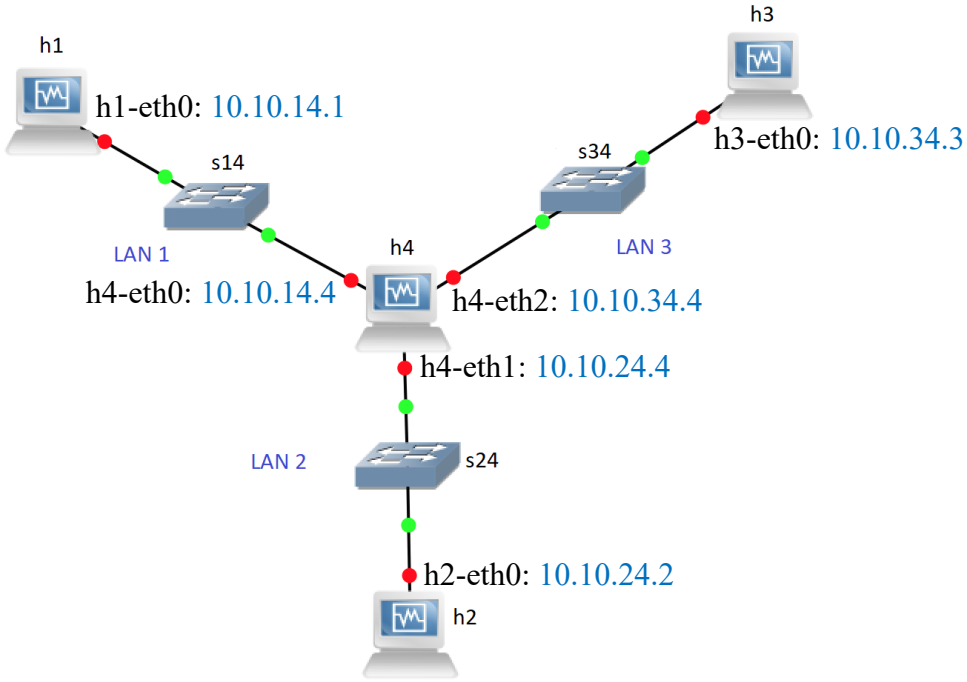
آزمایشگاه شبکه

آزمایش ۳: شبیه‌سازی حملهٔ فرد میانه (Man-in-the-Middle)

الف) پیکربندی توپولوژی شبکهٔ محلی

پیش‌شرطِ انجام آزمایش جاری، پیکربندی توپولوژی شکل ۱ است که قبلاً در قالب آزمایش ۱ انجام داده‌اید. اسکریپت پایتون lab3.py را ملاحظه کرده و در صورت نیاز، آن را اصلاح نمایید تا کلیهٔ پیکربندی‌های مورد نظر روی کلیهٔ ماشین‌ها و لینک‌ها به‌درستی انجام شده باشد.

