دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

دانشکده مهندسی کامپیوتر

تمرین عملی

درس مبانی امنیت اطلاعات

استاد: دکتر نستوه طاهری جوان

تیم تدریسیاری:

رضا توسلی

سید سجاد پیشوائیان

تیر 1399

1) Port Scanning:

Port Scanning روشی است که در آن مهاجم بررسی می‌کند که کدام یک از پورت‌های یک host مشخص، باز هستند و سرور از چه برنامه‌ای بر روی interfaceهایی که بصورت عمومی در دسترس هستند، استفاده می‌کند. با این اطلاعات، مهاجم می‌تواند درک بهتری از اینکه چگونه می‌تواند به سرور حمله کند، به دست آورد.

در این بخش باید از ابزار nmap استفاده کنید تا سرور **scanme.nmap.org** را اسکن کنید. در این بخش باید موارد زیر را در نظر بگیرید:

- از اسکن TCP SYN استفاده کنید. (با مطالعه‌ی مستندات nmap، flag مناسب برای این کار را بیابید.)
- موارد traceroute – script scanning – version detection – OS detection را فعال کنید.
- quick scan انجام دهید.
- تمام پورت‌ها را اسکن کنید.
- ترافیک شبکه هنگام اسکن را با استفاده از wireshark بررسی کنید.(تمرین 2 را ببینید)

بعد از انجام موارد بالا، به سوالات زیر پاسخ دهید:

1. دستور و flagهایی را که برای اجرای اسکن به کار برده‌اید، بنویسید.
2. چه پورت‌هایی بر روی سروری که بررسی کردید، باز هستند؟
3. چه برنامه‌هایی بر روی پورت‌هایی که بررسی کردید، در حال اجرا هستند؟
4. فرق بین اسکن TCP SYN و اسکن TCP Connect را توضیح دهید.

2) Wireshark Packet Sniffing:

وایرشارک ابزاری برای بررسی ترافیک شبکه است. در این بخش از وایرشارک برای بررسی ترافیک شبکه‌ای که هنگام اسکن با nmap در قسمت ۱ بدست آمده، استفاده می‌کنیم. شما باید قبل از انجام قسمت اول، وایرشارک را راه‌اندازی کنید و ترافیک واسطی را که nmap قرار است از آن استفاده کند، record کنید و سپس اسکن را انجام دهید. با استفاده از فیلترهای مناسب ببینید که nmap چگونه یک پورت را اسکن می‌کند و سپس به سوالات زیر پاسخ دهید:

1. هنگامی که در nmap یک پورت بصورت closed نشان داده می‌شود، سرور چه جوابی را در پاسخ به بسته‌ی SYN که به آن پورت فرستاده شده، برمی‌گرداند؟ (اطلاعات بسته‌ای را که سرور برمی‌گرداند بنویسید)
2. هنگامی که در nmap یک پورت بصورت filtered نشان داده می‌شود، سرور چه جوابی را در پاسخ به بسته‌ی SYN که به آن پورت فرستاده شده، برمی‌گرداند؟ (اطلاعات بسته‌ای را که سرور برمی‌گرداند بنویسید)
3. nmap چه درخواست‌های HTTP را، علاوه بر درخواست HTTP GET به وب‌سرور می‌فرستد؟

3) XSS Vulnerability:

حملات Cross-site Scripting (XSS) یکی از جدی‌ترین آسیب‌پذیری‌های برنامه‌های کاربردی تحت وب است. در این حملات، attacker از یک web application استفاده می کند تا کد های مخرب را به وبسایت مقصد (در قالب script) بفرستد. حملات XSS به چند دسته تقسیم می‌شوند، مشهورترین این حملات در دو دسته‌ی ذخیره‌شده (stored) و بازتابی (reflected) هستند. در این قسمت ابتدا ابزار DVWA را نصب کنید. این ابزار یک وب اپلیکیشن آسیب‌پذیر است که شما می‌توانید حملات مختلف را توسط آن شبیه‌سازی کنید.

در این ابزار :

1. دو روش مطرح شده برای حملات XSS شامل بازتابی و ذخیره شده را شبیه‌سازی کنید.
2. این حملات را در سه سطح امنیتی low, medium, high بررسی کنید.
3. گزارش کاملی از مراحل انجام کار با استفاده از تصاویر و توضیحات بنویسید.

برای اطلاعات بیشتر می‌توانید به لینک‌های زیر مراجعه کنید:

برای نصب DVWA:

https://github.com/ethicalhack3r/DVWA#installation

برای حملات بازتابی:

https://youtube.com/watch?v=6-WM7K1Q_bA

برای حملات ذخیره‌شده:

https://youtube.com/watch?v=ivvTrTie16I

4) Cain and Abel:

Cain and Abel (به طور خلاصه به Cain) ابزاری برای بازیابی رمز عبور برای مایکروسافت ویندوز است. این نرم افزار می تواند انواع مختلفی از رمزهای عبور را با استفاده از روشهایی مانند network packet sniffing ، شکستن انواع hash های رمز عبور با استفاده از روش هایی مانند حملات dictionary، brute force و حملات cryptanalysis بازیابی کند. حملات Cryptanalysis از طریق rainbow table ها انجام می شود که با برنامه winrtgen.exe تهیه شده با Cain and Abel تولید می شود.

هدف از این تمرین استفاده از ابزارهای مختلف رمزنگاری گذرواژه موجود در نرم افزار Cain and Abel و تعیین کارآیی و اثربخشی هر تکنیک می باشد(برای آشنایی با این نرم افزار میتوانید از این لینک استفاده کنید).

بدین منظور لازم است تا سه دسته از گذر واژه ها مورد بررسی قرار گیرند(حداکثر 7 کارکتر):

1. متن ساده با حروف کوچک مانند testing
2. حروف کوچک همراه با عدد مانند test123
3. حروف کوچک، حروف بزرگ، عدد و نماد مانند @tsTng1

لازم است گزارشی تهیه نموده و تمامی مراحل را از نصب تا بررسی گذرواژه ها در گزارش خود آورده و همچنین به سوالات زیر پاسخ دهید:

1. در مورد دو نوع حمله مختلف که می توانند در Cain and Abel برای شکستن کلمات عبور کاربر استفاده شوند ، توضیح دهید. به نظر شما کدام یک موثرتر است و چرا؟
2. نتایج حاصل از دو روش استفاده شده برای شکستن حسابها را با یکدیگر مقایسه کنید. پس از استفاده از این دو روش ، چه چیزی می توانید نتیجه بگیرید؟
3. در مورد الگوریتم دیگری را که برای ذخیره کلمه عبور مورد استفاده قرار می گیرد ، تحقیق کنید و نتیجه را در گزارش خود بیاورید.
4. آنتی ویروس Cain and Abel را بدافزار تشخیص می دهد. آیا شما نیز فکر می کنید که Cain and Abel بدافزار است؟ چرا و چرا نه؟

نکات تحویل:

1. برای هر تمرین گزارشی کامل **شامل مراحل انجام +توضیح هر مرحله + پاسخ سوالات پرسیده شده** می بایست نوشته شده و به فرمت **Exercise#_std#.pdf** نام گذاری شود.
2. تمام گزارش ها داخل یک فایل به فرمت **Practical_stdName_stdNum.zip** قرار داده شده و ارسال شود.
3. در صورت مشاهده تقلب، **برای طرفین نمره صفر منظور می گردد.**
4. **تنها راه تحویل تمرین، آپلود آنها در مودل است. به دلیل باگ موجود در سایت درس حتما بعد از آپلود کردن یکبار فایل آپلود شده را دانلود کنید تا به درست آپلود شدن آن یقین پیدا کنید.**
5. برای ارتباط با تدریس یاران از طریق ایمیل netsecfall2019@gmail.com در ارتباط باشید.