

به نام خدا

کار با کارکرد های Web, DNS

فصل دو، آزمایش دو



محمد جواد زندیه 9831032

21 اردیبهشت 1400

دانشکده مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر

سوال 1:

remarks: (Domain Holder) alireza Bagheri

person: alireza bagheri  
e-mail: [soft98.ir@gmail.com](mailto:soft98.ir@gmail.com)

سوال 2:

nserver: ir1.hostdl.com  
nserver: ir2.hostdl.com

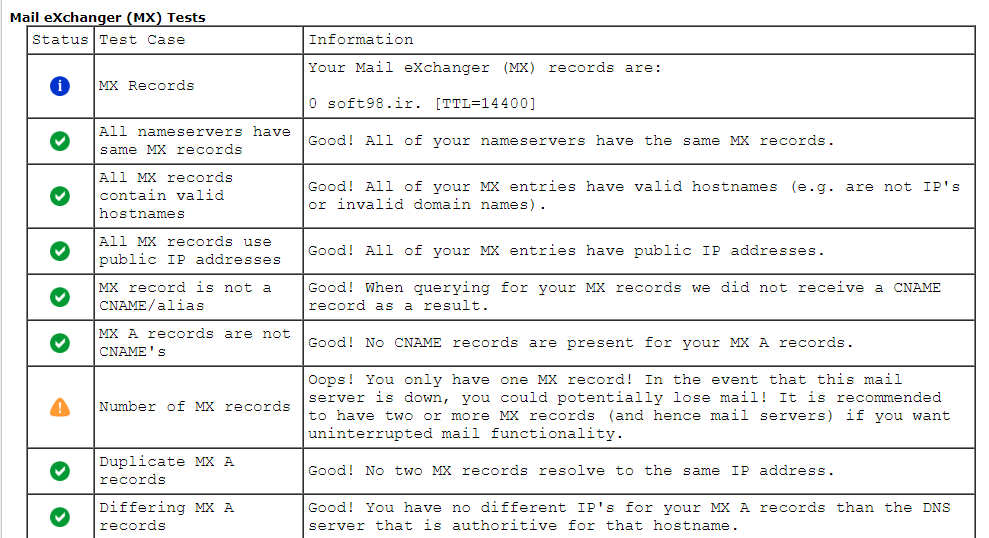
سوال 3:

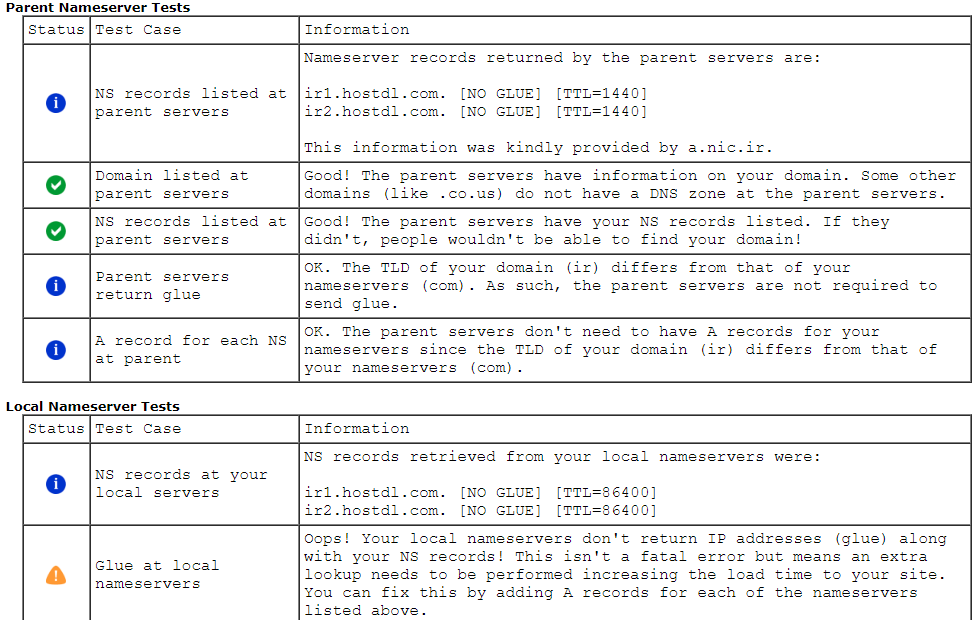
NS: name server : حاوی نام سرور معتبر، به همراه یک دامنه یا منطقه برای DNS می باشد. وقتی که یک کاربر برای یک آدرس ip درخواست می کند، میتواند آدرس ip خود را از یک رکورد NS از طریق جست و جوی DNS پیدا کند.

A: address : آدرس ip دامنه درخواست شده را تعیین می کند.

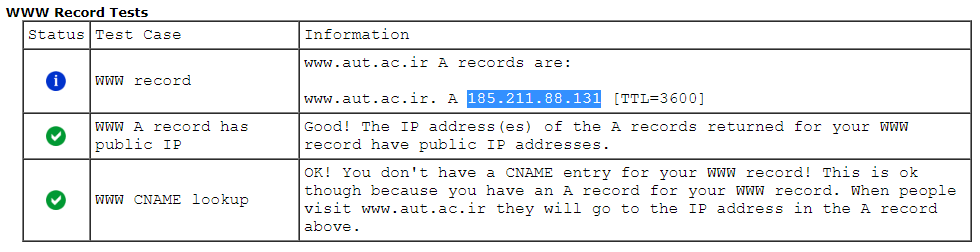
TXT: تعین مالکیت دامنه و اطمینان از منیت ایمیل از جمله کاربرد های آن است.

MX: mail exchange : ایمیل را به mail server هدایت می کند. رکورد MX نشان می دهد که چگونه پیام های ایمیل باید مطابق با پروتکل انتقال نامه ساده (SMTP، پروتکل استاندارد برای همه ایمیل ها) مسیریابی شوند. مانند رکوردهای CNAME، یک رکورد MX همیشه باید به دامنه دیگری اشاره کند.



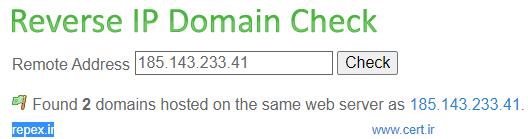


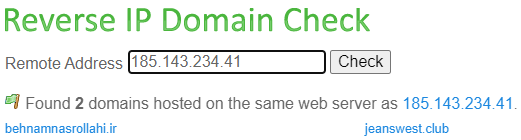
سوال 4:



سوال 5:

[behnamnasrollahi.ir](http://behnamnasrollahi.ir/) , [jeanswest.club](http://jeanswest.club/) , [repex.ir](http://repex.ir/)





behnamnasrollahi.ir (185.143.233.41, 185.143.234.41)

jeanswest.club (185.143.233.41, 185.143.234.41)

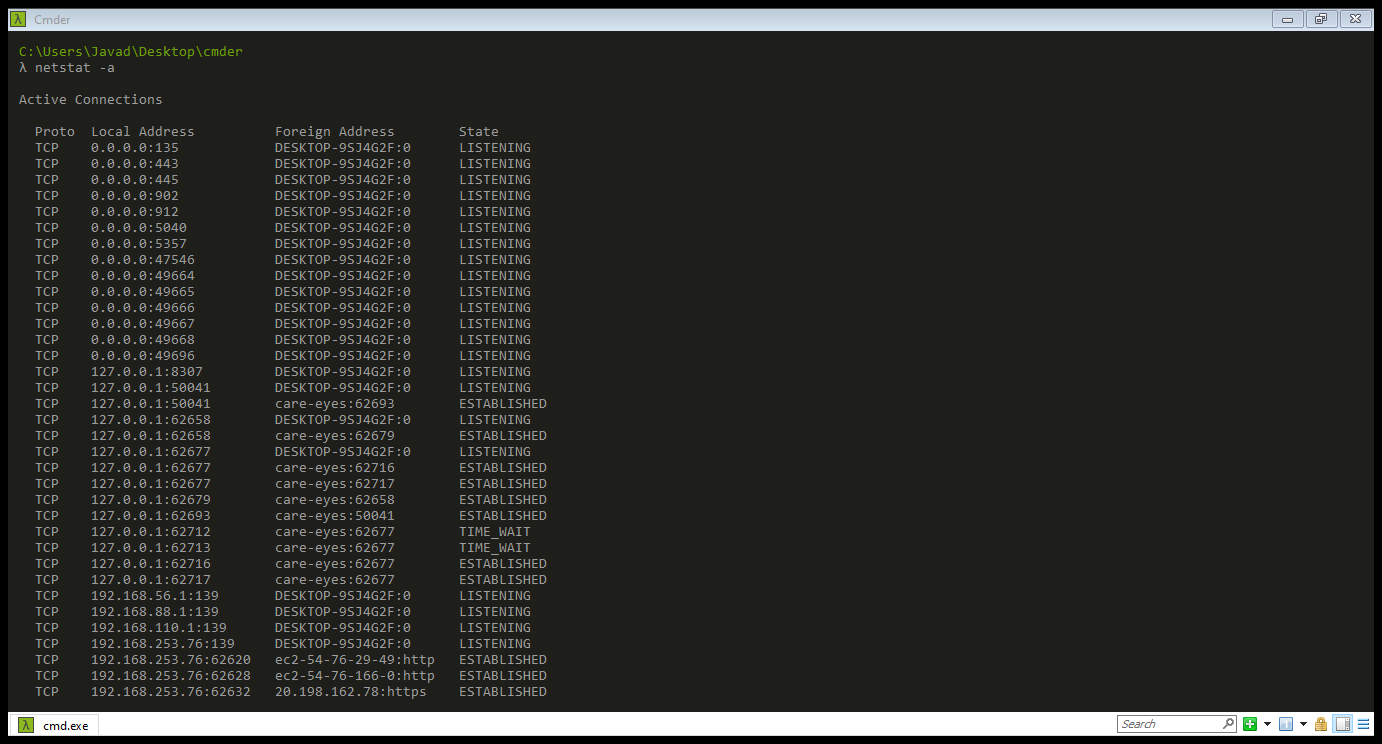
repex.ir (185.143.234.41, 185.143.233.41)

cert.ir (185.143.233.41, 185.143.234.41)

آدرس ip همگی یکسان است.

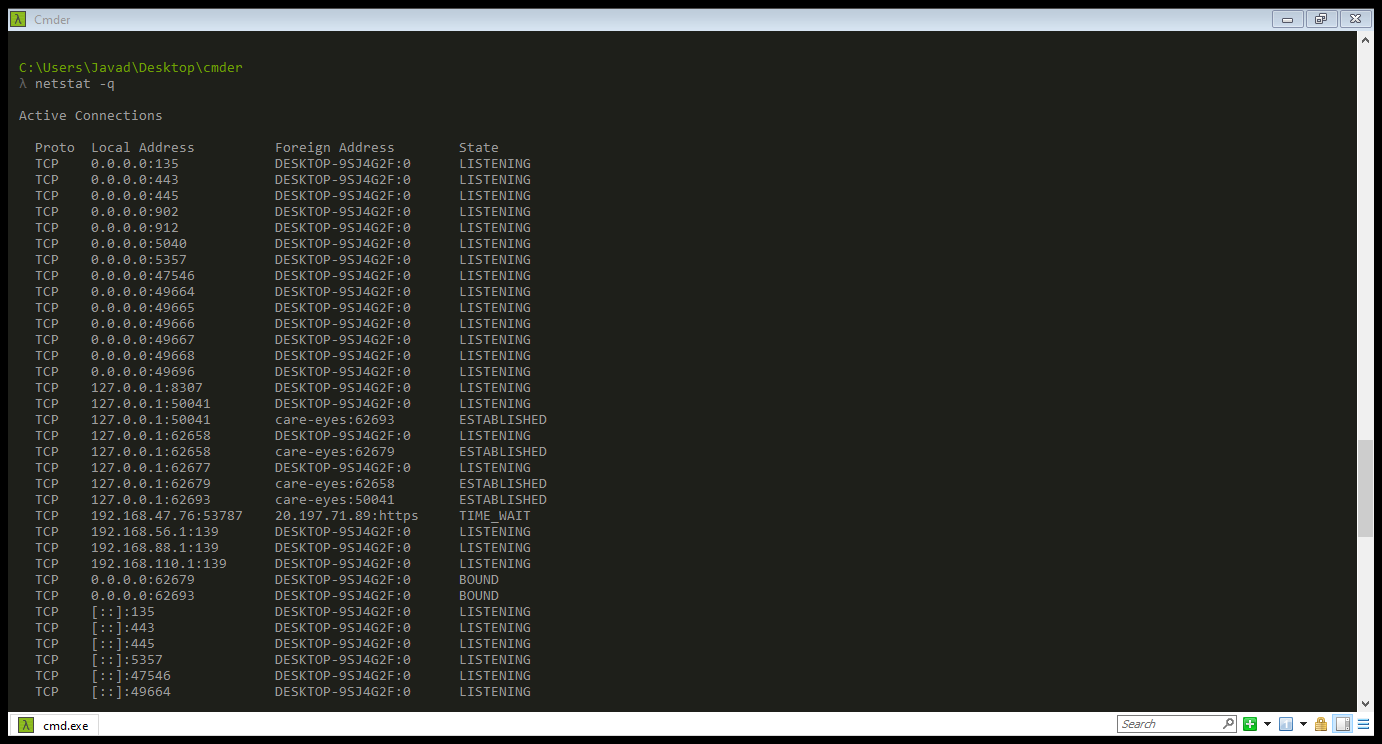
سوال 6: بله همانند مالتی پلکسینگ آدرس آیپی وب سرور مربوطه جست و جو میشود. مرورگر مورد استفاده از طریق جستجو در حافظه کش خود یا با استفاده از DNS ها آدرس IP را به دست می آورد. سپس تشخیص می دهد اطلاعات سایت شما در چه مسیری قرار دارد.

