

Forum: [Hack Forums](#)

Thread: [VNC Exploitation / Pentest Approach](#)

Money- - November 7, 2021, 3:29 am

I just wana ask you guys, what are your approach when it comes to VNC ports? Example , port 5800 and 5900 and so on.

I usually try for default creds and brute force with a small vnc default word lists. That's about it. Don't really dig much into it.

Money- - November 30, 2021, 3:55 am

Anyone have specific and interesting approach here?

Dolla\$ - December 7, 2021, 6:56 am

(Nov 30, 2021 04:55 AM)Money- Wrote: [\[CITE\]](#) Anyone have specific and interesting approach here? I don't know if this will help you, but here is my approach I use to work a bit on the topic for a company.

This is what I've done for my audit:

1) What do you target? A company.

2) How do they integrate their VNC servers on their devices?

- Manual Install ?

- Using Integration servers with Pre-packaged software, in my use case they used script. Scripts may still be on the computer in the /Temp/ repository. You'll be surprised toto the see the amount of sensitive information you could find.

--> First, you need to identify the VNC server used

Usually if the VNC port 5900/5800 is open. You can type on your Web Browser the target address:

<https://127.0.0.1:5900>

It should disclose the version of the VNC server.

I was able to find a miss configuration in the integration scripts which allowed me to connect remotely to a generically session without the user knowing.

--> Check for default credentials/bruteforcing

--> If you want to train :

--> Check the vulnerabilities associated with the VNC server used:

<https://www.cvedetails.com/cve/CVE-2021-42785/>, for instance on tightvnc (23 November) --> Write your own exploit or find them on the web.

Hope I helped, xx

Money- - December 9, 2021, 3:07 am

(Dec 7, 2021 07:56 AM)Dolla \$ign Wrote: [\[CITE\]](#) I don't know if this will help you, but here is my approach I use to work a bit on the topic for a company.

This is what I've done for my audit:

1) What do you target? A company.

2) How do they integrate their VNC servers on their devices?

- Manual Install ?

- Using Integration servers with Pre-packaged software, in my use case they used script. Scripts may still be on the computer in the /Temp/ repository. You'll be surprised to see the amount of sensitive information you could find.

--> First, you need to identify the VNC server used

Usually if the VNC port 5900/5800 is open. You can type on your Web Browser the target address:

<https://127.0.0.1:5900>

It should disclose the version of the VNC server.

I was able to find a miss configuration in the integration scripts which allowed me to connect remotely to a generic session without the user knowing.

--> Check for default credentials/bruteforcing

--> If you want to train :

--> Check the vulnerabilities associated with the VNC server used:

<https://www.cvedetails.com/cve/CVE-2021-42785/>, for instance on tightvnc (23 November) --> Write your own exploit or find them on the web.

Hope I helped, xx

Thanks for the info , most of the time when I browse the webpage it doesn't disclose any information and gives error or a blank page from my pentest experience anyways.

I usually will just nmap it for the version instead. So far default credentials seem to work but meh.

ice_c00l - January 19, 2022, 5:22 am

There are a few nmap scripts to query the version, look on official nmap site for the NSE you want.

```
nmap -p 5901 --script vnc-info ipaddress
```

From here check exploit dB for a way in.

On one of my pen tests I found the vnc password hash in the config file in program files on a windows box. Vncpwd.exe cracked it in less than 2 secs. This password was also used for local admin. Always worth having a look around on the system that winpeas / seatbelt missed.

Money- - February 2, 2022, 3:46 am

(Jan 19, 2022 06:22 AM)ice_c00l Wrote: [\[CITE\]](#) There are a few nmap scripts to query the version, look on official nmap site for the NSE you want.

```
nmap -p 5901 --script vnc-info ipaddress
```

From here check exploit dB for a way in.

On one of my pen tests I found the vnc password hash in the config file in program files on a windows box. Vncpwd.exe cracked it in less than 2 secs. This password was also used for local admin. Always worth having a look around on the system that winpeas / seatbelt missed.

Yea I am using that, usually there isn't much stuff on my end though. When it comes to the version. Though I did find some default credentials for VNC before which is interesting.

If you got anymore info about VNCs , let me know. Thanks!

Stanley - *September 13, 2022, 7:23 am*

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley