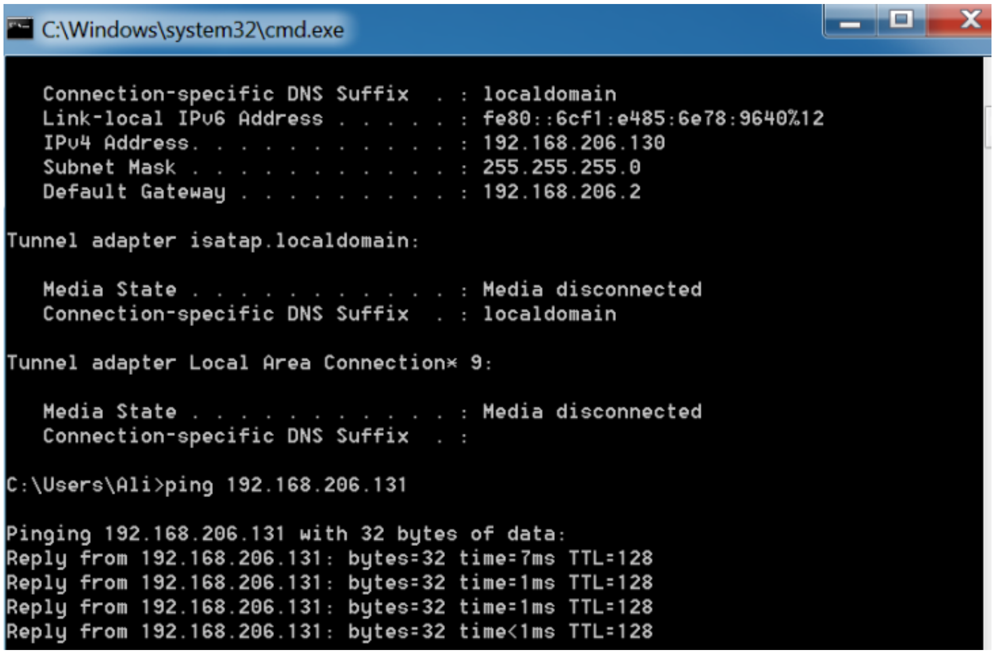
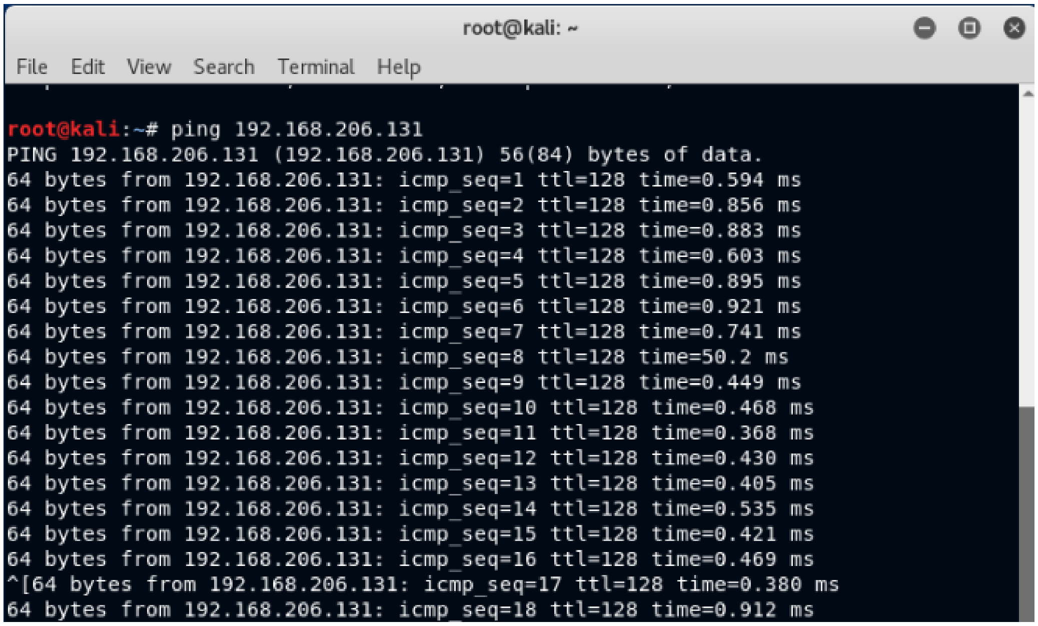
محمد علی عرب یزدی 9431046 بسمه تعالی بخش اول

