La cassetta degli attrezzi del bravo hacker

Dic 09, 2019 Giancarlo Calzetta Approfondimenti, Hacking, In evidenza, RSS, Software 0

Sergio Caruso è un esperto di sicurezza che abbiamo già avuto il piacere di intervistare in occasione di una sua breve ricerca sulle truffe online via cellulare. Il video, che svela cosa succede quando si clicca su una pubblicità malevola o una pagina solitamente fornita all'utente tramite browser-jacking, era molto interessante e lo trovate qui sotto:
[embedded content]
Adesso, Sergio ci ha fatto un gran regalo: una guida, devo dire molto completa, sugli strumenti "di base" che vengono usati dagli hacker per gestire le quotidiane chiamate che spaziano dall'analisi dei malware all'investigazioni forensi, passando per reverse engeneering e sfide di Capture the Flag.

Ha diviso per noi l'elenco in macro categorie, aggiungendo una breve descrizione ad ogni strumento. Questo articolo è solo un punto di partenza, ma chi ha voglia di approfondire ha da fare per mesi. Grazie Sergio!

STRUMENTI DI REVERSE ENGINEERING, DECOMPILATORI E DEBUGGER

OllyDbg – Disponibile solo in versione a 32 bit, per sistemi Microsoft Windows.
OllyDbg traccia i registri, riconosce le funzioni e i parametri passati alle principali librerie standard, le

chiamate alle API del sistema operativo, eventuali salti condizionali, tabelle, costanti, variabili e stringhe.

Immunity Debugger – Nuovo modo efficace per scrivere exploit, analizzare malware e decodificare file binari. Si basa su una solida interfaccia utente con funzione grafica, il primo strumento di analisi heap del settore costruito appositamente per la creazione di heap e un'API Python ampia e ben supportata per una facile estensibilità.

GDB – GNU debugger è un programma libero sviluppato dal progetto GNU. È il debugger predefinito del sistema operativo GNU, gira su molte piattaforme ed è capace di analizzare numerosi linguaggi di programmazione, tra cui Ada, C, C++ e Fortran.

IDA Pro – L'Interactive Disassembler, più comunemente conosciuto con il nome IDA, è un disassembler largamente usato per il reverse engineering. Supporta numerosi formati di file eseguibili per diversi processori e sistemi operativi.

WinDbg – Debugger di Windows. Può essere utilizzato per eseguire il debug del codice in modalità kernel e in modalità utente, per analizzare i dump di arresto anomalo e per esaminare i registri della CPU durante l'esecuzione del codice.

PE Tools – Consente di ricercare attivamente file e processi PE. Sono inclusi Process Viewer e Editor di file PE, Dumper, Rebuilder, Comparatore, Analizzatore.

UPX – Ultimate Packer per eXecutables è un packer eseguibile open source che supporta numerosi formati di file da diversi sistemi operativi.

Radare2 – Framework completo per il reverse engineering e l'analisi dei binari; composto da un insieme di piccole utility che possono essere utilizzate insieme o indipendentemente da riga di comando.

Strace – Utility di debugging per Linux e altri sistemi Unix-like che esamina le chiamate di sistema usate da un programma e tutti i segnali che esso riceve, analogamente all'utility truss presente in altri sistemi Unix. Ciò è reso possibile da una funzionalità chiamata ptrace.

CFF Explorer – Suite di strumenti freeware che include un editor PE chiamato CFF Explorer e un visualizzatore di processi.

Barf – Binary Analysis and Reverse engineering Framework è un framework open source multipiattaforma per l'analisi binaria e il reverse engineering

Binary Ninja – Framework di Reverse Engineering

Hopper – Strumento di reverse engineering per OSX e Linux

Apktool – Strumento per il reverse engineering di app Android. Può decodificare le risorse in una forma quasi originale e ricostruirle dopo aver apportato alcune modifiche.

dex2jar – Strumento per lavorare con i file Android .dex e java .class

Androguard – Reverse engineering, analisi di malware e goodware di applicazioni Android

Apk2Gold – Strumento CLI per la decompilazione di app Android in Java.

Jadx – Strumenti da riga di comando e GUI per produrre codice sorgente Java da file Dex e Apk Android

Java Decompilers – Decompilatore online per APK Java e Android

RABCDAsm – Raccolta di utilità incluso un assemblatore/disassemblatore ActionScript 3.

Swftools – Raccolta di utility per lavorare con file SWF

Xxxswf – Uno script Python per l’analisi dei file Flash.

Detox – Strumento per supportare l’analisi manuale di codice Javascript dannoso.

Krakatau – Decompilatore e disassemblatore Java

STRUMENTI PER L’ANALISI DEL CODICE STATICO

RIPS – Software di analisi del codice statico per il rilevamento automatico delle vulnerabilità della sicurezza nelle applicazioni PHP e Java. Lo strumento iniziale è stato scritto da Johannes Dahse e rilasciato durante il mese di PHP Security nel maggio 2010 come software open source.

OWASP Code Crawler – È uno strumento di revisione del codice statico che cerca argomenti chiave all’interno del codice .NET e J2EE / JAVA.

OWASP LAPSE Project – Security scanner per rilevare le vulnerabilità di data injection nelle applicazioni Java EE.

Flawfinder – Analizzatore di codice sorgente statico per C / C ++. Segnala possibili punti deboli di sicurezza

ANALISI FORENSE

SANS Investigative Forensic Toolkit (SIFT) – Distribuzione di informatica forense che installa tutti gli strumenti necessari su Ubuntu per eseguire un esame digitale forense dettagliato e di risposta agli incidenti. È compatibile con i formati dei testimoni esperti, i formati forensi avanzati, i formati di prove di analisi non elaborate e di memoria.

Volatility – Framework di Memory Forensics open source per la risposta agli incidenti e l’analisi dei malware. È scritto in Python e supporta Microsoft Windows, Mac OS X e Linux.

Sleuth Kit – Raccolta di utility basate su Unix e Windows per facilitare l'analisi forense dei sistemi informatici. È stato scritto ed è gestito principalmente dall'investigatore digitale Brian Carrie.

Xplico – Network Forensic Analysis Tool (NFAT), ovvero un software che ricostruisce i contenuti dalle acquisizioni eseguite con packet sniffer (ad esempio Wireshark o tcpdump).

Binwalk – Strumento veloce e facile da usare per l'analisi, il reverse engineering e l'estrazione di immagini del firmware.

ExifTool – Software gratuito e open source per la lettura, la scrittura e la manipolazione di metadati di immagini, audio, video e PDF. È indipendente dalla piattaforma, disponibile sia come libreria Perl sia come applicazione da riga di comando.

CAINE – Computer Aided INvestigative Environment è una distribuzione live GNU / Linux italiana creata come progetto Digital Forensics. Offre un ambiente forense completo organizzato per integrare strumenti software esistenti come moduli software e fornire un'interfaccia grafica intuitiva.

DEFT Linux – Distribuzione GNU/Linux live di software libero basata su Ubuntu per usi legati alla Computer Forensics e alla sicurezza informatica.

Aircrack-Ng – Suite completa di strumenti per valutare la sicurezza della rete WiFi 802.11 WEP e WPA-PSK

Ophcrack – Software di password cracking, dedicato al cracking di password di sistemi Windows. E' gratuito, open source e basato su Rainbow Tables. E' disponibile anche sotto forma di Live CD, una volta fatto il boot, in automatico preleva i file SAM di windows e avvia le procedure di cracking.

Creddump – Strumento in Python per estrarre varie credenziali dal registro di Windows

Strumento Exif – Legge, scrive e modifica i metadati dei file

Extundelete – Utilizzato per il recupero di dati persi da immagini montabili

Fibratus – Strumento per l’esplorazione e la traccia del kernel di Windows

Fsck.ext4 – Usato per riparare filesystem corrotti

Malzilla – Strumento per l’hunting di malware

NetworkMiner – Strumento di analisi forense della rete

PDF Streams Inflater – Trova ed estrae file zlib compressi in file PDF

ResourcesExtract – Estrae vari tipi di file dagli ex

Shellbags – Esamina i file NT_USER.dat

UsbForensics – Tool che contiene molti strumenti per la analisi forense su dispositivi USB

RegistryViewer – Utilizzato per visualizzare i registri di Windows

John The Ripper – Strumento per il cracking delle password. Supporta il riconoscimento automatico degli hash e vari tipi di attacco: vocabolario o forza bruta. Attualmente può essere eseguito su 15 differenti piattaforme.

Hashcat – Strumento per il cracking delle password. Contiene tutte le funzioni di John The Ripper, ma è pensato per velocizzare le operazioni di cracking sfruttando il calcolo parallelo con le GPU.

FeatherDuster – Strumento di crittografia modulare automatizzato

PkCrack – Uno strumento per rompere la crittografia PkZip

RSACTFTool – Uno strumento per recuperare la chiave privata

RSA con vari attacchi

RSATool – Genera chiave privata con conoscenza di p e q

XORTool – Uno strumento per analizzare la crittografia xor multi-byte

John The Jumbo – Versione migliorata di John the Ripper

Nozzlr – Framework di brute force modulare e intuitivo.

STEGANOGRAFIA

Exif – Mostra le informazioni EXIF □□nei file JPEG

Exiv2 – Strumento di manipolazione dei metadati di immagine

ImageMagick – Strumento per manipolare le immagini

Outguess – Strumento steganografico universale

Pngtools – Per varie analisi relative ai PNG

SmartDeblur – Utilizzato per eseguire il deblur e correggere immagini sfocate

Steganabara – Strumento per analisi stegano scritto in Java

Stegbreak – Lancia attacchi brute force con dizionario sulle immagini JPG

StegCracker – Utilità di forza bruta Steganography per scoprire dati nascosti all'interno dei file

stegextract – Rileva file e testo nascosti nelle immagini

Steghide – Strumento eccezionale che può essere utilizzato per incorporare o estrarre dati in vari tipi di file di immagini e audio

Stegsolve – Applica varie tecniche di steganografia alle immagini

Zsteg – Analisi dei file PNG / BMP per la rilevazione di tecniche di steganografia

MP3Stego – Consente di nascondere del testo nei file MP3

STRUMENTI UTILIZZATI PER ESEGUIRE VARI TIPI DI ATTACCHI

Exploit-db – Database sulle vulnerabilità con libero accesso.

Burp Suite – Strumento per testare la sicurezza delle applicazioni Web. Scritto in Java e sviluppato da PortSwigger Web Security.

OWASP ZAP – Progetto di sicurezza delle applicazioni Web, simile a Burp ma gratuito e open source

WPScan – Scanner per vulnerabilità WordPress

Reaver – Strumento d'attacco di brute force contro i PIN del Wifi Protected Setup (WPS) al fine di recuperare le passphrase WPA/WPA2.

Nmap – Portscanner Open Source con plug-in per la valutazione delle vulnerabilità e il rilevamento della rete

Wireshark – Sniffer di rete e analizzatore di protocolli per Unix e Windows

Netcat – Programma open source a riga di comando di comunicazione remota, utilizzabile sia col protocollo TCP sia col protocollo UDP. Netcat è stato pensato per essere utilizzato facilmente da altri programmi o scripts.

Masscan – Scanner per IP massivo.

Raccoon – Strumento di sicurezza ad alte prestazioni per la scansione di vulnerabilità.

Sqlmap – Software Open Source per il penetration testing, che

permette di automatizzare il rilevamento e lo sfruttamento delle SQL injection e prendere così il controllo dei server DBMS. Il software lavora a linea di comando.

W3af – Attacco alle applicazioni Web e framework di audit.

XSSer – Tool per attacchi di tipo XSS automatizzato

Metasploit Framework – Oltre ad essere un framework di test di penetrazione, Metasploit ha moduli per lo sfruttamento automatico e strumenti per la creazione di exploit.

Bettercap – Framework per eseguire attacchi MITM (Man in the Middle).

DLLInjector – Inietta dll nei processi

libformatstr – Semplifica lo sfruttamento delle stringhe di formato.

Pwntools – CTF Framework per scrivere exploit

Gadget ROP – Framework per lo sfruttamento ROP

V0lt – Security CTF Toolkit

Monit – Strumento Linux per controllare un host sulla rete (e altre attività non di rete).

Nipe – Script per rendere Tor Network il gateway predefinito.

Zmap – Scanner di rete open source.

Position Grabber – Strumento per la creazione di link di cattura personalizzati. Quando verrà aperto dal bersaglio automaticamente arriverà una mail con un link ad una Mappa interattiva con la posizione.

OSINT – OPEN SOURCE INTELLIGENCE TOOLS

Maltego – Tool sviluppato dalla società Paterva, che offre la possibilità di raccogliere informazioni tramite la consultazione di dati pubblicamente accessibili e raggrupparle in formato grafico.

Google Dorks – Query, utilizzate principalmente sul motore di ricerca Google, che utilizza operatori di ricerca avanzati al fine di trovare informazioni che non sono prontamente disponibili su un sito Web. Google Dorking, noto anche come Google hacking, può restituire informazioni difficili da individuare tramite semplici query di ricerca.

Metagoofil – Strumento di raccolta di informazioni progettato per l'estrazione di metadati di documenti pubblici (pdf, doc, xls, ppt, docx, pptx, xlsx) appartenenti a un'azienda target.

Recon-ng – Framework di ricognizione progettato con l'obiettivo di fornire un ambiente potente e open source.

Check Usernames – Controlla l'uso di un marchio o nome utente su 160 Social Network

TinEye – Motore di ricerca di reverse image. È il primo motore di ricerca di immagini sul Web a utilizzare la tecnologia di identificazione delle immagini anziché parole chiave, metadati o filigrane.

Searchcode – Motore di ricerca gratuito di documentazione e codici sorgente. Gli snippet di codice e i repository open source (software libero) sono indicizzati e ricercabili.

Recorded Future – Soluzione basata sull'intelligenza artificiale per la previsione delle tendenze e l'analisi dei big data. Utilizza vari algoritmi AI e dati strutturati e non strutturati per prevedere il futuro. Gli utenti possono

ottenere dati OSINT sulle tendenze passate e sulle tendenze future.

SpiderFoot – Strumento di ricognizione open source disponibile per Linux e Windows. Si integra con una GUI semplice e interattiva con una potente interfaccia a riga di comando.

Wayback Machine – Archivio digitale del World Wide Web e altre informazioni su Internet. Contenente una copia cache della Internet pubblica.

VirusTotal – Sito web che permette l'analisi gratuita di files e/o URLs per scovarne virus o malwares all'interno. Utilizza più di 70 software di antivirus tra cui Kaspersky, Avira, BitDefender, AVG, ESET, G-Data, Comodo, Malwarebytes e McAfee. VirusTotal permette l'invio di files di dimensione massima di 128 MB

GeoTweet – Programma per la ricerca di tweet, tag, hashtag e utenti, con posizioni e mappe

RedditInvestigator – Raccoglie i dati che Reddit rende disponibili e li elabora per ottenere alcune nuove informazioni utili.

Spokeo – Aggregatore di social network che raccoglie e accorpa dati da fonti online e offline. Questi dati aggregati possono contenere dati demografici, proprietà e indici di ricchezza.

theHarvester – Strumento per ottenere email e informazioni relative a domini.

Shodan – Motore di ricerca che fornisce molte informazioni sulle risorse che sono state connesse alla rete. I dispositivi possono variare da computer, laptop, webcam, segnali stradali e vari dispositivi IOT.

Creepy – Strumento open source che raccoglie informazioni sulla geolocalizzazione utilizzando varie piattaforme di social network e servizi di hosting di immagini che sono già

pubblicati altrove.

Social Mention – Piattaforma di ricerca e analisi sui social media che aggrega i contenuti generati dagli utenti provenienti da tutto il mondo in un unico flusso di informazioni.

NameCHK – Applicazione web gratuita che consente di visualizzare la disponibilità di un determinato nome utente.

PasteLert – Sistema semplice per cercare "paste" e impostare avvisi (come gli avvisi di Google) per le voci di pastebin.com.

Whoisology – Un database consultabile con riferimenti incrociati dei record di proprietà dei nomi di dominio correnti e storici.

GlobalFileSearch – Motore di ricerca FTP con ricerca file avanzata su server ftp in tutto il mondo. software gratuito,

OneMillionTweetMap – Strumento di social media che può essere utilizzato per visualizzare tweet e dati aggregati di Twitter in una mappa del mondo.

GitRob – Strumento che aiuta a trovare file potenzialmente sensibili inviati a repository pubblici su Github.

Sublist3r – Strumento Python progettato per enumerare i sottodomini di siti Web utilizzando OSINT.

Knowem – Consente di verificare immediatamente l'uso di un marchio, prodotto, nome personale o nome utente su oltre 500 siti Web di social media popolari ed emergenti.

Tinfoleak – Sito Web in cui è possibile ottenere informazioni dettagliate su un utente di Twitter. Utilizza le informazioni geografiche visualizzate nei tweet e nelle immagini caricate per individuare il luogo in cui si trovava l'utente.

InSpy – Strumento di enumerazione LinkedIn basato su Python

Domain Hunter – Controlla i domini scaduti per la categorizzazione/reputazione e la storia su Archive.org per determinare i candidati idonei per phishing e nomi di dominio C2.

DNS Twist – Generatore di nomi di domini simili a quello che viene inserito, con controllo dell'effettiva registrazione. Utile per rilevare errori di battitura, attacchi di phishing, frodi e spionaggio aziendale.

CignoTrack – Strumento di spionaggio aziendale per testare la privacy e la sicurezza utilizzando OSINT e il social engineering.

UINames – Strumento per generare nomi falsi da utilizzare in progetti e modelli. (incluse imagini da associare alle persone).

Condividi l'articolo

- Analisi forenze, attacchi, capture the flag, Codice Statico, Debugger, Decompiulatore, Hacker etico, Hacking, Osint, reverse engineering, Seganografia, Sergio Caruso

Mosca: i poliziotti vendono l'accesso alle telecamere di controllo

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/12/09/la-cassetta-degli-attre

zzi-del-bravo-hacker/