СУ "Св. Климент Охридски"

Мрежова сигурност I

(изборен курс към ФМИ на СУ, зимен семестър, 2004/2005 г.)

Преподавателски екип:

Николай Недялков security-course@nedyalkov.com	**Георги Чорбаджийски** georgi@unixsol.org	**Йордан Димов** jdimov@nsegcorp.org
Георги Георгиев cTaPnEc@gmail.com	**Васил Колев** vasil@ludost.net	**Петър Пенчев** roam@ringlet.net
Александър Велин velin@zadnik.org	**Атанас Бъчваров** nasko@nove.bg	

Анотация:

Курсът "Мрежова сигурност" е предназначен за студенти във ФМИ на СУ, които се интересуват от основните концепции за сигурност в Интернет и локални компютърни мрежи. Курсът има за цел да запознае аудиторията със сигурността при различни платформи, като Win32, UNIX и др. Разглеждат се инструменти за откриване на пробиви и потенциални уязвимости, локални и отдалечени атаки. Обръща се внимание на сигурността на основни услуги в Интернет, като SMTP (email), HTTP (WWW) , FTP и др., както и мерките за предотвратяване на потенциални пробиви в тях. Разглежда се теорията на някои основни уязвимости, експлойти, криптография и физически атаки. Дават се конкретни съвети и препоръки за предпазване от потенциални атаки.

Изисквания към студентите:

- Основни познания по ***компютърни мрежи***, ***организация на Интернет*** и ***системно програмиране***
- Владеене на ***английски език*** – част от учебните материали са на английски език
- Курсът е предназначен за всички специалности

Изпити и оценки:

Изпитът ще се състои от два теста и задължителен проект. Тестовете ще представляват 30 въпроса върху предавания материал. Съгласно тази система за оценяване от един
тест могат да се спечелят до 30 точки, а от двата теста общо - до 60 точки. Проектът е задължителен, като ще се даде възможност на студента да избира между софтуерна разработка и и писмена разработка по предварително зададена тема. Темите най-вероятно няма да се преподават на курса или ще изискват допълнителна и по-подробна информация, относно поставения проблем.
Проекта носи 40 точки.

Точки	Оценка
50 – 59	Среден 3
60 – 69	Добър 4
70 – 79	Мн. добър 5
80 - 100	Отличен 6

Дни и часове на провеждане:

Всеки вторник и четвъртък в зала 325 на ФМИ от 19.00 до 21.00 часа

Учебна програма:

1. Въведение - Какво е мрежова сигурност?
Разглеждат се концепциите, които са залегнали в основата на Интернет, а именно протоколи, услуги и информация. Дефинират се понятията уязвимост, информационен риск, хакер, кракер, както и чисто психологични аспекти на информационната сигурност

1.1 Основи на Интернет. Протоколи. Услуги. Информация.
1.2 Какво означава уязвимост в системата?
1.3 Какви са рисковете?
1.4 Какво е хакер,кракер, атакуващ и т.н. ?
1.5 Защо точно нас? (психологията на лошите хора)
1.6 Разлика между инструменти и намерения.

2. Криптография.
Представят се основите на криптографията, както и по известни алгоритми за кодиране и хеширане. Специално внимание се отделя на приложенията на криптографията в смисъла на PKI и web-of-trust (PGP)

2.1 Основи на криптографията.
2.2 Преглед. Криптографски алгоритми. SSL, RC4, MD5, PGP
2.3 Приложения на криптографията - web-of-trust (PGP),PKI

3. Datalink Layer security threats.
Разглеждат се основните протоколи на datalink слоя, пряко свързани с преносните си среди - PPP, ethernet, безжични мрежи (801.11), DOCSIS (по кабелни мрежи за пренос на телевизионен сигнал), VPN мрежи, както и мрежи за управление на специални устройства.

3.1 PPP
3.2 Ethernet
3.3 Wireless мрежи
3.4 DOCSIS
3.5 CAN, LIN
3.6 IP,TCP,UDP
3.7 VPN

4. Network, transport layer
Разглеждат се протоколите на мрежовия и транспортния слой, IP, TCP, UDP, и проблемите на сигурността, свързани с тях.

5. Операционни системи.
Разглеждат се основните принципи на операционните системи, след което се обясняват проблемите при Microsoft базираните, unix базираните, и някои специфични операционни системи, ориентирани към реално-времеви приложения или специфични устройства.

5.1 Основни принципи на операционните системи
5.2 UNIX операционни системи
5.3 Microsoft OSes
5.4 Real-time OSes, embedded OSes

6. Основни услуги и предоставящите ги сървери.
Разглеждат се основните протоколи, предоставящи услуги в Internet - DNS, пощенски такива, такива за пренос на файлове, както и някои използвани в Peer-to-peer мрежи и такива за отдалечено изпълнение на процедури (RPC)
6.1 DNS
6.2 SMTP,POP3,IMAP
6.3 FTP
6.4 HTTP
6.5 P2P протоколи
6.6 RPC/DCOM

7. Auditing tools
Разглеждат се инструменти за откриване на познати проблеми по сигурноста - различни скенери и анализатори.

8. Отдалечено администриране
Разглеждат се средства за отдалечена администрация на различни отдалечени системи - текстово-ориентирани, графично-ориентирани, и такива за наблюдение и контрол на крайни устройства.
8.1 Windows NT Terminal Server/2000/XP/2003
8.2 X Window
8.3 Network monitoring и администрация (snmp, tftp, syslog)
8.4 Web administration
8.5 Text console terminal sessions
8.6 Multi Platform

9. Автоматизиран back-up на файлови системи
Обясняват се основните принципи и средства да се постигне по-добра защита на данните от потребителска намеса или проблеми с техниката.
9.1 Security включва и reliability!
9.2 Що е то файлова система и защо не е просто "IDE partition" ?
9.3 Начини за backup: dump/restore, tar/zip/pax, dd, MS Backup
9.4 Къде да backup-ваме: локални файлове, магнитна лента,network
9.5 backup
9.6 Автоматизиран back-up: dump/restore, amanda

10. Отдалечени атаки.
Разглеждат се протичането на една отдалечена атака. Какви средства и действия са необходими. Начини за защитата и предотвратяване на такъв тип атаки.
10.1 Нива на атака.
10.2 Средства за защита, "Firewalls".
10.3 Spoofing.
10.4 Други отдалечени атаки.

11. Pluggable Authentication Modules.
Описва се идеята на модулната идентификационна система PAM.
11.1 Основни идеи и малко история (още една добра идея от Sun).
11.2 Инсталация и конфигуриране.
11.3 Поддръжка в различни програми: login, su, sudo, sshd и др
11.4 Готови PAM модули: plaintext, password file, OTP,
11.5 db,Kerberos, etc.
11.6 Примерна програма, използваща PAM
11.7 Примерен PAM модул

12. Single sign-on.

Описват се методи за идентификация от типа single sign-on (като Kerberos).

12.1 Дефиниция.
12.2 Active Directory
12.3 Взаимодействие между Active Directory и Kerberos
12.4 SSO auth за web sites: NTLM, SPNEGO (Kerberos, AD)

13. One-time passwords.

Описват се методи за идентификация с пароли за еднократна употреба.

13.1 Основна идея - Преодоляване на sniffer-ите и replay attacks!
13.2 Реализации - S/Key, logdaemon, OPA, OPIE
13.3 Поддръжка в различни програми: PAM, login, su
13.4 Примерна програма, използваща OPIE

14. Active Directory 2003 и .NET

14.1 ADSI
14.2 Authorization Manager
14.3 Примерени програми използващи ADSI и Authorization Manager
14.4 Други примери

Първа сбирка:

5.10.2004 (вторник) – 19 ч., зала 325, ФМИ

За повече информация:

http://netsec.iseca.org/