بهراد اسلامی فر

مقدمه ای از دیوار آتش (iptables)

شبکه کاربردی

آشنایی کوتاه برای یک کاربر معمولی

۱۳۹۰-۲-۵

سرفصل های سمینار

- مفاهیم اولیه
  - لایه های شبکه
  - جریان اطلاعات در شبکه
  - لایه Datalink
  - لایه Network
  - لایه Transport
  - لایه Application
- پیکربندی
- عیب یابی

لایه های شبکه

۷- Application
۶-
۵-
۴- Transport
۴- Network
۲- Datalink
۱-

جریان اطلاعات در شبکه

- شبکه محلی (Switching)
  - مثال دادزدن توی شبکه
- Network و Internetwork
- مثال صندوق پستی و تحویل گیرنده
  - پاتوق آخر gateway
  - دادزدن به سمت gateway

لایه Datalink

- Switching
- Mac address
- معرفی ebtables

- Source address
- Destination Address

- Source and destination port
- Connection tracking
- Packet state
  - New, established , related , invalid
- Packet flags
  - Syn , ack و ...

پیکربندی (معرفی netfilter)

- Netfilter
  - به عنوان بخشی از کرنل
- Iptables
  - اینترفیسی که در اختیار کاربر است

پیکربندی (معرفی iptables)

- جدول ها tables
  - filter , nat , mangle , raw
- زنجیره ها chains
  - هر جدول زنجیر های خود را دارد
  - INPUT و OUTPUT از جدول filter
- Actionها
  - ACCEPT و DROP و ...

پیکربندی (syntax)

- مشخص کردن جدول
  - iptables -t filter
- مشخص کردن زنجیره
  - iptables -t filter -A INPUT
- مشخص کردن پروتکل
  - iptables -t filter -A INPUT -p ip

پیکربندی

- مشخص کردن جزییات پروتکل
  - iptables -t filter -A INPUT -p ip -s ۱۹۲.۱۶۸.۱.۰/۲۴
- مشخص کردن عمل یا action
  - iptables -t filter -A INPUT -p ip -s ۱۹۲.۱۶۸.۱.۰/۲۴ -j DROP

عیب یابی و بررسی صحت عملکرد

- iptables -L -v
  - Chain INPUT (policy DROP ۲۸ packets, ۲۳۱۶ bytes)
  - pkts bytes target prot opt in out source destination
  - ۶۱۹۲۹ ۳۶۹۸K tcp -- any any anywhere anywhere tcp dpt:ssh state NEW recent: SET name: DEFAULT side: source
  - ۱۴۰۱۵ ۸۳۸K ACCEPT tcp -- eth۰ any anywhere anywhere tcp dpt:ssh state NEW
  - ۹۳ ۵۲۶۴ ACCEPT tcp -- eth۰ any anywhere anywhere tcp dpt:smtp state NEW

عیب یابی (پاک کردن رول های نوشته شده)

- پاک کردن کلیه رول ها
  - iptables -t <table> -F
- پاک کردن یک رول مشخص
  - iptables -t <table> -D <chain> <complete rule>
  - iptables -t <table> -D <chain> [rulenumber]
- برای دیدن شماره رول ها
  - iptables -L --line-numbers