بنام خداوند بخشنده مهربان

سوالات مربوط به درس امنیت

استاد: دکتر علی فانیان

1. تست نفوذ چیست ؟ و اهمیت آن بنویسید ؟

تست نفوذ ؛ تست امنیتی است که که در آن با ارزیابی شبیه سازی حملات دنیا واقعی ؛روش های دور زدن ویژگی های امنیتی نرم افزار؛سیستم یا شبکه شناسایی می شود. این امر اغلب شامل حملات واقعی در سیستم های واقعی و داده هایی است که توسط ابزارها و تکنیک های معمول مهاجمان استفاده می شود. تست نفوذ به عبارتی یک هک اخلاقی شناخته می شود در حقیقت کاری است که یک هکر قانونمند انجام می دهد. اهمیت آن از آنجا برمی آید که تضمین کیفیت و تست سازماندهی هدف گسترده ای است که بتوان اطمینان حاصل کرد که نرم افزار های کاربردی عملکرد های خود را در راستای نیازمندی های تجاری برآورده می سازند یا نه.

2. تست نفوذ توسط چه کسانی انجام می گیرد ؟ چرا؟

تست امنیتی نیاز به استفاده از مفهوم کلاه سیاه و کلاه سفید و دیگر روش ها خواهد داشت. در تست کلاه سفید، اطمینان داریم که ویژگی های امنیتی با آگاهی کار می کنند و از این رو حمله گر به آسانی نمی تواند به سیستم حمله کند. اغلب تمام تست های نفوذ بر اساس روش های هکر های کلاه سیاه هستند. اغلب شبیه سازی تفکر آدم های بد برای تست نفوذ ضروری هم می باشد!

3. مراحل چرخه ی توسعه ی امن نرم افزار را بنویسید ؟

مرور کد , تحلیل ریسک معمارانه, سناریو های سو کاربرد, نیازمندی های امنیتی, اقدامات اپراتوری امنیت , تست نفوذ و تست های امنیتی ریسک مبنا

4. فرق بازرسی آسیب پذیری و تست نفوذ را بنویسید ؟

یکی از پر اهمیت ترین بخش ها مربوط به امنیت بازرسی آسیب پذیری می باشد ؛ ابزار های مختلفی برای اسکن آسیب پذیری مورد استفاده قرار می گیرد مثلا میتوان با این ابزار ها اپلیکیشن هایی که بر روی یک سیستم قرار دارد را شناسایی کرد یا حتی پسورد و فایل هایی که اجازه دسترسی ضعیف دارند را شناسایی کرد. این ابزار ها قادر هستند نقاط امنیتی که سازندگان نرم افزار مشخص کرده اند و یا

تهدید مربوط را شناسایی و اسکن بنماید. اما Penetration Testing که بعد از همین بازرسی آسیب پذیری مورد استفاده قرار می گیرد در حقیقت به بررسی عمق حملات احتمالی و بر جسته کردن نقاط ضعف امنیتی که توسط ابزارهای آسیب پذیر اسکن نشده است می پردازد در کل هدف از تست نفوذ بررسی و پیدا کردن نقاط آسیب پذیر نمی باشد بلکه در اینجا چگونگی استفاده کردن از ضعف ها و سو استفاده (Exploit) هکر ها و مخربها از آسیب پذیری های مربوط به محصول مدل و بررسی می شود .

5. مراحل تست نفوذ طبق استاندارد PTES (Penetration Testing Exaction Standard) را نام ببرید ؟

1.اقدامات پیش از درگیری اولیه 2.جمع آوری اطلاعات 3.مدل سازی تهدید 4.تحلیل آسیب پذیری 6. اکسپولیت نمودن آسیب ها 6. انجام عملیات بعد از اکسپولیت 7. گزارش دهی

6. یکی از فاکتور های اصلی و مورد نیاز در یک نرم افزار که خود می تواند به عنوان مشکل امنیتی مطرح شود را بنویسید ؟

اما در تست امنیتی نکاتی بسیار مهم در مورد اهمیتی که باید به ورودی ها دهیم وجود دارد که باید به انها دقت ویژه ای کرد ؛ اولا بزرگترین مشکل امنیتی نرم افزار این است که نرم افزار ورودی می گیرد و دوم سوالی که توسعه دهندگان باید به آنها فکر کنند (آیا می توان به وردوی ها اعتماد کرد؟!؛ اعتماد به ورودی ریشه اصلی مشترک از سرریز بافر تا تزریق sql یا حتی XSS) ؛ به همین دلیل نیاز به کنترل و بررسی هر چه بیشتر وردوی خواهیم داشت و ابزارهای حمله تا حد زیادی روی تمرکز خواهند داشت ؛ البته تست نفوذ نیز روی ورودی ها تمرکز می کند و رویکرد لیست سیاهی (برای نپذیرفتن ورودی های بد) جواب نمی دهد چون که نیاز است که همه ورودی ها را به جز لیست سفید رد کرد .

7. ابزارهای تست نفوذ را نام ببرید ؟

ابزارهای تزریق خطا ؛ دیباگرها ؛ دیس اسمبلر ها و دیکامپایلر ؛ابزار های فراخوانی و DLL ها مثل DLLSPY ابزارهای بررسی پیمانه ها و وابستگی ها و Fuzzing

8. فرق تست امنیتی با تست نفوذ را بنویسید ؟

یکی از تفاوت های موجود در تست نفوذ با تست امنیتی در سطح کاری تست می باشد و تفاوت دیگر این دو در زمان تست خواهد بود . در حقیقت تست نفوذ زمانی که نرم‌افزار کامل شده و در محیط عملیاتی نصب شد انجام می‌گیرد تستی نسبتا مختصر به شمار می‌آید و اما تست امنیتی می‌تواند پیش از اتمام نرم‌افزار و در سطح مولفه‌ها انجام گیرد .

9. تست امنیتی ریسک مبنا را توضیح دهید ؟

تست ریسک مبنا یعنی یک سری ریسک ها را مشخص کنیم و یک سری تست ها مشتق شده از همین ریسک ها انجام دهیم بنابراین تستر میتواند بر روی ناحیه ای از کد تمرکز کند . در صورتی که تست نفوذ زمانی انجام خواهد شد که نرم افزار به طور کامل نصب و در محیط عملیاتی خود قرار گرفته است ، تست نفوذ به صورت outside → in ولی تست امنیتی ریسک مبنا میتواند قبل از تکمیل شدن کامل نرم افزار و روی اجزای آن اجرا شود و به صورت inside → out میباشد.

10. محدودیت های تست نفوذ را بنویسید ؟

تست توسط افراد امنیتی بر تیم نرم افزار اعمال شود ؛همانطور که در قبل گفته شد میتوان از هکر هایی که به اصطلاح خوب شده اند و دیگر کار بد نمی کنند استفاده کرد دوم اینکه رویکرد باید از بیرون به درون باشد ولی این شرط لازم ولی ناکافی است و سوم اینکه تلاش خیلی ناچیز-خیلی دیر برای پیگیری مشکلات امنیتی در پایان چرخه توسعه انجام میشود! رفع این مشکل در این برهه هزینه بر است و اغلب بجای درمان تنها پانسمان است ! اغلب اقدامات در نتیجه تست نفوذ ذاتا واکنشی و منفعلانه هستند. ضمنا در در عمل تست نفوذ استاندارد مورد قبولی که در حال استفاده باشد ندارد.