МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗАХИСТУ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Управління кіберінцидентами та аналіз подій»

**Тема № 2**. Електронна комунікаційна мережа об’єкта кіберзахисту як джерело ознак кіберінциденту.

**Заняття № 2/8**. Канал електронної комунікації як вектор нав’язування payload.

**Аналіз мережевого дампу та пошук ознак атаки типу man**

**in the middle**

**Виконав:** курсант навчальної групи 314

солдат \_\_\_\_\_\_\_\_\_\_\_\_\_Янковський О.О

21.04.2024

**Перевiрив:** викладач кафедри № 33

Капітан \_\_\_\_\_\_\_Прийма О.О.

Київ – 2024

1. IP-адреса жертви: 192.168.100.14

2. IP-адреса зловмисника: 107.161.178.166

3. Протокол (канал) що використано зловмисником для ексфільтрації

данних жертви: FTP

4. Ім’я хоста жертви: USER-PC

5. Логін який використовувався зловмисником для аутентифікації на FTPсервері: amanni@artrsllc.com

6. Пароль який використовувався зловмисником для аутентифікації на FTP-сервері: WY{9+?ae}qt

7. Дата і час початку передачі викраденої інформації від жертви [YYYYMM-DD HH:MM:ss]: 2022 07-11 21:30:03

8. Назва файлу що був завантажений з ексфільтрованими даними: PW\_admin-USER-PC\_2022\_07\_11\_22\_30\_00.html

9. Загальний об’єм інформації, що було викрадено у жертви: 567 bytes

10. Назва і версія операційної системи, що встановлена у жертви: Windows 7 Professional

11. Марка та модель процесора на ПК жертви: Intel i5-6400

12. Обліковий запис жертви для поштового клієнту: honey@pot.com \ honeypass356

13. Браузери з яких були викрадені облікові записи жертви: Chrome та Firefox

Додаткові завдання\* (для бажаючих):

14. Альтернативні способи визначення хоста жертви?

15. Визначте геолокацію IP адреси зловмисника

16. Підготуйте технічні рекомендації для внесення змін до політик безпеки з метою блокування даної активності в ІКС ЗС України

**Висновок:** при виконанні наданого завдання було відпрацьовано фільтрування пакетів з дампу за допомогою Wireshark, аналіз пакетів за протоколами та знаходження даних авторизації зловмисника для розслідування атаки типу man in the middle.