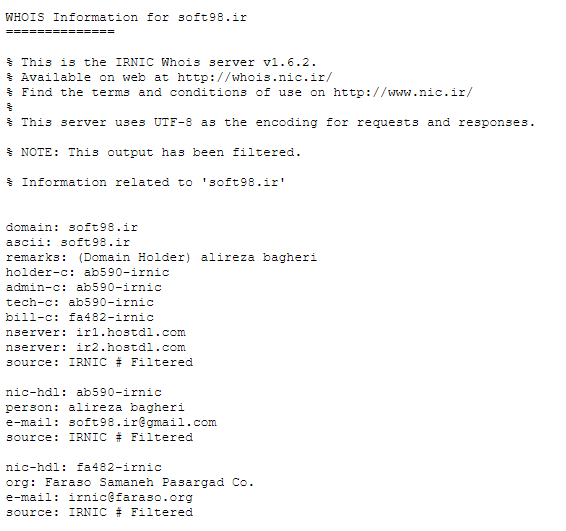
**گزارش دستورکار چهارم آزمایشگاه درس شبکه­های کامپیوتری**

نگار موقتیان، 9831062

1. **نام و اطلاعات فردی که دامنه به اسم آن ثبت شده­است چیست؟**

مطابق اطلاعات بخش زیر این دامنه به نام علیرضا باقری ثبت شده و ایمیل مربوط به آن [soft98.ir@gmail.com](mailto:soft98.ir@gmail.com) می­باشد.



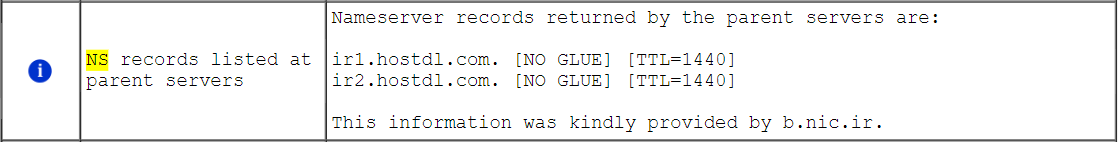
1. **آدرس name server آن چیست؟**

طبق بخش­های مشخص شده در بالا آدرس name server این وبسایت ir1.hostdl.com و ir2.hostdl.com می­باشد.

1. **رکوردهای NS، A، TXT و MX را مشخص کنید. هر یک از این رکوردها چه چیزی را مشخص می­کنند؟**

رکورد NS:

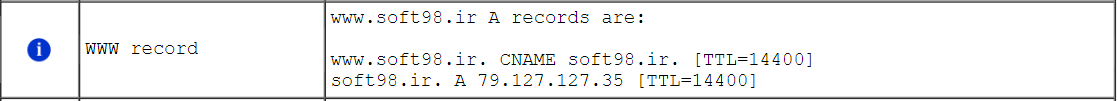
رکوردهایی از این نوع برای مشخص کردن نام دامنۀ name server ای که به یک دامنۀ خاص سرویس ارائه می­دهد استفاده می­شود. این رکورد hostname هر name server را به main domain آن مربوط می­کند.



رکورد A:

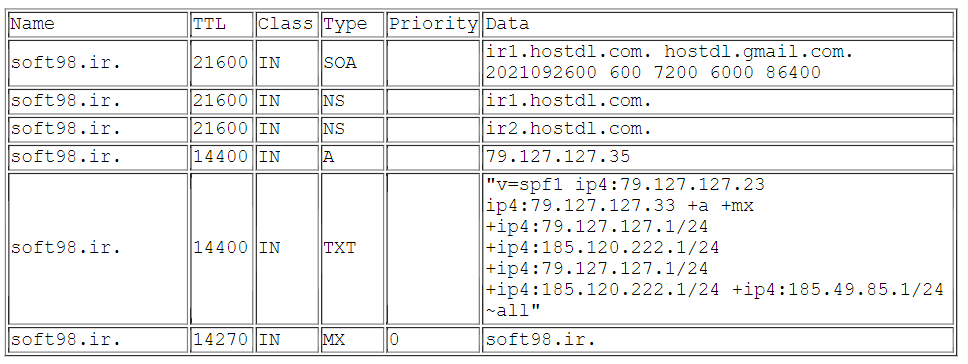
در این نوع از رکوردها هر hostname به یک آدرس IP نگاشت می­شود.

