KALI LINUX vs PARROTSEC vs BACKBOX

Date : 8 settembre 2017

Quando si parla di sicurezza informatica e sistemi operativi dedicati a simulazioni e test di intrusione, Linux, il mondo Unix-like e l’open source dettano legge.

Le distribuzioni dedicate al pentesting sono oramai diverse, facilmente reperibili e sempre più user-friendly. Mentre fino a qualche anno fa la scelta cadeva inevitabilmente su BackTrack e BugTraq, il professionista IT moderno ha l'imbarazzo della scelta quanto a strumenti da aggiungere al proprio arsenale.

Ad oggi lo stato dell'arte è rappresentato da Kali Linux, il fiore all'occhiello della Offensive-Security di Mati Aharoni nonché successore del progetto BackTrack, che dal 2004 cominciò a tenere incollati allo schermo fino a tardi i più incalliti smanettoni e appassionati di hacking e affini.

Ma qual è la distribuzione Linux più indicata per un pentesting?

Chiunque abbia avuto punti di contatto con il mondo Cyber security si è posto questo interrogativo. La questione, spesso oggetto di dibattito su forum e blog, risulta senz’altro interessante, non solo per il professionista navigato ma anche per il neofita che si avvicina alla sicurezza informatica applicata.

Per rispondere dobbiamo prima passare brevemente in rassegna le caratteristiche dei più diffusi sistemi operativi e trarre qualche conclusione; tralasciando il progetto made in India Cyborg Linux causa troppa esuberanza (si tratta di un sistema che raccoglie tutti i tool in circolazione dedicati al pentesting), ad oggi Kali Linux, gli italiani Parrot Security OS e Backbox sono i candidati più autorevoli di cui il pentester/smanettone dispone.

Come detto, Kali è il punto di riferimento per tutti: chiunque ha iniziato da qui e qualsiasi dev ha preso spunto da questa distribuzione per i propri progetti. È molto sicura, è sviluppata dal più rinomato team di Cyber security e racchiude tutti i tool e framework che occorrono. E ancora, la documentazione a corredo, le svariate possibilità di personalizzazione della propria ISO e l'elevata stabilità di sistema, fanno propendere la maggior parte degli utenti per questo OS.

Di contro i repository predisposti sono piuttosto limitanti per un utilizzo più ‘tranquillo’, l'accesso

di default come utente root -sebbene facilmente rimediabile con qualche comando da terminale- non è certo il massimo della vita e l'interfaccia grafica si è un po' appesantita nel corso degli anni. Insomma, pur lasciando inappagati diversi utenti (autore compreso), è la distribuzione pensata nè più nè meno per il professionista IT, che senza tanti fronzoli vuole avere a disposizione tutto l'occorrente per poter mettere in crisi una rete, un'applicazione web, un sistema operativo.

Fortunatamente le community si danno sempre da fare e oggi troviamo alcuni interessanti progetti italiani che giungono in soccorso dell'insoddisfatto utente.
Parrot, nella sua versione full , comprende tutti gli strumenti racchiusi in Kali con diversi repository in più, è anch'essa disponibile per architetture ARM e si presenta con un ambiente desktop più snello e vicino alle esigenze dell'utente medio. Troviamo poi, a differenza di Kali, rilevanti raccolte di tool dedicati ad analisi forense, programmazione e crittografia, oltre a una sezione relativa all'anonimato ricca di interessanti script automatici che forzano tutte le connessioni di sistema sotto rete Tor.

Anche l'attività di sviluppo post-release è degna di nota; il team di sviluppo fornisce risposte praticamente in tempo reale su social e blog, rilasciando fix con encomiabile costanza.

Infine, il progetto Parrot offre la possibilità di noleggiare VPS a prezzi contenuti, con tutto l'occorrente per proseguire le proprie attività di pentesting su cloud.
Nonostante l'ottimo potenziale, si segnalano alcune note dolenti, vedasi la presenza di bug, difficoltà negli aggiornamenti di sistema che spesso si traducono in fastidiosi grattacapi o instabilità di sistema e una compatibilità hardware out-of-the-box non all'altezza di Kali.

Backbox si pone come alternativa ai due sistemi descritti poc'anzi; caratteristiche principali sono l'estrema leggerezza e semplicità di utilizzo, tipica dei sistemi Ubuntu-based . La distribuzione si presenta con un numero più limitato di tool e repository in un ambiente desktop ad ogni modo snello e ben organizzato; tutorial ufficiali consentono comunque di modificare i sorgenti software e appoggiarsi a quelli di Kali. Ottimo e molto stabile il sistema di anonimizzazione e di cancellazione della RAM allo spegnimento. Anche Backbox offre la possibilità di acquistare piattaforme cloud per le proprie attività ma non supporta installazioni su architetture ARM.

Bene, dopo questa didascalica e pedante presentazione delle principali distribuzioni, diamo una risposta all'interrogativo iniziale riguardo a quale sia la più indicata: tutte, o magari nessuna.

A mio avviso non sarebbe corretto optare aprioristicamente per un sistema piuttosto che un'altro; la scelta dipende dall'utilizzo finale e dalle esigenze del singolo: il professionista esperto che non ha, in ragione del suo lavoro, particolari necessità di privacy o anonimato probabilmente sceglierà la collaudata Kali, il neofita che desidera un sistema più sfruttabile e che si sta appassionando alla realtà Cyber security preferirà Parrot e ancora l'utente che cerca una suite di programmi funzionali, strutturati in un ambiente stabile e di immediata gestione, avrà bisogno di Backbox.

Nulla vieta poi all'utente di personalizzare e rendere più vicino al proprio modus operandi la distribuzione scelta; chi ha a che fare con il mondo della sicurezza informatica sa che non è il

numero di tool preesistenti a fare la differenza ma l'approccio e la metodologia di indagine intrapresi, oltre -come è giusto che sia- alle proprie conoscenze specifiche.

Per concludere, ritengo che non sia così decisiva e vincolante la scelta del sistema operativo da cui partire per i propri test e dunque non sia il caso di indugiare più di tanto in tale operazione: certo, siamo nel 2017 e avendo diversi mezzi a nostra disposizione è assolutamente lecito domandarsi cosa sia meglio per l'utente. Ricordiamoci solo che, in fin dei conti, la maggior parte del lavoro sporco viene quasi sempre svolta dal caro vecchio terminale indipendentemente dalla distribuzione Linux adoperata ed è chi si trova dietro lo schermo a fare il vero pentesting!

A cura di: **Milo Caranti**