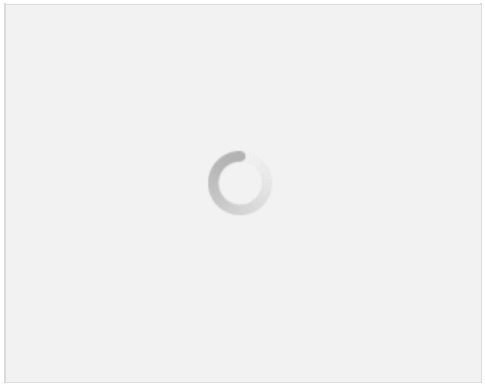
آموزش وایرشارک (Wireshark) کنترل ترافیک شبکه قسمت ۷ (نسخه PDF)

آموزش وایرشارک (Wireshark) کنترل ترافیک شبکه قسمت ۷ (نسخه چاپی)

خب دوستان پایه این جلسه رو گذاشتیم بر ادامه جلسه قبلی جلسه قبلی اومدیم لایه چهارم رو از این پروتکل بررسی کردیم و امروز میخواییم به لایه های زیرین بپردازیم.من دیه این جلسه مقدمه ندارم سریع میرم سر اصل مطلب کسانی که میخوان بدونن جریان چیه جلسات قبل رو کامل بخونن.



```
Ethernet II, Src: Giga-Byt_70:12:9e (00:1d:7d:70:12:9e), Dst: Tp-LinkT_b7:c5:5a (d8:5d:4c:b7:c5:5a)
```

خب دوستان این لایه سوم هستش بازش کنم ببینید برق از سرتون میپره که این نرم افزار داره چی نشون میده خب لایه رو باز میکنم .خود لایه سوم ۳ تا زیر لایه داره یعنی هدر داره هدر اول:

```
Destination: Tp-LinkT_b7:c5:5a (d8:5d:4c:b7:c5:5a)
```

میگه که دیستنیشن ادرس شما یعنی مک ادرس شما که به سمت سرور درخواست ارسال کردین اینه و این مک ادرس از یه مودم tp-link با این ادرس ارسال شده که اگه شما بخواید ریز مدل رو بدونید فقط کافیه اطلاعات رو تو گوگل بریزید تا ببینید چی بهتون میده.همونطوری که مشاهده میکنید خود این لایه رو که باز میکنم یه سری هدر دیگه به من میده بریم بررسی کنیم

```
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
```

همونطوری که ملاحضه میکنید میگه ادرسی که ارسال شده یه ادرس فیزیکی معتبرمیتونه باشه که از طرف کارخانه سازنده بر روی دستگاه ست شده یا یک ادرس فیزیکی که معتبر نیست(من اینو فهمیدم شما چیز دیگه ای فک میکنید تو قسمت نظرات بگید) یه لایه برمیگردیم عقب این هدر رو چک میکنیم

```
Source: Giga-Byt_70:12:9e (00:1d:7d:70:12:9e)
```

میگه مک ادرس ای پی که شما پینگ گرفتی یا همون ای پی مقصد این هستش و یه مدلدستگاه رو نشون داده حالا همینو باز میکنم ببینم چیزی دستگیرم میشه یا نه

```
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
```

همونطوری که ملاحضه میکنید میگه ادرسی که ارسال شده یه ادرس فیزیکی معتبرمیتونه باشه که از طرف کارخانه سازنده بر روی دستگاه ست شده یا یک ادرس فیزیکی که معتبر نیست(من اینو فهمیدم شما چیز دیگه ای فک میکنید تو قسمت نظرات بگید) اما یه هدر دیگه هم هست که اینه:

```
Type: IPv4 (0x0800)
```

میگه که ای پی مقصد شما یا همون ای پی که پینگ گرفتی یه ای پی ورژن ۴ هستش.خب این لایه سوم هم کارش تموم شد برمیگردیم به عقب و لایه ۲ رو باز میکنیم که میشه اینی که میبینید:

```
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 8.8.8.8
```

این لایه کلا ip ما رو مورد بررسی قرار داده و میخواد بسته ip رو که تو osi میشه network و درون لایه neywork ای پی ادرس قرار میگیره رو با ریز جزئیات مخصوص این عملایتی که انجام شده به ما نشون بده.خود لایه به ما میگه ادرس منبع یا سورس ادرس ۱۹۲.۱۶۸.۱.۱۰۰ هستش و ادرس مقصد یا دستینیشن ادرس ۸.۸.۸.۸ هستش و ورژن ای پی ۴ **خب بازش میکنیم:**

```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
```

ای پی ورژن ۴ و اندازه این هدر ۲۰ بایت هستش.

```
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
```

میگه چه سرویس های همراه این بسته عبور کردن که تو این عملیات هیچی نشون نمیده ممکنه شما یه ادرس اینترنتی رو با نرم افزار چک کنین یعنی یه بسته http که اینجا سرویس ها رو هم بهتون نشون بده.پس دیه داخلشو توضیح نمیدم برمیگردم به عقب و لایه بعدی رو بررسی میکنم.

```
Total Length: 60
Identification: 0x0eec (3820)
```

میگه که اندازه هدر ۶۰ بایته و یه پورت شناسای کردم رو این ادرس که ۳۸۲۰ هستش که مخصوص tcp/udp هستش. بریم سراغ بعدی

```
Flags: 0x00
```

فلگ های ارسالی برای برقراری ارتباط رو نشون داده که بررسی نمیکنیم

```
Fragment offset: 0
Time to live: 128
Protocol: ICMP (1)
```

خب این افست فریم رو به ما نشون داده که صفر هستش . میگه ttl=۱۲۸ شده برا این ادرس و پروتکلی که در اینجا بررسی شده icmp بودش

```
Header checksum: 0x0000 [validation disabled]
```

هدر هایی که همراه بسته ارسال میشه برا برقراری ارتباط

```
Source: 192.168.1.100
Destination: 8.8.8.8
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
```

ادرس منبع و مقصـد رو نشون داده و میگه نمیـدونم این دو تا سیسـتم ای پی ها رو از کـدوم منبع دریافت کردن.خب این هدر هم تموم میشه بریم سراغ بعدی.

```
Internet Control Message Protocol
```

خب میگه icmp یعنی پروتکل کنترل پیام اینترنت بازش میکنیم که هدر هاشو بررسی کنیم.

```
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4d5a [correct]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence number (BE): 1 (0x0001)
Sequence number (LE): 256 (0x0100)
[Response frame: 395]
```

میگه شما ۸ تا پیغام پینگ جمعا ارسال و دریافت کردین که کـدش ۰ بوده و شـناسه های ارسالی و دریافتی رو به صورت هگزا نشون داده که ترتیب شماره ها رو هم به صورت هگزا نمایش داده و شماره فریم واکنشی یا دریافتی ما ۳۹۵ بوده. بریم رو هدر data و هدر درونش:

```
Data (32 bytes)
Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
[Length: 32]
```

میگه که این اطلاعـات رو من از این داده ها به دست اوردم که ۳۲ بایت بود. خب دوسـتان من تو پینگی که گرفتم ۸ تا پروکل icmp رد و بدل شد که فقط اولین بسـته رو من اومدم باز کردم شما میتونید همشونو باز کنید و بررسی کنید.دوستان من یه برنامه اموزشی ریختم که پیاده کنم رو وب سایت حالا اگه شـد با فیلم اگه هم نشد مینویسم ولی درخواستی که از شـما دارم اینه که اموزش هایی که رو سایت قرار میدم با لایک کردن و نظر دادن منو حمایت کنید تا بتونم تمام برنامه اموزشی رو قرار بدم پاینده باشین.

نویسنده : مصطفی چگنی

منبع : جزیره امنیت اطلاعات و ارتباطات وب سایت توسینسو

Reza

اغا مرسي داری

فقط اگه از اون بر و بـچ پایه هستي که انتقاد رو دوس دارن بایـد بگم که اگه میشد کمي جزییات رو بیشتر و کامل تر بگي خیلي بهتر میشد

بازم بگم که این کار تو لایک داره،اونم نه یکي ،۴ -۵ تا با هم

مصطفی چگنی

فـدایی داری اقـا رضا خیلی ممنونم شـما لطف داری دیه این دوره اینطوری شـد اگه خـدا بخواد این دوره بشه پیش زمینه دوره های حرفه ای که دیه اونا با فیلم میاد رو سایت کع هم من سرعتر میگم هم شما همه جزئیات رو یاد میگیرید

مصطفی چگنی

فـدایی داری اقا رضا خیلی ممنونم شـما لطف داری دیه این دوره اینطوری شـد اگه خـدا بخواد این دوره تایید بشه پیش زمینه دوره های حرفه ای که دیه اونا با فیلم میاد رو سایت کع هم من سرعتر میگم هم شما همه جزئیات رو یاد میگیرید

حامد حق شناس

ممنون بابت آموزشتون ، خیلی کاربردی و فکر میکنم مورد نیاز همه بچه های شبکه کار ...

فکر میکنم منظور از

(Source: Giga-Byt_۷۰:۱۲:۹e ۰۰:۱d:۷d:۷۰:۱۲:۹e) آدرس فیزیکی کارت شبکه شما و

(Destination: Tp-LinkT_b۷:c۵:۵a d۸:۵d:۴c:b۷:c۵:۵a) آدرس فیزیکی مودم شـماست که در نود بعدی قرار گرفته و اطلاعات به سمت اون میره ...

حالا اگه من اشتباه میکنم لطفا توضیح بدید ...

مصطفی چگنی

اره همینه که شـما میگی اگه توجه کنی من یه پکت رو بررسـی کردم و پکـتی که از طرف سـرور دریـافت کردم پکت پـایینیشه که اونو نگفتم همش مث همه فقط اطلاعاتی که در اون هست مال سروره که پکت رو برا من ارسال کرده

fatemeh۲۰۲۰

سلام ممنون بابت مطالب خوب و مفیدتون

من خیلی از طرز بیان شما خوشم اومد اما راستش اصلا به این نرم افزار وارد نستم و خیلی گیج میشم

این نرم افزار هم برای درس شبکه نصب کردم که باید تمرینارو با این نرم افزار انجام بدم

میخاستم بگم اگه برای شما امکانش هست حداقل تو حل یه سوال بمن کمک کنید چون واقعا متوجه هیچی نمیشم

ممنون میشم اگه کمکم کنید

aboola aalivand

ممنون بابت آموزش عالی و دلچسبتون برادر

مصطفی چگنی

سلام داداش مرسی داری من یه مدت نبودم ایشا.. برمیگردم با قدرت زیاد و فدای مهربونیاتون

پژمان قاسمی

واقعا ممنون مهندس

ممنون که وقت میزارید

مطلب اصلی