سوال 7: دستور netstat -a ارتباط های فعال را به ما می دهد.



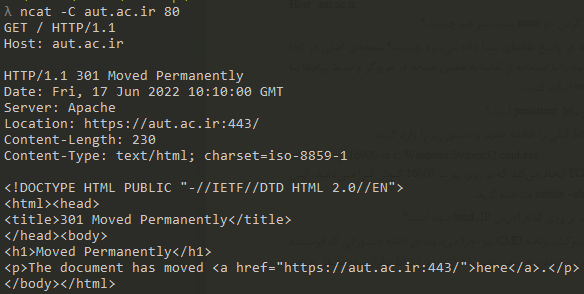
سوال 8:

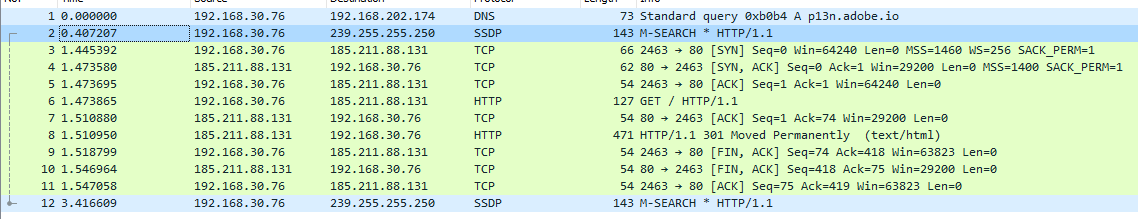
با دستور netstat -q میتوان این کار را انجام داد



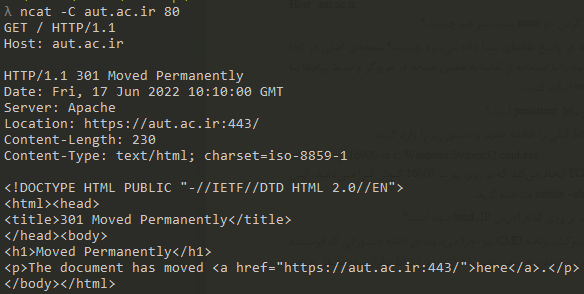
سوال 9: به این معنا است که در پیام HTTP خود فیلد دیگری نمیخواهیم قرار دهیم و با همین اطلاعات که وارد شده است، میخواهیم فرایند صورت گیرد.

سوال 10: پیام Moved Permanently در پاسخ داده میشود که به معنای redirect است. صفحه اصلی در Location: <https://aut.ac.ir:443/> قرار دارد طبق پیام داده شده.





سوال 11: persistent است زیرا از ورژن 1.1 برای HTTP استفاده شده است که میدانیم به صورت persistent عمل میکند.



