Příloha k protokolu o SZZ č.

Vysoká škola: JU Pedagogická fakulta

Katedra: informatiky

Datum odevzdání posudku: 27.5.2009

Diplomant: Jakub MAURIC

Aprobace: VTI

Vedoucí bakalářské práce:

Ing. Ladislav Beránek, CSc.

POSUDEK BAKALÁŘSKÉ PRÁCE

IDS systém SNORT

(téma)

Předložená práce se zabývá systémy IDS (detekce průniků). Práce se skládá ze šesti kapitol, její struktura jde od vysvětlení pojmu IDS, teoretický základ IDS vč. chyb typu false-positive a false-negative, přes popis několika vybraných systémů IDS a zvláště systému SNORT spolu s analytickými nástroji pro interpretaci vytvořených logů. Dále se věnuje implementaci systému SNORT a vybraných analytických nástrojů a v závěru se dotýká zhodnocení implementace a dalším výhledům. Na začátku práce je uveden též malý slovníček zkratek, což je pro tuto práci, kde se těchto zkratek objevuje poměrně dost, velmi vítané. Struktura práce je celkově zvolena velmi vhodně.

První kapitola je obecným úvodem, kde autor rozebírá možnosti zabezpečení počítače v internetu. Druhá kapitola je obsažnější a zabývá se systémy IDS, jejich efektivitou a rozdělením. Zdá se, že citace z práce Davida Šumského, obsažené v kapitolách 2.2, 2.4.1 a 2.4.2 jsou jednak poměrně rozsáhlé a jednak zřejmě doslovné. Je sice pravdou, že se jedná o teoretické základy IDS, avšak přesto je mohl autor zpracovat dle citované práce samostatně. Celkově je dobře provedeno rozdělení na NIDS, HIDS a DIDS, kde u DIDS by mohl být na přiloženém obrázku (s. 17) označena i možnost nasazení HIDS na mailovém serveru a jeho zapojení do DIDS.

Třetí kapitola se zabývá přehledem používaných systémů IDS. Domnívám se, že výstižnější název by byl "Výběr ze systémů IDS", neboť zde jistě nejsou uvedeny všechny systémy a zřejmě by to ani nebylo možné. Snad by zde mohl být zmíněn systém Tripwire, kdysi volně šiřitelný a dnes komerční, který byl jedním z prvních systémů HIDS, příp. na něj volně navazující systém AIDE, který je šířen pod licencí GPL. Nicméně je zde zmíněn vždy zástupce z každé kategorie (NIDS, HIDS i HIMS), což je přínosné.

Ve čtvrté kapitole začíná popis systému SNORT. Jsou zde zmíněny HW i SW požadavky na běh systému, popsána jeho architektura, řeší se případná úskalí nasazení a jsou zde zmíněny i požadavky na bezpečnost samotného systému s instalací SNORT-u. Dále se zde autor věnuje pravidlům, nad kterými SNORT pracuje a také je zde popis vygenerované výstrahy tímto systémem. Dále se autor věnuje systémům hodnocení výstrah vygenerovaných systémem SNORT a popisuje systémy BASE, SGUIL a IDScenter.

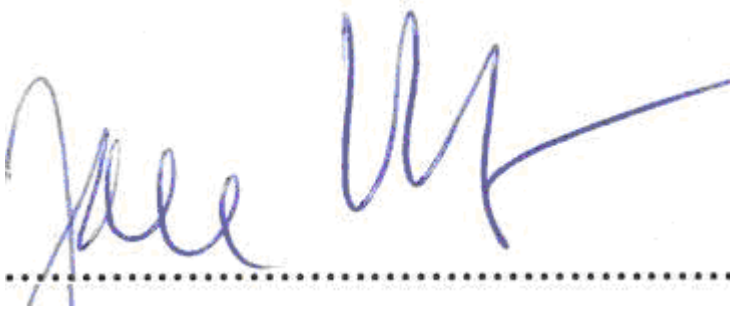
V páté kapitole autor uvádí do struktury sítě, ve které byl instalován IDS systém SNORT a dále také očekávání, které jsou do nasazení systému SNORT vkládána. Zabývá se též konkrétním HW, na kterém SNORT

poběží a vhodně určuje místa nasazení. Dále velmi podrobně popisuje instalaci hostitelského systému, který je tvořen linuxovou distribucí Ubuntu.Instalace je zde probrána krok za krokem, což je velmi instruktivní. Z pohledu člověka, který používá linuxové systémy denně již více než 10 let bych snad doporučil v každém případě použití žurnálovacího systému ext3, neboť jeho režie je minimální a start s jeho použitím je jistě rychlejší (s. 38), dále se zde objevilo několik nepřesností (spíše překlepů): na s. 40 autor jistě místo OpenSSL mínil OpenSSH, na s. 41 nahoře to vypadá, že v příkazu apt-get je mezera, naproti tomu mezera chybí v uvedeném příkazu cd /usr/local/src. Na s. 50 je chyba v názvu souboru, má zde být /etc/resol**v**.conf. Přesto se jedná pouze o překlepy, které nejsou příliš důležité a takto popisný postup vítám. Současně je i dobré, že se autor rozhodl zkompilovat SNORT ze zdrojových kódů, většinou tato akce přináší výhody v nejnovější bezpečnostní aktualizaci, nevýhodou takového postupu je ovšem nutnost hlídat následné bezpečnostní aktualizace a pokaždé provést rekompilaci aplikace. Na konci této kapitoly autor popisuje problémy se systémem Barnyard, které se nakonec staly důvodem jeho vyřazení z komplexního řetězce systému SNORT a systému pro analýzu logů.

V šesté kapitole se autor věnuje zhodnocení nasazení systému SNORT v dané konkrétní síti a také interpretací zjištěných výsledků a přijatým bezpečnostním opatřením. Hodnocení je provedeno kvalifikovaně a bezpečnostní opatření jsou jak přiměřená, tak účinná.

Předložená práce se daným tématem zabývá poměrně podrobně, autor prokazuje zkušenost s instalací i konfigurací systému a také vhodně hodnotí výstupy tímto systémem získané. Mnou navrhované hodnocení: **výborně**.

Návrh na klasifikaci bakalářské práce: výborně



Podpis recenzenta bakalářské práce

V Č. Budějovicích dne 27.5.2009

Stupeň klasifikace	výborně	velmi dobře	dobře	nevyhověl