České vysoké učení technické v Praze

Fakulta elektrotechnická

Katedra telekomunikační techniky

Diplomová práce

Možnosti zvýšení zabezpečení pobočkové ústředny pro IP telefonii

Possibilities of security hardening of the IP PBX

leden 2018 **Diplomant: Bc. Jan Kabelka**

Vedoucí práce: Ing. Pavel Troller, CSc.

Čestné prohlášení

Prohlašuji, že jsem zadanou diplomovou práci „Možnosti zvýšení zabezpečení pobočkové ústředny pro IP telefonii“ zpracoval sám s přispěním vedoucího práce a používal jsem pouze literaturu uvedenou na konci práce. Souhlasím se zapůjčováním práce a jejím zveřejňováním.

Datum: 27.12.2018

.....

podpis diplomanta

Poděkování

Chtěl bych především poděkovat svému vedoucímu práce Ing. Pavlu Trollerovi za jeho čas, který mi během psaní diplomové práce věnoval. Dále bych rád poděkoval panu Petru Hněvkovskému ze společnosti HPE za poskytnutí instalačního software ArcSight a dočasné licence. V neposlední řadě můj velký dík patří mé ženě za trpělivost během celé doby mého studia na ČVUT FEL.

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Kabelka** Jméno: **Jan** Osobní číslo: **341138**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra telekomunikační techniky**

Studijní program: **Komunikace, multimédia a elektronika**

Studijní obor: **Komunikační systémy**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Možnosti zvýšení zabezpečení pobočkové ústředny pro IP telefonii

Název diplomové práce anglicky:

Possibilities of security hardening of the IP PBX

Pokyny pro vypracování:

Projděte a zanalyzujte metody zvýšení zabezpečení běžné IP pobočkové ústředny (například systému Asterisk) proti uskutečňování podvodných volání a dalším způsobům zneužití. Vybrané možnosti implementujte a prověřte jejich účinnost sadou penetračních testů při porovnání s holým neupraveným systémem.

Seznam doporučené literatury:

[1] Sohn, G.; Na, J.: System Architecture for Physical/IT Security Event Integration. International Journal of Computer Science and Network Security, 2012, p. 66-70.
[2] Coppolino, L.; D'Antonio, S.; Formicola, V.; Romano, L.: Integration of a System for Critical Infrastructure Protection with the OSSIM SIEM Platform: A dam case study. Lecture Notes in Computer Science, 6894, 2011, p. 199-212.
[3] Karlzen, H.: An Analysis of Security Information and Event Management Systems: The Use of SIEMs for Log Collection, Management and Analysis (Master Thesis). Chalmers University of Technology, University of Gothenburg, Gothenburg, Sweden, 2009.

Jméno a pracoviště vedoucí(ho) diplomové práce:

Ing. Pavel Troller, CSc., katedra telekomunikační techniky FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **20.09.2017** Termín odevzdání diplomové práce: **09.01.2018**

Platnost zadání diplomové práce: **18.02.2019**

Ing. Pavel Troller, CSc. podpis vedoucí(ho) práce	podpis vedoucí(ho) ústavu/katedry	prof. Ing. Pavel Ripka, CSc. podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

23.2.2018
Datum převzetí zadání

Podpis studenta

Anotace

Informační bezpečnost je po právu považována za jednu z klíčových oblastí světa IT. Schopnost předcházet útokům a reagovat na vzniklé bezpečnostní události je nedílnou součástí podnikového řízení informační bezpečnosti.

Náplní této diplomové práce je problematika informační bezpečnosti, jejího řízení, možných hrozeb, kterým dnes informační systémy musí čelit a způsob nakládání s bezpečnostními incidenty. V praktické části se věnuji nasazení systému SIEM ArcSight pro zpracování bezpečnostních událostí. Bezpečnostní události jsou generovány VoIP ústřednou Asterisk, která byla po instalaci cílem útoků. Součástí této diplomové práce jsou také návrhy protiopatření proti použitým typům útoků.

Klíčová slova

SIEM, ArcSight, Asterisk, Incident, Log, syslog

Anotation

Information security is rightly considered one of the key areas of the IT world. Ability to prevent attacks and responding to emerging security incidents is an integral part of enterprise information security management.

This diploma thesis deals with the issue of information security, its management and possible threats to which information systems must face today including the way of dealing with security incidents. In the practical part, I am deploying the SIEM ArcSight system for processing security events. Security events are generated by Asterisk's VoIP PBX, which was the target of attacks after its installation. This diploma thesis also includes proposals for countermeasures against various types of attacks.

Index Terms

SIEM, ArcSight, Asterisk, Incident, Log, syslog

Obsah

1 Úvod

U dnešních korporátních, moderních a velmi rozsáhlých sítí se stovkami koncových stanic a serverů, které nutně obsahují množství směrovačů (routers) a přepínačů (switches), DNS a DHCP serverů, doménových kontrolerů, load balancerů, VPN přístupových bodů, proxy serverů a dalších technologií, by měla být samozřejmostí přítomnost bezpečnostních technologií,jako jsou především anti-DoS/DDoS zařízení na perimetru sítě, firewally, web aplikační firewally, IPS/IDS systémy, bezpečnostní proxy brány, emailové brány, segmentační firewally a v neposlední řadě HIPS softwary a antivirové programy na koncových stanicích. Všechny tyto technologie plní více či méně svou funkci a mohou generovat a zpravidla také generují zprávy (logy) popisující dění na síti. Množství těchto událostí je potřeba neustále zpracovávat a vyhodnocovat, což klade nemalé nároky na vlastníky a správce informačních systémů. Velkým problémem dnešních informačních systémů je mít přehled o tom, co se na síti děje a dávat vše do souvislostí v reálném čase. Téměř nemožným úkolem se může jevit rychle a adekvátně reagovat na možnou bezpečnostní událost tak, aby byla tato událost správně klasifikována a byly provedeny kroky nezbytné k minimalizaci negativního dopadu na síťovou infrastrukturu a síťové služby. Situace, kdy bezpečnostní analytici dohlížející na dění na síti přistupují k jednotlivým systémům zvlášť a vyhodnocují logické a časové souvislosti dílčích událostí odděleně, se stala neudržitelnou. Množství technologií a jejich různorodost ve smyslu účelu, ke kterému jsou technologie určeny, ale také rozdílný přístup jednotlivých výrobců k řešení stejných problémů, to vše vedlo k požadavku na centralizaci správy těchto technologií. S tímto požadavkem úzce souvisí centralizovaný přístup k logům generovaných jednotlivými zařízeními a jejich automatickému vyhodnocování. Vyústěním těchto potřeb byl vznik technologií pod jednotným názvem Security Information and Event Management. Security Information and Event Management (SIEM) technologie umožňují efektivní správu logů, zobrazení událostí ve srozumitelné formě a v reálném čase, vytváření reportů, dále pak na základě korelací a pravidel k vynuceným automatickým změnám v síťovém prostředí a v neposlední řadě také k propojení s tiketovacími systémy.

Jsem přesvědčen o narůstající důležitosti informační bezpečnosti v IT světě, kde bude technologie SIEM hrát stále důležitější, časem možná primární úlohu. Především z tohoto

důvodu je v této diplomové práci kladen důraz na automatické zpracování logů, jejich korelaci a zobrazení prostřednictvím zvolené SIEM technologie tak, jak to vyžadují dnešní moderní společnosti, které to myslí s informační bezpečností vážně. Mým cílem v této diplomové práci je komplexně popsat zásadní oblasti informační bezpečnosti nezbytné pro správné uchopení potřeb a cílů týkajících se zabezpečení tak, jak to vyžaduje dnešní rychle se měnící doba.V praktické části pak praktické nasazení SIEM technologie ArcSight od společnosti Micro Focus a demonstrace zpracování bezpečnostních událostí SIEM systémem v reálném čase. K tomuto účelu jsem nainstaloval a zkompiloval ústřednu Asterisk, která byla terčem aktivity s cílem minimálně získat informace, dále pak pokusů o průnik do systému, a to jak pomocí veřejně dostupných nástrojů, tak i vlastních programových řešení. Tímto bych rád demonstroval sílu řešení SIEM a ukázal jeho efektivní využití při zpracování bezpečnostních událostí.

2 Základní pojmy z oblasti informační bezpečnosti

Většina firem, organizací a institucí se více či méně spoléhá na dostupnost a správnou funkčnost informačních systémů. S narůstajícím propojením informačních technologií s činnostmi a potřebami člověka se bezpečnost těchto systémů dostává zaslouženě stále více do popředí v diskuzích jak odborné, tak i laické veřejnosti. V dnešní době je naštěstí stále méně a méně organizací, které otázku informační bezpečnosti ignorují. Je to samozřejmě dáno faktem, že jedno z nejdůležitějších aktiv ve společnostech se stávají data a jejich dostupnost. Moderní společnosti mají problematiku informační bezpečnosti řešenu procesně. Před tím, než popíši systém SIEM, jeho nasazení, správu a vyhodnocování bezpečnostních událostí, v následujících kapitolách objasním význam základních pojmů z oblasti informační bezpečnosti, základní principy procesního přístupu k řízení informační bezpečnosti, legislativní rámce a další oblasti, které jsou klíčové pro správné uchopení problematiky informační bezpečnosti.

Data

Data jsou získané a zachycené údaje popisující realitu. Jsou to fyzicky zaznamenané výsledky pozorování reality, fakta, poznatky nebo znalosti a vědomosti. Data existují a jsou uložena na různých mediích nebo nosičích (např. papír, elektronické médium nebo lidská mysl). Interpretací dat a jejich vztahů za pomoci znalostí vznikají informace [1].

Informace

Informace je velmi široký pojem chápaný různými obory různě. Pro naše potřeby lze informace chápat jako strukturovaná, organizovaná, shrnutá a interpretovaná data. Pro nejmenší možnou informaci, tj. odpověď „ano-ne“ pak byla odvozena jednotka informace $1bit = -\log_2(1/2)$ [2].

Informační systém

Informační systém (IS) je celek složený z počítačového hardwaru a souvisejícího softwaru, k němuž patří také lidé, kteří tento hardware a software využívají, a procesy, které přitom vykonávají za účelem sběru, zpracování a šíření informací potřebných k plánování, rozhodování a řízení [3].

Služba IT

Služba je prostředek tvorby hodnot pro zákazníky. Poskytuje zákazníkům sjednané výsledky, aniž by tito museli nést zodpovědnost za specifické náklady a rizika spojená se službami [4]. Služba se také chápe jako explicitně definovaná a popsaná funkcionalita, poskytovaná informačními technologiemi, která podporuje či přímo umožňuje chod nějakého podnikového procesu, resp. podnikové činnosti [5].

Aktivum

Aktivum (Asset) je komponenta nebo určitá část celého systému, které organizace přikládá jistou hodnotu a pro kterou je třeba mít nastavený způsob ochrany. Je důležité uvědomit si, že aktivum vůbec nemusí být tvořeno hardwarem nebo softwarem. Mezi nejdůležitější aktiva řadíme informace, hardware, software, komunikační zařízení, dokumenty, personál a image společnosti [6].

Informační bezpečnost je obvykle definována na základě konceptu známého pod zkratkou CIA, která v tomto případě označuje anglická slova Confidentiality, Integrity a Availability. Koncept CIA je obecně přijímaným vymezením obsahu informační bezpečnosti. Akceptuje jej i česká právní praxe a právní řád. Jde o následující hodnoty [7].

Důvěrnost (Confidentiality)

Ochrana informací před neoprávněným přístupem, tj. stanovení, kdo a za jakých podmínek má k dané informaci přístup.

Integrita (Integrity)

Ochrana informace před neoprávněnou změnou nebo smazáním.

Dostupnost (Availability)

Zajištění trvalé, spolehlivé a bezpečné dostupnosti informace oprávněným osobám.

Následující pojmy jsou stěžejní pro uchopení informační bezpečnosti z pohledu výpočtu hodnot aktiva a analýzy rizik. Odborná veřejnost se ne vždy shodne na jejich přesné

definici, uvedené definice jsou jen jedním z mnoha způsobů, jak se dané pojmy chápou a definují[8].

Riziko (Risk)

Riziko je pravděpodobnost, s jakou bude daná hodnota aktiva zničena nebo poškozena působením konkrétní hrozby, která působí na slabou stránku této hodnoty. Je to tedy míra ohrožení konkrétního aktiva.

Hrozba (Threat)

Hrozba je skutečnost, událost, síla nebo osoby, jejichž působení (činnost) může způsobit poškození, zničení, ztrátu důvěry nebo hodnoty aktiva. Hrozba může ohrozit bezpečnost (např. přírodní katastrofa, hacker, zaměstnanec aj.).

Zranitelnost (Vulnerability)

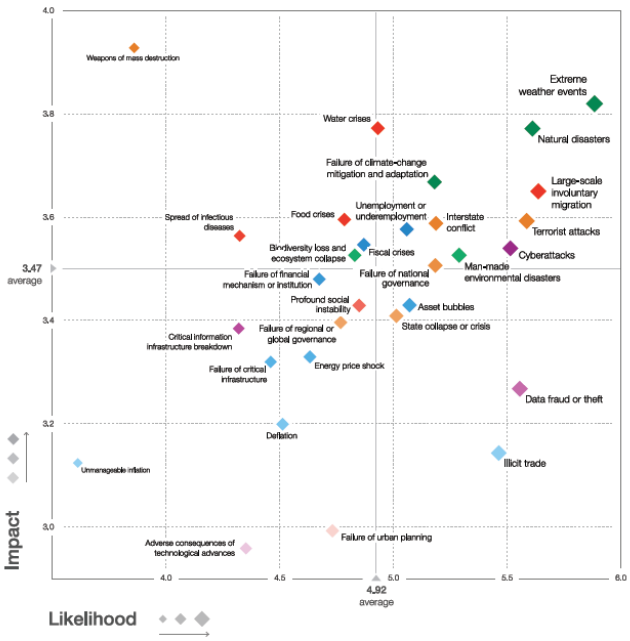
Slabinu informačního systému využitelnou ke způsobení škod nebo ztrát útokem na informační systém nazýváme zranitelné místo. Existence zranitelných míst je důsledek chyb, selhání v analýze, v návrhu a/nebo v implementaci informačního systému, důsledek vysoké hustoty uložených informací, složitosti softwaru, existence skrytých kanálů pro přenos informace jinou než zamýšlenou cestou apod.

Dopad (Impact)

Dopad je výsledek nežádoucího incidentu [9]. Dopad je výsledkem působení hrozby na konkrétní zranitelnost.

3 Analýza a řízení rizik

Analýza a řízení rizik je v podnikové sféře nedílnou součástí úspěchu. V oblasti informačních technologií se schopnost pracovat s rizikem stává stále naléhavější. Důvodem je především narůstající využívání informačních technologií a tedy i narůstající závislost organizací na informačních systémech. Dále pak narůstající složitost informačních systémů a s tím spojený trvalý pokles odbornosti správců a uživatelů těchto systémů. Podnikatelský úspěch společnosti a její vývoj je tedy úzce spjat se znalostí rizik informačních a komunikačních technologií (ICT). Za zmínku určitě stojí, že rizika spojená s kybernetickými útoky byla v roce 2017 organizací WEF (World Economic Forum) ohodnocena jako pátá nejpravděpodobnější z pohledu možnosti jejich vzniku.



Obr.1: Globální pohled na míru rizika pro jednotlivé hrozby, Zdroj: [1]

Řízením rizik v oblasti informačních technologií se zabývá norma ČSN ISO/IEC 27005. Základní oblasti řízení rizik jsou oblasti ohodnocení aktiv, analýza rizik a zvládnutí rizik. Ve stručnosti je věnována pozornost i těmto jednotlivým aspektům řízení rizik ICT.

Aby bylo možné aktiva ohodnotit, je potřeba je nejdříve identifikovat. To zahrnuje logické seskupování aktiv, typicky podle jejich funkce a obsahu. Vznikají tak skupiny

programových aktiv, hardwarových aktiv, aktiva spojená s papírovými dokumenty, aktiva služeb, obchodní aktiva a podobně. Dále je potřeba identifikovat nebo přidělit každému aktivu, popřípadě skupinám aktiv jejich vlastníka. S vlastníkem se spolupracuje na vytvoření potřebné dokumentace a na ohodnocení daných aktiv či skupin aktiv, kdy se musí zvolit vhodná stupnice a hodnotící kritéria.

Analýza rizik je jedna z nejdůležitějších součástí řízení bezpečnosti ICT. Cílem analýzy rizik je identifikace zranitelností informačního systému a identifikace hrozeb, které jsou s danou zranitelností spojeny. Konečným cílem je stanovení míry rizika spojené s každým zranitelným místem a na něj působící hrozbou [10].

Odpovědné osoby na základě výstupů z minulých dvou fází mohou rozhodnout o konkrétních protiopatřeních, které se mají implementovat. Jedná se zde o zvládnutí rizika. Obecně pro každé jednotlivé riziko musí organizace zvážit několik základních možností. Jsou to především možnosti přijetí rizika, zabránění riziku, přenos nebo sdílení rizika, zmírnění rizika a ignorování rizika [11].

4 Procesní řízení informační bezpečnosti

Řízení informační bezpečnosti je budováno v souladu s celkovým systémem řízení organizace. Důraz je samozřejmě kladen na ochranu informací jako jednoho z nejcennějších aktiv. Zavedení systému řízení informační bezpečnosti založeného na uznávaných standardech umožňuje organizaci naplňování vnitřní politiky v oblastech kvality služeb, spokojenosti zákazníků, kompetentního managementu a řízení společnosti [12].

Existují různé návrhy procesně orientovaných modelů, kterými lze koncipovat a strukturovat správu služeb IT. Nejdůležitější a nejrozšířenější rámec pro navrhování, správu a optimalizaci v ITSM je IT Infrastructure Library (ITIL). ITIL představuje ve formě sbírky knih rozsáhlý a všeobecně dostupný návod pro správu služeb IT. Uvedené zkušenosti a doporučení se v mezičase staly nejlepšími praktikami, de facto standardem. Jako rámec poskytují dostatečnou flexibilitu pro přizpůsobení doporučení z knih ITIL vlastním požadavkům a potřebám konkrétní organizace. ITIL poskytuje volně dostupný rámec, zahrnující celý cyklus služeb IT [12].

Obr.2: ITIL životní cyklus IT služeb, Zdroj: [31]

Za klíčové publikace ITIL je označováno pět knih. Každá kniha představuje jednu fázi životního cyklu a popisuje příslušné principy, procesy, funkce, organizační a technologické aspekty a další příslušná témata [12]. Jednotlivé knihy ITIL, respektive fáze životního cyklu IT služeb, jsou následující.

Strategie služeb (Service Strategy)

První fázi lze chápat jako návod, jak se navrhuje, vyvíjí a implementuje správa služeb. Obsah tohoto svazku se vztahuje např. k vývoji na domácích a zahraničních trzích, aktivům služby a implementaci strategie pro celý životní cyklus služby.

Návrh služeb (Service Design)

Nabízí návody pro návrh a vývoj služeb a procesů. Představuje designové metody a principy, pomocí kterých lze převést strategické cíle do portfolia služeb a aktiv služby.

Přechod služeb (Service Transition)

Stará se o zavádění nových nebo pozměněných služeb do výrobního prostředí.

Provoz služeb (Service Operation)

Zabývá se činnostmi s ohledem na účinnost a efektivitu dodávky a provozu služeb.

