任务二 DHCP欺骗劫持与防御策略

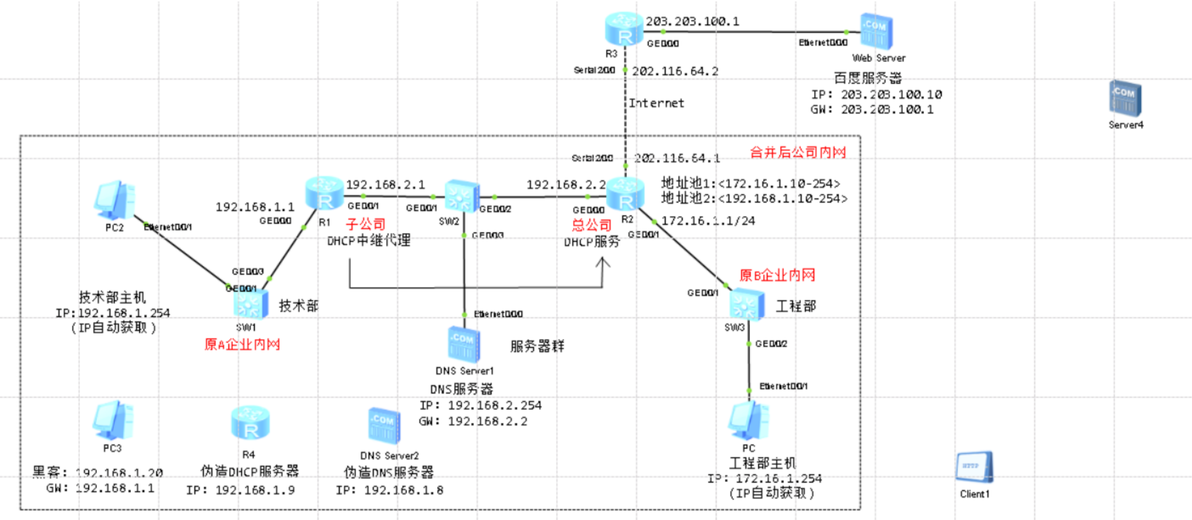
一、任务目的

掌握DHCP的欺骗原理与DHCP监听配置。

二、任务设备、设施

win10、华为eNSP、vmvare、win7、typora

三、任务拓扑结构图



四、基本配置

1.接口IP与默认路由配置

R1

```
<Huawei>sys
[Huawei]sys
[Huawei]sysname R1
[R1]undo info-center enable
[R1]int g0/0/0
[R1-GigabitEthernet0/0/0]ip add 192.168.1.1 24
[R1-GigabitEthernet0/0/0]q
[R1]int g0/0/1
[R1-GigabitEthernet0/0/1]ip add 192.168.2.1 24
[R1-GigabitEthernet0/0/1]q
[R1]rip 1
[R1-rip-1]version 2
[R1-rip-1]netwo
[R1-rip-1]network 192.168.1.0
[R1-rip-1]network 192.168.2.0
[R1-rip-1]q
[R1]ip route-static 0.0.0.0 0.0.0.0 192.168.2.2

[R1]dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[R1]int g0/0/0
```

```
[R1-GigabitEthernet0/0/0]dhcp select relay
[R1-GigabitEthernet0/0/0]dhcp relay server-ip 192.168.2.2
[R1-GigabitEthernet0/0/0]q

```

R2

```
<Huawei>sys
[Huawei]sys R2
[R2]undo info enable
[R2]int g0/0/0
[R2-GigabitEthernet0/0/0]ip add 192.168.2.2 24
[R2-GigabitEthernet0/0/0]q
[R2]int g0/0/1
[R2-GigabitEthernet0/0/1]ip add 172.16.1.1 24
[R2-GigabitEthernet0/0/1]q
[R2]int s2/0/0
[R2-Serial2/0/0]ip add 202.116.64.1 24
[R2-Serial2/0/0]q
[R2]rip 1
[R2-rip-1]version 2
[R2-rip-1]network 192.168.2.0
[R2-rip-1]network 172.16.0.0
[R2-rip-1]q
[R2]ip route-static 0.0.0.0 0.0.0.0 serial 2/0/0
```

