- 1、概述
- 2、环境准备
  - 2.1 网卡配置
  - 2.2 INetSim安装
  - 2.3 apateDNS
  - 2.4 测试
- 3 小结

1、概述

在进行恶意文件分析时，很多病毒文件都会进行联网检测，若发现无法访问互联网，恶意文件将处于静默模式，无法看到它的动态行为，盲目将恶意文件在互联网主机行进行运行会有一定风险，所以尝试搭建虚拟网络环境，诱骗恶意文件运行。

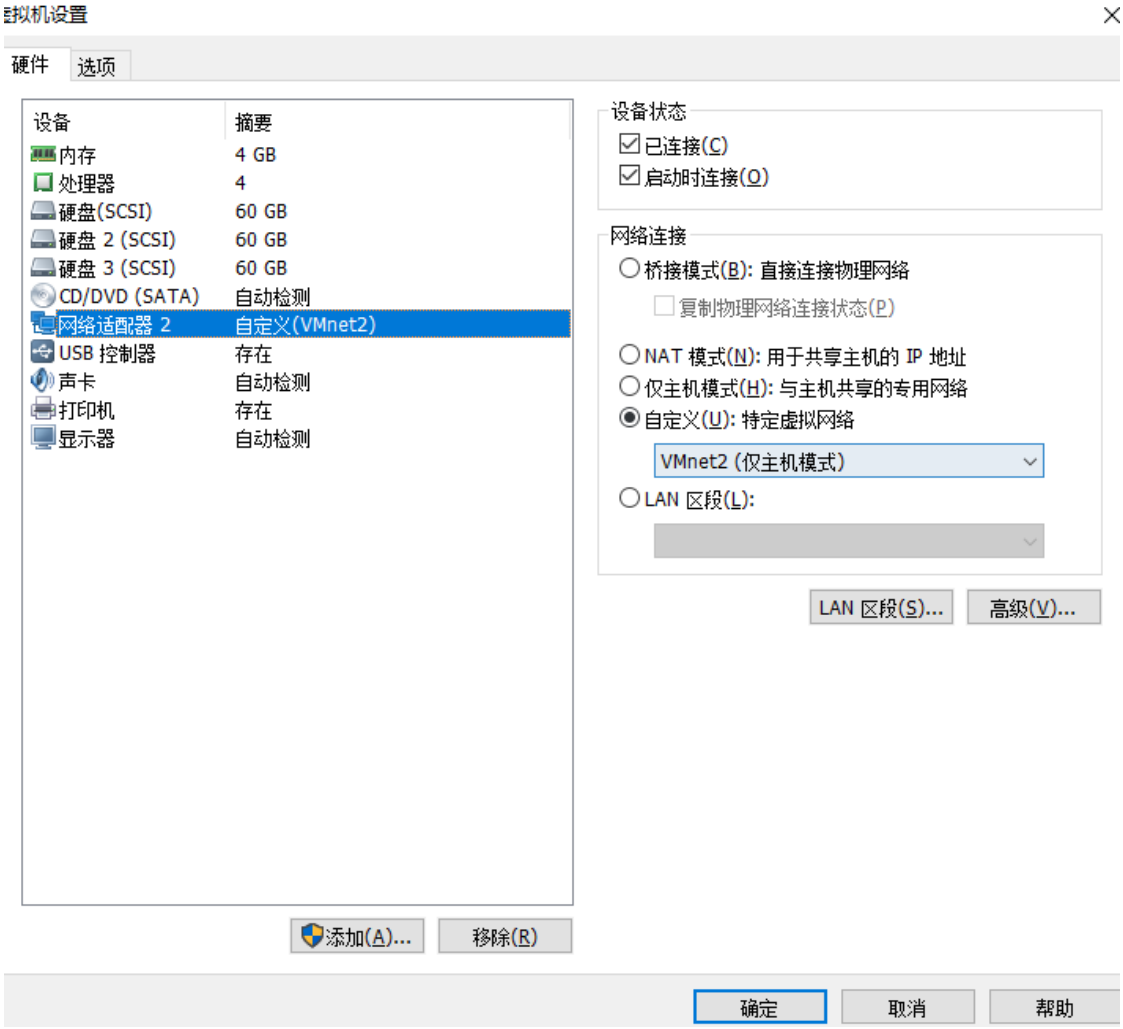
2、环境准备

配置需求：主机直接可以进行互联，但是不能访问互联网

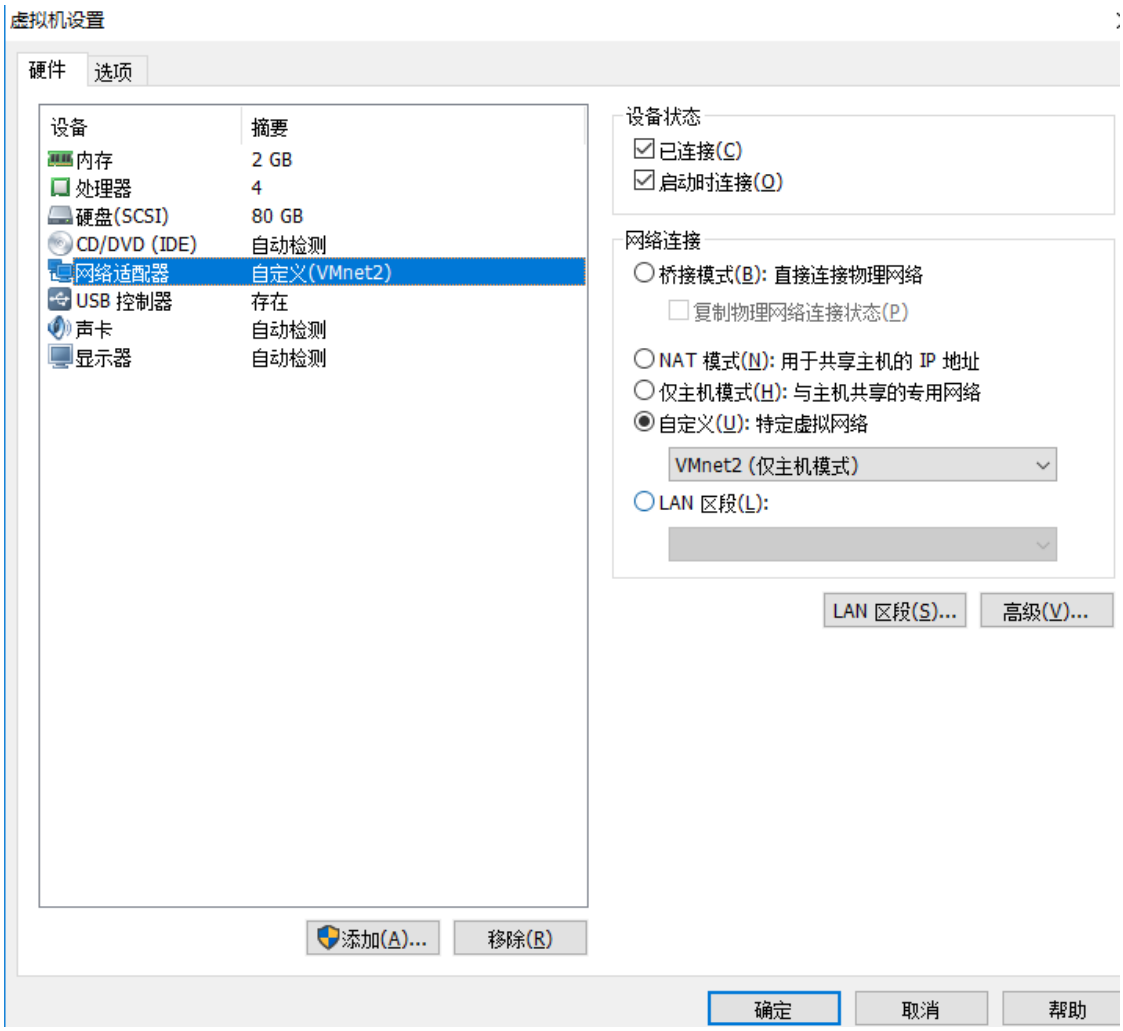
运行恶意代码进行分析的虚拟机：win7
启动服务器的虚拟机：Kali
工具使用：
Apatedns：ApateDNS是一个用于控制DNS响应的工具，主要用在本地系统上的DNS服务器。 ApateDNS可以欺骗由恶意软件生成的DNS请求至UDP端口53上的指定IP地址。
Inetsim：INetSim是一个基于Linux的工具，主要用于恶意软件分析，它可以模拟最常见的互联网服务，如http、https、DNS、FTP以及其他的。在Windows机器上执行动态恶意软件分析时，你可以使用和恶意软件分析机器在同一网络中的虚拟机来运行INetSim。 INetSim能够伪造恶意软件可能使用的常见的互联网服务，并回答相应的请求。

