

wireshark

Introduction and exercise

PRACTICAL HOMEWORK

Prepared For :

Network course at Isfahan university of
technology

Dr . Ali Fanian

Zahra Sarami - Ali Dakik

Deadline:

sunday 28th Ordibehesht



مقدمه :

هدف از این تکلیف آشنایی با نرم افزار وایرشارک و بررسی پروتکل ها در لایه های مختلف معماری TCP/IP است.

نرم افزار وایرشارک (wireshark) یک نرم افزار کنترل ترافیک شبکه است که در حوزه های مختلفی مثل امنیت و شبکه کاربرد دارد. وایرشارک برای موارد مختلفی مثل آموزش شبکه، تجزیه و تحلیل، توسعه پروتکل ارتباطی و عیب یابی شبکه استفاده می شود.

استفاده از این نرم افزار به شما این امکان را می دهد که بتوانید تمام ترافیک های سیستم خود، ورودی و خروجی را در هر زمان که قصد دارید ثبت و ضبط نمایید و در زمان مناسب به تحلیل آن ها بپردازید.

وایرشارک روی پلتفرم های مختلفی از جمله windows، linux، xos و unix اجرا می شود. این نرم افزار به صورت متن باز و رایگان در دسترس است.

نصب :

نصب در ویندوز

فایل آن را از اینجا [دانلود](#) و نصب کنید.

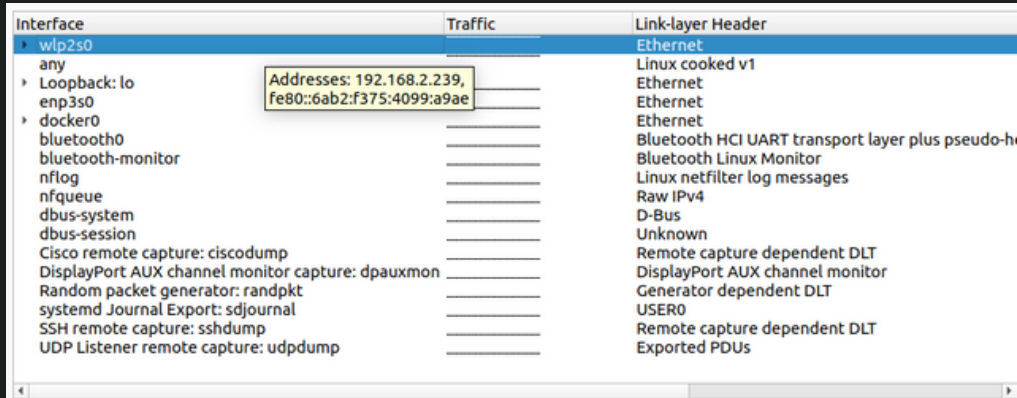
نصب در اوبونتو

```
sudo apt-get install wireshark  
sudo dpkg-reconfigure wireshark-common  
sudo wireshark
```

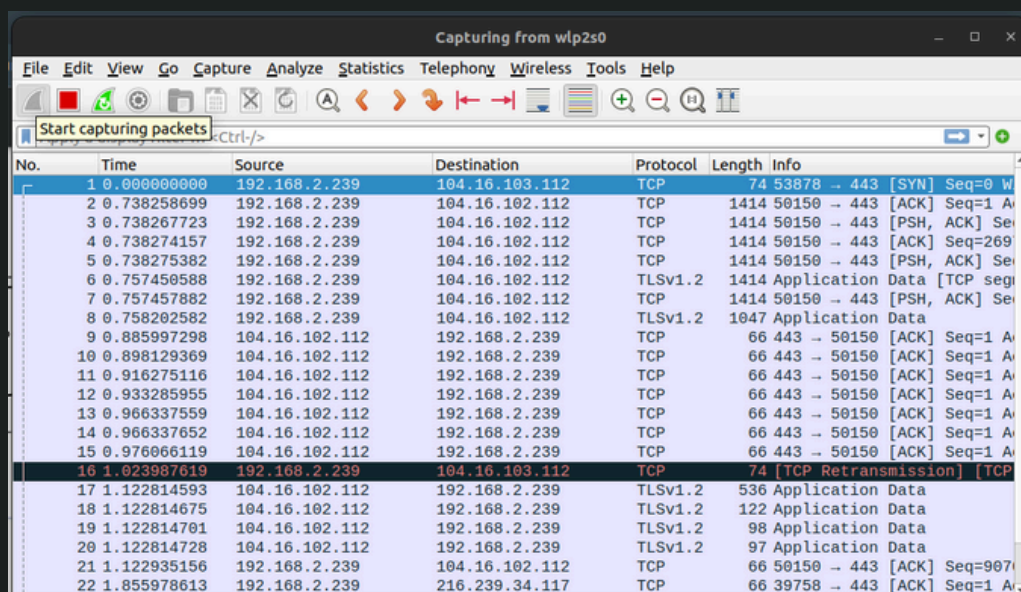


شروع به کار :

ابتدا باید اینترفیسی که آن را می‌خواهید شنود کنید انتخاب کنید:



شروع شنود :



در هر زمان که خواستید با کلید CTRL+E یادکمه قرمز رنگ شنود را متوقف کنید .

در منوی VIEW -> COLORING RULES می‌توانید معانی رنگ های پکت های دریافتی را مشاهده کنید .



No.	Time	Source	Destination	Protocol	Length	Info
141	8.427841779	192.168.2.239	185.73.202.4	TCP	1454	37432 → 443 [ACK] Seq=...
142	8.427842886	192.168.2.239	185.73.202.4	TLSv1.3	1416	Application Data
143	8.427864337	192.168.2.239	185.73.202.4	TCP	1454	37432 → 443 [ACK] Seq=...
144	8.427865824	192.168.2.239	185.73.202.4	TCP	1454	37432 → 443 [ACK] Seq=...
145	8.427867116	192.168.2.239	185.73.202.4	TLSv1.3	1454	Application Data
146	8.427868115	192.168.2.239	185.73.202.4	TCP	1454	37432 → 443 [ACK] Seq=...
147	8.427869368	192.168.2.239	185.73.202.4	TCP	1454	37432 → 443 [PSH, ACK] Seq=...
148	8.429128895	192.168.2.239	185.73.202.4	TLSv1.3	185	Application Data
149	8.466696665	185.73.202.4	192.168.2.239	TCP	66	443 → 37432 [ACK] Seq=...
150	8.468634388	185.73.202.4	192.168.2.239	TCP	66	443 → 37432 [ACK] Seq=...
151	8.478013965	185.73.202.4	192.168.2.239	TCP	66	443 → 37432 [ACK] Seq=...
152	8.475854699	185.73.202.4	192.168.2.239	TCP	66	443 → 37432 [ACK] Seq=...
153	8.475854837	185.73.202.4	192.168.2.239	TCP	66	443 → 37432 [ACK] Seq=...
154	8.489677725	185.73.202.4	192.168.2.239	TCP	66	443 → 37432 [ACK] Seq=...
155	8.483512959	185.73.202.4	192.168.2.239	TCP	66	443 → 37432 [ACK] Seq=...
156	8.484531177	185.73.202.4	192.168.2.239	TCP	66	443 → 37432 [ACK] Seq=...
157	8.486841153	192.168.2.239	192.168.2.239	TCP	66	443 → 37432 [ACK] Seq=...
158	8.521768337	185.73.202.4	192.168.2.239	TLSv1.2	172	Application Data
159	8.526098083	185.73.202.4	192.168.2.239	TLSv1.2	778	Application Data
160	8.526239933	192.168.2.239	185.73.202.4	TCP	66	59608 → 443 [ACK] Seq=...
161	8.526706479	192.168.2.239	185.73.202.4	TLSv1.2	192	Application Data
162	8.572286856	185.73.202.4	192.168.2.239	TCP	66	443 → 59608 [ACK] Seq=...

- همانطور که در تصویر بالا می بینید، این پنجره به ۳ بخش اصلی تقسیم شده است:
- **بخش اول (بالاترین بخش):** در این قسمت Packet هایی که Capture می شوند، نمایش داده می شوند.
 - **بخش دوم (قسمت وسط):** با کلیک بر روی هر Packet در بخش اول، جزئیات مربوط به آن، به تفکیک Header در این قسمت نمایش داده می شود.
 - **بخش سوم (قسمت پایین):** در این قسمت نیز اطلاعات مربوط به Packet ای که در بخش اول انتخاب کردیم نمایش داده می شود البته به صورت Hexadecimal و کد ASCII.

در اینجا برخی از جزئیات در مورد هر ستون در صفحه بالا آمده است:

- **شماره یا No:** این ترتیب شماره بسته ای است که ضبط شده است. براکت نشان می دهد که این بسته بخشی از یک مکالمه است.
- **زمان Time:** این ستون به شما نشان می دهد که چه مدت پس از شروع ضبط، این بسته ضبط شده است. اگر نیاز به نمایش چیز دیگری دارید، می توانید این مقدار را در منوی تنظیمات تغییر دهید.
- **منبع Source:** این آدرس سیستمی است که بسته را ارسال کرده است.
- **مقصد Destination:** این آدرس مقصد آن بسته است.
- **پروتکل Protocol:** این نوع بسته است، به عنوان مثال، TCP، DNS، DHCPv6، یا ARP.
- **Length:** این ستون طول بسته را برحسب بایت به شما نشان می دهد.
- **اطلاعات Info:** این ستون اطلاعات بیشتری در مورد محتویات بسته به شما نشان می دهد و بسته به نوع بسته آن متفاوت خواهد بود.



بعد از توقف ضبط بسته، میتوانید از فیلترهای نمایشگر برای محدود کردن بسته‌ها در فهرست بسته‌ها استفاده کنید .
مثال:

`ip.src==IP-address and ip.dst==IP-address`

این فیلتر بسته‌هایی را از یک کامپیوتر (ip.src) به کامپیوتر دیگر (ip.dst) به شما نشان می‌دهد.

