Atharva C Gaikwad

College: - AISSMS IOIT

SYSTEM HACKING

Password Attack: -

1. Hydra: -

Abstract: -

Security of server in all contexts is dominating in every field of computing, while working on the servers numerous threats and attacks like cracking of passwords, knowing the root of machine, giving privilege to unauthorized users are common attacks that can harm the system and take access of servers. The most prevalent commands like Hydra and Medusa, Ncrack are there which can be used for cracking the passwords of server and unauthorized users can take the access of server by applying these commands.

Objective: -

Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add. This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

Introduction: -

Hydra – a very fast network logon cracker which supports many different services. It is a parallelized login cracker which supports numerous protocols to attack. New modules are easy to add, besides that, it is flexible and very fast. This tool gives researchers and security consultants the possibility to show how easy it would be to gain unauthorized access from a remote to a system.

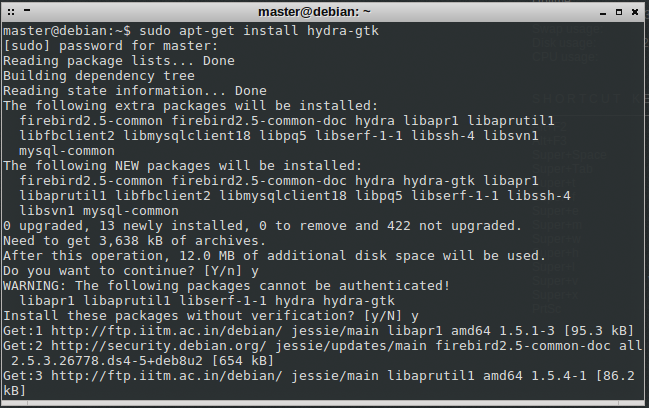
Currently this tool supports: adam6500, afp, asterisk, cisco, cisco-enable, cvs, firebird, ftp, ftps, http[s]-{head|get|post}, http[s]-{get|post}-form, http-proxy, http-proxy-urlenum, icq, imap[s], irc, ldap2[s], ldap3[-{cram|digest}md5][s], mssql mysql(v4), mysql5, ncp, nntp, oracle, oracle-listener, oracle-sid, pcanywhere, pcnfs, pop3[s], postgres, rdp, radmin2, redis, rexec, rlogin, rpcap, rsh, rtsp, s7-300, sapr3, sip, smb, smtp[s], smtp-enum, snmp, socks5, ssh, sshkey, svn, teamspeak, telnet[s], vmauthd, vnc, xmpp

For most protocols, SSL is supported (e.g., https-get, ftp-SSL, etc.).  If not, all necessary libraries are found during compile time, your available services will be less.  Type “hydra” to see what is available.



Methodology: -

Installing Hydra from Source Repository: -

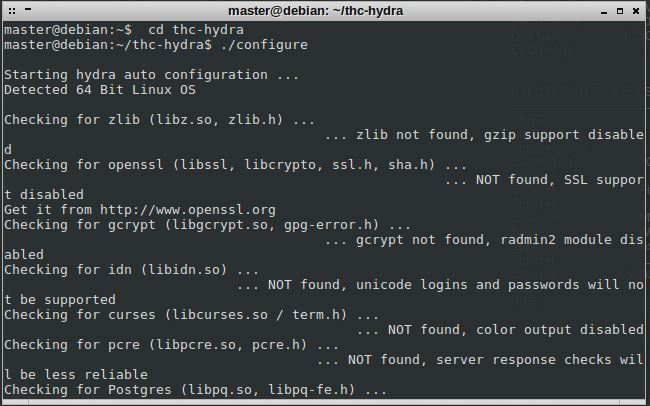


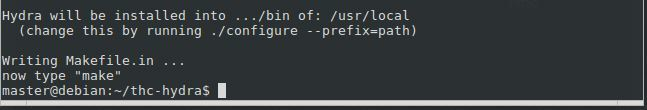
2)Locate to the cloned folder directory in your terminal.

cd thc-hydra

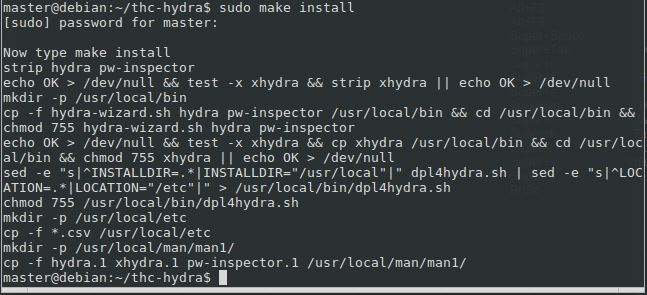
3)After locating to the directory we need to configure it