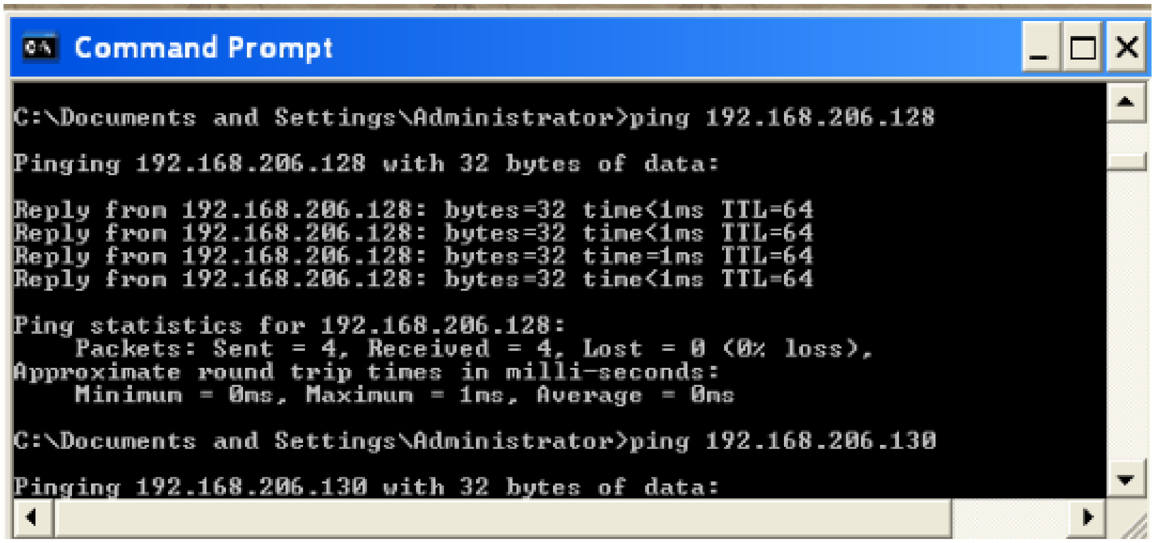
مرحله اول:



```
   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::6cf1:e485:6e78:9640%12
   IPv4 Address. . . . . . . . . . . : 192.168.206.130
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.206.2

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain

Tunnel adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Ali>ping 192.168.206.131

Pinging 192.168.206.131 with 32 bytes of data:
Reply from 192.168.206.131: bytes=32 time=7ms TTL=128
Reply from 192.168.206.131: bytes=32 time=1ms TTL=128
Reply from 192.168.206.131: bytes=32 time=1ms TTL=128
Reply from 192.168.206.131: bytes=32 time<1ms TTL=128
```



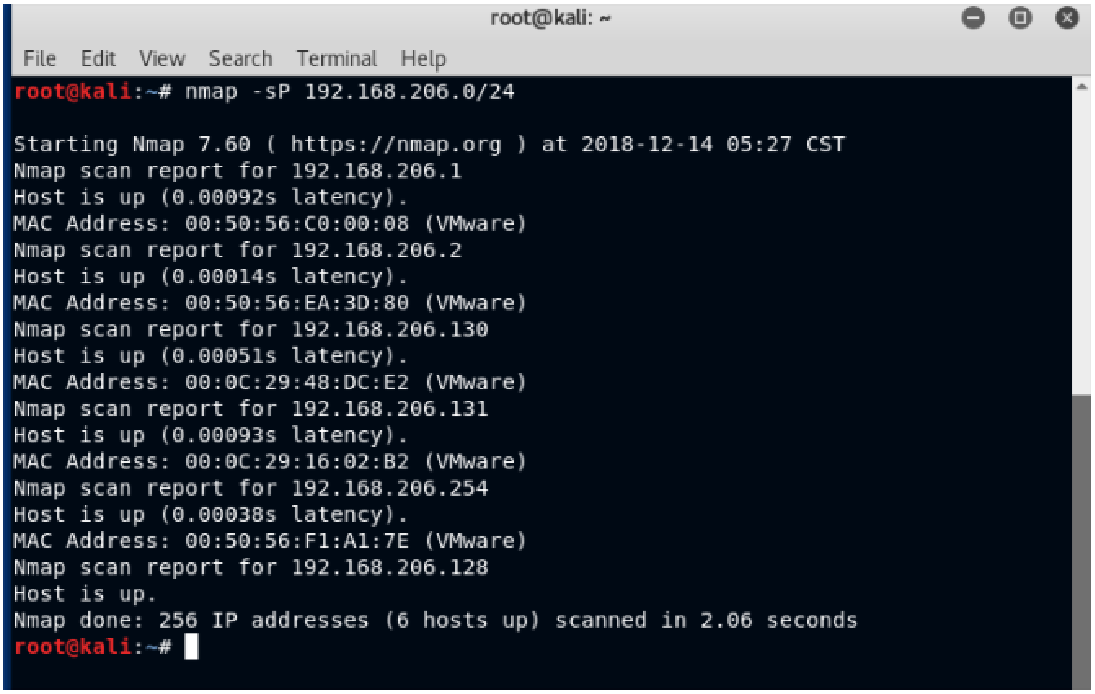
```
root@kali:~# ping 192.168.206.131
PING 192.168.206.131 (192.168.206.131) 56(84) bytes of data.
64 bytes from 192.168.206.131: icmp_seq=1 ttl=128 time=0.594 ms
64 bytes from 192.168.206.131: icmp_seq=2 ttl=128 time=0.856 ms
64 bytes from 192.168.206.131: icmp_seq=3 ttl=128 time=0.883 ms
64 bytes from 192.168.206.131: icmp_seq=4 ttl=128 time=0.603 ms
64 bytes from 192.168.206.131: icmp_seq=5 ttl=128 time=0.895 ms
64 bytes from 192.168.206.131: icmp_seq=6 ttl=128 time=0.921 ms
64 bytes from 192.168.206.131: icmp_seq=7 ttl=128 time=0.741 ms
64 bytes from 192.168.206.131: icmp_seq=8 ttl=128 time=50.2 ms
64 bytes from 192.168.206.131: icmp_seq=9 ttl=128 time=0.449 ms
64 bytes from 192.168.206.131: icmp_seq=10 ttl=128 time=0.468 ms
64 bytes from 192.168.206.131: icmp_seq=11 ttl=128 time=0.368 ms
64 bytes from 192.168.206.131: icmp_seq=12 ttl=128 time=0.430 ms
64 bytes from 192.168.206.131: icmp_seq=13 ttl=128 time=0.405 ms
64 bytes from 192.168.206.131: icmp_seq=14 ttl=128 time=0.535 ms
64 bytes from 192.168.206.131: icmp_seq=15 ttl=128 time=0.421 ms
64 bytes from 192.168.206.131: icmp_seq=16 ttl=128 time=0.469 ms
^[64 bytes from 192.168.206.131: icmp_seq=17 ttl=128 time=0.380 ms
64 bytes from 192.168.206.131: icmp_seq=18 ttl=128 time=0.912 ms
```



```
C:\Documents and Settings\Administrator>ping 192.168.206.128

Pinging 192.168.206.128 with 32 bytes of data:

Reply from 192.168.206.128: bytes=32 time<1ms TTL=64
Reply from 192.168.206.128: bytes=32 time<1ms TTL=64
Reply from 192.168.206.128: bytes=32 time=1ms TTL=64
Reply from 192.168.206.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.206.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Documents and Settings\Administrator>ping 192.168.206.130

Pinging 192.168.206.130 with 32 bytes of data:
```

مرحله دوم:

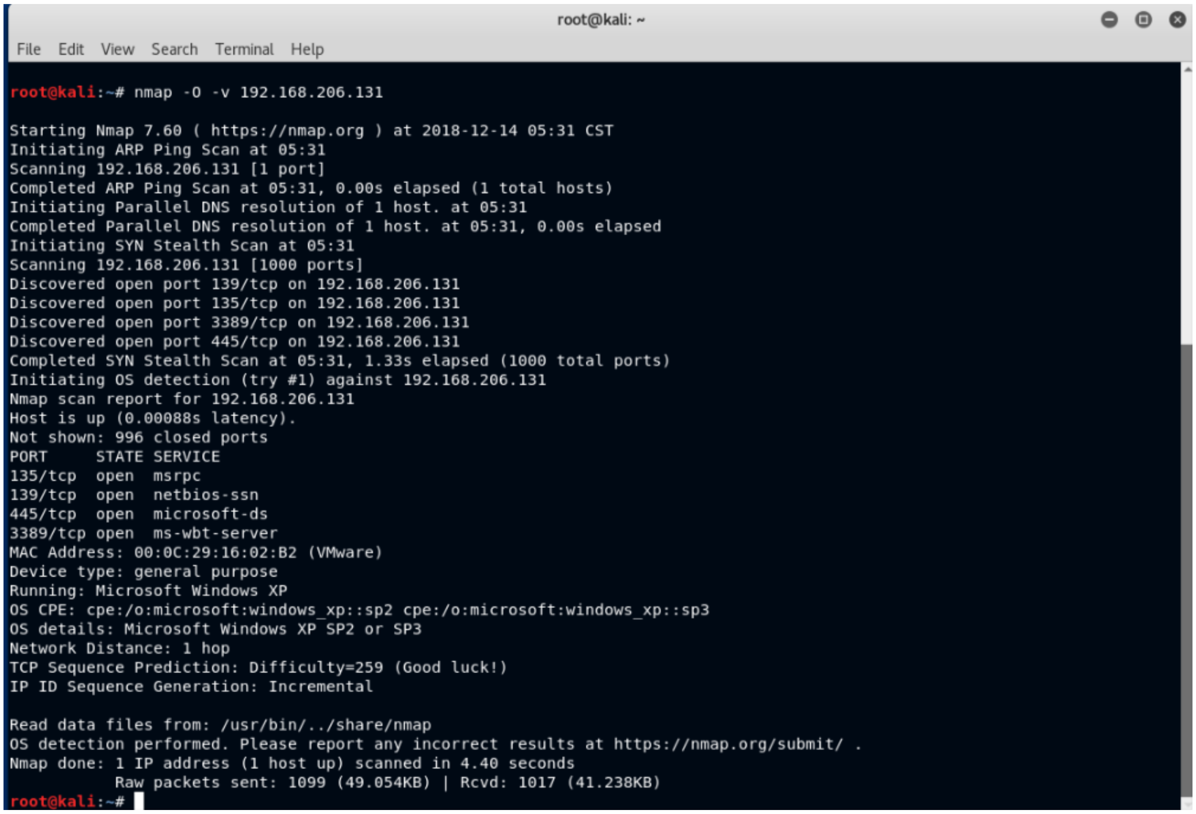
پیدا کردن سیستمهای موجود در شبکه



```
root@kali:~# nmap -sP 192.168.206.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-14 05:27 CST
Nmap scan report for 192.168.206.1
Host is up (0.00092s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.206.2
Host is up (0.00014s latency).
MAC Address: 00:50:56:EA:3D:80 (VMware)
Nmap scan report for 192.168.206.130
Host is up (0.00051s latency).
MAC Address: 00:0C:29:48:DC:E2 (VMware)
Nmap scan report for 192.168.206.131
Host is up (0.00093s latency).
MAC Address: 00:0C:29:16:02:B2 (VMware)
Nmap scan report for 192.168.206.254
Host is up (0.00038s latency).
MAC Address: 00:50:56:F1:A1:7E (VMware)
Nmap scan report for 192.168.206.128
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.06 seconds
root@kali:~#
```

مرحله سوم:

-شناسایی سیستم عاملها:

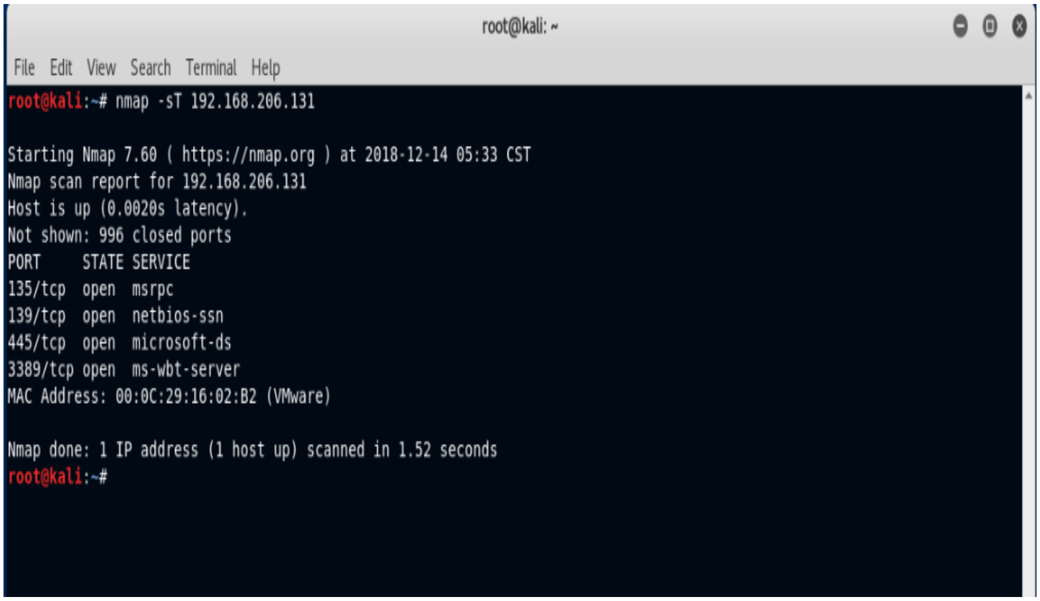


```
root@kali:~# nmap -O -v 192.168.206.131

Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-14 05:31 CST
Initiating ARP Ping Scan at 05:31
Scanning 192.168.206.131 [1 port]
Completed ARP Ping Scan at 05:31, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:31
Completed Parallel DNS resolution of 1 host. at 05:31, 0.00s elapsed
Initiating SYN Stealth Scan at 05:31
Scanning 192.168.206.131 [1000 ports]
Discovered open port 139/tcp on 192.168.206.131
Discovered open port 135/tcp on 192.168.206.131
Discovered open port 3389/tcp on 192.168.206.131
Discovered open port 445/tcp on 192.168.206.131
Completed SYN Stealth Scan at 05:31, 1.33s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.206.131
Nmap scan report for 192.168.206.131
Host is up (0.00088s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:16:02:B2 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.40 seconds
           Raw packets sent: 1099 (49.054KB) | Rcvd: 1017 (41.238KB)
root@kali:~#
```

Nmap این کار را استفاده از tcp/ip fingerprint انجام میدهد.

