دانشکده‌ی مهندسی کامپیوتر

آزمایشگاه شبکه

آشنایی پیشرفته با نرم‌افزار wireshark، نحوه‌ی تنظیم DNS Server

مدرس: مهدی جعفری

مقدمه

در جلسه‌ی قبل نحوه‌ی کارکرد نرم‌افزار wireshark و هم‌چنین کاربرد DNS را آموختیم. حال در این جلسه می‌خواهیم که بیش‌تر با آن‌ها آشنا شده و بتوانیم کارهای عملی‌تر با آن‌ها انجام دهیم.

۱ wireshark

با نرم‌افزار wireshark در جلسه‌ی قبل آشنا شدید. با استفاده از این نرم‌افزار می‌توانید ترافیک شبکه را تحلیل کنید. حال می‌خواهیم در این قسمت برخی از قابلیت‌های کاربردی این نرم‌افزار را به شما یاد دهیم.

۱.۱ به‌دست آوردن captcha

شما می‌توانید با این نرم‌افزار ترافیک گرفته شده را در فایلی با پسوند pcap. ذخیره کنید. این پسوند برای فایل‌هایی به‌کار می‌رود که ترافیک شبکه را ذخیره کرده‌اند. برای این قسمت سناریوی زیر را انجام دهید.

۱. فایل captcha.pcapng را در نرم‌افزار باز کنید.

۲. در این pcap سایت بانک ملت https://ebanking.bankmellat.ir/ebanking/ باز شده است. این سایت با استفاده از پروتکل TLS محتویات سایت را برمی‌گرداند. حال شما برای پیدا کردن محتویات داخل هر بسته که رمز شده است نیاز به کلید جلسه دارید که در فایل sslkeylog.log این کلید وجود دارد. از قسمت Edit > Preferences، به قسمت Protocols رفته و در قسمت SSL فایل sslkeylog.log را در قسمت log (Pre)-Master-Secret همانند شکل ۱ قرار دهید.

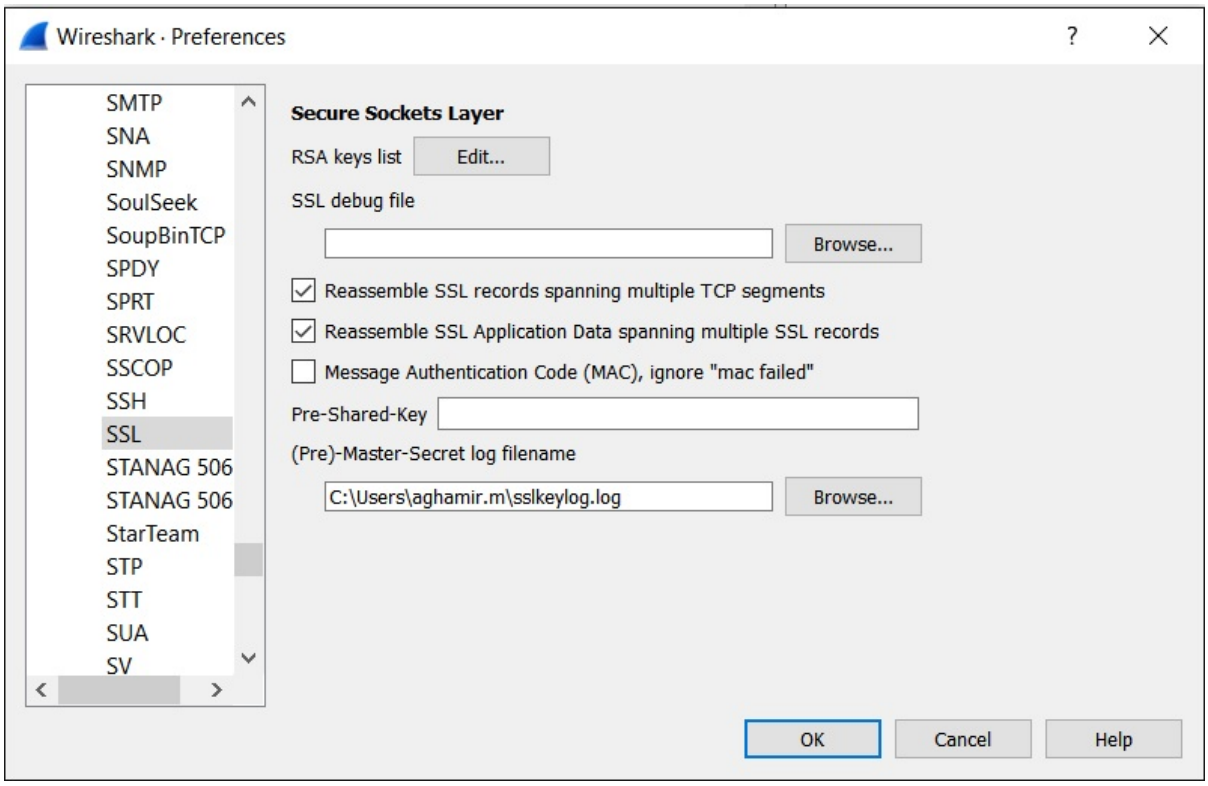
۳. در قسمت فیلتر عبارت http && ssl را بنویسید. با این کار آن بسته‌هایی که از طریق پروتکل TLS رد و بدل شده‌اند و همچنین توانستیم آن‌ها را رمزگشایی کنیم به‌دست خواهند آمد.

۴. با استفاده از File > Objects Export > HTTP تصویر داده شده در این ارتباط را ذخیره کرده و مقدار captcha داده شده از طرف بانک ملت به کاربر را گزارش کنید.

۲.۱ سوال‌ها

۱. تحقیق کنید ببینید که اطلاعات آماری بسته‌ها در نرم‌افزار wireshark به چه صورت به‌دست می‌آید و بگویید که این اطلاعات به ما چه کمک‌هایی می‌توانند بکنند. به‌طور مثال یکی از کمک‌های این اطلاعات آماری زمانی است که ما کلید جلسه بسته‌های رمز شده را نداشته باشیم. اگر خواستید می‌توانید در این زمینه بیش‌تر تحقیق کنید.

۲. پروتکل RTP چیست و توضیح دهید که چگونه نرم‌افزار wireshark در تحلیل آن به ما کمک می‌کند.



شکل ۱: SSL-Config

۲ راه‌اندازی DNS

توجه: این قسمت باید بر روی Linux انجام شود.
با مقدمات DNS در جلسه‌ی قبل آشنا شدید. حال می‌خواهیم نحوه‌ی راه‌اندازی یک کارگزار DNS را در این قسمت یاد دهیم. برای این کار برنامه‌ی bind۹ را بر روی سیستم‌عامل خود نصب نمایید. آدرس سرویس‌دهنده‌ی DNS را به ۱.۰.۰.۱۲۷ تنظیم کرده و در صورتی که سیستم‌عامل شما Fedora است، فایل "/etc/named.conf(/var/named/named.conf" و در صورتی‌که Ubuntu است "/etc/bind/named.conf.local" را به صورت زیر تغییر دهید:

```
zone "<Zone_Name"> IN {
  type <type>;
  file "<File_Name>."zone;
  allow-query {any;};
};
```

توجه: در سیستم‌عامل اوبونتو کلمه‌ی IN نوشته نمی‌گردد.
صفت type بیان‌کننده‌ی نوع رابطه‌ی سرویس‌دهنده‌ی DNS و دامنه‌ی موردنظر است. در صورتی‌که این مقدار master اعلام شود، بدین معنی است که سرویس‌دهنده‌ی DNS می‌تواند نام دامنه‌ی داده‌شده را با نام محل قرارگیری سرویس درخواست شده جایگزین نماید. برای راه‌اندازی این سرویس، مقدار type را master تعریف نمایید.
یک نمونه از تنظیمات انجام شده به‌صورت زیر است:

```
[...]
zone "example.com" {
  type master;
  file "/etc/bind/db.example.com";
};
[...]
```

```
zone "1.168.192.in-addr.arpa" {
  type master;
  notify no;
  file "/etc/bind/db.192";
};
```

با توجه به مشخصات داده شده، تنظیمات مورد نظر را اعمال فرمایید. فایل‌های نام برده شده را ترجیحا در مسیر "/var/-named" ایجاد نمایید. محتویات نمونه آن‌ها به صورت زیر است:

```
;
; BIND data file for local loopback interface
;
$TTL 604800
@ IN  SOA ns.example.com. root.example.com. (
              1       ; Serial
              604800  ; Refresh
              86400   ; Retry
              2419200 ; Expire
              604800) ; Negative Cache TTL
;
@ IN  NS  ns.example.com.
ns  IN  A 192.168.1.10
box IN  A 192.168.1.10
```

یک مثال از رکورد معکوس نیز به صورت زیر است:

```
;
; BIND reverse data file for local loopback interface
;
$TTL 604800
@ IN  SOA ns.example.com. root.example.com. (
              2       ; Serial
              604800  ; Refresh
              86400   ; Retry
              2419200 ; Expire
              604800) ; Negative Cache TTL
;
@ IN  NS  ns.
10  IN  PTR ns.example.com.
```

برای راحتی کار می‌توانید فایل "db.local" را کپی کرده و برروی آن تغییرات مورد نظر را انجام دهید. توضیحات در ادامه با اشاره به تنظیمات پیش‌فرض این فایل ارایه می‌گردد.
مقدار ۱.۰.۰.۱۲۷ را به مقدار IP سرویس‌دهنده‌ی مورد نظر تغییر دهید. همچنین root.localhost را به نام دامنه‌ای که مورد نظر است تغییر دهید. دقت نمایید که در انتهای نام دامنه "." گذاشته شود.
توجه: جایگزین root یک نام تعریف شده به عنوان کاربر اصلی و مدیر برای دامنه در نظر گرفته می‌گردد. این مقدار گاهی hostmaster نیز تعریف می‌گردد.
مقدار سریال به عنوان شماره نسخه تنظیمات بوده و در هر بار به‌روز رسانی تنظیمات DNS اضافه می‌گردد. مقادیر عددی به ثانیه بوده و صفاتی هم‌چون زمان اعتبار، زمان سعی مجدد و ... را نشان می‌دهند.
انواع رکوردها:

۱. رکورد آدرس: یک آدرس IP را به یک نام دامنه متصل می‌نماید.

```
www IN  A 1.2.3.4
```

۲. رکورد نام مستعار: جهت تعریف نام مستعار برای یک رکورد A تعریف شده، استفاده می‌گردد.

```
mail   IN   CNAME www
www IN   A  1.2.3.4
```

۳. رکورد نام سرویس‌دهنده: نشان می‌دهد چه کپی‌هایی از این سرویس‌دهنده وجود دارد.

```
  IN NS ns.example.com.
  [...]
ns   IN   A  1.2.3.4
```

۴. رکورد تبادل ایمیل: برای تعریف سرویس‌دهنده‌های ایمیل و اولویت آن‌ها به کار می‌رود.

```
  IN   MX   10   mail.example.com.
  [...]
mail   IN   A  1.2.3.4
```

توجه: بعد از اعمال تغییرات سرویس bin باید راه‌اندازی مجدد شود تا تغییرات اعمال گردند. برای این کار می‌توانید در صورتی که به عنوان مثال از bind۹ استفاده می‌کنید از دستور

```
$ /etc/init.d/bind9 restart
```

استفاده نمایید.
توجه: برای چک کردن syntax تنظیمات می‌توانید از دستور

```
$ sudo named-checkconf
```

استفاده نمایید.
توجه: برای این‌که سرویس‌دهنده‌ی شما قبل از همه‌ی سرویس‌دهنده‌های "trusted" سیستم کاربر مورد استفاده قرار بگیرد، لازم است در سیستم‌عامل اوبونتو اسم سرویس‌گیرنده در /etc/resolv.conf قرار بگیرد. برای این‌کار می‌توانید از دستور

```
$ sudo vi /etc/resolvconf/resolv.conf.d/head
```

برای بازکردن فایل و تغییر آن به صورت

```
search example.com  # your private domain
nameserver 10.128.10.11  # ns private IP address
```

استفاده نمایید. بعد از این‌کار از دستور

```
$ sudo resolvconf -u
```

برای قرارگیری نام سرویس‌دهنده در /etc/resolvconf استفاده کنید. بعد از این می‌توانید از دستوراتی مانند dig، nslookup و ping برای تست سرویس‌دهنده‌ی خود استفاده نمایید.

۱.۲ سناریو آزمایش

- در این آزمایش باید یک منطقه بسازید. برای این‌کار لازم است تا یک سرویس‌دهنده‌ی DNS بر روی لینوکس نصب نمایید. سرویس را در حالت اجرا قرار دهید.
- یک منطقه با عنوان NetLab#.edu ایجاد کنید. به‌جای # شماره‌ی گروه خود را قرار دهید. بر روی این منطقه دو میزبان با نام group۱ و group۲ با آدرس‌های IP سیستم‌های خود تعریف کنید.
- برای هر یک از میزبان‌های تعریف شده، یک نام مستعار نیز تعریف کنید.
- رکورد مناسب را جهت جستجوی معکوس اضافه کنید.
- با استفاده از دستوراتی مانند dig و nslookup و ... از درستی سرویس‌دهنده اطمینان حاصل نمایید.

۲.۲ سوالات

۱. بسته‌های تبادل شده در اجرای دستور dig یا nslookup را با استفاده از wireshark ذخیره و تحلیل نمایید.

۲. نوع رکورد منبع (resource records) هر یک از رکوردهای تعریف‌شده فوق را بیان کنید.