Post-Exploitation - Pivoting as an Attack Weapon

Filipi Pires[1]

[1] Researcher and Cyber Security Specialist

E-mail: filipi86@hotmail.com

Abstract

When conducting a web application penetration test there are times when you want to be able to pivot through a system to which you have gained access, to other systems in order to continue testing. There are many channels that can be used as avenues for pivoting. This paper examines the most common used channels for pivoting like: SSH local port forwarding and during one of my activities, I talked to a friend who presented me with an excellent tool for executing the pivoting technique, this tool is known as Chisel. This technique can be used in many different activities in Penetration Testing or in many CTFs - Capture the Flags within the context of using them with key tools in the penetration tester's arsenal including: Nmap, netcat, etc.. Each tool that you use to progressing in your test environment, can guarantee many benefits, but the important thing that we'll talk during this paper, such as ease of implementation, performance of execution, among others and so the more knowledge of how the packaging of the protocol works and how this communication is done, the better the application of the tool will be..

Keywords: Pivoting, Post Exploitation, Pentesting, Red Team.

---

1 Introduction

When conducting a web application penetration test there are times when you want to be able to pivot through a system to which you have gained access, to other systems in order to continue testing.

Usually during a penetration test or security assessment, depending, of course, of the strategy used during this work that could be started with an external network often with research and pentesting of machines and services available from the global network, this phase of the discovery is called Reconnaissance, many times we can see, that attempts are being made to find a security hole and, if it succeeds, then a penetration into the local network is performed in order to capture as many systems as possible.

Local network traffic is non-routable, that is, other computers that are physically connected to this network can access the resources of the local network, and the attacker cannot access them.

So, Pivoting is a set of techniques that allow an attacker to gain access to local resources, in essence, making traffic routable that is normally non-routable, during a Penetration Test, this phase called Post Exploitation.

Pivoting helps an attacker to configure the working environment to use the tools in such a way as if he were in the organization's local network, that is, using pivoting is achieved, you can get access to local resources and the ability to use tools to scan and search for vulnerabilities from your computer in a remote local network, as if they were installed right there, so, hacker tools gain access to the local network, which under normal conditions is impossible for non-routable traffic.

2 Pivoting Techniques

Pivoting is the use of a first compromised system in conjunction with routing techniques at the protocol or application level to allow and even help compromise other systems present on the same network.

In other words, we can say that it is the technique that opens the way for an attacker to move laterally "inside a corporation," jumping "to other machines seeking to gain access to other systems through an already penetrated system. This facility usually happens at the network layer, by redirecting ports or packets, allowing to bypass firewalls and penetrate systems that would otherwise be inaccessible.

During a Penetration Testing when we get to compromise a first target, it was excited with the first step, because can open a "world" of options, this phase is known as Post Exploitation.

Post exploitation basically means the phases of operation once a victim's or target's system has been compromised by the attacker/pentester. The value of the compromised system is determined by the value of the actual data stored in it and how an attacker may make use of it for malicious purposes. The concept of post exploitation has risen from this fact only as to how you can use the victim's compromised system's information.

This phase actually deals with collecting sensitive information, documenting it, and having an idea of the configuration settings, network interfaces, and other communication channels. These may be used to maintain persistent access to the system as per the attacker's needs.

In this phase that we can use the Pivoting Techniques, today you can find many different tools to use to perform a pivoting, the most common is SSH Port Forwarding, or SSH Port Forwarding with proxy chains, when you can use the SSH with dynamic port forwarding to create a socks proxy, with proxychains to help with tools that can't use socks proxies. You can leverage this tunnel two way.

Another technique is using Metasploit, the most popular penetration testing framework, offers four main ways of pivoting: Portfwd, Route, AutoRoute and Packet Pivoting.

During one of my activities, I talked to a friend who presented me with an excellent tool for executing the pivoting technique, this tool is known as **Chisel**[1].

This technique can be used in many different activities in Pentesting or in many Capture the Flags environment, like Hack The Box Machine's - *Hack The Box is an online platform allowing you to test your penetration testing skills and exchange ideas and methodologies with thousands of people in the security field. Click below to hack our invite challenge, then get started on one of our many live machines or challenges*.

In this paper I'll show those steps in my own environment as well.

3 Environment

In this first step we will create an environment to be compromised. Some concepts are extremely important to be understood, mainly the concepts of Networks, Routing and how it all works.

Let's imagine the following scenario:

An attacker has an IP (192.168.1.128) – I'll use the Kali Linux Machine.

The attacker compromises a **Linux Machine** with IP 192.168.1.131 and 10.128.0.5

So, the attacker checks the 10.128.0.x network and finds an active IP 172.15.128.0 (Linux) and then moves on and tries to compromise it as well.

Now, what should be noted is that IP 172.15.128.0 (**Windows**) is not directly accessible to the attacker, but it can still be compromised by the "Pivoting" technique.

Let set up this environment to practice this technique:

Requirements:

- Attacker Machine (Kali or ParrotOS)
- Linux (Metasploitable)
- Windows 10 64bits

Lab enviroment

Attacker

eth0 | 192.168.1.128 – As you can see, this IP is belong from **C Class of IPs;**

```
root@hacking:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.128  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fe35:854c  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:35:85:4c  txqueuelen 1000  (Ethernet)
        RX packets 7044  bytes 1444630 (1.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5974  bytes 421721 (411.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 609  bytes 64196 (62.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 609  bytes 64196 (62.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 1: Attacker Machine
created by owner (2020)

Victim

eth0 | 192.168.1.131 – The same Class from the Attacker

eth1 | 10.128.0.5 – Here we can see another kind of class of IPs, know like **A Class of IPs**;

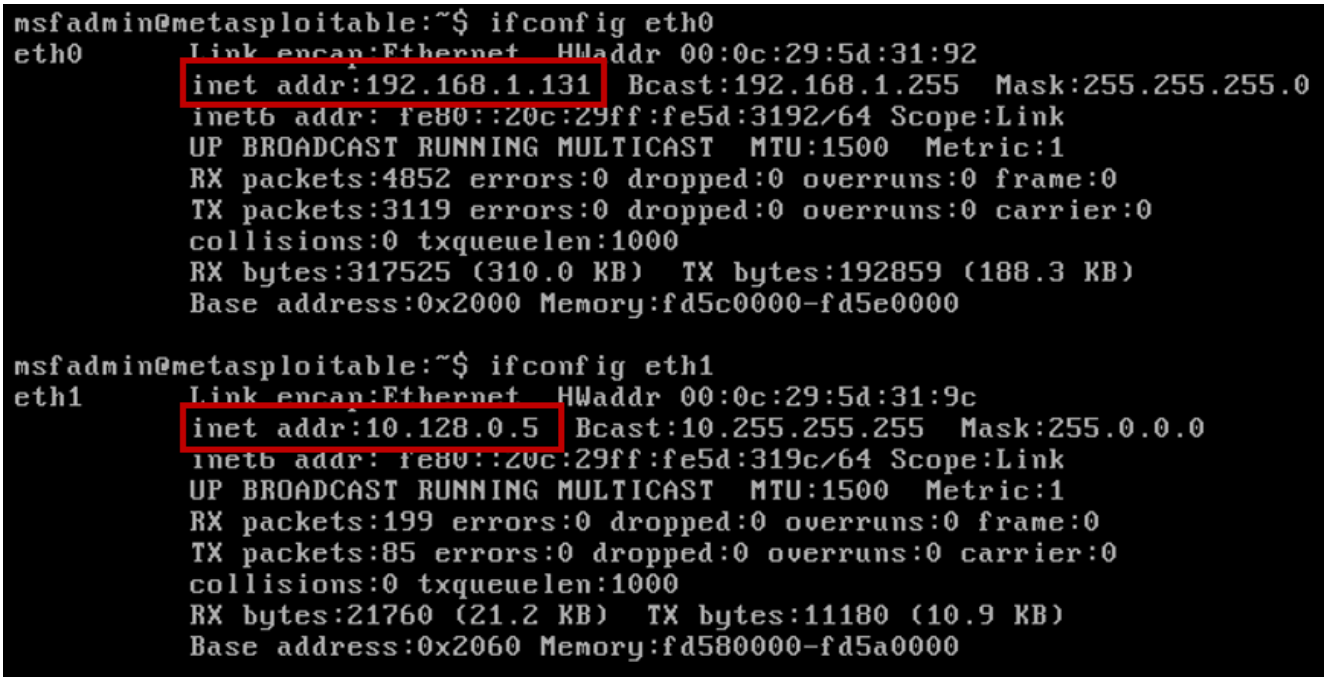

Figure 2: Victim Machine
created by owner (2020)

Windows Machine

eth1 | 10.128.0.6 - The same Class from the Victim;

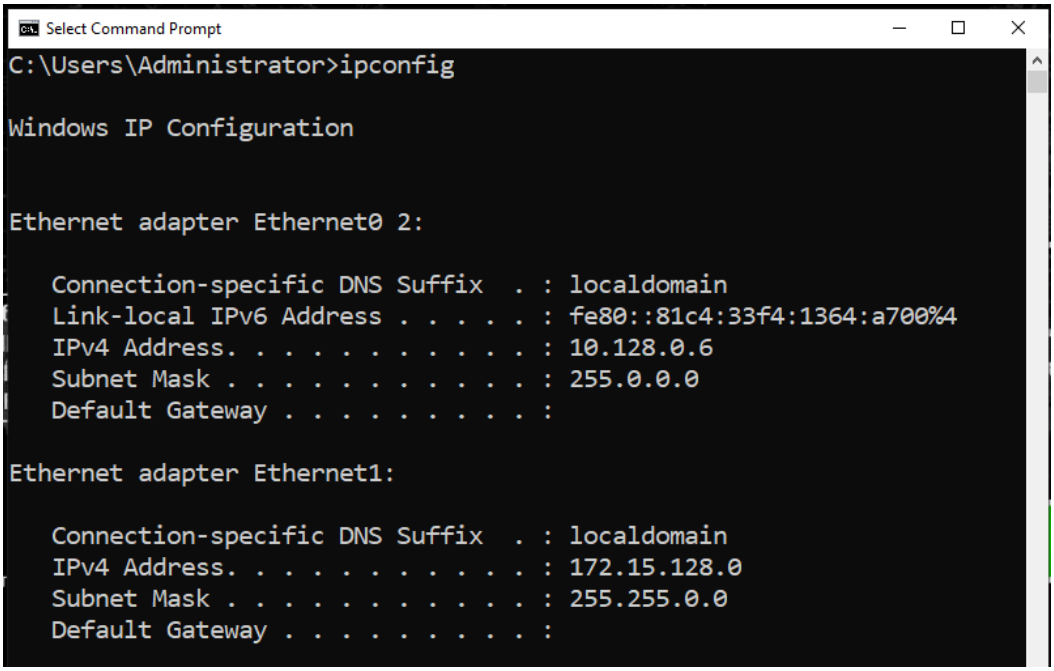

Figure 3: Vulnerable Machine
created by owner (2020)

In this case, supposing that we are performing a Penetration Testing, usually we should starting by **Reconnaissance**, after to use **nmap tool** with this command (*nmap -A -T5 192.168.1.19*), of course, that I'm using the aggressive mode command, because I'm using in my own environment, we can see that we have web application in port 80, using Apache 2.2.8

```
root@hacking:~/WebApp# nmap -A -T5 192.168.1.131
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-12 13:46 CEST
Nmap scan report for 192.168.1.131
Host is up (0.00057s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.128
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
```

Figure 4: NMAP Tool – Recon phase
created by owner (2020)

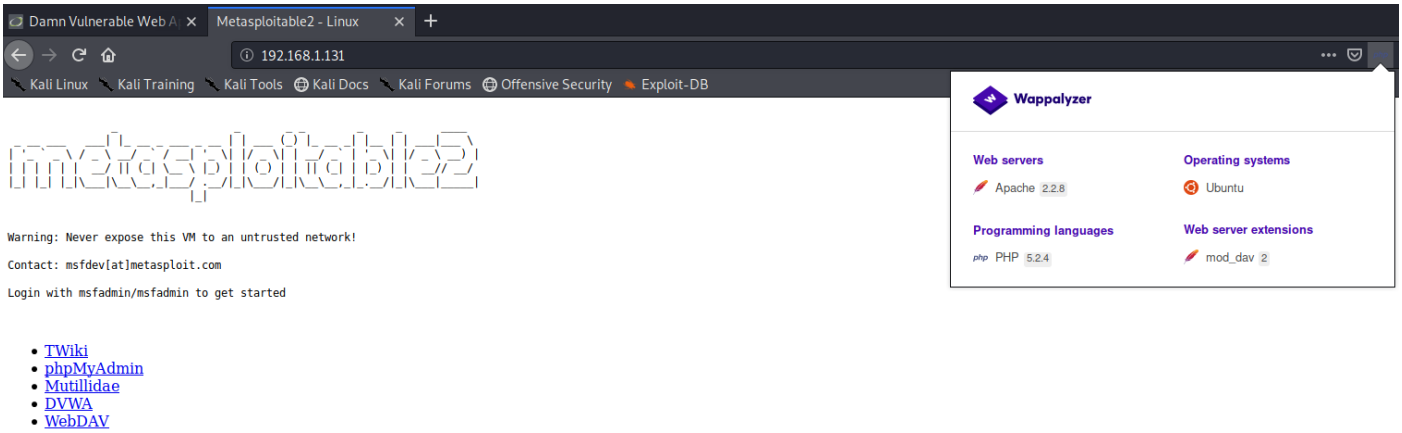

Figure 5: Access Web Application – Recon phase
created by owner (2020)

After that this, we can explore various options that you know you can look the website and try to explore with many ways, as our idea in this paper is to explore the Pivoting technique, I will first list the Directories and Sub-Directories so that we get access and as soon as we gain access to the machine victim we can start the **Pivoting** technique.

