МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

КАФЕДРА КІБЕРЗБЕЗПЕКИ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Управління кіберінцидентами та аналіз подій»

**КАНАЛ ЕЛЕКТРОННОЇ КОМУНІКАЦІЇ ЯК ВЕКТОР НАВ’ЯЗУВАННЯ PAYLOAD**

Дата 19.04.2024

**Виконав:** курсант 314 навчальної групи

старший солдат\_\_\_\_\_\_\_\_\_\_\_КОКУРА І.В.

**Перевiрив:** старший викладач кафедри 33

капітан\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ПРИЙМА О.О.

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 FTP-

сервері.

[amanni@artrsllc.com](mailto: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 [YYYY- MM-DD HH:MM:ss].

2022-07-12 00:30:03

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 байтів

10. Назва і версія операційної системи, що встановлена у жертви.

Microsofr Windows 7 Proffesional

11. Марка та модель процесора на ПК жертви.

Intel(R) Core(TM) i5-6400 CPU

12. Обліковий запис жертви для поштового клієнту.

Username: [honey@pot.com](mailto:honey@pot.com)

Password: honeypass356

13. Браузери з яких були викрадені облікові записи жертви.

Chrome, Firefox