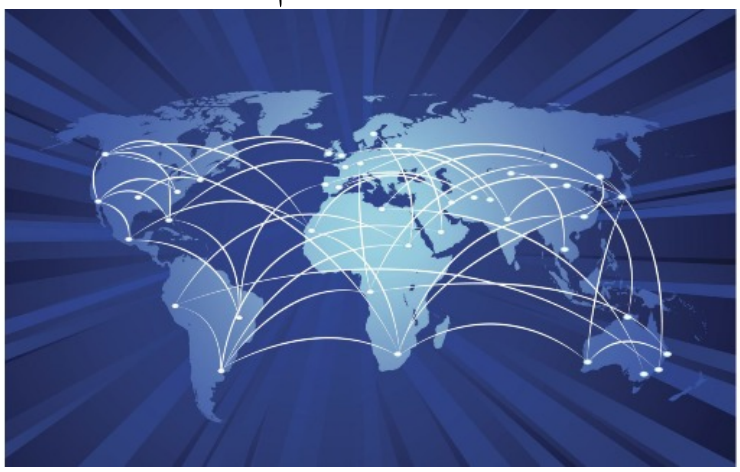
بسم الله الرحمن الرحیم



دانشکده مهندسی کامپیوتر

آزمایشگاه شبکه‌های کامپیوتری

استاد : خانم دکتر زهرا رشیدی

گزارش کار آزمایش دو

سید محمد مهدی رضوی

فروردین ۱۴۰۲

فهرست مطالب

۱ سوال اول

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

```
(h4) iptables -t nat -A PREROUTING -p icmp -s 10.10.24.2 -d 10.10.14.1 -j DNAT
–to 10.10.34.3
```

```
(h3) iptables -t nat -A PREROUTING -p icmp -s 10.10.24.2 -d 10.10.34.3 -j DNAT
–to 10.10.14.1
```

۲ سوال دوم

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

```
(h4) iptables -t nat -A PREROUTING -p icmp -s 10.10.24.2 -d 10.10.14.1 -j DNAT
–to 10.10.34.3
```

```
(h3) iptables -t nat -A PREROUTING -p icmp -s 10.10.34.3 -d 10.10.14.1 -j DNAT
–to 10.10.24.2
```

در تمام دستورات فوق باید فایل `disableRPF.sh` را اجرا نماییم که تشخیص صورت نگیرد.

۳ سوال سوم

آیا این حمله را می‌توانستیم صرفا با دستکاری جداول مسیریابی روتر `h4` محقق کنیم ؟

با توجه به این که در حین این حمله سیستم `Reverse Path Filtering (RPF)` غیرفعال شده است و هم آدرس‌های مبدا بسته‌ها تغییرکرده است ، اگر بتوان با دستکاری جداول مسیریابی این کارها را انجام داد که امکان پیاده‌سازی حمله از آن طریق نیز وجوددارد و گرنه در غیراین صورت نمی‌توان چنین‌کاری انجام‌داد.

۴ سوال چهارم

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

شاید به طور دقیق نتواند بررسی کند که مورد حمله قرارگرفته است اما از روی شواهد می‌توان به مساله مشکوک شد.
چرا که میزان زمان `rtt` , `ttl` وابسته به تعداد روترها میان مبدا و مقصد خواهد بود ، در صورتی که این زمان کاهش پیدا کند ، می‌توان این فرضیه را مطرح نمود که ممکن است یک روتر اضافی در این میان دارد به شنود داده بین مبدا و مقصد حقیقی می‌پردازد.
درنتیجه یکی از رویکردهایی که می‌توان از این کار جلوگیری کرد پینگ گرفتن دایمی میان مبدا و مقصد حقیقی خواهد بود.