HACKERATO

GUIDA PRATICA E DEFINITIVA A KALI LINUX E ALL'HACKING WIRELESS, CON STRUMENTI PER TESTARE LA SICUREZZA INFORMATICA

TEKTIME

ALAN T. NORMAN

HACKERATO

Guida pratica e definitiva a Kali Linux e all'Hacking Wireless, con strumenti per testare la sicurezza informatica

Alan T. Norman

Traduttore: Manuel Martignano

Indice

Capitolo 1. Kali Linux

Prima di addentrarci nell'hacking wireless, occorre conoscere i ferri del mestiere. Non esiste strumento migliore, soprattutto per un hacker principiante, di Kali Linux. È un software gratuito, stabile, ben mantenuto e incredibilmente completo per l'analisi della sicurezza informatica, si è sviluppato nel crogiolo delle distribuzioni open source di Linux ed è emerso come il re di tutti i sistemi operativi per l'hacking. È il successore della famigerata distribuzione BackTrack e possiede tutto ciò di cui un hacker, dal principiante al più esperto, ha bisogno.

Breve storia di Unix e Linux

Nei primi anni '70 del Novecento, il S***istema Operativo*** (SO) ***Unix***, abbreviazione di UNICS (UNiplexed Information and Computing Service), nacque da un defunto progetto sviluppato dai laboratori AT&T Bell Labs allo scopo di consentire a più utenti l'accesso simultaneo ai computer mainframe. Dopo essere stato ufficializzato, la sua popolarità crebbe e iniziò a rimpiazzare i primi sistemi operativi su alcune piattaforme mainframe comuni. Venne scritto originariamente in linguaggio ***assembly***, ma la riscrittura nel linguaggio di programmazione ***C*** migliorò la sua portabilità. Alla fine, diverse versioni di Unix emersero sul circuito commerciale, inclusa una per microcomputer. Nei decenni successivi presero forma molti SO ***"Unix-like"*** e da esso derivati, tra cui ***Mac OS*** della Apple, ***Solaris*** della Sun Microsystem e ***BSD*** (Berkeley Software Distribution).

Gli sforzi per creare una versione libera di Unix iniziarono negli anni '80 con il progetto ***GNU*** ("GNU's Not Unix") ***GPL*** (General Public License), che però fallì nel produrre un sistema efficace. Questo spinse il programmatore finlandese Linus Torvalds a sviluppare, come progetto studentesco, un innovativo ***kernel*** (il nucleo di un SO) di Unix. Utilizzando il sistema operativo Unix-like ***Minix***, creato per scopi accademici, Torvalds nel 1991 codificò con successo un kernel di un SO,

rendendo il codice sorgente libero al download pubblico e alla manipolazione da parte della GNU GPL. Il progetto venne poi chiamato ***Linux*** (combinando il nome di Torvalds, "Linus", con "Unix").

Sebbene il termine Linux inizialmente si riferisse solo al kernel sviluppato da Torvalds, alla fine finì per indicare qualsiasi pacchetto di SO basato sul kernel Linux. Essendo uno strumento ***open source***, diverse distribuzioni Linux si svilupparono nel corso dei decenni, con set unici di librerie software, driver hardware e interfacce utente. La flessibilità e l'efficienza di Linux portarono a una sua diffusa adozione da parte di appassionati di informatica e di alcune grandi aziende, sia come misura di risparmio, sia per eludere il monopolio sui sistemi operativi da parte di Microsoft.

Poiché il software aziendale e di consumo più famoso è scritto per le piattaforme Microsoft e Apple, Linux non ha mai avuto l'ubiquità o l'attrattiva commerciale dei sistemi operativi Windows e Macintosh. Tuttavia, la flessibilità, la portabilità e la natura open source di Linux lo rendono ideale per la creazione di distribuzioni leggere e altamente personalizzabili che servono a scopi molto specifici. Queste distribuzioni sono solitamente costruite a partire dal kernel, installando solo le librerie minime e le componenti necessarie per raggiungere gli scopi dell'hardware host. Questa strategia produce un sistema operativo che utilizza la memoria, l'archiviazione e le risorse del processore al minimo ed è poco vulnerabile in termini di sicurezza. Linux, con la struttura e la sintassi di Unix su cui è basato, è uno strumento essenziale nonché conoscenza di base per un hacker moderno.

