实验名称：检测dns污染、劫持

1. 环境拓扑

**GW:172.28.102.126**

KALI

虚拟机

**172.28.102.39**

桥接

普通用户

真实机

**172.28.102.7**

Internet

环境说明：

受害者电脑：普通用户，IP地址为172.28.102.7

攻击者电脑：KALI虚拟机，IP地址为172.28.102.39

二、实验步骤

1. DNS欺骗

|  |
| --- |
| 修改ettercap DNS文件。    vi /etc/ettercap/etter.dns，在文件中加入一行内容，表示所有的域名请求都解析为172.28.102.39地址。  \* A 172.28.102.39    :wq保存一下。 |

1. 制作欺骗性网页

|  |
| --- |
| 1. 设置欺骗性网页   echo welcome to mywebsite >/var/www/html/index.html     1. 重启apache服务器   /etc/init.d/apache2 start     1. 验证欺骗性网页 |

1. 启用kali中的ethercap程序

|  |
| --- |
| 在终端输入ettercap -G来进入ettercap的图形界面  root@kali-test:/etc/init.d# ettercap -G    点击sniff->Unfied sniffing来选择网卡，点确定 |

1. 扫描网络主机

|  |
| --- |
| 1. 选择Hosts>scan for hosts，扫描网络主机   IMG_259   1. 查看网络主机列表      1. 选择欺骗目标，选择172.28.102.7 add to target 1 172.28.102.126 add to target 2，在targets->current targets中查看结果如下图      1. 启用ARP欺骗   点击mitm>arp poisoning，勾选sniffer remote connections后确定     1. 启用DNS\_spoof插件   plugins>mangge the plugins，双击dns\_spoof插件 |

1. 开始DNS欺骗

|  |
| --- |
| 点击strat>start sniffing开始DNS欺骗 |

1. 在真实机上验证结果

|  |
| --- |
| 查看arp缓存记录，我们发现真实机和KALI机器的物理地址一致，实现了ARP的欺骗    IE浏览器验证  我们访问www.hao123.com，发现网页被篡改了 |

1. 实验完成，停止欺骗

|  |
| --- |
| 再次验证相关信息，一切正常 |