

Linux e Sicurezza Informatica

A cura di: Simone Quatrini, Francesco Morucci, Marco Rondini



LINUX
D A Y
I T A L I A

Linux e sicurezza Informatica

Introduzione:

In questo talk verranno discussi argomenti sulla sicurezza informatica a livello locale e remoto propri dei sistemi Unix.

Cos'è un Bug e da dove ha origine il suo nome;

Introduzione ai Local Root / Privilege Escalation;

Stack Overflow e Buffer Overflow;

Cenni teorici e cenni pratici;

Local Root / Privilege Escalation;

Sicurezza al livello remoto;

Approfondimento su l'utilizzo dei permessi Apache e perché utilizzarli;

Software di Penetration Testing;



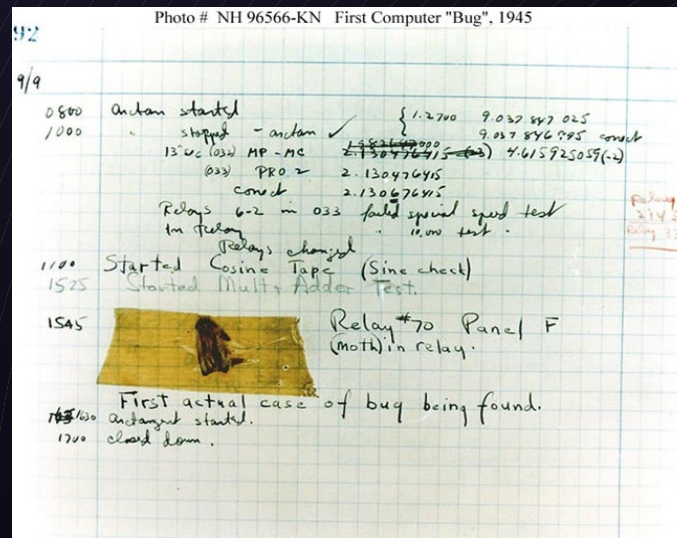
Linux e sicurezza informatica

Kernel bug:

Esistono molte versioni del kernel, ne escono di nuove soprattutto per supportare piu HW possibili, ottimizzare la gestione del sistema, ma anche per risolvere le falle della sicurezza generale.

Il primo *bug* della storia è stato scoperto nel 1946 da Grace Hopper, che trovò all'interno di una macchina una blatta che aveva fatto saltare i circuiti. Da qui il termine (*bug, insetto in inglese*).

Per 'bug' del kernel si intende il malfunzionamento sia software che dell'hardware, come anche errori esistenti nella programmazione che possono essere usati dagli *hackers* per accedere il sistema (es. aree di memoria mal gestite o incontrollate).



Linux e sicurezza Informatica

Introduzione a: Local Root / Privilege Escalation

Questa tipologia di attacco, oggi anacronistica, permette a chi ne fa utilizzo di prendere pieno controllo della macchina;

Questa metodologia di intrusione sfrutta le applicazioni che mal gestiscono la memoria; L'attacco basa la sua efficacia nell'utilizzo di una tecnica chiamata Buffer Overflow;

Che cos'è un Buffer Overflow?



Linux e sicurezza Informatica

Stack Overflow / Buffer Overflow:

Il buffer è come una scatola, una zona di memoria usata temporaneamente per l'input o l'output dei dati. I cosiddetti "dati" sono le variabili sia locali che globali del programma in esecuzione;

Insieme al buffer abbiamo lo stack; al cui interno troviamo i riferimenti alle funzioni del programma. Dobbiamo però precisare che il buffer ha dimensione massima. L'overflow, (dall'inglese sovraccarico), avviene quando i dati inseriti escono al di fuori di questa scatola chiamata buffer.

Il buffer overflow è uno degli errori di programmazione più comuni nei linguaggi di programmazione a buffer statici, come C, C++ e tutti i linguaggi da essi derivati. Il buffer overflow è uno degli errori più pericolosi per la sicurezza di un'applicazione, come anche di un sistema informatico. Benchè sia conosciuto e documentato da anni, al punto di essere spesso dipinto come 'la tecnica hacker per eccellenza', i bollettini di sicurezza pubblicano ancora, giornalmente, notizie su applicazioni o servizi soggetti a questo tipo di vulnerabilità. Questo a testimonianza del fatto che, oltre a essere un tipo di errore studiato e documentato, la sua applicazione è a tuttoggi valida.

Linux e sicurezza Informatica

Stack Overflow / Buffer Overflow:

A livello macchina, un buffer overflow consiste nel 'trabordamento' di un'area di memoria ove l'applicazione non ha diritto d'accesso.

Tale trabordamento è dovuto a un mancato controllo sulla dimensione della stringa di destinazione, con la conseguenza che i valori in eccesso trabordano al di fuori dello spazio massimo assegnato e sovrascrivono aree di memoria fondamentali.

