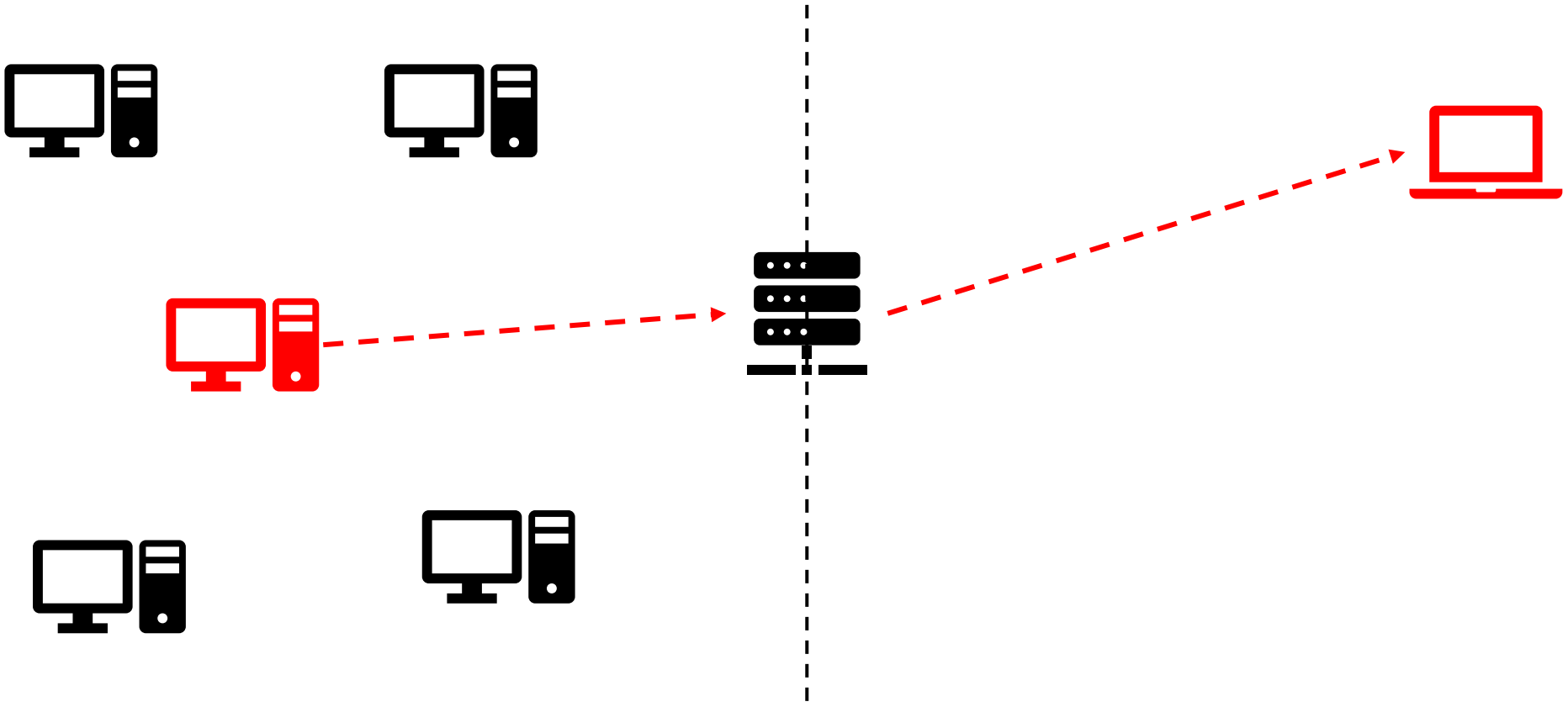
《计算机网络》期末考试



ICMP隐蔽通信--原理分析与技术实现

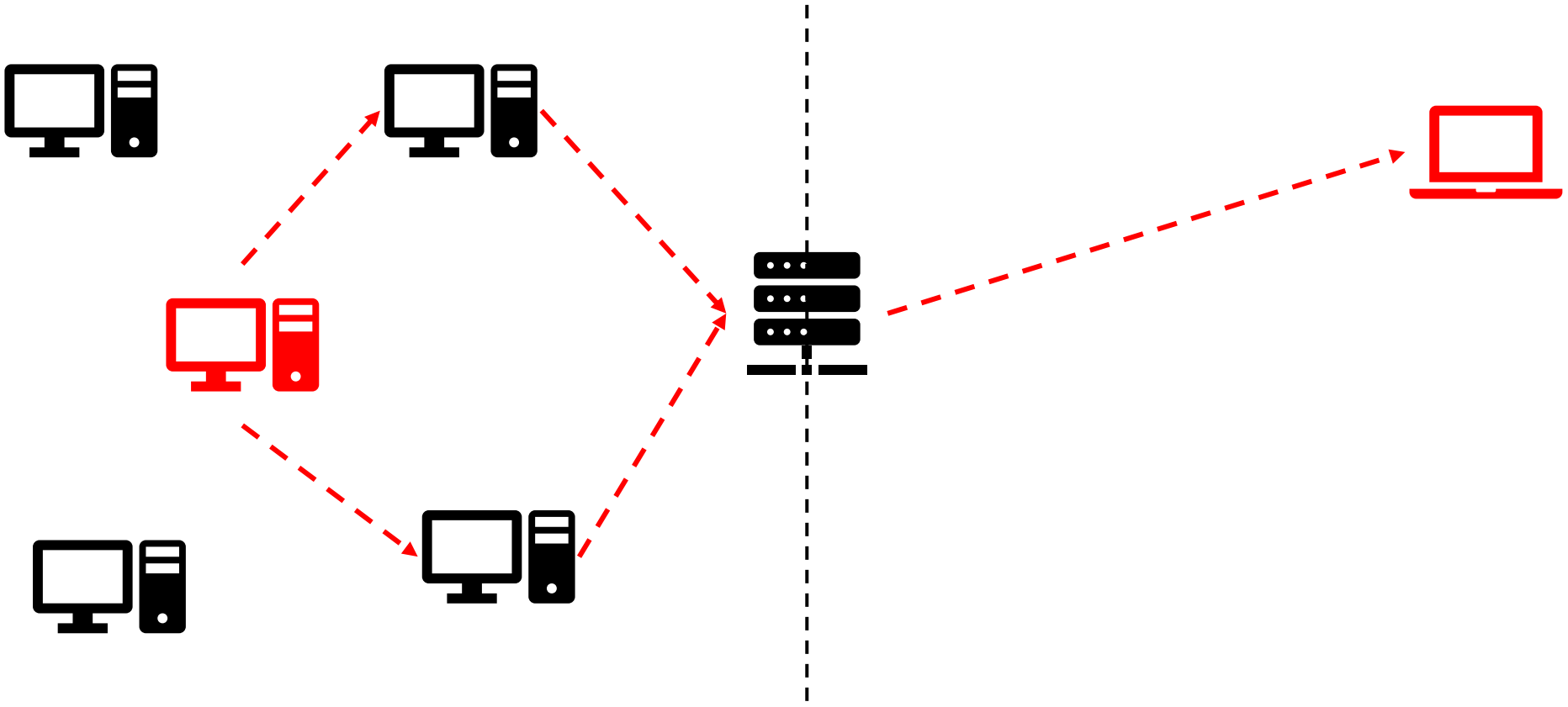
ICMP隐蔽通信--原理分析与技术实现

STEP1：在合法授权下，你已经渗透进入了某目标内网，并成功控制了其中某台计算机（图中虚线左侧红色台式机）。现在你需要将计算机上的关键文件，偷偷的传出内网，发送给在外网焦急等待的接收者（图中虚线右侧红色笔记本）。因为内网网关设备（图中虚线上设备）对TCP和UDP报文都有非常严格的检测，你需要使用ICMP协议来建立隐蔽信道传输数据。伪装成PING外网，实际上传输文件。请用SM4算法加密混淆你的payload，密钥可以硬编码在程序内。

请实现上述隐蔽通信的发送和接收程序，自己动手构造环境进行实验（可以租用为云、阿里云、腾讯云等，选择免费的学生试用或者用按使用时间计费的方式，考试全程的云端租用成本应不会超过30元），验证程序确实达到了预期的效果。撰写报告，简述这套系统的工作原理，分析其被检测发现的风险，以及可能的改进手段。

源代码我们会使用一些系统进行查重，发现抄袭的，抄和被抄的本门课程总分都计0分

