Теми за Мрежова Сигурност - 1

Основни критерии за оценяване:
- Положителни:
  - За изчерпателност 10 т.
  - За точност 10 т.
  - За яснота на изложението 10 т.
  - За яснота и точност на обосновките 10 т.
- Отрицателни:
  - За правописни и стилистични грешки: до -5 т.
  - За фактологични грешки: до -5 т.
  - За липса на обосновка: до -10 т.
  - За едностранност (липса на изчерпателност): до -10 т.
  - За създаване на проблем: -15 т.

Важен момент за всички теми е сигурността на всяко ниво, физическо, мрежово и социално. Важно също така е да се обърне внимание на повечето съществуващи решения, не само на определени (например чисти Sun или Microsoft решения). Важно е да се обърне внимание на това, доколко мерките за сигурност ще пречат на нормалното използване на услугите.

Създаването на проблем означава неправилно използване на инструменти или начини за събиране на информация. Отнася се за X темите.

За изключително добри теми преподавателите си запазват правото да дадат до 10 допълнителни точки.

Проектите се предават на хартия И се изпращат по в PDF формат email на netsec2004-1@iseca.org. Самите проекти ще се публикуват на страницата на курса, заедно с оценката и кратка рецензия.

Проектите трябва да са поне 30 000 символа (с празните символи (интервал и табулация)), написани на грамотен български език.

За всеки проект трябва да се опише библиография на използваните източници.

Към всяка тема има приблизителен/препоръчителен план.

Повече информация за писането на самите теми може да се намери в [HCP].

Студентите могат сами да измислят тема, по която да си правят курсовия проект, след като я съгласуват с преподавателите.

Теми от Васил Колев <vasil@ludost.net>

Дефиниции:

Малка фирма - състои се от 30 човека. Занимава се с търговия с детски играчки. Има един офис.

Голяма корпорация - има 100 000 служители, има офиси в 15 държави на 3 континента. Занимава се с IT (за пример може да се използва IBM)

Военна структура (армия) - Армията на държава в Европа, притежаваща флот, сухопътни и въздушни войски, както и ядрено оръжие.

1. Сигурна електронна поща

Да се опишат различните съставни части на една сигурна система за електронна поща - клиенти, сървъри, протоколи, криптографски и други защити и вариантите за комбиниране/връзка м/у тях. Да се определят подходящи решения за следните различни варианти - домашен потребител, малка фирма, голяма корпорация, военна структура, и да се обосноват.

Примерен/препоръчителен план:

1. Обзор на потока на e-mail
1.1. Клиенти
1.2. Сървъри
1.3. Протоколи
1.4. Криптография и криптографска защита
1.5. Съвместимост
2. Домашен потребител
2.1. Изисквания към услугата
2.2. Нужно ниво на сигурност
2.3. Решение
2.3.1. Клиент
2.3.2. Сървър
2.3.3. Протоколи и криптография
2.3.4. Обобщение
3. Малка фирма
(дефинициите на малка фирма и т.н. са в началото на документа)
3.1. Изисквания към услугата
3.2. Нужно ниво на сигурност
3.3. Решение
3.3.1. Клиент
3.3.2. Сървър
3.3.3. Протоколи и криптография
3.3.4. Обобщение
4. Голяма корпорация
4.1. Изисквания към услугата
4.2. Нужно ниво на сигурност
4.3. Решение
4.3.1. Клиент
4.3.2. Сървър
4.3.3. Протоколи и криптография
4.3.4. Обобщение
5. Военна структура
5.1. Изисквания към услугата
- да могат да използват email за по-голямата част от комуникациите си, освен спешните.

5.2. Нужно ниво на сигурност
5.3. Решение
5.3.1. Клиент
5.3.2. Сървър
5.3.3. Протоколи и криптография
5.3.4. Обобщение

Трудност: 8/10
За 2 студента

2. Сигурен отдалечен достъп

Да се опишат вариантите за отдалечен достъп до услуги за печат, файлови сървъри, поща и бази данни през неосигурени мрежи. Да се опишат вариантите при 3 решения, изградени на база на различни производители. Да се определят разликите, ако се прави за малка фирма, корпорация и армия.

Примерен/препоръчителен план:

1. Обзор на услугата
1.1. Нужда за отдалечен достъп
1.1. Възможни типове решения
- Тези са дадени само като пример, не са задължителни!

1.2.1. Dial-up
1.2.2. VPN
1.2.3. Пряк достъп през Internet
1.3. Различни производители и решения

- Тези са дадени само като пример, не са задължителни!

1.3.1. Cisco
1.3.2. Microsoft
1.3.3. Free&Open Source Software
2. Малка фирма
2.1. Изисквания към услугата
2.2. Нужно ниво на сигурност
2.3. Решение
2.3.1. Клиент
2.3.2. Сървър
2.3.3. Протоколи и криптография
2.3.4. Обобщение
3. Голяма корпорация
3.1. Изисквания към услугата
3.2. Нужно ниво на сигурност
3.3. Решение
3.3.1. Клиент
3.3.2. Сървър
3.3.3. Протоколи и криптография
3.3.4. Обобщение
4. Военна структура
4.1. Изисквания към услугата
4.2. Нужно ниво на сигурност
4.3. Решение
4.3.1. Клиент
4.3.2. Сървър
4.3.3. Протоколи и криптография
4.3.4. Обобщение

Трудност: 9/10
За 3 студента

3. Сигурна мрежа за общежития

Да се опишат и обосноват 2 различни варианта за изграждане на сигурна мрежа в рамките на няколко блока, както и административните процедури, нужни за поддръжката на тази мрежа.

Примерен/препоръчителен план:

1. Обзор

- Имаме 6 блока, по 8 етажа, студентски общежития. Трябва да се предостави локална мрежа и достъп на студентите до Internet. Студентите учат основно в специалности, свързани с информатиката.

2. Нужни защити
2.1. Защити на локално ниво
2.2. Защити от външни атаки
2.3. Защита на Internet от изходящи от нас атаки
3. Администрация и процедури
3.1. Acceptable Use Policy (AUP)
3.2. Приемане на нов студент
3.3. Напускане на студент
3.4. Добавяне и махане на машина на студент
3.5. Принудително откачане на машина от мрежата
3.6. Правила за достъп до стаите/килерите с техника и окабеляване
3.7. Други
4. Първи вариант
5. Втори вариант

Трудност: 7/10
За 2 студента

4. Сигурност във фирма за разработка на софтуер

Да се опише системата за сигурност на различните услуги, използвани в средно голяма фирма за разработка на софтуер.

Примерен/препоръчителен план:

1. Обзор
- Средно голяма фирма (300 човека), занимаваща се с разработка на софтуер за embedded устройства и игри за PC пазара.

2. Нужди
2.1. Вътрешна (между-отделова) защита
2.2. Защита от външни заплахи
2.3. Защита от изтичане на информация
3. Защита на различните услуги
3.1. Source control
3.2. email
3.3. web service
3.4. Други
4. Административни
4.1. AUP
4.2. Правила за работа с мрежата на разработчици и др.

Трудност: 7/10
За 2 студента

5. Сигурен квартален доставчик на Internet

Да се опишат нужните услуги, които предоставя такъв доставчик (например пренос на данни, mail сървър, хостинг), нужните мерки за сигурност и процедури при работа с клиенти.

Трудност: 5/10
За 3 студента

6. Защита на информацията от откриване

Да се изгради защитена срещу откриване и подслушване стеганографска система за пренос на данни чрез Internet. Да се обоснове защитата й.

Трудност: 10/10
За 2 или 3 студента, решава се на място.

7. Система за следене на трафик

Да се опише и обоснове система за проследяване, подслушване и анализ на криптиран и некриптиран трафик, за използване в разузнавателни организации (подобна на Carnivore).

Трудност: 7/10
За един или 2 студента

x1. Да се провери сигурността на ФМИ

Да се провери сигурността на Факултета, достъпът и възможностите за промяна на информация на мрежово ниво, както и вариантите за защита. При проверката не трябва да остават следи. Информацията от това изследване ще се предостави на факултета.

Трудност: 8/10
За 3 студента

x2. Сигурност на доставката на Internet за България

Да се провери сигурността и самите външни канали за доставка на Internet за България, как могат да бъдат атакувани (на физически и мрежов слой), какво е нужно за допълнителна защита.

Трудност: 10/10
За 2 студента.

Теми от Петър Пенчев <roam@ringlet.net>:

1. Сигурна поддръжка и достъп до World-Wide Web

Да се опишат различните услуги и програми, използвани при създаване и достъп до съдържание, разпространявано чрез World-Wide Web. Особено внимание да се обърне на т.нар. active content от всички типове и мерките, които се вземат и при сървъри, и при клиенти за предотвратяване на пробиви в сигурността, предизвикани от active content.
[тази тема в три варианта:
- разглеждане от клиентската страна - 1 човек
- разглеждане от сървърната страна - 1 човек
- разглеждане от двете страни - 2 души]

Трудност 6/10

2. Сигурност при peer-to-peer реализации на file sharing

Да се опишат различните технологии за peer-to-peer file sharing (Napster, Kazaa и др.) и възможностите за атаки върху тях – подмяна на файлове, представяне на фалшиви "удостоверения за самоличност" (credentials), неправомерен достъп до ресурси на клиентския компютър (достъп до файловата система, изпълнение на код, ...) и други. Да се опишат мерките за защита, взети от различните file sharing системи, и възможностите за тяхното преодоляване.

За 2 студента
Трудност 7/10

3. Сигурност при реализации на file sharing от тип клиент-сървър

Да се опишат различните технологии за client-server file sharing (NFS, SMB, NetWare, ...) и възможностите за атаки срещу тях – подмяна на файлове, представяне на фалшиви "удостоверения за самоличност" (credentials), неправомерен достъп до ресурси на клиента или сървъра (достъп до файловата система, изпълнение на код, ...) и други. Да се опишат мерките за защита, взети от различните file sharing системи, и възможностите за тяхното преодоляване.

За 2 студента
Трудност 5/10

4. Сигурен достъп до Интернет в България

Да се разгледат различните методи за връзка с Интернет, предоставяни от българските доставчици (dial-up, ISDN, наета линия, residential LAN, ...). За всеки метод (евентуално и за различните доставчици, когато има разлики в начина на предоставяне на услугата) да се опишат възможностите на атакуващи лица, разположени на различни места (между клиента и доставчика, физически близо до клиента, физически близо до доставчика, споделен ресурс особено в случая на LAN и подобни, както и други възможности според методите), да подслушват и/или подменят трафика, както и да използват неправомерно ресурси на клиента или доставчика с помощта на придобитата информация.
[тази тема в три варианта:
- разглеждане от страна на потребител - 1 човек
- разглеждане от страна на доставчик - 1 човек
- разглеждане от двете страни - 2 души]

Трудност 8/10

5. Бърз анализ на трафик, преминал през мрежа

Да се създаде програма, която допълва работата на tcpdump <URL:http://www.tcpdump.org/> или WinDump <URL:http://netgroup-serv.polito.it/windump/>, като показва хостовете с най-голям обем на преминалия трафик в реално време. Входните данни може да се четат или от резултата от "tcpdump -w -", или директно с използване на libpcap, като и в двата случая потребителят указва интерфейса и незадължителни филтри.

През определен интервал от време, по подразбиране 5 секунди, програмата обновява съдържанието на екрана, като показва няколко (поне 10) IP адреса, от които или към които е бил изпратен най-много трафик сумарно от началото на работата на програмата до текущия момент, подредени по количество на трафика. Данните за всеки адрес съдържат общия размер на изпратен/получен трафик и времето (timestamp) на първия и последния изпратен или получен пакет.

След завършване на работата на програмата на стандартния изход или в указан от потребителя файл да бъде изведена статистика за активността на всеки IP адрес, който е изпращал или получавал пакети през това време. Статистиката да съдържа времето (timestamp) на първия и последния изпратен/получен пакет, както и общия размер на трафика, преминал през всеки IP адрес.

За 2 студента
Трудност 8/10

6. Детектор на ARP poisoning и ARP flood атаки

Да се напише програма, която следи трафика, пристигащ по един или повече мрежови интерфейси, и открива вероятни опити за ARP poisoning и ARP flood атаки. Според настройките (зададени в конфигурационен файл, но поддържащи промяна на параметри чрез команден ред и/или текстов/графичен интерфейс) програмата да може да работи в пасивен или активен режим: в пасивен режим следи и изпраща предупреждения, в активен режим да може да преустанови изпращането и получаването на мрежови трафик по атакуваните интерфейси в зависимост от възможностите на операционната система. Да се предвиди възможност за изпращане на различни видове предупреждения: системни журнални файлове (log files), известяване на един или повече потребители, които използват компютъра, изпращане на съобщения чрез e-mail и други.
Дават се bonus точки, ако приложението се компилира и работи на повече от 2 класа операционни системи.

За 1 студент
Трудност 9/10

7. Извличане на информация от PPP връзка

Да се създаде инструмент, който получава на стандартния си вход или чете от файл PPP пакети (фреймове), анализира ги и търси в потока информация за потребителски имена и пароли. Входната информация е представена като последователност от фреймове, форматирани по следния начин:

1 байт - маркер, байт 0x46 ('F')
1 байт - посока, 0 за клиент -> сървър, 1 за сървър -> клиент
2 байта - дължина на фрейма в байтове
- самият фрейм, както е описан в RFC 1661 (protocol/info/padding)

Резултатът от работата на инструмента трябва да бъде:
- списък от всички PPP протоколи, използвани във връзката;
- списък от всички предложени и приети PPP протоколи;
- списък от всички предложени и отхвърлени PPP протоколи;
- списък от всички auth credentials
- ако е възможно, списък от всички auth credentials, които могат да бъдат извлечени в "чист вид" (чист текст или нещо подобно, готово за използване от атакуващ)
- списък от всички предложени и приети IPCP, IPV6CP и NBFCP опции;
- списък от всички предложени и отхвърлени IPCP, IPV6CP и NBFCP опции.

За 2 студента
Трудност 9/10

8. Извличане на файлове от HTTP връзка [НОВА]

Да се създаде инструмент, подобен на filesnarf, urlsnarf и mailsnarf от пакета dsniff, който следи TCP/IP трафика по определен интерфейс, отделя HTTP връзките и запазва в зададена директория резултатите от заявките. Да се запазват само изцяло предадени файлове, т.е. частични трансфери (HTTP 1.1 Range) да бъдат игнорирани. В отделен файл да се записва информация за source/destination адреси и портове, HTTP content type и HTTP authorization за запазените файлове, като от HTTP authorization да се извлича колкото може повече информация (напр. потребителското име и паролата при Basic authorization).

Бонус: Инструментът да може да работи както с "истински" връзки между клиент и HTTP сървър, така и с

връзки, минаващи през proxy сървъри, като във втория случай да следи и файлове, поискани от клиента със схема 'ftp'.

За 2 студента
Трудност 9/10

Теми от Атанас Бъчваров <chervarium@sigbus.nove.bg>

1. Offices (WAN)

Фирма има делокализирана структура с няколко офиса из страната. Да се изготви решение за сигурни връзки между офисите с топология звезда (с един централен node, към който са закачени останалите) и граф (в WAN-а няма node, който е централен, тоест може да има връзки от всеки до всеки). Да се вземе предвид възможността за хетерогенност на така изградения WAN (различни операционни системи). Да се направи проучване за ефективността на така предложените решения.

Трудност: 10/10
За 2 студента

2. Print servers

Да се направи проучване и да се напише paper за сигурността на наличните на bg пазар print сървъри (да се провери в ценовите листи на големите дистрибутори на хардуер и да се подберат 3 модела). Да се подбере модел с най-добро съотношение на качество/цена и сигурност/цена като възможен за изграждане на print решение. Print server е такъв standalone device, в който може да се включи принтер и мрежов кабел и експортва принтера в локална мрежа по няколко възможни протоколи за печат (UNIX System V lp/BSD lpd, Novell Netware, Windows, ...).

Трудност: 9/10
За 2 студента

Теми от Николай Недялков <nikolay@nedyalkov.com>

1.Управление и защитата на корпоративна поща

Целта на темата е да се изследват възможностите за изграждане и управление на сигурна и надеждна корпоративна електронна поща и instant messaging системи.

Темата включва наблюдение, изследване и решения на проблеми свързани с засичането на спам, вируси и троянски коне, изграждане на правилници за ползване и работа с електронна поща както и Instant Messaging.

Очаква се по темата да работят група от 2 до 4-ма студенти.
Като ключови или възлови моменти се очертават следните изисквания:

Направата или използването на вече направена централизирана система за управление на потребители и потребителски групи във фирмата или корпорацията.

Примери: Може да се предположи, че имат изградена инфр. с windows domain controller или се използва произволен LDAP / Active Directory. Идеята е пощата и комуникациите да работят с потребители и правата им (доколкото е възможно) именно чрез LDAP, AD, Windows DC ...

От друга страна като резултат от разработката се очакват набор от кратки документи или приложения, които описват дадена процедура по работа с ел. поща, или правилник за използване на IM и други необходими документи.

Разработката трябва да е ориентирана към това как реално фирмите могат да спестят време, пари, да осуетяват и правно въздействат посредством:
- Намаляване до минимум на нежеланата поща без загуба на нормални писма
- Защита на instant messaging

- Създаване на план за реагиране при инциденти
- Бързо и ефективно овладяване на атаките с вируси по ел.поща
- Да отговаря на законите и стандартите за запазване на конфиденциалността на личните данни и за запазване на архивни копия.
- Осигуряване на конфиденциалността и за в бъдеще
- Обучаване на персонала за различните практики за сигурна комуникация
- Реализиране на лесна за ползване и сигурна система през мобилни мрежи (например емайл през WAP, ssl/vpn в/у GPRS ...)

Конкретни приложения (подтеми) :

Приложение A: Създаване на ефективни и надеждни процедури и програми по архивиране и складиране на ел. поща

Приложение B: Защита на комуникацията и използването на електронна поща на отдалечени потребители.

- Защита на ниво протоколи за електронна поща - SMTP, POP3, IMAP
- Възможности и най-добри практики за тунелиране на обмена на поща през различни сигурни протоколи и механизми, като SSL или чрез S/MIME

Приложение C: Програми и средства за преодоляване на измамите и "Phishing" атаките с ел. поща.

- Какво е "Phishing" атака ? На какво се разчита при нея и методи за защита?
- Конкретни практики при изграждане на инфраструктурата на корп. ел. поща
- Филтри по съдържанието, по формата на съобщението, по източника и т.н.
- Документи, указващи и регламентиращи правилата по които да се третират и преодоляват такъв вид атаки
- други

Приложение D: Как да направим Instant Messaging сигурен и как да реализираме мониторинг.

- Какво е Instant Messaging (IM)?
- Съществуващ софтуер и възможности за реализация
- Конкретни практики при изграждане на инфраструктурата на корп. IM
  Инсталиране, конфигуриране и интегриране на софтуера
  Подсигуряване и защита на комуникационните канали
  Мониторинг и управление на комуникациите - logs и т.н.

Трудност: 8/10
За 4 студента

*Ще се доуточнят въпросите и конкретните приложения съвместно с екипа на мрежова сигурност, при желание за разработка на проекта.

2. Certification Authority

Да се направи план с обосновка за изграждане на CA. Да се опишат основните процедури.

Приема се, че става въпрос за изграждане на CA на територията на Република България)

Примерен/препоръчителен план:

[да се допише от Недялков]

Трудност: 9/10
За 2 студента

Библиография

[НСР] Васил Колев, “Как се пише курсова работа за курса по мрежова сигурност”,
http://vasil.ludost.net/pisaniq/howto-cp.pdf

[tcpdump] The TCPDump tool,
http://www.tcpdump.org/

[windump] tcpdump for Windows,
http://netgroup-serv.polito.it/windump/