Ora vedremo un esempio teorico di funzionamento del buffer overflow:

Codice sorgente in C vulnerabile all'attacco:

codice:

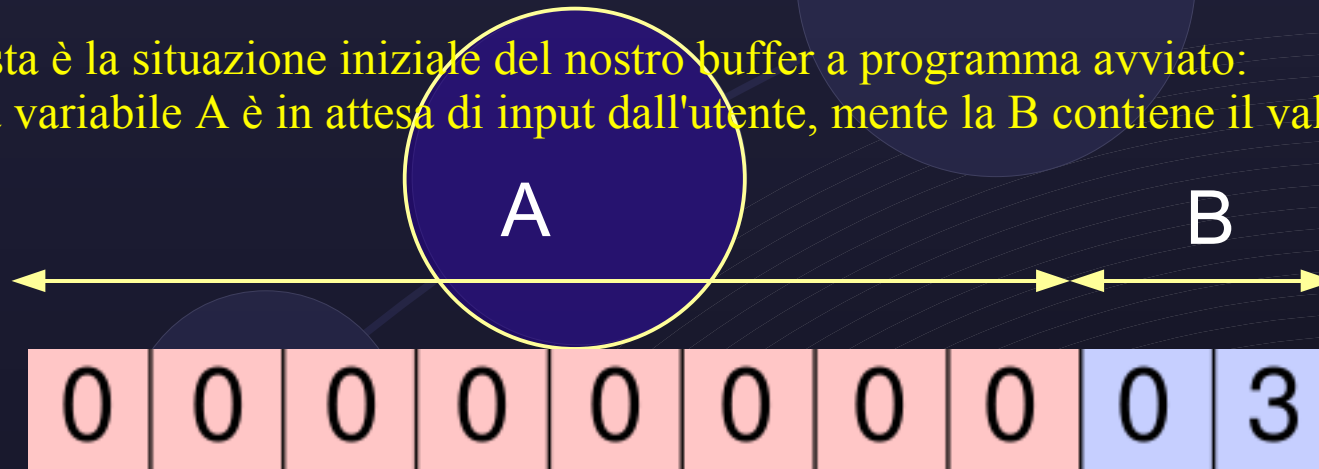
```
#include <stdio.h>

int main()
{
    char A[8] = {0};
    char B[2] = {0,3};
    printf("Inserisci il valore di A:\n");
    /*inserendo più di 8 caratteri il programma andrà in
    * Segmentation Fault(Buffer Overflow)*/
    scanf("%s",A);
    printf("Il nuovo valore di A è %s\n",A);
}
```

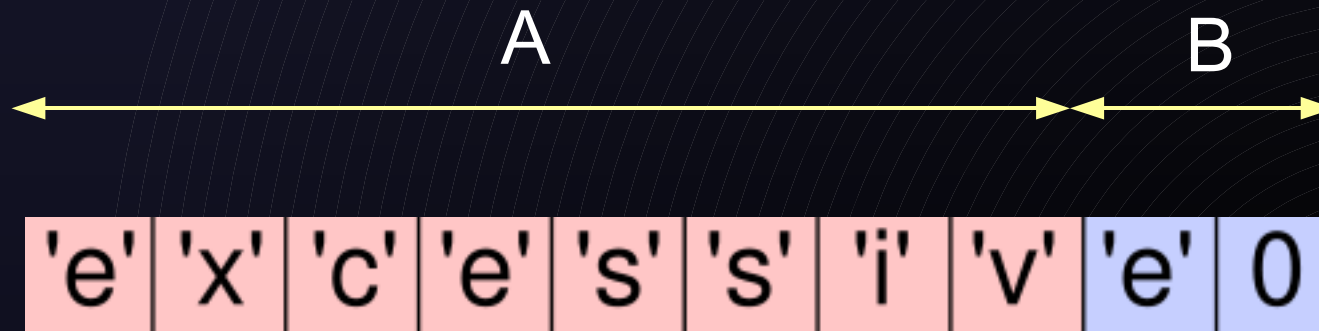
Linux e sicurezza Informatica

Stack Overflow / Buffer Overflow:

Questa è la situazione iniziale del nostro buffer a programma avviato:
La variabile A è in attesa di input dall'utente, mentre la B contiene il valore 03.



