Силабус освітнього компонента
Програма навчальної дисципліни

Етичний хакінг

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Освітньо-професійна програма Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістрї

Тип дисципліни
Загальна підготовка, Обов'язкова

Семестр
2

Мова викладання
Українська, Англійська

Викладачі, розробники

МІЛОВ Олександр Володимирович
oleksandr.milov@khpi.edu.ua
Доктор технічних наук, професор кафедри кібербезпеки НТУ «ХПІ».

Автор понад 200 наукових та навчально-методичних праць. Науковий керівник з захищених кандидатських робіт, гарант освітньо-професійної програми другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Математичні основи криптології та криптоаналіз», «Структури даних», «Промисловий та офісний шпіонаж» , «Цифрова криміналістика», у студентів бакалавріата та магістратури, Розділ «Методологія наукової та педагогічної діяльності в науках кіберзахисту» для аспірантів.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Процес тестування на проникнення призначено для 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.

Мета та цілі дисципліни

Підготовка фахівців, в області інформаційної безпеки, безпеки телекомунікаційного забезпечення, і мобільних пристроїв, а також фахівців з тестування на проникнення та етичного хакінгу, на базі 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.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

КЗ–1. Здатність застосовувати знання у практичних ситуаціях.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

Обсяг дисципліни

Загальний обсяг дисципліни 90 год. (3 кредити ECTS): лекції – 16 год., лабораторні роботи – 16 год., самостійна робота – 58 год.

Передумови вивчення дисципліни (пререквізити)

Цифрова криміналістика, Інноваційне підприємництво та управління стартап проєктами, Математичні основи криптології, Основи криптографічного захисту, Основи програмування.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Вступ.
Цілі та завдання навчальної дисципліни «Тестування на проникнення та етичний хакінг». Місце дисципліни у навчальному процесі підготовки спеціаліста з кібербезпеки. Структура, зміст тематичного плану вивчення дисципліни; навчально-методична література. Особливості вивчення дисципліни; форми контролю знань, умінь та навичок учнів. Напрями науково-дослідної роботи студентів..
Тема 2. Методології оцінки вразливості .
Основні умови. Злом та етичний злом. Що роблять справжні хакери. Методологія тестування на проникнення: OSTMM, ISSAF та ін. Управління проектами з тестування на проникнення. Огляд хакерських інструментів. Застосовні закони. Робота з третіми особами. Питання соціальної інженерії. Логування. Складання звітів..
Тема 3. Огляд інструментів етичного злому.
Етичне робоче місце хакера: Kali Linux. Цілі: Metasploitable 2 і т.д. Сканери портів. Сканери вразливостей. Експлуатаційні рамки.
Тема 4. Структуровані підходи до збирання інформації.
Методи розвідки із відкритим вихідним кодом. Огляд методів структурованого аналізу. Типи інформації, що збирається: ділова інформація (фінансова, клієнти, постачальники, партнери). Інформація про IT-інфраструктуру. Виявлення джерел інформації.
Тема 5. Збір технічної інформації.

Виявлення IP-адресів. Трасування. Використання Мальтего. Перенесення зони DNS. DNS Брутфорс.
Тема 6. Аналіз уразливостей.
Типи вразливостей. Ручний пошук уразливостей. Автоматичний пошук уразливостей. Інструменти аналізу уразливостей.
Тема 7. Базова експлуатація Фреймворк Метасплот.
Що таке експлойт. Використовувати бази даних Google для тестерів на проникнення: www.exploit-db.com. Локальна та віддалена експлуатація. Огляд платформи Metasploit. Типи корисного навантаження. Атаки «людина посередині».
Тема 8. Парольні атаки.
Атаки на паролі: онлайн та офлайн. Хеші паролів. Мистецтво ручного підбору пароля. Пройти хеш атаку.
Тема 9. Експлуатація веб-застосунків.
Типова структура Web-програми. Поширені веб-уразливості. Проекти OWASP. Огляд посібника з тестування OWASP. лом Google. Злом бази даних Google (GHDB). Інструменти тестування веб-безпеки. еб-сканери. Локальні проксі. Фазери. Спеціалізовані браузери та плагіни для браузерів.
Тема 10. Соціальна інженерія.
Соціальна інженерія. Огляд проекту «Інструментарій соціальної інженерії».
Тема 11. Експлуатація з використанням атак клієнтів.
Експлойти на стороні клієнта. Огляд проекту інфраструктури експлуатації браузера.
Тема 12. Підтримка доступу.
Підтримка техніки доступу. Використання інтерпретатора.
Тема 13. Тестування на проникнення бездротових мереж.
Тема 14. 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 15. Злом та захист акаунтів у соціальних мережах.
Цілі та виконавці злому акаунтів. Збір інформації. Методи злому. Зламування електронної пошти. Соціальний інжиніринг. Перебір пароля. Фішинг або фейкова сторінка. Клавіатурний шпигун. Підміна DNS.
Тема 16. Складання звіту і представлення результатів тестування на вторгнення.
Важливість оформлення звіту щодо результатів тестування на вторгнення. Узагальнений шаблон звіту про вторгнення. Види звітів та методика їх складання. Спеціаліст з етичного хакінгу як свідок. Порівняння ролей експертів і технічних спеціалістів

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Базова конфігурація Kali Linux та Metasploitable 2.
Тема 2. Використання Google для OSINT у проектах тестування на проникнення. Технічна розвідка IT-інфраструктури. Використання Maltego для розвідки.
Тема 3. Аналіз вразливостей Сканування портів. Ручна оцінка вразливості. Використання сканерів уразливостей для оцінки вразливостей. Огляд конфігурації. Спеціальні інструменти сканування.
Тема 4. Експлуатація Атака з використанням ARP-спуфінгу. Використання командного рядка Metasploit для експлуатації вразливостей. Використання Armitage для експлуатації вразливостей. Атаки на паролі баз даних. Атаки на паролі для різноманітних сервісів.
Тема 5. Експлуатація веб-застосунків Сканування веб-застосунків. Вибір пароля веб-програми. Виконання команд ОС через веб-сервер.
Тема 6. Експлуатація веб-застосунків.SQL-ін'єкція та офлайн-злом пароля. Експлуатація XSS-вразливості.
Тема 7. Експлуатація з використанням атак клієнтів Експлуатація клієнта з BeEF.
Тема 8. Підтримка доступу Встановлення та використання руткітів.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.
Зокрема, окремі теми даної компоненти можуть бути враховано у разі успішного завершення таких курсів CISCO:
Ethical Hacker
https://www.netacad.com/catalogs/learn?category=course.

Література та навчальні матеріали

Основна література

1. Oriyano Sean-Philip. Penetration Testing Essentials. Sybex, a Wiley brand, 2017, 363 p. 2. Baloch Rafay. Ethical hacking and penetration testing guide. Auerbach Publications, 2017, 523 p. [Електронний ресурс]. – Режим доступу:
https://www.tsoungui.fr/ebooks/Ethickal-haking-postexploitation.pdf
2. Євсеєв С.П. Кібербезпека: Лабораторний практикум з основ криптографічного захисту. – Львів "Новий світ-2000", 2020. – 241 с. [Електронний ресурс]. – Режим доступу:
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
3. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. — Львів : Видавництво Львівської політехніки, 2019. — 580 с. — ISBN 978-966-941-339-0. [Електронний ресурс]. – Режим доступу:
https://pdf.lib.vntu.edu.ua/books/2021/Bobalo_2019_580.pdf.

Додаткова література

4. Aaron Philipp, David Cowen, Chris Davis. Hacking exposed computer forensics. Second edition. The McGraw-Hill Companies, 2010. [Електронний ресурс]. – Режим доступу:
https://needuxnworkplace.wordpress.com/wp-content/uploads/2014/01/hacking-exposed-computer-forensics-secrets-solutions.pdf
5. Wilhelm, Thomas. Professional penetration testing: Creating and learning in a hacking lab. Newnes, 2013, 525 p. [Електронний ресурс]. – Режим доступу:
http://ppdi.stmik-banjarbaru.ac.id/data.bc/13.%20Hacking/2013%20Professional%20Penetration%20Testing%20Creating%20and%20Learning%20in%20a%20Hacking%20Lab.pdf.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 40% семестрової оцінки;
•контрольна робота: 20% семестрової оцінки;
•іспит: 40% семестрової оцінки.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту. Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	28.08.2024		Завідувач кафедри Сергій ЄВСЕЄВ
	28.08.2024		Гарант ОП Ольга КОРОЛЬ