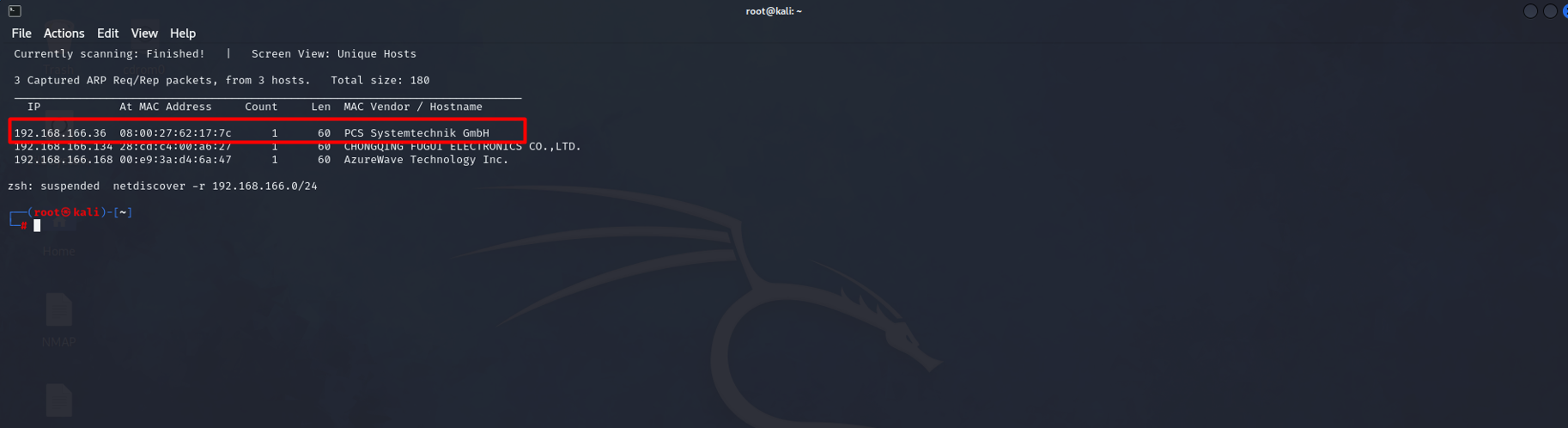
**CSM EXAM PAPER – INEURON**

**Question 1- Scanning:**

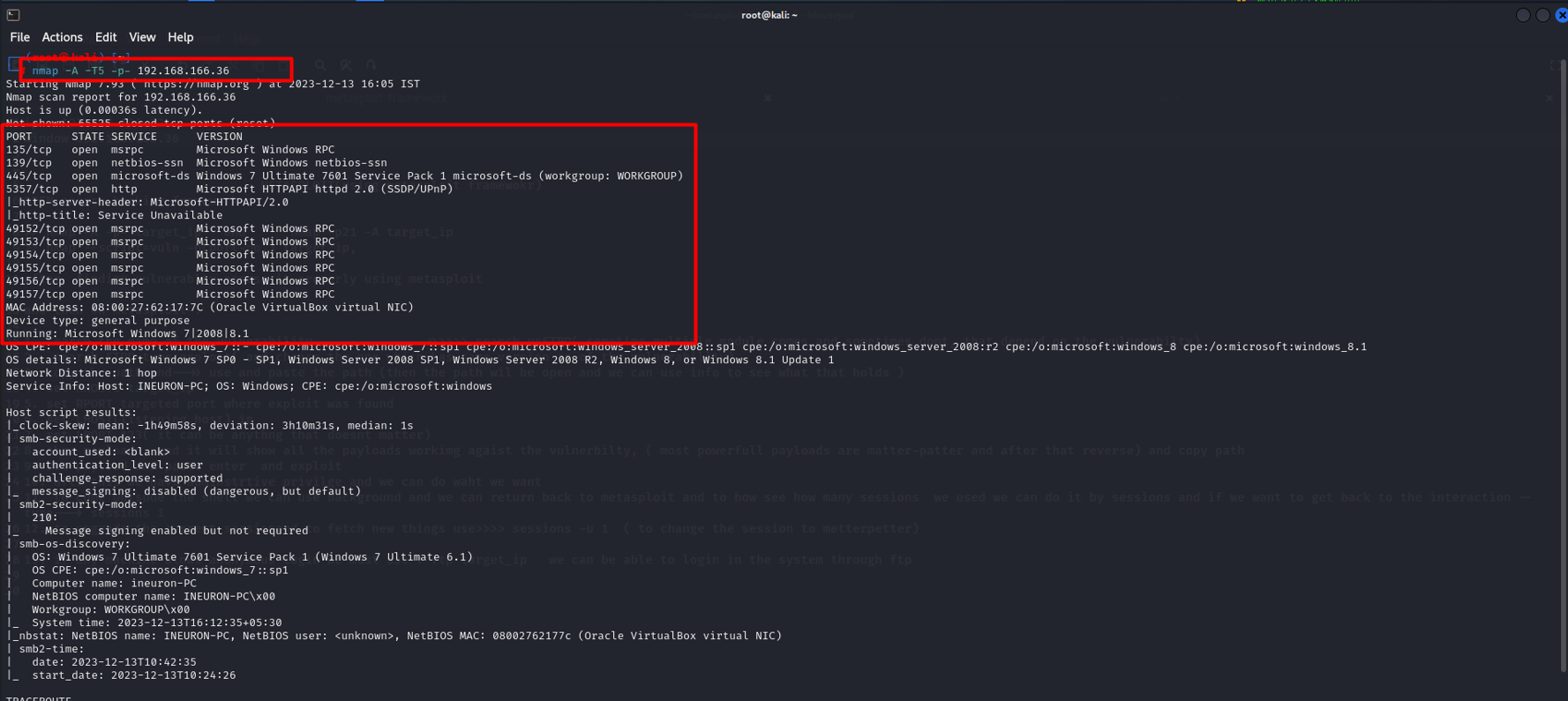
* Task One -: Lab setup done.
* Task Two-: Both Kali and windows set-up in Host-Only network.

Lab Setup done.

* Task 3-: Host Found using command: **net-discover.**

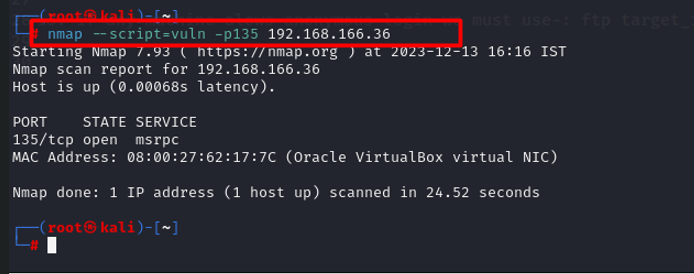


* Performed **NMAP** scan on the Host found.



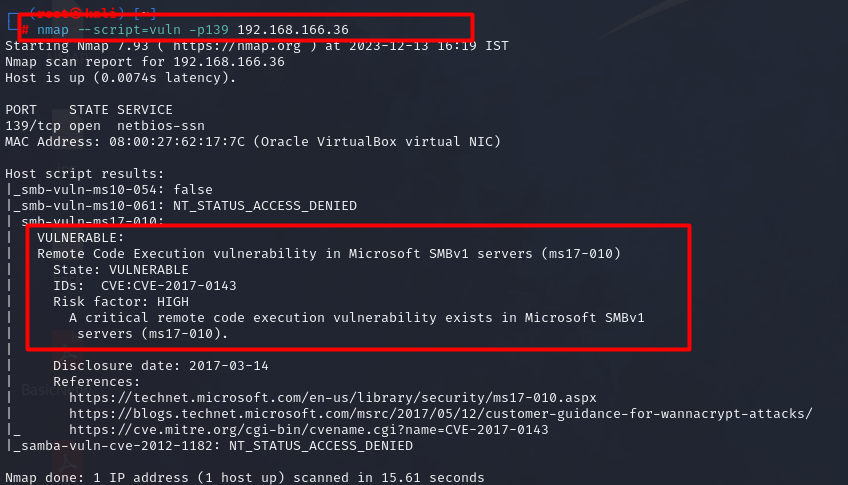
Found multiple open ports like- **135, 139, 445 and 5357.**

* Next up I Scanned port 135 for any vulnerabilities.



Found Nothing.

* Next I scanned port 139.

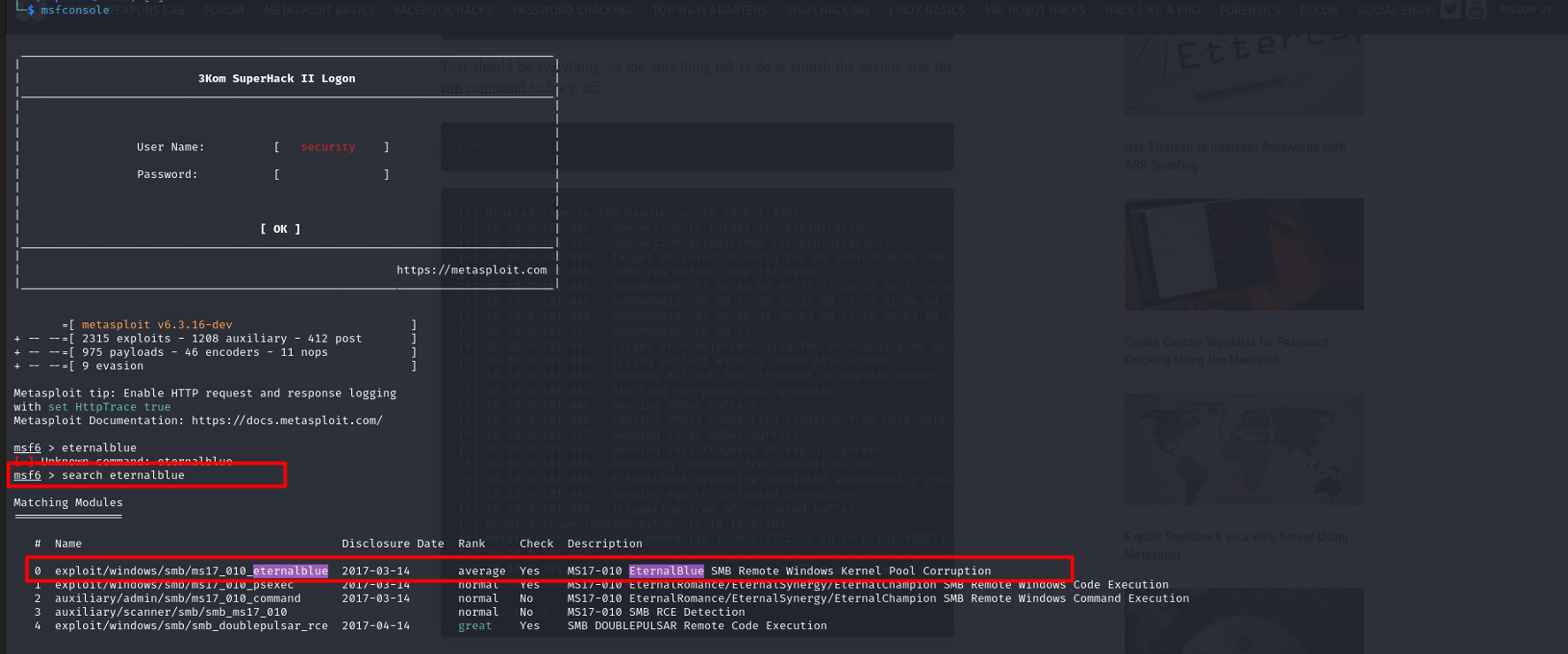


**Found RCE and the vulnerable version (ms17-010).**

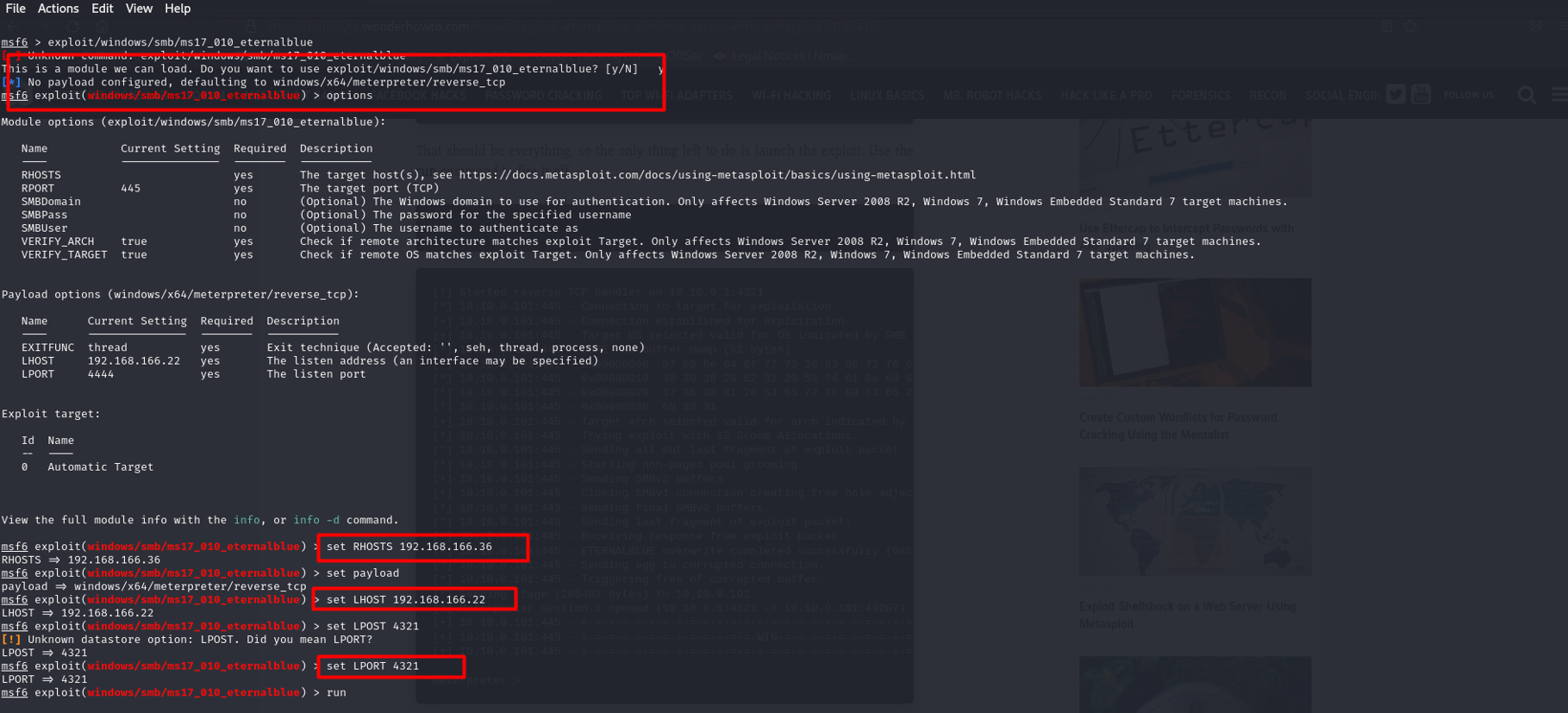
**Question -2: Exploitation**

Next Up is started METASPLOIT to get RCE.

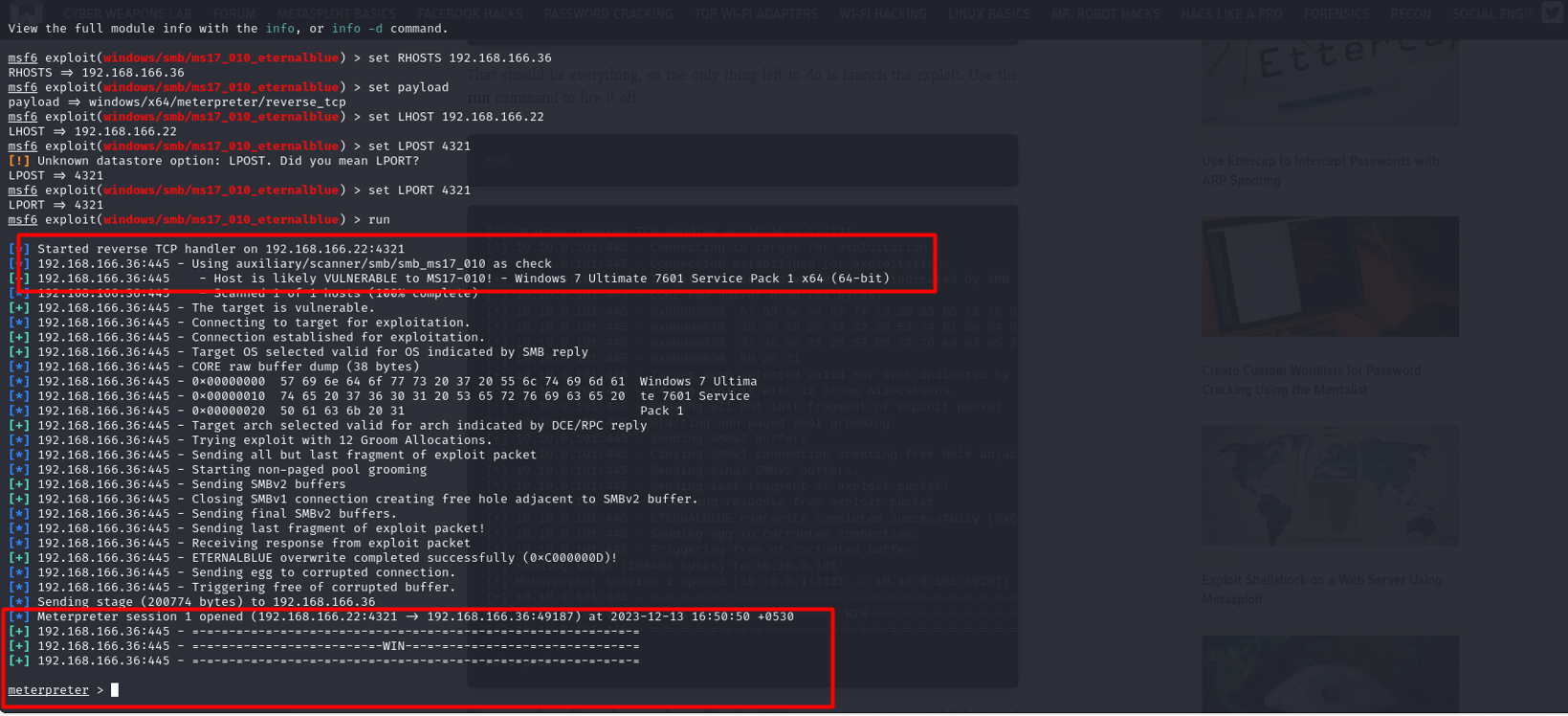
* Searched eternalblue got the exploit.



* Next, setting up with RHOST, LHOST, LPORT.



* Got meterpreter.



**Question 3- Password Attack**

* Started session in the meterpreter and found multiple users.



* Dumped password for each-user.

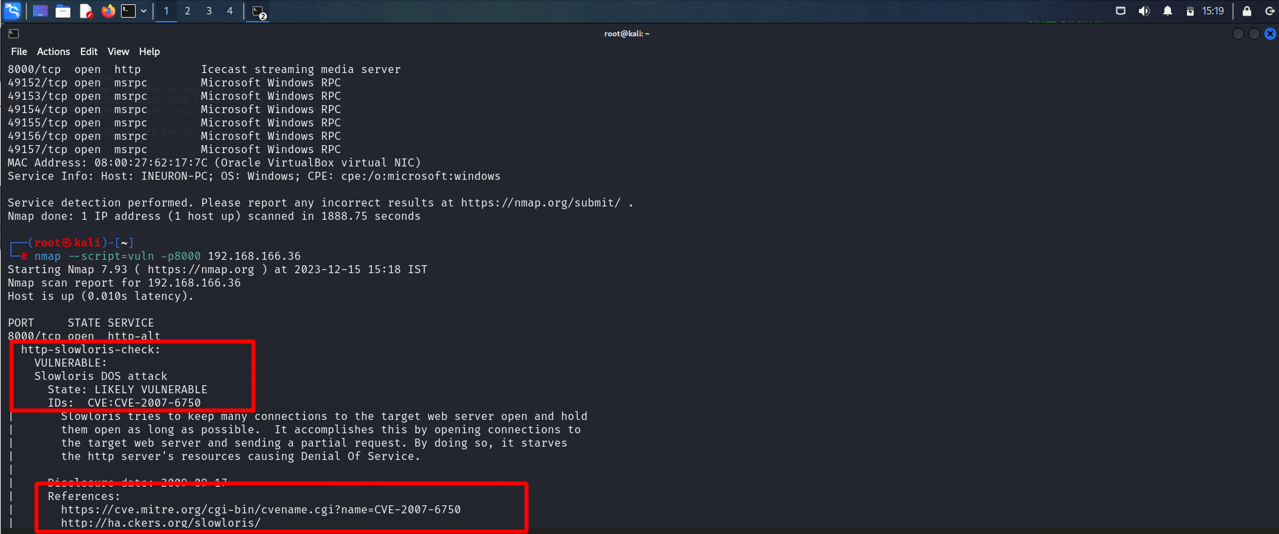


**ICE-CAST SERVER-:**

* ICE-Cast stands for "Internet Communication Engine CAST" is an open-source streaming media server software that allows users to stream audio content over the Internet. It supports various audio formats such as MP3, Ogg-Vorbis, and AAC, making it versatile for different streaming needs.
* It is capable of serving a large number of concurrent listeners around the globe. It operates on the client-server model, where the server hosts audio files and streams them to clients (such as media players or web browsers) that request them.

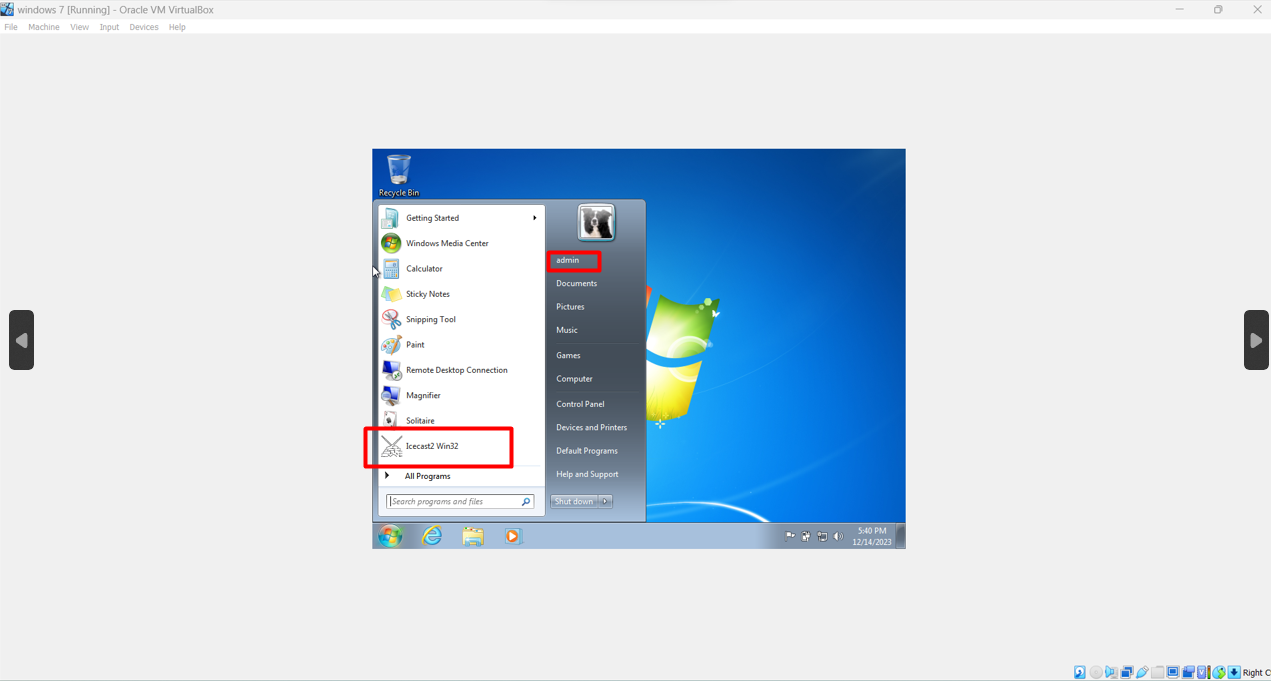
**Vulnerability Related to ICE-CAST SERVER-:**

* **Buffer-Overflow(CVE-2018-18820**) **-:** A buffer overflow is a software vulnerability where a program writes more data into a buffer than it can hold, causing excess data to overwrite adjacent memory locations. This can lead to data corruption, program crashes, or, if exploited by attackers, unauthorized code execution, potentially compromising the security and stability of the system.
* **Exploitation-:** By sending malicious requests containing carefully crafted payloads designed to overflow the buffer, an attacker can potentially overwrite critical data structures or execute arbitrary code within the server's memory space. This can lead to the server becoming unstable, crashing, or becoming unresponsive.
* **Impact-: “**Buffer-Overflow can lead to Denial-of-service.**”** Exploiting a buffer overflow vulnerability in ICE-Cast could result in a DoS condition. When the server crashes or becomes unresponsive due to the buffer overflow, it can no longer serve legitimate requests from clients, effectively denying service to legitimate users.

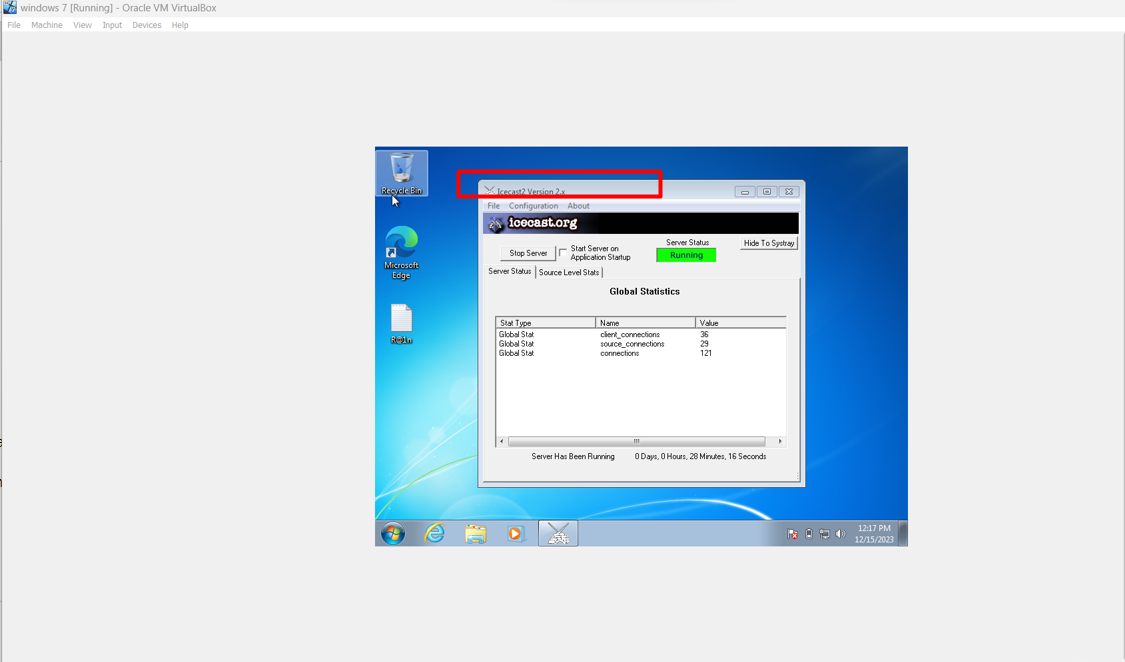


**Question 4- Vulnerability Analysis and Exploit Research-:**

* Got the password and logged in Admin user.



* Started Ice-cast server-:



* Again performed NMAP scan and found on which port the service is working.



***Remark-:*** Due to lack of configuration unable to perform web-server based exploitation.

**Question 6 -: Wireshark analysis**

Ans1-: **Hydra**

Ans2-: **Jenny**

Ans3-: **password123**

Ans4-: **var/www/html**

Ans5-: **shell.php**

Ans6**-: INEURON-PC**

Ans7-: **Site CHMOD 777 shell.php**

Ans8-: **Rootkit**