Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Bakalářská práce

2015 **Tomáš Hronek**

Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Vulnerability management v podnikové IT infrastruktuře

Vypracoval: Tomáš Hronek

Vedoucí práce: Ing. Jaromír Veber, Ph.D.

Rok vypracování: 2015

Čestné prohlášení:

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Veškeré použité podklady, ze kterých jsem čerpal informace, jsou uvedeny v seznamu použité literatury a citovány v textu podle normy ČSN ISO 690.

V Praze dne 28.4.2015 Podpis: .....

Tomáš Hronek

Poděkování

Děkuji vedoucímu mé bakalářské práce Ing. Jaromíru Veberovi, Ph.D. za poskytnuté konzultace, náměty a rady při jejím zpracování a Mgr. Haně Bartůňkové za pomoc při stylistice.

Abstrakt

Práce se zabývá oblastí řízení zranitelností a jejich vztahu k informační bezpečnosti. Jejím cílem je zasazení tematiky řízení zranitelností do kontextu informační bezpečnosti podniku a vysvětlení jejího vztahu k souvisejícím disciplínám. V praktické části jsou porovnány vybrané nástroje k hodnocení zranitelností a je aplikována metodika k určení kritičnosti zjištěných zranitelností ve vztahu k dodávaným IT službám.

Cílů bylo dosaženo rešerší odborných informačních zdrojů, osobními konzultacemi s pracovníkem odpovídajícím za informační bezpečnost v J&T Bance a srovnáním výsledků nástrojů k hodnocení zranitelností (Nessus, Retina, OpenVAS, Nexpose, Tripwire).

Dosud nebyla publikována žádná vysokoškolská závěrečná práci věnující se výhradně tématu řízení zranitelností. Tato závěrečná práce je první, která poskytuje srovnatelné výsledky skenování zranitelností vůči stejným cílům. Neméně přínosná je rovněž aplikace metodiky Common Vulnerability Scoring System k určení kritičnosti zjištěných zranitelností ve vztahu k dodávaným IT službám.

Klíčová slova

Zranitelnost, expozice, řízení zranitelností, hodnocení zranitelností, soulad s bezpečnostní konfigurací, srovnání nástrojů, kritičnost, CVSS, Nessus, Tripwire, Retina, OpenVAS, Nexpose,

Abstract

The present thesis deals with the area of vulnerability management and its relation to information security. Its main purpose is to set the topic of vulnerability management in context of company information security and to explain its relationship to related disciplines. In the practical part, selected vulnerability assessment tools are compared and methodology is applied to determine the criticality of the vulnerabilities identified in relation to the provided IT services.

The objectives were achieved by literature review, personal consultations with employees responsible for information security at J&T Bank and by comparing the results of several tools for assessing vulnerability (Nessus, Retina, OpenVAS, Nexpose, Tripwire).

To date, there has not been published a thesis devoted exclusively to the topic of vulnerability management. This thesis is the first one to provide comparable results of vulnerability scanning of the same targets. Equally valuable is the application of Common Vulnerability Scoring System to determine the criticality of the vulnerabilities identified in relation to delivered IT services.

Keywords

Vulnerability, exposure, vulnerability management, vulnerability assessment, security configuration compliance, tools comparison,severity, CVSS, Nessus, Tripwire, Retina, OpenVAS, Nexpose

Obsah

1. Úvod

1.1 Cíl práce

Zasazení vulnerability management do kontextu informační bezpečnosti podniku a vysvětlení vztahu k souvisejícím disciplínám. V praktické části porovnám vybrané nástroje k hodnocení zranitelností, vyberu a aplikuji metodiku k určení kritičnosti zjištěných zranitelností ve vztahu k dodávaným IT službám.

1.2 Současný stav vulnerability management

Za aktuální relevantní zdroj o současném stavu vulnerability managementu (VM) považuji studii vydanou společností Gartner, která patří mezi uznávané autority v oblasti IT poradenství. Rochford (2014) jako autor studie, v říjnu 2014 hodnotil trh s nástroji pro skenování zranitelností, jako vyspělý. Ve své analýze uvádí tato klíčová zjištění:

1. Skenování zdrojů (komponenty) jako jsou serverové operační systémy a operační systémy koncových stanic, je standardně podporováno mezi výrobci vulnerability assessment nástrojů.
2. Skenování zranitelností v cloudu, operational technology systémech a v mobilních technologiích je sporadické (málo rozvinuté).
3. Výrobci skenovacích nástrojů poskytují kromě skenování zranitelností i další služby, jako například hodnocení souladu s pravidly (baseline).

Dále Rochford (2014) uvádí funkcionalitu dostupných řešení:

1. Zjištění dostupných zdrojů, které jsou součástí podnikové sítě.
2. Reportují jejich bezpečnostní konfiguraci
3. Hodnotí rizika a určují prioritu při nápravě zranitelností, v kontextu kritičnosti (severity).
4. Informuje administrátory o možných způsobech nápravy zranitelností
5. Řídí skener zranitelností

1.3 Cílová skupinu

Práce je určena čtenářům z řad specialistů na IT bezpečnost a bezpečnostním manažerům, rovněž lze využít jako doplňující zdroj informací pro předměty zabývající se bezpečností IS/IT vyučované na VŠE, či jiných školách.

1.4 Předpoklady a omezení práce

Rozsah této práce neumožňuje podrobné vysvětlení všech souvisejících disciplín informační bezpečnosti, a správy IT infrastruktury. Chuvakin (2012) ve své studii zmiňuje celou řadu

souvisejících disciplín s VM, níže uvedeným se v této práci nebudu z důvodu rozsahu věnovat, tyto oblasti patří spíše pod téma síťové bezpečnosti a řešení chyb v aplikacích/systémech:

- Network-based Intrusion Prevention System (NIPS) – Monitoruje síťový provoz a zabraňuje podezřelým aktivitám
- Host-based intrusion prevention system (HIPS) – Agent monitorující podezřelou aktivitu na koncovém zařízení
- Network Access Control (NAC) – Technologie posuzující, zdali je zařízení připojující se do sítě v souladu s požadavky dané sítě
- Monitor/Report (Sledovat a reportovat), pomocí security information and event management nástrojů. (SCARFONE, a další, 2007)
- Eliminate root cause (Odstranit příčinu vzniku zranitelnosti) – tato činnost je plně v režii výrobce dané aplikace/systému

Z interních důvodů J&T banky mi nebylo umožněno testování skenovacích nástrojů na IT infrastruktuře banky, proto jsem se ho provedl ve své domácí síti. Někteří neumožňují stažení vyšších edice svých skenovacích nástrojů, proto jsem do srovnání zařadil nižší edice nástrojů.

1.5 Struktura práce

Kapitola 2 – Rešerše zdrojů, představuje čtenáři dostupné zdroje a související závěrečné práce,

Kapitola 3 - Bezpečnost IS/ICT uvádí čtenáře do problematiky Informační bezpečnosti a charakterizuji její vztah k Vulnerability managementu.

Kapitola 4 - Vulnerability management – Řízení zranitelností

Kapitola 5 - Oblasti související s VM, se věnuje souvisejícím disciplínám (ISMS, řízení rizik, řízení pravidel, řízení konfigurací, řízení incidentů, řízení záplatování)

Kapitola 6 – Praktická část, se skládá ze dvou částí:

- Analýza zadaného problému: Určení kritičnosti zjištěných zranitelností ve vztahu k dodávaným IT službám
- Srovnání nástrojů pro skenování zranitelností

1.6 Výběr tématu

Od poloviny roku 2014 pracuji v J&T Bance a.s. jako IT Trainee v oddělení reportingu. Zde jsem se dozvěděl o možnosti psát bakalářskou práci na téma vulnerability management v podnikové praxi.

K oblasti bezpečnosti a provozu informačních systémů mám blízko, hlavně ze svého působení ve společnosti Asseco Central Europe, kde jsem pracoval na projektu pro společnost Škoda Praha Invest. Cílem bylo porovnat dostupné možnosti pro klasifikaci dat v aplikaci Microsoft Office 2010 Professional. Testoval jsem aplikaci Titus Classification for Office, následovalo rozhodnutí o vývoji vlastního klasifikačního addinu do Ofiice 2010 , tento úkol jsem realizoval.

2. Rešerše zdrojů

Podklady pro práci získávám z těchto dostupných zdrojů:

- The National Institute of Standards and Technology (NIST) – Americká vládní organizace založena roku 1901, vydává standardy v mnoha vědních oborech, včetně bezpečnosti IS/IT.
- Kniha Řízení rizik ve firmách a jiných organizacích – Ve své práci využiji pouze kapitolu 4, věnující se riziku obecně a kapitolu 5 popisující metody snižování rizika.
- Kniha Řízení bezpečnosti informací, 2. vydání – Z této publikace využiji kapitoly věnující metodikám řízení bezpečnosti informací, systému řízení bezpečnosti, bezpečnostním opatřením a institucím zabývající se bezpečností informací.
- Forum of Incident Response and Security Teams – je nevládní organizace sdružující bezpečnostní specialisty z akademických, komerčních a vládních sfér. Vydává metodiku Common Vulnerability Scoring System pro hodnocení rizik zranitelností.
- Open Web Application Security Project (OWASP) – nezisková organizace vydávající volně dostupnou metodiku pro zvyšování bezpečnosti aplikací.
- dokumentace a whitepapers výrobců skenovacích nástrojů (Nessus, Retina, OpenVAS, Nexpose, Tripwire)
- Výzkum poradenských společností (Gartner)
- odborných článků – knihovna ProQuestu

Ze souvisejících bakalářských a diplomových prací jsem vybral následující:

Název: Využití automatizovaných nástrojů pro řízení bezpečnosti informací

Autor: Bc. Emil Budín (2014)

Diplomová práce

Obsah: analýza normy řady ČSN ISO/IEC 27000. Automatizované nástroje pro řízení bezpečnosti informací.

Podobnost s tématem Vulnerability management v podnikové IT infrastruktuře:

V kapitole 12.1 Pokročilé nástroje pro řízení bezpečnosti informací je provedeno srovnání nástrojů pro VM: Tenable SecurityCenter a QualysGuard Vulnerability Management, ale pouze po stránce uživatelského rozhraní, podporovaných standardů a funkcionality.

Název: Vulnerability Reports Analysis and Management

Autor: Bc. Dušan Domány (2011)

Matematicko-fyzikální fakulta

Diplomová práce

Obsah: Práce zahrnuje vytvoření aplikace umožňující sběr pravidel/doporučení pomocí text mining technologií pro vulnerability management. Dále se popisuje tvorbu vlastního skenovacího nástroje.

Podobnost s tématem Vulnerability management v podnikové IT infrastruktuře:

Nenalezl jsem žádná společná oblasti, ze kterých by bylo možné čerpat.

Název: Hodnocení přístupů k analýze bezpečnostních rizik

Vysoká škola ekonomická v Praze

Diplomová práce (KOUDELA, 2011)

Obsah: Práce vysvětluje základní pojmy informační bezpečnosti, aktivum, dopad, hrozbu, zranitelnost, opatření a riziko. Poskytuje přehled metod použitelných pro analýzu rizik(detailně se zabývá normou 27005)

Podobnost s tématem Vulnerability management v podnikové IT infrastruktuře:

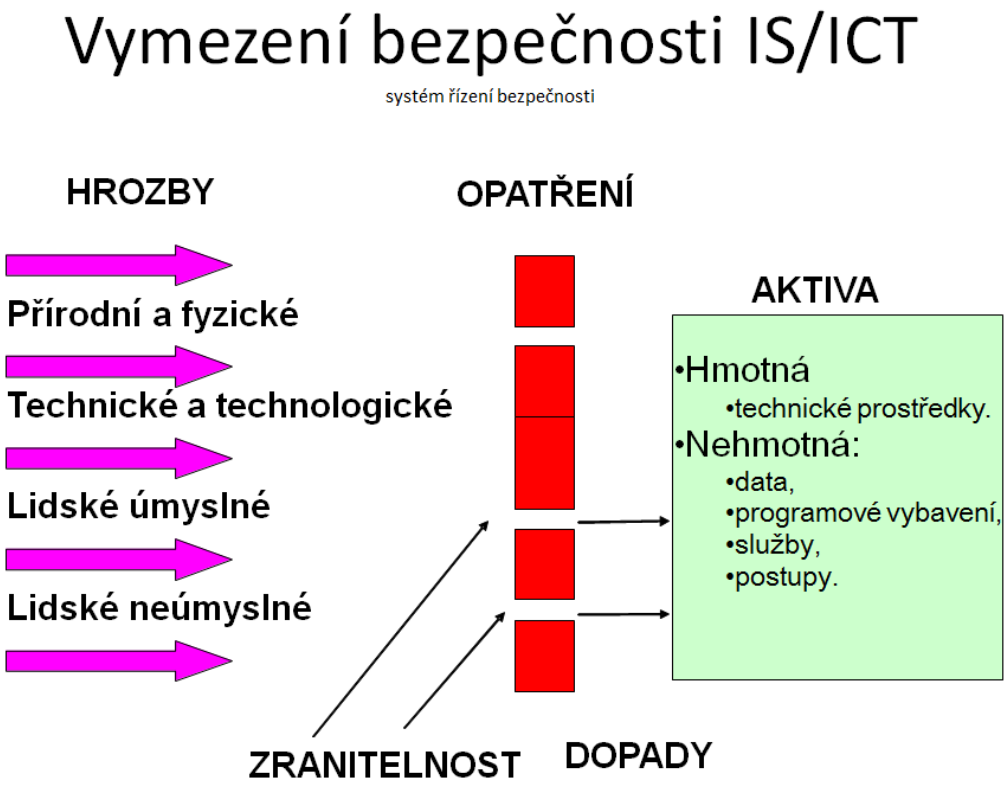
Ve své práci taktéž provádím analýzu bezpečnostních rizik

3. Bezpečnost IS/ICT

Práci začnu vymezením bezpečnosti IS/ICT. Pokud chce společnost provádět jakoukoliv činnost, při které jsou využívány informační a komunikační technologie, musí počítat s hrozbami. Doucek (2011) je rozděluje do následujících kategorií:

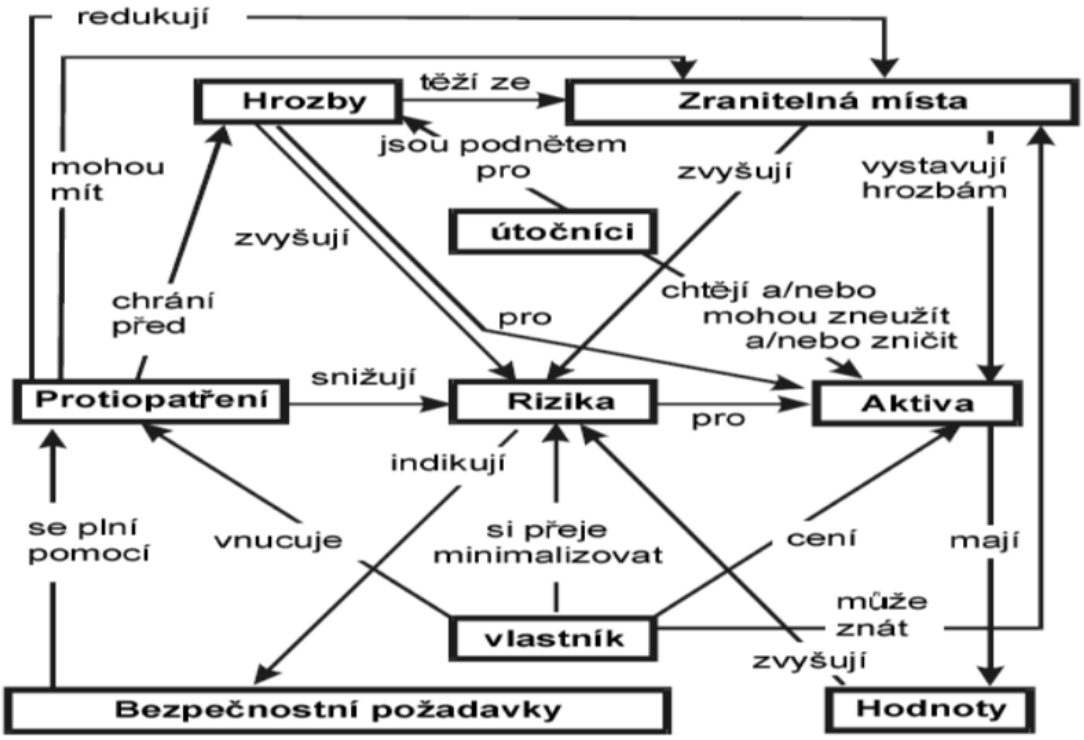
1. Přírodní a fyzické (zaplavení, pád na zem)
2. Technické a technologické (selhání komponenty, nevhodné užití)
3. Lidské úmyslné (útok na systém společnosti osobou mimo společnost, vynesení citlivých dat zaměstnancem společnosti)
4. Lidské neúmyslné (špatná konfigurace systému)

Proti hrozbám neexistuje stoprocentní ochrana, cílem zvyšování bezpečnosti IS/ICT je najít/ využít taková opatření, která sníží dopad (impact) a riziko vzniku (likehood) hrozby na přijatelnou úroveň viz Obrázek 3-1. Opatření vznikají k ochraně aktiv. Více se tomuto tématu věnuji v kapitole řízení rizik.



Obrázek 3-1 - Vymezení bezpečnosti (Zdroj: Prezentace BIS - Doucek)

Doucek (2011) dále uvádí vazby mezi jednotlivými komponentami bezpečnosti IS/ICT Obrázek 3-2. Z pohledu VM skenovací nástroje naleznou zranitelná místa (např. nevhodná konfigurace), při dosažení určité kritičnosti (severity) zranitelnosti, která se ohodnotí metodikou z oblasti hodnocení rizik, vznikne bezpečnostní incident. Incident se zpracuje podle metodiky incident managementu, pokud je tato konfigurace vyžadována pro činnost nějaké služby, vznikne výjimka, ta je následně zapsána do configuration management databáze. Výstupem incidentu managementu je v tomto případě provedení protiopatření, touto problematikou se podrobně zabývám v podkapitole patch management. Provedením protiopatření se proces VM uzavírá.



Obrázek 3-2 - Vazby v bezpečnosti IS/IT (Zdroj: Prezentace BIS - Doucek)

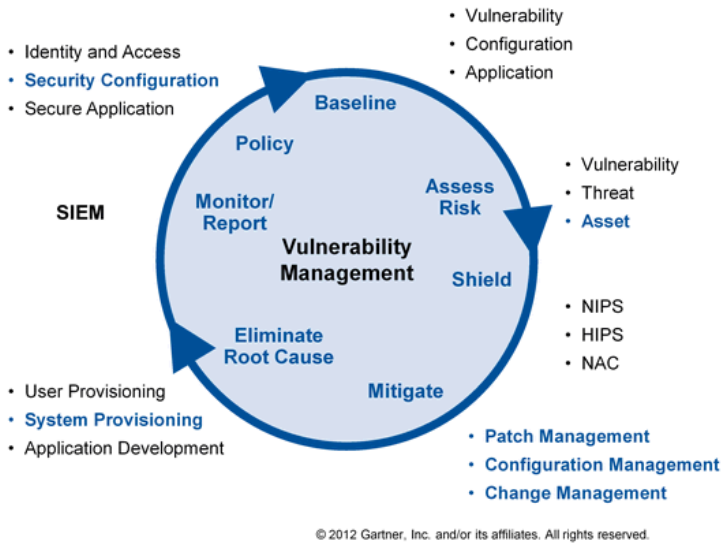
4. Vulnerability management – Řízení zranitelností

Řízení zranitelností (VM), představuje oblast bezpečnosti IS/IT, jejíž aplikování vede ke zvýšení bezpečnosti IS/IT infrastruktury, odhalením a eliminací/zmírněním zranitelných míst viz Obrázek 3-1 - Vymezení bezpečnosti (Zdroj: Prezentace BIS - Doucek)

První nástroj umožňující skenování zranitelností Security Administrator Tool for Analyzing Networks, byl vyvinut roku 1995. (CHUVAKIN, 2012) V současné době jsou dostupná řešení ve formě SaaS (Software jako služba), která usnadňují nasazení a snižují náklady na provoz VM řešení.

Řízení zranitelností není pouze o skenování zranitelností, je tvořeno celou řadou činností a souvisejících disciplín. Obrázek 4-1 znázorňuje činnosti prováděné při VM: (CHUVAKIN, 2012)

1. stanovení policy (pravidel)
2. konfigurace systémů dle baseline (doporučená konfigurace)
3. Asses risk (hodnotit riziko)
4. Shield - dočasné zabránění zneužití zranitelností (SCARFONE, a další, 2007)
    a. Network-based Intrusion Prevention System (NIPS) – Monitoruje síťový provoz a zabraňuje podezřelým aktivitám
    b. Host-based intrusion prevention system (HIPS) – Agent monitorující podezřelou aktivitu na koncovém zařízení
    c. Network Access Control (NAC) – Technologie posuzující, zdali je zařízení připojující se do sítě v souladu s požadavky dané sítě
5. Mitigate (Zmírnit) – Patch, Configuration, Change management v případě zranitelností incident management viz Kapitola 5.5
6. Eliminate root cause (Odstranit příčinu vzniku zranitelnosti) – tato činnost je plně v režii výrobce dané aplikace/systému
7. Monitor/Report (Sledovat a reportovat), pomocí security information and event management (SIEM) nástrojů.



