Relatório de CTF

UltraTech - TryHackMe

Informações do documento	
Referência	CTF de estudo – Gabriel Garritano de Mendonça Villela
N° Revisão	1
Data de publicação	01/09/2025
Link	https://tryhackme.com/room/ultratech1

Redação	Gabriel Garritano	Estudante
Revisão	Nome do revisor	Orientador
Aprovação	Nome do aprovador	Diretor

Histórico de revisões		
N°	**Entregas**	**Descrição**
0	DD/MM/AAAA	Produção
1	DD/MM/AAAA	Revisão
2	DD/MM/AAAA	Aprovação

Informações do CTF	
Nível de Dificuldade	Médio
Tipo de acesso	Gratuito
Conceitos envolvidos	WebHacking
Plataforma	TryHackMe
Área	Red Team

Sumário

Contextualização

Conceitos utilizados

Desenvolvimento

It's enumeration time!

Let the fun begin

The root of all evil

Conclusão

Contextualização

You have been contracted by UltraTech to pentest their infrastructure.

It is a grey-box kind of assessment, the only information you have

is the company's name and their server's IP address.

Conceitos utilizados

Mapeamento de portas

Exploração de diretórios

Manipulação de URL para execução remota de códigos

Associação de hash à senhas

Escalonamento de privilégios

Desenvolvimento

It's enumeration time!

Para a primeira tarefa precisa-se encontrar cinco respostas: Qual serviço roda na porta 8081, qual a porta não padrão utilizada, qual software roda nesta porta, a distribuição Linux do servidor e quantas rotas da api REST está sendo redirecionada para a aplicação web.

Para realizar esta tarefa foi utilizada a ferramenta de escaneamento de portas nmap. Bastou rodar o comando para encontrar as respostas de 1 a 4. A quinta pergunta será respondida no próximo tópico.

1: Node.js

2: 31331

3: Apache

4: Ubuntu

Let the fun begin

Agora, é necessário responder a três perguntas. Qual o filename do banco de dados, o hash da senha do primeiro usuário e sua respectiva senha. A primeira etapa é utilizar um explorador de diretórios na aplicação web. Na porta 8081 encontra-se a API Node.js no qual a aplicação da porta 31331 está rodando.

Para procurar o nome do banco de dados, utiliza-se uma ferramenta de exploração de diretórios em aplicações web. Utilizando o gobuster no endereço com a porta 8081 encontram-se apenas os diretórios /auth e /ping. Dessa forma, responde-se também a quinta pergunta da primeira etapa, que há apenas duas rotas da API sendo redirecionadas para a aplicação. Acessando a /ping encontra-se o seguinte erro (Imagem 1):

```
TypeError: Cannot read property 'replace' of undefined
    at app.get (/home/www/api/index.js:45:29)
    at Layer.handle [as handle_request] (/home/www/api/node_modules/express/lib/router/layer.js:95:5)
    at next (/home/www/api/node_modules/express/lib/router/route.js:137:13)
    at Route.dispatch (/home/www/api/node_modules/express/lib/router/route.js:112:3)
    at Layer.handle [as handle_request] (/home/www/api/node_modules/express/lib/router/layer.js:95:5)
    at /home/www/api/node_modules/express/lib/router/index.js:281:22
    at Function.process_params (/home/www/api/node_modules/express/lib/router/index.js:335:12)
    at next (/home/www/api/node_modules/express/lib/router/index.js:275:10)
    at cors (/home/www/api/node_modules/cors/lib/index.js:188:7)
    at /home/www/api/node_modules/cors/lib/index.js:224:17
```

Como o ping na URL é um comando linux sendo executado na máquina alvo via API, podemos tentar explorar a URL para executar comandos remotamente. Adicionando ?ip=`whoami` após “ping” encontra-se o seguinte resultado: “ping: www: Temporary failure in name resolution “, o output do comando whoami + um erro na execução do ping. Como precisamos extrair informações relacionadas a um banco de dados, buscaremos se este se encontra no mesmo diretório da aplicação web. Alterando “whoami” para “ls” no parâmetro da URL encontra-se: utech.db.sqlite. Este, é o nome da Database, respondendo a primeira pergunta da segunda etapa. Para descobrir o que está registrado neste arquivo, ?ip=`less utech.db.sqlite`

```
ping: ) ���(Mr00tf357a0c52799563c7c7b76c1e7543a32)Madmin0d0ea5111e3c1def594c1684e3b9be84: Parameter string not correctly encoded
```

Ou seja, encontramos a hash para o usuário r00t e para admin. Respondendo assim, qual a hash do primeiro usuário: f357a0c52799563c7c7b76c1e7543a32.

Para descobrir a senha associada a este hash, utiliza-se uma ferramenta de decodificação como hashcat ou john. Utilizando o john, encontra-se a senha n100906, respondendo a última questão da segunda etapa.

The root of all evil

Para responder a última pergunta é necessário acessar o servidor via protocolo SSH. Utilizando o usuário r00t e a senha n100906, consegue-se a conexão. O comando id mostra os serviços com privilégio de acesso a /root. O serviço docker está rodando como root. Utilizando GTFOBins encontra-se o comando que pode ser utilizado para aproveitar-se deste privilégio e conseguir acesso. Utiliza-se o comando docker run -v /:/mnt --rm -it alpine chroot /mnt sh para conseguir o acesso. Por último, agora já com privilégio de super-usuário basta explorar o diretório root com ls -la e acessar a chave privada com less /root/.ssh/id_rsa. Respondendo no TryHackMe os nove primeiros carácteres da chave resolve-se por fim a sala inteira. MIIEogIBA

Conclusão

Caso a situação apresentada fosse uma situação real, medidas de segurança seriam necessárias. O maior erro na configuração que comprometeu a segurança foi a falta de filtragem na URL da /ping que possibilitou acesso ao conteúdo do utech.db.sqlite. Na montagem da página web, seria necessário filtrar o que poderia ser executado.