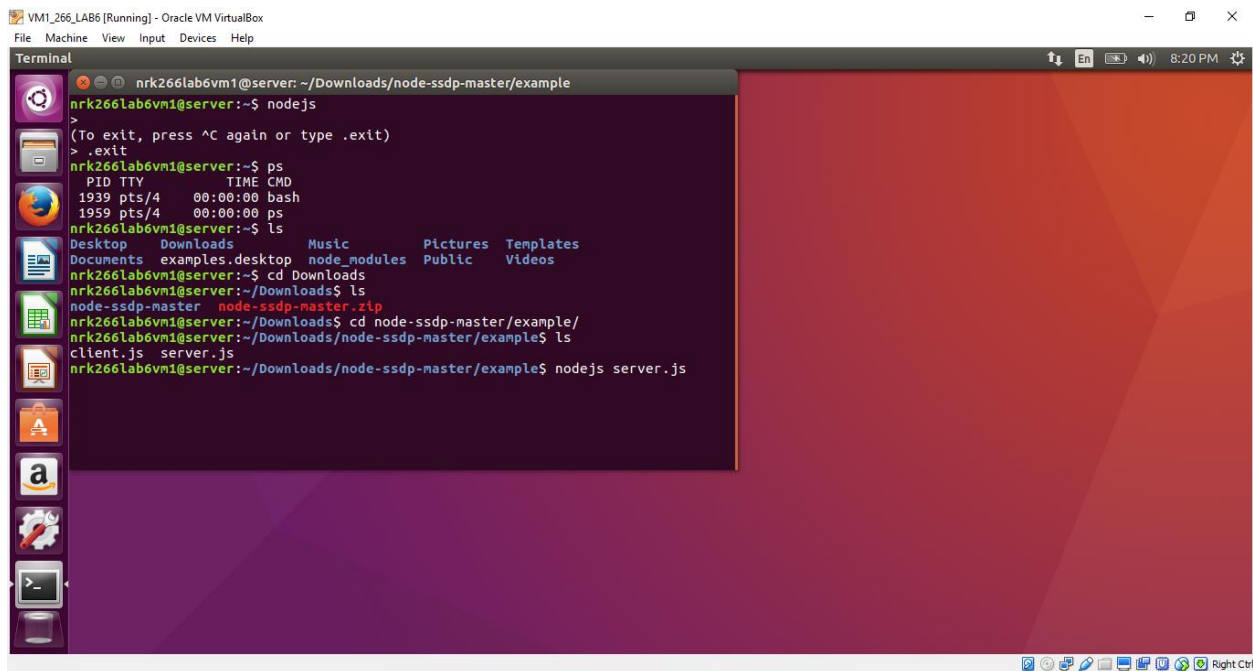


TASK 1:**Exploiting UPnP to attack on IOT:**

UPnP stands for Universal Plug and Play protocol. This protocol allows devices in a network to identify and connect to other devices within the network. Generally used for streaming between devices. This protocol has simple configuration and setup. For this a UPnP compatible router and server program is required as well as compatible UPnP device is required. Even though the purpose of UPnP is to ease the communication between devices there are few ways in which interfaces are exposed to internet that allows hackers to find and get access to the private network devices.

Referring to the paper on “Low-Cost Flow-Based Security Solutions for Smart-Home IoT Devices”, their flow-based detection system monitors IoT devices in which UPnP is enabled. In such a situation use of SSDP protocol would request for interconnected devices and wherever UPnP is enabled, the device might respond with an XML file which contains a URL that can be used to cause an event in that device via HTTP request (POST), thus attacking the device. For example, Port-Forwarding attack is possible or “AddingPortMappingFunctionality” can be executed via SOAP without authentication itself.



```
VM1_266_LAB6 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
nrk266lab6vm1@server: ~/Downloads/node-ssdp-master/example
nrk266lab6vm1@server:~$ nodejs
>
(To exit, press ^C again or type .exit)
> .exit
nrk266lab6vm1@server:~$ ps
  PID TTY          TIME CMD
 1939 pts/4    00:00:00 bash
 1959 pts/4    00:00:00 ps
nrk266lab6vm1@server:~$ ls
Desktop  Downloads  Music      Pictures  Templates
Documents  examples.desktop  node_modules  Public    Videos
nrk266lab6vm1@server:~$ cd Downloads
nrk266lab6vm1@server:~/Downloads$ ls
node-ssdp-master  node-ssdp-master.zip
nrk266lab6vm1@server:~/Downloads$ cd node-ssdp-master/example/
nrk266lab6vm1@server:~/Downloads/node-ssdp-master/example$ ls
client.js  server.js
nrk266lab6vm1@server:~/Downloads/node-ssdp-master/example$ nodejs server.js
```

Figure shows server side 'server.js' started.

VM2_266_LAB6 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminal

```
nrk266lab6vm2@client: ~/Downloads/node-ssdp-master/example
"size": 323
}
Got a response to an m-search:
200
{
  "ST": "uuid:f40c2981-7329-40b7-8b04-27f187aecfb5",
  "USN": "uuid:f40c2981-7329-40b7-8b04-27f187aecfb5",
  "LOCATION": "10.0.2.9/desc.html",
  "CACHE-CONTROL": "max-age=1800",
  "DATE": "Mon, 16 Oct 2017 03:19:12 GMT",
  "SERVER": "node.js/6.11.4 UPnP/1.1 node-ssdp/3.2.5",
  "EXT": ""
}
{
  "address": "10.0.2.9",
  "family": "IPv4",
  "port": 1900,
  "size": 266
}
nrk266lab6vm2@client:~/Downloads/node-ssdp-master/example$
```

Figure shows client side where client.js is running and has received m-search response from ipv4 10.0.2.9 which is the server VM's IP address.

VM2_266_LAB6 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Capturing from enp0s3

Apply a display filter ... <Ctrl-/>

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
39	60.144748543	10.0.2.9	239.255.255.250	SSDP	366	NOTIFY * HTTP/1.1
40	60.145005578	10.0.2.9	239.255.255.250	SSDP	311	NOTIFY * HTTP/1.1
41	60.145016032	10.0.2.9	239.255.255.250	SSDP	302	NOTIFY * HTTP/1.1
42	70.152912830	10.0.2.9	239.255.255.250	SSDP	354	NOTIFY * HTTP/1.1
43	70.152923362	10.0.2.9	239.255.255.250	SSDP	366	NOTIFY * HTTP/1.1
44	70.153084305	10.0.2.9	239.255.255.250	SSDP	368	NOTIFY * HTTP/1.1
45	70.153087426	10.0.2.9	239.255.255.250	SSDP	311	NOTIFY * HTTP/1.1
46	70.153088449	10.0.2.9	239.255.255.250	SSDP	302	NOTIFY * HTTP/1.1
47	80.153899607	10.0.2.9	239.255.255.250	SSDP	354	NOTIFY * HTTP/1.1
48	80.156052350	10.0.2.9	239.255.255.250	SSDP	366	NOTIFY * HTTP/1.1
49	80.156064839	10.0.2.9	239.255.255.250	SSDP	368	NOTIFY * HTTP/1.1
50	80.156068936	10.0.2.9	239.255.255.250	SSDP	311	NOTIFY * HTTP/1.1
51	80.156071235	10.0.2.9	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
52	81.285965376	10.0.2.10	239.255.255.250	SSDP	54	Membership Report / Join group 239.255.255.250 for any sources
53	81.286737873	10.0.2.10	224.0.0.22	IGMPv3	363	HTTP/1.1 200 OK
54	81.287120887	10.0.2.9	10.0.2.10	SSDP	54	Membership Report / Join group 239.255.255.250 for any sources
55	82.270748837	10.0.2.10	224.0.0.22	IGMPv3	136	M-SEARCH * HTTP/1.1
56	86.228752365	10.0.2.10	239.255.255.250	SSDP		

Frame 1: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface 0

Ethernet II, Src: PcsCompu_4a:90:4e (08:00:27:4a:90:4e), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)

Internet Protocol Version 4, Src: 10.0.2.10, Dst: 224.0.0.251

User Datagram Protocol, Src Port: 5353, Dst Port: 5353

0000 01 00 5e 00 00 fb 08 00 27 4a 90 4e 08 00 45 00 ..^.... 'J.N..E.

0010 00 49 91 f1 40 00 ff 11 fc ac 0a 00 02 0a e0 00 .I..@.....

0020 00 fb 14 09 14 09 00 35 e0 40 00 00 00 00 025..K.....

0030 00 00 00 00 00 05 5f 69 70 70 73 04 5f 74 63 ipps..tc

0040 70 05 6c 6f 63 61 6c 00 00 0c 00 01 04 5f 69 70 p.local.ip

0050 70 c0 12 00 0c 00 01

User Datagram Protocol (udp), 8 bytes

Packets: 69 - Displayed: 69 (100.0%)

Profile: Default

Figure shows wireshark analysis of client side VM, where SSDP protocol is followed.