2.1 网卡配置

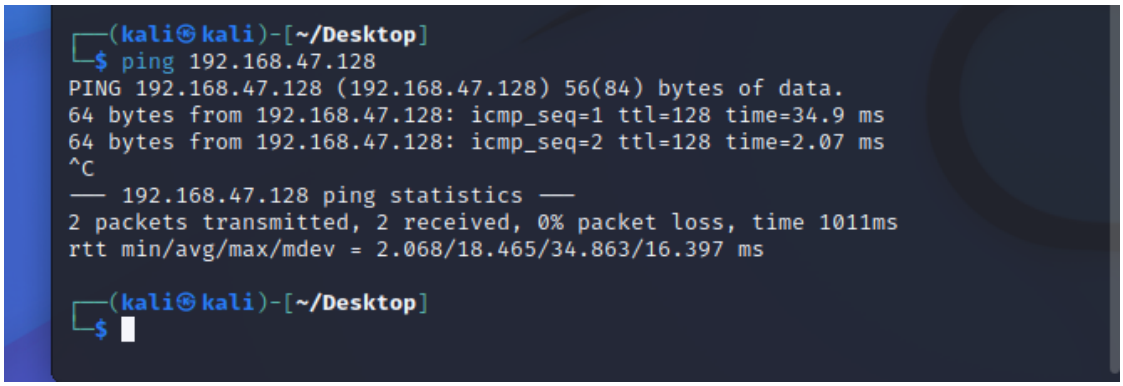
win7：ip地址 192.168。47.128



kali： ip：192.168.47.129



测试发现网络可通：

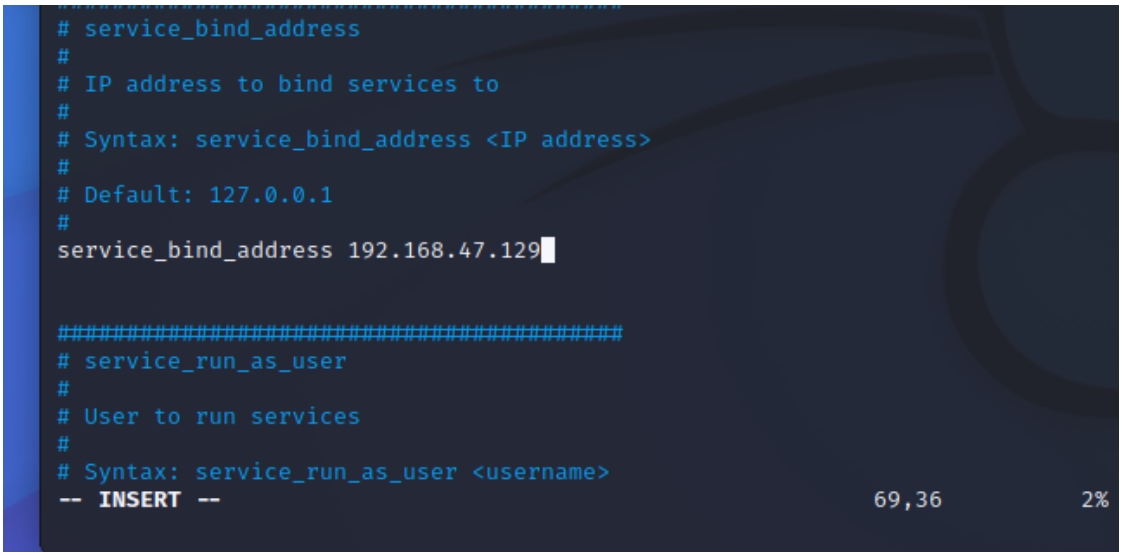


2.2 INetSim安装

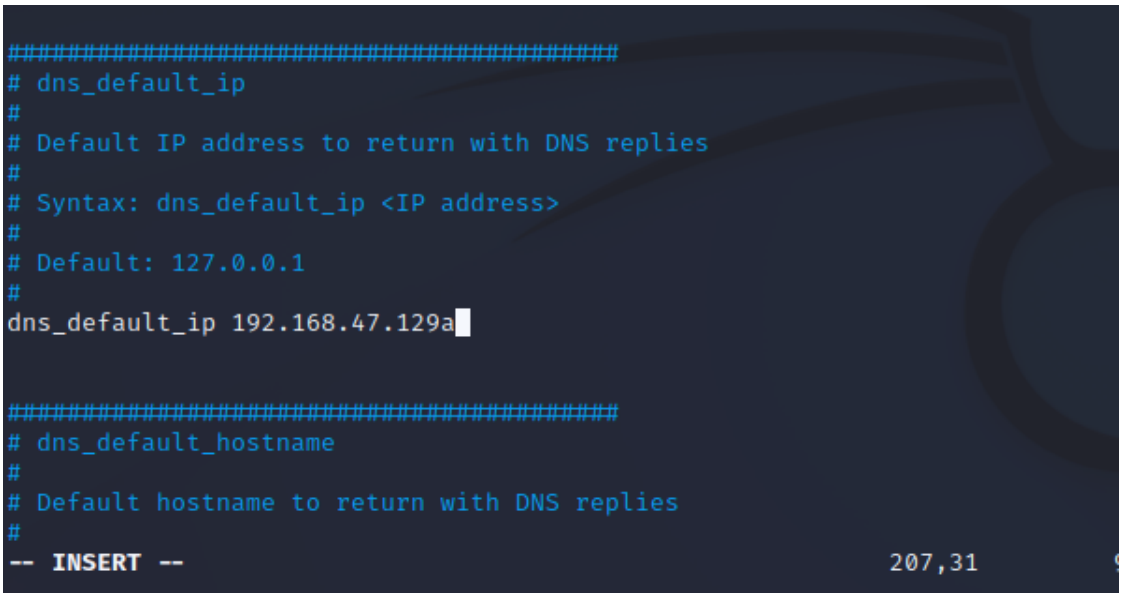
kali：自带有INetSim，无需安装。环境变量中已经加入其路径，直接输入INetSim（root权限）就可运行

只需要进入到/etc/inetsim文件夹修改inetsim.conf文件，修改内容如下：

绑定本机IP：service_bind_address： 192.168.47.129（Kali虚拟机IP）

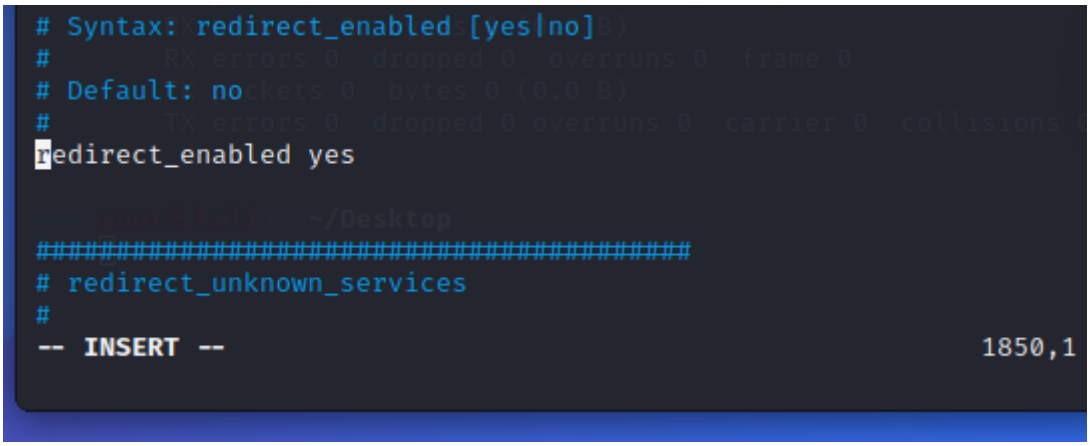


DNS解析IP，将流量重定向到本机：dns_default_ip： 192.168.47.129

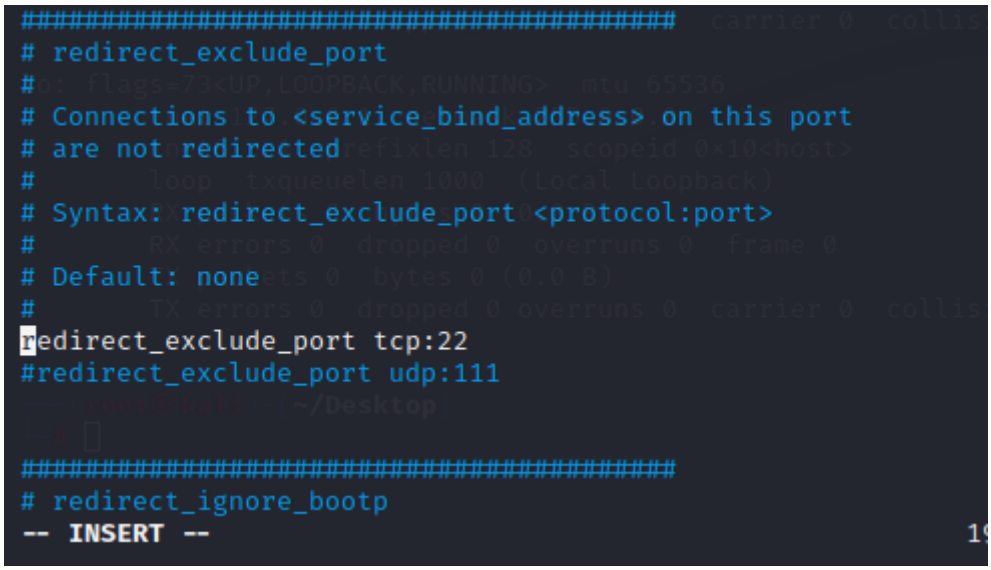


重定向开启

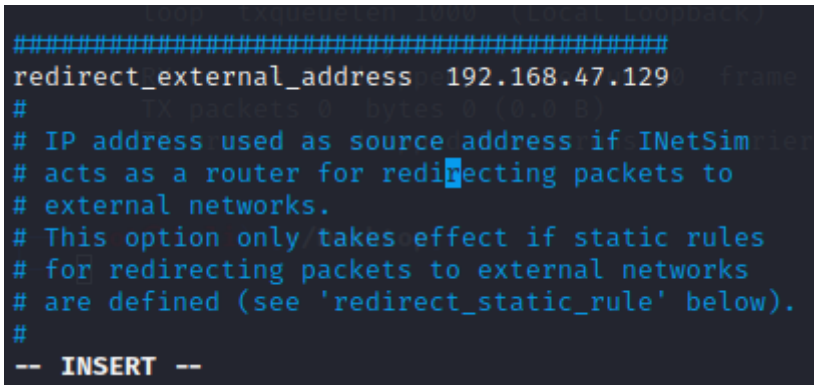
redirect_enabled yes



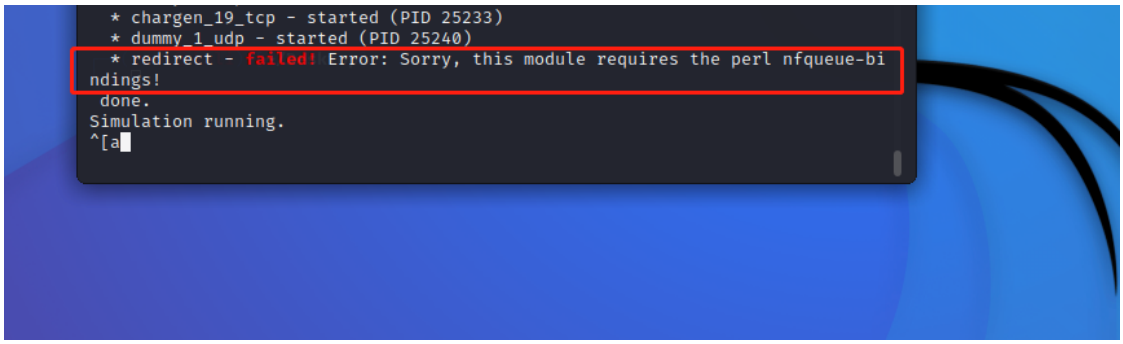
连接绑定ip的tcp端口ect_exclude_port tcp:22



重定向外部地址（非注释信息，有些机器更改配置时自动更改，最好确认一下）
redirect_external_address 192.168.47.129

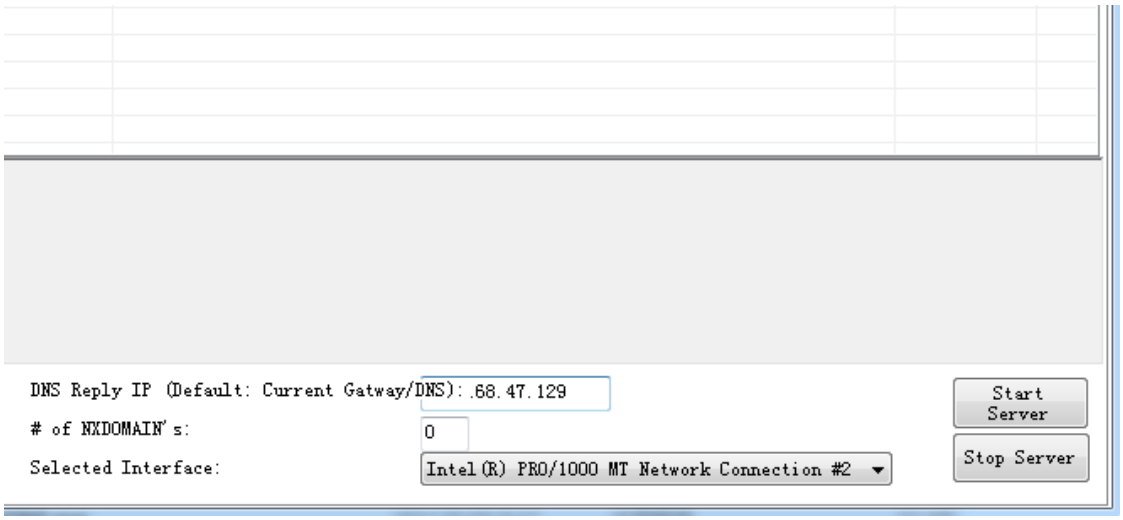


输入 inetsim启动服务，图中的报错是缺少组件，但是不影响实验

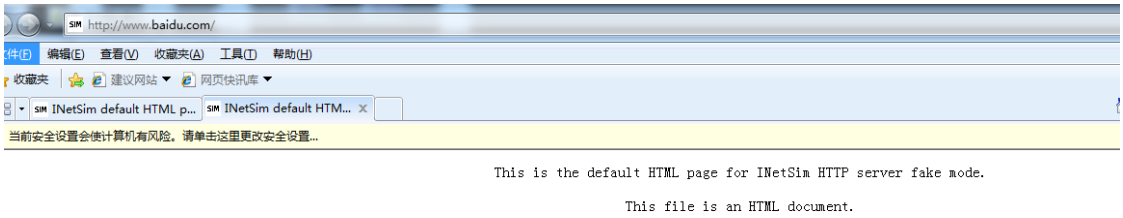


2.3 apateDNS

配置apatedns：
DNS Reply IP处添加需要将请求包欺骗至的IP地址，此处为kali的ip地址，如下图

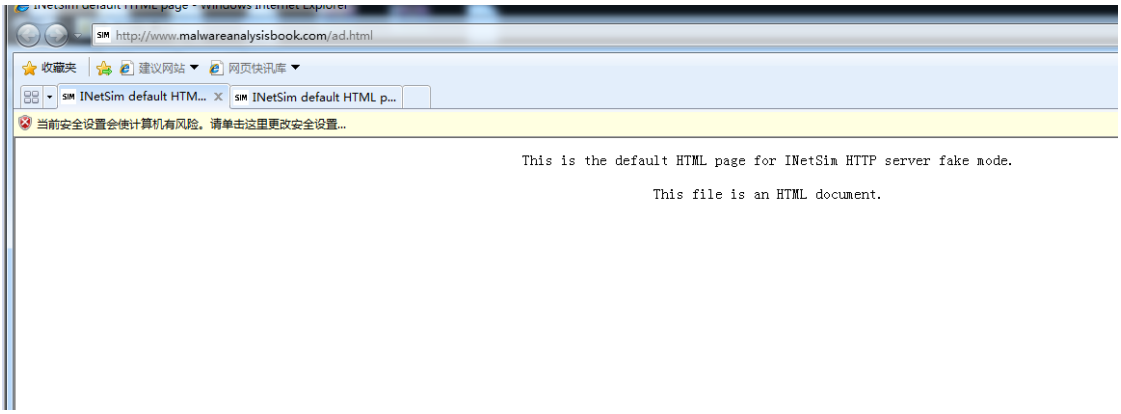


此时浏览器访问网站打开页面如下：

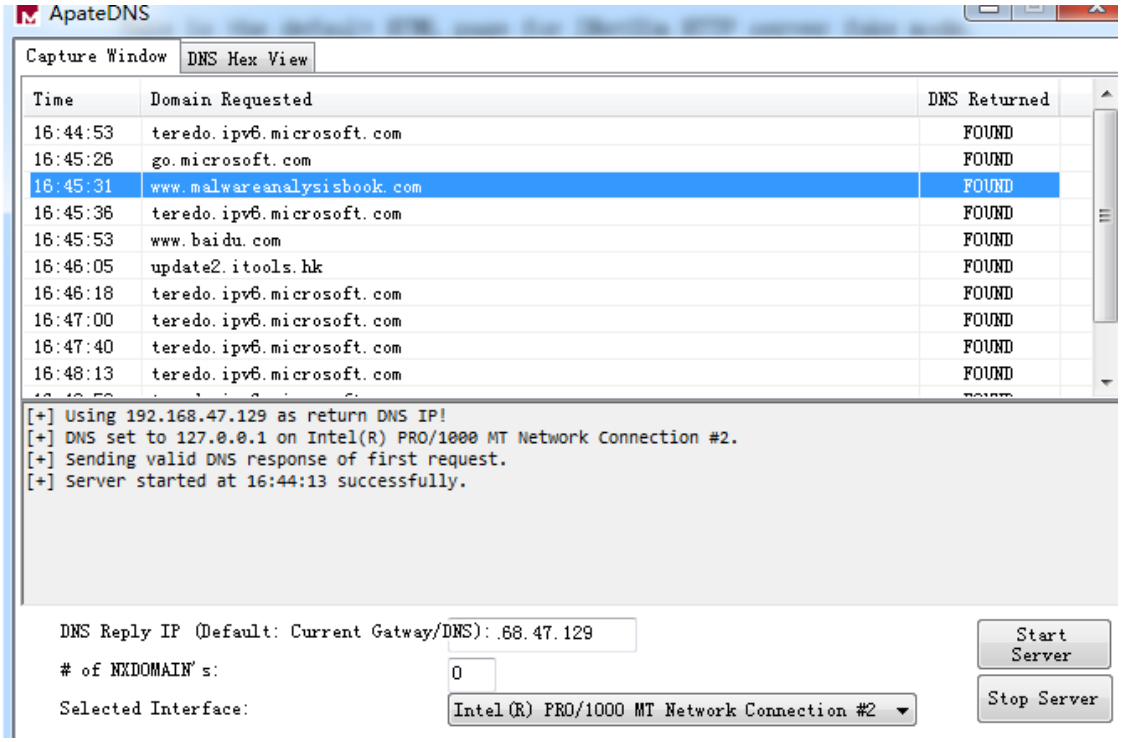


2.4 测试

打开恶意程序：Lab01-03.exe，浏览器打开如下页面



从apateDNS软件的capture windows可看到相关数据



可看到恶意软件请求了如下url：www.·malwareanalysisbook·com

3 小结

虚拟网络环境的搭建对于应急来说还是很常见的，尤其是分析一些恶意文件时，可在不访问互联网的情况下，分析木马的一些动态行为。