МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра кібербезпеки

Затверджено
На засіданні кафедри кібербезпеки
факультету прикладної математики та інформатики
Львівського національного університету імені Івана Франка
(Протокол № 15/23 від 29 серпня 2023 р.)

Завідувач кафедри .

Петро ВЕНГЕРСЬКИЙ

Силабус з навчальної дисципліни

“Події, опрацювання та аналіз логів”, що викладається в межах ОПП Кібербезпека першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 125 – кібербезпека та захист інформації

Львів 2023 р.

Назва дисципліни	Події, опрацювання та аналіз логів
Адреса викладання дисципліни	Львівський національний університет імені Івана Франка, вул. Університетська 1, м. Львів, Україна, 79000
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра кібербезпеки
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 125 – кібербезпека та захист інформації
Викладачі дисципліни	Костяк Марина Юріївна, к.т.н., доцент кафедри кібербезпеки Карпюк Роман Валентинович, асистент\аспірант кафедри кібербезпеки
Контактна інформація викладачів	Maryna.Kostiak@lnu.edu.ua roman.karpiuk@lnu.edu.ua
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/практичних занять (за попередньою домовленістю).
Сторінка курсу	https://ami.lnu.edu.ua/course/systemni-podii-ikh-opratsiuvannia-ta-analiz-kb
Інформація про дисципліну	Дисципліна “Події, опрацювання та аналіз логів” є нормативною дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається в 7-му семестрі в обсязі 3-ох кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей, розвиток системи знань про основні види, методи збору та аналізу системних подій\журналів подій в різних операційних системах та мережевих пристроях, оскільки “логування” є основним джерелом даних в кібербезпеці.
Мета та цілі дисципліни	Метою курсу є формування у студентів теоретичних знань щодо поняття “журналу подій”, які види є журналів подій, в чому їхня різниця в різноманітних інформаційних системах; практичних навиків щодо збору “логів” та базового, подальшого, аналізу.
Література для вивчення дисципліни	1. Practical Linux System Administration: A Guide to Installation, Configuration, and Management 1st Edition, O’Reilly, 2023 2. Офіційна документація Microsoft 3. Офіційна документація Red Hat 4. Офіційна документація Apple Inc 5. Event Logs - Windows Server Cookbook [Book] - O'Reilly
Обсяг курсу	Загальний обсяг: 90 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 26 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **познайомитись з:** • - логуванням Windows OS • - логуванням *NIX подібних систем • - логуванням Mac OS

	• - журналами подій базових служб (AD, DNS, DHCP, etc.) • - розширеним логуванням - Sysmon **вміти:** - читати журнали подій різних операційних систем - централізовано збирати журнали подій - базово аналізувати (знаходити релевантні події щодо кібербезпеки) Курс забезпечує набуття таких компетентностей: ІК, КЗ 1, КЗ 2, КЗ 5, КФ 2, КФ 3, КФ 5, КФ 8, КФ 9, КФ 11, КФ 12 ; та програмних результатів навчання: ПРН 2, ПРН 3, ПРН 4, ПРН 5, ПРН 6, ПРН 9, ПРН 10, ПРН 11, ПРН 12, ПРН 13, ПРН 14, ПРН 15, ПРН 16, ПРН 17, ПРН 18, ПРН 19, ПРН 20, ПРН 22, ПРН 27, ПРН 28, ПРН 29, ПРН 30, ПРН 31, ПРН 33, ПРН 34, ПРН 39, ПРН 41
Ключові слова	Кібербезпека, журнали подій, логування, операціні системи, sysmon, аналіз даних, критичність, logs.
Формат курсу	Очний Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у Схемі курсу нижче
Пререквізити	1. Основи кібербезпеки 2. Операційні системи та комп'ютерні мережі 3. Інструменти SecOps
Підсумковий контроль, форма	Екзамен у кінці 7 семестру
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції, лабораторні роботи, RangeForce платформа. Модульний контроль. Лекції та лабораторні: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу. Самостійна робота: репродуктивний метод, дослідницький метод.
Необхідне обладнання	Комп'ютери, комп'ютерні системи та мережі. Віртуальні машини. Інтернет ресурси.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • модульний контроль, тестування, усне опитування: 50% семестрової оцінки; максимальна кількість балів 50 • екзамен: 50% семестрової оцінки; максимальна кількість балів 50 Підсумкова максимальна кількість балів 100. **Академічна доброчесність**: Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахуванння викладачем, незалежно від масштабів плагіату чи обману. **Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні зайняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів визначених для виконання всіх видів письмових робіт та індивідуальних завдань, передбачених курсом.

	Література. Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих. П**олітика виставлення балів.** Враховуються бали набрані при поточному тестуванні, самостійній роботі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час практичного заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін. Жодні форми порушення академічної доброчесності не толеруються.
Питання до екзамену.	1. Що таке журнали подій? 2. Основні атрибути логів? 3. Де записуються логи на різних операціних системах? 4. Як централізовано збирати логи з різних операційних систем? 5. Що таке Sysmon? Навіщо він потрібен? 6. Розібрати по умовним полям журнал подій з IDS 7. Розібрати по умовним полям журнал подій з EDR 8. Розібрати по умовним полям журнал подій з MS Security log 9. Розібрати по умовним полям журнал подій з *NIX sshd 10. Розібрати по умовним полям журнал подій з *NIX root/user access 11. Розібрати по умовним полям журнал подій з *NIX crash data 12. Розібрати по умовним полям журнал подій з DNS 13. Розібрати по умовним полям журнал подій з DHCP
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу

Теми	**Тема, план, короткі тези**	**Форма діяльності/ заняття**	**Література.** **Інтернет-ресурси**	**Термін виконання**
1	**Introduction to the course**	лекція – 2 год самостійна робота – 2год	[1-5]	тиждень
2	Windows OS logging	лекція – 6 год лабораторна – 6 год самостійна робота – 2 год		3 тижні
3	**Centralized collection of logs from Windows OS**	лекція – 2 год лабораторна – 2 год самостійна робота –		тиждень

		2 год		
4	***NIX similar OS logging**	лекція – 6 год лабораторна – 6 год самостійна робота – 2 год		3 тижні
5	**Centralized collection of logs from *NIX similar systems**	лекція – 2 год лабораторна – 2 год самостійна робота – 2 год		тиждень
6	**MacOS logging**	лекція – 2 год лабораторна – 2 год самостійна робота – 2 год		тиждень
7	**Advanced logging with Sysmon**	лекція – 4 год лабораторна – 6 год самостійна робота – 2 год		2 тижні
9	**Analysis and correlation of typical events from various systems, services**	лекція – 2 год лабораторна – 2 год самостійна робота – 3 год		тиждень
10	**Finding basic patterns of attacking commands in event logs**	лекція – 6 год лабораторна – 6 год самостійна робота – 3 год		3 тижні
	Всього	**90**		