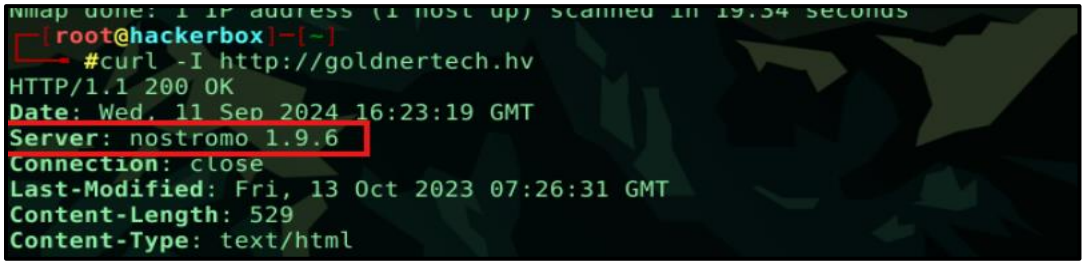
GLITCH ISINMASI

INFO: Bu alıştırma, yaygın olarak kullanılan nostromo web sunucusunda zafiyet araştırmacılığının nasıl yapılacağını ve linux tabanlı sistemlerde yetki yükseltme saldırılarının nasıl yapılabileceğini öğretmeye odaklanır.

Bir web uygulamasında zafiyet tespit edilmesi, zafiyetin istismar edilmesi ve linux çekirdeğinden kaynaklı yetki yükseltme saldırıları ile ilgili alıştırmalar yapmak için önerilir.

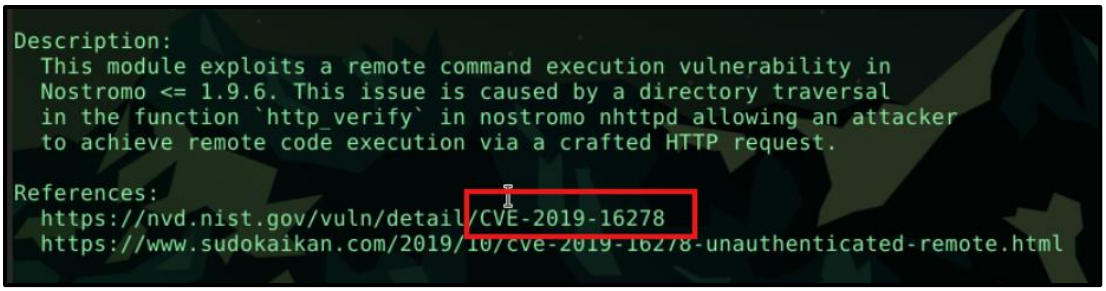
1. *Hangi portlar açık?*
   Bilgi: Önce "nslookup" komutu ile "ıp adresi" öğrenilir, ardından nmap atılarak port taraması gerçekleştirilir.

2. *Çalışan web sunucusunun adı nedir?*
   Bilgi: Terminal veya komut satırında "curl" komutunu kullanarak sunucunun yanıt başlıklarını inceleyebiliriz. Bu komut, hedef web sitesinin yanıt başlıklarını gösterecektir. Server: satırı, web sunucusunun adını ve bazen versiyonunu belirtir.
   curl -I http://siteadresi.com

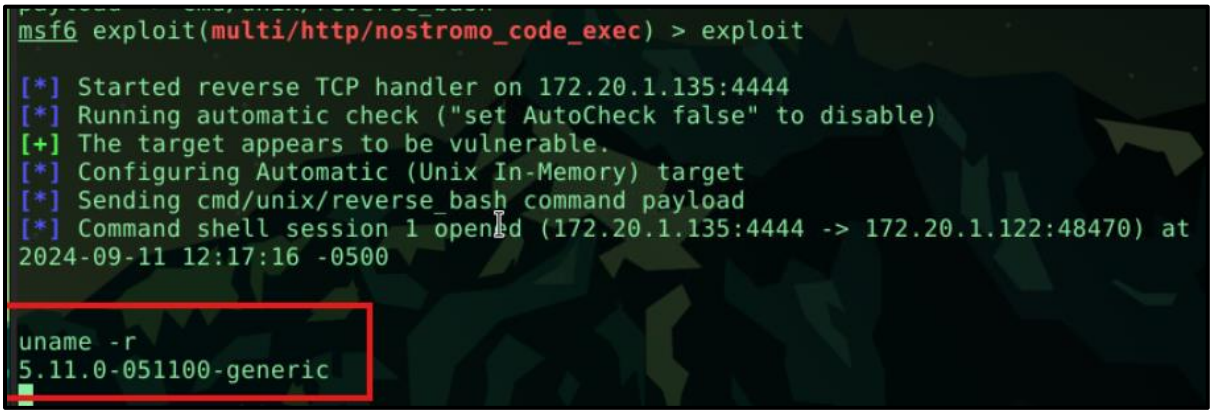


3. *Güvenlik zafiyetinin CVE kodu nedir?*
   Bilgi: msfconsoleda araştırma yapılır ve "CVE kodu" bulunur.

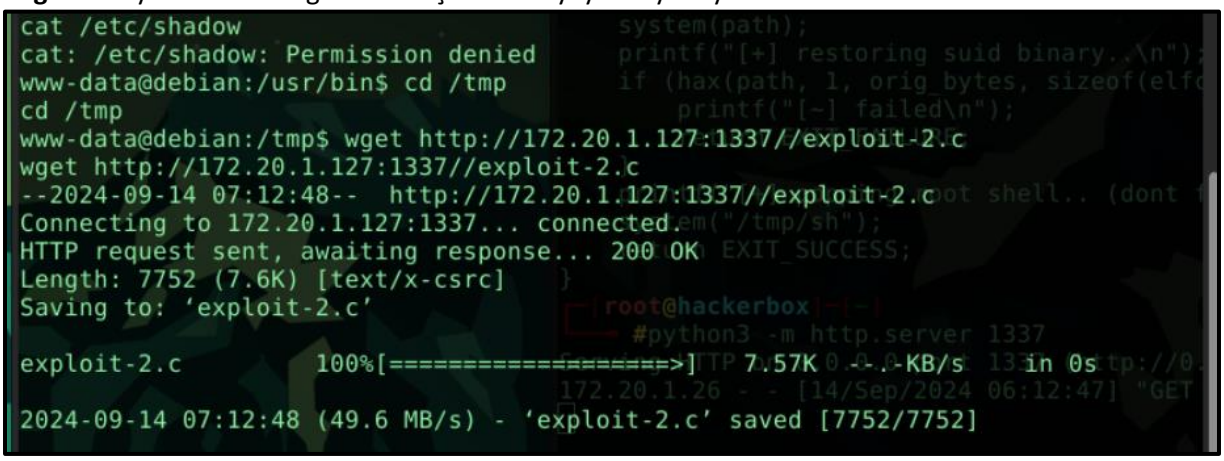
“ınfo” komutu ile bilgi alınır.



4. *Linux çekirdek sürümü nedir?*
   Bilgi: Linux çekirdek sürümünü öğrenmek için öncelikle exploiti entegre etmemiz gerekiyor. Exploiti entegre edip “uname –r” komutu ile öğrenebiliriz.
   - *RHOSTS: Hedef makine (Nostromo sunucusu) IP'si: 172.20.1.1*
   - *RPORT: Hedef port (varsayılan HTTP portu): 80*
   - *LHOST: Senin makinenin (saldırganın) IP'si: 172.20.1.135*
   - *LPORT: Ters bağlantı için kullanılacak port: 4444*
   - *Payload: cmd/unix/reverse*

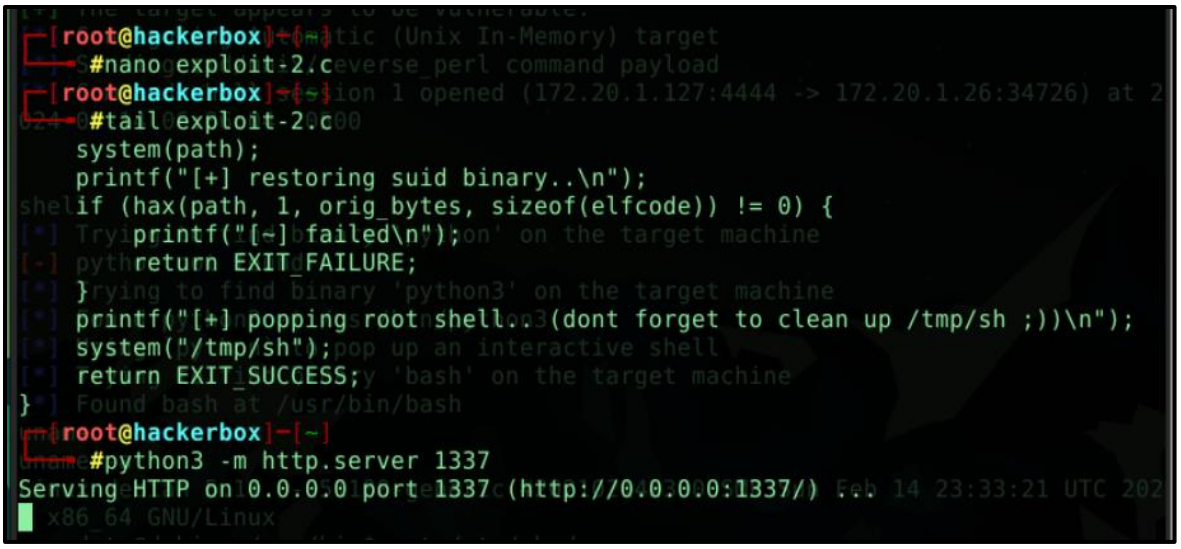


5. *"hackviser" kullanıcısı için /etc/shadow içindeki parola hash değeri nedir?*
   Bilgi: Yetki yükseltmemiz gerekecek çünkü dosyayı okuyamıyoruz.



Yetki yükseltmek için https://github.com/AlexisAhmed/CVE-2022-0847-DirtyPipe-Exploits/blob/main/exploit-2.c “yi kullanacağız.

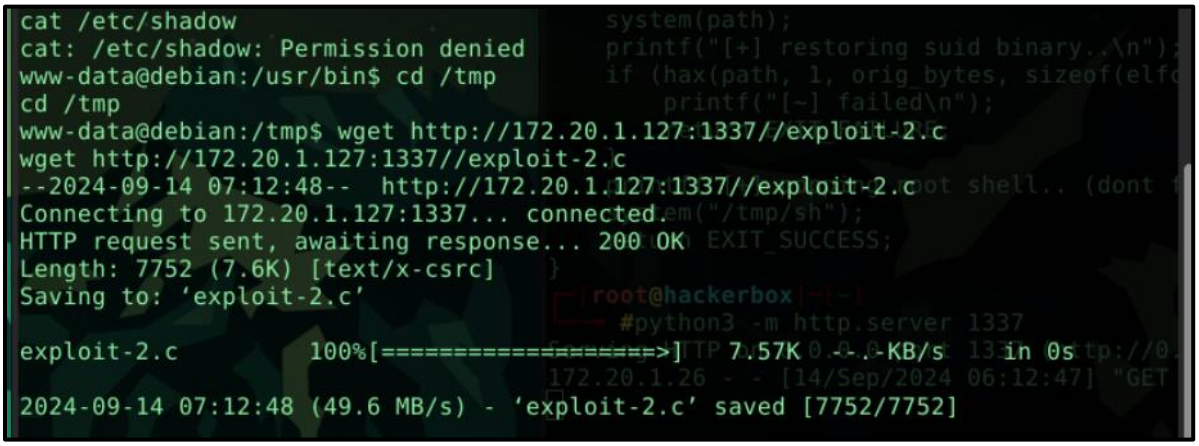
Öncelikle makinemize kodları kopyalayarak dosyayı oluşturalım. Bundan sonrasında hedef makinemize bunu yükleyebilmemiz gerekecek, bu yüzden de makinemizle server ayağa kaldırıyoruz.



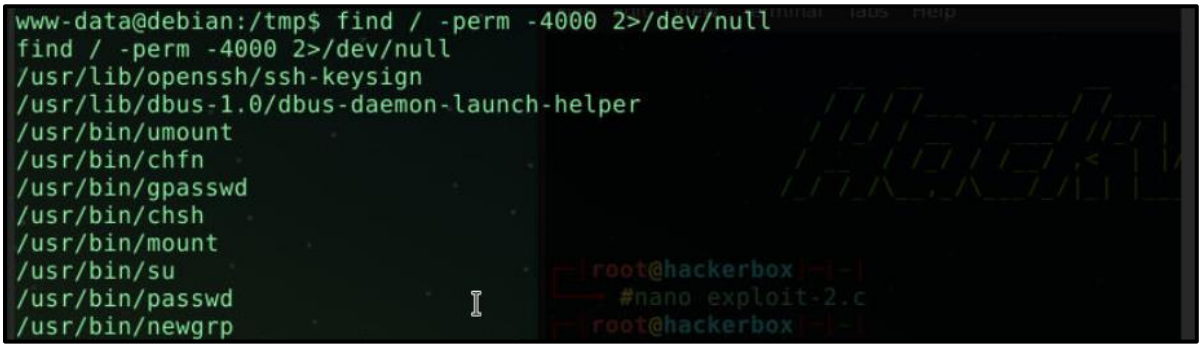
Ardından hedef makinemize geçerek yetki yükseltme işlemlerine başlıyoruz. Exploit-2.c dosyasını hedef makinemize indiriyoruz.

Komut açıklaması: Linux veya benzeri Unix tabanlı sistemlerde gcc (GNU Compiler Collection) derleyicisi kullanılarak C dilinde yazılmış bir dosyayı derlemek için kullanılır.

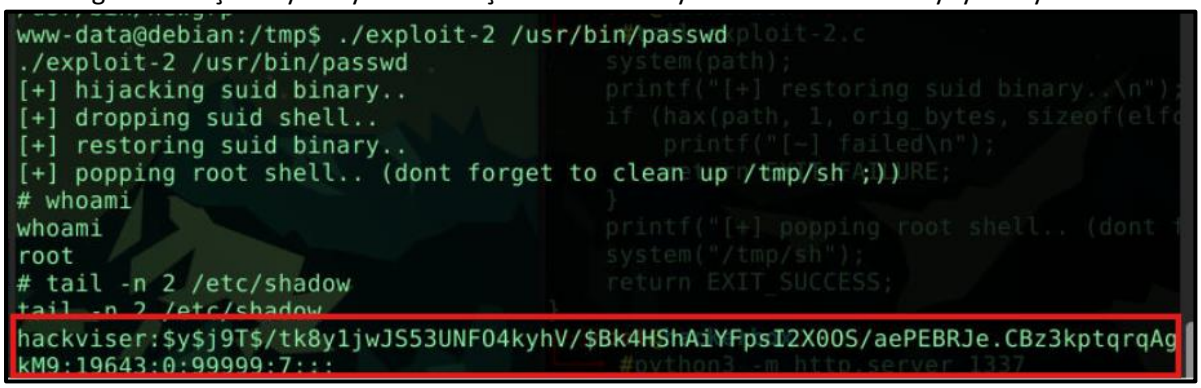
- *gcc: C dilinde yazılmış kodları derlemek için kullanılan komut.*
- *exploit-2.c: Derlenmek istenen kaynak kod dosyasının adı. Bu dosya, C dilinde yazılmış bir program içeriyor.*
- *-o exploit-2: Derlenen programın çıktı dosyasının adını belirtir. Burada, derlenen dosyanın ismi exploit-2 olacak.*



Ardından yetki yükseltebileceğimiz SUID dosyalara bakıyoruz.



Herhangi birini seçerek yetki yükseltme işlemini tamamlıyoruz ve istenilen dosyayı okuyoruz.



-ISINMA TAMAMLANDI-