**گزارش دستورکار ششم آزمایشگاه درس شبکه­های کامپیوتری**

نگار موقتیان، 9831062

تینا توحیدخواه، 9831134

1. **سوال 3: این لیست چه کاری انجام می­دهد؟**

دستور access-list یک لیست از IP هایی که می­توانند به روتر فوق دسترسی داشته باشند ایجاد می­کند. برای مثال در دستور موجود در دستورکار دسترسی به IP های 192.168.100.0 و 0.0.0.255 داده می­شود.

1. **سوال 4: این دستور چه کاری انجام می­دهد؟**

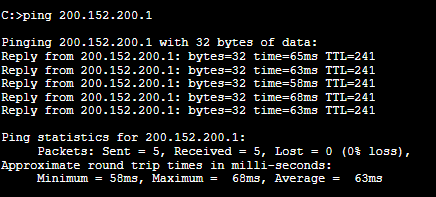
با توجه به شکل بالا اتصال برقرار شده برای ارسال این بسته از نوع keep-alive می­باشد، به این معنا که ارتباط برقرار شده پایا می­باشد و چند پیغام HTTP می­توانند بر روی یک اتصال TCP منتقل شوند.

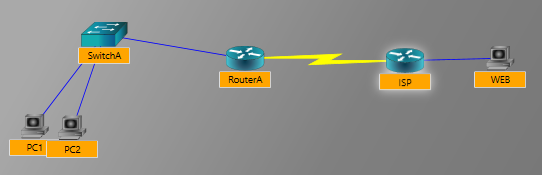
همچنین درخواست داده شده از نوع GET بوده و برای دریافت فایل index.html سایت مورد نظر فرستاده شده­است.

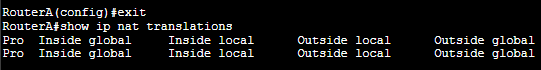
مقدار هدر User-Agent برای فرستادن اطلاعات مربوط به سیستم عامل و مرورگر استفاده شده به کار می­رود. مقدار این هدر از آن­جایی می­تواند اهمیت داشته باشد که بعضی از قابلیت­های وبسایت­ها ممکن است برای یک مرورگر خاص قابل استفاده نباشد. در این صورت باید به کاربر پیغام خاصی نشان داده شود و یا از برنامۀ جایگزینی استفاده شود. مقدار این هدر برای بستۀ فرستاده شده مانند زیر می­باشد:

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36 Edg/101.0.1210.32

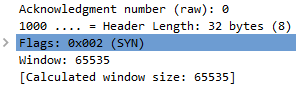
1. **سوال 5**



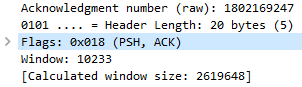




برای اولین بستۀ TCP مقدار Flags برابر با SYN می­باشد، بنابراین می­توان گفت از این بسته برای شروع ارتباط از سمت کلاینت به سرور استفاده شده­است.



همچنین برای اولین بستۀ HTPP مقدار Flags برابر با (PSH, ACK) است، به این معنا که این بسته برای اعلام ACK بوده و پیش از پر شدن segment، PUSH شده­است (زیرا ACK دادۀ کوچکی است که باید پیش از اتمام time out فرستاده شود).

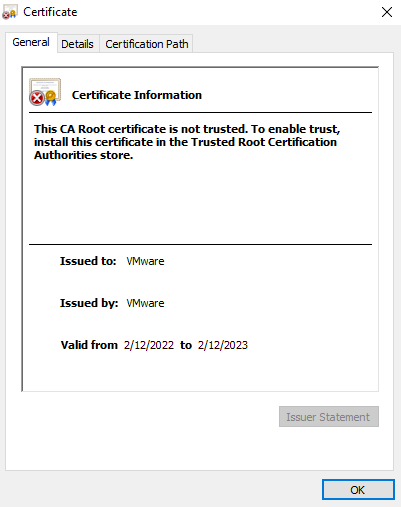


1. **تفاوت میان دو سایت اجرا شده بر روی یک وب­سرور**

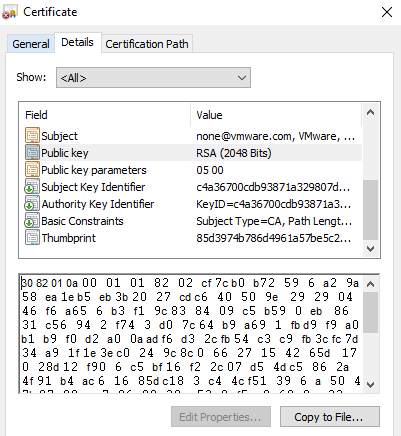
با توجه به هدرهای بسته­های منتقل شده در این اتصال، می­توان مشاهده کرد که آدرس IP و شماره پورت این دو سایت یکسان، اما مقدار هدر host آن­ها متفاوت است. از این طریق با توجه به آدرسی که در مرورگر خود وارد می­کنیم می­توانیم مشخص کنیم که می­خواهیم به کدام یک از سایت­های روی وب­سرور دسترسی داشته باشیم.

