بسم الله الرحمن الرحیم

تستر نفوذ و ماموریت های آن

نویسنده:حامد هکینگ

تاریخ:فروردین ۹۶

مقدمه:

دنیای صفر و یک جذابیت های خاصی داره که ما رو به طرف خودش جلب میکنه اما یک چیز می ماند که ما بتونیم ازش درست استفاده کنیم،سختی های زیادی داره اما بازم ما به طرفش میایم این دنیا رو درکش میکنیم،چرا؟چون کارمون همینه ، تخصص مون همینه،رشته تحصیلی مون همینه چه اصلی و فرعی ، زندگی مون همینه و...

اینجا یک سوال پیش میاد اون اینه که منظور از رشته اصلی و فرعی چیه؟

پاسخ: کمتر کسی پیدا میشه تو زندگی یک رشته یا یک کار رو دوست داشته باشه منظور از رشته اصلی داری تحصیل میکنی و در دانشگاه میخونید و رشته فرعی اینه که بجز رشته اصلی به یک رشته دیگه هم علاقه داری و داری اون رو هم یاد میگیری بیرون از محل تحصیلت .

حرف های حامد به زبان عام و ساده:

موقعی که برای اولین بار داشتم انتخاب رشته میکردم،خیلیا میگفتن چرا رشته کامپیوتر میری،چرا ریاضی و تجربی نمیری،بهشون گفتم دلیل شو در آینده خودتون می فهمید.

همیشه به ندای قلبتون گوش بدید نه به حرف دیگران،متاسفانه خانواده ها نمیذارن خواسته هامون رو خودمون انتخاب کنیم،موقعی که این رشته رو انتخاب کردم به خودم قول دادم که به جای بالا میرسم و خانواده ام رو سر بلند میکنم و اثبات میکنم که رشته ای که رفتم آینده داره.

موقعی که در زمینه امنیت فعالیتم رو آغاز کردم که حدود 4 سال میگذره،بیشتر شب ها تا ساعت2 بیدار بودم،با اینکه گاهی روزا سر صبح کلاس داشتم اما به کارم ادامه دادم و نتیجه شو دیدم.و این رو یاد گرفتم که همیشه آدم فول اپشن نمیشه مخصوصا تو دنیای صفر ویک ، هیچ موقع ادعا نکنید تو این دنیا متاسفانه خیلی از آدما هستن ادعا میکنن و این ادعا باعث شکست میشه ،هنوز که هنوزه به خودم جرعت ندادم که بگم چیزی بلدم بلکه هیچی بلد نیستم واقعا هم بلد نیستم،یادگیری چیزه خوبیه اما وقتی ما چیزی رو یاد میگیریم به رخ دیگران میکشیم.

برای موفقیت در این راه شما نیاز به زمان و تلاش دارید ،بستگی انجام گذراندن این راه به خودتون داره نه کسی دیگه ای.توی مدارس و دانشگاه ها چیزی که به ما یاد میدن یک مقدمه ی کوتاه ست.

زندگی ما بستگی به خودمون داره پس باید زندگی و کشورمون رو باید خودمون بسازیم،نه به نژاد و قومیت مون بستگی داره،نه به ظاهر و ثروت و بی پولی مون بستگی داره،بلکه به خودمون بستگی داره.

برای یک مختصص یا مهندس شدن شما نیاز به مدرک ندارید نیاز به علم دارید.

تذکر بسیار مهم:هر چیزی که یاد میگیرید ازش درست استفاده کنید

تستر نفوذ(متخصص امنیت و نفوذ)

همان تستر نفوذ(Penetration Tester) که هکر اخلاقی (Ethical Hacker) نیز نامیده می شود به کاوش پرداخته و آسیب پذیری های امنیتی موجود در اپلیکیشن های وب ، شبکه ها و سیستم ها را بکارگیری می کند.

به عبارت دیگر شما برای هک قانونی پول دریافت می کنید. در این حوزه شما با ابزارهای نفوذ زیادی سروکار خواهید داشت. برخی از این ابزارها از پیش توسط دیگر متخصصین طراحی شده اند و در اختیار شما هستند و در برخی موارد شما نیاز به طراحی ابزارهای خود دارید تا حملات سایبری واقعی را همانند سازی کشنید. هدف نهایی شما کمک به یک سازمان به منظور بهینه سازی امنیت می باشد.

مسئولیت های تستر نفوذ

حوزه هک قانونی بسیار جذاب ولی در عین حال بسیار خسته کننده و ملال آور است. برخلاف هکرهای واقعی که زمان نامحدود برای نفوذ به شبکه را در اختیار دارند و می توانند در هر محدوده ای به صورت غیرقانونی فعالیت کنند , شما محدود به زمان و فعالیت هستید.

ممکن است در قرارداد شما با سازمان هدف تنها چند روز فرصت برای بررسی وجود داشته باشد! همچنین شما نمی توانید به صورت آزادانه به سیستم های هدف نفوذ کنید . از نظر قانونی محدوده فیزیکی حمله از نظر بخش های مورد نظر و سرورهای شبکه سازمان و کارهایی که می توانید بر روی این سرورها انجام دهید برای شما تعیین می شود.

شاید سازمان هدف به شما تنها امکان حمله به سیستم های کلاینتی را بدهد و نفوذ به سرورهای حیاتی اکیدا منع شده باشد. ممکن است تنها چیز خاصی از شبکه سازمان برای هدف در نظر گرفته شود. مثلا بخش فروش و سرورهای فروش که از نظر اطلاعاتی و محرمانگی محدود شده باشند.

موضوع خسته کننده درباره این حوزه این است که شما دایما بایستی یافته های خود را ثبت کرده و مستنداتی برای ارائه به سازمان هدف ایجاد کنید . به علاوه بایستی یافته ها و روش های نفوذ

خود را برای مدیران شبکه سازمان هدف توضیح دهید و حتی گزارشی قابل فهم برای برخی مدیران که شاید از نظر دانش فنی در سطح پایینی هستند ایجاد کنید.

وظایف کلی تستر نفوذ:

- **انجام تست های نفوذ بر روی شبکه ها ، سیستم های کامپیوتری و اپلیکیشن های مبتنی بر وب.**
- **اعمال ارزیابی امنیت فیزیکی سرورها، سیستم ها و دستگاه های شبکه.**
- **طراحی و ساخت ابزارهای نفوذ و تست جدید**
- **کاوش آسیب پذیری ها در اپلیکیشن های وب , اپلیکیشن های Thin Client ها و دیگر اپلیکیشن های استاندارد.**
- **بررسی دقیق و اشاره دقیق به متدهایی که نفوذگران می توانند با استفاده از آنها ضعف های امنیتی را بکارگیری کنند.**
- **اجرای حملات مهندسی اجتماعی به منظور نمایان کردن حفره های امنیتی**
- **ترکیب کردن ملاحظات کسب و کار با دیگر استراتژی های امنیتی موجود**
- **تحقیق ، مستندسازی و بحث و گفتگو درباره یافته های امنیتی با تیم های IT و مدیریت شبکه**
- **مرور و تعریف نیازمندی ها و راهکارهای امنیت اطلاعات و شبکه**
- **کار بر روی بهینه سازی های امنیت خدمات که شامل ارتقا متدلوژی های امنیتی موجود و ابزارهای پشتیبانی می باشد.**
- **ارائه بازخوردها و تایید برطرف سازی این مشکلات امنیتی پس از اطلاع رسانی به سازمان.**

در طی فرایند تست نفوذ شما به صورت معمول بر روی بکارگیری آسیب پذیری ها می پردازید ولی در حالت عادی شما نیاز ندارید تا هدف خود را اثبات کنید. این کار به ارزیابی امنیتی محول خواهد شد.

یک تستر نفوذ می تواند به سادگی تصاویری از یافته ها و نفوذهای خود گرفته و دسترسی کامل به پایگاه داده و دیگر موارد را نمایش دهد و نیازی به انجام کارهایی که مجرمان سایبری انجام می دهند،ندارد.

مقایسه تستر نفوذ در مقابل ارزیاب آسیب پذیری

ابهام های زیادی درباره تفاوت بین تستر نفوذ و ارزیاب آسیب پذیری وجود دارد.

تست های نفوذ به منظور بدست آوردن یک هدف حمله شبیه سازی شده طراحی شده است. این اهداف شبیه سازی شده بایستی توسط مشتریان ارائه شوند. یک هدف عمومی می تواند دسترسی به محتویات ارزشمند مشتریان سازمان و نفوذ به پایگاه داده های خرید و اطلاعات امنیتی باشد. این اطلاعات امنیتی به صورت معمول در شبکه داخلی سازمان قرار دارند . همچنین می توان به سیستم های منابع انسانی سازمان نفوذ کرد و اطلاعات طبقه بندی شده کاربران سازمان را ارائه کرد.

ارزیابی آسیب پذیری به منظور بدست آوردن یک لیست اولیت بندی شده از آسیب پذیری ها طراحی شده است. این کار برای اعضا سازمان انجام می شود .مشتریان می دانند که دارای مسائل و مشکلاتی هستند و تنها نیازمند کمک برای شناسایی و اولویت بندی آنها هستند.

