网络空间安全导论实践

王东滨

dbwang@bupt.edu.cn

- **课程目的：**

旨在结合网络空间安全导论课程知识的学习，学习利用相关工具及资源，开展网络空间安全导论实践活动，培养创新创业意识与思维、对网络空间安全技术的兴趣。通过自主设计网络空间安全实验场景、实验实践活动，激发学生的创新意识，培养初步动手实践能力。

- **课程类型：**

创新实践活动

不同于理论课、实验课，需要同学们课后独立自主实践。

- **课程内容：**

网络安全政策及产业发展

创新创业概论

网络安全竞赛

网络安全实践作品

- **课程考核**

  平时成绩（40%）+期末作品成绩（60%）

- **网络安全实践作品**

1）采用推荐命题与开放式自主命题相结合的方式，完成网络安全实践作品。（可以选择推荐命题，也可以自命题，不影响评判结果）

2）需要自己搭建环境实现

3）不能在互联网上（包括校园网、公网等）实施攻击。

- **选取某一漏洞，了解其漏洞利用原理，搭建和实现漏洞利用场景。**

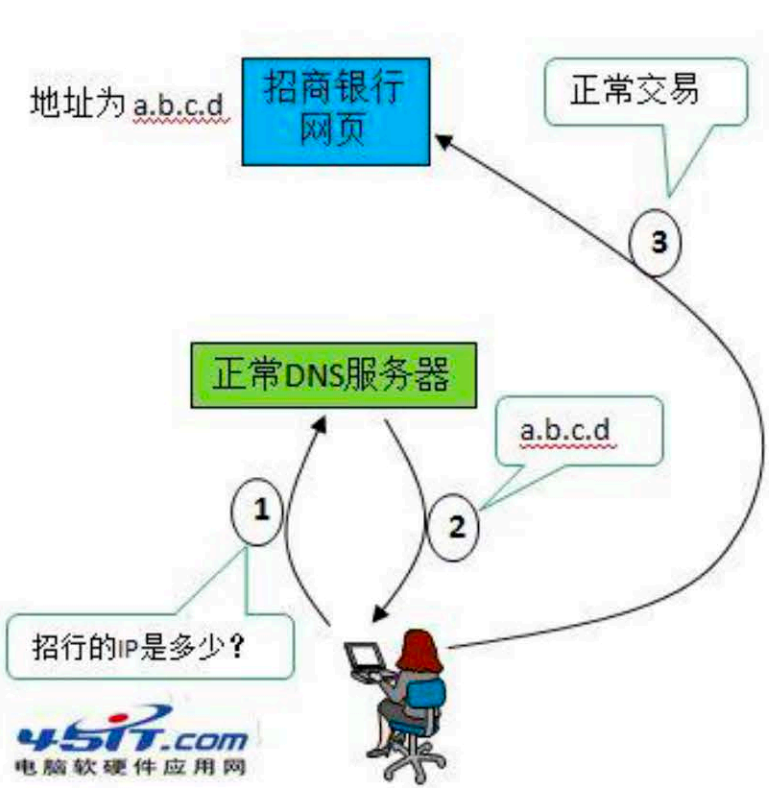
例如：

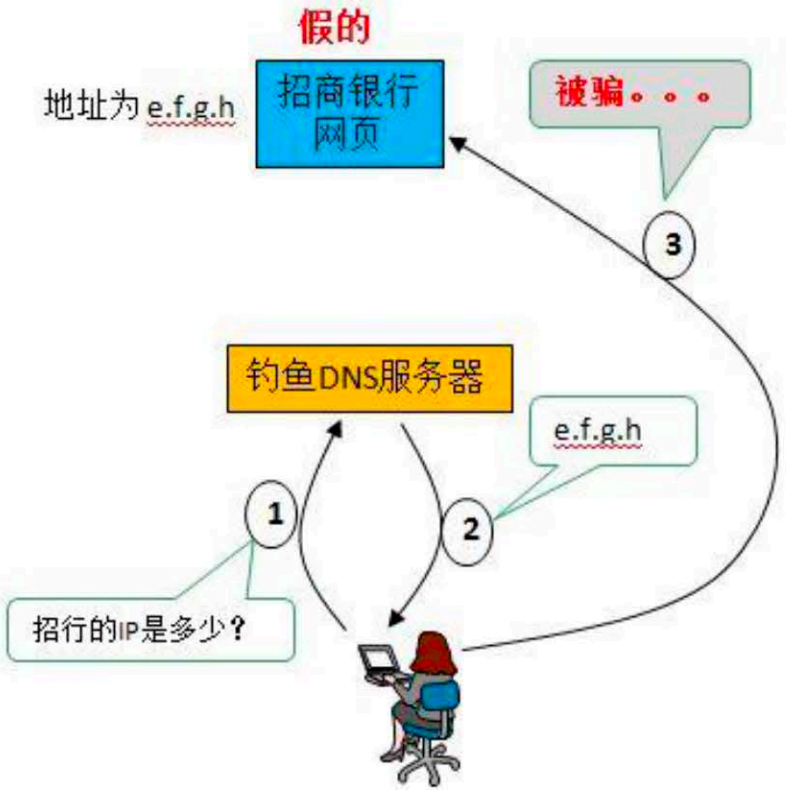
命令执行漏，通过URL发起请求，在Web服务器端执行未授权的命令，获取系统信息，篡改系统配置，控制整个系统，使系统瘫痪等。

--通过目录遍历漏洞，访问系统文件夹，执行指定的系统命令；

--攻击者提交特殊的字符或者命令，Web程序没有进行检测或者绕过Web应用程序过滤，把用户提交的请求作为指令进行解析，导致执行任意命令。

- 了解DNS解析相关原理，搭建环境实现一次DNS劫持攻击。如可搭建DNS解析环境，实现虚假DNS解析功能或中间人攻击功能。





- 了解数据库，SQL语言相关应用场景，并完成一次SQL注入攻击。

- **了解Vmware搭建虚拟机的实现原理与使用方式，搭建kali linux并尝试使用其中1-2种工具。**

Kali Linux预装了许多渗透测试软件，包括nmap 、Wireshark 、John the Ripper，以及Aircrack-ng

nmap:网络连接端扫描,确定哪些服务运行

wireshark： 网络数据报文分析

John the Ripper ： 弱口令检测

Aircrack-ng： 802.11 标准的无线网络分析

- **了解并安装Metasploit，学习其使用流程，利用其中的漏洞完成一次远程攻击。**

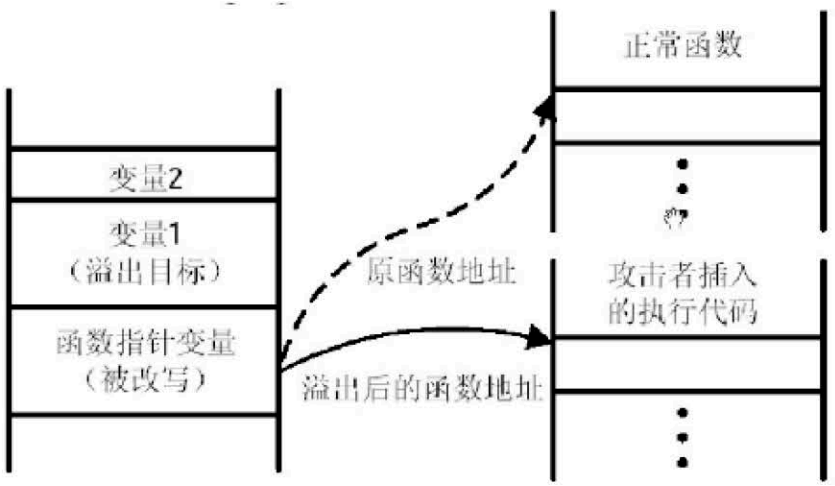
Metasploit是一款开源安全漏洞检测工具，附带数百个已知的软件漏洞,可以帮助验证漏洞的缓解措施。包括智能开发，代码审计，Web应用程序扫描，社会工程。

https://www.metasploit.com/

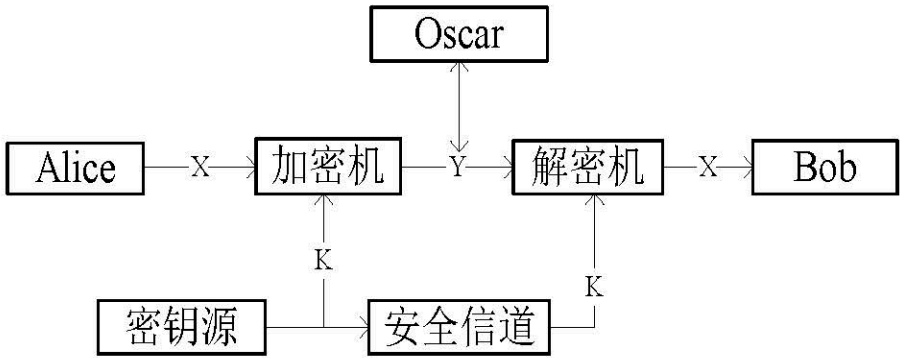
- **了解二进制漏洞以及操作系统的防御手段，尝试进行一次缓冲区溢出攻击。**

缓冲区溢出（buffer overflow），是针对程序设计缺陷，向程序输入缓冲区写入使之溢出的内容（通常是超过缓冲区能保存的最大数据量的数据），从而破坏程序运行，获取程序乃至系统的控制权。

```
void function(char *str)
{
    char buffer[16];
    strcpy(buffer,str);
}
```



