Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Využití Windows Server 2016 pro zabezpečení LAN

Diplomová práce

Autor: Bc. Lenka Folprechtová

Studijní obor: Aplikovaná informatika

Vedoucí diplomové práce: Mgr. Horálek Josef, Ph.D.

Hradec Králové Srpen 2019

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracovala samostatně a s použitím uvedené literatury.

V Hradci Králové dne 15.08.2019 Bc. Lenka Folprechtová

Poděkování:

Děkuji tímto vedoucímu diplomové práce, panu Mgr. Josefu Horálkovi, Ph.D., za jeho trpělivé metodické směrování a užitečné rady při tvorbě této práce.

Anotace

Cílem práce je provést podrobnou analýzu principů zabezpečení LAN za využití Windows Serveru 2016 a jeho nových vlastností z oblasti bezpečnosti. Autor práce zmapuje a podrobně popíše nová bezpečnostní opatření implementované ve Windows Serveru 2016 a navrhne jejich nasazení a využití pro zvýšení bezpečnosti LAN. V praktické části autor představí konkrétní postupy a konfiguraci Windows Serveru 2016 s dopadem na zabezpečení LAN formou případové studie v reálném prostředí firmy.

Annotation

Title: Usage of Windows Server 2016 for LAN security

The aim of this thesis is to conduct a detailed analysis of LAN security principles by using Windows Server 2016 and its new security features. The author of the thesis will review and describe the new security measures that are implemented in Windows Server 2016 and will propose their deployment and usage to increase LAN security. In the practical part the author will present the specific procedures and Windows Server configuration with the impact to LAN security by the case study in a real company environment.

Obsah

Teoretická část práce

1 Úvod

Moderní životní styl nabízí používání informačních a komunikačních technologií téměř na každém kroku. Informační systémy se objevují nejen v podnikání, ale také v soukromém životě. Útoky cílené proti informačním technologiím se vyskytují po celém světě a všudypřítomné kybernetické hrozby vyžadují zaměření se na ochranu důležitých aktiv. Tato aktiva se stále více přesouvají do kyberprostoru, kde jim hrozí narušení z různých zdrojů. Důležitost kybernetické bezpečnosti, a reálnou hodnotu aktiv si jejich vlastník uvědomí až při zničení, zneužití nebo jejich nedostupnosti.

Veškerá rizika kybernetické bezpečnosti není možné naprosto eliminovat, aniž bychom nepřestali využívat síťová připojení a internet. Kyberútoky jsou stále více sofistikovanější a zranitelnosti se vždy najdou, dříve či později. Proto je potřeba se naučit je nacházet dřív, než by mohly být zneužity a takové situace zvládnout. Hodnocením a konzultací, monitorováním a přezkoumáváním rizik se zabývá proces řízení rizik. Řízením rizik zvyšujeme úspěšnost organizace dosáhnout svých cílů s optimálním využitím cenných zdrojů. Systém řízení bezpečnosti informací (Information Security Management Systém, ISMS) je odrazem cyklického procesu řízení rizik a dokumentuje ochranu informačních aktiv. Více je pojem ISMS popsán v normách ISO/IEC 27000.

Jelikož je nemožné rizika absolutně vyloučit, bylo napsáno tisíce návodů, dokumentací a rad, jak rozpoznat hrozbu dřív, než nám uškodí. Existuje několik modelů, jak kybernetické hrozby zařadit a rozpoznat. Jeden z nich je i model CIA. Základní atributy podle modelu CIA jsou důvěrnost, integrita a dostupnost (Confidentiality – Integrity – Availability, tz. CIA triad). Kybernetické útoky jsou vedeny na tyto tři pilíře. Model nás seznamuje s tím, jak zacházet s daty, jak je analyzovat, upravovat a přistupovat k nim. Podobné modely jsou vhodným úvodem do informační a kybernetické bezpečnosti, která musí aktivně podporovat obchodní cíle společnosti. Tato práce se snaží přiblížit popisem vhodných technologií k ideálu hladkého firemního provozu.

Cílem práce je sestavením návrhu LAN naplnit požadavky kladené v systému ISMS a náležitosti ve vyhlášce o kybernetické bezpečnosti – vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat. V této práci budou popsány možnosti zabezpečení operačního systému Windows Server 2016 ve vybraném prostředí LAN, které budou spojeny s vyhláškou o kybernetické bezpečnosti především z technického hlediska. Práce bude zjišťovat, jestli Windows Server poskytuje dostatečné prostředky pro splnění nejdůležitějších požadavků pro fungování v praxi a následně představí jejich implementaci v případové studii. Budou využity obvyklé a vyzkoušené prostředky ze starších verzí serverových operačních systémů Microsoft, ale i nově přidané funkcionality, které v předchozích verzích systémů použít nelze. Ve vyhlášce se kybernetická bezpečnost dělí na procesní a technické požadavky.

V procesních požadavcích jsou popsány nároky na řízení procesů, organizační bezpečnost a kontinuita činností v provozu, a následné auditování se zvládáním kybernetických bezpečnostních událostí a incidentů. Technická opatření popisují správu identit v síti a heslové politiky, požadavky na ochranu před škodlivým kódem, zaznamenávání procesů a logování událostí, kryptografické prostředky a penetrační testování navržených řešení. Udávají požadavky na oprávnění a přístupy uživatelů v síti, monitorování potencionálních zranitelností. Celý zákon je k dispozici online ve zdroji (NCKB, 2018, cit. 2019-26-6).

Práce je rozdělena na teoretickou a praktickou část. V druhé kapitole budou popsány možnosti využití Windows Serveru 2016, krátce seznámí se serverovými rolemi a rolí Active Directory. Třetí kapitola vyjmenuje nové možnosti, které byly do této verze systému přidány, budou popsány jejich technické požadavky a příklady, kdy dané funkcionality využít. Podrobněji zde budou popsány Windows kontejnery, nové způsoby využití virtuálních strojů a část věnující se novým zabezpečujícím možnostem. Další kapitoly se vrací k známým způsobům využití prostředí Microsoft Windows, čtvrtá kapitola se zabývá konkrétněji Active Directory a problematice trustu mezi doménami. Následují kapitoly popisují principy fungování LDAP, SSO a protokolu Kerberos. Kapitola osm se zabývá možnostmi firewallu a jeho rozdělení. Následuje

kapitola devátá, která nastiňuje základy shellu a skriptovacího jazyka od Microsoftu – Windows Powershell.

Desátá kapitola pojednává o síťových prvcích obecně, seznámí s modelem ISO/OSI a zaměřuje se na slabá místa některých protokolů, které se v síťování používají. Poslední kapitola v teoretické práci ukazuje průzkum nedávných hrozeb s doporučením, jak se jim vyhnout. Také jsou zde s pomocí statistik z CVE krátce porovnány dvě poslední verze Windows Serveru.

V praktické části jsou popsány kroky konfigurace serverové stanice a pracovních stanic pomocí nástrojů Powershell. Stoje jsou virtualizovány s VMware Workstation a přes router s firewallem jsou spojeny s internetem na hostitelském počítači. Požadavky pro tuto síť budou nasazeny na potřeby malé firmy zabývající se vývojem webových aplikací. Popsány budou konfigurace Active Directory a group policy, DNS, DHCP a novinky pro Windows Server 2016 jako jsou kontejnery, Just Enough Administration nebo Credential Guard. Budou se brát ohledy na bezpečnost a splnění požadavků ve vyhlášce o kybernetické bezpečnosti. V dalších kapitolách praktické části budou popsány možnosti Windows firewallu a auditování událostí, které se dějí na stanicích v LAN. Nakonec bude v práci popsán budoucí vývoj a další doporučení.

2 Možnosti Windows Server 2016

S Windows Server lze vystavět funkční a flexibilní řešení firemní sítě. Pokud nevybereme instalaci Windows Server Core, serverové role lze klasicky nainstalovat přes známou konzoli Server Manager, která od poslední verze sice prošla pár změnami, není ale pochyb, že změny směřují k lepší a přehlednější správě firemních strojů. Přes Server Manager lze spravovat celou infrastrukturu sítě, k tomu pomáhá vzdálený přístup a několik dalších vestavěných nástrojů jako jsou RSAT (Remote Server Administratiton Tool) a PAW (Privileged Access Workstation). Ve Windows Server Core není Server Manager dostupný, stejně tak některé role a služby nejsou zahrnuty a ke správě slouží PowerShell. Do PowerShell přibylo pro správu mnoho nových příkazů, o kterých se bude psát v pozdější části práce. Při výběru instalačního balíčku velice záleží na potřebách sítě a administrátorských zkušenostech.

V této kapitole budou popsány nejhlavnější serverové role, které jsou potřeba pro implementaci v praktické části práce. Přidávání rolí znamená přidávání zásadních funkcionalit a komponent spouštějících danou funkcionalitu důležitou pro server. Role lze uživatelsky upravovat a doplňovat pomocí služeb a features. Důležitou část práce přestavuje i Active Directory, které hraje v architektuře sítě velkou roli, v kapitole proto bude popsáno, jak zajišťuje bezpečnostní prvky.

2.1 Hyper-V a virtualizace

Role Hyper-V nám dovoluje vytvářet několik virtuálních strojů na stejném hardwaru, využíváme tak hardware mnohem efektivněji. Virtuálním strojům říkáme, že hostují na svém Hyper-V hostiteli. Základem je hypervisor Hyper-V, virtualizační vrstva. Můžeme tak centrálně spravovat infrastrukturu (VDI, Virtual desktop infrastructure) – clustery, migrace a rozložení zdrojů v síti. WS2016 podporuje nově i instalaci Linuxových a FreeBSD virtuálních strojů.

Virtuální stroje jsou přenosné a při použití Hyper-V Replica poskytují strategii pro zajištění obnovy virtuálních strojů a dat na nich uložených. S novým stavem virtuálního stroje Connected Standby může být stroj uložený v úsporném režimu, když jeho zdroje nejsou zrovna používány. Přesto ale může ihned přejít do plně funkčního stavu.

Pro failover cluster můžeme mít maximální počet uzlů 64, s až 8 000 virtuálních strojů v clusteru. Proběhlo navýšení podporované velikosti RAM až na 12TB (pouze pro VM generation 2), což se pravděpodobně bude týkat velkých datových center, než běžných firemních podmínek. Nová feature Nested virtualization se dá použít v testovacích a vývojových prostředích, když na virtuálním stroji využijeme znovu Hyper-V a použijeme ho jako hostitele pro další virtuální stroj. WS2016 také zaručuje okamžitý přechod na záložní virtuální stroj, pokud má primární zdroj výpadek. Jestliže se tak u jednoho znovu spuštěného stroje situace opakuje, systém uloží virtuální stroj automaticky do karantény – Node quarantine zjistí, že se objevuje nějaký problém a izoluje stroj od ostatních, nevyužívá pak zdroje a nelze ho použít ani pro migrace. V tu chvíli může přijít administrátor a manuálně zjistit, co se v síti stalo a stroj znovu zprovoznit. Možnosti Hyper-V jsou rozsáhlé a na veškerý popis funkcionalit by bylo potřeba mnohem více prostoru.

Přestože samotný návrh LAN bude vystavěn přes nástroje VMware, funkcionalita virtualizace bude využita v praktické části práce v části o kontejnerech. V kapitole o nových možnostech bude lépe popsán nový Nano server a security hardening v oblasti virtuálních strojů, zahrnující Secure boot, Shielded VMs a TPM. Stejně tak nové funkcionality ve virtualization-based security, jedná se o Device Guard a Credential Guard.

2.2 DNS a DHCP

Služby AD DS (Active Directory Domain Services) jsou úzce spjaté s DNS (Domain Name Services), bez které v podstatě nemohou fungovat. DNS slouží pro překlad jmen objektů na adresy v síti, distribuuje databázi se jmennými prostory a doménami, v AD lokalizuje doménový řadič. Je to jeden z nejdůležitějších prvků pro Windows administrátory, proto služba DNS bude v práci zmíněna ještě několikrát. Při pohledu na bezpečnost, je DNS často napadána způsobem, kdy jsou změněny DNS záznamy a tím přesměrována komunikace (DNS cache poisoning). Mohou se tím způsobit výpadky při přihlašování v síti nebo problémy při replikaci a další. Proti tomu se WS2016 brání například podporou DNSSec, který používá šifrovací nástroje pro

záznamy v tabulkách. Ve WS2016 je nově feature DNS policies, ve kterých mohou administrátoři spravovat, jak bude DNS server odpovídat na klientské požadavky.

Důležitou součástí je spravování DNS zón a jejích záznamů a delegování informací na doménové řadiče v síti. Pravidlem bývá, že při vyšším počtu DNS serverů na jednom pracovišti pro překlad jmen odkazují nejprve navzájem a následně až samy sebe. Vhodných řešení je několik, práce se snaží řídit se jimi v souladu s bezpečností.

O automatické přiřazování IP adres a nakonfigurování defaultní brány se stará server s rolí DHCP (Dynamic Host Configuration Protocol). Pro sítě s desítkami klientů a zařízení by bylo nemožné adresovat vše manuálně, k tomu má DHCP v databázi přiřazený rozsah adres, se kterými může pracovat z centrálního místa (v případě výpadku se requesty odesílají na záložní DHCP server).

Pokud se rozhodneme používat SDN, k překladu jmen slouží integrovaná služba iDNS (Internal DNS). Stejně jako v klasické LAN je potřeba, aby v SDN virtuální stroje a aplikace mohly komunikovat mezi sebou nebo externími zdroji v Internetu. Jelikož iDNS server je oddělený přes iDNS proxy (ten je na každém Hyper-V hostiteli) od virtuálních sítí, chrání ji tak před škodlivými transakcemi, a přitom vidíme provoz v síti. Výhodou je provázanost s Active Directory.

2.3 File and Storage Services

File and Storage Services je role, která je defaultně nainstalovaná ve Windows Server i ve Windows Server Core. Rozšiřuje ji však mnoho služeb jako je Data Deduplication, DFS Namespaces, DFS Replication, File Server Resource Manager a další. Služby definují, jestli chceme ušetřit místo na disku a deduplikovat data, seskupovat sdílené soubory na rozdílných serverech do logicky spojených celků. Můžeme nastavit replikaci, která bude v záloze měnit pouze soubory, které se od poslední replikace změnily a nepřenášet zálohu celou. Lze nainstalovat službu s iSCSI blokově orientovaným protokolem pro úložiště spojující cílové diskové pole s klientem.

Windows používá šifrovací technologii **BitLocker**, která se poprvé objevila už ve Windows Vista a Windows Server 2008. Od té doby je součástí všech serverových řešení, u desktopových řešení není dostupná v edici Home. S BitLockerem můžeme

šifrovat celé disky nebo pouze některé oddíly, SD karty, aj. Jako šifrovací algoritmus používá symetrický blokový AES (Advanced Encryption Standard), kdy si sami můžeme nastavit délku klíče (128bit/256bit), ve Windows 10 můžeme i zvolit způsob šifrování oddílů mezi AES-CBC a XTS-AES. Microsoft doporučuje mít na klientské stanici, kde chceme použít BitLocker, SSD disk a TPM 2.0. Zálohy z počítače tak můžeme uložit v AD DS zašifrované a chráněné.

O nových možnostech Storage Space Services a souborovém systému ReFS bude více napsáno v pozdější kapitole.

2.4 Role Active Directory

Oficiální dokumentace od Microsoft poskytuje několik doporučení, jak zvýšit bezpečnost služby AD, chránit klíčové segmenty sítě a jak provádět kontroly IT prostředí.

V AD se většinou cílí na menší segmenty organizační topologie, než se útok rozšíří do dalších částí jako jsou aplikační a datové servery nebo uživatelské pracovní stanice. Provést takový útok lze přes nesprávně nastavená práva účtů a skupin. Často jde o účty s příliš vysokými privilegii, která nejsou potřeba pro práci uživatele. V AD můžeme implementovat skupinu Secure Administrative Hosts, což jsou hostitelské stanice, ze kterých je bezpečné řídit administraci v AD. Tyto podmínky nám potom zakazují provádět administrátorské úkony z nedůvěryhodných zdrojů a podporují nás ve vícefaktorové autentizaci, kdy nesmíme zapomenout ani na fyzickou bezpečnost úložiště pro důvěryhodné hostitele (např. velké firemní serverovny). Přestože se většina firem brání firewally, antiviry a dalšími nástroji pro sledování nebezpečí, která přicházejí z veřejné sítě, často je problém hlavně u internistů. Jakmile má někdo fyzický přístup k interním prostorům, má přístup i ke stanicím, odkud lze zjistit spoustu věcí, které se na první pohled mohou zdát bezvýznamné. Z toho důvodu je vícefaktorová autentizace tolik zdůrazňována, stejně tak šifrování virtuálního prostředí (např. Shielded VMs, kdy i po zcizení VHD je v podstatě k ničemu, pokud nevlastníte dostatečná práva).

Nastavení politik pro skupiny uživatelů, Group Policy, je jeden ze způsobů zabezpečení infrastruktury. Od minulých verzí se hlavní struktura ve WS2016 příliš

nezměnila, přidalo se pouze několik nových funkcionalit, např. nové cmdlety pro PowerShell. Skupinové politiky se dají nastavit v Group Policy Management Console pro uživatele, domény, organizační jednotky nebo pro sites. Skupinové politiky jsou užitečné při nastavení heslové politiky, nebo zakázání USB zařízení, tedy zamknutí portů pro USB, a dalších.

Pomocí skupinových politik lze také nastavit auditování bezpečnostních logů v síti. Jelikož může na jednom doménovém řadiči projít velké množství informací, které bychom se snažili sledovat, je vhodné nastavit, že chceme pozorovat pouze některé kategorie logů. Ve WS2016 máme dvě možnosti – Basic security audit policies a Advanced security audit policies. Lze se zaměřit třeba jen na neúspěšné pokusy o přihlášení nebo autentizaci, přístupy k objektům, změny v privilegiích účtů nebo stavy procesů. V dalším kroku je potřeba logy také zpracovat a prakticky zobrazit, k čemuž se využívá několik různých řešení – ať už komerční nebo neplacené řešení. Na řadu zde mohou přijít i skripty s cdmlety v PowerShell, které si správce sítě musí napsat sám, popřípadě investovat do řešení od jiných firem, jak bude popsáno v praktické části práce.

Active Directory Domain Services

Větší pozornost je potřeba věnovat zabezpečení doménového řadiče, který je pro roli AD DS klíčový a hostuje AD databázi v ntds.dit souboru. AD DS řídí celé Active Directory, autentizaci a autorizaci uložených objektů, se kterými v síti pracujeme, je vhodné v něm definovat skupinové politiky. Dle zkušeností se ukazuje, že nejčastější pochybení jsou zapříčiněna lidskou chybou. Jednou z možností, jak se proti takovým chybám bránit, je používat Server Core instalace, kde je nižší možnost útoku, namísto systémů s desktopovými prvky. Další možnost, kterou přinesl až WS2016, je princip Just Enough Administration a Just in Time Administration, které budou více probrány v kapitole o nově přidaných možnostech. Správci sítě někdy zbytečně používají vysoká administrátorská privilegia k úkonům, ke kterým to není potřeba. Jedná se o účty jako jsou Domain Admins, Enterprise Admins, Schema Admins a Built-in Administrators pro jednotlivé skupiny, které mají defaultně přístup k AD. Nad přiřazením uživatele do administrátorské skupiny je třeba se důkladně zamyslet a takové účty přísně monitorovat.

Vzdálený přístup na doménový řadič přes PowerShell je příhodnější než využití RDP, protože snižuje možnost zanesení malware na doménový řadič. Stejně tak můžeme využívat pro ovládání a přístup do AD konzole – AD Administrative Center, AD Users and Computers, AD Sites an Services, AD Domains and Trusts.

AD Administrative Center je velmi ceněný pomocník kvůli funkcionalitě vyhledávání. Jak radí v knize (Thomas, 2017, ch. 4), lze vyhledávat uživatele, kterým je potřeba věnovat vyšší pozornost – uživatele, kteří se nepřihlásili po určitou dobu, uživatele s nastaveným heslem, jehož platnost nikdy nevyprší, nebo poslední úpravy na vybraném uživateli.

AD Sites and Services slouží k replikaci provozu v síti a dalších aspektů spojení (např. přidávání uzlů, geografická lokace sites), souvisí s propojením domén v rámci lesa, které sdílí sites. AD Domains and Trusts spravuje vztahy mezi trusty. Defaultně všechny domény v rámci lesa mají mezi sebou trust, v této konzoli lze nastavit trusty mezi domény ostatních lesů nebo Kerberos realms.

Zahrnuté PAM (Privileged Access Management) v AD DS pomáhá kontrolovat prostředí AD s ohledem na bezpečnost a privilegia účtů, hlídá i dočasné členství ve skupinách pomocí vypršelých TGT a TGS (bude vysvětleno v kapitole o protokolu Kerberos), což v dnešní době hybridních sítí chrání uživatelská oprávnění před zneužitím.

Active Directory Lightweight Directory Services

Role AD LDS v podstatě poskytuje podobné funkcionality jako AD DS, není ale závislý na DNS, nepodporuje skupinové politiky ani na něm nelze ukládat globální katalog. Přestože na něj lze replikovat data z DC přes sites, nepodporuje trusty a nemůžeme přes LDS spravovat ostatní pracovní stanice. Můžeme ho využít jako „odlehčenou“ verzi adresáře poskytující informace o uživatelích pro webové služby, které je někdy kvůli bezpečnosti lepší oddělit od informací, které ke svému chodu vůbec nepotřebuje. Když nainstalujeme roli na server (lze instalovat i na klientské stanice), na kterém běží aplikace, přístup k informacím je mnohem rychlejší a nemusíme server vést jako doménový řadič.

Certificate Services

Nespočet organizací používá PKI (Public Key Infrastructure) pro bezpečnostní opatření, např. k zabezpečení webových serverů, šifrování emailů, autentizace s pomocí certifikátů a digitálních podpisů, a další. AD CS poskytuje implementaci k přístupu k digitálním certifikátům a certifikačním autoritám (CA, Certification Authorities). Obsahuje služby k připojení uživatele k certifikační autoritě (CA Web Enrollment), k získání informací o jejich zápisu v certifikační politice (Certificate Enrollment Policy Web Service), služby umožňující obnovovat certifikáty, i když je uživatel zrovna mimo bezpečné hranice sítě (Certificate Enrollment Web Service), služby pro získání nových certifikátů pro síťová zařízení (Network Device Enrollment Service), dostávat oznámení o tom, jestli jsou certifikáty stále validní a není potřeba je aktualizovat.

Umožňuje zabezpečit VPN, NAP (Network Access Protection), IPSec (Internet Protocol Security). Předtím než se nainstaluje role AD CS, je potřeba, aby server byl zařazený do domény s AD DS a byla mu přiřazena statická IP adresa, protože po instalaci tyto specifikace již nelze změnit. Po nainstalování můžeme využívat výhod spojení se skupinovými politikami a přiřazovat k uživatelům a zařízením, které typy certifikátů mohou používat.

Windows Server Update Services

Klíčovou komponentou pro troubleshooting vystavěné sítě, je dobrý popis aktuálního stavu v dokumentaci. Přestože může být dokumentace vedena kvalitně, průběžné aktualizace jednotlivých částí můžou být větším problémem. Konfigurace síťových zařízení se často mění, podstupují renovací a na tyto změny je třeba reagovat.

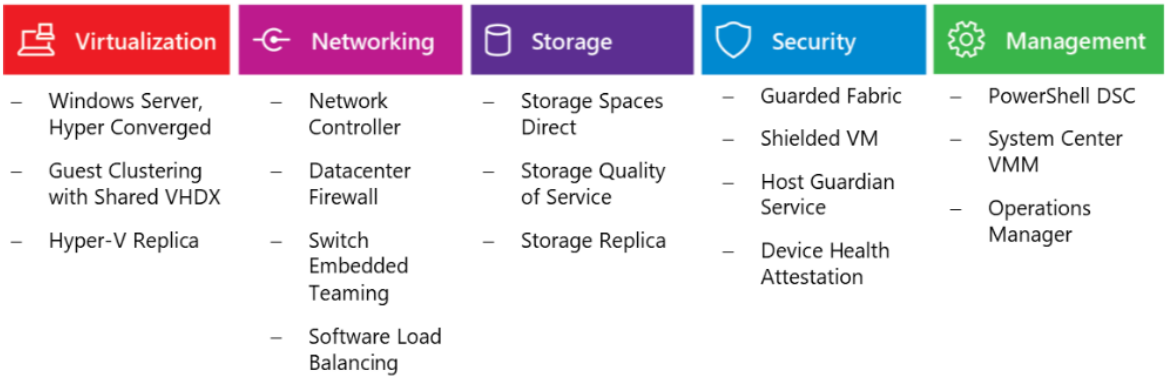
WSUS umožňuje stahování posledních aktualit produktů od Microsoft, spravování verzí software na všech stanicích v síti z jednoho centralizovaného místa. Lze nastavit automatický update, popřípadě povolit aktualizace jen některých částí nebo se můžeme rozhodnout, že se update automaticky nebude provádět vůbec, dokud je administrátor ručně nespustí. Důležitost aktualizací bude zdůrazněna v kapitole č. 11, kdy budou popsány zranitelnosti vzniklé kvůli zastaralým částem softwaru nebo používání zastaralých principů.

Ve Windows Server máme samozřejmě několik dalších rolí jako jsou Federation Services, Rights Management Services, Remote Access, Print and Document services nebo Web Server IIS, podrobnější informace o všech rolích lze najít v oficiální dokumentaci od Microsoft. Je třeba brát v potaz i dodatečné služby, které se k některým z rolí instalují defaultně. Takové služby kolikrát ani nevyužijeme a mohou se stát zbytečnou zranitelností – je na místě kontrolovat, jestli jsou takové služby pro naši infrastrukturu potřebné a případně je zak

ázat.

3 Nové možnosti využití Windows Server 2016

Aby služby od firmy Microsoft zůstaly stále jedny z nejoblíbenějších, je nutné pozorovat trendy a vyvíjet stále nová a lepší řešení. V této kapitole bude popsáno, co je nové ve WS2016 a co nebylo v předchozí verzi Windows Server 2012 (WS2012). Budou popsány funkce a výhody, kvůli kterým by měli IT správci přemýšlet o nasazení WS2016. Objeví se zde změny v rozestavění sítě, využití úložiště, uživatelského prostředí a jeho správy a v neposlední řadě zásady bezpečnosti, o níž se vývojáři WS2016 zajímali více do hloubky. Jedná se hlavně o mnohem komplexnější zabezpečení virtuálních prostředí.



Obr. 1: Virtualizace a technologie
Zdroj: Windows Server Software-Defined solution (Microsoft, 2017)

Dříve, když Microsoft vydal novou verzi OS Windows Serveru, zjišťoval, jak se zákazník zachová a jaké služby využije. Na základě toho pak přišly změny, které přidal do verze Release 2 (např. WS2012 R2). Zatímco hotfixy vydává Microsoft

do podporovaných verzí OS každý měsíc, větší opravy pro zvýšení výkonu, nebo někdy i přidání nové funkcionality, se přesouvají do Service Release, do verze R2.

Pro WS2016 se tento trend lehce mění, protože většina nových služeb a technologií, které budou popsány níže, se nejdříve objevily k vyzkoušení a ověření funkčnosti ve službě Microsoft Azure. Následující podkapitoly o novinkách čerpají ze série videí dostupných na Microsoft Virtual Academy (Hynes a Ralston, 2016).

3.1 Licenční podmínky

Ke změnám technického rázu, ale i k větším změnám v licenčních podmínkách došlo už při vydání WS2012. Licenční politika se zjednodušila, z mnoha edic a modulů přiřazování se staly dvě hlavní edice rozdělující licence dle počtu procesorů a množství uživatelů v provozu – Standard a Datacenter, které doplňuje edice Essentials pro menší organizace. I v takovém případě se mohlo v praxi stát, že se vyskytly nejasnosti ve výkladu a pochopení, kolik licencí je potřeba, aby nevznikly licenční chyby.

Nyní se místo počtu procesorů licencují fyzická jádra, což je nejvýraznější změna k licenční politice ve WS2016. Práva pro virtualizaci zůstávají podobná jako pro dřívější verze Standard, kde jsme mohli na fyzickém stroji spustit dva virtuální stroje (je třeba si dávat pozor na pokrytí licencí při celkovém minimu, což je 16 jader, tedy 8 balíčků – ty se musí násobit, pokud chceme na daném serveru spustit více virtuálních strojů), a Datacenter, kde počet virtuálních strojů není omezen.

Pokud má zákazník předplacenou službu Software Assurance (SA), můžeme využít úplně nové právo použít k provozu veřejný cloud Microsoft Azure (Microsoft TechNet, 2016) a čerpat další výhody.

Edice se liší i tím, co mohou z novinek popsaných dále nabídnout. Pro kontroly a audity je ale nutné mít správné licence na všechny své stroje, hlavně ve virtualizovaných prostředích, kde se často virtuální stroje přesouvají nejen kvůli odstávkám serverů a uzlů v síti, ale i kvůli přeorganizovaní zátěže jednotlivých strojů a následné úspoře elektrické energie. Je nutné znát všechny migrační scénáře a nejlépe mít tyto scénáře důkladně sepsané ve firemní dokumentaci, pro případné kontroly licencí přiřazené určitým strojům, abychom se vyhnuli složité správě migrací licencí (ty se od určitého stroje nedají předat dříve než po uplynutí 90 dní) a nesnižovalo se

tak robustnost řešení. SA se dá využít i k použití práva License Mobility, které je velice výhodné, pokud firma provozuje aplikační servery a nechce na všechny uzly v síti pořizovat drahá licenční řešení, jež se liší od licenční politiky Windows Server (na ty se License Mobility uplatnit nedá, pro každý cluster využívající Live Migration je potřeba mít licenci pro souběžně spuštěné virtuální stroje).

3.2 Nano server

Myšlenka Nano serveru tkví v tom, že pokud chceme co nejlépe rozložit zátěž sítě, je potřeba minimální množství paměti pro službu nebo aplikaci, aby byla snadno přenositelná a zbytečně nezabírala místo pro další prostředky. Proto se vyvinul Nano server, podobá se Windows Serveru v Core módu, je ale ještě menší s nejdůležitějšími vlastnostmi pro běh jádra, bez uživatelského interface (GUI) a nadbytečných aktualizací, proto je zde snížená možnost útoku na takový server. Zranitelnost serveru snižuje i nízký počet aplikací, které jsou zde spuštěné. Podporuje pouze 64-bit aplikace a nemá winlogon, přihlásit se k němu lze pouze vzdáleně. K jeho správě je nutné ovládat PowerShell nebo lze použít Remote Server Administration Tools.

Nano server snižuje nároky na správu serveru a jelikož velikost Nano serveru záleží na naší konfiguraci (Just enough OS), nevyžaduje tolik zdrojů jako kdybychom řídili obvyklý server. Z toho důvodu také nemůžeme instalovat Nano Server z obyčejného média s Windows Server 2016 bez toho, aniž by na instalační soubor nebyly přidány námi vybrané role a drivery. Pokud bychom na Nano server chtěli přidat novou roli navíc, je lepší vytvořit nový instalační soubor s přidanou funkcionalitou a nabootovat server znovu.

Nano server můžeme využít pro služby DNS, jako File Server, Hyper-V, Failover Clustering, jako webový server, na kterém běží Internet Information Services (ISS), nebo jako hostitele pro vyvíjení aplikací, které jsou vyvíjeny přes cloudové prostředí a založeny na kontejnerech a micro-services. Naopak není možné, aby Nano server hostoval doménový řadič nebo byl připojen jako proxy server k přístupu do Internetu. Nejsou podporovány ani skupinové politiky, pro nastavení se používá DSC (Desired State Configuration). DCS konfigurační soubory jsou v podstatě šablony, jak má být server nakonfigurován, např. konfigurační soubor pro server, který hostuje roli DHCP.

3.3 Containers

Kontejnery nám umožňují vyvíjet své aplikace, které pak můžeme přes cloudový provoz nasadit kdekoli, kde to potřebujeme, s velmi malou provizí. V místní síti, v jiné doméně nebo kdekoli v cloudovém prostředí, popřípadě nasazení stejné aplikace u více zákazníků. Aplikace zde je konzistentní a lze ji lehce testovat, vydávat rychlé hotfixy nalezených chyb a spravovat jednotlivé verze. Aplikace uvnitř má všechny zdroje, které potřebuje a neví, jestli mimo kontejner probíhají jiné procesy nebo jsou spuštěny další kontejnery.

Přístup kontejnerů se již dlouho používá v sadě postupů a principů v metodologii DevOps, nyní je možnost vytvářet aplikace podobným způsobem i v prostředí WS2016. Kontejnery je snadné vytvořit (stačí pouze dva příkazy v PowerShellu s použitím Dockeru), ale je potřeba rozlišovat dva druhy kontejnerů, dle toho jakou budou plnit funkci a jaká míra izolace je potřeba – Windows Server Containers a Hyper-V Containers. Oba lze zprovoznit pomocí Docker API a následně je ovládat pomocí Docker příkazů (pro WS2016 je defaultní – `isolation process`, pro Windows 10 je defaultní – `isolation hyperv`). V praktické části práce bude funkcionalita Windows Containers spojených s Dockerem vyzkoušena a použita pro účely firmy zabývající se vývojem webových aplikací.

Kontejnery jsou kompatibilní s technologiemi jako .NET, ASP.NET, PowerShell a další. Jakmile je kontejner vytvořen, všechny změny (instalace softwaru nebo editace souborů v systému) jsou zachyceny v sandboxu. Následně je možné se rozhodnout, kdy ze sandboxu bude vytvořen image, který zdědí všechny změny, které byly provedeny. Lze tak vytvořit několik kontejnerů, jež se můžou rozvíjet odlišným směrem, zároveň ale stále používat zdroje svého hostitele. Závislosti mezi jednotlivými kontejnery jsou popsány v manifestu v souboru docker-compose.yml. Může se zdát, že se jedná o stejnou věc jako je známý virtuální stroj, liší se od sebe ale tím, že kontejner nemá vlastní kernel OS, protože využívá OS hostitele, na kterém je spuštěný. Při vytvoření virtuálního stroje je potřeba část RAM a dalších zdrojů, a přestože na dvou stejných virtuálních strojích jsou spuštěné odlišné aplikace, nemusí spotřebovat tolik zdrojů, kolik jim jich bylo přiřazeno.

Docker kontejnery jsou vyvíjeny lokálně, je k nim přiložen manifest, ve kterém je definováno, jaké mezi sebou mají images vazby, následně je odeslán kód aplikace společně s Docker manifestem na zálohovací místo, což může být například repozitář v Gitu.

Hostitel kontejneru používá virtuální adaptér (vNIC), kterým tak spojí kontejnery k vlastnímu virtuálnímu switchi (vSwitch). Každý kontejner má svou IP adresu, aby mohly být provolány služby, které poskytuje, a je připojen přes port (např. defaultní TCP nebo UDP port). Používá se několik druhů síťové komunikace:

- NAT – defaultní nastavení, kontejneru přidělena interní IP adresa, která je překládána na adresu hostitele, připojen k internímu vSwitchi
- Transparent – kontejneru přiděluje adresu DHCP, virtuální adaptér požaduje povolení MAC address spoofing, připojen k externímu vSwitchi
- L2 Bridge / L2 Tunnel – používá se v soukromých cloudových řešeních

Bezpečnostní hrozby týkající se kontejnerů je několik, jedná se o špatně nastavená privilegia nebo validace úložišť s images. Musíme brát v potaz, že i images mohou být nakaženy nebo poškozeny a po jejich spuštění je v ohrožení hostitel kontejneru. Pro bezpečnost je nezbytné monitorovat stav kontejnerů a jejich integritu v celém procesu od vývoje, přes uložení v DockerHub registrech, až po nasazení do produkce. Je potřeba zabezpečit samotné síťování mezi kontejnery, hostitelem a pracovními stanicemi. Ať už máme kontejnery nasazené v lokální síti anebo v cloudových prostředcích.

Kontejnery používají sdílené jádro a služby hostitele, což se může stát problematickým a každá drobná zranitelnost v jádru se stává důležitou. Na rozdíl od virtuálních strojů není jádro hostitele chráněno vrstvou hypervisora. Bezpečnější variantou se zdá spouštění kontejnerů v neprivilegovaném modu, namísto privilegovaného, ve kterém má kontejner povolen přístup ke všem zařízením a procesům hostitele, jako kdyby se jednalo o nativně spuštěný proces v jádru. Naopak je výhodou, že pokud je aplikace správně definována a rozdělena do mikro služeb (pozn. kontejnery lze ale využít i pro vývoj monolitických aplikací), sníží se tak celková plocha útoku. Pokud také útočník získá přístup k jednomu kontejneru, mělo by být zabráněno tomu, aby se dostal do ostatních kontejnerů nebo k samotnému hostiteli. Používá se k tomu tzv. orchestrátor, díky kterému řídíme vztahy mezi kontejnery,

jedná se o např. Kubernetes nebo Docker Swarm. Kontejnerům se také doporučuje přidělit určité množství alokovaných zdrojů. Náročný úkol, jak zabránit eskalaci privilegií, popřípadě vyřazení celého hostitele se všemi ostatními kontejnery.

Bezpečnost kontejnerů ve shrnutí závisí na třech hlavních pilířích – izolaci procesů prováděných uvnitř kontejneru uživatelem, oddělení těchto procesů od hostitelského jádra a síťových operací mezi kontejnery. Tyto hlavní komponenty popisuje i práce To Docker or not to Docker: a security perspective (Combe et al., 2016), zaměřující se hlavně na bezpečnost Dockeru a celý proces jeho použití. Jako řešení nabízí použití orchestrátora, který nabízí vyšší stupeň izolace kontejnerů tím, jak řídí procesy Dockeru. V další práci (Martin et al., 2018) jsou popsány obecné use-case pro Docker kontejnery, jejichž správným použitím se můžeme vyvarovat nebezpečí útoku. Hlavním problémem dle práce je, když jsou kontejnery používány pro stejné use-case jako virtuální stroje.

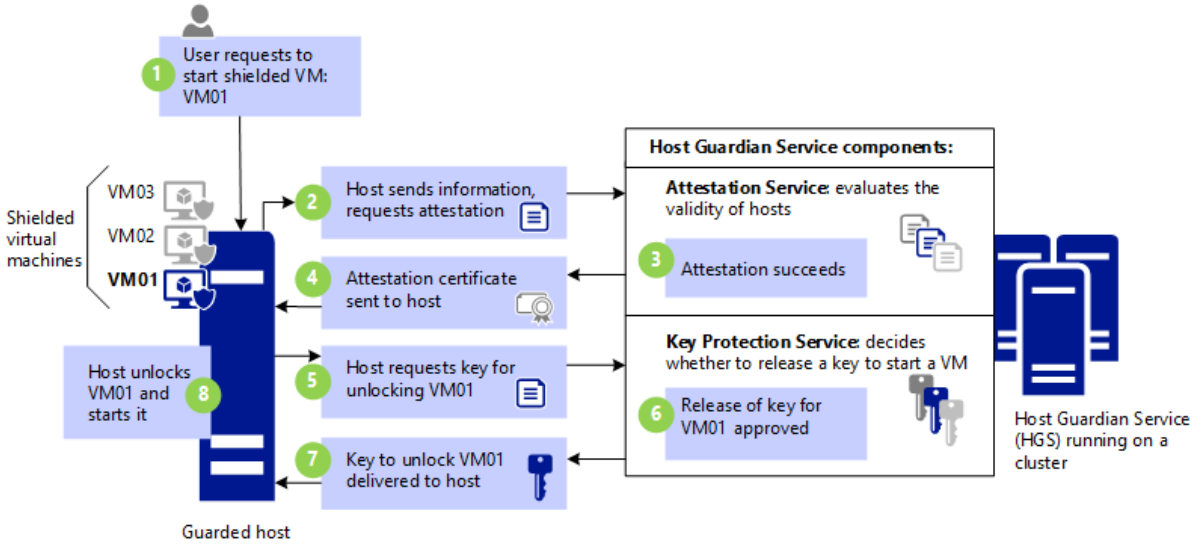
3.4 Shielded VMs

Ochrana virtuálních strojů (VM, virtual machine) poskytovaných přes Hyper-V je rozšířena o bootování z Unififed Extensible Firmware Interface (UEFI), oproti klasickému BIOSu, a poskytuje šifrování celého virtuálního stroje. Díky šifrování BitLocker můžeme disky virtuálního stroje zapouzdřit – jeho poslední stav, například kvůli migracím. Je potřeba pouze nainstalovat službu Host Guardian Service (HGS), která umí virtuální stroje rozšifrovat, protože vlastní správné klíče. HGS zná celou infrastrukturu a povolené přístupy k virtuálním strojům, pro tuto ochranu je ale potřeba mít virtuální stroje druhé generace (Generation 2 VM). V takovém prostředí se vyskytují pouze důvěryhodné strany a zašifrované virtuální stroje. HGS je nainstalované na WS2016 s rolí Hyper-V, je potřeba mít také aktivní VBS (Virtulization-Based Security) a TPM, až potom se z hostitele stane důvěryhodná identita (Guarded Host) k tomu, aby dešifroval a spouštěl virtuální stroje.

I když se kdokoli dostane k Virtual Hard Disku (VHD), zkopíruje virtuální prostřední na USB disk a pokusí se ho spustit přes Hyper-V, nedokáže se identifikovat, protože nevlastní klíč od HGS a nemůže se potvrdit jeho identita. Virtualizace zvyšuje pravděpodobnost útoků, protože lze k souboru VHD přistupovat i vzdáleně přes

souborový systém, odpadá fyzická bariéra, což byl důvod pro vývoj Shielded VM, do které se přes šifrování nedostanete ani přes PowerShell Direct. Přes Hyper-V manager můžeme pouze vidět, jestli je virtuální stroj spuštěný a má dostatečné zdroje, o vnitřních uspořádání stroje a jeho aplikací ale bez náležitých práv nevíme nic. Virtuální stroj je chráněný i při Live Migration.

Již roky se virtualizuje hardware, v případě šifrovaných virtuálních strojů vytváříme softwarovou verzi Trusted Platform Module (TPM), což je malý čip připájený do zařízení (např. notebooky, mobily nebo externí USB disky), který nám zajišťuje, že vždy víme, s kým komunikujeme.



Obr. 2: Shielded VMs
Zdroj: (Apolinario, 2016)

Na obrázku č. 2 vidíme, jak fungují Shielded VMs, kdy uživatel vyšle požadavek pro spuštění virtuálního stroje VM01 na Guarded Host, který zažádá o atestační služby u HGS. Pokud vše proběhne úspěšně, vyšle HGS na hostitele certifikát s povolením, aby dostal klíč k zašifrovanému stroji. Ten je následně s pomocí klíče rozšifrován a virtuální stroj VM01 se spustí.

Je třeba zajistit, aby dané virtualizované řešení, bez ohledu na to, jestli je uložené u poskytovatele cloudu nebo na vlastním hardwaru, vždy mělo integritu kódu a díky TPM získalo digitální podpis. V případě útoku na strukturu dat, změnu kódu jádra, se podpis poruší a systém se zachová dle toho, kde útok proběhl (je nahlášena podezřelá aktivita daným nástrojem pro monitoring, anebo se virtuální stroj vůbec nespustí).

3.5 Storage Spaces Direct, Storage Replica, QoS

Další metodou, jak zabezpečit data, je používat RAID (Redundant Array of Independent disks). RAID umožňuje spojit anebo proložit dohromady více pevných disků na několika levelech, či jejich kombinací. Kooperací tak dosáhne redundantně uložených dat na fyzicky oddělených discích. S jejich softwarovou verzí přišel i WS2012, WS2016 pojal Storage Spaces více distribuovaně. Zároveň ale nezapomíná i na HW vylepšení úložišť, kdy můžeme využívat výhod SATA SSD nebo NVM pro lepší výkon v ukládání dat, které se na sdílených discích dříve používat nedalo.

Díky Storage Spaces Direct je možné rychle vytvořit cluster ze serverů, mezi kterými probíhá komunikace SMB3 (Server Message Block version 3), z jednoho clusteru se doporučuje vytvořit jeden svazek (Storage Pool). Je třeba nastavit v pravidlech firewallu, aby provoz přes SMB3 povolil, pak můžeme používat všechny výhody této technologie, např. RDMA nebo multichannel. Nad celou SAN (Storage Area Network) je zapnutá služba, která diagnostikuje provoz a můžeme si vybrat, jestli pro replikaci dat mezi servery a clustery využijeme synchronní nebo asynchronní replikaci, což zajistí, že data jsou k dispozici kdykoli, i když přijdeme o několik částí z clusteru.

Storage Replica odesílá pakety zašifrované pomocí AES-128-GCM, kontroluje integritu a využívá Kerberos pro autentizaci mezi komunikací server-to-server nebo cluster-to-cluster. S řešením Windows Failover Cluster nám dovoluje vytvořit stretch cluster mezi dvěma lokalitami (sites) a oba uzly přitom zůstanou aktivní. Používá se bloková replikace a s několika bezpečnostními opatřeními zaručuje, že je Storage Replika „zero data loss“. Pokud se má jedno úložiště (datacentrum nebo cluster) vypnout, automaticky se klienti přesměrují na záložní variantu, záleží na use-case, které máme v našem řešení nakonfigurované. Pro jednu repliku může existovat i více scénářů, např. synchronní a asynchronní provoz, dle zatížení linky. Důležité je, aby primární a sekundární zdroj měli stejný objem a byly naformátovány NTFS nebo ReFS. Otestovat, jestli mají oba zdroje stejné komponenty a jsou kompatibilní, můžeme cdmletem `Test-SRTopology`, než přistoupíme k samotné konfiguraci přes `New-SRPartnership`. Storage Replica podporuje spojení s Nano serverem.

Storage Quality of Service (Storage QoS) dovoluje centrálně monitorovat výkon úložišť, alokovat zdroje a přidělovat práva pro výkon virtuálních strojů. Je to jedna z nainstalovatelných služeb zahrnutých v roli Hyper-V.

Storage QoS dává správci možnost zaručit, že úložiště jednoho VHD negativně neovlivní výkon jiného VHD spuštěného na stejném hostiteli. Docílí toho tím, že dává správci možnost specifikovat maxima a minima zatížení I/O, které se zadávají v IOPS hodnotách (Operations per second) pro každý virtuální disk na virtuálním stroji zvlášť (Panek, 2018).

3.6 ReFS, primary file system

Resilient File System (ReFS), nový souborový systém se začal vyvíjet už pro Windows 8 a WS2012 pro některé případy, v nichž se už nedalo spoléhat pouze na NTFS, který byl víc než dekádu let hlavním souborovým systémem pro OS Windows. Požadavky pro práci s větším objemem dat s nejnižšími náklady se stále navyšovaly, a tak byl ReFS vyvíjen s ohledem na spolehlivost, odolnost a kompatibilitu.

Výhodné spojení se Storage Spaces udělalo ve WS2016 ReFS jeho primární souborový systém. Zrychluje výkon Hyper-V a virtuálních strojů. Vylepšuje vysokorychlostní přesuny a nově přidává klonování bloků mezi soubory, jak uvádí oficiální dokumentace (Microsoft, 2018). Klonování bloků je tak účinné díky metadatům, není jako obvyklé čtení a zápis do souboru. Je tím povoleno více souborům sdílet stejný logický cluster, zatímco je blok dat namapován na fyzickou lokaci v clusteru. Klonování bloků má ale i své limity, blok nesmí přesáhnout velikost 4GB, maximální počet bloků mapovaných na stejný region je 8175, nebo že zdroj a cílová oblast se nesmí překrývat a musí být na stejném ReFS svazku. ReFS zrychluje práci s virtuálními stroji, pro příklad je zde technologie Sparse VDL – při vytváření nového virtuálního stroje (VHD disku) trvalo ve starším NTFS i několik minut, při použití ReFS jde o pouhé vteřiny.

Nad metadaty jsou prováděny kontrolní součty, které tak detekují nekonzistentnosti. Systém může sám detekovat problémy s integritou a následně je automaticky opravit z uložené kopie. Kontrola datové integrity samotných souborů ale snižuje výkon zápisů, proto se můžeme rozhodnout, kdy bude zapnutá, popřípadě ji zapnout pouze pro některé soubory či složky, které jsou důležitější. Jelikož ReFS ze své podstaty sám kontroluje integritu dat, již není potřeba používat příkaz chkdsk a při jeho spuštění je pouze oznámeno, že tento souborový systém není potřeba kontrolovat

tímto způsobem. Pokud se nekonzistentnost vyskytne, ReFS sám izoluje poškozená data a následně se je pokusí opravit.

Pro sledování nastavení datové integrity jednotlivých souborů, se používají cdmlety `Get-FileIntegrity` a pro povolení kontroly integrity `Set-FileIntegrity`. Abychom zjistili, jestli se integrita provádí nad soubory v dané složce, použijeme příkaz:

```
PS C:\> Get-Item -Path 'C:\Docs\*' | Get-FileIntegrity
```

Pro povolení kontroly můžeme použít příkaz přímo na celou složku:

```
PS C:\> Set-FileIntegrity C:\Docs -Enable $True
```

ReFS využívá B+ stromovou strukturu souborů, což je struktura, ve které se díky ukazatelům a klíčům snižuje počet IOPS k nalezení prvku ve stromu. Zvládne maximální objem dat 1 yottabyte, což se může zdát jako dostatečné, ale musíme brát v potaz, že oblast IT se vyvíjí velmi rychle.

Největší přínosy z jeho používání plynou ze spojení se Storage Spaces, i když tento souborový systém můžeme používat i nezávisle na Storage Spaces. Ve Storage Spaces Direct lze s ReFS pro zálohu dat použít mirror-accelerated parity, která vznikla z výhod ze dvou základních technik – mirroring a parity. Mirroring není tak výkonnostně složitý, zatímco parity šetří místo v paměti. ReFS provádí realtime rotaci mezi mirroring a paritou, zápisy jsou tedy rychlé a zároveň efektivně uložené na disku.

3.7 Bezpečnost a autentizace

Virtualizace a cloudová řešení jsou trend, a pro Docker kontejnery nebo přístupný Azure cloud jsou stále dodávána nová řešení, jak infrastrukturu zabezpečit. Po uvedení WS2016 na trh Microsoft zdůrazňoval prioritu bezpečnosti – jedná se hlavně o technologie o identifikaci a řízení přístupů. V podkapitole si popíšeme novinky v oblasti bezpečnosti, v praktické části práce prozkoumáme otázku bezpečnosti mnohem hlouběji a některé novinky budou implementovány.

Credential Guard

Dříve byl potřeba fyzický přístup do budovy, aby se odcizila data uzamčená na zařízení, nebo bylo nutné prolomit VPN. Nyní může každý používat své vlastní zařízení pro pracovní úkony, nebo dokonce veřejně přístupné zařízení (internetové kavárny, veřejné knihovny, atp.) a připojit se na dálku, mizí tedy fyzická bariéra budov nebo logická bariéra firewallu. Pověření pro volný pohyb v doméně může zůstat kdekoli nechráněn, stačí když se uživatel přestane hlídat. Pokud v síti máme zavedené SSO řešení, máme zde také cache paměti, ve které uchováváme informace o uživateli – Kerberos Granting tickety nebo uživatelská hesla v Local Security Authority Subsystem (lsass). Takové informace se mohou stát cílem útoků, po připojení k síti a využití penetračních nástrojů lze najít hashované informace o heslech. Takové útoky se nazývají Pass-the-Ticket a Pass-the-Hash.

Credential Guard je technologie vytvářející virtuální bezpečnostní vrstvu, která izoluje informace před neoprávněným přístupem. Používá k tomu protokol Kerberos, jehož principy jsou popsány v pozdější kapitole práce a NTML hashe. Vrstva Local Security Authority (LSA) je oddělená od zbytku operačního systému a nehostuje žádné další drivery zařízení, pouze nejdůležitější procesy pro zajištění bezpečnosti. Tyto procesy jsou podepsány certifikační autoritou, která je v systému důvěryhodná, nelze je tedy změnit a při každém přístupu souborů do LSA jsou certifikáty znovu validovány. Pro aktivaci Credentials Guard je třeba přestat používat NTLM autentizaci. Zároveň je ale důležité zjistit, jestli v síti nejsou používány aplikace, které by NTLM autentizaci vyžadovali – v takovém případě se mohou vyskytnout problémy s přihlašováním uživatele. Nejsou povoleny ani protokoly MS-CHAPv2 a NTLMv1, Digest a CredSSP, pro připojení Wi-fi a VPN je třeba přejít na autentizační protokoly používající certifikaci, jako jsou PEAP-TLS nebo EAP-TLS.

Pro nasazení je vyžadováno používání 64-bit OS Windows 10 Enterprise nebo WS2016, UEFI firmware v2.3.1 a verze vyšší, které podporují Secure Boot (funkcionalita bude popsána později), TPM 1.2 nebo 2.0, jež uchovávají šifrovací klíče, a podporu pro VBS. Nelze také používat Kerberos unconstrained delegation (tzn. neomezená delegace, u které nemůžeme kontrolovat jakým službám lze věřit) a šifrování DES.

Podporu pro RDP přenosy a přesměrování Kerberos ticketů využije Remote Credential Guard, ta je napojená na Single Sign On postupy, které se v obyčejném RDP využít nedají, SSO je popsáno v pozdější kapitole. Pro aktivaci Remote Credential Guard je požadováno, aby klient byl v doméně, která ho považuje za důvěryhodného, popřípadě s ní byl v trustu, a abychom využívali pouze autentizaci Kerberos. Protože pokud se klient nedokáže připojit k doménovému řadiči, komunikace selže a znovu se zkusí autentizovat přes NTLM – to ale kvůli ohrožení informací při přenosu není povoleno. Klient i hostitel musí mít minimálně Windows 10 verzi 1607 nebo WS2016. Hostiteli musíme navíc v registrech povolit Restricted Admin spojení (hodnota DisableRestrictedAdmin), nebo stejnou hodnotu nastavit přes Group Policy nebo Windows Defender.

Advanced Threat Analytics

Abychom vůbec rozpoznali, že se naše síť stala cílem kyber útoku, ve WS2016 je k dispozici platforma Advanced Threat Analytics (ATA), která sleduje síťový provoz, dokáže zachytit informace o protokolech, jež úzce souvisí s autentizací a autorizací – Kerberos, DNS, NTLM a další. Zná zranitelnosti protokolů a umí se učit dle vzorců (Machine Learning) identifikovat pochybné činnosti. Dle oficiální dokumentace Microsoft pro sběr informací ATA využívá metody:

- Port mirroring zapnutý (fyzické i virtuální switche) u doménových řadičů a DNS serverů a odesílání komunikace přes ATA Gateway
- Nasazení ATA Lightweight Gateway (LGW) přímo na doménový řadič

ATA dokáže detekovat útoky jako jsou Pass-the-Ticket, Pass-the-Hash, Forged PAC (MS14-068), Golden Ticket, Reconnaissance, Brute force nebo Remote execution.

Just in Time Administration

Mnoho uživatelů s adminskými právy, která jim byla přidělena už dávno, nakonec mohlo z firmy odejít, ale práva na nich zůstala a nebyla zrušena. V podstatě veškeré účty s vysokými právy vždy představují riziko. WS2016 nabízí přidělení administrátorských práv Just in Time Administration pouze po určitou dobu, ve kterou jsou taková práva potřeba. Můžete takové oprávnění dostat na 24 hodin (např. když si

objednáme servisní kontrolu člověka, který u nás dlouhodobě nepracuje) a po jejich vypršení oprávnění zase ztratíte, dostanete přesně jen tolik povolení, kolik jich ke své práci skutečně potřebujete, **Just Enough Administration**. Určitému uživateli specifikujeme, které cmdlety a funkce může spouštět. Lze přidělit pouze cdmlety, které souvisí s DNS, aniž bychom byli nuceni přidělovat vysoká práva doménového administrátora s přístupem k celému Active Directory.

Pro používání JEA jsou k dispozici od Microsoft předvyplněné skripty pro PowerShell, dostupné jsou pro verzi PowerShell 5.0 a vyšší. S pomocí skriptů se ovládají pravomoci pro účty a specifikují se role. Dle dokumentace Microsoft, jsou potencionálně nebezpečné příkazy například: `Add-ADGroupMember`, `Add-LocalGroupMember`, `net.exe`, `dsadd.exe`, protože by mohli povolit obcházení pravidel zavedených JEA, nebo také `Start-Process`, `New-Service`, `Invoke-Item`, `Invoke-CimMethod`, `Invoke-Command`, `New-ScheduledTask` a další, jež dovolují spouštět vlastní skripty s potencionálně škodlivým kódem.

Po správném zavedení JEA, se zabrání útokům, kdy útočník zjistí, kdo v určité firmě pracoval dříve a jestli má stále nějaká oprávnění. Někdy je jednoduché informaci o stále existujících právech zjistit, vyzkoušet napsat dotyčnému email a pokud se email odešle, je zde potencionální bod, kde začít s útokem. Rada vypůjčena z videa Microsoft Virtual Academy (Hynes a Ralston, 2016). S tím se mění také role dřívějšího superadmina, který měl kontrolu nad celým systémem a dohled nad doménami. Nyní lze zavést model používání více vrstev a schvalovacích postupů od několika lidí najednou – tedy není možné, aby se jeden člověk rozhodl, že převezme kompletní systém a vytvoří jakoukoli změnu, která se mu zachce.

Secure Boot

Útokům, které se snaží převzít kontrolu nad právě se spouštěným serverem (rootkits, bootkits nebo kernel-level malware), se snažíme předejít pomocí Secure Boot, což je funkce odhalující podezřelé chování, nedůvěryhodné části kódu a následně server nespustí. Funkce Secure Boot byla představena už ve Windows Server 2012 R2, ale dala se použít pouze u virtuálních strojů s OS Windows. Nyní je možnost použít funkcionalitu i na virtuální stroje, na kterých jsou i distribuce Linuxu.

Se Secure Boot je každý proces používaný při spouštění stroje digitálně podepsaný a validovaný proti změně. Kontrolu podpisů zajišťuje OEM firmware – při každém spouštění kontroluje EFI aplikace, UEFI firmware drivery a pak samotný operační systém. Po úspěšné validaci předá kontrolu nad strojem boot managerovi, který vyhledá umístění operačního systému a může ho nahrát. Aby byl boot manager důvěryhodný, i jeho podpis musí být přidaný do databáze UEFI. Na firmaware NV-RAM jsou dohromady tři databáze. Jedna uchovává hashe aplikací a driverů, které lze nahrát při bootování, druhá obsahuje ty, které nahrávat nechceme, a třetí databáze s klíči určenými k podepisování certifikátů v předchozích dvou databází.

Defaultně je pro WS2016 součástí antivirový nástroj Windows Defender, doplněný například o **Device Guard,** hlídající integritu kódu jádra pomocí vytváření politik, ty určují, který kód je důvěryhodný a může se vykonávat. Aby se politiky nedaly změnit, samy jsou ochráněny certifikáty, pro jejich změnu jsou potřeba administrátorská práva a zároveň také přístup k certifikátům, které firma vlastní.

Control Flow Guard – platforma, která má na starost sledování přidělování paměti pro jednotlivé aplikace a nezvyklé podezřelé chování aplikací (např. memory corruption attacks, které budou zmíněny i v kapitole č. 11) nebo zařízení nahlásí administrátorovi. Pro Windows Defender lze doinstalovat roli **Windows Server Antimalware**.

Dle (Hynes a Ralston, 2016) kontrolní a monitorovací nástroje rozpoznávají podezřelou aktivitu pomocí logiky poskytnuté z Azure. Není nutná konfigurace, protože nástroje sledují vzorce chování a aplikují je na určitý síťový provoz. Po rozpoznání naučených vzorců se znalosti použijí a vyhodnotí, jestli je systém v chybném stavu či se do něj cokoli instalovalo bez našeho vědomí.

Podrobnější informace lze nalézt v oficiální dokumentaci od Microsoft nebo v odborné knize MCSA Windows Server 2016 complete study guide (Panek, 2018).

4 Active Directory a vztahy důvěry

Než bude popsán problém forest trusts a domén, jejich vzájemné komunikaci v struktuře, v kapitole budou popsány nejhlavnější využívané pojmy.

Všechny objekty a elementy sítě, které můžeme spravovat, jsou uchovány v databázi – v adresáři. Jedná se o počítače, tiskárny, uživatelské účty, atp., ke všem objektům jsou přiřazena data, obrázky nebo certifikáty, různé zdroje pro ověření přístupových práv. Objektem může být cokoli, co může správce sítě sledovat a sdružovat do skupin, aby se v adresáři snáze orientovalo. Dodržuje se zde hierarchická stromová struktura. Nad tím vším funguje adresářová služba, která se stará o organizaci objektů, uskutečňuje přístupy k adresáři a kontroluje, kdo sem přistupuje a jaká jsou jeho privilegia. V Active Directory můžeme kombinovat několik protokolů (Kerberos, LDAP a CIFS), díky kterým komunikujeme se strukturou.

Adresářové služby nejsou určeny k prezentaci dat nebo přenosu souborů, není vhodné v nich provádět rozsáhlé transakce, jak je možné v relačních databázích. Data se zde příliš nemění a není zajištěna jejich referenční integrita. Proto je důležité brát ohledy nejen na současné potřeby firmy, ale i na rozšiřující se potřeby společnosti v budoucnosti, aby nevyhořeli na nedostatečné škálovatelnosti (scalability). K těmto účelům jsou navrhnuty protokoly a služby, které nám poslouží lépe pokud je v schéma dobře umístíme.

4.1 Doménová struktura

Strukturu pomáhají tvořit logické prvky – domény (domains), stromy (trees) a lesy (forests). Strukturu uvnitř domény tvoříme organizačními jednotkami (OU). Po přidání doménového řadiče (tvz. Domain Controller, zkráceně DC) se vytvoří doména a zároveň také začátek stromu a lesa. Stromy se vystavují na základu, kořenové doméně, kterou nazýváme root. První vytvořená doména v rámci lesa se stává rootem. Domény od sebe mohou dědit (např. vztahy důvěry, jmenné prostory). Jak již bylo zmíněno, jde o hierarchickou strukturu, na jejímž vrcholku je les. Je obvyklé, aby každá doména v sobě měla alespoň jeden doménový řadič zodpovědný za řízení domény.

Druhou částí struktury jsou fyzické prvky, které tvoří sites, což jsou v podstatě rozsahy adres, tedy subnety, a jsou voleny dle lokace sítě (lokací LAN). Objekty v AD jsou přesně dané dle pravidel schématu, to určuje, jaké druhy objektů uchováváme a jaké k nim náleží atributy. Díky sites jsou spojené doménové řadiče, což napomáhá např. replikaci dat. Používá se multimaster replikace mezi řadiči, což zajišťuje dostupnost dat, zároveň ale vyžaduje určité zatížení zdrojů.

Doménové řadiče obsahují globální katalog (Global Catalog), dle kterého můžeme hledat objekty z jiné domény, informace o uživatelích v rámci lesa a jejich členství v univerzálních skupinách (Universal Group Membership). GC ukazuje na všechny objekty v rámci lesa a využijeme ho, pokud hledáme objekt mimo vlastní doménu. Na doménovém řadiči je nainstalovaná role AD DS, nasazený LDAP a Kerberos.

Více o doménové struktuře bude popsáno v praktické části práce, kde bude zobrazeno na konkrétním příkladu LAN společně s implementací a problémy, na které lze narazit při nasazení AD.

4.2 Problém Forest Trust

Trust se v síti vytváří mezi doménami AD a mezi jednotlivými lesy. Úspěšné propojení dovoluje sdílet zdroje z domén, ke kterým uživatel, služba nebo počítač, nenáleží. Pro vytvoření trustu musíme dostat náležitá oprávnění nebo být ve skupině doménových administrátorů. Je důležité mít korektně nastavené DNS na obou stranách, které chceme spojit, hlavně zóny a podmíněný forwarding adres.

Trusty lze vnímat jako tranzitivní nebo intranzitivní. Všechny trusty uvnitř domény v rámci lesa jsou tranzitivní. Tranzitivní trust se přidává automaticky při přidání nové domény v rámci lesa, všechny domény si uvnitř tedy vzájemně věří a obousměrně (two-way trust, vysvětleno dále) mohou přistupovat ke svým sdíleným zdrojům, pokud neřekneme jinak (Soukup, 2009). Tranzitivní trust znamená, že pokud si dvě domény navzájem důvěřují, jejich vztah není omezen pouze na ně, ale důvěryhodnost lze rozšířit na třetí doménu.

Definujeme, jaký má trust směr: one-way (incoming and outgoing) nebo two-way direction trust. One-way direction trust je vztah první domény k druhé doméně,

kdy první doména může čerpat zdroje od druhé domény, ale ne naopak, druhá doména v tomto případě nemá oprávnění čerpat zdroje první domény.

Kromě zděděných trustů mezi doménami stejného stromu (Parent-child trust a Tree-root trust), existují, dle oficiální dokumentace Microsoft a článku Managing Active Directory trusts in Windows Server 2016 (Sharma, 2018), typy trustu:

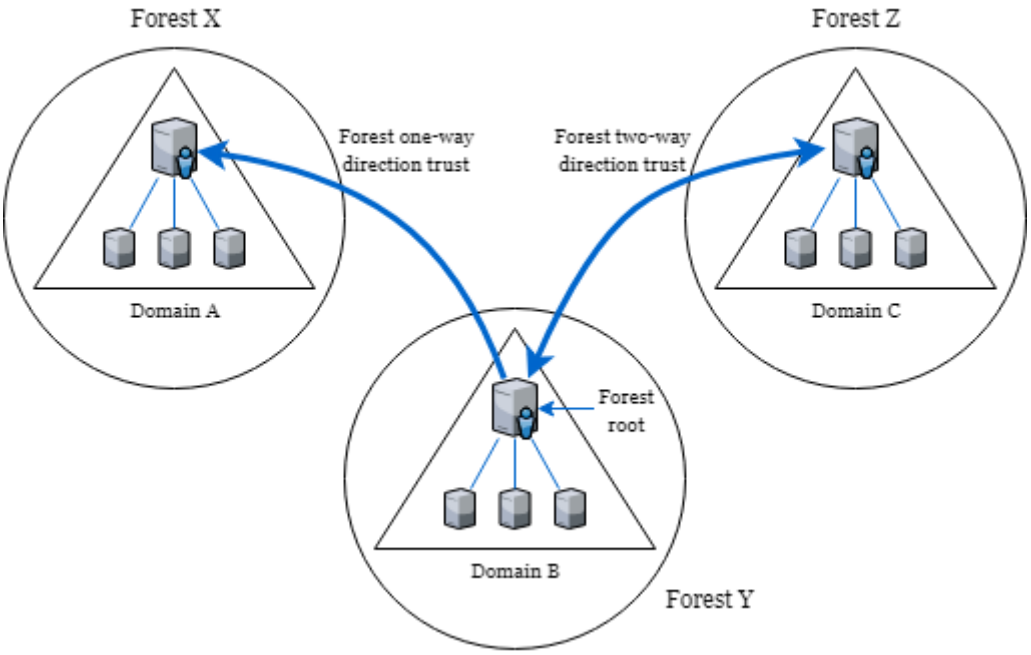
- **External trust**. Vytváříme ho vždy, když vyžadujeme zdroje, které pocházejí z domény v rozdílném lese. Může být one-way nebo two-way, ale vždy je intranzitivní.
- **Realm trust**. Vytváříme ho, pokud přistupujeme do domény, která má jiný systém než Windows Server (např. Unixové varianty systému), používá tedy i jiný adresářový systém, ale musí používat ověřování pomocí Kerberos. Může být tranzitivní nebo intranzitivní, spojen one-way nebo two-way direction.
- **Forest trust**. Tvoří se mezi celými lesy (všemi doménami). Můžeme použít one-way nebo two-way direction, ale spojení je vždy tranzitivní.
- **Shortcut trust**. Urychluje spojení mezi doménami stejného lesa pro případ, že potřebujeme opravdu rychlé přihlášení a sdílení zdrojů mezi doménami. Shortcut trust je vždy tranzitivní, může být spojen one-way nebo two-way direction.

I když vytvoříme trust mezi doménami, můžeme udělit výjimky, kdo ve vybrané důvěryhodné doméně nemůže komunikovat – tato omezení lze udělovat pouze v typu external a forest trust. Administrátor nastavuje trusty v nástroji AD Domains and Trusts.

Díky forest trust můžeme vytvořit two-way direction spojení mezi doménami v síti, data přenášená tímto spojením jsou autorizována protokolem Kerberos, a přitom zachovat flexibilitu administrace a izolovanost oprávnění v jednotlivých doménách. Lze využít v různých druzích prostředí, jedno provozní a druhé testovací, kde zkoušíme nová řešení předtím, než jsou připravena k nasazení v praxi.s

Předtím než vytvoříme trust, je potřeba zajistit, aby byl synchronizovaný systémový čas. Protože se identity root domény ověřují pomocí Kerberos, pro úspěšnou autentizaci je potřeba mít čas nastavený dle externího časového zdroje.

Pokud není čas synchronizovaný, trust se nevytvoří kvůli selhání autentizace (Olsen, 2008).



Obr. 3: Forest trusts
Zdroj: vlastní zpracování

Na obrázku č. 3 je příklad trustů mezi lesy X, Y a Z. Forest one-way direction trust mezi X a Y je intranzitivní, což znamená, že klienti v lese X můžou čerpat zdroje pouze z root domény v lese Y a z žádné další domény v rámci lesa Y. Druhé spojení na obrázku, forest two-way direction trust mezi Y a Z je tranzitivní, z toho vyplývá, že klienti v lese Y mohou čerpat zdroje z jakékoli domény v lese Z, zároveň klienti v lese Z mohou čerpat zdroje z jakékoli domény v lese Y. Klienti v lese X nemůžou čerpat zdroje z domén v lese Z, nevede k nim žádný trust, který by je spojoval.

5 Lightweight Directory Access Protocol

LDAP (Lightweight Directory Access Protocol) se vyvinul ze standardu X.500, kterému původně sloužil jako mezikrok v komunikaci, později byl zjednodušen a začal se používat jako samostatný adresářový protokol, seznam funkcí pro přístup do adresáře v prostředí TCP/IP. Nejčastější uplatnění protokolu je jako úložiště uživatelských nastavení a konfigurací aplikací, adresář kontaktů a zaznamenaná struktura organizace nebo autentizace uživatelů. Je to jeden z protokolů, který můžeme použít pro komunikaci v nasazených službách Active Directory. Protokol využívá

textový formát pro definici dat v adresáři, LDAP Data Interchange Format (LDIF). LDIF slouží k snadnému exportu a importu dat mezi dalšími servery. Kapitola čerpá informace z diplomové práce (Benák, 2004).

Se serverem se protokol dorozumívá pomocí zpráv, když klient vyšle požadavek o informaci v adresáři. Při komunikaci klient–server se používá několik typů příkazů.

- `Add`, `delete`, `modify`, `modify DN` – přidávání nebo úprava dat.
- `Search`, `compare` – vyhledání záznamů uložených v adresáři a porovnávání, jestli obsahují hledané atributy. Pro optimalizaci začíná vyhledávání z výchozího bodu hledání, který se určuje pomocí DN (vysvětleno níže v kapitole)
- `Bind`, `unbind`, `abandon` – tato volání jsou potřeba pro spojení a autentizaci, nebo jestli server ukončí spojení s klientem (a naopak), v případě operace abandon je to náhlé přerušení vyhledávání.

Každá zpráva, ať už žádost nebo odpověď, obsahuje návratový kód, vyžádaná data a identifikátor zprávy, ke kterému se váže daná odezva. Pokud by protokol nerozpoznal identifikátor zprávy, došlo by k odpojení klienta a zahození zprávy. Identifikátor zprávy je zde i kvůli pořadí. Jestliže vyšleme několik zpráv najednou, není zaručeno, že se vrátí v tom pořadí, jak jsme o ně žádali, proto nám server k přiložené odpovědi odesílá identifikátor zprávy. Pro zajištění celistvosti záznamu, jsou všechna data kódována jednoduchými pravidly, říkáme jim Lightweight Basic Encoding Rules (LBER). (Voglmaier, 2004, s. 17–20)

5.1 Modely LDAP

V relačních databázích máme navrhnuté schéma, kde udržujeme informace o struktuře databáze, vzory tabulek a sloupců v nich. I v protokolu LDAP jsou definované elementy, jejichž podobu následně musíme dodržovat – schéma LDAP obsahuje 4 typy modelů. Bezpečnostní, informační, jmenný a funkční model

Bezpečnostní model

Jak bylo zmíněno, data sice nejsou v čisté textové podobě jako např. u HTTP a nemůžeme je číst díky Telnetu, ale kódování LBER není žádný bezpečnostní problém

pro analyzátory síťového provozu. Proto se bezpečnost komunikace zajišťuje pomocí autentizace a přidělení přístupových práv. Proti odposlechu slouží SSL/TLS, chrání spojení proti odposlechu, hlavně pokud se spojení mezi serverem a klientem neotevírá uvnitř LAN, která může být odstíněna od nedůvěryhodného Internetu např. firewallem. Defaultně LDAP používá pro komunikaci port 389 v komunikaci TCP a UDP, LDAPS chráněný SSL používá port 636.

Autentizaci můžeme provádět různými způsoby, dle práce (Perutka, 2014) většinou volíme možnosti:

- Anonymní autentizace – při navázání spojení (`bind` operace) nejsou odesílány žádné identifikační údaje o uživateli nebo o jeho přístupových právech
- Jednoduchá autentizace – při spojení se po nechráněném kanále odesílá DN a heslo uživatele. Heslo by mělo být na straně serveru zašifrováno nebo hashované.
- Jednoduchá autentizace přes zabezpečený kanál – heslo a DN uživatele se odesílá po kanále, který je chráněný TLS/SSL.
- Proxy autentizace – je utvořen uživatel, který má možnost nahlížet na hesla ostatních uživatelů, může zjistit, jestli uživatel, který chce navázat spojení zná své heslo a jméno a má daná přístupová práva. Ověřovací uživatel pak pomocí operace `compare` autentizuje uživatele.
- Simple Authentication and Security Layer (SASL) – umožňuje využít přídavné moduly nebo příslušné protokoly, které zajišťují autentizaci uživatele.

Informační model

V informačním modelu definujeme, jaké datové typy můžeme v adresáři uchovávat. Popisuje organizační strukturu a atributy objektů. Adresář má záznamy uložené ve stromové struktuře, která zajišťuje přehlednost. Říkáme jí Directory Imformation Tree (DIT). Záznamům (entry) v adresářovým službám se vážou k objektům, ty mají vždy typ a snaží se popsat reálný objekt pomocí atributů. Objekty řadíme do tříd objektů (objectClass), např. user, OU, domain, group, většinou jsou

odvozeny z nadřazených tříd a dědí od nich. Atributy dodržují syntaxi a pravidla shody (matching rules). Objektová třída má nepovinné atributy a povinné atributy, bez kterých není možné záznam do adresáře uložit. Kontroluje se i datový typ vzkládaného záznamu, pokud souhlasí s datovým typem atributu (např. string, integer nebo boolean).

Jmenný model

DIT je složený z listů, což jsou záznamy, které už nemají žádné další potomky a říkáme jim leaf object, a uzlů, které v sobě obsahují další objekty a říkáme jim container object. Je důležité, abychom ke všem záznamům měli zaznamenanou cestu. K tomu jsou navrženy jmenné prostory ve jmenném modelu, určují způsob, jak se přistupuje k datům. Příkladem je (`uid=876543, ou=hradec, ou=zamestnanci, dc=example, dc=cz`). Na prvním místě je object identifier, unikátní pro celý strom, ukazující na pracovníka ve firmě, kořen je uveden až na konci.

Můžeme čerpat několik výhod při správném navržení struktury stromu. Přiřazovat práva určitému managerovi pro jedno město, ve kterém je pobočka, kterou manager spravuje, stejně tak se efektivněji vytvoří záloha dat, pokud chceme zálohovat pouze jednu pobočku. Potom je velmi snadné najít jedinečný záznam, což umožňuje i rozlišovací název (Distinguished Name, DN) a relativní rozlišovací název (Relative Distinguished Name, RDN). RDN se nachází v rámci uzlu a musí být jedinečné i na úrovni stromu, nejen v daném kontejneru. Úplná cesta DN se pak skládá z jednotlivých RDN z každého uzlu.

Funkční model

V LDAP používáme 3 kategorie s příkazy, které definují, jak zacházet s informacemi v modelu. Jedná se o autentizaci (`bind`, `unbind`, `abadon`), dotazování (`search`, `compare`) a aktualizační operace (`add`, `delete`, `modify`, `modify DN`). Operace jsou stručně popsány na začátku této kapitoly.

6 Single Sign-on

Ve firemní sféře, kde se používá i nepříliš složitý informační systém v podnikové síti, se za den provedou stovky příkazů a požadavků, které musí dojít až ke správnému serveru, jež může požadavky vyřídit. Pro příklad to můžou být dotazy do databáze, které můžeme mazat nebo modifikovat, jde o příkazy pro aplikaci běžící na jiném počítači než klientském, nebo čtení zpráv v poštovním klientovi. Je potřeba vynaložit úsilí pro nejoptimálnější rozložení podnikové sítě nebo se může stát, že přijdeme o drahý čas, který by pracovník mohl využít lépe.

Jedna z věcí pomáhající zrychlit procesy práce, které se za den několikrát opakují, je přístup Single Sign-on. Někdy se překládá jako jednotné přihlášení nebo se používá zkratka SSO. Firmě jde o maximalizaci efektivity pracovníka, rychlost práce a zároveň o bezpečnost. V posledně době se rozmáhá trend aplikací založených na cloudovém systému SaaS (Software as a Service), z toho důvodu se uživateli může nahromadit několik rozmanitých uživatelských jmen a hesel. Tato hesla je potřeba měnit, jsou dlouhá a složitá a pro uživatele je složité uchovávat je všechna v paměti. Později si začne hesla zaznamenávat v počítači, popřípadě na papír a zde nastává velká možnost lidské chyby. Vygenerování náhodného hesla bez srozumitelných slov a číselných řad je příliš náročné, obzvlášť když je zavedeno pravidlo, že se heslo musí generovat každý měsíc nové. Při zadávání hesla je ještě možnost doplnit přihlašování pomocí čipových karet nebo klíčů a certifikátů unikátní pro určitého uživatele. I když je zde stále možnost odcizení dodatečného zařízení, je to jedna z cest pro zvýšení bezpečnosti. SSO snižuje nároky na uživatele a je zároveň v rovnováze s vyžadovanou bezpečností. Například ve firmách s rozsáhlými ERP (Enterprise resource planning) systémy je SSO téměř nutností.

Realizaci SSO můžeme provést několika způsoby, jediným požadavkem, jak napovídá překlad termínu, ale zůstává pouze redukce všech uživatelských účtů napříč aplikacemi na jeden. Bezpečnost komunikace je zajištěna šifrovaným přenosem lístků mezi komplexně spravovanými účty. Stále je ale velice doporučované, aby jednotné heslo bylo silné, nejlépe pod správou password policies, nesnadno prolomitelné např. brute force útoky.

Dle diplomové práce o protokolu Kerberos (Nečas, 2009, kap. 2.4) se autor řídí třemi hlavními koncepty, jak SSO lze implementovat, tyto koncepty odvodil od architektury příslušných implementací a následně dodává jejich praktické příklady.

V této práci popíšeme hlavně způsob, jakým SSO implementuje Microsoft v doménovém prostředí, a jak pracuje s protokolem Kerberos.

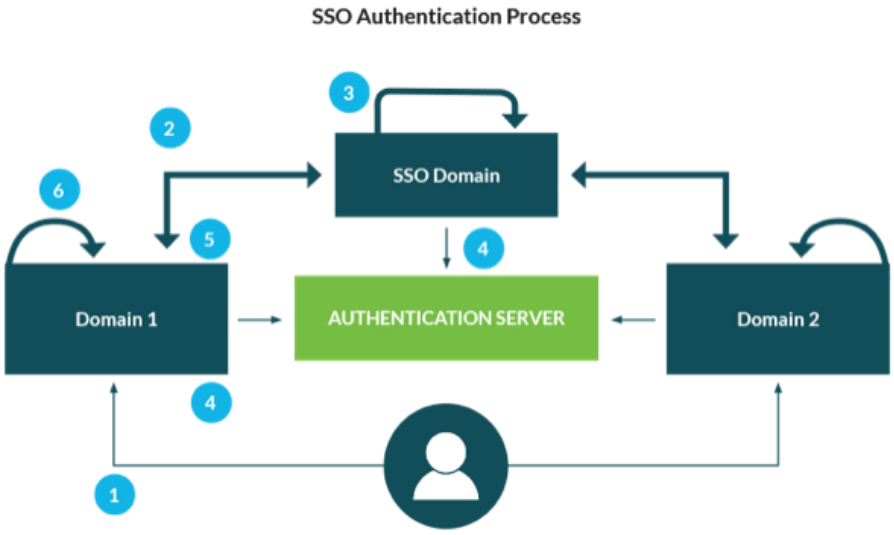
6.1 Princip autentizace třetí osobou

Přihlašovací informace se verifikují na centrálním místě a ke službě požadované od uživatele se vůbec nedostanou, služba dostane pouze důvěryhodný příkaz. Čímž se dostáváme také k velké nevýhodě SSO, protože když je napaden centrální prvek, útočník se může dostat k několika službám. Zároveň při výpadku centrálního prvku s identitami se nikdo nikam nepřihlásí, je potřeba mít data zálohovaná a ihned dostupná z duplikovaného serveru.

Autentizaci provádí Key Distribution Center (KDC) běžící na doménových řadičích (DC), služba, která je popsána v kapitole o Active Directory. Pro využití SSO musí mít klient přístup k DC, zde můžeme nastavit i důvěryhodnost oproti dalším doménám, kdybychom chtěli posílat požadavky i do vzdálenějších částí sítě, popřípadě do Internetu. Tyto zprávy jsou posílány šifrovaně a pomocí tiketů. Po přihlášení na službu se provede autentizace díky SSO, následně i autorizace. Jestliže autorizace selže, protože s daným účtem nemáme dostatečná práva, může být služba nastavena tak, že se zobrazí nové přihlášení, ve kterém se přihlásíme pod jiným účtem. Kvůli tomu je potřeba, aby u každé služby byl přidán aplikační modul nebo byla služba nakonfigurována pro správné použití SSO.

Řešení SSO lze nastavit několika způsoby, musíme brát v potaz strukturu domén, komunikaci v rámci jednoho lesa, ale také mezi doménami v odlišných lesech.

Tlakem na bezpečnost je také princip BYOD (Bring Your Own Device). Někdy je potřeba, aby pracovník mohl pracovat odkudkoli a použil k tomu své zařízení, které samozřejmě není pod kontrolou firemního IT oddělení, k tomu lze nastavit síťovou komunikaci v rámci VPN nebo standard Security Assertion Markup Language. Zaštítit přístupy zvenčí nám pomáhá i služba Active Directory Federation Services a Device Registration Service.



Obr. 4: Princip přihlašování přes SSO
Zdroj: (Killoran, 2017)

Na obrázku č. 4 vidíme stručný princip SSO. Uživatel vybere svůj cíl, doménu, kam se chce přihlásit. Doména přesměruje uživatele na centrální doménu SSO, kde uživatel zadá své přihlašovací údaje, které centrální doména vyhodnotí. Při úspěchu je uživatel přesměrován zpátky na cílovou doménu a obdrží token zaručující jeho autenticitu. Token se pak používá pokaždé, když uživatel znovu žádá o vstup do dalších domén zařazených do známé infrastruktury.

7 Kerberos Single Sign-on

Kerberos je autentizační protokol splňující jednoduchost a bezpečnost zároveň. Je to již dlouho používaný protokol nejen ve Windows, tato práce ale bude vycházet hlavně z principu, jak je Kerberos využívaný na platformách od Microsoft a jeho doménovém prostředí. Poslední verze Kerberos v5 je specifikována v RFC 4120.

7.1 Náležitosti Kerberos SSO

Jak bylo již zmíněno v dřívější kapitole, v této metodě ověřování se autentizační údaje (heslo nebo jeho hash) vůbec nepřenáší přes sít, vše funguje díky šifrovaným tiketům, nebo také lístkům. Neslouží k autentizaci pouze klienta, autentizovat můžeme

i samotnou službu. Využívá časové známky, proto je důležitá synchronizace času v doménovém prostředí a stran, které se ověřují.

Ke komunikaci používáme třetí stranu, Key Distribution Center (KDC). KDC je server, který obstarává dvě hlavní služby – Authentication Service (AS) a Ticket-Granting Service (TGS). Úkolem serveru je tedy správná autentizace uživatele a odesílání tiketů na požadovanou službu. Jelikož je KDC součástí každého doménového řadiče, má přístup k informacím o účtech a heslech. K samotným informacím tedy klient nemá přímý přístup, veškerá komunikace prochází přes KDC.

Používá se symetrické šifrování, což znamená, že k šifrování i dešifrování dat je použit pouze jeden veřejný klíč. Ve zkratce, plaintext je danou technikou zašifrován, získáme tak ciphertext. Pomocí klíče dešifrujeme zpátky původní text.

Aby se mohl uživatel nebo služba identifikovat, je třeba na něj správně odkazovat. K tomu se používá PN (Principal Name). Skládá se ze jména domény, ze které uživatel nebo služba pochází, a přihlašovacího jména, tyto dvě části jsou spojené znakem @. Každé PN má svůj specifický klíč – hashované heslo, které je definováno jako long-term klíč (pomocí různých technik se nemůže stát, že by uživatelé se stejným heslem měli stejné klíče).

7.2 Průběh autentizace pomocí Kerberos

- Komunikace probíhá mezi třemi stranami – uživatel (klient), KDC a server s nainstalovanou službou – začíná se přihlášením uživatele na svou pracovní stanici.
- Vyšle se zašifrovaný požadavek s autentizací ke KDC serveru, který díky sdílenému klíči patřícímu určitému uživateli (Secret key) rozšifruje požadavek s paketem. Pokud je tento krok úspěšný, požadavek je přijat, přidělí se mu TGT (Ticket Granting Ticket). TGT je časově omezen, ale dá se prodlužovat, je uložen v cache počítače. V podstatě se využívá k identifikaci uživatele.
- Jestliže chce uživatel využít službu v síti, využije se princip SSO. Požadavek prochází přes server se službou Ticket Granting Service (TGS), ve Windows je tato služba součástí na každém doménovém řadiči,

kde se kontroluje, jestli daný uživatel má ke službě povolený přístup a pokud ano, může mu být udělen Service Ticket. Service Ticket je zašifrovaný pomocí Secret Key samotné služby a slouží k identifikaci uživatele u služby. Service Ticket může být bezpečně odeslán ke klientovi, protože on samotný ho neumí rozšifrovat, pouze ho poslat dál.

- Service Ticket je spolu s daty odeslán klientem na aplikační server pomocí komunikačního protokolu. Service ticket je požadovanou službou rozšifrován a zjistí se identita uživatele, následně je spuštěna požadovaná akce povolena uživateli. Pro dokončení může být požadována Mutual Authentication, od aplikačního serveru tedy odejde ještě informace o tom, která služba byla povolena. Kvůli bezpečnosti je v této odpovědi přiložena časová známka, která je porovnána na straně klienta.

Autentizace Kerberos bude použita v praktické části práce. Bude potřeba zajistit, aby v testovací LAN byly implementované služby AD DS, DNS a PN, správná časová synchronizace.

8 Firewall

Nejde pouze o programové a technické provedení, firewall je jádrem dobře definovaných zásad bezpečnostní politiky. Na rozdíl od protokolů chrání síť před útoky zvenčí. Nutí veškerý síťový provoz procházet přes sebe a díky předdefinovaným pravidlům určuje, které pakety jsou podezřelé a které může poslat dál. Díky základním pravidlům můžou být nová pravidla určována i dynamicky (Khoumsi et al., 2018).

Firewallem může být router nebo počítač s vhodným OS a alespoň dvěma síťovými kartami. Může jít o hardware nebo software zařízení. Před jeho umístěním je potřeba zvážit naše možnost a co přesně chceme chránit. Špatné umístění prvku může zapříčinit přijmutí nebezpečných paketů a odmítnutí těch potřebných. Firewall rozdělujeme do dvou hlavních skupin dle jeho chování – paketové filtry a aplikační brány.

Paketové filtry se starají pouze o vyhodnocování, jestli je daný paket vhodný přijmout nebo zahodit, což určuje podle hlavičky paketu a důvěryhodnost odesilatele. Jsou rychlé, protože nedokážou vyhodnotit samotný obsah paketu.

Aplikační brány fungují na aplikační vrstvě, někdy se jim říká Proxy brány. Pokud chceme vyslat požadavek do veřejného Internetu, projde přes aplikační bránu (přebírá roli pomyslného zprostředkovatele nebo směrovače), která otevírá samostatný požadavek, aby se skryly zdroje, ze kterého pakety pocházejí. Zároveň ale zkontroluje obsah a podle něj se rozhoduje.

9 PowerShell

PowerShell se poprvé objevil už ve Windows Server 2008 a Windows 7. Jedná se o objektově orientovaný skriptovací jazyk od Microsoft, založený na platformě .NET Framework, ze které čerpá několik výhodných prostředků. Používá se k ovládání výpočetních systémů přes zadávání příkazů do příkazové řádky, do klasické textové konzole, neboli shell. Microsoft je známý svými operačními systémy s přívětivým uživatelským prostředím, přes které se dá nastavit téměř celý systém bez hlubších znalostí programování.

A přestože jako u shellů v Unixových systémech má PowerShell své příkazy pro nápovědu k jednotlivým příkazům (např. `Get-Help Name-of-cmdlet -Detailed`), v poslední verzi WS2016 je aspoň základní znalost skriptovacího jazyka pro administrátora nezbytná. Na druhou stranu dokáže dobře vytvořený skript automatizovat různé operace a zjednodušit tak správu systému.

9.1 Cdmlety, aliasy a roury

Cdmlet (neboli command-let) je příkaz vykonávající určitou službu. Skládá se ze slovesa a podstatného jména, což usnadňuje zapamatování si příkazů a jejich snadné pochopení. Syntaxe příkazů není složitá, ty nejužívanější jsou vypsány v seznamu:

- `Get-Location`, `Set-Location` – zobrazí aktuální adresář, nastaví zvolený adresář
- `Get-Process`, `Stop-Process`, `Get-Service`, `Stop-Service` – základní práce s procesy a službami
- `Select-String` – vyhledává textovou shodu v souborech nebo ve výstupech
- `Copy-Item`, `Remove-Item`, `Move-Item`, `Rename-Item`, `New-Item` – základní operace se soubory

Pomocí `Get` se tážeme a dostáváme odpověď, `Set` nastavuje a mění parametry. Pro představu cdmlet `Set-Location` má PowerShell alias jako `sl`, `cd` nebo `chdir`, v klasické příkazové řádce cmd.exe bychom stejný příkaz zapsali jako `cd`, a pro porovnání v Unixových nebo Linux systémech měníme aktuální pozici pomocí `chdir`. Aliasy můžeme i sami vytvářet (`Set-Alias`), abychom svou práci co nejvíce zefektivnili. Výstupy můžeme přesměrovávat nebo zřetězovat, popřípadě před spuštěním funkce pouze otestovat, co nastane po spuštění. Vždy se díky historii příkazů lze podívat na poslední zadané a znovu je použít.

Z jednoduchých celků skládáme spustitelné funkce, které mohou mít vstupní parametry a návratovou hodnotu. Skripty a funkce lze psát v obyčejném poznámkovém bloku nebo Notepadu, ale ve Windows je také zabudováno rozhraní PowerShell ISE (Integrated Scripting Environment), kde přehledně vidíme soubory .ps1 (soubory se skriptem) a v pravé části i seznam všech dostupných příkazů, prostředí umí i barevně vyznačit psanou syntaxi. Následovníkem PowerShell je Windows PowerShell Core, který má obrovskou výhodu v tom, že skripty, které napíšeme, budou fungovat i na dalších podporovaných operačních systémech (distribuce Linuxu nebo MacOS).

Jeden z nejdůležitějších konceptů, které se používají, jsou roury (pipelines). Ty se vytvoří, pokud spojíme dva příkazy pomocí „|“, výstup z první části příkazu se použije jako vstup do části druhé. Jelikož je vše v PowerShellu bráno jako objekt, přes roury lze posílat objekty mezi dvěma či více programy. V kapitole o rourách a aliasech bylo čerpáno z oficiální dokumentace k PowerShell (Microsoft, 2018).

9.2 Služby PowerShell

S verzí PowerShell 2.0 přišla i možnost spravovat adresářové služby Active Directory. Díky tomu můžeme na serveru spravovat uživatelské účty, manipulovat s objekty a s přístupovými politikami. Instalovat programy na několik strojů najednou a další zjednodušení rutinních procesů. Je to jedna z možností, jak ovládat Windows Server Core, kde nemáme k dispozici obvyklé GUI. V nejnovější verzi WS2016 už používáme verzi PowerShell 5.1, kde byly přidány nové cdmlety pro DNS, Hyper-V, administraci IIS nebo Windows Defenderu.

Příkladem zajímavé služby je PowerShell Direct, kterým se skrze VMBus lze spojit s virtuálním strojem, aniž bychom byli závislí na síťovém spojení nebo nám v přístupu bránil firewall. VMBus existuje mezi každým hostitelem a virtuálním strojem, PowerShell direct vytvoří session, přes kterou nastavíme potřebné konfigurace. Na hostiteli virtuálního stroje přihlášení jako administrátor použijeme `Enter-PSSession -VM1 <VM1>`, přihlásíme se a můžeme vkládat další cdmlety nebo skripty, instalovat nové role a features nebo měnit Group policies.

Přes Desired State Configuration (DSC) lze konfigurovat síťovou infrastrukturu nejen s Windows Servery, ale také servery s OS Linux, pokud je v LAN používáme.

Jak bylo zmíněno, následovník PowerShell Core by mohl být náhradou za PowerShell 5.1 kvůli jeho všestrannosti. Můžeme tak předpokládat i podle možnosti update, kdy do PowerShell lze vložit update už jen kritických chyb, na rozdíl od PowerShell Core, který přebral veškerou podporu a opravy chyb, jak píše ve svém článku (Brinkmann, 2018).

10 Základní popis síťových prvků a protokolů

V této kapitole autor stručně popíše základní principy fungování sítí a seznámí s hlavními pojmy, následně přejde k popisu komunikačních protokolů a způsobů, jak napadnout systém přes nesprávně nastavené protokoly.

Přenos dat v lokální počítačové síti (Local Area Network, LAN) probíhá přes několik protokolů a nakonfigurovaných pravidel zajišťující jinou část přenosu. Když

mluvíme o LAN, jedná se o skupinu dvou a více propojených počítačů, jejíž součásti mohou být i další zařízení jako tiskárny a periferní zařízení.

Aby se komunikace mezi různými výrobci standardizovala a byla kompatibilní, vyvinul se referenční model ISO/OSI. Skládá se ze 7 vrstev, které zodpovídají za své úkoly, ať už jde o vzájemnou identifikaci uživatelů nebo kontrolu formátu přenášených dat a detekci chyb.

Druhá skupina protokolů vycházející z modelu ISO/OSI, je zkrácená na čtyři vrstvy a slouží pro sjednocení internetové komunikace – TCP/IP (Transmission Control Protocol/Internet Protokol). Popis jednotlivých vrstev není předmětem této práce, zaměříme se hlavně na jednotlivé protokoly pracující, které v pozdější části práce budeme moci pozorovat.

Ve shrnutí je model OSI jen koncepčním modelem, popis a pochopení vrstev, jeho funkcí, oproti tomu TCP/IP je navržen tak, aby řešil specifickou řadu problémů celé sady protokolů pracujících na různých vrstvách v internetu. Bezpečnost procházení vrstev se většinou řeší až na aplikační vrstvě. Výpis vrstev v obou modelech je naznačen v tabulce č. 1, jsou zde zařazené i jednotlivé protokoly.

<table>
<tr><th>OSI model</th><th>TCP/IP model</th><th>Protokoly a služby</th></tr>
<tr><td>7. Aplikační</td><td rowspan="3">Aplikační vrstva</td><td rowspan="3">HTTP, FTTP, Telnet, NTP, SMB, DHCP, DNS, SMTP nebo FTP</td></tr>
<tr><td>6. Prezentační</td></tr>
<tr><td>5. Relační</td></tr>
<tr><td>4. Transportní</td><td>Transportní vrstva</td><td>TCP, UDP</td></tr>
<tr><td>3. Síťová</td><td>Síťová vrstva</td><td>IP, ICMP, IGMP nebo ARP</td></tr>
<tr><td>2. Linková</td><td rowspan="2">Vrstva síťového rozhraní</td><td rowspan="2">Ethernet, Token ring nebo jiné typy protokolů</td></tr>
<tr><td>1. Fyzická</td></tr>
</table>

Tab. 1: Modely a síťové protokoly
Zdroj: vlastní zpracování

10.1 Napadnutelné protokoly

Protokoly přenáší pakety napříč internetem, základní internetový protokol (IP) se stará o to, aby každý paket přišel k tomu správnému počítači nebo routeru. Dříve se

používala 32bitová tečková notace, po vyčerpání všech adres se přešlo na 128bitové IPv6 adresy. Nyní si popíšeme nejčastěji využívané chyby v protokolech z rodiny TCP/IP, jejich nevýhody a potencionální hrozby.

