Заплахи за сигурността. Средства за защита

проф. д-р инж. Венета Алексиева

Основни моменти

- Заплахи за сигурноста на мрежата и данните
- Видове атаки
- Стъпки на атаката
- Противодействие на атаката
- Термини, свързани с мрежови атаки
- Злонамерен код (вируси)

Заплаха за сигурността

Това е потенциална опасност за:

– информацията

– компютърната система

– мрежовата услуга

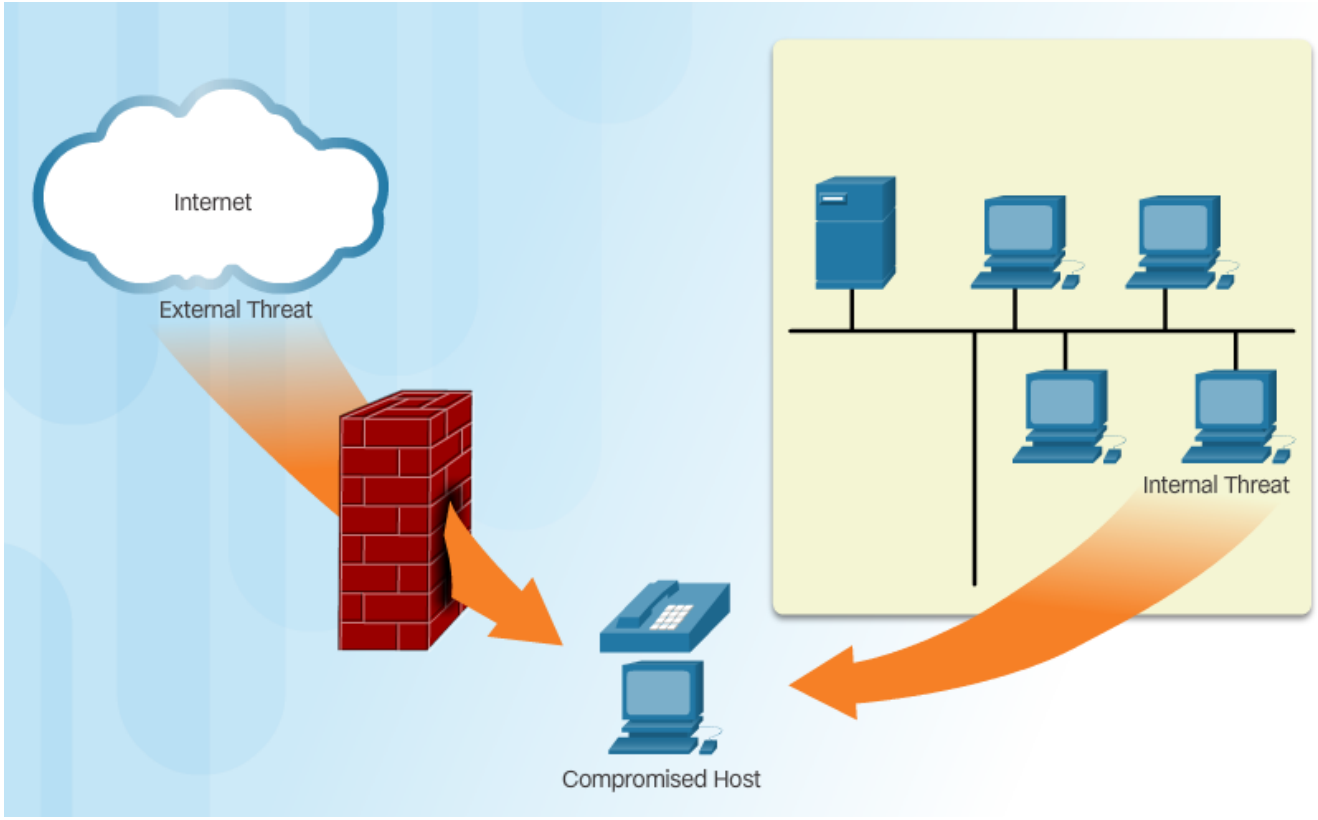
Класове физически заплахи

- Хардуерни
  - физически да се развалят сървъри, маршрутизатори, 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

По произход са:

- Вътрешни
- Външни



Видове заплахи по начин на организиране

По начин на организиране са:

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

Видове заплахи по начин на провеждане на атаката

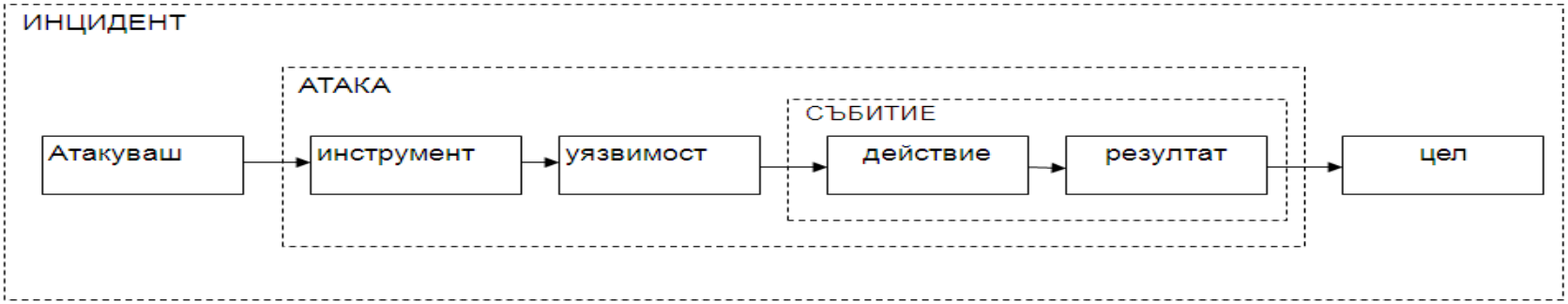
По начин на провеждане на атаката са:

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

Фактите

- С годините атаките към мрежовата сигурност се развиват.
  - През 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.
- Методите за атака се развиват, но и 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. Разузнай!
   - От IP адресите на сървърите могат да се вземат security profile за служителите и фирмата.
2. Пресметни информацията.
   - Може да ползва програми за мониторинг на мрежовия трафик със sniffer и да извлече информация за версията и броя на FTP и mail сървърите.
3. Манипулирай потребителите, за да получиш достъп.
   - Лесни за прихващане пароли
4. Увеличи си привилегиите.
   - След получаване на базов достъп, достигайки системата, той си го увеличава.
5. Събери допълнителни пароли и привилегии, с които ще получиш достъп до защитена и чувствителна информация.
6. Остави си задни вратички.
   - С тях ще влезеш в системата без да те открият. Напр. backdoor е списъка с отворени портове на TCP иUDP.
7. Приспособи системата към нуждите си.
   - Използвай я за да атакуваш други хостове в мрежата

Подходи за предпазване от атаки

- Разделяне;
- Защита на най-слабото звено (Weakest link);
- Употреба на “тапа”(choke points);
- Предоставяне на защита в дълбочина;
- Сигурност при провал;
- Ограничаване на непредвидими действия;
- Предпочитане на простотата;
- Назначаване на подходящи потребители;
- Убеденост в мерките за сигурност;
- Въпроси;
- Бдителност;
- Наблюдение на наблюдаващите.

Изисквания към защитата

- Мобилност;
- Унифицираност;
- Минималност на привилегиите;
- Самостоятелност;
- Гъвкавост;
- Минималност на човешкото участие;
- Възможност за ъпгрейд;
- Възможност за контрол;
- Проверимост;
- Безкомпромисност;
- Приложимост;
- Употребимост.

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 атакуващи

- 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.
- 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.

Видове хакери

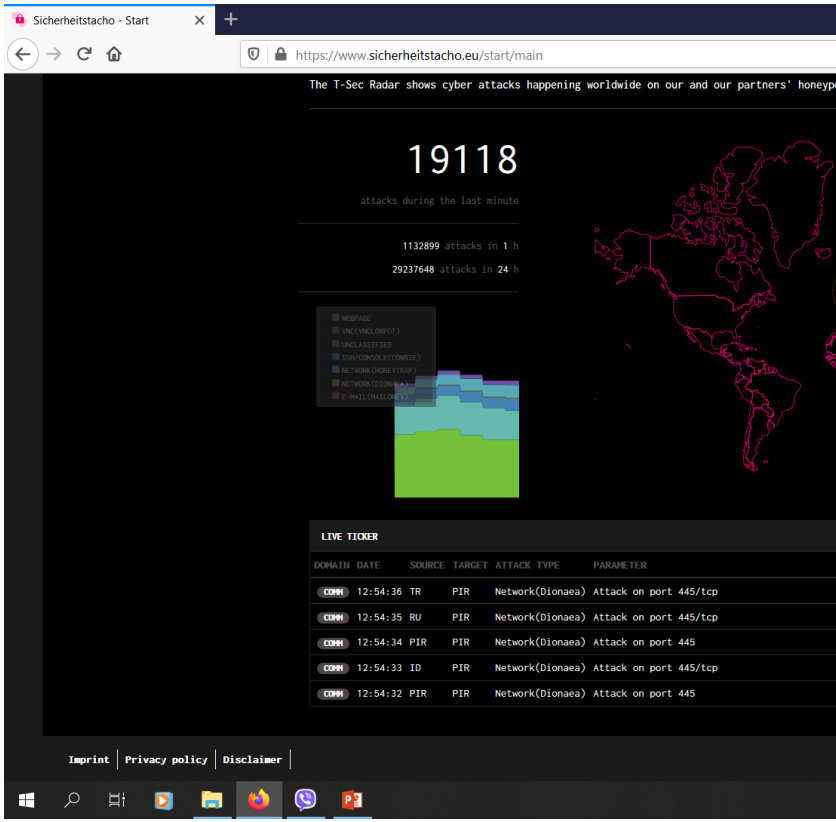
- **White hat-** Следи за уязвимости в системите или мрежите и ги докладва на собствениците им, за да ги затворят. Те се фокусират върху сигурни системи ИТ, където black hat биха ги атакували.
- **Grey hat** - Нарушава сигурността на система без истинско злонамерено намерение, но често без предварителното знание или съгласие на собственика или разработчика, но който по-късно докладва за уязвимости на системата на собстеника й, понякога за лична изгода.
- **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.

