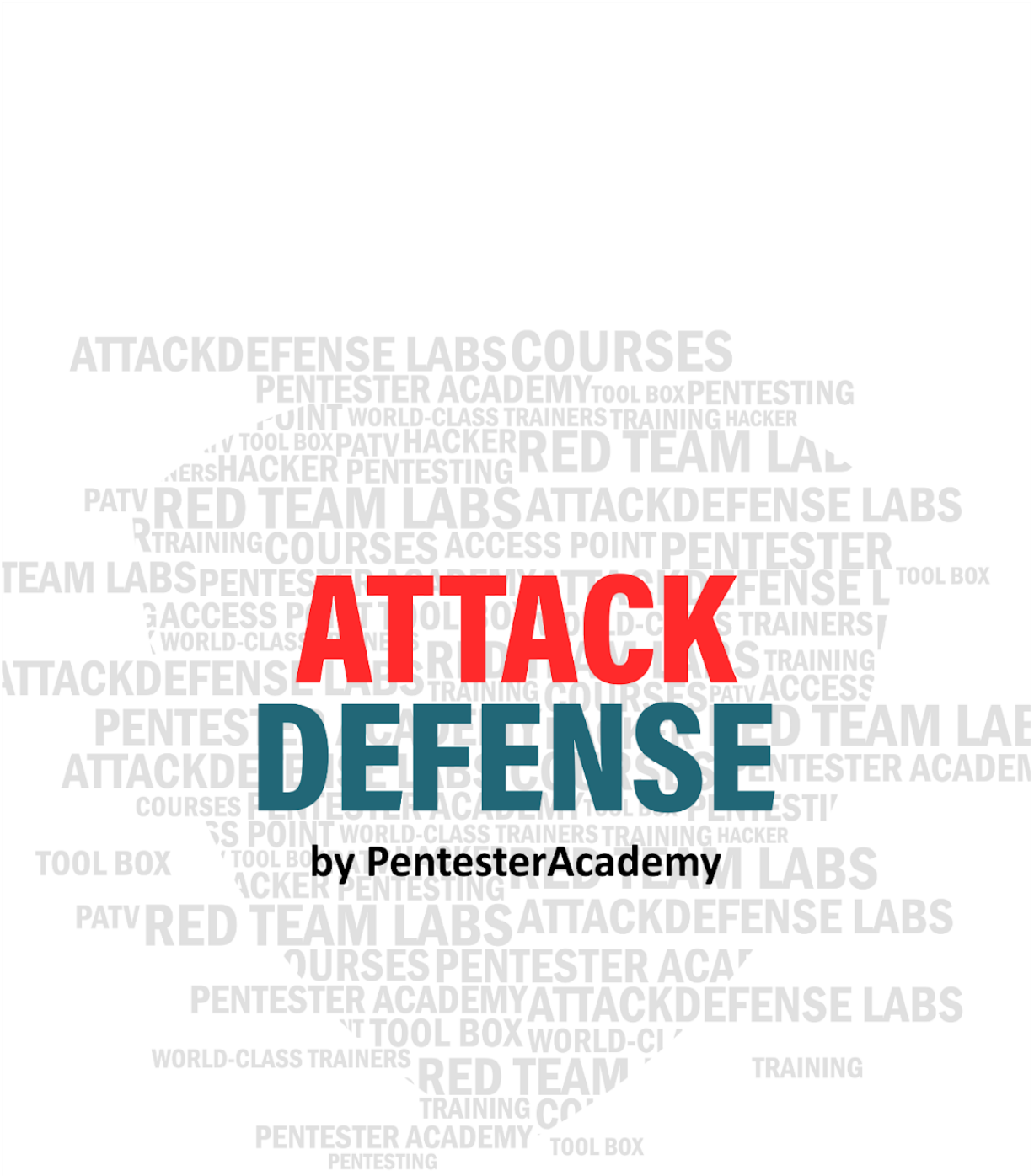
ATTACK
DEFENSE
by PentesterAcademy

Name	Network Backdoor II
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

```
root@attackdefense:~# ls -l
total 3840
-rw-r--r-- 1 root root 3932160 Sep 30 05:35 firmware.bin
root@attackdefense:~#
```

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

Command: binwalk -e firmware.bin

```
root@attackdefense:~# binwalk -e firmware.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
512           0x200           LZMA compressed data, properties: 0x6D, dictionary size: 8388608 bytes, uncompressed size: 3517868 bytes
1160240       0x11B430        Squashfs filesystem, little endian, version 4.0, compression:xz, size: 2327362 bytes, 1028 inodes, blocksize: 262
144 bytes, created: 2018-09-30 05:35:27

root@attackdefense:~#
```

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

```
root@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.

/usr/bin/start_essentials &

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

It is executing another file kept at usr/bin/start_essentials. Check this file.

```
#!/bin/sh

INPUT="opt"
PROG=/usr/bin/firewallid
NAME=Firewall
PIDCOUNT=0
PID=5676
PIDFILE="/$INPUT/$PID"

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

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

        . /lib/functions.sh
        . /lib/functions/network.sh

        config_load "${NAME}"
        config_foreach dropbear_instance dropbear
        $PIDFILE
}

~
"usr/bin/start_essentials" 27L, 413C
```

On checking the code closely, it is clear that the file is calling another file kept at opt/5676. Check that file.

```
root@attackdefense:~/_firmware.bin.extracted/squashfs-root# cat opt/5676
#!/usr/bin/env bash

/usr/bin/webhelper &
root@attackdefense:~/_firmware.bin.extracted/squashfs-root#
```

And finally, this script is calling a binary.

```
root@attackdefense:~/_firmware.bin.extracted/squashfs-root# file usr/bin/webhelper
usr/bin/webhelper: ELF 32-bit MSB executable, MIPS, MIPS32 rel2 version 1 (SYSV), dynamically linked, interpreter /lib/ld.so.1, for GNU/Linux 3
.2.0, BuildID[sha1]=430a2a6fd2f94e171dfd76cf616235d260607d77, not stripped
root@attackdefense:~/_firmware.bin.extracted/squashfs-root#
```

Step 4: Run strings command on this binary and dump the strings into a file.

Command: strings usr/bin/webhelper > strings.txt

Check the strings.txt file to find the desired information

```
$'9     4
fhgs35794dlale199
witrap.com
POST /message=%s HTTP/1.0
/etc/shadow
%s.%s
Sending request:
Response for request:
GCC: (Ubuntu 7.3.0-27ubuntu1~18.04) 7.3.0
/usr/lib/gcc-cross/mips-linux-gnu/7/include
"strings.txt" 282 lines --19%--
```

The backdoor is actually posting sensitive information (such as the contents of /etc/shadow) to witrap.com

Flag: shadow

References:

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