- اعداد تصادفی واقعی:
  - برای تولید جفت کلیدهای RSA
  - به عنوان بذر اولیه در تولید اعداد شبه تصادفی
  - برای تولید ورودی دیگری در خلال تولید اعداد شبه تصادفی
- اعداد شبه تصادفی
  - برای تولید کلیدهای اجلاس
  - برای تولید بردارهای شروع (IV) همراه با کلید اجلاس در مُود رمزنگاری CFB

۲۵- کدام سرویسها به ترتیب توسط پروتکل های AH و ESP ایجاد میشوند؟ ( )

۱) محرمانگی دیتا- اعتبارسنجی منبع دیتا ۲) محرمانگی دیتا- صحت دیتا در حالت غیر اتصالی

۳) کنترل دستیابی- محرمانگی دیتا ۴) محرمانگی محدود جریان ترافیک- کنترل دستیابی

☑ ۳ ⇦ سرویسهای IPSec : IPSec سرویسهای امنیتی در سطح IP را بنحوی فراهم می آورد که سیستم قادر است تا پروتکلهای امنیتی لازم را انتخاب کرده، الگوریتم های لازم برای سرویس ها را تعیین نموده و کلیدهای رمزنگاری لازم برای سرویسهای درخواست شده را در محل مناسب قرار دهد. دو پروتکل برای ایجاد امنیت بکار میرود یک پروتکل اعتبار سنجی که بتوسط سرآیند پروتکل یعنی Authentication Header (AH) شناسایی شده و یک پروتکل مخلوط رمزنگاری/ اعتبار سنجی که توسط فرمت بسته آن پروتکل Encapsulating Security Payload (ESP) شناسائی میگردد. سرویس ها بقرار زیراند:

کنترل دست یابی

صحت دیتا در حالت غیر اتصالی

اعتبار سنجی مبدأ دیتا

رد بسته های بازخوانی شده

محرمانگی رمزنگاری)

محرمانگی محدود جریان ترافیک

جدول زیر نشان میدهد که کدام سرویسها توسط پروتکلهای AH و ESP ایجاد میشوند برای ESP دو حالت وجود دارد حضور و یا عدم حضور اعتبار سنجی بصورت اختیاری AH و ESP هر دو محمل هایی برای کنترل دست یابی اند که مبتنی بر توزیع کلیدهای رمزنگاری و مدیریت جریانهای ترافیک مرتبط با این پروتکل های امنیتی میباشند.

	AH	ESP (فقط رمزنگاری)	ESP (رمزنگاری بعلاوه اعتبارسنجی)
کنترل دست‌یابی	✓	✓	✓
صحت دیتا در حالت غیراتصالی	✓		✓
اعتبارسنجی منبع دیتا	✓		✓
رد بسته‌های بازخوانی شده	✓	✓	✓
محرمانگی دیتا		✓	✓
محرمانگی محدود جریان ترافیک		✓	

۲۶- در سرآیندهای اعتبارسنجی، منظور از میدان Reserved (16 bits) چه می باشد؟ ( )

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.

☑ ۲ ⇦ سرآیند اعتبارسنجی شامل میدانهای زیر است:

(Next Header (8) bits : نوع سرایندی که بلافاصله پس از این سرآیند قرار می گیرد را مشخص می کند.

(Payload Length (8 bits : طول سرآیند اعتبار سنجی بر حسب کلمات ۳۲ بیتی منهای ۲. به عنوان مثال، طول پیش فرض میدان اعتبار سنجی دیتا ۹۶ بیت و یا ۳ کلمه -۳۳ بیتی است. با یک سرآیند ثابت سه کلمه ای، شش کلمه در سرآیند وجود خواهد داشت و اندازه میدان Payload Length برابر ۴ خواهد بود.

(Reserved (16 bits: برای مصارف آینده رزرو شده است.

(Security Parameters Index (32 bits:یک اتحاد امنیتی را مشخص میکند.

(Sequence Number(32bit : یک شمارنده که اندازه آن بطور یکنواخت زیاد میشود و بعداً مورد بحث قرارخواهد گرفت.

(Authentication Data (variable: یک میدان با طول متغیر (که بایستی مضرب صحیحی از کلمات ۳۲ بیتی باشد) که شامل (Integrity CheckValue (ICV یا MAC برای این بسته است و بعداً در مورد آن صحبت خواهیم کرد.

۲۷- کاربرد Key Exchange Payload چیست؟ ( )

۱) جهت تعیین هویت طرفین ارتباط. ۲) انتقال یک گواهینامه کلید-عمومی.

۳) تعریف یک تبدیل امنیتی. ۴) استفاده برای تکنیک های متنوع مبادله کلید.

☑ ٤ ⇦ Key Exchange payload میتواند برای تکنیکهای متنوع مبادله کلید بکار رود که شامل Diffie -Hellman،Oakly و مبادله کلید RSA-based برای PGP است.

میدان دیتایKey Exchange، شامل دیتای مورد نیاز برای تولید یک کلید اجلاس بوده و مستقل از الگوریتم مبادله کلید بکار رفته است.

۲۸-پیامد تهدید "انکار سرویس" کدام است؟ ( )

۱) از بین رفتن اطلاعات ۲) لو رفتن ماشین

۳) ایجاد اذیت و آزار ۴) معرفی غلط کاربر

☑ betafile.ir ۳ ⇦ جدول زیر خلاصه ای از انواع تهدیدهای امنیتی که در استفاده از وِب با آنها مواجهیم را نشان میدهد. یک روش برای دسته بندی این تهدیدها این است که آنها را بر اساس حملات غیرفعال و فعال دسته بندی کنیم. حملات غیرفعال شامل استراق سمع ترافیک شبکه بین مرورگر و سِرور و دستیابی به اطلاعات یک سایت وِب است که قرار بوده است محرمانه باشد. حملات فعال شامل جا زدن خود بجای شخص دیگر، تغییر پیام های در حال ترانزیت بین کلاینت و سِرور و همچنین تغییردادن اطلاعات یک وِب سایت هستند. راه دیگری برای طبقه بندی تهدیدهای وِب این است که آنها را بر حسب محل تهدید طبقه بندی نمائیم : سِرور وِب، مرورگر وِب و ترافیک شبکه ای بین مرورگر و سِرور..

	تهدیدها	پیامد تهدیدها	روش‌های مقابله
صحت	• دستکاری در داده‌های کاربر • مرورگر اسب تروا • دستکاری حافظه • دستکاری ترافیک پیام در حال ترانزیت	• از بین رفتن اطلاعات • لورفتن ماشین • آسیب‌پذیری به انواع تهدیدهای دیگر	استفاده از جمع‌های کنترلی مرتبط با رمزنگاری
محرمانگی	• استراق سمع روی اینترنت • دزدی اطلاعات از سِرور • کسب اطلاعات در مورد پیکربندی شبکه • کسب اطلاعات در مورد این‌که کدام کلاینت با سِرور در تماس است.	• از بین رفتن اطلاعات • از بین رفتن محرمانگی	رمزنگاری، استفاده از پروکسی‌های وِب
انکار سرویس	• قطع رشته‌های ارتباطی کاربر • ایجاد سیلابی از تهدیدهای ساختگی • پرکردن حافظه‌های کامپیوتر • ایزوله کردن ماشین با حملات DNS	• ایجاد وقفه • ایجاد اذیت و آزار • بازماندن کاربر از انجام کارهای عادی	جلوگیری از این تهدیدها مشکل است
اعتبارسنجی	• جعل هویت کاربران قانونی • تقلب در داده‌ها	• معرفی غلط کاربر • ایجاد باور نسبت به صحت اطلاعات غلط	تکنیک‌های رمزنگاری

}RUBI۹۷{ یک مقایسه از تهدیدهای امنیتی وِب

( ) کدام است؟ "۲۹ Handshake- مشخصه "پروتکل

الف. به سرور وکلاینت اجازه می دهد - که هویت یکدیگر را تایید نمایند.

ب. برای رساندن هشدارهای مرتبط با SSL به واحد نظیر بکار میرود.

ج. ساده ترین پروتکل مختصSSL است.

د. پیچیده ترین بخش SSL مربوط به این پروتکل است.

۱) الف وب. ۲) ب وج ۳) ج ود. ۴) الف ود

☑ ٤ ⇦ پروتکل Handshake: پیچیده ترین بخش SSL مربوط به پروتکل Handshake است. این پروتکل به سِرور و کلاینت اجازه میدهد تا هویت یکدیگر را تایید نموده و راجع به یک الگوریتم رمزنگاری و MAC و همچنین کلیدهای رمزنگاری که قرار است دیتای ارسال شده در یک رکورد SSL را محافظت کنند توافق نمایند. پروتکل Handshake قبل از اینکه هیچ گونه

پروتکل Handshake شامل یک سری پیام های رد و بدل شده بین کلاینت و سِرور است. هر پیام شامل سه میدان است:

نوع (۱بایت): نمایشگر یکی از ۱۰ نوع پیام متفاوت است. جدول زیر انواع پیامهای مرتبط را نشان داده است.

طول (۳بایت): طول پیام بر حسب بایت.

محتوا (۰ بایت ≤): پارامترهای مرتبط با این پیام این پارامترها در جدول زیر لیست شده اند.

نوع پیام	پارامترها
hello_request	null
client_hello	version, random, session id, cipher suite, compression method
server_hello	version, random, session id, cipher suite, compression method
certificate	chain of X.509v3 certificates
server_key_exchange	parameters, signature
certificate_request	type, authorities
server_done	null
certificate_verify	signature
client_key_exchange	parameters, signature
finished	hash value

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

۱) نوع Credit ۲) نوع payment capture

۳) نوع purchase Request ۴) نوع Merchant registration

☑ ۲ ⇦ نوع payment capture ، به فروشنده اجازه میدهد تا دروازه پرداخت، تقاضای پول نماید.

Cardholder registeration	دارندگان کارت قبل از این که بتوانند پیام‌های SET را برای فروشندگان بفرستند، بایستی در یک CA ثبت نام شده باشند.
Merchant registeration	فروشندگان قبل از این که بتوانند پیام‌های SET را با مشتریان و دروازه‌های پرداخت مبادله نمایند، بایستی در یک CA ثبت نام شده باشند.
Purchase Request	پیامی که از جانب مشتری برای فروشنده ارسال شده و شامل OI برای فروشنده و PI برای بانک است.
Payment authorization	مبادلهٔ بین فروشنده و دروازهٔ پرداخت تا مقدار مشخصی پول برای یک خرید را از طریق یک کارت اعتبار بخشد.
Payment capture	به فروشنده اجازه می‌دهد تا از دروازهٔ پرداخت تقاضای پول نماید.

۳۱- کدام گزینه از مزایای معماری SNMP می باشد؟ ( )

۱) نقش موجودیت SNMP توسط مدولهائی که در آن پیاده سازی شده اند تعریف میشود.

۲) ساختار پودمانی (مدولار) مشخصه ها باعث میشود که بتوان نسخه های مختلفی از هر مدول را تعریف کرد.

۳) قابلیت جایگزین کردن و یا ارتقاء توانائیها برای جنبه های معینی از SNMP، بدون نیاز به عبور به نسخه استاندارد شده بالاتر ایجاد می گردد.

۴) همه موارد

☑ ٤ ⇦ موجودیت SNMP : هر موجودیت (entity) SNMP شامل یک موتور (engine) SNMP است.

یک موتورSNMP عملیات ارسال و دریافت پیامها، اعتبار سنجی و رمزنگاری/رمزگشایی پیامها و کنترل دستیابی به موضوعات مدیریت شده را پیاده سازی می نماید. این عملیات برای سرویس دادن به یک یا چند کاربرد بتوسط موتور SNMP پیکربندی شده و یک موجودیت SNMP را تشکیل میدهند.

