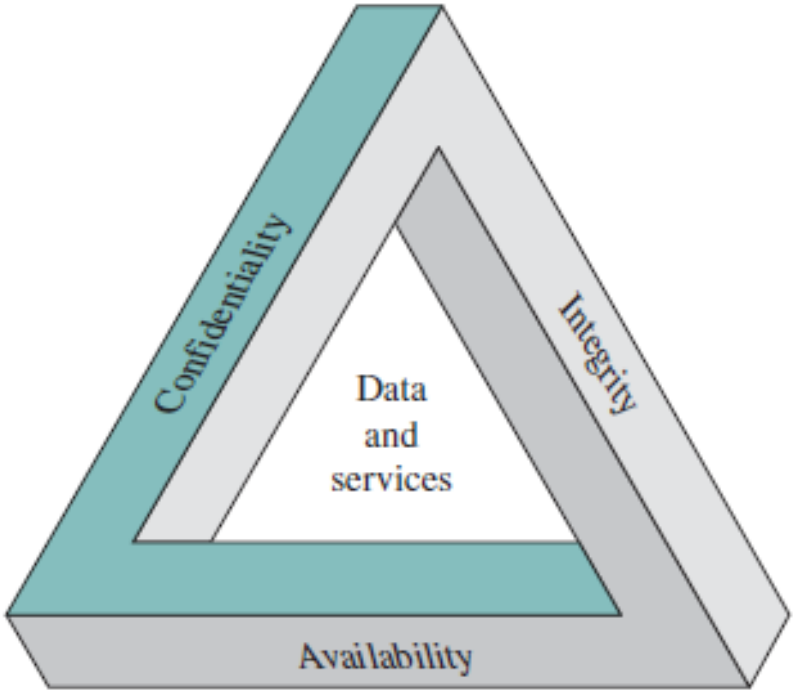
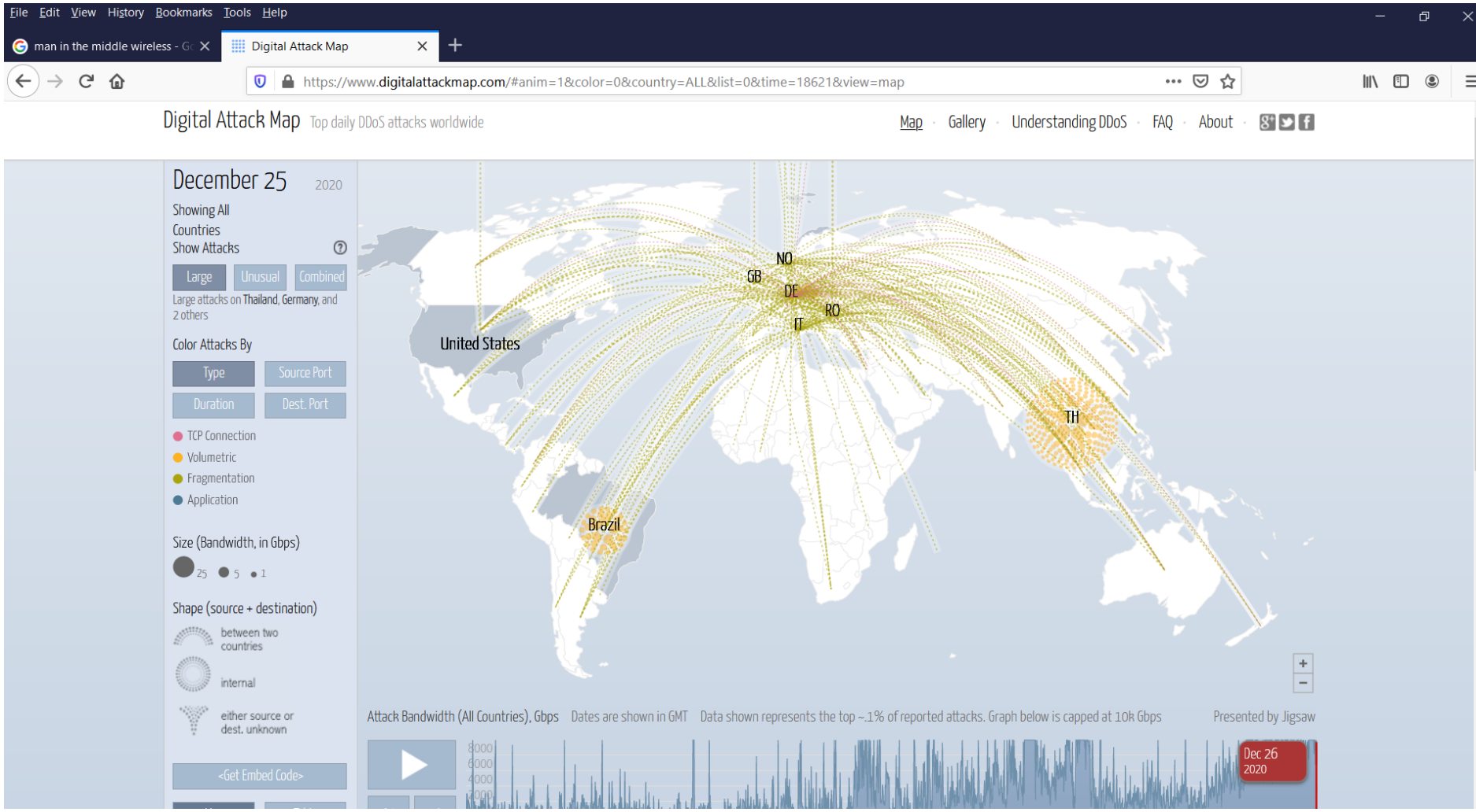
Заплахи за сигурността

Компютърна сигурност

Цели:

- Конфиденциалност
- Интегритет
- Наличност




File Edit View History Bookmarks Tools Help
man in the middle wireless - G
Digital Attack Map
https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18621&view=map
Digital Attack Map
Top daily DDoS attacks worldwide
Map · Gallery · Understanding DDoS · FAQ · About ·
December 25
2020
Showing All Countries
Show Attacks
Large
Unusual
Combined
Large attacks on Thailand, Germany, and 2 others
Color Attacks By
Type
Source Port
Duration
Dest. Port
TCP Connection
Volumetric
Fragmentation
Application
Size (Bandwidth, in Gbps)
25
5
1
Shape (source + destination)
between two countries
internal
either source or dest. unknown
<Get Embed Code>
NO
GB
DE
RO
IT
United States
TH
Brazil
Attack Bandwidth (All Countries), Gbps
Dates are shown in GMT
Data shown represents the top ~.1% of reported attacks. Graph below is capped at 10k Gbps
Presented by Jigsaw
8000
6000
4000
Dec 26
2020

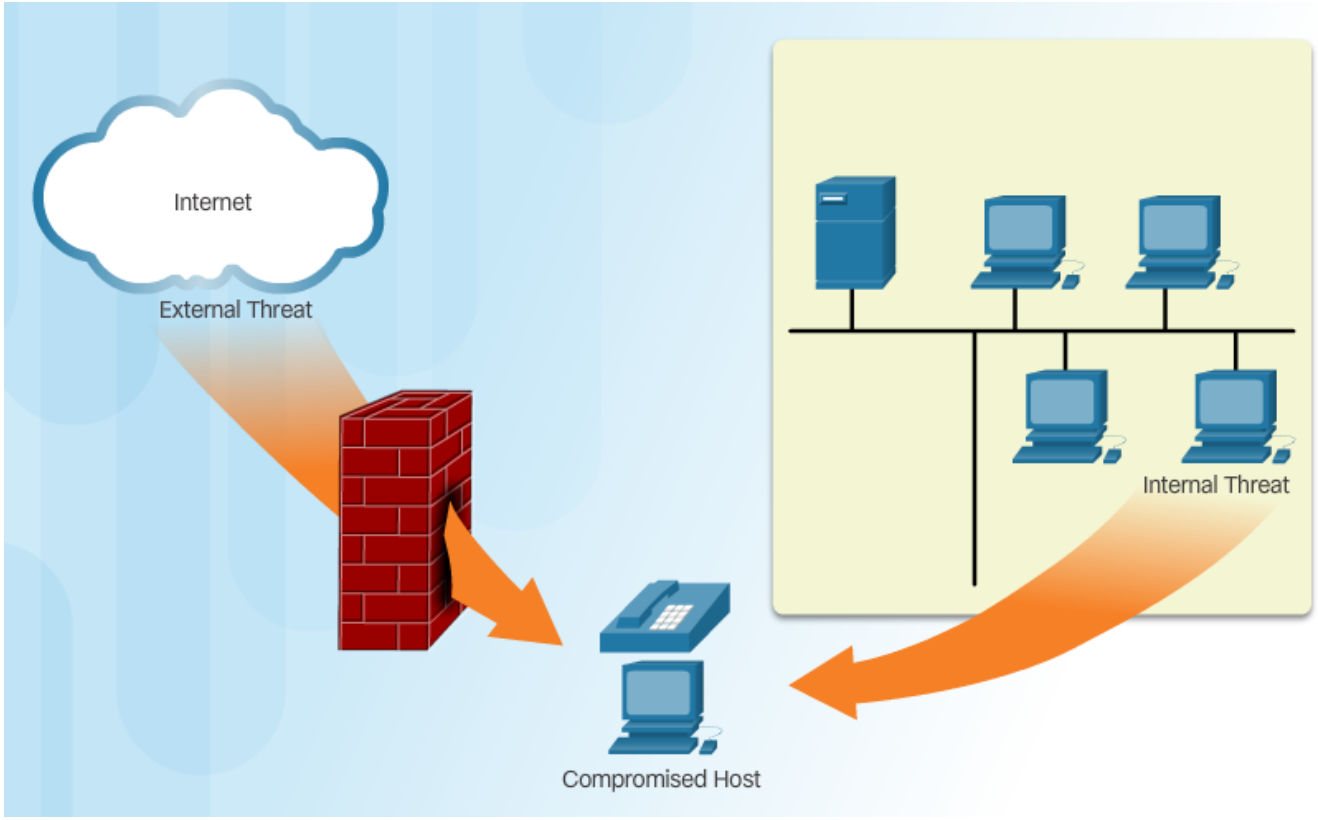
Класове физически заплахи

- Хардуерни
  - физически да се развалят сървъри, рутери, комутатори, окабеляване, работни станции
- От обкръжението
  - Твърде високи или твърде ниски температури или твърде сухо или твърде влажно.
- Електрически
  - Пикове в напрежението, поднапрежение, шум в сигнала, загуба на захранване
- При експолатация
  - лошо поведение на компонентите – електростатични разряди, липса на резервни части, лошо окабеляване, лошо означаване на етикетите на кабелите

Видове заплахи

По произход са:

- Вътрешни
- Външни



Видове заплахи

По начин на организиране са:

- Структурирани – предварително прецизно планирани
- Неструктурирани – не са планирани

Видове заплахи

По начин на провеждане на атаката са:

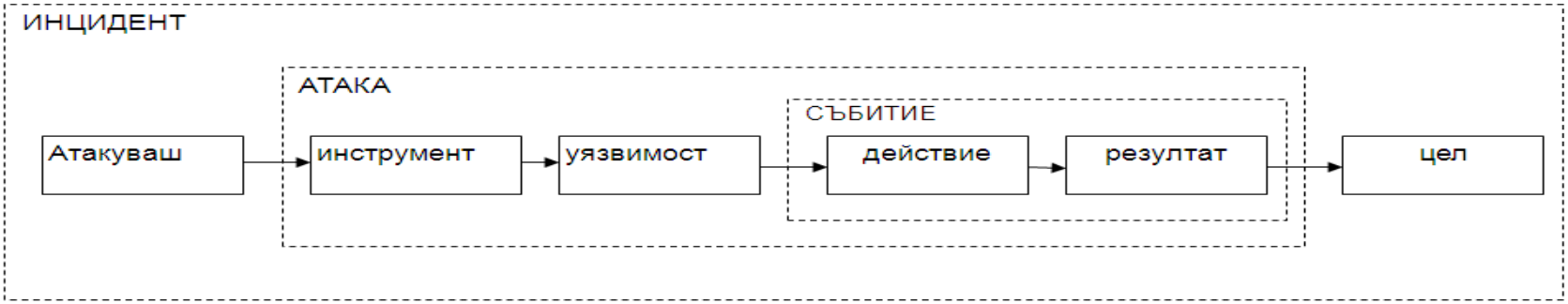
- Пасивни – снифер на пароли, анализ на трафика...
- Активни – опит за логване, потискане на услугата, маскарадинг, модификация на съобщения

Еволюция на заплахите

С годините атаките към мрежовата сигурност се развиват:

- Към 1985 атакуващият трябва да е много добре запознат с компютъра, програмирането, да има знания по мрежи, да познава детайлите на средствата, с които ще атакува.
- Средствата, с които се атакува се развиват и вече не изискват високи знания в компютърната област.
- Хората, които преди не са правили компютърни престъпления поради незнание в ИТ областта, вече могат да ги правят.

Процес на атаката



- Пасивно разузнаване и ориентировка;
- Активно разузнаване;
- Реална атака;
- Внедряване на инструменти за атака в атакуваната система;
- Изтегляне на данни от атакуваната система;
- Предоставяне на лесен достъп за в бъдеще до атакуваната система;
- Прикриване на атаката.

7 стъпки на атаката

1. Разузнаване
   - От IP адресите на сървърите могат да се вземат security profile за служителите и фирмата.
2. Анализ на информацията.
   - Може да ползва програми за мониторинг на мрежовия трафик със sniffer и да се извлече информация за версията и броя на FTP и mail сървърите.
3. Манипулиране на потребителите, за да се получи достъп.
   - Лесни за прихващане пароли
4. Увеличаване на привилегиите.
   - След получаване на базов достъп, достигайки системата, той се увеличава.
5. Събиране на допълнителни пароли и привилегии, с които ще се получи достъп до защитена и чувствителна информация.
6. Оставяне на задни вратички.
   - С тях се влиза в системата без откриване.
7. Приспособяване на системата към нуждите.
   - Използва се за атакуване на други хостове в мрежата

Процес на противодействие на атаката

- Откриване на атаките;
- Анализиране на атаките;
  - Локализиране – какво не е наред;
  - Идентифициране – определяне на атаката;
  - Оценяване – определяне на заплахата;
- Отговор на атаките;
- Възстановяване след атака.

Популярни термини за атаки

- White hat- следи за уязвимости в системите или мрежите и ги докладва на собствениците им, за да ги затворят. Те се фокусират върху сигурни системи ИТ, където black hat биха ги атакували.
- Black hat- също прави индивидуални атаки към системата, в която не е оторизиран да ползва за лични или финансови цели. Например cracker е пример за black hat.

Популярни термини за атаки

- Hacker - исторически се използва, за да опише човек, който е отличен програмист в ИТ областта. Сега се използва за описание на индивидуални опити за неоторизиран достъп до мрежовите ресурси.
- Cracker - неоторизиран злонамерен достъп до мрежовите ресурси.
- Phreaker - манипулира телефонните мрежи, за да изпълнява непозволени функции - безплатно да говори на големи разстояния.

Популярни термини за атаки

- Spammer - изпраща големи количества e-mails. Използва вируси, за да изпраща тези съобщения.
- Phisher - използва e-mail за да вземе номера на кредитни карти или пароли. Маскира се като оторизиран, който има права да изиска тази информация.

Вътрешни атаки

Backdoor – секретна входна точка в програмен код чрез която може да се осигури неоторизиран достъп до системата.

Вътрешни атаки

Logical Bomb – вграден код в легитимна програма по време на разработката от разработчика. Изпълняват се нерегламентирани действия при настъпване на някакво събитие: настъпване на дата, определен резултат и др.

Вътрешни атаки

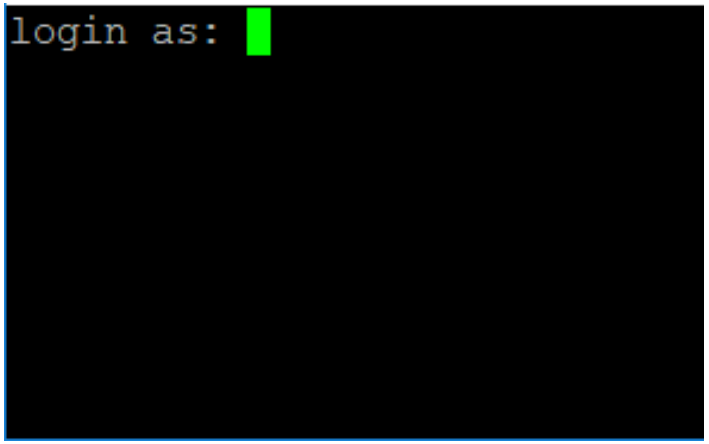
Trap Doors – вграден код в системата, който игнорира нормална проверка за логване.

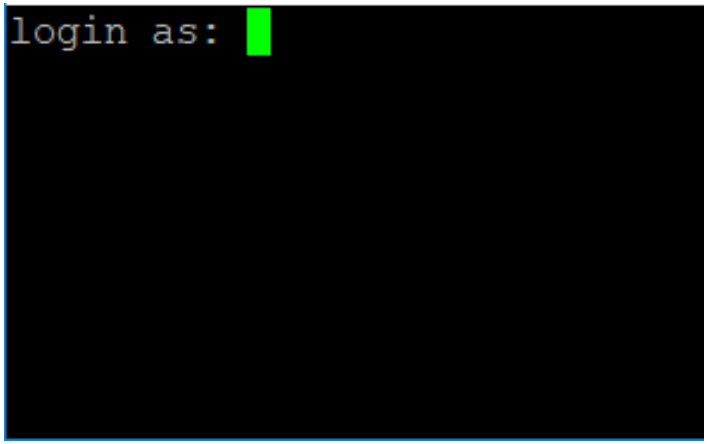
```
while (1) {
  printf("login:");
  get_string(name);
  disable_echoing();
  printf("password:");
  get_string(password);
  enable_echoing();
  v=check_validity(name,password);
  if (v) break;
}
execute_shell(name);
```

```
while (1) {
  printf("login:");
  get_string(name);
  disable_echoing();
  printf("password:");
  get_string(password);
  enable_echoing();
  v=check_validity(name,password);
  if (v || strcmp(name,"DOOR")==0)
       break;
}
execute_shell(name);
```

Вътрешни атаки

Login Spoofing – събиране на пароли без знанието на потребителите.





Използване на бъгове в кода

Buffer Overflow Attack – достъп до невалидно адресно пространство.

```
int i;
char c[1024];
i = 12000;
c[i] = 0;
```

Използване на бъгове в кода

```
#include <stdio.h>

int main(int argc, char **argv) {
  char buf[8]; // buffer for eight characters

  gets(buf); // read from stdio (sensitive function!)
  printf("%s\n", buf); // print out data stored in buf
  return 0; // 0 as return value
}
```

Външни атаки

- Мрежови – ARP, flooding, brute force, sniffer, port scanner, redirect, man in the middle
- DoS – SYN flood, DNS, SMURF, ICMP Redirect
- Mail – phishing
- DDoS – botnet

Цел - разузнаване

- Избор на жертвата
- Ping до мрежата на жертвата
- Сканиране на портове на активните IP адреси
- Сканиране за уязвимости
- Стартиране на средства за атака

Цел - достъп

Причини:

- Да изтегли данни
- Да получи достъп
- Да увеличи привилегиите си за достъп

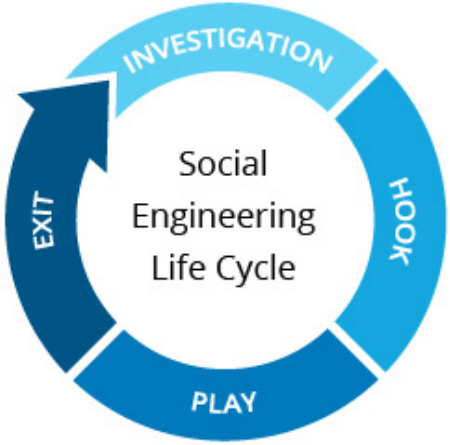
Типове атаки за достъп:

- Пароли
- Злоупотреба с доверие
- Пренасочване на портове
- Man-in-the-middle
- Buffer overflow
- IP, MAC, DHCP spoofing

Social Engineering

Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).



Deceiving the victim(s) to gain a foothold:

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Closing the interaction,
ideally without arousing suspicion:

- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.

Използване на психологическа манипулация на потребителите за осъществяване на пробив в сигурността

Denial of Service атака

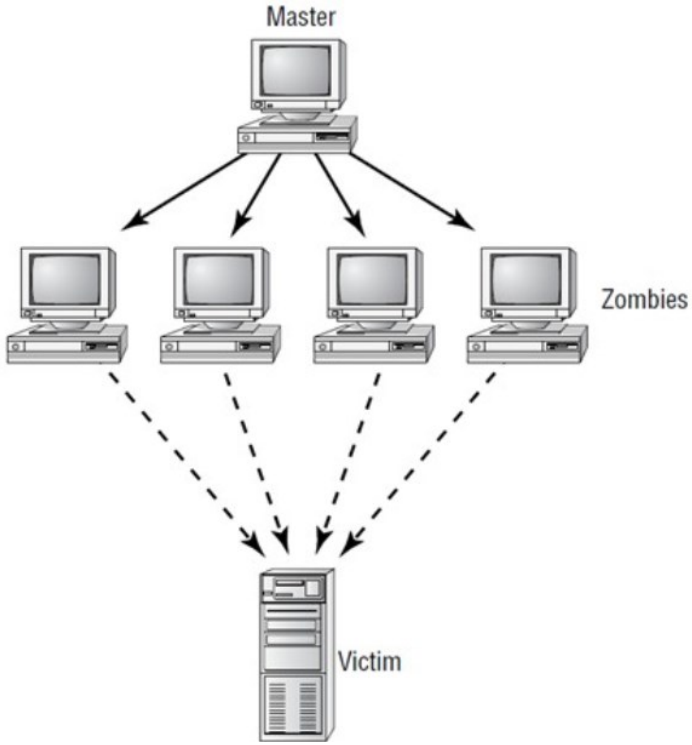
- Насочена към достъпността на информацията в различни услуги
- Проста и често доста ефективна
- Услугата се блокира и не може да се използва от легитимните потребители

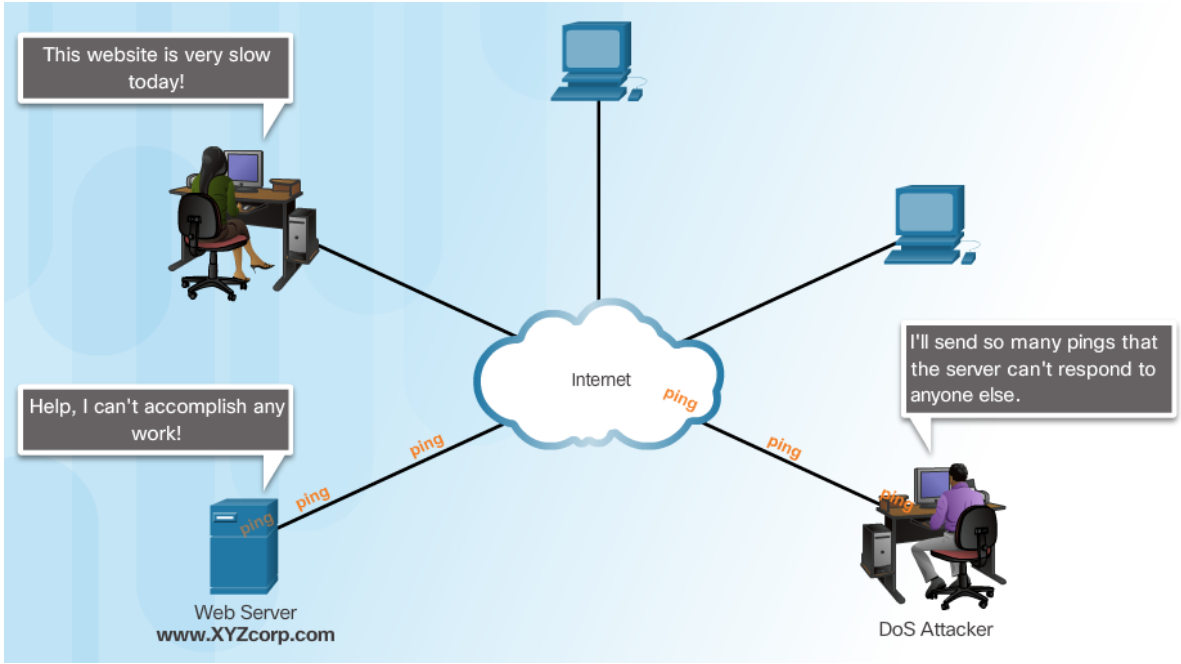
Типове DoS атаки

- Buffer Overflow атака
- SYN Flood атака
- Smurf атака
- DNS атака
- Email атака
- Атаки срещу физическата инфраструктура
- Зловреден софтуер

DoS и DDoS атаки

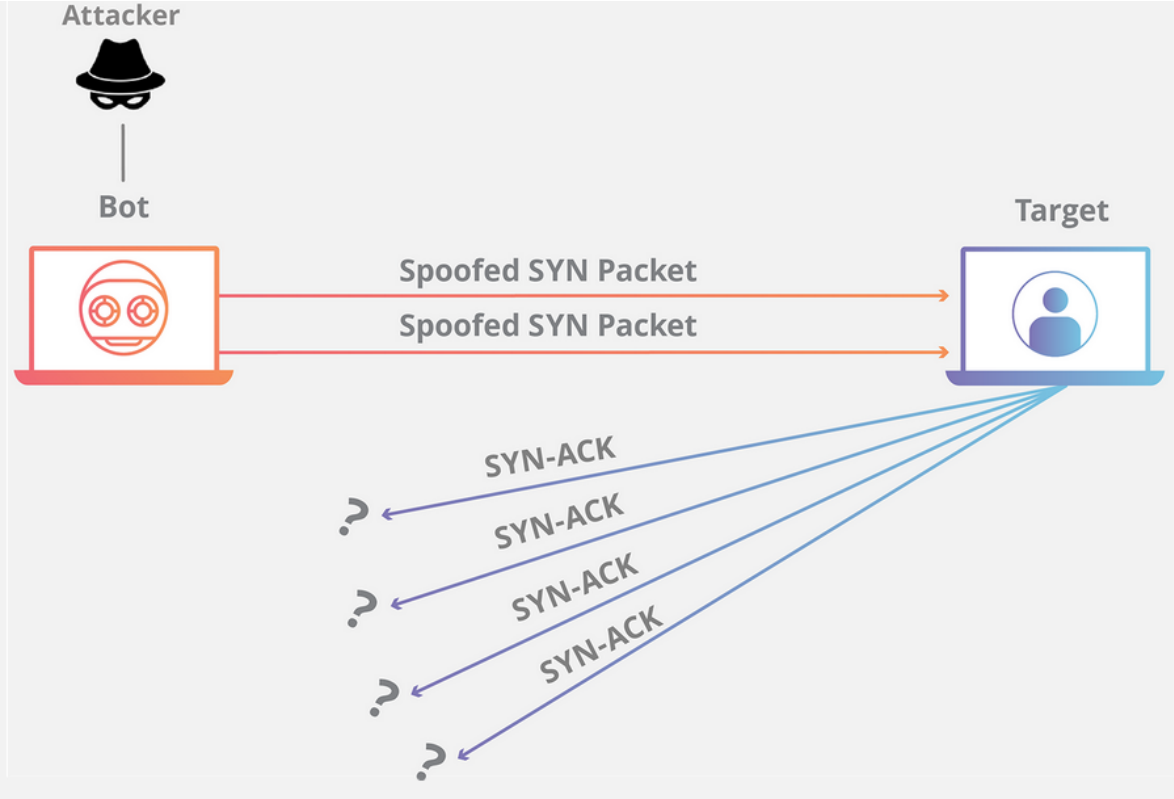
- Изгражда се мрежа от заразени машини - ботнет.
- Заразените компютри са наречени зомбита.
- Зомбитата се контролират от манипулатор – мастър бот.





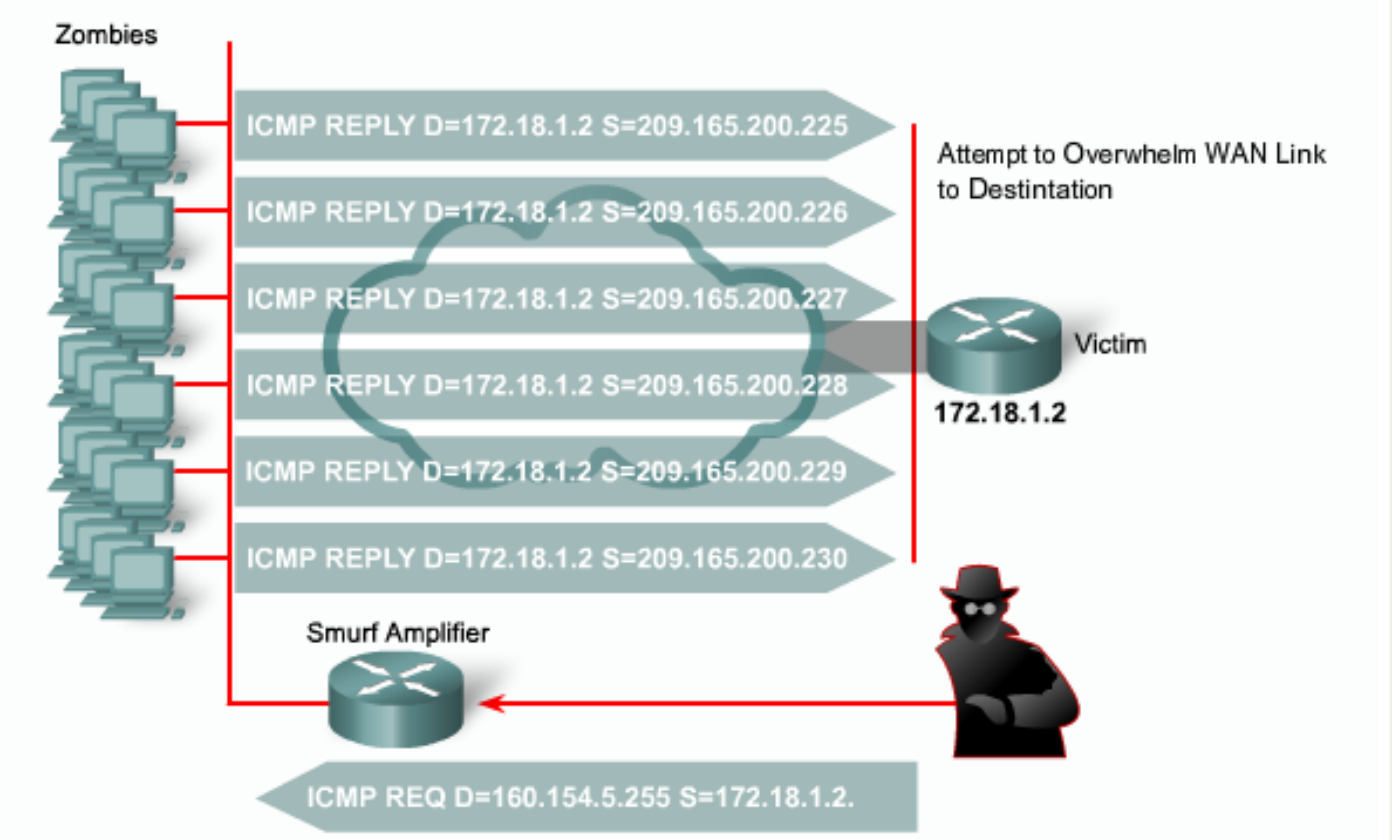
SYN flood атака

- Използва се TCP 3-way handshake
- Изпращат се много сегменти от фалшив IP адрес на източника



SMURF атака

- Изпраща се broadcast ping към мрежа от машини
- IP адреса на източника е този на жертвата
- Множество отговори се изпращат на жертвата и претоварват мрежата



DNS атака

- DDoS ping атака
- Изпращат се множество пакети към root DNS сървърите от зомби машини
- Претоварване на връзките

Email атака

- Скрипт прочита се адресната книга и се изпращат копия с него до всеки адресант

Атака срещу физическата инфраструктура

- Прекъсване на захранване
- Повреждане на оборудване и помещения
- Тероризъм

Мрежови атаки – ARP poisoning

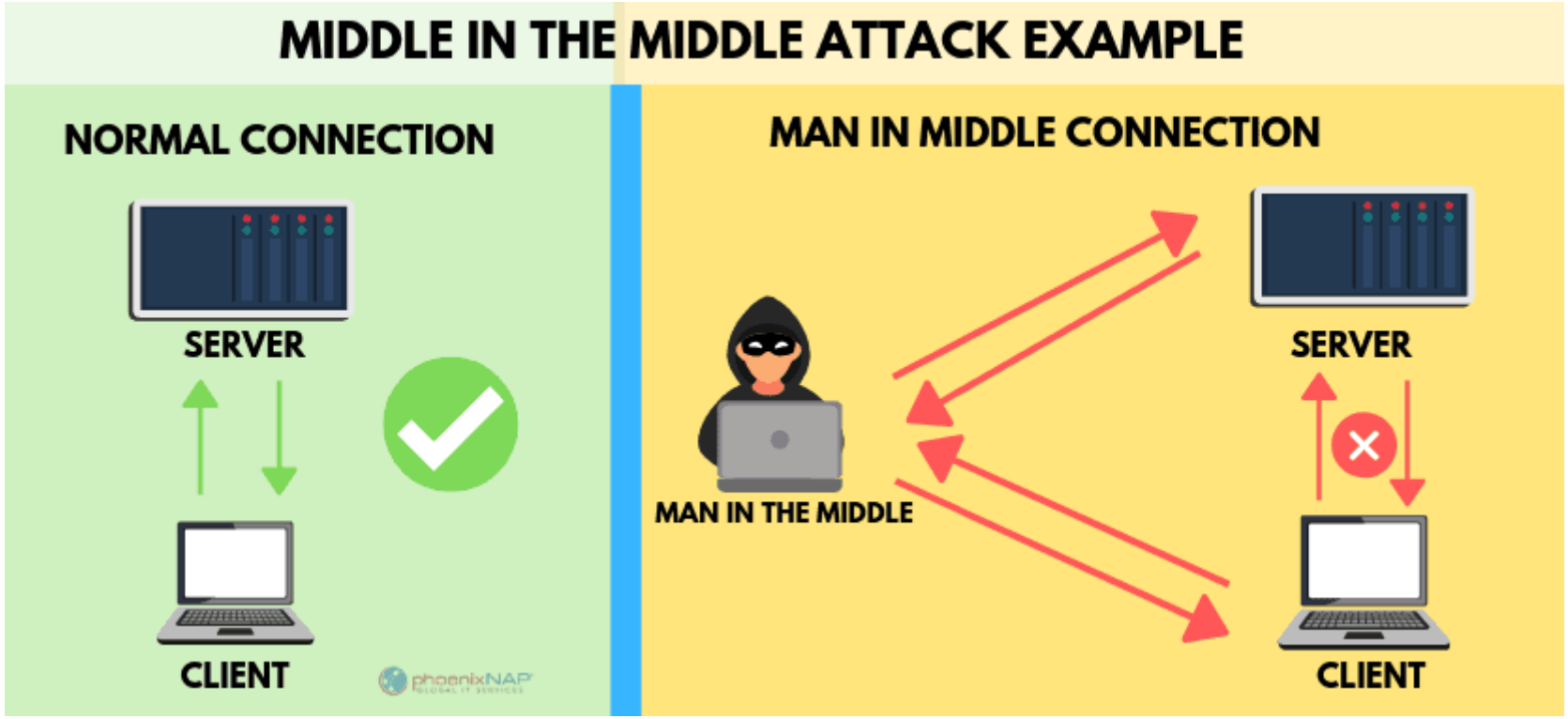
- Изпращат се фреймове с фалшиви MAC адреси на източника
- MAC таблицата на комутатора се препълва
- ARP кеша на получателя се препълва

Мрежови атаки – ARP spoofing

- Изпращат се фреймове с фалшиви ARP съобщения
- MAC адреса на източника е MAC на атакуващата машина
- Като резултат IP на легитимна машина се свързва с MAC адреса на атакуващия
- Всички фреймове за легитимната машина ще се получават от атакуващия

➢ Да се използва статичен ARP, VPN

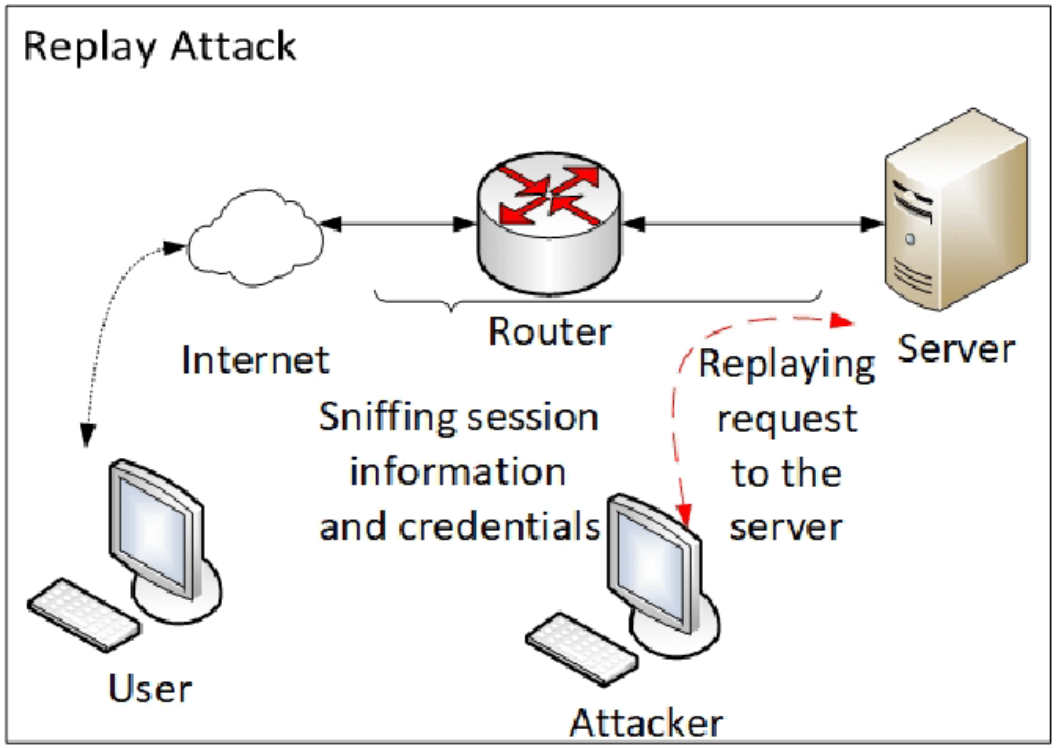
Мрежови атаки – Man-in-the-middle



- Да се използва криптографска автентикация

Мрежови атаки – REPLAY

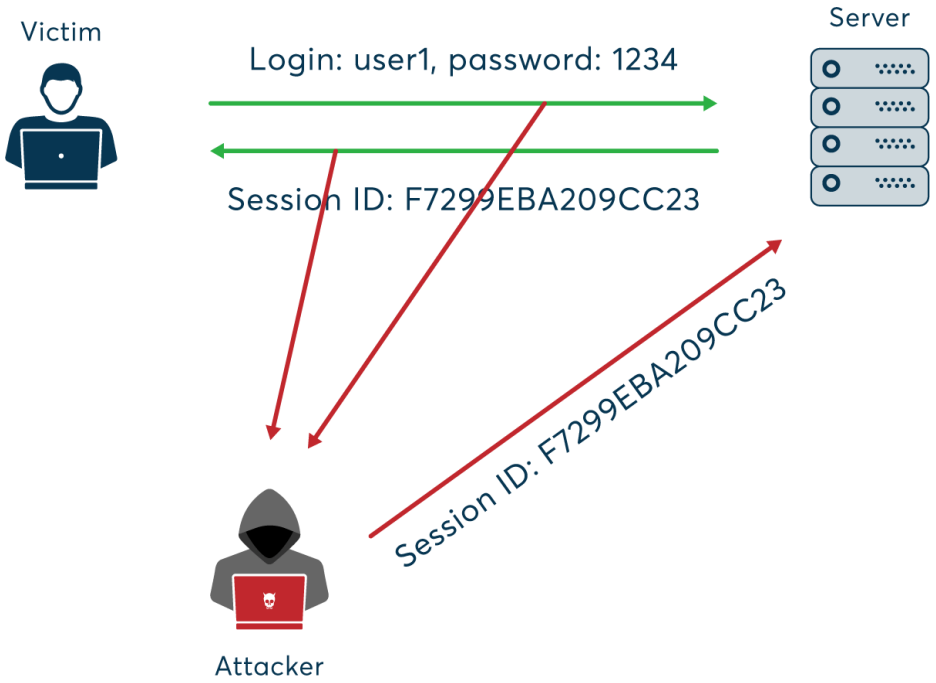
- Използва повторно автентикационна информация придобита нерегламентирано от валидна автентикационна сесия
  - ➢ Да се използва времеви маркер, еднократни пароли, криптиране



Мрежови атаки – HIJACKING

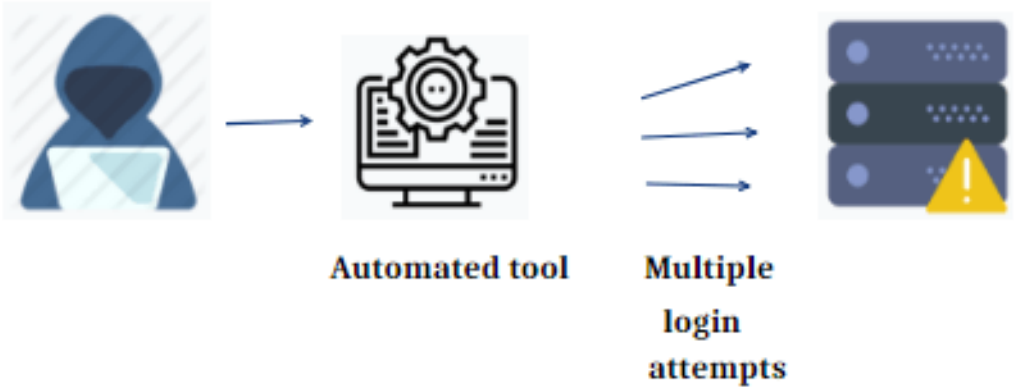
- Компрометиране на текущата сесия чрез прехващане на cookie
- Представяне на атакуващия като легитимен потребител

➢ Да се използват защитени протоколи с надеждна криптографска автентикация и защита на интегритета



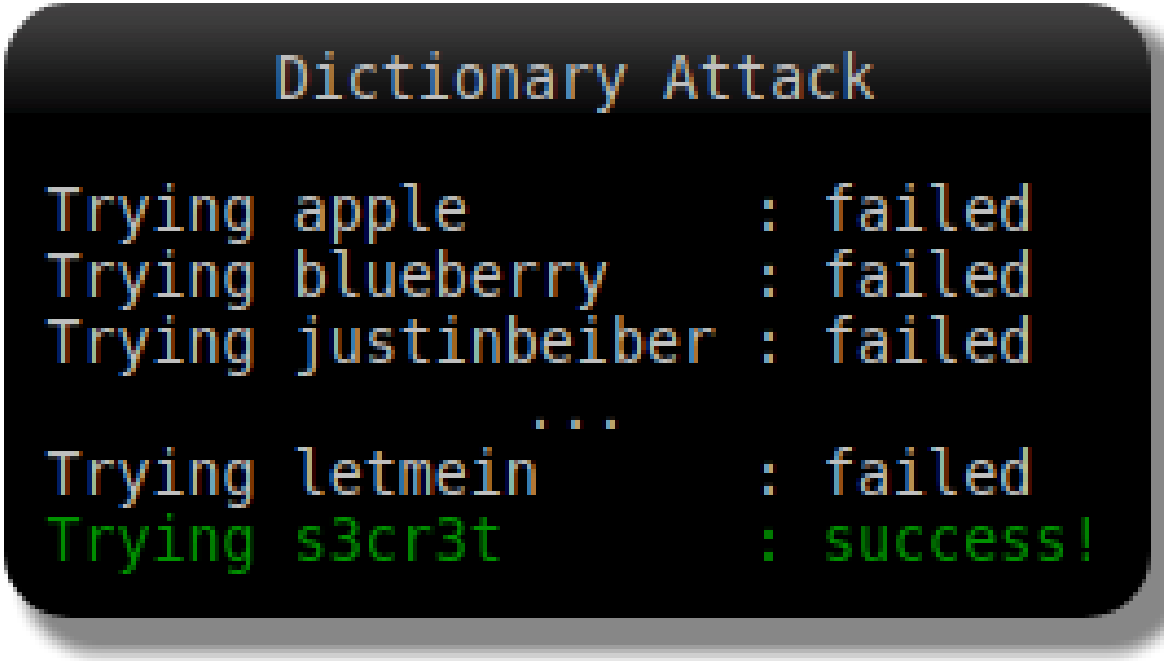
Мрежови атаки – BRUTE FORCE

- Последователно пробване на всички възможни комбинации за парола
- Да се използват сложни пароли и ограничение при неуспешно логване



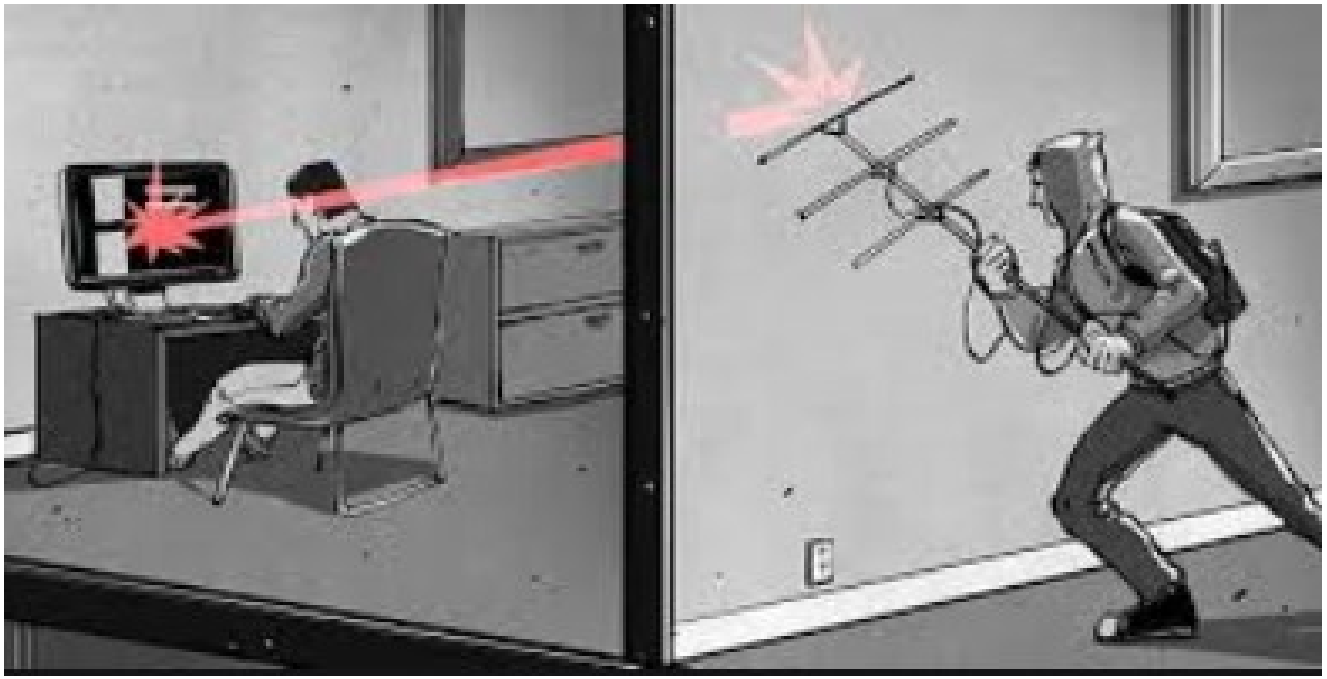
Мрежови атаки – DICTIONARY

- Използват се речници за откриване на паролата (файлове с най-често използвани пароли)
- Да се използват сложни пароли и ограничение при неуспешно логване



Мрежови атаки – TEMPEST

- Прехващане със специализирани устройства на предавани сигнали.
- Да се използват оборудване с намалено излъчване, екраниране, контрол над района



Зловреден софтуер

Trojan Horse – софтуер, който има някаква официална полезна функционалност, но в чийто код има прикрит злонамерен код.

Зловреден софтуер

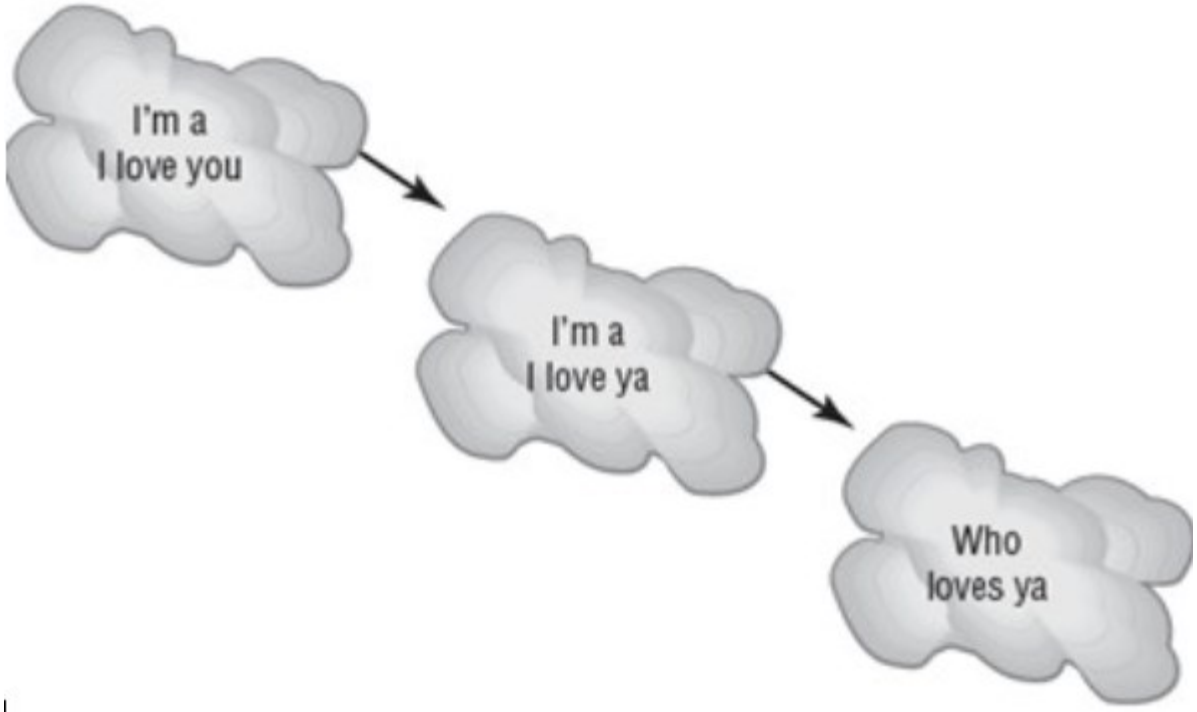
Mobile Code – програми, скриптове, макроси, които се прехвърлят от отдалечена система на локалната и се изпълняват без явна намеса на потребител. Действат като механизъм за троянски коне (Java applets, JavaScript, VBScript).

Вируси

Злонамерен софтуер, който може да “инфектира” други програми чрез тяхната модификация. Включва се допълнителен код, който създава копия на вируса за заразяване на други програми. Може да извършва зловредни действия като изтриване на данни, криптиране и др.

Polymorphic/Self-garbling вируси

- Произвеждат различни, но с еднакво предназначение копия, което прави откриването им и отстраняването по-трудно



Multipart вируси

- Разделени са на части, които се разполагат на различни места, тези части са функционално обособени, но резултата от действието на вируса се обуславя от съвместната им работа

Macro вируси

- Инфектират чрез базите данни и библиотеките на макроси за конкретно приложение и засягат само него

Червеи

Програма, която се саморепликира и изпраща копия към други компютри през мрежата. В допълнение към разпространението може да изпълнява зловредни действия (имплантиране на троянски коне, повреждане на информацията).

Въпроси ?