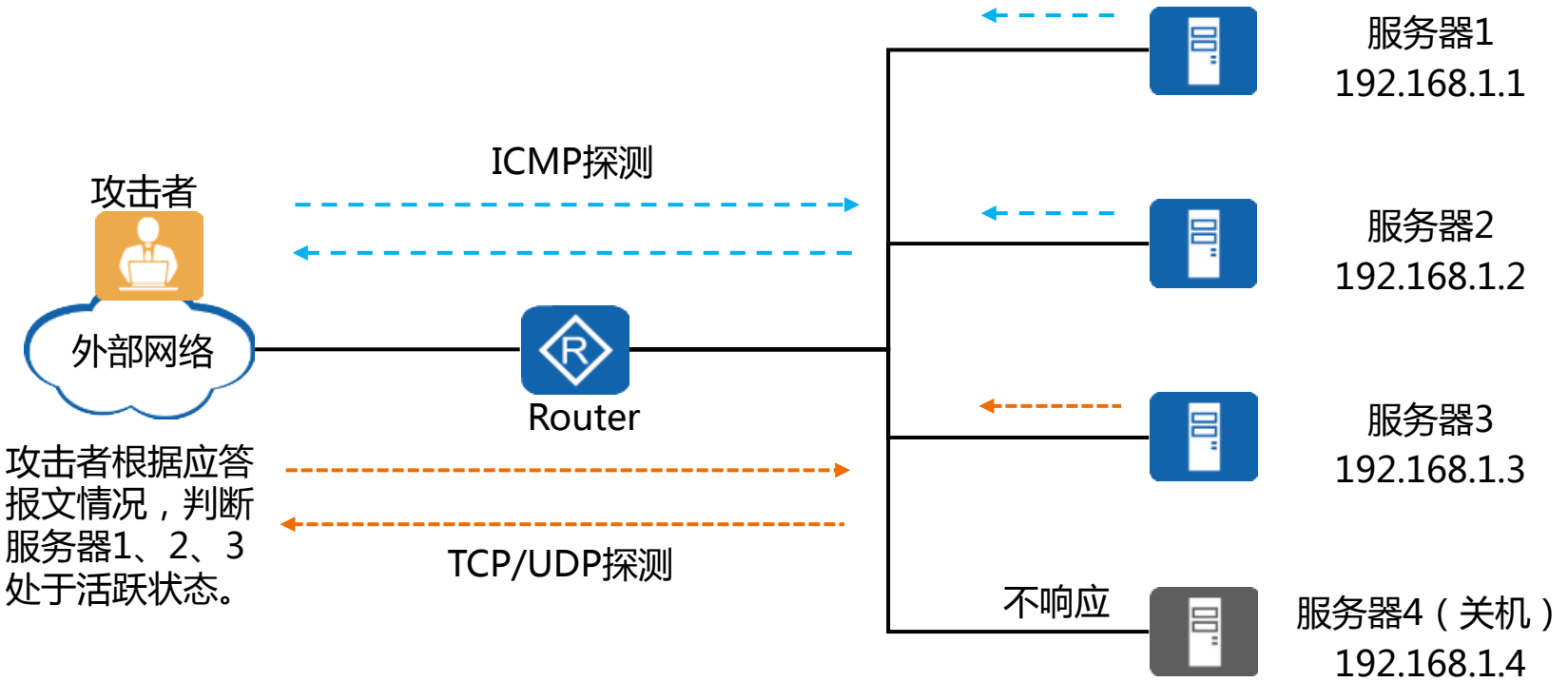
网络扫描原理
及入侵检测策略配置

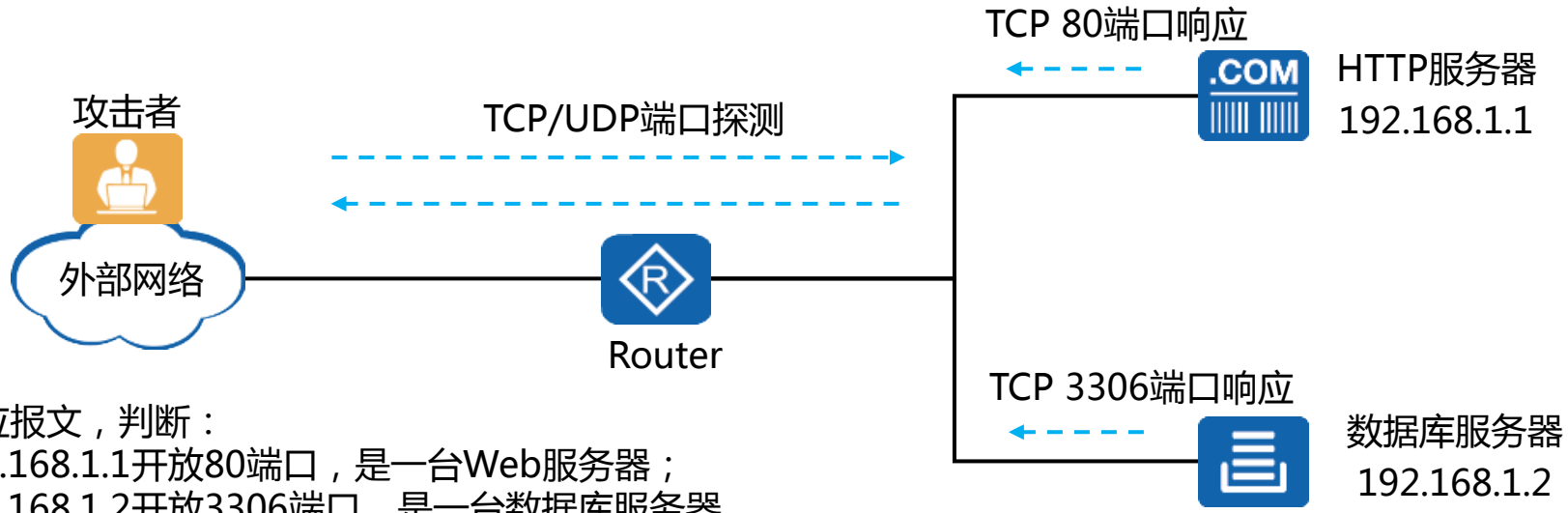
地址扫描

- 攻击者运用ICMP报文（如Ping和Tracert命令）探测目标地址，或者使用TCP/UDP报文对目标地址发起连接（如TCP Ping），若能收到对应的响应报文，则表明目标主机处于活跃状态。



端口扫描

- 攻击者通过对端口进行扫描，探寻被攻击对象目前开放的端口，以确定攻击方式。在端口扫描攻击中，攻击者通常使用端口扫描攻击软件，发起一系列TCP/UDP连接，根据应答报文判断主机是否使用这些端口提供服务。



攻击者根据响应报文，判断：

1. 服务器192.168.1.1开放80端口，是一台Web服务器；
2. 服务器192.168.1.2开放3306端口，是一台数据库服务器。

服务识别

- 如果识别到主机上开启的服务，甚至确定了服务软件的版本，则攻击者可以有更多的资源来进行攻击。
- 某些协议会主动告知访问者自己的身份，例如ssh，当客户端与服务器完成TCP握手时，会主动发送欢迎消息（banner），这其中就可能包含版本信息，具有这种特征的协议还有FTP、telnet、SMTP等
- 例如可以查到对端的22端口使用OpenSSH 7.2p2版本

```
root@localhost:~# telnet 170.170.8.102 22
Trying 170.170.8.102...
Connected to 170.170.8.102.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
```

```
root@localhost:~# nmap -sV 170.170.8.102
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-28 14:35 CST
Nmap scan report for 170.170.8.102
Host is up (0.000061s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protoc
ol 2.0)
80/tcp   open  http        Apache httpd 2.4.37 ((Ubuntu))
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp  open  ssl/http    Apache httpd 2.4.37 ((Ubuntu))
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.7.27-0ubuntu0.16.04.1
MAC Address: 00:50:56:8D:3F:4C (VMware)
Service Info: Host: TEST-VIRTUAL-MACHINE; OS: Linux; CPE: cpe:/o:linux:linux_ker
nel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.34 seconds
root@localhost:~#
root@localhost:~#
```

