Ex0b0

Gary Jones

Contents

Executive Summary

Goals

The goal of this exercise is to learn about pivots and connecting to an otherwise inaccessible web server.

Summary of Findings

The development box is accessible and can be accessed through port 80.

Technical Report

Vulnerability Description

By connecting to the system and using chisel proxychain I was able to find open ports for devbox.artstailor.com and access the site.

Confirmation method

This was confirmed by utilizing the kali web browser to access the site on port 80.

Attack Narrative

I first ran tail proxychains4.conf and ip a to identify the default port of socks5 and the ip address for kali (figures 1 and 2). After this I connected to the client with the administrator credentials provided, turned off the real time virus protection and mounted the /temp folder so that I could share files between the systems. I then ran chisel as the server from the kali end (see figure 3) and then ran ./chisel.x64.exe using the information I identified through proxychains4.conf and ip a in figures 1 and 2 (see figure 4).

Once the two systems were connected and I was able to share information through the firewall without issue I then performed an nmap scan of devbox.artstailor.com through proxychains and found that ports 22 and 80 were open. In addition I found that these ports indicate that the devbox.artstailor.com system is run on linux (see figures 5 and 6).

Following this the two ports were again inspected closer and it was found that there is a development version running on those ports (see figures 7 and 8). To confirm this both ports were inspected and the chisel connection was forwarded to devbox.artstailor.com. However, only port 80 loaded a functional page (see figures 9 and 10).

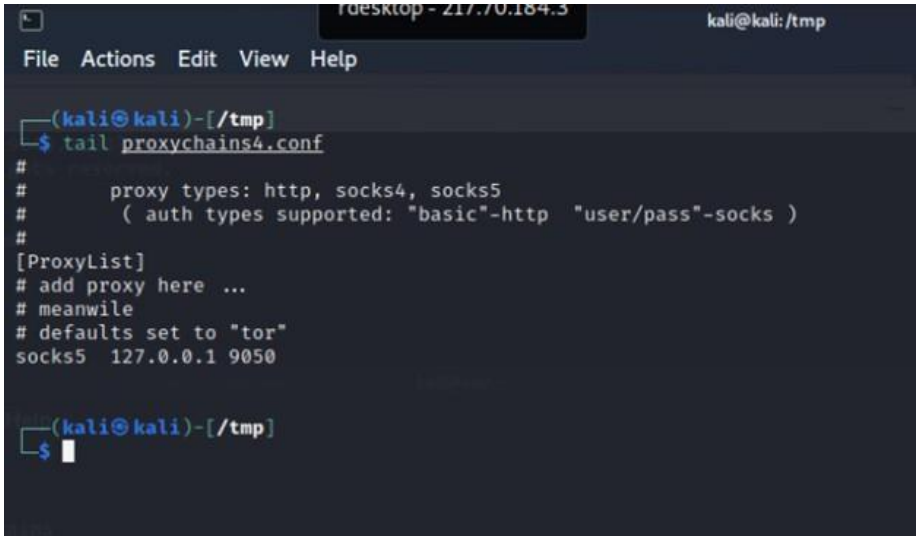

Figure 1:

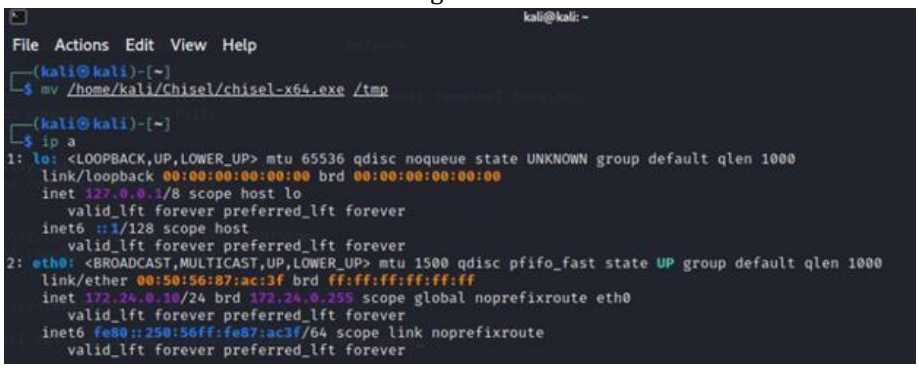

Figure 2:

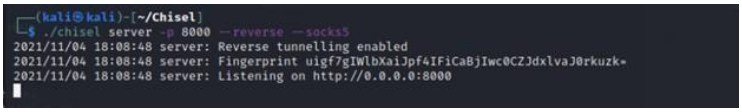

Figure 3:

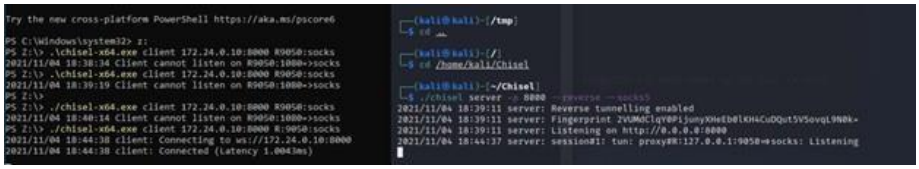

Figure 4:

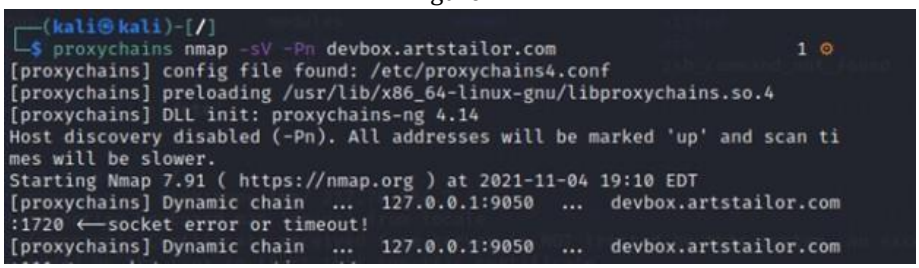

Figure 5:

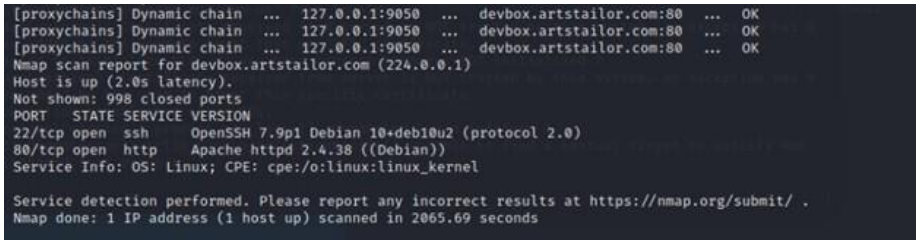

Figure 6:

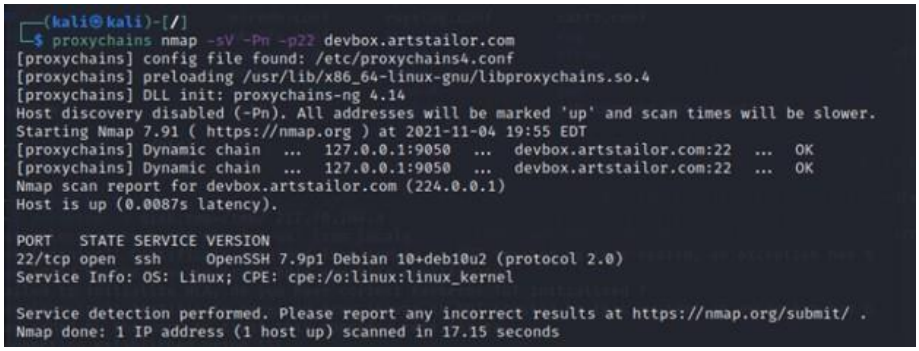

Figure 7:

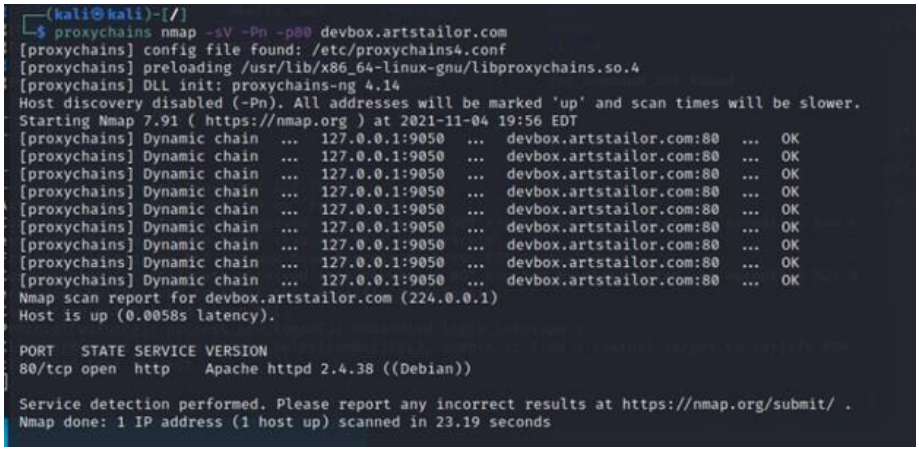

Figure 8:

Figure 9:

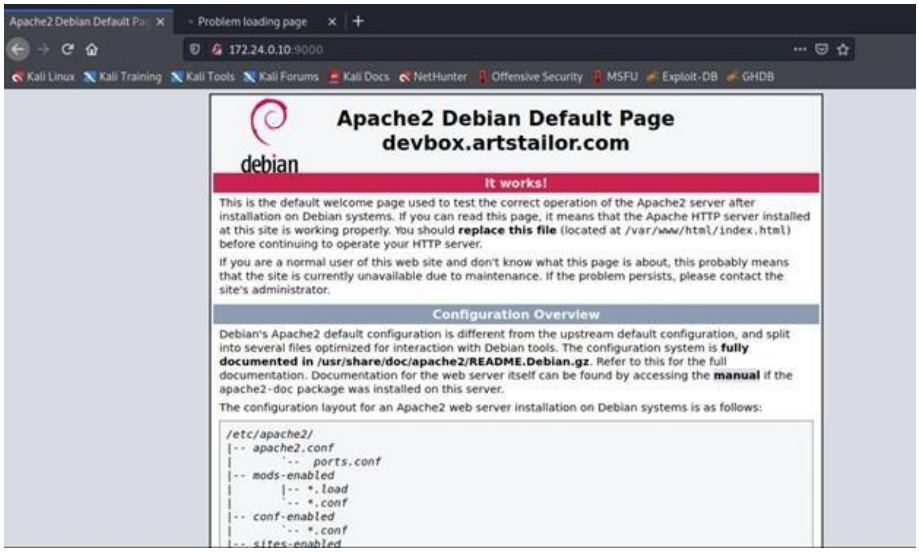
Apache2 Debian Default Pa
Problem loading page
172.24.0.10:9000
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Apache2 Debian Default Page
devbox.artstailor.com
debian
It works!
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.
The configuration layout for an Apache2 web server installation on Debian systems is as follows:
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled

Figure 10: