Name: Zac Fawcett
Date: February 16th, 2022
Submission: Kali Linux Research
Report Tools: Legion & Ophcrack

Table of Contents

Project Introduction

Kali Linux is a specialized Linux distribution, focused on security applications, specifically: penetration testing, OS hardening and digital security forensic analysis. Within Kali there are many hundreds of tools at the user's disposal, with varying uses and abilities. This report serves as an instruction manual for two such tools. Legion is a multipurpose tool aiming to bring the most popular penetration testing tools into one easy to use outlet. Ophcrack cracks passwords using advanced cryptographic math tables. Both tools will be introduced; their finer details and uses examined. All from the point of view of someone brand new to these applications.

Legion

Introduction

Legion simplifies penetration testing by integrating many popular tools into a single python coded GUI. Tools like NMAP are invaluable to Kali Linux's penetration testing suite, but they require the user to memorize many commands and run scans individually through terminal. Legion aims to house these varied avenues of attack in one place, with each app ready to be called up easily to a user experience that is dense with options to customize each reconnaissance and attack.

History

Legion was created by SECFORCE, a UK based cybersecurity consultancy that offers penetration testing. Originally called Sparta, Legion has evolved by adding deeper NMAP option customization, task routines, estimated completion times, and many one-click scans, scripts and vulns of available targets. There is still a dedicated team that works on improving Legion who have kept it open-source, making the program extremely user friendly [1].

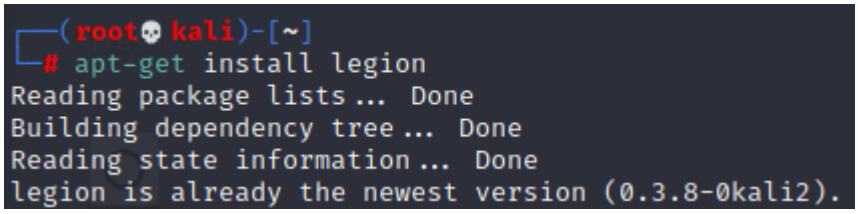
Use Case

In the "Council Certified Ethical Hacker training guide" [2]. The steps for starting to gauge a network's penetrability are: check for hosts that are "up", find open ports, search for vulnerabilities and create a network map. Usually a Kali Linux user will use NMAP scans, netstat, and netcat to poke around in order to show all the hosts, open ports and vulnerabilities. Results of interest would usually be saved in text or database form. Legion simplifies this crucial step in the process by having all that information on-screen or accessible within one or two clicks. If the user forgot to save a piece of info and then cleared the screen on a terminal they would have to search through log history to try to find it or rerun the command. In Legion nothing is lost unless the app is shutdown. The program provides a central graphical repository from which host scan (including versions, services, open ports etc), possible useful scripts, CVE (Common Vulnerabilities and Exposures) options and even brute force password options can be launched from. The app offers a level of autonomy, wherein it will try certain procedures (like password scans and taking screen shots of web server pages) for the user as the scan progresses. Each of these features will be covered in the basic user manual section.

Installation

Since this is a Kali Research project, the assumption that the user is using Kali Linux will be made. Legion comes prepackaged with most versions of Kali, but if the user is worried that they are out of date a simple “apt-get update” entered in the terminal will check for updates for all packages. To single out Legion the user can enter: “apt-get install legion”. If a Kali user doesn’t have Legion installed, they can also use “apt-get install legion”. If a non-Kali user would like Legion the process is more complicated depending on the system. A user on the Parrot Linux platform can install Legion the same as Kali, however, Ubuntu requires certain dependent packages to run Legion, the explanation of which is beyond this report’s scope [3].

SC#1 – Attempting to install Legion on a system that already has it.



Use and Features

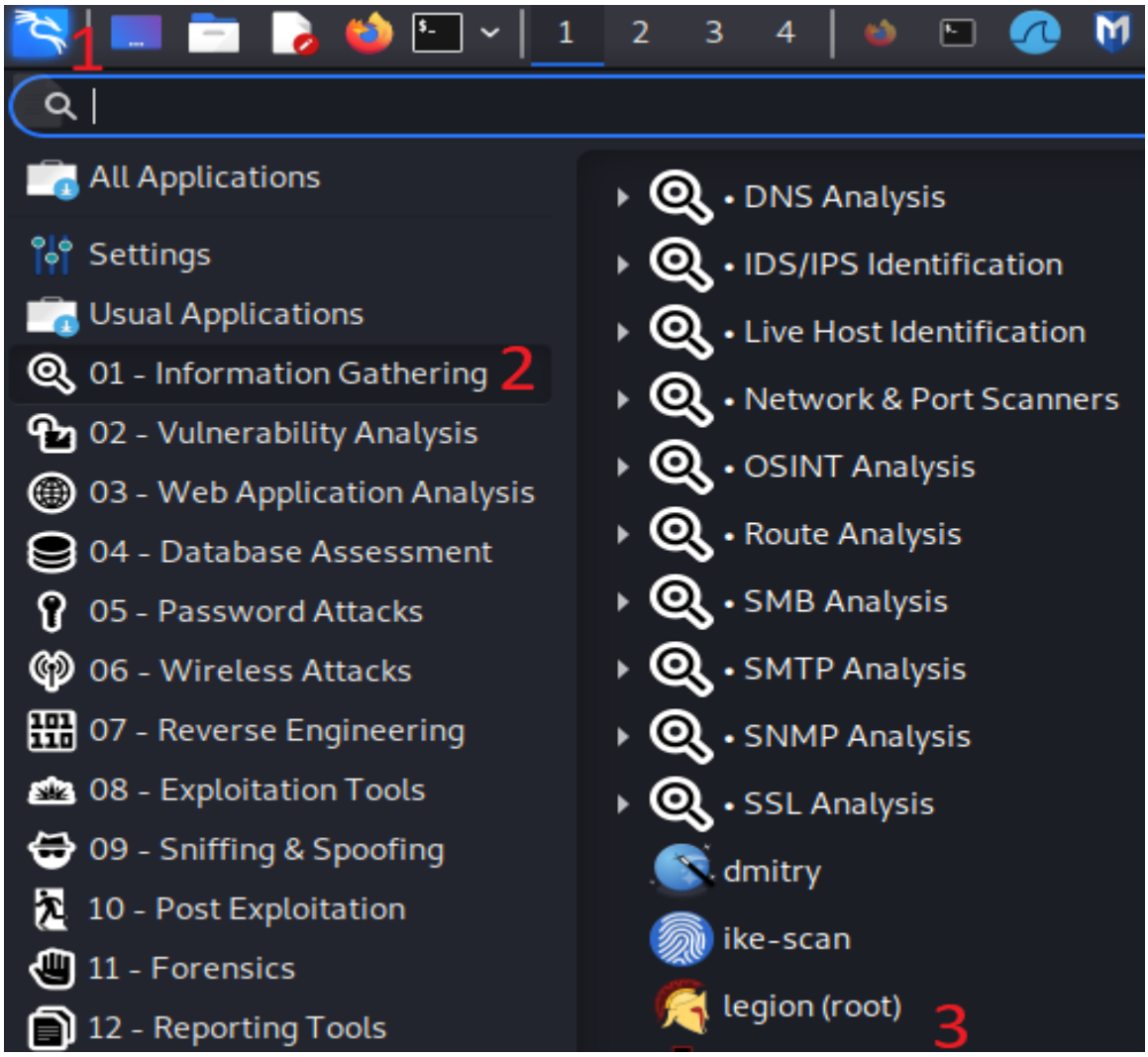
Starting Legion

Once the user is ready to start up Legion there have two options at their disposal. If the user is within a terminal window they can simply enter “legion” and the program will start up

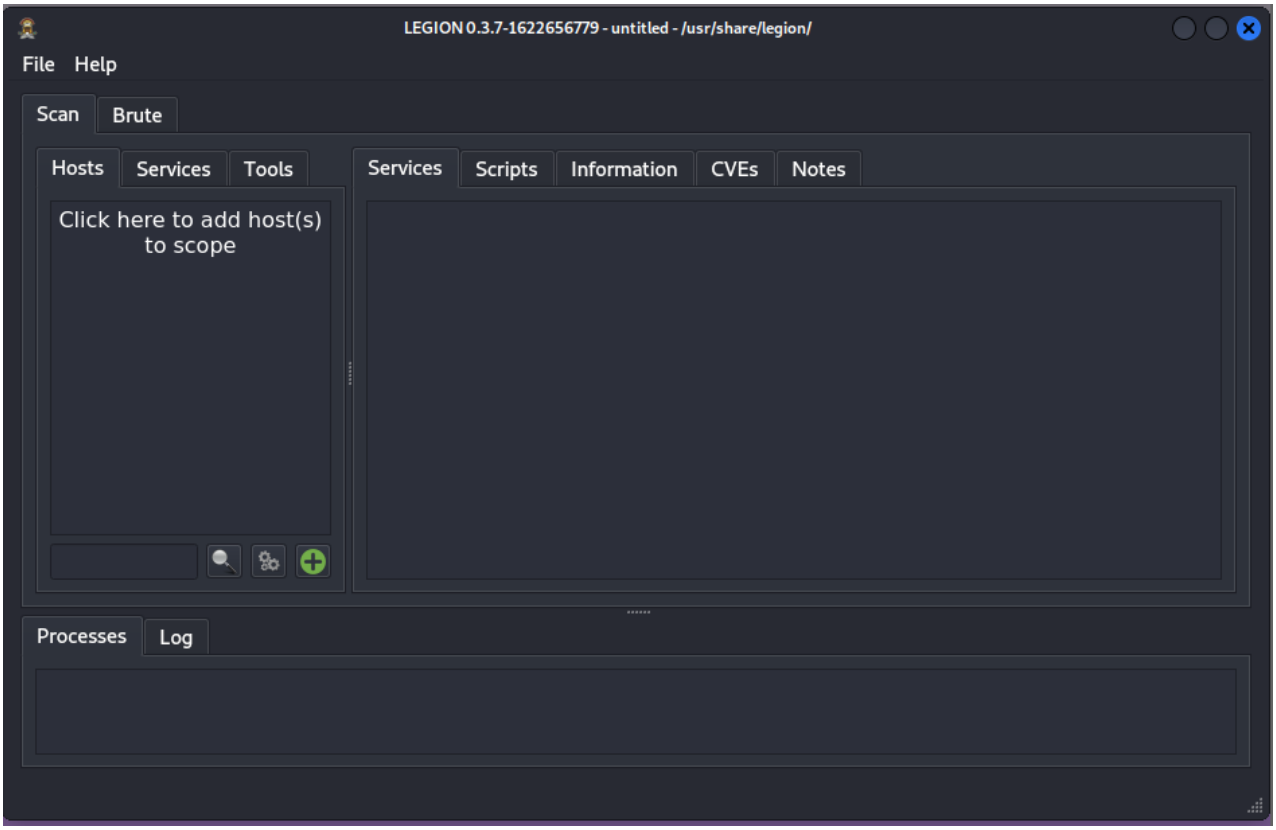
SC#2 – Terminal method of opening Legion

Alternatively, the user can navigate to the Kali icon in the top-left corner (White dragon), then navigate down to the Information Gathering section and then look for the Legion icon (Spartan Helmet) at the bottom

SC#3 – GUI method of opening Legion



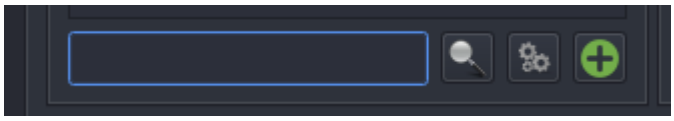
SC#4 – Legion Initial Screen



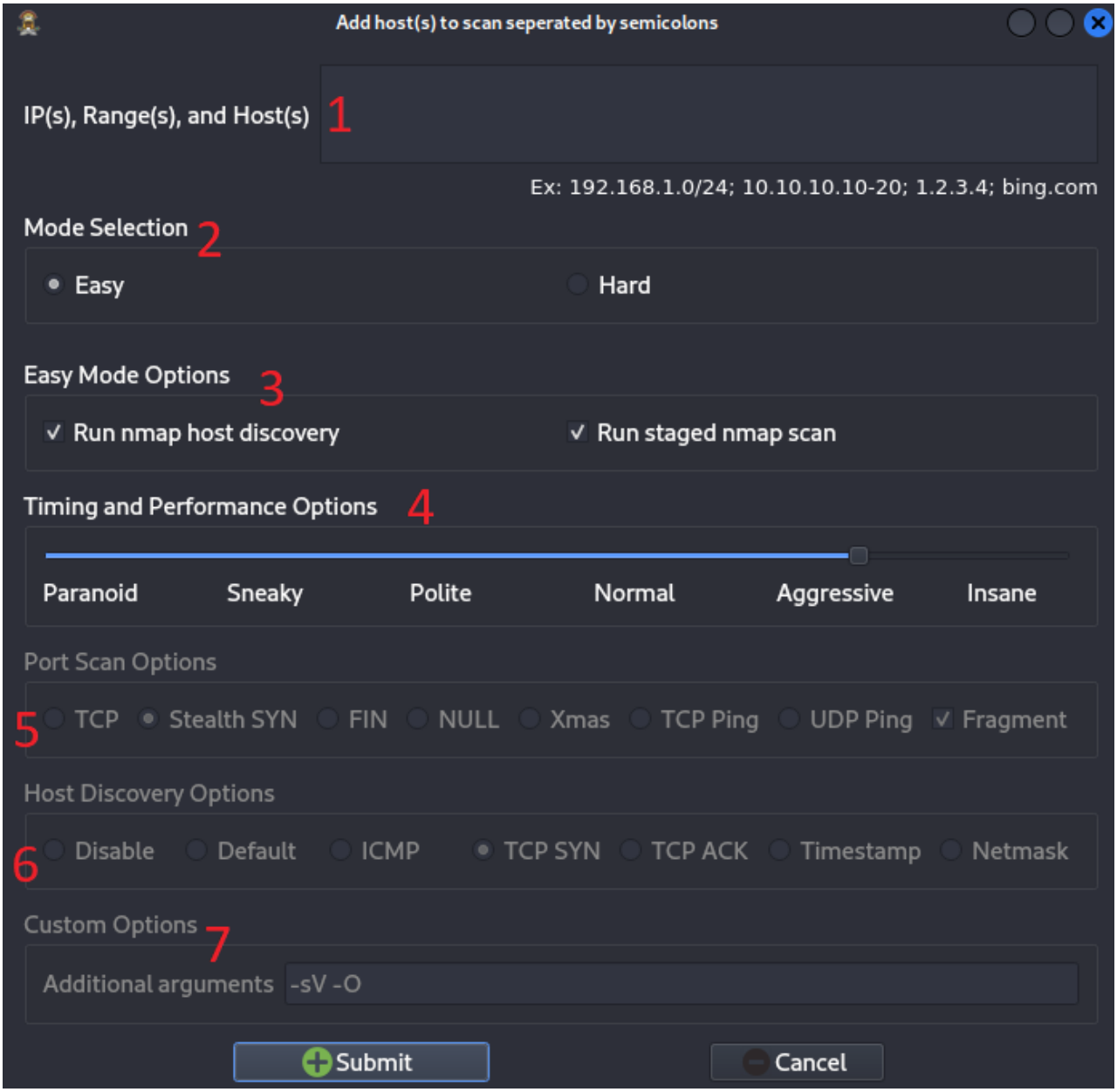
Using Legion

The first step in using Legion is to define the scope and type of scan desired and find some hosts. The user will click the green plus sign and be greeted with the scan customization screen.

SC#5 – Green plus sign to open scope screen



SC#6 – Scope customization screen

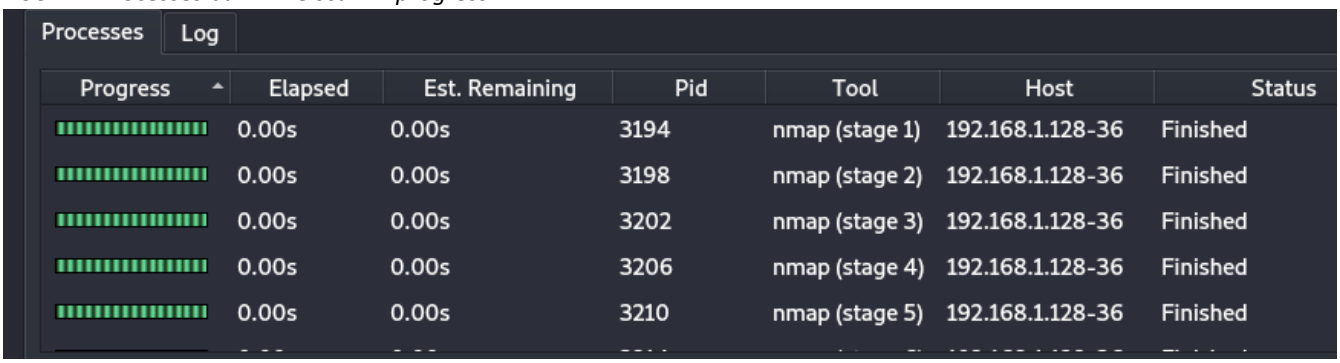


The scope customization screen contains all the options one would consider when doing an NMAP scan, but all nestled within one screen. The options of interest are (as numbered on the previous screenshot):

1. IP(s), Range(s), and Host(s) – here the user enters their choices for host scanning specifics. Individual hosts can be entered as singular IP addresses (e.g. 192.168.1.1), a range can be entered (e.g. 192.168.1.128-254) or a whole subnet can be entered by using the subnet address and mask (e.g. 192.168.1.0/24). Hostnames can be entered as well (e.g. sait.ca) and each entry can be entered simultaneously by separating them with a semi-colon and space.
2. Mode selection – this option tailors the type of scan to the user's desire. Easy mode has two options, while hard mode unlocks the options at numbers 5, 6, and 7.
3. For the easy mode options the user can run a host discovery which will just suss out if there are hosts up within the scope. Also in easy mode is the staged NMAP scan. This option runs 6 stages of various types of NMAP (think switches like "-sS, -sU, -sX, -f" etc), that Legion thinks the average use would want to use. It basically throws the kitchen sink at the scan. These can be used individually or in conjunction if the user wants.
4. After choosing a mode, the user can choose timing and performance options. These are the switches in NMAP that look like "-T0, -T4" etc. and decide how noisy, aggressive or stealthy the scan will be.
5. See number 7
6. See number 7
7. Options 5, 6, and 7 are customization options unlocked only while in hard mode. They correspond with the switches in NMAP like XMAS, FIN and other specialized options to help find vectors for attack. Option 7 is for the user to enter any additional switches/arguments that are not included in this screen [4].

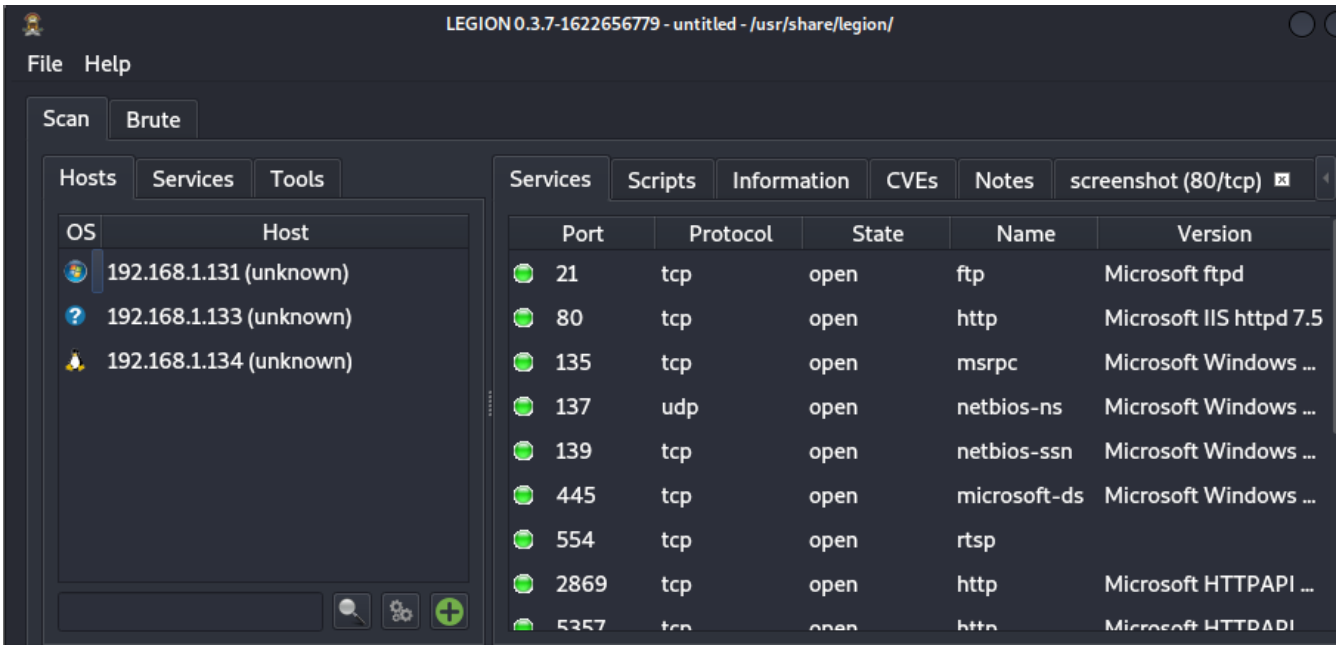
After choosing all their options the user will press the submit button and leave the customization screen back to the main screen (SC#4). The progress of the scan will be shown in the processes bar and as results are returned the Hosts section will fill.

SC#7 – Processes bar while scan in progress



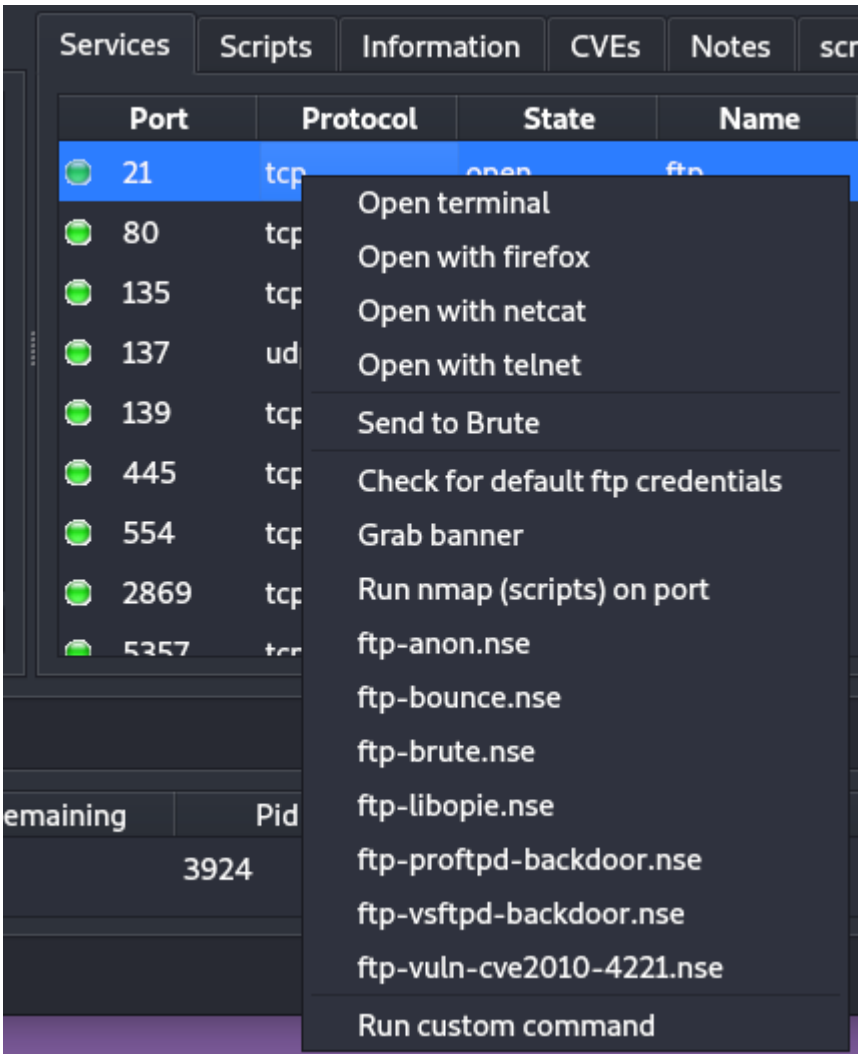
Once the scan has been completed the Hosts space will be populated with any machines that were found with an icon beside stating the OS (if the scan could find it).

SC#8 – Post scan view



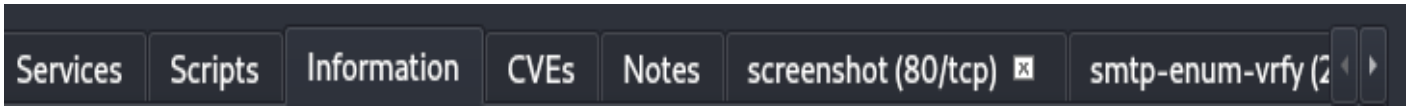
On the screen are all the open ports, corresponding protocols, port name, and versions. Right-clicking on one of the ports will bring up a menu of actions Legion thinks may be usable on that port. These include opening terminal and trying FTP, Telnet, NetCat, or scripts that can be run through NMAP.

SC#9 – Options for port attacks



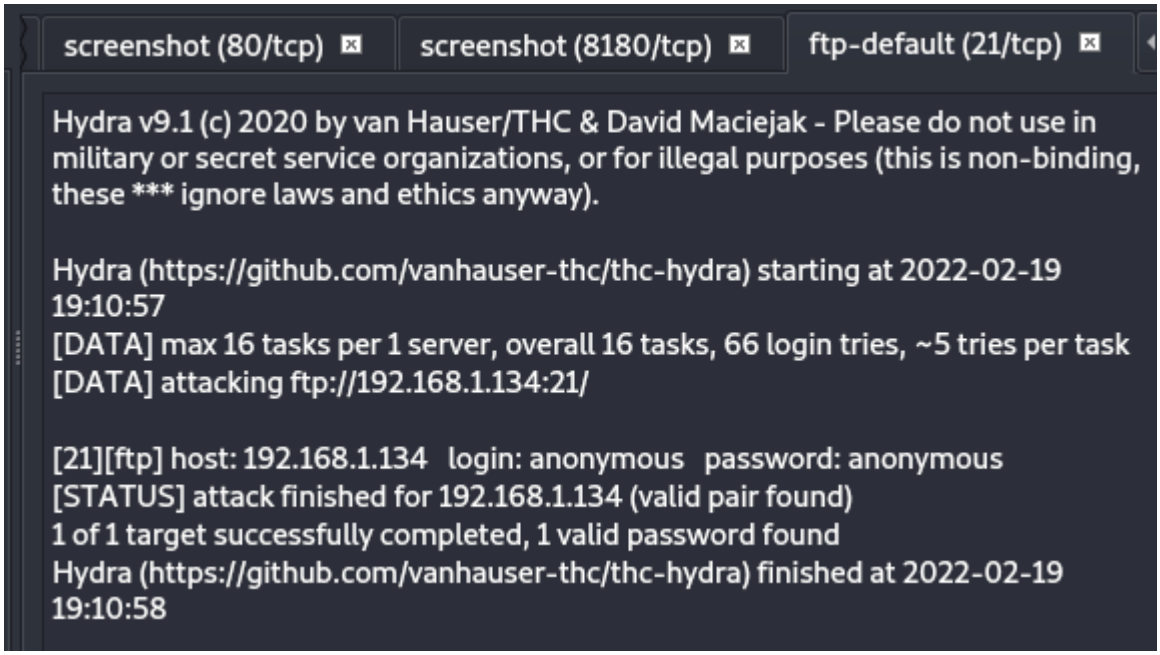
Along the top above the ports section is a bar that can be moved left and right that holds different menus. Services shows all the services open that the scan found. Scripts shows the scripts Legion thinks might work. Information shows info about the host system. CVEs shows some of the common exploits Legion detects may work against that host [5]. Further along the bar are the screenshots that Legion takes of each page it finds on the host's web servers and also some auto attempts Legion makes at brute forcing or exploiting passwords and enumerating users.

SC#10 Menu bar atop hosts section



Here is an example of the auto password attempts that Legion makes:

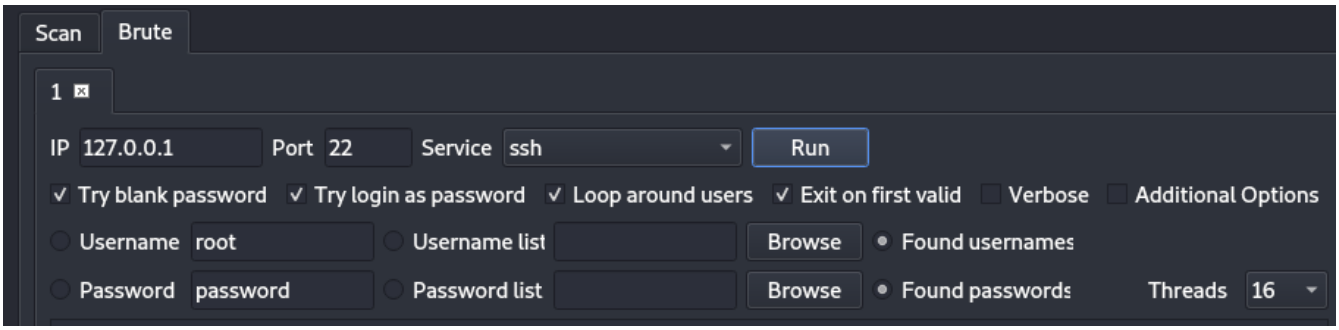
SC#11 – Auto password crack by Legion



The FTP server on the 192.168.1.134 host has been revealed. With this information the user has a vector for penetration testing without even trying.

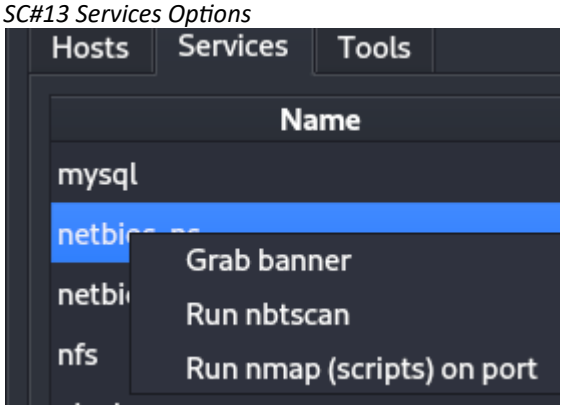
In the brute force section of Legion the user can choose individual usernames and passwords to run against all the open services or even specify word lists they have available to try and brute force their way into a service.

SC#12 – Brute force section



In the services section the user will see all services with open ports in alphabetical order. Each one has different options, seen by right clicking on the service.

SC#13 Services Options



These options are service specific and allow an easy way to do things like run NMAP scripts associated with that service. When selected the progress and results of these actions will be housed in new tabs on the sliding bar shown in SC#10.

Some other useful features include the ability to name and save Legion sessions (open file then save session, type in name and choose file path), which lets the user always come back to their work. NMAP scans done and saved out side of Legion can be imported (file, import NMAP), so the user can add previous or outside scans into their environment for ease of access. The log menu (located beside processes bar on main screen, SC#4), shows detailed records for each process attempted. Finally, the ability for Legion to seamlessly start other applications and transfer information from the scans is extremely useful. Legion has integration with, among others: Nikto, Dirbuster and PyShodan, allowing for instant transfer to those apps or in some cases running those app processes as process tabs within Legion.

After completing all the scans, noting open ports and possible vulnerabilities and exploits the user will have points to attack and monitor. Some of the actions they can take with this knowledge are:

- take CVE numbers and search Metasploit for corresponding exploit to use
- take the results of the brute force scans, log into services and try to get root, take valuable data or inject payloads for further access
- if the scans are of the user's own network they can use the results to harden defenses, close openings and check for evidence of attacks

Ophcrack

Introduction

Ophcrack is a password cracker. It takes hashes (encrypted passwords) from Windows machines and decrypts them. Ophcrack is presented in an attractive GUI that contains progress bars, estimated completion times and tables that lay out the usernames and associated hashes next to their cracked passwords. [6].

History

Ophcrack was created by the Swiss cyber security consultancy Objectif Sécurité [7]. The program is available for Windows, Linux and Mac OS, but it cracks passwords that are encrypted using the windows hash types (LM and NTLM). The application is based on “Rainbow Tables”, which are large databases of plain text with corresponding hashes. By preloading these databases (which can be under 1GB, and up to multiple TBs in size) into RAM, Ophcrack can use whats called a “time/memory trade off”. This method dedicates more memory to cracking and decreases the time taken to decrypt the password [8]. There are many versions of Rainbow Tables, which correspond to the operating system (Windows XP, Vista, 7, 10), as well as the length and complexity (upper/lower case letters, numbers and special characters) of passwords that can be cracked.

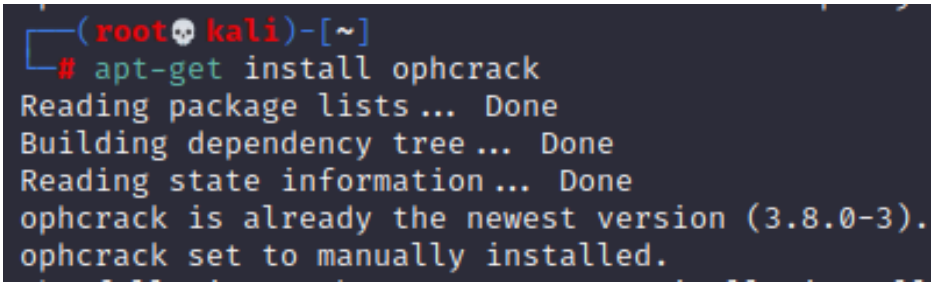
Use Case

There are many reasons a user may need to crack the encrypted hash of a saved password. If the password is totally lost but the data housed behind it is vital then having a way to retrieve it could be priceless. There are also nefarious purposes, such as a network intruder attempting to bypass encrypted passwords to get sensitive or valuable data. Ophcrack makes no distinction between these purposes, but simply serves the use case of cracking the hashes present on Windows systems. It can take in individual hashes and extract passwords one at a time, or PWDUMP (Password Dump) files and extract multiple passwords.

Installation

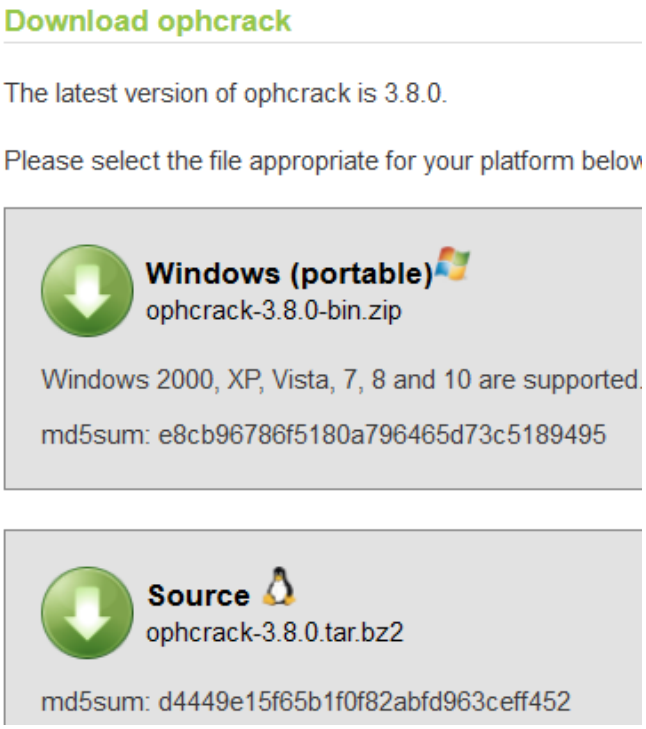
Since this is a Kali Research project, the assumption that the user is using Kali Linux will be made. Ophcrack comes prepackaged with most versions of Kali, but if the user is worried that they are out of date a simple “apt-get update” entered in the terminal will check for updates for all packages. To single out Ophcrack the user can enter: “apt-get install ophcrack”. If a Kali user doesn’t have Ophcrack installed, they can also use “apt-get install ophcrack”.

SC#1 – Attempting to install Ophcrack on a system that already has it



If a non-Kali user would like Ophcrack there are official Windows and Linux versions available from: https://ophcrack.sourceforge.io/download.php?type=ophcrack

SC#2 – Download page for other Ophcrack versions

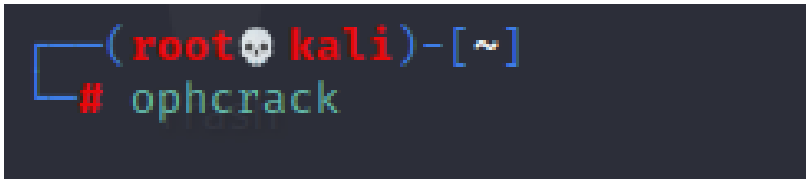


Use and Features

Starting Ophcrack

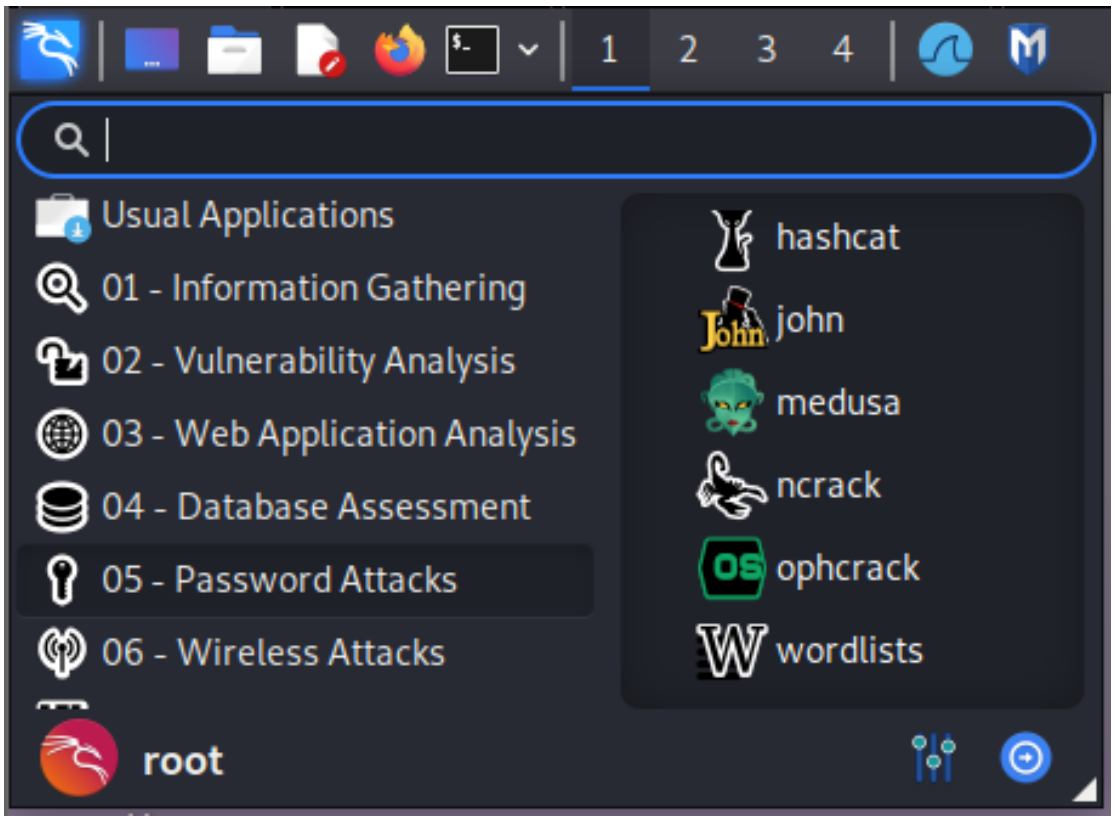
Once the user is ready to start up Ophcrack they have two options at their disposal. If the user is within a terminal window they can simply enter “ophcrack” and the program will start up.

SC#3– Terminal method of opening Ophcrack

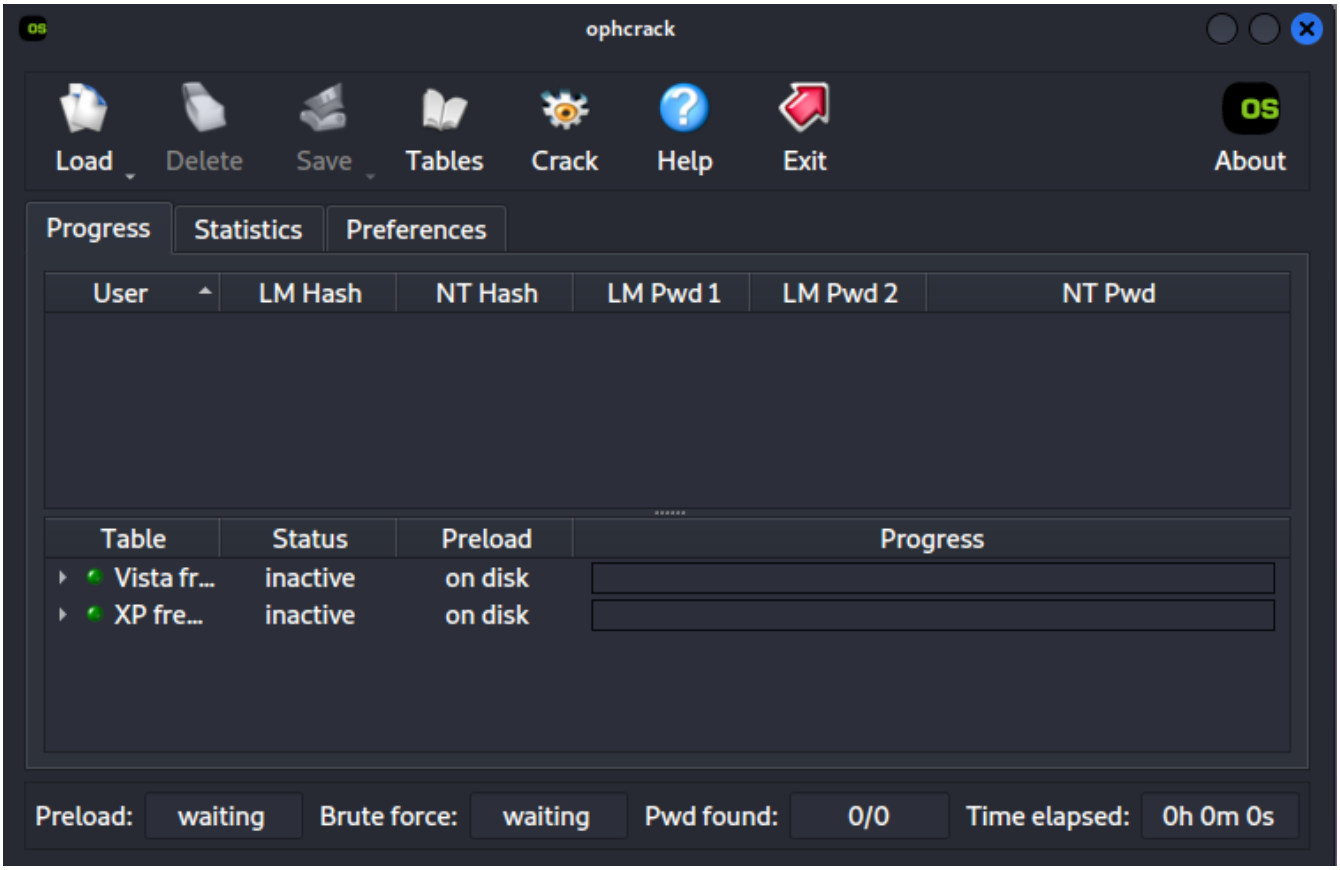


Alternatively, the user can navigate to the Kali icon in the top-left corner (White dragon), then navigate down to the Password Attacks section and then look for the Ophcrack icon.

SC#4 – GUI method of opening Ophcrack



SC#5 – Ophcrack initial screen

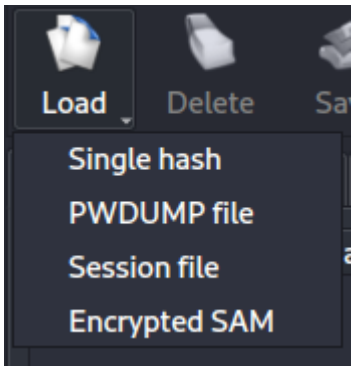


Using Ophcrack

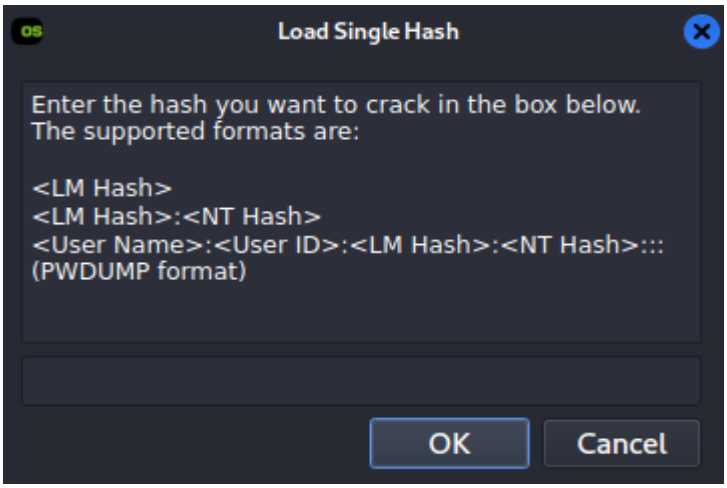
Using Ophcrack is incredibly simple. There are basically three main sections: loading, tables and cracking. To load up hashes click the load button. The user will be shown the formats accepted by Ophcrack and choose the one they will use. If the user selects the load option (SC#6) they are presented with the loading options. They can choose to select a single hash (one password), a PWDUMP file, session file or Encrypted SAM file. PWDUMP and encrypted SAM files are extracted from Windows systems (through the use of specialized apps), and contain multiple usernames/hash pairs.

In the single hash section the user is shown the formatting required in order for Ophcrack to decrypt the password.

SC#7 – Ophcrack load options



SC#8 – Formats accepted for single hash decryption



If single hash is selected then the hash must be typed or pasted into the menu. Single hash selection does not support the loading of files. The basic format needed by Ophcrack is a file with one hash per line in clear text. If it is a LM/NT (meaning a Windows Vista and up) hash, then the two hashes must be in LM then NT order and separated by a colon. For the PWDUMP format (multiple users) the format must be: ":::user:userID:LM:NT:::". The triple colon's indicate start and end of each entry and Ophcrack needs them to process multiple hashes within a text file.

Formatting Examples for Ophcrack

Single LM Hash

3A599CB0902AD3AAE5E55D3FD61BC4D6

LM/NT Hash

3A599CB0902AD3AAE5E55D3FD61BC4D6:E168E3FD26939E85213DF8C610C288BF

Single LM/NT Hash with username, no ID

zac::3A599CB0902AD3AAE5E55D3FD61BC4D6:E168E3FD26939E85213DF8C610C288BF

PWDUMP Format single hash

zac:007:3A599CB0902AD3AAE5E55D3FD61BC4D6:E168E3FD26939E85213DF8C610C288BF:::

PWDUMP Format multiple users

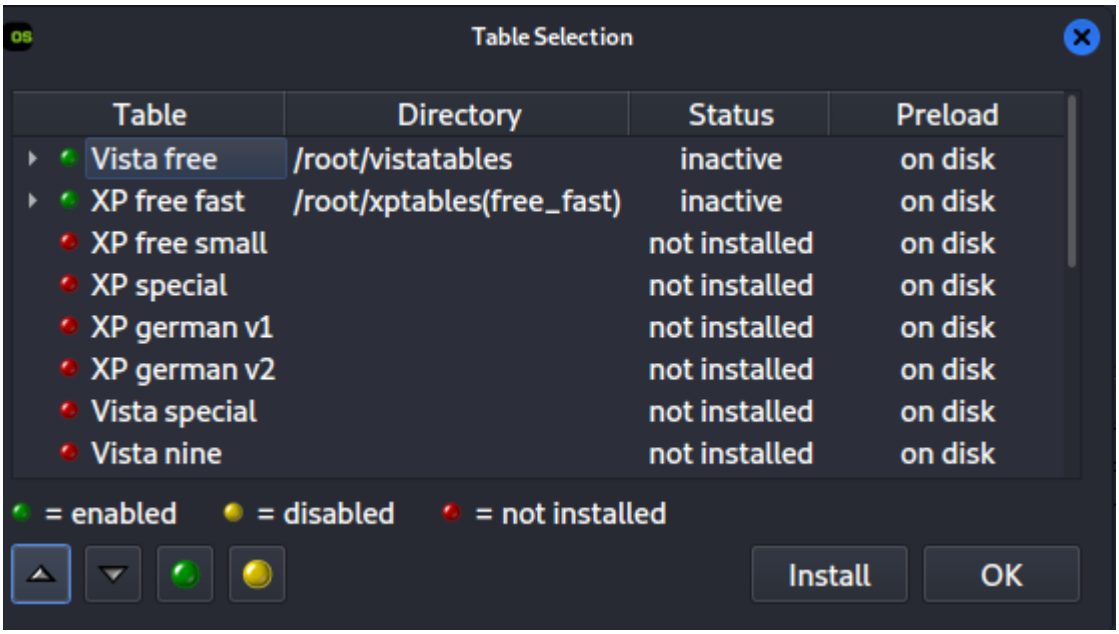
jane_somers:1001:AAD3B435B51404EEAAD3B435B51404EE:89C7EF6C7F5D58214F6B0A413965CF37:::

Guest:501:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0:::

Administrator:500:AAD3B435B51404EEAAD3B435B51404EE:99CD4F982B2AA1C382FEF7F88F873580:::

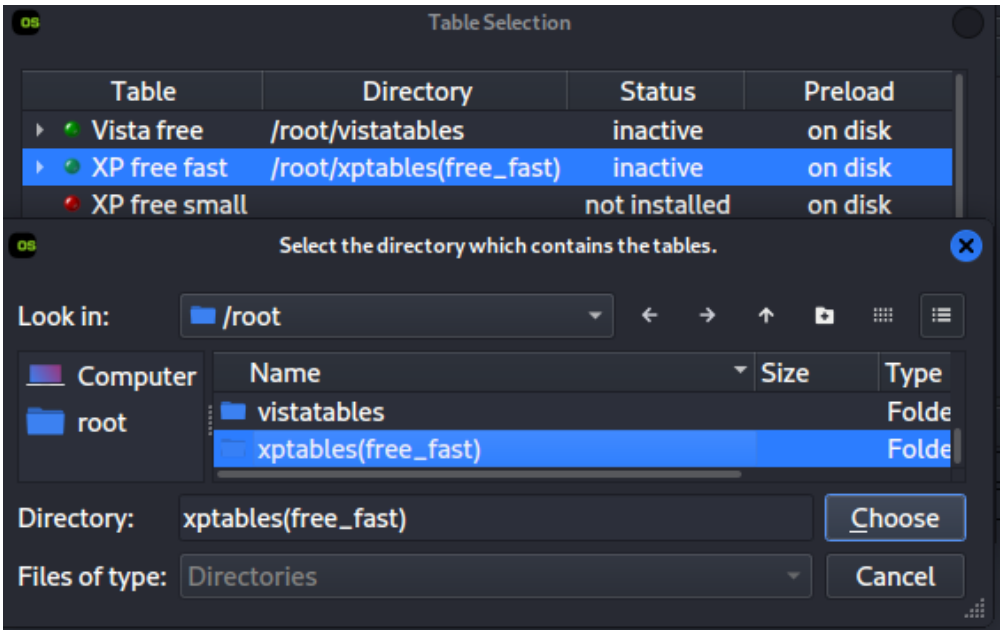
In the tables section the user is able to designate folders that hold the Rainbow tables needed by Ophcrack to function. No tables come preinstalled with the program and must be downloaded. The creators of Ophcrack offer official tables, but there are also much larger tables that have been added to over time by the public.

SC#9 – Ophcrack tables section screen



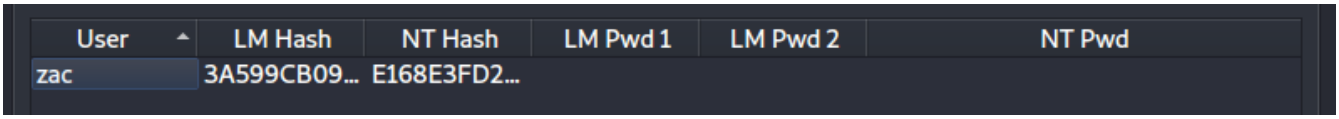
Still at the tables menu the user can see all the tables offered by Ophcrack If they highlight the table they want to install then click the Install button, they will be asked to point to a directory that holds that table. Once installed the table will be used in the cracking process when needed. The XP tables work with Windows XP, but will not crack passwords past Windows XP. The Vista tables will crack Vista, Windows 8 and Windows 10

SC#10 – Choosing a directory that holds the specified table



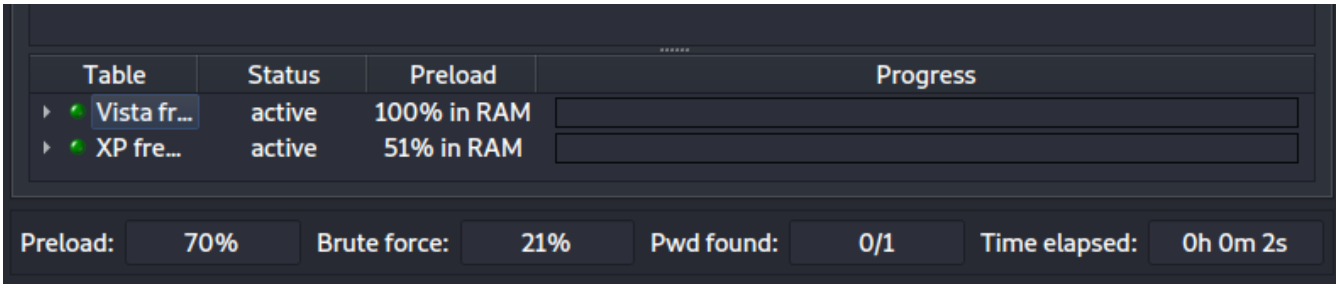
Here a single LM hash with username has been loaded into Ophcrack:

SC#11

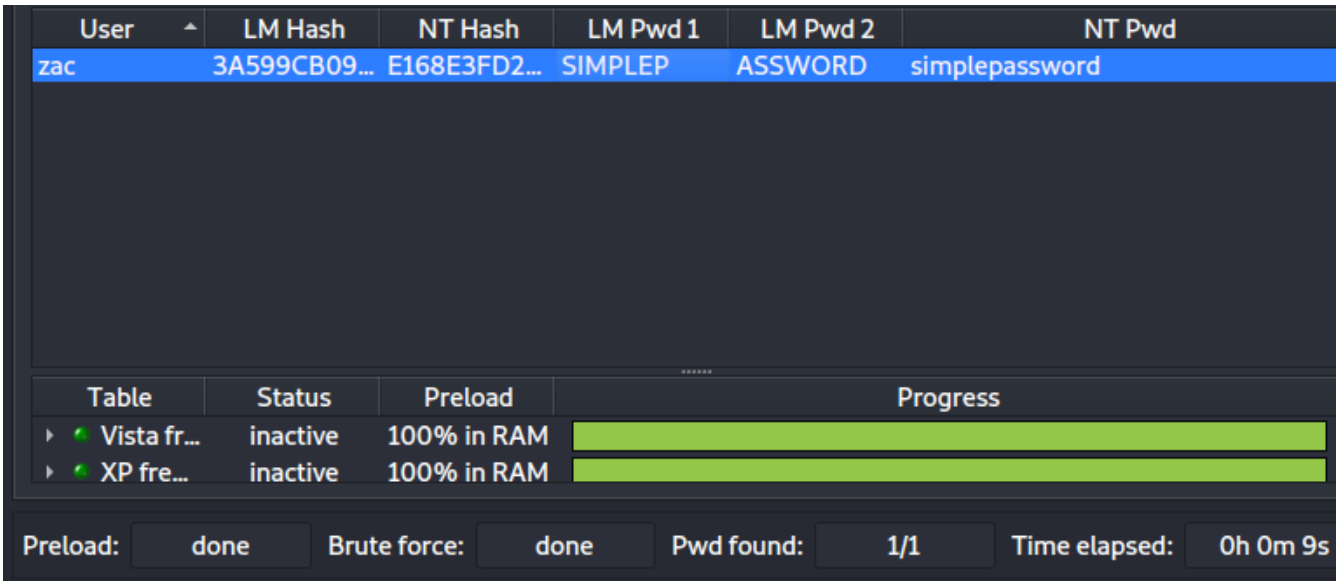


Pressing the crack button will tell Ophcrack to begin the crack. Depending on the type of password (LM vs NT), the table being used at the bottom will vary. Once the crack is initiated, the progress bar will commence.

SC#12 Crack in progress



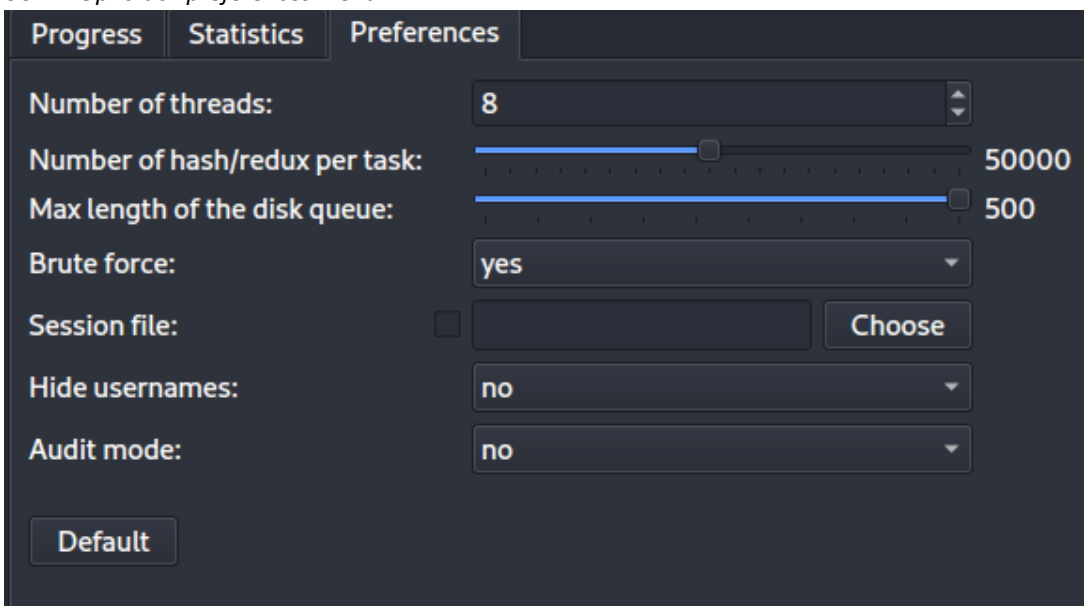
SC#13 Successfully completed crack



If successful the bottom will read how many passwords were found and time elapsed. The decrypted passwords will be shown along with the usernames and original hashes.