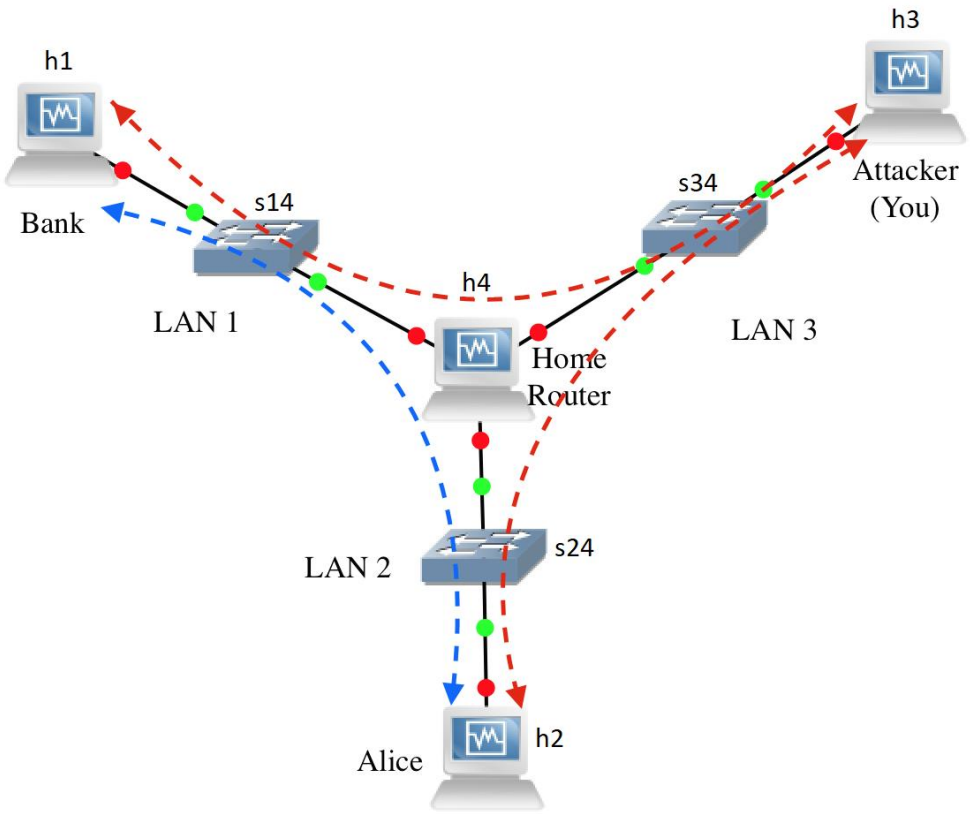


شکل ۱- توپولوژی شبکهٔ محلی پیکربندی شده در آزمایش ۱

ب) تعریف نقش گره‌های شبکه برای پیاده‌سازیِ سناریویِ حمله

- به منظور پیاده‌سازیِ حملهٔ «فرد میانه»، گره‌های توپولوژیِ شکل ۱ را بر اساس نقش جدیدشان برچسب می‌زنیم (شکل ۲ را ملاحظه نمایید).
  - h1 نقش سِرورِ بانک را بازی می‌کند.
  - h2 را کاربر Alice در نظر می‌گیریم که در پی دسترسی به حساب بانکی‌اش است.
  - h3 سِرور مورد استفادهٔ مهاجم است و هدف، تغییر مسیر تعاملات بانکی Alice به مقصد این سِرور و سرقت پول وی می‌باشد.
  - h4 نیز روتر مورد استفادهٔ Alice برای ارتباط گرفتن با بانک است. جلوتر، فرض خواهیم کرد که این روتر برای پیاده‌سازی حمله، دستخوش دستکاری‌هایی خواهد شد.

- فرض می‌کنیم که یک ping موفق بین Alice و بانک معادل با یک عملیات انتقال پول موفق بین آنهاست. هدفِ مهاجم این است که به Alice و بانک القاء کند که دارای یک ارتباط موفق هستند (که در شکل ۲ با پیکان آبی نشان داده شده) در حالی که در واقعیت، هر محاوره‌ای میان این دو از سِرور مهاجم (h3) گذر داده می‌شود (پیکان‌های قرمز در شکل ۲).
- فرض بر این است که برای پیاده‌سازی حمله تنها می‌توان روی روتر h4 و نیز سِرور مهاجم (h3) تغییر ایجاد کرد.



شکل ۲- توپولوژی شبکهٔ محلی تحت حملهٔ «فرد میانه»

ج) مکانیزمِ «فیلترسازی بر مبنای مسیر معکوس» در روترِ h4

- جلوتر خواهیم دید که به منظور پیاده‌سازیِ حملهٔ «فرد میانه»، در مرحله‌ای نیازمند جعل آدرس IP کاربر Alice خواهیم بود (IP spoofing). یکی از راهکارهای پیشگیری از چنین حملاتی در روترها، مکانیزمی است تحت عنوان «فیلترسازی بر مبنای مسیر معکوس» (Reverse Path Filtering یا RPF).
- مکانیزم RPF ابتدا آدرس فرستنده بسته را در نظر گرفته و بررسی می‌کند که بسته‌های ارسالی از آن آدرس، به طور قانونی باید از کدام اینترفیس دریافت شوند. سپس اینترفیس بدست آمده را با اینترفیسی که بسته از آن وارد شده، مقایسه می‌نماید و در صورت مغایرت، بسته را دور می‌ریزد. جهت آشنایی بیشتر با RPF، به اسلایدهای ضمیمهٔ این آزمایش با نام Man-in-the-Middle.pdf مراجعه کرده و آنها را مطالعه نمایید.
- با توجه به اینکه برای پیاده‌سازی حمله، سِرور مهاجم باید قادر به فوروارد کردن بسته‌ها نیز باشد، این قابلیت را برای h3 فعال می‌نماییم (با اجرای دستوری نظیر آنچه در آزمایش ۱ فرا گرفتید).

د) پیکربندی حملهٔ «فرد میانه»

- به منظور پیکربندی حمله، از قابلیت ویژه‌ای بهره می‌گیریم که کِرنل لینوکس برای پردازش بسته‌ها در اختیار adminهای شبکه می‌گذارد. در واقع، یک برنامهٔ سمت کاربر به نام iptables از سوی کِرنل لینوکس پشتیبانی می‌شود که از طریق آن، ما می‌توانیم با تعریف زنجیره‌ای از قوانین، پردازش‌های مورد نظر خود را روی بسته‌های IPv4 انجام دهیم.
- با استفاده از برنامهٔ iptables، ابتدا روتر h4 را طوری دستکاری می‌کنیم تا ترافیکِ به مقصد بانک را برای سِرور مهاجم بفرستد. البته، از آنجایی که Alice ممکن است دارای حجم زیادی فعالیت‌های شبکه‌ای غیرمرتبط با مصرف پهنای باند بالا داشته باشد (مثلاً: بازی آنلاین و غیره)، باید به طریقی بتوانیم فقط نوع ترافیکی را که به آن علاقه‌مندیم (بسته‌های ICMP) و از سوی آدرس IP کاربر Alice هم منشأ می‌گیرد (10.10.24.2) برگزینیم.

سوال ۱- دستورات لازم برای تحقق هدف فوق را بنویسید.

- حال، با راه‌اندازیِ برنامهٔ WireShark روی h3 بررسی کنید که آیا هدایت ترافیکِ بانکی از روتر h4 به سوی سِرور مهاجم موفق بوده است یا خیر.
- در گام بعدی، باید سِرور مهاجم (h3) را طوری پیکربندی نماییم که ترافیک وارده از سوی سیستم Alice را دریافت کرده، آن را دستکاری نموده و در نهایت برای بانک بفرستد. برای این منظور، باید آدرس IP مقصد بسته را با آدرس IP سِرور بانک (10.10.14.1) جایگزین نماییم. امّا، هنگام خروج از h3، آدرس IP مبدأ بسته، باید برابر با آدرس سیستم Alice قرار داده شود (به دلیل همان مکانیزم فیلترسازی بر مبنای مسیر معکوس).
- تا اینجا، روی سِرور مهاجم (h3)، باید بسته‌هایی از مبدأ 10.10.24.2 به مقصد 10.10.34.3 (و برعکس) را ملاحظه نمایید و همینطور از مبدأ 10.10.34.3 به مقصدِ 10.10.14.1 (و برعکس).
- با راه‌اندازیِ WireShark روی سِرور بانک (h1)، وضعیت بسته‌های دریافتی توسط بانک را بررسی کنید.
- روی سِرور بانک (h1) هم باید بسته‌هایی از مبدأ 10.10.34.3 ملاحظه کنید. امّا به این ترتیب، بانک به سادگی متوجه غیرخودی بودن این بسته‌ها خواهد شد (مثلاً: سِرور بانک ممکن است دارای یک لیست «کنترل دسترسی» باشد که صرفاً به ارتباطات وارده از سوی آدرس‌های IP مشتریانش اجازهٔ دسترسی می‌دهد). در این گام، دستورات iptablesای پیشنهاد دهید که با استفاده از آنها بتوانید روتر h4 را طوری پیکربندی کنید که کاربر Alice را به جایِ سِرور مهاجم جا بزند (تعویض آدرس مبدأ بسته‌های h3 به h1).

سوال ۲- دستورات لازم برای تحقق هدف فوق را بنویسید.

- به این ترتیب، کار پیاده‌سازی حملهٔ «فرد میانه» تمام می‌شود. فقط به دو سوال دیگر پاسخ دهید:

سوال ۳- آیا این حمله را می‌توانستیم صرفاً با دستکاری جداول مسیریابی روتر h4 محقق کنیم؟

سوال ۴- آیا در محیط LAN مورد مثال ما، کاربر Alice راهکاری برای تشخیص اینکه تحت حمله قرار گرفته دارد (البته به جز اینکه متوجه خالی شدن حساب بانکی‌اش بشود)؟!