Ex060 Report

Benjamin Ruddy

2022-10-14

Contents

Goal

The goal in this exercise was to perform a vulnerability scan on `www.artstailor.com` with **Nessus**, and subsequently exploit it.

Technical Report

Finding: *VSFTPD 2.3.4 Backdoor*

Severity Rating

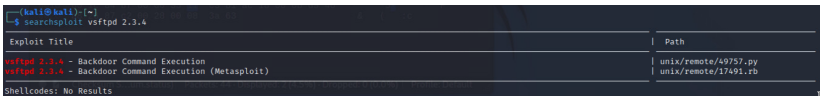
CVSS Base Severity Rating: 8.0 AV:N AC:L PR:N UI:N S:U C:L I:H A:H

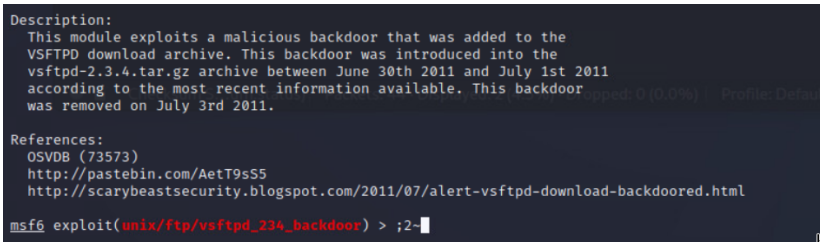
Vulnerability Description

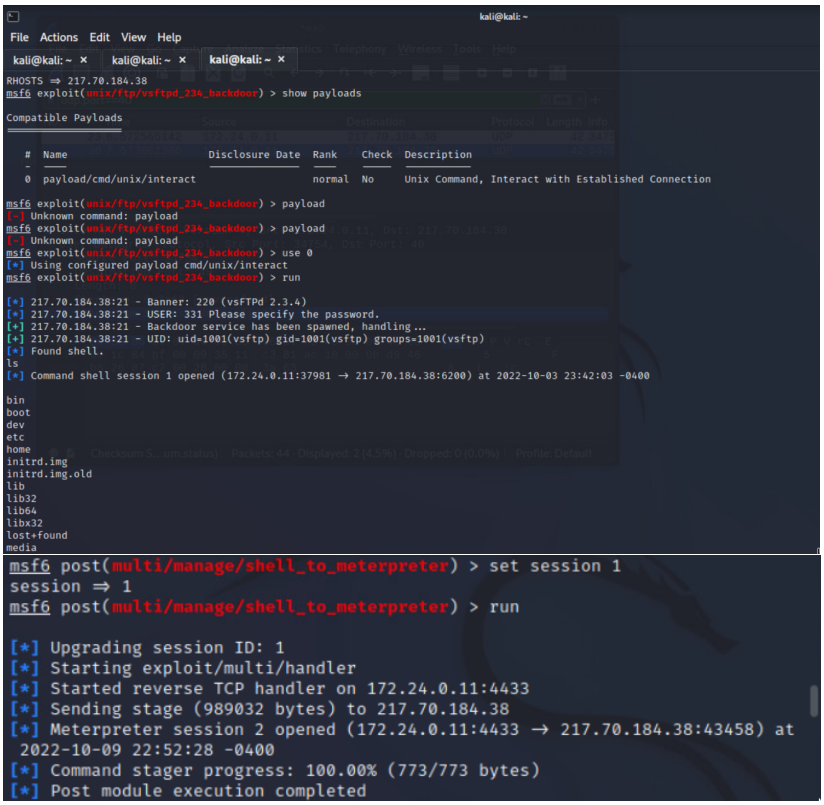
This vulnerability involves a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011, and was removed on July 3rd 2011. It allows malicious users to connect to a shell listening on port 6200 on the remote machine upon logging into the FTP service with a username of `':)'`.

Note: This backdoor typically grants root privileges upon access, however, it only provided access to the `vsftp` upon exploiting it. Thus, the exploit is rated a 8.0 as opposed to the maximum of 10.