Obrázek 4-1 - Životní cyklus Vulnerability Managementu (Zdroj: Gartner, 2012)

4.1 Zranitelnost (vulnerability)

„Zranitelností je slabé místo aktiva nebo opatření, které může být využito hrozbou. Slabá místa mohou vést k neautorizovanému přístupu ke zdrojům systému.“ (DOUCEK, a další, 2011)

Zranitelnost je chyba v softwaru, která může být přímo zneužita útočníkem k přístupu k systému nebo do sítě.[1]

Chyba, kaz, slabina nebo expozice (vystavení riziku) aplikace, systému, zařízení nebo služby, která může vést ke ztrátě důvěrnosti, integrity, nebo dostupnosti. [2]

„Zranitelnost je nedostatek, slabina nebo stav analyzovaného aktiva (případně subjektu nebo jeho části), který může hrozba využít pro uplatnění svého nežádoucího vlivu.“ (SMEJKAL, a další, 2013)

4.1.1 Databáze zranitelností

Existuje mnoho databází zranitelností, ve své práci považuji za referenční databázi National Vulnerability Database, využívající standard CVE. Ostatní zdroje uvádějí referenci na CVE:

1. The Common Vulnerabilities and Exposures
    - www.cve.mitre.org.
    - Autor standardu CVE, databáze se všemi informacemi/vazbami je dostupná skrze portál National Vulnerability Database
2. The National Institute of Standards and Technology’s National Vulnerability Database
    - http://nvd.nist.gov
    - Poskytuje a aktualizuje databázi (CVE, checklistů a dalších standardů)
    - Integruje standardy (CVE, CCE, CPE, CVSS, XCCDF, OVAL) do protokolu SCAP umožňující automatizované skenování zranitelností/expozic
3. The United States Computer Emergency Readiness Team (CERT) Vulnerability Notes Database
    - www.kb.cert.org/vuls/
4. SecurityFocus
    - http://www.securityfocus.com/
    - Používá vlastní standard pro evidenci zranitelností: Bugtraq

[1] *„An information security "vulnerability" is a mistake in software that can be directly used by a hacker to gain access to a system or network.“ (MITRE CORP., 2013)*

[2] „a bug, flaw, weakness, or exposure of an application, system, device, or service that could lead to a failure of confidentiality, integrity, or availability.“(Mell et al. 2007)

4.1.2 Příklad zranitelnosti

Uveden dle standardu Common Vulnerabilities and Exposures. Jedná se o zranitelnost týkající se produktů Micorsoft Office a SharePoint serveru v určitých verzích. Zranitelnost umožňuje spuštění škodlivého kódu i odepření služby viz Obrázek 4-2 - Příklad zranitelnosti (Autor: NVD, 2015).

- V sekci impact (Dopad) je uvedena na stupnici 0-10 kritičnost podle metodiky .
- Common Vulnerability Scoring System (CVSS), více o této metodice naleznete v kapitole 5.2.2

V další části se nacházejí odkazy na řešení, níže uvedený odkazuje na stránky výrobce dané aplikace, tato reference je typu patch information, to znamená, že jsou zde informace o nápravě zranitelnosti:

Vulnerability Summary for CVE-2015-0064

Original release date: 02/10/2015
Last revised: 02/18/2015
Source: US-CERT/NIST

Overview

Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word Automation Services in SharePoint Server 2010, Web Applications 2010 SP2, Word Viewer, and Office Compatibility Pack SP3 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted Office document, aka "Office Remote Code Execution Vulnerability."

Impact

CVSS Severity (version 2.0):
CVSS v2 Base Score: 9.3 (HIGH)
Impact Subscore: 10.0
Exploitability Subscore: 8.6
CVSS Version 2 Metrics:
Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism
Access Complexity: Medium
Authentication: Not required to exploit
Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

References to Advisories, Solutions, and Tools

External Source: MS
Name: MS15-012
Type: Advisory; Patch Information
Hyperlink: http://technet.microsoft.com/security/bulletin/MS15-012

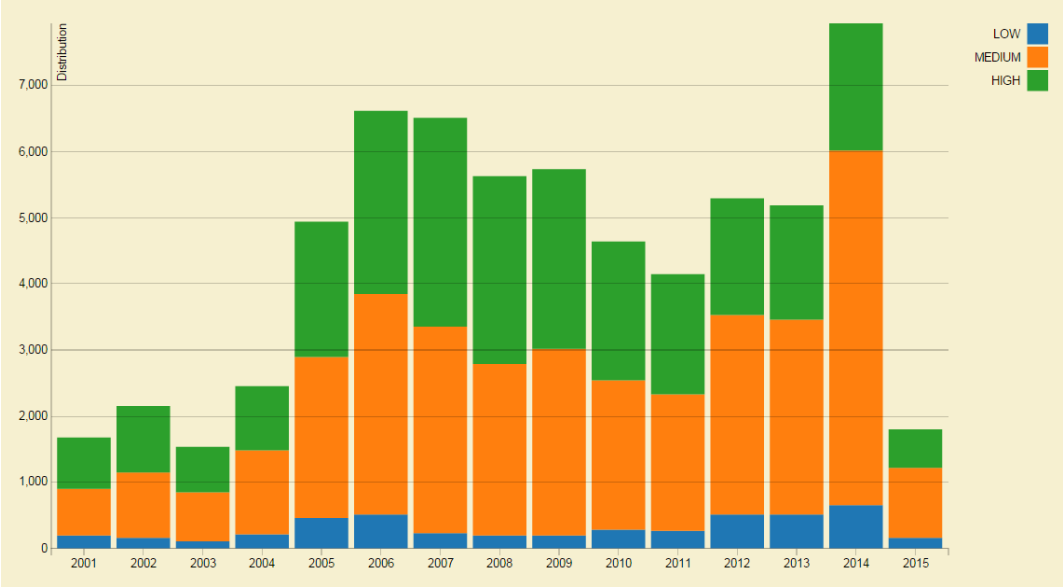
Obrázek 4-2 - Příklad zranitelnosti (Autor: NVD, 2015)

4.1.3 Trend vývoje zranitelností podle CVE

Obrázek 4-3 znázorňuje vývoj počtu záznamů CVE za jednotlivé roky, barevně je odlišena kritičnost, přičemž dle National Vulnerability Database je kritičnost určena metodikou CVSS převedena do třech kategorií (Low, Medium, High), takto (NVD, 2007):

Tabulka 1 -Převod CVSS na kritičnost (Zdroj: NVD 2015)

Kritičnost	CVSS score
High (Vysoká)	7.0-10.0
Medium (Střední)	4.0-6.9
Low (Nízká)	0.1-3.9



Obrázek 4-3 - Trend vývoje zranitelností CVE (Zdroj: NVD, 2015)

4.2 Expozice, vystavení riziku (Exposure)

Je chybná konfigurace systému, která umožňuje přístup k informacím nebo schopnostem, které mohou být zneužity útočníkem k průniku do systému nebo sítě.[3] (MITRE CORP., 2013)

Rozdíl oproti zranitelnosti spočívá v tom, že expozice známá už počátku vzniku aplikace, zařízení i operačního systému. Touto oblastí se zabývá disciplína security configuration compliance, více se o ní zmiňuji v kapitole 5.3 Policy management

[3] *„An information security "exposure" is a system configuration issue or a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network.“ (MITRE CORP., 2013)*

4.2.1 Common Configuration Enumeration (CCE)

Pro evidenci Expozic se v době psaní této práce využíval Common Configuration Enumeration (CCE), tento standard jednoznačně identifikuje chybnou konfiguraci (CCE ID), její popis (CCE Description), možnou konfiguraci (CCE Parameters), kde lze konfigurace změnit (CCE Technical Mechanisms), poslední pole tvoří referenci na výrobce nebo nástroj kde byla expozice publikována. (MANN, 2008)

Tabulka 2 -Příklad CCE

CCE ID	CCE Description	CCE Parameters	CCE Technical Mechanisms	Microsoft Security Compliance Manager (SCM) Baselines and Settings Packs
CCE-11651-7	The "Require a Password When a Computer Wakes (Plugged In)" machine setting should be configured correctly.	enabled/disabled	Computer Configuration\Administrative Templates\System\Power Management\Sleep Settings\Require a Password When a Computer Wakes (Plugged In) HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51	Microsoft Tool: Security Compliance Manager (SCM) Microsoft Baseline: Windows Server 2008 R2 SCM URL: http://go.microsoft.com/fwlink/?LinkId=113940

4.3 Vulnerability Management

Chuvakin (2012) ve své zprávě uvádí VM jako činnost zahrnující zaměstnance, procesy a technologii. Nástroje VM jsou důležitou částí VM, ale k úspěšnému řízení zranitelností nestačí.

4.3.1 Definice Qualys

Qualys (2008) ve své publikaci popisuje VM jako proces skládající se z těchto činností:

1. Zajistit, aby pravidla definována v IT policy managementu dané společnosti korespondovala s checklisty používanými ve VM.
2. Určení assets (komponent) ve společnosti, které se budou prověřovat.
3. Skenování assest pro určení zranitelnosti
4. Klasifikace rizik
5. Testování navržených změn, provedení změn
6. Skenování napraveného stavu

4.3.2 Definice NIST

Mell (2005) v publikaci vydané NIST definuje VM jako seznam povinností, které by měla určená skupina pracovníků vykonávat:

1. Vytvořit seznam komponent – lze využit už existující databázi konfiguračních položek, obsahující: hardwarové zařízení, operační systémy a aplikace užívané organizací.
2. Sledovat zranitelnosti, jejich možné nápravy (Patche) a ohrožení v kontextu používaných komponent uvnitř organizace.
3. Určit priority při nápravě zranitelností.
4. Vytvořit databázi náprav.
5. Využívat standardní konfigurace – Tato aktivita šetří prostředky při hromadném nasazení aplikací, zařízení.
6. Kontrolovat nápravu zranitelností.
7. Informovat lokální administrátory o zranitelnostech a možných nápravách.
8. Provádět automatizované nasazení patchů pro IT zařízení využívající enterprise patch management tools.
9. Nastavit automatickou aktualizaci aplikací, kdykoliv je to možné a vhodné. – Vhodnost je často těžké určit. V praxi jsem se setkal se situací, kdy automatická aktualizace aplikace Microsoft Office 2010 způsobila týdenní nefunkčnost docházkového systému pro celou společnost, který byl založen na aplikace vytvořené v MS Excel 2010.
10. Kontrolovat nápravu zranitelností skrze síťové a lokální skenování zranitelností.
    a. Síťové skenování- mapuje síť organizace, zjišťuje otevřené porty, zranitelné aplikace, nevhodně provedené konfigurace. Výhodou je, že administrátor nemusí provádět instalaci skenovacího softwaru na každý systém. Nevýhodou jsou neúplné informace o zranitelnostech, způsobené firewally, které blokují některé požadavky skenovacích aplikací. V dnešní době převládají síťové skenovací nástroje, v roce 2005 byla situace dle Mell (2005) jiná.
    b. Lokální (Host) skenování - Skenovací aplikace musí být nainstalovaná na každém skenovaném systému. Pro zjištění všech zranitelností, je vhodné spouštět skenovací aplikaci pod uživatelem s nevyššími právy, tj. root, nebo administrátor.

4.4 Trendy v Řízení zranitelnosti

Na trhu jsou dostupné nástroje pro audit a jiné pro řízení zranitelností. U velkých organizací vzniká problém při prvotním nasazení skenovacích aplikací, kdy u jednoho skenovaného zařízení vznikne v průměru 50 upozornění (CHUVAKIN, 2012), u nich je nutné určit prioritu v kontextu kritičnosti dané komponenty, podporující určitou IT službu. Množství a závažnost zjištěných nedostatků je přímo závislá na úrovni policy managementu a patch managementu.

Chuvakin (2012) dále uvádí, že společnosti by měli věnovat větší pozornost skenování webových aplikací, protože ohrožení je vyšší, než uvnitř podnikové sítě. Při vývoji aplikací by se měly využívat techniky dynamic application security testing (DAST). Testování webových aplikací a DAST jsou mimo rozsah této práce.

Na trhu jsou 3 kategorie nástrojů podporující VM: (CHUVAKIN, 2012)

1. vulnerability assessment - sloužící k odhalení rizik
2. security configuration assessment - doporučená konfigurace, například baseline od Microsoftu
3. compliance auditing – prověřuje, zdali konfigurace a procesy odpovídají určitému standardu.

Výrobci nástrojů se snaží tyto oblasti integrovat do jednoho komplexního řešení (CHUVAKIN, 2012).

Příklad standardů (CHUVAKIN, 2012):

1. Payment Card Industry Data Security Standard (PCI DSS) – Standard v oblasti platebních karet, rozšířen v bankovním sektoru.
2. Federal Information Security Management Act (FISMA) – Norma využívaná federálními útvary USA.
3. United States Government Configuration Baseline (USGCB) – Standardní konfigurace koncových stanic federálních útvarů USA. V době psaní práce byla vytvořena pro Red Hat - RHEL 5, Windows 7 a starší aplikace i to svědčí o tom, že standard není v současné době aktuální.

5. Oblasti související s VM

V této kapitole se věnuji souvisejícím oblastem, upozorňuji čtenáře, že obsahem této práce není podrobný popis každé ze souvisejících oblastí, ale pouze uvedení do problematiky spolu s vysvětlením návaznosti na VM.

5.1 Information Security Management System – ISMS

Systém řízení, definovaný normou ISO/IEC 27001. Systém zavádějící kontinuální systém řízení bezpečnosti informací v organizaci. Jeho jednotlivé kroky jsou: plan, do, check a act (plánuj, dělej, kontroluj a jednej), to zaručuje zpětnou vazbu a zlepšování daného systému. (DOUCEK, a další, 2011)

5.1.1 Definice ČSN ISO/IEC 27001

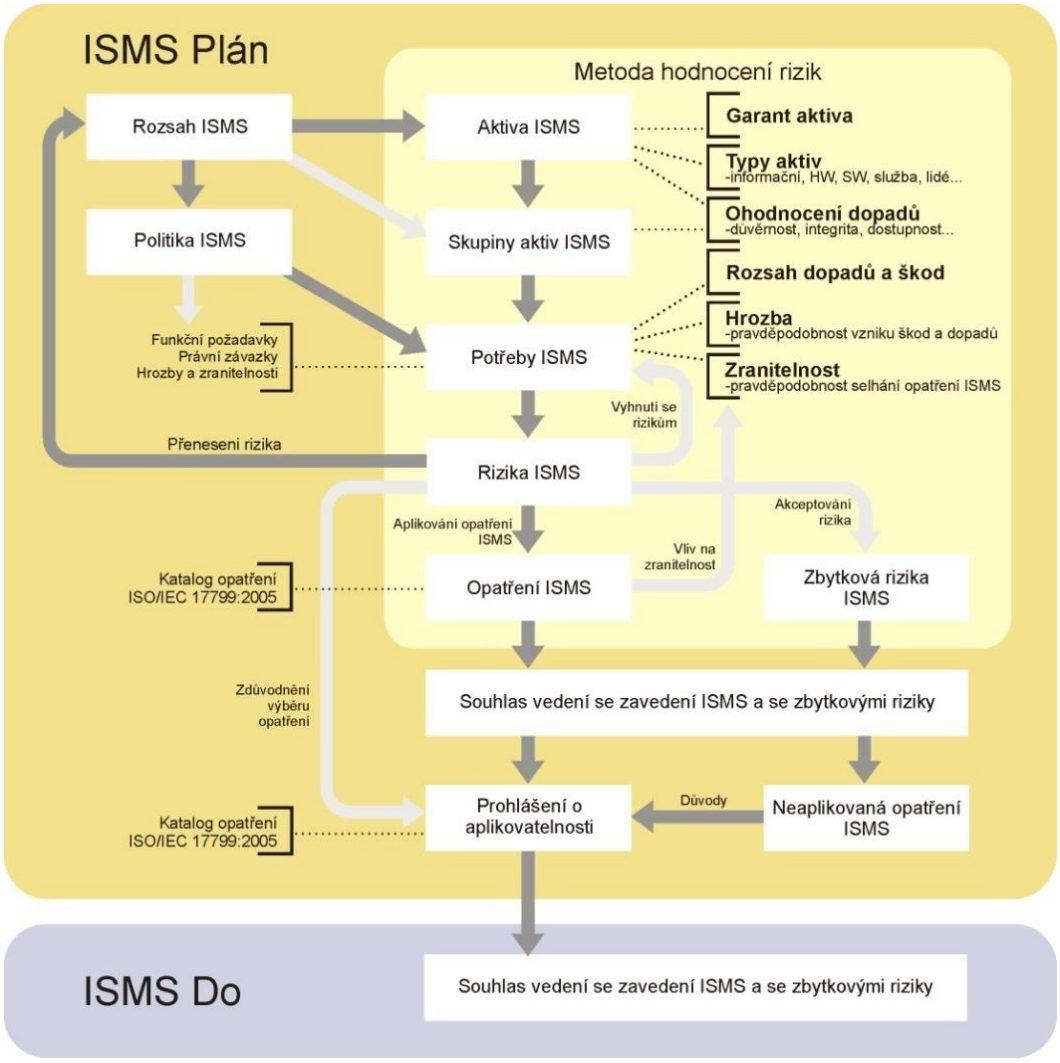
„Systém řízení bezpečnosti informací – ISMS (Information Security Management System) – část celkového systému řízení organizace, založená na přístupu (organizace) k rizikům činností, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací.“ (ČSN ISO/IEC 27001:2005, 2005)

5.1.2 Fáze plánování (Plan)

Prvním krokem při zavádění ISMS je fáze plánování, jejíž obsah popisuje definice:

„Budování ISMS začíná vlevo nahoře určením rozsahu ISMS, který přímo ovlivňuje politiku ISMS a aktiva, která jsou do ISMS zahrnuta a z nichž se, pro větší přehlednost, vytvářejí skupiny aktiv s obdobnými bezpečnostními parametry. Toto vše určuje potřeby ISMS, jimž se musí návrh ISMS podřídit“ (DOUCEK, a další, 2011)

Diagram procesu plánovaní znázorňuje Obrázek 5-1 - ISMS Fáze plánování (Zdroj: Prezentace BIS - Doucek)



Obrázek 5-1 - ISMS Fáze plánování (Zdroj: Prezentace BIS - Doucek)

Z pohledu VM se sledují tyto komponenty:

1. aktiva, která se rozdělují do skupin, například: Operační systémy, databáze, aplikace.
2. současné zranitelnosti a hrozby, které jsou dodány z databází zranitelností a expozic (CVE)
3. Zvládání rizik formou patch managementu, který se snaží snížit zranitelnost nebo změnou konfigurace, která sníží expozici.

5.1.3 Fáze dělání (Do)

Věnuje se realizaci naplánovaných činností. Odpovědnost je na projektovém manažerovi. Vzniká plán zvládání rizik, který zahrnuje:

1. Činnosti (včetně jejich cílů a priorit)
2. Omezující faktory
3. Zdroje (personální, technologické, finanční, znalostní a další) (DOUCEK, a další, 2011)

VM se v této fázi provádí, to obnáší skenování zranitelností s určitými zdroji (skenovací nástroj) a znalostmi (databáze zranitelností)

5.1.4 Fáze Kontroly (Check)

V této fázi se vyhodnocují bezpečnostní incidenty, monitoruje se počet, druh a závažnost těchto incidentů, měří se účinnost ISMS, probíhá příprava interních auditů a vypracuje se zpráva o stavu ISMS (DOUCEK, a další, 2011), v kontextu VM to může být například srovnání počtu bezpečnostních incidentů za jednotlivé období.

5.1.5 Fáze Jednání (Act)

Zabývá se zlepšováním ISMS, k tomu využívá vnitřní zpětnou vazbu od účastníků na ISMS. Rovněž hledá nedostatky a jejich možné řešení, to je možné provést dvěma způsoby: opatřením k nápravě, nebo preventivním opatřením. (DOUCEK, a další, 2011)

V kontextu VM můžeme mluvit například o zvyšování relevance využívané databáze zranitelností a expozic, nebo změnu bezpečnostní konfigurace.

