Лабораторна робота №7

з дисципліни «мережеві технології»

«Засоби фільтрації пакетів та брандмауери»

Виконав: студент групи ІП-73мп
Олександр Ковальчук

Контрольні запитання:

1. На яких рівнях еталонної моделі OSI може виконуватися фільтрація в IPFW?

   На мережевому і транспортному

2. Переваги і недоліки різних типів брандмауерів.

Packet filter

+ Відносна простота конфігурації (будується на структурі пакета)

- Через фрагментацію пакети можуть обходити фільтр

- Складність підтримування (додавання та оновлення інформації) повного списку доступів

- Деякі служби (наприклад, де номер порту стає відомим тільки в момент встановлення з'єднання) не можуть бути відфільтровані

Proxy filter

+ Надають високий рівень захисту

- При зломі цього фільтра зловмисник отримує доступ до внутрішньої мережі

- Додавання нових служб — непроста задача

- Низька швидкодія при високих навантаженнях

- Наявні в ОС вразливості можуть бути використані для його злому

Stateful packet filter

+ Виконується аналіз кожного пакета окремо, під час якого пакет звіряється з даними про дозволені з'єднання

+ Забезпечує більшу пропускну здатність, ніж packet filter або proxy-filter

3. З якою метою можуть використовуватися ключові слова in і out в IPFW?

Ключові слова in та out можуть використовуватися, щоб застосувати правило виключно для вхідних та вихідних пакетів відповідно.

4. Яким чином в IPFW реалізується фільтр, що враховує стан?

   Фільтр пакетів, що враховує стан даних, зберігає інформацію про кожнен оброблений пакет даних. Кожен раз при створенні з'єднання з зовнішнім або внутрішнім вузлом інформація про це з'єднання зберігається в спеціальній таблиці контролю стану потоку даних (stateful session flow table). У таблиці контролю стану потоку даних міститься інформація про ініціаторів та цілі з'єднань, номери портів, службова інформація протоколу TCP і додаткові параметри для кожного з'єднання, які відповідають строго визначеним сеансам зв'язку. Оскільки ініціатором сеансу зв'язку є брандмауер, то, таким чином, зв'язок клієнта з даним вузлом мережі відбувається за допомогою брандмауера і, як наслідок, всі вхідні і вихідні пакети проходять перевірку в таблиці контролю стану. Дані можуть пройти через брандмауер тільки в тому випадку, якщо їх параметри відповідають якому-небудь з'єднанню, описаному в таблиці контролю станів.

5. Чи може пакету відповідати кілька правил в IPFW?

   Так. Якщо набір правил включає одне або кілька правил з опцією keep-state, то IPFW передбачає роботу зі збереженням стану (stateful behaviour), тобто при успішному зіставленні створюватиме динамічні правила, відповідні конкретним параметрам (адресам і портам) пакета.

6. З якою метою в IPFW вводиться правило з номером 65535?

   Конфігурація завжди включає стандартне правило із номером 65535, яке не може бути змінено і яке відповідає будь-якому пакету. З цим стандартним правилом може бути пов'язана дія deny або allow, залежно від конфігурації ядра.

7. Які дії можуть виконуватися над пакетом в правилі IPFW?

   - allow — пакет буде пропущено далі

- deny — пакет буде відхилено, а відпраник НЕ буде про це повідомлений
- reject — пакет буде відхилено і відправнику буде надіслано ICMP-повідомлення, що вузол мережі недоступний
- unreach <code> — те ж, що і reject, тільки дозволяє вказати код помилки
- reset — пакет буде відхилено, а відправнику надісланий TCP-пакет з прапорцем RST
- count — порахувати пакет і передати далі по списку правил
- divert <port> — переслати пакет в порт <port>
- fwd <ipaddr> [,port] змінити next-hop для пакета

8. Типи брандмауерів і їх особливості.
   - Фільтр пакетів - це зазвичай брандмауер, який здійснює фільтрацію пакетів TCP / IP на транспортному або мережевому рівні (Internet) стеку протоколів TCP / IP. Дані можуть бути піддані фільтрації, якщо вони передаються по мережі, заснованої на стандартному стеку протоколів TCP / IP (або будь-якому іншому стандартному стеку протоколів). Оскільки розташування полів, які містять інформацію (наприклад, IP-адреса відправника даного пакета, IP-адреса одержувача і порт), в пакеті відомо, на основі цих даних можна здійснювати фільтрацію пакетів. Слід також зазначити, що фільтрами пакетів аналізується лише статична інформація заголовків пакетів. Правила, згідно з якими буде працювати брандмауер, створюються на основі деяких критеріїв, які включають в себе адреси відправників пакетів і адреси одержувачів пакетів.
   - Проксі-фільтри - це пристрої, що виконують функції брандмауерів і перевіряють пакети на більш високому рівні еталонної моделі OSI, (зазвичай рівень 4 семирівневої моделі OSI), ніж розглянуті вище фільтри пакетів. З огляду на цю особливість проксі-фільтрів, можна зробити висновок про те, що вони надають високий рівень захисту, який, однак, негативно позначається на

продуктивності всієї системи. Ці пристрої приховують важливі дані про користувача за допомогою з'єднання останнього через проміжний сервер. Користувач отримує доступ до мережі шляхом відкриття сеансу і проходження через певні процедури аутентифікації і авторизації. Це означає, що користувач може з'єднатися з зовнішніми серверами за допомогою спеціального додатку (проксі-сервера), що використовується в якості шлюзу в зовнішню незахищену зону.

