Силабус освітнього компонента
Програма навчальної дисципліни

Етичний хакінг

Шифр та назва спеціальності
256 – Національна безпека (за окремими сферами забезпечення і видами діяльності)

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Національна безпека у сфері кіберзахисту

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалавр

Тип дисципліни
Профільна підготовка, Вибіркова

Семестр
4

Мова викладання
Українська

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

Навчальна дисципліна "Етичний хакінг" є вибірковою навчальною дисципліною. Вивчення дисципліни забезпечує особистісний і професійний розвиток студента та спрямована на формування ефективного дослідника, здатного до використання сучасних методів дослідження кіберпростору та передачі знань. В курсі розглядається методологія тестування на проникнення та її етапи. Окремо приділена увага створенню звітів на проникнення, як одному із важливих етапів при здійсненні оцінки захищеності інформаційної системи.

Мета та цілі дисципліни

Підготовка фахівців, в області інформаційної безпеки, а також фахівців з 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 етичного хакінгу.

Формат занять

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

Компетентності

КЗ–6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
КЗ–7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
ФК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.
ФК-9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.
ФК-10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.
ФК-11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

ПРН-3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.
ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.
ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.
ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
ПРН-11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.
ПРН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.
ПРН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
ПРН-17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.

ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

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)

Інформаційна безпека держави, Математичні основи криптології та криптоаналіз, 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, індивідуальні групові проєкти, майстер-класи.

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.
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.
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.
https://pdf.lib.vntu.edu.ua/books/2021/Bobalo_2019_580.pdf
4. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
5. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, O. Milov, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
6. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, O. Milov, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Додаткова література

7. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
http://kist.ntu.edu.ua/textPhD/tzi.pdf
8. Security of Linux operating system: laboratory workshop / S. Yevseiev, S. Pogasiy, A. Goloskokova, O. Shmatko, M. Melnik (Кібербезпека: безпека операційної системи Linux: лабораторний практикум: навчальний посібник для студентів вищих навчальних закладів англійською мовою / Євсеєв С.П., Погасій С.С., Голоскокова А.О., Шматко О.В., Мельник М.О. – Львів: Видавництво «Новий Світ – 2000», 2021. – 256 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
9. Євсєєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
10. Технологія Ethernet : лабораторний практикум / М. О. Білова, С. П. Євсеєв, О. С. Жученко, І. С. Іванченко, О. В. Шматко.– Львів: «Новий Світ- 2000», 2020 . – 196 с.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
11. Aaron Philipp, David Cowen, Chris Davis. Hacking exposed computer forensics. Second edition. The McGraw-Hill Companies, 2010.
https://needuxnworkplace.wordpress.com/wp-content/uploads/2014/01/hacking-exposed-computer-forensics-secrets-solutions.pdf

12. Wilhelm, Thomas. Professional penetration testing: Creating and learning in a hacking lab. Newnes, 2013, 525 p.
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;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 10% 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 Андрій ТКАЧОВ