

[PROBLEMA 1] Johnny... Crypto

Agentul Johnny English a plecat într-o nouă aventură! În ultima sa misiune, a primit de la MI6 o aplicație Windows *CTF1.exe* (obținută de Agentul 000 într-o misiune recentă în Rusia, împreună cu alte fișiere binare codate) din linia de comandă se poate apela în mai multe moduri, după cum urmează:

- *CTF1.exe -f <file>* (e.g. *CTF1.exe -f demo.dat*)
 - aplicația se știe că prelucrează cumva fișierul text dat în linia de comandă, returnând o informație despre care nu se știe nimic

Misiunea 1: Agentul English a aflat de la colegul său că aceeași aplicație a fost folosită pentru a encoda un fișier codat (***binary1.dat***) care se presupune că ar conține, printre altele, codurile nucleare de la rachetele folosite de marina rusească – și deci este imperativ necesar să decodifice conținutul acestui fișier, pentru a evita un posibil dezastru nuclear. Misiunea voastră este să-l ajutați să decodifice acest conținut, folosind orice mijloc aflat la dispoziția voastră, și să identificați aceste coduri.

Misiunea 2: De asemenea, Agentul 000 a observat codarea unui fișier ***binary2.dat*** cu o nouă opțiune din linia de comandă, pentru aceeași aplicație *CTF1.exe*. Prin tehnicile sale impecabile, agentul Johnny English a descoperit încă un mod de execuție pentru binarul primit. Mai exact, este vorba despre cel de jos:

- *CTF1.exe -c <file>*
 - Aplicația și în acest caz prelucrează datele din fișierul text transmis ca și argument, afișându-le pe ecran într-o nouă formă codată, despre care iarăși nu se știe nimic.

Se presupune că serviciile secrete ruse ar fi folosit acest mod pentru binarul ***binary2.dat*** menționat anterior. Nu se știe dacă metoda folosită este identică sau nu cu cea anterioară sau nu, dar pentru că fișierul *binary2.dat* trebuie neapărat să fie decodificat

Misiunea 3: În lupta sa continuă și neînfricată cu lumea rece a spionajului cibernetic, Agentul Johnny English a descoperit o a treia posibilitate de a folosi aplicația suspicioasă. Ea este redată mai jos:

- *CTF1.exe -x <file>*
 - Se pare că aplicația și în acest caz prelucrează datele din fișierul text transmis ca și argument, afișându-le pe ecran într-o formă codată, despre care, ca de obicei, nu se știe nimic.

Un al treilea fișier codat, ***binary3.dat***, a fost furnizat de către colegul Agentul 000, iar misiunea voastră este să încercați să îl descifrați, pe lângă celelalte două. Oricare din aceste fișiere ar putea conține cheia către rachetele nucleare și ar putea preveni un dezastru!

Barem de punctare:

Misiunea 1: (30p)

- a) identificare algoritm de criptare (Base64) – 10p
- b) decriptarea fișierului și identificarea flag-ului – 10p
- c) includerea de screenshot-uri relevante – 10p

```
1 Welcome to IT*FEST*2020!
2
3 We're excited to have you here - and we're sure you will enjoy the challenges!
4
5 ~Stay safe & enjoy the fun!
6 Agent 000 @ IT Fest 2020
7
8 P.S.: There's no codes in here. But... they're hidden somewhere in here!
9
10 Motto: "When the salt is sour, the whole world sweetens up!"
```

Misiunea 2: (60p)

- a) identificarea criptării cu Base64 a fișierului *binary2.dat* – 10p
- b) decriptarea fișierului din Base64 într-un fișier binar *binary2_2.dat* – 10p
- c) identificarea algoritmului de criptare pentru noul fișier *binary2_2.dat* (cifru aditiv/XOR) – 10p
- d) identificarea cheii potrivite (fie prin observații empirice, fie prin forță brută → cheia 'X') – 10p
- e) decriptarea fișierului *binary2_2.dat* folosind cheia găsită – 10p
- f) identificarea flag-ului în fișierul *binary2_2.dat* decriptat – 10p

```
1 Congratulations for making it this far, Agent Johnny English!
2
3 This is very impressive. We're sure you're on the right track.
4
5 Don't worry, the codes are ALMOST at your fingertips.
6
7 ~The guys at IT*FEST :-)
```

