

Tiger Write-up

Giriş

Tiger ısınma makinesi, VNC servisi ile ilgili temel alıřtırmalar yapmak için ideal bir başlangıç noktasıdır. Bu makinede, VNC servisinin yanlış yapılandırılmasından kaynaklanan güvenlik açıklarını bulmayı ve bunları nasıl kullanacağınızı öğreneceksiniz. Ayrıca VNC'nin temel işleyişini ve bağlanma yöntemlerini de öğreneceksiniz.

Virtual Network Computing (VNC)

Virtual Network Computing (VNC), uzaktaki bir bilgisayara grafik arayüz üzerinden erişim sağlayan bir masaüstü paylaşım sistemidir. İnternet veya yerel ağ üzerinden iki bilgisayar arasında görüntü, klavye ve fare girişlerinin iletimini mümkün kılarak, uzak bir sistem üzerinde çalışma imkanı sağlar. VNC, RFB (Remote Framebuffer) protokolünü kullanır ve platform bağımsız çalışabilir; yani farklı işletim sistemleri üzerinde kullanılabilir.

Görev 1

VNC'nin açılımı; **Virtual Network Computing**.

Bilgi Toplama

Hedef makinemize yönelik port taraması yaparak bilgi toplamaya başlayalım.

Görev 2

Yaptığımız port taraması sonucunda **5901** portunun açık olduğunu tespit ettik.

```
root@hackerbox:~# nmap -sV 172.20.6.141
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-03 07:45 CST
Nmap scan report for 172.20.6.141
Host is up (0.00037s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
5901/tcp  open  vnc      VNC (protocol 3.8)
MAC Address: 52:54:00:E2:63:7F (QEMU virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds
```

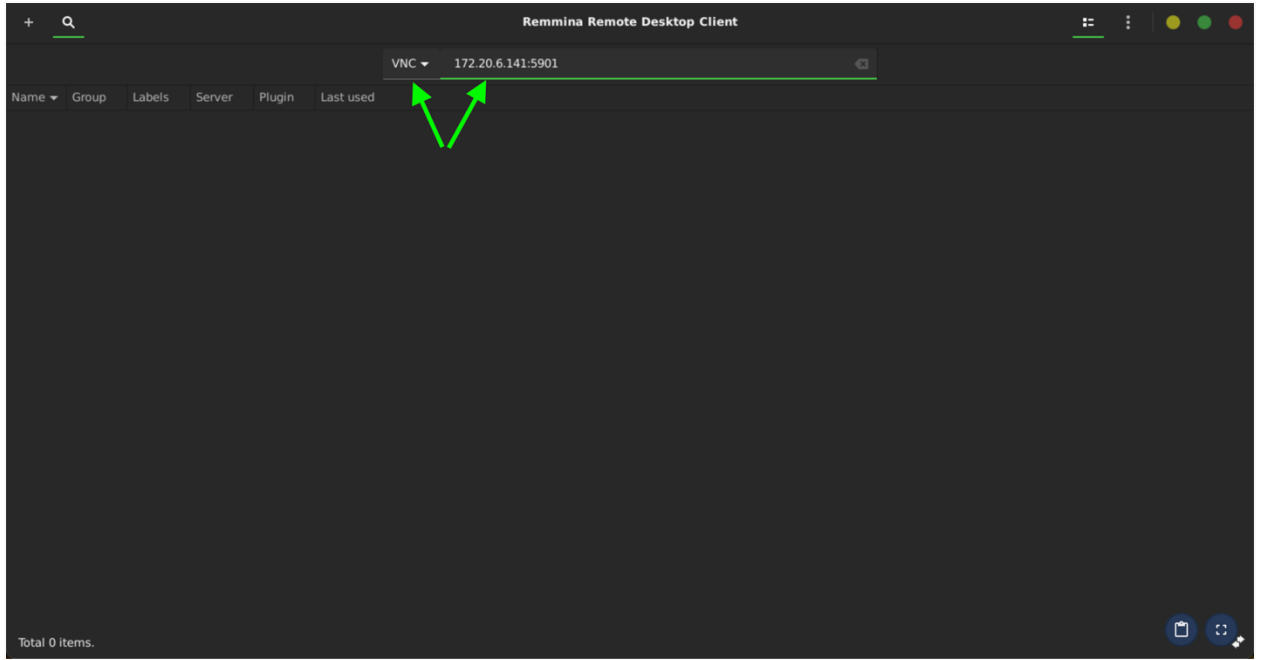
Sisteme Eriřim

Görev 3

Bu görevde istenen bilgiye ulaşabilmek için hedef makineye VNC ile bağlanmamız gerekiyor.

