REPORT BASIC PENTESTING 2

Riccardo Bruzzese

Services of the device to exploit:

22: SSH

80: HTTP

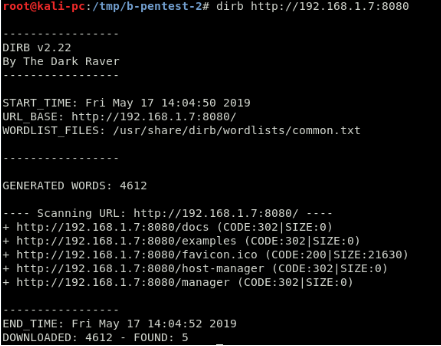
445:Samba

139:Samba

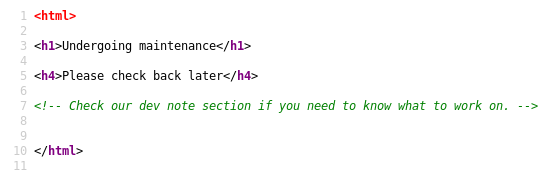
8009: server web Tomcat and Jserv

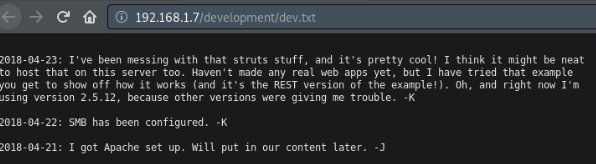
8080:

Dirbuster process:

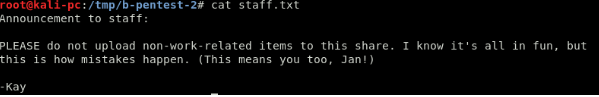


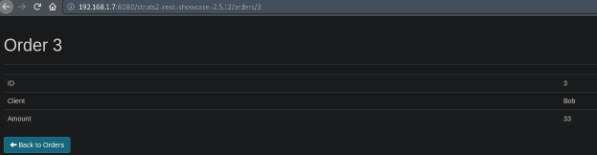
Inspecting website:



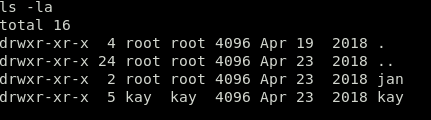
In the section development/dev.txt i found:

From this information I understand that the machine is using struts and through REST information and version 2.5.12, I can find this exploit:<https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/exploit/multi/http/struts2_rest_xstream.md>

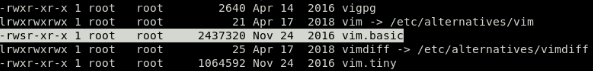
By accessing the samba portal in this way, I add a virtual host and find an Anymous folder and inside there is a staff file:

Through this information we know that Kay and Jay may be users who may have accessed with SSH   
  
Then I need a uri to make the struts exploit work, through numerous attempts I discovered that it was enough to add the version

done this I get a shell and they log me in as user tomcat9 and running in directories I find users kay and jan



and doing ls -la su kay I find that he is part of the administrators only that I am not allowed to access the pass.bak  
  
Through help of my companions I find that I need a program with SETUID then I go to check the executables present in /bin, realizing that, vim calls through another link in /etc/alternatives/ vim.basic, that if executed I momentarily turns into root





Opening the pass.bak I get the password that is heresareallystrongpasswordthatfollowsthepasswordpolicy  
  
through that password I john on the folder /etc/passwid and get jan’s password and then I can access the SSH

The device was not very complicated to pierce also because there were numerous clues   
  
Difficulties encountered in:  
I spent a lot of time finding the uri for the exploit struts and also accessing the pass.bak file for the rest was not complicated