Introduzione

Gli attacchi sferrati contro aziende e perfino contro Stati sovrani sono molto aumentati nel corso dell'ultimo decennio. Nel 2021, gli hacker hanno sottratto più di 100 milioni di dollari in criptovalute, hanno tentato di avvelenare l'approvvigionamento idrico della Florida, hanno violato il produttore di vaccini COVID-19 Pfizer Pharmaceuticals, hanno attaccato la Colonial Pipeline con un ransomware e hanno preso di mira agenzie governative e figure politiche in Francia, Germania, India, Paesi Bassi, Svezia, Ucraina ed Emirati Arabi Uniti. Poiché gran parte della nostra produttività dipende dalle tecnologie, gli attacchi alla nostra infrastruttura tecnologica possono avere conseguenze sociali ed economiche anche gravi.

Capire come difendere questa infrastruttura non è sufficiente. Abbiamo bisogno della protezione di sempre più hacker etici. Gli *hacker etici* sono persone che scoprono come attaccare le infrastrutture e individuano le vulnerabilità prima che vengano sfruttate da hacker malintenzionati. Gli hacker etici pubblicano quasi quotidianamente le nuove vulnerabilità nel National Vulnerability Database. Molti praticano anche una divulgazione responsabile, avvisando le aziende prima di rendere pubblica una vulnerabilità.

Perché leggere questo libro?

Questa guida pratica vi offre le competenze fondamentali di cui avete bisogno per diventare hacker etici. Dopo la lettura di questo libro, dovreste sentirvi più a vostro agio nell'iniziare una carriera di penetration tester, nel partecipare a una competizione capture-the-flag e perfino nel candidarvi per una posizione da "red team" di un'azienda. Ogni capitolo introduce un tipo di attacco, spiega i fondamenti della tecnologia trattata e presenta gli strumenti e le tecniche utili per sfruttarla. Acquisirete familiarità con strumenti come Kali Linux, Metasploit, la libreria pyca/cryptography e Maltego. Imparerete a raccogliere informazioni open-source, a sottoporre a scansione i sistemi e le reti alla ricerca di vulnerabilità, a scrivere exploit personalizzati e a progettare botnet.

Imparerete anche a creare i vostri strumenti con il linguaggio di programmazione Python, per comprendere i meccanismi che sono alla base dei comandi comunemente eseguiti dagli hacker. Entro la fine di questo libro, dovreste ritrovarvi a pensare come un hacker etico, in grado di analizzare attentamente i sistemi e creare nuovi modi per accedervi.

In sostanza, questo libro è rivolto a chiunque desideri imparare a svolgere attività di hacking. Non è richiesta alcuna esperienza di networking o informatica per comprendere le spiegazioni. È certamente meglio se avete una certa esperienza di programmazione, in particolare in Python. Ma anche se siete alle prime armi nel campo della programmazione, non preoccupatevi; troverete comunque istruttiva questa guida, per quanto riguarda la spiegazione delle tecnologie di rete e delle strategie degli strumenti di hacking. In alternativa, potete consultare il libro *Python* di Naomi Ceder, Apogeo 2019.

Installazione di Python

Le macchine virtuali che utilizzerete in questo libro sono preinstallate con Python 3, quindi non avete bisogno di installare esplicitamente Python per seguire i progetti presentati nel libro.
Vi consiglio vivamente di sviluppare all'interno di questo ambiente virtuale. Tuttavia, se utilizzate un sistema operativo che non offre preinstallato Python 3, dovrete installarlo. Potete scaricare l'ultima versione di Python 3 per il vostro sistema operativo visitando `https://www.python.org/downloads` e poi scaricando ed eseguendo il programma di installazione.

I contenuti del libro

Comincio mostrandovi come impostare l'ambiente del laboratorio virtuale in cui eseguirete gli attacchi descritti nel libro. Ogni nuovo capitolo descrive un diverso tipo di attacco, che potreste eseguire passo passo, dalla connessione a una rete WiFi in un bar alla violazione della rete di una grande azienda.

