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

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.

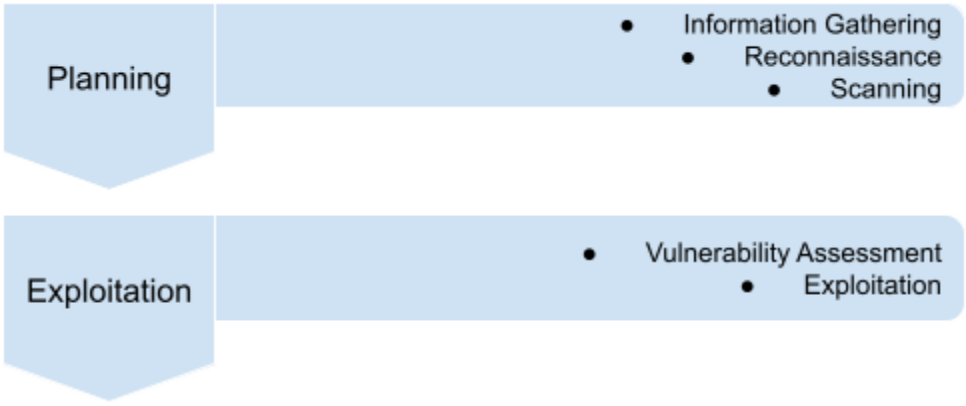
1.3. Assumption

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

<table>
<tr><th>IP Address</th><th>System Type</th><th>OS information</th><th colspan="3">Open Ports</th></tr>
<tr><td></td><td></td><td></td><td>Port #</td><td>Protocol</td><td>Service name</td></tr>
<tr><td>192.168.100.9</td><td>Samsung Smart TV</td><td>Bada OS</td><td>7676</td><td>tcp</td><td>upnp (ALL Share)</td></tr>
<tr><td></td><td></td><td></td><td>8080</td><td>tcp</td><td>http-proxy</td></tr>
</table>

```
┌──(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    lighttpd
| http-enum:
|_  /test/logon.html: Jetty (401 Unauthorized)
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 13.83 seconds

┌──(satakali㉿satakali)-[~]
└─$
```

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

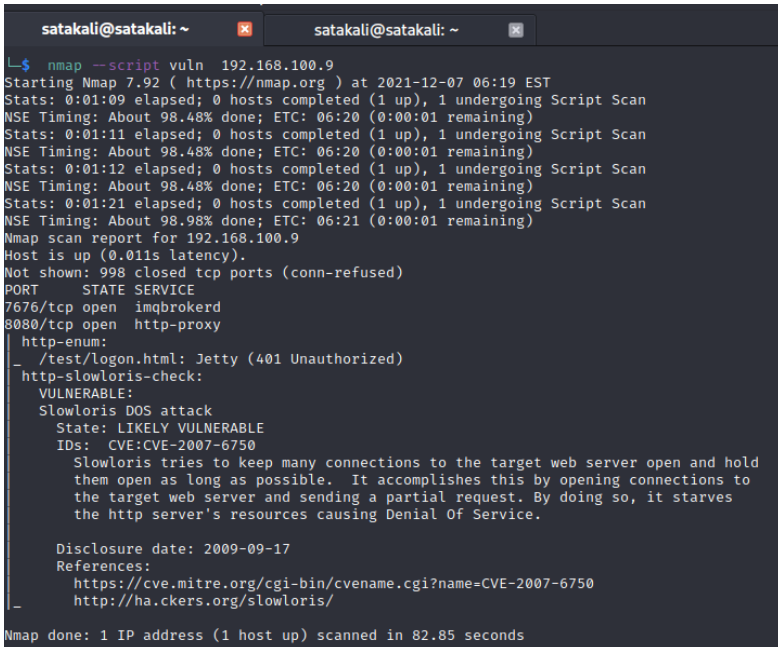


Figure 1

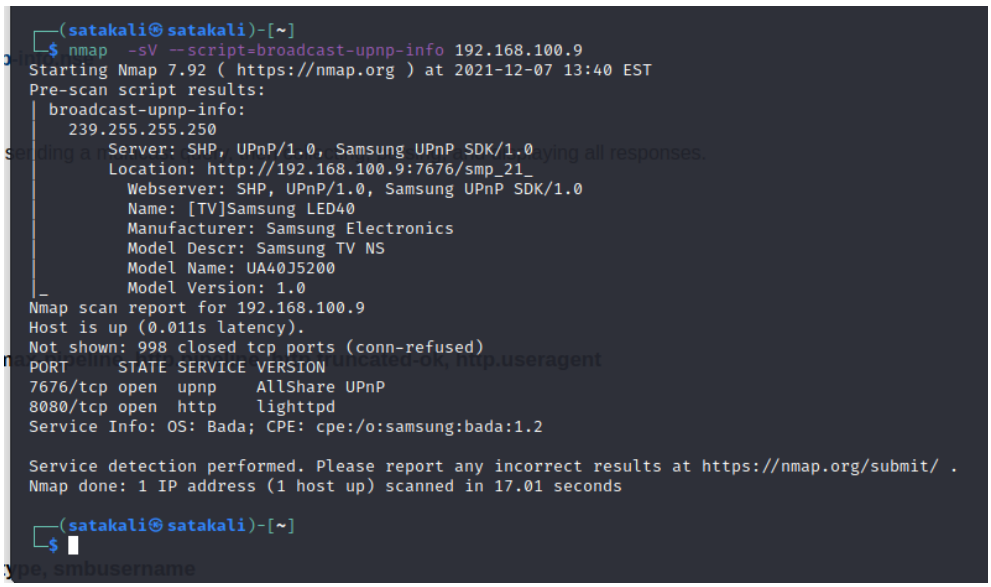


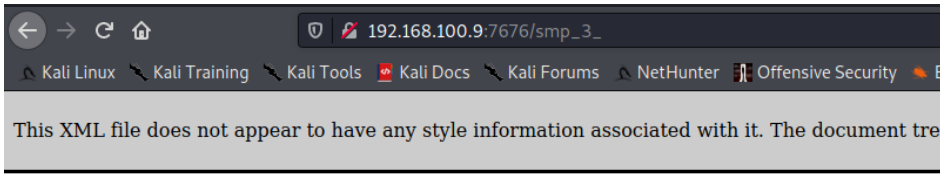
Figure 2

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

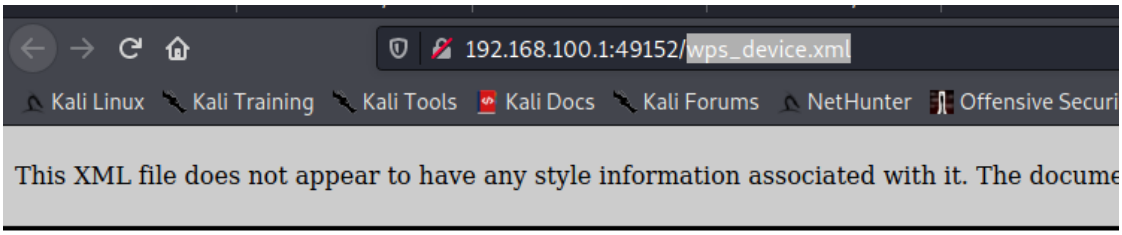
No vulnerability was found to access the shell.

