VNC Authentication a11y.text VNC Authentication Metasploit Auxiliary Module â€“ VNC None Scanner | Metasploit unleashed VNC Authentication Check withÂ the None Scanner a11y.text VNC Authentication Check withÂ the None Scanner The VNC Authentication None ScannerÂ is an Auxiliary Module for Metasploit. This tool will search a range of IP addresses looking for targets that are running a VNC Server without a password configured . Pretty well every administrator worth his/her salt sets a password prior to allowing inbound connections but you never know when you might catch a lucky break and a successful pen-test leaves no stone unturned. In fact, once when doing a pentest, we came across a system on the target network with an open VNC installation . While we were documenting our findings, I noticed some activity on the system. It turns out, someone else had found the system as well! An unauthorized user was live and active on the same system at the same time. After engaging in some social engineering with the intruder, we were informed by the user they had just got into the system, and came across it as they were scanning large chunks of IP addresses looking for open systems. This just drives home the fact that intruders are in fact actively looking for this low hanging fruit, so you ignore it at your own risk. To use the VNC Scanner, we first select the auxiliary module , define our options, then let it run.

```
msf auxiliary(vnc_none_auth) > use auxiliary/scanner/vnc/vnc_none_auth
msf auxiliary(vnc_none_auth) > show options

Module options:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    5900             yes       The target port
   THREADS  1                yes       The number of concurrent threads
```

```
msf auxiliary(vnc_none_auth) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(vnc_none_auth) > set THREADS 50
THREADS => 50
msf auxiliary(vnc_none_auth) > run

[*] 192.168.1.121:5900, VNC server protocol version : RFB 003.008
[*] 192.168.1.121:5900, VNC server security types supported : None, free access!
[*] Auxiliary module execution completed Next WMAP Web Scanner Prev SMB Login Check
```