Ex050

Gary Jones

Contents

Technical Report

Introduction

Finding: *Descriptive NaMe*

Risk Rating

Two risks were identified. The first was a backdoor command found in the vsftpd 2.3.4 software which is a major risk and the second is a local privilege escalation software present in the Apache 2.4.17 software which is a medium risk.

Attack Narrative

Utilizing the nmap tool www.artstailor.com was probed and 4 ports were found to be open (see figures 1 and 2). When the OS was probed the results were in-conclusive (see figure 2). These results were found by probing with TCP.

When nmap was used to prove www.artstailor.com with UDP the only open port found with 21 (see figure 3). Between the two types of scan UDP took longer than TCP and resulted in fewer observations.

While working in groups our team observed that some members had port 40 appear in their probe while others did not.This led the team to investigate further into this port (see figures 4 and 5) a response was observed coming from it yielding a key value: KEY007-9sGDcP6yOz9NqfkXEmX43A==

Utilizing nmap and searchsploit out team was able to identify two exploits (see figure 6). These exploits are with a backdoor present in the vsftpd 2.3.4 code and a local privilege escalation present int the Apache 2.4.17 code.

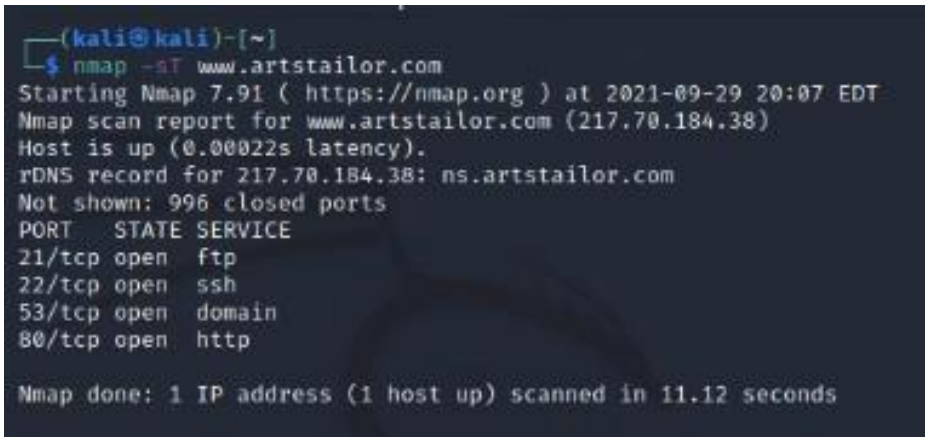

Figure 1:

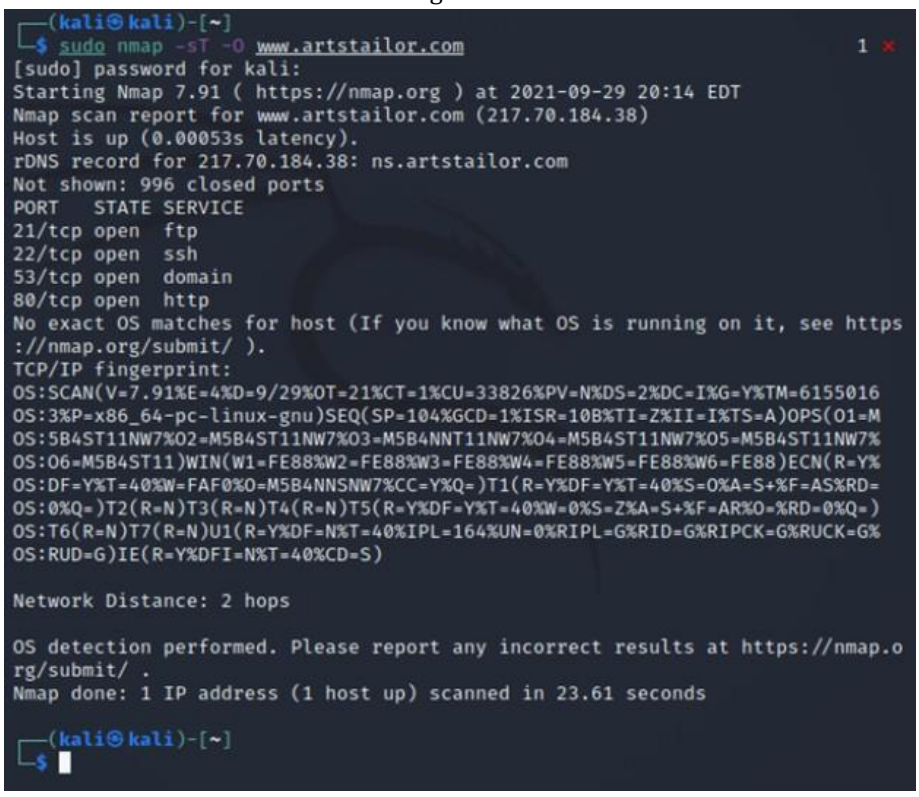

Figure 2:

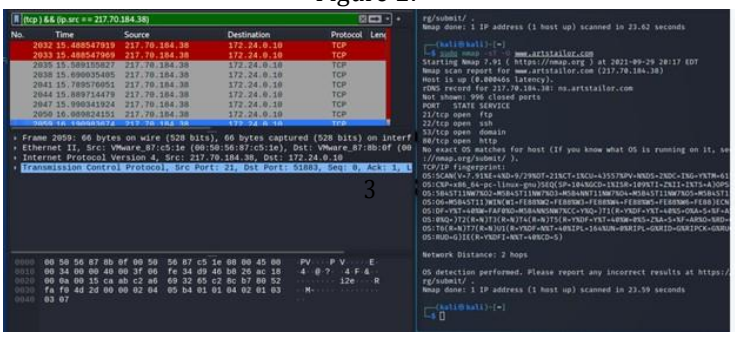

Figure 3:

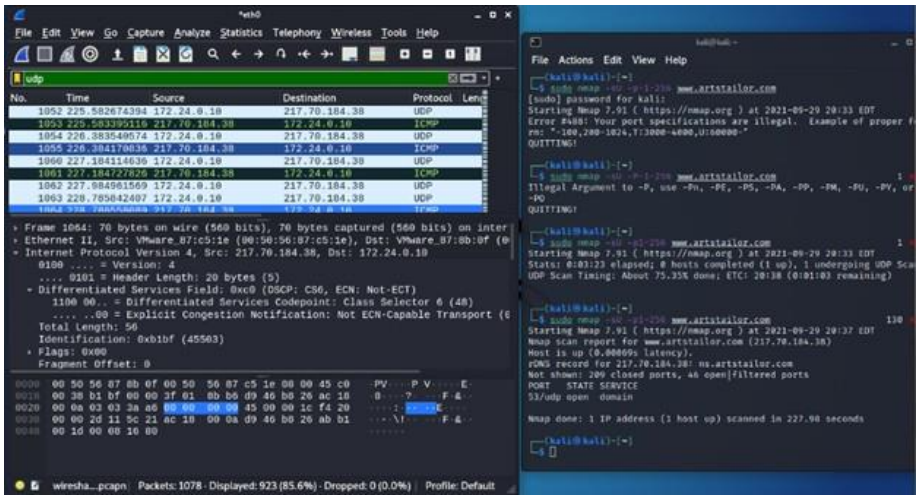

Figure 4:

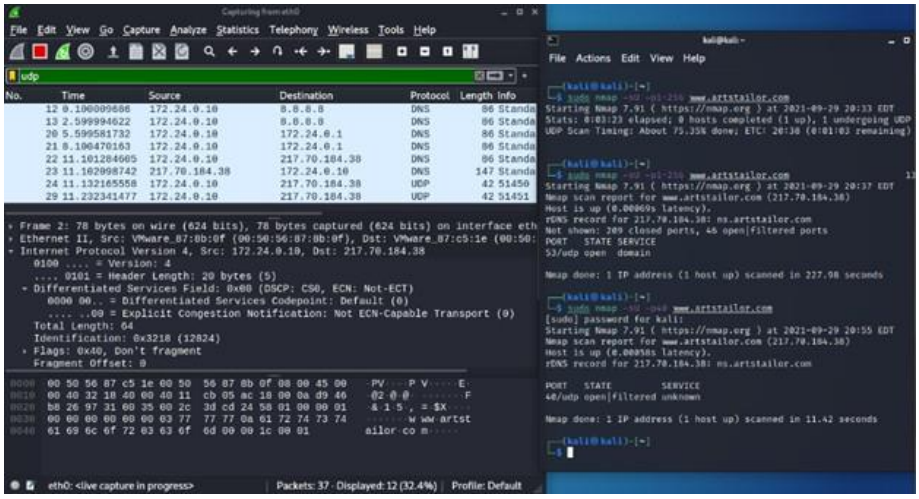

Figure 5:

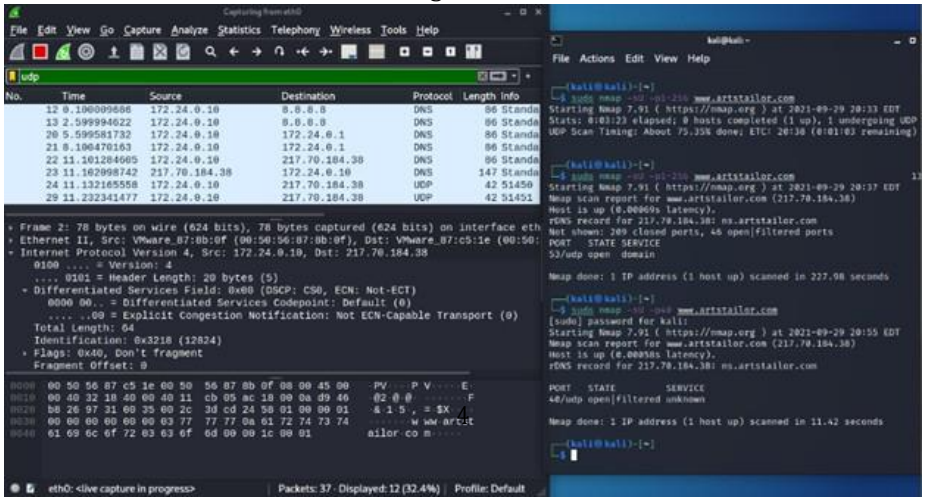

Figure 6: