**01/06/2024 - ANONYMOUS**

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

1. Escaneamento com Nmap
   1. escaneando primeiro com -p- para reconhecer portas abertas sem escanear versões e sistema operacional­

Texto

Descrição gerada automaticamente

* 1. escaneamento profundo das portas encontradas

Texto

Descrição gerada automaticamente

* 1. smb – serve para compartilhar recursos na rede

1. FTP com login anonymous
   1. não precisa de senha para login

Texto

Descrição gerada automaticamente

* 1. baixando scripts do diretório via ftp

Imagem em preto e branco

Descrição gerada automaticamente

* 1. visualizando os arquivos

Texto

Descrição gerada automaticamente

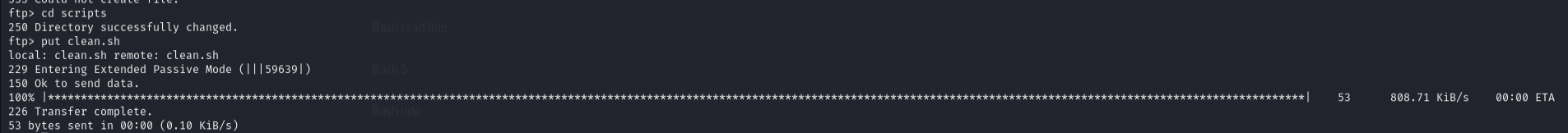
Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Cronjob no clean.sh
   1. o clean.sh aparenta estar sendo executado periodicamente pelo servidor, caracterizando um cronjob
   2. fazendo upload via ftp de um reverse shell no arquivo clean.sh para criar conexão remota via netcat
   3. a ideia é o arquivo com reverse shell sobrescrever o arquivo executado periodicamente (<https://www.revshells.com/>)



* 1. foi necessário adicionar no início do arquivo sh ‘#!bin/bash’ para ser executado igual ao clean.sh anterior (também tinha).

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

* 1. encontrando a flag user.txt

Texto

Descrição gerada automaticamente com confiança média

1. Privilege Escalation
   1. usando linpeas.sh para encontrar formas de escalar os privilégios
   2. possível SUID no /bin/env



Interface gráfica do usuário, Texto

Descrição gerada automaticamente



* 1. usando SUID para privesc (<https://gtfobins.github.io/gtfobins/env/#sudo>)

Texto

Descrição gerada automaticamente

* 1. pegando a flag root.txt

Texto

Descrição gerada automaticamente