Misiunea 3: (60p)

- a) identificarea criptării cu Base64 a fișierului *binary3.dat* – 10p
- b) decriptarea fișierului din Base64 într-un fișier binar *binary3_2.dat* – 10p
- c) identificarea algoritmului de criptare pentru noul fișier *binary3_2.dat* (cifru aditiv/XOR cu cheie variabilă) – 10p
- d) identificarea cheii potrivite (fie prin observații empirice, fie prin forță brută) ca fiind 'sour' (vezi misiunea 1) – 10p
- e) decriptarea fișierului *binary3_2.dat* folosind cheia găsită – 10p
- f) identificarea flag-ului în fișierul *binary3_2.dat* decriptat – 10p

```
1 Amazing work!!!
2
3 Your nuclear codes are: WAR*@*IT*FEST*2020
```

Total: 150p

[PROBLEMA 2] Engineering with Johnny

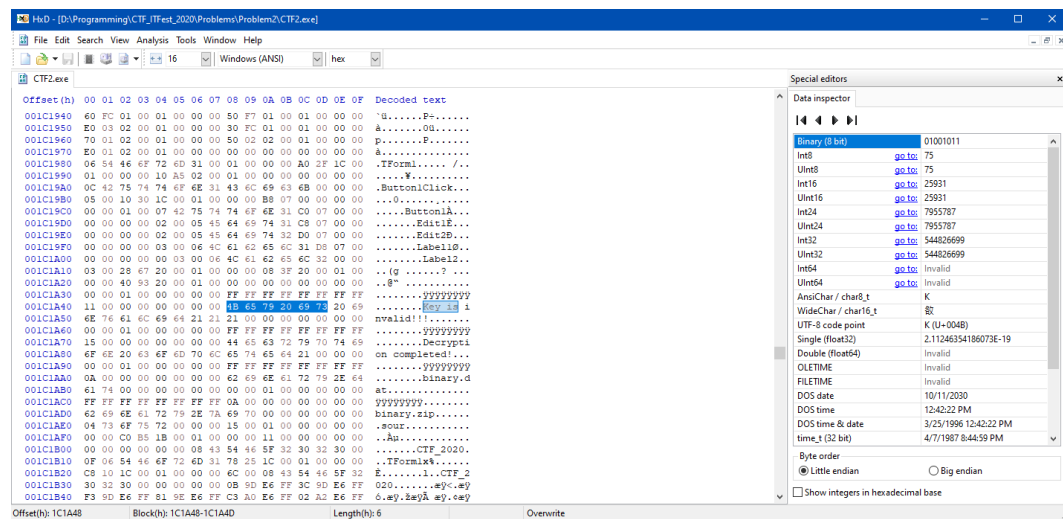
Ceea ce se știe până acum:

- Cerințele pentru voi sunt așadar următoarele:

Misiunea 2: Acum că misiunea 1 este, sperăm, completată cu succes, putem trece la misiunea 2. Aici, Johnny își propune să facă aplicația să accepte orice combinație de date, indiferent dacă este sau nu validă cheia introdusă de utilizator.

Barem de punctare:

a) identificarea corectă a unui editor hexa (e.g. HxD) pentru editarea fișierului binar – 10p



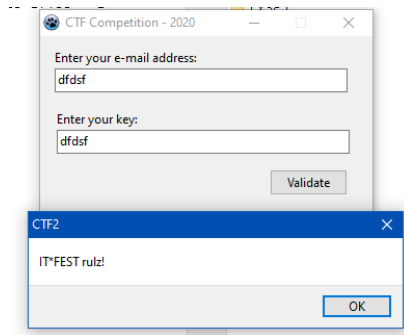
b) identificarea mesajului, cu ajutorul editorului hexa, în secțiunea de cod a executabilului – 10p

c) modificarea mesajului, cu ajutorul editorului hexa, în secțiunea de cod a executabilului – 10p

```
1C1A40: 11 00 00 00 00 00 00 00 |.....
1C1A48: 49 54 2A 46 46 53 54 20 |IT*FEST
1C1A50: 72 75 6C 7A 21 20 20 20 |rulz!
1C1A58: 20 00 00 00 00 00 00 00 |.....
1C1A60: 00 00 01 00 00 00 00 00 |.....
```

```
1C1A40: 11 00 00 00 00 00 00 00 |.....
1C1A48: 4B 65 79 20 69 73 20 69 |Key is i
1C1A50: 6E 76 e1 6C 69 64 21 21 |Invalid!!
1C1A58: 21 00 00 00 00 00 00 00 |!.....
1C1A60: 00 00 01 00 00 00 00 00 |.....
```

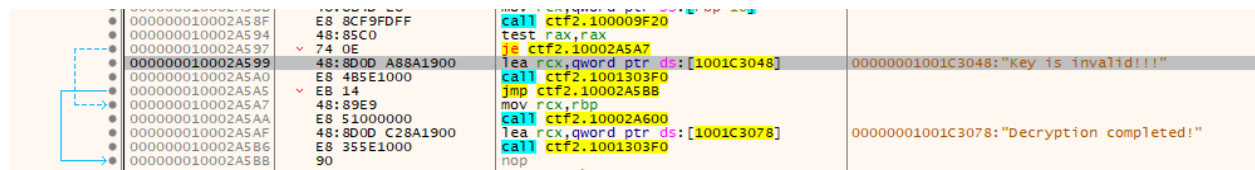
d) verificarea funcționalității și includerea de screenshot-uri relevante – 10p



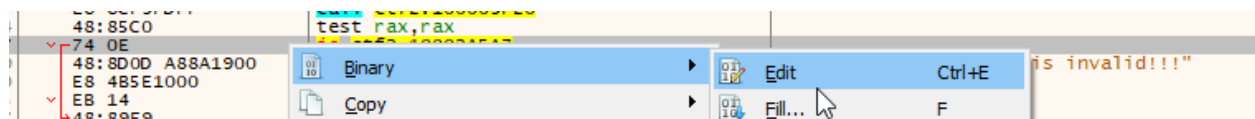
Misiunea 2:

a) identificarea corectă a unui debugger x64 (e.g. x64dbg) pentru execuția și dezasamblarea fișierului executabil – 10p

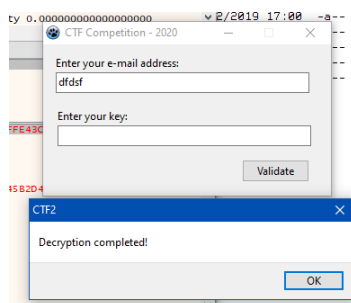
b) identificarea metodei/metodelor unde se realizează validarea cheii cu ajutorul debuggerului și a debugging-ului – 10p



c) înlocuirea în codul assembly al programului, a instrucțiunilor pentru obfuscarea validării (e.g. jz vs jnz) – 10p

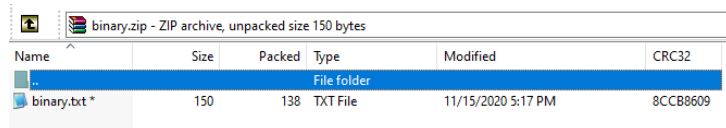


d) verificarea funcționalității și includerea de screenshot-uri relevante – 10p



Misiunea 3:

a) identificarea, ca urmare a verificării funcționalității de la c), a fișierului produs la decriptare și clasificarea lui ca fișier ZIP parolat – 10p



Name	Size	Packed	Type	Modified	CRC32
..			File folder		
binary.txt *	150	138	TXT File	11/15/2020 5:17 PM	8CCB8609

b) identificarea corectă a tool-urilor necesare (e.g. fcrackzip) pentru atacurile de tip forță brută împotriva fișierelor ZIP parolate – 10p

c) realizarea unui atac de tip forță brută asupra fișierului ZIP parolat folodind tool-urile identificate – 10p

d) găsirea parolei 'CTF' pentru fișierul ZIP parolat și identificarea flag-ului în fișierul din arhiva ZIP – 10p

```
1 Excellent work, lads!  
2  
3 IT*FEST 2020 is congratulating you for yet another challenge overcome! Good job!  
4  
5 ~Stay tuned, there's more exciting stuff!
```

Total: 120p

MAXIM POSIBIL: 270 puncte