湘潭大学

计算机学院·网络空间安全学院

《网络攻击与防御》

实验报告

计算机科学与技术学院

计算机系网络教研室制

|  |  |
| --- | --- |
| 课程名称： | 网络安全技术 |
| 实验名称： | openssl协议heartbleed漏洞分析 |
| 指导教师： | 唐欢容 |
| 学生姓名： | 宁凯 |
| 学 号： | 201705551125 |
| 实验日期： | 2020.6.24 |
| 实验成绩： |  |

一、实验目的

1. 了解Openssl“心血”安全漏洞形成的原因
2. 掌握基本的漏洞利用及使用方法
3. 能够给出修复方案

二、实验环境



Openssl服务器：centos6.0，IP地址：10.1.1.136

测试者：win2003，IP地址随机分配。

三、实验内容与实验要求

1. 打开浏览器输入Openssl服务器的ip，随意输入一个用户名和密码。
2. 使用openssl漏洞测试工具，就服务器进行测试。
3. 修复方案。

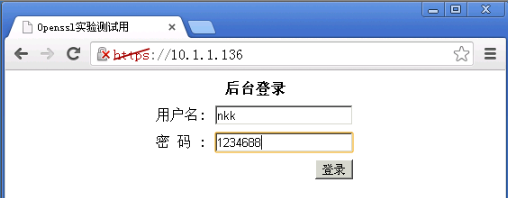
四、实验过程与分析

实验步骤一

打开浏览器输入Openssl服务器的ip，随意输入一个用户名和密码；

任务描述：在浏览器里面打开https://10.1.1.136

在页面随便输入用户名和密码。





实验步骤二

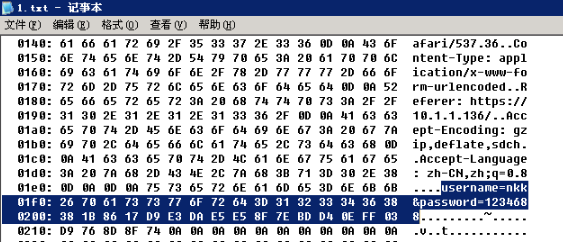
使用openssl漏洞测试工具，就服务器进行测试

任务描述：测试工具（ssltest.py）已经下载好了，在C盘的根目录。



对测试工具获取到的数据进行分析

任务描述：对上面得到的数据，进行分析。



打开步骤二重定向得到的文件，发现里面直接可以看到刚刚我们输入的用户名和密码。

实验步骤三

修复方案

任务描述：给出加固方案（分apache下的和Nginx下的）

Apache下的修复方案：

升级OpenSSL至1.0.1g版本。

升级完成后，重启相关服务，不清楚就重启系统。

Nginx下的修复方案：

升级OpenSSL至1.0.1g版本。

使用“nginx -V”会出现如下的提示：

nginx version: nginx/1.5.6

built by gcc 4.4.7 20120313 (Red Hat 4.4.7-3) (GCC)

TLS SNI support enabled

configure arguments: --prefix=/opt/nginx --with-http\_stub\_status\_module --with-http\_ssl\_module --with-pcre=/opt/pcre-8.33 --with-openssl=/opt/openssl-1.0.1e --with-zli b=/opt/zlib-1.2.8 --add-module=/opt/nginx\_ajp\_module-master

关键的一行“--with-openssl=/opt/openssl-1.0.1e”，虽然使用“openssl version”查看到的是1.0.1g版本。但实际上nginx使用的还是1.0.1e版本。重新编译安装下就可以了，在configure时是最重要的，一定要注入“--with-openssl=”这个选项，只要指定那个1.0.1g的路径就可以了。

五、实验结果总结

通过这次实验，我了解Openssl“心血”安全漏洞形成的原因：OpenSSL在实现TLS和DTLS的心跳处理逻辑时，存在编码缺陷。OpenSSL的心跳处理逻辑没有检测心跳包中的长度字段是否和后续的数据字段相符合，攻击者可以利用这点，构造异常的数据包，来获取心跳数据所在的内存区域的后续数据。这些数据中可能包含了证书私钥、用户名、用户密码、用户邮箱等敏感信息。该漏洞允许攻击者，从内存中读取多达64KB的数据。同时，我也掌握了基本的漏洞利用及使用方法，例如打开浏览器输入Openssl服务器的ip，随意输入一个用户名和密码，然后使用openssl漏洞测试工具，就服务器进行测试。通过学习，我也能够给出修复方案。这次实验让我收获满满。