Transportní vrstva

TCP (Transmission Control Protocol) na transportní vrstvě je spojový a spolehlivý protokol, vykonávající detekci chyb v data paketech, což více zatěžuje linky a zpomaluje přenos. Nespolehlivá verze TCP je UDP (User Datagram Protocol), znamená to ale pouze to, že se využívá pro jiná spojení, kde je důležitější rychlý přenos než správnost odesílaných dat, a kde si již sama aplikace zkontroluje přijatá data. Oba protokoly využívají zdrojový a cílový port a spojují se pomocí three-way handshake.

Three-way handshake pro navázání spojení je jeden z článků, který lze napadnout. Útočník odesílá počátky spojení (SYN flood attack) na každý port s falešnou IP adresou, takových spojení je tolik v krátkém časovém úseku, že je server nedokáže zpracovávat a spojení nechává neuzavřená. Jakmile tabulky pro spojení přetečou, server už další požadavky prostě nepřijme a selže. Je to jeden z Distributed Denial of Service (DDoS) útoků, ty zatěžují cíl požadavky s účelem snížit dostupnost služby. Proto je důležité, aby všechny porty, které zrovna nevyužíváme, byly uzavřeny. Rozšířené možnosti odposlechů sítě nabízí spousta nástrojů a aplikací (např. port sniffery), které se zaměří na jednotlivé porty nebo IP adresy a vyčkávají. Na druhou stranu je ale možné využít takové aplikace i pro svůj prospěch, monitorovat vlastní síťový provoz a hledat napadnutelné nedostatky předtím, než je objeví útočník.

Se správnými aplikacemi používající procházející algoritmy, je pro útočníka možné odposlouchávat a sledovat odesílané sekvence čísel, které TCP odesílá. Po uhodnutí sekvence není pro útočníka těžké vložit svou vlastní a provádět změny (např. přidání účtu nového uživatele nebo vložení škodlivého kódu). Bránit se takovému útoku (tzv. Blind Spoofing) lze náhodným vygenerováním počáteční sekvence, tím se pravděpodobnost odhalení sekvence snižuje. Podobné útoky odposlouchávání nazýváme „Man In the Middle“, kdy útočník vstupuje mezi dvě důvěryhodné strany a maskuje se jako někdo s věrohodnou IP adresou, ať už softwarově nebo s fyzickým přístupem k datové kabeláži.

Zvláštním případem je protokol SSL (Secure Socket Layer), který je mezi vrstvou transportní a aplikační. Jak napovídá jeho název, zabezpečuje autentizaci dvou komunikujících stran pomocí asymetrického šifrování a volitelně i autentizaci certifikátem. Pro příklad ho využíváme ve verzi protokolu HTTPS, aby komunikaci neodposlouchávala třetí strana. SSL je předchůdcem TLS (Transport Layer Security), pro správně navázanou komunikaci s certifikáty je třeba, aby komunikující měli kompatibilní verze – hrozba Poodle Attack.

Síťová vrstva

V předchozí kapitole bylo zmíněno zahlcení služeb serveru útokem DDoS. Z podobného důvodu je lepší blokovat protokol ICMP (Internet Control Message Protocol), díky kterému se útočník může dozvědět o aktivních hostech v síti v horších případech obejít i firewall (CVE Details, cit. 2019-2-23). Dle článku Independent Security Evaluators (Branch, 2016) blokují pouze části ICMP protokolu a zajišťuje tak lepší bezpečnost než při úplném zablokování, což se zdá jako přijatelné řešení problému.

Aplikační vrstva

HTTP (Hypertext Transfer Protocol) zajišťuje komunikaci mezi WWW servery a klienty, zde prohlížeče, kteří odesílají požadavky pro konkrétní webové stránky. Není zde možnost autentizace uživatele ani šifrování, proto se protokol používá ve spojení s SSL/TLS, které se snaží zneviditelnit komunikaci mezi servery a klienty, aby nedocházelo k útokům jako SQL Injections nebo XSS (Cross-site scripting).

V posledních letech byl ale vyvinut nový protokol HTTP/2, ke kterému se váže mnoho změn v tom, jak přenáší data.

Objevila se i velká slabina v protokolu SMB (Server Message Block), sloužící ke sdílení souborů, disků nebo periferních zařízení v síti LAN. Nejaktuálnější verze je SMB 3.0, útočníci ale dokázali využít starší verze SMB, které se v síti nestačily aktualizovat, a přes speciálně vytvořené zprávy pro SMB se úspěšně dokázali přihlásit na uživatelské účty (Center for Internet Security, 2017). Na tomto příkladu je ukázáno, jak je důležité nové aktualizace prověřovat a instalovat oficiální patche vydané od Microsoft, ještě důležitější mít správně nakonfigurované politiky práv pro všechny uživatele a skupiny v síti.

11 Průzkum bezpečnostních chyb a aktuality

Nebezpečný software, obecně označovaný jako malware, se může chovat různými způsoby. A ať už škodí jakkoli, po napadení se vždy dostaneme k výsledku, že jsme přišli o finanční prostředky v podobě našeho času nebo ztracených výhod. Každý systém nebo síť má své chyby a nedostatky v bezpečnosti, které staví naše prostředky před rizika odcizení nebo poškození. Můžou se vyskytovat v operačním systému a firemních aplikacích, nebo na hardwaru na kterém dané služby provozujeme.

V nejlepším případě své vlastní zranitelnosti známe a umíme je ochránit, v tom horším je sice známe, ale opravit nedokážeme (např. nedostatečné finanční prostředky – je pak k zamyšlení, jestli případné zneužití zranitelnosti pro firmu bude mít horší finanční dopad než vynaložit finance pro ochranu známé zranitelnosti) a nejhorší případ nastává, pokud o zranitelnosti vůbec nevíme. Objeví se zde cesta pro potencionální útoky a zneužití (exploits) našich prostředků.

CVE (Common vulnerabilities and exposures) byla spuštěna v roce 1999, aby dokázala pojmenovat všechny nalezené zranitelnosti, spravuje ji MITRE Corporation. Je to seznam poskytující popis zranitelností různých operačních systémů, protokolů anebo funkcionalit, které může veřejnost použít pro svou kybernetickou bezpečnost (Venter et al., 2008). Seznam obsahuje technické informace

Cituji, jak CVE definuje zranitelnost (vulnerability):

"A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety)." (NIST: National vulnerability database, 2018)

CVE není jediná databáze zranitelností (CERT/CC Vulnerability Notes Database, The Exploit Database by Offensive Security, aj.), v této práci jsou použita dostupná data z CVE, aby bylo možno krátce zanalyzovat stav řešení verze WS2012 a WS2016 a zjistit, jestli jsou taková data informačně přínosná, a na kterou oblast bezpečnosti je třeba se zaměřit.

Na začátku musí být zmíněno, že nad staženým datovým setem nelze provést kompletní statistickou analýzu, jelikož chybí spoustu proměnných, které bychom k celkové analýze potřebovali. Populační vzorek, který je k dispozici, není dostatečně relevantním zdrojem dat pro statistický rozbor. Není možné zjistit, jestli je v databázi zaznamenán celý výčet zranitelností, protože z různých důvodů některé firmy ani nenahlásí, že určitá chyba byla zneužita. Děje se tomu tak kvůli prestiži nebo ochraně uniklých dat. CVEDetails nezveřejňuje, kolik klientů používá daný operační systém.

Můžeme polemizovat, jestli je vůbec možné analyzovat všechny problémy ve WS2016 a jen díky statistice spolehlivě říct, že se jedná o bezpečný systém. Analýza dat v této práci slouží hlavně k přehledu nejproblémovějších zranitelností, kde se vyskytují, a jestli je lze reálně řešit.

Na dvou tabulkách ukážeme počet zaznamenaných zranitelností v systému WS2012 (Tab. 2: Windows server 2012 Vulnerabilities) a WS2016 (Tab. 3: Windows server 2016 Vulnerabilities), stručně budou popsány sloupce v tabulkách. V prvním sloupci je rok zaznamenání zranitelnosti, kdy v roce 2012 a 2016 vyšly verze, a proto je zranitelností pochopitelně méně, stejně tak v roce 2019 je počet nižší (poslední revize dat 2019-2-25). Hodnoty v druhém sloupci „# of Vulnerabilities“ ukazují celkový počet zranitelností za daný rok. Sloupec DoS odkazuje na počet zranitelností, kdy útočník cílí na nedostupnost služby. Code Execution je podsunutí vlastního kódu, který má napadený stroj vykonávat. Sloupec Overflow, dat dočasně uložených v bufferu může být tolik, že další příkazy už program nepřijme, což může zapříčinit, že nepřijme i některé důležité příkazy se specifickou funkcí bránící útočníkovi zneužití dat. Memory Coruption využije chyby v napsaném programu a přesměruje paměťové prostředky. Útok XSS jsme zmínili v kapitole o protokolech a síťových vrstvách, jde o hledání slabin v kódu webových aplikací. Directory Traversal Attack prochází přes pravidla ACL (Access Control List), přičemž se dostane k adresářům na webovém serveru. Bypass something je v podstatě obcházení pravidel nastavených v síti (např. úplně přeskočit autentizační krok). Gain Information, získání informací (např. o topologii sítě). Gain Privileges, získání oprávnění v systému. Poslední sloupec „# of exploits“ ukazuje, kolik zranitelností (zaznamenaných v konkrétním roce) bylo ve skutečnosti zneužito.

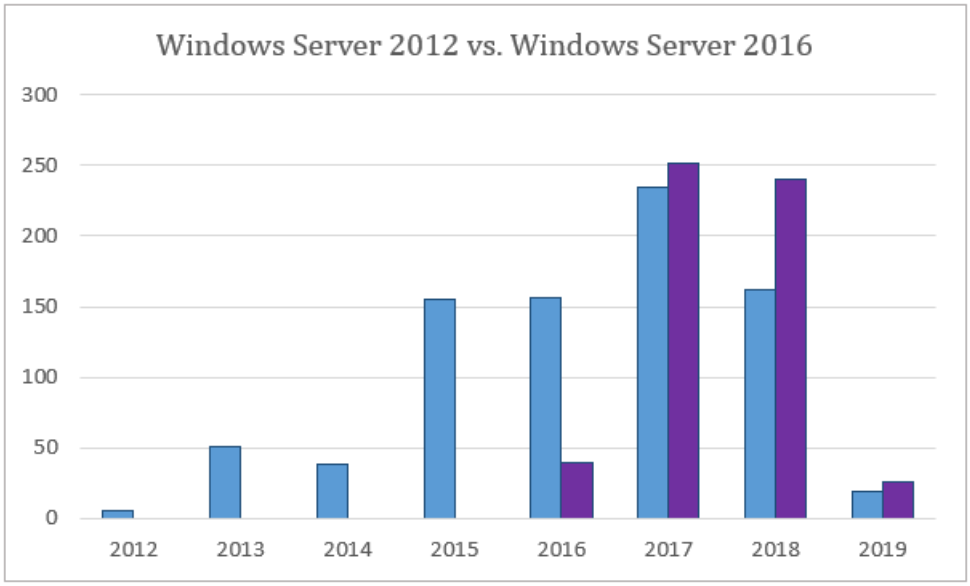
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	XSS	Directory Traversal	Bypass something	Gain Information	Gain Privileges	# of exploits
2012	5		2	2				1		2	
2013	51	12	17	17	3		1	2	2	21	4
2014	38	9	11	5	3			6	5	12	4
2015	155	16	46	11	9		1	31	26	60	1
2016	156	8	42	19	7			16	28	76	
2017	235	24	51	18	4	1		6	107	15	
2018	162	11	34	15	1	1		12	64		
2019	19		11	11					4		
Total	821	80	214	98	27	2	2	74	236	186	9
% of all		9,74%	26,07%	11,94%	3,29%	0,24%	0,24%	9,01%	28,75%	22,66%	

Tab. 2: Windows Server 2012 Vulnerabilities
Zdroj: (CVE Details, 2019)

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	XSS	Directory Traversal	Bypass something	Gain Information	Gain Privileges	# of exploits
2016	39	1	7	12	2			3	6	23	
2017	252	29	50	12	4	1		17	103	13	
2018	240	18	41	17	1	1		40	67		
2019	26		13	11					5		
Total	557	48	111	52	7	2	0	60	181	36	0
% of all		8,62%	19,93%	9,34%	1,26%	0,36%	0,00%	10,77%	32,50%	6,46%	

Tab. 3: Windows Server 2016 Vulnerabilities
Zdroj: (CVE Details, 2019)

Dle záznamů ve verzi WS2012 bylo v průměru za rok zaznamenaných méně zranitelností než ve verzi WS2016. Přesnější srovnání vidíme v grafu na obrázku č. 5, graf byl sestaven z dat z tabulek výše, ze sloupce „# of Vulnerabilities“. Vyšší počet zranitelností ve WS2016 může být způsoben nasazením několika nových služeb, které v dřívějších verzích nebyly dostupné, i přesto že tyto služby byly dříve nasazené v cloudu Azure. Tento fakt mohla zapříčinit ale také zvýšená pozornost profesionálů, kteří cílili na bezpečnostní prvky nového řešení. Na druhou stranu si můžeme všimnout, že ve WS2016 nebylo zaznamenáno žádné zneužití zranitelností. Jak už bylo zmíněno, zneužití zranitelnosti se vůbec nemuselo nahlásit nebo klient ani nemusí vědět, že jeho systém byl napaden anebo kterou cestu útočník k jeho systému využil.



Obr. 5: Porovnání počtu zranitelností mezi dvěma verzemi Windows Server
Zdroj: vlastní zpracování, data získána z tabulek CVE

Nyní se zaměříme na konkrétní zranitelnosti zaznamenané v CVE, rozebereme tabulku č. 3, Windows Server 2016 Vulnerabilities. Jednotlivé zranitelnosti mají své score, v práci se zaměříme na ohodnocení vyšší než 5 (CVSS score >= 5), celá metodika určování rizikovosti zranitelnosti je popsána v CWSS (Mitre, 2014).

Nejvíce početnou skupinou zranitelností je sice Gain Information, ale skládá se převážně z méně rizikových zranitelností. Najdeme zde ale chyby v autentizaci a nesprávně přiřazených oprávnění (CVE-2018-8434, CVE-2017-11772, CVE-2017-0077), nebo ve špatné kontrole přijímaných IP paketů (CVE-2018-8493). Druhá nejrizikovější skupina je Code Execution, ve které najdeme téměř všechny nejohroženější zranitelnosti (většina má CVSS score >= 7). Pro příklad se jedná o chyby ve Windows Search a jak ukládá objekty v paměti (CVE-2017-8543), nebo zranitelnost v DNS a způsobu ukládání požadavků na serveru (CVE-2018-8626), nebo nedostatky ve službě TFTP (CVE-2018-8476). Třetí nejpočetnější skupinou Bypass something, zde najdeme zranitelnosti v novém Device Guard, který nesprávně validoval integritu kódu v souborech nebo ho potencionální útočník může obejít přes PowerShell session (CVE-2017-11899, CVE-2017-11823), objevila se i zranitelnost v Kerberos při výměně lístků a zmanipulování hodnoty v SNAME (CVE-2017-8495). V datech se objevilo i nebezpečí, kdy Kerberos autentizace neprošla a musela se jako defaultní použít NTLM autentizace (CVE-2017-8563). Právě autentizaci a přidělená práva budeme více prozkoumávat v praktické části práce.

11.1 Potencionální hrozby pro Windows a jak se jim vyhnout

WS2016 je zatím poslední verze serverového OS řešení od Microsoft, která se zaměřovala hlavně na zvýšení bezpečnosti. Řešení v sobě má zabudované služby, které umí automaticky detekovat škodlivý software, většina je popsána v kapitole o novinkách oproti starším verzím a v části o rolích WS2016. Nic ale není stoprocentní, dokud prostředí WS2016 nepřizpůsobíme konkrétnímu řešení LAN a používaným službám.

Microsoft má své rady, jak se preventivně bránit malwaru v dokumentaci Prevent malware infection (Microsoft, 2019). Jejich produkty by měly být vždy aktuální, na možnosti update softwaru umí produkty sami upozornit. Vydáváním patchů každé druhé úterý v měsíci se začalo říkat Patch Tuesday (PT), útočníci mohou využít seznam opravených zranitelných míst v OS, které ještě nebyly opraveny nebo vyzkoušet, jestli dříve nalezené chyby nejsou stále nedokončené. Vypuštění ještě neznámého malware hned po Patch Tuesday také maximalizuje potencionální životnost exploitu a ještě víc podpoří možnost rozšíření (Zseby et al, 2013).

Když informujeme o hrozbě vlastní zaměstnance, o podezřelých odkazech v e-mailech a nevstupování na nebezpečné webové stránky, nepoužívání neznámých datových médií a počítačů, zvyšujeme bezpečnostní zásady, pomohou i přednášky o existenci sociálního inženýrství.

V roce 2017 byl rozšířen ransomware WannaCrypt, který dokázal zašifrovat soubory v nakažené klientské stanici a po zaplacení určité částky měl údajně odeslat klíč k rozšifrování, technické informace ve zdroji Multiple Vulnerabilities in Microsoft Windows SMB Server Could Allow for Remote Code Execution (CVE-2017-0144). Chvíli poté se objevil ransomware Petya, který zneužíval podobnou zranitelnost v SMB, upozornění a doporučení obrany vydány v článku Cyber Alert: Petya Ransomware (CIS, 2017). Obyčejně se ransomware sám od sebe nešíří, WannaCrypt a Petya se přes zranitelnost EternalBlue dokázali šířit v infrastruktuře LAN (Hern, 2017).

Pro takové případy je nutné mít zaručenou správu všech uživatelských účtů a domén, aby se při nákaze malware přinejmenším dál nešířil. Ve WS2016 jsou rozšířené možnosti, jak spravovat účty a přiřazovat jim uživatelská práva. Pomocí novinek jako Credential Guard, Advanced Threat Analytics, Just in Time Administration

nebo Just Enough Administration máme kontrolu nad právy pro každého uživatele zvlášť. Kam může přistupovat, jaké zprávy a žádosti pro služby v síti odesílat, jaké zdroje každý uživatel může používat. Návrh sítě by se měl řídit zásadou „co není povoleno, je zakázáno“. Je velice příhodné, že přiřazování a schvalování administrátorských práv je nyní pod správou více osob, protože ochrana účtů s vysokými pravomocemi by měla být prioritou.

K vyšší bezpečnosti slouží i několik nástrojů. Pro příklad – Threat detection je základní vlastnost bezpečnostní politiky Windows Serveru. Čím rychleji je hrozba (threat) nalezena, tím rychlejší může být náprava, než útočník převezme kontrolu nad chybou. Microsoft poskytuje Threat detection pro Windows servery jako součást Windows Defender Advanced Threat Protection. Zaznamenává v logu podezřelé aktivity, jako jsou: zapojení USB zařízení, úprava hesla, která nebyla v plánu, uzavření uživatelského účtu nebo vzdálené přístupy. Odstavec přeložen z průvodce (Windows Server 2016 Security Guide, 2017).

Pokud všechny ochranné prvky sítě selžou a firma přijde o svá data kvůli jakémukoli útoku, lze se obrátit na zálohy, ze kterých svá data může získat zpátky. WS2016 nabízí několik zálohovacích řešení, jedna z cest, jak udržovat své zálohy, je pomocí metody „zálohovacího pravidla 3-2-1“. V článku An Efficient Data Protection Strategy (Mayer, 2017) je metoda popsána stručně jako:

- Uchovávejte alespoň tři kopie vašich dat
- Uchovávejte zálohy na dvou rozdílných médiích
- Udržte jednu kopii offsite

Díky File Storages a dalším features je snadné vytvořit alespoň tři zálohy dat, mít pouze jednu zálohu se stále zdá jako vysoké riziko, že o data přijdeme. Druhé pravidlo o rozdílných médiích je o různých technologiích, jak lze zálohu uchovávat. Kromě fyzické úschovy na jednom serveru jsou k dispozici cloudová řešení, externí disky a jiná zařízení, kde redundantně uchováváme data. Musí být bráno v potaz, že každý disk nebo server jednou selže, nevydrží navěky. Třetí pravidlo, uchovávat jednu kopii ve vzdálené lokaci – v jiné budově, ještě lépe v jiném městě nebo zemi. Proti rozsáhlým katastrofám, které někdy zasáhnou široké okolí.

Přestože existuje celá řada rad a metodik, jak uchovávat svá data a zařízení před útoky a ztrátami, nejspíš není možné vyvinout dokonalé řešení. K dokonalému řešení se můžeme pouze co nejvíce přibližovat.

Praktická část práce

12 Analýza prostředí a nasazení řešení

Se spoluprací s firmou bude v této části práce popsán návrh řešení rozestavění sítě a její konfigurace, za použití teoretických znalostí z předchozích kapitol. Budou zde použity technologie popsané v teoretické části práce. Zmíněná firma si nepřála být jmenována právě kvůli bezpečnosti – v případě že použije popsané řešení, není vhodné, aby bylo možné celou konfiguraci stáhnout online. Cílem řešení je doporučení, jak zefektivnit work-flow a zvýšit jeho bezpečnost. Navržení centralizované správy vývoje aplikací a zabezpečená komunikace prvků v síti LAN, analýza prostředí zahrnuje plánování, design a řízení prostředků v síti tak, aby byla zajištěna bezpečnost jak síťových prostředků, tak služeb poskytnutých firmou. Následující kapitoly jsou zaměřeny na vystavění robustní sítě v simulovaném prostředí pomocí programu VMware Workstation Pro, který poskytuje vhodné nástroje pro testování řešení. Následné řešení již bude možné převést na fyzické stroje pomocí konfigurace popsané v této práci.

Jedná se o firemní prostředí zabývající se vývojářskou činností. Zaměřují se hlavně na tvorbu webových aplikací a správu aplikačních serverů. Dosud byla k vývoji používána developerská platforma GitHub, na kterou si vývojáři ve firmě ukládali a sdíleli s ostatními svůj dosavadní progres ve vývoji. V poslední době ale firma dostala několik výhodných a rozsáhlých nabídek, u kterých bylo potřeba, aby na jednom projektu pracovalo více jak jeden vývojář. Vyskytly se problémy s kompatibilitou a samotným testováním aplikací, jejich nasazením s odlišnými komponentami a prostředím (např. rozdílné nastavení webového serveru IIS může způsobit, že na vývojářově počítači lze aplikaci spustit, na klientově už nikoli). Časové prodlevy byly příliš velké a práce se tak nestačila splnit do zadaného termínu.

Při konfiguraci jsou brány ohledy na bezpečnost nových funkcionalit, které Microsoft poskytuje, práce analyzuje možné zranitelnosti a snaží se je zabezpečit. LAN je stavěna tak, aby v příštích letech zajistila možnost rozvoje a zároveň dlouhodobě splnila požadavky firmy, které se časem vrátí prostředky, jež byly vloženy do sestavení

a správy sítě. Serverový počítač by měl mít dostatečně kvalitní komponenty zajišťující stabilitu, spolehlivost a optimalizovaný výkon.

12.1 Prvky ve VMware Workstation Pro

VMware Workstation Pro je platforma pro provoz několika operačních systémů jako virtuální stroje (VM) na jednom hostitelském počítači bez ohledu na jeho operační systém (VMware, 2019). Prostředí vystavěné v programu VMware nese výhodu v tom, že je zcela izolované a nabízí širokou paletu nástrojů pro testování i na profesionální úrovni. Nástroje VMware pro vybudování virtuální LAN byly zvoleny z osobních preferencí a zkušeností autora práce. Přestože by se dalo použít několik virtualizačních řešení (např. Windows Hyper-V), cílem práce není ověřování a testování virtualizačních technologií, ale prozkoumání bezpečnosti prvků samotného Windows Serveru a jejich nasazení v prostředí LAN. Autor práce se domnívá, že přenesení řešení popsaného v dalších kapitolách na jinou virtualizační platformu je pouze technická záležitost a neměla by zásadně ovlivnit nasazené prvky.

Jednou z funkcionalit VMware je spojení několika virtuálních strojů pod jednu síť. V praxi lze funkcionalitu přirovnat k spojování strojů pomocí kabeláže, switchů a routerů. V našem simulovaném prostředí budeme používat jeden router, jeden hlavní serverový počítač a klientské stanice, které se budou připojovat pomocí VMware switche ke kontejnerům spuštěným na serverovém počítači. Přes router s firewallem lze přistupovat k internetovému připojení, to musí být dostatečně odstíněné, protože je hlavní bránou mimo síť LAN. Jednoduché schéma je naznačeno na obrázku č. 6. Schéma obsahuje router R1 s firewallem filtrující připojení k internetu, stanici Win10, hlavní server WS2016, na kterém bude vytvořen virtuální switch vSW1 (nat) s připojenými kontejnery pro vývoj aplikací, a síťové prvky shrnuté switchem SW1 uprostřed. Takové schéma není těžké v budoucnosti rozšiřovat a napojovat na něj další části, pokud bude potřeba škálovatelnosti. Vývojové prostředí se všemi virtuálními stroji bylo vypracováno na notebooku Dell Inspiron 5567, Intel Core i5-7200U, RAM 8GB.

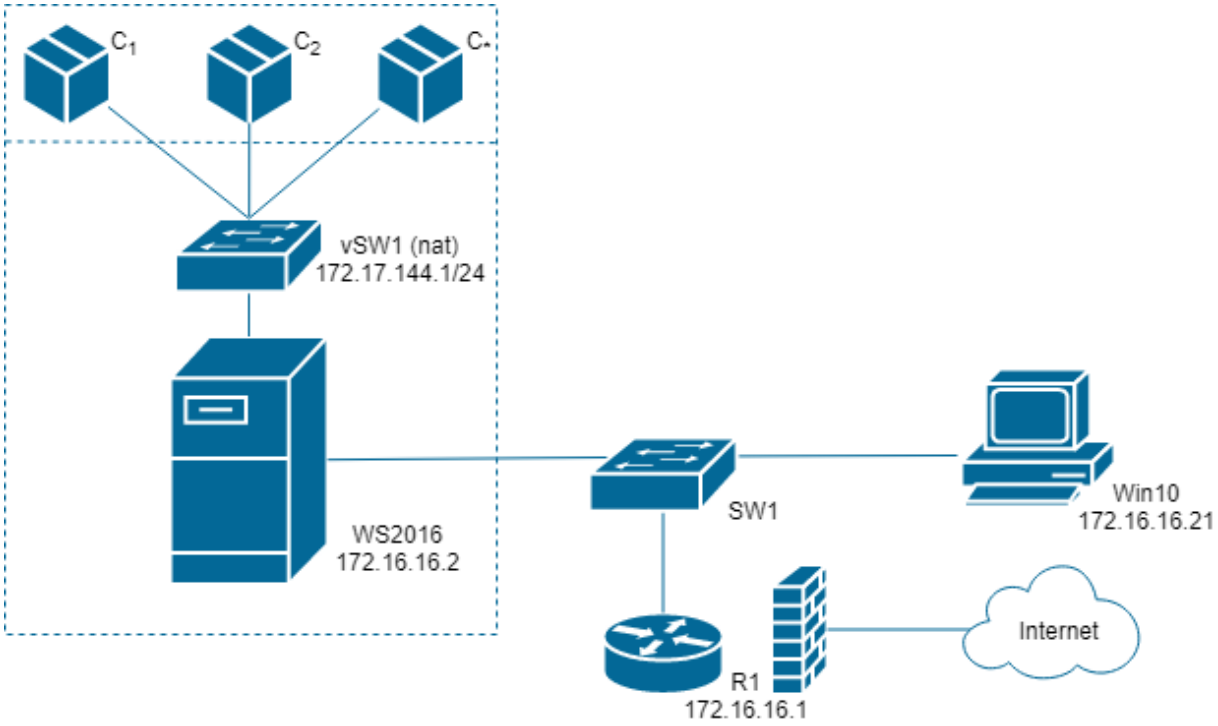
Hlavní router s firewallem je připojen k internetu přes staticky zadanou IP adresu, filtruje příchozí a odchozí komunikaci. Je připojený ke switchi, který se stará

o rozesílání další komunikace k serveru a ke klientským stanicím zaměstnanců. Firma není příliš rozsáhlá, na celou LAN nám prozatím stačí jeden subnet IP adres. O přidělování IP adres se bude starat služba na DHCP serveru, ta bude popsána později.

Častý rozsah adres, používaný v interních sítích je rozsah 192.168.1.0/24, tento rozsah je ale i velmi často používán jako defaultní rozsah u zakoupených modemů a routerů, a dalších síťových zařízení. Pokud bychom ho tedy zvolili do naší LAN sítě, může se stát, že dojde ke konfliktu a bude obtížné rozeznat správné spojení k identifikovanému zařízení. K tomu, aby byl provoz hladký, je lepší řešení používat odlišný rozsah IP adres uvnitř lokální sítě – z tohoto důvodu byl zvolen rozsah 172.16.16.0/24.

Nevyužité porty u switche je potřeba chránit před neautorizovaným přístupem, pravidelně je monitorovat a je třeba se ujistit, že jsou vypnuté. Nicméně, konfigurace všech síťových prvků není prvotním cílem práce, proto se soustředí hlavně na serverový počítač a klientské stanice.

V následujících kapitolách budou popsány základní prvky a služby zprovozněné v LAN, problémy, na které lze narazit a zranitelnosti, které je potřeba ošetřit.



Obr. 6: Návrh LAN
Zdroj: vlastní zpracování

12.2 Windows Server 2016 Datacenter

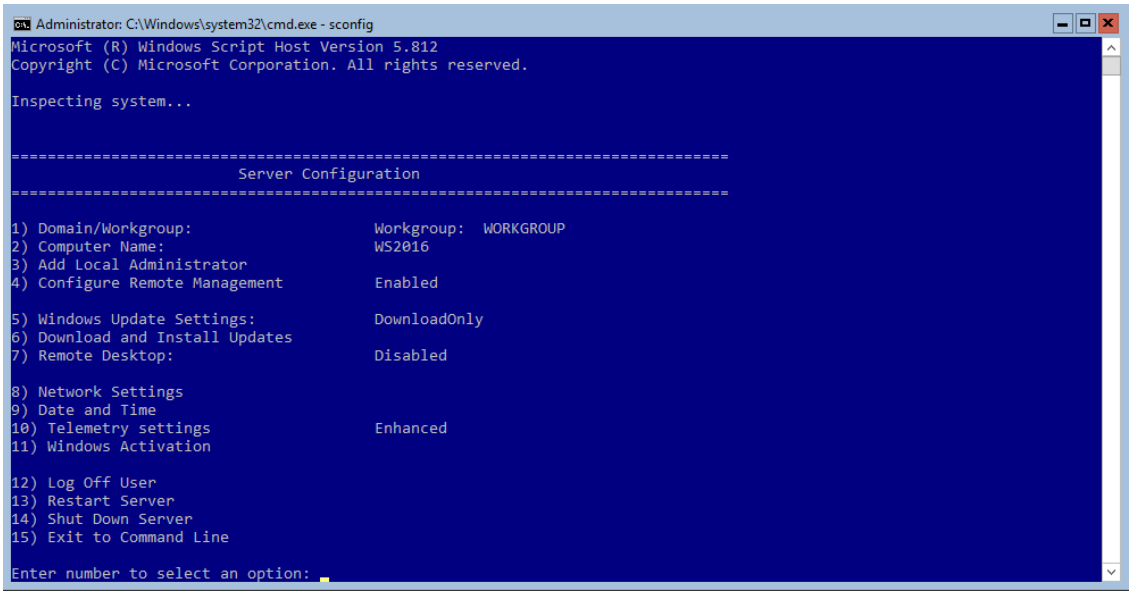
Volba vystavění vývoje aplikací v LAN byla pro firmu volbou hlavně proto, že již má k dispozici výkonný serverový počítač. Počáteční náklady se tím výrazně snížily a firma tak mohla uvažovat o uceleném způsobu vývoje aplikací.

Pro účely návrhu byla vybrána edice Windows server 2016 Datacenter, pro kterou jsme vytvořili virtuální stroj v programu VMware a později ji propojíme s ostatním zařízením v LAN. Virtuálnímu stroji jsme přiřadili počet procesorů a jader na jeden procesor, alokovali jsme optimální množství paměti, kterou může využít z hostujícího počítače. Proběhl boot virtuálního stroje s ISO souborem s instancí WS2016.

V instalaci ještě rozeznáme obvyklé grafické uživatelské rozhraní, což je ale jedno z mála, které na této stanici uvidíme. Specifikujeme, který jazyk bude OS používat, časovou zónu a preferovanou klávesnici. Intuitivně pokračujeme, důležité je, že vybereme možnost instalace OS bez uživatelského rozhraní, tedy Windows Server Core. Pro konfiguraci serveru většinou nevyužijeme uživatelské rozhraní, pouze konzoli PowerShell, popřípadě vzdálený přístup. Následně přijmeme licenční podmínky, vybereme disk pro instalaci (v našem případě jeden prázdný 80G disk, který jsme alokovali na virtuálním stroji) a můžeme potvrdit instalaci. Instalace netrvá dlouho a můžeme začít s prvotní konfigurací.

Po automatickém restartu jsme vyzváni vytvořit heslo k zařízení a k účtu Administrator, než se dostaneme do cmd.exe. Bez účtu s administrátorskými právy se do systému nelze dostat, ten je automaticky vytvořen s instalací. Pro úplné začátky je příjemné použití příkazu `sconfig`, ve kterém nastavíme základy systému. Variantou je spustit `powershell`, ve kterém přejmenujeme počítač:

```
Rename-Computer -Name WS2016
Restart-Computer
```



Obr. 7: Příkaz sconfig spuštěný z powershellu

Zdroj: vlastní zpracování

Na obrázku č. 7 je vidět již přejmenovaný počítač po zadání příkazu sconfig. Doménu řešit nemusíme, ještě žádnou vytvořenou nemáme a počítač není připojen k žádné síti. Až zprovozníme službu AD a vytvoříme první doménový les, server se přidá do domény automaticky. S tím se pojí i kontrola Date and Time, která by se sice měla nastavit při instalaci podle časové zóny, ale někdy se i může stát, že času a datu neodpovídají a my musíme čas manuálně zadat, aby serverové služby pracovaly správně. Možnost Windows Update Settings je defaultně nastavena na DownloadOnly, což nám prozatím vyhovuje, automaticky se nebude nic instalovat. Pro LAN s malým počtem serverů nebude problém aktualizovat pouze ručně. Remote desktop povolíme v pozdější části práce, stejně tak přidělíme serveru statickou IP adresu ze zvoleného subnetu. Jakmile budeme připojeni k internetu, ve volbě Download and Install updates vyhledáme dostupné aktualizace a můžeme vybrat, které jsou důležité a doporučené jako opravy některých bezpečnostních chyb.

12.3 Active Directory a DNS

Nesprávná konfigurace DNS serveru může vést k vážným problémům, jako je přenastavení a přesměrování DNS zón na jiné IP adresy, čímž se může přesměrovat e-mailový přenos anebo provoz na webovém serveru, nebo otevřít cesty k různým formám DDoS útokům. Společně s DNS přichází i služba AD, kterou nainstalujeme následujícím příkazem:

```
netsh interface ipv4 set address name="Ethernet0" source=static
address=172.16.16.2 mask=255.255.255.0 gateway=172.16.16.1

Install-WindowsFeature -Name AD-Domain-Services
-IncludeManagementTools
```

Po příkazu není potřeba server restartovat. Se službou AD DS je automaticky nainstalována i služba DNS. Před nainstalováním role DNS bylo přiřazena serveru IP adresa, abychom s ním mohli komunikovat. Statická adresa nám zaručí, že nedojde ke konfliktu, pro doménový řadič ani není povolené, aby měl dynamickou IP adresu. Příkaz `netsh` slouží k nastavení síťové komunikace, tento příkaz se vztahuje k interface Ethernet0, jehož jméno jsme zjistili pomocí příkazu `ipconfig`.

Po úspěšné instalaci služeb AD, vytvoříme první les – zadáme safemodeadministratorpassword a potvrdíme restart počítače. Jelikož je vytvořena první doména, server se automaticky stane doménovým řadičem a přiřadí se do domény corp.secure.cz.

```
Install-ADDSForest -DomainName "corp.secure.cz"
```

Důležitou částí DNS je nastavení zón, které bude server používat. Do zón přidáme primární zónu naší domény corp.secure.cz (přidán parametr ReplicationScope Forest, který replikuje tuto zónu i na případné ostatní DNS servery v rámci AD lesa).

```
Add-DnsServerPrimaryZone -Name corp.secure.cz -ComputerName WS2019
-ReplicationScope Forest
```

Server si obvykle poslední vyhledávané záznamy ponechává, kdyby bylo potřeba hledat stejné záznamy (cache lookup). Pak zaznamenává forward lookup zóny, které mapují jednotlivé IP adresy, a reverse lookup zóny ukazující na z IP adres na jména domén (PTR records). Pokud adresa ve forward lookup 10.20.30.40 ukazuje na domena.cz, není zárukou, že stejná adresa v reverse lookup zóně vede na stejnou doménu. Jedním z důvodů, proč nastavit správnou reverse lookup zónu, jsou mailové servery, v případě této práce bylo nutné přidání PTR recordu (`Add-DnsServerResourceRecordPtr`) kvůli použití příkazu `Invoke-WebRequest`, troubleshootingu instalace Dockeru a správného fungování služby DNS. Powershell má mnoho možností, jak testovat funkčnost DNS (př. `Test-DnsServer -IPAddress` nebo

`nslookup`). Windows Server 2016 a novější verze OS mají také defaultně povolený DNS Cache Locking a DNS Socket Pool, zvyšující bezpečnost.

Rozšířením DNS a zvýšení bezpečnosti docílíme implementací DNSSEC, jehož nástroje jsou ve Windows k dispozici. Kontroluje integritu informací ze zdrojů a ověřuje jejich důvěryhodnost, používá digitální podpisy uložené v RRSIG záznamech.

12.4 Služba DHCP

Dalším krokem je zprovoznění služby DHCP a autorizace serveru v infrastruktuře AD. Autorizace je důležitá pro distribuci IP adres v doméně, provádět ji může pouze administrátor se členstvím v Enterprise Admins skupině nebo někdo, komu jsme na to delegovali práva. Náš server je zároveň doménový řadič a server by se měl automaticky autorizovat, pakliže tak není, použijeme příkaz `Add-DhcpServerInDC`. Seznam autorizovaných serverů lze vypsat příkazem `Get-DhcpServerInDC`.

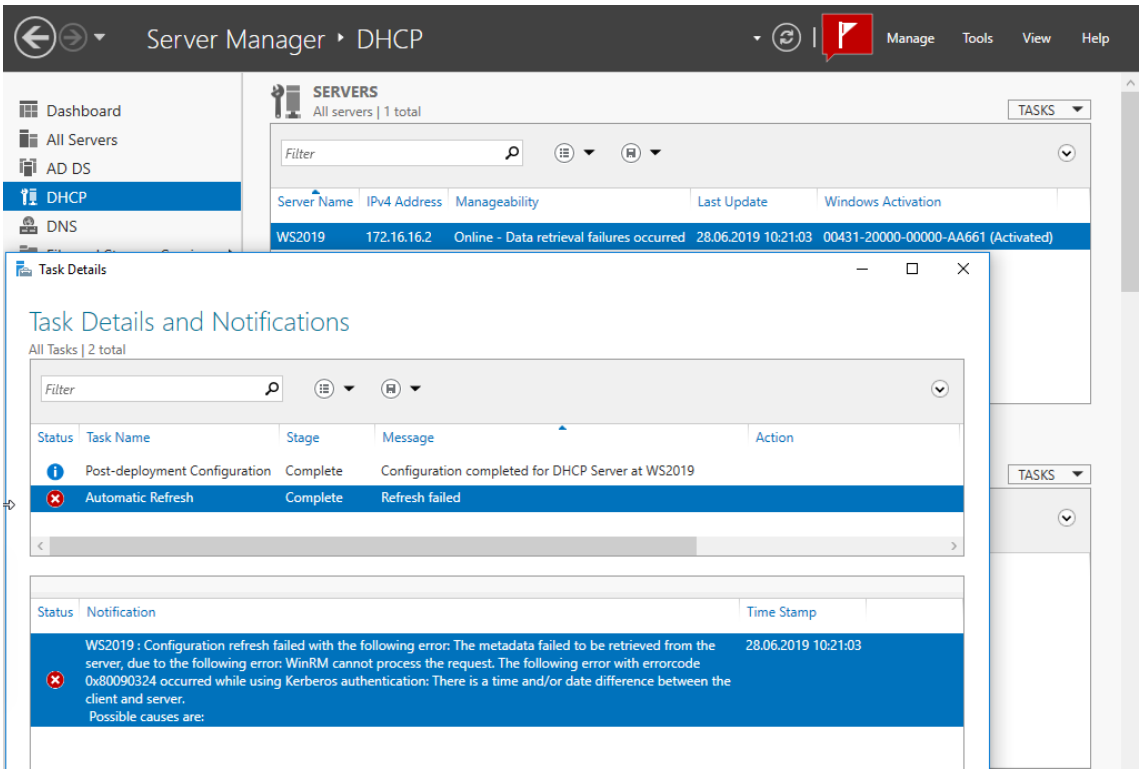
```
Install-WindowsFeature -Name DHCP -IncludeManagementTools
Add-DhcpServerInDC -DnsName "WS2016.corp.secure.cz" -IPAddress
172.16.16.2
```

Na řadě je určit, jaký rozsah IP adres bude server poskytovat a automaticky přiřazovat do připojených zařízení nebo dalších DHCP klientů do sítě. Je třeba dbát na adresy, které jsou přiřazeny staticky a vyčlenit je do zvláštního rozsahu, jež nebude přiřazován klientským stanicím – jedná se o server WS2016 a router. V ExclusionRange zůstane i další rezerva, dohromady vyčleníme 20 IP adres pro statické adresy. Nakonec službu DHCP restartujeme, aby se rozsahy aktivovali.

```
Add-DhcpServerV4Scope -Name "SecureCorp" -StartRange 172.16.16.1 -
EndRange 172.16.16.254 -SubnetMask 255.255.255.0 -State Active
Add-DhcpServerV4ExclusionRange -ScopeID 172.16.16.0 -StartRange
172.16.16.1 -EndRange 172.16.16.20
Set-DhcpServerV4OptionValue -DnsDomain corp.secure.cz -DnsServer
172.16.16.2 -Router 172.16.16.1
Restart-Service dhcpserver
```

Přestože byl server autorizován, po prvotní konfiguraci se vyskytl problém zobrazený na obrázku č. 8. Objevila se chyba 0x80090324 při ověřování serveru pomocí Kerberos, která značila rozdíly v času na klientské stanici a serverové stanici.

Byla provedena synchronizace času a následně vyčištěna cache všech Kerberos tiketů pomocí `KList purge`, což vyřešilo problém a chyba se již znovu neobjevila.



Obr. 8: Problém autorizace Kerberos
Zdroj: vlastní zpracování

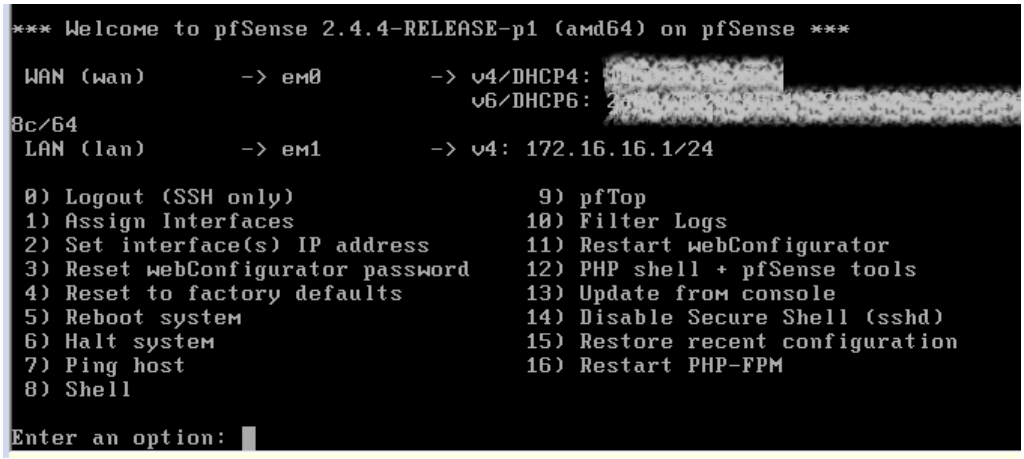
12.5 Router a firewall

Pro prostředí byl vybrán jako router a firewall systém pfSense založený na FreeBSD. Projekt je zdarma a open-source, lze ho nainstalovat na libovolný hardware, který splňuje určité podmínky popsané v dokumentaci, není problém ho používat i v prostředí virtuálním jako v této práci. Pokud by bylo řešení použito v praxi, neměl by být problém zakoupit i komerční řešení a zahrnout ho do stávajícího návrhu i se zákaznickou podporou.

Přestože je router s firewallem umístěn na výstupu ze sítě, nezaručí naprostou bezpečnost, i když jedním z primárních funkcí pfSense je chovat se jako firewall. Jak bylo zmíněno v teoretické části práce, firewall se dělí na paketové filtry a aplikační brány. V případě firewallu na routeru se jedná o paketový filtr, z toho důvodu bude

potřeba nastavit i vhodnou formu aplikačního firewallu na každé pracovní stanici v interní síti, abychom se vyhnuli nakažení LAN malwarem.

V prostředí VMware je pfSense nainstalovaný na samostatném virtuálním stroji, kterému stačí méně než 1GB paměti. Přiřazené má dva síťové adaptéry – jeden připojen k subnetu naší sítě, druhý nastaven na adaptér pro připojení k internetu přes hostitelský počítač. S ISO souborem provedeme instalaci operačního systému než je pfSense restartován a připraven ke konfiguraci. Jednou z funkcí je i přidělování adres pro zařízení v síti, ale jelikož k tomuto účelu nám bude sloužit samostatný DHCP server, všechny možnosti přidělování adres odmítneme. Objeví se nabídka s několika volbami, ve které přidělíme zařízení IP adresu 172.16.16.1, tyto volby a přidělenou IP adresu vidíme i na obrázku č. 9. Adresa vedoucí do internetu je detekována automaticky, ať už je router připojen fyzickým konektorem, nebo v našem případě zařazen do virtuálního síťového adaptéru. Nyní už může být zařízení v síti viditelné a lze provést konfiguraci přes klientskou stanici a webové rozhraní. Je důležité nastavit časovou zónu, známé DNS servery, používání HTTPS, a přesměrování provozu na adekvátní porty. Pro budoucí potřeby této práce je tu i možnost povolit VPN spojení, kterým bude možné klient přistupovat do LAN.



Obr. 9: Nastavení pfSense
Zdroj: vlastní zpracování

12.6 Uživatelé a group policy

Dvě hlavní skupiny, na kterých lze uplatnit group policy, jsou uživatelé a počítače. Uživatelské politiky se kontrolují při přihlášení uživatele, politiky

aplikované na počítače již při startu počítače, a pak se obnovují podle periodického času gpupdate, který zadáme v pravidlech group policy.

