**Worker**

Difficulty: Medium

*Machine: Windows*

**Nmap**

Starting off with our aggressive nmap scan, we discover ports 80 and 3690 are open. Port 80 is a standard IIS 10.0 web server whereas port 3690 is running svnserve - a new program for me.

|  |
| --- |

**SVN**

Doing some quick research on SVN, we figure out it is a git-like program that can be connected to with “svn://”. There is a program called “svn” on Kali we can use to connect. Looking at the documentation for this program, we use the following command to look at the contents.

| *Svn list svn://10.10.10.203* |
| --- |

The interesting file here is “moved.txt”. This can be inspected with the “cat” command with svn.

| *Svn cat svn://10.10.10.203/moved.txt* |
| --- |

We got a hostname for a new site. Adding this to /etc/hosts and going to the site brings up nothing. Time to backtrack to svn.

Going over the commands in svn, we have a limited selection. Doing the “info” command gves us some basic information about the repo along with a potential user. Additionally, we see the number of revisions.

| *Svn info svn://10.10.10.203* |
| --- |

Testing out the “checkout” command, we see a list of all files in the repo along with the information that this is again revision 5. If this program acts anything like git, then we may be able to view previous editions of the repo.

| *Svn checkout svn://10.10.10.203* |
| --- |

Looking at the help page for “checkout” we find the “-r” flag which will help us view different revisions. Doing this with revisions 0 to 4 shows us an interesting file called “deploy.ps1”

| *Svn checkout -r <NUM> svn:10.10.10.203* |
| --- |



