Доклад за сигурността на мрежата на Факултета по Математика и информатика на Софийски Университет

Изготвен от:
Антон Николаев Андреев (team leader) фн 43709
Стоян Добрев Добрев фн 43708
Деян Гунчев Гунчев фн 43724

Настоящият документ описва: устройството на мрежата на ФМИ, мерките, взети от системните администратори на ФМИ, мерките, взети от университеския изчислителен център. Описани са предполагаеми начини за атака и начини за защита от тях, както и пролуки или предполагаеми опасности, открити от самите нас (гореспоменатите).

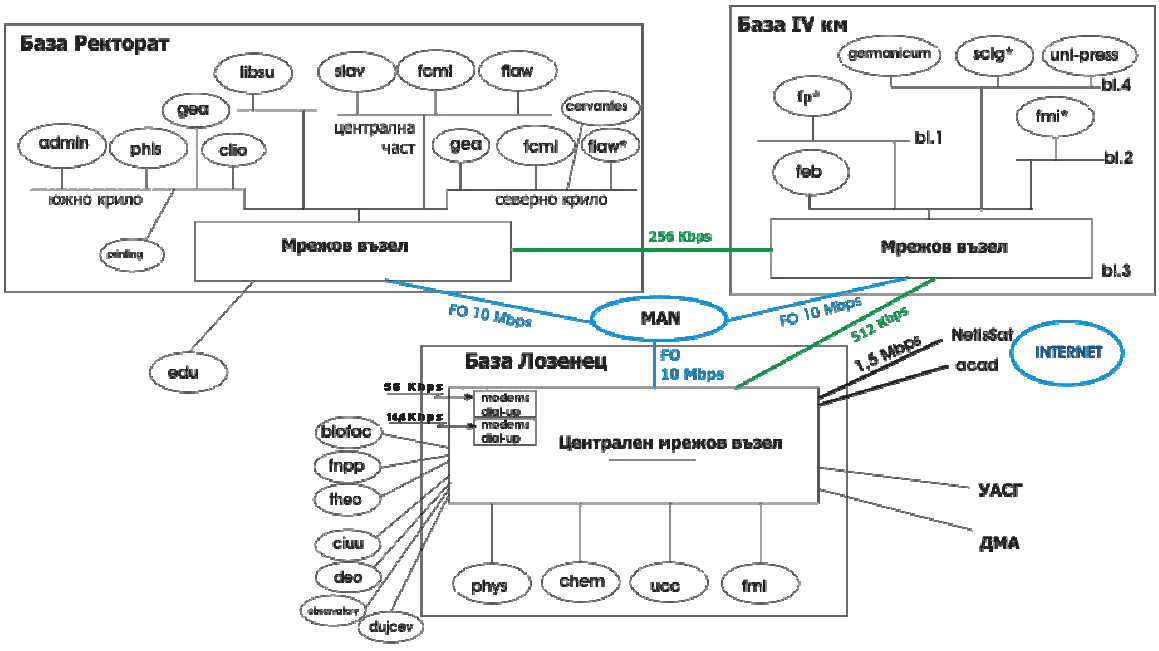
Физическо ниво на защита.

Няма човек, който да следи дали някой не прави нещо нередно в залите за свободен достъп на факултета: закачане на HDD, отмъкване на мишка/ клавиатура и т.н От факултета непрекъснато влизат и излизат компютри – без това да се следи от портала. Много вероятно е да излезеш с компютър под ръка и при въпрос къде отиваш просто да кажеш: “Аз съм от администаторите и го нося във физическият факултет – споко.” Администраторите трябва да имат отличителен знак?? Друг е въпросът, че ако човек ще взема компютър, то той ще го тикне в голям сак и ще си излезе. Компютрите във факултета са защитени чрез греди, метални решетки и аларма. Опасността идва от факта, че алармата се изключва при портиера (с код обаче) и е съвсем близо до входа. Ако някой успее да влезе при него, може да го заплаши и да я изключи. Нивото на сигурност пада драстично след елиминарането на алармата. Решетката на залите на третият етаж е само с един куфар, който се маха за 10 секунди с едни големи дълги клещи. Може да звучи малко по - така, но има начин за преодоляване на греди и той е като се изреже врата под тях. Достатъчно е това да е вратата на двупроцесорните сървъри на ФМИ. Това ще вдигне шум, но в близост до факултета не живеят много хора. Трябва да се отбележи и че вратите не са от най-тънките. Факултета вечер вече е осветен от всякъде (малко като затвор) и това би попречило на масово изнасяне на техника, но доскоро не беше

така. Скоро имаше кражба във фирмата за компътърна техника във физическият факултет – съществува реална опасност! Пример за място, където се правят опити да се държи на сигурността на физическо ниво е студентският компютърен клуб. Всеки студент там се записва в книга: име, факултетен номер и подпис. Какъв е проблемът обаче накой да напише фалшиви данни? В клуба винаги има човек, който следи дали всичко е наред. Domain controller-а на ФМИ пази информация за всеки log-нал се към него – дата, време, продължителност, компютър. .NET има класове за работа с Active Directory. Това може да се използва, ако даден студент е търсен за нещо. Преди няколко месеца студент открадна портфейла на своя колежка от ФМИ. Възможно е да се напише програма, която при log-ването на даден потребител в domain-а да съобщава (където трябва) къде е съответният човек и той да бъде хванат.

Устройство на мрежата - топология

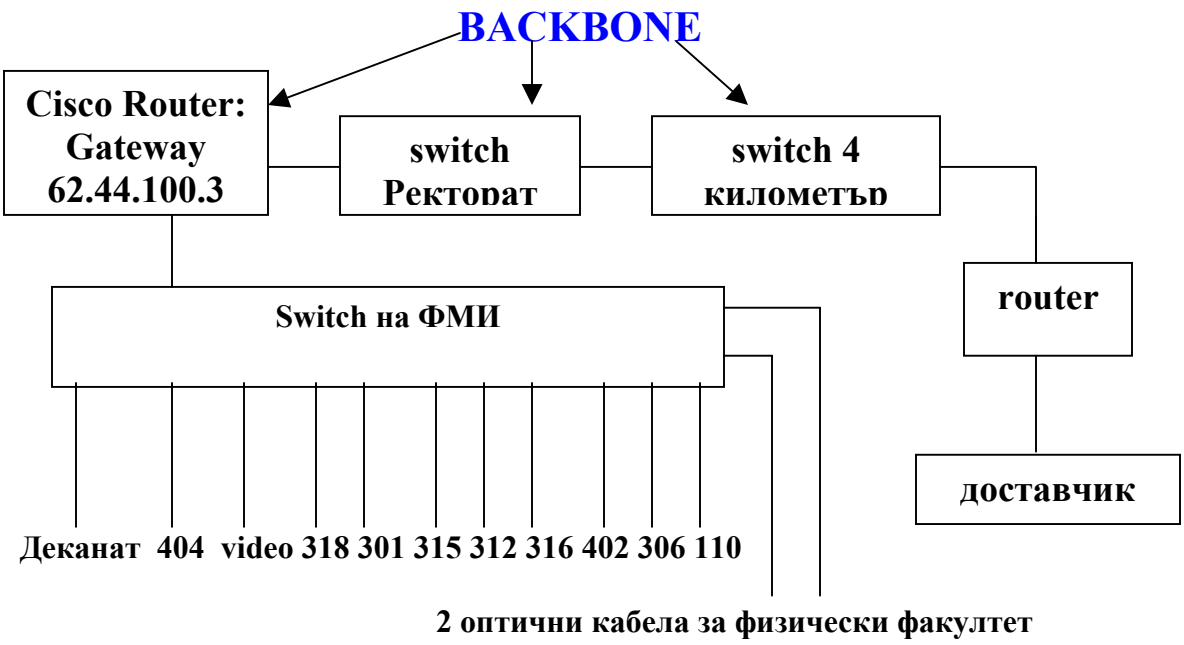
Мрежата на Софийски университет притежава 32 по 255 IP адреса (учудващо много). За domain-а uni-sofia.bg извлякохме следната DNS информация :ns.uni-sofia.bg (62.44.96.1), ady.uni-sofia.bg (62.44.96.7) sns.netissat.bg (212.72.193.55). Това са основните DNS сървъри на Софийски Университет. Мрежата на ФМИ е 10Mbit, защото главният router на ФМИ в Изчислителния център е 10Mbit, въпреки че между компютрите в залите е 100Mbit-ва заради самите switch-ове. Използвахме cheops6.0pre4 под Fedora Core1 да визуализираме част от мрежата на ФМИ, а друга информация ни бе любезно предоставена от Изчислителния център.



FO – оптичен кабел

Интернета пристига в Университетския изчислителен център по оптични кабели, радио модеми и др от NetisSat, Acad (www.acad.bg) и БАН. Има backup връзка към

Цифрови системи, която много не се ползва. След това бива разпределен по показаната по-горе схема на 3 основни възела, а от там за всеки един факултет на Софииски Унивеситет. Става въпрос за една сравнително голяма мрежа. Интернет може да бъде предоставян и по dial-up за някои преподаватели. Страницата на изчислителния център е: http://noc.uni-sofia.bg. Другите факултети имат по един кабел към главният router (това са всъщност няколко switch-а). ФМИ има над 10 кабела ☺.



Това е приблизителната схема на окабеляването, но много често кабелите на ФМИ са свързани към други switch-ве. Трафика на ФМИ се рутира от gateway.fmi.uni-sofia.bg.

