

Rozvoj IDS s podporou IPv6

Radoslav Bodó, Michal Kostěnek
Západočeská univerzita v Plzni
Centrum informatizace a výpočetní techniky
email: {bodik, kostenec}@civ.zcu.cz

2. dubna 2012

Abstrakt

Bezprostředním cílem předkládaného projektu je zkvalitnění a rozšíření systémů pro detekci a prevenci průniků v síti WEBnet, která je součástí sítě CESNET2.

Při dnešních rozměrech Internetu, je udržení sítě bez jediného napadeného počítače nemožné. Z obranných, studijních a výzkumných důvodů se tedy využívá různých typů IDS¹. V souvislosti se zaváděním protokolu IPv6 se objevují nové možnosti útoků na síť s podporou tohoto protokolu.

Hlavním cílem navrhovaného projektu je průzkum dostupných IDS s podporou IPv6, jejich nasazení v síti WEBnet (cca 1-2 produkční systémy) a publikování doporučených nastavení pro ostatní členy sdružení CESNET.

1 Současné IDS v síti WEBnet

V současnosti je v síti WEBnet provozováno několik IDS systémů, které byly vybudovány v rámci grantů FR Cesnet [2, 3]. Jejich provoz významně přispívá k zabezpečení sítě WEBnet i CESNET2.

Žádný z nich však nepodporuje protokol IPv6. Vzhledem k celosvětovému úsilí spojenému se zaváděním protokolu IPv6 vznikají nové vektory útoků pro napadání výpočetních prostředí. Provoz IDS systémů je jedním ze způsobů používaných pro dosažení vyšší bezpečnosti i dostupnosti poskytovaných služeb. V prostředí univerzitních počítačových sítí, s nekončícím koloběhem studentů a jejich rozličných síťových zařízení, je provoz IDS nezbytností.

V síti WEBnet existují pouze 2 vysoce experimentální studentské projekty [4, 5] – implementace Labrea/Tarpit pro IPv6, avšak bez pravidelného vyhodnocování a monitoringu.

¹Intrusion Detection System

2 Cíle projektu

Cílem předkládaného projektu je rozšíření aktuálně provozovaných IDS o systémy s podporou IPv6. Dále jejich zapojení do infrastruktury organizace, vytvoření a publikace reportovacích nástrojů a metodik vytvořených v rámci projektu. Cílem této části je získání znalostí o skutečném charakteru útoků v sítích s podporou IPv6 a shodě či naopak rozdílech od útoků v sítích IPv4.

Dále je cílem výměna získaných informací s ostatními členy sdružení.

Protože je provozování a vyhodnocování dat IDS činnost náročná na praktické ale i teoretické znalosti, chtěli bychom v rámci tohoto projektu zvýšit vzdělání bezpečnostního týmu účastí na konferenci s vhodnou tematikou.

3 Způsob řešení

3.1 Instalace a provoz IDS s podporou IPv6

Rozšíření IDS v síti WEBnet bychom chtěli provést instalací několika IDS systémů nebo úpravou stávajících projektů tak, aby dokázaly odhalovat útoky v síti IPv6. Instalace všech testovacích prostředí bychom chtěli provozovat na virtualizačním serveru typu Xen pořízeném z prostředků grantu. V rámci řešeného projektu bychom chtěli vyzkoušet následující systémy, z nichž 1 nebo 2 vybrané provozovat v produkčním nasazení i po skončení projektu.

Kippo Kippo je honeypot s vysokou interakcí vytvořený pro logování brute-force útoků na službu SSH. Po uhodnutí definovaného hesla poskytne útočníkovi virtuální prostředí emulující napadený systém (prostředí linuxového shellu).

Dionaea Dionaea je honeypot s nízkou interakcí s primární funkcí emulovat službu SMB (tcp/445) používanou v systémech MS Windows. Dionaea obsahuje i implementaci dalších služeb HTTP(S), FTP, TFTP, MSSQL, MySQL a SIP.

Web honeypot WWW je v současnosti nejrozšířenější aplikační platformou napříč celým Internetem. Webové služby budou jedny z prvních, které budou reálně podporovat (nebo již podporují) protokol IPv6.

LaBrea Tarpit honeypot pracující na síťové a transportní vrstvě. Využívá vlastností TCP protokolu k detekci a pozdržení útoků[1].

FTAS FTAS je systém pro monitoring vysokorychlostních sítí vyvíjený sdružením CES-NET. Z jeho záznamů je možné získávat informace o anomáliích v síťových tocích. Vhodné využití těchto informací by bylo užitečné a automaticky dostupné pro všechny členské sítě.

Informace získávané z provozu výše uvedených systémů bychom chtěli využít v rutinním provozu sítě při řešení bezpečnostních incidentů podobně jako v případě projektu *Rozvoj systémů pro detekci průniků v síti WEBnet*[2] – vypracováním monitorovacích nástrojů a jejich začleněním do procesu řešení bezpečnostních incidentů v síti WEBnet/CESNET2.

3.2 Zvýšení odbornosti

Předpokládáme, že ke správnému návrhu finálního řešení a jeho implementaci budeme potřebovat zvýšit odborné znalosti z oblasti počítačových sítí a metodik jejich zabezpečování. Toho bychom chtěli dosáhnout účastí obou řešitelů na vhodné konferenci, zahraniční stáží nebo absolvováním školení s vhodnou tematikou (např. Chaos Communication Congress, sans.org, CCNP, ...). Dále nákupem a studiem literatury.

3.3 Prostředky na implementaci

Na vypracování navrženého řešení předpokládáme potřebné prostředky dle následující tabulky. Vyčíslení finančních nákladů je provedeno v kapitole 7.

