Зміст

ВСТУП

В сучасному цифровому світі, де інформація стала найціннішим активом, безпека інформаційних систем стає надзвичайно важливою. Захищеність інформаційних систем від несанкціонованого доступу, втручання, втрати або пошкодження є критичною для забезпечення конфіденційності, цілісності та доступності інформації.

Однак, зростаючі загрози від хакерських атак, вразливості програмного забезпечення, соціально-інженерних методів та інших форм зловживання вимагають від організацій усвідомлення необхідності оцінки рівня захищеності їх інформаційних систем.

Оцінка рівня захищеності інформаційної системи є комплексним процесом, який дозволяє оцінити поточний стан безпеки ідентифікуваної інформаційної системи. Цей процес включає аналіз загроз безпеці, виявлення вразливостей, оцінку ризиків та ефективності заходів безпеки.

Метою оцінки рівня захищеності інформаційної системи є не лише виявлення потенційних загроз та вразливостей, але й розробка рекомендацій щодо покращення безпеки. Це може включати впровадження нових технологій, зміну політик безпеки, навчання персоналу та імплементацію контрольних механізмів.

У даній роботі ми розглянемо основні аспекти оцінки рівня захищеності інформаційної системи, включаючи методи та інструменти, використовувані для проведення оцінки. Також будуть розглянуті ключові етапи процесу оцінки, від визначення об'єкта дослідження до отримання висновків та рекомендацій.

Необхідність оцінки рівня захищеності інформаційної системи стає все більш актуальною в сучасному цифровому середовищі. Розуміння принципів, методів та практик оцінки рівня захищеності є важливим завданням для будь-якої організації, що прагне забезпечити безпеку своїх інформаційних активів та відповідати вимогам сучасного інформаційного світу.

Розділ 1. Теоретичні аспекти захисту інформації в інформаційних системах.

1.1. Загальні поняття інформаційної безпеки

Інформаційна безпека - це захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, перекручення, модифікації або знищення. Вона охоплює різні принципи, практики та технології, призначені для забезпечення конфіденційності, цілісності та доступності інформації.

Однією з фундаментальних концепцій інформаційної безпеки є конфіденційність, яка передбачає збереження конфіденційної інформації приватною і доступною лише уповноваженим фізичним або юридичним особам. Зазвичай це досягається за допомогою шифрування, контролю доступу та захищених каналів зв'язку.

Цілісність - ще один ключовий аспект інформаційної безпеки. Вона стосується точності, повноти та достовірності інформації і передбачає запобігання несанкціонованим модифікаціям, змінам або видаленню. Для забезпечення цілісності даних використовуються такі методи, як перевірка даних, контрольні суми та цифрові підписи.

Доступність є третім стовпом інформаційної безпеки і зосереджена на забезпеченні того, щоб інформація та інформаційні системи були доступними та придатними для використання в разі потреби. Це передбачає впровадження надлишковості, систем резервного копіювання та планів аварійного відновлення для пом'якшення наслідків потенційних збоїв або відмов.

Аутентифікація та авторизація є важливими поняттями в інформаційній безпеці. Автентифікація перевіряє ідентичність користувачів або систем, які намагаються отримати доступ до інформації або ресурсів, тоді як авторизація визначає привілеї та дозволи, надані автентифікованим фізичним або юридичним особам.

Управління ризиками відіграє вирішальну роль в інформаційній безпеці. Воно передбачає виявлення, оцінку та зменшення потенційних ризиків і вразливостей, які можуть поставити під загрозу безпеку інформаційних систем. Стратегії управління ризиками включають проведення оцінки ризиків, впровадження засобів контролю, а також постійний моніторинг та оцінку ефективності заходів безпеки.

Поінформованість і навчання з питань безпеки є життєво важливими компонентами інформаційної безпеки. Ознайомлення користувачів з найкращими практиками, політиками та процедурами безпеки допомагає розвивати культуру безпеки та зменшує ризик людських помилок або недбалості, що призводять до інцидентів безпеки.

Дотримання правових, регуляторних та галузевих стандартів є важливим фактором інформаційної безпеки. Організації повинні дотримуватися відповідних законів і правил, що регулюють захист конфіденційних даних, таких як інформація, що дозволяє ідентифікувати особу (PII), або фінансова документація. Нормативні документи, такі як Загальний регламент про захист даних (GDPR) або Стандарт безпеки даних індустрії платіжних карток (PCI DSS), надають рекомендації щодо забезпечення інформаційної безпеки.

Нарешті, безперервний моніторинг, реагування на інциденти та аудит безпеки є важливими для своєчасного виявлення та реагування на інциденти або порушення безпеки. Це передбачає моніторинг мережевого трафіку, системних журналів і дій користувачів, а також створення планів реагування на інциденти та проведення регулярних оцінок безпеки.

Загалом, інформаційна безпека - це багатовимірна дисципліна, яка вимагає поєднання технічних, організаційних і людських факторів для захисту цінних інформаційних активів і підтримки довіри окремих осіб, організацій і суспільства в цілому.

1.2. Класифікація загроз та видів атак на інформаційні системи

Класифікація загроз і типів атак на інформаційні системи є важливим аспектом у сфері кібербезпеки. Розподіл цих загроз та атак на різні категорії допомагає краще зрозуміти їхні характеристики та ризики, які вони становлять для інформаційних систем.

Одна з основних категорій класифікації базується на джерелі атаки. Це означає, що атаки можуть здійснюватися зовнішніми агентами або внутрішніми особами, які мають санкціонований доступ до системи. Зовнішні атаки можуть походити з інтернету або зовнішніх мереж, тоді як внутрішні атаки відбуваються всередині самої організації або системи.

Інша категорія класифікації стосується методів, які використовуються для здійснення атак. Сюди можна віднести такі види атак, як вторгнення через використання шкідливого програмного забезпечення або системних вразливостей, соціальна інженерія, фішинг, перехоплення даних, DoS або DDoS-атаки та багато інших. Кожен тип атаки має свої особливості та наслідки для інформаційної системи.

Крім того, атаки можна класифікувати на основі їхніх цілей, таких як несанкціонований доступ до системи, розкриття конфіденційної інформації, маніпулювання даними, порушення цілісності системи або відмова в обслуговуванні.

Класифікація загроз і типів атак на інформаційні системи є важливим інструментом для аналізу, розуміння і визначення заходів безпеки. Вона допомагає розробникам систем безпеки та мережевим адміністраторам бути в курсі потенційних загроз і вживати ефективних заходів для їх запобігання та виявлення.

Загрози інформаційній безпеці можна класифікувати за декількома критеріями, а саме:

1. За джерелом походження:

   - внутрішні, тобто викликані діяльністю працівників організації, які мають доступ до інформаційної системи;
   - зовнішні, тобто викликані діяльністю осіб або організацій, які не мають дозволу на доступ до інформаційної системи.

2. За метою:

   - шпигунство, тобто отримання конфіденційної інформації;

- порушення цілісності, тобто зміна або видалення інформації;
- виток інформації, тобто несанкціоноване поширення конфіденційної інформації;
- відмова в обслуговуванні, тобто перешкоджання нормальній роботі інформаційної системи.

3. За способом реалізації:

- соціально-інженерні атаки, тобто використання соціальної інженерії для отримання доступу до інформаційної системи;
- фізичні атаки, тобто напад на апаратну частину інформаційної системи;
- логічні атаки, тобто використання програмних вразливостей для отримання доступу до інформаційної системи;
- комбіновані атаки, тобто використання кількох способів одночасно для отримання доступу до інформаційної системи.

До типових видів атак на інформаційні системи можна віднести наступні:

- Перехоплення даних (Sniffing) - це використання програм або пристроїв для перехоплення і аналізування мережевого трафіку з метою зловживання конфіденційної інформації, яка передається між комп'ютерами.

- Введення ложних даних (Spoofing) - це використання підроблених IP-адрес для зловживання доступом до мережі, яка базується на довірі до певної адреси.

- Атака методом переповнення буфера (Buffer overflow) - це використання програмного коду, що викликає переповнення буфера, що дозволяє зловмиснику виконувати віддалені команди або запускати зловмисний код на вразливій системі.

- Віруси та черв'яки (Viruses and Worms) - це програми, які можуть розповсюджуватися по мережі та внедрюватися у системи з метою пошкодження, видалення або крадіжки інформації.

- Атака методом зміни поведінки (Behavioral attack) - це використання програмного коду, який може змінювати поведінку вразливої системи, зловмисник може змінити настройки, перехоплювати трафік, виконувати інші дії без дозволу користувача.

- Атака з використанням вразливостей в програмному забезпеченні (Exploiting software vulnerabilities) - це використання вразливостей в програмному забезпеченні для виконання зловмисних дій, таких

як встановлення шкідливого програмного забезпечення або отримання несанкціонованого доступу до системи.

- Атака методом соціальної інженерії (Social engineering attack) - це використання маніпулювання людьми з метою отримання доступу до інформації або системи

Статистика атак за 1-й квартал 2022 року:

На основі графіків кібератак, опублікованих за перші три місяці 2022 року, була складена статистика. За цей період було зафіксовано 646 подій, що складає приблизно 7,18 подій на день. Ця кількість помітно менша, ніж 713 подій, зібраних протягом першого кварталу 2021 року.

За даними статистики, кіберзлочинність продовжує лідирувати в мотиваційній діаграмі з показником 70,3%. Однак цей відсоток значно нижчий, ніж рік тому (86%), що є прямим результатом зростання кількості подій, спровокованих хактивізмом, кібершпигунством та навіть кібервійною, які характеризують останній період в контексті того, що відбувається в Україні. Віруси та шкідливі програми також продовжують лідирувати в діаграмі методів атак з показником 31,3%, що майже рівно до 32,3% у минулому році. Діаграма розподілу цілей також дуже схожа на ту, що була рік тому, з кількома галузями, що мають найвищий показник 25,9%, порівняно з 16,7% у попередньому році.

Ці дані свідчать про продовження трендів в кібератаках та мотиваціях, що показують необхідність подальшого зміцнення заходів з кібербезпеки та захисту інформаційних систем.

Загальна кількість подій:

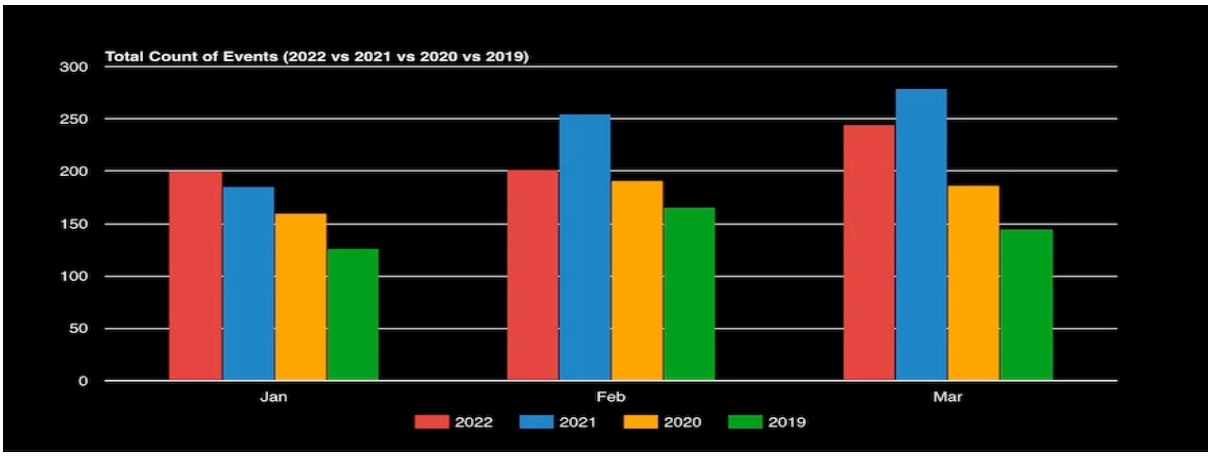


Рис 1.2.1. – Графік кібератак за інші роки

Щоденний тренд мотивів:

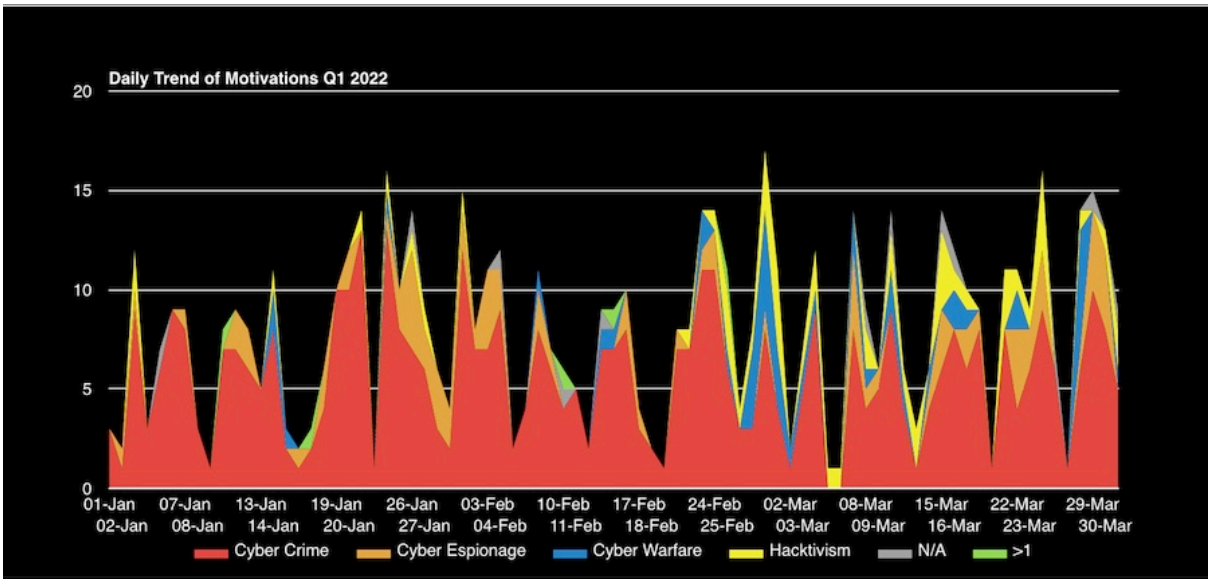


Рис 1.2.2. – Графік послаблень

Щоденний тренд методів атак:

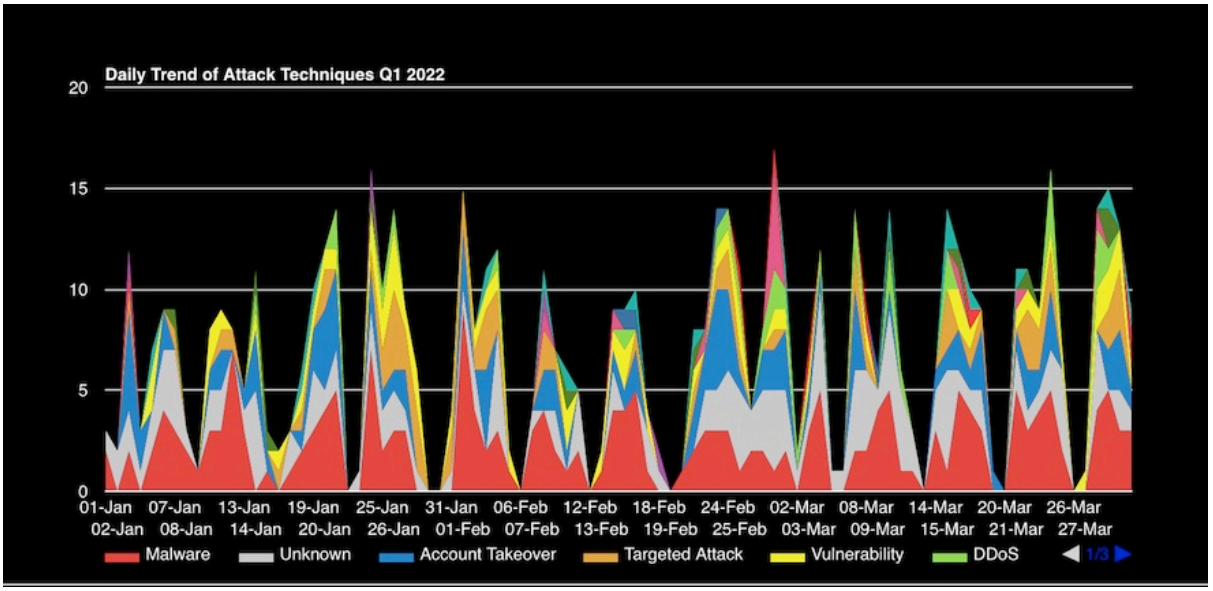


Рис 1.2.3. – Графік методів атак

Місячні мотиви розподілу розподіл атак:

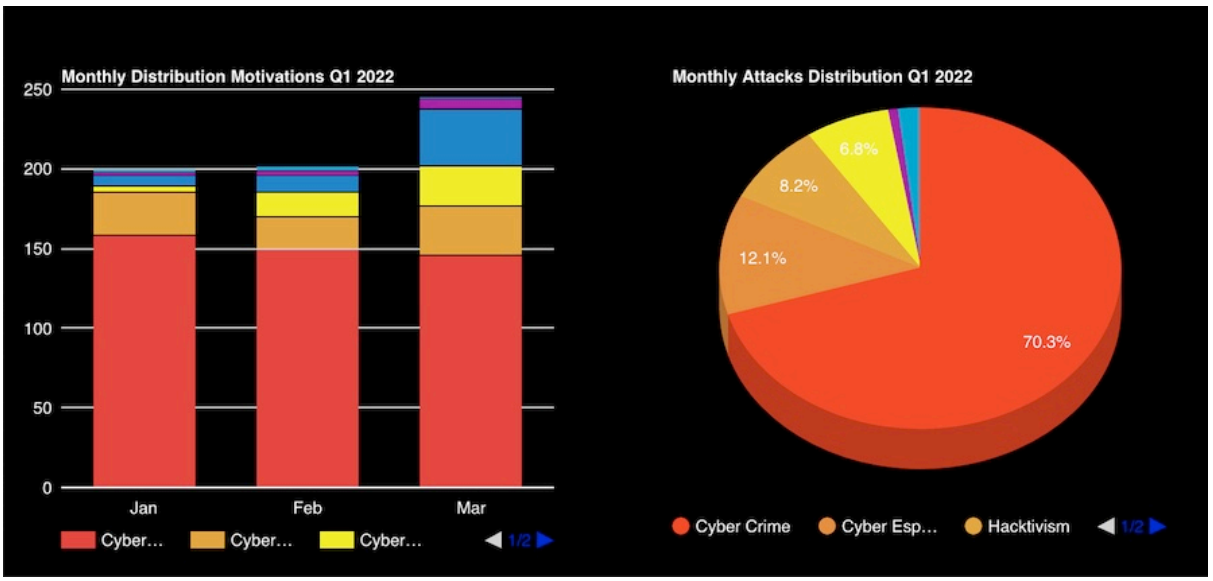


Рис 1.2.4. – Графік розподілів

Методи атак:

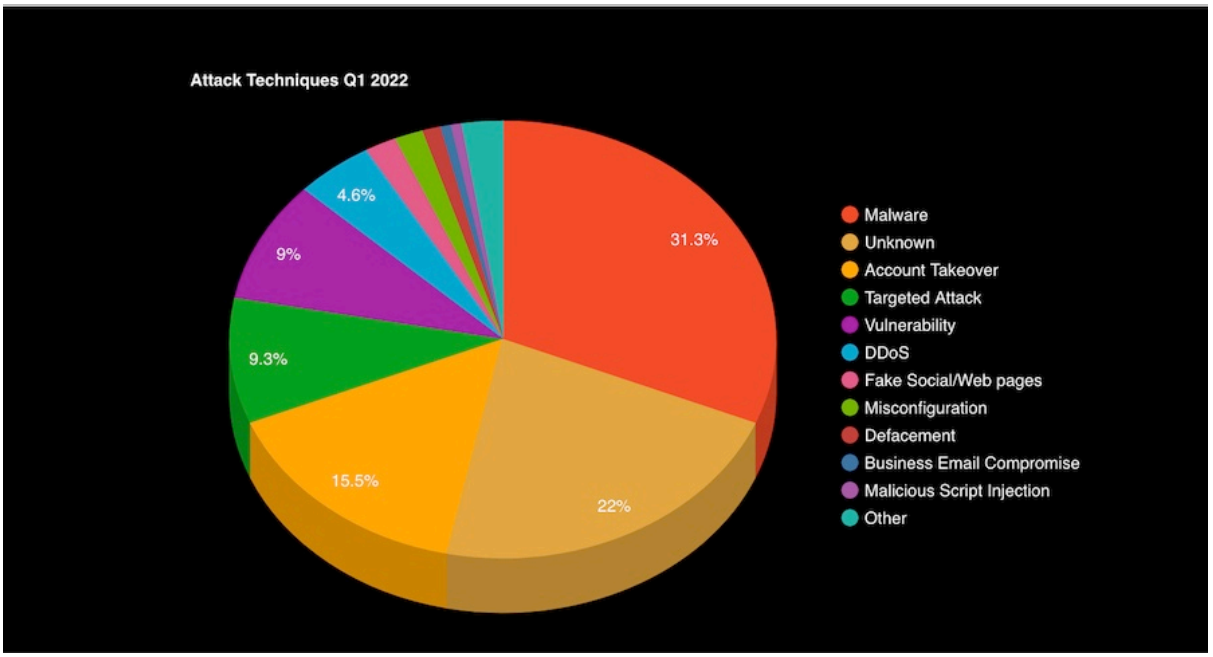


Рис 1.2.5. – Графік методів атак

Цільові мотиви:

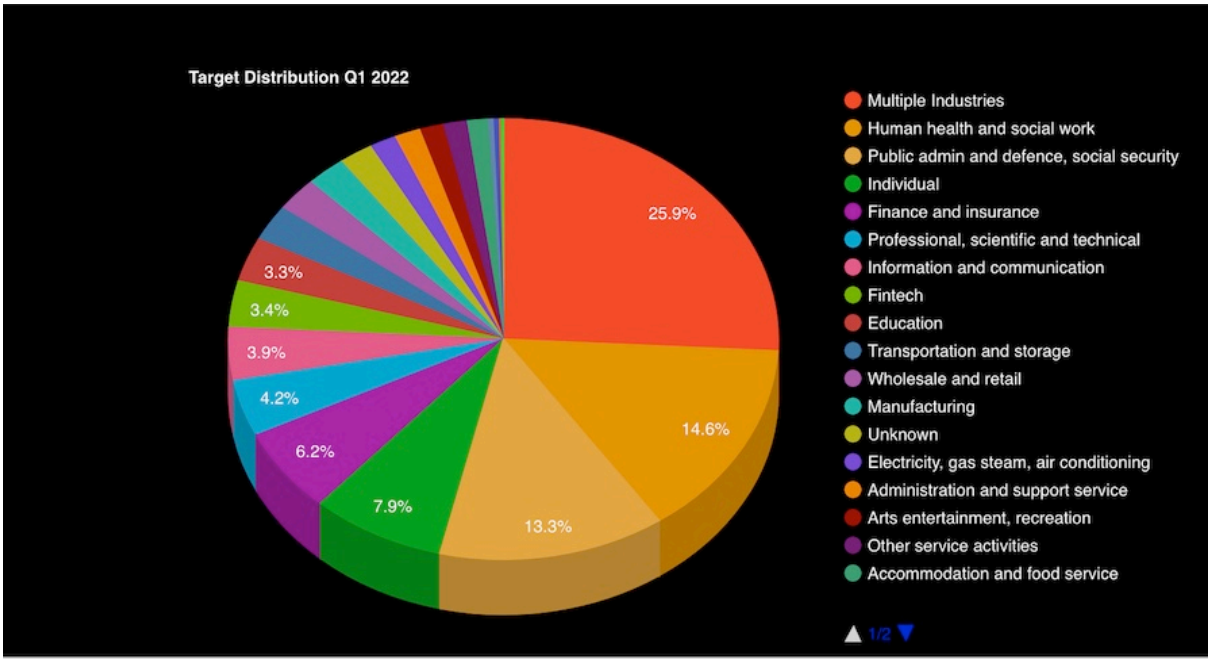


Рис 1.2.6. – Графік цільових мотивів

Сектори за розбивкою атак:

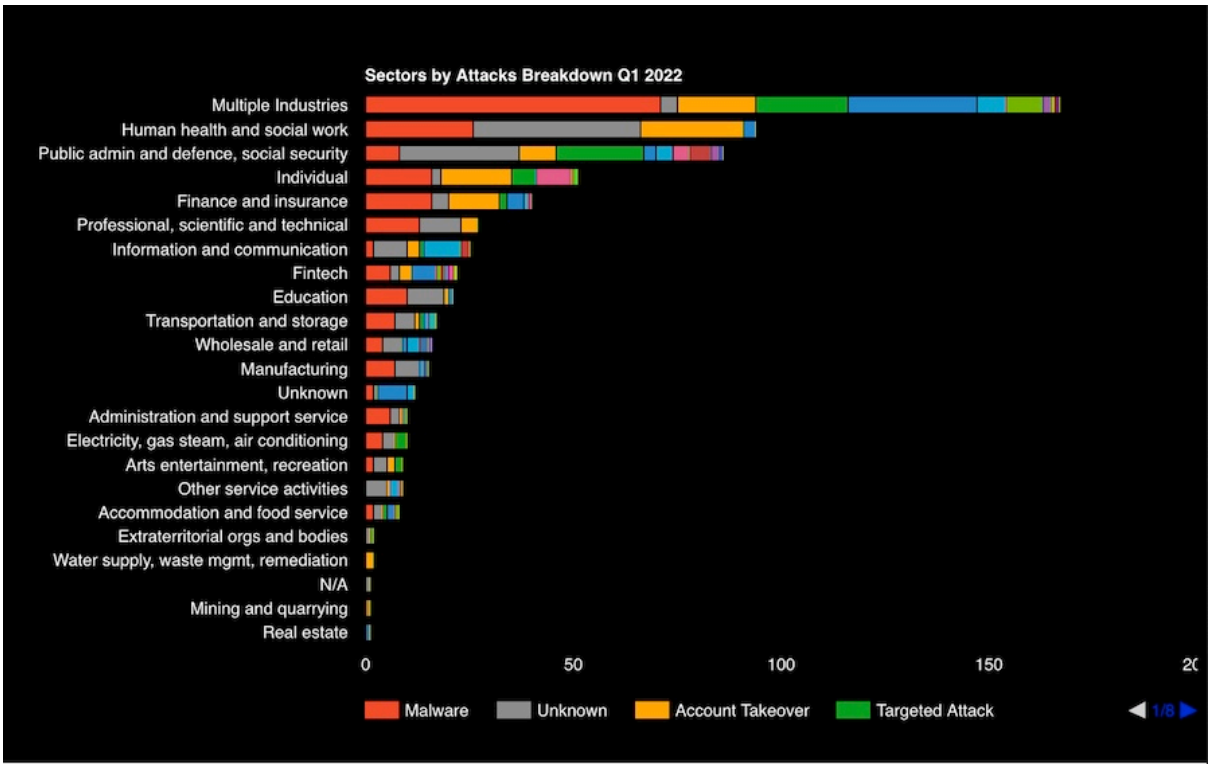


Рис 1.2.7. – Графік секторів атак

Сектори за розбивкою мотивацій:

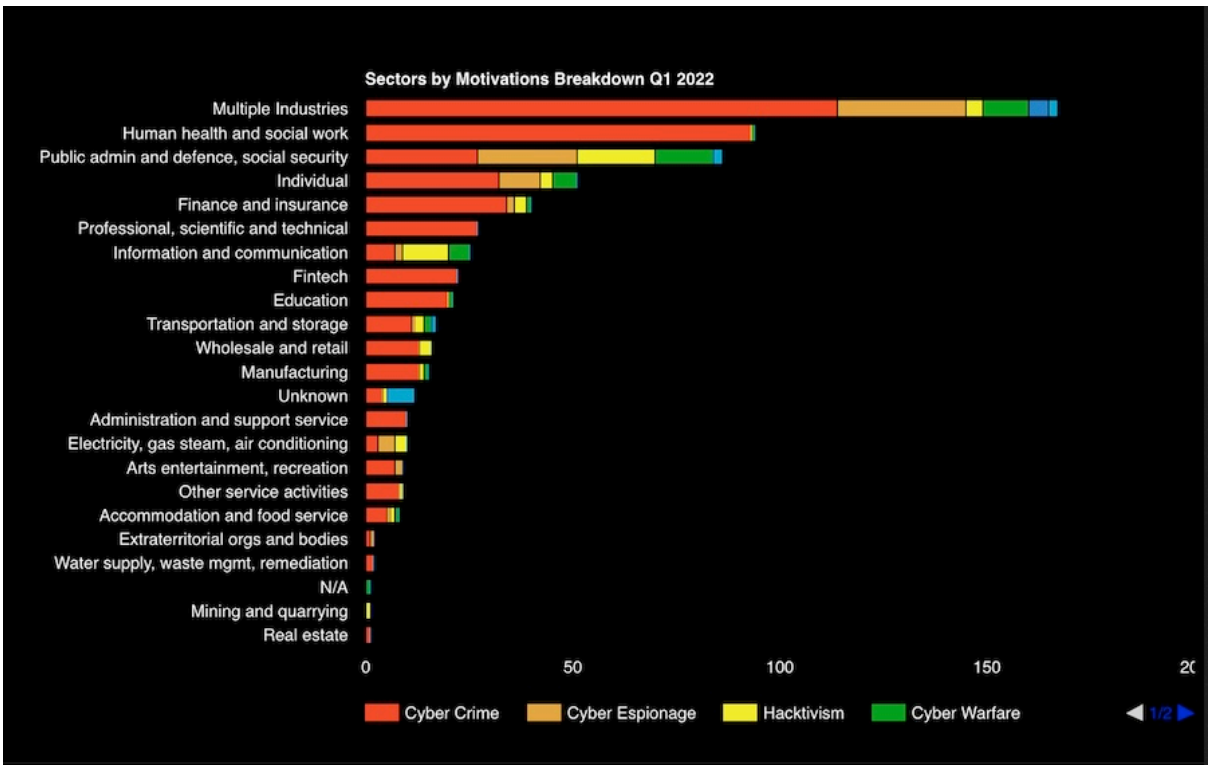


Рис 1.2.7. – Графік секторів мотивацій

Атаки по цілям:

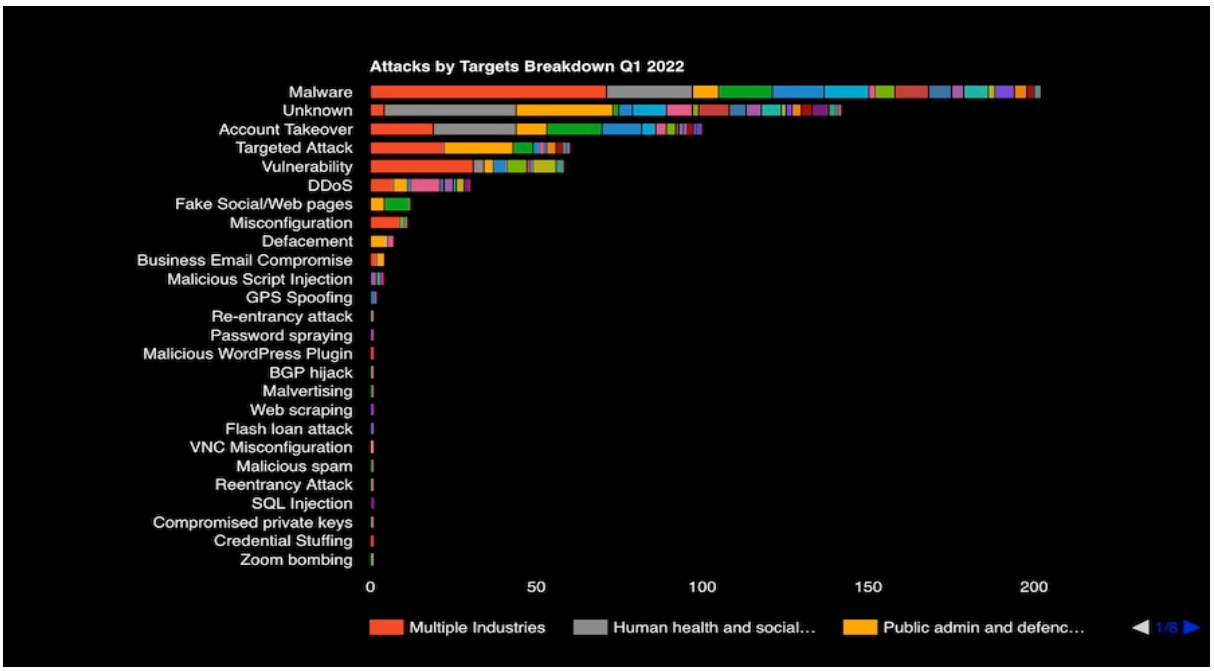


Рис 1.2.8. – Графік цілей

Мотиваційні атаки:

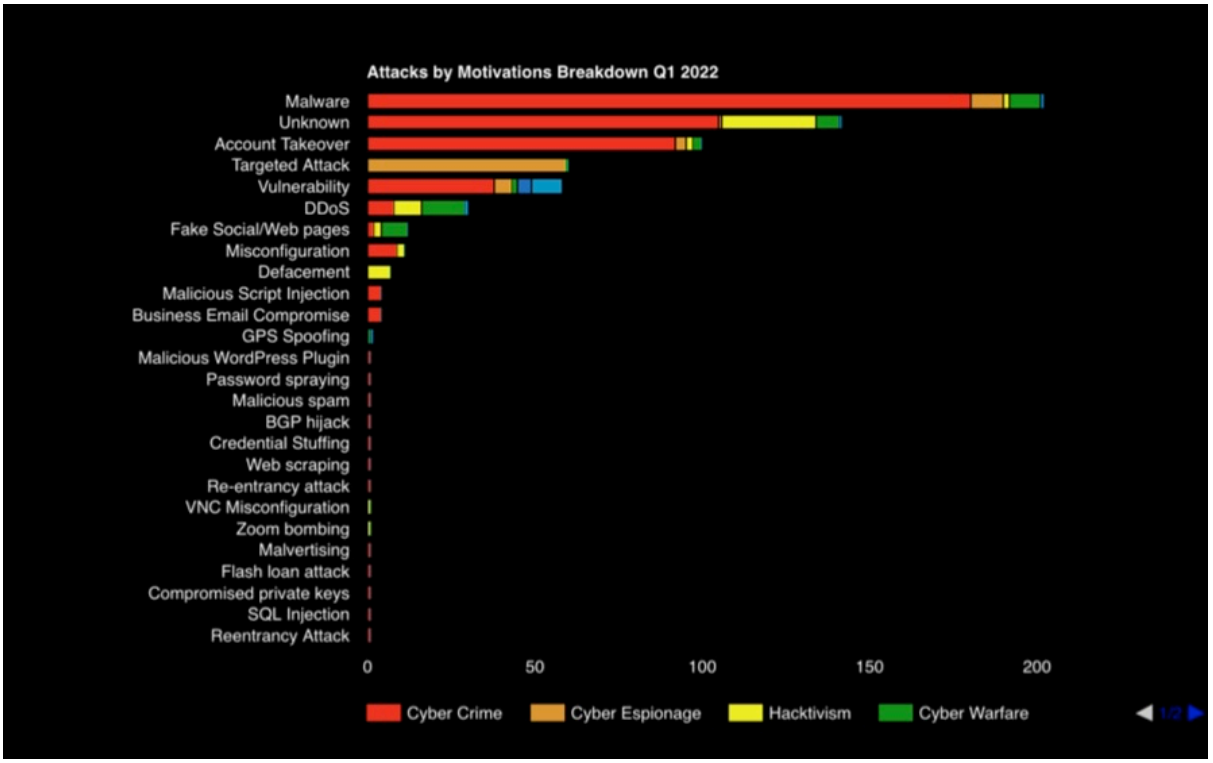


Рис 1.2.9. – Графік мотиваційних атак

Статистика атак за квітень місяць 2023 року:

На діаграмі мотивацій видно, що кіберпреступність продовжує лідирувати, хоча її відсоток знизився до менше 80% у порівнянні з попереднім місяцем (75,1% проти 82,6%). Операції, пов'язані з кібершпигунством, зросли до 12,3% з 9,3%, тоді як хактивізм збільшився до 7,6% з 5,1%, а кібервійна становить 8 подій, що підвищило її відсоток з 1,4% до 2,3%.

Вредонебезпечне програмне забезпечення продовжує лідирувати в методах атак з відсотком 35,5% у порівнянні з 32,3%, випереджаючи вразливості, на які все ще впливає серія подій, пов'язаних з масовим використанням Fortra CVE-2023-0669. Таким чином, відсоток вразливостей зменшився до 12% порівняно з 16,5% в попередньому місяці, а зловживання обліковими записами продовжує зменшуватися до 8,2% з 10,5%.

У діаграмі розподілу цілей знову видно, що проводяться кампанії проти кількох організацій, які продовжують тенденцію до зниження до 19,6% з 21%, випереджаючи окремих осіб (10,9%) та публічних адміністраторів до 8,8% з 12%.

Для більш детального огляду ландшафту загроз рекомендується ознайомитися з інтерактивними діаграмами та статистикою, які також доступні у вигляді інфографіки.

Варто зазначити, що ці дані базуються виключно на атаках, які включені до хронології, доступної з відкритих джерел, таких як блоги та новинні сайти. Очевидно, що ця вибірка не може бути повною, і вона призначена лише для загального огляду кіберзагроз.

Події на день квітень 2023:

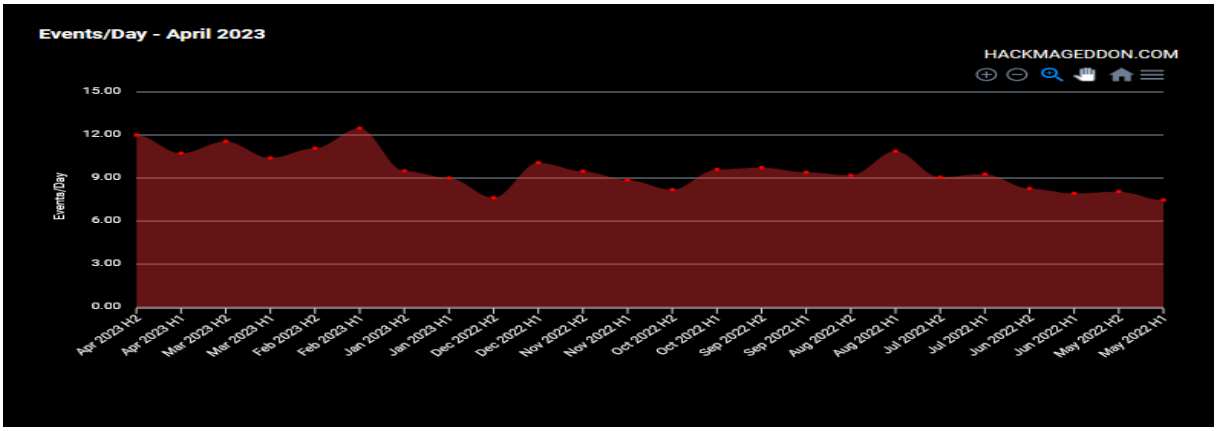


Рис 1.2.10 – Графік подій

Щоденні атаки:

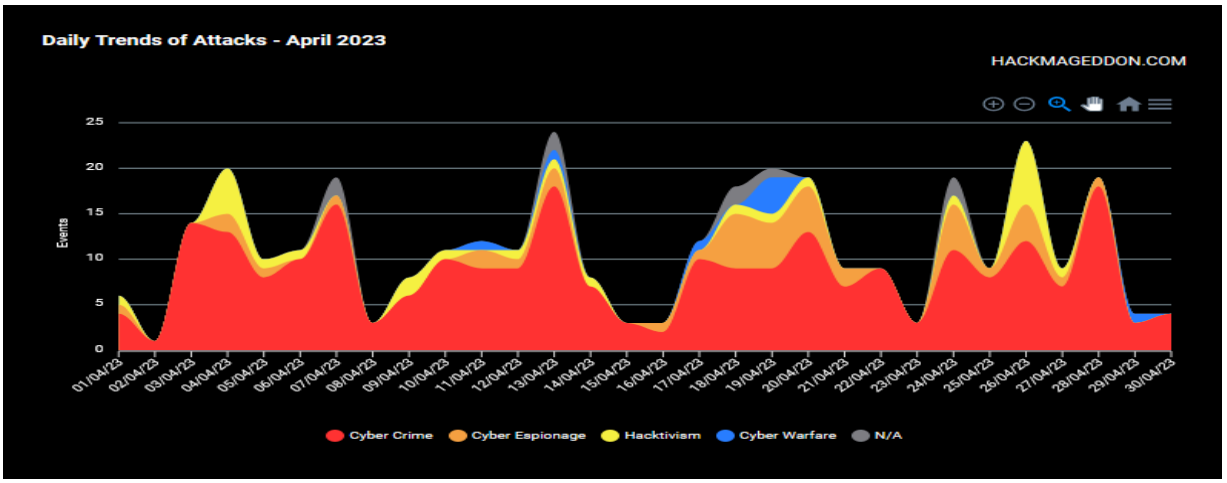


Рис 1.2.11. – Графік атак

Мотивації:

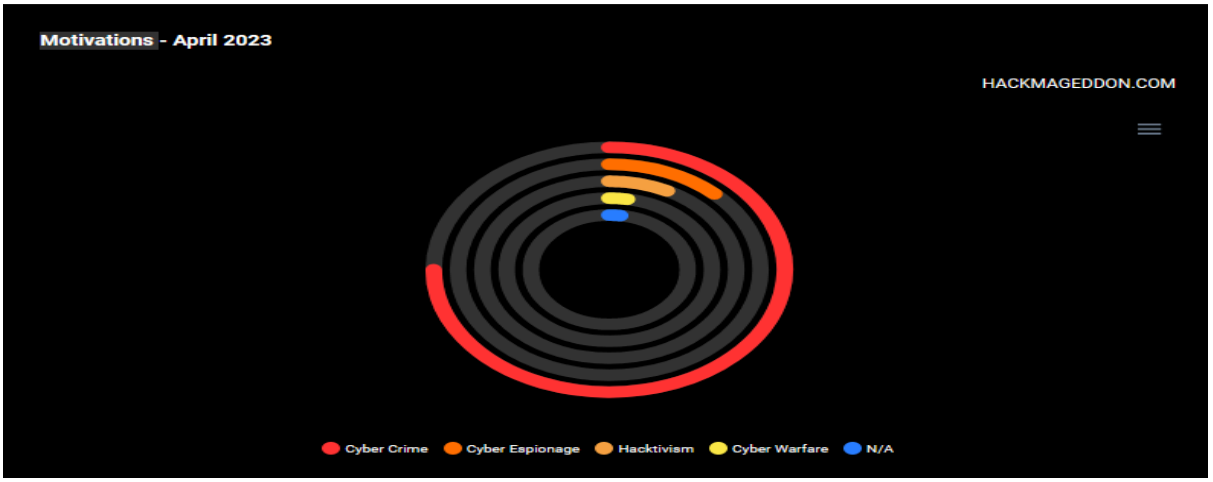


Рис 1.2.12 – Графік мотивацій

Розподіл мотивацій:

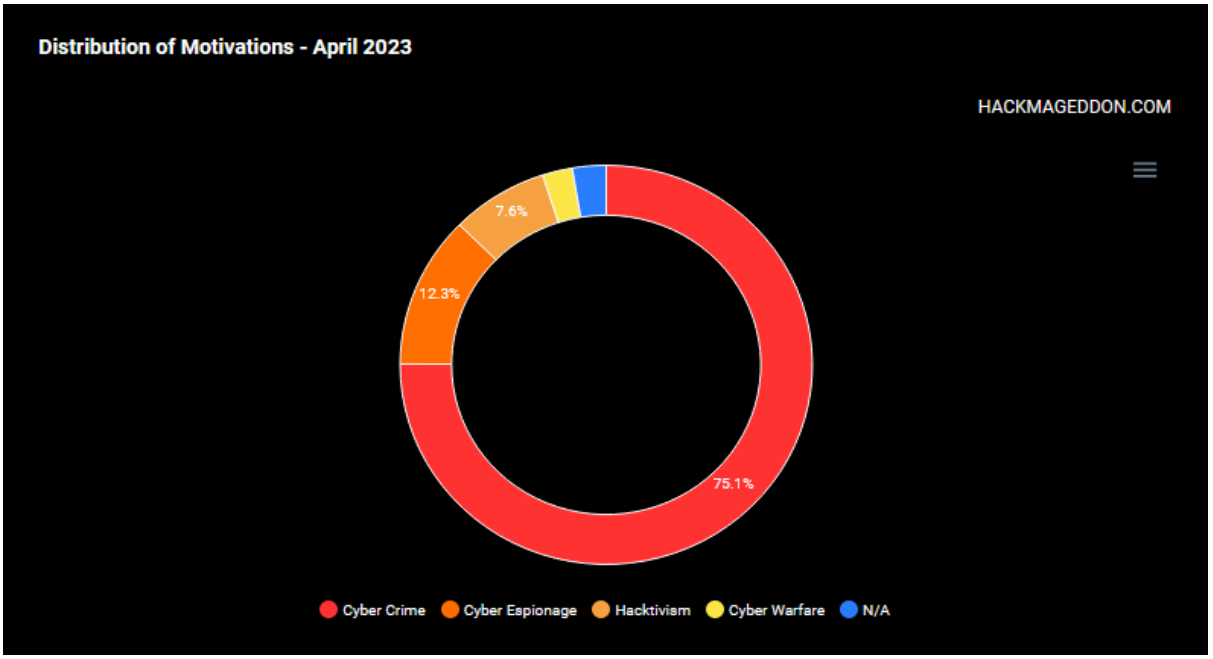


Рис 1.2.13. – Графік мотивацій

Атаки:

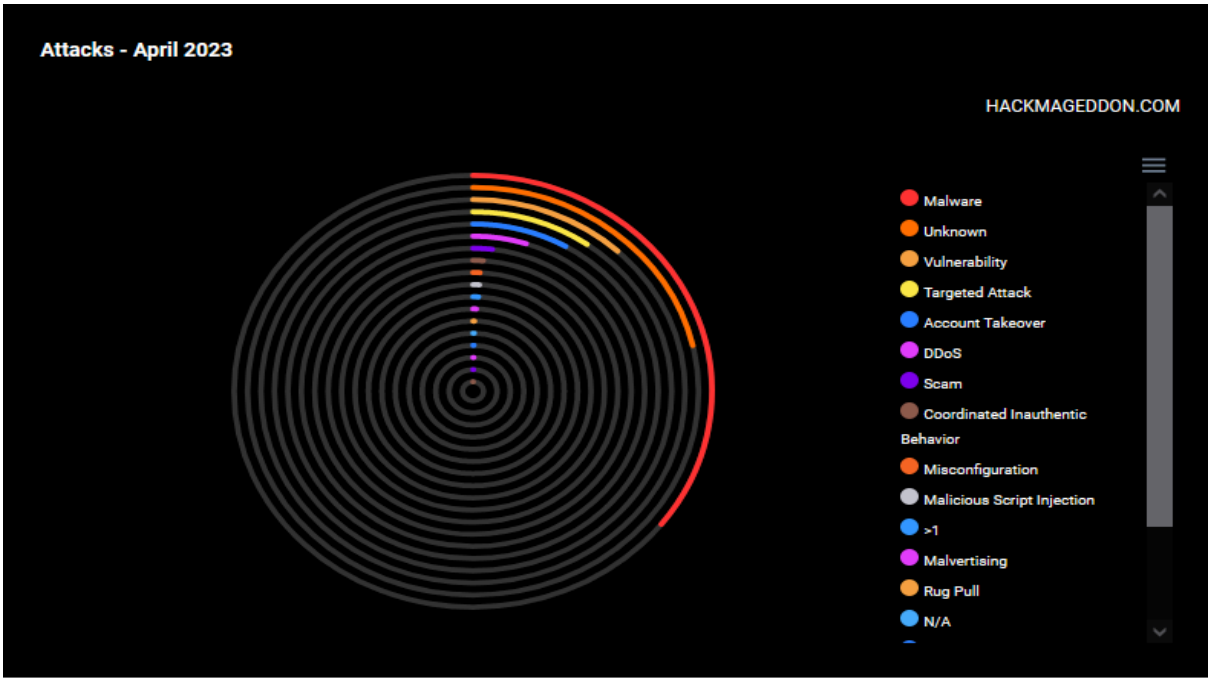


Рис 1.2.14. – Графік атак

Розподіл атак:

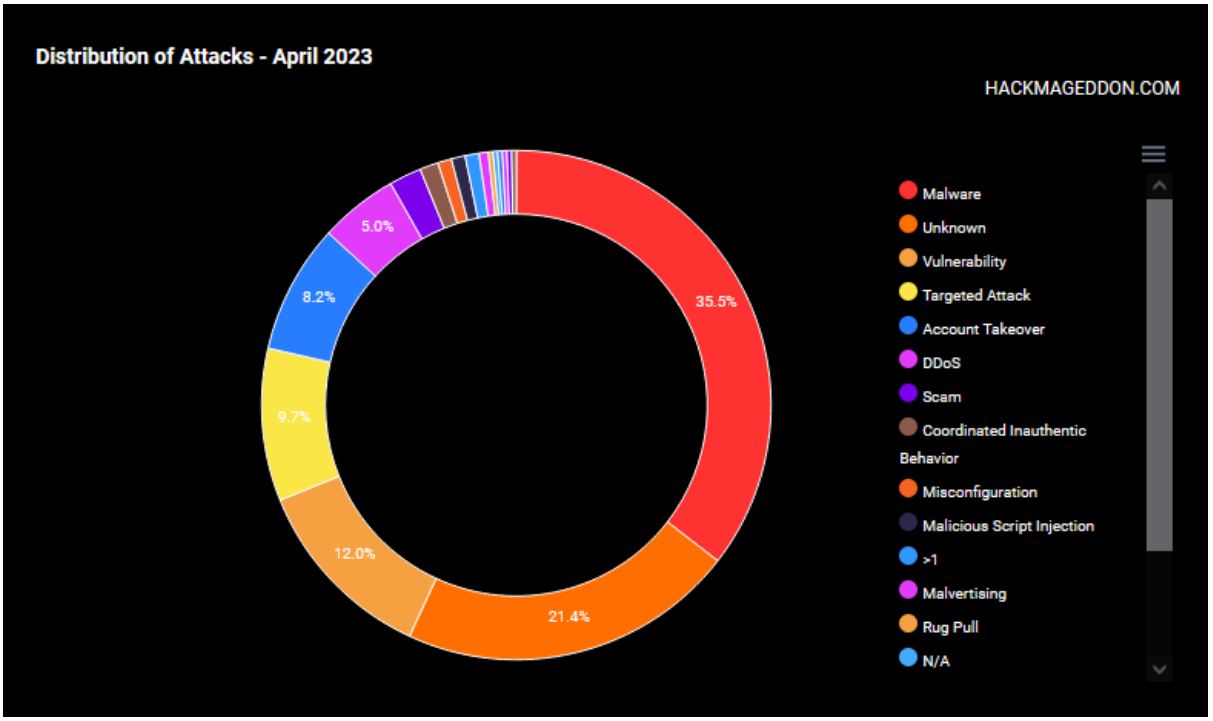


Рис 1.2.15 – Графік розподілу атак

Цілі:

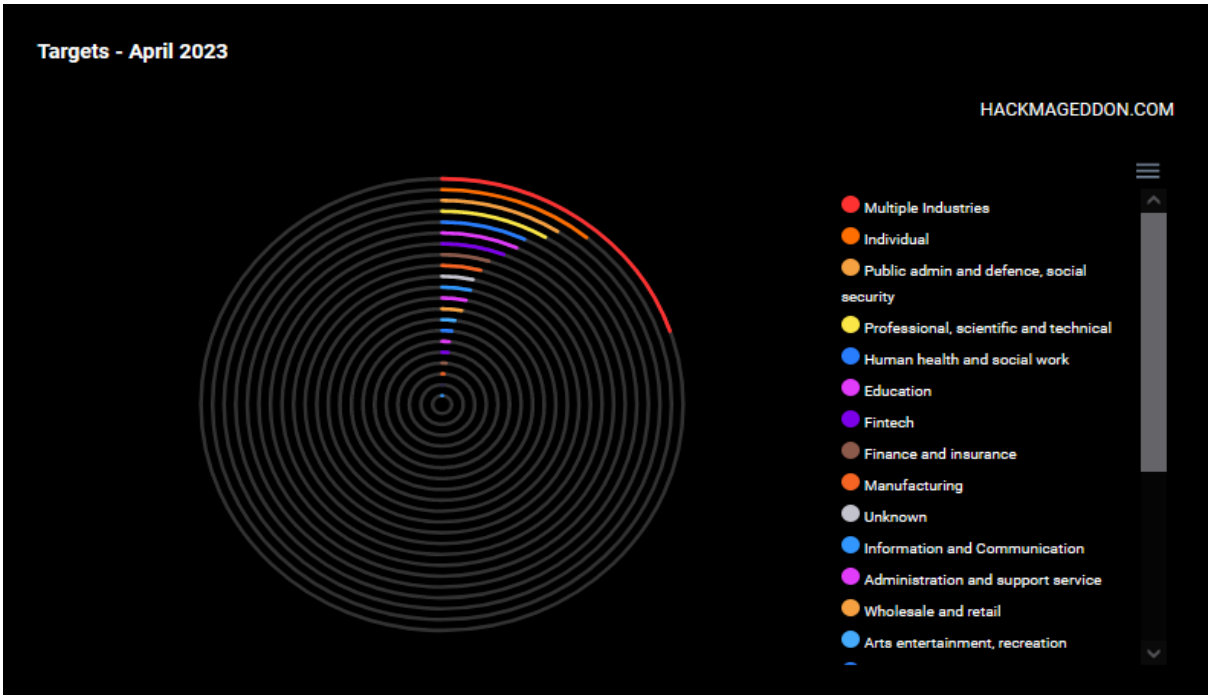


Рис 1.2.16 – Графік цілей

Розподіл цілей:

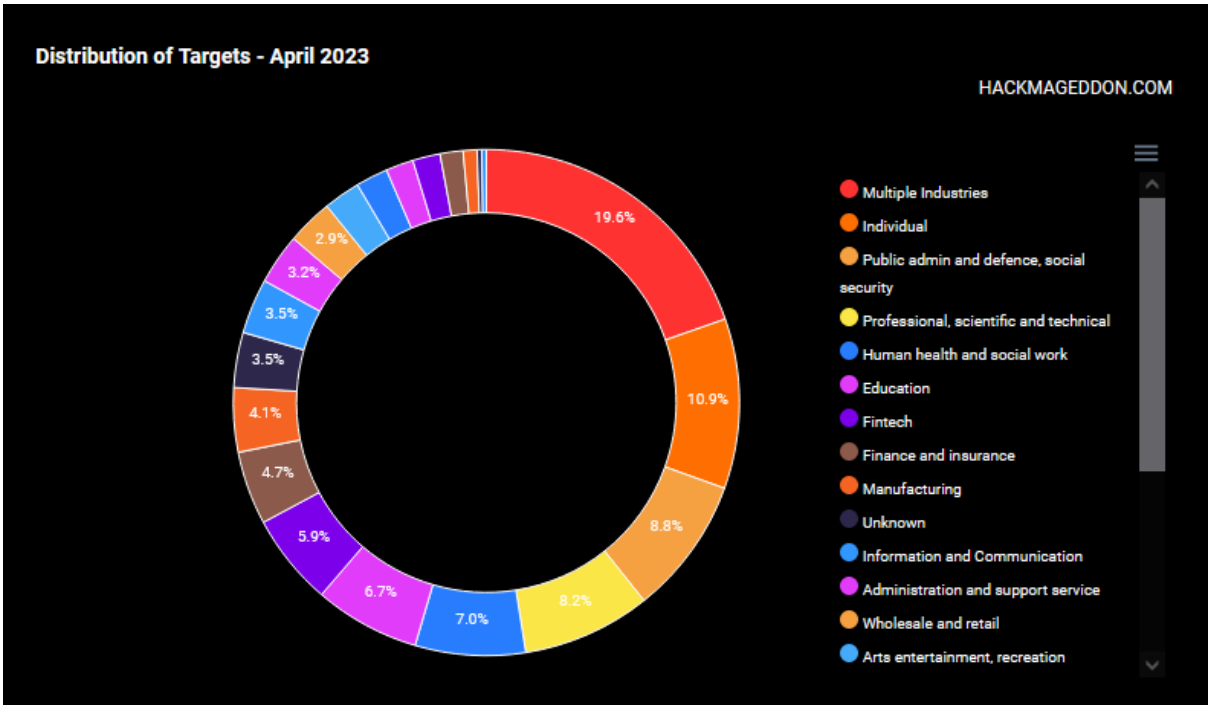


Рис 1.2.17. – Графік розподілу цілей

Розподіл мотивацій по секторам:

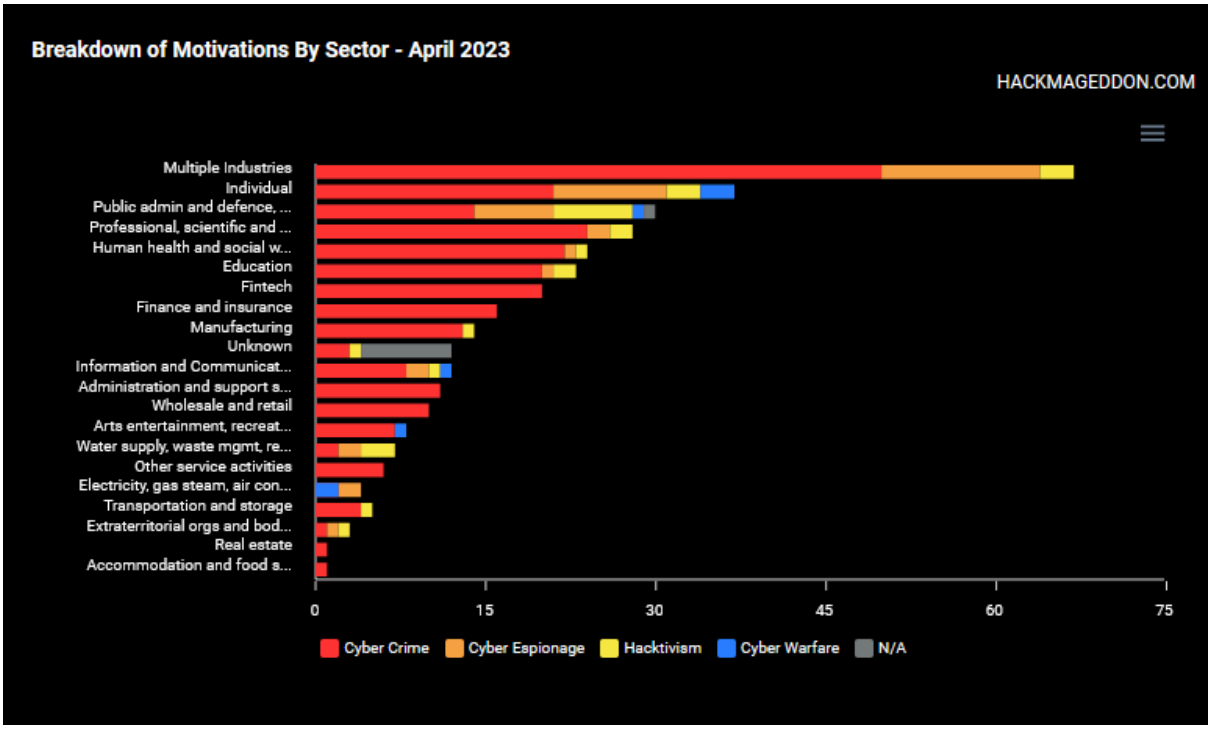


Рис 1.2.18. – Графік розподілу мотивацій

Графік розподілу по атакам:

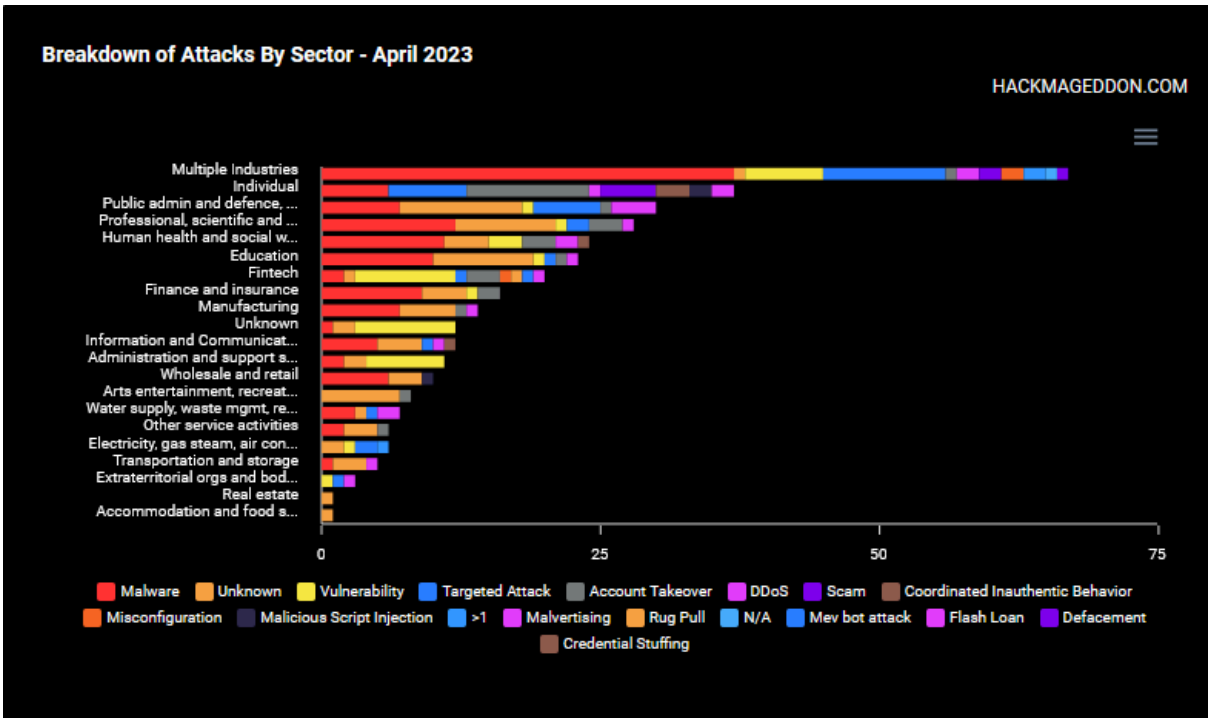


Рис 1.2.19. – Графік розподілу атак

Події на вересень 2023:

Як завжди, кіберзлочинність лідирує в діаграмі мотивації з 77,2% , що є меншим за 80% другий місяць поспіль і майже наближається до 78,6% попереднього місяця. Операції, спричинені кібершпигунством, зросли до 11,5% з 8,9%, тоді як активізм різко впав до 4,7% з 8,3% з 2,3% , тоді як із лише 2 подіями Cyber Warfare заробила лише 0,5% з 1,8%.

У діаграмі методів атак лідирує зловмисне програмне забезпечення з 38,1% проти 35,7%, тоді як атаки, здійснені через уразливості , посідають друге місце з 16,3% , що трохи нижче з 17,6%. Третє місце серед відомих методів посідають цілеспрямовані атаки з 8,7% , випереджаючи захоплення облікових записів (8,2%), яке займало друге місце в серпні .

Розподіл цілей знову очолює кілька організацій, що знизилося до 16,8% з 22,9%, перед охороною здоров'я з 13,4% і фінансами з 10% . Державні адміністратори, оборона та соціальне забезпечення опустилися на четверте місце з 9,5% , випереджаючи технічні та професійні цілі з 8,2% .

Події на день:

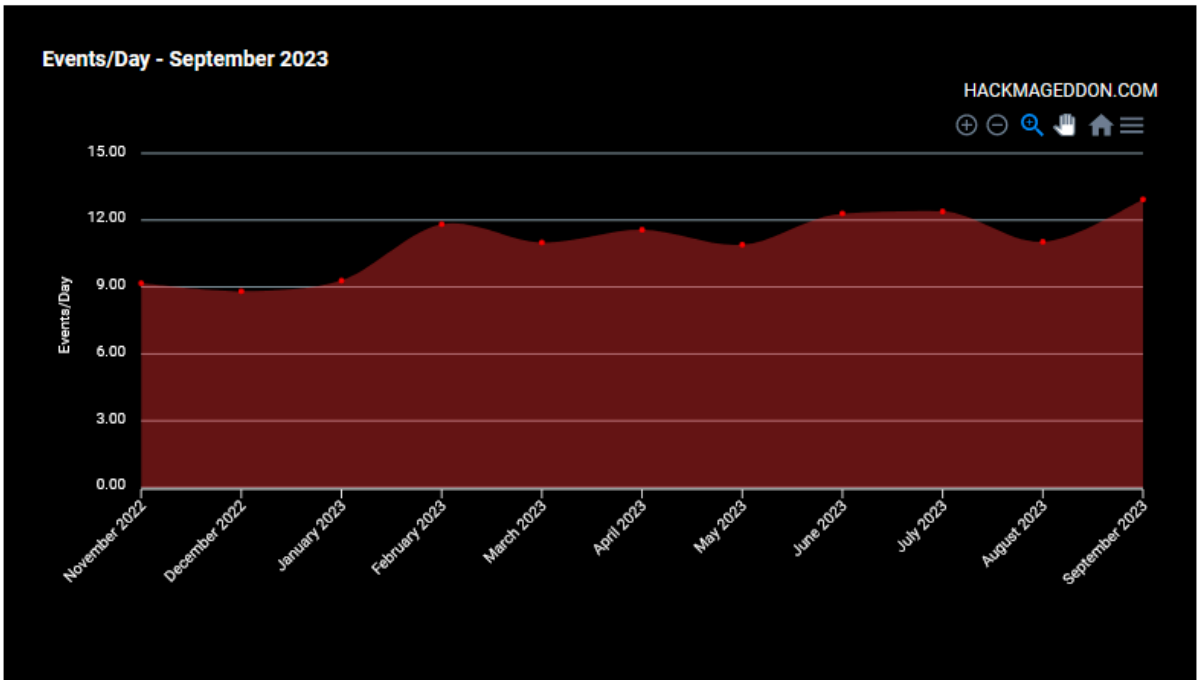


Рис 1.2.20 – Графік подій на день

Графік щоденних тендецій атак:

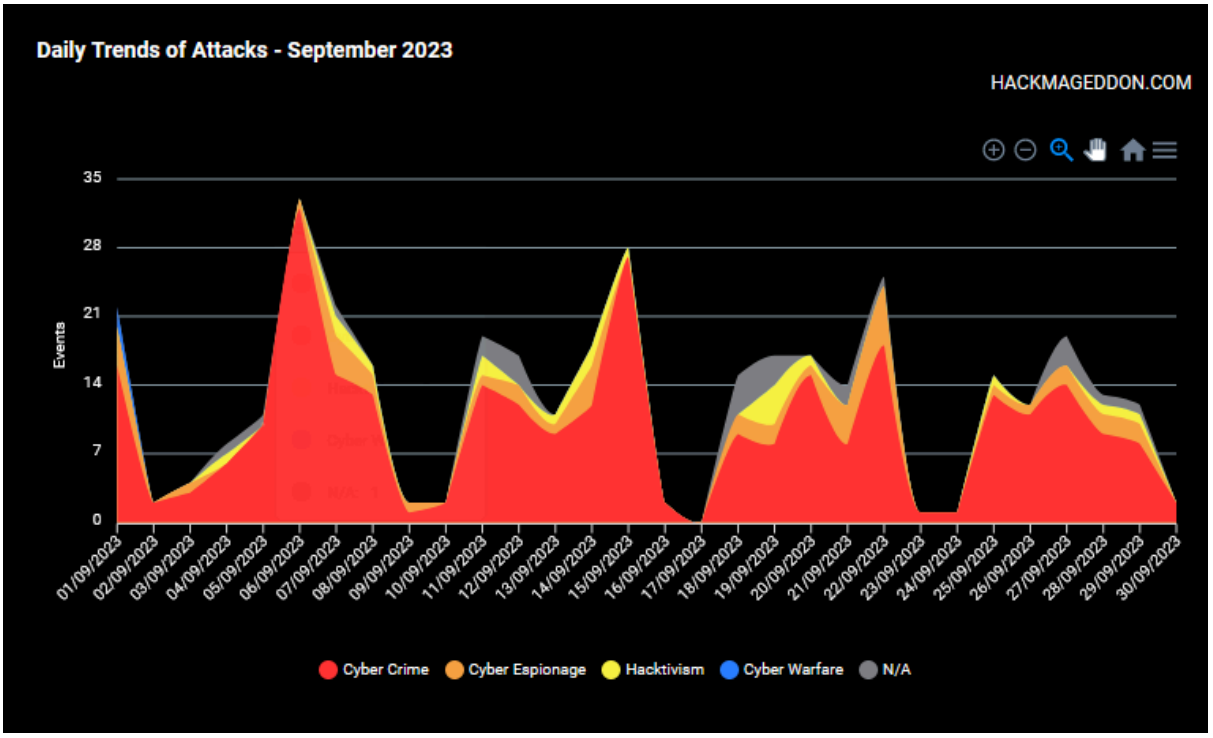


Рис 1.2.21 – Графік подій

Мотивації:

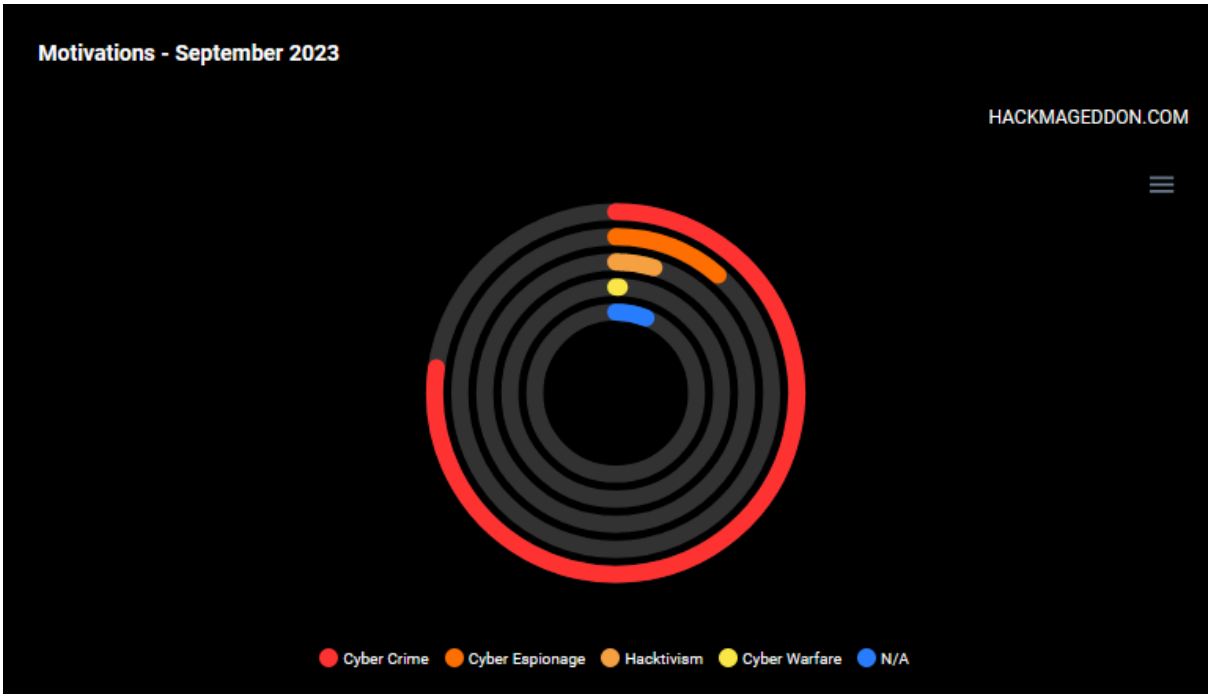


Рис 1.2.22 – Графік мотивацій

Атаки:

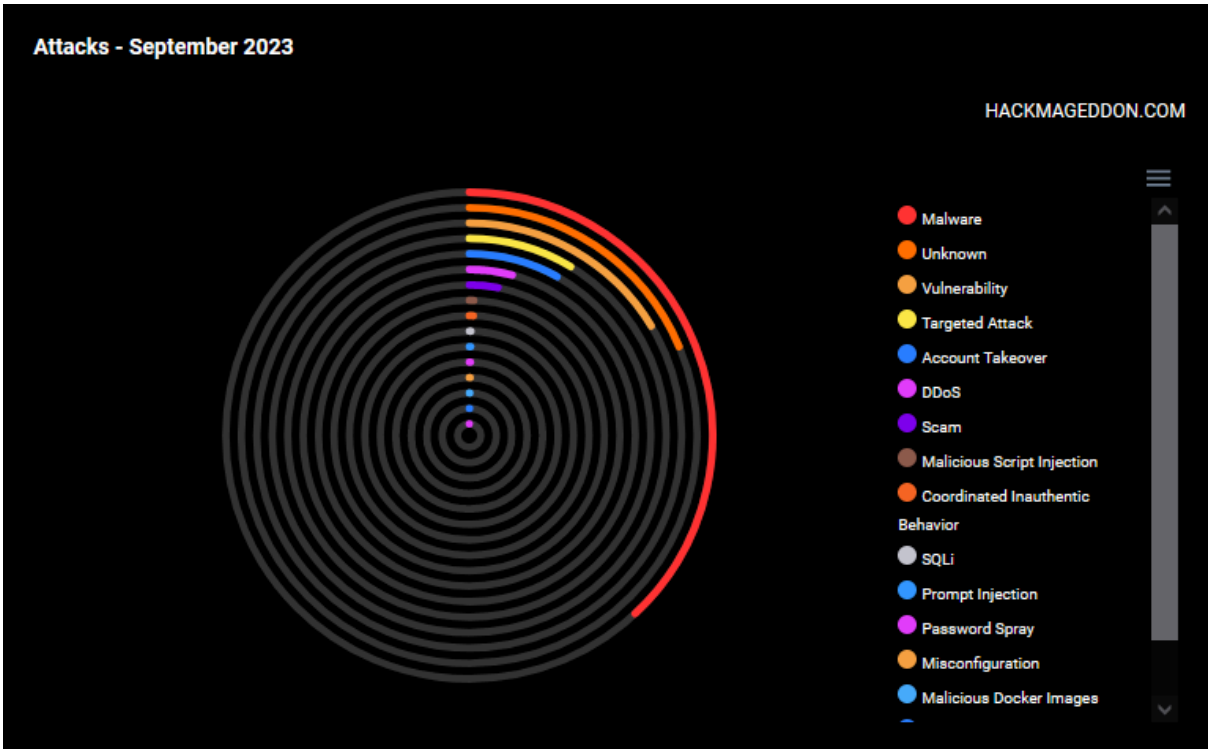


Рис 1.2.23 – Графік списку атак

Цілі:

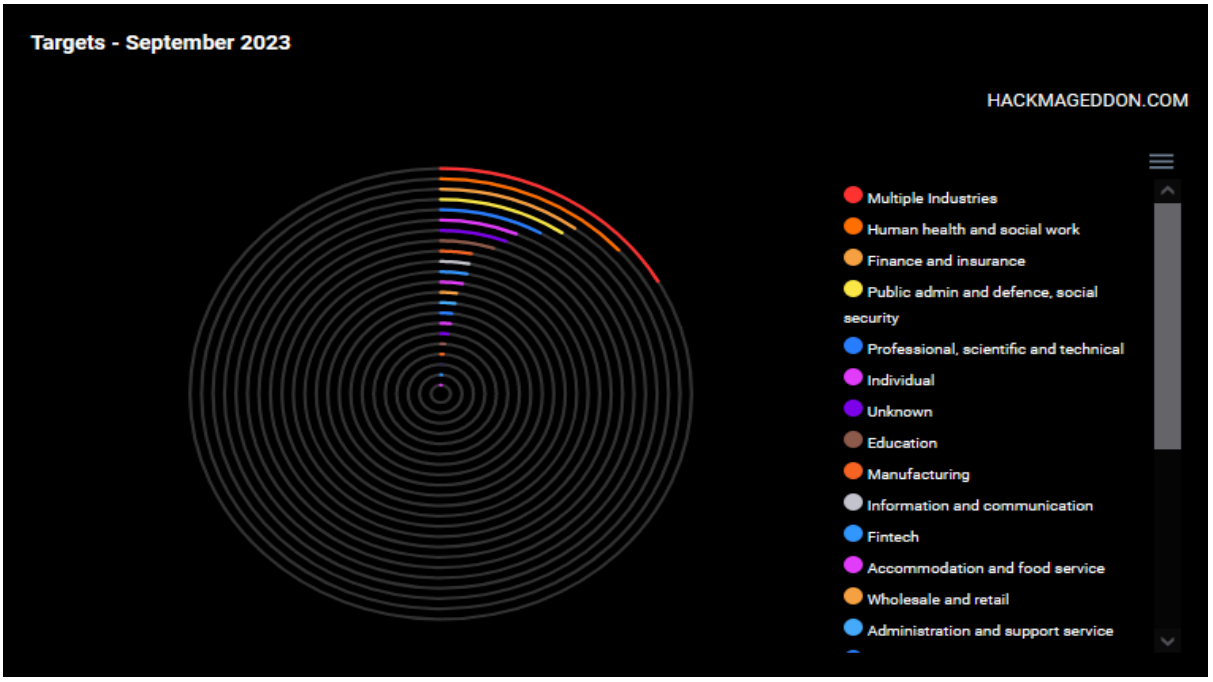


Рис 1.2.24 – Графік списку цілей

Розподіл атак:

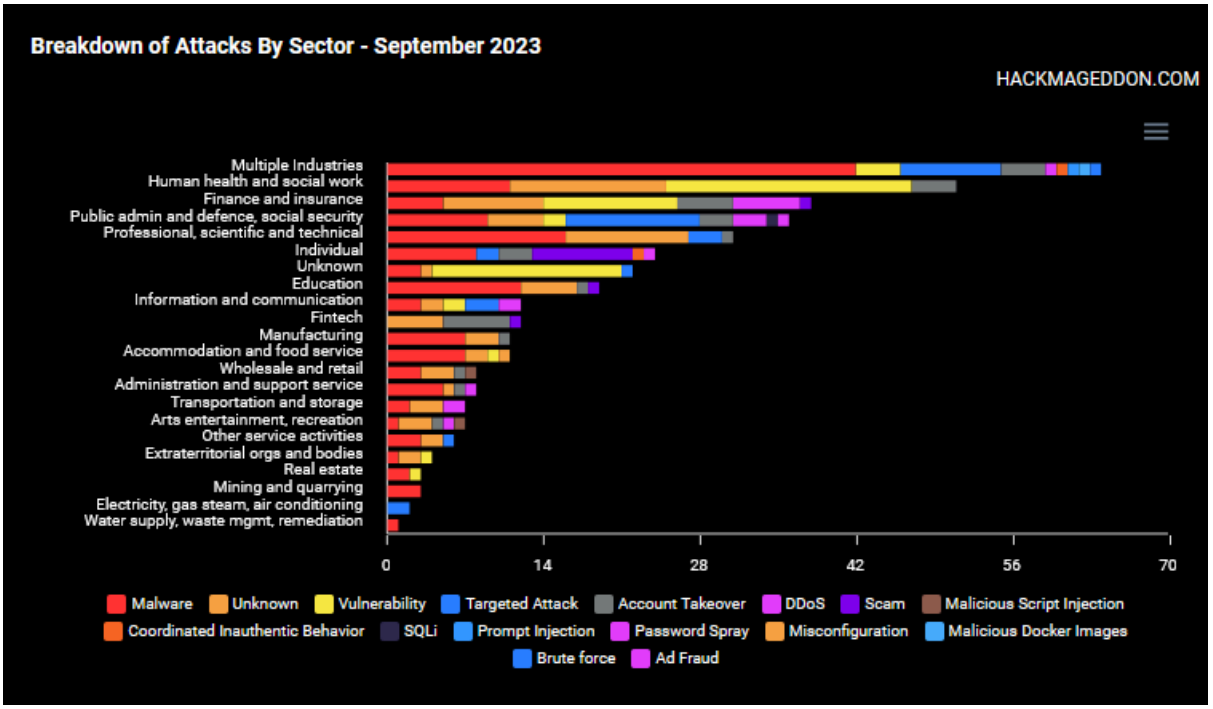


Рис 1.2.25 – Графік розподілу атак по секторам

Жовтень 2023:

Як завжди, кіберзлочинність лідирує в діаграмі мотивації з 76,7% , що є меншим за 80% третій місяць поспіль і майже наближається до 77,2% попереднього місяця. Операції, спричинені кібершпигунством, знизилися до 8,3% з 11,5%, а активізм , викликаний війною на Близькому Сході, подвоїв свій відсоток і посів друге місце з 9,4% з 4,7% у вересні. Лише за 4 події Cyber Warfare подвоїла свій скромний відсоток до 1,1% з 0,5%.

Діаграму методів атак лідирує зловмисне програмне забезпечення з 34,2% , порівняно з 38,1%, а атаки, здійснені через використання вразливостей , посідають друге місце з 15,2% , дещо нижче з 16,3%. Третє місце серед відомих технік займає Account Takoeovers з 11% проти 8,2%. І останнє, але не менш важливе: цілеспрямовані атаки зменшилися до 6,1% з 8,7%.

Розподіл цілей знову лідирує з кількома організаціями до 19,3% з 16,8%, випереджаючи операції проти окремих осіб (10,7%,) з тим же значенням, що й охорона здоров’я, знизившись з 13,4% попереднього місяця.

Події на день:

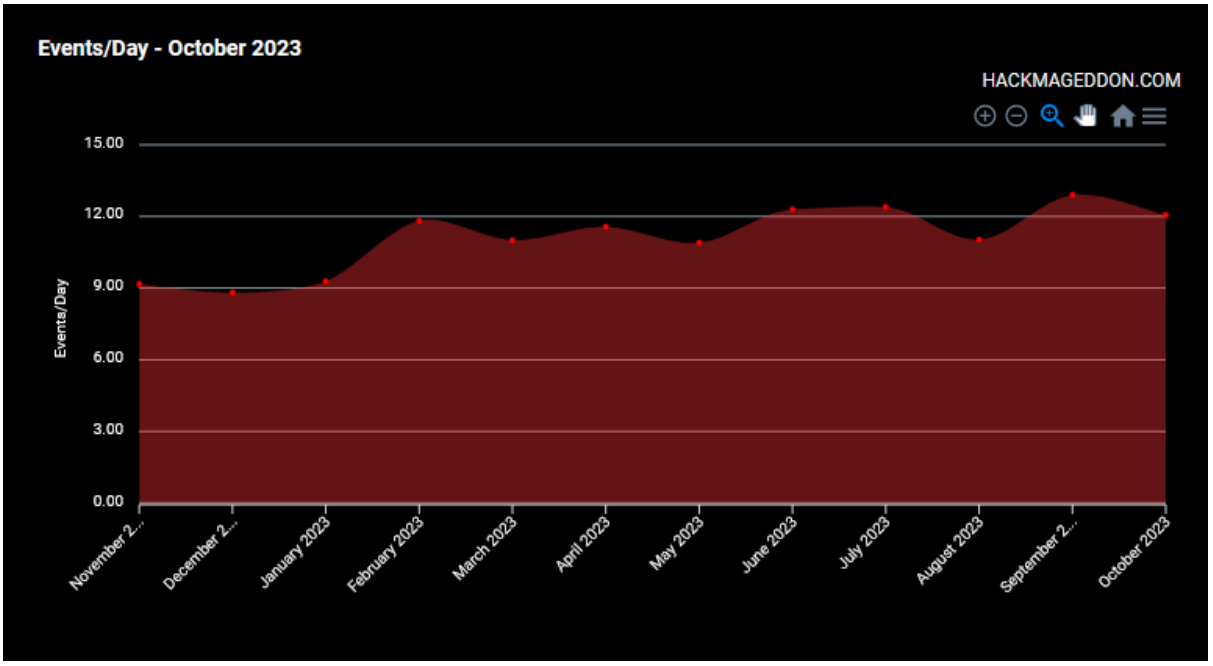


Рис 1.2.26 – Графік подій на день

Графік щоденних тендецій атак:

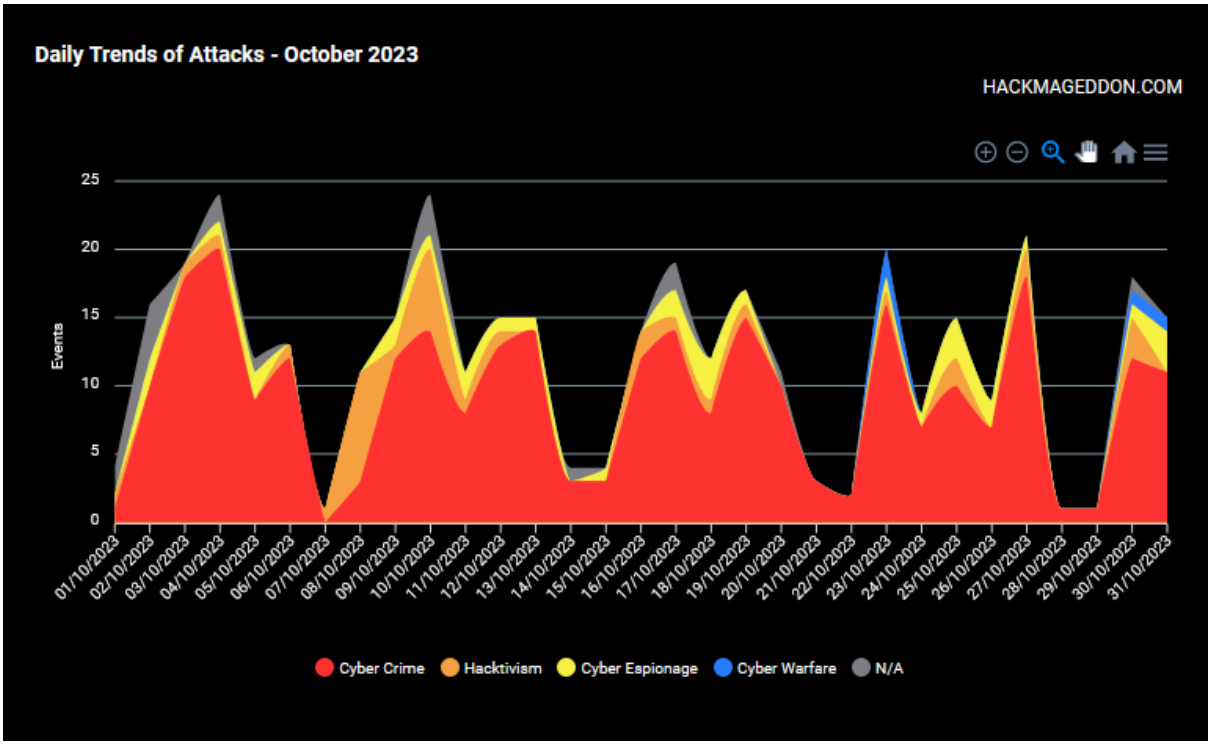


Рис 1.2.27 – Графік подій

Мотивації:

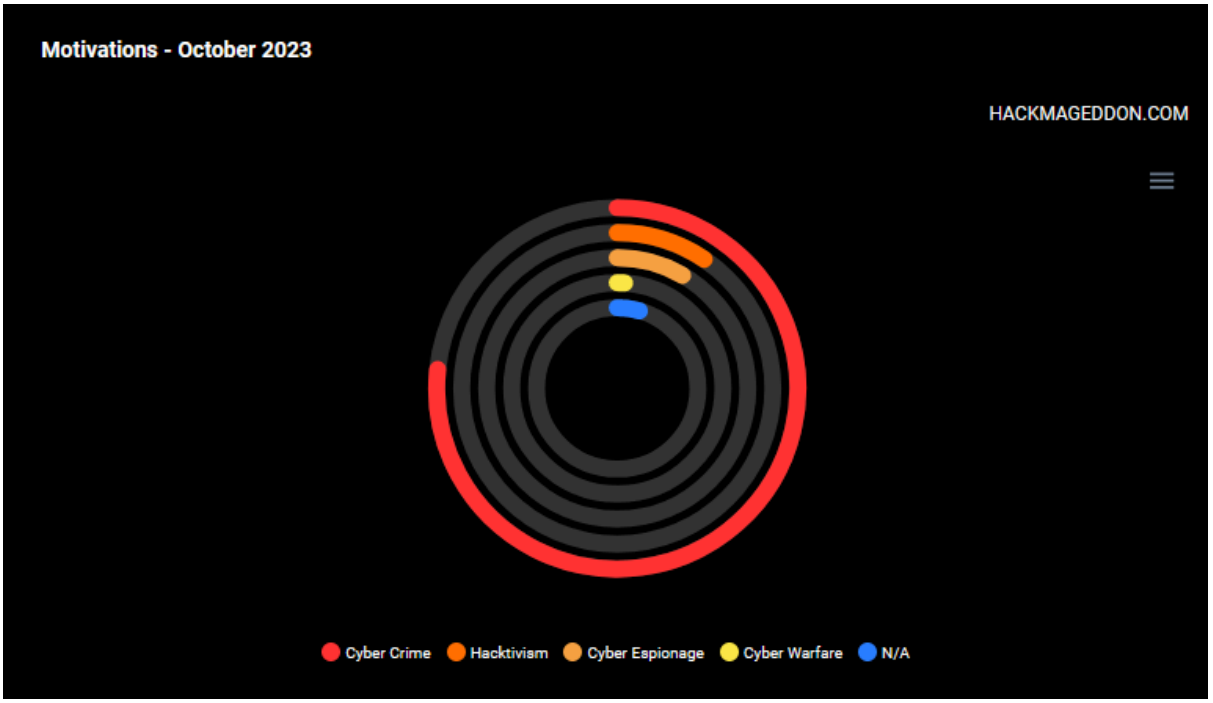


Рис 1.2.28 – Графік мотивацій

Атаки:

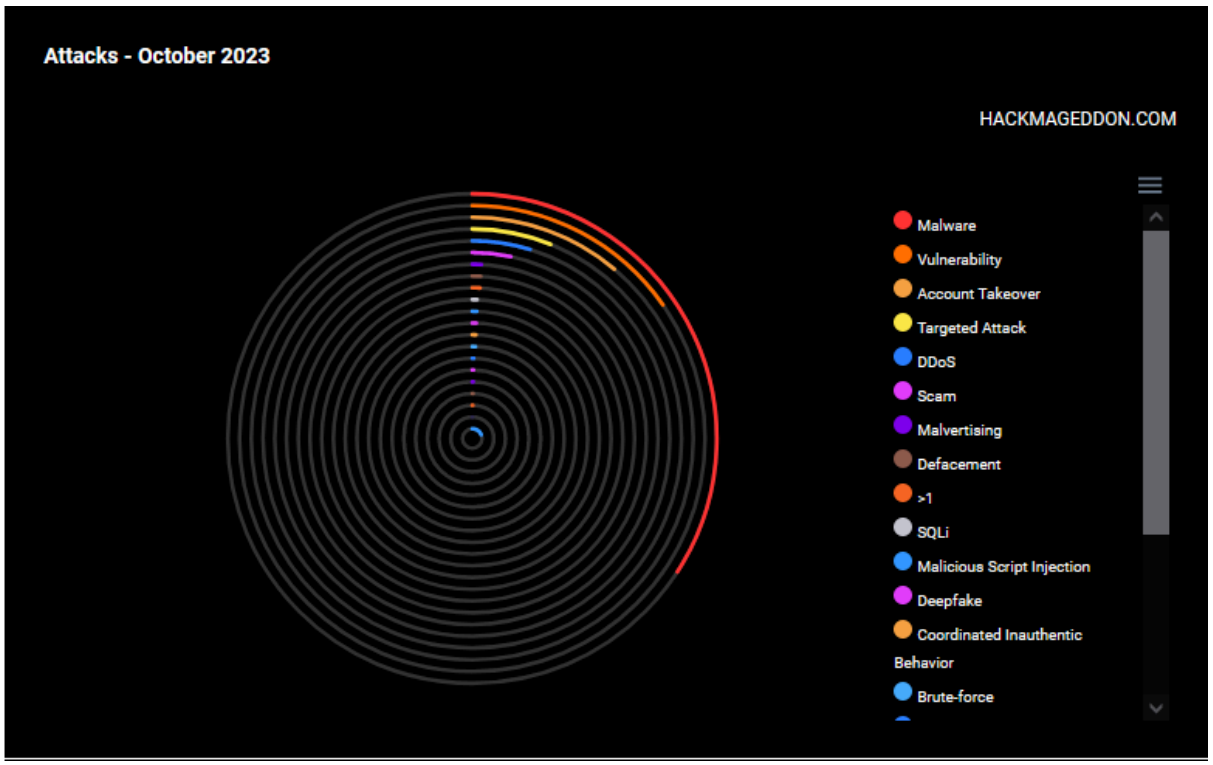


Рис 1.2.29 – Графік атак

Цілі:

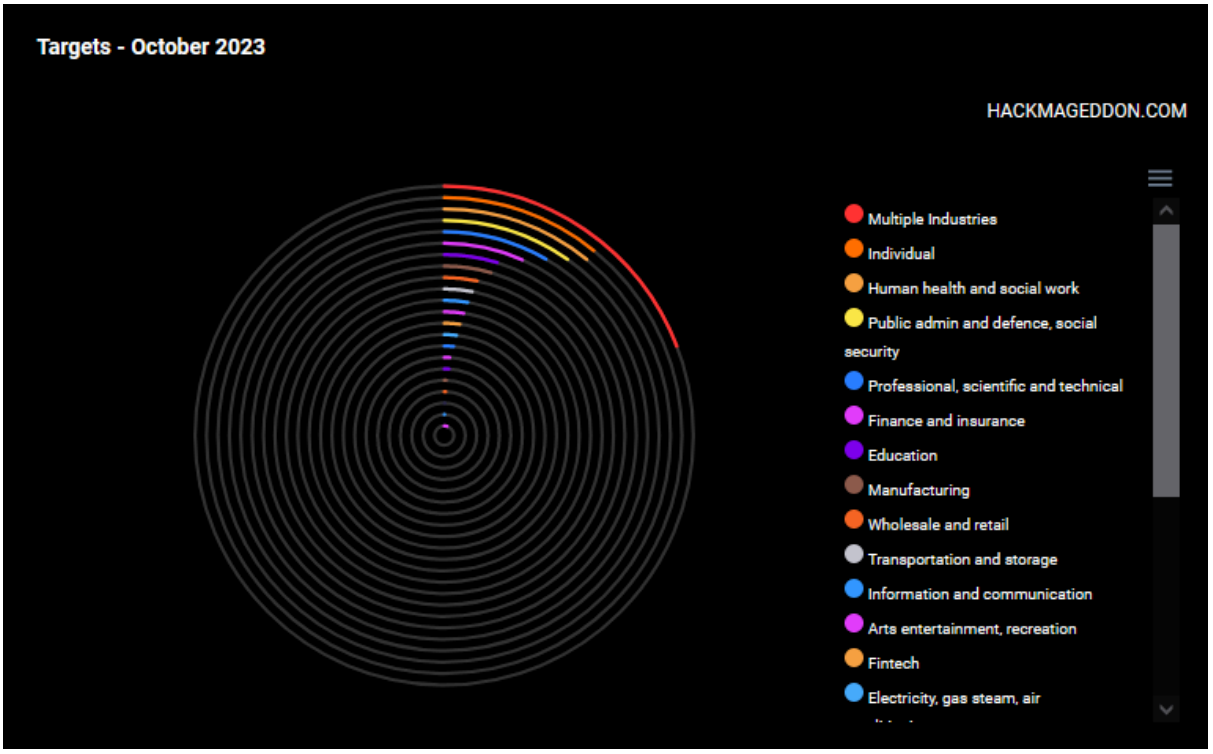


Рис 1.2.30 – Графік цілей

Розподіл атак:

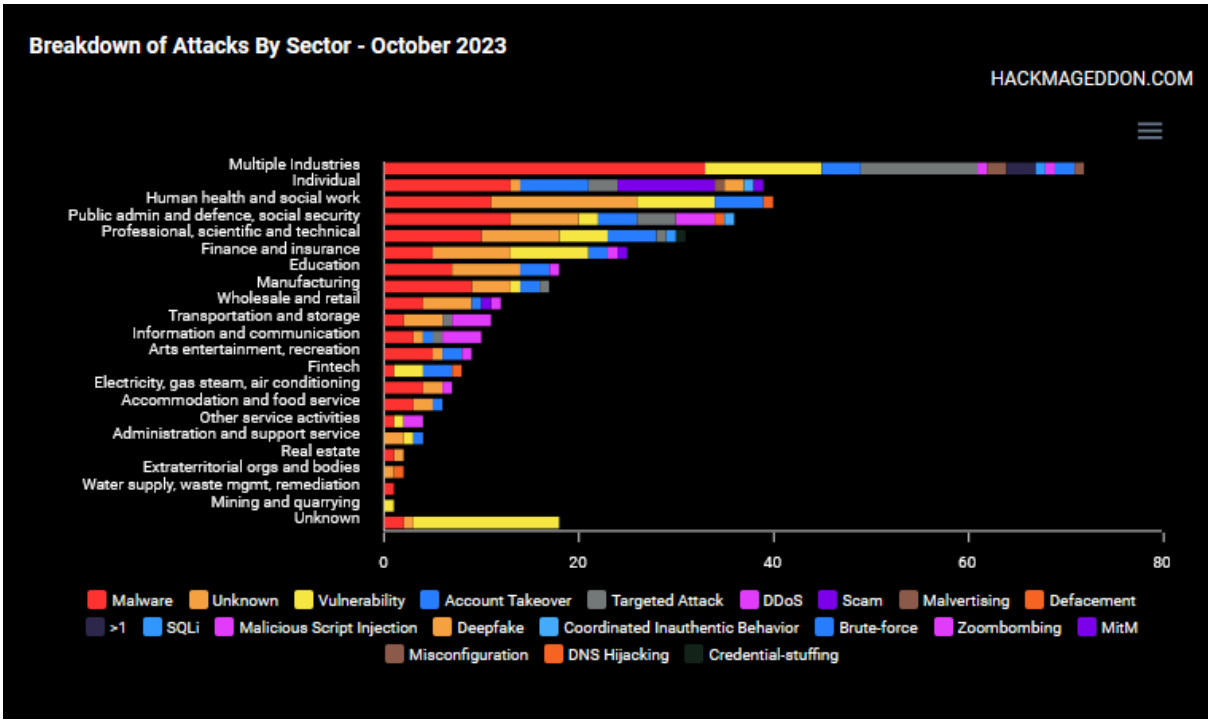


Рис 1.2.31 – Графік розподілу атак по секторам

Листопад 2023:

Як завжди, кіберзлочинність лідирує в рейтингу мотивацій із 78,7% , що трохи більше порівняно з 76,7% у жовтні, але знову нижчим за 80% (четвертий місяць поспіль). Операції, здійснені кібершпигунством , трохи зросли до 9,7% з 8,3 % , тоді як Хактивізм впав до 5,4% з 9,4% . Чотири події характеризували Cyber Warfare з відсотком, який подвоївся, другий місяць поспіль, до 2,1% з 1,1% .

Діаграму методів атак очолює зловмисне програмне забезпечення з 42,1% порівняно з 34,2% , а атаки, здійснені через уразливості , посідають друге місце з 11,3% , трохи нижче порівняно з 15,2% попереднього місяця. Третє місце серед відомих методів займають цілеспрямовані атаки з 7,2% проти 6,1% і випереджають захоплення облікових записів з відсотком (5,4%), зменшивши вдвічі значення попереднього місяця (11%).

Розподіл цілей знову лідирує з кількома організаціями, трохи знизившись до 17,7% з 19,3% , випереджаючи охорону здоров'я з 14,1% трохи підвищившись порівняно з 13,4% попереднього місяця.

Події на день:

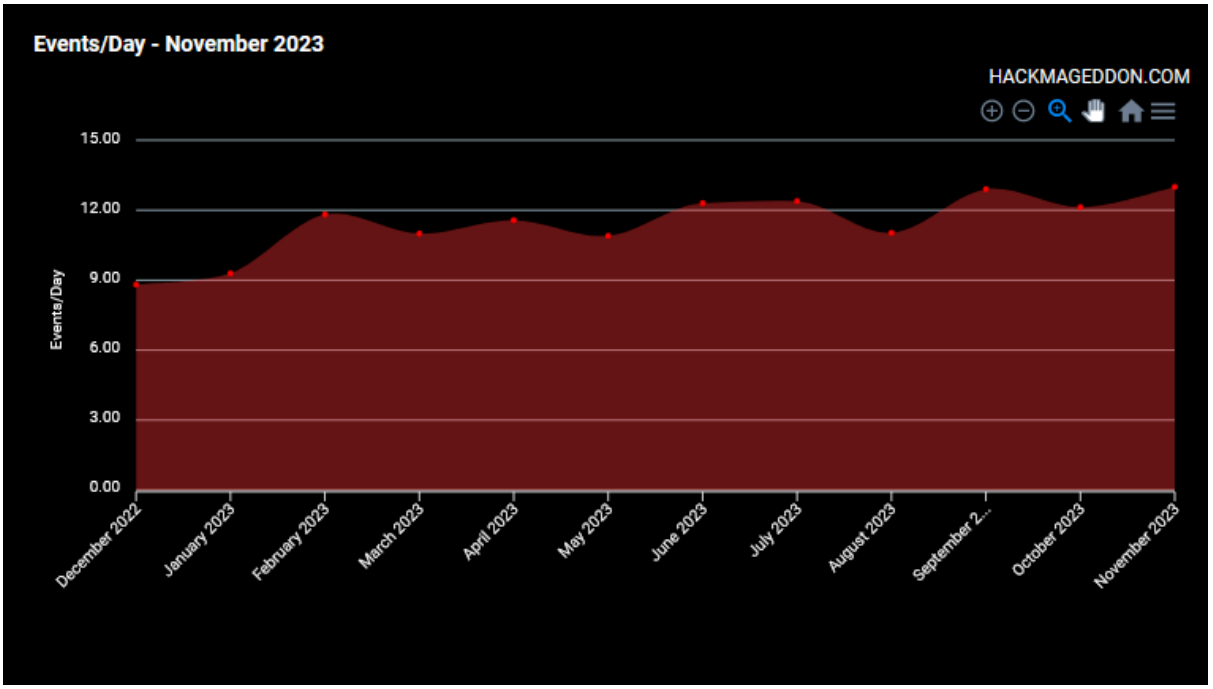


Рис 1.2.32 – Графік подій на день

Графік щоденних тендецій атак:

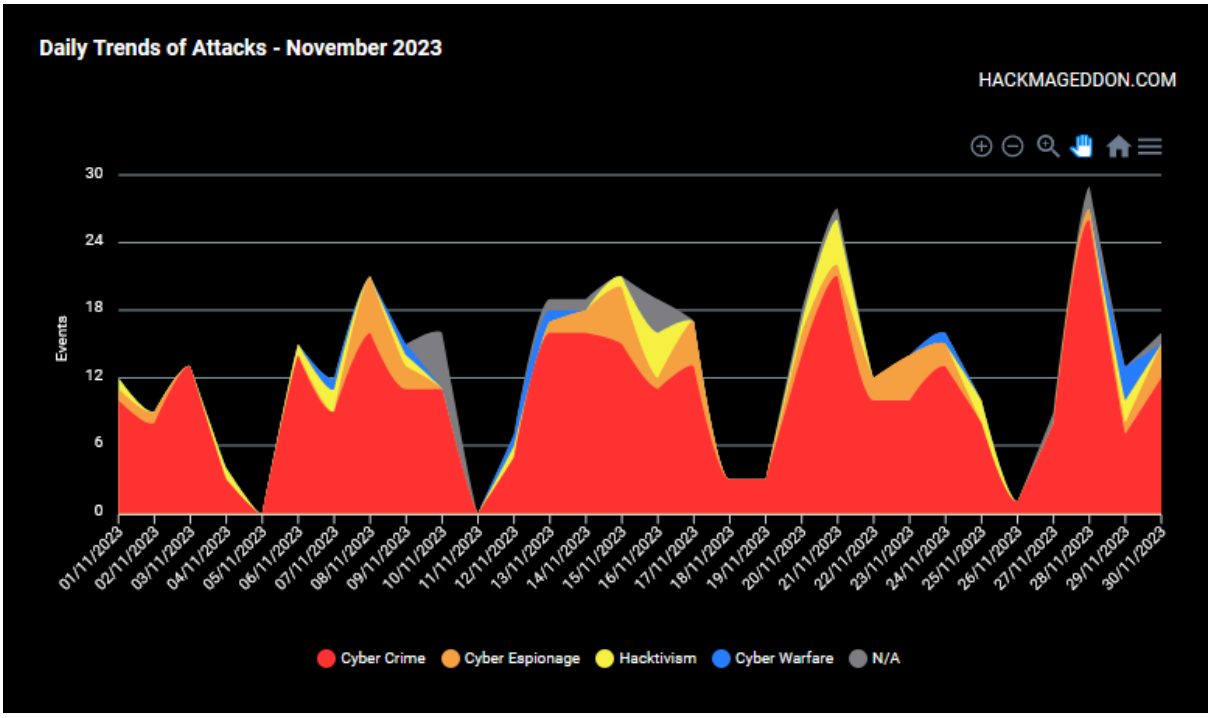


Рис 1.2.33 – Графік подій

Мотивації:

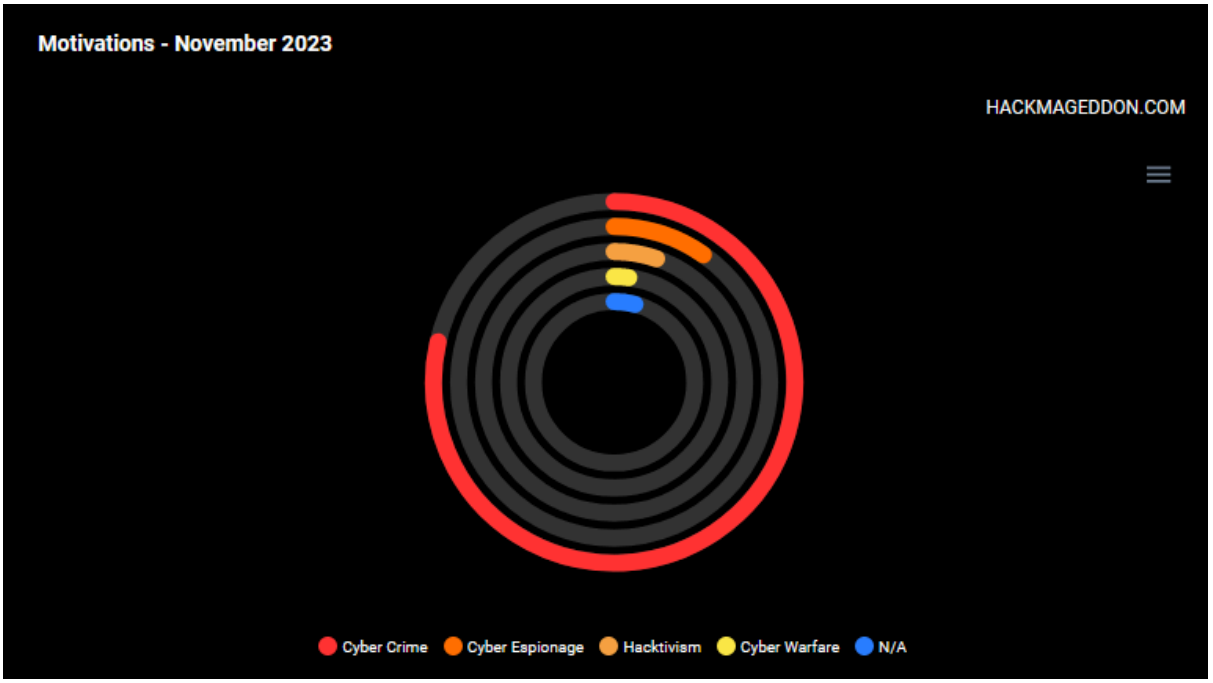


Рис 1.2.34 – Графік мотивацій

Атаки:

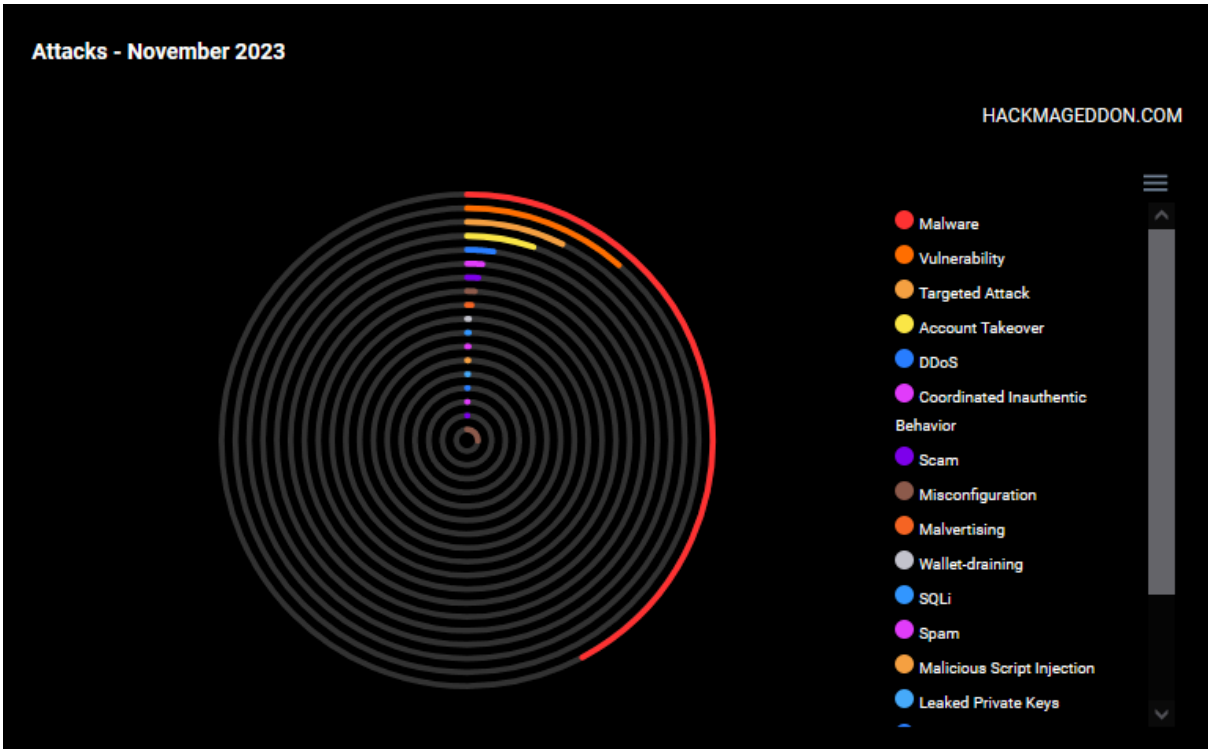


Рис 1.2.35 – Графік атак

Цілі:

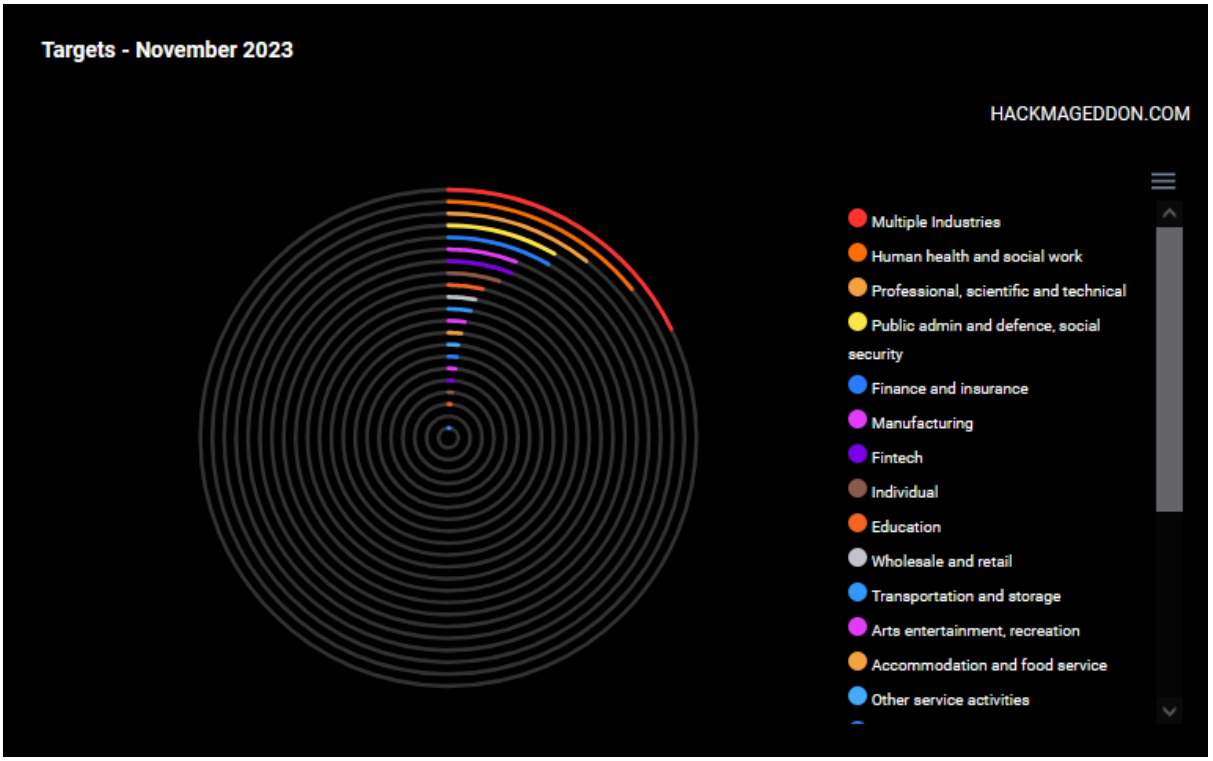


Рис 1.2.36 – Графік цілей

Розподіл атак:

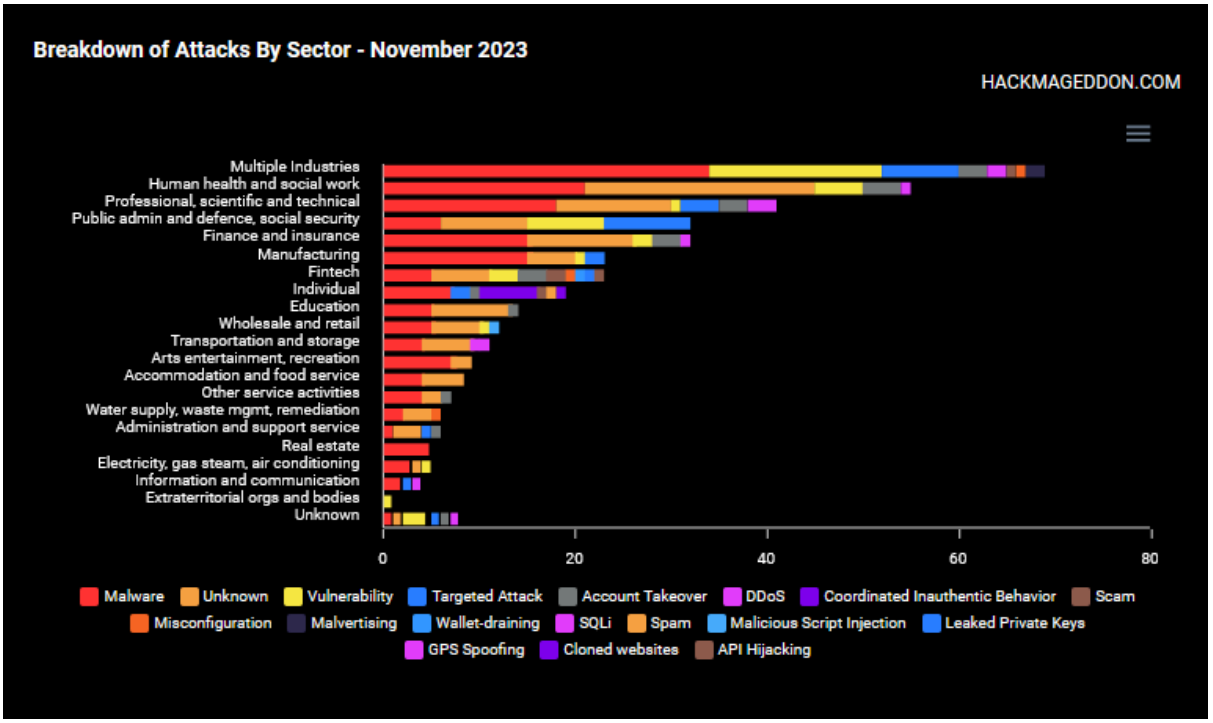


Рис 1.2.31 – Графік розподілу атак по секторам

1.3. Методи захисту інформації в інформаційних системах

Захист інформації в інформаційних системах є критично важливим аспектом забезпечення конфіденційності, цілісності та доступності конфіденційних даних і ресурсів. Для захисту інформації від несанкціонованого доступу, розкриття, модифікації або знищення використовуються різні методи та заходи.

Одним із найпоширеніших методів є контроль доступу, який передбачає впровадження механізмів обмеження доступу до інформації та ресурсів на основі привілеїв і ролей користувачів. Сюди входять процеси аутентифікації для перевірки особи користувачів і механізми авторизації для визначення рівня доступу, наданого кожному користувачеві. Контроль доступу може здійснюватися за допомогою облікових записів користувачів, паролів, ключів шифрування, біометричної автентифікації та інших факторів автентифікації.

Шифрування - ще один широко застосовуваний метод захисту інформації. Воно передбачає перетворення даних у нечитабельну форму за допомогою алгоритмів шифрування та криптографічних ключів. Шифрування гарантує, що навіть якщо неавторизовані особи отримають

доступ до даних, вони не зможуть інтерпретувати або використовувати їх без відповідних ключів для розшифрування. Шифрування зазвичай використовується для захисту даних під час зберігання, передачі та спілкування.

Заходи мережевої безпеки застосовуються для захисту інформаційних систем від зовнішніх загроз. Сюди входить використання брандмауерів, систем виявлення та запобігання вторгненням, віртуальних приватних мереж (VPN) та безпечних мережевих протоколів. Ці заходи допомагають виявити та запобігти несанкціонованому доступу, мережевим атакам та витоку даних.

Резервне копіювання даних і планування аварійного відновлення є важливими методами захисту інформаційних систем від втрати даних і забезпечення безперервності бізнесу. Регулярне резервне копіювання даних і впровадження надійних стратегій резервного копіювання та відновлення допомагають організаціям відновити критично важливу інформацію в разі збоїв обладнання, стихійних лих або інших непередбачуваних подій.

Впровадження виправлень та оновлень безпеки є важливим для захисту інформаційних систем від відомих вразливостей та експлойтів. Регулярне оновлення програмного забезпечення, операційних систем і додатків допомагає усунути слабкі місця в системі безпеки та запобігти несанкціонованому доступу або використанню.

Програми підвищення обізнаності та навчання з питань безпеки застосовуються для інформування користувачів про ризики, найкращі практики та політики безпеки. Тренінги підвищують обізнаність про поширені загрози, методи соціальної інженерії, спроби фішингу та важливість дотримання протоколів безпеки. Пропагуючи культуру безпеки, організації можуть зменшити ризики, пов'язані з людськими помилками, та покращити загальний рівень інформаційної безпеки.

Заходи фізичної безпеки також важливі для захисту інформаційних систем. Це включає захист центрів обробки даних, серверних кімнат та іншої критично важливої інфраструктури за допомогою фізичного

контролю доступу, систем спостереження, сигналізації та контролю навколишнього середовища.

Крім того, впровадження політик, процедур та інструкцій з безпеки забезпечує основу для управління та підтримки інформаційної безпеки. Політики визначають правила та очікування щодо обробки інформації, контролю доступу, реагування на інциденти та інших аспектів, пов'язаних з безпекою. Регулярні аудити та оцінки безпеки допомагають виявити вразливі місця та прогалини в заходах безпеки, що дозволяє постійно вдосконалювати та посилювати захист інформації.

Загалом, комплексний підхід до захисту інформації поєднує технічні, процедурні та організаційні заходи. Використовуючи різні методи та постійно адаптуючись до нових загроз, організації можуть підвищити рівень безпеки своїх інформаційних систем і захистити конфіденційні дані від несанкціонованого доступу або компрометації.

Розділ 2. Методика оцінки рівня захищеності інформаційної системи

Методологія оцінки рівня безпеки інформаційної системи - це структурований підхід, який допомагає організаціям оцінити ефективність і надійність своїх заходів безпеки. Ця методологія передбачає систематичний і всебічний аналіз різних аспектів інформаційної системи для виявлення вразливостей, ризиків і областей для поліпшення.

Процес зазвичай починається з визначення обсягу оцінки, що включає визначення активів, ресурсів і компонентів інформаційної системи, які будуть оцінюватися. Цей крок допомагає встановити чіткі цілі та межі оцінювання.

Наступний крок передбачає збір інформації про систему, зокрема про її архітектуру, мережеву інфраструктуру, програмні та апаратні компоненти, контроль доступу та політику безпеки. Ця інформація забезпечує основу для розуміння поточного стану безпеки системи та її потенційних вразливостей.

Після етапу збору інформації проводиться оцінка ризиків для виявлення потенційних загроз, вразливостей і ризиків для інформаційної

системи. Це передбачає аналіз різних факторів, включаючи зовнішні загрози, внутрішні вразливості, потенційні наслідки та ймовірність виникнення. Оцінка ризиків допомагає визначити пріоритетність заходів безпеки і визначити, куди слід спрямувати ресурси для усунення найбільш критичних ризиків.

На основі результатів оцінки ризиків впроваджуються засоби контролю безпеки та контрзаходи, спрямовані на зменшення виявлених ризиків та вразливостей. Ці засоби контролю можуть включати технічні заходи, такі як брандмауери, системи виявлення вторгнень, шифрування та контроль доступу, а також процедурні та адміністративні заходи, такі як політики безпеки, навчальні програми та плани реагування на інциденти.

Після того, як засоби контролю безпеки впроваджені, проводяться тестування та оцінка їхньої ефективності. Це може включати проведення тестування на проникнення, сканування вразливостей та аудит безпеки для виявлення будь-яких слабких місць або вразливостей, які необхідно усунути.

Заключний етап методології передбачає постійний моніторинг і вдосконалення. Регулярний моніторинг допомагає виявляти нові загрози та вразливості, які можуть виникнути з часом, гарантуючи, що заходи безпеки залишаються актуальними та ефективними. Крім того, періодично проводяться переоцінки, щоб оцінити безпековий ландшафт, що змінюється, і внести необхідні корективи в стратегію безпеки.

В цілому, методологія оцінки рівня безпеки інформаційної системи забезпечує структурований і систематичний підхід до визначення, оцінки та посилення безпеки системи. Дотримуючись цієї методології, організації можуть краще захистити свої інформаційні активи, мінімізувати ризики та підтримувати конфіденційність, цілісність і доступність своїх систем і даних

2.1. Етапи процесу оцінки рівня захищеності інформаційної системи

Процес оцінки рівня безпеки інформаційної системи є важливим аспектом забезпечення захисту та цілісності конфіденційних даних. Він передбачає систематичний і структурований підхід до оцінки ефективності заходів безпеки, виявлення вразливостей і слабких місць, а також оцінки загального стану безпеки системи. Ось короткий огляд етапів цього процесу:

1. **Планування та визначення обсягу:**
   - Визначте сферу оцінювання, включаючи системи, активи та компоненти, що підлягають оцінюванню.
   - Визначте цілі, завдання та бажані результати оцінювання.
   - Визначте методологію та інструменти оцінювання, які будуть використані.

2. **Збір інформації:**
   - Зберіть інформацію про інформаційну систему, таку як архітектура системи, топологія мережі та програмні компоненти.
   - Зберіть документацію, політики та процедури, пов'язані з контролем безпеки та конфігураціями.
   - Виявлення потенційних загроз і вразливостей, які можуть існувати.

3. **Оцінка вразливостей:**
   - Проведення сканування вразливостей для виявлення відомих вразливостей в системі.
   - Проаналізуйте результати сканування вразливостей і визначте пріоритетність вразливостей на основі їхньої серйозності та потенційного впливу.

4. **Оцінка ризиків:**
   - Оцініть виявлені вразливості в контексті толерантності до ризику та бізнес-цілей організації.
   - Оцініть ймовірність та потенційний вплив використання вразливостей.
   - Визначте пріоритетність ризиків на основі їхньої серйозності та розробіть план зменшення ризиків.

5. Оцінка засобів контролю безпеки:

- Оцініть ефективність існуючих засобів контролю безпеки, таких як контроль доступу, механізми автентифікації, шифрування та системи моніторингу.
- Протестуйте засоби контролю на відповідність найкращим галузевим практикам і стандартам безпеки.
- Визначте будь-які слабкі місця або прогалини в засобах контролю безпеки.

6. Тестування на проникнення:

- Проведіть контрольовані спроби використання вразливостей і отримання несанкціонованого доступу до системи.
- Перевірте стійкість системи до різних векторів атак, таких як мережеві атаки, атаки на рівні додатків, соціальна інженерія тощо.
- Визначити слабкі місця в системі безпеки та потенційні точки входу для зловмисників.

7. Звітність та рекомендації:

- Підготуйте комплексний звіт, що підсумовує результати, вразливості, ризики та рекомендовані дії.
- Надайте практичні рекомендації щодо усунення виявлених вразливостей та покращення загального стану безпеки.
- Повідомте про результати зацікавленим сторонам, зокрема керівництву, IT-персоналу та відповідним департаментам.

8. Усунення та подальші дії:

- Впровадити рекомендовані заходи безпеки та заходи з усунення виявлених вразливостей і ризиків.
- Регулярно здійснювати моніторинг та оцінювати ефективність впроваджених засобів контролю безпеки.
- Проводити періодичні переоцінки для забезпечення постійного вдосконалення безпеки інформаційної системи.

2.2. Методи оцінки рівня захищеності інформаційної системи

Методи оцінки рівня безпеки інформаційної системи включають в себе різні підходи і техніки для оцінки ефективності засобів контролю безпеки і виявлення потенційних вразливостей. Ось коротке пояснення деяких поширених методів:

1. **Оцінка вразливостей:** Цей метод спрямований на виявлення відомих вразливостей в інформаційній системі. Зазвичай він передбачає використання автоматизованих інструментів або ручних методів для сканування програмного забезпечення, конфігурацій та мережевої інфраструктури системи на наявність відомих вразливостей. Оцінка дає уявлення про слабкі місця, які можуть бути використані зловмисниками.

2. **Тестування на проникнення:** Тестування на проникнення, також відоме як етичний хакінг, передбачає імітацію реальних атак на інформаційну систему. Кваліфіковані фахівці намагаються використати вразливості, щоб отримати несанкціонований доступ, підвищити привілеї або скомпрометувати конфіденційні дані. Тестування на проникнення забезпечує комплексну оцінку безпеки системи шляхом виявлення вразливостей, які не можуть бути виявлені за допомогою автоматизованого сканування.

3. **Аудит безпеки:** Аудит безпеки - це систематична оцінка засобів контролю, політик і процедур безпеки інформаційної системи. Вони оцінюють відповідність галузевим стандартам, найкращим практикам та нормативним вимогам. Аудит безпеки може проводитися як внутрішніми, так і зовнішніми аудиторами, щоб переконатися, що система відповідає стандартам безпеки, і виявити сфери, які потребують вдосконалення.

4. **Оцінка ризиків:** Оцінка ризиків передбачає виявлення та оцінку потенційних ризиків для інформаційної системи. Вона враховує загрози, вразливості та потенційний вплив інциденту, що може статися. Аналізуючи ймовірність і вплив ризиків, організації

можуть визначити пріоритети у своїх зусиллях щодо їх зменшення та ефективно розподілити ресурси.

5. **Оцінка відповідності:** Оцінка відповідності зосереджена на оцінці того, чи відповідає інформаційна система конкретним нормативним або галузевим вимогам. Вона включає в себе перевірку засобів контролю, політик і процедур для забезпечення відповідності відповідним стандартам і правилам, таким як GDPR, HIPAA або PCI DSS.

6. **Показники та вимірювання безпеки:** Показники безпеки передбачають вимірювання та кількісну оцінку різних аспектів безпеки інформаційної системи. Сюди входить відстеження ключових показників ефективності (KPI), таких як кількість інцидентів безпеки, час реагування, ефективність управління виправленнями або рівень відповідності. Показники безпеки допомагають оцінити ефективність засобів контролю безпеки та надають інформацію для постійного вдосконалення.

Важливо відзначити, що ці методи слід застосовувати систематично та комплексно, враховуючи унікальні характеристики та вимоги інформаційної системи, яка оцінюється. Крім того, комбінація цих методів може бути використана для забезпечення більш цілісного уявлення про стан безпеки системи.

2.3. Застосування методики оцінки рівня захищеності інформаційної системи

Застосування методології оцінки рівня безпеки інформаційної системи передбачає використання структурованого та систематичного підходу до оцінки засобів контролю безпеки, виявлення вразливостей та оцінки загального стану безпеки. Нижче наведено огляд типових етапів застосування такої методології:

1. **Планування**: Визначте цілі, сферу застосування та обмеження оцінювання. Визначте методи та інструменти оцінювання, які будуть використані. Визначте залучені зацікавлені сторони та встановіть чіткі канали комунікації.

2. **Збір інформації**: Зберіть відповідну інформацію про інформаційну систему, включаючи її архітектуру, компоненти, мережеву інфраструктуру, політику та процедури безпеки. Перегляньте будь-яку доступну документацію, таку як системні схеми, конфігурації та попередні оцінки.

3. **Моделювання загроз**: Проаналізуйте потенційні загрози та ризики, характерні для інформаційної системи. Визначте можливі вектори атак, вразливості та потенційні наслідки. Цей крок допомагає визначити пріоритетність заходів з оцінювання та зосередитися на критичних сферах.

4. **Виконання оцінки**: Виконайте заходи з оцінювання на основі обраної методології. Це може включати сканування вразливостей, тестування на проникнення, аудит контролю безпеки, аналіз ризиків та перевірку відповідності. Використовуйте відповідні інструменти та методи для виявлення слабких місць, вразливостей та прогалин у засобах контролю безпеки.

5. **Аналіз даних**: Проаналізуйте результати та дані, зібрані під час оцінювання. Оцініть серйозність і потенційний вплив виявлених вразливостей і недоліків. Визначте пріоритетність висновків на основі рівня ризику та потенційного впливу на організацію.

6. **Складання звіту**: Підготуйте комплексний звіт, який підсумовує результати оцінки, включаючи виявлені вразливості, ризики та рекомендації щодо вдосконалення. Чітко повідомте про результати відповідним зацікавленим сторонам, надавши практичні висновки та рекомендації щодо посилення безпеки системи.

7. **Усунення та подальші дії**: співпрацюйте з організацією для усунення виявлених вразливостей і недоліків. Розробляйте та впроваджуйте план усунення проблем, посилення контролю безпеки та зменшення ризиків. Відстежуйте хід усунення недоліків і проводьте подальші оцінки для перевірки ефективності вжитих заходів.

8. **Постійне вдосконалення**: Сприяти розвитку культури постійного вдосконалення, враховуючи уроки, отримані в процесі оцінювання. Оновлюйте політику та процедури безпеки, проводьте регулярні тренінги з безпеки та створіть механізми для постійного моніторингу, оцінки та вдосконалення безпеки інформаційної системи.

Важливо пристосувати методологію до конкретного контексту та вимог організації та інформаційної системи, що оцінюється. Крім того, забезпечте дотримання відповідних законів, нормативних актів і галузевих стандартів протягом усього процесу оцінювання.

Розділ 3. Аналіз результатів оцінки рівня захищеності інформаційної системи.

Аналіз результатів оцінки рівня безпеки інформаційної системи є важливим кроком у розумінні сильних і слабких сторін заходів безпеки системи. Цей аналіз включає в себе всебічний огляд висновків і рекомендацій, наданих в процесі оцінки, що дозволяє організаціям приймати обґрунтовані рішення і вживати відповідних заходів для посилення своєї системи безпеки. Нижче наведено огляд ключових етапів аналізу результатів оцінювання:

1. Ознайомлення з методологією оцінювання: Почніть з вивчення методології, використаної для оцінки безпеки. Зрозумійте підхід, методи та інструменти, що використовувалися під час оцінювання. Цей аналіз гарантує, що оцінка була проведена з використанням визнаних стандартів, рамок та найкращих практик, що підтверджує достовірність отриманих результатів.

2. Оцініть результати оцінювання: Ретельно проаналізуйте результати та вразливі місця, виявлені під час оцінювання. Розподіліть їх за категоріями, виходячи з їхньої серйозності, можливості використання та потенційного впливу на інформаційну систему та організацію. Ця оцінка дає уявлення про поточний стан безпеки та висвітлює сфери, які потребують негайної уваги.

3. Визначте пріоритетність виявлених ризиків: Визначте пріоритетність виявлених ризиків на основі їхньої критичності та потенційного впливу. Візьміть до уваги ймовірність використання, потенційні наслідки та вартість активів, які можуть постраждати. Таке визначення пріоритетів допомагає організаціям зосередити свої ресурси на усуненні найбільш значущих ризиків та вразливостей у першу чергу.

4. Оцініть наявні засоби контролю безпеки: Оцініть ефективність існуючих засобів контролю та заходів безпеки. Визначте, чи вони адекватно реагують на виявлені ризики та вразливості. Визначте будь-які прогалини, слабкі місця або сфери, де контроль може бути недостатнім. Ця оцінка допомагає організаціям зрозуміти, де потрібні вдосконалення для посилення захисту їхньої безпеки.

5. Запропонуйте заходи з усунення недоліків: На основі результатів оцінки розробіть комплексний план усунення виявлених вразливостей та ризиків. Цей план має включати конкретні заходи з виправлення ситуації, такі як впровадження нових засобів контролю, оновлення існуючих, вдосконалення процесів або підвищення рівня обізнаності та навчання з питань безпеки. Кожен запропонований захід має бути чітко визначеним, здійсненним і узгодженим з цілями та пріоритетами організації.

6. Розгляньте вимоги відповідності: Оцініть, чи відповідає інформаційна система відповідним нормативно-правовим вимогам, галузевим стандартам і політикам організації. Визначте будь-які проблеми невідповідності та включіть їх у план виправлення. Забезпечення відповідності допомагає зменшити юридичні ризики та сприяє формуванню культури безпеки в організації.

7. Розробіть план дій: Створіть детальний план дій, в якому будуть вказані рекомендовані заходи з усунення недоліків, відповідальні особи, терміни та виділені ресурси. Цей план слугує дорожньою картою для впровадження запропонованих покращень у сфері безпеки. Він має бути реалістичним, здійсненним та адаптивним,

щоб врахувати будь-які нові ризики або зміни в організаційному середовищі.

8. Моніторинг та аналіз прогресу: Постійно контролюйте виконання заходів з усунення недоліків та регулярно аналізуйте їхню ефективність. Встановіть метрики та ключові показники ефективності для відстеження прогресу та вимірювання впливу заходів з посилення безпеки. Проводити періодичні переоцінки, щоб переконатися, що заходи безпеки залишаються ефективними та відповідають ландшафту загроз, що змінюється.

9. Інформування про висновки та рекомендації: Ефективно повідомляйте результати аналізу, план усунення недоліків та оновлення інформації про прогрес відповідним зацікавленим сторонам, таким як вище керівництво, IT-команди та інший персонал, залучений до забезпечення безпеки інформаційної системи. Чітке інформування допомагає підвищити обізнаність, заручитися підтримкою та забезпечити прихильність організації до ініціатив з покращення безпеки.

10. Налагодити безперервне управління безпекою: Впроваджуйте надійні практики управління безпекою, щоб підтримувати покращення безпеки після початкового оцінювання. Це включає встановлення чітких ролей та обов'язків, визначення процесів реагування на інциденти та управління ними, проведення регулярних тренінгів з підвищення обізнаності з питань безпеки, а також постійний моніторинг та оцінку ефективності засобів контролю безпеки.

Дотримуючись цих кроків, організації можуть отримати цінну інформацію про стан безпеки своєї інформаційної системи, визначити сфери, які потребують вдосконалення, і розробити дорожню карту для підвищення безпеки. Дуже важливо залучати кваліфікованих фахівців з безпеки, які володіють досвідом проведення оцінки безпеки та аналізу результатів. Їхні знання та розуміння сприятимуть точності та надійності аналізу, забезпечуючи здатність організації зменшити ризики та захистити критичні активи.

Треба пам'ятати, що безпека - це безперервний процес, і постійний моніторинг, оцінка та адаптація є важливими для підтримки ефективної позиції безпеки перед обличчям загроз, що постійно змінюються.

3.1. Виявлення недоліків та потенційних загроз інформаційної безпеки

Виявлення недоліків та потенційних загроз інформаційній безпеці є критично важливим кроком у забезпеченні безпеки нашого цифрового світу. Як людина, яка взяла на себе відповідальність за це завдання, я самостійно провела процес виявлення таких вразливостей та потенційних загроз. Протягом своєї практичної роботи я використовував декілька інструментів, а саме Aircrack-ng, Nmap, Metasploit та Wireshark, щоб виконати комплексний аналіз безпеки в моєму робочому середовищі.

Використовуючи Aircrack-ng, я зосередився на аналізі безпеки нашої Wi-Fi мережі. Я оцінив вразливості в протоколах шифрування і визначив можливі способи злому паролів. Цей інструмент дозволив мені оцінити силу нашої бездротової мережі та розробити рекомендації щодо її посилення.

Nmap виявився безцінним інструментом для сканування портів і виявлення вразливостей на системному рівні. Він допоміг мені зібрати інформацію про активні системи, виявити відкриті порти та оцінити їх на предмет потенційних проблем безпеки. Результати сканування за допомогою Nmap стали основою для подальшого аналізу та усунення виявлених проблем.

Metasploit був використаний для проведення тестування на проникнення в нашу систему. За допомогою цього інструменту я змоделював різні типи атак, протестував вразливості та оцінив стійкість системи до реальних загроз. Це дозволило мені виявити потенційні вектори атак.

Wireshark став незамінним інструментом для аналізу мережевого трафіку та виявлення аномальної активності. За допомогою цього інструменту я відстежував пакети, перехоплював дані та аналізував їх, щоб виявити потенційні загрози та зловмисну поведінку в мережі.

Використовуючи ці інструменти, я систематично виявляв слабкі місця та потенційні загрози інформаційній безпеці в моєму робочому середовищі. Детальний аналіз, проведений за допомогою цих інструментів, надав мені цінну інформацію для розробки та впровадження заходів для покращення безпеки та запобігання потенційним атакам.

1. **Aircrack-ng**

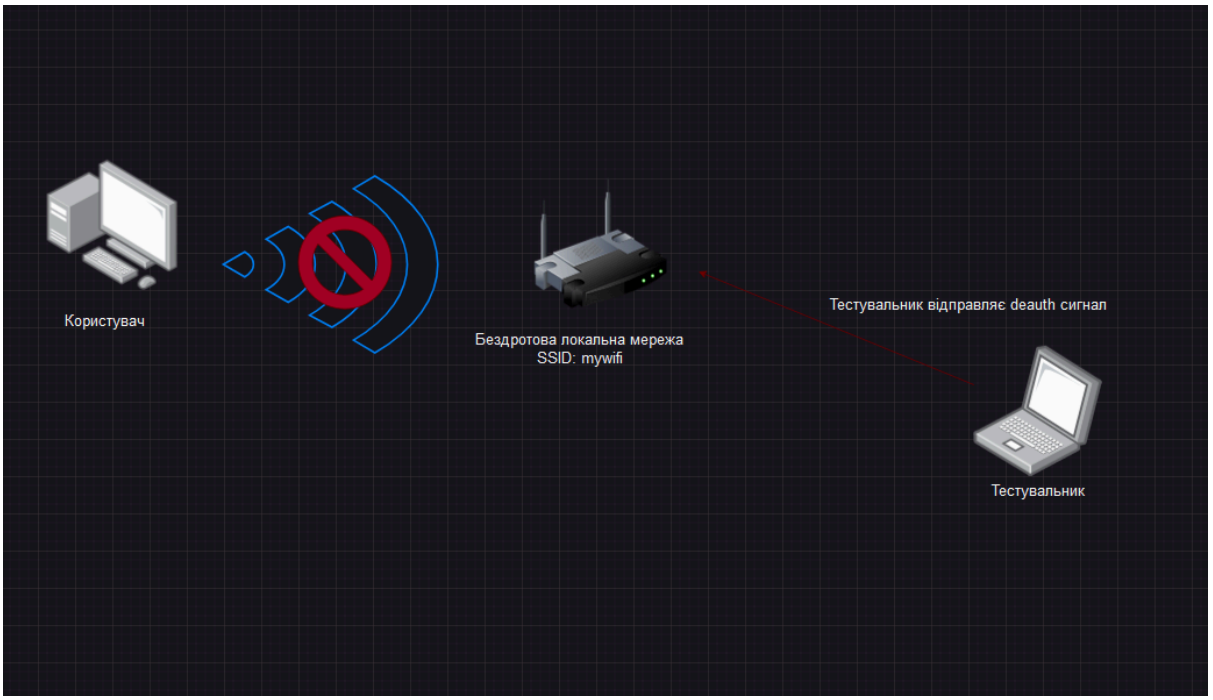


Рис 3.1.1. - Схема Бездротової атаки

В ролі тестувальника, я можу відправити деаутентифікаційний сигнал (deauth) для спровокування відключення пристроїв від обраної бездротової мережі. Це дозволяє мені перевірити реакцію мережі та виявити потенційні проблеми з безпекою.

Деаутентифікаційний сигнал є спеціальним пакетом, який відправляється до бездротових пристроїв, щоб змусити їх відключитися від мережі. Це може бути корисним випробуванням безпеки, оскільки дозволяє оцінити, як мережа реагує на такі атаки і які заходи захисту можуть бути необхідні.

Деаутентифікаційний сигнал (deauth) - це спеціальний тип бездротового пакета, який використовується для відключення бездротових пристроїв від бездротової мережі. Він використовується для спровокування відключення або змушення пристроїв покинути мережу.

Зазвичай, деаутентифікаційний сигнал відправляється відправником, який претендує на роль точки доступу або аутентифікаційного сервера, до конкретного бездротового пристрою. Цей сигнал може бути використаний для різних цілей, таких як проведення тестування безпеки мережі, діагностика проблем мережі або зловживання в разі недоброзичливих намірів.

Зазвичай, деаутентифікаційний сигнал використовується тестерами та адміністраторами мереж для перевірки реакції мережі на такий тип атаки та для виявлення можливих проблем з безпекою. Однак важливо пам'ятати, що використання деаутентифікаційного сигналу без належної авторизації або згоди власника мережі може бути незаконним та неправомірним.

Як це виглядає на практиці:

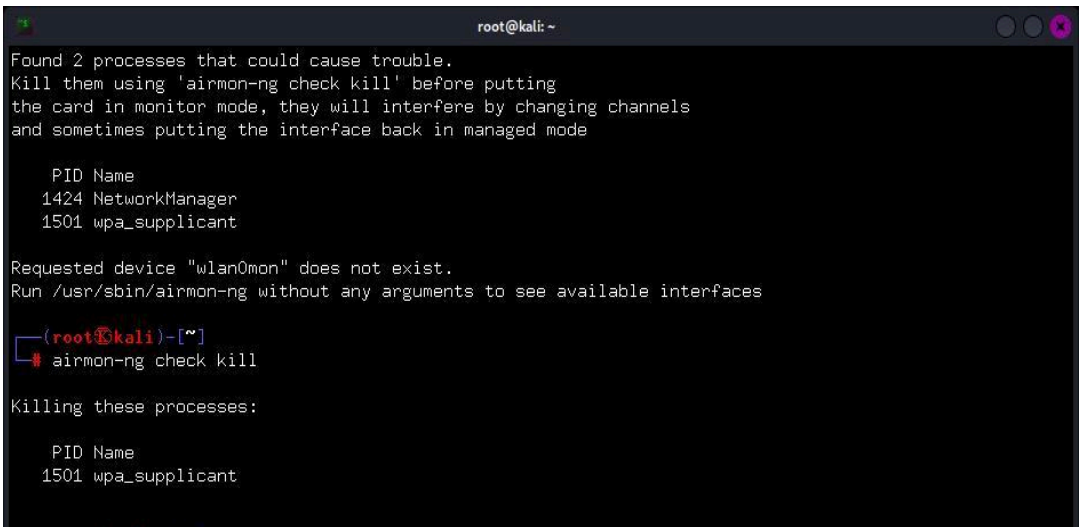


Рис 3.1.2. - Відключення зайвих процессів

Команда "airmon-ng check kill" використовується для перевірки будь-яких процесів, які можуть заважати режиму моніторингу на бездротових інтерфейсах, і для їх припинення, якщо необхідно.

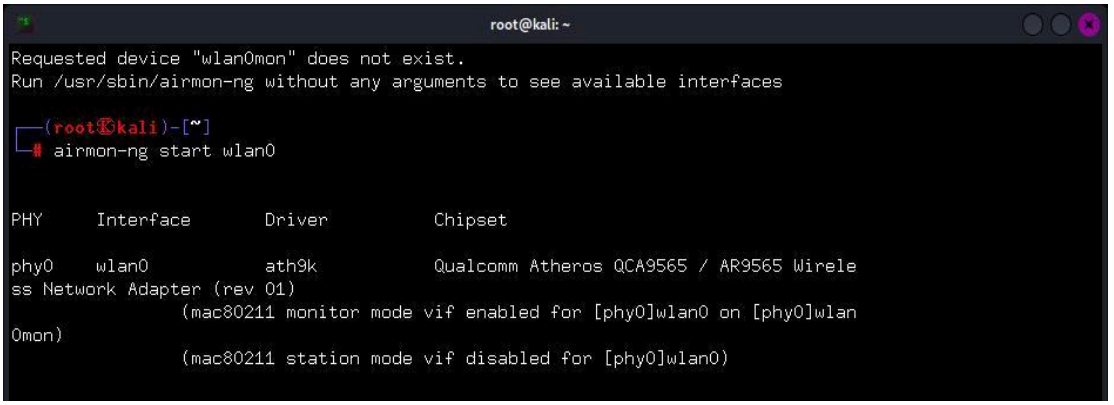


Рис 3.1.3. – Початок роботи в режиму моніторингу

Команда «airmon-ng start wlan0» використовується для запуску режиму монітору на бездротовому інтерфейсі «wlan0» за допомогою набору Aircrack-ng.

Коли я виконую цю команду, «airmon-ng» спробує перевести вказаний бездротовий інтерфейс у режим моніторингу. Режим моніторингу дає змогу фіксувати та аналізувати трафік бездротової мережі, що корисно для тестування безпеки бездротового зв’язку, аналізу пакетів та інших пов’язаних дій.

Після виконання команди «airmon-ng» створить новий інтерфейс у режимі монітора, який зазвичай називається «wlan0mon» або подібним. Цей новий інтерфейс можна використовувати з іншими інструментами та утилітами, наданими Aircrack-ng або іншими інструментами бездротового аналізу.

Далі я за допомогою команди "**airodump-ng wlan0mon**" почав пошук мережі.

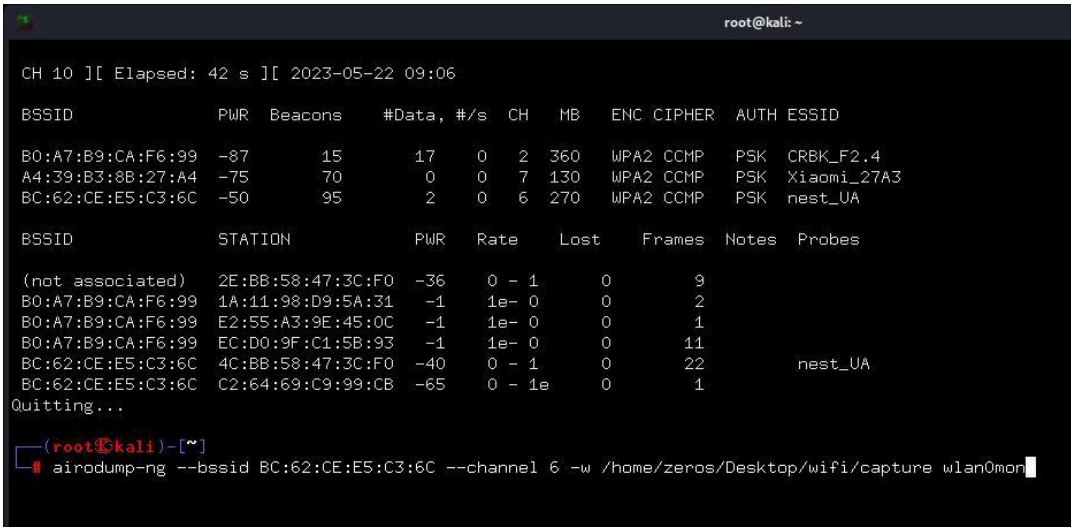


Рис 3.1.4. – Сканування мережі

Після того я обираю мережу для подальшої з нею роботи. Для роботи з обраною мережею, я прописую таку команду:

`airodump-ng -bssid BC:62:CE:ES:C3:6C -channel 6 -w /home/zeros/Desktop/wifi/captute wlan0mon`,

де `-bssid` – це MAC-адрес бездротової мережі. `-channel` – канал на якому працює мережа, `-w` -путь та назва файла у якому буде записан мій HandShake.

*HandShake в контексті безпеки бездротового зв'язку означає процес встановлення безпечного з'єднання між клієнтським пристроєм і точкою доступу (AP) у мережі Wi-Fi. Рукостискання є вирішальним кроком у процесі автентифікації та обміну ключами.

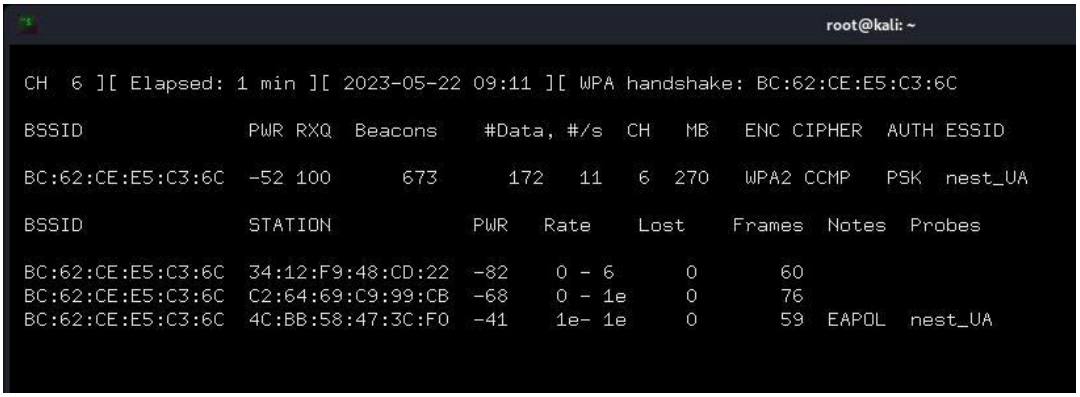


Рис 3.1.5. – Спрямоване сканування мережі

На Рис 3.4. можна побачити крім моєї локальної мережі, ще інші MAC-адреса під STATION – це клієнти які під’єднані до мережі. Їх можна примусово від’єднати за допомогою команди:

```
airplay-ng –deauth 20 -a BC:62:CE:ES:C3:6C -c C2:64:69:C9:99:CB wlan0mon
```

де `–deauth 20` – кількість пакетів які будуть відправлятись для деаутентифікації клієнта, `-a BC:62:CE:ES:C3:6C` – це точка доступа, `-c C2:64:69:C9:99:CB` – клієнтський MAC-адрес.

Мені цього робити не потрібно, я просто відключаюсь на іншому пристрої від мережі, а потім знову підключаюсь.

Після того коли я відключився і знову підключився, я отримаю таке повідомлення:

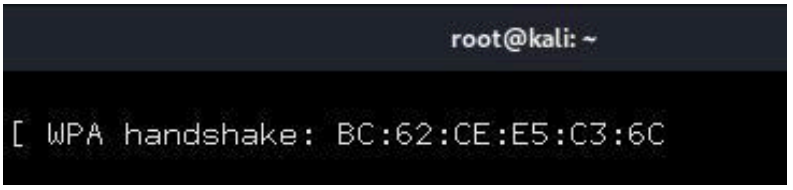


Рис 3.1.6. – Отриманий handshake

Далі я переходжу до директорії де зберігається handshake.

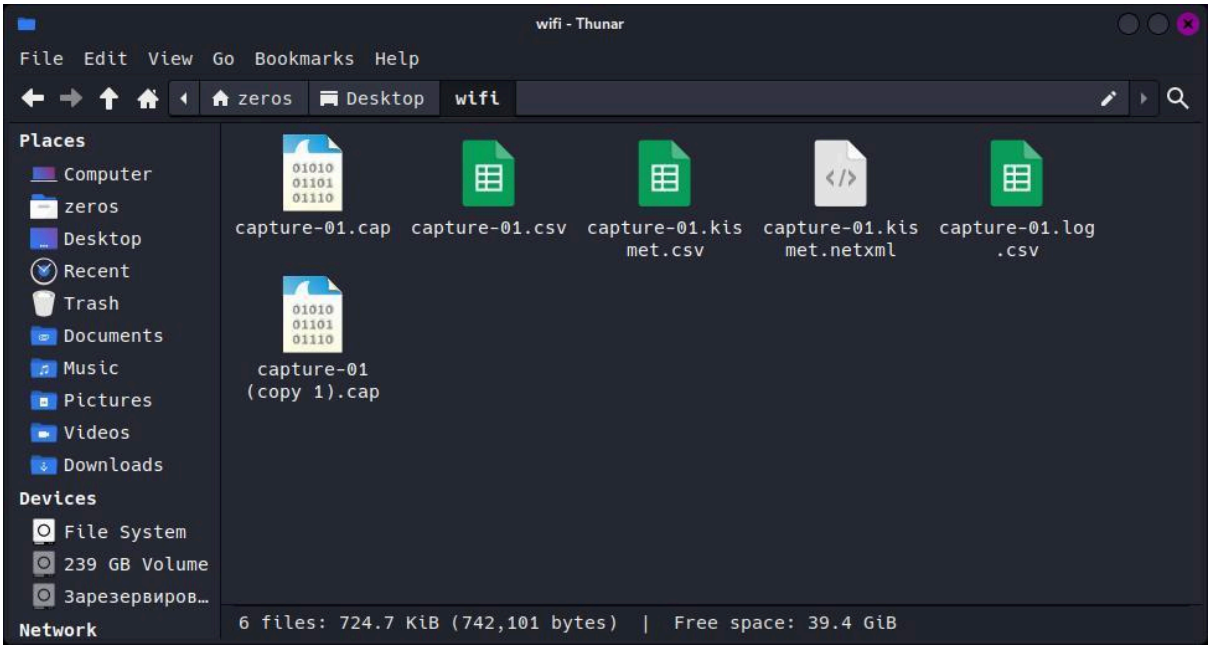


Рис 3.1.7 – Схоплені handshake

Після цього я обираю файл який мені потрібен для роботи – це файл **capture-01.cap**. У цьому файлі всі handshake, які я захопив, для того щоб швидкість підбора паролю була швидше, треба його очистити:

```
┌──(root㉿kali)-[~]
└─# wpaclean /home/zeros/Desktop/cleanHand /home/zeros/Desktop/wifi/capture-01.cap
Pwning /home/zeros/Desktop/wifi/capture-01.cap (1/1 100%)
Net bc:62:ce:e5:c3:6c nest_UA
Done
```

Рис 3.1.8. – Очищення файлу

Далі йде метод підбора паролю. Для того щоб підібрати пароль, треба створити словник у якому будуть написані ймовірні варіанти паролю:

```
root@kali: ~
┌──(root㉿kali)-[~]
└─# aircrack-ng -w /home/zeros/Desktop/info.txt -b bc:62:ce:e5:c3:6c /home/zeros/Desktop/cleanHand.
cap
```

Рис 3.1.9. – Введення параметрів для підбору паролю

де -w – параметр з якого буде підбирати пароль, -b – це точка доступа і я вказую туди мій очищений handshake.

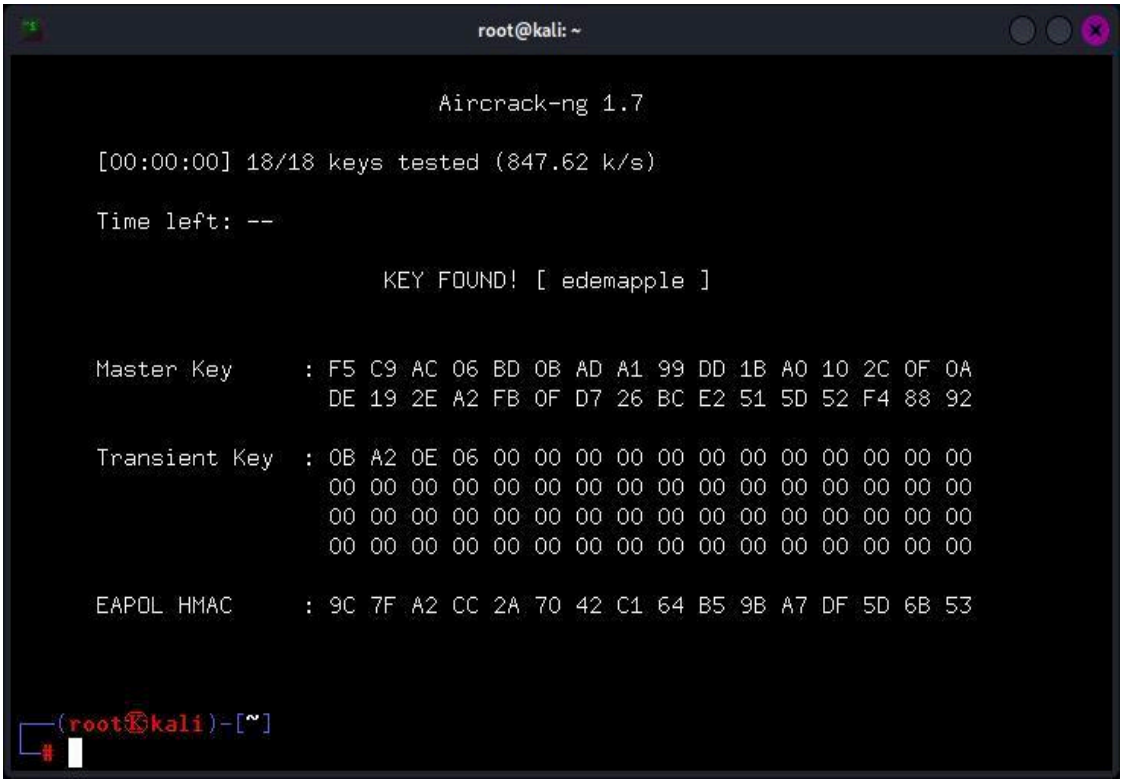


Рис 3.1.10 – Знаходження паролю

Який тут недолік, недолік полягає в тому пароль є простим.

Рис 3.1.11. – Графік схоплення пакетів

- Вертикальна вісь, позначена як "Packets/1 sec", вказує на кількість пакетів, захоплених протягом однієї секунди. Це відображає інтенсивність або швидкість передачі пакетів у мережі в певний момент часу. Чим вище значення на вертикальній осі, тим більше пакетів було перехоплено за цей період.

- Горизонтальна вісь, позначена як "Time(s)", представляє часову шкалу, де кожна одиниця відповідає певному часовому інтервалу. Це дозволяє аналізувати розподіл пакетів за певний період часу.

Спостерігаючи за графіком I/O Wireshark, я можу визначити розподіл пакетів у часі, виявити піки активності, періоди зниження активності та загальні тенденції. Це допоможе мені виявити характеристики мережевої активності, виявити проблеми з трафіком, проаналізувати закономірності і зробити відповідні мережеві конфігурації.

2. Nmap + Wireshark

Перед початком сканування портів у Nmap та Wireshark, мені потрібно дізнатися IP від двох пристроїв. Для цього у обох пристроїв я прописую команду ipconfig, щоб дізнатися IP від пристроїв.

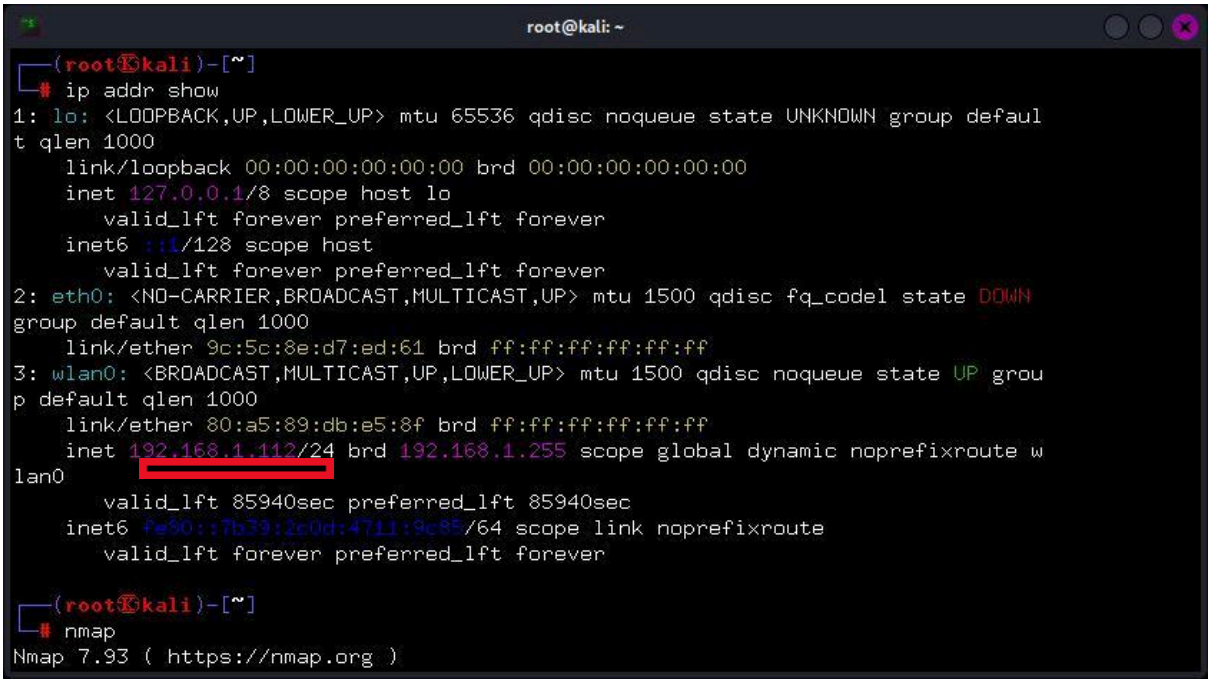


Рис 3.1.12. – IP пристрою у Kali Linux

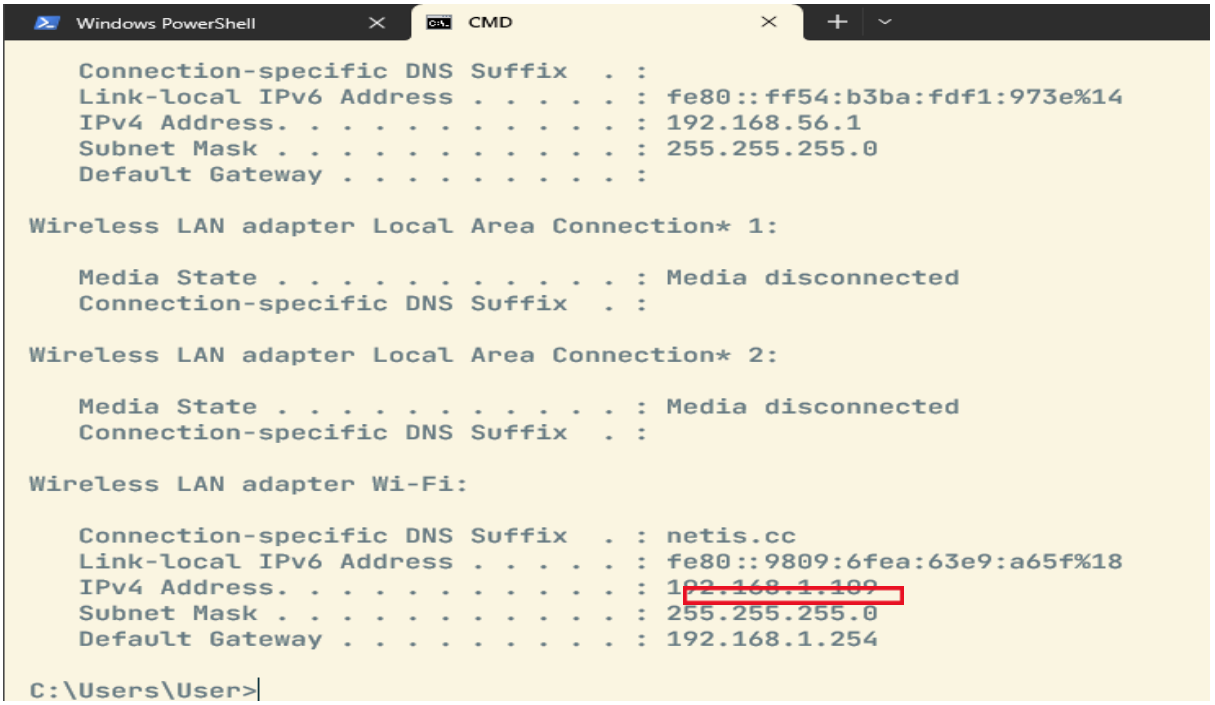


Рис 3.1.13. – IP пристрою у Windows

Windows: 192.168.1.109 – ціль

Kali Linux: 192.168.1.112 – тестер (я)

Далі я продемонструю, як використовувати Wireshark для перехоплення мережевих пакетів, коли зловмисник використовує метод сканування портів NMAP для сканування цілі. У цьому розділі ви можете побачити, як Wireshark записує різні пакети мережевого трафіку для відкритих і закритих портів.

- **Сканування TCP**

TCP-сканування шукає такі TCP-порти, як 22, 21, 23, 445 тощо, і перевіряє, чи порт прослуховування (відкритий) з'єднаний тристороннім рукостисканням з портом призначення. Якщо порт відкритий, джерело надсилає SYN-пакет як запит, адресат надсилає SYN і ACK-пакет у відповідь, джерело надсилає ACK-пакет, і, нарешті, джерело ще раз надсилає RST і ACK-пакет.

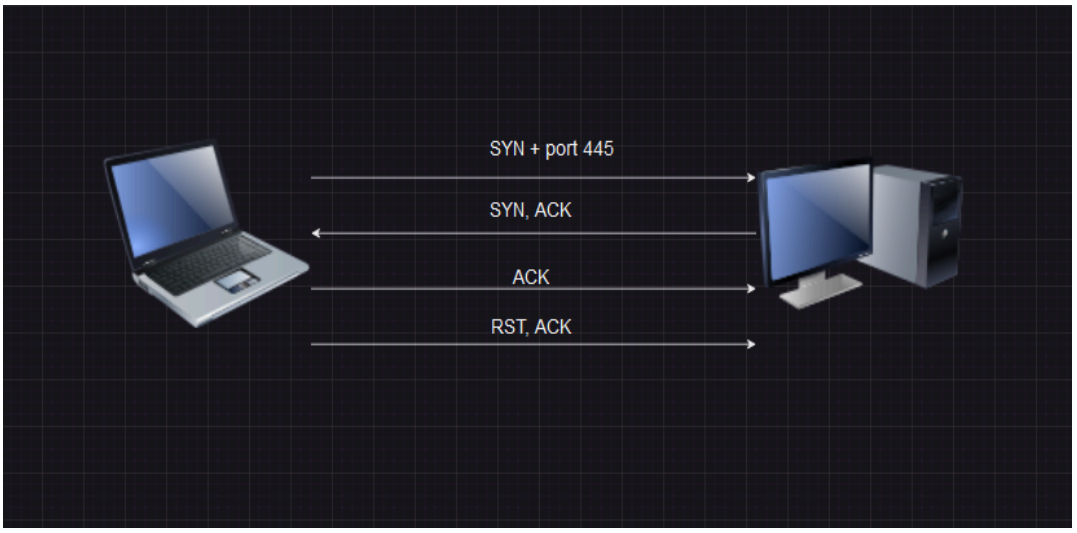


Рис 3.1.13 – Схема роботи сканування SYN

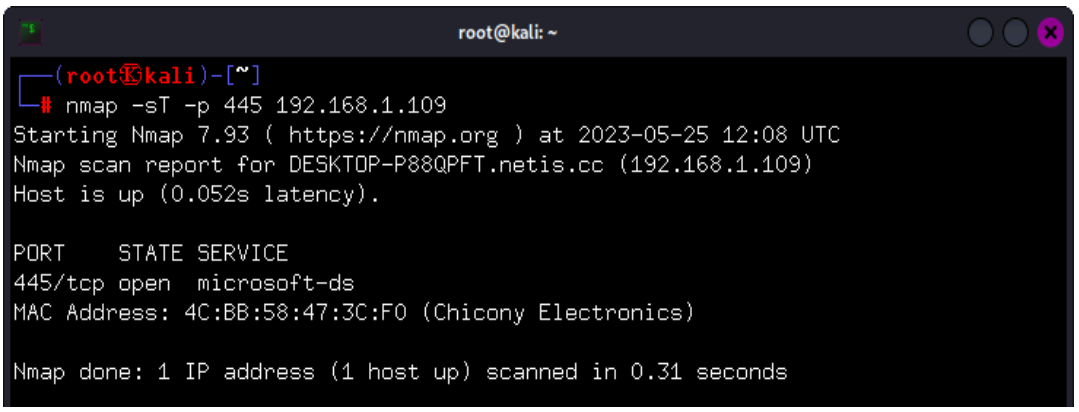


Рис 3.1.14. – Сканування порта 445

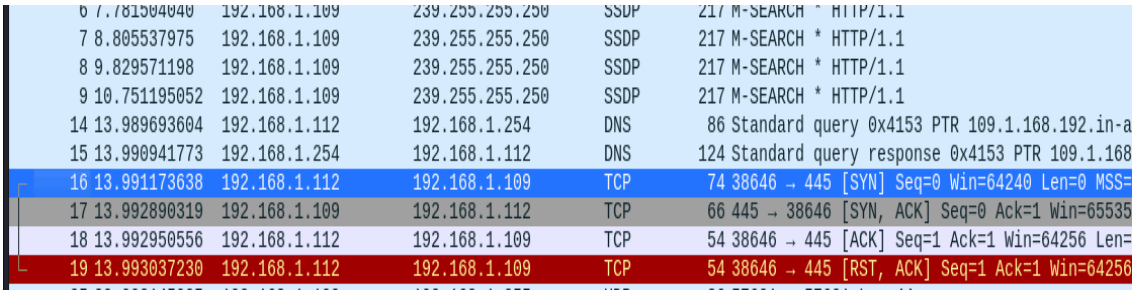


Рис 3.1.15. – Послідовність передачі пакетів у 445 порт в Wireshark

- **Сканування TCP для порта який фільтрується**

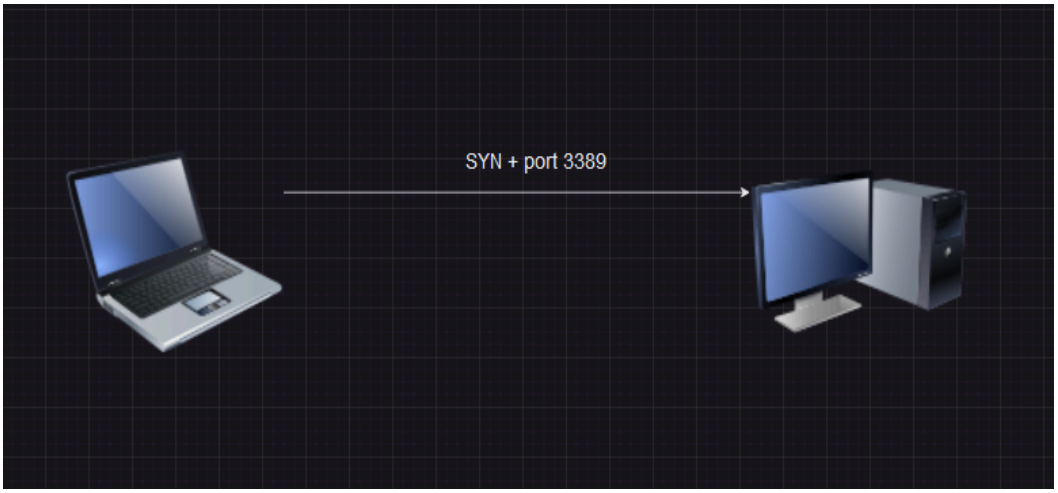


Рис 3.1.17 – Схема роботи сканування SYN

```
┌──(root㉿kali)-[~]
└─# nmap -sT -p 3389 192.168.1.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-25 12:12 UTC
Nmap scan report for DESKTOP-P88QPFT.netis.cc (192.168.1.109)
Host is up (0.097s latency).

PORT     STATE    SERVICE
3389/tcp filtered ms-wbt-server
MAC Address: 4C:BB:58:47:3C:F0 (Chicony Electronics)

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds
```

Рис 3.1.16. – Сканування порта 3389

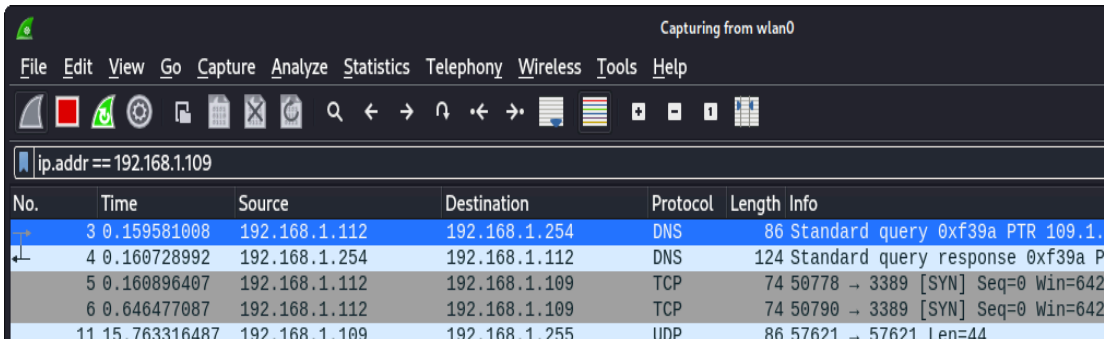


Рис 3.1.17. – Передачі пакетів у 3389 порт в Wireshark

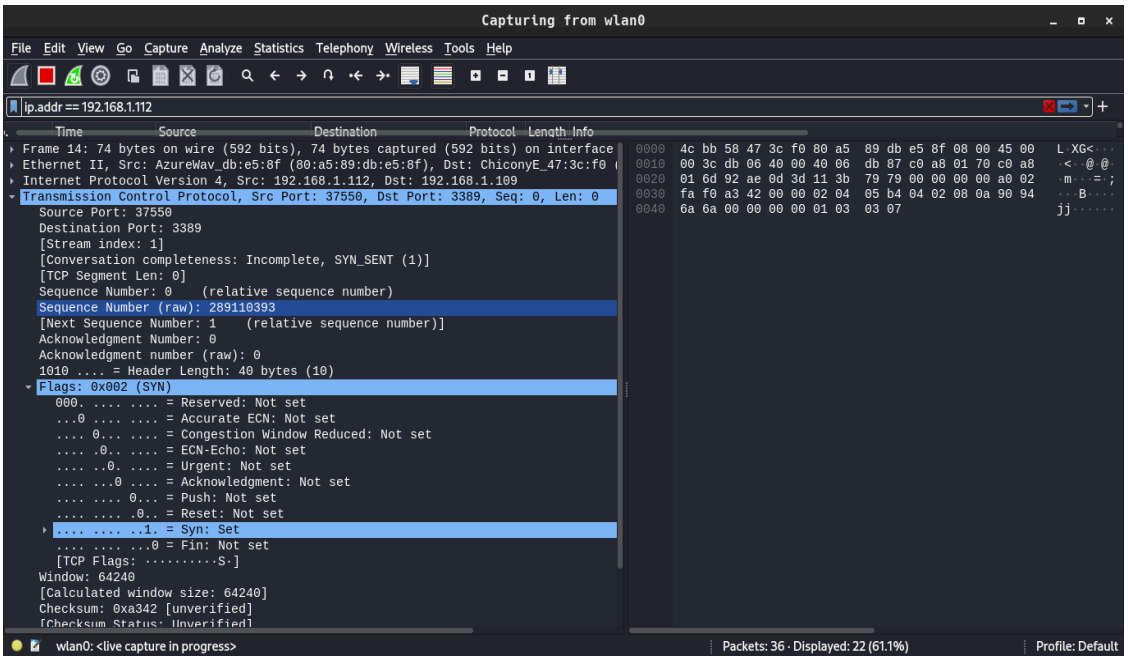


Рис 3.1.18. – Аналіз

Можна побачити, що відповіді немає, так як порт фільтрується і Nmap не може його визначити.

- **Сканування Stealth для порта який фільтрується**

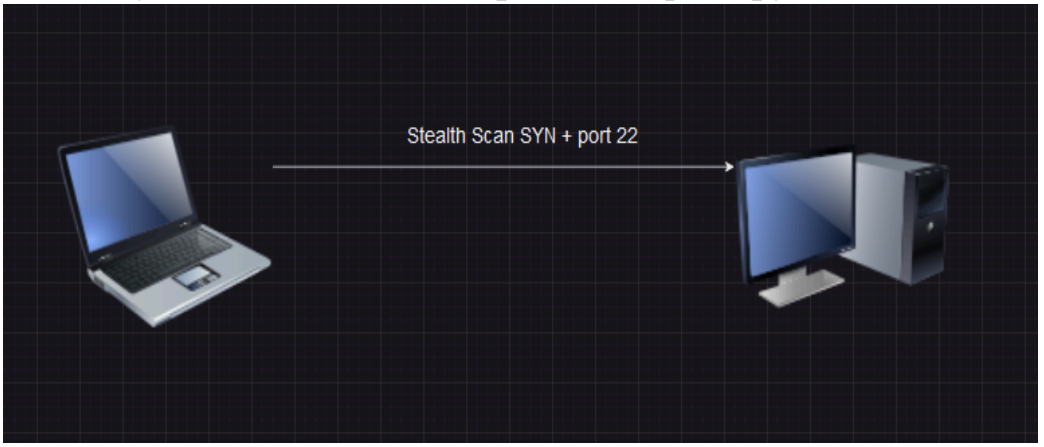


Рис 3.1.19 – Схема роботи сканування Stealth для 22 порта

```
┌──(root㉿kali)-[~]
└─# nmap -sS -p 22 192.168.1.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-25 12:20 UTC
Nmap scan report for DESKTOP-P88QPFT.netis.cc (192.168.1.109)
Host is up (0.075s latency).

PORT   STATE    SERVICE
22/tcp filtered ssh
MAC Address: 4C:BB:58:47:3C:F0 (Chicony Electronics)

Nmap done: 1 IP address (1 host up) scanned in 1.11 seconds
```

Рис 3.1.20. – Stealth сканування порта 22

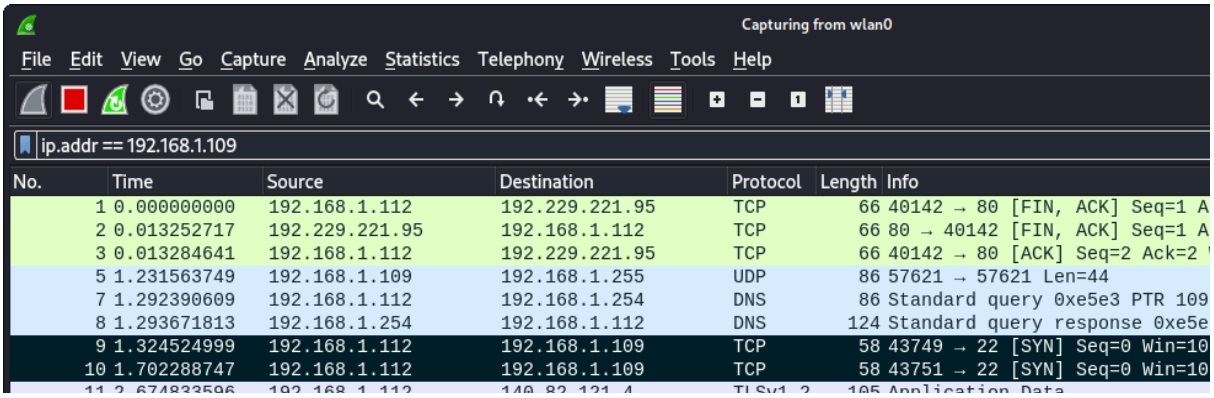


Рис 3.1.21. – Передача пакетів у 22 порт з Stealth сканування Wireshark

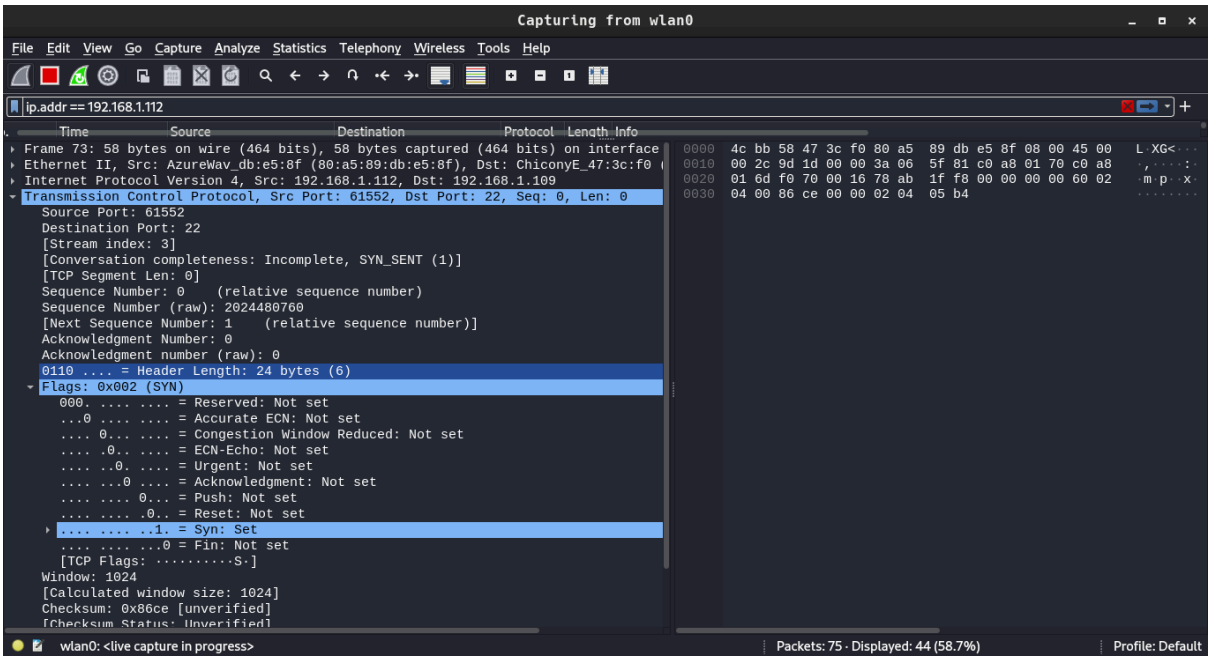


Рис 3.1.22. – Аналіз

Рис 3.1.23 – Схема роботи сканування Stealth для 3389 порта

```
┌──(root㉿kali)-[~]
└─# nmap -sS -p 3389 142.250.203.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-25 12:29 UTC
Nmap scan report for waw07s06-in-f3.1e100.net (142.250.203.131)
Host is up (0.015s latency).

PORT     STATE    SERVICE
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
```

Рис 3.1.24. – Stealth сканування для порта 3389

6	0.015463461	142.250.203.131	192.168.1.112	TCP	58 443 → 42146 [SYN, ACK] Seq
7	0.015482565	192.168.1.112	142.250.203.131	TCP	54 42146 → 443 [RST] Seq=1 Wi
8	0.015504796	142.250.203.131	192.168.1.112	TCP	54 80 → 42146 [RST] Seq=1 Win
9	0.067638692	192.168.1.112	192.168.1.254	DNS	88 Standard query 0x86c7 PTR
10	0.069211641	192.168.1.254	192.168.1.112	DNS	126 Standard query response 0x
11	0.099637188	192.168.1.112	142.250.203.131	TCP	58 42402 → 3389 [SYN] Seq=0 W
12	0.199866669	192.168.1.112	142.250.203.131	TCP	58 42404 → 3389 [SYN] Seq=0 W
17	5.502798364	192.168.1.109	192.168.1.255	UDP	86 57621 → 57621 Len=44

Рис 3.1.25. – Передача пакетів у 3389 порт з Stealth сканування Wireshark

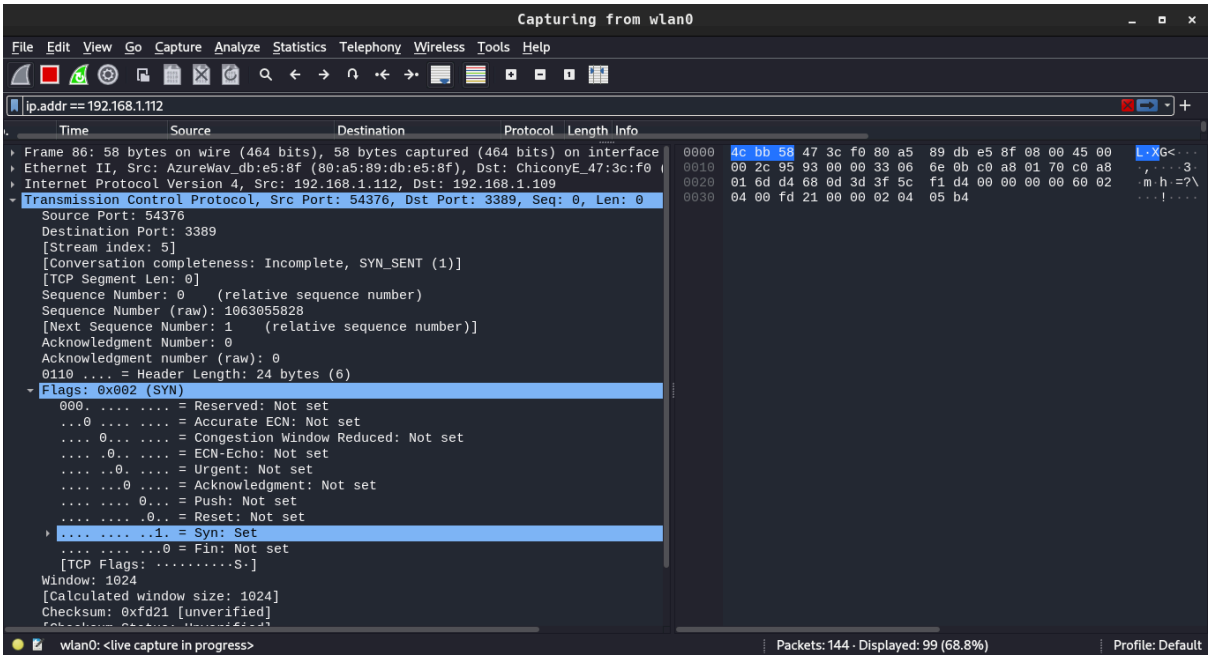


Рис 3.1.26. – Аналіз

- **Сканування FIN**

Після завершення передачі даних зазвичай використовується FIN-пакет для завершення TCP-з'єднання між портом-джерелом і портом-призначенням. Nmap запускає FIN-сканування, використовуючи FIN-пакет замість SYN-пакета. Якщо порт відкритий, надсилання FIN-пакета через порт-джерело не призведе до отримання відповіді від порту-приймача.

Рис 3.1.27. – Схема FIN сканування для порта 22

```
┌──(root㉿kali)-[~]
└─# nmap -sF -p 22 192.168.1.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-25 12:31 UTC
Nmap scan report for DESKTOP-P88QPFT.netis.cc (192.168.1.109)
Host is up (0.10s latency).

PORT   STATE         SERVICE
22/tcp open|filtered ssh
MAC Address: 4C:BB:58:47:3C:F0 (Chicony Electronics)

Nmap done: 1 IP address (1 host up) scanned in 1.43 seconds
```

Рис 3.1.28. – FIN сканування для порта 22

1	0.000000000	192.168.1.109	192.168.1.255	UDP	86	57621 → 57621 Len=44
5	1.090375519	192.168.1.112	192.168.1.254	DNS	86	Standard query 0x649b PTR 109.1.168.192.in-ad
6	1.091575716	192.168.1.254	192.168.1.112	DNS	124	Standard query response 0x649b PTR 109.1.168.
7	1.122427636	192.168.1.112	192.168.1.109	TCP	54	44299 → 3389 [FIN] Seq=1 Win=1024 Len=0
10	1.689869612	192.168.1.112	192.168.1.109	TCP	54	44301 → 3389 [FIN] Seq=1 Win=1024 Len=0
11	2.969521330	192.168.1.109	192.168.1.255	UDP	86	57621 → 57621 Len=44
12	28.512765749	192.168.1.109	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _spotify-connect._t

Рис 3.1.29. – Передача пакетів у 22 порт з FIN сканування Wireshark

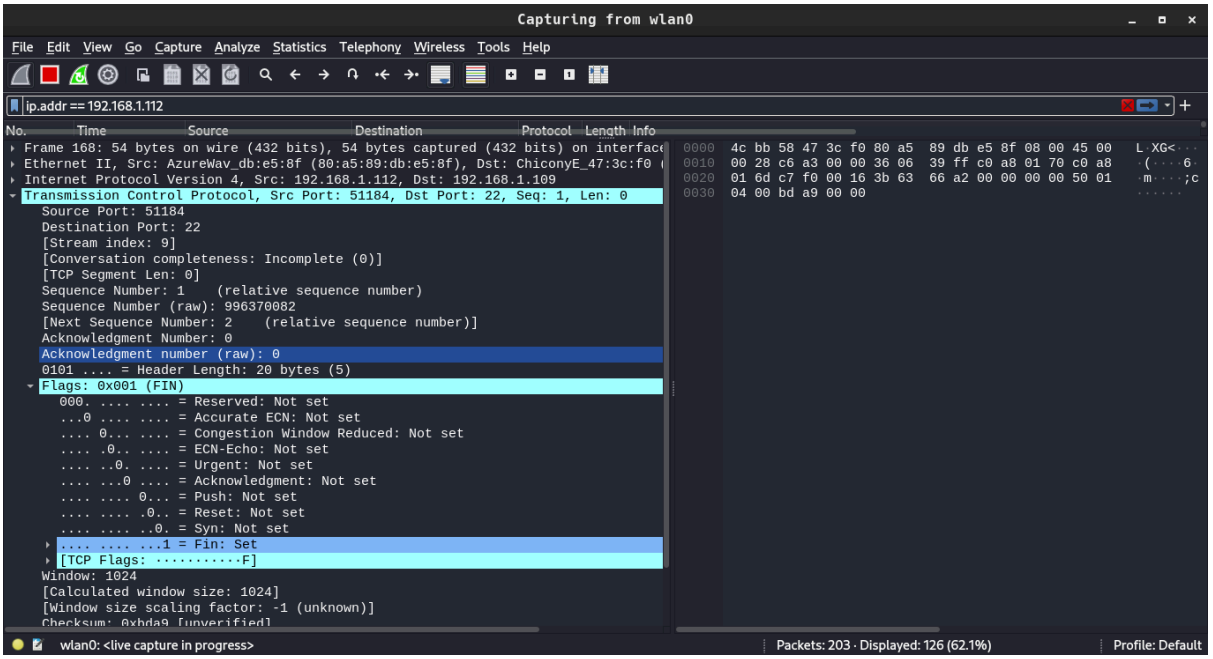


Рис 3.1.130. – Аналіз

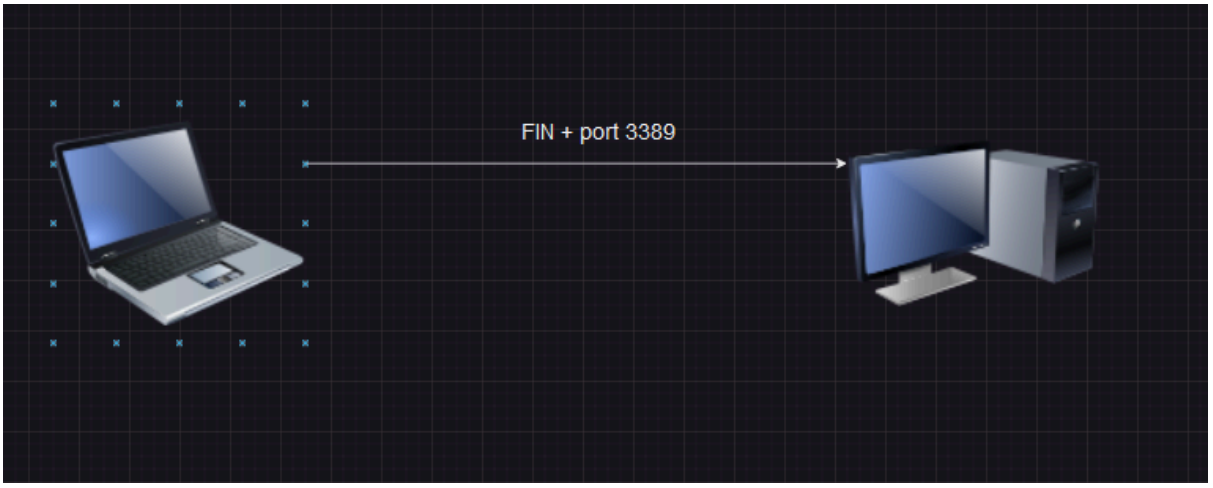


Рис 3.1.31. – FIN сканування для порта 3389

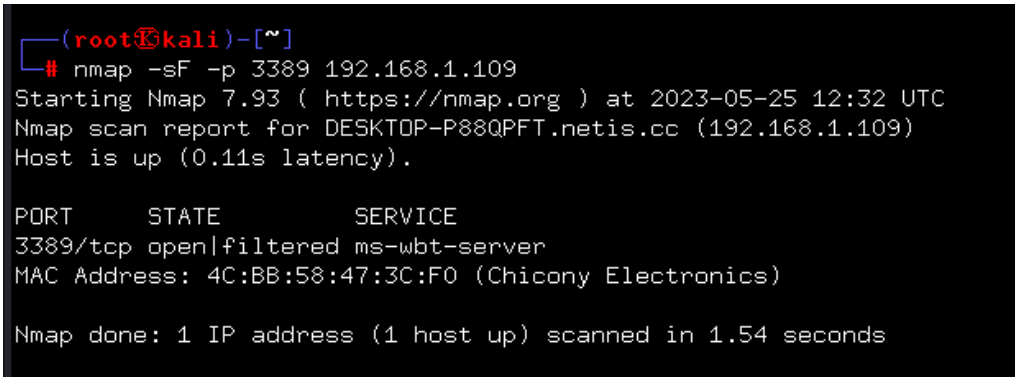


Рис 3.1.32. – FIN сканування для порта 22

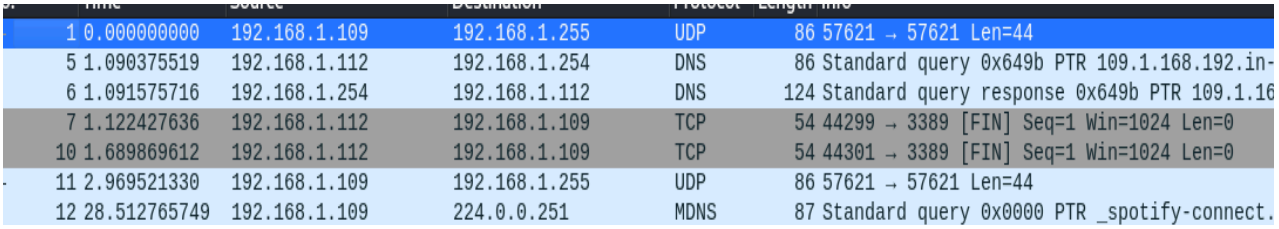


Рис 3.1.33. – Передача пакетів у 3389 порт з FIN сканування Wireshark

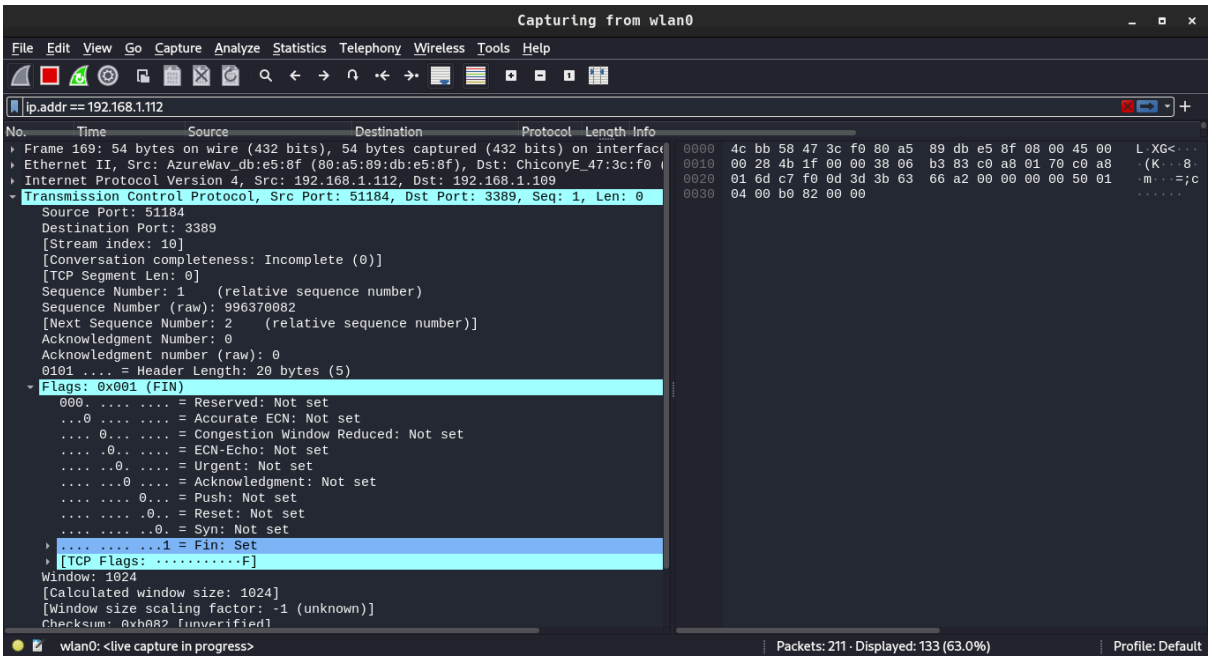


Рис 3.1.34. – Аналіз

- Нульове сканування (NULL Scan)

Нульове сканування — це серія TCP-пакетів, які містять порядковий номер «нулі» (0000000), і оскільки не встановлено жодного прапора, адресат не знатиме, як відповісти на запит. Пакет буде відхилено, і відповідь не буде надіслана, що означає, що порт відкрито.

Рис 3.1.35 – Схема Null Scan для порта 22

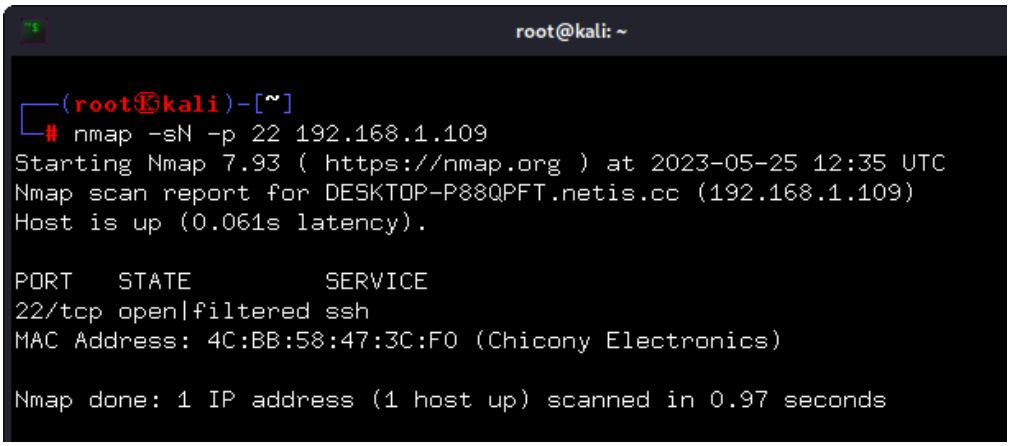


Рис 3.1.36. – Сканування порта 22 за допомогою NULL Scan

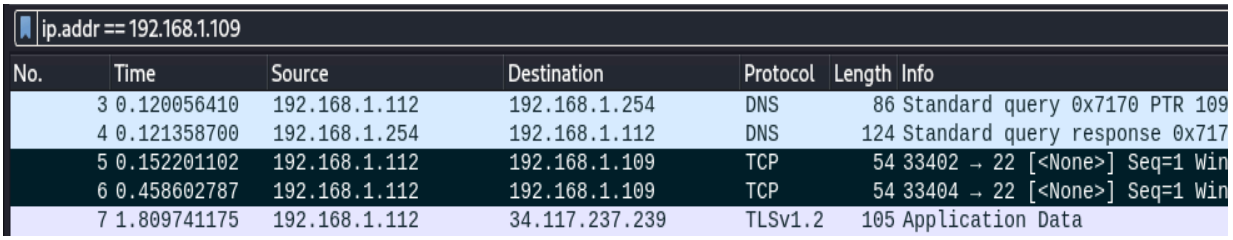


Рис 3.1.37. – Передача пакетів у 22 порт з NULL Scan сканування Wireshark

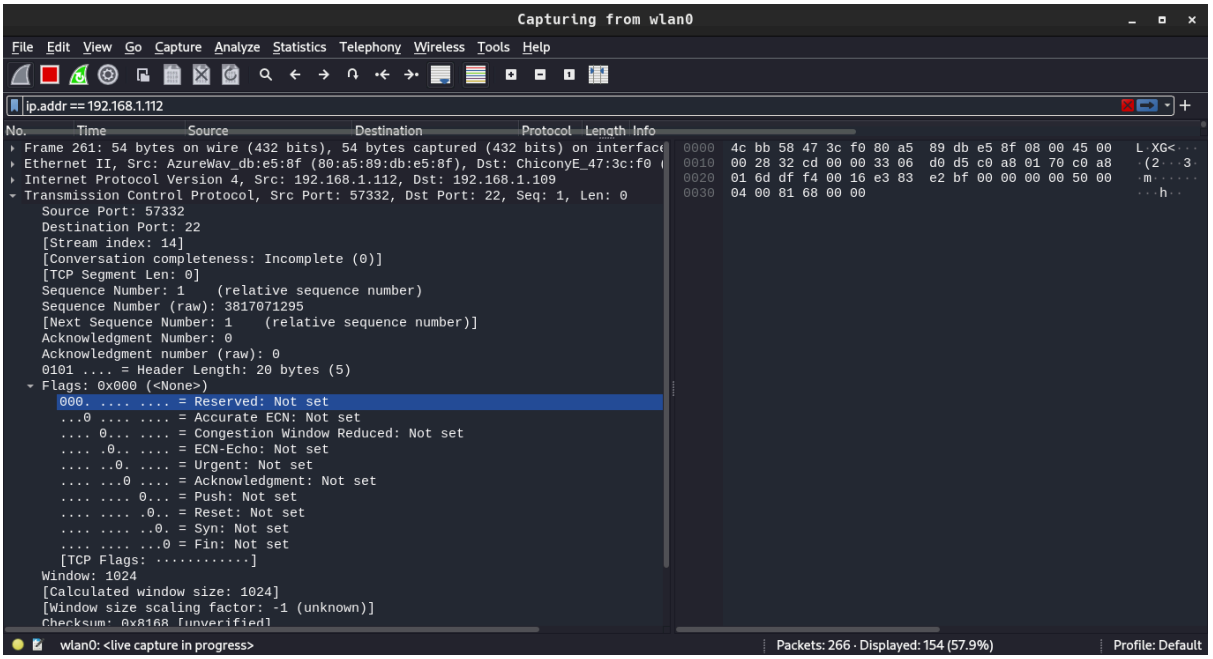


Рис 3.1.38. – Аналіз

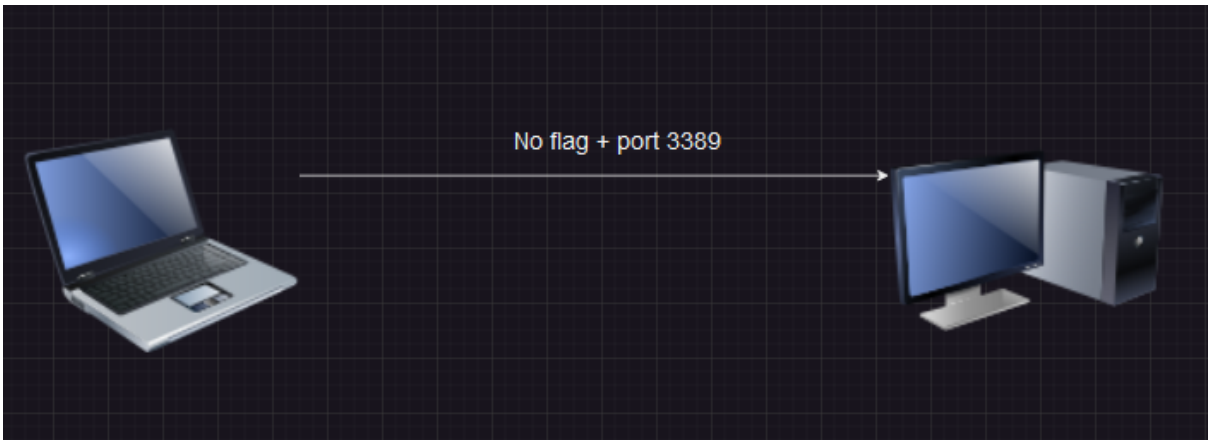


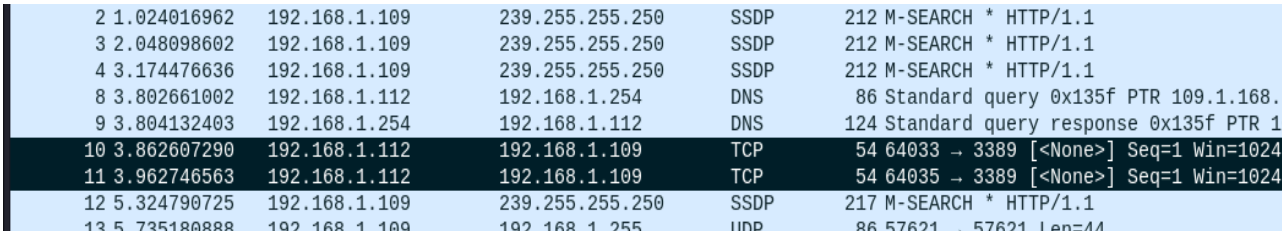
Рис 3.1.39 – Схема Null Scan для порта 3389

```
┌──(root㉿kali)-[~]
└─# nmap -sN -p 3389 192.168.1.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-25 12:34 UTC
Nmap scan report for DESKTOP-P88QPFT.netis.cc (192.168.1.109)
Host is up (0.0051s latency).

PORT     STATE         SERVICE
3389/tcp open|filtered ms-wbt-server
MAC Address: 4C:BB:58:47:3C:F0 (Chicony Electronics)

Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds
```

Рис 3.1.40. – Сканування порта 3389 за допомогою NULL Scan



2	1.024016962	192.168.1.109	239.255.255.250	SSDP	212 M-SEARCH * HTTP/1.1
3	2.048098602	192.168.1.109	239.255.255.250	SSDP	212 M-SEARCH * HTTP/1.1
4	3.174476636	192.168.1.109	239.255.255.250	SSDP	212 M-SEARCH * HTTP/1.1
8	3.802661002	192.168.1.112	192.168.1.254	DNS	86 Standard query 0x135f PTR 109.1.168.
9	3.804132403	192.168.1.254	192.168.1.112	DNS	124 Standard query response 0x135f PTR 1
10	3.862607290	192.168.1.112	192.168.1.109	TCP	54 64033 → 3389 [<None>] Seq=1 Win=1024
11	3.962746563	192.168.1.112	192.168.1.109	TCP	54 64035 → 3389 [<None>] Seq=1 Win=1024
12	5.324790725	192.168.1.109	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
13	5.735180888	192.168.1.109	192.168.1.255	UDP	86 57621 → 57621 Len=44

Рис 3.1.41. – Передача пакетів у 3389 порт з NULL Scan сканування Wireshark

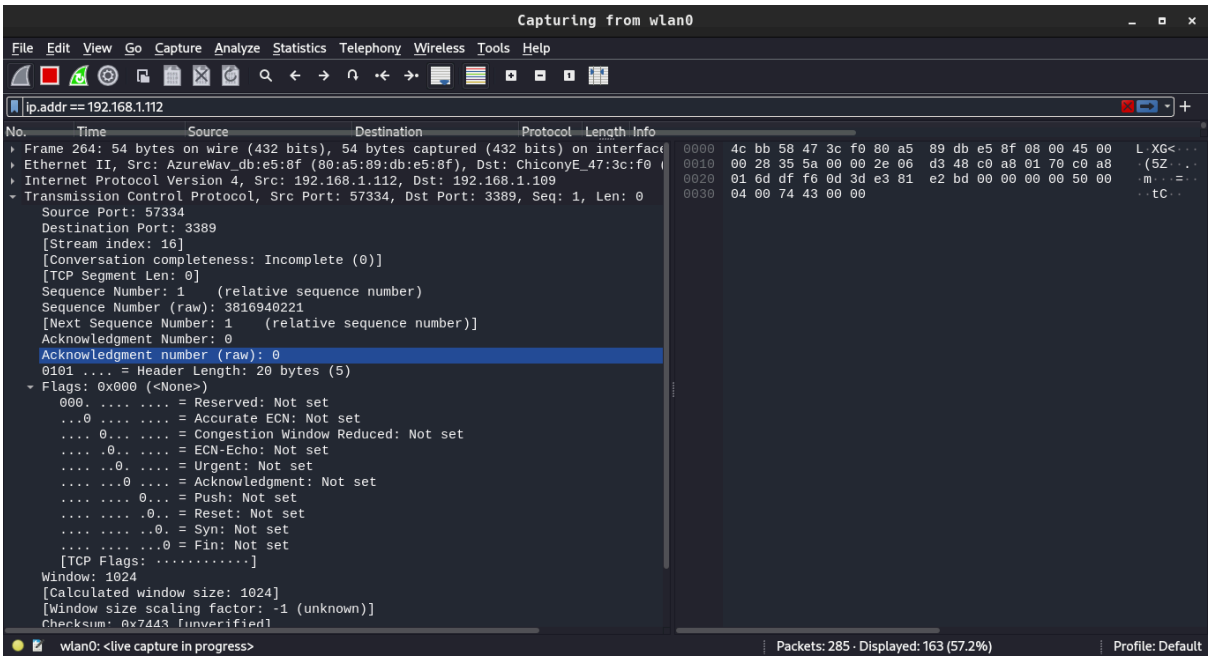


Рис 3.1.45. – Аналіз

- **Сканування XMAS**

Ці сканування призначені для маніпулювання прапорами PSH, URG і FIN заголовка TCP. Встановлює прапори FIN, PSH і URG, освітлюючи пакет, як новорічну ялинку. Якщо джерело надсилає пакети FIN, PUSH і URG на певний порт і якщо порт відкритий, адресат відхиляє пакети та не надсилає жодної відповіді джерелу.

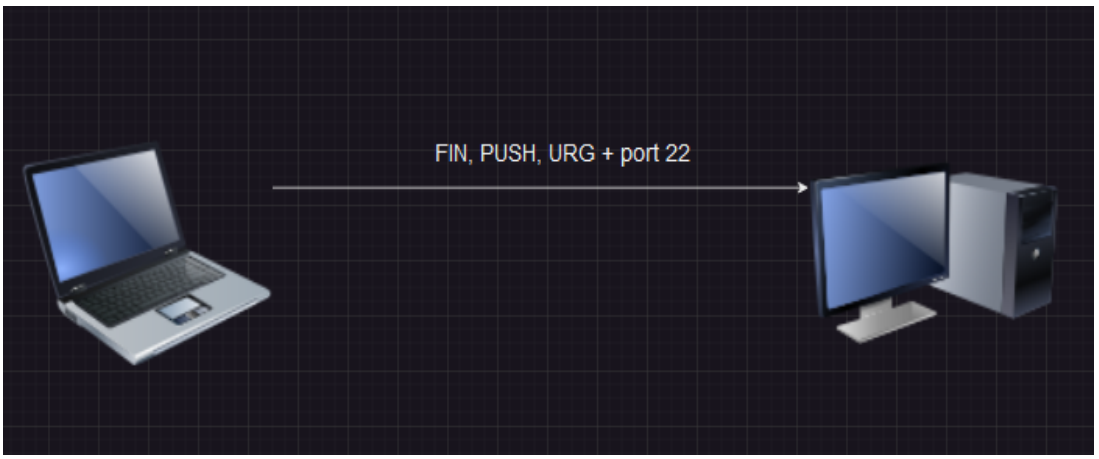


Рис 3.1.46 – Схема XMAS сканування для порта 22

```
┌──(root㉿kali)-[~]
└─# nmap -sX -p 22 192.168.1.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-25 12:40 UTC
Nmap scan report for DESKTOP-P88QPFT.netis.cc (192.168.1.109)
Host is up (0.076s latency).

PORT   STATE         SERVICE
22/tcp open|filtered ssh
MAC Address: 4C:BB:58:47:3C:F0 (Chicony Electronics)

Nmap done: 1 IP address (1 host up) scanned in 1.13 seconds
```

Рис 3.1.47 – XMAS сканування для порта 22

7	3.126978341	192.168.1.109	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1
10	4.621809354	192.168.1.112	192.168.1.254	DNS	86 Standard query 0x7515 PTR 109.1.168.192
11	4.623069691	192.168.1.254	192.168.1.112	DNS	124 Standard query response 0x7515 PTR 109.1
12	4.653851919	192.168.1.112	192.168.1.109	TCP	54 50433 → 22 [FIN, PSH, URG] Seq=1 Win=10
13	5.036625539	192.168.1.112	192.168.1.109	TCP	54 50435 → 22 [FIN, PSH, URG] Seq=1 Win=10
14	7.273845301	192.168.1.101	224.0.0.251	MDNS	103 Standard query 0x000c PTR _37F83649._sub
15	9.479058297	192.168.1.109	192.168.1.255	UDP	86 57621 → 57621 Len=44

Рис 3.1.48. – Передача пакетів у 22 порт з XMAS сканування Wireshark

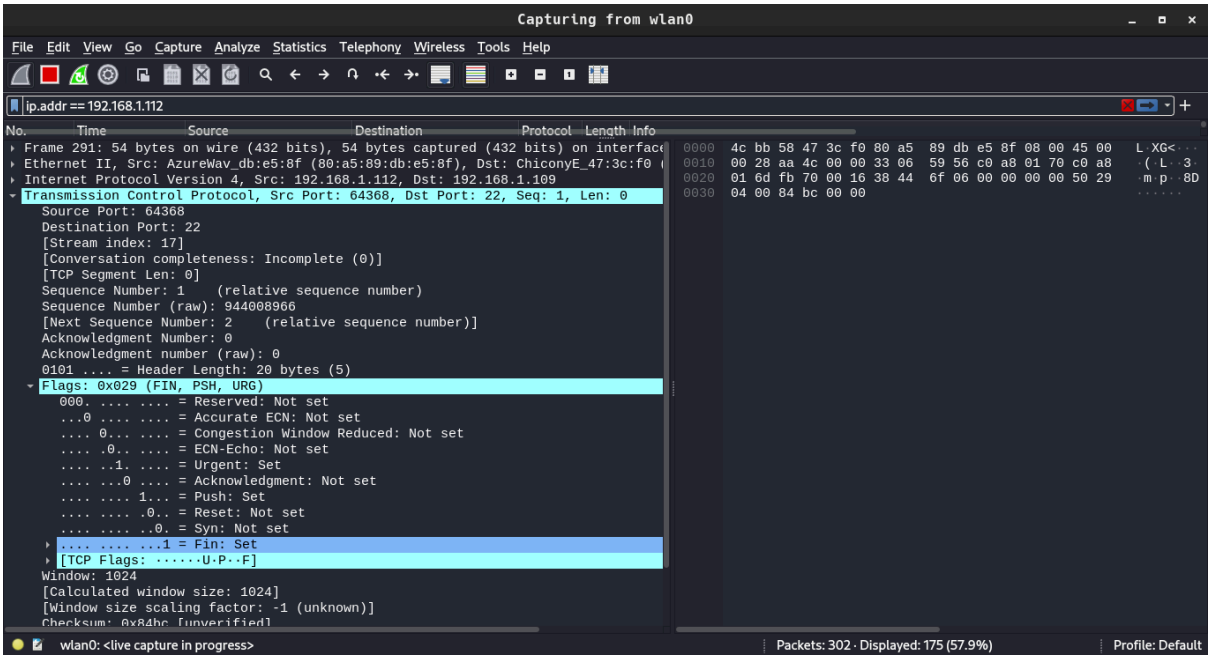


Рис 3.1.49. – Аналіз

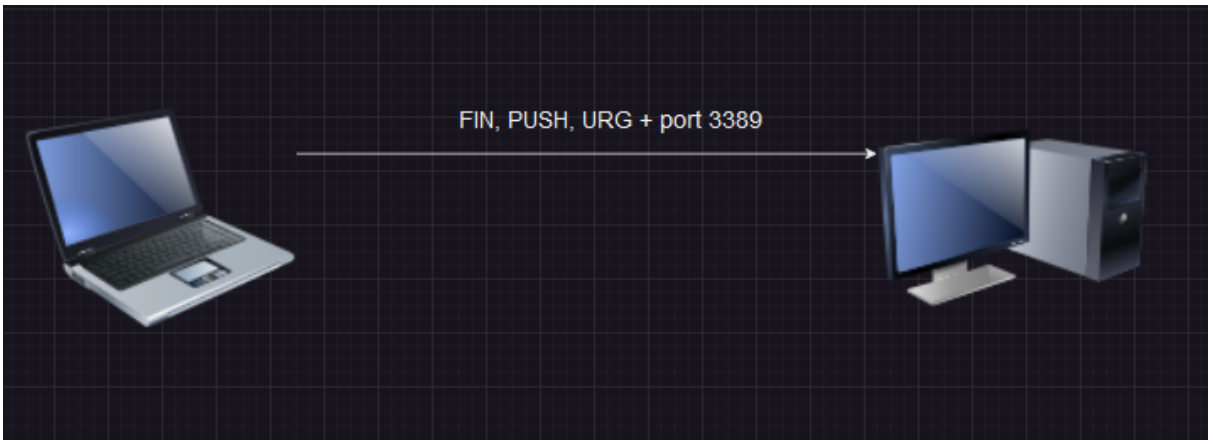


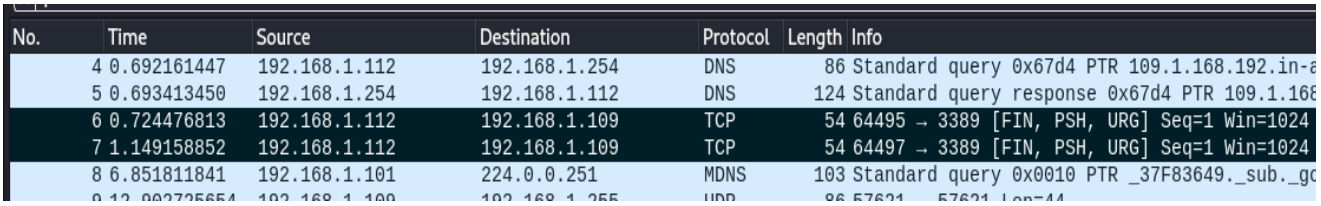
Рис 3.1.50. – XMAS сканування для порта 3389

```
┌──(root㉿kali)-[~]
└─# nmap -sX -p 3389 192.168.1.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-25 12:41 UTC
Nmap scan report for DESKTOP-P88QPFT.netis.cc (192.168.1.109)
Host is up (0.085s latency).

PORT     STATE         SERVICE
3389/tcp open|filtered ms-wbt-server
MAC Address: 4C:BB:58:47:3C:F0 (Chicony Electronics)

Nmap done: 1 IP address (1 host up) scanned in 1.21 seconds
```

Рис 3.1.51. – XMAS сканування для порта 22



No.	Time	Source	Destination	Protocol	Length	Info
4	0.692161447	192.168.1.112	192.168.1.254	DNS	86	Standard query 0x67d4 PTR 109.1.168.192.in-a
5	0.693413450	192.168.1.254	192.168.1.112	DNS	124	Standard query response 0x67d4 PTR 109.1.168
6	0.724476813	192.168.1.112	192.168.1.109	TCP	54	64495 → 3389 [FIN, PSH, URG] Seq=1 Win=1024
7	1.149158852	192.168.1.112	192.168.1.109	TCP	54	64497 → 3389 [FIN, PSH, URG] Seq=1 Win=1024
8	6.851811841	192.168.1.101	224.0.0.251	MDNS	103	Standard query 0x0010 PTR _37F83649._sub._g

Рис 3.1.52. – Передача пакетів у 3389 порт з XMAS сканування Wireshark

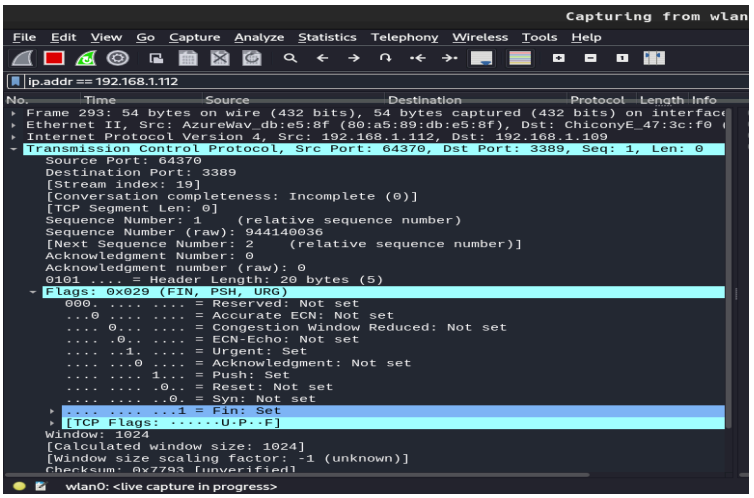


Рис 3.1.53. – Аналіз

- **Metasploit**

SMB – це протокол, який став мішенню для кількох вразливостей протягом багатьох років. SMBLoris - це віддалена неавторизована DoS-атака на операційні системи Microsoft Windows систем Microsoft Windows. Ця атака споживає великі обсяги пам'яті на цільовій машині, надсилаючи SMB-запити з максимально можливим значенням заголовку NetBios Session Service (NBSS) Length Header. Впливаючи на всі сучасні версії Windows, починаючи з Windows 2000 і закінчуючи Windows 10, ця атака може призвести до недоступності критично важливих для бізнесу сервісів.

Перед запуском msfconsole і використанням auxiliary модуля SMBLoris NBSS Denial of Service1 ми повинні змінити ліміт на відкриті файли в нашій системі. Для цього ми можемо скористатися командою ulimit з опцією -n для відкритих файлів і встановити її на 99999. Потім завантажте модуль в msfconsole, встановіть IP-адресу цілі і виконати атаку:

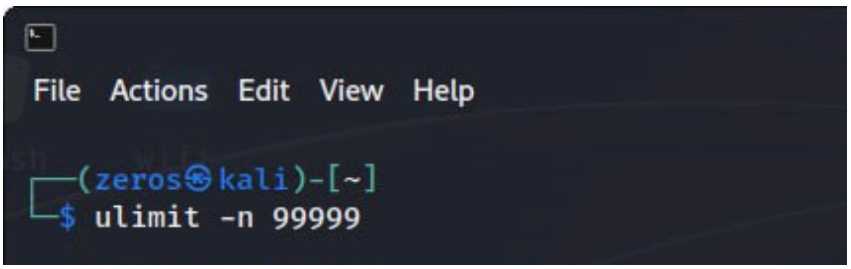


Рис 3.1.54. – Зміна ліміту

Далі я запускаю Metasploit:

Рис 3.1.55. – Запуск

Потім я вже обираю модуль з яким я буду працювати:

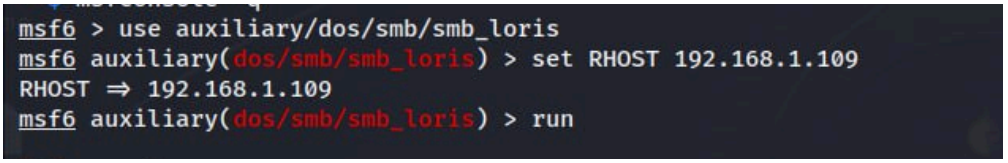


Рис 3.1.56. – Обирання модуля

На рис 3.1.43. можно побачити **‘set RHOST’ –** параметр RHOST у Metasploit відноситься до віддаленого Host, тобто цільову IP-адресу або ім'я хоста системи, яку ви хочете атакувати або перевірити на вразливості. Це важливий параметр, який використовується в різних модулях та експлоітах Metasploit для вказівки цільової систему.

Run – це запуск.

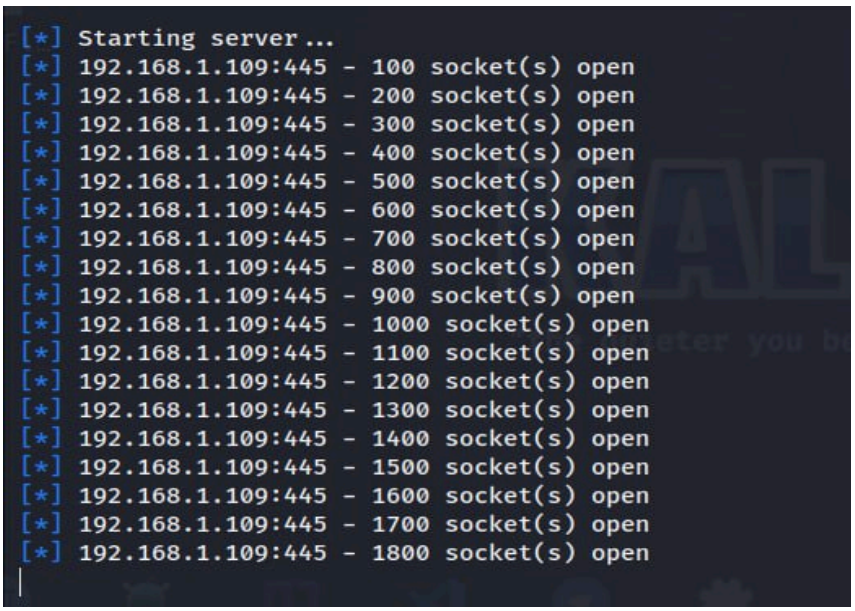


Рис 3.1.57. – Робота

Далі я переходжу до Task Manager, натискаю на Perfomance, обираю Memory:

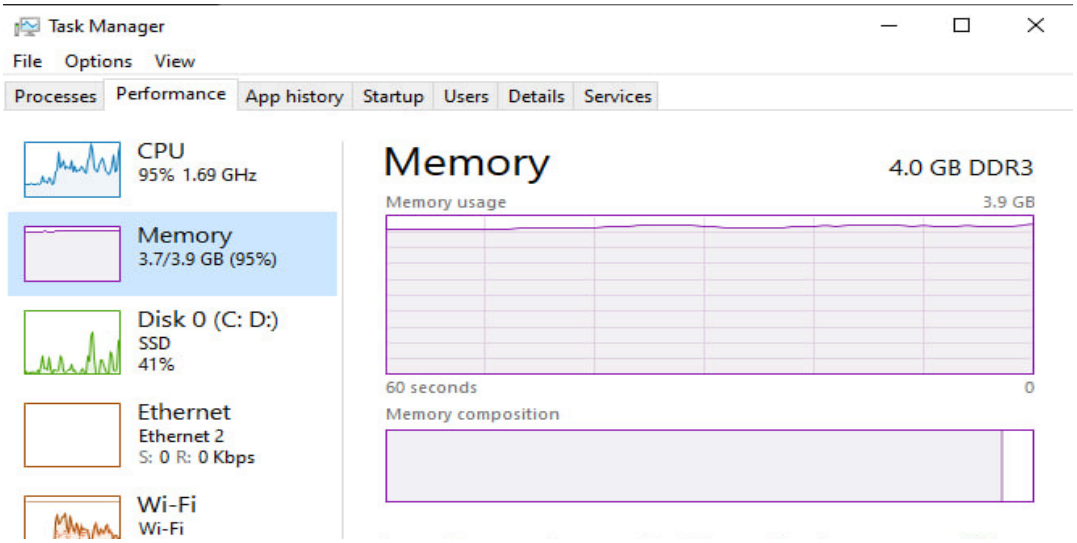


Рис 3.1.58. – Робота ОЗУ

Metasploit і Nmap для пошуку вразливостей:

Для того щоб я почав робити сканування, мені потрібно запустити Metsplopit:

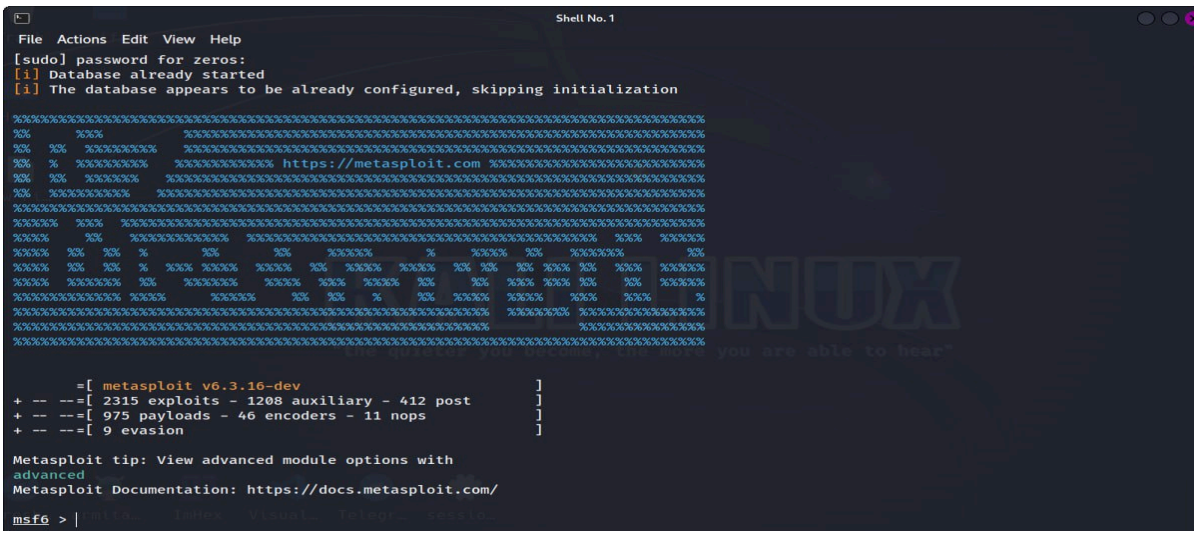


Рис 3.1.59. – Metasploit

Далі я прописую **use auxiliary/scanner/portscan/tcp,** для того щоб запустити модуль сканера портів.

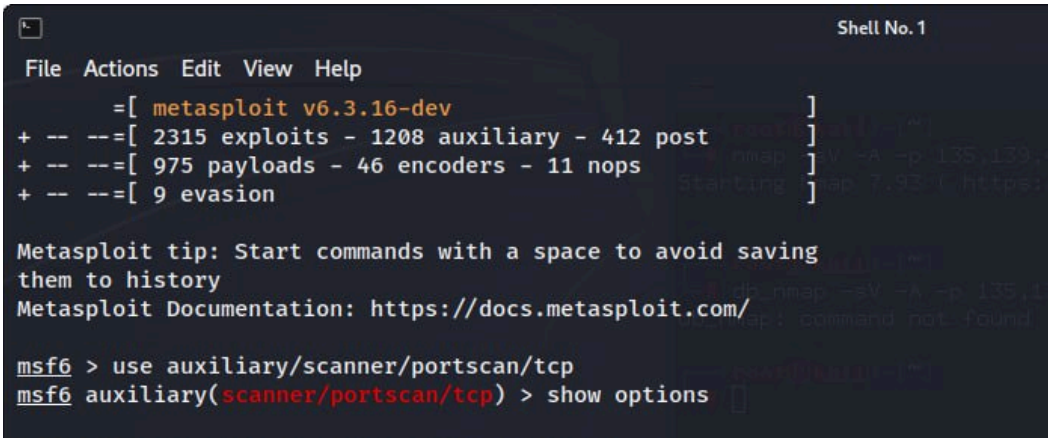


Рис 3.1.60. – Запуск модуля

Команда show options показує, що ще треба прописати для того щоб з цім працювати:

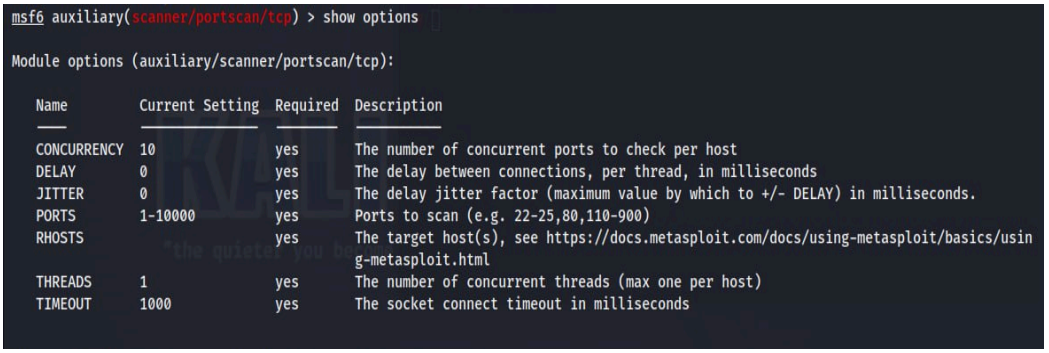


Рис 3.1.61. – Опції модуля

далі я прописую адресу своєї машини у **RHOST** (192.168.1.109).

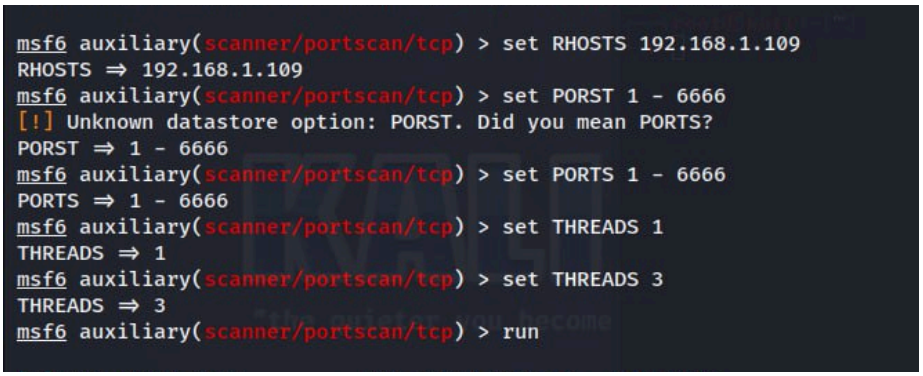


Рис 3.1.62. – Настройка модуля

Далі я прописую set PORTS 1 – 6666, це діапазон сканування портів, тобто воно буде сканувати всі порти від 1 до 6666.

Команда set THREADS – це кількість одночасних потоків на сканування.

Run – запуск.

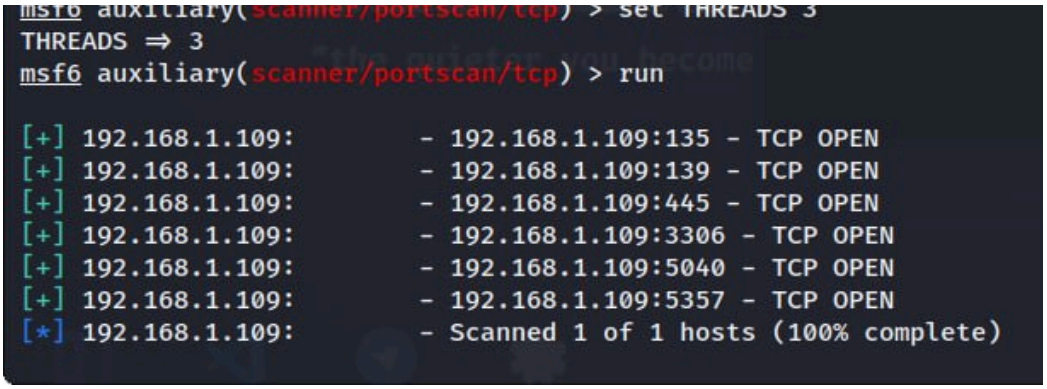


Рис 3.1.63. – Результат сканування

Як сканування закінчилось, я можу побачити, що порти 135, 139, 445, 3306, 5040, 5357 – відкриті.

За що відповідають ці порти:

- Порт 135 - Зв'язок клієнт-сервер RPC.
- Порт 139 - Сервіс сеансів NetBIOS
- Порт 445 - Служби каталогів Microsoft для Active Directory (AD) і для протоколу Server Message Block (SMB) через TCP/IP.
- Порт 3306 – MySQL протокол
- Порт 5040 - Слухач RPC для сервера Windows Deployment Services
- Порт 5357 - Використовується Microsoft Network Discovery

Після цього коли закінчилось сканування, я прописую команду db_nmap -sV -A -p 135, 139, 445, 3306, 5040, 5357 192.168.1.109, де:

- **-sV:** Ця опція дозволяє визначити версію служби. У разі використання Nmap намагається визначити версію та відповідну інформацію про служби, що працюють у цільовій системі. Він надсилає спеціальні зонди та аналізує відповіді, щоб ідентифікувати службу та номер її версії. Це може надати цінну інформацію для оцінки вразливості та визначення конкретних версій програмного забезпечення, що використовуються.

- **-A:** Цей параметр дозволяє агресивне сканування, яке включає в себе комбінацію передових методів для збору додаткової інформації про цільову систему. Він включає різні сценарії, визначення версій, виявлення ОС, сканування сценаріїв і traceroute. Агресивне сканування може забезпечити більш повне уявлення про цільову систему, але також може бути більш нав’язливим і ресурсомістким.

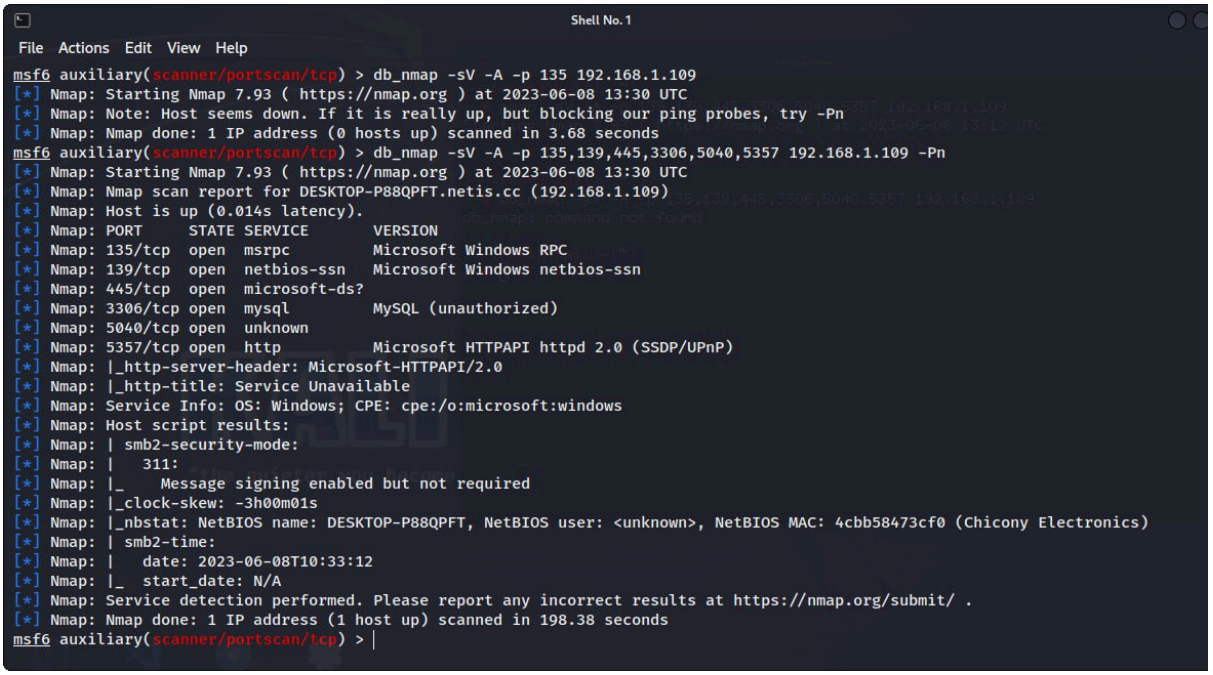


Рис 3.1.64. – Аналіз сканування

3.2. Пропозиції щодо підвищення рівня захищеності інформаційної системи

Підвищення рівня безпеки інформаційної системи має вирішальне значення для захисту конфіденційних даних і запобігання несанкціонованому доступу або порушенням. Ось кілька пропозицій щодо підвищення рівня безпеки:

- Впровадити надійну автентифікацію: Забезпечити використання надійних та унікальних паролів для облікових записів користувачів. Розгляньте можливість впровадження двофакторної автентифікації (2FA) або багатофакторної автентифікації (MFA), щоб додати додатковий рівень безпеки.

- Регулярне оновлення та виправлення системи: Оновлюйте все програмне забезпечення, операційні системи та додатки найновішими виправленнями та оновленнями безпеки. Вразливості в застарілому програмному забезпеченні можуть бути використані зловмисниками.

- Регулярно проводьте оцінку вразливостей і тестування на проникнення: Виконуйте регулярні оцінки безпеки, включаючи сканування вразливостей і тестування на проникнення, щоб виявити і усунути потенційні слабкі місця в системі.

- Впровадити брандмауер та системи виявлення/попередження вторгнень: Використовуйте брандмауери для контролю вхідного та вихідного трафіку та встановіть системи виявлення та запобігання вторгнень (IDS/IPS) для моніторингу мережевого трафіку та виявлення зловмисних дій.

- Використовуйте надійне шифрування: Переконайтеся, що конфіденційні дані зашифровані як під час передачі, так і в стані спокою. Використовуйте надійні алгоритми та протоколи шифрування для захисту цілісності та конфіденційності даних.

- Впроваджуйте контроль доступу: Застосовуйте принцип найменших привілеїв (PoLP), надаючи користувачам мінімальний рівень доступу, необхідний для виконання їхніх завдань. Впровадьте контроль доступу на основі ролей (RBAC) і регулярно переглядайте дозволи користувачів.

- Проводьте тренінги з підвищення обізнаності про безпеку: Розкажіть працівникам про найкращі практики безпеки, зокрема про гігієну паролів, виявлення спроб фішингу та безпечний перегляд веб-сторінок. Регулярні тренінги допоможуть запобігти людським помилкам і підвищити загальну обізнаність про безпеку.

- Відстежуйте та реєструйте дії: Впроваджуйте централізовані рішення для реєстрації та моніторингу, щоб відстежувати системні дії, виявляти підозрілу поведінку та своєчасно реагувати на інциденти безпеки.

- Регулярне резервне копіювання даних та планування аварійного відновлення: Створіть надійну стратегію резервного копіювання даних і протестуйте процес відновлення. Розробіть комплексний план аварійного відновлення, щоб мінімізувати вплив потенційних інцидентів безпеки або системних збоїв.

- Будьте в курсі загроз безпеці: Будьте в курсі останніх загроз безпеці, вразливостей та нових технологій. Регулярно відстежуйте рекомендації з безпеки, новини галузі та беріть участь у відповідних форумах і спільнотах.

Пам'ятайте, що безпека - це безперервний процес, який вимагає постійних зусиль і проактивних заходів для адаптації до нових загроз. Рекомендується проконсультуватися з фахівцями або експертами з безпеки, щоб адаптувати ці пропозиції до конкретних потреб вашої інформаційної системи та організації.

Розділ 4. Використання інструментів Kali Linux для виявлення вразливостей інформаційної системи

Kali Linux - це потужний і широко визнаний дистрибутив Linux, який здобув популярність серед фахівців з безпеки, тестувальників проникнення та етичних хакерів. Він спеціально розроблений для забезпечення комплексної платформи для проведення оцінки безпеки, тестування вразливостей, цифрової криміналістики та інших пов'язаних завдань.

Однією з ключових особливостей Kali Linux є велика колекція попередньо встановлених інструментів. Ці інструменти охоплюють різні аспекти тестування безпеки, включаючи сканування мережі, аналіз вразливостей, безпеку бездротових мереж, злам паролів, тестування веб-додатків, соціальну інженерію та багато іншого. Від популярних інструментів, таких як Nmap, Wireshark і Metasploit, до спеціалізованих утиліт, таких як John the Ripper і Aircrack-ng, Kali Linux пропонує широкий арсенал можливостей для фахівців з безпеки.

Kali Linux надає середовище, що легко налаштовується і дозволяє користувачам конфігурувати свої системи відповідно до їхніх конкретних потреб. Він підтримує кілька середовищ робочого столу, таких як GNOME, KDE, Xfce і багато інших, що дозволяє користувачам вибрати інтерфейс, який відповідає їхнім уподобанням. Ця гнучкість поширюється і на процес встановлення, з можливістю запуску Kali Linux у реальному середовищі з завантажувального USB або DVD, або встановлення її як основної операційної системи на комп'ютері.

На додаток до можливостей тестування на проникнення, Kali Linux також обслуговує сферу цифрової криміналістики та реагування на інциденти. Вона включає в себе інструменти для аналізу образів дисків, відновлення видалених файлів, дослідження мережевого трафіку та проведення криміналістичних розслідувань. Це робить його цінним активом для професіоналів, які працюють у сфері кібербезпеки, правоохоронних органів та інших суміжних галузях.

Спільнота Kali Linux відіграє важливу роль у розробці та підтримці дистрибутива. Офіційний веб-сайт Kali Linux містить вичерпну документацію, навчальні посібники та форуми, де користувачі можуть отримати доступ до інформації, звернутися за допомогою та обмінятися знаннями. Регулярно проводяться оновлення та вдосконалення, щоб гарантувати, що інструменти залишаються актуальними та ефективними в постійно мінливому ландшафті кібербезпеки.

Важливо зазначити, що використання Kali Linux та її інструментів завжди має бути етичним та законним. Несанкціоноване або неетичне використання інструментів може призвести до серйозних наслідків. Важливо отримати належний дозвіл і згоду перед проведенням будь-яких оцінок безпеки або тестування на проникнення в системах або мережах.

Kali Linux, розроблений і підтримуваний Offensive Security, побудований на міцному фундаменті операційної системи Debian. Він включає в себе знання і досвід спеціальної команди професіоналів з безпеки, що гарантує, що він залишається на передньому краї тестування безпеки і етичного хакінгу.

Одним з важливих аспектів Kali Linux є його орієнтація на зручність та доступність. Інтерфейс користувача розроблений таким чином, щоб бути інтуїтивно зрозумілим і зручним для користувача, що дозволяє як досвідченим фахівцям з безпеки, так і початківцям ефективно орієнтуватися і використовувати його функції. Kali Linux також надає обширну документацію та навчальні посібники, що дозволяє користувачам вдосконалювати свої навички та знання в галузі кібербезпеки.

Kali Linux не обмежується однією цільовою платформою. Він підтримує широкий спектр апаратних архітектур, включаючи 32-розрядні, 64-розрядні, ARM і платформи віртуалізації. Ця універсальність дозволяє фахівцям з безпеки використовувати Kali Linux на різних пристроях і середовищах, таких як ноутбуки, настільні комп'ютери, сервери і віртуальні машини.

Репозиторій Kali Linux регулярно поповнюється новими інструментами, гарантуючи, що фахівці з безпеки мають доступ до новітніх технологій і методів виявлення вразливостей та оцінки безпеки системи. Ці оновлення також включають виправлення помилок, покращення продуктивності та сумісності, що робить Kali Linux надійною та стабільною платформою.

Окрім своїх технічних можливостей, Kali Linux сприяє розвитку енергійної та активної спільноти. Спільнота робить свій внесок у розробку, тестування та вдосконалення Kali Linux, забезпечуючи її постійну актуальність та ефективність. Характер Kali Linux, керований спільнотою, заохочує співпрацю, обмін знаннями та вивчення нових ідей у сфері кібербезпеки.

Kali Linux - це не просто автономна операційна система, вона також може бути інтегрована в існуючі середовища. Її гнучкість дозволяє використовувати її як віртуальну машину, включати в мультизавантажувальну систему або запускати разом з іншими операційними системами. Така адаптивність дозволяє фахівцям з безпеки легко інтегрувати Kali Linux в існуючі робочі процеси та інфраструктуру.

Оскільки сфера кібербезпеки продовжує розвиватися, Kali Linux залишається надійним і незамінним інструментом для фахівців з безпеки. Потужний набір функцій, вичерпна документація, потужна підтримка спільноти та прихильність до етичного хакінгу роблять його найкращим вибором для тих, хто займається оцінкою безпеки, тестуванням вразливостей та тестуванням на проникнення.

Загалом, Kali Linux слугує комплексною, універсальною та надійною платформою для професіоналів, які займаються захистом інформаційних систем, виявленням вразливостей та випередженням нових загроз. Постійний розвиток, широкий набір інструментів та зручний інтерфейс роблять її цінним надбанням для всіх, хто працює у сфері кібербезпеки.

4.1. Огляд інструментів Kali Linux для тестування на проникнення

4.1.1. Nmap

Nmap (Network Mapper) - це потужний інструмент для сканування та дослідження мереж з відкритим вихідним кодом. Він широко використовується у сфері інформаційної безпеки та мережевого адміністрування для різних цілей, таких як мапування мережі, оцінка вразливостей та тестування на проникнення. Nmap надає повний набір функцій, які дозволяють користувачам виявляти хости, сканувати порти, виявляти операційні системи і збирати інформацію про мережеві служби, що працюють на цільових системах.

Однією з ключових особливостей Nmap є можливість сканування портів. Сканування портів передбачає систематичне зондування мережевих портів цільової системи для виявлення відкритих і закритих портів, а також служб, запущених на цих портах. Ця інформація є цінною для мережевих адміністраторів для розуміння стану безпеки мережі, а для фахівців з безпеки - для виявлення потенційних вразливостей.

Nmap підтримує різні методи сканування, включаючи сканування TCP, UDP, SYN і ACK. Він пропонує гнучкі можливості для вказівки цільових хостів і визначення параметрів сканування. Користувачі можуть налаштовувати типи сканування, параметри часу і формати виводу відповідно до своїх потреб. Nmap також надає розширені функції, такі як визначення версії, дактилоскопія ОС і сканування скриптів, що дозволяють користувачам збирати детальну інформацію про цільові системи.

На додаток до сканування портів, Nmap можна використовувати для мапування та розвідки мережі. Він може виявляти живі хости в мережі, визначати їхні IP-адреси та створювати візуальну карту топології мережі. Це допомагає зрозуміти структуру мережі та визначити потенційні точки входу.

Nmap має високу розширюваність і підтримує написання сценаріїв за допомогою Nmap Scripting Engine (NSE). NSE дозволяє користувачам писати і виконувати власні сценарії для автоматизації завдань, виконання передових методів сканування і збору певної інформації з цільових систем. Репозиторій скриптів NSE містить велику колекцію скриптів, створених спільнотою Nmap, що охоплюють широкий спектр функціональних можливостей.

Крім того, Nmap добре інтегрується з іншими інструментами безпеки та фреймворками. Його можна використовувати разом зі сканерами вразливостей, системами виявлення вторгнень (IDS) та рішеннями для управління інформацією та подіями безпеки (SIEM) для покращення моніторингу мережевої безпеки та можливостей реагування на інциденти.

Мережеві протоколи, що використовуються в комп’ютерних мережах:

- TCP (Transmission Control Protocol (Протокол керування передачею))
- UPD (User Datagram Protocol (Протокол користувацьких дейтаграм))
- SYN (Synchronize (Сихнронізація))
- ACK (Acknowledgment (Підтверження))

TCP - це протокол, орієнтований на з'єднання, який забезпечує надійну та впорядковану доставку даних між пристроями в мережі. Він встановлює з'єднання між відправником і одержувачем, розділяє дані на пакети і гарантує, що пакети прибувають до місця призначення в правильному порядку. TCP також включає в себе механізми управління потоком, виявлення та виправлення помилок.

UDP, з іншого боку, є протоколом без встановлення з'єднання, який забезпечує швидший, але менш надійний метод передачі даних. Він не встановлює з'єднання перед відправкою даних і не забезпечує перевірку помилок або повторну передачу втрачених пакетів. UDP зазвичай використовується для додатків у режимі реального часу, таких як потокове

мультимедіа або онлайн-ігри, де швидкість важливіша за гарантовану доставку.

SYN і ACK - це специфічні для TCP прапори, що використовуються в тристоронньому рукостисканні TCP, яке є процесом встановлення з'єднання між двома пристроями. Коли клієнт хоче встановити TCP-з'єднання з сервером, він надсилає серверу пакет SYN. Сервер відповідає пакетом ACK, який підтверджує запит клієнта і надсилає свій власний SYN-пакет. Нарешті, клієнт відправляє пакет ACK назад на сервер, і з'єднання встановлюється.

Прапори SYN і ACK є частиною заголовка TCP і вказують на стан процесу встановлення з'єднання. SYN використовується для ініціювання запиту на з'єднання, тоді як ACK використовується для підтвердження отриманого пакета або підтвердження встановлення з'єднання.

Розуміння TCP, UDP, SYN і ACK важливо при роботі з мережевими протоколами, аналізі мережевого трафіку або усуненні несправностей в мережі. Різні протоколи та пов'язані з ними прапори мають специфічну поведінку і характеристики, які впливають на надійність, швидкість і функціональність мережевого зв'язку.

Nmap Scripting Engine (NSE) - це потужна функція Nmap, яка дозволяє користувачам писати і виконувати власні сценарії для автоматизації завдань, виконання розширених методів сканування і збору певної інформації з цільових систем під час сканування мережі.

NSE розширює функціональність Nmap, надаючи основу для розробки і запуску сценаріїв, які можуть взаємодіяти з перевіреними хостами, маніпулювати результатами сканування і виконувати додаткові перевірки безпеки. Ці скрипти написані на мові програмування Lua, яка є легкою і універсальною мовою сценаріїв.

Скрипти NSE можна використовувати для виконання широкого спектру завдань, зокрема:

- Виявлення служб і версій: Скрипти можуть бути написані для виявлення певних служб, що працюють на відкритих портах, і визначення їхніх версій. Це допомагає виявити потенційні вразливості, пов'язані з певними версіями сервісів.

- Сканування вразливостей: Скрипти NSE можна використовувати для пошуку відомих вразливостей в цільових системах. Ці скрипти використовують різні методи для виявлення вразливих сервісів, неправильних конфігурацій або слабких місць, якими можна скористатися.

- Експлуатація та доставка корисного навантаження: Деякі сценарії NSE призначені для використання відомих вразливостей або доставки корисного навантаження на цільові системи. Ці скрипти можна використовувати для імітації атак і оцінки стану безпеки перевірених хостів.

- Збір інформації: Скрипти NSE надають можливість збирати детальну інформацію про цільові системи, таку як відомості про операційну систему, топологію мережі, інформацію DNS, дані SNMP тощо. Ця інформація допомагає зрозуміти цільове середовище і виявити потенційні ризики для безпеки.

- Перевірки відповідності: Сценарії NSE можна використовувати для перевірки відповідності цільових систем певним стандартам безпеки або системам відповідності. Ці сценарії допомагають оцінити відповідність систем найкращим галузевим практикам і нормативним вимогам.

NSE постачається з широким спектром попередньо створених сценаріїв, які охоплюють різні функціональні можливості. Ці скрипти

підтримуються спільнотою Nmap і охоплюють популярні сервіси, протоколи та перевірки безпеки. Крім того, користувачі можуть розробляти власні скрипти для задоволення конкретних потреб або виконання унікальних завдань.

Для використання скриптів NSE ви можете вказати їх за допомогою опції **--script** у команді Nmap. Nmap завантажить і виконає вказані сценарії під час сканування, надаючи додаткову інформацію і виконуючи потрібні завдання.

Важливо зазначити, що при використанні скриптів NSE необхідно переконатися, що ви маєте належні повноваження для сканування і взаємодії з цільовими системами. Несанкціоноване або неетичне використання скриптів NSE може порушувати закони і правила, тому дуже важливо отримати належні дозволи і дотримуватися правових і етичних норм при проведенні оцінок безпеки або тестів на проникнення.

Перевірка стану портів є важливою функцією Nmap. Це дозволяє визначити, чи порт відкритий, закритий чи відфільтрований. Відкриті порти означають активні служби, закриті порти означають, що жодна служба не прослуховує, а відфільтровані порти означають, що доступ заблоковано брандмауером або фільтруючим пристроєм. Ця інформація допомагає виявити потенційні вразливості та оцінити безпеку мережі.

Порти які ідентифікує Nmap:

- **Відкритий**

Програма активно приймає з’єднання TCP, дейтаграми UDP або асоціації SCTP на цьому порту. Їх пошук часто є основною метою сканування портів. Люди, які піклуються про безпеку, знають, що кожен відкритий порт – це шлях для нападу. Зловмисники та тестувальники хочуть використовувати відкриті порти, тоді як адміністратори намагаються закрити або захистити їх за допомогою брандмауерів, не перешкоджаючи законним користувачам. Відкриті порти також цікаві для сканування, не пов’язаного з безпекою, оскільки вони показують служби, доступні для використання в мережі.

- **Закритий**

Закритий порт доступний (він отримує та відповідає на пакети зонда Nmap), але немає жодної програми, яка його слухає. Вони можуть бути корисними для показу того, що хост працює на IP-адресі (виявлення хосту або сканування ping), а також як частину виявлення ОС. Оскільки закриті порти доступні, можливо, варто сканувати пізніше, якщо деякі відкриються. Адміністратори можуть захотіти заблокувати такі порти брандмауером. Тоді вони з'являться у відфільтрованому стані, про що йдеться далі.

- **Фільтрований**

Nmap не може визначити, чи відкритий порт, оскільки фільтрація пакетів не дозволяє його зондам досягати порту. Фільтрування може відбуватися за допомогою спеціального брандмауера, правил маршрутизатора або програмного забезпечення брандмауера на основі хоста. Ці порти засмучують зловмисників, оскільки надають дуже мало інформації. Іноді вони відповідають повідомленнями про помилку ICMP, наприклад тип 3 з кодом 13 (одержувач недоступний: зв'язок адміністративно заборонено), але фільтри, які просто скидають зонди без відповіді, набагато поширеніші. Це змушує Nmap повторити спробу кілька разів на випадок, якщо зонд було відкинуто через перевантаження мережі, а не через фільтрацію. Це різко сповільнює сканування.

- **Нефільтрований**

Нефільтрований стан означає, що порт доступний, але Nmap не може визначити, відкритий він чи закритий. Лише сканування ACK, яке використовується для відображення наборів правил брандмауера, класифікує порти в цьому стані. Сканування нефільтрованих портів за допомогою інших типів сканування, наприклад сканування вікон, сканування SYN або сканування FIN, може допомогти визначити, чи відкритий порт.

- **Відкритий|Фільтрований**

Nmap переводить порти в цей стан, якщо не може визначити, чи порт відкритий чи відфільтрований. Це трапляється для типів сканування, у яких відкриті порти не відповідають. Відсутність відповіді також може означати, що фільтр пакетів пропустив зонд або будь-яку відповідь, яку він викликав. Тож Nmap не знає напевно, чи порт відкритий, чи його

фільтрують. Сканування UDP, IP-протоколу, FIN, NULL і Xmas класифікують порти таким чином.

- **Закритий|Фільтрований**

Цей стан використовується, коли Nmap не може визначити, закрито чи відфільтровано порт. Він використовується лише для сканування IP ID у режимі очікування.

Переваги та Недоліки Nmap:

Переваги:

- Універсальні можливості сканування: Nmap пропонує широкий спектр методів і опцій сканування, що дозволяє користувачам виконувати комплексне сканування мережі для виявлення хостів, відкритих портів, служб і операційних систем.

- Портативність: Nmap доступний для багатьох платформ, включаючи Windows, macOS, Linux і BSD, що робить його легко доступним і придатним для використання в різних операційних системах.

- Комплексна підтримка протоколів: Nmap підтримує широкий спектр протоколів, включаючи TCP, UDP, ICMP, ARP та інші. Це дає змогу ретельно сканувати та аналізувати різні мережеві рівні та протоколи.

- Розширюваність: Nmap можна розширити за допомогою додаткових сценаріїв і модулів, покращуючи його функціональність і використовуючи спеціальні методи сканування та аналізу.

- Механізм створення сценаріїв: Механізм створення сценаріїв Nmap (NSE) дозволяє користувачам писати та виконувати сценарії для розширеного мережевого сканування та автоматизованих завдань, що робить його дуже гнучким і настроюваним.

- Надійність і ефективність: Nmap відомий своєю надійністю, швидкістю та ефективністю під час сканування мереж, навіть у великих мережах. Він використовує оптимізовані алгоритми та

методи для мінімізації впливу мережі та отримання точних результатів.

Недоліки:

- Складність: Nmap має круту криву навчання, особливо для початківців. Розуміння та ефективне використання його широкого набору функцій і параметрів може потребувати часу та зусиль.

- Інтрузивний характер: деякі методи сканування, які використовує Nmap, наприклад сканування SYN або ICMP, можуть вважатися інтрузивними та можуть ініціювати сповіщення системи безпеки або блокуватися певними засобами захисту мережі, залежно від конфігурації мережі.

- Помилкові спрацьовування та помилково негативні результати: хоча Nmap загалом точний, існує ймовірність помилкових спрацьовувань (що вказує на відкритий порт або вразливість, якої не існує) або помилково негативних результатів (неможливо виявити відкритий порт чи вразливість). Правильна конфігурація та інтерпретація результатів сканування мають вирішальне значення для мінімізації цих проблем.

- Юридичні та етичні міркування: Nmap є потужним інструментом, який можна використовувати для несанкціонованих дій. Важливо відповідально використовувати Nmap, дотримуючись правових і етичних принципів і маючи належний дозвіл для тестування безпеки.

- Вплив на мережу: інтенсивне сканування мережі за допомогою Nmap може генерувати значний мережевий трафік, який може вплинути на продуктивність мережі або викликати сигналізацію безпеки в певних середовищах. Слід подбати про мінімізацію впливу на роботу мережі.

- Довіра до активного сканування: Nmap в основному покладається на методи активного сканування, що означає, що він може не виявляти пасивних або прихованих загроз, які не реагують на скануючі зонди.

Варто зазначити, що хоча Nmap є потужним інструментом, його використання має бути етичним і відповідальним. Несанкціоноване сканування або зондування систем без належного дозволу є незаконним і неетичним. Важливо отримати належні дозволи і дотримуватися правових та етичних норм при проведенні оцінок безпеки або тестів на проникнення.

4.1.2.Wireshark

Wireshark - це потужний і широко використовуваний аналізатор мережевих протоколів, який дозволяє перехоплювати, аналізувати і перевіряти мережевий трафік в режимі реального часу. Він надає повний набір функцій для усунення несправностей мережі, розробки протоколів, аналізу безпеки та моніторингу мережі.

За допомогою Wireshark ви можете перехоплювати пакети з мережевого інтерфейсу або читати файли перехоплення пакетів, щоб вивчити деталі мережевої взаємодії. Він підтримує широкий спектр протоколів, включаючи Ethernet, TCP/IP, HTTP, DNS, UDP, SSL/TLS і багато інших. Це дозволяє аналізувати поведінку і взаємодію різних мережевих протоколів і додатків.

Однією з ключових особливостей Wireshark є його інтуїтивно зрозумілий і зручний графічний інтерфейс, який надає багатий набір інструментів і опцій для аналізу пакетів. Ви можете переглядати перехоплені пакети в різних форматах, застосовувати фільтри, щоб зосередитися на певному трафіку, і розбирати пакети, щоб витягти цінну інформацію про мережеві розмови. Wireshark також пропонує розширені функції, такі як розфарбовування, правила розфарбовування пакетів і декодування для конкретних протоколів, щоб зробити процес аналізу більш ефективним і глибоким.

Wireshark дозволяє перевіряти вміст пакетів на різних рівнях мережевого стека, включаючи кадри Ethernet, IP-пакети, протоколи транспортного рівня (такі як TCP і UDP) і протоколи прикладного рівня. Це дозволяє виявити і усунути проблеми, пов'язані з підключенням до

мережі, продуктивністю, вразливостями безпеки і неправильною конфігурацією протоколів.

На додаток до аналізу пакетів, Wireshark надає різні статистичні інструменти і графіки, які допоможуть вам зрозуміти поведінку мережі. Ви можете генерувати зведену статистику, відстежувати потоки розмов, візуалізувати хронометраж пакетів, а також аналізувати час проходження і затримки в мережі. Ці функції допомагають діагностувати мережеві проблеми, оптимізувати продуктивність мережі і виявляти аномалії в мережевому трафіку.

Крім того, Wireshark підтримує різні розширення і плагіни, які розширюють його функціональність. Ви можете використовувати ці розширення для виконання спеціалізованого аналізу, інтеграції з іншими інструментами або автоматизації повторюваних завдань. Крім того, Wireshark пропонує надійний інтерфейс для написання сценаріїв на мові Lua, що дозволяє розробляти власні аналізатори, фільтри та сценарії аналізу відповідно до ваших конкретних потреб.

Переваги та Недоліки Wireshark:

Переваги:

- Комплексний аналіз мережі: Wireshark — це потужний аналізатор мережевих протоколів, який забезпечує глибоке розуміння мережевого трафіку. Він фіксує та аналізує мережеві пакети, дозволяючи користувачам діагностувати проблеми з мережею, усувати проблеми та аналізувати поведінку мережі.

- Підтримка протоколів: Wireshark підтримує широкий спектр мережевих протоколів, у тому числі такі популярні, як TCP, UDP, HTTP, DNS тощо. Це дозволяє проводити глибокий аналіз і декодування мережевого трафіку на рівні протоколу.

- Багатий набір функцій: Wireshark пропонує безліч функцій, включаючи розширену фільтрацію, захоплення та аналіз пакетів, настроювані параметри відображення, моніторинг у реальному

часі та можливість експортувати отримані дані для подальшого аналізу.

- Сумісність між платформами: Wireshark доступний для різних операційних систем, включаючи Windows, macOS і Linux, що робить його доступним для користувачів на різних платформах.

- Зручний інтерфейс: Wireshark забезпечує зручний та інтуїтивно зрозумілий інтерфейс, що полегшує як новачкам, так і досвідченим користувачам навігацію та аналіз мережевого трафіку.

Недоліки:

- Складність і криве навчання: Wireshark — це складний інструмент, який вимагає хорошого розуміння мережевих концепцій і протоколів. Користувачам-початківцям може бути складно використовувати весь потенціал і ефективно інтерпретувати отримані дані.

- Величезний обсяг даних: Wireshark збирає велику кількість даних мережевого трафіку, аналіз яких може бути величезним, особливо в середовищах із високим трафіком. Фільтрування та зосередження на конкретних цікавих пакетах є важливими, щоб уникнути перевантаження інформацією.

- Конфіденційність і юридичні проблеми: Аналіз мережевого трафіку за допомогою Wireshark викликає проблеми конфіденційності та юридичні проблеми. Перехоплення та аналіз мережевих пакетів без належного дозволу може порушити правила конфіденційності та юридичні межі.

- Вплив на продуктивність: процес захоплення пакетів Wireshark може створити навантаження на системні ресурси, особливо під час захоплення мережевого трафіку у високошвидкісних мережах

або протягом тривалого часу. Це може вплинути на продуктивність головної машини.

- Обмежені параметри віддаленого захоплення: функція віддаленого захоплення Wireshark має певні обмеження та вимагає додаткової конфігурації та налаштування для захоплення пакетів із віддалених систем. Це може бути складно в певних мережевих середовищах.

Варто зазначити, що хоча Wireshark є цінним інструментом для мережевого аналізу, його слід використовувати відповідально і в межах правових та етичних норм. Захоплення і аналіз мережевого трафіку без належного дозволу є незаконним і неетичним. Важливо переконатися, що ви маєте необхідні дозволи і дотримуєтеся чинних законів і правил при використанні Wireshark або будь-якого іншого інструменту мережевого аналізу.

В цілому, Wireshark є універсальним і незамінним інструментом для мережевих адміністраторів, фахівців з безпеки, розробників і всіх, хто зацікавлений в розумінні і усуненні несправностей мережевого зв'язку. Багатий набір функцій, широка підтримка протоколів і зручний інтерфейс роблять його важливим компонентом будь-якого набору інструментів для мережевого аналізу.

4.1.3. Metasploit

Metasploit - це потужний і широко використовуваний фреймворк для тестування на проникнення, який надає комплексний набір інструментів для проведення оцінки безпеки, розробки експлойтів і дослідження вразливостей. Це проект з відкритим вихідним кодом, що підтримується Rapid7, призначений для допомоги фахівцям з безпеки у виявленні та використанні вразливостей у цільових системах.

В основі Metasploit лежить велика і постійно оновлювана база даних експлойтів, корисного навантаження та допоміжних модулів. Вона охоплює широкий спектр векторів і методів атак, що дозволяє дослідникам

безпеки і тестувальникам на проникнення імітувати реальні атаки і оцінювати стан захищеності цільових систем.

Однією з ключових особливостей Metasploit є його фреймворк для експлуатації, який спрощує процес виявлення та використання вразливостей. Він надає зручний інтерфейс та інтерфейс командного рядка (CLI) для взаємодії з фреймворком. За допомогою Metasploit можна легко знайти вразливості, вибрати відповідний експлойт, налаштувати корисне навантаження і запустити атаку на цільову систему.

Metasploit підтримує різноманітне корисне навантаження, включаючи віддалене виконання команд, впровадження командного коду, сеанси meterpreter тощо. Ці функції надають розширені можливості для подальших дій, таких як підвищення привілеїв, латеральне переміщення та витік даних. Зокрема, корисне навантаження meterpreter дозволяє здійснювати інтерактивний контроль і надає широкі функціональні можливості для пост-експлуатації в скомпрометованих системах.

На додаток до можливостей експлуатації, Metasploit пропонує допоміжні модулі для таких завдань, як розвідка, сканування та збір інформації. Ці модулі дозволяють виявляти мережеві сервіси, перераховувати хости, збирати системну інформацію та виконувати інші важливі завдання під час тестування на проникнення. Metasploit також підтримує пост-експлуатаційні модулі, які полегшують подальшу експлуатацію та підтримують доступ до скомпрометованих систем.

Розширюваність Metasploit - ще один важливий аспект фреймворку. Він надає середовище розробки для створення власних експлойтів, модулів та корисного навантаження. Ця гнучкість дозволяє фахівцям з безпеки адаптувати та налаштовувати фреймворк для задоволення конкретних потреб, пошуку нових вразливостей або розробки експлойтів для перевірки концепції.

Metasploit інтегрується з іншими інструментами та фреймворками безпеки, що робить його цінним компонентом комплексного набору

інструментів для оцінки безпеки. Він підтримує взаємодію з популярними сканерами вразливостей, такими як Nexpose і OpenVAS, що полегшує інтеграцію результатів сканування вразливостей в процес експлуатації.

Ключові можливості та особливості Metasploit:

- Розробка експлойтів: Metasploit дозволяє фахівцям із безпеки розробляти та тестувати власні експлойти на відомі вразливості. Він забезпечує комплексне середовище розробки для створення надійних і ефективних експлойтів.

- Сканування вразливостей: Metasploit містить сканер вразливостей, який може ідентифікувати відомі вразливості в цільових системах. Він використовує велику базу даних вразливостей і пов’язаних з ними експлойтів, щоб допомогти оцінити стан безпеки мережі.

- Модулі експлойтів: Metasploit пропонує велику колекцію готових модулів експлойтів, які можна використовувати для виявлення певних уразливостей у різних системах і програмах. Ці модулі спрощують процес запуску атак, надаючи готові до використання експлойти.

- Постексплуатація: коли систему зламано, Metasploit надає низку постексплуатаційних модулів для підтримки доступу, збору інформації, підвищення привілеїв і переходу до інших систем у мережі. Ці модулі допомагають імітувати реальні сценарії атак і оцінювати потенційний вплив успішного злому.

- Соціальна інженерія: Metasploit містить інструменти для проведення атак соціальної інженерії, таких як фішингові кампанії або доставка корисного навантаження через шкідливі файли або веб-сайти. Ці функції допомагають оцінити ефективність навчання організації з питань безпеки та захисту від методів соціальної інженерії.

- Звітування та співпраця: Metasploit надає функції звітування для створення комплексних звітів про оцінку. Він також підтримує співпрацю, дозволяючи командам обмінюватися інформацією, експлойтами та техніками через централізоване сховище.

- Інтеграція: Metasploit можна інтегрувати з іншими інструментами та фреймворками безпеки, розширюючи загальні можливості інфраструктури тестування безпеки організації.

Переваги та Недоліки Metasploit:

Переваги:

- Розробка та тестування експлойтів: Metasploit надає величезну колекцію експлойтів, корисних навантажень і допоміжних модулів, які допомагають у розробці та тестуванні вразливостей безпеки. Це дозволяє фахівцям із безпеки оцінювати та підтверджувати ефективність захисту та оцінювати потенційні слабкі місця в системах.

- Швидке тестування на проникнення: Metasploit спрощує й автоматизує процеси тестування на проникнення, дозволяючи командам безпеки ефективно виявляти та використовувати вразливості в цільових системах. Це спрощує робочий процес, заощаджуючи час і зусилля під час оцінки безпеки.

- Велика база даних про експлойти: Metasploit підтримує велику базу даних про відомі вразливості та експлойти, що робить її цінним ресурсом для професіоналів із безпеки. Постійно оновлювані модулі експлойтів забезпечують доступ до найновіших технологій і методологій.

- Постексплойт-фреймворк: Metasploit пропонує пост-експлуатаційний фреймворк, який дозволяє користувачам підтримувати доступ до скомпрометованих систем, збирати додаткову інформацію, підвищувати привілеї та виконувати різні дії після експлуатації.

- Спільнота та співпраця: Metasploit має активну спільноту професіоналів із безпеки, які активно сприяють його розвитку, діляться знаннями та надають підтримку. Природа, керована громадою, забезпечує постійне вдосконалення та доступ до багатства ресурсів.

Недоліки:

- Складність і криве навчання: Metasploit — це складний інструмент, який потребує глибокого розуміння методології тестування на проникнення, розробки експлойтів і різноманітних мережевих протоколів. Його широкі можливості та функції можуть бути приголомшливими для початківців.

- Потенційне зловживання: Metasploit, як і будь-який потужний хакерський інструмент, можна використовувати не за призначенням або використовувати для зловмисних цілей. Важливо використовувати Metasploit відповідально, з належним дозволом і в рамках закону.

- Помилкові спрацьовування та помилкові негативи: ефективність експлойтів Metasploit залежить від точної ідентифікації та успішного використання вразливостей. Можуть виникати хибні спрацьовування (неіснуючі вразливості, які можна використати) і хибні негативи (пропущені вразливості), що вимагає ручної перевірки та підтвердження.

- Виявлення на основі сигнатур: деякі антивірусні системи та системи виявлення вторгнень можуть виявляти діяльність Metasploit і позначати її як підозрілу або зловмисну. Це може перешкоджати ефективності певних експлойтів і вимагати додаткових методів ухилення.

- Обмежена сумісність з платформами: хоча Metasploit підтримує кілька платформ, деякі експлойти та корисні навантаження можуть мати обмеження або краще працювати в певних операційних системах. Проблеми сумісності можуть виникнути під час націлювання на різні середовища.

Хоча Metasploit є потужним інструментом для фахівців з безпеки, важливо підкреслити важливість етичного та відповідального використання. Metasploit слід використовувати лише в тих системах, до яких у вас є відповідний дозвіл. Незаконне або несанкціоноване використання Metasploit або будь-якого іншого інструменту для злому суворо заборонено і може призвести до юридичних наслідків.

Таким чином, Metasploit - це універсальний і багатофункціональний фреймворк для тестування на проникнення, який допомагає фахівцям з безпеки виявляти і експлуатувати вразливості. Його велика база даних експлойтів, корисного навантаження і модулів, а також зручний інтерфейс роблять його цінним інструментом для проведення оцінки безпеки і зміцнення загальної системи безпеки організацій.

4.1.4. Aircrack-ng

Aircrack-ng - це потужний інструмент, який широко використовується для оцінки безпеки бездротових мереж і тестування на проникнення. Він пропонує повний набір функцій і можливостей для аналізу та оцінки вразливостей бездротових мереж.

За допомогою Aircrack-ng ви можете перехоплювати і аналізувати бездротовий мережевий трафік, отримуючи інформацію про дані, якими обмінюються пристрої. Він підтримує різні бездротові інтерфейси, дозволяючи відстежувати і вивчати активність пакетів в режимі реального часу.

Однією з особливостей Aircrack-ng є його здатність зламувати ключі шифрування WEP і WPA/WPA2. Захоплюючи достатню кількість пакетів і використовуючи різні методи атаки, такі як FMS, PTW і перехоплення рукостискання WPA, він може оцінити надійність мережевого шифрування.

Крім того, Aircrack-ng дозволяє виконувати атаки на деаутентифікацію і роз'єднання підключених клієнтів, порушуючи їх підключення і потенційно полегшуючи подальшу експлуатацію або розвідку.

Інструмент також надає можливості моніторингу та аналізу бездротових клієнтів і точок доступу. Він дозволяє збирати інформацію про найближчі мережі, рівень їхнього сигналу, підтримувані методи шифрування та підключених клієнтів. Ця інформація допомагає виявити потенційні вразливості та оцінити безпеку мережі.

Aircrack-ng включає в себе різні інструменти для злому, які націлені на конкретні слабкі місця в бездротових мережах. Ці інструменти використовують такі вразливості, як фрагментація, ChopChop і статистичний аналіз для збору важливої інформації та оцінки безпеки мережі.

Крім того, Aircrack-ng підтримує відновлення паролів для різних мережевих протоколів, таких як WEP, WPA, WPA2 і WPA-PSK. Він може аналізувати перехоплені пакети або використовувати попередньо обчислені хеш-таблиці (rainbow-таблиці) для спроби відновлення пароля.

Інструмент є крос-платформним, сумісним з Linux, Windows і macOS і підтримує широкий спектр бездротових мережевих адаптерів і стандартів (802.11a/b/g/n/ac).

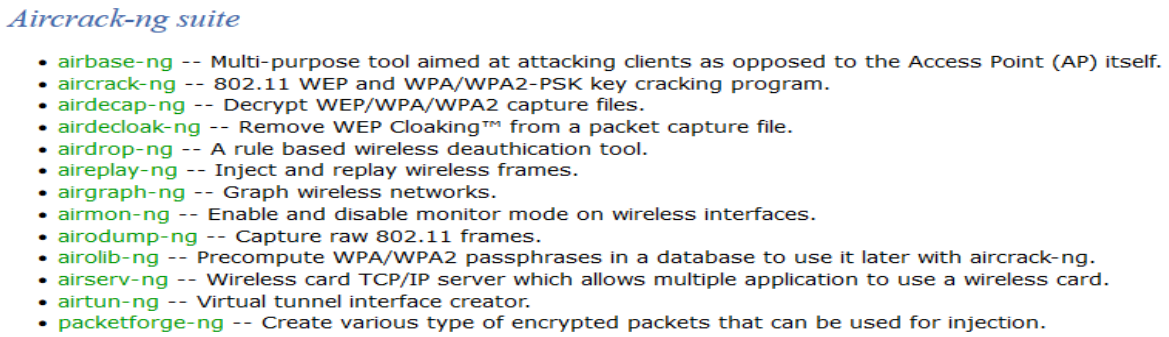


Рис 4.1.1. – Команди які використовують у Aircrack-ng

Переваги та Недоліки Aircrack-ng:

- Комплексна оцінка безпеки бездротового зв'язку: Aircrack-ng пропонує широкий спектр функцій і інструментів для аналізу та оцінки безпеки бездротових мереж, включаючи захоплення та аналіз мережевого трафіку, злом ключів шифрування та моніторинг мережевої активності.

- Сумісність і підтримка платформ: Aircrack-ng — це кросплатформний інструмент, який працює на різних операційних системах, зокрема Linux, Windows і macOS. Він сумісний із широким спектром бездротових мережевих адаптерів і підтримує кілька бездротових стандартів.

- Злом ключа шифрування: Aircrack-ng надає можливості для злому ключів шифрування WEP і WPA/WPA2, дозволяючи фахівцям із безпеки оцінювати силу шифрування мережі та виявляти потенційні вразливості.

- Атаки деаутентифікації: Aircrack-ng дозволяє виконувати атаки деаутентифікації, які можуть бути корисними для тестування захисту мережі, виявлення слабких місць або вивчення поведінки мережі у відповідь на збої.

- Відновлення пароля: Aircrack-ng підтримує відновлення пароля для різних мережевих протоколів, таких як WEP, WPA, WPA2 і WPA-PSK. Він може аналізувати захоплені пакети або використовувати попередньо обчислені хеш-таблиці (райдужні таблиці) для відновлення пароля.

Недоліки:

- Етичні та юридичні міркування: використання Aircrack-ng, як і будь-якого іншого інструменту оцінки безпеки, має відповідати правовим та етичним принципам. Несанкціоноване або зловмисне використання може порушити закони про конфіденційність і призвести до правових наслідків.

- Потрібні технічні знання: Aircrack-ng — це потужний інструмент, який потребує хорошого розуміння бездротових мереж, мережевих протоколів і механізмів шифрування. Рекомендується для досвідчених фахівців з безпеки, які володіють необхідними знаннями та навичками.

- Обмежена ефективність проти суворих заходів безпеки: хоча Aircrack-ng може успішно зламати слабкі або погано налаштовані ключі шифрування, він може зіткнутися з проблемами, коли має справу із суворими заходами безпеки, такими як складні паролі, надійні алгоритми шифрування або належним чином реалізований захист мережі.

- Витратність часу та ресурсів: Злом ключів шифрування може бути трудомістким процесом, особливо для мереж із більш суворими заходами безпеки. Це вимагає захоплення достатньої кількості пакетів і виконання інтенсивних обчислень, що може зайняти значний час і ресурси.

- Можливість зловживання: Aircrack-ng, як і будь-який інший інструмент безпеки, може бути використаний особами зі зловмисними намірами. Щоб забезпечити безпеку та конфіденційність мереж і окремих осіб, важливо використовувати інструмент відповідально та з належним дозволом.

Поля, які відображає airodump-ng:

BSSID - MAC-адреса точки доступу. У розділі «Клієнт» ідентифікатор BSSID «(не пов’язаний)» означає, що клієнт не пов’язаний з жодною точкою доступу. У цьому неасоційованому стані він шукає точку доступу для підключення.

PWR - Рівень сигналу, який повідомляє адаптер Wi-Fi. Його значення залежить від водія, але в міру наближення до точки доступу або

станції сигнал стає вищим. Зазвичай це RSSI. Якщо BSSID PWR дорівнює -1, тоді драйвер не підтримує звітування про рівень сигналу. Якщо PWR дорівнює -1 для деяких точок доступу, це означає, що точка доступу знаходиться поза діапазоном, однак airodump-ng отримав принаймні кадр, надісланий їй. Якщо PWR дорівнює -1 для обмеженої кількості станцій, це стосується пакета, який надійшов від точки доступу до клієнта, але передачі клієнта знаходяться поза діапазоном для вашого адаптера Wi-Fi. Це означає, що ви чуєте лише 1/2 спілкування. Якщо всі клієнти мають PWR як -1, то, ймовірно, драйвер не підтримує звітування про рівень сигналу. Сильний сигнал близько -40. Середня - близько -55, а слабка - близько -70. Нижня межа адаптерів Wi-Fi (він же чутливість прийому) часто становить близько -80/-90.

RXQ - Якість отримання вимірюється відсотком пакетів (керування та кадрів даних), успішно отриманих за останні 10 секунд.

Beacons - Кількість пакетів оголошень, надісланих точкою доступу. Кожна точка доступу надсилає близько десяти маяків на секунду з найнижчою швидкістю (1 млн), тому їх зазвичай можна вловити дуже далеко.

 # Data - Кількість захоплених пакетів даних (якщо WEP, унікальна кількість IV), включаючи широкомовні пакети даних.

#/s - Вимірювання кількості пакетів даних за секунду за останні 10 секунд.

CH - Номер каналу (береться з пакетів маяків). Примітка: інколи пакети з інших каналів перехоплюються, навіть якщо airodump-ng не стрибає, через радіоперешкоди або перекриття каналів.

MB - Максимальна швидкість, яку підтримує AP. Якщо МБ = 11, це 802.11b, якщо МБ = 22, це 802.11b+, а до 54 – це 802.11g. Усе вище – це 802.11n або 802.11ac. Крапка (після 54 вище) означає, що підтримується коротка преамбула. Відображає «e» після значення швидкості МБ, якщо в мережі ввімкнено QoS.

ENC - Використовується алгоритм шифрування. OPN = без шифрування, «WEP?» = WEP або вище (недостатньо даних для

вибору між WEP і WPA/WPA2), WEP (без знака питання) означає статичний або динамічний WEP, а WPA, WPA2 або WPA3, якщо присутні TKIP або CCMP (WPA3 із TKIP дозволяє WPA або Асоціація WPA2, чистий WPA3 дозволяє лише CCMP). OWE — це Opportunistic Wireless Encryption, або Enhanced Open.

CIPHER - Шифр виявлено. Один із CCMP, WRAP, TKIP, WEP, WEP40 або WEP104. Не обов'язковий, але TKIP зазвичай використовується з WPA, а CCMP – з WPA2. WEP40 відображається, коли індекс ключа перевищує 0. Стандарт стверджує, що індекс може становити 0-3 для 40 біт і має бути 0 для 104 біт.

AUTH - Використаний протокол автентифікації. Один із MGT (WPA/WPA2 з використанням окремого сервера автентифікації), SKA (спільний ключ для WEP), PSK (попередньо загальний ключ для WPA/WPA2) або OPN (відкритий для WEP).

ESSID - Показує назву бездротової мережі. Так званий «SSID», який може бути порожнім, якщо активовано приховування SSID. У цьому випадку airodump-ng спробує відновити SSID із відповідей зонда та запитів на асоціацію. Перегляньте цей розділ для отримання додаткової інформації про приховані ESSID.

STATION - MAC-адреса кожної пов'язаної станції або станцій, які шукають точку доступу для з'єднання. Клієнти, наразі не пов'язані з точкою доступу, мають BSSID «(не пов'язано)».

Rate - Швидкість прийому станції, а потім швидкість передачі. Після кожної швидкості відображається «e», якщо в мережі ввімкнено QoS.

Lost - Кількість пакетів даних, втрачених за останні 10 секунд на основі порядкового номера. Дивіться примітку нижче для більш детального пояснення.

Packets - Кількість пакетів даних, надісланих клієнтом.

Notes - Додаткова інформація про клієнта, наприклад захоплений EAPOL або PMKID.

Probes - ESSID, перевірені клієнтом. Це мережі, до яких клієнт намагається підключитися, якщо він наразі не підключений.

Використовуючи Aircrack-ng або будь-який інший інструмент оцінки безпеки, дуже важливо діяти відповідально і етично. Переконайтеся, що у вас є належний дозвіл перед доступом до бездротових мереж або спробою зламати ключі шифрування. Дотримуйтесь правових та етичних норм для проведення оцінки безпеки і захисту конфіденційності та безпеки мереж і окремих користувачів.

Пам'ятайте, що Aircrack-ng - це лише один з компонентів комплексного набору інструментів для оцінки безпеки. Поєднуйте його з іншими інструментами і методологіями для проведення ретельних оцінок і підвищення загальної безпеки мережі.

4.2. Використання інструментів Kali Linux для виявлення вразливостей інформаційної системи

Kali Linux надає широкий спектр потужних інструментів для тестування на проникнення та оцінки безпеки. Ці інструменти можуть допомогти фахівцям із безпеки виявити вразливі місця, оцінити безпеку системи та захистити від потенційних загроз.

1) Aircrack-ng

Для того щоб працювати з Aircrack-ng, для цього потрібно у меню Kali Linux, натиснути на Root Terminal:

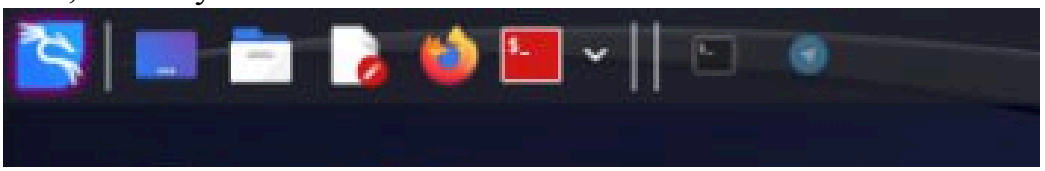


Рис 4.2.1. – Червони відображено Root Terminal

Натиснувши на нього, відкривається вікно:

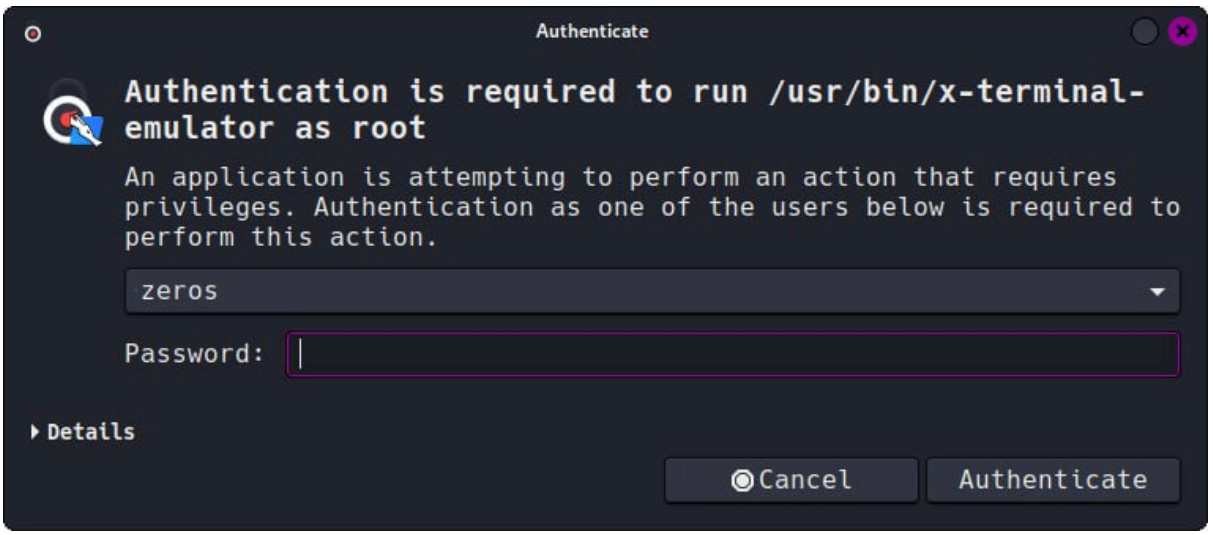


Рис 4.1.2. – Вікно аутентифікації

Далі вводиться пароль який стоїть у системі і далі відкривається сам термінал:

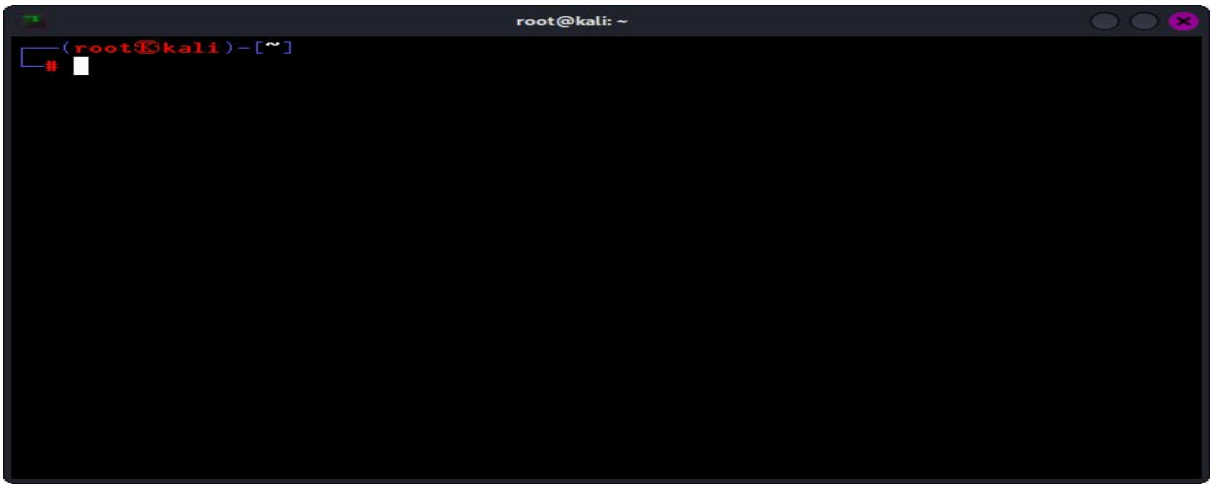


Рис 4.1.3. – Вікно Root Terminal

Далі прописується команда ‘airmon-ng check kill’, для того щоб відключити зайві процеси і воно не заважало роботі, при прописані цієї команди бездротові сервіси недоступні:

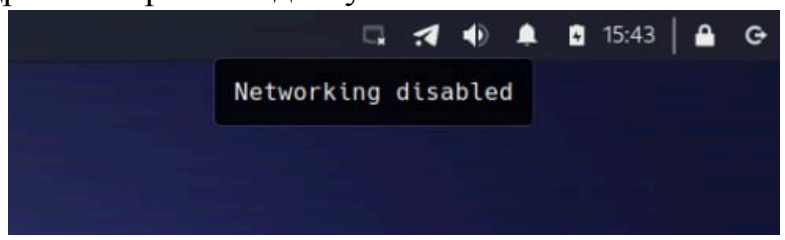


Рис 4.2.4. – Відключення бездротового зв’язку

Далі прописується ‘airmon-ng start wlan0’:

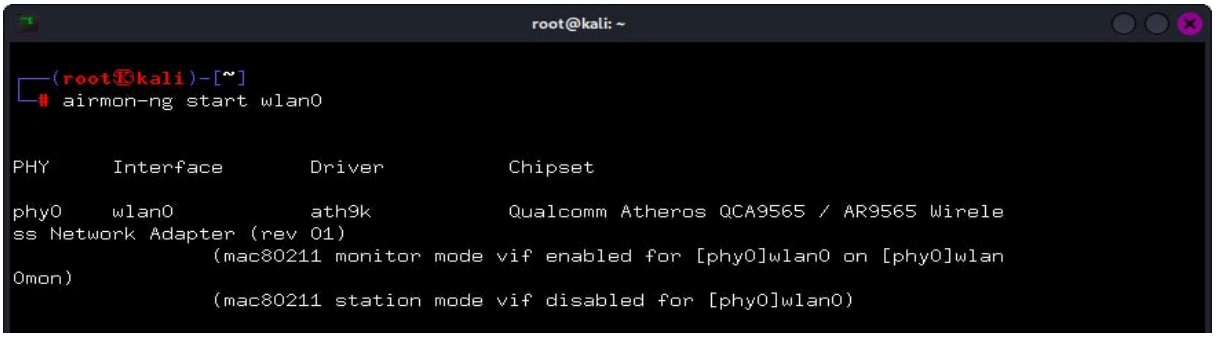


Рис 4.1.5. – Прописування airmon-ng start wlan0

Далі прописується команда '**airodump-ng wlan0mon**':

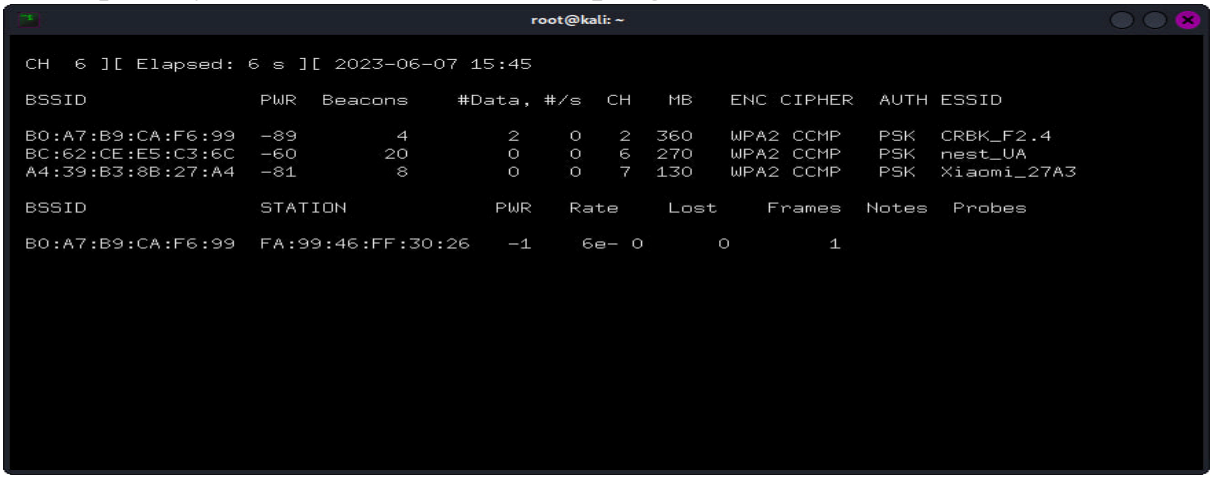


Рис 4.1.6. – Початок роботи

Далі я обираю, що мені потрібно і починаю з цим працювати.

2) Nmap

Як із роботою aircrack-ng потрібні root права.

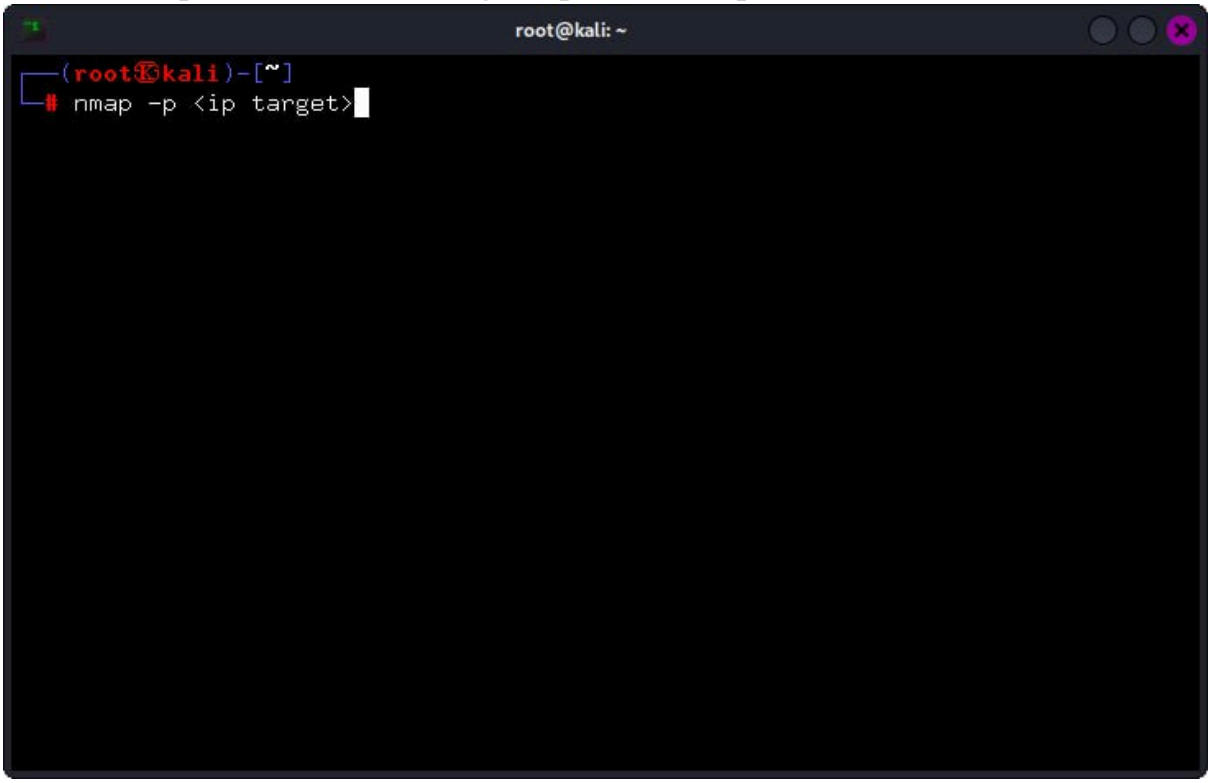


Рис 4.1.7. – Робота з Nmap

де, **-p** – це порт, **<ip target>** - адрес цілі.

Нижче наведено приклад роботи Nmap:

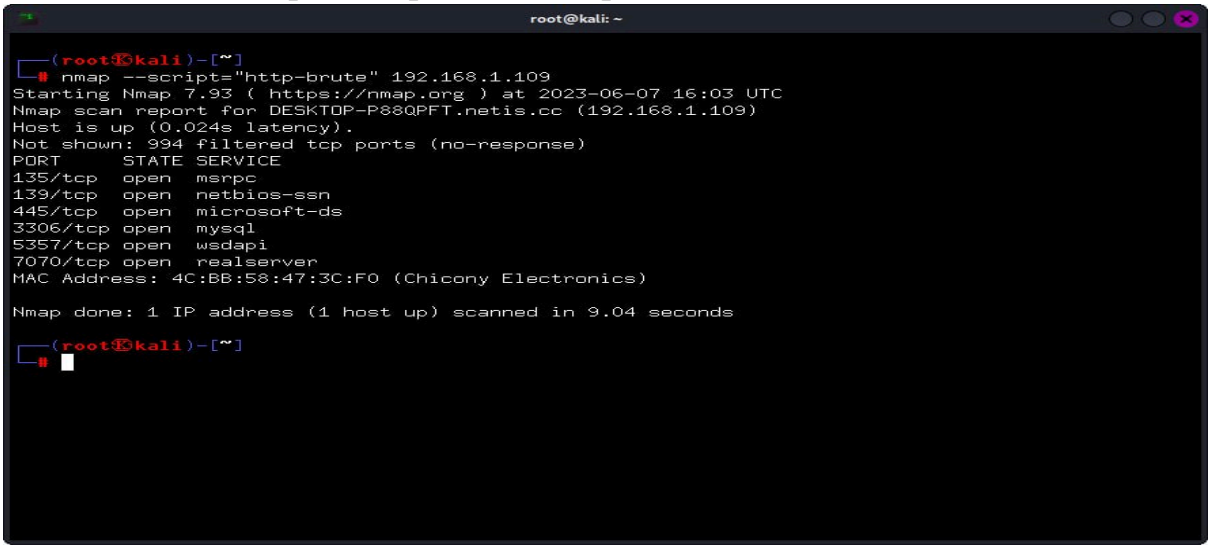


Рис 4.1.8. – Приклад роботи

* Сценарій http-brute у Nmap використовується для виконання атак грубої сили на веб-системи автентифікації. Він намагається вгадати імена користувачів і паролі, систематично пробуючи різні комбінації.

```
Nmap 7.93SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
           <Lua scripts> is a comma-separated list of script-files or
           script-categories.
OS DETECTION:
```

Рис 4.1.9. – Команди які можна використати

```
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --noninteractive: Disable runtime interactions via keyboard
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
```

Рис 4.1.10. – Команди які можна використати

3) Wireshark

Для роботи з Wireshark також потрібні root права:

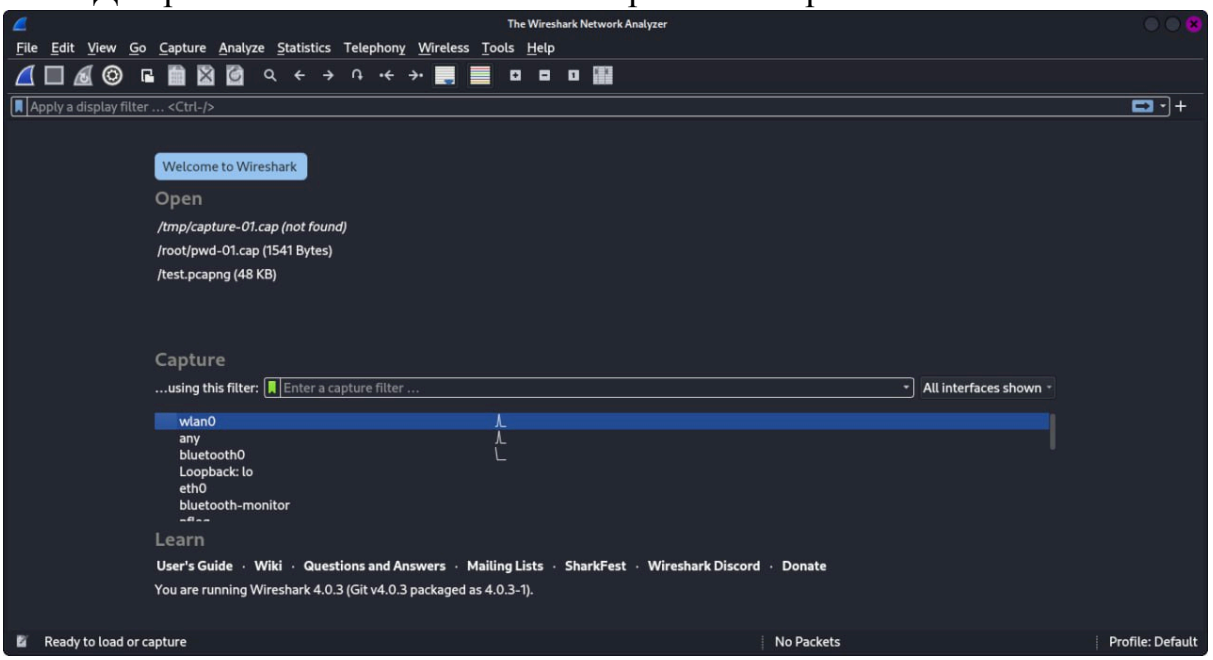


Рис 4.1.11. – Меню Wireshark

Далі я обираю інтерфейс якій мені потрібен і починаю з ним працювати:

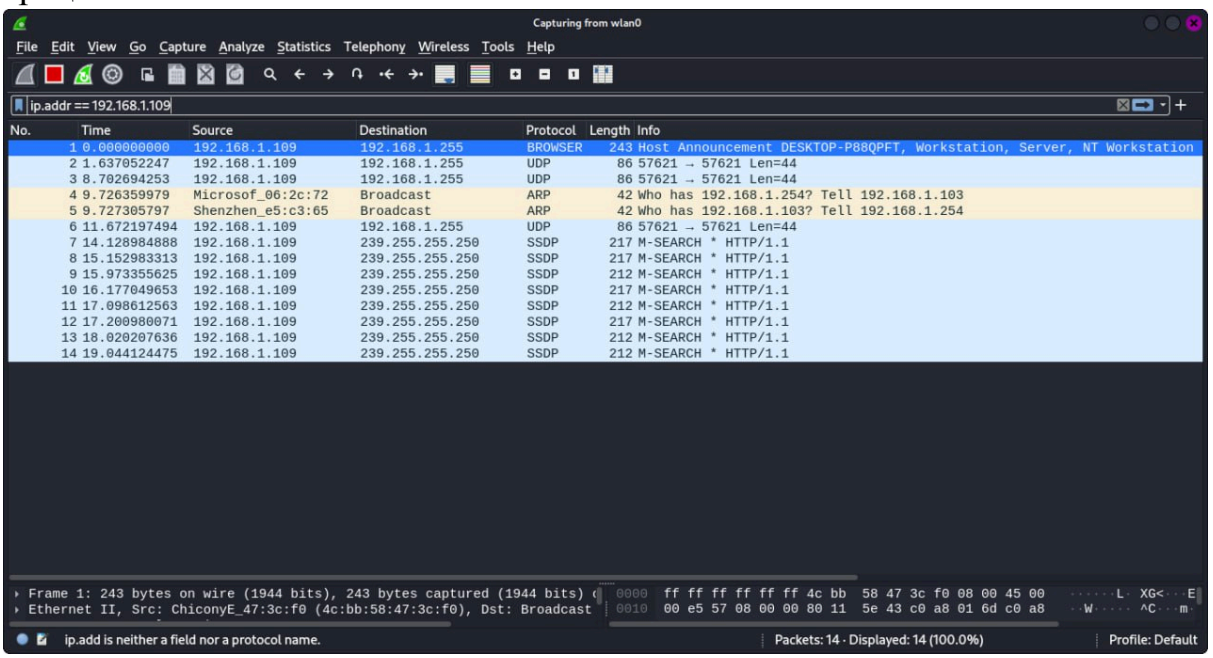


Рис 4.1.12. – Приклад роботи

4) Metasploit

Так як із минули програмами потрібно Root права, для щоб запустити Metasploit можна вибрати його з меню у пуску, або ввести команду **‘msfconsole’**:

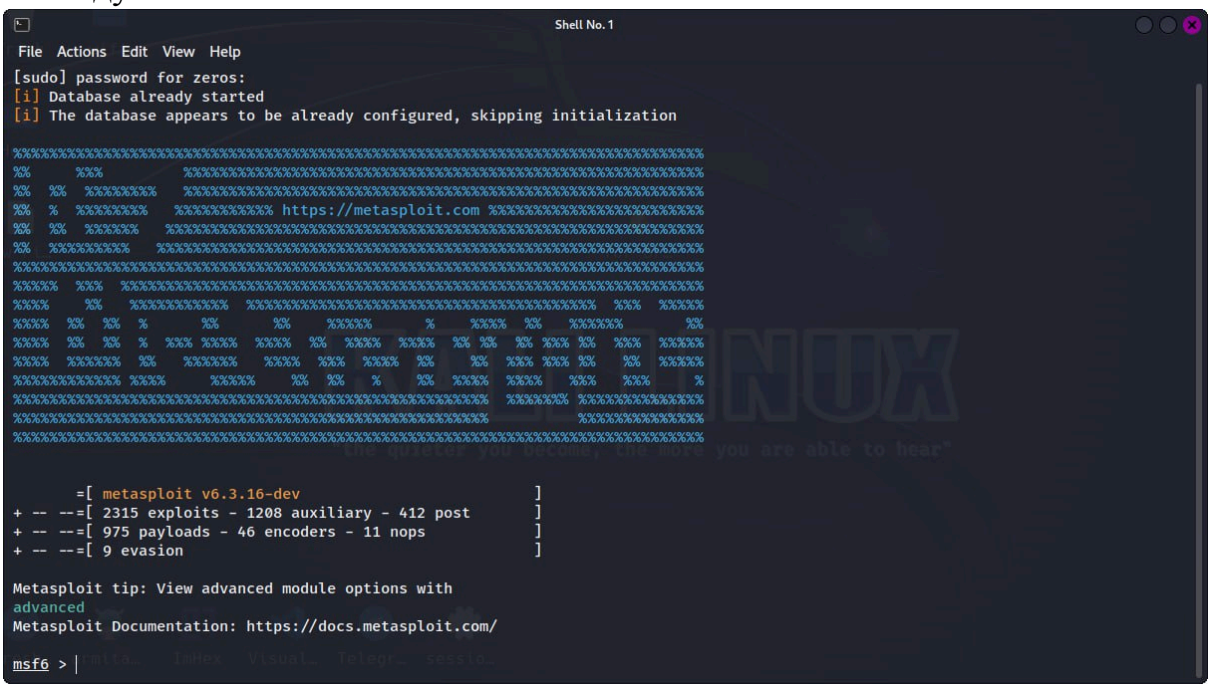


Рис 4.1.13. – Робота програми

Щоб почати роботу, треба ввести путь до модуля або експлоїта, наприклад**, use auxiliary/dos/misc/dopewars** – це мене перекинить до модуля де я вже буду з ним працювати. Також можна зробити **use auxiliary/dos** – де покаже повний список які пов’язані з **auxiliary/dos:**

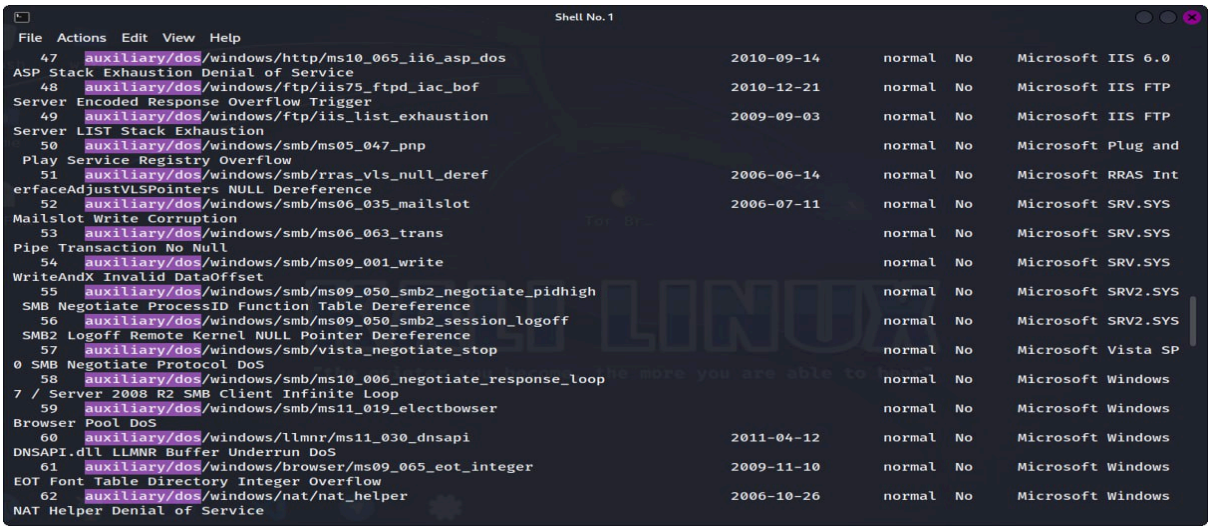


Рис 4.1.14. – Приклад **use auxiliary/dos**

Розділ 5. Заходи щодо підвищення рівня захищеності інформаційної системи на основі результатів аналізу

5.1. Рекомендації щодо підвищення рівня захисту інформації в інформаційній системі

Ключові рекомендації щодо підвищення рівня захисту інформації у інформаційній системі, які базуються на аналізі, проведеному за допомогою Nmap, Wireshark, Metasploit та Aircrack-ng:

1) **Впровадити надійну стратегію мережевої безпеки:**
   Проводьте регулярне сканування мережі за допомогою Nmap для виявлення вразливостей, відкритих портів та потенційних ризиків безпеки. Негайно усувайте виявлені слабкі місця для посилення мережевої безпеки.

2) **Покращуйте аналіз мережевого трафіку:**
   Використування Wireshark для моніторингу та аналізу мережевого трафіку в режимі реального часу. Шукайте будь-які підозрілі або несанкціоновані дії, такі як перехоплення пакетів або атаки типу "зловмисник посередині". Вживайте негайних заходів для зменшення виявлених ризиків.

3) **Проведення тестування на проникнення:**
   Використовуйте Metasploit для комплексного тестування на проникнення, щоб виявити вразливості та слабкі місця у вашій інформаційній системі. Використовуйте отримані результати для вдосконалення заходів безпеки та виправлення виявлених вразливостей.

4) **Посилення безпеки Wi-Fi:**
   Використовуйте Aircrack-ng для оцінки безпеки вашої Wi-Fi мережі. Перевірте надійність паролів Wi-Fi, визначте потенційні вразливості та впровадьте відповідні протоколи шифрування. Регулярно контролюйте безпеку Wi-Fi та оновлюйте заходи за потреби.

5) **Впровадження надійного контролю доступу:**
   Забезпечте належний контроль доступу, щоб обмежити привілеї користувачів і запобігти несанкціонованому доступу. Використовуйте висновки, отримані в результаті аналізу, для визначення сфер, які

потребують покращення контролю доступу, та впроваджуйте відповідні заходи.

Впровадження цих рекомендацій значно підвищить безпеку інформаційної системи, захистивши її від потенційних вразливостей та атак. Регулярні оновлення, навчання співробітників і планування реагування на інциденти також повинні бути враховані для підтримки надійної системи безпеки.

5.2. Рекомендації щодо реалізації заходів з підвищення рівня захисту інформації в інформаційній системі

Рекомендацій щодо впровадження заходів для підвищення рівня захисту інформації у інформаційній системі, які базуються на результатах аналізу за допомогою Nmap, Wireshark, Metasploit та Aircrack-ng:

1) **Регулярне сканування та оцінка вразливостей:**
   Використовування Nmap для регулярного сканування мережі та систем для виявлення потенційних вразливостей та неправильних конфігурацій. Регулярне оновлення інструментів сканування та відстеження нових вразливостей, щоб залишатися проактивними у вирішенні проблем безпеки.

2) **Моніторинг і аналіз мережевого трафіку:**
   Використовування Wireshark для моніторингу та аналізу мережевого трафіку на предмет будь-яких підозрілих або несанкціонованих дій. Відстежуйте незвичні шаблони, мережеві аномалії та ознаки потенційних атак. Оперативне розслідування та реагування на будь-які виявлені інциденти безпеки.

3) **Тестування на проникнення та оцінка безпеки:**
   Використовування Metasploit для проведення тестів на проникнення у інформаційну систему, щоб виявити вразливості та перевірити ефективність засобів контролю безпеки. Регулярне проведення комплексної оцінки безпеки, щоб виявити слабкі місця і визначити пріоритети для їх усунення.

4) **Підвищення безпеки бездротових мереж:**
   Використовування Aircrack-ng для оцінки безпеки бездротової мережі. Переконайтеся, що мережа Wi-Fi використовує надійні протоколи шифрування, такі як WPA2 або WPA3. Вживання заходів для захисту від несанкціонованого доступу, наприклад, зміна пароля за замовчуванням, вимикання непотрібних служб та використовування надійних, унікальних паролів.

5) **Регулярно встановлюйте оновлення та патчі безпеки**:
   Бути пильним у застосуванні оновлень та виправлень безпеки до систем, програм та мережевих пристроїв. Регулярне оновлення програмного забезпечення та мікропрограми, щоб усунути відомі вразливості та захиститися від нових загроз. Впровадження процес управління виправленнями, щоб забезпечити своєчасне оновлення у інформаційній системі.

Пам'ятайте, що інформаційна безпека - це безперервний процес. Постійно відстежуйте, оцінюйте та вдосконалюйте заходи безпеки відповідно до нових загроз та технологічних досягнень. Регулярно навчайте свій персонал найкращим практикам безпеки та встановлюйте чіткі політики та процедури безпеки, щоб сприяти розвитку культури безпеки у вашій організації.

ВИСНОВОК

У процесі дослідження та оцінки рівня захищеності інформаційної системи було використано такі популярні інструменти, як Nmap, Wireshark, Aircrack-ng і Metasploit. Кожен з цих інструментів надає можливості для виявлення потенційних проблем безпеки та вразливостей інформаційної системи.

Аналіз здійснювався за допомогою Nmap, який дозволяє сканувати мережі, виявляти активні хості, порти та служби, що працюють на них. Цей інструмент забезпечив можливість визначити доступність і стан безпеки різних систем, що дозволило виявити потенційні вразливості.

Wireshark був використаний для аналізу мережевого трафіку. Цей інструмент надає можливість перехоплювати та аналізувати пакети, що пересилаються по мережі. Завдяки Wireshark було виявлено можливі проблеми з безпекою, такі як незашифрований зміст, атаки типу "Man-in-the-Middle" та інші.

Aircrack-ng був використаний для аналізу та тестування безпеки бездротових мереж. Цей інструмент дозволяє перехоплювати пакети, зламувати паролі Wi-Fi та проводити аудит безпеки мереж. Завдяки Aircrack-ng були виявлені слабкі точки у безпеці бездротової мережі, що дало змогу розробити заходи для їх покращення.

Metasploit був використаний для тестування експлойтів та вразливостей систем. Цей фреймворк забезпечує широкі можливості для проведення тестування на проникнення, дослідження вразливостей та розробки заходів безпеки. За допомогою Metasploit були виявлені потенційні вразливості системи та виконано тестування на проникнення для оцінки рівня захищеності.

Аналіз результатів, отриманих з використанням Nmap, Wireshark, Aircrack-ng і Metasploit, показав, що інформаційна система має кілька вразливостей та можливих проблем безпеки. Виявлені ризики включають незахищені порти, слабкі паролі, недостатні заходи безпеки бездротової мережі та потенційні вразливості в програмному забезпеченні.

З метою поліпшення рівня захищеності інформаційної системи рекомендується прийняти наступні заходи:

- Забезпечити регулярне оновлення програмного забезпечення та патчів безпеки.
- Встановити сильні паролі та регулярно їх змінювати.
- Захистити бездротову мережу шифруванням та використанням сильних ключів.
- Використовувати брандмауер та інші заходи безпеки для захисту незахищених портів та служб.
- Провести навчання та посвідчення працівників щодо безпеки інформації.

Оцінка рівня захищеності інформаційної системи є важливим етапом в процесі забезпечення безпеки даних та захисту від потенційних загроз. Виявлення вразливостей та проблем безпеки дозволяє організаціям приймати своєчасні заходи для підвищення рівня захисту та запобігання можливим атакам. Постійна моніторинг та оновлення безпекових заходів дозволять забезпечити безпеку інформаційної системи та збереження конфіденційності, цілісності та доступності даних.

ДЖЕРЕЛА