Univerzita Pardubice
Fakulta ekonomicko-správní

Návrh zabezpečení počítačové sítě a služeb operačního systému

Diplomová práce

2019 Bc. Jiří Helvich

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2018/2019

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Jiří Helvich**
Osobní číslo:	**E160046**
Studijní program:	**N6209 Systémové inženýrství a informatika**
Studijní obor:	**Informatika ve veřejné správě**
Téma práce:	**Návrh zabezpečení počítačové sítě a služeb operačního systému**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je návrh a implementace zabezpečení počítačové sítě a a služeb operačního systému ve firemním prostředí

Práce bude obsahovat:

- vymezení vybraných základních pojmů v návaznosti na již řešenou bakalářskou práci;
- popis a analýzu situace;
- návrh řešení;
- implementaci řešení.

Rozsah pracovní zprávy: **cca 50 stran**
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

BIGELOW, Stephen J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. Brno: Computer Press, 2004. ISBN 80-251-0178-9.
DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. ISBN 80-251-0106-1.
BRUCKNER, Tomáš. Tvorba informačních systémů: principy, metodiky, architektury. Praha: Grada, 2012. Management v informační společnosti. ISBN 978-80-247-4153-6.
SCAMBRAY, Joel, George KURTZ a Stuart MCCLURE. Hacking bez tajemství. 2. aktualiz. vyd. Praha: Computer Press, 2002. Komunikace a sítě. ISBN 80-7226-644-6.
SPORTACK, Mark A. Směrování v sítích IP: [autorizovaný výukový průvodce : samostudium : kompletní zdroj informací o směrování a protokolech v sítích IP]. Brno: Computer Press, 2004, xvi, 351 s. Cisco systems. ISBN 80-251-0127-4.
TVRDÍKOVÁ, Milena. Aplikace moderních informačních technologií v řízení firmy: nástroje ke zvyšování kvality informačních systémů. 1. vyd. Praha: Grada, 2008. Management v informační společnosti. ISBN 978-80-247-2728-8.

Vedoucí diplomové práce: **doc. Ing. Jiří Křupka, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání diplomové práce: **3. září 2018**
Termín odevzdání diplomové práce: **30. dubna 2019**

L.S.

doc. Ing. Romana Provazníková, Ph.D.
děkanka

doc. Ing. Pavel Petr, Ph.D.
vedoucí ústavu

V Pardubicích dne 3. září 2018

Prohlašuji:

Tuto práci jsem 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., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, 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.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 26. 11. 2019

Bc. Jiří Helvich

PODĚKOVÁNÍ

Touto cestou bych rád poděkoval vedoucímu práce doc. Ing. Jiřímu Křupkovi, PhD. za jeho odbornou pomoc a cenná doporučení, která mi pomohla při zpracování mé diplomové práce.

ANOTACE

Tato diplomová práce se zabývá návrhem a implementací zabezpečené počítačové sítě a služeb operačního systému ve firemním prostředí. Návrh řešení je vytvořen pro účely malé až střední firmy. V práci je provedena analýza současného stavu firmy s cílem navrhnout bezpečné prostředí pro provoz počítačové sítě a informačního systému. V textu jsou popsány druhy, životní cykly a metodiky vývojů informačních systémů. Práce obsahuje popis bezpečnostní a provozní dokumentace, včetně právních a technických norem.

KLÍČOVÁ SLOVA

Bezpečnost, LAN, operační systém, router, server, vývoj IS

TITLE

Proposal of Computer Network Security and Operating System Services

ANNOTATION

This thesis deals with the design and implementation of a secured computer network and the services of an operating system in a company environment. The design proposal is intended to be used for small or medium companies. The analysis of the current state of the company was carried out in order to design a safe working environment for the computer network and the information system. The different types, life cycles and methodologies of the systems development are mentioned in the thesis. The description of safety and process documentation, legal and technical standards are delineated here as well.

KEYWORDS

Security, LAN, operating system, router, server, IS development

OBSAH

SEZNAM TABULEK

SEZNAM ILUSTRACÍ

SEZNAM ZKRATEK A ZNAČEK

ACID	Atomicity Consistency Isolation Durability
ACL	Access Control List
AD	Active Directory
AES	Advanced Encryption Standard
APS	Advanced Planing and Scheduling
APT	Advanced Packaging Tool
ASD	Adaptive Software Development
CAD	Computer Aided Design
CAM	Computer Aided Manufacture
CAP	Computer Aided Planning
CAQ	Computer Aided Quality
CCM	Counter Mode with Cipher Block Chaining and Message Authentication Code Protocol
CIS	Communication Information Systems
CIS	Customer Information System
CRM	Customer Relation Management
CVE	Common Vulnerabilities and Exposures
DHCP	Dynamic Host Configuration Protokol
DNS	Domain Name System
DSDM	Dynamic Systems Development Method
eCryptfs	Enterprise Cryptograhic Filesystem
EDI	Electronic Data Interchange
EIS	Executive Information System
EUP	Enterprise Unified Process
FDD	Feature Driven Development
FDQN	Fully qualified domain name
GIS	Geographical Information System
GPM	Group Policy Management
GPO	Group Policy
GUI	Graphical User Interface
HW	Hardware
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technologies
IKT	Informační a komunikační technologie
IT	Informační technologie
LAN	Local Area Network
LGPO	Microsoft Local Group Policy Object Utility
MAC	Media Access Control
MIS	Management Information System
MMDIS	Multidimensional Management and Development of Information System
MSF	Microsoft Solutions Framework
MTZ	Materiálně Technické Zabezpečení
NAP	Network Policy Server
NAT	Network Address Translation
OIS	Office Information System
OOSPICE	Software Process Improvement and Cabability Determination for Object Oriented/Component Based Software Development

OPEN	Object–oriented Process Environment and Notation
PAM	Práce a Mzdy
PARTS	Precision Accuracy Relevance Tolerance Scale
PING	Packet InterNet Groper
PPC	Production Planing and Control
PSK	Pre-shared key
RAD	Rapid Application Development
RFC	Request for Comments
RSAT	Remote Server Administration Tools
RUP	Rational Unified Process
SCM	Security Compliance Manager
SCM	Suply Chain Management
SDM	System Development Method
SMART	Specific Measurable Achievable Realistic Time-bound
SPA	Software Process Assesment
SSH	Secure Shell
SSL	Secure Sockets Layer
SW	Software
TLS	Transport Layer Security
UFW	Uncomplicated Firewall
VM	Virtual Machine
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access

ÚVOD

V současnosti skoro každá firma disponuje prostředky výpočetní techniky. Většina těchto zařízení v podobě počítačů, mobilních telefonů apod. je připojená k celosvětové datové síti internet. Nepostradatelnou potřebou ve firemní sféře je zajištění informační podpory firemním procesům. Informace jsou převážně sdíleny v elektronické podobě. Zde nastává problém, který je základem této práce, jak tyto procesy, informace a prostředky pro zpracování těchto informací chránit proti kybernetickým útokům a zneužití. V případě malého počtu klientských zařízení je možné každé zařízení nastavit a chránit samostatně. Avšak firmy disponují větším a různorodým počtem zařízení, které můžeme chránit začleněním do zabezpečeného informačního systému. Informační systém jako celek zahrnuje data, lidi, software a hardware, z čehož nám vyplývá, co všechno je nutné v informačním systému řídit. Výhodou informačního systému je jednoduché a spolehlivé nastavení sdílení informací podle pravidla „need to know".

Tato práce navazuje na bakalářskou práci „*Bezpečnost informačních systémů v prostředí počítačových sítí*" (výchozí práce), která se zabývá architekturou sítí, bezpečností sítí a ochranou dat. Výchozí práce popisuje historii, architektury sítí, bezpečnost sítí a ochranu dat. Navržená ukázka řešení pro Windows Server 2008 je zaměřena na instalaci OS (operační systém), funkcí NAP (Network Policy Server), BitLocker Drive Encryption, AD (Active Directory) a GPO (Group Policy) a je jednou z mnoha možností, jak informační systém chránit prostřednictvím služeb MS Windows. Obsah této práce navazuje na vybrané kapitoly výchozí práce, které rozebírá podrobněji.

Hlavním tématem této práce je popsat a vysvětlit principy při navrhování zabezpečené počítačové sítě, služeb operačního systému včetně jejich implementace. Je koncipována jako možná pomůcka pro majitele firem, architekty IS a administrátory malých sítí a informačních systémů. Dále obsahuje vymezení základních pojmů z oblasti operačních systémů, informačních systémů, bezpečnostní a provozní dokumentace, ale také ukázku možného nastavení HW (hardware) a OS jako základu funkčního a zabezpečeného informačního systému. Jak již bylo napsáno ve výchozí práci, bezpečnost v oblasti ICT a CIS je v dnešní době kybernetických a teroristických útoků velmi aktuální téma. Jedná se zejména o ochranu HW a informací. Bezpečnost je jedním z hlavních klíčových požadavků na nově vznikající a vyvíjející se sítě a operační systémy, přičemž existuje značný nedostatek snadno implementovatelných metod a strategií zabezpečení [15].

Použité postupy a návrhy, které jsou uvedeny v této práci, vycházejí z norem, odborné literatury, standardů, zkušeností a již provozovaných ICT a CIS (Information and Communication Technologies / Communication Information Systems).

Ve sféře malých firem se setkáváme s častou absencí ochranných prvků sítí a informací. Z převážné části je příčinou tohoto stavu finanční stránka nabízených řešení, přičemž málokterá firma má povědomí o možnosti bezplatného řešení dané problematiky, jež v této práci tvoří základ ukázky nastavení serverového operačního systému.

Motto:

Každý řetěz je silný jen tak, jak je silný jeho nejslabší článek.

Arthur Conan Doyle

1 CÍL PRÁCE

Cílem práce je popsat a vysvětlit doporučené principy při navrhování zabezpečené počítačové sítě a operačního systému ve firemním prostředí. Text lze využít jako možnou pomůcku při tvorbě nového informačního systému nebo jeho upgrade, a to zejména v oblasti tvorby požadavků na IS, projektu, financí, tvorby dokumentace a nastavení.

Rámec celé práce nepřesahuje základní požadavky pro malou až střední firmu. Podle Agentury pro podporu podnikání a investic malý až střední podnik zaměstnává méně než 50 osob a roční obrat nepřesahuje 10 miliónů EUR [2]. Nicméně použité algoritmy nastavení operačního systému mohou být aplikovány i v instituci, která čítá cca 350 aktivních uživatelů systému.

Doporučené metody uvádějí různé literární zdroje. Většinou jsou zaměřeny jen na dílčí část řešeného problému. Postupy uvedené v internetových zdrojích jsou někdy neúplné, nefunkční, nebo dokonce snižují bezpečnost. Shrneme je a otestujeme na vytvořeném modelu v laboratorních podmínkách.

Z finančního hlediska práce nabízí velice levné řešení vzhledem k hardwaru a softwaru. V oblasti návrhu a vývoje informačního systému bude cena závislá na volbě dodavatele informačního systému. Informační systém je možné navrhnout a implementovat svépomocí, nebo outsourcingem.

Následující text je rozdělen do několika logických částí, které na sebe navazují. Vynechání některých z těchto kroků může mít za následek sníženou úroveň bezpečnosti nebo funkčnosti systému. Vybrané části jsou popsány jednodušší formou s odkazy na literaturu, která tuto problematiku řeší.

2 VYMEZENÍ ZÁKLADNÍCH POJMŮ

V této kapitole vymezíme některé pojmy z oblasti operačních a informačních systémů.

Informace

Pojem informace má značně široký význam. V oblasti IT se jedná o data, která jsou interpretována díky znalosti člověka. Co je informace pro jednoho člověka, nemusí být informace pro druhého, přičemž kvalitní informace snižuje naši neznalost nebo nejistotu. Informací rozumíme relevantní údaje, které mají hodnotu pro osobu se znalostí a můžou být časově omezené. Kvalita informace může být ovlivněna komunikačním kanálem, kterým je šířena. Může být pozměněna úmyslným nebo neúmyslným zásahem, a tak se z ní může stát dezinformace. Relevantní informace jsou klíčovým faktorem pro úspěšné řízení firmy a tyto informace jsou někdy nazývány jako informační aktiva. [50], [21]

Systém

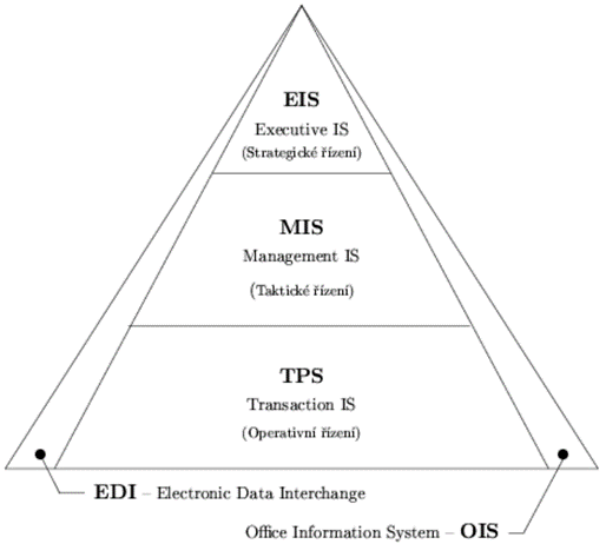
Pojem systém je stejně jako informace velice starého původu. Ve starověku znamenal systém sjednocení nebo celek. V současnosti je chápán jako množina prvků, která má vazby mezi sebou a má vztah ke svému okolí. Systém můžeme označit jako část reálného života, která má charakteristické vlastnosti. Systém je tvořen prvky, vazbami, okolím a strukturou. [50], [25]

Informační systém

Informační systém spadá do oblasti umělých systémů, přičemž kvalita systému je ovlivňována člověkem a technologiemi. V oblasti organizací existuje tzv. byznys systém, jehož neoddělitelnou součástí je právě informační systém. Jeho základní struktura obsahuje technické, programové a organizační prostředky, lidskou složku a reálný svět. Všechny tyto složky ovlivňují kvalitu IS. Základními stavebními kameny informačních systémů jsou informační a komunikační technologie, které nám zprostředkovávají přenos, zpracování, ukládání a sdílení dat. [50], [6]

2.1 Informační systémy z hlediska řízení

Informační systémy dělíme podle úrovně řízení na strategické, taktické a operativní. Pro tyto stupně jsou definovány informační systémy EIS, MIS a TPS (viz obrázek 1).



Obrázek 1: Rozdělení IS podle úrovně řízení

Zdroj: [10]

TPS (Transaction Processing System)

Tyto transakční systémy jsou určeny pro podporu hlavních činností na operativní manažerské úrovni. Výstupy ze systémů bývají v podobě denních přehledů a zpráv. U jednotlivých organizací se liší podle charakteru podniku a objemu výroby. Účelem systému je mechanizace úloh na operativní úrovni, jako jsou agendy, evidence, účetní systémy, skladové systémy apod. Transakce systému můžeme definovat jako ACID vlastnosti (Atomicity – nedělitelnost, Consistency – konzistence, Isolation – izolovanost, Durability – trvanlivost potvrzených transakcí). Konzistencí jsou myšlena pouze ověřená data. Izolovaností rozumíme viditelnost dat pouze po potvrzení. [10], [6], [50]

Transakční systémy mohou obsahovat podle charakteru podniku následující komponenty:

- CAD (Computer Aided Design) – automatizované návrhy výrobků,
- CAM (Computer Aided Manufacture) – automatizace podpory řízení výrobních procesů,
- CAP (Computer Aided Planning) – automatizace plánování technologické přípravy,
- CAQ (Computer Aided Quality) – kontrola procesu výroby a kvality produkce,
- CIS (Customer Information System) – evidence zákazníků,
- GIS (Geographical Information System) – práce s prostorovými daty a jejich geografickými údaji,
- PPC (Production Planing and Control) – kapacitní plánování a operativní řízení výroby. [10], [6]

MIS (Management Information System)

Informační systémy managementu se zabývají podporou činností na taktické úrovni, která obsahuje organizační, ekonomické a obchodní oblasti. Struktura systému je standardizovaná a může být podobná u organizací s různým charakterem podniku a objemem výroby. MIS systémy často čerpají informace z transakčních systémů TPS. [10], [6], [50]

MIS systémy mohou obsahovat podle charakteru podniku následující komponenty:

- SCM/APS (Suply Chain Management / Advanced Planing and Scheduling) – řízení vztahů s dodavateli,
- CRM (Customer Relation Management) – řízení vztahů se zákazníky,
- MTZ (Materiálně Technické Zabezpečení) – sklady a doprava,
- PAM (Práce a Mzdy) – finanční řízení. [6]

EIS (Executive Information System)

Na nejvyšší, strategické, úrovni v pyramidě řízení jsou systémy EIS. Slouží pro vrcholové vedení organizace a pracují s informacemi, které charakterizují fungování organizace jako celku. Strukturovaná a agregovaná data, která jsou vstupem do systému, většinou vycházejí z nižších TPS a MIS. Jedná se o data, pocházející z širšího časového úseku. Systém je nastaven i pro získávání dat z externích zdrojů. Typickou vlastností dat je multidimenzionalita, umožňující rychlé vytváření dat a jejich analýzu z hlediska souvislostí, zákonitostí a indikací odchylek. Systém používá také prostředky BI (Business Intelligence), DSS (Decilion Support System) a ESS (Expert Support System). DSS systémy slouží pro podporu rozhodování a ESS systémy imitují spolupráci s expertem a spadají do kategorie umělé inteligence. Oba systémy mohou využívat bázi znalostí. [10], [50]

OIS (Office Information System)

Podsystém OIS obsahuje standardní kancelářské a komunikační prostředky pro podporu kancelářských procesů na všech úrovních řízení. V rámci tohoto podsystému můžeme vytvářet a distribuovat dokumenty, plánovat pomocí kalendářů, sledovat úkoly, přijímat a odesílat elektronickou poštu, vytvářet webové stránky, archivovat dokumenty, provozovat videokonference a intranet. Součástí OIS může být i workflow služba, která řídí tok dokumentů a procesů organizací. [10], [6]

EDI (Electronic Data Interchange)

Podsystém EDI slouží pro standardizovanou výměnu formulářů v elektronické podobě s okolím organizace. [10], [37]

2.2 Informační systémy z hlediska životního cyklu

Životní cyklus systému udává strukturovaný postup od stanovení koncepce až po vyřazení nebo upgrade systému. Cyklus obsahuje jednotlivé etapy, které musí být definovány v projektu IS. Jednotlivé etapy mají daný obsah a čas. Součástí etap (fází) jsou činnosti a úkoly, které mají definované i odpovědnosti projektového týmu. Životní cyklus je většinou řešen v rámci projektového managementu. Projekt musí obsahovat odpovědi na základní otázky „*Proč? Co? Kdo? Kdy?*“ a cíle projektu by měly být v souladu s přístupem SMART (Specific – konkrétní, Measurable – měřitelný, Achievable – dosažitelný, Realistic – realistický, Time-bound – ohraničený v čase). [6], [35]

Jednotlivé etapy projektu se mohou lišit podle použité metodiky a požadavku na projekt. Metodika MMDIS (Multidimensional Management and Development of Information Systems) obsahuje etapy pro vývoj IS a metodika ASAP pro implementaci typového IS, viz tabulka 1. V projektu nesmíme zapomenout na pořízení majetku ICT. [6]

Tabulka 1: Členění etap projektu

VP: Výběr IS/ICT	VP: Vývoj IS	VP: Implementace typového IS
Definování cílů a kritérií výběrového řízení	Úvodní studie	Příprava projektu
Poptávkové řízení	Globální analýza a návrh	Cílový koncept
Vyhodnocení nabídek	Detailní analýza a návrh	Realizace
	Implementace	Příprava produktivního provozu
	Zavedení do provozu	Zahájení produktivního provozu

Zdroj: upraveno podle [6]

Výše uvedené etapy můžeme podle potřeby rozšířit o provoz a vyřazení, viz následující odrážky:

- úvodní studie,
- globální analýza a návrh,
- detailní analýza a návrh,
- vývoj IS a testování (Implementace),
- zavedení do provozu,
- provoz a údržba,
- vyřazení IS. [6], [10]

Úvodní studie (UST)

Cílem úvodní studie je analyzovat situaci organizace vzhledem k finanční stránce a rentabilitě projektu. Výsledkem analýzy by měl být poznatek, zda a za jakých podmínek projekt realizovat. Mezi činnosti úvodní studie patří například definice obchodních cílů, popis cílového stavu, definice uživatelských aplikací, návrh koncepcí řešení aplikací, nasazení aplikací do aplikační architektury IS, popis aktuálního stavu IS, odhad zdrojů, organizace projektu, přínosy, rozpočet, rizika a harmonogram projektu. [10], [6]

Globální analýza a návrh (GAN)

Cílem globální analýzy je vytvoření globální architektury IS včetně koncepce celého projektu, v souladu s formulací požadavků na kvalitu a bezpečnost aplikací na konceptuální úrovni. Konceptuální úroveň řeší obsah a podstatu aplikace v obchodním pojetí. Dále navrhuje technické a programové prostředky včetně technologické architektury. Mezi nejdůležitější činnosti patří například obchodní analýza, specifikace požadavků, návrh změn procesů a logických vazeb, specifikace rozhraní vzhledem k ostatním IS a definice provozního prostředí. [10], [6]

Detailní analýza a návrh (DAN)

Tato fáze se zabývá konkrétním řešením informačního systému. V průběhu detailní analýzy a návrhu dochází, za použití vhodných transformací, k přeměně konceptuální úrovně do technologické. Mezi nejdůležitější činnosti patří například návrh testování, návrh migrací dat, návrh potřebné technologické infrastruktury, návrh práv uživatelů a rozhraní pro další aplikace. [10], [6]

Vývoj IS a testování (implementace IMP)

V rámci fáze vývoje a testování vytváříme fyzický model systému, který testujeme před nasazením. Informační systém transformujeme z technologické úrovně do implementační. V této fázi dochází ke kompletaci dokumentace, která vznikala v průběhu předchozích fází. Během této etapy by se měly objevit nedostatky z fáze analýzy, podle závažnosti od dílčích problémů až po neschopnost dokončení projektu. Mezi nejdůležitější činnosti patří například vytvoření a aktualizace dokumentace, vytvoření provozního prostředí a databází, nastavení přístupových práv, funkční, zátěžové a integrační testování včetně oprav chyb. [10], [6]

Zavedení do provozu (ZAV)

V této poslední fázi vývoje a zavedení je prováděna instalace, popřípadě úprava stávající technologické infrastruktury, instalace programového vybavení, migrace dat do nové struktury,

proškolení uživatelů a administrátorů a zkušební provoz s cílem odhalit nedostatky, které jsou v průběhu provozu odstraňovány. Mezi nejdůležitější činnosti patří například instalace technologické infrastruktury a aplikací v provozním prostředí, vytváření zpráv ze zkušebního provozu, provádění akceptačních testů a vytváření předávacích protokolů. [6], [41]

Provoz a údržba (PUR)

Jedná se o konečnou a nejdelší fázi životního cyklu IS. V této fázi je systém provozován se snahou dosáhnout definovaných cílů v části návrhu. V průběhu provozu je prováděna údržba jak fyzické infrastruktury, tak aplikací podle nových požadavků a měnících se norem. Každý výpadek IS může mít negativní dopad na výkonnost podniku. Mezi nejdůležitější činnosti patří například informace poskytované aplikacemi, záloha dat a aplikací, hodnocení nákladů a přínosů, požadavky na změny, aplikované změny a výsledky měření plnění dlouhodobých SLA (Service Level Agreement), které definují měřitelnou úroveň poskytovaných služeb. [6], [41]

Vyřazení IS (VYR)

Vyřazením se rozumí odebrání aplikace nebo IS z provozu. Aplikace a systémy jsou vyřazovány, když už provoz není efektivní a je nerentabilní. Mezi nejdůležitější činnosti patří archivace dat, vyřazení komponent aplikací, změna rozhraní aplikací, změna procesů a zodpovědností. Vyřazení je často spojené s nasazením nového IS. [6], [37]

2.2.1 Modely životního cyklu

Modely životního cyklu udávají časový úsek od zámyslu až po vyřazení IS. Jednotlivé fáze jsou řešeny lineárně, ale mohou se i překrývat. V rámci projektu je možné využít pouze jeden životní cyklus nebo kombinaci více cyklů. Tato kapitola obsahuje popis nejpoužívanějších modelů. [6], [37]

Vodopádový model (SDM – System Development Method)

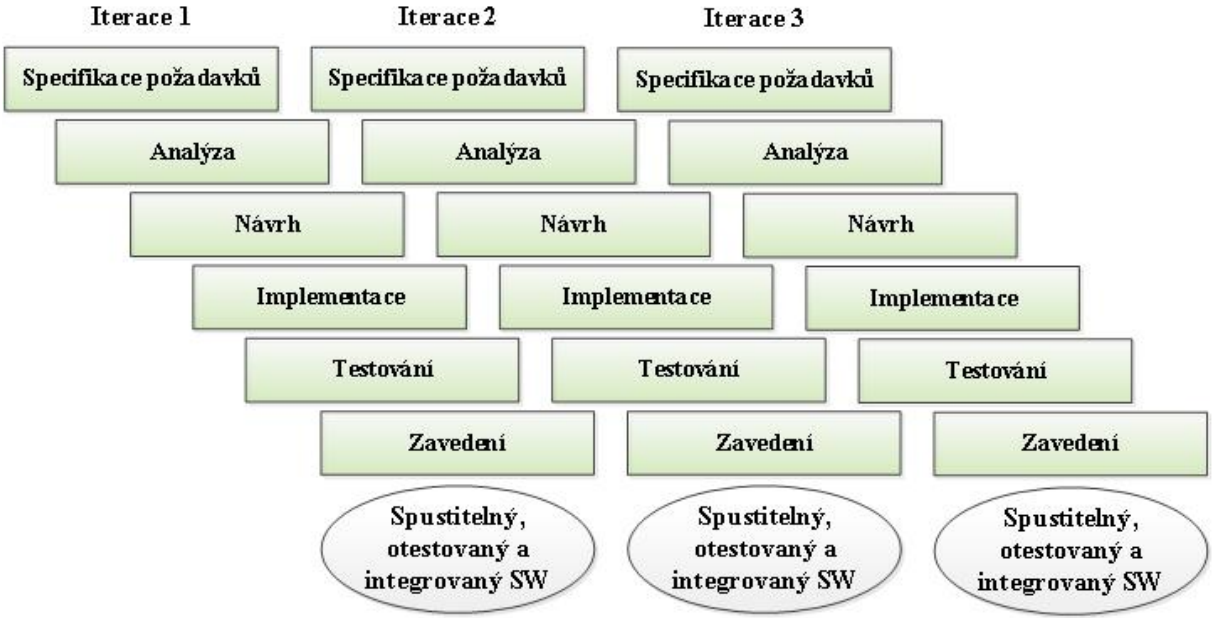
Tento model se rozšířil v 70. a 80. letech minulého století jako řešení požadavku na zavedení jednotného řádu do vývoje IS. Jednotlivé fáze modelu jsou odděleny a navazují na sebe vždy po ukončení předchozí. Sled fází je logicky seřazen podle projektu. Výhodou modelu je jednoduchost a nevýhodou je zapojení zadavatele do procesu na začátku a na konci projektu. Další nevýhodou je, že chyby v předchozích fázích, popřípadě změny v projektu se obtížně odstraňují a realizují. Možné pojetí vodopádového modelu je vyobrazeno na následujícím obrázku. [6], [37], [46]

Obrázek 2: Vodopádový model

Zdroj: upraveno podle [37]

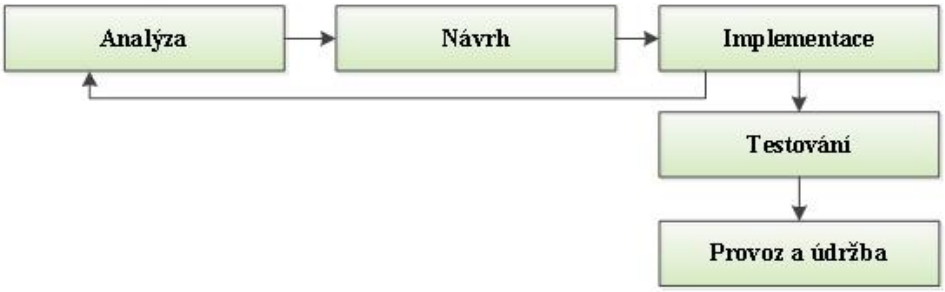
Iterativní vývoj

Model iterativního vývoje vznikl jako reakce na nevýhody vodopádového modelu, které odstraňuje. Zadavatel se aktivně podílí na projektu a má spoluodpovědnost na rozsahu řešených funkcí a plnění požadavků z úvodní studie. Model je sestaven z menších (dílčích) projektů, přičemž každá iterace obsahuje všechny fáze vývoje (viz obrázek 3). Dalším možným pojetím iteračního modelu je, že výsledkem každé iterace je funkční část systému, která končí dodávkou dílčí části systému. Výhodou modelu je dobrá informovanost zadavatele o průběhu projektu. [6], [46]



Obrázek 3: Iterativní vývoj

Zdroj: upraveno podle [6]

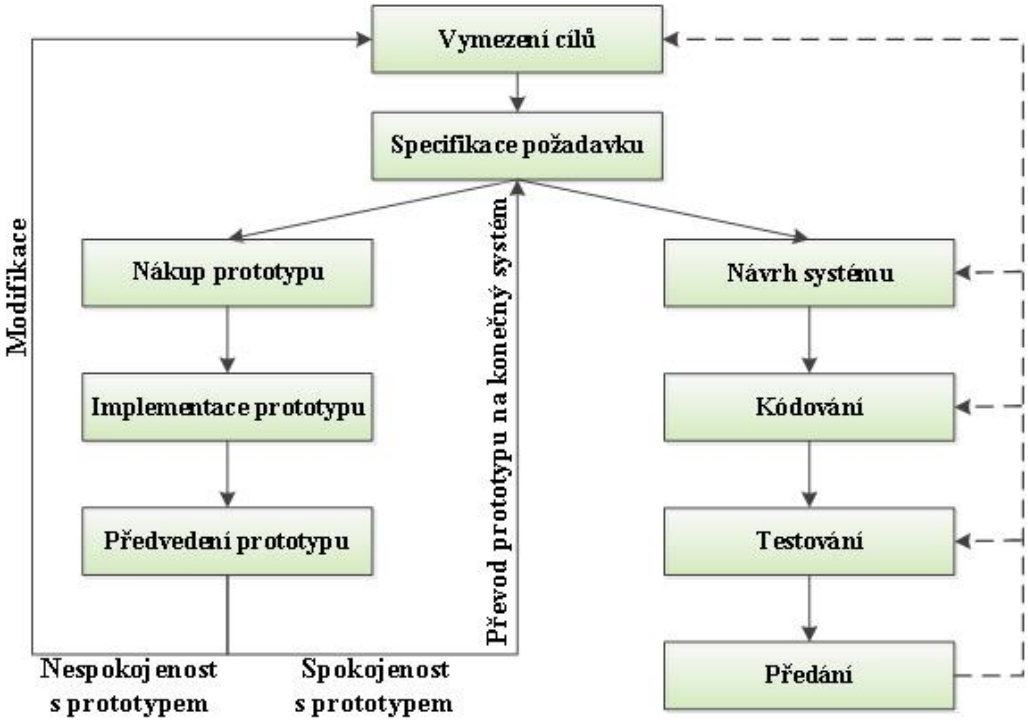


Obrázek 4: Iterativní model

Zdroj: upraveno podle [37]

Prototypový model

Model pochází z 80. let minulého století a jeho cílem je zrychlení tvorby IS při řešení pouze určité části z celkového systému. Jedná se o prototyp dílčí části systému, jako jsou například formuláře, které jsou vytvořeny pouze na úrovni zobrazení při absenci možnosti ukládání do systému. Prototypování je často kombinováno s metodou výzkumník. Prototyp lze chápat jako zjednodušenou implementaci celého systému nebo jako plnou implementaci části systému v co nejkratším časovém úseku. Jeho výhodou je přesnost dosažení požadavků od zadavatele a nevýhodou náročnost u rozsáhlých systémů. [37], [46]

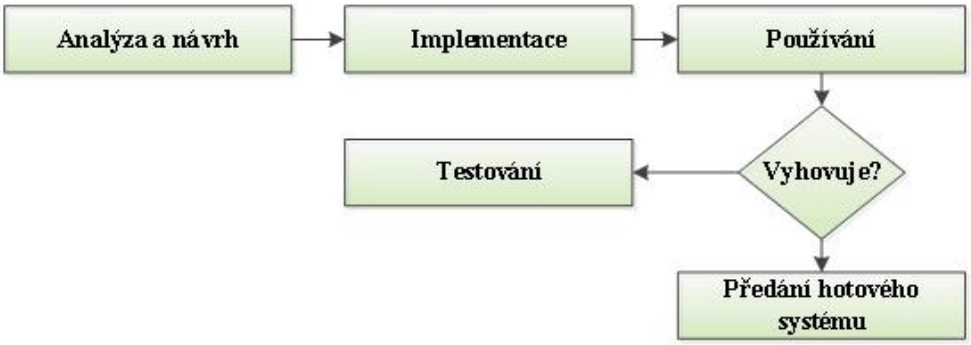


Obrázek 5: Prototypový model

Zdroj: upraveno podle [46]

Model výzkumník

Tento model povoluje zasahovat do dříve provedených fází a v nich provádět změny. Předání je realizováno poté, co zadavatel schválí všechny změny. Při změnách nejsou prováděny všechny následující fáze. Mezi hlavní nedostatky patří obtížnost odhadnout časové a finanční náklady na projekt a problematická tvorba dokumentace, která se musí v průběhu realizace měnit. Model výzkumníka je vyobrazen na následujícím obrázku. [37]

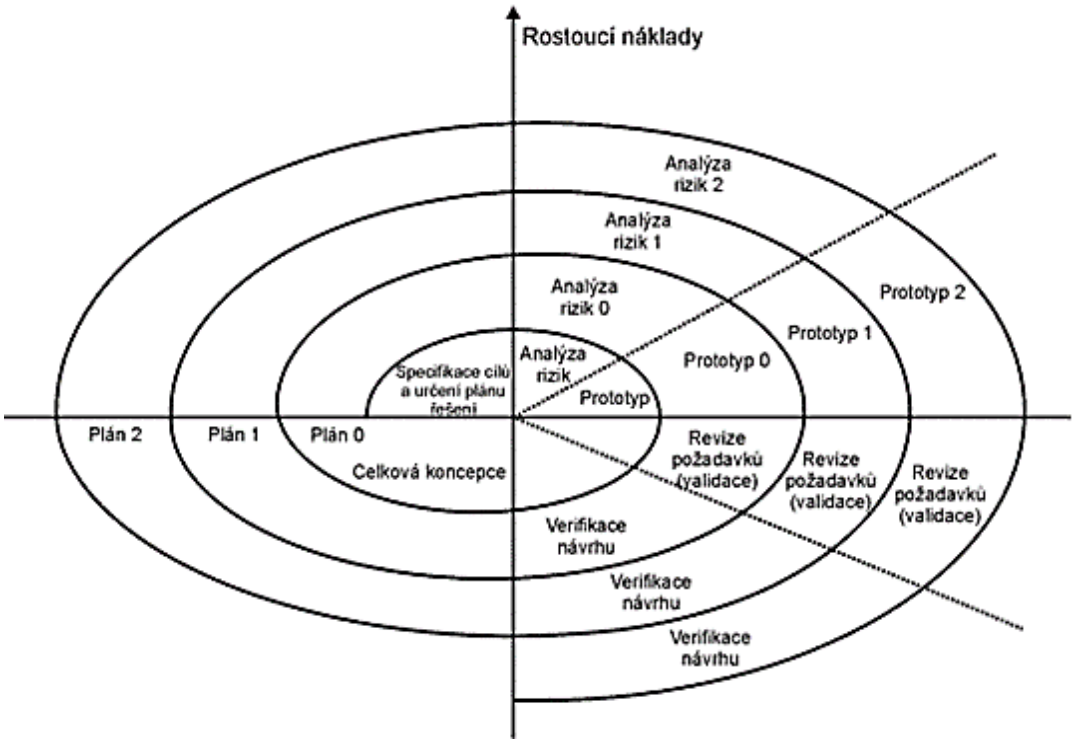


Obrázek 6: Model výzkumník

Zdroj: upraveno podle [37]

Spirálový model

Model pochází z 80. let minulého století a zavádí iterativní přístup a opakovanou analýzu rizik. Metoda vychází z teorie, že na začátku projektu je nemožné odhadnout všechny funkce. Princip spočívá ve stanovení obecného rámce projektu a po vývoji části systému včetně konzultace se zadavatelem se pokračuje dále. Celý vývoj probíhá ve spirále s postupnými iteracemi a jednotlivé iterace jsou shodné s původním vodopádovým modelem. Mezi hlavní výhody patří analýza rizik a předcházení chybám, schopnost modifikovat projekt na základě požadavků zadavatele a vhodnost pro složité systémy. Nevýhodou je požadavek na neustálou spolupráci se zadavatelem, celková komplikovanost, nemožnost naplánovat čas a finance na začátku projektu, provedení bezchybné analýzy rizik z důvodu navazujících fází, požadavek na zkušené programátory, kontroly výstupů a produkt je uvolněn až po ukončení posledního cyklu. [10], [46]



Obrázek 7: Spirálový model

Zdroj: [46]

2.3 Metodiky vývoje IS

Tato kapitola obsahuje pouze výčet používaných metodik. Kompletní popis a rozbor používaných metodik je nad rámec této práce a k těmto metodikám jsou dostupné postupy jak v elektronické, tak i v tištěné podobě.

Metodiky definují principy, procesy, praktiky, role, techniky, nástroje a produkty při vývoji, provozu a správě IS a měly by odpovídat na otázky „*Proč? Kdo? Kdy? Co?*“. [6], [7], [10]

Následuje výčet dělení metodik, jak je uvedeno v dostupných zdrojích [6], [7].

Podle zaměření:

- globální metodiky – týkají se celé organizace,
- projektové metodiky – činnosti v rámci jednoho projektu.

Podle rozsahu:

- metodiky pokrývající celý životní cyklus,
- dílčí metodiky – část životního cyklu.

Podle váhy PARTS (Precision, Accuracy, Relevance, Tolerance, Scale):

- těžké (rigorózní) metodiky – podrobné,

- lehké metodiky – minimálně dostatečné.

Podle typu řešení:

- Application Service Provision – forma outsourcingu,
- nové – vývoj nového IS,
- integrace – integrace řešení,
- upgrade – rozvoj a rozšíření,
- užití – užití řešení,
- typové – hotové řešení.

Podle typu domény:

- Business Intelligence,
- Customer Relationship Management,
- obecný software,
- Content Management,
- Enterprise Application Integration,
- E-commerce,
- Enterprise Resource Planning.

Podle přístupu k řešení:

- strukturovaný vývoj,
- rychlý vývoj aplikací – RAD (Rapid Application Development).

2.3.1 Rigorózní metodiky

Hlavním kritériem pro odlišení rigorózní a agilní metodiky je váha. Rigorózní metodiky jsou zpravidla založené na vodopádovém modelu, na iterativním a inkrementálním vývoji, jako například metodika OPEN (Object–oriented Process, Environment and Notation), RUP (Rational Unified Process), EUP (Enterprise Unified Process) a MSF (Microsoft Solutions Framework). Jedná se o tradiční, tzv. těžké metody, které jsou podrobné a formální. Samostatnou kategorii tvoří metodiky pro hodnocení SW procesů, mezi které patří SPA (Software Process Assesment), OOSPICE (Software Process Improvement and Cabability Determination for Object Oriented/Component Based Software Development) a Model zralosti (Capability Maturity Model). [6], [7], [10]

2.3.2 Agilní metodiky

Hlavním kritériem pro odlišení rigorózní a agilní metodiky je váha. Z důvodu dynamických změn v oblasti ekonomického prostředí a technologií dochází k požadavkům na rychlé změny IS a ICT. Z těchto důvodů jsou kladeny požadavky na změny v metodikách, které jsou schopné pružně reagovat na měnící se požadavky. Agilní přístupy nepopisují procesy, ale definují jen principy a praktiky. Jednotlivé metody jsou specifické, ale vycházejí ze stejných principů a hodnot. Tyto metodiky vznikají od 90. let minulého století a jejich podstata spočívá v rychlém navržení řešení, které je předloženo zadavateli. Na základě připomínek zadavatele je řešení upraveno. Agilní metody jsou řízeny Aliancí pro agilní vývoj softwaru na základě podepsaného dokumentu „*Manifest agilního vývoje software*“. Představiteli agilních metodik jsou DSDM (Dynamic Systems Development Method), ASD (Adaptive Software Development), FDD (Feature–Driven Development), Extreme Programming XP, Lean Development, Scrum, Crystal metodiky, Agile Modeling. [6], [7], [10]

2.4 Operační systém

Na otázku „*Co je to operační systém?*“ lze odpovědět velice stručně. Jedná se o nutnou nástavbu pro používání technického vybavení (hardware) počítače. Operační systém je software, který ovládá a spravuje interní a externí technické prostředky počítače. Jedná se o množinu programů, které umožňují ostatním programům pracovat s hardwarem. V současnosti jsou používané počítače čtvrté generace, jejichž struktura integrovaných obvodů střední, velké a velmi velké integrace vznikla v roce 1981. Mezi další zařízení, která jsou řízena a ovládána operačním systémem, patří mobilní a speciální zařízení. Všechna tato zařízení bez operačního systému mají omezenou funkčnost, danou použitým základním softwarovým vybavením, které se obecně nazývá firmware. [5], [14], [3], [9]

Cílem operačního systému je s maximální efektivností a bezpečností využívat hardwarové prostředky počítače a zajistit vhodné prostředí pro práci ostatním uživatelským programům, které nemají přímý přístup k hardwaru. Při souběžném zpracování dat jim určuje pořadí, prioritu a čas. Operační systémy ovládají hardwarové vybavení prostřednictvím ovladačů. Mezi další funkce operačního systému patří správa systému, paměti, procesů, souborů, uživatelů a úloh. Dále poskytují uživatelské, programové rozhraní a vlastnosti virtuálního počítače. Zjednodušený vztah od uživatele až po technické vybavení zařízení je vyobrazeno na obrázku 1. [5], [14], [9]

Operační systémy můžeme dělit podle struktury zpracovávaných úloh na jednoúlohové a víceúlohové. Dále je můžeme rozdělit podle účelu na střediskové, desktopové, mobilní a serverové. Z hlediska architektury je dělíme na monolitické, vrstvené a model klient–server. Podle procesů a času je dělíme na jednoprocesové, víceprocesové, zpracování v reálném čase a řízené událostmi. [5], [9]

Z výše uvedeného textu můžeme shrnout základní služby operačního systému vzhledem k uživateli a k systému.

Obrázek 8: Interakce mezi uživatelem a technickým vybavením

Zdroj: upraveno podle [31]

Služby operačního systému z pohledu uživatele

- Spouštění programů – vytváří prostředí pro spouštění uživatelských programů.
- I/O operace – vytváří prostředí pro používání vstupních a výstupních operací uživatelskými programy.
- Správa souborových systémů – umožňuje přístup k souborům na záznamovém médiu.
- Komunikace – umožňuje lokální a vzdálenou komunikaci procesů prostřednictvím sdílené paměti nebo zasílání zpráv.
- Detekce chyb – sleduje detekování chyb, aby nedošlo k selhání celého systému. [32], [2]

Služby operačního systému z pohledu systému

- Alokace zdrojů – řídí přidělování prostředků jednotlivým úlohám a uživatelům.
- Účtování – vede přehled o využívání zdrojů a vytváření statistik využívání zdrojů.
- Ochrana – zabezpečuje ochranu systémových prostředků před jednotlivými procesy a neautorizovaným přístupem. [32], [2]

Hlavní představitelé výrobců operačních systémů a verzí

- Microsoft – OS Windows,
- Apple Macintosh – Mac OS,
- IBM AIX (rodina UNIX),
- Hewlett-Packard – HP-UX (rodina UNIX),
- Distribuce LINUX – Ubuntu, Debian, Red Hat, openSUSE, Gentoo, Fedora,
- Google – Android. [14], [16]

2.5 Počítačová bezpečnost

Bezpečnost v oblasti počítačových sítí a informačních systémů je detailně popsána ve výchozí práci v kapitole 3 „*Bezpečnost sítí a ochrana dat*“. Informační systémy se skládají z hardwaru, softwaru, dat a také lidí, a proto je nutné zabývat se bezpečností zejména u těchto prvků.

Do ochrany počítačové bezpečnosti patří kryptografie a digitální podpisy, ochrana dat, autentizace a řízení přístupu, ochrana přenášených dat, ochrana připojených počítačů, ochrana proti škodlivému softwaru, fyzická ochrana prvků ICT, definování přístupů rolí, personální bezpečnost a aktuální bezpečnostní a provozní dokumentace. Při definování, realizaci a hodnocení bezpečnosti ochrany IT je nutné postupovat podle normalizovaných metod uvedených v ČSN ISO (EN), popřípadě odborných a vědeckých prací. Je nutné se zaměřit na bezpečnost vnitřního a vnějšího prostředí, proti atakům útočníků se znalostmi amatérů až profesionálů a proti jiným rizikům, jako jsou například katastrofy. Ochrana nám jednak slouží k eliminaci tzv. bezpečnostních děr, kterých útočníci využívají, ale také ke snížení nebo eliminaci škod způsobených nepředvídatelnou událostí. Bezpečnostní chyby můžou vzniknout v jakékoli oblasti, která se dotýká bezpečnosti ICT. Aktuální zdokumentované bezpečnostní chyby jsou velice dobře popsány na portále CVE (Common Vulnerabilities and Exposures). [12], [39]

Jeden z hlavních prvků ochrany je auditní systém, který ukládá předem definované druhy událostí. Tyto události slouží pro následnou analýzu nebo pro systémy včasného varování. Dalším podstatným prvkem je zálohování, které nám v případě pádu systému umožní obnovit data a systémy. [12]

Ochrana systémů a sítí proti útočníkům není jednoduchá. Uvedeme nejčastější postupy, které využívají útočníci. Útočníci užívají běžné nástroje operačních systémů, specializované utility a vlastní nástroje.

- Vyhledávání stop – zisk informací o subjektu v internetu.
    - Ochrana – odstranění všech nežádoucích informací z veřejně přístupných zdrojů o doméně, síti a kontaktech a promyšlená smlouva se zaměstnanci.
- Zkoumání DNS – zisk informací o IP adresách zařízení.
    - Ochrana – správně nastavený DNS a zakázaný přenos zón.
- Průzkum sítě – určení síťové topologie.
    - Ochrana – filtrování TCP/UDP portů, zakázání ICMP dotazů.
- Skenování – zisk informací o živých systémech, běžících službách a identifikace OS.
    - Ochrana – zakázání ICMP dotazů, povolení používaných a zabezpečených služeb (portů).
- Inventarizace – získání informací o sdílených síťových prostředcích, uživatelích a skupinách, aplikacích a jejich bannerech (výstupy z aplikace).
    - Ochrana – filtrování TCP/UDP portů, změna čísel portů, používání zabezpečených služeb, zakázání nepoužívaných služeb, seznámení s dokumentací výrobce SW.
    - Útoky na bezdrátové sítě – útoky na základě broadcastingové podstaty s cílem dosáhnout dálkového průniku do bezdrátové sítě a útoky související s nedostatky autentizačních protokolů.
        - Ochrana – používat ověřené metody kontrol přístupů, šifrování dat, filtrování provozu, dostatečně dlouhé a zabezpečené heslo bezdrátové sítě. [39]

Jednotlivé postupy nastavení zabezpečení se liší od daného hardwaru, firmwaru až po software. Základem pro zabezpečení prvků ICT je správně nastavený software, firewall a aktuální verze softwaru. Aktualizace lze provádět ručně nebo automaticky. U velkých a zabezpečených systémů jsou aktualizace prováděny ručně po odzkoušení na testovacím polygonu.

2.6 Bezpečnostní a provozní dokumentace IS

Bezpečnostní a provozní dokumentace je nedílnou součástí zabezpečeného informačního systému. Při tvorbě dokumentace záleží na úrovni zabezpečení IS a klasifikaci dat.

2.6.1 Bezpečnostní dokumentace

Bezpečnostní dokumentace je popsána ve výchozí práci v kapitole 3.2 „*Bezpečnost informačních systémů*“ [15]. Jedná se o bezpečnostní politiku IS, analýzu rizik a havarijní plán.

Minimální dokumentace, kterou by měl informační systém obsahovat, je analýza rizik, bezpečnostní směrnice bezpečnostního správce, bezpečnostní směrnice správce, bezpečnostní směrnice uživatele a havarijní plán.

Vhodnou pomůckou pro tvorbu bezpečnostní dokumentace je návod „*Zásady tvorby bezpečnostní dokumentace informačních systémů určených k nakládání s utajovanými informacemi*“, který obsahuje postup vytvoření bezpečnostní dokumentace v souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Struktura a obsah bezpečnostní dokumentace

1. Bezpečnostní politika informačního systému (BP IS) – základní dokument:
    a. úvodní ustanovení,
    b. personální bezpečnost,
    c. počítačová bezpečnost,
    d. kryptografická ochrana,
    e. fyzická bezpečnost,
    f. administrativní bezpečnost,
    g. řízení a plánování kontinuity,
    h. další bezpečnostní dokumentace.
2. Analýza rizik informačního systému – druhý nejdůležitější dokument vycházející z BP IS (pomůcka pro analýzu rizik viz ČSN ISO/IEC 27005 „Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací“):
    a. základní analýza rizik,
    b. doplňková analýza rizik.
3. Návrh bezpečnosti informačního systému – stěžejní dokument projektové bezpečnostní dokumentace IS:
    a. úvodní ustanovení,
    b. personální bezpečnost,
    c. počítačová bezpečnost,
    d. kryptografická ochrana,
    e. fyzická bezpečnost,
    f. administrativní bezpečnost,
    g. řízení a plánování kontinuity.

4. Bezpečnostní směrnice informačního systému:
    a. bezpečnostní směrnice bezpečnostního správce / správce,
    b. povinnosti dané role,
    c. práva dané role,
    d. procedury spojené s povinnostmi a právy dané role.
5. Bezpečnostní směrnice uživatele:
    a. popis informačního systému včetně jeho rozsahu a umístění,
    b. definici a rozdělení krizových situací včetně základního popisu toho, jak se uživatel podílí na řešení,
    c. definici a rozdělení bezpečnostních incidentů včetně základního popisu toho, jak se uživatel podílí na řešení,
    d. definici kompromitace včetně základního popisu toho, jak se uživatel podílí na řešení.
6. Havarijní plány a činnosti při krizových situacích a bezpečnostních incidentech. [59]

2.6.2 Provozní dokumentace

Provozní dokumentace obsahuje popisy a návody spojené s provozováním systému.

Projektová dokumentace

Projektová dokumentace je vypracována vývojovým týmem a je určená výhradně pro vývojové pracovníky. Obsahuje popis modelů na konceptuální, technologické a implementační úrovni. Dále obsahuje dokumenty, které vznikly v procesu zadání, analýzy, návrhu a implementace systému. [34], [23]

Uživatelská dokumentace

Uživatelská dokumentace je určena pro uživatele, kteří se systémem pracují. Uživatelská dokumentace může obsahovat technologickou, operátorskou a uživatelskou referenční příručku. Technologická příručka slouží pro popis provozní technologie v rámci zpracovatelského cyklu. Operátorská příručka popisuje ovládání IS při jednotlivých procedurách včetně uživatelské obrazovky a ovládání. Uživatelská příručka popisuje funkce aplikací, druhy zpracování a jejich význam. Popisuje vstupy, výstupy a řešení standardních i nestandardních situací. [34], [23]

Administrátorská dokumentace

Administrátorská dokumentace je určena výhradně pro administraci systému a přístup k této dokumentaci by měli mít pouze administrátoři. Následující odrážky obsahují doporučenou strukturu dokumentu. [34], [23]

- *Základní funkční specifikace informačního systému.*
- *Technologický postup práce s daným IS.*
- *Technický návrh informačního systému.*
- *Organizačně provozní zajištění informačního systému.*
- *Instalace a konfigurace serverových komponent.*
- *Instalace a konfigurace klientských komponent.*
- *Instalace a konfigurace síťových komponent.*
- *Popis a konfigurace bezpečnostních prvků v systému.*
- *Popis bezpečnostního zálohování dat a programů informačního systému.*
- *Popis provozního archivování dat a rušení dat z provozní databáze.*
- *Dohled a prověřování stavu systému.*
- *Řešení nestandardních stavů systému, scénáře řešení apod.*
- *Organizace činnosti při zavádění informačního systému do provozu.* [34], [23]

2.7 Ostatní bezpečnostní prvky IS a ochrana

Další bezpečnostní prvky včetně ochrany IS jsou uvedeny ve výchozí práci. Jedná se o personální bezpečnost, bezpečnost informací a mechanismy, útoky na informační technologie, škodlivý programový kód, časté chyby zabezpečení, ochrana proti možným útokům, monitoring, auditní systém a řízení přístupu. [15]

2.8 Základy zabezpečení OS Ubuntu

V OS Ubuntu je nutné věnovat pozornost nastavení účtu root. Účet root nesmí být použit pro běžnou práci a vzdálené připojování k OS. Musí mít nastavené bezpečné heslo, které je dostatečně dlouhé a složité. Ubuntu 18.04 používá dvě základní řešení zabezpečení. Jedná se o utilitu AppArmor a firewall UFW. Další možností zabezpečení služeb OS je používání certifikátů a eCryptfs (Enterprise Cryptograhic Filesystem) pro šifrování dat na discích.

AppArmor chrání části operačního systému před nechtěným provedením operace. Definuje práva aplikací vzhledem k operačnímu systému a jeho systémovým souborům. AppArmor je definován v profilech, které obsahují příslušné nastavení. [52], [51]

Firewall UFW (Uncomplicated Firewall) je součástí instalace Ubuntu. UFW vychází z iptables firewallu. Jedná se o jednoduchý firewall k zabezpečení IPv4 a IPv6 provozu. Funguje na základě vytvořených pravidel, která mohou být uložena v konfiguračním souboru pravidla nebo zadaná formou příkazové řádky. [52], [51]

2.9 Základní normy při výstavbě IS

Zákonné normy

- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.
- Nařízení Evropského parlamentu a rady č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů.
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.
- Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).
- Zákon č. 40/2009 Sb., trestní zákoník.
- Zákon č. 563/1991 Sb., o účetnictví.

Technické normy

- ČSN ISO (27000-27011) Informační technologie – Bezpečnostní techniky.
- ČSN ISO (27013-27019) Informační technologie – Bezpečnostní techniky.
- ČSN ISO (31000) – Management rizik.

3 POPIS A ANALÝZA SITUACE

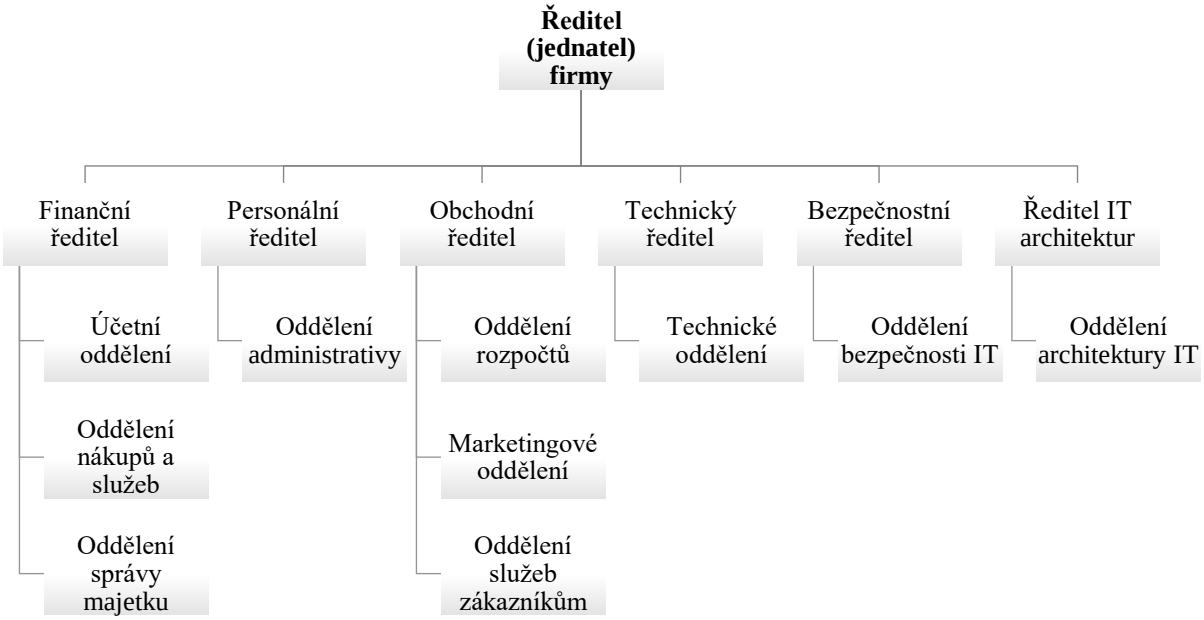
Pro praktickou ukázku je vybrána hypotetická společnost s názvem Komunikační inteligence s. r. o. Ukázka nastavení zabezpečené počítačové sítě a operačního systému je realizována na úrovni nastavení routeru a základního nastavení serveru jako řadiče domény s AD.

Výchozí situace

Firma působí na trhu od roku 2016 v oblasti prodeje komunikačních služeb a podpory. Zaměstnává 45 osob a finanční stránka firmy není úplně příznivá. Firma poptává levnější řešení dodávky informačního systému. Strukturovaná síť včetně aktivních prvků je již vybudovaná. Vybavení firma pořídila v letech 2016–2018. Připojení k interní síti intranet je realizováno metalickými kabely a bezdrátovým spojem. Připojení do celosvětové sítě internet je realizováno bezdrátovým spojem. Firma provedla upgrade všech předchozích verzí OS Windows na Windows 10 Pro. Veškerá aktiva jsou v zabezpečené budově a řídicí prvky počítačové sítě jsou umístěny v místnosti s řízeným vstupem. Celá budova je pod EZS a personální bezpečnost firma řeší výpisy z rejstříku trestů a smlouvou.

Organizační struktura firmy

Funkcionální organizační struktura je vyobrazena na následujícím obrázku.



Obrázek 9: Organizační struktura

Zdroj: vlastní zpracování

3.1 Specifikace požadavku

Firma vytvořila základní požadavky na zabezpečení a služby IS. Hlavním kritériem je minimální cena, kterou stanovila na 50 tisíc Kč. V rámci této ceny požaduje dodat funkční informační systém podle následujících požadavků.

Požadavky na IS:

a) Dodání zabezpečené počítačové sítě a serveru:
   - řadič domény,
   - implementace AD,
   - automatické přidělování IP adres,
   - zabezpečení firewallu
   - řízené sdílení složek.

b) Připojení zařízení ICT:
   - počítače stolní a přenosné,
     - distribuce politik GPO,
     - připojení k VPN.

c) Bezpečný přístup z internetu:
   - vytvoření VPN serveru.

d) Oddělená síť pro hosty firmy:
   - vytvoření Wi-Fi pro hosty.

e) Připojení ostatních zařízení ICT:
   - tiskárny,
   - mobilní telefony.

f) Replikace VM (Virtual Machine).

g) Auditní systém.

h) Zálohování účetního programu POHODA.

i) Zavedení CRM systému.

j) Zálohování na placené úložiště.

k) Vytvoření bezpečnostní, administrátorské a uživatelské dokumentace.

Firma celý projekt vývoje IS řeší na základě následujících fází projektu. My se budeme pohybovat v rámci ukázky ve fázi vývoje IS a testování. V této práci jsou plněny pouze body a) až d), které patří do požadavku firmy.

Fáze projektu

- úvodní studie,
- globální analýza a návrh,
- detailní analýza a návrh,
- vývoj IS a testování (implementace), ☜
- zavedení do provozu,
- provoz a údržba
- vyřazení IS.

3.2 Omezení ukázky nastavení IS

Z důvodu rozsahu problematiky a omezení této práce je ukázka koncipována jako základ možného nastavení, které je vhodné pro další rozšíření bezpečnostních a funkčních prvků. Některé konfigurace jako zálohování účetního programu jsou triviální a jsou v souladu s nastavením pro zabezpečení sdílení složek včetně nastavení cest podle příručky dodavatele softwaru.

3.3 Technické údaje

Pro potřeby testování jsou vybrány níže uvedené prvky z oblasti hardwaru a softwaru.

Hardware

- Server DELL (PowerEdge R515 - 2U).
- Systém zabezpečení dat disků – RAID 01 [15].
- Router MikroTik RB2011UiAS-2HnD-IN s RouterOS 6.45.2.
- Počítač přenosný.

Software

- Hyper-V Core 2016.
- OS Linux Ubuntu 18.04 server.
- OS Windows 10 Pro.

4 NÁVRH ŘEŠENÍ

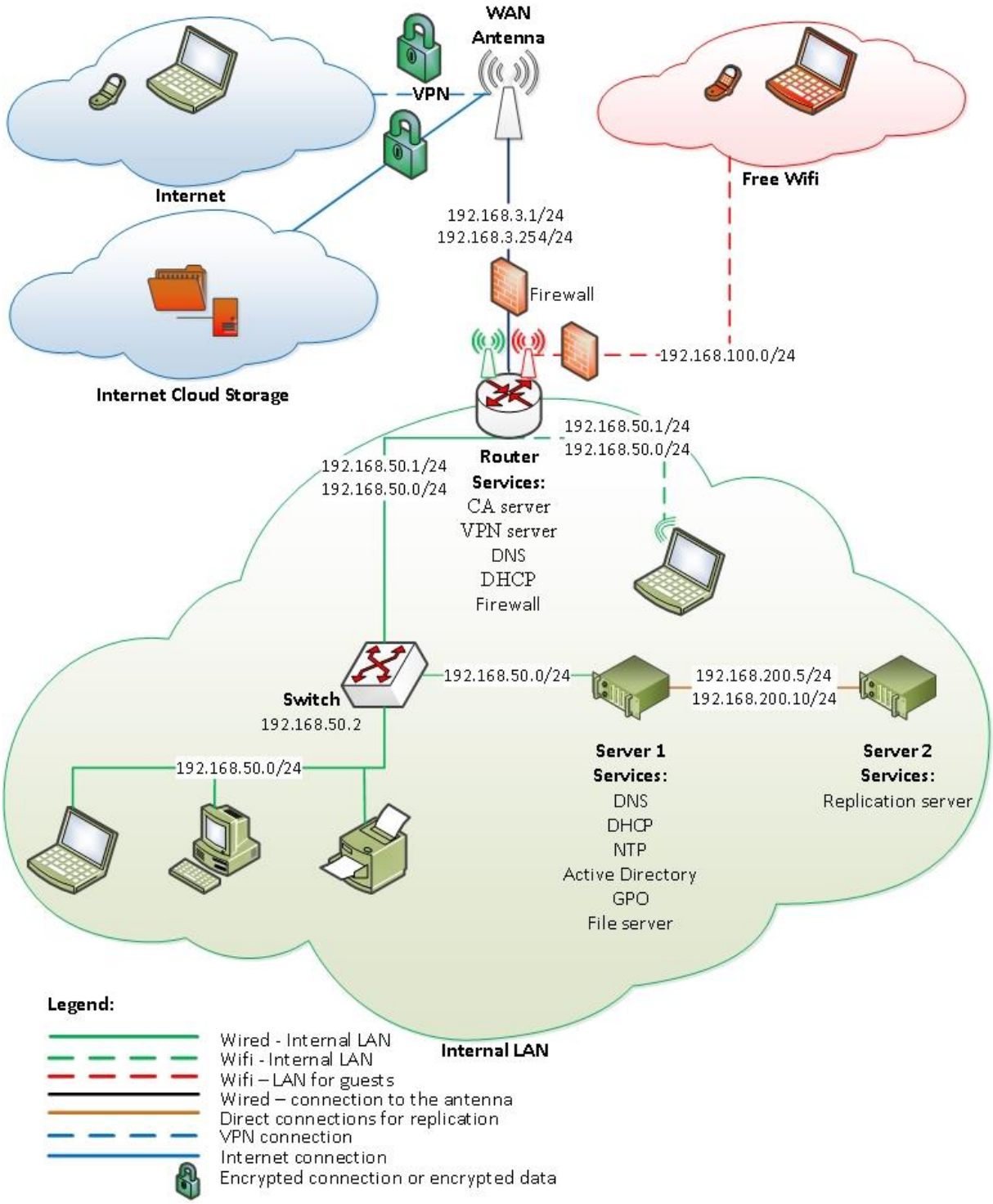
V této kapitole se dostáváme ke stěžejní části této práce. Před samotným nastavením routeru a operačního serverového systému musíme nejdříve definovat údaje o službách, sítích a zařízeních. Nejdříve navrhneme sítě pro jednotlivé části vnitřní LAN. Pro vnitřní zabezpečenou síť navrhneme network 192.168.50.0 při 24bitové masce. Síť pro hosty bude provozována na síti 192.168.100.0/24. Virtuální privátní síti přidělíme network 192.168.51.0/24. Pro replikaci virtuálních mašin (VM) přidělíme network 192.168.200.0/24 (není součástí ukázky). Detailní rozdělení služeb a přidělení adres je uvedeno v následující tabulce.

Tabulka 2: Přehled vnitřních síťových služeb a adres

	Internal LAN (Wired / Wifi)	**VPN**	**Free Wifi**
Domain	comintelligence.cz	comintelligence.cz	
Wi-FI SSID	Wifi-Firma		Wifi-Firma-Free
Control	Server / Router	Router	Router
Network	192.168.50.0/24	192.168.51.0/24	192.168.100.0/24
Gateway	192.168.50.1		192.168.100.1
Servers	192.168.50.5		
DNS	192.168.50.5	192.168.50.5	8.8.8.8 185.43.135.1
DHCP	192.168.50.5	VPN Server	192.168.100.1
NTP	192.168.50.5		
DHCP pool	192.168.50.20-100	192.168.51.20-100	192.168.100.20-200
Services	• DNS • DHCP • NTP • Active Directory • GPO • File server	• Certificate Authority server • VPN server • DHCP	• DNS • DHCP

Zdroj: vlastní zpracování

Pro lepší pochopení celého systému využijeme grafické znázornění všech sítí, adres a komponentů, viz obrázek 10. Jednotlivé sítě jsou barevně rozlišeny a přenosové médium je znázorněno typem čáry. Kabelové propojení pro replikaci VM neprochází žádným aktivním prvkem.



Obrázek 10: Schéma sítí a služeb

Zdroj: vlastní zpracování

Jak již bylo řečeno, tak celá instalace a nastavení IS je v následující ukázce řešena pouze do úrovně nastavení routeru MikroTik a serveru na platformě OS Linux. Ukázka konfigurace routeru a serveru je z větší části vytvořena v příkazovém módu.

5 IMPLEMENTACE NAVRHOVANÝCH ŘEŠENÍ

Implementaci řešení můžeme rozdělit do několika částí. V první části ukázky je provedeno nastavení vybraného routeru. V následující části je instalován vybraný operační systém včetně nastavení požadovaných služeb. Poslední část je věnována testování aplikovaných nastavení. Ukázka obsahuje detailní nastavení, které se v textu skládá z mnoha vizualizací, příkazů a obsahů konfiguračních souborů. Některé postupy a konfigurace jsou uvedeny v přílohách.

Celý postup nastavení je chronologicky seřazen následovně:

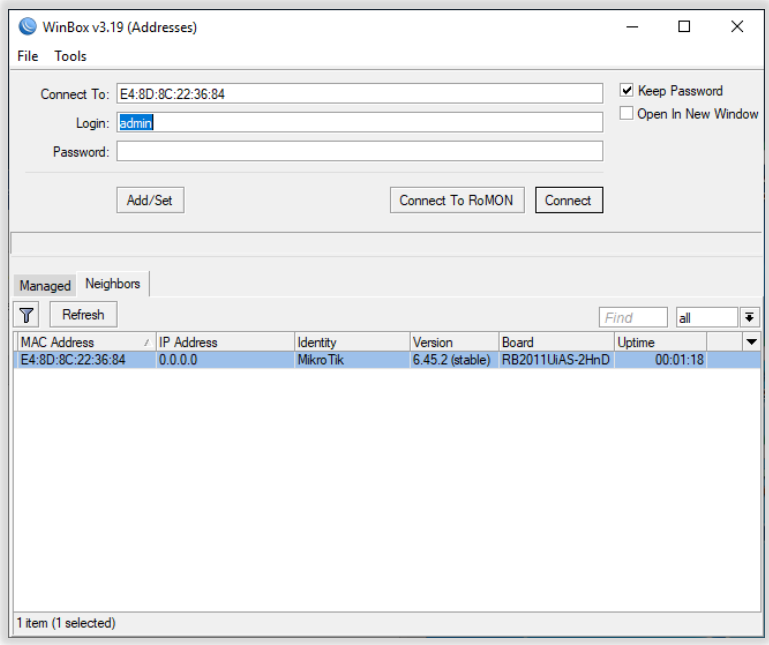
a) Nastavení routeru.
b) Instalace operačního systému serveru.
c) Instalace a nastavení požadovaných služeb.
d) Vytvoření bezpečného prostředí.
e) Připojení klientů.
f) Testování zabezpečení.

5.1 Nastavení síťového prostředí a routeru

Na základě definovaných požadavků a návrhu řešení můžeme přejít ke konfiguraci routeru. Pro pochopení celé problematiky byl vybrán router od firmy MikroTik. Tento router je možné konfigurovat v grafickém prostředí GUI (Graphical User Interface) nebo v příkazovém řádku. V našem případě použijeme příkazový řádek v aplikaci WinBox, protože protokol SSH a telnet budou na routeru zakázány.

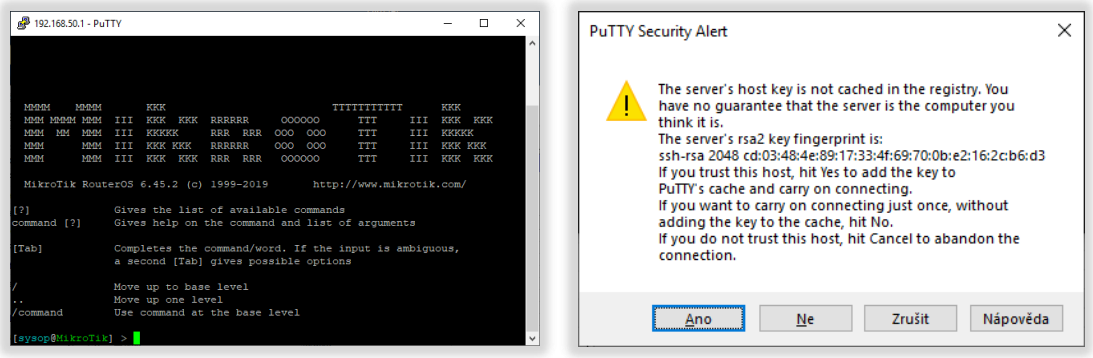
5.1.1 Připojení k routeru

Pro první připojení k routeru můžeme použít výchozí IP adresu nebo MAC (Media Access Control) adresu. Při použití výchozí konfigurace routeru je nutné nastavit síťové připojení ovládacího počítače do stejné sítě LAN 192.168.88.0/24. Výchozí IP adresa routeru je 192.168.88.1/24. Ovládací počítač musí mít nastavenou rozdílnou IP adresu z rozsahu dané sítě, což je 2 až 254 v posledním oktetu. Pojem IP a MAC adresa je detailně rozebrán v textu výchozí práce [15]. Vhodnější je použít, do doby zakázání, službu MNDP (Neighbor Discovery Protocol), která umožňuje automatické vyhledání MAC adresy routeru prostřednictvím aplikace WinBox, viz obrázek 11. Další způsob připojení je prostřednictvím SSH a aplikace PuTTY, viz obrázek 12.



Obrázek 11: Připojení k routeru prostřednictvím aplikace WinBox

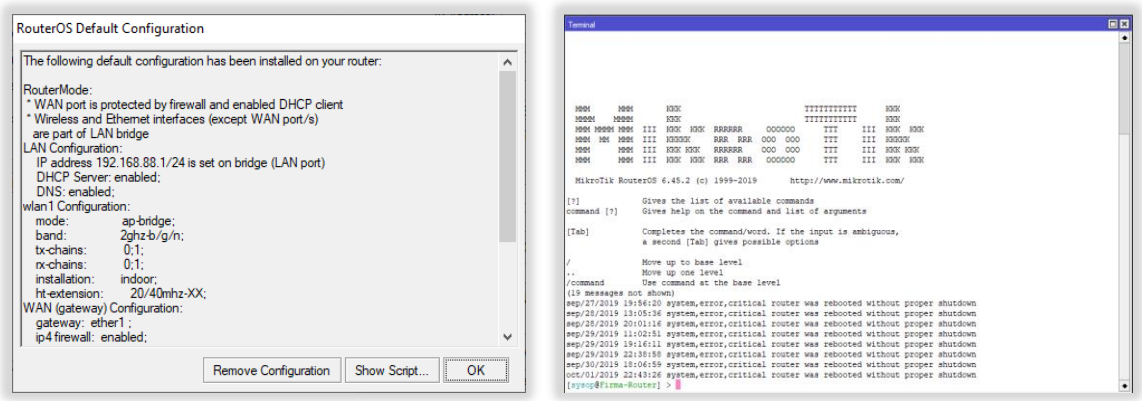
Zdroj: vlastní zpracování



Obrázek 12: Připojení k routeru prostřednictvím aplikace PuTTY

Zdroj: vlastní zpracování

Po prvním přihlášení k routeru je zobrazena úvodní stránka, která obsahuje informace o výchozí konfiguraci routeru. V našem případě vybereme volbu odebrání konfigurace, viz obrázek 13 vlevo, nebo můžeme konfiguraci odstranit příkazem „*system reset-configuration no-defaults=yes*“ v okně terminálu, viz obrázek 13 vpravo [28].

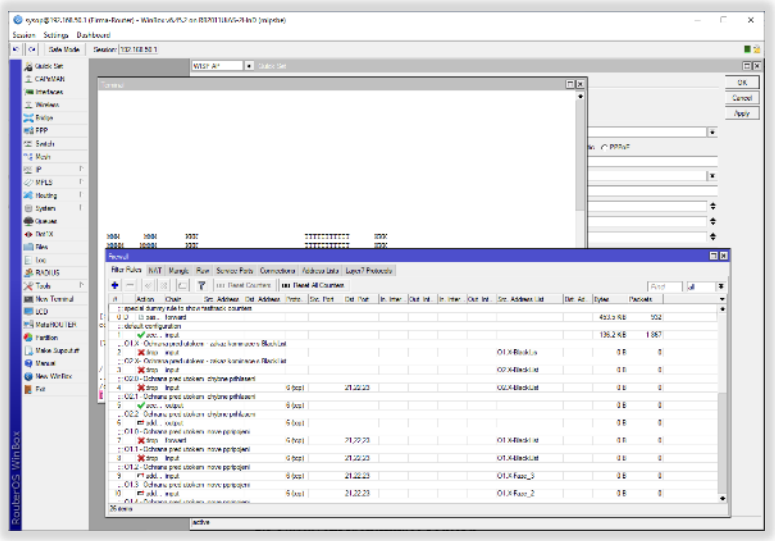


Obrázek 13: Úvodní obrazovka po přihlášení a okno terminálu

Zdroj: vlastní zpracování

5.1.2 Základní ovládání aplikace WinBox

Grafické rozhraní aplikace se skládá ze dvou částí. V levé části je umístěno vysouvací menu, které obsahuje volby pro nastavení routeru v grafickém rozhraní. Prostřední část okna slouží pro vizualizaci jednotlivých modulů, které jsou vyvolány z vertikálního menu, viz obrázek 14.



Obrázek 14: Aplikace WinBox

Zdroj: vlastní zpracování

5.1.3 Nastavení přístupových práv

Z důvodu zabezpečení jako první nastavíme účet a heslo pro privilegovaný účet. Obecně se nedoporučuje ponechávat uživatelská jména, která jsou nastavena výrobcem zařízení. Jedná se zejména o účty s názvem administrátor, admin, název zařízení apod. V našem případě použijeme jako název účtu sysop (System Operator). Přidání účtu s heslem a právy

administrátora, včetně povolení sítě, ze které je možné se přihlásit, provedeme pomocí následujících příkazů [28], [26].

user add name=sysop password=HesloProSysop group=full
user set sysop address=192.168.50.0/24,192.168.51.0/24 comment="User with full access"

Po přihlášení novým účtem můžeme původní účet vymazat.

user remove admin [28], [26]

5.1.4 Základní nastavení routeru

V této kapitole provedeme nastavení síťových rozhraní a identifikaci routeru v síti LAN. Název zařízení nastavíme pomocí příkazu „*system identity set name=Firma-Router*“. V průběhu nastavování je prováděna kontrola pomocí příkazu „*print*“. Tento příkaz vypíše na obrazovku aktuální nastavení dané úrovně konfigurace. [28]

5.1.5 Konfigurace síťového rozhraní

Kontrolu síťových rozhraní je možné provést příkazem „*interface ethernet print*“ [28]. Kontrolu bridge provedeme příkazem *„interface bridge port print“* [28]. Při vymazané konfiguraci routeru musejí být výpisy prázdné. Následujícím příkazem vytvoříme interface s názvem Bridge a statickou fyzickou adresou MAC v hexadecimálním tvaru.

interface bridge add admin-mac=E4:8D:8C:22:36:83 auto-mac=no comment="Internal LAN" name=bridge [28]

Rozhraní bridge slouží k vytvoření tzv. mostu (propojení) mezi jednotlivými ethernetovými rozhraními. Tato rozhraní budou mezi sebou komunikovat na druhé linkové vrstvě modelu ISO/OSI. Na této vrstvě dochází k neomezenému šíření všeobecných a skupinových adres (broadcast, multicast). [47], [3], [42] Následujícími příkazy propojíme jednotlivé rozhraní s vytvořeným mostem [28].

/interface bridge port
add bridge=bridge comment="Internal LAN" interface=ether2
add bridge=bridge comment="Internal LAN" interface=ether3
add bridge=bridge comment="Internal LAN" interface=ether4
..
..
add bridge=bridge comment="Internal LAN" interface=ether8
add bridge=bridge comment="Internal LAN" interface=ether9
add bridge=bridge comment="Internal LAN" interface=ether10
add bridge=bridge comment="Internal LAN" interface=sfp1
add bridge=bridge comment="Internal LAN" interface=wlan1

Výpis nastavení jednotlivých rozhraní a příslušnosti k mostu vypíšeme příkazem „*/interface bridge port print*“ [28]. V případě nekorektního či neúplného výpisu provedeme restart routeru a příkaz s výpisem opakujeme.

5.1.6 Nastavení IP adresy pro přístup

Před zakázáním protokolu Neighbor musíme nastavit statickou IP adresu zařízení. V našem případě je to adresa 192.168.50.1/24.

/ip dns static add address=192.168.50.1 comment="Internal LAN" name=router.lan
/ip dns static print [28]

5.1.7 Nastavení adres a routování

V této části nastavíme jednotlivým rozhraním (v každé síti musí být minimálně jedno) IP adresy. Prvním příkazem nastavíme adresu pro rozhraní, které bude připojeno do celosvětové datové sítě internet, a druhému rozhraní nastavíme adresu tohoto zařízení ve vnitřní síti. [28]

/ip address add address=192.168.3.254/24 interface=ether1 network=192.168.3.0 comment="WAN"
/ip address add address=192.168.50.1/24 interface=ether2 network=192.168.50.0 comment="LAN+WIFI"
/ip address print

5.1.8 Nastavení směrování

Směrování, také nazýváno routování, je jednoduše řečeno směrování paketů mezi jednotlivými sítěmi za pomoci směrovacích (routovacích) tabulek. Jednotlivé sítě mezi sebou bez směrovače nemohou komunikovat. Všeobecně je IP adresa routeru známa jako Gateway (brána). [47], [3], [42]

Následujícím příkazem nastavíme, že všechny dotazované adresy, které nejsou místní, budou směrovány na bránu. [28]

/ip route add distance=1 gateway=192.168.3.1
/ip route print

5.1.9 Nastavení Wi-Fi adaptéru a přístupu

Komunikace v prostředí počítačových sítí je realizována prostřednictvím metalických, optických kabelů a bezdrátových spojů. V současnosti se velice často používají bezdrátové

spoje o frekvenci 2,4 a 5 GHz. Následující postup je věnován nastavení bezdrátového rozhraní na bázi 2,4 GHz podle normy IEE 802.11 b/g/n. Jedná se o připojení s maximální rychlostí 11/54/600 Mb/s a šířkou pásma 20 MHz a 40 MHz [16], [57].

Uvedené nastavení je navržené pro Českou republiku, automatickou frekvenci, vnitřní instalaci, omezení kanálu a vysílacího výkonu. Bezdrátová síť bude pracovat v módu AP-Bridge. [28]

/interface wireless set [find default-name=wlan1] antenna-gain=4 band=2ghz-b/g/n channel-width=20/40mhz-XX country="czech republic" disabled=no distance=indoors frequency=auto frequency-mode=regulatory-domain installation=indoor mode=ap-bridge ssid=Wifi-Firma wireless-protocol=802.11
/interface wireless print [28]

Po nastavení adaptéru je nutné vytvořit profil, který obsahuje údaje pro připojení k bezdrátové síti. Router MikroTik nabízí různé druhy šifrovacích nástrojů, jako jsou WPA a WPA2 (Wi-Fi Protected Access) v kombinaci s šifrovacím algoritmem AES CCM a TKIP šifrovacím protokolem. V našem případě zvolíme šifrovací nástroj WPA2 PSK (Wi-Fi Protected Access - Pre-shared key) v kombinaci s AES CCM (Advanced Encryption Standard – Counter Mode with Cipher Block Chaining and Message Authentication Code Protocol). [56], [40]

Nastavení provedeme následujícím příkazem. [28]

/interface wireless security-profiles set [find default=yes] authentication-types=wpa2-psk mode=dynamic-keys supplicant-identity=MikroTik wpa-pre-shared-key=HesloProWifi wpa2-pre-shared-key=HesloProWifi

5.1.10 Nastavení Interface list

Pro přehlednost vytvoříme seznam virtuálních rozhraní a přidělíme jim rozhraní, která jsme dříve nastavili.

/interface list add comment="External WAN" name=WAN
/interface list add comment="Internal LAN" name=LAN
/interface list member add comment="Internal LAN" interface=bridge list=LAN
/interface list member add comment="External WAN" interface=ether1 list=WAN
/interface list print [28]

5.1.11 Nastavení DNS

Dalším krokem je nastavení DNS serverů, které nám slouží pro překlad názvů, respektive adres v podobě názvů na IP adresy [47], [3], [42].

/ip dns set servers=77.236.192.130,77.236.192.150,8.8.8.8 allow-remote-requests=yes
/ip dns print [28]

5.1.12 Nastavení synchronizace času

Pro správnou funkci routeru a relevantnost údajů v auditních záznamech je nutné provést synchronizaci času. Nastavení provedeme následujícím příkazem. Jako nadřazené časové servery, z kterých budeme provádět synchronizaci, jsme vybrali servery poskytovatelů CESNET, z. s. p. o. a CZ.NIC, z. s. p. o.

/system clock set time-zone-autodetect=no time-zone-name=Europe/Prague
/system ntp client set enabled=yes server-dns-names=192.168.50.1
primarntp=195.113.144.201 secondary-ntp=217.31.202.100
/system clock print [28]

5.1.13 Zabezpečení služeb routeru a nastavení firewalu

Router nabízí mnoho služeb. Nepsané pravidlo v oblasti zabezpečení mluví o tom, co nepotřebujeme nebo nevíme, k čemu je, tak vypneme. Sice můžou nastat problémy s funkčností, ale tak zjistíme, jestli službu opravdu využijeme, nebo ne. Následující restrikce vycházejí z požadavků zadavatele a návodů pro router MikroTik.

Firewall routeru plní funkci pro zabezpečení provozu v síti, ale také pro definování NAT (Network Address Translation) a značkování paketů. [28]

5.1.14 Překlad lokálních a veřejných adres

Jedná se o dynamický NAT, kdy paketům pocházejícím z vnitřní sítě je změněna zdrojová IP adresa a je dále odeslán na základě směrovací tabulky. Původní port včetně IP adresy je uložen v routeru a příchozím paketům je IP adresa přepsána na zdrojovou adresu. [3], [28]

/ip firewall nat add action=masquerade chain=srcnat comment="Internal LAN:
masquerade" ipsec-policy=out,none out-interface-list=WAN
/ip firewall nat print [28]

5.1.15 Nastavení služeb routeru

Z důvodu zabezpečení routeru vypneme nebo nastavíme služby podle požadavků. Příkazy jsou popsány jednoduše, jelikož je zřejmé, o jaká nastavení se jedná. Následující příkazy vycházejí z návodů pro router MikroTik [26].

Nastavení IP adresy pro povolení přístupu prostřednictvím WinBoxu

/ip service set winbox address=192.168.50.0/24,192.168.51.0/24

Zakázání neighbor discovery

/ip neighbor discovery-settings set discover-interface-list=none

Zakázání bandwidth server

/tool bandwidth-server set enabled=no

Zakázání DNS Cache

/ip dns set allow-remote-requests=no

Zakázání IP proxy

/ip proxy set enabled=no

Zakázání IP socks

/ip socks set enabled=no

Zakázání UPNP

/ip upnp set enabled=no

Zakázání DDNS

/ip cloud set ddns-enabled=no update-time=no

Nastavení úrovně šifrování

/ip ssh set strong-crypto=yes

Vypnutí služeb routeru

/ip service disable telnet,ftp,www,api,api-ssl
/ip service print

Změna čísla portu pro SSH

/ip service set ssh port=2222

Vypnutí mac-telnet services

/tool mac-server set allowed-interface-list=none

Vypnutí mac-winbox services

/tool mac-server mac-winbox set allowed-interface-list=none

Vypnutí mac-ping service

/tool mac-server ping set enabled=no

5.1.16 Nastavení pravidel firewallu

Při nastavování se budeme zabývat pouze pravidly pro IPv4, jelikož IPv6 nebude v naší síti podporována.

Pravidla pro router

Níže uvedená pravidla slouží ke snížení zátěže routeru, povolení seznamu povolených IP adres pro přístup, zakázání ICMP (Internet Control Message Protocol) a zamítnutí všeho, co nesplňuje zavedené pravidlo.

/ip firewall filter
add action=drop chain=input protocol=icmp comment="Reject ICMP communication on the router's interface"
add action=drop chain=input in-interface-list=WAN comment="Reject all communication to the WAN interface"
add action=accept chain=input comment="default configuration" connection-state=established,related
add action=accept chain=input src-address-list=allowed_to_router comment="Allowed to router for local LAN"
add action=drop chain=input comment="Restricting communication outside the internal LAN" [26]

Vytvoření seznamu povolených IP adres

/ip firewall address-list
add address=192.168.50.0/24 list=allowed_to_router comment="Internal LAN" [26]

Pravidla pro klienty

Níže uvedená pravidla řeší povolení FastTrack pro zrychlení přenosu a snížení zatížení CPU, nastavení přesměrování portů, odmítnutí paketů, které nesplňují NAT, odmítnutí paketů, které nemají veřejnou IP adresu, odmítnutí paketů, které jsou uvedeny v seznamu adres anebo nemají lokální IP adresu. Nejprve restartujeme router, z důvodu správného pořadí pravidel. V průběhu zadávání následujících pravidel nesmíme router restartovat.

/ip firewall filter
add action=fasttrack-connection chain=forward comment=FastTrack connection-state=established,related
add action=accept chain=forward comment="Established, Related" connection-state=established,related
add action=drop chain=input comment="Drop invalid" connection-state=invalid log=yes log-prefix=invalid place-before=2
add action=drop chain=forward comment="Drop invalid" connection-state=invalid log=yes log-prefix=invalid place-before=2
add action=drop chain=forward comment="Drop tries to reach not public addresses from LAN" dst-address-list=not_in_internet in-interface=bridge log=yes log-prefix=!public_from_LAN out-interface=!bridge place-before=2
add action=drop chain=forward comment="Drop incoming packets that are not NATted" connection-nat-state=!dstnat connection-state=new in-interface=ether1 log=yes log-prefix=!NAT place-before=2

add action=drop chain=forward comment="Drop incoming from internet which is not public IP" in-interface=ether1 log=yes log-prefix=!public src-address-list=not_in_internet place-before=2
add action=drop chain=forward comment="Drop packets from LAN that do not have LAN IP" in-interface=bridge log=yes log-prefix=LAN_!LAN src-address=!192.168.50.0/24 place-before=2 [26]

Definování seznamu adres

Na základě RFC6890 definujeme speciální IP adresy a jejich použití.

/ip firewall address-list
add address=0.0.0.0/8 comment=RFC6890 list=not_in_internet
add address=172.16.0.0/12 comment=RFC6890 list=not_in_internet
add address=192.168.0.0/16 comment=RFC6890 list=not_in_internet
add address=10.0.0.0/8 comment=RFC6890 list=not_in_internet
add address=169.254.0.0/16 comment=RFC6890 list=not_in_internet
add address=127.0.0.0/8 comment=RFC6890 list=not_in_internet
add address=224.0.0.0/4 comment=Multicast list=not_in_internet
add address=198.18.0.0/15 comment=RFC6890 list=not_in_internet
add address=192.0.0.0/24 comment=RFC6890 list=not_in_internet
add address=192.0.2.0/24 comment=RFC6890 list=not_in_internet
add address=198.51.100.0/24 comment=RFC6890 list=not_in_internet
add address=203.0.113.0/24 comment=RFC6890 list=not_in_internet
add address=100.64.0.0/10 comment=RFC6890 list=not_in_internet
add address=240.0.0.0/4 comment=RFC6890 list=not_in_internet
add address=192.88.99.0/24 comment="6to4 relay Anycast [RFC 3068]" list=not_in_internet [26]

5.1.17 Bezdrátová síť pro hosty

Ve firemním prostředí je nutné vytvořit bezdrátovou síť pro hosty, která bude oddělená od lokální sítě. Postup je analogický jako v případě vytváření předchozí bezdrátové sítě, viz kapitola 5.1.9. Rozdíl je pouze v tom, že budeme konfigurovat virtuální rozhraní. Virtuální rozhraní je závislé na fyzickém rozhraní pro bezdrátovou síť. Rozdíl v nastavení je pouze u DHCP (Dynamic Host Configuration Protokol) a firewallu. Pro vnitřní síť bude zabezpečovat služby DHCP a DNS server a pro veřejnou síť router. Následující konfigurace vychází z návodů pro router MikroTik [28].

Vytvoření profilu

/interface wireless security-profiles add authentication-types=wpa2-psk eap-methods="" mode=dynamic-keys name=Wifi-Firma-Free supplicant-identity="" wpa2-pre-shared-key=HesloProWifiFree

Vytvoření rozhraní

/interface wireless add comment="AP for guests" disabled=no keepalive-frames=disabled mac-address=E6:8D:8C:22:36:8C master-interface=wlan1 multicast-buffering=disabled name=wlan-guest ssid=Wifi-Firma-Free wds-cost-range=0 wds-default-cost=0 wps-mode=disabled security-profile=Wifi-Firma-Free

Rozsah adres pro DHCP

/ip pool add comment="DHCP pool for WIFI free" name=dhcp_pool_Wifi_Free ranges=192.168.100.20-192.168.100.200

Nastavení DHCP serveru

/ip dhcp-server add address-pool=dhcp_pool_Wifi_Free disabled=no interface=wlan-guest lease-time=1h name=Wifi_Free

Nastavení sítě a adresy routeru

/ip address add address=192.168.100.1/24 comment=Wifi-Firma-Free interface=wlan-guest network=192.168.100.0
/ip dhcp-server network add address=192.168.100.0/24 comment="WIFI free" dns-server=8.8.8.8,185.43.135.1 gateway=192.168.100.1 netmask=24

Překlad lokálních a veřejných adres

/ip firewall nat add action=masquerade chain=srcnat comment="Wifi free" ipsec-policy=out,none out-interface-list=WAN src-address=192.168.100.0/24

Nastavení pravidel firewallu

Nyní nastavíme pravidla pro IPv4. Nejprve restartujeme router, z důvodu správného pořadí pravidel.

Zakázání komunikace s lokální sítí a zpět

/ip firewall filter
add action=drop chain=forward comment="Disable communication between LAN and WIFI free" dst-address=192.168.100.0/24 src-address=192.168.50.0/24 place-before=7
add action=drop chain=forward comment=" Disable communication between WIFI free and LAN" dst-address=192.168.50.0/24 src-address=192.168.100.0/24 place-before=7

5.2 OpenVPN

Poslední fází nastavení routeru je vytvoření serveru VPN. Pro ukázku nastavení je vybrán OpenVPN server. Celá konfigurace OpenVPN je vytvořena podle [28], [49], [24].

Vytvoření certifikátů v OS routeru

Postup tvorby certifikátů se skládá z několika kroků. Nejdříve musíme certifikáty vytvořit, pak podepsat a nakonec distribuovat.

Vytvoření šablon certifikátů

V prvním kroku vytvoříme šablony certifikátů pro certifikační autoritu, server a klienta. Certifikační autorita má platnost certifikátu 730 dní a server s klientem 720 dní.

```
/certificate
add name=ca-template country=CZ state=CZ locality=Pardubice
organization=ComIntelligence common-name=myCa days-valid=730 key-size=4096 key-
usage=crl-sign,key-cert-sign
add name=server-template country=CZ state=CZ locality=Pardubice
organization=ComIntelligence common-name=serverCA days-valid=720 key-size=4096 key-
usage=digital-signature,key-encipherment,tls-server
add name=client-template country=CZ state=CZ locality=Pardubice
organization=ComIntelligence common-name=clientCA days-valid=720 key-size=4096 key-
usage=tls-client unit=VPN-Users
```

Podepsání certifikátů

V tomto kroku podepíšeme výše vytvořené certifikáty certifikační autoritou. Podepsání certifikátů může trvat delší dobu. Před podepisováním je doporučeno restartovat router (kvůli uvolnění systémových prostředků). Pokud se objeví hlášení routeru „*action timed out - try again*“, je nutné vyčkat do podepsání certifikátu.

```
/certificate
sign ca-template name=ca-certificate
sign server-template name=serverCerticate ca=ca-certificate
sign client-template name=clientCertificate ca=ca-certificate
```

Označení důvěryhodnosti

Před exportováním certifikátu je nutné, aby vytvořené certifikáty byly označeny jako důvěryhodné, tj. flag = T.

```
/certificate
set ca-certificate trusted=yes
set serverCerticate trusted=yes
```

```
/certificate print
Flags: K - private-key, L - crl, C - smart-card-key, A - authority, I - issued, R -
revoked, E - expired, T - trusted
#      NAME               COMMON-NAME  SUBJECT-NAME FINGERPRINT
0 KAT  ca-certificate           myCa
       a338fd1e08bb90...
1 KIT  serverCerticate     serverCA                              ebceaab3469783...
2 KI   clientCertificate   clientCA                              79e1130d72bd24...
3      ca-template         myCa
```

Export certifikátů

Při exportu certifikátů je nutné u certifikátu pro klienta zadat heslo.

/certificate
export-certificate ca-certificate
export-certificate clientCertificate export-passphrase="HesloCertifikatu"

Konfigurace serverové části OpenVPN

V této kapitole je popsáno nastavení serverové části OpenVPN. V následujících příkazech je vytvořen profil pro připojení k VPN serveru, rozsah adres pro VPN klienty a rozhraní VPN.

Rozsah adres pro DHCP

Rozsah adres pro VPN klienty nastavíme z nové sítě pro VPN 192.168.51.0/24 v rozsahu posledních oktetů od 20 do 200.

/ip pool add name="VPN_pool" ranges=192.168.51.20-192.168.51.200 comment="DHCP pool for VPN clients"

Vytvoření profilu

Při vytvoření profilu definujeme povinné šifrování, rozsah adres a DNS server.

/ppp profile add name="Profile-OpenVPN " use-encryption=yes local-address=VPN_pool dns-server=192.168.50.5 remote-address=VPN_pool

Vytvoření uživatele

Uživateli definujeme výchozí profil a heslo. Pro každého uživatele je nutné vytvořit nový uživatelský účet pro přihlášení k VPN.

/ppp secret add name=VPNUser profile=Profile-OpenVPN service=ovpn password=HesloDoOVPN

Nastavení rozhraní

V konečné fázi vytvoření VPN serveru musíme definovat VPN rozhraní. Definujeme výchozí profil, že se jedná o certifikační server a že je požadován klientský certifikát. Autentizace bude prováděna za pomocí sha1 a šifrování na základě AES 256 bitů.

/interface ovpn-server server set default-profile=Profile-OpenVPN certificate=serverCerticate require-client-certificate=yes auth=sha1 cipher=aes256 enabled=yes

5.2.1 OpenVPN a firewall

Posledním krokem v konfiguraci routeru je nastavení firewallu pro povolení komunikace OpenVPN portu, respektive připojení k VPN serveru.

/ip firewall filter add chain=input protocol=tcp dst-port=1194 action=accept comment="Allow OpenVPN connection" place-before=7 [28], [49], [24]

Vytvoření seznamu povolených IP adres

/ip firewall address-list
add address=192.168.51.0/24 list=allowed_to_router comment="OVPN LAN" [26]

Povolení komunikace mezi interní sítí a VPN sítí

/ip firewall filter
add action=accept chain=input src-address-list=allowed_to_router comment="Allowed communication between own networks" place-before=4
add action=accept chain=forward src-address-list=allowed_to_router comment="Allowed communication between own networks" place-before=4 [28], [49], [24]

5.2.2 Instalace a konfigurace OpenVPN klienta

Nejprve je nutné stáhnout aplikaci OpenVPN ze stránek výrobce a nainstalovat ji. V době vytváření této práce byla dostupná verze 2.4.7. Instalační soubor stáhneme v podobě EXE instalačního souboru z adresy https://openvpn.net/community-downloads/. Veškeré volby v průvodci instalace ponecháme ve výchozím nastavení. V následujícím odstavci je popsána konfigurace v rámci 64bitového operačního systému Windows. V prvním kroku vytvoříme konfigurační soubor pro OpenVPN.

Vytvoření konfiguračního souboru

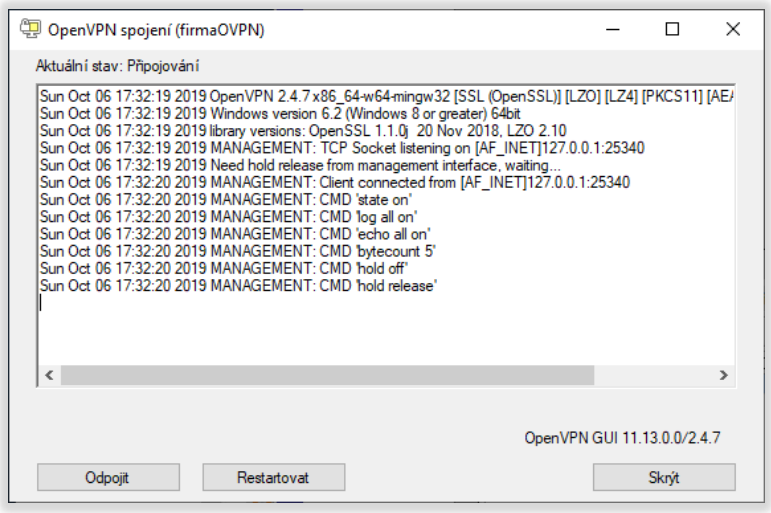
Vytvoříme soubor s názvem firmaOVPN.ovpn. Tento soubor upravíme v textovém editoru, jako je například Notepad nebo PSPad. Pro přehlednost jsou poznámky ke konfiguraci uvedeny v konfiguračním souboru podle [28], [49], [24], [30]. V našem případě pro účely testování není nastavena veřejná IP. Vyexportované certifikáty klienta a certifikační autority, včetně konfiguračního souboru, nakopírujeme do „*C:\Program Files\OpenVPN\config*“. Po spuštění OpenVPN klienta je nutné zadat uživatelské přístupové údaje k VPN a heslo k privátnímu klíči.

Obsah konfiguračního souboru *firmaOVPN.ovpn*

```
#Určení konfigurace
client
dev tun
#Povolení protokolu TCP
proto tcp
#Definování veřejné IP adresy a portu nebo názvu FDQN serveru OpenVPN
```

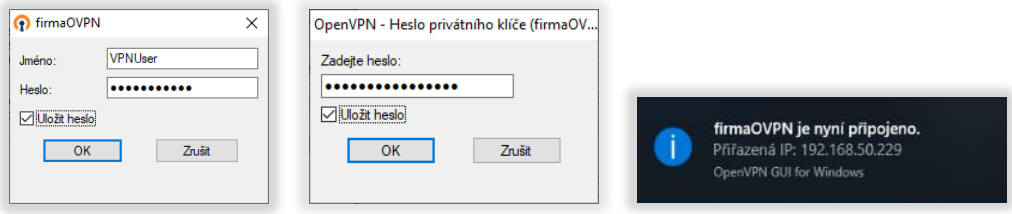
```
remote 192.168.3.254 1194
#Nekonečné opakování při chybě překladu názvu hostitele (doménového názvu).
resolv-retry infinite
#Přidělování dynamických portů pro vracení paketů
nobind
#Ponechání klíčů při restartu
persist-key
persist-tun
#Nastavení cest k certifikátům a klíči
ca cert_export_ca-certificate.crt
cert cert_export_clientCertificate.crt
key cert_export_clientCertificate.key
#Vyžaduje podepsání certifikátu serverem
remote-cert-tls server
#Definice algoritmu šifrování
cipher AES-256-CBC
auth SHA1
#Uložení autentizačních údajů do virtuální paměti
auth-user-pass
#Nastavení přímé brány – vhodné pro potlačení soukromých podsítí
redirect-gateway def1
#Nastavení úrovně auditování je doporučeno ponechat 3
verb 3
```

Na následujících obrázcích je vyobrazen postup při přihlášení k OpenVPN serveru. Poslední obrázek nám zobrazí, pod kterou IP adresou jsme přihlášeni do vzdálené sítě.



Obrázek 15: Úvodní obrazovka po přihlášení k OpenVPN serveru

Zdroj: vlastní zpracování



Obrázek 16: Přihlášení k OpenVPN serveru

Zdroj: vlastní zpracování

5.3 Instalace operačního systému serveru

V této kapitole provedeme instalaci serveru včetně bezpečného nastavení základních služeb. Serverový operační systém Ubuntu 18.04 LTS je distribuován jako svobodný software, který budeme instalovat na virtuální stroj, vytvořený na platformě Hyper-V. Jednotlivé podkapitoly obsahují podrobné informace, potřebné pro správnou konfiguraci operačního systému a jeho služeb. Následující postup je analogicky rozdělen do několika částí. V první části po zavedení instalace OS provedeme nastavení základních voleb v průvodci instalace. Dále navazuje změna oprávnění pro vzdálené přihlášení, instalace podpůrných aplikací a nastavení síťového rozhraní. Celá tato kapitola, včetně podkapitol, vychází z oficiálních manuálů pro Ubuntu [52], [51], [48] a vlastního dopracování za pomocí manuálů v OS „*man*“ a popisů v originálních konfiguračních souborech vzhledem k předem stanoveným cílům. Další použité zdroje jsou citovány v textu.

Syntaxe manuálové stránky

man <služba nebo program>

5.3.1 Instalace a prvotní přihlášení k OS

Instalace operačního systému je jedním z nejdůležitějších kroků. Před započetím instalace musíme mít ujasněno, jakou úlohu bude server plnit. Zda se bude jednat o řadič domény, webový server, kolik serverů ve virtuálním prostředí bude nasazeno apod. Tyto poznatky je nutné řetězit a podle nároků zvolit HW konfiguraci fyzického serveru. V návaznosti na HW konfiguraci serveru zvolíme i prostředky, které budou vyčleněny pro virtuální stroje. U těchto virtuálních strojů je nutné počítat s minimálními nároky na HW, jako při instalaci fyzického serveru. Na základě ujasnění výše uvedených poznatků provedeme vyčlenění diskového prostoru fyzického HDD, na kterém vytvoříme virtuální disky o požadované velikosti.

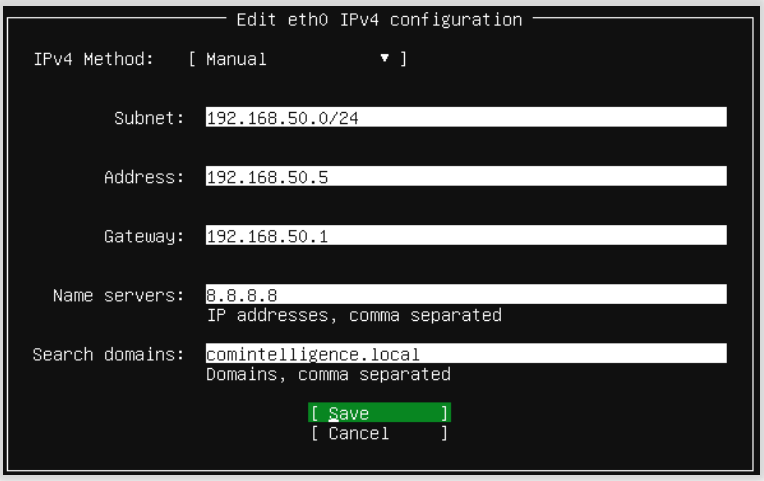
Po nastavení zdroje zavedení instalace operačního systému a spuštění instalace se objeví výchozí menu s možnostmi instalace, viz obrázek 17.

Obrázek 17: Výchozí menu instalace OS Ubuntu

Zdroj: vlastní zpracování

V následujícím kroku vybereme lokalizaci systému. Zvolíme angličtinu, jelikož čeština v instalaci není podporována.

Pokračujeme nastavením síťových rozhraní. V průběhu instalace je nutné nastavit alespoň jedno rozhraní, jehož fyzické připojení a nastavení umožní instalačnímu programu komunikaci se servery v internetu, viz obrázek 18. Součástí nastavení je také možnost zadání adresy proxy serveru.



Obrázek 18: Nastavení síťového rozhraní

Zdroj: vlastní zpracování

Následuje nastavení zrcadla (mirror) pro stahování balíčků. Toto nastavení ponecháme na výchozí hodnotě.

Dostáváme se k dalšímu důležitému nastavení oddílů disků (partition) a souborového systému. Na základě zmíněných poznatků vytvoříme jednotlivé oddíly se souborovým systémem v pořadí, které je uvedené v následující tabulce.

Tabulka 3: Nastavení oddílů disků a souborových systémů

Pč.	**1**	**2**	**3**	**4**	**5**
Partition	Primární	Primární	Primární	Primární	Primární
Velikost	50 GB	512 MB	20 GB	10 GB	500 GB
Souborový systém	EXT4	FAT32	EXT4	swap	EXT4
Přípojný bod	/	boot/EFI	/var	/swap	/Data
Poznámka		Vytváří se automaticky při /			

Zdroj: vlastní zpracování

Po definování oddílů disků a souborových systémů potvrdíme operaci, která je nevratná a dojde ke smazání disků.

Tímto se dostáváme k dalšímu důležitému kroku. Nastavení názvu serveru, pod kterým bude vystupovat v síti (hostname), a identifikační údaje, pod kterými se bude možné přihlásit k serveru, jsou vyobrazeny na obrázku 20. Název musíme mít dopředu promyšlený, jelikož následná změna názvu je v této verzi problematická.

Obrázek 19: Nastavení identifikace serveru a účtu uživatele

Zdroj: vlastní zpracování

Pokračujeme nastavením vzdáleného přístupu prostřednictvím SSH protokolu (OpenSSH). Tento protokol povolíme z důvodu zabezpečeného vzdáleného přístupu do serveru.

Následuje výběr balíčků k instalaci, které nebudeme instalovat. Po ukončení instalace provedeme restart serveru.

5.4 Instalace a nastavení základních služeb

Po prvním přihlášení k serveru provedeme úpravy, které poskytnou rychlejší konfiguraci serveru. Sice tím porušíme doporučení nepovolovat účet root pro přímé vzdálené připojení protokolem SSH, ale po ukončení konfigurace systému nastavíme zákaz přihlášení zpět. Následující konfigurace jsou převážně prováděny v textovém editoru Nano. Před každým zásahem do konfiguračního souboru vytvoříme kopii tohoto souboru.

V prvním kroku nastavíme příkazem „*sudo passwd root*“ heslo pro uživatele root.

5.4.1 Nastavení OpenSSH serveru

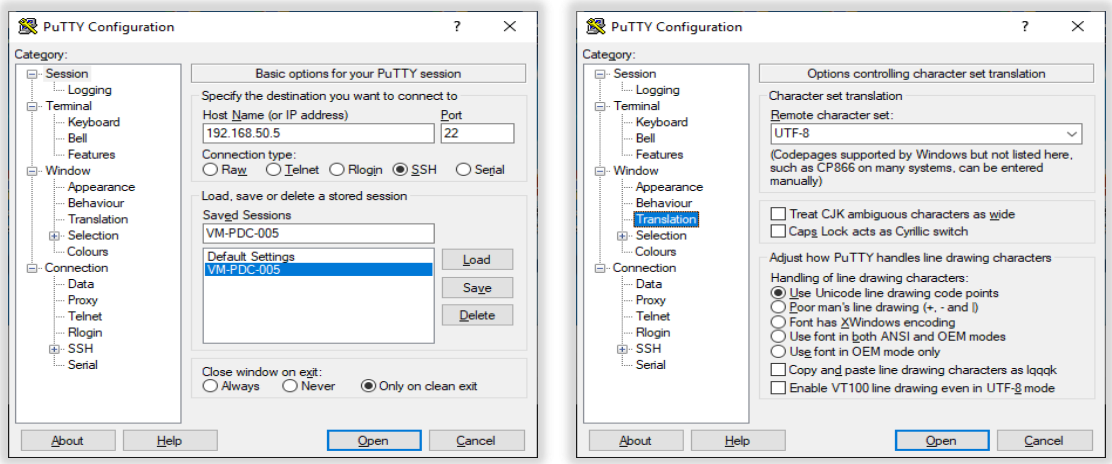
Následnou konfigurací povolíme přihlášení uživatele root k OpenSSH serveru. V konfiguračním souboru změníme hodnotu „*PermitRootLogin prohibit*“ na „*PermitRootLogin yes*“ a provedeme restartování služby SSH.

cp /etc/ssh/sshd_config /etc/ssh/sshd_config.beforeRoot
nano /etc/ssh/sshd_config
`PermitRootLogin prohibit-password ----> PermitRootLogin yes`
Uložit konfiguraci pomocí klávesové zkratky CTRL+X.

service ssh restart
Provedeme restartování služby SSH.

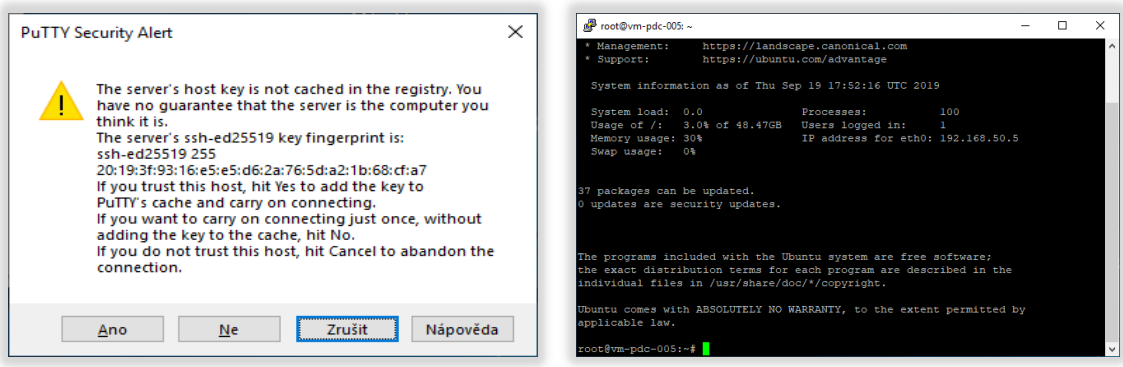
Přihlášení prostřednictvím SSH

Pro přihlášení k serveru použijeme aplikaci PuTTY, která nám dovolí vkládat příkazy přímo do serveru z datové schránky ovládacího počítače. Před prvním přihlášením je nutné provést nastavení adresy IP a kódování, viz obrázek 20. Při přihlášení je nutné potvrdit bezpečnostní hlášení, viz obrázek 21.



Obrázek 20: Nastavení aplikace PuTTY

Zdroj: vlastní zpracování



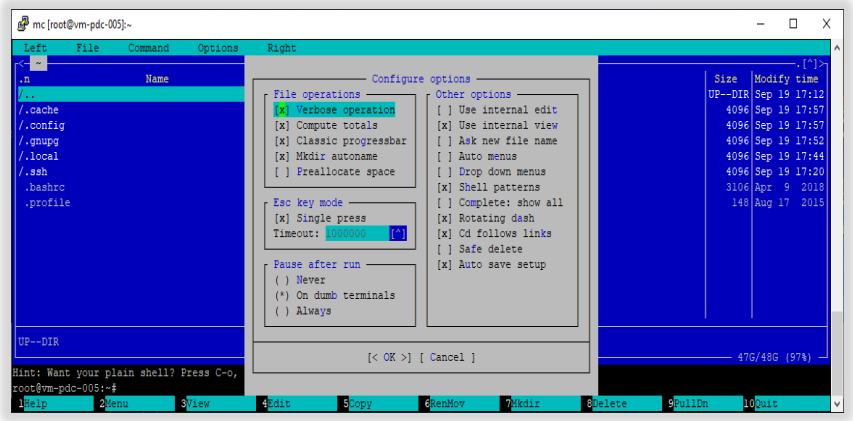
Obrázek 21: Přihlášení prostřednictvím aplikace PuTTY

Zdroj: vlastní zpracování

5.4.2 Instalace programu Midnight Commander

Z důvodu komfortu a přehlednosti nainstalujeme souborový manager. V našem případě se jedná o Midnight Commander (MC). Po instalaci MC je nutné provést základní nastavení, viz obrázek 22. Instalace v OS Ubuntu je prováděna příkazem „*apt-get*“ v různých syntaxích podle manuálu. Balíčky, které nejsou součástí přímé distribuce ze zdroje Ubuntu, je možné stáhnout přímo z internetu nebo zdroj zadat do repositáře APT. Prostřednictvím následujících příkazů zavedeme repositář Universe [18].

cp /etc/apt/sources.list /etc/apt/sources.list.orig.beforeUniverse
add-apt-repository universe
sudo apt-get install mc



Obrázek 22: Nastavení programu Midnight Commander

Zdroj: vlastní zpracování

5.4.3 Instalace WebMin

Dalším vhodným nástrojem pro ovládání serveru je WebMin. Jedná se o webovou aplikaci pro administrátory, v které je možné provádět nastavení a monitoring systému. WebMin není v repositáři Ubuntu, proto ho musíme přidat následujícími příkazy [55].

cp /etc/apt/sources.list /etc/apt/sources.list.orig.beforeWebMin

Přidání GPG key

wget -qO- http://www.webmin.com/jcameron-key.asc | sudo apt-key add

Přidání repository

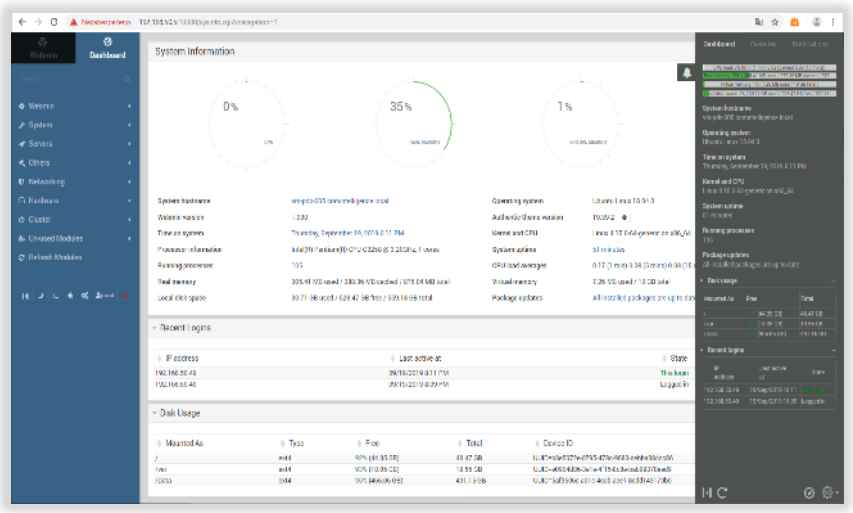
sudo add-apt-repository "deb http://download.webmin.com/download/repository sarge contrib"

Provedení instalace

apt-get update
apt-get upgrade
apt-get install webmin

Přihlášení k aplikaci WebMin

Po instalaci je možné se přihlásit prostřednictvím webového prohlížeče, a to zadáním URL s portem „*https://192.168.50.5:10000*“. Po zadání uživatelského jména root a jeho hesla se zobrazí úvodní obrazovka, viz obrázek 23.



Obrázek 23: Úvodní obrazovka WebMin

Zdroj: vlastní zpracování

5.4.4 Nastavení síťového rozhraní

Po instalaci podpůrných programů se dostáváme k přípravě systému pro instalaci aplikací potřebných pro korektní funkcionalitu řadiče domény. Než začneme konfiguraci serveru, je nutné připravit síťové rozhraní. Verze Ubuntu 18.04 používá odlišné nastavení rozhraní v porovnání s předešlými verzemi. Je nutné si dávat pozor na správnou syntaxi a dodržování celé struktury konfiguračního souboru. Při nekorektním nastavení dojde k odpojení sítě a přerušení komunikace serveru s SSH klientem.

Z důvodu připojení do internetu a stahování aplikací musíme ponechat jiný DNS, než je plánován. Ostatní síťové volby a hodnoty připravíme pro nasazení řadiče domény [48], viz následující konfigurace.

cp /etc/netplan/50-cloud-init.yaml /etc/netplan/00-eth0-network-card.yaml
mv /etc/netplan/50-cloud-init.yaml /etc/netplan/50-cloud-init.yaml.orig

nano /etc/netplan/00-eth0-network-card.yaml

```
network:
    ethernets:
        eth0:
            addresses:
            - 192.168.50.5/24
            dhcp4: false
            gateway4: 192.168.50.1
            nameservers:
                addresses:
                - 8.8.8.8
                - 127.0.0.1
                search:
                - comintelligence.local
    version: 2
```

netplan generate
netplan apply
Generování a aplikace nastavení.

Kontrola resolv.conf.d

V konfiguračním souboru resolv.conf jsou nastaveny údaje, které slouží k překladům názvů.. Následující konfiguraci v žádném případě neměníme, pouze kontrolujeme. Adresa IP 127.0.0.53 udává, že překlad zabezpečí vnitřní resolver (systemd-resolved). [52], [48]

nano /etc/resolv.conf

```
nameserver 127.0.0.53
options edns0
search comintelligence.local
```

Neměnit, pouze zkontrolovat shodnost údajů s /etc/netplan/*.yaml.

Kontrola host.conf

Konfigurační soubor host.conf udává pořadí vyhledávání překladů adres. První je soubor s definovanými překlady a další je DNS server. Hodnota „*multi on*“ znamená definování vracení všech validních adres ze souboru hosts, který obsahuje ručně definované překlady. [52], [48]

nano /etc/host.conf

```
order hosts,bind
multi on
```

Kontrola hostname

V průběhu instalace byl nastaven název serveru, který je uložen v níže uvedeném souboru. Následující příkazy zobrazí výpis nastavení [48].

nano /etc/hostname

```
vm-pdc-005
```

Neměnit, pouze zkontrolovat název serveru.

Kontrola zavedení názvu serveru

hostname

```
vm-pdc-005
```

Výpis údajů o systému

hostnamectl

```
  Static hostname: vm-pdc-005
        Icon name: computer-vm
          Chassis: vm
       Machine ID: 56835f25cc884daa83021e44bd7ed059
          Boot ID: 8065cc140f2f478787788b98ed73ec79
    Virtualization: microsoft
  Operating System: Ubuntu 18.04.3 LTS
            Kernel: Linux 4.15.0-64-generic
      Architecture: x86-64
```

Nastavení hosts

Konfigurační soubor hosts slouží pro statické překlady adres a je ho nutné upravit podle aktuální IP adresace. [38]

cp /etc/hosts /etc/hosts.orig
nano /etc/hosts

```
127.0.0.1       localhost.localdomain   localhost localhost4
localhost4.localdom$
192.168.50.5    vm-pdc-005. comintelligence.local vm-pdc-005
# The following lines are desirable for IPv6 capable hosts
::1     localhost.localdomain localhost localhost6 localhost6.localdomain6
ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Zavedení a kontrola nastavení

Poslední fází při nastavování síťových rozhraní je zavedení a kontrola výše provedených konfigurací.

hostname restart
netplan apply
V případě, že networking hlásí chybu nebo se nezmění údaje, je nutné restartovat server „*shutdown -r now*“.
Do vyřešení problému nepokračovat!

Kontrola nastavení LAN

ifconfig

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.50.5  netmask 255.255.255.0  broadcast 192.168.50.255
        inet6 fe80::215:5dff:fe32:3101  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:32:31:01  txqueuelen 1000  (Ethernet)
        RX packets 44591  bytes 58986645 (58.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23510  bytes 5294071 (5.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 284  bytes 27058 (27.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 284  bytes 27058 (27.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Restartování serveru

Před další konfigurací provedeme restartování serveru příkazem „*reboot*“.

5.4.5 Aktualizace serveru

Před dalším pokračováním pomocí utility APT provedeme kontrolu a instalaci aktualizací, viz následující příkazy a výpisy z OS.

apt-get update

```
Hit:1 http://cz.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://cz.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Ign:3 http://download.webmin.com/download/repository sarge InRelease
Get:4 http://cz.archive.ubuntu.com/ubuntu bionic-backports InRelease [74.6 kB]
Hit:5 http://download.webmin.com/download/repository sarge Release
Get:6 http://cz.archive.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Fetched 252 kB in 1s (278 kB/s)
Reading package lists... Done
```

apt-get upgrade

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  dpkg
1 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,136 kB of archives.
After this operation, 4,096 B of additional disk space will be used.
Do you want to continue? [Y/n]
```

Výpis nesmí obsahovat chybové hlášení.

5.5 Samba 4 s interním DNS

V této kapitole se dostáváme k podstatě celé této práce. Sambu nastavíme tak, aby se chovala jako řadič domény s AD.

V prvním kroku musíme připravit prostředí Linuxu pro instalaci Samby. Podpůrné balíčky instalujeme vždy vzhledem k požadované funkcionalitě Samby. Samba může sloužit jen jako prostředek pro sdílení, nebo sofistikovaněji jako řadič domény s rozšířenou službou.

Celá tato kapitola včetně podkapitol vychází z oficiálních manuálů pro Samba 4 [38], [48], vlastního dopracování na základě dílčích manuálů v OS „*man*“ a popisů v originálních konfiguračních souborech. Další použité zdroje jsou citovány v textu.

5.5.1 Instalace závislých a podpůrných balíčků

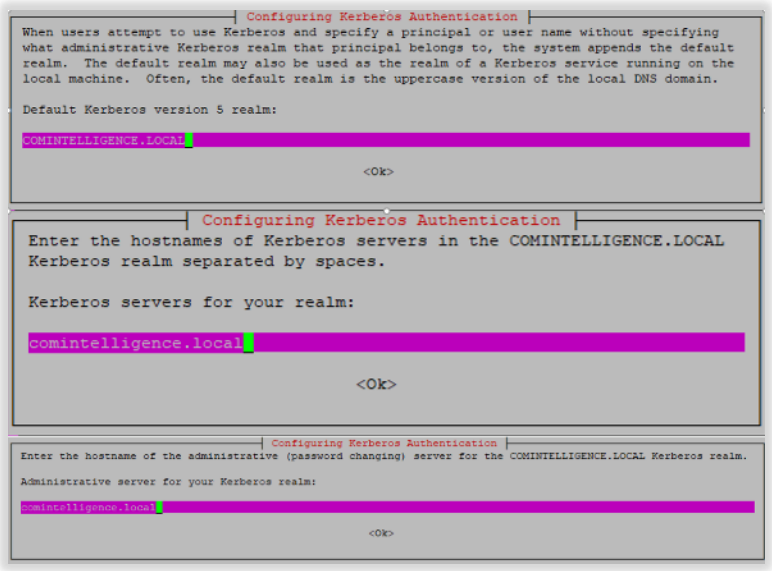
Následující příkaz nainstaluje všechny potřebné balíčky.

apt-get install acl attr autoconf bison build-essential debhelper dnsutils docbook-xml docbook-xsl flex gdb krb5-user libacl1-dev libaio-dev libattr1-dev libblkid-dev libbsd-dev libcap-dev libcups2-dev libjson-perl libpopt-dev libreadline-dev perl perl-modules pkg-config python-all-dev python-dev python-dnspython python-crypto xsltproc zlib1g-dev libjansson-dev libarchive-dev libgnutls28-dev libgpgme-dev nettle-dev python-dbg python3-dnspython python-markdown python3-markdown python3-dev liblmdb-dev lmdb-utils libldap2-dev libncurses5-dev libpam0g-dev libparse-yapp-perl libsystemd-dev libgpgme11-dev python-m2crypto python-gpg python3-gpg winbind libnss-winbind libpam-winbind smbclient

Konfigurace Kerberos

Protokol Kerberos nám zprostředkovává bezpečnou autentizaci v nezabezpečené síti. V průběhu výše uvedené instalace budeme dotázáni na hodnoty protokolu.

