THESEUS

.109 - theseus

1. Header from nmap scan should give you "welcome to FTP Server Spring 2017"
2. Google that and you will get on github: https://github.com/pachev/pachev_ftp
3. there is an issue reported which leads you to find the https://www.exploit-db.com/exploits/47956 is where I got the idea for exploit using lftp as the command to connect to it manually as the exploit/ftp module did not work for me. i am assuming cause tls and "lftp" takes care of all of that so you can connect using it creds are
    a. default user: pachev
    b. pass: <EMPTY>
4. Use the vulnerability of directory traversal to enumerate all shares download smbpasswd.bak, passwd zip and smb conf zip form different shares available (download everything from all shares to make it seem legit and go through them)
5. You will get 4 hashes for 4 users from smb conf you see mary has shell access you also see there is a setting called "magic script" configured. Google it and you will see that the file with that names gets executed as the user thats logged in.
6. Use smbclient to login as mary using pass-the-hash upload a script containing rev shell of your choice with that name
7. use nc to listen for the rev shell as soon as you put the file in the share it will get executed (mary can only access one share so you.
8. The priv esc is an unquoted service path.