**ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА**

**ІНФОРМАТИЗАЦІЇ**

КАФЕДРА КІБЕРБЕЗПЕКИ

**ЗВІТ**

про виконання практичної роботи:

з дисципліни «Управління кіберінцидентами та аналіз подій»

**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.

Розглянуто та ухвалено на засіданні кафедри кібербезпеки:

**Виконав:** курсант навчальної групи 314

солдат \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Сідненко Д.В.

10.04.2024

**Перевiрив:** викладач кафедри № 33

капітан\_\_\_\_\_\_\_\_\_\_\_ Прийма О.О

Київ – 2024

**Звіт TeslaAgent**

1. IP-адреса жертви. **192.168.100.14**
2. 2. IP-адреса зловмисника. **107.161.178.166**

3. Протокол (канал) що використано зловмисником для ексфільтрації

данних жертви.  **FTP (File Transfer Protocol)**

4. Ім’я хоста жертви. **USER PC**

5. Логін який використовувався зловмисником для аутентифікації на FTP-

сервері.

**amanni@artrsllc.com**

6. Пароль який використовувався зловмисником для аутентифікації на

FTP-сервері.

**=WY{9+?ae}qt**

1. Дата і час початку передачі викраденої інформації від жертви

**Arrival Time: Jul 12, 2022 00:30:03.778660000 Финляндия (лето)**

1. Назва файлу що був завантажений з ексфільтрованими даними.

**PW\_admin-USER-PC\_2022\_07\_11\_22\_30\_00.html**

10. Загальний об’єм інформації, що було викрадено у жертви.

**567 байт**

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

**Windows 7 Professional 3583.61 MB**

1. Марка та модель процесора на ПК жертви.

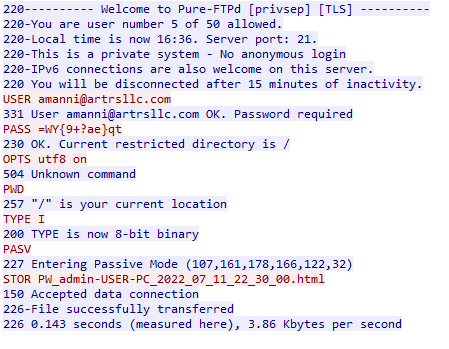
**: Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz**

13. Обліковий запис жертви для поштового клієнту.

**Username:honey@pot.com  
 Password:honeypass356**

14. Браузери з яких були викрадені облікові записи жертви.

**Chrome; Firefox**



Снимок экрана 2024-04-21 105300

