CVE-2019-6447
Android Vulnerability in ES File Explorer

TANMAY TYAGI
University of Delhi
tanmay.tyagi8@gmail.com

I. INTRODUCTION

This Research paper will shed light on manual exploitation of ES File explorer vulnerability. This works on version v4.1.9.7.4. Allows the attackers on the same network to execute applications, read files and sensitive personal data. The application leaves TCP port 59777 open during runtime and responds to counterfeit requests over http. We will perform this in a virtual environment with proof of concept to get better understanding.

II. KEY TERMS

ES File Explorer, TCP ports, Metasploit Framework, CVE-2019-6447, Local Wifi network , HTTP requests/response

III. DEFINITIONS

[1] ES File Explorer
A file manager by a subsidiary of DO global i.e. ES Global. It is the most popular file manager on Android with over 100 million + installations. The Play Store removed it for click fraud.

[2] TCP ports
A port is a communication endpoint. It's not physical but a logical construct. Identifies type of network services. Now, a TCP port is a unique number assigned to certain applications or services. There are 65535 ports in the tcp/ip model. In our application i.e. ES file explorer, it uses port 59777.

[3] Metasploit Framework
It is owned by rapid7 which is a Boston, Massachusetts-based security company. It's a ruby based Open source framework which is a penetration testing aid. Used by DevSecOps Pros, white hat hackers.

MODULES:

a. Exploits - Tool used to take advantage or exploit the system vulnerabilities.
b. Payloads - Sets of malicious code that runs remotely.
c. Auxiliary Function - Supplementary tools and commands. Include port scanners, fuzzers, sniffers.
d. Encoders - Convert code or information.
e. Listeners - To gain access this malicious software hides itself.
f. Shellcode - It activates itself inside the target, at once.
g. Post-exploitation code - After gaining access we attempt to extend and elevate that access, using post exploitation scripts.
h. NOPS - Prevents the payload from crashing

[4] CVE-2019-6447
BASE SCORE - 8.1 HIGH
Current Description at NIST : The ES File Explorer File Manager application through 4.1.9.7.4 for Android allows remote attackers to read arbitrary files or execute applications via TCP port 59777 requests on the local Wi-Fi network. This TCP port remains open after the ES application has been launched once, and responds to unauthenticated application/json data over HTTP.

[5] Local Wifi Network
This works only if the attacker is on the same network as you are. Scenarios can be like at an airport using the open wifi without VPN, open wifi on coffee shops, restaurants, hotels. The attacker can easily scan the IPs on the network and attack at an open service.

[6] HTTP requests/response
There are two types of messages: Requests sent by clients and responses by the server. In HTTP messages the textual information is encoded in ascii. In earlier versions like HTTP/1.1 messages were sent across the connection openly. In latest versions, HTTP/2.0, the human readable message is divided into HTTP frames providing many performance improvements.
There are 4 main features :

a. Request Multiplexing - Multiple requests can be sent parallely.
b. Binary protocol - The headers are sent in binary form so the computer understands faster than before.
c. Header compression - It uses a more advanced method of header compression called HPACK, which eliminates redundant information in http header packets.
d. Server Push - If a client asks for a resource x and the server knows that x is related to y then it automatically pushes y with the x response to the client. This saves time.

Affected version :-
ES explorer = V4.1.9.7.4

Unaffected versions : -
ES explorer = V4.2.4.3.2
ES explorer < V4.1.9.7.4<ES explorer

Advisories/Solution/Mitigation -
ES explorer released many patched versions after the bug/vulnerability was reported in late 2019. Users are advised to upgrade to the latest version.

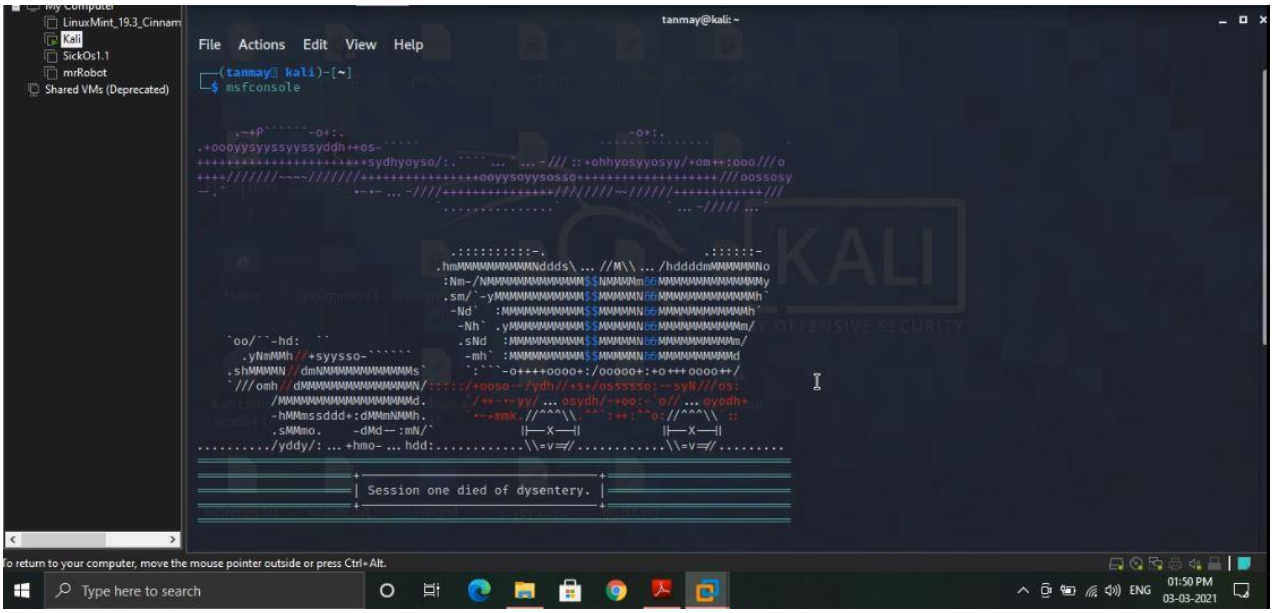
IV. VIRTUAL ENVIRONMENT

$ My setup was made like this - Kali Linux(Bridged mode) on the VM Workstation Pro as my attacking machine and my host machine was windows 10 home.
$ I downloaded the affected ES explorer version i.e. 4.1.9.7.4 and installed on my phone, this was the machine to be attacked.
$ Now both the machines should be on the same network.
$ Also the app must be running on the phone so that port 59777 remains open.

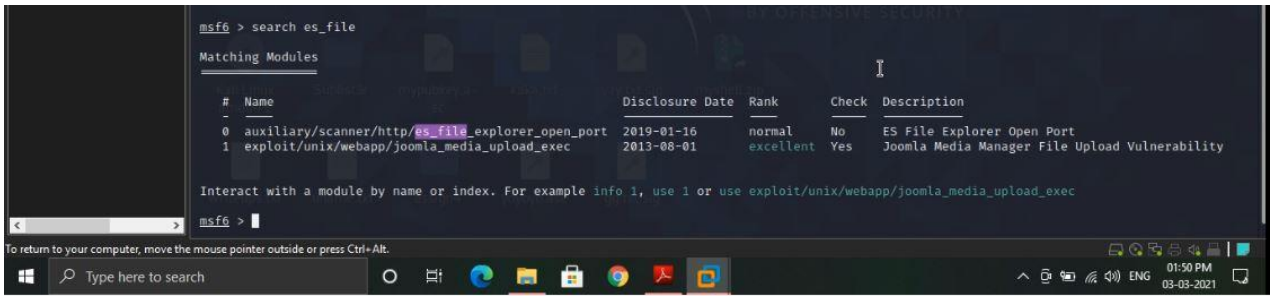
Let's begin with the Exploitation now.

V. EXPLOITATION

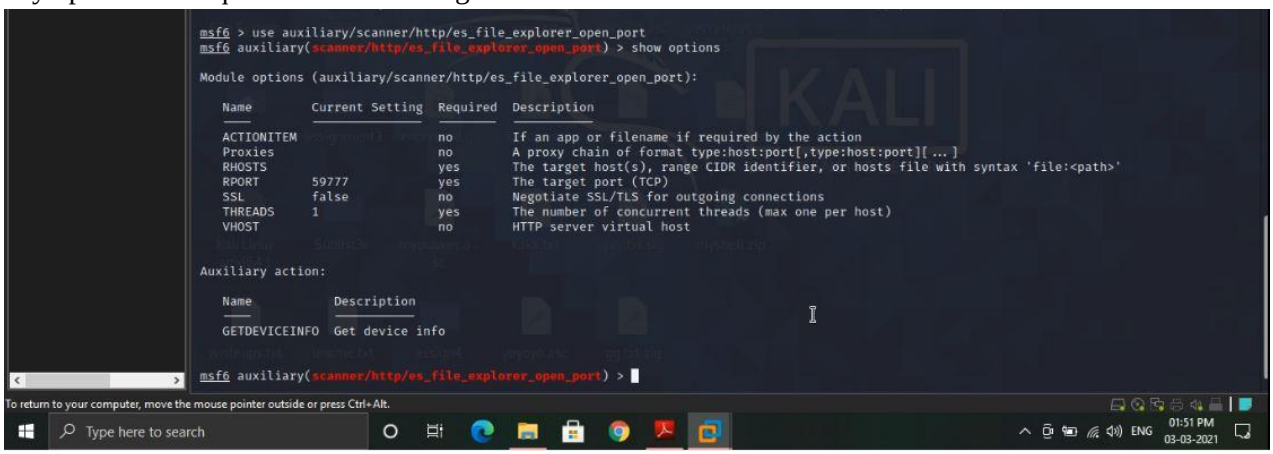
[1] I ran the msfconsole command in the terminal in kali as root. This starts the metasploit framework



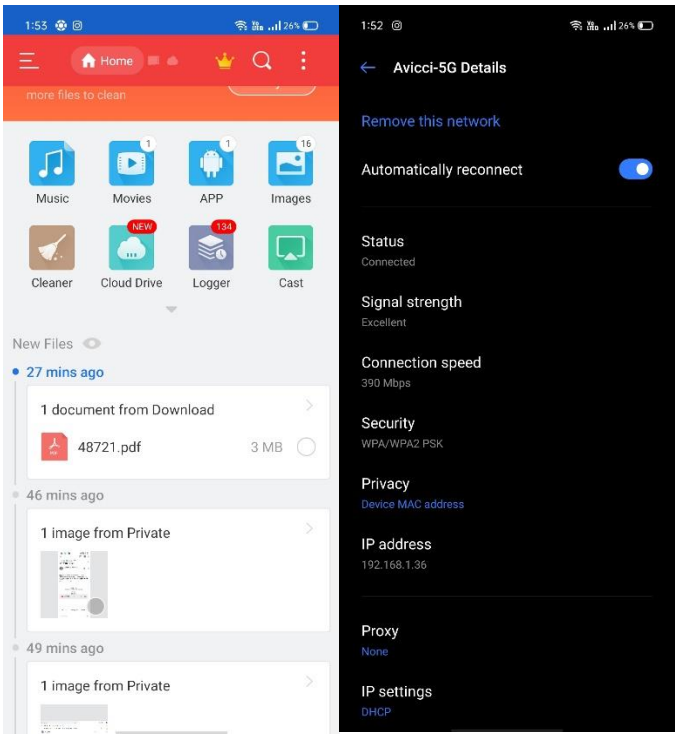
[2] Searched for Es_file exploit, to check if any exploit is available on metasploit database. Luckily it was!

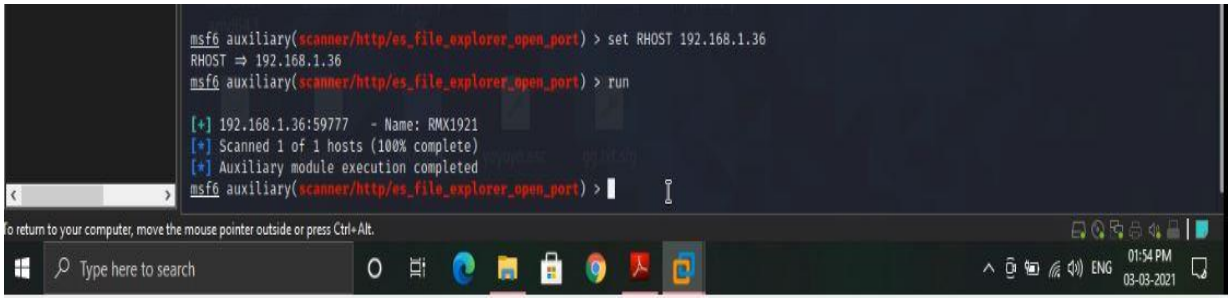


[3] I ran use [exploit_name]. I got the name from the previous command. Then I ran, show options to check if any options are required before running.

