06/04/2024 – TryHackMe – Retro

Link: <https://tryhackme.com/r/room/retro>

1. Port Scanning

Texto

Descrição gerada automaticamente

1. Acessando a página WEB, tem-se uma página padrão do Windows ISS. Usando o *gobuster* para procurar diretórios, tem-se:

Texto

Descrição gerada automaticamente

1. Acessando a página, tem-se:

Interface gráfica do usuário

Descrição gerada automaticamente

1. Ao analisar o site, encontra-se um comentário em uma postagem:

Texto

Descrição gerada automaticamente

1. Portanto, utilizando as credenciais *wade:parzival* via *RDP*, tem-se:



Interface gráfica do usuário

Descrição gerada automaticamente com confiança baixa

1. Lendo o arquivo *user.txt*, tem-se a primeira flag. Ao baixar o script *winPEAS.exe* (<https://github.com/peass-ng/PEASS-ng/blob/master/winPEAS/winPEASexe/README.md>), verifica-se informações do sistema operacional:

Texto

Descrição gerada automaticamente

1. Procurando falhas para Windows Server 2016, encontra-se a seguinte CVE (<https://github.com/SecWiki/windows-kernel-exploits/tree/master/CVE-2017-0213>):

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

1. Seguindo os passos do tutorial, tem-se:





Interface gráfica do usuário, Texto

Descrição gerada automaticamente

1. Indo no diretório *Desktop* do *Administrator*, encontra-se a última flag:  
   