Pro vzdálenou správu WS2016 vytvoříme účet DomainSecure patřící do skupiny doménových adminů. Defaultně se do domény přidají předdefinované skupiny administrátorů, hostů a dalších uživatelů, Domain Admins je jedna z nich (další v CN=Builtin a CN=Users). Nastavíme heslo tak, aby se nezadávalo přes plaintext (bez parametrů `ConvertTo-SecureString -AsPlainText "p@ssw0rd"`). Povolíme účet v infrastruktuře AD a nakonec přidáme do skupiny adminů.

```
New-ADUser -SamAccountName "domainadmin" -GivenName Petr -Surname
Kovar -Path "CN=users,DC=corp,DC=secure,DC=cz"
Set-ADAccountPassword DomainAdmin
Enable-ADAccount DomainAdmin
Add-ADGroupMember 'Domain Admins' DomainAdmin
```

Vytvoříme novou organizační jednotku, do které budou patřit všichni vývojáři ve firmě a budou vlastnit stejná práva, do jednotky přiřadíme nového uživatele, nastavíme heslo a povolíme v AD.

```
New-ADGroup -Name "Developers" -GroupScope DomainLocal -PassThru
New-ADUser -SamAccountName "lenydeveloper" -GivenName "Leny" -
Surname "Folprecht" -DisplayName "Leny Folprecht" -Path
"CN=users,DC=corp,DC=secure,DC=cz"
Enable-ADAccount LenyDeveloper
Add-ADGroupMember 'Developers' LenyDeveloper
```

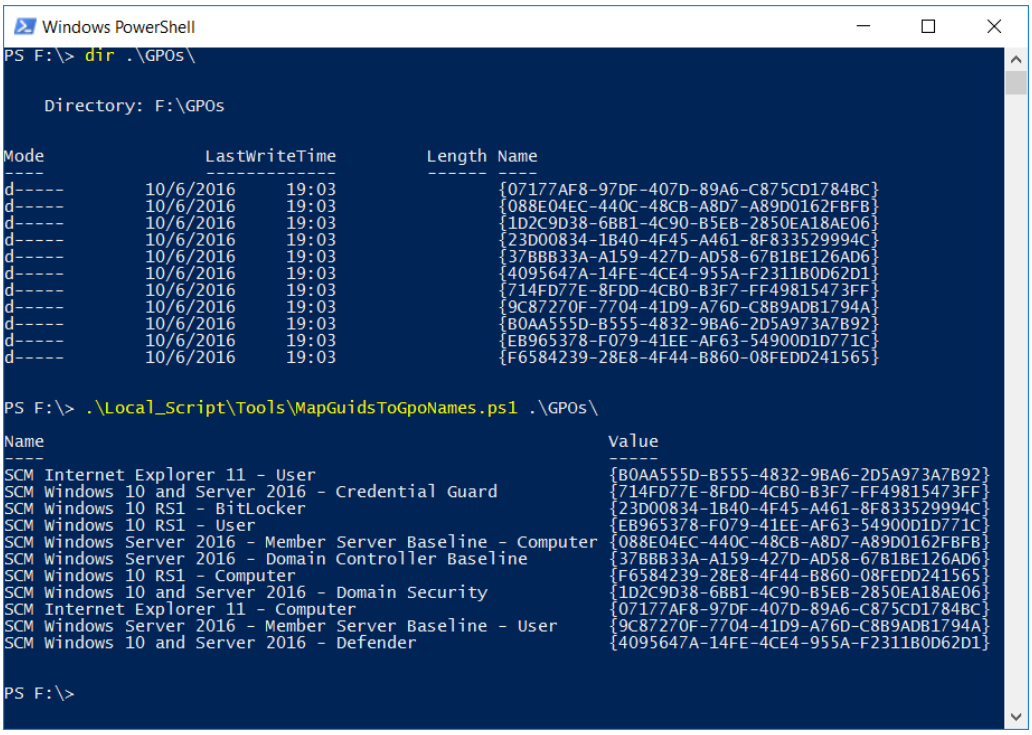
Stejně jako jsme vytvořili virtuální stroj pro server a router, přidáme do infrastruktury VMware i klientský počítač s Windows 10 Pro (dále jen Win10). I na virtuálním stroji lze nastavit funkcionalitu Secure boot, která byla popsána v teoretické části práce. Po běžné instalaci je potřeba pouze přiřadit počítač do domény corp.secure.cz a jestliže byl DHCP server správně nastavený, po restartu počítače je mu automaticky přiřazena IP adresa. Do domény počítač zařadíme přes Settings -> System -> About -> Join a domain, je po nás vyžadováno heslo na účet s dostatečnými právy pro přístup do domény, použijeme účet DomainSecure, který byl před chvílí vytvořen. Po restartu už se můžeme přihlásit do počítače k účtu CORP/DomainSecure (Petr Kovar). Přes tuto stanici byl nakonfigurován i router s firewallem.

Pro další konfiguraci byl stažen na stanici Win10 nástroj Remote Server Administration Tools (RSAT) umožňující vzdáleně spravovat server a také group policy. Obsahuje nástroje Server Manager, Microsoft Management Console (MMC)

snap-ins a nové cmdlety pro správu v PowerShell. Microsoft vydává doporučené základy, jak zabezpečit stanice a servery v síti, pomocí nástroje Microsoft Security Compliance Toolkit můžeme porovnat stávající zásady s nově zavedenými (Microsoft Security Compliance Toolkit, 2019). Po instalaci RSAT můžeme přistupovat přes Server Manager k serveru WS2016 v doméně, přes Add other servers to manage > vyhledáme jméno serveru, potvrdíme volbu a následně už vidíme stav serveru a všechny služby, které jsme přidali (AD DS, DHCP, DNS, File and Storage Services). Abychom se dostali ke všem nastavením počítače vzdáleně, je potřeba povolit několik firewall pravidel nebo udělit výjimky jenom pro vzdálený přístup. Příkazem `Enable-PSRemoting -Force`, nastartujeme služby pro WinRM, které se automaticky spustí při startu systému, povolí připojení přes session a udělí výjimky pro firewall pravidla, která jsou vypsaná v dalším odstavci:

```
Enable-NetFirewallRule -DisplayGroup "Remote Event Log Management"
Enable-NetFirewallRule -DisplayGroup "Remote Service Management"
Enable-NetFirewallRule -DisplayGroup "File and Printer Sharing"
Enable-NetFirewallRule -DisplayGroup "Performance Logs and Alerts"
Enable-NetFirewallRule -DisplayGroup "Remote Volume Management"
Enable-NetFirewallRule -DisplayGroup "Windows Defender Firewall
Remote Management"
```

Stáhneme soubor se Security Baselines, složku rozbalíme – na obrázku č. 10 je vidět seznam doporučených nastavení GPO. Otevřeme konzoli Group Policy Management, kde vytvoříme nové GPO, kam naimportujeme soubor s doporučeným nastavením pro náš server. V konzoli můžeme vybrat, na kterou doménu a doménový řadič budou nastavení zásad použity.



Obr. 10: Security baselines pro Windows 10 a Windows Server 2016
Zdroj: (Margosis, Microsoft Security Guidance Blog, 2019)

Po importu spustíme příkaz `gpupdate /force`, aby se změny projevily. Lze použít i další nastavení pro celou doménu nebo jednotlivé uživatele. V konzoli se nastavují politiky o vypršení hesla v síti, jeho délku nebo kolik posledních hesel se ukládá v paměti, aby uživatel nemohl používat stále stejná, nebo povolení auditování. V tomto natavení LAN se navíc vychází z defaultně vytvořených GPO jmenující se Default Domain Policy a Default Domain Controllers Policy, které vznikly při instalaci Active Directory. Default Domin Policy se dělí na podkategorie Password Policy, Account Lockout Policy a Kerberos Policy. V Default Domain Controller Policy se nastavují User Rights Assignment a Security Options. Tato defaultní pravidla byla zpřísněna pro potřeby zamykání účtů, politiky hesel a politiky Kerberos. Ostatní politiky byly přesunuty do nových GPO, kde se privilegia jednotlivých účtů dají rozdělit do organizačních jednotek, u nichž některé ani nepotřebují administrátorská práva. Což se týká hlavně skupiny Developers, do které budou vkládány účty vývojářů.

V síti bylo přes politiky zakázáno použití NTLM, místo toho se používá silnější Kerberos nutný pro Active Directory. V dalším GPO byl omezen pro uživatele přístup k ovládacím panelům. Bylo zakázáno ukládání hashů při změnách hesla (Network security: Do not store LAN Manager hash value on next password change), vynucený restart počítače při instalaci aktualizací (No auto-restart with logged on users for

scheduled automatic updates installations), nebo zakázání všech externích médií (All removable storage classes: Deny all accesses). Zásada Accounts: Guest Account Status již byla defaultně zakázána. Přes Group policy, nebo příkazem: net user administrator /active:no, je vhodné zakázat lokální administrátorské účty předtím, než se stanice dostane do rukou klienta – potřebné úkoly můžeme dokončit centrálně z účtu s potřebnými právy.

Group policy jsou užitečná a vhodná řešení, jak splnit řízení přístupových oprávnění z vyhlášky o kybernetické bezpečnosti, jejich úplné vypsání a prozkoumání je pro rozsah této práce příliš široký a podrobný popis všech pravidel je materiál na samostatnou diplomovou práci.

Předtím než jsou ale jakákoli nová pravidla použita a aplikována v produkčním prostředí, je doporučeno je pečlivě otestovat a vyzkoušet. Při prvních pokusech aplikace některých nových zásad přestala fungovat služba DNS, klientská stanice se tedy odpojila a nemohla najít doménu corp.secure.cz. Na hlavním serveru nebyla nalezena konektivita k LDAP (Name resolution is not funkcional. _ldap._tcp.corp.secure.cz. failded on the DNS server 172.16.16.2), což bylo způsobeno špatně nastavenými zásadami skupin doménových řadičů a nedostatečným definováním firewall pravidel, který blokoval požadavky DNS.

12.7 Vzdálený přístup a certifikační autorita

Jelikož byla na serveru zprovozněna služba vzdálené plochy, je třeba ošetřit, aby komunikaci nebylo snadné odposlouchávat a na připojeném serveru nemohl uživatel provádět cokoli. V kapitole ošetříme komunikaci LDAP pomocí SSL/TLS technologií a certifikátů.

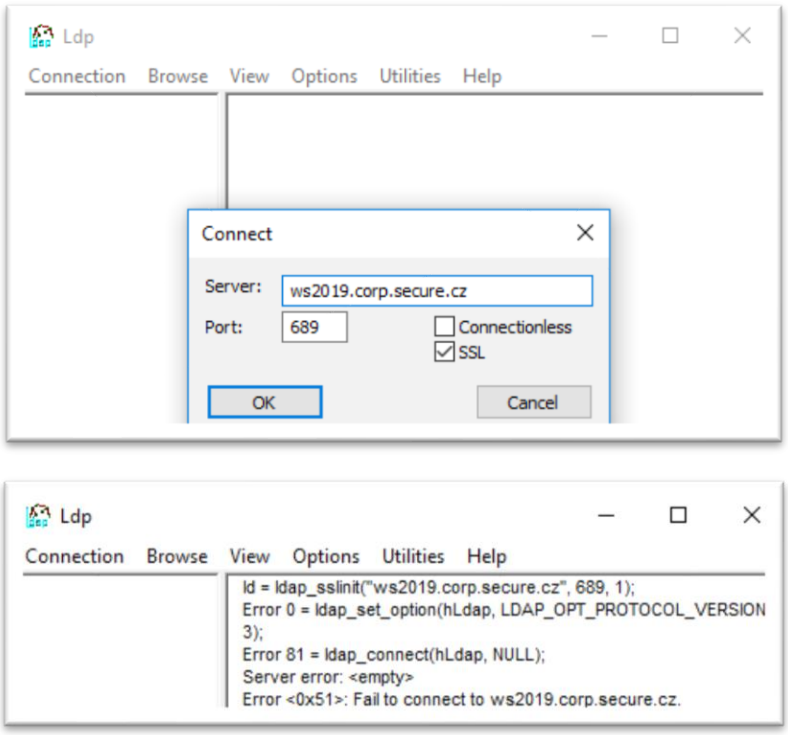
Z novinek pro Windows Server 2016 a Windows 10 může být použit Remote Credential Guard, který přes vzdálený přístup k počítači přesměrovává Kerberos lístky a ochraňuje spojení, dovoluje používat prostředky SSO, jak bylo zmíněno v teoretické části práce. Zařízení, ke kterému se chceme připojit, musí být v AD ve stejné doméně, nebo v doméně, ke které je vytvořen trust.

Problém ale nastane, když nevlastníme správnou edici klientské stanice Windows 10 – v této práci je použita edice Professional, ale nová funkcionalita je

k dispozici pouze v edici Enterprise a na edicích Windows Serveru. Je pouze na klientovi, jestli se mu vyplatí investovat do edice Enterprise, pro firmu, která velikostí nedosahuje velkého korporátu. Remote Credential Guard lze zapnout pouze na Windows Serveru 2016, což nabude efektu pouze pokud i klientská stanice bude mít spuštěnou funkcionalitu. Zapnutí je jednoduché, přes group policy management konzoli (Credential Delegation > Restrict delegation of credentials to remote servers > Require Remote Credential Guard) nebo úpravou registrů, kde přidáme hodnotu DWORD DisableRestrictedAdmin a změníme ji na hodnotu 0, čímž je vlastnost povolena. Nejen, že je chráněno heslo při spojení, ale i po skončení vzdálené session.

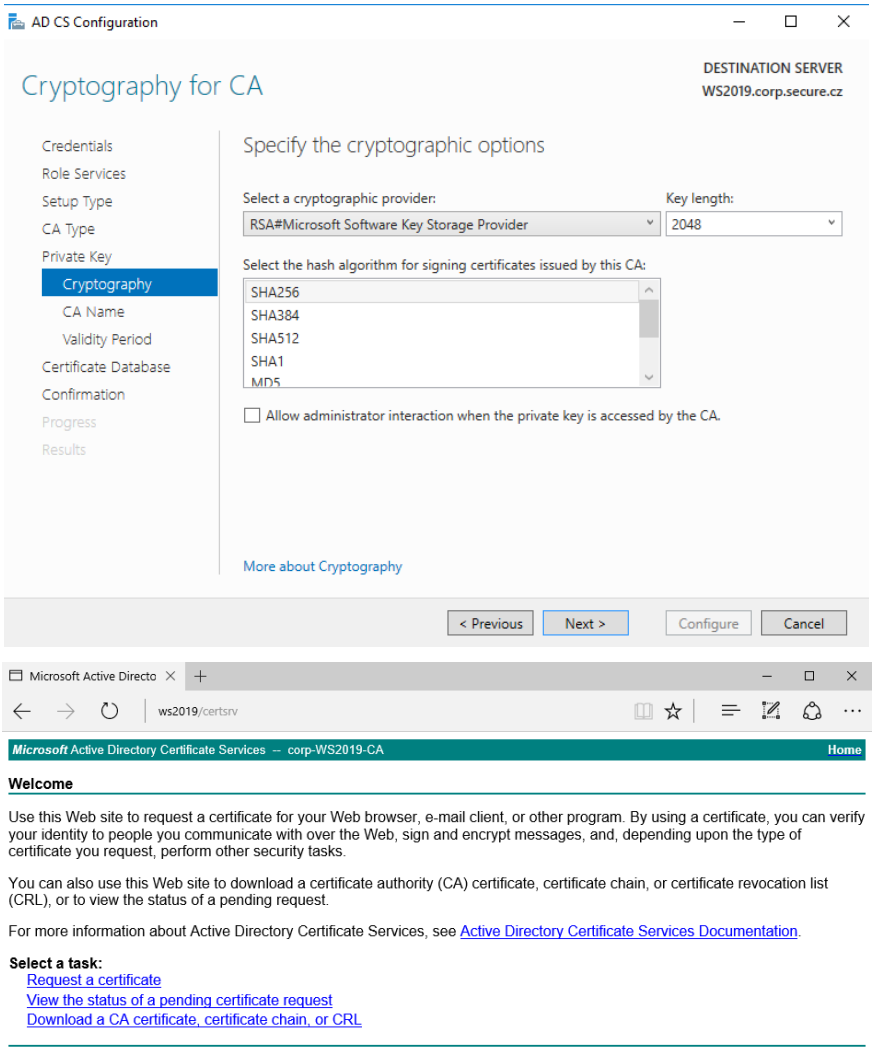
```
reg add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v
DisableRestrictedAdmin /d 0 /t REG_DWORD
```

Pro další zabezpečení komunikace bude v prostředí LAN ošetřeno LDAP, které je mezi klientem a serverem defaultně nešifrováno (např. oproti Kerberos, který má své vlastní šifrování). Na obrázku č. 11, je vidět test spojení se serverem na portu 689 bez nakonfigurovaného SSL. Chyba říká, že certifikát obdržený z připojeného serveru byl vydán nedůvěryhodnou certifikační autoritou. Pokud přidáme certifikační autoritu, díky SSL/TLS získáme důvěrné a bezpečné spojení (LDAPS).



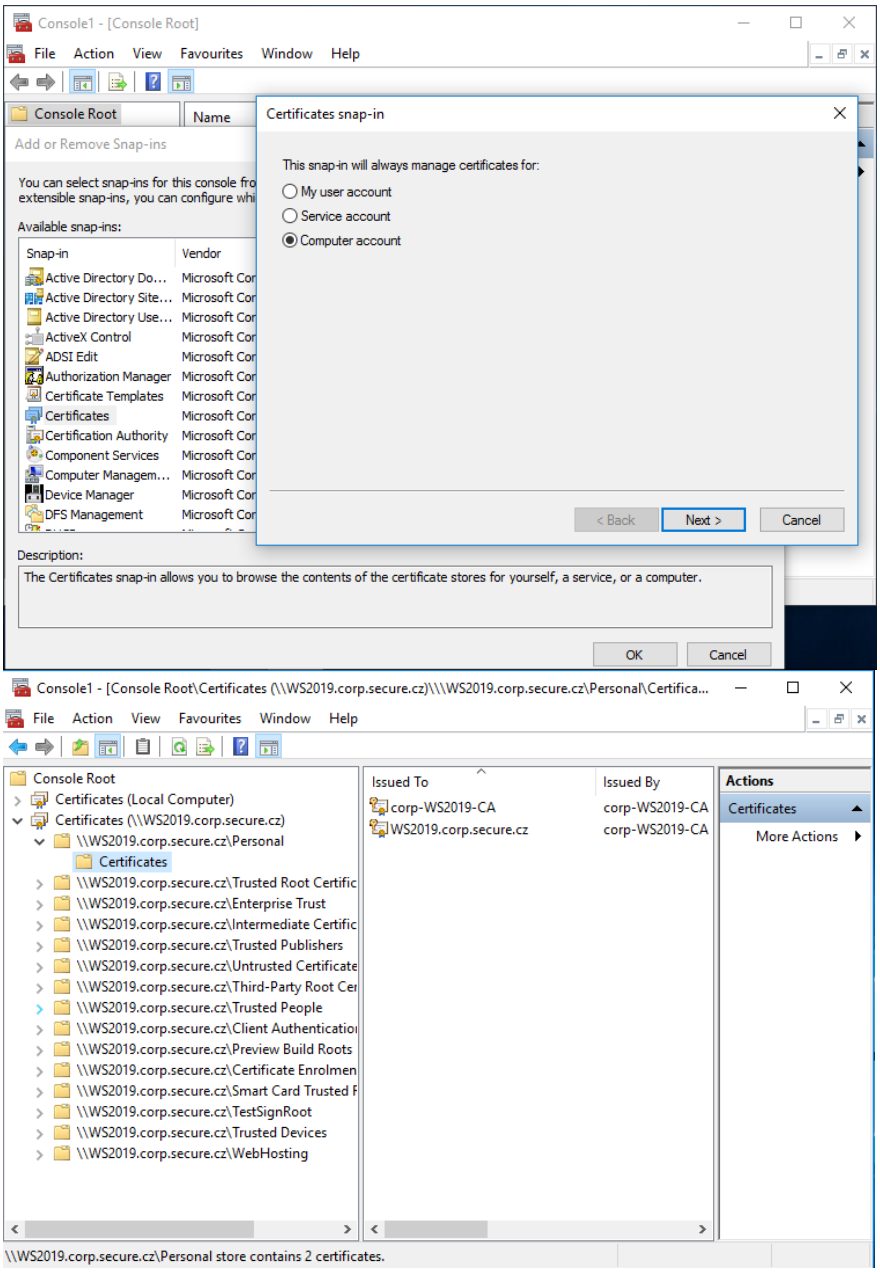
Obr. 11: Komunikace LDAP na portu 689
Zdroj: vlastní zpracování

Vyžadována je instalace certifikační autority na doménový řadič, přes který se bude komunikace ověřovat. Z důvodu přehlednosti byla služba AD CS nainstalována vzdáleně přes Server Manager ze stanice Win10. K samotnému AD CS byla přidána role Certification Authority a Certification Authority Web Enrollment, po tomto kroku je v průvodci oznámeno, že na serveru musí být nainstalována i role webového serveru IIS. Umožníme tak získávání certifikátů přes protokol HTTPS. Instalaci provedeme rovnou v průvodci, anebo použijeme krátký powershell cdmlet pro instalaci IIS přímo na serveru. Instalací vytvoříme nový soukromý klíč pro lokální certifikační autoritu a vybereme způsob šifrování, jak je vidět na obrázku č.12. V druhé části obrázku si můžeme všimnout, že o certifikáty lze žádat i přes webový prohlížeč po zadání https://<CA-server>/certsrv.



Obr. 12: Instalace AD CS a použité šifrování
Zdroj: vlastní zpracování

Pokračujeme otevřením Certificate Templates Console, ve které ověříme, že nechybí template Server Authentication (Object Identifier 1.3.6.1.5.5.7.3.1), jež je nejdůležitější pro konfiguraci LDAPS.

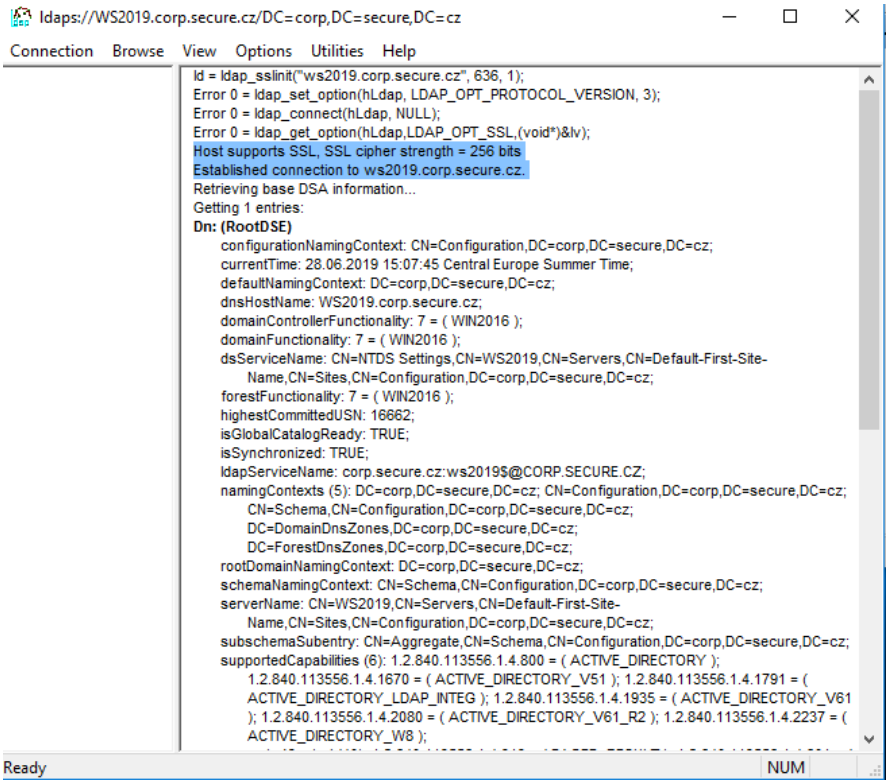


Obr. 13: Microsoft Management Console, přidané templates pro počítač i server
Zdroj: vlastní zpracování

Po spuštění Microsoft Management Console (mmc) přidáme templates pro server (Action > Add or Remove Snap-ins), jak je znázorněno na obrázku č. 13. Šablony se přidají do složky Personal\Certificates. Klikneme na složku pravým tlačítkem a vybereme Request New Cerfiticate. V průvodci se dostaneme do části, kde vybíráme Active Directory Enrollment Policy, kde žádáme o typ certifikátu – pro server zvolíme

Domain Controller. Jelikož používáme veřejný certifikát, nemusíme ho exportovat z řadiče a importovat do zařízení.

Nakonec restartujeme stanice a znovu otevřeme konzoli ldp a připojíme se. Na obrázku č. 14 je znázorněno, že certifikační autorita je potvrzena a nyní se používá LDAPS.