Parte I

Questa parte del libro si concentra sui fondamenti del networking ed esamina i vari modi in cui è possibile attaccare una rete. Tratteremo il protocollo TCP e l'architettura di Internet, oltre ai numerosi modi in cui gli hacker sfruttano queste tecnologie.

- Nel *Capitolo 1* configurerete il vostro laboratorio virtuale. Il vostro ambiente virtuale conterrà cinque macchine virtuali: un router che esegue pfSense, un desktop Kali Linux contenente gli strumenti di hacking, il server che violerete e due macchine desktop Ubuntu.
- Il *Capitolo 2* spiega in che modo Internet trasmette i dati e osserva come un malintenzionato può utilizzare l'ARP Spoofing per intercettare e leggere il traffico non crittografato di un utente. Poi, utilizzeremo alcuni strumenti pubblicamente disponibili per eseguire un attacco ARP Spoofing nel nostro ambiente virtuale ed estrarre gli URL dei siti visitati da un utente. Concluderemo il capitolo con un esercizio che incoraggia a scrivere un nuovo strumento di spoofing ARP in Python.
- Il *Capitolo 3* presenta lo stack del protocollo Internet e mostra come utilizzare Wireshark per acquisire e analizzare i pacchetti raccolti durante l'attacco ARP Spoofing.

Vi mostrerò anche come catturare i pacchetti che attraversano il firewall nel vostro ambiente virtuale.

- Il *Capitolo 4* esplora i fondamenti dei socket e della comunicazione fra processi. Quindi, vi mostrerò come scrivere la vostra reverse shell che potete usare per controllare da remoto una macchina. E sebbene controllare una macchina sia fantastico, gli hacker di solito vogliono controllare più macchine. Quindi vi mostrerò come farlo scrivendo un tipico strumento da hacker chiamato *botnet*. Come caso di studio, esamineremo l'architettura della botnet Mirai.

Parte II

In questa parte del libro discuteremo i fondamenti degli algoritmi di cifratura utilizzati per rendere sicure le comunicazioni digitali. Vi fornirò anche le basi per capire come funzionano diversi algoritmi di crittografia.

- Il *Capitolo 5* esamina le tecniche di crittografia simmetrica e asimmetrica, come gli One-Time Pad, i generatori pseudocasuali, i cifrari a blocchi e la crittografia RSA. Crittograferete e decrittograferete dei file e invierete un'e-mail crittografata. Concluderemo il capitolo scrivendo un ransomware.
- Il *Capitolo 6* si concentra sulla comunicazione sicura. Inizia con una discussione del protocollo TLS (*Transport Layer Security*). Quindi, tratterò l'algoritmo per lo scambio delle chiavi Diffie-Hellman e la sua alternativa più sicura, Elliptic Curve Diffie-Hellman. Concluderemo il capitolo estendendo il client ransomware, in modo che possa comunicare su un canale crittografato.

Parte III

In questa parte del libro, vi mostrerò in che modo gli hacker utilizzano le tecniche di ingegneria sociale e l'intelligence open-source per indurre le vittime a concedere loro un accesso indebito. In tal modo, vi mostrerò come potete sottoporre ad hacking chiunque, usando l'esca adatta.

- Il *Capitolo 7* discute i fondamenti delle tecnologie di posta elettronica e mostra come un malintenzionato potrebbe inviare un'e-mail falsificata. Discutiamo anche di come vengono generati i video deepfake e concludiamo generandone uno.
- Il *Capitolo 8* esplora alcune sofisticate tecniche di raccolta di intelligence open-source, nonché il modo in cui un malintenzionato può utilizzare Shodan e Masscan per cercare macchine vulnerabili in tutta Internet. Questo capitolo mostra anche come un malintenzionato può utilizzare strumenti come Nessus e `nmap` per identificare le vulnerabilità nei sistemi.

Parte IV

In questa parte, ci immergeremo nei numerosi modi in cui un malintenzionato può sfruttare una vulnerabilità che ha scoperto. Ogni vulnerabilità è unica, ma rientra in alcuni modelli generali. Esamineremo casi di sfruttamento di vulnerabilità nel mondo

reale, evidenziando gli schemi utilizzati. Esamineremo anche l'utilizzo delle pagine web come vettore di infezione.