Nmap تعدادی بسته tcp و udp به مقصد میفرستد و بیت های پاسخ را بررسی میکند .

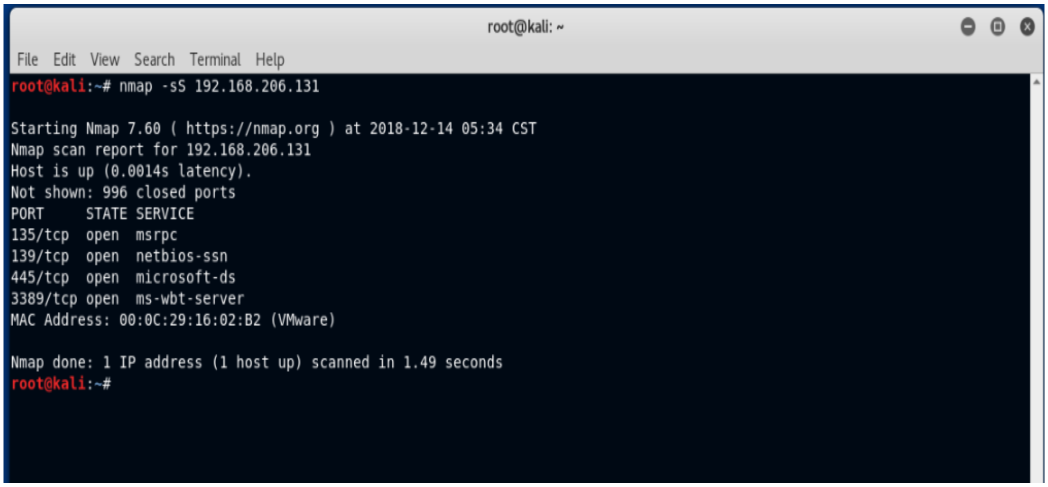
: Full connect scan-



```
root@kali:~# nmap -sT 192.168.206.131

Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-14 05:33 CST
Nmap scan report for 192.168.206.131
Host is up (0.0020s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:16:02:B2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds
root@kali:~#
```

در nmap tcp connection، nmap از شبکهای که بر روی آن سوار است درخواست برقراری ارتباط با مقصد با استفاده از فرستادن سیستم کال connect را میکند. مشکل این نوع ارتباط این است که اتمام آن طول میکشد. از طرف دیگر احتمال این که مقصد اجازه ارتباط را بدهد بیشتر است زیرا این نوع ارتباط مانند ارتباط کاربردهایی مثل ارتباط web browserها است.

-Stealth scan:



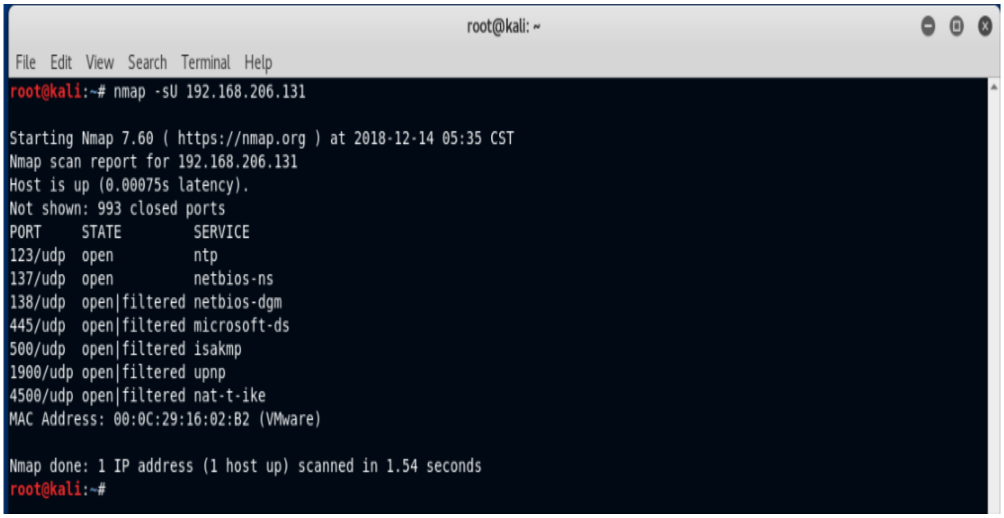
```
root@kali:~# nmap -sS 192.168.206.131

Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-14 05:34 CST
Nmap scan report for 192.168.206.131
Host is up (0.0014s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:16:02:B2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
root@kali:~#
```

این نوع ارتباط با استفاده از three way handshaking است.

در حالت open state مشابه زیر انجام میشود:

Nmap ابتدا tcp syn را به مقصد میفرستد سپس مقصد SYN/ACK را به مبدا برمیگرداند و در نهایت مبدا ارتباط را reset میکند.

-UDP scan:



```
root@kali:~# nmap -sU 192.168.206.131

Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-14 05:35 CST
Nmap scan report for 192.168.206.131
Host is up (0.00075s latency).
Not shown: 993 closed ports
PORT     STATE         SERVICE
123/udp  open          ntp
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
445/udp  open|filtered microsoft-ds
500/udp  open|filtered isakmp
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
MAC Address: 00:0C:29:16:02:B2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
root@kali:~#
```

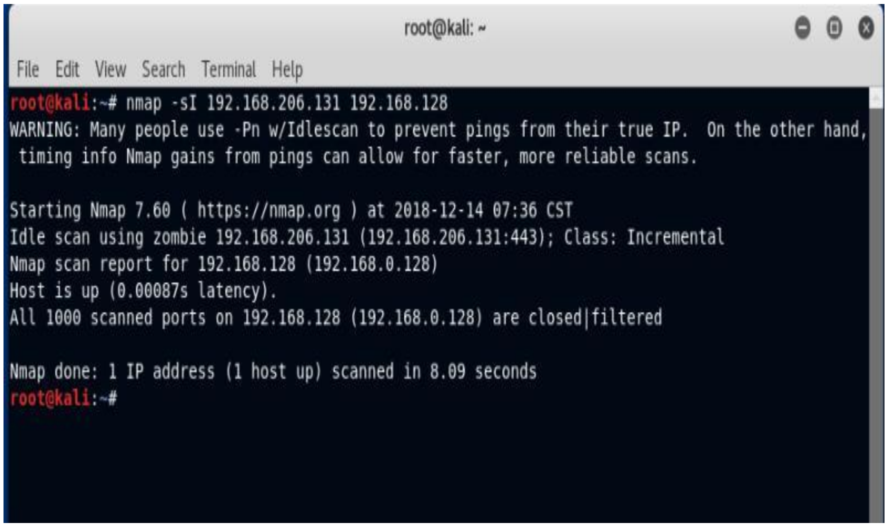
این نوع ارتباط برخلاف tcp از نوع connectioless است. این نوع اسکن مکانیزمی مطابق زیر برای تست باز یا بسته بودن پورت ها انجام میدهد:

اگر پورت باز باشد بسته تویط مقصد قبول میشود و پاسخی داده نمیشود.

اگر پورت بسته باشد یک بستهICMP   با error codeای برگرداند میشود.

-idle scan: مشاهده میشود که پورت

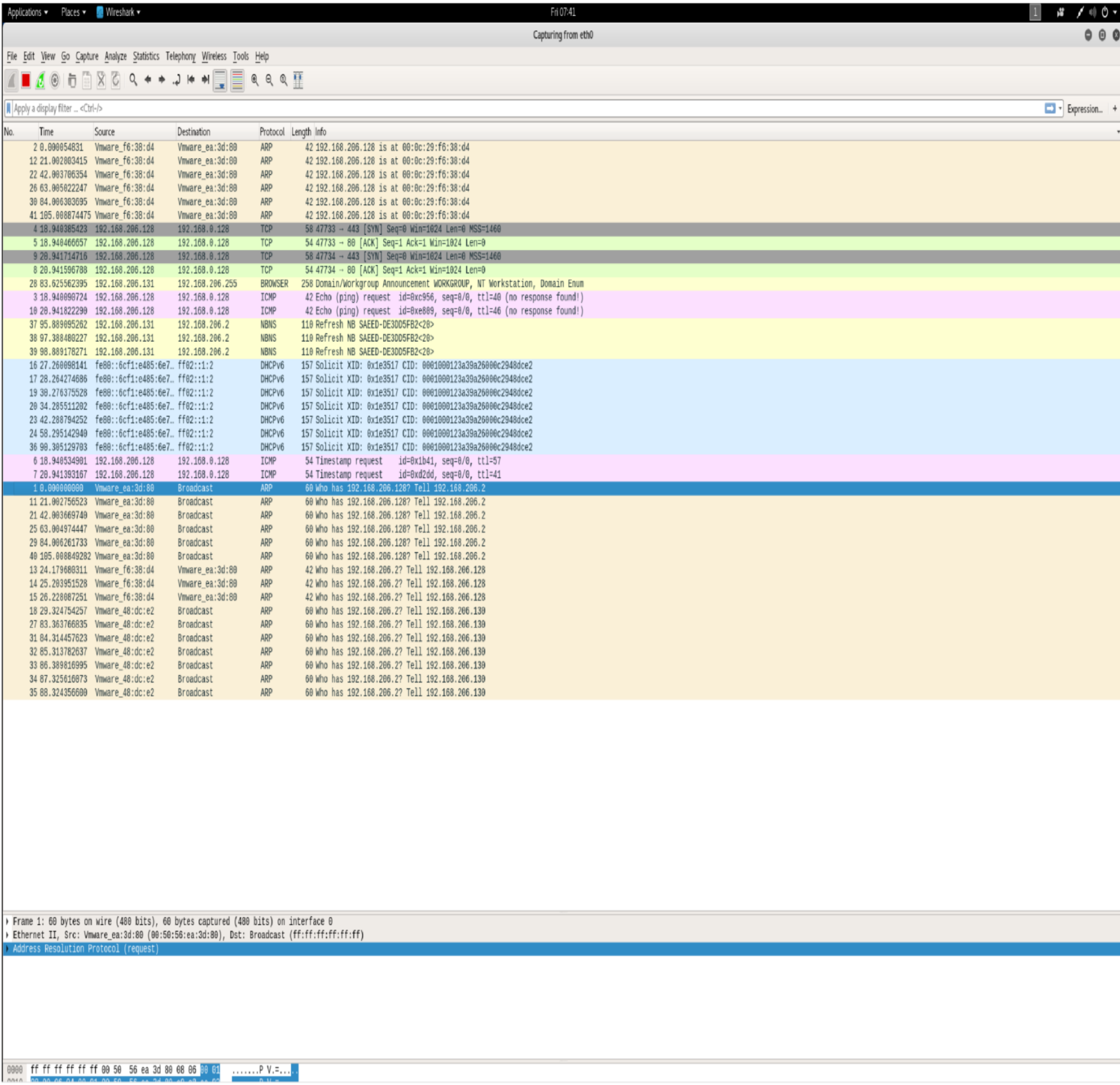
ها بسته اند.



```
root@kali:~# nmap -sI 192.168.206.131 192.168.128
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP.  On the other hand,
 timing info Nmap gains from pings can allow for faster, more reliable scans.

Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-14 07:36 CST
Idle scan using zombie 192.168.206.131 (192.168.206.131:443); Class: Incremental
Nmap scan report for 192.168.128 (192.168.0.128)
Host is up (0.00087s latency).
All 1000 scanned ports on 192.168.128 (192.168.0.128) are closed|filtered

Nmap done: 1 IP address (1 host up) scanned in 8.09 seconds
root@kali:~#
```

