Модуль 4. Основи хакінгу та розслідування інцидентів в ISC/SCADA системах

Лекція 2: **Поширені техніки та інструменти хакерства**

Мета лекції

забезпечити глибоке практичне розуміння розповсюджених технік і інструментів кібератак на системи ICS/SCADA, а також надати знання та навички для їх ефективного виявлення та протидії в операційних технологічних (OT) середовищах.

Основні

Розуміння векторів атак

Пояснити класичні вектори експлуатації, такі як переповнення буфера, SQL-ін'єкції та різновиди шкідливого програмного забезпечення (віруси, черв'яки, ransomware), у контексті ICS/SCADA систем.

Захист та пом'якшення

Продемонструвати ефективні методи захисту та пом'якшення: безпечне кодування, сегментацію мережі та DMZ, реалізацію принципу allowlist та контроль знімних носіїв.

Інструменти атакера

Навчити використовувати та розуміти ключові інструменти як для захисника, так і для атакера, включаючи Metasploit, Kali Linux, Snort та OSINT.

Виявлення та моніторинг

Розвинути навички виявлення та моніторингу загроз: аналіз сигнатур та аномалій, інтеграція з SIEM-системами, а також використання індикаторів компрометації.

Етичні та правові аспекти

Закріпити розуміння етичних та правових рамок етичного хакінгу та відповідального використання інструментів у сфері кібербезпеки.

Методологія пентесту для OT

Відпрацювати безпечну методологію проведення пентесту для OT-середовищ: робота з тестовими стендами, обмеження впливу на виробничі процеси та розробка плану відкату.

2.1. Переповнення буфера, SQL-ін'єкції, шкідливе ПЗ (черв'яки, віруси)

2.1.1. Еволюція кіберзагроз для промислових систем

Традиційні IT-загрози

Хакери активно діляться інформацією та техніками на веб-сайтах або в даркнеті, продають "0-day" експлойти. Будь-який зловмисник, зацікавлений в атаці на SCADA-системи, може легко отримати знання про їх операційні системи, мережі та компоненти.

- Веб-сайти з програмним забезпеченням для злому
- Поради щодо створення вірусів та хробаків
- Інструкції для атак на комп'ютерні системи

Існує безліч ресурсів, які пропонують програмне забезпеченням та поради щодо злому, що робить кіберзлочинність більш доступною для широкого кола зловмисників.

2.1.2. Переповнення буфера в промислових системах

Механізм атаки

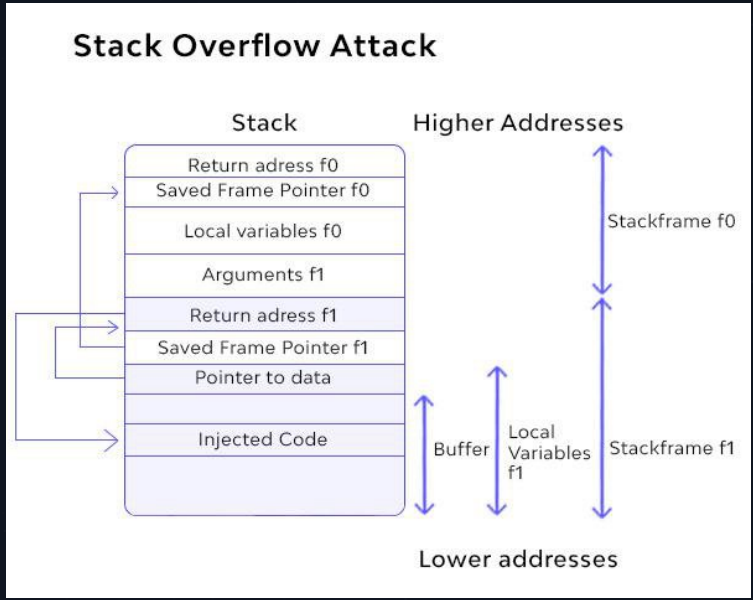
Програма намагається записати дані за межі виділеної області пам'яті (буфера), що призводить до пошкодження сусідніх областей пам'яті.

Наслідки

Може призвести до збою програми або, що гірше, дозволити зловмиснику виконати довільний код в системі.

Специфіка ICS/OT

Незважаючи на поширену думку про стійкість ПЛК, вони запускають програмне забезпечення і можуть бути схильні до таких атак.



У традиційних IT-системах переповнення буфера є однією з найдавніших і найнебезпечніших вразливостей. Деякі старі промислові протоколи були стійкими до переповнення буфера, оскільки відхилення від очікуваної структури повідомлення призводило до його відкидання. Однак з переходом на більш складні протоколи та операційні системи, ризик зростає.

2.1.3. SQL-ін'єкції: загроза для SCADA-баз даних

Механізм атаки

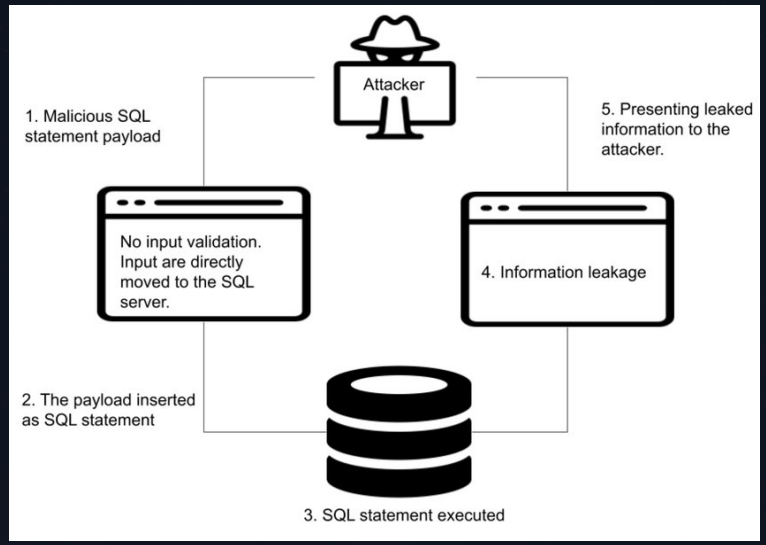
SQL-ін'єкція використовує вразливість, спричинену неправильними практиками програмування. Спеціально сформований зловмисний текст вводиться в поля введення даних на веб-сторінках, змушуючи логіку виконувати вбудовану SQL-команду.

Наслідки успішної атаки:

- Розкриття конфіденційних таблиць бази даних
- Зміна або знищення таблиць та їх даних
- Компрометація цілісності системи

ISA рекомендує розміщувати реляційні бази даних в DMZ для захисту SCADA/DCS систем від надмірного завантаження даних та потенційних шляхів атаки.

⚠ **Увага!** Сучасні SCADA-системи часто використовують комерційні реляційні бази даних (SQL Server®, Oracle®, OSI-PI®), що робить їх вразливими до SQL-ін'єкцій.



2.1.4. Шкідливе програмне забезпечення: класифікація загроз

Віруси

Шкідливі програми, які приєднуються до легітимних програм та поширюються, коли ці програми виконуються, заражаючи інші файли в системі.

Ренсомвер

Програми-вимагачі, які блокують доступ до систем або даних, вимагаючи викуп. LockerGoga, WannaCry та Petya завдали мільярдних збитків і зачепили робочі станції АСУ ТП.

Черв'яки

Самореплікуючі шкідливі програми, які поширюються по мережі, не потребуючи втручання користувача. Можуть споживати мережеві ресурси та поширювати додаткове шкідливе ПЗ.

Руткити

Набори інструментів, що дозволяють зловмиснику приховати свою присутність та діяльність у скомпрометованій системі, ускладнюючи виявлення та видалення.

2.1.5. Шляхи проникнення шкідливого ПЗ в ICS/SCADA

Корпоративна мережа

Системи SCADA часто підключені до корпоративної WAN, яка має доступ до Інтернету, створюючи шлях для шкідливого ПЗ.

Знімні носії

Співробітники можуть ненавмисно занести шкідливе ПЗ за допомогою USB-накопичувачів. Приклад Stuxnet показує поширення через USB навіть в ізольовані системи.

Соціальна інженерія

Фішингові атаки або "лист-бомби" з шкідливими вкладеннями для компрометації комп'ютерів у корпоративній мережі з подальшим проникненням в OT-мережу.

Скомпрометовані постачальники

Шкідливе ПЗ може поширюватися через скомпрометовані веб-сайти завантаження програмного забезпечення/прошивок виробників ICS.

2.1.6. Рекомендації щодо захисту від базових загроз

01

Загартовування систем

Мінімізація поверхні атаки шляхом видалення або відключення непотрібних служб, утиліт та програм в промислових системах.

02

Регулярне оновлення

Своєчасне тестування та застосування патчів для відомих вразливостей, враховуючи вимоги до безперервності роботи в ОТ-середовищах.

03

Безпечне програмування

Дотримування практик безпечного кодування для запобігання вразливостям, таким як переповнення буфера та SQL-ін'єкції.

04

Антивірусний захист

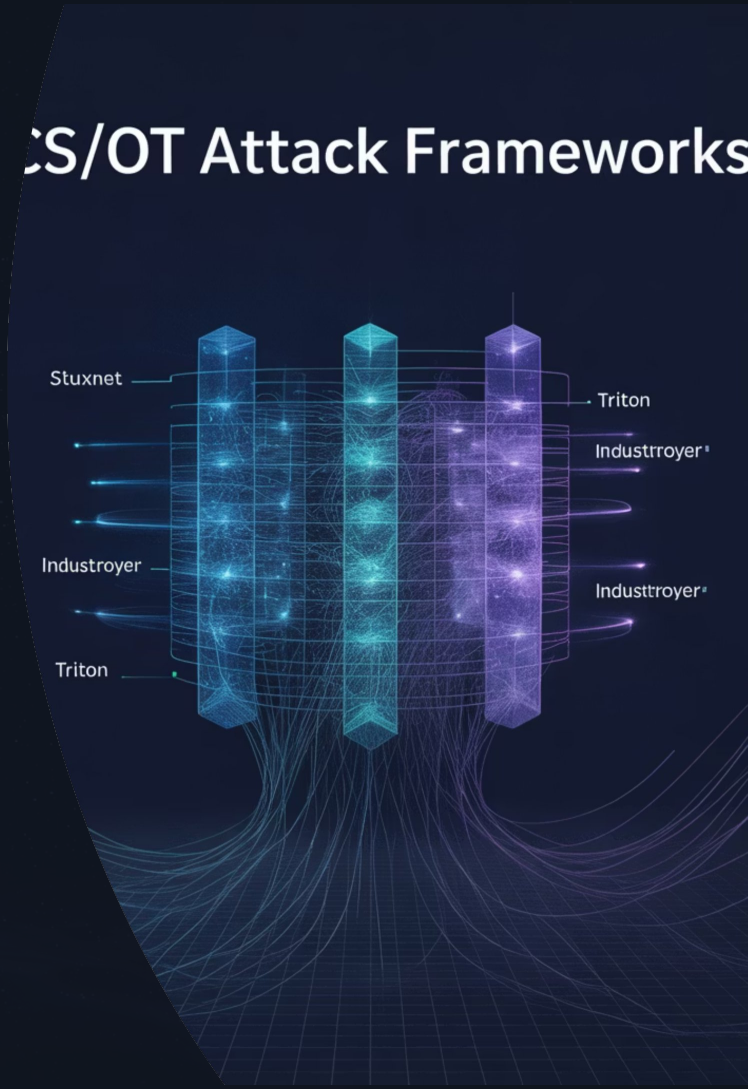
Використання антивірусних програм, систем кінцевого захисту (EDR) та спеціалізованих скануючих станцій для перевірки знімних носіїв.

05

Мережева сегментація

Ізоляція критичних ICS/SCADA систем від корпоративних мереж та Інтернету за допомогою DMZ та фаєрволів.

2.2. Специфічні фреймворки атак ICS/OT (наприклад, Stuxnet, Industroyer, Triton)



2.2.1. Stuxnet: перша кібер-фізична зброя

> Stuxnet, що з'явився у 2010 році, вважається "Хіросімою" кібербезпеки та міжнародних відносин, оскільки це був перший відомий випадок кібератаки однієї нації-держави на критичну інфраструктуру іншої.

Мета атаки

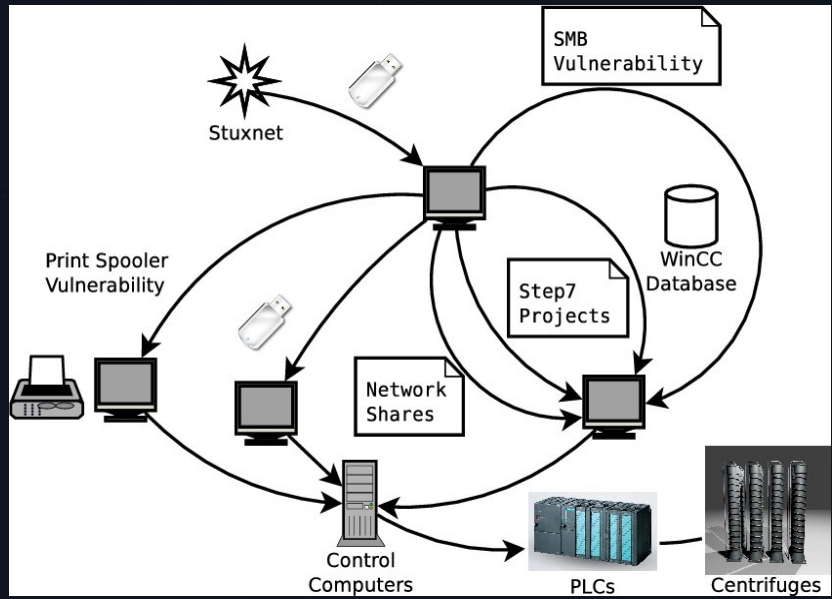
Іранська ядерна програма, зокрема центрифуги для збагачення урану. Stuxnet був розроблений для пошкодження центрифуг шляхом маніпуляцій з ПЛК Siemens.

Механізм дії

Два основні "кібер-фізичні" корисні навантаження: перевищення тиску у центрифугах та маніпуляції швидкістю роторів для виведення їх з ладу.

2.2.2. Stuxnet: технічні деталі атаки

1. **Доставка**
   Поширення через USB-накопичувачі, незважаючи на фізичну ізоляцію цільового об'єкта.
2. **Експлуатація**
   Використання чотирьох раніше невідомих вразливостей "нульового дня" у Windows, що свідчить про значні інвестиції.
3. **Проникнення**
   Зараження ПЛК Siemens через SCADA-мережу, використовуючи навіть "захардкоджені" паролі.
4. **Маскування**
   Надання фальшивої інформації операторам, приховування шкідливих дій та створення ілюзії нормальної роботи.

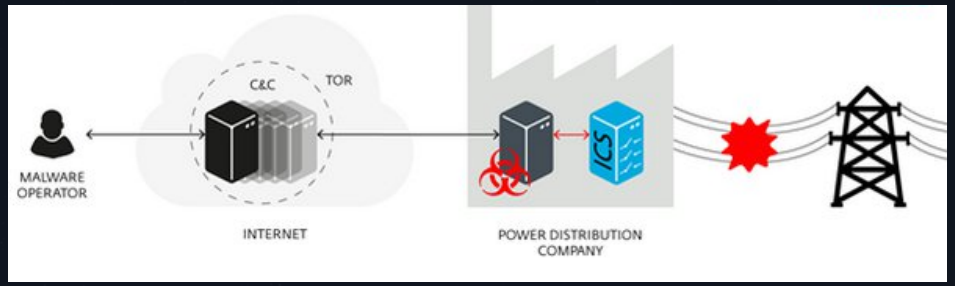


Хоча Stuxnet не зміг значно затримати іранську програму через передчасне виявлення, він "відкрив скриньку Пандори" кібер-фізичних атак. Код потрапив в Інтернет, дозволивши іншим зловмисникам вивчати методи та адаптувати їх для нових атак.

2.2.3. Industroyer: атака на енергетичну інфраструктуру

Характеристики атаки

Шкідливий фреймворк, використаний для атаки на енергетичні системи України у 2016 році, що призвела до відключення електроенергії. Industroyer є одним із найбільш просунутих зразків шкідливого ПЗ для ICS.



Ключові особливості:

- Модульна архітектура для легкого додавання підтримки нових протоколів
- Максимізація успіху атаки через адаптивність
- Спеціальна розробка для енергетичних систем

Атака була націлена на комунікаційні протоколи електроенергетичних мереж, демонструючи експлуатацію застарілих протоколів без належних механізмів безпеки.

2.2.4. Triton: атака на системи безпеки

Атака Triton 2017 року на нафтопереробному підприємстві Близького Сходу була спрямована на системи безпеки (SIS) і була особливо небезпечною через потенціал спричинення фізичної шкоди та людських жертв.

Мета атаки

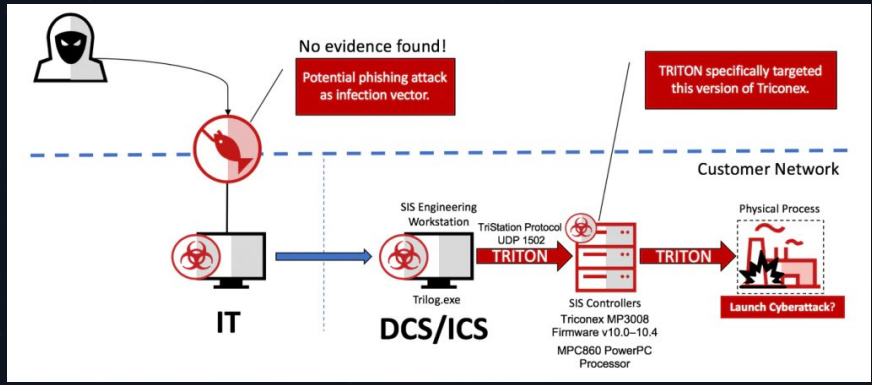
Маніпулювання контролерами функціональної безпеки Triconex для потенційного спричинення фізичної шкоди замість простого порушення роботи.

Тривалість

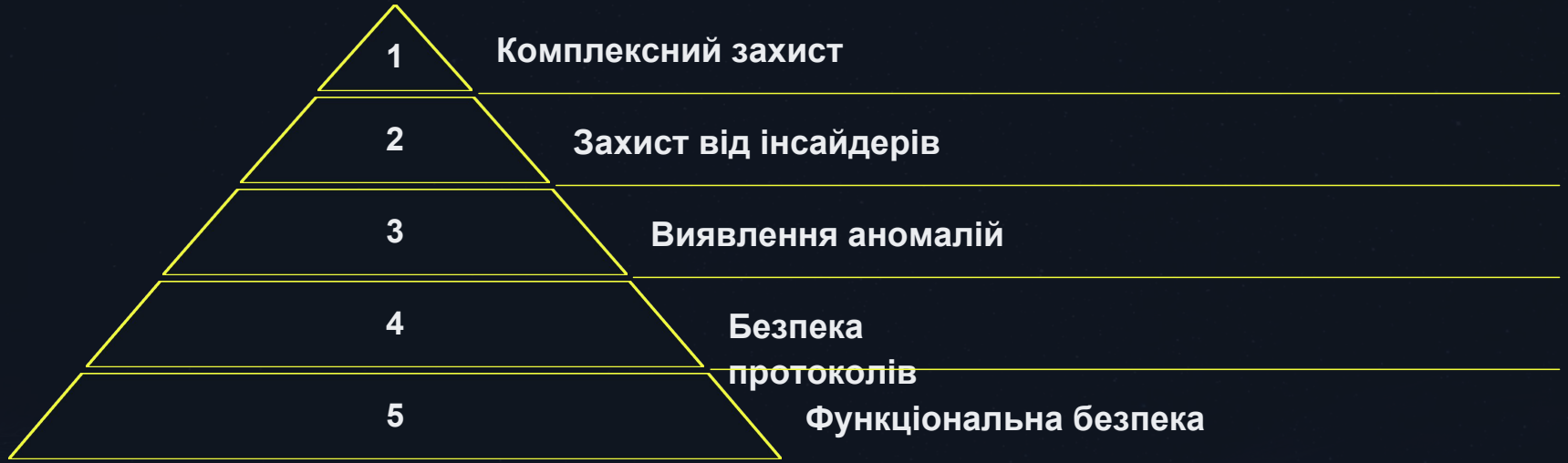
Зловмисники контролювали технологічну мережу підприємства кілька місяців до виявлення атаки.

Механізм доступу

Використання привілейованого профілю користувача техпідтримки виробника, що підкреслює ризики "бекдорів" та неконтрольованого доступу.

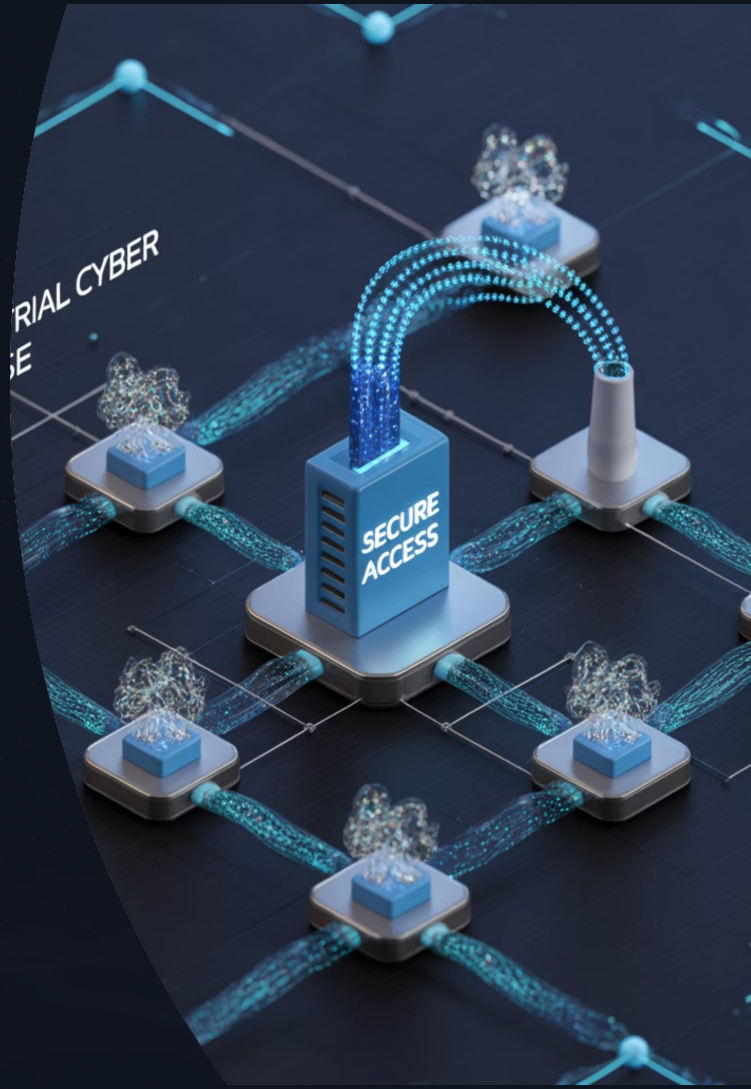


2.2.5. Уроки знакових кібератак на ICS/OT



Ці знакові атаки підкреслюють, що загрози для ICS/OT є реальними, можуть мати руйнівні фізичні наслідки та вимагають постійної уваги до кібербезпеки. Необхідно впроваджувати багаторівневий захист (Defense-in-Depth), що охоплює як кібер-, так і фізичні аспекти безпеки.

