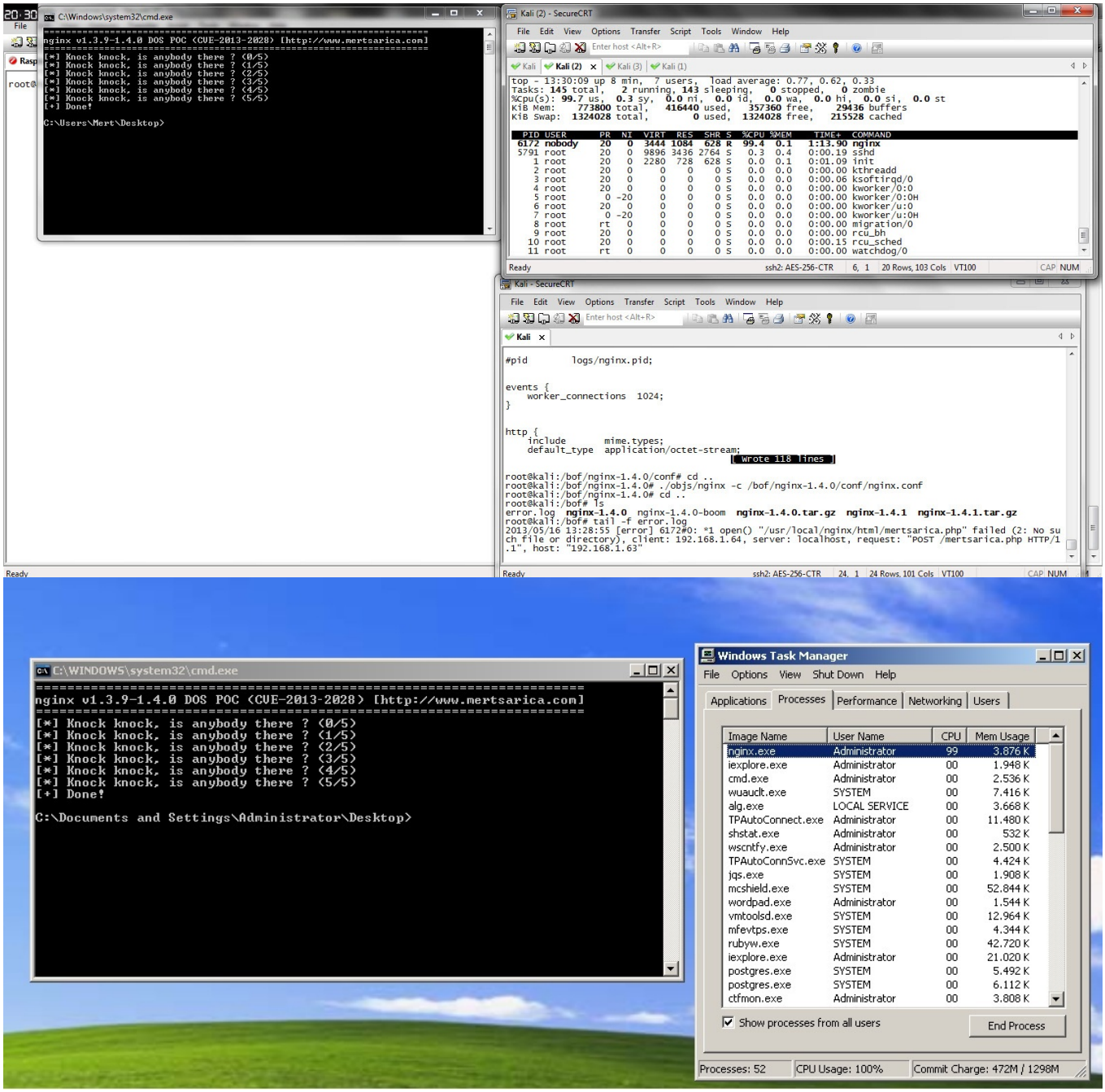
Nginx DoS İstismar Kodu

written by Mert SARICA | 17 May 2013

7 Mayıs tarihinde Nginx'in resmi web sayfasında, Greg MacManus tarafından nginx v1.3.9 ve 1.4.0 sürümlerinde tespit edilen bellek taşması güvenlik zafiyeti (CVE-2013-2028) için bir yama yayınlandığı belirtilmişti. Can sıkıntısı nedeniyle bu zafiyet üzerinde yaptığım 1 saatlik bir araştırmada, bu zafiyeti istismar eden ve nginx web sunucusunu hizmet dışı bırakan bir istismar kodu hazırladım.

Kali ve Windows XP işletim sistemleri üzerinde denediğim ve Exploit-DB'ye gönderdiğim istismar koduna buradan ulaşabilirsiniz.



Not: Exploit-DB ve Packetstorm’a dosyaları gönderirken CVE-2013-2028 yerine CVE-2013-2070 olarak göndermişim, doğrusu CVE-2013-2028 olacaktır.
I submitted the POC code with wrong CVE (CVE-2013-2070) to Exploit-DB & PacketStorm so the correct one is CVE-2013-2028.