V následujícím pořadí zadáme hodnoty říše (oblast) <*COMINTELLIGENCE.LOCAL*> a pak dvakrát název serveru v podobě domény <*comintelligence.local*>, viz obrázek 24.



Obrázek 24: Nastavení Kerberos při instalaci

Zdroj: vlastní zpracování

Instalace resolvconf

Z důvodu instalace SAMBA 4 s interním DNS je nutné nainstalovat balíček pro ovládání resolveru.

apt-get install resolvconf

5.5.2 Synchronizace času

Při provozování domény s AD je nutné mít synchronizovaný čas. Z toho důvodu provedeme nastavení NTP klienta a serveru.

Instalace NTP klienta

apt-get install ntp ntpdate
Klienta instalujeme, pokud není nainstalován.

sntp --version
```
sntp 4.2.8p10@1.3728-o (1)
```

Nastavení časových serverů

Deaktivujeme výchozí časové servery a nahradíme je vlastními, včetně povolení dotazování klientů AD.

service ntp stop
cp /etc/ntp.conf /etc/ntp.conf.orig.beforeNTP
nano /etc/ntp.conf
```
ntpsigndsocket /var/lib/samba/ntp_signd/
# Use servers from the NTP Pool Project.
# pool 0.ubuntu.pool.ntp.org iburst
# pool 1.ubuntu.pool.ntp.org iburst
# pool 2.ubuntu.pool.ntp.org iburst
# pool 3.ubuntu.pool.ntp.org iburst
# Use Ubuntu's ntp server as a fallback.
# pool ntp.ubuntu.com
#Czech NTP servers
server tik.cesnet.cz    #CesNET NTP
server ntp.nic.cz       #NIC NTP
```

Nastavení aktuálního času

timedatectl set-timezone Europe/Prague
ntpdate -B tik.cesnet.cz
```
30 Sep 20:04:28 ntpdate[13615]:adjust time server 195.113.144.201 offset 0.0534 sec
```
sudo service ntp start

Kontrola nastavení času

date
```
Mon Sep 30 20:04:51 CEST 2019
```

Kontrola NTP služby

service ntp status
```
● ntp.service - Network Time Service
   Loaded: loaded (/lib/systemd/system/ntp.service; enabled; vendor preset: enab
   Active: active (running) since Mon 2019-09-30 20:04:28 CEST; 1min 7s ago
..
..
```

Vytvoření vlastního NTP serveru

Nejdříve nainstalujeme službu NTP a poté ji nastavíme jako NTP server pro síť 192.168.50.0/24.

Instalace NTP serveru a nastavení oprávnění

sudo apt-get install ntpdate
sudo chown root:ntp /var/lib/samba/ntp_signd/
sudo chmod 750 /var/lib/samba/ntp_signd/

Konfigurace NTP serveru

V konfiguraci upravíme, nebo přidáme „*ntpsigndsocket*“.

cp /etc/ntp.conf /etc/ntp.conf.orig.beforeNTP
nano /etc/ntp.conf

```
#restrict -4 default kod notrap nomodify nopeer noquery limited
#restrict -6 default kod notrap nomodify nopeer noquery limited
#restrict source notrap nomodify noquery
ntpsigndsocket /var/lib/samba/ntp_signd
restrict 192.168.50.0 mask 255.255.255.0 notrap nomodify noquery
```

Kontrola nastavení NTP serveru

systemctl restart ntp
netstat -tulpn | grep ntp

```
udp        0      0 192.168.50.5:123        0.0.0.0:*
13760/ntpd
udp        0      0 127.0.0.1:123           0.0.0.0:*
13760/ntpd
udp        0      0 0.0.0.0:123             0.0.0.0:*
..
..
```

ntpq -p

```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 tik.cesnet.cz   195.113.144.238  2 u   36   64    1   10.991    0.751   0.000
 ntp.nic.cz      .GPS.            1 u   33   64    1   11.080    0.570   0.000
```

Vypnutí vnitřní služby synchronizace času

Před zapnutím NTP serveru vypneme vnitřní systém synchronizace času příkazem „*timedatectl set-ntp no*“ [13].

Zapnutí NTP

systemctl enable ntp
systemctl start ntp
systemctl status ntp.service

5.5.3 Instalace a konfigurace Samba 4

Sambu instalujeme z repositáře Ubuntu, jež je pro něj kompilována.

Instalace prostřednictvím Apt

apt install samba

```
Reading package lists... Done
..
0 upgraded, 11 newly installed, 0 to remove and 0 not upgraded.
..
```

Konfigurace Samba 4 s interním DNS

Před samotnou konfigurací ukončíme a vypneme zavádění všech deamonů Samba 4.

systemctl stop samba-ad-dc.service smbd.service nmbd.service winbind.service
systemctl disable samba-ad-dc.service smbd.service nmbd.service winbind.service

Provedení kontroly instalace

Před konfigurací řadiče domény zkontrolujeme verzi a cesty uvedené v Samba 4.

samba -V

```
Version 4.7.6-Ubuntu
```

Zobrazení verze Samby a informace o sestavení.

samba -b

```
Samba version: 4.7.6-Ubuntu
Build environment:
Paths:
   BINDIR: /usr/bin
   SBINDIR: /usr/sbin
   CONFIGFILE: /etc/samba/smb.conf
   NCALRPCDIR: /var/run/samba/ncalrpc
   LOGFILEBASE: /var/log/samba
   LMHOSTSFILE: /etc/samba/lmhosts
   DATADIR: /usr/share
   MODULESDIR: /usr/lib/x86_64-linux-gnu/samba
   LOCKDIR: /var/run/samba
   STATEDIR: /var/lib/samba
   CACHEDIR: /var/cache/samba
   PIDDIR: /var/run/samba
   PRIVATE_DIR: /var/lib/samba/private
   CODEPAGEDIR: /usr/share/samba/codepages
   SETUPDIR: /usr/share/samba/setup
   WINBINDD_SOCKET_DIR: /var/run/samba/winbindd
   NTP_SIGND_SOCKET_DIR: /var/lib/samba/ntp_signd
```

Pokud jsou nefunkční výpisy, je nutné ručně spustit SMB příkazem „*Samba start*“.

ps ax | egrep "samba|smbd|nmbd|winbindd"

```
17505 pts/3    S+     0:00 grep -E --color=auto samba|smbd|nmbd|winbindd
```

Kontrola spuštěných služeb.

smbd -b | grep "CONFIGFILE"

```
CONFIGFILE: /etc/samba/smb.conf
```

Umístění smb.conf.

hostname

```
vm-pdc-005
```

Kontrola hostname. Pokud hostname obsahuje název restart, pak je nutné provést restart OS.

nano /etc/hosts
Kontrola obsahu souboru hosts.

Nastavení DNS a překladů

V konfiguraci síťového rozhraní odstraníme všechny DNS servery, kromě vlastního serveru.

nano /etc/netplan/00-eth0-network-card.yaml

```
network:
    ethernets:
        eth0:
            addresses:
            - 192.168.50.5/24
            dhcp4: false
            gateway4: 192.168.50.1
            nameservers:
                addresses:
                - 127.0.0.1
                search:
                - comintelligence.local
    version: 2
```

Vypnutí resolveru

Máme již nainstalovány všechny potřebné balíčky a můžeme tedy vypnout překládání názvů.

systemctl disable systemd-resolved.service && service systemd-resolved stop
netplan generate && netplan apply
Generování a aplikace nastavení.

Restartování serveru

Před konfigurací řadiče domény je doporučené restartovat server příkazem „*reboot*“.

Vytvoření PDC s Active Directory

V prvním kroku odstraníme výchozí konfiguraci.

mv /etc/samba/smb.conf smb.conf.orig.beforeConfigurationSamba
Odstranění výchozí konfigurace.

Po odstranění konfiguračního souboru spustíme neinteraktivní konfiguraci řadiče domény s AD. Cílem je vytvoření řadiče domény na úrovni Windows Server 2008, což zrealizujeme následujícím příkazem. Syntaxí definujeme vytvoření řadiče domény, povolení ukládání atributů z Linuxu do AD, doménu, heslo administrátora, roli serveru a interní DNS.

samba-tool domain provision --use-rfc2307 --realm comintelligence.local --domain COMINTELLIGENCE --adminpass HesloProAdministrátora --server-role=dc --dns-backend=SAMBA_INTERNAL

```
No nameserver found in /etc/resolv.conf
Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
```

```
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=comintelligence,DC=local
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=comintelligence,DC=local
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba AD has been generated at
/var/lib/samba/private/krb5.conf
Setting up fake yp server settings
Once the above files are installed, your Samba AD server will be ready to use
Server Role:           active directory domain controller
Hostname:              vm-pdc-005
NetBIOS Domain:        COMINTELLIGENCE
DNS Domain:            comintelligence.local
DOMAIN SID:            S-1-5-21-3630673056-3893501400-3183116740
```

Kontrola vytvořeného řadiče domény

samba-tool domain level show

```
Domain and forest function level for domain 'DC=comintelligence,DC=local'
Forest function level: (Windows) 2008 R2
Domain function level: (Windows) 2008 R2
Lowest function level of a DC: (Windows) 2008 R2
```

Nastavení Kerberos pro Samba

Následujícím příkazem přesuneme vytvořený konfigurační soubor protokolu Kerberos a navážeme na něj symbolický link. Konfigurační soubor musí obsahovat níže uvedené volby a hodnoty.

mv /etc/krb5.conf /etc/krb5.conf.orig.beforeSamba
mv /var/lib/samba/private/krb5.conf /etc/krb5.conf
ln -s /etc/krb5.conf /var/lib/samba/private/
cat /etc/krb5.conf
cat /var/lib/samba/private/krb5.conf

```
 [libdefaults]
        default_realm = COMINTELLIGENCE.LOCAL
        dns_lookup_realm = false
        dns_lookup_kdc = true
```

Výpisy z obou souborů musí být totožné.

Příkazy pro ovládání Samba

systemctl unmask samba-ad-dc
systemctl enable samba-ad-dc

```
Synchronizing state of samba-ad-dc.service with SysV service script with
/lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable samba-ad-dc
```

Povolení automatického spuštění služby.

systemctl daemon-reload
Zavedení systemd rekonfigurace.

systemctl disable samba-ad-dc
Zakázání spuštění služby.

systemctl start samba-ad-dc
systemctl stop samba-ad-dc
systemctl restart samba-ad-dc
systemctl daemon-reload
Spuštění, zastavení, restart, znovunačtení služby.

systemctl status samba-ad-dc

```
● samba-ad-dc.service - Samba AD Daemon
   Loaded: loaded (/lib/systemd/system/samba-ad-dc.service; enabled; vendor pres
   Active: active (running) since Wed 2019-09-25 17:35:21 UTC; 11ms ago
     Docs: man:samba(8)
           man:samba(7)
           man:smb.conf(5)
 Main PID: 1916 (samba)
   Status: "winbindd: ready to serve connections..."
    Tasks: 24 (limit: 966)
   CGroup: /system.slice/samba-ad-dc.service
           ├─1916 /usr/sbin/samba --foreground --no-process-group
           ..
           ├─1950 /usr/sbin/smbd -D --option=server role check:inhibit=yes --for
           ├─1951 /usr/sbin/samba --foreground --no-process-group
           ..
           ├─1956 /usr/sbin/winbindd -D --option=server role check:inhibit=yes -
           ├─1957 /usr/sbin/samba --foreground --no-process-group
           ..
           ├─1961 /usr/bin/python2.7 /usr/sbin/samba_dnsupdate
           ├─1962 /usr/sbin/samba --foreground --no-process-group
           ├─1963 /usr/bin/python2.7 /usr/sbin/samba_spnupdate
           ├─1966 /usr/sbin/smbd -D --option=server role check:inhibit=yes --for
           └─1967 /usr/sbin/smbd -D --option=server role check:inhibit=yes --for

Sep 25 17:35:20 vm-pdc-005 systemd[1]: Starting Samba AD Daemon...
Sep 25 17:35:20 vm-pdc-005 samba[1916]: [2019/09/25 17:35:20.698196,  0] ../sour
Sep 25 17:35:20 vm-pdc-005 samba[1916]:   samba version 4.7.6-Ubuntu started.
Sep 25 17:35:20 vm-pdc-005 samba[1916]:   Copyright Andrew Tridgell and the Samb
Sep 25 17:35:20 vm-pdc-005 samba[1916]: [2019/09/25 17:35:20.827350,  0] ../sour
Sep 25 17:35:20 vm-pdc-005 samba[1916]:   samba: using 'standard' process model
Sep 25 17:35:21 vm-pdc-005 winbindd[1956]: [2019/09/25 17:35:21.051953,  0] ../s
Sep 25 17:35:21 vm-pdc-005 winbindd[1956]:   initialize_winbindd_cache: clearing
Sep 25 17:35:21 vm-pdc-005 systemd[1]: Started Samba AD Daemon.
Sep 25 17:35:21 vm-pdc-005 winbindd[1956]: [2019/09/25 17:35:21.590508,  0] ../l
Sep 25 17:35:21 vm-pdc-005 winbindd[1956]:   STATUS=daemon 'winbindd' finished s
```

Korektní zavedení služby a nastavení.

Provedeme restartování serveru příkazem „*reboot*“.

5.5.4 Prověření funkčnosti Samba a DNS

Prověření zavedení služeb provedeme níže uvedenými příkazy. Jednotlivé příkazy vypíšou zavedení služeb SMB, Samba a DNS, včetně síťových portů a IP adres, na kterých naslouchají.

Test spuštění Samba

ps ax | grep "samba|smbd|nmbd|winbindd"

```
  1813 pts/0    S+     0:00 grep --color=auto samba|smbd|nmbd|winbindd
```

netstat -tulpn | egrep smbd

```
tcp    0      0 0.0.0.0:445       0.0.0.0:*           LISTEN       1383/smbd
..
```

Výpis je uveden v příloze A.

netstat -tulpn | egrep samba

```
tcp    0      0 0.0.0.0:464       0.0.0.0:*           LISTEN       1386/samba
..
```

Výpis je uveden v příloze A.

Kontrola spuštěného DNS serveru

netstat -anp | grep "LISTEN" | grep 53

```
tcp    0      0 0.0.0.0:53        0.0.0.0:*           LISTEN       1394/samba
tcp    0      0 0.0.0.0:49153     0.0.0.0:*           LISTEN       1371/samba
tcp6   0      0 :::53             :::*                LISTEN       1394/samba
tcp6   0      0 :::49153          :::*                LISTEN       1371/samba
```

Kontrola názvů a LAN

Příkazem „*ping*“ prověříme funkčnost síťových rozhraní.

ping 127.0.0.1

```
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.013 ms
```

ping 192.168.50.5

```
64 bytes from 192.168.50.5: icmp_seq=1 ttl=64 time=0.015 ms
```

ping vm-pdc-005

```
64 bytes from vm-pdc-005. (192.168.50.5): icmp_seq=1 ttl=64 time=0.014 ms
```

ping vm-pdc-005.comintelligence.local

```
64 bytes from vm-pdc-005. (192.168.50.5): icmp_seq=1 ttl=64 time=0.009 ms
```

Kontrola DNS

Prověříme funkčnost Active Directory a DNS v pořadí LDAP, Kerberos a „A“ záznam v DNS.

host -t SRV _ldap._tcp.comintelligence.local

```
_ldap._tcp.comintelligence.local has SRV record 0 100 389 vm-pdc-
005.comintelligence.local.
```

Test SRV record pro ldap prostřednictvím TCP.

host -t SRV _kerberos._udp.comintelligence.local

```
_kerberos._udp.comintelligence.local has SRV record 0 100 88 vm-pdc-
005.comintelligence.local.
```

Test SRV record pro Kerberos prostřednictvím UDP.

host -t A vm-pdc-005.comintelligence.local
```
vm-pdc-005.comintelligence.local has address 192.168.50.5
```
Test překladu názvu serveru.

Přidání reverzní zóny

Reverzní zóna funguje opačně než primární zóna. Reverzní zónou překládáme IP adresy na název a následujícím příkazem ji zavedeme do DNS.

samba-tool dns zonecreate -Uadministrator vm-pdc-005.comintelligence.local 50.168.192.in-addr.arpa
```
Zone 50.168.192.in-addr.arpa created successfully
```

Kontrola správnosti tiketu Kerberos

Následujícím příkazem otestujeme správnost funkčnosti Kerberos a pomocí příkazu „*klist*“ je vypsán seznam přidělených tiketů.

kinit administrator
```
Warning: Your password will expire in 41 days on Wed 06 Nov 2019 05:27:19 PM UTC
```

klist
```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@COMINTELLIGENCE.LOCAL
Valid starting       Expires              Service principal
09/25/2019 18:00:35  09/26/2019 04:00:35
krbtgt/COMINTELLIGENCE.LOCAL@COMINTELLIGENCE.LOCAL
        renew until 09/26/2019 18:00:07
```

Zrušení expirace platnosti hesla administrátora

samba-tool user setexpiry administrator --noexpiry
```
Expiry for user 'administrator' disabled.
```

Nastavení požadavků na hesla uživatelů domény

Hesla mají požadavek na složitost, nejsou uložená v plaintextu, mají minimální délku 14 znaků, maximální dobu expirace 60 dní a možnost změnit heslo kdykoli. Při zadání deseti špatných hesel dojde k uzamčení účtu na 15 minut. Resetování čítače při chybné autentizaci je nastaveno na 15 minut.

samba-tool domain passwordsettings set --complexity=on
samba-tool domain passwordsettings set --store-plaintext=off
samba-tool domain passwordsettings set --min-pwd-length=14
samba-tool domain passwordsettings set --history-length=24
samba-tool domain passwordsettings set --max-pwd-age=60
samba-tool domain passwordsettings set --min-pwd-age=0
samba-tool domain passwordsettings set --account-lockout-duration=10
samba-tool domain passwordsettings set --account-lockout-threshold=15
samba-tool domain passwordsettings set --reset-account-lockout-after=15
samba-tool domain passwordsettings show

5.5.5 Nastavení hlavního konfiguračního souboru smb.conf

Nastavení sdílení a zabezpečení je definováno v konfiguračním souboru smb.conf. Níže uvedená konfigurace obsahuje minimální nastavení pro bezpečnou a správnou funkčnost řadiče domény. Zde se zastavíme u několika voleb a hodnot. První z nich je server role, která definuje, jakou roli bude server mít. V našem případě je to řadič domény s AD. Další volbou je „*dns forwarder*“. Tato volba udává, kdo bude zodpovídat lokálně nepřeložené DNS dotazy. Volba „*name resolve order*“ udává pořadí překladů názvů. A poslední velmi důležitá volba je definování minimální požadované verze protokolu SMB. V další skupině voleb definujeme kódování pro správné zobrazení češtiny. Ochrana komunikačního kanálu je od verze 4.4.1 nastavena na výchozí hodnotu SSL nebo TLS. Externí aplikace, které toto šifrování nepodporují, se k LDAP nepřipojí.

Další konfigurace slouží pro nastavení hlavních složek řadiče domény. Složka SysVol obsahuje objekty GPO a informace o doméně. NetLogon obsahuje skripty, které jsou zaváděné při přihlášení k počítači.

Konfigurace smb.conf

mv /etc/samba/smb.conf /etc/samba/smb.conf.orig.beforeSambaSet
nano /etc/samba/smb.conf

```
# Global parameters
[global]
        workgroup = COMINTELLIGENCE
        realm = comintelligence.local
        wins support = yes
        netbios name = vm-pdc-005
        netbios aliases = server homedir
        server role = active directory domain controller
        idmap_ldb:use rfc2307 = yes
        dns forwarder = 8.8.8.8 193.17.47.1 185.43.135.1
        allow dns updates = secure
        server string = Server PDC firmy ComIntelligence
        name resolve order = wins host bcast
        client min protocol = SMB2
# Diacritics for shared folders
        dos charset = CP852
        unix charset = UTF-8
 [netlogon]
        path = /var/lib/samba/sysvol/comintelligence.local/scripts
        read only = No
        guest ok = no
        read only = no
        browsable = no
        comment = © NetLogon - domain comintelligence.local ©
 [sysvol]
        path = /var/lib/samba/sysvol
        read only = No
        comment = © SysVol - domain comintelligence.local ©
```

Z důvodu korektního zavedení změn provedeme restartování služby Samba.

systemctl restart samba-ad-dc && systemctl status samba-ad-dc

```
● samba-ad-dc.service - Samba AD Daemon
   Loaded: loaded (/lib/systemd/system/samba-ad-dc.service; enabled; vendor preset:
enabled)
..
```

Výpis je uveden v příloze B.

Test nastavení

Nyní provedeme test zavedení konfigurace a zobrazení sdílených složek.

smbclient -L localhost -U%

```
Sharename       Type      Comment
---------       ----      -------
sysvol          Disk      © SysVol - domain comintelligence.local ©
IPC$            IPC       IPC Service (Server PDC firmy ComIntelligence)
                          SMB1 disabled -- no workgroup available
```

Kontrola přihlášení administrátorským účtem

Níže uvedeným příkazem otestujeme přihlášení prostřednictvím administrátorského účtu.

smbclient //localhost/netlogon -U administrator -c 'ls'

```
  .                                   D        0  Wed Sep 25 16:41:28 2019
  ..                                  D        0  Wed Sep 25 16:41:30 2019

                20509264 blocks of size 1024. 18611536 blocks available
```

Kontrola nastavení DNS

Provedeme poslední kontrolu DNS příkazem „*nslookup*“.

nslookup comintelligence.local

```
Server:         127.0.0.1
Address:        127.0.0.1#53
Name:   comintelligence.local
Address: 192.168.50.5
```

nslookup VM-PDC-005.comintelligence.local

```
Server:         127.0.0.1
Address:        127.0.0.1#53
Name:   VM-PDC-005.comintelligence.local
Address: 192.168.50.5
```

nslookup seznam.cz

```
Server:         127.0.0.1
Address:        127.0.0.1#53
Non-authoritative answer:
Name:   seznam.cz
Address: 77.75.75.172
Name:   seznam.cz
Address: 77.75.75.176
..
```

host -t A centrum.cz

```
centrum.cz has address 46.255.231.106
```

5.6 Souborový server

V této kapitole se dostáváme k vytváření sdílených a zabezpečených složek. V první fázi musíme nastavit disk, kde budou data uložena.

Celá tato kapitola, včetně jejích podkapitol, vychází z oficiálních manuálů pro Samba 4 [38], [48] a vlastního dopracování za pomocí dílčích manuálů v OS „*man*“ a popisů v originálních konfiguračních souborech. Další použité zdroje jsou citovány v textu.

Nastavení práv k disku

Níže uvedenými příkazy nastavíme práva pro vlastníka root a skupinu root.

chmod 755 /Data
chmod g-s /Data
chmod u-s /Data
mkdir /Data/Samba
chmod 755 /Data/Samba
chmod g-s /Data/Samba
chmod u-s /Data/Samba
chown root.root /Data
chown root:"Domain Admins" /Data/Samba

Kontrola práv

ls -ld /Data && ls -ld /Data/Samba
```
drwxr-xr-x 4 root 4096 Sep 26 17:49 /Data
drwxr-xr-x 7 root COMINTELLIGENCE\domain admins 4096 Sep 26 17:49 /Data/Samba
```

Povolení přístupu k AD

Z důvodu rozšířené správy práv musíme povolit přístup Linuxu k AD. To provedeme níže uvedenou konfigurací.

cp /etc/nsswitch.conf /etc/nsswitch.conf.orig.beforeSamba
nano /etc/nsswitch.conf
```
group:          compat systemd winbind
```

Vypnutí služby WinBind

systemctl disable winbind.service
systemctl stop winbind.service

Kontrola a výpis skupin uložených v AD

wbinfo -g

```
COMINTELLIGENCE\cert publishers
COMINTELLIGENCE\ras and ias servers
COMINTELLIGENCE\allowed rodc password replication group
COMINTELLIGENCE\denied rodc password replication group
COMINTELLIGENCE\dnsadmins
COMINTELLIGENCE\enterprise read-only domain controllers
COMINTELLIGENCE\domain admins
COMINTELLIGENCE\domain users
COMINTELLIGENCE\domain guests
COMINTELLIGENCE\domain computers
COMINTELLIGENCE\domain controllers
COMINTELLIGENCE\schema admins
COMINTELLIGENCE\enterprise admins
COMINTELLIGENCE\group policy creator owners
COMINTELLIGENCE\read-only domain controllers
COMINTELLIGENCE\dnsupdateproxy
```

Kontrola přístupu k uživatelům uloženým v AD

wbinfo -u

```
COMINTELLIGENCE\administrator
COMINTELLIGENCE\guest
COMINTELLIGENCE\krbtgt
```

Znovunačtení konfigurace Samba

smbcontrol all reload-config

5.6.1 Řízení práv

ACL práva (Access Control List) nám umožňují rozšíření základních práv v OS Linux. Tato práva potřebujeme pro nastavení práv u sdílených složek, jako v OS Windows.

Kontrola ACL v SMB

smbd -b | grep HAVE_LIBACL

```
HAVE_LIBACL
```

Výpis přidělených práv

net rpc rights list accounts -U'COMINTELLIGENCE\administrator' -I vm-pdc-005.comintelligence.local

```
BUILTIN\Print Operators
SeLoadDriverPrivilege
SeShutdownPrivilege
..
```

Výpis je uveden v příloze C.

Nastavení práv pro Domain Admins

net rpc rights grant 'COMINTELLIGENCE\Domain Admins' SeDiskOperatorPrivilege -U' COMINTELLIGENCE\administrator'

```
Successfully granted rights.
```

5.6.2 Vytvoření fyzických složek pro sdílení

Nyní vytvoříme fyzické složky na disku, které použijeme pro sdílení nastavené v konfiguračním souboru smb.conf. Jedná se o složky 001_Company_data, 003_Information, 090_Administrators a 091_Backup.

Pro účely rychlého vytvoření a nastavení práv složek máme níže uvedené soubory příkazů se vstupní proměnnou. Druhý soubor příkazů slouží pro vytvoření domácích složek uživatelů.

```
varNameSharedFolder=001_Company_data
echo $varNameSharedFolder
$varNameSharedFolder
mkdir -p /Data/Samba/$varNameSharedFolder/
chown root:"Domain Admins" /Data/Samba/$varNameSharedFolder/
chmod 0770 /Data/Samba/$varNameSharedFolder/
unset varNameSharedFolder
echo $varNameSharedFolder

varNameSharedFolder=002_Users_Data
echo $varNameSharedFolder
mkdir -p /Data/Samba/$varNameSharedFolder/
chgrp -R "Domain Users" /Data/Samba/$varNameSharedFolder/
chmod 2750 /DiskData/Samba/$varNameSharedFolder/
unset varNameSharedFolder
echo $varNameSharedFolder
```

Kontrola nastavení práv

*getfacl /Data/Samba/**

```
getfacl: Removing leading '/' from absolute path names
# file: Data/Samba/001_Company_data
# owner: root
# group: COMINTELLIGENCE\134domain\040admins
user::rwx
group::rwx
other::---

# file: Data/Samba/002_Users_Data
# owner: root
# group: users
user::rwx
group::r-x
other::r-x

# file: Data/Samba/003_Information
# owner: root
# group: COMINTELLIGENCE\134domain\040admins
user::rwx
group::rwx
other::---

# file: Data/Samba/090_Administrators
# owner: root
# group: COMINTELLIGENCE\134domain\040admins
user::rwx
group::rwx
```

```
other::---

# file: Data/Samba/091_Backup
# owner: root
# group: COMINTELLIGENCE\134domain\040admins
user::rwx
group::rwx
other::---
```

5.6.3 Vytvoření sdílených složek

V konfiguračním souboru smb.conf nastavíme sdílení pro složku home a další sdílené složky podle potřeby. Složka home je určená pro připojení domácí složky během přihlášení účtu k PC. Při vytvoření účtu musíme přidat cestu k domovské složce např. „*Z:\\Shared.comintelligence.local\home\%username%*“.

nano /etc/samba/smb.conf

```
[home]
        path = /Data/Samba/002_Users_Data
```

..

Konfigurace je uvedena v příloze D.

Restartování služby Samba a kontrola konfiguračního souboru

Provedeme restartování služby Samba pro korektní načtení všech změn a kontrolu konfiguračního souboru smb.conf.

systemctl restart samba-ad-dc
systemctl status samba-ad-dc

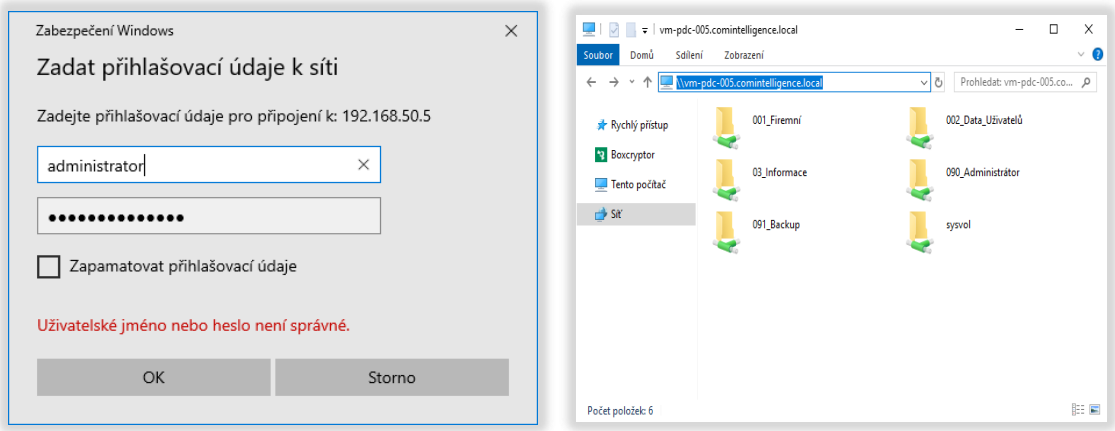
testparm

```
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Processing section "[netlogon]"
Processing section "[sysvol]"
Processing section "[home]"
Processing section "[001_Firemní]"
Processing section "[002_Data_Uživatelů]"
Processing section "[003_Informace]"
Processing section "[090_Administrátor]"
Processing section "[091_Backup]"
Loaded services file OK.
WARNING: You have some share names that are longer than 12 characters.
These may not be accessible to some older clients.
(Eg. Windows9x, WindowsMe, and smbclient prior to Samba 3.0.)
Server role: ROLE_ACTIVE_DIRECTORY_DC

Press enter to see a dump of your service definitions
…
…
```

Kontrola nastavení sdílení složek

Po vytvoření sdílených složek je možné přejít k jejich připojení. Toto můžeme realizovat například v Průzkumníkovi v OS Windows zadáním síťové adresy ve tvaru „*\\vm-pdc-005.comintelligence.local*“ a následném přihlášení, viz obrázek 25.



Obrázek 25: Přihlášení ke sdíleným složkám

Zdroj: vlastní zpracování

5.7 DHCP server

Posledním krokem před nasazením serveru jako řadiče domény je instalace DHCP serveru, který bude přidávat a odebírat záznamy do DNS, čímž vytvoříme dynamické DNS (DDNS).

Instalace

Balíček DHCP serveru je uložen v repositáři Ubuntu. Instalaci provedeme službou APT. [52], [38]

apt-get install isc-dhcp-server

Nastavení Kerberos

DHCP server musí mít práva pro zápis do DNS. Tato práva zabezpečíme prostřednictvím protokolu Kerberos. V prvním kroku nastavíme cestu s uloženými údaji o pověření v mezipaměti, tzv. cache. Následně vytvoříme v AD pomocí příkazu „*samba-tool user create*“ účet pro DHCP se zrušenou expirací platnosti hesla. Následuje exportování souborů s pověřením a šifrovaným klíčem (keytab). Na základě těchto pověření vytvoříme konfigurační soubor s volbami definujícími cesty a doménové údaje. Tyto údaje použijeme ve skriptu pro přihlášení. Následuje vytvoření skriptu pro dynamické změny DNS a nastavení vlastního DHCP serveru. Server připravíme pro přidělování adres z našeho adresního prostoru v rozsahu 20 až 100 v posledním oktetu. Nastavíme pronájem adres na 10 hodin a informace o NTP serveru. Konfigurace také obsahuje pravidla pro činnosti, které se mají vykonávat, když je IP adresa přidělena, obnovena a expirována. Dále je potřeba nastavit síťové rozhraní, na kterém bude DHCP komunikovat (v našem případě Eth0). Přidělíme práva k souborům a otestujeme přidání DNS záznamu.

Nastavení uložení pověření [33], [19], [1]

cp /etc/krb5.conf /etc/krb5.conf.orig.beforeDHCP
nano /etc/krb5.conf

```
[libdefaults]
        default_realm = COMINTELLIGENCE.LOCAL
        dns_lookup_realm = false
        dns_lookup_kdc = true
        default_ccache_name = FILE:/tmp/%{username}.krb5cc
```

Vytvoření účtu pro DHCP [8], [1]

samba-tool user create dhcpdadmin --description="Unprivileged admin for DDNS"
samba-tool user setexpiry dhcpdadmin --noexpiry
samba-tool group addmembers DnsAdmins dhcpdadmin

Exportování keytab [8], [1]

samba-tool domain exportkeytab --principal=dhcpdadmin@comintelligence.local dhcpdadmin.keytab
install -vdm 755 /etc/dhcp/
mv dhcpdadmin.keytab /etc/dhcp
chown root:dhcpd /etc/dhcp/dhcpdadmin.keytab
chmod 440 /etc/dhcp/dhcpdadmin.keytab

Kontrola vytvořeného účtu a práv k připojení [52], [38]

kinit dhcpdadmin
klist

```
Valid starting       Expires              Service principal
09/30/2019 20:48:41  10/01/2019 06:48:41
krbtgt/COMINTELLIGENCE.LOCAL@COMINTELLIGENCE.LOCAL
        renew until 10/01/2019 20:48:35
```

Nastavení údajů pro připojení k AD a DNS [1], [11]

nano /etc/dhcp/dhcpd-update-samba-dns.conf

```
# Variables
KRB5CC="/tmp/dhcpd4.krb5cc"
KEYTAB="/etc/dhcp/dhcpdadmin.keytab"
DOMAIN="comintelligence.local"
REALM="COMINTELLIGENCE.LOCAL"
PRINCIPAL="dhcpdadmin@${REALM}"
NAMESERVER="vm-pdc-005.${DOMAIN}"
ZONE="${DOMAIN}"
```

Skript pro přihlášení

Skript je převzat jako celek z internetového zdroje [11].

nano /usr/bin/dhcpd-update-samba-dns.sh

```
#!/bin/bash
..
..
```

Skript je uveden v příloze E.

Skript pro ovládání záznamů v DNS

Skript je převzat jako celek z internetového zdroje [11].

nano /usr/bin/samba-dnsupdate.sh

```
#!/bin/bash
..
..
```

Skript je uveden v příloze E.

Konfigurace DHCP serveru [22], [8], [1], [58]

mv /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.orig.beforeDHCP
nano /etc/dhcp/dhcpd.conf

```
# COMINTELLIGENCE.LOCAL
subnet 192.168.50.0 netmask 255.255.255.0 {
option subnet-mask 255.255.255.0;
option routers 192.168.50.1;
option domain-name "comintelligence.local";
option domain-name-servers 192.168.50.5;
option ntp-servers ntp.comintelligence.local;
option broadcast-address 192.168.50.255;
db-time-format local;
default-lease-time 36000; # 10 hours
max-lease-time 43200; # 12 hours
authoritative;
log-facility local7;
pool {
max-lease-time 36000; # 10 hodin
range 192.168.50.20 192.168.50.100;
}

on commit {
    set ClientIP = binary-to-ascii(10, 8, ".", leased-address);
    set ClientName = pick-first-value(option host-name, host-decl-name,
config-option host-name, noname);
    set ClientMac = binary-to-ascii(16, 8, ":", substring(hardware, 1, 6));
    execute("/usr/bin/dhcpd-update-samba-dns.sh", "add", ClientIP,
ClientName, ClientMac);
  }

  on release {
    set ClientIP = binary-to-ascii(10, 8, ".", leased-address);
    set ClientName = pick-first-value(option host-name, host-decl-name);
    set ClientMac = binary-to-ascii(16, 8, ":", substring(hardware, 1, 6));
    execute("/usr/bin/dhcpd-update-samba-dns.sh", "delete", ClientIP,
ClientName, ClientMac);
  }

    on expiry {
    set ClientIP = binary-to-ascii(10, 8, ".", leased-address);
    set ClientName = pick-first-value(option host-name, host-decl-name);
    set ClientMac = binary-to-ascii(16, 8, ":", substring(hardware, 1, 6));
    execute("/usr/bin/dhcpd-update-samba-dns.sh", "delete", ClientIP,
ClientName, ClientMac);
  }
}
```

Nastavení rozhraní DHCP serveru [17]

cp /etc/default/isc-dhcp-server /etc/default/isc-dhcp-server.orig.beforeDHCP
cp /etc/default/isc-dhcp-server.orig.beforeDHCP /etc/default/isc-dhcp-server
nano /etc/default/isc-dhcp-server

```
INTERFACESv4="eth0"
#INTERFACESv6=""
```

Restartování služby DHCP

systemctl restart isc-dhcp-server.service
systemctl status isc-dhcp-server.service

Nastavení přístupových práv ke skriptům

Následující příkazy nastaví práva rwx pro uživatele a skupinu root. Ostatní uživatelé mají práva rx.

chown root:root /usr/bin/dhcpd-update-samba-dns.sh
chmod 775 /usr/bin/dhcpd-update-samba-dns.sh
chown root:root /usr/bin/samba-dnsupdate.sh
chmod 775 /usr/bin/samba-dnsupdate.sh

Test přidání DNS záznamů

/usr/bin/dhcpd-update-samba-dns.sh add 192.168.50.50 Test

```
<30>Sep 30 21:08:09 dhcpd: Adding A record for host Test with IP 192.168.50.50 to
zone comintelligence.local on server vm-pdc-005.comintelligence.local
Record added successfully
<30>Sep 30 21:08:09 dhcpd: Adding PTR record 50 with hostname Test to zone
50.168.192.in-addr.arpa on server vm-pdc-005.comintelligence.local
Record added successfully
```

/usr/bin/dhcpd-update-samba-dns.sh delete 192.168.50.50 Test

```
<30>Sep 30 21:08:19 dhcpd: Removing A record for host Test with IP 192.168.50.50
from zone comintelligence.local on server vm-pdc-005.comintelligence.local
Record deleted successfully
<30>Sep 30 21:08:19 dhcpd: Removing PTR record 50 with hostname Test from zone
50.168.192.in-addr.arpa on server vm-pdc-005.comintelligence.local
Record deleted successfully
```

5.8 AppArmor

Při prověřování funkčnosti DDNS bylo zjištěno, že záznamy do DNS jsou přidávané pouze staticky. Záznamy logovacího souboru „*dhcp.log a syslog*“ obsahují záznamy o zakázaných přístupech „*Unable to execute /usr/bin/dhcpd-update-samba-dns.sh: Permission denied*“. Existují dvě varianty, jak konfigurovat AppArmor. První variantou je možnost měnit profily služeb v AppArmor a druhou je využít příkaz „*aa-logprof*“, který prohledá logovací soubory a navrhne vhodné řešení, viz následující příkazy a výpis z OS [52].

apt install apparmor-utils apparmor-profiles
reboot

Instalace balíčků AppArmor a restartování serveru.

systemctl status apparmor
Kontrola spuštění služby.

aa-logprof
```
Reading log entries from /var/log/syslog.
..
Profile:  /usr/sbin/dhcpd
Path:     /dev/tty
New Mode: rw
Severity: 9
..
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) /
Abo(r)t / (F)inish
Adding #include <abstractions/consoles> to profile.
..
(S)ave Changes / Save Selec(t)ed Profile / [(V)iew Changes] / View Changes b/w
(C)lean profiles / Abo(r)t
Writing updated profile for /usr/sbin/dhcpd.
```
Automatická konfigurace a potvrzení volby Allow a Save.

5.9 Firewall

V této kapitole se dostáváme k nastavení zabezpečení síťového provozu. Operační systém Ubuntu 18.04 používá firewall UFW. Nastavíme firewall tak, aby veškerá komunikace, která není povolená, byla zakázána. Nejprve je potřeba si ujasnit, které porty a protokoly potřebujeme. Porty zjistíme buď z dokumentace k danému programu, nebo z přehledu oficiálně uznaných portů autoritou pro přidělování portů (IANA) [20]. V našem případě potřebujeme níže uvedené porty, viz tabulka 4. Pravidla lze zadávat přímo příkazem, nebo je možné vytvořit soubory s konfigurací pro jednotlivá pravidla [54].

Tabulka 4: Nastavení firewall

Služba / Program	TO Port	ACTION	FORM	COMMAND
SSH	22/tcp	ALLOW IN	ANYWHERE	ufw allow 22/tcp
WebAdmin	10000/tcp	ALLOW IN	192.168.50.0/24 192.168.51.0/24	ufw allow from <IP> to any app ufw_ntp
Samba	464,49152:65535,53,88,445,137,138,389/udp 135,464,49152:65535,636,3268,53,88,139,445,3269,389/tcp	ALLOW IN	192.168.50.0/24 192.168.51.0/24	ufw allow from <IP> to any app ufw_sambaad
NTP	123/udp	ALLOW IN/OUT	ANYWHERE	ufw allow from any to any app ufw_ntp ufw allow out ufw_ntp
DNS	53/udp 53,445/tcp	ALLOW OUT	ANYWHERE	ufw allow out ufw_lanservicesout

Zdroj: vlastní zpracování

Zakázání veškeré komunikace [52], [53], [54]

sudo ufw default deny incoming
sudo ufw default deny outgoing

Zakázání ICMP protokolu [52], [53], [54]

cp /etc/ufw/before.rules /etc/ufw/before.rules.orig.beforeUFW
nano /etc/ufw/before.rules

```
# ok icmp codes for INPUT
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j DROP
-A ufw-before-input -p icmp --icmp-type time-exceeded -j DROP
-A ufw-before-input -p icmp --icmp-type parameter-problem -j DROP
-A ufw-before-input -p icmp --icmp-type echo-request -j DROP
```

Zapnutí UFW [52], [53], [54]

systemctl enable ufw
systemctl start ufw
systemctl status ufw
ufw enable

```
Command may disrupt existing ssh connections. Proceed with operation (y|n)? n
```

Po spuštění UFW dojde k odpojení komunikace s OpenSSH službou.

Povolení SSH (sudo ufw allow 22) [52], [53], [54]

sudo ufw allow ssh

Vytvoření a zavedení konfigurací pro jednotlivé služby

nano /etc/ufw/applications.d/webmin

```
[ufw_webmin]
title=Webmin
description=Webmin HTTPS
ports=10000/tcp
```

ufw allow from 192.168.50.0/24 to any app ufw_webmin
ufw allow from 192.168.51.0/24 to any app ufw_webmin

nano /etc/ufw/applications.d/sambaad

```
[ufw_sambaad]
title=Samba
description=Communicate with Samba AD
ports=123,464,49152:65535,53,88,445,137,138,389/udp|135,464,49152:65535,636
,3268,53,88,139,445,3269,389/tcp
```

ufw allow from 192.168.50.0/24 to any app ufw_sambaad
ufw allow from 192.168.51.0/24 to any app ufw_sambaad

nano /etc/ufw/applications.d/ntp

```
[ufw_ntp]
title=ntp
description=Network time protocol
ports=123/udp
```

ufw allow from any to any app ufw_ntp
ufw allow out ufw_ntp

nano /etc/ufw/applications.d/apt

```
[ufw_aptout]
title=Apt_OUT
description=Apt OUT
ports=443,80/tcp
```

ufw allow out ufw_aptout

nano /etc/ufw/applications.d/lanservicesout

```
[ufw_lanservicesout]
title=LAN_Services_Out
description=DNS OUT
ports=53/udp|53,445/tcp
```

ufw allow out ufw_lanservicesout

Ladění chyb z logovacího souboru ufw.log

Po nastavení firewallu je nutné zkontrolovat logovací soubor, který obsahuje výpisy zakázaných komunikací. V našem případě se jedná o port 137 a 67. Tyto porty povolíme následujícími příkazy.

ufw allow out from any to 192.168.50.0/24 proto udp port 137
ufw allow out from any to 192.168.51.0/24 proto udp port 137
ufw allow out from any to 192.168.50.0/24 proto udp port 67
ufw allow out from any to 192.168.51.0/24 proto udp port 67

Výpis použitých pravidel

Po dokončení konfigurace routeru vygenerujeme následujícím příkazem výpis zavedených pravidel. [52], [54]

ufw status numbered

```
Status: active
     To                         Action      From
     --                         ------      ----
[ 1] ufw_webmin                 ALLOW IN    192.168.50.0/24
[ 2] ufw_webmin                 ALLOW IN    192.168.51.0/24
[ 3] ufw_sambaad                ALLOW IN    192.168.50.0/24
[ 4] ufw_sambaad                ALLOW IN    192.168.51.0/24
[ 5] ufw_ntp                    ALLOW IN    Anywhere
[ 6] ufw_aptout                 ALLOW OUT   Anywhere                   (out)
[ 7] ufw_lanservicesout         ALLOW OUT   Anywhere                   (out)
[ 8] 22/tcp                     ALLOW IN    Anywhere
[ 9] 192.168.50.0/24 137/udp    ALLOW OUT   Anywhere                   (out)
[10] 192.168.51.0/24 137/udp    ALLOW OUT   Anywhere                   (out)
[11] 192.168.50.0/24 67/udp     ALLOW OUT   Anywhere                   (out)
[12] 192.168.51.0/24 67/udp     ALLOW OUT   Anywhere                   (out)
```

5.10 Zásady skupin

Zásady Group Policy (GP) jsou využívány pro centrální správu zařízení prostřednictvím AD, které jsou připojeny do domény. Cílem zásad skupin je centrálně distribuovat bezpečnostní a funkční nastavení počítačů a uživatelů v rámci domény. [44], [43]

Výchozí bezpečnostní sady zásad vycházejí ze standardních hodnot zabezpečení (baselines) od firmy Microsoft. Pro základní editaci, vytvoření a zálohování je možné využít program Microsoft Security Compliance Manager (SCM), Microsoft Local Group Policy Object Utility (LGPO), Microsoft Policy Analyzer a Group Policy Management (GPM). [27]

Pro vytvoření zásad použijeme program SCM, který má velice intuitivní ovládání. V programu stáhneme výchozí šablony zásad zabezpečení a následně je aplikujeme na vybrané organizační jednotky v rámci AD. V ukázce jsou použity pouze předdefinované sady zásad.

Z důvodu přehlednosti je vhodné jednotlivé zásady rozdělit podle oblastí do několika objektů a také je pojmenovat podle jmenné konvence.

Jmenná konvence

Konvenci názvu stanovíme následovně: <pořadové číslo ve tvaru <xxx>_<určení politiky „*Domain,Computers,Users*“>_<popis politiky>.

Příklad jmenné konvence:

- 001_Domain_Main_Policies
- 002_DomainControllers_Main_Policies
- 101_Computers_Local_Policies
- 201_Users_Local_Policies

Instalace SCM

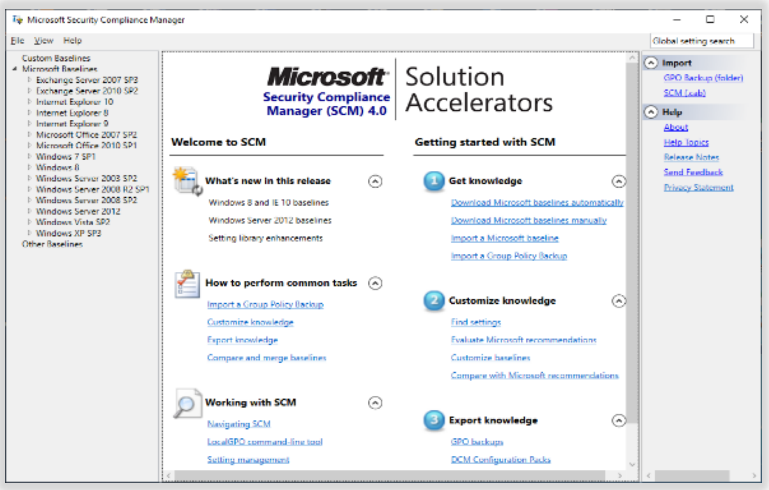
SCM stáhneme ze stránek Microsoftu a nainstalujeme ji s výchozími hodnotami. Postup instalace se může lišit podle předinstalovaného programového vybavení.

Požadavky SCM:

- Microsoft Visual C++ 2010 – automaticky doinstaluje.
- NET Framework 3.5 – nutné připojení k internetu, nebo stáhnout off-line instalaci.
- Microsoft SQL Server 2008 Express – nutné připojení k internetu, nebo stáhnout off-line instalaci.

Ovládání SCM

SCM disponuje plně grafickým rozhraním a je dostupné pouze v AJ, viz obrázek 26.

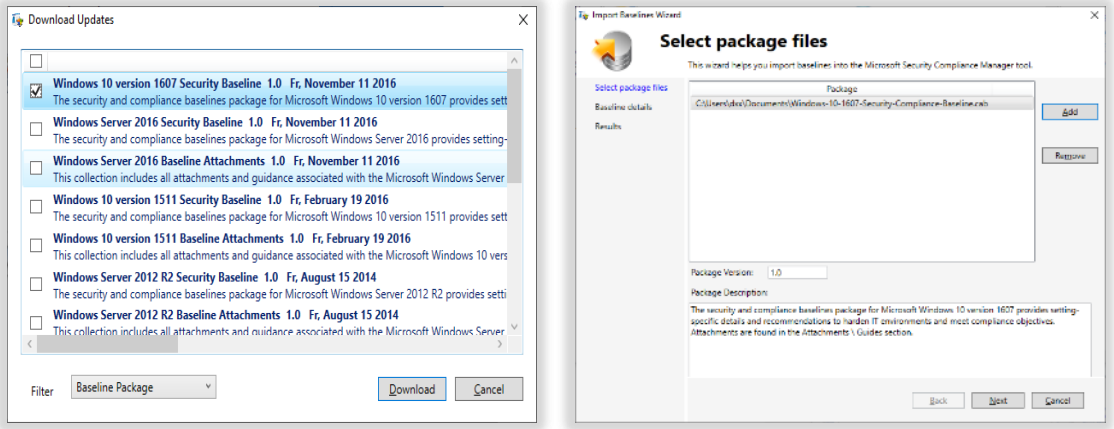


Obrázek 26: Grafické rozhraní SCM

Zdroj: vlastní zpracování

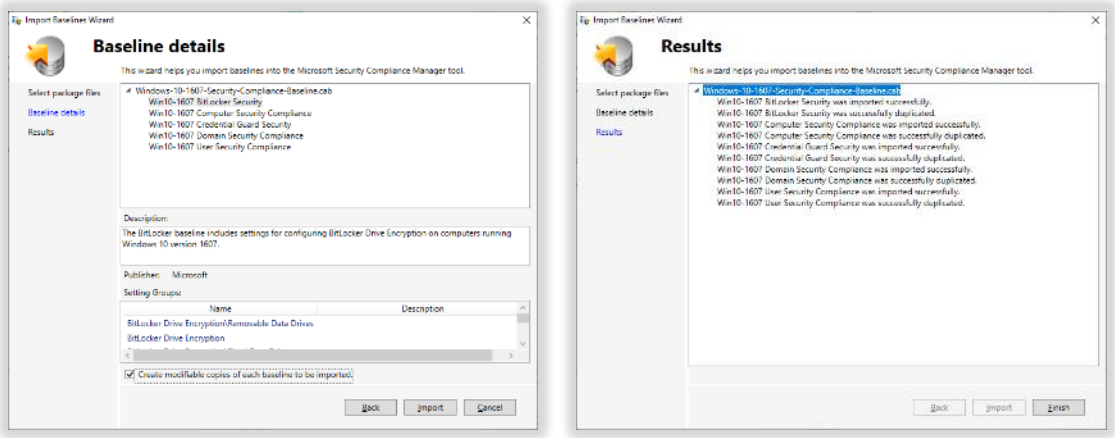
Import standardních hodnot zabezpečení (baseline)

V rámci importu uvažujeme o dvou variantách. U SCM připojeného do internetu je import plně automatický, nebo musíme standardní hodnoty stáhnout ze stránek Microsoftu a importovat je z lokálního úložiště. V našem případě použijeme automatické stažení baselines pomocí volby „*Download Microsoft baselines automatically*“ pro Windows 10, viz obrázek 27 a obrázek 28. Při importu je nutné zaškrtnout volbu „*Create modifiable copies*“



Obrázek 27: Stažení baselines

Zdroj: vlastní zpracování

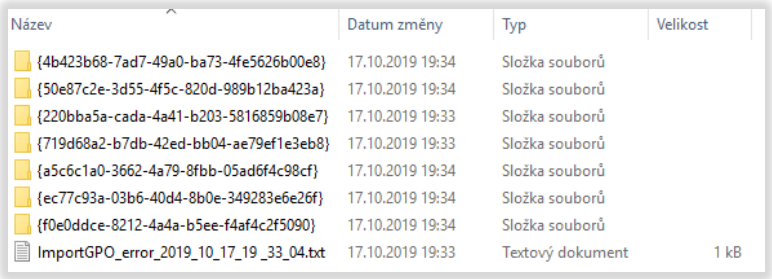


Obrázek 28: Importování baselines

Zdroj: vlastní zpracování

Export a import z SCM do GPO

Exportování výsledných sad zásad provedeme volbou „*GPO Backup*“. Vybereme umístění pro exportované zásady na lokální, případně síťový disk, viz obrázek 29.



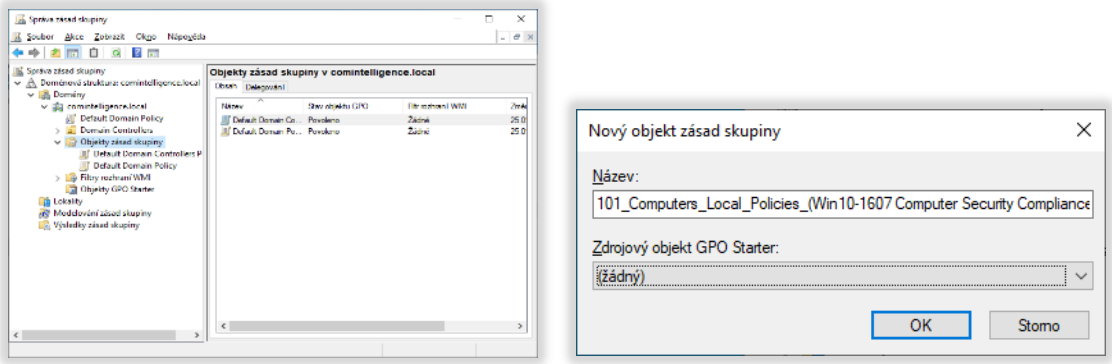
Obrázek 29: GPO Backup

Zdroj: vlastní zpracování

Importování zásad do řadiče domény s AD

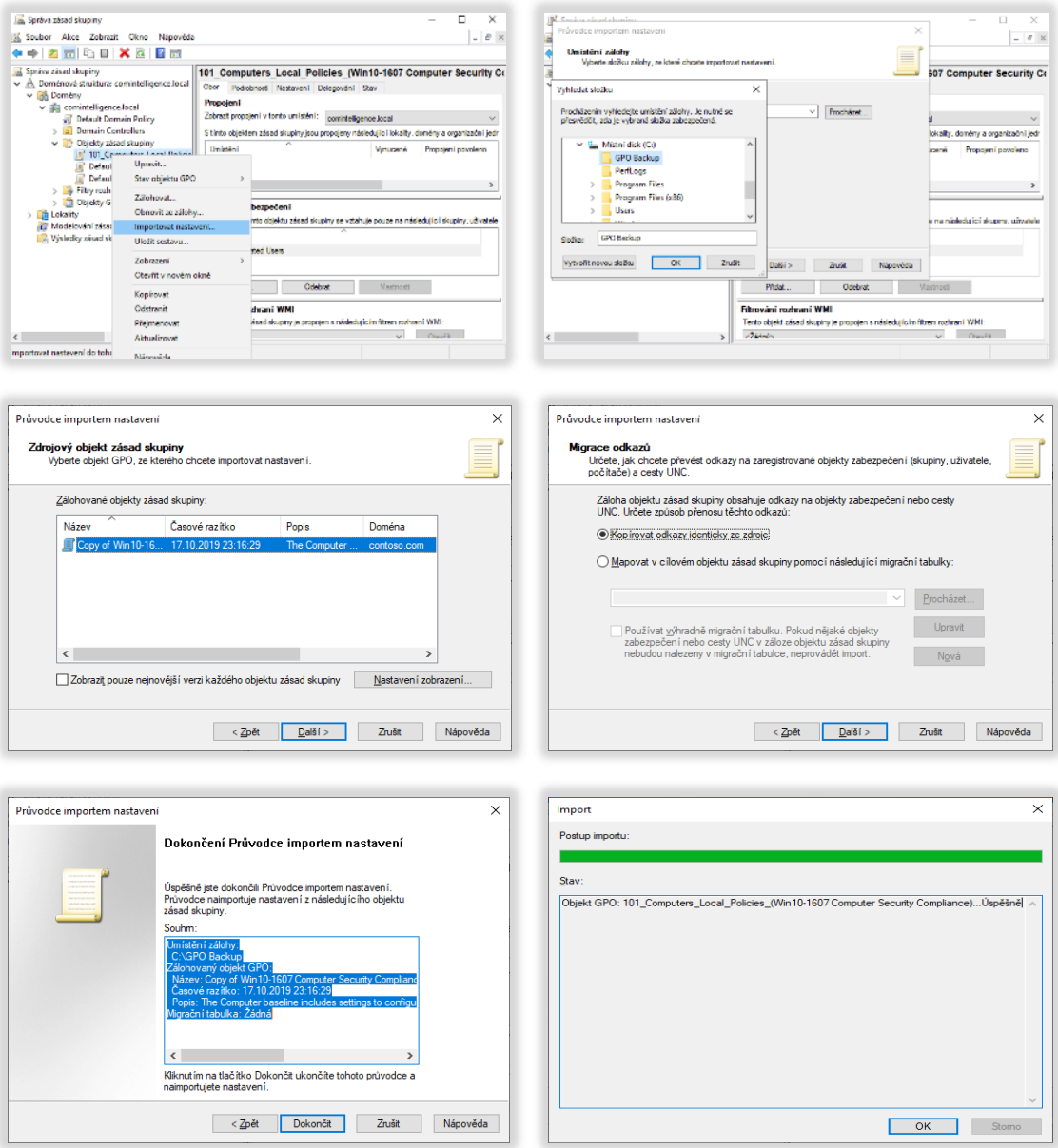
Importování zásad provedeme z jakéhokoli počítače s OS Windows, na kterém je nainstalován Remote Server Administration Tools (RSAT). Ideální stav nastává, když počítač máme připojený do domény a přihlásíme se k němu administrátorským účtem. Kompletní popis instalace je možné nalézt na stránkách Microsoftu. [36]

Při importování použijeme konzoli pro správu zásad skupiny. V prvním kroku je nutné vytvořit novou zásadu a následně importujeme dříve exportovanou zásadu z SCM. Celý postup je vyobrazen na níže uvedených obrázcích. Vytvořenou zásadu propojíme s danou organizační jednotkou, viz obrázek 32.



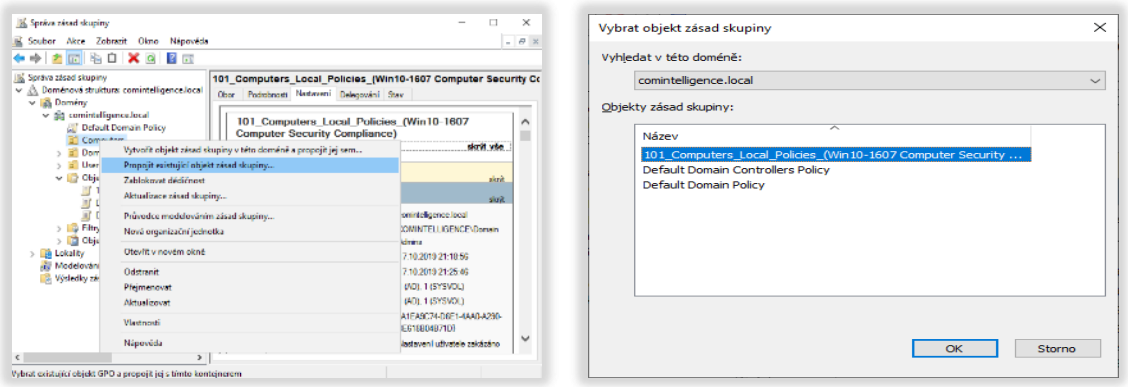
Obrázek 30: Vytvoření zásady zabezpečení

Zdroj: vlastní zpracování



Obrázek 31: Importování nastavení zásad skupiny

Zdroj: vlastní zpracování



Obrázek 32: Propojení objektu zásad skupiny s OU

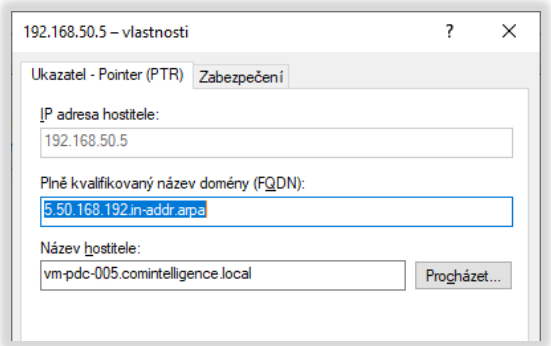
Zdroj: vlastní zpracování

5.11 Testování nastavení

V této části otestujeme konfiguraci serveru a routeru. V první řadě musíme prověřit síťové prostředí na korektnost přidělení IP adres a informací o dalších síťových službách. Následně otestujeme služby AD a souborového serveru. V poslední fázi prověříme zabezpečení portů u routeru ze strany připojení k internetu a u serveru.