1. **اطلاعات مربوط به گواهی وبسایت ساخته شده**

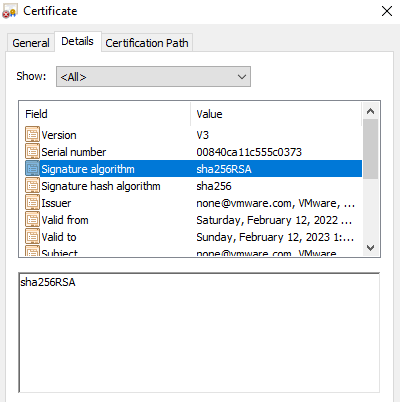
با توجه به قسمت نشان داده در شکل زیر این گواهی توسط VMware و برای VMware صادر شده و مدت اعتبار آن یک سال می­باشد



همچنین کلید عمومی صادر کننده در قسمت زیر قابل مشاهده است.



به علاوه با توجه به قسمت زیر امضای دیجیتال انجام شده از الگوریتم sha256RSA استفاده کرده و توسط الگوریتم sha256 هش شده است.



1. **بررسی متن ارتباط در پروتکل TLS**

خیر؛ متنی که برای ارتباط در این پروتکل استفاده شده بر خلاف پروتکل HTTP قابل خواندن نیست و داده­های آن رمزنگاری شده­اند، بنابراین اگر کسی بسته­های منتقل شده را شنود کرد نمی­تواند به محتوای آن­ها پی ببرد. به همین دلیل این پروتکل به نسبت HTTP می­تواند امنیت را در ارتباط تامین کند.

1. **تفاوت گواهی وبسایت google با وبسایت ساخته شده**

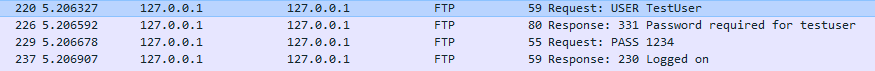
از تفاوت­های این دو گواهی می­توان به موارد زیر اشاره کرد:

1. صادر کنندۀ گواهی (GTS CA 1C3) و کسی که گواهی برای آن صادر شده (تمام وبسایت­هایی که با آدرس google.com خاتمه می­یابند) متفاوت است.
2. کلید عمومی گوگل از نوع ECC و کلید عمومی سایت ساخته شده از نوع RSA است که قدر رمزنگاری متفاوتی دارند.
3. گواهی گوگل بخش­های اضافه­ای از جمله Enhanced Key Usage، Authority Information Access، Subject Alternative Name، Certificate Poilicies، CLR Distribution Point، SCT List و Key Usage دارد.
4. گواهی سایت گوگل دارای سلسه مراتبی بوده و status آن بر خلاف وبسایت ما “This Certificate is OK” است.
5. **اطلاعات مربوط به پروتکل FTP**

همانطور که در قسمت زیر مشاهده می­شود، سرور با دریافت دستور LIST از سمت کلاینت با استفاده از پروتکل FTP-DATA لیست فایل­های موجود در دایرکتوری فعلی را برای او ارسال کرده­است.



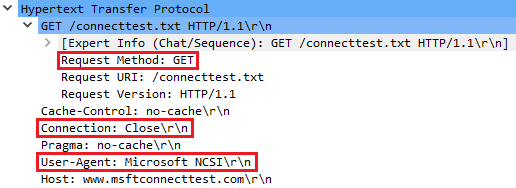
همچنین در قسمت زیر نام کاربری (TestUser) و گذرواژۀ (1234) کاربری که به فایل­ها دسترسی پیدا کرده (و آن را به عنوان ادمین اضافه کرده­ بودیم) قابل مشاهده است.



طبق اطلاعات زیر در رابطه با لایۀ transport، برای انتقال این بسته از پروتکل TCP با شماره پورت مبدا 54899 و شماره پورت مقصد 21 استفاده شده­است.



1. **هدرهای استفاده شده در پروتکل HTTP**



با توجه به شکل بالا اتصال برقرار شده برای ارسال این بسته از نوع close می­باشد، به این معنا که ارتباط برقرار شده ناپایا می­باشد و تنها یک پیغام HTTP می­تواند بر روی یک اتصال TCP منتقل شود. بنابراین پس از پاسخ سرور به کلاینت اتصال باید بسته شود.

همچنین درخواست داده شده از نوع GET بوده و برای دریافت داده از روی سایت مورد نظر فرستاده شده­است.

مقدار هدر User-Agent برای فرستادن اطلاعات مربوط به سیستم عامل و مرورگر استفاده شده به کار می­رود. مقدار این هدر از آن­جایی می­تواند اهمیت داشته باشد که بعضی از قابلیت­های وبسایت­ها ممکن است برای یک مرورگر خاص قابل استفاده نباشد. در این صورت باید به کاربر پیغام خاصی نشان داده شود و یا از برنامۀ جایگزینی استفاده شود. مقدار این هدر برای بستۀ فرستاده شده برابر با Microsoft NCSI می­باشد.

1. **مقدار هدر Flags در پروتکل TCP**

برای اولین بستۀ TCP مقدار Flags برابر با SYN می­باشد، بنابراین می­توان گفت از این بسته برای شروع ارتباط از سمت کلاینت به سرور استفاده شده­است.