÷



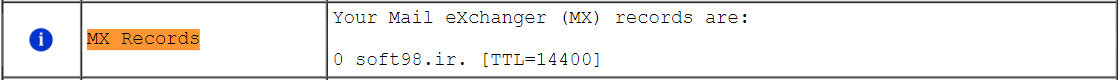
رکورد TXT:

رکوردهایی هستند که در قالب سوابق متنی اطلاعاتی را دربارۀ سرورها نگهداری می­کنند. با توجه به اینکه رکورد TXT مربوطه در قسمت DNS Report وبسایت معرفی شده نمایش داده نمی­شد، اطلاعات زیر از بخش DNS Record Lookup سایت بدست آمده­است که شامل اطلاعات مربوط به رکورد TXT و دیگر رکوردها می­باشد.



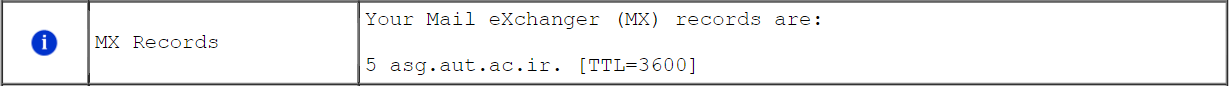
رکورد MX:

برای یک رکورد از این نوع Value نام کانونی سرور ایمیلی است که یک نام alias با نام Name دارد. این نوع از رکوردها به کمپانی­ای که از آن­ها استفاده می­کند اجازه می­دهند تا یک نام alias مشترک برای سرورهای ایمیل و دیگر سرورهای خود داشته باشند (برای مثال aut.ac.ir هم نام دامنۀ ایمیل­ها را مشخص می­کند و هم نام دیگر سرورهای دانشگاه).

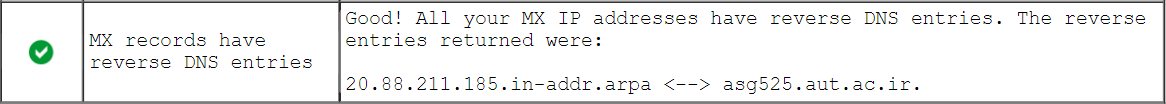


1. **در قسمت DNS Report با وارد کردن دامنۀ دانشگاه (aut.ac.ir)، mail server دانشگاه را مشخص کنید. آیا آدرس IP آن را می­توانید مشخص کنید؟**

با توجه به توضیحات قسمت قبل برای بدست آوردن اطلاعات مربوط به mail server ها باید به رکوردهای MX مراجعه کنیم. با توجه به شکل زیر آدرس mail server دانشگاه asg.aut.ac.ir می­باشد.



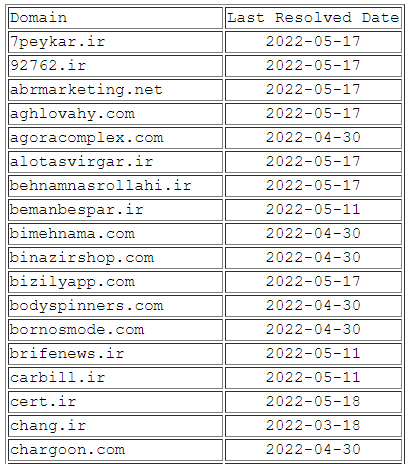
به علاوه همانطور که در قسمت زیر مشاهده می­شود IP مربوط به این mail server برابر است با 185.211.88.20.



1. **چه وبسایت­های دیگری بر روی همین سرور قرار دارند؟ چند مورد از آن­ها را نام ببرید.**

وبسایت­های مشخص شده در شکل زیر همگی بر روی یک سرور مشترک با cert.ir قرار دارند. نمونه­ای از این وبسایت­ها عبارت­ است از:

7peykar.ir, abrmarketing.net, agoracomplex.com, alotasvirgar.ir, brifenews.ir, carbill.ir, …



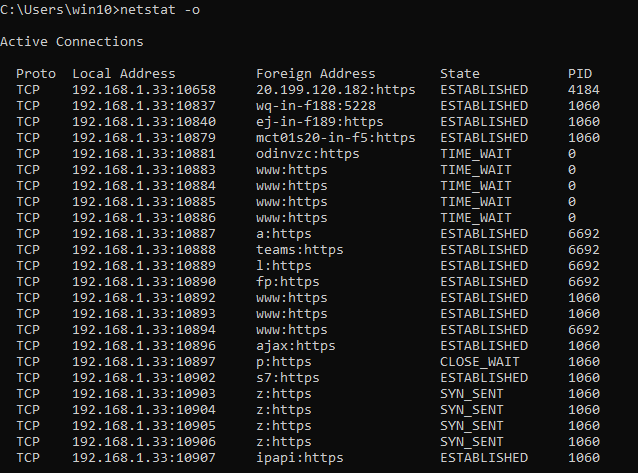
1. **به نظر شما سرور چگونه وب سرور درخواست شده را تشخیص می­دهد؟ آیا این روش نیز نوعی multiplexing است؟**

