International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)

ISSN: 2456-236X

Vol. **04** Issue **02** |**2020**

Bypassing ownCloud AV and Hacking the Host using Kali Linux

SumukhShashidhar[1],ShrinikethDayalu[2]

[1,2] *Master Student, Department of MCA, Jain Deemed-to-be University, Bengaluru, Karnataka, India*

ABSTRACT

ownCloudAV is an application in ownCloud based on ClamAV. ClamAV is that of an open-source antivirus used for the detection of Trojans, virus, malware and other harmful malicious threats which occur. In this paper, we learn how to configure and secure ownCloud using ClamAV Antivirus. Cloud is a very lucrative and sought-after platform for the hackers as the gains from an exploited cloud platform is tremendous. Since there are numerous users active on a cloud platform at any given time, it makes it that much more necessary and harder to protect all that data from getting hacked.

ownCloud combines with these tools of antivirus by giving a connection to them via:

- ***A URL and port***
- ***A socket***
- ***In real-time the data from the command-line via the pipe path with an arranged to run by a computer.***

In this case ClamAV, ownCloud sends an antivirus file of extension through a stream to the ClamAVservice (which maybe the same on that of an ownCloud server or that of another server within that of the same network) which in turn scans them and returns a result to stdout.

The information is then parsed, or an exit code is evaluated if no result is available to determine the response from the scan. The OwnCloud response registering the idea of a correct step to be taken, such as that a recording a log message or detecting the referred file.

ClamAV is an open-source, multi-platform antivirus which supports multiple file-formats with file and archive unpacking. It detects multiple signature languages and is the only antivirus program supported by ownCloud. It also has command-line utilities for on-demand file support with automatic signature updates. It is a versatile antivirus with a multi-threaded daemon which makes it a great tool to keep your system secure.

1. INTRODUCTION

OwnCloud is a combination of client-server software used for creating and using file hosting services. The working of this is similar to the file service called Dropbox, which is majorly used everywhere. The only thing which is the difference in these two is that OwnCloud does not provide the data centre capacity to the host storage files. The server edition of this isfree and open-source, so anyone can install and operate it without using the private server.

ownCloud gives us universal access to our files through the web interface. ownCloud provides us with a platform to easily view contacts, calendars and bookmarks across all our devices. It is also easy to install with minimal server requirements. It doesn't need any special permissions. ownCloud is extendable via a powerful API for applications and plugins.

The default installed Ubuntu contains much software such as Libreoffice, Transmission etc. There are also two min games that are Sudoku and Chess. The additional packages which come along with this are can be accessed by the user which are also built-in's like APT based package management tools. There are some of the additional packages which are not installed by the default are as follows like SYNAPTIC, Evolution etc., But these are accessed and used by the user in the main tools or package tools management. There is a feature that the other packages which can be installed related to the MIRCOSOFT software Operating System. The default file manager is GNOME files. Formerly known as the Nautilus.

The developer of this ownCloud is ownCloud GmbH and community. The repository is found in github.com/ownCloud. This is actually written in PHP and JavaScript. The operating system used with the server is Linux and the Clients with interaction is off with Windows,macOS,Linux, Android, iOS. This is basically online storage of data. ownCloud AV is an application in ownCloud based on Clam AV.

Individual chunks are not scanned. The whole file is scanned when it is moved to the final location. Scanner exit status rules are mainly used to correct the errors when the ClamAV is made to run on a CLI mode. Scanner Output rules are mainly used in the low priority mode/or direct connection mode.

This toolkit provides scalable and flexible multi-threaded daemon. It is a command-line scanner and a tool for automatic updating via the Internet. These programs are based on a shared library distributed with ClamAV package. The virus database should be regularly updated.

The download supports extension that allows working in Google Drive, with that of an online document editing, calendar, contact synchronization and many more. The client'sconnection, limits of users, data storage capacity are only calculated and depended on the physical capabilities of the server.

ClamAV Antivirus is an open-source antivirus used to detect threats such as Trojans, malware, viruses. In this project, we learn how to configure and secure ownCloud using ClamAV Antivirus. Cloud is a very rewarding and desirable platform for the hackers as they gain so much from an exploited cloud platform. As there are numerous active users on a cloud platform, it makes it much more necessary and difficult to protect the data from getting hacked.

Kali Linux is a Linux distribution designed for penetration testing and digital forensics. This is developed and maintained by offensive security. The kernel type of this is that it is a Monolithic Kernel.

1.1 LITERATURE REVIEW

This paper is about bypassing ownCloud AV and hacking the host using Kali Linux.They are the producers of the script responsible for bypassing ownCloud AV and hacking the host using Kali Linux. The working of ownCloud AV and ClamAV Antivirus, and how to bypass it by hacking the host is explained in this paper. In this paper,the developer is using Ubuntu, Windows 10, Kali Linux Virtual Machines and Administrative privileges to run the tool. The mechanism used in this paper is, it uploads a malicious file into the ownCloud and breach all the security and hack the host. ownCloud AV or Clam AV detects multiple signature languages and is the only antivirus program supported by ownCloud. It also has command-line utilities for on-demand file support with automatic signature updates. It is a versatile antivirus with a multi-threaded daemon which makes it a great tool to keep your system secure.

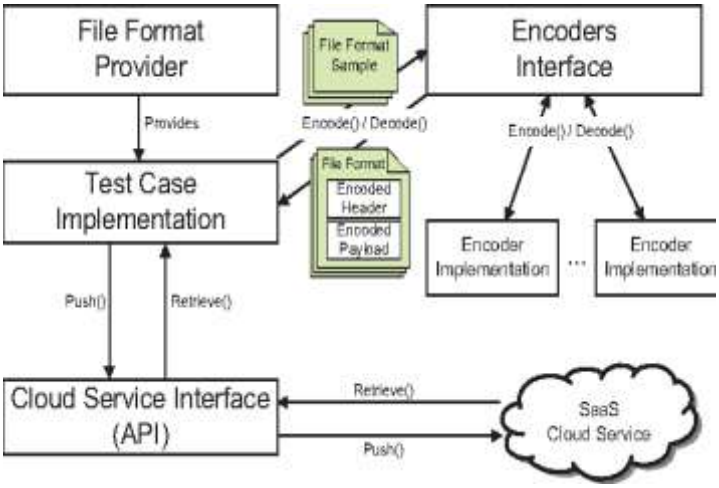

Fig-1: Cloud Concept of System's Architecture

2. ClamAV AND own cloud

ClamAV is an open-source and multi-platform antivirus which supports multiple file-formats with file and archive unpacking. ClamAV is the only antivirus program which supports ownCloud and it detects multiple signature languages. It also has command-line utilities for on-demand file support with automatic signature updates. It is a versatile antivirus with a multi-threaded daemon which makes it a great tool to keep your system secure. ClamAV includes various utilities such as command-line scanner, automatic database updater and so on.

The developer of this OwnCloud is OwnCloud GmbH and community. The repository is found in github.com/ownCloud. This is actually written in PHP and JavaScript. The operating system used with the server is Linux and the Clients with interaction is off with Windows,macOS,Linux, Android, iOS. This is basically online storage of data. OwnCloud AV is an application in ownCloud based on Clam AV.

The OwnCloud supports extension that allows working in Google Drive, with that ofan online document editing, calendar, contact synchronization and many more. The client's connection,limits of users,data storage capacity are only calculated and depended on the physical capabilities of the server. ClamAV is an antivirus toolkit used in Unix. The main purpose of this antivirus is the integration with mail servers.

2.1 Features of Hacking

- **Confidentiality:** It ensures that the information is accessible to authorized persons only. The reason for this is to protect the sensitivity of information from reaching unauthorized people. It maintains the privacy of the people and getting into the wrong hands. Encryption is the best example of this.
- **Availability:** Information should be available for the authorized person when the user requests. This makes sure that the information is only available for the authorized person only. The recovery measures, backup, and keeping the hardware and software in regular intact with updated features will make sure of the data available.
- **Integrity:** This maintains the proper and correctness or accuracy of the information where the data is in transit, processing and storage form. This makes sure the data is totally trusted worthy and not duplicated. This makes sure of the attribute that an unauthorized person cannot be able to modify the data. RSA digital signature is the best example of this.
- **Authentication:** This is basically the user, data, transaction involved is unique. This makes sure that the unique or the correct person is accessing it. Login thing can be used to verify the person of authority to access the data.

