Introduzione

E se l'arma informatica più potente del mondo non fosse un exploit zero-day ma il trucco più vecchio del mondo? In questo panorama in rapida evoluzione della sicurezza informatica, la creazione di script bash è rimasta un'abilità fondamentale, offrendo molto più di un semplice modo comodo per interagire con il sistema operativo.
Scritta da Brian Fox nel 1989, la shell bash è impiegata dalla maggior parte delle versioni del sistema operativo Linux, che gestisce una quota impressionante dell'infrastruttura di calcolo mondiale. Trovate Linux nella vasta rete di server che costituiscono la spina dorsale di Internet, ma anche impiegato a orchestrare missioni spaziali, abilitare transazioni finanziarie e far progredire l'intelligenza artificiale.
L'ubiquità di Linux ha reso lo scripting bash un'abilità essenziale per gli hacker che intendono padroneggiare l'arte di *vivere coi piedi per terra*, ovvero usare gli strumenti e i processi nativi di un sistema per condurre attacchi, il che può permettere loro di mimetizzarsi da attività legittime per evitare di essere scoperti. Più i penetration tester si affidano troppo a un arsenale sempre crescente di strumenti sviluppati da terzi, più faranno fatica a operare in ambienti ristretti con un accesso limitato agli strumenti.
Inoltre, lo scripting bash consente agli hacker di automatizzare l'esecuzione degli strumenti a riga di comando. Per esempio, consente loro di concatenare più strumenti, di rivolgerli contro più obiettivi o di pianificare strategicamente la loro esecuzione. Realizzando script, gli hacker possono sviluppare potenti ed efficienti routine di penetration testing adatti alle loro esigenze.
Che siate penetration tester, cacciatori di taglie, studenti che muovono i primi passi nel campo della sicurezza informatica o incaricati della difesa che sperano di immaginare le tecniche degli hacker, questo libro vi insegnerà a sfruttare lo scripting bash in tutte le fasi di un impegno attivo alla sicurezza. Imparerete a realizzare script offensivi riutilizzabili, a usare la shell bash per girovagare nelle reti e a immergervi nel sistema operativo Linux.

Che cosa troverete in questo libro

Questo libro si apre trattando le basi della sintassi e dello scripting bash. Poi applica quelle competenze a ogni fase delle attività di un penetration test su una rete target basata su Linux, dall'accesso iniziale all'esfiltrazione dei dati. Nel farlo, esploreremo il sistema operativo Linux e in tal modo affinerete le vostre competenze di hacking con la shell bash.

- Il Capitolo 1 presenta una panoramica di alto livello della sintassi della shell bash, incluso l'assegnamento di variabili, l'uso di operatori aritmetici, la gestione dei codici di input e di output e molto altro ancora.
- Il Capitolo 2 copre concetti più avanzati, come le condizioni di test, l'uso dei cicli, il consolidamento del codice in funzioni e l'invio di comandi in background. Imparerete anche alcuni modi per personalizzare l'ambiente bash per il penetration testing.
- Il Capitolo 3 guida nella creazione della macchina-laboratorio da usare nel resto del libro. Useremo Kali Linux e un ambiente target vulnerabile basato su Docker per fare pratica con l'hacking tramite la shell bash.
- Il Capitolo 4 tratta le attività di ricognizione su una rete da un punto di vista a black box. Combinerete l'uso di vari strumenti di hacking e degli script bash per automatizzare la raccolta di informazioni.
- Il Capitolo 5 esplora i modi per usare la shell bash per identificare e sfruttare le vulnerabilità. Imparerete a realizzare script bash per attività di scansione e fuzzing, passaggi cruciali per qualsiasi attività di penetration testing.
- Il Capitolo 6 si addentra nelle tecniche per ottenere un punto d'appoggio con privilegi limitati su un sistema target, con particolare attenzione all'implementazione di web shell e all'iniezione di comandi del sistema operativo. Scoprirete anche vari modi per estendere l'operatività in ambienti shell limitati, gettando le basi per i successivi attacchi.
- Il Capitolo 7 si occupa della creazione di reverse shell, una tecnica di accesso iniziale che scambia la direzione della connessione ai server remoti. Imparerete la teoria che è alla base del funzionamento delle reverse shell, quindi le sfrutterete per ottenere un accesso stabile a una macchina remota.
- Il Capitolo 8 esplora i modi per raccogliere informazioni da un host Linux violato senza inviare pacchetti attraverso la rete, i quali potrebbero rivelare le vostre attività. Navigherete nella directory dei file e nel sistema di autorizzazioni di Linux, raccoglierete informazioni sulle sessioni utente, esplorerete il software installato e molto altro ancora.
- Il Capitolo 9 esamina i possibili percorsi per un'escalation dei privilegi, come autorizzazioni configurate in modo errato, risorse condivise e altri difetti del sistema.
- Il Capitolo 10 esplora i modi per rendere il vostro accesso a una rete resiliente ai cambiamenti dell'ambiente. Sottrarrete credenziali, modificherete configurazioni di servizio e molto altro ancora.
- Il Capitolo 11 descrive gli approcci a "spostamento laterale" per raggiungere altri server sulla rete target.
- Il Capitolo 12 copre i controlli di sicurezza difensivi comunemente presenti negli ambienti aziendali. Imparerete a manomettere gli strumenti di sicurezza ed esfiltrare informazioni da un sistema in modi elusivi.