مزیت این نوع اسکن این است که مبدا با استفاده از یک zombie به شناسایی پورت مقصد میپردازد و و خود شناسایی نمیشود.

ابتدا مبدا به zombie یک syn/ackمیفرستد تا IP/ID زامبی را شناسایی کند. سپس به مقصد یک synمیفرستد و ip مبدا را ip زامبی میگذارد در نتیجه مقصد syn/ack را به زامبی میفرستد اگر پورت باز باشد و زامبی در جواب reset میدهد و ip/id اش را یکی افزایش میدهد. در انتها مبدا دوباره به زامبی syn/ack میفرستد و زامبی در جواب reset میدهد و ip/id خود را یکی افزایش میدهد. بنابراین اگر ip/id دو واحد افزایش یافته باشد نشان از این دارد که پورت مقصد بازبوده است. ابتدا مبدا به زامبی سپس مبدا به مقصد با استفاده از broadcast و در ادامه ارتباط بین مقصد و زامبی و در انتها ارتباط بین مبدا و زامبی مشاهده میشود.



```
No.     Time         Source                Destination       Protocol Length Info
      2 0.000054831  Vmware_f6:38:d4       Vmware_ea:3d:80   ARP        42 192.168.206.128 is at 00:0c:29:f6:38:d4
     12 21.002803415 Vmware_f6:38:d4       Vmware_ea:3d:80   ARP        42 192.168.206.128 is at 00:0c:29:f6:38:d4
     22 42.003706354 Vmware_f6:38:d4       Vmware_ea:3d:80   ARP        42 192.168.206.128 is at 00:0c:29:f6:38:d4
     26 63.005022247 Vmware_f6:38:d4       Vmware_ea:3d:80   ARP        42 192.168.206.128 is at 00:0c:29:f6:38:d4
     30 84.006303695 Vmware_f6:38:d4       Vmware_ea:3d:80   ARP        42 192.168.206.128 is at 00:0c:29:f6:38:d4
     41 105.008874475 Vmware_f6:38:d4      Vmware_ea:3d:80   ARP        42 192.168.206.128 is at 00:0c:29:f6:38:d4
      4 18.940385423 192.168.206.128       192.168.0.128     TCP        58 47733 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
      5 18.940466657 192.168.206.128       192.168.0.128     TCP        54 47733 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
      9 20.941714716 192.168.206.128       192.168.0.128     TCP        58 47734 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
      8 20.941596788 192.168.206.128       192.168.0.128     TCP        54 47734 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
     28 83.625562395 192.168.206.131       192.168.206.255   BROWSER   258 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
      3 18.940090724 192.168.206.128       192.168.0.128     ICMP       42 Echo (ping) request  id=0xc956, seq=0/0, ttl=40 (no response found!)
     10 20.941822290 192.168.206.128       192.168.0.128     ICMP       42 Echo (ping) request  id=0xe809, seq=0/0, ttl=46 (no response found!)
     37 95.889095262 192.168.206.131       192.168.206.2     NBNS      110 Refresh NB SAEED-DE3DD5FB2<20>
     38 97.388480227 192.168.206.131       192.168.206.2     NBNS      110 Refresh NB SAEED-DE3DD5FB2<20>
     39 98.889178271 192.168.206.131       192.168.206.2     NBNS      110 Refresh NB SAEED-DE3DD5FB2<20>
     16 27.260098141 fe80::6cf1:e485:6e7… ff02::1:2         DHCPv6    157 Solicit XID: 0x1e3517 CID: 0001000123a39a26000c2948dce2
     17 28.264274686 fe80::6cf1:e485:6e7… ff02::1:2         DHCPv6    157 Solicit XID: 0x1e3517 CID: 0001000123a39a26000c2948dce2
     19 30.276375528 fe80::6cf1:e485:6e7… ff02::1:2         DHCPv6    157 Solicit XID: 0x1e3517 CID: 0001000123a39a26000c2948dce2
     20 34.285511202 fe80::6cf1:e485:6e7… ff02::1:2         DHCPv6    157 Solicit XID: 0x1e3517 CID: 0001000123a39a26000c2948dce2
     23 42.288794252 fe80::6cf1:e485:6e7… ff02::1:2         DHCPv6    157 Solicit XID: 0x1e3517 CID: 0001000123a39a26000c2948dce2
     24 58.295142940 fe80::6cf1:e485:6e7… ff02::1:2         DHCPv6    157 Solicit XID: 0x1e3517 CID: 0001000123a39a26000c2948dce2
     36 90.305129703 fe80::6cf1:e485:6e7… ff02::1:2         DHCPv6    157 Solicit XID: 0x1e3517 CID: 0001000123a39a26000c2948dce2
      6 18.940534901 192.168.206.128       192.168.0.128     ICMP       54 Timestamp request    id=0x1b41, seq=0/0, ttl=57
      7 20.941393167 192.168.206.128       192.168.0.128     ICMP       54 Timestamp request    id=0xd2dd, seq=0/0, ttl=41
      1 0.000000000  Vmware_ea:3d:80       Broadcast         ARP        60 Who has 192.168.206.128? Tell 192.168.206.2
     11 21.002756523 Vmware_ea:3d:80       Broadcast         ARP        60 Who has 192.168.206.128? Tell 192.168.206.2
     21 42.003669740 Vmware_ea:3d:80       Broadcast         ARP        60 Who has 192.168.206.128? Tell 192.168.206.2
     25 63.004974447 Vmware_ea:3d:80       Broadcast         ARP        60 Who has 192.168.206.128? Tell 192.168.206.2
     29 84.006261733 Vmware_ea:3d:80       Broadcast         ARP        60 Who has 192.168.206.128? Tell 192.168.206.2
     40 105.008849282 Vmware_ea:3d:80      Broadcast         ARP        60 Who has 192.168.206.128? Tell 192.168.206.2
     13 24.179680311 Vmware_f6:38:d4       Vmware_ea:3d:80   ARP        42 Who has 192.168.206.2? Tell 192.168.206.128
     14 25.203951528 Vmware_f6:38:d4       Vmware_ea:3d:80   ARP        42 Who has 192.168.206.2? Tell 192.168.206.128
     15 26.228087251 Vmware_f6:38:d4       Vmware_ea:3d:80   ARP        42 Who has 192.168.206.2? Tell 192.168.206.128
     18 29.324754257 Vmware_48:dc:e2       Broadcast         ARP        60 Who has 192.168.206.2? Tell 192.168.206.130
     27 83.363766835 Vmware_48:dc:e2       Broadcast         ARP        60 Who has 192.168.206.2? Tell 192.168.206.130
     31 84.314457623 Vmware_48:dc:e2       Broadcast         ARP        60 Who has 192.168.206.2? Tell 192.168.206.130
     32 85.313782637 Vmware_48:dc:e2       Broadcast         ARP        60 Who has 192.168.206.2? Tell 192.168.206.130
     33 86.389816995 Vmware_48:dc:e2       Broadcast         ARP        60 Who has 192.168.206.2? Tell 192.168.206.130
     34 87.325616073 Vmware_48:dc:e2       Broadcast         ARP        60 Who has 192.168.206.2? Tell 192.168.206.130
     35 88.324356600 Vmware_48:dc:e2       Broadcast         ARP        60 Who has 192.168.206.2? Tell 192.168.206.130
```

```
▸ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: Vmware_ea:3d:80 (00:50:56:ea:3d:80), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 50  56 ea 3d 80 08 06 00 01   .......P V.=.....
```