2.3. Тестування на проникнення та концепції етичного хакінгу для ICS/OT



2.3.1. Тестування на проникнення в ICS/OT: особливості

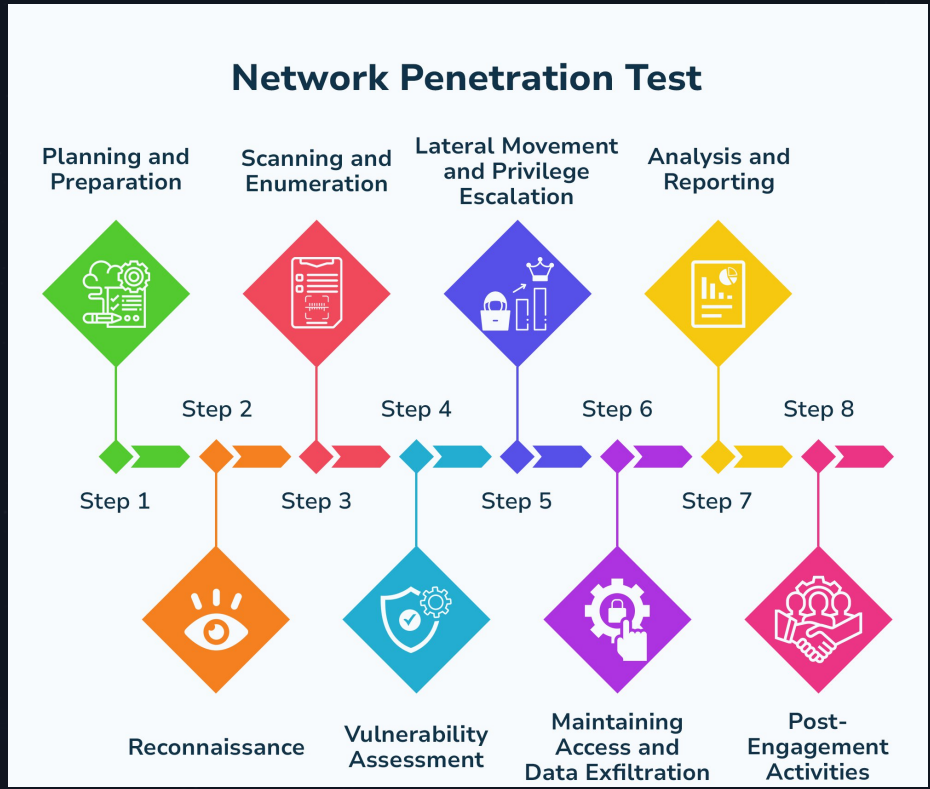
Етичні міркування

Найважливішим аспектом пентесту в ICS/OT є забезпечення безпеки та доступності системи. На відміну від IT, збій в OT-середовищі може мати катастрофічні фізичні наслідки: загрозу життю людей, екологічні збитки або пошкодження обладнання.

Пріоритети безпеки в ICS/OT:

1. Фізична безпека (людей, навколишнього середовища)
2. Доступність
3. Цілісність
4. Конфіденційність

⚠ Проведення пентесту на "живій" виробничій системі без ретельного планування та дозволу є неприпустимим!



2.3.2. Методологія атак: SANS ICS Kill Chain

Кібер-вторгнення

Фаза, де зловмисник отримує початковий доступ до мережі через різні вектори атаки.

Розробка атаки на ICS

Збір інформації про цільові ICS-компоненти, розробка шкідливого ПЗ або експлойтів. Може включати реверс-інжиніринг ПЛК або протоколів.

Виконання атаки на ICS

Фаза, де шкідливий вплив реалізується на фізичному процесі, що може призвести до реальних наслідків.

Методології атаки, такі як MITRE ATT&CK Framework, надають тактики, техніки та процедури (TTPs), які можуть бути використані як атакерами, так і захисниками для розуміння та імітації кібератак.

2.3.3. Особливості тестування промислових систем

Реверс-інжиніринг ПЛК

Через пропрієтарний характер деяких компонентів ICS, пентестерам може знадобитися реверс-інжиніринг для розуміння роботи та виявлення вразливостей.

Відсутність облікових даних

Часто в ICS-системах не використовуються складні облікові дані або їх взагалі немає, що робить їх особливо вразливими до атак.

Маніпуляції з фізичними процесами

У OT-середовищі атака може призвести до прямих фізичних маніпуляцій, як це було у випадку Stuxnet з центрифугами.

Вразливості Windows-середовищ

Багато сучасних SCADA-систем побудовані на комерційному ПЗ та ОС, таких як Microsoft Windows, що вимагає відповідних навичок пентесту.

2.3.4. Рекомендації для безпечного пентестингу

1 **Суворе планування та контроль**

Кожен пентест повинен супроводжуватися детальним планом, що включає цілі, обсяг, методи та механізми відкоту, а також чіткі дозволи від керівництва.

2 **Використання тестових середовищ**

Завжди віддавати перевагу тестуванню на ізольованих тестових стендах або віртуальних машинах, що імітують виробниче середовище.

3 **Спеціалізовані навички**

Команди пентестерів ICS/OT повинні мати глибокі знання як IT-безпеки, так і унікальних аспектів промислових систем, включаючи протоколи, обладнання та фізичні процеси.

4 **Принцип "Assume Breach"**

Розробка сценаріїв, які припускають отримання початкового доступу, для зосередження на виявленні та стримуванні латерального переміщення та впливу на OT-системи.

2.4. Інструменти: Metasploit, Kali Linux, Snort, OSINT інструменти

2.4.1. Metasploit Framework: потужний інструмент експлуатації

Функціональність

Metasploit — це потужний фреймворк для тестування на проникнення, який автоматизує експлуатацію відомих вразливостей. Хоча він переважно використовується в IT-світі, з появою Stuxnet у нових версіях з'явилися модулі для ICS.

Можливості:

- Широкий спектр атак від VNC-ін'єкцій до експлуатації вразливостей
- Значне спрощення процесу експлуатації відомих вразливостей
- Модулі для промислових протоколів та систем

Подвійне використання: Пентестери використовують Metasploit для перевірки власних систем, а зловмисники - для досягнення своїх цілей.

2.4.2. Kali Linux: операційна система для кібербезпеки

Сканування вразливостей

Nmap, OpenVAS, sqlmap для виявлення відкритих портів, служб та потенційних вразливостей в мережевій інфраструктурі.

Веб-додатки

Burp Suite, Nikto для аналізу безпеки веб-інтерфейсів SCADA-систем та виявлення вразливостей веб-додатків.

Бездротові атаки

Aircrack-ng та інші інструменти для тестування безпеки бездротових мереж та виявлення слабких точок доступу.

Цифрова криміналістика

Інструменти для аналізу інцидентів, відновлення даних та розслідування кібератак на промислові системи.

Kali Linux — це спеціалізований дистрибутив Linux для тестування на проникнення та цифрової криміналістики з величезною кількістю вбудованих інструментів, включаючи Metasploit Framework та Armitage.

2.4.3. Snort: система виявлення вторгнень для ICS

Архітектура та можливості

Snort — це система виявлення вторгнень в мережу (NIDS) з відкритим вихідним кодом, яка може працювати як система запобігання вторгненням (NIPS). Має модульну архітектуру та гнучку мову правил.

Функціональність:

- Сигнатурне виявлення відомого шкідливого ПЗ
- Аналіз шкідливого трафіку та віддалених експлойтів
- Виявлення аномального трафіку
- Моніторинг невідомих IP-адрес та портів

DHS фінансувало розробку наборів правил Snort для промислових протоколів (Modbus/IP, IEC-60870-5-104, DNP3), що робить його цінним для ICS-мереж.

2.4.4. OSINT: розвідка на основі відкритих джерел

OSINT (Open-Source Intelligence) — це збір та аналіз інформації з публічно доступних джерел. Це критично важлива фаза будь-якої кібератаки, оскільки дозволяє зловмисникам збирати дані про цільову систему або мережу.

Веб-пошукові системи	Спеціалізовані системи	DNS-розвідка
Google, Bing, DuckDuckGo з "Google Dorks" для виявлення веб-інтерфейсів ICS або чутливої інформації в Інтернеті.	Shodan та Censys для пошуку промислових пристроїв, підключених до Інтернету, за портами, протоколами та виробниками.	DNSdumpster, SubFinder, Amass для пасивного виявлення субдоменів, IP-адрес та мережевої інфраструктури.

2.4.5. Shodan: пошукова система для IoT та ICS

Можливості пошуку

Shodan індексує інформацію про пристрої та сервіси, підключені до Інтернету, що робить його потужним інструментом для виявлення промислових систем.

Критерії пошуку:

- Порти: 502 для Modbus, 44818 для Ethernet/IP
- Протоколи: Modbus, S7, DNP3, BACnet
- Виробники: Schneider, Rockwell, Siemens, Allen Bradley
- Типи активів: PLC, HMI, SCADA-сервери

⊗ Виявлення внутрішніх IP-адрес через Shodan свідчить про низький рівень безпеки та неправильну конфігурацію мережі.

2.4.6. Додаткові OSINT інструменти для розвідки

Censys

Проводить глибоке сканування всіх TCP-портів та зосереджується на цифрових сертифікатах для виявлення веб-сервісів та їх конфігурацій.

WHOIS

Дозволяє знайти контактну інформацію про власників доменів та IP-адрес, що може бути корисним для соціальної інженерії.

Соціальні мережі

LinkedIn для пошуку інформації про співробітників, структуру організації та використовуване обладнання/програмне забезпечення.

Витоки даних

Have I Been Pwned, Dehashed для пошуку скомпрометованих імен користувачів та паролів співробітників організації.

2.4.7. Практичні рекомендації щодо використання інструментів

01

Навчання та тренування

Фахівці з кібербезпеки повинні регулярно навчатися та тренуватися з використанням цих інструментів для виявлення вразливостей та оцінки ефективності заходів захисту.

02

Проактивний моніторинг

Організації повинні використовувати OSINT-інструменти для моніторингу власної присутності в Інтернеті та виявлення потенційно чутливої інформації.

03

Використання для захисту

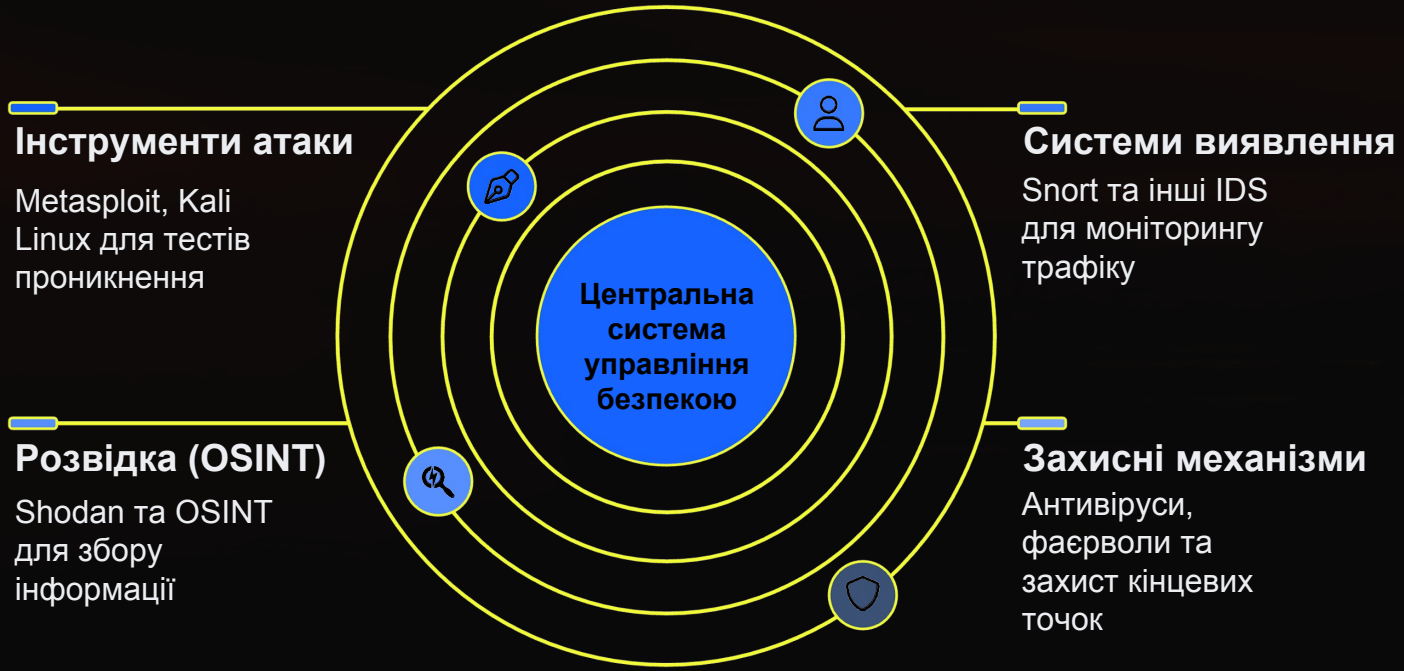
Інструменти, такі як Snort, можуть бути налаштовані для виявлення активності, характерної для використання Metasploit або інших хакерських інструментів.

04

Створення "медових пасток"

Розгортання імітацій ПЛК, SCADA-серверів та інших активів для залучення зловмисників та вивчення їхніх тактик, технік та процедур.

2.4.8. Інтеграція інструментів у стратегію кібербезпеки



Знання та вміле використання цих інструментів є ключовим як для атакерів, так і для захисників. Організації повинні розуміти можливості цих інструментів, щоб ефективно захищатися від них та використовувати їх для покращення власної безпеки.

2.5. Висновки: готовність до сучасних кіберзагроз

> Конвергенція IT та OT технологій створює нові можливості, але також відкриває нові вектори атак. Розуміння інструментів та методів зловмисників є першим кроком до ефективного захисту.

Постійне навчання

Кіберзагрози постійно еволюціонують, тому фахівці повинні регулярно оновлювати свої знання про нові техніки та інструменти атак.

Проактивний підхід

Використання тих самих інструментів, що й зловмисники, для виявлення власних вразливостей до того, як їх експлуатують.

Комплексна стратегія

Поєднання технічних заходів, навчання персоналу та організаційних процедур для створення надійної системи кібербезпеки.

Список використаних джерел

1. Radvanovsky, R., & Brodsky, J. (2016). Handbook of SCADA/Control Systems Security (2nd ed.). CRC Press.

2. Colbert, E. J. M., & Kott, A. (Eds.). (2016). Cyber-Security of SCADA and Other Industrial Control Systems. Springer.

3. Shaw, W. T. (2020). Cybersecurity for SCADA Systems (2nd ed.). PennWell Books.

4. Brooks, C. J., & Craig Jr., P. A. (2022). Practical Industrial Cybersecurity: ICS, Industry 4.0, and IIoT. Wiley.

5. Kouremetis, M. (2014). Defending a SCADA System with the Snort IDS [Presentation]. ECSSE Department.

6. National Telecom Regulatory Authority (NTRA). (2022). IoT Cyber Security Framework. EG-CERT.

7. Emerson. (2021). Industrial Security in SCADA Systems: IEC 62443-3-3 Certification. Emerson Automation Solutions.

8. Krotofil, M. (2023). Industrial Control Systems: Engineering Foundations and Cyber-Physical Attack Lifecycle. Technical White Paper.

9. UtilSec, LLC. (2024). Getting Started in ICS/OT Cyber Security: Lab Manual. UtilSec.

Дякую за увагу!