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 netsec-projects@nedyalkov.com. 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].

Теми от Васил Колев <vasil(at)ludost(dot)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. Сигурна услуга за печат

Да се опишат различните варианти за печат и проблемите на сигурността им. Да се опишат и обосноват решения за малка фирма, голяма корпорация, военна структура.

Примерен/препоръчителен план:

1. Обзор на услугата
1.1. Типове клиенти
1.2. Типове крайни устройства
- цветни, черно-бели, лазерни и мастилено-струйни принтери, плотери, и т.н.

1.3. Сървъри и протоколи за работа с тях
1.4. Поддръжка на криптография
1.5. Съвместимост
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: 3/10
За 1 студент

3. 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

4. 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

5. 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

6. 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

7. Защита на ethernet мрежи

Да се разработят концепция и да се реализира съвкупност от софтуерни инструменти за защита от различните атаки на ethernet мрежи, изградени от обикновени swtich-ове и hub-ове. Решението трябва да поддържа поне 4 различни операционни системи и да няма сериозно отражение в/у използваемостта на мрежата. Да се напише ясна обосновка на сигурността на решението и концепцията.

Трудност: 6/10
За 2 студента
(софтуерен проект и тема)

8. 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.

9. 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:

1. Обзор на проекта
1.1. Цели на CA
1.2. Смисъл на CA
2. Нужди
2.1. Физически
2.2. Технически
2.2.1. Хардуерни
2.2.2. Софтуерни
2.3. Социални
3. Решение
3.1. Физическо
3.2. Техническо
3.3. Социално
3.4. Правила
3.5. Процедури
3.5.1. Подписване на ключ
3.5.2. Revocation на подпис
3.5.3. Смяна на master ключа за подписване
3.5.4. Други

Трудност: 9/10
За 2 студента

10.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.

Трудност: 7/10
За един или 2 студента, решава се на място

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(at)ringlet(dot)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.

[чудя се кое ще е по-добре: да разделим тази тема на две (клиенти и сървъри), да я дадем на повече от един човек, или и двете (да имаме три теми - една за клиенти, една за сървъри, и една обща за екип)]

Трудност: 7/10
За 1 или 2ма, в зависимост от разделението.

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.

Трудност: 8/10
За 1 или двама човека, преценява се на място.

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.

Трудност: 8/10
За 2 студента.

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.

[и тук, както при първия въпрос, се чудя за трите варианта - да го разбием за клиент и доставчик и/или да го дадем на няколко души]

Трудност: 7/10
За 1 или 2 студента, в зависимост от разделението.

Теми за софтуерни проекти

5. Бърз анализ на трафик, преминал през мрежа

Да се създаде инструмент, който допълва работата на [tcpdump] или [windump], като взима за входни данни файлове, съдържащи запис на преминал трафик (tcpdump -w), и прави 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.

При избора на език за програмиране и използвани библиотеки да се поддържа възможност за компилация на поне 3 различни класа операционни системи/архитектури.

Трудност: 5/10
За 1 студент

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.

[тук не ми се иска да подсказвам много, но имам предвид firewall и/или събаряне на интерфейса down]

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.

При избора на език за програмиране и използвани библиотеки да се поддържа възможност за компилация на поне 3 различни класа операционни системи/архитектури.

Трудност: 8/10
За 1 студент

7. Добавяне на диагностични възможности към популярни софтуерни продукти

Да се разширят входните данни (команди, заявки) на един от изброените по-долу програмни продукти по указания начин, като се предостави възможност извършване на поне три от следните дейности:

- READ fname [start [end] [unit]]
  четене на цял файл или на зададен фрагмент от него; незадължителните параметри start и end (цели числа) задават съответно началото и края на фрагмента, а unit (символ) задава единиците - 'l' за редове, 'c' или 'b' за символи/байтове, 'k' за килобайти, 'm' за мегабайти. Ако start или end започват със знак '-', позицията се пресмята от текущия край на файла.
- WRITE fname start unit truncf string
  запис на последователност от байтове от определена позиция на файла нататък. start и unit имат същото значение като при READ, truncf е цяло число - ако е различно от нула, файлът трябва да бъде съкратен (truncated) непосредствено до края на записания низ, т.е. записаните символи да се окажат последните символи във файла.
- LIST dirname
  извеждане на списък на файловете в дадената директория и информация за тях във формат, зависещ от операционната система и използваните библиотеки.
- EPLF dirname
  извеждане на списък на файловете в дадената директория и информация за тях във формат EPLF, описан от Prof. Daniel J. Bernstein в [eplf].
- MLST dirname
  извеждане на списък на файловете в дадена директория и информация за тях във формат MLST, описан в [eftp].
- EXEC progname [args...]

изпълнение на външна програма, като ако тя извежда данни на стандартния изход, те трябва да бъдат предадени на клиента като отговор на командата.

- EXSH [program-path]
  изпълнение на интерактивен команден интерпретатор (command shell) (само ако е приложимо за програмата). Всички данни, постъпили от клиента в същата сесия, се предават на командния интерпретатор или на програмите, изпълнени от него, като стандартен вход; всички данни, изведени от командния интерпретатор или програмите, изпълнени от него, на стандартния изход или стандартния изход за грешка, се предават на клиента.

Програми:

- Sendmail SMTP server: добавяне на команда DBUG с първи параметър командата и последващи евентуално параметри на командата; пример: DBUG LIST /tmp
- qmail SMTP server (qmail-smtpd): аналогично;
- Microsoft Exchange 2000 или 2003 SMTP server: аналогично
  [тук трябва някой, който се е занимавал с Exchange или нещо такова, или поне знае къде може да се прочете, да каже дали това изобщо е възможно: можеш ли да си напишеш модулче за Exchange, което да добави команда?]
- ProFTPd FTP server: аналогично добавяне на FTP команда DBUG;
- wu-ftpd FTP server: аналогично;
- Microsoft IIS FTP server: аналогично
  [и тук някой, който си е играл с IIS/FTP, да каже дали може]
- Microsoft IIS HTTP server: аналогично
  [тук съм 95% сигурен, че е възможно, но все пак не напълно.. ISAPI май дава доста възможности; дава ли възможност и за това?]
- BIND DNS server/resolving cache: специална обработка на заявки за записи тип 'A' за top-level domain 'dbg'. Второто ниво на hostname е командата, от третото нататък започват незадължителните параметри;
  пример: /tmp.list.dbg
- tinydns DNS server: аналогично;
- dnscache DNS resolving cache: аналогично;
- Microsoft DNS server/resolving cache: аналогично
  [тук *изобщо* не съм сигурен дали е възможно... но все пак да го дадем, пък те да си решат дали ще го правят :]
- OpenSSH SSH server: специална обработка на SSH2_MSG_IGNORE пакет, който има данни, започващи с DBUG; форматът на командата и параметрите в данните са аналогични на тези за SMTP и FTP.
- ssh.com SSH server: аналогично.

Трудност: 8/10
За 1 студент, за всеки различен сървър

Теми от Светлин Наков <svetlin(at)nakov(dot)com>

1. Защитни стени (firewalls):

   Примерен/препоръчителен план:
   1. Технически преглед - технологии, хардуер, софтуер, начин на работа, приложение
   2. Инсталиране и конфигуриране:
   2.1. Със специализиран хардуер - например Cisco
   2.2. под Linux
   2.3. под Windows
   2.4. под други ОС
   3. Принципи за правилно конфигуриране на firewalls
   3.1. Изграждане на двоен firewall и firewalls на повече нива
   3.2. Препоръки за правилна настройка за всеки от отделните протоколи
   4. Възможни атаки и начини за защита от тях

   Трудност: 8/10
   За 1 студент

2. SPAM и системи за защита от SPAM:

   Примерен/препоръчителен план:
   1. Технически преглед - технологии, начин на работа на mail услугата в Интернет, протоколи, приложение

2. Филтри за SPAM
2.1. По съдържание
2.2. Според изпращача
2.2.1. Начини за проверка на изпращача
2.3. Черни списъци на спамерите
3. Инсталиране и конфигуриране на различните видове филтри за SPAM към масово използваните mail-сървъри:
3.1. qmail
3.2. sendmail
3.3. MS Exchange
4. Възможни начини за заобикаляне на SPAM филтрите
4.1. Заобикаляне на филтрите по съдържание. защита
4.2. Заобикаляне на филтрите по изпращач. защита

Трудност: 6/10
За 1 студент

Теми от Атанас Бъчваров <chervarium(at)sigbus(dot)nove(dot)bg>

1. LAN

Да се проектира локална мрежа от тип ethernet и възможност за 100 машини в нея като се съблюдава съществуването на различните уязвимости и съответно решаването (или поне намаляване на неприятните ефекти) на всяка от тях в рамките на проектираната мрежа.

Трудност: 6/10
За 1 студент

2. 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

3. 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

Библиография

[HCP] 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/

[eplf] Easily Parsed LIST format,
http://cr.yp.to/ftp/list/eplf.html

[eftp] Extensions to FTP,
http://www.ietf.org/internet-drafts/draft-ietf-ftpext-mlst-16.txt