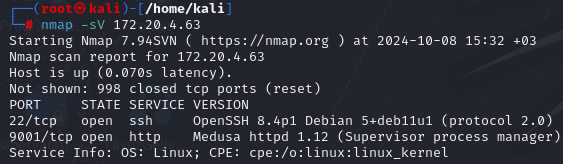
**SUPER PROCESS WRİTE-UP**

Bu yazımda sizlere Hackviser platformu üzerinde bulunan Super Process adlı warmup’ın çözümünü anlatacağım.

**SORU 1:** Hangi portlar açık?  
Bu sorunun cevabını bulmak için Nmap taraması yapıyoruz.



**22** ve **9001** portlarının açık olduğunu bulduk.

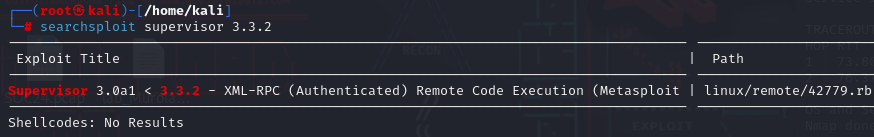
**SORU 2:** Web uygulamasında bulunan güvenlik açığının CVE kodu nedir?

Bunun için biraz siteye gidip bilgi toplamamız gerekecek. 9001 portunu kullanarak siteye gidiyorum.

Sayfanın en altında şöyle bir bilgiye rastladım: 

Şimdi bunun hakkında herhangi bir açık bulunup bulunmadığını kontrol edelim.

Bunun için de searchsploit aracını kullandım.

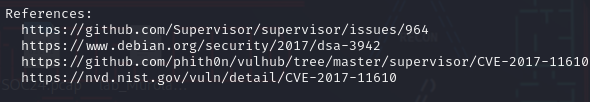


Böyle bir açık gerçekten varmış. Şimdi detayları görmek için metasploit framework’ü kulanacağım. Terminale gelip msfconsole yazarak başlatıyoruz.

Yukarıdaki bilgileri de kullanarak msfconsole içerisinde zaafiyeti buluyoruz.



Use 2 diyerek zaafiyeti seçiyoruz. Info yazarak da bu zafiyet hakkında bilgi sahibi oluyoruz.

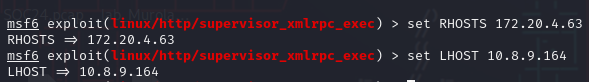


Cevabımız: **CVE-2017-11610**

**SORU 3:** Güvenlik zafiyeti bulunan servis hangi kullanıcının izinleri ve yetkileri ile çalışıyor?

Bu sorunun cevabını bulabilmemiz için Shell almamız gerekmektedir. Şimdi bizden istenilen bilgileri doldurarak Shell almaya çalışacağım.

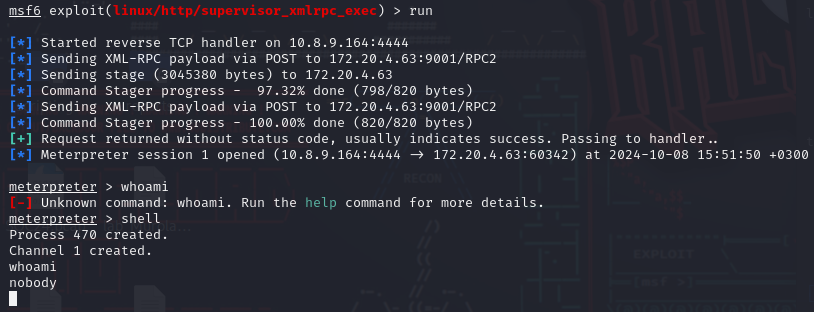
 Yes yazan kısımları dolduralım.



LHOST: Bizim kendi IP adresimizdir.

RHOST: Hedef IP adresidir.

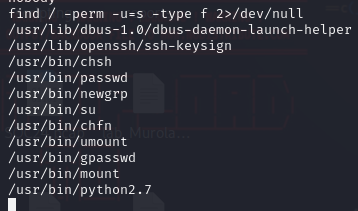
RUN diyerek çalıştıralım.

 Shell diyerek bağlantıyı kurduk. Burada bize hangi kullanıcı yetkileri ile çalıştığını sormuştu.

Buradan da anlayacağımız gibi cevap **nobody**

**SORU 4:** Yetki yükseltme için kullanabileceğimiz SUID izinlerine sahip uygulamanın adı nedir?

Bu sorunun cevabını bulabilmemiz için bu komutu kullanmamız gerekiyor: “*find / -perm -u=s -type f 2>/dev/null*”

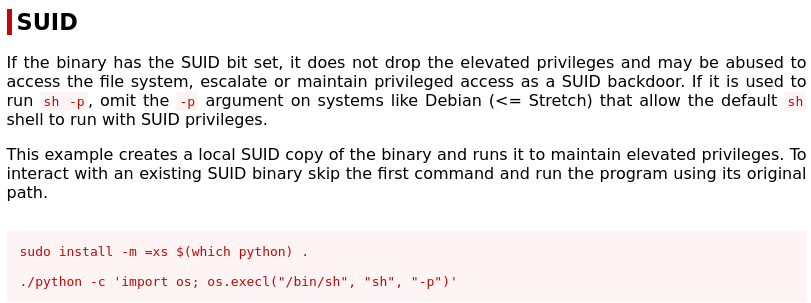


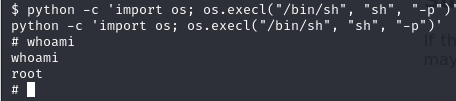
En altta sorunun cevabına ulaşmış olduk. Cevap: **python2.7**

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

Son sorumuzun cevabı için öncelikle bizim root olmamız gerekiyor. Bunun için de Privilege Esculation dediğimiz Yetki Yükseltme işlemini yapmamız gerekiyor.

Biraz araştırmalarım sonucunda yetki yükseltme için [GTFOBins](https://gtfobins.github.io/) sitesini ziyaret ettim. Bu sitede python aratınca komut olarak şunları buldum:

En alttaki komutu denedim.

 Ve artık root olduk ☺



Cevap: **$y$j9T$e8KohoZuo9Aaj1SpH7/pm1$mu9eKYycNlRPCJ51dW8d71.aPH0ceBM0AKxAaiil7C5**