10 Hacking Web Applications and Databases

Lab Scenario

Today, we have a Web Application Pen Test to perform. You have been given specific tasks to handle as one of the team members. You will need to be able to explain in detail the steps you take to perform the hacks. Please take detailed notes.

Lab Objectives

1. Gain an understanding of how to perform Input Manipulation.
2. Learn how to shovel a shell and understand the differences between a forward and reverse shell.
3. Perform both horizontal and vertical privilege escalation and understand the capabilities inherent in this type of attack.
4. See the use of Cross Site Scripting and be able to perform that test on a regular basis.
5. Document every task you perform in such a way that a thorough report can be compiled.

Lab Details - Step-by-Step Instructions

10.1 Brute-Force Web Authentication with Hydra

During a Pen Test, you're likely to come across web login forms, similar to the one used in Damn Vulnerable Web Application (DVWA).

Login forms such as these are your gateway to a treasure trove of sensitive information, if you can get the creds! Before you attempt to use a wordlist or brute force, it's important to know a few valid usernames. You can find valid usernames using your information gathering skills. In this exercise, we'll use admin as the username.

Start up your Kali Linux and Metasploitable VM. Take note of the IP address assigned to Metasploitable. This exercise assumes the IP address of Metasploitable is 192.168.1.111. Your's may vary!

Open your browser (in Kali) and point it to <IP of Metasploitable>/dvwa/login.php

You are presented with a login page. In order to attack this page, you'll have to figure out what parameters are used, protocol (HTTP/HTTPS), and the invalid response format, at a minimum. Real world examples may also include session cookies, lockout thresholds and CAPTCHA requirements.

From the Kali Applications menu, launch BurpSuite to help gather the required fieldsnames and resource information, which will later be used in Hydra GTK.

Configure your browser to use a proxy on 127.0.0.1:8080

Select 'Preferences' from browser menu at top right of browser window

Click the Advanced tab.

Click the Network tab.

Click the Settings… button, to the right of Connection.

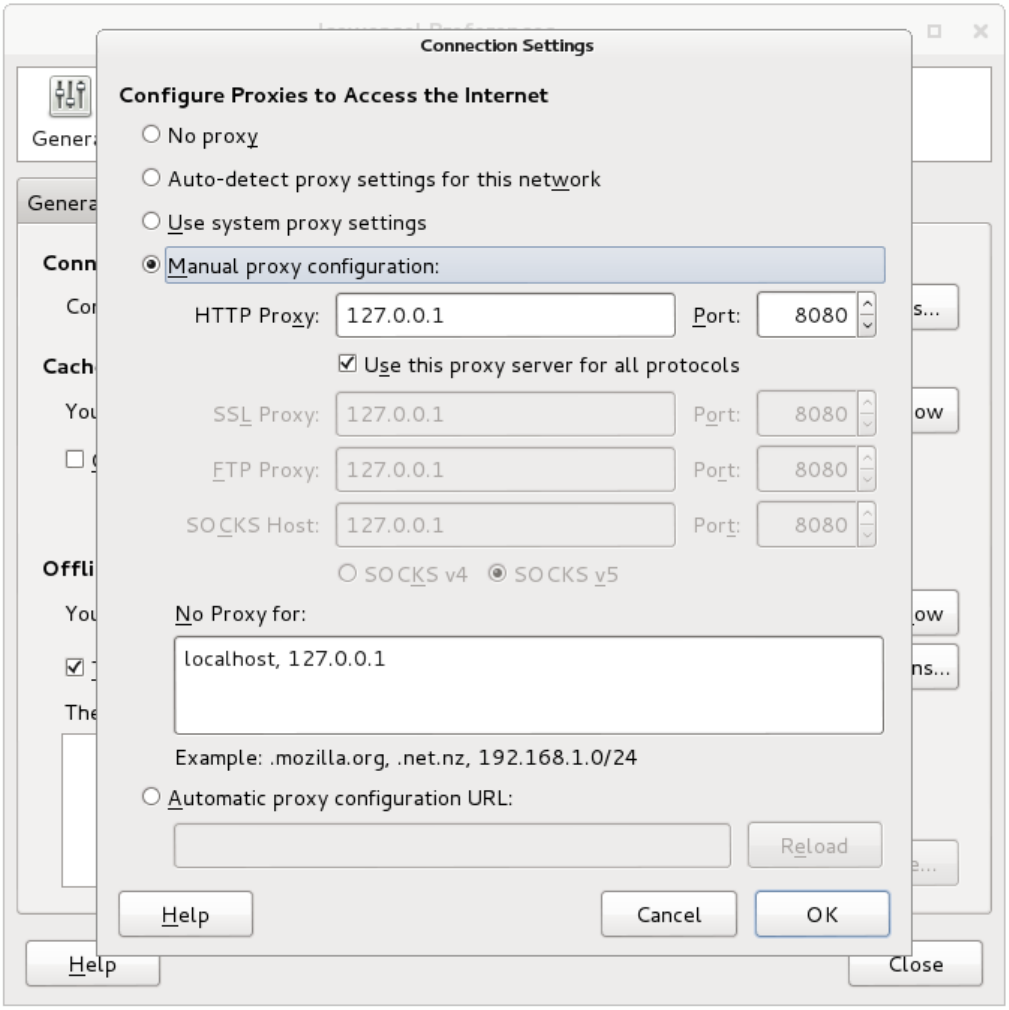
Select Manual proxy configuration:

