取有效措施堵塞安全漏洞，为开展信息系统密码应用整改提供客观依据和解决方案。

2 渗透测试

2.1 渗透测试

渗透测试是安全从业人员模拟黑客对信息系统进行安全测试的一种行为，渗透测试工程师对被测试单位的网络、主机、应用及数据进行分析，以发现信息系统存在的脆弱点，并合理利用这些脆弱点，将漏洞危害提升[6]。根据 OWASP 发布的高风险漏洞列表,包括 SQL 注入漏洞、跨站脚本漏洞、文件上传漏洞和安全配置错误等等，网站一旦出现上述中的漏洞，并被恶意攻击者利用的话，都可能会造成不可挽回的巨大损失。而与之不同的话，渗透工程师则以发现漏洞、验证漏洞危害为主，只会对其进行授权范围内的测试，不会进行脱库、挖矿、DDOS 攻击、CC 攻击等非法操作。

简要理解渗透测试，其中渗透二字的理解代表着由浅入深、由外至内，安全工程师通过信息收集，了解目标对象的资产分布，分析整个资产中的薄弱点，首先从薄弱点入手，进行安全排查，再一步步深入系统，通过各种漏洞利用获取到目标的服务器权限，至此外网打点完成，后渗透阶段就由此服务器进入内网测试。既然是安全测试，就会存在安全风险，可能会导致网络系统在测试中受到损坏，安全测试人员也会对其进行控制，尽可能的消除风险，提升网络渗透测试的安全程度，在必要时会向客户申请某个重要功能点的测试情况，表明可能存在的危害[7]。

渗透测试的主要目的是消除信息系统的未知风险，提高信息系统的安全性与稳定性，并且渗透测试结果也是很好的内部网络安全培训的案例，可提高相关负责人员的安全意识。随着信息安全等级保护制度的实施，渗透测试就显得更为重要，它是信息安全风险评估中的关键一环，并且渗透测试在检测密码应用是否规范时具备很高可行性[8]。

2.2 渗透测试分类

渗透测试从测试方式来区分，分为三类，白盒测试、黑盒测试和灰盒测试。将软件程序比作一个盒子，白盒测试就是能明确看到盒子内部的结构，就是指渗透测试工程师在拥有客户所有知识（包括资产分布、网络架构、测试账号、甚至系统源码）的情况下进行测试；黑盒测试则不能将这个盒子打开，不用考虑内部的结构和特性，只能根据客户提供的测试范围，从无到有的逐个子系统、逐个功能点进行风险排查。而灰盒测试可比作盒子处于打开状态，却未完全开放，我们只能了解其中一部分的结构特性，这是一种综合测试技术，多用于集成测试。

白盒测试的优点在于：当测试工程师拥有所有的内部知识，并可以在不需要害怕被阻断的情况下任意地实施攻击行为，其找出信息系统漏洞的效率就高，且得到资产分布、网络架构、系统源码之后就能通过网络拓扑分析、代码审计等方式对系统进行一次较全面的安全隐患筛查，从而发现大部分的系统薄弱点。其缺点是无法有效地预测客户的应急响应能力，且对于信息系统业务的逻辑性漏洞难以通过代码直观的发现，故还需结合业务的具体流程进行测试。

黑盒测试的测试周期较长，且对安全人员的技术的要求也较高，能更逼真地模拟一次真正的黑客攻击过程。黑盒测试依靠测试人员的专业技能探测并获取目标系统的可用信息点，接着就是信息点的利用，或 SQL 注入点或文件上传点或者是某个平台的通用漏洞等等，最终目的就是获取目标服务器的控制权限。获得服务器权限后，此次的渗透测试就较为圆满了，接

着就是跟进客户的需求，决定是否进行提权、内网渗透、以及从多方面渗透，找出更多的信息系统薄弱点。

灰盒测试的测试结果可以对应到程序内部路径，便于漏洞点的定位、分析、解决，它是黑盒测试的补充，能够防止某些不常用或不显眼的功能点被遗忘，也能在一定程度上减轻测试过程中对系统造成的可能影响。其缺点是投入时间、对安全人员的技术要求均比黑盒测试高，测试深度不如白盒测试。

可根据客户的具体情况选择是否使用漏洞扫描器，自动化加手工验证的效率会有所提高，漏洞扫描器在时间紧任务重的情况下是一大助力，扫描器能对业务信息进行自动化的测试，根据本身的漏洞规则库向目标服务器发送大量的数据包，枚举所有可能存在的漏洞类型，也能根据使用者的设置情况针对某一类型的漏洞进行单一漏洞扫描，如今常见的扫描器有AWVS、Appscan、Nessus 等，其存在一定的误报率，最后需安全工程师去校验扫描结果[9]。

3 测试环境搭建

3.1 测试环境搭建

测试环境由三台 PC 机组成，其中一台 Centos7 搭建 Web 服务，是渗透测试目标服务器；一台 Windows Server2008r2 用作目标内网 PC；一台 Kali Linux 作为攻击机。三台 PC 机均通过虚拟化软件 VMware 部署。虚拟测试网络拓扑如图 1 所示。

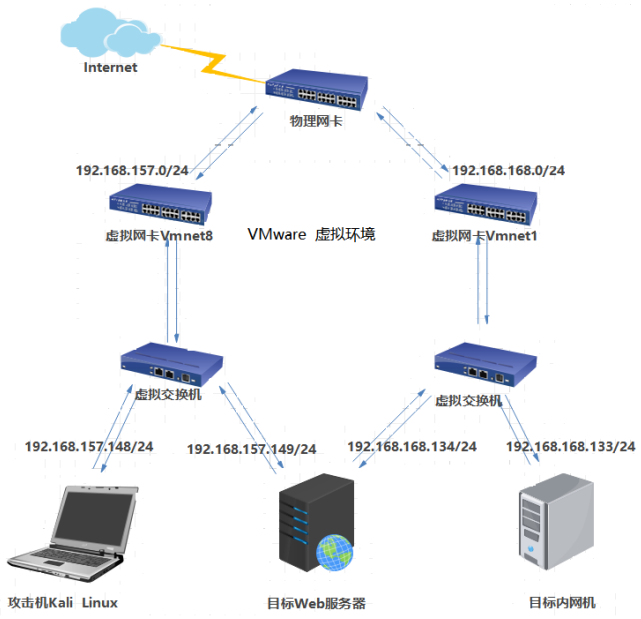

图 1 虚拟测试网络拓扑

因规定不能向未授权的网站进行渗透测试，故利用开源的内容管理系统（CMS）搭建一个简易的测试环境，并在数据库写入基础的测试数据，以方便后续项目提取数据进行密码应用安全性分析。测试环境利用迅睿 CMS 搭建，版本为最新版 v4.5.5，该 CMS 是一款基于 CodeIgniter4 开发的内容管理框架，在 CodeIgniter4 框架上增加了多个实用模块，如基础内容模块管理、后台管理、插件功能、迅睿模板引擎、常用扩展类、常用模型类等程序组件，让 CI4 框架中文化，能更好的服务于国内的生态环境。Web 环境使用 LNMP，即 Centos Linux、Nginx、Mysql 和 PHP。

3.3 测试工具简介

（1）Kali

Kali 是一个基于 Debian 的 Linux 发行版，与 Ubuntu、Red Hat等发行版不同，Kali linux不适合日常使用和充当服务器，它主要应用于渗透测试方面，该系统中集成了大量的开源工具以及各种环境配置，从而让安全测试人员免去工具安装、环境搭建等繁琐工作，能大幅度提高工作效率。如下介绍的工具均集成在Kali当中，无需下载安装。

（2）Nmap

Nmap是一个网络扫描工具，主要作用是对网络设备进行主机存活探测、端口扫描、服务版本与操作系统版本扫描、漏洞扫描等，Nmap常用的命令如下。

命令：nmap -sV －v -O 127.0.0.1

其中，sV参数表示扫描端口对应的服务程序版本，v参数为显示冗余信息（扫描细节）,O参数为探测操作系统，将127.0.0.1更改为目标IP地址即可对其进行扫描，若不指定-p参数，则默认扫描1000个常用端口。

