Logotipo

Descrição gerada automaticamente com confiança baixa

Relatório de CTF

Valley – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Valley CTF – João Vitor Ferrenha |
| **N° Revisão** | 1 |
| **Data de publicação** | 14/10/2025 |
| **Link** | https://tryhackme.com |

|  |  |  |
| --- | --- | --- |
| **Redação** | João Vitor Ferrenha | 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, redes, privesc |
| **Plataforma** | TryHackMe |
| **Área** | Red |

**Sumário**

[Contextualização 3](#_heading=h.gjdgxs)

[Desenvolvimento 3](#_heading=h.1fob9te)

[Pergunta 1 3](#_heading=h.3znysh7)

[Pergunta 2 3](#_heading=h.2et92p0)

[Pergunta 3 3](#_heading=h.tyjcwt)

[Pergunta 4 3](#_heading=h.3dy6vkm)

[Conclusão 3](#_heading=h.1t3h5sf)

[Referências 3](#_heading=h.4d34og8)

**Contextualização**

A sala Valley do TryHackMe propõe um cenário de segurança ofensiva com foco em enumeração web, coleta de credenciais a partir de artefatos expostos (código‑fonte e tráfego capturado), e escalada local usando análise de binário estático e abuso de permissões/grupos em Linux. O objetivo foi conquistar acesso inicial ao host, elevar privilégios até root e capturar as flags user e root, documentando a cadeia de exploração e as respectivas evidências.

Principais tópicos trabalhados: enumeração HTTP/FTP, leitura de código front‑end, manipulação de wordlists, análise de PCAP, uso de strings/UPX, reconhecimento de SUIDs, inspeção de cron/grupos e *module hijacking* em Python (import path).

**Desenvolvimento**

**Reconhecimento e enumeração:**

De inicio foi feito a enumeração de portas e serviços utilizando o nmap:

Texto

O conteúdo gerado por IA pode estar incorreto.

Com isso sabe-se que temos 2 serviços conhecidos nas portas 22 e 80 (ssh e http). O próximo passo que foi feito após a descoberta do http foi a enumeração e diretório. Segue a imagem abaixo:

Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

**Exploração inicial:**

A primeira ação foi abrir o navegador e ir até a página do serviço web:

Linha do tempo

O conteúdo gerado por IA pode estar incorreto.

De primeira vista pode-se notar que o site trata-se de uma galeria de fotos. Olhando o código fonte da página não encontrei nada valioso. parti para a página de galeria:

Interface gráfica do usuário, Site

O conteúdo gerado por IA pode estar incorreto.

Olhando o código fonte da página:

Texto

O conteúdo gerado por IA pode estar incorreto.

Pode-se notar que as imagens estão indexadas por números que são passados na url: <http://ip/gallery/static/index>. Isso levou a primeira tentativa de um fuzzing manual, testando outros index, com a intenção de “quebrar” a aplicação e ver como ela reage. Tentando alguns indexes consegui uma nota:

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

é possível notar um diretório e alguém dizendo que é para checar os logs do SIEM. Ao acessar o diretório:

Interface gráfica do usuário, Aplicativo, Site

O conteúdo gerado por IA pode estar incorreto.

Sem sucesso, tentei algumas senhas padrões como “admin” e outras do tipo. Então observei o código-fonte da página:

Texto

O conteúdo gerado por IA pode estar incorreto.

O site está validando no código que está exposto no front-end se o usuário é “siemDev” e a senha é “california”, se for ele muda para um outro diretório, então ao acessar:

Interface gráfica do usuário, Texto, Aplicativo

O conteúdo gerado por IA pode estar incorreto.

O bilhete fala sobre parar de usar credenciais, se atentar em updates e trocar a porta de ftp padrão, nesse momento rodei um outro nmap para confirmar o ftp:

Texto

O conteúdo gerado por IA pode estar incorreto.

Então loguei via FTP no servidor:

Texto

O conteúdo gerado por IA pode estar incorreto.

Segui a dica e reutilizei a senha e usuário para logar, no servidor consegui extrair arquivos de captura de pacotes (confirmando a dica dos logs do siem):

Texto

O conteúdo gerado por IA pode estar incorreto.

Fui para análise dos pacotes, em “siemftp.pcap” não foi encontrado nada de valioso, porém no “http1.pcap” foi encontrado mais credenciais em um pacote post http:

Texto

O conteúdo gerado por IA pode estar incorreto.

**Exploração logando no servidor via shh:**

Seguindo mais uma vez a dica do ctf, tentei logar via ssh usando essas credenciais:

Texto

O conteúdo gerado por IA pode estar incorreto.

Pegando a primeira flag:

Texto

O conteúdo gerado por IA pode estar incorreto.

Agora o próximo objetivo é escalar os privilégios. Primeira coisa que foi feita foi rodar um “sudo -l” e descobri que o usuário não pode rodar comandos com sudo, olhando os grupos usando “id” também não achei nada de valioso. Rodei também um comando para buscar por bits suid (quando o bit está setado o arquivo pode rodar com permissões de root mesmo sem o usuário ser root):

Texto

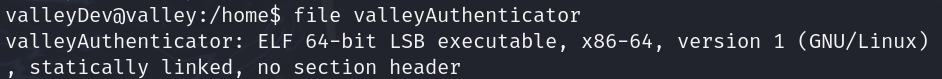
O conteúdo gerado por IA pode estar incorreto.

Conferi esses binários no site GFTO BINS e não encontrei nada de útil, tentei também ver as versões que estavam rodando mas não achei nenhuma vulnerabilidade. Decidi voltar e procurar mais coisas, comecei a navegar pelo servidor e voltando um diretório tinham alguns outros diretórios:

Texto

O conteúdo gerado por IA pode estar incorreto.

Não tinha permissão para entrar nos diretórios, e notei que o “valleyAuthenticator” era um executável:



Rodando o executável:

Texto

O conteúdo gerado por IA pode estar incorreto.

Até tentei com as outras credenciais mas sem sucesso. Então tentei rodar o comando “strings” para procurar strings, mas o server não tinha o programa. Então subi um srever usando python e baixei o executavel para a minha maquina:  
Texto

O conteúdo gerado por IA pode estar incorreto.

Texto

O conteúdo gerado por IA pode estar incorreto.

Ao rodar o “strings”:

Uma imagem contendo Texto

O conteúdo gerado por IA pode estar incorreto.

Olhando não consegui, a primeira vista observar nada, até porque estava bem desorganizado, normalmente retorna-se strings mais “legiveis” e isso me levou a pensar que talvez estaria compactado, ao ler as ultimas duas linhas pode-se notar que está escrito “upx” um jeito de comprimir arquivos. Para descomprimir “upx -d valleyAuthenticator”. Depois “strings” de novo:

Texto

O conteúdo gerado por IA pode estar incorreto.

Observando pode-se notar a existencia de duas linhas que se parecem hashes de senha, decodificando:

Interface gráfica do usuário, Texto, Aplicativo, chat ou mensagem de texto

O conteúdo gerado por IA pode estar incorreto.

Interface gráfica do usuário, Texto, Aplicativo, chat ou mensagem de texto

O conteúdo gerado por IA pode estar incorreto.

Mais um usuário e senha, após isso loguei de novo no ssh só que com esse outro usuário e acessei seu diretório:

Texto

O conteúdo gerado por IA pode estar incorreto.

Ao checar o id percebe-se o grupo “valleyAdmin” o que me leva a suseitar de algo relacionado a ele por conta do “admin”. Meu próximo passo foi ir atrás de outro jeito para escalar os privilégios, tentei ver a crontab:

Texto

O conteúdo gerado por IA pode estar incorreto.

Tem um arquivo diferente em python na última linha do arquivo:

Texto

O conteúdo gerado por IA pode estar incorreto.

Porém não temos permissão para alterar esse arquivo, então voltei para o grupo:

Interface gráfica do usuário, Texto

O conteúdo gerado por IA pode estar incorreto.

Achei dois arquivos que pertencem a esse grupo, pode-se notar que podemos editar o arquivo da biblioteca do base64, que está sendo usado no código que está rodando na crontab. Nesse caso vou modificar/adicionar um script nesse script de forma que eu consiga uma shell de root:

Texto

O conteúdo gerado por IA pode estar incorreto.

Depois foi só rodar o comando e pegar a flag:

Texto

O conteúdo gerado por IA pode estar incorreto.

**Conclusão**

A exploração do Valley evidenciou a importância da enumeração disciplinada e do encadeamento de pistas: (1) leitura do código‑fonte levou a credenciais e a FTP; (2) PCAP revelou novas credenciais para SSH; (3) a análise de binário estático exposto forneceu ainda mais material; e (4) a compreensão de permissões/grupos viabilizou o hijack de módulo Python, culminando em root. O caso reforça práticas de defesa: proteger segredos, endereçar superfícies expostas, endurecer permissões e revisar rotinas automatizadas.

**Referências**

TryHackMe – Valley (sala): documentação e enunciado da atividade.

GTFOBins — técnicas de abuso de binários em sudo -l: https://gtfobins.github.io/

UPX — packer/desempacotamento de executáveis: https://upx.github.io/

Wireshark Docs — análise de PCAP/HTTP: https://www.wireshark.org/docs/

Python Module Search Path — sys.path e import precedence: https://docs.python.org/3/tutorial/modules.html#the-module-search-path

Cron — tarefas agendadas e segurança: man 5 crontab, man 8 cron