VNC ile bağlantı kurmak için bir çok araç bulunuyor. Biz **Remmina** isimli aracı kullanarak VNC bağlantısı kurmayı deneyelim.

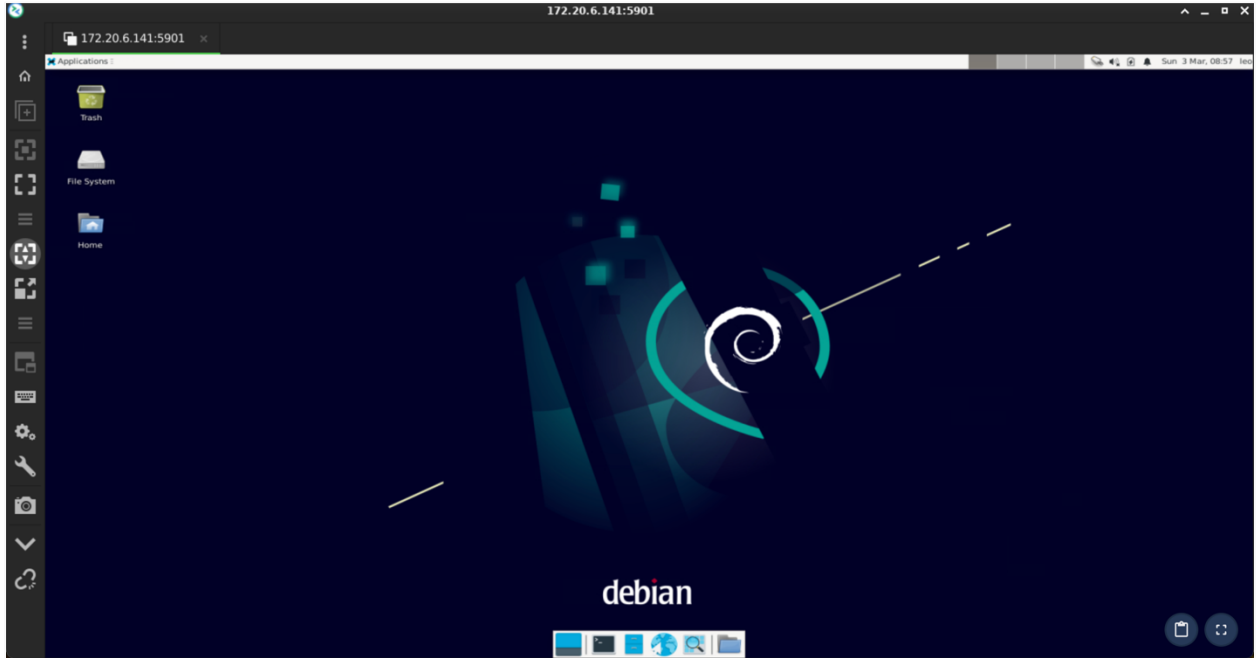
HackerBox'ta uygulamalar içerisinde **Remmina** aracını bulup çalıştırabilirsiniz.



Remmina aracını açtıktan sonra yukarıdaki görselde de görüldüğü üzere **VNC** protokolünü seçip hedef makinenin **IP** adresini ve **port** numarasını yazalım.

Ardından **enter** tuşuna basarak bağlanmayı deneyelim.

Evet, VNC ile bağlanmayı başardık. Hedef makinede çalışan VNC servisi güvensiz bir şekilde konfigüre edilmiş ve parolasız bir şekilde doğrudan bağlantı kurulabiliyor. Artık hedef makineye doğrudan erişim kazanmış durumdayız.

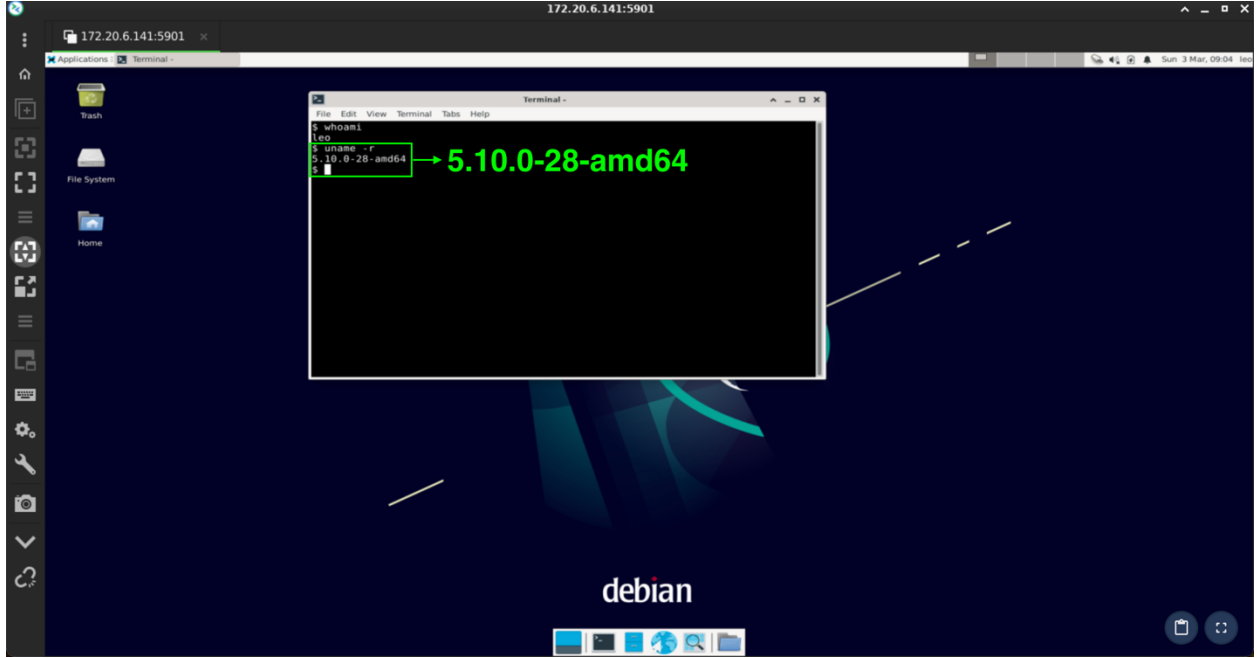


Görevde istenen bilgiye ulaşmak için terminali açıp **whoami** komutunu çalıştırabiliriz.