R3

```
<Huawei>sys
[Huawei]sys R3
[R3]int g0/0/0
[R3-GigabitEthernet0/0/0]ip add 203.203.100.1 24
[R3]int s2/0/0
[R3-Serial2/0/0]ip add 202.116.64.2 24
[R3-Serial2/0/0]q
```

2.路由器R2 Easy-IP配置

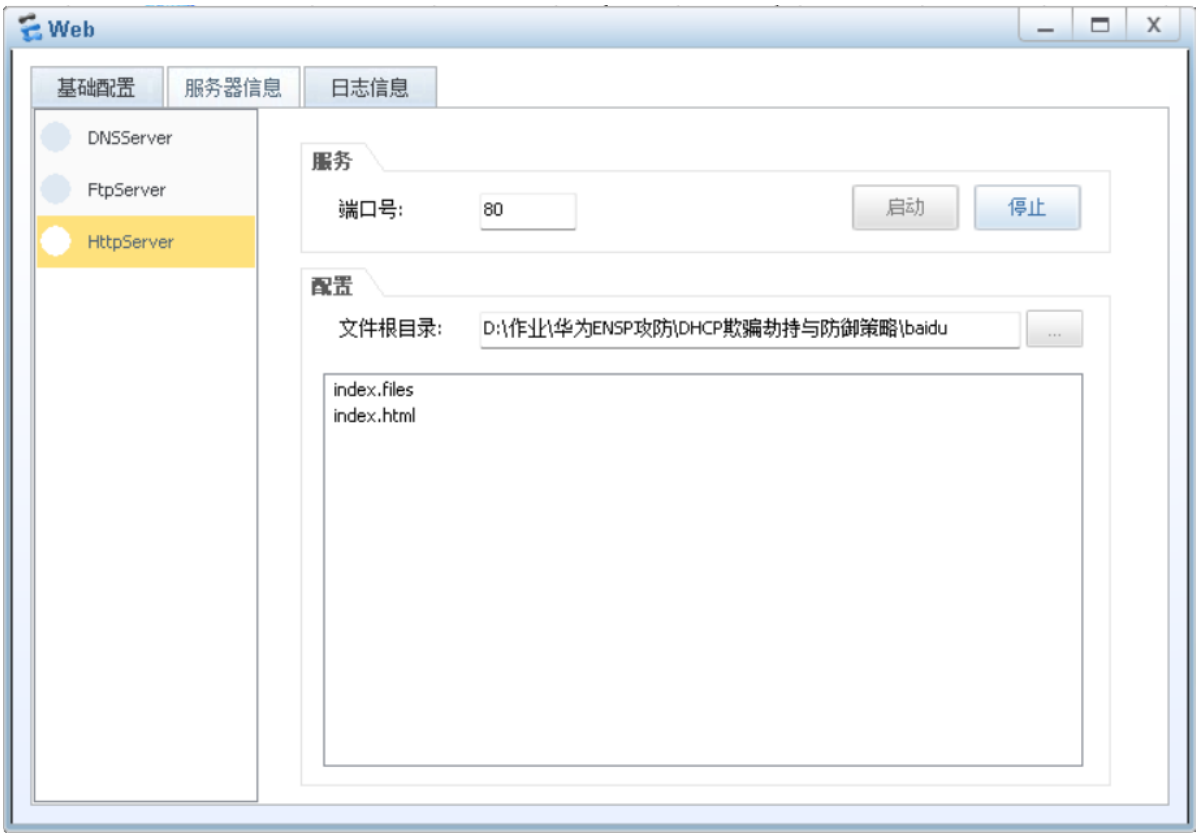
```
[R2]acl 2000
[R2-acl-basic-2000]rule permit source 192.168.1.0 0.0.0.255
[R2-acl-basic-2000]rule permit source 192.168.2.0 0.0.0.255
[R2-acl-basic-2000]rule permit source 172.16.1.0 0.0.0.255
[R2-acl-basic-2000]q
[R2]int s2/0/0
[R2-Serial2/0/0]nat outbound 2000
[R2-Serial2/0/0]q
```

3.配置R2路由器DHCP服务 给技术部和工程部主机分配IP地址

```
[R2]dhcp enable
[R2]ip pool jishu
[R2-ip-pool-jishu]network 192.168.1.0 mask 24
[R2-ip-pool-jishu]gateway-list 192.168.1.1
```

```
[R2-ip-pool-jishu]dns-list 192.168.2.254
[R2-ip-pool-jishu]excluded-ip-address 192.168.1.2 192.168.1.9
[R2-ip-pool-jishu]q

[R2]ip pool gongcheng
[R2-ip-pool-gongcheng]network 172.16.1.0 mask 24
[R2-ip-pool-gongcheng]gateway-list 172.16.1.1
[R2-ip-pool-gongcheng]dns-list 192.168.2.254
[R2-ip-pool-gongcheng]excluded-ip-address 172.16.1.2 172.16.1.9
[R2-ip-pool-gongcheng]q

[R2]int g0/0/0
[R2-GigabitEthernet0/0/0]dhcp select global
[R2-GigabitEthernet0/0/0]int g0/0/1
[R2-GigabitEthernet0/0/1]dhcp select global
[R2-GigabitEthernet0/0/1]q
```

4.配置百度服务器HttpServer

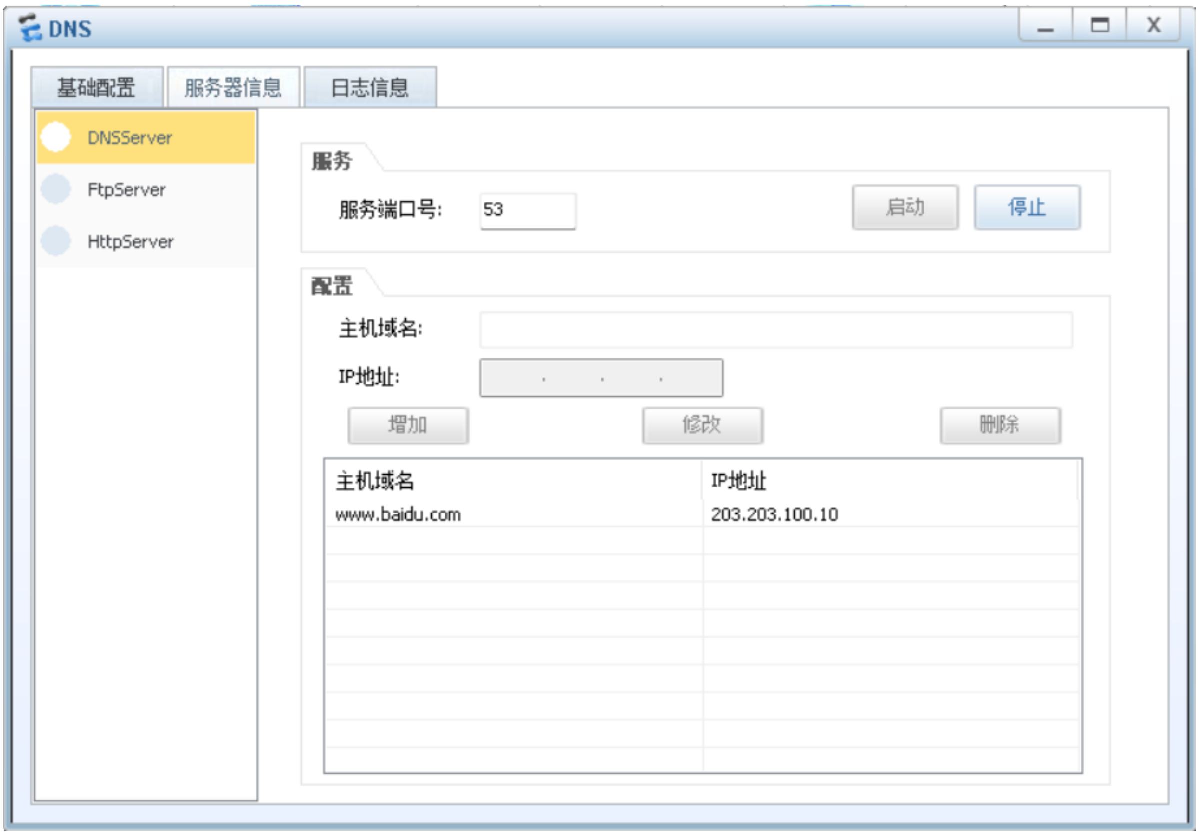


端口号: 80

文件根目录: D:\作业\华为ENSP攻防\DHCP欺骗劫持与防御策略\baidu

index.files
index.html

5.配置DNS Server



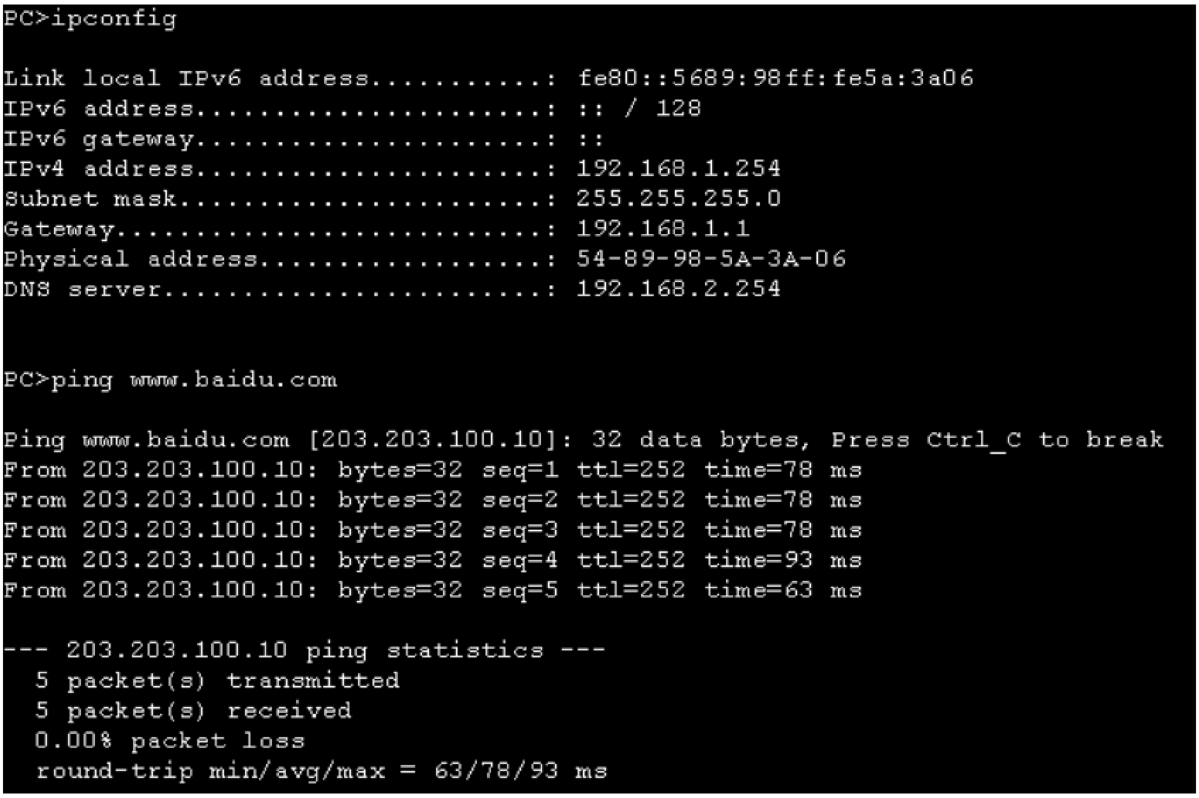
服务端口号: 53

主机域名:

IP地址:

主机域名	IP地址
www.baidu.com	203.203.100.10

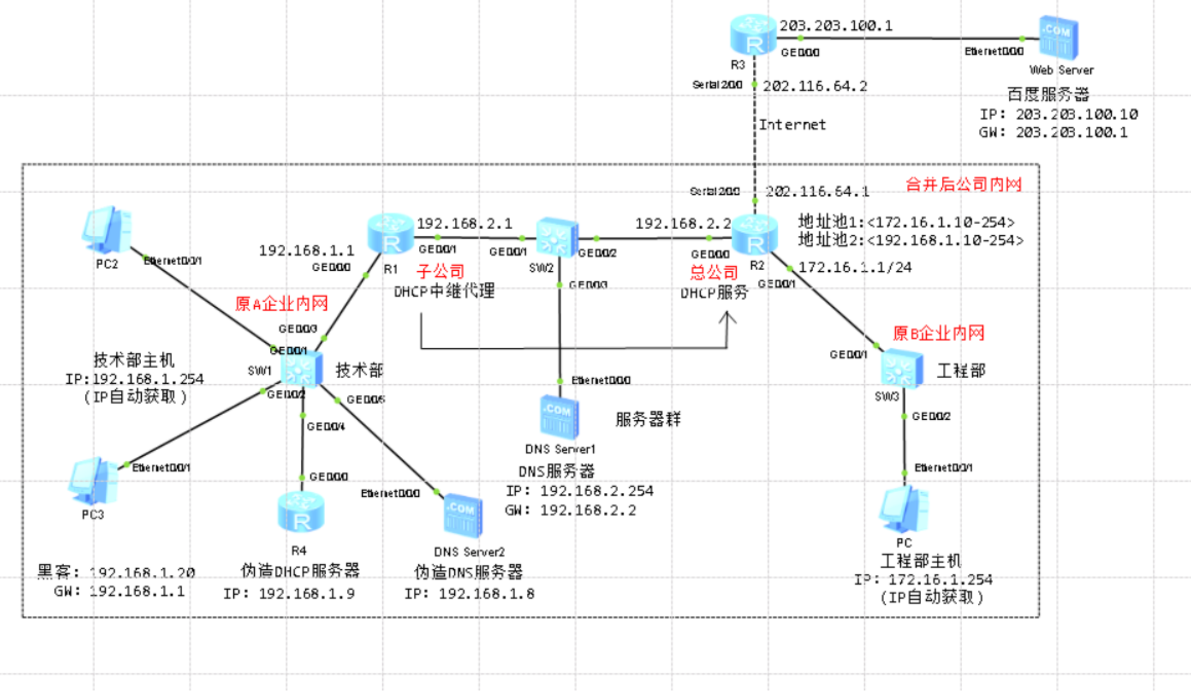
6.基本配置验证



```
PC>ipconfig

Link local IPv6 address...........: fe80::5689:98ff:fe5a:3a06
IPv6 address......................: :: / 128
IPv6 gateway......................: ::
IPv4 address......................: 192.168.1.254
Subnet mask.......................: 255.255.255.0
Gateway...........................: 192.168.1.1
Physical address..................: 54-89-98-5A-3A-06
DNS server........................: 192.168.2.254


PC>ping www.baidu.com

Ping www.baidu.com [203.203.100.10]: 32 data bytes, Press Ctrl_C to break
From 203.203.100.10: bytes=32 seq=1 ttl=252 time=78 ms
From 203.203.100.10: bytes=32 seq=2 ttl=252 time=78 ms
From 203.203.100.10: bytes=32 seq=3 ttl=252 time=78 ms
From 203.203.100.10: bytes=32 seq=4 ttl=252 time=93 ms
From 203.203.100.10: bytes=32 seq=5 ttl=252 time=63 ms

--- 203.203.100.10 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 63/78/93 ms
```

五、基本配置

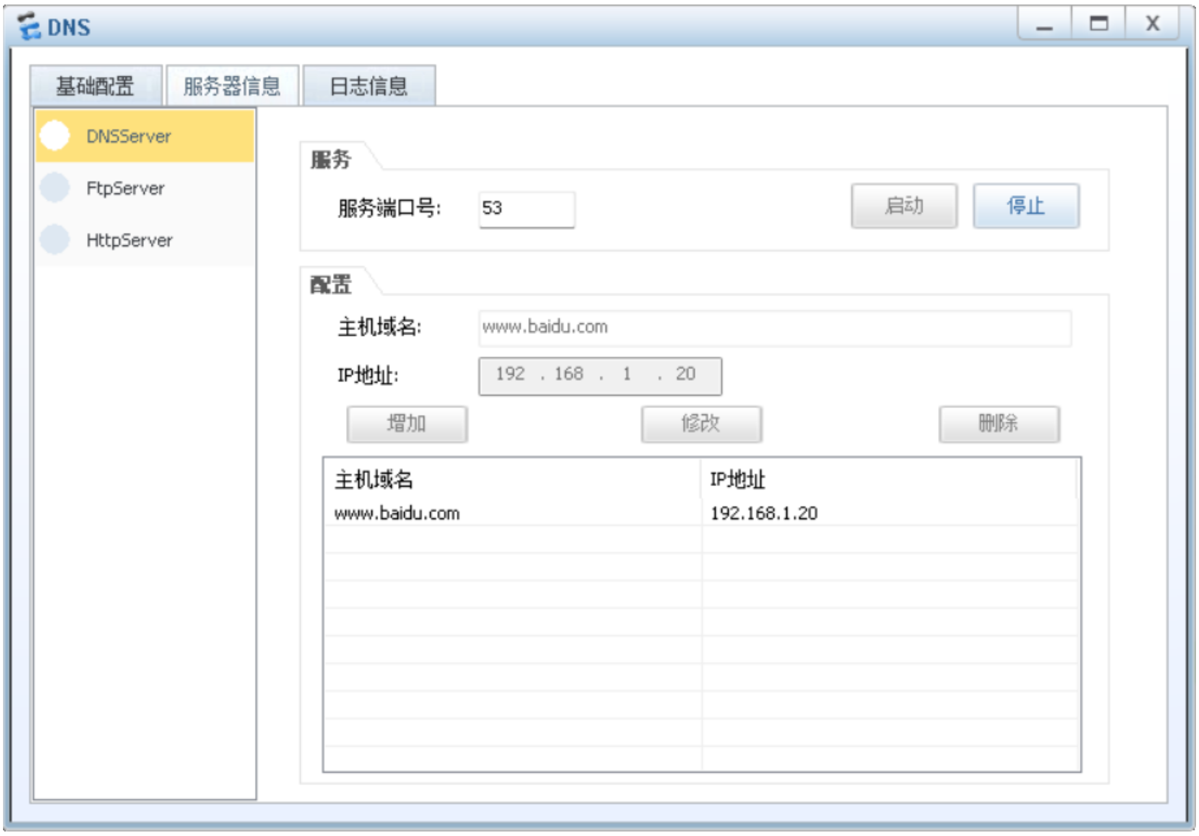
拓扑图



1.伪造DHCP服务器R4

```
<Huawei>sys
[Huawei]sys R4
[R4]undo info enable
[R4]int g0/0/0
[R4-GigabitEthernet0/0/0]ip add 192.168.1.9 24
[R4-GigabitEthernet0/0/0]q
[R4]dhcp enable
[R4]ip pool forged
[R4-ip-pool-forged]network 192.168.1.0 mask 24
[R4-ip-pool-forged]gateway-list 192.168.1.1
[R4-ip-pool-forged]dns-list 192.168.1.8
[R4-ip-pool-forged]q
[R4]int g0/0/0
[R4-GigabitEthernet0/0/0]dhcp select global
[R4-GigabitEthernet0/0/0]q
```

