UNIVERZITA PARDUBICE

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Diplomová práce

2019 Bc. Jiří Danielka

Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Skenovací nástroje pro síťovou zranitelnost

Bc. Jiří Danielka

Diplomová práce

2019

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2018/2019**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jiří Danielka**
Osobní číslo:	**I17203**
Studijní program:	**N2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Skenovací nástroje pro síťovou zranitelnost**
Zadávající katedra:	**Katedra softwarových technologií**

Z á s a d y p r o v y p r a c o v á n í :

Diplomová práce se bude zabývat zabezpečením počítačových sítí a systémů. V teoretické části autor představí příslušné normy ISO 27000 a standard ISO/IEC 27033-3:2010. V teoretické části se bude autor rovněž hledáním takových softwarových nástrojů, které jsou schopny do jisté míry automatizovat hledání a vyhodnocování potenciálních nebezpečí jak v síti, tak i jejím vnějším perimetru. Autor provede komparativní analýzu těchto nástrojů umožňujících automatizaci managementu bezpečnosti v počítačové síti. V praktické části implementuje student případovou studii na smyšlené podnikové síti, kdy jednotlivé nástroje nasadí a porovná je dle nejdůležitějších kritérií, jako jsou míra úspěšnosti co do nalezených problémů, míra schopnosti automatické práce takového nástroje, jednoduchost nasazení, cena a možnost dalšího využití výsledků, ať se pod tím skrývá cokoliv.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování diplomové práce: **tištěná**

Seznam odborné literatury:

PRITCHETT, Willie L a David DE SMET. Kali Linux cookbook. Birmingham: Packt Publishing, 2013, 1 online resource (261 pages). ISBN 9781783289608, CUNNINGHAM, Bryan a Jeff TAYLOR. The best damn IT security management book period. Oxford: Elsevier Science [distributor], c2007, xliii, 913 p. ISBN 15-974-9227-2.

Vedoucí diplomové práce: **Ing. Soňa Neradová, Ph.D.**

Katedra informačních technologií

Datum zadání diplomové práce: **22. října 2018**

Termín odevzdání diplomové práce: **18. května 2019**

Ing. Zdeněk Němec, Ph.D.
děkan

L.S.

prof. Ing. Antonín Kavička, Ph.D.
vedoucí katedry

V Pardubicích dne 17. listopadu 2018

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 15. 07. 2019

Bc. Jiří Danielka

PODĚKOVÁNÍ

Rád bych poděkoval své vedoucí práce, Ing. Soně Neradové, Ph.D., za vstřícnost, ochotu a cenné rady, které mi poskytla v průběhu zpracování diplomové práce. Dále bych chtěl poděkovat rodině a přátelům za podporu v průběhu studia.

ANOTACE

Diplomová práce se zaměřuje na popis norem ISO/IEC 27000 a ISO/IEC 27033-3, které se zabývají bezpečností v rámci počítačových sítí a systémů. Práce se dále zabývá hledáním softwarových nástrojů, které umožnují detekovat a vyhodnocovat nebezpečí, která se skrývají v počítačových sítích na jejich vnitřním nebo vnějším perimetru. Skenovací nástroje jsou v rámci práce nasazeny a následně porovnány dle zadaných kritérií, mezi které patří cena, kvalita detekce zranitelností nebo možnosti automatizace.

KLÍČOVÁ SLOVA

ISO/IEC 27000, ISO/IEC 27033-3, bezpečnost, počítačové sítě, OpenVAS

TITLE

Scanning Tools for Network Vulnerability

ANNOTATION

The thesis focuses on the description of ISO / IEC 27000 and ISO / IEC 27033-3 standards, which are related to security in computer networks and systems. The work also deals with the search for software tools that allow to detect and evaluate risks that are hidden in computer networks on their internal or external perimeter. Scanning tools are deployed and then compared by specified criteria, including price, vulnerability detection quality, and automation capabilities.

KEYWORDS

ISO/IEC 27000, ISO/IEC 27033-3, safety, computer networks, OpenVAS

OBSAH

SEZNAM ILUSTRACÍ

SEZNAM TABULEK

SEZNAM ZKRATEK A ZNAČEK

3DES	Triple DES
AES	Advanced Encryption Standard
AMD	Advanced Micro Devices
APT	Advanced Packaging Tool
ARM	Advanced RISC Machine
BSOD	Blue Screen of Death
CBC	Cipher Block Chaining
CD	Compact Disc
CF	Compact Flash
CGI	Common Gateway Interface
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
DDR	Double Data Rate
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DVD	Digital Versatile Disc
FTP	File Transfer Protocol
GNOME	GNU Network Object Model Environment
GNU	GNU's Not Unix
GUI	Graphical User Interface
HMAC	Keyed-hash Message Authentication Code

HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
CHAP	Challenge-Handshake Authentication Protocol
IEC	International Electrotechnical Commission
IM	Instant Messaging
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	IP Security Protocol
ISMS	Information Security Management System
ISO	International Organization for Standardization
KRACK	Key Reinstallation Attacks
LAN	Local Area Network
MD5	Message-digest Algorithm
MIPS	Microprocessor without Interlocked Pipeline Stages
MKV	Matroska Multimedia Container
NASA	National Aeronautics and Space Administration
NASL	Nessus Attack Scripting Language
NAT	Network Adress Translation
NSE	Nmap Scripting Engine
P2P	Peer to Peer
PCI	Peripheral Component Interconnect
PDF	Portable Document Format
PHP	Personal Home Page

PKI	Public Key Infrastructure
RAM	Random Access Memory
RAR	Roshal Archive
RISC	Reduced Instruction Set Computer
RS-232	Recommended Standard 232
SAN	Storage Area Network
SCADA	Supervisory Control and Data Acquisition
SE	Standard Edition
SMB	Server Message Block
SMS	Short Message Service
SOAP	Simple Object Access Protocol
SOHO	Smal Office Home Office
SQL	Structured Query Language
SS	Security Scanner
SSD	Solid State Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign On
TLS	Transport Layer Security
TR	Technical Report
UAC	User Account Control
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus

USD	United States dollar
VLC	VideoLAN Client
VMP	Vulnerability Manager Plus
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WLAN	Wireless LAN
WPA2	Wi-Fi Protected Access 2
WWAN	Wireless Wide Area Network
XML	eXtensible Markup Languag

ÚVOD

Autoři moderních operačních systémů a aplikací jsou pod neustálým konkurenčním tlakem, který je nutí vymýšlet a vyvíjet novou funkcionalitu, kterou následně přidávají do svých aplikací a systémů. Tyto nové funkce zlepšují uživatelský komfort a různé opravy činní software bezpečnější a stabilnější. S každou takovou aktualizací rostou počty řádků zdrojových kódů, které je nutné dále udržovat. Údržba rozsáhlého zdrojového kódu je složitá a složitost s přibývající funkcionalitou dále roste. Tento fakt následně nahrává nekalým praktikám, protože v rozsáhlém zdrojovém kódu se snadno schová příležitost pro útočníka, který ji může zneužít pro svoji potřebu. Vzhledem ke složitosti dnešních aplikací může odhalení takových zranitelností trvat měsíce, někdy i roky, a i tak není zajištěná jejich okamžitá eliminace. Tvůrcům softwaru nějaký čas zabere řešení samotné zranitelnosti a následná distribuce aktualizované verze postižené aplikace mezi uživatele.

V případě, kdy je aktualizace na zranitelný software vydána, je nutné zajistit její rychlou instalaci. V rozsáhlých sítích je pak problémem identifikace všech strojů, které danou zranitelností trpí. S tím mohou vypomoci skenovací nástroje pro síťovou zranitelnost, kterými se zabývá tato práce.

Počáteční kapitola této práce představuje normu ISO/IEC 27000, která se zabývá definicí a popisem základních pojmů z oblasti bezpečnosti informačních systémů. Norma dále představuje další normy řady 27000, které se bezpečností detailněji zabývají.

Ve druhé kapitole je následně na první kapitolu navázáno důkladným rozborem třetí části normy ČSN ISO/IEC 27033. Ta ve svém textu definuje další pojmy z oblasti bezpečnosti informačních systémů, které následně využívá u několika ukázkových případů využití počítačových sítí v praxi. Součástí popisu těchto scénářů jsou i možná rizika, která tento způsob užití sítě přináší, a krátké představení prostředků, které slouží pro jejich eliminaci.

Třetí kapitola představuje vybrané skenovací nástroje, které následně budou porovnávány v praktické části. U každého nástroje je krátce popsána jeho funkcionalita, autoři a jiné informace. Na tuto kapitolu těsně navazuje kapitola čtvrtá, která představuje použité hardwarové a softwarové vybavení, využité pro otestování vybraných nástrojů.

Kapitola s pořadovým číslem pět představuje přehled omezení bezplatných verzí skenovacích nástrojů, který dále rozšiřuje přehledem cen za plné verze bez omezení. V rámci kapitoly jsou také představeny platformy, preferované nástroji pro své fungování.

Praktická část práce prezentuje zkušenosti, které byly získány při nasazení vybraných skenovacích nástrojů jak na vnitřním, tak i vnějším perimetru sítě. Vnitřní perimetr zabezpečuje sada virtualizovaných počítačů, představujících moderní způsob provozu IT infrastruktury. Virtualizace je v dnešní době velmi populární, protože dokáže zajistit podnikům flexibilitu a úsporu nákladů. Skenovací nástroje jsou zde podrobené řadě testů, které dále pokračují na vnějším perimetru testováním zařízení MikroTik. Závěr kapitoly patří srovnáním možností automatizace, které jednotlivé nástroje nabízí a představuje způsoby, jak je o zjištěných zranitelnostech informován uživatel.

1 ISO/IEC 27000

Norma ISO/IEC 27000, která byla přijata v přeloženém stavu jako ČSN EN ISO/IEC 27000 definuje ve své poslední verzi z května roku 2017 základní pojmy z oblasti systémů řízení bezpečnosti informací a následně popisuje řadu norem, které dále specifikují požadavky na ISMS. Další směrnice této řady popisují procesy, jak definovat cíle k implementaci ISMS, poskytují pokyny k implementaci těchto systémů a seznamují s možnostmi auditů. Poslední řada směrnic specifikuje systémy řízení bezpečností informací pro jednotlivá odvětví, kde je možné tyto systémy použít. Například se jedná o konkrétní využití v oblasti financí nebo energetice. (ÚNMZ, 2017, s. 8-9)

Tabulka 1 - Řada norem ISMS

Řada norem ISMS	Spadající normy
Norma slovníku	27000
Norma požadavků	270001, 27006, 27009
Normy směrnic	27002, 27003, 27004, 27005, 27007, TR 27008, 27013, 27014, TR 27016
Normy dle oborů	27010, 27011, 27015, 27017, 27018, 27019
Normy směrnic dle opatření	2703x, 2704x

Zdroj: zpracováno dle (ÚNMZ, 2017)

1.1 Systém řízení bezpečnosti informací

V každé organizaci dochází k procesu tvorby, přenosu a zpracování informací. Informace jsou brány jako důležité aktivum, které umožnuje organizacím dosahovat cílů, které si vytyčily. V průběhu nakládání s informacemi vznikají rizika, která mohou informační aktivum ohrozit. K ohrožení může dojít například:

- útokem,
- chybou,
- nebo přírodními vlivy.

Toto aktivum je tedy vhodné chránit, protože zcizení či ztráta tohoto aktiva může znemožnit plnění cílů organizace a přinést velké finanční ztráty. (ÚNMZ, 2017, s. 20-21)

Systémy řízení bezpečnosti informací, zkráceně ISMS, jsou soubory ucelených politik, postupů a směrnic, které pomáhají ochránit toto důležité aktivum v rámci organizace. Pro správně nastavený systém řízení bezpečnosti informací je nutné specifikovat požadavky na ochranu informačních aktiv a současně posoudit možná rizika, které je možné eliminovat. Na některá

rizika se pro jejich nepravděpodobný výskyt nevyplatí implementovat vhodná protiopatření, protože náklady, které by vedly k potlačení těchto rizik, by převýšily hodnotu chráněného aktiva. (ÚNMZ, 2017, s. 20-21)

Obecně se klade důraz na tři základní atributy v oblasti bezpečnosti informací. Jsou to:

- důvěrnost,
- dostupnost,
- integrita.

1.1.1 Důvěrnost

Atribut důvěrnosti deklaruje, že v každém okamžiku, kdy je s informacemi nakládáno, je zajištěna určitá minimální úroveň utajení. Tato úroveň by měla být dosažena jak v případě, kdy dochází k uchovávání informací, jejich přenosu, tak i ve chvíli doručení osobě, která je oprávněna s informací dále pracovat. (Marťák, 2005)

V určitých situacích může docházet k narušení důvěrnosti. Jedná se například o stavy, kdy je sledován síťový provoz, je použito zařízení typu keylogger, které umožnuje sledovat stisknuté klávesy nebo za pomoci sociálního inženýrství, kdy dochází k manipulaci s uživateli s cílem získat jejich osobní údaje. (Marťák, 2005)

K porušení důvěrnosti může dojít i lidskou chybou, když například zapomene pověřená osoba odesílanou zprávu zašifrovat. Tyto chyby mohou být úmyslné nebo neúmyslné. (Marťák, 2005)

Zajistit důvěrnost můžeme například šifrováním. Možné je použití symetrické i asymetrické kryptografie. Šifrování je možné provést již při ukládání dat na úložiště nebo ve chvíli, kdy dochází k jejich přenosu. Pro zajištění důvěrnosti můžeme využít například protokol Kerberos, který umožnuje v nezabezpečené síti prokázat svoji identitu, a proto zabraňuje jak odposlechu, tak útokům na integritu dat. Dále je možné použít například PKI, které umožnuje použít cizí veřejné klíče k ověření elektronických podpisů. (Marťák, 2005)

1.1.2 Dostupnost

Kvalitní systém by měl být v maximální míře dostupný, tak aby jeho chování neomezovalo produktivitu organizace. Vyřazení systému z provozu může být způsobeno:

- útokem,
- selháním zařízení,

- přírodními živly,
- lidskou chybou.

Dostupnost můžeme zajistit hlavně dostatečnou kapacitou linek, které umožnují sytému včas vyřizovat požadavky, aby nebyla negativně ovlivněna produktivita. Na obranu proti selhání zařízení je možné použít redundantní linky nebo zařízení, které v případě výpadku zajistí náhradu. Přírodní živly je možné eliminovat například vhodným umístěním zařízení, v případě výpadku elektrické energie dostatečnou kapacitou UPS jednotek nebo dieselagregáty. Lidské chyby je možné omezit vhodným proškolením personálu. Vyloučit tyto chyby úplně však možné není. (Marťák, 2005)

Na omezení dostupnosti cílí velmi často také potencionální útočníci. Jedná se o útoky typu DoS/DDoS, které zahltí cílové služby velkým množstvím požadavků, které systém není schopen zpracovávat a následně přestane odpovídat. To vede k nedostupnosti částí nebo celku systému, na který je útok veden. Bránit se proti těmto útokům je možné: pomocí zařízení typu firewall, použitím přístupových seznamů, které blokují adresy, ze kterých je veden útok nebo nasazením systému IPS, který dokáže detekovat škodlivou činnost, zaznamenat její průběh a následně ji zablokovat a odeslat upozornění o aktivní škodlivé činnosti. (Marťák, 2005)

1.1.3 Integrita

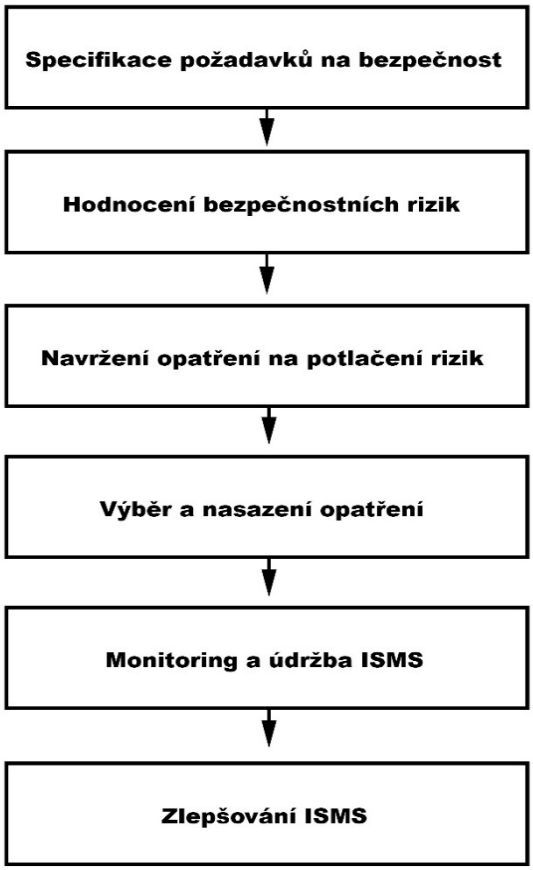
Integritou dat se rozumí situace, kdy uložená data jsou přesná a odpovídají stavu, kdy není možné je neautorizovaným zásahem změnit. Všechny prostředky, které se podílí na výměně informací, musí data doručovat přesně, v nezměněné podobě a bez poškození. (Marťák, 2005)

Integrita dat může být narušena úmyslně, kdy dojde například k napadení systému počítačovým virem, který pozmění uložená data nebo přístupem neautorizované osoby, která chce způsobit škodu a úmyslně změní uložená data. K narušení integrity dat může dojít i neúmyslně, například nepozorností uživatele, který omylem část dat pozmění nebo dokonce smaže. Integrita může také utrpět v případě selhání hardware, kdy může dojít k poškození či ztrátě dat. (Marťák, 2005)

Ochránit integritu dat dokáže například šifrování, které v případě, že dojde ke změně dat, během přenosu detekuje, zdali data nejsou korektní a není možné je dešifrovat zpět do původní podoby. Integritu dat je dále možné zajistit pomocí kontrolních součtů, které případné změny dat detekují a mohou na ně upozornit. Obranou proti nechtěnému smazání nebo úpravě dat je možné řešit vhodně nastaveným systémem zálohování. (Marťák, 2005)

1.2 Návrh, údržba a monitoring ISMS

Pro optimální stav, kdy je výsledkem dobře fungující a správně nastavený ISMS je nutné podstoupit stanovený sled úkonů. Tyto úkony je vhodné neustále cyklicky opakovat, aby byla vhodně potlačena nově vznikající rizika, která se v průběhu času objevují.



Obrázek 1 - Fáze nasazení ISMS

Zdroj: vlastní

1.2.1 Specifikace požadavků na bezpečnost

V první fázi procesu stanovení systému řízení bezpečnosti informací dochází k shromáždění požadavků na bezpečnost informací v rámci organizace. Tyto požadavky vycházejí ze strategií a cílů organizace. Požadavky dále ovlivňuje velikost a geografické rozložení organizace. (ÚNMZ, 2017, s. 23)

V první řadě je nutné zjistit povahu informačních aktiv a stanovit hodnotu, kterou pro organizaci mají. Dále je nutné posoudit, jak je s informacemi nakládáno, jaké jsou formy výměny tohoto aktiva a vše zkombinovat se smluvními a právními požadavky organizace.

K požadavkům se dále metodicky specifikují rizika, které informačním aktivům hrozí. (ÚNMZ, 2017, s. 23)

1.2.2 Hodnocení bezpečnostních rizik

Ihned po vyhledání rizik následuje fáze, ve které je nutné stanovit pomocí vhodných metod míru závažnosti rizik. Tyto metody by měly umožnit kvantifikovat rizika, hlavně po stránce nákladů na jejich potlačení, a následně stanovit prioritu, jak budou přijímána opatření. Všechna tato hodnocení musí být v souladu s cíli organizace. Hodnocení bezpečnostních rizik by mělo být výstupem tzv. rizikové analýzy. (ÚNMZ, 2017, s. 23)

Hodnotit bezpečnostní rizika je vhodné periodicky, protože v oblasti bezpečnosti dochází k neustálému vývoji. Současně periodické hodnocení zaručí, že budou podchycena veškerá rizika, která se objeví ve správě informačních aktiv, protože interní systémy organizace se neustále vyvíjí a s tímto vývojem vznikají další potencionální hrozby, které je nutné ohodnotit a ošetřit. Hodnocení rizik by mělo být prováděno metodickou formou tak, aby byla zaručena reprodukovatelnost výsledku a jejich vzájemné porovnání. Posuzováním rizik se v rámci řady norem ISO/IEC 27000 zabývá norma ISO/IEC 27002, která obsahuje pokyny a metody pro posuzování rizik. (ÚNMZ, 2017, s. 23)

1.2.3 Navržení opatření na potlačení rizik

Před návrhem opatření by měla organizace rozhodnout, která rizika budou ošetřena, a která je možné akceptovat. Kritériem pro akceptaci rizika je cena, kterou stojí potlačení rizika ve srovnání s možným přínosem a pravděpodobnost, s jakou se může dané riziko objevit. Obecně je možné s riziky nakládat:

- aplikací vhodných protiopatření v rámci organizace, které riziko sníží nebo vyruší,
- přijetím rizika, pokud se ošetření nevyplatí nebo nenaruší zásadně chod organizace,
- vyhnutím se riziku, pomocí například změn činností a procesů v rámci organizace,
- zapojením jiných společností, například pojišťoven, které dané riziko zastoupí.

Pro rizika, u nichž je rozhodnuto, že dojde na implementaci opatření, je nutné vybrat vhodná opatření a následně tato opatření nasadit do praxe. (ÚNMZ, 2017, s. 23-24)

1.2.4 Výběr a nasazení opatření

Opatření je vhodné zvažovat již v době specifikace požadavků na bezpečnost. Předejdeme tak dodatečným nákladům na implementaci těchto opatření nebo situaci, kdy je vybrané řešení méně efektivní. S výběrem opatření je také možno využít předpřipravené normy. Norma

ISO/IEC 27002 nemusí být pro potřeby zkoumané organizace použitelná a je nutné navržená opatření v této normě vhodně upravit. (ÚNMZ, 2017)

V průběhu implementace opatření je možné, že dojde po určitou dobu ke zvýšení rizika. O této situaci je nutné informovat veškeré strany, které se podílí na implementaci, aby bylo možné přijmout některá krátkodobá opatření, která i tyto situace pokryjí. (ÚNMZ, 2017)

Výsledkem procesu nasazení je soubor opatření, který pomáhá zvýšit bezpečnost informačního aktiva. Tento soubor nemůže být nikdy dokonalý, a proto je potřeba neustálého monitoringu a údržby. (ÚNMZ, 2017)

1.2.5 Monitoring a údržba ISMS

Neustálá kontrola a hodnocení ISMS je jednou z důležitých součástí systému řízení bezpečnosti informací. Je nutné systém neustále monitorovat, aby byla zaručena maximální efektivita opatření a případně přezkoumat části, jejichž výkonnost není ideální. V průběhu monitoringu dochází k tvorbě zpráv, které se předávají managementu organizace, který na základě těchto reportů může verifikovat použitá opatření, kontrolovat, jestli přijatá opatření pokrývají veškerá rizika, která nebyla akceptována, navrhovat nápravná opatření a případně sledovat, jestli mají požadovaný efekt. (ÚNMZ, 2017, s. 24)

1.2.6 Zlepšování ISMS

Cílem snahy zlepšování systému řízení bezpečnosti informací je zachování hlavních atributů, tj. důvěrnost, dostupnost a integrita. U existujícího systému je nutné neustále hledat příležitosti pro zlepšení, které mohou být efektivnější nebo levnější než současná řešení, která jsou v rámci organizace implementována. Pro identifikaci částí, které by bylo možné vylepšit, je možné použít zpětnou vazbu od zákazníků, audity nebo přezkum systému řízení bezpečnosti informací. (ÚNMZ, 2017, s. 24-25)

1.3 Přehled norem řady ISO/IEC 27000

1.3.1 ISO/IEC 27001

Norma ISO/IEC 27001 specifikuje požadavky na vybudování, zavedení, provoz a následný monitoring a údržbu systému řízení bezpečnosti informací. V této normě jsou uvedena také specifika pro případnou certifikaci ISMS. Text normy je vhodný pro organizace všech typů a velikostí. (ÚNMZ, 2017, s. 26-30)

1.3.2 ISO/IEC 27002

Tato norma definuje seznam nejlepších praktik, které je možné využít k implementaci bezpečnostních opatření, jejichž cílem je zvýšit zabezpečení informačního aktiva v rámci organizace. Opatření jsou rozdělena do 14 oblastí, mezi která patří například:

- bezpečnost lidských zdrojů,
- technologie krytování,
- bezpečnost pro dodavatele,
- zvládání bezpečnostních incidentu a jiné. (Management Mania, 2017)

1.3.3 ISO/IEC 27003

ISO/IEC 27003 poskytuje soubor doporučení k implementaci požadavků, které jsou specifikované v normě ISO/IEC 27001. Znění této normy není pro organizace závazné, samy si mohou určit, která doporučení odpovídají jejich specifikům. Některá doporučení nejsou vhodná pro organizace vzhledem k jejich velikosti, jejich nasazení by bylo kontraproduktivní. (ÚNMZ, 2017, s. 26-30)

1.3.4 ISO/IEC 27004

Norma ISO/IEC 27004 definuje pokyny, které pomáhají organizacím měřit a hodnotit výkonnost a efektivnost nasazeného systému řízeni bezpečnosti informací. Zajišťuje rámec, který zvládne analyzovat a zhodnotit systém, jestli plní požadavky dle normy ISO/IEC 27001. Znění normy je vhodné pro všechny typy a velikosti organizací. (ÚNMZ, 2017, s. 26-30)

1.3.5 ISO/IEC 27005

Tato norma definuje doporučení pro správu rizik, ale nenabízí pro tuto činnost konkrétní metodiku. Způsob řízení rizik nechává plně v kompetenci organizace, protože každý ISMS je specifický pro svoji velikost nebo průmyslové odvětví. Text normy je zaměřen pro pracovníky, kteří jsou odpovědní za správu rizik a je vhodný pro všechny typy a velikosti organizací. (ÚNMZ, 2017, s. 26-30)

1.3.6 ISO/IEC 27006

Norma poskytuje pokyny, které umožnují orgánům, které jsou k tomu pověřené, provádět audit a certifikaci systému řízení bezpečnosti informací. Definuje proces, který vede k akreditaci orgánů, které umožnují certifikaci a současně specifikuje požadavky a odborné způsobilosti, které jsou na tyto orgány kladeny. (ÚNMZ, 2017, s. 26-30)

1.3.7 ISO/IEC 27007

Tento dokument popisuje pokyny pro řízení auditů systémů řízení bezpečnosti informací. Dále obsahuje pokyny k provádění interních a externích auditů a obsahuje kompetence a hodnocení auditorů ISMS. Vše je napsáno v souladu s normou ISO/IEC 27001. (ÚNMZ, 2017, s. 26-30)

1.3.8 ISO/IEC TR 27008

Technický report obsahuje sadu doporučení pro auditory, které se používají na přezkum systémů řízení bezpečnosti informací. Tato zpráva zkoumá převážné implementaci a provozní opatření, které srovnává s normami bezpečnosti informací. (ÚNMZ, 2017, s. 26-30)

1.3.9 ISO/IEC 27013

Norma ISO/IEC 27013 se zabývá společnou implementací norem ISO/IEC 27001 a ISO/IEC 20000-1. Definuje pokyny pro případy, kdy je buď jedna či druhá norma implementována nebo i pro případy, že budou obě implementovány naráz. Obsahuje také pokyny pro sjednocení implementací obou norem, když jsou již v systému implementované. Dalším účelem této normy je ulehčit organizacím pochopení podobností a odlišností obou norem. (ÚNMZ, 2017, s. 26-30)

1.3.10 ISO/IEC 27014

Tento dokument specifikuje procesy, které se používají pro správu a monitoring systému bezpečnosti informací. Pro organizace je klíčová bezpečnost, a proto narůstají nároky na zajištění vlastní bezpečnosti a současně i na organizace, které provádí dohled nad bezpečností informací. Organizace zodpovědné za bezpečnost musí provádět často dohled nad těmito systémy a tím pomáhají držet bezpečnost informací na dostatečné úrovni, což zabezpečuje snazší dosahování cílů organizace, kde je dohled prováděn. (ÚNMZ, 2017, s. 26-30)

1.3.11 ISO/IEC TR 27016

Tato technologická zpráva je určena především organizacím, kterým pomáhá lépe oceňovat informační aktiva, zejména po ekonomické stránce. Zpráva dále obsahuje návody, jak hodnotit dopady rizik, které tomuto aktivu hrozí a v neposlední řadě poskytuje nástroje pro vyčíslení ekonomických přínosů, které nastanou v případě, že je toto aktivum vhodně ochráněno. V celkovém součtu je tedy možné pomocí této zprávy stanovit konkrétní částku, která je potřeba pro ochranu informačního aktiva. (ÚNMZ, 2017, s. 26-30)

1.3.12 Normy specifické dle odvětví

Každé odvětví má svá specifika, která ovlivňují i systém řízení bezpečnosti informací. Pro každou specifickou oblast je nutné tyto systémy upravovat, a proto pro různá odvětví vznikly řady norem, které normy uvedené v této kapitole dále specifikují pro konkrétní nasazení. Speciální normy má například odvětví telekomunikací (ISO/IEC 27011), financí (ISO/IEC TR 27015), cloudových služeb (ISO/IEC 27017) nebo energetiky (ISO/IEC TR 27019). (ÚNMZ, 2017, s. 26-30)

2 ČSN ISO/IEC 27033-3

Část této normy, jejíž poslední vydání pochází z března roku 2015, popisuje konkrétní síťové scénáře, u kterých poukazuje na možné hrozby, specifikuje opatření, která tyto hrozby mohou eliminovat, a případně odkazuje na další normy, kde je možné se dozvědět více informací o technikách zabezpečení.