Политика

Използвайки над 200 реални IP адреса ФМИ представлява една реална мрежа и именно тук започват проблемите. Реалните IP адреси предполагат, че съответните машини са изложени на непрекъснато сканиране отвън. Възниква въпросът – нужни ли са те за машини, които се използват само за програмиране и достъп до Интернет? Портовете под 1024 са блокирани навътре с (изключение на 80 порт) от Изчислителния Център с цел подобрение на сигурността. След нашето сканиране се убедихме, че това е логично решение. Впечатление прави, че и порт 443 http protocol over TLS/SSL е затворен!(поне в настоящият момент). Оказва се , че много от mail сървърите на другите факултети са open-relay. Също така все още има стари работещи BSD машини с неясно колко стар и бъгав **sendmail**. Това води до излишен трафик – спам. Изчислителният център също така следи и за подозрителен трафик и честа практика е да отреже някое клонче (студентският

компютърен клуб) от мрежата и с това да се решат проблемите ☹(без дори да информират). След като се оправи съответният компютър ги пускат... Имаме 2 типа машини: на хора, които по-разбират (могат да си пуснат web-server, mail server, ssh server, ASP.NET server) и на обикновени потребители, които програмират и ползват интернет. Първият тип хора се възползва от реалните IP адреси, но ограничението на портовете не позволява тези хора да си пускат нормално услуги, тъй като те са точно на портове под 1024. Така ограничението върху портовете, наложено заради втората група от хора, тежи и върху първата. Това обикновено се преодолява чрез качване на услугата на по-висок порт, но някои услуги са си точно на опеделен порт! За пример ще дадем асистент Никола Владов, който работи със Slackware Linux и има собствен mail server, но заради блокирането на портовете, mail server-а му вече не работи. Изчислителният център има приемно време от 14-16 часа, в което човек може да поиска да му бъде отворен порт (или нещо друго) и ако е достатъчно основателно може и да успее. Разрешение на този конфликт може да стане ако обикновените компютри(втората група) са с локални IP адреси, а интернета им да е през NAT (няма да може лошите хора от вън да се обръщат към тях) и да няма филтрация върху трафика за останалите (първата група). Заради блокиранто на портовете студентите не могат да се връзват към факултетският file сървър store, където са им личните директории. Това може да стане през Debian и ssh на порт 2200. От там с командата smbmount се връзвате към store (не забравяйте $ в края на името на директорията си). По отношение на политиката трябва да отбележим, че има хора които използват firewall – Kerio Personal Fireall, още Hacker Eliminator, а други просто смятат, че изключният компютър е най-сигурният компютър ☺.

Колко сигурна е глобалната защита?

Филтрацията на трафика става със споменатия вече Cisco router. Появява се следният потенциален проблем: могат ли да преминат навътре фрагментирани TCP пакети? В тази пакети TCP хедъра е разделен (фрагментиран) на две например. Switch-а разглежда пакетите един по един. Например: искаме да пратим TCP пакет и разделяме хедъра от да кажем 20 byte-а на един пакет, в който има 16 от тях и на още един, в който има 6 byte-а. Switcha-а не се усеща и като резултат тези пакети биват съединени в TCP/IP стека на операционната система (към която са предназначени) като едно цяло. Описаното не проработи - сканирахме с nmap и опция за фрагментирани TCP пакети. Възможно е освен proxy за трафика навън да има и proxy за трафикът навътре, което ще разбира от application level протоколи и ще държи сметка за фрагментацията на пакетите преди да ги пусне навътре в мрежата. Дочухме, че switch-а, който филтрира трафика е бил излязал извън строя за около 2 седмици – работел е колкото да се каже, че работи, но ACL(Access Contol list) му бил отпаднал. Това е доста опасно, защото някои хора знаят за защитата на портовете и се успокояват с нея ... ☹ оставят компютрите си включени по цяла нощ...

Залите

"Залите" наричаме стаите разположени на третия етаж от 313 до 322, където всички студенти имат почти свободен достъп до компютрите. За залите се грижи Лаболатория Информационо Обслужване (ЛАБИО) – стая 312 и 318. Опрерационните системи са Windows NT 4.0 и Windows 2000. Лесно може, когато имаш физически достъп до определена машина, да откраднеш паролите на юзърите от нея. Това става като от системна дискета с windows 98 се зарежда NTFS-DOS и се mount-ва локалния диск. След това спокойно се копира файла с паролите, който се намира в C:\winnt\system32\config\SAM. После (не много трудно) си изтегляме от интернет декодер за пароли за Windows NT, например L0phtCrack 2.5 и той сравнително бързо с помоща на dictionary attack и brute-force attack открива паролите. BIOS-ите на компютрите в залите са без пароли, което позволява boot-ването от флопи и използването на системна дискета. За щастие паролите на всички потребители на FMI domain-a се пазят от Domain controller-a, което теоритически означава, че от залите може да бъде откраднатa само локалната администраторска парола. Лошо е обаче, че локалната администраторска парола на залите се сменя горе-долу веднъж в годината. Направихме опити да вземем администраторската парола – неуспешни. Причината е, че от Microsoft съществува utility syskey.exe, което е налично за версии на Windows NT 4.0 и нагоре. С него може да бъде зададено криптиране на самият SAM файл. Стандартно това не е активирано, а просто операционата система отказва достъп до този файл (и самите пароли не се съхраняват, а само техните хешове). Има два начина за защита на SAM. При първият след криптиране вие можете да въведете парола за неговото разкодиране при стартирането на системата, а може и това да става автоматично без парола (Windows сам си го разкодира). При вторият ще запазите ключа на дискета, от която ще се нуждаете при стартиране на системата. Съществуват някои програми за премахване на администраторската парола, базирани на Linux операционата система и driver за работа с NTFS, разпространявани безплатно – всеки може да си ги изтегли от Интернет. Изтриването на SAM води до анулирането на администраторската парола. В студентски град може да се открие и регистрираната версия NTFSPRO, която позволява и триене, а не само четене. Peter Nordahl е открил и е създател на точно такава програма, която успешно вмъква акаунти. По-интересен е фактът, че акаунти могат да се вмъкват дори, когато е използван syskey.exe с ключ запазен на дискета!!! Просто след вмъкване на новият системен user и рестартиране, новите хешове автоматично се конвертират в SYSKEY версии и човек спокойно се логва като администратор (windows не се пита от къде са дошли тия хешове). С тази програма може да се прави всичко: изключване на syskey (което на практика не е необходимо) , подмяна на пароли на потребители, промяна на registry. Единствена защита е в пароли на BOIS-а и изключване на зареждането от Floppy … и CD. Доста трудно за потенциален хакер ще стане ако ключа от syskey е на дискета, но това е неприложимо на постоянно използвани работни станции. Направихме опит и успяхме да подменим паролата на локалният администратор ☺. После я върнахме пак същата, защото един от нас е Domain Admin на ФМИ (и знае истинската парола). Използването на програмата е опасно – може да наруши цялостта на NTFS, но при нас всичко мина гладко ☺.

Трябва да се отбележи и факта, че Windows кешира hash-ове на потребители. Това е опасно, защото някои smbclients предоставят възможността за достъп до NT сървър само със хеша на паролата. Една интересна атака е synflood на порт 88 на Domain Controller-а. Това ще попречи на използването на kerberos протокола и ще принуди всички клиенти да използват NT 4.0 процедури за удостоверяване. Това не е пробвано и е добра идея за проект по мрежова. (не можем да пробваме всичко) Сега може да се използва L0phtcrack за прихващане и кракване на LM и NTLM хешове. Статията от Hernan Ochoa от CORE-SDI показва как данните, свързани с удостоверяване на личността, могат да бъдат променяни директно в паметта, така че да се имитира всеки един потребител, ако е достъпен хеша му! (експлоити от подобен вид не са широко разпространени) Кеширането може да бъде спряно чрез промени в registry:

Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows NT\CurrentVersion\Winlogon
Name: CachedLogonsCount
Type: REG_SZ
Value: 0 не кеширай пароли
Value: 1 препоръчително – само една
Value: 2-50
Value: 51 (не може повече от 50)

Друг начин е със следните registry промени:

Hive: HKEY_CURRENT_USER
Hive: HKEY_LOCAL_MACHINE
Key: Software\Microsoft\Windows\CurrentVersion\Policies\Network
Name: DisablePwdCaching
Type: REG_DWORD
Value: 0 (спри да кешираш)

Ако искаме само паролите на групата Domain Admin да не се кешират:

Hive: HKEY_LOCAL_MACHINE
Key: Network\Logon
Name: NoDomainPwdCaching
Type: REG_DWORD
Value: 1

Между отделните компютри в самия domain няма никаква защита, като да речем ограничение на портовете. Така че доста голяма заплаха е човек, който е в залите, получил администраторски достъп неправомерно(ограничението за портовете за него не важи), инсталирал троянски кон, който слуша на порт над 1000. Това прави възможно той да се връзва към тази машина отдалечено. Помага му и факта, че машината е с реално IP и не през NAT(Network Address Translation). Повечето стари компютри са занемарени. Например над WINNT директорията понякога всички имат права. Това позволява триене и подмяна на системни файлове. Същността на нещата е в това, че факултетски компютри биват хаквани и

използвани за хакване на други компютри, което руши имиджа на факултета и на университета като цяло. С изключение на някои администраторски машини, компютрите нямат инсталирани firewall-и, като някой разчитат точно на защитата на портовете под 1024. За по-голяма сигурност някои администратори са извън domain-а.

Доста често факултетската база от компютри бива използвана като Game-Club. Играе се предимно Starcraft. За някои не е сигурно дали са студенти в ФМИ и дали не ползват чужди акаунти – дадени им от студенти във ФМИ или откраднати?

Domain Controller-а на ФМИ

За Domain Controller-а може да се каже още, че той работи в **mixed mode**, а не в **native** (Windows 2000). Това се дължи на машини, работещи с Windows 95,98 и Windows NT Workstation 4.0. Native режима затяга повече сигурността и от тази гледна точка е препоръчителен. Има клиенти за старите операционни системи за native режим на Active-Directory (на инсталационния диск на Win200 \clients\win9X\dsclient.exe), но те не се използват! Тези клиенти не поддържат протокола за аутентикация kerberos, което е съществен недостатък. Тук опираме до човешкия фактор. Пак имаме 2 групи хора: по-advance потребители и просто потребители. Първите (някои закачат Laptop-и) трябва да си инсталират клиентите, като ще е малко трудно да бъдат уведомени за промяната. При вторите системен администратор ще трябва го инсталира и тества на всяка машина. Проблем са и все още работещи MAC-ове във физическият факултет, които вероятно(99%) няма да могат да browse-ват мрежата на FMI. От помощ би била страница на Лаборатория Информационо Обслужване, където да пише различни настройки, промени и подробното им обяснение и инсталиране. Естествено потребителите ще трябва да знаят за тази страница.

На Domain Controller-а открихме Web-server IIS 5.0 (със скенера Internet Periscope). НЕ ТРЯБВА на такава важна машина да има и Web-server, както знаем архитектурата ISS 5.0 е лоша, а и има безброй много дупки и пачове за него. Там се намират някои факултетски страници, но по-добре е да има специална машина – web-server за странците на факултета (което е запланувано). Тази роля (засега) се изпълнява от admin – www.fmi.uni-sofia.bg. На него пък открихме неизползван FTP сървър. Още на Domain Controller-а се намира и DNS сървъра на факултета, който може би е по-добре също да бъде изместен на друга машина и пуснат под Linux OS, въпреки че Microsoft препоръчват да са на една машина. Добра идея е втори Domain Controller, като 2 –та са с една и съща база данни на обектите в Active Directory (репликират) и работят едновремено. Така, ако нещо се случи (хакване, изгаряне на хард диск …), работата на потребителите няма да бъде нарушена. А може и вторият да играе ролята на standby и да се активира в момента, в който другият излезе извън строя. За подобряване на сигурността може да се използва SMB (Server Message Block authentication protocol) подписване. Поддържа се от NT

4.0 и нагоре. SMB предоставя аутентикация като поставя цифров подпис във всеки пакет, който после се проверява и от клиента, и от сървъра. Подписването на всеки пакет не се отразява на трафика, но затова пък натоварва процесора и на клиента, и на сървъра с миниум 10-15%. Това може да се окаже проблем, защото говорим за стари Compaq на по 200-300Mhz.

Още сме на тема Domain Controller! Най-често използваната OS е Windows. Това се дължи на няклко причини: самият Domain Controller е под Windows, Microsoft зарибяват ФМИ и администрацията (не че не правят хубави работи), Visual Studio е само за Microsoft –ска платформа. Алтернатива? Да. Алтернативата е да има и машини под Linux. Това ще излезе по-евтино, а и в някои отношения по-сигурно. Linux например си има вграден firewall – **iptables**. Вграден firewall при Windows? Да има, но само във версия XP/2003. Този firewall е доста слабо конфигуруем, въпреки че това щяло да се промени в XP SP2 и първият service pack за 2003. За целта трябва да се използва SAMBA като domain terminal client. Това обаче става сложно с помоща на PAM (Password Authentication Manager) и winbind. Трябва някой да си загуби времето и да пробва. А по отношение на Visual Studio – големите надежди са в Mono, но трябва и среда за разработка като например C#Studio … На тая тема може доста да се говори ☺.

Всеки студент на факултета има свой собствен потребителски domain акаунт, с който може да се логва на всеки компютър в залите (теоритически на всеки компютър във ФМИ). Този акаунт му предоставя правото да разполага с 200MB дисково пространство на server-a Store. Share директории са скрити ($) и само съответния потребител има достъп до тях, а Domain администраторите нямат. Разрешена е само една конекция за всяка share-ната директория. Това всъщност е неудобство... Направихме опит за разбиване на паролите на share-натите директории с xSharez + Xintruder(използван за атака върху NetBIOS протокола), но без успех (явно е приложен съотвтният пач).

Възможни ли са атаки върху ARP протокола?

Решихме да проверим дали са възможни ARP Spoofing/Poisoning атаки. Но мрежата на факултета е разделена на сегменти(около 10) от главния rooter на факултета. Сървърите са в отделен сегмент (заключени в отделна стая). Така че в най-добрия случай можеш да излъжеш компютрите от своя собствен сегмент.

Факултетска поща

Smtp.fmi.uni-sofia.bg е машината (първият mail exchanger), която получава цялата поща пристигаща във факултета, сканира за вируси, SPAM и проверява в blacklist-a. Mail.fmi.uni-sofia.bg е mail-box-a (вторият mail exchanger). OS е Winnt 4.0, а software Netscape Messaging Service (има и Netscape directory server – отделен от Microsoft Active Directory). Проверката за SPAM става трудно, защото някои потребители използват надстройка на Outlook Express, която в края на всеки mail

прибавя едно съобщение, което се третира от SPAM filter-а като SPAM. Тъй като пощата е едно от най-важните неща във факултета, компютърът, изпълняващ ролята на mail server, е доста солидна машина (двупроцесорна по 950Mhz, 1GB RAM и два SCSI диска). А какво ще стане, ако някой реши да прати поща от 20MB на всички. В един момент единият exchanger ще даде alert и ще спре да приема, а останалата поща ще стои в опашката на другият exchanger. Поддържат се протоколите POP3, SMTP, IMAP, но не и SSL/TLS, защото трябва да се инсталират сертификати, криптирането също така би забавило връзката при изпращане на големи файлове при по-стари машини, а и дори SSL/TLS да бе активиран, повечето хора няма да се сетят да го ползват, ако изрично не им се каже или покаже, така че паролите на mail-овте на всички хвърчат в чист вид. Чуват се слухове, че факултета ще купи сертификат и от Изчислителният Център има "раздвижване" по този въпрос, но не се знае ... Може би ще се направи собствено certification authority. Netscape имат certificate server със certificate based authentication. Squirrel mail (web базираната поща) да бъде през https и да се махне http. Работи се по въпроса. Засега ако държите на сигурността, може да настоявате пощата ви на mail сървъра на факултета mail.fmi.uni-sofia.bg да се препраща към mail сървъра на debian.fmi.uni-sofia.bg и от там да се връзвате към него със SSH(Putty) клиент и от там да си я проверявате с (Pine). Друг начин е лично наша идея: ако на mail сървъра се инсталира SSH server за Windows (например WinSSHD). Всеки клиент ще трябва да стартира SSH сесия ауторизирайки се с парола и да тунелира 110 и 25 порт. Това трябва да се направи да става автоматично – с една програмка - потребителя цъква, въвежда парола и след това пуска Outlook. Outlook ще трябва да се връзва към localhost, но с това се свършва всичко. Може да се използва SSH Secure Shell Client, който може да бъде изтеглен безплатно. В "settings" се маркира опция "request tunnels only" и след това в полето "Tunnels" - "Outgoing" се въвеждат 2 тунела за 25 и 110 порт, както и адреса на mail сървъра. Настройките се запазват в profile. После за обикновенят потребител остава само да избере мяню profiles, след това да въведе domain паролата си и Outlook или който и да друг mail-client би трябвало да работят безпроблемно. В последствие установихме, че тази идея (малко странна) се използва и от други. Има и MTA, които поддъжат ssh (fetchmail например).

Ftp.uni-sofia.bg

Използва се proftpd 1.2.9, което веднага показа, че самата операционна система е от Linux/Unix тип. При някои FTP сървъри може да се нагласи името на сървъра да не се изписва при свързване и да се избегне елементарният подход с просто намиране на exploit. Потърсихме за bug, после за exploit. Открихме 3 такива на сайта на security focus в частта bugtraq. Успяхме да компилираме и използване един, но той завърши с "Sorry, no root for you today". ☺ По късно видяхме, че има и директория proftpd, а в нея patches, от където директно можеше да се останови състоянието на ftp сървъра. От самият FTP сървър се вижда, че Изчислителният център разполага (това не гарантира, че използва) голямо разнообразие от ОС: debian, BeOS, PLAN9, FreeBSD, NetBSD, OpenBSD и около 15 Linux дистрибуции. Това е добре (ако са сравнително нови версии).

Debian.fmi.uni-sofia.bg

Debian-a е бил използван за хакерски атаки и заради това достъпът му до интернет е само през proxy-то на Изчислителният Център. Администраторът на Debian-a се грижи за това той да е винаги update-нат. Заради сигурността на достъпа до Debian-a потребителите се логват и обменят файлове САМО през SSH. Няма някаква допълнителна защита, като firewall, IDS. Защо, попитахме ние? Отговорът беше, че Debian-a не е толкова интересен за хакерите, защото достъпът до Интернет минава през факултеското proxy и е ограничен само до ssh,http и ftp. А и Debian се използва предимно за web странички??? Въпрос на политика ...

Сканиране

Nessus е порт и vulnerability скенер.Той се дели на client и server. Server-a е само под UNIX like операционни системи, но клиенти има и за Windows. Може да прави атаки върху различни операционни системи. Има си собствена база от потребители. Връзката става на Port 1241. При инсталирането се генерира публичен ключ. Връзката става през TLSv1,SSH и др.

Nessus откри следните уязвимости по компютрите във ФМИ:

Новите компютрите в залите са оставени на windows auto-update. Update services Майкрософт може да бъде използван за откриване на коя машина какви пачове липсват.

Fmi403-10.fmi.uni-sofia.bg

1. Проблем с RPC(remote procedure call service –135 port). С експлоит хакер може да придобие администраторски достъп до машината или да бъде инфектиран от червей (Msblast). Пачове могат да се изтеглят от: http://www.microsoft.com/technet/security/bulletin/MS03-039.asp и http://www.microsoft.com/technet/security/bulletin/MS03-026.asp .
2. Може да се установи null-session, която позволява извличането на информация, която може да се използва от хакер за по-нататъчни атаки. Това може да се коригира с ключ в registry RestrictAnonymous (статии Q143474 (NT 4.0) и Q246261 (Windows 2000)).
3. Хубаво е администраторският акаунт да се преименува – това поне ще забави хакерът. Трябва да се филтрира порт 139 тъй като може да използва за извличане на потребители:
4. –Администраторски акаунт: Administrator (id 500)
   - Guest account name : Guest (id 501)
   - ridvan (id 1000)
   - 403 (id 1002)
   - FMI403 (id 1003)
   - SDK (id 1004)

Zeratul.fmi.uni-sofia.bg

1. OS: Fedora Core 1, Linux kernel patch 2140
2. Стара версия на ssh daemon-a, може да бъде експлоитната, но това не е много сигурно при условие, че на тази машина са сложени всички update-и от Redhat.
3. Предполагаема опастност в rpc.statd daemon.

Cauchy.fmi.uni-sofia.bg

1. Проблем с RPC.
2. null-session,
3. Администраторският акаунт да се преименува – това поне ще забави хакерът.
4. Administrator account name : Administrator (id 500)
   - Guest account name : Guest (id 501)
   - georgetk (id 1000)
   - iliana (id 1001)
   - roumen (id 1002)
   - krassen (id 1003)
   - andy (id 1004)
   - darina (id 1005)
   - nicky (id 1007)
   - john (id 1008)
   - vspirid (id 1009)
   - TOWER$ (id 1016)
   - DEBUT1$ (id 1025)
   - SQLExecutiveCmdExec (id 1027)
   - kbankov (id 1039)
   - desi (id 1045)
   - ivailo (id 1048)
   - DTK1$ (id 1057)
   - angel (id 1058)
   - markov (id 1063)
   - Teachers (id 1067)
   - richy (id 1068)
   - admin (id 1070)
   - SDLOCAL (id 1074)
   - SDREMOTE (id 1075)
   - Domain SDLOCAL (id 1076)
   - Domain SDREMOTE (id 1077)
   - db2admin (id 1083)
   - WS1$ (id 1084)
   - dianal (id 1087)
   - pmihnev (id 1090)
   - BOJO$ (id 1091)
   - conference (id 1092)

- dejan (id 1100)
- DTK-SERVER$ (id 1106)
- DTK$ (id 1108)
- anton (id 1113)
- varbanov (id 1115)
- martin (id 1116)
- MTS Impersonators (id 1122)
- svetla (id 1133)
- lary (id 1134)
- NetShow Administrators (id 1137)
- coursedev (id 1139)
- Domain Printusers (id 1140)
- ELICA$ (id 1141)
- skounev (id 1143)
- sangelov (id 1144)
- iossifov (id 1145)
- javor (id 1147)
- MTS Trusted Impersonators (id 1167)
- WS2$ (id 1171)
- bojo (id 1172)
- IUSR_ZENITH1 (id 1181)
- kiriln (id 1182)
- Informix-Admin (id 1191)
- informix (id 1192)
- cmsdbusr (id 1193)
- DEBUT3$ (id 1194)
- vasko (id 1195)
- angelov (id 1196)
- DEBUT_2$ (id 1197)
- TOSHIBA-NOTE$ (id 1198)
- eliza (id 1200)

5. Повечето от горните акаунти никога не са били използвани,а някои от тях са disabled. Админи са: administrator, krassen, ivailo.

Tinko.fmi.uni-sofia.bg

1. Оставен е да работи messenger service, в който има buffer overflow bug. Освен това машината може да бъде flood-ната с много съобщения.

Riemann.fmi.uni-sofia.bg

1. Съществува възможност да се заобиколи защитната стена чрез UDP пакети със source port 53.

Thinkpad.fmi.uni-sofia.bg

1. Null-session
2. Възможно е да се логнеш на отдалечената система със следните комбинации потребител/парола:
3. 'administrator'/''
   'administrator'/'administrator'
   'guest'/''
   'guest'/'guest'
4. Пачът за Relative Shell Path не е сложен.
   (http://www.microsoft.com/technet/security/bulletin/ms00-052.asp)
5. Пачът за IP Fragment Reassembly не е сложен.
   (http://www.microsoft.com/technet/security/bulletin/ms00-029.asp)
6. Следните директории и файлове са достъпни като администратор – това позволява тяхната подмяна или изтриване:
   - tex-archive - (readable)
   + Content of this share :
   - .
   - ..
   - CiitDV_scr.pdf
   - fonts
   - install.pdf
   - localtexmf.zip
   - packages
   - readme
- systems
- texbytopic.pdf

- films - (readable)
+ Content of this share :
- .
- ..
- Analyze That.avi
- Analyze That.sub.txt
- Hitchkock Collection
- matrix_reloaded
- Seven DVD RIP CD1.avi
- Seven DVD RIP CD1.sub.txt
- Seven DVD RIP CD2.avi
- The Chubbchubbs.avi

- SharedDocs - (readable, writeable)
+ Content of this share :
- .
- ..
- desktop.ini
- favorites

- My Music
- My Pictures

7. Не са сложени и пачове: 'ResetBrowser Frame' и 'HostAnnouncement flood'. (http://www.microsoft.com/technet/security/bulletin/ms00-036.asp).
8. Липсва и пач за 'NetBIOS Name Server Protocol Spoofing'.
9. Трябва и пач за LPC vulnerability. (http://www.microsoft.com/technet/security/bulletin/ms00-070.asp)

Има и още ...

Jim.fmi.uni-sofia.bg RPC,Messenger,null-session (виждат се много потребители)

Fmi403-11.fmi.uni-sofia.bg RPC,null-session

Fmi403-15.fmi.uni-sofia.bg

1. RPC,null-session, shares с админ достъп.
2. 'ResetBrowser Frame' , 'HostAnnouncement flood' 'NetBIOS Name Server Protocol Spoofing'
3. Трябва и пач за LPC vulnerability.

Spoint.fmi.uni-sofia.bg

1. Стара версия на Apache server – трябва upgrade.
2. Стара версия на PHP server трябва upgrade to PHP 4.3.3.
3. Уязвимост в MSSQL server - пач http://www.microsoft.com/technet/security/bulletin/ms02-061.asp
4. Messenger bug.

Logic.fmi.uni-sofia.bg и stella.fmi.uni-sofia.bg

1. 'Etherleak' – проблем с драйвера на мрежовата карта. (http://www.atstake.com/research/advisories/2003/a010603-1.txt)

kbankov.fmi.uni-sofia.bg

Universal Plug n Play трябва да се спре.

compaq1-315.fmi.uni-sofia.bg

2. Compaq1 има МНОООООГО дупки в сигурността: RPC, IIS сървъра има проблеми с конфигурацията,buffer overflow и т.н.

Ipx.fmi.uni-sofia.bg Може да се извлече информация от SNMP, защото отговаря на community strings: public и internal.

Gateway.fmi.uni-sofia.bg – Cisco router-a

Angel.fmi.uni-sofia.bg Messenger service и univeral plug and play трябва да се изключат

Val.fmi.uni-sofia.bg

1. RPC, Messeger service buffer oveflow, 'RPC Endpoint Mapper Service on NT 4'
2. The registry key HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters може да се променя от неадминистратори .(http://www.microsoft.com/technet/security/bulletin/ms00-095.asp)
3. Липсва пач за IIS 6.0 Q828750 (MS03-040).

На кратко:

За съжаление настоящият документ не може да побере всичките 250 компютъра и безбройно много дупки в тях. Ние разполагаме с цялата тази информация в удобен HTML формат в размер на 2.7MB, който е/или ще бъде приложен към настоящият документ. За всеки компютър има отделен подробен доклад: дупки, предполагаеми дупки, препоръки и обяснение как да бъдат поправени. Най-често не са инсталирани пачове, небрежност при конфигуриране на системата (ако въобще е конфигурирана), което води до извличане на много информация от компютъра. Честа грешка е хората да се логват с администраторски акаунт, който е без парола (или паролата е "1" или "a"), а remote connection-а е включен (самоубийство).

Какво може да се направи?

Проверка за пачове може да стане по 2 начина. Microsoft имат програмка hfnetchk.exe, с която от централизирано място може да стане това. Също така може да се използва новата версия на Microsoft Update services. Още може да се използва IDS – Traffic Analizer. Хубаво би било във всеки сегмент да има по един агент, които да следи трафика и да изпраща обобщен доклад на централен сървър, където да бъде прегледан от системните администратори. Има хубави такива IDS системи и то безплатни, но са под Linux. Това прави нещата по-сложни, защото е твърде вероятно в сегмента да няма Linux машина. Възможно е използването на cygwin или Microsoft Services for UNIX (новата версия е доста добра, безплатна и дори получи награда от Linux обществото), но трябва да се експериментира.

Малко за SNORT

Открихме порт на популярният IDS SNORT на http://download.datanerds.net/binaries/snort-1.7-win32-static.zip, но той не е на на принципа на агенти. Ако човек иска, може да си смъкне и графична среда IDSCenter или Snort Panel. Snort се нуждае и от winpcap библиотеката. Съществува и Intelligent IDS http://www.securityprofiling.com/ , който е разделен на части и базиран на snort. Може да инсталира пачове на всякакви операционни системи, да следи за мрежовият трафик и да дава real-time alerts. Състои се от: server за updates, централизиран

server в локалната мрежа, конзола за комуникация с него, sensor и агенти. Ама е платен ... май.

Заключение:

Няма кой да обикаля и да оправя компютрите на всички във факултета. Остава въпросът дали въобще потребителите (преподавателите) ще се съгласят да им се инсталират пачове от администатор докато са заети да пишат mail (може да вземат да го линчуват?). Лаболатория Информационо Обслужване трябва да има страница. Адреса на тази страница трябва да е написан на лист хартия и залепен на видно място. Университета на Standford има нещо такова! На страницата трябва да се наблегне на това, че всеки компютърно грамотен човек трябва да се грижи и за сигурността (не че такива няма!!!). Там, освен настройките за самата мрежа, трябва да има и секция Security: “Как да подсигурим нашият Windows”. Простичко, на български, с препратки да се напишат най-елементарни защитни мерки: първо, второ, трето ... Това няма да е полезно само за факултетските компютри. Може да има и секция “Как да оптимизираме?” Същото трябва да се направи и за Linux. А може би mailing list, където всеки да получава предупреждение (на български), точно, но кратко (понякога просто не ти се четат такива работи или си казваш, че няма да го разбереш). А форум? А хора, които да се занимават с това?

☺ ☺ ☺