**VulnHub 1 – ICA 1 Walkthrough**

1. I began this by performing a scan of the devices on the network. “sudo netdiscover -i eth1 -r 192.168.56.0/24”
   1. Victim: 192.168.56.105
   2. Kali: 192.168.56.101 (eth1)
2. A screen shot of a computer

   Description automatically generatedNext, I proceeded to perform a port scan using nmap.

* This reveals that ssh, http and mysql is used on this machine.
* If http is being ran than means that wordpress could be used or basic apache web-server could be used.
* If mysql is being ran then their could be some databases worth exploring.
* SSH means that there could be a private key somewhere or a password.

1. A screenshot of a computer screen

   Description automatically generatedI decided to use the tool nikto to discover some information about that ip address.

* A screenshot of a computer

  Description automatically generatedThere was mention of possibility of XXS vulnerability and it did find that the machine is an apache server.

1. A screenshot of a computer

   Description automatically generatedI then proceeded to explore the webpage to determine any information that could be used to get into this system. This just showed a very basic login page, with qdPM 9.2.

* Exploring /template revealed the plugin information and other website information.

1. According to an article I found about this version of ‘qdPM’ you can do a connectionless database download if you navigate to a specific directory.

* A screenshot of a computer screen

  Description automatically generatedNavigating to this link will download a database file called ‘databases.yml’.

**LINK**: https://www.exploit-db.com/exploits/50176

* A screenshot of a computer program

  Description automatically generatedThis file shows an account username and password. This is the credentials for mysql?
* I also discovered that this version (9.2) can be XXS to change the credentials, however this only works when the account is logged in. I also looked through searchsploit for qdpm 9.2, but it doesn’t show any exploits for that version.

1. I attempted to connect remotely to the mysql command line, using the command:
   * ‘Mysql -u qdpmadmin -h 192.168.56.105 -p UcVQCM..S6J’.

* A screenshot of a computer

  Description automatically generatedThis gave me terminal access to mysql.

A screen shot of a computer

Description automatically generated

* A screen shot of a computer

  Description automatically generatedI can see all databases, and decided to look into staff database.

A screenshot of a computer program

Description automatically generated

* I then decided to look at the login table of the database, which shows the encrypted password and the user id. The passwords appear to be base64 (due to the padding including 2 equal signs).

1. A screenshot of a computer

   Description automatically generatedNext is the step to begin cracking the passwords. I converted each password into its base64.

A computer screen shot of a program

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

1. A screenshot of a computer

   Description automatically generatedOnce I ssh into the accounts I quickly checked the desktop files and found two files. Dexter had a note stating their was some executables that were viewable. I thought to use the find command to search for SUID.

* Something looked interesting called ‘get\_access’ so I called the ‘file’ command to determine what it is and it is a executable, however it didn’t run.

A screen shot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

1. I then tried running strings to see if I could find anything else. Here I saw an interesting item, ‘cat /root/system.info’.
2. I couldn’t execute cat on the file, so I had to create my own version and replace the old one.

* ‘cd /tmp/’ then create ‘cat’ then write ‘chmod +x cat’ for execution, finally ‘export PATH=/tmp:$PATH’ (replace the original cat path). Next, vim it and type ‘chmod u+s /bin/bash’ and run the ‘../opt/get\_access’. You should only see “All service are disabled…”.
* Check the newly established privileges.
* Now you can run bash in privilege mode by running ‘bash -p’. Quickly return ‘cat’ back to the original path ‘PATH=/usr/…/games’. You can then ‘cd’ and go into ‘root’ and there will be ‘root.txt’ and you can display the contents to reveal the project.

A screenshot of a computer program

Description automatically generated