Kromě síťových scénářů definuje norma další bezpečnostní faktory, například nepopiratelnost či opacitu, které nebyly probrány v předchozí kapitole v rámci normy ISO/IEC 27000. K těmto bezpečnostním pojmům dále definuje možné mechanismy, které pomáhají tyto faktory naplnit.

V příloze se nachází podrobný příklad politik, které souvisí s používáním internetu a katalog hrozeb, u kterých je specifikováno, jaké situace konkrétní hrozby zahrnují.

2.1 Faktory bezpečnosti

2.1.1 Řízení přístupu

Faktor řízení přístupu zajišťuje pomocí mechanismů autentizace a autorizace stav, kdy mohou k daným datům, aplikacím nebo zařízením přistupovat uživatelé, kteří k tomu mají oprávnění. Oprávnění kontroluje systém při pokusu o přístup ke konkrétnímu aktivu a v případě, že uživatel oprávnění nemá, tak přístup zamítne. V případě zamítnutí přístupu je vhodné tuto situaci zaznamenat. Oprávnění může být přiděleno konkrétnímu uživateli či skupině uživatelů. Mechanismy používané k zajištění řízení přístupů jsou přístupové seznamy, tzv. access control list, ve kterých je jasně definováno, kdo má ke konkrétnímu aktivu přístup. (ÚNMZ, 2015, s. 10)

2.1.2 Autentizace

Procesu ověření identity uživatele se říká autentizace. V případě, že chceme přistoupit do zabezpečených části systému, tak musíme nějak svoji identitu doložit. Tento proces se uskutečňuje pomocí jednoduchých mechanismů, založených na jméně a hesle, digitálních certifikátech, digitálních podpisech, biometrických údajích nebo pomocí CHAP či SSO. Každý z těchto systému má své výhody a nevýhody, a proto se často různě kombinují. (ÚNMZ, 2015, s. 10)

Autentizace může mít několik podob, které rozlišujeme podle úrovně zabezpečení, které chceme dosáhnout. V praxi se nejčastěji používá jednofaktorová autentizace, kde se pro doložení identity používá například již zmíněné jméno a heslo. U systému, kde se očekává větší míra důvěry, typicky bankovní služby, se používá dvoufaktorová autentizace, kde se kromě

uživatelského jména a hesla používá ještě další krok. Typicky se jedná o mobilní telefon, do kterého je odeslána SMS zpráva s kódem. Méně se používá třífaktorová autentizace, kde se navíc ještě přidávají biometrické prvky, například otisk prstu. (ÚNMZ, 2015, s. 10, ManagementMania.com, 2018)

2.1.3 Bezpečnost komunikace

O zaručení správné cesty toku informací se stará atribut bezpečnosti komunikace. Pro ustanovení bezpečné cesty mezi konci komunikačního kanálu je důležité, aby celá cesta vedla napříč autorizovanými body. Tento stav zajistí, že komunikace nemůže být odkloněna nebo zachycena. Vhodným opatřením, které je zde možné aplikovat, je použití technologie IPsec nebo využití soukromých linek a oddělených sítí. (ÚNMZ, 2015, s. 10-11)

2.1.4 Nepopiratelnost

Atribut nepopiratelnosti se zabývá důkladným zaznamenáváním událostí, které se v systému dějí. Tento záznam dokáže identifikovat jednotlivé osoby, které se například snažili získat přístup k datům, ke kterým nemají oprávnění nebo vysledovat osoby, které zanesly chybné údaje do systému. Mechanismy, které se používají k zachování nepopiratelnosti, jsou především logovací soubory, které zaznamenávají každou událost včetně časových značek. Uživatelé jsou identifikování pomocí digitálních podpisů a současně se zde používá řízení přístupu, kde jsou nadefinované jednotlivé uživatelské role. (ÚNMZ, 2015, s. 10-11)

2.1.5 Opacita

Opacita ochraňuje informace, které je možné odvodit ze sítového provozu. Tento princip se nezabývá ochranou informací jako takových, ale utajením činností, které souvisí s přenosem a tvorbou těchto informací. Příkladem může být telefonní hovor. Informace předané pomocí tohoto hovoru podléhají atributu důvěrnosti, ale samotná činnost, tzn. uskutečněný hovor mezi dvěma osobami, podléhá opacitě, která by měla tuto skutečnost utajit. Možnosti, jak zajistit opacitu v síti je několik. Je možné využít například technologii VPN s IPsec nebo NAT. (ÚNMZ, 2015, s. 10-11)

2.2 Síťové scénáře

2.2.1 Služby přístupu k internetu pro zaměstnance

Na moderní pracoviště patří i možnost připojení zaměstnanců k internetu. Zaměstnanci mohou díky němu v pracovní době komunikovat s kolegy, dále se vzdělávat nebo dohledávat potřebné údaje, například kontakty na jiné subjekty. Pro organizaci je tedy výhodné umožnit zaměstnancům přístup k internetu, ale má to svá úskalí. Je nutné stanovit určitá pravidla, která

tento přístup omezí. Je žádoucí, aby zaměstnanci zbytečně netrávili pracovní dobu internetovými sázkami nebo zbytečně neubírali šířku pásma pro pirátskou činnost, například stahováním a šířením multimediálního obsahu. (ÚNMZ, 2015, s. 11)

Mezi nejčastější útoky v případě přístupu k internetu patří různé druhy virů a malware. Zavedení virů a malware může přivodit organizaci ztrátu dat, zcizení dat nebo vést ke ztrátě kontroly nad IT zařízeními. Způsobů, jak je možné viry a malware do infrastruktury zavést je mnoho. Zaměstnanci mohou v pracovní době stahovat soubory z internetu, z příloh e-mailů nebo vyměňovat soubory pomocí služeb pro okamžité zasílání zpráv (IM). Uživatel většinou takový soubor stáhne a spustí neúmyslně, ale výsledkem je přesně stav, který si útočník přál. Nainstalovaná škodlivá aplikace se pak pomocí technik, mezi které patří port agility nebo šifrování, dokáže vyhýbat bezpečnostním opatřením a škodit. (ÚNMZ, 2015, s. 11-13)

Některé druhy útoků využívají k zavedení virů zranitelností běžně používaných aplikací jako například webové prohlížeče. V takovém případě dochází k aplikaci malware, který je použije k zavedení další virové infekce, která může ovlivnit dostupnost některých částí sítě a způsobí nežádoucí šíření viru. V těchto případech dochází tedy k ovlivnění atributu dostupnosti. K ohrožení důvěrnosti dochází v případě, že dojde k nakažení pomocí trojského koně, který umožní přístup neautorizovaných uživatelů. (ÚNMZ, 2015, s. 11-13)

Řešením této hrozby je v prvním řadě omezení přístupu k internetu. Je vhodné blokovat služby, které uživatelé nepotřebují k výkonu své pracovní činnosti, a tak omezit riziko, že dojde k zavedení nechtěného softwaru. V další řadě je žádoucí, aby byl na branách a stanicích, kde se přistupuje k internetu, instalován antivirový software, který obsahuje nejnovější virové signatury. Vhodná je i neustálá verifikace integrity souborů pomocí kontrolních součtů, aby byla odhalena situace, kdy je například k existujícímu softwarovému vybavení dodán nežádoucí kód. V neposlední řadě je nutné používat poslední pravidelně aktualizovaný internetový prohlížeč, který ideálně umí blokovat automaticky otevíraná okna. (ÚNMZ, 2015, s. 11-13)

Další bezpečnostní hrozbou je únik informací. Většinou je jí zneužito v případě spuštění neautorizovaného přenosného kódu, který komunikuje s webovým serverem, na který nahrává citlivá data. V případě, kdy je přenos šifrovaný, například pomocí TLS, tak není možné formou logovaní tento stav dostatečně zachytit. Řešením úniku informací, který je zapříčinění spuštěním tohoto mobilního kódu, je tento kód filtrovat na vstupních branách a zavést seznam povolených stránek, odkud je možné tento kód bez rizika přijímat. Současně je vhodné zajistit,

aby byl přijat pouze kód, který byl řádně podepsán certifikačními autoritami. (ÚNMZ, 2015, s. 12-13)

Bezpečnostní hrozba, kdy dochází k neautorizovanému použití a přístupu systému, se může specifikovat jako odebrání kontroly nad systémem, což může snadno vést k omezení přístupu k systému pro autorizované osoby nebo využít systém k podvodu a zfalšovat data v něm uložená. Tento typ hrozby je možné eliminovat omezením přístupu, aby každý uživatel měl přístup jen k těm částem systému, které skutečně potřebuje k výkonu své činnosti. Další možnosti spočívají v důkladném logovaní všech činností v systému, které umožnují přenos dat do internetu. (ÚNMZ, 2015, s. 12-13)

V rámci zaměstnaneckého přístupu k internetu může dojít k nedodržení právních předpisů, které jsou specifikované v rámci legislativy, regulí nebo politik organizace. Tyto typy pochybení je možné odhalit pomocí logování, kde je vyznačen čas a uživatel, který daný pokyn provedl. Předcházet se těmto pochybením dá vhodným proškolením zaměstnanců. (ÚNMZ, 2015, s. 12-13)

Posledním typem hrozby je snížení dostupnosti sítě v případě, kdy nestačí dostupná šířka pásma. K této hrozbě může docházet v případě, kdy zaměstnanci nadměrně využívají služby pro streamování obsahu nebo P2P služby. Seznam opatření v takovém případě zahrnuje omezení šířky pásma pro streamovaná média a současně je vhodné přikročit k zákazu sdílení souborů za využívání P2P služeb, které nesouvisí s pracovní činností zaměstnance. Výhodné je také monitorování síťového provozu. (ÚNMZ, 2015, s. 12-13)

2.2.2 Služby typu společnost – společnost

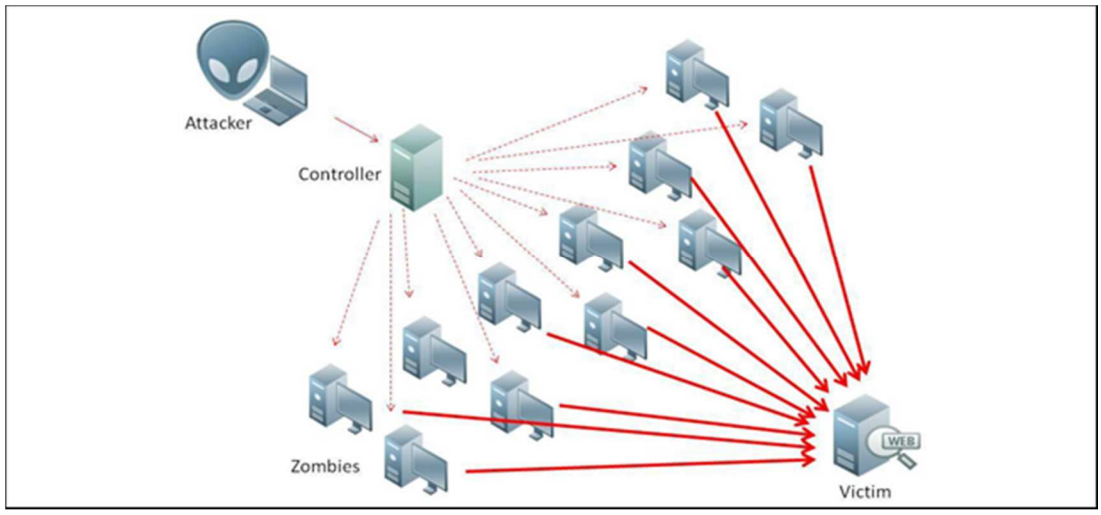
V dnešní době stoupá požadavek na komunikaci jak mezi lidmi, tak mezi společnostmi. Komunikovat spolu mohou výrobci, společnosti, které produkty dále prodávají, ale i ty, které zajišťují následující servis a údržbu. V minulosti byly k těmto účelům využívané pronajaté linky nebo síťové segmenty. V současnosti je pro společnosti výhodnější komunikovat přes internet, který přináší více možností, ale současně i nová rizika. (ÚNMZ, 2015, s. 14)

V rámci scénáře typu společnost – společnost se všechny komunikující subjekty znají, protože jsou předem registrovaní. Ke komunikaci se nejčastěji využívá internet, ale existují případy, kdy se využívá pouze extranet nebo kombinace extranetu a internetu. Služby, provozované podle tohoto scénáře, mají obvykle specifické požadavky na dostupnost a spolehlivost komunikace. Společnosti jsou většinou na těchto službách závislé. Použití internetu přináší úplně nový pohled na komunikaci v rámci společností, ale je potřeba uvažovat rozdílné

vlastnosti. U internetu se nedá předpokládat kvalita použité služby, která byla známa z využívání pronajatých okruhů. Je také nutné potlačit bezpečnostní rizika spojená s využitím internetu. Mezi největší rizika patří ztráta důvěrnosti, v případě, že k sdíleným datům přistoupí neautorizovaný subjekt a dostupnost, která může být ohrožena útoky, vedené například konkurencí. Pro organizace je žádoucí se s těmito výzvami vypořádat, protože to posiluje jejich vzájemnou důvěru. (ÚNMZ, 2015, s. 14)

Stejně jako u scénáře v předchozí kapitole, tak i zde hrozí virové útoky a zavedení malware. Malware v těchto systémech slouží k neoprávněnému přístupu do systému, kde se může útočník dostat k důvěrným datům. Současně může využít zranitelnosti ve webových službách k zavedení dalších virů. Obranou proti této hrozbě je instalace antivirových řešení na branách systémů, kde skenují veškerý provoz. Důležitý je také dohled nad aktualizacemi těchto systému, protože bez aktuálních definic nemůže antivirové řešení zajistit spolehlivou ochranu. Dalším způsobem ochrany je skenovaní všech uložených souborů na přítomnost virů, trojských koní a ostatního malwaru. S tímto krokem souvisí i kontrola těchto souborů pomocí kontrolních součtů, protože virus může narušit integritu těchto souborů a být jejich součástí. (ÚNMZ, 2015, s. 14)

Další formou útoku je odepření služby, tzv. DoS útoky. Existují i ve formě distribuovaných útoků, kdy se na útoku podílí vetší množství distribuovaných zařízení. Tyto útoky jsou vedeny proti portálům společností nebo na jejich extranety. Potlačit tyto útoky není snadné. Je nutné zablokovat porty nepoužívaných služeb, aby je nebylo možné napadat. Současně je dobré ztížit situaci pro útočníky vyřazením důležitých informací z výstražných nebo chybových hlášek, protože je pro ně pak složitější zjistit, jak je systém navržen. (ÚNMZ, 2015, s. 14)



Obrázek 2 - DDoS útok

Zdroj: zpracováno dle (Stewart, 2016)

Útok na systém může přijít i zevnitř organizace. Může být veden zaměstnanci, pro které je systém určen. Ti následně mohou přistupovat k datům, která dále šíří, například je předávají konkurenci. Snížit riziko těchto útoků je možné za pomocí firemních politik, které jasně definují uživatelské role a odpovědnosti. Důležité je omezit práva všech uživatelů, protože každý zaměstnanec nemusí mít přístup k celému systému, ale stačí pouze části, které jsou nutné pro výkon jeho práce. Vhodné také je veškeré činnosti logovat, aby byla zajištěna nepopiratelnost. (ÚNMZ, 2015, s. 15)

Poslední hrozbou u systémů typu společnost – společnost je padělání obsahu a transakcí. Tyto útoky manipulují se zprávami, které jsou předávány v rámci komunikace mezi společnostmi. Útočník může zprávy přesměrovat, takže nedorazí k určenému příjemci nebo může padělat jejich obsah, aby příjemce dostal jiná data, než o která si žádal. Obranou proti těmto hrozbám jsou transakční logy a digitální podpisy. (ÚNMZ, 2015, s. 15)

2.2.3 Služby typu společnost – zákazník

Scénář, kdy dochází ke komunikaci mezi společností a zákazníkem, se využívá především v e-komerci, e-bankovnictví a e-governmentu. Pro většinu těchto služeb je důležité zachování atributů integrity a důvěrnosti, obzvláště u služeb typu e-bankovnictví. U všech těchto služeb je očekávána maximální bezpečnost komunikace po cestě mezi službou a zákazníkem. K tomuto předpokladu se řadí převážně odolnost proti Man in the middle útokům a Man in the browser. Pro e-komerci je důležité zachování maximální dostupnosti, protože nedostupná služba může generovat ztráty v astronomických sumách. (ÚNMZ, 2015, s. 15)

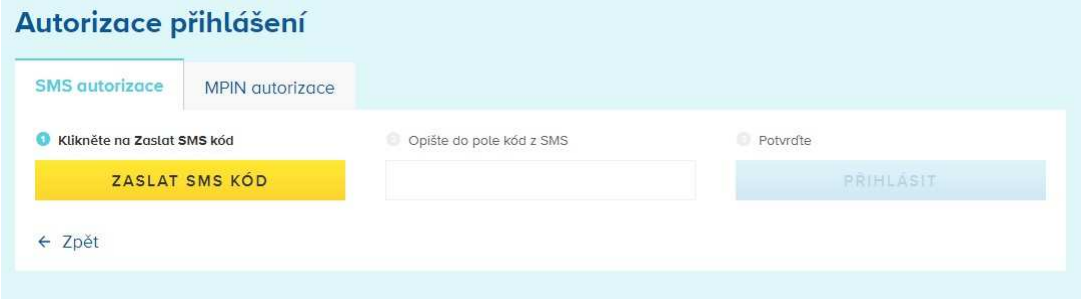
V informační bezpečnosti v rámci systému typu společnost – zákazník je nutné vzít v potaz fakt, že je možné mít dva typy koncových zařízení, pomocí kterých je do systému přistupováno. Jedná se o možnost, kdy je využita platforma, která je zaručená a je pod kontrolou dané organizace, ve které se snadno nastavují vhodná pravidla pro potlačení rizik. Druhým přístupem je platforma zákazníka, která představuje klasický počítač. V takovém prostředí je obvykle těžší nasadit potřebná opatření na udržení bezpečnosti. Taková platforma představuje značné riziko, a proto je dobré smluvně stanovit základní soubor pravidel, která zaručují bezpečné připojení do systému organizace. (ÚNMZ, 2015, s. 15)

V první řadě je u systému riziko v podobě virových útoků a možnost zavedení malware. Tato hrozba s sebou přináší narušení bezpečnosti a možný přístup k citlivým údajům. Možné je i využití zranitelností v rámci webových prohlížečů a aplikací, které může vést k umístění virové infekce a trojských koní. Obranou proti této hrozbě je nasazení software na kontrolu virových definic na vstupních branách systémů a koncových zařízení. Současně je vhodné zajistit pravidelné skenovaní uložených souborů, u kterých je vhodné kontrolovat přítomnost virů a současně sledovat jejich integritu pomocí kontrolních součtů. (ÚNMZ, 2015, s. 15-16)

Dalším rizikem je neautorizovaný přístup do systémů. Může mít několik podob. Je možné, že útočník napadne databázi služby, ze které následně vytáhne data pomocí některého známého útoku, například SQL injection nebo útoku typu cross-site scripting. Jinou možností je získání informací o uživatelském účtu pomocí odpovědí aplikace, která jsou reakcí na pokusy o autentizaci uživatele. Velmi často se k těmto pokusům využívají automatizované skripty, které dokáží zjistit identifikátory uživatele. V posledních letech roste také riziko útoků za využití sociálního inženýrství, kde je využíváno phishingu nebo podvržení DNS záznamů, které přesměrují uživatele na věrohodně vypadající, ale falešné stránky útočníka, kam zadají své osobní údaje, které následně útočník zneužije. Útočník se může pokusit o celou řadu dalších útoků, které je možné využít k páchání nekalé činnost, jejímž cílem je krádež citlivých údajů nebo jejich modifikace či zničení. (ÚNMZ, 2015, s. 15-16)

Obranou proti těmto útokům je vhodné omezení oprávnění systému. V rámci útoků na databázi je vhodné zajistiti omezení přístupu z webové aplikace. Ve webové aplikaci je také žádoucí, aby docházelo k filtrování vstupních formulářů, které by mohly být využity k útoku typu SQL injection. Vhodnou obranou proti tomuto útoku je také využití překompilovaných dotazů. Dále je nutné zajistit bezpečnou registraci nových uživatelů systému, u kterých musí být naprosto jisté, že přístupová práva získá pouze autentický uživatel. Toto je možné zajistit pomocí

nezávislé registrační autority. V dalším kroku je nutné autentizovat uživatele. Možnosti, kterých je možno využít, je celá řada. Mezi nejpoužívanější se řadí digitální certifikáty, hesla, biometrické údaje nebo speciální hardware jakým jsou například čipové karty. V případech, kdy je nutná větší úroveň zabezpečení, je žádoucí zvolit vícefaktorovou autentizaci, například kombinací hesla a SMS kódu. Důležitou součástí opatření je dále logovaní všech událostí v systému a jejich pravidelná kontrola, aby došlo k odhalení veškerého nežádoucího jednání. (ÚNMZ, 2015, s. 16, ManagementMania.com, 2018)



Obrázek 3 - Příklad SMS autentizace v e-bankovnictví

Zdroj: vlastní

Zvláštní kategorií opatření je šifrování. V systémech typu společnost – zákazník by měla být šifrována veškerá data, která jsou trvale uchovávána. Dále by měla být zabezpečena komunikace mezi klientem a webovým serverem. K tomu je možné využít protokoly SSL ve verzi 3 nebo TLS, které zajišťují šifrování a autentizaci komunikujících stran. V rámci webové aplikace je potom nutné šifrovat veškerá data, která se nachází v URL, cookies a skrytých prvcích. Je to opatření pro zachování integrity. Veškeré proměnné údaje je dobré opatřit časovou značkou, aby bylo možné zjistit čas poslední modifikace. Pro citlivá data je pak vhodné využít kryptografické hašovací funkce. (ÚNMZ, 2015, s. 16)

Hrozbou pro tyto služby je i možnost odepření přístupu. Nastává v případech, kdy jsou portály služeb přetěžovány velkým množstvím požadavků. V takovém případě je služba pro ostatní uživatele nedostupná a generuje po dobu své nefunkčnosti ztrátu. Obranou proti těmto útokům je blokace nepotřebných služeb, protokolů a portů, aby cílový systém nemusel reagovat na požadavky, které na ně vedou. Dále je vhodné blokovat nadměrný provoz, který pochází z určitého zdroje nebo zdrojů. (ÚNMZ, 2015, s. 16-17)

Posledním typem útoků je padělání obsahu transakce. Jedná se o útok, kdy jsou přenášená data kompromitována a je změněn jejich obsah. Může dojít i k přesměrování zprávy do jiné

destinace, než kam byla zamýšlena. Obranou proti tomuto typu útoku je vedení transakčního logu a využití digitálních podpisů. (ÚNMZ, 2015, s. 16-17)

2.2.4 Rozšířené služby založené na spolupráci

V organizacích, které zaměstnávají větší množství zaměstnanců, je většina interních procesů spojena se sdílením dokumentů, výměnou informací ať už formou webových služeb, emailových konverzací nebo komunikací založené na přenosu hlasu a obrazu. Elektronická výměna informací usnadňuje práci zaměstnanců, zvyšuje efektivitu a šetří náklady. Například v případě několika poboček v rámci celého světa je levnější uspořádat poradu pomocí videohovoru než za pomoci osobního setkání, protože náklady na uspořádání videohovoru jsou podstatně nižší a současně je ušetřen čas spojený s cestováním a jiné další návazné problémy. (ÚNMZ, 2015, s. 17)

Systémy pro spolupráci je možné rozdělit do několika kategorií. První dělení je na systémy interní, které jsou použity v jen v rámci organizace a externí, které jsou použity jak v rámci organizace, tak pro komunikaci s externími partnery. Druhé dělení je na systémy, které si implementuje konkrétní organizace přímo na míru sama anebo druhou možností je nákup systému třetí strany. Obojí nese řadu výhod i nevýhod. V případě interních systémů může být výhodnější, když si daný systém napíše organizace na míru vlastním požadavkům. V takovém případě je systém lépe přizpůsoben procesům uvnitř organizace, nepotřebuje komunikační rozhraní pro externí subjekty, takže je o něco jednodušší a současně zde odpadá řada bezpečnostních rizik. Na druhé straně nasazení systému třetí strany je levnější, protože není třeba investovat do tvorby, provozu a údržby vlastního systému. V případě externích systému je vhodnější použití systému třetí strany, protože obsahují standardizované komunikační rozhraní, takže se snadněji navazuje komunikace s externími subjekty. Vždy záleží na konkrétní situaci v organizaci, není možné říci, že tyto výhody a nevýhody platí u obou druhů systémů vždy. (ÚNMZ, 2015, s. 17)

Mezi bezpečnostní hrozby u systému pro spolupráci se řadí neautorizovaný přístup vedoucí k vyzrazení citlivých informací. Tato hrozba vede k zneužití těchto systému pro sdílení nelegálního obsahu, který porušuje autorská práva nebo naopak umožnuje krádež, jejímž výsledkem je získání citlivých dat, jejichž vyzrazení může být pro organizaci nebezpečné, protože může vést k finančním ztrátám nebo ztrátě důvěry v organizaci. Dále je možné pomocí těchto systému šířit nevyžádanou poštu nebo reklamu. Obranou proti těmto útokům je vhodné nastavení uživatelských rolí, které jasně definují přístup k aplikacím a uložištím. Uživatelé je

možné podle rolí dělit do VLAN, které mají různě definované úrovně oprávnění. Ověření uživatelů by mělo být zajištěno pomocí silné autentizace a autorizace a současně je nutné zajistit, aby veškerá data, která se nachází v systému, byla šifrována. (ÚNMZ, 2015, s. 17-18)

Hrozba virového útoku a zavedení malwaru je zde možná díky sdílení souborů v rámci systému, které usnadňuje distribuci na zařízení. Adekvátní obranou na tento útok je umožnit pouze terminálový přístup ke službám, protože dochází k minimalizaci přenosu dat v rámci systému. (ÚNMZ, 2015, s. 18)

Poslední hrozba systému spolupráce je omezení dostupnosti sítě, které může být způsobeno přetížením sítě komunikací, která je legitimní anebo využitím zranitelností protokolů, které využívají služby nasazené v tomto systému. Vhodným opatřením proti této hrozbě je využití virtuálních SAN sítí, které vede ke zlepšení dostupnosti. Možné je také nasazení monitorovacího software, který slouží k zaznamenávání událostí, které nastanou v případě, kdy je nějaká aplikace nebo sítový zdroj nedostupný. (ÚNMZ, 2015, s. 18)

2.2.5 Segmentace sítě

Jednou z technik, která se využívá k rozšíření principu řízení přístupu, je segmentace sítě. Síť je možné segmentovat podle typů aplikací, aktivit nebo systémů. Pro každý segment pak platí určitá pravidla a mají do něj přístup jen někteří uživatelé. Segmentaci je možné využít například pro oddělení kritických systémů. V určitých případech řeší segmentace i legislativní problémy, protože velikost segmentu je stanovena jako území jedné země. Jedná se o případy, kdy země požaduje, aby data jejich uživatelů nebyla přenášena přes hranice do jiného státu. (ÚNMZ, 2015, s. 18-19)

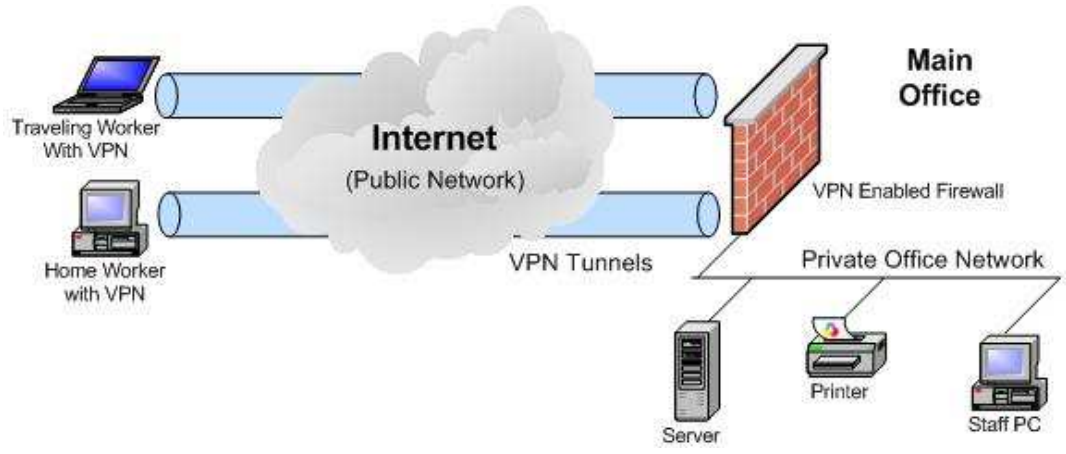
Norma ČSN ISO/IEC 27033-3 nespecifikuje mnoho bezpečnostních hrozeb. Jedna z nich je odpovědnost v důsledku nedodržování právních předpisů. Systém tedy nesplňuje legislativu dané země. V takovém případě je nutné tento stav opravit a současně mít povědomí o kompletním znění legislativy v dané zemi, aby systém v segmentu používal povolené šifrovací technologie, dodržoval zákony tykající se odposlechu, uchovávání, přenosu a zpracování osobních údajů. (ÚNMZ, 2015, s. 19)

Druhou hrozbou je možnost úniku dat. Tato hrozba vzniká v případě, že segmentace špatně kopíruje hranice států a dochází tak ke sdílení dat i do jiné země, než pro kterou jsou data určena. Řešením je využití bezpečnostních bran, proxy serverů a šifrování dat. (ÚNMZ, 2015, s. 19)

2.2.6 Síťová podpora pro domácí kanceláře a malé firmy

Některé organizace umožnují svým zaměstnancům práci z domova. To přináší výhody v podobě většího pohodlí a ušetřených nákladů za dopravu pro zaměstnance. Na druhé straně tento způsob práce přináší potencionální bezpečnostní rizika, jejichž eliminace není v domácích podmínkách snadná. (ÚNMZ, 2015, s. 19)

Přední bezpečnostní hrozbou u scénáře domácí kanceláře je možnost neautorizovaného přístupu. Tento stav vzniká při použití běžných SOHO zařízení, která jsou velmi často ponechána v továrním nastavení a nemají změněná výchozí hesla pro přístup do administrace. Dalším problémem bývá slabé fyzické zabezpečení používaných zařízení. Vhodnou obranou proti těmto hrozbám je vynucení silných hesel, zařízení by měla být zbavena výchozích nebo nulových hesel. Dalším bodem obrany je kontrola konfigurací sítových prvků, aby nebyly ponechány bez nastavení a měli aktivované některé funkce, které zvyšují bezpečnost, například šifrovaní Wi-Fi sítí nebo oddělené sítě pro hosty a současně deaktivovat zbytečné služby, které uživatel nevyužívá. Pro přístup ke službám organizace je žádoucí, aby byla využita technologie virtuálních privátních sítí, která zajistí bezpečné spojení přes nedůvěryhodnou sít. (ÚNMZ, 2015, s. 20)



Obrázek 4 - Využití VPN

Zdroj: zpracováno dle (Kaczmarek, 2011)

Další hrozbou v domácím prostředí nebo malé kanceláři je možnost virového útoku a zavedení malwaru. K naplnění této hrozby dochází, když zařízení nejsou opatřena softwarem, který chrání před malware. Další riziko vzniká ve chvíli, kdy uživatel pro svoji soukromou činnost používá stejné zařízení jako pro výkon povolání. V takovém případě se mísí bezpečné služby z firemního prostředí s těmi, které používá pro své soukromé účely, například P2P služby pro sdílení obsahu, který nemusí být vždy bezpečné a můžou obsahovat škodlivý software. Velmi

často také dochází k zanedbání aktualizací software, kdy uživatelé neinstalují aktuální záplaty a vystavují se tak zvýšenému riziku zavedení malwaru. Mezi opatření, která je vhodné dodržovat, patří pravidelná kontrola a udržovaní aktuálních verzí softwaru spolu s pravidelnou a automatickou aktualizací virových definic pro antivirový software. Dále je vhodné skenovat všechny soubory na přítomnost virových definic a kontrolovat jejich integritu. V poslední řadě je také žádoucí, aby byl nastaven optimální systém zálohování, který umožní rychle zotavení v situaci, kdy dojde k napadení zařízení. (ÚNMZ, 2015, s. 20)

Poslední hrozbou definovanou v této normě je možnost neautorizovaného vyzrazení citlivých informací. K této situaci dochází v případech, kdy je při uchování a přenosu dat opomenuto šifrování. V jiných případech je možné zneužití WLAN připojení, které není chráněno přístupovým heslem pro neautorizovaný přístup k datům. Potlačení těchto rizik je možné pomocí zabezpečení přístupových míst do sítě, použít šifrovaní na uložená a přenášená data a současně zvyšovat znalosti uživatelů pomocí školení, aby věděli, že v domácích podmínkách s využitím běžných sítových prvků není možné dosáhnout stejné bezpečnosti jako u přístupových bran, které používají organizace k propojení poboček. (ÚNMZ, 2015, s. 20)

2.2.7 Mobilní komunikace

Pro přístup v terénu se pro zaměstnance hodí přístup pomocí mobilních zařízení, jakými jsou mobilní telefony nebo tablety. Zařízení pomáhá uživateli vyřizovat emaily, připojovat se k systémům organizace nebo vyhledávat informace na internetu. Většinou se k těmto aktivitám využívá přístroj, který je buď v osobním vlastnictví zaměstnance, nebo přístroj služební, který může zaměstnanec použít i pro soukromé účely. V obou případech kombinované použití pro soukromé a pracovní účely zanáší do procesu využívání zařízení bezpečnostní rizika. (ÚNMZ, 2015, s. 21)

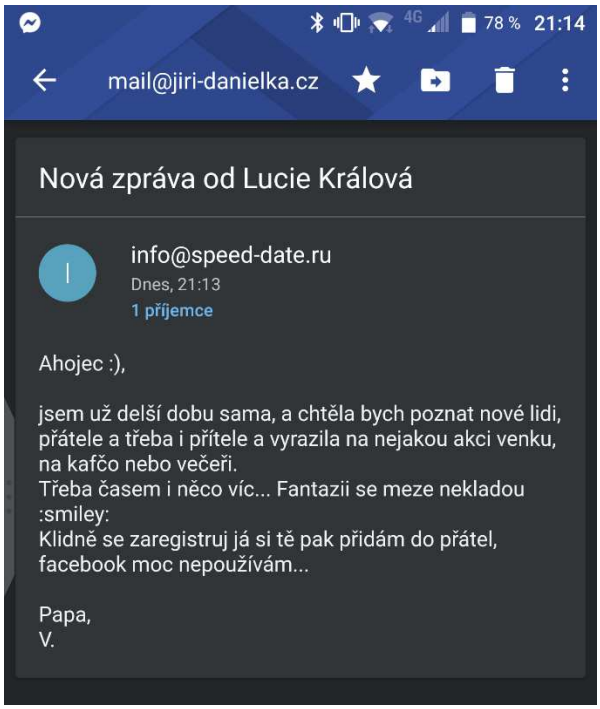
Jednou z hrozeb, která hrozí mobilnímu zařízení, je nedovolený přístup k informacím, které jsou uložené v mobilním zařízení. Tento problém vzniká v případě, kdy je mobilní zařízení nedostatečně chráněno před přístupem neautorizované osoby, například není použita zamykací obrazovka či heslo. Řešením je použití těchto prvků například v kombinaci s časovým odpočtem, který zajistí zamknutí zařízení po určité době, kdy je zařízení nevyužito. Dále je vhodné nenechávat zařízení delší dobu bez dozoru a současně při zabezpečení použít silná hesla. (ÚNMZ, 2015, s. 21-22)

Dalším nebezpečím, které u mobilních zařízení hrozí, je možnost neautorizovaného zpřístupnění citlivých a lokalizačních dat. Hlavní nebezpečí tkví v instalovaných aplikacích

třetích stran, které mohou úmyslně vysílat data o poloze zařízení. Stejné aplikace mohou odposlouchávat veškerý provoz na zařízení a předávat ho za využití sítě dále nebo je možná i situace, kdy je provoz zcela legitimní, ale je uskutečněn za využití nešifrovaných spojení, které může útočník snadno odposlechnout. Nebezpečí zpřístupnění dat ze zařízení hrozí i při nesprávné likvidaci zastaralého přístroje, kdy nedojde k jeho vymazání, a proto je pak možné, že při postupu likvidace může někdo zařízení oživit a citlivá data získat. Soubor opatření, který je zde možné použít, tvoří převážné využití šifrovaní při přenosu a ukládání dat. Při využití služeb třetí strany je nutné dostatečné ujištění, že třetí strana používá dostatečné zabezpečené komunikační protokoly. Pro vzdálená připojení do organizace je také možno využít technologie virtuální privátní sítě. V rámci organizace je také dobré stanovit vhodné postupy pro nakládání s vyřazenými zařízeními, hlavně se zaměřením na bezpečné vymazání obsahu těchto zařízení před předáním k likvidaci. Pro zajištění bezpečí v rámci lokalizačních služeb je vhodné vynutit si stav, kdy je nutné požádat uživatele o informace o poloze, aby byly poskytnuty jen v případě, kdy jsou opravdu potřebné. (ÚNMZ, 2015, s. 21-22)

Hrozba modifikace dat v zařízení je možná za pomoci využití zranitelností aplikací a operačního systému, který se nachází v mobilním zařízení. Je zde i možnost, kdy si uživatel sám stáhne aplikaci z neověřeného zdroje a zavede si tak nežádoucí malware, který byl k aplikaci přibalen. Bezpečnostní opatření proti této hrozbě obsahují pravidelné a nejlépe automatické instalace aktualizací software a záplat operačního systému a současně povolit možnost, že software je možné instalovat pouze z ověřených zdrojů, nejlépe s využitím digitálních podpisů těchto zdrojů, které slouží k jejich ověření. (ÚNMZ, 2015, s. 21-22)

Mobilní zařízení může ohrozit také přijímání spamu. Útočník ho může využít k formám sociálního inženýrství, které vede k neúmyslnému vyzrazení citlivých údajů o uživateli. Příjem spamu je také nežádoucí v případě, kdy mobilní zařízení disponuje připojením do internetu, které je účtováno za objem přenesených dat. V takovém případě přináší příjem těchto nevyžádaných zpráv další zbytečné náklady, které jsou potřeba na provoz mobilního zařízení. Proti spamu je možné se bránit nasazením filtrování emailové korespondence a útoky pomocí sociálního inženýrství potlačit pomocí vzdělávání zaměstnanců, kteří je dokáží odhalit, a proto jim nepodlehnou. Velmi často se takové zprávy vyznačují podivnými zdrojovými adresami, gramatickými chybami nebo obsahují přesměrování na adresy, které jsou umístěny v cizině. (ÚNMZ, 2015, s. 21-22)



Obrázek 5 - Příklad spamu na mobilním telefonu

Zdroj: vlastní

Charakter přenosnosti mobilního zařízení z něj dělá snadný cíl pro krádež. Velmi často jsou tyto prostředky používány na veřejných prostranstvích nebo v dopravních prostředcích. Tyto místa jsou charakteristická velkým počtem osob, které se v nich pohybují, což může v případě zapomenutí nebo ztráty dozoru nad zařízením vést k jeho odcizení a následné ztrátě dat nebo jejich zneužití. Z těchto důvodů je vhodné mít veškerý obsah na zařízení šifrovaný a chráněný heslem, vhodné je mít nastavené takové prostředky, které umožnují dálkovou blokaci zařízení a současně je pro případ ztráty vhodné mít nastavený systém zálohování, který nám umožní snadnou migraci do nového zařízení bez ztráty dat. (ÚNMZ, 2015, s. 21-22)

2.2.8 Síťová podpora pro cestující uživatele

V rámci cest je pro zaměstnance užitečné, když může na cestách pracovat. K tomu je často využíván firemní intranet. Jeho využití na cestách přináší efektivní využití pracovního času, ale současně bezpečnostní rizika. (ÚNMZ, 2015, s. 23)

Norma definuje hrozbu v podobě neautorizovaného přístupu, který se týká přístupu k intranetu nebo kompromitaci bezpečnostních bran na cestě k intranetu anebo v podobě přístupu k datům na zařízení, které má uživatel u sebe. Obranou před těmito hrozbami je použití pokročilých technik autentizace pro přihlášení do firemního intranetu. Vhodné je vícefaktorové přihlášení, popřípadě využití certifikátů. Pro ustanovení bezpečné cesty je žádoucí využít technologii VPN.

Klientskou stanici zabezpečit pomocí osobního firewallu a veškerá data uložená na ní šifrovat. Při využití webových služeb využívat protokolů SSL nebo TSL. (ÚNMZ, 2015, s. 23)

Ve scénáři je dále možnost hrozby v podobě omezení dostupnosti sítě, které je způsobené například nekvalitním pokrytím WWAN sítí. Řešením tohoto problému může být buď zapojením více poskytovatelů, kteří poskytují internetové služby nebo zajistit lepšího, který poskytuje kvalitnější služby. Ve smlouvě s poskytovateli je žádoucí stanovit určitou úroveň kvality služeb, aby byla zajištěna dostatečná spolehlivost a výkonost pro práci na cestách. (ÚNMZ, 2015, s. 23)

2.2.9 Služby za jištěné subdodavateli

Pro organizace je v určitých případech výhodné využívat některé služby od subdodavatelů, protože to vede ke snížení nákladů. Tento přístup využívání služeb zavádí některá rizika, která je nutné řešit jak na straně subdodavatele, tak na straně uživatele. Dodavatelé těchto služeb potřebují pro výkon svých činností velmi často přístup k interní infrastruktuře a aktivům, velmi často s nejvyšší úrovní oprávnění. Tento přístup může být dočasný, ale i trvalý. Pak je nutné ošetřit rizika spojená i s tímto přístupem. Podrobněji se problémy se subdodavatelskou strategii zajišťování služeb zabývá norma ISO/IEC 27036. (ÚNMZ, 2015, s. 24)

Mezi nebezpečí, která mohou přijít od dodavatele služby, řadíme zneužití jiné služby, než kterou má dodavatel spravovat. Subdodavatel může využít porty pro vzdálenou správu a přidělená oprávnění. Takovým situacím je možné zabránit silnou autentizací, jednoznačným přidělením uživatelských identifikátorů k dané službě a dodatečně je možné zneužití odhalit kontrolou logů, které se generují po každé události v rámci systému. (ÚNMZ, 2015, s. 24-25)

Další hrozbou je zpřístupnění citlivých údajů, které se dostanou k dodavateli. Většinou je to způsobeno nedostatečnou separací uživatelů, kdy může dodavatel získat přístup k uloženým datům, výměnným mediím nebo odposlouchávat komunikaci v systému. Problémem je i sdílení hesel k částem systémů, které se neřídí pravidly, která by zaručila bezpečnost a přehled, kdo s daným přístupovým údajem nakládá. Řešením je šifrování klientských dat, stanovení jednoznačných pravidel pro nakládání dat, pravidelné kontroly, jestli jsou dané politiky dodržovány a současně je důležité proškolení všech zainteresovaných zaměstnanců, aby byli dobře obeznámeni s těmito pravidly. (ÚNMZ, 2015, s. 24-25)

Problémem u subdodavatele může být i riziko zavedení malware. Riziko je největší v průběhu vývoje softwaru, k čemuž vede nedostatečná bezpečnost v procesech vývoje a zavedení software. K infiltraci může dojít i v průběhu přenosu hotového softwaru nebo při dálkovém

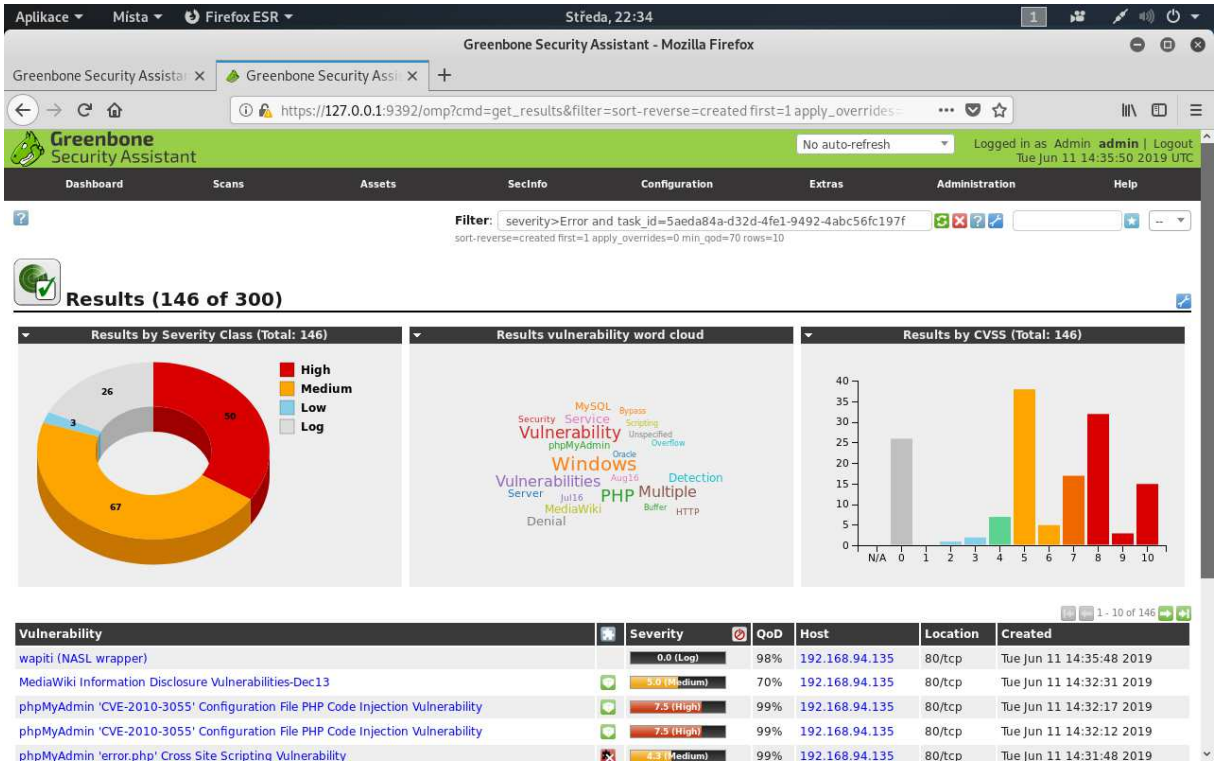
nasazení, v případě, že jsou využité nezabezpečené technologie vzdáleného přístupu. Řešením těchto rizik je nastavení pravidel a postupů, které zajistí bezpečné programovaní a zajistit, aby vývojové stanice byly pravidelně kontrolovány aktualizovaným antivirovým softwarem na veškeré hrozby. (ÚNMZ, 2015, s. 24-25)

Poslední hrozbou je, že dodavatel není plně seznámen s legislativou v dané zemi, protože pochází z jiného státu, než je zákazník. V takovém případě může poskytovat služby, které odporují legislativě a využívat technologie, které jsou zakázané nebo nedostatečné. Důležité je proto, aby byl subdodavatel informován o místních předpisech a svoji službu podle nich patřičně upravil. (ÚNMZ, 2015, s. 24-25)

3 SKENOVACÍ NÁSROJE

3.1 OpenVAS

OpenVAS je pokročilý skener zranitelností systému. Tento skener umožnuje skenovat širokou škálu jak nízko úrovňových, tak vysokoúrovňových protokolů. Obsahuje moduly pro skenování průmyslových protokolů a také algoritmy, které umožnují na základě předchozích znalostí urychlit proces skenování systému. (Greenbone Networks, 2018)



Obrázek 6 - Ukázka webového rozhraní OpenVAS

Zdroj: vlastní

Historie tohoto nástroje se začala psát v roce 2005, kdy došlo k rozhodnutí, že nástroj Nessus, který byl do této doby šířen pod licencí Open Source, přejde na nový obchodní model. Tento model zahrnoval uzavření zdrojových kódu, a proto se v reakci na tuto situaci vynořilo několik následovníků, kteří započali vyvíjet pokračovatele nástroje Nessus s otevřeným zdrojovým kódem. Do dnešní doby je z těchto následovníků aktivně vyvíjen jen OpenVAS. Jeho vývoj zastřešuje německá společnost Greenbone Network. OpenVAS je v současnosti velmi populární, využívá ho například společnost AIRBUS, konkrétně její část, která se zabývá vývojem obranných vojenských systémů a průzkumem vesmíru. Vývoj také podporuje německý Spolkový úřad pro bezpečnost informační techniky, jehož hlavním úkolem je zajistit

bezpečnost informačních systémů německé vlády a jejích úřadů. (Greenbone Networks, 2018, Pritchett, 2013, Selecký, 2012)

Nástroj OpenVAS obsahuje v současné době přes 50 000 testů zranitelností. Tyto testy je možné dále rozšiřovat pomocí jazyka NASL, který slouží pro specifikaci zranitelnosti, kterou pak OpenVAS využije v rámci svých skenů. (Greenbone Networks, 2018)

OpenVAS je nyní dostupný ve verzi 9, která je k dispozici v podobě zdrojových kódů[1] nebo jako balíček v repositářích distribuce Kali Linux. (Greenbone Networks, 2018)

3.2 Nessus Essentials

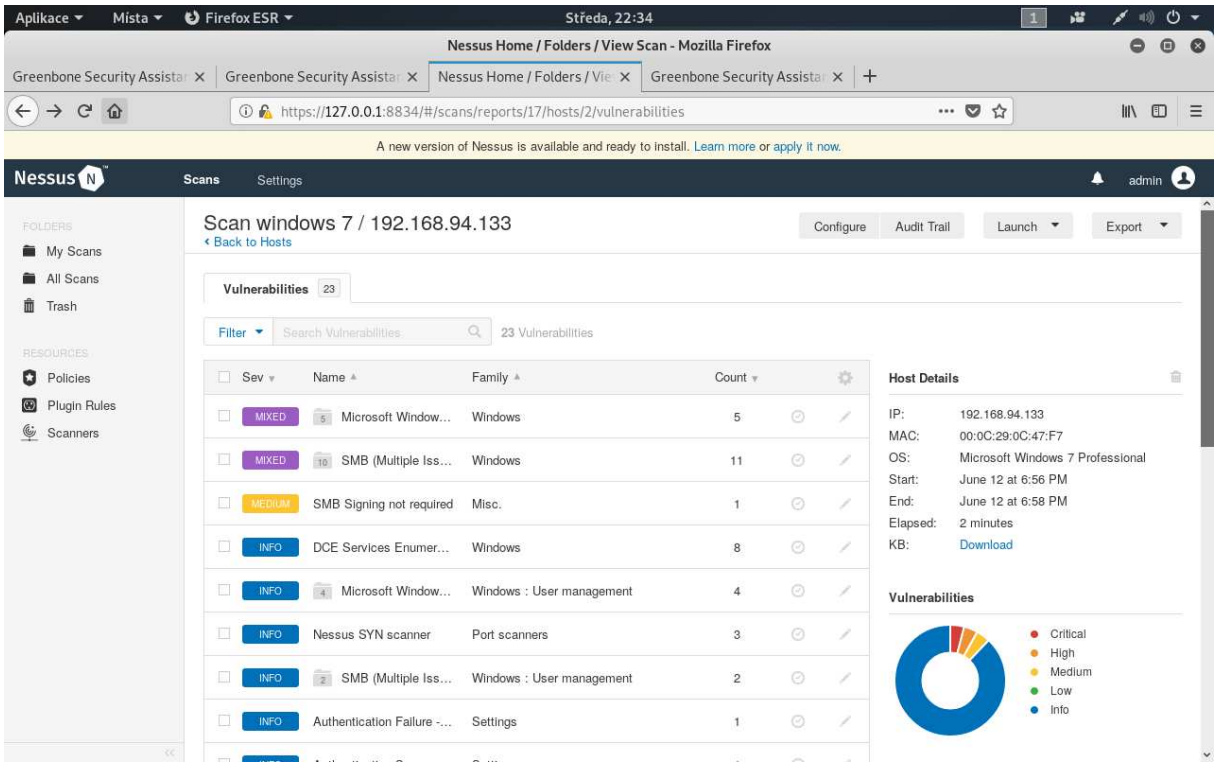
Nástroj Nessus je proprietární skener zranitelností, který vznikl v roce 1998. Za jeho vývojem stojí Renaud Deraiso, který v roce 2002 spoluzaložil firmu Tenable, která tento nástroj dále vyvíjí. V roce 2005 uzavřela společnost Tenable zdrojové kódy a dále vyvíjí Nessus ve dvou verzích. Placená verze bez omezení a volně dostupná s omezeními, která se týkají hlavně počtu cílů, které je možné v rámci jednoho skenu otestovat. Na původním jádře Nessus 2, které mělo do roku 2005 otevřené zdrojové kódy, byl později vystavěn nástroj OpenVAS. (Tenable, 2019)

Nessus pokrývá širokou řadu technologií, která zahrnuje operační systémy, sítová zařízení, databáze, webové servery a nejpoužívanější webové aplikace anebo například systémy SCADA, které umožnují monitoring a řízení průmyslových procesů. Takovéto systémy se často používají v elektrárnách, chemických rafineriích nebo dopravních prostředcích, například zaoceánské lodě. (Tenable, 2019, Microsys, 2017)

Zranitelnosti jsou popisované, stejně jako u nástroje OpenVAS, pomocí jazyka NASL, který specifikuje podrobnosti o zranitelnosti a seskupuje algoritmy, které slouží k otestování, zda testovaný systém danou zranitelností trpí. (Tenable, 2019)

Nástroj je nyní dostupný ve verzi 8.4, kterou je možné stáhnout na stránkách výrobce[2]. Je dostupný pro Linux, Windows a MacOS. (Tenable, 2019)

[1] https://github.com/greenbone/openvas
[2] https://www.tenable.com/downloads/nessus



Obrázek 7 - Výsledky prezentované ve webovém prostředí Nessus Essentials

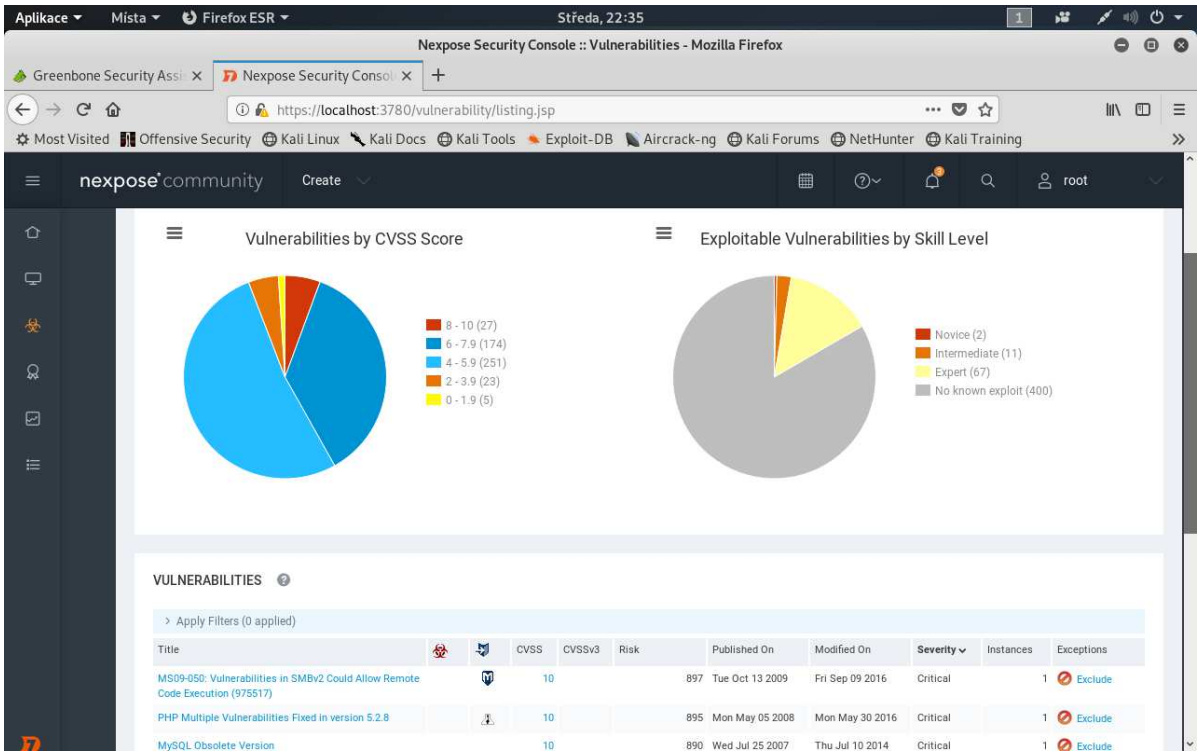
Zdroj: vlastní

3.3 Nexpose Community Edition

Skener zranitelností Nexpose vyvíjí společnost Rapid7, která v současné době produkuje celou řadu nástrojů., které se zabývají správou zranitelností, testováním aplikací a správou logovacích informací. Vedle nástroje Nexpose vyvíjí podobný nástroj pro skenování zranitelností, který se jmenuje InsightVM, který se liší od nástroje Nexpose hlavně zapojením cloudových technologií a přítomností vlastního agenta, který je na cílových zařízeních nainstalován, aby poskytl více informací než tradiční způsoby skenování založené na službách, které poskytují operační systémy. (Rapid7, 2019)

Nástroj v současnosti integruje i Metasploit, který společnost Rapid7 získala v roce 2009 a nyní ho dále vyvíjí. Metasploit je projekt, který poskytuje infrastrukturu, informace a nástroje pro penetrační testování. V současné době má otevřené zdrojové kódy a využívá ho i několik dalších komerčních nástrojů. (Rapid7, 2019)

Tvůrci nástroje uvádí, že v současné verzi je schopen detekovat přes 75 000 zranitelností a kontroluje další 185 000 potencionálně nebezpečných nastavení jak na cílových zařízeních, tak na sítových prvcích. Všechny nalezené problémy seřadí podle míry rizika. (Rapid7, 2019)



Obrázek 8 - Výsledek skenu prezentovaný v Nexpose Community Edition

Zdroj: vlastní

Nexpose existuje ve dvou variantách, bezplatná edice Nexpose Community Edition s omezeními a komerční verze bez omezení. Nástroj je nyní v bezplatné podobě dostupný ve verzi 6.5.68, která je ke stažení na stránkách firmy Rapid7[3]. Dostupné jsou verze pro operační systémy Windows i Linux. (Rapid7, 2019)

3.4 Nmap

Nmap je nástroj, který vytvořil Gordon Lyon jako volně dostupný skener sítí. Tento nástroj dokáže detekovat zařízení, které se nachází na síti, odhalit otevřené porty, u kterých je schopný identifikovat služby, které na těchto portech běží, včetně jejich verzí. Dále dokáže detekovat operační systémy, a i skenovat cílový systém na možné zranitelnosti. (Gordon Lyon, 2018)

To je možné díky přítomnosti NSE, které umožnuje uživatelům psát a sdílet jednoduché skripty, které automatizují práci s Nmapem. Jedním takovým skriptem je *vuln*, který spojuje několik dalších skriptů, které pomocí Nmapu dokáží odhalit základní zranitelnosti v cílových systémech. Je možné detekovat zranitelnosti protokolů SMB, HTTP, FTP, SSL a jiných. Tyto skripty jsou součástí instalace Nmapu. Kromě těchto skriptů existuje několik projektů třetích

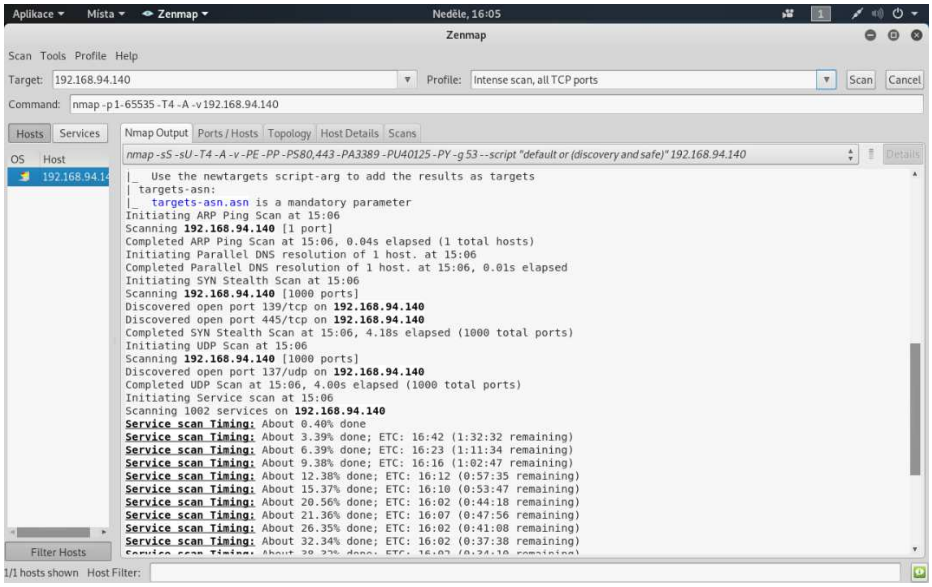
[3] https://nexpose.help.rapid7.com/docs/download

stran, které se zabývají skenováním zranitelnosti, například projekt *vulscan*[4]. Tento skript umožnuje Nmapu procházet nejznámější databáze zranitelností a ty pak pomocí dat získaných z Nmapu vyhodnocovat. Funkčnost Nmapu je možné dále rozšířit pomocí grafických nástaveb, kterých je k dispozici několik. (Gordon Lyon, 2018, Selecký, 2012)

Nmap je v současnosti dostupný ve verzi 7.70, má otevřené zdrojové kódy[5] a je také součástí linuxové distribuce Kali Linux.

3.4.1 Grafické nástavby

Existuje několik grafických nástaveb, které se různými způsoby snaží zpřehlednit a graficky reprezentovat výsledky získané z provedených skenů Nmapu. Bohužel většina těchto nástaveb se věnuje nastavení samotných skenů nebo reprezentaci výsledků, kde většinou zobrazí standardní výstup z Nmapu a na základě získaných informací vykreslí diagram sítě, ale žádný z nich nedokáže zatím dále zpracovat výsledky skriptů, které vyhledávají zranitelnosti. Jedinou přidanou hodnotou je tedy možnost konfigurace v okně a případně export výstupu do formátu typu XML nebo HTML.



Obrázek 9 - Výstup Nmapu v Zenmapu

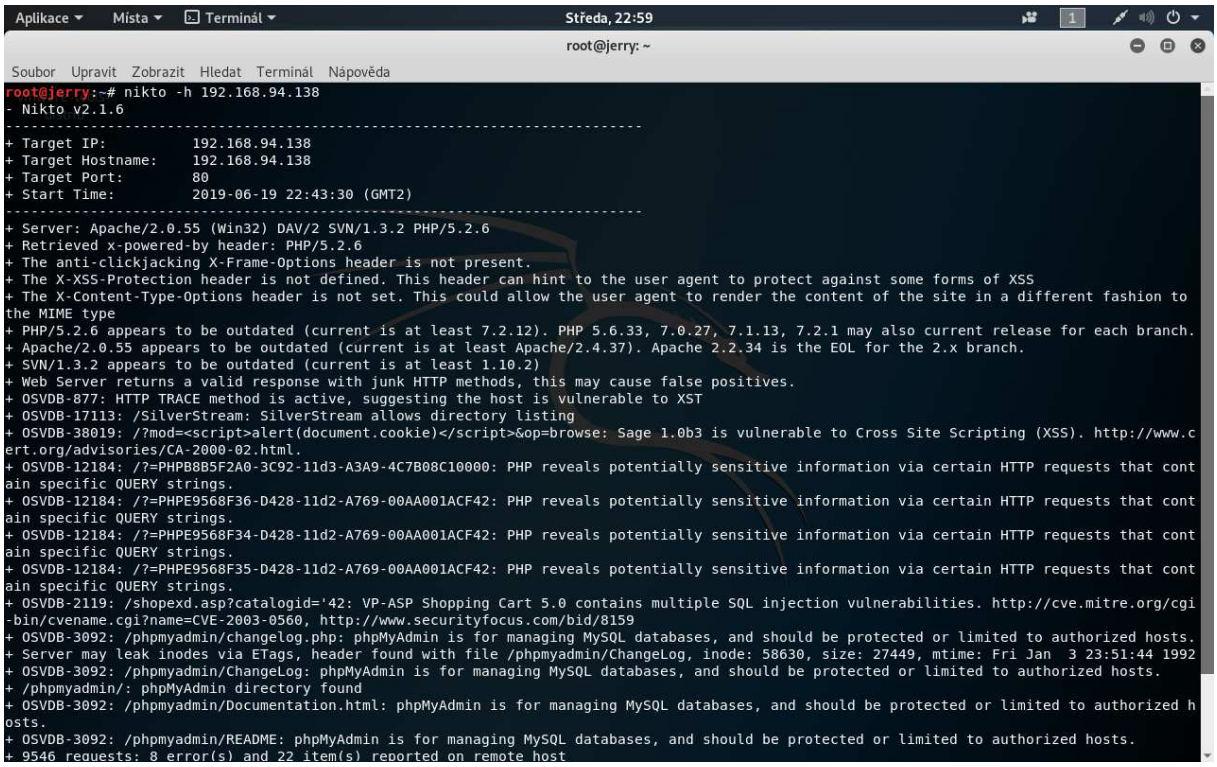
Zdroj: vlastní

3.5 Nikto2

Tato sada skriptů je úzce specializovaná na zranitelnosti týkající se webových serverů. Mezi její přednosti patří rychlost a jednoduchost. Skripty psané v jazyce Perl dokáží odhalit zastaralé

[4] https://github.com/scipag/vulscan
[5] https://svn.nmap.org/nmap

a nezabezpečené webové servery, detekovat nezabezpečená nastavení na webových serverech a potencionálně nezabezpečené služby, mezi které patří například otevřený přístup do administračních webových nástrojů a aplikací (například phpMyAdmin). (Chris Sullo, 2019, Selecký, 2012)



Obrázek 10 - Dokončený sken v nástroji Nikto2

Zdroj: vlastní

Nástroj Nikto2 má otevřený zdrojový kód[6] a je k dispozici v distribuci Kali Linux ve verzi 2.1.6. Současně je často využíván některými sofistikovanějšími nástroji, například nástrojem OpenVAS. (Chris Sullo, 2019)

3.6 Retina Network Security Scanner Comunity

Retina Network Security Scanner Comunity je nástroj pro hledání zranitelností od společnosti BeyondTrust, která ho v současné době vyvíjí. Je dostupný jako bezplatná verze s časovým omezením nebo plná placená verze bez omezení. (BeyondTrust, 2019)

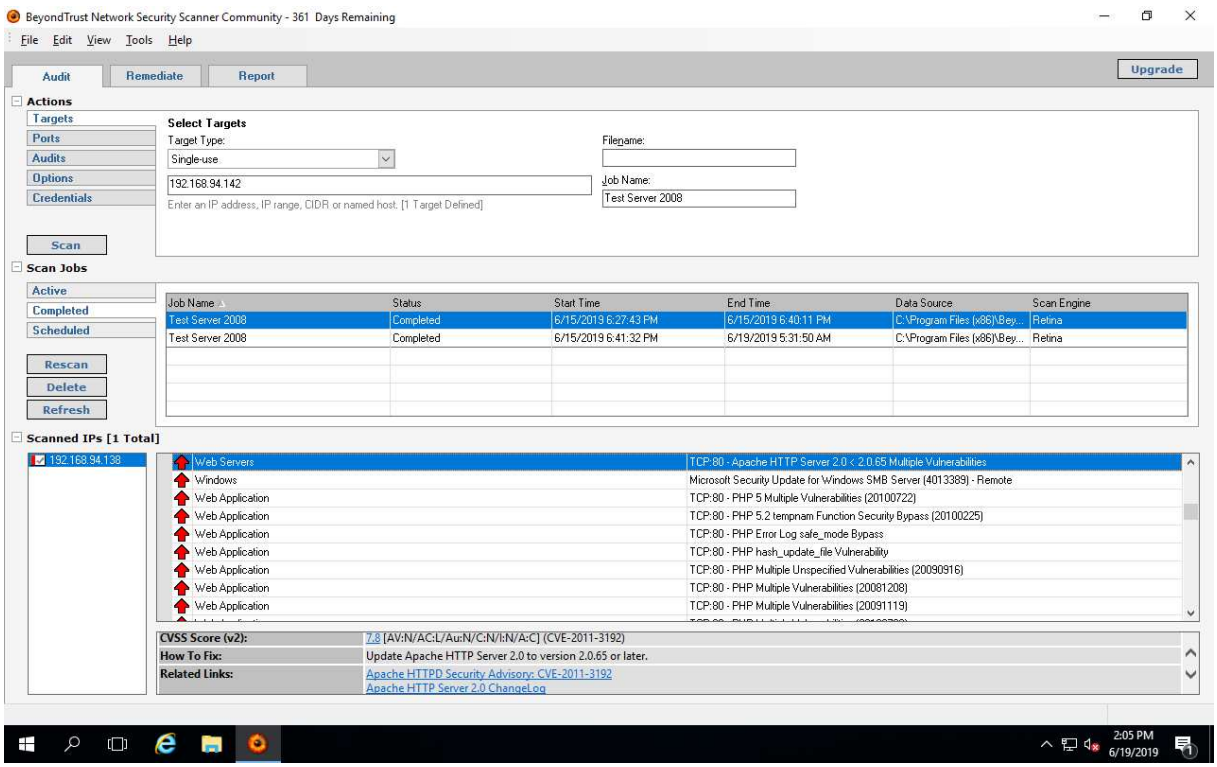
Tvůrce nástroje se chlubí nízkou mírou falešných hlášení. Podle webových stránek zvládá skenovat běžné služby systému Windows, zranitelné webové aplikace, databázové systémy, a dokonce i virtuální prostředí založená na řešení od společnosti VMware. Nástroj dále zvládá

[6] https://github.com/sullo/nikto

odhalovat zranitelnosti na zařízeních od společností Cisco a také jiných zařízení, jejichž operační systém je postaven na bázi Linuxu, kde komunikuje se zařízením pomocí SSH. (BeyondTrust, 2019)

Tento nástroj je dostupný ve verzi 6.6.1, která je volně dostupná ke stažení na stránkách výrobce[7]. Nejedná se o multiplatformní nástroj, je dostupný pouze pro zařízení se systémem Windows. (BeyondTrust, 2019)

V době psaní práce došlo k přejmenování z Retina Network Security Scanner Comunity na BeyondTrust Network Security Scanner Community. Přejmenování je velmi čerstvá záležitost, proto se stále v dokumentaci i jako název staženého instalátoru vyskytuje původní název. (BeyondTrust, 2019)



Obrázek 11 - Dokončený sken v BeyondTrust Network Security Scanner Community

Zdroj: vlastní

3.7 ManageEngine Vulnerability Manager Plus

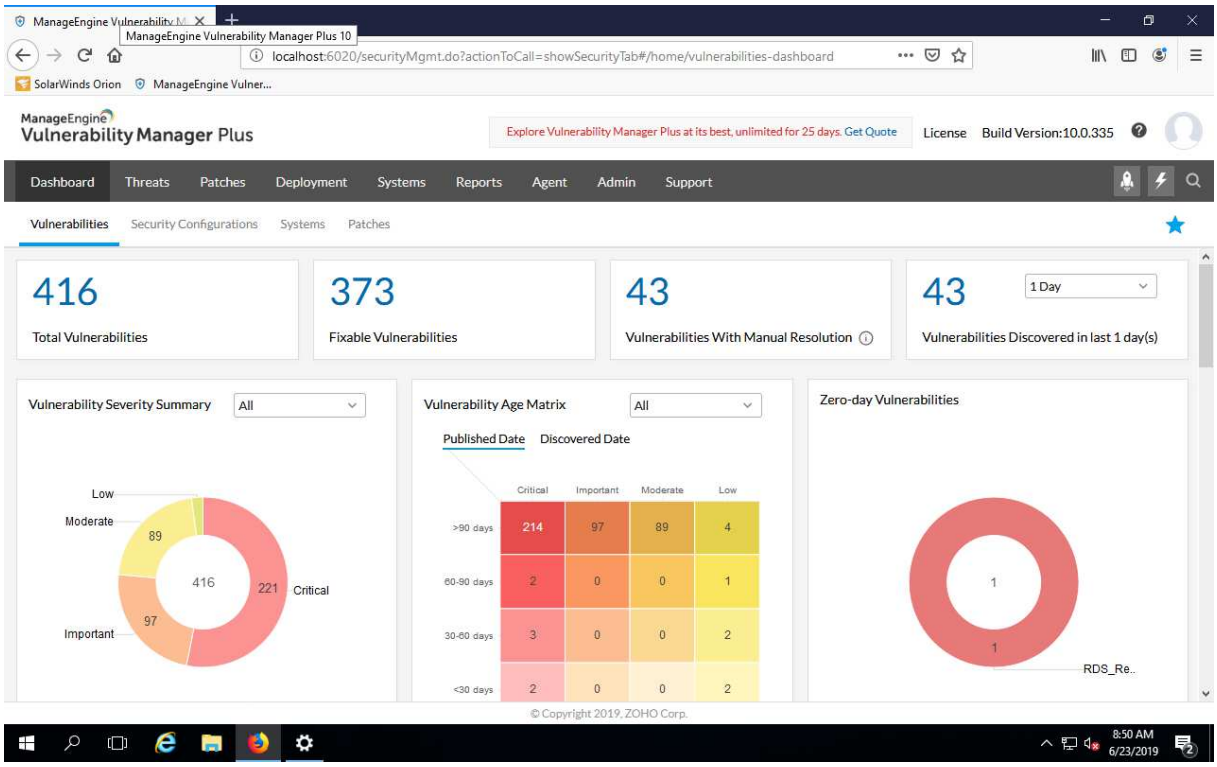
Společnost ManageEngine vyvíjí nástroj ManageEngine Vulnerability Manager Plus, který se zabývá vyhledáváním a správou zranitelností, které dokáže odhalit. Tento software dokáže odhalit zranitelnosti, které se týkají chybějících záplat v nainstalovaném software na zařízení,

[7] https://www.beyondtrust.com/tools/vulnerability-scanner

nezabezpečená nastavení operačních systémů, chyby na webových serverech či přímo ve webových aplikacích nebo vyhledávat nebezpečný software, například pro P2P, které může být použito k páchání nelegální činnosti. (ManageEngine, 2019)

Vulnerability Manager Plus používá pro zjištění zranitelností vlastního agenta, který je nainstalován na hlídaném zařízení. Tento agent díky přímé přítomnosti na zařízení může zařízení dále monitorovat a případně na dálku zajistit řešení, které zranitelnost eliminuje. (ManageEngine, 2019)

Nástroj je dostupný jako časově omezená testovací verze bez funkčních omezení na stránkách výrobce[8], nyní ve verzi 10.0.335. (ManageEngine, 2019)



Obrázek 12 - Ukázka prostředí z ManageEngine Vulnerability Manager Plus

Zdroj: vlastní

[8] https://www.manageengine.com/vulnerability-management/download.html

4 POUŽITÉ VYBAVENÍ

4.1 Softwarové vybavení

Z důvodů, že některé ze skenovacích nástrojů nejsou dostupné pro více platforem, bylo přistoupeno při tvorbě práce k použití jak operačního systému založeného na Linuxu, tak operačního systému založeného na platformě Windows.

4.1.1 Kali Linux

V rámci platformy Linux byla zvolena distribuce Kali Linux, která je primárně zaměřena na penetrační testování. Hlavní předností této distribuce jsou obsáhle softwarové repositáře, které obsahují velké množství nástrojů, včetně některých, které jsou použity v rámci této práce. Jejich instalace je tak snadná a bezproblémová.

Distribuce Kali Linux vznikla v roce 2013 jako kompletní přepracování svého předchůdce, který se jmenoval BackTrack. Je založena na Debianu a v současnosti obsahuje více než 600 nástrojů pro penetrační testování. Oproti jiným distribucím nabízí například možnost sebedestrukce, kdy při jejím vyvolání dojde k znepřístupnění všech dat na disku, která tak budou ochráněna před nežádoucím přístupem. (Offensive Security, 2019)

Obrázek 13 - Ukázka Kali Linux 2019.1 s GNOME

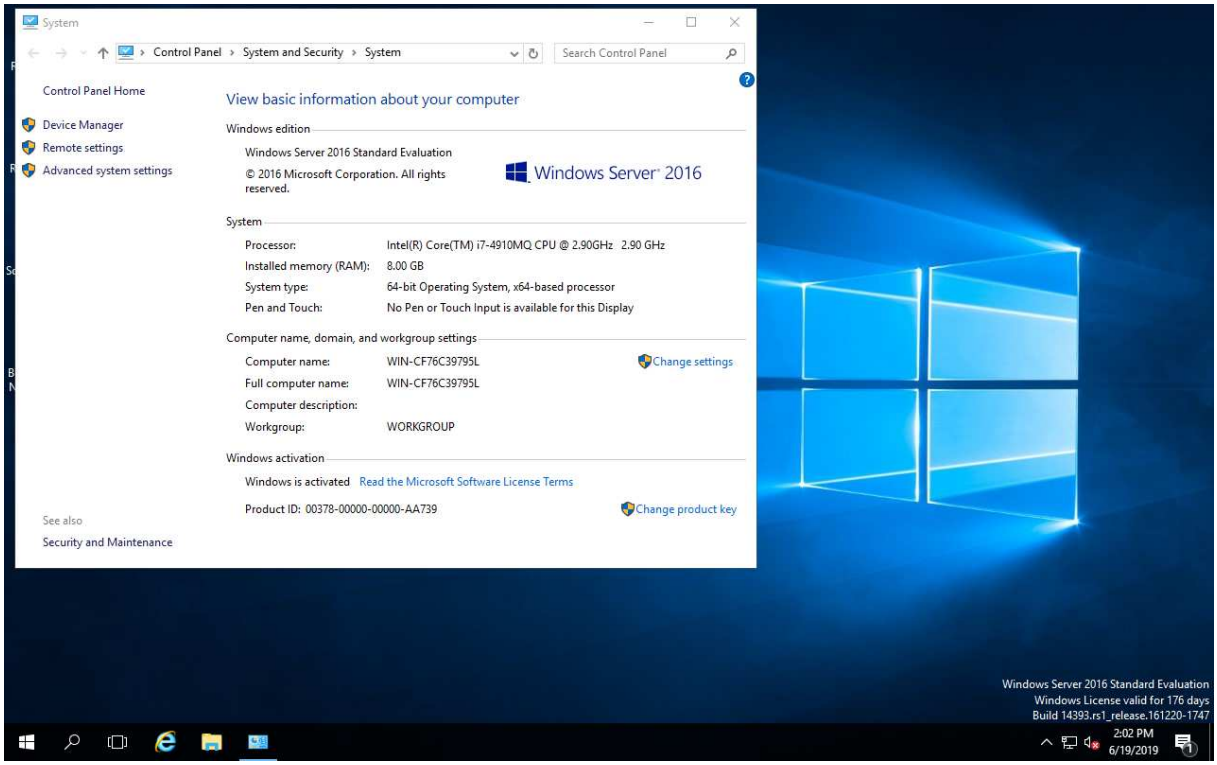
Zdroj: vlastní

Systémové požadavky pro instalaci této distribuce nejsou v dnešní době nijak velké. Pro instalaci je nutné disponovat alespoň 20 GB místa na disku. Dále je potřeba minimálně 1 GB

paměti RAM a podpora CD/DVD mechaniky nebo USB disků. Distribuce je volně ke stažení na webových stránkách[9] jak pro platformu i386, amd64 nebo ARM. Je zde také možnost stažení a instalace z Microsoft Store, kde je distribuce pak integrována v rámci Windows Subsystem for Linux v rámci operačního systému Windows 10. V současnosti je dostupná verze 2019.2 z 21. května 2019. (Offensive Security, 2019)

4.1.2 Windows Server 2016

Tento operační systém je primárně zaměřen pro serverové využití. Jedná se o komerční řešení společnosti Microsoft, které vyšlo 26. září 2016 jako nástupce Windows Server 2012 R2. V současné době má již svého následníka v podobě Windows Server 2019. (Microsoft, 2019)



Obrázek 14 - Ukázka prostředí Windows Server 2016 Standard

Zdroj: vlastní

Windows Server 2016 je dostupný v několika edicích, konkrétně jsou to:

- edice Essential,
- edice Standard,
- edice Datacenter.

[9] https://www.kali.org/downloads/

Edice se mezi sebou liší cenou, dodatečnou softwarovou výbavou a také omezeními, která jsou hlavně zaměřená na infrastrukturu, kde tento operační systém běží. Omezujícími podmínkami je například počet procesorů, velikost paměti RAM anebo omezení na počet virtuálních strojů, která může systém provozovat. Minimální požadavky na instalaci jsou obdobné jako ve výše uvedené části. Je nutné disponovat procesorem o minimálním taktu 1.4 GHz, 512 MB RAM v případě instalace bez grafického prostředí (s GUI je minimální hodnota 2 GB) a 32 GB volného místa na disku. Windows Server 2016 jsou dostupné pouze v 64bitové variantě. (Microsoft, 2019)

Pro psaní práce byla použita edice Standard, kterou je možné stáhnout v podobě ISO obrazu na stránkách Microsoftu[10]. Jedná se o verzi pro zkušební použití, která je plně funkční po dobu 180 dní. (Microsoft, 2019)

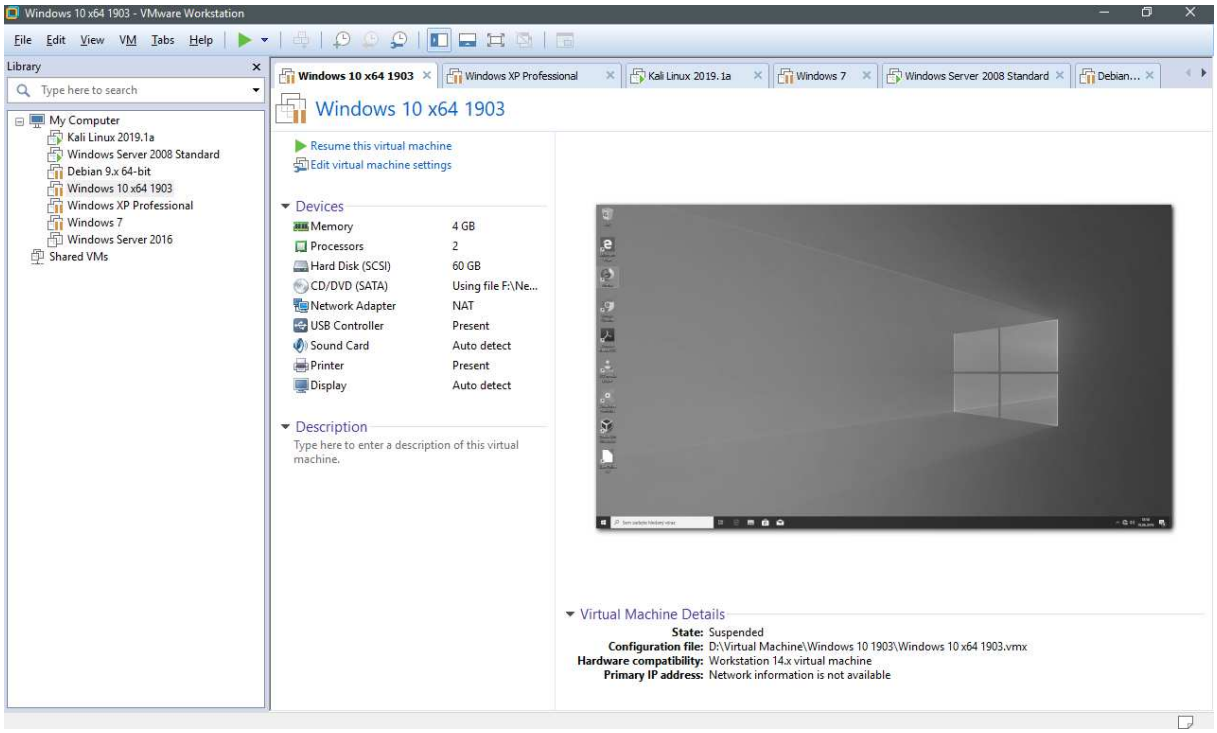
4.1.3 VMware Workstation

VMware Workstation je virtualizační nástroj, který slouží ke spuštění několika virtuálních počítačů, které jsou založené na různých operačních systémech (nejčastěji Windows nebo Linux) v rámci jednoho fyzického zařízení. Je vyvíjen firmou VMware, která je v současné době součástí společnosti Dell. (VMware, 2019)

Tento nástroj je dostupný ve dvou verzích. Bezplatná verze VMware Workstation Player sloužící pro jednodušší virtualizace, protože je v ní neaktivní větší část nastavení, které se týkají virtuálních sítí, virtuálních úložišť nebo automatizace instalace jednotlivých virtuálních systémů. Z těchto důvodů byla pro psaní práce využita placená verze VMware Workstation Pro, která je dostupná i jako 30denní zkušební verze bez dalších omezení.[11] V současné době je aktuální verze 15.1 z jara roku 2019. (VMware, 2019)

Minimální systémové požadavky na samotný program nejsou velké. Je nutné vlastnit 64bitový procesor z roku 2011 a novější s minimální taktovací frekvencí 1.3GHz. Dále je potřeba minimálně 2 GB RAM, ideálně je však potřeba více, protože je nutné zohlednit běžící virtuální počítače a aplikace v nich nainstalované. Samotná instalace programu zabere přibližně 1.2 GB místa na disku, ale opět je nutné myslet na instalované virtuální počítače. Důležitý je také fakt, že nejsou podporované některé řady procesorů Intel Atom a procesory AMD založené na architektuře Llano a Bobcat. (VMware, 2019)

[10] https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016
[11] https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html



Obrázek 15 - Ukázka prostředí VMware Workstation

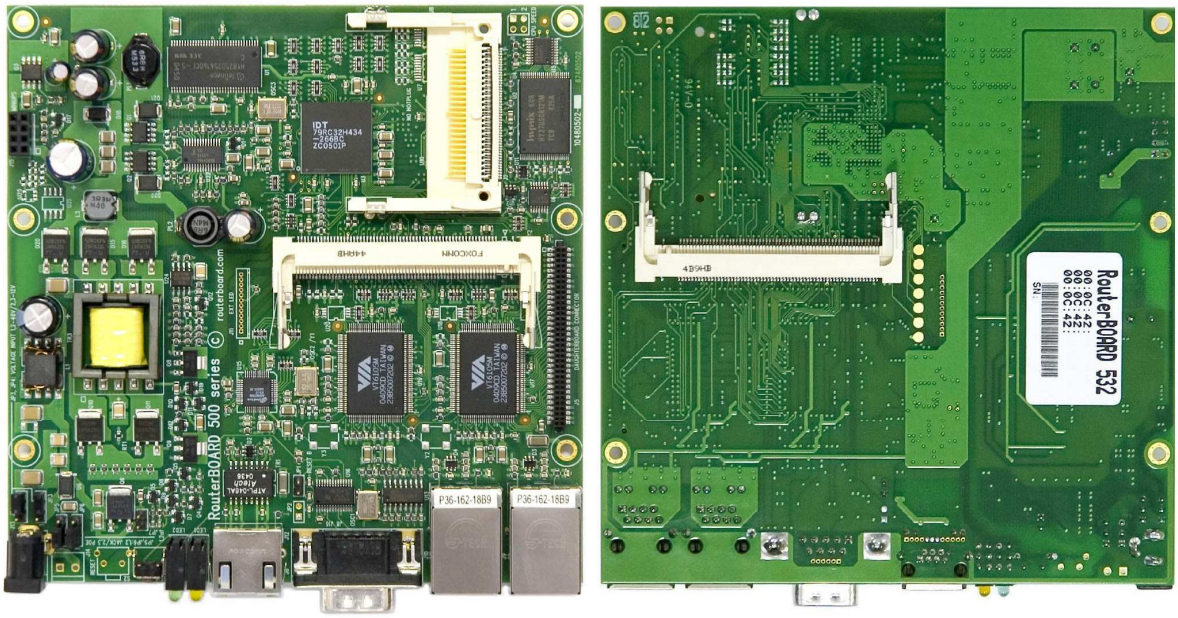
Zdroj: vlastní

4.2 Hardwarové vybavení

Pro potřeby skenů na tzv. vnějším perimetru sítě bylo vybráno zařízení MikroTik RouterBoard 532, které představuje výchozí bránu z lokální sítě. Toto zařízení disponuje procesorem MIPS32 4kc, který je taktován na 266MHz. Dále je vybaveno 32 MB DDR pamětí a 128 MB NAND pamětí pro uchování operačního systému a nastavení. Tuto paměť je možné dále rozšířit pomocí integrovaného slotu na CF kartu. MikroTik dále disponuje třemi porty Fast Ethernet a je možné ho rozšířit pomocí dvou MiniPCI slotů, které u konkrétního testovaného kusu obsahovaly Wi-Fi moduly, které nebyly pro potřeby této práce využity. (MikroTik, 2006)

Na zařízení byl nainstalován operační systém RouterOS ve verzi 6.31. Zařízení je možné konfigurovat buď po sériové lince (rozhraní RS-232) a následně pomocí volně dostupného programu PuTTY[12], po síti za pomocí programu přímo od výrobce Winbox[13] nebo je možnost využít SSH. (MikroTik, 2006)

[12] https://www.chiark.greenend.org.uk/~sgtatham/putty/
[13] https://mikrotik.com/download



Obrázek 16 - Pohled na MikroTik RouterBOARD 532

Zdroj: zpracováno dle (MikroTik, 2006)

Veškeré virtuální počítače, ať už testované nebo virtuální počítače, které zabezpečovaly chod testovaných nástrojů, byly provozovány na notebooku Dell Precision m4800. Tento notebook je osazen procesorem Intel Core i7 4910QM, který disponuje 4 jádry, které tikají na základní frekvenci 2.9 GHz, kterou je možné dočasně zvýšit až na 3.9 GHz a technologií HyperThreading. Dále obsahuje 32 GB RAM paměti a dva SSD disky o kapacitě 256 GB. Tyto parametry stačily pro bezproblémový a svižný chod všech cílových virtuálních počítačů v jeden okamžik. (Intel, 2014)

5 POROVNÁNÍ NÁSTROJŮ

5.1 Porovnání dle ceny neomezených licencí

Cenová politika se v rámci vybraných nástrojů velmi liší. Některé jsou zcela bezplatné, jiné si účtují konečnou cenu podle počtu hlídaných zařízení nebo se platí za každý rok či jinou kombinaci těchto podmínek.

Tabulka 2 – Porovnání ceny plných licencí

Název skeneru	Cena [Kč][14]
OpenVAS	0
Nessus Professional	48 965/rok
insightVM (Nexpose)	495 za zařízení/rok
Nmap (*vuln* script)	0
Nmap (*vulscan* script)	0
Nikto2	0
Retina Network SS	41 795/rok
ManageEngine VMP Enterprise	26 710 za 100 zařízení

Zdroj: zpracováno dle webových stránek tvůrců

První kapitolou jsou bezplatné nástroje, které povětšinou vyvíjí komunita uživatelů. Tam spadají zástupci konzolových aplikací založených na Nmapu a skener Nikto2. Bezplatný je také robustnější nástroj OpenVAS, který je sice vyvíjen společností Greenbone Networks, ale ta těží finanční prostředky z jiných projektů.

Další kategorie nástrojů je omezena pouze časově. Do ní patří nástroje Nessus a Retina, kde se platí za celoroční licenci, která se v závislosti na nástroji pohybuje mezi 40 až 50 tisíci korun českých. Výhodou takové cenové politiky je fakt, že v případě velmi rozsáhlé sítě, platí koncový uživatel aplikace pouze za ní, bez závislosti na počtu hlídaných zařízení, a proto je taková licence výhodná pro větší firmy, které dále rostou.

Platbu za počet zařízení využívá například ManageEngine, u kterého je minimem počtu zařízení, pro které je možné skener objednat stanoven na 100 kusů. Tato cena je bez dalších omezení, a proto se jedná o vhodnější software pro malé firmy, protože je v takovém případě ze všech nejlevnější.

[14] K přepočtu cen byl použit kurz z 29. 6. 2019, kde 1 USD = 22.35Kč.

Nejpřísnější cenovou politiku má nástroj insightVM, který je plnou verzí nástroje Nexpose. U něho se platí nejenom za počet zařízení, která jsou hlídána, tak i za období, po kterou jsou hlídána. Nejmenší jednotka, která může být fakturována, je jeden rok, přičemž tato cena platí pro 512 zařízení. Pro méně zařízení je cena vyšší, ale i tak se může jednat o výhodné řešení v rámci malých firem, kde může být po bezplatných řešeních nejlevnější.

5.2 Porovnání omezení bezplatných verzí

Každý testovaný nástroj nabízí na vyzkoušení různě omezenou verzi. Tyto verze je možné bezplatně stáhnout, většinou výměnou za několik osobních údajů jako například jméno a příjmení, emailová adresa a účel, za kterým si nástroj stahujeme.

Tabulka 3 – Porovnání omezení bezplatných verzí

Název skeneru	Omezení
OpenVAS	bez omezení
Nessus Essentials	16 IP adres na sken
Nexpose Community	30 dní používání
Nmap (*vuln* script)	bez omezení
Nmap (*vulscan* script)	bez omezení
Nikto2	bez omezení
Retina Network SS	1 rok používání, bez modulu databáze a webových aplikací
ManageEngine VMP	30 dní používání

Zdroj: zpracováno dle webových stránek tvůrců

Nástroje můžeme opět rozdělit do několika kategorií. První kategorií jsou nástroje bezplatné, které tím pádem nenabízí žádné zkušební verze a jsou v tabulce uvedené jen pro pořádek, protože si je v podstatě můžeme vyzkoušet bez omezení. Do této kategorie spadá například OpenVAS, Nmap nebo Nikto2.

Další kategorií tvoří nástroje, které je možné vyzkoušet bez funkčních omezení po krátkou dobu, typicky 30 dní. Tuto kategorii tvoří například Nexpose nebo ManageEngine. Jiný typ omezení zvolil nástroj Nessus, který je možné bez funkčních omezení používat až pro testování 16 zařízení.

Nejvíce omezenou zkušební verzi tohoto výběru má nástroj Retina, který je omezen na rok používání, ale také jako jediný neposkytuje možnost vyzkoušet si plnou verzi aplikace.

Zkušební verze má deaktivované skenery pro databáze a webové aplikace, takže potencionální zákazníci si nemohou důkladně otestovat možnosti detekce před nákupem skeneru.

5.3 Porovnání dle platforem

Jednotlivé nástroje se liší především v podpoře jednotlivých platforem. Některé nástroje jsou striktně omezeny jen na jednu. U platformy Windows je zkoumaná podpora Windows 7 a novější, protože starší verze operačních systémů většina nástrojů už stejně nepodporuje.

Tabulka 4 – Porovnání dle platforem, kam je možné skenery instalovat

Platforma / Skener	Windows	Linux	Mac OS
OpenVAS	☐	☒	☐
Nessus Essentials	☒	☒	☒
Nexpose Community	☒	☒	☐
Nmap	☒	☒	☒
Nikto2	☒	☒	☒
Retina Network SS	☒	☐	☐
ManageEngine VMP	☒	☐	☐

Zdroj: zpracováno dle webových stránek tvůrců

Výsledky nejsou překvapivé, většina nástrojů podporuje Windows, až na OpenVAS, který sice v minulosti pro Windows vyšel, ale v současné době není pro Windows aktivně vydáván. Tento stav se může v budoucnu změnit.

Nástroje Retina a ManageEngine podporují pouze Windows. U ManageEngine je situace s podporou složitější, protože je ještě nutné poznamenat, že agent, který se používá na testované počítače má podporu daleko širší než samotné jádro skeneru. Agent podporuje podle dokumentace Windows od verze XP a novější, podporován je také Linux od jádra 2.6.33 a novější, a dokonce je podporován i Mac OS od verze 10.7. Podpora Mac OS je jinak vcelku špatná, chlubí se jí oficiálně jen tvůrci Nessusu, Nikto2 a Nmapu.

5.4 Podpora prohlížečů

Celkem čtyři vybrané nástroje disponují uživatelským rozhraním, které je dostupné pomocí webového prohlížeče. Podpora prohlížečů je napříč nástroji různá.

Tabulka 5 - Porovnání dle podpory webových prohlížečů

Prohlížeč / Skener	Microsoft Edge	Google Chrome	Mozilla Firefox	Safari
OpenVAS	neuvedeno			
Nessus Essentials	☒	☒	☒	☒
Nexpose Community	☒	☒	☒	☐
ManageEngine VMP	☒	☒	☒	☐

Zdroj: zpracováno dle webových stránek tvůrců

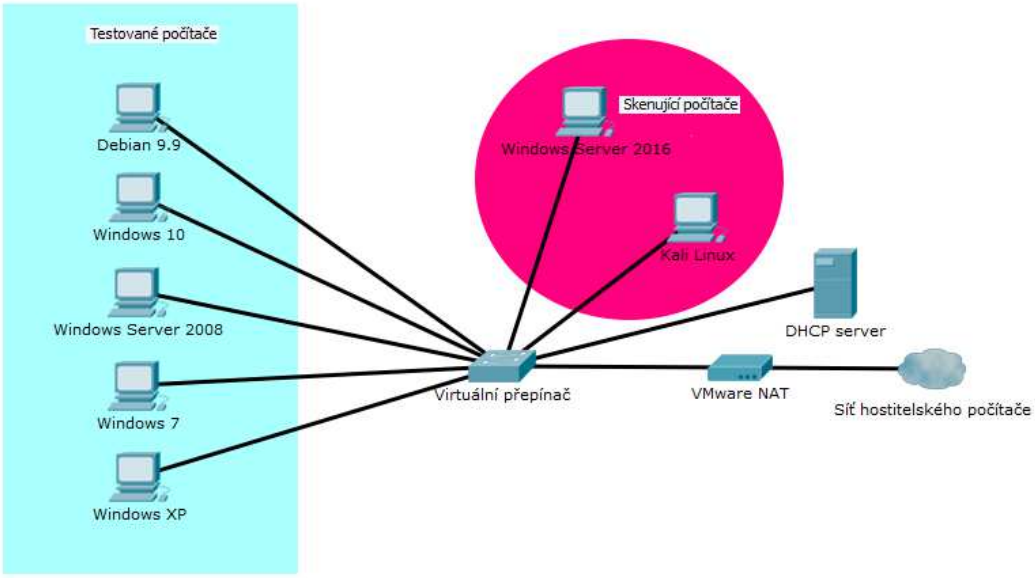
Nástroje vesměs mají dobrou podporu nejpoužívanějších prohlížečů, jediný rozdíl je u webového prohlížeče Safari, který nástroje nepodporující Mac OS rovněž nepodporují. Málokdo si na Windows nebo Linux tento prohlížeč nainstaluje, takže je tento fakt zanedbatelný. U nástroje OpenVAS tvůrci podporu neuvádějí.

6 PRAKTICKÁ ČÁST

Tato část práce představuje konkrétní nasazení nástrojů pro skenování zranitelností. V prvních podkapitolách byla ověřována kvalita detekce na smyšlené podnikové síti, kde byly účelně vytvořené zranitelnosti. Pomocí nástrojů byl nejprve prověřen perimetr lokální sítě, na kterém se testovala sada předpřipravených virtuálních počítačů. Následně jejich účinnost byla poměřena na vnějším perimetru, kde bylo jejich úkolem prověřit zranitelnosti na fyzickém zařízení MikroTik. Následující kapitoly se zabývají porovnáním možností automatizace skenování, které jsou u těchto nástrojů rozdílné, v další části byly posouzeny možnosti řešení nalezených zranitelností, které testované skenovací nástroje nabízí.

6.1 Vnitřní perimetr sítě

Vnitřní perimetr sítě zde zastupuje kompletně virtualizovaná síť postavená na technologiích společnosti VMware. Tvoří ji celkem 5 virtuálních počítačů, které byly podrobeny skenování na možný výskyt zranitelností. V síti se dále nacházely dva virtuální počítače, na kterých byly nainstalovány skenovací nástroje a virtuální prostředky, které se staraly o chod sítě. Mezi tyto prostředky patří virtuální přepínač, DHCP server, který virtuálním počítačům přiděluje adresy z rozsahu 192.168.94.0/24. O překlad adres mezi virtuální sítí a hostitelským počítačem se stará NAT.



Obrázek 17 - Schéma virtuální lokální sítě, zpracováno pomocí Cisco Packet Tracer

Zdroj: vlastní

Virtuální počítače obsahovaly operační systémy Windows od verze XP po nejnovější verzi Windows 10 a také jeden exemplář s linuxovým operačním systémem Debian. Tyto stroje měly

předinstalovaný další zranitelný software, který je podrobně rozepsán v přílohách této práce. Stroje měly vždy předinstalovaný software k určitému datu, tak jak to v některých firmách chodí, protože i přes rozšíření systému automatických aktualizací velké množství uživatelů tyto systémy vypíná a nechává tak operační systém či programy v něm nainstalované na neaktuální verzi. Občas aktualizacím nebrání samotní uživatelé, ale špatně nastavené firemní politiky, které běžnému uživateli nedovolí aktualizovat software, protože je zapotřebí zdlouhavého procesu schvalování příslušných verzí.

Každý virtuální počítač byl skenován zvlášť, přičemž byl kladen důraz na kvalitu detekce všech známých zranitelností. Zkoumanými veličinami byly čas, po který se skenování vykonávalo a případné nestandardní chování v jejich průběhu. Výsledky jsou prezentovány tabulkovou formou s komentářem.

6.1.1 Konfigurace virtuálních strojů

Pro důkladné otestování virtuálních strojů byla nutná určitá základní konfigurace, aby zvolené nástroje mohly plně přistupovat ke skenovaným systémům. Díky tomu bylo možné odhalit více nebezpečných zranitelností nebo je bylo možné detekovat s vyšší mírou spolehlivosti.

U cílových počítačů s operačním systémem Windows bylo nutné provést následující kroky:

- vytvořit nebo poskytnou přihlašovací údaje k účtu s právy administrátora,
- udělit výjimky pro SMB protokol ve Windows Firewall,
- zkontrolovat a případně nastartovat službu vzdálené registry.

První krok je v zásadě jednoduchý, protože stačí vytvořit unikátní lokální účet s právy administrátora, který poslouží k přístupu do skenovaného systému. Je možné také použít doménový účet, který je nutné dále nastavit, aby byl členem lokální skupiny administrátorů. V opačném případě by neměl požadovanou úroveň oprávnění při přístupu k cílovému zařízení. (Rapid7, 2019)

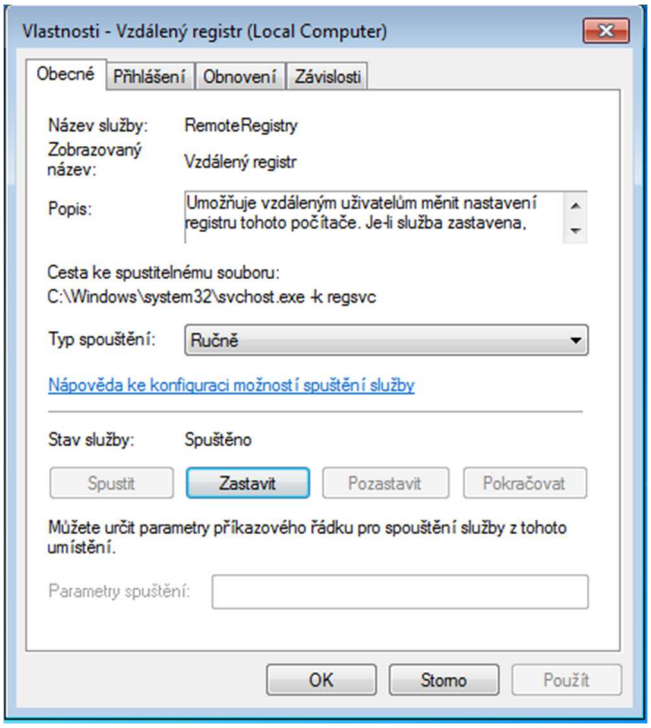
Dále je nutné povolit přístup k SMB protokolu v rámci integrovaného řešení Windows Firewall, které ve výchozím stavu tento protokol blokuje. Konkrétně se jedná o porty 139 a 445, které se využívají pro komunikaci pomocí tohoto protokolu. V systému Windows jsou tyto porty součástí volby Sdílení souborů a tiskáren, pro kterou je nutné udělit výjimku, která umožní skenovacímu nástroji připojit se k cílovému počítači.

Tento postup je doporučený a tvůrci skenovacích nástrojů preferovaný, důležité je si uvědomit, že názory vyskytující se v internetových diskuzích, které upřednostňují úplné vypnutí Windows

Firewall jsou zcestné, neboť se tak v průběhu provádění bezpečnostního auditu zbavíme možnosti otestovat správnost nastavení Windows Firewall.

V třetím kroku je nutné zkontrolovat službu vzdálených registrů. To je možné pomocí následujícího postupu:

- nejprve je nutné vyvolat nabídku *Spustit*, kterou je možné nalézt v nabídce Start,
    - alternativně je možné ji vyvolat pomocí klávesové zkratky Windows + R,
- dále do dialogového okna zadat *services.msc*, který vyvolá seznam služeb systému Windows,
- v seznamu služeb vyhledat službu *Vzdálený registr*[15],
- zkontrolovat, jestli služba běží a případně ji spustit.



Obrázek 18 – Spuštěná služba Vzdálený Registr ve Windows 7

Zdroj: vlastní

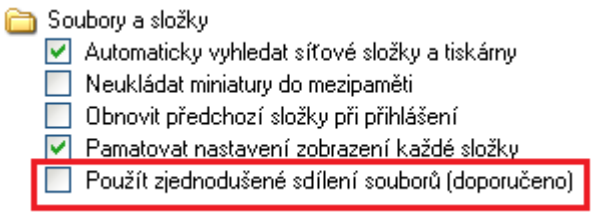
Výše uvedené kroky jsou dostatečné pro Windows Vista a novější. U Windows XP je nutné provést ještě jeden mezikrok. Je nutné vypnout možnost Zjednodušené sdílení souborů, které je ve výchozím stavu zapnuté. Tato služba automaticky nastavuje úrovně oprávnění na místech, kde ke sdílení dochází a obsahuje i průvodce, který umožní toto sdílení nastavit. Bohužel tento

[15] V anglické jazykové mutaci Windows se služba jmenuje *Remote Registry*.

nástroj nepočítá se skenovacími nástroji, které se používají na zjištění zranitelností, a tak je nutné tuto službu deaktivovat. (Bouška, 2019)

Deaktivaci je možné provést následovně:

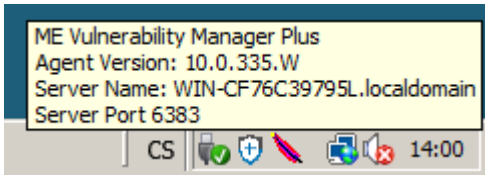
- pomocí nabídky start vyvoláme *Ovládací panely*,
- zde nalezneme položku *Možnosti složky,* kterou otevřeme,
- v Možnostech složky deaktivujeme položku *Použít zjednodušené sdílení soubor*[16] .



Obrázek 19 – Vypnuté zjednodušené sdílení souborů ve Windows XP

Zdroj: vlastní

Některé skenovací nástroje používají pro spojení vlastního agenta, který je nainstalován na cílovém zařízení. Toto řešení má své výhody i nevýhody. Mezi výhody patří lepší přístup k informacím z daného stroje, kdy není agent omezený pouze na předpřipravené služby a protokoly Windows a současně není nutné cílový počítač konfigurovat pomocí postupu uvedeného výše. Mezi nevýhody patří stále běžící služba agenta, která je přítomna na cílovém zařízení. Služba spotřebovává navíc systémové prostředky a současně není uživateli známo, jak a které informace přesně přenáší. Toto řešení využívá například ManageEngine Vulnerability Manager Plus.



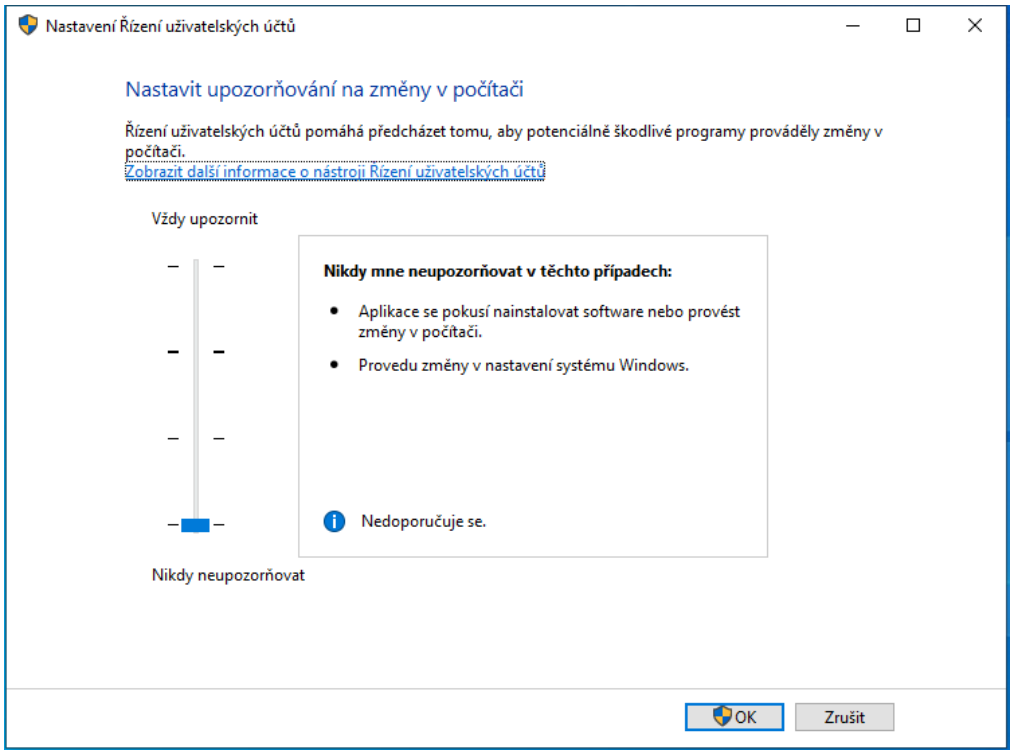
Obrázek 20 - Agent běžící na cílovém stroji

Zdroj: vlastní

V případě skenování operačních systémů Windows Vista a novější může problémy způsobovat také obranný nástroj Windows, který je možný dohledat pod zkratkou UAC, což se do češtiny překládá jako řízení uživatelský účtů. Tento nástroj omezuje oprávnění běžícím aplikacím na

[16] V anglické jazykové mutaci Windows XP se položka jmenuje *Use simple file sharing.*

úroveň běžného uživatele, kterým je možno až po souhlasu uživatele dát oprávnění vyšší. Bohužel nižší oprávnění může znemožnit přístup k částem systému, které skenery používají k detekci problémů, a proto je žádoucí po dobu provádění testů tuto funkcionalitu zcela vypnout.



Obrázek 21 - Vypnuté řízení uživatelských účtů u Windows 10

Zdroj: vlastní

V případě operačního systému založeného na Linuxu je nutné zajistit přístup pomocí protokolu SSH. Toho je možné dosáhnout na systému Debian instalací balíčku openssh-server příkazem *apt-get install openssh-server*. Balíčkovací systém APT zařídí instalaci balíčků, vytvoří potřebné klíče a konfigurační soubory. Výchozí nastavení je dostatečné pro většinu skenovacích nástrojů. Vhodné je, aby uživatel, který je použit pro přihlášení k systému, měl práva srovnatelná s uživatelem root, protože některé konfigurace systémů nemůže uživatel bez těchto oprávnění prohlížet a případně editovat.

6.1.2 Nastavení skenovacích nástrojů

Skenovací nástroje disponují širokou paletou testů, které je možné dále konfigurovat nebo omezovat jejich pole působnosti. Pro potřeby testování byl vždy vybrán nejkomplexnější test, který zahrnoval veškeré oblasti, které dokázal skener otestovat. Byly použité následující varianty skenů:

- u OpenVAS sken s názvem „Full and very deep ultimate“,
- u skeneru Nessu to byl „Advanced Scan“,
- u nástroje Nexpose se sken jmenuje „Full Audit“,
- Nmap s *vuln* skriptem byl spouštěn příkazem nmap -v --script *vuln ip-adresa-cíle*
- a v případě *vulscan* skriptu příkazem nmap -sV --script=vulscan/vulscan.nse *ip-adresa-cíle,*
- skripty Nikto2 byli spouštěny příkazem nikto -h *ip-adresa-cíle,*
- skener Retina obsahuje kombinace voleb „All Audit“ a „All ports“ a
- skener ManageEngine byl aktivován pomocí volby „Scan systems“.

Skenery ve většině případů měří čas, který proces vyhledávání zranitelností trval, výjimkou jsou skenery Nmap a Nikto2, u kterých bylo k měření času využito externího příkazu time, který je dispozici v rámci příkazové řádky systému Linux.

6.1.3 Testování virtuálního stroje s Windows XP

První testovaný stroj obsahuje nejstarší, avšak stále hojně používaný operační systém Windows XP. Podle statistik[17] není jeho rozšíření zanedbatelné a je například rozšířenější než jeho nástupci v podobě Windows Vista nebo Windows 8. Virtuální počítač dále obsahuje software, který je typický pro běžného uživatele. Je v něm zahrnutý například webový prohlížeč, přehrávač videí, kancelářský balík Microsoft Office nebo čtečka PDF souborů. Většina verzí těchto programů pochází z roku 2012, takže jsou plné zranitelností.

Nástroje by měly detekovat:

1. nepodporovanou verzi operačního systému,
2. chybějící záplaty systému Windows, hlavně SMB protokolu,
3. zranitelnosti v zastaralé verzi Microsoft Office XP,
4. zranitelný a zastaralý prohlížeč Mozilla Firefox,
5. zranitelný a zastaralý prohlížeč Google Chrome,
6. zastaralou a zranitelnou verzi Adobe Reader,
7. větší množství zranitelností v Java 6 SE,
8. nebezpečný doplněk Adobe Flash Player,
9. neaktualizovaný antivir Avast,

[17] Statistiky lze nalézt například na: https://netmarketshare.com/operating-system-market-share.aspx.

10. zranitelnosti v Oracle VirtualBox,
11. známé zranitelnosti v přehrávači VLC
12. a zranitelnosti v kompresním programu WinRAR.

Tabulka 6 - Výsledek detekcí ve Windows XP

Číslo problému / Použitý nástroj	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.
OpenVAS	☒	☒	☒	☐	☒	☒	☒	☒	☐	☒	☒	☒
Nessus Essentials	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☐
Nexpose Community	☒	☒	☒	☒	☒	☒	☒	☒	☐	☐	☒	☒
Nmap (*vuln* script)	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Nmap (*vulscan* script)	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Nikto2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Retina Network SS	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
ManageEngine VMP	nebylo možné test provést											

Zdroj: vlastní

V následující tabulce je zobrazeno další důležité kritérium, kterým je doba trvání skenů jednotlivých nástrojů.

Tabulka 7 - Čas skenů jednotlivých nástrojů u stroje s Windows XP

Použitý nástroj	Čas skenu [mm:ss]
OpenVAS	12:15
Nessus Essentials	07:00
Nexpose Community	02:12
Nmap (*vuln* script)	00:20
Nmap (*vulscan* script)	00:23
Nikto2	00:40
Retina Network SS	11:05
ManageEngine VMP	netestováno

Zdroj: vlastní

První sken přinesl řadu překvapení. I když byl testovaný virtuální stroj vybavený jednoznačně zastaralým operačním systémem a historickými verzemi uživatelského software, řada nástrojů velmi zklamala. Nástroj OpenVAS odhalil většinu problémů, ovšem nedokázal si poradit

s třetím nejrozšířenějším prohlížečem[18] Mozilla Firefox. Ten zde byl nainstalován ve velmi staré a kriticky zranitelné verzi, ale nástroj ho vůbec nedetekoval. U OpenVASu se v průběhu testu objevil ještě jeden problém. Grafické prostředí ztrácelo v průběhu skenu kontakt se skenovacím démonem a vypisovalo chybové hlášky. Na vyhodnocení výsledků to nemělo vliv, ale bylo obtížné sledovat průběh skenu. Skenery Nexpose a Nessus si vedly o něco lépe, největší zranitelnosti dokázaly detekovat, neporadily si pouze se softwarem, ve kterém zranitelností není mnoho (WinRAR) nebo nemá tak velkou uživatelskou základnu (VirtualBox).

Obrázek 22 - Ztráta spojení při skenu v nástroji OpenVAS

Zdroj: vlastní

Samotnou kapitolou je Nmap a jeho skripty. Ty v tomto testu zcela propadly. Skript *vuln* dokázal odhalit pouze jednu zranitelnost, což je velmi nedostatečné. V jeho případě alespoň nedošlo na další falešné detekce. Horší situace nastala u skriptu *vulscan*. Ten na první pohled nalezl všechny problémy, které byly testované. Zajímavé ovšem bylo, že nástroj detekoval ohromné množství zranitelností (přes 33 000), což je velmi podezřelé, a proto byl znovu podroben testu, tentokrát na čisté instalaci Windows XP. Nový sken dopadl shodně, protože nástroj opět detekoval stejné množství zranitelností, a protože se ve výsledném logu vyskytovalo velké množství zranitelného softwaru, který ani nebyl nainstalován, není možné jeho výsledky považovat za důvěryhodné.

Nástroj Nikto2 byl do testu zařazen spíše z důvodu, zda nepředvede nějakou falešnou detekci, protože je primárně zaměřen na skenování webových serverů a ten na počítači přítomen nebyl. V tomto tedy obstál na výbornou.

Výborně detekoval veškeré zranitelnosti nástroj Retina Network Security Scanner, který to navíc zvládl za 11 minut. Jedná se sice o druhý nejpomalejší čas, ale kvalita detekce tento neduh dorovnává a je tak nejlepší nástroj, který si s daným zranitelným strojem nejlépe poradil.

[18] Statistiky prohlížečů k nalezení například zde: http://gs.statcounter.com

Poslední nástroj ManageEngine VMP nakonec testován nebyl, protože nebylo možné nainstalovat agenta na cílový počítač. Při instalaci se objevovaly hlášky o chybějící knihovně advapi32.dll, která v systému přítomna byla. Tvůrce na svých stránkách uvádí zmatené informace o podpoře Windows XP, a proto je nejpravděpodobnější, že podpora už byla ukončena a není kompletně zaktualizovaná dokumentace tohoto nástroje.

6.1.4 Testování virtuálního stroje s Windows 7

Dalším na řadě byl virtuální počítač s nainstalovaným o něco novějším operačním systémem Windows 7. Stroj dále obsahoval podobnou skladbu softwarového vybavení jako jeho předchůdce s jediným rozdílem, veškerý software pocházel z přelomu let 2014 až 2016. Jedná se o dostatečně zranitelný, ale také velmi značně rozšířený operační systém a software, a proto prvotní očekávání byla velká. Nástroje by s tímto virtuálním počítačem neměly mít problémy.

V testovaném stroji je možné nalézt:

1. aktivní Telnet,
2. chybějící záplaty systému Windows, hlavně SMB protokolu,
3. zranitelnosti v zastaralé verzi Microsoft Office 2010,
4. zranitelný a zastaralý prohlížeč Mozilla Firefox,
5. zranitelný a zastaralý prohlížeč Google Chrome,
6. zastaralou a zranitelnou verzi Adobe Reader,
7. větší množství zranitelností v Java 7 SE,
8. neaktualizovaný antivir Avast,
9. zranitelnosti v Oracle VirtualBox,
10. známé zranitelnosti v přehrávači VLC
11. a zranitelnosti v kompresním programu WinRAR

Tabulka 8 - Výsledek detekcí ve Windows 7

Číslo problému / Použitý nástroj	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.
OpenVAS	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Nessus Essentials	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☐
Nexpose Community	☒	☒	☒	☒	☒	☒	☒	☐	☐	☐	☒
Nmap (*vuln* script)	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐
Nmap (*vulscan* script)	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Nikto2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Retina Network SS	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
ManageEngine VMP	☒	☒	☒	☒	☐	☐	☐	☒	☒	☒	☒

Zdroj: vlastní

V následující tabulce je zobrazen přehled časové náročnosti skenů zranitelností v rámci stroje s operačním systémem Windows 7.

Tabulka 9 - Čas skenů jednotlivých nástrojů u stroje s Windows 7

Použitý nástroj	Čas skenu [mm:ss]
OpenVAS	11:13
Nessus Essentials	09:00
Nexpose Community	14:58
Nmap (*vuln* script)	00:20
Nmap (*vulscan* script)	00:32
Nikto2	00:40
Retina Network SS	10:11
ManageEngine VMP	14:46

Zdroj: vlastní

Výsledky v podstatě splnily očekávání. Nástroj OpenVAS bezchybně detekoval veškeré zranitelnosti v poměrně dobrém čase. O jeden problém méně nalezl nástroj Nessus, jehož výsledek se dá také považovat za výborný, i se zahrnutím skenovacího času, který byl o dvě minuty kratší než jeho úspěšnější konkurence. Mírné zaváhání je vidět na straně nástroje Nexpose, který nedokázal detekovat celkem tři problémy. Vše je ještě navíc podtrženo nejhorším časem.

Skripty Nmapu své špatné výsledky z předchozího testu nevylepšily. Skript *vuln* detekoval pouhé dva problémy, což je velmi nedostatečné. Mnohem hůře dopadl skript *vulscan*, který tentokrát detekoval ještě více problémů než v předchozím případě. Bohužel i tentokrát naprosto selhal, protože detekoval mnoho zranitelností, které v daném stroji neexistují a ani existovat nemohly. Ve výsledku jich našel přes 43 000, bohužel byl zopakován test na úplně čistém stroji, kde nalezl stejný počet, a proto není možné brát jeho výsledky vážně.

Nikto2 opět nedetekoval žádný problém, protože na testovaném stroji nebyl nainstalovaný žádný webový server, takže se zachoval naprosto správně, nebyla zde žádná falešná detekce.

Skener Retina od společnosti BeyondTrust opět předvedl bezchybný výkon, protože zvládl detekovat vše. Navíc sken proběhl v rozumném čase. Vytknout se mu dá pouze pád v průběhu prvního pokusu o test, kdy se skener zastavil a dále nehledal. Po restartu aplikace vše proběhlo v pořádku.

ManageEngine Vulnerability Manager Plus byl tentokrát úspěšně otestován, protože instalace agenta na cílový stroj proběhla bez problémů. Skener odhalil větší část problémů, ale i přes přítomnost vlastního agenta na cílovém stroji nedokázal tři problémy odhalit. Jeho výkon se dá označit za průměrný a srovnatelný se skenerem Nexpose. V kvalitě detekce jsou tedy v rámci tohoto virtuální stoje vítězové dva, a to skener OpenVAS a Retina, kteří podali bezchybný výkon v podobném čase.

6.1.5 Testování virtuálního stroje s Windows 10

Tento testovaný stroj obsahuje nejnovější operační systém od společnosti Microsoft, ve své poslední verzi. Obsahuje také běžný uživatelský software, který je zde ve svých relativně aktuálních verzích. Obsažené problémy byly objeveny v období od posledního kvartálu roku 2018 do konce druhého kvartálu 2019. Nejstarší zranitelnosti pocházející z roku 2018 byly v programech WinRAR, Thunderbird a LibreOffice. Naopak úplně nejčerstvější zranitelnosti pochází z týdne před provedením testů v programu VLC, které jsou v pořadí od nejnovějších následovány zranitelnostmi v Adobe Acrobat DC, které jsou staré přibližně měsíc, přes dva měsíce staré bezpečnostní problémy v Mozilla Firefox až po zranitelnost v programu VirtualBox, která pochází z počátku roku 2019. Nástroje byly před provedením testu aktualizovány na poslední verze svých databází[19], aby bylo možné zachytit, jak důsledně tvůrci nástrojů reagují na nové hrozby.

[19] Aktualizace i test proběhly dne 1. 7. 2019.

V testovaném stroji by měli nástroje nalézt:

1. Firefox se zranitelností CVE-2019-9805, která může vést k narušení paměti,
2. Firefox se zranitelností CVE-2019-9792, kde je možné pomoci Javascriptu narušit paměť,
3. VLC se zranitelností CVE-2019-12874, která způsobuje nestabilitu při čtení narušeného souboru formátu MKV,
4. VLC se zranitelností CVE-2019-5439, které způsobuje přetečení vyrovnávací paměti,
5. Acrobat DC, více zranitelností od CVE-2019-7111 do CVE-2019-7841, většinou možnost vzdáleného volání kódu,
6. LibreOffice se zranitelností CVE-2018-16858, která umožnuje makru spustit Python skript,
7. WinRAR se zranitelností CVE-2018-20250, která způsobuje chybu při zpracování ACE formátu,
8. VirtualBox se zranitelností CVE-2019-2511, která umožnuje pomocí SOAP protokolu způsobit pád programu,
9. deaktivovaný antivirus Avast,
10. zranitelnost CVE-2018-12368, která umožnuje v Thunderbirdu spustit instalátor bez vědomí uživatele,
11. aktivní zranitelnou verzi 1 protokolu SMB
12. a slabé heslo Administrátora přístupného přes SMB.

Tabulka 10 - Výsledek detekcí ve Windows 10

Číslo problému / Použitý nástroj	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.
OpenVAS	☒	☒	☐	☐	☐	☒	☒	☒	☐	☒	☒	☒
Nessus Essentials	☒	☒	☒	☒	☐	☒	☒	☒	☒	☒	☒	☐
Nexpose Community	☒	☒	☐	☐	☐	☐	☒	☐	☐	☒	☐	☐
Nmap (*vuln* script)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐
Nmap (*vulscan* script)	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Nikto2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Retina Network SS	☒	☒	☐	☐	☐	☐	☐	☒	☐	☐	☒	☒
ManageEngine VMP	☒	☒	☐	☐	☐	☐	☐	☐	☒	☐	☒	☐

Zdroj: vlastní

Následuje tabulkový přehled časové náročnosti skenerů pro provedení skenů zranitelností na testovaném systému.

Tabulka 11 - Čas skenů jednotlivých nástrojů u stroje s Windows 10

Použitý nástroj	Čas skenu [mm:ss]
OpenVAS	10:34
Nessus Essentials	06:18
Nexpose Community	01:23
Nmap (*vuln* script)	00:21
Nmap (*vulscan* script)	00:23
Nikto2	00:10
Retina Network SS	17:26
ManageEngine VMP	04:07

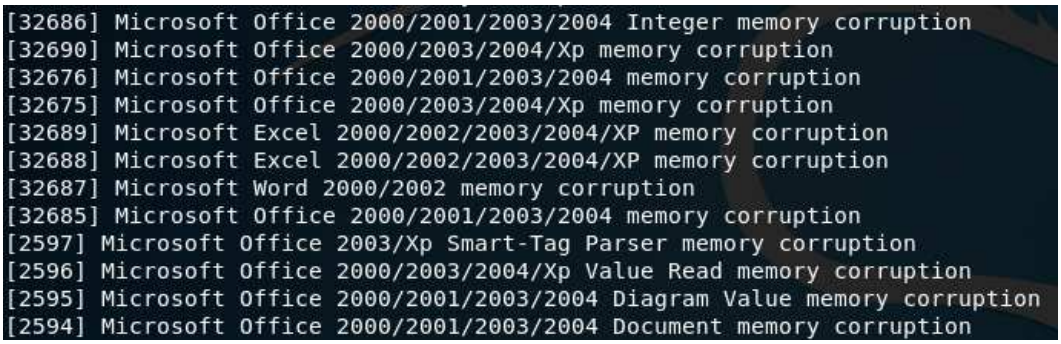
Zdroj: vlastní

Jako první přišel na řadu nástroj OpenVAS, který dokázal detekovat zranitelnosti, které byly objeveny přibližně měsíc před provedením skenu. V testovaném případě tedy nové zranitelnosti u VLC a Adobe Acrobat detekovat nedokázal. O mnoho lépe si vedl skener Nessus. Ten detekoval veškeré zranitelnosti, jen nedokázal odhalit slabé heslo při připojení pomocí SMB protokolu. I přesto je jeho výkon nejlepší, protože vše navíc zvládl v poměrně krátkém čase.

Nexpose v testu poměrně propadl, protože sice detekoval relativně aktuální zranitelnosti ve webovém prohlížeči, ale jiné, které jsou staršího data, mu dělaly problémy. Za zmínku stojí například zranitelnost v LibreOffice z konce roku 2018 nebo zranitelný VirtualBox.

U konzolových nástrojů se velký úspěch čekat nemohl, protože nemají přímý přístup do registru systému Windows, kde by detekovaly nainstalované verze softwarového vybavení. Ovšem i tak nezklamal nástroj Nmap v kombinaci se sadou skriptů *vulscan*, který detekoval přes 32 000 zranitelností. Problém je, že většina z nich byla falešná. Nikto a *vuln* falešné detekce neměli, a dokonce skript *vuln* detekoval protokol SMB verze 1.

Nástroje pro Windows neměly problém se zranitelnou verzí Mozilla Firefox a starou verzí SMB protokolu, ale tím možnosti jejich detekce téměř končí, protože až na pár výjimek nic dalšího neodhalily. Vítězem tohoto testu je tedy Nessus, který předvedl, že disponuje nejaktuálnější a nejkompletnější databází zranitelností.



Obrázek 23 - Jedny z mnoha falešných detekcí u *vulscan* scriptu

Zdroj: vlastní

6.1.6 Testování virtuálního stroje s Windows Server 2008

Tento testovaný stroj prověří nástroje hlavně z oblasti webu a webových aplikací. Virtuální počítač má nakonfigurovaný webový server Apache, na kterém běží několik známých webových aplikací. Současně obsahuje PHP a databázi MySQL, které tyto aplikace používají. Vše běží na dnes již starém serverovém operačním systému Windows Server 2008. Virtuální počítač má nakonfigurovaný přístup k portům 80, 443 a 3306 zvenčí, aby bylo možné používat webové aplikace a dělat zásahy do databáze. V testovaném stroji je možné nalézt:

1. zastaralou a zranitelnou verzi webového serveru Apache,
2. nepodporovaná verze Apache,
3. velké množství kritických zranitelností v PHP,
4. nepodporovanou verzi PHP,
5. zranitelná a zastaralá webová aplikace phpMyAdmin,
6. zastaralá a zranitelná webová aplikace MediaWiki,
7. nepodporovaná verze MediaWiki,
8. větší množství zranitelností ve Wordpressu
9. zranitelnou a zastaralou verzi MySQL,
10. výchozí uživatel root bez hesla v MySQL,
11. nepodporovaná verze MySQL
12. a zranitelnosti v SMB z důvodu chybějících aktualizací.

Tabulka 12 - Výsledek detekcí ve Windows Server 2008

Číslo problému / Použitý nástroj	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.
OpenVAS	☒	☒	☒	☒	☒	☒	☒	☒	☒	☐	☒	☒
Nessus Essentials	☒	☒	☒	☒	☐	☐	☐	☐	☐	☐	☐	☒
Nexpose Community	☒	☐	☒	☐	☒	☐	☐	☒	☒	☒	☒	☒
Nmap (*vuln* script)	☒	☐	☐	☐	☒	☐	☐	☐	☒	☐	☐	☒
Nmap (*vulscan* script)	☒	☐	☒	☐	☒	☐	☐	☒	☒	☐	☐	☒
Nikto2	☒	☒	☒	☒	☒	☐	☐	☐	☐	☐	☐	☐
Retina Network SS	☒	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☒
ManageEngine VMP	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒

Zdroj: vlastní

V následujícím přehledu je zobrazena délka procesu skenovaní u jednotlivých nástrojů, který obsahuje překvapivé výsledky hlavně u skeneru OpenVAS.

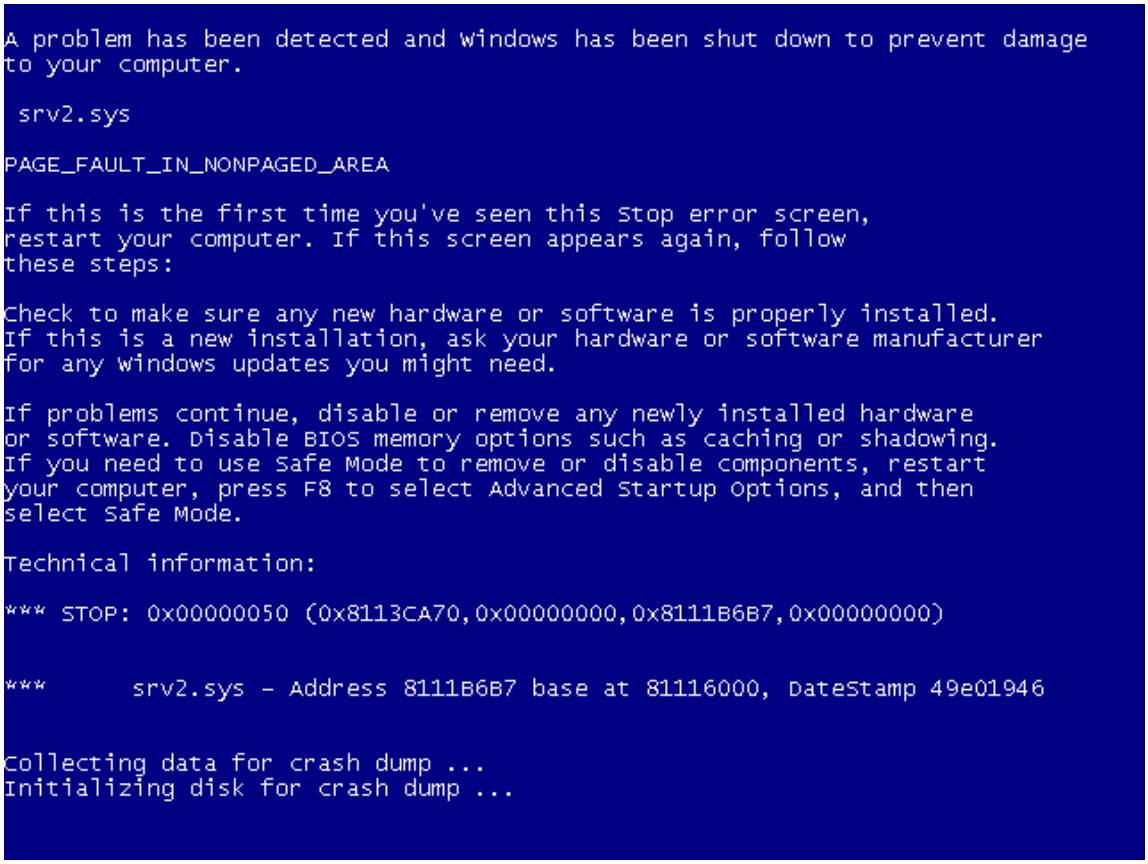
Tabulka 13 - Čas skenů jednotlivých nástrojů u stroje s Windows Server 2008

Použitý nástroj	Čas skenu [h:mm:ss]
OpenVAS	1:53:17
Nessus Essentials	0:26:00
Nexpose Community	0:07:03
Nmap (*vuln* script)	0:07:17
Nmap (*vulscan* script)	0:00:45
Nikto2	0:14:49
Retina Network SS	0:22:15
ManageEngine VMP	0:02:06

Zdroj: vlastní

Skenování serverové edice Windows přineslo celou řadu překvapení. Vítězem co do kvality detekce se stal nástroj OpenVAS, který detekoval nejvíce problémů, ovšem za cenu extrémně dlouhého skenovacího času. Žádný jiný skener se nedostal ani přes půl hodiny, kdežto OpenVAS atakoval téměř dvě hodiny. V testu poměrně propadl skener Nessus, který ač obsahuje databázi zranitelných webových aplikací, tak v podstatě žádnou z nich nepoznal. Stejný problém měl i s databázi MySQL, u které dokázal detekovat pouze její přítomnost. Nexpose na tom byl o něco lépe, nedokázal si poradit pouze s MediaWiki.

Skripty Nmapu tentokrát vyprodukovaly použitelné informace. Skript *vuln* detekoval celkem 4 problémy z dvanácti, přičemž jeden z podružených skriptů dokonce při své činnosti způsobil BSOD. Skript *vulscan* vyprodukoval poprvé použitelné výsledky, které odpovídají zranitelnostem v rámci testovaného stroje. Problémem jsou ovšem stálé falešné detekce, kdy byl například detekován Drupal, který na tomto stroji nikdy nainstalován nebyl.



Obrázek 24 - Obrazovka smrti při skenu *vuln* skriptem

Zdroj: vlastní

Pro sadu skriptů Nikto2 toto měl být test, kde měl nejvíce excelovat, místo toho odhalil pouze necelou polovinu problémů. Největší potíže měl s webovými aplikacemi, kde dokázal poznat pouze phpMyAdmin.

Nástroj Retina Network dosáhl oproti minulým testům hodně špatných výsledků. Zde je to dáno omezením zkušební verze, která netestuje webové aplikace ani databáze. Nástroj pouze detekoval jejich existenci a vyzval k pořízení placené verze. ManageEngine VMP také nepředvedl přesvědčivý výsledek, pouze upozornil na webový server a chybějící aktualizace, ostatních problémů si ani nevšiml, maximálně dokázal detekovat otevřené porty a služby, které je používají, ale na další vyhodnocení nedošlo. Vítězem tohoto testu je tedy nástroj OpenVAS, který detekoval téměř všechny problémy.

6.1.7 Testování virtuálního stroje s Debian 9

Linuxový virtuální stroj je svoji softwarovou výbavou velmi specifický, protože obsahuje software pro poskytování mapových dat. Oblast kartografického software byla vybrána proto, aby skenovací nástroje prověřila, zda umí detekovat a následně vyhledat zranitelnosti u software, který se v uživatelských instalacích vyskytuje vzácně.

V instalaci se nacházel MapServer, který poskytuje platformu pro poskytování geospeciálních dat. Jeho prvotní vývoj finančně zajišťovala NASA, která tento nástroj používala pro distribuci satelitních snímků veřejnosti. V současné době je možné MapServer provozovat buď jako CGI program anebo pomocí knihovny MapScript, která umožňuje přístup z nejrůznějších programovacích jazyků.

Dále byl do instalace přidán modul MapCache, který slouží k urychlení načítání mapových dat za pomocí předpřipravených mapových dlaždic, které je možné generovat z mapových zdrojů, které poskytuje například výše zmíněný MapServer. MapCache je možné provozovat jako CGI program nebo jako modul webového serveru Apache.

Posledním instalovaným kartografickým nástrojem je terénní server. Jedná se o speciálně nakonfigurovaný webový server Nginx, který s daným nastavením dokáže poskytovat výšková data ve formátu Quantized Mesh. Tento formát se využívá v knihovně CesiumJS pro modelování 3D terénu v kombinaci s mapovými podklady,

Detekce těchto nástrojů je navíc ztížena přítomnosti technologie Docker, ve kterém část tohoto software běží. Tento počítač také prověří detekce běžných webových serverů, které se nachází mimo své typické porty. Stejná situace je i u databáze PostgreSQL, kde jedna instance běží v prostředí Dockeru a druhá mimo něj, ale na netypickém portu. Ověřena bude také identifikace slabých nebo žádných hesel u SSH a databáze.

Nástroje by měly odhalit:

1. běžící Docker,
2. webový server Apache v několika instancích na netypických portech (8283 a 8080),
3. webový server Nginx na netypickém portu (8888),
4. u webového serveru detekovat u HTTPS certifikát podepsaný sám sebou (sefl signed),
5. detekovat MapServer dostupný pomocí CGI uvnitř docker image,
6. detekovat nainstalovaný Apache modul MapCache,
7. u MapServeru a MapCache poznat zranitelnost CVE-2017-12808,

8. odhalit kombinaci root/root uživatelského jména a hesla pro přihlášení přes SSH,
9. detekovat dvě běžící instance PostgreSQL (porty 5432 a 5433)
10. a detekovat vzdálený přístup do databáze PostgreSQL s výchozím uživatelem bez hesla.

Tabulka 14 - Výsledek detekcí v Debian 9

Číslo problému / Použitý nástroj	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.
OpenVAS	☒	☐	☒	☒	☐	☐	☐	☒	☐	☐
Nessus Essentials	☐	☒	☒	☒	☐	☐	☐	☐	☐	☐
Nexpose Community	☒	☐	☒	☒	☐	☒	☐	☒	☒	☒
Nmap (*vuln* script)	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Nmap (*vulscan* script)	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐
Nikto2	☐	☒	☒	☐	☐	☐	☐	☐	☐	☐
Retina Network SS	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ManageEngine VMP	nebylo možné test dokončit									

Zdroj: vlastní

Tabulka představuje délky trvání skenů u jednotlivých skenovacích nástrojů. Časy se zde také velmi liší od desítek vteřin po desítky minut.

Tabulka 15 - Čas skenů jednotlivých nástrojů u stroje s Debian 9

Použitý nástroj	Čas skenu [mm:ss]
OpenVAS	20:39
Nessus Essentials	06:01
Nexpose Community	03:42
Nmap (*vuln* script)	05:22
Nmap (*vulscan* script)	00:31
Nikto2	3:40
Retina Network SS	12:31
ManageEngine VMP	nedokončený test

Zdroj: vlastní

Výsledků těchto skenů dopadly velmi špatně. Většina nástrojů byla zmatena z netypických portů, a proto nedokázala detekovat správně všechny služby. Ještě větší problém ovšem způsobil software z kartografického odvětví. Zde až na jednu malou výjimku nástroje zcela

propadly. Nástroj OpenVAS zvládl celkem čtyři úkoly z deseti, kdy mu největší problém dělal kartografický software, kde úplně selhal. Stejně tak si neporadil s netypickými porty u webového serveru Apache a databáze PostgreSQL Služby běžící na standardních portech detekoval bezchybně a problém mu nedělalo ani slabé heslo u SSH. Bohužel test slabých přihlašovacích údajů si neporadil s otevřením přihlášením do databáze, které detekovat nedokázal.

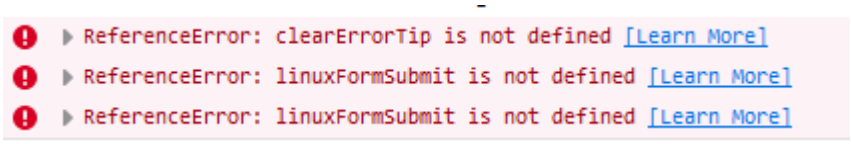
Nástroj Nessus dopadl ještě o něco hůře. S netypickými porty velký problém neměl, i když databázi mimo typický port 5432 odhalit nedokázal. Nevšiml si ani běžícího prostředí Docker, stejně tak mu dělal problém veškerý kartografický software.

Nexpose dopadl ze všech skenerů nejlépe. Problém měl pouze s netypickým portem u webového serveru Apache a jako jediný dokázal odhalit alespoň běžící modul MapCache, který se používá k urychlení načítání mapových podkladů pomocí předpřipravených souborů mapových dlaždic. Detekovat MapServer ovšem nedokázal, stejně tak nevaroval před v něm přítomnou zranitelností.

Skripty Nmapu také úplně propadly. Nedá se jim vyčítat fakt, že nepoznají běžící Docker, ale detekovat služby by už zvládnout mohly, bohužel se tak nestalo a *vuln* dokázal detekovat pouze dvě instance webového server Apache ze tří a jeden běžící databázový server. *Vulscan* dopadl lépe, ten přidal úspěšnou detekci webového serveru Nginx, ale také přibližně 3000 falešných detekcí. To nelze považovat za uspokojivý výsledek.

Skener Nikto2, který se zaměřuje na webové servery, byl úspěšný v detekci na všech portech, bohužel nedokázal úspěšně najít cestu k CGI skriptům, kterou bylo nutné dodatečně specifikovat. Do příkazu byl přidán přepínač *-C*, jehož argumentem je cesta, kde se CGI programy nachází. Příkaz vypadal například takto: *nikto -h 192.168.94.143 -C cgi-bin.* I přes tuto specifikaci nástroj MapServer nedetekoval.

Nástroje, běžící pouze na platformě Windows, selhaly úplně. Skener Retina sice sken provedl, ale i přes to, že se tvůrci chlubí, že umí skenovat prostředí Docker, tak ho ani neregistroval. Horší situace nastala u ManageEngine, který sice Linux také podporuje, ale už při nastavení skeneru docházelo k problémům při použití prohlížeče Mozilla Firefox, který je oficiálně podporován. Když se nástroj povedlo nastavit, úspěšně se vygeneroval agent, který ale následně při procesu skenovaní na cílovém stroji selhal a sken nebylo možné dokončit. Pomyslným vítězem tohoto testu je tedy skener Nexpose.



Obrázek 25 - Výpis chyb v konzoli prohlížeče Firefox u ManageEngine

Zdroj: vlastní

6.1.8 Shrnutí

V rámci případové studie byla představena malá virtuální síť, která byla pestrá jak do verzí použitých operačních systémů, tak do použitého softwarového vybavení, kterým disponovaly jednotlivé virtuální stroje. V průběhu testování bylo zkoumáno celkem 57 zranitelností a špatných nastavení systémů, se kterými si musely nástroje poradit. Jejich celkovou úspěšnost je možné vidět níže.

Tabulka 16 – Celkový počet úspěšných detekcí napříč testy

Použitý nástroj	Počet úspěšných detekcí	Úspěšnost [%]
OpenVAS	44	77,1
Nessus Essentials	39	68,4
Nexpose Community	37	64,9
Retina Network SS	31	54,4
ManageEngine VMP	15	26,3
Nmap (*vuln* script)	7	12,2
Nmap (*vulscan* script)	7	12,2
Nikto2	7	12,2

Zdroj: vlastní

Skener OpenVAS s přehledem zvítězil, i když na kvalitě jeho detekce je stále co vylepšovat, protože i přes vítězství nedokázal detekovat necelou čtvrtinu problémů. Tento fakt je o to příjemnější, že se jedná o nástroj, který je zdarma a má otevřené zdrojové kódy.

Tabulka 17 – Celkový čas skenů jednotlivých nástrojů

Použitý nástroj	Čas skenu [h:mm:ss]
OpenVAS	2:47:58
Retina Network SS	1:13:28
Nessus Essentials	0:54:19
Nexpose Community	0:29:18

ManageEngine VMP[20]	0:20:59
Nikto2	0:19:59
Nmap (*vuln* script)	0:13:40
Nmap (*vulscan* script)	0:02:34

Zdroj: vlastní

Na druhém a třetím místě se umístily komerční nástroje Nessus a Nexpose, které mají podobnou kvalitu detekce, která je sice horší než u nástroje OpenVAS, na druhou stranu je jejich práce rychlejší, kdy podle tabulky celkových časů zvládli své skeny dokončit za třetinový až pětinový čas.

Čtvrté místo obsadil skenovací nástroj Retina, který detekoval přibližně polovinu zranitelností a problémů. Ze začátku se zdál jako jasný favorit, protože v prvních testech předvedl bezchybnou detekci všech problémů, ale později už tak úspěšný nebyl a jeho výsledek dokonala omezení, která výrobce nastavil bezplatné zkušební verzi.

Páté místo obsadil jediný zástupce, který spoléhal při skenovaní na svého agenta. ManageEngine Vulnerability Manager Plus zklamal na plné čáře. Pomocí tohoto nástroje nebylo možné otestovat dva virtuální stroje, protože jeho nasazování provázely problémy, i když výrobce se chlubil kompatibilitou s daným systémem. V ostatních testech si nevedl také nejlépe, takže se svojí cenou za plnou verzi se jedná o software, který není možné doporučit.

Poslední tři místa obsadily skripty nástroje Nmap a sada skriptů Nikto2, které byly od začátku penalizovány faktem, že nedisponují prostředky přímého přístupu do systému přes vestavěné nebo vlastní prostředky, například pomocí vzdálených registrů nebo agentů. Tento fakt se podepsal na jejich špatném výsledku, protože bez těchto nástrojů není možné s vysokou spolehlivostí detekovat instalovaný software, a proto je nelze doporučit. Nejvíce problémový byl skript *vulscan*, který nelze obzvlášť doporučit, protože v průběhu provádění testů vykazoval tisíce falešných detekcí, mezi kterými se skutečně správné výsledky nedaly dohledat, pokud uživatel nevěděl, co konkrétně hledá. Smysl samostatného použití sady skriptů Nikto2 také není valný, protože je v rámci některých nástrojů rovnou integrován jako jejich součást, a proto je jeho použití vhodné doporučit v rámci skenovacího nástroje OpenVAS.

[20] Výsledek není objektivní, skener se některých testů neúčastnil.

6.2 Vnější perimetr sítě

Dalším úkolem bylo prověřit testované skenery na vnějším perimetru. K tomuto účelu bylo využito zařízení MikroTik, které bylo podrobeno testům. Toto zařízení je typické pro malé poskytovatele internetu, kteří na nich staví své sítě.

Zařízení disponovalo celou řadou zranitelností, které vyplývají ze špatného nastavení, kam patří například nepoužití hesla do administrací, aktivní zbytečné služby jako telnet anebo povolené nebezpečné šifrovací a hašovací algoritmy. Další zranitelnosti, kterými zařízení disponuje, mají počátek v zastaralé verzi operačního systému RouterOS.

Na zařízení MikroTik se nacházel:

1. aktivní Telnet, který přenáší data a hesla nešifrovaná,
2. aktivní FTP, které posílá data nešifrovaná,
3. běžící SSH,
4. povolený CBC mód pro šifrovací algoritmy (AES, 3DES) u SSH,
5. použití HMAC-MD5 u SSH,
6. běžící webovou administraci na portu 80,
7. uživatele admin bez hesla u zařízení při použití SSH a webové administrace,
8. zranitelnost CVE-2018-7445, která umožňuje vzdálené volání kódu přes SMB
9. zranitelnosti CVE-2018-1156 až CVE-2018-1159, které umožňují přetečení zásobníků a narušení paměti,
10. zranitelnost CVE-2018-10070, pomocí které je možné zařízení přes FTP zahltit,
11. zranitelnost CVE-2018-14847, která umožňuje stažení databáze uživatelů, pomocí které se pak může útočník přihlásit na zařízení a převzít kontrolu,
12. zranitelnost KRACK, která je vedena na WPA2 protokol.

Tabulka 18 - Výsledek detekcí u zařízení MikroTik

Číslo problému / Použitý nástroj	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.
OpenVAS	☒	☒	☒	☒	☒	☒	☐	☒	☒	☒	☒	☒
Nessus Essentials	☒	☒	☒	☒	☒	☐	☐	☒	☒	☐	☒	☐
Nexpose Community	☒	☒	☒	☐	☐	☐	☒	☐	☐	☐	☐	☐
Nmap (*vuln* script)	☒	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐
Nmap (*vulscan* script)	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Nikto2	☐	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐
Retina Network SS	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
ManageEngine VMP	test nemohl proběhnout											

Zdroj: vlastní

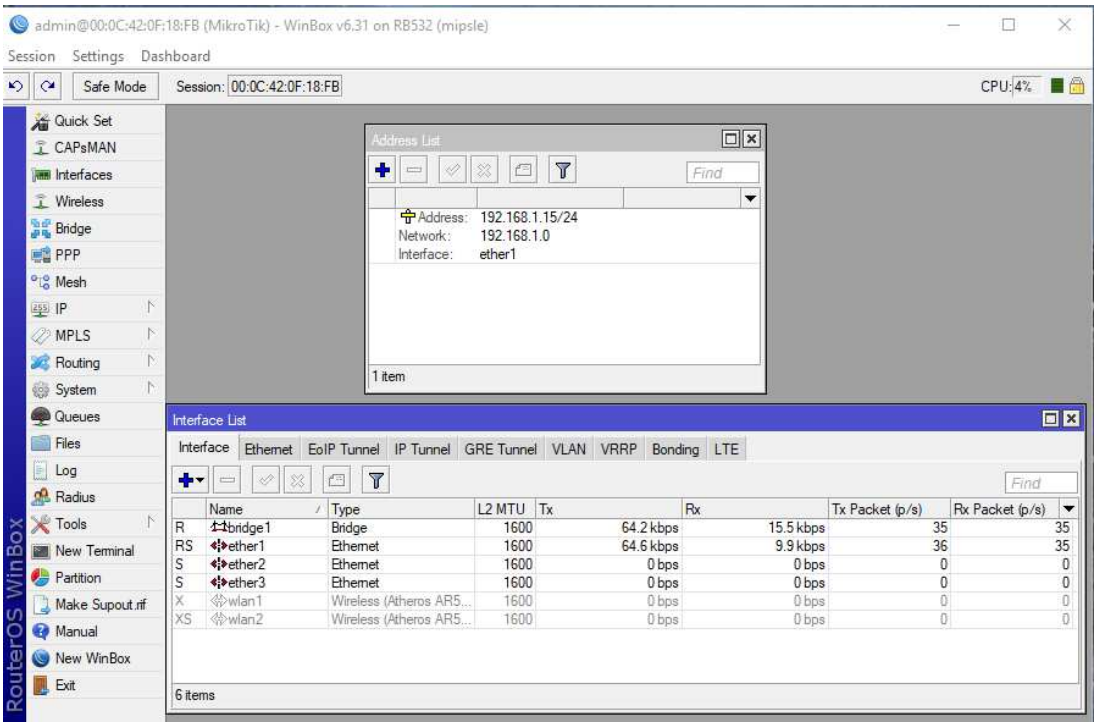
V následujícím přehledu je zobrazena časová náročnost skenovacího procesu jednotlivých nástrojů, který obsahuje překvapivé výsledky hlavně u skeneru OpenVAS. Ten měl nejdelší čas skenování ze všech testovaných nástrojů.

Tabulka 19 - Čas skenů jednotlivých nástrojů u zařízení Mikrotik

Použitý nástroj	Čas skenu [mm:ss]
OpenVAS	26:24
Nessus Essentials	04:08
Nexpose Community	03:27
Nmap (*vuln* script)	07:57
Nmap (*vulscan* script)	04:12
Nikto2	09:38
Retina Network SS	07:53
ManageEngine VMP	nebylo možné otestovat

Zdroj: vlastní

Při ověřování vnějšího perimetru sítě se ukázalo, že pouze dva nástroje disponují dostatečnou detekcí a je možné je doporučit. Nejúspěšnější byl nástroj OpenVAS, který detekoval jedenáct z dvanácti možných problémů. Byl následován rychlejším, ale méně schopným Nessusem, který detekoval 8 problémů z dvanácti možných.



Obrázek 26 - Prostředí administrace MikroTiku v průběhu testu

Zdroj: vlastní

Nástroj Nexpose a skript *vuln* předvedly podobné možnosti detekce, jejich výsledek je už ale velmi slabý pro reálné použití. Ještě horších výsledků však dosáhl skript *vulscan*, který sice veškeré možné hrozby detekoval, ale přidal k nim několik tisíc dalších falešných detekcí, a proto jeho výsledek nemá správnou vypovídací hodnotu. Skener Nikto2 v tomto testu mohl ze své podstaty odhalit pouze běžící webovou administraci. Tento úkol zvládl a nepřidal žádná další nedůvěryhodná data.

Nástroje pro operační systém Windows nedopadly také dobře. Skener Retina si s testovaným zařízením neporadil a nedetekoval nic, co by mělo nějakou užitnou hodnotu. U ManageEngine nemohl sken proběhnout, protože testované zařízení není podporováno tvůrci skenovacího nástroje. Vítězem této části se tak stává OpenVAS, který si poradil s danou situací nejlépe.

6.3 Možnosti automatizace

Většina pokročilých nástrojů nabízí vetší nebo menší možnosti automatizace. Automatizace zjednodušuje práci při hledání zranitelností, automatizuje některé úkony, a dokonce hlídá a upozorňuje na nově nalezené hrozby. Tyto informace následně zobrazuje pomocí svého uživatelského rozhraní nebo doručí informace pomocí e-mailu.

Nástroje umí následující:

1. skenovat rozsah adres, celou síť nebo podsíť,
2. automatické periodické provádění skenů,
3. automatické vyhodnocení skenů a tvorba reportů,
4. odeslání e-mailu v případě nalezení zranitelností,
5. automatická oprava nalezených problémů.

Tabulka 20 – Porovnání možností automatizace nástrojů

Číslo vlastnosti / Použitý nástroj	1.	2.	3.	4.	5.
OpenVAS	☒	☒	☒	☒	☐
Nessus Essentials	☒	☒	☒	☒	☐
Nexpose Community	☒	☒	☒	☒	☐
Nmap (*vuln* script)	☒	☒	☐	☐	☐
Nmap (*vulscan* script)	☒	☒	☐	☐	☐
Nikto2	☒	☒	☐	☐	☐
Retina Network SS	☒	☒	☒	☒	☐
ManageEngine VMP	☒	☒	☒	☒	☒

Zdroj: vlastní

Nástroje nabízí vcelku podobné možnosti automatizace. Jediný rozdíl tvoří konzolové aplikace, které nedisponují například plánováním, protože je u nich potřeba využít nějaký další nástroj, kterým může být třeba Cron. Nevyšší stupeň automatizace ze všech nástrojů nabízí ManageEngine, který dokáže i nalezené problémy automaticky řešit v případech, kdy sám řešení zná.

6.4 Řešení nalezených zranitelností

Jednotlivé nástroje se liší způsobem, jakým informují o nalezených problémech. Obecně je možné skenery rozdělit na tři skupiny, nástroje konzolové, skenery s webovým uživatelským rozhraním a desktopové aplikace. Nástroje založené na skeneru Nmap a sada skriptů Nikto2 patří do první skupiny, Nessus, OpenVAS, Nexpose a ManageEngine spadají do kategorie, která disponuje webovým grafickým rozhraním a jediný nástroj Retina je dodáván jako klasická aplikace pro desktopové prostředí Windows. Další dělení je možné na základě popisu nalezených zranitelností.

6.4.1 Textová definice

První kategorie zprostředkuje pouze základní informace o nalezeném problému, které spočívá v jednoduchém popisu zranitelnosti, v jejím identifikačním čísle, pomocí kterého je možné dohledat podrobnosti a popřípadě odkaz, kde je možné najít další informace.

```
VULNERABLE:
Slowloris DOS attack
  State: LIKELY VULNERABLE
  IDs:  CVE:CVE-2007-6750
    Slowloris tries to keep many connections to the target web server open and hold
    them open as long as possible.  It accomplishes this by opening connections to
    the target web server and sending a partial request. By doing so, it starves
    the http server's resources causing Denial Of Service.

  Disclosure date: 2009-09-17
  References:
    http://ha.ckers.org/slowloris/
    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
```

Obrázek 27 - Textový popis zranitelnosti *vuln* skriptu

Zdroj: vlastní

6.4.2 Návod na řešení

Další skupina nástrojů umí stejné možnosti jako ta předchozí, ale navíc přidává i možnosti, jak daný problém vyřešit. Řešení je většinou popsáno textovou formou, kde je specifikováno, na kterou verzi je nutné danou aplikaci aktualizovat nebo kterou část aplikace deaktivovat, aby nebezpečí vyplývající z dané zranitelnosti pominulo. Tento způsob řešení nabízí nástroje OpenVAS, Nexpose, Nessus a Retina.

Solution

Upgrade to Apache version 2.0.63 or later. Alternatively, ensure that he affected modules are not in use.

Obrázek 28 - Návrh na řešení zranitelnosti ve skeneru Nessus

Zdroj: vlastní

6.4.3 Automatické řešení

Poslední skupinu tvoří nástroje, které po detekci zranitelnosti dokáží na dálku provést nápravná opatření. Opatření mohou být různého typu od aktualizace software, přes změnu nastavení na bezpečnější variantu až po odinstalaci daného nástroje. Z testovaných nástrojů touto funkcionalitou disponuje pouze ManageEngine, který vše zvládá pomocí svého agenta.

6.5 Jednoduchost nasazení

Nejjednodušší nasazení mají nástroje Nikto2 a skripty, které využívají Nmap. Tyto nástroje se vzdáleně nepřihlašují k cílovému stroji a není nutné pro ně dále nic konfigurovat. V případě Nikto2 stačí nástroj pouze nainstalovat a používat. Stejná situace je i u Nmapu, u které je již po instalaci dostupný skript *vuln*. *Vulscan* je nutné stáhnout zvlášť, ale tím odlišnosti od skriptu *vuln* končí.

O něco složitější je situace u ManageEngine Vulnerability Manager Plus, který je nutné nainstalovat na počítač správce a následně zajistit distribuci agentů na hlídané stroje. Agenti následně cílové stroje automaticky nakonfigurují, a proto není nutné aplikovat další nastavení.

```
$RemoteRegistry = Get-CimInstance -Class Win32_Service -ComputerName $Computer -Filter 'Name = "RemoteRegistry"' -ErrorAction Stop
    if ($RemoteRegistry.State -eq 'Running') {
        Write-Output "$Computer is already Enabled"
    }

    if ($RemoteRegistry.StartMode -eq 'Disabled') {
        Set-Service -Name RemoteRegistry -ComputerName $Computer -StartupType Manual -ErrorAction Stop
        Write-Output "$Computer : Remote Registry has been Enabled"
    }

    if ($RemoteRegistry.State -eq 'Stopped') {
        Start-Service -InputObject (Get-Service -Name RemoteRegistry -ComputerName $Computer) -ErrorAction Stop
        Write-Output "$Computer : Remote Registry has been Started"
    }
```

Obrázek 29 - Ukázka skriptu v PowerShell ke spuštění vzdálených registrů

Zdroj: vlastní

Nástroje OpenVAS, Nessus, Nexpose a Retina mají nejsložitější sled konfigurací, který zajistí jejich plnou funkčnost. Je nutné dodat, že bez těchto konfigurací je možné nástroje také provozovat, ale některé problémy nedokáží detekovat a jiné pouze s nižší spolehlivostí. Konfigurace podle kapitoly 6.1.1 je možné dále automatizovat. V případě Windows je možné napsat skript s využitím skriptovacího jazyka PowerShell nebo v případě Linuxu je možné použít Bash.

ZÁVĚR

Cílem této práce bylo provést výzkum možností, které nabízí dostupná softwarová řešení zabývající se detekcí zranitelností v počítačových sítích. Při tomto výzkumu byl především kladen důraz na kvalitu detekce zranitelností, ale i na další důležité parametry, mezi které patří například cena, možnost prezentace výsledků nebo způsoby automatizace, které nástroje nabízí.

V prvních kapitolách byly představeny důležité normy, které se zabývají bezpečností informačních systémů. Tyto normy poskytují teoretický základ pro vyhledání potencionálně zranitelných míst při používání informačních systémů. Dále k těmto zranitelným místům navrhují opatření, která minimalizují nebo zcela eliminují možnost jejich využití.

Další kapitoly práce poskytují teoretickou přípravu pro praktickou část, protože se zabývají výběrem a základním představením nástrojů, které byly následně zkoumány. Popsány byly také další prostředky, které byly použity pro prováděné testy. Před započetím praktické části bylo také nutné porovnat nástroje z hlediska omezení jejich bezplatných verzí nebo z pohledu ekonomický nákladů, které by stálo pořízení jejich neomezených verzí.

V rámci praktické části práce byly předvedené testy nástrojů na vnitřním i vnějším perimetru sítě. Testy vnitřního perimetru byly provedeny na virtuální síti, kde byla v první části uvedena její topologie, na kterou dále navázala potřebná sada kroků, které bylo nutné učinit, aby skenovací nástroje pracovaly korektně. Po provedení testů následovalo krátké shrnutí dosavadních výsledků a následně byly skenery otestovány na vnějším perimetru, který v práci představovalo zařízení MikroTik. Po těchto testech byly nástroje porovnány ještě z hlediska automatizace a prezentace výsledků.

Nástroj OpenVAS se tak stal celkovým vítězem jak na vnitřním perimetru sítě, kde se 77 % detekovaných problémů dopadl nejlépe, tak i na vnějším perimetru, kde rozdíl mezi úspěšnými a neúspěšnými nástroji byl o mnoho větší. Možnosti automatizace jsou u nástrojů velmi podobné, takže i zde skener nepropadl a v jeho reportech byl vždy uveden i popis, jak bylo možné danou zranitelnost řešit. V celkovém souhrnu nejlepší automatizaci z testovaných nástrojů nabízí nástroj ManageEngine Vulnerability Manager Plus, který ale bohužel selhal v ostatních testech a není možné ho dále doporučit.

Testované skenery byly také prověřeny v detekci zranitelností u kartografického software, který zde zastupoval kategorii programového vybavení, které má malou uživatelskou základnu. V rámci tohoto testovacího scénáře byla také nasazena populární technologie Docker, která se

těší oblibě hlavně mezi vývojáři, kteří potřebují držet několik verzí stejného programu. Docker toto umožňuje a současně řeší možné problémy se vznikem konfliktů u závislých knihoven. Výsledky poukázaly na fakt, že nástroje neumí s technologií Docker pracovat a současně použitý exotický software jim dělá také problémy. V této oblasti nejlépe exceloval nástroj Nexpose, který se v celkových výsledcích na vnitřním perimetru sítě umístil až na třetím místě.

Tato práce zcela jasně poukazuje na fakt, že stejně jako je nutné dbát na bezpečnost informačních systémů, tak je potřeba i pečlivě vybírat skener zranitelností, protože mezi nástroji jsou ohromné rozdíly, které v důsledku mohou znamenat ohrožení bezpečnosti dat. Jedná se o situace, kdy nekvalitní skener včas neupozorní na existující zranitelnosti, které následně využije útočník. Jak i z výsledků této práce vyplývá, komerční produkt není zárukou úspěšné detekce, protože v celkovém souhrnu vyhrál nástroj, který je k dispozici zcela zdarma a s otevřenými zdrojovými kódy.

7 POUŽITÁ LITERATURA

Autentizace, ověření, identifikace (Authentication). In: ManagementMania.com [online]. Wilmington (DE) 2011-2019, 13.02.2018 [cit. 02.03.2019]. Dostupné z: https://managementmania.com/cs/autentizace-identifikace.

BeyondTrust Vulnerability Management [online]. Washington, DC: BeyondTrust, 2019 [cit. 2019-06-23]. Dostupné z: https://www.beyondtrust.com/docs/vulnerability-management/index.htm.

BOUŠKA, Petr. Správné nastavení sdílení adresáře ve Windows. Samuraj-cz [online]. Praha: Samuraj, 2019, 28.05.2007 [cit. 2019-06-23]. Dostupné z: https://www.samuraj-cz.com/clanek/spravne-nastaveni-sdileni-adresare-ve-windows/.

Co je to SCADA? PROMOTIC [online]. Ostrava: Microsys, 2017 [cit. 2019-04-17]. Dostupné z: https://www.promotic.eu/cz/pmdoc/WhatIsPromotic/WhatIsScada.html.

ČSN EN ISO/IEC 27000. Čtvrté vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.

ČSN EN ISO/IEC 27033-3. První vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2015.

Intel® Core™ i7-4910MQ Processor [online]. Santa Clara: Intel, 2014 [cit. 2019-06-20]. Dostupné z: https://ark.intel.com/content/www/us/en/ark/products/78939/intel-core-i7-4910mq-processor-8m-cache-up-to-3-90-ghz.html.

ISO 27002 – nejlepší bezpečnostní praktiky. In: ManagementMania.com [online]. Wilmington (DE) 2011-2019, 24.03.2017 [cit. 02.03.2019]. Dostupné z: https://managementmania.com/cs/iso-27002-nejlepsi-bezpecnostni-praktiky.

KACZMAREK, Tom. THE TOMK CONSULTING GROUP. Virtual Private Networks (VPNs) – a key Business Enabler [online]. August 2011 [cit. 10.3.2019]. Dostupný na WWW: http://tomkconsulting.com/news019-about-VPNs.htm.

Kali: by offensive security [online]. Offensive Security, 2019 [cit. 2019-06-20]. Dostupné z: https://www.kali.org.

ManageEngine Vulnerability Manager Plus: Gain 360 degree visibility into your security exposure. [online]. Washington, DC: ManageEngine, 2019 [cit. 2019-06-23]. Dostupné z: https://www.manageengine.com/vulnerability-management/.

MARŤÁK, Pavel. Bezpečnost dat v praxi. *Systém Online* [online]. Brno: CCB, duben 2005 [cit. 2019-02-17]. Dostupné z: https://www.systemonline.cz/clanky/bezpecnost-dat-v-praxi.html.

Nmap.org [online]. Palo Alto, California: Gordon Lyon, 2018 [cit. 2019-06-23]. Dostupné z: https://nmap.org.

Nikto2. CIRT.net: Suspicion Breeds Confidence [online]. Chris Sullo, 2019 [cit. 2019-04-15]. Dostupné z: https://cirt.net/Nikto2.

OpenVAS – Open Vulnerability Assessment System [online]. Osnabrück: Greenbone Networks, 2018 [cit. 2019-05-15]. Dostupné z: http://www.openvas.org.

PRITCHETT, Willie L a David DE SMET. Kali Linux cookbook. Birmingham: Packt Publishing, 2013, 1 online resource (261 pages). ISBN 978-1-78328-959-2.

RouterBOARD 500 Series User‘s Manual: Rev. M (4-Jul-2006) [online]. Latvia: MikroTik, 2006 [cit. 2019-06-20]. Dostupné z: https://manualzz.com/doc/726414/mikrotik-routerboard-1200-user-s-manual.

SELECKÝ, Matúš. Penetrační testy a exploitace. Brno: Computer Press, 2012. ISBN 978-80-251-3752-9.

STEWART, Dennis. What Are Denial of Service and DdoS Attacks? [online]. 28. 11. 2016 [cit. 10.3.2019]. Dostupný na WWW: https://www.howtogeek.com/281707/what-are-denial-of-service-and-ddos-attacks/.

Tenable [online]. Columbia, MD, U.S.: Tenable, 2019 [cit. 2019-06-17]. Dostupné z: https://www.tenable.com.

VMware Workstation Pro Documentation [online]. Palo Alto: VMware, 2019 [cit. 2019-06-20]. Dostupné z: https://docs.vmware.com/en/VMware-Workstation-Pro/index.html.

Welcome to the Knowledge Base: Welcome to the Rapid7 Knowledge Base! [online]. Boston: Rapid7, 2019 [cit. 2019-06-23]. Dostupné z: https://kb.help.rapid7.com/docs.

Windows Server documentation: Windows Server is the platform for building an infrastructure of connected applications, networks, and web services, from the workgroup to the data cente [online]. Redmond: Microsoft, 2019 [cit. 2019-06-20]. Dostupné z: https://docs.microsoft.com/cs-cz/windows-server/.

8 PŘÍLOHY

Příloha A – *Konfigurace cílového virtuálního počítače s Windows XP*

Hardwarová konfigurace virtuálního počítače:

- 2 jádra procesoru
- 2048 MB RAM
- 40 GB diskového prostoru
- Akcelerovaná 3D grafika s 256 MB grafické paměti
- Režim sítě nastaven na NAT

Softwarové vybavení virtuálního počítače:

- Windows XP Professional s aktualizací Service Pack 3, 32-bit edice
- Microsoft Office XP Professional
- Vmware Tools for Windows 10.0.12
- Adobe Reader 11.0.1
- Mozilla Firefox 3.6.28
- Google Chrome 10.0
- Java 6 Standard Edition update 21
- Adobe Flash Player 11.2
- Avast Antivirus 4.8
- WinRAR 4.20
- Oracle VirtualBox 4.2.6
- VLC 2.0.4

Příloha B – *Konfigurace cílového virtuálního počítače s Windows 7*

Hardwarová konfigurace virtuálního počítače:

- 2 jádra procesoru
- 4096 MB RAM
- 60 GB diskového prostoru
- Akcelerovaná 3D grafika s 256 MB grafické paměti
- Režim sítě nastaven na NAT

Softwarové vybavení virtuálního počítače:

- Windows 7 Professional s aktualizací Service Pack 1, 32-bit edice
- Microsoft Office 2010 Professional s aktualizací Service Pack 1
- Vmware Tools for Windows 10.2.5
- Adobe Reader 11.0.21
- Mozilla Firefox 42
- Google Chrome 43.0
- Java 7 Standard Edition update 40
- Avast Antivirus 11.2.2729
- WinRAR 5.01
- Oracle VirtualBox 5.1.12
- VLC 2.2.3

Příloha C – *Konfigurace cílového virtuálního počítače s Windows 10*

Hardwarová konfigurace virtuálního počítače:

- 2 jádra procesoru
- 4096 MB RAM
- 60 GB diskového prostoru
- Akcelerovaná 3D grafika s 512 MB grafické paměti
- Režim sítě nastaven na NAT

Softwarové vybavení virtuálního počítače:

- Windows 10 Professional, verze 1903, 64-bit edice
- LibreOffice 6.1.1
- Vmware Tools for Windows 10.2.5
- Adobe Acrobat Reader DC 2019
- Mozilla Firefox 65.0
- Google Chrome 75.0
- Java 11.0.3 Standard Edition
- Avast Antivirus 19.5.4444
- WinRAR 5.60
- Oracle VirtualBox 6.0.0
- VLC 3.0.5
- Thunderbird 59.0b1

Příloha D – *Konfigurace cílového virtuálního počítače s Windows Server 2008*

Hardwarová konfigurace virtuálního počítače:

- 2 jádra procesoru
- 4096 MB RAM
- 40 GB diskového prostoru
- Akcelerovaná 3D grafika s 256 MB grafické paměti
- Režim sítě nastaven na NAT

Softwarové vybavení virtuálního počítače:

- Windows Server 2008 Standard s aktualizací Service Pack 2, 32-bit edice
- VMware Tools for Windows 10.2.5
- Apache 2.0.55
- Mozilla Firefox 3.6.28
- phpMyAdmin 2.11.6
- MediaWiki 1.18.0
- Wordpress 4.0.6
- MySQL 5.0.67
- PHP 5.2.6
- WinRAR 5.61

Příloha E – *Konfigurace cílového virtuálního počítače s Debian 9.9*

Hardwarová konfigurace virtuálního počítače:

- 2 jádra procesoru
- 4096 MB RAM
- 60 GB diskového prostoru
- Akcelerovaná 3D grafika s 256 MB grafické paměti
- Režim sítě nastaven na NAT

Softwarové vybavení virtuálního počítače:

- Debian 9.9, Kernel 4.9.0, 64-bit edice
- Open-vm-tools 2.10.1.5
- Apache 2.4.25
- Mozilla Firefox 60.7 ESR
- Libapache2-mod-mapcache 1.4.1
- PostgreSQL 9.6
- Docker-ce 18.09
- Docker image „database“
    - PostgreSQL 11.3
    - PostGIS 2.5
- Docker image „apache“
    - Apache 2.4.18
- Docker image „mapserver“
    - Apache 2.4.18
    - Mapserver 7.0.7
    - Libapache2-mod-fastcgi 2.4.7
- Docker image „terrain server“
    - Nginx 1.10.3

Veškeré Docker image jsou postavené na základu Ubuntu verze Xenial Xerus, balíčky jsou požité verze z repositářů dané verze Ubuntu.

Příloha F – *Konfigurace testujícího virtuálního počítače s Kali Linux*

Hardwarová konfigurace virtuálního počítače:

- 8 jádra procesoru
- 8192 MB RAM
- 40 GB diskového prostoru
- Akcelerovaná 3D grafika s 768 MB grafické paměti
- Režim sítě nastaven na NAT

Softwarové vybavení virtuálního počítače:

- Kali Linux 2019.1a, 64-bit edice
- Open-vm-tools 2.10.1.5
- OpenVAS 9.0.3
- Mozilla Firefox 60.5.1 ESR
- Nessus Essentials 8.4
- Nexpose Community Edition 6.5.68
- Nmap 7.70
- Nikto2 2.1.6

Příloha G – *Konfigurace testujícího virtuálního počítače s Windows Server 2016*

Hardwarová konfigurace virtuálního počítače:

- 4 jádra procesoru
- 8192 MB RAM
- 60 GB diskového prostoru
- Akcelerovaná 3D grafika s 256 MB grafické paměti
- Režim sítě nastaven na NAT

Softwarové vybavení virtuálního počítače:

- Windows Server 2016 Standard, 64-bit edice
- VMware Tools for Windows 10.2.5
- Microsoft Baseline Security Analyzer 2.3
- Mozilla Firefox 67.0.4
- Google Chrome 75.0
- BeyondTrust (Retina) Network Security Scanner 6.6.1
- ManageEngine Vulnerability Manager Plus 10.0.335