Posudek oponenta bakalářské práce

Autor/autorka práce: **Martin Beránek**

Název práce: **Pokročilé zabezpečení heterogenní IT infrastruktury pomocí Log IDS**

Obsah práce

Práce popisuje možnosti pokročilého zabezpečení IT infrastruktury pomocí logových výstupů systémů a IDS sond. Této problematice se věnuje kapitola 2. Tato kapitola je napsána velmi povrchním a nepřesným způsobem. Jednotlivé podkapitoly na stejné úrovni v kapitole 2.1 popisují zcela odlišné způsoby dělení bezpečnostních hrozeb, navíc nejsou ničím uvedeny a působí vytrženě z kontextu. Je na zvážení zda *vybombardování datového skladu* je opravdu problematika patřící do této kapitoly.

Následuje výčet nejběžnějších síťových útoků či problémů. S uvedeným výběrem se bohužel nedá zcela souhlasit, neboť mezi dva nejběžnější problémy v dnešních firemních sítích patří hádání hesel a šíření spamu či obecně zneužívání zdrojů. Ani jedna z těchto problematik není ani zmíněna. Student zmiňuje, že po síťových útocích zůstává v síti patrný otisk, ale již u jednotlivých typů útoků nepíše o jaký otisk se jedná a ani kde jej hledat. Ke kapitole analýza logů nemám výhrad.

Následuje kapitola 2.5 OSSEC, která není žádným textem uvedena a čtenáři není příliš jasný význam jejího zařazení. V kapitole 2.5.2 je uveden seznam zařízení, se kterými umí systém OSSEC pracovat pomocí vzdáleného logování. S tím se nedá souhlasit, neboť pokud jsou logy předávány normalizovaným protokolem syslog, je možné napojit jakýkoliv systém, který tento protokol podporuje. V kapitole 2.5.4 jsou popsány další podobné systémy, které mi ale přijdou svým zaměřením rozdílné, neboť SNORT neslouží jako agregátor logu a syslog-ng zcela jistě není IDS. V tabulkách v kapitole 2.5.5 student provedl pokus o srovnání systémů, bohužel z těchto tabulek i díky rozdělení na dvě části, není zcela patrný výsledek srovnání.

V kapitole 3. Nastavení OSSEC student popisuje instalaci konfiguraci OSSEC, zde je v posledním odstavci uveden postup SMS notifikace, který je v chybném formátu číslo@sms.o2.cz, který nefunguje.

Následuje kapitola 3.3 Regulární výrazy, jejichž význam nechápu, neboť kromě informace, že se nejedná o původní text, ale překlad neobsahuje žádný další text. Kapitoly 3.4.3 a 3.4.4 jsou obsahově v pořádku, ale logicky nezapadají pod kapitolu 3.4 Použité výrazy. Následuje popis instalace agentů a WWW rozhraní. U instalace WWW rozhraní se předpokládá funkční server Apache, ale není zde popis ani odkaz jak tohoto stavu dosáhnout. Připojené screenshoty čtyř obrazovek jsou bez bližšího vysvětlení.

V kapitole 4 jsou přehledně popsány možnosti tvorby dekodérů a pravidel reakcí na jednotlivé události. Tato kapitola je nejlepší z celé práce.

Kapitola 5. Podpora OSSEC popisu detailně dostupnou podporu OSSEC a myslím, že její rozsah je zbytečně rozsáhlý.

V kapitole 6. je pokus o popis modelového prostředí a provedení testů nad tímto modelem. Bohužel tato kapitola je velmi strohá a nepřesná. V první řadě student vybral pro modelové prostředí 3 různé linuxové distribuce a tři varianty Microsoft Windows. Na základě čeho byl tento výběr proveden není nikde uvedeno. Stejně tak není uvedeno, jaké služby jsou na jednotlivých strojích provozovány, což je

pro následné testování zcela zásadní. V neposlední řadě je v názvu práce uvedeno, že se jedná o bezpečnost IT infrastruktury, tedy nepochybně by model měl brát v potaz síťovou infrastrukturu, jako routery, switche, WiFi či firewally. Tyto síťové prvky nejsou v práci vůbec řešeny, přesto že bezpečnost ovlivňují zcela zásadním způsobem. Po nástinu testovaného modelu je v bodech představeno sedm vybraných testů, pomocí kterých chce student funkčnost OSSEC otestovat. Výběr těchto testů není nijak zdůvodněn a navíc nekoresponduje s kapitolou 2.1., kde student popisuje jednotlivé bezpečnostní incidenty. Průběh testů i hodnocení jejich výsledků je uvedeno jen ve velmi skromných nástinech. Na konci kapitoly jsou výsledky testů shrnuty do dvou tabulek. Jelikož se v případě OSSEC jedná o systém na sběr, analýzu a agregaci logů, nejsem si jist, zda správně chápu jednotlivé tabulky. Výsledky v tabulkách působí pouze jako testování IDS sondy.

V závěru práce student shrnuje svoji práci a dosažené výsledky. Bohužel stejně jako celá práce působí i závěr rozporuplně. V druhém odstavci je uvedeno, že OSSEC se ukázal jako velmi vhodný nástroj pro agregaci logů. Ale na konci třetího odstavce je uvedeno, že student nasazení OSSEC nedoporučuje tam, kde se jedná o kritické nasazení, ale jen jako doplňkovou funkcionalitu. Což je v rozporu s předchozím odstavcem, kde je tento systém doporučen.

Kvalita řešení a dosažených výsledků

Z bezpečnostního pohledu bohužel nemá praktická část práce významnou vypovídající hodnotu. Není zdůvodněn návrh prostředí ani návrh jednotlivých testů. V obou případech nebyla volba provedena zcela správně. V rámci praktické části je přínosem jen část popisující instalaci OSSEC a jeho nastavení.

Formální úroveň

Dokument je plný nepřesností a informací, které nejsou vhodně uvedené v textu či jsou vytržené z kontextu, což práci činní pro čtenáře nepřehlednou. Jednotlivé kapitoly na sebe logicky nenavazují, jako je tomu například v kapitolách 3.3 a 3.4. Obsah kapitol jako je 3.3 či 5 dokumentu příliš informací nepřidává. Některé poznámky pod čarou, jako odrážka 4. na stránce 18 patrně do aktuálního textu nepatří.

Práce s literaturou

Práce obsahuje 14 odkazů na externí zdroje, kde se v 12 případech jedná o odkaz na webové stránky, což je škoda, neboť o bezpečnosti existuje velké množství kvalitních textů, na které by se mohl autor odkázat. Neobvyklé je i řazení zdrojů, kde prvním citovaným je desátý odkaz. Například odkaz na první bod z literatury jsem v textu použitý nenašel.

Splnění zadání

Vzhledem k tomu, že v práci je velké množství nepřesností je rozhodnutí o splnění zadání u některých bodů problematické. Speciálně bod tři, tedy návrh modelového prostředí ve středně velké firmě je splněn velmi povrchně. V úplně základním rozsahu však jednotlivé body v rámi práce zmíněné jsou.

Dotazy k práci

1. Nebylo by vhodné minimálně hádání hesel a případně odesílání spamů uvést jako jedno z problematických chování v počítačových sítích středně velkých

firem?

2. Jak jste stanovil obsah běžného prostředí ve středně velké firmě ?
3. Proč je v práci zcela ignorována bezpečnost síťových zařízení jakou jsou routery, switche či WiFi, přestože právě ony tvoří významnou část infrastruktury?
4. Proč nejsou u jednotlivých testovaných systémů uváděny žádné služby, ty dle vás bezpečnost testovaných systémů neovlivňují ?

Celá práce není provedena příliš pečlivě, obsahuje velké množství nepřesností a v některých bodech otázky spíše vyvolává než zodpovídá. Po důkladném prostudování práce a předvedení praktické části studentem mohu říci, že alespoň v základním rozsahu se student věnuje všem bodům zadání. S přihlédnutím k faktu, že student systém OSSEC a velmi strohé testovací prostředí zprovoznil, práci po delším váhání **doporučuji k obhajobě** a hodnotím známkou **dobře**.

V Plzni 22.5.2015

Ing. Luboš Matějka