（3）Dirsearch

Dirsearch为目录扫描工具，是基于python3的开源工具，用来扫描敏感的页面或备份文件等，其功能丰富，命令行高亮且简洁，渗透测试中较为常用。在渗透测试的信息收集过程中，端口、目录和子域名都是重要的信息点。常用命令如下：

python dirsearch.py -e * -u http://192.168.157.149/

（4）Wireshark

Wireshark是一款开源的网络封包分析软件，指定某个网卡然后对途径该网卡的数据包做截取，然后在软件中回显出该数据包的具体信息，Wireshark使用WinPCAP作为接口，直接与网卡进行数据报文交换。该软件的关键点在于过滤器的使用，正确合理的使用过滤器会提升工作效率。

（5）Metasploit

Metasploit是世界上最常用的渗透测试工具，

Metasploit Framework（MSF）是免费的、开源的，是由Ruby程序语言编写的模块化框架，具有很好的扩展性，便于渗透测试人员开发及定制工具模板。因为其的开源、可用性强的特定，故拥有了大量的安全相关人员使用。目前，Metasploit拥有世界上最大的渗透测试攻击数据库，集成了大量的漏洞验证POC和漏洞利用EXP，深受安全从业人员的推崇，该工具Kali linux上默认带有，命令行输入msfconsole即可进入控制台。

Metasploit由五个基础模块组成：Auxiliaries (辅助模块)、Exploit (漏洞利用模块)、Payload (攻击载荷模块)、Post (后期渗透模块)、Encoders (编码工具模块)。其中，Auxiliaries模块负责资产发现、漏洞扫描、嗅探、指纹识别等辅助测试功能；Exploit模块对信息收集发现、Auxiliaries扫描出的风险点进行漏洞利用，常见的利用方式包括缓冲区溢出、Web应用程序攻击等；Payload模块用于在攻击成功时获取目标系统的控制权限；Post模块用于内网渗透；Encoders模块可以对代码进行混淆，绕过安全防火墙或杀软的检测。

4 渗透测试

如果是真实的渗透测试项目，测试前期一定得拿到客户的书面授权，因为如今国内环境下无授权渗透测试是违法行为，然后根据客户给予的测试资产制定相应的渗透方案，而后对目标资产展开测试工作。

4.1 信息收集

本文渗透目标为一个内网自建系统，故无公网 IP、无备案、无具体公司、无法通过常规搜索引擎、网络空间搜索引擎等来收集信息，所以摒弃某些正常渗透下必要的信息收集，我们只针对收集 IP、C 段、开放端口、网站路径、应用框架等应用层面和网络层面的信息，而不针对业务层面、社会资产暴露面去规整收集相关信息。

可以将收集到的相关联信息做成文档或表格形式，当信息收集结束时就进行信息筛查、漏洞发掘。Nmap 扫描结果如图 2 所示。扫描命令如下：

```
nmap -sV  – v -O -p 1-65535 192.168.157.149
```

收集 C 段的 NMAP 命令推荐如下：

```
nmap -sV -PR -v 192.168.157.149/24
```

其中，PR 参数为 ARP 协议扫描，速度快、精度高且没有任何安全策略会阻止正常的 ARP 请求，192.168.157.149/24 的作用则是扫描 192.168.157.1-192.168.157.255 这个网段的网络设备，即 C 段扫描。

分析上一步的扫描结果，22 端口为 SSH 服务，应用版本 OpenSSH 7.4，搜索可知 OpenSSH <= 7.8 的 OpenSSH 存在一个用户名枚举漏洞，同时 SSH 可被暴力破解；80 端口为 WEB 服务，可深入业务进行安全测试；111 端口为 rpcbind 服务，rpcbind 是 NFS 中用来进行消息通知的服务，其版本为 2-4，疑似存在漏洞；3306 端口为 Mysql 服务，MariaDB 完全兼容 MySQL，包括 API 和命令行，可将其视作为 MySQL，其版本未知，漏洞未知，部署至公网存在爆破风险；最后一点是目标系统为 Linux 服务器，开发版未知，采用虚拟环境 Vmware 部署。

图 2 NMAP 扫描结果

接着，可以使用 Dirsearch 来对网站进行目录扫描，目的找出更多藏在深处的业务面，或者是源码备份、数据备份等敏感文件。结合测试得到的信息，可大致推断出目标服务器的环境部署，即服务器操作系统、中间件、数据库应用、后端语言等。了解这些信息的目的是为了在后续渗透过程中能更好的寻找漏洞利用点。

4.2 漏洞发现

（1）端口开放情况

各个端口开放情况如表1所示。

表 1 端口服务开放

端口	服务	描述
22 端口	SSH服务 (OpenSSH7.4)	存在用户名密码枚举风险，若成功枚举则可能直接获取系统控制权限。
80 端口	Web服务 (nginx1.18.0)	数据库备份文件sql.zip泄露；后台登录地址泄露admin.php
111 端口	Rpcbind服务 (Rpcbind2-4)	经搜索发现rpcbind服务在某些配置下存在漏洞，待验证。
3306 端口	Mysql服务 (MariaDB)	存在被暴力破解的风险，若攻击成功则可能直接操作数据库。

（2）22端口SSH分析

OpenSSH7.4版本存在用户名枚举漏洞，此处不再

深入利用，因为Linux默认root用户为管理员账号，现在针对root账号的弱口令问题进行攻击，若采用弱账号弱口令则易于被暴力破解，反之则SSH服务就难以进一步利用，暴力破解其取决于字典强度，若服务器没做限制规则，理论上时间富裕、字典足够丰富时用户密码定会被枚举成功。

爆破SSH服务的工具很多，这里使用Metasploit集成的辅助模块即可。

（3）111端口Rpcbind服务分析

该服务是一个RPC服务，主要作用是NFS共享时负责通知客户端。利用Nmap可扫描出该服务的一些其他信息，命令如下：

nmap -p 111 --script=rpcinfo 192.168.157.149

该服务可能存在拒绝服务攻击，可用Metasploit尝试发起攻击，不过可能会导致系统崩溃，与我们此处渗透目的不相符，所以不再深入探测该漏洞。

（4）3306端口Mysql服务分析

MySQL直接部署至公网上，存在爆破风险。若攻击失败，MSF暂不支持该服务的MYSQL版本，暂且跳过该点。

（5）80端口主Web服务分析

访问URL下载Dirsearch扫描出的备份文件（http://192.168.157.149/sql.zip），解压即可看到只有一个xunrui.sql文件，分析该文件猜测是往期管理员导出的数据库备份，不能代表实时数据库的存储信息，分析并找到存储用户账户信息的用户表dr_member，其密码字段进行过加密处理。因该网站是由迅睿CMS v4.5.5搭建，故从互联网搜索下载该CMS v4.5.5的源程序代码。

程序源代码下载之后理清程序的文件结构，配置文件，入口文件以及MVC架构的传参规则，必要时可代码审计之后搭建模拟环境进行漏洞确认。代码审计是一个很好的切入点，可分析挖掘出高危0day漏洞来实施渗透攻击，不过这里我们利用另一个切入点，分析密码校验规则，分析找到后台登录处的源代码。可见该代码的加密方法也很简单，前后各一次对原密码进行MD5计算之后两次MD5值中间拼接数据库dr_member表中随机加密码字段（salt），然后对整个拼接后的值进行MD5计算，并将MD5后的值其保存至dr_member表加密密码字段（password）中。该加密从安全性来说，安全等级比单纯MD5高出不少，若单纯采用MD5哈希算法来加密保存用户密码，则可通过自构彩虹表或MD5在线破解平台进行密码碰撞，从而得出原登录密码，而该算法就算得到数据库中的密码字段，也较难构造出原始登录密码。

尽管一般来说，得到数据库中的密码字段也较难构造出用户的原始登录密码，但是如果我们还知道随机加密码salt，这时候就可通过编写代码来实现hash值枚举，这也可以理解为简单的彩虹表模式，不过源代码是经过了2次MD5计算，枚举代码如下所示，

```
import hashlib
def main():
  #随机加密码
  salt=”1f0e3dad99”
  #加密密码
  password=”5e776bd384c332354ff55a74e04803a”

    #加载明文密码字典
  with open(‘dict.txt’,’r’,encoding-’utf-8’) as dictFile：
     for passwd in dictFile.readlines():
        passwd=passwd.strip()
        result_1=hashlib.md5(passwd.encode(encoding
= ’UTF-8’)).hexdigest()
        result_3=result_1+salt+result_1
        result_2=hashlib.md5(result_3.encode(encoding
= ’utf-8’)).hexdigest()
        if(result_2==password):
          print(‘碰撞成功，原始密码为:{},随机码为:{},加密密
码为:{}’.format(passwd,salt,passwd))
          break;
if_name_”_main_”:
   main()
```

其中，salt和password字段来自上述步骤网站备份xunrui.sql文件的admin用户。

理论上字典量足够大就必定能破碰撞出原始密码，执行结果如图3所示，可见成功碰撞出后台管理员admin用户的原始密码为123456。

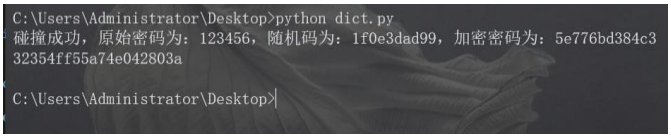

图 3 脚本执行结果

4.3 漏洞利用

接下来是漏洞深度利用。上述枚举出后台管理员admin的密码，故访问Dirsearch扫描出的后台页面，输入账号admin，密码123456即可登录进入后台系统中。

通常情况下，进入渗透目标的管理后台不会立即测试漏洞，而是进行后台业务分析，梳理所有的功能点。渗透测试人员还会将关键功能点和可能存在隐患点表述记录起来，等梳理完成之后再进行安全测试。

分析之后发现有个SQL执行点，因为在上述备份文件中我们发现了一个SQL备份文件，经分析该备份文件为一个月之前的SQL备份，与现在的实时数据存在出入，并且分析备份文件发现一个名为“dr_user”的数据表较为可疑，该表在备份SQL中为空，不存在任何的数据信息[10]。

执行SQL查询命令“SELECT * FROM

`dr_user` ;”。通过数据表的列名可分析出该表存储了一些系统、组件用户的账号密码，如userid为1001的xunrui用户是MySQL的用户名，userid为1002的root用户是系统管理员的账户，passwd_md5字段从字段名可以得出该字段存储用户md5哈希之后的密码值。此时我们就依靠SQL查询得到了root账号以及密码的md5值（7dfefea92a20fc099596fcef67abbcd3），由于md5哈希算法存在脆弱性，互联网上存在不少通过反向查询枚举得出原始字符串的站点，比如cmd5（https://www.cmd5.com/），解密得出root账号的明文密码（qweR1234）。

CMD5解密得出系统管理员root账号的密码qweR1234，尝试ssh登录目标系统，如下图4所示，可见登录成功。

图 4 SSH登录目标服务器

4.4 后渗透

SSH 登录 root 账号之后攻击者就拥有了服务器的管理员控制权限，可以用多种渠道来登录至数据库中，比如开启 root 账号登录 mysql 数据库（该系统不允许 root 用户登录数据库），或者通过查看站点配置文件来找到站点数据库账号以及密码。

后渗透阶段的工作是免杀、持久化、提权、以及内网横向渗透、域环境渗透等[17]。使用 ifconfig 命令可知该服务器存在内网网段 192.168.168.0/24。然后可通过 nmap 或者 arp 等来实现内网机器信息收集，arp 命令可发现内网中存在 192.168.168.133 这台 PC。因本文论述重点不在此处，故不继续描述后渗透阶段的具体攻击实施。

本节为具体的渗透测试阶段，从信息收集开始，收集开放端口、对应服务、中间件、后端语言、CMS、敏感目录与敏感文件，然后综合性对收集的信息进行分析，得到可用信息之后对其进行风险点利用，记录渗透测试过程，为下一后的密码学应用规范部分做材料基础。

5 隐患点分析与密码优化调整

若为真实的渗透测试项目，测试前期一定得拿到客户的书面授权，因为如今国内环境下无授权渗透测试是违法行为，然后根据客户给予的测试资产制定相应的渗透方案，而后对目标资产展开测试工作。

5.1 隐患点分析

22端口开启的SSH服务、建议更改默认端口，禁止root账号远程登录，使用密码强口令，或者使用密钥登录。

80端口开放的web服务存在备份SQL文件泄露漏洞，导致了数据库信息被攻击者利用，破译出明文密码后就以此账号密码登录系统后台，系统后台泄露也是一个较大的安全隐患点，当系统后台被攻击者以各种方式拿下后就可能会对整个站点产生不可挽回的结果。我们需将备份文件删除，将后台页面迁移或实施安全策略使用IP白名单访问。

111端口Rpcbind服务只服务于NFS，若无使用必要则不应暴露至公网上面，建议防火墙配置防护策略，不对外开放该端口服务，甚至可以停止该服务运行。

3306端口为数据库Mysql服务，正常若外部无业务调用该数据库，应在防火墙限制其端口服务不对外网开放，这样能在一定程度上减少资产暴露面。

每个系统对用户账号密码等敏感信息的存储方式是不一样的，多数系统会将用户的密码hash计算后保存，常见的使用MD5算法，本处漏洞点就是在后台实时查询出系统管理员的root账号以及MD5后的密码值，破译MD5后得到原始密码，通过SSH登录即获取目标服务器权限。

对于端口服务而言，因遵从最小化原则，关闭所有不必要的服务，多一个服务就多一份危险，非必要不往公网开放服务，如MySQL，Redis等，同时SSH建议应用密钥登录，免除被爆破风险[11][12]。

5.2 国密应用实施

（1）应用国密 SSL/TLS 协议

渗透测试过程我们发现目标站点是基于 HTTP 通信的，HTTP 通信的所有信息都以明文传输，就存在窃听风险、篡改风险、冒充风险，攻击者可以获取、修改通信内容，设置冒充他人身份参与通信，这样的通信方式是存在巨大风险的，所以我们需要在站点应用 TLS 协议。TLS（安全传输层），在 TCP/IP 模型中处于 4.5 层，在传输层与应用层之间，基于 TCP 协议，服务于应用层，其前身是 SSL（安全套接字层），该协议存在的目的是使网络通信更加安全，它将应用层报文（如 http,ftp,smtp 等）进行加密后再交由 TCP 进行传输，保证了网络通信的保密性、完整性以及完成通信双方的身份认证。

TLS 安全通信的本质是通信对端采用安全的密码协商协议，协商过程中涉及到签名、验签、密钥交换等多种加密算法，每种加密算法都有可能因为某个潜在的后门漏洞而使整个系统陷入网络风险漩涡。所

以本文对于测试环境的安全优化首先选用国密版的 SSL/TLS 协议来实现安全通信，部署 HTTPS 环境。

部署具体过程此处不再论述，可以从以下两个方面来观测国密 SSL/TLS 协议应用前后站点的差别：

其一可以直观的在浏览器地址栏看出应用前后的不同点，未配置 SSL/TLS 协议地址栏标注 HTTP，走的是服务器端的 80 端口。而配置国密 SSL/TLS 协议后地址栏显示 HTTPS，走的是服务器端的 443 端口。应用 TLS 之后 SSL 证书是使用国密站点默认证书，并非自己配置的 SSL 证书。

其二通过 Wireshark 抓取数据包来观测应用国密 TLS 协议前后的比对效果。可通过 info 信息来定位登录处的关键流量包，点击该流量包即可看到具体的传输信息。当我们向服务端交互的信息时，就能以明文显示在流量包中。当攻击者采用嗅探或其他方式来攻击时即可窃取、修改传递的参数值，这将产生巨大威胁。通过在目标服务器应用国密版 TLS 协议之后的 Wireshark 抓包结果，可以看出 Wireshark 中流量包全部加密处理，不仅传输内容无从得之，甚至连 info 字段也不显露出具体的请求 URL，这让攻击者无从下手去嗅探、修改用户所传递的参数值。

