МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра протидії кіберзлочинності факультету №4

МЕТОДИЧНІ МАТЕРІАЛИ
ДО ЛАБОРАТОРНИХ ЗАНЯТЬ

з навчальної дисципліни "Безпека інформаційно-комунікаційних систем"
обов'язкових компонент
освітньої програми першого рівня вищої освіти
"Кібербезпека (безпека інформаційних та комунікаційних систем)"

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол №7 від 30.08.2023

СХВАЛЕНО
Вченою радою факультету №4
Протокол № 8 від 16.08.2023

ПОГОДЖЕНО
Секцією науково-методичної ради
ХНУВС з технічних дисциплін
Протокол №7 від 29.08.2023

Розглянуто на засіданні кафедри протидії кіберзлочинності (протокол № 19 від 15.08.2023)

Розробник: професор кафедри протидії кіберзлочинності ХНУВС, к.т.н. доцент Носов В.В.

Рецензенти:

доцент кафедри кібербезпеки та DATA-технологій факультету №6 Харківського національного університету внутрішніх справ к.т.н. доцент Тулупов В.В.

завідувач кафедри інформаційних управляючих систем Харківського національного університету радіоелектроніки, д.т.н. професор Петров К.Е.

1. Розподіл часу навчальної дисципліни за темами

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни					Вид контролю
	Всього	з них:				
		лекції	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр №5						
Тема №1. Основні відомості про кібербезпеку	16	6		2	8	залік
Тема №2. Пасивний збір інформації	24	4		8	12	
Тема №3. Активний збір інформації про мережу	24	4		8	12	
Тема №4. Аналіз трафіку в комп'ютерних мережах	16	4		4	8	
Тема №5. Перехоплення сесій передачі даних в комп'ютерних мережах	10	2		2	6	
Всього за семестр №5	**90**	**20**		**24**	**46**	
Семестр №6						
Тема №6. Безпека в безпровідних мережах	24	6		6	12	залік
Тема №7. Безпека в операційних системах	28	6		8	14	
Тема №8. Шкідливе програмне забезпечення	24	6		6	12	
Тема №9. Переповнення буферу	8	2		2	4	
Тема №10. Безпека веб-серверів та веб-застосувань	36	6		12	18	
Всього за семестр №6	**120**	**26**		**34**	**60**	
Семестр №7						
Тема №11. Атака «відмова в обслуговуванні»	16	2		4	10	екз.
Тема №12. SQL-ін'єкції	40	6		10	24	
Тема №13. Соціальна інженерія	24	4		6	14	
Тема №14. Тестування на вразливість до атак	26	2		4	20	
Тема №15. Сервіси та механізми захисту мережі	44	12		6	26	
Всього за семестр №7	**150**	**26**		**30**	**94**	
Всього за дисципліною	**360**	**72**		**88**	**200**	

2. Методичні вказівки до лабораторних занять

Тема №1. Основні відомості про кібербезпеку

Лабораторне заняття 1.1. Встановлення віртуальних машин

Навчальна мета заняття: навчитися інсталювати спеціалізовану ОС, що використовується для тестування безпеки

Кількість годин: 2 год.

Навчальні питання

1. Встановлення VirtualBox
2. Встановлення Kali Linux
3. Встановлення Metasploitable2
4. Встановлення Windows
5. Налаштування віртуальної мережі та Metasploitable2

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику ОС Kali Linux. Надати посилання до місця розміщення дистрибутиву ОС.

Охарактеризувати засіб віртуалізації – VirtualBox. Надати посилання до місця розміщення дистрибутиву.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №2. Пасивний збір інформації

Лабораторне заняття 2.1. Пасивний збір інформації

Навчальна мета заняття: навчитися користуватися програмними засобами пасивного збору інформації про об'єкт атаки при тестуванні безпеки

Кількість годин: 4 год.

Навчальні питання

1. Збір інформації про веб-сайти
2. Збір інформації за допомогою Google
3. Збір інформації за допомогою Whois
4. Збір інформації DNS
5. Збір інформації про мережу

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику пасивному збору інформації. Надати посилання до місця розміщення дистрибутивів програмних інструментів.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 2.2. Аналіз результатів пасивного збору інформації

Навчальна мета заняття: навчитися аналізувати результати пасивного збору інформації

Кількість годин: 2 год.

Навчальні питання

1. Побудова та аналіз зв'язків за результатами пасивного збору інформації
2. Збір інформації за заголовками електронної пошти

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику сервісів і засобів аналізу результатів пасивного збору інформації. Надати посилання на відповідні засоби.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 2.3. Засоби та сервіси OSINT

Навчальна мета заняття: навчитися користуватися засобами і наявними сервісами OSINT

Кількість годин: 2 год.

Навчальні питання

1. Наявні OSINT сервіси.
2. Відомі OSINT утиліти

Література: пошукові сервіси глобальної мережі.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику актуальних OSINT сервісів і засобів. Надати посилання на відповідні засоби.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №3. Активний збір інформації про мережу

Лабораторне заняття 3.1. Активний збір інформації про мережу

Навчальна мета заняття: навчитися користуватися програмними засобами активного збору інформації про мережу при тестуванні безпеки

Кількість годин: 4 год.

Навчальні питання

1. Засоби для перевірки доступності вузла
2. Засоби для визначення ОС
3. Сканування портів
4. Перехоплення банерів

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику активному збору інформації. Надати посилання до місця розміщення дистрибутивів програмних інструментів.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 3.2. Засоби перерахування сервісів мережі

Навчальна мета заняття: навчитися користуватися засобами активного отримання інформації за протоколами NetBIOS, SNMP, LDAP, SMTP, DNS.

Кількість годин: 2 год.

Навчальні питання

1. Засоби отримання інформації з протоколів NetBIOS, SNMP, LDAP.

2. Засоби отримання інформації з протоколів SMTP, DNS

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику засобам активного отримання інформації за протоколами NetBIOS, SNMP, LDAP, SMTP, DNS. Надати посилання на відповідні засоби.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 3.3. Засоби пошуку вразливостей

Навчальна мета заняття: навчитися користуватися засобами пошуку вразливостей віддалених ресурсів.

Кількість годин: 2 год.

Навчальні питання

1. Сканер вразливостей OpenVAS.
2. Налаштування SSH-тунелю

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику сканеру вразливостей. Надати посилання на порядок встановлення і використання сканеру вразливостей.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №4. Аналіз трафіку в комп'ютерних мережах

Лабораторне заняття 4.1. Аналіз трафіку в комп'ютерних мережах

Навчальна мета заняття: навчитися користуватися інструментами аналізу трафіку в комп'ютерних мережах

Кількість годин: 2 год.

Навчальні питання

1. Перехоплення трафіка
2. MAC затоплення (MAC flooding)
3. ARP Spoofing

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику способам і інструментам аналізу трафіку в комп'ютерних мережах. Вказати спосіб встановлення додаткових застосунків в ОС.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 4.2. MITM атаки

Навчальна мета заняття: ознайомитися із засобами проведення MITM атак

Кількість годин: 2 год.

Навчальні питання

1. Xerosploit.
2. Evilginx2.
3. Morpheus Framework.

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику MITM атакам. Вказати порядок встановлення і використання засобів проведення MITM атак.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №5. Перехоплення сесій передачі даних в комп'ютерних мережах

Лабораторне заняття 5.1. Перехоплення сесій передачі даних в комп'ютерних мережах

Навчальна мета заняття: навчитися користуватися інструментами перехоплення сесій передачі даних в комп'ютерних мережах при тестуванні безпеки

Кількість годин: 2 год.

Навчальні питання

1. Використання Ettercap
2. Використання Xplico
3. Перехоплення сесії за допомогою Hamster та Ferret

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику способам і інструментам аналізу трафіку в комп'ютерних мережах. Вказати спосіб встановлення додаткових застосунків в ОС.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №6. Безпека в безпровідних мережах

Лабораторне заняття 6.1. Безпека в безпровідних мережах

Навчальна мета заняття: навчитися користуватися інструментами тестування безпеки безпровідних комп'ютерних мереж

Кількість годин: 2 год.

Навчальні питання

1. Аналіз безпровідних мереж
2. Злам безпровідних мереж
3. Засоби прискорення підбору паролю

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику технології WiFi та напрямам тестування безпеки безпровідних комп'ютерних мереж. Вказати спосіб встановлення додаткових застосунків в ОС.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 6.2. Втручання у роботу WiFi мереж

Навчальна мета заняття: ознайомитися із засобами проведення DoS атак і створення підроблених точок доступу WiFi мереж

Кількість годин: 4 год.

Навчальні питання

1. DoS атака на безпровідні мережі.
2. Створення підроблених точок доступу.

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Вказати порядок встановлення і використання засобів проведення активного втручання у роботу WiFi мереж.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №7. Безпека в операційних системах

Лабораторне заняття 7.1. Фреймворк атаки операційних систем

Навчальна мета заняття: навчитися користуватися інструментами тестування безпеки операційних систем

Кількість годин: 2 год.

Навчальні питання

1. Metasploit framework
2. MetasploitHelper

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику Metasploit Framework та видам атак на ОС.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 7.2. Комплексні атаки на віртуальні машини

Навчальна мета заняття: навчитися користуватися інструментами тестування безпеки операційних систем

Кількість годин: 4 год.

Навчальні питання

1. CTF-Sahu
2. CTF-Five86-1

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику сценарію атак на віртуальні машини. Активувати віртуальні машини.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 7.3. Стеганографічні засоби приховування даних

Навчальна мета заняття: навчитися користуватися засобами стеганографії і виявляти стеганографічні контейнери

Кількість годин: 2 год.

Навчальні питання

1. Виконання практичних задач.

Література: https://www.hackingarticles.in/steganography-the-art-of-concealing/.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику методам стеганографії.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №8. Шкідливе програмне забезпечення

Лабораторне заняття 8.1. Шкідливе програмне забезпечення

Навчальна мета заняття: навчитися користуватися інструментами створення шкідливого програмного забезпечення для тестування антивірусних систем

Кількість годин: 4 год.

Навчальні питання

1. Створення троянів
2. Протидія і виявлення
3. Створення та аналіз шкідливого коду для Android

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику способам і інструментам інструментами створення шкідливого програмного забезпечення, принципам роботи антивірусних систем. Вказати спосіб встановлення додаткових застосунків в ОС.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 8.2. Шкідливе програмне забезпечення ОС Android

Навчальна мета заняття: ознайомитися із засобами створення шкідливого програмного забезпечення для ОС Android

Кількість годин: 2 год.

Навчальні питання

1. Утиліта MSFvenom.

2. Утиліта SpyNoteShell.

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Вказати порядок встановлення і використання засобів створення шкідливого програмного забезпечення для ОС Android.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №9. Переповнення буферу
Лабораторне заняття 9.1. Переповнення буферу

Навчальна мета заняття: навчитися аналізувати вразливість переповнення буферу
Кількість годин: 2 год.

Навчальні питання

1. Аналіз коду програми
2. Усунення вразливості переповнення буферу

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику вразливості переповнення буферу. Вказати спосіб встановлення додаткових застосунків в ОС.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №10. Безпека веб-серверів та веб-застосувань
Лабораторне заняття 10.1. Безпека веб-серверів та веб-застосувань

Навчальна мета заняття: навчитися користуватися інструментами дослідження вразливостей веб-сервера

Кількість годин: 6 год.

Навчальні питання

1. Програмні засоби дослідження вразливостей веб-сервера
2. Атаки на паролі веб-застосувань
3. Використання вразливостей у ПЗ ОС та веб-сервера

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику вразливості переповнення буферу. Вказати спосіб встановлення додаткових застосунків в ОС.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 10.2. Міжсайтові підробка запиту і скриптинг

Навчальна мета заняття: ознайомитися із техніками атак Cross Site Request Forgery і Cross Site Scripting

Кількість годин: 6 год.

Навчальні питання

1. Міжсайтова підробка запиту (Cross Site Request Forgery).
2. Stored XSS.
3. Reflected XSS.
4. XSStrike.

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику техніками атак Cross Site Request Forgery і Cross Site Scripting. Вказати порядок встановлення і використання тестового веб-додатку DVWA.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №11. Атака «відмова в обслуговуванні»

Лабораторне заняття 11.1. Атака «відмова в обслуговуванні»

Навчальна мета заняття: навчитися користуватися інструментами атак «відмова в обслуговуванні» при дослідженні безпеки веб-сервера

Кількість годин: 4 год.

Навчальні питання

1. SYN flood атаки
2. Атака на веб-сервер
3. Slowhttptest атаки

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику атак «відмова в обслуговуванні». Вказати спосіб встановлення додаткових застосунків в ОС.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №12. SQL-ін'єкції

Лабораторне заняття 12.1. SQL-ін'єкції

Навчальна мета заняття: навчитися користуватися інструментами тестування на можливість SQL- ін'єкції

Кількість годин: 6 год.

Навчальні питання

1. Код, вразливий до SQL-ін'єкцій
2. Використання UNION SELECT
3. Тестування на можливість SQL-ін'єкції в автоматичному режимі
4. Захист від SQL-ін'єкцій

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику SQL-ін'єкцій та методам захисту. Вказати спосіб встановлення потрібних застосунків в ОС.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 12.2. Засоби тестування SQL-ін'єкцій

Навчальна мета заняття: ознайомитися інструментами тестування SQL-ін'єкцій

Кількість годин: 6 год.

Навчальні питання

1. Використання SleuthQL.
2. Використання LazySQLMap.

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику інструментам тестування SQL-ін'єкцій. Вказати порядок встановлення і їх використання на тестовому веб-додатку.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №13. Соціальна інженерія

Лабораторне заняття 13.1. Соціальна інженерія

Навчальна мета заняття: навчитися користуватися інструментами створення фішингових сайтів для тестування методів захисту

Кількість годин: 4 год.

Навчальні питання

1. The Social-Engineer Toolkit
2. Ngrok
3. Trape
4. Weeman

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику методам створення фішингових сайтів та методам протидії фішингу. Вказати спосіб встановлення потрібних застосунків в ОС.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 13.2. Засоби забезпечення соціальної інженерії

Навчальна мета заняття: ознайомитися із засобами забезпечення соціальної інженерії

Кількість годин: 2 год.

Навчальні питання

1. QRLJacking.
2. Camelishing.
3. Gophish.

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику засобами забезпечення соціальної інженерії. Вказати порядок їх встановлення і використання.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №14. Тестування на вразливість до атак

Лабораторне заняття 14.1. Тестування на вразливість до атак

Навчальна мета заняття: навчитися користуватися інструментами тестування безпеки окремих вузлів мережі

Кількість годин: 4 год.

Навчальні питання

1. CTF-Sunset-dusk
2. CTF- Five86-2

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику сценарію атак на віртуальні машини. Активувати віртуальні машини.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №15. Сервіси та механізми захисту мережі

Лабораторне заняття 15.1. Механізми захисту мережі від збору інформації, сканування та проникнення

Навчальна мета заняття: навчитися користуватися механізмами захисту мережі від збору інформації, сканування та проникнення

Кількість годин: 2 год.

Навчальні питання

1. IDS Snort
2. Персональний міжмережний екран Iptables

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику механізмам захисту мережі від збору інформації, сканування та проникнення. Вказати спосіб встановлення додаткових застосунків в ОС.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 15.2. Пастки Honeypot

Навчальна мета заняття: навчитися користуватися засобами імітування цілей атаки.
Кількість годин: 2 год.

Навчальні питання

1. Пастка IoT-Honeypot.
2. Пастка Heralding.
3. Пастка Kippo.

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику засобам імітування цілей атаки. Вказати порядок встановлення і використання засобів.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Лабораторне заняття 15.3. Ідентифікації актуальних кіберзагроз за допомогою MISP

Навчальна мета заняття: навчитися встановлювати та налаштовувати платформу ідентифікації актуальних кіберзагроз.

Кількість годин: 2 год.

Навчальні питання

1. Розгортання моделі MISP на віртуальній машині.
2. Тестування моделі MISP.

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику платформі ідентифікації актуальних кіберзагроз. Вказати порядок встановлення і налаштування MISP.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Основна

1. Кібербезпека для спеціальних агентів кіберполіції (лекції). OSCE. 2016.
2. Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
3. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

Додаткова

1. Allen L., Cardwell K. Advanced Penetration Testing for Highly-Secured Environments. Second edition. — Packt Publishing, 2016.
2. NIST Special Publication 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations. https://doi.org/10.6028/NIST.SP.800-53r5.

Інформаційні ресурси

1. https://csrc.nist.gov/
2. https://attack.mitre.org/
3. https://owasp.org/www-project-top-ten/
4. https://app.hackthebox.com/
5. https://www.root-me.org/
6. https://tryhackme.com/hacktivities?tab=practice