ایران عرضه
فروشگاه کالاهای دانلودی
IRANARZE.IR

سوالات استخدامی امنیت شبکه

توضیحات:

- بخشی از محصول
- شامل ۲۱ سوال
- با قابلیت پرینت
- کد محصول: es1061

برای دانلود رایگان جدیدترین سوالات استخدامی امنیت شبکه، اینجا بزنید

همچنین جهت مشاهده آخرین اخبار استخدامی، اینجا بزنید

« انتشار یا استفاده غیر تجاری از این فایل، بدون حذف لوگوی ایران عرضه، مجاز می باشد »

@iranarze

@iranarze

٤ سوال ابتدایی این فایل، دارای پاسخنامه تشریحی می باشد. در صورت تمایل به دریافت سوالات بیشتر با جواب تشریحی
می توانید این محصول را از سایت ایران عرضه خریداری نمایید.
خرید محصول

❖ سوالات امنیت شبکه تالیف ایران عرضه ۱۴۰۳

۱- نوع حمله فعال را با توجه به مشخصه زیر تعیین کنید؟ (iranarze.ir)

"دزدیدن غیرفعال واحدهای دیتا و ارسال مجدد آنها با تاخیر"

۱) نقابدار ۲) تغییر پیام ۳) انکار سرویس ۴) بازخوانی

☑ **پاسخ سایت ایران عرضه: گزینه ٤** ⇦ حملات فعال شامل ایجاد تغییرات در جریان دیتا و یا خلق جریان جدیدی از داده هاست و میتوان آنها را به چهار دسته تقسیم کرد: نقابدار، بازخوانی، تغییر پیام و انکار سرویس .

یک حمله نقابدار وقتی صورت میپذیرد که شخصی یا واحدی وانمود کند که شخص یا واحد دیگری است.

حمله بازخوانی شامل دزدیدن غیر فعال واحدهای دینا و ارسال مجدد آنها با تأخیر برای ایجاد یک اثر مخرب است.

تغییر پیام بسادگی دارای این معنی است که بخشی از یک پیام قانونی تغییر داده شود.

انکار سرویس مانع کارکرد نرمال تجهیزات شده و یا از مدیریت تسهیلات ارتباطی جلوگیری می نماید.

۲- در مورد استانداردسازی اینترنت، کدامیک از موارد زیر از شروط استاندارد شدن یک مشخصه نیست؟ (iranarze.ir)

۱) دارای صور پیاده سازی واحد و مستقل باشد. ۲) از حمایت عمومی، برخوردار باشد.

۳) رقیب تکنیک های دیگر باشد. ۴) در بخش یا تمام بخش های اینترنت مفید باشد.

☑ **پاسخ سایت ایران عرضه: گزینه ۱** ⇦روند استانداردسازی: تصمیم گیری راجع به اینکه کدام RFC یک استاندارد اینترنت شود بتوسط IESG و بر اساس توصیه IETF صورت می پذیرد. برای اینکه یک مشخصه بصورت استاندارد در آید بایستی دارای شرایط زیر باشد.

• پایدار بوده و خوب درک شده باشد.

• از نظر تکنیکی رقیب تکنیک های دیگر باشد.

• دارای صور پیاده سازی متعدد، مستقل و متعامل با تجارب عملیاتی قابل توجه باشد.

• از حمایت عمومی چشمگیری برخوردار باشد.

• بطور قابل ملاحظه ای در بخشی و یا تمام بخشهای اینترنت مفید باشد.

۳- تحقق واقعی یک رمز قالبی متقارن بستگی به انتخاب چه پارامتری دارد؟ (iranarze.ir)

۱) اندازه بلوک کوچکتر ۲) اندازه کوچک کلید

۳) پیچیدگی بیشتر در الگوریتم زیر کلید ۴) وجود یک دُوررمز نگاری

☑ **پاسخ سایت ایران عرضه: گزینه ۳** ⇦ تحقق واقعی یک رمز قالبی متقارن بستگی به انتخاب پارامترهای زیر و موارد طراحی دارد:

• اندازه بلوک: هر چقدر اندازه بلوکها بزرگتر باشد با فرض ثابت بودن سایر پارامترها امنیت بیشتر ولی سرعت رمزنگاری رمزگشایی کمتر است. مصالحه مناسب در این مورد انتخاب بلوکی با طول ۱۳۸ بیت بوده که در طراحی رمز قالبی، تقریباً انتخابی همگانی است.

• اندازه کلید: اندازه بزرگتر کلید بمنزله امنیت بیشتر است. ولی ممکن است سرعت رمزنگاری، رمزگشایی را کاهش دهد. معمول ترین کلیدها در الگوریتم های مدرن دارای طول ۱۲۸ بیت هستند.

• تعداد دورها: جوهره یک رمز قالبی متقارن در این است که تنها یک دور رمزنگاری امنیت مناسبی را ایجاد نمی کند. و بنابراین دورهای بیشتری از رمزنگاری برای افزایش امنیت، مورد نیاز است. اندازه معمول در این مورد ۱۶ دور است.

• الگوریتم تولید زیر کلید: پیچیدگی بیشتر در این الگوریتم بایستی باعث افزایش پیچیدگی در شکستن رمز گردد.

• تابع دور: باز هم پیچیدگی بیشتر معمولاً بمعنای مقاومت بیشتر در مقابل کشف رمز است.

٤- برای چه پیامهایی، ECB امن تر است؟ (iranarze.ir)

۱) متون ساده کوتاه ۲) پیام بشدت ساختار یافته

۳) پیام دارای عناصر تکرار شونده ۴) پیام های دارای نظم

☑ **پاسخ سایت ایران عرضه: گزینه ۱** ⇦ یک رمز قالبی متقارن، داده ها را بصورت یک بلوک در هر زمان پردازش میکند. در DES و DES3 طول بلوک ۶۴ بیت است. برای متون ساده با طول بیشتر، لازم است تا متن به بلوکهای -۶۴ بیتی تقسیم شود (اگر لازم باشد، آخرین بلوک با بیتهای اضافی کامل میشود). ساده ترین راه برای این کار چیزی است که آن را مُود کتاب کد الکترونیکی (ECB (codebook electronic گویند که در آن در هر لحظه، ۶۴ بیت از متن ساده تحت پردازش قرار گرفته و همه بلوکهای متن با کلید واحدی پردازش میشوند. اصطلاح کتاب کد(codebook (از این جهت بکار گرفته شده است که برای یک کلید واحد، یک متن رمزشده یکتا برای هربلوک ۶۴ - بیتی دیتا حاصل میشود. بنابراین میتوان یک کتاب کد عظیمی را تصور کرد که در آن برای هر بلوک -۶۴ بیتی ممکن از متن ساده، یک متن رمزشده نظیر آن وجود داشته باشد.

در ECB، اگر همان بلوک ۶۴- بیتی متن ساده بیش از یکبار در پیام ظاهر شود، همیشه همان متن رمز شده دفعه اول حاصل خواهد شد. به همین دلیل برای پیامهای طولانی، مُود ECB ممکن است امن نباشد. اگر پیام بشدت ساختار یافته باشد، یک شکننده رمز ممکن است بتواند از این نظم سوء استفاده کند. بعنوان مثال اگر معلوم باشد که پیام همیشه با میدانهای از قبل تعریف شده معینی شروع میشود، آنگاه شکننده رمز ممکن است تعدادی زوج متن ساده- متن رمز شده را در اختیار داشته و روی آنها کار کند. اگر پیام دارای عناصر تکرار شده ای باشد که پریود تکرار آنها مضربی از ۶۴ بیت باشد، آنگاه این عناصر می توانند توسط تحلیلگر شناخته شوند. این موارد ممکن است به تحلیل رمز کمک کرده و یا ممکن است فرصتی برای جایگزینی و یا تغییر سازمان بلوک بدست دهند.

٥- جنبه مهّم اعتبارسنجی پیام چیست؟ (iranarze.ir)

۱) تایید قانونی بودن پیام ۲) تحقیق دربازه معتبر بودن منبع پیام

۳) تحقیق درباره دست نخورده بودن پیام ۴) همه موارد

٦- درپردازش کامل یک پیام برای تولید چکیده قدم سوم، کدام است؟ (iranarze.ir)

۱) وصل کردن بیت لائی ها به پیام ۲) پر کردن حافظه hash با مقادیر اولیه

۳) پردازش پیام در بلوکهای ۱۰۲۴ بیتی ۴) وصل کردن طول پیام

۷- کدام نوع الگوریتم در امضای دیجیتال مورد استفاده قرار میگیرد ولی در مبادله کلید، کاربرد ندارد؟ (iranarze.ir)

۱) الگوریتم RSA ۲) الگوریتم Diffie- Hellman

۳) الگوریتم DSS ۴) الگوریتم Elliptic - Curve

۸- طرح زیر بیانگر کدام نوع سرویس مبادله پیام ها در ورژن ۴ Kerberos می باشد؟ (iranarze.ir)

$$\mathbf{C \rightarrow TGS:} \quad ID_v \| Ticket_{tgs} \| Authenticator_c$$
$$\mathbf{TGS \rightarrow C:} \quad E(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$$
$$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_c \| AD_c \| ID_{tgs} \| TS_2 \| Lifetime_2])$$
$$Ticket_v = E(K_v, [K_{c,v} \| ID_c \| AD_c \| ID_v \| TS_4 \| Lifetime_4])$$
$$Authenticator_c = E(K_{c,tgs}, [ID_c \| AD_c \| TS_3])$$

۱) مبادله سرویس اعتبارسنجی: برای کسب بلیت اعطاکننده بلیت

۲) مبادله سرویس اعطاء- بلیت: برای کسب بلیت اعطاکننده سرویس

۳) مبادله اعتبارسنجی کلاینت/ سِرور: برای کسب سرویس

۴) ۱ و ۳

۹- کدام گزینه از نقایص محیطی نسخه چهارم Kerberos نمی باشد؟ (iranarze.ir)

۱) وابستگی به سیستم رمزنگاری. ۲) نامنظمی بایتهای پیام.

۳) وابستگی به پروتکل اینترنت. ۴) طول عمر محدود بلیت.

۱۰- دلیل رشد PGP چیست؟ (iranarze.ir)

الف. نسخه های متعددی از آن بر روی کامپیوترهای مشابه ولی با سیستم عامل متنوع کار میکنند.

ب. بر مبنای الگوریتم هایی قراردارد که بسیار امن تلقی می شوند.

ج. دارای فضای معطر ضد تشکیلاتی خود است.

د. توسط یک دولت و یک سازمان استانداردسازی شده تولید شده است.

۱) الف وب ۲) الف ود ۳) ج ود ٤) ب وج

۱۱- کدام مورد از محدودیت های پروتکل SMTP/822 نیست؟ (iranarze.ir)

۱) SMTP نمیتواند فایلهای اجرائی یا سایر اشیاء بایتری را انتقال دهد.

۲) SMTP نمی تواند داده های متنی شامل کاراکترهای زبانهای ملی را انتقال دهد.

۳) دروازه های SMTP به شبکه های پست الکترونیک X.٤٠٠ نمی توانند از پس داده های غیر متنی موجود در پیام های برآیند.

۴) سِرورهای SMTP ممکن است پیامهای کوتاه تر از اندازه معینی را نپذیرند.

۱۲- PGP با چه هدفی از اعداد شبه تصادفی استفاده میکند؟ (iranarze.ir)

۱) برای تولید کلیدهای اجلاس

۲) برای تولید جفت کلیدهای RSA

۳) به عنوان بذر اولیه در تولید اعداد شبه تصادفی.

۴) برای تولید ورودی دیگر در خلال تولید اعداد شبه تصادفی.

۱۳- در سرآیندهای اعتبارسنجی، منظور از میدان Reserved (16 bits) چه می باشد؟ (iranarze.ir)

۱) یک اتحاد امنیتی را مشخص میکند. ۲) برای مصارف آینده رزرو شده است.

۳) نوع سرایند بعدی را مشخص می کند. ۴) یک شمارنده که که اندازه آن بطور یکنواخت زیاد میشود.

۱٤-پیامد تهدید "انکار سرویس" کدام است؟ (iranarze.ir)

۱) از بین رفتن اطلاعات ۲) لو رفتن ماشین

۳) ایجاد اذیت و آزار ۴) معرفی غلط کاربر

۱۵- کدامیک از گردش اسناد SET زیر به فروشنده اجازه میدهد تا از دروازه پرداخت، تقاضای پول نماید؟ (iranarze.ir)

۱) نوع Credit ۲) نوع payment capture

۳) نوع purchase Request ۴) نوع Merchant registration

۱٦- در مدل امنیتی USM ، تهدید زیر مربوطبه کدام گزینه است؟ (iranarze.ir)

" مشاهده یک مجموعه از فرامین که کلمات عبور را تغییر میدهد، یک حمله کننده را قادر خواهد ساخت تا کلمات عبور جدید را بدست آورد "

۱) افشا ۲) نقاب گذاری ۳) دستکاری اطلاعات ۴) دستکاری جریان پیام

۱۷- مشخصه مهاجم از نوع "سواستفاده کننده" چه می باشد؟ (iranarze.ir)

۱) کاربر غیر قانونی که به برنامه ها بطور قانونی دست می یابد.

۲) فردی که کنترل سوپروایزری سیستم را بدست می گیرد.

۳) فردی که اشتراک یک کاربر قانونی را مورد سواستفاده قرار می دهد.

۴) کاربر قانونی که به دیتا و برنامه یی که قانونا مجاز نیست، دست می یابد.

۱۸- منظور از استراتژی کنترل غیرفعال کلمه عبور چیست؟ (iranarze.ir)

۱) سیستم رمز هراز گاه غیرفعال شود.

۲) سیستم هرچند وقت یکبار برنامه شکستن کلمه عبور داخلی خود را اجراکند.

۳) قابلیت حدس کلمه رمز را نداشته باشد.

۴) همه موارد

۱۹- کدام گزینه از قابلیتهای یک کِرم شبکه جهت تکثیر خود نمی باشد؟ (iranarze.ir)

۱) به عنوان یک کاربر در یک سیستم دوردست وارد شده وفرامینی را جهت کپی کردن خود بکار میبرد.

۲) هر لحظه قادر به تخریب کپی خود بر روی دیگر سیستم ها می باشد.

۳) یک کپی خود را در سیستم دیگر اجرا می کند.

۴) کرم کپی خود را به سیستم های دیگر پست میکند.

۲۰- کاربرد روش" Topological " در استراتژی های عمل اسکن کردن چیست؟ (iranarze.ir)

۱) هر میزبان به دام افتاده به آدرس های تصادفی نفوذ کرده وبرای هرکدام از یک seed مختلف استفاده میکند.

۲) اگر میزبانی در پشت یک دیوار آتش آلوده شود این میزبان بدنبال آلوده کردن اهداف دیگر خواهد رفت.

۳) پس از تهیه لیست از ماشینهای دارای پتانسیل آسیب پذیری شروع به آلوده کردن آنها می نماید.

۴) از اطلاعات ماشین قربانی استفاده کرده تا بتواند میزبانهای جدید برای اسکن پیدا کند.

۲۱- دو قانونی را که باید یک سیستم امن چند سطحه رعایت کند، کدام است؟ (iranarze.ir)

۱) نخواندن سطح بالاتر، ننوشتن سطح پایینتر

۲) نخواندن سطح بالاتر، اما نوشتن سطح پایینتر

۳) نخواندن سطح پایینتر و ننوشتن سطح بالاتر

۴) خواندن سطح بالاتر و نوشتن سطح پایینتر