МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА
Колледж приборостроения и информационных технологий

Типы сетевых угроз.

Преподаватель ПЦК Информационной безопасности
Дмитренко Павел Сергеевич

Идентификация, аутентификация, авторизация

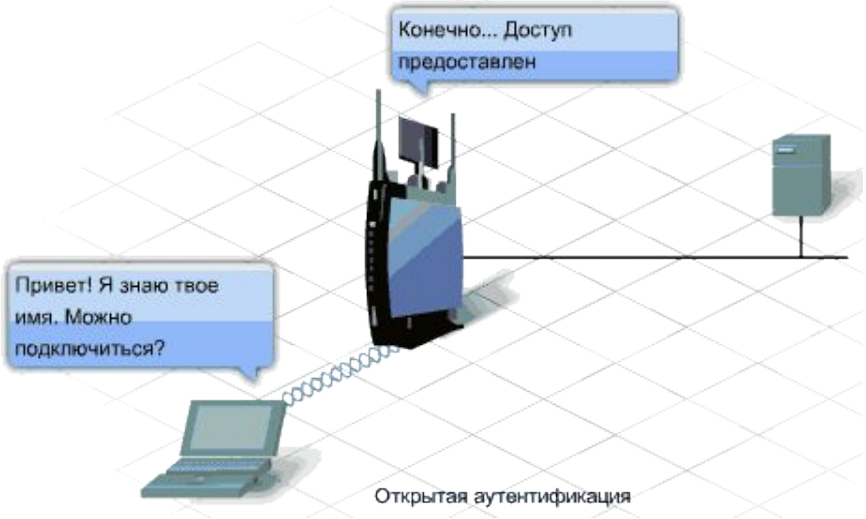
Идентификация — процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно определяющий этого субъекта в информационной системе.

Аутентификация — процедура проверки подлинности, например проверка подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных.

Авторизация — предоставление определенному лицу или группе лиц прав на выполнение определенных действий.

Аутентификация

Аутентификация – это предоставление разрешения на вход в сеть по результатам проверки подлинности набора учетных данных. Ее цель - выяснить, является ли устройство, пытающееся установить соединение, доверенным устройством.



Типы сетевых угроз

Атаки на информационные ресурсы в сети бывают двух категорий:

- «пассивные», когда злоумышленник перехватывает данные, проходящие через сеть;
- «активные», в которых злоумышленник инициирует команды, чтобы нарушить нормальную работу сети или провести сетевой анализ, чтобы найти и получить доступ к информации через сеть.

Типы сетевых угроз

К пассивным можно отнести следующие виды атак:

- сканирование портов;
- sniffing.

Активные:

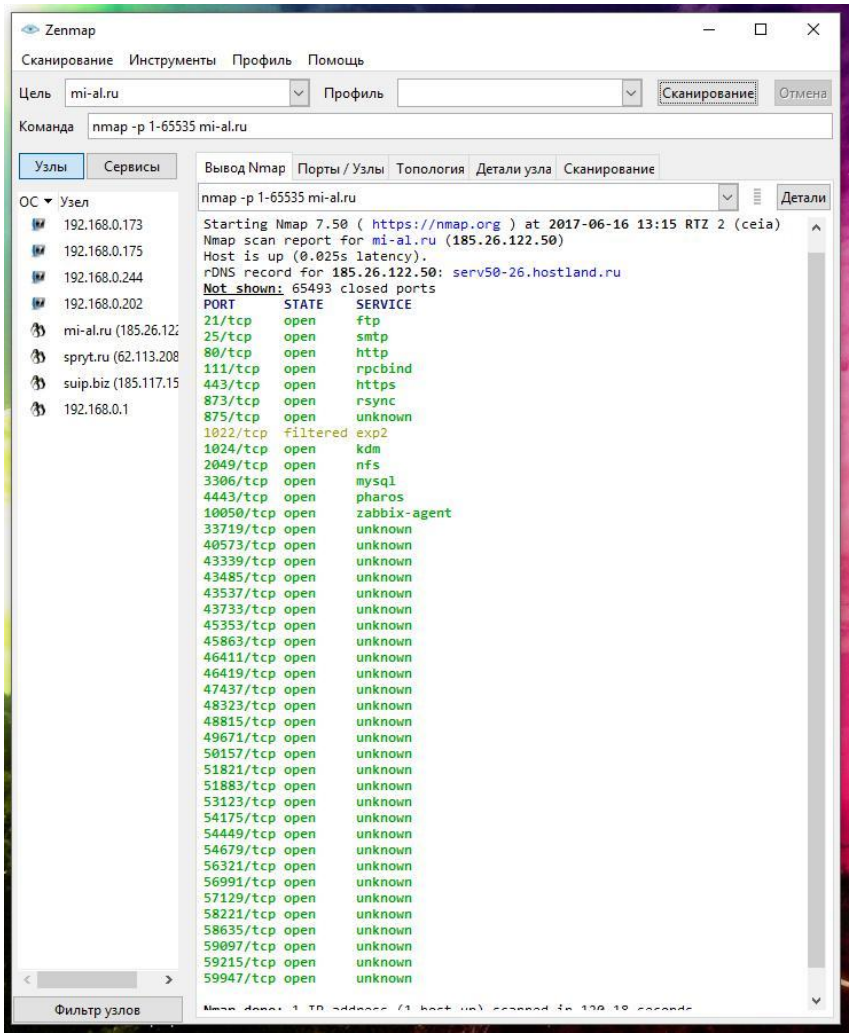
- dns spoofing;
- mitm;
- sql injection;
- bruteforce;
- ddos.

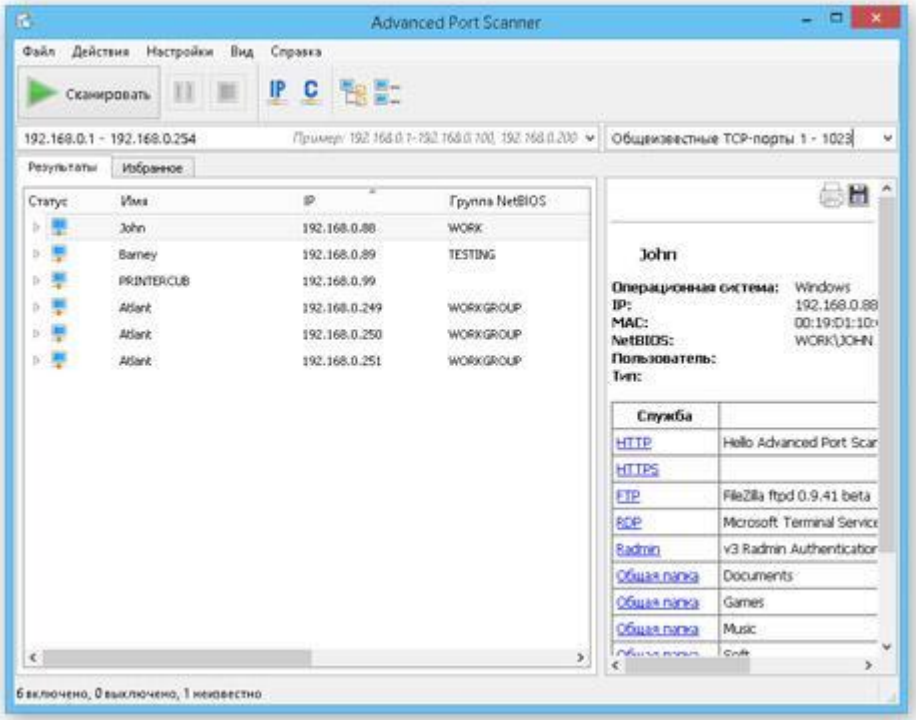
Сканер портов

Сканер портов – это приложение, разработанное для проверки сервера или хоста на наличие открытых портов. Такое приложение может использоваться администраторами для проверки политик безопасности их сетей и злоумышленниками для идентификации сетевых служб, работающих на хосте, и использования уязвимостей.

Сканирование портов – это процесс, во время которого происходит отправка запросов клиентов на диапазон адресов портов сервера на хосте с целью поиска активного порта. Большинство применений сканирования портов – это не атаки, а простые тесты для определения служб, доступных на удаленной машине.

Сканер портов





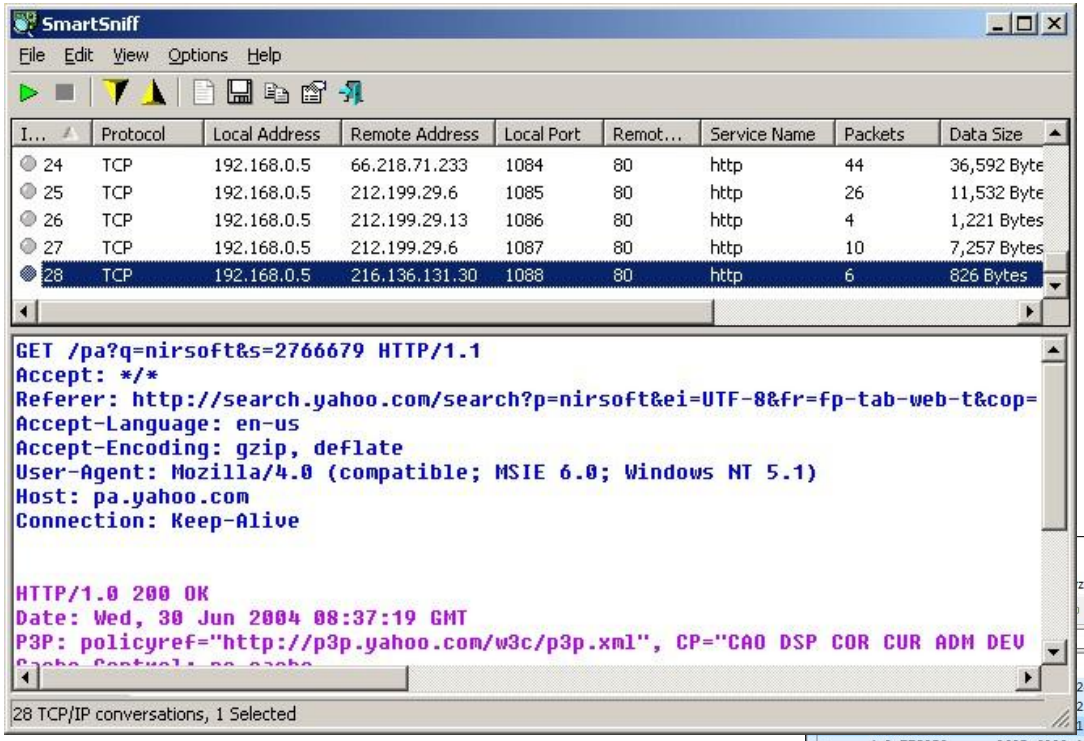
Сканер портов

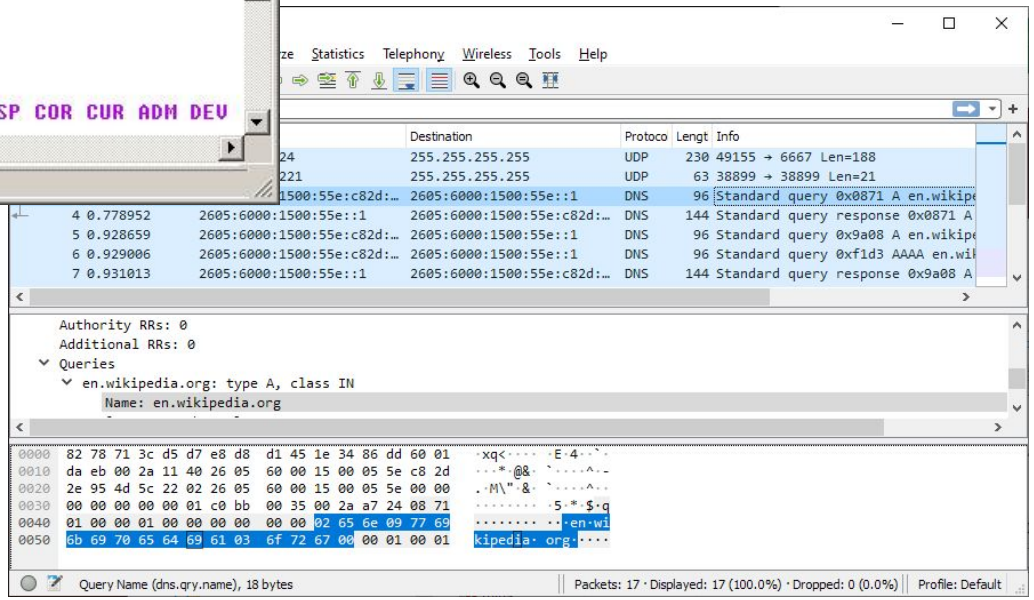
Для защиты от сканирования портов, применяются как аппаратные фаерволы так и программные, основанные на отслеживание подозрительного трафика на сетевых портах, и при возникновении данной ситуации отрабатывает правило и добавляет в черный список адрес с которого происходило сканирование.

Sniffing

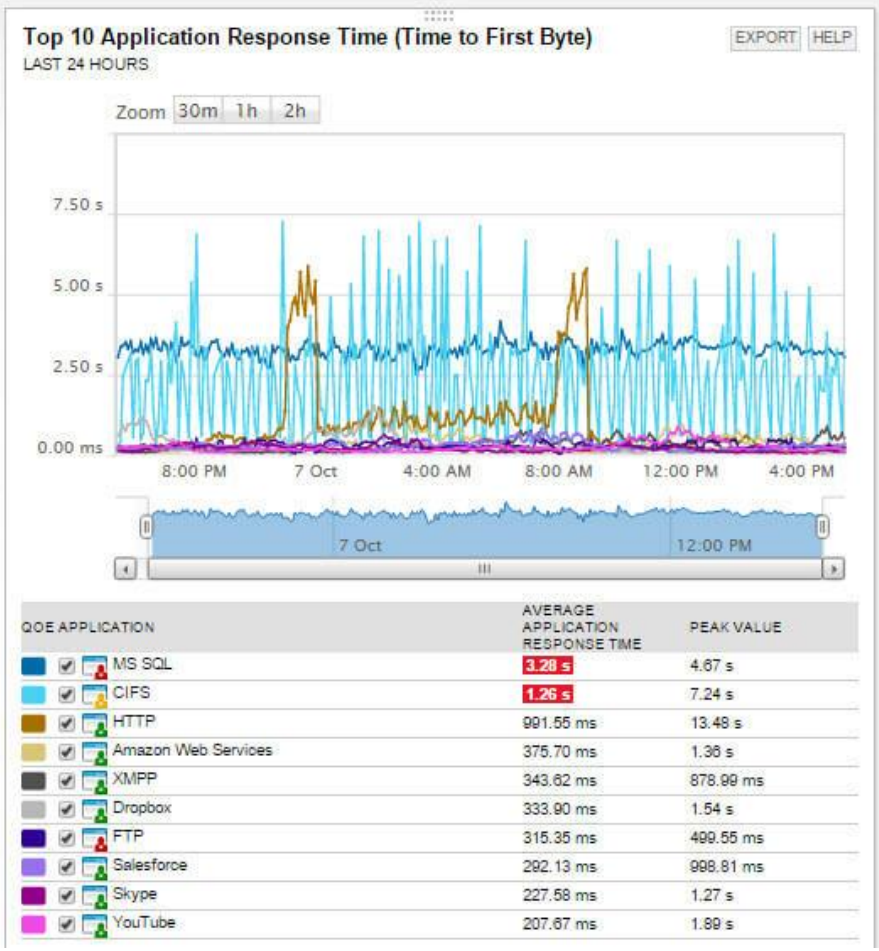
Sniffing – процесс отслеживания и перехват сетевого трафика. В контексте сетевой безопасности атака перехватчика соответствует краже или перехвату данных путем захвата сетевого трафика с помощью перехватчика (приложение, предназначенное для перехвата сетевых пакетов). Когда данные передаются по сетям, если пакеты данных не зашифрованы, данные в сетевом пакете могут быть считаны с использованием анализатора. Используя приложение анализатора, злоумышленник может проанализировать сеть и получить информацию, которая в конечном итоге может привести к сбою или повреждению сети, или прочитать сообщения, проходящее по сети.

Sniffing

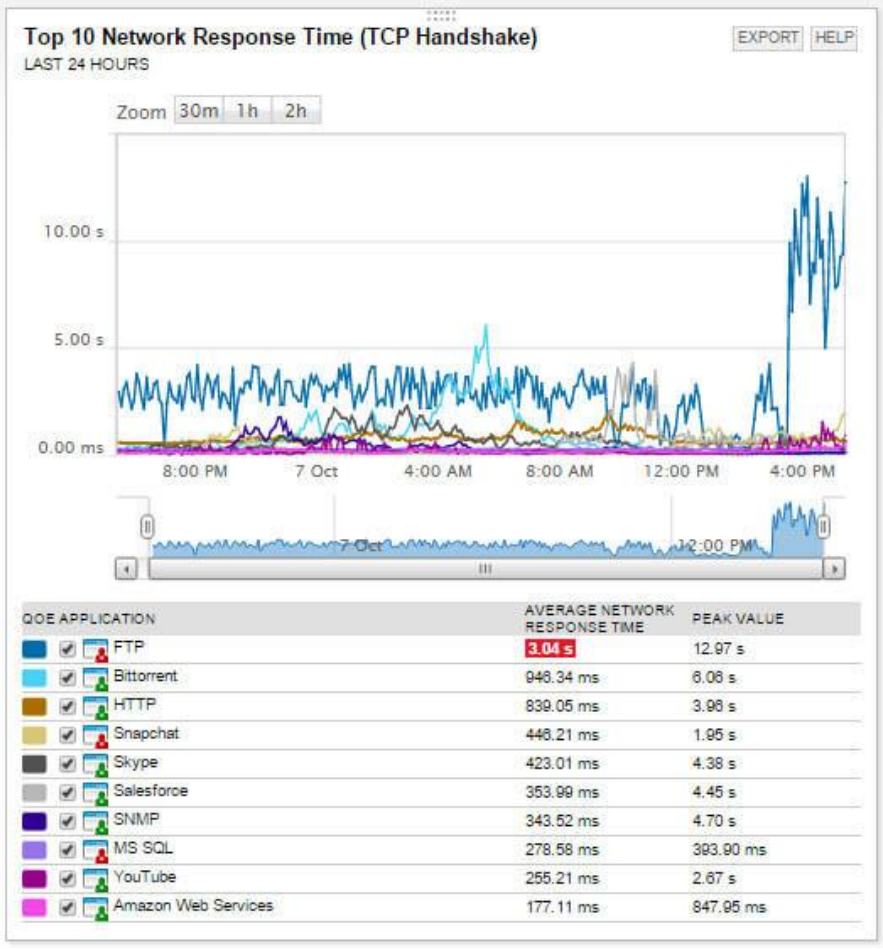

SmartSniff
File Edit View Options Help
I... Protocol Local Address Remote Address Local Port Remot... Service Name Packets Data Size
24 TCP 192.168.0.5 66.218.71.233 1084 80 http 44 36,592 Byte
25 TCP 192.168.0.5 212.199.29.6 1085 80 http 26 11,532 Byte
26 TCP 192.168.0.5 212.199.29.13 1086 80 http 4 1,221 Bytes
27 TCP 192.168.0.5 212.199.29.6 1087 80 http 10 7,257 Bytes
28 TCP 192.168.0.5 216.136.131.30 1088 80 http 6 826 Bytes
GET /pa?q=nirsoft&s=2766679 HTTP/1.1
Accept: */*
Referer: http://search.yahoo.com/search?p=nirsoft&ei=UTF-8&fr=fp-tab-web-t&cop=
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: pa.yahoo.com
Connection: Keep-Alive
HTTP/1.0 200 OK
Date: Wed, 30 Jun 2004 08:37:19 GMT
P3P: policyref="http://p3p.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV
28 TCP/IP conversations, 1 Selected


Statistics Telephony Wireless Tools Help
Destination Protoco Lengt Info
255.255.255.255 UDP 230 49155 → 6667 Len=188
255.255.255.255 UDP 63 38899 → 38899 Len=21
2605:6000:1500:55e::1 DNS 96 Standard query 0x0871 A en.wikipe
4 0.778952 2605:6000:1500:55e::1 2605:6000:1500:55e:c82d:... DNS 144 Standard query response 0x0871 A
5 0.928659 2605:6000:1500:55e:c82d:... 2605:6000:1500:55e::1 DNS 96 Standard query 0x9a08 A en.wikipe
6 0.929006 2605:6000:1500:55e:c82d:... 2605:6000:1500:55e::1 DNS 96 Standard query 0xf1d3 AAAA en.wi
7 0.931013 2605:6000:1500:55e::1 2605:6000:1500:55e:c82d:... DNS 144 Standard query response 0x9a08 A
Authority RRs: 0
Additional RRs: 0
Queries
en.wikipedia.org: type A, class IN
Name: en.wikipedia.org
0000 82 78 71 3c d5 d7 e8 d8 d1 45 1e 34 86 dd 60 01
0010 da eb 00 2a 11 40 26 05 60 00 15 00 05 5e c8 2d
0020 2e 95 4d 5c 22 02 26 05 60 00 15 00 05 5e 00 00
0030 00 00 00 00 00 01 c0 bb 00 35 00 2a a7 24 08 71
0040 01 00 00 01 00 00 00 00 00 00 02 65 6e 09 77 69
0050 6b 69 70 65 64 69 61 03 6f 72 67 00 00 01 00 01
Query Name (dns.qry.name), 18 bytes
Packets: 17 · Displayed: 17 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

Sniffing Solar Winds



QOE APPLICATION	AVERAGE APPLICATION RESPONSE TIME	PEAK VALUE
MS SQL	3.28 s	4.67 s
CIFS	1.26 s	7.24 s
HTTP	991.55 ms	13.48 s
Amazon Web Services	375.70 ms	1.36 s
XMPP	343.62 ms	878.99 ms
Dropbox	333.90 ms	1.54 s
FTP	315.35 ms	499.55 ms
Salesforce	292.13 ms	998.81 ms
Skype	227.58 ms	1.27 s
YouTube	207.67 ms	1.89 s



QOE APPLICATION	AVERAGE NETWORK RESPONSE TIME	PEAK VALUE
FTP	3.04 s	12.97 s
Bittorrent	946.34 ms	6.06 s
HTTP	839.05 ms	3.96 s
Snapchat	446.21 ms	1.95 s
Skype	423.01 ms	4.38 s
Salesforce	353.99 ms	4.45 s
SNMP	343.52 ms	4.70 s
MS SQL	278.58 ms	393.90 ms
YouTube	255.21 ms	2.67 s
Amazon Web Services	177.11 ms	847.95 ms

Sniffing Zabbix

Sniffing

Атаки с помощью прослушивания можно сравнить с прослушиванием телефонных разговоров, и по этой причине его также называют прослушиванием, применяемым к компьютерным сетям. Используя инструменты отслеживания, злоумышленники могут прослушивать конфиденциальную информацию из сети, включая трафик электронной почты, веб–трафик, трафик FTP (аутентификация Telnet, пароли Samba) и многие другие.

Sniffing

Чтобы сети не подвергались атакам со стороны перехвата, организации и отдельные пользователи должны держаться подальше от приложений, использующих небезопасные протоколы, такие как базовая проверка подлинности HTTP, протокол передачи файлов (FTP) и Telnet. Вместо этого следует отдавать предпочтение безопасным протоколам, таким как HTTPS, протокол безопасной передачи файлов (SFTP) и Secure Shell (SSH).

DNS Spoofing

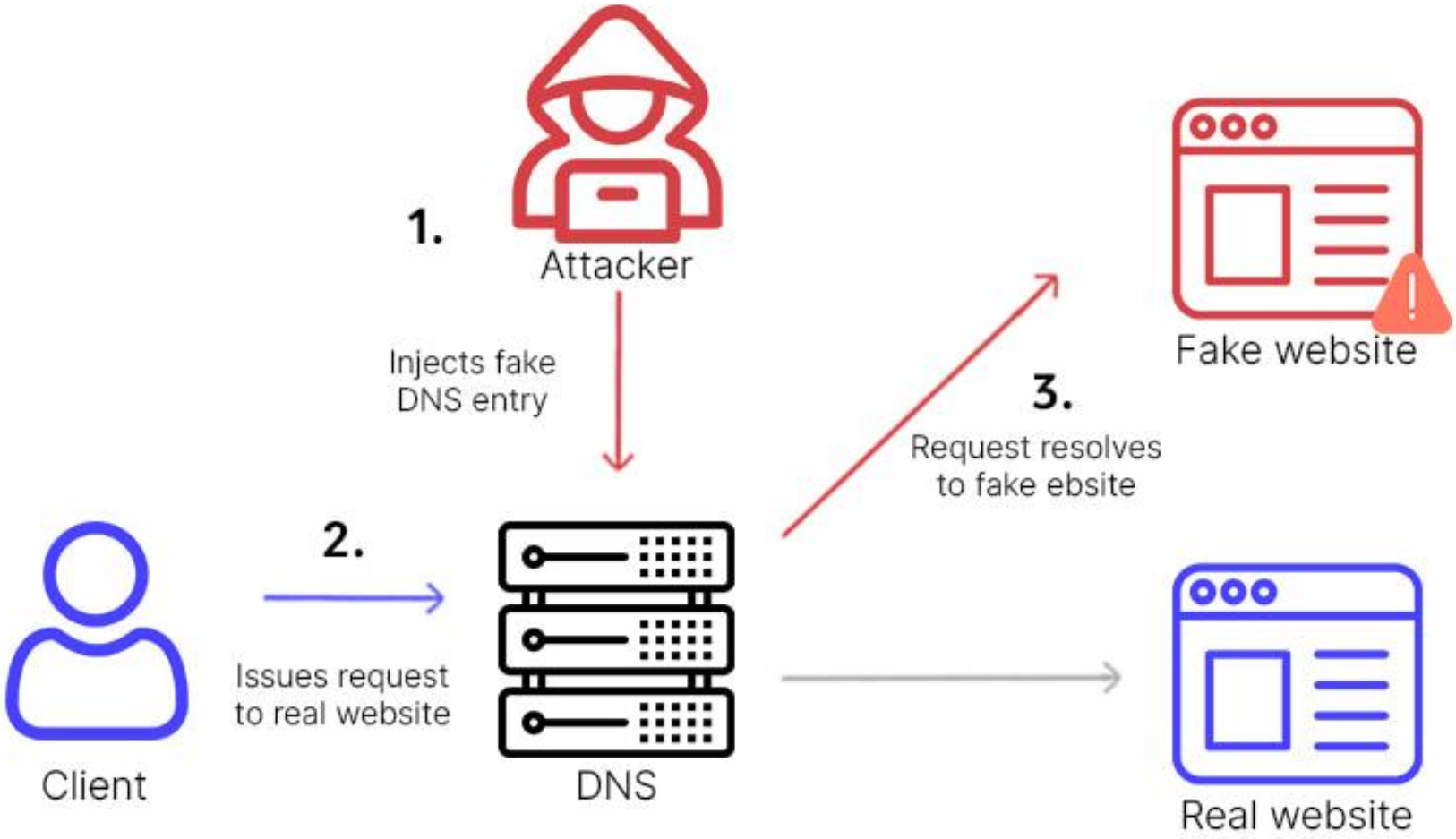
DNS Spoofing – также называемая заражением DNS – кэша, является формой взлома компьютерной безопасности, при котором поврежденные данные системы доменных имен вводятся в кэш распознавателя DNS, в результате чего сервер имен возвращает неверную запись результата, например, IP – адрес. В результате трафик перенаправляется на компьютер злоумышленника (или любой другой компьютер).

DNS Spoofing

Обычно сетевой компьютер использует DNS – сервер, предоставленный поставщиком Интернет – услуг или организацией пользователя компьютера. DNS – серверы используются в сети организации для повышения производительности отклика разрешения путем кэширования ранее полученных результатов запроса.

Атаки отравлением на один DNS – сервер могут повлиять на пользователей, обслуживаемых непосредственно скомпрометированным сервером, или тех, кто обслуживается косвенно его нижестоящими серверами, если это применимо.

DNS Spoofing



DNS Spoofing

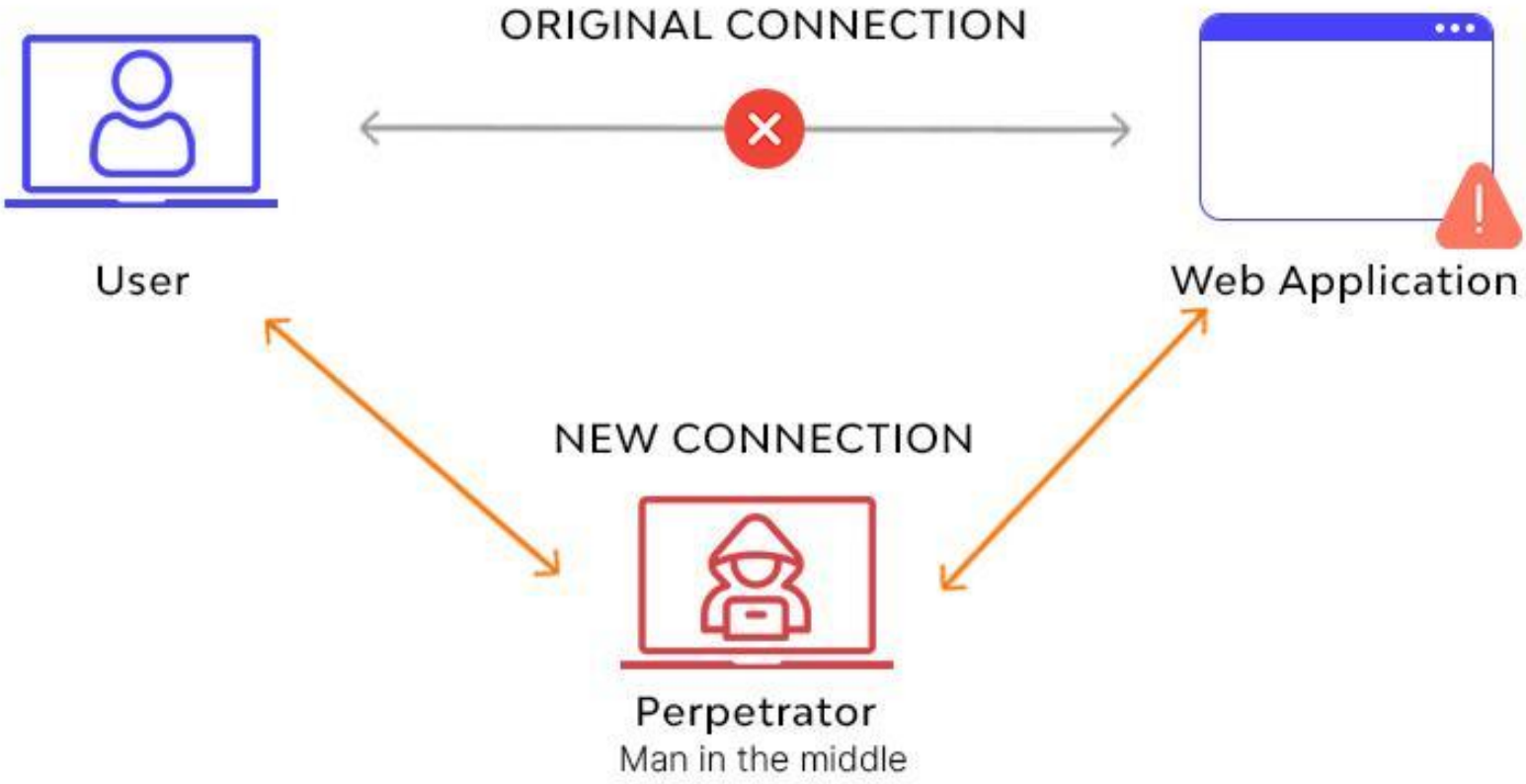
Эта атака может использоваться для перенаправления пользователей с веб–сайта на другой сайт по выбору злоумышленника. Например, злоумышленник подделывает записи DNS–адреса IP–адреса для целевого веб–сайта на данном DNS–сервере и заменяет их IP–адресом сервера, находящегося под их контролем. Затем злоумышленник создает файлы на сервере под своим контролем с именами, совпадающими с именами на целевом сервере. Эти файлы обычно содержат вредоносный контент, такой как компьютерные черви или вирусы. Пользователь, чей компьютер ссылался на отравленный DNS–сервер, обманом принимает контент, поступающий с неаутентичного сервера, и неосознанно загружает вредоносный контент

MitM

«Человек по середине» (MitM) – вид атаки, реализуемой, когда злоумышленник позиционирует себя между пользователем и приложением, чтобы либо подслушивать, либо выдавать себя за одну из сторон, создавая впечатление нормального обмена информацией.

Целью атаки является кража личной информации, такой как учетные данные, данные учетной записи и номера кредитных карт. Целями обычно являются пользователи финансовых приложений, сайтов электронной коммерции и других веб–сайтов, где требуется вход в систему.

