LAB ASSIGNMENT 6 **SJSU ID**: 012018487 **NAME**: NIVEDHITHA RAMARATHNAM KRISHNA

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.

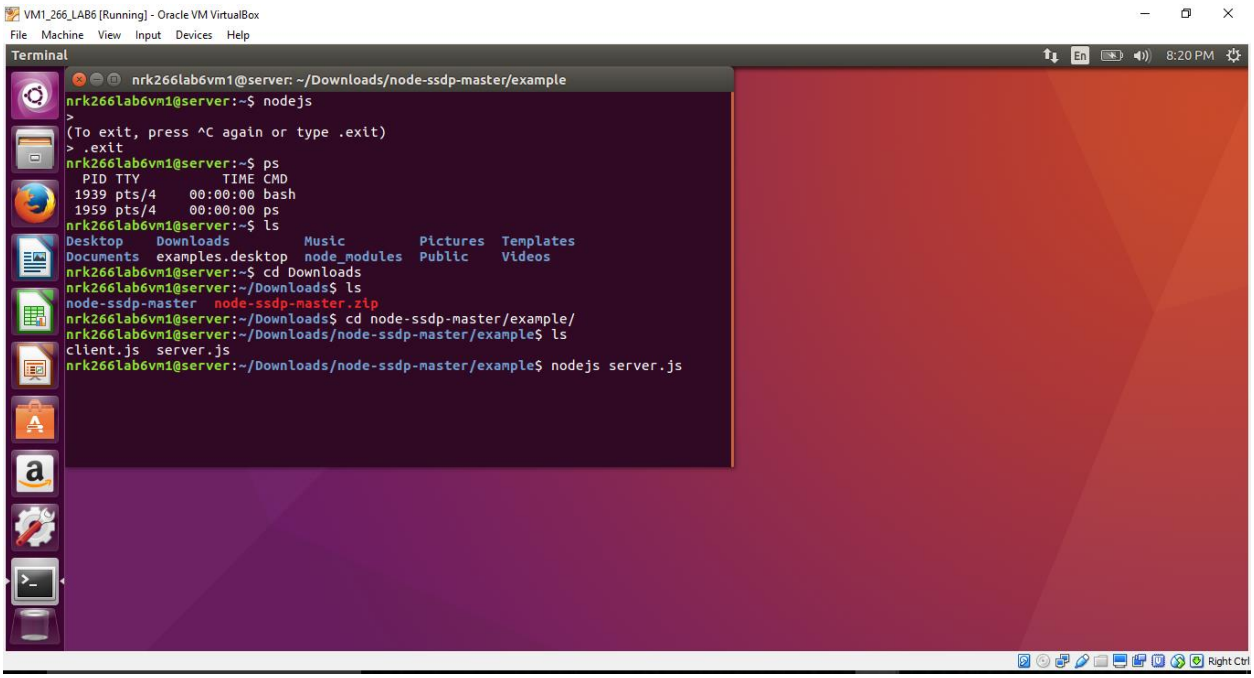

Figure shows server side 'server.js' started.

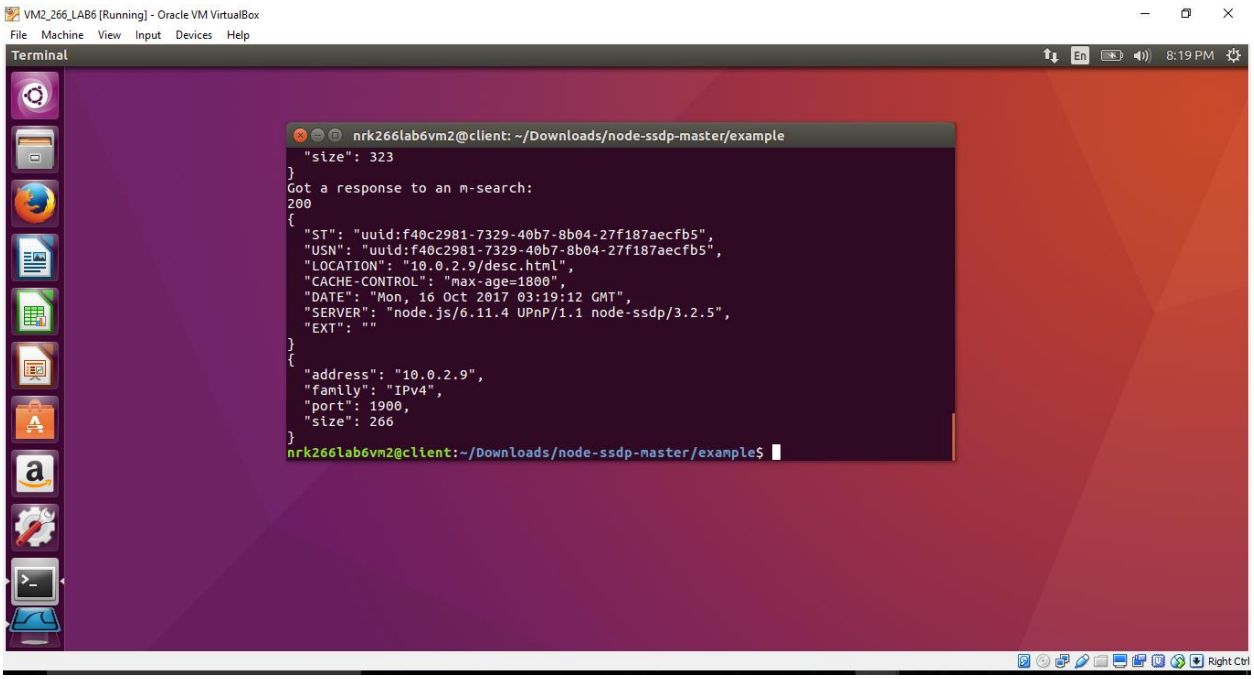

Figure shows client side where client.js is running and has received m-search response from ipv4 10.0.2.9 which is the server VM's IP address.

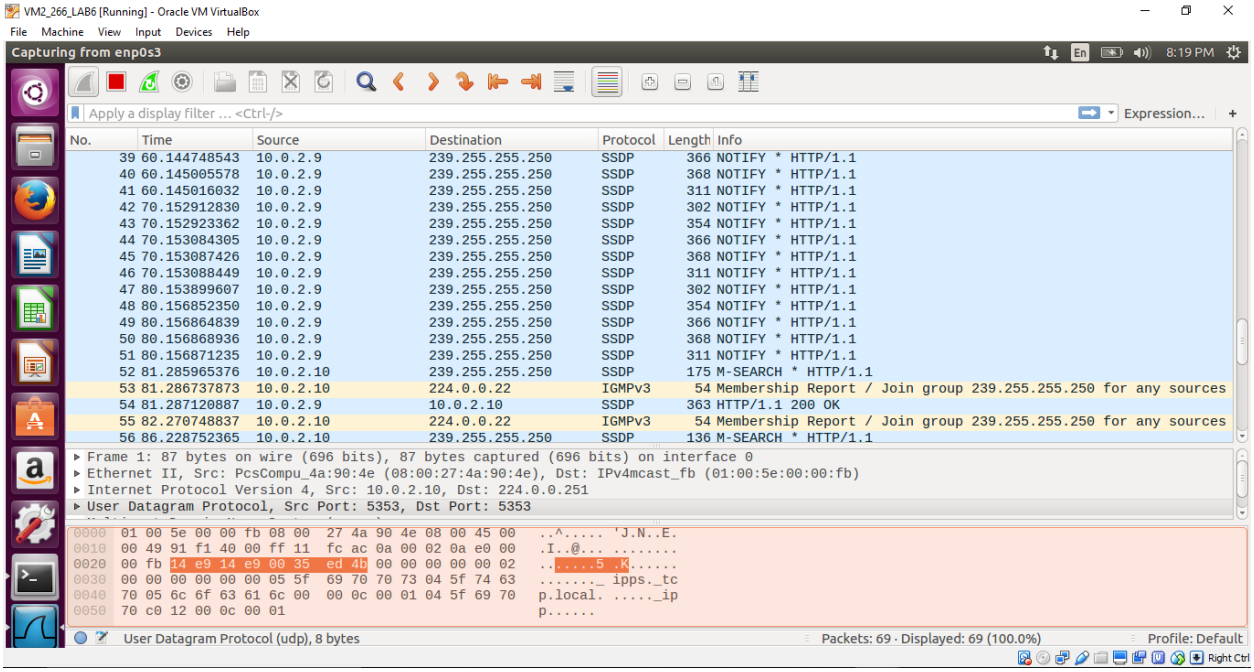

Figure shows wireshark analysis of client side VM, where SSDP protocol is followed.