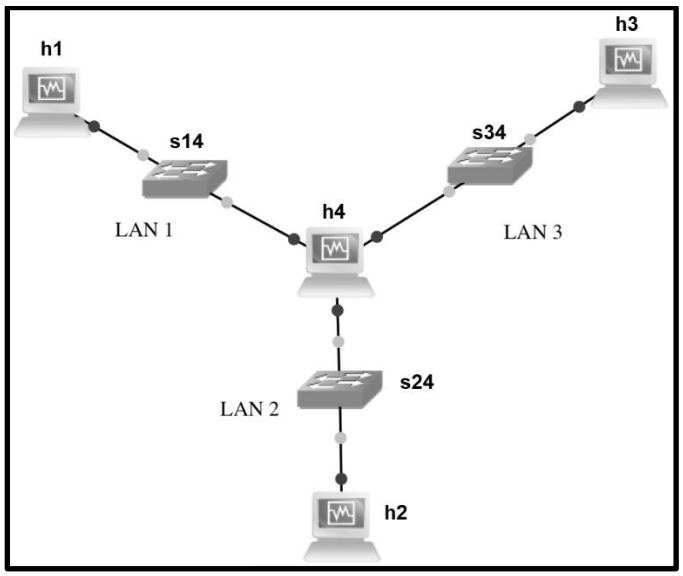
آزمایشگاه شبکه

شبیه‌سازیِ حملهٔ مرد میانه (Man-in-the-Middle)

الف) پیکربندی توپولوژی شبکهٔ محلی

پیش‌شرطِ انجام آزمایش جاری، پیکربندی توپولوژی شبکهٔ محلیِ نمایش داده شده در شکل ۱ است که قبلاً در قالب آزمایش جلسهٔ گذشته انجام داده‌اید.

سؤال ۱- این بار به جای پیکربندیِ گام-به-گام در محیط دستوری، اسکریپت پایتون lanTopo.py را طوری تکمیل کنید که به محض اجرا، کلیهٔ پیکربندی‌های مورد نظر را روی کلیهٔ ماشین‌ها و لینک‌ها انجام دهد.



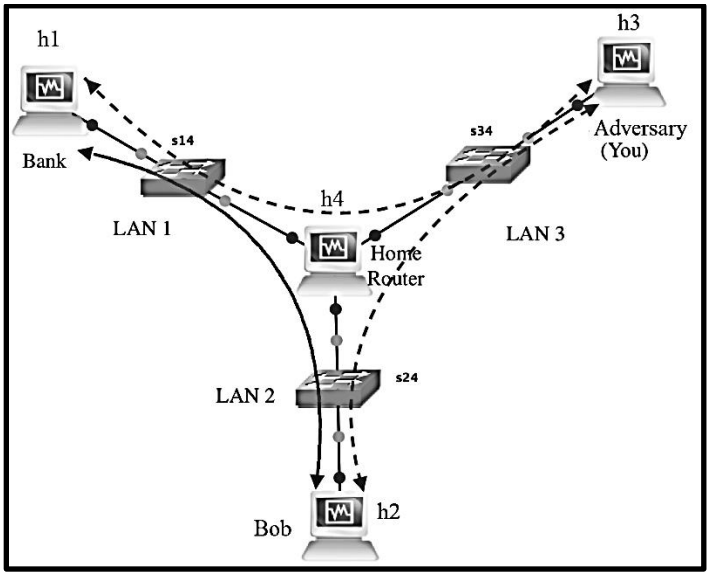
شکل ۱- توپولوژی شبکهٔ محلی پیکربندی شده در آزمایش قبلی

ب) تعریف نقش گره‌های شبکه برای پیاده‌سازیِ سناریویِ حمله

- به منظور پیاده‌سازیِ حملهٔ «مرد میانه»، گره‌های توپولوژیِ شکل ۱ را بر اساس نقش جدیدشان برچسب می‌زنیم (شکل ۲ را ملاحظه نمایید).
  - h2 را کاربر Bob در نظر می‌گیریم که در پی دسترسی به حساب بانکی‌اش است.
  - h1 نقش سِرورِ بانک را بازی می‌کند.
  - h4 نیز روتر مورد استفادهٔ Bob برای ارتباط گرفتن با بانک است. جلوتر، فرض خواهیم کرد که این روتر برای پیاده‌سازی حمله، دستخوش دستکاری‌هایی خواهد شد.

- h3 نیز سِرور مورد استفادهٔ موجودیت «متخاصم» است و هدف، تغییر مسیر تعاملات بانکی Bob به مقصد این سِرور و سرقت پول وی می‌باشد.

- فرض می‌کنیم که یک ping موفق بین Bob و بانک معادل با یک عملیات انتقال پول موفق بین آنهاست. هدفِ موجودیت «متخاصم» این است که به Bob و بانک القاء کند که دارای یک ارتباط موفق هستند (که در شکل ۲ با پیکان منحنی توپر نشان داده شده) در حالیکه در واقعیت، هر محاوره‌ای مابین این دو از سِرور متخاصم (h3) گذر داده می‌شود (خطوط منحنی خط-چین در شکل ۲).
- فرض بر این است که برای پیاده‌سازی حمله تنها می‌توان روی روتر Bob (h4) و نیز سِرور متخاصم (h3) تغییر ایجاد کرد.



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

ج) غیرفعال‌سازیِ مکانیزمِ "فیلترسازی بر مبنای مسیر معکوس" در روترِ Bob

- جلوتر خواهیم دید که به منظور پیاده‌سازیِ حملهٔ «مرد میانه»، در مرحله‌ای نیازمند جعل آدرس IP کاربر Bob 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).

- جهت آشنایی بیشتر با سازوکار RPF، به اسلایدهای ضمیمهٔ این آزمایش با عنوان فایلِ Man-in-the-Middle (supplmenets).pdf مراجعه کرده و آنها را مطالعه نمایید.

- برای میسّر ساختن امکان حملهٔ «مرد میانه»، ابتدا مکانیزمRPF در روتر Bob را غیرفعال می‌سازیم. البته، بعداً در رابطه با سؤال ۲ از بخش (د) و مشکل دیگری که آنجا برخواهیم خورد، ملاحظه خواهیم کرد که در این آزمایش

اساساً لزومی به این کار نبود. با این حال، انجام این آزمایش، بهانه مناسبی است برای یادگیری در رابطه با این قابلیت در سازوکار شبکه‌ای لینوکس.

- به منظورِ غیرفعال‌سازی RPF روی تمامی اینترفیس‌های روتر Bob، اسکریپت واقع در فولدر ~/lab1 با عنوان disableRPF.sh را اجرا نمایید.

- حال، با توجه به اینکه برای پیاده‌سازی حمله، سِرور متخاصم باید قادر به فوروارد کردن بسته‌ها نیز باشد، این قابلیت را برای h3 فعال نمایید (با اجرای دستوری نظیر آنچه در آزمایش قبلی فرا گرفتید).

د) پیکربندی حملهٔ «مرد 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 Bob را طوری دستکاری می‌کنیم تا ترافیکِ به مقصد بانک را برای سِرور متخاصم بفرستد. البته، از آنجاییکه Bob 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 علاقمندیم (بسته‌های ICMP) و از سوی آدرس IP کاربر Bob هم منشأ می‌گیرد (10.10.24.2) برگزینیم.

سؤال ۲- دستورات لازم برای تحقق هدف فوق را بنویسید (برای آشنایی با چگونگی کار با iptables و مکانیزم‌های پردازش بسته به اسلایدهای ضمیمهٔ آزمایش با عنوانِ Man-in-the-Middle (supplement).pdf **رجوع نمایید).**

- حال، با راه‌اندازیِ برنامهٔ WireShark روی h3 بررسی کنید که آیا هدایت ترافیکِ بانکی از روتر Bob به سوی سِرور متخاصم موفق بوده است یا خیر.
- در گام بعدی، باید سِرور متخاصم (h3) را طوری پیکربندی نماییم که ترافیک وارده از سوی سیستم Bob 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 Bob قرار داده شود (چرا؟).
- تا اینجا، روی سِرور متخاصم (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 Bob (h4) را طوری پیکربندی کنید که کاربر Bob را به جایِ سِرور متخاصم جا بزند (تعویض آدرس مبدأ بسته‌های h3 به h1).

سؤال ۳- دستورات لازم برای تحقق هدف فوق را بنویسید.

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

سؤال ۴- آیا این حمله را می‌توانستیم صرفاً با دستکاری جداول مسیریابی روتر Bob محقق کنیم؟

سؤال ۵- آیا در محیط LAN مورد مثال ما، کاربر Bob راهکاری برای تشخیص اینکه تحت حمله قرار گرفته دارد (البته به جز اینکه متوجه خالی شدن حساب بانکی‌اش بشود)؟!
