Ex060

Gary Jones

Contents

Technical Report

Finding: *Descriptive NaMe*

Risk Rating

The risk is critical and allows users direct access into the system.

Vulnerability Description

Utilizing vsftpd 234 backdoor users are able to access the website files.

Attack Narrative

After running Nessus several vulnerabilities were detected including a one yielding severity level high: vsftpd Smiley Face Backdoor (see figure 1). This vulnerability was found to be impacting port 21 and is of classification TCP (see figure 2). In addition to this it was found to be exploitable with Metasploit (VSFTPD v2.3.4 Backdoor Command Execution) (see figure 3). Searching for this vulnerability in Metasploit a single payload was found and subsequently used (see figure 4). By issuing this command the file system was identified and the user was able to see the files present on the host system (see figure 5). By utilizing Wireshark and following the TCP Stream the Username and Password was identified (see figure 6). However, it was also found that despite having access to the system, using the tools available thus far, root privelidges were not granted and access was limited.

Identified Key8: KEY008-7pRFQFucThmw16ibIv72EA==

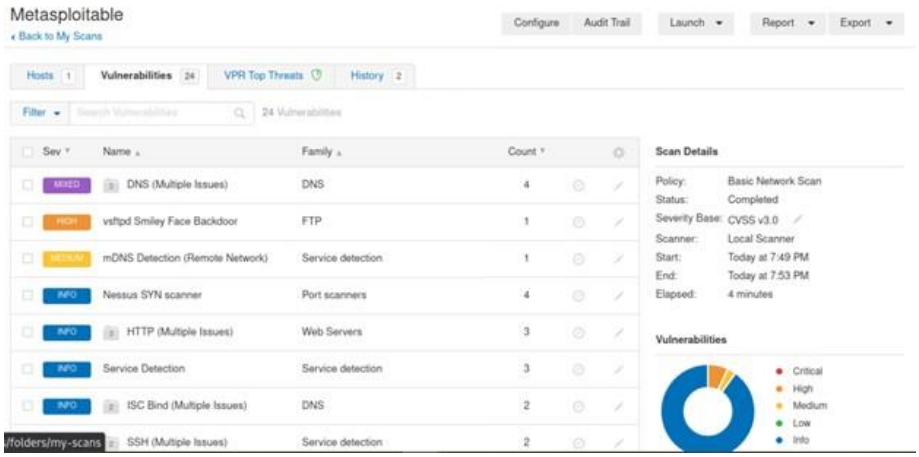

Figure 1:

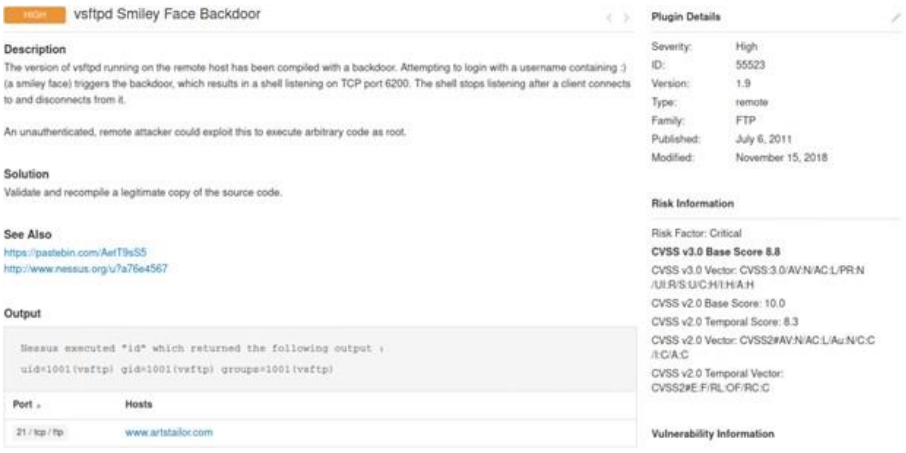

Figure 2:

Vulnerability Information

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: July 3, 2011

Vulnerability Pub Date: July 3, 2011

Exploitable With

Metasploit (VSFTPD v2.3.4 Backdoor Command Execution)

Reference Information

EDB-ID: 17491

BID: 48539

Figure 3:

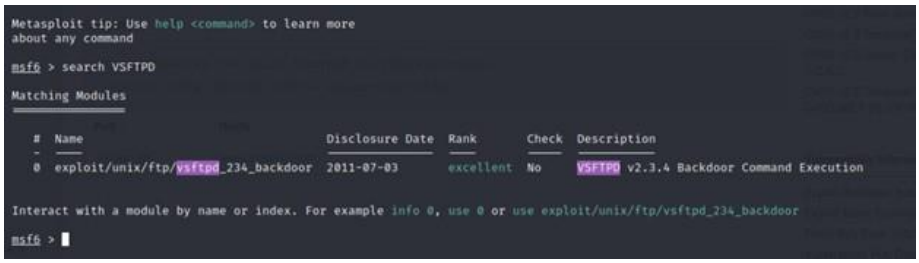

Figure 4:

Figure 5:

Figure 6: