

Ex0b0

Gary Jones

Contents

Executive Summary	2
Goals	2
Summary of Findings	2
Technical Report	2
Vulnerability Description	2
Confirmation method	2
Attack Narrative	2

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).

```
File Actions Edit View Help
(kali@kali)-[~/tmp]
└─$ tail proxychains4.conf
#
#       proxy types: http, socks4, socks5
#       ( auth types supported: "basic"-http "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks5 127.0.0.1 9050
(kali@kali)-[~/tmp]
└─$
```

Figure 1:

```
File Actions Edit View Help
(kali@kali)-[~/Chisel]
└─$ mv /home/kali/Chisel/chisel-x64.exe /tmp
(kali@kali)-[~/Chisel]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
   link/ether 00:50:56:87:ac:3f brd ff:ff:ff:ff:ff:ff
   inet 172.24.0.30/24 brd 172.24.0.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::250:56ff:fe87:ac3f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Figure 2:

```
(kali@kali)-[~/Chisel]
└─$ ./chisel server -p 8000 --reverse --socks5
2021/11/04 18:08:48 server: Reverse tunnelling enabled
2021/11/04 18:08:48 server: Fingerprint uigf7g1WbKalJpf41FiCaBjIwc0C2JdxlvaJ0rkuzk-
2021/11/04 18:08:48 server: Listening on http://0.0.0.0:8000
```

Figure 3:

```

Try the new cross-platform PowerShell https://aka.ms/powershell
PS C:\Windows\system32> .\chisel-x64.exe client 172.24.0.10:8000 R9050:socks
2021/11/04 18:38:34 client: cannot listen on R9050:1000->socks
PS Z:\> .\chisel-x64.exe client 172.24.0.10:8000 R9050:socks
2021/11/04 18:39:19 client: cannot listen on R9050:1000->socks
PS Z:\> .\chisel-x64.exe client 172.24.0.10:8000 R9050:socks
2021/11/04 18:40:14 client: cannot listen on R9050:1000->socks
PS Z:\> .\chisel-x64.exe client 172.24.0.10:8000 R:9050:socks
2021/11/04 18:44:38 client: Connecting to ws://172.24.0.10:8000
2021/11/04 18:44:38 client: Connected (Latency 1.0043ms)

(kali@kali)-[~/tmp]
└─$ cd ..
(kali@kali)-[~/]
└─$ cd /home/kali/Chisel
(kali@kali)-[~/Chisel]
└─$ ./chisel server -s 8000 -R9050 --socks
2021/11/04 18:39:11 server: Reverse tunnelling enabled
2021/11/04 18:39:11 server: Fingerprint 740MDC1q8P1umYX0E04LKHxCuQ0ut5V5ovqU9Wk-
2021/11/04 18:39:11 server: Listening on http://0.0.0.0:8000
2021/11/04 18:44:37 server: session#1: tun: proxyR:127.0.0.1:9050->socks: Listening

```

Figure 4:

```

(kali@kali)-[~/]
└─$ proxychains nmap -sV -Pn devbox.artstailor.com 1
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-04 19:10 EDT
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... devbox.artstailor.com
:1720 ← socket error or timeout!
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... devbox.artstailor.com

```

Figure 5:

```

[proxychains] Dynamic chain ... 127.0.0.1:9050 ... devbox.artstailor.com:80 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... devbox.artstailor.com:80 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... devbox.artstailor.com:80 ... OK
Nmap scan report for devbox.artstailor.com (224.0.0.1)
Host is up (2.0s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp   open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp   open  http     Apache httpd 2.4.38 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2065.69 seconds

```

Figure 6:

```

(kali@kali)-[~/]
└─$ proxychains nmap -sV -Pn -p22 devbox.artstailor.com
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-04 19:55 EDT
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... devbox.artstailor.com:22 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... devbox.artstailor.com:22 ... OK
Nmap scan report for devbox.artstailor.com (224.0.0.1)
Host is up (0.0087s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.15 seconds

```

Figure 7:

```

(kali@kali)-[~/]
└─$ proxychains nmap -sV -Pn -p80 devbox.artstailor.com
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-04 19:56 EDT
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... devbox.artstailor.com:80 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... devbox.artstailor.com:80 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... devbox.artstailor.com:80 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... devbox.artstailor.com:80 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... devbox.artstailor.com:80 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... devbox.artstailor.com:80 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... devbox.artstailor.com:80 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... devbox.artstailor.com:80 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:9050 ... devbox.artstailor.com:80 ... OK
Nmap scan report for devbox.artstailor.com (224.0.0.1)
Host is up (0.0058s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.38 ((Debian))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.19 seconds

```

Figure 8:

```

PS Z:\> ./chisel-x64.exe client 172.24.0.10:8000 R:9050:devbox.artstailor.com:80
2021/11/05 00:02:38 client: Connecting to ws://172.24.0.10:8000
2021/11/05 00:02:38 client: Connected (Latency 1.0359ms)

```

Figure 9:

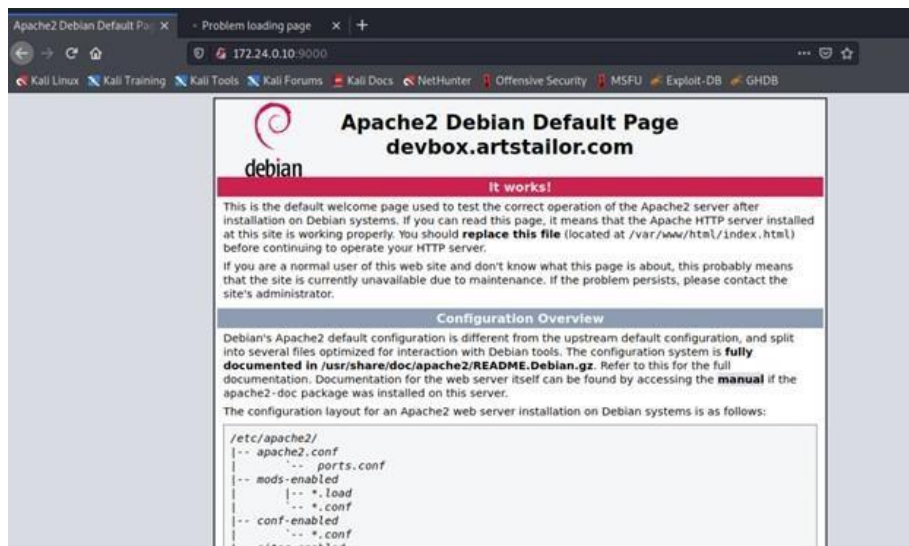


Figure 10: