Posudek k diplomové práci

Hlavním cílem práce bylo vytvoření kontrolního seznamu pro bezpečnostní testování protokolů IPv6 a ICMPv6 včetně soupisu možných zranitelností s jejich popisem. Dále pak návrh a implementace nástrojů pro jejich automatizované testování.

Teoretická část je vhodně strukturalizována. Popsaný průběh testu ztvárněný diagramem na obrázku 3.1 a s tím spojený seznam popisovaných testů obsahuje ale bohužel jen velmi malou část testů, které by měl tester během testování realizovat. Vzhledem k omezené sadě testovacích případů, které studenka ve své práci zmiňuje, lze konstatovat, že na jejím základě není možné provést komplexní bezpečnostní test IPv6 sítě a připojených zařízení. V práci nejsou zmíněné například slabiny IPv6 ve spojitosti se soukromím uživatelů a běžně používané metody, které brání útokům na toto soukromí, jež je při použití veřejných IPv6 adres silně ohroženo.

Z textů uvedených u jednotlivých testů si také nejsem zcela jist, zda studentka správně chápe rozdíl mezi blackbox, whitebox a greybox metodou testování a nemohu tak zcela souhlasit se všemi jí uvedenými informacemi. Dále si nejsem jist, zda studentka dostatečně porozuměla problematice protokolu IPv6 a zda by byla schopna fungování protokolu popsat a v praxi tyto vědomosti uplatnit. Pro ověření těchto vědomostí, doporučuji položit studentce během obhajoby některou z níže uvedených otázek.

V praktické části práce vytvořila studentka pouze minimální možné množství nástrojů pro automatizované testování, přičemž během vývoje využila velké množství již existujících nástrojů, které pouze vhodně použila a zkombinovala ve svých skriptech. Vzhledem ke způsobu, jakým studentka vývoj pojala nástrojů, jí lze vytknout malou snahu o vývoj většího množství nástrojů sloužících pro otestování i dalších zranitelností, které v práci popisuje. Studentka tak sice splnila zadání, ale pouze v minimálním možném rozsahu.

U jednotlivých nástrojů mi dále chybí uživatelská dokumentace, která by novým uživatelům poskytovala informace o tom, k čemu daný nástroj slouží, jak funguje a jak jej lze používat. Dovolím si konstatovat, že pouze z dokumentace (soubory readme.txt), která je distribuována společně s nástroji, nebude uživatel schopen účel nástrojů správně pochopit a bez potíží je použít.

Návrh otázek k obhajobě

- Pokud se pomocí Vašeho nástroje *pticmpv6spoofing* podaří přesvědčit některý stroj na síti o tom, že počítač testera je router (dostaneme se do pozice MiTM), znamená to, že veškerá odchozí komunikace oběti bude směrována na počítač testera, nebo jen některá? Jak by komunikace vypadala například tehdy, pokud by otrávená oběť šla navštívit webové stránky, kde doména má v DNS uveden pouze záznam typu A. Jak se bude chovat zařízení oběti, pokud útočník vypne svůj počítač? Vyprchá otrava u oběti samovolně po nějakém čase?

V Luběnicích 30.5.2022
Roman Kümmel