

بسمه تعالی



آزمایشگاه شبکه

دانشکده برق و کامپیوتر

دانشگاه صنعتی اصفهان

زمستان ۱۴۰۱

دکتر حیدرپور، دکتر فانیان

آشنایی با مقدمات شبکه، پروتکل‌ها و wireshark

## هدف آزمایش:

در این آزمایش سعی بر آن است که به صورت عملی با دستورات شبکه و همچنین پروتکل‌های پرکاربرد در شبکه آشنا شده و به کار ببریم.

### گام اول:

آدرس سیستم و gateway خود را بررسی نمائید و مشخص کنید این آدرس‌ها مربوط به کدام کلاس ip هستند. (با استفاده از UI گرافیکی سیستم عامل)

### گام دوم:

پوشه‌ای را بر روی سیستم خود به اشتراک بگذارید و سپس یک فایل که نام آن مطابق نام شما و محتوای آن یک متن دلخواه است را درون پوشه قرار دهید؛ همچنین به پوشه‌ی به اشتراک گذاشته‌ی هم‌گروهی خود بروید و فایل داخل آن را بررسی نمائید. (توجه فرمایید اگر از لینوکس استفاده می‌کنید می‌توانید از سرویس samba بهره ببرید)

### گام سوم:

موارد زیر را از طریق خط فرمان (command line) بررسی نمائید:

- آدرس سیستم شما چیست؟
- آدرس سیستم شما به صورت دستی تنظیم شده است یا اتوماتیک؟
- با استفاده از دستور مناسب، آدرس‌های فیزیکی (mac address) را بدست آورید.

گام چهارم:

کامپیوتر هم‌گروهی خود را پینگ (ping) بگیرید و مشخص کنید چه اطلاعاتی در هر یک از پیام‌های برگردانده شده وجود دارد. همچنین از آپشن مناسب برای دستور پینگ استفاده کنید تا فقط ۸ بسته‌ی ICMP ارسال و دریافت شود.

همچنین صحت ارتباط خود با `www.google.com` را بررسی نمایید؛ چه پیغامی مشاهده می‌کنید؟

گام پنجم:

- با استفاده از دستور `nslookup` آدرس سرورهای `google` و `yahoo` را بدست آورید.
- با استفاده از دستور `arp` جدول `arp` را نشان داده و اطلاعات آن را تحلیل نمایید.
- با استفاده از دستور `netstat` جداول `routing`، وضعیت `interface` ها و همچنین وضعیت پورت‌ها را مشخص نمایید. همچنین عملکرد آپشن‌های `a` و `n, p` را نیز بررسی نمایید.
- با استفاده از دستور `whois` تمامی اطلاعات مربوط به دامنه‌ی `google.com` را بدست آورید. همین کار را یک‌بار دیگر با آیپی ماشین هم‌گروهی خود انجام دهید.
- با بهره‌گیری از دستور `traceroute` یا `tracert` مسیر بسته‌ها به آدرس `google.com` را بررسی نمایید. همین کار را یک‌بار دیگر با آیپی ماشین هم‌گروهی خود انجام دهید. مشخص نمایید دستور زیر چه کاری انجام می‌دهد:

```
tracert -h 30 -w 60 google.com #in windows
traceroute -m 30 -w 1 google.com #in linux
```

- با استفاده از دستور `hping3` سه بسته که فلگ‌های `FIN, SYN` و `ACK` آنها ۱ باشد بر روی پورت دلخواه و آدرس دلخواه ارسال فرمایید. (می‌توانید برای بررسی پورت‌های باز یک آدرس دلخواه از ابزار `nmap` استفاده نمایید) (امتیازی – بهتر است انتهای کار از `linux` استفاده کنید)

گام ششم: **netsh** (امتیازی)

ip سیستم خود را به صورت استاتیک به آدرس 192.168.58.3 تغییر دهید.

این بار ip جدیدی از DHCP server درخواست کنید.

DNS server خود را به صورت استاتیک به 18.72.0.3 تغییر دهید.


DNS server جدیدی را از DHCP بخواید.

گام هفتم:

یک مرورگر باز کرده و آدرسی را در آن سرچ کنید. سپس با بهره‌گیری از ابزار wireshark موارد

زیر را مشخص نمایید:

- ابتدا با استفاده از دستور مناسب، کش میزبان خود را خالی کنید. همچنین کش مرورگر را نیز پاک کنید.
- آدرس فرستنده‌ی DNS query و آدرس پیغام‌های پاسخ را مشخص نمایید.
- نوع پروتکل (TCP / UDP) را در بسته‌های DNS مشخص نمایید. همچنین پورت‌های مبدا و مقصد را نیز بیابید. تایپ DNS response را نیز مشخص نمایید. وضعیت بیت‌های پرچم و همین‌طور فلگ‌های بسته‌ای را مشخص نمایید.
- برنامه‌ی wireshark را بر روی فیلتر http قرار داده و سپس مشخص کنید مرورگر شما از کدام یک از ورژن‌های http استفاده می‌کند. (به صورت امتیازی می‌توانید تفاوت آنها را توضیح دهید). علاوه بر مراحل یاد شده، عملیات three way handshake را در سناریوی یاد شده مشخص نمایید.
- نتایج بدست آمده را با عنوان فایلی به فرمت زیر در مسیر دسکتاپ ذخیره نمایید.

 userID-1.pcap

- گام قبل را فقط برای ذخیره‌سازی بسته‌های ICMP انجام دهید.

 userID-2.pcap

- این بار DNS Server خود را تغییر دهید و مجدداً کش مرورگر و سیستم را پاک کرده و بار دیگر وایرشارک را در حال شنود گذاشته و همچنین آدرس سایتی را جستجو فرمایید؛ بسته‌های مربوط به پروتکل DNS را مشاهده نمایید. آیا آدرس سرور DNS ای که پاسخ داده است، همان آدرس DNS تنظیم شده است؟
- با استفاده از ابزار tcpdump ابتدا ترافیک کارت شبکه اترنت خود را در فایل traffic.pcap ذخیره کرده و سپس با استفاده از wireshark محتوای این فایل را آنالیز کنید. (امتیازی – بهتر است انتهای کار از linux استفاده کنید)

خسته نباشید (:)