World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:17, No:01, 2023

Exploiting SLMail Server with a Developed Buffer Overflow with Kali Linux

Authors : Senesh Wijayarathne

Abstract : This study focuses on how someone could develop a Buffer Overflow and could use that to exploit the SLMail Server. This study uses a Kali Linux V2018.4 Virtual Machine and Windows 7 - Internet Explorer V8 Virtual Machine (IPv4 Address - 192.168.56.107). This study starts by sending continued bytes to the SLMail Server to find the crashing point range and creating a unique pattern of the length of the crashing point range to control the Extended Instruction Pointer (EIP). Then by sending all characters to SLMail Server, we could observe and find which characters are not rendered properly by the software, also known as Bad Characters. By finding the 'Jump to the ESP register (JMP ESP) and with the help of 'Mona Modules', we could use msfvenom to create a non-stage windows reverse shell payload. By including all the details gathered previously on one script, we could get a system-level reverse shell of the Windows 7 PC. The end of this paper will discuss how to mitigate this vulnerability.

Keywords : slmail server, extended instruction pointer, jump to the esp register, bad characters, virtual machine, windows 7, kali Linux, buffer overflow, Seattle lab, vulnerability
Conference Title : ICCH 2023 : International Conference on Cybersecurity and Hacking
Conference Location : London, United Kingdom
Conference Dates : January 23-24, 2023