Posudek na práci

Analýza možností zapouzdření síťových protokolů do aplikačních a metod detekce na firewallech

Martin Nepivoda

Tématem práce je problematika zneužívání aplikační vrstvy TCP/IP pro tunelování komunikace na úrovni síťové vrstvy.

V práci je předložena analýza problematiky, naznačeny způsoby detekce tunelování a uvedena implementace řešení jednoho navrženého způsobu filtrace nežádoucího provozu.

Analýza předložená v kapitole 2 je zajímavá. Jsou uvedeny způsoby zneužití čtyř protokolů, které jsou v běžném „správném" provozu v podstatě nenahraditelné a tedy obvykle poskytované (HTTP, HTTPS, ICMP a DNS), takže je potenciální útočník má v podstatě vždy k dispozici. Autor ukazuje konkrétní možnosti zneužití za pomoci snadno dostupných prostředků.

V kapitole 3, věnované detekci zneužívání, autor probírá jednotlivé protokoly jednak z hlediska detekce pomocí analýzy obsahu a v druhé části kapitoly z hlediska detekce pomocí statistických metod. Tato kapitola obsahuje též náměty na řešení uvedených problémů.

Tato část práce je velmi přehledná a jasná. Ukazuje, že se autor v problematice dobře zorientoval a zdá se, že velmi dobře rozumí tomu, o čem píše.

Naproti tomu vytvořený program icmp-f pro filtraci zneužívání ICMP vzbuzuje značné rozpaky. Rozsahem je totiž velmi malý, až nicotný; zaměřuje se na jedinou funkci, pro kterou navíc využívá již existující knihovny libnetfilter_queue. Působí proto dojmem, že byl vytvořen pouze proto, aby byl naplněn implementační cíl práce daný zadáním. Vytvořený program je složený ze třech souborů (jeden hlavičkový + dva s implementací) a čítá celkem 15 tisíc znaků resp. 500 neprázdných řádků (vč. komentářů a ladících tisků). To je opravdu velmi málo, přestože deklarovanou funkčnost zjevně poskytuje. Vzhledem k autorem předloženým znalostem bych očekával výrazně větší dílo.

Drobnou poznámku si zaslouží ještě anglický abstrakt práce, který je psán velmi neobratně a je téměř nečitelný. Vlastní text (česky) je psán jasně, čitelně a bez chyb, což je jev bohužel řídký.

Doporučuji, aby práce byla přijata jako diplomová a byla připuštěna k obhajobě.

V Praze, 18.9.2008

RNDr. David Obdržálek