Introduzione

Benvenuti a *Wireshark e Metasploit*. Scrivere questo libro è stato entusiasmante: è stato il lavoro combinato di più persone di formazione diversa (dalla sicurezza allo sviluppo del software, dallo sviluppo online di laboratori virtuali all'insegnamento) e il risultato dovrebbe essere di interesse per molti.
Wireshark è *lo* strumento per catturare e analizzare traffico di rete. Inizialmente si chiamava Ethereal, ma poi il nome è stato modificato nel 2006 e ora Wireshark è un programma consolidato e rispettato. Ma sono cose che già sapete, altrimenti perché avreste investito tempo e denaro in questo libro? Sicuramente siete qui per capire meglio come Wireshark possa semplificare il vostro lavoro e rendere più efficaci le vostre competenze.

Rassegna del libro e della tecnologia

Questo libro spera di raggiungere tre obiettivi.

- Ampliare le competenze dei professionisti della sicurezza informatica grazie a Wireshark.
- Fornire risorse di apprendimento, fra cui laboratori ed esercizi, per applicare quello che imparerete.
- Dimostrare come Wireshark sia di aiuto in situazioni reali mediante lo scripting con Lua.

Non dovrete solo leggere, ma fare. Qualsiasi libro può raccontare quanto possa essere meraviglioso Wireshark, ma questo vi dà anche la possibilità di esercitare le vostre abilità, di perfezionare le vostre competenze e di padroneggiare le caratteristiche di Wireshark. Queste possibilità hanno varie forme. In primo luogo, per applicare quello di cui si parla nel testo, farete esercitazioni in un laboratorio. Costruirete l'ambiente di laboratorio agli inizi del libro e lo utilizzerete nei capitoli seguenti. La seconda possibilità è alla fine di ogni capitolo (tranne l'ultimo), con esercizi che si basano sul laboratorio per mettervi ulteriormente alla prova, senza che qualcuno vi tenga per mano. Fra esperimenti di laboratorio ed esercizi, il tempo che passerete con Wireshark vi darà la certezza che quello della lettura sia tempo ben speso.
L'ambiente di laboratorio è stato creato mediante la tecnologia di containerizzazione, e il risultato è un ambiente virtuale piuttosto leggero che potrete installare ed eseguire sul

vostro sistema. Tutto l'ambiente è stato pensato specificamente perché possiate mettere in pratica i contenuti del libro. Il laboratorio è stato sviluppato ed è manutenuto da uno degli autori, Jessey Bullock. Il codice sorgente per le esercitazioni è disponibile online (i dettagli sono nel Capitolo 2).
In breve, il libro è una guida a Wireshark orientata alla pratica, creata per voi, professionisti della sicurezza informatica. Gli esercizi vi aiuteranno a continuare a migliorare la vostra conoscenza di Wireshark molto oltre l'ultima pagina.

Come è organizzato il libro

La struttura del libro si basa sul presupposto che il lettore parta dall'inizio e proceda con ordine. I tre capitoli iniziali introducono non solo Wireshark ma anche la tecnologia utilizzata per il laboratorio, nonché i concetti di base necessari. I lettori che già conoscono Wireshark dovranno comunque leggere il capitolo sull'installazione del laboratorio, poiché i capitoli successivi dipendono da quello. I primi tre capitoli sono necessari per poter utilizzare al meglio quelli che seguono.
La maggior parte del libro è poi strutturata in modo da analizzare Wireshark nel contesto della sicurezza informatica. Che si parli di catture, di analisi o di conferme degli attacchi, i contenuti del libro e le esercitazioni di laboratorio sono stati pensati in funzione dei professionisti della sicurezza.
L'ultimo capitolo riguarda Lua, il linguaggio di scripting che aumenta molto la flessibilità di Wireshark come potente analizzatore di rete. Inizialmente avevamo disperso gli script di Lua nei vari capitoli, ma poi abbiamo deciso di riunirli in un capitolo a sé stante, pensando che in fondo non tutti i lettori saranno anche programmatori.
Ecco una breve panoramica dei contenuti del libro.

- Il Capitolo 1, *Introduzione a Wireshark*, è per chi ha poca o nessuna esperienza con Wireshark. L'obiettivo principale è aiutarvi a non avere timore, introdurre l'interfaccia e mostrare come Wireshark possa esservi amico.
- Il Capitolo 2, *Configurazione del laboratorio*, non va assolutamente saltato. Partendo dalla impostazione di una macchina virtuale, vedremo poi come installare il W4SP Lab, che poi userete molte volte nei capitoli successivi.
- Il Capitolo 3, *Elementi fondamentali*, affronta i concetti di base e si divide in tre parti, relative rispettivamente alle reti, alla sicurezza delle informazioni e all'analisi dei pacchetti. Immaginiamo che molti lettori conoscano già uno o due di questi campi, ma il capitolo non dà nulla per scontato.
- Il Capitolo 4, *Cattura dei pacchetti*, analizza le catture di rete, ovvero la registrazione dei pacchetti di rete. Entreremo in profondità nei modi in cui Wireshark cattura, manipola e interpreta i pacchetti. Discuteremo anche di come lavorare con i molti tipi di dispositivi che si incontrano in una rete.
- Il Capitolo 5, *Diagnosi degli attacchi*, usa il W4SP Lab per ricreare vari tipi di attacchi che si possono incontrare facilmente nel mondo reale: attacchi Man-in-the-Middle, *spoofing* di vari servizi, attacchi di tipo Denial of Service e altri ancora.
- Il Capitolo 6, *Wireshark offensivo*, parla ancora di traffico maligno, ma assumendo il punto di vista dell'hacker. Verranno utilizzati ancora ampiamente Wireshark e il W4SP Lab per il lancio, il debug e la comprensione di exploit.

