**1. Enumeration Basics**

**Overview**

**Enumeration**

The first thing you may ask yourself is "what is enumeration". The answer is pretty simple. All we are doing is collecting information. Essentially, it is the process of conducting recon on the machine. Once we have collected enough information, we look at how we can leverage that data to form an attack.

**Basic Recon**

Imagine for a second you have been asked to conduct a penetration test against an unknown target (also known as black-box testing).

Let's make a list of a couple of things we need to know about the box to start our pentest.

1. IP address / hostname (normally given)

2. Operating system

3. Services running

Say we have run our tools and found all the items in the above list, we now know the hypothetical target is a Linux machine and we found the two ports open below (don't worry if you don't know how it's done, still explaining what it is).

**Ports**

|  |  |
| --- | --- |
| **TCP Ports** | **UDP Ports** |
| 22, 80 |  |

Against these ports, we start to note the hypothetical service versions.

**SSH on port 22**

This is running OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

**Web server on port 80**

This is running nginx 1.14.2

**What can we do with it?**

So far, we have enumerated:

1. The operating system as Linux

2. The service on port 22 as SSH at version 7.9p1

3. The service on port 80 as an nginx web server at version 1.14.2

We now know a little about the target, so we can start to form up our attack. However, we are not done collecting data as we have many unknowns.

Our next step is to identify if we can enumerate anything else from the services we have found. **Service Enumeration**

We have two services; SSH and nginx. We need to decide which is more likely to aid us and as a result, be targeted first.

**SSH on port 22**

We have no valid credentials for the SSH server. If it was a version <7.7 , we could continue enumeration there and search for valid usernames using something like

https://www.rapid7.com/db/modules/auxiliary/scanner/ssh/ssh\_enumusers/. This isn't an option for us so alternatively, we could use a tool like hydra to run through sets of default credentials and hope for the best. <https://tools.kali.org/password-attacks/hydra>

Why would this not be a good approach? for one, it's noisy. What if we lock ourselves out of the machine by triggering a protection mechanism like fail2ban - that would be less than ideal. Our highest chance of success would be to continue enumeration on the web server and see what we can find there.

**Web server on port 80**

The web server is a more attractive option. We may find references to internal databases, depending on site services it may have a large attack surface, and we may find usernames from page posts or backup files etc.

**Enumerating a web server**

As for the web server, we are interested in finding what pages / files may be available. You could use a tool such as dirb or dirseach or even gobuster . Once you have found some sites, it is worth looking at the technologies the site uses. For this, the browser extension Wappalyzer will give you a list.

Our results have come in, it has found a site at index.php along with a web folder called backup . Once we navigate to index.php , Wappalyzer reports the site is running an old version of wordpress.

We now have a starting place and several places of interest have been enumerated for further investigation.

**Summary**

Time to look at what we have covered.

1. We have looked at enumerating ports and services

2. We have briefly looked at how we would prioritize two simple services

3. We have looked at some of the tools and plugins we could use for enumerating more data from a discovered service.

We can use tools to automate the initial enumeration phase. This will be covered separately.