СЕМИНАРСКА РАБОТА
ХАКЕРСКИ НАПАДИ

ПРЕДМЕТ
Е-Општество

Содржина

1.Историјат и развој на компјутерскиот криминал

За првпат зборот “hack” бил употребен во 1960 година во група за правење на модели на возови на МИТ, во врска со начинот на манипулирање со моделите на возови.

Во 1970 година почнало појавувањето на првите телефонски “криминалци” т.н. phreaks. Тие се занимвале со провала во телефонските централи од каде извршувале бесплатни повици. Најпознат од оваа категорија на криминалец (phreaker) е John Draper (*Captain Crunch*). Тој е креатор на “blue box” – електронска направа која произведува звуци со одредена бранова должина со кои може да се остваруваат бесплатени телефонски повици. Исто така во оваа категорија спаѓаат и **Steven Wozniak** и **Steve Jobs** (основачите на **Apple**), кои започнуваат сериско производство на вакви направи.

Во 1983 година е снимен филмот “War Games” кој претставува како инспирација за голем број луѓе низ целиот свет, да станат хакери. Истата година била фатена група со име “414” , која во рој од 9 дена, провалила над 60 компјутери меѓу кои спаѓале и компјутерите на “*Los Alamos National Labaratory*” – фирма која се занимавала со делови за нуклеарно вооружување.

1984 год. се појавува првиот хакерски магазин “2600”

1986 год. бил донесен првиот закон за компјутерски криминал кој бил со многу недостатоци за лица кои се компјутерски криминалци.

Во 1988 год. бил создаден првиот црв(**worm**). Креатор на овој црв бил **Robert T.Morris** кој бил студент на Cornell University и син на главниот научник во NSA (*National Security Agency*). Тој го тестира својот "црв" на ARPAnet и тој се проширил на 6000 компјутери. Тој добива 3 години условна казна и 10.000' парична казна.

Во 1990 год. операцијата "Sundevil" во 14 града низ САД, тајната служба врши апсење на членови од BBS (*Bulletin Board Systems).* Обвинението на членовите на BBS се: злоупотреба на телефони и телефонски системи, неовластено користење на кредитни картички и слично.

Во 1993 год. **Kevin Poulsen** (повеќе познат како ***Dark Dante***) провалува во телефонска централа во Los Angeles за да биде единствениот кој што ќе може да се јави во радио емисија каде што главната награда било: автомобил Порше и две патувања. За ова дело тој добива казна затвор 5 години.

Во 1995 год. била извршена голема компјутерска кражба вредна 10 милиони долари. Одговорноста за ова дело е на **Владимир Левин**, водач на руска хакерска група. Тој успева да "извлече" од CityBank 10 милиони долари и да ги префрли истите на сметки во Финска и Израел. Од 10-те милони долари, 400.000 долари никогаш не се пронајдени. За овој случај тој добива 3 години затвор.

1995 год. уште е запаметена по апсењето на **Кевин Митник,** еден од најдобрите хакери на сите времиња. Тој имаше безброј обвинението меѓу кои се: крадење на 20.000 кредитни картички, упад и неовластено користење на бројни компјутерски системи во USA, како на приватни фирми така и во државни институции. Заради ова тој 4 години во затвор ја чекал судската пресуда, а таа била: уште 4 години затвор. Во 2003 година Кевин Митник почнува да се занимава со компјутерска безбедност. Тој е основач на Defensive Thinking во Лос Анџелес, фирма која се занимава со компјутерска безбедност и денеска претставува еден од најпознатите експерти на тоа поле.

Во 2000 год. се случуваат најголемите DOS (Denial Of Service) напади. Притоа хакерите прават најголеми напади на: eBay, Yahoo, Amazon и други поголеми компании. Истата година хакери провалуваат во Microsoft мрежа и го крадат source code-от за најновите верзии на Windwos i Office. Исто така во 2001 година Microsoft станува жртва на DOS напади и блокирање на DNS адреси. Резултатот на тоа е: милиони луѓе немаат пристап до Microsoft сајтот 2 дена.

Во 2002 год. меѓу позначајните компјутерски криминали се смета делото на Британецот **Garry McKinnon** кој неавторизирано пристапува во компјутерската мрежа на NASA и во американската воена мрежа и причинува штета околу 900.000 долари.

Според статистиките за 2006 година на Институтот за компјутерска сигурност во САД, беше проценето дека просечната штета на компјутерска измама изнесува 150,000 американски долари, додека просечната штета од физички кражби изнесува 10,000 долари.Оваа статистика е објаснета со примерот дека сајбер криминалец ќе направи измама и ќе добие пристап до кредитни картички, има поголем пристап до средства отколку оној криминалец кој ќе украде прирачник. Хакерот кој ќе добие неовластен пристап до

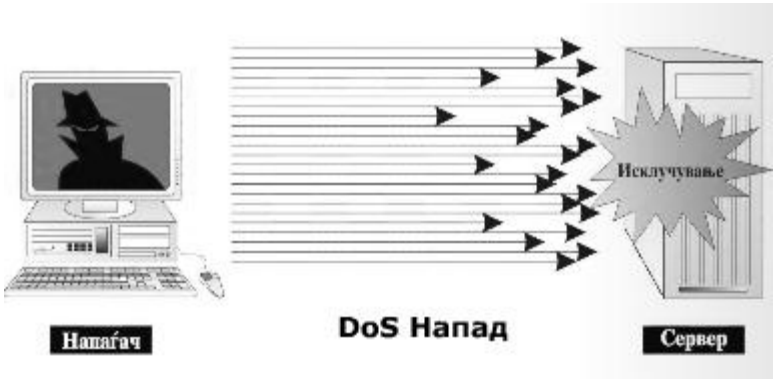
комерцијален веб сајт може да добие пристап до илјадници разни кредитни картички.

Сепак за скоро се постои превентива и секоја приказна има две страни. Во случајот на компјутерски криминал, со цел да се заштитиме од самите себе, но овој пат во дигиталниот свет, мораме да развиеме нови системи за превенција и детекција на сајбер криминални активности. Мора да се создадат специјални одреди кои ќе ги истражуваат нелегалните активности, но истите, заради проблемите со анонимноста и човечките права, наскоро се соочија со големи проблеми заради нарушување на приватноста – битка која сеуште се води.

Единствениот поголем прболем зошто превенцијата на сајбер криминалот не е толку ефективна е бидејќи детекцијата и заштита од истиот се навистина скапи.

2. DOS(Denial of Service) напади

DOS нападите се едни од најкористените хакерски стратегии. За разлика од вирусите,црвите и тројанците овие напади не извршуваат трајна штета (бришење на податоци од хард дискот, крадење на лозинки или броеви на кредитни картички) туку предизвикуваат оневозможување на работата на некој ресурс (на пр. некој сервер). Првите DOS напади се користеле со едноставни алатки кои генерираат и праќаат пакети од едно место до друго. Со текот на времето тие биле унапредувани да извршуваат напади од еден извор до повеќе цели, од повеќе извори на една цел или повеќе извори на повеќе цели. DOS нападите се извршуваат со користење на DOS алатки кои праќаат голем број на пакети преку интернет. Тие пакети ги преплавуваат (анг. flood) ресурсите на жртвата и на тој начин “жртвите” остануваат неискористени. Секој компјутер или било кој уред кој е споен на интернет и кој има мрежни услуги кои се темелат на TCP (Transmission Control Protocol) претставуваат потенцијални жртви.



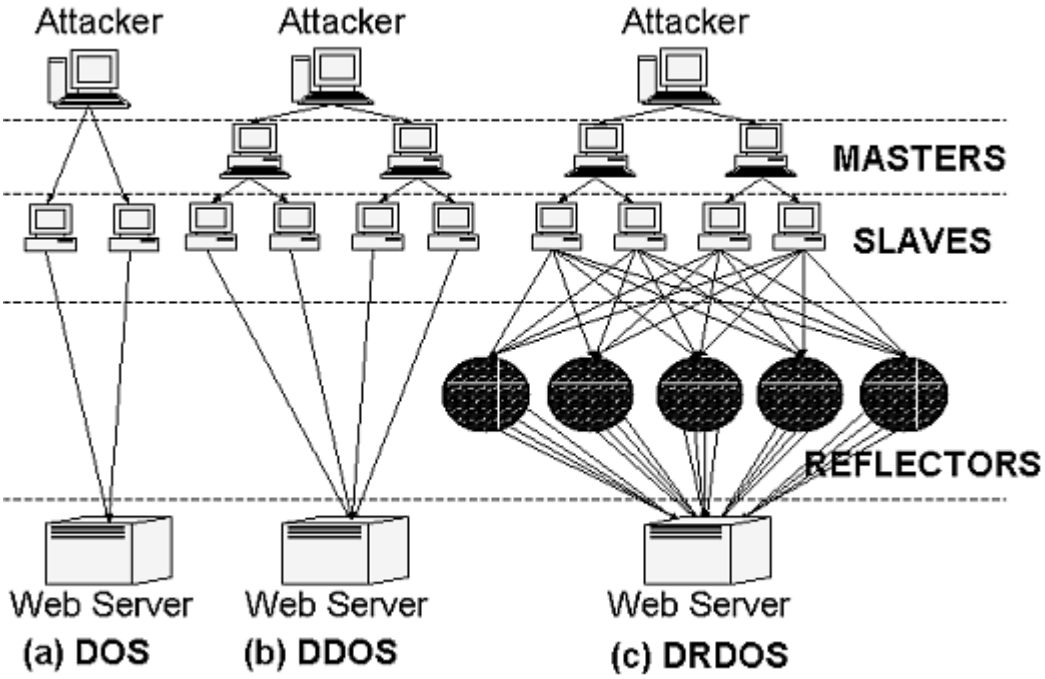
DOS нападите може да се поделат на софтверско искористување и поплавување (анг. flooding). Нападите со поплавување се засноваат на едно правило: тој што има најголем bandwidth победува. Напади со поплавување може да се поделат на напди со еден извор, напади со повеќе извори или напади со рефлексија.

Во нападите со еден извор постои еден напаѓач кој ја поплавува жртвата, додека во нападите со повеќе извори постојат повеќе напаѓачи. Во двата случаи може да се користат додатни zombie компјутери (zombie претставува компјутер кој е претходно заразен со искористување на некој сигурносен пропуст). Таков компјутер содржи скриена програма која овозможува далечинско управување на компјутерот.

Напади со рефлексија се специјални случаеви на напди од повеќе извори. Тие се користат за прикривање на идентитетот на вистинскиот напаѓач или за поголем напад. Рефлектор е било кој компјутер кој одговара на побарувањата. Било кој компјутер може да се користи како рефлектор со додавање на IP адресата на компјутерот-жртва во изворното поле на побарувањето. Со додавање на тие информации компјутерот – рефлектор ќе испрати одговор на жртвата наместо напаѓачот. Ако постојат многу компјутери – рефлектори резултатот на тоа ќе биде DoS напад. Разликата помеѓу zombie компјутер и компјутер-рефлектор е тоа што рефлекторите претставуваат легални корисници на интернет услугите. Заради тоа нападот со помош на рефлексија е многу тешко да се уништи.

Понапреден облик на DoS напад претставува DDoS (Distributed Denial of Service) при кој тројанец – напаѓач се инсталира на повеќе компјутери и така врши напади од повеќе локации во исто време. Овој напад претставува еден од најмоќните софтверски напади што досега воопшто е откриен. Со DDoS напади биле неколку пати дисконектирани и серверите на најголемите светски веб страници, како што се Yahoo, eBay, Amazon, CNN и многу други. Овој тип на напад е најнепредвидлив и затоа е многу тешко да се сопре ваков напад, бидејќи хакерите користат неколку стотина или многу повеќе претходно инфектирани компјутери кои ѓи имаат под своја контрола (zombie) и ја користат нивната моќ т.е. нивната интернет конекција напаѓајќи го на некој веб сервер или само обичен компјутер. Тие го прават тоа така што ја пингираат (ping) на жртвата од сите компјутери кои ги имаат под своја контрола во исто време. Тоа го прават со посебен софтвер кој ги контролира сите компјутерите кои ги имаат под своја контрола. Пингирањето на некоја жртва со толку голема интернет конекција ќе доведе до преоптоварување на капацитетот на мрежата (buffer

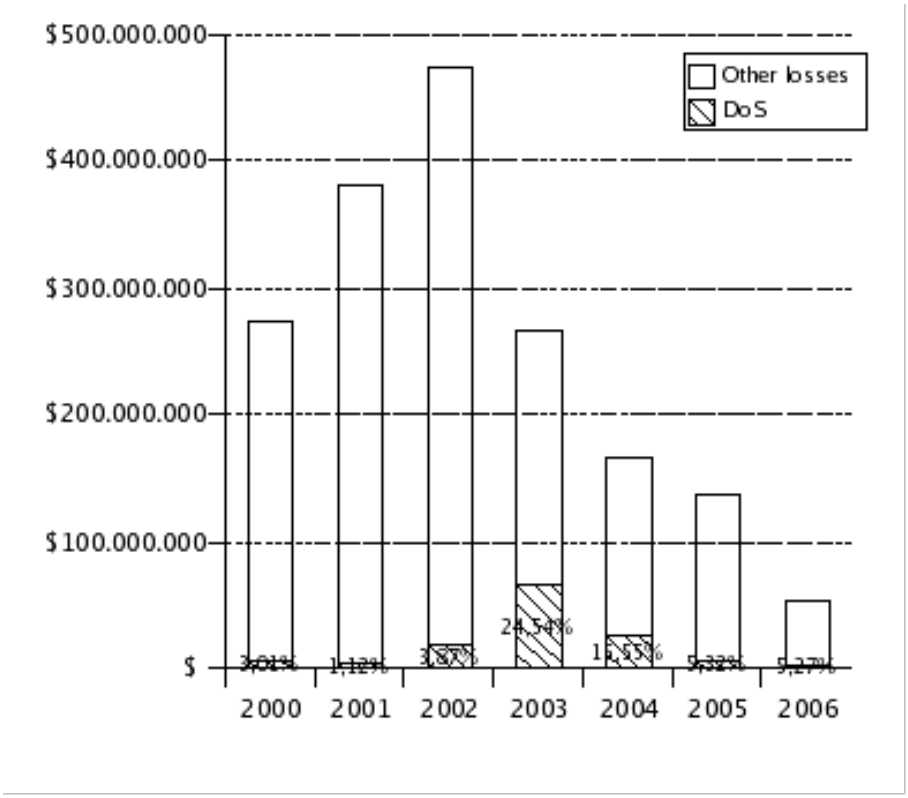
overflow) на конкретниот сервер или компјутер што е жртва на овој напад, по што се разбира ќе следи и пад на целиот систем. Една од мерките која ја користат големите компании за да се заштитат од ваков тип на напад е инсталација на специјализиран софтвер што го контролира протокот на податоци.Односно доколку една IP адреса побарува (request) многу повеќе податоци од лимитот кој е зададен, софтверот автоматски го прекинува протокот на податоци кон таа IP адреса се додека побарувањето на податоци од таа IP адреса не падне под нормалата.



На сликата се претставени три различни видови на DoS напади

Решение за овој проблем имаат најавено две компании од Бостон, САД кои самите компании се големи конкуренти на светскиот пазар. Тоа се Arbor Networks Inc. и Mazu Networks Inc. кои откриваат сосема нова тактика во борба против нападите т.е. спречување на нападите пред да дојдат до серверите. Тоа претставува начин нападите да се пресретнат порано односно на т.н. peering точки на интернетот, местото дека Интернет-провајдерските фирми се спојуваат со backbone-овите, односно на главните “магистрали” на светската мрежа. На тие точки ке се инсталираат уреди со посебен софтвер кој ќе може да прави разлика помеѓу вообичаен сообраќај и пакети со лажни побарувања. Нареден чекор подразбира лоцирање на напаѓачот, односно компјутерите од кои се упатени нападите и нивна изолација. На тој начин детектираните компјутери ќе бидат исклучени а нападот нема да стаса до својата цел.

На следниот график е прикажано споредба на штети предизвикани од DoS напади и останати штети во текот од 2000 до 2006 година во USA



Во текот на 2006 година е изгубено скоро 3 милиони долари заради DoS нападите. Исто така DoS нападите во 2006 година претставувале 5,27% од вкупните губитоци кои настанле заради повреда на сигурноста.

3.ВИРУСИ И ЦРВИ

Во компјутерската терминологија зборот вирус по дефиниција означува програма која самата се реплицира и шири копии од самата себе во некои извршни датотеки или документи.

Терминот “вирус” прв пат бил употребен во 1972 година во научно – фантастичната новела на Дејвид Џеролд “When H.A.R.L.I.E. Was One” која содржела опис на некоја програма која се нарекувала “вирус”. Компјутерскиот вирус функционира на сличен начин како и биолошкиот. Појавата при која се вметнува копија од вирусот во некоја програма се вика инфекција, а инфицираната датотека – домаќин (Host). Овде треба да се напомене дека во основа компјутерскиот вирус не може директно да оштети физички дел на компјутерот, туку само датотека (File).

Иако вирусите може да бидат многу деструктивни т.е. да уништи документи, поголемиот број вируси ја успоруваат работата на компјутерот или со саморазмножувањето ги преполнуваат ресурсите на компјутерот.

Некои вируси имаат одложено време на активирање кои се нарекуваат Bomb. На пример вирусот може да се активира на претходно одреден датум (Time Bomb) кога инфицира одреден број на домаќини или кога корисникот извршува некоја работа на компјутерот (Logic bomb).

Во обичниот говор терминот “вирус” се употребува да се заокружат сите групи на инфективни програми, а тие може да се поделат на четири групи:

1. Worm (Црв)
2. Trojan Horse (Тројанец)
3. Spyware (Програма за шпионирање)
4. Adaware (Програма за рекламирање)

3.1 Worm (Црв)

Станува збор за независна програма (или сет од програми) кои се во можност да ги множат своите оперативни делови на ист компјутер или на други компјутери користејќи веќе постоечка мрежа (преку Интернет или преку вмрежени компјутери). Под независна програма се подразбира да оваа група на виурс не е потребна програма – домаќин на кој ке се закачи. Според начинот на размножувањето постојат два типа на овој вирус:

1. Црв со еден домаќин
2. Мрежен црв

Првиот тип се одликува да кога се размножува на друг компјутер оригиналот го брише (така да постои само една копија кај вмрежените компјутери). Популарното име на овој тип на црв е Rabbit(зајак).

Мрежниот црв се состои од повеќе делови (segments), кај што секој дел функционира на друг компјутер во мрежата (неретко извршува различни функции). Една од функциите од сите делови е понатамошно размножување на друг компјутер. Мрежниот црв кој го содржи главниот сегмент т.е. кој ги контролира другите се нарекува Octopus (октопод). Постојат некои напредни техники за нивно бришење, а најчесто решение на овој проблем е преинсталација на системот.

3.2 Trojan Horse (Тројанец)

Името го има добиено по освојувањето на Троја и има за цел исклучиво да се “вовлече” на компјутерот и да отвори некоја порта (во компјутерска терминологија врата) низ која напаѓачот треба да пристапи до податоците на компјутерот. Овие вируси уште се нарекуваат и Back Door вируси. Во врска со бројот на портите (65.536) станува збор за многу голем број на комбинации.

3.3 Spyware (Програми за шпионирање)

Шпионските програми настојуваат, откако ќе влезат во компјутерот, да соберат сите можни шифри кои се чуваат на компјутерот. Тука се подразбира корисничко име и лозинка на компјутерот т.е. администраторот на системот и конекцијата на Интернет. Секако, ако можат да го извршат ова ќе може да

шпионираат било што на компјутерот. Постојат повеќе видови на софтвер кој служи за заштита од овој тип на вируси. Пр: Spyware Doctor, Microsoft AntiSpyware и сл.

3.4 Adaware (Рекламни вируси)

Advertising - рекламните вируси претставуваат еден тип на "досадни" вируси. Единствена работа на овие вируси е рекламирање на фирми и отвараат прозорци со реклами (pop-up) без одобрение на корисникот. Тие работат на тој начин кога се поврзува корисникот на Интернет собираат адреси од оние фирми кои најчесто даваат пари за ваков вид на огласување. Уште една особина што ја имаат овие вируси е тоа што ја менуваат почетната страница на Интернет пребарувачот. Оваа група на вируси не е деструктивна, туку само смета на нормалната работа на корисникот.

Хронолошки поглед на 10-те најопасни вируси на сите времиња

CIH или уште познат како **Чернобил (1998)**.

Проценета штета: 20 до 80 милиони долари, безброј уништени податоци

Овој вирус за прв пат е пуштен од Тајван 6 Јули, 1998 година и е еден од најопасните и најштетни вируси до сега. Вирусот ги ифицирал Windows 95, 98, и ME извршните фајлови и бил способен да остане во меморијата на компјутерот од каде продолжувал да заразува други извршни фајлови. Тоа што го прави овој вирус толку опасен е тоа што кратко после активацијата тој податоците во компјутерот ги правел веќе неупотребрливи. Исто така можел да го флешира биосот на заразениот компјутер правејќи го компјутерот веќе да не може да се бутира. Бидејќи ги инфицирал извршните фајлови тој можел лесно да се дистрибутира преку многу програми вклучувајќи ја и демо верзијата на играта Sin. CIH е познат и како Чернобил (анг. Chernobyl) бидејќи датата на неговата активација е иста со датата кога се случила нуклеарната катасртофа во Чернобил. Овој вирус денес не преставува сериозен проблем благодарејќи на компаниите кои се занимаваат со сигурноста на компјутери и широкораспространетоста на поновите оперативни системи имуни на овој вирус.

Melissa (1999)

Проценета штета: 300 до 600 милиони долари

На 26 март 1999 година за W97M/Melissa пишувало на насловните страници на сите весници во светот. Проценките укажувале дека овој вирус инфицирал околу 15 до 20 проценти од сите компјутери. Вирусот се разширил толку брзо така што големите компании како Intel, Microsoft и други кои користеле Outlook биле принудени да ги исклучат нивните маил сервери. Вирусот го користел Microsoft Outlook да се препрати на 50 имиња од контакт листата. Во Емаил

[1

пораките пишувало: “Here is that document you asked for…don’t show anyone else. ” и имало прикачен документ. Со отварањето на документот вирусот го инфицирал компјутерот и продолжувал со распространувањто. Со инфицирањето вирусот ги модифицирал документите на корисникот бришајќи го оригиналниот текст, а на негово место испишувал цитати од анимираната серја Симпсонови.

I LOVE YOU (2000)

Проценета штета: 10 до 15 милјарди долари

Познат уште и како Loveletter односно љубовно писмо и The Love Bug (љубовната бубачка). Тоа било скрипта направена во Visual Basic со паметно направена и привлечителна мамка: ветување за љубов. На 3-ти Мај 2000 година, црвот ILOVEYOU најпрво бил забележан во Хонконг. Тој бил пренесен преку е-маил со наслов на пораката “ILOVEYOU” и прикачен фајл Love-Letter-For-You.TXT.vbs. Слично на Melissa, вирусот сам се препраќал на сите контакти во кој ги имал корисникот во Microsoft Outlook. Илјадници корисници паднале на мамката на љубовното писмо отварајќи го инфицираниот фајл. Вирусот ги презапишувал музичките фајлови, сликите и други фајлови со копија од него, а исто така и пребарувал низ компјутерот за лични податоци на корисникот како и лозинки и ги препраќал по пошта на авторот на вирусот. Интересно е да се напомене дека авторот на вирусот е од Филипините но поради тоа што во тоа време немало закон за пишувањето на вируси авторот на вирусот не е обвинет за никакво криминално дело.

Code Red (2001)

Проценета штета: 2.6 милјарди долари

Code Red бил компјутерски црв пуштен низ мрежата на 13 Јули 2002 година. Тој ги напаѓал компјутерите кои имале стратувано Microsoft’s Internet Information Server (IIS) веб сервер. Уште познат и како Bady, Code Red бил дизајниран да направи максимална штета. Веднаш по инфекцијата веб сајтовите кои биле хостирани на заразен IIS ја прикажувале пораката “HELLO! Welcome to http://www.worm.com! Hacked By Chinese!“. Тогаш вирусот гледал за други ранливи сервери и ги инфицирал и нив. Тоа се случувало приближно 20 денови и тогаш сите заразени компјутери правеле DoS (denial of service) напади на одредени ИП адреси вклучувајќи го и серверот на Белата Куќа. За помалку од една недела овој вирус инфицирал скоро 400,000 сервери, а проценките за вкупниот број на инфицирани компјутери било околу 1 милион

SQL Slammer (2003)

Проценета штета: Бидејќи SQL Slammer бил пуштен во сабота, штетата направена од него била мала. Како и да е тој заразил 500,000 сервери низ светот всушност го исклучил мрежниот капацитет на Јужна Кореја за 12 часови. SQL Slammer познат и како Sapphire бил пуштен на 25 Јануари 2003 година. Тоа бил црв кој имал забележлив негативен удар врз светскиот интернет

трафик. Вирусот бил 376 бајти и рандом генерирал IP адреси и се препраќал на нив. Ако IP адресата била на компјутер без последните сигурносни надградби за Microsoft's SQL Server Desktop Engine, компјутерот веднаш почнувал со распространување на вирусот на рандом генерирани ИП адреси. Со овој начин на рспространување вирусот заразил 75,000 компјутери само за 10 минути.

Blaster (2003)

Проценета штета: 2 до 10 милјарди долари стотици илјади заразени компјутери

Во летото 2003 година IT професионалци биле сведоци на пуштањето на црвите Blaster и Sobig. Blaster, познат уште и како Lovsan или MSBlast бил прв на удар. Вирусот бил забележан на 11 Август и брзо се расширил достигајќи го врвот само за 2 дена. Пренесувајќи се преку мрежата и Интернет сообраќајот овој црв ја искористил ранливоста на Windows 2000 и Windows XP оперативните системи. Кога се активирал на корисникот му покажувал заканувачки диалог прозорец најавувајќи дека гасењето на системот е неминовно. Скриен во кодот на MSBLAST.EXE (извршниот фајл на вирусот) била сместена пораките. "I just want to say LOVE YOU SAN!!" и "billy gates why do you make this possible? Stop making money and fix your software!!". Вирусот содржел код кој требало да активира DoS напади на windowsupdate.com на 15 Април.

Sobig.F (2003)

Проценета штета: 5 до 10 милјарди долари и над 1 милион инфицирани компјутери

Sobig го направил месецот Август, 2003 година, мизерен за корпорациите и домашните корисници на персонални компјутери. Нај лошата варијанта бил Sobig.F кој се распространувал толку брзо, поставувајќи рекорд со над еден милион копии во првите 24 часа. Тој ги инфицирал компјутерите преку прикачен фајл на е-маил (со име application.pif и thank_you.pif). Кога се активирал тој се препраќал на сите контакти од е-маилот на инфицираниот корисник. Крајаниот резултат било правење на голем трафик на интернет. На 10 Септември, 2003 вирусот сам се деактивирал и повеќе не претставува закана. Microsoft објавиле награда од $250,000 за секој кој ќе го идентификувал авторот на Sobig.F, но до денеска виновникот сеуште не е фатен.

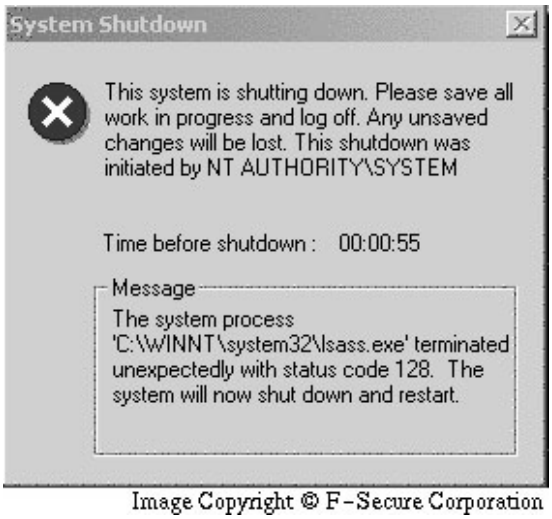
Bagle (2004)

Проценета штета: Десетици милиони долари

Bagle, класичен но софистициран црв, кој за прв пат се појавил на 18 Јануари 2004 година. Злонамерниот код ги инфицирал корисниците преку стандардниот начин, препраќајки се преку маил, и пребарувал низ фајловите на компјутерот барајќи е-маил адреси на кои би се препратил. Вистинската опасност на Bagle (познат и како Beagle) и неговите 60 до 100 варијанти, е тоа што кога црвот инфицирал компјутер отварал задна врата на TCP портот кој можело да се искористи за оддалечен пристап кон компјутерот и до сите податоци во него. Bagle.B, која била друга варијанта на Bagle била дизајнирана да престане со распространувањето на 28 Јануари 2004 година, но многу други варијанти на овој вирус продолжуваат да ги тормозат корисниците и до ден денешен.

MyDoom (2004)

Проценета штета: кога го достигнал врвот на распространување перформансите на Интернет биле намалени за 10 проценит, а времето на отварање веб страни се зголемило со 50 проценти. За период од неколку часа на 26 Јануари 2004 година MyDoom се распространил насекаде во глобалната мрежа преку е-маил. Црвот познат и како Norvarg, се распространил на заобиколен начин како прикачен фајл на е-маил порака која стигнувала како е-маил грешка содржејќи го текстот “Mail Transaction Failed.” MyDoom истотака се распространувал преку споделените фолдери на корисниците на Kazaa peer-to-peer. Размножувањето било толку успешно така што компјутерски експерти велеле дека на секои 10 пораки пратени во текот на првиот час содржеле вирус. MyDoom бил програмиран да сопре со ширењето после 12 Февруари 2004 година



Sasser (2004)

Проценета штета: Десетици милиони долари

Sasser почнал да се распространува на 30 Април 2004 година и бил доста деструктивен за да исклучи сателит за комункација на некои Француски новински агенции. Тој исто така бил причина за откажувањто на некои авионски летови и изгасувањето на системите на бројни компании на интернет. За разлика од повеќето црви Sasser не се пренесувал преку е-маил и не барал никакво вземнодејствие од корисникот за да го активира. За распространување црвот искористил не апдејтирани системи со инсталиран Windows 2000 или Windows XP оперативен систем. Веднаш штом ќе заразел некој компјутер тој почнувал да скенира за друг незаштитен систем и да се пренесе на него. Заразените компјутерски системи почнувале да паѓаат и да стануваат нестабилни.

4.Sniffer (прислушкувач)

Сниферите служат за надгледување на мрежниот сообраќај во кој учествува компјутерот кој се наоѓа на мрежата или во непосредна близина (на пр. некоја локална мрежа). Сниферите се употребуваат за проверување на работата на client/server апликациите, за проверка на некои филтри за проверка на податоци т.е. дали истите правилно функционираат. Како и поголемиот број на компјутерски алатки така и овие може да се злоупотребат и да се искористат за собирање на лозинки кои понатаму може да се искористат за упади во некои компјутерски системи. Кај безжичните мрежи каде што имаме заеднички медиум овие алатки многу често се коритстат, притоа се многу опасни, а нивен најголем адут е тоа што многу често можат да собираат податоци од сообраќајот без при тоа да бидат откриени односно во најголем број на случаеви тие не праќаат никакви пакети до останатите уреди на мрежа односно не комуницираат со нив туку едноствано само собираат пакети. Во зависност од комплексноста на вметнатите алгоритми и структурата на самата програма/уред постојат обични програми кои можат да собираат пакети па за

задача на корисникот е нив да ги анализира понатаму, па се до комерцијални, а пред се владини наслушувачи кои имаат можност по собирањето на пакетите да ги составуваат оригиналните податоци кои биле пратени, фаќаат лозинки, имаат можности за филтрирање на податоците, делење на различни групи и подгрупи. Исто така се овозможува да се открие кој се е приклучен на мрежата, кога ќе се фатат одредени податоци се знае од кого потекунуваат и за кого се упатени т.е. може многу лесно да се одреди кој со кого во кое време (колку и што) комуницирал. Постојат многу вакви open source програми од кои најдобри се: Ethereal, WireShark, Nmap и др. Но исто така постојат и специјални кои се креирани строго за одредена намена т.е. за употреба на владините агенции, таков е примерот со алатката за масовно следење на сообраќајот наречена Carnivore, а е направена пред неколку години за потребите на FBI. Интересно е тоа што нејзината работа и нејзиното постоење не е чувано во тајност (освен некои детали околку архитектурата).

Како работат sniffer-ите

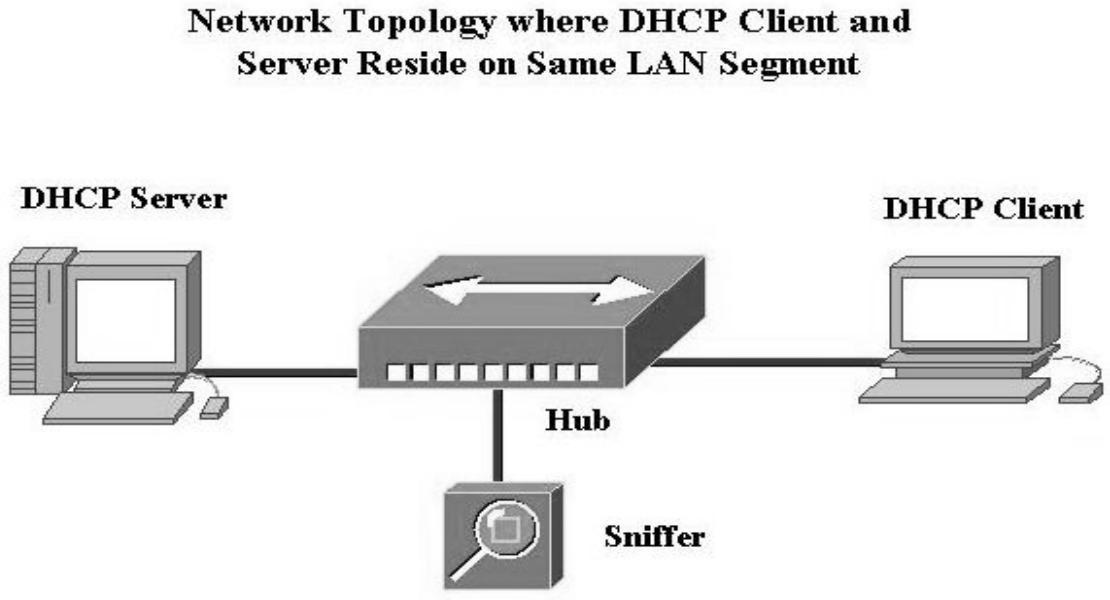
За да може да се наслушуваат пакетите прво треба можат да бидат примени од страна на вашата мрежна картичка. За да се овозможи ова таа мора да работи во така наречен promiscuous мод, кој овозможуваа таа да ги прима сите пакети кои се пренесуваат преку мрежата. Ова е важно бидејќи картичките вообичаено се конфигурирани да ги примаат пакетите кои одговараат исклучиво за нивната MAC адреса. Една негативност кај овој мод на работа е што при неговата работа испраќа податоци до мрежата и нај тој начин лесно може да биде откриен. Најчесто се користи при наслушување на жичани мрежи. Овој проблем не постои кај безичните мрежи бидејќи етерот претставува заеднички делив медиум и секој може да слуша на него нез притоа да мора да се автентицира или асоцира. Затоа овде се користи друг мод на работа кој се нарекува monitor мод. Со него картичката може да влезе во мод на слушање, во кој таа не праќа никакви податоци на мрежата па затоа и не може да биде откриена. За да не настанат забуни, мора да се напомене дека картичка конфигурирана во promiscuous мод ќе си работи подеднакво добро како и во жичена мрежа така и во безжична мрежа. Работата е што и во двата случаи може да биде откриена, и поради самата природа на етерот како медиум може да се избегне овој мод на работа а притоа да се постигнат истите резултати без страв од откривање. Често се поставува прашањето зошто е овозможен ваков мод на работа кога тој се користи за добивање на информации, чепкање по ничија приватност и како помошно средство при изведување на напади. Одговорот е многу прост и едноставен. Овој мод не бил направен и овозможен за таа цел. Целта му била да се користи за поправки на мрежата. Тој и понатаму најмногу се користи за таа намена. Кога имате проблем со картичката прво што ќе направи некој техничар кој е задолжен да ја „поправи“ е да го уклучи овој мод и да види што се случува на мрежата и со самите пакети а потоа и да заклучи кој е проблемот. Исто така се користат и од консултантски фирми. И не само работата во овој мод туку и најголемиот број на програми за наслушување се направени за корситење од страна на консултантски фирми кои вршат анализа на сообраќајот во вашата компанија, извршуваат тестирања на сигурносното ниво, или пак се користат од страна на администраторите на мрежи за да видат дали вработените го трошат работното време сурфајќи по некои непожелни сајтови. Битно само да се знае е дека постојат два начини на праќање на податоците преку мрежа: енкриптирани или како чист текст. Доколку се праќаат енкриптирани тогаш тие генерално се сигурни (се разбира

дека постојат начини тие да се декриптираат) додека пак податоците пратени како чист текст се лесно видливи и разбирливи. Многу често многу апликации а и самиот интернет го користат овој начин бидејќи така побрзо патуваат податоците односно не се троши време и простор за нивно криптирање и декриптирање. На пример кога пишуваме меил, буквите што ние ги читаме на екран како такви се праќаат на мрежа и со помош на ваква програма може слободно са се читаат пораки и слични податоци. На овој начин често податоците се праќаат од страна на Chat програмите, емаил програмите, веб страните и многу други програми (иако може да се постави енкрипција на mIRC, Messneger, ISQ, по дифолт овие опции не се поставени, и многу корисници не ги користат). Обично емаил клиентите, ftp клиентите , telnet, веб прелистувачите ги праќаат лозинките како чист текст, па доволно е да се исталира sniffer на мрежата или со лаптотп да се дојде во некоја безжична мрежа и да ги имате многу брзо сите лозинки и кориснички имиња на вработените во компанијата.

Битно да се напомене е дека слушањето во безжична мрежа сеуште не е противзаконско. Имено ако некој вика на повиско тон и ги кажува лозинките од неговите кредитни картички, а вие тоа „случајно“ го слушате, не правите ништо нелегално. Но доколку вршите декрипција на пакетите тогаш тоа е нелегално дејствие.

Заштита од наслушување

За заштита од sniffer-и на картички кои работат во promiscous мод постојат посебни програми кои исто така вршат наслушување на физичко ниво и бараат sniffer-и. Една таква програма е AntiSniff. Но таа се користи на приватни мрежи т.е на мрежи од одредени компании или институции, додека за домашни корисници и не може нешто повеќе да се направи т.е со сигурност никогаш нема да знаете дали некој ги наслушува вашите пакети. Затоа најдобра сигурност е ако користите енкрипија на апликациско ниво. Добра заштита е користење на SSL(Secure Sockets Layer) заштитени веб страни. Исто така добра работа е да се користи енкрипција за Chat канали, mIRC, Messenger-и.



Добра програма за енкрипцијана емаил е PGP (Pretty Good Privacy) но има и

уште подобра open source програма правена по теркот на PGP а се нарекува GPG.

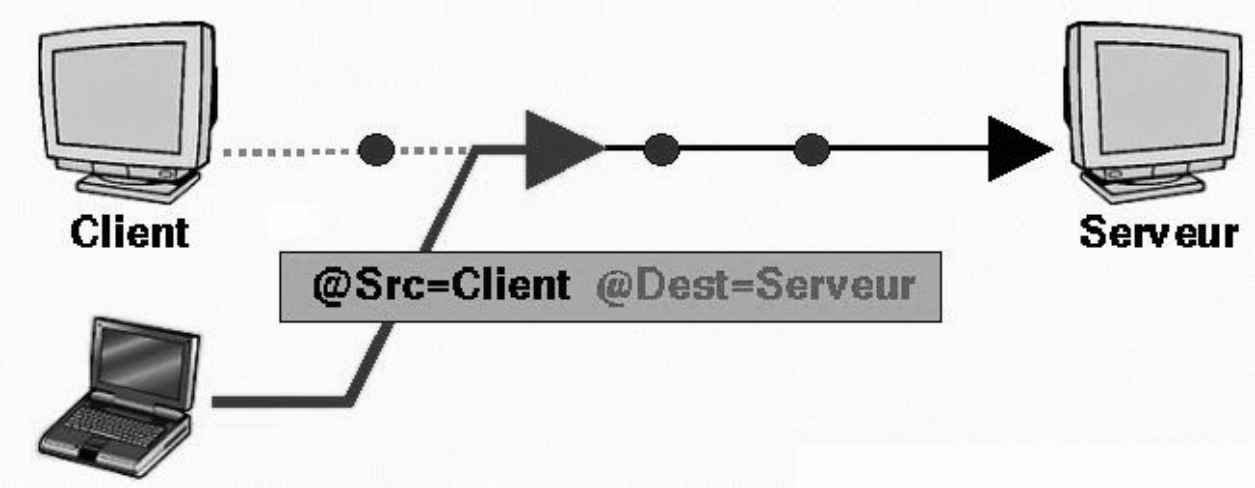
5.Spoofing attack(Лажно претставување)

Под зборот spoofing обично се подразбира метод вој се праќаат лажни информации до одреден компјутер односно се лаже одреден хост да мисли дека ние сме некој кој не сме. Има многу широка примена па затоа има и многу подтипови и негови варијации. Многу често се користи за да се скрие локацијата од која доаѓа напаѓачот. Hijacking-от е тесно поврзан со spoofing-от односно дури и може да се каже дека е продолжение или една понапредна варијација на spoofing-от. Тој подразбира преземање на нечиј идентитет со цел да му се преземе негова сесија. Поради тоа што во самиот метод на hijacking се користи и spoofing-от, во продолжение ќе бидат објаснети двата методи заедно.

Најпознатиот spoofing напад се нарекува IP spoof. Тој се заснова на IP ниво, односно на фактот за да се оствари отворена конекција TCP/IP бара адреса на испраќачот т.е. повратна адреса да биде сместена по пристигнатите

пакети. Многу често овде се става лажна адреса со што напаѓачот останува сокриен.

Најдобро идејата на нападот би се опишала со конкретен напад. Да се претпостави дека има два хоста, хост А и хост Б кои комуницираат преку интернет мрежата. Тоа што сака да го направи напаѓачот е да ги излаже двата хоста за нему да му ѓи испраќаат податоците т.е. да се претстави хост А дека тој е хост Б и обратно на Б да му се претстави дека е А. Тоа го прави на тој начин што треба да го убеди хост А дека IP адресата на хост Б е променета и приота да ја наведе својата IP адреса како нова IP адреса на Б, а истото да го направи и на другата страна т.е. на Б да му каже дека IP адресата на А е променета и неговата адреса да му ја каже дека е новата адреса на А(Man in the Middle напад).



Работата е во тоа што А и Б да не знаат што се случува, притоа сите меѓусебни пораки ќе ги праќаат до напаѓачот кој ќе ги чита, може да ги менува, некои од нив да ги брише и сл. Откако ќе ги добие посакуваните резулатати, се користи практика да ги извести уште еднаш А и Б за промена на IP адресата т.е. да им ја каже овојпат нивната вистинска IP адреса, бидејќи ако не го направи тоа ризикува тие да откријат дека цело време некој друг ги следел нивните пораки.

Кажувањето на новата адреса е многу едноставно и се одвива со користење на ARP (Adress Resolution Protocol) барање напаѓачот ќе им ја прати истата порака кажувајќи им ја новата IP адреса, поставена веднаш до MAC адресата, дека е лозирана на XXX.XXX.XXX.XXX. Ова ќе ги натера А и Б да ја update-уваат својата ARP табела со новата адреса со што сите податоци ќе се праќаааат до компјутерот на напаѓачот. Овде треба да се напомене дека едни од најпознатите напади DoS и DDoS всушност претставуваат еден вид на Spoofing напади.

5.1.MAC Spoofing

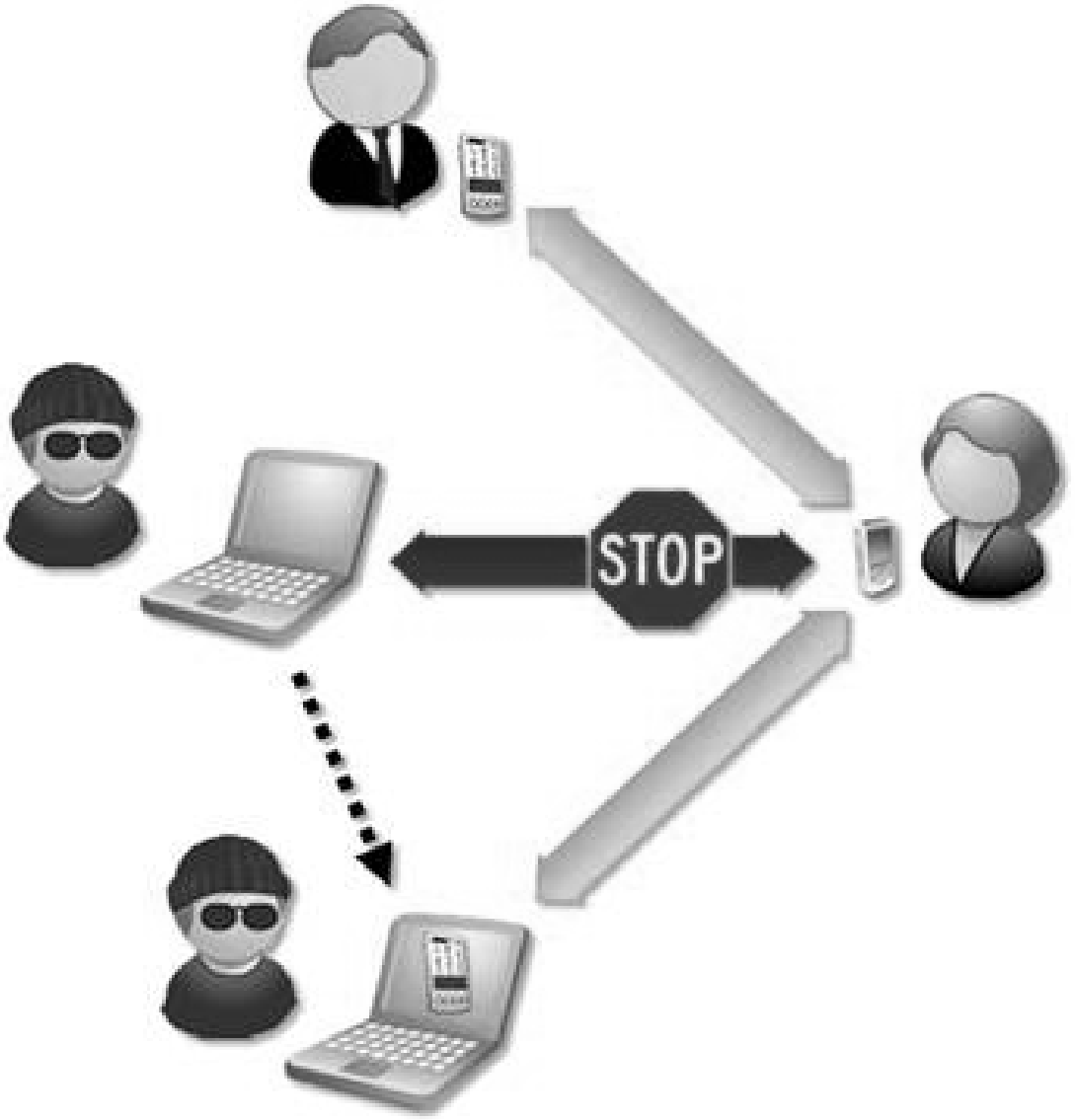
Некои пристапни точки(Access Point) имаат опција да овозможат (или неовозможат) пристап до мрежата врз база на MAC адресата која ја има вашата безжична картичка. Овие адреси (најчесто дозволуваат до максимум 20 различни адреси) се чуваат во една листа, од каде кога ние сакаме да се автентицираме и асоцираме со пристапната точка, таа ја гледа нашата MAC

адреса која патува низ етерот и стигнува до пристапната точка и ја споредува со листата, доколку ја најде во таа листа нас ни е дозволен пристап, во спротивно пристапот не е дозволен.

Ова претставува скоро никаква заштита од професионалци, но бидејќи поголемиот број корисници и не ги интересира баш многу техниката и се мало разбирање, може да послужи како одбрана. Иако со правите програми може да се добие пристап за неколку секунди. Можно е напаѓачот да ја наслушува мрежата и доколку има барем еден легитимен корисник т.е. лесно да ја открие неговата MAC адреса, бидејќи таа патува незаштитено низ етерот, таа се детектира за неколку секунди со програми како Etherial или WireShark. Откако се добие адресата на легитимниот корисник, треба нашата MAC адреса да се промени во таа на корисникот т.е. да се клонира. Значи ние не ја менуваме хардверски оваа адреса (на самата картичка и понатаму си останува напишана оригиналната MAC адреса од производителот) туку само во софтверот се менува и се става друга. За ваков тип на напад постои корисна програма наречена SMAC. Оваа програма работи само на Windows оперативни системи, и истата е користена од CISSP, CISA, MSCE и професионалните софтверски инжинери. Таа има едноставна навикација и нуди доста информации за мрежната картичка како што се:

- ID на уредот
- Активен статус
- Објаснување(информации за) NIC
- Спуфиран статус(ДА/НЕ)
- IP адреса
- Активна MAC адреса
- Спуфирана MAC адреса
- NIC харверски ID
- NIC конфигурациски ID

По стартувањето на програмата таа дава листа на активни мрежни адаптери. Тука се гледа дали добиваме информации од тоа дали е активен адаптерот, дали е спуфиран, неговото име, IP адресата и неговата MAC адреса.



6.Мрежна безбедност

Заштитата на податоците од секогаш е бил важен фактор на некои поединци или компании. Информацијата која се штити може да биде од најразличен карактер: техничка, комерцијална, финансиска, лична и др. Информацијата може да се чува во заштитена просторија, на пример компанија која има обезбедување на влезот и влез е дозволен само на поединци.

Но со текот на времето технологијата напреднува и постои потреба за поголема количина на податоци и информации т.е. се преминува на компјутерски системи кои имаат потреба од заштита на тие податоци, а посебно кога станува збор за компјутерски системи кои се поврзани во компјутерски мрежи. Компјутерските мрежи биле создадени со цел спојување на компјутери од различни локации така да можат да делат и разменуваат податоци т.е. да комуницираат меѓусебно. Корисниците мора да бидат сигурни дека нивните мрежи ќе бидат осигурени од неовластено надгледување и заштита од неовластени корисници се со цел заштита на приватните информации и од менувањето на истите во текот на преносот преку мрежата.

Сигурноста на информацијата има три основни својства: тајност, интегритет и достапност (Confidentiality, Integrity and Availability). Остварената сигурност изгледа едноставна – само треба да се зачуваат овие три својства. Иако ова изгледа како едноставно во пракса тоа не е лесно да се оствари заради испреплетеноста и големиот број на информации, делење на исти информации помеѓу повеќе особи и сл.

На сигурноста во мрежите поедноставно може да се гледа на следниот начин:

- **Сигурност во пристапувањето**
  - Автентикација
  - Авторизација
- **Сигурност во преносот на податоци**
  - Енкрипција
  - Тунелирање.

Сигурност во пристапувањето

Автентикацијата е процес во кој се проверува идентитетот на некоја особа (или група) во системот. Тоа се врши со внесување на корисничко име и лозинка. Тоа е една од наједноставните заштити во пристапот и исто така наједноставна за имплементација. Системот на кој се пристапува ги има сите парови на кориснички имиња и лозинки и доколку еден пар не одговара системот го отрфла (не му дозволува да пристапи).

Авторизацијата кажува дали личноста која го поминала чекорот на автентикација идентификувана во системот има (и ако има) одобрените за пристапот до ресурсите и до кое пристапничко ниво(анг. Security clearance). Тоа во секојдневниот живот може да се спореди со проверката на картите во некоја кино сала, и местото за седење кое е одредено со таа карта.

Сигурност во преносот

Тунелирањето служи за заштита на податоците при преносот. Меѓу најпознатите и најкористените протоколи за оваа заштита се: PPTP, L2TP, IPSec, SSL(Secure Socket Layer), TLS(Transport Layer Security), EAP(Extensible Authentication Protocol), EAP TTLS – EAP Tunneled TLS Authentication Protocol.

PPTP протокол - Е мрежен протокол кој овозможува сигурен пренос на податоците од одалечен Windows корисник до Windows сервер во одредена мрежа со креирање на VPN(Virtual Private Network) преку TCP/IP базирана мрежа.

L2TP протокол – Карактеристиките на L2TP протоколот(протокол од второ ниво) обезбедува платформа за VPN базирана на стандарди и ги исполнуваат условите за безбедност и интегритет на податоците кои и се потребни на фирмите за пренос на осетливи податоци. Елементите што се потребни за реализација на оваа заштита се:

- L2TP пристапен концентратор (LAC – L2TP Access Concentrator)
- L2TP мрежен сервер (LNS – L2TP Network Server)
- Сервер за мрежен пристап (NAS – Network Access Server).

IP-IPSec, Сигурносен протокол - Сигурносен IP е базиран на стандардите кои ги развила групата IETF. Станува збор за отворен стандард кој обезбедува сигурна приватна комуникација преку мрежа. IPSec обезбедува тајност, интегритет и автентикација на податоците помеѓу двете страни кои што комуницираат преку јавна IP адреса. IPSec применува автентикација и енкрипција на мрежно ниво на OSI моделот, обезбедува сигурно решение од точка до точка во самата мрежна архитектура, па заради тоа крајните системи и апликации немаат потреба од друга активност за да имаат појака заштита. Благодарение на овие карактеристики во голема мерка се намалуваат трошоците за имплементација и управување.

Проверка на интегритетот во преносот

Checksum – Еден од најстарите начини за проверка на интегеритетот на податоците кој исто така може да претставува начин на автентикација заради тоа што (Invalid checksum) податоците се на некој начин компромитирани. Checksum се одредува на 2 начини:

Да се претпостави дека checksum-от на еден пакет е 1 byte. Познато е дека 1 byte = 8 bits и секој бит може да има само две состојби, од каде што заклучуваме дека вкупно може да има 2^8 можни комбинации. Исто така познато е дека броењето на битовите започнува од 0 и вкупно има до 255 вредности. Доколку има 1 бајт зададениот пакет вкупно имаме 255 вредности или помалку толку checksum има точна вредност, а пак доколку сумата на бајтот на дадениот пакет има поголема вредност од 255 тогаш checksum добиената вредност ја дели со 256. Во продолжение е даден еден пример.

Пример:

Byte1	Byte2	Byte3	Byte4	Byte5	Byte6	Byte7	Byte8	Вкупно	Checksum
212	232	54	135	244	15	179	80	1151	127

- 1151/256 = 4.496(заокружено на 4)
- 4 x 256 = 1024
- 1151 – 1024 = 127

CRC (Cyclic Redundancy Check) – Овој начин на проверка е многу сличен на концептот на проверка како checksum со тоа што користи т.н. полиномиално делење (анг. Polynomial division) за да ја дознае вредноста на CRC која обично е 16 или 32 битна. Добрата особина кај проверката со CRC е тоа што е многу прецизна техника од причина што ако само еден бит е различен, конечната вредност на CRC нема да се совпаѓа и со тоа ќе пријави грешка. Недостаток на оваа проверка е тоа што може да се прави корекција во текот на преносот на информацијата, а во исто време не нуди никаква заштита од нападите на податоците. Во тој случај се користат по софистицирани техники како што се јавните или симетрични клучеви.

Апликациски сервиси

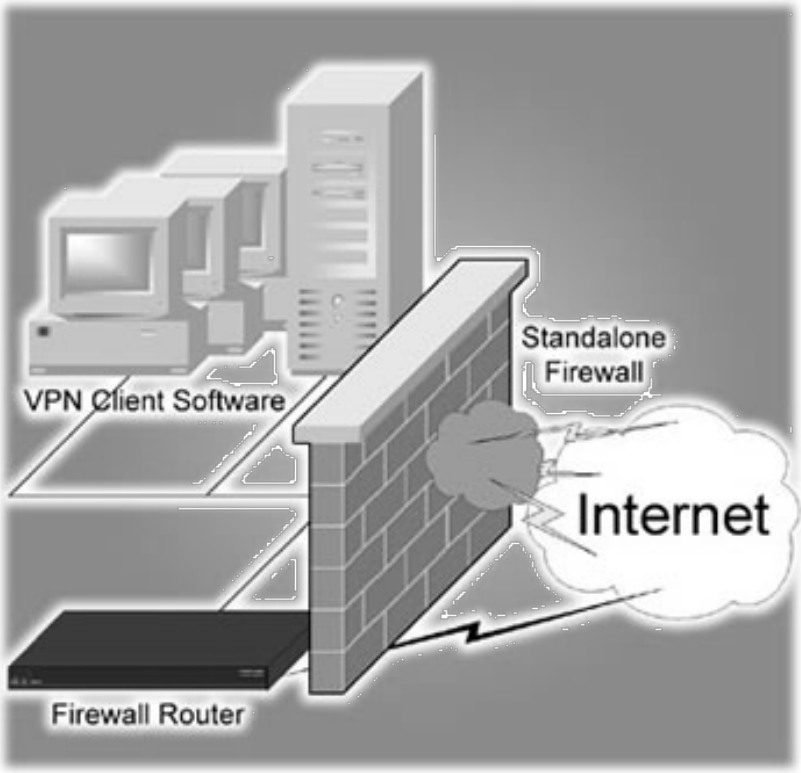
- PGP – Pretty Good Privacy
- S/MIME - Secure/Multipurpose Internet Mail Extensions
- SET – Secure Electronic Transaction
- Kerberos
- SSL/HTTPS.

Наведените апликациски сервиси се најчесто користени во компјутерските мрежи (Интернет).

7.FIREWALL (Огнен ѕид)

Огнениот ѕид (Firewall-от) претставува една од основните заштити на мрежите. Со нив се заштитува локалната мрежа од напади надвор од мрежата. Секој LAN се поврзува на Интернет преку gateway кој обично вклучува и firewall. Со firewall може секој проток на податоци кој не е дозволен да се дозволи или да се дозволи секој проток кој не е забранет. Постојат два вида на firewall-ови:

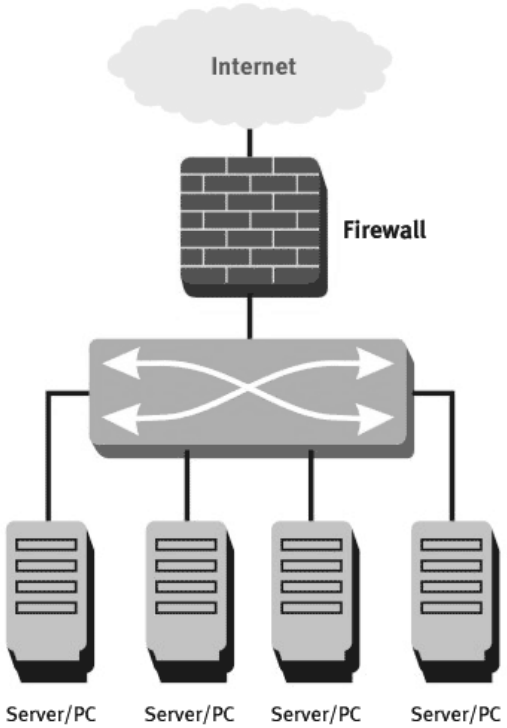
packet-filtering firewalls и application-level gateways. Firewall-ите за филтрирање на пакети (packet filtering firewalls) ги испитуваат сите податоци испратени надвор од надвор – кон локалната мрежа (LAN) и автоматски ги одбиваат пакетите кои имаат адреси од локалната мрежа. Пример, ако некој напаѓач т.е. некој хакер надвор од мрежата ја открие мрежната адреса на компјутер од локалната мрежа и се обиде да испраќа пакети преку firewall-от кој филтрира пакети, тој ќе ги одбие пакетите бидејќи имаат локална адреса, а потекнуваат надвор од мрежата. Проблем е тоа што овие firewall-ови го испитуваат само изворот на пакетите, а не и самите пакети. Целта на другиот тип на firewall т.е. application-level gateway е да ја испита содржината на податоците.



Во следната табела се дадени множество на правила дефинирани кај еден firewall од типот на packet-filtering.

Изворна адреса	Изворна порта	Дестинациска адреса	Дестинациска порта	Акција	Опис

Any	Any	192.168.1.0	> 1023	Дозволи	Дозволува повратни TCP конекции до внатрешната подмрежа
192.168.1.1	Any	Any	Any	Забрани	Спречи го Firewall-от сам директно да се конектира било каде
Any	Any	192.168.1.1	Any	Забрани	Спречи ги надворешните корисници директно да пристапат до Firewall-от.
192.168.1.0	Any	Any	Any	Дозволи	Внатрешните корисници можат да пристапат до надворешните сервери
Any	Any	192.168.1.2	SMTP	Дозволи	Дозволи на надворешни корисници да ни пратат email
Any	Any	192.168.1.3	HTTP	Дозволи	Дозволи пристап на надворешни корисници до WWW серверот
Any	Any	Any	Any	Забрани	"Catch-All" правило - Сè што не е дозволено - е забрането



8.ЗАКЛУЧОК

Сигурноста во информатичката технологија во денешно време претставува многу важен фактор. Со зголемувањето на информациите воопшто, а со тоа и сообраќајот низ комплексно дизајнираните информациони мрежи, нивната досапност, интегритет и тајноста на истите условува да се развива нова

технологија (хардверска или софтверска) т.е. решенија кои ќе обезбедат побрз пренос и што е поважно побезбеден во поглед на сигурноста. Со порастот на креирање на безбедни решенија расте и бројот на сигурносни напади како во компјутерските мрежи така и во други типови на преносни системи. Со воведување на нови сигурносни протоколи за пренос на податоци и информации и примени на нови техники се условува и развој на нови типови на сигурносни напади бидејќи тие зависат едни од други т.е. како што расте брзиот развој и техника на заштита и превенција на податоци од напади така има брз развој на нови техники и методи кои се развиваат за напади и злоупотреба на информации и податоци.

Користена литература:

1. Microsoft Encarta 2005 Енциклопедија
2. Wikipedia, The free encyclopedia
3. Hacking for Dummies 2nd Edition, Kevin Beaver
4. Многубројни форуми поврзани со IT Сигурноста.