网络监控和
高级网络配置

前 言

- 对于服务器而言，确定网络服务在哪个端口运行，是很重要的事情。额外多开的端口，将会为攻击者提供攻击的途径。
- IP 别名，同一块物理网卡，相同的MAC Address，配置不同的 Layer 3 - IP 地址，适用于 Web 托管、HA容错、路由…等机制。
- 本章节将介绍以下几点：
  - 检测开放端口
  - 网络端口配置 - IP别名
  - 静态路由配置

培训目标

- 学完本课程后，您应该能够：
  - 检测开放端口
  - 网络端口配置 - IP别名
  - 静态路由配置

目 录

检测本地端口

- netstat -tupln | grep :25
  - t：TCP 仅显示 tcp 相关选项
  - u：UDP 仅显示 udp 相关选项
  - p：Procedure 显示建立相关连接的程序名
  - l：List 仅列出正在 Listen (监听) 的服务状态
  - n：拒绝显示别名，能显示数字的全部转化成数字

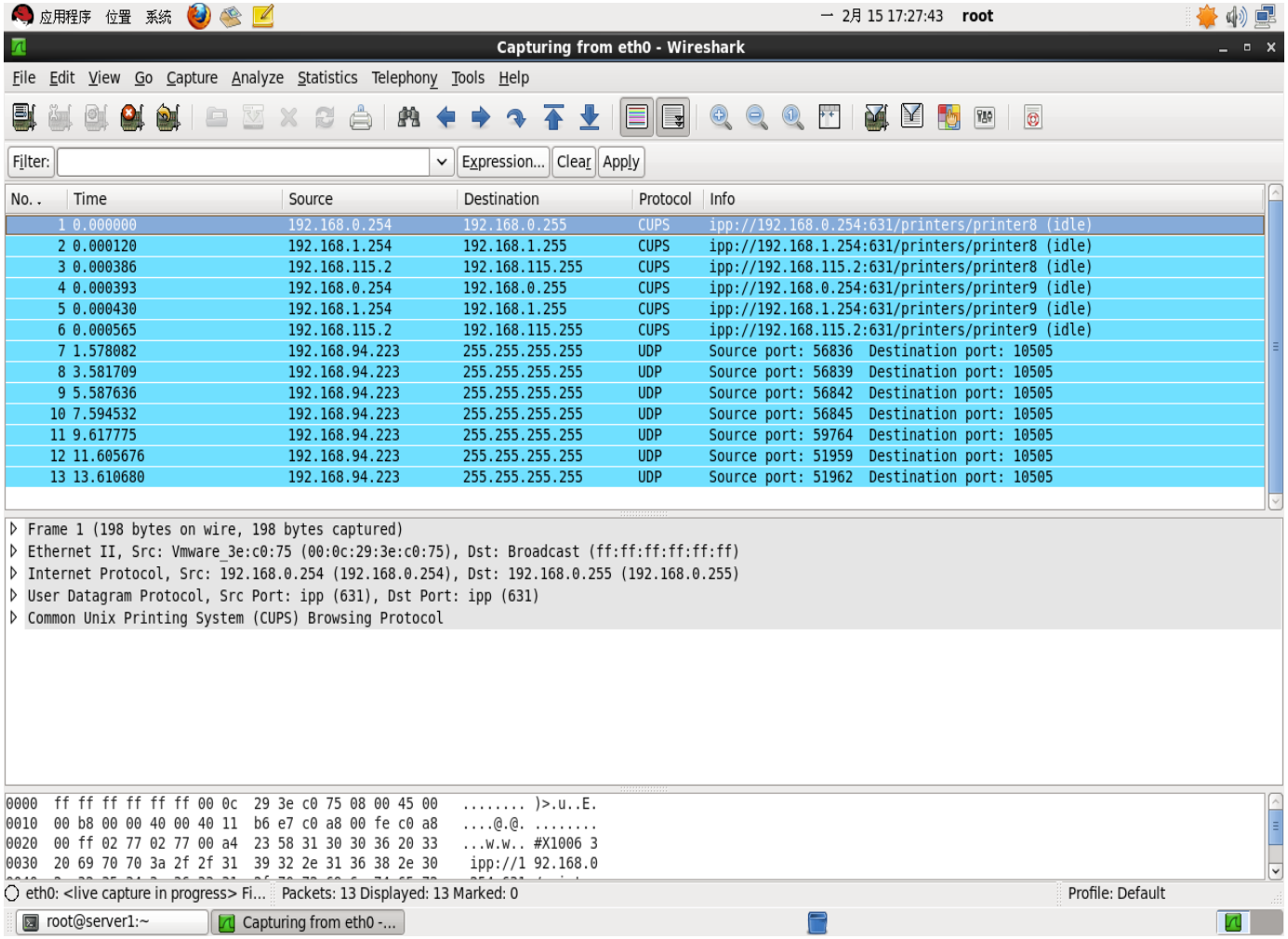
```
[root@server1 ~]#
[root@server1 ~]# netstat -tupln | grep :25
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN      2537/master
[root@server1 ~]#
```

