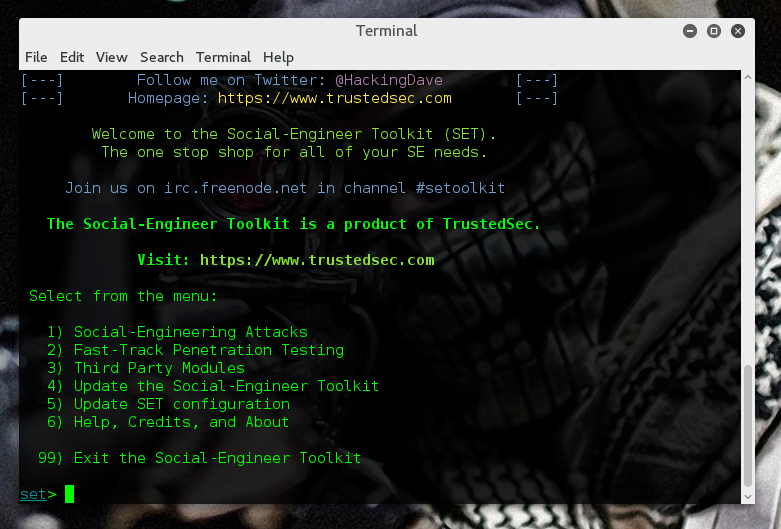
LAB 7 Phishing

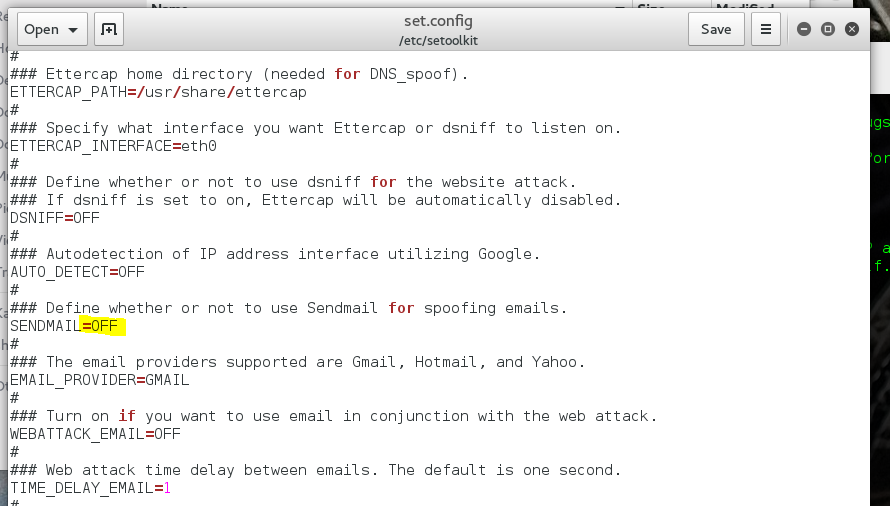
By

So in this lab were doing a very common attack used today. We are going sent a rogue mail to open back door on user system.

First start “Social Engineering Toolkit”, famous and is shown in TV shows like “Mr. Robot”.

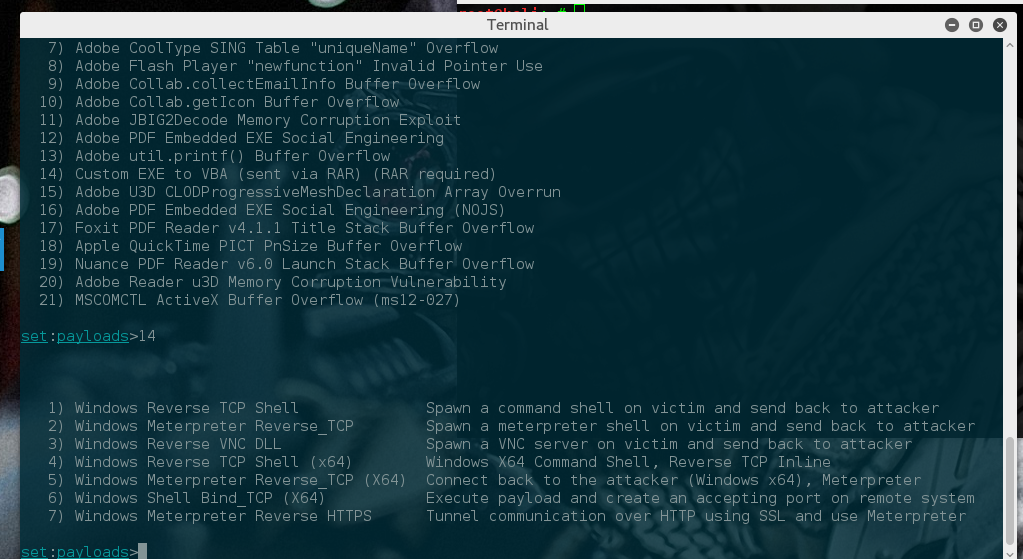


Then press 1), 1) and then 3) to create “Social-Engineering-Template”. If you don’t have “sendmail” installed install that first: “$apt-get install sendmail-bin” and then “$apt-get install sendmail”. Edit /etc/settoolkit/set.config.

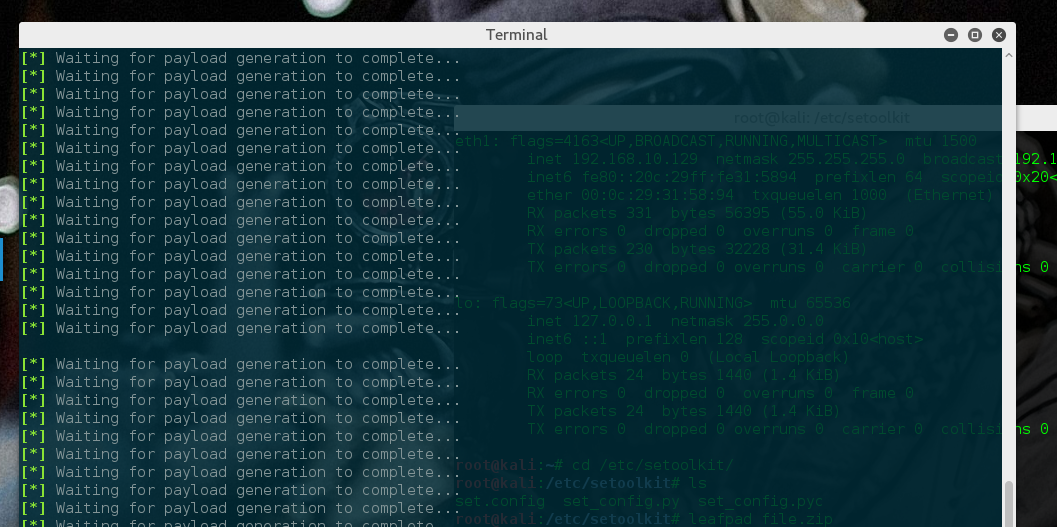


Change SENDMAIL=OFF TO SENDMAIL=ON. You can change email provider and apache directory if you need to. Leave it at default if you don’t know.

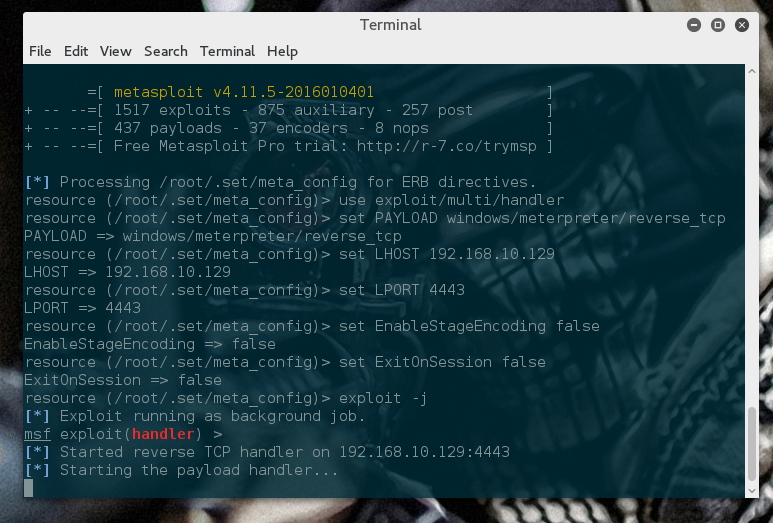
After creating template (end editing by pressing ctrl+c) then press 2 for “Create a FileFormat Payload”. Option 14 sounds nice but choose what you want. Then 7 for Reverse HTTPS but Reverse TCP Shell is good also.



In LHOST fill in local IP for shared network with victim. Of course if you are real hacker and doing this over the internet you would use a dynamic DNS from a service like noip.com. Whatever port you like. I use 4443 out of habit but just remember if you are doing this over the internet to forward/open port in your gateway router and use a bridge if you are using virtual machine. After just wait for payload generation to complete. I had to do more than once because it failed a couple of times.



Wait for it. Now you are ready to send. Go to 1), 1), 1), 1). Choose default or a custom payload. Then fill in info. 7) To import your own or 1 for default meterpreter. Then just go go go and when asked about template choose the one we created or take premade. Fill out random info and send from your gmail. I got warning from Avast so had to turn off antivirus also. Then go open mail and click link or open file, depending on what you chose and go back to meterpreter and wait for connection. If it doesn’t connect then you have wrong Nat settings.



All done.