



La sicurezza in Unix – *Seconda parte*

Nel corso della mia carriera universitaria, iniziando a programmare in C++, ebbi la prima prova della potenza distruttiva del buffer overflow. Ricordo come grazie alle semplici funzioni C quali ad esempio strcpy() e strcat(), riuscivo a far “traboccare” un semplice daemon. Mi accorsi subito che mettendo in input al programma un blocco di dati superiore ai byte del buffer, potevo semplicemente mettere in crash l'intera esecuzione e il bel programmino che avevo scritto con tanta pazienza, andava distrutto.

In Unix, avviene esattamente la stessa cosa, con la grande differenza che un Hacker che effettua con successo l'overflow di un daemon, avrà finalmente accesso come root al sistema. E' evidente a questo punto come l'attacco di buffer overflow sia molto pericoloso e continua a creare problemi di sicurezza.

La soluzione come indicato nel mio primo articolo è quello di scrivere ottimo software. Innanzitutto, diciamo subito una cosa, non esiste un software privo di bug! Anzi molto spesso, per esigenze di business, i programmatori sono costretti loro malgrado a dover sviluppare software velocemente trascurando dettagli che possono danneggiare la sicurezza dello stesso.

Non starò qui a dirvi come programmare correttamente, perchè ci vorrebbe un intero libro. Quello che posso consigliare è che prima di mettersi a scrivere codice, si deve fare un' eccellente analisi del software con tutti i requisiti che vengono richiesti al suo funzionamento.

Questo modo di procedere alla realizzazione di un software è detta Ingegneria del Software. Tale branca infatti, studia l'intero processo di sviluppo software secondo determinate tecnologie e metodologie.

Se si applicassero sempre questi principi, saremmo certamente sicuri di aver realizzato un software robusto e quanto meno più sicuro. Invito quindi tutti ad informarsi maggiormente sull'Ingegneria del Software, recuperando qualche utile materiale da internet o da uno dei tanti libri in circolazione. Detto questo possiamo sicuramente definire alcune pratiche di protezione da questo tipo di attacco. Innanzitutto possiamo validare l'input dell'utente, con un controllo sia sui byte sia su l'uso di librerie, ma soprattutto possiamo, anzi dobbiamo, fare tanti e tanti test sul nostro software. In Unix un ottimo progetto che riguarda appunto test di codice Unix, è OpenBSD (<http://www.openbsd.org>) .

Questo progetto è continuamente aggiornato ed è diventato uno dei punti di riferimento per quanto riguarda la sicurezza del codice Unix.

Nel prossimo articolo

Nel prossimi articoli parleremo dei problemi di sicurezza legati alla shell e ai servizi ftp ed rpc. Ah dimenticavo! Ecco una serie di programmi che aiutano a proteggersi contro gli attacchi di forza bruta, lascio a voi trovare i rispettivi link : **npasswd**, **cracklib**, **OpenSSH** e **SRP**.

PROFILO DOTT. SAVINO

Socio Sostenitore ANORC.

Laurea in Ingegneria Informatica presso l'Università Federico II di Napoli.

Presidente della Commissione Tecnica Open Source in ANORC.

Master ANORC, Xplor Italia e AssolIT in Gestione e Conservazione Digitale e Sostitutiva dei Documenti - Il Responsabile della Conservazione sostitutiva : ruoli, funzioni, strategie.

Relatore come esperto della Conservazione Sostitutiva a Docubusiness.

Corso avanzato di 3 giorni sulla Gestione del documento informatico negli adempimenti amministrativi del dottore commercialista presso la Sede Ordine dei Commercialisti ed Esperti Contabili di Napoli.

ISO 9001:2000 certified Networking Concepts Test.

ISO 9001:2000 certified Test of Knowledge of Joomla 1.5.

ISO 9001:2000 certified Information Technology Awareness and Terminology Certification.

Information Management Day IBM 2009.

Corso avanzato su Windows Server 2008 e Red Hat Linux Technical Overview a cura di Microsoft, Computer Gross S.p.a. e Fujitsu.

Seminari tecnici di 20 ore IBM Power System I presso l'Università Federico II di Napoli.

Documento Digitale : procedure per rendere l'ufficio più agile. Roma 1 Ottobre 2009.

Autore e giornalista presso la HTML S.r.l, sezione PMI.it (sito di informazione tecnologica dedicato interamente alle Piccole e Medie imprese Italiane)