**27/05/2024 – AGENT SUDO**

<https://tryhackme.com/r/room/agentsudoctf>

1. Escaneamento de portas com Nmap
   1. escaneando todas as portas com -p- (sem descobrir versões nem sistemas operacionais)

Texto

Descrição gerada automaticamente

* 1. mapeando versões das portas descobertas anteriormente com -A

Texto

Descrição gerada automaticamente

1. Enumeração de diretórios com Gobuster
   1. utilização da wordlist common.txt

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

1. Exploração web
   1. a tela inicial indica que deve-se mexer no user-agente do request headers

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

* 1. fazendo requisições no repeater com outras letras do alfabeto, chega-se à uma resposta com status 302 (found) e um arquivo php indicado

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

* 1. acessando o arquivo descobre-se que o agente chama-se Chris

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

1. Brute force FTP com Hydra
   1. utilizando usuário chris e rockyou para senha

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

* 1. conectando com FTP usando o usuário e a senha encontrada

Texto

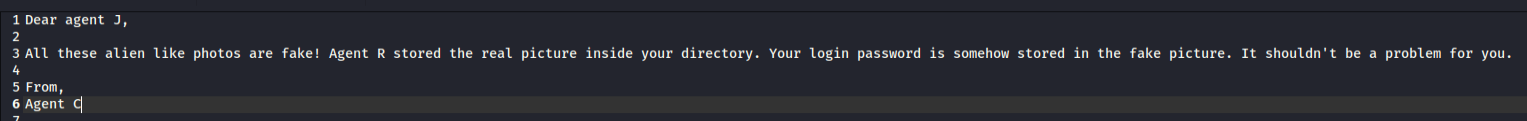
Descrição gerada automaticamente

* 1. explorando conexão e pegando arquivos

Uma imagem contendo Interface gráfica do usuário

Descrição gerada automaticamente

1. Explorando arquivos baixados por FTP
   1. arquivo txt destinado a outro agente dizendo que a senha está armazenada nas fotos dos aliens (cutie\_alien.png e cutie.png)



* 1. coletando informações das imagens usando binwalk (analisa binários das imagens) – cutie.png está integrado com um arquivo zip com o nome To\_agentR.txt

Texto

Descrição gerada automaticamente

* 1. extraindo pasta zip da imagem com binwalk -e

Texto

Descrição gerada automaticamente

* 1. explorando pasta \_cutie.png.extracted



* 1. a extração de 8702.zip demanda uma senha

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

1. Brute force da senha do zip usando zip2john e John the Ripper
   1. referência utilizada: <https://medium.com/@ujjawal.soni2002/cracking-a-password-protected-zip-file-using-john-the-ripper-f39e657cbfa8>



Texto

Descrição gerada automaticamente

* 1. extraindo arquivo e visualizando

Linha do tempo

Descrição gerada automaticamente

1. Decodificando o texto
   1. utilizando base64 para decodificar o texto (<https://www.dcode.fr/base-64-encoding>)

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

1. Utilizando Stenography
   1. segundo o portal THM, “Área51” era uma senha de stenography das imagens
   2. utilizando steghide para decriptografar

Interface gráfica do usuário, Site

Descrição gerada automaticamente

* 1. descobre-se, então, o usuário do agente e a senha para fazer conexão SSH

1. Conexão com SSH e busca por flag
   1. conexão com usuário e senha encontrados

Texto

Descrição gerada automaticamente

* 1. senha e imagem buscada estão na pasta do usuário

1. Privilege escalation
   1. importando e executando linpeas.sh

Uma imagem contendo Texto

Descrição gerada automaticamente

* 1. sinalização de um exploit

Texto

Descrição gerada automaticamente

* 1. procurando exploit no exploit db para fazer privesc - https://www.exploit-db.com/exploits/47502
  2. baixando exploit usando wget via máquina local

Texto

Descrição gerada automaticamente

* 1. executando e procurando flag

Texto

Descrição gerada automaticamente