**Міністерство освіти та науки України**

**Державний торговельно-економічний університет**

***Кафедра інженерії програмного забезпечення та кібербезпеки***

**ЗВІТ**

***З ЛАБОРАТОРНОЇ РОБОТИ № 4***

*з дисципліни*

**«ОСНОВИ КІБЕРБЕЗПЕКИ»**

**НА ТЕМУ:**

ВІЗУАЛІЗАЦИЯ «ЧОРНИХ» ХАКЕРІВ

(назва теми)

**Виконала:** студентка факультету інформаційних технологій

Групи 4 курсу 3

Авєріна Наталія Ігорівна

**Викладач:** Ковальова Людмила Ігорівна

Київ 2024

**Лабораторна робота №4**

**Тема**: візуалізация «чорних» хакерів

**Ціль**: вивчити та проаналізувати інциденти кібербезпеки

**Хід роботи:**

Сценарій 1:

Хакер під псевдонімом «WebJack» є членом хакерської групи «Cyberanarchy», який прагне грошей та слави, атакує корпоративні системи з метою викрадення конфіденційної інформації та вимагання викупу за її повернення. Він використовує соціально-інженерні атаки та фішингові кампанії для зламу паролів та отримання доступу до корпоративних мереж. Вразливістю атакованих компаній полягає в недостатній освітленості співробітників щодо соціально-інженерних атак та фішингу, а також в слабкому управлінні паролями та недостатньому захисті корпоративних мереж.

Для того, щоб запобігти цим атакам, компаніям слід було б організувати регулярні тренінги з кібербезпеки для персоналу, особливо щодо соціально-інженерних атак та фішингових кампаній. Також вони мали б вимагати від користувачів використання складних паролів та ввімкнення двофакторної автентифікації для додаткового захисту. Встановити системи моніторингу мережі для виявлення підозрілої активності, такої як надмірні спроби входу, і вчасно реагувати на потенційні загрози.

Сценарій 2:

Хакер, відомий під ім'ям «Virusall», є самотнім хакером, але іноді співпрацює з іншими злочинними групами. Його мотивом є хаос і руйнування. Він виконує цілеспрямовані атаки на урядові та фінансові організації з метою спричинення паніки та збитків. Хакер використовує шкідливі програми, такі як віруси, троянці та черви, для введення в корпоративні мережі та системи. Його мета - призвести до тимчасового або постійного припинення роботи систем, що може завдати серйозної шкоди репутації та фінансовому стану організації. Вразливість полягає в неактуалізованому програмному забезпеченні та недостатньому моніторингу мережі.

Щоб цього запобігти, організації мають забезпечити регулярне оновлення всього програмного забезпечення, включаючи операційні системи та застосунки, для виправлення вразливостей і запобігання використанню їх зловмисниками. Встановити і налаштувати ефективне антивірусне програмне забезпечення та файрволи для виявлення та блокування шкідливих програм та надмірної мережевої активності. Регулярно створювати та зберігати резервні копії даних для відновлення інформації в разі успішної атаки або зараження вірусами.

Сценарій 3:

Хакер, відомий як «EmmaSh» належить до хакерської групи «Datalords», яка спеціалізується на викраденні розробок та продажу їх на чорному ринку. EmmaSh влаштувала атаку на корпорацію «MedCorp», які займається розробкою лікарських препаратів. Хакер використовувала метод експлуатації вразливостей у веб-додатках та програмному забезпеченні, що використовувалося компанією, які дозволяли їй виконувати віддалені команди або отримувати несанкціонований доступ до даних. Недостатньо захищені сервери для зберігання конфіденційних даних та недостатньо ефективні механізми виявлення та відстеження несанкціонованого доступу створили можливості для хакера втрутитися в систему компанії і викрасти цінну інформацію.

«MedCorp» могла б застосувати такі заходи, для запобігання атакам такого типу:

* Проведення регулярних аудитів безпеки програмного забезпечення дозволить виявити вразливості в системі та вчасно їх виправити, перш ніж вони будуть використані зловмисниками.
* Використання безпечних методів програмування та врахування принципів безпеки в процесі розробки програмного забезпечення може допомогти уникнути багатьох типів вразливостей, що можуть бути використані для атак.
* Встановлення веб-файрволів та інших захисних заходів на серверах та в мережі компанії може допомогти виявити та блокувати спроби експлуатації вразливостей в програмному забезпеченні.
* Встановлення систем моніторингу безпеки, які надають можливість виявлення незвичайної активності та несанкціонованого доступу, дозволить оперативно виявляти атаки та приймати необхідні заходи для їх припинення.
* Проведення тренінгів та навчання персоналу щодо методів атак та заходів безпеки може допомогти персоналу розпізнавати підозрілі ситуації та вчасно повідомляти про них.