**Windows xp**

**Name:- Binay Chaudhary**

**Add:- Satungal**

**Date:- 2/12/2023**

**Time:- 12 pm**

**Introduction**

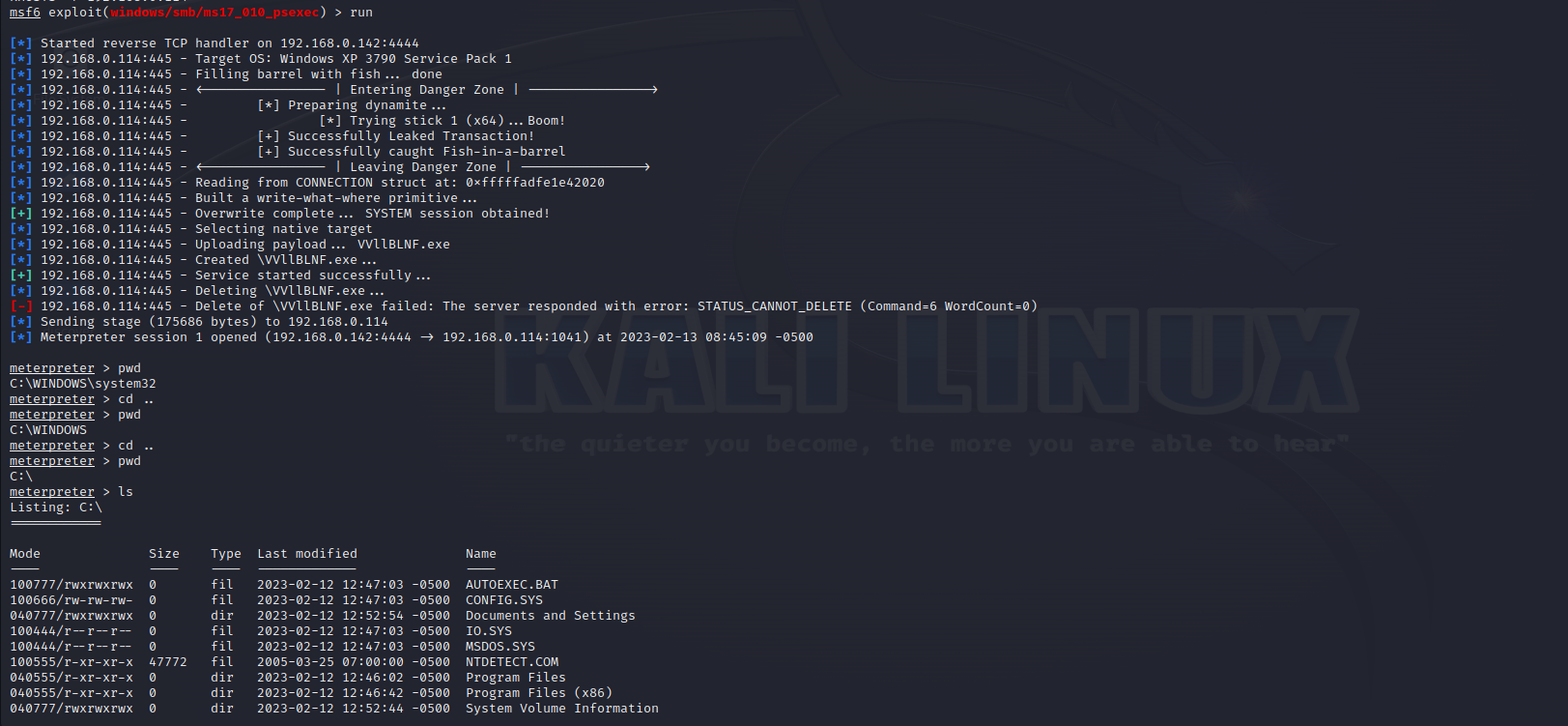
1. **Nmap**
2. **Metasploit**

**Nmap**

Nmap provides a number of features for probing computer networks, including host discovery and service and [operating system](https://en.wikipedia.org/wiki/Operating_system) detection. These features are extensible by [scripts](https://en.wikipedia.org/wiki/Scripting_language) that provide more advanced service detection,[[6]](https://en.wikipedia.org/wiki/Nmap#cite_note-Nmap_Scripting_Engine-6) vulnerability detection,[[6]](https://en.wikipedia.org/wiki/Nmap#cite_note-Nmap_Scripting_Engine-6) and other features. Nmap can adapt to network conditions including [latency](https://en.wikipedia.org/wiki/Network_latency) and [congestion](https://en.wikipedia.org/wiki/Network_congestion) during a scan.

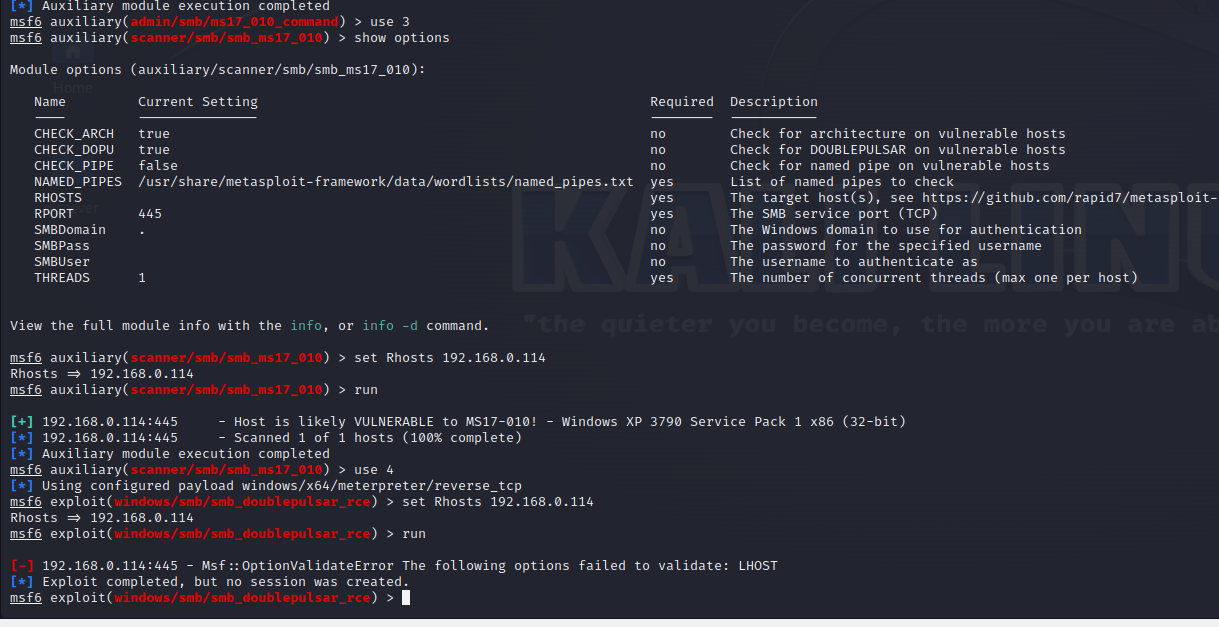
Here, in this above picture we can see the vulnerability that are find in the windows xp through the Open port. We can get access the root directory of windows xp and the data of the company may compromise.

**Microsoft Windows system vulnerable to remote code execution (MS08-067)**



In this, in this above picture I’ve found the loop holes, that be exploited and can be access the company’s computer which may loss them

Here, in this section we have exploited the loop holes and can get access his sensitive data.



Here in this above picture, we can see that there is no any loops holes that can be exploited but the no. 1 loop holes is exploited due to which we can get access company computer and may harm them.