Introduction

Our company was commissioned by a new customer (Inlanefreight) to perform an external and internal penetration test. As already mentioned, proper Operating System preparation is required before conducting any penetration test. Our customer provides us with internal systems that we should prepare before the engagement so that the penetration testing activities commence without delays. For this, we have to prepare the necessary operating systems accordingly and efficiently.

Penetration Testing Stages & Situations

Every penetration test is different in terms of scope, expected results, and environment, depending on the customer's service line and infrastructure. Apart from the different penetration testing stages we usually go through; our activities can vary depending on the type of penetration test, which can either extend or limit our working environment and capabilities.

For example, if we are performing an internal penetration test, in most cases, we are provided with an internal host from which we can work. Suppose this host has internet access (which is usually the case). In that case, we need a corresponding Virtual Private Server (VPS) with our tools to access and download the related penetration testing resources quickly.

Testing may be performed remotely or on-site, depending on the client's preference. If remote, we will typically ship them a device with our penetration testing distro of choice pre-installed or provide them with a custom VM that will call back to our infrastructure via OpenVPN. The client will elect to either host an image (that we must log into and customize a bit on day one) and give us SSH access via IP whitelisting or VPN access directly into their network. Some clients will prefer not to host any image and provide VPN access, in which case we are free to test from our own local Linux and Windows VMs.

When traveling on-site to a client, it is essential to have both a customized and fully up-to-date Linux and Windows VM. Certain tools work best (or only) on Linux, and having a Windows VM makes specific tasks (such as enumerating Active Directory) much easier and more efficient. Regardless of the setup chosen, we must guide our clients on the pros and cons and help guide them towards the best possible solution based on their network and requirements.

This is yet another area of penetration testing in which we must be versatile and adaptable as subject matter experts. We must make sure we are fully prepared on day 1 of the assessment with the proper tools to provide the client with the best possible value and in-depth assessment. Every environment is different, and we never know what we will encounter once we start enumerating the network and uncovering issues. We have to compile/install tools or download specific scripts to our attack VM during almost every assessment we perform. Having our tools set up in the best way possible will ensure that we don't waste time in the early days of the assessment but instead only have to make changes to our assessment VMs for specific scenarios we encounter during the assessment.

Setup & Efficiency

Over time, we all gather different experiences and collections of tools that we are most familiar with. Being structured is of paramount importance, as it increases our efficiency in penetration testing. Searching for individual resources and even needing additional tools to make these resources work by the time an engagement starts can be eliminated by having access to a prebaked, organized, and structured environment. Doing so requires some preparation and knowledge of different operating systems.

Next ➡

✔ Mark Complete & Next

Table of Contents

Introduction

Operating Systems

Virtual Private Server

My Workstation

OFFLINE

▶ Start Instance

1 / 1 spawns left