Ethical Hacking Essentials - Summer 2024

Sambuddho

July 29, 2024

Ethical Hacking Exercise (total points: 100)

Due date: Aug. 4. Time: 23:59 Hrs.

You are being provided with a VM with several known vulnerabilities. Your task would be to launch a penetration test on the VM and discover the vulnerabilities and exploit them, e.g. to brute force the password, launch a shellcode *etc.* You could use various tools for the entire process, *e.g.* `nmap` and `nikto` for reconnaissance and directory scanning, `exploitDB` to determine known vulnerabilities of the services running, running `metasploit` to actually exploit the discovered vulnerabilities, using tools like `msfvenom` to actually craft shellcode, *etc.*

You submit a report with the following:

1. Details of the steps taken, starting from reconnaissance to the exploit along with all the screenshots, commands/tools used with their descriptions and the arguments and their semantics, *i.e.* what each of those commands and their respective arguments are expected to do and what they finally do. **50 points**

2. One of the tasks is to discover a non-root/non-admin user in the VM and the user's password. You may use various password bruteforce tools for this like `hydra.` You must show the steps involved, the arguments used and their semantic meanngs, along with their outcomes. **50 points**