Mettiamo il caso che l'utente inserisca un valore che ha più di 8 caratteri (in questo caso “excessive”), vediamo che tutto l'eccesso andrà fuori dal buffer di “A” (nel nostro caso all'interno dell'area di memoria della variabile “B”), ma come abbiamo detto è un esempio teorico, perché l'eccesso potrebbe andare in altre zone di memoria



Linux e sicurezza Informatica

Local Root / Privilege Escalation:

Ora che abbiamo le basi di funzionamento di un attacco Buffer Overflow possiamo continuare con lo spiegare in dettaglio il funzionamento di un Local Root (anche chiamato attacco di privilege escalation);

Questo tipo di attacco sfrutta le librerie che si appoggiano al kernel, quest'ultime hanno quindi bisogno di girare a livello amministratore (runlevel 0).

In base a ciò che abbiamo descritto nell'esempio teorico di buffer overflow, invece dell'inserimento di caratteri, è possibile inserire un codice (chiamato shellcode) che altro non è che istruzioni assembly.

Quando la libreria attaccata andrà a leggere nella zona di memoria dov'è presente lo shellcode, quest'ultimo andrà in esecuzione con il possibile risultato di trovarci fra le mani una shell di amministratore.

Lo shellcode (come da nome), è un programma in linguaggio assembly che richiede una shell, dato che viene eseguito su una libreria che lavora da runlevel 0 la shell ritornerà con privilegi di root.

Per maggiori informazioni sulle shellcode per i vari sistemi operativi ed architetture visitate:
<http://shellcode.org/>

Teniamo sempre presente che dalla versione 2.6.21 del kernel l'allocazione della memoria non permette con tale facilità un Buffer Overflow come sopra descritto.

Linux e sicurezza Informatica

Differenza fra attacchi locali e remoti:

In realtà non c'è molta differenza fra queste due tipologie di attacco, ma in remoto la pericolosità è maggiore perchè il PC non è aperto solo alla rete locale, ma bensì a tutta la rete internet.

L'attacco più utilizzato a livello remoto e locale è il Buffer Overflow (già descritto in precedenza).

Elenco dei principali servizi che si interfacciano alla rete:

Porta	Descrizione
21/tcp	FTP - Il file transfer protocol - control
22/tcp	SSH - Secure login, file transfer
23/tcp	Telnet insecure text communications
25/tcp	SMTP - Simple Mail Transfer Protocol
80/tcp	HTTP
88/tcp	Kerberos
110/tcp	POP3
139/tcp	NETBIOS
143/tcp	IMAP
389/tcp	LDAP
443/tcp	HTTPS

Linux e sicurezza Informatica

Bug di applicazioni server:

I server sono ormai alla base della comunicazione degli utenti che si interfacciano alla rete. Il server è un elemento fondamentale dell'infrastruttura IT (di cui fa parte), in quanto i suoi malfunzionamenti si ripercuotono su tutti i client che lo usano. Pertanto, si adottano accorgimenti volti a garantire affidabilità e la sicurezza di ogni singolo server. Di seguito prenderemo in esame il settaggio dei permessi di un WebServer con Apache.



Linux e sicurezza Informatica

Problemi dei permessi utente:

La comodità dei webserver è quella di poter inserire più siti internet sulla stessa macchina (Hosting), senza spendere soldi per comprare un server per ogni sito web (Housing).

Il 90% degli utenti preferisce questa opzione, in quanto il costo è di molto inferiore se confrontato all'Housing.

Un amministratore di rete competente dovrebbe porre molta attenzione alla configurazione di un WebServer di Hosting e soprattutto all'assegnazione dei permessi degli utenti che ospita.

La maggior parte degli amministratori che gestiscono una Hosting Farm creano un unico utente (generalmente chiamato apache) che ha tutti i permessi di lavorare su quella directory di lavoro (generalmente /apache/www/).

Avendo i permessi di muoversi sulla root /apache/, è possibile vedere tutti i siti del server, cosa che non dovrebbe mai succedere (generalmente situati in /apache/www/[nome_dominio]/htdocs/).

Proprio per sfruttare queste dimenticanze, sono usciti su internet degli strumenti che, prendendo in esame un sito nel web, ne estraggono la lista di tutti gli altri "siti" presenti sullo stesso server (Reverse IP).

Vediamo ora come evitare ciò su un WebServer Apache.



Linux e sicurezza Informatica

Configurazione dei permessi su webserver Apache:

Il metodo più semplice ed efficace per mettere al sicuro le directory dei nostri clienti è quello di creare un utente per ogni sito web ospitato sulla macchina.

