NASTAVNO-NAUČNOM VEĆU ELEKTROTEHNIČKOG FAKULTETA U BEOGRADU

Komisija II stepena Elektrotehničkog fakulteta u Beogradu imenovala nas je za članove Komisije za pregled i ocenu master rada kandidata Boška Jolića pod naslovom „***IPv6 Security***". Nakon pregleda rada podnosimo sledeći

IZVEŠTAJ

1. Biografski podaci

Boško V. Jolić je rođen 18.09.1987. godine u Užicu. Elektrotehničku školu je završio u Užicu sa odličnim uspehom. Elektrotehnički fakultet u Beogradu upisao je 2006. godine, na modulu za Telekomunikacije i informacione tehnologije - smer Radio komunikacije. Diplomirao je u septembru 2011. godine sa prosečnom ocenom na ispitima 7.73, na diplomskom 10. Master studije na Elektrotehničkom fakultetu u Beogradu je upisao septembra 2011. na modulu Sistemsko inženjerstvo i radio komunikacije. Položio je sve ispite sa prosečnom ocenom 9.20. U avgustu 2012. godine je na Cisco akademiji Elektrotehničkog fakulteta u Beogradu položio *CCNA Exploration* kurs, pri čemu je dobio *Cisco CCNA Certifications*.

2. Predmet master rada

Predmet ovog master rada je IPv6 protokol i bezbednosne pretnje sa kojima se susreće IPv6 infrastruktura i njeni korisnici. IPv6 ima i prednosti i nedostatke sa stanovišta bezbednosti. IPv6 ima mnogo poboljšanih osobina koji ga čine bitno drugačijim od svog predhodnika. Ove osobine između ostalog uključuju prošireni adresni prostor, autokonfiguraciju, strukturu zaglavlja, zaglavlja proširenja, IPsec, mobilnost, kvalitet servisa, agregaciju ruta i efikasan prenos. Sve ove osobine omogućuju nove načine napada na mrežnu infrastrukturu. U okviru master rada, kandidat je analizirao Internet arhitekturu baziranu na IPv6 protokolu sa stanovišta sigurnosti.

3. Osnovni podaci o master radu

Master rad kandidata Boška Jolića „*IPv6 Security*", obuhvata 62 strane štampanog teksta sa 22 slike i 4 tabele. Rad je organizovan tako da sadrži uvod, pet poglavlja, zaključak, spisak literature i konfiguracije Cisco rutera.

4. Sadržaj i analiza rada

U uvodnom poglavlju Master rada razmotrena je neophodnost i značaj IPv6 protokola, odnosno razmotreni su razlozi za izradu teze.

U drugom poglavlju dat je kratak osvrt na IPv6 adresiranje. Predstavljeni su koncepti koji su relevantni za stavljanje u rad hosta na IPv6 mreži.

U trećem poglavlju predstavljene su osnovne karakteristike IPv6 protokola: format paketa, zaglavlja i odgovarajući mehanizmi.

U četvrtom poglavlju data je analiza bezbednosnih pretnji koje su se pojavile zahvaljujući novim aspektima u IPv6 i pretnji koje su ostale iste kao i kod IPv4 protokola.

U petom poglavlju predstavljeni su raspoloživi alati za zaštitu IPv6 mreža, pošto je bezbednosne polise i alate potrebno implementirati i koristiti u različitim delovima mreže.

U šestom poglavlju je opisano funkcionisanje *firewall*-ova u IPv6 okruženju, kao nezaobilaznih uređaja u procesu zaštite IPv6 mreža.

Sedmo poglavlje predstavlja zaključak i u okviru njega je dat pregled doprinosa ove master teze.

5. Zaključak i predlog

Sličnosti između pretnji zasnovanih na IPv4 i IPv6 navode da bezbednosne mere koje su definisane i proverene u slučaju IPv4 treba da budu korišćene i za IPv6, gde je to moguće, pri čemu su izvedeni sledeći zaključci:

1. Treba postaviti jednu adresnu šemu za komunikaciju sa hostovima unutar interne mreže i drugu za komunikaciju sa hostvima koji se nalaze van interne mreže.
2. Potrebno je sprečiti sobraćaj koji potiče od internih adresa da napusti mrežu. Zadržati *multicast* saobraćaj većeg obima unutar granica mreže. Filtrirati ICMP saobraćaj, ali imati na umu operativne funkcije ICMPv6, kao što je otkrivanje PMTU jedinice. Sprečiti saobraćaj koji sadrži nepotrebna proširenja zaglavlja za postavljene servise da pređe granice mreže. Sprečiti IPv6 fragmente upućene ka mrežnim elementima. Odbaciti fragmente paketa za koje ne može da se utrvdi viši sloj. Implementirati RFC 2847 filtriranje da bi se sprečili *spoofing* napadi. Blokirati saobraćaj koji za izvornu adresu ima *multicast* adresu. IPv4 *firewall*-ovi i filteri treba da blokiraju delove za mehanizme za tunelovanje koji nisu postavljeni na mreži.
3. Potrebno je implementirati zaštitu aplikacija i na nivou hosta i na nivou mreže (pomoću *firewall*-ova, sve dok IDS funkcionalnost ne bude raspoloživa).
4. Aplikacije bi trebalo da koriste šifrovanje kad god je to moguće. Koristiti autentifikaciju za BGP i IS-IS protokole za rutiranje. Koristiti IPsec za OSPFv3 i RIPng. Koristiti IPv4 IPsec-zaštićene puteve za IPv6 tunele. Zaštititi prenete podatke između rutera pomoću IPv6 IPsec-a.
5. Postavke sa dvojnim stekom se lakše osiguravaju i trebalo bi da imaju prednost u odnosu na tunelovanje. Ako se tunelovanje koristi za međusobno povezivanje IPv6 ostrva, statički tuneli su poželjniji nego dinamički, jer su bezbedniji.

Na osnovu svega izloženog, članovi Komisije predlažu Komisiji II stepena Elektrotehničkog fakulteta u Beogradu da rad Boška Jolića, pod naslovom „***IPv6 Security***“ prihvati kao master tezu i da kandidatu odobri javnu usmenu odbranu.

Beograd, 16.01.2013.

Članovi komisije:

dr Aleksandar Nešković, vanr. prof.

dr Nataša Nešković, vanr. prof.