ATTACK DEFENSE

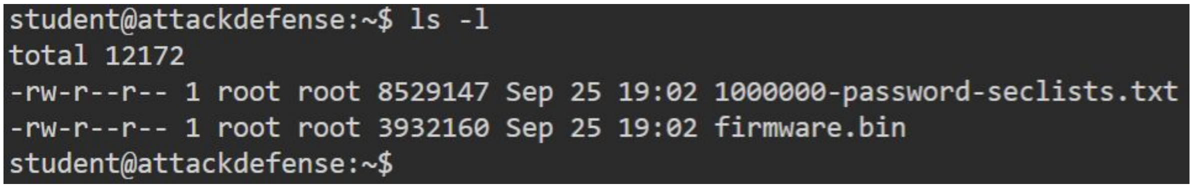
by PentesterAcademy

Name	Weak Root Password
URL	https://www.attackdefense.com/challengedetails?cid=99
Type	Firmware Analysis : WiFi Routers

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

Step 1: Check the given files

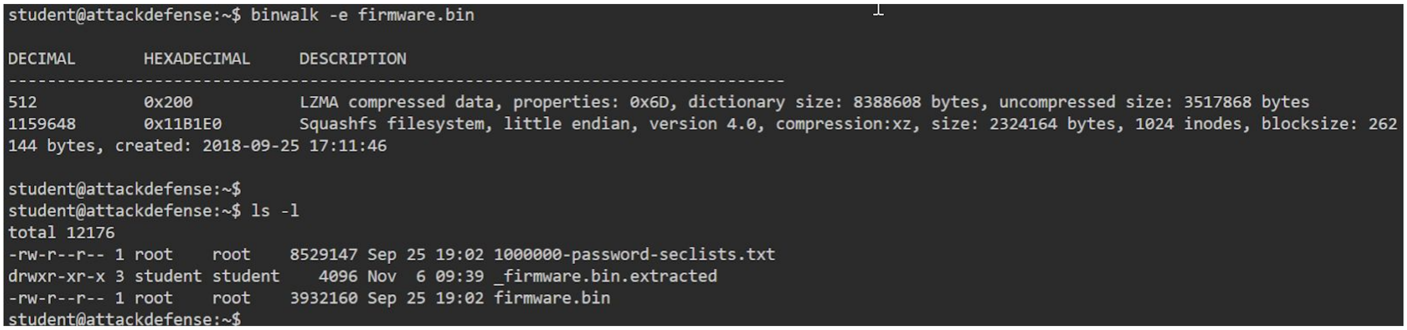
Command: ls -l



```
student@attackdefense:~$ ls -l
total 12172
-rw-r--r-- 1 root root 8529147 Sep 25 19:02 1000000-password-seclists.txt
-rw-r--r-- 1 root root 3932160 Sep 25 19:02 firmware.bin
student@attackdefense:~$
```

Step 2: Extract the firmware using binwalk and check the contents of the current directory again.

Command: binwalk -e firmware.bin



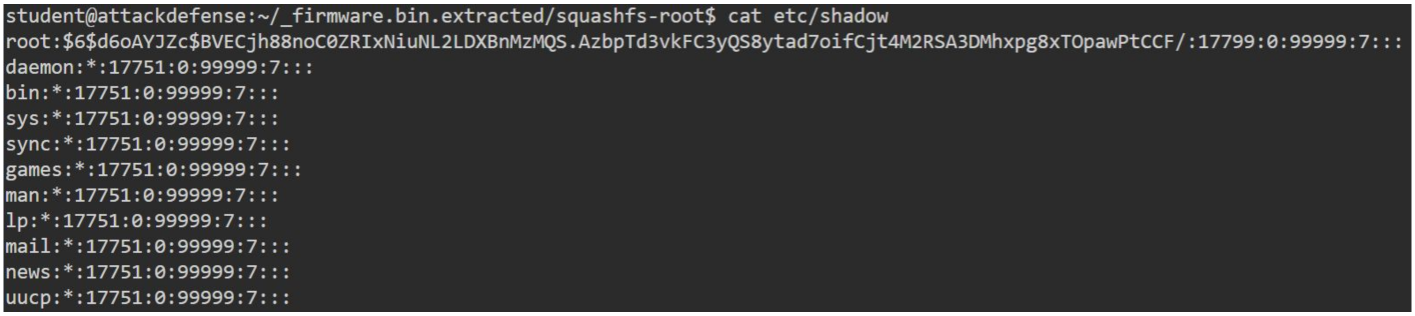
```
student@attackdefense:~$ binwalk -e firmware.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
512           0x200           LZMA compressed data, properties: 0x6D, dictionary size: 8388608 bytes, uncompressed size: 3517868 bytes
1159648       0x11B1E0        Squashfs filesystem, little endian, version 4.0, compression:xz, size: 2324164 bytes, 1024 inodes, blocksize: 262
144 bytes, created: 2018-09-25 17:11:46

student@attackdefense:~$
student@attackdefense:~$ ls -l
total 12176
-rw-r--r-- 1 root    root    8529147 Sep 25 19:02 1000000-password-seclists.txt
drwxr-xr-x 3 student student    4096 Nov  6 09:39 _firmware.bin.extracted
-rw-r--r-- 1 root    root    3932160 Sep 25 19:02 firmware.bin
student@attackdefense:~$
```

Step 3: Explore the file system of the firmware and access shadow file.

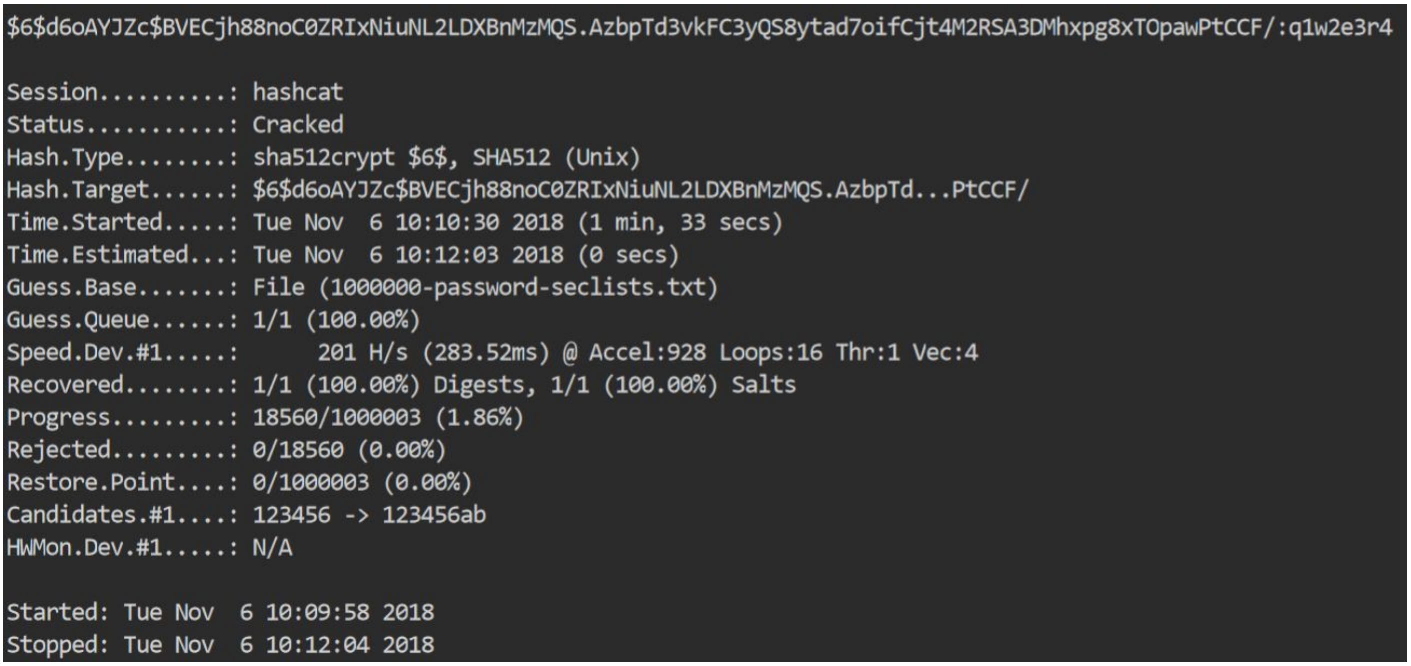
Command: cat etc/shadow



```
student@attackdefense:~/_firmware.bin.extracted/squashfs-root$ cat etc/shadow
root:$6$d6oAYJZc$BVECjh88noC0ZRIxNiuNL2LDXBnMzMQS.AzbpTd3vkFC3yQS8ytad7oifCjt4M2RSA3DMhxpg8xTOpawPtCCF/:17799:0:99999:7:::
daemon:*:17751:0:99999:7:::
bin:*:17751:0:99999:7:::
sys:*:17751:0:99999:7:::
sync:*:17751:0:99999:7:::
games:*:17751:0:99999:7:::
man:*:17751:0:99999:7:::
lp:*:17751:0:99999:7:::
mail:*:17751:0:99999:7:::
news:*:17751:0:99999:7:::
uucp:*:17751:0:99999:7:::
```

Step 4: Crack the root password of the firmware

Command: hashcat -m 1800 -a 0 _firmware.bin.extracted/squashfs-root/etc/shadow 1000000-password-seclists.txt



```
$6$d6oAYJZc$BVECjh88noC0ZRIxNiuNL2LDXBnMzMQS.AzbpTd3vkFC3yQS8ytad7oifCjt4M2RSA3DMhxpg8xTOpawPtCCF/:q1w2e3r4

Session..........: hashcat
Status...........: Cracked
Hash.Type........: sha512crypt $6$, SHA512 (Unix)
Hash.Target......: $6$d6oAYJZc$BVECjh88noC0ZRIxNiuNL2LDXBnMzMQS.AzbpTd...PtCCF/
Time.Started.....: Tue Nov  6 10:10:30 2018 (1 min, 33 secs)
Time.Estimated...: Tue Nov  6 10:12:03 2018 (0 secs)
Guess.Base.......: File (1000000-password-seclists.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:      201 H/s (283.52ms) @ Accel:928 Loops:16 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 18560/1000003 (1.86%)
Rejected.........: 0/18560 (0.00%)
Restore.Point....: 0/1000003 (0.00%)
Candidates.#1....: 123456 -> 123456ab
HWMon.Dev.#1.....: N/A

Started: Tue Nov  6 10:09:58 2018
Stopped: Tue Nov  6 10:12:04 2018
```

Flag: q1w2e3r4

References:

1. Binwalk (https://github.com/ReFirmLabs/binwalk)