بله؛ یکی از خدمات مهمی که پروتکل­های لایۀ انتقال (TCP و UDP) ارائه می­دهند این است که انتقال داده میان دو سیستم انتهایی که لایۀ IP ارائه می­کند را به انتقال داده میان دو اپلیکشن (یا پردازه) که بر روی سیستم­های انتهایی اجرا می­شوند گسترش دهد؛ به این کار multiplexing و demultiplexing لایۀ انتقال گفته می­شود.

زمانی که می­خواهیم به یک وب سرور درخواست دهیم باید IP و شماره پورت آن را مشخص کنیم. آدرس IP مشخص می­کند که می­خواهیم به چه سیستمی در شبکه پیغام را برسانیم (کدام سرور). شماره پورت در هدر بسته­ها قرار خواهد گرفت و در حقیقت مشخص می­کند که درخواستی که به سرور می­دهیم باید به کدام وب سرور تحویل داده شود.

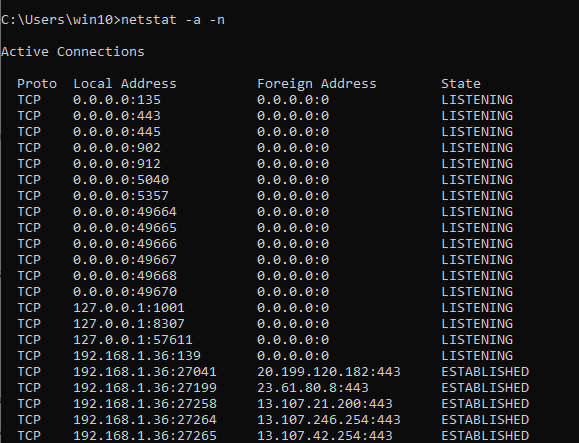
1. **برای لیست کردن برنامه­هایی که در حال حاضر پورت­های لایۀ انتقال را بر روی سیستم باز کرده­اند، از چه دستور خط فرمانی استفاده می­شود؟**

با استفاده از دستور netstat و آرگومان –o مطابق شکل زیر می­توان لیستی از پورت­هایی که در حال حاضر فعال هستند، وضعیت آن­ها و pid پردازه­ای که آن­ها را در اختیار دارد را مشاهده کرد.



1. **دستوری را پیدا کنید که به وسیلۀ آن تمام پورت­های سیستم در هر وضعیت اتصالی همراه با مبدا و مقصد اتصال به صورت عددی لیست شوند.**

برای این کار از دستور netstat استفاده کرده و به منظور لیست کردن تمام پورت­ها (و نه فقط پورت­های فعال) از آرگومان –a و برای لیست کردن مبدا و مقصد اتصال به صورت عددی از آرگومان –n استفاده می­کنیم. خروجی این دستور مانند زیر می­باشد.



1. **دلیل وارد کردن دو enter پشت سر هم چیست؟**

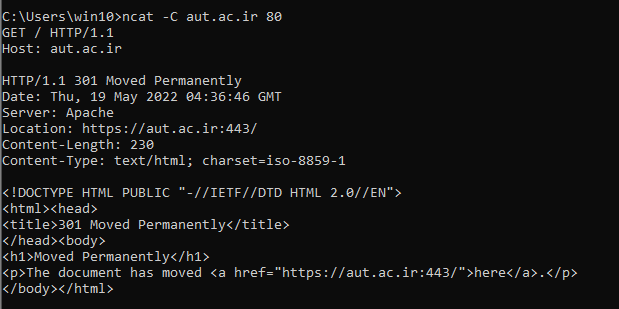
در فرمت درخواست­های HTTP پس از آن­که header ها به پایان رسیدند لازم است که یک خط خالی گذاشته شده و پس از آن بدنۀ پیام آورده شود. در مورد درخواست گفته شده در این سوال، بدنۀ درخواست مورد نظر خالی است، لذا enter اول برای جداسازی سرآیند پیام از بدنۀ آن و enter دوم برای ارسال درخواست بوده­است.