Creare un nuovo utente su linux:

```
sudo useradd comuneviterbo
```

sudo = comando che permette di eseguire operazioni da super utente

useradd = comando che permette di creare un nuovo utente all'interno della macchina

comuneviterbo = il nome del nuovo utente

Creare la cartella di Apache per il nuovo utente:

```
sudo mkdir /apache/www/comuneviterbo/
```

MKDIR = Questo comando crea semplicemente una nuova cartella

Linux e sicurezza Informatica

Configurazione dei permessi
su webserver Apache:

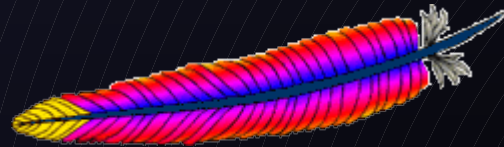
Settare i permessi alla cartella di Apache:

```
sudo chown comuneviterbo /apache/www/comuneviterbo/*
```

chown = Il comando è un'abbreviazione di Change Owner (cambia il possessore); Specifica che in quella determinata cartella può lavorarci solamente l'utente "Owner", gli altri utenti "non Owner" non potranno né scrivere, né modificare o leggere i file in essa contenuti.

comuneviterbo = sarà l'unico utente autorizzato a lavorare in quella determinata cartella.

* = L'asterisco (star) serve ad includere tutte le sottocartelle all'interno di /apache/www/comuneviterbo/



Linux e sicurezza Informatica

Penetration Testing:

Il processo di penetration testing è la metodologia di valutazione della sicurezza di un sistema.

L'analisi comprende più fasi, e ha come obiettivo l'evidenziare le debolezze della piattaforma fornendo il maggior numero di informazioni sulle vulnerabilità che hanno permesso l'accesso non autorizzato.

L'analisi è condotta al contrario, cioè dal punto di vista di un potenziale attaccante, e consiste nello sfruttamento delle vulnerabilità rilevate al fine di ottenere più informazioni possibili per accedere indebitamente al sistema.

Tutti i problemi di sicurezza rilevati vengono quindi presentati al cliente assieme ad una valutazione del loro impatto nel sistema e nello scenario del business aziendale, fornendo inoltre una soluzione tecnica o proposta di migrazione e mitigazione dello stesso

Il penetration test fornisce una stima chiara sulle capacità di difesa e del livello di penetrazione raggiunto nei seguenti confronti:

- * delle vulnerabilità interne al sistema;
- * delle vulnerabilità esterna al sistema;
- * della sicurezza fisica.

Linux e sicurezza Informatica

Software di Penetration Testing: BackTrack

Backtrack è una distribuzione Linux Live che deriva dalla fusione di WHAX e dalla Auditor Security Collection. Permette all'utente di utilizzare script modificabili, tool aggiuntivi e personalizzazione del kernel.

Il progetto backtrack fu creato da **Mati Aharoni** e **Max Moser** ed è il risultato di uno sforzo di collaborazione da parte di tutta la Comunità.

Sin dal 2006 questa distribuzione nasce con lo scopo di poter effettuare Penetration Testing in modo semplice ed assistito, avendo a disposizione centinaia di programmi divisi per categorie di tipologia:

Penetration Tester

Scanners

Password Attacks

Sniffers

Wireless Tools

Database Tools

Forensic Tools

Reversing

Dal sito ufficiale è possibile scaricare varie versioni (sia CD che USB) avviabili comodamente su qualsiasi computer ci si trovi.

L'ultima versione stabile è la BackTrack 3, rilasciata nel 1 luglio 2008 e include più di 300 tool di sicurezza e si focalizza principalmente sulla maggiore compatibilità/flessibilità hardware.



Linux e sicurezza Informatica

Software di Penetration Testing:
Backtrack, i tool più famosi:

Vediamo ora i più famosi tool che possiamo anche trovare su questa distribuzione:

Metasploit (Cat. "Penetration Tester") - Il Software più completo di PenTesting con la sua interfaccia avviabile da browser permette di scansionare una rete alla ricerca di vulnerabilità conosciute e di creare shellcode "ad-hoc";

Nmap (Cat. "Scanners") - Il più famoso, potente ed utilizzato port scanner mai creato; Velocità e dettaglio nel reporting dell'informazione; Possibilità di scansionare grandi range di IP;

Wireshark (Cat. "Sniffers") - E' un tool che analizza il traffico passante sia su rete cablata che da wifi; In tempo reale è possibile vedere, filtrare e bloccare i pacchetti passanti;

Suite Aircrack-NG (Cat. "Wireless Tools") - Gli strumenti principali della suite sono: un packet sniffer, un cracker ed un packet injector che insieme ci permettono di trovare la password di una rete WEP o WPA;

Linux e sicurezza Informatica

Links:

Raccolta di Local Root ed Exploit - <http://www.milw0rm.com> - <http://selfexploit.ihteam.net>
Bollettini di sicurezza - <http://secunia.com/advisories/>
BackTrack 3 - <http://www.remote-exploit.org>
Metasploit - <http://www.metasploit.com/>
Nmap - <http://nmap.org/>
WireShark - <http://www.wireshark.org/>
Suite Aircrack - <http://www.aircrack-ng.org/>

Domande?

www.ihteam.net

IHT

*Inclusion Hunter
Team*