5.2 Řízení rizik - Risk management

Řízení rizik je proces, při němž se subjekt řízení snaží zamezit působení již existujících i budoucích faktorů a navrhuje řešení, která pomáhají eliminovat účinek nežádoucích vlivů a naopak umožňují využít příležitosti působení pozitivních vlivů. (SMEJKAL, a další, 2013)

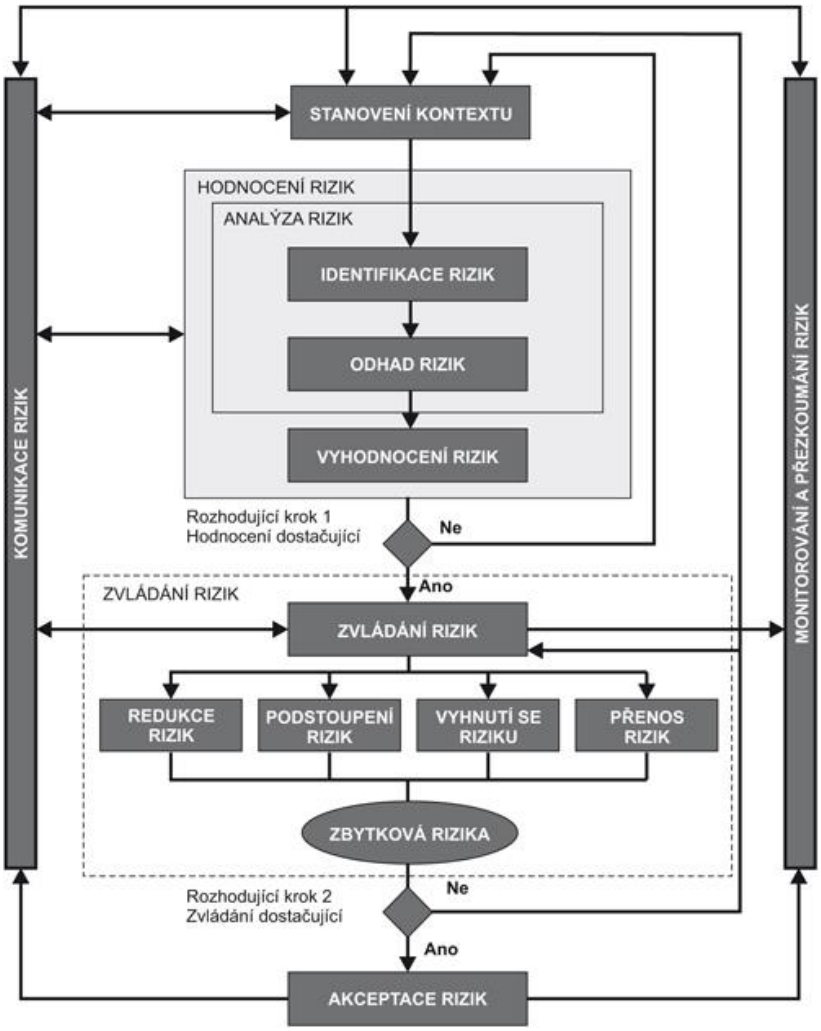
Proces řízení rizik se skládá z těchto činností (DOUCEK, a další, 2011):

- Hodnocení rizik
  - Analýza rizik
  - Vyhodnocení rizika
- Zvládání rizik
- Akceptace rizika

Locke (2011) v publikaci od NIST uvádí tuto definice: Je kontinuální proces, který obnáší tyto úkoly :

1. Definovat (ohraničit) riziko
2. Ohodnotit riziko
3. Reagovat na riziko
4. Sledovat riziko

Norma 27005 znázorňuje proces řízení rizik takto: Obrázek 5-2 - Proces řízeni rizik (Zdroj: www.businessinfo.cz)



Obrázek 5-2 - Proces řízeni rizik (Zdroj: www.businessinfo.cz)

Souvislost s VM se nachází v části identifikace rizik, kdy skenovací nástroj odhalí zranitelnosti. Poté je nutné odhalené zranitelnosti klasifikovat, to odpovídá činnosti vyhodnocení rizik. Když jsou zranitelnosti odhaleny a oklasifikovány, následuje jejich zvládání, v případě VM jsou možné pouze tyto způsoby zvládání:

1. redukce rizika - aplikování patche (záplaty) na zjištěnou zranitelnost
2. podstoupení rizika – o zjištěné zranitelnosti subjekt ví, ale z důvodu nízké kritičnosti, nebo možného ovlivnění dostupnosti/kvality závislých služeb ji nechá bez nápravy.

5.2.1 Kritičnost služby

Určení vztahu komponent (aplikací, hardware, operačních systému) k poskytovaným IT službám je důležitá činnost při následném posuzování kritičnosti služby. ITIL(2010) rozděluje služby do 4 kategorií:

2. Mission Critical – Služba vyžadující nepřetržitý provoz, omezení nebo nedostupnost služby přináší vysoké ztráty, dostupnost musí být zaručena téměř za každou cenu.
    - Příklad: Výběr z bankomatu, Realizace nákupních a prodejních příkazů na burze.
3. Business Critical – Krátké přestávky v dostupnosti jsou přístupné, zákazník je ovlivněn.
    - Příklad: Internetové bankovnictví
4. Business Operational – neovlivňují přímo zákazníka, slouží pro vnitřní potřeby organizace.
    - Příklad: Reporting, elektronická pošta uvnitř organizace.
5. Administrative Services – Služby, které lze v případě nedostupnosti snadno nahradit. Ovlivňují jednotlivce uvnitř organizace.
    - Příklad: Zpomalení koncového zařízení (desktopu), kancelářské aplikace.

5.2.2 Common Vulnerability Scoring System (CVSS)

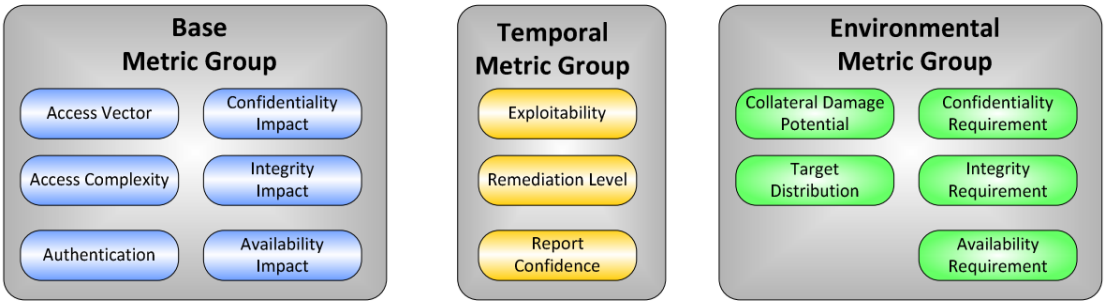
Metodika pro hodnocení dopadů zranitelností, je implementován do CVE. Skládá se ze tří kategorií, jejichž vyhodnocení dává konečné skoré (score) hodnocené zranitelnosti viz Obrázek 5-3. Smyslem jednotné metodiky pro hodnocení dopadů zranitelnosti je umožnit subjektům využívající IT infrastruktůru, jasné a porovnatelné měřítko k hodnocení závažnosti zranitelností. Mezi hlavní výhody použití CVSS patří:

1. Standardizované hodnocení zranitelností – část ohodnocení (score) je vztažena na konkrétní prostředí, ve kterém se zranitelnost může projevit
2. Otevřená a jasně definovaná metodika – Pokud je vydáno ohodnocení zranitelnosti organizací, která je ohodnotila pomocí neveřejné metodiky, tak takové ohodnocení ztrácí na důvěryhodnosti a jiná organizace může přijít s odlišným ohodnocením.
3. Určení priorit při nápravě zranitelností- část hodnocení je určena v kontextu organizace. (Mell et al. 2007)

Metodika rozděluje hodnocení do tří skupin:

1. Base (Základní) – Položky této skupiny jsou hodnoceny primárně výrobci daného systému, případně bezpečnostním analytikem firmy působících v oblasti bezpečnosti IT.
2. Temporal (Proměnlivé) – Tyto položky se mění v čase. Do této skupiny patří:
    - Exploitability (Zneužitelnost) – Dostupnost technik ke zneužití zranitelnosti (dostupnost postupů, škodlivý kód)
    - Remediation Level (Úroveň nápravy) – Krátce po objevení, neexistuje většinou žádná možnost nápravy (Patch.,Fix), po určité době vznikne Workaround (neoficiální dočasné řešení), poté Temporary Fix (dočasná záplata), pokud se výrobci podaří odstranit vzniklou zranitelnost, vydá Official Fix/Patch (Oficiální záplata)
    - Report Confidence (Jistota existence zranitelnosti) – Hodnotí, zdali zranitelnost opravdu existuje, čeká se na potvrzení výrobce systému, kde se vyskytla.
3. Environmetal (Okolí)

- Collateral Damage Potential (Potenciál škody) – zdrojem tohoto měřítka může být například klasifikace aktiv podle jejích kritičnosti v návaznosti na podporované IT služby
- Target Distribution (Procentní zastoupení cílů v organizaci)
- Confidentiality (důvěrnost) – riziko získání přístupu důvěrným údajům
- Integrity (integrita)- riziko neuprávněné změny dat
- Availability (dostupnost) - riziko omezení dostupnosti



Obrázek 5-3 - Common Vulnerability Scoring System (Zdroj: www.first.org/cvss, 2007)

5.3 Policy management – Řízení pravidel

Systém pravidel, směrnic, norem pro řízení podnikové informatiky, zejména pravidel provozování podnikové informatiky, zajištění bezpečnosti, pro řízení projektů apod. (MBI, 2015)

Cobit (2015) uvádí policy management jako vývoj a správu pravidel k podpoře IT strategie. Tyto pravidla by měla zahrnovat[4] :

1. Cíl, který podnik sleduje
2. Role v organizaci
3. Odpovědnosti
4. Proces přidělování výjimek
5. Přístup k řešení shody s pravidly (Compliance approach)
6. Odkazy na standardy, pokyny a jiné závazné dokumenty

Příklady pravidel v originále „Policy“

a. Standardní konfigurace aplikačních, databázových nebo webových serverů.
b. Pravidla na složitost a interval změny hesla uživatelů, správců.
c. Pravidla pro aktualizaci aplikací, neboli „Patchování“

Dodržování policy v kontextu informační bezpečnosti je možné provádět automatizovanými nástroji jako je například Microsoft Security Compliance Manager.

5.3.1 Checklist

S Checklistem se lze setkat v mnoha oblastech lidské činnosti:

- Seznam položek, které je potřeba nakoupit
- Před vzletová kontrola, prováděná piloty dopravních letadel
- Postup instalace operačního systému na koncové stanice v prostředí podniku

U všech checklistů, jejichž nesplnění může mít fatální následky na lidský život (např. před vzletová kontrola), nebo představuje riziko pro podnik, je vhodné se při jejich definici inspirovat autoritou, která má s vybranou problematikou dlouholeté a prokazatelné zkušenosti. Autoritou v oblasti checklistů je Americká státní agentura NIST spravující National Vulnerability Database. NVD je databáze standardů/pravidel pro určování zranitelností systémů. Tato data umožňují automatizovat správu slabých míst, měření zabezpečení a dodržování předpisů. NVD zahrnuje databáze bezpečnostních kontrolních seznamů, softwarové chyby související s bezpečností, chyby konfigurace, názvy produktů a metrik k měření dopadu zranitelností. (NIST, 2009)

[4] Develop and maintain a set of policies to support IT strategy. These policies should include policy intent; roles and responsibilities; exception process; compliance approach; and references to procedures, standards and guidelines. Their relevance should be confirmed and approved regularly. (COBIT, 2015)

Další možností je využít přímo aplikaci od výrobce, pro produkty společnosti Microsoft je to Microsoft Security Compliance Manager (na začátku roku 2015, byla dostupná verze 3.0), podrobný popis je v kapitole 6.10.1. Další možností je využití standardů FISMA nebo USGCB.

5.3.1.1 Security Content Automation Protocol (SCAP)

Je soubor pravidel vytvářených komunitou pro zjišťování zranitelností. Protokol SCAP je definován XML schématem, jsou zde i některé pokročilé kontroly, které zajišťuje Schematron. Konkrétní checklisty jsou zapsané v XML souboru, který je validní vůči použitému schématu, aktuální verze na začátku roku 2015 je 1.2. (NIST, 2009)

SCAP obsahuje tyto standardy (NIST, 2009):

1. SCAP Content Validation Tool -Nástroj umožňující kontrolu XCCDF dokumentů, zdali odpovídají schématu a tím i normě NIST SP 800-126.
2. XCCDF -The Extensible Configuration Checklist Description Format – standardy pro tvorbu checklistů.
3. OVAL: Open Vulnerability and Assessment Language -Obsahuje pravidla a jejich popis.
4. OCIL: Open Checklist Interactive Language - Standard k tvorbě otázek ohledně bezpečnosti systémů pro pracovníky bez znalostí IT bezpečnosti.
5. ARF: Asset Reporting Format - Standard pro výměnu informací o zdrojích (komponentách)
6. CCE: Common Configuration Enumeration - jednoznačný identifikátor konfigurační položky systému.
7. CPE: Common Platform Enumeration - jednoznačný identifikátor aplikace/systému.
8. CVSS: Je otevřený standard pro hodnocení zranitelností. SCAP využívá tuto metodiku pro určení vah (weight) jednotlivých pravidel v checklistech.
9. CCSS: Common Configuration Scoring Systém - standard pro hodnocení kritičnosti způsobené špatnou konfigurací
10. TMSAD: Trust Model for Security Automation Data – Standard zajišťující integritu SCAP protokolu.
11. CVE: Common Vulnerabilities and Exposures – standard pro vydávání hlášení o zranitelnostech a expozicích.

Základní struktůra checklistu XCCDF

Ukázky dokumentu viz příloha 10.1 Ukázka profilu, hodnoty a pravidla podle SCAP

XML dokument se skládá z:

1. Rule (Pravidlo)
    - Popisuje konkrétní pravidlo s referencí na value
2. Profile (Profil)
    - Umožňuje propojit pravidlo s hodnotou
3. Value (Hodnota)
    - XML element, kde jsou uloženy všechny dostupné hodnoty
    - Příklad: Počet pokusů se špatně zadaným heslem, kdy dojde k zamčení účtu.

5.4 Configuration Management - Řízení konfigurací

Podle ITIL definuje tyto základní pojmy:

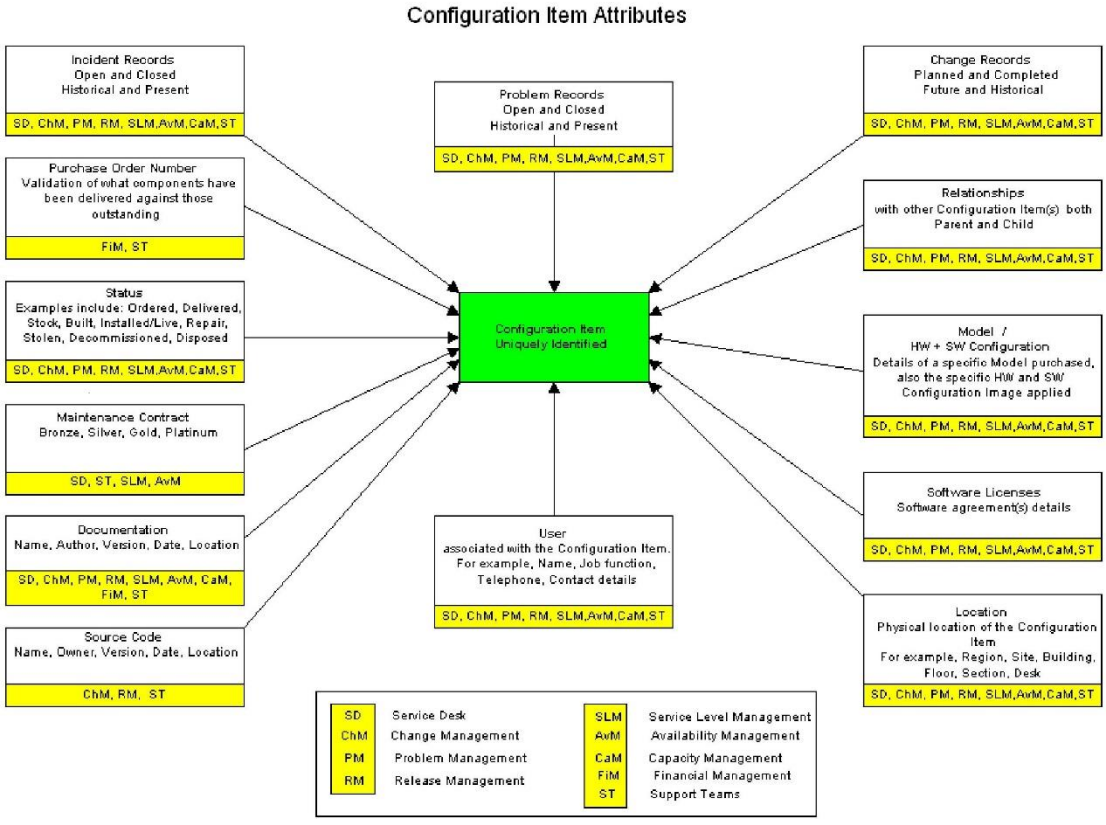
5.4.1 Asset (Zdroj)

Každý zdroj nebo schopnost, která se podílí na dodávce IT služby.

Typy: řízení, organizace, proces, znalost, lidé, informace, aplikace, infrastruktura, kapitál.

5.4.2 Configuration item (Konfigurační položka)

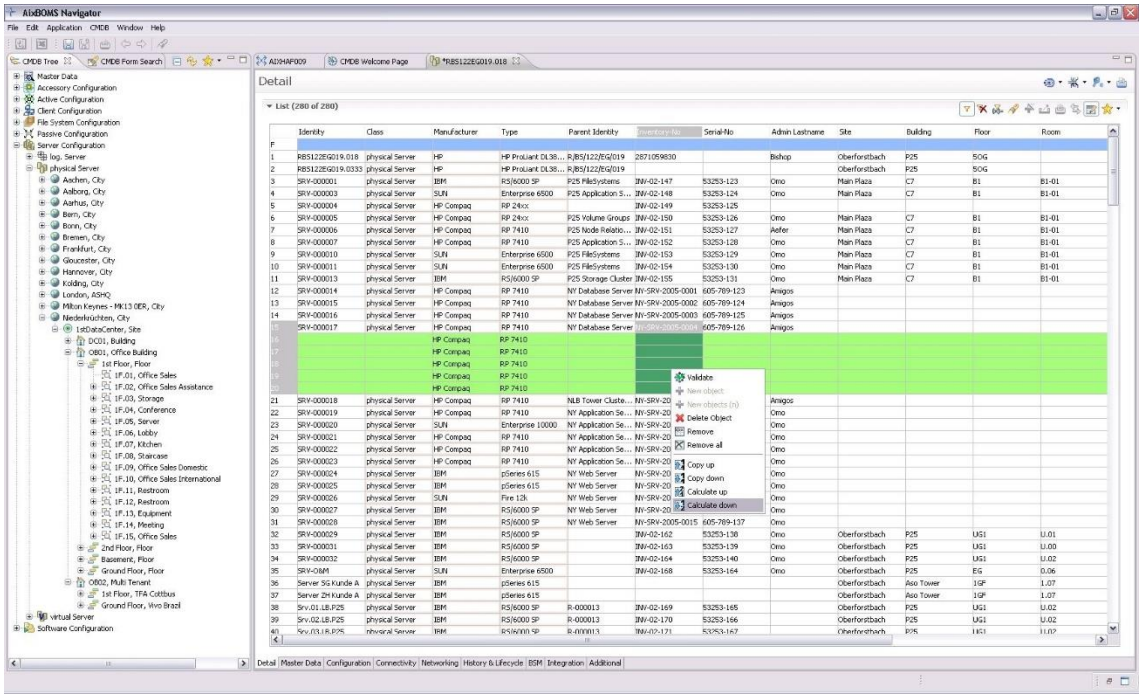
Je základní položka Configuration Managementu, vzniká zaznamenáním Asset (Zdroje) do configuration management database (Databáze konfiguračních položek). Obrázek 5-4 uvádí příklad atributů, které se vážou na konfigurační položku.



Obrázek 5-4 - ITIL Configuration Management - Configuration Item Attributes (Zdroj: http://www.itilnews.com/)

5.4.3 Configuration management database (Databáze konfiguračních položek)

Podle ITIL (2010) je Configuration management database databáze umožňující uložení konfiguračních záznamů během jejich životního cyklu. Pokud se nad databází vytvoří, nebo koupí aplikace, jedná se o Configuration Management System (Systém správy konfigurací). Příklad uvádí Obrázek 5-5.



Obrázek 5-5 - AixBOMS Configuration Management (Zdroj: www.aixpertsoft.de)

5.4.4 Souvislost v VM

Databáze konfiguračních položek obsahuje záznamy (konfigurační položky) všech komponent (aplikací, zařízení) používaných a vlastněných danou organizací, tuto databázi lze naimportovat do VM nástrojů jako seznam IP adres. Vhodné je pokud nástroj umožňuje určení kritičnosti daného aktiva (komponenty).

5.5 Incident management (IM) - Řízení incidentů

5.5.1 Incident

ITIL označuje incident jako neplánované přerušení dostupnosti dodávané IT služby, nebo snížení její kvality (AXELOS, 2011) rovněž může incident vyvolat událost (event), která předznamenává přerušení dostupnosti dodávané IT služby, nebo snížení její kvality. Například zvýšení teploty pevných disků nad 60 °C. Výstupem skenovacího nástroje je při splnění definované kritičnosti zjištěné zranitelnosti incident.

5.5.2 Proces IM

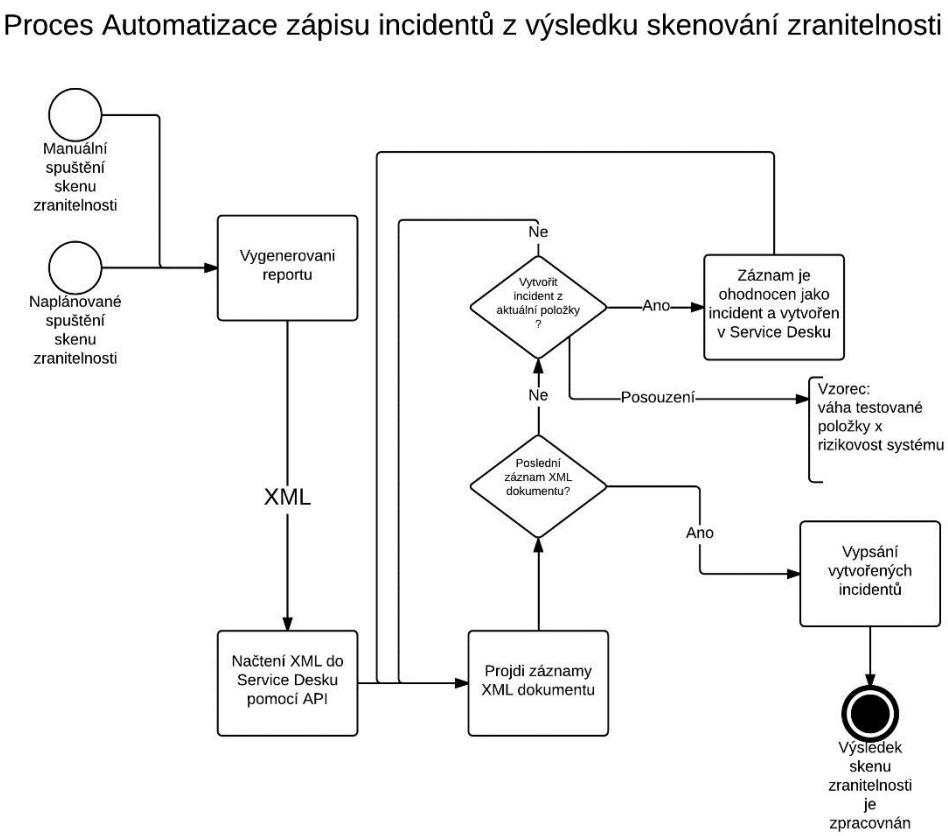
Žďára (2012) uvádí přehled činností IM takto:

1. Identifikaci – Rozpoznání přerušení dostupnosti nebo snížení kvality poskytované IT služby
2. Zaznamenání – Provedení záznamu incidentu do systému na jejich správu.
3. Určení naléhavosti – Zařazení incidentu do jedné ze tří kategorií, podle nárůstu způsobených škod v čase nedostupnosti IT služby.
    a. Vysoká – velice rychlé zvyšovaní škody v čase
    b. Střední – značné zvyšovaní škody v čase
    c. Nízká – mírné zvyšovaní škody v čase (STEFAN, 2013)
4. Určení dopadu - Zařazení incidentu do jedné ze tří kategorií, podle dopadu na uživatele IT služby, lze rozlišovat podle počtu ovlivněných osob, finanční ztráty, či jiných ukazatelů. Jednotlivé kategorie
    a. Vysoká – Je ovlivněna pobočka
    b. Střední – Je ovlivněno oddělení
    c. Nízká – Je ovlivněn jeden, nebo několik zaměstnanců (STEFAN, 2013)
5. Eskalaci – přesun incidentu na vyšší stupeň podpory, například z 1. Úrovně - Service Desk na 2. Úroveň – Aplikační podpory
6. Řešení – Akce vykonaná pro nápravu, nebo dočasné řešení incidentu.
7. Uzavření incidentů – Oznámení zadavateli incidentu o jeho vyřešení.

5.5.3 Souvislost s VM

Skenovací nástroje produkují zjištěné zranitelnosti, AXELOS Best Practice (2011) tuto činnost označuje na vznik události, které se po překročení definovaného stupně rizika dají označit za vznik incidentu. Z důvodu úspory času, je vhodné využití automatizované zadávání incidentů. Například Nexpose umožňuje správu incidentů přímo ve skenovací aplikaci, rovněž je možné naplánování zasílání mailového upozornění při zjištění zranitelnosti, tyto zprávy lze přesměrovat na service desk, který disponuje funkcionalitou automatického založení incidentu z došlého mailu.

Dodavatelé aplikací na správu incidentů umožňují doprogramováni další funkcionality pomocí Application Programming Interface (API), Obrázek 5-6 znázorňuje proces umožňující automatizovaný zápis incidentů na základě výsledku skenování.



Obrázek 5-6 - Proces Automatizace zápisu incidentů z výsledků skenování zranitelnosti (Zdroj: Autor)

5.6 Patch management – Řízení záplatování

5.6.1 Patch – fix – hotfix

Mell (2005) uvedí zaměnitelnost termínů patch, fix a hotfix, aplikování bezpečnostní záplaty opraví zranitelnost, záplata obsahuje kód, který modifikuje (mění) program aplikace k odstranění problému. [5]

5.6.2 Definice NIST

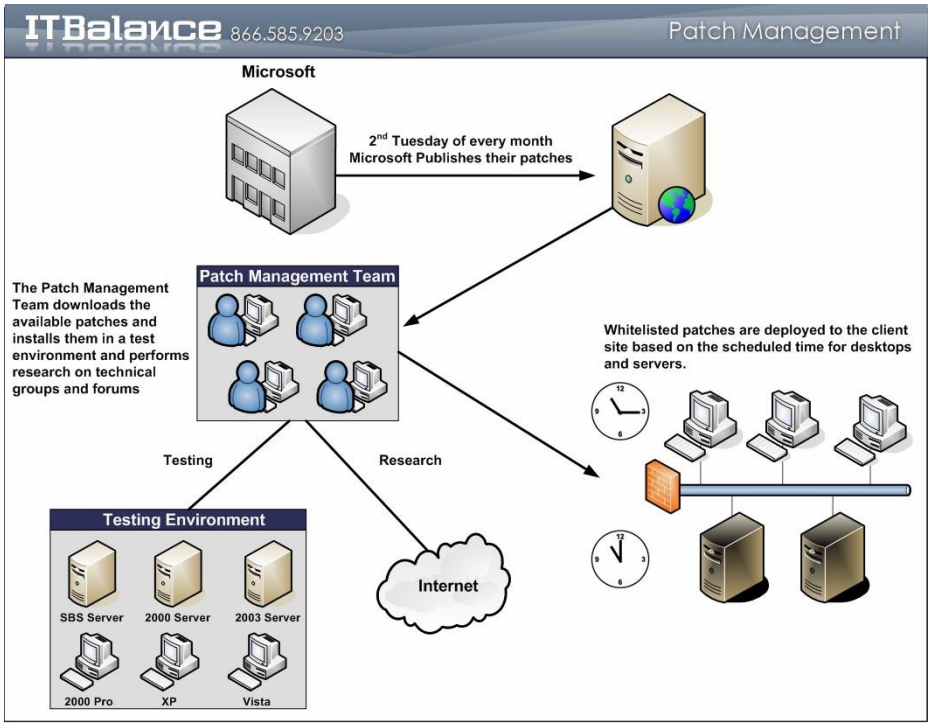
Patch management je proces pro identifikaci, získávání, instalaci a kontrolu záplat (patch, fix) softwarových produktů a systémů. Patch napravuje bezpečnost a problémy ve funkcionalitě SW a firmware[6] (SOUPPAYA, a další, 2013)

5.6.3 Proces patch managementu

Proces začíná vydáním záplaty výrobcem záplatované aplikace, tým nebo zaměstnance zodpovědný za patch management provede stažení záplat a v testovacím prostředí tyto záplaty nasadí a zjišťuje, jestli je zachována původní funkcionalita ve stejné nebo vyšší kvalitě. Pokud záplata úspěšně projde testováním, je nasazena na produkční systémy/aplikace.

[5] „Applying a security patch (also called a “fix” or “hotfix”) repairs the vulnerability, since patches contain code that modifies the software application to address and eliminate the problem“ (MELL, a další, 2005)

[6] „Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Patches correct security and functionality problems in software and firmware.“ (SOUPPAYA, a další, 2013)



Obrázek 5-7 - Patch management proces (Zdroj: www.itbalance.com)

5.6.4 Souvislost s VM

Poté, co se výrobce aplikace dozví o objevené zranitelnosti, vydá s určitým zpožděním záplatu, která danou zranitelnost odstraní, nebo alespoň zmírní její případná dopad. Záplatování je metoda vedoucí k vyřešení vzniklého incidentu

6. Praktická část

Praktická část se skládá ze dvou částí:

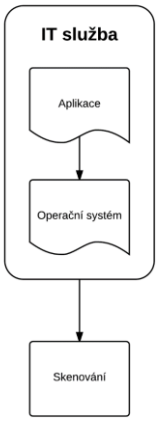
1. Analýza zadaného problému: Určení kritičnosti (severity) zjištěných zranitelností ve vztahu k dodávaným IT službám
2. Srovnání nástrojů pro skenování zranitelností

6.1 Určení kritičnosti zjištěných zranitelností ve vztahu k dodávaným IT službám

Navrhnout metodiku skenování zranitelností zohledňující tyto faktory:

1. Poskytovaná IT služba
    - Kritičnost skenovaných komponent je závislá na kritičnosti podporované IT služby
    - Reporting, Konsolidace, Provoz banky (platby, účty) a další
2. Komponenta Operační systém
    - Windows Server 2008 R2, Fedora 22e, CentOS 7 a další
3. Komponenta Aplikace
    - Oracle 11g, Internet Explorer 11, Office 2010 a další

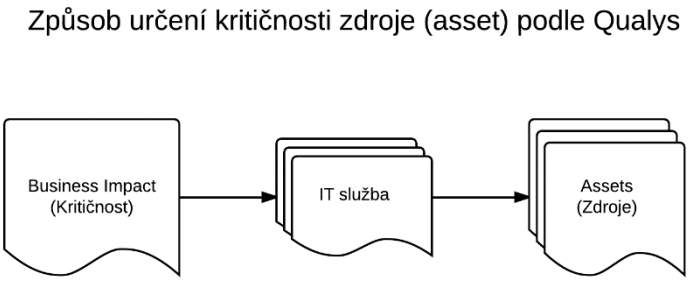
Obrázek 6-1 - IT služba a její komponenty (Zdroj: Autor) znázorňuje tento problém jako informační vstup vstupující do procesu skenování. Smyslem klasifikace zranitelností je snížit množství nerelevantních výsledků vrácených skenováním. Například je vhodné určit, které zranitelnosti nejsou závažné u testovacího serveru oproti těm, na které by se měl brát zřetel i v testovacím prostředí.



Obrázek 6-1 - IT služba a její komponenty (Zdroj: Autor)

6.2 Řešení

V publikaci Vulnerability Management (QUALYS, 2008) se uvádí postup určení kritičnosti zdrojů, prostřednictvím poskytovaných služeb viz Obrázek 6-2. Touto funkcionalitou disponuje například nástroj Nexpose počínaje verzí Community edition.



Obrázek 6-2 - Určeni kritičnosti zdrojů přes služby (Zdroj: Qualys.com)

V J&T Bance bylo navrženo vytvořit matici aplikace x operační systém, uvnitř matice by se pak nacházelo označení konkrétního checklistu (sada kontrolovaných zranitelností), tato myšlenka by způsobila neúměrné množství práce pro odpovědné pracovníky, protože nové zranitelnosti vycházejí každý den a není v kompetenci pracovníka aby posuzoval, které zranitelnosti zařadit do skenování. Skenovací nástroje automaticky vyberou skenované zranitelnosti k určeným cílům, pracovník po skončení testu vyhodnotí, které jsou v kontextu dodávaných IT služeb relevantní.

Rozdělením služeb do 4 kategorií (ITIL, 2010) lze získat podklad pro přidělení odpovídajících kategorií v případě Nexpose (very high, high, medium, low, very low), přičemž kategorii low a very low spojím do jedné low:

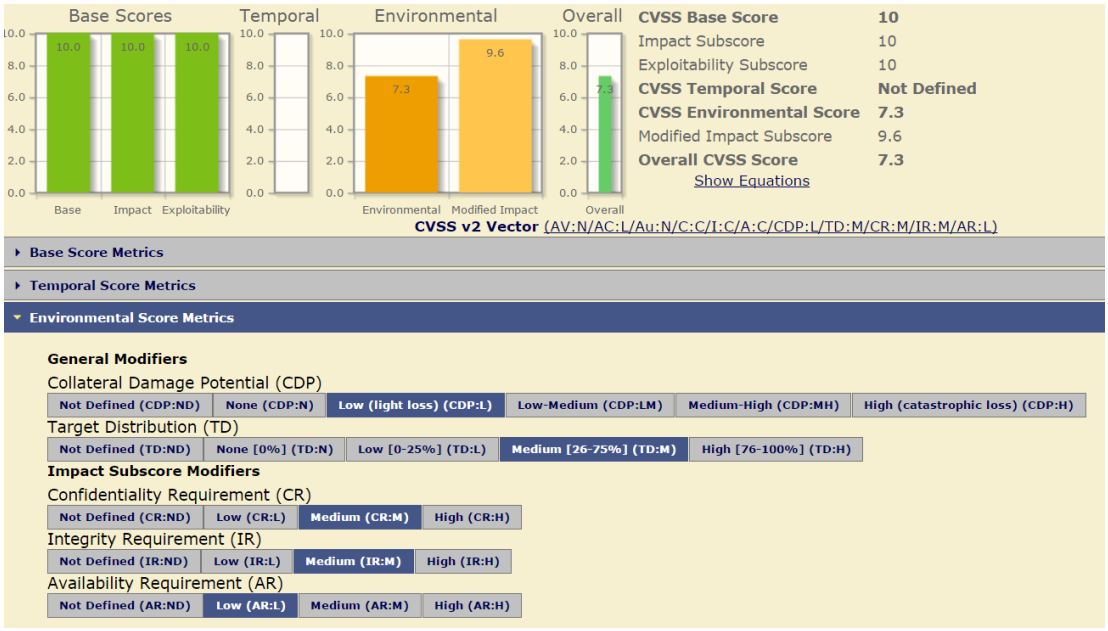
1. Mission Critical (very high) – Služba vyžadující nepřetržitý provoz, omezení nebo nedostupnost služby přináší vysoké ztráty, dostupnost musí být zaručena téměř za každou cenu.
    - Příklad: Výběr z bankomatu, Realizace nákupních a prodejních příkazů na burze.
2. Business Critical (high) – Krátké přestávky v dostupnosti jsou přístupné.
    - Příklad: Internetové bankovnictví
3. Business Operational (medium) – neovlivňují přímo zákazníka, slouží pro vnitřní potřeby organizace.
    - Příklad: Reporting, elektronická pošta uvnitř organizace.
4. Administrative Services (low) – Služby které lze v případě nedostupnosti snadno nahradit. Ovlivňují jednotlivce uvnitř organizace.
    - Příklad: Zpomalení koncového zařízení (Desktopu), Kancelářské aplikace

Nástroj Nexpose i ve verzi community umožňuje určení kritičnosti zdrojů (komponent), tato funkcionalita není konzistentní, při změně kritičnosti celé komponenty se změna ve většině případů nepropíše na jednotlivé zranitelnosti.

6.2.1 CVSS

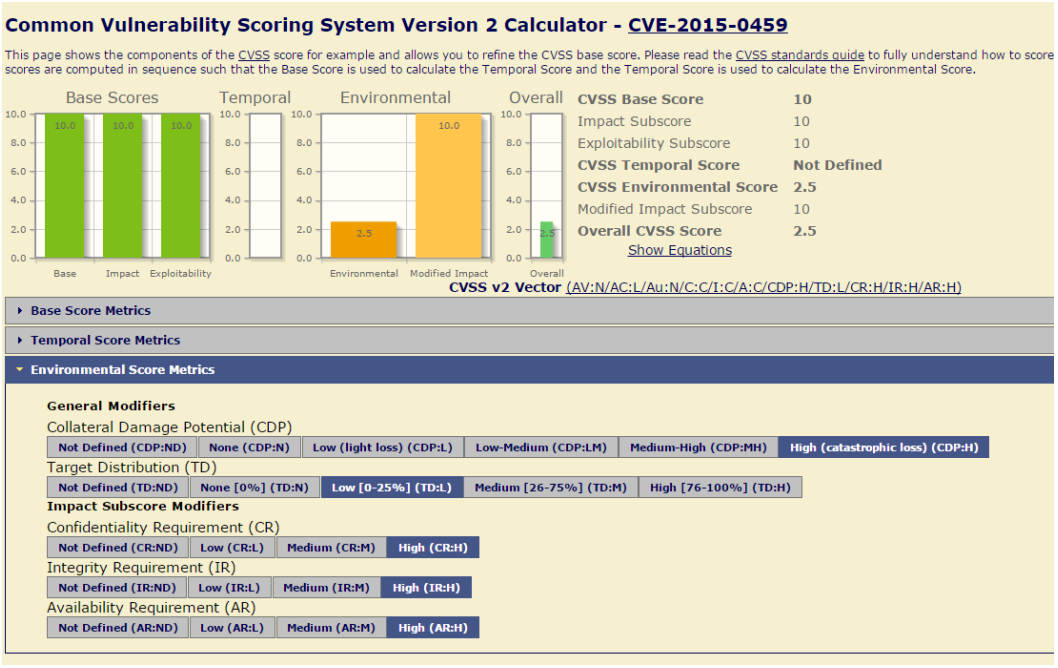
Použití této metodiky obnáší přepočítat skoré každé zjištěné zranitelnosti. Z výsledků přepočtu je zřejmé, že metodika není vhodná pro užití v kontextu kritičnosti služby. Pro názornost provedu přepočet pro tyto zranitelnosti CVE-1999-0535 a CVE-2015-0459

Account policy (Politika účtů) CVE-1999-0535 tato zranitelnost byla přidána do standardu CVE roku 1997. V databázi NVD má základní score 10. Dopočítáním Environmental score lze získat kritičnost v kontextu IT služby/Zdroje na kterém byla nalezena. Výsledek přepočtu je vidět na Obrázek 6-3 - Přepočet CVSS. Výsledné score pokleslo na 7.3 bodu.



Obrázek 6-3 - Přepočet CVSS (Zdroj: Autor)

Obrázek 6-4 ukazuje přepočet zranitelnosti CVE-2015-0459 pro mission critical komponentu, nevhodnost této metodiky je vidět na poklesu score z 10 na 2,5, pouze tím, že se snížil podíl výskytu komponent s danou zranitelností na low. Tento negativní efekt se pokusím vyřešit použitím pouze modifikátoru Collateral Damage Potencial (CDP), změna CDP z not defined postupně na hodnotu none, low, medium a high nevedla ke snížení výsledného score, to je v případě mission critical komponenty v pořádku. Pokud se stejná zranitelnost nachází se na komponentě s nízkou kritičností, přepočet nezabráni zbytečnému poplachu. Impact Subscore Modifiers mají na výsledné score minimální vliv, jejich nastavení z not defined na low sníží score o 0,2 bodu, změna na hodnotu high score nezvýší.



Obrázek 6-4 - Přepočet CVSS, mission critical (Zdroj: Autor)

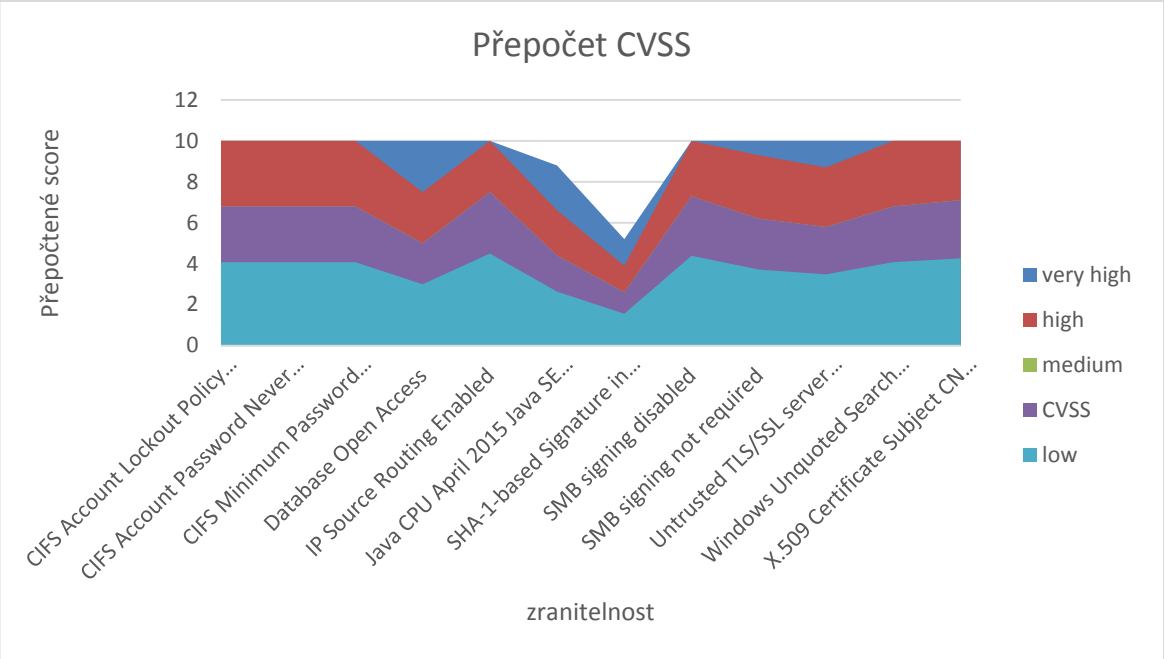
6.2.1 CVSS score v kontextu kritičnosti IT služby

Z tohoto důvodu jsem vytvořil vlastní vzorec pro výpočet CVSS v kontextu rizikové kategorie. Výpočet vypadá následovně: CVSS score, získané ze skenování, či NVD, vynásobím jedním z koeficientů (2; 1, 5; 1; 0,6), v případě, že by vyšlo číslo vyšší než 10, za výsledné score dosadím 10 viz Obrázek 6-5. Koeficienty i jednotlivé rizikové skupiny lze měnit.

koeficient	2	1,5	1	0,6
CVSS base + temporal	very high	high	medium	low
10	10	10	10	6
5,5	10	8,25	5,5	3,3
2	4	3	2	1,2
0	0	0	0	0

Obrázek 6-5 - CVSS vlastní přepočet (Zdroj: Autor)

Přepočet jsem aplikoval na vybrané zranitelnosti ze skenování v Nexpose (všechny zjištěné zranitelnosti měly uvedené CVSS). Výsledek znázorňuje Obrázek 6-6, fialovou barvou je znázorněno vstupní CVSS score, které se překrývá s přepočteným v kategorii medium. Váhy byly nastaveny stejně, jak ukazuje Obrázek 6-5



Obrázek 6-6 - Přepočet CVSS, pro zjištěné zranitelnosti (Zdroj: Autor)

6.3 Srovnání nástrojů pro skenování zranitelností

Z interních důvodů mi nebylo dovoleno porovnat nástroje v infrastruktuře banky, proto budu skenování provádět na své infrastruktuře skládající se z Windows 7 64Bit Service Pack 1 English a routeru Comtrend VR-3026e.

Metodiku pro hodnocení nástrojů jsem zvolil takto:

1. Na výsledky skenování byla aplikována metoda váženého součtu
2. Testované cíle: Windows 7 64Bit Service Pack 1 English, router Comtrend VR-3026e
3. Uživatelská přívětivost, stabilita aplikace – tato část nevstupuje do celkového pořadí nástrojů.

Testování provádím na stanici v této konfiguraci:

- Procesor: AMD Vishera FX-6300 3,5Ghz (6 jader)
- Operační paměť: 8GB DDR3
- Operační systém: Windows 7 64Bit English

Podmínky skenování:

1. Skenování se zadanými přihlašovacími údaji k cílovému zařízení/aplikaci s administrátorským přístupem
2. Full scan (skenuji všechny dostupné zranitelnosti podporované nástrojem)
3. Pro zdárné skenování u všech nástrojů bylo vyvinuto maximální úsilí, to obnášelo čtení dokumentace, vyhledávání rad v odborných diskuzích.

Výběr nástrojů

Při výběr nástrojů jsem zohledňoval tyto faktory:

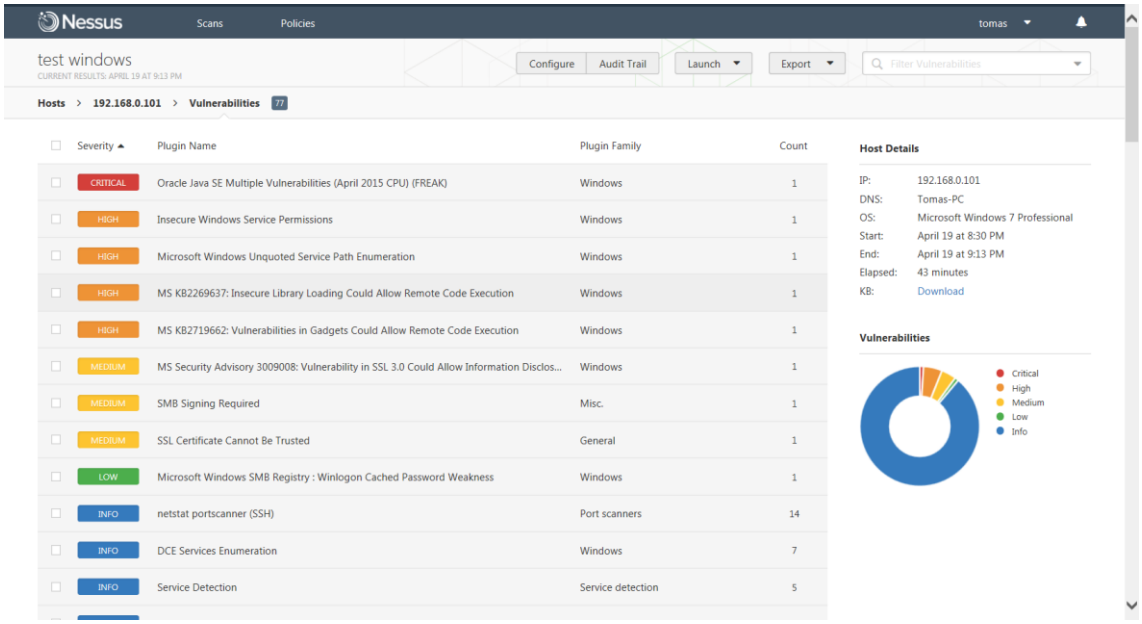
1. Podíl na trhu, Chuvakin uvádí, že v roce 2012 se 80% příjmů za VM nástroje rozdělilo mezi 5 dodavatelů: eEye Digital Security, McAfee, nCircle, Qualys, Rapid7, Tenable (CHUVAKIN, 2012).
2. Komerční řešení jsem rozšířil o Open source nástroje zastoupené produkty OpenVAS.
3. Typ edice jednotlivých nástrojů nemá vliv na počet zjištěných zranitelností. Vyšší edice rozšiřuje funkcionalitu například o:
    a. security configuration assesments, pro tento účel využiji Microsoft Security Compliance Manager z důvodu téměř 90% zastoupení produkty Microsoftu v J&T Bance.
    b. Compliance Audits (PCI DSS, CIS, FDCC, NIST a další) tyto audity nejsou u všech edic nástrojů podporovány, například u Nessusu není možné tuto funkcionalitu získat u verze Professional v testovací verzi, ta je dostupná pouzi při zakoupení nástroje. (NESSUS, 2015)

6.4 Nessus Home 6.3

Komerční sada aplikací sloužící ke skenování zranitelnosti. Nessus používá pro zranitelnost své označení plugin. Přehled pluginů je dostupný přímo v aplikaci i na stránkách výrobce v sekci plugins: http://www.tenable.com/plugins

Instalace kromě výběru místa instalace a potvrzení instalace aplikace Winpcap nevyžaduje žádné další uživatelské zásahy. Winpcap umožňuje číst obsah paketů procházející přes síťové adaptéry používané daným operačním systémem. Po zdárné instalaci se otevře webové rozhraní aplikace, vyzívající k vytvoření uživatelského účtu.

Skenování obnáší pouze zadaní názvu testu a IP adresy zařízení, které chceme skenovat (aplikace umožňuje zadat i rozsahy), dále můžeme zadat administrátorské přihlašovací údaje k testovaným zařízením, deaktivovat některé skupiny pluginů (defaultně jsou použity všechny) a spustit test. Výsledný report lze exportovat do: PDF,HTML,CSV a Nessus DB (vlastní formát Nessusu) nebo zobrazit přímo v aplikaci.



Obrázek 6-7 - Nessus výsledek skenování (Zdroj: Autor)

Vyhodnocení práce s nástrojem

Za klady nástroje považuji:

1. jeho snadnou instalaci a konfiguraci, příjemné uživatelské prostředí
2. Používání není omezenou dobou, ale limitem rozsahu 16 IP adres (lze opakovaně skenovat 16 zařízení v síti, pokud se jim nemění IP adresa)
3. Nessus provedl skenování Systému Windows 7 s přihlašovacími údaji administrátora, jinak by byl ve výsledném report uveden informativní nález „Authentication Failure“ (TENABLE, 2015)

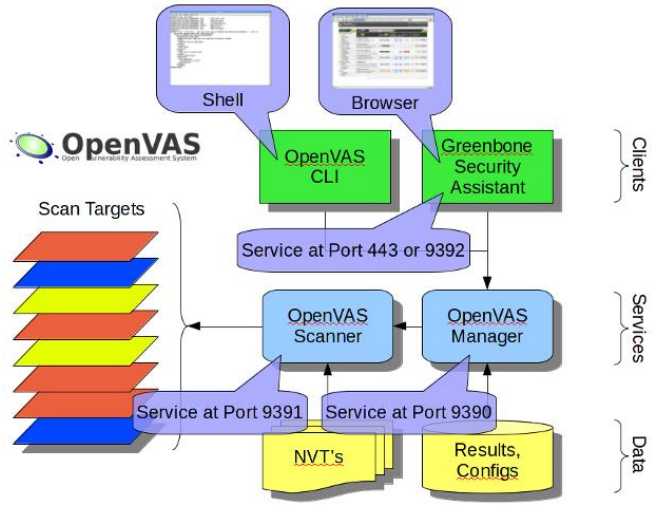
Za slabiny považuji:

1. Počet zjištěných zranitelností je nižší než u konkurence
2. Dokumentace nezmiňuje nic o možnosti klasifikace skenovaných komponent

6.5 OpenVAS 7

Nástroj pod licencí GNU General Public License dostupný na Linuxové systémy, sloužící ke skenování zranitelností. Nástroj tvoří tyto komponenty:

1. OpenVAS CLI - klient komunikující přes OpenVAS Management Protocol (OMP) umožňuje ovládání přes příkazový řádek
2. Greenbone Security Assistant – webový klient komunikující přes OMP
3. OpenVAS Scanner – Skener umožňující skenovat více cílů najednou
4. OpenVAS Manager – centrální služba řídí a spojuje ostatní
5. NVT (Network Vulnerability Tests) – vlastní databáze zranitelností je doplněna o další zdroje, SCAP a CERT. (OPENVAS, 2015)



Obrázek 6-8 - OpenVAS architektůra (Zdroj: openvas.org)

Pro testování jsem použil linuxovou distribuci Kali linux 1.1.0 64Bit, tato distribuce má předinstalovanou celou řadu nástrojů sloužící k testování i prolamovaní bezpečnosti, včetně OpenVAS 7.

Nástroj je nutné nejdříve nakonfigurovat, to se provede skrze příkazový řádek zadáním

```
openvas-check-setup
```

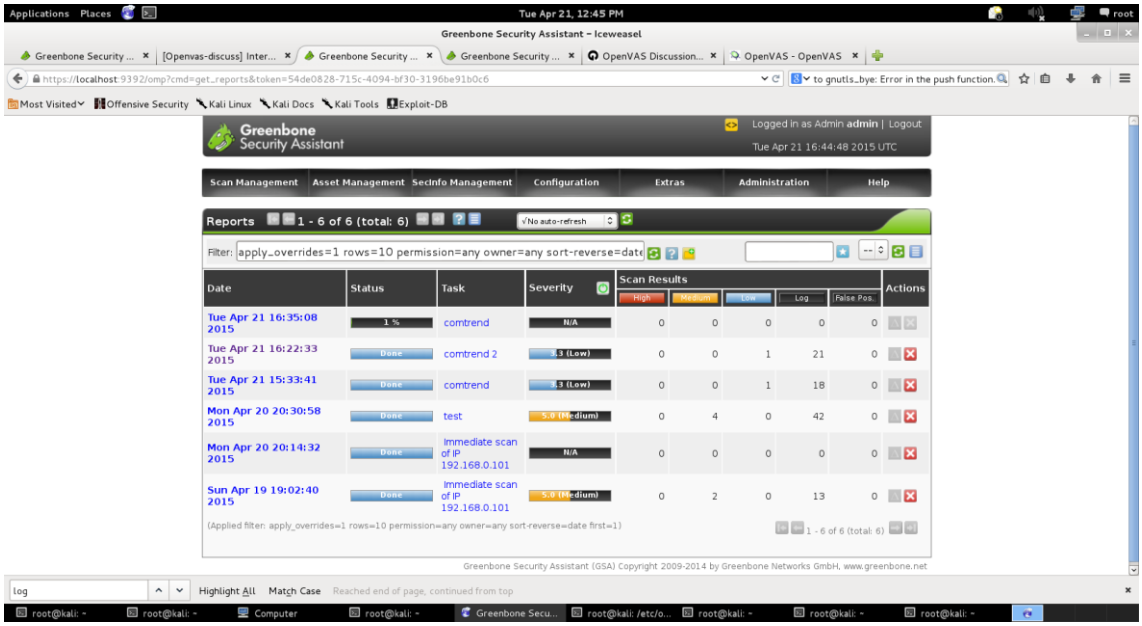
Vrácený výsledek vypadá například takto:

```
ERROR: The number of NVTs in the OpenVAS Manager database is too low.
FIX: Make sure OpenVAS Scanner is running with an up-to-date NVT collection and
run 'openvasmd --rebuild'.
```

Z výsledku je zřejmá chybná konfigurace (ERROR) a způsob její nápravy (FIX).

Grafické rozhraní se pustí přes webový prohlížeč na adrese https://localhost:9392.

Jako první krok byly vytvořeny přihlašovací údaje k testovaným cílům. Tyto přihlašovací údaje byly přiřazeny cíli skenování, ten se definuje podle IP adresy nebo jako více IP adres, oddělených středníky. Poté se v úkolech (Tasks) vytvoří nové skenování s přiřazeným targetem (cílem). Pro porovnatelnost skenování je nastaven Full scan, který při skenování kontroluje všechny dostupné zranitelnosti. Na obrázku Obrázek 6-9- OpenVAS proběhlá skenování (Zdroj: Autor) jsou zobrazená proběhlá skenovaní.



Obrázek 6-9- OpenVAS proběhlá skenování (Zdroj: Autor)

Vyhodnocení práce s nástrojem

Za klady nástroje považuji:

1. jeho snadnou instalaci a konfiguraci, což u linuxových řešení nebývá vždy standardem.
2. Používání není omezenou dobou ani množstvím oskenovaných IP adres
3. Úspěšné skenování systému Windows 7, ale bez přihlášení zadanými přihlašovacími údaji

Za slabiny považuji:

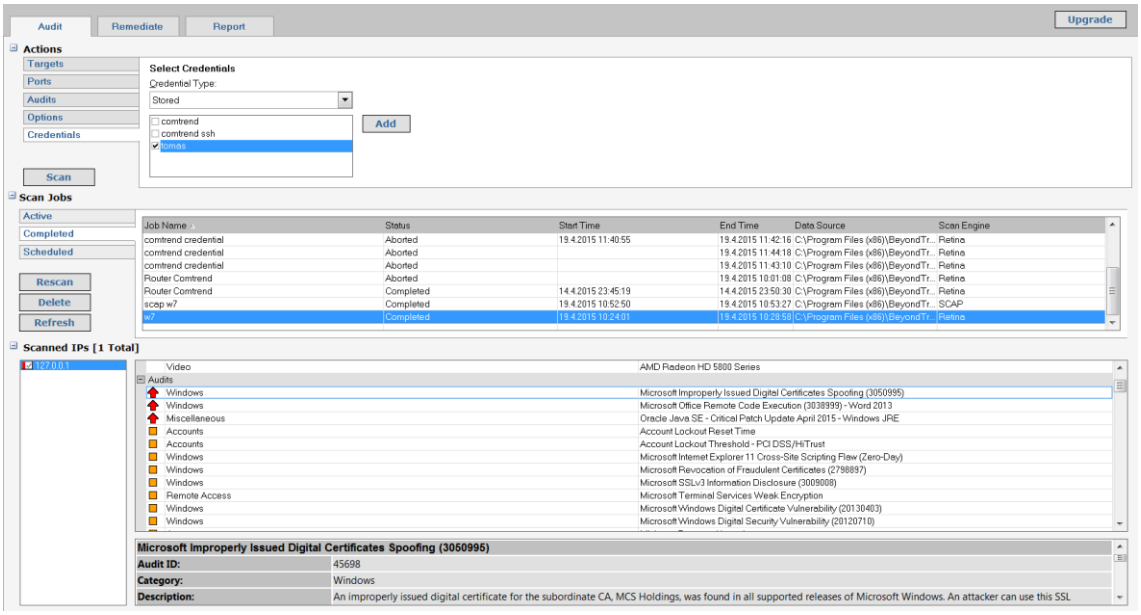
1. Z výsledku testu není zřejmé, zdali bylo přihlášení zadaným jménem a heslem k cílovému systému úspěšné.
2. U routeru Comtrend se výsledek skenování nelišil při použitých přihlašovacích údajích, oproti skenovaní bez nich

6.6 Retina Community 5

Je nástroj od společnosti eEye Digital Security, která byla založena roku 1998.

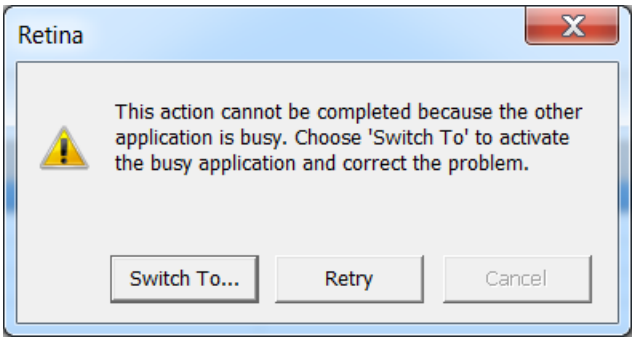
Instalaci byla provedena na Windows 7 64Bit, bez jakýchkoliv komplikací. Po spuštění Retina.exe souboru se aplikace spustí. Pro zahájení skenování je nutné definovat cíle, zadáním IP adresy (rozsahem adres), nebo podle hostname (Jméno zařízení v síti). Poté se vyberou porty ke skenování. V nabídce Audits bylo zvoleno All Audits pro nalezení všech zranitelností. V Sekci Options byly při skenování Microsoft aplikací povoleny volby: Enable Windows Management Instrumentation[7] a Enable Remote Rigistry Service[8]. V Poslední volbě Credentials byly zadány přístupové údaje k administrátorským účtům skenovaných cílů.

[7] Umožňuje přístup k základním informacím o nainstalovaném systému a aplikacích



Obrázek 6-10 - Retina výsledek testu (Zdroj: Autor)

Po provedení testu aplikace umožňuje zobrazit výsledky testu ve formě reportu, otevřením webového prohlížeče nebo aplikací Word. Volba zobrazení ve webovém prohlížeči způsobila zacyklení aplikace s následující chybou Obrázek 6-11



Obrázek 6-11- Retina chyba aplikace (Zdroj: Autor)

Vyhodnocení práce s nástrojem

Nástroj je jednoduchý na ovládání, za výhodu považuji možnost přímé instalace, bez použití virtuálního stroje a schopnost skenování podle SCAP protokolu.

Za slabiny považuji:

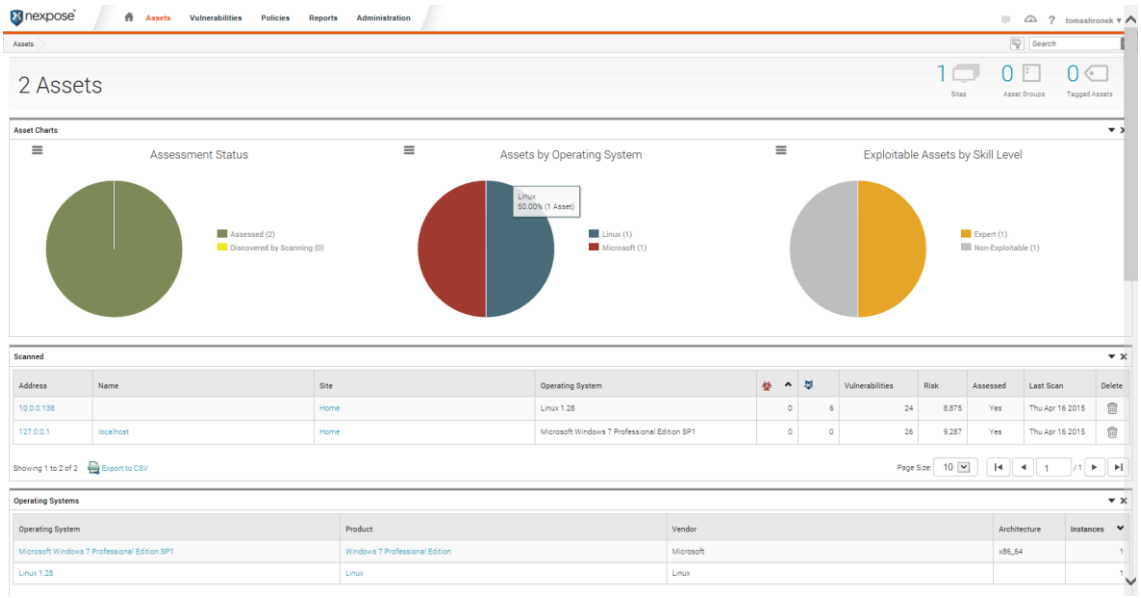
- Občasné pády aplikace
- Autentizované skenování routeru se zastavilo na portu 2583, po hodině trvání skenování, test nedoběhl.
- Nápověda aplikace nezmiňuje nic o možnosti klasifikace skenovaných komponent
- Chybí možnost stažení dokumentace, ta není volně dostupná ani k jiným edicím

[8] Umožňuje vzdálenou správu registrů

6.7 Nexpose Express Edition 5.13

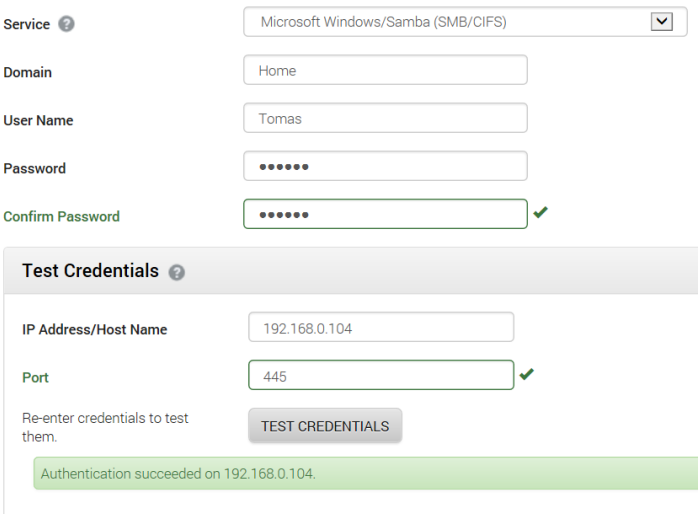
Výrobcem nástroje je společnost Rapid7 založená roku 2000. Tato verze aplikace podporuje pouze funkcionalitu skenování zranitelností, SCA umožňuje až vyšší verze Consultant.

Instalaci byla provedena na Windows 7 64Bit, bez jakýchkoliv komplikací. Aplikace se ovládá skrze webové rozhraní Obrázek 6-12



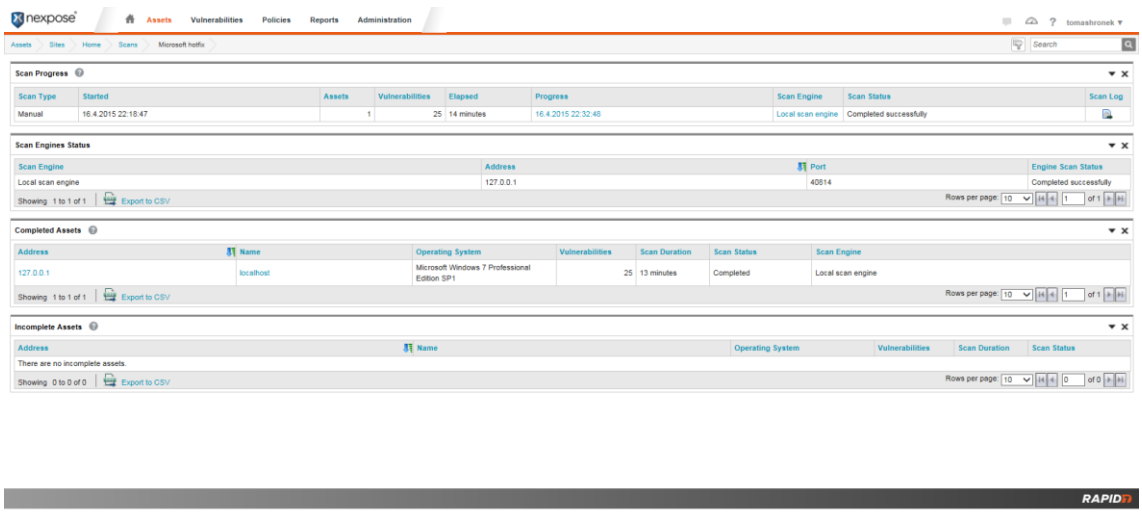
Obrázek 6-12 - Nexpose hlavní obrazovka (Zdroj: Autor)

Při prvním spuštění aplikace je nutné vytvořit skupiny/lokality (Site) a naplnit je zdroji (assets). Po vytvoření skupiny je nutné přiřadit skener, u rozsáhlých sítí je vhodné použít více skenerů pro distribuci zátěže při skenování a omezení počtu firewallů, které mohou blokovat komunikaci nástroje s célem během skenování. (NEXPOSE, 2015) Následuje výběr skenovacího templatu (šablony), která určuje sadu zranitelností k testování. Dalším krokem je zadání přihlašovacích údajů administrátora pro autentizované skenování Obrázek 6-13, poté lze nad aktuální skupinou

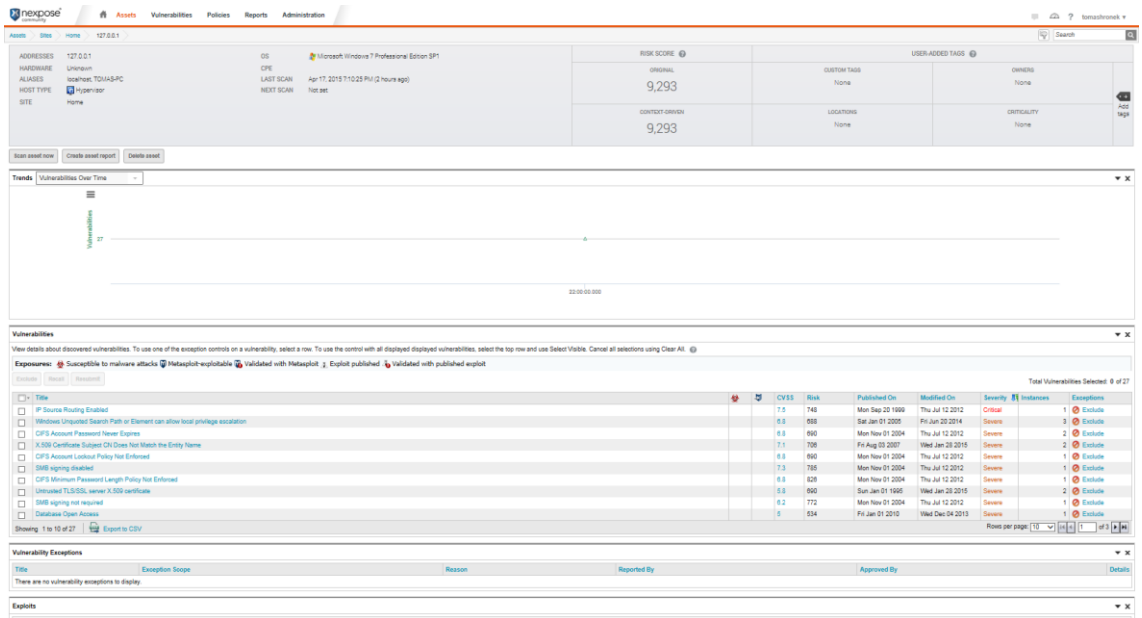


Obrázek 6-13 - Nexpose autentizované skenování (Zdroj: Autor)

spustit skenování. Výsledkem je obrazovka Obrázek 6-14 - Nexpose výsledek skenování (Zdroj: Autor). Bohužel zde nejsou vidět zjištěné zranitelnosti, ty jsou dostupné, pokud se vygeneruje report z tohoto skenování, nebo z obrazovky zdrojů: Obrázek 6-15 - Nexpose zranitelnosti na zdroji (Zdroj: Autor)



Obrázek 6-14 - Nexpose výsledek skenování (Zdroj: Autor)



Obrázek 6-15 - Nexpose zranitelnosti na zdroji (Zdroj: Autor)

Nástroj umožňuje propojení s databází PostgreSQL, to umožňuje integraci s dalšími systémy, nebo vlastní tvorbu reportů.

Reporty lze generovat za jednotlivé proběhlé skenování. Výsledný report může být uložen do PDF, HTML nebo XML souboru. Jeho obsahem jsou statistiky o zjištěných zranitelnostech v kategoriích (kritičnost, výrobce a další). Užitečný je detail jednotlivých zranitelností obsahující CVE (v případě, že existuje) a způsob nápravy, tento report lze následně předat administrátorům k provedení náprav.

Vyhodnocení práce s nástrojem

Za klady nástroje považuji:

1. Přehlednost.
2. možnost přímé instalace, bez použití virtuálního stroje.
3. Možnost přiřazení kritičnosti jednotlivým zdrojům (assets), výsledky této funkcionalita, ale nejsou konzistentní.

Za slabiny považuji:

1. Z vygenerovaného reportu skenování není zřejmé, jaký skenovací template byl použit, to lze zjistit pouze v logu.
2. Nedostupnou databázi zranitelností, ze které se vybírají zranitelnosti do skenovacího templatu. v plné verzi je možné omezit pouze některé kategorie a typy zranitelností:

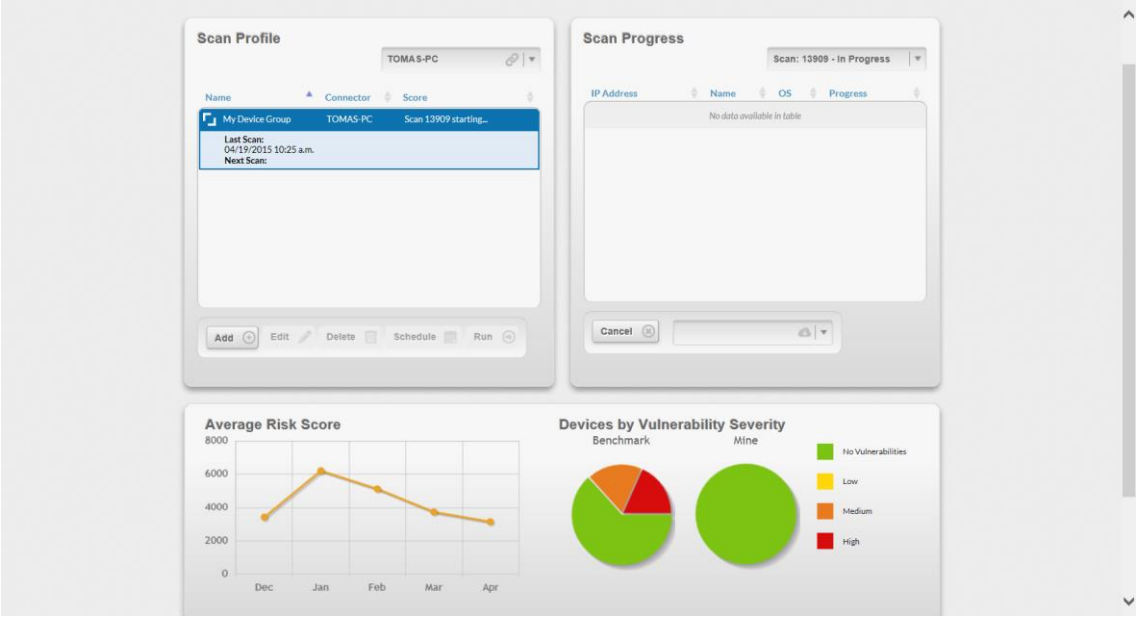
„A scan template may specify certain checks as being disabled, which means that the application will scan for all vulnerabilities except for those vulnerability check types or categories with that template. In other words, if no checks are disabled, it will scan for all vulnerabilities.While the exhaustive template includes all possible vulnerability checks“ (NEXPOSE, 2015)

6.8 Tripwire SecureScan

Společnost Tripwire koupila v roce 2013 výrobce IT bezpečnostních nástrojů nCircle, která před tím poskytovala skenovací nástroj nCircle IP360. Na webu společnosti nejsou dostupné informace o dostupných edicích a funkcionalitě.

Nástroj ke svému ovládání využívá webové rozhraní, skenování provádí pomocí agenta instalovaného do počítače.

Tento nástroj má nejjednodušší uživatelské rozharní z testovaných nástrojů Obrázek 6-16. Práce s nástrojem probíhá následovně: nainstaluje se connector (skenovací agent) do počítače, vybere



Obrázek 6-16 - TripWire rozhraní (Zdroj: Autor)

se IP adresa (rozsah adres), zvolí se zdali budou hledat zranitelnosti (ano/ne), zadájí se administrátorské přihlašovací údaje k testovaným zařízením a spustí se test.

Vyhodnocení práce s nástrojem

Nástroj je přehledný, za výhodu považuji možnost využití skenovacího agenta. Licence neumožnila provést skenovaní routeru Comtrend, z důvodu překročení limit 2 skenů za měsíc.

Za slabiny považuji:

1. Nemožnost volby jaké zranitelnosti se budou testovat.
2. Nejslabší výsledek v testu na hodnocení zranitelností, nástroj nalezl pouze 3 s označením informativní na skenovaném systému Windows 7 64B
3. Report nepravdivě uvádí, že nebyly poskytnuty přihlašovací údaje.
4. Dokumentace není dostatečně detailní.

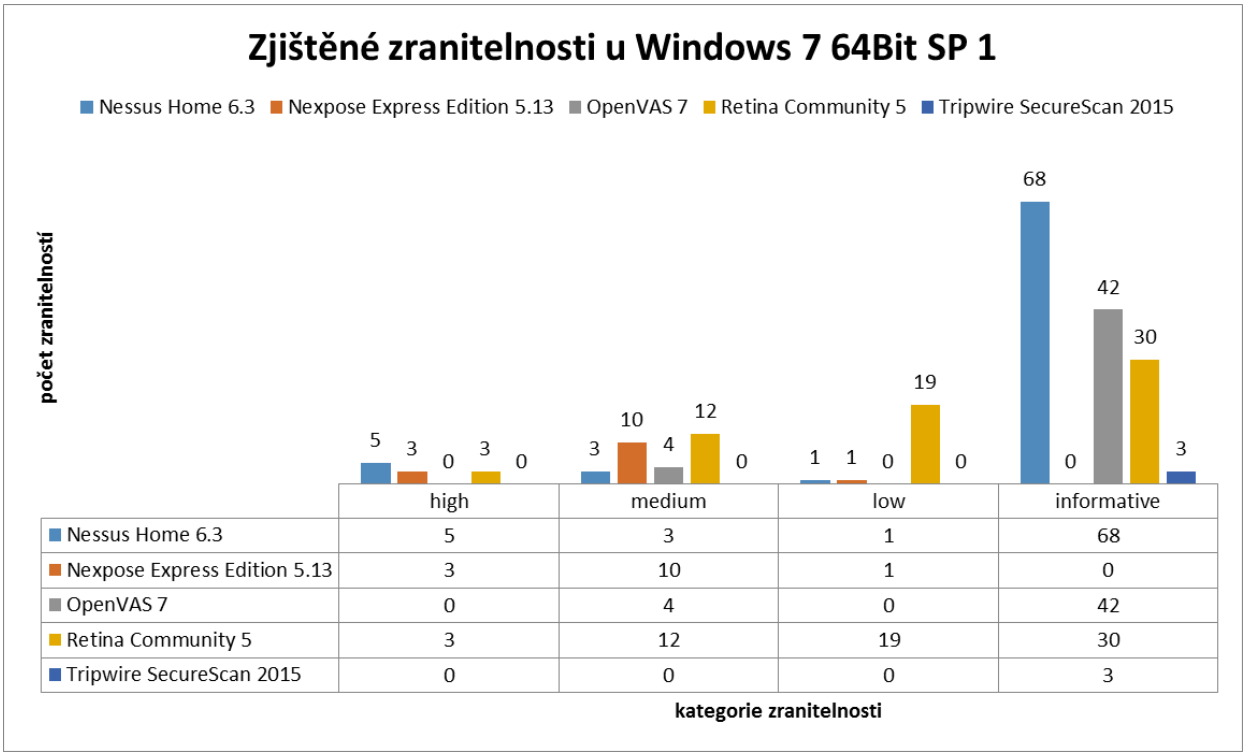
6.9 Srovnání výsledků skenování

Zjištěné zranitelnosti byly rozděleny podle zjištěného CVSS score do 3 kategorií kritičnosti, 4. kategorie informative jsem přidal z důvodu výskytů záznamů s popisem informative Tabulka 3 - Převod CVSS na kritičnost (Zdroj: Autor):

Tabulka 3 -Převod CVSS na kritičnost (Zdroj: Autor)

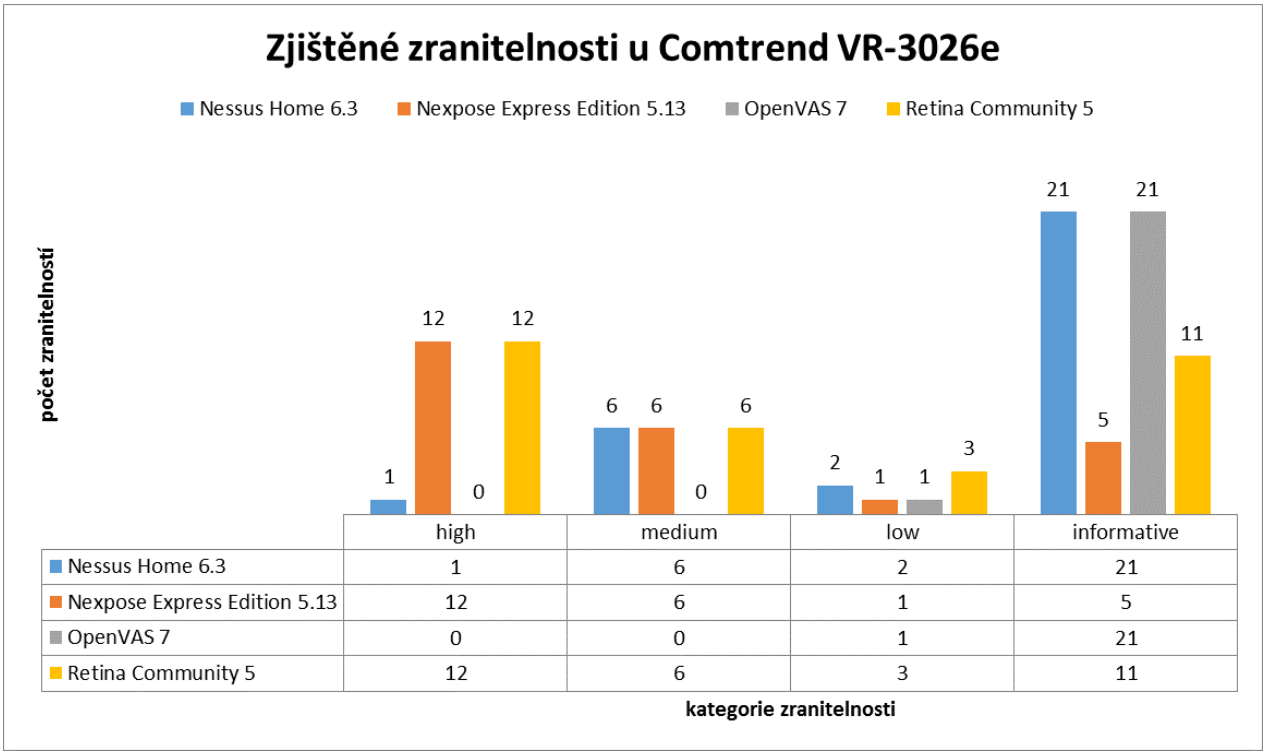
Kritičnost	CVSS score
High (Vysoká)	7.0-10.0
Medium (Střední)	4.0-6.9
Low (Nízká)	0.1-3.9
Informative (Informativní)	0

Z výsledků je na obrázcích Obrázek 6-17 a Obrázek 6-18 zřejmé, že nejvíce zranitelností je v kategorii informativní. Počet zranitelností v kategorie high, medium a low je závislí na úspěšnosti autentizovaného skenováni a velikosti databáze zranitelností daného výrobce.



	high	medium	low	informative
Nessus Home 6.3	5	3	1	68
Nexpose Express Edition 5.13	3	10	1	0
OpenVAS 7	0	4	0	42
Retina Community 5	3	12	19	30
Tripwire SecureScan 2015	0	0	0	3

Obrázek 6-17 - Počet zjištěných zranitelností u Windows 7 64Bit SP1 (Zdroj: Autor)



	high	medium	low	informative
Nessus Home 6.3	1	6	2	21
Nexpose Express Edition 5.13	12	6	1	5
OpenVAS 7	0	0	1	21
Retina Community 5	12	6	3	11

Obrázek 6-18 - Počet zjištěných zranitelností u Comtrend VR-3026e (Zdroj: Autor)

Pro porovnání výsledků skenování byla aplikována metoda váženého součtu, s těmito váhami jednotlivých kategoriím kritičnosti viz Obrázek 6-19

high	medium	low	informative
0,50	0,30	0,15	0,05

Obrázek 6-19 - Váhy kategorií (Zdroj: Autor)

Vítězem je nástroj Retina. Na druhém místě se umístil Nexpose, na třetím místě Nessus Home. Poslední skončil OpenVAS. TripWire nebyl do celkového hodnocení zařazen.

Nástroj	Užitek	Pořadí
Retina Community 5	0,97	1.
Nexpose Express Edition 5.13	0,76	2.
Nessus Home 6.3	0,37	3.
OpenVAS 7	0,03	4.

Obrázek 6-20 – Celkové srovnání výsledků skenovaní (Zdroj: Autor)

Licence pro nástroj Tripwire SecureScan neumožnil provést více skenování v jednom měsíci, proto uvádím jeho výsledek pouze pro Windows 7 64B SP1 a nezařazuji ho do celkového hodnocení. Z testování vyplývá, že výsledky jsou konzistentní pro jednotlivý nástroje, jinými slovy, že pokud byl nástroj úspěšný u Windows 7 tak i u Comtrendu.

Dílčí výsledky srovnání uvádí Obrázek 6-21 a Obrázek 6-22

Testovaný cíl	Windows 7 64Bit SP1	
Nástroj	**užitek**	**Pořadí**
Retina Community 5	0,77	1.
Nessus Home 6.3	0,63	2.
Nexpose Express Edition 5.13	0,56	3.
OpenVAS 7	0,13	4.
Tripwire SecureScan 2015	0,00	5.

Obrázek 6-21 - Srovnání výsledků skenovaní pro Windows 7 (Zdroj: Autor)

Testovaný cíl	Comtrend VR-3026e	
Nástroj	**užitek**	**Pořadí**
Retina Community 5	0,97	1.
Nexpose Express Edition 5.13	0,80	2.
Nessus Home 6.3	0,47	3.
OpenVAS 7	0,05	4.

Obrázek 6-22 - Srovnání výsledků skenovaní pro Comtrend VR-3026e (Zdroj: Autor)

Doplňující informace k testování

Data ze skenování jsou v originální podobě dostupné v elektronické příloze pod názvem: zdrojovaData.zip, výpočty a grafy jsou rovněž v elektronické příloze pod názvem: SrovnaniVMnastroju.xlsx

Retina u svých zranitelností v některých případech neuvádí aktuální CVSS score například u CVE-1999-0524 (NVD, 2015) je ve výsledcích skenování uvedeno CVVS 10 na NVD pouze 2. Tento fakt komplikuje porovnávání, kdy je nutné prověřit aktuální kritičnost zranitelností i následné vyhodnocení zdali je zjištěná zranitelnost opravdu kritická.

Úspěšnost při autentizovaném skenování měla značný vliv na počet odhalených zranitelností, Nexpose, Nessus částečně i Retina provedly úspěšnou autentizaci viz Obrázek 6-23

Nástroj	Cena licence za rok v $	Podpora SCAP protokolu	Podpora CVE	Autentizované skenování Windows 7 64Bit SP1	Autentizované skenování Comtrend VR-3026e
Nessus Home 6.3	zdarma pro domácí užití, komerční verze Professional stojí 2190	ne	ano	ano	ano
OpenSCAP + nadstavba SCAP Workbench	0	Ano	ano	ne	ne
OpenVAS	0	Ano	ano	ne	ne
Nexpose Express Edition 5.13	2000	ne	ano	ano	ano
Tripwire SecureScan 2015	neznámá	ne	ano	ne	ne
Retina Community	1800	ano	ano	ano	ne

Obrázek 6-23 - Parametry nástrojů a úspěšnost při autentizovaném skenováni (Zdroj: Autor)

6.10 Ostatní nástroje nezařazené do testování

V této podkapitole uvedu příklady použití nástrojů, které nemohly být zařazeny ke srovnání. Nástroje Microsoft Security Compliance Manager slouží ke správě policy. OpenSCAP a Workbench neumožňují skenování Windows 7 a v době psaní práce nebyl dostupný checklist pro Comtrend VR-3026e. Nástroj Qualys SSL Labs uvádím jako příklad široké podpory standardu CVE a jako

méně komplexní alternativu k vyšším edicím komerčních skenovacích nástrojů umožňující skenování webových aplikací.

6.10.1 Microsoft Security Compliance Manager (SCM)

Aplikace neumožnuje skenování zranitelnosti. Jejím hlavním úkolem je zajistit centralizovanou správu konfigurace systémů v originále security configuration assessment, Microsoft používá výraz Baseline, v terminologii NIST se značí jako pravidlo (Rule) a k němu přiřazená příslušná hodnota (Value).

Výhodou je funkcionalita umožňující stažení všech dostupných Microsoft Baseline v rámci aplikace. Poté, co jsou staženy aktuální Baseline, lze z každé vytvořit kopii, v níž může uživatel odebírat a měnit jednotlivé Baseline a jejich hodnoty. Když je s výslednou konfigurací spokojen, exportuje konfiguraci jako GPO, následně ji lze nasadit pomocí Active Directory Domain Services (centrálně na systémy v doméně) nebo LocalGPO (individuálně i mimo doménu).

Instalační požadavky

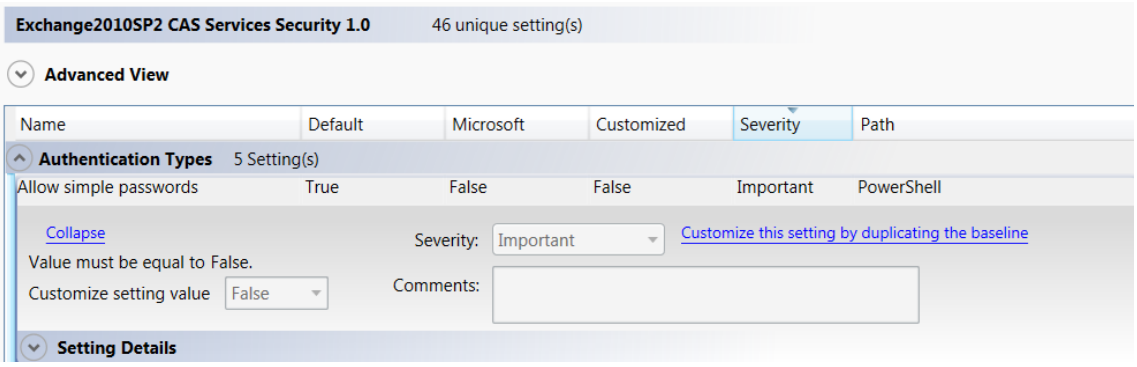
Pro zdárnou instalaci Microsoft požaduje operační systém Windows 7 nebo Windows 8. Není uvedena podpora Windows Server. V průběhu instalace bude provedeno automatické doinstalování MS SQL Server 2008 Express edice, v případě, že instalátor nenalezne tuto, nebo vyšší verzi.

Práce s baseline

Obrázek 6-24 uvádí přiklad Baseline pro Microsoft Exchange 2010 Service Pack 2. Konkrétně se jedná o kategorii Service Security Baseline verze 1. Dále se každá kategorie dělí na subkategorie, zde Authentication Types (Způsoby ověření totožnosti) na položce Allow simple passwords (Povolit jednoduchá hesla).

U každé Baseline jsou uvedeny 4 parametry viz Obrázek 6-24:

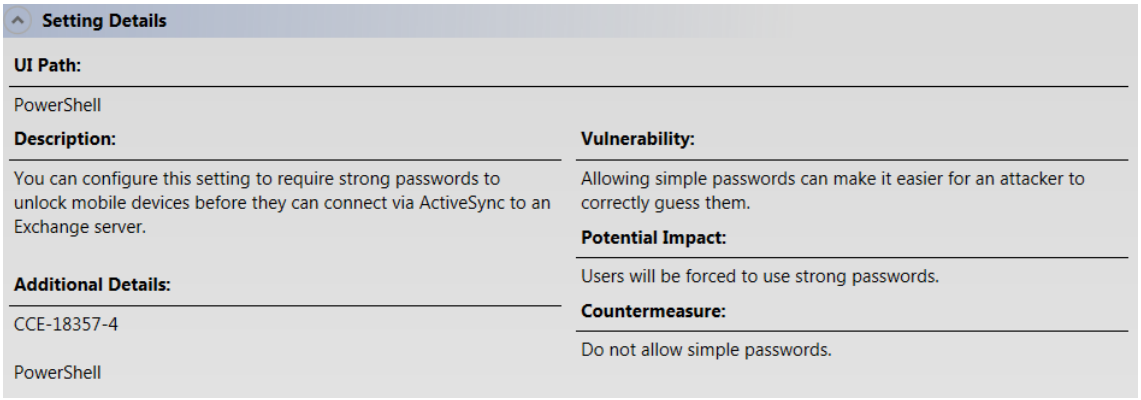
1. Default - nastavení od výrobce
2. Microsoft – Doporučené nastavení
3. Customized - Nastavení upravené uživatelem
4. Severity – Umožňuje výběr jedné z možností:
    a. None (nedefinovaná),
    b. Optional (volitelná, podle situace)
    c. Important (Důležitá)
    d. Critical (Kritická)
5. Path - Cesta k ručnímu nastavení parametru



Obrázek 6-24 - Microsoft Security Compliance, baseline (Zdroj: Autor)

Detail pro Baseline Allow simple passwords viz Obrázek 6-25:

1. UI Path - Cesta k ručnímu nastavení parametru
2. Description - Popis pro Baseline
3. Additional Details – Obsahuje doplňující informace k Baseline například:
    a. Common Configuration Enumeration (CCE)
        i. jednoznačný identifikátor konfigurační položky systému
    b. Skript umožňující změnu konfigurace
4. Vulnerability – Možná zranitelnost způsobena nevhodnou konfigurací
5. Potential Impact – Možné důsledky (omezení) po aplikování doporučené konfigurace
6. Countermeasure – Protiopatření k redukci zranitelnosti.



Obrázek 6-25 - Microsoft Security Compliance, baseline detail (Zdroj: Autor)

Porovnání baseline

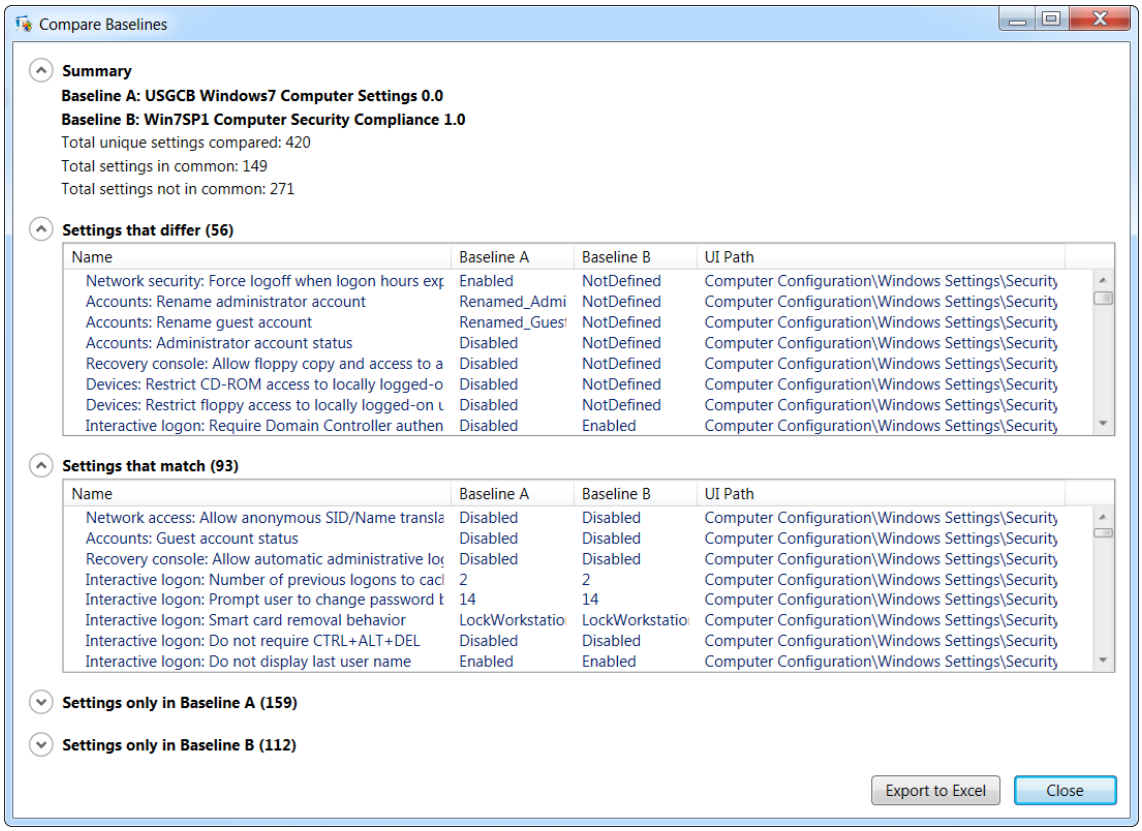
Byly porovnány USGCB Windows7 Computer Settings a Win7SP1 Computer Security Compliance 1.0 vydané Microsoftem, výsledky jsou následující Obrázek 6-26:

	USGCB Windows7 Computer Settings	Win7SP1 Computer Security Compliance 1.0
Datum poslední úpravy	10.11.2011	25.1.2013
Počet baseline	223	261

Společné baseline	149 (z toho má 56 jinou hodnotu a 93 shodnou)
Rozdílné baseline	271

Obrázek 6-26 -Porovnání baseline (Zdroj: Autor)

Z porovnání je zřejmé, že celkového počtu 420 baseline se plně shoduje pouze 93. Stejným způsobem je možné provést srovnání exportovaného GPO společnosti, ty jsem bohužel v době psaní práce neměl k dispozici. Výstup z aplikace viz Obrázek 6-27



Obrázek 6-27 - Security Compliance srovnani (Zdroj: Autor)

Hodnocení nástroje Microsoft Security Compliance Manager

Nástroj splňuje svoji funkci v oblasti hodnocení bezpečnosti konfigurací (SCA) pro aplikace od Microsoftu. Jako pozitivum bych uvedl:

1. nevyžaduje nákup licence
2. baseline jsou pravidelně aktualizovány přímo Microsoftem
3. umožňuje snadný import (testovaných/referenčních) a export (upravených) GPO

Slabé stránky vidím v těchto oblastech:

1. hodnocení bezpečnosti konfigurací pouze pro řešení od Microsoftu
2. Ruční import a export GPO, časově náročný u větších IT infrastruktur

6.10.2 Qualys FreeScan

Pro aktivaci účtu je vyžadována firemní emailová adresa, adresy na centrum.cz ani gmail.com nebyly přijaty. Školní emailová adresa na doméně vse.cz, zdárně prošla registračním procesem.

Webovou část aplikaci se spustí z odkazu, který přišel na email, pro který byla provedena registrace. Do pole pro IP adresu se zadá IP adresa cíle. Pokud je adresa dostupná z internetu provede se test. V případě, že je adresa dostupná pouze z lokální sítě, vyzve aplikace ke konfiguraci virtuálního stroje, na kterém se spustí skenování

Po rozběhnutí virtuálního stroje se staženým imagem, aplikace provede automatickou konfigurace, ta se nezdařila z důvodu chyby: Invalid IPv6 mode of operation, k chybě nebyly v době psaní této práce žádné informace v dokumentaci, či v odborných internetových diskuzích, podpora společnosti mě odkázala na návod, který nepomohl. Router Comtrend VR-3026e, který pro své testování používám, IPv6 podporuje a v době testování bylo povoleno. Test v této fázi končím.

6.10.3 OpenSCAP 1.2.1

OpenSCAP je v době psaní práce bylo oficiálně možné nainstalovat pouze na Linuxových systémech.

Testování aplikace bylo provedeno v prostředí virtuálního stroje VMware Player. Na virtuálním stroji jsem bežel operační systém Fedora verze 21 v 64 bitové verzi. Instalace OpenSCAP je příjemně jednoduchá, stačí pod uživatelem root (uživatel s nevyššími pravý systému), spustit příkaz:

```
yum install openscap openscap-utils openscap-content
```

Ten spustí nástroj „yum“ sloužící ke správě instalačních balíčků, z repositáře stáhne aktuální stabilní verzi, v době psaní práce to byla 1.2.1 a automaticky provede instalaci. Po úspěšné instalaci příkaz `oscap -V` vypíše informace o aplikaci:

```
OpenSCAP command line tool (oscap) 1.2.1
Copyright 2009--2014 Red Hat Inc., Durham, North Carolina.
Pro kompatibilitu s checklisty je důležitá tato část:
==== Supported specifications ====
XCCDF Version: 1.2
OVAL Version: 5.10.1
CPE Version: 2.3
CVSS Version: 2.0
```

```
CVE Version: 2.0
Asset Identification Version: 1.1
Asset Reporting Format Version: 1.1
```

Z portálu https://web.nvd.nist.gov/view/ncp/repository byly staženy checklisty. Příkazu `oscap info scap_gov.nist_USGCB-ie8.xml` zjistí verzi a základní informace o checklistu. Níže uvedený výpis odpovídá Checklistu pro aplikaci Microsoft Internet Explorer 8,

Jako výsledek se vypíšou tyto informace:

```
Document type: Source Data Stream
Imported: 2013-10-21T13:52:00
Stream: scap_gov.nist_datastream_USGCB-ie8-1.2.3.1.zip
Generated: 2012-02-24T10:00:00
Version: 1.2
Checklists:
    Ref-Id: scap_gov.nist_cref_USGCB-ie8-xccdf.xml
           Profiles:
xccdf_gov.nist_profile_united_states_government_configuration_baseline_version_1
.2.3.1
```

Druhý checklist je určen pro Apache 2.2. Ověříní validity (zdali odpovídá schématu XCCDF), pomocí příkazu:

```
oscap xccdf validate U_Apache_2-2_Server_UNIX_V1R6_Manual-xccdf.xml
```

Pokud příkaz nic nevypíše, Checklist je validní.

Pro skenování na sítí pomocí SSH, je nutné převést Checklist na DataStream příkazem:

```
oscap ds sds-compose U_Apache_2-2_Server_UNIX_V1R6_Manual-xccdf.xml test.xml
```

Výstup:

```
File '/home/tomashronek/Downloads/test.xml' line 2: Element
'{http://scap.nist.gov/schema/scap/source/1.2}data-stream': Missing child
element(s). Expected is ( {http://scap.nist.gov/schema/scap/source/1.2}checks ).
File '/home/tomashronek/Downloads/test.xml' line 2: Element
'{http://checklists.nist.gov/xccdf/1.1}Benchmark': This element is not expected.
Expected is one of ( {http://checklists.nist.gov/xccdf/1.2}Benchmark,
{http://oval.mitre.org/XMLSchema/oval-definitions-5}oval_definitions,
{http://scap.nist.gov/schema/ocil/2.0}ocil,
{http://cpe.mitre.org/dictionary/2.0}cpe-list,
{http://checklists.nist.gov/xccdf/1.2}Tailoring ).
```

Převod neproběhl úspěšně, protože nelze převádět XCCDF Checklist verze 1.1, nástroj umí převádět pouze aktuální verzi 1.2. Takto je nutné postupovat v případě každé komponenty a aplikace, která je určena ke skenování.

6.10.4 SCAP Workbench

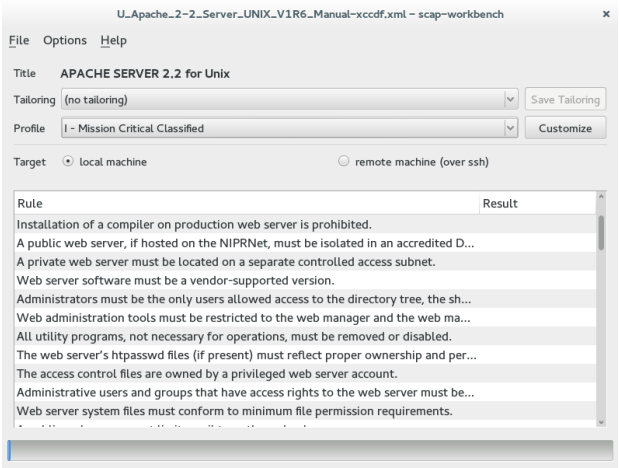
Grafická nadstavba pro OpenSCAP, instalace:

```
yum install scap-workbench
```

příkaz z repositáře stáhne aktuální stabilní verzi, v době psaní práce to byla 1.0.3 a automaticky provede instalaci.

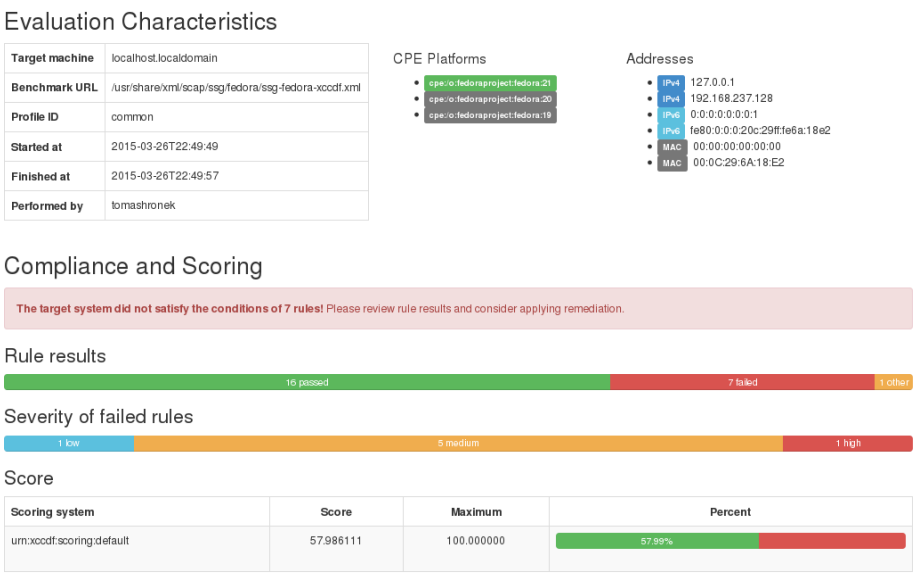
Po spuštění SCAP Workbench lze nahrát příslušný checklist ve formátu XML validní k schématu XCCDF Verze 1.2. Obrázek 6-28

Skenování se nepodařilo spustit, protože k SSH skenování je nutný převod na datastream, který se nezdařil.



Obrázek 6-28 - SCAP workbench (Zdroj: Autor)

Lokální výsledek skenování Fedory uvádí Obrázek 6-29 a Obrázek 6-30



Evaluation Characteristics

Target machine	localhost.localdomain
Benchmark URL	/usr/share/xml/scap/ssg/fedora/ssg-fedora-xccdf.xml
Profile ID	common
Started at	2015-03-26T22:49:49
Finished at	2015-03-26T22:49:57
Performed by	tomashronek

CPE Platforms

- cpe:/o:fedoraproject:fedora:21
- cpe:/o:fedoraproject:fedora:20
- cpe:/o:fedoraproject:fedora:19

Addresses

- IPv4 127.0.0.1
- IPv4 192.168.237.128
- IPv6 0:0:0:0:0:0:0:1
- IPv6 fe80:0:0:0:20c:29ff:fe6a:18e2
- MAC 00:00:00:00:00:00
- MAC 00:0C:29:6A:18:E2

Compliance and Scoring

The target system did not satisfy the conditions of 7 rules! Please review rule results and consider applying remediation.

Rule results

16 passed | 7 failed | 1 other

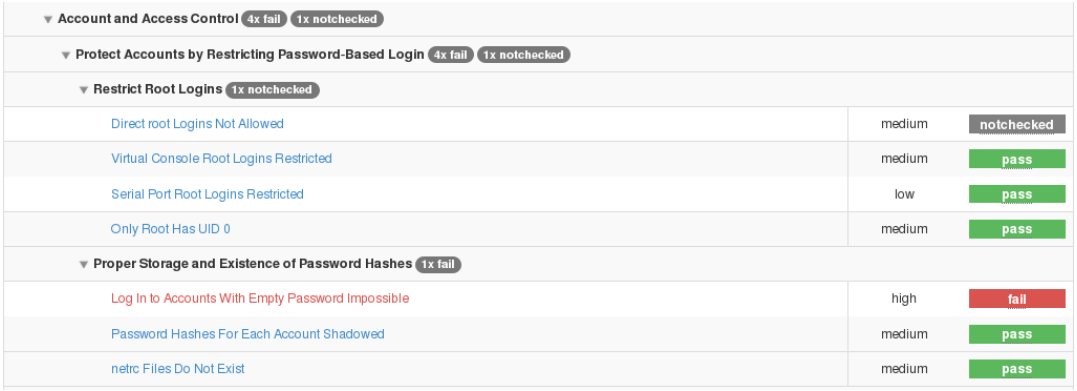
Severity of failed rules

1 low | 5 medium | 1 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	57.986111	100.000000	57.99%

Obrázek 6-29 - SCAP Workbench report (Zdroj: Autor)



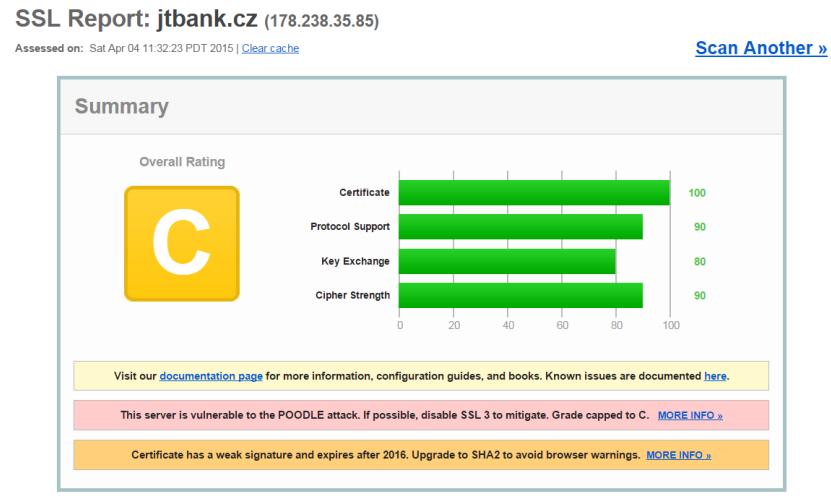
▼ Account and Access Control 4x fail 1x notchecked		
▼ Protect Accounts by Restricting Password-Based Login 4x fail 1x notchecked		
▼ Restrict Root Logins 1x notchecked		
Direct root Logins Not Allowed	medium	notchecked
Virtual Console Root Logins Restricted	medium	pass
Serial Port Root Logins Restricted	low	pass
Only Root Has UID 0	medium	pass
▼ Proper Storage and Existence of Password Hashes 1x fail		
Log In to Accounts With Empty Password Impossible	high	fail
Password Hashes For Each Account Shadowed	medium	pass
netrc Files Do Not Exist	medium	pass

Obrázek 6-30 - SCAP Workbench report detail (Zdroj: Autor)

6.10.5 Qualys SSL Labs

V současné době využívají podniky pro kontakt se zákazníky i své interní potřeby celou řadu webových aplikací. Protokol SSL (Secure Sockets Layer) v současné době přejmenován na TLS (Transport Layer Security) umožnuje zabezpečenou komunikaci na internetu.

Výsledek skenování portálu J&T banky byl vyhodnocen známkou C, Obrázek 6-31. Pod výslednou známkou jsou uvedeny chyby v konfiguraci v kontextu aktuálních zranitelností. Konkrétně u tohoto skenu, bylo vyhodnoceno jako rizikové povolené použití SSL 3, u kterého byla v říjnu roku 2014 objevena zranitelnost vůči POODLE útoku CVE-2014-3566, ta spočívá ve využití útoku Man in the Middle a padding sekce v šifrovaném textu.



Obrázek 6-31 - Quaylus SSL labs (Zdroj: Autor)

7. Závěr

Vulnerability management (VM) je komplexní oblast vyžadující systémový přístup, tato oblast není pouze o skenovacích nástrojích. V práci se mi podařilo zasadit disciplínu řízení zranitelností do kontextu informační bezpečnosti podniku a vysvětlit její vztah k souvisejícím disciplínám, jmenovitě:

- risk management – hodnotí kritičnost komponent v kontextu dodávaných IT služeb
- policy management – říká, jakými pravidly se bude IT infrastruktura řídit
- configuration management – spravuje komponenty a určuje jejich příslušnost k IT službám
- incident management – řeší, jak zacházet se vzniklou zranitelností
- patch management – eliminuje/zmírňuje zranitelnosti

Pokud podnik s rozsáhlou IT infrastrukturou nasadí skenovací nástroj, bez ohledu na související oblasti, bude skenovací nástroj produkovat nerelevantní upozornění na zranitelnosti, které v kontextu dodávané služby nejsou kritické a naopak. Tuto skutečnost se mi podařilo zmírnit přepočtem kritičnosti zjištěných zranitelností pomocí vlastního vzorce, stejný výpočet zvýší úroveň kritičnosti zranitelností u komponent navázaných na kritické IT služby.

Dosud nebyla publikována žádná závěrečné práci věnující se výhradně tématu řízení zranitelností. Tato závěrečná práce je první, která poskytuje srovnatelné výsledky při skenování zranitelností vůči stejným cílům, čehož bylo docíleno metodou váženého součtu a stejných podmínek pro testované nástroje.

Porovnávané nástroje se umístily v tomto pořadí: Retina, Nexpose, Nessus, OpenVAS. Srovnání přineslo statisticky významné odchylky ve schopnosti odhalit zranitelnosti. Konečné rozhodnutí je závislé i na dalších parametrech jako je například funkcionalita umožňující klasifikovat kritičnost skenovaných komponent. Nástroje OpenVAS nelze vzhledem k výsledkům tohoto srovnání doporučit do produkčního prostředí podniku.

Neméně přínosná je rovněž aplikace metodiky Common Vulnerability Scoring System k určení kritičnosti zjištěných zranitelností ve vztahu k dodávaným IT službám. Z jejího aplikování vyplynulo, že metodika neumožňuje konzistentní určení kritičnosti zranitelností vzhledem k dodávaným IT službám, proto zde byl vytvořen a aplikován vlastní přepočet.

Všechny vytyčené cíle se podařilo splnit.

8. Seznam literatury

„Cizojazyčné texty byly přeloženy autorem této práce“

AXELOS. 2011. ITIL – výkladový slovník a zkratky. *AXELOS.* [Online] AXELOS Limited 2012, 29. 8 2011. [Citace: 1. 4 2014.] [PDF] Dostupné z: https://www.axelos.com/glossaries-of-terms.

BUDÍN, Bc. Emil. 2014. *Využití automatizovaných nástrojů pro řízení bezpečnosti informací dle norem řady ČSN ISO/IEC 27000.* Filozofická fakulta, Informační studia a knihovnictví/Informační studia a knihovnictví, Masarykova univerzita. Brno : Budín, Bc. Emil, 2014. Vedoucí: PhDr. Petr Škyřík, Ph.D..

CHUVAKIN, Anton. 2012. Vulnerability and Security Configuration Assessment Solutions Comparison. *Gartner.* [Online] 12. 3 2012. [Citace: 12. 4 2015.] http://www.gartner.com/technology/media-products/reprints/qualys/Qualys_225382.html. ID:G00225382.

COBIT. 2015. it policies management. *isaca.org.* [Online] 5. 1 2015. [Citace: 16. 3 2015.] Dostupné z: http://www.isaca.org/Groups/Professional-English/po6-3-it-policies-management/Pages/Overview.aspx.

ČSN ISO/IEC 27001:2005. 2005. *Informační technologie - Bezpečnostní techniky - Systémy.* Praha : Úřad pro technickou normalizaci,, 2005. Třídící znak 369790.

DOMÁNY, Mgr. Dušan. 2011. *Vulnerability Reports Analysis and Management.* Matematicko-fyzikální fakulta (MFF), Katedra teoretické informatiky a matematické logiky (32-KTIML). Praha : Domány, Mgr. Dušan, 2011. Vedoucí: Daniel Toropila.

DOUCEK, Petr, a další. 2011. *Řízení bezpečnosti informací, 2. vydání.* Praha : Professional publishing, 2011. 978-80-7431-050-8.

ITIL. 2010. ITIL Service Catalogue: How to produce a Service Catalogue. *itilnews.* [Online] 25. 6 2010. [Citace: 20. 4 2014.] http://www.itilnews.com/ITIL_Service_Catalogue_How_to_produce_a_Service_Catalogue.html.

KOUDELA, Bc. Radek. 2011. *Hodnocení přístupů k analýze.* Fakulta informatiky a statistiky, Vysoká škola ekonomická v Praze. Praha : Bc. Radek Koudela, 2011. Vedoucí: prof. Ing. Petr Doucek, CSc..

LOCKE, Gary a Gallagher, Patrick. 2011. *Information Security.* Gaithersburg : National Institute of Standards and Technology, 2011. NIST Special Publication 800-39.

MANN, David. 2008. *An Introduction to the Common Configuration Enumeration.* [Online] místo neznámé : MITRE Corporation, 2008. https://cce.mitre.org/documents/Introduction_to_CCE_White_Paper_July_2008.pdf.

MBI. 2015. Management Byznys Informatiky. [Online] 1. 1 2015. [Citace: 16. 4 2015.] http://mbi.vse.cz/mbi/index.html#obj/OBJECTMNG-9. OM009.

MELL, Peter, Bergeron, Tiffany a Henning, David. 2005. *Creating a Patch and Vulnerability Management Program.* Gaithersburg : National Institute of Standards and Technology, 2005. NIST Special Publication 800-40 version 2.0.

MELL, Peter, SCARFONE, Karen a ROMANOSKY, Sasha. 2007. *A Complete Guide to the Common Vulnerability Scoring System Version 2.0.* místo neznámé : First.org, 2007. Dostupnost z: https://www.first.org/cvss/cvss-guide.

MICROSOFT. 2013. Microsoft Security Compliance Manager. *http://technet.microsoft.com/.* [Online] Microsoft, 28. 1 2013. [Citace: 17. 1 2015.] Dostupné z: http://technet.microsoft.com/en-us/library/cc677002.aspx.

MITRE CORP. 2013. Terminology. *Common Vulnerabilities and Exposures.* [Online] Mitre Corp., 27. 2 2013. [Citace: 4. 4 2015.] Dostupné z: http://cve.mitre.org/about/terminology.html.

NESSUS. 2015. Which Version of Nessus is Right for You? *Nessus.* [Online] 1. 1 2015. [Citace: 15. 4 2015.] http://www.tenable.com/products/nessus-vulnerability-scanner.

NEXPOSE. 2015. Nexpose User Guide. *Nexpose.* [Online] 8. 4 2015. [Citace: 17. 4 2015.] Dostupné z: https://community.rapid7.com/docs/DOC-1387.

NIST. 2009. The National Institute of Standards and Technology. *Abou us:The National Institute of Standards and Technology.* [Online] NIST, 1. 5 2009. [Citace: 15. 4 2015.] Dostupné z: http://scap.nist.gov/index.html.

NVD. 2015. NVD. *National Vulnerability Database.* [Online] NIST, 1. 4 2015. [Citace: 11. 4 2015.] Dostupné z: https://nvd.nist.gov/.

—. 2007. NVD Common Vulnerability Scoring System Support v2. *The National Vulnerability Database.* [Online] NIST, 20. 6 2007. [Citace: 4. 4 2015.] Dostupné z: https://nvd.nist.gov/cvss.cfm.

OPENVAS. 2015. About OpenVAS Software. *OpenVAS.* [Online] 1. 1 2015. [Citace: 15. 4 2015.] Dostupné z: http://www.openvas.org/software.html#feature_overview.

QUALYS. 2008. *Vulnerability Management For Dummies.* Chichester : John Wiley & Sons, Ltd, 2008. 978-0-470-69457-2.

ROCHFORD, Oliver a KAVANGH, M.,Kelly. 2014. Market Guide for Vulnerability Assessment. *Gartner.* [Online] 15. 10 2014. [Citace: 1. 4 2015.] Dostupné z: www.gartner.com/technology/reprints.do?id=1-26R9NOK&ct=150105&st=sb.

SCARFONE, Karen a MELL, Peter. 2007. *Guide to Intrusion Detection.* Gaithersburg, : National Institute of Standards and Technology , 2007. Special Publication 800-94 .

SMEJKAL, Vladimír a Rais, Karel. 2013. Jak volit nástroje pro snižování rizika. *http://www.businessinfo.cz/.* [Online] 9. 4 2013. [Citace: 12. 3 2015.] http://www.businessinfo.cz/cs/clanky/metody-snizovani-rizika-52919.html.

—. 2013. *Řízení rizik ve firmách a jiných organizacích.* Praha : Grada, 2013. 978-80-247-4644-9.

SOUPPAYA, Murugiah a Scarfone, Karen,. 2013. *Guide to Enterprise Patch Management Technologies.* Clifton : National Institute of Standards and Technology, 2013. Special Publication 800-40 Revision 3.

STEFAN, Kempter. 2013. Checklist Incident Priority. *IT Process Maps.* [Online] IT Process Maps GbR, 13. 9 2013. [Citace: 12. 2 2015.] Dostupné z: http://wiki.en.it-processmaps.com/index.php/Checklist_Incident_Priority.

TENABLE. 2015. Nessus Documentation. *Tenable.* [Online] 11. 3 2015. [Citace: 5. 4 2015.] Dostupné z: https://www.tenable.com/products/nessus/documentation.

ŽĎÁRA, T. 2012. Úloha: Řízení incidentů. *Management Byznys Informatiky.* [Online] 19. 12 2012. http://mbi.vse.cz/mbi/index.html#obj/TASK-78.

9. Seznam obrázků

10. Přílohy

Data ze skenování jsou v originální podobě dostupné v souboru zdrojovaData.zip

Výpočty a grafy jsou v souboru SrovnaniVMnastroju.xlsx

10.1 Ukázka profilu, hodnoty a pravidla podle SCAP

```
<xccdf:Profile
id="xccdf_gov.nist_profile_united_states_government_configuration_baseline_version_
1.2.3.1">
  <xccdf:title>United States Government Configuration Baseline 1.2.3.1
  </xccdf:title>
  <xccdf:description>This profile represents guidance outlined ...
  </xccdf:description>
  <xccdf:select idref="xccdf_gov.nist_rule_maximum_password_age" selected="true"/>
  <xccdf:refine-value         idref="xccdf_gov.nist_value_password_maximum_age_var"
selector="5184000_seconds"/>
</xccdf:Profile>
<xccdf:Value id="xccdf_gov.nist_value_password_maximum_age_var" operator="less than
or equal" type="number">
  <xccdf:title>Maximum Password Age
  </xccdf:title>
  <xccdf:description>The maximum age in seconds before a password expires. (90
days = 7776000 seconds; 60 days = 5184000)
  </xccdf:description>
  <xccdf:value>7776000
  </xccdf:value>
  <xccdf:value selector="5184000_seconds">5184000
  </xccdf:value>
  <xccdf:value selector="7776000_seconds">7776000
  </xccdf:value>
</xccdf:Value>
<xccdf:Rule     id="xccdf_gov.nist_rule_maximum_password_age"     selected="false"
weight="10.0">
  <xccdf:title>Maximum Password Age
  </xccdf:title>
  <xccdf:description>This forces users to change their passwords regularly....
  </xccdf:description>
  <xccdf:reference>
    <dc:type>GPO
    </dc:type>xccdf_gov.nist_value_password_maximum_age_var
    <dc:source>Computer  Configuration\Windows  Settings\Security  Settings\Account
Policies\Password Policy
    </dc:source>
```

```
  </xccdf:reference>
  <xccdf:ident system="http://cce.mitre.org">CCE-9193-4
  </xccdf:ident>
  <xccdf:check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
    <xccdf:check-export        export-name="oval:gov.nist.usgcb.windowsseven:var:18"
value-id="xccdf_gov.nist_value_password_maximum_age_var"/>
    <xccdf:check-content-ref                          href="USGCB-Windows-7-oval.xml"
name="oval:gov.nist.usgcb.windowsseven:def:5"/>
  </xccdf:check>
</xccdf:Rule>
```