دانشکده برق، کامپیوتر و فناوری‌های پیشرفته

گروه مهندسی کامپیوتر

دستورکار آزمایشگاه امنیت اطلاعات

تهیه کننده:

دکتر میر سامان تاجبخش

تاریخ تنظیم:

مهرماه ۱۴۰۳

فهرست آزمایش‌ها

آزمایش ۱
بررسی حمله ARP Poisoning

حمله ARP Poisoning نوعی حمله است که در آن حمله کننده قادر است ترافیک رد و بدل شده در داخل شبکه محلی را شنود کند.

۱-۱ هدف

هدف این تمرین آشنایی دانشجویان با مفهوم ARP و هم چنین نحوه آسیب پذیری این پروتکل است. به علاوه با تکنیک‌های مقابله با این حمله نیز آشنا می‌شوند که بتوانند کانفیگ شبکه را در نقاط بحرانی مدیریت کنند. به علاوه ابزارهای مانیتورینگ نیز معرفی می‌شود.

۱-۲ دستور کار

در این آزمایش، ابتدا مفاهیم تئوری ARP و همچنین مشکل این پروتکل که منجر به انجام حمله ARP Poisoning می‌شود، مورد بحث قرار می‌گیرد. در مورد این که چرا پروتکل ARP احراز هویت ندارد و سناریوهایی که امکان احراز هوریت به طور کامل امکان پذیر نیست مورد بررسی قرار می‌گیرد.

۱-۳ گزارش

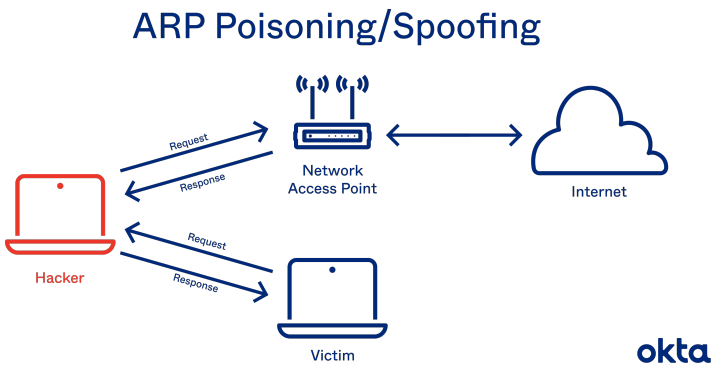
دانشجویان در پایان این تمرین باید سه ماشین مجازی کانفیگ کنند. برای این منظور می‌توانند از شبیه سازی مانند Virtual Box، VMWare و یا QEMU استفاده کنند. سیستم‌عامل پیشنهادی نیز Ubuntu می‌باشد ولی سناریو مد نظر با سیستم عامل Windows نیز قابل پیاده سازی است. در هر صورت سه ماشین باید کانفیگ شود که یکی نقش قربانی [۱]، دیگری نقش حمله کننده [۲] و سومی نقش درگاه اینترنتی [۳] که خودش نیز یک قربانی است را ایفا می‌کند.

دانشجویان در گزارش خود بایستی ترافیک ماشین حمله کننده را با ابزاری مانند Wireshark یا tcpdump بررسی کنند و ببینند که داده‌های انتقالی بین قربانی و درگاه اینترنتی به چه صورت تبادل می‌شود. همچنین دانشجویان مشاهده خواهند کرد که داده‌های رمز شده (SSL/TLS) قابلیت مشاهده را ندارد و این مورد پیشنیاز برای آزمایش ۵ می‌باشد.

برای حمله می‌توانند از ابزاری مانند ettercap در سیستم عامل لینوکس و یا Cain and Able در سیستم عامل ویندوز استفاده کنند.

---

[۱] Victim
[۲] Attacker
[۳] Gateway Default



شکل ۱-۱: نمای کلی حمله ARP Poisoning

آزمایش ۲

DNS Cache Poisoning

حمله DNS Cache Poisoning نوعی از حمله است که در آن حمله کننده بصورت از راه دور می‌تواند حافظه یک سرور Passive DNS مورد حمله قرار داده و در نتیجه تا مدت زمان مورد نظر حمله کننده، سرور DNS آدرس مد نظر حمله کننده را به آدرس IP مد نظر حمله کننده ترجمه کرده و در نتیجه کاربران شبکه حمله شده، بدون متوجه شدن به سرور حمله کننده متصل خواهند شد.

