**به نام خدا**

**گزارش کار پروژه درس سیستم های نهفته**

**(rasguard)**

**استاد گرامی: دکتر محمد زاد**

**تهیه و تنظیم:**

**امیرحسین علی محمدی**

**ایلیا شادروان**

1. **اضافه کردن فایل readme به پروژه:**

فایل readme توی github که توضیح از کل پروژه هست و نشون میده که توی این پروژه چه چیز هایی پیاده سازی شده.

1. **افزودن فایل dos\_protection:**

این فایل بررسی تمامی پکت هایی که بین دو پورت رزبری انتقال میابند را برعهده دارد. این کد طوری تنظیم شده که با بررسی تمامی پکت های ارسالی از تمامی آدرس آیپی ها، اگر ایپی خاصی بیش از اندازه در یک زمان خاص تعداد زیادی پکت syn و ack و syn-ack و fin ارسال کنه این کد اون آیپی رو به عنوان حمله کننده تشخیص میده و آیپی رو برای 300 ثانیه فیلتر میکنه تا هیچ دسترسی به سرور نداشته باشه.

1. **افزودن فایل های scripts:**

رزبری برای تبدیل شدن به یک فایروال و ناظر تمامی پکت ها نیاز به تنظیماتی دارد که باید به هنگام بوت شدن انجام بشه که این تنظیمات شامل:

1. bridge\_setup.sh:

رزبری برای فوروارد کردن پکت ها از سمت روتر به سمت سرور نیاز به بریج کردن دوپورت ether دارد که با این اسکریپت این دو پورت بریج شده تا پکت ها مستقیم از سمت روتر به سرور بدون تاخیر درجریان باشه.

1. packet\_queue.sh:

برای اینکه کد **dos\_protection** بتونه به همه پکت ها نظارت داشته باشه و همه اونارو بررسی کنه باید یه صفی تشکیل بدیم تا این پکت ها فوروارد بشن به اون صف تا کد ما بتونه این پکت هارو بررسی کنه. ما برای اینکار از کتابخونه **NetfilterQueue** استفاده کردیم.

1. br\_netfilter.sh:

اگه بخوایم به صورت منطقی به ماجرا نگاه کنیم یکی از مشکلاتی که هست اینکه بریجینگ به صورت لایه 2 پکت هارو داره فوروارد میکنه به اون یکی پورت ولی ما اگه بخوایم بررسی کنیم باید به لایه 3 دسترسی داشته باشیم تا هم بتونیم آیپی و هم نوع پکت هارو توسط کد ببینیم برای حل این مشکل از **br\_netfilter** استفاده کردیم.

1. setup\_network.sh:

بعد از بریج کردن دو پورت دسترسی رزبری به اینترنت به طور کامل قطع میشه و ما برای حفظ اتصال از اینترفیس **WIFI** رزبری استفاده میکنیم و باید برای حفظ این ارتباط توی جدول روت رزبری روتی اضافه کنیم که نشون میده برای دسترسی به اینترنت باید همیشه از اینترفیس **WIFI** استفاده کنی.

1. **افزودن فایل های systemd:**

رزبری پای برای اینکه بتونه فایل های اسکریپتی که باید موقع بوت شدن رزبری اجرا بشن رو بخونه و به صورت اتوماتیک اجرا بشه باید از سرویس های **systemd** استفاده کنیم. این سرویس ها به صورت اتوماتیک با تنظیمات منحصر به فردی فایل های اسکریپتی رو اجرا میکنن. این فایل های **systemd** در دایرکتوری **/etc/systemd/system/** قرار دارند.

1. **وجود مشکلاتی در کد اصلی (dos\_protection):**

ما با بررسی و آزمون خطای بسیار متوجه مشکلاتی شدیم یکی از این مشکلات تشخیص آیپی سرور به عنوان حمله کننده توسط کد اصلی ما بود. دلیل این مشکل این بود که وقتی از سمت کاربر به سمت سرور درخواستی ارسال میشه آیپی منبع آیپی کاربر هست ولی بعد از پاسخ سرور آیپی منبع آیپی سرور هست که رزبری پای این آیپی رو به عنوان حمله کننده تشخیص میداد و فیلتر میکرد. ما برای حل مشکل متغییری تعریف کردیم که کد ما شخص ادمین آیپی سرور رو بگیره تا بتونه پکت هارو به صورت دقیق تری از هم دیگه جدا کنه. از دیگر از مشکلات بررسی و فیلترینگ چندین باره یک آیپی بود که این عمل باعث میشد فایروال از لحاظ کیفیت افت بساری داشته باشه و منابع زیادی از رزبری رو استفاده کنه چون حملات DD**oS** به شدت بزرگ بوده و نباید برای فیلتر کردن یک آیپی منابع زیادی از رزبری استفاده کرد تا رزبری پای بتونه درحملات بزرگ هم پکت هارو کامل بررسی کنه و شبکه به خطر نیوفته و تاخیری نداشته باشه برای همین در کد اصلی تغییری ایجاد کردیم که اگر آیپی که به صورت حمله کننده شناسایی میشه بررسی بشه که آیا این آیپی قبلا فیلتر شده یا نه تا شمارشی روی اون آیپی برای فیلترینگش انجام نشه.

1. **افزودن فایل setup\_guide:**

برای تنظیم رزبری به عنوان فایروال نیاز به تنظیمات و نصب پیش نیاز هایی بود که به صورت کامل و با جزییات بالا توی این فایل توضیح داده شده.

1. **افزودن فایل sms\_server:**

ما سیستمی طراحی کردیم که وقتی به سمت سرور حمله ای صورت میگیره بعد از تشخیص این حمله پیامکی به شخص ادمین مبنی بر حمله ای توسط این آیپی به شبکه شناسایی شد. این کار باعث میشه ادمین در لحظه از حمله ای که صورت گرفته باخبر بشه و اگر نیاز به بررسی باشه ادمین رسیدگی کنه. این یه سیستم مانیتورینگ کوچیک برای پروژه ما هستش. ما از اس ام اس سرور های sms.ir برای گرفتن **API** استفاده کردیم تا در حین شناسایی حمله صورت گرفته پیامک به ادمین ارسال بشه.

1. **حل مشکلاتی در پروژه:**

بعد از بررسی نهایی پروژه توی شبکه واقعی متوجه شدیم که سرور ها و آیپی هایی وجود دارند که در دقیقه تعداد زیادی درخواست **syn** ارسال میکنند و به همین دلیل رزبری پای این آیپی هارو به عنوان حمله کننده شناسایی میکرد. برای حل این مشکل تعداد درخواست های پکت های **syn** رو برای فیلتر کردن افزایش دادیم. و همچنین برای اینکه آیپی ها و درخواست ها در لحظه بررسی بشوند تابعی تنظیم کردیم که در هر دقیقه مقدار همه آیپی هایی که درخواست دادن به سرور کلا پاک بشوند و شمارش از اول شروع بشود.