Aplicatii ce pot ajuta la rezolvarea unor exercitii de tip Capture the Flag la OSC 2024

Documentul de mai jos prezinta o serie de aplicatii ce pot fi utile in rezolvarea unor exercitii la probele de la Olimpiada de Securitate Cibernetica, etapa pe judet, din 2024!

Documentul are un rol informativ. Participantii pot folosi si alte aplicatii pentru rezolvarea probelor. De asemenea, organizatorii pot da probe ce necesita si aplicatii ce nu se regasesc in aceasta lista.

Cuprins

Sisteme de operare

Sisteme de operare ce pot ajuta la rezolvarea exercitiilor:

- Android Tamer - Bazat pe Debian.
- BackBox - Bazat pe Ubuntu.
- BlackArch Linux - Bazat pe Arch Linux.
- Fedora Security Lab - Bazat pe Fedora.
- Kali Linux - Bazat pe Debian, unul din cele mai populare.
- Parrot Security OS - Bazat pe Debian.
- Pentoo - Bazat pe Gentoo.
- URIX OS - Bazat pe openSUSE.
- Wifislax - Bazat pe Slackware.
- Virtualbox - Virtualizare si masini virtuale

Exercitii de criptografie

Aplicatii utile în rezolvarea exercitiilor de Criptografie.

- CyberChef - Aplicație web pentru analiza și decodificarea datelor.
- FeatherDuster - Un instrument de criptanaliză modular și automatizat.
- Hash Extender - Un instrument utilitar pentru efectuarea de atacuri de extindere a lungimii hașurilor.
- padding-oracle-attacker - Un instrument CLI pentru a executa atacuri de tip padding oracle.
- PkCrack - O unealtă pentru spargerea codului de criptare PkZip.
- QuipQuip - Un instrument online pentru spargerea cifrului de substituție sau a cifrului vigenere (fără cheie).
- RSACTFTool - Un instrument pentru recuperarea cheii private RSA cu diferite atacuri.
- RSATool - Generarea unei chei private cunoscând p și q.
- XORTool - Un instrument de analiză a cifrului xor multi-byte.

Exercitii cu activitati bruteforce

Aplicatii utile pentru activitati de brute force (de exemplu pentru parole etc.)

- Hashcat - Cracker de parole
- Hydra - Un cracker de autentificare paralelizat care suportă numeroase protocoale pentru a ataca
- John The Jumbo - Versiunea îmbunătățită de comunitate a lui John Spintecătorul.
- John The Ripper - Password Cracker.
- Nozzlr - Nozzlr este un cadru de forță brută, foarte modular și prietenos cu scripturile.
- Ophcrack - Cracare de parole pentru Windows bazat pe tabele curcubeu.
- Patator - Patator este un program de forțare brută multifuncțional, cu un design modular.
- Turbo Intruder - Extensie Burp Suite pentru trimiterea unui număr mare de cereri HTTP

Exercitii de inginerie inversa si exploatare a binarelor

Instrumente utilizate pentru rezolvarea provocărilor Exploits

- DLLInjector - Injectează dll-uri în procese.
- libformatstr - Simplifică exploatarea șirurilor de formate.
- Metasploit - Software de testare a penetrării.
    - Foaie de parcurs
- one_gadget - Un instrument pentru a găsi apelul one gadget execve('/bin/sh', NULL, NULL).
    - gem install one_gadget
- Pwntools - Cadru CTF pentru scrierea de exploit-uri.
- Qira - QEMU Interactive Runtime Analyser.
- ROP Gadget - Cadru pentru exploatarea ROP.
- V0lt - Set de instrumente CTF de securitate.
- Androguard - Aplicații Android de inginerie inversă.
- Angr - cadru de analiză binară agnostic pentru platforme.
- Apk2Gold - Încă un decompiler Android.
- ApkTool - Android Decompiler.

