ICT – HW4 – 9831073 – Keivan Ipchi Hagh

۱.

- Secure the environment: این روش یعنی پروت ها و فایل ها و فولدر ها را امن کنیم تا در محیط اطلاعات حساس لو نروند.

- Encrypt data at rest and in flight: یعنی تمام اطلاعاتی که می آیند و میروند رمزنگاری شده توسط SSL یا TSL

- Use an authentication and authorization layer: لایه ای برای احراز هویت داشته باشیم و لایه ای برای دسترسی دادن به افراد جهت حفظ امنیت دیتا حساس

- Assign and separate roles/duties: نقش ها جدا از هم و قابلیت تشخیص داشته باشند و دسترسی های محدود و مرتبط به حیطه خود تا امکان سوء استفاده کاهش یابد.

۲. نیازمندی ها عبارتند از: Secure, Reliable, Transparent, Scalable

۳. تفاوت های این دو ورژن:

- ورژن ۵ قابلیت های forwarding و renewing و posting به تیکت های خود اضافه کرده که ورژن ۴ صرفا به صورت خام دارد.

- ورژن ۴ با استفاده از الگوریتم رمزنگاری Receiver-makes-Right کار کرده، درصورتی که ورژن ۵ از الگوریتم ASN.1 استفاده میکند.

- ورژن ۵ این سیستم، قابلیت Authentication با استفاده از کلید مشترک را دارد که ورژن ۴ آن را پشتیبانی نمیکند (transitive cross-realm authentication)

- در نسخه ۵ بازه زمانی انقضاء تیکت ها را میتوان بر اساس معیار ها (دقیقه، روز، ساعت) تعیین کرد، در صورتی که ورژن ۴ این قابلیت را ندارد.

۴. یک session key ساخته شد تا از درخواست های متعدد برای ساخت کلید جدید از کلید master جلوگیری شود، یا به عبارتی داخل آن جلسه دیگر نیاز نیست برای هر درخواست، تیکت Kerberos جدید زده شود. این مکانیسم به صورت distributed است.

۵. تفاوت این دو سیستم در آن است که برای تبادل کلید، صرفا یک شیئ کلید را ساخته و به دیگری میدهد. این کار باعث ایجاد تهدید Man-In-The-Middle میشود، اما سیستم توافق کلید یک مکانیسم دو طرفه بوده که در آن هر دو طرف بر سر یک کلید مشترک توافق میکنند. منطقی است که سربار Key Agreement بیشتر باشد چرا که نیاز بیشتری به ارتباط اولیه برای ساختن کلید مشترک دارند، پس سربار زیادی دارد تا در همه جا از آن استفاده کنیم.

پس زمانی که بخواهیم ارتباط بلند مدت ایجاد کنیم و در آن کلید های دیگر بسازیم، بهتر است از این روش استفاده کنیم اما زمانی که ارتباط کوتاهی داشته باشیم این روش به صرفه نیست و استفاده از Key Exchange بهتر است چرا که ارتباط کوتاه تر از آن است که لو رود.

۶. در حالت کلی، یک connection ارتباط بین کلاینت و سرور بوده که با استفاده از پروتکل هایی نظیر TCP صورت میگیرد و معمولا کوتاه مدت است. سرور ها پس از مدتی ارتباط را قطع میکنند. اما در Session یک وضعیت نگهداری اطلاعات سمت سرور است تا ارتباط مجدد از سر گیرد. پس یک connection میتواند قطع شود اما session از بین نرود. برای SSL هم همین داستان تکرار میشود با این تفاوت که در session پارامتر های آن رمزنگاری شده.

