Blog writeup

Usando nmap no site vemos:

Nmap scan report for blog.thm (10.10.96.47)

Host is up (0.14s latency).

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 57:8a:da:90:ba:ed:3a:47:0c:05:a3:f7:a8:0a:8d:78 (RSA)

| 256 c2:64:ef:ab:b1:9a:1c:87:58:7c:4b:d5:0f:20:46:26 (ECDSA)

|\_ 256 5a:f2:62:92:11:8e:ad:8a:9b:23:82:2d:ad:53:bc:16 (ED25519)

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

|\_http-generator: WordPress 5.0

| http-robots.txt: 1 disallowed entry

|\_/wp-admin/

|\_http-server-header: Apache/2.4.29 (Ubuntu)

|\_http-title: Billy Joel&#039;s IT Blog &#8211; The IT blog

139/tcp open netbios-ssn Samba smbd 3.X — 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)

Service Info: Host: BLOG; OS: Linux; CPE: cpe:/o:linux:linux\_kernel

E podemos ver no robots.txt /wp-admin/ isso indica que o site roda WORDPRESS

Fazendo um bruteforce nos usuarios achamos:

kwheel : cutiepie1

E na internet podemos achar um exploit para o WordPress 5.0 e utilizando as credenciais podemos usar e ganhar a shell dentro do sistema

Vemos que dentro do codigo do programa CHECKER se a variavel de ambiente ADMIN=ADMIN estiver no PATH ele será executado como root

Então é so executar os comandos:

EXPORT ADMIN=ADMIN

ELE SETARA O SEU UID PRA 0 (ROOT)

E rodar o programa e pegar a flag