Demo Company
Security Assessment Findings Report

Date: November 19th, 2022

My name is Adrian Saiz and this is a small report on the vulnerabilities found during the Schenider hackathon. Note that this is my first hackathon and it has been the first "machine" that I try to solve without any walkthrough.

So far my knowledge about vulnerabilities is based purely on read documentation and little practice (we will improve this little by little).

With this in mind, let's start with the report:

INTRODUCTION

The first step to enter the repository via IP (in our case '18.133.187.152') has been to transform the OpenSSH credentials to RSA. It might not have been necessary, but I didn't know other ways to connect to the machine.

Once inside as instructed we had to modify the hosts file to be able to view the web page that had been compromised. Once this intermediate step is completed, in the vese-projects-code folder we can see 4 different utilities. Each of these utilities has a different vulnerability and in turn, the ssh connection made, suffers from a security flaw.

Now, let's start with the 3 vulnerabilities found:

1) The first one is about an anomaly on the "smb" protocol. If we list the set of users that our machine has, we observe that surprisingly it presents a UserID higher than 1000 that is related to users that are not by default (i.e. has been added to the system). Despite trying several ways to exploit this, I have not managed to escalate privileges, but I am pretty sure that by running some common program and applying this protocol, you can root the system.

Risk level: Critical

2)In the switch.py file of the pseudo-terminal functionality, we observe that the cmd_banner function has an important security breach, because if we introduce as parameters an s initially and edit the variable self.bannertext, but then we introduce something empty, it will execute as a command any instruction that we have introduced in the variable described above.

Risk level: High

3) Finally we leave the one that for me has been the clearest to interpret when I discovered it. And it is a vulnerability in the web, specifically in the file test-comment.php which has hidden in a line of code a revershell. This is easily manipulated and if you manage to enter your attacker ip, you are able to access the system. To do this you must enter:

-> $name == "test1" && $email == "test@test.com" && $message == "test2"

Risk level: High

I would like to thank the nuwe team for this hackathon as it has managed to test some of the little knowledge that I know but I am slowly learning.

Adrian Saiz