检测远程服务

- nmap 软件包
- 可以单独检测服务器
  - 例如：nmap 192.168.0.101
- 可以检测整个 class C
  - 例如：nmap 192.168.0.0/24
  - 不支持 255.255.255.0 的语法
- 如果没有防火墙干扰，应该跟 netstat 结果一致

通过 wireshark 捕获/分析网络封包

- 软件包：wireshark*
- 跟 tcpdump 使用相同格式



目 录

IP alias - IP 别名

- 在相同的 Layer 1【网卡】及 Layer 2【MAC Address】，指定不同的 Layer 3 - IP 地址
- 命名原则：
  - eth0
  - eth0:0
  - eth0:1 …

那些不支持 IP 别名

- DHCP 不支持别名
- NetworkManager 不支持别名
  - NetworkManager 也不支持网卡绑定
  - service NetworkManager stop
  - chkconfig NetworkManager off

配置 IP 别名

- 命令行：
  - ifconfig eth0:0 192.168.1.101 netmask 255.255.255.0
  - 网络服务重启，或服务器重启后失效
  - 方便测试
- 配置文档
  - /etc/sysconfig/network-scripts/ifcfg-eth0:0
  - 网络服务重启，或服务器重启后依然有效
  - 语法跟一般网卡配置相同

目 录

开启路由

- 启用数据包从一块网卡进，一块网卡出的功能
- 默认是关闭
- 启动路由、NAT，必须要先开启路由

```
[root@server1 ~]# cat /proc/sys/net/ipv4/ip_forward
0
[root@server1 ~]# echo "1" > /proc/sys/net/ipv4/ip_forward
[root@server1 ~]#
[root@server1 ~]# cat /proc/sys/net/ipv4/ip_forward
1
[root@server1 ~]#
```

/etc/sysctl.conf

- net.ipv4.ip_forward = 1
- sysctl -p /etc/sysctl.conf：立刻生效
- /etc/rc.d/rc.sysctl，执行 sysctl -p /etc/sysctl.conf

添加静态路由 - 命令行

- route add -net 192.168.101.0 netmask 255.255.255.0 gw 192.168.0.101

```
[root@server1 ~]# route add -net 192.168.101.0 netmask 255.255.255.0 gw 192.168.0.101
[root@server1 ~]#
[root@server1 ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.101.0   192.168.0.101   255.255.255.0   UG    0      0        0 eth0
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U     1002   0        0 eth0
0.0.0.0         192.168.0.254   0.0.0.0         UG    0      0        0 eth0
[root@server1 ~]#
```

添加静态路由 - 配置文件

- /etc/sysconfig/network-scripts/route-iface
  - ADDRESS0=192.168.101.0
  - NETMASK0=255.255.255.0
  - GATEWAY0=192.168.0.101

说明文件 - 1

- Red Hat Enterprise Linux Security Guide
  - 第 2.2.8 节：验证正在侦听那些端口
- Red Hat Enterprise Linux Security Guide
  - 第 1.2.3.1 节：通过 nmap 扫描主机
- netstsat(8)
- nmap网站：http://www.insecure.org
- wireshare(1)

说明文件 - 2

- wireshare网站：http://www.wireshark.org
- tcpdump(8)
- /usr/share/doc/initscripts-*/sysconfig.txt
- Red Hat Enterprise Linux Deployment Guide
  - 第 4.2.3 节：别名和克隆文件
- Red Hat Enterprise Linux Deployment Guide
  - 第 19.3.9.4 节：/proc/sys/net

说明文件 - 3

- /usr/share/doc/kernel-doc-*/Documentation/sysctl/
- Red Hat Enterprise Linux Deployment Guide
  - 第 4.4 节：配置静态路由

问 题

- NetworkManager是否支持 IP 别名?
- 试比较 netstat 与 nmap 的差异?

总 结

- 本课程中，我们学习了：
  - 检测开放端口
  - 网络端口配置 - IP别名
  - 静态路由配置

谢谢

Thank You