هم موتور SNMP و هم کاربردهای پشتیبانی شده توسط این موتور، بصورت مجموعه ای از مدولهای گسسته تعریف شده اند. این نوع معماری مزایای متعددی دارد. اول این که نقش موجودیت SNMP توسط مدولهائی که در آن پیاده سازی شده اند تعریف میشود. تعداد مشخصی از مدول ها، مورد نیاز یک عامل SNMP بوده در حالیکه تعداد مشخص دیگری (ممکن است همپوشانی هم وجود داشته باشد) مورد نیاز یک مدیر SNMP هستند. ثانیاً ساختار پودمانی (مدولار) مشخصه ها باعث میشود که بتوان نسخه های مختلفی از هر مدول را تعریف کرد. این بنوبه خود باعث میشود که (۱) قابلیت جایگزین کردن و یا ارتقاء توانائیها برای جنبه های معینی از SNMP، بدون نیاز به عبور به نسخه استاندارد شده بالاتر (مثلاً SNMPv٤)، ایجاد گردد و ۲) بطور روشنی روشهای همزیستی استراتژی، و های عبور تعیین شود (RFC ۲۵۷٦).

۳۲- در مدل امنیتی USM ، تهدید زیر مربوطبه کدام گزینه است؟ ( )

" 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

☑ ۱ ⇦ مدل امنیتی کاربر: RFC 2574 مدل امنیتی کاربر User security Model(USM) راتعریف می کند.USM سرویس های اعتبار سنجی و محرمانگی را برای SNMP فراهم می آورد. USM علی الخصوص برای حفظ امنیت در برابر تهدیدهای زیر طراحی شده است:

- دستکاری اطلاعات: یک موجودیت ممکن است یک پیام در حال ترانزیت، که توسط یک موجودیت معتبر تولید شده است. را طوری تغییر دهد که باعث انجام عملیات مدیریتی غیر مجاز گردد. نتیجه این تهدید این است که یک موجودیت غیر مجاز بتواند هر پارامتر مدیریتی که از جمله شامل پیکربندی، عملیات و حسابرسی است راعوض کند.
- نقاب گذاری: عملیات مدیریتی غیر مجاز برای یک موجودیت، ممکن است بتوسط آن موجودیت که نقاب یک موجودیت مجاز را به چهره گذاشته است، انجام شود.

- دستکاری جریان پیام: SNMP برای کاربرد روی یک پروتکل حمل و نقل بدون اتصال طراحی شده است. اینتهدید وجود دارد که پیام های SNMP جابجا شده، به تاخیر افتاده و یا بازخوانی شده و به عملیات غیر مجاز مدیریتی منجر گردند. برای مثال پیامی برای reboot کردن یک دستگاه ممکن است کپی شده و در آینده مجدداً ارسال گردد.
- افشا: یک موجودیت ممکن است مبادلات بین یک مدیر و یک عامل را مشاهده کرده و از این طریق اندازه های موضوعات مدیریت شده و همچنین پیشامدهای قابل اخطار را کشف کند. برای مثال، 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.

USM برای مقابله با دو تهدید زیر طراحی نشده است:

- انکار سرویس: یک حمله کننده ممکن است مانع مبادلات بین یک مدیر و یک عامل شود.
- تحلیل ترافیک: یک حمله کننده ممکن است الگوی عمومی ترافیک بین مدیران و عوامل را مشاهده نماید.

۳۳- در رابطه با مدیریت کلید و عدم لو رفتن کلید کدام گزینه صحیح است؟ ( )

الف. کلیدهای یک کاربر برای عامل های مختلف متفاوت است.

ب. هرکاربردارای یک کلید اعتبارسنجی و کلید رمزنگاری یکتا است.

ج. کلیدهای یک کاربر برای عوامل یکسان، متفاوت است.

د. هر کاربر فقط دارای دو کلید رمزنگاری می باشد.

۱) الف ود. ۲) الف وب ۳) ب ود. ۴) ج ود

☑ ۲ ⇦ برای مدیریت کلید اهداف زیر را می توان تعریف نمود.

▪ هر سیستم عامل SNMP در یک شبکه گسترده، دارای یک کلید یکتا برای هر کاربر معتبری است که می خواهد آن را مدیریت نماید. اگر کاربران متعددی به عنوان مدیران معتبر شناخته می شوند، عامل دارای یک کلید اعتبار سنجی یکتا و یک کلید رمزنگاری یکتا برای هر کاربر است، در نتیجه اگر کلید یک کاربر لو برود، کلیدهای کاربران دیگر لو رفته نخواهند بود.

▪ کلیدهای یک کاربر برای عاملهای مختلف متفاوت اند. بنابراین اگر یک عامل لو برود، تنها کلیدهای کاربر برای آن عامل لو رفته و کلیدهای متعلق به عاملان دیگر لو رفته نخواهند بود.

▪ مدیریت شبکه از هر نقطه شبکه صرف نظر از پیکربندی سیستم مدیریت شبکه (NMS)، امکان پذیر است. این امر به کاربر اجازه میدهد تا عملیات مدیریتی را از هر ایستگاه مدیریت انجام دهد. این قابلیت توسط الگوریتم تبدیل کلمه عبور- به -کلید امکان پذیر است

۳٤- مشخصه مهاجم از نوع "سواستفاده کننده" چه می باشد؟ ( )

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.

☑ ٤ ⇦ یکی از دو تهدید عمده امنیت سیستم، مهاجمین هستند (دیگری ویروسها می باشند)، که معمولاً از آنها با نام هَکر (hacker) و یا کِرکِر (cracker) یاد میشود. در یکی از مطالعات مهم مربوط به مهاجمین، آندرسن [۸۰ANDE] سه دسته از مهاجمین، را شناسایی نموده است.

• نقاب دار (Masquerader) : فردی است که مجاز به استفاده از کامپیوتر نیست ولی از کنترل های دستیابی به سیستم عبور کرده و اشتراک یک کاربر قانونی را مورد سوء استفاده قرار می دهد.

• سوء استفاده کننده (Misfeasor): یک کاربر قانونی است که به دیتا، برنامه ها و یا منابعی دست می یازد که قانوناً اجازه دستیابی به آنها را ندارد. این فرد ممکن است مجاز به دستیابی به آنها باشد ولی از آنها بطور غیر قانونی در جهت خواسته های خود استفاده می نماید.

•کاربر خُفیه (Clandestine User): فردی است که کنترل سوپروایزری سیستم را بدست گرفته و از این کنترل برای فرار از شناخته شدن و یا خنثی کردن عملیات شناسایی استفاده نماید.

۳۵- کدامیک از موارد زیر از معیارهای تشخیص تهاجم مبتنی بر پروفایل مفید محسوب <u>نمی شوند</u>؟ ( )

۱) شمارنده، بعنوان یک عدد صحیح غیر منفی که نمی تواند کم شود.

۲) فاصله زمانی بین دو ورود به سیستم از سوی یک کاربر مشخص باشد.

۳) پیمانه، بعنوان یک عدد صحیح غیر منفی که فقط می تواند زیاد شود.

۴) زمان سنج که زمان بین وقوع دو پیشامد یکسان را نشان میدهد.

☑ ۳ ⇦ مثال هایی از معیارهای تشخیص، که در تشخیص تهاجم مبتنی بر پروفایل مفید هستند، بقرار زیراند:

• شمارنده : یک عدد صحیح غیر منفی که می تواند زیاد شده ولی نمیتواند کم شود، مگر اینکه با یک فرمان مدیریتی صفر گردد. معمولاً شمارش یک پیشامد در طول دوره زمانی مشخصی مورد توجه است. نمونه هایی از این دست شامل تعداد تلاش ها برای ورود به سیستم از طرف یک کاربر مشخص در طول یک ساعت، تعداد دفعات اجرای یک فرمان در زمان یک اجلاس، و یا تعداد تلاشهای تا موفق برای ورود به سیستم از طریق کلمات عبور غلط ظرف یک دقیقه است.

• پیمانه: یک عدد صحیح غیر منفی که میتواند هم زیاد و هم کم شود. یک پیمانه معمولاً برای اندازه گیری مقدار یک چیز بکار می رود. مثالهای این مورد نظیر تعداد اتصالات منطقی به یک برنامه کاربردی و یا تعداد پیام های خروجی است که برای پردازش در صف انتظار قرار گرفته اند.

• زمان سنج: زمان بین وقوع دو پیشامد یکسان را نشان میدهد. مثال امر، فاصله زمانی بین دو ورود به سیستم از سوی یک کاربر مشخص است.

• بکارگیری منابع: اندازه کّمی منابعی که در طول زمان مشخصی بکار گرفته شده اند را نشان می دهد. نمونه این موارد عبارت از تعداد صفحات چاپ شده در خلال یکبار اتصال به سیستم و یا زمان صرف شده برای اجرای یک برنامه است.

۳۶- منظور از استراتژی کنترل غیرفعال کلمه عبور چیست؟ ( )

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

☑ ۲ ⇦ یک استراتژی کنترل غیر فعال کلمه عبور این است که خود سیستم هر چند وقت یکبار برنامه شکستن کلمه عبور داخلی خود را اجرا کرده تا کلمات عبور قابل حدس را پیدا کند. سیستم اگر بتواند یک کلمه عبور را با حدس بدست آورد آن را حذف کرده و کاربر را از این موضوع مطلع میکند. این تاکتیک چندین نقطه ضعف دارد. اول اینکه اگر قرار باشد تا عمل درست انجام شود. منابع سیستم را بشدت بکار خواهد گرفت. دوم اینکه یک دشمن مصمم که قادر به ربودن یک فایل کلمات عبور باشد میتواند ساعتها و یا حتی روزها تمام زمان CPU را برای دسترسی به هدف خود بکار گیرد. علاوه بر این هر کلمه عبور، موجود تا زمانی که کنترل غیر فعال کلمه عبور آن را کشف کند قابل تعرض خواهد ماند.

۳۷- ویژگی مطرح شده ی زیر نشان دهنده کدام نرم افزار "بداندیش" است؟ ( )

"کد مختص به یک آسیب پذیر منفرد و یا مجموعه ای از آسیب پذیرها"

۱) نرم افزار Exploits　　۲) بداندیش Virus Worm

۳) بداندیش Auto rooter　　۴) نرم افزار Zombie

☑ ۱ ⇦ کد مختص به یک آسیب پذیر منفرد ویا مجموعه ای از آسیب پذیرها، مربوط به نرم افزار بداندیش Exploits است.

نام	توصیف
Virus	خود را به یک برنامه متصل کرده و کپی‌هائی از خود را به برنامه‌های دیگر منتقل می‌کند
Worm	برنامه‌ای که کپی‌های خود را به کامپیوترهای دیگر منتقل می‌کند
Logic Bomb	وقتی فعال می‌شود که پیشامد خاصی روی دهد
Trojan Horse	برنامه‌ای که شامل قابلیت‌های اضافی غیرمنتظره است
Backdoor (trapdoor)	دستکاری یک برنامه بطوری که دست‌یابی غیرمجاز به عملیاتی را امکان‌پذیر نماید
Exploits	کُد مختص به یک آسیب‌پذیری منفرد و یا مجموعه‌ای از آسیب‌پذیری‌ها
Downloaders	برنامه‌ای که اقلام جدیدی را روی ماشین مورد تهاجم نصب می‌کند. یک downloader معمولاً با یک نامهٔ الکترونیک ارسال می‌شود
Auto-rooter	ابزارهای یک نفوذگر بداندیش که از آنها برای ورود به ماشین‌های جدید از راه دور استفاده می‌کند
Kit (virus generator)	مجموعه‌ای از ابزارها برای تولید ویروس‌های جدید بصورت خودکار
Spammer programs	برای ارسال حجم زیادی از هَرزنامه‌های الکترونیک بکار می‌رود
Flooders	برای حمله به شبکه‌های کامپیوتری از طریق ایجاد حجم بالائی از ترافیک بکار می‌رود تا یک حملهٔ انکار سرویس (DoS) را سازمان دهد
Keyloggers	حرکات صفحه کلید در یک کامپیوتر مورد حمله را می‌یابد
Rootkit	مجموعه‌ای از ابزارهای نفوذگری که پس از اینکه نفوذگر به سیستم راه یافت از آنها برای دسترسی به root-level استفاده می‌کند
Zombie	برنامه‌ای که روی یک ماشین آلوده شده فعال می‌شود تا حملات بر روی ماشین‌های دیگر را سامان دهد

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

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.

☑ ۲ ⇦ یک کرم یک برنامه است که میتواند خود را تکثیر کرده و کپی های تکثیرشده را در عرض یک شبکه کامپیوتری از رایانه ای به رایانه دیگر منتقل نماید. پس از ورود به یک سیستم، کرم ممکن است فعال شده، شروع به تکثیر نموده و مجدداً انتشار یابد.

برای تکثیر خود، یک کِرم شبکه از برخی قابلیتهای شبکه

-تسهیلات پست الکترونیک: یک کرم کپی خود را به سایر سیستم ها پست می کند.

- قابلیت اجرا در دور دست: یک کرم یک کپی خود را در سیستم دیگر اجرا می کند.

- قابلیت ورود به سیستم در دوردست: یک کرم به عنوان یک کاربر در یک سیستم دوردست وارد شده و سپس فرامینی را بکار میگیرد که خود را از یک سیستم به سیستم دیگر کپی نماید.

۳۹- برنامه های ساکن در حافظه، که ویروس را با فعالیت آن در یک برنامه آلوده شده شناسایی می کنند، چه می گویند؟

۱) نسل اول آنتی ویروس ها ۲) نسل چهارم آنتی ویروس ها

۳) نسل سوم آنتی ویروس ها ۴) نسل دوم آنتی ویروس ها

☑ ۳ ⇦ نسل سوم آنتی ویروس ها، برنامه های ساکن در حافظه هستند که ویروس را با فعالیت آن، و نه با ساختار آن، در یک برنامه آلوده شده شناسایی میکنند. حسن چنین برنامه هایی این است که لازم نیست تا امضاها و قواعد ذهنی برای ردیف وسیعی از ویروسها را تولید کرد بلکه تنها کافی است که مجموعه کوچکی از فعالیتها که نمایشگر تلاش برای آلوده سازی سیستم است را شناسایی نموده و سپس برای پاک سازی مداخله کرد.

٤٠- 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.

☑ ٤ ⇦ MIRK04 از استراتژیهای زیر برای عمل اسکن نام می برد:

Random، هر میزبان به دام افتاده، به آدرسهای تصادفی در فضای آدرسهای IP نفوذ کرده و برای هر کدام از یک seed مختلف استفاده میکند. این تکنیک حجم بالایی از ترافیک اینترنت را بوجود می آورد که ممکن است. حتی قبل از آغاز حمله اصلی سرویس را مختل سازد.

Hit-List حمله کننده ابتدا یک لیست طولانی از ماشین هایی که پتانسیل آسیب پذیری دارند را تهیه می کند. این امر ممکن است به کندی و در طول زمان انجام شود تا از تشخیص این که حمله ای در شرف وقوع است اجتناب شود. وقتی که لیست تهیه و جمع آوری گردید حمله کننده شروع به آلوده کردن ماشین های موجود در لیست می نماید. به هر ماشین آلوده شده، بخشی از لیست برای اِسکن کردن واگذار میشود. این استراتژی به اسکن سریع تعداد زیادی ماشین در مدت کوتاهی منجر شده که میتواند تشخیص وقوع آلودگی را با دشواری مواجه سازد.

Topological این روش از اطلاعات موجود در ماشین قربانی استفاده کرده تا میزبانهای جدیدی را برای اِسکن کردن بیاید.

Local subnet: اگر میزبانی که پشت یک دیوار آتش قرار دارد بتواند آلوده شود، آنگاه این میزبان در شبکه محلی خود به دنبال آلوده کردن اهداف دیگر خواهد رفت. این میزبان از ساختار آدرس زیر شبکه استفاده کرده تا میزبان های دیگری را که در غیر اینصورت تحت حفاظت دیوار آتش می بودند پیدا کند.

٤۱- ویژگی دیوار آتش از نوع"دروازه سطح مدار" چیست؟ (iranarze.ir)

الف. این نوع دروازه نسبت به فیلترهای بسته های دیتا امن ترند.

ب.سگمنت های TCP شامل داده های کاربر دو نقطه انتهایی را رِله میکند.

ج. این دیوار آتش می تواند یک سیستم منفرد یا عمل خاص باشد.

د. معمولا سگمنت های TCP را از یک اتصال به اتصال دیگر رِله میکند.

۱) الف وب. ۲) ج ود ۳) الف ود. ۳) ب وج

☑ ۲ ⇦ دروازه سطح مدار: این دیوار آتش میتواند یک سیستم منفرد بوده و یا می تواند عمل خاصی باشد که توسط دروازه سطح کاربرد برای کاربردهای معینی انجام شود. یک دروازه سطح کاربرد اجازه یک اتصال TCP سر- به - سر را نمی دهد، بلکه دروازه ای بین دو اتصال TCP ایجاد میکند که یک اتصال بین خودش و استفاده کننده از TCP در میزبان داخلی، و اتصال دیگر بین خودش و استفاده کننده از TCP در یک میزبان خارجی واقع شده است. زمانی که دو اتصال برقرار گردید دروازه معمولاً سگمنت های TCP را، بدون اینکه محتویات آنها را بررسی کند. از یک اتصال به اتصال دیگر رله میکند تدبیر امنیتی بکار گرفته شده در این مورد فقط تعیین آن است که برقراری چه اتصالاتی مجاز هستند. دروازه سطح مدار معمولاً وقتی مورد استفاده قرار میگیرد که مسئول سیستم به کاربران داخل سیستم اعتماد داشته باشد. دروازه را میتوان طوری پیکربندی کرد که سرویس سطح کاربرد یا سرویس پروکسی در اتصالات داخل محدوده، و عملیات سطح مدار در اتصالات خارج محدوده را حمایت نماید. در این نوع پیکربندی، دروازه میتواند سرباره بررسی داده های کاربردی ورودی برای عملیات ممنوع را تحمل کرده ولی در عوض نیازی به بررسی سرباره داده های خروجی برای این منظور نداشته باشد

۴۲- دو قانونی را که باید یک سیستم امن چند سطحه رعایت کند، کدام است؟ ( )

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

☑ ۱ ⇦ وقتی دسته ها و یا سطوح متفاوت داده ها مطرح می شوند، نیاز امنیتی آنها را امنیت چند سطحه (multilevel security) خوانند. بیان عمومی مسئله امنیت چند سطحی بدین ترتیب است که یک کاربر سطح بالاتر ممکن نیست اطلاعات را به یک کاربر سطح پائین تر و یا سطح غیر قابل مقایسه با خود بدهد مگر اینکه این امر با دقت کامل از اراده یک کاربر معتبر ناشی شده باشد. برای اجرای این هدف، این نیاز به دو بخش تقسیم شده و به سادگی بیان گردیده است. یک سیستم امن چند سطحه بایستی دو قانون زیر را رعایت نماید: {ا یر ا ن عر ضه}

- نخواندن سطح بالاتر: یک سوژه تنها میتواند موضوعی را بخواند که در سطح او و با پائین تر از سطح او قرار داشته باشد. این امر را معمولاً خاصیت امنیتی ساده (Simple Security Property) گویند.
- ننوشتن در سطح پائین تر: یک سوژه تنها میتواند در موضوعی دخل تصرف نماید که در سطح او و با بالاتر از سطح او قرار داشته باشد. در متون امنیتی این امر را star property Property) گویند.

نمونه سوالات استخدامی

پایگاه داده

تعداد سوالات : ۱۰۰ سوال چهارگزینه ای

همراه با پاسخنامه