UNIVERZITA HRADEC KRÁLOVÉ
FAKULTA INFORMATIKY A MANAGEMENTU

Katedra informačních technologií
Obor: informační management

Forenzní analýza digitálních dat

SEMESTRÁLNÍ PRÁCE

Autor: Bc. Josef Kadlec
Obor: IM2-K (1. ročník)
Předmět: OBDAI
Vyučující: Ing. Miloslav Feltl

Rok 2004

Prohlášení

Prohlašuji, že jsem tuto semestrální práci vypracoval samostatně a uvedl jsem veškerou použitou literaturu.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským.

V Hradci Králové dne 25. října 2004 Josef Kadlec

Poděkování

Tímto bych chtěl poděkovat mé přítelkyni ”woodsboro”, která mi dodává potřebnou motivaci a doufám, že v tom bude pokračovat i nadále.

Anotace

Seminární práce je jakýmsi úvodem do problematiky forenzní analýzy digitálních dat. Postupně se seznámíme s tím, co tento obor všechno obnáší. Projdeme problémy od samotné přípravy na incident, přes vyšetřování až ke konečné obnově. Vše je probíráno v obecné rovině, nezávisle na použité platformě a na použitých investigativních prostředcích.

Obsah

Kapitola 1

Úvod

"Lidi vymejšlej bejkárny, prostě takhle to je a bude."

MJR. ING. JIŘÍ DASTYCH

V dnešní době se již digitálním zařízením prakticky nevyhneme. Tato zařízení, ať už jsou v podobě osobních počítačů, PDA zařízení, mobilních telefonů, USB flash disků a mnoho dalších, jsou tak dostupná, že se rychle zařadily mezi běžné součásti našeho každodenního života a staly se našimi nástroji denního používání. Lze předpokládat, že tato zařízení postupem času, původní zařízení, postupy a zvyky úplně nahradí.

Logicky vyvodíme, že tedy i tato zařízení se stávají terčem útoků a také samozřejmě nástrojem zločinu - takový zločin je pak nazýván cybercrime[1]. Proto bylo potřeba vytvořit vědu (nebo metody), která toto prostředí digitálních dat bude zkoumat.

Když se stane vražda nebo vloupaní, budou lidé zainteresováni v takovém případu (zřejmě policie nebo jiné oprávněné složky) zkoumat a ohledávat místo činu za účelem rekonstrukce dané události, nalezení viníků a sběru důkazů. Prostředkem tohoto sběru informací bude například fotografování místa činu, snímání otisků prstů, sběr genetického i jiného materiálu a shromažďování důkazů.

Obecně lze říci, že tato rekonstrukce probíhá obdobně v případech, kde je potřeba zkoumat počítače a jiná digitální zařízení či pouze data. A to je přesně práce pro forenzní analýzu digitálních dat. Samozřejmě, že mezi

[1] Více o pojmu cybercrime v následující části.

těmito dvěma oblastmi jsou rozdíly. Digitální data jsou velmi náchylná ke změně - tzn. že jsou velmi nestálá. Tomu pak musí být přizpůsobeno nakládání s těmito daty, ať už se jedná o samotný sběr, uchovávání nebo transport. Takový sběr důkazů může být velmi časově náročný a to především v závislosti na množství zkoumaných dat. Ovšem zase rekonstrukce události (či událostí) není zpravidla náročná na fyzický prostor, takže lze takovou rekonstrukci provést například přímo v soudní síni.

Příklad z praxe - nedávný případ zabavení počítačů člověka, který si přezdívá Benny a to za podezření na tvorbě červa SQLSlammer[2], který napáchal před 2 lety vysoké škody. Lze předpokládat, že tyto počítače (počítač) jsou nyní zkoumány za účelem sběru důkazů.

Ještě nepříliš dostatečná obecná obeznámenost v oblasti forenzní analýzy digitálních dat a nebo vůbec obeznámenost ve znalostech digitálních zařízení, počítačových systému a dalších, dělá tuto oblast velmi problémovou a proto je potřeba ji dále podrobně zkoumat.

Cybercrime

Obecné povědomí je takové, že pod pojmem cybercrime se skrývají zločiny, které se odehrávají ve virtuálním prostoru počítačů a počítačových sítí (tzv. "cyberspace"). Ale pojem cybercrime zahrnuje více než tento prostor. Výzkum digitálních dat je často potřeba v případech, ve kterých by to asi málo kdo čekal. Když například policie ohledává byt, ve kterém pobýval drogový dealer, a ve kterém se našel kontraband, měl by policii zajímat i počítač, který v této situaci může vypadat relativně nevinně. Stal se případ, kdy v takovém počítači byly nalezeny kompletní informace o zákaznících, dodávkách a další pro případ prospěšní informace. Takže vidíme, že počítač nebo jiná zařízení s obsahem digitálních dat nemusejí být v roli oběti a také nemusí mít nic společného se zločiny páchanými na takovýchto zařízeních nebo na dosahování vyšších cílů skrze tato zařízení.

Abychom celou problematiku zločinného dění v digitálním světe zjednodušili a mohli jí lépe porozumět a hlavně vysvětlit, budeme brát počítač jako objekt, na kterém dochází k incidentům, které se vymykají normálnímu stavu - většinou k incidentům bezpečnostním. Samotná forenzní analýza je jen část celku. Celá metodologie reakce na incident je složená z

[2] http://www.viry.cz/zobraz.php?id=2390&s=rss

více kroků, které jsou v různých zdrojích definovány odlišně, ale základní podstata by měla být stejná. Dále také záleží na tom, jestli daná organizace má vytvořenou metodologii, kterou bude postupovat při detekování takového incidentu. Pokud ano, tak bude zřejmě zařazena v bezpečnostní politice dané organizace. Na druhou stranu je potřeba vyšetřovat případy, kdy žádná příprava na incident nepředcházela, detekce problému byla zcela náhodná nebo byl problém tak nápadný, že nebylo pochyb, že k incidentu došlo. Pak může být situace rekonstrukce incidentu, sběru důkazů, hledání zodpovědných lidí a dalších kroků samozřejmě o to obtížnější.

Kapitola 2

Forenzní analýza digitálních dat

Forenzní analýza digitálních dat (angl. digital forensics) je relativně mladá věda. Někde se říká, že to není ani tak věda, jako spíše umění. Tato věda a její název vlastně vznikly z původního výrazu forenzní analýza počítačů a počítačových systémů (angl. computer forensics), která zkoumala pouze počítače. Forenzní analýza digitálních dat se zabývá digitálními technologiemi ve všech podobách - kromě počítačů například mobilní telefony, mobilní sítě, datová média a mnoho dalších.

Zatímco forenzní analýza počítačů a počítačových systémů je definována jako souhrn technik a nástrojů k hledání důkazů na počítači [2], tak forenzní analýza digitálních dat je definována jako užití vědecky odvozených a osvědčených metod k izolování (ochraně), sběru, zhodnocení, identifikaci, analýze, interpretaci, dokumentaci a prezentaci digitálních důkazů ze zdrojů digitálních dat s cílem usnadnění rekonstrukce událostí shledaných zločinnými nebo k odhalení neautorizovaných akcí, které působí rušivě na plánovaný běh operací [3].

Takových definic je samozřejmě více, ale v zásadě se neliší. Pokud bychom to řekli laicky, tak tato věda analyzuje jakákoliv digitální data s cílem určit, co se stalo, kdy se to stalo, jak se to stalo a koho se to týká. Metodologicky je to podobné, jako když se vyšetřuje jiný incident ve fyzické světě - například vražda nebo loupež. Složky zkoumající tyto incidenty také bude zajímat co se stalo, kdy se to stalo, atd. Ve světe digitálních dat jsou tyto informace často skryty v podobě smazaných souborů, fragmentů dat uložených v alokované paměti existujících souborů (tzv. slack space), dat uložených v dočasné paměti RAM nebo v podobě záznamů (tzv. logů) činnosti jednotlivých služeb, které na daném zařízení běží. Proto jsou potřeba k získání těchto informací a důkazů speciální

nástroje, znalosti a zkušenosti. Stejně jako když v rámci nějakého případu bude nalezena kulka ze střelné zbraně a bude potřeba ji identifikovat. Tuto práci nemůže udělat jakýkoliv člen zainteresovaný v takovém případu, ale pouze odborník na balistiku.

Uvádějí se i další podskupiny pro forenzní analýzu digitálních dat, jako například síťová forenzní analýza, která se zabývá výhradně vyšetřováním v oblasti počítačových sítí nebo forenzní analýza mobilního telefonního systému GSM nebo forenzní analýza notebooků a laptopů. Když půjdu ještě do nižšího levelu, tak můžeme rozlišovat forenzní analýzu jednotlivých operačních systémů.

Nyní si povíme blíže, co hlavní body definice forenzní analýzy digitálních dat znamenají. Izolování a ochrana důkazů znamená to, že pro následující sběr a analýzu digitálních dat je potřeba zachovat jejich původní sterilitu, takže musíme zabránit jejich pozměnění či ztrátě. V praxi se to většinou provádí tzv. forenzní duplikací zkoumaného digitálního média. Zkoumání pak probíhá na této kopii. Pokud nemůžeme provést forenzní duplikaci, lze např. nastavit dané médium tak, aby bylo jen ke čtení a nebyl na něj umožněn zápis, pokud je to tedy možné.

Sběr důkazů znamená to, že tyto důkazy musíme z původního pracovního média vyextrahovat na jiné médium a nebo do formy vhodné pro tisk.

Identifikace důkazů znamená v počáteční fázi identifikaci samotných relevantních médií, na kterých by se mohly důležité informace nacházet. Podstatou je to, že samotné médium (pevný disk, USB flash disk, atd.) není samo o sobě důkazem, ale pouze zdrojem takových důkazů. Ve fázi analýzy má identifikace důkazů, co do činění s identifikací jednotlivých dat a informací.

Interpretace informací, případně důkazů může být klíčová. Díky dostupnosti různých skriptů a GUI utilit pro extrahování takových informací, mohou být informace získány prakticky kýmkoliv. Ale důkladně správně je vyložit, je věc druhá.

Další velmi podstatnou částí je dokumentace ve smyslu zaznamenávání všeho co děláme. A to opravdu všeho od začátku až do konce. Například kvůli tomu, že jako vyšetřovatelé budete moci být u soudu dotazováni a to i na podrobnosti. A už z principu musí být jasné, jaké všechny kroky jste podnikli.

Zjištěné skutečnosti je potřeba v nějaké formě prezentovat. Těžko budete vrcholovému managementu sdělovat zjištěné skutečnosti například výpisem logů aplikací nebo na takové odborné úrovni, že tomu management prostě nebude rozumět. Takže je potřeba prezentovat podstatné skutečnosti a závěry, pokud možno bez technických detailů, které jsou v konečném důsledku zbytečné. Managementu sdělte prostě například kdo je odpovědný, co bylo odcizeno, jaké jsou následky a škody, apod.

Jak jsem již zmínil na začátku, zkoumaný počítač může působit v roli nástroje zločinu a nebo může vystupovat v roli oběti - tzn. v pozici, kdy je takový počítač nebo jiné zařízení terčem zločinu (například byla-li z takového počítače odcizena nějaká data, atd.). V takovém případě většinou uplatňujeme metody reakce na incidenty. V prvním případě, kdy je počítač nástrojem nějakého zneužívání nás jako výzkumníky, popř. vyšetřovatele nemůže překvapit, že zkoumané zařízení se nám do rukou dostane vypnuté nebo dostaneme prostě pouze média (disky, atd.) ke zkoumání. Takže nebudeme moci vytěžit informace z dočasné paměti RAM, běžící procesy, sledovat síťová spojení, apod. Takové informace jsou však velmi důležité a často klíčové, proto musí být metodologie reakce na incidenty (kterou využijeme v druhém případě, kdy je počítač v pozici oběti) postavena tak, aby byly tyto informace zachovány.

Samozřejmě, že tento výzkum digitálních dat a sběr důkazů se nedělá pouze v případech, kdy má případ skončit před soudem, ale například pouze pro odhalení zodpovědných lidí za danou událost (a případně jejich potrestání). Ovšem nikdy nemůžete vyloučit, že nějaký případ před soudem neskončí - například proti svému zaměstnanci.

Jistě vám již došlo, že odborníci na forenzní analýzu digitálních dat musejí mít široké znalosti jak hardwaru, tak softwaru (operačních systémů, atd.). Často se probírá to, kde všude se odborníci v tomto oboru uplatní. Za prvé je to určitě ve složkách hájících právo a příbuzných - např. policie, FBI, CIA a jiné investigativní agentury. Další možnost uplatnění takových znalostí je v soukromých agenturách zabývajících se informační bezpečností, popřípadě přímo forenzní analýzou. Dalšími sektory působnosti může být například poskytování konsultací v tomto oboru. Obecně lze říci, že lidé v tomto oboru forenzní analýzy digitálních dat jsou v současné době štědře ohodnocováni - a to ze všech odborníků na různé oblasti informační bezpečnosti asi nejvíce (berte tuto informaci samozřejmě s jistou mírou nadhledu).

Pokud vyšetřujeme nějaký takový incident, je potřeba se často nekoukat pouze na samotné digitální médium, protože informace a často klíčové informace a důkazy vztahující se k případu mohou být i jinde - např. v blízkosti počítače, ať už to jsou hesla napsaná na spodní straně klávesnice, výstup na monitoru či tiskárně a nebo v logách externích prvků sítě jako proxy servery a firewally. Součástí takového výzkumu jsou i výslechy lidí, kteří jsou s případem provázáni. Pokud nebudeme brát toto v úvahu, mohou nám utéct často klíčové informace.

Kapitola 3

Reakce na incidenty

Jak už jsem již zmínil, incident je událost, která mění plánovaný chod, funkce nebo význam systému, i když daný incident nemusí přímo narušovat chod takového systému. Pokud například dojde k průniku do nějakého systému, neznamená to výhradně narušení chodu, ale je jasné, že je to něco, co by se stát nemělo, co se vymyká běžnému užívání a tudíž je to incident.

3.1 Příprava na incident a jeho detekce

Je potřeba mít na paměti, že pokud chceme vůbec detekovat daný incident, je potřeba se na něj připravit. Jak jsem již řekl, incident nemusí narušovat chod systému nebo nějakých podřadnějších funkcí, takže může být zcela nenápadný - například když narušitel pronikne do nějakého systému, odcizí nějaká data, zajistí si sofistikovanými prostředky cestu do systému pro pozdější přístup a nepozorovaně odejde. Pokud nejste na takový incident připraveni, tak ho vůbec nezaznamenáte a pokud ho zaznamenáte, tak to bude zřejmě otázka náhody.

Nejlepší způsob, jak předejít bezpečnostnímu incidentu nejen v oblasti počítačových systémů, je vytvoření takových preventivních i jiných prostředků k jeho zamezení. Ale nikdo není dokonalý, proto ani technika, kterou používáme nemůže být dokonalá. Nelze tedy zaručit stoprocentní bezpečnost, takže je potřeba brát v potaz, že k nějakému bezpečnostnímu incidentu může dojít - a často dříve, či později dojde. Příprava na incident by vám měla zajistit efektivní reakci na tento incident - tzn. najít příčinu problému a zajistit návrat do běžného stavu s minimálními škodami.

To jak předejít bezpečnostnímu incidentu (tzn. vlastně ochrana sítě, systému, atd.) a samotné detekování incidentu má mezi sebou velmi silnou vazbu, z velké části se překrývají a využívají často stejných prostředků. Zatímco detekci incidentu zajímá především to, co se přesně stalo - jaké systémy byly napadeny, jaké informace odhaleny a následně i identifikace zdroje těchto "nekalých" činností (v konečném důsledku útočníka), tak ochranu systémů, sítí, atd. zajímá především samotná eliminace těchto incidentů ještě než k nim dojde, popř. jejich další rozšíření a k tomu může využít informací (a nástrojů), které jsou důležité pro detekci incidentů. Všimněme si, že se bavíme o komplexním případu, kdy zkoumáme počítač, který je v roli napadeného systému (či systémů), které jsou navíc součástí nějaké obecné organizace.

Nebudu se v této práci zabývat samotným sestavováním bezpečnostní politiky a vůbec ochranou počítačů, systémů nebo sítě, ale pouze činnostmi, které se přímo týkají reakce na incident. Příprava na takový incident vypadá v praxi tak, že jsou určitým způsobem zkonfigurovány všechny počítače, popř. komplexně celá síť. Na počítačích jsou například vytvořeny databáze s kontrolními součty všech souborů pro pozdější kontrolu integrity systému (tyto součty mohou být uchovávány centrálně, aby nemohlo dojít k jejich modifikaci na jednotlivých systémech). Dále například aktivování logů, které zase mohou být shromažďovány centrálně a nebo instalace HIDS (Host Intrusion Detection System). Konfigurace spočívá především v instalaci firewallů, proxy, IDS (Intrusion Detection System), IPS (Intrusion Protection System) a jiných monitorovacích nástrojů. S tím samozřejmě souvisí návrh takové topologie, která bude pro takový monitoring vhodná.

3.2 Počáteční reakce

Na samotný incident může organizace reagovat různými způsoby. A to například ignorováním incidentu, sběrem informací o původu útoku (nebo útočníka), zabráněním pokračování v tomto útoku, atd. To jaký postup zvolíte záleží na mnoha faktorech - v klasické firmě to bude především dopad incidentu na činnost organizace, popř. právní stránka věci a nebo také technické prostředky, které jsou k dispozici. Důvody firmy proč zvolit tu nebo tu reakci mohou být často různé a rozhodně nemusejí být podobné modelu, kdy dojde k odhalení, dopadení a potrestání útočníka

nebo člověka zodpovědného. Firmy mohou hájit například reputaci firmy a nepřejí si, aby se vůbec o nějakém bezpečnostním incidentu někdo dozvěděl. Netouží po takovéto popularitě a nejradši by, aby se vše v tichosti vyřešilo. Optimální je asi provést analýzu incidentu, nalézt jeho příčinu[1], technickými prostředky zabránit v dalším pokračování útoku a pokud je to možné, tak odhalit útočníka. A tohoto modelu se my budeme držet.

Rozhodnutí, které uděláte se liší případ od případu a záleží na okolnostech, které incident doprovází. Takže naše rozhodnutí by se měla lišit na základě toho, jak citlivé jsou informace, které chráníme, jaké ztráty či výpadky můžeme tolerovat, kdo je potencionálním útočníkem, zda o incidentu ví veřejnost, apod. Asi nebude v silách nás jako napadené organizace například hledat autora viru, který napadl naše počítače. Od toho jsou tu jiné investigativní složky, které zase provádí svojí forenzní analýzu.

Samotné akce v reakcích na incidenty, které se týkají technických i dalších aspektů, by měl řešit vyškolený personál, který vlastně tvoří takový tým reakce na incidenty. Takový tým má na starosti veškeré vyšetřování, vyřešení bezpečnostních incidentů, určení škod, sběr důkazů a další kroky ve forenzní analýze digitálních dat a věcí příbuzných jako například poskytovat managementu fundovaná doporučení týkající se incidentu.

Konzultace všech kroků reakce a i samotné přípravy na incident musí být konzultována s právníky, aby se organizace samotná nedostala do problémů se zákonem například pro narušování soukromí svých zaměstnanců. Ne všechny informace mohou být prohlíženy třeba i osobou pověřenou bezpečností. Někdy je potřeba mít pověření, povolení nebo soudní příkaz. Někdy musejí být informace monitorovány takovým způsobem, aby byla zachována podstata, proč je monitorujeme, ale také, aby bylo zachováno právo na soukromí - často to znamená, že k informacím nesmí mít přístup žádná osoba a monitorovací systém musí být navržen tak, aby toto neumožňoval. Může se jednat například o sledování síťového provozu.

Ještě jsem neřekl, že se samozřejmě musíme bránit a monitorovat provoz, který přichází z vnějšku organizace, tak provoz, který pochází z vnitřku organizace, ale to by mělo být samozřejmé ze samotné podstaty informační bezpečnosti.

[1] Často se využívá výraz "smoking gun" (v překladu "kouřící zbraň").

Jak jsem již zmínil, měly by být všechny kroky, jak se bude postupovat a to nejen po zaznamenání incidentu, ale i samotná příprava a vůbec chod celého systému (není myšleno jako operační systém, ale informační systém jako celek v dané organizaci), zaznamenány v bezpečnostní politice - resp. uživatelské politice. Dodržováním takové politiky bychom měli docílit vyšší bezpečnosti takové organizace a to nejen z pohledu informační bezpečnosti (nedostatky v oblasti informační bezpečnosti se samozřejmě promítají i do bezpečnosti organizace jako takové) a také bychom měli docílit metodologického a tudíž i systematického řešení incidentů - identifikování odpovědných osob, apod.

Pokud máte v takové politice hodně aspektů, tak je výhodné takovou politiku rozkategorizovat na menší části - jako například politika přístupu na Internet, politika přístupu k výpočetním prostředkům, politika uživatelských přístupů, atd. Mezi jednotlivé aspekty takové politiky může patřit například čas, kdy je povolen přístup na terminály, kdo má povolen vzdálený přístup, kdo může manipulovat s konty uživatelů, kdo má právo používat konto superuživatele, jestli bude povoleno ICQ, atd.

3.3 Vyšetřování

Nyní se vrhneme na samotné zkoumání a vyšetřování důkazního média. Jako toto důkazní médium budeme brát disk počítače. V prvním případě, když máme zkoumat takový počítač, měla by nás zajímat dočasná data - tzn. že počítač by měl zůstat po detekci incidentu ve fázi zapnuto! Vypnutím počítače tato data a tím pádem i potencionální důkazy ztratíme. Ovšem zase tato práce představuje práci na "živém" systému a my jakožto vyšetřovatelé můžeme některé potencionální důkazy nechtěně znehodnotit. Kromě toho, že bychom měli v této oblasti mít dostatečné znalosti, abychom nenapáchali velké škody, je potřeba také každý náš krok pečlivě dokumentovat. Mezi dočasná data patří například obsah vyrovnávací a operační paměti, informace o síťových spojeních, informace o běžících procesech, atd. Pokud tato data pro vyšetřování nepotřebujete (například nevyšetřujete případ, kdy je relevantním prvkem síť - útok skrze síť), tak takovou analýzu vůbec nedělejte. Jedná se o náročnější proces než je analýza duplikovaného systému a můžete si tím zbytečně zmařit další vyšetřování.

Forenzní duplikace zdrojového média

Pokud to podmínky umožňují, je výhodné a často pro pozdější analýzu důkazů nutné, vytvořit tzv. forenzní duplikaci zkoumaného média (přesněji zkoumaných dat na médiu). Samozřejmě zda-li tento krok podniknete záleží například na množství času, který pro vyšetřování máte a nebo jestli je možné vůbec technicky takovou duplikaci provést. Tento krok se dělá proto, abychom si neznehodnotili původní zdroj důkazů - například přepsáním přístupových časů souborů. Ne nadarmo se forenzní analýze počítačů a počítačových systémů říká "pitva systému". Možná by zde šlo použít i úzkou asociaci s chirurgem, který operuje živý organismus. Takový člověk je pod mnohem větším tlakem a může cokoliv beznávratně zkazit. Kdežto takový patolog už na chodu organismu (systému) nic nezkazí, fádně řečeno. K forenzní duplikaci se používá široké portfolium nástrojů od jednoduchých unixových programů až po těžkotonážní komerční programy, které samozřejmě umí více, než pouhé zkopírování obsahu disku.

Z hlediska forenzní analýzy digitálních dat rozlišujeme 3 typy dat a to data aktivní. To jsou soubory (samozřejmě i adresáře, ale adresáře jsou vlastně také soubory, které pouze odkazují na soubory obsažené, takže proto budu vše nazývat soubory), které jsou normálně uživatelem viditelné, takže je lze z disku i nejjednodušeji získat. Dalším typem jsou archivovaná data. To jsou soubory, které naleznete na digitálních médiích typu CD, DVD, disketa, ZIP pásky a další. A posledním typem dat, které se nejobtížněji získávají jsou latentní data, která představují například smazané soubory nebo soubory částečné přepsané. Získávání všech typů těchto dat je obecně časově i finančně náročné.

Je také nutné počítat s tím, že extrahované soubory mohou být nějakým způsobem zašifrované. Potom musí přijít na scénu kryptologové, kteří se mohou pokusit takové soubory rozšifrovat. Pokud jsou ovšem soubory zašifrovány tak, aby je nebyla možnost se současnými prostředky rozšifrovat (není k dispozici šifrovací klíč nebo jiné indicie), potom jsou důkazy z těchto dat vyšetřovatelům skryty. Takže takové šifrované souborové systémy, kterými se často šifrují celé oddíly disků, budou asi noční můrou vyšetřovatelů. Kdybych chtěl vyšetřovatelům prakticky úplně znemožnit průzkum mého počítače, tak bych zašifroval celý systém (samozřejmě tak, aby šel nadále normálně používat), což například na unixových systémech lze[2]. Vyšetřovatelé pak nemají k dispozici zhola nic. Toto se však týká

[2] http://www.root.cz/clanek/2344 - jsem osobně autorem článku

především tehdy, když je počítat nástrojem zločinu. Pokud organizace šifruje data, dělá to kvůli ochraně dat před narušiteli, takže není důvodu, proč by vyšetřovatelům šifrovací klíč neposkytli.

Samozřejmě vytvářet duplikáty několika terabajtových disků může být velmi časově náročné a organizace nemusí mít dostatek prostředků takovou analýzu udělat - a už vůbec vždy, když je detekován incident. Proto se někdy neduplikuje celý systém a provádí se pouze tzv. logická kopie, která spočívá ve zkopírování např. systémových i aplikačních logů. Je tedy nutné zvážit zda-li je kompletní duplikace disku vůbec nutná s ohledem na závažnost incidentu nebo na tom, jestli je pravděpodobné, že se budou důležité důkazy nalézat například v podobě vymazaných souborů.

Samotnou duplikaci systému lze v podstatě provést třemi způsoby - z pohledu hardwaru. A to že buď odpojíme zkoumaný disk, který se bude duplikovat a připojíme ho k našemu rozhraní našeho stroje. Asi nejuniverzálnější metoda, která se hodí ve většině případů. Druhou možností je, že připojíme disk, na který vytvoříme obraz, do zkoumaného počítače. A třetí možností je zkopírování dat ze zkoumaného počítače přes síť. Samozřejmě tato síť musí být uzavřená, abychom vyloučili přístup třetí osoby a tím i případné narušení dat. Ověření toho, zda-li kopírování proběhlo bez chyb provedeme kontrolou integrity původních a zkopírovaných dat[3].

Duplikaci dat nikdy neděláme pomocí zkoumaného systému. Pokud tedy připojíme disk, na který se bude kopírovat obraz do zkoumaného počítače nebo budeme vytvářet obraz disku přes síť, je nutné nabootovat vlastní operační systém například z CD nebo diskety. K dispozici jsou různé "live" systémy na bázi Linuxu a nebo i "live" systémy vytvořené přímo pro tyto účely. Programy, které přímo vytvářejí duplikát musí být schopny zkopírovat všechna data od začátku disku až po služební stopu. Musí se také vyrovnat s chybami čtení - tzn. když nějaký sektor nelze přečíst, je potřeba toto místo vyplnit sektorem stejné délky s předem určeným obsahem. A dále by tyto programy měly zajišťovat kontrolu integrity vytvořeného obrazu. Disk na který vytváříte obraz by měl mít stejné parametry jako zkoumaný disk, proto je potřeba si tyto údaje zjistit například z Biosu.

[3]Rozhodně k tomuto kroku nepoužívejte hashovací funkce, ve kterých byla nalezena kolize (http://www.root.cz/clanek/2368)! Prolomeny byly funkce MD4, MD5, SHA-0, RIPEMD, HAVAL-128.

K vyhledávání konkrétních důkazů se používají dva druhy analýz. První je analýza fyzická, která má za úkol najít například nějaký řetězec z obsahu disku - a to v rámci všech sektorů disku. Berete celý disk jako celek. Zatímco logická analýza spočívá už v analýze jednotlivých souborů. Fyzická analýza musí samozřejmě počítat z odhalováním dat z neobsazeného diskového prostoru nebo s již zmíněnými slack prostory, kde zapisovaná data nedosahují ani minimální velikosti bloku definovaného operačním systémem. Vidíte, že to má co do činění s typem souborového systému, proto se i metody extrahování dat z různých souborových systémů souborů liší a příslušné nástroje s nimi musí počítat.

Vyšetřování sítě

Samozřejmě v době, kdy hlavním přenosovým médiem je síť, musíme počítat s tím, že jsme touto cestou ohrožováni. Nevím, jaké procento útoků je prováděno skrze síť (Internet i jiné), ale procento je to jistě velmi významné - ať už se jedná například o viry, červy a nebo individuální útoky. Samozřejmě síť je také klíčovým prvkem šíření nelicencovaného software či dětské pornografie.

Odhad je takový, že lidí, kteří alespoň jednou použili Internet, je asi 300 miliónů [4]. Dále se odhaduje, že asi 5 procent z tohoto počtu lidí nemá úplně čisté úmysly. To znamená, že tu máme nějakých 15 milionů lidí, kteří se snaží nějakým způsobem narušit bezpečnost sítí, počítačů, apod. s různými cíli. Řekněme, že 10 procent z tohoto počtu je opravdu zkušených, talentovaných a znalých profesionálů, kteří své práci opravdu rozumí. Závěr je takový, že touto jednoduchou analýzou jsme došli k počtu asi 1,5 milionu potencionálních útočníků, které bychom měli brát vážně.

Pokud chceme vyšetřovat a shromažďovat důkazy z akcí, které se děly přes síť, je většinou potřeba sledovat síťový provoz a výsledky zaznamenávat do logů pro pozdější analýzu. Takové sledování má úzký vztah se samotnou detekcí na incident (a jemu předcházející reakcí na incident). K vyšetřování tohoto typu dat je potřeba mít dostatečné znalosti sítí - tzn. především protokolu TCP/IP, služeb a aplikací používaných skrze tento protokol a další.

Pro tyto potřeby se používají nástroje, které odchytávají síťový provoz (tzv. sniffery). Tyto sniffery jsou často součástí IDS, kde tvoří komplexnější

řešení pro sofistikovanější detekce průniků. Dalším typem nástrojů jsou aplikace, které dokáží rekonstruovat odchycené pakety (nebo fragmenty paketů) do původního stavu.

Cílem takového dozoru je tedy detekovat, zda-li došlo k incidentu, identifikovat ho a tím následné zabránit, aby napáchal škody. Samozřejmě lze touto cestou sbírat důkazy a identifikovat narušitele. Tento monitoring může být např. použit i jako doplňující prostředek k potvrzení, či rozptýlení o nežádoucí činnosti - například na určité zaměstnance či jiné účastníky sítě.

Síťové důkazy jsou informace zjištěné o daných skutečnostech v dané síti či na určitém počítači, ale tyto informace se nemusí vždy nacházet jen na vyšetřovaném počítači. Sítě jsou tvořeny dalšími síťovými prvky jako například směrovače (routery), firewally, apod. Tyto stroje jsou často zdrojem cenných informací o dění v dané síti - posléze na daných počítačích. Zvláště když jsou tyto síťové prvky opatřeny IDS, což je nástroj přímo určený k "čmuchání", detekci podezřelých aktivit nebo logování. Takže k dispozici může být opravdu velké množství logů, které nemusejí být ve stejném formátu. Může být krajně náročné se v takových záznamech zorientovat - navíc pokud máte záznamy z různých časových pásem, které musíte analyzovat, vzniká další komplikace.

Vyšetřovatelé také musí počítat s tím, že logy, ke kterým se dostanou, nemusejí nemusí vypovídat o skutečné aktivitě. Narušitelé často používají například tzv. čističe logů, které dokáží odstranit (nebo modifikovat) ze síťového nebo jiného logu záznamy o určitém uživateli. Tato modifikace však nemusí být zcela dokonalá a vyšetřovatel si jí může všimnout.

3.4 Obnova

Pokud jsme analyzovali incident a víme, co se stalo, známe rozsah škod, tak je potřeba navrátit systém do původního stavu, ve kterým se systém (nebo celá síť) nacházel před incidentem. Samozřejmostí je opravení chyby nebo zabránění zneužití stejného postupu - stručně řečeno zabránit tomu, aby se tentýž incident opakoval. Je také možné, že bezprostředně po incidentu necháte vše jak je a budete útočníka pouze pozorovat a sbírat důkazy. Ovšem pokud chceme navrátit věci do původního stavu, je potřeba útočníka izolovat. To samozřejmě může kolidovat s dostupností

daného systému, proto záleží případ od případu, jak se zachováte. Můžete udělat kompromis a izolovat pouze napadený počítač a zde vyšetřovat útočníka. Tím zabráníte napadení ostatních systému v síti. Tato část sítě může dál normálně fungovat.

V souvislosti s izolováním útočníka bych chtěl zmínit tzv. honeypoty. To jsou stroje (dokonce i celé sítě takových strojů), které se vlastně doslova lákají útočníka, aby narušil jejich bezpečnost. Činnost útočníků je posléze podrobně zkoumána, takže tyto stroje musí být dobře monitorovány - často i předstírají jiný operační systém. Úkolem takových strojů je zjišťovat především nové postupy útočníků a tím následně lepší obrany proti těmto útokům.

Takže potom, co jsme dokončili vyšetřování a úspěšně izolovali systém a jsme si jisti, že nejsou ohroženy jiné systémy v souvislosti s vyšetřovaným incidentem, můžeme obnovit systém. Samotný systém můžete obnovit ze zálohy, která byla vytvořena před incidentem. Samozřejmě, jestli byla příčina incidentu v původní konfiguraci, tak ji je potřeba změnit tak, aby systém byl bezpečný.

Samozřejmostí je dokumentace všeho od začátku až do konce, z důvodu zdokumentování průběhu incidentu. Zdá se to být jako formální činnost, která může být navíc velmi zdlouhavá a nudná. Ale může mít zásadní vliv na závěry a reakce. Případ se může ocitnout u soudu a zde je dokumentace rozhodující. Navíc nikdo nemá takovou paměť, aby si vybavil všechna fakta, která mohou být i několik let stará. Další nutnou samozřejmostí je vytvoření závěrečné zprávy a tu opět vytváříte na základě dokumentace.

Kapitola 4

Závěr

Forenzní analýza digitálních dat je věda, která zaobírá velmi široký okruh témat. K jejímu pochopení je tedy potřeba mít znalost operačních systémů, sítí, hardwaru a dalších. Bez potřebných zkušeností nebudu schopni rozumně takovou analýzu provádět. Neodborná manipulace nejspíše povede k znehodnocení a ztrátě důkazů.

To jak budou organizace reagovat na incidenty závisí především na tom, zda-li budou připraveni, či ne. Samozřejmě musíte zanalyzovat vlastní zdroje, to co je potřeba chránit a jaké škody mohou nastat, pokud se stane nějaký neplánovaný krok. Provedení forenzní analýzy je obecně velmi nákladná záležitost. Je proto nutné dělat kompromisy a udělat samotnou bezpečnost, posléze reakci na incident, co nejefektivnější.

Literatura

[1] International Journal of Digital Evidence, online na Internetu: http://www.ijde.org/

[2] Michael A. Coloyannides, Computer Forensics and Privacy, Artech House, 2001

[3] Digital Forensics Research Workshop, online na Internetu: http://www.dfrws.org/

[4] Chris Prosise, Kevin Mandia: Incident Response and Computer Forensics, Osborne McGraw-Hill,

[5] Luther Troell, Yin Pan, Bill Stackpole: Forensic Course Development

[6] Erin Kenneally: Computer Forensics (The Magazine of Usenix & Sage)

[7] John Patzakis: Computer Forensics as an Integral Component of the Information Security Enterprise

[8] Karen Ryder: Computer Forensics - We'we had an incident, who do we get to investigate

[9] Diana J. Michaud: Adventures in Computer Forensics

[10] Brian D. Carrier, Eugene H. Spafford: Defining Event Reconstruction of Digital Crime Scenes

[11] Steve Hailey: What is Computer Forensics?, online na Internetu: http://www.cybersecurityinstitute.biz/

[12] Jeff Ballard, Dave DeCoster: Recovering From an Attack, online na Internetu: http://www.securitypipeline.com/

[13] Warren G. Kruse, Jay G. Heiser: What Exactly Is Computer Forensics?, online na Internetu: http://www.ebcvg.com/

Práce byla vytvořena sázecím jazykem LaTeX.