۷. عناصر اصلی این سرتیفیکیت:

- Email Certificates: برای ارتباط SMTP
- Digital Signature and Document Signing: امضای دیجیتال مدارک و اسناد
- TLS/SSL: امنیت ارتباطی پروتکل ها (رمزنگاری شده)
- Digital Identities: با استفاده از کلید ها
- Code Signing: مانند مورد دوم ولی در مورد اسکریپ ها و کد ها

۸. زیرا باعث میشد coupling بین پردازش handshake و رکورد ها زیاد شده و تغییر آن دشوار باشد. زیرا ابتدا یک handshake ایجاد شده (با پارامتر هایی خاص) و سپس Change Cipher Spec صدا زده شده و پیامی ارسال میشود که باعث تغییر پارامتر ها شده و یعنی handshake تمام شده و وارد فاز ارتباط میشویم. یکی بدون این دو فرایند از نظر تکنیک انجام شدنی است اما پیاده سازی و ارتقا را سخت تر میکند.

۹.

الف) SSL با رمزنگاری همه چیز باعث پیشگیری از این اتفاق میشود. چرا که Man-in-the-Middle نیاز دارد کلید SSL را بداند تا آن را رمزگشایی کرده و آن را تغییر دهد.

ب) مجدد مانند بهش قبلی SSL نمیگذارند کسی جز فرستنده و گیرنده محتوای واقعی پیام را بخواند پس نمیتواند پسورد را نیز پیدا کند.

ج) در این ارتباط handshake که کامل شده دیگر قبول نمیشود، زیرا بعد از رمزگشایی آن فیلد ها و پارامتر های محتوا مشخص کننده این موضوع هستند.

۱۰.

- Session Log File: لاگ های session
- Number of Partitions: تعداد پارتیشن های session
- Source File: اسم فایل مبدا
- Lookup File: اسم فایل مورد جست و جو
- Database Connection: مشخصات ارتباط با دیتابیس
- FTP Connection: یک کانکشن جهت ارسال و دریافت فایل
- Queue Connection: یک صف جهت نگهداری پیام ها

۱۱ Key Management یک پروتکل برای تولید و به اشتراک گذاری و نگهداری و استفاده و نابودی کلید های رمزنگاری و ارتباطی است. انواع متد های آن:

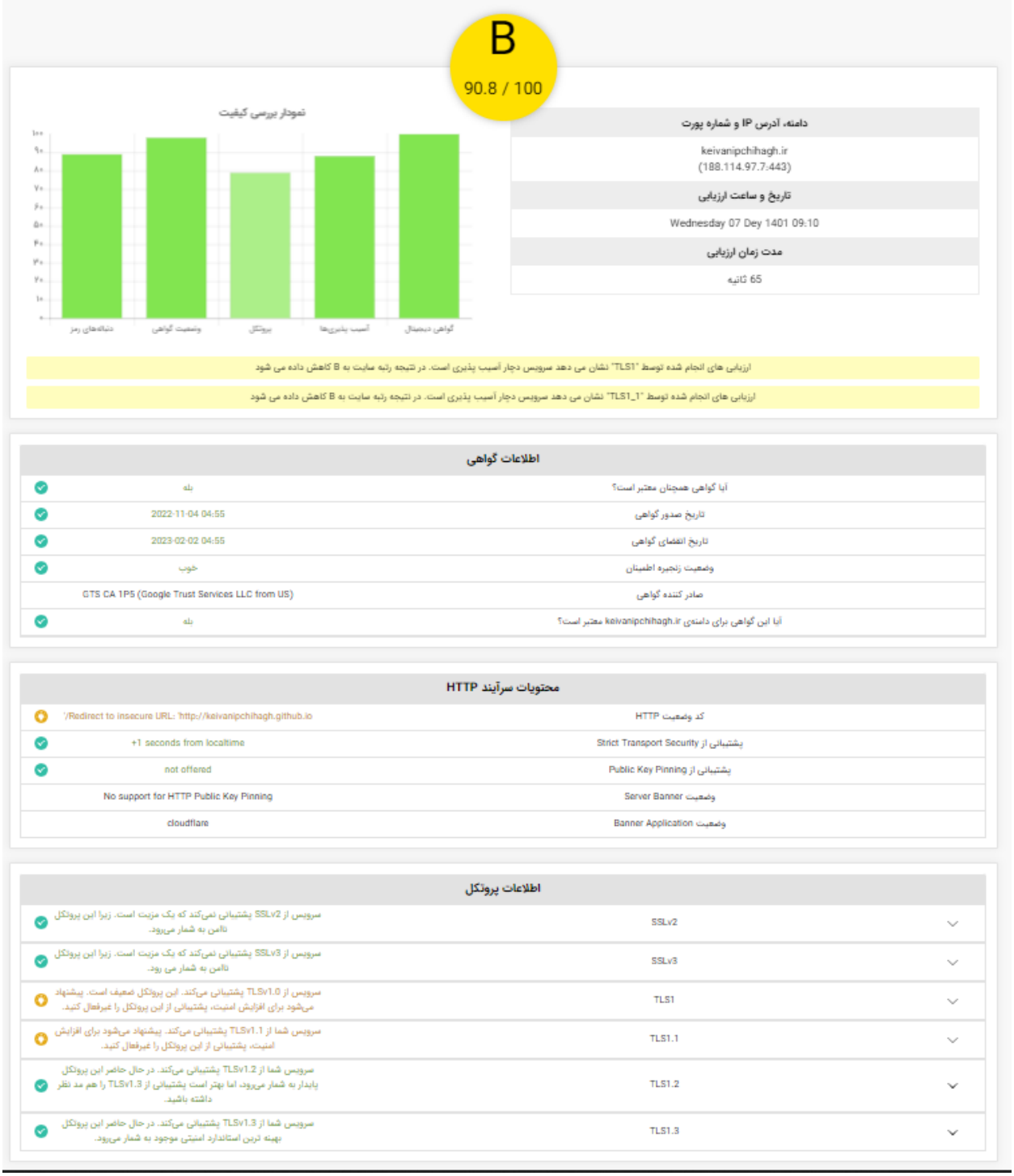
- IKE for IPsec SA Generation: یک روش انجام این کار است که تنظیمات ساده و رمزنگاری قوی دارد.
- Manual Keys for IPsec SA Generation: این روش سخت تر و ریسک بالاتری دارد چرا که اگر کلید ها لو روند خطر امنیت بالایی به سیستم های استفاده کننده وارد میکنند. بخاطر همین این سیستم رمز ها را مرتب عوض میکند و اینکار دستی انجام دادن کمی دشوار و خطا پذیر است.

ICT – HW4 – 9831073 – Keivan Ipchi Hagh

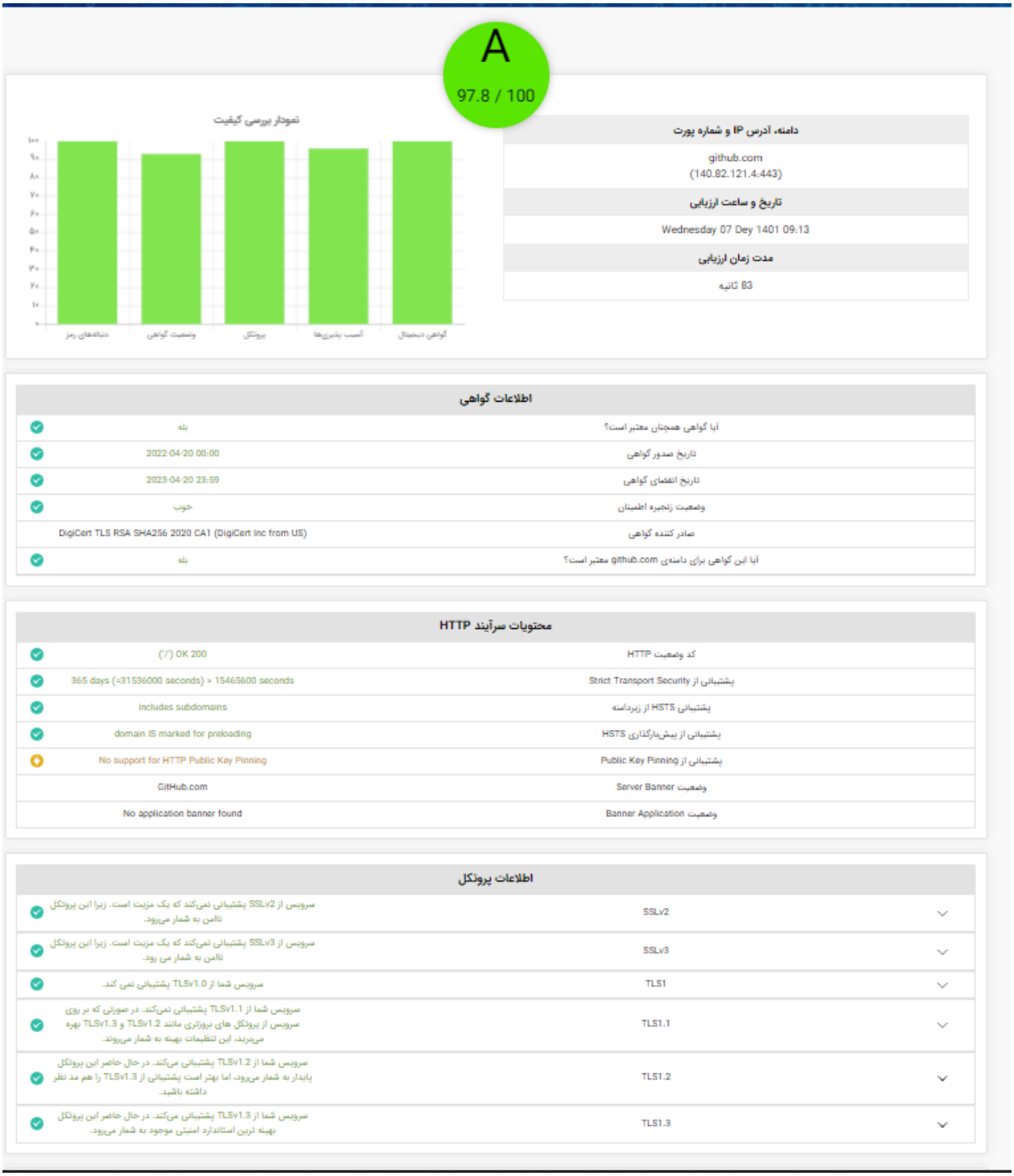
۱۲. یک پروتکل ارتباطی از جنس توافق بر SA و کلید هی مشترک ها توسط دو طرف ارتباط است که در RFC 2408 تعریف شده است. این پروتکل از UDP برای ارتباط استفاده میکند.

۱۳. توضیحات سوال ۱۲ برای این سوال نیز به کار میرود.

۱۴.



ICT – HW4 – 9831073 – Keivan Ipchi Hagh



A

97.8 / 100

نمودار بررسی کیفیت

دامنه، آدرس IP و شماره پورت
github.com (140.82.121.4:443)
تاریخ و ساعت ارزیابی
Wednesday 07 Dey 1401 09:13
مدت زمان ارزیابی
83 ثانیه

اطلاعات گواهی	
آیا گواهی همچنان معتبر است؟	بله
تاریخ صدور گواهی	2022-04-20 00:00
تاریخ انقضای گواهی	2023-04-20 23:59
وضعیت زنجیره اطمینان	خوب
صادر کننده گواهی	DigiCert TLS RSA SHA256 2020 CA1 (DigiCert Inc from US)
آیا این گواهی برای دامنه‌ی github.com معتبر است؟	بله

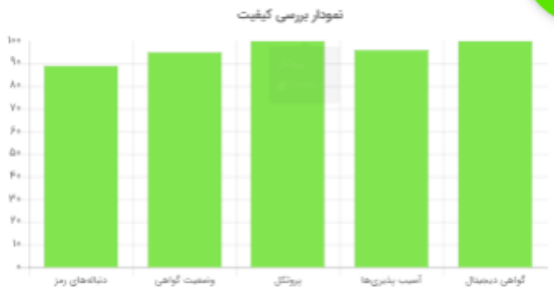
محتویات سرآیند HTTP	
کد وضعیت HTTP	('/') OK 200
پشتیبانی از Strict Transport Security	365 days (=31536000 seconds) > 15465600 seconds
پشتیبانی HSTS از زیردامنه	includes subdomains
پشتیبانی از پیش‌بارگذاری HSTS	domain IS marked for preloading
پشتیبانی از Public Key Pinning	No support for HTTP Public Key Pinning
وضعیت Server Banner	GitHub.com
وضعیت Banner Application	No application banner found

اطلاعات پروتکل		
SSLv2	سرویس از SSLv2 پشتیبانی نمی‌کند که یک مزیت است. زیرا این پروتکل ناامن به شمار می‌رود.	
SSLv3	سرویس از SSLv3 پشتیبانی نمی‌کند که یک مزیت است. زیرا این پروتکل ناامن به شمار می رود.	
TLS1	سرویس شما از TLSv1.0 پشتیبانی نمی کند.	
TLS1.1	سرویس شما از TLSv1.1 پشتیبانی نمی‌کند. در صورتی که بر روی سرویس از پروتکل های بروزتری مانند TLSv1.2 و TLSv1.3 بهره می‌برید، این تنظیمات بهینه به شمار می‌روند.	
TLS1.2	سرویس شما از TLSv1.2 پشتیبانی می‌کند. در حال حاضر این پروتکل پایدار به شمار می‌رود، اما بهتر است پشتیبانی از TLSv1.3 را هم مد نظر داشته باشید.	
TLS1.3	سرویس شما از TLSv1.3 پشتیبانی می‌کند. در حال حاضر این پروتکل بهینه ترین استاندارد امنیتی موجود به شمار می‌رود.	

ICT – HW4 – 9831073 – Keivan Ipchi Hagh

A

96 / 100



دامنه، آدرس IP و شماره پورت
kaggle.com (35.244.233.98:443)
تاریخ و ساعت ارزیابی
Wednesday 07 Dey 1401 09:13
مدت زمان ارزیابی
79 ثانیه

اطلاعات گواهی	
آیا گواهی همچنان معتبر است؟	بله
تاریخ صدور گواهی	2022-11-25 00:21
تاریخ انقضای گواهی	2023-02-23 00:21
وضعیت زنجیره اطمینان	خوب
صادر کننده گواهی	GTS CA 1D4 (Google Trust Services LLC from US)
آیا این گواهی برای دامنه‌ی kaggle.com معتبر است؟	بله

محتویات سرآیند HTTP	
کد وضعیت HTTP	('/') Found 302
پشتیبانی از Strict Transport Security	730 days (=63072000 seconds) > 15465600 seconds
پشتیبانی HSTS از زیردامنه	includes subdomains
پشتیبانی از پیش‌بارگذاری HSTS	domain IS marked for preloading
پشتیبانی از Public Key Pinning	No support for HTTP Public Key Pinning
وضعیت Server Banner	No Server banner line in header, interesting
وضعیت Banner Application	No application banner found

اطلاعات پروتکل	
SSLv2	سرویس از SSLv2 پشتیبانی نمی‌کند که یک مزیت است. زیرا این پروتکل ناامن به شمار می‌رود.
SSLv3	سرویس از SSLv3 پشتیبانی نمی‌کند که یک مزیت است. زیرا این پروتکل ناامن به شمار می رود.
TLS1	سرویس شما از TLSv1.0 پشتیبانی نمی کند.
TLS1.1	سرویس شما از TLSv1.1 پشتیبانی نمی‌کند. در صورتی که بر روی سرویس از پروتکل های بروزتری مانند TLSv1.2 و TLSv1.3 بهره می‌برید، این تنظیمات بهینه به شمار می‌روند.
TLS1.2	سرویس شما از TLSv1.2 پشتیبانی می‌کند. در حال حاضر این پروتکل پابدار به شمار می‌رود، اما بهتر است پشتیبانی از TLSv1.3 را هم مد نظر داشته باشید.
TLS1.3	سرویس شما از TLSv1.3 پشتیبانی می‌کند. در حال حاضر این پروتکل بهینه ترین استاندارد امنیتی موجود به شمار می‌رود.