HTTP Proxy: 127.0.0.1

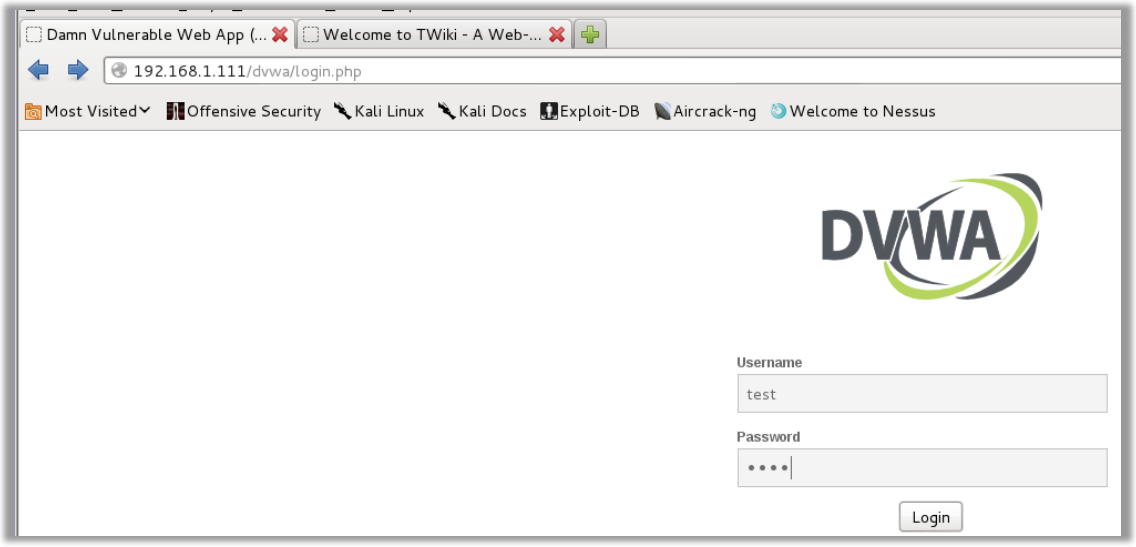
Port: 8080

Click OK.

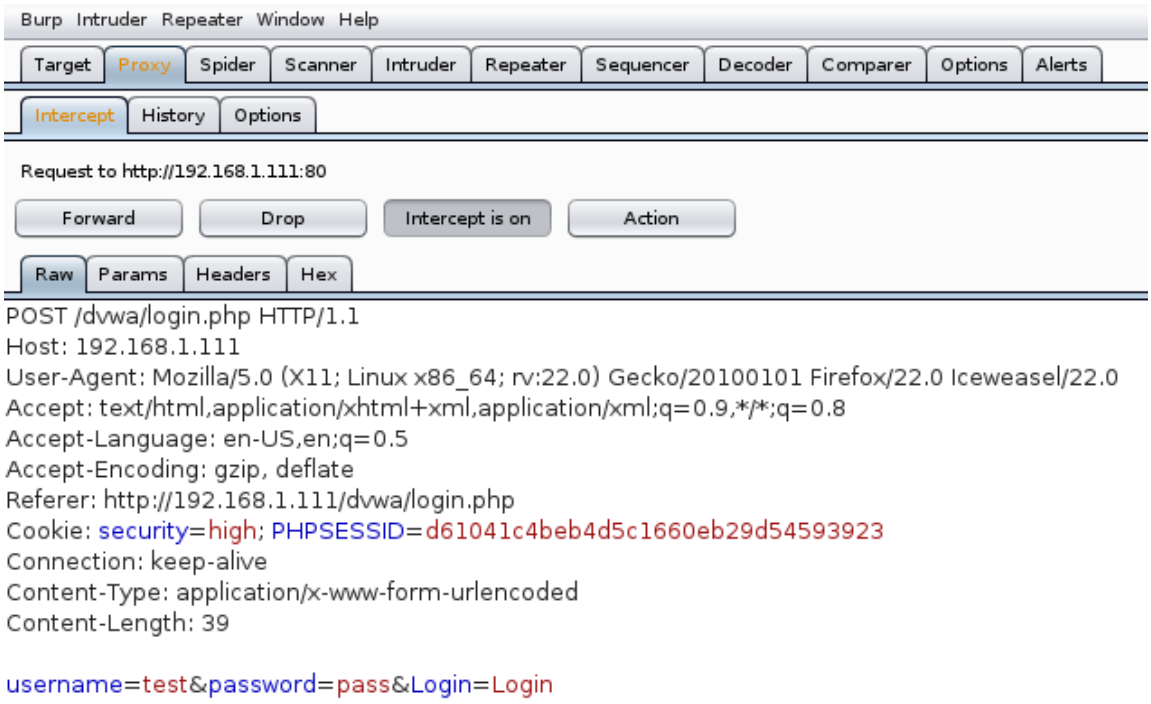
Click Close.



With BurpSuite running, attempt to log in to DVWA using the username “test” and the password “pass”.

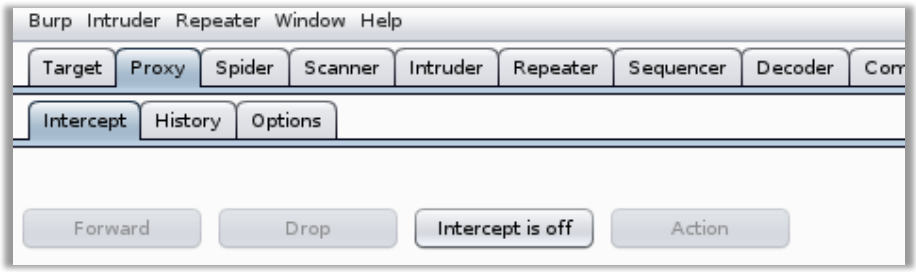


In BurpSuite, click the Proxy tab. You should see something similar to the example below.



BurpSuite is intercepting the POST request from your browser. You can review, modify, or forward the request before it is sent to the destination. Unlike an HTTP GET request which can be modified by simply changing the URL, an HTTP POST request sends the parameters as data which requires the use of a proxy (BurpSuite) or browser extension in order to modify the parameters.