Date	D	A	V	Title	Type	Platform
2016-12-23	⬇		✓	OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading	remote	Linux
2016-07-18	⬇	⬇	✗	OpenSSHd 7.2p2 - Username Enumeration	remote	Linux
2016-03-16	⬇		✗	OpenSSH 7.2p1 - (Authenticated) xauth Command Injection	remote	Multiple
2008-05-16	⬇	⬇	✓	OpenSSL 0.9.8c-1 < 0.9.8g-9 (Debian and Derivatives) - Predictable PRNG Brute Force SSH (Ruby)	remote	Linux

主机识别

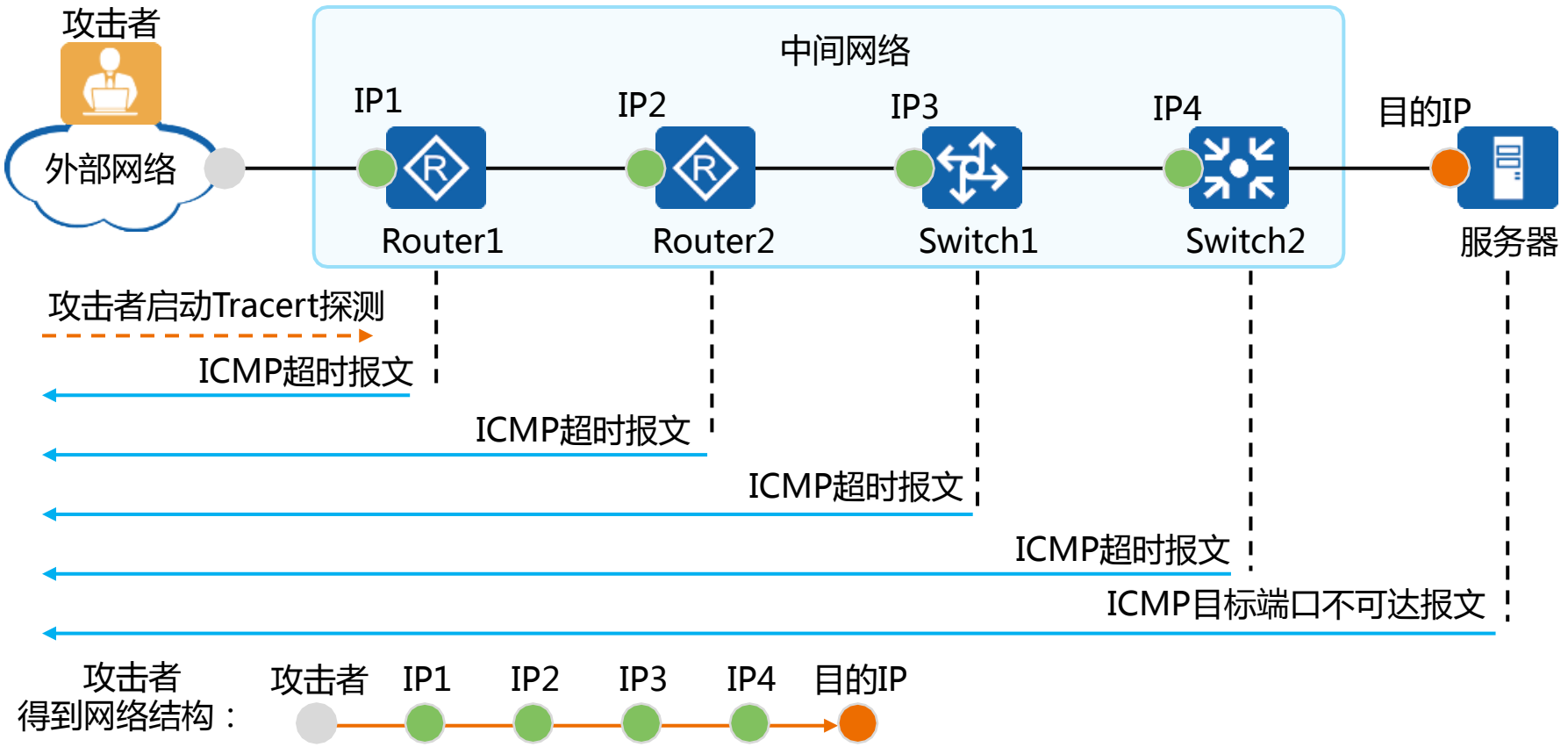
- 同服务识别类似，识别主机的操作系统，可以给攻击提供很多便利，例如利用操作系统本身的漏洞等。
- 图中nmap使用-O选项来识别主机，识别结果为windows操作系统，版本可能是windows 7、windows server 2008或者windows 8.1.

```
root@localhost:~# nmap -O 170.170.16.116
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-28 14:32 CST
Nmap scan report for 170.170.16.116
Host is up (0.00018s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:DB:D1:1E (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:mic
rosoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:m
icrosoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Serv
er 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.21 seconds
```