Sono emerse centinaia di singole distribuzioni Linux commerciali e open source che, attualmente, girano su qualsiasi dispositivo, dai più piccoli come i cellulari e gli smartwatch, ai personal computer, i server mainframe e gli hardware militari. Molte di queste distribuzioni si sono diramate a partire da una manciata di pacchetti Linux precedenti, tra cui ***Debian***, ***Red Hat*** e ***SLS***.

Debian Linux e Knoppix

Debian, uno dei primi progetti di distribuzione Linux gratuiti e open source, è stato intenzionalmente creato per rimanere tale pur mantenendo elevati standard di qualità. Debian ha avuto diverse importanti distribuzioni proprie, oltre a decine di progetti spin-off che utilizzano il kernel Debian e la libreria di base. Mentre due di questi progetti, ***Linspire*** e ***Ubuntu*** (una distribuzione molto popolare), erano principalmente destinati agli utenti di PC domestici, il progetto ***Knoppix*** è stato progettato per essere eseguito direttamente da un supporto esterno, come un CD-ROM. Questo, insieme alla sua capacità di interfacciarsi con una vasta gamma di hardware, ha reso Knoppix uno strumento ideale per la risoluzione dei problemi, il salvataggio dei dati, il recupero delle password e altre operazioni tecniche. Knoppix è stata una base naturale da cui sono state successivamente generate le varie sotto-distribuzioni di sicurezza, forensi e di ***penetration testing***.

BACKTRACK LINUX

Due distribuzioni basate su Debian Knoppix che si concentravano sul penetration testing furono ***WHAX*** (precedentemente ***Whoppix***) e la ***Auditor Security Collection***. Entrambi i progetti furono eseguiti su Live CD e presentavano un ampio repository di strumenti per i test di penetrazione. WHAX e Auditor Security alla fine si fusero nella famosa distribuzione nota come ***BackTrack***.

KALI LINUX

La suite completa per la sicurezza offensiva e difensiva inclusa in BackTrack Linux, lo ha reso lo strumento preferito da hobbisti, professionisti della sicurezza, penetration tester ufficiali e hacker con intenti criminali (black hat). La società sviluppatrice di BackTrack, Offensive Security, alla fine riscrisse la distribuzione, rinominando il progetto in ***Kali*** Linux. I pacchetti di installazione di Kali e le immagini delle macchine virtuali sono disponibili gratuitamente. Offensive Security offre anche corsi a pagamento per l'utilizzo di Kali in sicurezza, nonché certificazioni professionali e un ambiente online di penetration testing.

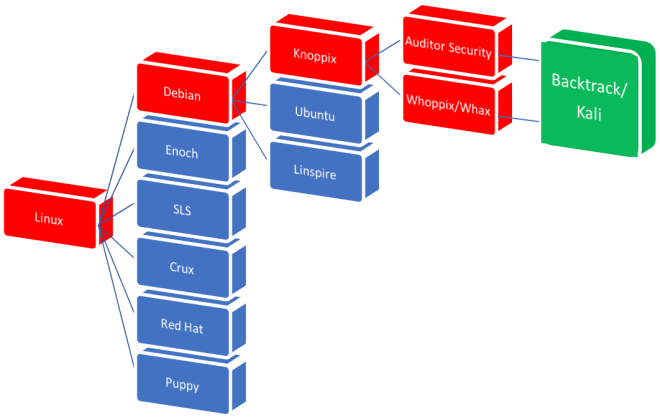

Figura 2 - Evoluzione di Kali Linux

Strumenti di Kali

Il fulcro di Kali Linux, nonché la ragione principale della sua popolarità tra gli hacker e i professionisti della sicurezza, è la sua ampia e ben organizzata suite di strumenti gratuiti. Kali comprende attualmente più di 300 strumenti, tra cui: raccolta di informazioni passive, valutazione delle vulnerabilità, analisi forense, password cracking, analisi della rete, hacking wireless e una potente serie di strumenti di exploitation. Sebbene tutti gli strumenti inclusi con Kali siano gratuiti e open source, e possano essere scaricati e installati su gran parte delle versioni Linux (basate su Debian), avere un SO testato e approvato che possiede di serie una vasta gamma di strumenti è una risorsa inestimabile.