- 了解密码学相关概念和原理，选择一种加密方式，以及一段需要加密的信息，完成加密与解密。



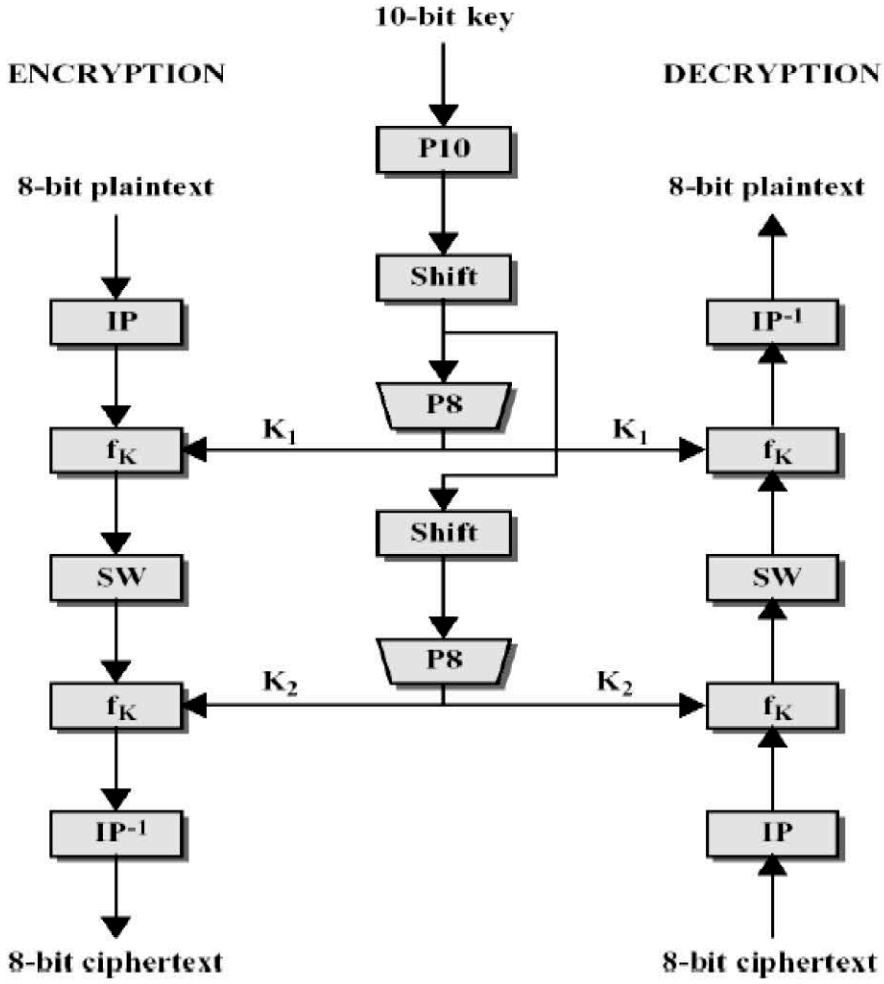


Figure 3.1 Simplified DES Scheme

- **了解信息安全黑产相关概念与手段，实现一次密码撞库或暴力破解攻击。**

Morris和 Thompson在1979年分析了3289个真实的用户口令，发现其中有86%的数据落入普通字典，33%的数据能在5分钟内搜索出来。后续的研究表明，会选择常用单词作为口令，做一些简单的变换，以满足站点口令设置策略的需求。 如“password123”可以满足 “字母 +数字 ”的策略需求 。

表 5-2 各数据集中最流行的前 10 个口令分析

口令排名	网易	天涯论坛	机锋网	12306	Linkedin	Yahoo	Fling	Neopets
1	123456	12345678	123456	123456	123456	123456	12345678	123456
2	12345678	123456789	12345678	123456789	123456789	password	123456	password
3	111111	11111111	password	111111	password	12345678	iloveyou	qwerty
4	password	woaini1314	123123	password	iloveyou	abc123	love123	asd123

- **自主命题：自主选取与网络空间安全相关的命题，设计并实现某一安全功能的工具或系统。**

入侵检测、病毒检测、恶意代码分析、木马分析、密码分析、安全协议分析等。

1. 提交材料

1）按照给定报告模板提交报告一份，文档命名方式为：

学号-姓名-题目名称.docx

2）其它材料

- 如为软件设计，需提供：程序源代码（请规范注释）、运行程序、演示视频（程序执行过程）；
- 如为场景类设计，需提供：演示视频（内容包含原理说明、环境拓扑、场景还原展示、实现效果等）

2. 时间要求

请于2024年5月21日前提交。

3. 其他要求

做好5分钟的PPT。

➢ 评判依据

评判结果主要依据规范性（15%）、工作量（45%）、设计难度（40%）等方面。

规范性主要依据文档命名规范、文档版式（排版、布局、字体等）、认真态度等；

工作量主要依据实现的功能复杂度、代码量或场景复杂度；

设计难度主要依据新颖性、创新性、实现难度等方面。

谢谢!

Q&A