

SUPERCOMPUTER

SECTALKS CTF[0x01] SOLUTION

Lets fire this dude up



A terminal window with a dark background and light green text. The window title bar shows 'File Edit View Go Bookmarks Help'. The prompt is 'aazzbl azter@aazzbl azter-virtual-ma'. The command entered is './supercomputer'. The output is '... Welcome To SuPeRcOmPuT3r...' followed by '... We are PERFORMANCE Driven...'. Below the output is a directory listing showing folders: Home, Desktop, Documents, Music, Pictures, Videos, and Downloads. To the right of the listing are three icons labeled 'ELFkickers', 'Music', and 'Pictures'.

```
File Edit View Go Bookmarks Help
aazzbl azter@aazzbl azter-virtual-ma
./supercomputer
... Welcome To SuPeRcOmPuT3r...
... We are PERFORMANCE Driven...
Home Desktop Documents Music Pictures Videos Downloads
ELFkickers Music Pictures
```

Alght sweet

- So as always, I'll fire up kaaza pro
- Search for supercomputer
- `supercomputer.crack.100.percent.working.not.malware.arj`

azzbl azter@azzbl azter-virtual-machine ~/Desktop \$
arj e supercomputer.crack.100.percent.working.no
t.malware.arj

ARJ32 v 3.10, Copyright (c) 1998-2004, ARJ Softwa
re Russia. [10 May 2013]

Processing archive: supercomputer.crack.100.perce
nt.working.not.malware.arj

Archive created: 2014-01-22 08:35:44, modified: 2
014-01-22 08:35:44

Extracting MadPatcher

1 file(s)

OK

DEMO HERE

Will it work?!

azzbl azter@azzbl azter-vi rtual -machi ne ~/

./supercomputer

... Welcome To SuPeRcOmPuT3r...

... We are PERFORMANCE Driven...

flag : sup3ri sFAST!

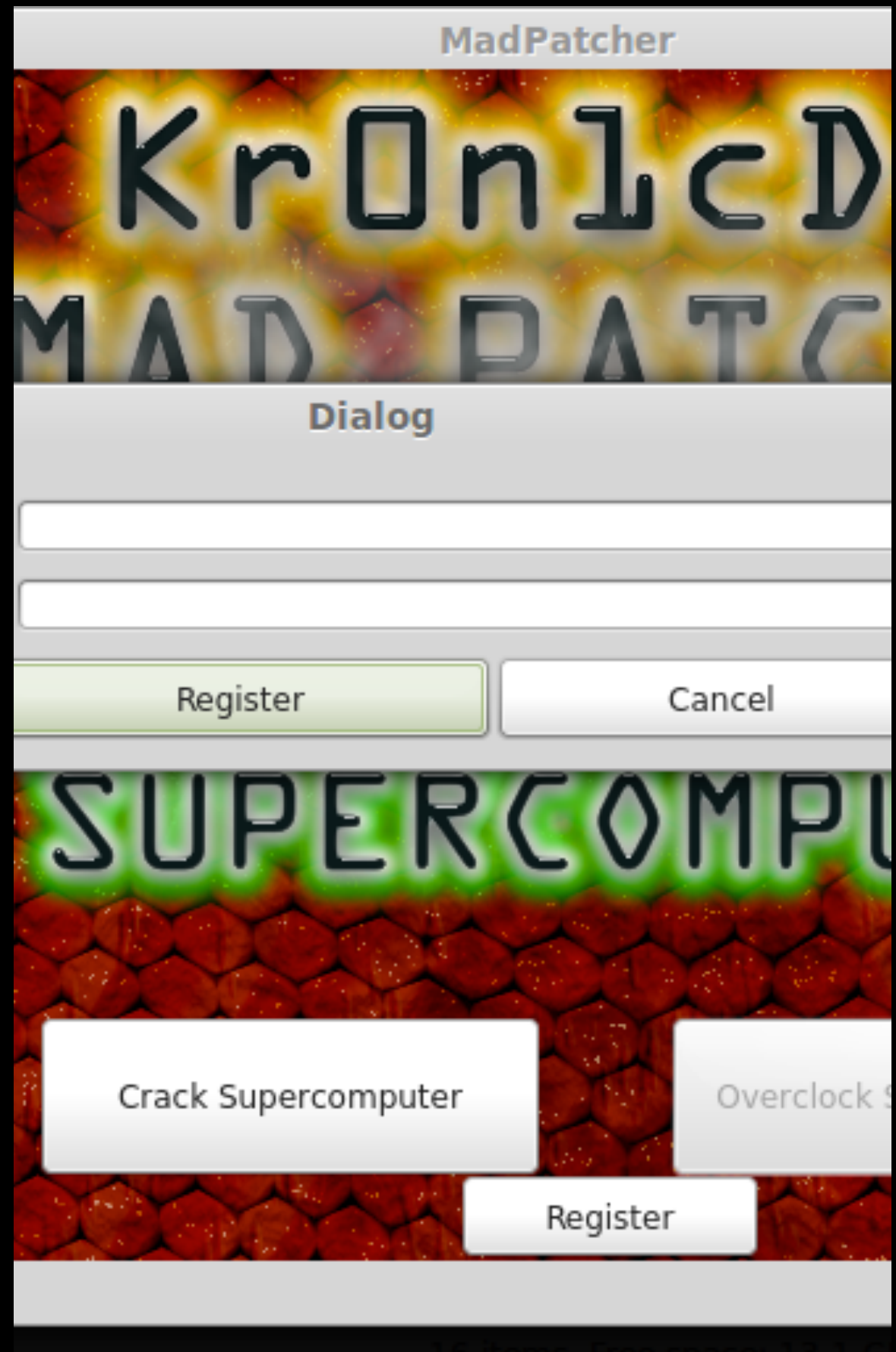
azzbl azter@azzbl azter-vi rtual -machi ne ~/