MitM


ORIGINAL CONNECTION
User
Web Application
NEW CONNECTION
Perpetrator
Man in the middle

MitM

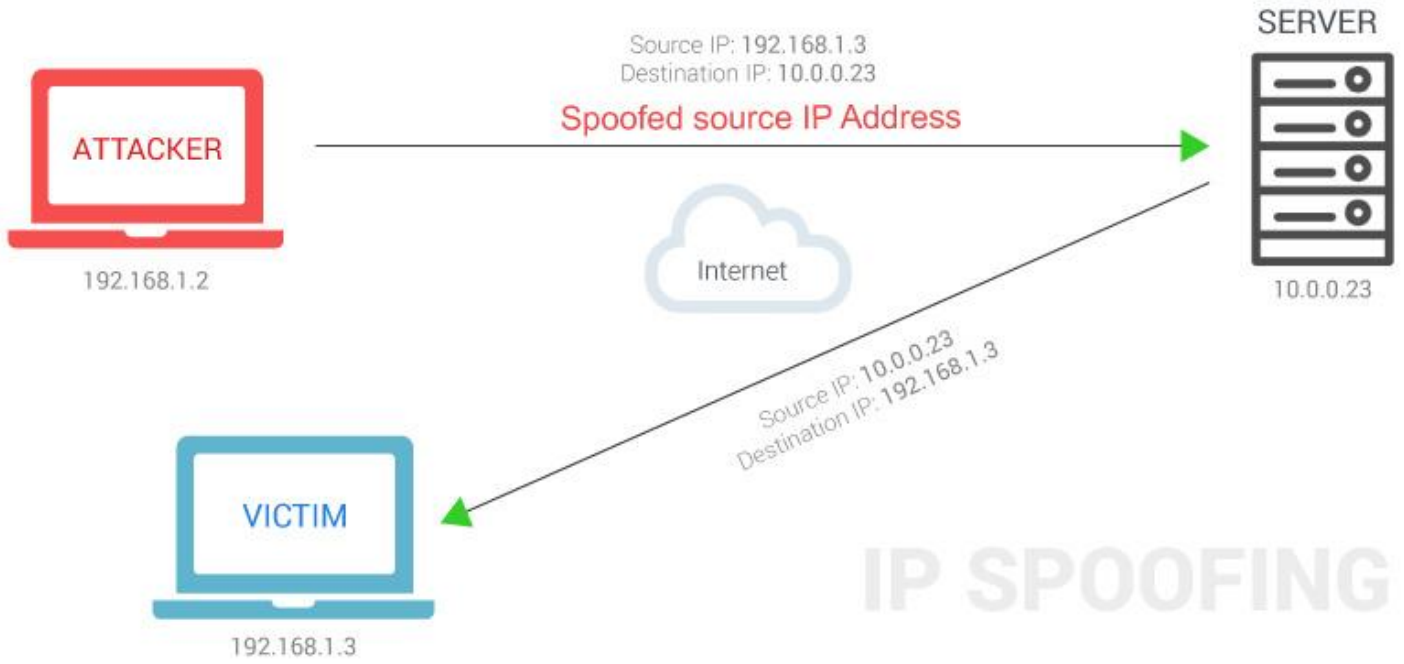
Информация, полученная во время атаки, может использоваться для многих целей, включая кражу личных данных, несанкционированные переводы средств или незаконную смену пароля.

Кроме того, он может быть использован для закрепления внутри защищенного периметра во время этапа проникновения в атаке с использованием усовершенствованной постоянной угрозы.

Атака MitM это то же самое, что почтальон, открывающий выписку из вашего банка, записывающий данные вашей учетной записи, затем повторно запечатывающий конверт и доставляющий его к вашей двери.

MitM

ip spoofing подразумевает, что злоумышленник маскирует себя под приложение, изменяя заголовки пакетов в IP-адресе. В результате пользователи, пытающиеся получить доступ к URL-адресу, связанному с приложением, отправляются на веб-сайт злоумышленника;



MitM

arp spoofing – это процесс связывания MAC – адреса злоумышленника с IP – адресом легитимного пользователя в локальной сети с использованием поддельных сообщений ARP. В результате данные, отправленные пользователем на IP – адрес хоста, вместо этого передаются злоумышленнику;

dns spoofing, также известна, как заражение DNS – кэша, включает в себя проникновение на DNS – сервер и изменение адресной записи веб – сайта. В результате пользователи, пытающиеся получить доступ к сайту, отправляются с помощью измененной записи DNS на сайт злоумышленника.

SQL injection

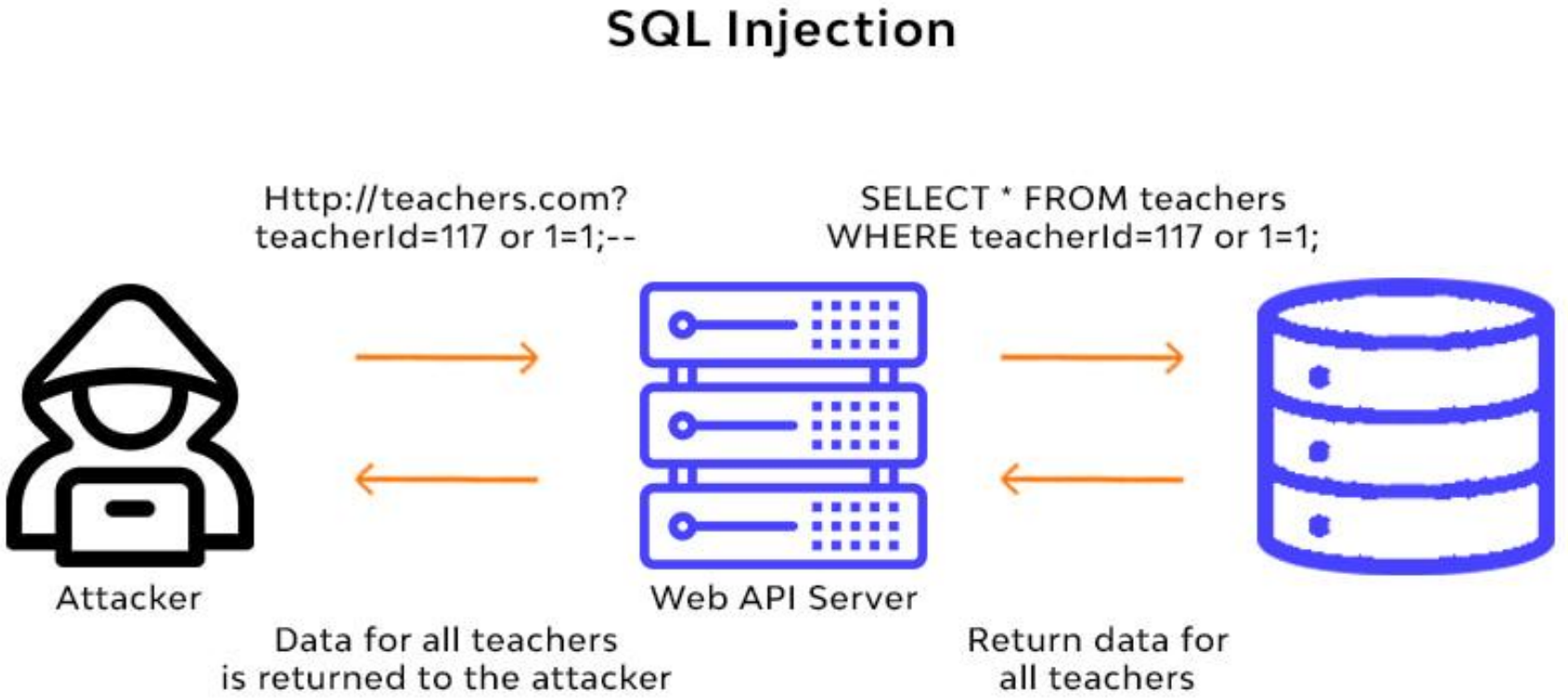
Инъекция SQL (SQLI) – тип атаки, при котором злоумышленник использует уязвимость программного обеспечения в веб–приложениях с целью кражи, удаления или изменения данных, а также получения административного контроля над системами, на которых работают уязвимые приложения.

