Jenkins - Discovery & Enumeration

Jenkins is an open-source automation server written in Java that helps developers build and test their software projects continuously. It is a server-based system that runs in servlet containers such as Tomcat. Over the years, researchers have uncovered various vulnerabilities in Jenkins, including some that allow for remote code execution without requiring authentication. Jenkins is a continuous integration server. Here are a few interesting points about Jenkins:

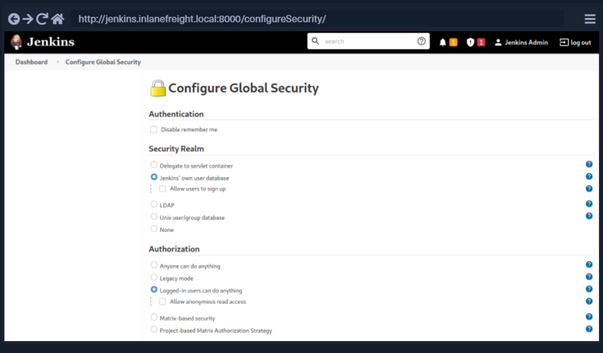
- Jenkins was originally named Hudson (released in 2005) and was renamed in 2011 after a dispute with Oracle
- Data shows that over 86,000 companies use Jenkins
- Jenkins is used by well-known companies such as Facebook, Netflix, Udemy, Robinhood, and LinkedIn
- It has over 300 plugins to support building and testing projects

Discovery/Footprinting

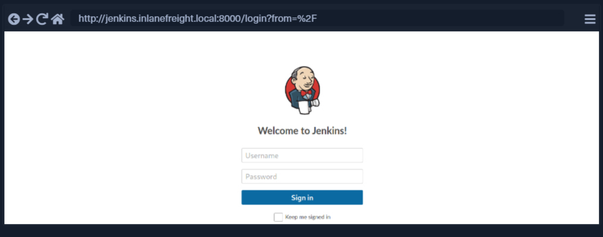
Let's assume we are working on an internal penetration test and have completed our web discovery scans. We notice what we believe is a Jenkins instance and know it is often installed on Windows servers running as the all-powerful SYSTEM account. If we can gain access via Jenkins and gain remote code execution as the SYSTEM account, we would have a foothold in Active Directory to begin enumeration of the domain environment.

Jenkins runs on Tomcat port 8080 by default. It also utilizes port 5000 to attach slave servers. This port is used to communicate between masters and slaves. Jenkins can use a local database, LDAP, Unix user database, delegate security to a servlet container, or use no authentication at all. Administrators can also allow or disallow users from creating accounts.

Enumeration



The default installation typically uses Jenkins' database to store credentials and does not allow users to register an account. We can fingerprint Jenkins quickly by the telltale login page.



We may encounter a Jenkins instance that uses weak or default credentials such as `admin:admin` or does not have any type of authentication enabled. It is not uncommon to find Jenkins instances that do not require any authentication during an internal penetration test. While rare, we have come across Jenkins during external penetration tests that we were able to attack.

Start Instance

∞ / 1 spawns left

Waiting to start...

Questions

Answer the question(s) below to complete this Section and earn cubes!

Cheat Sheet

Get VPN Key

Target: Click here to spawn the target system!

vHosts needed for these questions:

- `jenkins.inlanefreight.local`

Authenticate to with user "admin" and password "admin"

+1 Log in to the Jenkins instance at http://jenkins.inlanefreight.local:8000. Browse around and submit the version number when you are ready to move on.

2.303.1

Submit

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left