گروه شماره ۱ : مهدی محمدی (۴۰۰۱۰۵۲۳۹) - ملیکا علیزاده (۴۰۱۱۰۶۲۵۵) - معین آعلی (۴۰۱۱۰۵۵۶۱)

# گزارش آزمایش شماره‌ی ۲

**فهرست مطالب**

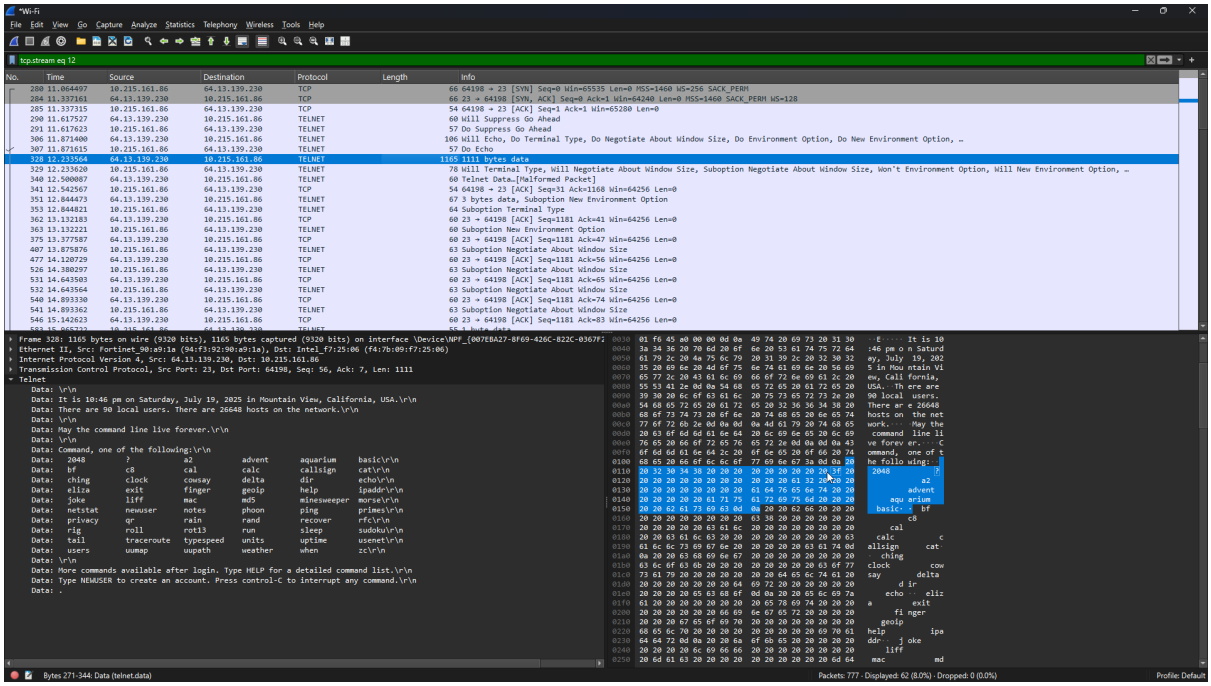
بررسی ارتباط از طریق Telnet . . . . . ۲

## بررسی ارتباط از طریق Telnet

در ابتدا نیاز است تا telnet را روی ویندوز فعال کنیم. وارد control panel می‌شویم و در بخش Programs گزینه‌ی Turn Windows features on or off را انتخاب می‌کنیم. سپس به دنبال telnet client می‌گردیم و آن را فعال می‌کنیم.

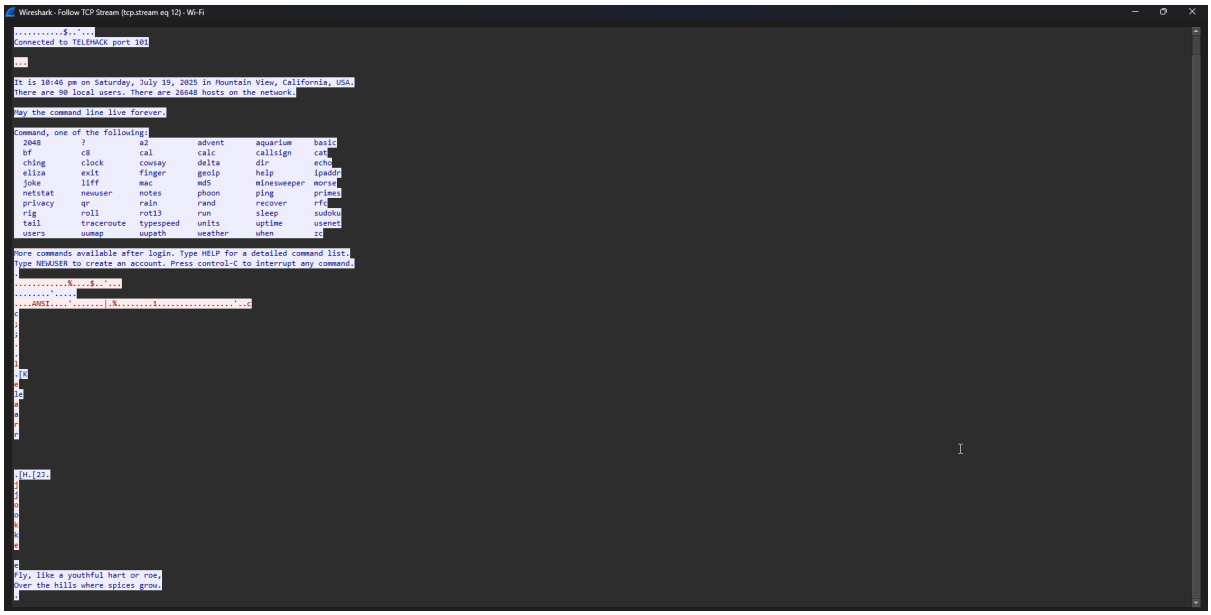
حال وارد cmd شده و با استفاده از دستور telnet telehack.com به آن متصل می‌شویم. البته قبل از آن باید wire-shark را در حالت capture بر روی interface اینترنت خود قرار دهیم. سپس تعدادی از دستورات را امتحان کرده و در نهایت capture را متوقف می‌کنیم.

در Wireshark فیلتر را روی telnet قرار داده و بسته‌ها را مشاهده می‌کنیم:



به عنوان مثال این بسته مربوط به پیام welcome این سیستم است که دستورات خود را به ما معرفی کرده است.

برای این که پیام‌ها را دنبال کنیم، روی این بسته کلیک راست کرده و از منوی follow گزینه‌ی tcp stream را انتخاب می‌کنیم.

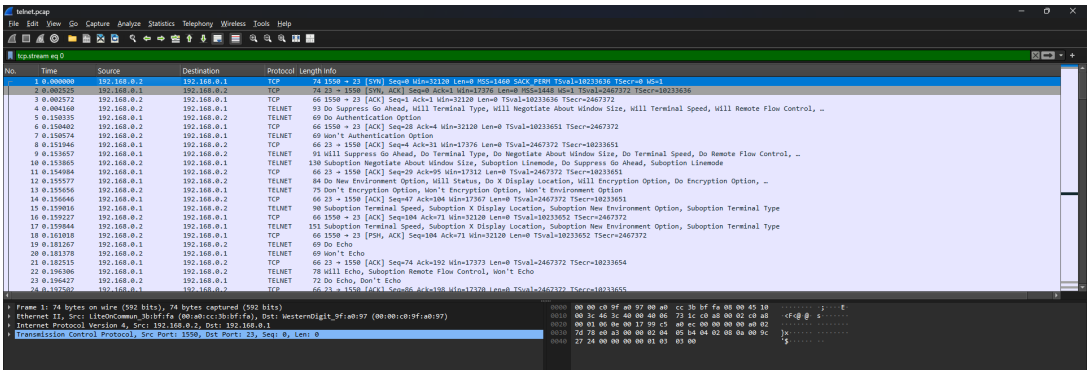


همانطور که در تصویر مشخص است، من با استفاده از کامند joke درخواست یک جوک کردم و در اخرین بسته این جوک به دست من رسیده است.

نکته مهمی که در شل گرفتن قابل توجه است، این است که وقتی ما در شل تایپ می‌کنیم. هر کارکتر در یک بسته جدا به سمت سرور فرستاده می‌شود و سپس از سمت سرور اگر به درستی به دستش رسیده باشد همان را برای ما برمی‌گرداند. این موضوع داخل tcp trace فوق قابل مشاهده است.