2.伪造DNS服务器配置



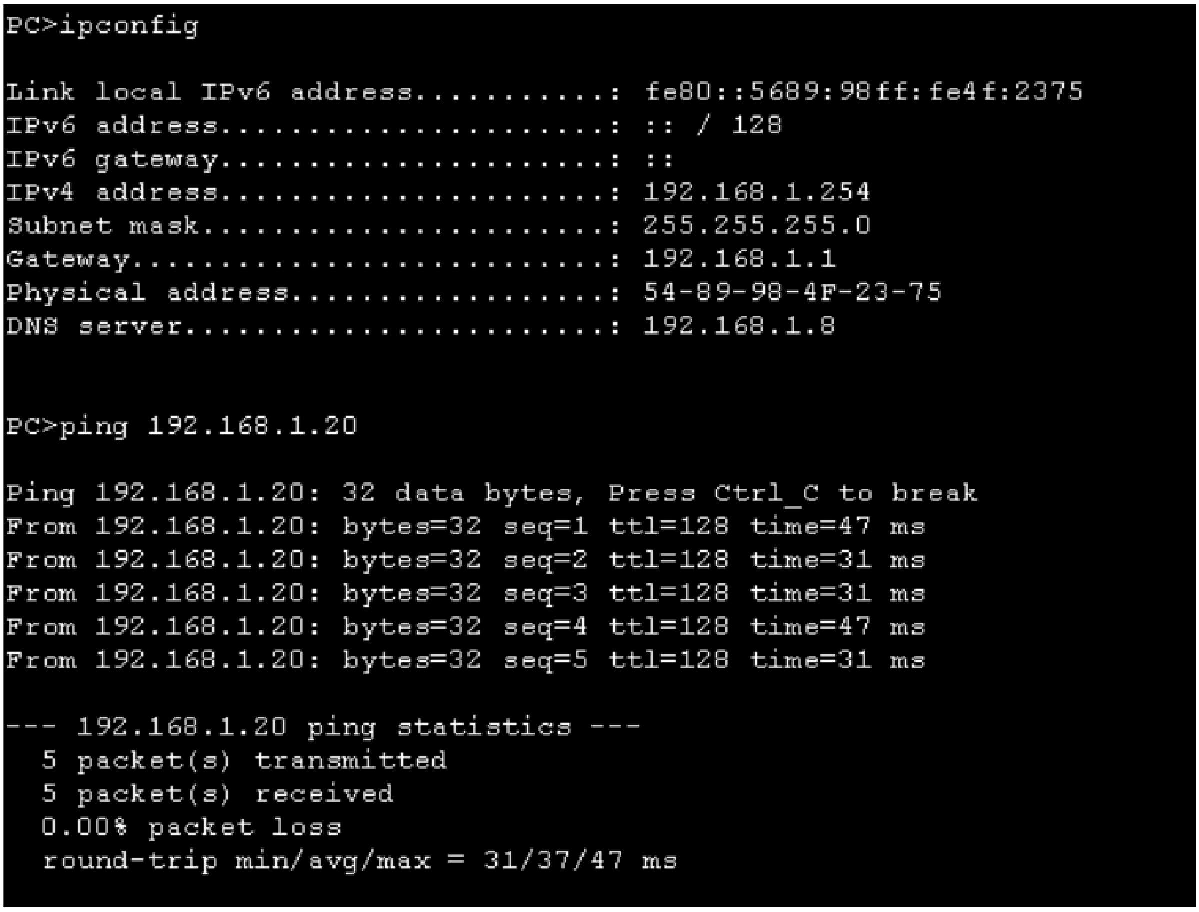
服务端口号: 53

主机域名: www.baidu.com

IP地址: 192 . 168 . 1 . 20

主机域名	IP地址
www.baidu.com	192.168.1.20

3.验证入侵结果



```
PC>ipconfig

Link local IPv6 address...........: fe80::5689:98ff:fe4f:2375
IPv6 address......................: :: / 128
IPv6 gateway......................: ::
IPv4 address......................: 192.168.1.254
Subnet mask.......................: 255.255.255.0
Gateway...........................: 192.168.1.1
Physical address..................: 54-89-98-4F-23-75
DNS server........................: 192.168.1.8


PC>ping 192.168.1.20

Ping 192.168.1.20: 32 data bytes, Press Ctrl_C to break
From 192.168.1.20: bytes=32 seq=1 ttl=128 time=47 ms
From 192.168.1.20: bytes=32 seq=2 ttl=128 time=31 ms
From 192.168.1.20: bytes=32 seq=3 ttl=128 time=31 ms
From 192.168.1.20: bytes=32 seq=4 ttl=128 time=47 ms
From 192.168.1.20: bytes=32 seq=5 ttl=128 time=31 ms

--- 192.168.1.20 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 31/37/47 ms
```

六、防御机制

在交换机SW1启用DHCP监听 添加信任端口

```
<Huawei>sys
[Huawei]sys R1
[R1]sys SW1
[SW1]undo info en
[SW1]dhcp enable
[SW1]dhcp snooping enable
[SW1]dhcp snooping enable vlan 1
[SW1]int g0/0/3
[SW1-GigabitEthernet0/0/3]dhcp snooping trusted
[SW1-GigabitEthernet0/0/3]q
```

七、任务总结

1启用DHCP监听功能的前提是开启DHCP服务

2在路由器上可以开启DHCP服务，但是无法启用DHCP监听功能，只有在交换机上才可以启用DHCP监听功能

3如果在DHCP监听区域含多个vlan，命令如dhcp snooping enable vlan 10 20 30.如果vlan连续，命令如dhcp snooping enable vlan 1 to 5.

4计算机DNS缓存不会立刻刷新需等待一段时长，如需手动刷新，可运行命令为ipconfig/flushdns

5DHCP欺骗劫持不属于病毒木马，不能通过安装反病毒软件达到防范效果