Tracert攻击原理

- Tracert攻击是攻击者利用TTL为0时返回的ICMP超时报文，以及到达目的地址时返回的ICMP端口不可达报文，来发现报文到达目的地所经过的路径，主要用于窥探目标网络的结构。

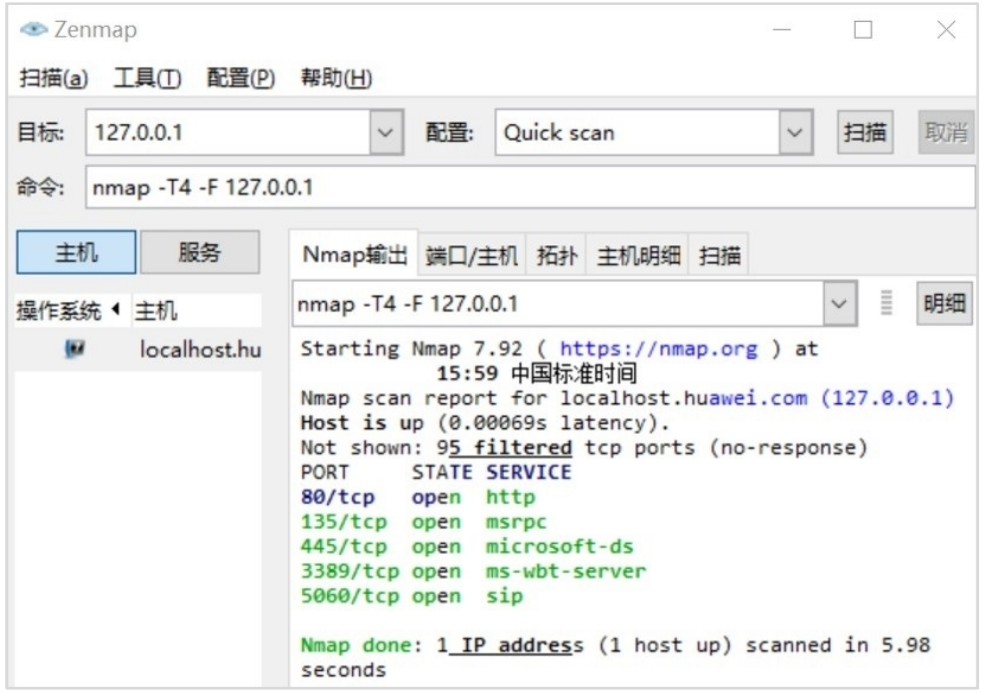


渗透测试工具 - Nmap

Nmap，即Network Mapper，最早是Linux下的网络扫描与嗅探工具，现发展为跨平台的综合扫描软件，支持Windows、Linux、macOS等多种操作系统。

Nmap具备如下扫描功能：

- 主机发现：检测目标主机是否在线；
- 端口扫描：检测端口状态和提供的服务；
- 操作系统侦测：检测主机使用的操作系统。




```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -Pn 192.168.238.178
Starting Nmap 7.94 ( https://nmap.org ) at              23:23 CST
Nmap scan report for 192.168.238.178
Host is up (0.0042s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
8000/tcp open  http-alt
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 16.32 seconds
```

