Ex050 Report

Benjamin Ruddy

2022-10-04

Contents

Goal

The goal in this exercise was to explore available hosts on `www.artstailor.com` with **nmap**, and to find a key along the way.

Technical Report

Finding: *VSFTPD 2.3.4 Backdoor*

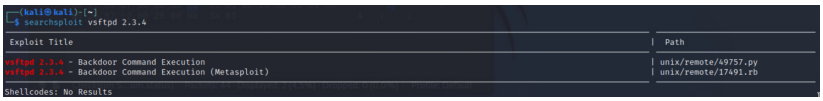
Severity Rating

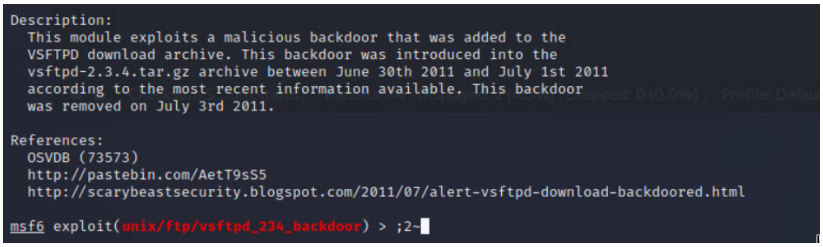
CVSS Base Severity Rating: 9.5 AV:N AC:L PR:N UI:N S:U C:H I:H A:H

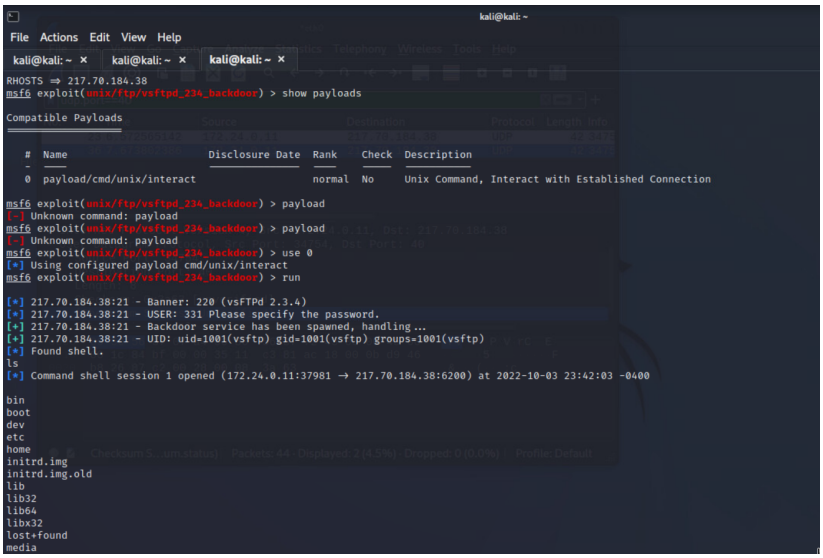
Vulnerability Description

Here you provide a brief description of the nature of the vulnerability. 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.

Confirmation methods







Mitigation or Resolution Strategy

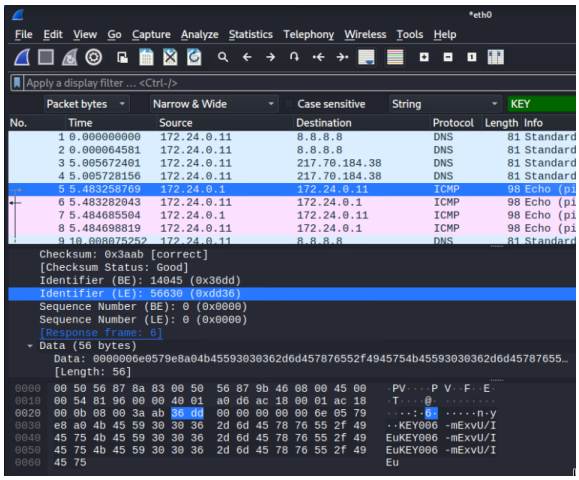
Uninstall the backdoored version immediately, and replace with one that has been verified against the PGP signature of the developers.

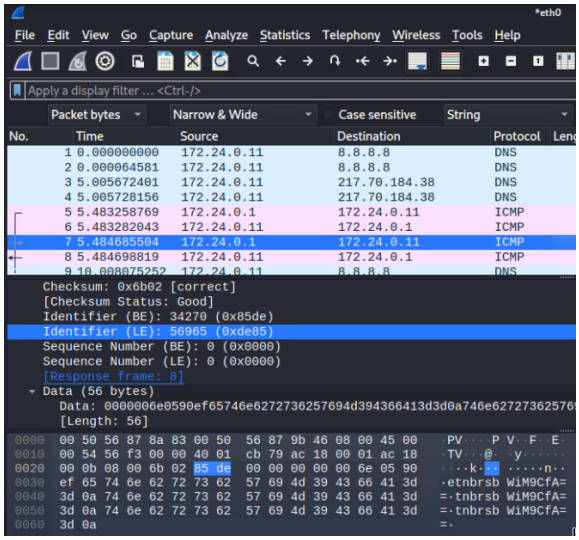
Attack Narrative

Port Scanning

We first started sniffing our network traffic with Wireshark, after which we ran an nmap version detection scan against Art's Tailor Shoppe (`nmap -sV www.artstailor.com`).

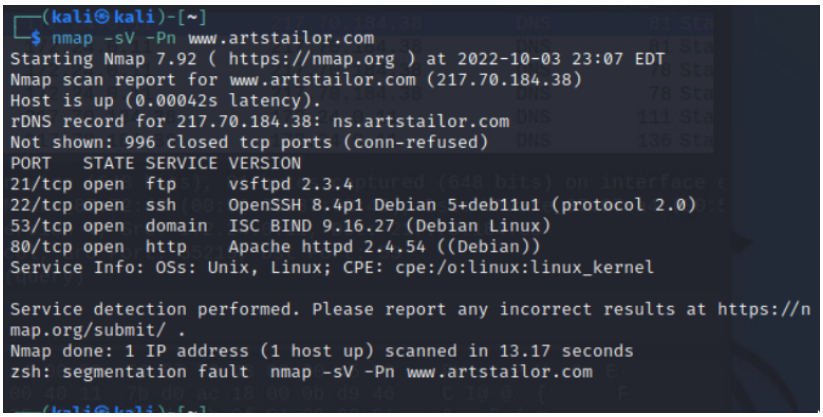
Before we could even notice our nmap scan traffic within wireshark, a KEY was observed within the content bytes of an ICMP Echo request from 172.24.0.1 – our local network gateway for the Kali machine:

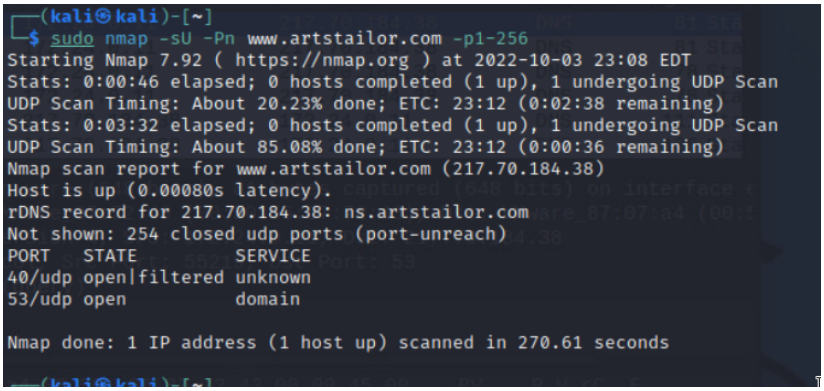




`KEY006-mExvU/IEutnbrsbWiM9CfA==`

This is a similar key discovery method to that of Ex040.





As seen from the above nmap outputs, the nmap UDP scan took a significant amount of time longer (270.61 seconds compared to 13,17 for the TCP scan).

The most obvious reason for this lies in the fact that UDP is a connectionless protocol. In other words, while a TCP scan can instantly receive a response indicating whether a connection was made or not, UDP scans often have to wait for timeouts – which can be relatively long – to truly confirm that no response is being sent back.

Some interesting ports in the output include:

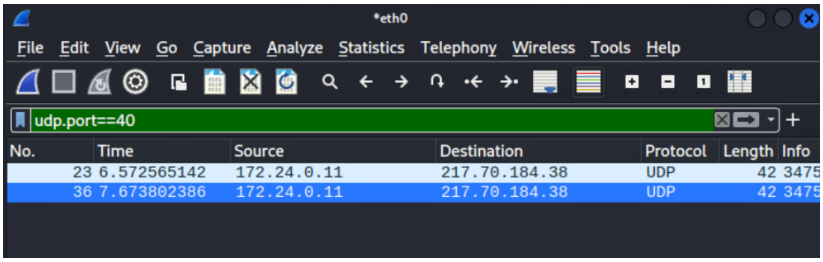
- SSH on TCP port 22, running OpenSSH 8.4p1
- FTP on TCP port 21, running vsftpd 2.3.4
- DNS on both TCP *and* UDP port 53 (this makes sense – DNS uses both protocols)
- An unknown service running on UDP port 40

To elaborate on the odd port number 40, we can reference the nmap wiki page for the UDP scan: https://nmap.org/book/scan-methods-udp-scan.html.

The page tells mentions how often, open UDP ports will not respond to empty probes, and only to specifically formatted probes for whatever service is running.

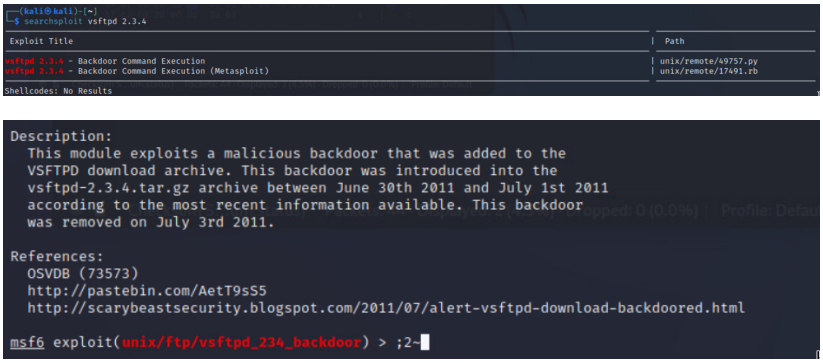
Looking online, there seems to be no universally-agreed service that runs on port 40. As a result, it would make sense that nmap declared the port as `open|filtered` – it cannot craft the right packet to get a response from it, so it is either open *or* filtered.

Our nmap scan confirms the fact that we got no response, because when we apply the filter `udp.port==40`, we can observe that only outgoing packets are captured to port 40:

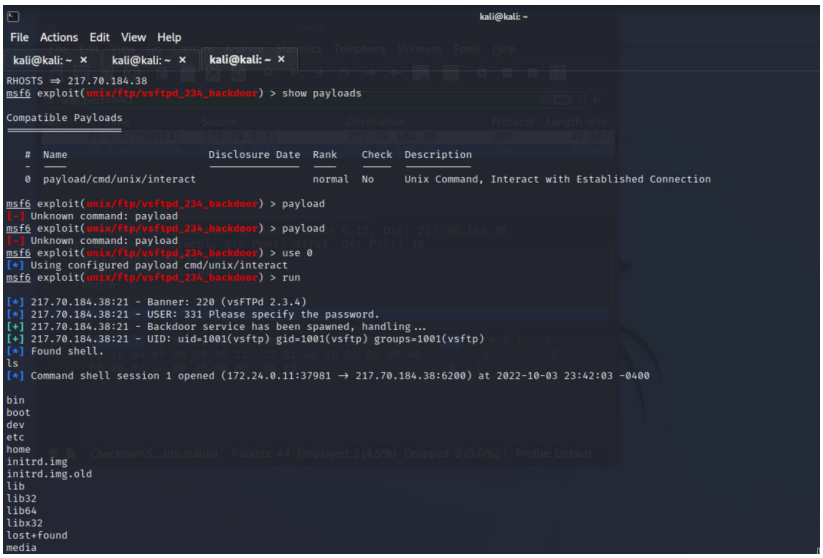


Vulnerable Service

After researching different services on the machine, it was found that the particular vsftpd version that was running on www.artstailor.com had a backdoor embedded into it, from when the version was maliciously published onto the vsftpd website.



The exploit was successfully run with the associated Metasploit module, which gave us terminal access to the remote machine through the vsftpd user:



MITRE ATT&CK Framework TTPs

TA0007: Discovery

T1046: Network Service Discovery

: