**西安邮电大学**

**网络空间安全学院**

**实验报告**

**（2020/ 2021学年第2学期）**

实验名称： 网络空间安全基础实践

学生姓名： 王璐 \_\_\_\_\_\_\_

专 业： 网安2101班 \_\_

学 号： 26213035（35） \_\_\_\_\_

指导教师： 冯景瑜

**西安邮电大学网络空间安全学院网络空间安全基础实践课程**

**考核表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **学生姓名** | **王璐** | **班级/学号** | | **26213035** | |
| **承担任务实验室（单位）** | **网络空间安全实验室** | **所在部门** | | **网络空间安全系** | |
| **实施时间** | **2022年 4月 24日 — 2021年5月 8日** | | | | |
| **实验内容** | **（一）经典网络空间攻防案例中的法律分析**  **（二）漏洞扫描器的使用**  **（三）网络嗅探熟悉** | | | | |
| **指导教师（师傅）姓名** | **冯景瑜** | **职务或职称** | | **副教授** | |
| **指导教师（师傅）**  **对学生的评价** | **评价点** | **评价内容** | | | **评价得分** |
| **平时成绩**  **（20分）** | **投入学习时间、课堂纪律及学习态度、遵守实验室的规章制度等情况** | | |  |
| **实验能力**  **（30分）** | **法律意识能力、漏洞扫描能力、嗅探分析能力** | | |  |
| **实验验收**  **（20分）** | **实验要求达成情况**  **实验演示与答辩情况** | | |  |
| **实验报告**  **（30分）** | **语言及文字表达能力**  **实验报告工作量及撰写规范性** | | |  |
| **总评成绩** |  | | **五级制** |  | |
| **指导教师（师傅）评语** | **指导教师（师傅）签字**  **2022年 4月 30 日** | | | | |

### 实验一：经典网络空间攻防案例中的法律分析

**1.实验目的和要求**

**1.1实验目的**

熟悉《网络安全法》，梳理清楚经典网络空间攻防案例中包含的攻防知识，给出相关法律分析。

**1.2实验要求：**

1.2.1认真学习《网络安全法》；

1.2.2整理和分析经典攻防案例，用来激发学习兴趣和梳理攻防知识；

1.2.3结合《网络安全法》，针对某一个具体的攻防案例，梳理包含的攻防知识，分析其中违反的法律条例，深思《网络安全法》的重要性，并撰写实验报告，；

1.2.4引导学生树立正确的价值观，以国家和民族利益为根本，珍惜和平，

在实验报告中阐述如何坚定不移地做一名合格的网络空间安全专业技术人员。

**2实验原理**

《网络安全法》

网上查找资料等。

**3实验内容及步骤**

**3.1选取一个经典的网络空间攻防案例；**

政治因素一直是黑客发动网络攻击的一个重要动机。2015年12月，著名黑客组织匿名者(Anonymous)发布视频谴责土耳其支持ISIS，并向土耳其发动了史上最大规模的DDoS攻击。

2015年12月14日开始，大规模网络攻击导致土耳其银行、政府网站离线，土耳其三家知名银行Ziraat银行，Isbank和Garanti确认受到攻击，攻击流量峰值带宽高达40Gbps。

一名土耳其电信代理商发言人Onur Oz在接受路透社采访时称：“这次网络攻击事件是很严重的，但是这次目标不是土耳其电信，相反，土耳其的银行和公共机构网络受到了严重的攻击。现在大多数的土耳其机构使用土耳其电信作为网络服务商，目前我们在积极应对这次网络攻击并做好防御工作。”

土耳其大多数的银行和政府网站在华为Anti-DDoS系统防御之下，大流量攻击导致防御系统性能过载。华为工程师现场紧急扩容板卡，研发远程7\*24小时值守，虽然黑客不断变更攻击手法，但所有攻击均被成功阻断，网站访问正常。

