Relazione Find String

Progetto per il corso di Gestione di Reti A.A 2018/2019

Piangatello Marco

Introduzione

In questo progetto si analizzano alcune tecniche di attacchi informatici conosciute con il nome di Data exfiltration.

La parola Data exfiltration viene utilizzata per descrivere un trasferimento di dati non autorizzato da un computer o da un server. Questa attività può essere svolta in molteplici modi e con l'utilizzo delle più disparate tecniche, tipicamente è utilizzata da cyber criminali su Internet o in altre reti. L'esfiltrazione dei dati può essere compiuta manualmente, da un individuo con accesso fisico ad un computer, o può essere automatizzata attraverso l'utilizzo di programmi che utilizzano la rete come veicolo per i dati esportati.

Di seguito presenterò alcune possibili contromisure utilizzabili per identificare alcuni attacchi di questo tipo.

Descrizione Progetto

Il progetto Find Strings si basa sull'idea del riconoscimento di testo, in formato leggibile da un umano, all'interno dei pacchetti che transitano in uscita da una rete.

Monitorando i flussi di pacchetti che escono da una rete è possibile individuare eventuali minacce per la sicurezza dei dati. Il controllo è effettuato sul payload dei pacchetti. All'interno di questi viene ricercato del testo in chiaro in un formato leggibile da essere umano. In caso affermativo si può lanciare una allarme di sicurezza riguardante la connessione in cui transita il pacchetto.

Implementazione

Breve descrizione dei file che compongono il progetto

1. Find string.c : Implementa le funzioni che vengono utilizzate per il rilevamento di testo in chiaro all'interno dei byte del pacchetto. Ho

implementato due livelli di filtraggio delle stringhe. Il primo ripulisce da tutti i caratteri diversi da lettere o numeri, utilizzando la codifica ASCII. Il secondo invece utilizza un vocabolario di bigrammi(due caratteri consecutivi) che non possono trovarsi in parole in lingua inglese. Ogni volta che nella stringa viene riconosciuto uno di questi, i caratteri considerati sono scartati.

2. Test find strings.c Modulo utilizzato per testare le funzioni sopra descritte.

Istruzionoi per la Compilazione

lanciare il comando make per la compilazione

il comando [sudo] ./find_strings <nome.file> per lanciare il programma di test su un file di test.