Hell yeah

Haxed

But... Its slow :(I wanna OC
this thing..

It wants a serial, what?



SECTALKS CTF 0x02

Generate a serial for your name

If you build a keygen with rad music I will buy you a beer.

CTF Walkthrough

```
000000000000400ae0 EB0E      jmp      0x400af0
; Basic Block Input Regs: r13 - Ki
000000000000400ae2 4883C301      add      rbx, 0x1
000000000000400ae6 4C39EB        cmp      rbx, r13
000000000000400ae9 7505          jne      0x400af0
; Basic Block Input Regs: <nothing>
000000000000400aeb BB00000000    mov      ebx, 0x0
; Basic Block Input Regs: rbx r12 -
000000000000400af0 4C39E3        cmp      rbx, r12
000000000000400af3 75ED          jne      0x400ae2
; Basic Block Input Regs: <nothing>
000000000000400af5 48C78508FFFFFF90E4000      mov      qword [ss:rbp-
```

00000400ae2	4883C301	add	rbx, 0x
00000400ae6	4C39EB	cmp	rbx, r1
00000400ae9	7505	jne	0x400af
00000400aeb	BB00000000	mov	ebx, 0x
00000400af0	4C39E3	cmp	rbx, r1
00000400af3	74ED	jbe	0x400ae
00000400af5	48C78508FFFFFFFF90E4000	mov	qword [s
00000400b00	48C78510FFFFFFFFB0E4000	mov	qword [s
00000400b0b	48C78518FFFFFFFFD0E4000	mov	qword [s

ONE BYTE

LEET

TOO SLOW

```
                                ; Basic Block Input Regs: <noth:
                                __plt__sleep:
000000000000400570 FF25B21A2000                                jmp          qword [ds:
                                ; endp
000000000000400576 6805000000                                push         0x5
00000000000040057b E990FFFFFF                                jmp          0x400510
                                ;
                                ; Segment .text
                                ;
```

```

===== B E G I N   O F   P R O C E D U R E =====
; Basic Block Input Regs: rsp
__plt__sleep:
0000000000400570 C3          ret
; endp
0000000000400571          db          0x25
0000000000400572          db          0xb2

```

ONE BYTE

FAST NOW

“Type a quote here.”

– *Peter Hannay*