Модерни хакерски атаки

- **Skids-** неквалифициран човек, който използва скриптове или програми, разработени от специалисти, за да атакува компютърни системи и мрежи и да обезобразява уебсайтове.
- **Брокери на уязвимости** – grey hats, които се опитват да открият експлойти и да ги докладват на доставчици, понякога срещу награди.
- **Хактивисти** -получават неоторизиран достъп до компютърни файлове или мрежи с цел постигане на социални или политически цели.
- **Кибер престъпници -**престъпни дейности, извършвани чрез компютри или Интернет –да повредят устройства, да забранят услуги, да получат финансова изгода, да разпространят зловреден софтуер, да получат незаконна информация...
- **Спонсорирани от държавата хакери -**работят за насърчаване на интересите на дадена държава - срив на уебсайт, критичен към държавата; осакатяване на определени финансовите системи ; да повлияят на различни потребители на социални медии чрез онлайн кампании в полза на определени държавни интереси

Видове атаки

- Мрежови – ARP, flooding, brute force, sniffer, port scanner, redirect, man in the middle…
- DoS – buffer overflow, SYN flood, DNS, SMURF, ICMP Redirect…
- DDoS- botnet, zombie…
- Mail – phishing,..
- Червеи
- Вируси
- Троянски коне



Еволюция на средствата за атаки

- “Хакване” на пароли
- “Хакване” на Wireless
- “Хакване” на операционни системи
- Сканиране за достъпни мрежи и “Хакване” на мрежи
- Генериране на пакети
- Подслушване на пакети
- Следене за уязвимости и използване на уязвимости
- Използване на дебъгери
- Криптиране

Еволюция на атаките

- Подслушване (Eavesdropping)
- Промяна на данните (Data modification)
- Подправяне на IP адрес (IP address spoofing)
- Базирани на пароли (Password-based)
- Отказ на услуга (Denial-of-service)
- Човек-в-средата (Man-in-the-middle)
- Променен ключ (Compromised-key)
- Sniffer

Еволюция на средствата за атаки

Предназначение	Средство за атака
Хакване на пароли	John the Ripper, Ophcrack, L0phtCrack, THC Hydra, Rainbow Crack, and Medusa
Хакване на wireless мрежи	Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep, and ViStumbler
Сканиране на мрежи за отворен достъп	Nmap, SuperScan, Angry IP Scanner, and NetScanTools
тестване на устойчивостта на защитната стена	Използват се специално подправени пакети. Hping, Scapy, Socat, Yersinia, Netcat, Nping и Nemesis.
Снифери на пакети	Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy, and SSLstrip.

Еволюция на средствата за атаки

Предназначение	Средство за атака
Rootkit Detectors	проверка на целостта на директории и файлове AIDE, Netfilter, and PF: OpenBSD Packet Filter
откриване на уязвимости на сигурността на PC	Skipfish, Wapiti, and W3af
Forensic Tools	Търсят следи от доказателства за дейност на PC Sleuth Kit, Helix, Maltego, and Encase
Дебъгери	За обратно проектиране на двоични файлове при писане на експлойти GDB, WinDbg, IDA Pro, and Immunity Debugger
ОС, предназначени за хакване на мрежи	Kali Linux, BackBox Linux
Криптиране	VeraCrypt, CipherShed, OpenSSH, OpenSSL, Tor, OpenVPN, and Stunnel
Инструменти за използване на уязвимости	Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit, and Netsparker
Сканиране на уязвимости	Nipper, Core Impact, Nessus, SAINT, and OpenVAS

Действия при 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

Действия при 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

Видове атаки за Social Engineering

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

Видове:

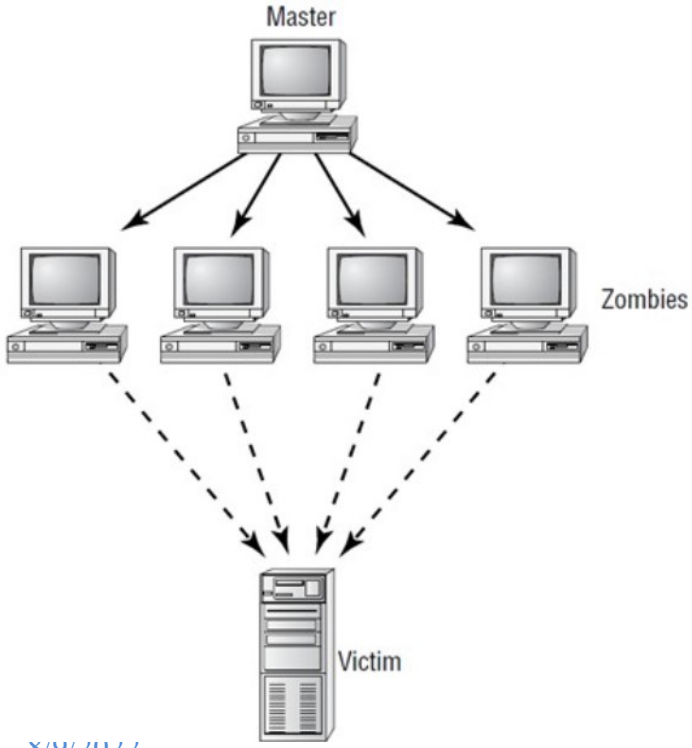
- Pretexting
- Phishing
- Spearphishing
- Spam
- Tailgating
- Something for Something
- Baiting

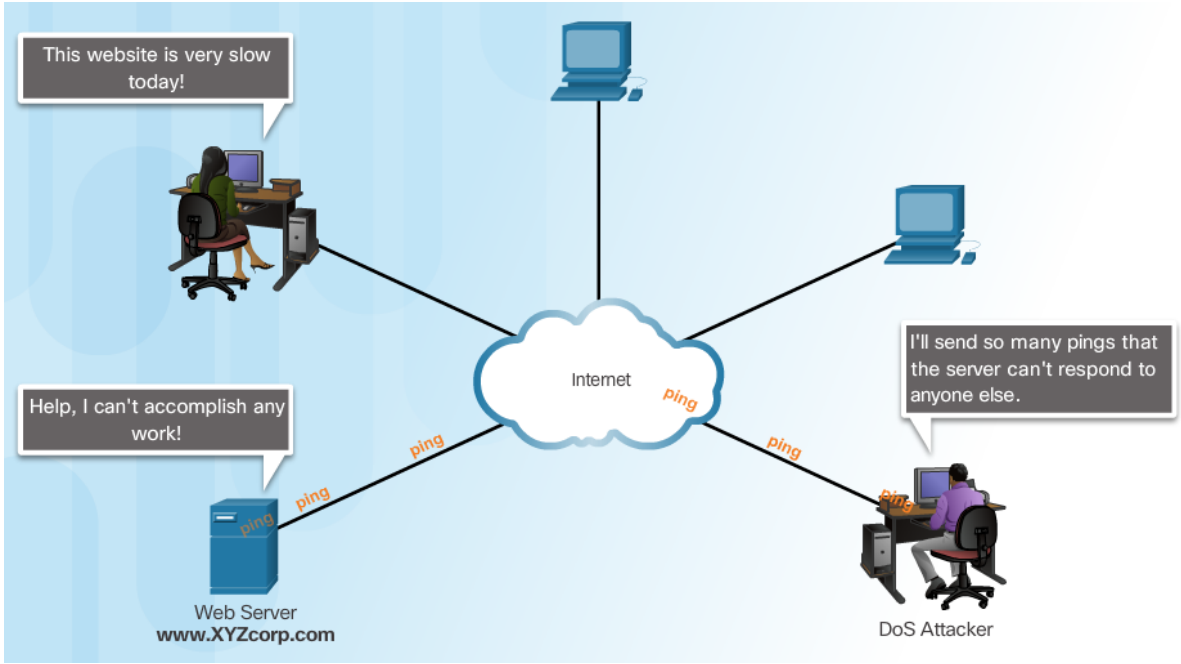
Видове атаки за IP мрежи

- **ICMP атака**
  - Използват icmp echo пакети, за да откриват подмрежи и хостове в защитена мрежа, да генерират DoS flood атаки и да променят таблици за маршрутизиране на хоста.
- **DoS и DDoS атаки**
- **Address spoofing атаки**
  - Подправят IP адреса на източника в IP пакета.
- **Man-in-the-middle атаки**
  - Наблюдават прозрачно, улавят и контролират комуникацията.
- **Session hijacking**
  - получават достъп до физическата мрежа и след това използват Man-in-the-middle атаки

Видове DoS и DDoS атаки

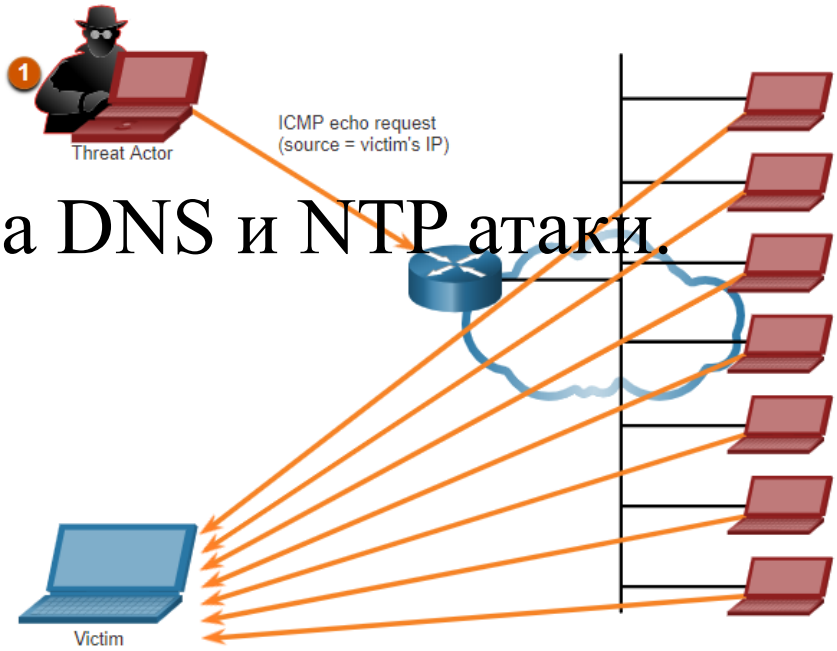
- Изгражда се мрежа от заразени машини - ботнет.
- Заразените компютри са наречени зомбита.
- Зомбитата се контролират от манипулатор – мастър бот.





ICMP атака

- Smurf атака, използвана за пренатоварване на хоста- жертва.
- 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

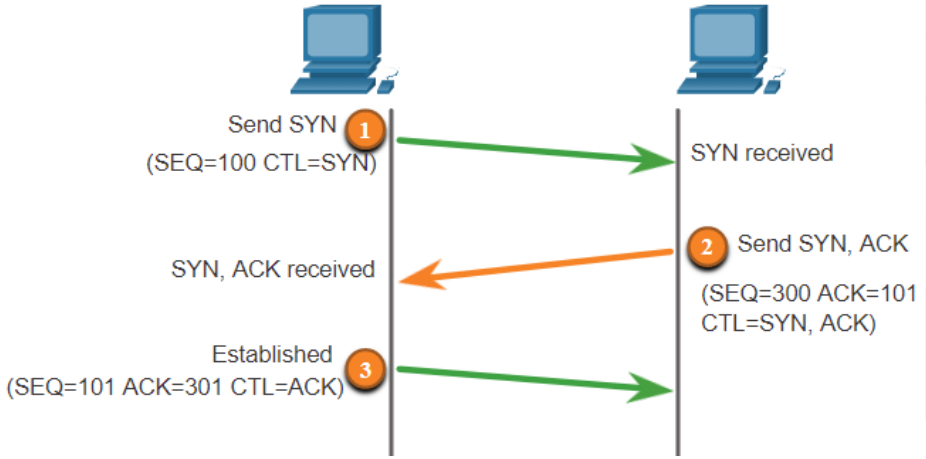


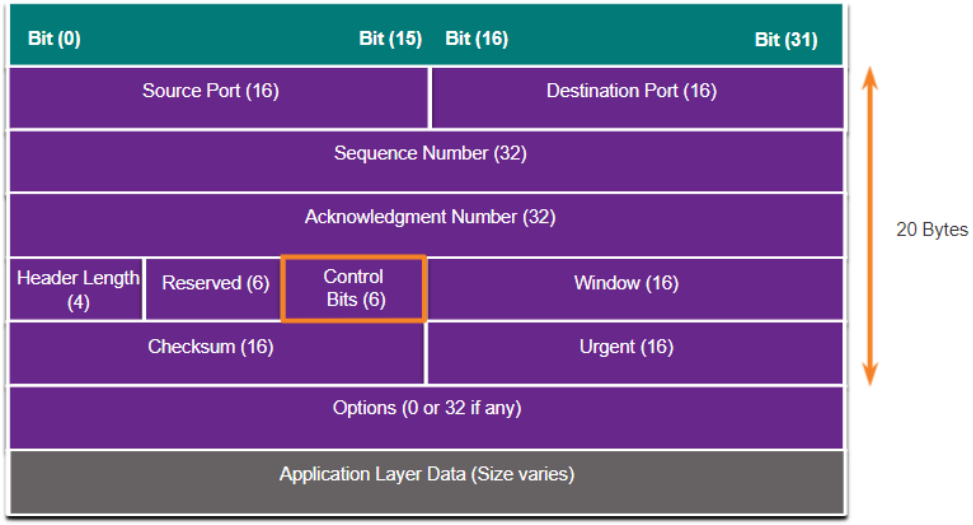
- Аналогични са базирани на DNS и NTP атаки.

ICMP

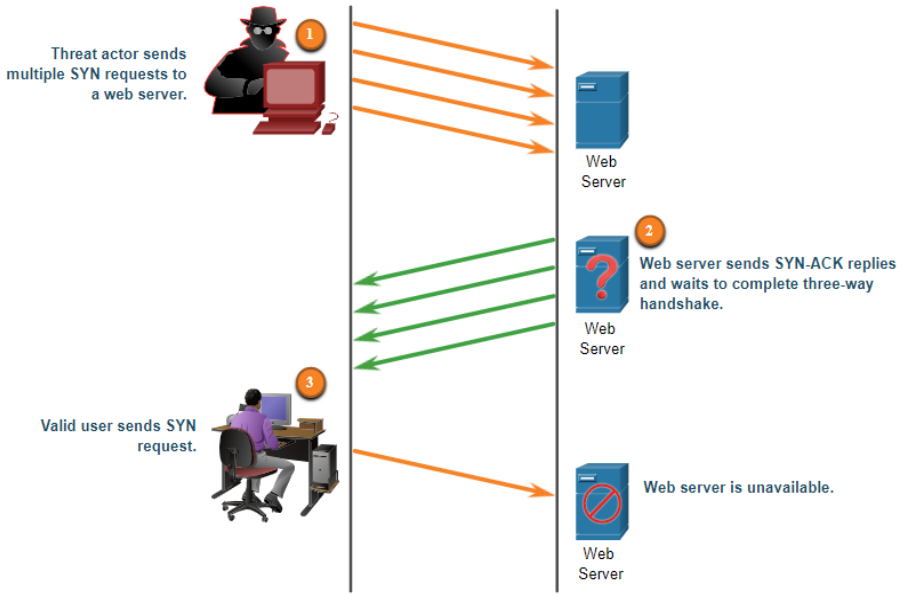
- **ICMP echo request and echo reply**
- за извършване на проверка на достъпност на хоста и DoS атаки
- **ICMP unreachable**
- за извършване на мрежови разузнавателни и сканиращи атаки.
- **ICMP mask reply**
- за картографиране на вътрешна IP мрежа.
- **ICMP redirects**
- за примамване на целевия хост да изпраща целия трафик през компрометирано устройство и да създаде man-in-the-middle атака
- **ICMP router discovery**
- за инжектиране на фалшиви маршрути в маршрутната таблица на атакувания хост

TCP SYN Flood атака

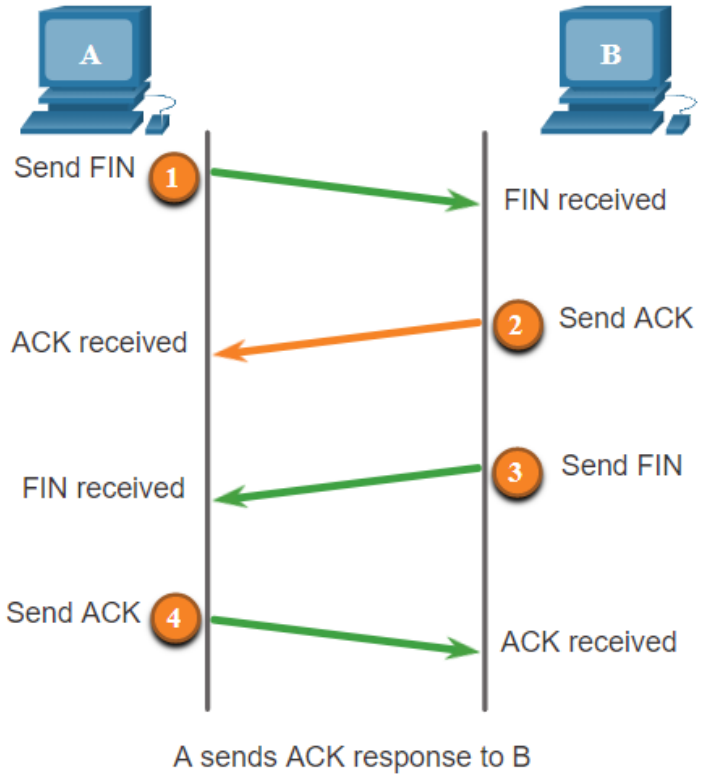




- Изпращат се множество SYN заявки до уеб сървъра.
- Той отговаря със SYN-ACK за всяка SYNзаявка и чака да завърши трипосочното ръкостискане.
- Атакуващият не реагира на SYN-ACK.
- Валиден потребител няма достъп до уеб сървъра, тъй като уеб сървърът има твърде много полуотворени TCP връзки.