5.11.1 Síťové prostředí

Test spočívá v připojení k jednotlivým sítím a výpisu z OS Windows pomocí příkazu „*ipconfig /all*“. Budeme testovat připojení k sítím Wifi-Firma-Free, Wifi-Firma a Internal LAN. Zajímají nás hlavně informace, jako jsou IP adresa, DNS servery a NTP servery. Požadujeme-li, aby byl server DNS známý pro klienta, musíme přidat tento server prostřednictvím příkazu nebo v konzoli DNS do reverzní zóny. Záznam přidáváme jako ukazatel PTR na název serveru, viz obrázek 33.



Obrázek 33: Přidání reverzního záznamu PTR

Zdroj: vlastní zpracování

Test dynamického nastavení rozhraní z DHCP

Níže uvedené části výpisů z operačního systému OS Windows vykazují správné nastavení podle požadavků. Výpis vyvoláme příkazem „*ipconfig /all*“ v příkazovém řádku OS Windows.

Wifi-Firma-Free

```
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . :
192.168.100.200(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.1
   DHCP Server . . . . . . . . . . . : 192.168.100.1
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       185.43.135.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Wifi-Firma:

```
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . : comintelligence.local
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . :
192.168.50.20(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.50.1
   DHCP Server . . . . . . . . . . . : 192.168.50.5
   DNS Servers . . . . . . . . . . . : 192.168.50.5
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Internal LAN:

```
Ethernet adapter Ethernet:
   Connection-specific DNS Suffix  . : comintelligence.local
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . :
192.168.50.51(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.50.1
   DHCP Server . . . . . . . . . . . : 192.168.50.5
   DNS Servers . . . . . . . . . . . : 192.168.50.5
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Test funkčnosti dvou síťových rozhraní

ping centrum.cz

```
Pinging centrum.cz [46.255.231.106] with 32 bytes of data:
Reply from 46.255.231.106: bytes=32 time=5ms TTL=246
```

Test nastavení DNS

V tomto kroku prověříme správnost nastavení DNS. Příkaz „*nslookup*“ spustíme na klientském zařízení.

nslookup comintelligence.local

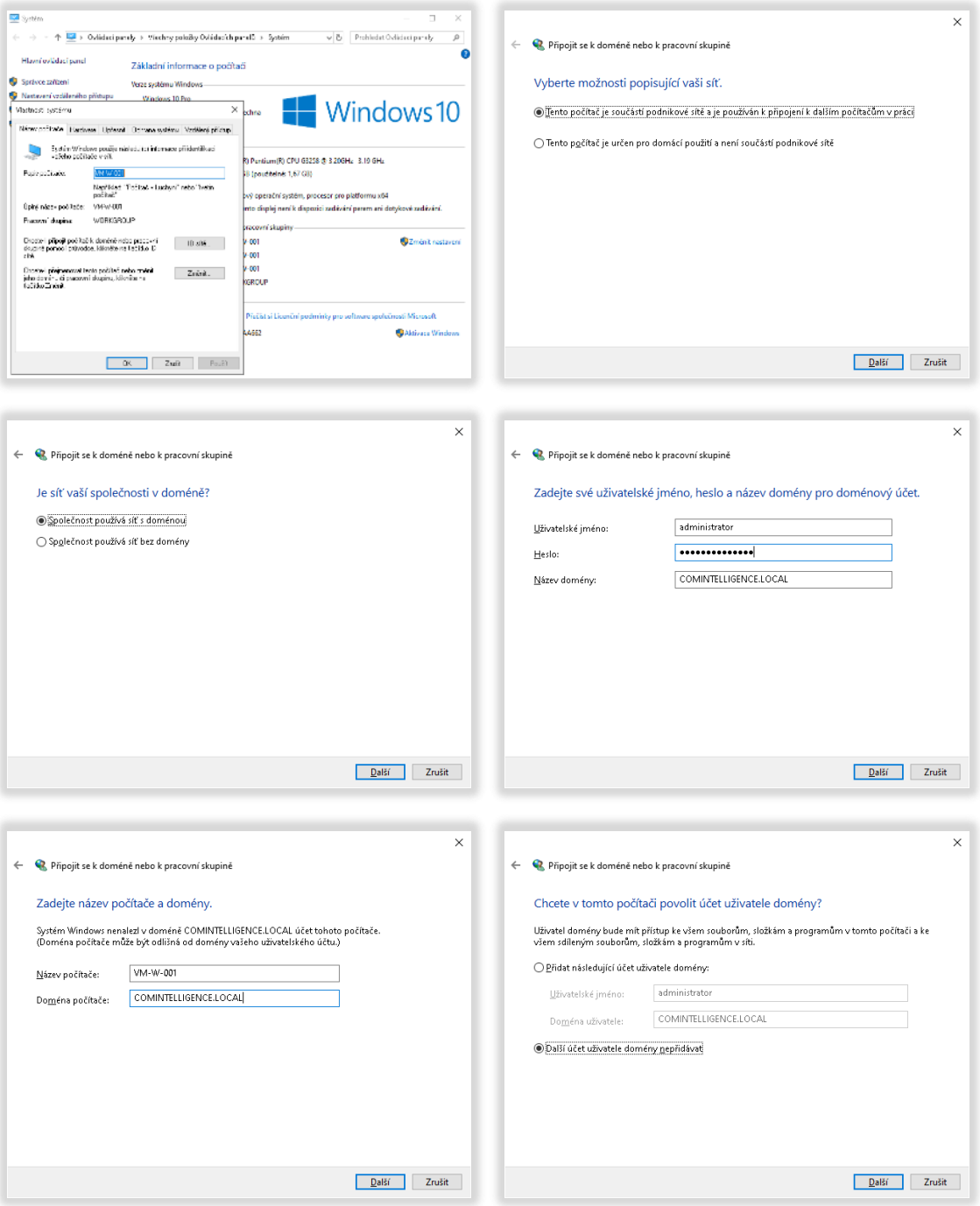
```
Server:  vm-pdc-005.comintelligence.local
Address:  192.168.50.5
Name:    comintelligence.local
Address:  192.168.50.5
```

nslookup centrum.cz

```
Server:  vm-pdc-005.comintelligence.local
Address:  192.168.50.5
Non-authoritative answer:
Name:    centrum.cz
Addresses:  2a00:da80:f::106
          46.255.231.106
```

5.11.2 Připojení počítače k doméně

Připojení k doméně realizujeme prostřednictvím nástroje OS Windows, který vyvoláme volbou „*Změnit nastavení*“ ve vlastnostech systému, viz obrázek 34. Pro připojení k doméně potřebujeme autentizační údaje doménového administrátora, viz obrázek 34.

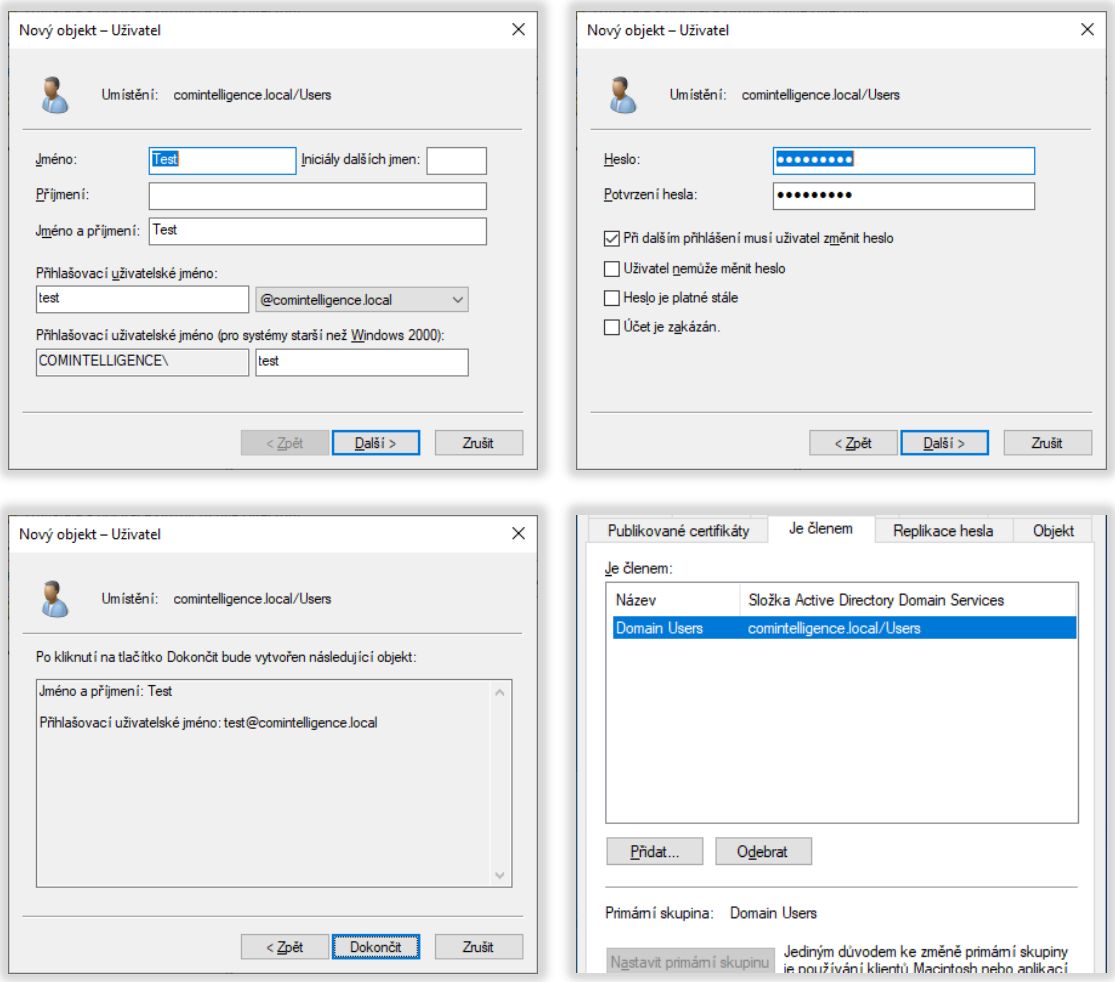


Obrázek 34: Připojení k doméně

Zdroj: vlastní zpracování

5.11.3 Přidání uživatelského účtu do AD

Před dalším testováním musíme přidat uživatelský účet do AD. Přidání provedeme konzolí RSAT „*Uživatelé a počítače služby Active Directory*“, viz obrázek 35.



Obrázek 35: Přidání uživatelského účtu do AD

Zdroj: vlastní zpracování

5.11.4 Zavedení GP do klientského počítače

Dalším krokem je otestování zavedení přidělených GP do klientského počítače. Zajímá nás zavedení zásad pro počítače a uživatele. Aplikování zásad pro počítače můžeme vidět na přihlašovací zprávě, viz obrázek 36. Zavedení můžeme vynutit příkazem „*gpupdate*“.

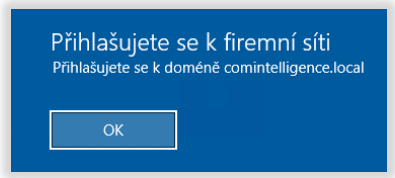
gpupdate

```
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

gpresult /R

```
Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
..
```

Výpis je uveden v příloze B.



Obrázek 36: Přihlašovací zpráva

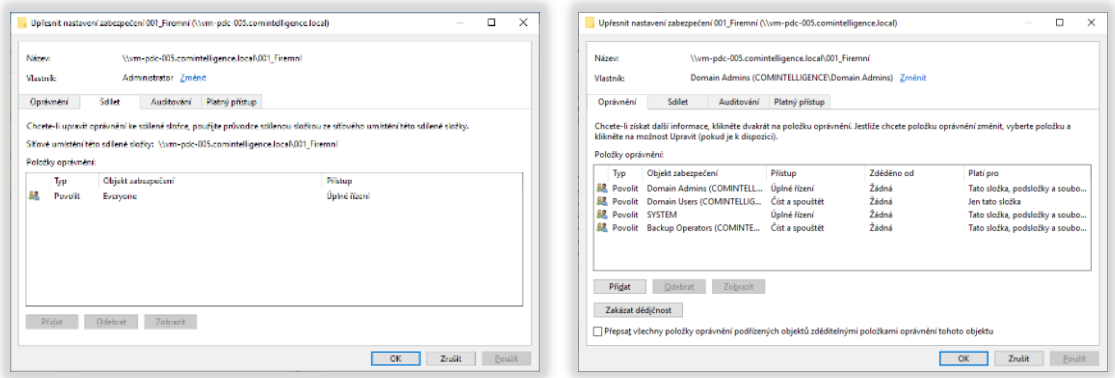
Zdroj: vlastní zpracování

5.11.5 Nastavení práv ke sdíleným složkám

V této části provedeme nastavení sdílených složek a otestujeme korektnost těchto úprav. Z důvodu rozsahu textu budeme nastavovat pouze jednu kořenovou složku.

Nastavení práv kořenových složek

Oprávnění ke sdílení nastavíme pro skupinu „*Everyone*“ s právy pro úplné řízení. Oprávnění k přístupu do složky nastavíme podle požadavků, viz obrázek 37. V kořenové složce vytvoříme tři podsložky se vzorovými právy, která jsou určena pro sdílení dat s oprávněním přístupu pro čtení, zápis a osobní složky. Ve složce pro čtení může vlastník provádět jakékoli operace a ostatní uživatelé mohou data pouze číst. Ve složce pro zápis může provádět jakékoli operace pouze vlastník. Ostatní uživatelé mohou data vkládat, ale mazat mohou pouze taková data, u kterých jsou přisazeni jako vlastníci. V poslední osobní složce může vlastník provádět jakékoli operace a ostatní uživatelé nemají do této složky přístup. Jedná se o základní možnosti nastavení, které lze i kombinovat, popřípadě měnit dědění práv v podstromu sdílených složek. Nastavení těchto složek je detailně popsáno v následující tabulce. Na základě vlastních zkušeností doporučuji práva ke složkám přidělovat na úrovni skupin a jednotlivé uživatele přidávat do skupin. Hlavním důvodem je zanechání identifikačního čísla účtu ve formátu objectSid, v případě odstranění účtu z AD.



Obrázek 37: Sdílení kořenové složky

Zdroj: vlastní zpracování

V následující tabulce jsou vyznačena základní přístupová práva ke složkám a souborům. Tato práva nastavujeme v OS Windows.

Práva:

- W –Write
- R – Read
- X – Execute and Delete

Tabulka 5: Nastavení přístupových práv ke sdíleným složkám

Skupina/Účet	Typ – (P povolit, O odepřít)	Platí pro	Úplné řízení	Procházet složkou/Spouštět soubory	Zobrazovat obsah složky/Číst data	Číst atributy	Číst rozšířené atributy	Vytvářet soubory/Zapisovat data	Vytvářet složky/Připojovat data	Zapisovat atributy	Zapisovat rozšířené atributy	Odstraňovat podsložky a soubory	Odstraňovat	Číst oprávnění	Měnit oprávnění	Přebírat vlastnictví
Pro čtení																
Skupina/Účet RWX	P	Tato složka, podsložky a soubory		X	X	X	X	X	X	X	X	X		X		
Skupina/Účet RWX	P	Jen podsložky a soubory	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Skupina/Účet RX	P	Tato složka, podsložky a soubory		X	X	X	X							X		
System RWX	P	Tato složka, podsložky a soubory	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Domain Admins	P	Tato složka, podsložky a soubory	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Backup Operators	P	Tato složka, podsložky a soubory	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Pro zápis																
Skupina/Účet RWX	P	Tato složka, podsložky a soubory		X	X	X	X	X	X	X	X	X		X		
Skupina/Účet RWX	P	Jen podsložky a soubory	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Skupina/Účet W	P	Tato složka, podsložky a soubory		X	X			X	X	X	X			X		
Creator Owner	P	Jen podsložky a soubory	X	X	X	X	X	X	X	X	X	X	X	X	X	X
System	P	Tato složka, podsložky a soubory	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Domain Admins	P	Tato složka, podsložky a soubory	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Backup Operators	P	Tato složka, podsložky a soubory	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Skupina/Účet	Typ – (P povolit, O odepřít)	Platí pro	Úplné řízení	Procházet složkou/Spouštět soubory	Zobrazovat obsah složky/Číst data	Číst atributy	Číst rozšířené atributy	Vytvářet soubory/Zapisovat data	Vytvářet složky/Připojovat data	Zapisovat atributy	Zapisovat rozšířené atributy	Odstraňovat podsložky a soubory	Odstraňovat	Číst oprávnění	Měnit oprávnění	Přebírat vlastnictví
Osobní složky																
Skupina/Účet RWX	P	Tato složka, podsložky a soubory		X	X	X	X	X	X	X	X	X		X		
Skupina/Účet RWX	P	Jen podsložky a soubory	X	X	X	X	X	X	X	X	X	X	X	X	X	X
System	P	Tato složka, podsložky a soubory	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Domain Admins	P	Tato složka, podsložky a soubory	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Backup Operators	P	Tato složka, podsložky a soubory	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Zdroj: vlastní zpracování

5.12 Testování zabezpečení routeru a serveru

Pro testování použijeme utilitu NMAP, která detekuje otevřené porty na serveru a routeru. Otevřené porty budeme zjišťovat na protokolu TCP a UDP. Syntaxe příkazu je následující: *„nmap <přepínač><časování><cíl>“* [29].

nmap	příkaz
sT	test TCP portů
sU	test UDP portů
T5	časování

Test serveru z interní sítě

nmap -sT -sU -T5 192.168.50.5

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-20 19:56
Nmap scan report for vm-pdc-005.comintelligence.local (192.168.50.5)
Host is up (0.000064s latency).
Not shown: 987 open|filtered ports, 985 filtered ports
PORT      STATE  SERVICE
22/tcp    open   ssh
53/tcp    open   domain
88/tcp    open   kerberos-sec
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
389/tcp   open   ldap
445/tcp   open   microsoft-ds
464/tcp   open   kpasswd5
636/tcp   open   ldapssl
3268/tcp  open   globalcatLDAP
3269/tcp  open   globalcatLDAPssl
10000/tcp open   snet-sensor-mgmt
```

```
49152/tcp open   unknown
49153/tcp open   unknown
49154/tcp open   unknown
53/udp    open   domain
123/udp   open   ntp
137/udp   open   netbios-ns
389/udp   open   ldap
49172/udp closed unknown
49184/udp closed unknown
49186/udp closed unknown
50708/udp closed unknown
52503/udp closed unknown
57958/udp closed unknown
61322/udp closed unknown
61370/udp closed unknown
61685/udp closed unknown
MAC Address: 00:15:5D:32:31:01 (Microsoft)
Nmap done: 1 IP address (1 host up) scanned in 29.59 seconds
```

Test routeru z interní sítě

nmap -sT -sU -T5 192.168.50.1

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-20 19:58 Stoední Evropa
Warning: 192.168.50.1 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.50.1
Host is up (0.00s latency).
Not shown: 998 closed ports, 998 filtered ports
PORT     STATE         SERVICE
2222/tcp open          EtherNetIP-1
8291/tcp open          unknown
67/udp   open|filtered dhcps
123/udp  open|filtered ntp
MAC Address: E4:8D:8C:22:36:83 (Routerboard.com)
Nmap done: 1 IP address (1 host up) scanned in 89.26 seconds
```

Test serveru z Wifi-Free

nmap -sT -sU -T5 192.168.50.5

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-20 20:05 Stoední Evropa
Nmap scan report for 192.168.50.5
Host is up.
All 2000 scanned ports on 192.168.50.5 are filtered (1000) or open|filtered (1000)
Nmap done: 1 IP address (1 host up) scanned in 167.01 seconds
```

Test routeru z Wifi-Free

nmap -sT -sU -T5 192.168.50.1

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-20 20:02 Stoední Evropa
Nmap scan report for 192.168.50.1
Host is up.
All 2000 scanned ports on 192.168.50.1 are filtered (1000) or open|filtered (1000)
Nmap done: 1 IP address (1 host up) scanned in 165.49 seconds
```

Test routeru z externí sítě připojené k portu WAN

nmap -sT -sU -T5 -Pn 192.168.3.254

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-20 20:30 Stoední Evropa
Nmap scan report for 192.168.3.254
Host is up (0.00s latency).
All 2000 scanned ports on 192.168.3.254 are filtered (1000) or open|filtered (1000)
MAC Address: E4:8D:8C:22:36:82 (Routerboard.com)
Nmap done: 1 IP address (1 host up) scanned in 52.98 seconds
```

5.13 Uzavření konfigurace OS Ubuntu

Po úspěšné konfiguraci serveru je nutné zavést opatření k zabezpečení administrátorského a superuživatelského účtu.

Vytvoření administrátora

V každém systému je doporučené zakázat výchozí administrátorský účet. Nestačí ho jenom přejmenovat, ale měli bychom ho zakázat, protože výchozí administrátor v OS Windows má vždy stejný objectSid. Následujícím příkazem vytvoříme administrátorský účet „*adminComintelligence*“ ve stejných skupinách, jako je zařazen výchozí administrátor.

samba-tool user create adminComintelligence --description="Domain Administrator"
samba-tool user setexpiry adminComintelligence --noexpiry
samba-tool group addmembers Administrators adminComintelligence
samba-tool group addmembers DnsAdmins adminComintelligence
samba-tool group addmembers "Domain Admins" adminComintelligence
samba-tool group addmembers "Domain Users" adminComintelligence
samba-tool group addmembers "Enterprise Admins" adminComintelligence
samba-tool group addmembers "Group Policy Creator Owners" adminComintelligence
samba-tool group addmembers "Schema Admins" adminComintelligence
kinit adminComintelligence
klist

```
Ticket cache: FILE:/tmp/root.krb5cc
Default principal: adminComintelligence@COMINTELLIGENCE.LOCAL

Valid starting       Expires              Service principal
11/11/2019 18:00:30  11/12/2019 04:00:30
krbtgt/COMINTELLIGENCE.LOCAL@COMINTELLIGENCE.LOCAL
        renew until 11/12/2019 18:00:16
```

samba-tool user disable administrator
Zakázání účtu administrátora.

Zakázání přihlášení účtu root

V souladu s kapitolou 5.4 a 5.4.1 vrátíme zpět konfiguraci, která povoluje přímé připojení účtu root k operačnímu systému Ubuntu. Provedeme opačnou úpravu konfiguračního souboru, viz následující konfigurace, a provedeme restartování služby SSH.

nano /etc/ssh/sshd_config