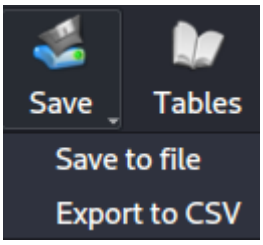
In the preferences menu the user can customize certain options such as how many CPU threads will be dedicated to the cracking, queue lengths as well as whether to try brute force in addition to cracking.

SC#14 Ophcrack preferences menu

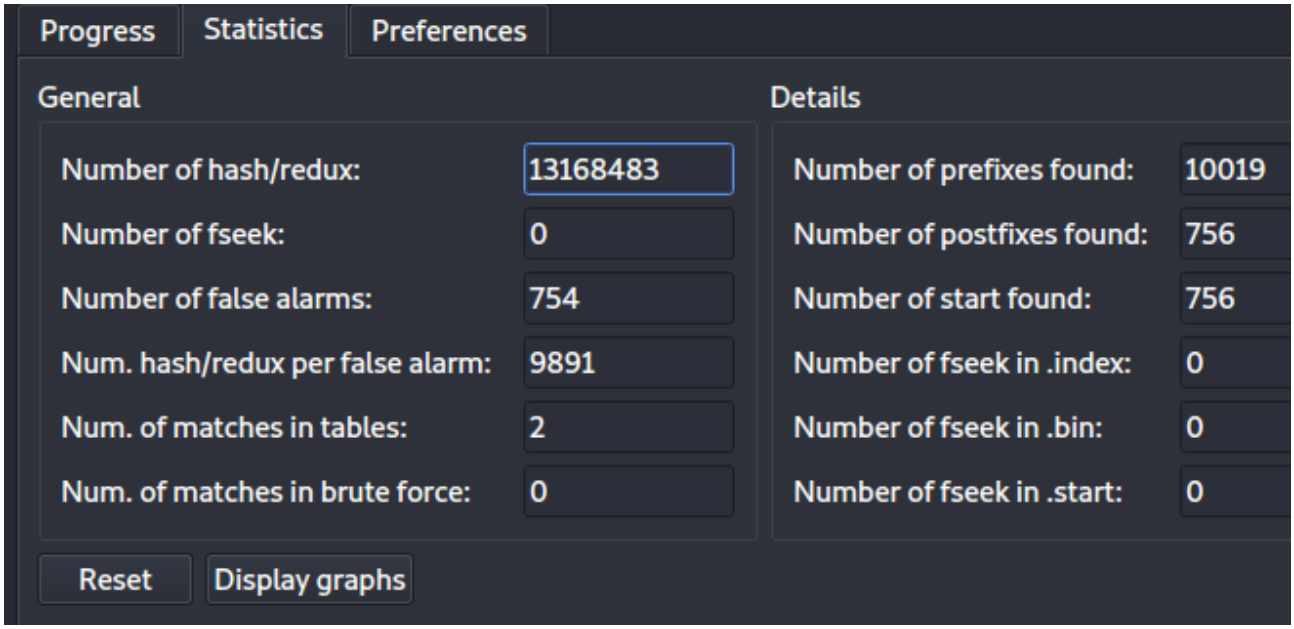


Some additional features are the ability to view statistics for the current Ophcrack session in both numerical (click statistics bar) and graphical representations (click statistics bar then display graphs icon), and the ability to save the current session as either a plain text document or in CSV format (click save icon then choose format). The output of the saved session includes any usernames, IDs, hashes and passwords currently loaded into the program.

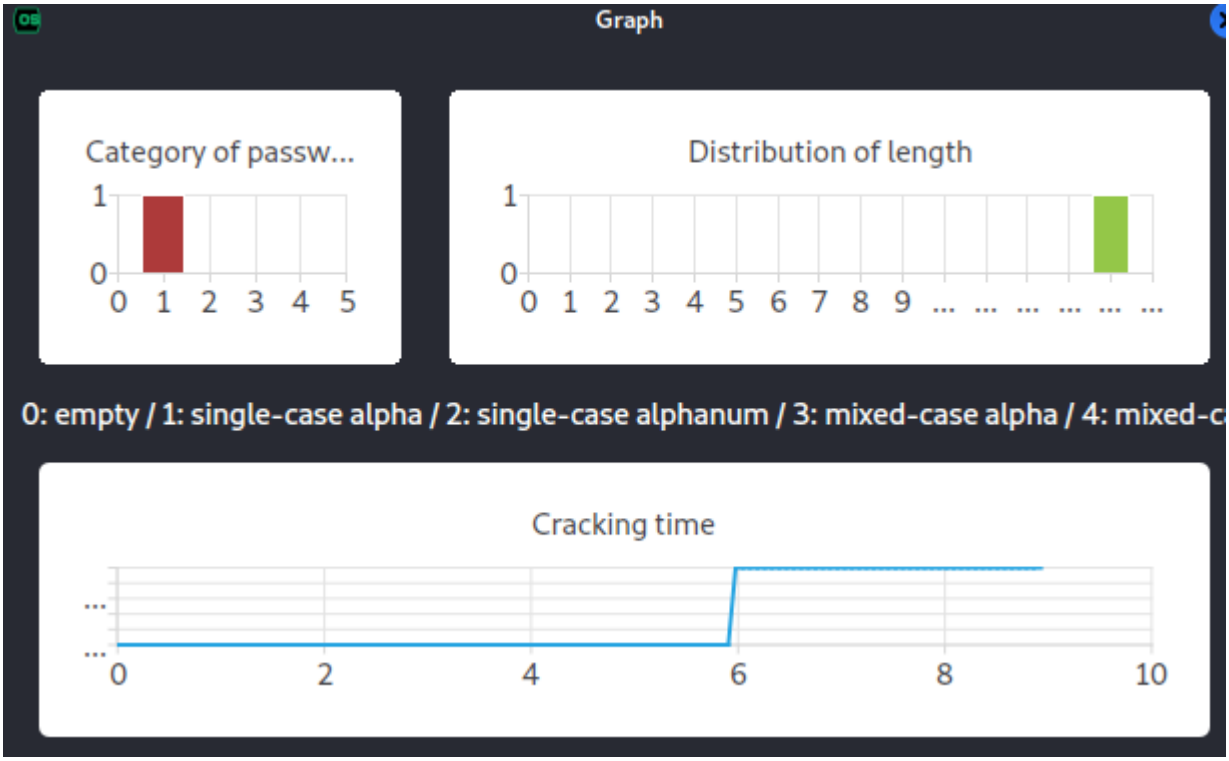
SC#15 Save options



SC#16 Ophcrack preferences menu



SC#17 Ophcrack session statistics graphs



References (Legion & Ophcrack)

1	https://www.secforce.com/about-us/
2	CEH v10: EC-Council Certified Ethical Hacker Complete Training Guide for Exam 312-50
3	https://hakin9.org/legion-open-source-network-penetration-testing-tool/
4	Getting Started with Legion Pentesting Framework (https://www.youtube.com/watch?v=7MoWs5RkZpo)
5	https://www.zerodaysnoop.com/tools/apps-packages/legion-network-penetration-testing-framework/
6	https://www.objectif-securite.ch/en/ophcrack
7	https://www.objectif-securite.ch/en/
8	*Eric Conrad, Joshua Feldman, in Eleventh Hour CISSP (Second Edition), 2014*
9	https://sourceforge.net/p/ophcrack/wiki/ophcrack%20Howto/