Report on Windows XP vulnerability

Logo, company name

Description automatically generated

Submitted by:

Uttam Kumar Rajbanshi

Submitted to:

Director of SB Computer

Date: 2023/01/02

Time: 08:31 PM

Contents

[Introduction to Windows XP 3](#_Toc123661012)

[Scanning 4](#_Toc123661013)

[Nmap 4](#_Toc123661014)

[Exploitation 5](#_Toc123661015)

[Searching for listed vulnerability 5](#_Toc123661016)

[Set target and get exploit 6](#_Toc123661017)

[Conclusion 7](#_Toc123661018)

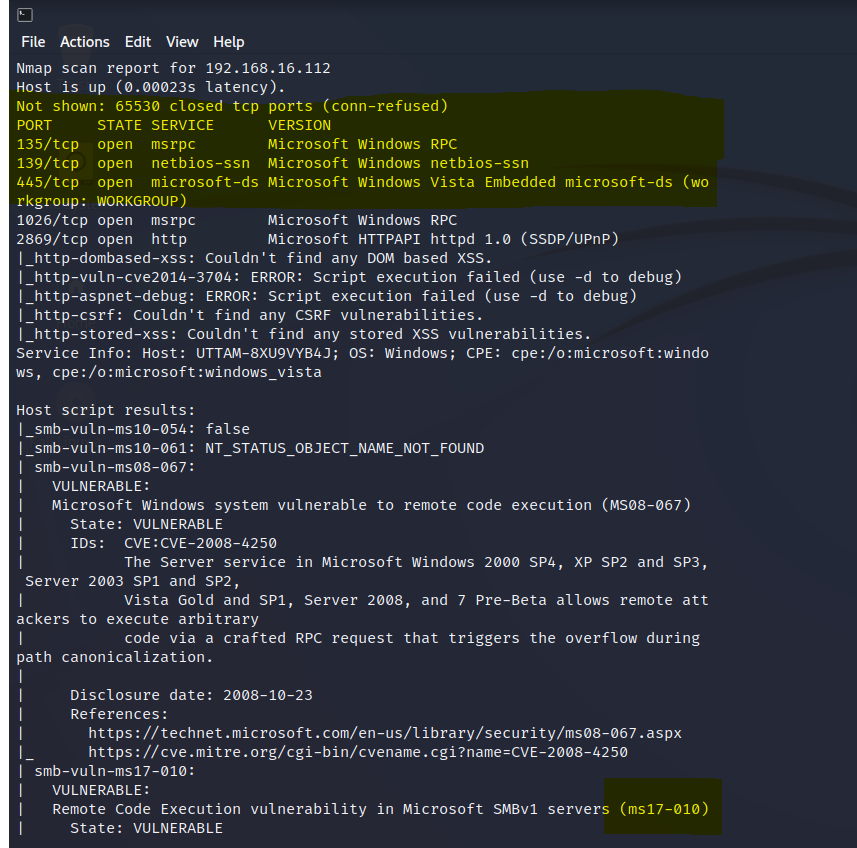
# Introduction to Windows XP

Windows XP is an operating system that was produced by Microsoft as part of the Windows NT family of operating systems. It was released to the public on October 25, 2001, and was the successor to the Windows 2000 operating system. Windows XP was designed to be a more stable and user-friendly version of Windows, and it included several new features such as a revamped user interface, improved support for multimedia, and better networking capabilities. It was widely used until the release of its successor, Windows Vista, in 2007. Although Microsoft stopped supporting Windows XP in 2014, it remains a popular operating system, particularly in developing countries.

This is an old operating system of Microsoft which has no security support now. Which make it vulnerable from external threats.

# Scanning

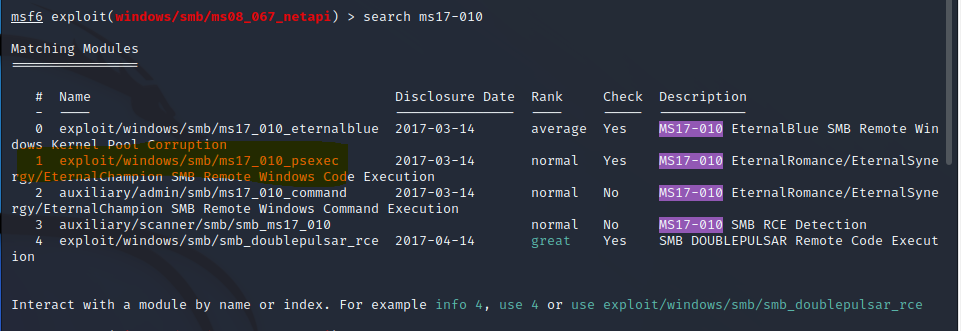
## Nmap



At the bottom of the screenshot above we can see highlighted the RCE vulnerability ms17-010. Through this we can get meterpeter shell access through Metasploit framework.

# Exploitation

## Searching for listed vulnerability



First I searched for vulnerability that is shown in the nmap scan, after that I used Metasploit framework for exploitation as shown in the above screenshot. I used 1 option for the exploitation we can see in the below picture.

Text

Description automatically generated

## Set target and get exploit

Text

Description automatically generated

Here we can see I set ipaddress of the victim and set target and used run command. And at the end I got meterpreter shell we can see in the above screenshot in the bottom.

# Conclusion

Vulnerability ms17-010 which is in the windows xp that is vulnerable which provide backdoor to the attacker which can access through meterpreter shell.