Členění prací	Rozsah [člověkodny]
Analýza dostupných řešení a návrh implementace v síti	7
Vývoj podpory IPv6 protokolu do vybraných IDS	14
Instalace jednotlivých IDS	7
Vývoj reportovacích a monitorovacích nástrojů	14
Analýza získaných informací	14
Celkem	56

4 Využití a prezentace výsledků

Projekt má rozvojově vzdělávací charakter a jeho splnění by přispělo ke zvýšení bezpečnosti sítě WEBnet a tím i sítě CESNET2. Informace získávané z provozu těchto systémů bychom chtěli využít v rutinním provozu při řešení bezpečnostních incidentů, tedy z vypracovaných nástrojů získávat aktuální informace o probíhajících útocích a ty pak následně řešit dle standardních postupů pro řešení bezpečnostních incidentů.

Získané výsledky, metodiky a nástroje bychom chtěli prezentovat formou závěrečné zprávy, přednáškou na semináři řešitelů nebo některém z odborných seminářů nebo na setkání vybraných pracovních skupin. Výsledky projektu tak budou dostupné všem členům sdružení.

Dále pak aktivním sdílením informací s bezpečnostními týmy CESNET-CERTS, CSIRT-MU a Metacentrum a pracovními skupinami CESNETu pro IPv6 a CESNET-CERTS.

Návrh projektu byl projednán s vedoucím *Oddělení podpůrných služeb a CSIRTu*, který s jeho obsahem a cíli souhlasí a vidí je jako přínosné.

5 Charakteristika řešitelského týmu

- Ing. Radoslav Bodó (hlavní řešitel) – je absolventem Fakulty aplikovaných věd Západočeské univerzity v Plzni v oboru Distribuované systémy. Od roku 2003 pracoval jako externí pracovník v Laboratoři počítačových systémů, Centra informatizace výpočetní techniky, kde se podílel na vývoji distribuovaného výpočetního prostředí Orion; zejména v oblasti vývoje pod operačním systémem Linux. Od roku 2005 pracuje v tomto útvaru interně jako správce operačního systému Linux a člen bezpečnostní skupiny WEBnet Incident Response Team.
- Ing. Michal Kostěnek (spoluřešitel) – je absolventem Fakulty aplikovaných věd Západočeské univerzity v Plzni v oboru Distribuované systémy a počítačové sítě. Od roku 2006 pracoval jako externí pracovník v Laboratoři počítačových systémů, Centra informatizace výpočetní techniky, kde vyvíjel síťově orientované nástroje. Od roku 2009 pracuje v tomto útvaru jako správce metropolitní sítě WEBnet a je lektorem regionální Cisco Networking akademie.

6 Navrhovaná doba trvání projektu

Navrhovaná doba trvání projektu je 12 měsíců.

7 Finanční rozvaha

Náklady potřebné pro navržené řešení jsou vyčísleny v tabulce níže a činí celkem 333 824,- Kč. Z toho navrhujeme příspěvek fondu rozvoje ve výši 205 000,- Kč a spoluúčast nositele projektu 128 824,- Kč (tj. 39%). Cena za člověkodenní (pro vyčíslení mezd) byla stanovena na 2 500,- Kč.

Položka	Cena	Plátce	Cena ZČU	Cena Cesnet	Kategorie Cesnet
Xen server	75000	ZČU	75000		dl.hm.m.
Režie	38824	ZČU	38824		ostatní služby
Stravné	15000	ZČU	15000		cestovné
Literatura	5000	Cesnet		5000	knihy, uč. Pomůcky
Doprava	10000	Cesnet		10000	cestovné
Ubytování	10000	Cesnet		10000	cestovné
Vložené na konference	40000	Cesnet		40000	ostatní služby
Náklady na mzdy pracovníků	104487	Cesnet		104487	mzdy
Sociální a zdrav. poj.	35522	Cesnet		35522	sociální a zdrav. poj.
Celkem [Kč]	333824		128824	205000	
Celkem [%]			39	61	

Náklady na cestovné byly odhadnuty dle loňských poplatků za konferenci Chaos Communication Camp 2011 a Black Hat Europe 2010 a náklady za dopravu a ubytování

byly stanoveny přibližně dle současných cen. Všechny položky jsou voleny s rezervou pro případný výběr jiné konference v Evropě.

Literatura a odkazy

- [1] Pavel Vachek: *CESNET Intrusion Detection System*
Technická zpráva CESNETu číslo 5/2006
<http://www.cesnet.cz/doc/techzpravy/2006/ids/>
- [2] Radoslav Bodó, Aleš Padrta: Rozvoj systémů pro detekci průniků v síti WEBnet
Závěrečná zpráva FR CESNET projektu 230R2/2007
<http://fondrozvoje.cesnet.cz/projekt.aspx?ID=230>
- [3] Radoslav Bodó, Michal Kostěnek: Zkvalitnění procesu řešení bezpečnostních incidentů v síti WEBnet
Závěrečná zpráva FR CESNET projektu 369/2010
<http://fondrozvoje.cesnet.cz/projekt.aspx?ID=369>
- [4] Antonín Slezáček: IDS systém typu Tarpit pro IPv6
BP ZČU Plzeň 2010
<https://portal.zcu.cz/stag?urlid=prohlizeni-prace-detail&praceIdno=37750>
- [5] Martin Čížek: IDS systém typu Tarpit pro IPv6
BP ZČU Plzeň 2011
<https://portal.zcu.cz/stag?urlid=prohlizeni-prace-detail&praceIdno=43627>