Hacking tools (autore: Vittorio Albertoni)

Premessa

I filoni su cui opera la sicurezza informatica sono sostanzialmente tre.

Abbiamo innanzi tutto il filone dell'Open Source Intelligence (in acronimo OSINT) che comprende attività finalizzate a raccattare in maniera mirata informazioni provenienti da fonti aperte (open source è qui usato in questo senso) cioè da luoghi (soprattutto siti internet) nei quali, volutamente, di necessità o per distrazione queste informazioni sono disponibili senza protezione. Qui si va da tool che si occupano di rastrellare indirizzi email a quelli che si occupano di cluster analysis su elementi desunti da comportamenti sui social network, più a meno collegata a geolocalizzazione (al fine di estrarre da tutta la marea dei così detti big data qualche cosa di classificabile ed elaborabile).

Altro filone quello dell'informatica forense, dove ci si occupa di analizzare qualsiasi dispositivo elettronico suscettibile di contenere informazioni allo scopo di renderle disponibili e formalmente utilizzabili per un processo giuridico. Qui si va da tool per il recupero di file cancellati o danneggiati a quelli per il recupero di exif di foto ritoccate onde ricostruire la foto prima del ritocco e ad altre finezze di questo tipo. Ovviamente anche con tool che rendono impossibile fare queste cose.

Infine abbiamo il filone che fa perno sui penetration test che si occupa di come, ogniqualvolta vi siano almeno due apparecchiature collegate tra loro, si possa vulnerare la riservatezza del loro collegamento per impadronirsi di dati o, addirittura, del governo di una o più delle apparecchiature collegate. Qui si va dal più banale tool per hackerare password WiFi a tool per sferrare attacchi mirati a una rete o a una macchina specifica.

Indice

1 Raccolte di tools

Gli strumenti utilizzati per l'kacking sono centinaia e si tratta di programmi per computer, come tutti gli altri installabili su un sistema operativo in grado di farli girare.

La numerosità di questi programmi, in parte dovuta al fatto che esistono più programmi che, pur con sfumature diverse, fanno le stesse cose, è anche e soprattutto dovuta alla grande varietà delle attività che si sono sviluppate nel campo della sicurezza informatica ed alla estrema specializzazione dei programmi per svolgerle.

Anche un esperto hacker ci si può perdere dentro e proprio gli hacker hanno pensato di organizzare raccolte di questi programmi. Anzi, visto che si tratta sempre di software

libero concepito per il sistema Linux e visto che il kernel Linux si presta alla costruzione di raccolte di programmi comprensive del sistema operativo per farli funzionare (le così dette distribuzioni, gergalmente «distro») si sono create, appunto, raccolte dotate del sistema operativo.

Le due raccolte che presento in questo manualetto sono di questo tipo.

2 Kali Linux

E' la distribuzione dedicata alla sicurezza informatica, basata su Debian Linux, più ricca di tools e più usata.

Nasce nel 2006 con il nome di BackTrack e dal 2013 è curata dalla Offensive Security e si chiama Kali Linux.

Il suo sito web è *https://www.kali.org/* e vi troviamo una ricca documentazione, purtroppo in inglese. Da qui possiamo scaricare le immagini ISO che ci vengono proposte con tante possibilità di scelta: a 32 bit (anche in versione light) o a 64 bit (in varie versioni del desktop).

Presentandosi confezionata in un file immagine ISO, essa si presta ad essere installata sul computer, a lato di altri sistemi operativi presenti o su macchina virtuale all'interno di un sistema operativo presente, oppure su supporto USB esterno.

Se penso ai dilettanti evoluti ai quali dedico i miei manualetti direi che l'installazione su computer è sconsigliata in quanto mi sembra sproporzionata all'uso effettivo che si farà di quanto installato.

Buona alternativa potrebbe essere l'installazione su supporto USB esterno.

Per un utilizzo saltuario che non preveda la gestione di progetti della durata di settimane o mesi con necessità di memorizzazione di passaggi intermedi - diciamo così, per un semplice vedere di cosa si tratta - sono convinto che la via più semplice sia quella dell'uso di una versione live attraverso l'inserimento dell'immagine ISO su supporto avviabile (DVD o pennetta USB). In questo modo nulla si perde nell'efficacia di funzionamento dei vari programmi: unici inconvenienti quello di una certa lentezza se lavoriamo da DVD e, in ogni caso, quello di non poter memorizzare cose da ritrovare alla prossima seduta (ivi comprese eventuali personalizzazioni del desktop).
Infine, nel caso dell'utilizzo della versione live, il piccolo fastidio di dover lavorare con tastiera USA: le lettere sono allo stesso posto rispetto alla tastiera italiana, ma molti simboli sono in posti diversi, come risulta dallo schema riprodotto nella seguente figura 1:

Figura 1: Schema della tastiera USA

Per lavorare in versione live basta scaricare l'immagine ISO e masterizzarla su DVD o inserirla su pennetta USB avviabile.

Quest'ultima operazione si può fare con il software unetbootin, scaricabile da
https://unetbootin.github.io/
nella versione adatta al nostro sistema operativo (Linux, Windows o Mac OSX).
Chi usa Linux Mint può ricorrere al tool MintStick che si trova installato con il sistema operativo (su *https://pkgs.org/download/mintstick* si può scaricare il file .deb per l'installazione su Debian e Ubuntu).

Visto che mi rivolgo non a veri e propri hacker ma a aspiranti tali o semplici dilettanti curiosi, devo rammentare che, sia per installare quanto ci serve sul computer, sia per installarlo su chiavetta USB, sia se scegliamo la strada di utilizzare l'immagine in modo live su DVD o chiavetta, dobbiamo predisporre il computer ad avviarsi dal supporto che utilizziamo: in genere, infatti, il computer nasce predisposto ad avviarsi dal disco fisso interno; anzi i più recenti computer dotati (chiamiamoli «dotati» con questo eufemismo) di sistema operativo Windows da 8 in poi sono anche protetti in maniera tale da poter fare solo questo e ci obbligano a diventare hacker ancor prima di esserlo per rimuovere la protezione in tal senso, chiamata Secure Boot[1].

Chi non sappia districarsi in questa materia può facilmente trovare chiari suggerimenti e tutorial in rete. Per gli utenti Windows, in particolare, mi pare molto efficace ciò che si trova all'indirizzo
https://www.ceotecnoblog.com/come-fare-boot-da-chiavetta-usb-con-uefi-bios/

La versione 2018.4 di Kali Linux, rilasciata nell'ottobre 2018, a 64 bit con desktop xfce si presenta come dalla seguente figura 2.

Figura 2: Come si presenta Kali Linux xfce

Al momento dell'accesso vengono richiesti identificativo utente e password ed occorre inserire, rispettivamente, `root` e `toor`.

[1] In proposito rimando al mio articolo «Più difficile essere liberi con UEFI, anche grazie a Windows» del marzo 2017, archiviato nella categoria Suggerimenti vari nel mio blog all'indirizzo *www.vittal.it*.

I tool che troviamo in questa distribuzione sono veramente tanti.

La seguente figura 3 mostra quelli presenti specificamente in tema di Open Source Intelligence, campo nel quale Kali Linux è più debole.

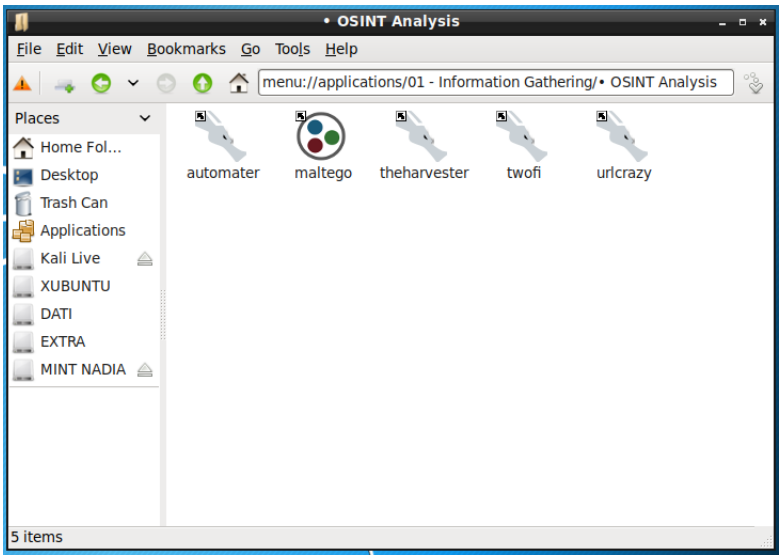

Figura 3: I tools di Kali Linux in tema di OSINT

Circa la presenza del software Maltego, elaborato dalla Paterva e proprietario, va chiarito che quella presente in Kali Linux è la versione Community, che, ovviamente, ha meno funzionalità rispetto alla molto costosa versione in vendita sul sito della Paterva (*https://www.paterva.com/web7/*). Per utilizzare Maltego Community va comunque aperto un account gratuito su questo stesso sito.

La seguente figura 4 mostra la scelta che ci viene offerta in tema di informatica forense.

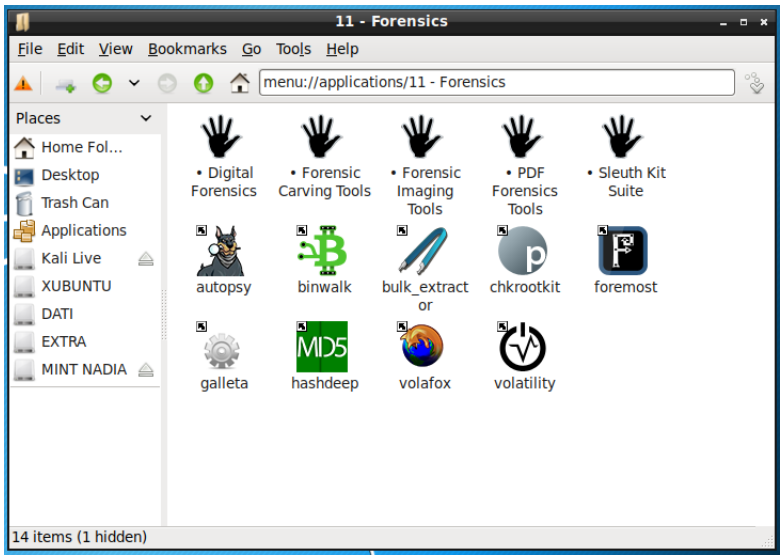

Figura 4: I tools di Kali Linux in tema di informatica forense

Infine la zona più ricca, quella dell'attacco e dei penetration test. La seguente figura 5 mostra l'ampia scelta di tool per attacchi a reti wireless.

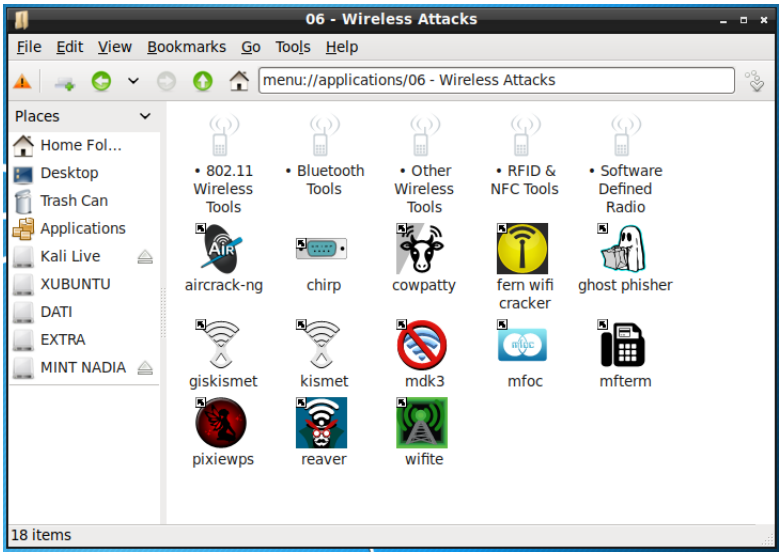

Figura 5: I tools di Kali Linux in tema di attacchi wireless

Per avere un'idea della quantità di tools che ci offre Kali Linux basti pensare che quello che abbiamo visto è il contenuto di soltanto tre delle tredici voci di menu che abbiamo a disposizione e che risultano dalla seguente figura 6.

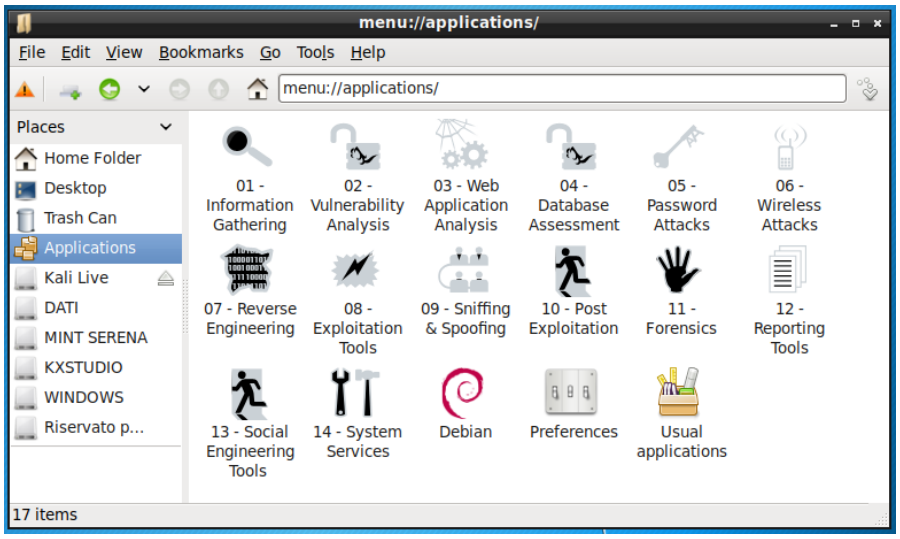

Figura 6: Le voci di menu di Kali Linux

Tra ciò che non abbiamo visto va citata la suite Burp, preziosa raccolta di strumenti per la sicurezza web, costoso software proprietario che in Kali Linux è presente con la Community Edition, ovviamente con funzionalità limitate.

La versione live di Kali Linux può essere avviata e utilizzata in forensic mode. In questa modalità abbiamo la certezza assoluta che il disco del computer ospite non verrà mai toccato, nemmeno nella memoria swap, e nessuna parte del file system del computer ospite verrà montata automaticamente.

3 Buscador

Buscador si integra bene con Kali Linux in quanto è prevalentemente orientato all'OSINT investigation, che abbiamo visto essere il campo in cui Kali Linux è meno dotato.

Lo troviamo all'indirizzo *https://inteltechniques.com/buscador/.*

Fino alla versione 1.2 rilasciata nell'Agosto 2018 veniva distribuito il file immagine ISO.

Purtroppo, con una decisione del suo patron Michael Bazzel che non riesco a comprendere ispirata da che cosa, la versione 2.0, rilasciata il 19 gennaio 2019 è distribuita soltanto su file per macchina virtuale, file con estensione .ova, e ci vengono proposti i file per la VirtualBox Oracle e per la VMWare.

La cosa ancora più tragica sta nel fatto che i file immagine ISO delle precedenti versioni, l'ultima non poi tanto vecchia, sono introvabili.

Pertanto, anche solo per vedere di che cosa si tratta, bisogna sobbarcarsi l'installazione e la configurazione di una macchina virtuale.

Sul sito da cui scarichiamo il file .ova per la macchina virtuale che intendiamo utilizzare troviamo istruzioni dettagliate in un facile inglese.

Per l'accesso ci viene proposto il nome dell'user `osint` e noi dobbiamo rispondere con la password `osint`.

In comune con Kali Linux contiene i tools più importanti dell'OSINT, TheHarvester e Maltego, quest'ultimo sempre nell'edizione Community.

In più qui troviamo tutta una serie di tools per l'esplorazione di siti e domini (Aquatone, EyeWitness, Recon-n, Spiderfoot, Sublist3r), per la geolocalizzazione (Creepy).

Altri tools utili, non proprio tipicamente orientati all'OSINT, ritengo siano Metagoofil (per l'estrazione di metadati) e BleachBit (per la pulizia del disco, delle memorie cache, ecc. in modo da rendere mai più leggibili e recuperabili i file eliminati).

Il browser Firefox che troviamo in Buscador ha preinstallati alcuni componenti aggiuntivi utili per le investigazioni sul web. Li vediamo dalla seguente figura 7.

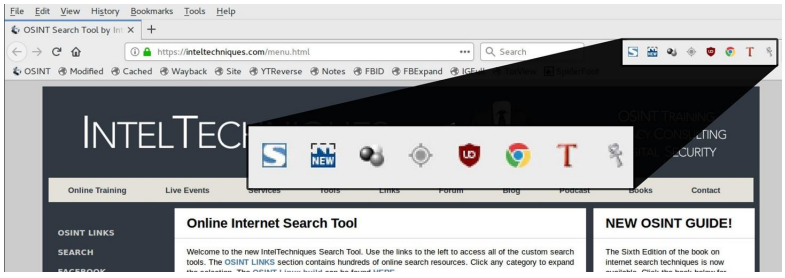

Figura 7: Componenti aggiuntivi Firefox preinstallati in Buscador

Nell'ordine abbiamo:
FireShot e Nimbus, per acquisire schermate dettagliate di pagine web per elaborarle e archiviarle;
DownloadHelper e Bulk Media Downloader, per la raccolta di video e audio pubblicati online;
Ublock Origin, per il filtraggio dei contenuti delle pagine web;
User-Agent Switcher, che ci consente di impersonare qualsiasi dispositivo al fine di ottenere diverse versioni delle pagine web;

Google Translate, per ottenere la traduzione delle pagine in varie lingue;
Resurrect Pages, per trovare vecchie versioni di pagine web.

In Buscador è installato anche il browser Chrome, già predisposto per la navigazione anonima, pure arricchito da una serie di componenti aggiuntive, come vediamo dalla seguente figura 8.

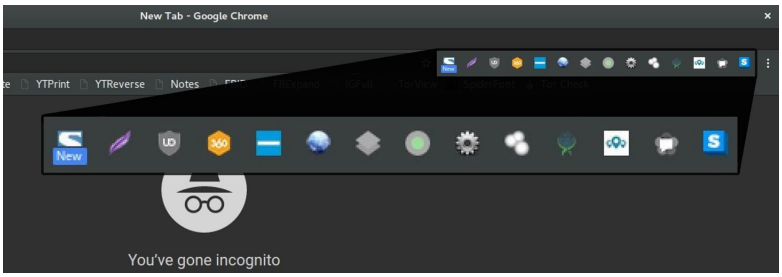

Figura 8: Componenti aggiuntivi Chrome preinstallati in Buscador

Nell'ordine abbiamo:
Fireshot e Take a screenshot, per acquisire schermate dettagliate di pagine web per elaborarle e archiviarle;
Ublock Origin, per il filtraggio dei contenuti delle pagine web;
360social e Prophet, per ricerche su siti sociali di informazioni su determinate persone;
User-Agent Switcher, Wappalyzer, SwitchyOmega e Web Developer, per impersonare qualsiasi dispositivo al fine di ottenere diverse versioni delle pagine web e per analizzare la tecnologia sottostante un sito web;
Shodan, ThreatPinch e ipinfo.io, per scoprire informazioni su un sito specifico;
Web RTC Leak Prevent Toggle e HTTPS Everywhere, come strumenti di privacy per l'investigatore e per isolare l'investigazione di pagine web dannose.

A proposito di navigazione anonima, Buscador ci offre anche il Tor Browser, che ne è la massima espressione.

4 Capirci qualche cosa

Abbiamo la possibilità di sapere cosa fanno esattamente i vari tools contenuti nelle distribuzioni che abbiamo visto ricorrendo alle relative documentazioni in lingua inglese.

Per quanto riguarda Kali Linux dobbiamo ricorrere al suo sito *https://www.kali.org/*, in particolare alla pagina
https://www.kali.org/tool-listing.
Qui troviamo elencati, suddivisi per categoria, tutti i tools direttamente accessibili in quanto installati ed anche tools non installati ma installabili con `sudo apt install` (ciò che non possiamo fare in maniera stabile se lavoriamo in live come io ho consigliato di fare tanto per cominciare).
Cliccando sul nome del tool che ci interessa apriamo una finestra in cui troviamo la descrizione di tutto ciò che esso fa, con esempi di utilizzo.

Per quanto riguarda Buscador non esiste altrettanta documentazione e per avere qualche cosa di prima mano dovremmo acquistare il libro dell'ideatore di Buscador, Michael Bazzell - Open Source Intelligence Techniques: praticamente il buon Mike ci regala il

software ma ci fa pagare la documentazione e ci offre una ricca serie di corsi on-line a pagamento per imparare l'hacking buono.

Sulle tecniche di hacking che utilizzano i tools che abbiamo visto troviamo comunque buoni libri, anche in italiano.

Per un inizio suggerisco, di Karina Astudillo, Hacking etico 101, disponibile come ebook su Amazon.

Un po' più tosto, di Riccardo Meggiato, Imparare l'hacking, edito da Apogeo su carta.