سوال 12: آدرسی که bind شده است(حاصل اجرای netstat -abn) -> 0.0.0.0



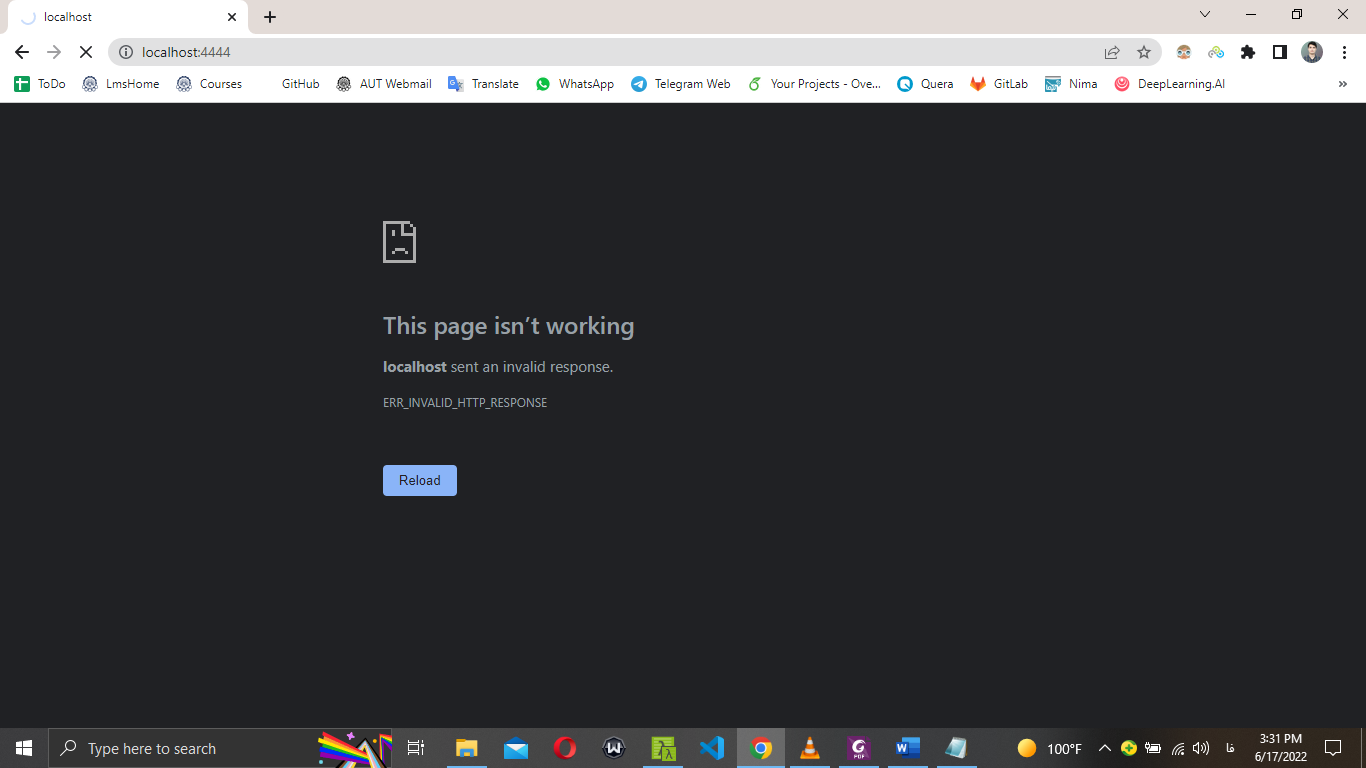
سوال 13:

این خط جدا کننده header و body است و اگر نباشد، در پاسخ، پیامی که در body وجود دارد نمایش داده نمیشود و انگار body ای نداریم.

اگر خط اول وجود نداشته باشد، پیغام زیر به عنوان خطا داده خواهد شد:

Localhost sent invalid response یعنی پیامی غیر معتبر (به دلیل نبود هدر ارسال شده است) و به پیام ارسال شده HTTP ایراد میگیرد.

در واقع این هدر، پروتکل و ورژن مربوطه را بیان میکند و پیامی که ندانیم از طریق چه پروتکلی ارسال کنیم دچار خطا خواهد شد.



سوال 14: لینوکس cpe:/o:linux:linux\_kernel:3.13 cpe:/o:linux:linux\_kernel:4

سوال 15: از 1000 پورتی که scan کرده است، پورت های زیر باز بوده اند:

Scanning aut.ac.ir (185.211.88.131) [1000 ports]

Discovered open port 25/tcp on 185.211.88.131

Discovered open port 443/tcp on 185.211.88.131

Discovered open port 1723/tcp on 185.211.88.131

سوال 16: سرویس tcp بوده است.