2.2 Features of Kali Linux

- **A Live System:** This live system contains the tools mostly used by the penetration testers. If the activities which are not in kali, you can simply insert the disk or USB drive and reboot to run in Kali. This will not default configuration will not make any changes between reboots. The things can be modified and kept it as a clean drive and save the report where the changes will be retained across reboots.
- **Forensic Mode:** When these kinds ofsensitivity of the data are working wouldn't want anyone to alter the data. But anyways the modern computers are capable of foreign interference in the system to make changes. To avoid this, Kali has a separate feature for this to enable these features which intern disables the other features.
- **Custom Linux Kernel:** this gives the customized Linux kernel based on the version the user need. This makes sure of the solid hardware support. These are very useful in the wireless support systems also of a wide range. Few of them are not installed by default because they are closed source and they are not the part of proper Linux.
- **Trustable Operating System:** The users of this distribution wants to know whether this can be trusted or not, because this has been developed on the plain sight, allowing anyone to see the source code. This is a very small team who are working transparently for better security. The packages are check and summed and then distributed as part of a signed repository.

2.3 Features of ownCloud

- **File-Sharing:** It is easy to share the files to anyone at any point of time using the ownCloud app on the mobile phone. We need not fire up our laptop, access the internet, access the VPN, start an email and attach the file. File Sharing can be done within few seconds using our mobile phone.
- **Syncing:**ownCloud keeps a track of all the file versions with the help of sync client that keeps the web, desktop and mobile device on the same page. The users need not worry about the latest file version even if they are away from their laptop. ownCloud actively monitors the changes in the files and pushes the latest version to all devices and all relevant users wherever they are.

3. Procedures to Bypass OwnCloud AV and hack the host

- Delete all the cookies in the browser in which you are hosting ownCloud.
- Start the Ubuntu machine and make sure the apache server is running.
- Start the Kali Linux virtual machine. Now log-in and launch the terminal window to create a payload file and hit Enter.
- The command creates the payload file on the desktop. Copy it to the shared folder, in the terminal window and hit Enter.
- Start the Apache webserver type service apache2 start and hit Enter. Then create and start the listener and now make the listener, first start the Metasploit console.
- Then the Metasploit framework is launched and hit Enter. Next specify the payload type, LHost, LPort and hit Enter.

- Now Start the listener and hit Enter. Leave the listener running and switch to windows 10 machine. Download the payload to upload in ownCloud by using windows 10 machine. This will help to download.
- Now from the same user account, we will upload the malicious file in ownCloud, same user account for ownCloud was configured in Windows 10. Now upload payload and Navigate to the shared folder in the ownCloud directory and then the downloaded exploit file of ownCloud automatically starts syncing the changes to the cloud.
- Now switch to Ubuntu machine and open browser. The admin user credentials will appear and enter it. Files page opens by default you will see the malicious file, click the download option.
- Now Opening exploit file pop-up appears to click the save file button to download this file on the victim machine hosting the ownCloud. Now open a terminal and you will be asked to enter the password, input your password and hit Enter.
- Now execute the exploit file and hit Enter. Switch back to kali Linux machine and open up the terminal window you will see that a command shell session has been established with the victim.
- Now leave the session to interact with the victim machine. You can also view the IP of the victims. You will be shown the victim's internet adapter configuration.
- To also get more information like the current working directory.
- View the system user and here you can see that we have the root user access to the victim's machine.

4. CONCLUSION

To conclude, Mini-Project "Bypassing ownCloudAV and hacking the host using Kali Linux". This project helps us to understand the different ways of attacking the host system and breaching its security hence gaining access to the host OS. Thus the project entitled above should include all the above-mentioned features and it is confirmed that it is up to the specifications entitled for the project.

Key features of this application: ownCloudAV protects the platform from malicious file uploads using ClamAV Antivirus. Threats which can be prevented from uploading are Trojans, Viruses, and Malware. Yet, with all the security there was still a minor vulnerability because of which the security of the system was breached.

5. ACKNOWLEDGEMENT

Weare sincerely thankful to Jain University for providing me with the opportunity to write a research paper on this topic. We are also thankful to Mr Subarna Panda, Assistant Professor and Dr Lakshmi JVN, Associate Professor for guiding me in every single stage of this research paper and supporting throughout the process in preparing a meaningful paper. We are also thankful to Dr.N.MNachappa (Head of School-CS& IT) of Jain (Deemed-to-be University) who have helped me during the course of this research paper in different ways. Through this paper, we have learnt how information security &ethical hacking function in different platform. It has helped me analyze how the information can be secured and its advantages and disadvantages.

6. REFERENCES

[1] https://linuxtechlab.com/install-clamav-clamtk-linux/
[2] https://www.quora.com/topic/ClamAV?q=clamav
[3] https://www.kali.org/downloads/
[4] https://ubuntu.com/download/desktop
[5] https://ownCloud.org/
[6] https://www.softpedia.com/get/Antivirus/ClamAV.shtml