

H1 kutsu, vuohi ja pimeän verkon päiväkirjat

- a) Asensin WebGoatin kahdelle alustalle, Debian ja Kali käyttöjärjestelmille. WebGoattia asentaessa Debianille käytin tehtävään löytyviä ohjeita kurssin sivuilta, eli käytössä oleva versio oli 8.0.0. Kalille asennettu versio oli uusimman, eli 8.2.2. Asensin sen lataamalla uusimman version Githubista ja lataamalla siihen sopivan openjdk version, jotta sain WebGoatin toimimaan. Harjoituksiin pääsy localhost portin kautta onnistui ja käyttäjien luonnissa ei ollut ongelmia
- b) HTTP Basics osuudessa opin tunnistamaan GET pyynnön ja POST pyynnön, ja miten hyötyä käyttää niitä verkkosivuja tutkiessa. Tehtävän viimeisessä osuudessa piti selvittää, oliko annettu komento POST tai GET katsomalla kehittäjä työkalun network osuudesta lähetetyn tapahtuman. Tehtävässä kysytty "taikanumero" saatiin selville menemällä tapahtuma request osuuteen, jossa näkyi lomakkeen tiedot ja haluttu "taikanumero".

Status	Method	Domain	File
200	GET	localhost:8080	AssignmentStatusModel.js
200	POST	localhost:8080	attack2

Headers	Cookies	Request	Response	Timings	Stack Trace
---------	---------	---------	----------	---------	-------------

Filter Request Parameters

Form data

magic_num: "58"

Developer Tools osuudessa sain paremman käsityksen työkalujen ominaisuuksista ja jouduin samalla tavalla kuin edellisissäkin osiossa etsimään tapahtuman request kohdasta numerosarjan, jonka avulla sain tehtävän tehtyä.

- c) OverTheWire: Bandit harjoituksissa 0–2, piti ensimmäiseksi yhdistyä harjoituksen servereille komennolla:

```
$ ssh bandit0@bandit.labs.overthewire.org -p 2220
```

Tasolle 0 pääsemisen jälkeen piti lukea palvelimella oleva "readme" tiedosto, jossa oli seuraavan tason salasana. 1 tasolla piti lukea "-" merkillä nimetyn tiedoston sisältö. Ratkaisuna oli pistää "./" merkin eteen. Sisältö saatiin näkyviin komennolla:

```
bandit1@bandit:~$ cat ./-
rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi
```

Tasolla 2 piti lukea tiedoston tiedot, jonka nimessä oli välilyöntejä. Sain tiedon luettua komennolla:

```
bandit2@bandit:~$ cat spaces\ in\ this\ filename
aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG
```

Ratkaisuna oli siis pistää "\" merkki välilyönti kohtiin.

- d) Latasin Kalista viimeimmän levy version ja asensin sen Virtualboxiin. Asennuksessa ei ollut ongelmia

- e) 2021 Challenge.fi harjoituksista valitsin tehtävän “Where was this picture taken? 4/4 217”. Kuvassa oli Eiffel torni, mutta ei Pariisiin vaan Bahria Townin, mikä on kaupunki Pakistanissa. Selvitin sijainnin lataamalla kuvan ja käyttämällä komentoa:

```
exiftool d.jpg | grep GPS
Version ID           : 2.2.0.0
Latitude Ref         : North
Longitude Ref        : East
Altitude Ref         : Above Sea Level
Dilution Of Precision : 14.768
Date Stamp           : 2017:11:15
Altitude              : 54.2 m Above Sea Level
Latitude              : 31 deg 21' 21.54" N
Longitude              : 74 deg 11' 5.08" E
Position              : 31 deg 21' 21.54" N, 74 deg 11' 5.08" E
```

Exiftool komennon avulla saadaan erilaista metadataa kuvasta, ja komennolla grep etsin metadataa liittyen sijaintiin.