آز شبکه ۴

گرفتن بسته های پیام :

۱) پروتکل های مختلفی که در ستون مربوطه در لیست پکت ها موجود است:

TCP , HTTP , MDNS , ARP , ICMPV٦ , SSDP , TLSV۱,۳ , DHCPV٦ , DHCP , IGMPV۲ , DNS , LLMNR , TLSV۱,۲ , UDP , RIPV۲ , OCSP , QUIC

۲) از زمان ارسال HTTP GETتا زمان دریافت HTTP OK چقدر طول کشیده است:

زمان ارسال = ۱۳.۱۷۹۵۸۷

زمان دریافت = ۱۳.۶۹۲۸۳۳

۱۳.۱۷۹۵۸۷ - ۱۳.۶۹۲۸۳۳ = ۰.۵۱۳۲۴۶ ثانیه زمان طول میکشد.

۳) درخواست خروجی از سیستم ما به آدرس ۱۹۲.۱۶۸.۱.۱ رفته است. وقتی آدرس سایت مربوطه را در مرورگر وارد میکنیم ابتدا باید پروتکل dnsفعال شده تا نام سایت را به آیپی آن تبدیل کند پس باید پکت های مربوط به پروتکل dnsرا بررسی کنیم . میدانیم که وقتی یک درخواست dnsداریم اولین جایی که می رود dns server محلی ما است که ایپی آن(همانطور که با کامند ipconfig/all در cmd) بررسی کردیم ۱۹۲.۱۶۸.۱.۱ است.

پروتکل HTTP :

۱) ما توسط مرورگر درخواست خود را ارسال میکنیم پس مرورگر نقش کلاینت را دارد. اما HTTP سرور ، آن هاستی است که درخواست ما به آن ارسال میشود. پس برای بررسی نسخه مرورگر باید HTTP GET را بررسی کنیم که نسخه ۱.۱ را ساپورت میکند. اما برای بررسی نسخه HTTP سرور باید HTTP RESPONSE را بررسی کنیم که باز هم نسخه ۱.۱ است.

تفاوت بین نسخه ۱ و ۱.۱ : تفاوت عمده بین HTTP ۱,۰ وHTTP۱,۱ در این است کهHTTPv۱,۰ برای هر یک از پروسه های response , request یک ارتباط TCP جدید ایجاد می‌کند . در صورتی که در HTTPv۱,۱ برای مبادلات یک یا چندین response , request از یک ارتباط استفاده می کند و ارتباط جدیدی ایجاد نمی‌کند. به بیانی دیگر، HTTPv۱,۱ ارسال و دریافت چندین GET به صورت pipeline روی یک اتصال لایه انتقال TCP را معرفی کرد.

یک تفاوت دیگر این است که HTTP ۱,۰فقط می تواند تا ١٦ کد وضعیت را تعریف کند که یک شماره رزرو شده بود. اما HTTP ۱,۱ با ٢٤ کد وضعیت همراه بود که قادر به حل محدودیت های http ۱,۰ بود . گزارش خطا سریعتر انجام می شد و تشخیص آسان خطاها هنگام بروز رخ می داد.

تفاوت بعدی این است که HTTP ۱,۰احراز هویت ناامن است زیرا رمزگذاری نشده است اما HTTP ۱,۱امن است زیرا از چک لیست نام کاربری ، رمزعبور و مقدار یکبار استفاده می کند.

۲) Accept-Language: en-US,en;q= ۰٫۵\r\n
۳) آدرس ایپی کامپیوتر : ۱۹۲.۱۶۸.۱.۱۰۵

آدرس ایپی سرور: ۱۷۶.۱۰۱.۵۲.۱۵۵

۴) میدانیم که پروتکل لایه انتقال http همیشه tcp است. برای فیلد لایه انتقال در وایرشارک نیز transmission control protocol نوشته شده که مخفف آن همان tcp میشود.
۵) میدانیم که پورت ها در لایه انتقال مشخص شده اند. همانطور که مشاهده میکنیم پورت مبدا ۱۲۶۸۶ و پورت مقصد ۸۰ میباشد.
۶) با توجه به اینکه http response از سمت سرور به مرورگر برمیگردد پس این مورد نیز باید بررسی شود. که کد وضعیت ۳۰۱ میباشد که به معنای moved permanently میباشد.

ردیابی DNS :

۱) آدرس فرستنده DNS QUERY : ۱۹۲.۱۶۸.۱.۱۰۵

آدرس پیام های پاسخ : ۱۷۶.۱۰۱.۵۲.۱۵۵

میدانیم که مهم نیست ارتباط DNS امن باشد یا نه و فقط سرعت ارتباط برای ما مهم است پس از UDP استفاده میشود. همانطور که در وایرشاک در فیلد مربوط به لایه حمل و نقل نیز USER DATAGRAM PROTOCOL درج شده پس میفهمیم از پروتکل UDP استفاده میشود.

۲) پورت مقصد DNS QUERY و پورت مبدا DNS RESPONSE هردو یکسان هستند. پورت هردو شماره ۵۳ میباشد.
۳) پیام DNS QUERY به آدرس ایپی ۱۹۲.۱۶۸.۱.۱ ارسال شده است که آدرس همان DNS SERVER محلی ما است. با دستور ipconfig/all نیز همان ۱۹۲.۱۶۸.۱.۱ میباشد.
۴) این پیام از تایپ A میباشد. این تایپ یعنی هرچیزی که در درخواستمان برای dns server محلی فرستاده ایم dns server در جواب باید آیپی آن سایت را به ما برگرداند. درواقع یعنی اسم را میدهیم و آیپی را دریافت میکنیم. خیر، این پیام حاوی جواب نیست و کوئری فقط جواب دارد.
۵) فقط یک جواب ارائه شده است چون سایت فقط یک آیپی آدرس دارد. این جواب حاوی iut.ac.ir: type A, class IN, addr ۱۷٦,۱۰۱,۵۲,۱۵۵ است.
۶) بله مطابقت دارد. دقیقا همان آدرس آیپی ۱۷۶.۱۰۱.۵۲.۱۵۵ میباشد.
۷) بله. تصاویر داخل سایت لینک شده بودند که از سایت های دیگری لود شوند پس باید به ازای هرکدام از سایت هایی که از آن ها تصاویر را میگیرد DNS QUERY جدیدی بفرستیم که بتوانیم آیپی آن را بدست بیاوریم و عکس را بگیریم.

ردیابی بسته های ICMP : در زمان اجرای دستور PING پروتکل ICMP فعال میشود.