به نام خدا

آزمایشگاه شبکه و امنیت

تجزیه و تحلیل بسته ها

آشنایی با نرم‌افزار Wireshark

و پروتکل های HTTP,DNS

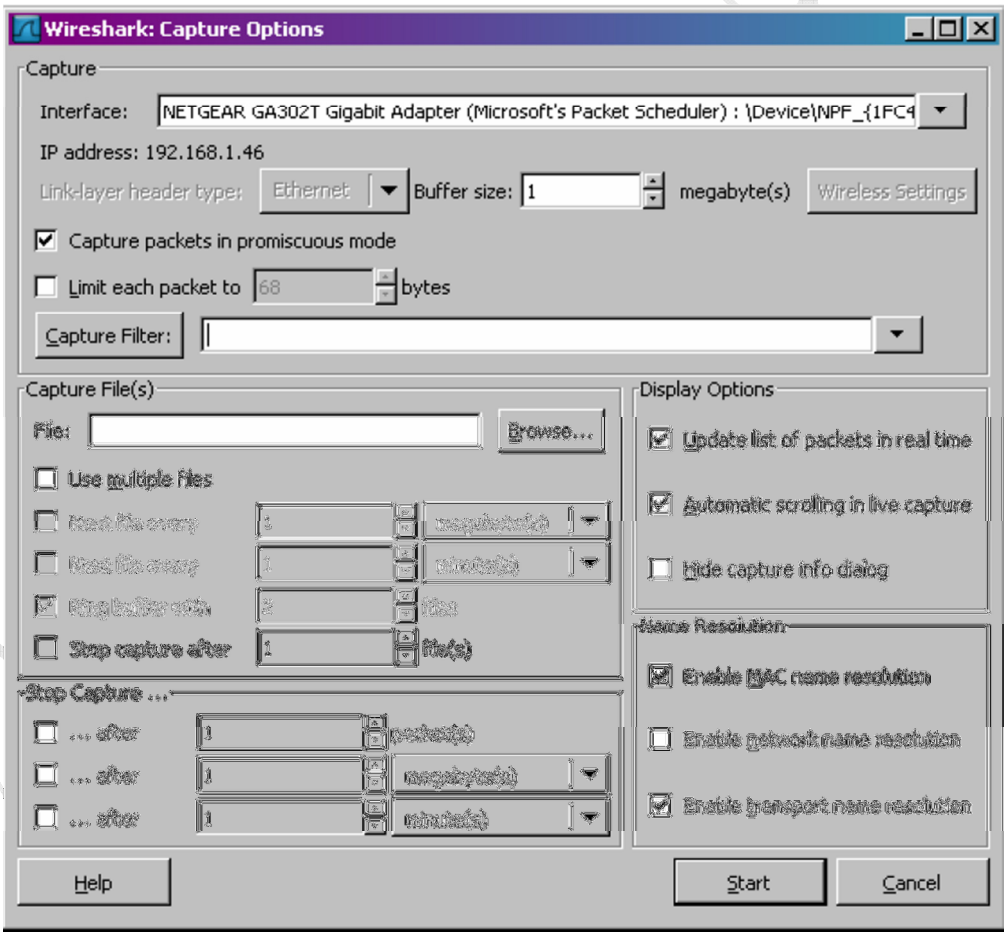
دکتر علی فانیان، مهندس تهمینه شبانیان

1- آشنایی با wireshark

➢ آزمایش 1-1-1: گرفتن بسته های پیام

یکی از کارهای اساسی Wireshark توانائی آن در دریافت کلیه بسته‌هایی است که بر روی شبکه LAN شما مبادله می‌شوند. در این قسمت به صورت مقدماتی سعی می‌کنیم تا تعدادی بسته پیام را از روی شبکه جمع‌آوری کنیم.

- ابتدا یک مرورگر دلخواه باز کنید.
- نرم افزار Wireshark را باز کنید، پنجره ای مشابه با شکل 1 خواهید دید.
- از command menus منوی capture را باز کرده وروی option کلیک کنید. پنجره ای مشابه شکل 5 باز خواهد شد.

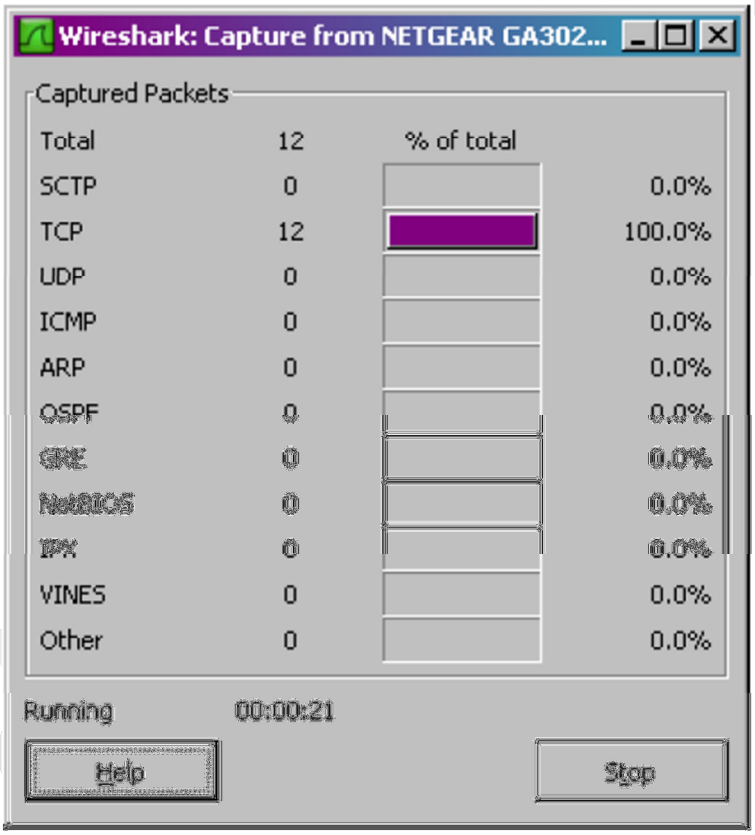


شکل 5: Wireshark Capture Options Window

⇦ از بیشتر مقادیر پیش فرض در این پنجره می توان استفاده نمود، گزینه "Hide capture info dialog" که در قسمت Display Options قرار دارد را غیر فعال نمایید.

در قسمت interface رابط شبکه خود را انتخاب کرده، اگر کامپیوتر شما بیش از یک رابط دارد، باید رابطی را انتخاب نمایید که برای ارسال و دریافت اطلاعات مورد استفاده قرار می گیرد. بر روی start کلیک نمایید.

⇦ پس از شروع جمع آوری بسته ها پنجره ی packet capture summary ظاهر می شود (شکل6). این پنجره آمارهایی از تعداد بسته های مختلف را نشان می دهد. در این پنجره دکمهstop وجود دارد، که در صورت کلیک برروی آن عملیات جمع آوری متوقف می شود. در حال حاضر نیازی به متوقف کردن عملیات نیست.



شکل6: Wireshark Packet Capture Window

⇦ در حالی که Wireshark در حال اجرا است، آدرس زیر را درمرورگر وارد نمایید.

http://IUT.AC.IR

پس از نمایش این صفحه در مرورگر، مرورگر شما به سرور HTTP در IUT.AC.IRوصل شده و با سرور پیام هایhttp مبادله کرده تا این صفحه بار گذاری شود.

⇦ پس از نمایش وب سایت دانشگاه در صفحه مرورگر wireshark را متوقف کرده (با استفاده از دکمه stop در Wireshark capture window)

این کار باعث می شود پنجره Wireshark capture ناپدید شده و پنجره اصلی تمام بسته های جمع آوری شده را نمایش دهد. حال شما داده های بسته های زنده ای را دارید که، شامل تمام پیام های مبادله شده توسط پروتکل های مختلفِ کامپیوتر شما و نهادهای دیگر شبکه است. پیام http مبادله شده با سرورIUT.AC.IR درجایی از لیست بسته های جمع شده وجود دارد.