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,ENCP,Y2015
     </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>
```

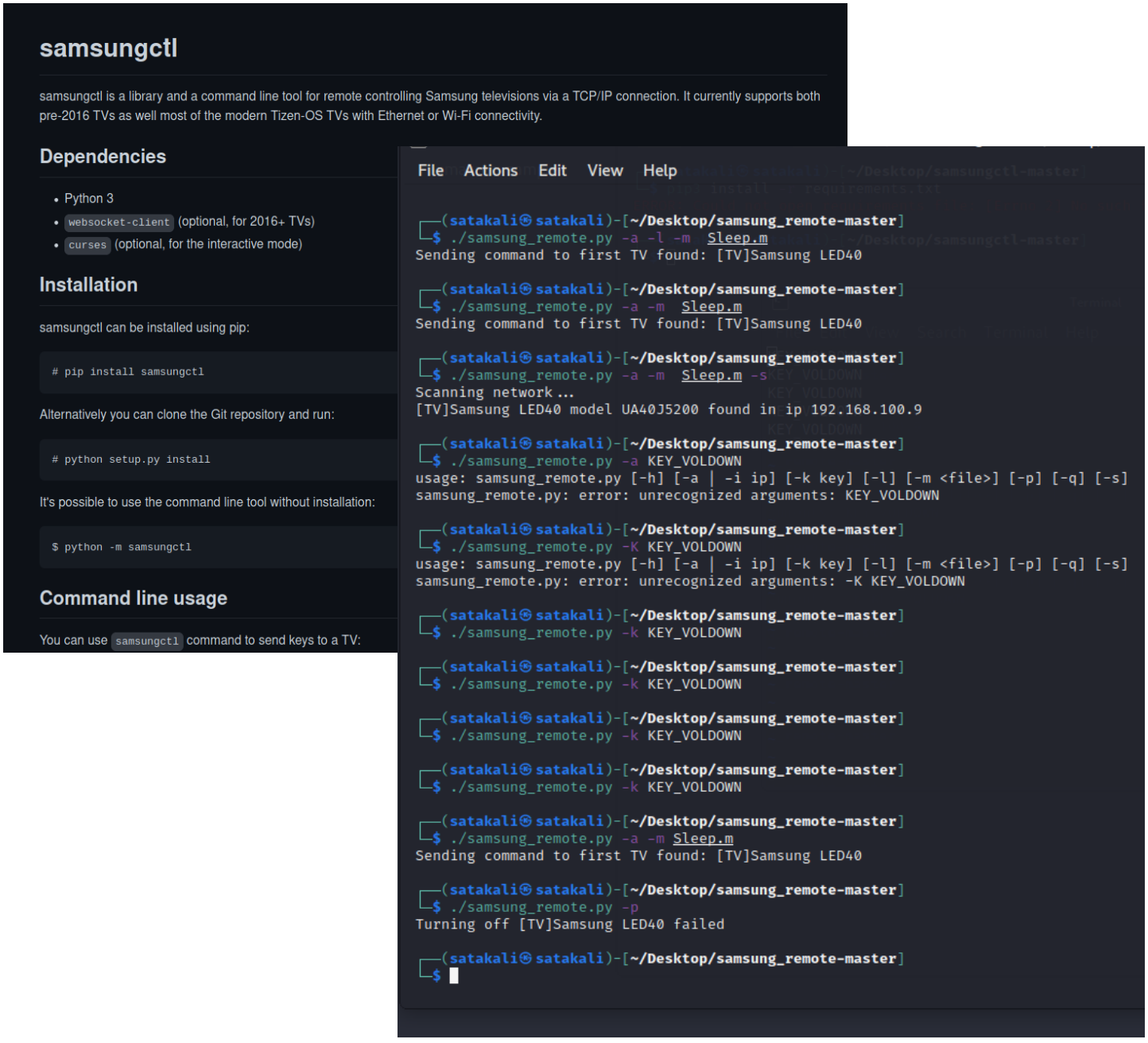



```
−<root>
  −<specVersion>
     <major>1</major>
     <minor>0</minor>
   </specVersion>
  −<device>
     <deviceType>urn:schemas-wifialliance-org:device:WFADevice:1</deviceType>
     <friendlyName>WPS Access Point</friendlyName>
     <manufacturer>huaweitec</manufacturer>
     <modelName>WAP</modelName>
     <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 samsung ctl 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.

