Ex0b0 Report

Benjamin Ruddy

2022-11-05

Contents

Attack Narrative

Chisel configuration, Proxychains

The exercise takes place in a network configuration in which kali.pr0b3.com cannot access devbox.artstailor.com directly, and instead has to *pivot* to it from costumes.artstailor.com.

Noting that the default proxychains port is set to 1080 in `/etc/proxychains4.conf`, we run the chisel with the following commands on the Kali machine and on costumes.artstailor.com, respectively (Kali is the Chisel server, costumes machine is the Chisel client):

```
┌──(kali㉿kali)-[~/Chisel]
└─$ ./chisel server -p 8000 --reverse --socks5
2022/11/04 22:18:47 server: Reverse tunnelling enabled
2022/11/04 22:18:47 server: Fingerprint Ny3SbugyygFcTKCdx+7QyuwSf8WgpCzV6GNjM
eqnJe4=
2022/11/04 22:18:47 server: Listening on http://0.0.0.0:8000
2022/11/04 22:18:47 server: session#1: tun: proxy#R:127.0.0.1:1080⇒socks: Li
```

```
C:\Users\pr0b3\Desktop\Chisel>chisel-x64.exe client 172.24.0.11:8000 R:1080:socks
2022/11/05 02:20:00 client: Connecting to ws://172.24.0.11:8000
2022/11/05 02:20:00 client: Connected (Latency 0s)
```

Nmap Scan, Operating System

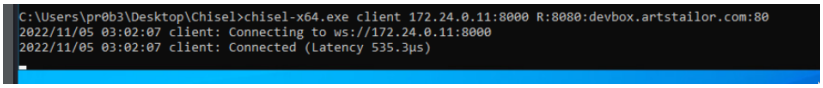
Having established a Chisel tunnel, we can route an nmap scan through the proxychains port we're forwarding to costumes.artstailor.com to find out the OS and web server that is running on the machine:

```
└─$ proxychains -f /etc/proxychains4.conf nmap -Pn -p 80,443,445,135,139,445,
3389 -sV 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 4.16
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-04 22:26 EDT
WARNING: Duplicate port number(s) specified.  Are you alert enough to be usin
g Nmap?  Have some coffee or Jolt(tm).
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  devbox.artstailor.com:139 ←—socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  devbox.artstailor.com:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  devbox.artstailor.com:443 ←—socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  devbox.artstailor.com:3389 ←—socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  devbox.artstailor.com:445 ←—socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  devbox.artstailor.com:135 ←—socket error or timeout!
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  devbox.artstailor.com:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  devbox.artstailor.com:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  devbox.artstailor.com:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  devbox.artstailor.com:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  devbox.artstailor.com:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  devbox.artstailor.com:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  devbox.artstailor.com:80  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  devbox.artstailor.com:80  ...  OK
Nmap scan report for devbox.artstailor.com (224.0.0.1)
Host is up (1.9s latency).

PORT     STATE  SERVICE       VERSION
80/tcp   open   http          Apache httpd 2.4.54 ((Debian))
135/tcp  closed msrpc
139/tcp  closed netbios-ssn
443/tcp  closed https
445/tcp  closed microsoft-ds
3389/tcp closed ms-wbt-server

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.92 seconds
zsh: segmentation fault  proxychains -f /etc/proxychains4.conf nmap -Pn -p 80,443,445,135,139,445,3389
```

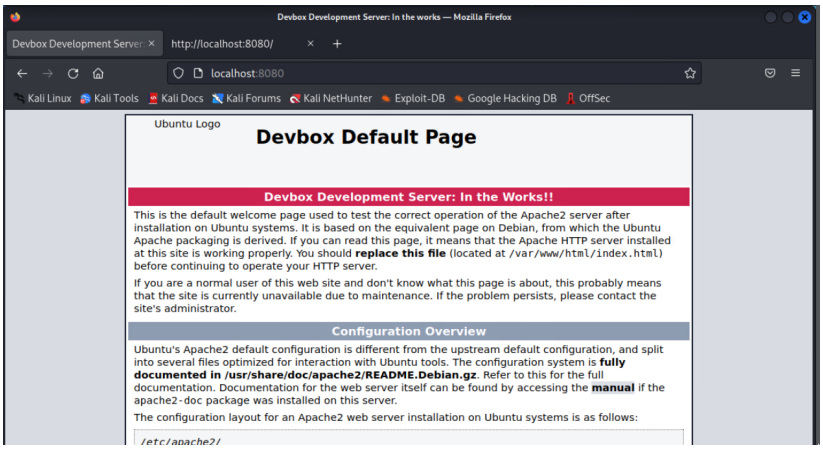
From this scan, we can see that the Apache server being is a version for Debian – this means that the devbox.artstailor.com host is running Linux.

HTTP Port forwarding

Having confirmed both our ability to tunnel through Chisel, as well as the existence of a web server on the devbox machine, we proceed to forward said web server to the localhost on Kali as follows (through the Chisel client on costumes.artstailor.com):

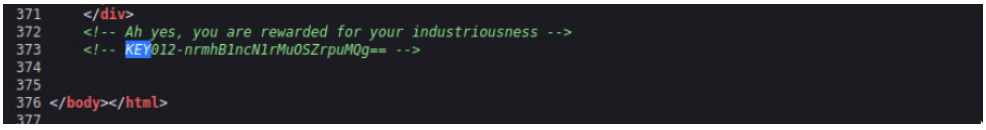


With the above command, we have forwarded all requests to localhost port 8080 on kali.pr0b3.com to the intermediary Chisel client on the costumes machine, and finally to port 80 on the devbox machine. As we can see in the following screenshot, the default Apache landing page is displayed along with a message notifying us that the Devbox Development Server is "in the works":



Key 012

Within the source code of the page (Right Click ¿ View Page Source) was a hidden key:



MITRE ATT&CK Framework TTPs

TA0011: Command and Control
- **T1090:** Proxy
  - **.001:** Internal Proxy