نویسنده

احسان امجدی

۱۹۸ | ۱ | ۴۶ | ۶۱۹

احسان امجدی ، مشاور امنیت اطلاعات و ارتباطات و تست نفوذ سـنجی ، هکر کلاه سـفید ، مدرس دوره های تخصصـی امنیت اطلاعات و شبکه ، تخصص در حوزه های سرویس های مایکروسافت ، Routing و Switching ، مجازی سازی ، امنیت اطلاعات و تست نفوذ ، کشف جرائم رایانه ای و سیستم عامل لینوکس ، متخصص در حوزه SOC و ...

سکیوریتی پلاس چیست؟ معرفی جامع دوره CompTIA Security+ بخش ۲

۱۰۲۳ | ۵ | ۷

در بخش اول، به معرفی اجمالی دوره Security+ و لزوم تسـلط بر آن برای ورود به دنیای امنیـ ـبه پرداختیم و در این بخش و بخش بعد که در آینده مطرح خواهد شد، نگاهی گذرا به سـرتیترهای مهم آموزشـی در این دوره خواهیم انداخت تا با دید بهتری بتوانیـد قدم به این دوره بگذارید. ساختار این دوره دقیقا طوری طراحی شده است تا از سـرفصل هایی که در امتحات خواهد آمد پیروی کند. در زیر خلاصه ای از مباحثی که در هر تاپیک مورد بحث قرار میگیرد، اشاره شده است:

مفاهیم عمومی امنیت : معرفی

این بخش به معرفی سه گانه AAA از مفاهیم امینتی میپردازد: کنترل دسترسی (access control)، احراز هویت (authentication) و بازرسی (auditing). دانشجویان این دوره همچنین با اصطلاحات موجود در زمینه امنیت کامپیوتر اشنا خواهند شد و درباره اهداف اصـلی امنیت شـبکه/ کـامپیوتر یعنی ایجـاد محرمـانگی داده، حفـظ یکپارچگی دیتا و اطمینان از در دسترس بودن اطلاعات برای کاربران مجاز یاد خواهند گرفت.

مفاهیم عمومی امنیت: کنترل دسترسی

این بخش بر راه هایی که متخصـصان امنیت شـبکه میتوانند دسترسـی موجود بر منابع شـبکه را در کنترل خود داشته باشند زوم میکند و درباره سه نوع مهم از کنترل دسترسی یعنی دسترسی کنترل اجباری (MAC)، دسترسی کنترل بر اساس مصلحت (DAC) و کنترل دسترسی مبتنی بر وظیفه (RBAC) به صحبت میپردازد.

مفاهیم عمومی امنیت : احراز هویت

این بخش بسیاری از روش های موجود در احراز هویت کاربران و کامپیوترها در یک شبکه پوشش میدهد. در تمامی این روش ها هویت یـک کـاربر و یـا یک کامپیوتر قبل از برقراری یک session ارتباطی، اعتبار سـنجی میشود. در ادامه پروتکل های اسـتاندارد صنعتی بررسی خواهند شد که شامل Kerberos (در هر دو پلت فرم یونیکس و سیستم عامل های جدید ویندوز برای احراز هویت درخواست هـای کاربران جهت دسترسـی به منابع) و پروتکل CHAP که در احراز هویت کاربران ریموت اسـتفاده میشود، هسـتند. پس از آن درباره اسـتفاده از گواهی های دیجیتال، توکن ها و احراز هویت یوزر/ پسورد بحث خواهـد شـد. احراز هویت های چند پارامتری (که در احراز هویت های چندگانه جهت امنیت بیشتر استفاده میشود)، احراز هویت متقابل (احراز هویت دو طرفه بین

کلاینت وسـرور) و احراز هویت بیومتریک (از خصوصـیات فیزیکی شـما برای شناسایی هویت استفاده میکند)، تماما مورد بررسی قرار خواهند گرفت.

مفاهیم عمومی امنیت : سرویس ها و پروتکل های غیرضروری

این بخش درباره آندسـته از سرویس ها و پروتکل هایی بحث میکند که غالبا بصورت پیش فرض بر روی سیستم های شبکه نصب میشونـد که دربسـیاری از موارد ، زمـانی که نیـازی به اجرای آن هـا نیست، جهت برقراری امنیت بیشتر میتوان آن ها را غیرفعال نمود.