Click the intercept button so that display indicates “Intercept is off”:

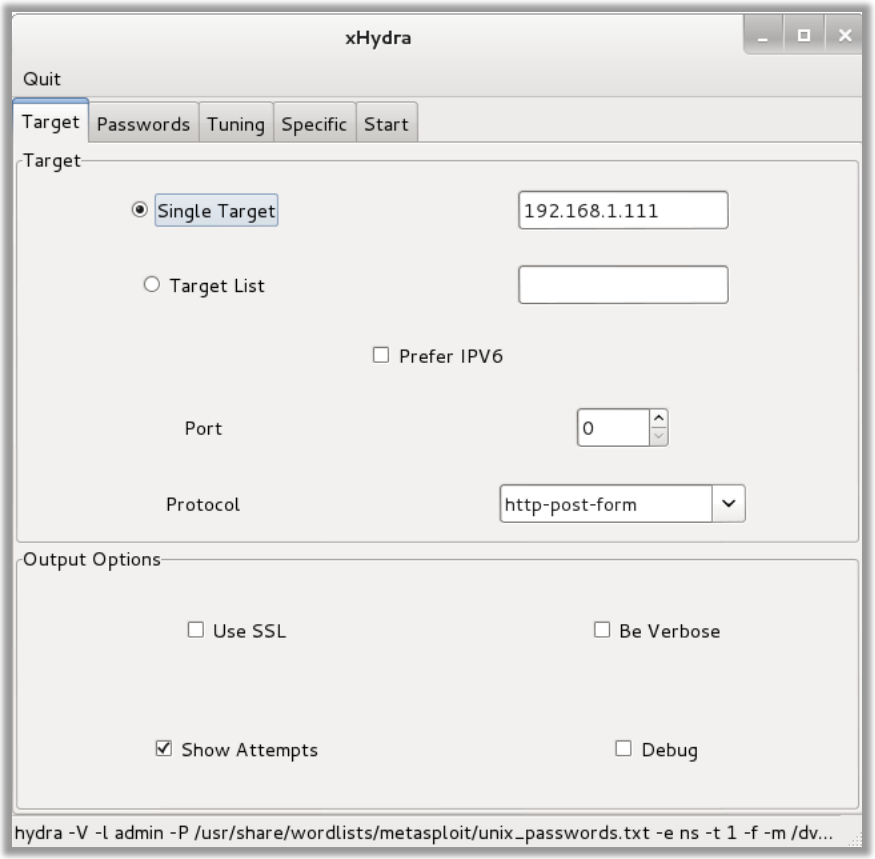


Open Hydra-gtk:
Applications > Kali Linux > Password Attacks > Online Attacks > Hydra-gtk

Use the following screenshots to help setup Hydra-gtk

From the Target tab:

Select Single Target, enter the IP Address of your Metasploitable VM.



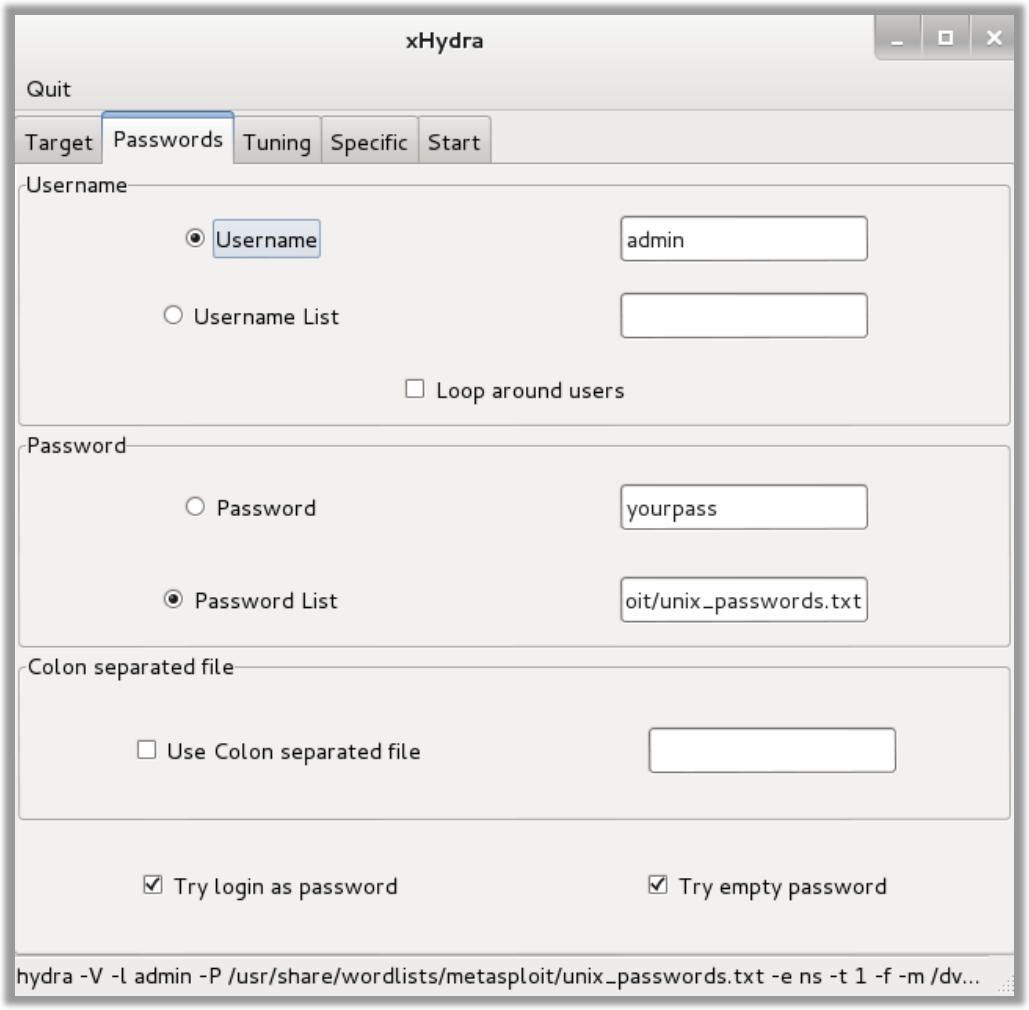
Select http-post-form from the Protocol drop-down list.

Check the box next to Show Attempts.

From the Paswords tab:

Select Username and enter admin as the username.

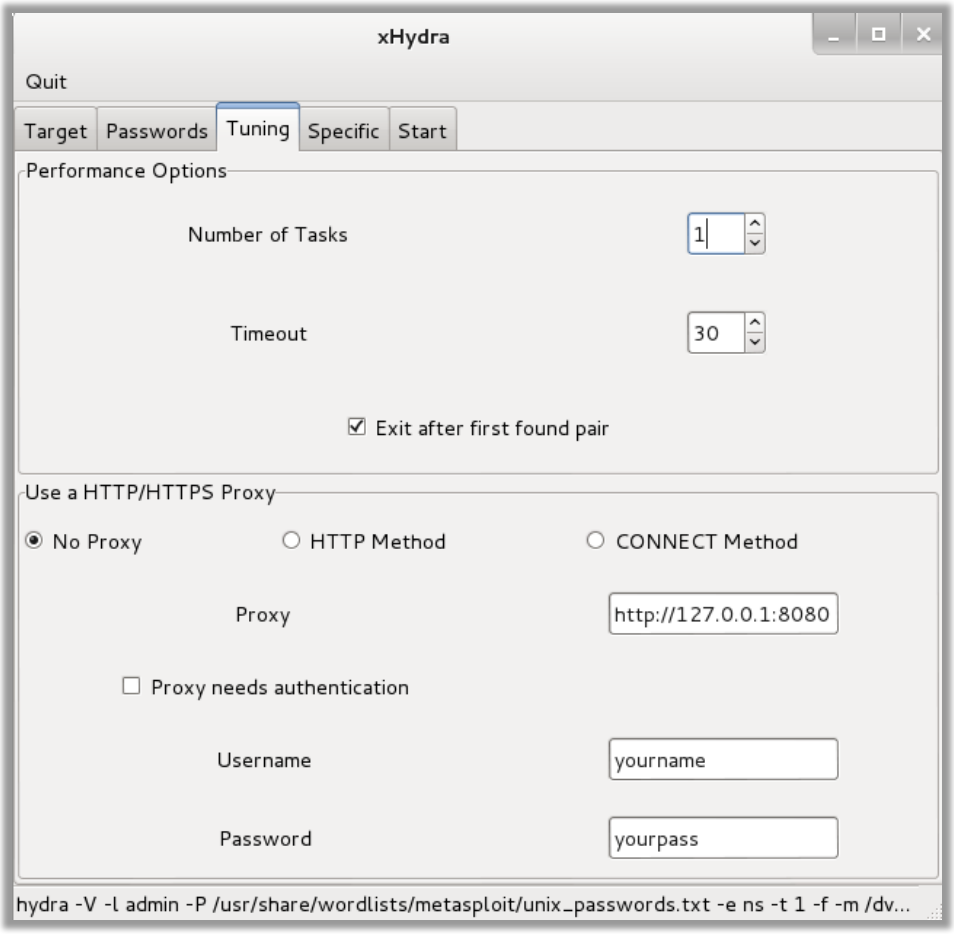
Select Password List, click in the entry box and in the browse window click on ‘File System’ on the left and then browse to /usr/share/wordlists/metasploit/unix_passwords.txt



From the Tuning tab:

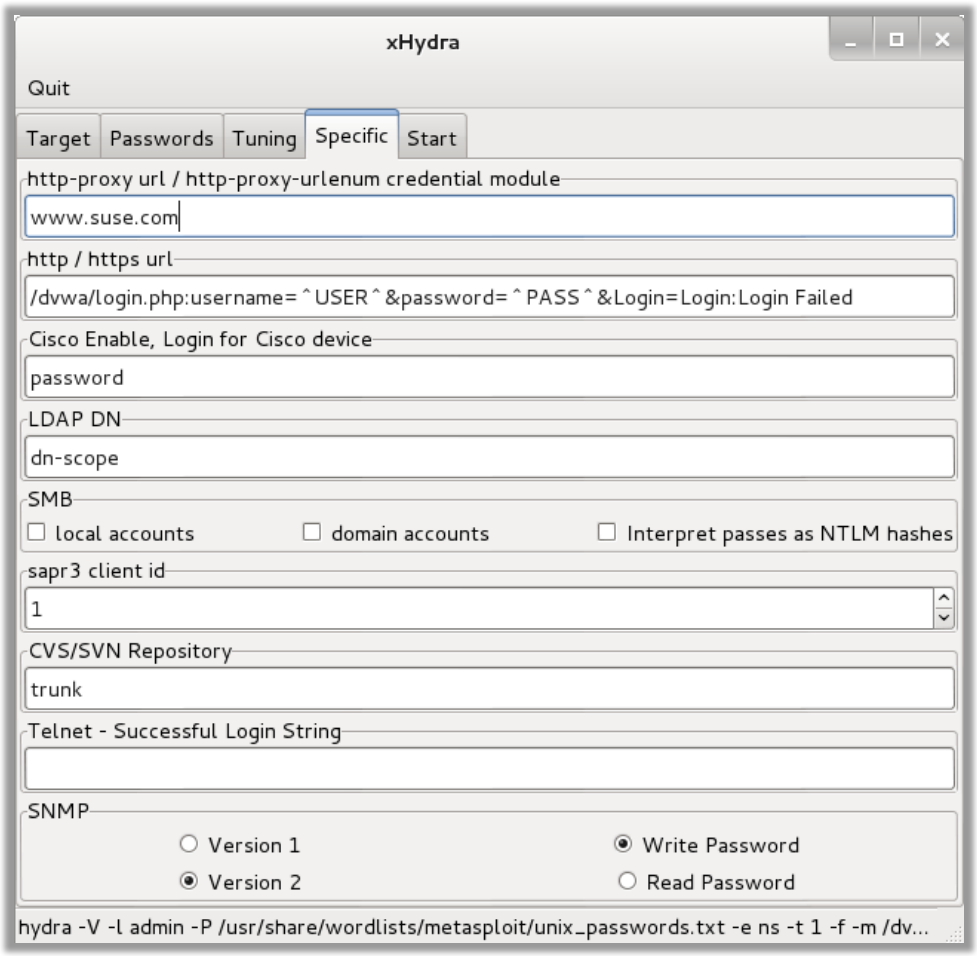
Change the Number of Tasks to 1.

Check the box next to Exit after first found pair.

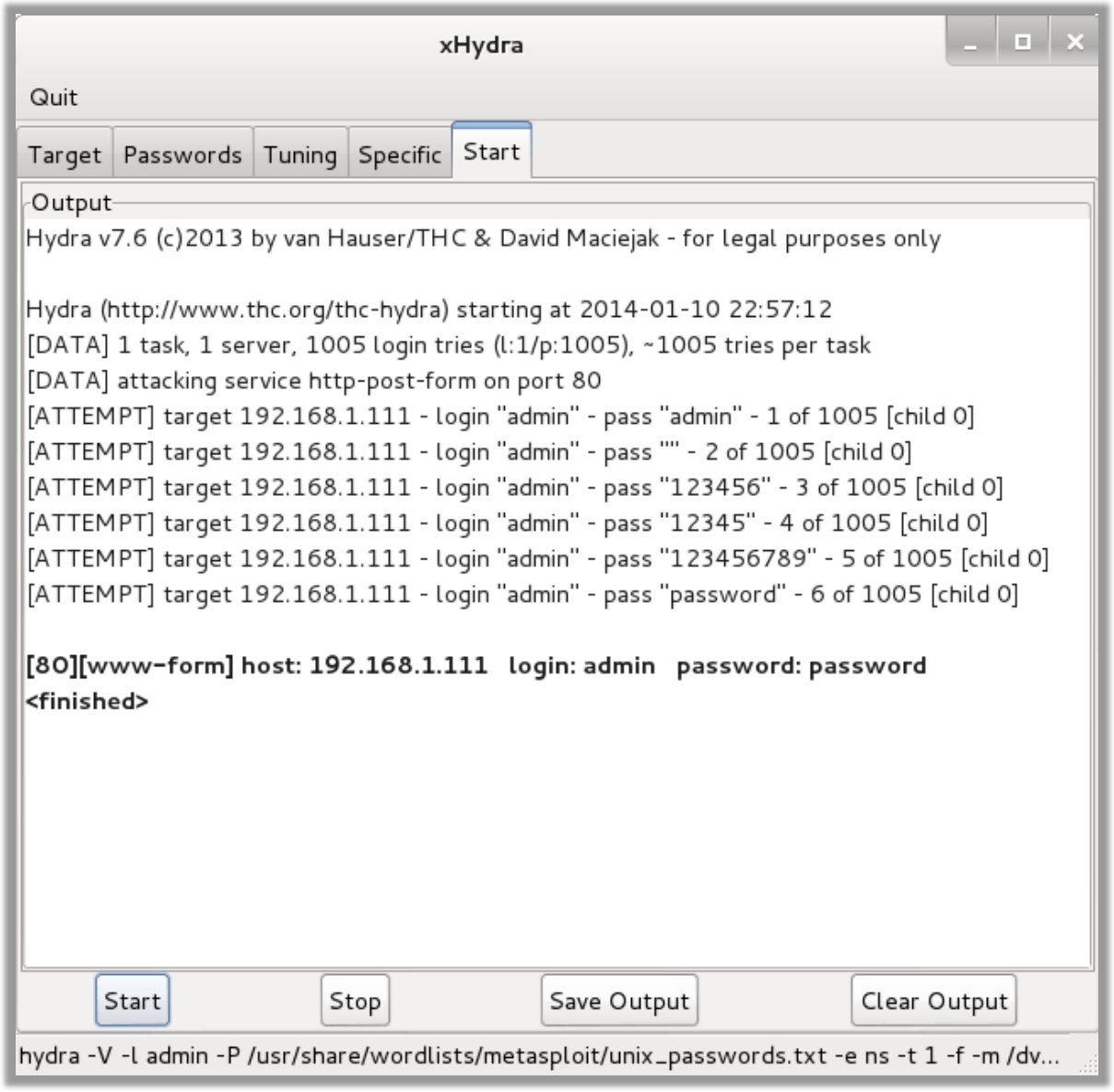


From the Specific tab:

Set the http / https url to:
/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login Failed



Click the Start tab, then click the Start button.

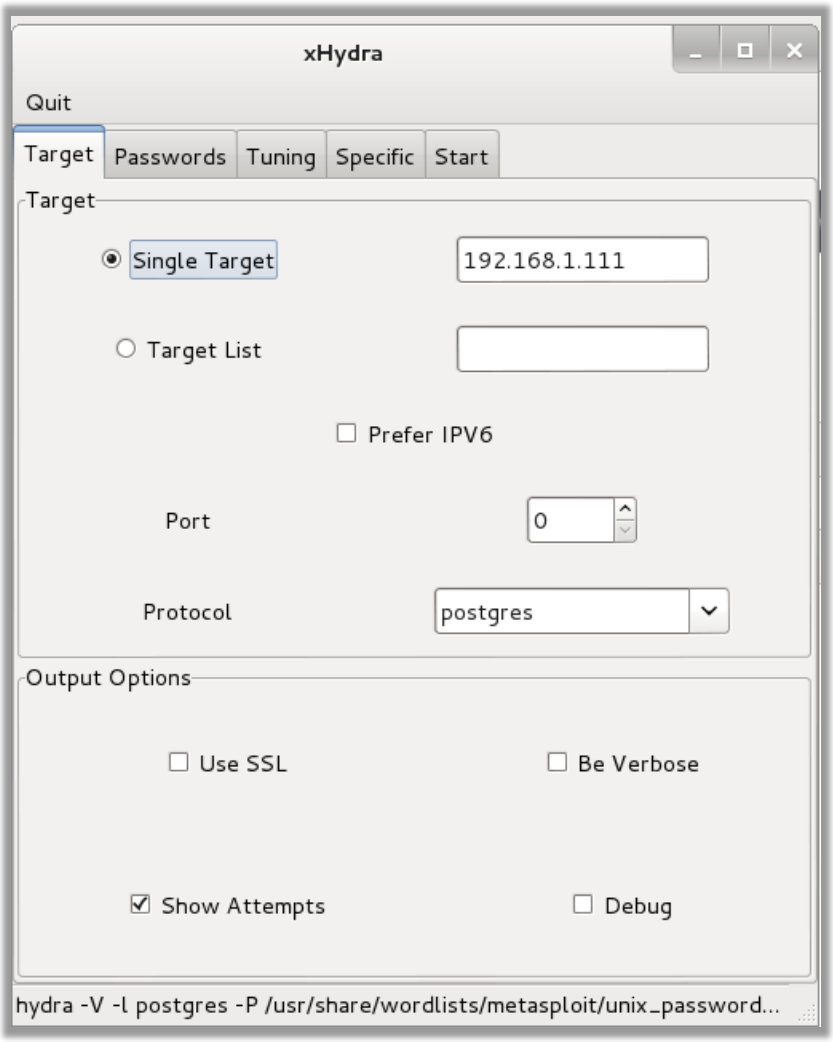


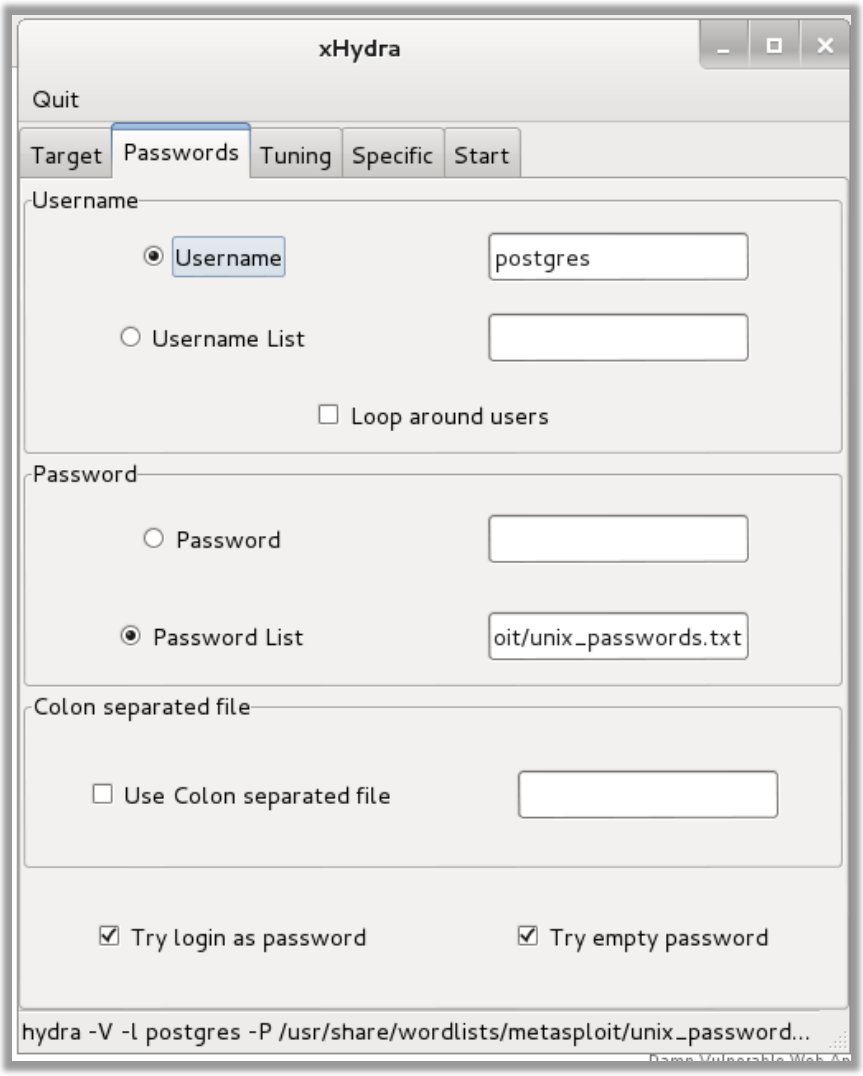
You should see a bolded log entry in the Output window. At this point, Hydra thinks it was successful. There are many variables which could cause false positives when brute forcing web applications. Use the newfound credentials in your web browser to verify the username and password. If something went wrong, double-check your settings or ask for help.