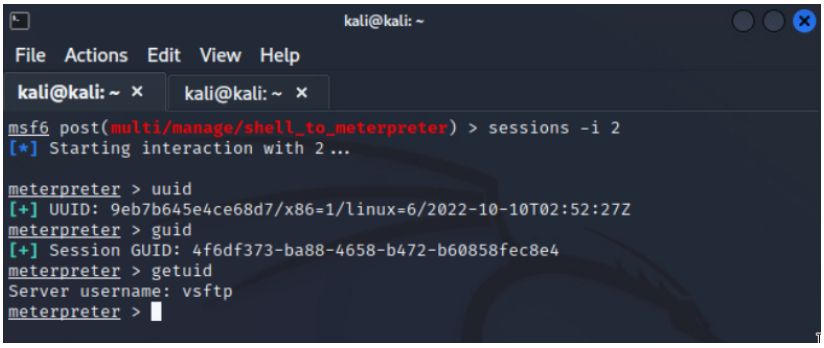
Confirmation methods

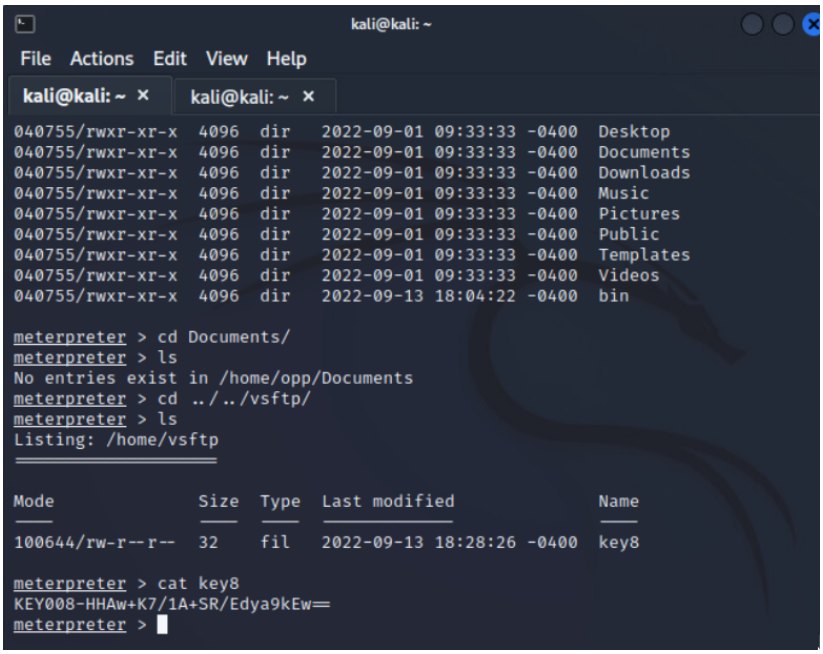




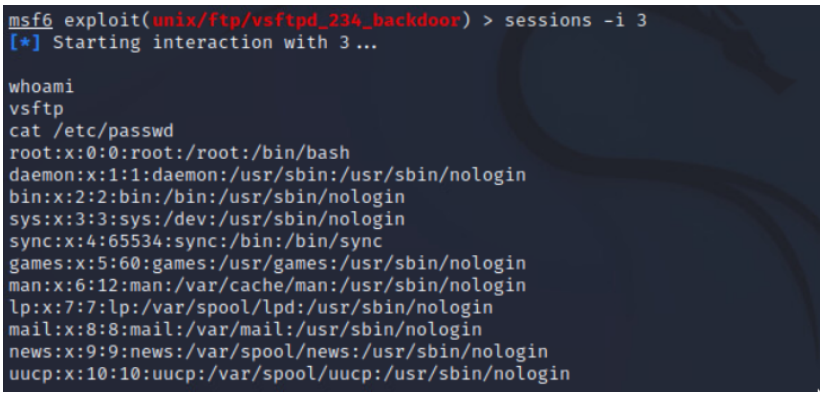


Attempting a shell upgrade using a post-exploitation module from Metasploit





Note the **KEY008** found above upon shell access.



For proof of compromise, the `/etc/passwd` file is shown above.

Mitigation or Resolution Strategy

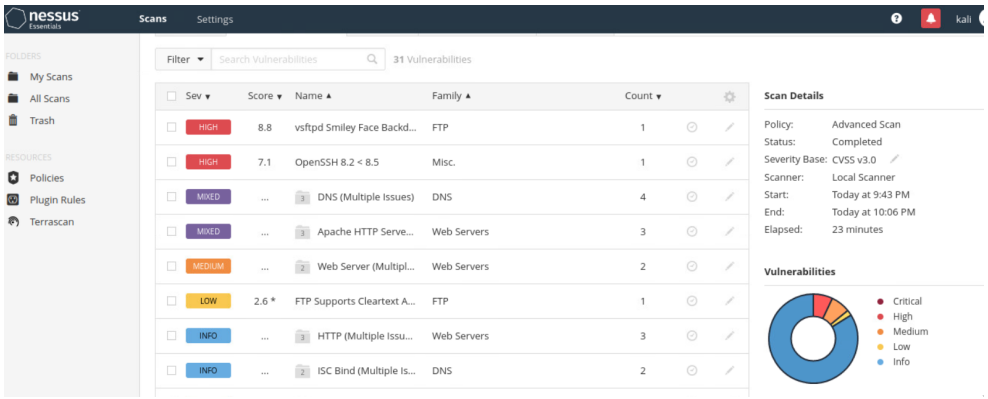
Uninstall the backdoored version immediately, and replace with one that has been verified against the PGP signature of the developers.

If immediate software upgrading/reinstallation is not possible, then at a minimum, block all traffic attempting to come in through port 6200 on the host.

Attack Narrative

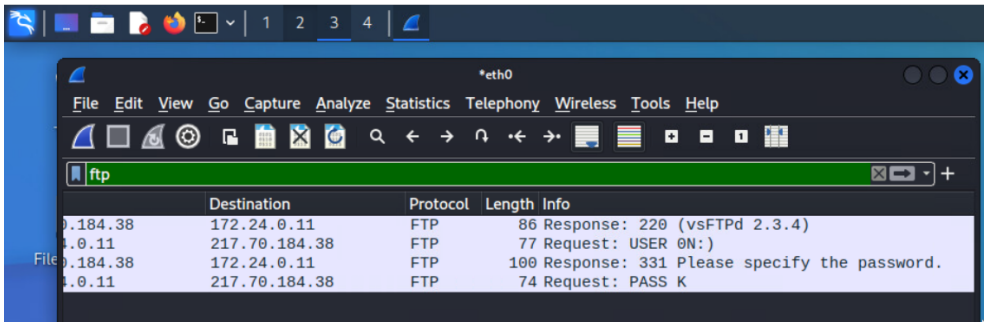
Nessus scan

After customizing a Nessus Advanced Scan for `ns.artstailor.com`, The VSFTPd 2.3.4 backdoor vulnerability was the highest severity finding, as shown below:

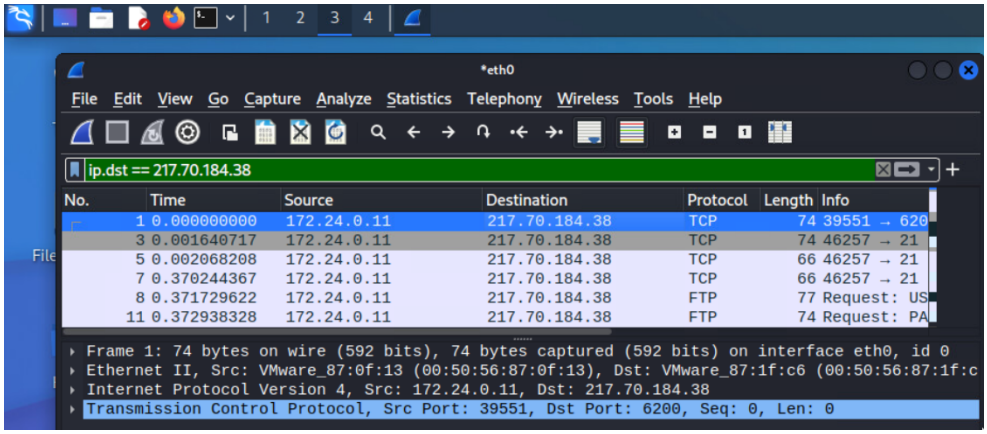


As mentioned in the vulnerability details within the **Technical Report** section, this is a malicious version of the otherwise benign software, VSFTPd. Very likely, attackers were able to replace the file download sources for VSFTPd and uploaded a version that installs a backdoor.

The aforementioned backdoor listens on port 6200 and is triggered when an attacker logs in to the FTP service with the username `':)'`. This was confirmed with a Wireshark scan that captured the credentials as our Metasploit payload was being ran:



Additionally, our packet sniffing with Wireshark confirmed the given information about a malicious shell listening on port 6200:



Using the Metasploit module `unixftpvsftpd_234_backdoor`, we were able to very simply set the target IP and exploit it.

The exact commands, as well as our successful procedure for upgrading the shell, are shown in the **Technical Report**. The `/etc/passwd` file is exfiltrated and shown in this section as well, for proof of comromise.

MITRE ATT&CK Framework TTPs

TA0007: Discovery
- **T1046:** Network Service Discovery
  - **:**

TA0043: Recoinassance
- **T1595:** Active Scanning
  - **.002:** Vulnerability Scanning,