به نام خدا

گزارش تمرین عملی دوم درس مبانی امنیت

امیرمحمد پیرحسین لو

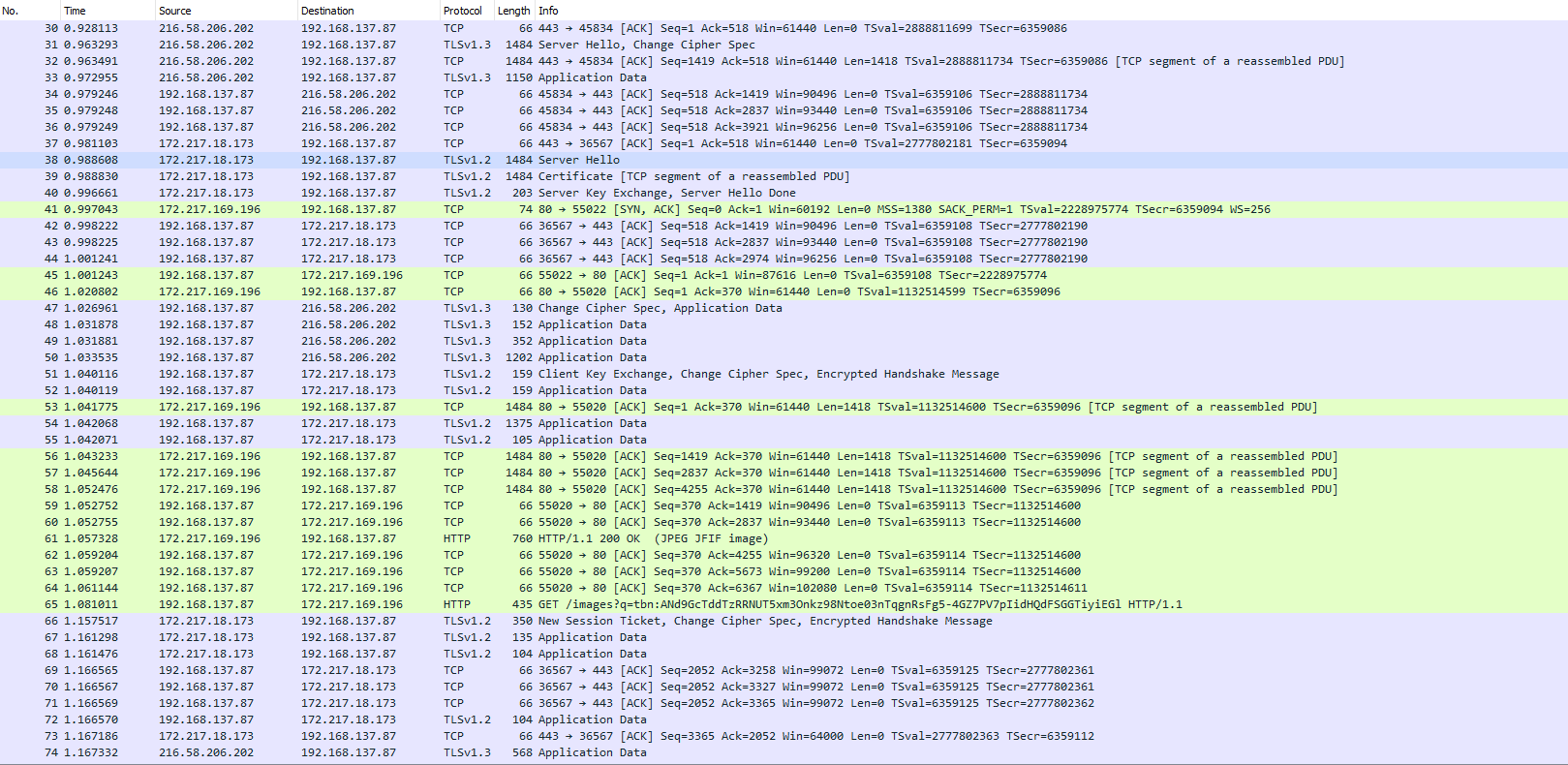
9531014

1. پروتکل های مورد استفاده:

TCP, TLSv1.2, TLSv1.3, ICMP

از پروتکل ICMP برای تبادل پیغام های مدیریتی در لایه 3 شبکه استفاده می شود.

پیام رسان پیام ها را به صورت رمزشده با استفاده از SSL(secure socket layer) ارسال می کند. به همین دلیل اکثر پیام ها حاوی پروتکل TLSv1.3 , TCP است.



طبیعتا چون پیام رسان پیام ها رو به صورت رمز شده می فرستد و تبادل پیام ها به صورت connection oriented است، پروتکل های TCP و TLSv1.3 فراوانی بیشتری دارند.

**کاربری ابزار های مانیتورینگ:**

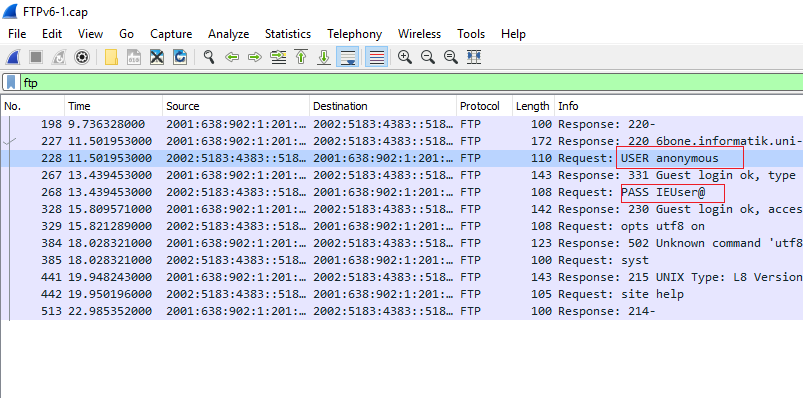
برای عیب یابی روتر ها و سایر اجزای شبکه و تشخیص خرابی اجزا،

تشخیص حملات و زمان هایی که پیک در نمودار ترافیک بر حسب زمان وجود دارد و

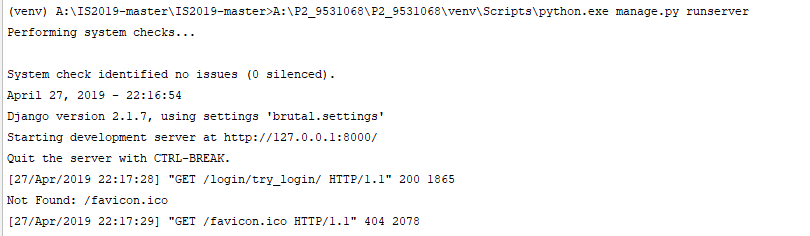
برنامه ریزی برای تغییر توپولوژی شبکه نیاز به مانیتورینگ توسط ادمین شبکه می باشد.

USER: anonymous

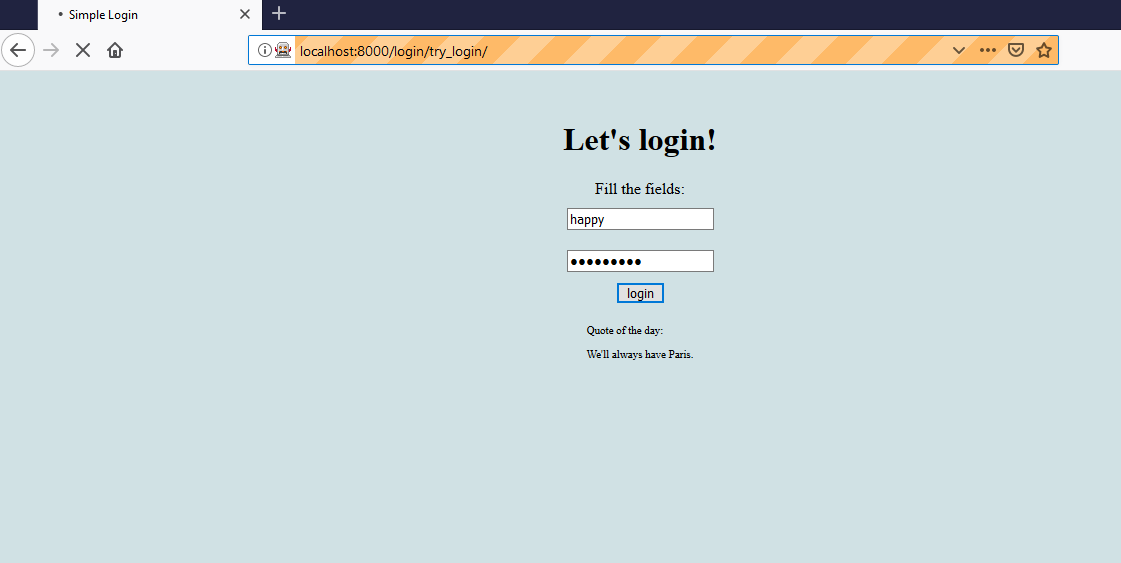
PASSWORD: IEUSER@



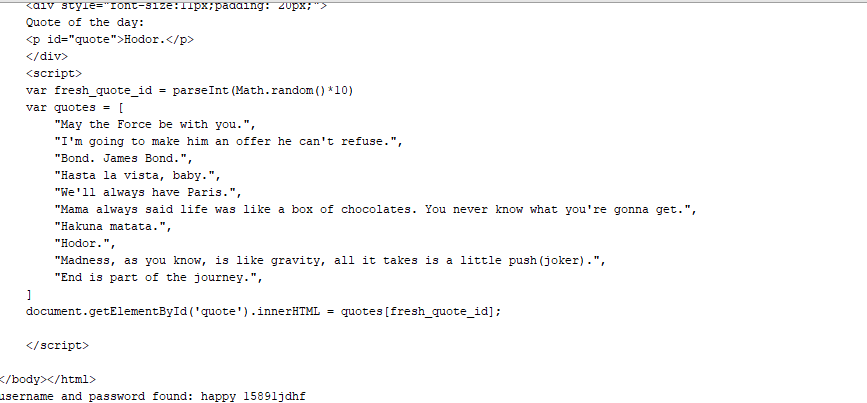
1. server setup:



filling username and password with help of selenium:



response of clicking button:



برای حل مشکل captcha می توان ip را در لایه سه بعد هر سه درخواست تغییر داد و به صورت iterative بین مجموعه ای از ip ها iterate کنیم تا session ip های قبلی منقضی شود.

برای جلوگیری از حملات فیشینگ باید در ابتدا url سایت را چک کرد و از صحت آن اطمینان پیدا کرد. همچنین باید چک شود که حتما پروتکل مورد استفاده Https باشد.

**کد حمله brute force:**

