کیامهر بهنیا

1. تفاوت سه پروتکل HTTP و DNS و DHCP چیست؟

پروتکل یک مجموعه قوانین و تکنیک هایی است که به ما اجازه می دهد که بین دو موجودیت در اینترنت ارتباط برقرار کنیم.

DNS یا Domain Name System :

پروتکلی است برای تبدیل Domain ها به IP که مانند دفترچه تلفنی است که به کاربران اجازه میدهد با استفاده از نام های دامنه و یا آدرس ها به اینترنت به صورت ساده دسترسی پیدا کنند.

DHCP یا Dynamic Host Configuration Protocol :

این پروتکل به ما این اجازه را میدهد تا بتوانیم به صورت اتوماتیک IP را به دستگاه های داخل شبکه تخصیص یا assign کنیم. که این اجازه را به ما می دهد تا به شکل اتوماتیک و سریع دستگاه خود را به شبکه پیوند بدهیم.

HTTP یا Hyper Text Transfer Protocol :

این پروتکل برای ارتباط برقرار کردن بین سرور و کاربر در وب استفاده می شود. مرورگر های وب می توانند صفحات وب را که می توانند شامل عکس ها، متن ها و یا ... باشند از سرور دریافت کنند و به کاربران نشان بدهند.

2. در مرورگر خود یک سایت را باز و ترافیک را با استفاده از **Wireshark** کپچر کنید. طی یک گزارش تک صفحه ای ترافیک کپچر شده را تحلیل نمایید. امکان استفاده از سایر پروتکل های مطرح مثل **DHCP** و **ICMP** هم وجود دارد.

اول wireshark را برای کپچر کردن فعال می کنیم بعد از آن صفحه مورد نظر مثلا google.com را باز می کنیم و تا زمانی که کامل لود شود صبر میکنیم، پس از آن کپچر کردن را خاموش میکنیم، ترافیک کپچر شده ما شامل چندین پروتکل مانند HTTP, DNS, DHCP, ICMP است و هر کدام در wireshark به رنگ خاصی نمایش داده می شود مثلا DNS به رنگ آبی، ما می توانیم بعضی از پروتکل های مورد نظر را فیلتر کنیم تا به پروتکل مورد نیاز راحت تر دسترسی داشته باشیم.

هر Packet که کپچر شده است شامل یک شماره (NO)، زمان(time)، مبدا (source)، مقصد (destination)، پروتکل (protocol)، طول (Length) و Info که اطلاعاتی از Packet که trace کردیم به ما می دهد.

پروتکل های HTTP شامل درخواست ها و پاسخ های HTTP هستند که معمولا به شکل POST و GET نمایش داده می شوند.

مرورگر با استفاده از درخواست GET به هر سروری که در اینجا google.com است وصل می شود و صفحه اصلی را درخواست می کند که با پاسخ 200 OK به درخواست پاسخ داده شده و صفحه اصلی گوگل برای ما ارسال می شود.

در خواست های DNS برای تبدیل نام دامنه به آدرس IP استفاده می شوند.

در اینجا مرورگر یک درخواست DNS را برای نام دامنه (Domain Name) google.com ارسال می کند و DNS با آدرس IP مربوط به google.com را برای ما ارسال می کند.

تخصیص IP توسط پروتکل DHCP انجام می شود که شامل درخواست ها و پاسخ هایی است.

در این قسمت کامپیوتر با استفاده از درخواست DHCP Discover به دنبال یک سرور DHCP می گردد که DHCP یک آدرس IP را در جواب به کامپیوتر پیشنهاد می کند.

ICMP هم شامل در خواست هایی مثل درخواست پینگ است.

در ان قسمت مرورگر اول یک در خواست پینگ (Ping) به google.com با استفاده از DHCP Discover ارسال می کند که سرور google.com با استفاده از Echo Reply به درخواست ما جواب می دهد.

و پروتکل های دیگری همچون TCP، QUIC (که در QUIC اول به دنبال پکت "Clinet Hello" می گردد و بعد از آن هند شیک QUIC یا همان (Quic Handshake) را برقرار می کند بعد از آن تمام استریم های مختلف QUIC را مشاهده و Identify می کند و داده های انکریپت و رمزنگاری شده و همچنین پکت های TLS Handshake را مشاهده میکند.) و یا پروتکل های دیگر که استفاده می شوند.

همچنین در قسمت پایین می توانیم هر Packet را به صورت جداگانه تحلیل کنیم و در سمت راست پایین Machine code هر packet را می توانیم ببینیم، همچنین شکل استرینگی همان را در کنارش مشخص شده است. که برای هر packet متفاوت است. در قسمت چپ، ما می توانیم به صورت عمیق تر و جدا شده پکت و دیتای خود را تحلیل کنیم.

مثلا برای زمانی که ما IP 4.2.2.4 را پینگ می کنیم مبدا IP ما است و مقصد IP 4.2.2.4 یک درخواستی فرستاده می شود و در جواب از طرف 4.2.2.4 یک جوابی به ما داده می شود و ما با حساب کردن زمان فرستادن و پاسخ دادن می توانیم پینگ را حساب کنیم مثلا .90ms این پکت از قسمت های Internet control Message Protocol، Internet protocol version Ethernet II, src = , dest = ، (4), src = , dest = و Frame

ما به ازای هر لایه که از سمت بالا یعنی اپلیکیشن پایین تر برویم یک Header به این بخش ها اضافه می شود.

در قسمت اول بعد از باز کردن آن ما یک سری Atrribute درون آن میبینیم مثل Type, code, checksum, Identifier (BE), Identifier (LE), Sequence Number (BE), Sequence Number (LE) و یک Data که به سمت مقصد ارسال می شود.

در یک لایه بالا تر در قسمت IP که در اینجا ورژن آن 4 است یک سری دیتا درباره اینکه IP ما چه ورژنی است، طول هدر آن چقدر است، Service field آن به چه شکلی است، Total length آن در نهایت چقدر می شود و فیلد های دیگر که مهم ترین آن آدرس مقصد و مبدا است .آنآن

در لایه بالاتر یعنی Ethernet: MAC Addrees مقصد و مبدا را فرستاده می شود که از 12 کاراکتر تولید شده و منحصر به فرد است. MAC Address برای شناسایی قطعات الکترونیکی موجود در Network استفاده می شود.

در لایه بالاتر یعنی Frame که تقریبا کاملا سخت افزاری است که دیتای مربوط به سخت افزار را به سمت سرور میفرستد مانند Section number, Interface type و ...

ICMP از پایه ترین پکت ها برای ارسال است و بقیه پکت ها معمولا لایه ها و تب های اضافه ای را دارند.

مثلا در پروتکل DNS که ما در مثال قبل استفاده کردیم به جای لایه ICMP لایه های UDP (User Datagram Protocol) و DNS(Domain name System) را داریم.

که در لایه UDP پورت مبدا، پورت مقصد و طول آن و اطلاعاتی مانند check sum, checksum status, stream index, stream packet number, Timestamps و UDP Payload که همان اطلاعات اصلی است که در حال ارسال است.

و در لایه پایین تر آن یعنی DNS اطلاعاتی مانند Transaction ID، فلگ ها، تعداد سوالات و Answer RRs، Authority RRs، Additional RRs که رکورد هایی هستند که مثلا در قسمت Answer RRs(Resource Records) رکوردهایی هستند که در جواب یک DNS query فرستاده می شوند. و همچنین اطلاعات query نیز نمایش داده می شوند که شامل Type, class, Name, Name length, Label count است.