1. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的arp\_spoof.py文件，填写该文件当中空缺的Flag1字符串，将该字符串作为Flag值（形式：Flag1字符串）提交；（arp\_spoof.py脚本功能见该任务第6题）

**time**

1. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的arp\_spoof.py文件，填写该文件当中空缺的Flag2字符串，将该字符串作为Flag值（形式：Flag2字符串）提交；（arp\_spoof.py脚本功能见该任务第6题）
2. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的arp\_spoof.py文件，填写该文件当中空缺的Flag3字符串，将该字符串作为Flag值（形式：Flag3字符串）提交；（arp\_spoof.py脚本功能见该任务第6题）

**dst**

1. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的arp\_spoof.py文件，填写该文件当中空缺的Flag4字符串，将该字符串作为Flag值（形式：Flag4字符串）提交；（arp\_spoof.py脚本功能见该任务第6题）

**type.0x0806**

1. 进入虚拟机操作系统：Ubuntu Linux 32bit中的/root目录，完善该目录下的arp\_spoof.py文件，填写该文件当中空缺的Flag5字符串，将该字符串作为Flag值（形式：Flag5字符串）提交；（arp\_spoof.py脚本功能见该任务第6题）
2. 在虚拟机操作系统：Ubuntu Linux 32bit下执行arp\_spoof.py文件，对靶机服务器进行ARP Spoofing渗透测试，使该渗透测试能够使靶机服务器场景ARP缓存中记录中的攻击机MAC地址对应IP地址192.168.1.1，将此时靶机服务器场景ARP缓存记录中的攻击机MAC地址对应IP地址192.168.1.1条目内容作为Flag值（形式：该条目内容的第1个字符串+第2个字符串+第3个字符串）提交；

**?+(192.168.1.1)+at**