К часто используемым веб-приложениям относятся:

- сайты социальных сетей;
- интернет–магазины;
- ресурсы учебных заведений;
- сайты малых и средних предприятий.

Особенно уязвимы, так как администраторы часто не знакомы с методами, используемыми злоумышленниками при атаке SQLI, и также не знают, как защититься от такой атаки.

SQL injection



SQL injection

Для предотвращение данного типа атаки, требуется выполнить следующие условия:

- обновить программное обеспечение для управления базами данных;
- соблюдение принципа наименьших привилегий, означает, что каждая учетная запись имеет достаточный доступ для выполнения своей работы и ничего более. Например, веб – учетная запись, которой нужен только доступ для чтения к определенной базе данных, не должна иметь возможности записывать, редактировать или изменять данные каким – либо образом;
- использовать подготовленные заявления или хранимые процедуры. В отличие от динамического SQL, подготовленные операторы ограничивают переменные для входящих команд SQL.

Bruteforce

Атака полным перебором или bruteforce – это метод проб и ошибок, используемый прикладными программами для декодирования зашифрованных данных, таких как пароли или ключи стандарта шифрования данных посредством исчерпывающих усилий (с использованием грубой силы), а не с использованием интеллектуальных стратегий. Bruteforce последовательно обрабатывает все возможные комбинации символов.

Хакер может использовать атаку методом «грубой силы» для получения доступа к ресурсу и учетной записи, затем украсть данные, закрыть сайт или выполнить атаку другого типа. Брутфорс считается безошибочным, хотя и трудоемким подходом. Взломщики иногда используются в организации для проверки сетевой безопасности, хотя их более распространенное применение – для злонамеренных атак.

Bruteforce

```
hashcat (v6.0.0) starting...

CUDA API (CUDA 10.2)
====================
* Device #1: GeForce GTX 1080, 7982/8112 MB, 20MCU

Minimum password length supported by kernel: 4
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers:
* Single-Hash
* Single-Salt
* Brute-Force
* Slow-Hash-SIMD-LOOP

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1725 MB

$bitlocker$1$16$303832343439373237313533303333732$10...09e60e:20200615

Session..........: hashcat (Brain Session/Attack:0xdd79fcf8/0xc2bc45aa)
Status...........: Cracked
Hash.Name........: BitLocker
Hash.Target......: $bitlocker$1$16$303832343439373237313533303333732$10...09e60e
Time.Started.....: Mon Jun 15 16:20:12 2020 (44 secs)
Time.Estimated...: Mon Jun 15 16:20:56 2020 (0 secs)
Guess.Mask.......: ?d?d20?d?d?d?d [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     1426 H/s (57.15ms) @ Accel:1 Loops:4096 Thr:1024 Vec:1
Recovered........: 1/1 (100.00%) Digests
Progress.........: 184320/1000000 (18.43%)
Rejected.........: 0/184320 (0.00%)
Brain.Link.All...: RX: 16 B, TX: 51 B
Brain.Link.#1....: RX: 16 B (0.00 Mbps), TX: 51 B (0.00 Mbps), idle
Restore.Point....: 0/100000 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:2-3 Iteration:1036288-1040384
Candidates.#1....: 22206007 -> 27203992
Hardware.Mon.#1..: Temp: 77c Fan: 49% Util:100% Core:1759MHz Mem:4513MHz Bus:1

Started: Mon Jun 15 16:19:45 2020
Stopped: Mon Jun 15 16:20:57 2020
```

```
hejab-zaeri ~ Brute_Force-master python3 B
Facebook Account: butuju@maxmail.in
<<<<<<++++Start  Attacking Email+++++>>>>>
Password [==] 12345
[!] False Login Password

Password [==] 123456
[!] False Login Password

Password [==] 12345678
[!] False Login Password

Password [==] trfyhtruuuyt
[!] False Login Password

Password [==] tyuytut
[!] False Login Password

Password [==] Hegap12345
[True][+] Password Found [Hegap12345][+]
```

Bruteforce

Общие способы предотвращения взлома методом перебора включают в себя:

- добавление к сложности пароля: любой процесс угадывания пароля займет значительно больше времени. Например, для некоторых веб – сайтов требуются пароли из 8 – 16 символов, по крайней мере, с одной буквой и цифрой со специальными символами (например, «.»), а также не позволяющие пользователю указывать свое имя, имя пользователя или идентификатор в своем имени/пароле;
- попытки входа в систему: добавление попыток входа в систему блокирует пользователя на указанное время, превышающее указанное количество попыток ввода паролей/имен пользователей;

Bruteforce

- captcha’s, в этих полях будет отображаться поле с искаженным текстом и спрашивать пользователя, что это за текст в поле. Это препятствует тому, чтобы боты выполняли автоматизированные сценарии, которые появляются в атаках методом грубой силы, и при этом человеку легко пройти мимо;
- двухфакторная аутентификация (тип многофакторной аутентификации), добавляет уровень безопасности к основной форме аутентификации. Для двухфакторной безопасности требуются две формы аутентификации (например, для входа на новое устройство Apple пользователям необходимо ввести свой Apple ID вместе с шестизначным кодом, который отображается на другом устройстве, ранее помеченном как доверенный).