به زبان ساده ارزیاب آسیب پذیری لیست گرا و تسترهای نفوذ هدف گرا هستند.

مسیرهای شغلی تستر نفوذ

تستر نفوذ می تواند از همه بخش ها وارد این حرفه شود. برخی از اشخاص تست نفوذ را در دانشگاه خود آغاز کرده و برخی دیگر مدارک CS می گیرند.

جدای از این موضوع که شما چه مسیری را تا اینجا طی کرده اید , کارفرمایان در صورتی که سواد چندانی نداشته باشید به احتمال زیاد شما را استخدام نخواهند کرد(مشکل کشور ما مدرک داشته باشی). شما همیشه می توانید در مشاغل زیر تجربه کافی را بدست آورید.

- ✓ مدیر امنیتی (Security Manager)
- ✓ مدیر سیستم (Network Manager)
- ✓ مهندس شبکه (Network Engineer)

پس از اینکه ارزش خود به عنوان یک تستر نفوذ را به اثبات رساندید می توانید به حوزه های زیربروید.

- ✓ تستر نفوذ ارشد (Senior Penetration Tester)
- ✓ مشاور امنیتی ارشد (Senior Security Consultant)
- ✓ معمار امنیتی ارشد (Senior Security Architect)

میانگین درآمد سالیانه تستر نفوذ

بر اساس آمار داده شده در سایت PayScale میانگین درآمد سالیانه یک تستر نفوذ بین 77,774 دلار می باشد(به پول کشور ما 2,507,667,082 ریال) . این درآمد شامل حقوق سالیانه شما , پاداش ها , کمسیون و حق ماموریت و دیگر موارد باشد .مسلما این حقوق بنا به میزان تجربه شما در کار , سابقه کاری و اعتبار و قدرت مالی سازمان مربوطه متفاوت خواهد بود.

مدارک دانشگاهی موردنیاز

بیشتر تسترهای نفوذ دارای یک مدرک خاص و تخصصی نیستند. ازآنجایی که هک قانونی (Ethical Hack) بیشتر درباره مهارت است تا اعتبار یک مدرک خاص , داشتن یک مدرک کارشناسی امنیت سایبری غیرضروری است چرا که شما بیشتر نیازمند تجربه کاری و شغلی دارید.

مهارت های تست نفوذ خود را به هر شیوه ممکن ارتقا دهید. به کنفرانس های هک رفته , مقالات امنیتی را مطالعه کنید، تمرین های تست نفوذ خود را انجام دهید و از دیگر تسترها کسب مهارت کنید.

سابقه کاری موردنیاز

بیشتر کارکنان فعال در این زمینه بین 2 تا 4 سال تجربه مرتبط با امنیت شبکه و کار در زمینه تست نفوذ و ارزیابی آسیب پذیری دارند.

مهارت های دشوار تستر نفوذ

تستر های نفوذ ، ارزیابی امنیتی ، توسعه کد ، اتوماسیون فرایندها و ... را پیاده سازی می کنند. پس تا جایی که می توانید درباره سیستم عامل ها ، نرم افزارها ، ارتباطات و پروتکل های شبکه دانش خود را ارتقا دهید.

در اینجا برخی از مهارت های فنی مورد نیاز را لیست می کنیم:

- **شناخت کامل سیستم عامل های ویندوز و یونیکس و لینوکس**
- **سرورهای شبکه و ابزارهای شبکه (نسوس، انمپ و...)**
- **زبان های برنامه نویسی++C ،Java،C#،ASM،PHP,Python،Perl**
- **سخت افزار کامپیوتر و سیستم های نرم افزاری**
- **ابزارهای امنیتی مثل Fortify ، AppScan و ...**
- **فریم ورک های امنیتی مثل Nist ، Hippa ، Sox و...**
- **فریم ورک قدرتمند متاسپلوییت**
- **آنالیز آسیب پذیری و مهندسی اجتماعی**
- **اصول رمزنگاری**
- **ابزارهای بازرسی قانونی**

گواهینامه های موردنیاز

هیچ لیستی از گواهینامه های مورد نیاز برای تستر نفوذ وجود ندارد. هرچند که در حوزه IT شما می توانید گواهینامه های زیر را برای اعتبار بیشتر خود کسب کنید.

- **Certified Ethical Hacker (CEH)**
- **Certified Penetration Tester (CPT)**
- **Offensive Security Certified Professional (OSCP)**
- **Certified Information Systems Security Professional (CISSP)**
- **GIAC Certified Incident Handler (GCIH)**
- **Certified Computer Forensic Examiner (CCFE)**

و...

فرایند تست نفوذ

فرایند تست نفوذ چیست و شامل چه مراحلی می باشد ؟

تست نفوذ در حقیقت زیرمجموعه ی هک اخلاقی می باشد. تست نفوذ در حقیقت یک عبارت حرفه ای تر برای توصیف کاری است که یک هکر قانونمند انجام می دهد. در صورتیکه به دنبال ایجاد زمینه های شغلی در زمینه نفوذ هستید , این عبارت را در آگهی های استخدام به دفعات مشاهده خواهید کرد.

فرایند تست نفوذ

هرچند تست نفوذ زیرمجموعه ای از هک اخلاقی است ولی از چندین منظر دارای تفاوت هایی می باشد.

در حقیقت فرایند تست نفوذ مسیری ساده تر و کارآمدتر برای شناسایی آسیب پذیری ها درون سیستم ها و بررسی این موضوع که آیا آسیب پذیری قابل بکارگیری هست یا خیر می باشد. تست نفوذ از طریق قراردادی که بین تستر نفوذ و صاحبان سیستم بسته می شود , جنبه قانونی و رسمی پیدا می کند. شما بایستی هدف تست را به منظور شناسایی آسیب پذیری ها و سیستم های شامل تست تعیین کنید .قوانین درگیری بایستی حتما تعریف گردند . از این طریق می توان راه و مسیر انجام تست نفوذ را تعیین کرد.

فرایند تست نفوذ از 7 بخش اصلی تشکیل شده است . این بخش ها شامل همه موارد مرتبط با تست نفوذ از ارتباط اولیه و دلیل تست نفوذ تا جمع آوری اطلاعات متن باز و فازهای مدل سازی تهدید می باشد.

گام های فرایند تست نفوذ

- **تعامل قبل از درگیری**
- **جمع آوری اطلاعات متن باز**
- **مدل سازی تهدید**
- **آنالیز آسیب پذیری**
- **بکارگیری**

- پس از بکارگیری
- گزارش دهی

از آنجایی که این استاندارد هیچ دستورالعمل فنی و نحوه اجرای تست نفوذ واقعی را ارائه نمی کند راهنمای فنی به همراه استاندارد ارائه می شود. فرایند تست نفوذ به صورت کلی سیستم های آسیب پذیر را شناسایی کرده و سپس اطلاعات بدست آمده را تحلیل کرده و با توجه به هدف تعیین شده سیستم هدف بکارگیری شده و نتایج در گزارش پایانی ایجاد می شود.

موانع و محدودیت های تست نفوذ

موانع تست نفوذ، هرچند تست های نفوذ در بیشتر موارد توصیه می شود و بایستی بر اساس یک برنامه منظم و به صورت پی در پی انجام شوند ولی یک سری محدودیت ها برای آن وجود دارند . موانع تست نفوذ کدامند کیفیت تست و نتایج بدست آمده به طور مستقیم به مهارت های تستر نفوذ تیم تست وابسته است. از آنجای که حوزه گسترده تست نفوذ محدود است ، تست های نفوذ قادر به پیداکردن همه آسیب پذیری ها نیستند.

موانع تست نفوذ شامل محدودیت دسترسی تستر نفوذ به محیط تست و محدودیت ابزارهای استفاده شده توسط تستر نفوذ می باشد. در اینجا به برخی از محدودیت های آزمون نفوذ اشاره می کنیم:

موانع تست نفوذ

محدودیت مهارت ها

همانطور که در بالا اشاره کردیم , موفقیت و کیفیت تست به صورت مستقیم به مهارت ها و تجربه تستر نفوذ وابسته است. تست های نفوذ را می توان به سه دسته تقسیم کرد:

- تست شبکه
- تست سیستم
- تست اپلیکیشن های وب

در صورتیکه تسترنفوذ مهارت تست نفوذ شبکه را داشته باشد مسلما نتایج دلخواهی در تست نفوذ یک اپلیکیشن وب را بدست نمی آورد. به دلیل تعداد عظیم تکنولوژی های توسعه یافته در

دنیای وب و اینترنت ، پیدا کردن شخصی با همه مهارت های تست کاری دشوار است. یک تستر ممکن است دانش بالایی در زمینه وب سرور آپاچی(Apache) داشته باشد ولی همین شخص ممکن است برای بار اول با وب سرور Internet Information Service(IIS) مواجه شده باشد.

تجربیات گذشته تستر نفوذ در موفقیت تست نقش کلیدی ایفا می کند. جستجو و پیدا کردن یک آسیب پذیری با ریسک پایین ولی با سطح تهدید بالا فقط با کار زیاد و کسب تجربه حاصل می شود.

محدودیت زمان

در بیشتر موارد تست نفوذ یک پروژه کوتاه است که بایستی در مدت زمانی محدود انجام شود. تستر نفوذ بایستی نتایج کافی و آسیب پذیری های مورد نظر را در این محدوده زمانی تعیین شده بدست آورد. در مقابل هکرها در حملات خود دارای زمان بالا برای کار بر روی پروژه های خود هستند. تسترها علاوه بر داشتن زمان محدود بایستی در پایان تست گزارش کاملی ایجاد کرده که توصیف کننده متدولوژی , آسیب پذیری های شناسایی شده و خلاصه اجرایی می باشد . همچنین بایستی در مراحل کار به صورت منظم تصاویری گرفته شوند تا به گزارش اضافه شوند. یک هکر هیچگاه نیازمند نوشتن گزارش نیست و می تواند وقت خود را به حملات بیشتر و بدست آوردن نتایج کامل تر اختصاص دهد اما تستر های نفوذ باید تمام مستندات را تحویل دهند

محدودیت اکسپلوییت های سفارشی

از مهم ترین موانع تست نفوذ توسعه اکسپلوییت های سفارشی می باشد . در برخی محیط های به شدت امن , فریم ورک های معمول تست نفوذ و ابزارهای رایج خیلی کارگشا نخواهند بود و تستر نفوذ نیازمند بکارگیری خلاقیت و ایجاد اکسپلوییت هایی به صورت دستی و نوشتن دستی اسکریپت ها می باشد . ایجاد اکسپلوییت ها بسیار زمان بر است و بخشی از مهارت های بیشتر تسترها نیست. نوشتن اکسپلوییت های سفارشی بر روی بودجه و زمان پروژه تست تاثیر مستقیم خواهد گذاشت.

اجتناب از حملات رد سرویس

هک و تست نفوذ هنر ایجاب یک کامپیوتر به انجام کارهایی است که کامپیوتر در حالت عادی نباید انجام دهد. در برخی موارد ممکن است تست نفوذ به جای فراهم کردن دسترسی به سیستم به یک حمله رد سرویس (DoS Attack) مبدل شود. بسیاری از تسترهای نفوذ به دلیل اینکه ممکن است سهواً سیستم ها با خرابی مواجه شوند از انجام این نوع تست ها اجتناب می کنند.در نتیجه از آنجایی که سیستم ها برای حملات DoS تست نمی شوند به سادگی توسط یک لمر ازکار می افتد .

محدودیت دسترسی

شبکه ها به بخش های مختلفی تقسیم می شوند و تستر نفوذ در بیشتر مواقع فقط به همان بخش های تعیین شده دسترسی دارد . هرچند که چنین تستی مشکلات پیکربندی و آسیب پذیری های موجود در شبکه داخلی که اعضا درگیر آن هستند را نشان نمی دهد.

محدودیت ابزارهای مورد استفاده

آخرین مورد از موانع تست نفوذ که به آن اشاره می کنیم , محدودیت ابزارهای مورد استفاده می باشد . در بیشتر مواقع تستر نفوذ تنها اجازه استفاده از لیست ابزارهای تایید شده و فریم ورک های بکارگیری خاصی را دارد .هیچ ابزاری کامل نیست ،تسترهای نفوذ بایستی دانش کافی از این ابزارها را داشته باشد و جایگزین هایی برای ویژگی های فاقد آن پیدا کند.

به منظور غلبه بر این محدودیت ها , سازمان های بزرگ دارای یک تیم اختصاصی تست نفوذ هستند که آسیب پذیری های جدید را تحقیق و به صورت منظم تست های خود را انجام می دهند . دیگر سازمان ها علاوه بر انجام تست های نفوذ به صورت مداوم پیکربندی سازمان را بررسی و ارزیابی می کنند.

معرفی چند سایت برای آموزش رایگان امنیت

owasp.org

risk3sixty.com

heimdalsecurity.com

safeandsecureonline.org

firstrespondertraining.gov

cyberaces.org

offensive-security.com

irtsectraining.nih.gov

cybrary.it

ایمیل

info.onsec@gmail.com

کانال تلگرام آموزش های امنیت (آنسک مرجع تخصصی امنیت و تست نفوذ)

Telegram.me/OnSec

کانال آپارات

Aparat.com/OnSec