Metasploit Exploit Report

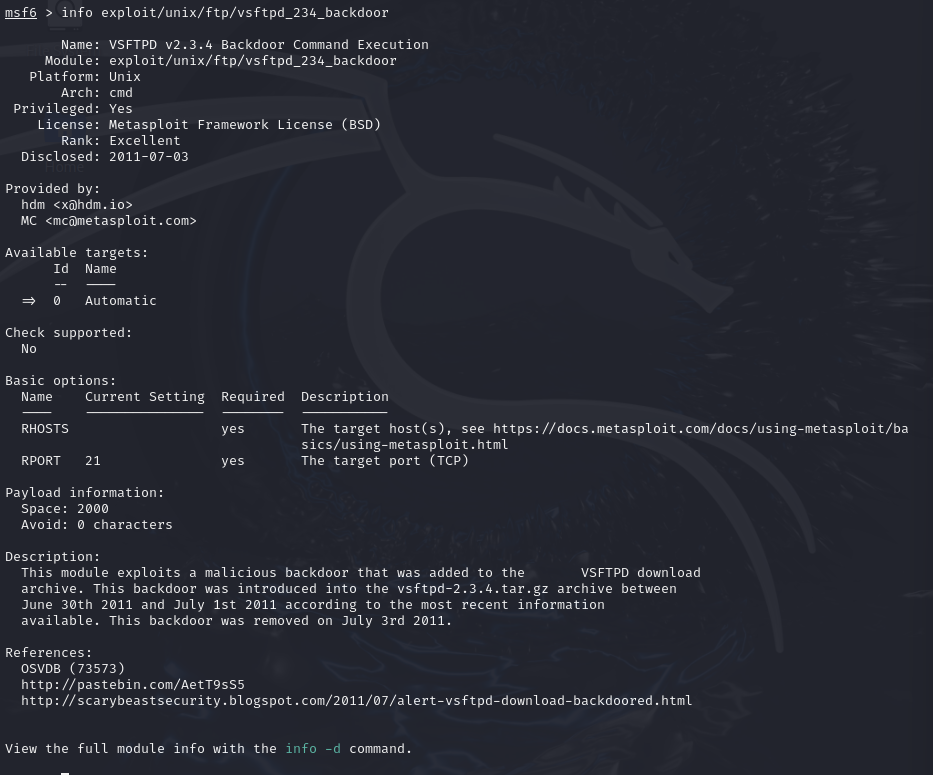
# 1. Introduction

This report demonstrates the use of the Metasploit Framework to search for and analyze a known exploit. The assignment involved launching Metasploit, searching for an exploit, and reporting its technical details.

# 2. Launching Metasploit

The Metasploit Framework was launched using the following command in Kali Linux:

msfconsole



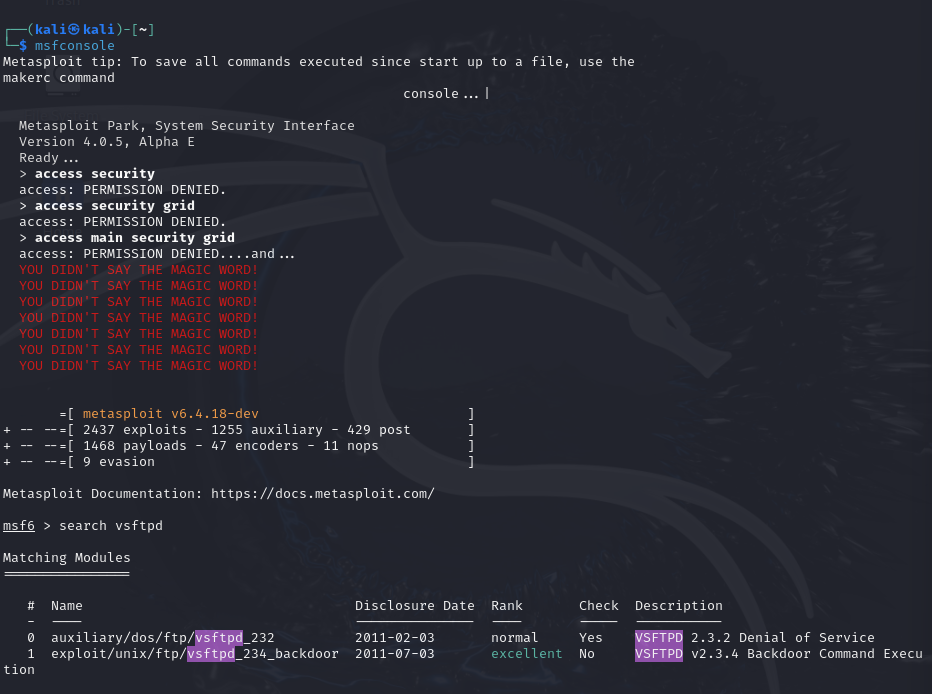
This initialized the Metasploit Framework and provided access to its modules and tools.

# 3. Searching for an Exploit

The following command was used to search for available exploits related to the 'vsftpd' service:

search vsftpd

The results showed two available modules, including a highly ranked backdoor exploit:



# 4. Exploit Details

The selected exploit was 'exploit/unix/ftp/vsftpd\_234\_backdoor'. Its details are as follows:

• Name: VSFTPD v2.3.4 Backdoor Command Execution  
• Platform: Unix  
• Architecture: cmd  
• Privileged: Yes  
• Disclosure Date: 2011-07-03  
• Rank: Excellent  
• RPORT: 21 (TCP Port)  
• RHOSTS: Target host(s)

This module exploits a malicious backdoor that was introduced into the vsftpd-2.3.4 archive. This backdoor allowed attackers to execute arbitrary commands on the server and was present between June 30 and July 1, 2011. It was removed shortly after discovery.

References:

• http://pastebin.com/AetT9sS5

• http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

# 5. Conclusion

The Metasploit Framework provides powerful tools to identify and analyze known vulnerabilities. This assignment demonstrated how to search for a specific exploit and understand its purpose and usage within penetration testing scenarios.