Тема 19. Заплахи за мрежовата сигурност

Външни заплахи
- Неоторизиран достъп чрез пароли и ключове
- Софтуер за мрежово следене
- ARP Positioning
- IP Spoofing
- DNS Spoofing
- DoS (Denial of Service) атаки
- TCP kill
- TCP nice
- SYN flood
- UDP flood attack
- ICMP flood
- Компютърни вируси и червеи
- Троянски коне

Вътрешни заплахи
- Корпоративен шпионаж
- Вътрешни политики
- Недоволни служители
- Случайни пробиви

Въпроси

Външни заплахи

В една локална мрежа, която не е свързана към Интернет, този вид заплахи не са сериозен проблем. Единственият вариант за включване на външен потребител към мрежата е да се прикачи с кабел към мрежата или да се включи с помощта на модем. Но днес, когато почти всяка локална мрежа има достъп до Интернет, външните заплахи са основен проблем за мрежовата сигурност. Вариантите за проникване в една система могат да бъдат различни – неоторизиран достъп, DOS атаки, компютърни вируси, троянски коне и др.

Под неоторизиран достъп се разбира неразрешен достъп до данните в една компютърна система.

Неоторизиран достъп чрез пароли и ключове

Паролите и ключовете се използват за предпазване на данните в една компютърна система от външно посегателство. ***Паролата*** представлява комбинация от букви, цифри и други специални символи. Тя дава оторизирано право за достъп на съответния потребител до компютърната система. ***Ключът*** е число или шифър и се използва за проверка на валидността на комуникацията.

Паролите и ключовете трябва да се пазят в тайна. Придобиването на паролата от друг човек създава възможност за неоторизиран достъп до вашата система. Проникването в друга система, без знанието на нейния собственик обикновено се нарича ***хакване***, а хората извършили това деяние се наричат ***хакери***.

Не е желателно използването на кратки пароли, както и пароли с имена на близки хора, домашни любимци, рождени дати, коли и телефонни номера. Дори и когато паролите са сложни, не е желателно използването на значеща дума. Съществува софтуер за „разбиване” на пароли, който използва файлове с речници.

Най-добрата парола е тази която съдържа незначещи думи, с комбинация от букви, цифри и специални символи. Желателно е тя да не бъде по-малка от 8 символа.

Софтуер за мрежово следене

Чрез този софтуер може да се осъществи атака само в рамките на локалната мрежа. Софтуерът за мрежово подслушване (sniffing) може да прихване всеки пакет, предаван по мрежата.

ARP Positioning

Атаката променя маршрута на мрежовия трафик, така че той да преминава през атакуващата машина. Атакуващата машина изпраща фалшиви (spoofed) ARP пакети към машината жертва и към нейния gateway. Принуждава целия интернет трафик на жертвата да преминава през атакуващия компютър.

IP Spoofing

IP спуфинг е метод за маскиране на едно устройство като друго. Реализира се чрез промяна в хедъра на пакетите на изпращащия компютър. IP адресът на изпращащия компютър се подменя с друг IP адрес. По този начин съобщенията от гледна точка на компютъра получател изглеждат така, сякаш са изпратени от компютър с друг IP адрес. IP спуфингът може да бъде използван за неотозизиран достъп, за кражба на данни и др.

DNS Spoofing

В резултат от IP спуфинг атака, атакуващият компютър се представя за DNS сървър на компютъра-жертва. Когато жертвата подаде заявка за намиране на IP адрес по име, примерно при отваряне на web сайт, атакуващият компютър прихваща заявката и връща собствения си IP адрес. Потребителят на компютъра-жертва се доверява на сайта-източник, без да подозира, че е подменен използва неговото съдържание.

DoS (Denial of Service) атаки

DoS атаките (т.е. атаки от типа „Отказ на услуга") са опит даден ресурс, предоставян от компютър (наричан жертва), да бъде направен недостъпен за целевите му потребители. Обикновено жертви на такива атаки стават популярни уеб сървъри, като целта е те да станат недостъпни за Интернет-потребителите. Това действие се класифицира като компютърно престъпление, нарушаващо Етиката в Интернет. Първата значима DoS атака беше червеят Morris (Ноември 1988 г.), откъснал около 5000 машини за няколко часа. Това бяха компютри на академични и изследователски центрове. По-късно други по-големи атаки бяха насочени към сървъри като Yahoo, eBay, Buy.com, CNN.com и др.

DoS атаките не влияят върху работата на съответния компютър, но прекъсват връзката на останалите потребители в мрежата към този компютър. Те работят като пращат в мрежата ненужни пакети или емулират мрежов проблем, при което компютърът жертва прекъсва връзката с мрежата.

DoS атаките имат много разновидности. Най-популярните в момента са:

TCP kill

Атаката използва механизма за изграждане на TCP сесии. В резултат от IP спуфинг атака, атакуващият знае TCP sequence номерата (поредните номера на сегментите) на отворена сесия на компютъра-жертва. Той генерира RST (reset) сегмент, с подменен IP адрес и правилен TCP sequence номер, в резултат на което прекратява връзката. Атаката прекратява съществуващите TCP сесии и не позволява отварянето на нови – прекратява интернет достъпа до машината-жертва.

TCP nice

Използва механизма за управление на TCP сесиите. В резултат от IP спуфинг (ARP Positioning) атака, атакуващият знае TCP sequence номерата на отворена сесия на компютъра-жертва. Той генерира сегмент, с подменен IP адрес, правилен TCP sequence номер, като подава информация за намаляване размера на прозореца (TCP Window Size). Друг подход е изпращане на фалшифициран ICMP пакет, който уведомява за намаляване

на MTU размера на пакети. В резултат на това TCP връзката се конфигурира грешно и се забавя.

SYN flood

Използва механизма за създаване на TCP сесии. (Механизмът е описан в Тема 16.) Атакуващата машина изпраща SYN сегменти с несъществуващи IP адреси. Операционната система добавя заявката в опашка и чака завършване на тристранното TCP договаряне. Опашката се препълва с чакащи връзки. Това прави невъзможно приемането на нови TCP сесии.

UDP flood attack

Това е DoS атака използваща UDP протокола. Атакуващият изпраща на компютъра-жертва UDP дейтаграми със случайни номера на портове. Поради липса на приложение, което да слуша (listen) порта, компютърът-жертва отговаря с ICMP съобщение „Назначението е недостъпно" (Destination Unreachable). Поради големият брой на UDP пакетите, компютърът-жертва изпраща голям брой ICMP съобщения, което го претоварва с трафик.

ICMP flood

Това е DoS атака използваща ICMP протокола. Изпращат се фалшифицирани ICMP пакети до броадкастни адреси (до голям брой хостове), съдържащи IP адрес на изпращача = адреса на компютъра-жертва. В резултат се генерират голям брой ICMP отговори, които претоварват компютъра-жертва с трафик.

Компютърни вируси и червеи

Компютърният вирус *е паразитна програма, която има способността да се самовъзпроизвежда и е създадена с цел да унищожи друга програма или файлове с данни.* Компютърният вирус не е самостоятелна програма. Той се свързва с програма – гостоприемник, като при нейното стартиране се стартира и вируса. При това големината на заразения файл се увеличава.

Действието на вирусите може да бъде различно. Някои от вирусите са по-безобидни – тяхното действие се свежда до извеждане на съобщения на екрана на компютъра. Съществуват и вируси, които са доста по-злонамерени – те могат да повреждат, променят и изтриват файлове от компютърната система, така че компютърът да не може да бъде стартиран. Известният вирус Чернобил изтрива съдържанието на EEPROM FLASH BIOS паметта, с което го уврежда.

Вирусите се класифицират по видове и към настоящия момент съществуват около 30 вида. Най-често срещаните от тях са:

- ***BOOT-секторни*** – вируси, заразяващи сектора за първоначално зареждане (boot record);
- ***BIOS - вируси***, заразяващи входно-изходната система на компютъра;
- ***Файлови - вируси***, заразяващи всички активни програмни файлове (*.COM, *.EXE, *.OVR, *.BIN, *.SYS);
- ***Стелт*** – те не променят размера на заразения файл. Секторите, които заразяват се маркират като лоши, въпреки че не са повредени;
- ***Макровируси*** – заразяват файлове с документи, притежаващи макроси (*.DOC, *.DOT, *.RTF, *.XLS, *.XLT);
- ***E - Mail вируси*** – особено актуална категория вируси. Разпространяват се чрез електронна поща и използват адресната книга, за да нападат нови компютри;
- ***Java вируси*** – това са вируси, които могат да заразяват само Java програми. Стартират се от java applet в браузъра или като самостоятелно java приложение.

Начините за разпространение и заразяване с компютърни вируси са следните:

1) Чрез дискове и дискети:
   - при копиране на файлове от дисков носител;

- при инсталиране на пиратски софтуер;
- при опит за зареждане на операционната система от заразен boot сектор;

2) Чрез интернет достъп:
   - по електронна поща
   - при свързване с WEB сайтове.
   - при файлов трансфер от Интернет (download).
3) При използване на хардуер, съдържащ заразен системен firmware[1].

Компютърният червей (computer worm) е самовъзпроизвеждаща се компютърна програма. Той използва компютърната мрежа, за да изпраща свои копия до компютрите. За разлика от компютърния вирус за него не е необходима програма–гостоприемник. Компютърният червей е самостоятелна програма. Червеите почти винаги причиняват вреда на мрежата, тъй като консумират от нейната пропускателна способност.

Червеите се разпространяват, като използват пролуки в операционните системи. Някои от компютърните червеи се разпространяват на отделни части по мрежата. Първо пристига стартиращ модул (Starter) – малка програма изтегляща и реконструираща червея. При пристигането на всички части на червея се „сглобява" компютърната програма, след което тя може да бъде стартирана. Преминаването само на малки фрагменти от информация през входно-изходната система не позволяват на антивирусните програми да разпознаят червея. Много червеи са полиморфни. При сглобяването програмните сегменти се разбъркват случайно. Това ги прави много трудни за откриване.

Троянски коне

Троянските коне са програми, отварящи вратичка в сигурността на системата. Те дават неоторизиран достъп на атакуващия компютър, намиращ се в Интернет. Атакуващият може да вижда съдържанието на екрана, да стартира и спира приложения, да изтегля и изпраща файлове, да изтрива файлове, да форматира дискове, да спира или рестартира компютъра и т.н.

Троянският кон е .EXE файл и заразяването става винаги чрез стартирането му от потребителя. Троянският кон обикновено е програма от две части – *клиент* и *сървър*. При стартиране на програмата сървър се отварят един или повече порта на заразения компютър. Чрез клиентската програма злонамерен потребител може да получи отдалечен достъп до този компютър.

Съществуват програми – троянски коне, които се представят като други програми. Това може да бъде например прозорец за логване в системата. При въвеждането от потребителя на името и паролата, данните се предават по мрежата и съответно този, който е стартирал програмата-клиент от троянския кон може да получи достъп до системата.

Вътрешни заплахи

Въпреки немалкият брой на заплахите за мрежовата сигурност отвън, не са за пренебрегване и заплахите вътре в локалната мрежа на една организация или фирма. Вътрешните заплахи можем да класифицираме в следните групи:

- Корпоративен шпионаж
- Вътрешни политики
- Недоволни служители
- Случайни пробиви

Корпоративен шпионаж

Корпоративният шпионаж е най-интелигентният тип вътрешна заплаха за сигурността. Важна задача, която стои пред всяка фирма е опазването на търговските тайни свързани с бизнеса. Конкуренцията винаги се стреми да научи повече информация за другите фирми от този бизнес. Възможни са ситуации, когато се назначават на работа „чужди" служители в дадена фирма с цел получаване на достъп отвътре до фирмените тайни.

[1] firmware – програма вградена в хардуерно устройство, например DVD-firmware

Обикновено хората, които могат да осъществяват корпоративен шпионаж са едни от най-интелигентните служители с високи професионални умения. Затова и разкриването на този вид шпионаж е доста трудна задача, която стои пред всяка фирма.

Вътрешни политики

Заплаха за сигурността на данните в една локална мрежа могат да бъдат и действията на някои от служителите във фирмата, които искат да саботират работата на отделни свои колеги. Техните мотиви могат да бъдат различни – откриване на възможности за повишение в друга длъжност, увреждане на репутацията на хора от екипа и др.

Действията на тези хора не са насочени към сигурността на данните на компанията, но въпреки всичко те могат да създадат множество проблеми на фирмата. Извършителите на този вид престъпления обикновено не са висококвалифицирани специалисти. Затова и по-лесно могат да бъдат предприети действия за предотвратяване или тяхното разкриване.

Недоволни служители

Друг много сериозен вид заплаха за мрежовата сигурност могат да бъдат уволнени служители или такива, които не са доволни например от своето възнаграждение. Те обикновено предприемат действия, с които целят да навредят на компанията. Тъй като те имат достъп до системата могат да изтрият важни данни за фирмата, да прекъснат мрежовите комуникации и др.

Съществуват много случаи на уволнени служители, които преди да си тръгнат от фирмата сменят паролите за достъп до системата или стартират програми, които отварят „вратичка" в сигурността на системата.

Политиката на мрежова сигурност трябва да има предвид и този вид заплаха, като действията могат да бъдат насочени например, към своевременно изтриване на потребителските акаунти на уволнените служители.

Случайни пробиви

Случайни пробиви в системата могат да се получат от неопитни служители, които в стремежа си да извършат едно или друго действие на компютъра изтрият неволно важна фирмена информация. Операционните системи с файлова система NTFS създават възможност да се задават нива на сигурност. По този начин мрежовият администратор може да ограничи действията на отделните групи потребители.

Въпроси

1. Какво разбирате под понятието „неоторизиран достъп"?
2. Кои основни правила трябва да се имат предвид при задаване на парола за достъп?
3. Какво представляват DoS атаките и за кого могат да бъдат опасни?
4. Какви са вариантите за заразяване с компютърен вирус?
5. Какво е действието на троянските коне при компютрите?
6. Какви могат да бъдат заплахите за мрежовата сигурност вътре в една фирма?