这次DDoS攻击事件中，Anonymous发动的是混合型的攻击，包含SYN flood、UDP flood、HTTP flood等多种类型的攻击。

**3.2梳理案例中使用的攻击手段，分析该如何防御该攻击手段；**

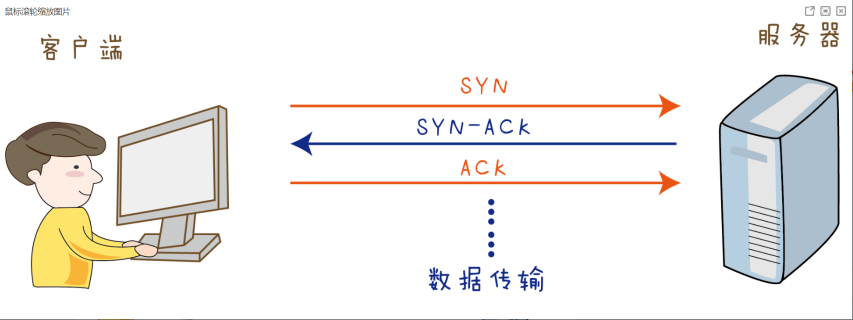
SYN flood

一提起SYN flood，大家都很熟悉吧。SYN flood是互联网上最经典的DDoS攻击方式之一，也是最原始的DDoS攻击，最早出现于1999年左右。在网络发展初期，由于系统的限制以及硬件资源性能的低下，SYN flood的出现对网络安全界是一大冲击。它与当时的单包攻击的不同在于，你很难通过单个报文的特征或者简单的统计限流防御住它，因为它“太真实”、“太常用”。 SYN flood能够一直占据江湖大佬地位这么多年依旧风生水起也是有原因的。SYN flood具有强大的变异能力，在攻击发展潮流中一直没有被湮没，这完全是他自身的优秀基因所决定的：

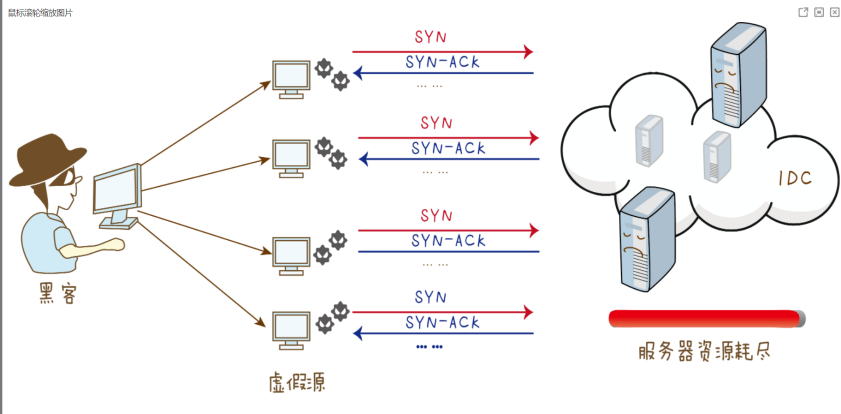
1、 攻击成本低，攻击过程简单。

2、 难防御，每个报文看起来都是一个正常的报文。

下面我们就来看看SYN flood是如何达到攻击的效果。SYN flood是基于TCP协议产生的，所以我们先回顾一下TCP的三次握手。



再来看SYN flood，SYN flood其实就是利用三次握手机制，制造多个半连接，消耗服务器的连接数。



黑客伪造源IP地址向服务器发送大量的SYN报文，请求建立三次握手。由于发送源IP是伪造的，所以服务器回应了SYN-ACK报文后，源IP并不会再继续回应ACK报文进行确认。这样服务器就会维持一个庞大的等待列表，不停地重试发送SYN-ACK报文，同时占用着大量的资源无法释放。这就导致，被攻击的服务器被恶意半连接占满，不再接受新的SYN请求，而合法用户无法完成三次握手建立TCP连接。

这就好比你去超市买东西，来了一大帮人，他们也不买东西，却把所有收银台都占满了，既不结账，也不走，这就是半连接。结果导致所有收银台都无法为正常客户结账，超市业务瘫痪，这就是资源耗尽。



对于SYN flood这种看似正常，没有明显攻击特征的报文，就不能再通过特征识别或者指纹学习的方式进行过滤。SYN flood是基于TCP协议的，TCP协议是面向连接的，我们就可以从SYN报文建立连接的“行为”入手，判定是不是真实源发出的请求。

对于这种面向连接的DDoS攻击，最有效的防御方式就是源认证。源认证有三个层面：

1、 TCP/IP源认证

2、 应用层源认证

3、 用户源认证

**3.3依据《网络安全法》，分析案例中违反的法律条例；**

第二十五条　网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第二十六条　开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

**3.4深思《网络安全法》的重要性，思考今后学习和掌握网络空间攻防技术后，如何做好遵纪守法。**

3.4.1不随意实施各种攻击，不在不经过允许的情况下窃取他人信息，对他人电脑进行攻击。

3.4.2不恶意破坏任何系统，恶意破坏他人的软件将导致法律刑责！

3.4.3不修改任何系统档，如果你是为了进入系统而修改它，请在达到目的后改回原状。

3.4.4不要轻易将你要入侵的网站告诉你不信任的朋友。

3.4.5不要在网络论坛上谈论黑客的任何事情。

3.4.6在传递文章的时候不要使用真名。

3.4.7正在入侵的时候，不要随意离开你的电脑。

3.4.8不要侵入或破坏政府机关的主机。

3.4.9不在电话中谈论黑客的任何事情。

3.4.10将你的笔记放在安全的地方。

3.4.11想要成为黑客就要真正地掌握黑客技术，读遍所有有关系统安全或漏洞的文件！

3.4.12已侵入电脑中的账号不得清除或修改。

3.4.13不得修改系统档案，如果为了隐藏自己的侵入而作的修改则不在此限，但仍须维持原来系统的安全性，不得因得到系统的控制权而将门户大开！

3.4.14不将你已破解的账号分享与你的朋友。

**4实验结果分析**

这次实验主要针对著名黑客组织匿名者(Anonymous)向土耳其发动了史上最大规模的DDoS攻击进行分析，了解到了此次攻击所带来的危害和这种攻击的主要解决方法。

**5实验总结及心得体会**

通过本次实验，了解到了各种网络攻击的手段和避免方法。学习到了《网络安全法》，了解了各种网络攻防案例。熟悉了网络攻击的途径，理解了网络防守的方法。

**实验二：漏洞扫描器的使用**

**1实验目的和要求**

**1.1实验目的：**

具备漏洞扫描的基本知识，总结一种常见漏洞扫描器使用过程

中遇到的问题和解决方法，分析漏洞扫描结果，得出自己的分析报告。（8学时）

**1.2基本要求：**

1.2.1选择一款常用的漏洞扫描器，比如Nessus；

1.2.2描述漏洞扫描器安装过程，给出截图；

1.2.3选择某一个网站进行扫描，描述扫描过程，给出扫描结果，如发现漏洞，应及时上报；

1.2.4撰写实验报告，并从“双刃剑”角度分析漏洞扫描器的两种不同价值；

**2实验原理**

**2.1实验准备**

2.1.1具备漏洞扫描的基本知识。

2.1.2到 Nessus 官方网站（http://www.nessus.org）下载 Nessus 的服务端和客户端，下载插件库。

2.1.3阅读 Nessus 官方安装文档和使用文档。

**2.2实验背景**

网络漏洞扫描基础知识

2.2.1安装 Nessus 的服务端、插件库和客户端；

2.2.2配置 Nessus 服务端，分配具体用户；

2.2.3用 Nessus 客户端对某个网站或者局域网主机进行扫描；

2.2.4给出扫描结果报告，获取系统的有用信息，最好能发现网络系统的安全漏洞。

**3实验内容及步骤**

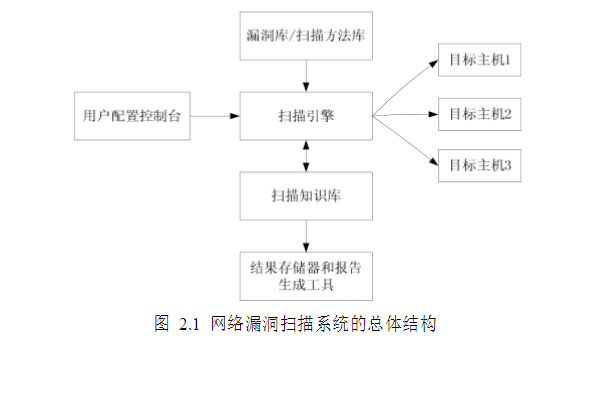
3.1安装 Nessus 的服务端、插件库和客户端；

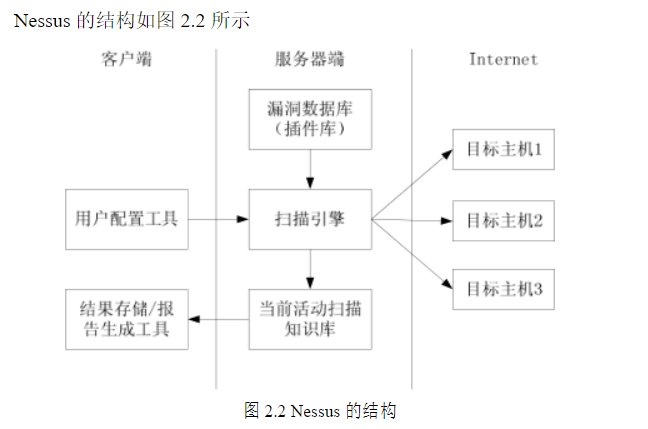
3.2配置 Nessus 服务端，分配具体用户；

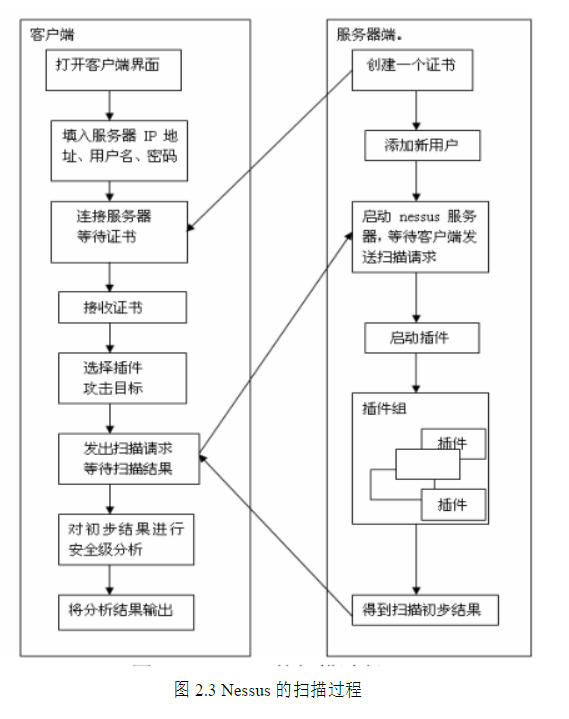
3.3用 Nessus 客户端对某个网站或者局域网主机进行扫描；

3.4给出扫描结果报告，获取系统的有用信息，最好能发现网络系统的安全漏洞。

使用Nessus扫描指定Windows系统漏洞。使用Windows 7系统作为目标主机。具体扫描步骤如下所示。





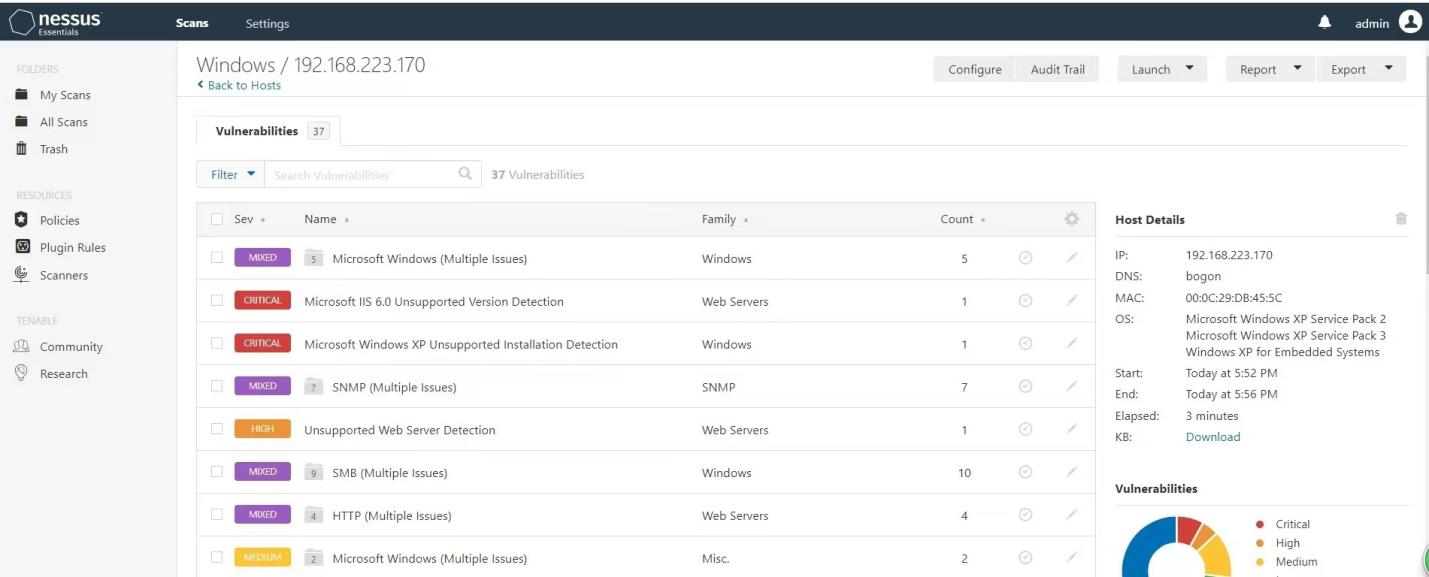


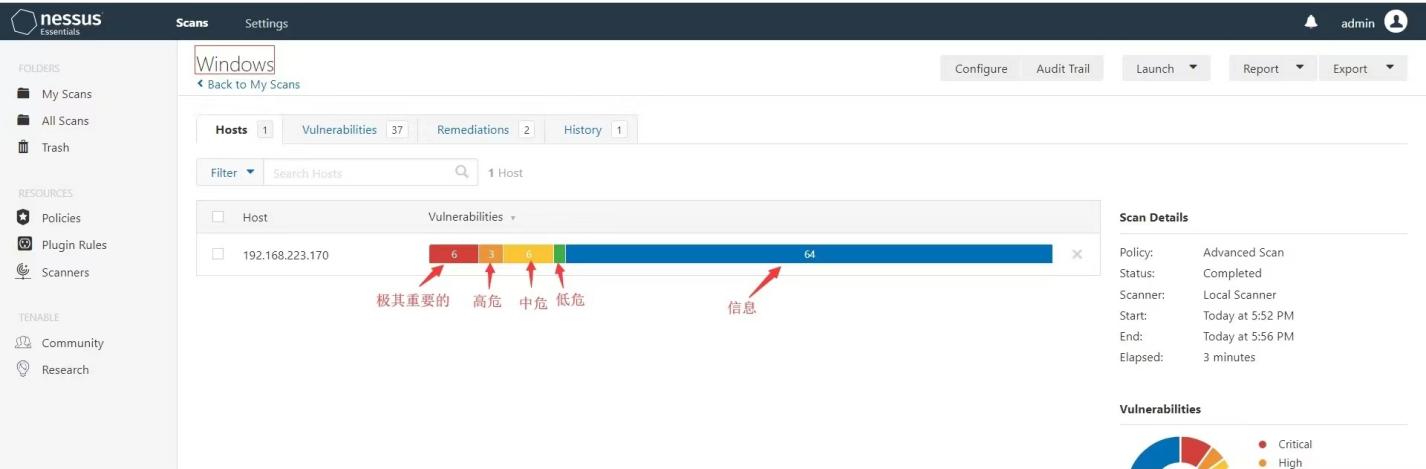
3.4.1新建名为Windows Vulnerability Scan策略。

3.4.2添加所需的插件程序

从该界面可以看到主机的漏洞情况

**4实验结果分析**

****

****

总结：Nessus软件能很好的将电脑中的漏洞扫描出来，并能展现各类型漏洞的占比和漏洞所在位置。

**5实验总结及心得体会**

Nessues的安装确实比较麻烦，但它的效果也非常明显。通过本次实验，我找到了电脑中的漏洞，明白了漏洞的各种分类，了解了以后应该怎样通过Nessus来查找电脑中的漏洞。