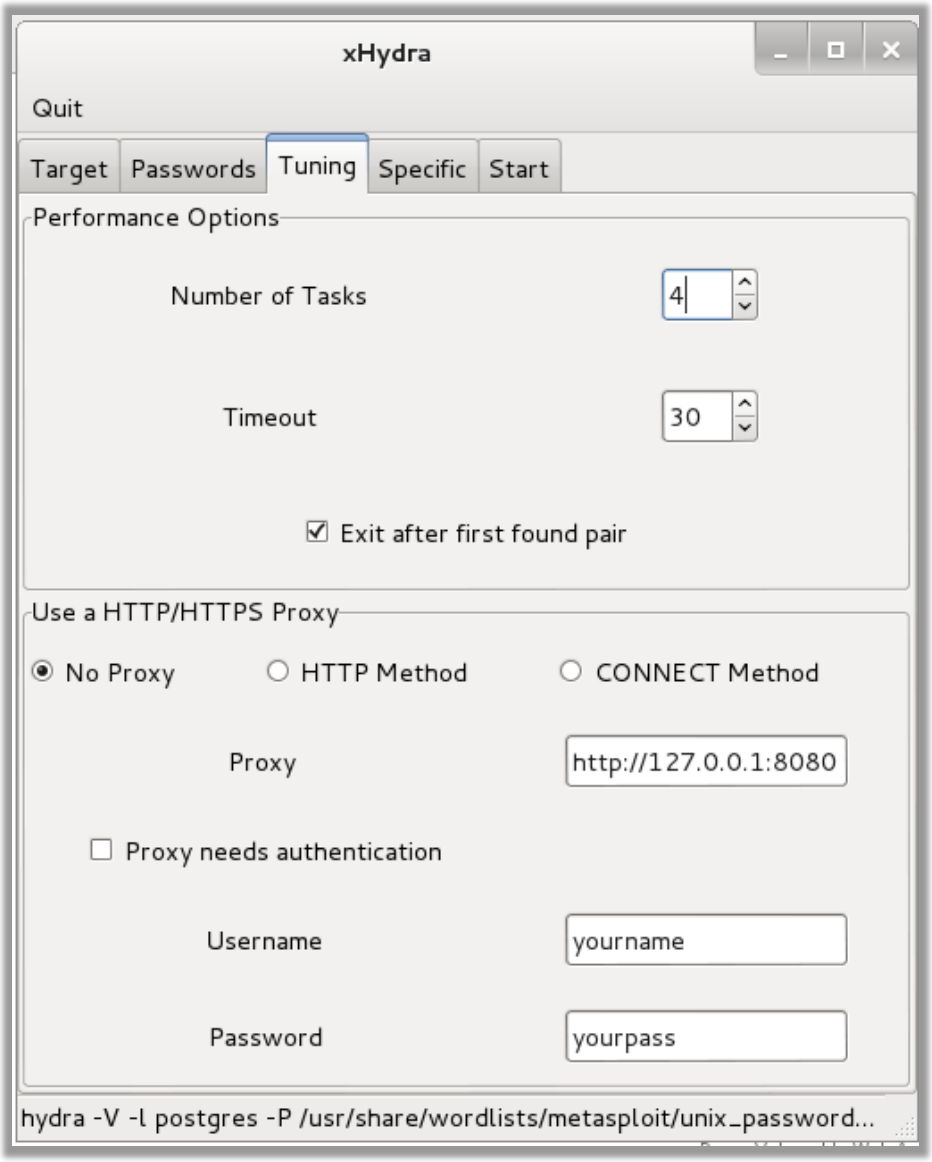
10.2 Brute-Force PostgreSQL with Hydra

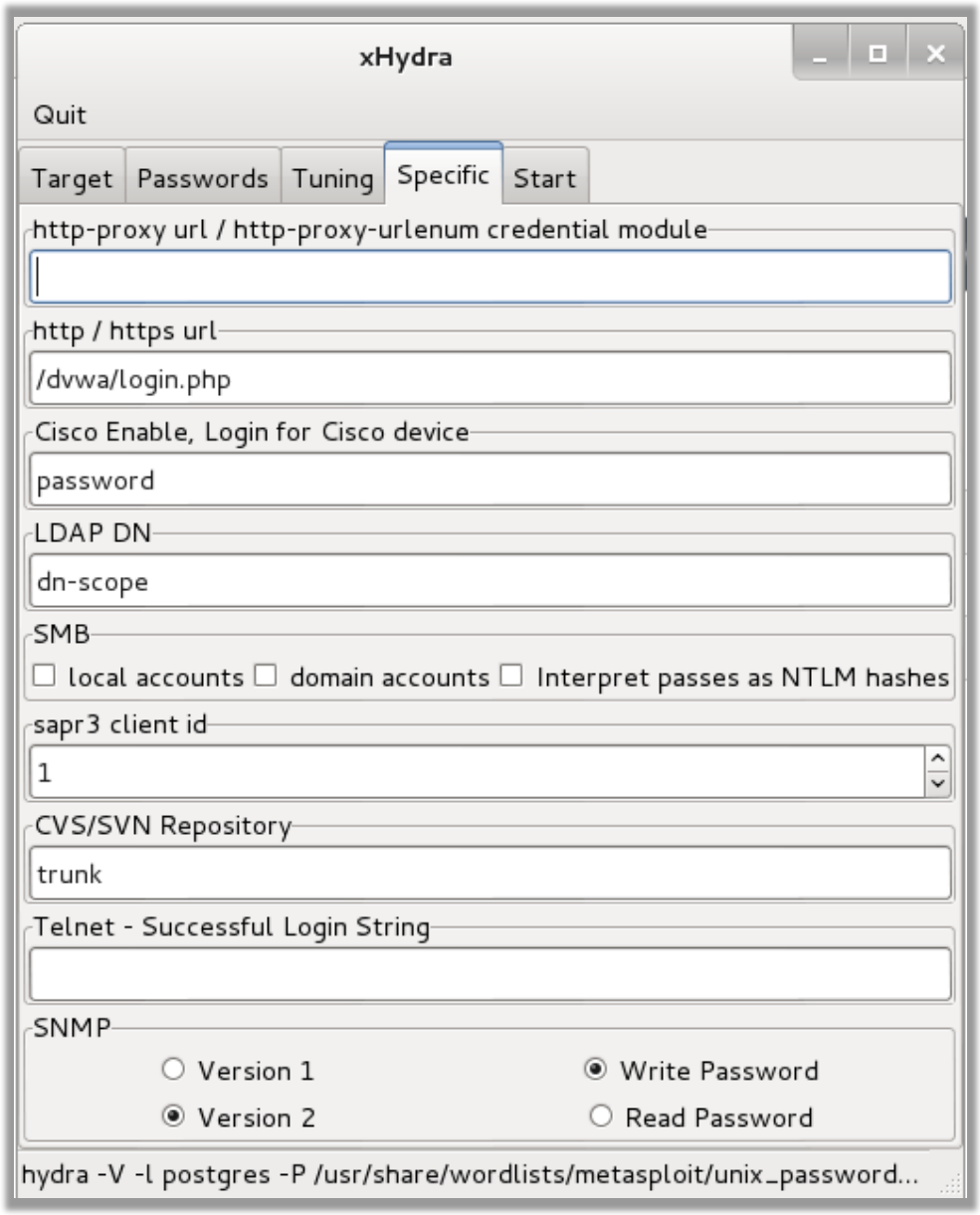
Finding an open database port is quite common during an internal Pen Test. In this exercise, we'll use Hydra to brute force PostgreSQL, running on your Metasploitable VM.