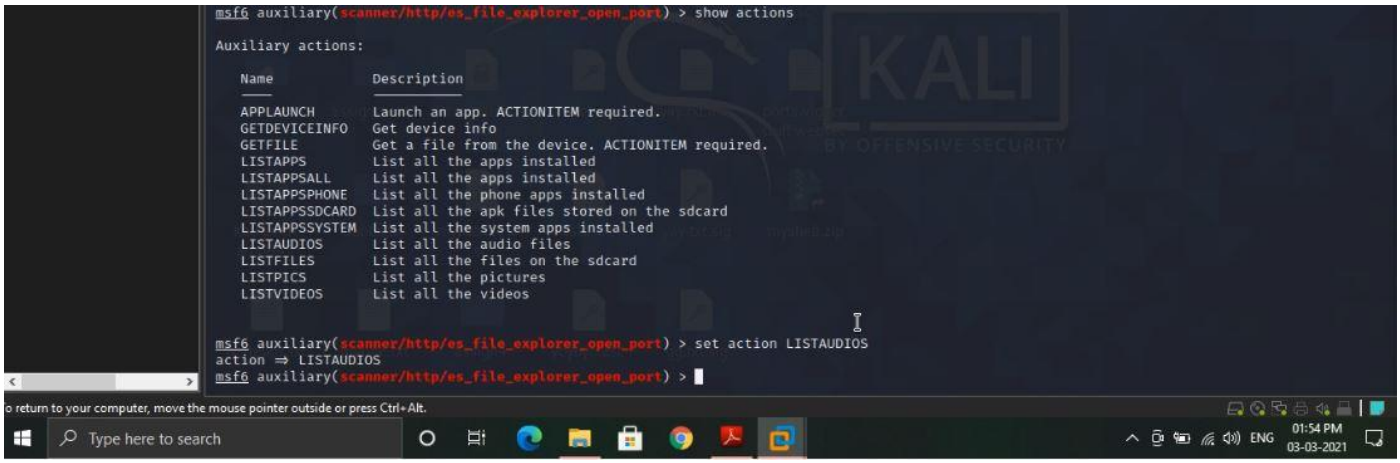


[4] So as we can see RPORT is already set to 59777, we need to set RHOST though. Now we need to run set RHOST <IPADDRESS>, which in this case is my phone's ip. So firstly I checked it (it was 192.168.1.36) and then ran the command.
Also the es file app has to run this whole time and should be on the same wifi. (I attached a screenshot of it too)
After that I ran "RUN" and could see the details of my mobile.

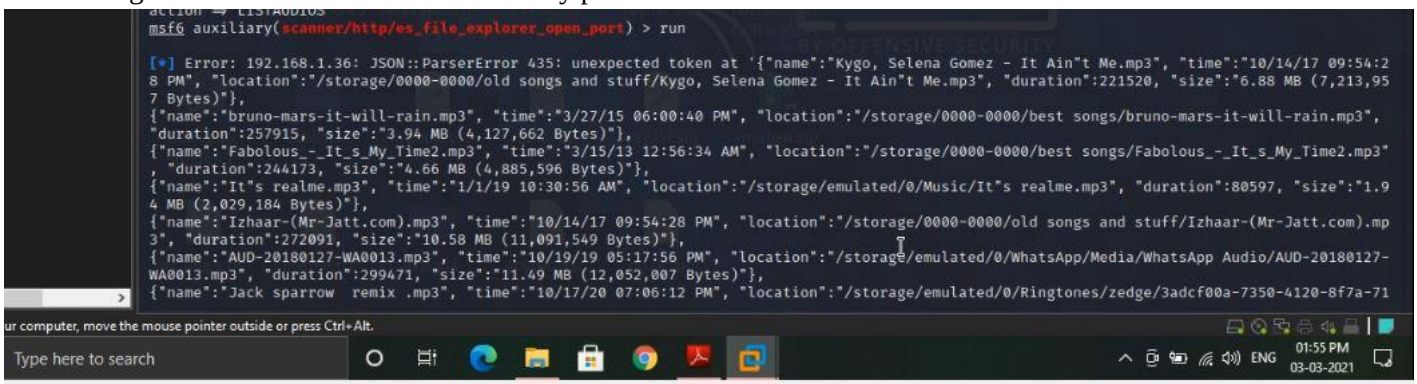




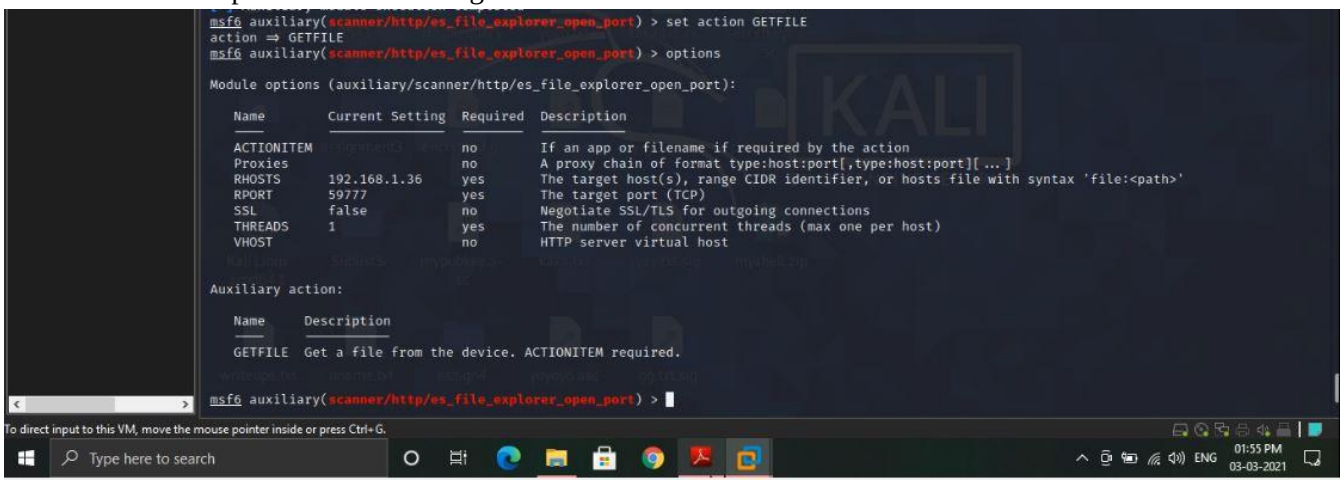
[5] Now run show actions to check available actions we can perform on the device.
Now from these I wanted to access the audio files. So ran set action LISTAUDIOS.



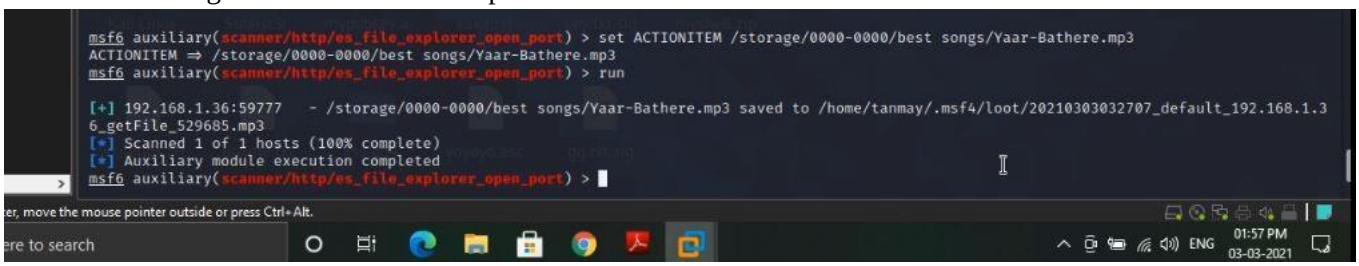
[6] Now we are all set. Give ‘RUN’ command.
See !! We got all the audio files that were on my phone.



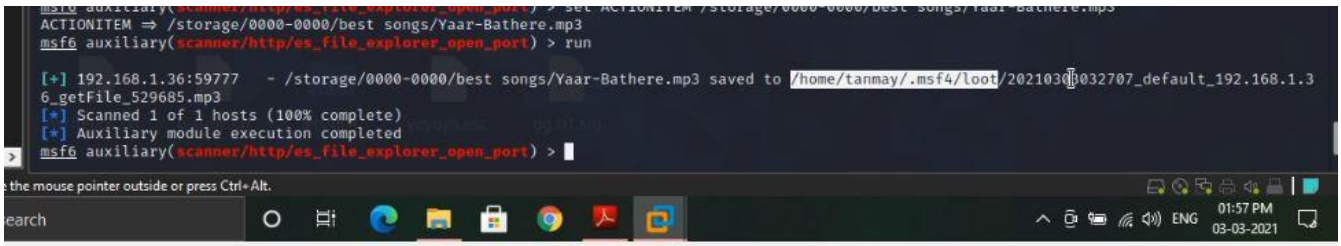
[7] Now we can download any file. Need to use GETFILE action with command set action GETFILE and also have to check the options before running.