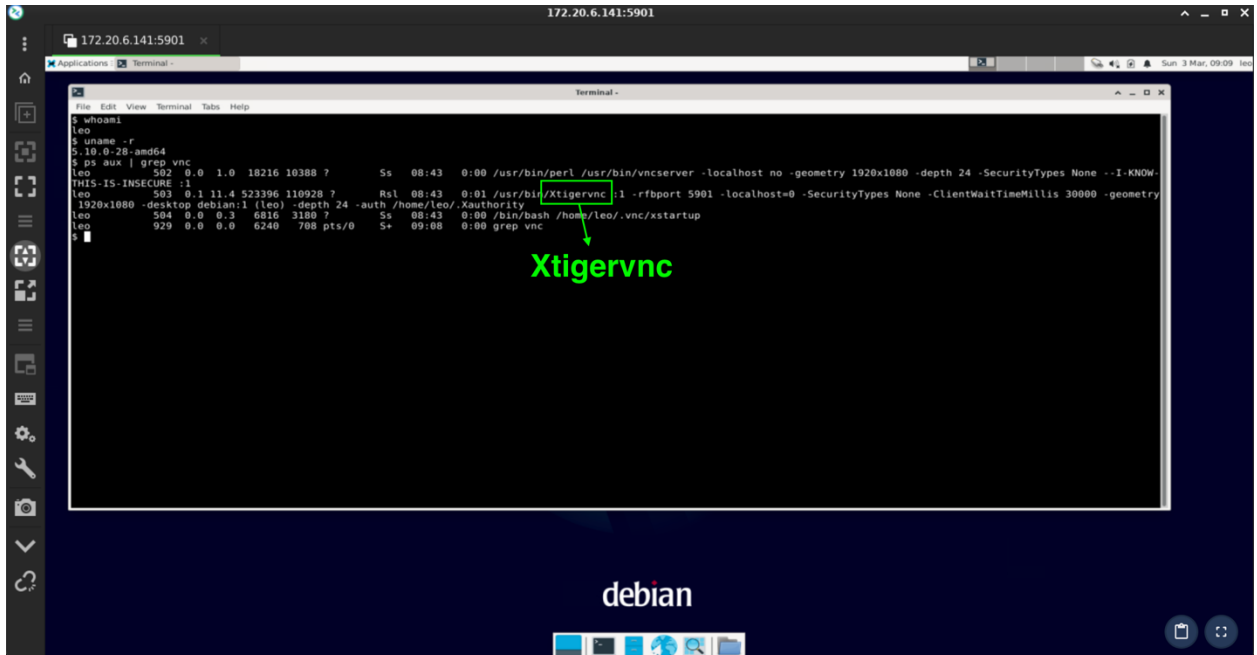
Görev 4

Görevde istenen Linux kernel versiyonunu öğrenmek için `uname -r` komutunu çalıştıralım.



Görev 5


Çalışan VNC yazılımını öğrenmek için öncelikle aktif processleri listeleyip, bu processler içinde bir arama yapabiliriz. Bunun için `ps aux | grep vnc` komutu çalıştıralım.



Görev 6

23 Şubat 2023 tarihinde VNC bağlantısı kuran bilgisayarın IP adresini tespit etmek için dosyalar arasında biraz gezerek **log** dosyalarını arayalım.

Dosyalar arasında biraz gezindikten sonra **/home/leo/.vnc** dizininde **connections.log.backup** isimli, dikkat çeken bir dosya bulduk.



```
drwxr-xr-x 5 leo leo 4096 Mar 3 08:43 .config
drwxr-xr-x 3 leo leo 4096 Mar 3 08:43 .dbus
drwxr-xr-x 2 leo leo 4096 Mar 1 07:52 Desktop
drwxr-xr-x 2 leo leo 4096 Mar 1 07:52 Documents
drwxr-xr-x 2 leo leo 4096 Mar 1 07:52 Downloads
drwxr-xr-x 3 leo leo 4096 Mar 3 08:43 .gnupg
-rw-r--r-- 1 leo leo 314 Mar 3 08:43 .ICEauthority
drwxr-xr-x 3 leo leo 4096 Mar 3 08:43 local
drwxr-xr-x 2 leo leo 4096 Mar 1 07:52 Music
drwxr-xr-x 2 leo leo 4096 Mar 1 07:52 Pictures
-rw-r--r-- 1 leo leo 887 Mar 1 07:51 .profile
drwxr-xr-x 2 leo leo 4096 Mar 1 07:52 Public
drwxr-xr-x 2 leo leo 4096 Mar 1 07:52 Templates
drwxr-xr-x 2 leo leo 4096 Mar 1 07:52 Videos
drwxr-xr-x 2 leo leo 4096 Mar 3 08:43 .vnc
-rw-r--r-- 1 leo leo 202 Mar 3 08:43 .Xauthority
$ cd .vnc
$ ls
connections.log.backup  debian:5901.log  debian:5901.pid  passwd  xstartup
$ ls -la
total 56
drwxr-xr-x 2 leo leo 4096 Mar 3 08:43 .
drwxr-xr-x 16 leo leo 4096 Mar 3 08:43 ..
-rw-r--r-- 1 leo leo 247 Mar 1 08:59 connections.log.backup
-rw-r--r-- 1 leo leo 31101 Mar 3 09:08 debian:5901.log
-rw-r--r-- 1 leo leo 4 Mar 3 08:43 debian:5901.pid
-rw-r--r-- 1 leo leo 8 Mar 1 08:04 passwd
-rwxr-xr-x 1 leo leo 78 Mar 1 08:18 xstartup
$ pwd
/home/leo/.vnc
$ cat connections.log.backup
Thu Feb 23 08:35:42 2023
Connections: accepted: 10.1.9.23:42391
SConnection: Client needs protocol version 3.8
SConnection: Client requests security type None(1)
VNCConnSf: Server default pixel format depth 24 (32bpp) little-endian rgb888
```

👉 Makineye VNC bağlantısı kuran IP adresini tespit ettik.

-

Tebrikler 🎉

✨ Bu alıştırmadaki tüm görevleri başarıyla tamamladınız.