Навчальна дисципліна

Методи кіберзахисту розподілених систем

Галузі знань: 10 «Природничі науки», 11 «Математика та статистика», 12 «Інформаційні технології», 15 «Автоматизація та приладобудування», 16 «Хімічна та біоінженерія», 17 «Електроніка та телекомунікації», 19 «Архітектура та будівництво»

Рівень вищої освіти	*другий (магістерський)*
Статус дисципліни	*вибіркова*
Обсяг дисципліни	150 годин/ 5 кредитів ЄКТС
Мова викладання	*українська*
Анотація	**Курс «Методи кіберзахисту розподілених систем»** дозволяє вивчити методи кіберзахисту і засоби аналізу та тестування (на проникнення) вразливостей, отримати практичні навички щодо їх використання, розроблення та вибору. **Мета:** отримати знання про сучасні методи наукового дослідження кіберзахисту розподілених інформаційних систем для забезпечення і дослідження гарантоздатної обробки, передачі та зберігання інформації. Завдання: вивчення і дослідження основних методів і моделей кіберзахисту інформації в гарантоздатних розподілених інформаційних системах. **Компетентності**, які набуваються: - здатність до пошуку, оброблення та аналізу інформації щодо кіберзахисту; - здатність ініціювати, розробляти і реалізовувати комплексні інноваційні проекти в кібербезпеці та дотичні до неї міждисциплінарні проекти, лідерство під час їх реалізації. **Основні теми:** - підготовка тестового оточення. Встановлення Damn Vulnerable Web Application. Встановлення на локальній машині платформи з вразливостями для дослідження. Закріплення навичок роботи в Linux-подібних системах. Отримання навичок встановлення і налаштування веб-сервера для подальшого встановлення на нього вразливого застосунка; - аналіз трафіку комп'ютерних мереж і дослідження сценарію атаки типу Man-in-the-Middle. Отримання навичок роботи з аналізатором трафіку Wireshark і платформою Burpsuite, знайомство з атакою Man-in-the-Middle. Знайомство зі структурою мережевих пакетів. Отримання навичок роботи в сніффером на прикладі Wireshark і Burpsuite. Аналіз сценаріїв MitM-атак веб-застосунку. Розробка методів захисту веб-застосунку від даного виду атак; - SQL-ін'єкції. Принципи, пошук і експлуатація SQL-ін'єкцій. Методи ін'єкцій та їх наслідки. Атаки з порушенням логіки запитів до бази даних. Робота з інструментальним засобом для пошуку і експлуатації ін'єкцій. Освоєння природи походження і принципів експлуатації вразливості в браузері. Використання утиліти sqlmap для експлуатації SQL-ін'єкцій. Порівняльний аналіз методів ін'єкцій при різній складності експлуатації вразливостей в DVWA; - робота з XSS-атаками. Особливості атак та їх наслідки. Сценарії здійснення атак та інструменти атак. Освоєння природи походження і принципів експлуатації вразливості в браузері. Отримання навичок використання утиліти xsser для пошуку вразливостей. Можливості XSS-атак. Розроблення заходів щодо захисту веб-застосунка від XSS-атак; - робота з шеллом в Metasploit. Наукове дослідження можливостей виконання довільних команд в атакованій системі.Отримання навичок роботи в фреймворку на прикладі модуля управління шеллом. Отримання навичок використання модулів фреймворка Metasploit. Отримання навичок управління атакованим сервером. Можливі наслідки експлуатації шелл. Розроблення заходів щодо захисту веб-застосунка від завантаження шелл; - основи сканування IP-мереж. Знайомство з призначенням і функціоналом утиліти nmap в ОС Kali Linux, знайомство з основними відкритими базами даних вразливостей.

<table>
<tr><td></td><td>Отримання навичок використання утиліти nmap. Отримання навичок пошуку інформації у відкритих базах вразливостей. Наукове дослідження методів і засобів виявлення сканування. Розроблення заходів щодо захисту мережі від сканування;
- забезпечення безпеки багатокомпонентного веб-застосунка. Аналіз можливих проблем безпеки веб-застосунка на етапі проєктування. Список вимог, які повинні бути перевірені перед здачею проєкту замовнику. Методи і засоби захисту від поширених атак. Наукове дослідження методів Web Application Firewall для виявлення потенційно небезпечного трафіку</td></tr>
<tr><td>Організація навчання</td><td>Види занять: лекції, лабораторні заняття.
Форми здобуття освіти: денна, заочна.
Форми контролю: модульний контроль, іспит</td></tr>
<tr><td>Кафедра</td><td>Кафедра комп'ютерних систем, мереж і кібербезпеки</td></tr>
<tr><td>Факультет</td><td>Факультет радіоелектроніки, комп'ютерних систем та інфокомунікацій</td></tr>
<tr><td>Викладач</td><td> 
<table><tr><td>ПІБ</td><td>Тецький
Артем Григорович</td></tr><tr><td>Посада</td><td>старший викладач</td></tr><tr><td>Вчене звання</td><td></td></tr><tr><td>Науковий ступінь</td><td>кандидат технічних наук</td></tr><tr><td>e-mail</td><td></td></tr></table></td></tr>
<tr><td>Посилання на електронні матеріали курсу</td><td></td></tr>
<tr><td>Посилання на робочу програму (силабус)</td><td></td></tr>
</table>