Tra gli strumenti più utili forniti con Kali ci sono:

Metasploit Framework: Metasploit è una popolare piattaforma di sfruttamento delle vulnerabilità contenente vari strumenti di analisi e penetrazione. Dispone di molteplici opzioni per l'interfaccia utente e fornisce la possibilità di attaccare quasi ogni sistema operativo. Kali contiene anche ***Armitage***, una piattaforma di gestione grafica che aiuta l'utente a organizzare le operazioni e le interazioni tra più strumenti Metasploit durante un attacco.

Wireshark: Wireshark è uno strumento multipiattaforma di analisi del traffico di rete in tempo reale. Tutto il traffico su un dato nodo di rete

viene acquisito e suddiviso in metadati di pacchetti utili, tra cui intestazione, informazioni di routing e payload. Wireshark può essere utilizzato per rilevare e analizzare gli eventi di sicurezza della rete e per risolvere i problemi di rete.

John the Ripper: John the Ripper è un leggendario strumento di password cracking contenente tantissimi algoritmi per attaccare le password. Sebbene originariamente scritto solo per Unix, è ora disponibile su diversi sistemi operativi. Una delle sue caratteristiche più utili è la capacità di rilevare automaticamente la crittografia di tipo "***hash***" delle password. La versione gratuita di John the Ripper disponibile su Kali supporta il cracking di molti algoritmi di hash delle password, ma non tanti quanti la sua controparte a pagamento.

Nmap: Nmap, abbreviazione di "Network Map" o "Network Mapper" (mappatore di rete), è un comune strumento di hacking che è essenziale per i test di penetrazione. Nmap consente all'utente di eseguire la scansione di una rete per tutti gli host e i servizi di rete collegati, in modo da avere una visione dettagliata della struttura e dei membri di quella rete. Inoltre, Nmap fornisce un elenco dei sistemi operativi installati da ciascun host e delle relative porte aperte. Ciò consente all'utente di puntare sulle vulnerabilità rilevate durante l'exploitation.

Aircrack-ng: Aircrack-ng è il pacchetto software per eccellenza per l'analisi wireless e i test di penetrazione, che si focalizza su protocolli di crittografia Wi-Fi come ***WEP*** (Wired Equivalent Privacy), ***WPA*** (Wi-Fi Protected Access) e ***WPA2-PSK***. È dotato di strumenti per lo sniffing e l'injection di pacchetti wireless, l'analisi della rete wireless e il cracking di password criptate. Aircrack-ng richiede un hardware di interfaccia di rete che supporti la funzione ***modalità monitor***. Kali dispone anche di un programma di hacking wireless noto come ***Fern***.

BurpSuite: BurpSuite è una raccolta di strumenti che si concentrano sullo sfruttamento delle applicazioni Web. Questi programmi interagiscono non solo per rilevare le vulnerabilità nel Web, ma anche per lanciare attacchi.

La lista di cui sopra non è affatto completa, funge solo da esempio rappresentativo della potenza e della flessibilità che Kali Linux fornisce come piattaforma per i test di penetrazione e per la sicurezza informatica in generale. Kali può essere eseguito da supporti ottici o USB, come SO autonomo su computer fisso o portatile, oppure in un sistema ad avvio multiplo o all'interno di una macchina virtuale contenuta a sua volta in un altro SO host. Il capitolo successivo descrive come installare e configurare Kali su vari sistemi operativi per creare un ambiente appropriato per l'hacking e i test di penetrazione.