- Barf - Binary Analysis and Reverse Engineering Framework (cadru de analiză binară și inginerie inversă).
- Binary Ninja - Cadru de analiză binară.
- BinUtils - Colecție de instrumente binare.
- BinWalk - Analizează, face inginerie inversă și extrage imagini de firmware.
- Boomerang - Descompilează binarele x86/SPARC/PowerPC/ST-20 în C.
- ctf_import - rulează funcții de bază din binarele dezactivate pe mai multe platforme.
- cwe_checker - cwe_checker găsește modele vulnerabile în executabilele binare.
- demovfuscator - Un deobfuscator în curs de realizare pentru binarele movfuscate.
- Frida - Injecție dinamică de cod.
- GDB - Depanatorul de proiecte GNU.
- GEF - Plugin GDB.
- Ghidra - Suita de instrumente de inginerie inversă cu sursă deschisă. Similar cu IDA Pro.
- Hopper - Instrument de inginerie inversă (dezasamblorator) pentru OSX și Linux.
- IDA Pro - Cel mai utilizat software de inversare.
- Jadx - Descompune fișiere Android.
- Java Decompilers - Un descompilator online pentru Java și Android APK-uri.
- Krakatau - Descompilator și dezasamblorator Java.
- Objecție - Runtime Mobile Exploration.
- PEDA - Plugin GDB (numai pentru python2.7).
- Pin - Un instrument dinamic de instrumente binare de la Intel.
- PINCE - Instrument GDB front-end/instrument de inginerie inversă, axat pe game-hacking și automatizare.
- PinCTF - Un instrument care utilizează pinii Intel pentru analiza canalelor laterale.
- Plasma - Un dezasamblorator interactiv pentru x86/ARM/MIPS care poate genera pseudocod indentat cu sintaxă colorată.
- Pwndbg - Un plugin pentru GDB care oferă o suită de utilități pentru a sparge GDB cu ușurință.
- radare2 - Un cadru portabil de inversare.

- Triton - Cadru de analiză binară dinamică (DBA).
- Uncompyle - Descompilează binarele Python 2.7 (.pyc).
- WinDbg - Depanator Windows distribuit de Microsoft.
- Xocopy - Program care poate copia executabile cu permisiune de execuție, dar fără permisiune de citire.
- Z3 - Un teorem prover de la Microsoft Research.
- Detox - Un instrument de analiză a programelor malware în Javascript.
- Revelo - Analizează codul Javascript ofuscat.
- RABCDAsm - Colecție de utilitare, inclusiv un asamblor/dezasamblorator ActionScript 3.
- Swftools - Colecție de utilitare pentru a lucra cu fișiere SWF.
- Xxxswf - Un script Python pentru analizarea fișierelor Flash.

Exercitii de criminalistica informatica

Instrumente utilizate pentru rezolvarea provocărilor din domeniul criminalisticii

- Aircrack-Ng - Sparge cheile WEP și WPA-PSK 802.11.
    - apt-get install aircrack-ng
- Audacity - Analizează fișiere de sunet (mp3, m4a, orice).
    - apt-get install audacity
- Bkhive și Samdump2 - Aruncă fișierele SYSTEM și SAM.
    - apt-get install samdump2 bkhive
- CFF Explorer - Editor PE.
- Creddump - Aruncă acreditările Windows.
- DVCS Ripper - Rips sisteme de control al versiunilor (distribuite) accesibile pe web.
- Exif Tool - Citește, scrie și editează metadatele fișierelor.
- Extundelete - Utilizat pentru recuperarea datelor pierdute din imagini montabile.
- Fibratus - Instrument pentru explorarea și urmărirea nucleului Windows.
- Foremost - Extrage anumite tipuri de fișiere folosind anteturi.
    - apt-get install foremost

- Fsck.ext4 - Folosit pentru a repara sistemele de fișiere corupte.
- Malzilla - Instrument de vânătoare de programe malware.
- NetworkMiner - Instrument de analiză criminalistică a rețelelor.
- PDF Streams Inflater - Găsește și extrage fișiere zlib comprimate în fișiere PDF.
- Pngcheck - Verifică integritatea PNG și descarcă toate informațiile la nivel de bucată în formă lizibilă pentru oameni.
    - apt-get install pngcheck
- ResourcesExtract - Extrage diverse tipuri de fișiere din ex-uri.
- Shellbags - Investighează fișierele NT_USER.dat.
- Snow - Un instrument de steganografie a spațiilor albe.
- USBRip - Un instrument simplu de criminalistică CLI pentru urmărirea artefactelor dispozitivelor USB (istoricul evenimentelor USB) pe GNU/Linux.
- Volatilitate - Pentru a investiga descărcările de memorie.
- Wireshark - Folosit pentru a analiza fișiere pcap sau pcapng
- OfflineRegistryView - Un instrument simplu pentru Windows care vă permite să citiți fișiere de registru offline de pe o unitate externă și să vizualizați cheia de registru dorită în format .reg.
- Registry Viewer® - Utilizat pentru a vizualiza registrele Windows.

Exercitii din categoria “Retea”

Instrumente utilizate pentru rezolvarea provocărilor de rețea

- Masscan - Scanner de porturi IP în masă, scanner de porturi TCP.
- Monit - Un instrument linux pentru a verifica o gazdă în rețea (și alte activități care nu țin de rețea).
- Nipe - Nipe este un script pentru a face din rețeaua Tor gateway-ul tău implicit.
- Nmap - Un utilitar open source pentru descoperirea rețelei și auditul de securitate.
- Wireshark - Analizați descărcările de date din rețea.
    - apt-get install wireshark
- Zeek - Un monitor de securitate de rețea cu sursă deschisă.
- Zmap - Un scaner de rețea open-source.

Exercitii de Steganografie

Instrumente utilizate pentru rezolvarea provocărilor legate de steganografie

- AperiSolve - Aperi'Solve este o platformă care realizează analiza straturilor pe imagine (open-source).
- Convert - Convertește imagini în formate b/n și aplică filtre.
- Exif - Afișează informațiile EXIF din fișierele JPEG.
- Exiftool - Citește și scrie informații meta în fișiere.
- Exiv2 - Instrument de manipulare a metadatelor de imagine.
- Steganografie de imagine - Încorporează text și fișiere în imagini cu criptare opțională. UI ușor de utilizat.
- Image Steganography Online - Acesta este un instrument Javascript pe partea de client pentru a ascunde imagini steganografice în interiorul "biților" inferiori ai altor imagini.
- ImageMagick - Instrument pentru manipularea imaginilor.
- Outguess - Instrument steganografic universal.
- Pngtools - Pentru diverse analize legate de PNG-uri.
    - apt-get install pngtools
- SmartDeblur - Utilizat pentru a deblura și a repara imaginile defocalizate.
- Steganabara - Instrument pentru analiza stegano scris în Java.
- SteganographyOnline - Codificator și decodificator de steganografie online.
- Stegbreak - Lansează atacuri de dicționar de forță brută asupra imaginilor JPG.
- StegCracker - Utilitar de forță brută de steganografie pentru a descoperi date ascunse în fișiere.
- stegextract - Detectează fișierele și textele ascunse în imagini.
- Steghide - Ascunde datele în diferite tipuri de imagini.
- StegOnline - Efectuează o gamă largă de operațiuni de steganografie a imaginilor, cum ar fi ascunderea/revelarea fișierelor ascunse între biți (open-source).
- Stegsolve - Aplică diverse tehnici de steganografie pe imagini.
- Zsteg - Analiza PNG/BMP.

Exercitii cu aplicatii web

Instrumente utilizate pentru rezolvarea provocărilor Web

- BurpSuite - Un instrument grafic pentru testarea securității site-urilor web.
- Commix - Instrument automatizat de injectare și exploatare a comenzilor de sistem de operare All-in-One.
- Hackbar - Addon Firefox pentru o exploatare ușoară a internetului.
- OWASP ZAP - Proxy de interceptare pentru a reda, depanarea și fuzzarea cererilor și răspunsurilor HTTP
- Postman - Add on pentru Chrome pentru depanarea cererilor de rețea.
- Raccoon - Un instrument de securitate ofensiv de înaltă performanță pentru recunoaștere și scanare a vulnerabilităților.
- SQLMap - Instrument automat de injecție SQL și preluare a bazelor de date. pip install sqlmap
- W3af - Web Application Attack and Audit Framework.
- XSSer - Testator XSS automatizat.
- Request Bin - Vă permite să inspectați cererile http către o anumită adresă URL.