请注意，如果从网络上抄代码，很可能多人无意间抄到同一份代码，可能全军覆没都是0分



ICMP隐蔽通信--原理分析与技术实现

ICMP隐蔽通信--原理分析与技术实现

STEP2:由于网关机器加强了安全检测，长期的从一台机器PING外网目标很容易被发现。因此你采用了ICMP反射的方法，通过伪造源地址，向内网不同的机器发射ICMP request报文，让他们向外网目标地址发射ICMP reply。

请分析：

1. ICMP reply复制ICMP request中payload的可行性。引用RFC标准，并做小实验验证（无需外网接收）
2. ICMP reply跨越网关的可行性，在报告中回答在什么情况的网络设置下，reply包可以到达外网目标接收机，什么样的情况则不能
3. 分析使用ICMP构建隐蔽信道的其他方法

报告和源代码请提交到每次交作业的email地址

源代码我们会使用一些系统进行查重，发现抄袭的，抄和被抄的本门课程总分都计0分

请注意，如果从网络上抄代码，很可能多人无意间抄到同一份代码，可能全军覆没都是0分

这是，期待已久的，24小时的愉悦

生旦净末丑，代码和报告，唱出从日出到日落的欢歌

要习惯快节奏，工作了赶项目进度都是如此

备足快乐水，是赶在deadline之前交上报告的奥义