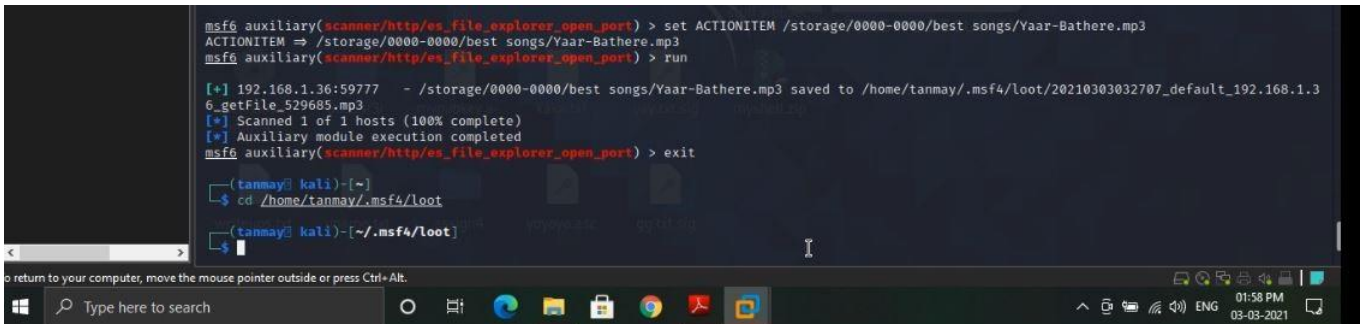
[8] Now as we can see we need to use ACTIONITEM. SO run set ACTIONITEM <location of file you want to download>.
Then simply type ‘run’ command.
And see! the file gets downloaded in our pc.

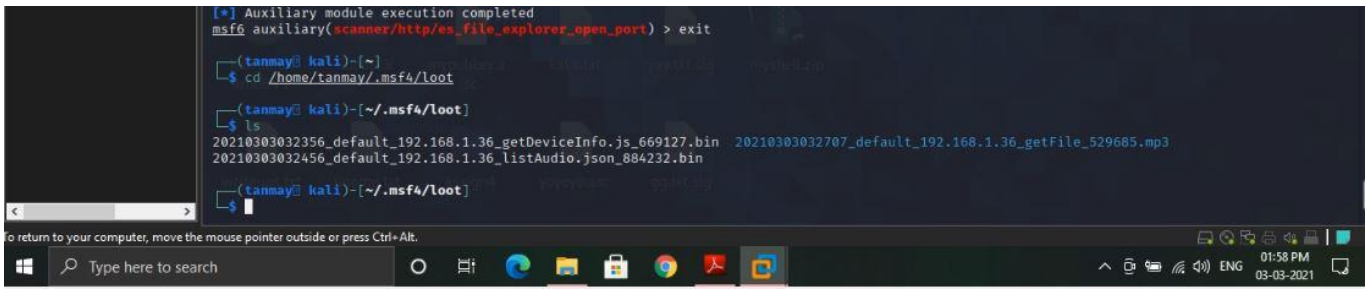


[9] Now let’s copy the location where it has been downloaded and check out the file after exiting from msfconsole.



Here I changed the directory where the file was downloaded





As you can see in the above screenshot, I got a user’s personal audio file without the user's permission or knowledge.

Now this was just an audio file, you can access anything like videos, files and moreover you can launch an app remotely.

VI. REFERENCES

JAVAPOINT.COM : TCP-PORT
WIKIPEDIA.ORG: ES_FILE_EXPLORER
VARONIS.COM : WHAT_IS_METASPLOIT
OFFENSIVESECURITY.COM : METASPLOIT_MODULES
SCIENCEDIRECT.COM : POST_EXPLOITATION
NVD.NIST.GOV : CVE-2019-6447
DEVELOPER.MOZILLA.ORG : HTTP
CLOUDFARE.COM : PERFORMANCE_HTTP2.0