۲-۱ هدف

هدف این تمرین آشنایی دانشجویان با نحوه کارکرد پروتکل DNS می‌باشد و با ساختار پیام DNS آشنا می‌شوند. البته این حمله قدیمی می‌باشد و اکنون رفع شده است ولی دانشجویان باید با مفاهیم پایه‌ای این حمله آشنا شوند تا بتوانند نسخه جدید این حمله را درک نمایند.

۲-۲ دستور کار

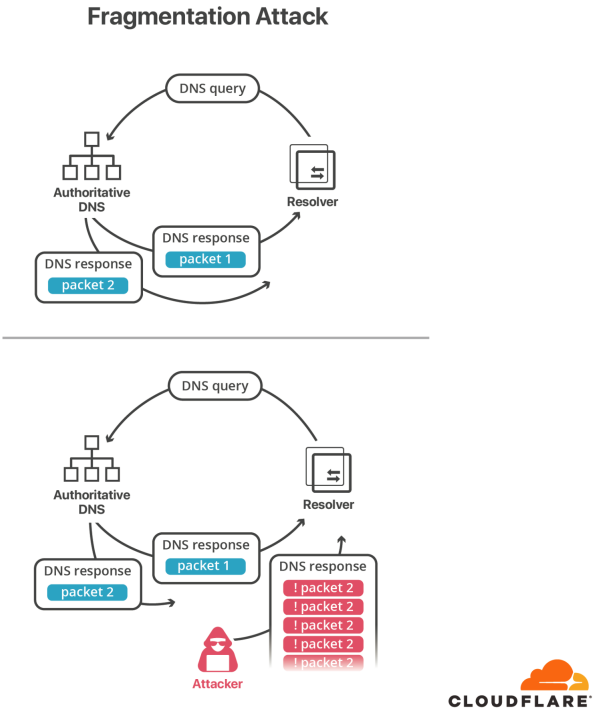
دانشجویان بایستی یک سرور Passive DNS را تنظیم کنند و سپس از طریق یک ماشین دیگر به آن حمله کنند. هر دو ماشین مجازی، پیشنهاد می‌شود که از یکی از توزیع‌های لینوکس باشد. برای حمله از ابزار زیر باید استفاده کنند:

https://github.com/seclab-ucr/SADDNS

که بتواند نسخه جدید حمله DNS Cache Poisoning را شبیه سازی کنند. در نهایت باید ترافیک را از سمت حمله کننده و قربانی مورد بررسی و تحلیل قرار دهند. برای تحلیل می‌توانند از ابزاری مانند Wireshark یا tcpdump استفاده کنند.

۲-۳ گزارش

جهت گزارش دهی، دانشجویان بایستی مراحل انجام حمله و پکت‌های حمله را هم از سمت حمله کننده و هم از سمت قربانی را مشخص کنند.



شکل ۲ - ۱ : نمای کلی حمله SADDNS

آزمایش ۳
PGP

PGP مخفف کلمات Pretty Good Privacy است و روشی است جهت اطمینان از داده ارسالی. اطمینان هم از این جهت که گیرنده داده دریافی را مطمئن ایت که فرستنده‌ای که ادعا می‌کند فرستاده را تایید می‌کند. از طرفی فرستنده مطمئن است که فقط گیرنده اصلی می‌تواند پیام دریافتی را باز کرده و محتوایش را متوجه شود.

۳-۱ هدف

هدف این تمرین آشنایی دانشجویان با نحوه کارکرد ابزار PGP می‌باشد و با ساختار پیام رمز شده و نحوه رمزنگاری آشنا می‌شوند.

۳-۲ دستور کار

برای آشنایی دانشجویان با مفهوم PGP می‌توان از ابزار Cryptool استفاده کرد.

https://www.cryptool.org/en/ct2/

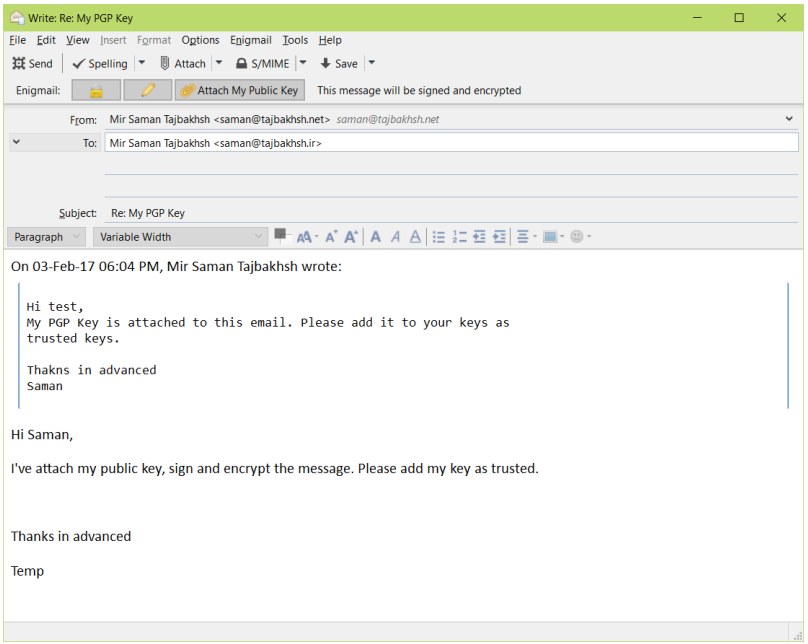
برای پیاده سازی سناریوی واقعی نیز می‌توانند از ابزار GPG4Win [۱] استفاده کنند. سپس از ابزار Kleopatra اقدام به ساخت کلید مخصوص خود بکنند. و با در دست داشتن کلید عمومی طرف مقابل، اقدام به ارسال ایمیل بکنند. بدین منظور می‌توانند از ابزار Thunderbird به همراه پلاگین EnigMail استفاده کنند. برای اطلاعات بیشتر به لینک زیر مراجعه کنید.

https://mstajbakhsh.ir/encrypting-emails-using-pgpgpg/

۳-۳ گزارش

برای گزارش، دانشجویان علاوه نحوه ارسال ایمیل، بایستی یک ایمیل رمز و امضا شده به استاد درس نیز ارسال کنند.

[۱] https://www.gpg4win.org/



شکل ۳-۱: ایمیل رمز شده و امضا شده توسط PGP

آزمایش ۴

DHCP Poisoning

حمله DHCP Poisoning برای پر کردن آدرس‌های موجود در سرور DHCP مورد سوءاستفاده قرار می‌گیرد. در اثر این حمله، حمله کننده ابتدا سرور DHCP مورد نظر را از کار می‌اندازد (با پر کردن آدرس‌های آزاد) و سپس سرور خود را راه اندازی کرده و افراد وارد شده به شبکه، از سرور حمله کننده آدرس IP دریافت می‌کنند. به علاوه آدرس DNS Resolver, Default Gateway را نیز دریافت می‌کنند. همچنین Lease Time نیز در اختیار حمله کننده است.

۴-۱ هدف

هدف این تمرین آشنایی دانشجویان با نحوه کارکرد پروتکل DHCP و ضعف‌های این پروتکل است.

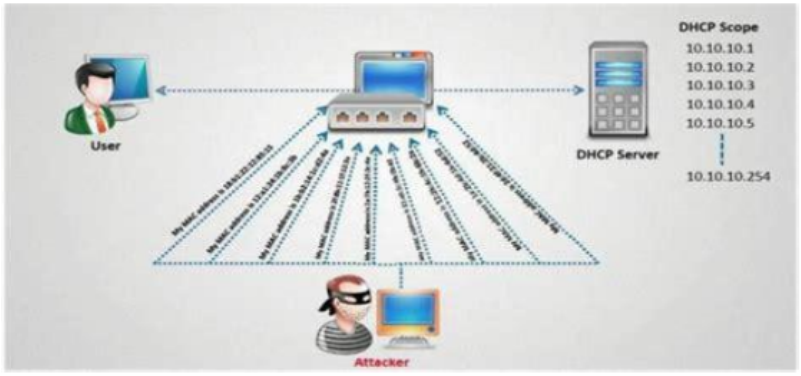
۴-۲ دستور کار

در ابتدا دانشجویان بایستی با مفاهیم DHCP و اینکه چرا این پروتکل از UDP استفاده می‌کند و روند پروتکل چگونه است، باید آشنا شوند.

برای مشاهده نتیجه این حمله دانشجویان می‌توانند از ابزار dhcpig برای تست در شبکه محلی خود استفاده کنند.

۴-۳ گزارش

جهت گزارش دهی، دانشجویان بایستی مراحل انجام حمله و پکت‌های ارسالی از سمت حمله کننده را در گزارش بیاورند.



شکل ۴-۱: نمای کلی حمله DHCP Poisoning

آزمایش ۵

SSL MITM Attack

SSL MITM مخفف کلمات Secure Socket Layer Man In The Middle است و روشی است که در آن جمله کننده خود را ما بین ارتباط مشتری با سرور قرار داده و گواهی جعلی خود را به جای گواهی اصلی گماشته و سعی در شنود داده‌های رمز شده‌ای است که مشتری می‌خواهد به سرور بفرستد.

۵-۱ هدف

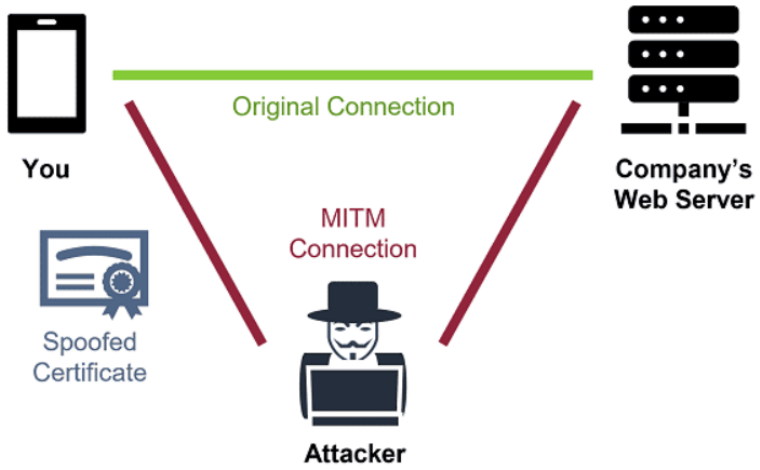
هدف این تمرین آشنایی دانشجویان با نحوه کارکرد SSL است و این که بدانند چطور باید تشخیص داد که گواهی ارسالی می‌تواند جعلی باشد. این مورد کاربرد زیادی در برنامه‌های سمت کلاینت (مانند برنامه‌های موبایلی) دارد.

۵-۲ دستور کار

برای این کار دانشجویان می‌توانند از ابزار sslsniff, mitmproxy استفاده کنند. با این ابزار می‌توانند در یک ماشین مجازی، ترافیک ماشین اصلی را شنود کنند و نتیجه را در سمت ماشین اصلی ببینند.

۵-۳ گزارش

برای گزارش، دانشجویان باید ترافیک شنود شده و رمز کشایی شده را ثبت و ضبط کرده و نتیجه را گزارش دهند.



شکل ۵-۱: شمای کلی حمله SSL MITM

آزمایش ۶

Tor

شبکه‌های گمنام سازی یکی از شبکه‌های در حال رشد و غیر قابل رد یابی هستند که آشنایی دانشجویان با این شبکه‌ها و نحوه مقابله با ترافیک ورودی از این شبکه‌ها به سرویس‌های خود، جزء الزامات این آزمایش است. در ایتدا استاد در مورد نحوه کار کرد شبکه تور و علت عدم توانایی در شناسایی مبدا درخواست، توضیح می‌دهد.

