Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Agent Sudo – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Agent Sudo – Sérgio Guidi Trovo |
| **N° Revisão** | 1 |
| **Data de publicação** | 29/08/2024 |
| **Link** | <https://tryhackme.com/r/room/agentsudoctf> |

|  |  |  |
| --- | --- | --- |
| **Redação** | Sérgio Guidi Trovo | 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 |

**Sumário**

[Contextualização 3](#_Toc175842400)

[Pergunta 1 - How many open ports? 3](#_Toc175842401)

[Pergunta 2 - How you redirect yourself to a secret page? 3](#_Toc175842402)

[Pergunta 3 - What is the agent name? 4](#_Toc175842403)

[Pergunta 4 - FTP password 4](#_Toc175842404)

[Pergunta 5 - Zip file password 5](#_Toc175842405)

[Pergunta 6 - steg password 6](#_Toc175842406)

[Pergunta 7 - Who is the other agent (in full name)? 6](#_Toc175842407)

[Pergunta 8 - SSH password 7](#_Toc175842408)

[Pergunta 9 - What is the user flag? 7](#_Toc175842409)

[Pergunta 9 - What is the incident of the photo called? 8](#_Toc175842410)

[Pergunta 10 - CVE number for the escalation 9](#_Toc175842411)

[Pergunta 11 - What is the root flag? 9](#_Toc175842412)

[Pergunta 12 - (Bonus) Who is Agent R? 10](#_Toc175842413)

[Conclusão 10](#_Toc175842414)

[Referências 10](#_Toc175842415)

Contextualização

O CTF Agent Sudo é um CTF de nível de dificuldade fácil que aborda partes importantes do processo de pentesting, com foco em enumeração, hash cracking e privilege escalation.

**Desenvolvimento**

Pergunta 1 - How many open ports?Parte superior do formulário

Começamos a resolução do CTF realizando um nmap para verificar as portas abertas.

Texto

Descrição gerada automaticamente

Identificamos três portas abertas rodando os serviços ftp, ssh e http.

Pergunta 2 - How you redirect yourself to a secret page?

**Parte superior do formulário**

Acessamos o serviço web para verificar possíveis vulnerabilidades.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

No contexto de serviços web, o user-agent é o software ou cliente que está fazendo a requisição para o site. Podemos tentar trocar o user-agent para fazer a requisição como um usuário diferente utilizando o comando *curl -A*. Considerando que o user-agent do usuário que nos deixou a mensagem é R:

Texto

Descrição gerada automaticamente

Pergunta 3 - What is the agent name?

**Parte superior do formulário**

Verificando que existem 25 funcionários, podemos utilizar as outras 25 letras do alfabeto como user-agent. Fazendo isso, encontramos o usuário chris.

Texto

Descrição gerada automaticamente

Pergunta 4 - FTP password

**Parte superior do formulário**

Podemos utilizar a ferramenta hydra para tentar brute-force a senha do usuário chris na porta com o serviço ftp.

Texto

Descrição gerada automaticamente

Pergunta 5 - Zip file password

**Parte superior do formulário**

Agora podemos nos conectar com servidor via ftp utilizando as credenciais encontradas.

Texto

Descrição gerada automaticamente

Explorando o sistema encontramos três arquivos, sendo um arquivo de texto e dois arquivos de imagem. Podemos fazer o download dos arquivos encontrados na nossa máquina utilizando o comando *mget*.

Texto

Descrição gerada automaticamente

Acessando a file texto To\_agentJ.txt:

Texto

Descrição gerada automaticamente

Podemos utilizar o comando *binwalk* para verificar arquivos anexados nas imagens encontradas. Fazendo isso, encontramos um arquivo zip 8702.zip anexado a foto cutie.png.

Texto

Descrição gerada automaticamente

Para extrair o arquivo zip encontrado precisamos de uma senha. Podemos utilizar john the ripper para encontrar essa senha.



Texto

Descrição gerada automaticamente

Utilizando john encontramos a senha alien.

Pergunta 6 - steg password

Parte superior do formulário

Extraindo o arquivo zip encontramos a file To\_agentR.txt.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Podemos decodificar a mensagem usando um base64 decoder.

Texto

Descrição gerada automaticamente

Encontramos a senha Aera51.

Pergunta 7 - Who is the other agent (in full name)?

O comando steghide permite é uma ferramenta do Linux que permite esconder informações em files. Podemos utilizar esse comando para verificar informações secretas na imagem cute-alien.jpg. Para isso, utilizamos a senha encontrada Area51.

Texto

Descrição gerada automaticamente

Encontramos a file message.txt que estava escondida na imagem cute-alien.jpg. Podemos utilizar o comando steghide para fazer o download dessa file.

Texto

Descrição gerada automaticamente

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Verificando a file message.txt encontramos um novo usuário James.VVParte superior do formulário]

Pergunta 8 - SSH password

No arquivo message.txt verificamos a senha para o usuário james no serviço ssh: hackerrules!

Pergunta 9 - What is the user flag?Parte superior do formulário

Podemos utilizar as credenciais encontradas para nos conectar com o servidor via ssh.

Texto

Descrição gerada automaticamente

Explorando os arquivos, encontramos a flag de usuário.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Pergunta 9 - What is the incident of the photo called?Parte superior do formulárioParte superior do formulário

Também encontramos a imagem Alien\_autospy.jpg. Podemos transferir essa imagem para a nossa máquina.

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Abrindo a imagem:

Foto em preto e branco deitado de barriga para cima

Descrição gerada automaticamente com confiança média

Utilizando o site ReverseImage encontramos que o evento é conhecido como Roswell alien autopsy.

Pergunta 10 - CVE number for the escalation Parte superior do formulárioParte superior do formulário

Verificando os commandos executáveis como administrador descobrimos que podemos utilizar qualquer comando.

Texto

Descrição gerada automaticamente

Pesquisando encontramos que a CVE dessa escalação é CVE-2019-14287.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Pergunta 11 - What is the root flag?Parte superior do formulárioParte superior do formulário

Basta mudarmos para o usuário root e então conseguimos pegar a flag de root.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Pergunta 12 - (Bonus) Who is Agent R?Parte superior do formulárioParte superior do formulário

Na file root.txt podemos encontrar também o nome do agente R: DesKel.

Conclusão

O CTF Agent Sudo é um CTF muito bom para aprender conceitos básicos do processo de pentesting. Esse CTF é indicado para aqueles que desejam praticar técnicas de desencriptarão e manipulação de arquivos do tipo png.

Referências

<https://www.exploit-db.com/>

<https://gtfobins.github.io/>

https://book.hacktricks.xyz/