نکته مهم دیگری که در این پروتوکل مورد توجه قرار می‌گیرد، این است که پیام‌ها و بسته‌ها به صورت رمزنگاری نشده رد و بدل می‌شود که نشان دهنده امنیت پایین‌تر این پروتوکل نسبت به پروتوکل‌های دیگر نظیر SSH است.

**سوال ۱.**

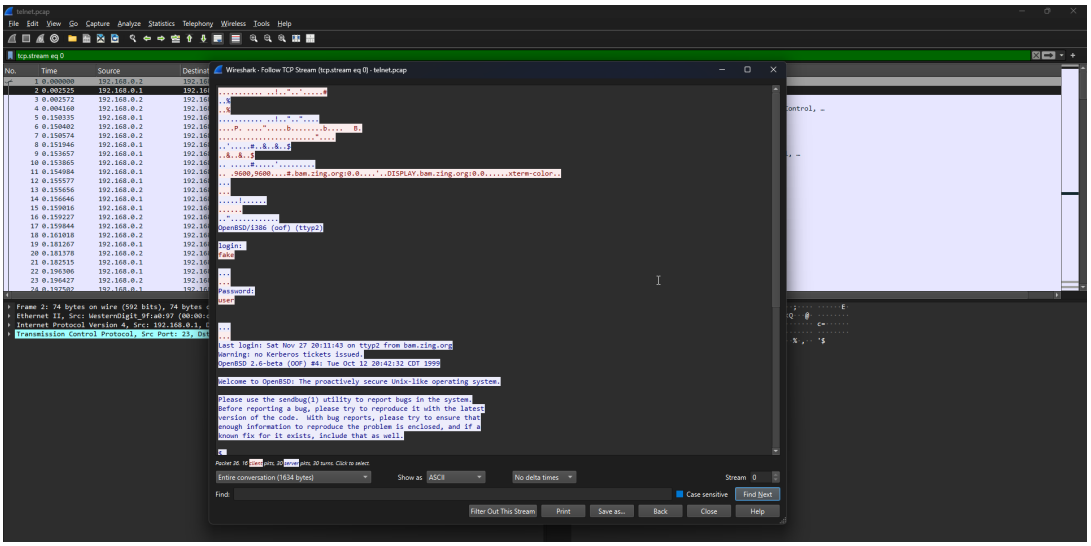


همانطور که در شکل فوق مشخص است، آیپی Source در اولین پکت 192.168.0.2 است که مربوط به کلاینت است و آیپی 192.168.0.1 مربوط به سرور است.

در سه بسته اول که از نوع TCP است فرایند TCP-Handshaking در حال انجام است و منطقا اولین پکت از سمت کلاینت ارسال شده است.

**سوال ۲.**

بر روی اولین پکت مربوط به این گفت‌وگو کلیک راست کرده و از منو follow گزینه‌ی TCP Stream را انتخاب می‌کنیم.



داخل تصویر فوق مشخص است که یوزرنیم و پسورد چه مقداری دارند. چون telnet پیام‌ها را رمزنگاری نمی‌کند، یوزرنیم و پسورد کلاینت به صورت raw داخل بسته‌های ارسالی قابل مشاهده است.

**سوال ۳.**

نیاز نیست کار سختی انجام دهیم، کافیست مجدد روی TCP Stream کلیک کنیم. پیام‌های قرمز از سمت کلاینت و پیام‌های آبی از سمت سرور هستند.

کاربر پس از لاگین، این دستورات را اجرا کرده است:

```
$
/sbin/ping www.yahoo.com

PING www.yahoo.com (204.71.200.67): 56 data bytes
64 bytes from 204.71.200.67: icmp_seq=0 ttl=241 time=69.885 ms
64 bytes from 204.71.200.67: icmp_seq=1 ttl=241 time=73.591 ms
64 bytes from 204.71.200.67: icmp_seq=2 ttl=241 time=72.302 ms
64 bytes from 204.71.200.67: icmp_seq=3 ttl=241 time=73.493 ms
64 bytes from 204.71.200.67: icmp_seq=4 ttl=241 time=75.068 ms
64 bytes from 204.71.200.67: icmp_seq=5 ttl=241 time=70.239 ms

.....
.....
.--- www.yahoo.com ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 69.885/72.429/75.068 ms
$
ls

$
ls -a

.          ..         .cshrc     .login     .mailrc    .profile   .rhosts
$
exit
```