```
#wfuzz -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt --hc=404 http://192.168.1.131/FUZZ
```

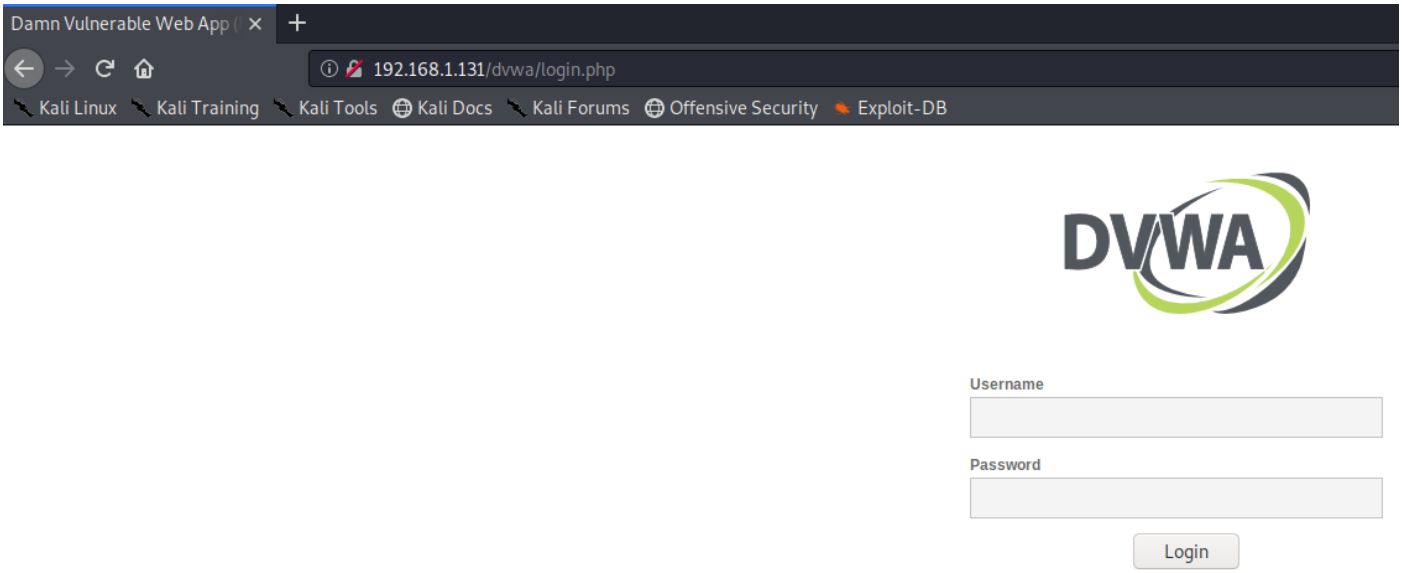

Figure 6: Access Web Application – Recon phase
created by owner (2020)

Many people who are doing Pentest Web practices can use DVWA as a vulnerable platform for exploitation, **Damn Vulnerable Web App (DVWA)** is a PHP / MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers / students to teach / learn web application security in a class room environment[2].

So, here we found a very known vulnerability called File Upload, that we'll use to explore and to get access in the victim environment.

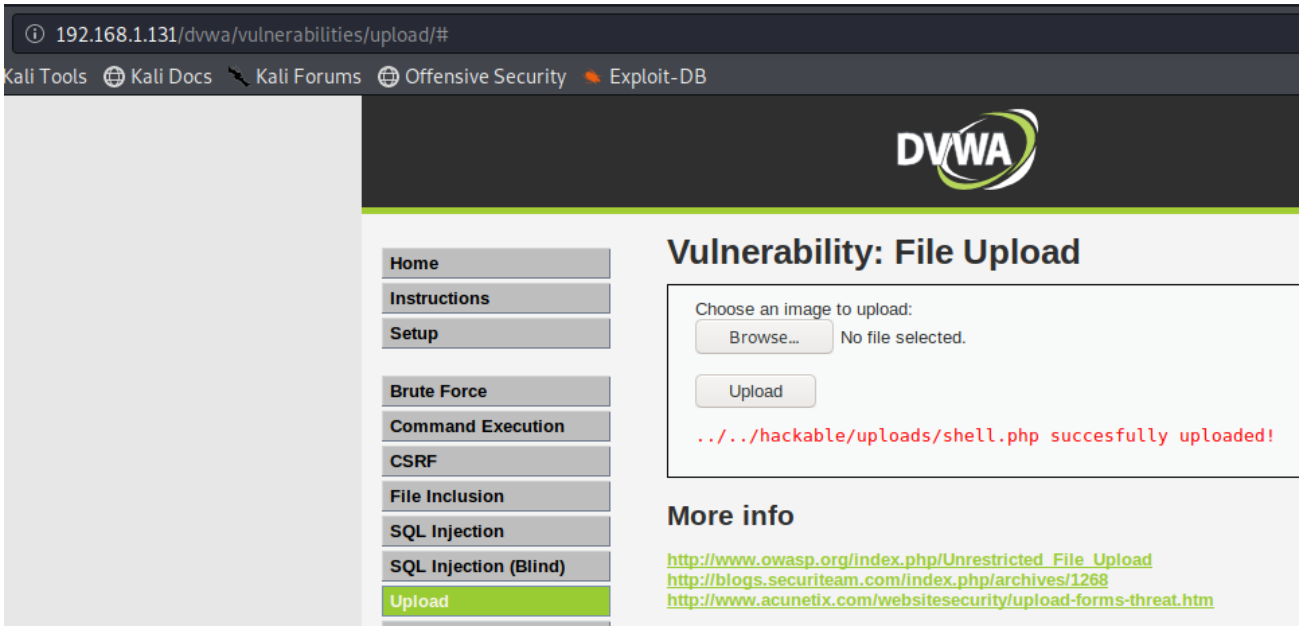

Figure 7: FileUpload – Exploitation
created by owner (2020)

After we got to upload a "reverse shell" in a .php file, we were able to access the victim's machine as we can see.

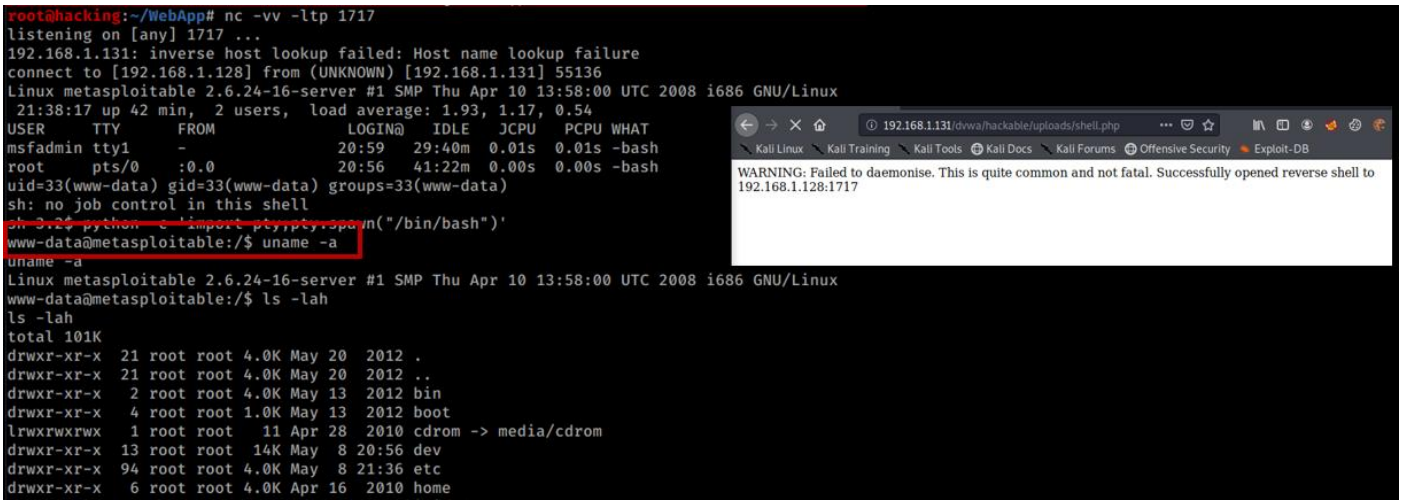

Figure 7: Reverse Shell – Exploitation
created by owner (2020)

Looking at the IP settings of the victim machine, we notice that it has a network card being connected to a different network than the initial network that the attacker is exploiting, and that until then, it was the only network available for exploitation.

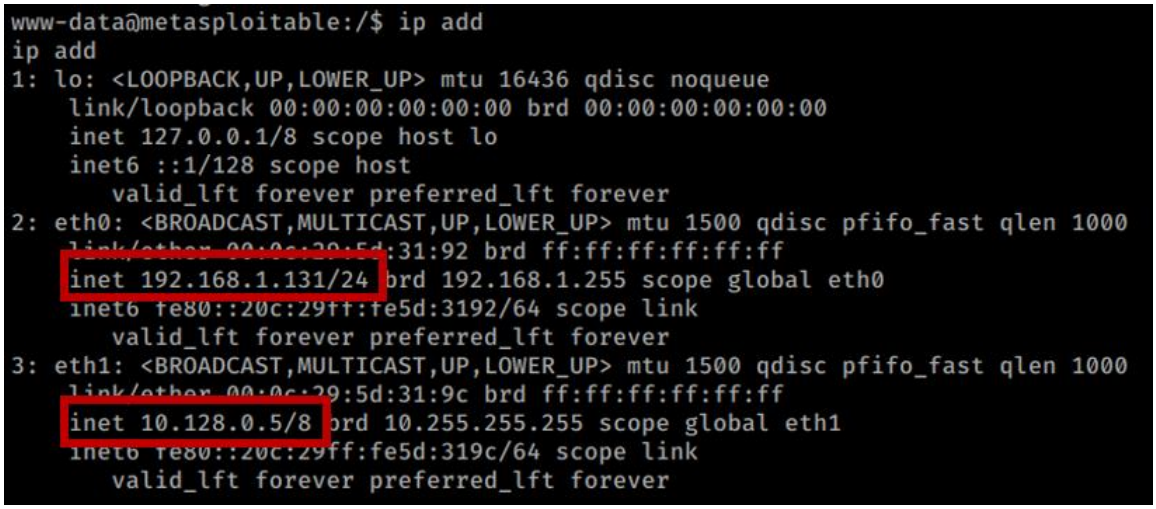

Figure 7: Reverse Shell – Exploitation
created by owner (2020)

Through the victim's machine, it is possible to execute various commands to map and find vulnerabilities even though they are on different networks.

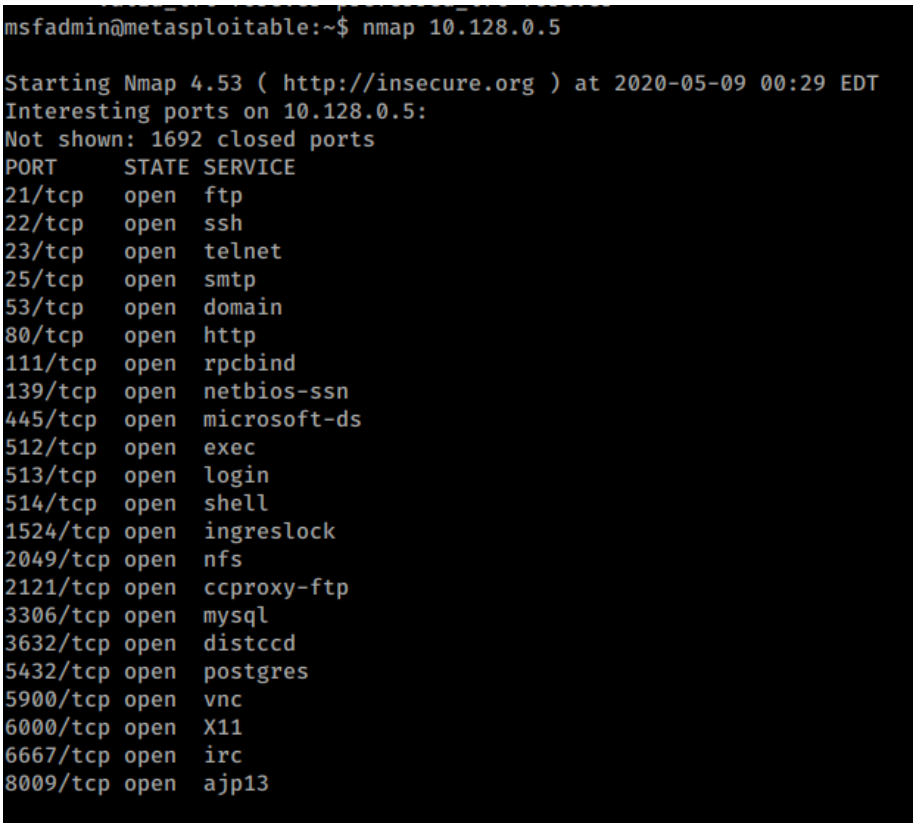

Figure 7: Reverse Shell – Exploitation
created by owner (2020)

After finding another machine within the new network segment, we can try to exploit this new machine and thus try to access it, even if it is on a network "not accessible" by the attacker.

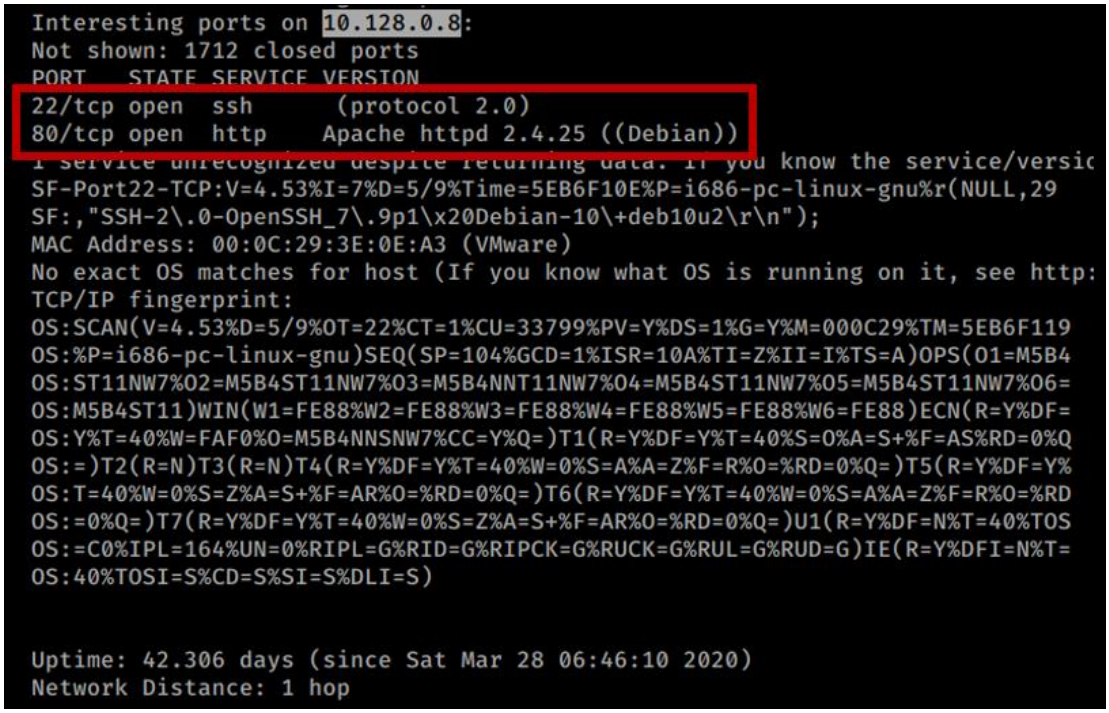

Figure 7: NMAP Exploitation
created by owner (2020)

4 Pivoting Technique

Pivoting is the use of a first compromised system in conjunction with routing techniques at the protocol or application level to allow and even assist in compromising other systems present on the same or different networks.

In other words, it is the post-exploitation technique that allows the attacker to “move laterally” within a network, bypassing the firewall and seeking to gain access to other systems through an already penetrated system.

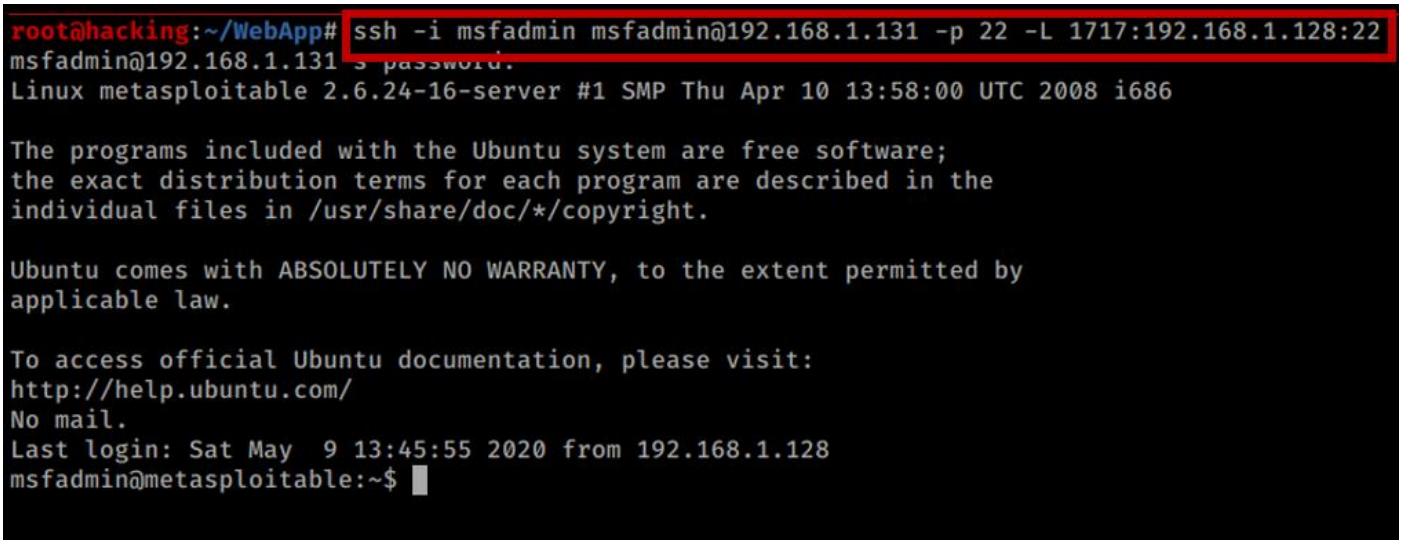

Figure 7: NMAP Exploitation
created by owner (2020)

After verifying that the second machine is on a different network can be accessed using an ssh key, we can try to perform the pivot directly from the attacker machine.

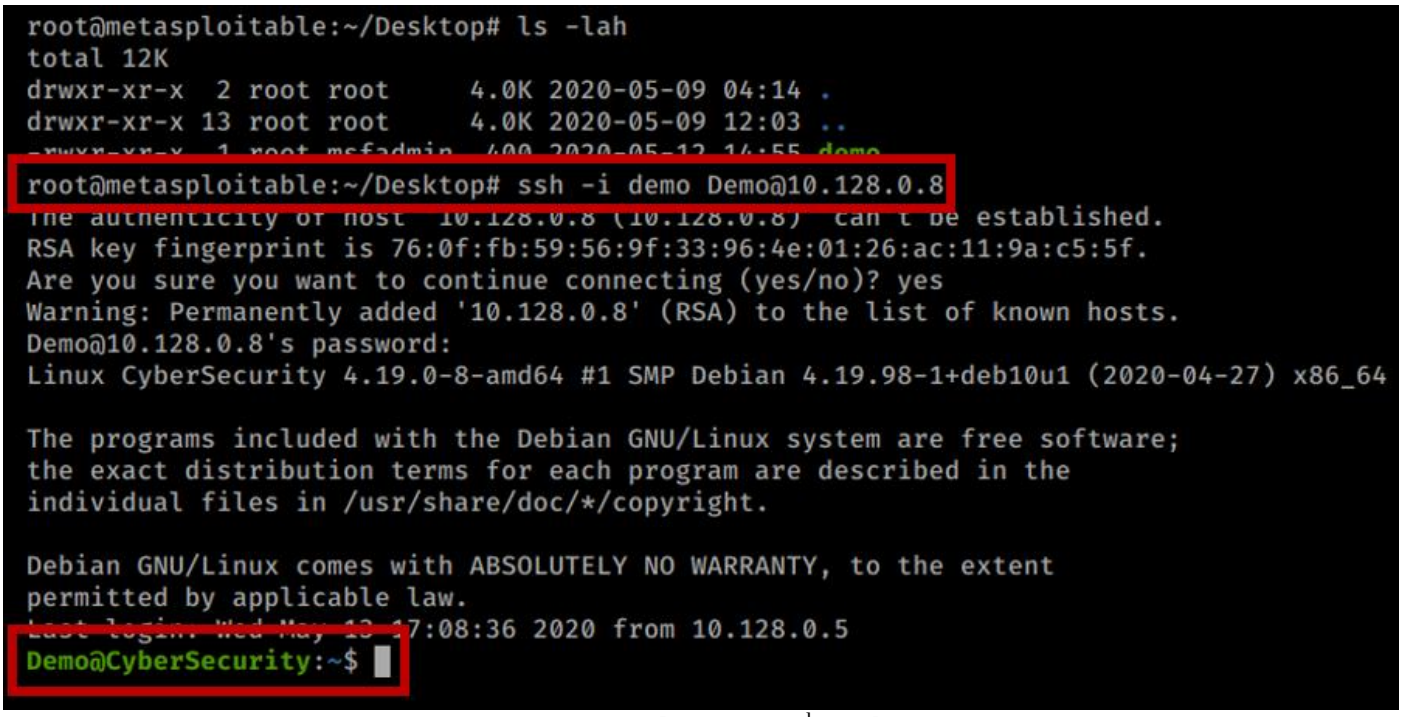

Figure 8: Exploitation 2nd machine
created by owner (2020)

In this example, I'm using the technique known as SSH Port Forwarding, as we can see, It listens on a local port established when the connection is set up. Anything sent to the local port is forwarded through the SSH tunnel. At the SSH server, the application protocol of the message being sent through the tunnel is used to determine where to send the traffic.

We start to listen the port 1717 to use as an SSH tunnel to get access another machine in another network (Class A).

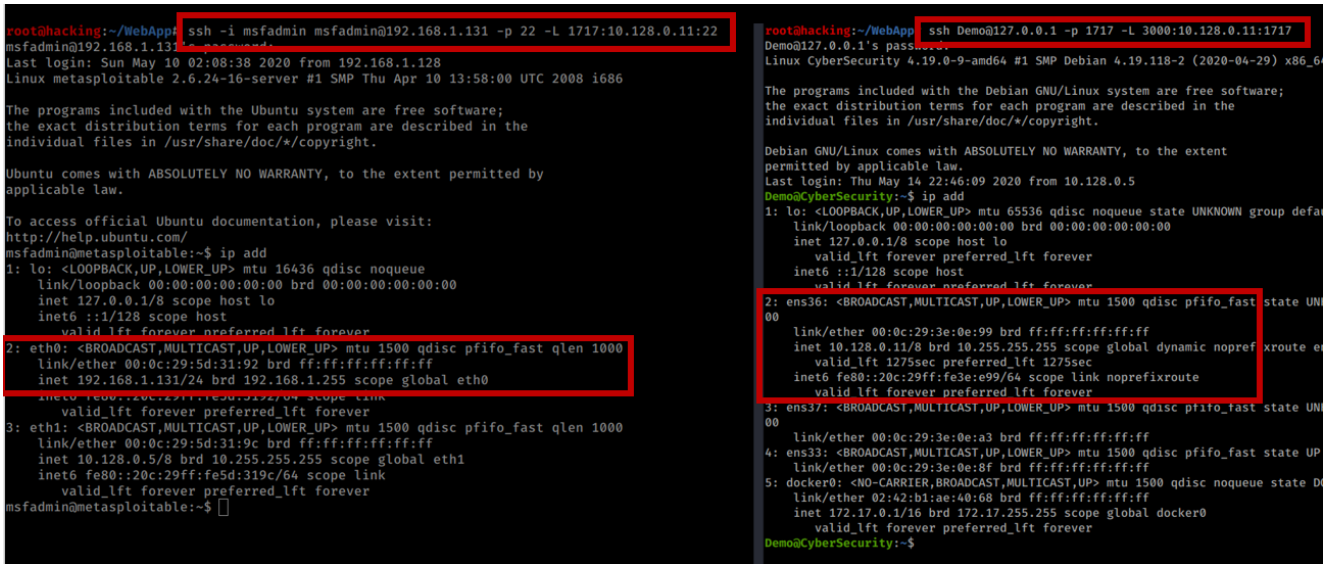

Figure 9: SSH Port Forwarding
created by owner (2020)

5 Chisel

Chisel is a fast TCP tunnel, transported over HTTP, secured via SSH. Single executable including both client and server. Written in Go (golang). Chisel is mainly useful for passing through firewalls, though it can also be used to provide a secure endpoint into your network. Chisel is very similar to crowbar though achieves much higher performance[3].

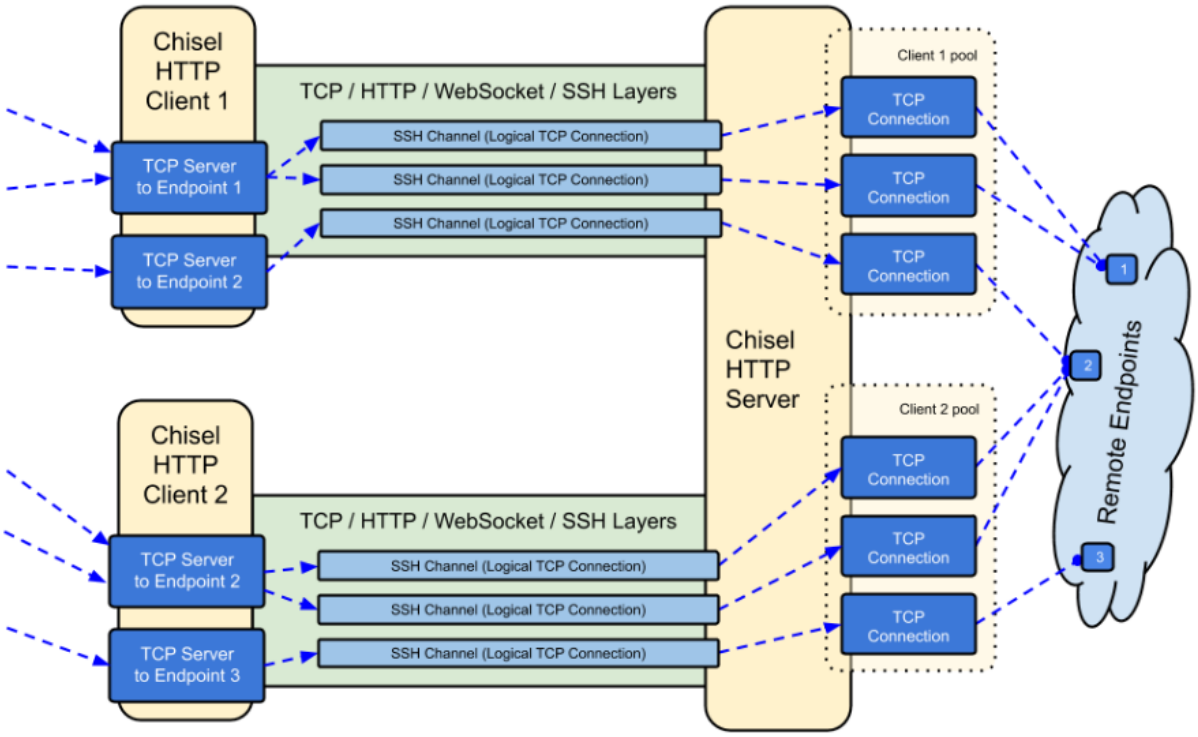

Figure 10: Chisel
https://github.com/jpillora/chisel(2020)

Below some features, where we can notice how Chisel is good and easy to use…

- Easy to use
- Performant
- Encrypted connections using the SSH protocol (via crypto/ssh)
- Authenticated connections; authenticated client connections with an users config file, authenticated server connections with fingerprint matching.
- Client auto-reconnects with exponential backoff
- Client can create multiple tunnel endpoints over one TCP connection
- Client can optionally pass through HTTP CONNECT proxies
- Server optionally doubles as a reverse proxy
- Server optionally allows SOCKS5 connections (See guide below)
- Reverse port forwarding (Connections go through the server and out the client)

6 Chisel Technique

We can run a server on any Pentesting platform like kali or parrot os machine, and then connect to it from target machines. On making that connection, you can define different kinds of tunnels you want to set up.

One of those possibilities is to set up the server on myself local.

Actually, chisel is a binary that built acts as both the client and the server, and many systems operations like Unix and Windows.

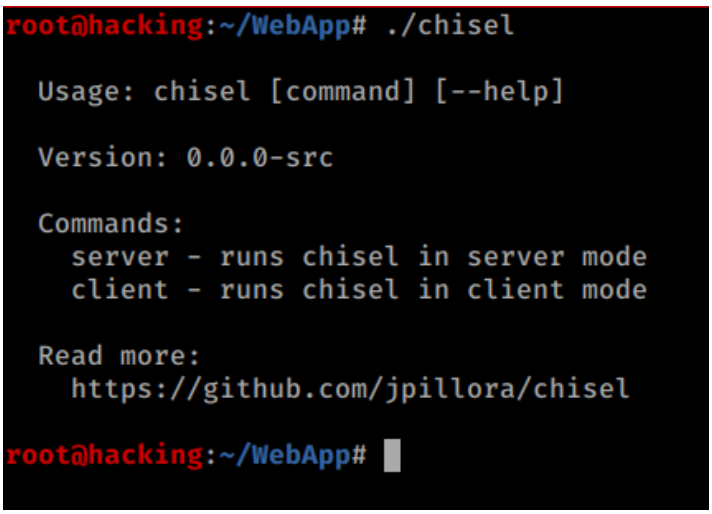

Figure 11: Chisel types
https://github.com/jpillora/chisel(2020)

So, to start the server, is simple process to execute, we run that command below, that will allow you to specify what port chisel listens on.

```
#./chisel server -p [port] --reverse. -p
```

If you don't provide this (listen port), it'll try 8080 by default, which often can fail, because many researchers almost always have an application running on 8080, like Burp or OWASP Zap. The "**--reverse**" tells the server that you want clients connecting in to be allowed to define reverse tunnels, that is, the clients connecting in can open listening ports on your local machine.

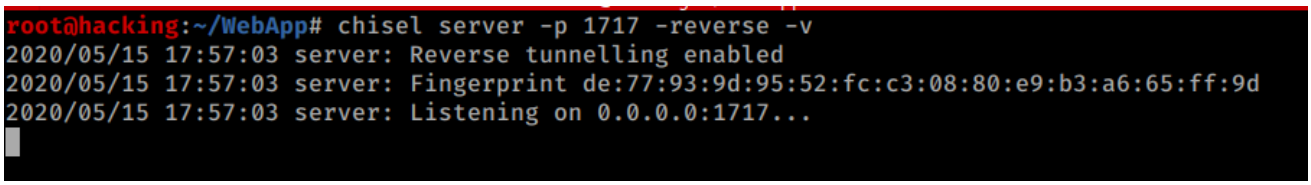

Figure 12: Chisel Server
https://github.com/jpillora/chisel(2020)

On the other hand, you have the client who is responsible for accessing the port being listened to by the server.

```
#./chisel client Attacker:[port] [port]:Victim:[Listen port]

Or localhost - Of course depending of the application

#./chisel client Attacker:[port] [port]:127.0.01:[Listen port]
```

You need to download Chisel for your victim machine and you'll be able to make the connection Victim x Attacker through the channel you opened earlier.

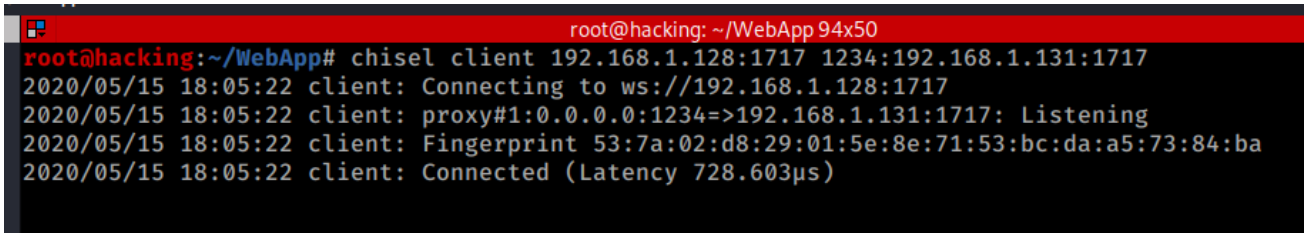

Figure 12: Chisel Server
https://github.com/jpillora/chisel(2020)

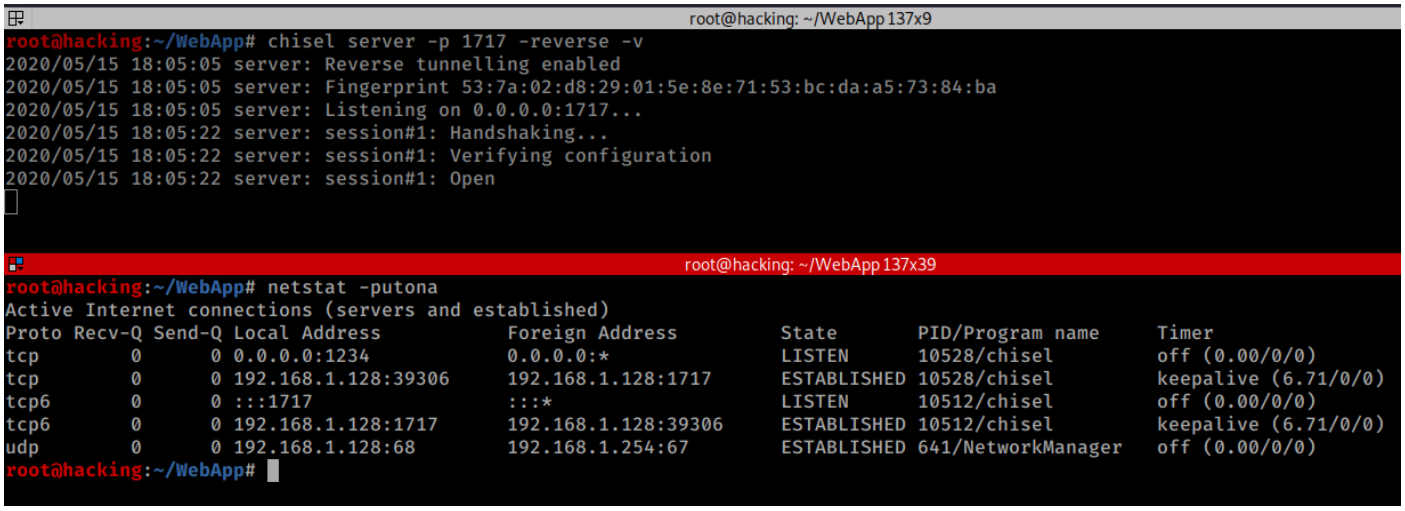

Figure 12: Chisel Server
https://github.com/jpillora/chisel(2020)

7 Conclusion

In this paper we went through all the steps to understand how works the Pivoting Techniques.

Pivoting is an important technique in the pen testers can use. It allows them to bridge networks through an intermediate system. By doing so, the pen tester can gain access to systems he would otherwise be unable to reach. As we mention in this simple paper, we see a few techniques that can be used to gain access and there are many tools that can be used to pivot.

Each tool that you use to progressing in your test environment, can guarantee many benefits as we talked about during this paper, such as ease of implementation, performance of execution, among others.

Some points that are important to evaluate when using tools for Pivot, what kind of blocks you are receiving and that you may face during the performance of your penetration testing.

Many times, when we get access to a vulnerable machine, many times our "shell" is totally limited, so the more knowledge of how the packaging of the protocol works and how this communication is done, the better the application of the tool will be.

Which should be pivoting technique is best?

There is no one correct answer. The answer depends of course, on what the pen tester is trying to do and the situation.

Is the port open? Is the prerequisite software installed? In order to choose the best pivoting technique, the pen tester needs to match the technique to the situation

As a suggestion for the next topics, it is interesting to work with different scenarios, such as different operating systems, in addition to the use of containers, as mentioned superficially in this article.

8 References

[1]https://github.com/jpillora/chisel- Access at 01/05/2020
[2]http://www.dvwa.co.uk/ - Access at 01/05/2020
https://nullsweep.com/pivot-cheatsheet-for-pentesters/ – Access at 01/05/2020
https://miloserdov.org/?p=2973 - Access at 01/05/2020
https://highon.coffee/blog/ssh-meterpreter-pivoting-techniques/ - Access at 02/05/2020
https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Network%20Pivoting%20Techniques.md - Access at 03/05/2020
https://artkond.com/2017/03/23/pivoting-guide/- Access at 03/05/2020
https://resources.infosecinstitute.com/pivoting-exploit-system-another-network/#gref - Access at 04/05/2020
https://blog.midri.com.br/pentest/pivoting-o-que-e-quais-as-opcoes-e-como-usa-las/ - Access at 05/01/2020
https://0xdf.gitlab.io/2019/01/28/tunneling-with-chisel-and-ssf.html - Access at 05/01/2020
https://www.puckiestyle.nl/pivot-with-chisel/ - Access at 05/01/2020
https://www.sans.org/reading-room/whitepapers/testing/tunneling-pivoting-web-application-penetration-testing-36117 - Access at 05/01/2020