**本学期学习目标**

1. **掌握网络安全基础**：操作系统、计算机网络、常见攻击手法。
2. **能熟练使用基础工具**：Kali Linux、Wireshark、Burp Suite、Nmap 等。
3. **能动手做一些小型实战**：例如搭建靶机、做 Web 渗透练习、尝试CTF新手题。
4. **形成学习成果**：写笔记/博客、做小实验，建立可展示的“学习档案”。

**时间分配（学期内）**

假设每周能抽出 **15~20 小时**（每天 2-3 小时，周末多一些），可以这样安排：

**第1-2个月（9月下旬 ~ 11月中旬） —— 打基础**

* **Linux & 基础环境**
  + 搭建虚拟机（VirtualBox/VMware），安装 Kali Linux + Windows 环境。
  + 熟练 Linux 常用命令（文件、用户权限、进程、网络配置）。
* **计算机网络**
  + 重点：TCP/IP、三次握手/四次挥手、ARP、DNS、HTTP/HTTPS。
  + 工具：Wireshark 抓包，理解数据包。
* **编程**
  + Python：文件操作、网络编程（socket）、正则表达式。
  + Bash 脚本：写一些自动化脚本（端口扫描、日志处理）。
* **安全入门**
  + 学习常见 Web 漏洞原理（SQL 注入、XSS、CSRF）。
  + 在 DVWA、bWAPP 这类靶机上练习。

阶段目标：能用 Linux + Python 完成一些小实验，比如写个简单端口扫描脚本；能在靶机里复现最基本的 SQL 注入。

**第3个月（11月下旬 ~ 12月） —— 工具与渗透**

* **渗透测试工具**
  + **Nmap**：扫描主机和端口。
  + **Burp Suite**：拦截 HTTP 请求，修改参数。
  + **Metasploit**：简单的漏洞利用。
* **漏洞利用**
  + 在本地靶机（如 DVWA、Metasploitable2、Vulhub）尝试实际渗透。
  + 了解提权的概念（Windows/Linux 提权思路）。
* **CTF 入门**
  + 开始做一些 **CTF Web/crypto/misc** 的简单题。
  + 平台推荐：CTFHub、BUUCTF。

阶段目标：能独立做完一个 Web 靶场（如 DVWA），写出一篇自己的“渗透测试练习报告”。

**第4个月（1月前，期末） —— 整理与成果**

* **知识整理**
  + 把学过的漏洞、工具、实验都整理成笔记或博客（建议用 Markdown + GitHub Pages）。
* **综合实验**
  + 模拟一个小项目：比如对某个靶机做完整的信息收集 → 扫描 → 漏洞利用