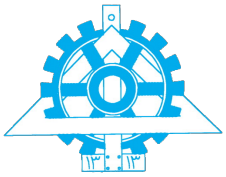
In the name of Allah

بسم الله‌الرحمن الرحیم

Network management and security Laboratory Manual



University of Tehran
دانشگاه تهران

School of Electrical and Computer Engineering
دانشکده مهندسی برق و کامپیوتر

Computer Network Lab
آزمایشگاه شبکه‌های کامپیوتری

Dr. Ahmad Khonsari - احمد خونساری
a_khonsari@ut.ac.ir

Amir Haji Ali Khamseh'i - امیر حاجی علی خمسه‌ء
khamse@ut.ac.ir

Sina Kashi pazha - سینا کاشی پزها
sina_kashipazha@ut.ac.ir

Mohammad Ali Shahsavand - محمد علی شاهسوند
mashahsavand@ut.ac.ir

Amirahmad Khordadi - امیر احمد خردادی
a.a.khordadi@ut.ac.ir

November 23, 2018

۲ آذر ۱۳۹۷

مقدمه

امنیت ارتباطات یکی از مهم‌ترین مسائل حال حاضر شبکه‌های ارتباطی است. در این آزمایش بنا داریم مواردی از لو رفتن رمز عبور و استفاده از iptables برای جلوگیری از دسترسی ناخواسته به هاست‌ها را بگیریم.
در کنار این موارد آشنایی کوتاهی با پروتکل ftp و tftp خواهیم داشت. از این دو پروتکل برای انتقال فایل استفاده می‌شود. پروتکل tftp انتقال فایل را با استفاده از پروتکل UDP انجام می‌دهد و خود به مدیریت ارسال و دریافت درست بسته‌ها می‌پردازد، استفاده از آن ساده‌تر، سرعت آن کندتر و پیاده‌سازی آن نسبت به ftp راحت‌تر است. در مقابل پروتکل ftp از پروتکل TCP استفاده می‌کند و نیازی نیست پروتکل ftp خود را درگیر این مسائل کند. از هر دوی این پروتکل‌ها به دلیل فقدان امنیت استفاده نمی‌شود.

1 iptables

۱.۱ گام اول

در این گام قصد داریم به کمک iptables یک فایروال روی یکی از هاست‌ها درست کنیم و بسته‌های ورودی و خروجی به آن را بررسی کنیم. برای شروع توپولوژی پیش‌فرض mininet را اجرا کرده و دستور زیر را روی **h1** اجرا کنید.

```
iptables -A INPUT -v -p TCP --dport 23 -j DROP
```

با اجرای دستور **iptables -L -v** می‌توانید اضافه شدن قاعده‌ی بالا به جدول فیلترها را ببینید. روی h1 و wireshark h2 را اجرا کنید و سپس از h2 به ه۱، telnet بزنید. (دستور telnet 10.0.0.1 را روی h2 اجرا کنید)

- آیا با اجرای دستور telnet روی h2 پاسخی از h1 دریافت می‌کنید؟
- با استفاده از خروجی wireshark، الگوریتم باز ارسال exponential بَچکفف را توضیح دهید.

۲.۱ گام دوم

با استفاده از دستور زیر قاعده‌ای که در گام قبلی ساختیم را حذف کنید.

```
iptables -D INPUT -v -p TCP -dport 23 -j DROP
```

با استفاده از دستور زیر قاعده‌ی جدیدی که بسته‌ها را به جای DROP، REJECT می‌کند، اضافه کنید.

```
iptables -A INPUT -v -p TCP --dport 23 -j REJECT --reject-with tcp-reset
```