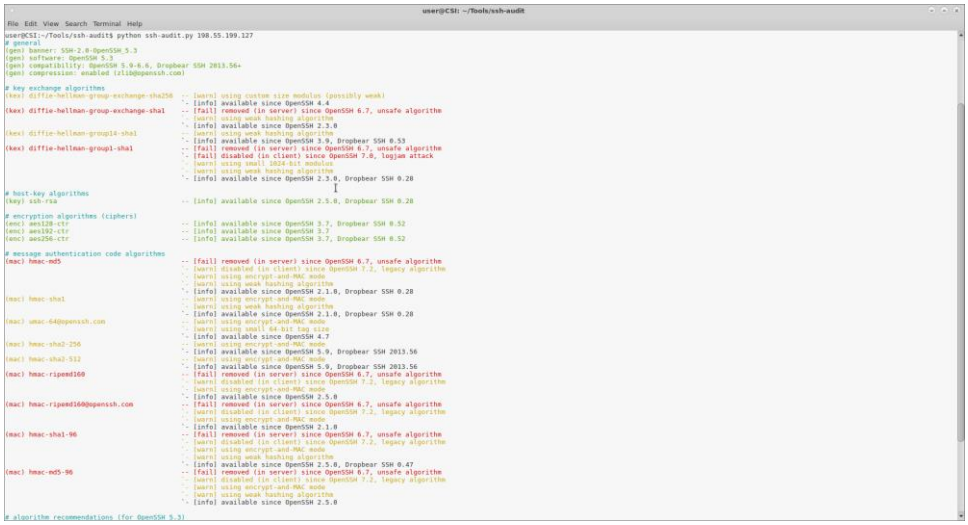
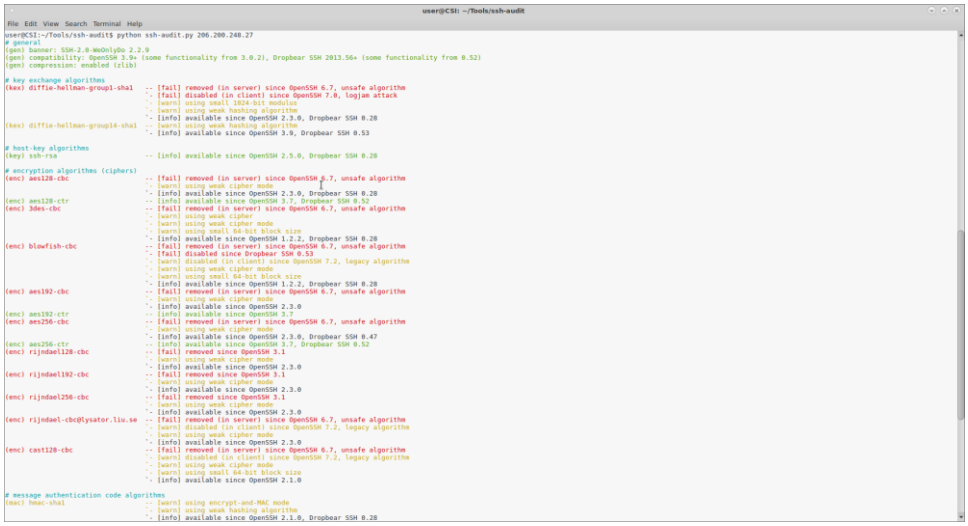
P3.1 - SSH

1:





2:

- 198.55.199.127:
  - Software: OpenSSH
  - Versão: 5.3

- 206.200.248.27:
  - Software: WeOnlyDo
  - Versão: 2.2.9

3: De acordo com o shodan, conseguimos concluir que o WeOnlyDo apresenta 5 vulnerabilidades enquanto o OpenSSH apresenta 11. Logo, concluímos que o OpenSSH apresenta mais vulnerabilidades.

4: A vulnerabilidade mais grave é a CVE-2010-3972, com um score de 10.0 (high)).

5: Esta vulnerabilidade é baseada num overflow de um Heap-based buffer. Isto permite aos atacantes executar codigos, arbitrariamente, ou executar ataces de Deniel of Service.

Esta vulnerabilidade afeta a confidencialidade, integridade e a disponivilidade do servidor. Esta tambem permite a sua modificação não autorizada e disclosure of information.