Силабус освітнього компонента
Програма навчальної дисципліни

Виявлення вторгнень у комп'ютерні мережі (мережеві аномалії)

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

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

Освітня програма
Освітньо-наукова програма Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

Тип дисципліни
Наукова підготока, Обов’язкова

Семестр
2

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 “ Виявлення вторгнень у комп'ютерні мережі (мережеві аномалії)дає основні визначення та поняття в галузі систем виявлення вторгнень та комп'ютерних атак. Розглянуто принципи побудови та структуру систем виявлення вторгнень. Аналізуються способи розгортання, переваги та недоліки існуючих систем виявлення вторгнень. Центральне місце у дисциплині приділено методам виявлення аномалій мережі. Розглянуто методи кратномаспгтабного вейвлет- та мультифрактального аналізу алгоритмів виявлення аномальних вторгнень. Проведено аналіз статистичних, інтелектуальних, імунних, нейромережевих та інших алгоритмів виявлення аномалій.

Мета та цілі дисципліни

Мета навчальної дисципліни “ Виявлення вторгнень у комп'ютерні мережі (мережеві аномалії)

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

Формат занять

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

Компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
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.
КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно 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.
КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
КФ11. Здатність здійснювати наукові та/або прикладні дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, формувати науково-технічну звітність.

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.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
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.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
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.
РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики.
РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 32 год., лабораторні роботи – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Технології захисту інформації.

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. Тестування на проникнення.
Існуючі види (мобільні додатки, веб додатки і т.д). Види тестувань (white box, black box, gray box). Фази тестування на проникнення (договір, розвідка, сканування, ескплотація, звіт). Зміст та розділи курсу.
Тема 2. SQL ін’єкції.
Ризики. Загальні типи та вектори атак.
Тема 3. Аутентицікація.
Різниця з авторизацією. Основні вразливості.
Тема 4. DIRECTORY TRAVERSAL (обхід шляху до файлу).
Визначення. Основні вразливості. Вплив на безпеку. Типові атаки. Методи захисту.
Тема 5. Контроль доступу.
Вертикальні та горизонтальні типи доступу. Неправильна реалізація контролю доступу.
Тема 6. Вразливості у завантаженні файлів.
Типові загрози та вплив на безпеку
Тема 7. Ін’єкції команд операційних систем.
Типові загрози та вплив на безпеку. Визначення. Виконання довільних команд. Сліпі командні вразливості в ОС.
Тема 8. Вразливості бізнес-логіки.
Що таке вразливості бізнес-логіки? Чому методи автоматизованого тестування безсилі. Як виникають вразливості типу бізнес-логіки. Вплив вразливостей бізнеслогіки на безпеку. Приклади.
Тема 9. Розкриття чутливої інформації.
Що таке розкриття чутливої інформації? Приклади. Загроза та вплив на безпеку застосунку.
Тема 10. SERVER-SIDE REQUEST FORGERY (SSRF).
Що таке SSRF? Типові атаки SSRF. Приклади.
Тема 11. XXE INJECTION.
Виникнення XXE. Типи XXE атак. Використання XXE для отримання файлів. Використання XXE для проведення SSRFатак. Сліпі уразливості XXE.

Тема 12. CROSS-SITE SCRIPTING (XSS).
Що таке Cross-site scripting(XSS)? Як працюють XSS? Які бувають атаки на XSS? Відображений міжсайтовий скриптинг. Stored XSS. DOM-based cross-site scripting. Вплив XSS на безпеку.
Тема 13. CROSS-SITE REQUEST FORGERY (CSRF).
Що таке Cross-site request forgery? Які бувають атаки? Механізми захисту. Шляхи експлуатації.
Тема 14. CROSS-ORIGIN RESOURCE SHARING (CORS).
Що таке Cross-origin resource sharing? Які бувають атаки? Механізми захисту. Шляхи експлуатації.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Збір інформації у комп'ютерних мережах.
Тема 2. Тестування комп'ютерної мережі на проникнення. Практикум.
Тема 3. Дослідження методів захисту баз даних від атак шляхом застосування SQL-коду.
Тема 4. Проведення аудиту веб-ресурсів.
Тема 5. Дослідження способів виконання та запобігання атак типу ARP-spoofing та DNS-spoofing.
Тема 6. Дослідження способів виконання та запобігання атакам типу Inject Forced Download, Inject Java Backdoor та WPAD.

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:
CyberOps
https://www.netacad.com/catalogs/learn?category=course.

Література та навчальні матеріали

Основна література:

1. Cybersecurity Fundamentals/ ISACA/ www/isaca/org/cyber? Cybersecurity Fundamentals Study Guide/ 2003.- 156 p.
2. Sankar R. Burpsuite – A Beginner's Guide For Web Application Security or Penetration Testing [Електронний ресурс] / Ravi Sankar. – 2018. – Режим доступу до ресурсу: https://kalilinuxtutorials.com/burpsuite/.
3. Ganore P. What Is A Web Server And How Does It Function? [Електронний ресурс] / Pravin Ganore. – 2017. – Режим доступу до ресурсу: https://www.milesweb.com/blog/hosting/web-server-function/.
4. How a Web server functions? [Електронний ресурс]. – 2006. – Режим доступу до ресурсу: https://www.eukhost.com/blog/webhosting/how-aweb-server- functions/.
5. Державна служба спеціального зв'язку та захисту інформації України./ www.dsszzi.gov.ua
6. Learn Ethical Hacking from Scratch: Your Stepping Stone to Penetration Testing
7. Mastering Modern Web Penetration Testing Prakhar Prasad 8. Common Vulnerability Scoring System Calculator Version 3/ https://nvd.nist.gov/vuln- metrics/cvss/v3-calculator.

Додаткова література :

1. Brewer J. Web Server Vulnerabilities and a Defense in Depth Strategy Using the Squid Proxy [Електронний ресурс] / Jim Brewer // GSEC Practical version 1.4b. – 2004. – Режим доступу до ресурсу: https://www.giac.org/paper/gsec/3729/web-server-vulnerabilitiesdefense-in-depth- strategy-squid-proxy/105970.
2. Melnick J. Top 10 Most Common Types of Cyber Attacks [Електронний ресурс] / Jeff Melnick. – 2018. – Режим доступу до ресурсу: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-ofcyber-attacks/
3. Top 8 Network Attacks by Type in 2017 [Електронний ресурс] // CALYPTIX. – 2017
4. How to Prevent SQL Injection Attacks [Електронний ресурс] // eSecurityPlanet. – 2018. – Режим доступу до ресурсу: https://www.esecurityplanet.com/threats/how-to-prevent-sql-injectionattacks.html.
5. How to Protect Against SQL Injection Attacks [Електронний ресурс] // UC Berkeley. – 2019. – Режим доступу до ресурсу: https://security.berkeley.edu/education-awareness/best-practices-howarticles/system- application-security/how-protect-against-sql.
6. Choudhary A. SQL Injection Attacks: Know How to Prevent Them [Електронний ресурс] / Archana Choudhary // Security Zone. – 2019. – Режим доступу до ресурсу: https://dzone.com/articles/sql-injectionattacks-know-how-to- prevent-them.
7. Cobb M. Cross-site scripting explained: How to prevent XSS attacks [Електронний ресурс] / Michael Cobb // 2009 – Режим доступу до ресурсу: https://www.computerweekly.com/tip/Cross-site-scriptingexplained-How-to- prevent-XSS-attacks.
8. Singh S. 5 Practical Scenarios for XSS Attacks [Електронний ресурс] / Satyam Singh // Pentest Tools. – 2018. – Режим доступу до ресурсу: https://pentest- tools.com/blog/xss-attacks-practical-scenarios/.
9. Cross-site Scripting (XSS) [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.owasp.org/index.php/Crosssite_Scripting_(XSS).
10. Cross Site Scripting (XSS) Attack Tutorial With Examples, Types & Prevention [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.softwaretestinghelp.com/cross-site-scripting-xssattack-test/.
11. Excess XSS [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://excess-xss.com.
2. Cross Site Scripting (XSS) Attack Tutorial With Examples, Types & Prevention [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.softwaretestinghelp.com/cross-site-scripting-xssattack-test

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
• лабораторні роботи: 30% семестрової оцінки;
• самостійна робота: 10% семестрової оцінки;
• контрольна робота: 20% семестрової оцінки;
• залік: 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			Завідувач кафедри
	28.08.2024		Сергій ЄВСЕЄВ
	28.08.2024		Гарант ОП Станіслав МІЛЕВСЬКИЙ