- Il Capitolo 7, *TLS, USB, keylogger e grafici di rete*, passa in rassegna varie attività in cui si può far leva su Wireshark. Dalla decifrazione di traffico SSL/TLS alla cattura di traffico USB su più piattaforme, l'obiettivo sarà dimostrare cose che potrete poi usare ovunque.
- Il Capitolo 8, *Scripting con Lua*, contiene circa il 95 per cento degli script del libro. Si apre con i concetti fondamentali dello scripting e l'impostazione di Lua, per chi lavora su Windows e per chi lavora su Linux. Gli script partono dall'inevitabile "Hello, World", ma arrivano al conteggio di pacchetti e ad argomenti molto più complessi. Vedremo come gli script possano modificare l'interfaccia grafica di Wireshark e si possano eseguire da riga di comando.

Per chi è questo libro

Dire che questo libro è per i professionisti della sicurezza può essere abbastanza specifico per chi in generale si occupa di IT, ma ancora un po' troppo generico per chi è di questo settore. Molti di noi si specializzano in qualche modo, e ci identifichiamo in base al ruolo o a ciò che ci appassiona: siamo amministratori di sistema o tecnici della sicurezza di rete, analisti di malware o responsabili della risposta agli incidenti.
Wireshark non è limitato a uno o due di questi ruoli. Possono aver bisogno di Wireshark i penetration tester come gli hacker etici, ruoli proattivi e impegnati. Ma anche gli analisti forensi, i verificatori di vulnerabilità e gli sviluppatori trarranno vantaggio dalla conoscenza di Wireshark, come mostreremo nei vari esempi.
Per quanto riguarda le conoscenze del lettore, il libro non dà nulla per scontato. Le specializzazioni nel campo della sicurezza sono abbastanza varie, per cui chi ha quindici anni di esperienza in un settore può essere del tutto alle prime armi in un altro. Wireshark ha un valore per tutti, ma richiede una conoscenza di base delle reti, della sicurezza e del funzionamento dei protocolli. Il Capitolo 3 servirà proprio a far sì che tutti i lettori abbiano a disposizione le informazioni indispensabili.
Nel seguito del libro, Wireshark verrà usato in contesti diversi, ma non sono richieste conoscenze specifiche per la comprensione degli argomenti o per un uso efficace del laboratorio. Per esempio, gli strumenti utilizzati nel Capitolo 6, *Wireshark offensivo*, saranno magari già noti ai penetration tester, ma il testo non presuppone alcuna esperienza e le istruzioni saranno comprensibili a tutti.
Per riepilogare: ci rendiamo conto che nel campo della sicurezza i ruoli possono essere molto diversi e che ciascuno ha un diverso livello di esperienza. Magari già ricoprite uno di questi ruoli e volete usare di più Wireshark, oppure state per assumere un nuovo ruolo e vi rendete conto che Wireshark è uno strumento essenziale. In ogni caso, il libro fa per voi.

Gli strumenti di cui avrete bisogno

L'unico strumento necessario per questo libro è un sistema. Il sistema non deve essere particolarmente potente; l'ideale è che sia una macchina che non abbia molti anni. Userete il sistema per la prima volta nel Capitolo 2; installerete e configurerete una macchina virtuale, poi su quella installerete il laboratorio.

Ovviamente, il libro può essere utile anche a chi non ha a disposizione un sistema, ma questo è necessario per seguire le esercitazioni di laboratorio presentate in tutto il testo.

Che cosa c'è sul sito web

Il sito web principale per questo libro è il repository GitHub per il codice del W4SP Lab. Il repository e i suoi contenuti sono illustrati nel Capitolo 2, dove scaricherete e costruirete l'ambiente del laboratorio virtuale.
Altri siti web sono citati nel corso del libro, in particolare come fonte di ulteriori risorse. Alcuni siti, per esempio, offrono centinaia di file di catture di rete, disponibili per l'analisi.

Riepilogo

Speriamo vorrete affrontare il libro e che troverete utili il testo, i suoi materiali e il laboratorio. Ci siamo impegnati molto, con l'unico desiderio di creare una risorsa che motivasse più persone a conoscere meglio Wireshark. Essendo a nostra volta professionisti della sicurezza informatica, abbiamo costruito questo libro per i nostri colleghi.