```
PermitRootLogin yes ----> PermitRootLogin prohibit-password
```

Uložit konfiguraci pomocí klávesové zkratky CTRL+X.
service ssh restart

ZÁVĚR

Cílem této diplomové práce bylo popsat a vysvětlit principy při navrhování zabezpečené počítačové sítě a služeb operačního systému včetně jejich implementace.

Text rozšiřuje bakalářskou práci „*Bezpečnost informačních systémů“* v oblasti vymezení informačních systémů, detailnějšího rozboru provozní a bezpečnostní dokumentace a síťových kybernetických útoků. Oproti výchozí práci je v ukázce použit router a bezplatný serverový operační systém.

Byly zde využity elektronické zdroje a literatura v knižní podobě. Kapitoly Informační systémy z hlediska řízení, životního cyklu a metodiky vývoje vycházejí převážně ze zdrojů [6], [10], [50]. V oblasti počítačové bezpečnosti práce čerpá ze zdroje, který se přímo zabývá touto problematikou [12]. Kapitola Bezpečnostní dokumentace byla vytvořena zejména podle internetových zdrojů [23], [34], [59]. Implementace navrhovaného řešení se inspiruje oficiálními dokumentacemi od výrobců routeru MikroTik [26], [28] a operačního systému Ubuntu [51], [52]. Při konfiguraci programu Samba 4, která vytváří z operačního systému Ubuntu řadič domény s AD, bylo nejvíce přihlíženo k oficiální dokumentaci [38] a linuxovému blogu [48].

V úvodní kapitole jsou představeny informační systémy z hlediska řízení, životního cyklu a metodiky vývoje. Na základě prostudování této problematiky lze říci, že pro správné navržení informačního systému musí být definován účel informačního systému a návaznost na další informační systémy. Volba operačního systému z hlediska architektury a požadované bezpečnosti operačního systému závisí na druhu a dodavateli informačního systému a jeho komponent.

Dále je práce věnována operačnímu systému a jeho službám včetně přehledu výrobců a verzí. Ty se dynamicky vyvíjejí a dochází jak ke vzniku nových systémů a verzí, tak k jejich zániku. Jednotlivé verze si mohou být velmi podobné, ale také se mohou diametrálně odlišovat, což klade vysoké nároky na správu těchto systémů a jejich služeb.

V kapitole Počítačová bezpečnost jsou uvedeny některé druhy kybernetických útoků, jenž útočník může zvolit. U každého útoku je uvedena i možná ochrana. Právě na tuto ochranu je práce zaměřena. V ukázce návrhu a implementace je ochrana řešena konfigurací firewallu, routeru a serveru. Nepotřebné služby jsou omezeny, nebo zakázány.

Bezpečnostní dokumentace patří mezi nejdůležitější články v oblasti kybernetické ochrany. Jakýkoli informační systém s chybějící dokumentací může být negativně ovlivněn nedefinováním doporučených oblastí, které tato dokumentace řeší. Bezpečnostní dokumentace jednoznačně definuje bezpečnost, povinnosti jednotlivých rolí, procedury aj. Provozní dokumentace pomáhá zvládat provoz informačního systému v průběhu posledních fází životního cyklu. Vždyť popsané procedury a nastavení mohou pomoci předcházet omezením a pádům informačního systému.

Oproti výchozí práci je v ukázce použit bezplatný software a nastavení serveru je vysvětleno pomocí příkazů. Právě díky syntaxím příkazů je možné pochopit celou problematiku nastavování serverových operačních systémů a routerů. V případě grafického rozhraní uživatel nebo administrátor neví, co programový kód dělá. Použitím interaktivního grafického prvku dojde ke skryté proceduře na pozadí. V rámci ukázky byl konfigurován router MikroTik, s cílem vytvořit bezpečné prostředí. Na základě omezení služeb, nastavení firewallu, konfigurace VPN serveru je dosaženo požadovaných vlastností, které byly ověřeny testem otevřených portů. Instalace a konfigurace serveru proběhla podle zažitých metod a zdokumentovaných postupů. Proti útokům ze síťového prostředí je server zabezpečen pomocí interního firewallu. Řízení domény a sdílených složek včetně zabezpečení je realizováno pomocí softwaru Samba 4. Cílem konfigurace systému bylo nastavit řízený přístup k datům a ochránit operační systém před možnými útoky.

Na základě výsledků práce lze říci, že firma může provozovat informační systém na levnější platformě operačního systému s celkem uspokojivým zabezpečením. Dalším faktorem pro zavedení OS Linux je fakt, že hardwarová náročnost je oproti MS Windows nižší. V oblasti škodlivého kódu je samozřejmě nutné nasadit antivirovou ochranu, a to zejména kvůli datům, která jsou sdílena s OS Windows. Velkou nevýhodou OS Linux je náročnost na administraci a aplikování předchozích řešení na nové verze a distribuce. Stejně jako u operačních systémů lze využít i informační systémy na platformě Open Source. Práce by mohla být rozšířena ještě o auditní systémy, zálohování prostřednictvím šifrovaných přenosů a tzv. „*Black List*“ u routeru.

Závěrem můžeme říci, že vytyčené cíle diplomové práce byly splněny.

POUŽITÁ LITERATURA

[1] Archlinux: Samba/Active Directory domain controller. *Archlinux* [online]. c2002-2019, 12 July 2018 [cit. 2019-10-14]. Dostupné z: https://wiki.archlinux.org/index.php/Samba/Active_Directory_domain_controller#DHCP_with_dynamic_DNS_updates

[2] Basics of Operating Systems: Operating System Services. *SlideShare: Discover. Share. Learn.* [online]. c2019, 13 January 2013 [cit. 2019-11-03]. Dostupné z: https://www.slideshare.net/myrajendra/operating-system-services-9?from_action=save

[3] BIGELOW, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů.* Brno: Computer Press, 2004. ISBN 80-251-0178-9.

[4] BROOKSHEAR, J. Glenn, David T. SMITH a Dennis BRYLOW. *Informatika*. Brno: Computer Press, 2013. ISBN 978-80-251-3805-2.

[5] BROOKSHEAR, J. Glenn, David T. SMITH a Dennis BRYLOW. *Informatika*. Brno: Computer Press, 2013. ISBN 978-80-251-3805-2.

[6] BRUCKNER, Tomáš. *Tvorba informačních systémů: principy, metodiky, architektury*. Praha: Grada, 2012. Management v informační společnosti. ISBN 978-80-247-4153-6.

[7] BUCHALCEVOVÁ, Alena. Metodiky budování informačních systémů. *Metodiky vývoje a údržby informačních systémů: kategorizace, agilní metodiky, vzory pro návrh metodiky* [online]. Praha: Grada, 2005, s. 1-59 [cit. 2019-09-25]. Management v informační společnosti. ISBN 80-247-1075-7. Dostupné z: https://nb.vse.cz/~BUCHALC/clanky/metodiky.pdf

[8] Configure DHCP to update DNS records with BIND9. *Samba Wiki: Samba* [online]. 2019, 20 March 2019 [cit. 2019-10-14]. Dostupné z: https://wiki.samba.org/index.php/Configure_DHCP_to_update_DNS_records_with_BIND9

[9] ČAPEK, Jan. *Operační systémy I*. Pardubice: Univerzita Pardubice, 2014. ISBN 978-80-7395-775-9.

[10] DANIEL, Roman. *Informační systémy* [online]. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava, 2013 [cit. 2019-09-10]. ISBN 978-80-248-3051-3. Dostupné z: http://projekty.fs.vsb.cz/463/edubase/VY_01_041/Informa%C4%8Dn%C3%AD%20syst%C3%A9my.pdf

[11] Djlucas/aur-samba-dhcpd-update. *GitHub* [online]. GitHub, c2019, 6 Dec 2015 [cit. 2019-10-14]. Dostupné z: https://github.com/djlucas/aur-samba-dhcpd-update

[12] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

[13] Enabling NTP Time Synchronization in Ubuntu 18.04. *Edmundo Fuentes' Blog: random entries and notes-to-self about programming and finance engineering* [online]. c2019, 19. November 2018 [cit. 2019-11-06]. Dostupné z: https://www.edmundofuentes.com/blog/2018/11/19/enable-ntp-ubuntu-18-04/

[14] GÁLA, Libor, Jan POUR a Prokop TOMAN. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi, technologie informačních systémů, řízení a rozvoj podnikové informatiky.* Praha: Grada, 2006. Management v informační společnosti. ISBN 80-247-1278-4.

[15] HELVICH, Jiří. *Bezpečnost informačních systémů v prostředí počítačových sítí*. Pardubice, 2016. Bakalářská práce. Univerzita Pardubice, Fakulta ekonomicko-správní. Vedoucí práce Pavel Jirava.

[16] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce.* 3., aktualiz. vyd. Brno: Computer Press, 2006, 211 s. ISBN 80-251-0892-9.

[17] How to Install and Configure DHCP on Ubuntu 18.04. *LinOxide* [online]. BTREME, c2019, 13 December 2018 [cit. 2019-10-15]. Dostupné z: https://linoxide.com/linux-how-to/install-configure-dhcp-ubuntu/

[18] How to install Midnight Commander (MC) on Ubuntu 18.04. *IT Blog* [online]. 7.11.2018 [cit. 2019-10-12]. Dostupné z: https://ixnfo.com/en/how-to-install-midnight-commander-mc-on-ubuntu-18-04.html

[19] How to set the Kerberos default_ccache_name attribute on a client without using KRB5CCNAME?. *Stackoverflow* [online]. c2019, 20 April 2015 [cit. 2019-10-14]. Dostupné z: https://stackoverflow.com/questions/29748818/how-to-set-the-kerberos-default-ccache-name-attribute-on-a-client-without-using

[20] *Iana* [online]. [cit. 2019-10-15]. Dostupné z: https://www.iana.org/

[21] Informace. *ManagementMania* [online]. c2011-2016, 14.12.2017 [cit. 2019-09-10]. Dostupné z: https://managementmania.com/cs/informace

[22] ISC Documentation. *ISC* [online]. ISC, c2001-2019, 17 September 2019 [cit. 2019-10-15]. Dostupné z: https://kb.isc.org/docs/using-this-knowledgebase#

[23] KAJZAR, Dušan. Dokumentace k IS. *Internetové učebnice* [online]. [cit. 2019-10-27]. Dostupné z: http://zdenek2.euweb.cz/doc3/prois92.html

[24] Konfigurace OpenVPN serveru na Mikrotiku: Konfigurace OpenVPN serveru na Mikrotiku (RouterOS ver. 6.37.1). *Djblond* [online]. 2017, 20. listopadu 2016 [cit. 2019-10-06]. Dostupné z: http://www.djblond.cz/index.php/2016/11/20/konfigurace-openvpn-serveru-na-mikrotiku/

[25] Křupka Jiří, Kašparová, Miloslava. *Úvod do teorie systémů* [Multimediální studijní opora na CD], Univerzita Pardubice: Pardubice, 2007. ISBN 978-80-7194-955-8

[26] Manual:Securing Your Router. *MikroTik* [online]. 2019, 31 May 2019 [cit. 2019-10-05]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router#RouterOS_services

[27] Microsoft Security Compliance Toolkit 1.0. *Microsoft* [online]. c2019, 26.11.2018 [cit. 2019-10-17]. Dostupné z: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10

[28] *MikroTik: Manual:TOC* [online]. MediaWiki, 2019 [cit. 2019-10-02]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:TOC

[29] *NMAP.ORG: Documentation* [online]. 1999 [cit. 2019-10-20]. Dostupné z: https://nmap.org/docs.html

[30] *OPENVPN OPEN SOURCE: Community Resources* [online]. c2002-2018 [cit. 2019-10-06]. Dostupné z: https://openvpn.net/community-resources/

[31] Operační systém. *Wikipedie* [online]. 2001, 21. 10. 2019 [cit. 2019-11-03]. Dostupné z: https://cs.wikipedia.org/wiki/Opera%C4%8Dn%C3%AD_syst%C3%A9m

[32] Operating System: What are the services provided by the Operating-System…? *Basic IT Topic* [online]. c2019, 3. July 2018 [cit. 2019-11-03]. Dostupné z: https://basicittopic.com/what-are-the-services-provided-by-the-operating-system/

[33] Oracle: krb5.conf. *Oracle* [online]. c2019, 13 June 2019 [cit. 2019-10-14]. Dostupné z: https://docs.oracle.com/cd/E88353_01/html/E37852/krb5-conf-5.html

[34] PAVLÍK, Lukáš. *Správa a provoz informačních systémů: Studijní opora pro kombinované studium* [online]. Olomouc: Moravská vysoká škola Olomouc, 2018 [cit. 2019-10-27]. Dostupné z: https://mvso.cz/wp-content/uploads/2018/02/Spr%c3%a1va-a-provoz-informa%c4%8dn%c3%adch-syst%c3%a9m%c5%af-studijn%c3%ad-text.pdf

[35] PETR, Pavel. *Projektový management II*. Pardubice: Univerzita Pardubice, 2014. ISBN 978-80-7395-845-9.

[36] Remote Server Administration Tools (RSAT) for Windows operating systems. *Microsoft* [online]. c2019, 2. 8. 2019 [cit. 2019-10-17]. Dostupné z: https://support.microsoft.com/cs-cz/help/2693643/remote-server-administration-tools-rsat-for-windows-operating-systems

[37] RYBIČKA, Jiří. *Informační systémy. Mendelova univerzita v Brně* [online]. Brno: Mendelova univerzita v Brně, c2018 [cit. 2019-09-15]. Dostupné z: https://akela.mendelu.cz/~rybicka/prez/infsyst.pdf

[38] Samba Wiki: User Documentation. *Samba Wiki* [online]. 2019 [cit. 2019-10-12]. Dostupné z: https://wiki.samba.org/index.php/User_Documentation

[39] SCAMBRAY, Joel, George KURTZ a Stuart MCCLURE. *Hacking bez tajemství*. 2. aktualiz. vyd. Praha: Computer Press, 2002. Komunikace a sítě. ISBN 80-722-6644-6.

[40] Security-portal: Bezpečnost a Hacking WiFi (802.11) - 4. část WPA a WPA2. *Security-portal* [online]. CC-BY-SA Security-Portal.cz, 2019, 3. listopadu 2010 [cit. 2019-10-05]. Dostupné z: https://www.security-portal.cz/clanky/bezpe%C4%8Dnost-hacking-wifi-80211-4-%C4%8D%C3%A1st-wpa-wpa2

[41] SODOMKA, Petr a Hana KLČOVÁ. *Informační systémy v podnikové praxi*. 2., aktualiz. a rozš. vyd. Brno: Computer Press, 2010. ISBN 978-80-251-2878-7.

[42] SPORTACK, Mark *A. Směrování v sítích IP:* [autorizovaný výukový průvodce : samostudium : kompletní zdroj informací o směrování a protokolech v sítích IP]. Vyd. 1. Brno: Computer Press, 2004. Cisco systems. ISBN 80-251-0127-4.

[43] STANEK, William R. *Microsoft Windows Server 2008: kapesní rádce administrátora*. Brno: Computer Press, 2008. Knihovnička administrátora (Computer Press). ISBN 978-80-251-1936-5.

[44] STANEK, William R. *Mistrovství v Microsoft Windows Server 2008: [kompletní informační zdroj pro profesionály]*. Brno: Computer Press, 2009. ISBN 978-80-251-2158-0.

[45] SUSE: kinit: Credential cache directory "/run/user/0/krb5cc" does not exist while getting default ccache. *SUSE: We adapt. You succeed.* [online]. c2019, 19 May 2017 [cit. 2019-10-14]. Dostupné z: https://www.suse.com/support/kb/doc/?id=7019000

[46] ŠMÍD, Vladimír. Životní cyklus informačního systému. *Fakulta informatiky Masarykova univerzita* [online]. Brno, 1994 [cit. 2019-09-18]. Dostupné z: https://www.fi.muni.cz/~smid/mis-zivcyk.htm

[47] ŠMRHA, Pavel a Vladimír RUDOLF. *Internetworking pomocí TCP/IP*. České Budějovice: Kopp, 1994. ISBN 80-858-2809-X.

[48] TecMint: Create an Active Directory Infrastructure with Samba4 on Ubuntu. *TecMint: The Idelal Linux Blog for Sysadmins & Geeks* [online]. c2019 [cit. 2019-10-12]. Dostupné z: https://www.tecmint.com/install-samba4-active-directory-ubuntu/

[49] Tomáš Pexa: OpenVPN - Přehledně. *Tomáš Pexa: Vše co se děje na internetu…* [online]. 2019, 2.5.2018 [cit. 2019-10-06]. Dostupné z: https://www.tomaspexa.cz/2018/05/02/openvpn-prehledne/

[50] TVRDÍKOVÁ, Milena. *Aplikace moderních informačních technologií v řízení firmy: nástroje ke zvyšování kvality informačních systémů.* Praha: Grada, 2008. Management v informační společnosti. ISBN 978-80-247-2728-8.

[51] *Ubuntu Česká republika* [online]. Ubuntu documentation team, 2019 [cit. 2019-10-10]. Dostupné z: https://wiki.ubuntu.cz

[52] *Ubuntu Server Guide* [online]. Ubuntu documentation team, c2018 [cit. 2019-10-09]. Dostupné z: https://help.ubuntu.com/lts/serverguide/serverguide.pdf

[53] UFW. *Official Ubuntu Documentation* [online]. c2019 [cit. 2019-10-15]. Dostupné z: https://help.ubuntu.com/community/UFW

[54] UncomplicatedFirewall. *Ubuntu WIki* [online]. 2019, 22.04.2019 [cit. 2019-10-15]. Dostupné z: https://wiki.ubuntu.com/UncomplicatedFirewall

[55] WebMin: Installing on Debian. *WebMin* [online]. c2006–2016 [cit. 2019-10-12]. Dostupné z: http://www.webmin.com/deb.html

[56] WHITMAN, Michael E. a Herbert J. MATTORD. *Principles of information security*. 4th ed. Boston, MA: Course Technology, c2012. ISBN 978-1-111-13821-9.

[57] Wi-Fi: Overview of the 802.11 Physical Layer and Transmitter Measurements. In: *Tektronix* [online]. 13.03.2014 [cit. 2019-10-04]. Dostupné z: https://download.tek.com/document/37W-29447-2_LR.pdf

[58] Wildcard DNS entries for DHCP leases. *Cweiske.de* [online]. 2019, 21.01.2016 [cit. 2019-10-15]. Dostupné z: https://cweiske.de/tagebuch/dns-wildcard-dhcp.htm

[59] *Zásady tvorby bezpečnostní dokumentace informačních systémů určených k nakládání s utajovanými informacemi: verze 1.0* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost, 2017 [cit. 2019-10-28]. Dostupné z: https://www.nbu.cz/download/bezpecnost-informacnich-systemu/DokumentaceIS-vzor.pdf

SEZNAM PŘÍLOH

Příloha A – Test spuštění Samby

ps ax | grep "samba|smbd|nmbd|winbindd"

```
  1813 pts/0    S+     0:00 grep --color=auto samba|smbd|nmbd|winbindd
```

netstat -tulpn | egrep smbd

```
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN
1383/smbd
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN
1383/smbd
tcp6       0      0 :::445                  :::*                    LISTEN
1383/smbd
tcp6       0      0 :::139                  :::*                    LISTEN
1383/smbd
```

netstat -tulpn | egrep samba

```
tcp        0      0 0.0.0.0:464             0.0.0.0:*               LISTEN
1386/samba
tcp        0      0 0.0.0.0:53              0.0.0.0:*               LISTEN
1394/samba
tcp        0      0 0.0.0.0:88              0.0.0.0:*               LISTEN
1386/samba
tcp        0      0 0.0.0.0:636             0.0.0.0:*               LISTEN
1384/samba
tcp        0      0 0.0.0.0:49152           0.0.0.0:*               LISTEN
1371/samba
tcp        0      0 0.0.0.0:49153           0.0.0.0:*               LISTEN
1371/samba
tcp        0      0 0.0.0.0:49154           0.0.0.0:*               LISTEN
1371/samba
tcp        0      0 0.0.0.0:3268            0.0.0.0:*               LISTEN
1384/samba
tcp        0      0 0.0.0.0:3269            0.0.0.0:*               LISTEN
1384/samba
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN
1384/samba
tcp        0      0 0.0.0.0:135             0.0.0.0:*               LISTEN
1371/samba
tcp6       0      0 :::464                  :::*                    LISTEN
1386/samba
tcp6       0      0 :::53                   :::*                    LISTEN
1394/samba
tcp6       0      0 :::88                   :::*                    LISTEN
1386/samba
tcp6       0      0 :::636                  :::*                    LISTEN
1384/samba
tcp6       0      0 :::49152                :::*                    LISTEN
1371/samba
tcp6       0      0 :::49153                :::*                    LISTEN
1371/samba
tcp6       0      0 :::49154                :::*                    LISTEN
1371/samba
tcp6       0      0 :::3268                 :::*                    LISTEN
1384/samba
tcp6       0      0 :::3269                 :::*                    LISTEN
1384/samba
tcp6       0      0 :::389                  :::*                    LISTEN
1384/samba
tcp6       0      0 :::135                  :::*                    LISTEN
1371/samba
udp        0      0 192.168.50.5:389        0.0.0.0:*
1385/samba
udp        0      0 0.0.0.0:389             0.0.0.0:*
1385/samba
udp        0      0 192.168.50.5:464        0.0.0.0:*
1386/samba
udp        0      0 0.0.0.0:464             0.0.0.0:*
1386/samba
```

```
udp        0      0 0.0.0.0:53              0.0.0.0:*
1394/samba
udp        0      0 192.168.50.5:88         0.0.0.0:*
1386/samba
udp        0      0 0.0.0.0:88              0.0.0.0:*
1386/samba
udp        0      0 192.168.50.5:137        0.0.0.0:*
1380/samba
udp        0      0 192.168.50.255:137      0.0.0.0:*
1380/samba
udp        0      0 0.0.0.0:137             0.0.0.0:*
1380/samba
udp        0      0 192.168.50.5:138        0.0.0.0:*
1380/samba
udp        0      0 192.168.50.255:138      0.0.0.0:*
1380/samba
udp        0      0 0.0.0.0:138             0.0.0.0:*
1380/samba
udp6       0      0 :::389                  :::*
1385/samba
udp6       0      0 :::464                  :::*
1386/samba
udp6       0      0 :::53                   :::*
1394/samba
udp6       0      0 :::88                   :::*
1386/samba
```

Příloha B – Výpis informací o službě Samba

systemctl status samba-ad-dc

```
samba-ad-dc.service - Samba AD Daemon
   Loaded: loaded (/lib/systemd/system/samba-ad-dc.service; enabled; vendor preset:
enabled)
   Active: active (running) since Wed 2019-09-25 18:16:49 UTC; 15s ago
     Docs: man:samba(8)
           man:samba(7)
           man:smb.conf(5)
 Main PID: 1981 (samba)
   Status: "smbd: ready to serve connections..."
    Tasks: 22 (limit: 966)
   CGroup: /system.slice/samba-ad-dc.service
           ├─1981 /usr/sbin/samba --foreground --no-process-group
           ├─2003 /usr/sbin/samba --foreground --no-process-group
           ├─2004 /usr/sbin/samba --foreground --no-process-group
           ├─2005 /usr/sbin/samba --foreground --no-process-group
           ├─2006 /usr/sbin/samba --foreground --no-process-group
           ├─2010 /usr/sbin/samba --foreground --no-process-group
           ├─2012 /usr/sbin/smbd -D --option=server role check:inhibit=yes --
foreground
           ├─2013 /usr/sbin/samba --foreground --no-process-group
           ├─2014 /usr/sbin/samba --foreground --no-process-group
           ├─2015 /usr/sbin/samba --foreground --no-process-group
           ├─2016 /usr/sbin/samba --foreground --no-process-group
           ├─2017 /usr/sbin/samba --foreground --no-process-group
           ├─2018 /usr/sbin/samba --foreground --no-process-group
           ├─2019 /usr/sbin/samba --foreground --no-process-group
           ├─2020 /usr/sbin/samba --foreground --no-process-group
           ├─2021 /usr/sbin/winbindd -D --option=server role check:inhibit=yes --
foreground
           ├─2022 /usr/sbin/samba --foreground --no-process-group
           ├─2023 /usr/sbin/samba --foreground --no-process-group
           ├─2030 /usr/sbin/smbd -D --option=server role check:inhibit=yes --
foreground
           ├─2031 /usr/sbin/smbd -D --option=server role check:inhibit=yes --
foreground
           ├─2033 /usr/sbin/winbindd -D --option=server role check:inhibit=yes --
foreground
           └─2034 /usr/sbin/smbd -D --option=server role check:inhibit=yes --
foreground

Sep 25 18:16:48 vm-pdc-005 samba[1981]:   Copyright Andrew Tridgell and the Samba
Team 1992-2017
Sep 25 18:16:48 vm-pdc-005 samba[1981]: [2019/09/25 18:16:48.299727,
0] ../source4/smbd/server.c:620(binary_smbd_main)
Sep 25 18:16:48 vm-pdc-005 samba[1981]:   samba: using 'standard' process model
Sep 25 18:16:48 vm-pdc-005 winbindd[2021]: [2019/09/25 18:16:48.543076,
0] ../source3/winbindd/winbindd_cache.c:3170(init
Sep 25 18:16:48 vm-pdc-005 winbindd[2021]:   initialize_winbindd_cache: clearing
cache and re-creating with version number
Sep 25 18:16:49 vm-pdc-005 systemd[1]: Started Samba AD Daemon.
Sep 25 18:16:49 vm-pdc-005 winbindd[2021]: [2019/09/25 18:16:49.136302,
0] ../lib/util/become_daemon.c:124(daemon_ready)
Sep 25 18:16:49 vm-pdc-005 winbindd[2021]:   STATUS=daemon 'winbindd' finished
starting up and ready to serve connections
Sep 25 18:16:49 vm-pdc-005 smbd[2012]: [2019/09/25 18:16:49.138047,
0] ../lib/util/become_daemon.c:124(daemon_ready)
Sep 25 18:16:49 vm-pdc-005 smbd[2012]:   STATUS=daemon 'smbd' finished starting up
and ready to serve connections
```

Příloha C – Výpis přidělených práv

net rpc rights list accounts -U'COMINTELLIGENCE\administrator' -I vm-pdc-005.comintelligence.local

```
BUILTIN\Print Operators
SeLoadDriverPrivilege
SeShutdownPrivilege
SeInteractiveLogonRight

BUILTIN\Account Operators
SeInteractiveLogonRight

BUILTIN\Backup Operators
SeBackupPrivilege
SeRestorePrivilege
SeShutdownPrivilege
SeInteractiveLogonRight

BUILTIN\Administrators
SeSecurityPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeSystemtimePrivilege
SeShutdownPrivilege
SeRemoteShutdownPrivilege
SeTakeOwnershipPrivilege
SeDebugPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeProfileSingleProcessPrivilege
SeIncreaseBasePriorityPrivilege
SeLoadDriverPrivilege
SeCreatePagefilePrivilege
SeIncreaseQuotaPrivilege
SeChangeNotifyPrivilege
SeUndockPrivilege
SeManageVolumePrivilege
SeImpersonatePrivilege
SeCreateGlobalPrivilege
SeEnableDelegationPrivilege
SeInteractiveLogonRight
SeNetworkLogonRight
SeRemoteInteractiveLogonRight

BUILTIN\Server Operators
SeBackupPrivilege
SeSystemtimePrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeShutdownPrivilege
SeInteractiveLogonRight

BUILTIN\Pre-Windows 2000 Compatible Access
SeRemoteInteractiveLogonRight
SeChangeNotifyPrivilege
```

Příloha D – Nastavení sdílených složek

Nastavení sdílených složek v souboru smb.conf.

nano /etc/samba/smb.conf

```
[home]
        path = /Data/Samba/002_Users_Data
        read only = no
        browseable = no
        comment = ©Home folders of domain users. ©
        force create mode = 0600
        force directory mode = 0700
[001_Firemní]
        directory_mode: parameter = 0700
        read only = no
        path = /Data/Samba/001_Company_data
        csc policy = disable
        comment = Firemní složky firmy ComIntelligence.
        public = no
        writeable = yes
        browseable = yes
[002_Data_Uživatelů]
        directory_mode: parameter = 0700
        read only = no
        path = /Data/Samba/002_Users_Data
        csc policy = disable
        comment = Osobní složky uživatelů IS.
        public = no
        writeable = yes
        browseable = yes
[003_Informace]
        directory_mode: parameter = 0700
        read only = no
        path = /Data/Samba/003_Information/
        csc policy = disable
        comment = Složky s informacemi pro uživatele IS.
        public = no
        writeable = yes
        browseable = yes
[090_Administrátor]
        directory_mode: parameter = 0700
        read only = no
        path = /Data/Samba/090_Administrators/
        csc policy = disable
        comment = Složky administrátorů IS.
        public = no
        writeable = yes
        browseable = yes
[091_Backup]
        directory_mode: parameter = 0700
        read only = no
        path = /Data/Samba/091_Backup/
        csc policy = disable
        comment = Složky záloh IS.
        public = no
        writeable = yes
        browseable = yes
```

Příloha E – DHCP skripty

Skript pro přihlášení

Skript je převzat jako celek z internetového zdroje [11].

nano /usr/bin/dhcpd-update-samba-dns.sh

```
#!/bin/bash
# Begin dhcpd-update-dns.sh
. /etc/dhcp/dhcpd-update-samba-dns.conf || exit 1
ACTION=$1
IP=$2
HNAME=$3
export KRB5CC KEYTAB DOMAIN REALM PRINCIPAL NAMESERVER ZONE ACTION IP HNAME
/usr/bin/samba-dnsupdate.sh -m &
# End dhcpd-update-samba-dns.sh
```

Skript pro ovládání záznamů v DNS

Skript je převzat jako celek z internetového zdroje [11].

nano /usr/bin/samba-dnsupdate.sh

```
#!/bin/bash
# Begin samba-dnsupdate.sh
sleep 5

checkvalues()
{
        [ -z "${2}" ] && echo "Error: argument '${1}' requires a
parameter." && exit 1

        case ${2} in

                -*)
                        echo "Error: Invalid parameter '${2}' passed to
${1}."
                        exit 1
                ;;

                *)
                        return 0
                ;;
        esac
}

showhelp()
{
echo -e "\n"`basename ${0}` "uses samba-tool to update DNS records in Samba
4's DNS"
echo "server when using INTERNAL DNS or BIND9 DLZ plugin."
echo ""
echo "    Command line options (and variables):"
echo ""
echo "      -a | --action      Action for this script to perform"
echo "                         ACTION={add|delete}"
echo "      -c | --krb5cc      Path of the krb5 credential cache
(optional)"
echo "                         Default: KRB5CC=/run/dhcpd.krb5cc"
echo "      -d | --domain      The DNS domain/zone to be updated"
```

```
echo "                           DOMAIN={domain.tld}"
echo "      -h | --help          Show this help message and exit"
echo "      -H | --hostname      Hostname of the record to be updated"
echo "                           HNAME={hostname}"
echo "      -i | --ip            IP address of the host to be updated"
echo "                           IP={0.0.0.0}"
echo "      -k | --keytab        Krb5 keytab to be used for authorization
(optional)"
echo "                           Default: KEYTAB=/etc/dhcp/dhcpd.keytab"
echo "      -m | --mitkrb5       Use MIT krb5 client utilities"
echo "                           MITKRB5={YES|NO}"
echo "      -n | --nameserver    DNS server to be updated (must use FQDN, not
IP)"
echo "                           NAMESERVER={server.internal.domain.tld}"
echo "      -p | --principal     Principal used for DNS updates"
echo "                           PRINCIPAL={user@domain.tld}"
echo "      -r | --realm         Authentication realm"
echo "                           REALM={DOMAIN.TLD}"
echo "      -z | --zone          Then name of the zone to be updated in AD.
echo "                           ZONE={zonename}
echo ""
echo "Example: $(basename $0) -d domain.tld -i 192.168.0.x -n 192.168.0.x
\\"
echo "             -r DOMAIN.TLD -p user@domain.tld -H HOSTNAME -m"
echo ""
}

# Process arguments
[ -z "$1" ] && showhelp && exit 1
while [ -n "$1" ]; do
        case $1 in

                -a | --action)
                        checkvalues ${1} ${2}
                        ACTION=${2}
                        shift 2
                ;;

                -c | --krb5cc)
                        checkvalues ${1} ${2}
                        KRB5CC=${2}
                        shift 2
                ;;

                -d | --domain)
                        checkvalues ${1} ${2}
                        DOMAIN=${2}
                        shift 2
                ;;

                -h | --help)
                        showhelp
                        exit 0
                ;;

                -H | --hostname)
                        checkvalues ${1} ${2}
                        HNAME=${2%%.*}
                        shift 2
                ;;
```

```
                -i | --ip)
                        checkvalues ${1} ${2}
                        IP=${2}
                        shift 2
                ;;

                -k | --keytab)
                        checkvalues ${1} ${2}
                        KEYTAB=${2}
                        shift 2
                ;;

                -m | --mitkrb5)
                        KRB5MIT=YES
                        shift 1
                ;;

                -n | --nameserver)
                        checkvalues ${1} ${2}
                        NAMESERVER=${2}
                        shift 2
                ;;

                -p | --principal)
                        checkvalues ${1} ${2}
                        PRINCIPAL=${2}
                        shift 2
                ;;

                -r | --realm)
                        checkvalues ${1} ${2}
                        REALM=${2}
                        shift 2
                ;;

                -z | --zone)
                        checkvalues ${1} ${2}
                        ZONE=${2}
                        shift 2
                ;;

                *)
                        echo "Error!!! Unknown command line opion!"
                        echo "Try" `basename $0` "--help."
                        exit 1
                ;;
        esac
done

# Sanity checking
[ -z "$ACTION" ] && echo "Error: action not set." && exit 2
case "$ACTION" in
        add | Add | ADD)
                ACTION=ADD
        ;;
        del | delete | Delete | DEL | DELETE)
                ACTION=DEL
        ;;
        *)
                echo "Error: invalid action \"$ACTION\"." && exit 3
        ;;
```

```
esac
[ -z "$KRB5CC" ] && KRB5CC=/tmp/dhcpd.krb5cc
[ -z "$DOMAIN" ] && echo "Error: invalid domain." && exit 4
[ -z "$HNAME" ] && [ "$ACTION" == "ADD" ] && \
     echo "Error: hostname not set." && exit 5
[ -z "$IP" ] && echo "Error: IP address not set." && exit 6
[ -z "$KEYTAB" ] && KEYTAB=/etc/dhcp/dhcpd.keytab
[ -z "$NAMESERVER" ] && echo "Error: nameservers not set." && exit 7
[ -z "$PRINCIPAL" ] && echo "Error: principal not set." && exit 8
[ -z "$REALM" ] && echo "Error: realm not set." && exit 9
[ -z "$ZONE" ] && echo "Error: zone not set." && exit 10

# Disassemble IP for reverse lookups
OCT1=$(echo $IP | cut -d . -f 1)
OCT2=$(echo $IP | cut -d . -f 2)
OCT3=$(echo $IP | cut -d . -f 3)
OCT4=$(echo $IP | cut -d . -f 4)
RZONE="$OCT3.$OCT2.$OCT1.in-addr.arpa"

kerberos_creds() {
export KRB5_KTNAME="$KEYTAB"
export KRB5CCNAME="$KRB5CC"

if [ "$KRB5MIT" = "YES" ]; then
    KLISTARG="-s"
else
    KLISTARG="-t"
fi

klist $KLISTARG || kinit -k -t "$KEYTAB" -c "$KRB5CC" "$PRINCIPAL" || chmod
600 "$KRB5CC" || { logger -s -p daemon.error -t dhcpd kinit for dynamic DNS
failed; exit 11; }
}


add_host(){
    logger -s -p daemon.info -t dhcpd Adding A record for host $HNAME with
IP $IP to zone $ZONE on server $NAMESERVER
   /usr/bin/samba-tool dns add $NAMESERVER $ZONE $HNAME A $IP -k yes
}


delete_host(){
    logger -s -p daemon.info -t dhcpd Removing A record for host $HNAME
with IP $IP from zone $ZONE on server $NAMESERVER
     /usr/bin/samba-tool dns delete $NAMESERVER $ZONE $HNAME A $IP -k yes
}


update_host(){
    logger -s -p daemon.info -t dhcpd Removing A record for host $HNAME
with IP $CURIP from zone $ZONE on server $NAMESERVER
     /usr/bin/samba-tool dns delete $NAMESERVER $ZONE $HNAME A $CURIP -k
yes
    add_host
}


add_ptr(){
    logger -s -p daemon.info -t dhcpd Adding PTR record $OCT4 with hostname
$HNAME to zone $RZONE on server $NAMESERVER
```

```
     /usr/bin/samba-tool dns add $NAMESERVER $RZONE $OCT4 PTR
$HNAME.$DOMAIN -k yes
}


delete_ptr(){
    logger -s -p daemon.info -t dhcpd Removing PTR record $OCT4 with
hostname $HNAME from zone $RZONE on server $NAMESERVER
     /usr/bin/samba-tool dns delete $NAMESERVER $RZONE $OCT4 PTR
$HNAME.$DOMAIN -k yes
}


update_ptr(){
    logger -s -p daemon.info -t dhcpd Removing PTR record $OCT4 with
hostname $CURHNAME from zone $RZONE on server $NAMESERVER
     /usr/bin/samba-tool dns delete $NAMESERVER $RZONE $OCT4 PTR $CURHNAME
-k yes
    add_ptr
}


case "$ACTION" in
    ADD)
        kerberos_creds
        host -t A $HNAME.$DOMAIN > /dev/null
        if [ "${?}" == 0 ]; then
          CURIP=$(host -t A $HNAME.$DOMAIN | cut -d " " -f 4 )
          if [[ "$CURIP" != "$IP" ]]; then
             update_host
          fi
        else
           add_host
        fi

        host -t PTR $IP > /dev/null
        if [ "${?}" == 0 ]; then
           CURHNAME=$(host -t PTR $IP | cut -d " " -f 5 | rev | cut -c 2- |
rev)
           if [[ "$CURHNAME" != "$HNAME.$DOMAIN" ]]; then
              update_ptr
           fi
        else
           add_ptr
        fi
    ;;

    DEL)
        kerberos_creds
        host -t A $HNAME.$DOMAIN > /dev/null
        if [ "${?}" == 0 ]; then
            delete_host
        fi

        host -t PTR $IP > /dev/null
        if [ "${?}" == 0 ]; then
            delete_ptr
        fi
    ;;

    *)
```

```
        echo "Error: Invalid action '$ACTION'!" && exit 12
    ;;

esac

# End samba-dnsupdate.sh
```

Příloha F – Zavedení Group Policy

Zavedení GP do klientského počítače.

gpresult /R

```
Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© 2019 Microsoft Corporation. All rights reserved.
Created on 17.10.2019 at 22:29:16

RSOP data for COMINTELLIGENCE\test on VM-W-001 : Logging Mode
-------------------------------------------------------------
OS Configuration:            Member Workstation
OS Version:                  10.0.18362
Site Name:                   N/A
Roaming Profile:             N/A
Local Profile:               C:\Users\test
Connected over a slow link?: No

USER SETTINGS
--------------
    CN=Test,OU=Users,DC=comintelligence,DC=local
    Last time Group Policy was applied: 17.10.2019 at 22:28:00
    Group Policy was applied from:      vm-pdc-005.comintelligence.local
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        COMINTELLIGENCE
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    -----------------------------
        201_Users_Local_PoliciesWin10-1607 User Security Compliance

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Default Domain Policy
            Filtering:  Not Applied (Empty)

        Místní zásady skupiny
            Filtering:  Not Applied (Empty)

    The user is a part of the following security groups
    ---------------------------------------------------
        Domain Users
        Everyone
        Remote Desktop Users
        BUILTIN\Users
        REMOTE INTERACTIVE LOGON
        NT AUTHORITY\INTERACTIVE
        NT AUTHORITY\Authenticated Users
        This Organization
        LOCAL
        Střední povinná úroveň
```

Příloha G – Obsah DVD

Přílohou diplomové práce je DVD disk, který obsahuje nastavený virtuální stroj (VM verze 9) na virtualizační platformě Hyper-V, konfiguraci routeru, testovací software, nastavení práv ke sdíleným složkám, uživatelské účty, hesla a popis uvedení VM do provozu.