1. **پیامی که در پاسخ تقاضای شما دهده می­شود چیست؟ صفحۀ اصلی در کجا قرار دارد؟**

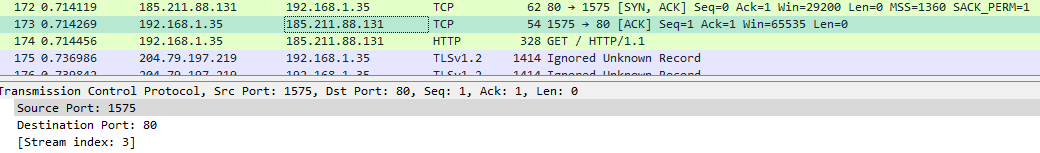
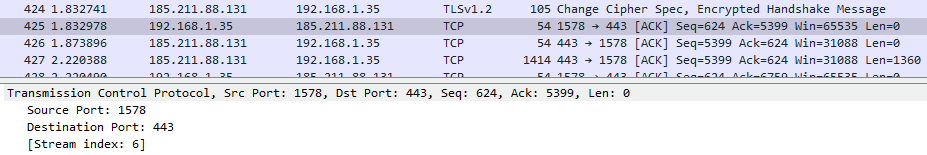
Status code پیغام داده شده 301 بوده و به این معناست که شیءای که درخواست آن داده شده­است به طور دائمی به آدرس دیگری منتقل شده­است. با توجه به پاسخ داده شده آدرس جدید صفحۀ اصلی عبارت است از:

<https://aut.ac.ir:443/>

به عبارتی وب سرور اصلی بر روی پورت 443 (و نه 80) اجرا می­شود.



اگر همین درخواست را توسط مرورگر داده و بسته­های انتقال یافته را توسط Wireshark شنود کنیم متوجه می­شویم که در ابتدا درخواستی بر روی پورت 80 داده شده و پس از آن باقی بسته­ها از طریق پورت 443 انتقال یافته­اند.

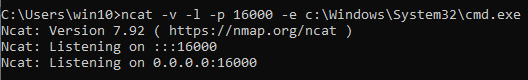


1. **آیا این ارتباط persistant است؟**

بله؛ زیرا پس از این که پیغام HTTP بالا را فرستادیم امکان ارسال پیغام­های بعدی نیز از طریق همان ارتباط ایجاد شده وجود دارد.

1. **این پورت بر کدام آدرس IP، bind شده­است؟**

مطابق شکل زیر این پورت (16000) به آدرس 0.0.0.0 بایند شده­است. به طور کلی این آدرس به host های unknown تخصیص داده می­شود.



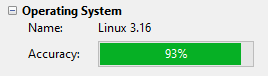
1. **دقت کنید یک خط خالی بین HTTP و <html> باید وجود داشته باشد. به نظر شما دلیل وجود خط اول در این فایل چیست؟**

در ابتدای این خط پروتکل استفاده شده برای انتقال پیام (HTTP) و ورژن آن (1.1) را مشخص کرده­ایم.

در ادامه از آن­جایی که در این قسمت در حال فرستادن یک HTTP Response هستیم، باید به گیرندۀ پیغام یک   
status code و status message نیز اعلام کنیم. این کد و message مشخص می­کند نتیجۀ درخواست کلاینت چه بوده­است. برای مثال در این پیغام کد را برابر با 200 و message آن را برابر با OK قرار داده­ایم، به این معنا که در دریافت و پردازش پیغام مشکلی وجود نداشته­است.

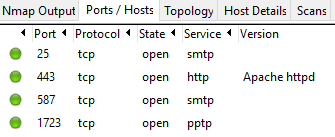
1. **سیستم عامل این وب­سایت چیست؟**

با توجه به قسمت زیر از نتایج اسکن وب­سایت، با دقت 93% سیستم عامل استفاده شده Linux 3.16 می­باشد.



1. **چه پورت­هایی بر روی این سرور باز است؟**

با توجه به قسمت زیر از نتایج اسکن وب­سایت، پورت­های 25، 443، 587 و 1723 بر روی این سرور باز هستند.



1. **سرویس­هایی که از طریق این پورت­ها ارائه می­شود چیست؟**

با توجه به شکل قسمت قبل سرویس SMTP بر روی پورت 25 و 587، سرویس HTTP بر روی پورت 443 و سرویس PPTP بر روی پورت 1723 ارائه می­گردد.