./configure

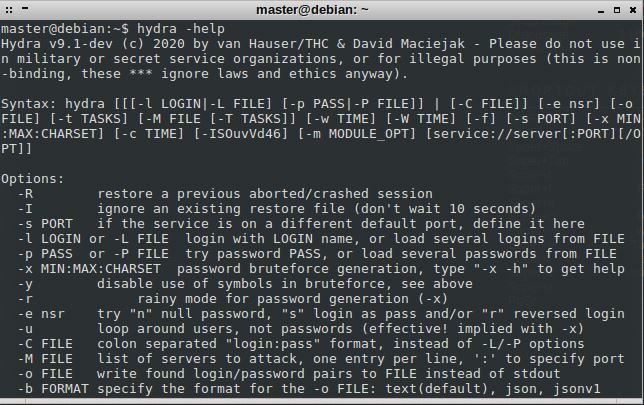




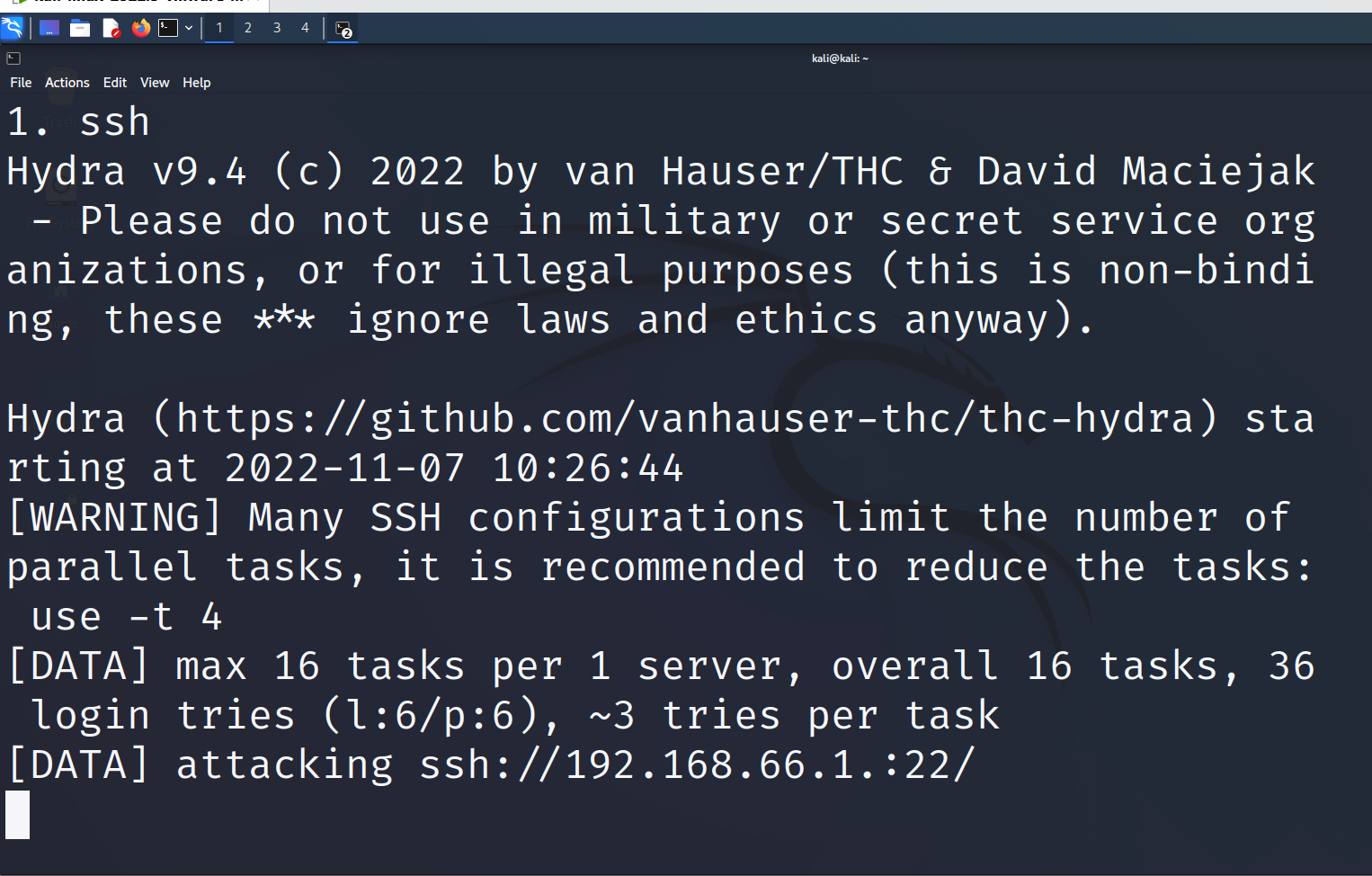
4)Now if you see this kind of screen with a message “make”, follow the instructions. Use root privileges for “make install”

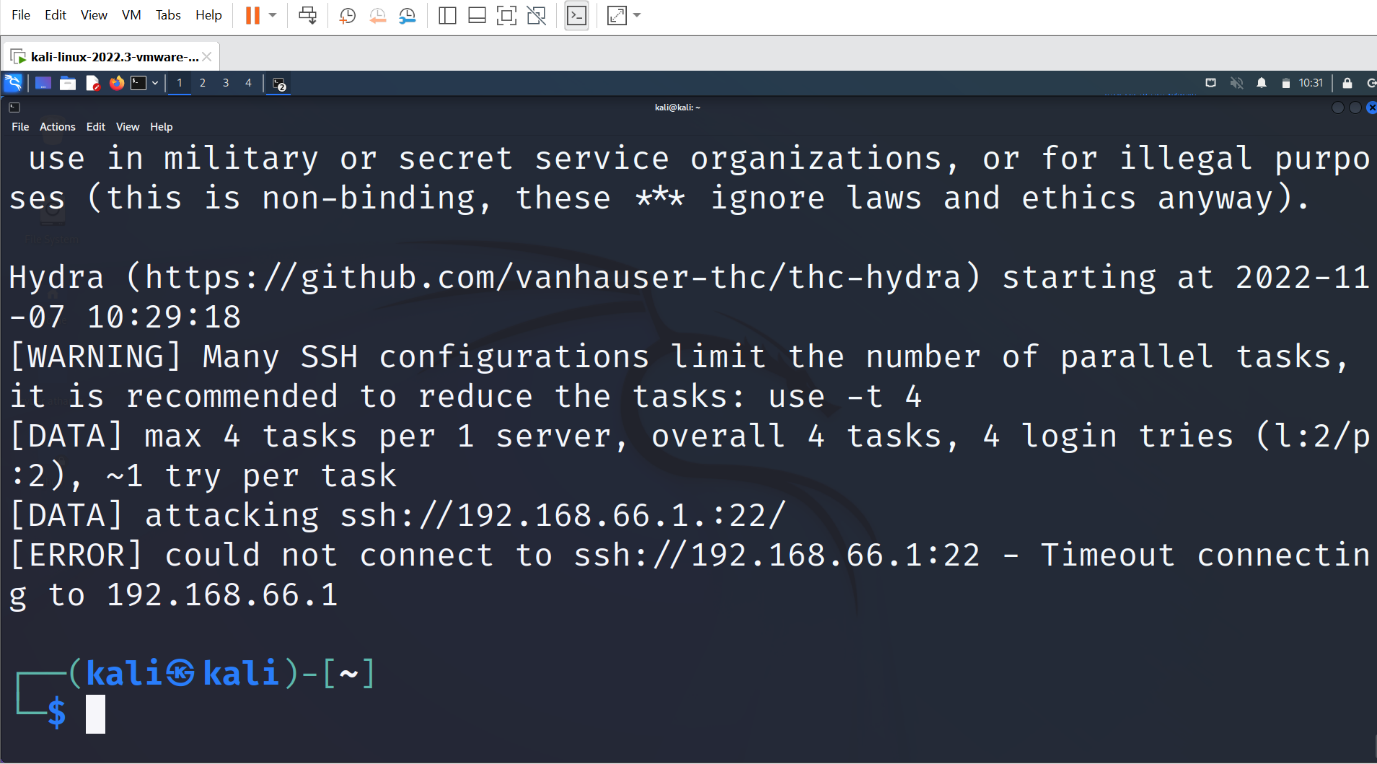


Go to your home directory and use “hydra -help” ensure hydra is installed properly and working well.



Screen Shot Hydra Attack: -





Conclusion :-

In this article we were able to demonstrate how to use Hydra password cracker and RSMangler to launch a hybrid brute force dictionary attack on a remote system. Although this approach is not the most subtle, and it will likely set off tripwires and red flags as it’s working. However, it is effective and in poorly monitored environments can result in an attacker getting in and out before a SysAdmin realizes what has happened.

1. Auxillary Module :-

Abstract: -

In metasploit any module that is not an exploit is an auxiliary module. Exploit modules always have a payload. Auxiliary modules are a fascinating feature of the framework allowing it to extend for a variety of purposes other than exploitation.

Objective: -

The Metasploit Framework includes hundreds of auxiliary modules that perform scanning, fuzzing, sniffing, and much more. Although these modules will not give you a shell, they are extremely valuable when conducting a penetration test.  
Introduction: -

Metasploit is the most commonly used pentesting tool that comes pre-installed in Kali Linux. The main components of Metasploit are **msfconsole** and the modules it offers.

What Is msfconsole?

**msfconsole** is the most commonly used shell-like all-in-one interface that allows you to access all features of Metasploit. It has Linux-like command-line support as it offers command auto-completion, tabbing, and other bash shortcuts.

It's the main interface that'll allow you to work with Metasploit modules for scanning and launching an attack on the target machine.

Now moving one of the main modules of Metasploit:

Auxiliary: The auxiliary module contains a set of programs such as fuzzers, scanners, and SQL injection tools to gather information and get a deeper understanding of the target system.

Auxiliary modules: -

In Metasploit any module that is not an exploit is an auxiliary module. Exploit modules always have a payload. Auxiliary modules are a fascinating feature of the framework allowing it to extend for a variety of purposes other than exploitation. You can create your own quick vulnerability scanners, port scanners, make MSF work as an FTP, HTTP or SMTP client and do a whole lot of other cool stuff. You have a ready to use code library at your disposal enabling quick development of such tools.

Throughout this chapter, we will look into various aspects and features of auxiliary modules and shall try to implement our own auxiliary module. This module will try to place files or delete files on web servers that allow the HTTP protocol's PUT and DELETE methods without any authentication. This is a good example of an auxiliary module since it isn't an exploit. It is just a simple tool to check web server mis-configurations.

Methodology: -

In this article we were able to demonstrate how to use Hydra password cracker and RSMangler to launch a hybrid brute force dictionary attack on a remote system. Although this approach is not the most subtle, and it will likely set off tripwires and red flags as it’s working. However, it is effective and in poorly monitored environments can result in an attacker getting in and out before a SysAdmin realizes what has happened.

Scanners: -

Scanning can be considered a logical extension (and overlap) of active reconnaissance that helps attackers identify specific vulnerabilities. It's often that attackers use automated tools such as network scanners and war dialers to locate systems and attempt to discover vulnerabilities.

Some list of auxiliary scanners: -

[DCERPC](https://www.offensive-security.com/metasploit-unleashed/scanner-dcerpc-auxiliary-modules/),[Discovery](https://www.offensive-security.com/metasploit-unleashed/scanner-discovery-auxiliary-modules/),[FTP](https://www.offensive-security.com/metasploit-unleashed/scanner-ftp-auxiliary-modules/),[HTTP](https://www.offensive-security.com/metasploit-unleashed/scanner-http-auxiliary-modules/),[IMAP](https://www.offensive-security.com/metasploit-unleashed/scanner-imap-auxiliary-modules/),[MSSQL](https://www.offensive-security.com/metasploit-unleashed/scanner-mssql-auxiliary-modules/),[MySQL](https://www.offensive-security.com/metasploit-unleashed/scanner-mysql-auxiliary-modules/),[NetBIOS](https://www.offensive-security.com/metasploit-unleashed/scanner-netbios-auxiliary-modules/),[POP3](https://www.offensive-security.com/metasploit-unleashed/scanner-pop3-auxiliary-modules/),[SMB](https://www.offensive-security.com/metasploit-unleashed/scanner-smb-auxiliary-modules/),[SMTP](https://www.offensive-security.com/metasploit-unleashed/scanner-smtp-auxiliary-modules/),

[SNMP](https://www.offensive-security.com/metasploit-unleashed/scanner-snmp-auxiliary-modules/),[SSH](https://www.offensive-security.com/metasploit-unleashed/scanner-ssh-auxiliary-modules/),[Telnet](https://www.offensive-security.com/metasploit-unleashed/scanner-telnet-auxiliary-modules/),[TFTP](https://www.offensive-security.com/metasploit-unleashed/scanner-tftp-auxiliary-modules/),[VMware](https://www.offensive-security.com/metasploit-unleashed/scanner-vmware-auxiliary-modules/),[VNC](https://www.offensive-security.com/metasploit-unleashed/scanner-vnc-auxiliary-modules/).

Server: -

ftp: - The **ftp** capture module acts as and FTP server in order to capture user credentials.

MSF > use auxiliary/server/capture/ftp

auxiliary(ftp) > show options

http ntlm: -The **http ntlm** capture module attempts to quietly catch NTLM/LM Challenge hashes over HTTP.

msf > use auxiliary/server/capture/http\_ntlm

msf auxiliary(http\_ntlm) > show options

imap: -The **imap** capture module acts as an IMAP server in order to collect user mail credentials.

msf > use auxiliary/server/capture/imap

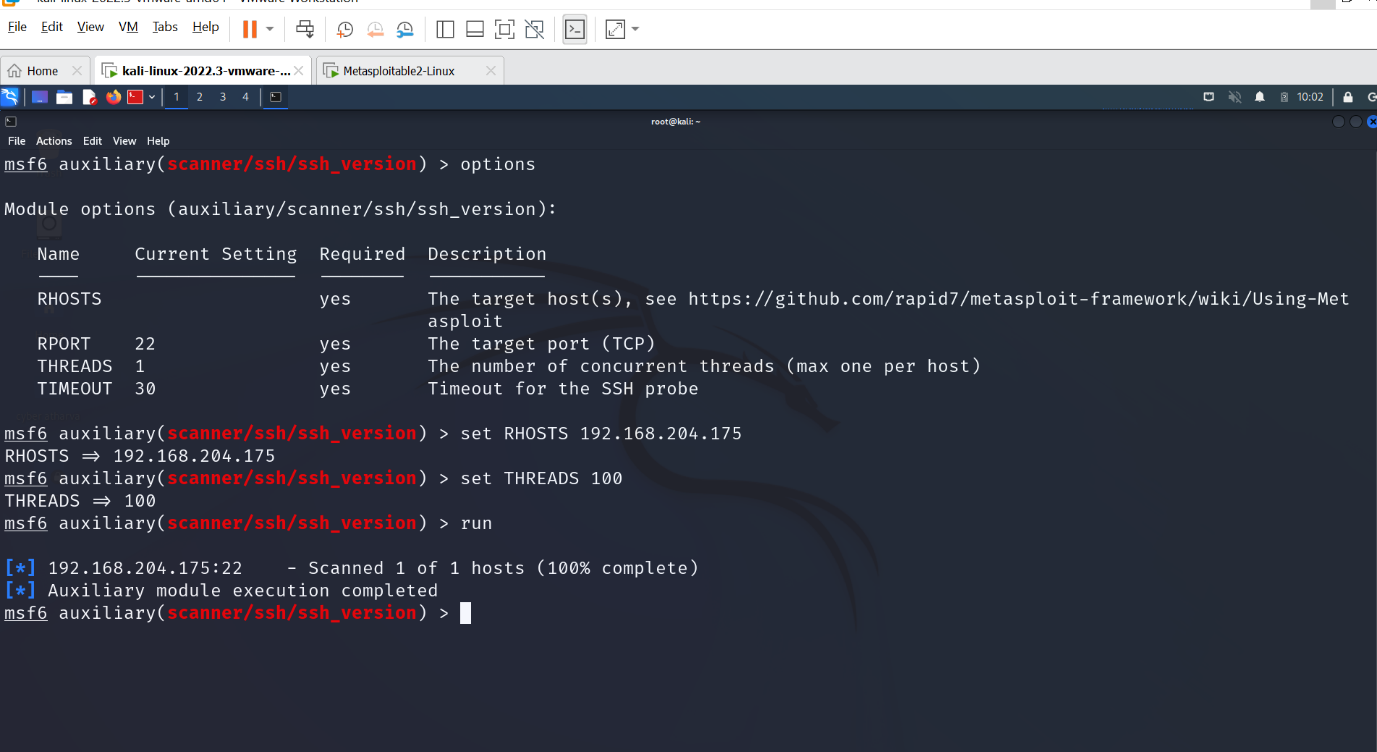
msf auxiliary(imap) > show options

smb: -The **smb** capture module acts as a SMB share to capture user password hashes so they can be later exploited.

msf > use auxiliary/server/capture/smb

msf auxiliary(smb) > show options

Screenshot of Auxiliary Module : -



Conclusion: -

Over here we had cleary understood how to use auxiliary module with the help of metaspliot frame work, we had done attack to a ipaddress by using ssh methods to find threads.

NSE Scripts: -

Abstract: -

Nmap, short for Network Mapper, is a free and open source tool used for vulnerability checking, port scanning and, of course, network mapping.

Objective: -

This program scans the network that a computer is connected to and outputs a list of ports, device names, operating systems, and several other identifiers that help the user understand the details behind their connection status. Nmap can be used by hackers to gain access to uncontrolled ports on a system.

Introduction: -

Nmap (“Network Mapper”) is a free and open source utility for network exploration and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and both console and graphical versions are available.

Methodology: -

1.UDP Scan (-sU): -

This technique is used to scan the open UDP ports of the target IP/host. Here, UDP scan sends UDP Packets to every ports of the target and waits till it get response. If, it receives error message stating that the [ICMP](https://searchnetworking.techtarget.com/definition/ICMP) is unreachable, this means that the port is closed. But, if gets any approachable response, then it means the port is open.

Command: nmap -sU <target>

Often, security auditors neglects UDP ports because it is generally slower and difficult to scan than TCP. This is one of the biggest mistake as, exploitable UDP ports are very common and attackers are well aware regarding this.

2. FIN Scan (-sF)

In Fin Scan technique, packets are sent with a Fin Flag. Sometimes, because of firewall, SYN Packets might be blocked. In such case, FIN Scan works by passing the firewall. FIN packets are send to closed ports, if no response is received, it is because either the packet is dropped by firewall or the port is open.

Command: nmap -sU <target>

3. Ping Scan (-sP)

This technique is only used to find out whether the host is available or not. Ping Scan is not used to detect open ports. It sends ICMP echo request and in return gets ICMP echo reply is the host is alive.

Command: nmap -sP <target>

4. TCP SYN Scan (-sS)

In this technique, Nmap sends SYN packets to the destination, but does not create any session. As a result, target computer won’t be able to create any log of interaction as no session was initiated.

Command: nmap -sS <target>

If there is no scan mentioned, avTCP SYN is used by default.

5. TCP Connect() Scan (-sT)

UNIX socket uses a system call named connect()to begin TCP connection and if it succeeds, connection can be made and if it fails, connections cannot be made, basically because the port might be closed.

Command: nmap -sT <target>

This technique is only used to find out TCP ports and not UDP.

6. Version Detection (-sV)

This technique is used to find out about specific service running on open port, it’s version and product Name. It is not used to detect open ports. However, this scan needs open ports in order to detect the version. It uses TCP SYN scan to know about the open ports.

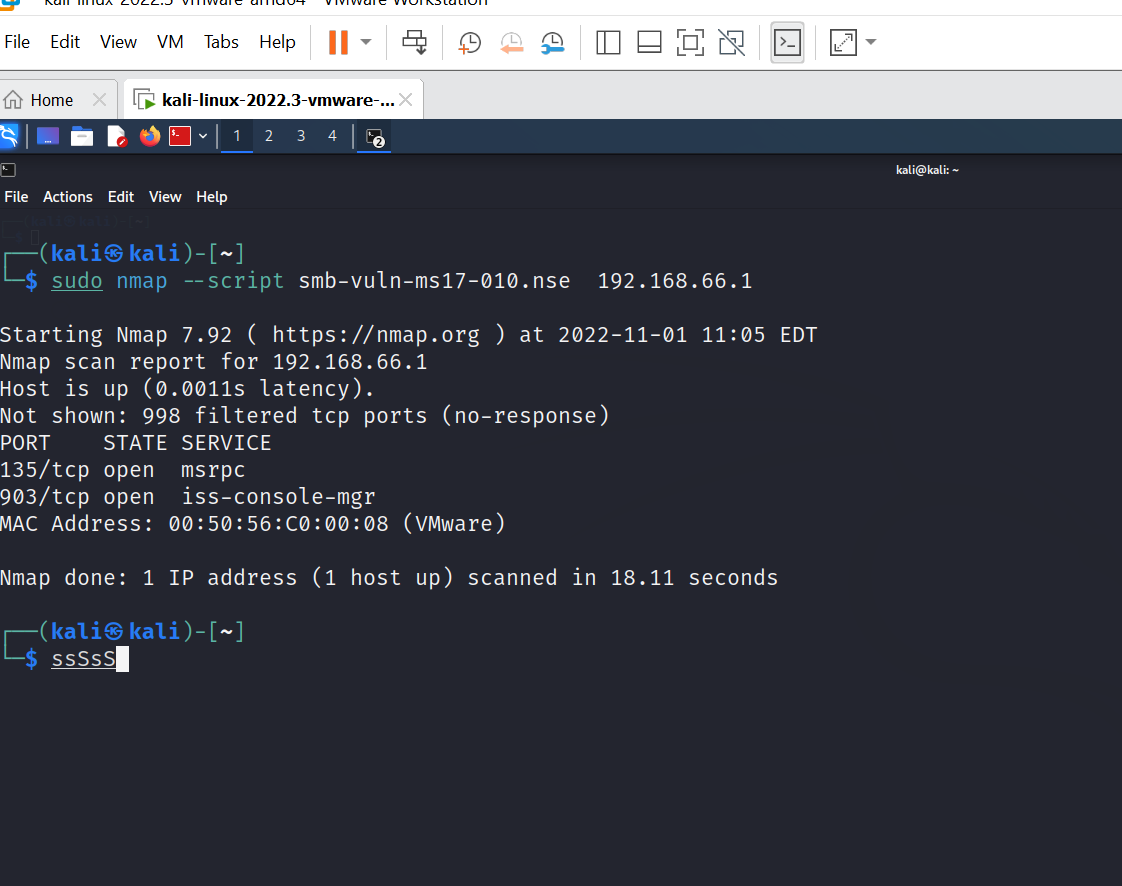
Command: nmap -sV <target>

7. Idle Scan (-sI)

Idle scan is an advance scan that does not send any packets from your IP address, instead it uses another host from the target network to send the packets.

Command: nmap -sI <target>

Screenshot of nmap attack/nes scripts:-



**conclusion: -**

 Nmap is a very powerful tool that can be used as first step towards penetration testing. This blog was written to discuss about Nmap and it’s scanning techniques from beginner to advance level. There are still lots of things you can do by using this tool, which we will be discussing in further blogs.

John the Ripper : -

Abstract : -

First released in 1996, John the Ripper (JtR) is a password cracking tool originally produced for UNIX-based systems. It was designed to test password strength, brute-force encrypted (hashed) passwords, and crack passwords via dictionary attacks.

Objective: -

john the Ripper is a tool designed to help systems administrators to find weak (easy to guess or crack through brute force) passwords, and even automatically mail users warning them about it, if it is desired.

Introduction :-

John the Ripper is a free password cracking software tool. It was designed to test password strength, brute-force encrypted (hashed) passwords, and crack passwords via dictionary attacks. John the Ripper is a part of the [Rapid7 family](https://www.itperfection.com/network-security/rapid7-products-security-insightidr-insightconnect-insightvm-insightops-insightops-insightappsec-insight-cloud/) of penetration testing/ hacking tools. Also, John is already installed on [Kali Linux.](https://www.itperfection.com/network-security/what-is-kali-linux-pen-testing-security-cybersecurity-monitoring/)

First, we advocate for ethical hacking.

Originally developed for the Unix operating system, it can run on many different platforms. John the Ripper supports hundreds of hash and cipher types, including for:

User passwords of Unix flavors (Linux, Solaris, etc.)

macOS

Windows

Web apps (such as WordPress)

Database servers (SQL, LDAP, etc.)

Network traffic captures

Encrypted private keys (such as SSH, and cryptocurrency wallets)

Filesystems and disks

Archives (ZIP, RAR, 7z)

Document files (PDF, Microsoft Office’s, etc.)

The tool comes in two versions :-

GNU-licensed: it is free and open source (FOSS) version.

Pro: It designed for use by professional pen testers, has additional features such as multilingual wordlists, performance optimizations and 64-bit architecture support. This version is the most used among penetration testers for cracking passwords.

Of course, an enhanced “jumbo” community release has also been made available on the [open-source GitHub repo.](https://github.com/openwall/john)

[The official website for John the Ripper is on Openwall](https://www.openwall.com/john/). You can grab the source code and binaries there.

Methodology : -

On Kali Linux, John the Ripper is preinstalled, so there’s no need to install anything! Just pick up the package, and take it for a ride.

**Scenario #1: You Just Got A Password Hash**

So, let’s assume that you were just handed a hash, an MD5 hash, to be specific. In real-life situations, you’d obtain these by scavenging a computer. In my case, I’m going to use the word password123:

echo 482c811da5d5b4bc6d497ffa98491e38 > hash.txt

To resolve the password, you’d use the simplest usage of the john the ripper code:

john hash.txt

Typically, John the Ripper automatically detects the hash type. But you can augment this as much as you want! So let’s say you want to add your own word list and specify the format, then you’d write:

So, the first time you run the latter, it will show the password on the screen, after which point, it will save it into a file called john.pot. In my case, the folder john.pot was located at /home/kali/.john/john.pot.

**Scenario #2: Password Protected Zip File**

Now let’s pretend there is a Zip file with a password lock. So at some point previously, you created a zip file that is password protected. For that, you’ll need to install zip:

sudo apt install zip

Then to create the zip file:

zip --password <password> <name of zip file> <directory to zip>  
  
Ex: zip --password password123 linuxhint.zip linuxhint.txt

(Here, the word password123 is the actual password protecting the zip file.)

Now, 6 months later, you’ve forgotten the password. What can you do? Well, use John the Ripper, but before we can, we first need to convert the zip to john.

To do so, we’ll use the zip2john command:

zip2john linuxhint.zip > linuxhint\_password.txt

The hash itself is located between the two dollar signs.

John the Ripper can retrieve the password using one of two methods: the dictionary attack or the bruteforce attack. A file with a list of potential passwords is compared to the hash at hand in a dictionary attack. If a match is found, it will chuck it out. On the other hand, if a password is not found, you can use a different password file or use a different method.

Next, we’d write:

john --wordlist=~/Downloads/passwordlist linuxhint\_password.txt

Here, what we did was crack a zip file, but it doesn’t have to be a zip file! It can be almost anything. Just remember that you have to, in such cases, use the {your\_module}2john. For example, if you were cracking Wifi, you’d use Aircrack-ng and obtain a cap file. Once you’ve obtained the cap file, you’d have to convert the cap file to an hccap file. Once you have a hccap file, use the hccap2john to convert it to the john format, which will yield results on John the Ripper.

You can find more of the 2john commands using:

locate 2john

**Scenario #3: Increment Style Or Brute Force**

The most powerful of all the methods available is the bruteforce method because it will check every possible combination out there! But this also means that it’s unlikely to ever end unless the passwords are reasonably simple.

For example, I will choose a 3 character password in the MD5 format: abc. I’m doing this so that I don’t have to spend hours waiting for it to detect it.

echo 900150983cd24fb0d6963f7d28e17f72 > incremental.txt

The simplest way of doing this is to type:

john --format=Raw-MD5 --incremental incremental.txt

Alternatively, you could have also written:

john --format=Raw-MD5 -i incremental.txt



As you can see, I found it in less than a second, and I didn’t even have to supply it with a dictionary.

Next, we’re going to mess around with the configuration file located at /etc/john/john.conf.

In the /etc/john/john.conf file, you will find a section on incremental modes. Here, you can add more if you want, but first, let’s try using one of them.

There’s one in /etc/john/john.conf that is as follows:

[Incremental:Digits]  
  
File= $JOHN/digits.chr  
MinLen= 1  
MaxLen= 20  
CharCount = 10

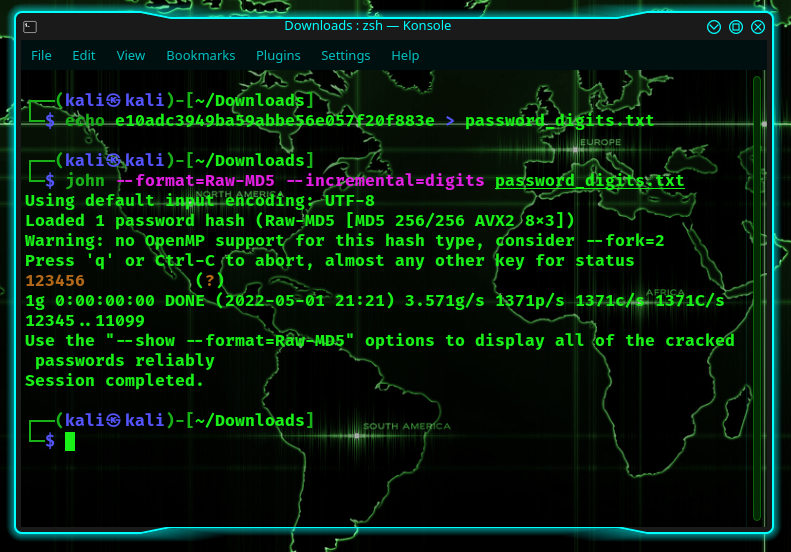
Here, let’s recreate an MD5 hash for the password 123456.

echo e10adc3949ba59abbe56e057f20f883e > password\_digits.txt

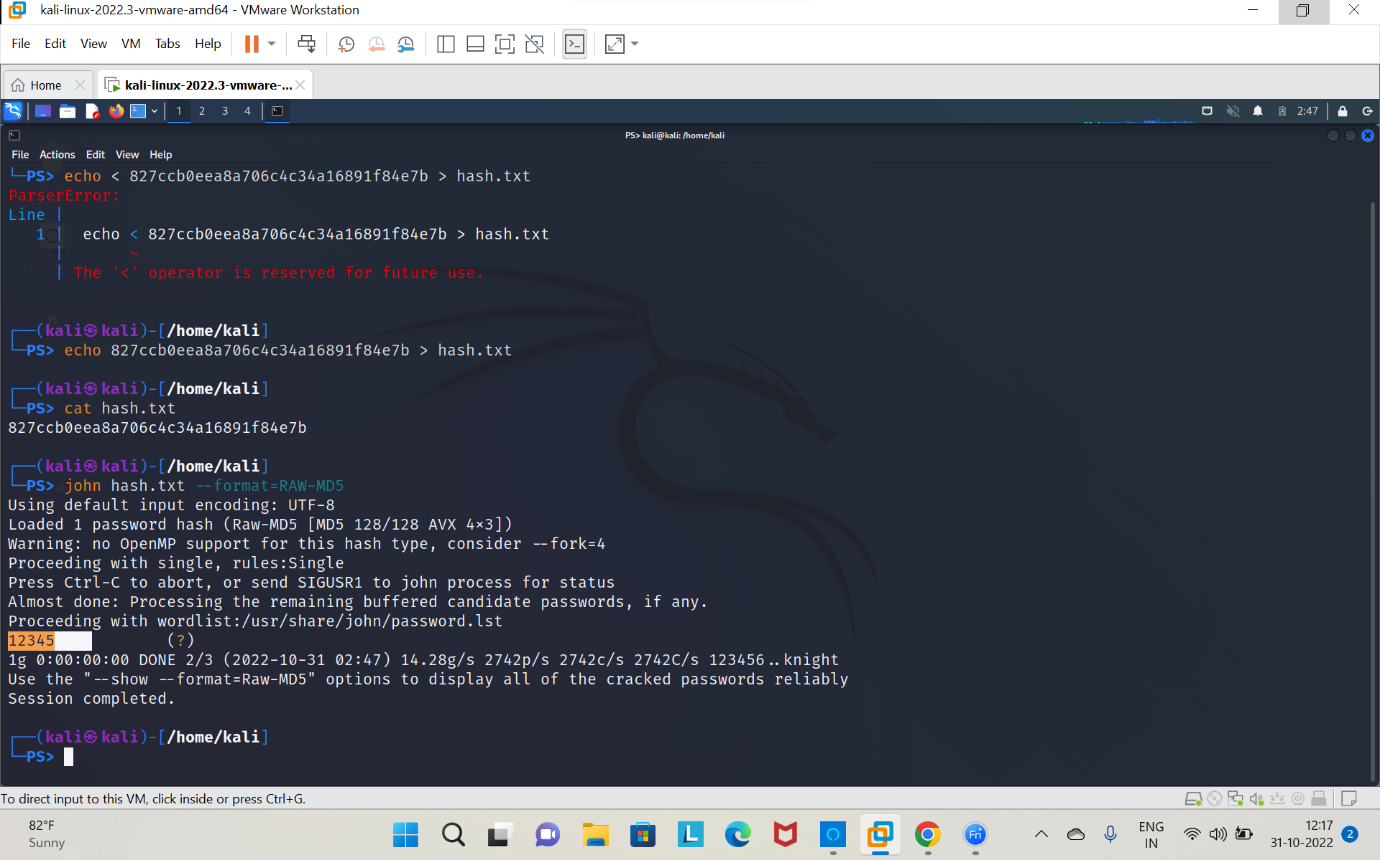
Now, let’s use the incremental mode:

john --format=Raw-MD5 --incremental=digits password\_digits.txt

The latter will search all possible combinations of digits. And since it was only a 6-digit password, it cracked it in less than one second.



Screenshot of john the ripper : -



Conclusion : -In this tutorial we have know how to use john the ripper with the help of kali linux to do attack,over here we have done hash attack.

PASSWORD GENERATING USING CRUNCH :-

Abstract :-

Crunch is a wordlist generator where you can specify a standard character set or any set of characters to be used in generating the wordlists. The wordlists are created through combination and permutation of a set of characters. You can determine the amount of characters and list size.

Objective : -

Crunch is a wordlist generating tool that comes pre-installed with Kali Linux. It is used to generate custom keywords based on wordlists. It generates a wordlist with permutation and combination. We could use some specific patterns and symbols to generate a wordlist.

Introduction :-

Often times attackers have the need to generate a wordlist based on certain criteria which are required for pentest scenarios like password spraying/brute-forcing. Other times it could be a trivial situation like directory enumeration. Crunch is a tool developed in C by **bofh28** that can create custom, highly modifiable wordlists that may aid an attacker in the situations mentioned above. It takes in min size, max size and alphanumeric character sets as input and generates any possible combination of words with or without meaning and writes it out in a text file. In this article, we’ll demonstrate crunch filters in detail.

Methodology : -

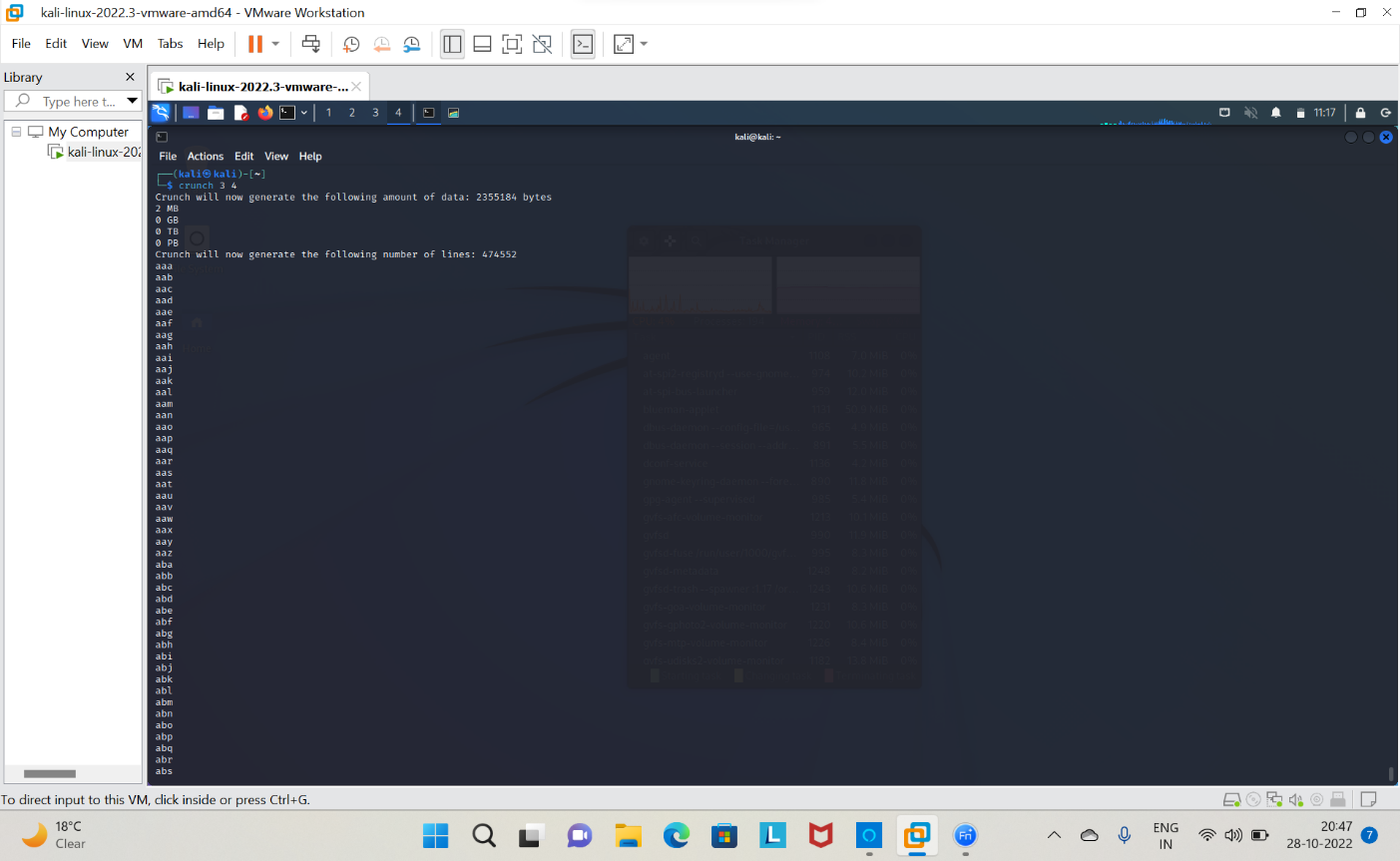
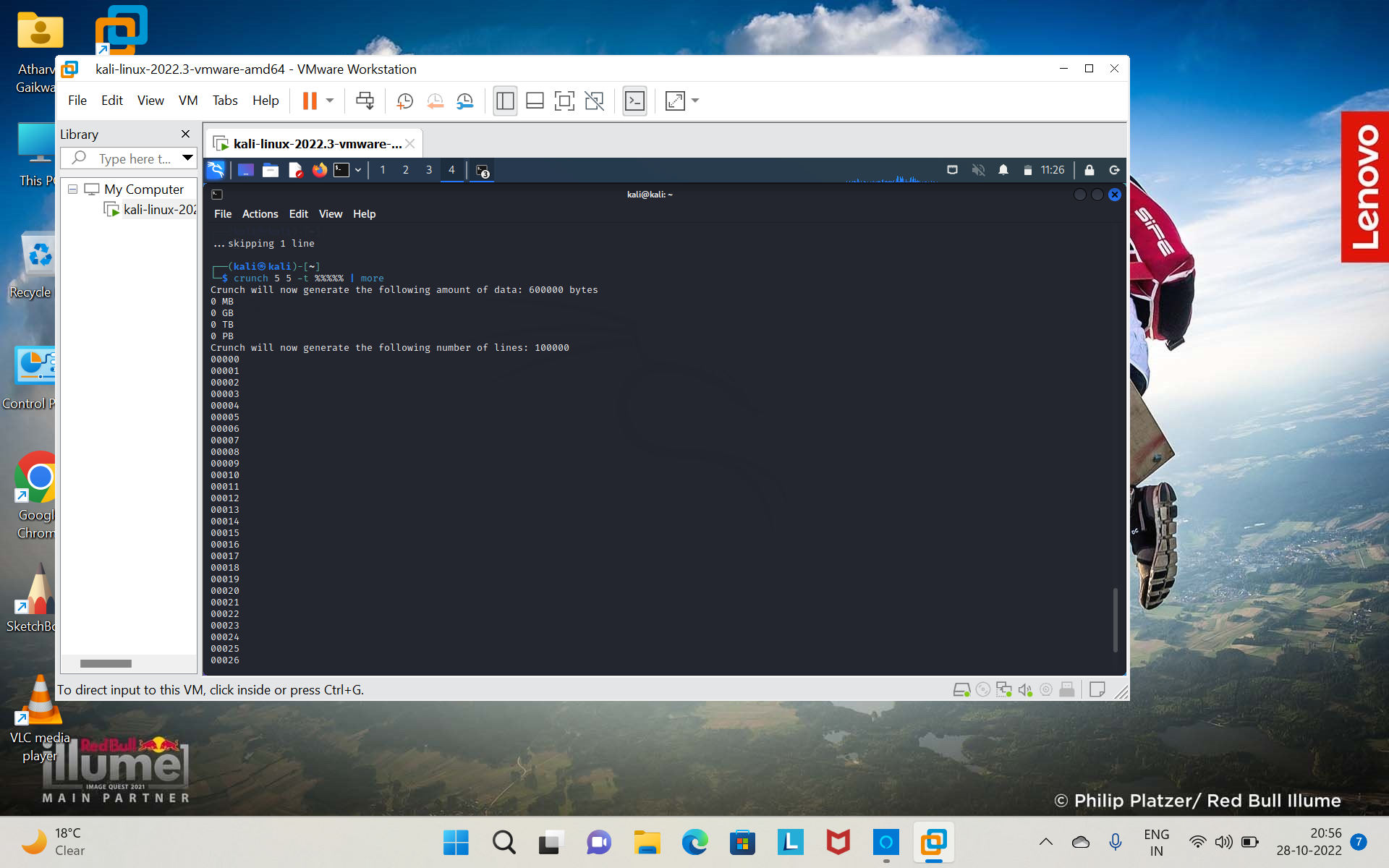
Installation and first run