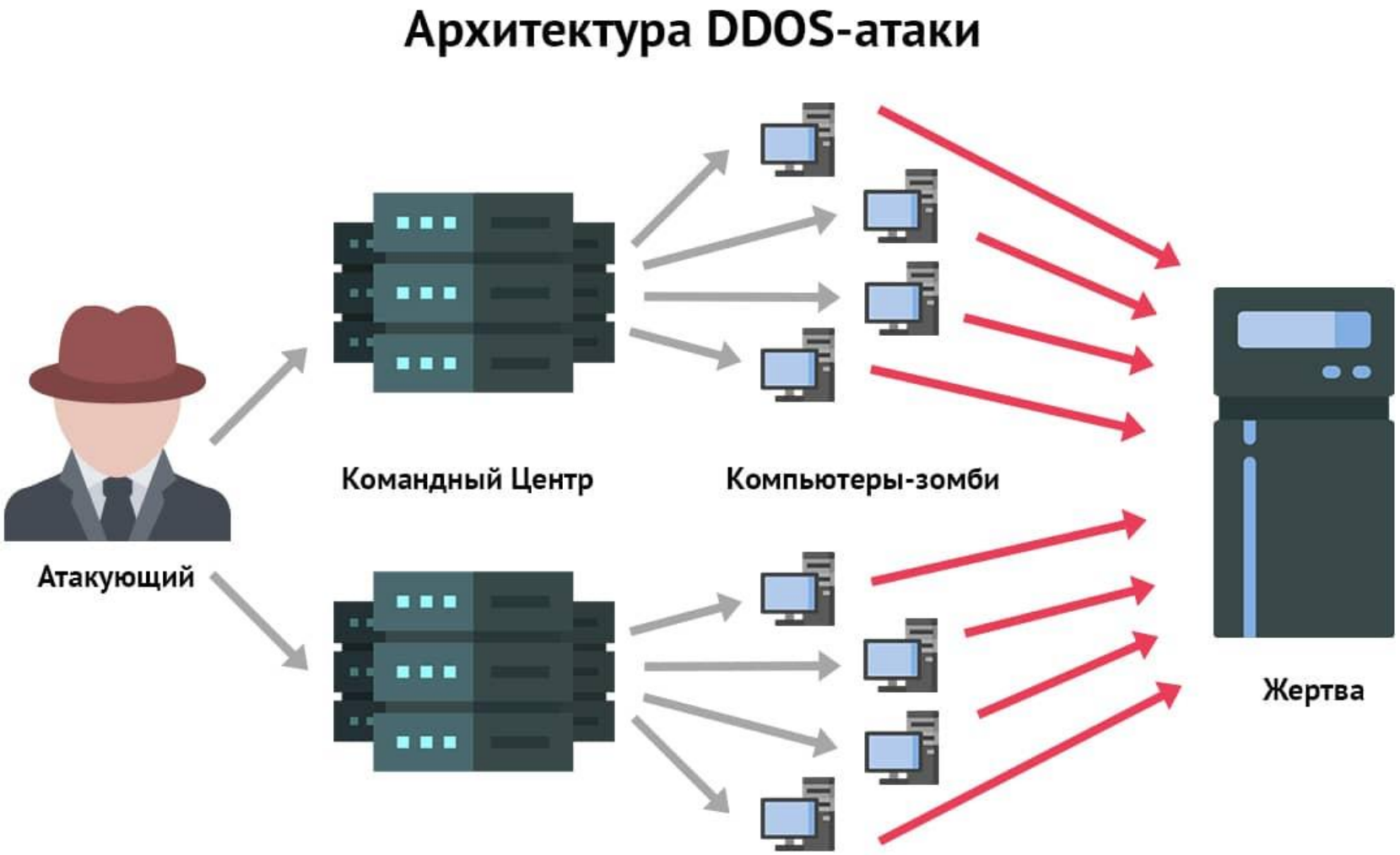
Хороший способ обезопасить себя от атак методом перебора – использовать все или комбинацию вышеуказанных стратегий.

DoS, DDoS

Распределенная атака типа «отказ в обслуживании» (DDoS) – это злонамеренная попытка нарушить нормальный трафик целевого сервера, службы или сети, перегружая цель или окружающую инфраструктуру потоком интернет-трафика. DDoS–атаки достигают эффективности, используя несколько скомпрометированных компьютерных систем в качестве источников трафика атаки. Эксплуатируемые машины могут включать компьютеры и другие сетевые ресурсы.

DDoS–атака требует от злоумышленника получить контроль над сетью компьютеров для проведения атаки. Компьютеры и другие машины заражены вредоносным ПО, превращая каждый из них в бота (или зомби). Затем злоумышленник получает дистанционное управление группой ботов, которая называется ботнетом. После того, как ботнет создан, злоумышленник может управлять машинами, отправляя обновленные инструкции каждому боту с помощью метода дистанционного управления.

DoS, DDoS


Архитектура DDOS-атаки
Атакующий
Командный Центр
Компьютеры-зомби
Жертва

DoS, DDoS

Когда ботнет использует целевой IP-адрес жертвы, каждый бот отвечает, отправляя запросы к цели, что может привести к переполнению сетевого буфера целевого сервера или сети, что приведет к отказу в обслуживании нормальному трафику. Поскольку каждый бот является законным интернет–устройством, отделить трафик атаки от обычного трафика может быть сложно.

Различные векторы DDoS–атак нацелены на различные компоненты сетевого подключения. Чтобы понять, как работают различные DDoS–атаки, необходимо знать, как осуществляется сетевое соединение. Сетевое соединение в Интернете состоит из множества различных уровней. Каждый шаг в модели имеет свое назначение.

DoS, DDoS

В то время как почти все DDoS–атаки включают в себя перегрузку целевого устройства или сети трафиком, атаки можно разделить на три категории. Злоумышленник может использовать один или несколько различных векторов атаки или циклические векторы атаки.

SYN Flood – эта атака использует рукопожатие TCP, отправляя целевому объекту большое количество пакетов SYN «запрос на соединение» TCP с поддельными IP–адресами источника. Целевая машина отвечает на каждый запрос на подключение, а затем ждет последнего шага рукопожатия, который никогда не происходит, истощая ресурсы цели в процессе атаки.

DNS Amplification – злоумышленник отправляет запрос на открытый DNS – сервер с поддельным IP–адресом (реальный IP–адрес цели), целевой IP–адрес затем получает ответ от сервера. Злоумышленник структурирует запрос так, чтобы DNS–сервер отвечал на цель атаки большим количеством данных. В результате цель получает усиление первоначального запроса атакующего.

DoS, DDoS

Ключевой задачей в смягчении атаки DDoS является различие между атакой и обычным трафиком. В современном Интернете, трафик DDoS существует во многих формах.

Трафик может варьироваться по дизайну, от несанкционированных атак из одного источника до сложных и адаптивных многовекторных атак. Мультивекторная атака DDoS использует несколько путей атаки, чтобы поразить цель различными способами, потенциально отвлекая усилия по смягчению на любой одной траектории. Атака, нацеленная на несколько уровней стека протоколов одновременно, такая как усиление DNS (нацеливание на уровни 3/4) в сочетании с потоком HTTP (нацеленность на уровень 7), является примером многовекторного DDoS.

DoS, DDoS

Смягчение многовекторной атаки DDoS требует различных стратегий для противодействия различным траекториям. Чем сложнее атака, тем больше вероятность того, что трафик будет трудно отделить от обычного трафика - цель злоумышленника состоит в том, чтобы как можно больше объединиться, сделав смягчение как можно более неэффективным. Попытки смягчения, которые включают в себя отбрасывание или ограничение трафика без разбора, могут отбрасывать хороший трафик с плохим, а атака также может изменяться и адаптироваться для обхода контрмер. Чтобы преодолеть сложную попытку срыва, многоуровневое решение даст наибольшую выгоду.

DoS, DDoS

Black Hole Routing.

Одним из решений, доступных практически всем сетевым администраторам, является создание черного маршрута и направление трафика по этому маршруту. В своей простейшей форме, когда фильтрация черной дыры реализуется без особых критериев ограничения, как законный, так и вредоносный сетевой трафик направляется на нулевой маршрут или черную дыру и удаляется из сети. Если свойство Интернета подвергается DDoS – атаке, поставщик услуг Интернета может отправить весь трафик сайта в черную дыру в качестве защиты.