به نام خدا
آزمایش اول
شبکه های بیسیم
استاد: دکتر سید وحید ازهری

لطفاً پیش از حل کردن تمرین به نکات زیر توجه کنید:

۱. در قسمت هایی که پاسخ تشریحی خواسته شده فهم خود از مطلب را مکتوب کرده و جداً از ترجمه کردن پرهیز کنید.
۲. به زبان فارسی بنویسید.
۳. این تمرین در محیط لینوکس باید انجام شود.
٤. لطفاً کپی نکنید!
٥. از فایل راهنمایی که کنار تمرین قرار گرفته کمک بگیرید.
٦. برای قسمت هایی که با علامت " * " مشخص شده اند تصویر اجرای تمرین را نیز در فایل جواب خود ضمیمه کنید.
۷. جواب را به صورت فایل PDF و با شماره دانشجویی خودتان تحویل دهید.(مثلا ۹۳۳۳۳۳۳۳.pdf)
۸. تمام فایل های خواسته شده را در کنار فایل جواب قرار داده و همه را در قالب فایلی به نام شماره دانشجویی خودتان فشرده کنید.(مثلا ۹۳۳۳۳۳۳۳.zip)
۹. در صورت برخورد با هرگونه مشکل در حل تمرین به karimy.f۹۲@gmail.com پیام بدهید.

در این آزمایش می‌خواهیم در محیط ترمینال با نرم‌افزار wireshark آشنا شویم. این نرم‌افزار تحلیلگر پروتکل های شبکه است و این امکان را به شما می‌دهد تا بسته های مبادله شده از کارت شبکه تان را مشاهده کنید. این نرم‌افزار به صورت رایگان و open source در دسترس است و می‌توانید آخرین نسخه آن را برای پلتفرم های گوناگون از سایت www.wireshark.com دانلود کنید. این نرم‌افزار به صورت پیش‌فرض روی Linux Kali نصب است.
برای این آزمایش تنها tshark (که یکی از مهمترین اجزای wireshark است) کافی است.
Tshark را روی سیستم خود نصب کنید.
برای این کار از دستور زیر استفاده کنید:

```
sudo apt-get install tshark
```

پس از نصب آن اگر می‌خواهید بدون نیاز به دسترسی root بسته ها را رصد کنید می‌توانید تنظیمات wireshark را تغییر دهید. برای این کار از دستور زیر استفاده کنید.

```
sudo dpkg-reconfigure wireshark-common
```

و سپس گزینه yes را انتخاب کنید. با این کار شما اجازه دسترسی را، به سایر کاربرانی که سطح دسترسی ادمین ندارند، به wireshark می دهید. برای اطمینان کاربر خودتان را به گروه wireshark اضافه کنید:

```
sudo adduser $USER wireshark
```

به یک اکسس پوینت اتصال بیسیم برقرار کنید.
۱. مشخصات کارت شبکه خود را بنویسید: (برای این کار می‌توانید از دستور زیر استفاده کنید)*

```
lspci | egrep -i 'wireless|wlan|wifi'
```

می‌توانید اطلاعات کارت شبکه خود را با دستور زیر ببینید:*

```
lspci -vv -s xx:xx.x
```

به جای xx:xx.x شناسه کارت خود را قرار دهید.

۲. مقدار rssi به چه معناست و چه چیزی را نشان می دهد؟ رابطه ی آن با snr و مقدار نویز چیست؟

۳. با استفاده از دستور iwconfig اطلاعات واسط شبکه ی خود را ببینید*
از چه پروتکلی استفاده می کند؟
روی کدام باند؟
نرخ بیت چقدر است؟
مقدار rssi چقدر است؟

مکان خود را جابجا کرده و دوباره دستور ۳ را اجرا کنید.
چه تغییراتی می بینید؟
(برای بهتر دیدن تغییرات از این دستور می توانید استفاده کنید: watch -n۱ iwconfig <interface>)

٤. از سایت دلخواهی بازدید کرده و با استفاده از tshark به تعداد ۵۰۰ بسته را ذخیره کنید.*
راهنمایی:

```
tshark -i <interface> -c ۵۰۰ -w packets.pcap
```

۵. فیلترهای زیر را روی فایل packets.pcap اعمال کنید و در فایل های خواسته شده ذخیره کنید.
الف) بسته های http (در فایل httpPackets.pcap)*
ب) بسته هایی که از اکسس پوینت ارسال شده اند و مقصدشان شما نبوده اید(در فایل ap.pcap)
راهنمایی: (از فیلد های ip.src و ip.dst استفاده کنید)*

٦. بسته های پروتکل ۸۰۲,۱۱ سه دسته ی اصلی دارند. آنها را نوشته و هرکدام را در دو سطر توضیح دهید.
هر کدام به زیر دسته هایی تقسیم می شوند . سه تا از زیر دسته های هر کدام را نام ببرید.

۷. فایل capturedPackets.pcap در کنار تمرین شما قرار گرفته است.
موارد خواسته شده را روی آن اجرا کنید:

الف) بسته های ack را در فایلی به نام ackPackets.pcap ذخیره کنید.*
ب) بسته های beacon چیست؟ بسته های beacon را در فایلی به نام beaconPackets.pcap ذخیره کنید.*
ج) بسته های data را در فایلی به نام dataPackets.pcap ذخیره کنید.*
د) بسته های rts و cts را در فایلی به نام rts_ctsPackets.pcap ذخیره کنید.*

۸. قسمت های ب و د را روی فایل packets.pcap (که در سوال ٤ ایجاد کردید) اجرا کنید.*
آیا می توانید بسته های مورد نظرتان را پیدا کنید؟ علت چیست؟ کامل توضیح دهید.

۹. مود های monitor و promiscuous چیست؟

۱۰. حال با توجه به آنچه از سوال ۹ متوجه شدید (!) سوال ٤ را به گونه ای تغییر دهید که بتوانید بسته های beacon و rts و cts را در آن ببینید . در فایلی به نام packets۲.pcap ذخیره کنید. و قسمت های ب و د سوال ۷ را روی آن تکرار کنید. (نتیجه را در فایلهای beaconPackets۲.pcap و rts_ctsPackets۲.pcap ذخیره کنید)

۱۱. دستور زیر را روی capturedPackets.pcap اعمال کنید و بگویید دقیقاً چه کاری انجام می دهد و هر فیلد چه چیزی را نمایش می دهد.*

```
tshark -r capturedPackets.pcap -T fields -e frame.number -e wlan_mgt.ssid -e
wlan_radio.signal_dbm
```

۱۲. تفاوت فیلتر display و capture چیست؟ لطفا کامل توضیح دهید. آیا می توان یک فیلتر capture روی فایل های pcap. اعمال کرد؟یک فیلتر display چطور؟
از سیستم خود یک سیستم دیگر که در شبکه ی خودتان است را ping کنید. برای پیدا کردن بسته هایی که مبدأشان شما و مقصدشان آن سیستم است و از پروتکل icmp استفاده کرده اند، یک فیلتر display و یک فیلتر capture بنویسید.

موفق باشید