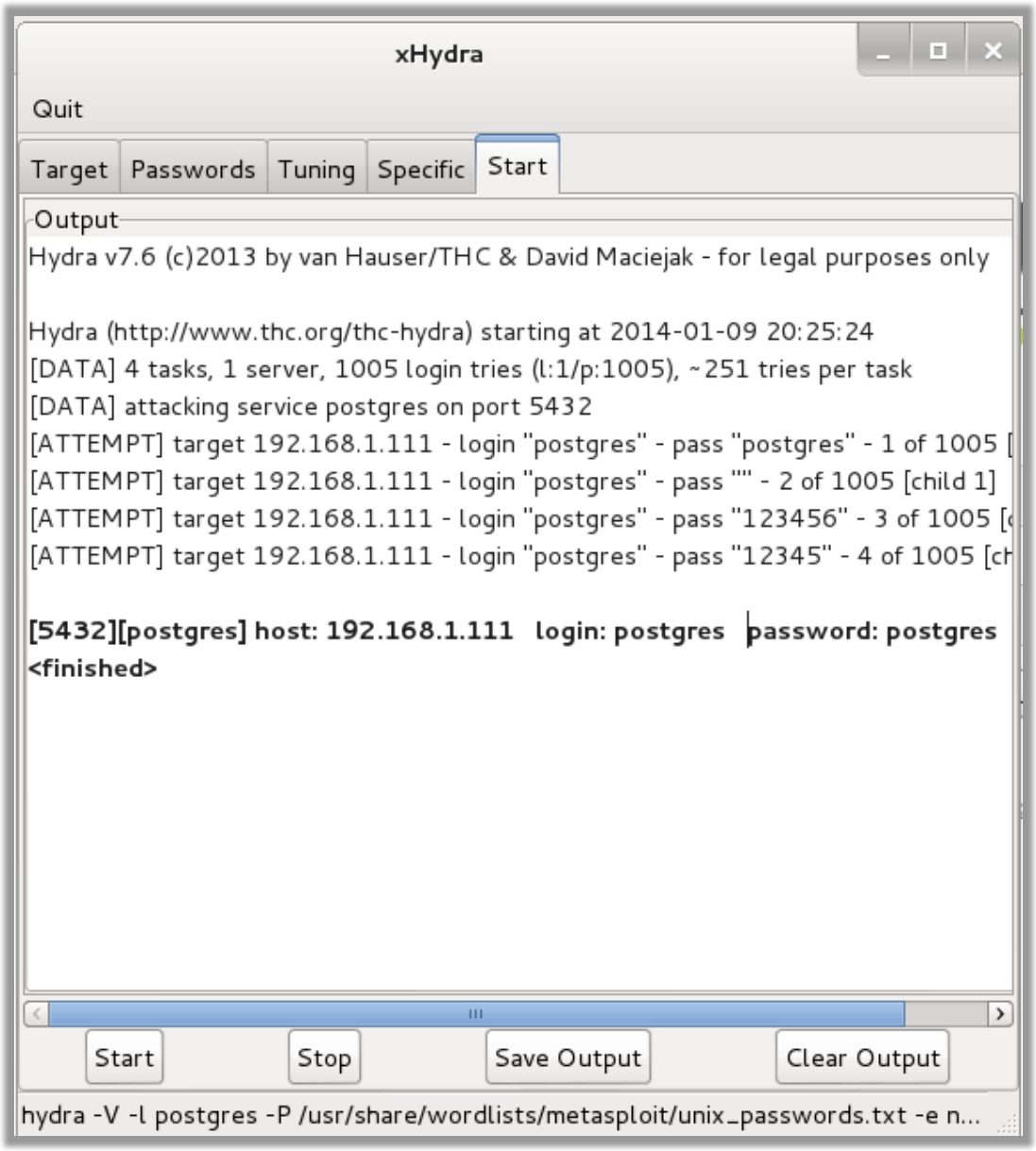
Since you're already familiar with Hydra, see if you can figure out the settings. If you need help, use the following screenshots as an example.




xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Username
Username
postgres
Username List
Loop around users
Password
Password
Password List
oit/unix_passwords.txt
Colon separated file
Use Colon separated file
Try login as password
Try empty password
hydra -V -l postgres -P /usr/share/wordlists/metasploit/unix_password...


xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Performance Options
Number of Tasks
4
Timeout
30
Exit after first found pair
Use a HTTP/HTTPS Proxy
No Proxy
HTTP Method
CONNECT Method
Proxy
http://127.0.0.1:8080
Proxy needs authentication
Username
yourname
Password
yourpass
hydra -V -l postgres -P /usr/share/wordlists/metasploit/unix_password...


xHydra
Quit
Target
Passwords
Tuning
Specific
Start
http-proxy url / http-proxy-urlenum credential module
http / https url
/dvwa/login.php
Cisco Enable, Login for Cisco device
password
LDAP DN
dn-scope
SMB
local accounts
domain accounts
Interpret passes as NTLM hashes
sapr3 client id
1
CVS/SVN Repository
trunk
Telnet - Successful Login String
SNMP
Version 1
Version 2
Write Password
Read Password
hydra -V -l postgres -P /usr/share/wordlists/metasploit/unix_password...


xHydra
Quit
Target
Passwords
Tuning
Specific
Start
Output
Hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only
Hydra (http://www.thc.org/thc-hydra) starting at 2014-01-09 20:25:24
[DATA] 4 tasks, 1 server, 1005 login tries (l:1/p:1005), ~251 tries per task
[DATA] attacking service postgres on port 5432
[ATTEMPT] target 192.168.1.111 - login "postgres" - pass "postgres" - 1 of 1005
[ATTEMPT] target 192.168.1.111 - login "postgres" - pass "" - 2 of 1005 [child 1]
[ATTEMPT] target 192.168.1.111 - login "postgres" - pass "123456" - 3 of 1005
[ATTEMPT] target 192.168.1.111 - login "postgres" - pass "12345" - 4 of 1005
[5432][postgres] host: 192.168.1.111 login: postgres password: postgres
<finished>
Start
Stop
Save Output
Clear Output
hydra -V -l postgres -P /usr/share/wordlists/metasploit/unix_passwords.txt -e n...