- به سوالات زیر پاسخ دهید:

1. پروتکل های مختلفی را که در ستون protocol در پنجره ی packet-listing ظاهر شدند را فهرست نمایید.
2. از زمان ارسال HTTP GET تا زمان دریافت HTTP OK چقدر طول کشیده است؟ (به صورت پیش فرض، مقدار موجود در ستون Time در پنجره packet-listing زمان را بر حسب ثانیه، از شروع جمع آوری نشان می دهد. برای نمایش زمان به صورت Time-of-day در منویview گزینه Time-of-day را درقسمت Time DisplayFormat انتخاب نمایید.)
3. درخواست خروجی از سیستم شما به چه آدرسی رفته است؟ این آدرس متعلق به کجاست؟چرا؟توضیح دهید.

➢ آزمایش 2-1-1:پروتکل HTTP

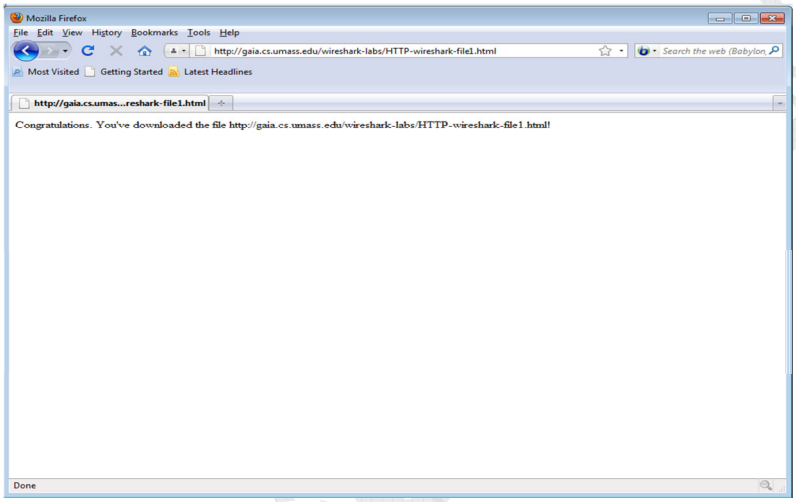
- مرورگر را باز کنید.
- wireshark را باز و در قسمت filter، http را تایپ نمایید در این حالت فقط پیام های http نمایش داده خواهد شد.

✓ در صورتی که نیاز به محدود کردن اطلاعات نمایش داده شده در پنجره packet-listing و یا نمایش اطلاعات خاص مد نظرباشد، می توان از این ویژگی Filtering استفاده کرد.

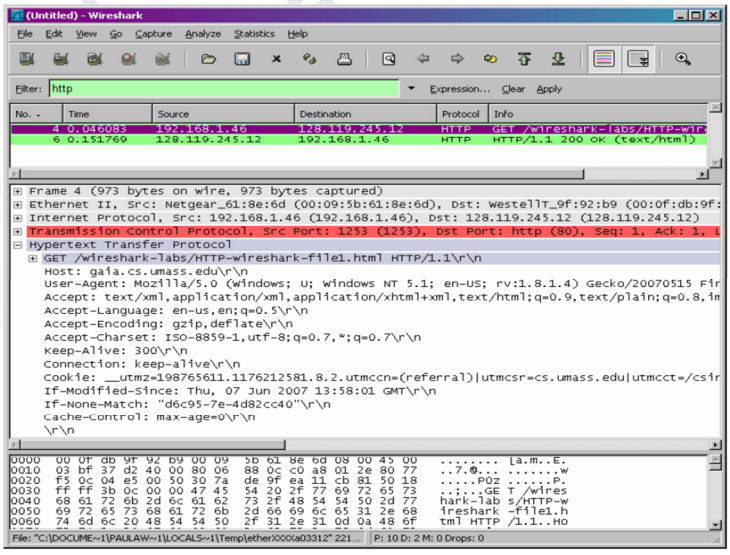
- لینک زیر را در مرورگر وارد نمایید.

http:// آدرس سرور موجود در آزمایشگاه/2/az2/2.htm

- مرورگر یک فایل http ساده و یک خطی را نمایش خواهد داد. (شکل 1)
- wireshark را متوقف نمایید.



شکل 1



شکل 2

در شکل2 در قسمت packet-listing دو پیام http نشان داده شده است: GET message (از مرورگر به سرور) و پیام پاسخ از سرور به مرورگر. پنجره packet-content جزییات پیام انتخاب شده را نشان می دهد. (در این شکل پیام HTTP GET انتخاب شده است).