（2）SM3 替换 MD5

我们在测试中，发现 MD5 算法共出现了两次。第一次是 SQL 备份文件中泄露了后台管理员 admin 用户的经过多次 MD5 原密码后的哈希值，因为 MD5 的不可逆性与该系统密码保存时应用了特有的算法逻辑，故测试过程只能通过编写脚本程序来实现特定算法结构下的 MD5 值枚举以得出原始密码值。从测试结果看到的该程序注册处的关键代码，发现密码字段的保存是左右各一段原密码 MD5 值，中间以随机数拼接（该随机数同样保存在用户表里），然后再将拼接后的值再进行一次 MD5 计算。从安全的角度出发，该密码的保存形式较为安全且效率较高。为此，此处不建议应用 SM3 算法来替换 MD5，因为 SM3 效率上会低于 MD5，而该功能点是常用功能点，替换之后将影响整个系统的优化，得不偿失。

第二次出现 MD5 算法的地方是在登录后台之后执行 SQL 语句找出的‘dr_user’表中。该表一开始在备份文件中没数据，在后台中执行 SQL 后就正在文件中发现有多个用户（数据库用户、系统用户）的账号密码信息，且密码是 MD5 保存的。可以在该处将使用 MD5 算法替换成 SM3 算法来保存用户密码，并且将列名 passwd_md5 修改为 passwd。这样做的好处是，即使攻击者得到哈希值，也一时难以猜测是何种算法进行加密处理。使用 SM3 算法加密的关键代码如下：

```
$sm3=new\oneSm\Sm3();

$user[‘user_id’]=$user[‘user_id’];
$user[‘user_name’]=$user[‘user_name’]?$user_name’]: ’ ’;
$user[‘passwd’]=$user[‘passwd’] ?$ sm3->sign($user[‘passwd’]: ’ ’;
$user[‘describe’]=$user[‘describe’] ?$user[‘describe’]: ’ ’;

$rt=$this->table(‘user’)->insert($user);
if(!$rt[‘cide’]) {
   return dr_return_data(code:0, &rt[‘msg’]);
}
```

6 结束语

本文利用开源 CMS 搭建一个模拟的信息系统，并在数据库中存入一些自我构造的虚拟数据，用于渗透阶段的分析。再结合网上较完善的渗透测试标准，制定渗透测试文档，按照文档规范来完成渗透测试，最后分析是否符合信息系统密码应用基本要求，验证密码应用在信息系统设备和计算安全、应用和数据安全中的应用是否合规、正确和有效。

参 考 文 献

[1] 庞智.Web 系统安全渗透测试方案的分析与设计[D].北京邮电大学,2011.

[2] Filiol Eric; Mercaldo Francesco; Santone Antonella. A Method for Automatic Penetration Testing and Mitigation: A Red Hat Approach[J]. ENSIBS, Cyberscurity Dept., Vannes, France & HSE Higher School of Economics, Moscow, Russia,2021.

[3] 蒋文正.面向信息系统密码应用安全评估的渗透测试技术研究[D].南宁：南宁学院，2021.

[4] Saundatikar Raj; Lakshmi J.V.N. Web Penetrator-Web App Penetration Testing Tool[J]. Department of MCA Jain University Bangalore India,2021.

[5] 赵丽娟.应用程序渗透测试方法研究[D].长沙：中南大学，2014.

[6] 吴文刚,张鑫.渗透测试在信息系统安全等级测评中的应用[J].电脑与电信,2018(Z1):67-69.

[7] 郭川.基于 Kali Linux 的渗透测试平台的研究[D]. 呼和浩特：内蒙古科技大学，2019.

[8] 毛忠亮.基于图的渗透测试方法的研究[D].吉林：长春工业大学,2016.

[9] 郭方舟.基于ＭＶＣ框架渗透测试系统的设计与实现[D].北京:北京邮电大学，2019.

[10] 蒲福连.基于协同自主的网络渗透测试技术研究[D].成都：电子科技大学,2014.

[11] 武杰.智能化网络渗透测试系统的设计与研究[D].吉林：长春工业大学,2018.

[12] 熊羿.自动化渗透测试平台的设计与实现[D]. 北京：北京邮电大学，2019.