2 网络扫描检测配置实验

网络扫描检测配置实验

关于本实验

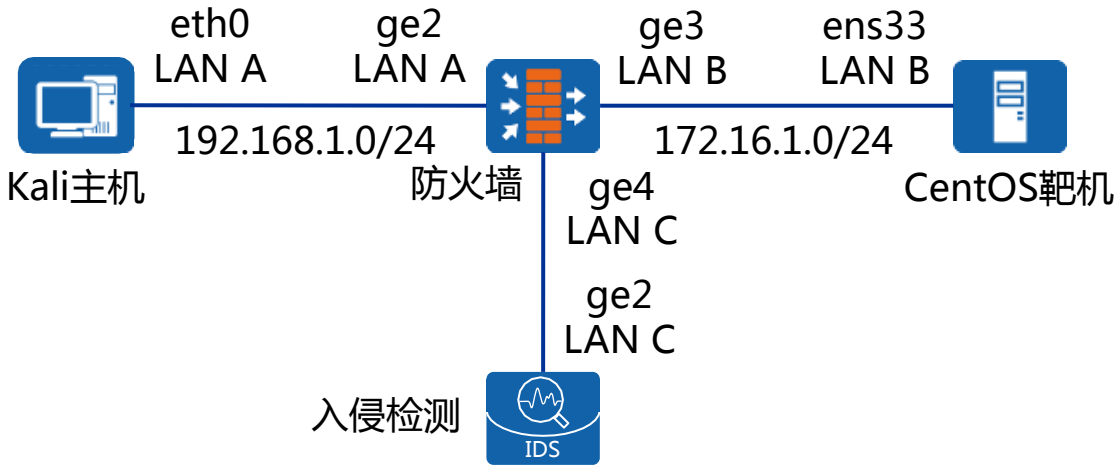
通过配置入侵检测策略，实现端口扫描攻击的检测。

实验目的

理解端口扫描攻击的原理，练习入侵检测策略的配置。

实验背景

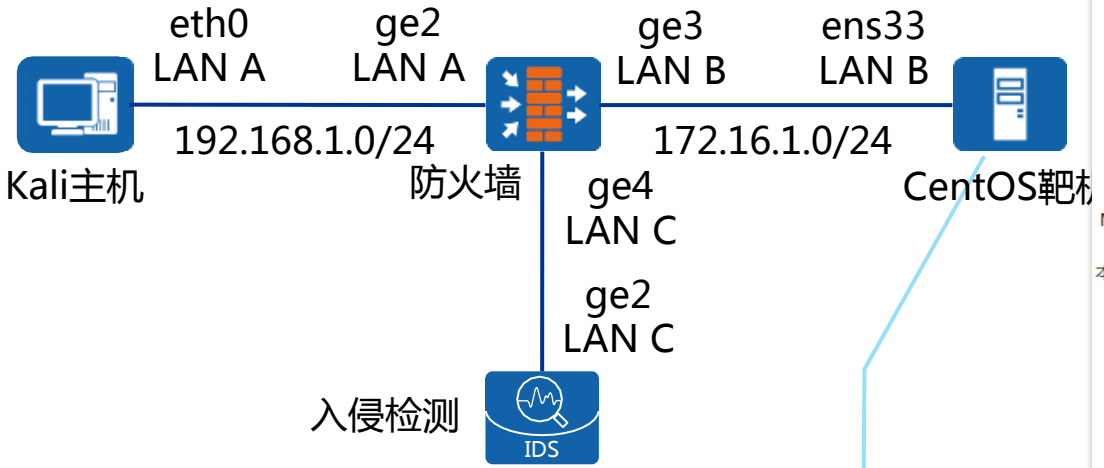
Kali主机和靶机之间，通过防火墙设备进行网络连接，防火墙将连接靶机的流量，通过端口镜像引流到入侵检测设备。



网络扫描检测配置实验-基础配置

拓扑搭建基础配置

➢ 1、防火墙接口IP地址配置




```
# 启动“pikachu” 靶场，sudo密码centos
[centos@localhost ~]# sudo docker start pikachu
```

ge2	路由模式	192.168.1.1/255.255.255.0 fe80::20c:29ff:fecf:22fc/64	0
ge3	路由模式	172.16.1.1/255.255.255.0 fe80::20c:29ff:fecf:2206/64	0
ge4	交换模式	access	