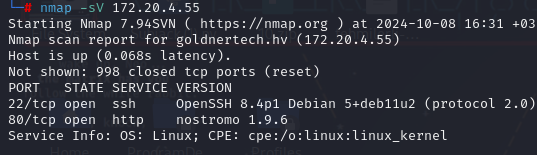
**GLITCH WRİTE-UP**

Bu yazımda sizlere Hackviser platformu üzerinde bulunan Glitch adlı warmup’ın çözümünü anlatacağım. Bu labı çözebilmemiz için öncelikle bağlantı kurduktan sonra Linux terminalimizde “nano /etc/hosts” dosyasına girerek Hackviser’da bize verilen “172.20.4.55 goldnertech.hv” kodlarını ekleme yaparak kaydediyoruz. Ve hazırız.

**SORU 1:** Hangi portlar açık?

Bu sorunun cevabını bulabilmek için Nmap taraması yapacağım.

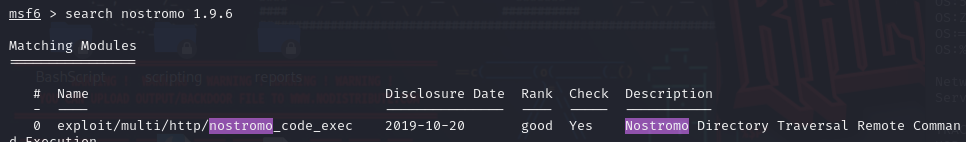
 **22** ve **80** portları açık.

**SORU 2:** Çalışan web sunucusunun adı nedir?

Yukarıdaki ekran fotoğrafında da görüldüğü üzere servisin ismi **nostromo**

**SORU 3:** Güvenlik zafiyetinin CVE kodu nedir?

Msfconsole komutu ile metasploit framework’e giriş yapıp nostromo ve versiyonunu kullanarak arama yapıyoruz.



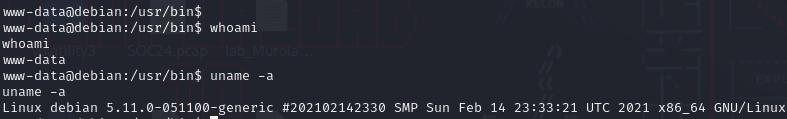
Şimdi seçip info diyerek CVE bilgisine ulaşıyoruz.



Cevap: **CVE-2019-16278**

**SORU 4:** Linux çekirdek sürümü nedir?

Bu sorunun cevabını bulabilmek için makineye erişim sağlamamız gerekiyor. Şimdi verilen bilgileri dodurup exploit edelim.



Başarılı bir şekilde Shell almayı başardık. Şimdi bağlantı kurduğumuz sistem hakkında bilgi almak için “uname –a” komutunu kullanıyoruz.

Ve istediğimizi bulduk. Cevap: **5.11.0-051100-generic**

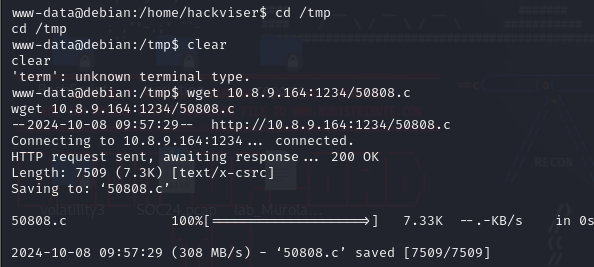
**SORU 5:** "hackviser" kullanıcısı için /etc/shadow içindeki parola hash değeri nedir?

Bu sorunun cevabını bulabilmemiz için root yetkisine sahip olmamız gerekiyor. Şimdi yetki yükseltme adımlarına başlayalım.

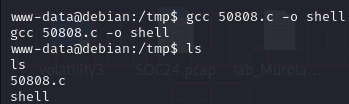
Burada bize verilen Linux çekirdek sürümünün açığı var mı yok mu diye kontrol yaptığımda bir zafiyet olduğunu buldum. [Site](https://www.exploit-db.com/exploits/50808) üzerinden açığa bakabilirsiniz. Dosyayı indiriyoruz. Dosyayı hedef sisteme yüklemek için geçici bir sunucu açıyoruz.



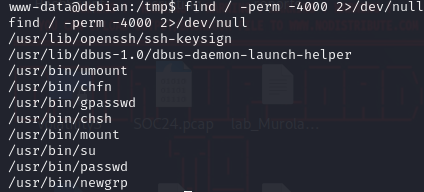
Şimdi hedef terminalden indirdiğimiz dosyayı yüklememiz gerekiyor.



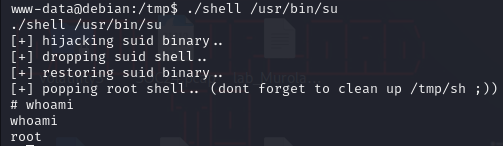
Yüklemeyi başarılı bir şekilde yaptık. Yüklediğimiz dosyayı derlemek için c dosyası değil de normal dosya olarak kaydedeceğiz.



Şimdi Shell dosyamız hazır. Hangi komutu kullanacağımızı bulalım

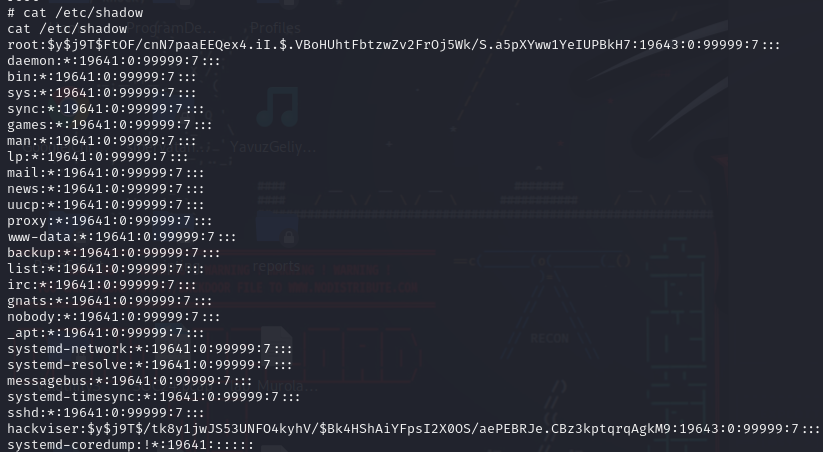


Biz su komutu ile bu işlemi gerçekleştirelim.



Ve artık root olmayı başardık ☺

Şimdi sorunun cevabını bulalım.



Cevap: **$y$j9T$/tk8y1jwJS53UNFO4kyhV/$Bk4HShAiYFpsI2X0OS/aePEBRJe.CBz3kptqrqAgkM9**