**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**

**БАНКІВСЬКИХ ТЕХНОЛОГІЙ ТА БІЗНЕСУ**

**КАФЕДРА КІБЕРБЕЗПЕКИ ТА СОЦІАЛЬНИХ НАУК**

**Лабораторна робота №2**

з дисципліни «Комп’ютерні системи та мережі»

Тема: «Изучение сетевых атак, а также инструментов

для аудита безопасности и проведения атак»

Виконав:

студент 3 курсу групи 303-Кб

Міліщук Андрій Ярославович

Перевірила:

к.е.н.,

Гордєєва Дар’я Валеріївна

Київ – 2020

# Часть 1: Изучение сетевых атак

Шаг 1: Изучите различные сетевые атаки.

**Світлофори в Лос-Анджелесі**

У 2006 році два інженера з організації дорожнього руху в Лос-Анджелесі зламали міські світлофори в знак протесту. Їм вдалося змінити програму роботи деяких світлофорів, розміщених на важливих ділянках, після чого вони стали горіти червоним кольором, що призвело до серйозних пробок.

**Сибірський нафтопровід**

Термін «Інтернет» приходить на розум щоразу, коли ми думаємо про кібер-атаках на критичну інфраструктуру. Але перша подібна кібер-атака сталася ще до появи Інтернету - в 1982 році.

Тоді група хакерів змогла встановити троян в SCADA-систему, яка контролювала роботу сибірського нафтопроводу, що призвело до потужного вибуху. Атака була організована ЦРУ, хоча про це не було відомо до 2004 року, коли колишній секретар Міністерства оборони США і радник Р. Рейгана Томас Рід опублікував свою книгу "At the Abyss: An Insider's History of the Cold War".

**Найвідоміший випадок кібер-атаки на критичну інфраструктуру: Stuxnet**

У 2008 році ми стали свідками одного з найбільш сумно відомих в історії випадків кібер-атак на критичні інфраструктури: Stuxnet. Зараз вже відомо, що це була скоординована атака ізраїльських і американських спецслужб, спрямована на зрив ядерної програми Ірану.

Вони створили хробака, який заразив комп'ютери, що керують урановими центрифугами на іранському заводі в Натанзі, в результаті чого вони стали працювати на повній швидкості, в той час як інженери на своїх моніторах спостерігали нормальний режим роботи. Це завдало фізичного збитку всім уранових центрифуг на заводі. Після цього випадку громадськість дізналася про подібного роду погрози.

Шаг 2: Заполните следующую форму по выбранной сетевой атаке.

Назва атаки – Stuxnet.

Тип атаки – мережевий хробак.

Дата атаки – 2008 рік.

Постраждалі комп'ютери / організації – всі уранові центрифуги на заводі.

Принцип дії і результати – були заражені комп’ютери, які керували урановими центрифугами на іранському заводі в Натанзі, в результаті чого вони стали працювати на повній швидкості, в той час як інженери на своїх моніторах спостерігали нормальний режим роботи. Результатом даної атаки є відкладення ядерної програми Ірана.

Варіанти нейтралізації – винайдені програми видалення вірусу Stuxnet у вільному доступі в інтернеті.

# Часть 2: Изучение инструментов аудита безопасности и проведения атак

Шаг 1: Изучите различные инструменты аудита безопасности и проведения атак.

Перечислите несколько инструментов, которые вы обнаружили в ходе изучения: ADManager Plus (ManageEngine), Windows-audit (PowerShell script), SekChek Security Auditing, Hardentools for Windows.

Шаг 2: Заполните следующую форму для выбранного инструмента аудита безопасности/проведения атак.

Найменування інструменту - SekCheck Security Auditing;

Розробник - Уильям Уэлч Делойт;

Тип інструменту - набір автоматизованих процесів для аналізу логічного профілю безпеки комп'ютера;

Місце використання – підприємтсва;

Вартість – 200$;

Опис ключових особливостей і можливостей продукту або інструменту - за результатами перевірок SekChek Security надає адміністраторам відповідні звіти. Отримані результати можуть порівнюватися з прийнятими в галузі стандартами та кращими практиками. Також за фактом порівняння може використовуватися рейтингова система.