عنوان پروژه: سیستم شناسایی و جلوگیری از حملات شبکه با استفاده از رزبری‌پای

گزارش پروژه

در این چند روز گذشته (اواخر اردیبهشت ماه سال ۱۴۰۴) من به همراه آقای مهدی گرزالدین (که مسئول پروژه و متخصص امنیت هستند) و دوست دیگرمان آقای سجاد کریمی روی یک پروژه مربوط به امنیت شبکه به عنوان کارآموز کار کردیم. این اولین تجربه من در این حوزه بود و چیزهای جدید و جالب زیادی یاد گرفتم.

موضوع پروژه

پروژه ما ساخت یک ابزار برای **تشخیص و جلوگیری از حملات شبکه** بود. این ابزار با زبان پایتون نوشته شد و می‌تواند بسته‌هایی که در شبکه ردوبدل می‌شوند را بررسی کند و اگر حمله‌ای در حال انجام باشد، آن را تشخیص داده و جلوی ادامه حمله را بگیرد.

ما روی سیستمی کار کردیم که در حوزه امنیت شبکه با عنوان‌های زیر شناخته می‌شود:

- **IDS (Intrusion Detection System):** یعنی سیستمی که حمله‌ها را شناسایی کرده و هشدار می‌دهد.
- **IPS (Intrusion Prevention System):** یعنی سیستمی که علاوه بر هشدار، جلوی حمله را هم می‌گیرد (مثلاً بلاک کردن **IP**).

سخت‌افزارهایی که استفاده کردیم؟

هسته اصلی پروژه بر روی یک **رزبری پای (Raspberry Pi)** اجرا شد. رزبری پای یک کامپیوتر کوچک و کم‌مصرف است که می‌تواند کارهای زیادی انجام بدهد. ما رزبری پای رو به شبکه وصل کردیم تا به‌عنوان **gateway** عمل کند و در آن پکت‌ها را ببینیم و حملات را شناسایی کنیم.

علاوه‌برآن، از سه تا لپ‌تاپ (اولی **Regular User** دومی **Attacker User** و سومی **A connected User to the Raspberrypi system**) هم برای اجرای کد، تست حملات و دیدن نتایج استفاده کردیم. لپ‌تاپ‌ها به ما کمک کردند تا بتوانیم پکت‌های مختلفی را در شبکه بفرستیم و ببینیم سیستم چطور واکنش نشان می‌دهد.

چه حملاتی رو بررسی کردیم؟

حملاتی مانند:

- **DoS Attack**: حمله‌ای که با درخواست زیاد باعث ازکارافتادن سیستم می‌شود.

- **Port Scanning**: بررسی پورت‌های باز برای نفوذ.

- **SSH Brute-force**: تلاش زیاد برای حدس‌زدن رمز عبور.

- **ARP Spoofing**: حمله یی که در آن مهاجم با ارسال پاسخ‌های جعلی خود را به‌جای یک دستگاه معتبر و قابل اعتماد جا می‌زند .در نتیجه، دستگاه‌های قربانی اطلاعات‌شان را به‌اشتباه به مهاجم می‌فرستند.

سیستم چگونه جلوی حمله‌ها را می‌گیرد؟

فرض کنید شخصی از یک دستگاه دیگر مرتب پیام‌هایی به شبکه ما ارسال می‌کند. مثلاً برای انجام حمله **DoS** یا حملات دیگر سیستم ما بسته‌های شبکه را بررسی می‌کند (مانند نگهبانی که جلوی در ایستاده و افرادی که وارد می‌شوند را بررسی می‌نماید). اگر تشخیص دهد که از یک **IP** خاص تعداد زیادی درخواست ارسال می‌شود، یا رفتار مشکوکی دارد، این اقدامات را انجام می‌دهد:

۱. نخست یک هشدار تولید می‌کند (در فایل لاگ ثبت می‌نماید).

۲. سپس یک ایمیل برای مدیر سیستم ارسال می‌کند، مثلاً: «شخصی از **IP** فلان در حال انجام حمله **DoS** است!»

۳. آنگاه با استفاده از ابزاری به نام **IPtables** آن **IP** را مسدود می‌نماید؛ یعنی دیگر اجازه نمی‌دهد هیچ بسته‌ای از آن **IP** وارد سیستم شود. و پس از گذشت ۱۰ دقیقه (این زمان را می‌توانیم به دلخواه تغییر بدهیم) اگر آن **IP** دیگر رفتار مشکوکی نداشت، مجدداً آن را آزاد می‌نماید.

من چه کار کردم؟

متاسفانه من در قسمت اصلی کدنویسی نقشی نداشتم؛ چون بچه‌ها مخصوصاً مهدی به خاطر محدودیت زمانی خیلی سریع پیش می‌رفتند و من دانش لازم برای همراهی کد را نداشتم اما:

۱. در اجرای پروژه و کارهای لازم دست به کار شدم.

۲. دیباگ کردن (وقتی کد به مشکل می‌خورد کامل پاک می‌کردیم و بعد از دیباگ دوباره آن را در ترمینال اضافه کرده، سپس Run می‌کردیم)

۳. کار با دستوراتی مانند (اتصال به رزبری پای از طریق پروتکل **SSH** {**ssh pi@raspberrypi.local**} – حذف کردن فایل {**rm file.py**} - آپدیت کردن فایل {**nano file.py**} - اجرای کد {**sudo python3 file.py**}

۴. موقع حمله‌های تستی کمک می‌کردم فایل را حذف کنیم، دوباره اجرا کنیم یا IP بلاک شده را آزاد کنیم.

چه چیزهایی یاد گرفتم؟

با مفاهیم جدیدی آشنا شدم، مثل:

- **Packet**: بسته‌های کوچکی از اطلاعات هستند که در شبکه بین دستگاه‌ها جابجا می‌شوند.

- **IPtables:** ابزاری در لینوکس که می‌تواند مشخص کند کدامIP ها اجازه ورود به سیستم را دارند. ما از آن برای بلاک کردنIP های مهاجم استفاده کردیم .

- **Sniffing**: یعنی‌شنود اتفاقاتی‌که‌درشبکه رخ‌می‌دهند. ما می‌توانستیم‌ببینیم در شبکه چه اتفاق‌ها و چه پکت‌هایی درحال ردوبدل شدن هستند.

- **Port:** درگاه‌هایی برای ارتباط هستند. مثلاً پورت ۲۲ مخصوص **SSH** است که در این پروژه به وفور از آن استفاده کردیم.

در کنار این‌ها، کار با **SSH** را یاد گرفتم؛ یعنی توانستم از راه دور به رزبری‌پای وصل شوم، فایل‌ها را مدیریت کنم و حتی کد اجرا کنم، بدون اینکه مستقیماً به آن دسترسی فیزیکی داشته باشم. و مهم‌تر از همه اینها فهمیدم که چطور می‌توانیم با پایتون کاری کنیم که سیستم خودش حملات را تشخیص دهد، ایمیل هشدار بفرستد، گزارش بنویسد و حتی از ادامه حمله جلوگیری کند.

چالش‌ها و خاطرات باحال

علاوه بر یادگیری، پروژه لحظه‌های بامزه‌ای هم داشت. مثلاً یک‌بار مهدی کابل **VGA** را اشتباهی به کیس وصل کرده بود، در حالی که باید به مانیتور وصل می‌کرد! و همه فکر می‌کردیم رزبری‌پای خراب شده است در حالی که اشتباه، کرده بودیم و فقط می‌گفتیم: «نکنه واقعاً رزبری پای سوخته؟!». همین چیزا باعث شد کلی بخندیم و فضا

خشک و حوصله سربر نباشد. همچنین رزبری‌پای را با هماهنگی از دانشگاه قرض گرفتیم و همین موضوع باعث شد احساس مسئولیت بیشتری داشته باشیم. چون تعداد محدودی در دسترس بود، خیلی با دقت و انگیزه کار کردیم تا هم نتیجه بگیریم و هم از فرصتی که در اختیارمان گذاشته شده بود، بهترین استفاده را بکنیم.

نتیجه‌گیری

این تجربه باعث شد با دنیای امنیت شبکه از نزدیک آشنا بشم .فهمیدم که حتی با یک سیستم کوچک مثل رزبری پای هم می‌توانیم حملات را شناسایی و متوقف کنیم. این اولین تجربه من در یک پروژه در حوزه امنیت شبکه بود، اما واقعاً برایم جالب و جذاب بود. علاقه‌مند شدم بیشتر یاد بگیرم و دوست دارم در آینده هم در پروژه‌های مشابه حضور داشته باشم و این مسیر را ادامه بدهم.

حالا اگر کسی بپرسد پروژه شما چه بود، در یک جمله یا خیال راحت می‌گویم:

"ما سیستمی ساختیم که ترافیک شبکه را زیر نظر می‌گیرد، حملات را شناسایی می‌کند، هشدار می‌فرستد و برای جلوگیری از آن‌ها وارد عمل می‌شود."