Security Assessment and Operations Lab

Exercise 2 - Exposing and cracking weak passwordsSS 2023

Introduction

To use guessing and cracking in order to expose weak passwords is an important step for each penetration test. Finding a public facing service in the network with a weakly set password can be enough to bypass the firewall and have an insider view on the system or network. In this exercise the password brute forcing tool John the Ripper will be used in conjunction with cewl, in order to create a wordlist, apply mutation on the wordlist and with the wordlist first enter a vulnerable web application and from there find a way to get root privileges on the system.

Helpful tools

All the tools necessary for this exercise are preinstalled on Kali

- John the ripper
- CeWl
- WPScan

Exercise 2-1: Enumeration and Inital Access

On your group's subnet this exercises machine is now available. You can find it with a ping sweep or through the reset page. The first step of this challenge is to break into the administrator account of a web application

Exercise 2-2: Gaining a Shell

The second step is to get a shell from the administration panel.

Exercise 2-3: Escalate Privileges

And the third step is to escalate the privileges to root privileges. Remember the theme of this exercise sheet is password cracking. Here is a good resource to start with `https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Linux%20-%20Privilege%20Escalation.md`

Hints

It is necessary for this exercise to write a custom mutation rule for john, as described in the lecture. We won't give you a more explanation by now. We want you to try first and ask us when you feel stuck (daniel.reti@dfki.de). Tell me what you have tried so far, and I will help you with further hints.

Report

Write a brief report including your solutions and your findings across all six machines. Then, submit the report via OLAT. You can find a LaTeXtemplate on OLAT.