

IT BIZTONSÁG

6. forduló



A kategória támogatója: EURO ONE
Számítástechnikai Zrt.

RENDELKEZÉSRE ÁLLÓ IDŐ:

60:00

Ismertető a feladathoz

A támadók a csatlományban található fenyegető üzenetet elhelyezték több workstationünk desktopján. A csapatoddal arra gyanakodtok, hogy a támadók nem voltak elég ügyesek a nyomok eltávolításakor, és hagytak apró morzsákat maguk után, amelyeket követve felfedhető a kilétük.

A fordulóhoz erősen ajánlott egy felhasználónév-kereső (pl. maigret) és egy metaadat-kezelő (pl. exiftool) program használata.

A forduló indítása előtt bizonyosodj meg róla, hogy az eszközeid megfelelően működnek és az elvárt outputot produkálják már ismert inputok esetében!

Felhasznált idő: 02:05/60:00

Elért pontszám: 0/90

1. feladat 0/10 pont

Mi a célpont hacker álneve, hacker-aliasa? (kis "m" betűvel kezdődő)

Válaszok

A helyes válasz:

movraxhax

Magyarázat

Az rtf fájlból nem törölte ki a célpont az Author taget, így látszik, mi volt a user fiók neve aki a fájlt elkészítette. Az Author tag pl. felfedhető a fájl Wordben megnyitásával, és azon belül a Fájl - Információ - Kapcsolódó személyek - Szerző szekcióban. Word nélkül is kideríthető az Author tag tartalma: szövegfájlként megnyitva az "\author" kulcsszóra keresve található meg, illetve az exiftool nevű metaadat-szerkesztő eszköz is kiírja nekünk az "exiftool message.rtf" parancs hatására.

2. feladat 0/20 pont

Mi a célpont álnevéhez közvetlenül kapcsolódó email címe?

Válaszok

A helyes válasz:

`movraxhax@protonmail.com`

Magyarázat

A felhasználónév birtokában a következő logikus lépés egy szkennelés indítása, hogy kiderítsük, hány publikus weboldalon van beregisztrált fiók ilyen fióknévvel. Ezt a maigret nevű eszközzel könnyedén megtehetjük:

```
$ maigret movraxhax
```

Az így kapott találatokból bennünket elsősorban a GitHub fiók érdekel:

<https://github.com/movraxhax>

A GitHubra látogatva láthatunk pár repót, amit a célpontunk forkolt más repositorykból, illetve láthatunk egy olyat is, ami teljesen saját készítésű:

<https://github.com/movraxhax/misc-exiftool-tricks>

Ebben a saját kis repóban érdemes elkezdni a keresést az email cím után - mint ismeretes, minden git commithoz tartozik egy szerző, akit a neve és email címe azonosít.

Amennyiben a célpont a commitot nem a GitHub felületén hozta létre, hanem lokálisan parancssorból, elképzelhető, hogy benne hagyta a fiókhoz tartozó email címét a git configban és ezáltal a GitHubra felkerült commitokban is.

Hogy megnézhessük a commitot létrehozó szerző email címét, vagy leklónozzuk lokálisan a repót és a "git log" paranccsal lekérjük a commitokat szerzői információkkal, vagy révén hogy a GitHubon vagyunk, egy kis trükkkel a GitHubtól is le lehet kérni a nyers commit/diff információt. Ehhez csak a legutolsó commitot kell megnyitnunk, és a címsorban hozzáírunk az URL végéhez a ".patch" kiterjesztést:

<https://github.com/movraxhax/misc-exiftool-tricks/commit/899c1aea199812922cf145956d8bc06fd6c43b46.patch>

3. feladat 0/10 pont

Mi a célpont másik online felhasználóneve? (kis "c" betűvel kezdődő)

Válaszok

A helyes válasz:

czarnyh4t

Magyarázat

A célpont GitHub profilján böngészve találhatunk egy, a filmweb.pl weboldalhoz kapcsolódó API repót is. Ha visszatekintünk a maigret találataira, azok között is jelen volt a filmweb.pl weboldal, ezért az a következő állomásunk:

<https://www.filmweb.pl/user/movraxhax>

A célpont profiljának leírásában megtaláljuk a másik általa használt álnevet:

"a.k.a. czarnyh4t"

4. feladat 0/20 pont

Melyik városban él a célpont?

Válaszok

A helyes válasz:

Poznań

Poznan

Poznań (Szamotulska 6, 60-366 Poznań, Poland)

Magyarázat

Az új felhasználónévvel felfegyverkezve érdemes újrafuttatni a maigret scant. A szokásos falszpozitív találatok mellett kettő olyan weboldal is felbukkan, amelyek érdekesek lehetnek számunkra:

- <https://www.wykop.pl/ludzie/czarnyh4t/>

- <https://czarnyh4t.tumblr.com/>

A wykop.pl egy lengyel közösségi oldal. A célpontunk profilján és posztjai között nem igazán találunk új, bármilyen hasznosítható információt, bár tény, hogy furcsa beszélgetésbe keveredett pár veteránnal az oldalról. :)

Az egyik posztjában megemlíti a célpont, hogy a tumblr egy érdekes oldal. Mivel a maigret talált fiókot azon a platformon is, oda vezet az utunk.

A posztokat végigböngészve a célpont kedvenc zenéin és érdeklődési körein kívül találhatunk még egy linket a flickr profiljára is:

<https://www.flickr.com/people/193996033@N07/>

A flickr profilon csak egy darab kép található:

<https://flickr.com/photos/193996033@N07/51503243063/in/dateposted-public/>

A célpont megemlíti a leírásban, hogy a városában készült a kép. A GitHub fiókban található sok exiftool utalás most jön jól igazán, ugyanis a képet eredeti formátumban letöltve (jobb alsó sarokban letöltés ikon -> Original) és arra az exiftoolt a repoban található paranccsal futtatva megkapjuk a kép helyének konkrét koordinátáit:

\$ exiftool -GPSPosition 51503243063_9dcd90fe48_o.jpg

GPS Position : 52 deg 24' 18.93" N, 16 deg 52' 53.95" E

A koordinátákat a Google Mapsbe beírva láthatjuk, hogy a kép Poznań városában készült:

<https://www.google.com/maps/place/52%C2%B024'18.9%22N+16%C2%B052'54.0%22E/>

5. feladat 0/20 pont

Mi a célpont teljes polgári neve?

Válaszok

A helyes válasz:

Jerzy Łysiak

Jerzy Lysiak

Lysiak Jerzy

Łysiak Jerzy

Jerzy_Lysiak

Magyarázat

A fotó alatti leírásban egy elrejtett Twitter fióknévről is szó esik. Itt is segít a célpont GitHub repója, ugyanis két olyan toolt is forkolt, amelyekkel zero-width space enkódolt tartalmat lehet kiszedni ártatlannak tűnő normál szövegből:

<https://github.com/movraxhax/zwsp-steg-js>

<https://github.com/movraxhax/zero-width-detection>

A null-hosszúságú szóközökkel és egyéb non-printing karakterekkel való szöveg-elrejtésről gyorstalpaló itt található:

<https://medium.com/@umpox/be-careful-what-you-copy-invisibly-inserting-usernames-into-text-with-zero-width-characters-18b4e6f17b66>

A fotó leírásában a két külön sor a két külön toolnak készült. A felsőbb sort a zwsp-steg-js vagy zwsp-steg-py toolok segítségével lehet dekódolni - a JavaScriptes repóban a demó linkjét updateelte a célpont egy Wayback Machine által lementettre, így nem kell egyik toolt sem letölteni és lokálisan futtatni ahhoz, hogy a szövegből kiszedhessük a rejtett tartalmat:

<https://web.archive.org/web/20210320114410/https://offdev.net/demos/zwsp-steg-js>

A Decoding szekció alatti Message mezőbe illesztve a szöveget könnyedén kihámozható a rejtett Twitter handle.

A másik sorból a zero-width-detection tool segítségével dekódolhatjuk a Twitter felhasználónevet, ebben az esetben csak szimplán beillesztjük a még élő demo oldal 3-as számú mezőjébe:

<https://www.umpox.com/zero-width-detection/>

Bármelyik toolt is használjuk, végül a célpont Twitter fiókja a jutalmunk:

https://twitter.com/Jerzy_Lysiak

A Twitter fiók legtetején a profilkép alatt megtaláljuk a célpont teljes nevét:

Jerzy Łysiak

6. feladat 0/10 pont

Mi a célpont személyes email címe?

Válaszok

A helyes válasz:

jurek.lsk@interia.pl

Magyarázat

Magyarázat: egy utolsó social média fiók átfésülésre van szükség az email cím megtalálásához.


A tweeteket elnézegetve találhatunk egyet, amelyen a célpont büszkén dicsekszik az új névjegykártya-dizájnival:

https://twitter.com/Jerzy_Lysiak/status/1440965651959631872/photo/1

A képen látható névjegykártyáról leolvasható a személyes email cím.

KESZITETTE

Megjelenés

 Világos 