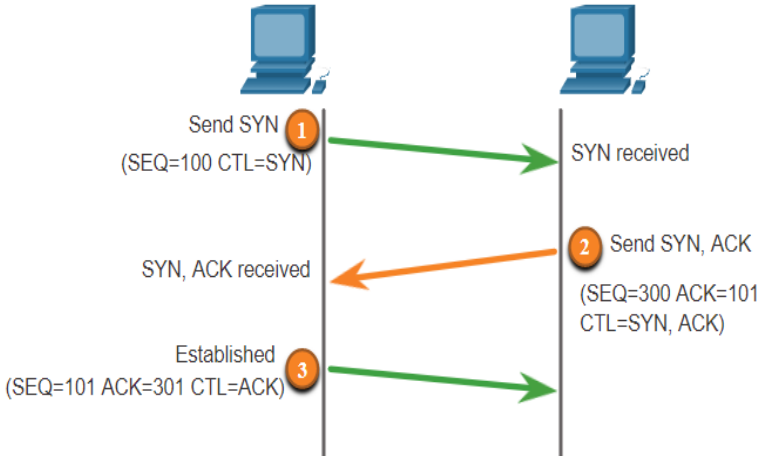


TCP RST атака



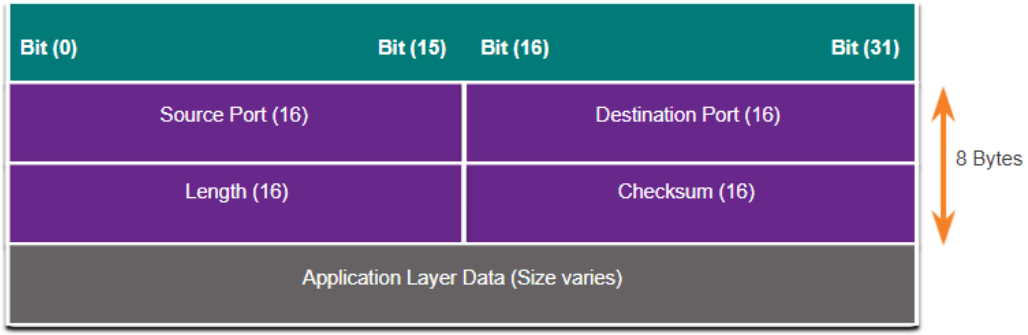
- Когато клиентът няма повече данни за изпращане в потока, той изпраща сегмент с зададен флаг FIN.
- Сървърът изпраща ACK, за да потвърди получаването на FIN, за да прекрати сесията от клиент към сървър.
- Сървърът изпраща FIN до клиента, за да прекрати сесията от сървъра към клиента.
- Клиентът отговаря с ACK, за да потвърди FIN от сървъра.
- Атакуващият може да извърши атака за прекратяване на TCP сесия и да изпрати фалшив пакет, съдържащ TCP RST до едната или и двете страни на връзката.

TCP hijacking атака



- Отвличането на TCP сесия е друга TCP уязвимост.
- Атакуващият поема комуникацията от вече удостоверен хост, докато комуникира с целта.
- Той трябва да подправи IP адреса на единия хост, да предскаже следващия пореден номер и да изпрати ACK до другия хост.
- Ако успее, участникът в заплахата може да изпраща, но не и да получава данни от целевото устройство.

UDP Flood атака

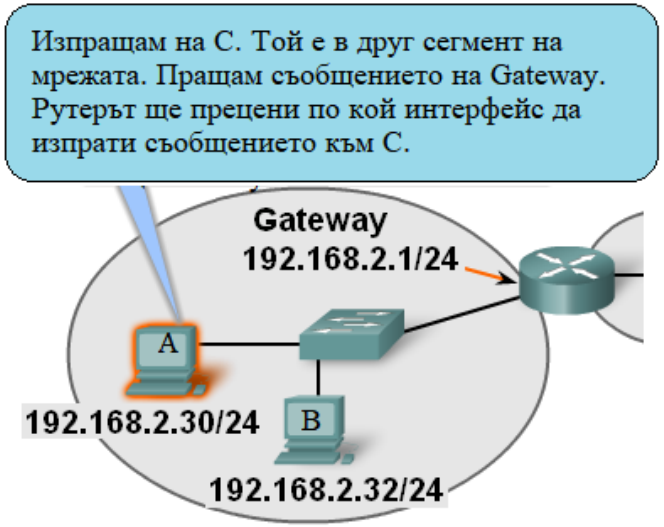


- UDP се използва от DNS, TFTP, NFS и SNMP, приложения в реално време, VoIP.
- Криптирането не е по подразбиране.
- Атакуващият използва инструмент UDP Unicorn или Low Orbit Ion Cannon). Тези инструменти изпращат поток от UDP пакети, често от фалшив хост, до сървър в подмрежата.
- Програмата проверява всички известни портове, опитвайки се да намери затворени портове. Това ще накара сървъра да отговори с ICMP port unreachable съобщение.
- Големият брой затворени портове създава много трафик в сегмента, който заема bandwidth-a.
- Резултатът е много подобен на DoS атака.

ARP атаки

- Хостовете изпращат ARP Request към други хостове в сегмента, за да определят MAC адреса на хост по определен IP адрес.
- Хостът със съответстващ IP адрес в ARP Request изпраща ARP Reply.
- Всеки хост може да изпрати непоискан ARP Reply- „безвъзмезден ARP“.
- Когато хост изпраща безвъзмезден ARP, други хостове в подмрежата съхраняват MAC адреса и IP адреса, съдържащи се в безвъзмездния ARP в техните ARP таблици.
- Тази функция на ARP също означава, че всеки хост може да твърди, че е собственик на който и да е IP или MAC адрес.
- Атакуващият може да промени ARP кеша на хостовете в локалната мрежа, създавайки man-in-the –middle атака за пренасочване на трафика.

ARP Cache Poisoning атака



ARP cache poisoning може да се използва за стартиране на различни man-in-the-middle атаки:

- PC-A изисква MAC адреса на рутера като изпраща ARP Request за MAC адреса на 192.168.2.1.
- Рутерът актуализира своя ARP кеш с IP и MAC адресите на PC-A.
- Рутерът изпраща ARP Request до PC-A, който след това актуализира своя ARP кеш с IP и MAC адресите на рутера.

- Атакуващият изпраща два фалшиви безвъзмездни ARP Reply, използвайки свой собствен MAC адрес за посочените IP адреси на дестинация.
- PC-A актуализира своя ARP кеш със своя GW, който сега сочи към MAC адреса на хоста на атакуващия.
- Рутерът също актуализира своя ARP кеш с IP адреса на PC-A, сочещ към MAC адреса на атакуващия.
- Атаката на отравяне с ARP може да бъде пасивна или активна:
  - Пасивно отравяне с ARP е когато атакуващият краде поверителна информация.
  - Активно ARP отравяне е когато атакуващият модифицира данните или инжектира злонамерени данни.

DNS Open Resolver атака

- DNS open resolver отговаря на заявки от клиенти извън административния си домейн.
- **DNS cache poisoning атака**
  - Атакуващият изпраща фалшифицирана информация за ресурсни записи (RR) до DNS resolver, за да пренасочват потребителите от законни сайтове към злонамерени сайтове.
- **DNS amplification and reflection attacks**
  - Атакуващият използва DoS или DDoS атаки срещу DNS open resolvers, за да увеличат обема на атаките и да скрият истинския източник на атака. Атакуващият изпраща DNS съобщения до DNS open resolvers, използвайки IP адреса на целевия хост.
  - Тези атаки са възможни, защото DNS open resolver ще отговаря на запитвания от всеки, който задава въпрос.
- **DNS resource utilization attacks**
  - DoS атака, която консумира ресурсите на DNS open resolvers, за да повлияе отрицателно на работата му.
  - Въздействието на тази DoS атака може да наложи рестартирането на DNS open resolvers или услугите да бъдат спрени и рестартирани.

DNS stealth атаки

- Атакуващите използват DNS стелт техниките, за да скрият своята самоличност.
- **Fast Flux**
  - Атакуващите скриват така своите сайтове за фишинг и доставка на злонамерен софтуер зад бързо променяща се мрежа от компрометирани DNS хостове.
  - DNS IP адресите се променят непрекъснато в рамките на минути.
  - Ботнет мрежите често използват техники Fast Flux за ефективно скриване на злонамерени сървъри.
- **Double IP Flux**
  - Атакуващите използват тази техника за бърза промяна на името на хоста, съответстващо на IP адреси и за промяна на авторитетния сървър за имена. Това увеличава трудността при идентифициране на източника на атаката.
- **Domain Generation Algorithms**
  - Атакуващите използват тази техника, за да генерират случайни имена на домейни, които след това могат да се използват като точки за достъп към техните сървъри за командване и контрол (C&C).

DNS domain shadowing атаки

- Проследяването на домейни включва атакуващият, който събира кредениции за акаунти на домейн, за да създаде множество поддомейни, които да се използват по време на атаките.
- Тези поддомейни обикновено пренасочват към злонамерени сървъри, без да предупреждават действителния собственик на родителския домейн.

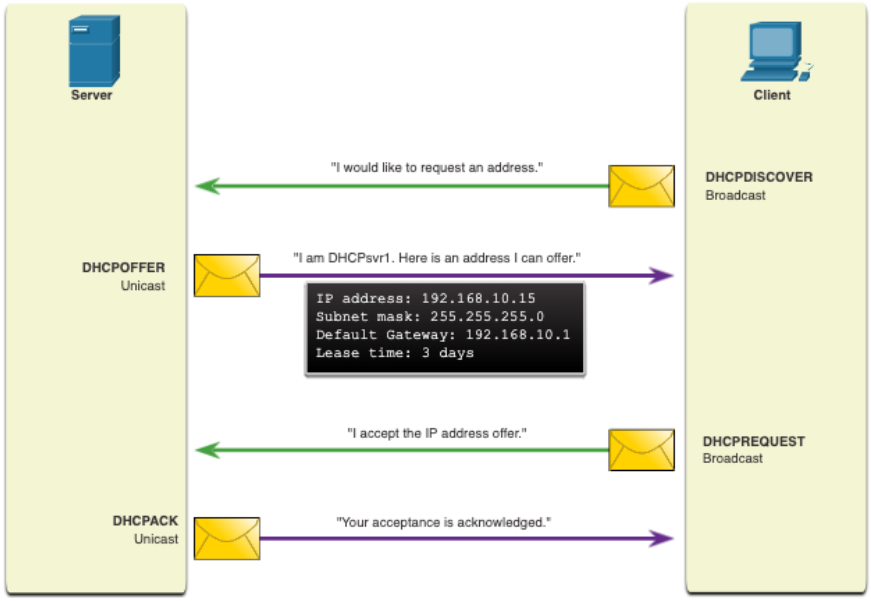
DNS tunneling атаки

- Атакуващият използва DNS тунелиране, като поставя не-DNS трафик в DNS трафик.
- Този метод често заобикаля решенията за сигурност, когато атакуващият желае да комуникира с ботове в защитена мрежа или да открадне данни от организацията.
- DNS тунелиране за команди CnC, изпратени до ботнет:
  - Данните за командата са разделени на множество кодирани парчета.
  - Всяко парче се поставя в етикет с име на домейн от по-ниско ниво на DNS заявката. Тъй като няма отговор от локалния или мрежов DNS на заявката, заявката се изпраща рекурсивно до DNS сървъра на ISP.
  - Рекурсивната DNS услуга ще препрати заявката към авторитетния сървър за имена на атакуващия.
  - Процесът се повтаря, докато не бъдат изпратени всички заявки, съдържащи парчетата от атаката.
  - Когато авторитетният сървър за имена на атакуващия получава DNS заявките от заразените устройства, той изпраща отговори за всяка DNS заявка, които съдържат капсулираните кодирани CnC команди.
  - Зловреднният софтуер на компрометирания хост рекомбинира парчетата и изпълнява командите, скрити в DNS записа.
- За да спре DNS тунелирането, мрежовият администратор трябва да използва филтър, който проверява DNS трафика(нетипично дълги DNS заявки или заявки, които имат подозрително име на домейн ...).

E-mail атаки

- Скрипт прочита адресната книга и се изпращат копия с него до всеки мейл в нея

DHCP spoofing атаки



Когато фалшив DHCP сървър е свързан към мрежата и предоставя фалшиви IP конфигурационни параметри на легитимни клиенти.

Проблеми

- **Wrong default gateway**
  - предоставя невалиден GW или IP адреса на своя хост, за да създаде man-in-the-middle атака. Това може да остане неоткрито.
- **Wrong DNS server -**
  - предоставя неправилен адрес на DNS сървър, насочващ потребителя към злонамерен уебсайт.
- **Wrong IP address**
  - предоставя невалиден IP адрес, невалиден IP адрес на GW или и двете. След това атакуващият създава DoS атака срещу DHCP клиента.

Видове атаки- BUFFER OVERFLOWS

- Цел:
  - Насочена към интегритета и достъпността на информацията
  - Обект е системният и приложен софтуер
  - Уязвимост- софтуерът не е добре проектиран и/или внедрен
- Начин на действие
  - Към атакуваното системно или програмно приложение се изпращат по-голямо количество данни, отколкото може да поддържа или данните са различни по същност и формат от тези, за които е проектирано.
- Противодействие
  - Средства за допълнително ограничаване на привилегиите.

Видове атаки- DENIAL OF SERVICE (1)

- Цел:
  - Насочена към достъпността на информацията
  - Обект са линиите за обмен на данни
  - Уязвимост- транспортните протоколи
- Начин на действие
  - TCP DoS - Атакуващият последователно започва процедури за установяване на връзка с атакувания елемент през по-малки интервали от време, от колкото е установено SYN timeout, но не ги завършва.
  - UDP DoS -Атакуващият изпраща UDP пакети, чието количество е по-голямо от максималния брой пакети, които системата може да обработи.
  - DDoS – botnet, zombie

Видове атаки- DENIAL OF SERVICE (2)

Наблюдава се:

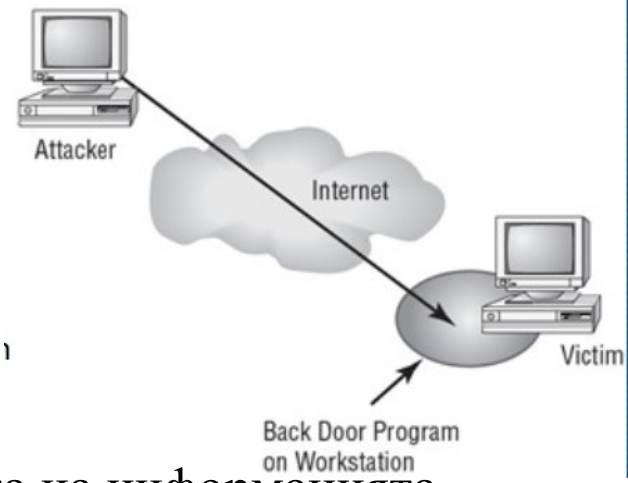
- TCP flag rate
  - 'F‘ – когато е SYN, FIN, RST, ACK, PSH, URG, NULL – броя на пакетите със специфичен флаг към броя на всички пакети.
- Protocol rate
  - брой пакети от TCP, UDP, ICMP към общия брой IP пакети
- Броя на HTTP requests в TCP сесия
  - R/C: Requests per connection
- Броя на едновременно установените TCP сесии
  - SC: Simultaneous Connection

Видове атаки- DENIAL OF SERVICE (3)

Противодействие:

- Надежден контрол на всички потребители на системата
- Филтри за пакети
- Динамични буфери
- Динамичен SYN timeout

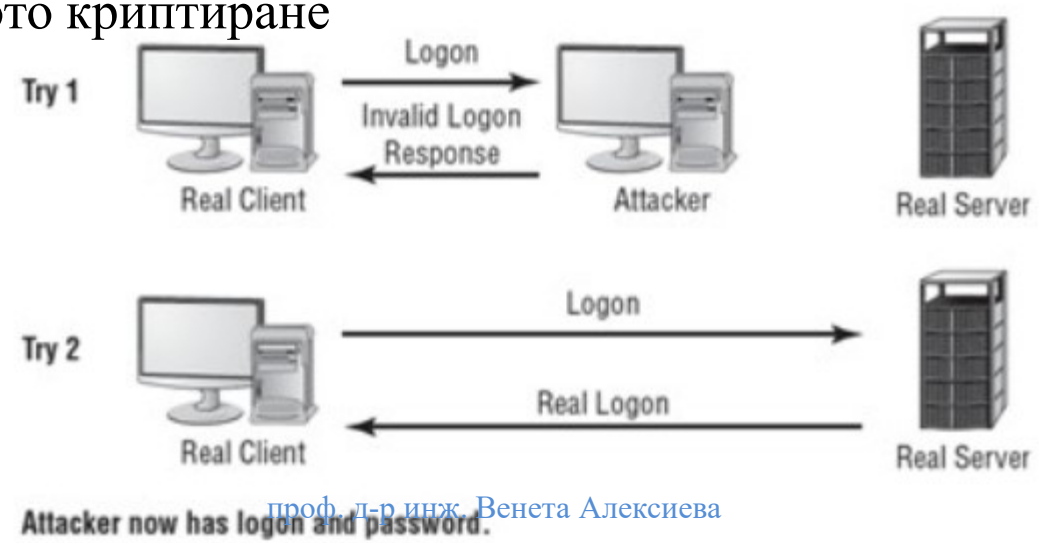
Видове атаки- BACK DOOR



- Цел:
  - Насочена към конфидециалността и интегритета на информацията
  - Обект са операционните системи
  - Уязвимост- системите от портове на операционните системи
- Начин на действие
  - Инсталиране и използване в по-късен момент на нерегламентиран софтуер, позволяващ нерегламентиран достъп.
  - Атакуващият управлява BD софтуера през неконтролиран порт на операционната система и BD му осигурява достъп през същия порт
- Противодействие
  - За откриване се използват антивирусни софтуери с дефиниции за BD и защитни стени с възможност за наблюдение на неизползваните портове на операционните системи
  - Противодейства се като се преинсталира операционната система

Видове атаки- SPOOFING

- Цел:
  - Насочена към интегритета на информацията
  - Обект са протоколите от второ, трето и седмо ниво на OSI модела
  - Уязвимост- адресацията
- Начин на действие
  - Атакуващият прибавя данните на легитимен за мрежата потребител към информацията, която изпраща и заблуждава получателя
- Противодействие
  - Средства за автентикация, базирани на метода на симетрично и асиметричното криптиране

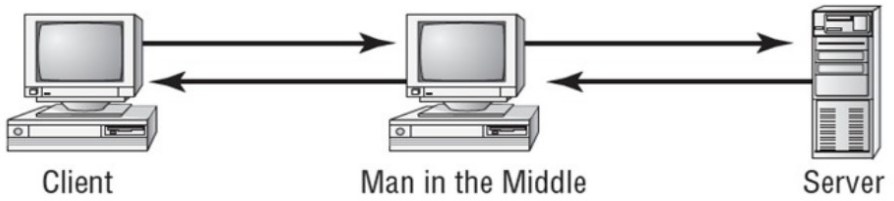


Видове атаки- SNIFFING

- Цел:
  - Насочена към конфиденциалността на информацията
  - Обект са стандартните мрежови протоколи
  - Уязвимост- незащитено предаване на информация чрез мрежови протоколи
- Начин на действие
  - Провежда се с помощта на софтуерни пакети, известни като “sniffing tool” и в се състои в четене на пакети, които не са адресирани до атакуващия
- Противодействие
  - Използване на мрежови протоколи, поддържащи криптиране на информацията

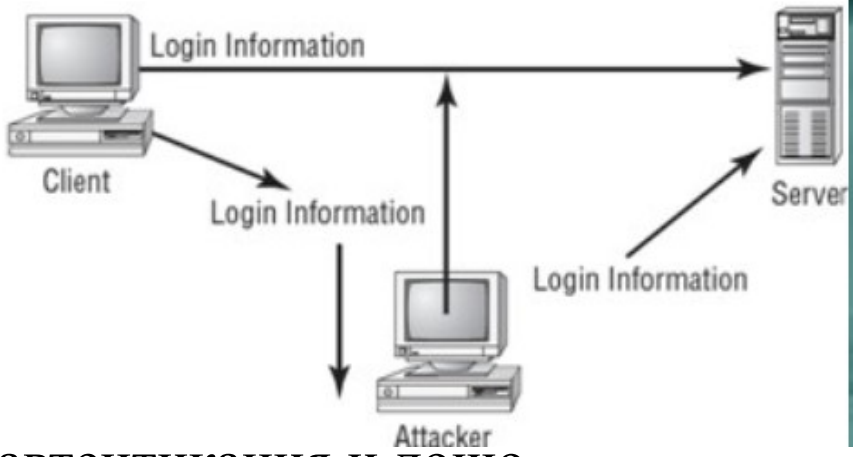
Видове атаки- MAN IN THE MIDDLE

- Цел:
  - Насочена към конфиденциалността и интегритета на информацията
  - Обект е мрежова среда проектирана и изградена с една или повече отдалечени части
  - Уязвимост- автентикация



- Начин на действие
  - Атакуващият се намира физически или логически между отдалечени части на АИС и имитира функционалността на определена отдалечена част
- Противодействие
  - Изпозване на криптографски метод за автентикация и еднократни пароли

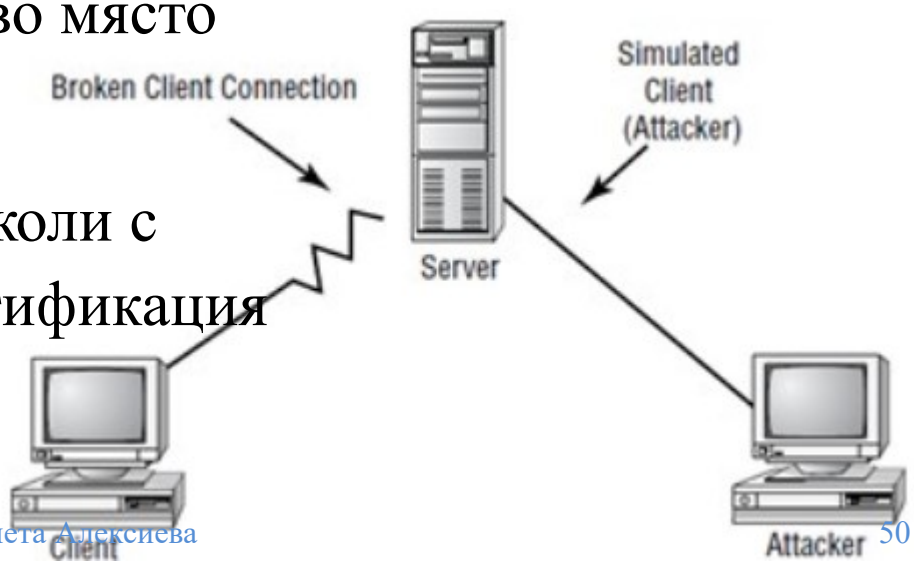
Видове атаки- REPLAY



- Цел:
  - Насочена към конфиденциалността и интегритета на информацията
  - Обект е автентикационната сесия
  - Уязвимост- простите механизми за автентикация и лошо проектираните криптографски протоколи
- Начин на действие
  - Атаката се провежда като се използва повторно автентикационна информация придобита нерегламентирано от валидна автентикационна сесия
- Противодействие
  - Внедряване на надеждни механизми за защита на линиите и употребата на еднократни пароли

Видове атаки- HIJACKING

- Цел:
  - Насочена към конфиденциалността и интегритета на информацията
  - Обект е логическата връзка в TCP/IP мрежите
  - Уязвимост- незащитеният TCP протокол
- Начин на действие
  - Провежда се като се разкачи единия от потребителите и атакуващия се закачи на негово място
- Противодействие
  - Използват се защитени протоколи с надеждна криптографска автентификация и защита на интегритета



Видове атаки- КРИПТОГРАФСКА

- Цел:
  - Насочена към конфиденциалността и интегритета на информацията
  - Обект са криптографските алгоритми или системи
  - Уязвимост- дизайнът и/или внедряването на криптографските алгоритми или системи
- Начин на действие
  - Провежда се със специален софтуер, който опитва да декриптира информацията
- Противодействие
  - Използват се публично достъпни стандарти и тествани алгоритми, които се внедряват коректно

Видове атаки- BRUTE FORCE

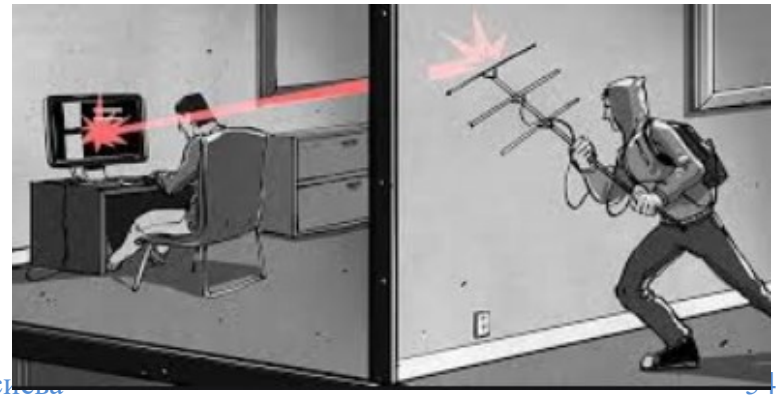
- Цел:
  - Насочена към конфиденциалността и интегритета на информацията
  - Обект са паролите и крипто-ключовете
  - Уязвимост- крайният възможен брой комбинации за пароли и крипто-ключове
- Начин на действие
  - Атаката се състои в последователното пробване на всичките възможни комбинации за паролата или ключа
- Противодействие
  - механизми, които следят броя на неуспешно въведените пароли
  - използва се крипто-ключ, чието средното време за изчисляване е по-малко от времето на актуалност на информацията. Смяната на ключа става през интервал от време също по малък от времето на актуалност на информацията.
  - наблюдение и контрол на вече криптираната информация

Видове атаки- DICTIONARY

- Цел:
  - насочена към конфиденциалността и интегритета на информацията
  - Обект са паролите
  - Уязвимост- логическия избор на пароли
- Начин на действие
  - Атакуващият използва списък (речник) за да открие паролата
- Противодействие
  - Предоставяне на ограничен брой опити за автентикация

Видове атаки- TEMPEST

- Цел:
  - Насочена към конфиденциалността на информацията
  - Обект са работните станции на АИС, активното оборудване и структурната кабелна система на мрежите
  - Уязвимост- електромагнитното излъчване
- Начин на действие
  - С помощта на специализирано оборудване се прихващат и реконструират видео изображения от мониторите, въвеждани символи от клавиатурата и предавана по мрежата информация
- Противодействие
  - Физически се контролира района, в който се разполагат;
  - Разполагат се в екранирани помещения;
  - Използва се Tempest оборудване (оборудване с намалено излъчване);
  - Заглушава се излъчването



Видове атаки- СОЦИАЛЕН ИНЖЕНЕРИНГ

- Цел:
  - Насочена към конфиденциалността на системната информация
  - Обект са служителите
  - Уязвимост- възможността хората да бъдат измамени
- Начин на действие

  Основните подходи при провеждането са:
  - просто питане
  - фалшивата помощ
  - фалшиви сайтове и опасни приложения
- Противодействие
  - въвеждане на строги правила за работа със системната информация
  - извършване на обучение и контрол на служителите.

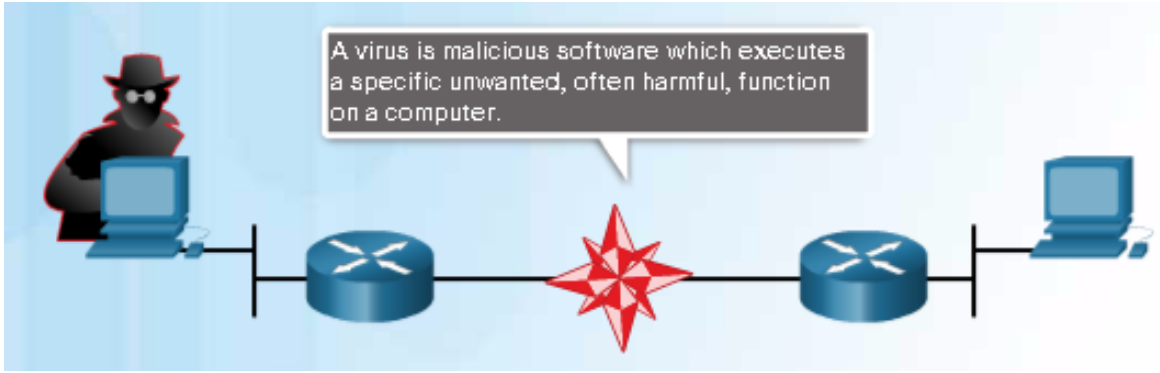
Злонамерен софтуер-Вируси

- Злонамерен софтуер, който може да “инфектира” други програми като ги модифицира.
- 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.

Злонамерен софтуер-Вируси

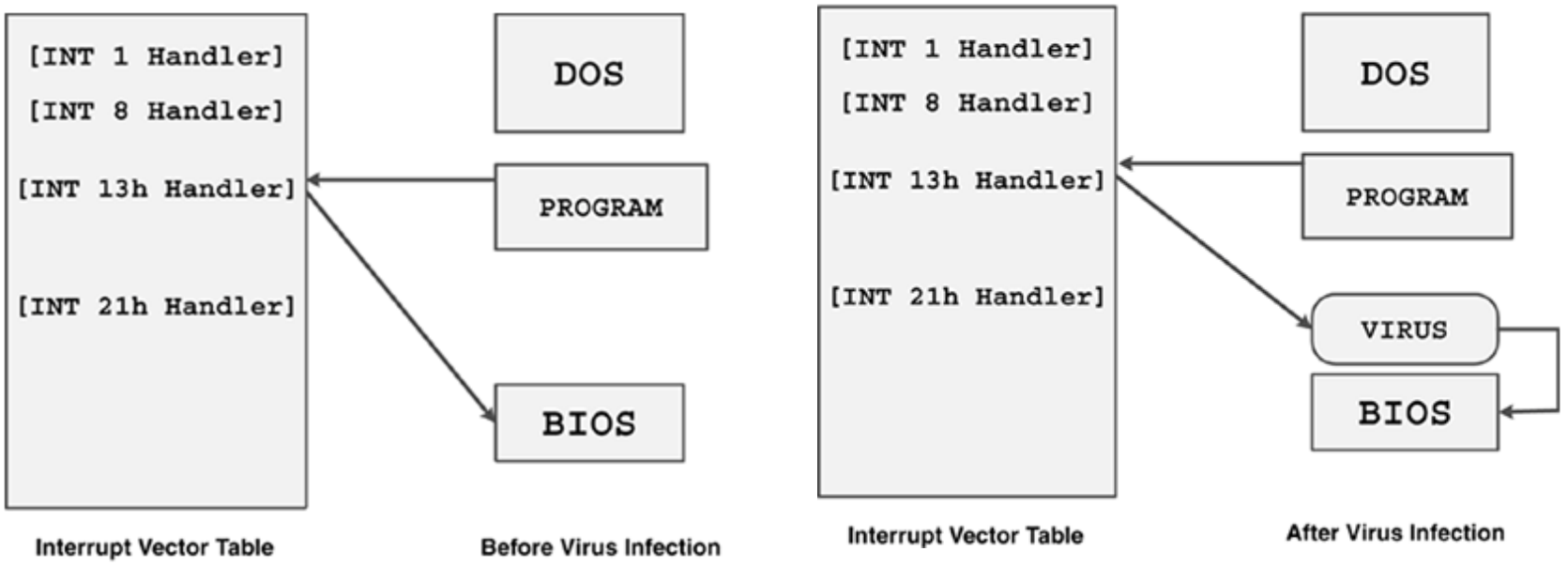
Видове:

- Boot sector вируси;
- Compressed вируси;
- Stealth вируси;
- Polymorphic/Self-garbling вируси;
- Multipart вируси;
- Macro вируси.



Boot sector вируси

- Некоректното маркиране в boot таблицата на сектори от паметта, като лоши.
- Резултатът:
  - Невъзможност за стартиране на програмни приложения и работа с информацията, когато пакетите им са разположени в маркирани като лоши сегменти.
  - Невъзможност за ефективно използване на паметта.

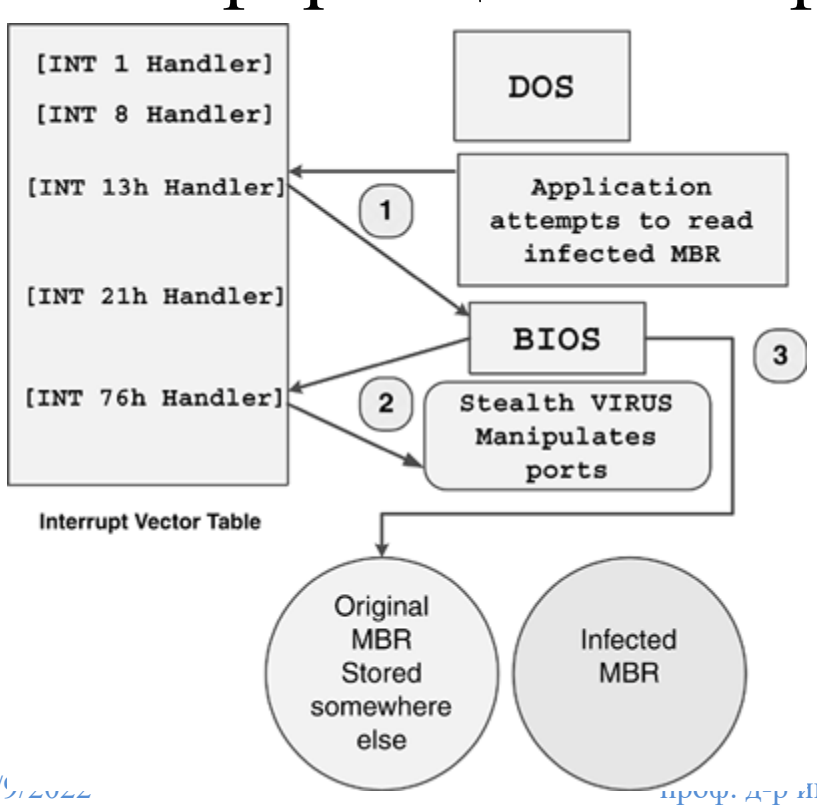


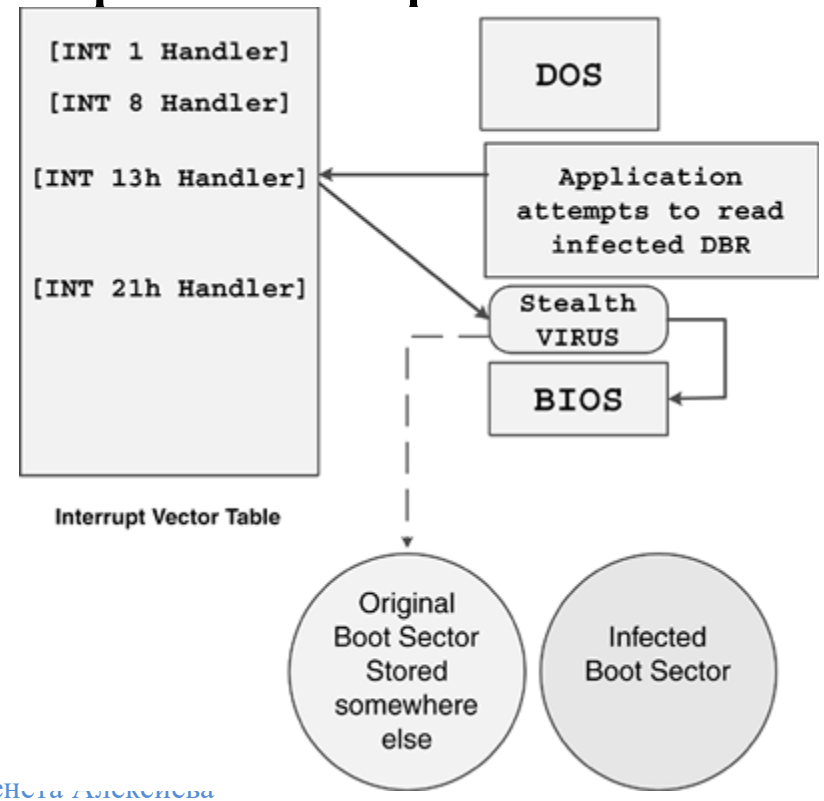
Compressed вируси

- Технологията на действие на вируса се състои в декомпресирането и изпълнението му преди всяко изпълнение на инфектираното приложение.

Stealth вируси

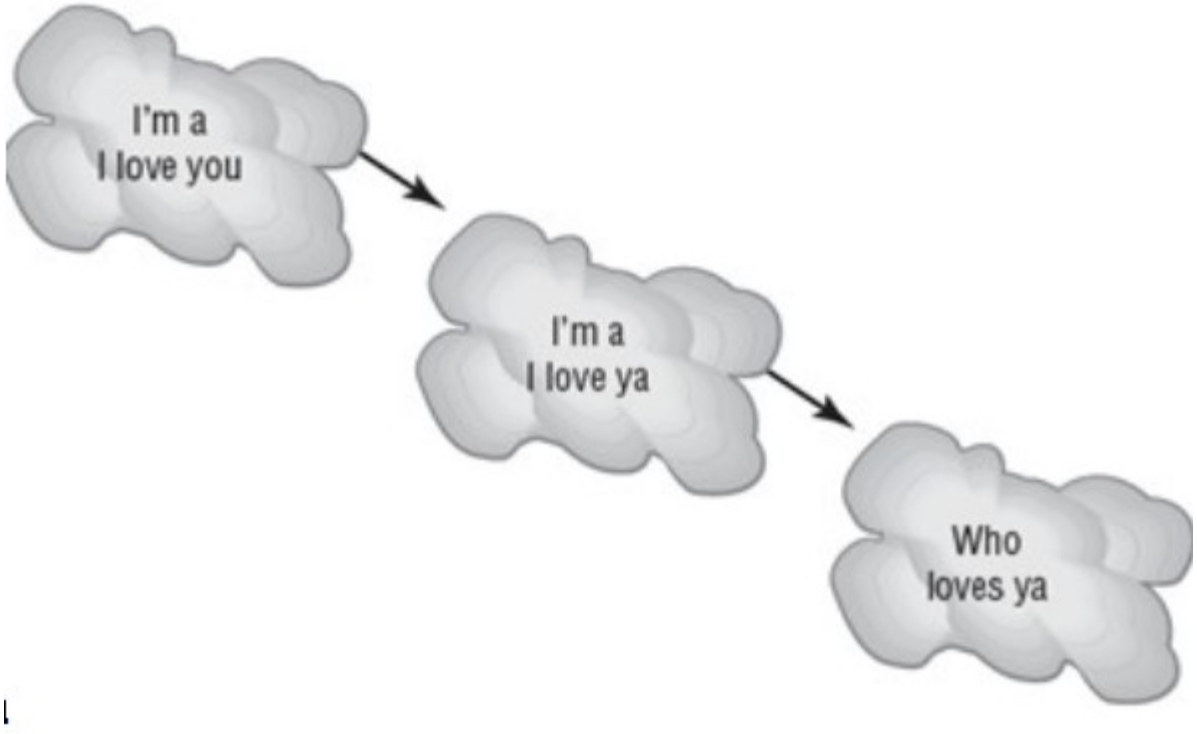
- Технологията на работата им се състои в представянето пред потребителя или антивирусния софтуер на фалшива информация за инфектираните приложения.





Polymorphic/Self-garbling вируси

- Произвеждат различни, но с еднакво предназначение копия, което прави откриването им и дезинфекцията 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

Подходи за откриване на вируси

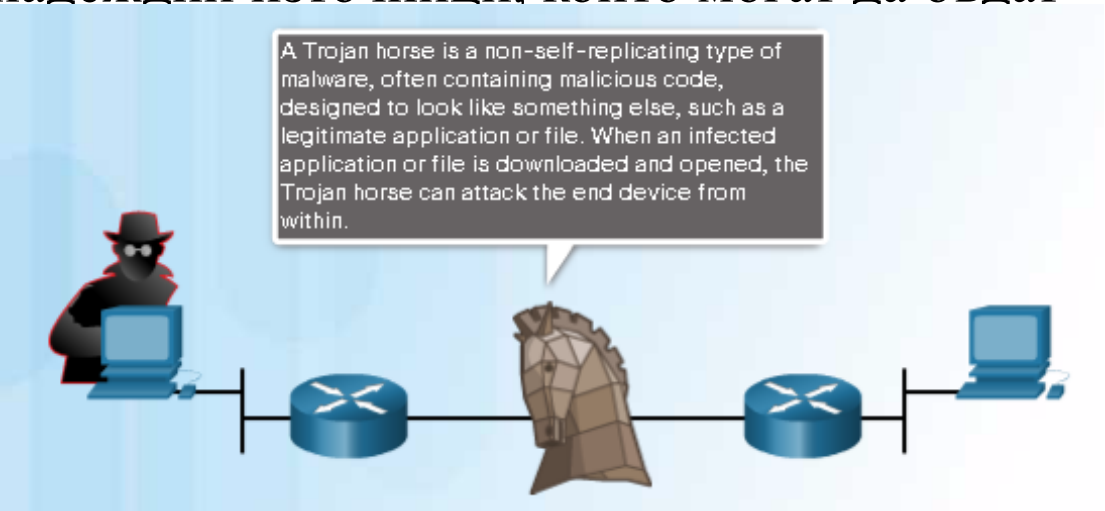
Антивирусните инструменти използват три основни подхода за откриване на вируси:

- Дефинитивен;
- Евристичен;
- Хибриден.

Злонамерен софтуер-Троянски коне

Троянските коне са злонамерен софтуер, който има някаква официална полезна функционалност, но в чиито код има прикрит злонамерен код.

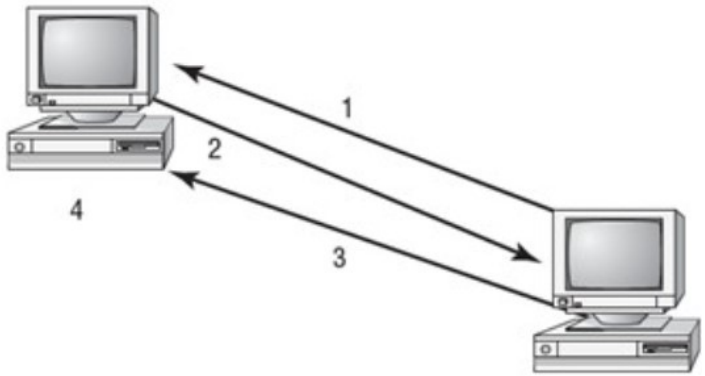
- **Начин на действие**
  - Когато се стартира троянски кон, за да използва полезната му функция се изпълнява и другата му прикрита и нерегламентирана функционалност
- **Противодействие**
  - Да се ползва софтуер от надеждни източници, които могат да бъдат проверени



Злонамерен софтуер - Логически бомби

Логически бомби се вграждат в кода на функционалните програмни приложения по време на разработката от разработчика.

- **Начин на действие**
  - Логическите бомби изпълняват нерегламентирани действия при настъпване на някакво събитие: настъпване на дата, определен изчислителен резултат и/или др.
- **Противодействие**
  - Да се ползва лицензиран приложен софтуер от проверен източник

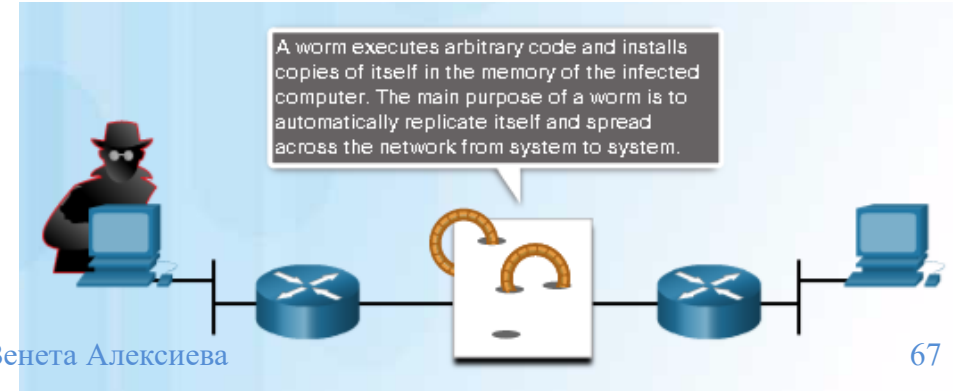


1. Attacker implants logic bomb.
2. Victim reports installation.
3. Attacker sends attack message.
4. Victim does as logic bomb indicates.

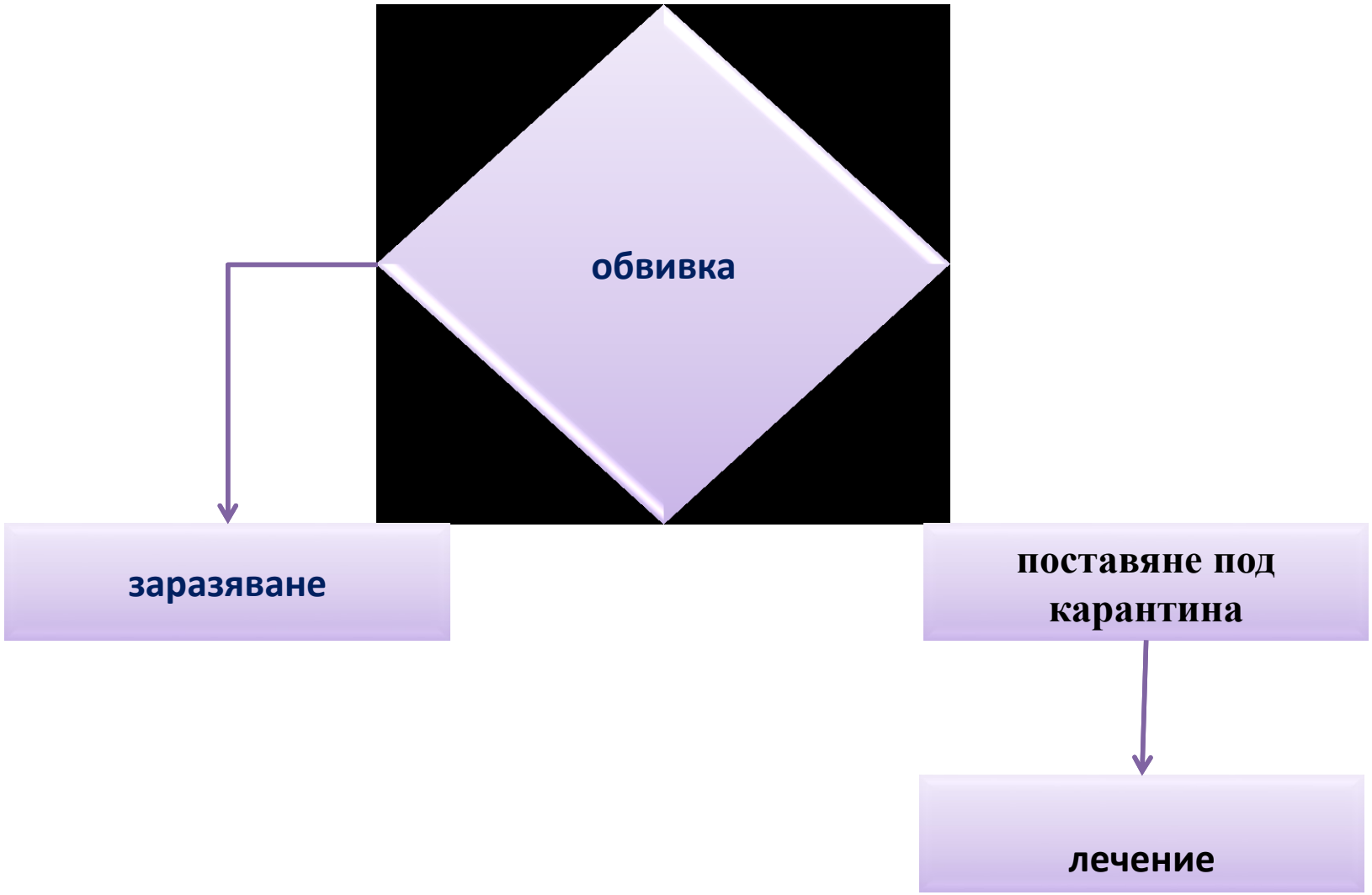
Злонамерен софтуер- Червеи

Червеят е самостоятелен злонамерен програмен код. Обикновено целта на червея не са приложенията, а управляваните от ОС ресурси на компютъра

- **Начин на действие:**
  - За да действа не му е необходимо да използва програмно приложение както правят троянските коне, логическите бомби и някой вируси.
- **Противодействие:**
  - Антивирусен софтуер



Противодействие на червеи



Злонамерен софтуер- Хибридни форми

- Притежават характеристиките на два или повече видове злонамерен програмен код

Въпроси ?

Благодаря за вниманието !