



Факултет: ФАКУЛТЕТ ПО ТЕЛЕКОМУНИКАЦИИ И МЕНИДЖМЪНТ

Катедра: ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

Професионално направление: 5.3. КОМУНИКАЦИОННА И КОМПЮТЪРНА ТЕХНИКА

Специалност: КИБЕРСИГУРНОСТ НА ВИСОКИТЕ ТЕХНОЛОГИИ

Образователно-квалификационна степен: ПРОФЕСИОНАЛЕН БАКАЛАВЪР

ОПИСАНИЕ НА ЛЕКЦИОНЕН КУРС

1. Наименование на курса: *Практикум по защита на сървъри*

2. Код на курса: P.18.044.1

3. Вид на курса: *задължителна*

4. Ниво: *професионален бакалавър*

5. Година на изучаване: *трета*

6. Семестър: 6

7. Брой кредити: 3

8. Име на лектора: *гл. ас. д-р инж. Страхил Соколов*

9. Резултати от обучението за дисциплината

Целта на курса е да предостави на студентите от спец. КСВТ на ВУТП практически умения за защита на сървърни ОС и уеб сървъри.

Студентите, приключили обучението си по дисциплината, *трябва да придобият:*

Основни знания за за способите за защита на сървъри от различни видове атаки.

Практически умения за конфигурация и предотвратяване на разнородни атаки..

Компетенции:

- конфигуриране на сървър и компоненти за съвместимост с политики за защита;
- създаване на политики за защита;
- организиране на дейности по управление на защита на сървър.

10. Начин на преподаване:

Обучението по дисциплината „Практикум по Защита на сървъри“ се извършва през шести семестър съгласно действащия учебен план на специалност КСВТ чрез практически упражнения, групирани в блок от 3 часа в продължение на семестъра.

Практически упражнения се провеждат по класическия начин като студентите се запознават последователно с предвидения материал. Твърденията се илюстрират с примери, които максимално улесняват работата на студентите в упражненията. Практическите упражнения се провеждат в лаборатория или на собствен компютър на студента, снабдени с необходимото оборудване – хардуер и сървърна операционна система. Преди всяко практическо занятие студентите са информирани за необходимостта от предварителна подготовка по съответната тема.

11. Предварителни изисквания:

Студентите следва да имат задълбочени познания в ОС Linux, Основи на Windows, Web сървъри, Балансиране на мрежово натоварване.

Курсове, ползващи дисциплината са: Разработване на дипломна работа.

12. Съдържание на курса:

Курсът „Практикум по защита на сървъри“ за спец. КСВТ на ВУТП съдържа три раздела. В Раздел 1 е представена Защита на Linux сървъри. Следните модули са част от предвиденото практическо обучение: Управление на потребители и мрежи. Защита на поверителни потребителски данни. Управление и защита на система за съхранение на данни. Облачни технологии и конфигуриране на защитни стени. Управление и защита на хипервайзор и приложения в контейнери. Управление защита на инструменти за трансфери споделяне на поверителни данни. DNSSEC и защита от DDoS атаки. Изгражданена система за наблюдение. Управление и защита на услуги за централизирано удостоверяване чрез автоидентификация и оторизация. Управление на VPN, SSH и TOR услуги. В раздел 2 е представена Защита на Windows сървъри: Инсталация и управление на потребители. Управление и криптиране на дисково пространство. Управление на сървърни роли. Управление и защита на хипервайзор и контейнери под Windows. Изграждане на система за наблюдение. Раздел 3 представя Защита на WEB сървъри със следните подтеми: Управление на Apache httpd. Управление на nginx. Инсталация и конфигурация на модули. Управление на IIS7.0 IIS7.5. Инсталация.

Управление на роли. Инсталиране на модули. Терминирание на SSL/TLS. Изграждане на система за наблюдение, изграждане на политики за сигурност и инструменти за проверка на защитата.

13. Библиография

Основна литература:

1. Chris Binnie, "Linux Server Security: Hack and Defend", ISBN 1119277655, 9781119277651, ISBN 1119277655, 9781119277651
2. Jordan Krause, "Windows Server 2016 Security, Certificates, and Remote Access Cookbook: Recipe-based guide for security, networking and PKI in Windows Server 2016", ISBN 1789135222, 9781789135220, Packt Publishing Ltd, 2018
3. Gerardus Blokdyk, "Server Security a Complete Guide - 2020 Edition", ISBN 1867344688, 9781867344681, Emereo Pty Limited, 2020

Допълнителна литература:

1. Axel Buecker, Kent Browne, Louis Foss, Jaco Jacobs, Vladimir Jeremic, Carsten Lorenz, Craig Stabler, Joris Van Herzele, IBM Redbooks, "IBM Security Solutions Architecture for Network, Server and Endpoint", ISBN 0738435430, 9780738435435, IBM Redbooks, 2011
2. Gerardus Blokdyk, "Server Security Complete Self-Assessment Guide", ISBN 0655521291, 9780655521297, Emereo Pty Limited, 2019
3. John R. Vacca, "Cyber Security and IT Infrastructure Protection", ISBN 0124200478, 9780124200470, Syngress, 2013

14. Методи и критерии на оценяване:

Окончателната оценка по дисциплината се оформя чрез финален тест. Писменият тест обхваща отворени и затворени въпроси върху материала, посочен в конспекта и представен на лекциите по дисциплината.

Критериите са: изчерпателност, точност и задълбоченост при отговаряне на поставените въпроси в теста.

Тестът по дисциплината се състои от до 60 въпроса. Оценява се отговора на всеки въпрос от теста. Изчерпателно, точно и задълбочено развиване на един въпрос от теста се оценява с 10 точки. Максимален брой точки – 100.

Получената оценка от текущ контрол (формира се от точките от практическите упражнения и проведените контролни работи за проверка на теоретичната и практическата усвояемост) и оценката от писмения изпит се трансформират в крайна оценка по шестобалната система.

4.5.2. Формиране на крайната оценка

Формирането на крайната оценка се оформя чрез оценка от писмения тест и оценка от текущ контрол (точки от лабораторните упражнения и проведените контролни работи за проверка на теоретичната и практическата усвояемост).

Формирането на оценка в курса на обучение на всеки от посочените етапи, съобразно получени точки и подредбата им по шестобалната система е дадено в Таблица 1.

Таблица 1.

Брой точки	Оценка по шестобалната система
0 – 20	Слаб 2 (F)
20 – 39	Слаб 2 (FX)
40 – 49	Среден 3,00 (E)
50 – 59	Среден 3,00 (D)
60 – 69	Добър 4,00 (C)
70 – 84	Мн. добър 5,00 (B)
85 – 100	Отличен 6,00 (A)

15. Език на преподаване: Български