با انتخاب HTTP GET، اطلاعات Ethernet fram، IP datagram، TCP segment و HTTP message header در قسمت packet-header نمایش داده می شوند. با کلیک روی علامت + در کنار Transfer ProtocolHyper terxt جزییات بیشتری را درباره http مشاهده نمایید و با کلیک بر روی علامت - در سمت چپ پنجره packet details جزییات مربوط به دیگر قسمت ها را کاهش دهید.

- **توجه:** تمام پیام های دریافت شده و فرستاده شده http مربوط به favicon.icon را نادیده بگیرید. اگر ارجاعی به این فایل دیدید، توسط مرورگر شما به طور اتوماتیک فرستاده شده است که از سرور درخواست فایل آیکون کوچک را دارد تا آن را در کنار URL نشان دهد. ما این فایل های مزاحم را نادیده می گیریم)

با توجه به اطلاعات موجود به سوالات زیر پاسخ دهید:

1. مرورگر شما کدام نسخه (version) http را اجرا میکند1.0 یا 1.1؟ نسخه http سرور چیست؟تفاوت این دونسخه در چیست؟
2. چه زبان هایی را مرورگر شما میتواند از سمت سرور قبول کند؟
3. آدرس IP کامپیوتر شما و سرور چیست؟
4. از کدام پروتکل لایه انتقال استفاده می‌شود؟
5. پورت مبدا و مقصد را مشخص کنید.
6. کد وضعیت[1] که از سرور به مرورگر شما برگشته چیست؟این کد بیان کننده چیست؟

➢ آزمایش 1-3: ردیابی DNS توسط wirshark

1. با استفاده از ipconfig /flushdns کش میزبان خود را خالی نمایید.

[1] status code

2. مروگر دلخواه را باز و کش آن را نیز پاک کنید.

3. wireshark را باز و "ip.addr == your_IP_address" را در فیلد فیلتر وارد نمایید.

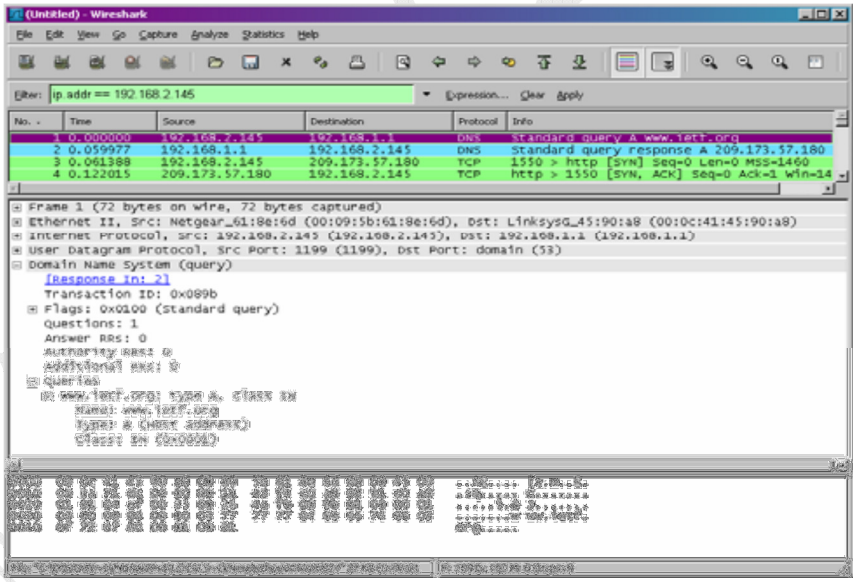
4. با استفاده از ipconfig آدرس IP خود را به دست می آورید. (آدرس IP کامپیوتری که wireshark بر روی آن اجرا می شود.) این فیلتر تمام بسته هایی را که مبدا و مقصدشان host شما نیست را، حذف می کند.

5. جمع آوری بسته ها در wireshark را شروع نمایید.

6. آدرس زیر را در مرورگر وارد نمایید.

http://netlab.iut.ac.ir

7. wireshark را متوقف نمایید.(شکل 3)



به سوالات زیر پاسخ دهید:

1. آدرس فرستنده DNS query و آدرس پیام های پاسخ[2] را بیابید. به وسیله UDP فرستاده شده اند یا TCP؟
2. پورت مقصدِ پیام DNS query و پورت مبدا پیام DNS response را مشخص نمایید؟ این شماره پورت مربوط به چه سرویسی است؟
3. پیام DNS query به کدام آدرس IP فرستاده شده است؟ با استفاده از دستور ipconfig/all نیز، آدرس سرور نام خود را بررسی نمایید. آیا هر دو آدرس یکسان هستند؟
4. پیام DNS query را بررسی و نوع آن را مشخص نمایید.آیا این پیام حاوی جواب[3] هست؟(منظور از نوع type درخواست میباشد)
5. پیام DNS response را بررسی نمایید. چه تعداد جواب ارائه شده است؟ محتوای هر یک از این جواب ها چیست؟
6. بسته TCP SYN فرستاده شده توسط میزبان خود را در نظر بگیرید. آیا آدرس IP مقصد بسته SYN با هر یک از درس های IP ارائه شده در پیام DNS response مطابقت دارند؟
7. صفحه وب شامل تصاویری بود. آیا قبل از بازیابی هر تصویر، میزبان شما DNS queries جدیدی فرستاده است؟

➢ 3-1-1: ردیابی بسته های ICMP

1. ابتدا با مراجعه به منوی Capture → Interfaces لیستی از واسط‌های شبکه در دسترس را مشاهده نمایید. سپس کلید Capture را برای واسط مورد نظر فشار دهید.
2. Wireshark را اجرا کنید.
3. دستور ping را در محیط Windows اجرا کنید و نتیجه اجرا را مشاهده کنید.

Ping 172.16.1.1

4. نتایج به دست آمده را تحلیل کنید. (بررسی کنید در زمان اجرای این دستور چه پروتکلی فعال میشود)

[2] response messages
[3] answer

5. با استفاده از گزینه ... Save as از منوی File بسته‌های دریافت شده را تحت نام "MyOwnCapture" ذخیره کنید.

6. حال در لیست همه بسته‌های از نوع ICMP را مشخص نموده و سعی کنید تا با گزینه ... Save as این بسته‌ها را در فایلی تحت نام "MyOwnICMP" ذخیره کنید.

➢ آزمایش 4-1-1: خواندن یک فایل از پیش تهیه شده

⇦ پس از اجرای نرم‌افزار، با استفاده از منوی File → Open فایل "SimpleCaptured" را از مسیر مناسب آن انتخاب و باز نمایید. اطلاعاتی مشابه آنچه در شکل2 نشان داده شده است، بر روی صفحه دیده خواهد شد

❶- ابتدا، لیست بسته‌ها را به ترتیب صعودی شماره مرتب کنید.

(چنانچه ترتیب آنها نزولی بود با کلیک بر روی فیلدnumber، ترتیب را صعودی کنید)

اولین بسته TCP درلیست را انتخاب کنید و در قسمت packet details بخش‌های مختلف Header را در آن تشخیص دهید. دراین بسته، پرچم‌های TCP(مربوط به Three way handshake) چه وضعیتی دارند و این به چه معنی است؟

❷- با مشاهده دومین بسته از نوع TCP، اطلاعات زیر را استخراج نمایید:

- **الف:** اندازه پنجره گیرنده(اندازه پنجره گیرنده نشاندهنده چیست؟)
- **ب:** وضعیت بیت‌های پرچم TCP (مربوط به Three way handshake)
- **پ:** شماره پورت Source و Destination

❸- با مشاهده اطلاعات بسته‌های از نوع DNS در قسمت packet details مشخص کنیدکه DNS از UDP استفاده می‌کند یا از TCP؟

- **الف:** با مشاهده اطلاعات بسته‌های DNS مشخص کنید که با تبادل این بسته‌ها، چه آدرسی باید تبدیل می‌شده است و نتیجه تبدیل را به دست آورید.(برای این منظور بسته های DNS quaryو DNS response را بررسی کرده و آدرس درخواست شده و جواب دریافت شده را مشاهده نمایید)