**12/05/2024 – BOILERCTF**

<https://tryhackme.com/r/room/boilerctf2>

1. Varredura com Nmap
   1. divisão em partes - -p X-Y
   2. -Pn – servidor bloqueava nmap
   3. FTP – anon login allowed

Texto

Descrição gerada automaticamente

1. Login anonymous FTP
   1. usuário anonymous não precisa de senha
   2. get arquivo – transfere para diretório onde foi conectado o ftp

Texto

Descrição gerada automaticamente Texto

Descrição gerada automaticamente

1. Escaneamento com Gobuster
   1. joomla – CMS (gestão de conteúdo WEB)
   2. robots.txt
   3. \_test – indica sar2html (tem exploit para rshell)

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

1. Explorando exploit no sar2html
   1. exploit: <https://www.exploit-db.com/exploits/47204>
   2. conexão ssh (user: basterd; pass: superduperp@$$)

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

1. Explorando usuário
   1. descobrindo outro usuário(stoner, superduperp@$$no1knows)

Texto

Descrição gerada automaticamente

1. Chave no arquivo oculto .secret

Texto

Descrição gerada automaticamente

1. Importando linpeas.sh
   1. faz varredura de exploits, privesc, flags, etc.
   2. uso do ip tun0

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

Interface gráfica do usuário

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Usando find como SUID para privesc
   1. referência ao gtfobins: <https://gtfobins.github.io/gtfobins/find/#shell>
   2. chmod – trabalhar com permissões de arquivos
   3. 777 – permissão de escrita, leitura e execução para todos
   4. chmod 777 /root – atribui permissão geral na pasta root

Texto

Descrição gerada automaticamente

