МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)

М. В. Афанасьєв

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ТА ЕТИЧНИЙ ХАКІНГ

робоча програма навчальної дисципліни

Галузь знань	**12 "ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ"**
Спеціальність	**125 "КІБЕРБЕЗПЕКА"**
Освітній рівень	**другий (магістерський)**
Освітня програма	**КІБЕРБЕЗПЕКА**

Вид дисципліни	**базова**
Мова викладання, навчання та оцінювання	**українська**

Завідувач кафедри *кібербезпеки та інформаційних технологій* Євсеєв С.П.

Харків
ХНЕУ ім. С. Кузнеця
2019

ЗАТВЕРДЖЕНО
на засіданні кафедри Кібербезпеки та інформаційних технологій
Протокол № 6 від 10.12.2019 р.

Розробник:
Шматко О.В., к.т.н., доц. кафедри КІТ

Лист оновлення та перезатвердження робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

1. Вступ

Навчальна дисципліна "Тестування на проникнення та етичний хакінг" є базоою та вивчається згідно з навчальним планом підготовки фахівців другого освітнього ступеня "магістр" спеціальності 125 "Кібербезпека" всіх форм навчання.

Анотація навчальної дисципліни: Дисципліна "Тестування на проникнення та етичний хакінг" є базовою навчальною дисципліною за спеціальністю “Кібербезпека”. Вона викладається у другому семестрі магістратури в обсязі 120 год.(4 кредита ECTS), зокрема: лекції – 20 год., лабораторні – 20 год., самостійна робота – 80 год, консультації – 4 год. У курсі передбачено два змістових модулі та одна модульна контрольна робота. Завершується дисципліна заліком.

Предметом навчальної дисципліни є основні поняття та методи тестування на проникнення, навики збору інформації та тестування вразливостей операційних систем Windows та Linux за допомогою інструментів з відкритим кодом.

Метою навчальної дисципліни є підготовка фахівців, в області інформаційної безпеки, безпеки телекомунікаційного забезпечення, і мобільних пристроїв, а також фахівців з тестування на проникнення та етичного хакінгу.

Головне завдання курсу – освоєння принципів та методів збору цифрової інформації для дослідження вразливостей операційних систем Linux та Windows, проведення статичного аналізу вразливостей інформаційних систем, використовуючи інструменти та методи тестування на проникнення.

У результаті вивчення навчальної дисципліни студент повинен **знати**:

- теоретичні основи і сучасні інформаційні технології тестування на проникнення та етичного хакінгу;
- особливості проведення тестування на проникнення ОС Windows, Linux;
- принципи роботи інструментів тестування на проникнення Kali Linux;
- сучасний стан і шляхи розвитку методів та технологій етичного хакінгу;

вміти:

- встановлювати і настроювати програмне забезпечення для тестування на проникнення;
- Виконувати пошук та аналіз вразливостей інформаційних систем;
- застосовувати Kali Linux;
- самостійно виконувати збір та аналіз цифрової інформації для етичного хакінгу;
- розробляти методи реагування та випадки порушень кібербезпеки;
- застосовувати інструменти тестування на проникнення для організації захисту даних в ОС Windwos, Linux;

Курс	**5**	
Семестр	**2**	
Кількість кредитів ECTS	**4**	
Аудиторні навчальні заняття	**лекції**	**20**
	семінарські, практичні	**-**
	лабораторні	**20**
Самостійна робота		**80**
Форма підсумкового контролю	**залік**	

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	**Наступні дисципліни**
Математичні основи криптології	Основи криптографічного захисту

2. Компетентності та результати навчання за дисципліною:

Загальні компетентності	**Результати навчання**
КЗ 1. Здатність застосовувати знання у практичних ситуаціях (Здатність до застосування концептуальних знань та певних знань сучасних досягнень у професійній діяльності)	РН-1. Застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки;
КЗ 2. Знання та розуміння предметної області та розуміння професії. (Здатність розуміти сутність та соціальну значущість майбутньої професійної діяльності, виявляти стійкий інтерес до неї)	РН-2. Проектувати майбутню професійну діяльність з урахуванням її значущості для громадянина та держави, а також напрямків розвитку інформаційної та кібербезпеки;
КЗ 6. Здатність до пошуку, обробки та аналізу інформації з різних джерел. (Здатність до самостійного пошуку, аналізу, синтезу та використання інформації, необхідної для ефективного розв'язання професійних завдань.)	РН-6. Використати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
Фахові компетентності	Результати навчання
КФ 1. Здатність використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо здійснення професійної діяльності	РН-15. Діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних; готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки;
КФ 2. Здатність до використання інфор-	РН-16. Здійснювати професійну діяль-

маційних і комунікаційних технологій	ність на основі знань сучасних інформаційно-комунікаційних технологій; застосувати програмні засоби, навички роботи в телекомунікаційних та комп'ютерних мережах; використати спеціалізовані комп'ютерні програми в професійній діяльності. Обирати відповідну технологію програмування, виконати аналіз специфікації задач; виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування;

3. Програма навчальної дисципліни

Змістовий модуль 1. Основи етичного хакінгу

Тема 1: Введення в етичний хакінг

Що таке етичний хакінг? Чому використовується поняття етичного хакінгу? Яка мета етичного хакінгу. Обмеження та труднощі застосування методів тестування на проникнення.

Тема 2: Методологія тестування на проникнення

Стандарти тестування на проникнення

Тема 3: Основи етичного хакінгу

Збір цифрової інформації. Пошук DNS. Пошук піддоменів.

Тема 4: Інструменти збору інформації для тестування на проникнення

Інструменти доменів. Збір інформації про сайти - Konckpy. Nmap – Network Security Scanner.

Змістовий модуль 2. Спеціалізоване програмне забезпечення для тестування на проникнення

Тема 5: Базові методи використання спеціалізованого програмного забезпечення

Огляд розділів інструментів Kali Linux. Коротка характеристика всіх розділів. Інструменти для збору інформації. Кращі хакерські програми. База даних експлойтів від Offensive Security (творців Kali Linux)

Тема 6: Тестування на проникнення бездротових мереж.

Кращі сумісні з Kali Linux USB Wi-Fi адаптери. Тестування Wi-Fi пароля (WPA / WPA2), використовуючи pyrit і cowpatty в Kali Linux. Тестування Wifi WPA / WPA2 паролів з використанням Reaver. Модифікація ФОРКОМ Reaver - t6x - для використання атаки Pixie Dust. Тестування паролів WPA2 / WPA за допомогою Hashcat в Kali Linux (атака перебором Wi-Fi паролів по масці). Мод Wifite з підтримкою Pixiewps. Тесту-

вання Wi-Fi мереж: інструменти, які не були в Kali Linux. Router Scan by Stas'M на Kali Linux (злом роутерів і Wi-Fi в промислових масштабах). Стрес-тест бездротової мережі з Wifi_Jammer: як глушити Wi-Fi. Стрес-тест бездротової мережі з Wifi_DoS.

Тема 7: Стрес-тести мережі

Стрес-тест мережі (DoS веб-сайту) з SlowHTTPTest в Kali Linux: slowloris, slow body і slow read атаки в одному інструменті. Стрес-тест мережі: DoS веб-сайту в Kali Linux з GoldenEye. Стрес-тест мережі з Low Orbit Ion Cannon (LOIC). Стрес-тест мережі: DoS з використанням hping3 і Спуфінга IP в Kali Linux

Тема 8: Аналіз вразливостей в веб-додатках

Інструкція по WhatWeb: як дізнатися движок сайту в Kali Linux. SQL-ін'єкції. Використання SQLMAP на Kali Linux: злом веб-сайтів і баз даних через SQL-ін'єкції. Сканування на уразливості WordPress: WPScanner і Plecost. Робота з W3af в Kali Linux. ZAProxy: тестування на проникнення веб-додатків. DIRB: пошук прихованих каталогів і файлів на веб-сайтах.

Лабораторні роботи

Тема 5

Лабораторна робота 1. Встановлення та настройка Kali Linux

Лабораторна робота 2. Встановлення та настройка Metasploit

Тема 6

Лабораторна робота 3. Тестування паролів WPA2 / WPA за допомогою Hashcat в Kali Linux

Тема 7

Лабораторна робота 4. Стрес-тест мережі (DoS веб-сайту) з SlowHTTPTest в Kali Linux

Тема 8

Лабораторна робота 5. Сканування на уразливості WordPress: WPScanner і Plecost. Робота з W3af в Kali

4. Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні, та лабораторні роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Відповідно до Тимчасового положення "Про порядок оцінювання результатів навчання студентів за накопичувальною бально-рейтинговою системою" ХНЕУ ім. С. Кузнеця, контрольні заходи включають:

поточний контроль, що здійснюється протягом семестру під час проведення лекційних та лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

модульний контроль, що проводиться у формі письмової контрольної роботи у вигляді тесту, який містить 20 тестових питань і проводиться з ініціативи викладача з урахуванням поточного контролю за відповідний змістовий модуль і має на меті *інтегровану* оцінку результатів навчання студента після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля;

підсумковий/семестровий контроль, що проводиться у формі семестрового екзамену, відповідно до графіку навчального процесу.

Порядок проведення поточного оцінювання знань студентів. Оцінювання знань студента під час лабораторних занять проводиться за такими критеріями:

"відмінно" (4 бали) - студент бездоганно засвоїв теоретичний матеріал з проблеми тестування на проникнення та етичного хакінгу, демонструє глибокі і всебічні знання методів та інструментальних засобів тестування на проникнення, основні положення наукових першоджерел та рекомендованої літератури, логічно мислить і будує відповідь, вільно використовує набуті теоретичні знання з тестування на проникнення та етичного хакінгу при аналізі практичного матеріалу, висловлює своє ставлення до тих чи інших проблем, демонструє високий рівень засвоєння практичних навичок з дослідження на проникнення операційних системі Windows та Linux;

- "добре" (3 бали) - студент добре засвоїв теоретичний матеріал, володіє основними аспектами з дослідження та тестування інформаційних систем на проникнення з першоджерел та рекомендованої літератури, аргументовано викладає його; має практичні навички з дослідження та тестування на проникнення операційних систем Windows/Linux, висловлює свої міркування з приводу тих чи інших проблем, але припускається певних неточностей і похибок у логіці викладу теоретичного змісту або при аналізі практичного;

- "задовільно" (1-2 бали) - студент в основному опанував теоретичними знаннями з тестування на проникнення та етичного хакінгу, орієнтується в першоджерелах та рекомендованій літературі, але непереконливо відповідає, плутає поняття, додаткові питання викликають у студента невпевненість або відсутність стабільних знань; відповідаючи на запитання практичного характеру, виявляє неточності у знаннях, не вміє оцінювати факти та явища, пов'язувати їх із майбутньою діяльністю;

- "незадовільно" (0 балів) - студент не опанував навчальний матеріал з методів та інструментальних засобів тестування на проникнення та етичного хакінгу, не знає визначень методів тестування, майже не орієнтується в першоджерелах та рекомендованій літературі, практичні навички з дослідження операційних систем на проникнення не сформовані.

Матеріал для самостійної роботи студентів, який передбачений в темі лабораторного заняття одночасно із аудиторною роботою, оцінюється під час поточного контролю теми на відповідному аудиторному занятті. Оцінювання тем, які виносяться на самостійне опрацювання і не входять до тем аудиторних навчальних занять, контролюються під час підсумкового контролю.

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі проведення семестрового екзамену, завданням якого є перевірка розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатності творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей.

Кожен екзаменаційний білет складається із 5 практичних ситуацій (два стереотипних, два діагностичних та одне евристичне завдання), які передбачають вирішен-

ня типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента і рівень його компетентності з навчальної дисципліни.

Результат семестрового екзамену оцінюється в балах (максимальна кількість – 40 балів, мінімальна кількість, що зараховується, – 25 балів) і проставляється у відповідній графі екзаменаційної "Відомості обліку успішності".

Студента слід **вважати атестованим**, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Розподіл балів за тижнями

Теми змістового модуля			Лекційні заняття	Лабораторні заняття	Письмова контрольна робота	Усього
Змістовий модуль	Тема	Тиждень				
Змістовий модуль 1.	1	1	2			2
	2	2	2			2
	3	3				0
		4	2			2
	4	5				0
		6	2			2
Змістовий модуль 2.	5	7		4		4
		8	2		20	22
		9		4		4
	6	10	2			2
		11		4		4
		12	2			2
	7	13		4		4
		14	2			2
		15	2			2
	8	16	2	4		6
	Іспит					40
Усього за 2 семестр			20	20	20	100

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	Зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано
1 – 34	F		

5. Рекомендована література

5.1 Основна

1. Тестирование на проникновение или пентест [Электронный ресурс]. – URL: http: //deflab.ru/blog/metodi-i-sredstva-zashiti/testirovanie-na-proniknoveniepentest.html

2. Тестирование на проникновение в соответствии с требованиями СТО БР ИББС-1.0–2014 [Электронный ресурс]. – URL: https: //habrahabr.ru/company/pentestit/blog/255113.

3. Этичный хакинг и тестирование на проникновение [Электронный ресурс]. – URL: http: //www.slideshare.net/heirhabarov/publ-57821636

4. Статистика уязвимостей корпоративных информационных систем 2014 [Электронный ресурс]. – URL: https: //www.ptsecurity.ru/download/PT_Corporate_vulnerability_2015_rus.pdf .

5. Скабцов Н.В. Аудит безопасности информационных систем. – СПб.: Питер, 2018, – 272 с.

6. Стародубцев Ю.И. Управление качеством информационных услуг / Ю.И. Стародубцев, А.Н. Бегаев, М.А. Дятлова; под общ. ред. Ю.И. Стародубцева. – СПб: Изд-во Политехн. Ун-та, 2017, – 454 с.

7. Weidman G. Penetration Testing: A Hands-On Introduction to Hacking. – NY.: Press.Inc, 2014, – 478 с.

8. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий/Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.

9. Бегаев А.Н., Тарасюк М.В. Контроль безопасности программного кода в составе объекта информатизации // Защита информации. Инсайд. 2013. № 5 (53). С. 63-67.

10. Дорофеев А. Тестирование на проникновение: демонстрация одной уязвимости или объективная оценка защищенности? // Защита информации. Инсайд. 2010. № 6 (36). С. 72-73.

5.2 Додаткова

11. Дорофеев А.В. Подготовка к CISSP: телекоммуникации и сетевая безопасность // Вопросы кибербезопасности. 2014. № 4 (7). С. 69-74.

12. Стародубцев Ю.И., Бегаев А.Н., Давлятова М.А. Управление качеством информационных услуг. СПб.: Изд-во Политехн. ун-та, 2017. 454 с.

13. Dorofeev A.V., Rautkin Y.V. Applied Aspects of Security Testing. In CEUR Workshop Proceedings, 2017, Vol-2081 (Selected Papers of the VIII AllRussian Scientific and Technical Conference on Secure Information Technologies, BIT 2017), pp. 49-53.

14. Дорофеев А.В., Марков А.С. Структурированный мониторинг открытых персональных данных в сети Интернет // Мониторинг правоприменения. 2016. № 1 (18). С. 41-53.

15.Doroveev A.V., Markov A.S., Tsirlov V.L. Social media in identifying threats to ensure safe life in a modern city // Communications in Computer and Information Science. 2016. V. 674. P. 441-449.

5.3 Інформаційні ресурси в мережі Інтернет

16. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни “Тестування на проникнення та етичний хакінг” https://pns.edu.ua/course/view.php?id=5684