

TIGER ISINMASI

INFO: Virtual Network Computing (VNC), kullanıcıların bir bilgisayara uzaktan bağlanıp kontrol etmesine olanak tanıyan bir protokoldür. VNC ile ilgili temel alıştırmalar yapmak için önerilir.

1. VNC'nin açılımı nedir?

Bilgi: VNC'nin açılımı 'Virtual Network Computing'dir. VNC, uzaktaki bir bilgisayarın masaüstünü görüntüleyip kontrol etmenize olanak tanıyan bir grafiksel masaüstü paylaşım protokolüdür. VNC, genellikle TCP 5900 portunu kullanarak çalışır ve platformlar arası uzak masaüstü erişimi sağlar.

2. Hangi port(lar) açık?

Bilgi: nmap ile port taraması yapılır.

Kullanımı:

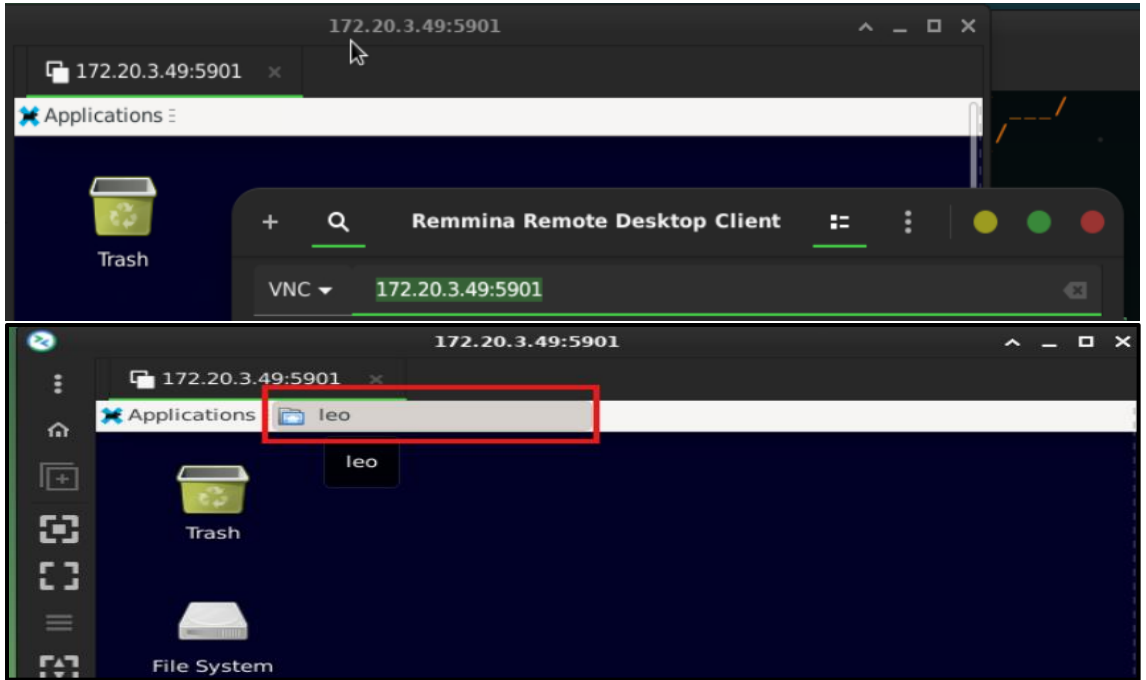
```
[*]-[root@hackerbox]-[~]
#nmap -p- 172.20.3.49
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-01 14:25 CDT
Nmap scan report for 172.20.3.49
Host is up (0.00020s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
5901/tcp  open  vnc-1
MAC Address: 52:54:00:B3:0C:66 (QEMU virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 15.49 seconds
```

Görüldüğü üzere 5901 portu açıktır.

3. VNC bağlantısı kurduğunuz kullanıcı kimdir?

Bilgi: Remina ile VNC bağlantısı kurulabilir.

Kullanımı: hacker-box'un içindeki remina'ya giriş yapılır ve bağlanılır. Ardından kullanıcıya erişilir.



Görüldüğü üzere kullanıcı "leo"dur.

4. *Linux kernel versiyonu nedir?*

Bilgi: Komut satırından versiyon bilgisi öğrenilebilir.

Kullanımı: Terminal ekranı açılır uname ile sistem öğrenilir ve uname -r parametresi ile de versiyon bilgisine ulaşılır.

```
Applications -> Terminal -
Terminal -
File Edit View Terminal Tabs Help
$ uname
Linux
$ uname -r
5.10.0-28-amd64
$
```

Görüldüğü üzere kernel versiyonu 10.0'dır.

5. *Çalışan VNC yazılımının adı nedir?*

Bilgi: ps aux, Linux ve Unix tabanlı sistemlerde çalışan tüm işlemleri (process) listelemek için kullanılan bir komuttur.

grep vnc: Çıktıda "vnc" kelimesini içeren satırları filtreler ve gösterir.

Kullanımı: ps aux | grep vnc

```
Applications -> leo
Terminal -
File Edit View Terminal Tabs Help
leo 731 0.0 2.3 341296 22912 ? Ss 15:24 0:00 /usr/lib/x86_
leo 732 0.1 3.1 267744 30288 ? Ss 15:24 0:01 /usr/lib/x86_
leo 733 0.0 2.8 196564 27420 ? Ss 15:24 0:00 /usr/lib/x86_
leo 734 0.0 3.5 240176 34412 ? Ss 15:24 0:00 /usr/lib/x86_
leo 749 0.0 2.6 195212 25644 ? Ss 15:24 0:00 /usr/lib/x86_
leo 776 0.0 1.2 348936 11964 ? Ss 15:24 0:00 /usr/libexec/
leo 784 0.0 0.7 384680 7732 ? Ss 15:24 0:00 /usr/libexec/
leo 791 0.0 0.6 159392 5944 ? Ss 15:24 0:00 /usr/libexec/
leo 893 0.2 4.0 461624 39312 ? Ss 15:35 0:00 xfce4-termia
leo 897 0.0 0.0 2480 508 pts/0 Ss+ 15:35 0:00 sh
leo 926 0.0 0.0 2480 512 pts/1 Ss 15:37 0:00 sh
leo 929 0.0 0.3 9756 3340 pts/1 R+ 15:37 0:00 ps aux
$ ps aux | grep vnc
leo 501 0.0 1.0 18288 10364 ? Ss 15:24 0:00 /usr/bin/perl /usr/bin/vncser
ver -localhost no -geometry 1920x1080 -depth 24 -SecurityTypes None --I-KNOW-THIS-IS-INSECURE :1
leo 502 0.9 12.4 536780 120848 ? Ssl 15:24 0:07 /usr/bin/Xtigervnc :1 -rfbpor
t 5901 -localhost=0 -SecurityTypes None -ClientWaitTimeMillis 30000 -geometry 1920x1080 -desktop
debian:1 (leo) -depth 24 -auth /home/leo/.Xauthority
leo 503 0.0 0.3 6816 3212 ? Ss 15:24 0:00 /bin/bash /home/leo/.vnc/xsta
rtup
leo 931 0.0 0.0 6240 636 pts/1 S+ 15:37 0:00 grep vnc
$
```

Görüldüğü üzere yazılımın adı "Xtigervnc"dir.

6. *23 Şubat 2023 tarihinde VNC bağlantısı kuran bilgisayarın IP adresi nedir?*

Bilgi: ls -la komutu, Linux ve Unix tabanlı sistemlerde dosya ve dizinlerin listesini görüntülemek için kullanılır.

- -l: Uzun formatta listeleme yapar. Bu, dosya/dizin izinlerini, sahiplerini, dosya boyutlarını ve son değiştirilme tarihini içerir.
- -a: Gizli dosyalar dahil tüm dosyaları gösterir. Gizli dosyalar, isimlerinin başında nokta (.) ile başlayan dosyalardır.

Kullanımı: ls -la ile dosya ve dizinlere erişilir. Erişilen dizinlerde bağlantı back-up dosyası bulunur ve dosyanın içeriği cat komutu ile okunur.

```
Applications: leo Terminal -
Terminal -
File Edit View Terminal Tabs Help
sh: 9: connections.log.backup: not found
$ ls -la
total 56
drwxr-xr-x  2 leo leo  4096 Sep  1 15:24 .
drwxr-xr-x 16 leo leo  4096 Sep  1 15:24 ..
-rw-r--r--  1 leo leo   247 Mar  1 2024 connections.log.backup
-rw-r--r--  1 leo leo 31397 Sep  1 15:29 debian:5901.log
-rw-r--r--  1 leo leo    4 Sep  1 15:24 debian:5901.pid
-rw-----  1 leo leo    8 Mar  1 2024 passwd
-rwxr-xr-x  1 leo leo    78 Mar  1 2024 xstartup
$ pwd
/home/leo/.vnc
$ cat /home^C
$ cat /home/leo/.vnc
cat: /home/leo/.vnc: Is a directory
$ 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)
VNCSTConnST: Server default pixel format depth 24 (32bpp) little-endian rgb888
$
```

Görüldüğü üzere ip adresi: 10.1.9.23'tür.

-ISINMA TAMAMLANDI-

Tebrikler

SweepingSpeedball56 Hackviser'ın Tiger ısınmasını başarıyla tamamladı