Neustálé zlepšování služeb (Continual Service Improvement)

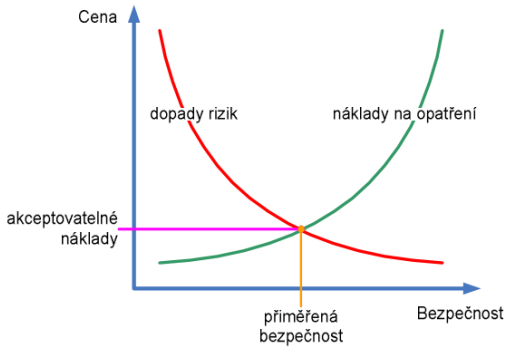
Poskytuje nástroje a návody pro nepřetržité zlepšování služeb a všech dříve zmíněných aspektů jako je návrh, zavádění a provoz služeb IT [12].

Bezpečnost informací je součástí druhé knihy ITIL. Cílem správy bezpečnosti informací je pro daný podnik vytvořit a udržovat definovanou bezpečnost informací. Bezpečnost IT se přitom musí řídit podle podnikové bezpečnosti. U aktiv, informací, dat a služeb IT jde o výše popsanou triádu CIA [12]. Formální systém sloužící k zavádění pravidel a cílů se nazývá Information Security Management Systems (ISMS), reprezentovaný řadou norem ISO/IEC 27001. Tento systém správy bezpečnosti informací tvoří součást řídicích činností organizace a jeho hlavním cílem je eliminovat nebo snížit rizika související s možným narušením důvěrnosti, integrity a dostupnosti informací [12].

Zvláštní pozornost patří správě incidentů narušení bezpečnosti. Správa incidentů detekuje a přijímá bezpečnostní incidenty. Při narušení bezpečnosti je odstartován samostatný proces. Je proto nesmírně důležité, aby bylo vůbec selhání bezpečnosti odhaleno. Při konečném

hodnocení je pak potřeba zjistit, jak mohlo k chybě vůbec dojít. Je tak možné zhodnotit a zlepšit účinnost a efektivitu procesu. Výsledkem tohoto procesu jsou například předpisy bezpečnosti informací, procesy analýzy a správy rizik, zprávy a hodnocení, bezpečnostní řídící mechanismy, audity a výkazy bezpečnosti, klasifikace bezpečnosti, přezkoumání narušení a poruch bezpečnosti (bezpečnostní incident) [12].

Zajištění bezpečnosti není hledáním dokonalého způsobu ochrany, ale aplikací takových opatření, která jsou přiměřená hodnotě předmětu ochrany (aktiv). Primárním předmětem ochrany jsou informace (nikoliv jejich nosiče nebo prostředky pro zpracování). Čím větší hodnotu pro nás informace mají, tím větší pozornost musíme věnovat bezpečnosti jejich nosičů. Každá organizace by si proto měla provádět alespoň základní hodnocení a kategorizaci svých informací a tomu přizpůsobit i způsob jejich ochrany [13].



Obr.3: Zvažování rizik a opatření (analýza nákladů a přínosů), Zdroj: [32]

Velikost úsilí a investic do bezpečnosti musí odpovídat hodnotě aktiv a míře možných rizik. Změny v procesech organizace při zavádění ISMS a při aplikaci opatření v ICT systémech musí dostatečně redukovat dopady možných rizik za akceptovatelných nákladů [13].

5 Zpracování bezpečnostních incidentů

Schopnost organizace reagovat na bezpečnostní události je kritická jak z důvodu zabránění negativního dopadu na organizaci, tak i z důvodu navyšování bezpečnosti. Kvalitně zpracovaná dokumentace k manipulaci s bezpečnostními incidenty je nedílnou součástí procesního přístupu k efektivnímu řízení informační bezpečnosti. Bezpečnostní události lze rozdělit do čtyř skupin.

	TRUE	FALSE
POSITIVE	True-Positive	False-Positive
NEGATIVE	True-Negative	False-Negative

Obr.4: Klasifikace bezpečnostních incidentů

Pravdivě pozitivní (True-Positive)

Bezpečnostní pravidlo (signature) bylo spuštěno a k útoku došlo.

Falešně pozitivní (False-Positive)

Bezpečnostní pravidlo bylo spuštěno a k útoku nedošlo.

Pravdivě negativní (True-Negative)

Bezpečnostní pravidlo nebylo spuštěno a k útoku nedošlo.

Falešně negativní (False-Negative)

Bezpečnostní pravidlo nebylo spuštěno a k útoku došlo.

5.1 Fáze nakládání s incidenty

Nakládání s bezpečnostními incidenty je v podstatě akční plán pro zpracovávání událostí zneužití počítačových systémů a sítí, jako jsou vniknutí do systému (Intrusions), infikace škodlivým kódem (Malicious code infection), kybernetická krádež (Cyber-theft), odmítnutí služby (Denial of service) a další.

Existují různé modely, jak zpracovávat bezpečnostní incidenty. Osobně jsem vybral členění společnosti SANS Technology Institute, která je významným hráčem v globálním měřítku na poli informační bezpečnosti. Součástí modelu této společnosti je celkem šest fází, které budou níže ve stručnosti popsány. Jsou to příprava (Preparation), identifikace (Identification), zamezení šíření (Containment), vymýcení (Eradication), obnovení (Recovery), ponaučení (Post-Incident Activity). Souslednost jednotlivých fází je vidět na obrázku níže.

Obr.5: Šestifázový cyklus manipulace s incidenty, Zdroj: [33]

5.1.1 Příprava

Organizace by měla být připravena i na ty nejméně pravděpodobné události s negativním dopadem na její byznys, samozřejmě s vědomím důležitosti daného aktiva. To zahrnuje celou řadu aspektů, na které musí být v této fázi brán zřetel. Jeden z nejpřehlíženějších aspektů v přístupu k informační bezpečnosti jsou lidé. Lidé jsou nejsnadnějším cílem útoků, jako jsou metody sociálního inženýringu (Social Engineering) a především phishingových emailových zpráv (Phishing Emails).

Každý systém musí být opatřen varovným banerem (Warning Banner). Informace obsažené v těchto prohlášeních upozorňují uživatele, že je přístup k systému povolen pouze autorizovaným uživatelům, že jsou zakázány modifikace systému, neautorizovaní uživatelé mohou čelit právním následkům, v neposlední ředě pak informace o tom, že může být systém monitorován a všechny změny mohou být zaznamenávány a v případě potřeby použity u soudu. Vzhledem k tomu, že se jedná o oficiální prohlášení organizace, musí být schváleno právním oddělením příslušné organizace.

Musí se také stanovit organizační kontaktní matice, která jasně vymezuje, komu se budou jaké incidenty hlásit, v jaké podobě a v jakých intervalech v případě dlouhotrvajícího incidentu. To zahrnuje také jasně stanovené postupy pro kontaktování policie a podobně.

V průběhu incidentu se zaznamenává každý krok a zjištění během jeho řešení. Poznámky mohou posloužit jako důkazy v případě soudního procesu i o několik let později. To zahrnuje zaznamenávání odpovědí na otázky typu kdo, co, kdy, kde, jak a proč.

5.1.2 Identifikace

Vyskytne-li se bezpečnostní incident v informačním systému, nejdříve se přidělí konkrétní osoba, která bude daný incident řešit (Incident Handler). V počátku této fáze není a nemůže být jasné, jaký bude mít incident průběh a důsledky, je proto vhodné sdílet informace o průběhu jeho řešení s co nejmenším okruhem lidí. Řešitel se opírá o dokumenty připravené v předchozí fázi.

Nebývá vždy jednoduchým úkolem zjistit, kde byl počátek incidentu. K detekci může dojít na několika úrovních, a to na síťovém perimetru (Network Perimeter Detection), na perimetru hostitelského systému (Host Perimeter Detection), na systémové úrovni (System-level Detection) a na aplikační úrovni (Application-level Detection).

Často dochází k identifikaci incidentu až po infiltraci, kdy je organizace informována o skutečnosti, že se sama stala útočníkem, nebo že už jsou její informační zdroje a služby blokovány třetími stranami. Z tohoto důvodu by měla být bezpečnost řešena v souladu s konceptem hloubkové ochrany (Defense in Depth), kdy jsou bezpečnostní principy

aplikovány ve více vrstvách, tedy na úrovních jak procesních, fyzických, tak i na všech úrovních v rámci ISO/OSI modelu.

Po nalezení incidentu a jeho zdroje se analyzují jeho skutečné příčiny a důsledky. Řešitel by měl mít poměrně detailní představu a standardním chování systému, aby měl možnost objevit nezvyklé skutečnosti a anomálie. To zahrnuje zaměření se na neobvyklé skutečnosti, jako jsou procesy a služby (Processes and Services), soubory (Files), využití síťových zdrojů (Network Usage), naplánované úlohy (Scheduled Tasks), účty (Accounts), systémové logy (Logs) a ostatní neobvyklé skutečnosti.

Cílem v rámci identifikace, jak byla popsána výše, je zjistit, zda se opravdu jedná o incident a pokud ano, získat co nejpřesnější představu o jeho příčinách a následcích. Chybové stavy systému nebo falešně pozitivní události by měly být také součástí procesního řízení a je potřeba jim předcházet a odstraňovat je.

5.1.3 Zamezení šíření

Cílem této fáze je zamezení šíření negativních dopadů bezpečnostního incidentu. Jde tedy o zamezení šíření a prevenci šíření nákazy, nebo negativního dopadu obecně, což zahrnuje jak prevenci proti automatickému šíření škodlivého kódu, tak i zamezení proniknutí útočníka hlouběji do systému. Tato fáze obsahuje tři subfáze, a to okamžité zamezení šíření (Short-Term Containment) sloužící k okamžitému zamezení šíření dopadu, následované obnovením systému ze záložních zdrojů (System Back-Up) a konečně průběžné zamezení šíření (Long-Term Containment), sloužící k získání jistoty, že byl útočníkovi znemožněn přístup k systémům.

Pro okamžité zamezení šíření se v ideálním případě systém izoluje od ostatních provozních systémů, a to vždy po schválení zainteresovaných byznys stran, jako jsou vlastníci dotčených služeb (Service Owners) a podobně. Možných způsobů, jak systém izolovat, je celá řada a jsou to především následující:

- Odpojení síťového kabelu
- Odpojení napájecího kabelu (zapříčiní ztrátu dat z paměti typu RAM a může mít negativní dopad na pevné disky (Hard Drives))

- Izolace L2 (Layer2) portu na separátní ohroženou VLAN (Virtual Local Area Network)
- Aplikace ACL (Access Control List) pravidel na směrovačích a/nebo pravidel na firewallech
- Vytvoření tzv. Null Route na směrovači, kdy je průchozí provoz (Traffic) zahazován (Drop)
- Změna DNS záznamu tak, aby směřoval na jinou IP adresu, např. na tzv. Honey Pot

Všechny tyto zásahy by měly proběhnout bez vlivu na systémové pevné disky, aby bylo možné vytvořit obraz těchto disků pro pozdější investigaci (Forensics Image). Pokud to situace dovolí a je to praktické, je doporučeno vytvořit obraz také z volatilních pamětí. Opět, pokud to situace dovolí, doporučuje se vytvořit kopii i souborových systémů (File Systems), a to jedna k jedné (Bit-by-Bit). Pro jednoznačnou identifikaci stavu systému se vypočítá a uloží výstup z hash funkce (např. MD5, SHA) jak originálního systému, tak i jeho obrazu.

Jsou-li získána všechna potřebná data pro pozdější, detailní analýzu, může být systém obnoven ze zálohy.

Pokud není možné afektovaný systém izolovat od zbytku sítě, tedy služby běžící na tomto systému musí zůstat dostupné i během investigace, v síti se nenachází záložní systém se stejnou funkcí, nebo nelze z kapacitních důvodů produkční provoz na záložní systém přesměrovat, pak se aplikují dočasná protiopatření k zamezení šíření negativního dopadu. Jsou-li vytvořeny zálohy pro forenzní analýzu, lze aplikovat především tato protiopatření.

- Aktualizace OS (Operating System), firmwaru a dalších (Patching)
- Aplikace vhodných pravidel na IPS
- Odstranění uživatelských účtů, které byly zneužity nebo vytvořeny útočníkem

- Vypnutí procesů příslušejících zadním vrátkům do systému (Backdoors)

5.1.4 Vymýcení

V této fázi se pracuje s informacemi získanými během předchozích dvou fází a cílem je zbavit se všech artefaktů, které byly do informačního systému zaneseny útočníkem. To zahrnuje určení přesných příčin útoku a jeho symptomů, tedy jakým způsobem došlo k napadení systému. Odstranit všechny části malwaru vloženého útočníkem nebývá jednoduchou činností a například v případě nakažení systému malwarem z rodiny RootKit a Kernel-Level RootKit je silně doporučeno systém obnovit z původní, čisté zálohy (Re-image). Součástí této fáze je také navýšení bezpečnosti na základě zjištěných vektorů útoku (Attack Vectors).

- Aplikace filtrů na směrovačích a firewallech
- Zvolení nových DNS jmen nebo IP rozsahů
- Null routing pro částečné IP rozsahy
- Aktualizace softwaru na nejnovější verze (Software Updates)

5.1.5 Obnovení

Jakmile byl systém obnoven a uveden do funkčního a bezpečného stavu, dojde k ověření funkčosti všech jeho komponent. Po dohodě s vlastníkem systému se zvolí doba, kdy dojde k nasazení systému zpět do produkční sítě, nejlépe pak mimo pracovní dobu. Vlastník systému otestuje jeho funkčnost v produkčním prostředí a potvrdí možnost uzavření incidentu. Osoby zodpovědné za řešení incidentu musí po vhodně zvolenou dobu pečlivě monitorovat systém pro případ, že by došlo k opětovnému napadení/infekci. Monitorování zahrnuje zájem i o sousední systémy, které mohly být také napadeny, ale zatím se neprojevily žádné skutečnosti, které by tomu nasvědčovaly.

5.1.6 Ponaučení

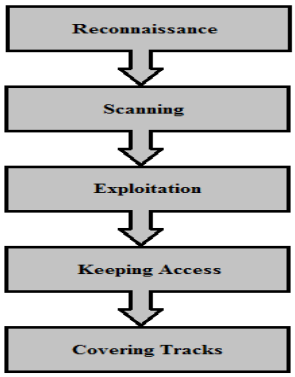
Poslední fází je fáze, do které spadá zhodnocení průběhu řešení bezpečnostního incidentu. To obnáší vytvoření reportů o incidentu zahrnující detailní popis investigace a všech

nálezů, způsobů odstranění dopadů a popis postupu uvedení všech afektovaných systémů do bezpečného stavu. Primárním cílem této fáze je ponaučení se z proběhnuvšího incidentu a jeho řešení, tedy nalezení slabých míst v procesech, dokumentech, technologiích, ale i lidech tak, aby mohlo dojít k jejich vylepšení a tím i navýšení informační bezpečnosti do budoucna.

6 Fáze kybernetického útoku

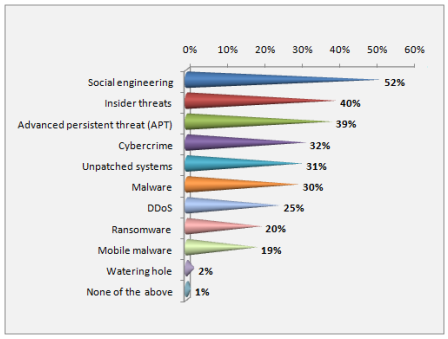
V této kapitole si kladu za cíl popsat logickou návaznost jednotlivých fází kybernetického útoku s některými nejběžnějšími příklady. Fáze kybernetického útoku se dají rozdělit do následujících.

- Průzkum (Reconnaissance)
- Skenování (Scanning)
- Průnik a zneužití (Exploitation)
- Udržování přístupu (Keeping Access)
- Krytí stop (Covering Tracks)



Obr.6: Fáze kybernetického útoku

Pro představu na obrázku níže uvádím dnešní nejčetnější hrozby, kterým se ve světě IT čelí.



Obr.8: Kybernetické hrozby, Zdroj: [35]

6.1 Průzkum

Útočník musí nejprve získat o svém cíli útoku co nejvíce informací, a to v ideálním případě takovým způsobem, aby o tomto shromažďování neměla oběť ponětí. K těmto účelům je dnes k dispozici obrovské množství informačních zdrojů a dedikovaných nástrojů. Internet je samozřejmě primárním zdrojem při získávání těchto informací.

6.1.1 Získání informací o doméně

Výchozím zdrojem bývají informace, které jsou vyžadovány registrátory domén a IP adres v jednotlivých geografických regionech. Pro Evropu je tímto registrátorem otevřené fórum RIPE NCC (více na www.ripe.net). Prostřednictví služby **whois lookup** (protokol WHOIS na portu TCP/43) lze získat množství užitečných informací, jako je čas registrace, doba expirace záznamu, osobu, na kterou je záznam veden, adresu, DNS servery pro danou doménu a mnoho dalšího. Domain Name System je plný užitečných informací o cíli. Vdalších krocích je cílem útočníka získat informace o co největším množství IP adres spojené s cílovou doménou. K tomuto účelu bývají hojně používány veřejně dostupné nástroje jako je **nslookup** a **dig**, které lze využít k interakci s DNS servery. Pomocí těchto nástrojů může útočník jednoduše získat IP adresy spojené s danou doménou (A záznamy), záznamy emailových serverů (Mail eXchange (MX) záznamy), informace o jmenných serverech (NS záznamy), ale i celé zónové soubory (Zone Files).

6.1.2 Webové služby

Nejjednodušší cesta jak získat informace je jednoduše se na ně zeptat. K těmto účelům skvěle poslouží vyhledávací nástroje typu Google, Biadu, Yahoo, Bing a další. Pro získání informací potřebné k fyzickému přístupu poslouží aplikace typu Google Maps, Google Street View a další, jejichž API (Application Programming Interface) může být propojeno s množstvím aplikací dalších subjektů. Mnoho z výše uvedených nástrojů nabízí užitečné vyhledávací ukazatele (Search Directives) pro průzkumnou fázi útoku. Takto lze získat například informace o nabízených IT Security pozicích v dané společnosti, a tedy i představu o tom, jaké technologie společnost používá. Dalším bonusem je, že mnoho souborů obsahuje tzv. metadata, jejichž součástí jsou informace o uživatelích, verzích softwaru (a tedy i informace o zranitelnostech dané verze), adresářová cesta k souboru (Directory Path) a podobně. Opět existuje velké množství veřejně dostupných nástrojů automatizujících a rozšiřujících tyto činnosti.

6.2 Skenovací techniky

Skenovací techniky slouží ke zjištění systémů, které jsou na síti aktivní, dále ke zjištění veřejně dostupných služeb na těchto systémech a jejich zranitelností. Zaměřím se zde nejdříve na skenování dostupných systémů a jejich služeb.

6.2.1 Mapování sítí

Prvním cílem při mapování sítí je zjistit, které ze systémů odpovídají a jsou tedy síťově dostupné. Útočník zasílá například jednoduché ICMP Echo Request pakety na celý síťový rozsah IP adres a z odpovědí ICMP Echo Reply tak může zjistit dostupnost jednotlivých IP adres, tzv. ping sweep. K tomuto účelu je v současné době nejpoužívanějším nástrojem **nmap**. V případě, kdy cílový host neodpoví, nemusí to nutně znamenat, že je neaktivní. ICMP Echo Request pakety jsou často blokovány na firewallech. Ke zjištění topologie skenované sítě lze s úspěchem využít nástroj **traceroute** (GNU/Linux) a **tracert** (Windows) prostřednictvím například programu Zenmap GUI. Nástroj **traceroute**, resp. **tracert** využívá ke své funkci pole TTL v hlavičce paketu IPv4, resp. pole Hop Limit

v hlavičce paketu IPv6. Ke grafickému zobrazení tohoto typu skenování slouží právě nástroj Zenmap GUI.

6.2.2 Skenování portů

Skenování portů slouží ke zjištění, zda na daném portu naslouchá nějaká služba a dále ke zjištění typu skenovaného systému. Seznam čísel portů a služeb k nim přiřazených spravuje organizace IANA. Opět se zde s úspěchem využívají široké možnosti nástroje **nmap**. Tento nabízí řadu přepínačů, jejichž pomocí lze provádět různé skenovací techniky s cílem obejít nastavení firewallů, směrovačů, ale i IPS/IDS systémů a zjistit o koncovém systému potřebné informace. Uvedu zde pro ilustraci pouze jeden ze základních způsobů, jak obejít blokaci příchozích TCP SYN (Synchronize) paketů na bezestavovém (Stateless) firewallu. Možnosti jsou ale samozřejmě mnohem širší, komplexnější a komplikovanější.

V případě, že firewall blokuje příchozí SYN pakety a znemožňuje tak navázat TCP spojení z vnější strany sítě, pomocí nástroje **nmap** lze zaslat pouze paket s příznakem (Flag) ACK (Acknowledgement), tedy poslední z paketů při třícestném navazování TCP spojení (Tree-Way Handshake). Tento paket standardně slouží k potvrzení inicializující strany o ustanovení TCP spojení, kdy následuje samotný přenos dat. Bezestavový firewall tento paket propustí, jelikož si nedrží informace o navazovaných spojeních. Skenovaný systém za firewallem tento paket neočekává, jelikož žádné spojení nenavazuje, a odešle paket RST (Reset) pro zrušení této komunikace. Útočník v této chvíli nezjistí, zda je daný port otevřen, ale minimálně se dozví, že je koncový systém aktivní a může pokračovat pomocí dalších technik ve zjišťování podrobnějších informací. Dalšími běžnými skenovacími technikami jsou např. SYN skeny, FIN (Finish) skeny, UDP skeny, RPC skeny a další.

Pokusy o určení operačního systému probíhají prostřednictvím zasílání variací typů paketů a analýzou došlých odpovědí. V příslušných RFC je specifikováno, jakým způsob by systémy měly odpovídat během inicializace TCP spojení. Není už však řečeno, jak by měla vypadat odpověď v případě nelegitimního nastavení TCP příznaků. Na straně výrobců operačních systémů probíhá implementace chování systémů v reakci na příchozí nelegitimní TCP pakety různě a tedy se různí i jejich odpovědi na tyto typy paketů. Nástroj **nmap** si udržuje databázi variací možných odpovědí a jim příslušejících operačních

systémů a je tak schopen s poměrně vysokou pravděpodobností určit typ cílového operačního systému.

6.2.3 Skenování zranitelností

Nástroje automatizující skenování zranitelností (Vulnerability Scanners) jsou extrémně účinné jak z pohledu potenciálního útočníka, tak i z pohledu společností, které se vážně zabývají informační bezpečností. Množství firem dnes nabízí komerčně dostupné služby, díky kterým se společnosti mohou dozvídat o zranitelných místech v jejich systémech. Je však potřeba brát v potaz limitace těchto nástrojů. Je to především fakt, že tyto nástroje mají možnost objevit pouze zranitelnosti o kterých ví a mají je tedy možnost testovat. Zranitelnosti, jejichž znalost není v těchto nástrojích implementována, nemůžou být jednoduše rozpoznány. Dalším limitujícím faktorem je schopnost korelace mezi jednotlivými zranitelnostmi. Dejme tomu, že se v systému nachází zranitelnosti A a B ohodnocené jako nízkoriziková, dále pak zranitelnost C ohodnocena jako středně riziková. Vzhledem k přítomnosti těchto tří zranitelností na jednom systému může být celková míra rizika ohodnocena jako extrémní, skener zranitelností tuto korelaci ale neprovede a míru rizika neohodnotí adekvátně. Potenciální útočník si vztahu těchto tří zranitelností může být vědom a může ho využít k napadení systému.

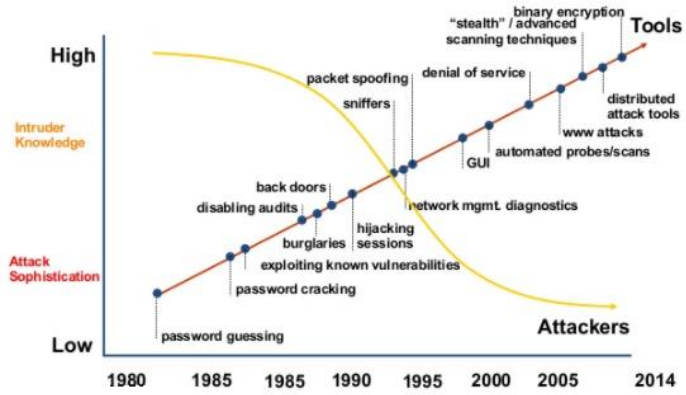
Ke komerčně nejúspěšnějším skenerům tohoto typu patří Rapid7 NeXpose, dále pak například Qualys a McAfee's Foundscan, které mohou být použity v nekomerčním prostředí zdarma.

Je potřeba si uvědomit, že používání těchto nástrojů může být považováno v některých státech za nelegální, v komerčním prostředí musí být jejich použití podloženo náležitými procesy už jenom z toho důvodu, že tyto nástroje mohou způsobit nepříjemnosti typu DoS/DDoS.

6.3 Průnik do systému a jeho zneužití

Není možné v této diplomové práci obsáhle popsat všechny možné kybernetické hrozby a útoky, kterým dnešní informační systémy čelí. Cílem této kapitoly je zmínit nejběžnější hrozby a způsoby, jakými se útočníci dostávají do informačních systémů. Na grafu níže je

znázorněn nepříznivě vyhlížející fakt, a to že potřebná odborná znalost útočníků se neustále snižuje (Script Kiddies), zatímco komplexnost útoků a tedy i potřebná odborná znalost na straně obětí a úroveň potřebného zabezpečení roste.



Obr.7: Úroveň kybernetických útoků versus potřebná technická znalost útočníků, Zdroj: [34]

6.3.1 Získání přístupu

Nejprve popíši některé nejběžnější techniky a hrozby, které spadají do oblasti získání přístupu k systému (Gaining Access).

BGB Hijacking

Útočník na ISP směrovače zpropaguje nežádoucí BGP záznamy, kdy je následně provoz směrován na adresu útočníka a ten pak, aby nebyl snadno odhalen, posílá provoz oběti tak, jak je očekáváno.

Pasivní a aktivní odposlouchávání

Útočník používá nástroje pro odposlouchávání (Sniffing)a změnu (Spoofing) průchozího provozu. Může tak pasivně odposlouchávat provoz na bezdrátové síti, nebo injektovat na druhé až sedmé vrstvě potřebné záznamy na příslušné systémy (DNS Poisonning, ARP Spoofing a další.) či podvrhnout obětí přijímaná či odesílaná data konkrétním způsobem v určité fázi komunikace (Session Hijacking a další).

Přetečení vyrovnávací paměti

Metoda přetečení zásobníku (Buffer Overflow) využívá zranitelností na úrovni jádra operačního systému, kdy program zapisující do vyrovnávací paměti překročí vyhrazené místo a zapíše nežádoucí instrukce do sousedních úseků paměti. Tyto úseky jsou pak využity při následném vyčítání instrukcí a systém se těmito instrukcemi samozřejmě řídí. Těmito technikami lze způsobit kolaps systému, nebo nestandardní chování systému vynucené a zamýšlené útočníkem.

Metasploit

Velice účinný nástroj vytvořený H.D.Moorem. Nástroj Metasploit se skládá ze dvou základních prvků. Prvním z nich je databáze tzv. exploitů, což jsou kódy využívající zranitelností. Druhým prvkem je tzv. payload, kód který je za pomoci exploitu přenesen na cílový systém a tam je spuštěn. Pomocí tohoto nástroje lze získat administrátorká práva, spuštění zadních vrátek do systému a mnoho dalšího. Tento nástroj je velmi populární především z důvodu snadnosti jeho použití.

Útoky na uživatelské účty

Při těchto útocích se útočník snaží získat platná uživatelská jména a hesla. Pokud útočník získal uživatelská jména v průzkumné fázi útoku, má několik možností, jak získat hesla. Jsou to především útoky hrubou silou (Bruteforce Attack), kdy útočník zkouší kombinaci všech možných hesel nebo používá databázi pravděpodobných a slabých hesel proti jednomu účtu, nebo malému množství uživatelských účtů. Možností je také použít několik málo hesel proti velkému množství uživatelských účtů (Password Spraying). Pokud má útočník k dispozici pouze hashe hesel, s úspěchem bývá využíváno databází s hesly a jim odpovídajících hashů, tzv. duhové tabulky (Rainbow Tables). Slabostí mnoha systémů je pak chybová hláška po zadání špatného uživatelského jména či hesla, kdy systém přímo ohlásí, která z možností byla zadána špatně. Díky této informaci lze sbírat jména platných uživatelských účtů (Account Harvesting).

6.3.2 Web aplikační útoky

Nejběžnějšími útoky na webové služby a aplikace jsou následující tři.

Injekce příkazů

Některé webové aplikaci berou vstup od uživatele jako vstup pro skript, který je následně spuštěn. Při nesprávně napsané aplikaci lze jako vstup vložit konkrétní kód, který je následně spuštěn a vykonán.

SQL Injection

Jedná se v podstatě o využití neošetřeného uživatelského vstupu při dotazech do webové databáze. Vhodně zvoleným SQL dotazem do databáze lze vyčítat data, která by uživatel vůbec neměl získat. Obrana proti tomuto typu útoku je poměrně jednoduchá, kdy se nadefinuje, jaké znaky a posloupnosti znaků uživatel nemůže použít. Bohužel vývojáři webových aplikací tento typ útoku podceňují.

Cross-site Scripting

Cross-site scripting (XSS) je metoda narušení WWW stránek využitím bezpečnostních chyb ve skriptech (především neošetřené vstupy). Útočník díky těmto chybám v zabezpečení webové aplikace dokáže do stránek podstrčit svůj vlastní javascriptový kód, což může využít k poškození vzhledu stránky, jejímu znefunkčnění, získávání citlivých údajů návštěvníků stránek nebo obcházení bezpečnostních prvků aplikace. Často je též využíván při phishingu tak, že je skrze XSS zranitelnosti uživateli ukázán jiný obsah na jinak důvěryhodné stránce [38].

6.3.3 Denial of Service

Odmítnutí služby (Denial of Service) zahrnuje mnoho technik, které vyústí v nedostupnost služby. Lze sem zařadit útoky na první vrstvě modelu ISO/OSI, jako je například fyzické odpojení služby, ale samozřejmě i útoky na vrstvách vyšších. Typickými příklady jsou zahlcení cachovacích MAC tabulek na přepínačích, routovacích tabulek na směrovačích, cachovacích tabulek DNS serverů, NAT tabulek a dalších. Na koncových systémech je nejtypičtějším zástupcem tzv. SYN Flood, kdy útočník zasílá na server velké množství SYN paketů, které jsou součástí každého navazování TCP spojení. Server si v dočasné paměti drží o tomto spojení záznam a čeká na jeho úplné navázání. V případě zahlcení

paměti pak nemá dostatečné prostředky na odbavování legitimního provozu a tento zahazuje.

6.4 Udržování přístupu

Po získání přístupu k systému s potřebnými právy útočník typicky potřebuje vytvořit zadní vrátka, díky nimž pro něj systém zůstane přístupný i v budoucnu. Škodlivé programy útočník může nainstalovat na všech úrovních operačního systému, to znamená jak na aplikační úrovni (Application Level Trojan Horse Backdoors), uživatelské úrovni (User-Mode Rootkits), tak i na úrovni jádra systému (Kernel-Mode Rootkits). Pro skrytí těchto programů se využívají techniky skrytí škodlivého programu v legitimních programech běžících na systému. Zadní vrátka na úrovni jádra operačního systému lze označit za nejzákeřnější, protože je velmi obtížné je odhalit. I když dojde k jejich odhalení, bývá často velmi náročné se jich zbavit a musí se proto přistoupit ke kompletnímu přeinstalování systému a obnovení jeho stavu ze zálohy.

6.5 Krytí stop

Metody krytí stop na kompromitovaném systému zahrnují mnoho dílčích technik. Může to znít banálně, ale velmi často stačí škodlivé programy pojmenovat nějakým důvěryhodným jménem, nebo pouze jedním znakem, kdy takovýto soubor často unikne pozornosti administrátora. Škodlivé soubory jsou často umísťovány do složek, které se příliš nepoužívají. Další běžnou a podstatnou součástí krytí stop je vymazání logů, které po sobě útočník zanechal. Na kritických systémech je proto více než žádoucí logy okamžitě odesílat na externí úložiště a do SIEM systému.

7 Security Information and Event Management

Technologie SIEM, celým názvem pak Security Information and Event Management, nabízí monitorování, ukládání a správu bezpečnostních událostí reprezentovaných logovacími záznamy, které jsou sbírány z definovaných zařízení nacházejících se v IT infrastruktuře. Pomocí analytických funkcí dokáže SIEM identifikovat bezpečnostní hrozby, které se mohou stát podkladem pro bezpečnostní incidenty. Grafické rozhraní SIEM umožňuje na jednom místě vyhodnocovat události z mnoha heterogenních zdrojů, mezi které můžeme zařadit operační, databázové, aplikační i síťové systémy a zařízení. Produkty SIEM obsahují také archivační moduly, které lze využít pro ukládání sesbíraných logů pro účely forenzní analýzy. Moderní produkty SIEM navíc dokáží sesbíraná data obohacovat o informace vytvářené profesionálními dohledovými týmy nepřetržitě analyzujícími bezpečnostní situaci ve všech částech planety [14].

Úspěšné nasazení SIEM technologie je podmíněno detailní analýzou prostředí a byznysu společnosti. Hodnota SIEM systému pro společnost závisí především na jeho správné a odpovídající implementaci. Před nasazením technologie SIEM je potřeba zodpovědět několik zásadních otázek, jejichž zodpovězení pomůže s výběrem vhodného řešení SIEM pro skutečné účely té které organizace. Jsou to zejména následující.

Jaké logy a jaké jejich množství bude zpracováváno?

Hodnota EPS (Events per Second) je velmi důležitý údaj, podle kterého dochází k dimenzování celého řešení. Většina dodavatelů SIEM technologií naceňuje své produkty pro zákazníka pomocí licencí, které jsou prodávány právě pro určité EPS, které bude systém zpracovávat. Jedná se tedy o navýšení operačních nákladů OPEX. Je proto potřeba definovat a spočítat, která zařízení budou logy zasílat, jaký typ logů, jejich množství a velikost. Hodnoty EPS je potřeba určit jak průměrné, například za jeden den, tak i ve špičkách.

Jak dlouho musí být logy archivovány?

Toto téma přináší otázky týkající se doby uchovávání dat a jejich destrukce. Právní nebo průmyslové regulace můžou vyžadovat uchování jistých typů dat po určitou časovou

periodu (Data Retention). Také zde můžou být právní či funkční směrnice, jakým způsobem se mají data po uplynutí dané periody likvidovat (Data Destruction) [15].

Je požadovaná redundance systému?

Nasazení jakékoli technologie v tzv. režimu vysoké dostupnosti HA (High Availability) s sebou přináší často až dvojnásobné vstupní kapitálové náklady CAPEX a samozřejmě i navýšení operačních OPEX nákladů.

Řešení SIEM se skládá z několika logických a funkčních komponent, které jsou ve vzájemném vztahu a interakci. Výčet níže není určitě kompletní, zároveň ne všechny komponenty jsou obsaženy ve všech řešeních poskytovaných níže uvedenými, ale i jinými výrobci. Při výběru SIEM systému je potřeba zhodnotit, které komponenty jsou žádoucí a které nikoli. Od složitosti použitého řešení se samozřejmě odvíjí také cena. Základními komponentami většiny SIEM systémů určených pro malé a střední podniky by měly být Log management a Korelace událostí [16].

7.1 Log management

Log management je první a klíčovou součástí jakéhokoli SIEM řešení. Pokud nejsou sbírány alespoň některé události, které jsou v síti produkovány, není samozřejmě možné z těchto událostí získat jakoukoli informaci, a tedy se pravděpodobně nedosáhne ani řádného řízení informační bezpečnosti, bez kterého nebudou naplněny potřebné funkcionality SIEM systému. Log management, při použití jednoduché analogie, si lze představit jako velké úložiště, kde se ukládají informace o událostech, které se dějí na síti. I bez jakékoli další přidané funkční hodnoty pro správu a ukládání událostí je zde možnost alespoň procházet data zpátky v čase.

Události se v Log managementu vyskytují jako jednotlivé logy s pevně danou strukturou. Formátů logů je velké množství, k těm nejpoužívanějším patří například Syslog, CLF (Common Log Format) a v prostředí SIEM technologie ArcSight od společnosti Micro Focus, která je představena v této diplomové práci a implementována v její praktické části, je to proprietální formát CEF (Common Event Format). Tento formát je normalizovaný,

což znamená, že původní logy generované jednotlivými zařízeními a aplikacemi v síti jsou syntakticky analyzovány (Parsing) specializovaným softwarem tak, aby měly jednotnou, předem definovanou strukturu s příslušnými hlavičkami. V prostředí SIEM ArcSight se tento software, který může být zakoupen i jako specializovaná hardwarová appliance, nazývá ArcSight konektor (ArcSight Connector). Jeho popis, nastavení a taktéž strukturu CEF logů popíši v praktické části této diplomové práce.

7.2 Korelace událostí

Mít k dispozici množství logů je určitě nezbytné pro dohledání například průchozího provozu na firewallu, který porušuje vnitřní nastavení bezpečnostních politik. Obráceně k tomuto příkladu lze takto také potvrdit, že nebyly příslušné politiky porušeny. K získání mnohem vetší informační hodnoty je však nezbytné jednotlivé události dávat do vzájemného vztahu – korelovat je. Přidržíme-li se příkladu s provozem, který je logován firewallem, jednotlivá událost sama o sobě nemusí znamenat nic závažného, ale ve spojení s událostmi generovanými například směrovačem, databázovým serverem nebo IPS/IDS systémem, ta samá událost získá jiný význam a může se ukázat, že se jedná například o útok na zranitelný systém. Korelace může být tedy definována jako nalezení vztahů mezi dvěma nebo více vstupními logy. Nejběžnější formou korelace je korelace založená na pravidlech (Rule-Based Correlation), která porovnává několik logů z jednoho zdroje, nebo porovnává hodnoty některých logovaných veličit z více zdrojů, jako jsou časové značky, IP adresy a typy událostí. Korelaci událostí lze provádět i jiným způsobem, a to statistickými metodami (Statistical Methods), nebo vizualizačními nástroji (Visualization Tools). Pokud je korelace prováděna pomocí automatizovaných metod, obecně je pak výsledkem korelace nový log, který spojuje vstupní informace do jednoho místa, logovaného záznamu. V závislosti na povaze těchto informací může pak infrastruktura vygenerovat varování (Alert), který informuje o potřebě další investigace [17].

7.3 Přední dodavatelé SIEM systémů

Na trhu působí v současné době velké množství dodavatelů systémů SIEM. Pro zhodnocení jednotlivých produktů je vhodné vycházet z veřejně dostupných analýz společností, které

dlouhodobě vývoj tohoto trhu sledují. Na obrázku níže je znázorněn tzv. magický kvadrant pro Security Information and Event Management systémy pro rok 2016 od společnosti Gartner, Inc. Tato americká společnost zabývající se výzkumem a poradenstvím v oblasti ICT je nepopiratelnou autoritou v hodnocení nejen SIEM systémů.

Obr.9: Magický kvadrant pro SIEM technologie pro rok 2016, Zdroj: [7]

Dlouhodobě se na předních místech umisťují a největší progresi mají produkty IBM QRadar, Splunk Enterprise Security, LogRhythm SIEM a HPE ArcSight (nyní vlastněno společností Micro Focus). Krátce zde budou některé společnosti a jejich produkty představeny.

IBM QRadar

Společnost IBM získala technologii QRadar pod svou ochrannou známku v rámci akvizice společnosti Q1 Labs. v roce 2011. Společnost Q1 Labs. byla primárně zaměřena na vývoj technologií určených k monitoringu, sběru a vyhodnocování bezpečnostních událostí. Cena této akvizice nebyla zveřejněna, ale v době nákupu měla společnost Q1 Labs. globálně přes 1800 klientů v různých průmyslových odvětvích, včetně veřejně obchodovatelných společností, finančních institucí, maloobchodní organizace, zdravotnická zařízení, výrobní a dopraví společnosti, vzdělávací instituce, federální, státní a místní vládní instituce. Q1

Labs. měla také strategické partnerství se společnostmi Juniper Networks, Enterasys, Nortel, McAfee, Foundry Networks a 3Com [18]. Společnost Q1 Labs. uvedla svůj SIEM produkt na trh v roce 2001 jako plnohodnotnou produktovou řadu. Technologie je nabízena jako softwarová i hardwarová appliance s možností instalace na vlastní hardware.

Splunk Enterprise Security

Splunk Enterprise Security je softwarový produkt společnosti Splunk Inc., která byla založena v roce 2003. Produkt je určen pro sběr a analýzu tzv. strojových dat (tj. dat generovaných v textové podobě nejrůznějšími systémy - serverové logy, aplikační logy, konfigurační soubory, webové logy, logy sociálních sítí, data z výrobních linek, seizmologických přístrojů apod.) [19]. Řešení Splunk dělá ale něco odlišného, než ostatní SIEM nástroje. Efektivně zachycuje a analyzuje masivní množství nestrukturovaných, textových a časově závislých dat [20]. Jedná se tedy o nástroj řadící se do oblasti zpracování tzv. big data, a to ne nutně pouze z oblasti informační bezpečnosti.

LogRhythm

Společnost LogRhythm založená v roce 2003 ve Spojených státech amerických, lídr v oblasti zprávy životního cyklu hrozeb (Threat Lifecycle Management), umožňuje organizacím po celém světě rychle rozpoznat, reagovat a neutralizovat škodlivé kybernetické hrozby. Společností patentovaná a ceněná platforma LogRhythm sjednocuje SIEM příští generace (Next-Generation SIEM), Log management, monitorování sítí a sledování koncových bodů, analyzátory chování uživatelských entit, automatizaci bezpečnosti a pokročilou bezpečnostní analýzu. Společnost LogRhythm je mimo získání mnoha průmyslových ocenění také situována stabilně v popředí v magickém kvadrantu hodnotící SIEM systémy společností Gartner, získala SC Labs ocenění pro SIEM a UTM systémy pro rok 2017 a umístila se na první pozici v kategorii Best SIEM v soutěži Best of 2016 Awards pořádané společností SANS Institute [21].

Micro Focus ArcSight

Společnost ArcSight byla založena v roce 2000 ve Spojených státech amerických a poskytovala řadu produktů v oblasti SIEM řešení, umožňující sledovat události týkající se

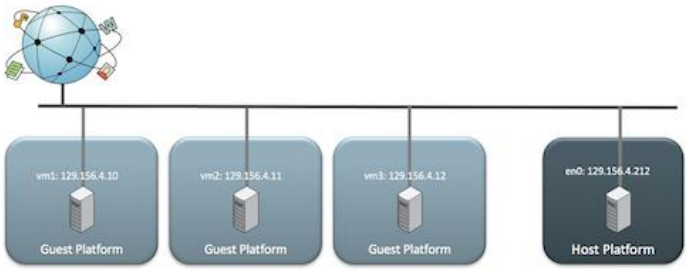
informačních asetů a zjišťování, zda byla porušena nastavená pravidla nebo došlo k zneužití systému samotných, a to jak aktéry ve vnitřní síti (Insiders), tak i ve vnější síti (Outsiders) [22]. ArcSight je navržen tak, aby umožňoval zákazníkům identifikovat a upřednostňovat bezpečnostní hrozby, organizovat a sledovat činnosti spojené s reakcí na bezpečnostní incidenty a zjednodušovat audity a činnosti související s dodržováním předpisů. Společnost ArcSight se stala dceřinnou společností společnosti Hawlett-Packard v roce 2010, a to za akvizici 1,5 miliardy amerických dolarů [23]. V průběhu tvorby této diplomové práce byla divize HPE, pod níž spadal i produkt ArcSight, koupena společností Micro Focus.

8 Případová studie

Případová studie této diplomové práce se zabývá instalací, kompilací a zprovozněním telefonní ústředny Asterisk, dvou VoIP telefonů, systému Micro Focus ArcSight ESM, jednoho konektoru Micro Focus ArcSight, dvou hostitelských PC určených pro virtualizaci výše zmíněných komponent a k provádění penetračních testů, dále pak jednoho PC určeného ke správě a k přístupu k ostatním zařízením. Detailní popis a konfigurace jednotlivých systémů je popsána v následujících kapitolách. Po instalaci všech potřebných komponent a programového vybavení jsem navrhl a realizoval možné scénáře útoků a na základě nich vytvořil konfiguraci zvoleného SIEM systému tak, aby tyto útoky odhalil.

9 Instalace a konfigurace jednotlivých prvků

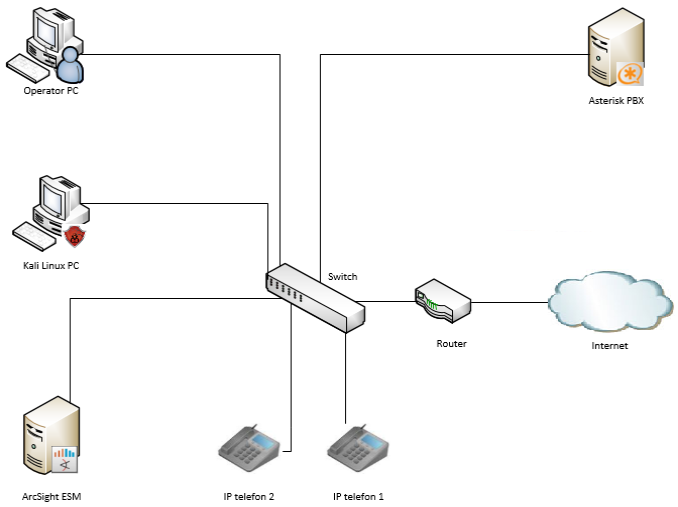
Všechny hostitelské systémy (Host Platforms) byly standardními laptopy s 64 bitovým operačním systémem Windows 7 Enterprise a 4GB operační paměti. Virtuální stroje (Guest Platforms) budou blíže popsány níže. Bylo nutné nastavit IP adresy fyzických i virtuálních rozhraní z rozsahu, který poskytuje ISP směrovač, a to 192.168.1.0/24. Samotný směrovač byl pak samozřejmě použit jako výchozí brána (Default Gateway) s IP adresou 192.168.1.1. Nevyužil jsem možnosti automatického získávání IP adres pomocí DHCP serveru běžícího na směrovači, a to z důvodu, abych měl po celou dobu práce na jednotlivých systémech stále ty samé IP adresy a bylo tak snazší identifikovat zdroje a cíle komunikace v záznamech na straně ArcSight ESM. Pro virtualizaci jsem použil volně dostupný nástroj Oracle VM VirtualBox. V síti jsem se rozhodl postavit virtuální stroje do stejné pozice jako hostitelské systémy, tedy bez využití překladu adres NAT. To znamená, že se virtuální stroje nacházely fyzicky na stejném ethernetovém segmentu a měly tedy přiděleny IP adresy ze stejného rozsahu jako hostitelské systémy. Pro tento účel nabízí Oracle VM VirtualBox nastavení síťového adaptéru do tzv. Bridge Mode. Logickou topologii pro tuto konfiguraci si lze představit následovně:



Obr.10: Logická topologie pro Bridge Mode, Zdroj: [37]

Pro práci s konfiguračními soubory na jednotlivých systémech jsem používal textový editor Vim. Pro vzdálenou správu jsem používal program PuTTY. V neposlední řadě jsem potřeboval mezi jednotlivými systémy přenášet soubory, k tomuto účelu mi posloužil nástroj WinSCP.

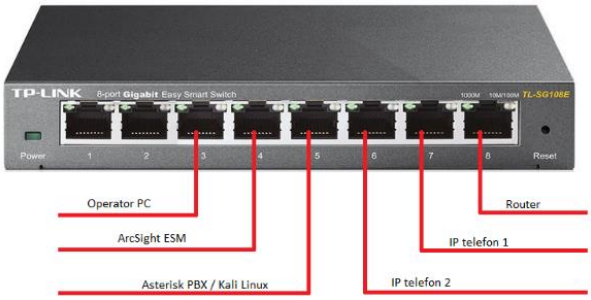
Logická topologie laboratorní sítě byla následující (vytvořeno pomocí programu Microsoft Visual Studio).



Obr.11: Logická topologie laboratorní sítě

9.1 Switch TP-Link TL-SG108E

Za ústřední prvek sítě jsem zvolil Switch TP-Link TL-SG108E. Jedná se o jednoduché, levné a lehce konfigurovatelné zařízení plnící základní funkce L2 přepínače. Tento přepínač má k dispozici 8 ethernetových portů pracujících na 10/100/1000 Mbit/s určených pro koncovku RJ45. U dnešních zařízení je prakticky standardem funkce Auto MDI / MDI-X, která zajišťuje možnost použití jak kříženého kabelu (Crossover Cable), tak i přímého kabelu (Straight Cable) nezávisle na připojených zařízeních. Další standardní funkcí těchto přepínačů je automatické vyjednávání parametrů na fyzické vrstvě, jako jsou rychlost a duplex. K přepínači se lze připojit přes kterýkoli ethernetový port na adrese 192.168.0.1 pomocí webového rozhraní. Přepínač nenabízí žádné bezpečnostní funkce kromě možnosti zvolení silného hesla. Přepínač jsem nastavil a jednotlivá zařízení zapojil následujícím způsobem.



Obr.12: Fyzické zapojení jednotlivých portů

9.2 Kali Linux

Tento systém jsem využil pro provádění jednotlivých testů a útoků. Kali Linux je linuxová distribuce odvozená od distribuce Debian, navržená pro digitální forenzní analýzu a penetrační testy. Je plně kompatibilní s vývojovou platformou Debianu, čemuž mimo jiné odpovídá i plná synchronizace s příslušnými Debian aktualizačními repozitáři. Distribuce je určena pro potřebu bezpečnostních testů v prostředí organizací [24]. Z domovských stránek této distribuce jsem stáhl ISO obraz Kali-linux-2018.3a-amd64.iso (dostupný na přiloženém CD). Nástroj Oracle VM VirtualBox poměrně jednoduše provede celou instalací. Nastavení parametrů síťového rozhraní se provádí editací konfiguračního souboru **/etc/network/interfaces**. Soubor **interfaces** byl obohacen o záznamy níže, definující statické nastavení pro rozhraní eth0:

```
auto eth0
iface eth0 inet static
    address 192.168.1.38
    netmask 255.255.255.0
    gateway 192.168.1.1
```

Nastavení DNS serveru proběhlo editací souboru **/etc/resolv.conf**.

```
#Generated by NetworkManager
search local.ltd
nameserver 192.168.1.1
```

Kali Linux nabízí množství nástrojů pro forenzní analýzu a penetrační testování. Pro aktualizaci stávajících balíků (Packages) obsahujících softwarové nástroje a instalaci nových balíků je potřeba systému sdělit, kde jsou jejich zdroje (Repositories). Nastavení se provádí editací souboru **sources.list** nacházejícího se v adresáři **/etc/apt/**.

Soubor **sources.list** musí obsahovat minimálně tyto položky:

```
deb http://http.kali.org/kali kali-rolling main non-free contrib
deb-src http://http.kali.org/kali kali-rolling main non-free contrib
```

Pro aktualizaci stávajících balíků a porovnání jejich verzí:

```
root@kali:/etc/apt/#apt-get update
```

Pro stažení nových verzí balíků:

```
root@kali:/etc/apt/#apt-get upgrade
```

Pro vzdálený přístup k ústředně bylo potřeba nainstalovat SSH server:

```
root@kali:~#/apt-get install openssh-server
```

Povolení služby SSH jako permanentní pomocí konfiguračního souboru **ssh.service**:

```
root@kali:~#/ systemctl enable ssh.service
```

Spuštění služby SSH bez nutnosti restartu systému:

```
root@kali:~#/ systemctl start ssh.service
```

Povolení přihlášení uživatele root pomocí SSH lze nastavit v konfiguračním souboru **/etc/ssh/sshd_config**, a to přidáním řádku s textem **PermitRootogin yes**.

Po těchto změnách bylo potřeba službu SSH restartovat.

```
root@kali:~#systemctl restart sshd
```

Ve výchozím nastavení server naslouchá na portu 22. To, že služba na daném portu skutečně naslouchá, lze ověřit následovně.

```
root@kali:~# netstat -nao | grep :22
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      off (0.00/0/0)
```

Systému jsem nastavil čas pomocí protokolu NTP. Nastavení správného času je nezbytné pro správnou korelaci událostí na straně ArcSight ESM. Zpočátku sytém SIEM upozorňoval na nesprávné nastavení času, jak bude ukázáno v kapitole 9.5.3. ArcSight ESM Console. Díky použití NTP protokolu se systémový čas získává pomocí synchronizace s NTP servery v Internetu. Instalace NTP proběhla následovně.

```
root@kali:~#aptitude install ntp
```

Časovou zónu jsem nastavil jako Europe/Prague v grafickém rozhraní pomocí příkazu níže.

```
root@kali:~#dpkg-reconfigure tzdata
```

Restart služby ntp jsem provedl příkazem níže.

```
root@kali:~# sudo service ntp restart
```

Zobrazení použitých NTP serverů je níže.

```
root@kali:~#ntpq -p
remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 0.debian.pool.n .POOL.          16 p    -   64    0    0.000    0.000   0.000
 1.debian.pool.n .POOL.          16 p    -   64    0    0.000    0.000   0.000
 2.debian.pool.n .POOL.          16 p    -   64    0    0.000    0.000   0.000
```

9.3 Asterisk PBX

Asterisk je softwarová implementace pobočkové ústředny PBX (Private Branch eXchange). Umožňuje telefonním přístrojům vzájemně komunikovat a interagovat s množstvím

ostatních hardwarových technologií pro vytváření vzájemných telefonních hovorů, dále pak umožňuje připojení k telefonním službám, jako je PSTN (Public Switched Telephone Network) a VoIP (Voice over Internet Protocol). Asterisk byl vytvořen v roce 1999 Markem Spencerem ve společnosti Digium. Původně byl Asterisk určen pro operační systémy Linux, dnes je možné ho provozovat na velkém množství různých operační systémů [26]. Pro účely této diplomové práce jsem software pobočkové ústředny Asterisk nainstaloval jako službu na virtuálním stroji Linux v distribuci Debian 4.9.0-4-amd64 x86_64 (dostupná na přiloženém CD). Níže budou popsány ve stručnosti jednotlivé kroky, které bylo potřeba splnit pro úspěšnou instalaci.

Instalací operačního systému Linux opět přehledně provedl Oracle VM VirtualBox. Nastavení parametrů síťového rozhraní se provádí opět editací konfiguračního souboru**/etc/network/interfaces**. Soubor **interfaces** byl obohacen o záznamy níže, definující statické nastavení pro rozhraní enp0s3:

```
allow-hotplug enp0s3
iface enp0s3 inet static
   address 192.168.1.181
   netmask 255.255.255.0
   gateway 192.168.1.1
```

Nastavení DNS serveru proběhlo editací souboru **/etc/resolv.conf**:

```
domain home
search home
nameserver 192.168.1.1
```

Soubor **sources.list** již obsahoval potřebné záznamy a nebylo třeba ho aktualizovat tak, jak tomu bylo u systému Kali Linux.

Z domovských stránek produktu Asterisk jsem stáhl soubor asterisk-14-current.tar.gz (dostupný na přiloženém CD).

```
root@debian-asterisk/
```

```
->wget https://downloads.asterisk.org/pub/telephony/asterisk/asterisk-14-current.tar.gz
```

Stáhl jsem také knihovnu DAHDI (Digium Asterisk Hardware Device Interface). Knihovna DAHDI obsahuje množství ovladačů a nástrojů, díky nimž může Asterisk komunikovat kromě jiného s analogovými a digitálními telefony (dostupná na přiloženém CD).

```
root@debian-asterisk/
->wget https://downloads.asterisk.org/pub/telephony/dahdi-linux-complete/dahdi-linux-complete-current.tar.gz
```

Následně byly stažené soubory rozbaleny.

```
root@debian-asterisk~
->tar -zxvf https://downloads.asterisk.org/pub/telephony/asterisk/asterisk-14-current.tar.gz
->tar -zxvf https://downloads.asterisk.org/pub/telephony/dahdi-linux-complete/dahdi-linux-complete-current.tar.gz
```

Instalace knihovny DAHDI proběhla následovně:

```
root@debian-asterisk~/dahdi-linux-complete-2.11.1+2.11.1
->make
->make install
->make config
```

Kompilace a instalace pobočkové ústředny Asterisk měla několik fází. Nebudu zde popisovat všechny příkazy nutné k úspěšné instalaci, pouze zmíním nejdůležitější z nich a stručně popíši jednotlivé kroky instalace a kompilace. Příkazem **./configure** se spustí z adresáře, kde se nachází zdrojový kód ústředny, nezbytná kontrola systému na přítomnost všech softwarových komponent a závislostí potřebných pro správný běh ústředny. Kontrola neproběhla úspěšně a bylo tedy nutné doinstalovat potřebné balíky. Pro tento účel se v instalačním balíku nachází skript **instal_prereq**, jehož spuštěním dojde ke stažení všech potřebných prerekvizit.

```
root@debian-asterisk~/asterisk-13.18.2/contrib/scripts
-> ./install_prereq install
```

Příkazem **make menuselect** jsem otevřel grafické rozhraní, ve kterém jsem vybral všechny dostupné kategorie a pod ně spadající komponenty, které mají být kompilovány a instalovány. Samotná instalace proběhla následovně.

```
root@debian-asterisk~/asterisk-13.18.2/
->make
->make install
```

Instalace konfiguračních souborů pro Asterisk proběhla následovně.

```
root@debian-asterisk~/asterisk-13.18.2/
->make samples
```

Posledním krokem je instalace inicializačního skriptu **initscript**, který zajistí spuštění pobočkové ústředny při spuštění serveru.

```
root@debian-asterisk~/asterisk-13.18.2/
->make config
```

Běžící ústředna samozřejmě generuje množství logů ukládaných do souborů, a proto se doporučuje instalace skriptu **logrotation**, který zajistí jejich kompresi a rotaci.

```
root@debian-asterisk~/asterisk-13.18.2/
->make install-logrotate
```

Posledním krokem pak bylo zajištění, že se ústředna Asterisk spustí při nabootování systému.

```
root@debian-asterisk~
-> chkconfig asterisk on
```

Pro vzdálený přístup jsem naistaloval SSH server zcela analogicky k instalaci na sytému Kali Linux. Systémový čas jsem nastavil obdobným způsobem, jako pro systém Kali Linux.

9.3.1 SIP účty a volací plán

Nejdůležitějšími konfiguračními soubory ústředny jsou **/etc/asterisk/sip.conf** a **/etc/asterisk/extension.conf**. Konfigurační soubor **sip.conf** obsahuje jednotlivé konfigurace všech k ústředně připojených harwarových či softwarových telefonů, které využívaji protokol SIP. Konfigurační soubor **extension.conf** obsahuje číslovací plán ústředny. Pojem **extension** lze chápat jako přípojku k zařízení. Soubor **sip.conf** je rozdělen do dvou sekcí, a to na sekci **[general]**, kde se definují parametry platné pro všechny SIP účty, a to potud, pokud není v sekci daného účtu řečeno jinak. Dalšími sekcemi jsou sekce definující parametry pro jednotlivé SIP účty. Konkrétní nastavení vypadalo následovně.

[general]

context=default ; určuje kontext, kam budou jednotlivé hovory umísťovány. Kontext může být určen v sekcích pro jednotlivé SIP účty zvlášť (kontext se nastavuje v konfiguračním souboru extension.conf).

useragent=Asterisk PBX 13.18.2 ; hodnota, která je součástí SIP hlavičky

bindaddr=0.0.0.0 ; adresa, na které server naslouchá. Adresa 0.0.0.0 znamená, že server naslouchá na všech dostupných adresách.

tcpenable=yes ; povolení protokolu TCP (ve výchozím nastavení protokol UDP). V případě použití enkrypce protokolem TLS služba automaticky běží na portu 5061/tcp.

bindport=5060 ; číslo portu, na kterém server naslouchá, ve výchozím nastavení je to port 5060 (RFC3261)

alwaysautreject=no; ústředna v odpovědi poskytuje informaci, zda došlo ke špatné autentizaci pro platný SIP účet

allow=ulaw ; nastavení použitého kodeku na G.711 μ-law

Účty SIP byly nastaveny pro dva hardwarové telefony, a to telefon Cisco SPA504G a telefon Cisco SPA962.

[100]; název SIP účtu pro telefon SPA504G

type=friend ; určuje vztah mezi ústřednou a klientem. Volba friend zajistí, že může klient hovory od ústředny jak přijímat, tak je i inicializovat.

callerid= SPA504G <100>; hodnota, která se bude zobrazovat volajícímu při volání z této klapky

username= SPA504G; toto pole je použito ústřednou Asterisk pro autentizaci vzdáleného SIP klienta při zpracovávání zprávy SIP INVITE

secret=100 ; heslo SIP účtu

host=dynamic ; povoluje registraci na všech IP adresách

insecure=invite,port ; zařízení a aplikace často generují zdrojový port náhodně. Volbou port zajistím, že ústředna přijme požadavek i z jiného portu než 5060.

qualify=yes ; ústředna periodicky zasílá SIP NOTIFY zprávu pro ověření dostupnosti vzdáleného zařízení a měří latenci jeho odpovědi

context=default; hovory z této klapky budou patřit do kontextu default v konfiguračním souboru extension.conf

[200]; název SIP účtu pro telefon 10SPA962

type=friend

callerid= 10SPA962<200>

username=10SPA962

secret=200

host=dynamic

insecure=invite,port

qualify=yes

context=default

Jak bylo řečeno výše, číslovací plán je dán souborem **/etc/asterisk/extensions.conf**. Tento soubor se dá bez nadsázky považovat za centrum ústředny Asterisk, jelikož zde jsou nadefinována všechna spojení a způsob, jak s nimi ústředna nakládá. Níže je vidět, jak jsem nadefinoval v souboru **extensions.conf** kontext **default**. Uvedené záznamy ústřednu instruují tak, že je-li volána klapka 100, hovor je spojen na telefon SPA540G a při volání klapky 200 je hovor spojen na telefon 10SPA962.

```
[default]
exten => 100,1,Dial(SIP/SPA504G)
exten => 200,1,Dial(SIP/10SPA962)
```

Do konzole ústředny Asterisk se lze dostat příkazem **asterisk –rvvvvv**, v tomto případě pak se zapnutím verbozity. V konzoli je pak potřeba zavést změny provedené v konfiguračních souborech pomocí příkazů níže.

```
debian-asterisk*CLI> sip reload
debian-asterisk*CLI> dialplan reload
```

9.3.2 Logování

Pro logování jsem zvolil samozřejmě standard protokolu syslog (RFC5424), který je základním logovacím formátem nainstalovaného virtuálního operačním systému Linux. Syslog je protokol typu klient/server, kdy na serveru je nainstalován tzv. syslog démon poskytující sběr, filtrování a ukládání systémových a aplikačních událostí. Výchozím portem prokolu syslog je port číslo 514. Logování jsem musel zprovoznit na dvou úrovních, a to na úrovni samotné ústředny Asterisk a pak na úrovni operačního systému Linux Debian.

Nejdříve jsem nastavil logování na samotném operačním systému Linux. Jak už bylo řečeno výše, o logování se stará tzv. syslog démon. Ten sbírá příchozí zprávy a na základě nastavení konfiguračního souboru **/etc/rsyslog.conf** tyto zprávy filtruje a ukládá do příslušných souborů. Každá zpráva kromě vlastního textu obsahuje dva atributy, a to prioritu (Priorities) a kategorii (Facilities). Priorita říká, jak je daná zpráva významná. Atribut kategorie říká, jaké oblasti se zpráva týká nebo od jaké služby pochází. Záznamy v konfiguračním souboru **rsyslog.conf** mají tvar **{kategorie.[!=]priorita -místo_určení}**. Tedy například záznam **auth,authpriv.* -/var/log/auth.log** říká, že všechny zprávy týkající se autentizace s jakoukoli jejich prioritou (hvězdička zde plní roli zástupného znaku) budou uloženy do souboru **auth.log**. V tomto ohledu jsem prošel nastavení konfiguračního souboru. Přidal jsem záznam ***.* @@192.168.1.50:10514**, čímž syslog démonu sděluji, aby posílal všechny zprávy všech kategorií a priorit na vzdálený

server 192.168.1.50 na port 10514, což je samozřejmě zařízení ArcSight Smart Connector, které bude blíže popsáno níže.

Výše popsaná konfigurace však nepokrývá všechny možnosti logování na systémech Linux. Výborným rozšířením logovacích možností je využití tzv. auditování. Pomocí audit démona lze sledovat např. bezpečnostní události a informace a na základě předdefinovaných pravidel generovat potřebné logy. Auditování nečiní systém zabezpečenějším, ale spíše umožňuje nalezení porušení zásad jeho zabezpečení. Program **Auditd** jsem jednoduše nainstaloval následovně.

```
root@debian-asterisk~
->apt-get install auditd audispd-plugins
```

Od společni Micro Focus jsem získal jimi doporučená auditní pravidla pro systémy Linux. Tento soubor s názvem **arcsight.rules** je k nalezení na přiloženém CD. Pro představu je níže uvedeno jedno takové pravidlo pro generování logu při změně hesla.

```
-a always,exit -F path=/usr/bin/passwd -F perm=x -F auid>=500 -F auid!=4294967295
-k privileged
```

Všechna pravidla obsažená v souboru **arcsight.rules** jsem překopíroval do konfiguračního souboru auditních pravidel **/etc/audit/audit.rules**, kde se již nacházelo velké množství pravidel z výchozí konfigurace. V neposlední řadě jsem musel audit démona instruovat k přeposílání logů na syslog démona. Toto jsem provedl úpravou konfiguračního souboru **/etc/audisp/plugins.d/syslog.conf**, kde bylo třeba tuto funkci učinit aktivní pomocí volby **active=yes**.

Restart služeb **rsyslog** a **auditd**.

```
root@debian-asterisk~
-> service rsyslog restart
-> service auditd restart
```

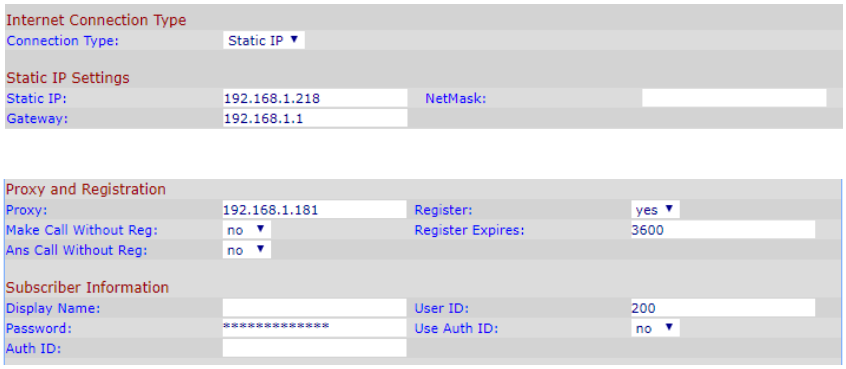
Pro logování událostí před spuštěním služby **auditd** jsem do konfiguračního souboru **/etc/grub.conf** přidal záznam **audit=1**. Posledním krokem pak bylo zajištění, že se audit démon spustí při startu systému.

```
root@debian-asterisk~
-> chkconfig auditd on
```

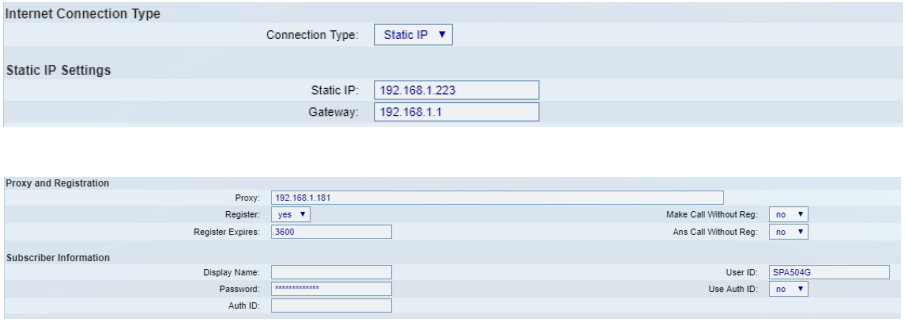
Dále bylo potřeba logovat události generované ústřednou Asterisk a přeposílat je přímo již spuštěnému syslog démonu. Možnosti logování ústředny Asterisk se nastavují v konfiguračním souboru **/etc/asterisk/logger.conf**. Jednotlivé záznamy mají formát **{název_souboru=>úroveň}**. Název souboru je samozřejmě umístění logů, úrovně pak popisují typy zpráv, které se do daného umístění mají přeposílat. Pro nastavení přeposílání prakticky všech úrovní logů na syslog démona jsem použil záznam **syslog.local0 => notice,warning,error,security,verbose,dtmf,fax**. Po těchto konfiguračních zásazích bylo potřeba restartovat službu Asterisk skrze její CLI, a to příkazem **core restart now**.

9.4 Cisco SPA504G a Cisco 10SPA962

V laboratorní síti byly zapojeny dva hardwarové telefony od společnosti Cisco. Telefon Cisco SPA504G jsem nastavoval podle jeho technické dokumentace [27]. Telefon Cisco SPA962 jsem nastavoval obdobně také podle jeho technické dokumentace [28]. Oba telefony lze ovládat buď tlačítkovou volbou přímo na těle každého z nich, nebo pak přes webové rozhraní. Oba telefony jsem resetoval tzv. factory reset, čímž se spustilo jejich tovární nastavení. Telefony jsem nejdříve tlačítkovou volbou nastavil na získání adresy pomocí DHCP, poté jsem se k nim připojil přes webové rozhraní a pokračoval v konfiguraci. U obou telefonů jsem nastavil statickou IP adresu, proxy server a příslušné jméno a heslo použité v souboru **sip.conf**. Konkrétní konfigurace pro oba telefony je zobrazena na následujících dvou obrázcích.



Obr.13: Nastavení telefonu Cisco 10SPA962



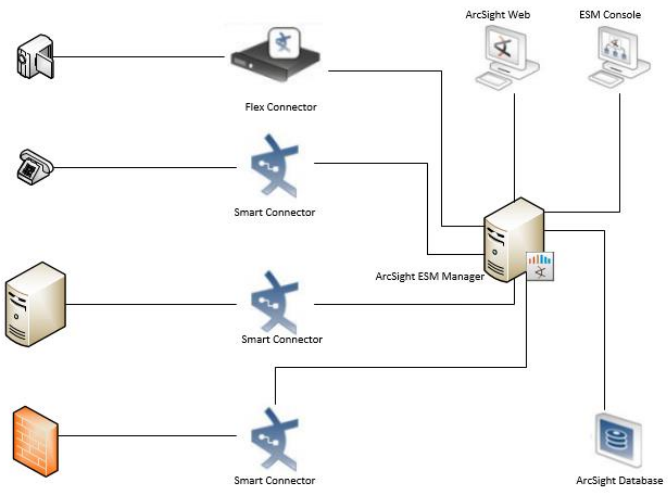
Obr.14: Nastavení telefonu Cisco SPA504G

Dostupnost obou telefonů a jejich správnou komunikaci jsem nejdříve ověřil přes konzoli ústředny Asterisk a posléze i úspěšně provedenými hovory.

```
debian-asterisk*CLI> sip show peers
Name/username  Host            Dyn Forcerport Comedia ACL Port  Status
Description
10SPA962/200   192.168.1.218 D  Yes Yes        5060 OK (20 ms)
SPA504G/100    192.168.1.223 D  Yes Yes        5060 OK (16 ms)
2 sip peers [Monitored: 2 online, 0 offline Unmonitored: 0 online, 0 offline]
```

9.5 Micro Focus ArcSight

Nejdříve je potřeba si říci, jaký je účel jednotlivých prvků při nasazení technologie Micro Focus ArcSight a způsob jejich komunikace. Typická topologie je zobrazena níže.



Obr.15: Typická architektura při použití technologie Micro Focus ArcSight

Ústředním prvkem technologie Micro Focus ArcSight je ArcSight ESM Manager. Tato hardwarové či softwarová applience tvoří jádro celého SIEM systému. Slouží k vyhodnocování událostí, jejich korelaci, zobrazování, k reportování, k vytváření automatických akcí, ke komunikaci se systémy třetích stran, k automatizaci pracovních postupů a mnoha dalším.

Po levé straně topologie na obr.13 se nacházejí jednotlivé síťové prvky, které generují události. Tyto události jsou zasílány na tzv. konektory. Konektory slouží ke sběru a sjednocení formátu událostí na ně přicházejících. Události se v log managementu vyskytují jako jednotlivé logy s pevně danou strukturou. Formátů logů je velké množství, k těm nejpoužívanějším patří například syslog, CLF (Common Log Format) a v prostředí SIEM technologie ArcSight od společnosti Micro Focus je to proprietální formát CEF (Common Event Format). Tento formát je normalizovaný, což znamená, že původní logy generované jednotlivými zařízeními a aplikacemi v síti jsou syntakticky analyzovány specializovaným softwarem na konektorech tak, aby měly jednotnou strukturu a hlavičky. CEF využívá transportního mechanismu protokolu syslog. Skládá se ze syslog předpony, záhlaví a množství rozšíření, jak je zobrazeno na příkladu níže [29]. Možných polí pro rozšíření je více než 400.

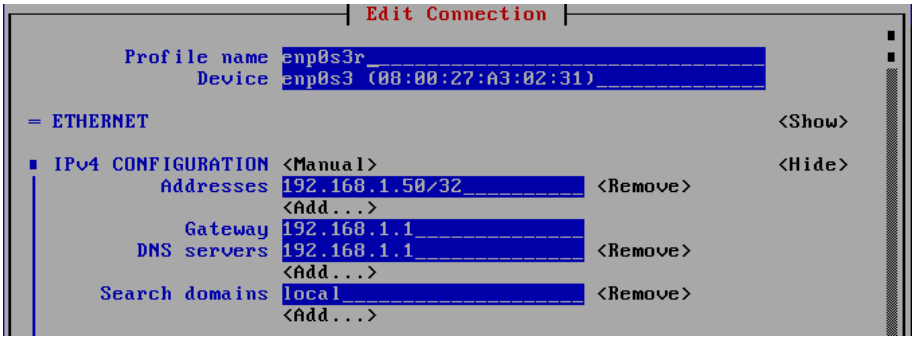
Jan 18 11:07:53 host CEF:Version|Device Vendor|Device Product|Device Version|Device Event Class ID|Name|Severity|[Extension]

Konektory se vyskytují ve dvou typech. Prvním z nich je tzv. Smart Connector. Smart Connector plní své funkce předdefinovaným způsobem pro více či méně známé formáty logů a jednotlivé výrobce IT technologií. V současné době jsou k dispozici desítky takto předdefinovaných konektorů. Druhým typem konektoru je tzv. Flex Connector. Tento typ konektoru, jak už vyplývá z jeho názvu, má obrovskou flexibilitu a může být konfigurován ke zpracovávání prakticky jakýchkoli textových řetězců. Samozřejmě je konfigurace takového konektoru mnohonásobně obtížnější než Smart Connectoru. V této diplomové práci byl použit jeden Smart Connector, jelikož jsem v síti generoval logy ve formátu syslog. Jednotlivé logy jsou ukládány a vyčítány z ArcSight Database.Množství generovaných a především zpracovávaných logů v rámci této diplomové práce nevyžadovalo instalaci a konfiguraci externího úložiště.

Ke správě ArcSight ESM Manageru slouží primárně tzv. ArcSight ESM Console. Jedná se o Java aplikaci pro vzdálený přístup a management. Další možností jak přistupovat k ArcSight ESM je použití webového rozhraní. Tento způsob však zdaleka nenabízí plné využití konfiguračních možností systému.

9.5.1 ArcSight ESM

Pro instalaci Arcsight ESM jsem musel nejdříve opět nainstalovat virtualizovaný stroj, na kterém byl ArcSight ESM nainstalován. V tomto případě ISO obraz operačního systému Linux 3.10.0-514.e17.x86_64 (distribuce CentosOS), který jsem stáhl z domovských stránek této distribuce (dostupný na přiloženém CD). Nástroj Oracle VM VirtualBox mě opět úspěšně provedl celou instalací. Nastavení síťového rozhraní jsem tentokrát provedl pomocí nástroje **nmtui**, které nabízí grafické rozhraní. Síťové parametry rozhraní včetně DNS jsem nastavil následovně.



Obr.16: Nastavení síťového rozhraní na CentosOS

Pro vzdálený přístup jsem naistaloval SSH server obdobně, jako na sytému Kali Linux. Významnou změnou zde bylo použití rozdílných příkazů z důvodu rozdílné distribuce operačního systému. Asi nejviditelnější změnou pak bylo použití příkazu **yum** namísto příkazů **apt-get** a **aptitude**. Systémový čas jsem nastavil také obdobným způsobem, jako pro systém Kali Linux. V případě operačního systému Centos jsem však musel dohledat konkrétní NTP servery pro příslušnou časovou zónu na stránkách **http://support.ntp.org**. Tyto servery jsem pak vložil do konfiguračního souboru **/etc/ntp.conf** ve formátu **server ntp_server_hostname_x iburst**. Z bezpečnostního hlediska je žádoucí v konfiguračním souboru **/etc/ntp.conf** ověřit a případně doplnit následující řádek **restrict default nomodify notrap nopeer noquery kod limited**. Tímto jsem zabránil zranitelnostem spojenými s dotazy **ntpq** a **ntpdc** a dotazy spojené s řízením serveru NTP.

Instalační soubor ArcSight ESM je dostupný na přiloženém CD. Instalace samotného ArcSight ESM byla poměrně složitá co se týče množství potřebných kroků, především z důvodu zapínání všech služeb potřebných pro správnou funkčnost. Následoval jsem instalačního průvodce, který je dostupný na přiloženém CD.

To, že jsou všechny nainstalované služby dostupné, lze ověřit příkazem níže.

[root@esm init.d]# /etc/init.d/arcsight_services status
Build versions:
esm:6.11.0.2339.0(BE2339)
storage:6.11.0.1887.0(BL1887)
process management:6.11.0-2149

```
      installer:6.11.0-2149
aps service is available
execprocsvc service is available
logger_httpd service is available
logger_servers service is available
logger_web service is available
manager service is available
mysqld service is available
postgresql service is available
```

9.5.2 ArcSight Smart Connector

Instalační soubor ArcSight ESM obsahuje instalační soubory jak pro Smart Connector, tak i Flex Connector. V zásadě bylo potřeba nejdříve nainstalovat tzv. core components (instalační soubor ArcSight-7.7.0.8044.0-Connector-Linux64.bin), což je v podstatě společné jádro pro všechny konektory, v jehož rámci se posléze instaluje konkrétní typ konektoru. Pro instalaci bylo potřeba vytvořit novou složku v adresáři **/opt/arcsight/SmartConnectors/Syslog** a instalaci provést z této nově vytvořené složky.

```
[root@esm SmartConnectors]$ mkdir Syslog
[root@esm SmartConnectors]$ cd Syslog/
[root@esm Syslog]$ /opt/arcsight/install/ArcSight-7.7.0.8044.0-Connector-Linux64.bin
```

Během instalace se zvolí adresář pro instalování **core components** a dále se postupuje podle pokynů zobrazených po úspěšné instalaci. Níže popisuji ty nejdůležitější kroky.

Instalace konkrétního typu Smart Connector měla dvě fáze, obě začínající spuštěním skriptu **runagentsetup.sh** z příslušného adresáře. Nejdříve bylo potřeba nastavit globální parametry a poté instalovat požadovaný konektor. Z globálních parametrů jsem využil možnosti vzdáleného přístupu na portu 9001 (výchozí nastavení), šifrování mezi konektorem a ArcSight ESM a preferování protokolu IPv4.

Z desítek možných konektorů jsem zvolil konektor typu syslog s názvem **Syslog Daemon**, což je typický název pro syslog server. Pro konektor jsem zvolil následující nastavení. Výchozí port 514 pro protokol syslog jsem z bezpečnostních důvodů změnil na 10514.

```
Network Port: 10514
IP Address: (ALL)
Protocol: UDP
Forwarder: false
Manager Hostname: esm.local
Manager Port: 8443
User: admin
Password: ********
Name[]: syslogTCP
```

Posledním krokem bylo zaregistrování a spuštění služby pod uživatelem **arcsight**.

```
[root@esm ~]# /home/arcsight/ArcSightSmartConnectors/current/bin/arcsight agentsvc -r -u arcsight
[root@esm ~]# /home/arcsight/ArcSightSmartConnectors/current/bin/arcsight agents
```

Ověření, že konektor naslouchá na portu 10514 a to, že přicházejí na tento port data, jsem provedl následujícím příkazem. Ve výpisu níže je samozřejmě také vidět, že je navázáno spojení na port 10514 z adresy 192.168.1.50, což je adresa systému Asterisk.

```
[root@esm ~]# netstat -nao | grep "10514"
tcp        0      0 0.0.0.0:10514           0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 192.168.1.50:10514      192.168.1.181:58162     ESTABLISHED off (0.00/0/0)
```

9.5.3 ArcSight ESM Console

ArcSight ESM Console slouží k přístupu přes GUI a ovládání ArcSight ESM. Doménové jméno ArcSight ESM jsem zvolil jako **esm.local**. Pro toto jméno samozřejmě neexistuje DNS A záznam s příslušnosu IP adresou 192.168.1.50 a bylo tedy třeba zajistit přeložení na

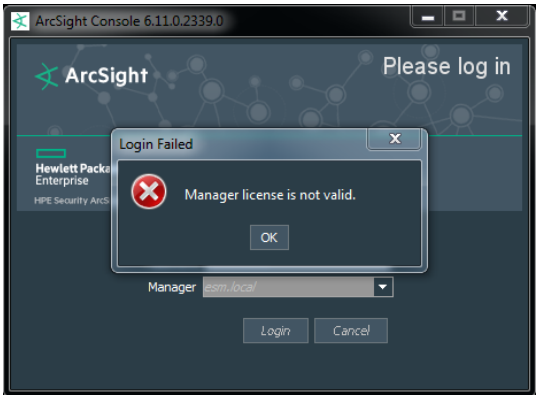
IP adresu lokálně. Tohoto lze docílit přidáním záznamu do souboru **C:\Windows\System32\drivers\etc\hosts**.

 # localhost name resolution is handled within DNS itself.

192.168.1.50 esm.local

ArcSight ESM Console je soubor typu **exe** s nutností instalace. Tato proběhla poměrně jednoduše v intuitivním grafickém rozhraní. Instalační soubor **ArcSight-7.0.0.2410.0-Console-Win.exe** je dostupný na přiloženém CD.

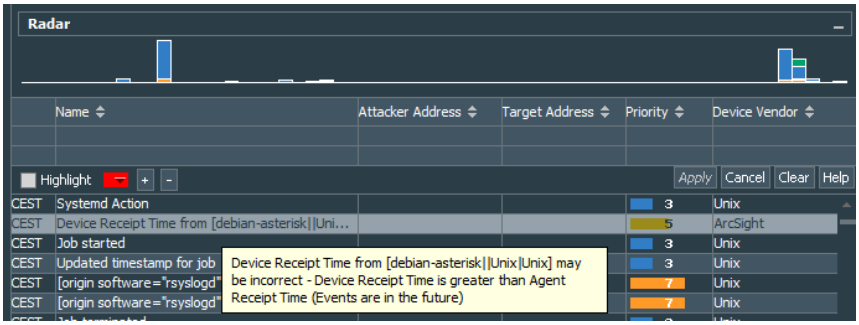
Při prvotním spuštění ArcSight ESM Console systém nahlásil chybu z důvodu neplatné licence pro ArcSight ESM Manager.



Obr.17: Chybějící licence pro ArcSight ESM

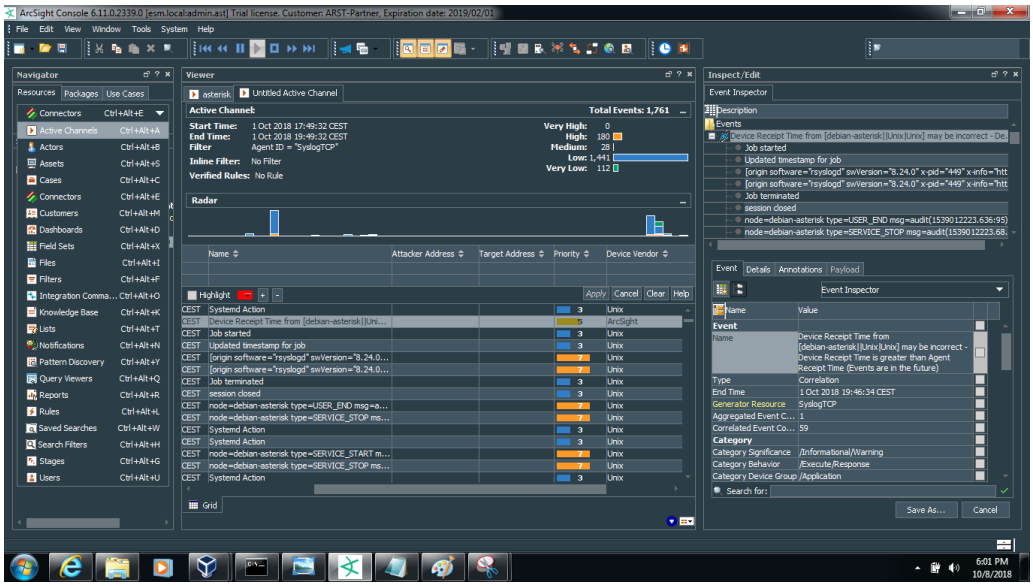
Platnou licenci **arcsight.lic** (dostupná na přiloženém CD) jsem nahrál do složky **[root@esm ~]$cd /opt/arcsight/install/**.

Po přihlášení do konsole byly události přicházející z ostatních systémů často doplněny o varování, že události přichází s budoucími časovými razítky v porovnání se systémovými časy ArcSight ESM. Níže je zobrazeno toto varování pro příchozí událost ze systému **[debian-asterisk]**. Správná časová korelace je nezbytná pro vyhodnocování událostí, a proto jsem musel na jednotlivých systémech nastavit časy prostřednictvím synchronizace s NTP servery v Internetu, jak jsem popsal v jednotlivých kapitolách popisující instalaci každého z nich.



Obr.18: Upozornění na chybné nastavení systémových časů

Popíši zde jednotlivé části grafického rozhraní tak, aby byl jasný jejich účel a možnosti použití v kapitolách popisující konkrétní konfiguraci obsahu. ArcSight ESM Console obsahuje tři základní panely, a to **Navigator**, **Viewer** a **Inspect/Edit**.



Obr.19: Grafické rozhraní ArcSight ESM Console

9.5.3.1 Navigator

Tento panel by se dal nazvat rozcestníkem ArcSight ESM Console. Tento panel umožňuje přístup ke všem zdrojům ArcSight ESM a umožňuje tak jejich správu. Níže popíši pouze ty zdroje, které budu využívat při konfiguraci.

Active Channels

Slouží k vytváření zobrazení, modifikaci a mazání bezpečnostních událostí přicházejících do systému. Umožňuje zobrazení na základě pravidel, filtrů a řazení událostí na základě polí, které lze nadefinovat ve zdroji **Field Sets**.

Connectors

Obsahuje nainstalované konektory. V mém případě se zde nachází **SyslogTCP** konektor a **Manager Internal Connector**. První z nich je samozřejmě konektor nainstalovaný pro přijímání logů ze systému Asterisk, druhý je pak výchozí konektor sloužící ke zpracování logů generovaných samotným systémem ArcSight ESM.

Field Sets

Tento zdroj umožňuje konfiguraci možných zobrazení setů pojmenovaných polí, kterých je více než 400. Pro různé technologie, potažmo různé **Use Cases**, které popisuji níže, je žádoucí zobrazovat pouze určitá pole, jako jsou zdrojové a cílové IP adresy, MAC adresy, časová razítka, akce spojené z danou událostí a podobně. Způsob vytváření těchto setů popíši při jejich prvním použití.

Filters

Filtry slouží k samotné konfiguraci toho, jaké události mají být zobrazeny. Filtry jsou základem složitějších pravidel. Logiku vytváření filtrů popíši detailně hned při jejich prvním použití, jelikož se jedná o základ ostatního složitějšího obsahu.

Integration Commands

Tyto zdroje slouží ke konfiguraci a spouštění příkazů, skriptů, interních nástrojů ale i nástrojů třetích stran.

Lists

Do listů lze načítat a vyčítat konkrétní hodnoty z jednotlivých událostí, vytvářet nad nimi úrovně pro spouštění jiných zdrojů, listy lze použít také jako součásti filtrů a pravidel, a to

například pro potlačení generování stejných událostí, jak bude popsáno v případě útoku na uživatelská jména.

Rules

Pravidla slouží ke korelaci a agregaci jednotlivých událostí a k vytváření nových událostí a akcí na základě přednastavených úrovní. To mohou být například reporty, spouštění dalších pravidel, plnění listů a mnoho dalšího.

9.5.3.2 Viewer

Toto pole slouží primárně k zobrazení **Active Channels**. Jeho možnosti jsou ale samozřejmě mnohem širší. Lze v něm zobrazit prakticky jakýkoli obsah nakonfigurovaný v ArcSight ESM. To znamená především jednotlivé události v rámci **Active Channels**, ale také logiku jednotlivých pravidel, grafy mnoha různých typů, reporty a mnoho dalšího.

9.5.3.3 Inspect/Edit

Pole **Inspect/Edit** je určeno k detailnímu náhledu na události vyskytující se v jednotlivých **Active Channels** v panelu **Viewer**. V tomto poli se také konfigurují všechny zdroje, které jsou dostupné v panelu **Navigator**.

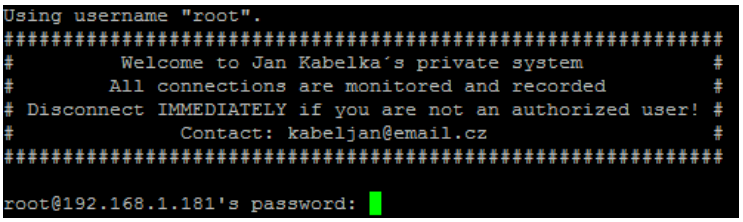
10 Konfigurace ArcSight ESM na základě útoků

V procesním řízení informační bezpečnosti je nezbytné mít znalost možných scénářů, které mohou nastat. Aby bylo možné efektivně čelit situacím, kdy dané scénáře nastanou, je opět nezbytné mít předem nastaveny bezpečnotní technologie k detekci těchto scénářů a v neposlední řadě procesy popisující kroky, které je třeba učinit v rámci nakládání se vzniklými incidenty. Této tématice jsem se věnoval v teoretické části. Scénáře, které se společnost rozhodne pokrýt a má potřebu na ně reagovat, se říká **Use Cases**.

Na praktických ukázkých možných útoků níže popíši, jaká je logika vytváření obsahu na straně ArcSight ESM. Tím mám především na mysli vytváření hyearchie filtrů, listů a dalších podmínek, pravidel a jejich agregace a možných akcí spouštěných po spuštění daného pravidla.

10.1 Warning banner

Jak jsem popsal v teoretické části, každý systém by měl uživatele před zalogováním upozornit minimálně na to, kam uživatel vstupuje a za jakých podmínek může vstoupit. Na systému Linux v distribuci Debian lze tuto zprávu pro připojení přes SSH nastavit odkomentováním a editací příslušného řádku v konfiguračním souboru **/etc/ssh/sshd_config**. V mém případě pak řádek vypadal jako **Banner /etc/banner.txt**. Vytvořil jsem soubor **/etc/banner.txt** a vložil do něj příslušný text. Obrazovka před přihlášením v tomto případě vypadala následovně.



Obr.20: Warning banner

10.2 Password guessing

Při správě mnoha serverů administrátoři využívají samozřejmě možnosti vzdáleného přístupu. U systémů běžících na platformě Windows se ke vzdálené správě typicky používá protokol RDP a v prostředí systémů Linux pak protokol SSH. Možné útoky zaměřené na získávání informací o uživatelských účtech a jejich prolamování jsem popsal v teoretické části. Přesně k těmto účelům lze využít nástroj THC Hydra. K testovacím účelům jsem povolil možnost vzdáleného přihlášení k ústředně protokolem SSH uživateli **root**, a to editací konfiguračního souboru **/etc/ssh/sshd_config**, kdy jsem změnil příslušný řádek na **PermitRootLogin yes**. Službu **ssh** bylo poté nutné restartovat. Heslo pro tohoto uživatele jsem již při prvotní instalaci nastavil na **root**. Bohužel je toto běžnou praxí líných správců, kteří si takto usnadňují práci. Nástroj THC Hydra umožňuje generovat uživatelská jména i hesla samostatně pro všechny kombinace povolených znaků. Umožňuje také vyčítat uživatelská jména a hesla samostatně z textových souborů. Příkazem níže jsem jako vstup zvolil konkrétní uživatelské jméno **root** a vyčítání možných hesel ze souboru **passwddip.txt**, který jsem si k tomuto účelu vytvořil a jehož obsahem byl samozřejmě také řetězec **root**.

```
root@kali:~# hydra -l root -P /root/passwddip.txt 192.168.1.181 ssh
```

Po úspěšném doběhnutí programu byl výstup v systému Kali následující (výstup byl zkrácen). Jak je vidět, úspěšně došlo k nalezení hesla k účtu **root**.

```
[DATA] attacking ssh://192.168.1.181:22/
[22][ssh] host: 192.168.1.181   login: root   password: root
1 of 1 target successfully completed, 1 valid password found
```

Logy lze samozřejmě na straně ústředny dohledat v souboru **/var/log/auth.log** (výstup byl zkrácen).

```
Nov  4 23:08:58 debian-asterisk sshd[2909]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.38  user=root
```

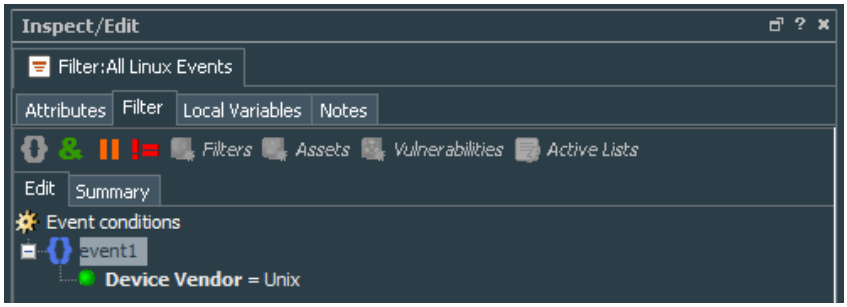
Nov 4 23:08:58 debian-asterisk sshd[2897]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.38 user=root
Nov 4 23:08:58 debian-asterisk sshd[2902]: Accepted password for root from 192.168.1.38 port 44024 ssh2
Nov 4 23:08:58 debian-asterisk sshd[2905]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.38 user=root

Vzhledem k logice tohoto útoku, tedy pokusu o autentizaci na základě znalosti jednoho konkrétního uživatelského jména a použití slovníku s hesly, jsem potřeboval nastavit na straně ArcSight ESM pravidlo, které by vygenerovalo specifickou událost při splnění následujících podmínek.

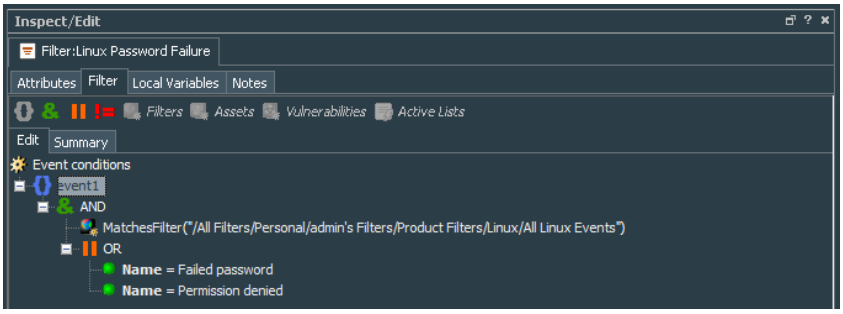
- Útok se provádí z jedné konkrétní IP adresy
- Útok se provádí proti jednomu konkrétnímu systému/IP adrese
- Útok se provádí proti jednomu konkrétnímu uživatelskému jménu
- Pokus o autentizaci se ve všech případech nezdařil
- K neúspěšné autentizaci dojde 5-krát během dvou minut

Jak jsem popsal výše, základem pravidel jsou filtry. Je žádoucí filtry vytvářet od těch nejjednodušších a teprve z těch vytvářet filtry složitější. Tím se zajistí nejen přehlednost obsahu, ale také jednoduchá použitelnost dílčích filtrů pro různé účely. S vědomím tohoto přístupu jsem vytvořil následující filtry, kde je vidět, jak jsou jednotlivé filtry vytvářeny s použitím filtrů základnějších.

Filtry, respektive jejich obsah, je postaven na Booleovské logice.



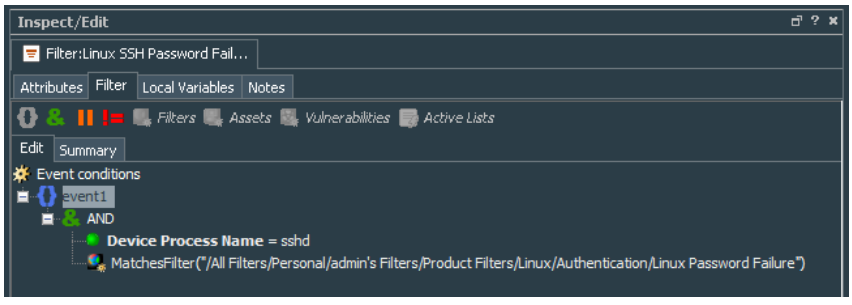
Obr.21: All Linux Evets: filtr pro všechny události ze systémů Linux



Obr.22: Linux Password Failure: filtr pro zamítnutí hesla

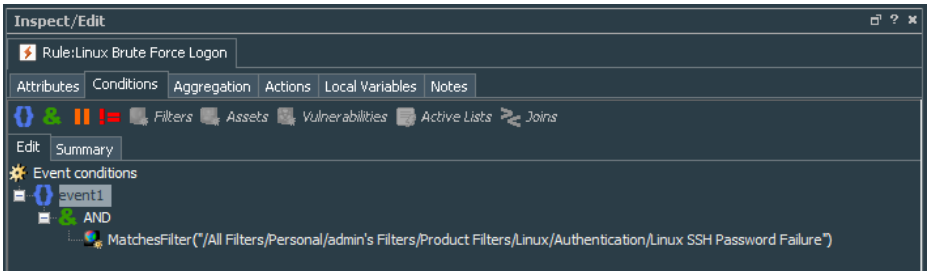
Booleovské logika vytváření filtrů a pravidel je zřejmá z obsahu záložky **Summary**.

event1 : (MatchesFilter(“All Linux Events“) AND (Name = Failed password OR Name = Permission denied))



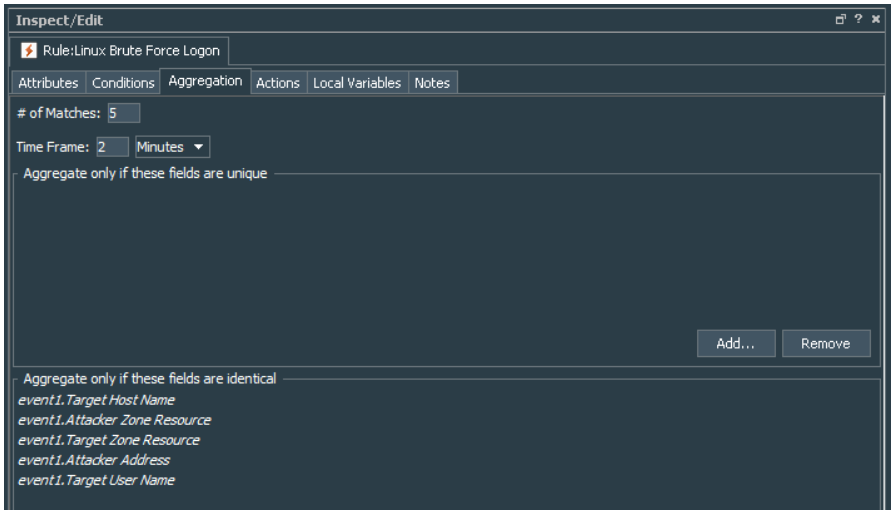
Obr.23: Linux SSH Password Failure: filtr pro zamítnutí hesla při SSH přihlašování

Poslední z filtrů, filtr **Linux SSH Password Failure**, jsem následně použil v nově vytvořeném pravidle, které jsem pojmenoval **Linux Brute Force Logon**.



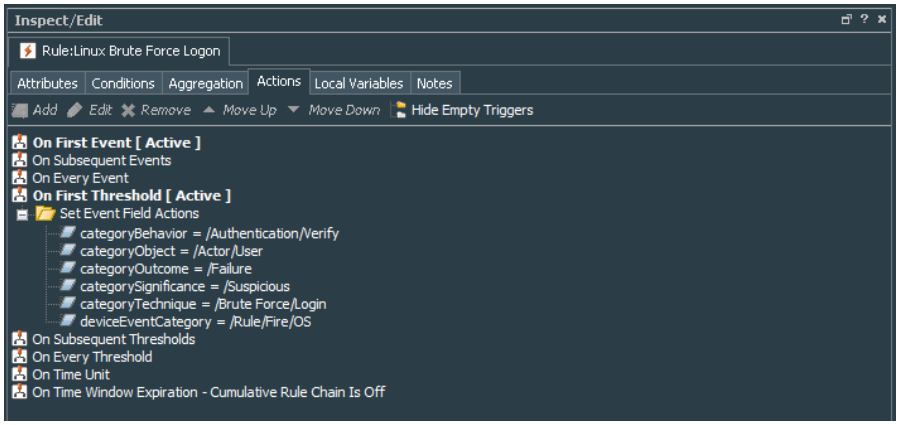
Obr.24: Pravidlo Linux Brute Force Logon

Agregaci událostí jsem nastavil tak, jak určuje logika útoku popsaná výše. Konkrétně pak ke spuštění pravidla dojde po pěti neúspěšných pokusech o autentizaci během dvou minut z jedné konkrétní IP adresy (Attacker Address), a to proti jednomu konkrétnímu cíli (Target Host Name) a jednomu konkrétnímu uživatelskému jménu (Target User Name). Všechny výše uvedené proměnné se tedy musí nacházet v sekci **Aggregate only if these fields are identical**, jak je vidět níže.



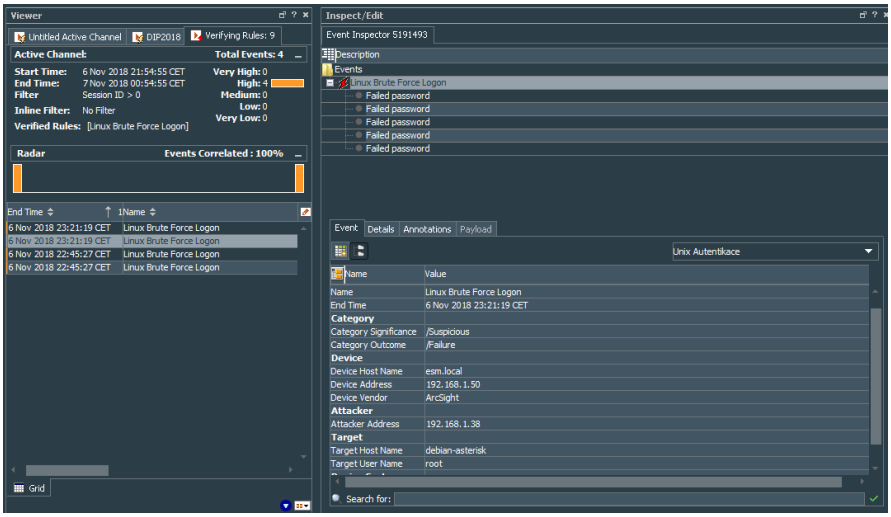
Obr.25: Podmínka agregace pravidla Linux Brute Force Logon

Akci spojenou se spuštěním pravidla jsem zvolil jako **On First Threshold**, jelikož se jedná o agregovanou událost. Jinými slovy při naplnění dílčích událostí a zároveň s agregací těchto událostí dojde k vygenerování nové události obsahující jméno tohoto pravidla a dalších polí s konkrétními hodnototami, jako je např. **categoryBehavior = /Authentication/Verify**, jak je vidět na následujícím obrázku.



Obr.26: Akce spojené s pravidlem Linux Brute Force Logon

Na obrázku níže je vidět událost, která byla vygenerována SIEM systémem ArcSight po útoku nástrojem THC Hydra proti systému Asterisk tak, jak jsem popsal výše. Na levé straně v poli **Viewer** je vidět čas, kdy k události došlo a název události.Na pravé straně v sekci **Inspect/Edit** je vidět v sekci **Description** všech pět dílčích událostí, na jejichž základě bylo pravidlo spuštěno. V pravo dole v sekci **Event** jsou pak samozřejmě k dispozici konkrétní informace, jako je adresa útočníka, uživatelské jméno na které bylo útočeno a další informace nezbytné pro analýzu dané události. Lze vytvořit **Field Set**, který by pokrýval další důležitá pole. Tento jsem vytvořil, nazval **Unix Authentication** a použil ho pro zobrazení události vygenerované pravidlem.



Obr.27: Událost vygenerovaná pravidlem Linux Brute Force Logon

Účinnou obranou proti tomuto typu útoku je samozřejmě nepovolení uživateli **root** – a všem dalším uživatelům s plnými právy k systému - přihlášení pomocí protokolu SSH. Ostatní uživatelé, a to včetně uživatelů zmíněných výše, musí používat silná hesla. Toho lze dosáhnou politikou hesel vynucenou správcem systému. Pro generování silných hesel lze s úspěchem použít k tomu určený program. Je zde ale možnost, jak se heslům úplně vyhnout. K autentizaci se dá použít asymetrická kryptografie, respektive s ní spojené klíče. V případě tohoto typu autentizace se na serveru nachází veřejná část klíče a uživatel k přihlášení používá soukromou část klíče. Použití klíče na straně klienta lze opět podmínit zadáním hesla, v tomto kontextu nazývaného přístupová fráze (Phassphrase).

10.3 Username guessing

K získání uživatelských jmen lze použít opět nástroj THC Hydra. V tomto případě jsem jako vstup zvolil soubor**/root/userdip.txt**, který obsahoval uživatelská jména. Útok jsem spustil následujícím příkazem.

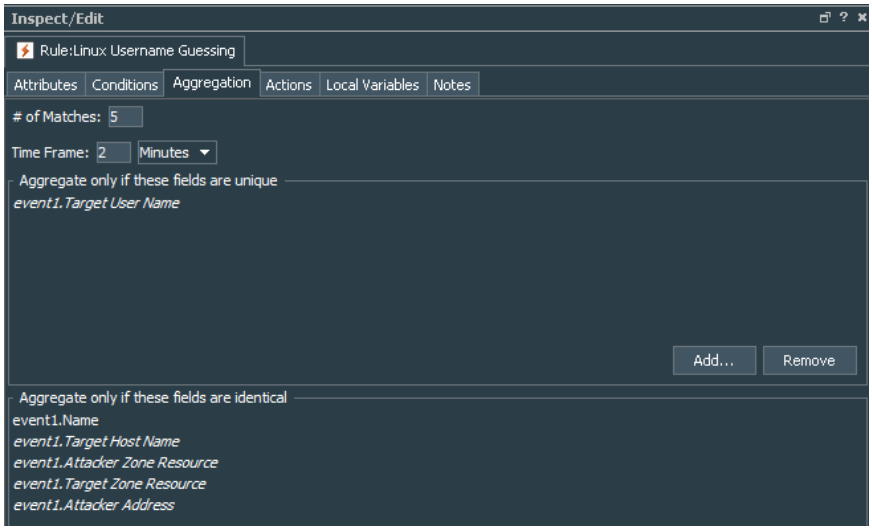
```
root@kali:~# hydra -L /root/userdip.txt -p admin1234 192.168.1.181 ssh
```

Vzhledem k logice tohoto útoku, tedy pokusu o získání informací o validitě uživatelských jmen, jsem potřeboval nastavit na straně ArcSight ESM pravidlo, které by vygenerovalo specifickou událost při splnění následujících podmínek.

- Útok se provádí z jedné konkrétní IP adresy
- Útok se provádí proti jednomu konkrétnímu systému/IP adrese
- Útok se provádí proti více uživatelským jménům
- Pokus o autentizaci se ve všech případech nezdařil
- K neúspěšné autentizaci dojde 5-krát během dvou minut

K vytvoření tohoto pravidla, nazvaného **Linux Username Guessing**, lze využít filtry, které jsem již vytvořil pro potřeby pravidla minulého, konkrétně pak pouze jeden filtr, a to **Linux SSH Password Failure**. Rozdíl oproti minulému pravidlu je v agregaci jednotlivých

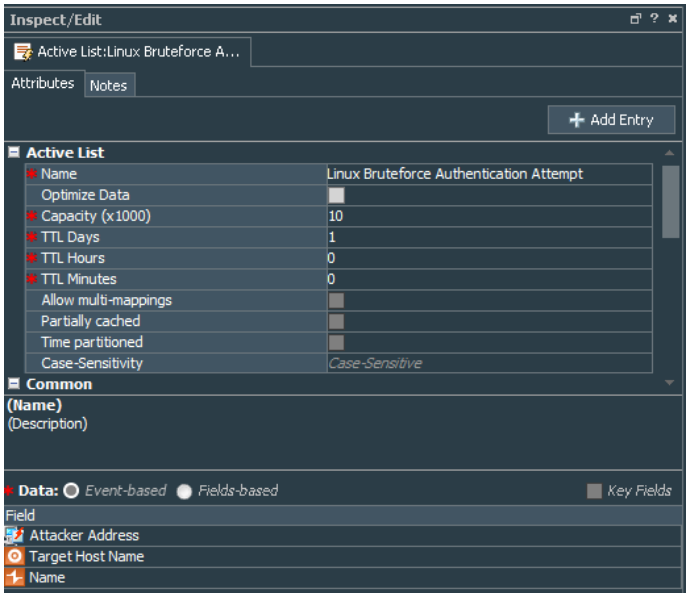
událostí. Zde bylo potřeba agregovat události v případě, kdy je obsah pole **Target User Name** různý, a tedy dochází ke změně uživatelského jména při pokusech o autentizaci.



Obr.28: Podmínka agregace pravidla Linux Username Guessing

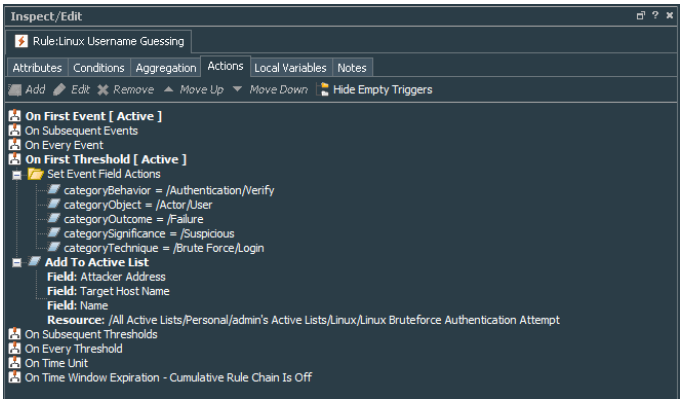
Při nastavení, které jsem popsal výše, se však pravidlo nespustilo. Bylo to dáno tím, že syslog zpráva neobsahovala v poli **name** řetězce **Failed password** nebo **Permission denied**, jak tomu bylo v případě existujícího uživatele a nesprávného hesla, ale řetězec **Failed password for invalid user**. Musel jsem tedy přidat tuto možnost do filtru **Linux Password Failure**.

Jak bylo vidět při spuštění pravidla **Linux Brute Force Logon**, tak i u tohoto pravidla bylo vygenerováno více událostí. V případě masivního útoku, kdy útočník zkouší tisíce a více možných uživatelských jmen a hesel, by byl analytik pracující se SIEM systémem zahlcen množstvím stejných událostí. Je proto vhodné stejné události na nějakou dobu potlačit. K tomuto účelu jsem vytvořil tzv. **Active List**, který je při spuštění pravidla obohacen o určitá pole a jejich hodnoty. Nastavení tohoto listu potlačení, který jsem nazval **Linux Bruteforce Authentication Attempt**, je vidět níže. List bude plněn událostmi, respektive obsahem jejich polí **Attacker Address**, **Target Host Name** a **Name**. Dobu potlačení (TTL) jsem zvolil na jeden den.



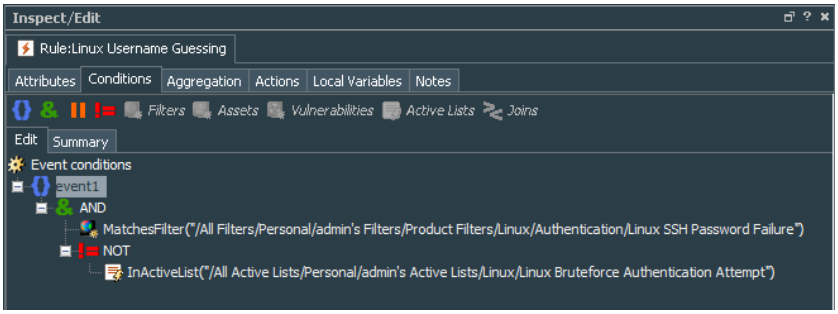
Obr.29: List potlačení Linux Bruteforce Authentication Attempt

K plnění listu dochází na základě spuštění pravidla. Toto se nastavuje v akcích spojenými s příslušných pravidlem.



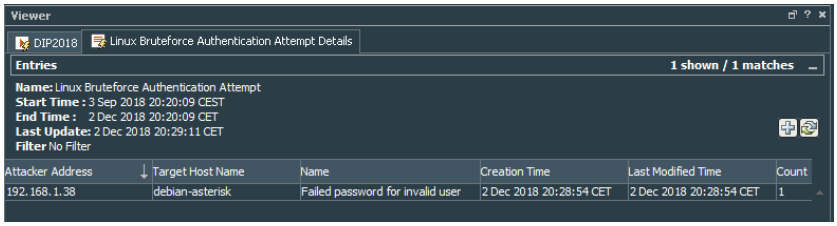
Obr.30: Akce spojené s pravidlem Linux Username Guessing

Podmínku spuštění pravidla jsem pak upravil tak, aby bylo pravidlo spuštěno pouze v případě, kdy se záznam, respektive konkrétní hodnoty polí nastavených v listu **Linux Bruteforce Authentication Attempt**, nenachází v tomto listu.



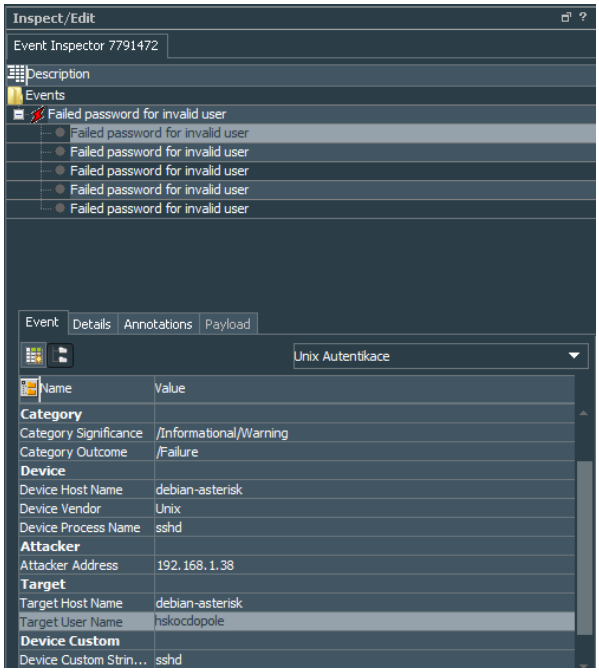
Obr.31: Pravidlo Linux Username Guessing s příslušným listem na potlačení

Od této chvíle dochází k plnění listu. Po spuštění pravidla na základě útoku se list automaticky obohatil o záznam níže.



Obr.32: Obsah listu potlačení Linux Bruteforce Authentication Attempt

Událost vygenerovaná pravidlem **Linux Username Guessing** a jejích pět základním událostí je vidět níže. Opět lze velmi jednoduše dohledat například konkrétní uživatelské jméno, které útočník zkusil uhádnout v poli **Target User Name**.



Obr.33: Událost vygenerovaná pravidlem Linux Username Guessing

10.4 Útok na uživatelské SIP účty

Distribuce Kali Linux byla vyvinuta především pro penetrační účely a ve výchozím nastavení obsahuje množství nástrojů. To platí i pro sadu nástrojů pod jednotným názvem SIPVicious. Skripty obsažené v této sadě jsou určeny k získávání informací a k útokům na zařízení využívající protokol SIP. SIPVicious obsahuje čtyři skripty. Spuštění skriptů lze samozřejmě ovlivnit velkým množstvím přepínačů. Jako vstup pro skripty mohou sloužit konkrétní hodnoty i obsahy textových souborů, jako jsou názvy uživatelských účtů a hesla.

svmap – skener SIP zařízení. Nalezne SIP zařízení pro daný rozsah IP adres.

svwar – identifikuje aktivní extensions na PBX

svcrack – slouží k prolamování hesel SIP účtů

svreport – řídí jednotlivá spojení a nabízí možnost exportovat zprávy v různých formátech

Skenování zařízení pomocí **svmap** na rozsahu IP adres lokální sítě.

```
root@kali:~# svmap 192.168.1.0/24
| SIP Device          | User Agent                  | Fingerprint |
-------------------------------------------------------------------------------
| 192.168.1.181:5060 | USEAsterisk PBX 13.18.2 | disabled    |
| 192.168.1.218:5060 | Linksys/SPA962-6.1.3(a)   | disabled    |
| 192.168.1.223:5060 | Cisco/SPA504G-7.4.9a      | disabled    |
```

Ve výpisu je vidět, že byla detekována verze jednotlivých SIP zařízení. Z bezpečnostního hlediska je minimálně pro ústřednu lepší tuto informaci útočníkům takto jednoduše neposkytnout. Stačí změnit hodnotu **useragent** v konfiguračním souboru **/etc/asterisk/sip.conf.** Výsledek skenování pak může vypadat následovně.

```
root@kali:~# svmap 192.168.1.0/24
| SIP Device          | User Agent                  | Fingerprint |
-------------------------------------------------------------------------------
| 192.168.1.181:5060 | NSA confidential system monitored    | disabled    |
| 192.168.1.218:5060 | Linksys/SPA962-6.1.3(a)  | disabled    |
| 192.168.1.223:5060 | Cisco/SPA504G-7.4.9a      | disabled    |
```

Všeobecně známým nástrojem **nmap** jsem pak lehce zjistil operační systém ústředny a díky MAC adrese jsem získal také informaci, že ústředna je nainstalována jako virtuální stroj.

```
root@kali:~# nmap -O 192.168.1.181
Starting Nmap 7.40 ( https://nmap.org ) at 2018-10-28 23:16 CET
Nmap scan report for 192.168.1.181
Host is up (0.0013s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
2000/tcp open  cisco-sccp
5060/tcp open  sip
MAC Address: 08:00:27:00:0D:22 (Oracle VirtualBox virtual NIC)
Device type: general purpose
```

Running: Linux 3.X|4.X

OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4

OS details: Linux 3.2 - 4.6

Network Distance: 1 hop

Po získání informací o ústředně se lze pomocí nástroje **svwar** spuštěného proti ústředně dostat k informacím o **extensions**, které jsou na ústředně nainstalované. Tohoto jsem docílil pomocí příkazu níže a s následujícím výstupem.

```
root@kali:/etc/init.d# svwar --force -e100-200 192.168.1.181
| Extension | Authentication |
-----------------------------
| 200       | reqauth        |
| 100       | reqauth        |
```

Je vidět, že byly identifikovány obě **extensions**. Nyní se pokusím prolomit hesla k těmto účtům, a to pomocí výše zmíněného nástroje **svcrack**. Útok jsem provedl proti extensions **100** s následujícím výstupem.

```
root@kali:/etc/init.d# svcrack -u 100 192.168.1.181
ERROR:ASipOfRedWine:We got an unknown response
| Extension | Password |
-----------------------
| 100       | 100      |
```

A jakým způsobem lze zabránit výše popsanému útoku? Získání informací pomocí skriptu **svwar** je dáno pokusem o autentizaci proti existujícím účtům, kdy ústředna ve výchozím nastavení poskytuje útočníkovi informaci o tom, zda daný účet existuje či nikoli. Asterisk však umožňuje tuto funkci vypnout, a to změnou příznaku záznamu níže z **no** na **yes** v konfiguračním souboru **sip.conf**.

```
alwaysautreject=no ; ústředna v odpovědi poskytuje informaci, zda došlo ke špatné autentizaci pro platný SIP účet
```

Výstup po spuštění skriptu **svwar** je pak následující.

```
root@kali:~# svwar --force -z4 -e100-200 192.168.1.181
WARNING:root:found nothing
```

Samozřejmě, tak jako u všech hesel, by se měla volit hesla komplexní a co možná nejdelší. Tímto by se účinně dalo tomuto útoku když ne zabránit, tak ho alespoň útočníkovi znesnadnit. Také se tím zvyšuje šance na detekci takového dění na síti. Slabostí konfigurace zde bylo také to, že byla zvolena lehce uhodnutelná jména uživatelských SIP účtů. Tato by měla být delší a komplexnější.

Na straně ArcSight ESM jsem pravidla a filtry nevytvářel, jelikož byly přijímány logy z ústředny způsobem, kdy byl celý log obsahem pouze jediného pole **name**. Nedochází zde ke správnému parsování logů generovaných ústřednou Asterisk na straně ArcSight Connector modulu. Níže je příklad zprávy o neúspěšném pokusu o registraci při použití skriptu **svwar**.

```
NOTICE[1061]: chan_sip.c:28633 in handle_request_register: Registration from '"185"<sip:185@192.168.1.181>' failed for '192.168.1.38:5060' - No matching peer found
```

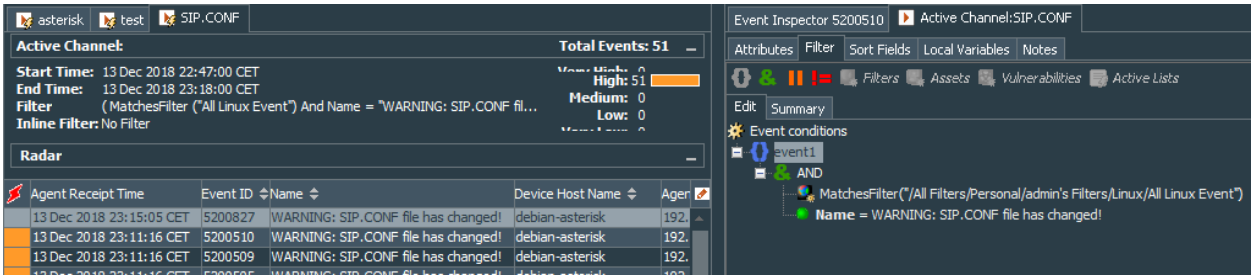
Možné důvody a způsoby řešení popíši v závěru této diplomové práce.

10.5 Detekce změny konfiguračních souborů

Konfigurační soubory **sip.conf** a **extensions.conf** jsou těmi nejdůležitějšími na ústředně Asterisk. Rozhodl jsem se proto detekovat jejich modifikaci. Pomocí skriptů, které jsem napsal (dostupné na přiloženém CD) s názvem **md5sipcheck.sh** a **md5extencheck.sh**, detekuji tuto změna na základě změny MD5 hashe těchto souborů v čase. Skripty bylo potřeba tzv. schedulovat, což znamená, že budou spuštěny na pozadí v konkrétní čas. Toho lze docílit úpravou souboru **/var/spool/cron/crontabs/root** obohacením o záznam typu *** * * * * /bin/bash /root/md5sipcheck.sh**. Pokud skripty zdetekují změnu v souborech, odešlou na syslog démona upozornění. Toho lze docílit následujícím řádkem kódu ve skriptu (zde pro **sip.conf**)

logger "WARNING: SIP.CONF file has changed!"

Vytvořil jsem nový **Active Channel** a **Filter**, kterým jsem zobrazil události reflektující změnu souboru **sip.conf**. Níže je na levé straně vidět příslušná událost a na pravé straně podmínky filtru k jejímu zobrazení.



Obr.34: Změna konfiguračního souboru sip.conf

11 Závěr

V rámci této diplomové práce se mi podařilo naistalovat a nastavit všechny komponenty systému SIEM ArcSight nezbytné k jeho úspěšnému provozu. Pro zvolené typy útoků proti systému Asterisk jsem demonstroval, jakým způsobem lze nakonfigurovat systém ArcSight tak, aby tyto útoky zaznamenal a zobrazil události takovým způsobem, aby bylo zřejmé, o jaký typ útoku se jedná.

Problémem se ukázalo zpracování logů přicházejících ze služby Asterisk. Příčinou je nastavení komponenty ArcSight Smart Connector, která je zodpovědná za sběr a automatickou syntaktickou analýzu logů. Použití Connectoru typu Smart se zvoleným nastavením pro zpracování logů ve formátu syslog se ukázalo jako nevhodné. Nedocházelo ke správné analýze logů a tyto se na straně ArcSight ESM nacházely v jednom poli, což znemožnilo efektivní korelaci událostí. Vidím zde dvě možnosti, jak zajistit správnou analýzu logů ze služby Asterisk. První z nich je vytvoření lokálních proměnných na straně ArcSight ESM a do těchto proměnných na základě regulárních výrazů vkládat jednotlivé části logů. Tento přístup je však konfiguračně zdlouhavý a s nejasným výsledkem. I z pohledu vytížení ArcSight ESM toto není vhodný přístup, jelikož ArcSight ESM má primárně provádět korelaci logů a ne jejich analýzu. Vhodnějším přístupem se proto jeví použití ArcSight Connectoru typu Flex. Jeho nastavení není triviální, ale lze tak zajistit automatickou analýzu logů ještě před tím, než budou tyto odeslány ke zpracování do ArcSight ESM.

SIEM systém ArcSight od společnosti Micro Focus je velmi komplexní řešení pokrývající potřeby řízení informační bezpečnosti. V případě nasazení VoIP ústředny Asterisk v produkčním prostředí bych doporučil konfiguraci asset modelů tak, aby byla ovlivněna důležitost událostí generovaných na základě nakonfigurovaných pravidel, a tak umožnit jejich prioritizaci před méně důležitými událostmi. V produkčním prostředí, kde se předpokládá použití dalších bezpečnostních řešení, jako jsou především firewally a IPS zařízení, bych určitě doporučil sbírat logy i z těchto zařízení a provádět korelaci i nad nimi, což by výrazně zvýšilo vhled do dění na síti a možnosti odhalení potenciálního útoku.

12 Přílohy

Seznam obrázků

Seznam použitých zkratek a symbolů

ACL	Access Control List
API	Application Programming Interface
ARP	Address Resolution Protocol
AS	Autonomous System
C&C	Command and Control
CAPEX	Capital Expenditures
CEF	Common Event Format
CIA	Confidentiality, Integrity, Availability
CLF	Common Log Format
CLI	Command Line Interface
ČSN	České Technické Normy
DAHDI	Digium Asterisk Hardware Device Interface
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS/DDoS	Denial of Service/Distributed Denial of Service
EPS	Events per Second
FTP	File Transfer Protocol
GNU	GNU's Not Unix
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HA	High Availability
HIPS	Host Intrusion Prevention System
HPE	Hewlett Packard Enterprise

HTTP	HyperText Transfer Protocol
IANA	Internet Assigned Numbers Authority
IAX	Inter-Asterisk Exchange
IBM	International Business Machines
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IoC	Indicators of Compromise
IP	Internet Protocol
IPS/IDS	Intrusion Prevention/Detection Systems
IS	Information System
ISMS	Information Security Management System
ISP	Internet Service Provider
ISS	Internet Information Services
IT	Information Technology
ITIL	IT Infrastructure Library
ITSM	IT Service Management
LAN	Local Area Network
MAC	Media Access Control
MD5	Message-Digest 5
MGCP	Media Gateway Control Protocol
MP3	Moving Picture Experts Group Layer-3 Audio
N/A	Not Available (Not Applicable)

NAT	Network Address Translation
NIC	Network Interface Controller
NTP	Network Time Protocol
OPEX	Operating Expenses
OS	Operating System
PBX	Private Branch Exchange
PBX	Private Branch eXchange
PDF	Portable Document Format
PSTN	Public Switched Telephone Network
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RFC	Requests for Comments
RIPE NCC	Reseaux IP Europeens Network Coordination Centre
RPC	Remote Procedure Call
RTP	Real-time Transport Protocol
SANS	SysAdmin, Audit, Network and Security
SCCP	Skinny Call Control Protocol
SDP	Session Description Protocol
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SSH	Secure Shell
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol

TLS	Transport Layer Security
TTL	Time To Live
URI	Uniform Resource Identifier
UTM	Unified Threat Management
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virual Private Network
Wi-fi	Wireless Fidelity
XSS	Cross Site Scripting

Bibliografie

[1] Data. [online]. [cit. 2017-08-27]. Dostupné z: https://managementmania.com/cs/data

[2] HRONEK, Jiří. Informační systémy. [online]. [cit. 2017-08-27]. Str. 21. Dostupné z: http://phoenix.inf.upol.cz/esf/ucebni/infoSys.pdf

[3] Informační systém. [online]. [cit. 2017-08-28]. Dostupné online: https://cs.wikipedia.org/wiki/Informa%C4%8Dn%C3%AD_syst%C3%A9m#cite_note-1

[4] BUCKSTEEG, Martin, Nadin EBEL and Frank EGGERT. ITIL® 2011 Stručný a srozumitelný výklad. Computer Press, Brno, 2012. Str. 24. ISBN 978-80-251-3732-1

[5] Co je to služba IT. [online]. [cit. 2017-08-27]. Dostupné z: https://www.bestpractice.cz/cs/Best-practice/-ITSM-ITIL-/-Co-je-to-sluzba-IT.alej

[6] CHLUP, Marek. BEZPEČNOST ICT. [online]. [cit. 2017-08-27]. Str. 11. Dostupné z: http://www.cimib.cz/ors/fileadmin/user_upload/dokumenty/CIMIB_Bezpecnost_ICT.pdf

[7] KOTZIAN, Robert. Právní úprava informační bezpečnosti pro orgány veřejné moci. [online]. [cit. 2017-08-27]. Dostupné z: https://www.epravo.cz/top/clanky/pravni-uprava-informacni-bezpecnosti-pro-organy-verejne-moci-96806.html

[8] DOBDA, Luboš. Ochrana dat v informačních systémech. Grada, Praha, 1998, str.13-14. ISBN 8071694797

[9] GOGELA, Robert. Standardy a definice pojmů bezpečnosti informací. [online]. [cit. 2017-08-27]. Dostupné z: https://www.cybersecurity.cz/data/Gogela.pdf

[10] CHLUP, Marek. BEZPEČNOST ICT. [online]. [cit. 2017-08-27]. Str. 14. Dostupné z: http://www.cimib.cz/ors/fileadmin/user_upload/dokumenty/CIMIB_Bezpecnost_ICT.pdf

[11] BŘICHÁČEK, Zdeněk. [online]. Dostupné z: https://blog.brichacek.net/audit-informacni-bezpecnosti-analyza-a-rizeni-rizik/#comments

[12] BUCKSTEEG, Martin, Nadin EBEL and Frank EGGERT. ITIL® 2011 Stručný a srozumitelný výklad. Computer Press Brno 2012. Str. 19. ISBN 978-80-251-3732-1

[13] GOGELA, Robert. Standardy a definice pojmů bezpečnosti informací. [online]. [cit. 2017-08-27]. Dostupné z: https://www.cybersecurity.cz/data/Gogela.pdf

[14] K čemu je SIEM? [online]. [cit. 2017-09-25]. Dostupné z: https://www.systemonline.cz/it-security/k-cemu-je-siem.htm

[16] MILLER, David R., Shon HARRIS, Harper ALLEN A. and Stephen VANDYKE. Security Information and Event Management (SIEM) Implementation. The McGraw-Hill Companies United States of America 2011. Str. 55. ISBN 978-0-07-170109-9

[17] KENT, M. S. Karen. Guide to Computer Security Log Management. [online]. [cit 2017-10-02]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf

[18] IBM Buys Network Security Intelligence Company Q1 Labs. [online]. [cit. 2017-09-25]. Dostupné z: https://techcrunch.com/2011/10/04/ibm-buys-network-security-intelligence-company-q1-labs/

[19] Splunk. [online]. [cit. 2017-10-01]. Dostupné z: https://cs.wikipedia.org/wiki/Splunk

[20] CARASSO, David. Exploring Splunk. CITO Research New York 2012. Str. 11. ISBN 978-0-9825506-7-0; 0-9825506-7-7

[21] LogRhythm Overview . [online]. [cit. 2017-10-01]. Dostupné z: https://logrhythm.com/about/

[22] HP eyes $1.46bn ArcSight security buy . [online]. [cit. 2017-10-01]. Dostupné z: https://www.theregister.co.uk/2010/09/12/hp_arcsight_rumor/

[23] ArcSight. [online]. [cit. 2017-10-01]. Dostupné z: https://en.wikipedia.org/wiki/ArcSight

[24] Kali Linux [online]. [cit. 2018-9-25] Dostupné z: https://cs.wikipedia.org/wiki/Kali_Linux

[25] Download Kali Linux Images [online]. [cit. 2018-9-25] Dostupné z: https://www.kali.org/downloads

[26] Asterisk (PBX) [online]. [cit. 2017-11-23]. Dostupné z: https://en.wikipedia.org/wiki/Asterisk_(PBX)

[27] CONFIGURATION CISCO SPA50XG [online]. [cit. 2017-11-26]. Dostupné z: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/csbpipp/ip_phones/user/guide/50X_sip_user_guide_source/500_SIP_user.pdf

[28] CONFIGURATION CISCO SPA9XX [online]. [cit. 2017-11-26]. Dostupné z: http://wiki.openip.fr/sites/default/files/configuration_cisco_spa9xx.pdf

[29] ArcSight Common Event Format (CEF) Implementation Standard [online]. [cit. 2018-10-1] Dostupné z: https://community.softwaregrp.com/t5/ArcSight-Connectors/ArcSight-Common-Event-Format-CEF-Implementation-Standard/ta-p/1645557?attachment-id=68077

[30] World Economic Forum® . The Global Risks Report . [online]. [cit. 2017-08-29]. Dostupné z: http://www3.weforum.org/docs/GRR17_Report_web.pdf

[31] ANDERSON, Bob. ITIL V3 Service Life Cycle. [online]. [cit. 2017-08-27]. Dostupné z: http://www.itservicemanagement-itil.com/itil-v3-service-life-cycle/

[32] GOGELA, Robert. Standardy a definice pojmů bezpečnosti informací. [online]. [cit. 2017-08-27]. Dostupné z: https://www.cybersecurity.cz/data/Gogela.pdf

[33] INCIDENT RESPONSE . [online]. [cit. 2017-08-30]. Dostupné z: http://www.eforensik.com/incident-response.html

[34] Increasing Attack Sophistication. Acad|CSIRT. [online]. [cit. 2017-08-30]. Dostupné z: https://www.slideshare.net/ignmantra/seminar-cyber-defence-unsoed-21-september-2014

[35] Cyber Attack Disrupting Critical Infrastructure In 2016 A Likelihood, Say Security Professionals. [online]. [cit. 2017-09-01]. Dostupné z: http://www.cioandleader.com/article/2016/01/14/cyber-attack-disrupting-critical-infrastructure-2016-likelihood-say-security

[36] Innovation Fuels IBM QRadar Leadership (Again) in Gartner's 2016 Magic Quadrant for SIEM. [online]. [cit. 2017-09-25]. Dostupné z: https://securityintelligence.com/innovation-fuels-ibm-qradar-leadership-again-in-gartners-2016-magic-quadrant-for-siem/

[37] Oracle VM VirtualBox: Networking options and how-to manage them. [online]. [cit. 2018-09-25]. Dostupné z: https://blogs.oracle.com/scoter/networking-in-virtualbox-v2

[38] Cross-site scripting [online]. [cit. 2018-12-15]. Dostupné z: https://cs.wikipedia.org/wiki/Cross-site_scripting

Obsah přiloženého CD