۶-۱ هدف

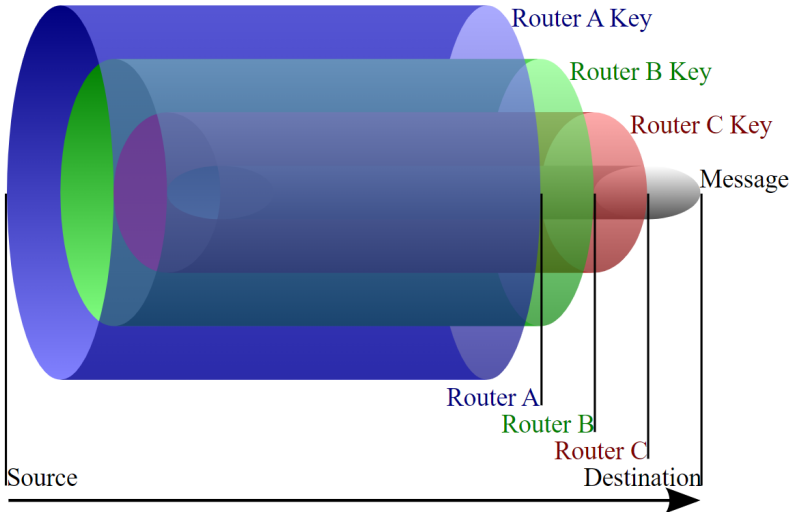
هدف این آزمایش آشنایی دانشجویان با شبکه‌های گمنام سازی است و نحوه تشخیص و جلوگیری از ترافیک ورودی از این سرویس جزء اهداف این آزمایش است.

۶-۲ دستور کار

دانشجویان بایستی یک سرور وب ایجاد کرده و از طریق شبکه تور درخواست فرستاده و ترافیک ورودی را ببینند. برای سمت وب می‌توانند از هاستّای رایگان استفاده کنند.

۶-۳ گزارش

برای گزارش، دانشجویان باید ترافیک ارسالی به وب سرور را دریافت کرده و در گزارش خود نحوه پیاده سازی این سناریو را گزارش کنند.



شکل ۶-۱: شمای کلی رمزنگاری در Tor

آزمایش ۷

Android

برنامه‌های آندرویدی به سبب برخورداری از زبان میانی، امکان لو رفتن کد بسیار بالاتر از برنامه‌های کامپایل شده به زبان ماشین است. بنابراین شناخت ساختار داخلی برنامه‌های آندرویدی حائز اهمیت است.

۷-۱ هدف

هدف این آزمایش آشنایی دانشجویان با ساختار داخلی برنامه‌های آندرویدی است و اینکه چطور می‌توان برنامه‌ای را مهندسی معکوس کرده و روش‌های ممانعت از مهندسی معکوس چیست.

۷-۲ دستور کار

دانشجویان یک برنامه را مهندسی معکوس کرده و بخشی از آن را تغییر می‌دهند. سپس یک برنامه‌ای که خودشان توسعه داده‌اند را با ابزار مبهم ساز مانند proguard مبهم سازند.

۷-۳ گزارش

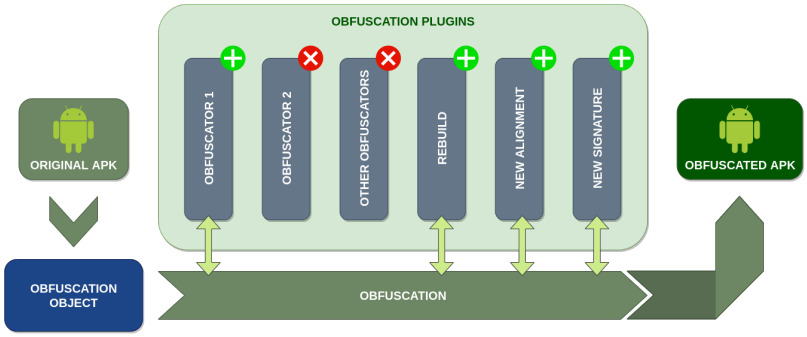
برای گزارش، دانشجویان باید برنامه مبهم شده و برنامه مبهم نشده را از نظر کد میانی با هم مقایسه و تحلیل کنند. برای مطالب بستر می‌توانند از مطالب زیر استفاده کنند.

https://mstajbakhsh.ir/smali-code-injection/

https://mstajbakhsh.ir/t-rex-playing-with-dino/

https://mstajbakhsh.ir/obfuscapk-obfuscate-your-apks/

https://mstajbakhsh.ir/smali-code-injection-playing-with-2048/



شکل ۷-۱: شمای کلی برنامه obfuscapk جهت مبهم سازی برنامه‌های آندروید