`tcp.port eq 25`

این فیلتر تمام ترافیک پورت 25 را به شما نشان می‌دهد که معمولاً ترافیک SMTP است.

`icmp`

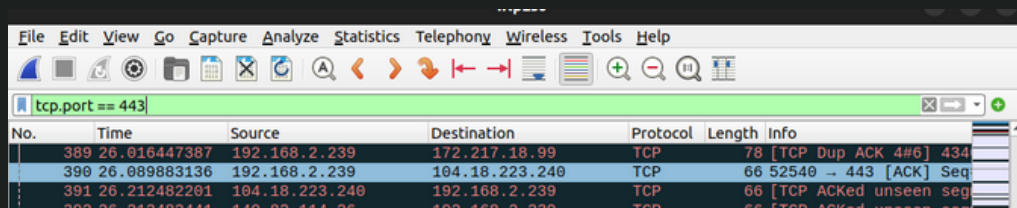
این فیلتر فقط ترافیک ICMP را در ضبط به شما نشان می‌دهد، به احتمال زیاد آن‌ها پینگ هستند.

`ip.addr!= IP_addres`

این فیلتر تمام ترافیک به‌جز ترافیک به یا از کامپیوتر مشخص‌شده را به شما نشان می‌دهد.

`ls_ads.opnum==0x09`

تحلیلگران حتی فیلترهایی برای شناسایی حملات خاص می‌سازند، مانند فیلتر بالا که برای شناسایی کرم Sasser ساخته شده



No.	Time	Source	Destination	Protocol	Length	Info
389	26.016447387	192.168.2.239	172.217.18.99	TCP	78	[TCP Dup ACK 4#6] 434
390	26.089883136	192.168.2.239	104.18.223.240	TCP	66	52540 → 443 [ACK] Seq
391	26.212482201	104.18.223.240	192.168.2.239	TCP	66	[TCP ACKed unseen seq
392	26.212482441	140.82.114.26	192.168.2.239	TCP	66	[TCP ACKed unseen seq

محل وارد کردن فیلتر



سوالات :

شروع به شنود بسته ها کنید. به اینترنت وارد شوید و چند دقیقه وب گردی کنید سپس به وایرشارک برگشته و شنود را متوقف کنید .

سوال یک

چه پروتکل هایی بیشتر مورد استفاده قرار گرفته است ؟ آنها را بنویسید .

سوال دو

یک بسته را به دلخواه انتخاب کنید و مشخص کنید به ترتیب چه پروتکل هایی در لایه های مختلف آن استفاده شده است؟
ترتیب قرارگیری بیت ها داخل بسته چه ارتباطی با لایه های مختلف دارد ؟
اندازه فریم لایه دو آن چقدر است ؟
اندازه بسته لایه ۳ آن چقدر است؟

سوال سه

آیا میتوانید بسته هایی را پیدا کنید که فاقد پروتکل های لایه , APPLICATION TRANSPORT یا NETWORK باشد؟
این بسته ها از چه پروتکلی استفاده کرده اند؟

سوال چهار

از یکی از بسته ها بخش مربوط به پروتکل tcp و udp را پیدا کنید . عدد مربوط به پورت مبدا و مقصد را یادداشت کنید
CHECKSUM مربوط به پروتکل های tcp و udp را در آن مشخص کنید.

سوال پنج

به سایت دانشگاه وصل شده و مراحل ارتباط tcp آن را دنبال و شنود کنید .
با نوشتن پارامتر های , syn, synack,seq number,ack number>window size , flags توضیح دهید که در هر مرحله چه بسته هایی با چه محتوایی ارسال و دریافت میشوند .

شامل مراحل handshake , connection closer , connection duration

سوال شش

در cmd یا ترمینال سیستم خود آدرس سایت دانشگاه و yahoo.com را پینگ بگیرید و با استفاده از وایرشارک response time آن را بدست آورید .
همچنین نشان دهید که از چه پروتکل هایی در یک dns query استفاده میشود .
جهت درک بهتر سوال میتوانید این-ویدیو را مشاهده کنید.



بخش امتیازی :

یک tcp stream را دنبال کنید و داده هایی (tcp content) که بین کلاینت و سرور در این کانکشن تبادل میشود را متوالیا نشان دهید .
از مراحل انجام این قسمت اسکرین شات قرار داده شود.

نکات پایانی:

مهلت تحویل :

شما تا پایان مهلت ددلاین فرصت دارید تکلیف را انجام داده و به صورت یک داکيومنت (pdf) در سامانه ی یکتا در ماژول مربوطه بارگزاری کنید .
دقت شود که باید از همه ی مراحل مورد نیاز در جواب سوالات اسکرین شات قرار داده شود و در صورت نیاز، توضیح هر تصویر در زیر آن درج گردد .

راه های ارتباطی :

Telegram : @zhra_sarami

Telegram : @X_AFDK_X

