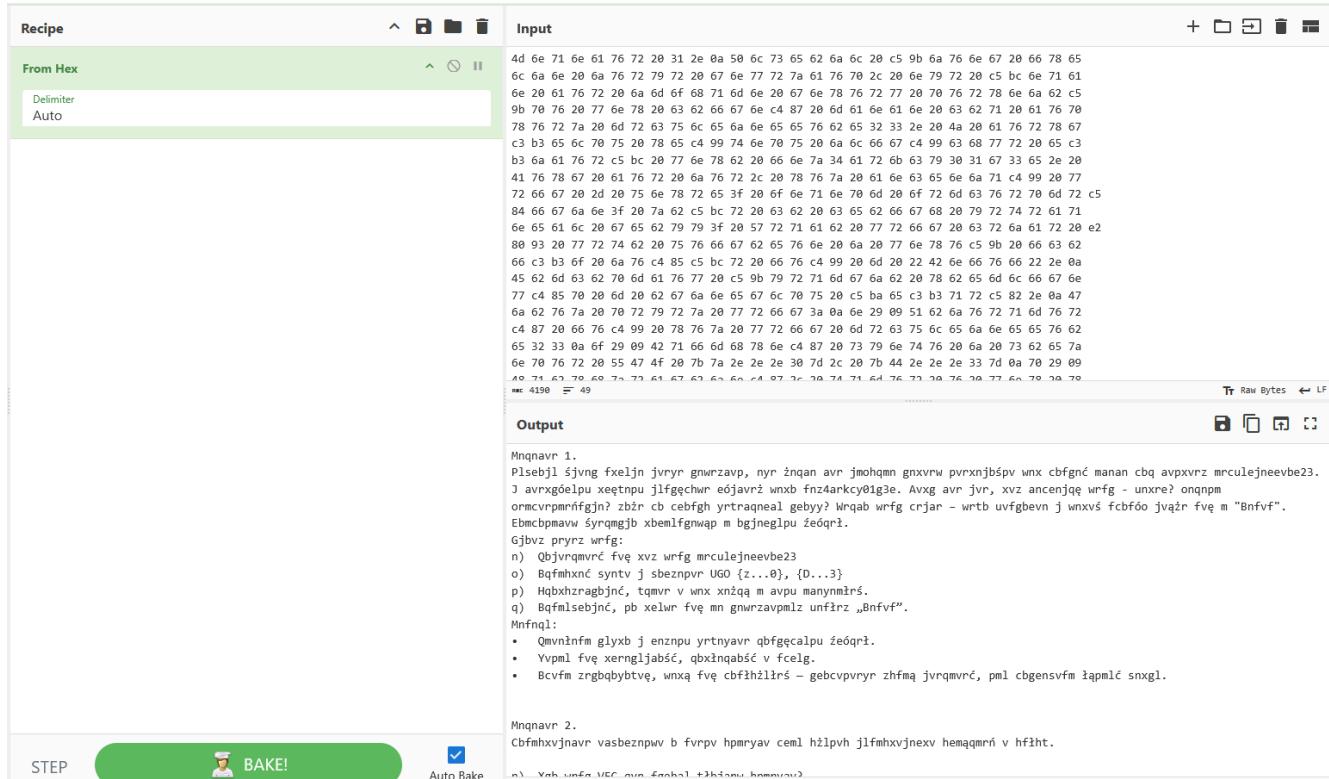


POLITECHNIKA WROCŁAWSKA  Wydział Informatyki i Telekomunikacji	Wydział: Informatyki i Telekomunikacji Kierunek: Cyberbezpieczeństwo Rok Akademicki: 2024/2025 Rok studiów, semestr: 2, 4 Grupa: 1 Termin: pon., 7:30
CBESI0053G Informatyka śledcza – Laboratorium 6	
Prowadzący: mgr inż. Adrian Florek	Autor: 1. Gerard Błaszczyk
Data wykonania ćwiczenia: 07.04.2025	
Data oddania sprawozdania: 13.04.2025	

1. Cel ćwiczenia

Wyszukiwanie informacji na temat użytkowników i urządzeń sieciowych za pomocą ogólnodostępnych narzędzi pasywnych.

2. Odszyfrowanie instrukcji laboratoryjnej



Rysunek 1: odkodowanie z formatu hex; narzędzie CyberChef

Szyfr Cezara - koder/dekoder online

Zakoduj lub rozkoduj wiadomość Szyfrem Cezara w zależności od wybranego przesunięcia.

Przesunięcie:

▼

Tekst:

Mnqnavr 1.
 Plsebjl šjvng fxeijn jvryr gnwrzavp, nyr žnqan
 avr jmohqmn gnxvrw pvrxnjbšpv wnx cbfgnć
 manan cbq apvxrz mrculejneevbe23. J
 avrxgöelpu xeętnpu jlfgčchwr eójavrž wnxb
 fnz4arkcy01q3e. Avxq avr jvr, xvz ancenjqq
 wrfg - unrex? ongnpm ormcavpmrifgjn?
 zbrz cb cebfgh yrtraqneq gebyy. Wraqb
 wrfg crjar - wrtb uvfgbevn j wnxv
 fcbbđo jvajr fvę m "Bnfvf". Ebmcbspmaw
 ſyrqngjč xbemlfgnwąp m bgjneglpu
 žeōqrł. Gjbzv pryzr wrfg:
 n) Objvrmwři fvę xvz wrfg mrculejneevbe23
 o) Bqfmhxnavr synty j sbeznpvū UGO {...}, {D...3}
 p) Hqbxhxrabjnjč, tqmnr v wnx xnžq m
 avpu manymlnř.
 q) Bqfmlsebjnjč, pb xelwr fvę mn
 gnwrzavpmz unfirz „Bnfvf”.
 Mnfnpl:
 • Omvninfm glyxb j enzunu yrtnyavr
 qbfgčalpu žeōqrł.
 • Yvpml fvę xerngljabsč,
 qbxiňqabšc w fcclg.
 • Bcvfm zrgbqbybtvę, wnxq fvę
 cbfžhžlrlś - gebcwpvryr
 zhfmq jvrqmvrč, pml
 cbgensvfm žapmlč snxgl.

Szyfr Cezara:

Zadanie 1.
 Cyfrowy świat skrywa wiele tajemnic, ale
 żadna nie wzbudza takiej ciekawości jak
 postać znana pod nickiem zephyrwarrior23.
 W niektórych kręgach występuje również
 jako sam4nexpl01t3r. Nikt nie wie, kim

Rysunek 2: rozszyfrowanie szyfrem cezara; skalkuluj.pl

2

Zadanie 1.

Cyfrowy świat skrywa wiele tajemnic, ale żadna nie wzbudza takiej ciekawości jak postać znana pod nickiem zephyrwarrior23. W niektórych kregach występuje również jako sam4nexpl01t3r. Nikt nie wie, kim naprawdę jest - haker? badacz bezpieczeństwa? może po prostu legendarny troll? Jedno jest pewne – jego historia w jakiś sposób wiąże się z "Oasis".

Rozpocznij śledztwo korzystając z otwartych źródeł.

Twoim celem jest:

- a) Dowiedzieć się kim jest zephyrwarrior23
- b) Odszukać flagi w formacie HTB {m...0}, {Q...3}
- c) Udokumentować, gdzie i jak każdą z nich znalazłeś.
- d) Odszyfrować, co kryje się za tajemniczym hasłem „Oasis”.

Zasady:

- Działasz tylko w ramach legalnie dostępnych źródeł.
- Liczy się kreatywność, dokładność i spryt.
- Opisz metodologię, jaką się posłużyłeś – tropicieli muszą wiedzieć, czy potrafisz łączyć fakty.

Zadanie 2.

Poszukiwanie informacji o sieci uczelni przy użyciu wyszukiarki urządzeń i usług.

- a) Kto jest ISP dla strony głównej uczelni?
- b) Jakie oprogramowanie serwerowe jest najczęściej występujące na PWR?
- c) Jaka najstarsza wersja oprogramowania serwerowego jest wciąż używana? Czy ma jakieś krytyczne podatności?
- d) Znajdź adres IP serwera gry.
- e) *Znajdź adresy IP konsoli do gier podpiętych do sieci uczelni.

W zadaniach używamy tylko narzędzi pasywnych!

Rysunek 3: jawną treść instrukcji

3. Realizacja zadań laboratoryjnych

Zadanie 1. Cyfrowy świat skrywa wiele tajemnic, ale żadna nie wzbudza takiej ciekawości jak postać znana pod nickiem zephyrwarrior23. W niektórych kregach występuje również jako sam4nexpl01t3r. Nikt nie wie, kim naprawdę jest - haker? badacz bezpieczeństwa? może po prostu legendarny troll? Jedno jest pewne – jego historia w jakiś sposób wiąże się z "Oasis".

Rozpocznij śledztwo korzystając z otwartych źródeł.

Twoim celem jest:

- a) Dowiedzieć się kim jest zephyrwarrior23

The screenshot shows a web browser displaying a resume. The title of the page is 'SAM4NEXPLO1T3R'. The resume is in Greek and English. It includes a profile picture of a person with blue hair, a name section with 'sam4nexpl01t3r' and 'ΕΠΙΣΚΕΨΗ ΣΕ ΠΡΟΦΙΛ', a 'Κοινή χρήση' section with the date 'Φεβρουαρίου 23, 2023', and a 'FIND MY CV HERE!' button. The main content area contains sections for 'Name', 'Education', 'Skills', and 'Work Experience'. The 'Name' section lists 'Name: Samantha "Zephyr" Williams', 'Email: samantha.zephyr.williams@gmail.com', 'Username: sam4nexpl01t3r', and 'Website: https://sam4nexpl01t3r.blogspot.com/2023/02/about-me.html'. The 'Education' section lists 'Bachelor of Science in Computer Science' from 'University of California, Los Angeles (UCLA)' with a graduation date of 'Graduated: May 2022'. The 'Skills' section lists proficiency in multiple programming languages (C++, Java, Python), experience in game development using Unity and Unreal Engine, strong analytical and problem-solving skills, excellent communication and collaboration abilities, familiarity with virtual reality hardware and software, and a proven track record of success in OASIS egg hunting. The 'Work Experience' section lists 'Game Developer'.

Rysunek 4: CV badanej osoby; sam4nexpl01t3r.blogspot.com

Z dokumentu można odczytać:

Name: Samantha “Zephyr” Williams

Email: samanthazephyrwilliams@gmail.com
Username: sam4nexpl01t3r

Tłumaczenie podsumowania: *Samantha „Sam” Williams* jest wysoko wykwalifikowaną absolwentką informatyki, pasjonującą się rzeczywistością wirtualną i grami. Mając doświadczenie w tworzeniu gier i historię sukcesów w polowaniu na jajka OASIS, Sam jest cennym uzupełnieniem każdego zespołu, który chce wprowadzać innowacje w przestrzeni wirtualnej.

b) Odszukać flagi w formacie HTB {m...0}, {Q...3}

Badając plik CV narzędziami do szczegółowej analizy plików znaleźć można:

```
(kali㉿kali)-[~/mnt/shared]
$ exiftool Samantha\ "Zephyr"\ Williams\ -\ CV\(1\).pdf
ExifTool Version Number      : 13.00
File Name                   : Samantha "Zephyr" Williams - CV(1).pdf
Directory                   :
File Size                    : 50 kB
File Modification Date/Time : 2025:04:13 14:36:10-04:00
File Access Date/Time       : 2025:04:13 14:38:10-04:00
File Inode Change Date/Time: 2025:04:13 14:36:53-04:00
File Permissions            : -rwxrwx—
File Type                   : PDF
File Type Extension         : pdf
MIME Type                   : application/pdf
Linearized                  : No
Page Count                  : 2
PDF Version                 : 1.5
Create Date                 : 0000:01:01 00:00:00
Producer                    :
Title                       :
Author                      : sam4nexpl01t3r
Creator                     :
Modify Date                 : 0000:01:01 00:00:00
Flag                         : HTB{met4d4t4_m1ghT_3xp053_1nf0}
Subject                     :
```

Rysunek 5: analiza CV narzędziem exiftool

Flaga: HTB{met4d4t4_m1ghT_3xp053_1nf0}

Wchodząc na profil użytkownika *sam4nexpl01t3r* na platformie „X” znaleźć można:



Rysunek 6: kod QR z profilu „X” użytkownika

Skaner QR

Wgrywać Skanowania QR code

Prześlij inny obraz

ZESKANOWANE ELEMENTY(1) BEEP Pobierz wszyst... Wyczyść ...

Nie Results

1 TXT: HTB{Qr_C0D35_4r3_n0T_th4t_s4f3}

Lista 50 RAW

Uwaga: Twoje skany pozostają prywatne — żadne dane nie są przechowywane na naszych serwerach; wszystko dzieje się w Twojej przeglądarce.

Rysunek 7: odkodowanie kodu QR; <https://qrscanner.net/pl>

Flaga: HTB{Qr_C0D35_4r3_n0T_th4t_s4f3}

- c) **Udokumentować, gdzie i jak każdą z nich znalazłeś.**

Obie strony na których znalazłem flagi są jedne z pierwszych, które pojawiają się po wpisaniu nazwy użytkownika w wyszukiwarkę. Przedmiot „Informatyka Śledcza” zobowiązuje do analizy plików odpowiednimi narzędziami, stąd znalezienie pierwszej flagi, druga nie była schowana szczególnie głęboko.

d) Odszyfrować, co kryje się za tajemniczym hasłem „Oasis”.

Według <https://github.com/supermedium/gunters-of-oasis> OASIS to akronim od: *Open and Super Immersive Simulation*

Zadanie 2. Poszukiwanie informacji o sieci uczelni przy użyciu wyszukiwarki urządzeń i usług.

a) Kto jest ISP dla strony głównej uczelni?

General Information	
Hostnames	pwr.edu.pl
Domains	PWR.EDU.PL
Country	Poland
City	Wrocław
Organization	Wroclaw Centre of Networking and Supercomputing
ISP	Wroclaw Centre of Networking and Supercomputing
ASN	AS8970

Rysunek 8: ISP - Wroclaw Centre of Networking and Supercomputing; shodan.io

b) Jakie oprogramowanie serwerowe jest najczęściej występujące na PWR?

Software Product:

- 133 WebSocket++
- 129 Linux
- 118 nginx
- 112 HTTPD
- 89 linux
- 79 apache
- 50 OpenSSH
- 47 Windows
- 45 HTTP API
- 44 windows
- 31 PHP
- 25 Postfix
- 23 Appweb
- 22 MySQL
- 20 openssh
- 18 Dovecot
- 15 AnyDesk
- 12 Envoy
- 10 AirTunes
- 10 BIG-IP LTM

More

Less

156.17.39.166

Linux WASK WROCMAN-EDU educational part of WASK network, Wrocław, Poland (8970) Lower Silesia, Poland

remote-access
_22/SSH 80/HTTP 443/HTTP

156.17.7.22 (informatyka.im.pwr.wroc.pl)

Debian Linux WASK WROCMAN-EDU educational part of WASK network, Wrocław, Poland (8970) Lower Silesia, Poland

jquery modernizr zurb-foundation
80/HTTP 443/HTTP

156.17.67.209 (gz-161.itcmp.pwr.wroc.pl)

Ubuntu Linux WASK WROCMAN-EDU educational part of WASK network, Wrocław, Poland (8970) Lower Silesia, Poland

alpine.js
80/HTTP 443/HTTP

156.17.7.47 (portal.im.pwr.edu.pl)

WASK WROCMAN-EDU educational part of WASK network, Wrocław, Poland (8970) Lower Silesia, Poland

80/HTTP 443/HTTP

156.17.7.27 (studuij.im.pwr.edu.pl)

Debian Linux WASK WROCMAN-EDU educational part of WASK network, Wrocław, Poland (8970) Lower Silesia, Poland

bootstrap grav jquery default-landing-page
22/UNKNOWN 80/HTTP 443/HTTP

156.17.9.40 (denali.kcrr.pwr.edu.pl)

Debian Linux WASK WROCMAN-EDU educational part of WASK network, Wrocław, Poland (8970) Lower Silesia, Poland

22/UNKNOWN 80/HTTP 222/UNKNOWN 443/HTTP 6667/UNKNOWN
8448/HTTP

Rysunek 9: *WebSocket++; censys.io*

c) **Jaka najstarsza wersja oprogramowania serwerowego jest wciąż używana? Czy ma jakieś krytyczne podatności?**

Najstarszą wersję jaką znalazłem to: *WebSocket++ 0.8.1*. Według security.snyk.io ta wersja jest narażona między innymi na ataki DoS, zalecane jest przejście do najnowszej wersji.

d) **Znajdz adres IP serwera gry.**

Nie udało mi się znaleźć takiego serwera, najpewniej jest to któreś urządzenie z podsieci: podsieci 156.17.228.0/24