Souhrnná zpráva za rok 2015 za projekt *„Návrh systému pro testování zabezpečení sítě IPv6 a zpracování incidentů v prostoru privátních adres“*

Smluvní výzkum „Návrh systému pro testování zabezpečení sítě IPv6 a zpracování incidentů v prostoru privátních adres“ zadaný organizací CESNET z.s.p.o. řeší problematiku bezpečnosti a účtování uživatelů v současných počítačových sítích.

Dnešní sítě postavené nad protokolem IPv6 musí splňovat stejné podmínky zabezpečení jako u sítí provozovaných pomocí protokolu IPv4. Stejně tak, při použití technologie NAT (překlad adres) je nutné správně spárovat globální a privátní adresy pro dohledání bezpečnostních incidentů. Smluvní výzkum mezi organizacemi VUT FIT a CESNET se snaží tyto problémy řešit a zaměřuje se na vývoj aktivní síťové sondy, která je schopna otestovat koncovou IPv6 síť z pohledu známých zranitelností. Problematiku mapování bezpečnostních incidentů projekt řeší vývojem rozšíření současných monitorovacích sond o export všech potřebných informací. Výstupy projektu tedy umožňují správci otestovat zabezpečení jeho IPv6 sítě zapojením aktivní sondy a jednoduše dohledat bezpečnostní incidenty i pokud jsou v síti používány privátní adresy společně s překladem adres.

Smluvní výzkum probíhá jeden rok a bude ukončen v květnu 2016. V průběhu roku 2015 probíhaly práce na vývoji penetračních nástrojů pro testování bezpečnosti IPv6 sítí se zaměřením na hlavní bezpečnostní zranitelnosti, zejména v lokálních sítích. Bylo zakoupeno několik zařízení a nástrojů určených pro vývoj – zejména levné síťové sondy, na kterých se budou vyvíjené nástroje používat a software určený pro vývoj nad specializovaným hardware firmy Xilinx.

Byly provedeny přípravné kroky (upraven firmware pro platformu ZE7000), které umožní vytvářené nástroje nahrát na specializované síťové sondy. V případě jednodušších sond postavených na platformě OpenWRT byla provedena základní portace potřebných programovacích knihoven, které využívají penetrační skripty. Současně byl vytvořen program zajišťující správné použití penetračních nástrojů pro zařízení s více síťovými porty. Díky tomu bude možné využít pouze jedno specializované zařízení (síťovou sondu) pro otestování zabezpečení IPv6 sítě oproti stávajícím řešením, kde je nutné mít více zařízení (síťovou sondu + zařízení pro analýzu síťových dat).

Část projektu zaměřena na detekci, párování a účtování uživatelů v prostoru privátních adres testovala dostupná řešení v provozním prostředí sítě VUT. Bylo otestováno několik volně dostupných nástrojů, které by bylo upravit a využít v rámci projektu, tak i komerční řešení firem Cisco a HP. Dílčí informace byly zveřejněny ve třech článcích na serveru root.cz [1,2,3].

Literatura:

[1] PODERMAŃSKI Tomáš a GRÉGR Matěj. Implementujeme Carrier Grade NAT: Nečekané nástrahy. *ROOT, informace nejen ze světa Linuxu*. Praha: 2015, roč. 2015, č. 1, s. 1-1. ISSN 1212-8309.

[2] PODERMAŃSKI Tomáš a GRÉGR Matěj. Implementujeme Carrier Grade NAT: Zálohování. *ROOT, informace nejen ze světa Linuxu*. Praha: 2015, roč. 2015, č. 1, s. 1-1. ISSN 1212-8309.

[3] PODERMAŃSKI Tomáš a GRÉGR Matěj. Implementujeme Carrier Grade NAT: Zákon, alternativy a IPv6. *ROOT, informace nejen ze světa Linuxu*. Praha: 2015, roč. 2015, č. 1, s. 1-1. ISSN 1212-8309.