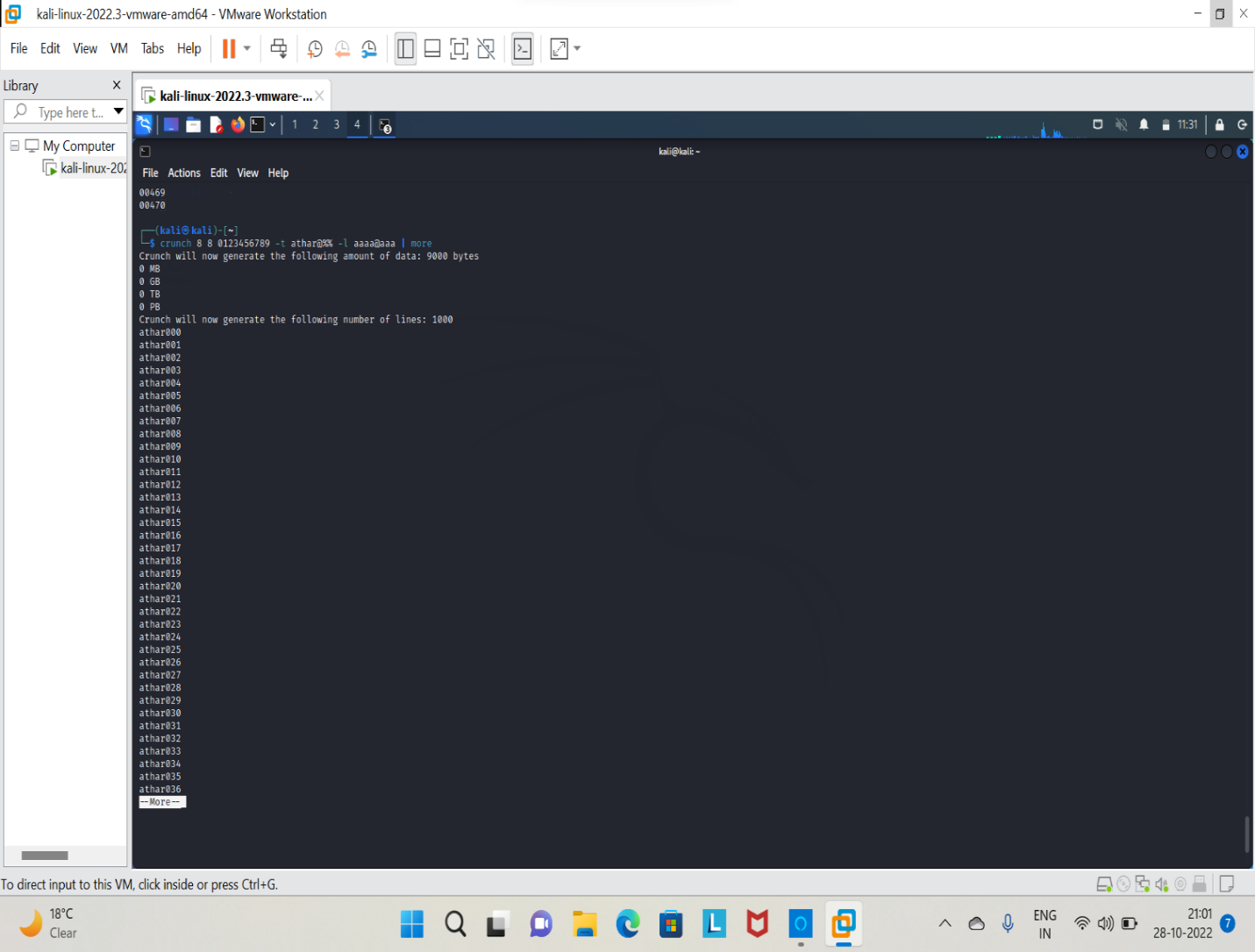
Crunch is installed by default on Kali Linux but can be installed using apt package manager using

apt install crunch

After it is installed, we can run crunch to generate a wordlist. When we input the min and max size of the word to be generated and just the output file, it automatically takes in small case alphabets as character sets and generates words.

Screeshot of Crunch Attack: -





Conclusion :-

The article is meant to be considered as a ready reference for quick and dirty wordlist generation using crunch. Crunch is a powerful and very fast tool written in C which is available by default in Kali Linux and is allowed to be used in competitive security certification exams. Hope you liked the article and thanks for reading it.