Gli esercizi di scripting

Nel corso dei capitoli, troverete 29 esercizi che vi aiuteranno a mettere in pratica le vostre nuove competenze di scripting bash. Alcuni vi guidano alla realizzazione di interi

script, e poi vi incoraggiano ad ampliarli o migliorarli; altri vi invitano a scrivere i vostri script partendo da zero. Utilizzando la shell bash, svolgerete esercizi come i seguenti.

- Organizzare i risultati di una scansione in base al numero di porta (Capitolo 4).
- Eseguire il parsing dell'output delle utility di scansione web (Capitolo 5).
- Costruire un'interfaccia per sfruttare una vulnerabilità all'iniezione di comandi del sistema operativo (Capitolo 6).
- Scrivere un'utility di forza bruta SSH in grado di attaccare gli account utente (Capitolo 7).
- Cercare ricorsivamente nel file system i file log leggibili (Capitolo 8).
- Modificare in modo dannoso gli script dei task pianificati (Capitolo 9).
- Creare un programma per l'installazione di pacchetti dannosi (Capitolo 10).
- Scrivere uno scanner di porte basato sulla frequenza (Capitolo 11).
- Eseguire la scansione degli host violati alla ricerca di strumenti di difesa (Capitolo 12) e molto, molto altro ancora.

Come usare questo libro

Vi incoraggiamo a sperimentare attivamente le tecniche che introduciamo nel libro. Iniziate clonando il repository GitHub del libro, che si trova su `https://github.com/dolevf/Black-Hat-Bash`. Questo repository è ricco di script, categorizzati per capitolo, che possono aiutarvi ad applicare ciò che state imparandoo.

Notate, tuttavia, che le tecniche presentate sono intese a fini puramente didattici. Eseguite i vostri test esclusivamente su sistemi per i quali avete un'autorizzazione esplicita. Per affinare in modo sicuro le vostre competenze, nel Capitolo 3 vi guideremo nella configurazione di un vostro ambiente-laboratorio, dove potrete sperimentare a piacere senza alcun rischio.

Gli autori

Dolev Farhi è ingegnere della sicurezza e coautore di *Black Hat GraphQL* (No Starch Press, 2023). Ha una vasta esperienza nella direzione di team di ingegneria della sicurezza nel settore fintech e di sicurezza informatica e attualmente è ingegnere della sicurezza presso Palo Alto Networks, dove realizza sistemi di difesa per la più grande azienda al mondo nel campo della sicurezza informatica. Ha svolto lavori di formazione per percorsi di certificazione ufficiali Linux e, nel tempo libero, si diverte a ricercare vulnerabilità nei dispositivi IoT e a creare strumenti di sicurezza offensivi open source.

Nick Aleks è un importante leader della sicurezza informatica, il cui lavoro è stato fondamentale per proteggere i dati finanziari di milioni di canadesi. È direttore senior della sicurezza presso Wealthsimple e ha ricoperto il ruolo di ingegnere della sicurezza presso TD Bank. Nick è anche il responsabile dell'hacking presso ASEC e coautore di *Black Hat GraphQL* (No Starch Press, 2023). Membro senior del consiglio consultivo per i programmi di sicurezza informatica dell'Università di Guelph e del George Brown

College, ha oltre un decennio di esperienza nell'hacking di un po' di tutto, dai siti web, alle casseforti, alle serrature, alle auto e ai droni fino agli edifici intelligenti.

Il revisore tecnico

Kc Udonsi (CISSP) è attualmente architetto della sicurezza presso Stan Technology Inc., dove supervisiona l'assetto di sicurezza dell'azienda progettando e costruendo le sue difese. Ha esperienza nella direzione di team di ricerca nel settore della sicurezza informatica e nel mentoring di professionisti della sicurezza. Offre formazione sulla piattaforma *OpenSecurityTraining* ed è istruttore a contratto per la sicurezza dei sistemi e delle reti presso la sua *alma mater*, l'Università di Toronto, Scarborough. Nel suo precedente ruolo di ricercatore senior delle vulnerabilità presso Trend Micro, ha rivelato vulnerabilità significative ad aziende del calibro di Adobe e Microsoft.