**《**工具培训之Wireshark和Tcpdump**》考试题目**

(考试时间: 60分钟，满分100 分)

姓名： 工号： 分数：

1. 单选题 (每题4分)
2. 截获所有210.27.48.1 的主机收到的和发出的所有的数据包（ ）

A) #tcpdump B) #tcpdump –i eth0 host 210.27.48.1

C) #tcpdump host 210.27.48.1 D) #tcpdump src 210.27.48.1

2、那个选项不是tcpdump 表达的修饰类型（）

A)type B) dir C)Length D)proto

3、tcpdump 抓包保存文件的命令参数（ ）

A)-W B) -Write C)-w D)-write

4、Wireshark 过滤源，只保留数据的发送源地址192.168.0.102，目标地址192.168.0.100的过滤条件是：（）

A) (ip.dst == 192.168.0.100) & (ip.src == 192.168.0.102)

B) (ip.dst == 192.168.0.100) | (ip.src == 192.168.0.102)

C) (ip.dst == 192.168.0.100) &&(ip.src == 192.168.0.102)

D) (ip.dst == 192.168.0.100) || (ip.src == 192.168.0.102)

5、Wireshark 主要应用方向（）

A)网络管理员用来解决网络问题

B)网络安全工程师用来检测安全隐患

C)开发人员用来测试协议执行情况

D)用来加密网络协议

1. 多选题(每题5分)

１、tcpdump将eth0 上的数据包抓取到并保存到制定的文件中,用到的命令参数包含（ ）

A)-r B) -W C)-i D)-w

2、tcpdump 支持的命令参数包括 （ ）

　　 A)port B) tcp C)udp D)-s

３、对Wireshark 说法正确的有（ ）

　　A) Wireshark能抓取无线空中数据包 B) Wireshark　能抓取http协议信息

C) Wireshark　能导出TCP 流 D) Wireshark　能抓取互联网上的所有数据

4、Wireshark 包列表信息包括（ ）

　 A)No. B) size C)Source D)protocol

5、Wireshark 数据包列表上下文菜单过滤说法正确的是（ ）

A)能对Time 进行过滤 B) 能对Source 列进行过滤

C)能对info　进行过滤 D) 能对protocol 列进行过滤

1. 判断题 (正确打√，错误打×) (每题4分)

1、tcpdump 可以不带任何参数运行 （ ）

2、tcpdump 抓取的数据，只有数据包头信息 （ ）

3、tcpdump 抓取的数据能被wireshark 解析 （ ）

4、wireshark 报错的http 视频流可以直接播放 ( 　)

５、电脑接上路由器，可以抓取路由器局域网上所有的数据包 （ ）

1. 简答题 (每题10分)
2. 如何通过tcpdump 查看设备eth0 ，端口1111 是否传输数据
3. Wireshark 抓取网络TS 流的方法
4. 案例分析题 (每题15分)

1、你在开发通过智能手机控制电视的软件中 ，发现有时电视不能被你的软件控制，你有哪些方法，如何分析解决此问题？