- Фільтри пакетів, які враховують стан. У цьому типі брандмауерів поєднуються найкращі технології звичайних фільтрів пакетів і проксі-фільтрів. Фільтр пакетів, що враховує стан даних, зберігає інформацію про кожен оброблений пакет даних. Кожен раз при створенні з'єднання з зовнішнім або внутрішнім вузлом інформація про це з'єднання зберігається в спеціальній таблиці контролю стану потоку даних (stateful session flow table).
- У таблиці контролю стану потоку даних міститься інформація про ініціаторів та цілі з'єднань, номери портів, службова інформація протоколу TCP і додаткові параметри для кожного з'єднання, які відповідають строго визначеним сеансам зв'язку. І оскільки ініціатором сеансу зв'язку є брандмауер, то, таким чином, зв'язок клієнта з даним вузлом мережі відбувається за допомогою брандмауера і, як наслідок, всі вхідні і вихідні пакети проходять перевірку в таблиці контролю стану. Дані можуть пройти через брандмауер тільки в тому випадку, якщо їх параметри відповідають якому-небудь з'єднанню, описаному в таблиці контролю станів.

9. Обробка пакетів в IPFW.

Брандмауер перевіряє по IPFW правилах кожен вхідний і вихідний IP-пакет, поки не буде знайдено відповідне правило. Після того, як відповідне правило знайдено, виконується дія, прописана в цьому правилі. При цьому пакет може покинути брандмауер або бути введеним в брандмауер повторно залежно від характеру дії, що визначається цим правилом, а також системних установок.

Налаштування файрволу

```
#!/bin/sh

# ==============
# Firewall rules
# ==============
cat << 'EOF' >/etc/ipfw.rules
# Drop all existing rules
ipfw -q flush

cmd="ipfw -q add"
ks="keep-state"

# Allow loopback
$cmd 65533 allow all from any to any via lo0
$cmd 65534 check-state

# Allow FTP to 10.18.49.0/24.
ftp_net="10.18.49.0/24"
$cmd 00100 allow tcp from me to $ftp_net 20 out setup $ks
$cmd 00101 allow udp from me to $ftp_net 20 out $ks
$cmd 00102 allow tcp from me to $ftp_net 21 out setup $ks
$cmd 00103 allow udp from me to $ftp_net 21 out $ks

# Allow POP3 to any network
$cmd 00104 allow tcp from me to any 106 out setup $ks
$cmd 00105 allow tcp from me to any 110 out setup $ks
$cmd 00106 allow udp from me to any 110 out $ks

# Allow SMTP to server
$cmd 00107 allow tcp from any to me 25 in setup $ks
$cmd 00108 allow udp from any to me 25 in $ks

# Allow IP from/to 10.18.48.0/24
ip_net="10.18.48.0/24"
$cmd 00109 allow ip from $ip_net to me in $ks
$cmd 00110 allow ip from any to $ip_net out $ks

# count incoming TCP
$cmd 00111 count tcp from any to me in

# log incomminf traffic from 10.18.51.0/24
logged_net="10.18.51.0/24"
$cmd 00112 allow log any from $logged_net to any
EOF

# =====================
# Startup configuration
# =====================
cat >/etc/rc.conf <<EOF
ifconfig_em0="DHCP"

ifconfig_em1="inet 10.18.51.100 netmask 255.255.255.0"
dhcpd_enable="YES"
```

```
sshd_enable="YES"
hostname="monica"

# firewall_enable="YES"
firewall_script="/etc/ipfw.rules"
firewall_quiet="YES"
firewal_logging="YES"
EOF

mkdir -p /var/log/ipfw
touch /var/log/ipfw/ipfw.log
chmod -R go-rwx /var/log/ipfw

# ======================
# Reboot and run firewall
# ======================

reboot
service ipfw onestart
```

```
# ipfw list
00100 allow tcp from me to 10.18.49.0/24 dst-port 20 out setup keep-state :defau
lt
00101 allow udp from me to 10.18.49.0/24 dst-port 20 out keep-state :default
00102 allow tcp from me to 10.18.49.0/24 dst-port 21 out setup keep-state :defau
lt
00103 allow udp from me to 10.18.49.0/24 dst-port 21 out keep-state :default
00104 allow tcp from me to any dst-port 106 out setup keep-state :default
00105 allow tcp from me to any dst-port 110 out setup keep-state :default
00106 allow udp from me to any dst-port 110 out keep-state :default
00107 allow tcp from any to me dst-port 25 in setup keep-state :default
00108 allow udp from any to me dst-port 25 in keep-state :default
00109 allow ip from 10.18.48.0/24 to me in keep-state :default
00110 allow ip from any to 10.18.48.0/24 out keep-state :default
00111 count tcp from any to me in
65533 allow ip from any to any via lo0
65534 check-state :default
65535 deny ip from any to any
#
```