Jednoduchý rootkit

Roman Janko, xjanko04

Projekt do předmětu Bezpečnost informačních systémů

3. 11. 2012

Implementace

Projekt je rozdělen na 2 programy napsané v jazyce C:

- server, který poslouchá na portu 8000 a komunikuje s klienty,
- modul pro jádro linuxu (rootkit).

Rootkit upravuje tabulku systémových volaní - konkrétně odkaz na funkci getdents() = get directory entries.

Před samotnou úpravou tabulky je nutné povolit zápis do stránek paměti, které jsou pouze pro čtení, protože zde se nachází ona tabulka systémových volání. Stačí vynulovat bit WP (write protect) v registru CR0.

Tabulka systémových volání (sys_call_table) není od verze jádra 2.6 exportována, takže je nutné zjistit její adresu jinak. Naštěstí jsou dále exportovány některá volání. Adresu tabulky zjistím postupným skenováním paměti a znalosti adresy volaní sys_close.

V upravené funkci getdetns() volám originální funkci, která naplní buffer strukturami linux_dirent. Každá struktura odpovídá jednomu adresáři. Pokud chci nějaký adresář skrýt, tak musím odstranit správnou strukturu z bufferu. Ve virtuálním adresáři /proc má každý proces svůj adresář se jménem odpovídajícímu jeho process id (PID). Proto musím zjistit ze struktur task_struct čísla PID patřící jednotlivým instancím serveru (podle jména).

Techniky skrývání

Skrytí serveru, který poslouchá na portu, zajišťuje modul do jádra. Skrytí modulu pro jádro je řešeno úpravou vnitřních struktur jádra. Ve výsledku není modul vidět ani přes přikaz lsmod (adresář /proc) ani v adresáři /sys/module/. Neřeším navrácení těchto struktur do původního stavu, proto modul nejde odebrat příkazem rmmod.

Použití

make

insmod rootkit.ko

./server

$ telnet localhost 8000

Login: **root**

Heslo: **1234**