REPORT BASIC PENTESTING 2

Riccardo Bruzzese

La macchina disponeva di alcuni serivizi aperti tra cui la porta

22: SSH

80: HTTP

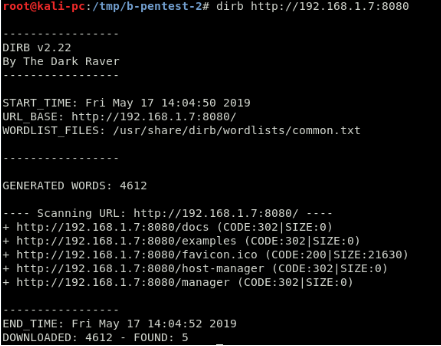
445:Samba

139:Samba

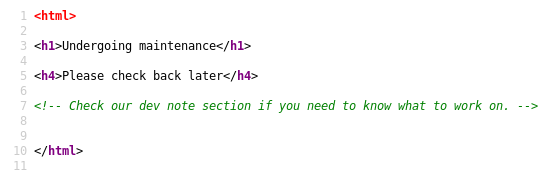
8009: server web tra cuit Tomcat e Jserv

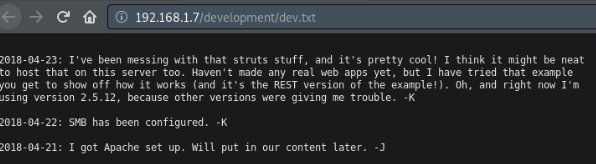
8080:

Partendo dalla porta 80 abbiamo fatto un dirbuster



Ispezionando il sito, si presenta così:

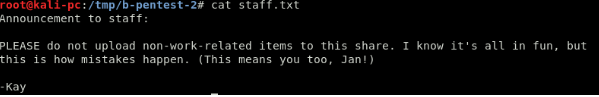


Nella sezione development/dev.txt ho trovato:

Da queste informazioni ho capito che la macchina sta utilizzando struts ed attraverso le informazioni del REST e la versione 2.5.12, riesco a trovare questo exploit:

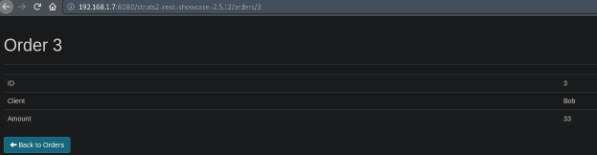
<https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/exploit/multi/http/struts2_rest_xstream.md>

Accedendo così al portale samba, aggiungo un host virtuale e trovo una cartella Anymous e all’interno c’è un file staff

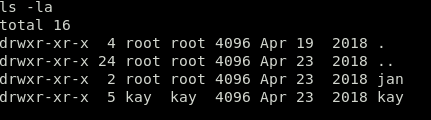


Attraverso questa informazione sappiamo che Kay e Jay possono essere degli utenti che possono essere entrati magari con SSH

Successivamente mi serve un uri per far funzionare l’exploit di struts, attraverso numerosi tentativi ho scoperto che bastava aggiungere la versione

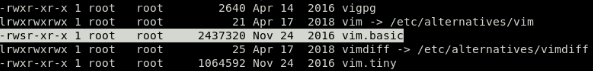


fatto questo ottengo una shell e mi fanno accedere come utente tomcat9 e girando nelle directory trovo gli utenti kay e jan



e facendo ls -la su kay scopro che lui fa parte degli amministratori solo che non ho il permesso di accedere al pass.bak

Attraverso aiuti dei miei compagni scopro che ho bisogno di un programma con SETUID quindi vado a controllare gli eseguibili presenti in /bin, accorgendomi che, vim richiama tramite un altro link in /etc/alternatives/ vim.basic, che se eseguito mi trasforma momentaneamente in root





Aprendo il pass.bak ottengo la password che è heresareallystrongpasswordthatfollowsthepasswordpolicy

atraverso quella password faccio un john sulla cartella /etc/passwid e ottengo la password di jan e quindi riesco ad accedere al SSH



La macchina non era molto complicata da bucare anche perchè c’erano numerosi indizi

Difficoltà incontrate:

ho impiegato molto tempo nel trovare l’uri per l’exploit struts ed anche nel accedere al file pass.bak per il resto non è stato complicato