нетология

Защита сети

Алексей
Федин

Алексей Федин

Ведущий инженер
по информационной безопасности

Алексей Федин

План занятия

1. Предисловие
2. Межсетевые экраны
3. СОВ
4. Защита от ARP-Spoofing
5. Защита от атак на перебор паролей
6. Защита WEB-трафика
7. Honeypot
8. Итоги
9. Домашнее задание

Межсетевые экраны

Защита сети: МЭ

Межсетевой экран (файрвол, firewall; брандмауэр, brandmauer) – программный или программно-аппаратный модуль, осуществляющий блокирование сетевого трафика по заданным правилам или алгоритмам.

Типы межсетевых экранов:

- пакетный фильтр;
- stateful firewall;
- firewall NG.

COB

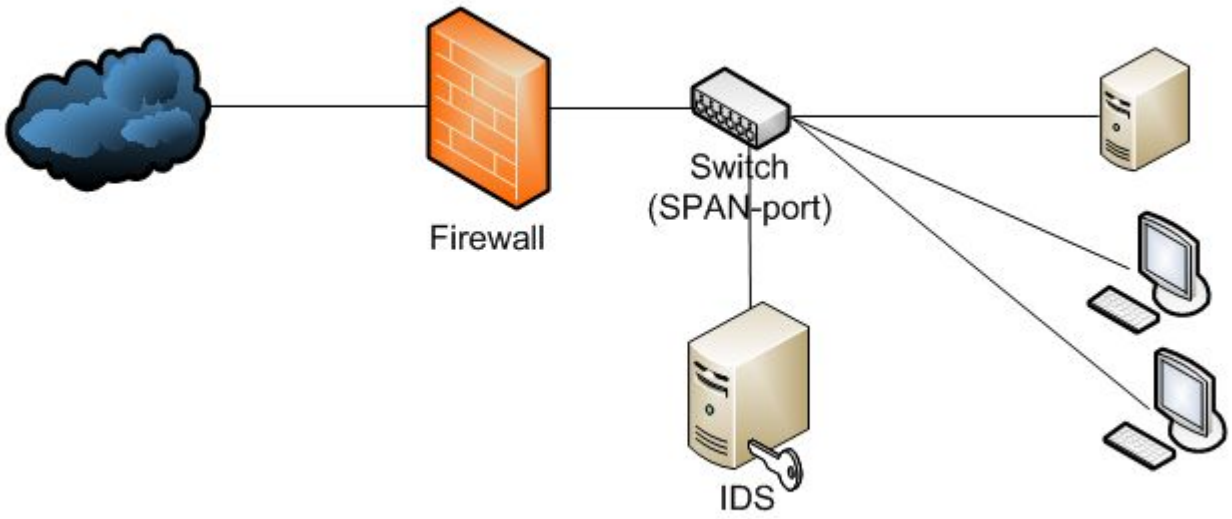
СОВ

Система Обнаружения Вторжений (Intrusion Detection System, IDS) – программное или аппаратное решение, определяющее вредоносную активности в системе или сетевом трафике.

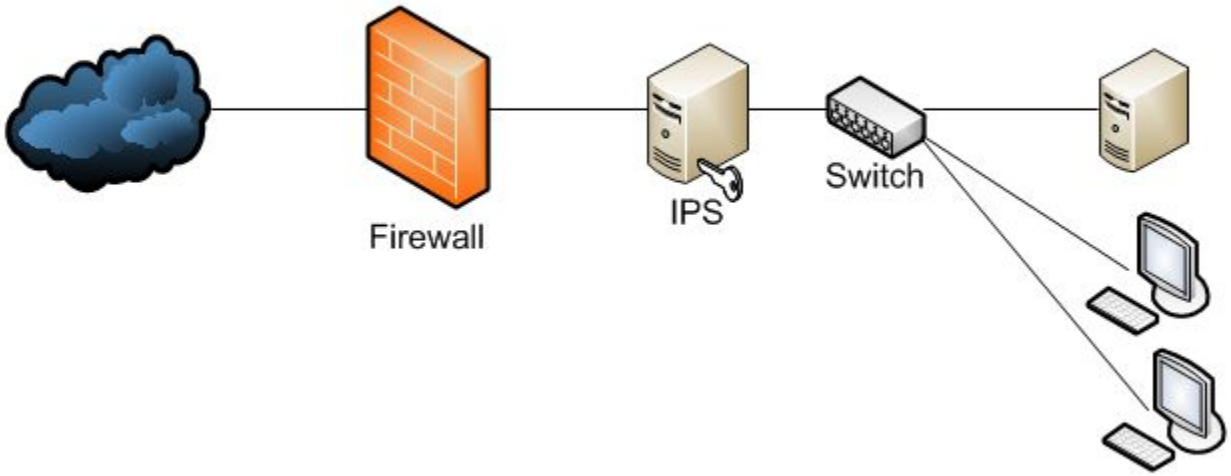
Система Предотвращения Вторжений (Intrusion Prevention Systems, IPS) – программное или аппаратное решение, предотвращающее вредоносную активности в системе или сетевом трафике.

В отечественных документах и IDS, и IPS пишут как «СОВ». Иногда, IPS обозначают как «активная СОВ».

СОВ: схема подключения IDS



СОВ: схема подключения IPS



СОВ: типы СОВ

По подключению:

- Сетевая СОВ (Network-based IDS, NIDS)
- Локальная СОВ (Host-based IDS, HIDS)

По методу обнаружения аномалий:

- Сигнатурный поиск (Signature-based detection)
- Статистическое определение аномалий (Statistical anomaly-based detection)

СОВ: недостатки СОВ

- Наличие ложно-позитивных срабатываний.
- Необходимо постоянное обновление правил.
- Существует временной лаг между появлением уязвимостей и созданием правил для их обнаружения.
- Невозможна обработка зашифрованного трафика.
- Почти невозможно определить уязвимости, вызванные неправильной настройкой (слабая аутентификации и т.д.).

Suricata: введение

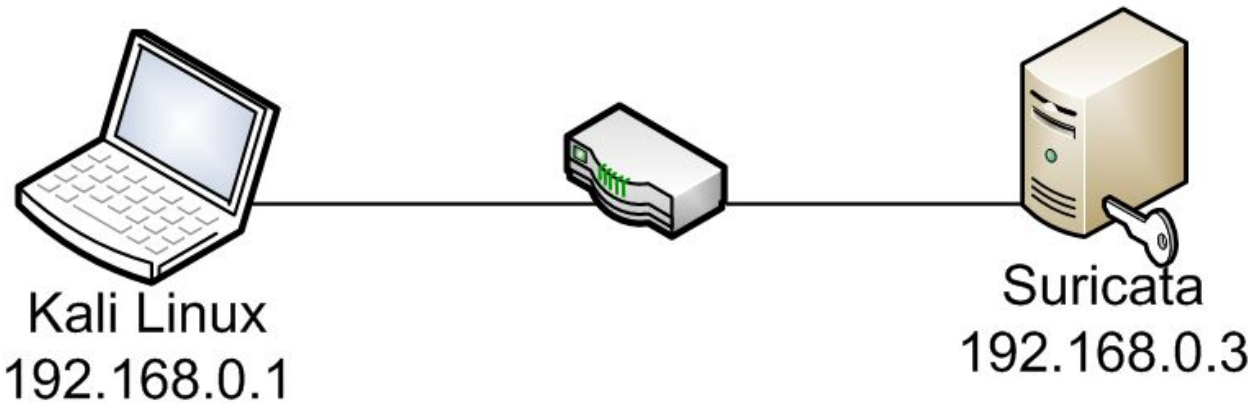
Suricata – сетевая IDS с открытым исходным кодом, разрабатываемая Open Security Foundation (OISF).

Сайт: suricata-ids.org

Исходный код: github.com/OISF/suricata

Изображение с сайта: www.suricata-ids.org

Suricata: схема сети



Suricata: установка

user@user:~$ sudo apt install software-properties-common

user@user:~$ sudo add-apt-repository ppa:oisf/suricata-stable

user@user:~$ sudo apt update

user@user:~$ sudo apt install suricata

user@user:~$ sudo suricata-update

Проверка установки:

user@user:~$ sudo systemctl status suricata

Suricata: настройка

user@user:~$ sudo nano /etc/suricata/suricata.yaml

И меняем значение параметра EXTERNAL_NET на "any"

user@user:~$ sudo systemctl restart suricata

Лог-файлы:

user@user:~$ sudo tail /var/log/suricata/suricata.log

user@user:~$ sudo tail /var/log/suricata/stats.log

Suricata: запуск

ubuntu@ubuntu:~$ sudo suricata -c /etc/suricata/suricata.yaml -i enp0s8

где параметр “i” указывает прослушиваемый интерфейс

```
24/10/2020 -- 21:54:30 - <Notice> - This is Suricata version 6.0.0 RELEASE running in SYSTEM mode
24/10/2020 -- 21:55:02 - <Notice> - all 1 packet processing threads, 4 management threads initialized, engine started.
```

откроем лог-файл, в котором будут отображаться предупреждения:

ubuntu@ubuntu:~$ sudo tail -f /var/log/suricata/fast.log

Suricata: SYN-сканирование

Перейдем на Kali и запустим SYN-сканирование:

kali@kali:~$ sudo nmap -sS 192.168.0.1

Посмотрим наш лог в Ubuntu (демонстрация).

Suricata: FIN-сканирование

Перейдем на Kali и запустим FIN-сканирование:

kali@kali:~$ sudo nmap -sF 192.168.0.1

Посмотрим наш лог в Ubuntu:

<нет изменений>

Это произошло потому, что в правилах по умолчанию нет этой атаки.

Suricata: подбор пароля ftp-сервера

Перейдем на Kali и запустим подбор пароля:

kali@kali:~$ hydra -L users.txt -P pass.txt 192.168.0.1 ftp

Посмотрим наш лог в Ubuntu (демонстрация).

Защита от ARP-Spoofing

ARP-spoofing: определение

ARP-spoofing – атака, использующая особенность протокола ARP, которая позволяет обработать ARP-ответ без предварительного ARP-запроса (протокол ARP не сохраняет свое состояние, stateless protocol).

Данная атака позволяет злоумышленнику перехватывать трафик между узлами локальной сети и является разновидностью **MITM**-атак (Man In The Middle, человек посередине).

ARP-spoofing: MITM

MITM (Man In The Middle, человек посередине, атака посредника) – атака, в результате которой атакующий скрытно принимает и передает информацию между двумя узлами. При этом, атакуемые узлы считают, что общаются друг с другом напрямую.

ARP-spoofing: статические arp-записи

Плюсы:

- записи, добавленные в ARP-таблицу вручную, имеют приоритет над динамическими;
- протокол ARP можно вообще отключить.

Минусы:

- на каждом хосте нужно создать ARP-таблицу из N-1 записей;
- при каждой замене оборудования или подключении нового, нужно перенастраивать **все** хосты.

ARP-spoofing: защита на уровне ядра ОС

Для ядер Linux/FreeBSD существует патч, позволяющий значительно **понизить вероятность успешного выполнения ARP-spoofing**.

Метод состоит в следующем:

1. При изменении MAC-адрес посылается ARP-запрос, требующий всем хостам сообщить свои MAC-адреса;
2. Если выполняется атака то по дублированию ответов она будет обнаружена;
3. Если изменение MAC-адреса произошло стандартно, то ответа, содержащего «старый» MAC-адрес, не будет.

ARP-spoofing: VLAN

Разбиение сети при помощи VLAN не предотвращает атаку ARP-spoofing, но ограничивает ее развитие. ARP-запросы не могут переходить из одного VLAN в другой.

Частным случаем (неприменимым в реальных офисных сетях) является создание VLAN на каждый порт коммутатора и добавление в него только одного хоста. В такой ситуации ARP-spoofing не имеет смысла.

ARP-spoofing: DAI

Динамическая проверка ARP (Dynamic ARP inspection, DAI) – функция защиты от ARP-атак на стороне коммутатора.

Для правильной работы **DAI** на коммутаторе необходимо указать доверенные (другой коммутатор) и ненадежные (клиенты) порты.

Коммутатор проверяет соответствие IP- и MAC-адресов на ненадежных портах по:

- базе данных DHCP;
- статическим записям.

ARP-spoofing: защита на прикладном уровне

XArp — программа, отслеживающая соответствие между IP и MAC-адресами. В случае обнаружения несоответствия, сообщает об этом пользователю.

XArp сначала анализирует ARP-таблицу, запоминает все полученные ARP-ответы и создает свою собственную таблицу IP- и MAC-адресов.

Если это соответствие нарушается или в сети появляются новые адреса, об этом будет выдано сообщение в системный журнал.

Защиты на прикладном уровне лучше всего запускать на SPAN-интерфейсе.

Защита от атак на перебор паролей

Стоимость атак на пароли (полный перебор)

Согласно исследованию https://www.thesecurityfactory.be/ (май 2020)

заплатив за аренду AWS $25 в час вы получите:

Password Length	Numerical 0-9	Upper & Lower case a-Z	Numerical Upper & Lower case 0-9 a-Z	Numerical Upper & Lower case Special characters 0-9 a-Z %$
1	instantly	instantly	instantly	instantly
2	instantly	instantly	instantly	instantly
3	instantly	instantly	instantly	instantly
4	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	20 sec
7	instantly	2 sec	6 sec	49 min
8	instantly	1 min	6 min	5 days
9	instantly	1 hr	6 hr	2 years
10	instantly	3 days	15 days	330 years
11	instantly	138 days	3 years	50k years
12	2 sec	20 years	162 years	8m years
13	16 sec	1k years	10k years	1bn years
14	3 min	53k years	622k years	176bn years
15	26 min	3m years	39m years	27tn years
16	4 hr	143m years	2bn years	4qdn years
17	2 days	7bn years	148bn years	619qdn years
18	18 days	388bn years	9tn years	94qtn years
19	183 days	20tn years	570tn years	14sxn years
20	5 years	1qdn years	35qdn years	2sptn years

Fail2Ban: ограничение скорости перебора

Самым простым решением ограничения скорости перебора паролей, является ограничение в доступе (бан) для адреса, с которого производится атака.

Для решения этой задачи существуют:

- Fail2Ban
- ipban
- DenyHosts
- и др.

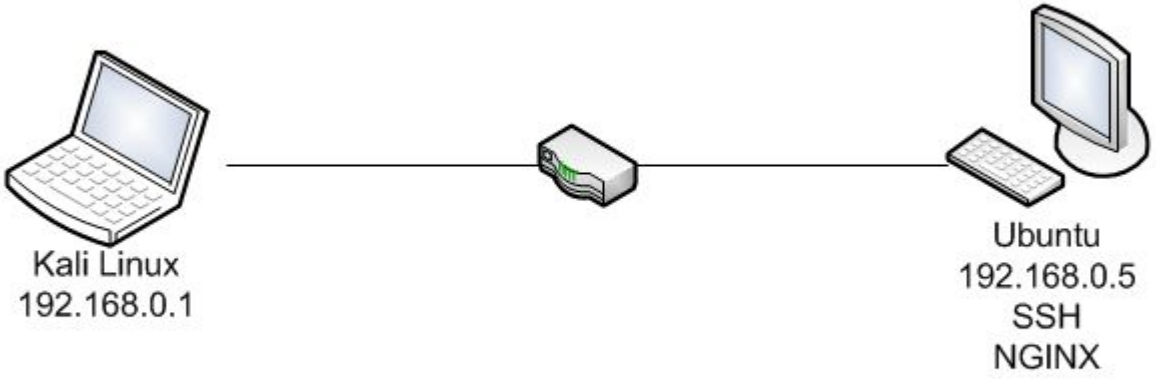
Fail2Ban: введение

Fail2Ban - одна из узкоспециализированных систем обнаружения вторжений (СОВ, Intrusion Prevention Software, IPS).

Fail2Ban сканирует лог-файлы, находит в них странное сетевое поведение (например, ошибки набора пароля) и блокирует подозрительные адреса IP-адреса на заданное время.

Изображение с сайта: www.fail2ban.org

Fail2Ban: установка и настройка



Fail2Ban: повторная атака на SSH

Выполним подбор паролей после установки **fail2ban**:

kali@kali:~$ hydra -L users.txt -P pass.txt 192.168.0.5 ssh

```
kali@kali:~$ hydra -L users.txt -P pass.txt 192.168.0.5 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military o

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-10-
[WARNING] Many SSH configurations limit the number of parallel tasks, i
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I t
[DATA] max 16 tasks per 1 server, overall 16 tasks, 64 login tries (l:8
[DATA] attacking ssh://192.168.0.5:22/
[ERROR] could not connect to ssh://192.168.0.5:22 - Connection refused
```

*Ваш вывод команды может немного отличаться - зависит от количества попыток подбора и порядка слов в словарях

Fail2Ban: просмотр лог-файлов

Проверим лог-файлы:

user@user-VirtualBox:~$ tail /var/log/auth.log

```
user@user-VirtualBox:~$ tail /var/log/auth.log
Oct 22 16:41:39 user-VirtualBox sshd[3454]: Failed password for invalid user msfadmin from 192.168.0.1 port 40712 ssh2
Oct 22 16:41:39 user-VirtualBox sshd[3465]: Failed password for user from 192.168.0.1 port 40736 ssh2
Oct 22 16:41:39 user-VirtualBox sshd[3463]: Failed password for user from 192.168.0.1 port 40732 ssh2
Oct 22 16:41:39 user-VirtualBox sshd[3461]: Failed password for user from 192.168.0.1 port 40726 ssh2
Oct 22 16:41:39 user-VirtualBox sshd[3464]: Failed password for user from 192.168.0.1 port 40734 ssh2
Oct 22 16:41:39 user-VirtualBox sshd[3482]: Failed password for invalid user postgres from 192.168.0.1 port 40740 ssh2
Oct 22 16:41:39 user-VirtualBox sshd[3462]: Failed password for user from 192.168.0.1 port 40730 ssh2
Oct 22 16:41:39 user-VirtualBox sshd[3484]: Failed password for invalid user postgres from 192.168.0.1 port 40744 ssh2
Oct 22 16:41:39 user-VirtualBox sshd[3485]: Failed password for invalid user postgres from 192.168.0.1 port 40746 ssh2
Oct 22 16:41:39 user-VirtualBox sshd[3520]: Failed password for invalid user postgres from 192.168.0.1 port 40750 ssh2
```

user@user-VirtualBox:~$ cat /var/log/fail2ban.log

```
2020-10-22 16:41:37,478 fail2ban.filter         [2531]: INFO    [sshd] Found 192.168.0.1 - 2020-10-22 16:41:37
2020-10-22 16:41:37,484 fail2ban.filter         [2531]: INFO    [sshd] Found 192.168.0.1 - 2020-10-22 16:41:37
2020-10-22 16:41:37,836 fail2ban.actions        [2531]: NOTICE  [sshd] Ban 192.168.0.1
```

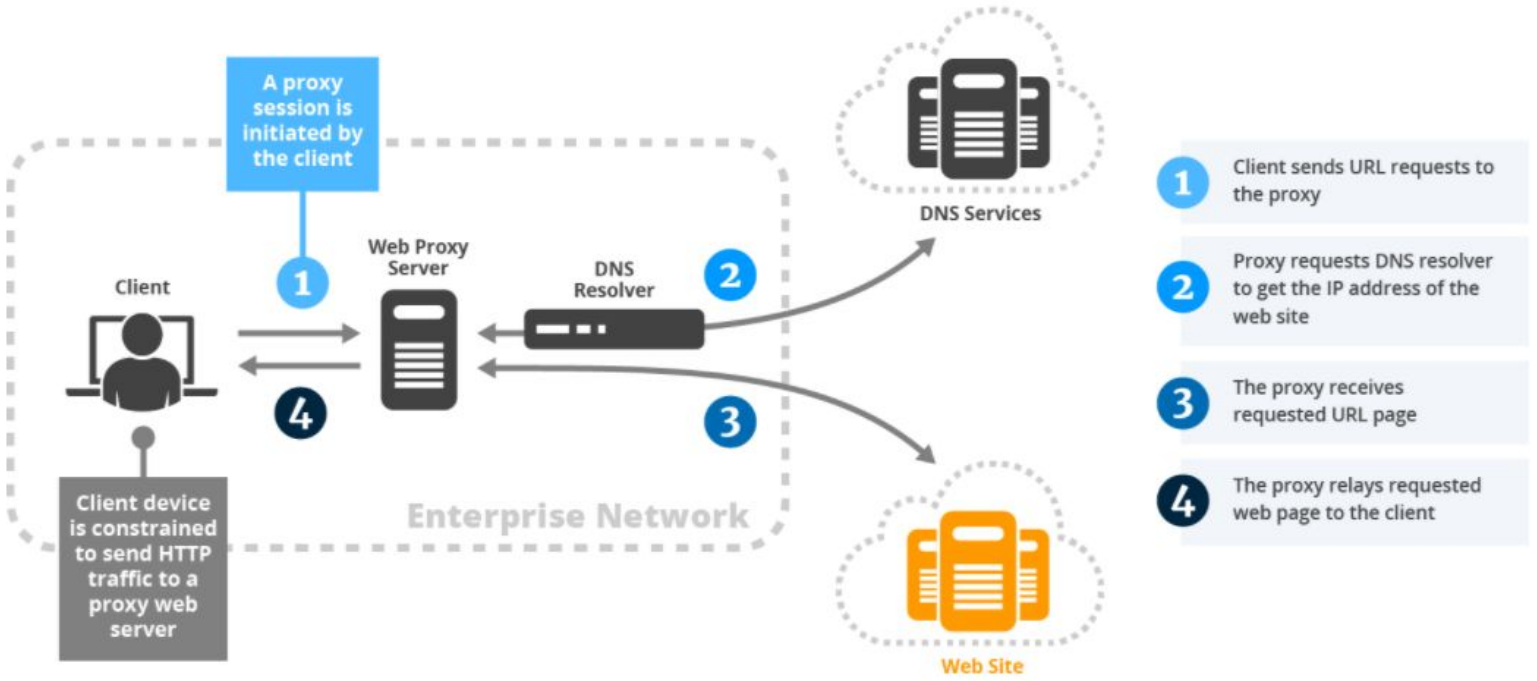
Защита WEB-трафика

WEB-трафик

- WEB-трафик сейчас составляет большую часть трафика в корпоративных сетях
- WEB-трафик бывает двух типов:
  - **исходящий** - сотрудники компании выходят в Интернет
  - **входящий** - пользователи из Интернета подключаются к публикуемым WEB порталам

Защита исходящего трафика

Для защиты исходящего трафика применяются прокси-сервера

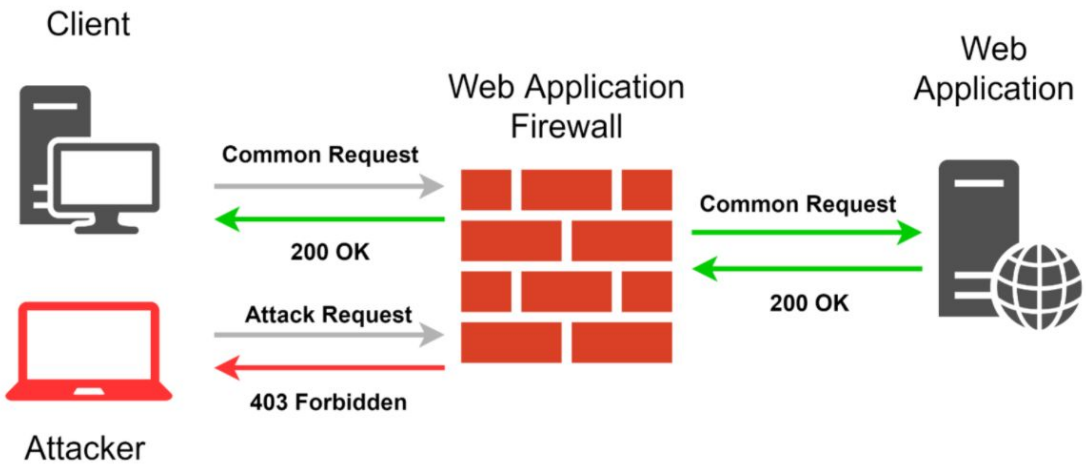


Типовые функции: работа с HTTPs, антивирус, URL фильтрация (категории сайтов), возможность фильтрации по типу файлов

Изображение с сайта www.efficientip.com/web-proxy-not-enough/

Защита входящего трафика

Для защиты входящего WEB трафика применяются Web Application Firewall (WAF):



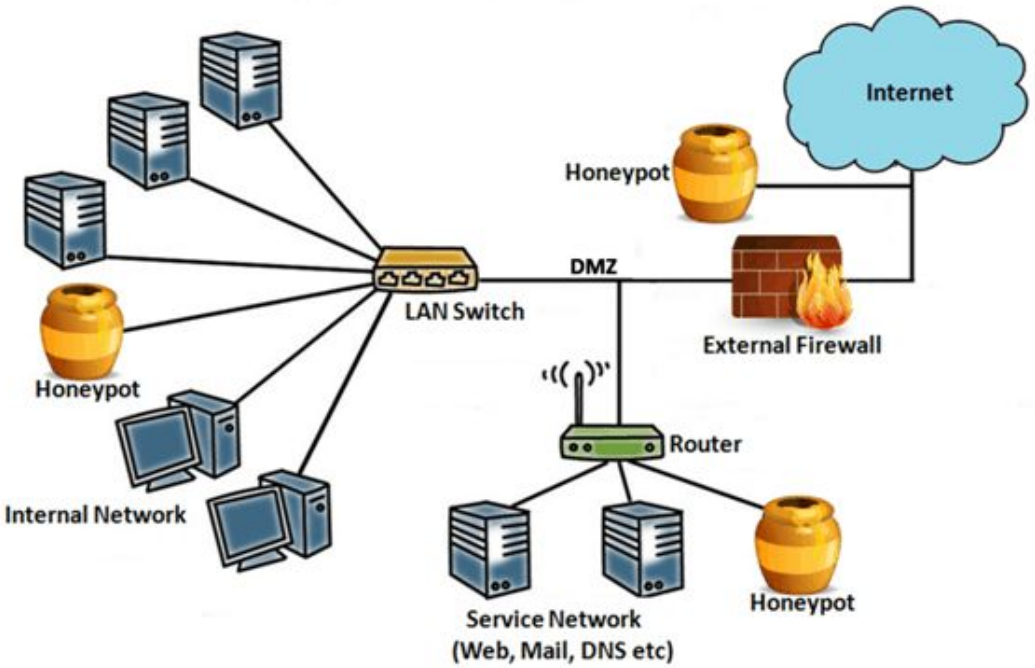
- Обеспечивает комплексную защиту от атак на веб-приложения
- Учитывает логику работы веб-приложений (сессии, cookies и т. д.)
- Защищает веб-приложения лучше межсетевых экранов и систем обнаружения вторжений
- Предоставляет защиту от веб-атак: SQL-инъекций, межсайтового скриптинга, небезопасных конфигураций и т. д.
- Определяет и блокирует уязвимости веб-приложений («виртуальный патчинг»)

Изображение с сайта https://habr.com/en/company/dsec/blog/454592/

Honeypot

Honeypot: введение

Honeypot (приманка, ловушка) - система предназначенная для обнаружения компьютерных атак через имитацию работы реальной системы.



Изображение с сайта: techpiton.com

Honeypot: типы

- Полная эмуляция системы (Pure honeypot)
- Высокоинтерактивные (High-interaction honeypot)
- Низкоинтерактивные (Low-interaction honeypot)

Honeypot: недостатки

- Если ловушка плохо настроена, её легко распознать.
- Ловушка может обнаружить только атаку на саму ловушку.
- Если ловушка распознана, на неё можно совершить “атаку”, чтобы отвлечь от реальных действий в системе.
- Если ловушка содержит уязвимости, через ней можно атаковать систему.

Итоги

Итоги

Сегодня мы познакомились с основными средствами защиты от сетевых атаками:

- СОВ
- Защита от ARP-spoofing
- Fail2Ban

Домашнее задание

Давайте посмотрим ваше домашнее задание.

- Вопросы по домашней работе задавайте **в чате** мессенджера Slack.
- Задачи можно сдавать **по частям**.
- Зачёт по домашней работе проставляется после того, как **приняты все задачи**.

нетология

Задавайте вопросы и пишите отзыв о лекции!

Алексей Федин

Алексей Федин