- Il *Capitolo 9* inizia con uno sguardo alla vulnerabilità OpenSSL Heartbleed e al codice per sfruttarla. Quindi, introdurrò le tecniche di fuzzing utilizzate dagli hacker per individuare queste vulnerabilità e scriverete un vostro semplice fuzzer. Concluderò il capitolo trattando altre tecniche, come l'esecuzione simbolica e l'esecuzione simbolica dinamica.
- Il *Capitolo 10* tratta i trojan: programmi dannosi che si mascherano da programmi legittimi. Li esploriamo prendendo in considerazione un secondo case study: il malware russo Drovorub, un eccellente esempio di malware moderno, e vi mostrerò come ricreare qualcosa di simile utilizzando Metasploit Framework. Quindi, vedremo come creare dei trojan per dispositivi Linux, Windows e Android e vari modi subdoli per nascondere il malware.
- *Capitolo 11*: una volta che un malintenzionato ha installato il malware, spesso vorrà evitare di essere rilevato. Un modo per farlo consiste nell'installare un rootkit, che può modificare il sistema operativo per aiutare a nascondere il malware. In questo capitolo scopriremo come scrivere un rootkit per il kernel di Linux.
- Il *Capitolo 12* prende in considerazione un attacco chiamato SQL Injection e mostra come un hacker può utilizzare uno strumento chiamato SQLmap per iniettare codice dannoso in un'app web e usarlo per estrarre informazioni dal database. Questi database spesso contengono codici hash di password, quindi vi mostrerò come usare John the Ripper e Hashcat per decifrare questi codici hash.
- Il *Capitolo 13* esplora un'altra categoria molto diffusa di vulnerabilità web, il cross-site scripting, e vi mostrerà come un malintenzionato può utilizzarlo per iniettare codice dannoso nel browser di una vittima. Potrà così utilizzare tale codice per sottrarre i cookie o perfino violare la macchina dell'utente.

Parte V

Nella parte finale del libro, vi rivelerò come un malintenzionato può passare dal controllo di una singola macchina al controllo di qualsiasi altra macchina sulla rete. Discuterò anche dell'architettura e dei protocolli utilizzati all'interno delle reti aziendali e di come vengono sfruttati dagli hacker.

- Il *Capitolo 14* esamina il pivoting e il modo in cui un malintenzionato può attraversare un firewall o un router violato per accedere a una rete privata. Concluderò discutendo le tecniche di escalation dei privilegi che consentono agli hacker di ottenere i privilegi root sfruttando i bug del sistema operativo.
- Il *Capitolo 15* illustra l'architettura delle reti aziendali e i protocolli che esse utilizzano. Esamineremo in dettaglio i protocolli NTLM e Kerberos, oltre agli attacchi comuni contro questi protocolli, come gli attacchi pass-the-hash e l'attacco Kerberos Golden Ticket.
- Il *Capitolo 16* mostra come configurare un server privato virtuale rinforzato, che vi consenta di controllare sistemi posti al di fuori del vostro ambiente virtuale. Tratterò anche alcune aree dell'hacking etico che non ho esplorato in questo libro, nonché alcuni ottimi modi per entrare in contatto con la comunità degli hacker etici.

L'autore

Daniel G. Graham è professore assistente di informatica presso l'Università della Virginia a Charlottesville. I suoi interessi di ricerca includono la sicurezza dei sistemi embedded e delle reti. Prima di insegnare all'UVA, Graham era program manager Microsoft. Pubblica sulle riviste della IEEE articoli relativi ai sensori e alle reti.

Il revisore tecnico

Ed Novak è professore assistente di informatica al Franklin and Marshall College di Lancaster, Pennsylvania. Ha conseguito nel 2016 un dottorato di ricerca presso il College of William and Mary. I suoi interessi ruotano attorno alla sicurezza e alla privacy per i dispositivi mobili intelligenti.