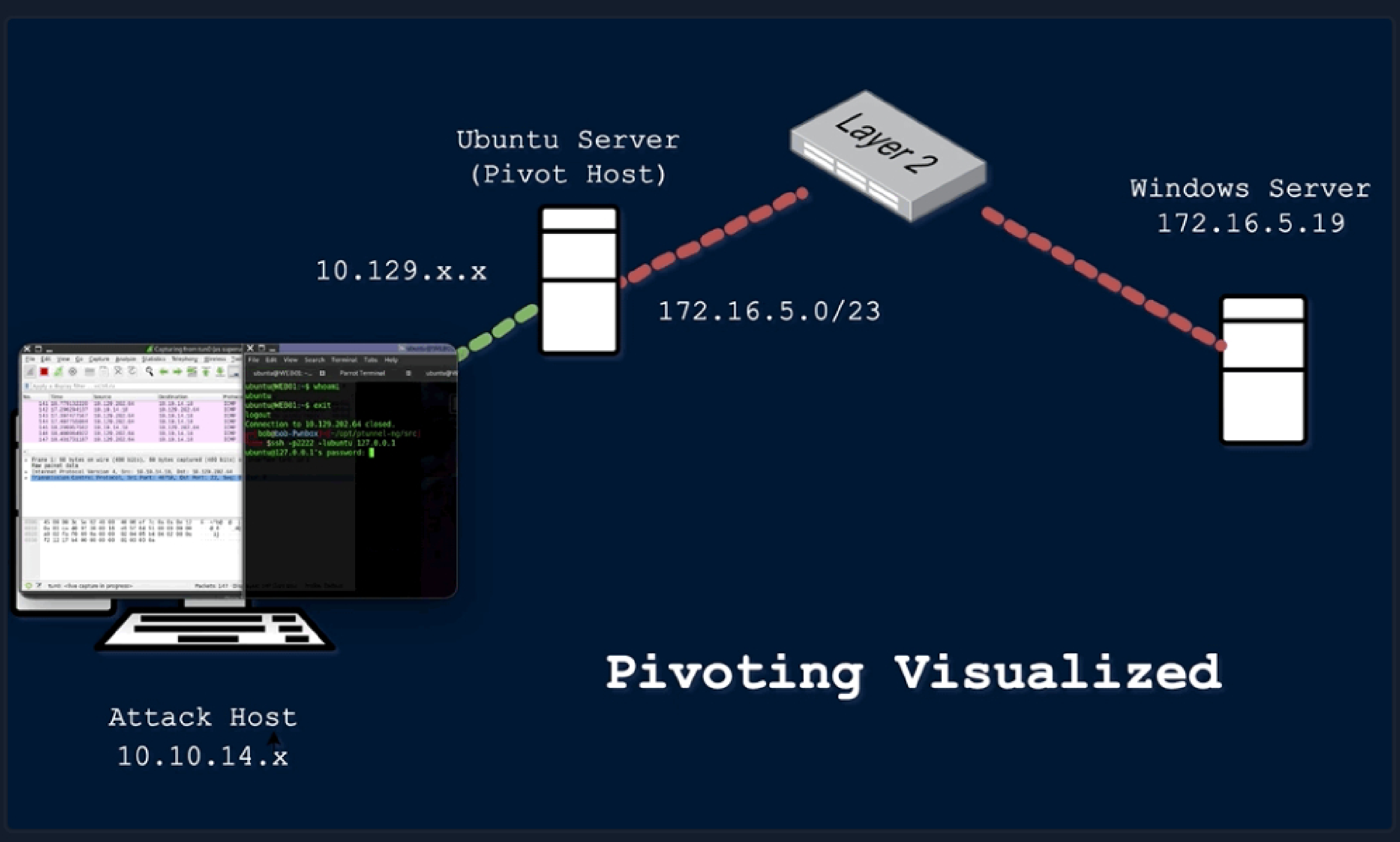
Introduction to Pivoting, Tunneling, and Port Forwarding



During a `red team engagement`, `penetration test`, or an `Active Directory assessment`, we will often find ourselves in a situation where we might have already compromised the required `credentials`, `ssh keys`, `hashes`, or `access tokens` to move onto another host, but there may be no other host directly reachable from our attack host. In such cases, we may need to use a `pivot host` that we have already compromised to find a way to our next target. One of the most important things to do when landing on a host for the first time is to check our `privilege level`, `network connections`, and potential `VPN or other remote access software`. If a host has more than one network adapter, we can likely use it to move to a different network segment. Pivoting is essentially the idea of `moving to other networks through a compromised host to find more targets on different network segments`.

There are many different terms used to describe a compromised host that we can use to `pivot` to a previously unreachable network segment. Some of the most common are:

- `Pivot Host`
- `Proxy`
- `Foothold`
- `Beach Head system`
- `Jump Host`

Pivoting's primary use is to defeat segmentation (both physically and virtually) to access an isolated network. `Tunneling`, on the other hand, is a subset of pivoting. Tunneling encapsulates network traffic into another protocol and routes traffic through it. Think of it like this:

We have a `key` we need to send to a partner, but we do not want anyone who sees our package to know it is a key. So we get a stuffed animal toy and hide the key inside with instructions about what it does. We then package the toy up and send it to our partner. Anyone who inspects the box will see a simple stuffed toy, not realizing it contains something else. Only our partner will know that the key is hidden inside and will learn how to access and use it once delivered.

Typical applications like VPNs or specialized browsers are just another form of tunneling network traffic.

We will inevitably come across several different terms used to describe the same thing in IT & the Infosec industry. With pivoting, we will notice that this is often referred to as `Lateral Movement`.

`Isn't it the same thing as pivoting?`

The answer to that is not exactly. Let's take a second to compare and contrast `Lateral Movement` with `Pivoting and Tunneling`, as there can be some confusion as to why some consider them different concepts.

Lateral Movement, Pivoting, and Tunneling Compared

Lateral Movement

Lateral movement can be described as a technique used to further our access to additional `hosts`, `applications`, and `services` within a network environment. Lateral movement can also help us gain access to specific domain resources we may need to elevate our privileges. Lateral Movement often enables privilege escalation across hosts. In addition to the explanation we have provided for this concept, we can also study how other respected organizations explain Lateral Movement. Check out these two explanations when time permits:

Palo Alto Network's Explanation

MITRE's Explanation

One practical example of `Lateral Movement` would be:

> During an assessment, we gained initial access to the target environment and were able to gain control of the local administrator account. We performed a network scan and found three more Windows hosts in the network. We attempted to use the same local administrator credentials, and one of those devices shared the same administrator account. We used the credentials to move laterally to that other device, enabling us to compromise the domain further.

Pivoting

Utilizing multiple hosts to cross `network` boundaries you would not usually have access to. This is more of a targeted objective. The goal here is to allow us to move deeper into a network by compromising targeted hosts or infrastructure.

One practical example of `Pivoting` would be:

> During one tricky engagement, the target had their network physically and logically separated. This separation made it difficult for us to move around and complete our objectives. We had to search the network and compromise a host that turned out to be the engineering workstation used to maintain and monitor equipment in the operational environment, submit reports, and perform other administrative duties in the enterprise environment. That host turned out to be dual-homed (having more than one physical NIC connected to different networks). Without it having access to both enterprise and operational networks, we would not have been able to pivot as we needed to complete our assessment.

Tunneling

We often find ourselves using various protocols to shuttle traffic in/out of a network where there is a chance of our traffic being detected. For example, using HTTP to mask our Command & Control traffic from a server we own to the victim host. The key here is obfuscation of our actions to avoid detection for as long as possible. We utilize protocols with enhanced security measures such as HTTPS over TLS or SSH over other transport protocols. These types of actions also enable tactics like the exfiltration of data out of a target network or the delivery of more payloads and instructions into the network.

One practical example of `Tunneling` would be:

> One way we used Tunneling was to craft our traffic to hide in HTTP and HTTPS. This is a common way we maintained Command and Control (C2) of the hosts we had compromised within a network. We masked our instructions inside GET and POST requests that appeared as normal traffic and, to the untrained eye, would look like a web request or response to any old website. If the packet were formed properly, it would be forwarded to our Control server. If it were not, it would be redirected to another website, potentially throwing off the defender checking it out.

To summarize, we should look at these tactics as separate things. Lateral Movement helps us spread wide within a network, elevating our privileges, while Pivoting allows us to delve deeper into the networks accessing previously unreachable environments. Keep this comparison in mind while moving through this module.

Now that we have been introduced to the module and have defined and compared Lateral Movement, Pivoting, and Tunneling, let's dive into some of the networking concepts that enable us to perform these tactics.

Next ➜ ✓ Mark Complete & Next

Cheat Sheet

Table of Contents

Introduction

Choosing The Dig Site & Starting Our Tunnels

Playing Pong with Socat

Pivoting Around Obstacles

Branching Out Our Tunnels

Double Pivots

Skills Assessment

Additional Considerations

My Workstation

OFFLINE

● Start Instance

∞ / 1 spawns left