به نام خدا

گزارش آزمایش جلسه‌ی ۱

نام و نام خانوادگی - شماره دانشجویی

نام و نام خانوادگی - شماره دانشجویی همگروهی

نکات اصلی:

نام فایل: به ترتیب از چپ، شماره آزمایش، ساعت گروه، شماره گروه و شماره دانشجویی اعضاء

CNL{1..10}-{10,13,16}-{1..8}-sn1_sn2.pdf

مشخصات افراد

قالب فایل:

- فونت نازنین ۱۱ یا ۱۲
- پرهیز از عکس و نوشتن محتوای لازم و خواسته شده، حاشیه‌ی اضافه برداشته شود و فقط بخش مربوط به جواب در آن قرار داشته باشد.
- پرهیز از حاشیه و زیاده گویی
- پاسخ دقیق به سوالات و نتایج حاصل از آزمایش

بیان نظرات، مشکلات و انتقادات در رابطه با هر جلسه (حل و تمرین، آزمایش، محیط، روال) و یا ارسال پیام شخصی

آزمایش ۱) سرویس TELNET:

برنامه‌های در حال اجرا قبل و بعد از دستور telnet. همان طور که دیده می‌شود شماره‌ی اجرای برنامه telnet برابر ۱۲۳ است.

```
root@netlab-term-3:/# ps -e
  PID TTY          TIME CMD
    1 pts/0    00:00:00 sh
   52 pts/0    00:00:00 bash
   81 ?        00:00:00 busybox
   97 pts/1    00:00:00 bash
   99 pts/1    00:00:00 busybox
  105 ?        00:00:00 xinetd
  111 ?        00:00:00 dhclient
  112 pts/1    00:00:00 bash
  123 pts/1    00:00:00 telnet
  124 pts/0    00:00:00 ps
```

```
root@netlab-term-3:/# ps -e
  PID TTY          TIME CMD
    1 pts/0    00:00:00 sh
   51 pts/0    00:00:00 sudo
   52 pts/0    00:00:00 bash
   58 pts/0    00:00:00 dhclient
   81 ?        00:00:00 busybox
   97 pts/1    00:00:00 bash
   99 pts/1    00:00:00 busybox
  105 ?        00:00:00 xinetd
  106 pts/0    00:00:00 ps
```

سوال‌ها:

۱) سرویس inetd، پایه ای ترین سرویس پیاده شده در سیستم های Unix برای ارائه‌ی خدمات اینترنت است. به عنوان مثال سرویس telnet, FTP, POP3, echo و ... است.

۲) خیر. این برنامه خیلی وقت است که با نسخه ارتقا یافته آن (xinetd) که معماری کامل تری دارد، جایگزین شده است.

۳) بله. ۱۰۵

آزمایش ۲) سرویس پیشفرض های شبکه:

```
➤ ls -l ser*
 UsersGrp     34926 Mar 22 07:59 ser-cat
 UsersGrp     17463 Mar 22 07:59 ser-cp
 UsersGrp     17463 Mar 22 07:58 ser-more
```

آزمایش ۳) دستورات شبکه در لینوکس:

۱. Arp: برنامه ای برای دیدن و تغییر حافظه‌ی موقت
۲. Arping: برنامه ای برای ارسال درخواست arp-request به شبکه‌ی محلی
۳. Ifconfig: برنامه‌ی تنظیم کردن واسط های شبکه
۴. Tcpdump: برنامه ای برای دیدن و ذخیره کردن بسته های ارسالی و دریافتی در شبکه
۵. Ping: برنامه برای ارسال درخواست icmp-echo_request
۶. Netstat: برنامه ی دیدن وضعیت اتصال های فعال، مسیریابی‌ها، وضعیت واسط ها، وضعیت مسیرهای ارسال گروهی است.
۷. Route: برنامه ای برای دیدن و تغییر مسیریابی‌های داخل هسته سیستم عامل لینوکس
۸. Wireshark: برنامه ی گرافیکی برای دیدن، ذخیره، فیلتر کردن و دستکاری بسته‌های شبکه
۹. iptables: برنامه‌ای برای کنترل بسته‌های دریافتی و ارسالی در لینوکس

آزمایش ۴) ضبط و ذخیره‌ی بسته:

برای قسمت پروتکل در لایه‌ی ip، مقادیر مختلفی مشاهده شد که پر تکرار ترین آن ها مربوط به TCP(6), IGMP(2) و UDP(17) بوده است. این قسمت در لایه‌ی ip مشخص کننده‌ی نوع داده و ساختار آن در لایه‌ی بالاتر است.

مقدار نوع بسته در لایه‌ی ۲ (Ethernet) برای بسته‌های ip برابر 0x0800 است.

آزمایش ۵) بسته‌های ARP:

مقدار نوع بسته برای بسته‌های ARP برابر 0x0806 مشخص شده است.

مقدار نوع بسته در لایه‌ی frame یا همان Ethernet مشخص می‌کند که بسته‌ی داخلی آن چه نوعی است.

آزمایش ۶) فیلتر کردن نتایج بسته:

دیدن بسته‌های شبکه به کمک ابزارهای معرفی شده ممکن است، اما در شرایط واقعی، حجم بسته‌ها و خروجی تولید شده، می‌تواند بسیار زیاد و گیج کننده باشد. به کمک فیلترهای کمکی می‌توان نتایج مورد نظر را در خروجی دید و مورد تحلیل و بررسی قرار داد. نتیجه برای مثال‌های داده شده به شرح زیر است:

- نمایش بسته‌های udp با درگاه ۵۲۰
- نمایش بسته‌های ip با نوع ۸۹ (الگوریتم مسیر یابی OSPF) را نمایش می‌دهد
- نمایش بسته های IP مبادله شده بین ip_addr1 و یکی از دو ماشین ip_addr2, ip_addr3
- نمایش بسته‌هایی که بین ماشین ۱ و هر ماشین دیگر به غیر از ماشین ۲ تبادل شده است.

آزمایش ۷) درگاه اتصال telnet:

درگاه در ماشین h1 برابر ۲۳ و در ماشین h2 برابر ۵۰۲۸ است. درگاه مقصد telnet یا همان درگاه ۲۳ در فایل services نوشته شده است.

آزمایش ۸) درگاه تصادفی)

وقتی از چند ماشین به یک ماشین ارتباط مشخصی را برقرار می‌کنیم، درگاه بسته برای مقصد بین تمام اتصال‌ها مشترک بوده و تنها درگاه مبدأ به شکل تصادفی انتخاب می‌شود. برای هر کدام از برنامه‌ها، یک پورت تصادفی به شماره‌های ۵۷۸۴ و ۸۸۷۳ انتصاب داده شده است.

پریز (socket) یک ارتباط داخلی (بر روی سکوی سیستم عامل) ساخته شده بین دو گره (کامپیوتر) در شبکه است که داده در داخل آن منتقل می‌شود. آدرس دهی به شکل متداول شامل یک زوج آدرس اینترنتی شبکه (ip) به همراه یک درگاه (port) می‌شود. به عنوان مثال یک پریز باز را دو آدرس 10.0.0.1:1234 و 10.0.0.2:2345 می‌تواند تعریف بشود.