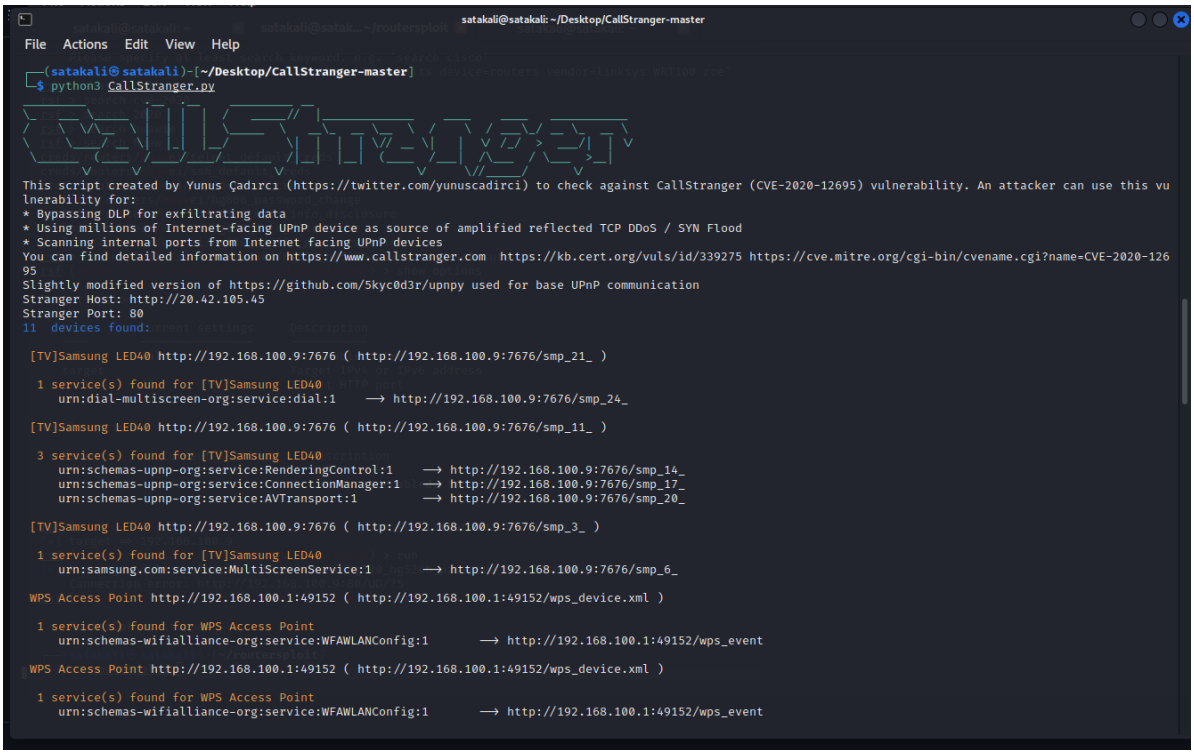


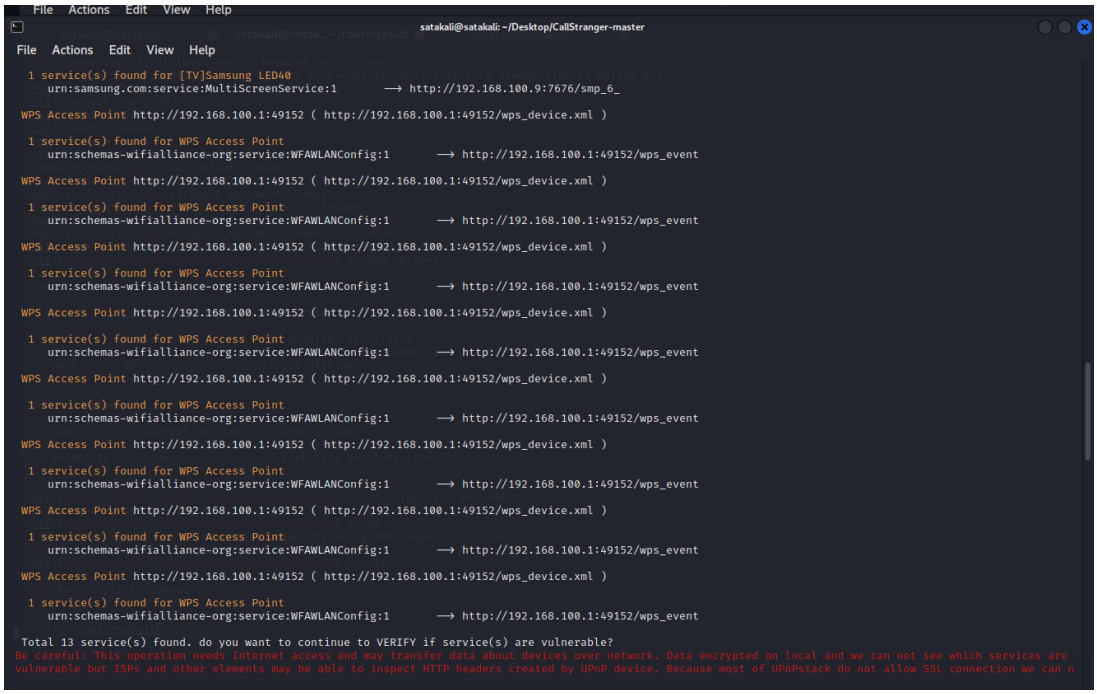
CallStranger Vulnerability Test (CVE-2020-12695)

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.





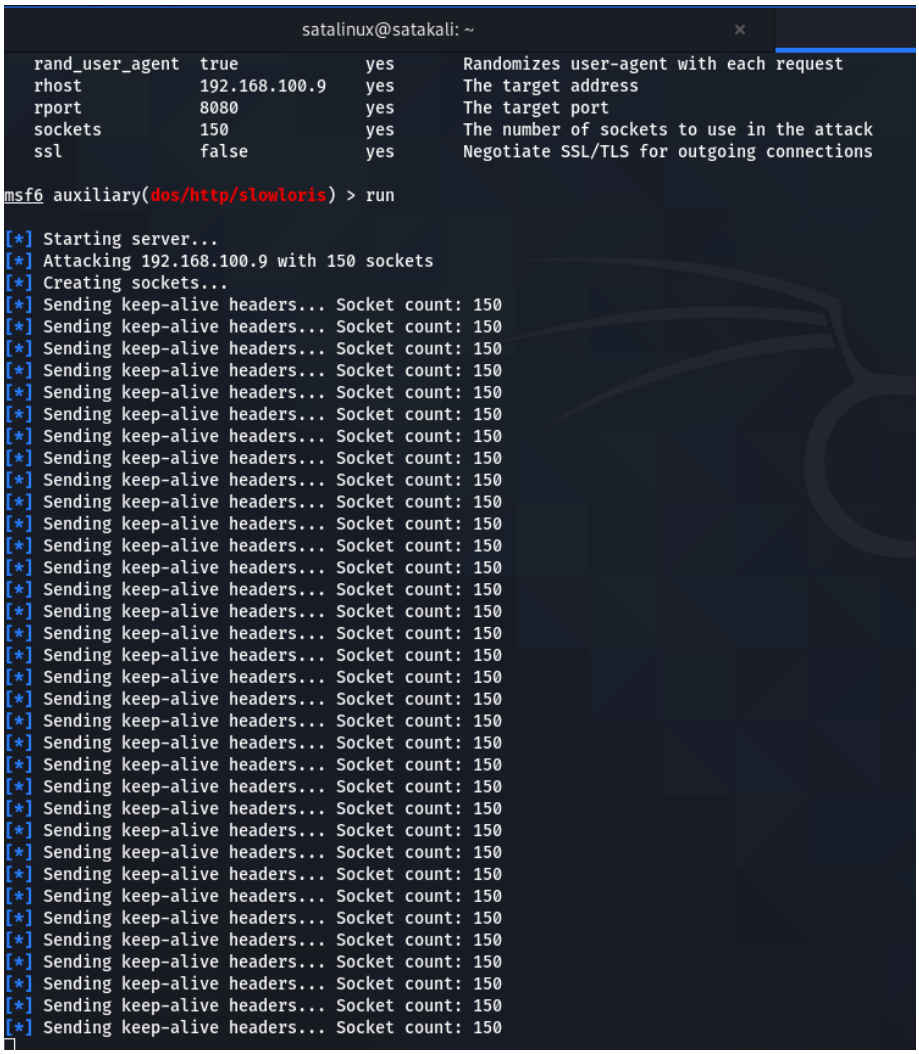
Vulnerability: CallStranger (CVE-2020-12695)
Threat Level :
HIGH
Vulnerability:
HIGH
Analysis:
Though no exploit was available, the device is still highly vulnerable to this attack because the attack is recent and the device is at least six years old.

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.

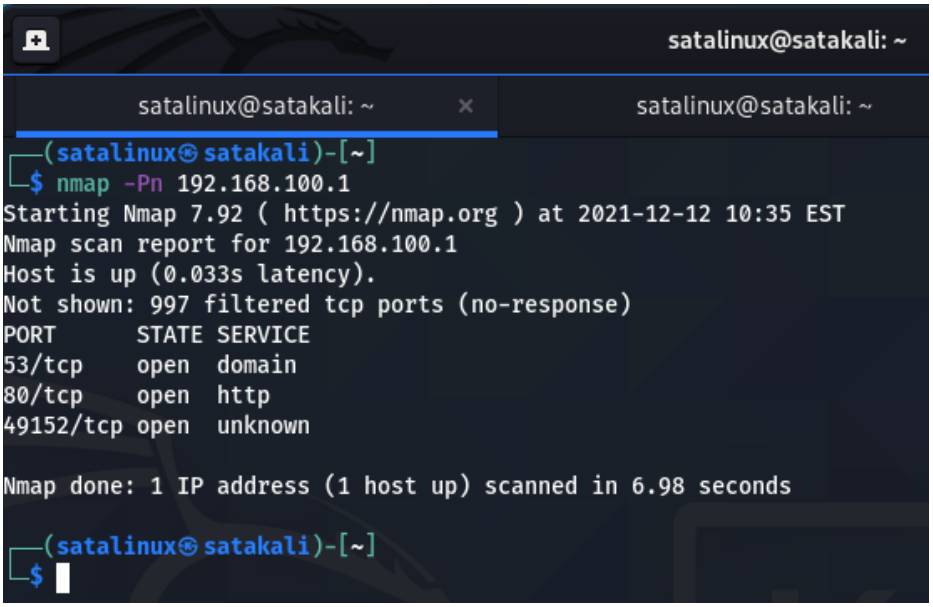
The DOS attack failed because there was nothing to be displayed to me because there was no web server running on smart tv..



Vulnerability: CVE:CVE-2007-6750(Slowloris DOS attack)
Threat Level :
Low
Vulnerability:
Low
Analysis:
No significant response was seen on tv.

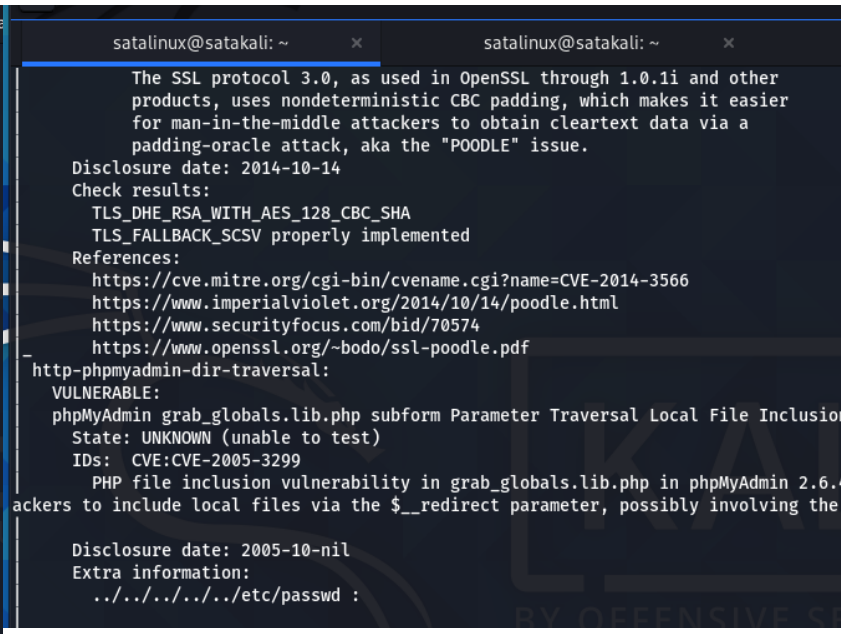
Router Reconnaissance

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



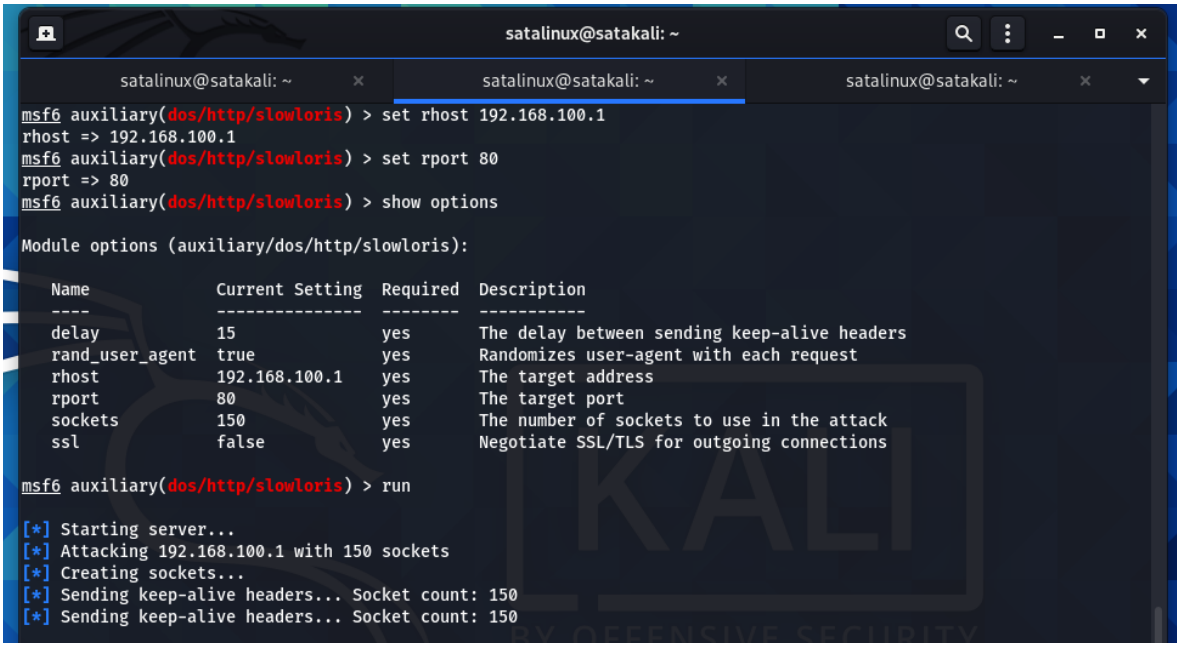
Vulnerabilities and Exploitation

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

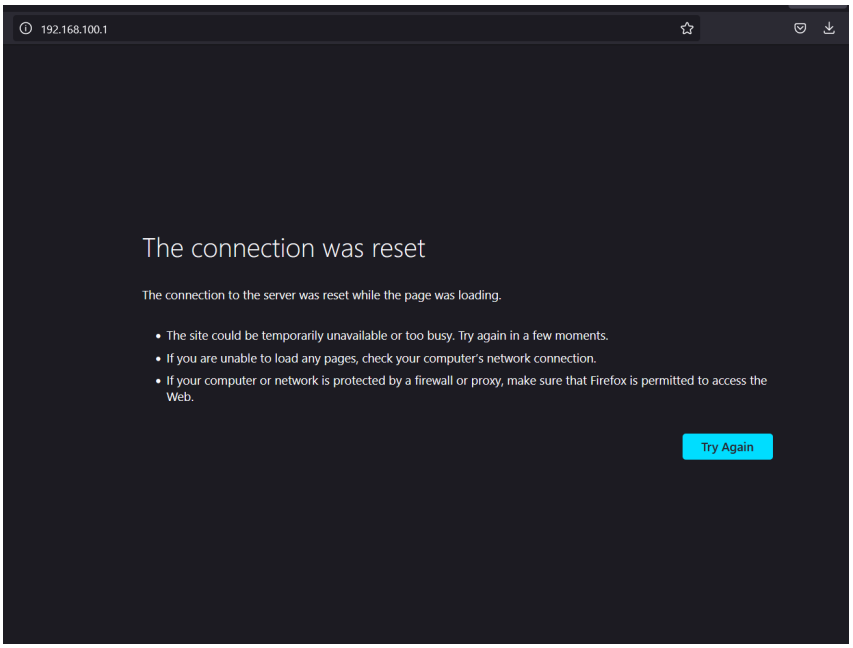


Vulnerability: CVE:CVE-2007-6750(Slowloris DOS attack)
Threat Level :
Medium
Vulnerability:
Medium
Analysis:
The **router was vulnerable to Slowloris DOS attack;** the dos attack disabled the access of the admin page running on IP 192.168.100.1.

Metasploit Results



The admin Page was not loading.

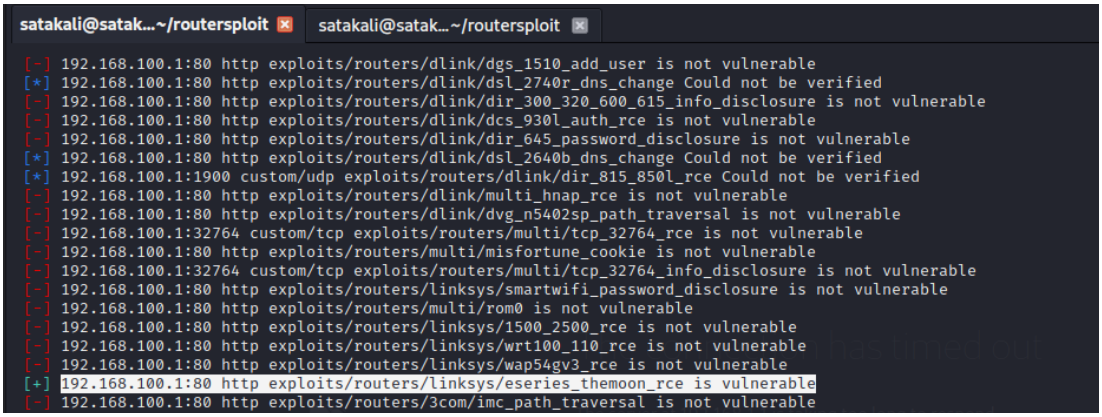


Vulnerability: CVE:CVE-2014-3566(SSL POODLE info Leak)
Threat Level :
Medium
Vulnerability:
Medium
Analysis:
The attacker might be able to sniff the traffic of the network.

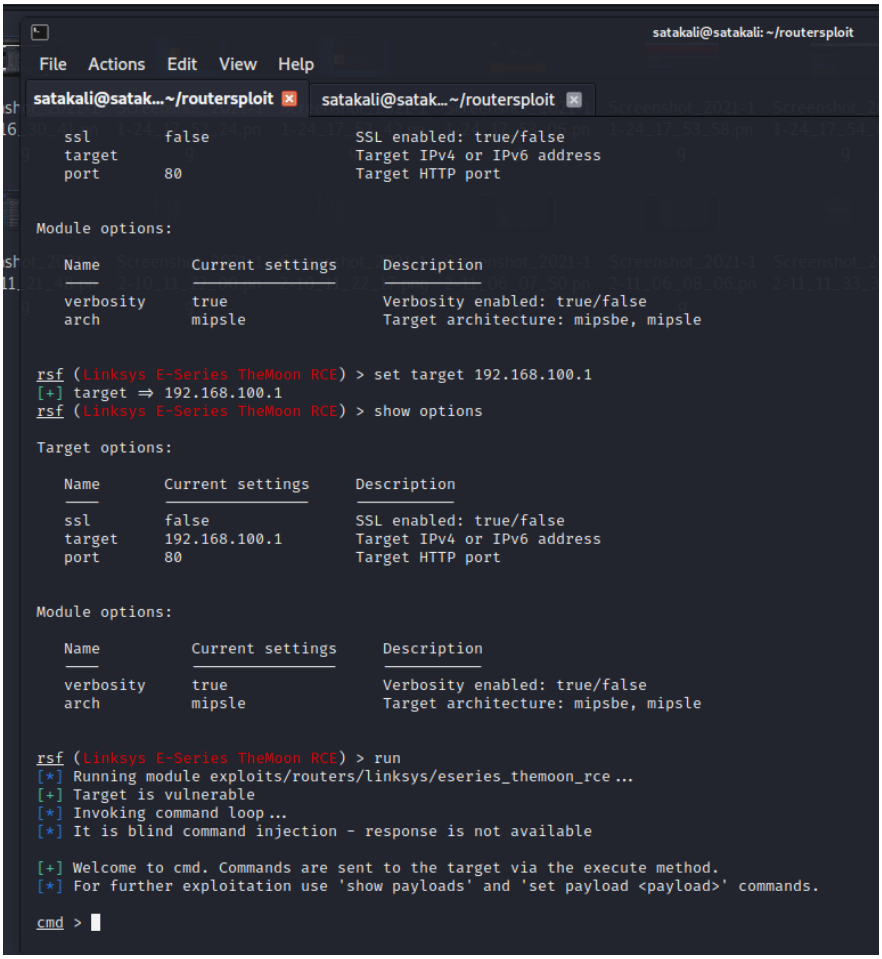
Router admin login credentials can also be sniffed by man in the middle attack.

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.



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.



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