مفاهیم عمومی امنیت : حملات

این بخش برخی از اکسـپلویت های مرسوم را که توسط هکرها برای حمله و یا اختلال در سیسـتم ها اسـتفاده میشود را توضـیح میدهـد. نمـونه این مـوارد میتـوان به حملـت منع سـرویس (DoS) حملات بکـدور، spoofing، حملـت TCP//IP، reply، MITM، hijacking، کلیدهای ضـعیف و اکسپلویت های محاسباتی، روش های کرک پسورد و اکسپلویت های نرم افزار اشاره نمود. در تمامی این مراحل بشـما جزئیات فنی درباره این که این حملات چگونه کار میکننـد، داده نمیشود اما درباره نحوه جلوگیری، شـناسایی و پاسخ دهی به این حملات مطالبی رو یاد خواهید گرفت.

مفاهیم عمومی امنیت : کدهای مخرب

در این بخش به بررسـی ویروس هـای کامپیوتری، برنامه های تروجان، بمب های منطقی، worm ها و دیگر بـدافزارهای مخرب که غالبا از طریق شبکه به سیستم – سهوا و یا عمدا- وارد میشوند، پرداخته میشود.

مفاهیم عمومی امنیت : مهندسی اجتماعی

در این بخش به بررسـی پدیده استفاده از مهارت های اجتماعی (نقش بازی کردن، جذاب بودن، توانایی متقاعد کردن) در بدست آوردن اطلاعاتی (مثل پسوردها و نام اکانت ها) که برای ورود غیرمجاز به یک سیستم و یا شبکه لازم است، پرداخت میشود.

مفاهیم عمومی امنیت : بازرسی و پیگیری لاگ ها

در این بخش نگاهی می انـدازیم به روش هایی که متخصـصان امنیت میتوانند از لاگ ها و ابزارهای اسـکن سیسـتم برای جمع آوری اطلاعـات(که به حملات و ایجاد اختلال کمک میکننـد، اسـتفاده میشود)، اسـتفاده کننـد. با این روش میتوان قبل از اینکه اتکرها باگ های امنیتی موجود در شـبکه و یا سیسـتم رو پیدا کنند، آن ها را شناسایی و نسبت به برطرف سازی آن ها اقدام کرد. دوره **+security** سـرفصل های متنوعی دارد که به همین جا ختم نمیشود. در بخش سوم، به بررسی سرتیترهای دیگر در این دوره میپردازیم.

ادامه دارد...

پایان بخش دوم

سربلند و مانا باشید.

نویسنده: احسان امجدی

منبع: جزیره امنیت اطلاعات و ارتباطات وب سایت توسینسو

عنوان

$

۱

سکیوریتی پلاس چیست؟ معرفی جامع دوره +C...

رایگان

۲

سکیوریتی پلاس چیست؟ معرفی جامع دوره +C...

رایگان

۳

سکیوریتی پلاس چیست؟ معرفی جامع دوره +C...

رایگان

زمان و قیمت کل

۰″

۰

۵ نظر

میثم رضوان دوست ۵۱ ماه قبل

با سلام خدمت آقای مهندس امجدی عزیز

عالی بود مهندس جان

متشکر و سربلند باشید

پسندها (۱)

mojgan۳۰۷۸ ۵۱ ماه قبل

با سلام

مگه AAA مخفف Authentication, Authorization, and Accounting نیست؟!

پسندها (۱)

احسان امجدی ۵۱ ماه قبل

تمام واژه های مخفف مثل AAA رو نمیشه منحصر به یک مفهوم خاص کرد. در این جا هم بسته به منظر و دیدی که داریم باید AAA رو تفسیر کرد. AAA در زمینه های مختلف ممکنه مفاهیم مختلفی داشته باشه که هیچکدومشون ربطی به دیگری نداشته باشند. کما اینکه در بحث IT هم بسته به اینکه دقیقا موضوع صحبت در چه زمینه ایه، AAA به صورت های مختلف تعبیر میشه.

در زمینه امنیت شبکه های کامپیوتری و در این زمینه ای که ما در این نکته صحبت کردیم، AAA دقیقا به همون مفهومیه که گفته شده و به عنوان یکی از بحث های پایه ای در امنیت با این مضمون کاملا شناخته شده است.

پسندها (۰)

mojgan۳۰۷۸ ۵۱ ماه قبل

ممنون از توضیح تون.

پسندها (۱)

siva_۰۰۷ ۱۶ ماه قبل

سلام

چرا این مدلیه !!

تمام ویدئو ها قیمت زده صفر و زمان هم زده صفر و قابل خرید نیستند

پسندها (۰)

نظر شما

برای ارسال نظر باید وارد شوید.

از سرتاسر توسینسو