Obr. 14: Komunikace LDAPS na portu 636
Zdroj: vlastní zpracování

12.8 Containers

Jak bylo zmíněno v dřívější části práce, kontejnery mají největší využití v oblasti vývoje aplikací, proto uplatníme jejich výhody i v této práci. Jako první nainstalujeme na server WS2016 samotnou funkci pro podporu kontejnerů:

```
Add-WindowsFeature Containers -IncludeAllSubFeature -
IncludeManagementTools
Restart-Computer
```

K chodu je ale potřeba nainstalovat i samotný Docker. Po potvrzení cdmletu povolíme i stažení balíčku NuGet.

```
Install-Module -Name DockerMsftProvider -Repository PSGallery -
Force
Install-Package -Name docker -ProviderName DockerMsftProvider
Restart-Computer -Force
```

Nyní je server připraven pro stažení prvního image pro kontejner. V této části se v dosavadním řešení objevil zásadní problém. Po spuštění stahování image pro kontejnery se pokaždé objevila chyba, která nám nedovolila stáhnout požadovaný image. Přestože Microsoft inzeruje, že verze Windows Server 2016 umí pracovat s kontejnery, nainstalovaný operační systém neměl dostatečnou funkcionalitu, přestože dle dokumentace Windows container version compatibility (Microsoft, 2019, cit. 2019-4-5) je jisté, že by ji mít měl. Proběhlo několik pokusů, jak zprovoznit kontejnery na WS2016, nicméně se vždy objevila chyba:

```
failed to register layer: re-exec error: exit status 1: output:
ProcessBaseLayer
C:\ProgramData\Docker\windowsfilter\a6fc4e13d0fb4a8ae116d0d3400b67
81408383cd1aa4050ce23fc49b1d651eaa: The parameter is incorrect.
```

Bylo vyzkoušeno několik různých parametrů k příkazu `docker pull`, bylo prohledáno celé úložiště, že kterého se image stahovalo. Verze Dockeru byla správná, přepínání mezi Windows/Linux verzemi kontejnerů nepomohlo (parametr OS/Arch), stejně tak nefungovalo přepnout Docker do Experimental modu (sandbox, který se nepoužívá v produkčním prostředí). Vypnuta byla i funkcionalita BitLockeru. Žádný update (Revision number patching) nevyřešil chybu. Stejná chyba se nedala nijak obejít ani jinou konfigurací virtuálního stroje.

Při instalaci kontejnerů je nejdůležitější sledovat Kernel Version (`docker info`) a informace v příkazu `docker version`, kdy pro Kernel Version: 10.0.17763.504 musíme při stahování image zadat správný tag :1809. Podmínkou u Windows kontejnerů je to, že kontejner se zvoleným image lze spustit pouze na určité verzi Windows. Na hostiteli Windows Server 2016 nelze spustit kontejnery s image s hostelem s Windows Server verzí 1709. Jediným způsobem je používat Hyper-V kontejnery (Hyper-V izolaci, spustit docker kontejner s parametrem `--isolation=hyperv`), která nám dovolí na novějším vydání (např. Windows Server verze 1709 nebo 1803) spustit image ze starší verze (např. Windows Server 2016). Jelikož je ale Windows Server 2016 první OS, který zavádí Windows kontejnery, Hyper-V izolace by nevyřešila problém s kompatibilitou. Kompatibilita s buildem

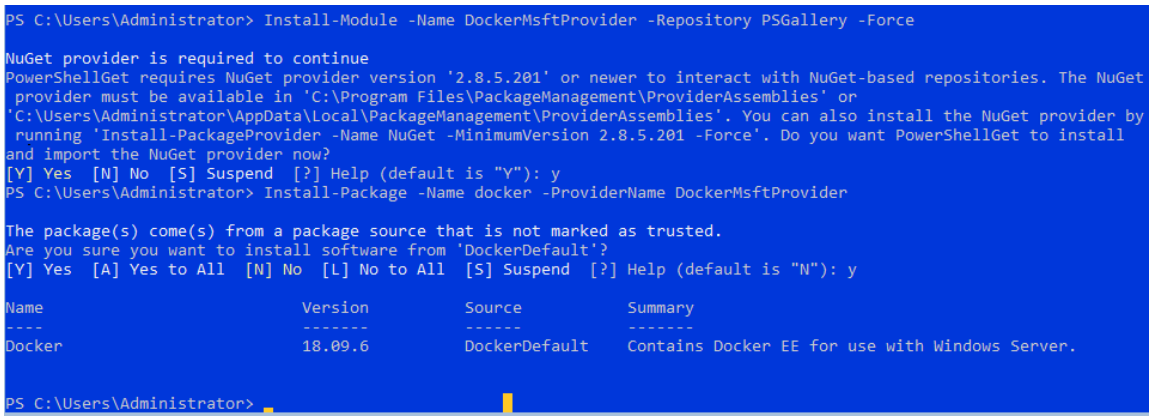
a stahovaným image je nejspíš problém, proč se objevovala chyba, a přestože proběhlo několik pokusů, jak chybu obejít, nepodařilo se docílit stažení image.

12.9 Containers - Windows Server 2019

Přes počáteční potíže s kompatibilitou stahovaných images, bylo rozhodnuto, že v práci bude použit systém Windows Server 2019, který byl představen v druhé polovině roku 2018. Nabízí stejné možnosti jako Windows Server 2016 a přidává některé nové funkcionality navíc. Místo virtuální serverové stanice WS2016 byla vytvořena nová, která byla pojmenována WS2019.

Další verze OS od Microsoft pokračuje v trendu zlepšování bezpečnosti a soustředí se na podporu hybridního cloudu. Změny, které ovlivní tuto práci, se týkají hlavně kontejnerů – images pro WS2019 jsou znatelně menší a nyní lze provozovat Windows a Linux kontejnery na jednom hostiteli zároveň (pod stejným Docker procesem). Rozdíl v konfiguraci byl ten, že na WS2016 a stanici Win10 byl zakázán protokol SMBv1 (Programs and Features > Turn Windows features on or off > SMB 1.0/CIFS File Sharing Support, nebo vyhledat parametr v registrech), který byl zmíněn v praktické části práce. Ve WS2019 už ale protokol není defaultně k dispozici. Stejně tak příkaz `Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2` už pro WS2019 nebyl potřeba.

Na druhou stranu, i když některé funkcionality již nemají podporu, nejedná se o ty, které byly doteď využity pro potřeby této práce. Instalace a konfigurace Windows Server 2019 ve verzi Core se od Windows Serveru 2016 v podstatě téměř neliší. Cdmlety pro Powershell fungují a zajišťují stejnou funkčnost pro služby Active Directory DC, DNS nebo DHCP. S instalací kontejnerů tentokrát nebyl problém, jak znázorňuje obrázek č. 15, zvolený image se stáhl bez problémů. V další části práce bude popsáno, jak kontejnery spouštět a komunikovat s nimi v LAN.



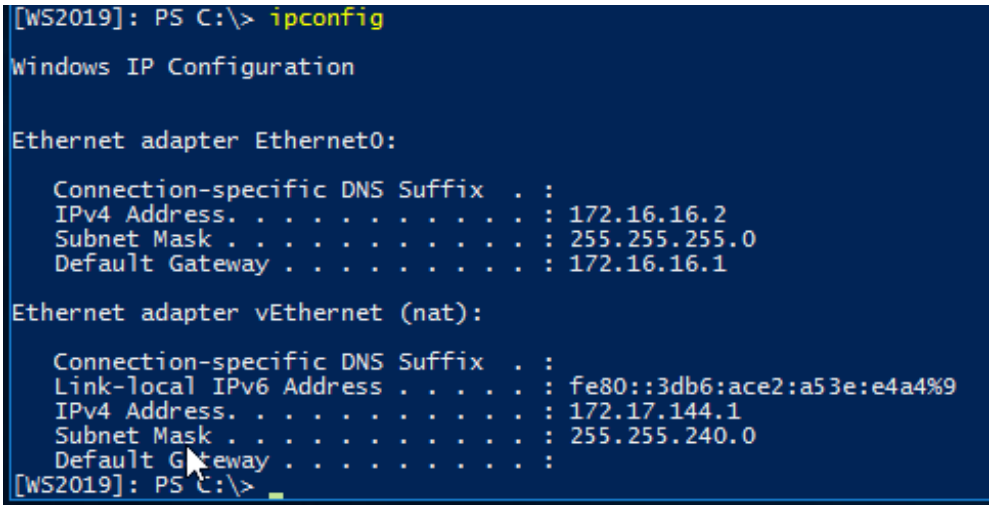
Obr. 15: Instalace Dockeru na Windows Server 2019
Zdroj: vlastní zpracování

S kontejnery lze pracovat pomocí Powershellu nebo Dockeru, jež nabízí i uživatelské rozhraní. Na uživatelích v LAN pak bude rozhodnutí, jaký způsob zvolí, v této práci použijeme způsob správy pomocí Powershellu.

V minulé kapitole byly na klientské stanici Win10 nainstalovány nástroje pro vzdálený přístup, na serveru povoleny firewall pravidla a otestováno vzdálené připojení. Přes lokální Powershell otevřeme session komunikující se serverem WS2019.

```
$session = New-PSSession -ComputerName WS2019 -Credential
Administrator
Enter-PSSession -Session $session
```

Systém se zeptá na heslo k účtu Administrator, popřípadě se můžeme vzdáleně přihlásit na účet ze skupiny Developers nebo na účet DomainSecure, záleží na tom, co chceme přes vzdálený přístup ovládat. V následující kapitole budou omezeny příkazy pro skupinu Developers. Na obrázku č. 16 je vidět, že jsme připojeni k počítači WS2019 a přes ipconfig vidíme staticky přidělenou adresu 172.16.16.2. Je zde také vidět, že po instalaci služby pro kontejnery byl vytvořen defaultní virtuální switch (nat) 172.17.144.1.



Obr. 16: Vzdálená session a virtuální switch vEthernet NAT
Zdroj: vlastní zpracování

Nyní už jde vytvořit kontejner ze základního image a připojit ho ke switchi. Do kontejneru lze vytvořit session, stejný princip jako když se připojujeme ke vzdálenému počítači nebo k virtuálnímu stroji, přes kterou můžeme tvořit jeho podobu. Necelý rok po vydání Windows Server 2016 cdmlety pro ovládání kontejnerů přestaly být validní a nyní jsou deprecated (`-Module Containers`) – vše se ovládá pomocí Docker cli (docker.exe) nebo přímo pomocí příkazů v knihovně Docker.DotNet. Více informací na (Microsoft, 2016, cit. 2019-2-4).

```
docker pull mcr.microsoft.com/windows/nanoserver:1809
docker run -it -p 800:800 <ID nebo jméno image>
```

Stáhneme předpřipravený image s nainstalovanou službou IIS, jak je vidět na obrázku č. 17, nebo obyčejný image Nano serveru, do kterého bychom potřebné funkcionality doinstalovali. Spustíme stažený kontejner (`docker run`) v LAN a namapujeme na porty 800:800, <port hostitele kontejneru>:<port pro vstup do daného kontejneru>. V síti pouze musíme dávat pozor, jestli některý z portů již není obsazený jiným procesem nebo není blokován pravidlem firewallu. O zbytek se už postará virtuální switch vEthernet NAT, ke kterému se vytvořený kontejner automaticky připojí. Cílové porty jsou zobrazeny i na obrázku č. 18, kde v tabulce najdeme ID kontejneru, z jakého vychází image, název spuštěné služby uvnitř, kdy byl vytvořený a jak dlouho běží, obsazené porty a jméno kontejneru (pozn. pokud v příkazu nepoužijeme parametr `-Name`, docker jméno automaticky vygeneruje, např. `objective_fermat`).

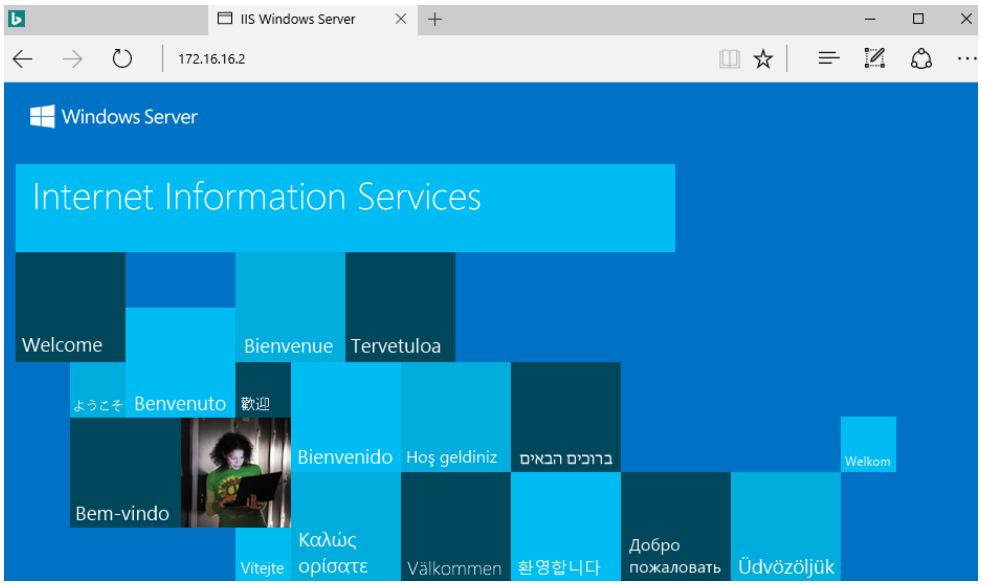
Po přihlášení na stanici Win10 ve webovém prohlížeči vložíme adresu buď samotného kontejneru (řešení adresy pro každý kontejner budou muset používat vývojáři, aby spouštěli pouze jeden konkrétní kontejner), nebo hostitelského počítače, jak je vidět na obrázku č. 19.

```
PS C:\Users\Administrator> docker pull mcr.microsoft.com/windows/servercore/iis:windowsservercore-1803
windowsservercore-1803: Pulling from windows/servercore/iis
d9e8b01179bf: Pull complete
2de32ee3b543: Pull complete
da5e0e982087: Pull complete
6754663f2c2b: Pull complete
3509d7ab4421: Pull complete
Digest: sha256:3be100fea167ebd04b724436a0fa3ee38c420d80e3854930bce5c26d05ee2ac5
Status: Downloaded newer image for mcr.microsoft.com/windows/servercore/iis:windowsservercore-1803
PS C:\Users\Administrator>
```

Obr. 17: Stažení image s IIS
Zdroj: vlastní zpracování

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>docker container ls
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS
  PORTS                         NAMES
87a5277c1d64        eb5ed1259d88        "C:\\ServiceMonitor.e…"   About an hour ago   Up About an hour
  80/tcp, 0.0.0.0:800->800/tcp   objective_fermat

C:\Users\Administrator>docker info
Containers: 2
 Running: 1
 Paused: 0
 Stopped: 1
Images: 3
Server Version: 18.09.7
Storage Driver: windowsfilter
 Windows:
Logging Driver: json-file
Plugins:
 Volume: local
 Network: ics l2bridge l2tunnel nat null overlay transparent
 Log: awslogs etwlogs fluentd gelf json-file local logentries splunk syslog
Swarm: inactive
Default Isolation: process
Kernel Version: 10.0 17763 (17763.1.amd64fre.rs5_release.180914-1434)
Operating System: Windows Server 2019 Datacenter Evaluation Version 1809 (OS Build 17763.379)
OSType: windows
Architecture: x86_64
CPUs: 4
Total Memory: 1.999GiB
Name: WS2019
```

Obr. 18: Výpis spuštěných kontejnerů na stanici WS2019 a stažených images
Zdroj: vlastní zpracování



Obr. 19: Kontejner s IIS spuštěný z klientské stanice Win10
Zdroj: vlastní zpracování

Jedním způsobem, jak tvořit kontejner, je přes jednotlivé docker příkazy. V další části ale rozebereme způsob s Dockerfile, kdy vytvoříme textový soubor s jednoduchým skriptem a seznamem příkazů, který sestaví kontejner najednou. Dockerfile je potom zahrnut do složky s celou aplikací a struktura může být ovládána z vývojového prostředí (např. Visual Studio).

```
FROM
   mcr.microsoft.com/windows/servercore/iis
      :windowsservercore-ltsc2019
LABEL maintainer="lenydeveloper@secure.cz"

RUN mkdir C:\testApp
RUN powershell -NoProfile -Command \
   Import-Module IISAdministration; \
   Install-WindowsFeature NET-Framework-45-ASPNET; \
   Install-WindowsFeature Web-Asp-Net45; \
   New-IISSite -Name "MyApp" -BindingInformation "*:80:" -
PhysicalPath C:\testApp -PassThru

EXPOSE 80

ADD bin/ /testApp
```

Po spuštění se vytvoří přímo v kontejneru složka `C:\testApp`, do které se budou ukládat soubory pro testovací aplikaci. Celý kontejner bude založen na základním image, který si můžeme stáhnout předem nebo image dostaneme z Docker Hub pomocí `FROM <image>`. Microsoft nedávno zakázal defaultní tag :latest, který se doplňuje za cestu k image pokaždé, když ji přímo nespecifikujeme. Vyvarujeme

se tak scénáři, kdy stáhneme rozdílný image, než je přesná verze našeho systému (Microsoft, 2019, cit. 2019-4-4). Zvolíme správný tag k image skládající se z komponent důležitých pro vytvoření webového serveru (IIS).

Příkazem `RUN powershell` otevřeme Powershell relaci (s parametrem `–NoProfile`, ten zajistí očekávané chování a nespustí neznámé Powershell profily), do té pak vložíme služby, které bude kontejner a aplikace v něm poskytovat. Za každým příkazem v Dockerfile vložíme znak "\", jak vyžaduje syntaxe. Nainstalujeme .NET Framework a ASP.NET 4.5 společně s nástroji pro ovládání IIS (`Import-Module IISAdministration`). Z modulu IISAdministration použijeme příkaz `New-IISSite`, abychom vytvořili novou website z určené složky na portu 80. Pomocí EXPOSE Dockeru oznamujeme, na jakém portu má přijímat požadavky, samotný příkaz ale zatím port neotevírá. Instrukce ADD přidává soubory do složky v kontejneru – v tomto případě vezme kompletní složku bin/ z adresáře, ve kterém je i Dockerfile, a přidá ji do /testApp v kontejneru. V této složce byl připravený jednoduchý index.html s kódem pro webovou aplikaci ("Hello World from container!"). Nyní se přes Powershell přesuneme do složky, kde je uložený Dockerfile a spustíme příkaz:

```
docker build .
```

Začne se stahovat image z Docker Hub a instalovat se všechny funkcionality, které jsme definovali. Mezitím v lokálním prostředí můžeme otevřít webovou stránku s aplikací (http://172.16.16.2/index.html), jak bylo zobrazeno dříve.

12.9.1 Doporučení pro implementaci Docker Windows Containers

Následující podkapitola shrnuje subjektivní názor a doporučení autora práce.

Při prvních implementacích Windows kontejnerů se vyskytly problémy s kompatibilitou, které byly popsány výše. Odborná internetová fóra byla plná užitečných rad a návodů, jak kontejnery zprovoznit a autor práce nebyl jediný, kdo narazil na popsané problémy. Přestože se nakonec podařilo dotáhnout návrh s kontejnery do přijatelné podoby, na stejných odborných fórech bylo problematické najít další řešení, které by tuto práci rozvíjelo. Jednou z nevýhod je i nedostatečná nabídka školení Windows kontejnerů, gopas.cz ani root.cz neposkytuje vhodný kurz pro budoucí vývojáře a pokud ano, jedná se pouze o zmínky nebo úplné začátky.

Což může být zapříčiněno i malou poptávkou. Pro vývojářskou firmu to ale znamená nízkou možnost rozvoje v této oblasti. Pro příklad by bylo potřeba, aby se vývojáři webových aplikací ve firmě naučili s Docker platformou a uměli ji ovládat na své stanici (např. přes Visual Studio Tools for Docker), než budou moci spouštět a testovat kontejnery i na firemním serveru.

Naopak krokem vpřed je od Microsoft zrušení příkazů pro kontejnery, což znamená, že je lze ovládat jen jedním způsobem přes docker.exe. Je ale diskutabilní, jestli prokazatelné klady z implementace Windows kontejnerů převažují jeho zápory.

Velkou mezerou v bezpečnosti se zdá stahování neznámých image z Docker Hub. Jak je vidět na obrázku č. 15, už při stahování samotného modulu Docker jsme upozorněni, že balíček nepochází z důvěryhodného zdroje. Je otázkou, jak moc jsou images z Docker Hub bezpečné a jak je ověřovat. Samotné ověřování integrity images je defaultně vypnuté dle oficiální dokumentace (Docker docs, cit. 2019-29-6). Údržba kódu uvnitř kontejnerů je kritickým bodem v bezpečnosti, pouhá kontrola při prvotním nasazení nestačí a je potřeba se o obsah aktivně zajímat, aby se nezvyšovalo riziko objevení tzv. backdoor. Dalším řešením se zdá vytvořit si vlastní podpisy, které by byly připojeny ke každému image. Vlastnoručně podepsaný image by se nahrál na soukromé úložiště nebo cloud, odkud by se stahoval na hostitele kontejnerů v LAN. Toto řešení bude v pokračující práci přezkoumáno.

Zdůrazněna musí být i komunikace mezi hostitelem kontejnerů (WS2019) a připojování k němu přes přístupové porty. Jak bylo zmíněno, tyto porty jsou popsány v dokumentu docker-compose.yml a musí být dohledatelné, které jsou používány a které nesmí být otevřené. Před nasazením do produkčního řešení budou muset probíhat autentizační testy přes firewall pravidla, aby se předešlo obcházení autentizačních mechanizmů a neautorizovaným změnám kódu.

Kontejnery ze své podstaty obsahují vyšší riziko pro napadení než virtuální stroje. Snížit toto riziko lze tak, že umístíme kontejner na virtualizované prostředí a zařídíme tak o stupeň vyšší izolaci na úkor většího zatížení. Bude potřeba proškolit vývojáře nejen o zacházení s Dockerem, ale i ohledně bezpečném zacházení s ním, což zabere další čas a finanční prostředky.

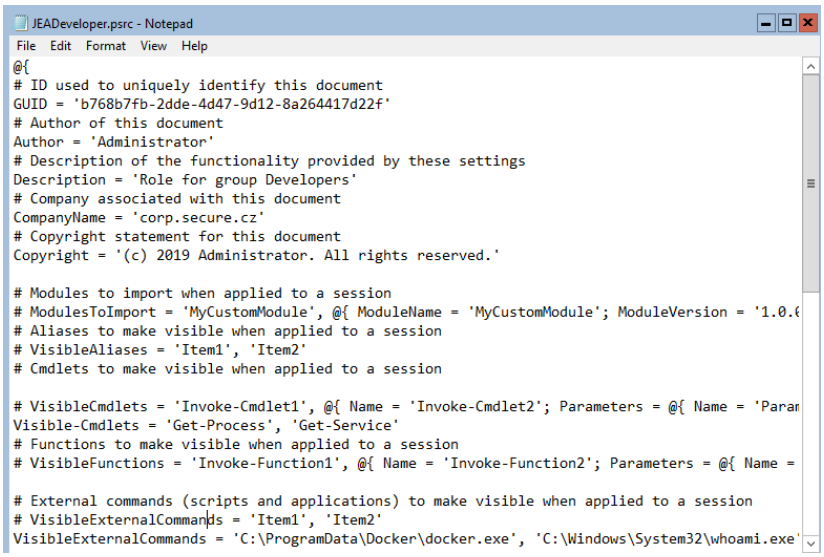
12.10 Just Enough Administration

Přestože můžeme používat vzdálený přístup, jehož komunikace probíhá šifrovaně, musí být zakázáno přistupovat do domény s neznámým zařízením, které není komplexně zabezpečeno jako ostatní počítače v síti. Dalším problémem je, když IT pracovník používá jeden účet pro všechny účely práce. Pokud používá účet s administrátorskými právy zároveň i pro prohlížení obyčejných mailů nebo stahování různého kontextu na pracovní stanici. Proto je potřeba zařídit, aby IT pracovník používal několik účtů s různými právy pro určité pracovní úkony. Na druhou stranu se může stát, že pracovní stanice je nakažena škodlivým softwarem, i když jsme přihlášeni na obvyklý účet bez administrátorských práv, později je na stejnou stanici přihlášen účet, který administrátorská práva vlastní a vystavujeme se tak potencionální hrozbě pro celou doménu. Problému se dá alespoň částečně předejít pomocí Just Enough Administration.

V kapitole o politikách zásad byla možnost zakázat přístup do Powershellu a cmd.exe, ale jelikož uživatelé v LAN budou někdy muset spolupracovat se serverem, na kterém jsou spuštěny kontejnery, je vhodnější pouze omezit rozsah cdmletů, které budou mít k dispozici. JEA se použije tehdy, když je potřeba definovat, co může uživatel nebo skupina měnit přes Powershell session. Pro JEA není nutné instalovat žádné služby navíc, ve Windows Server 2016 (a také ve Windows Server 2019) je služba povolena defaultně. Dokumentace Microsoft pouze silně doporučuje zapnout na pracovních stanicích zásady Turn on Module Logging a Turn on PowerShell Script Block Logging, díky kterým je zajištěno, že uživatelem spuštěné příkazy jsou zaznamenány a sledovány.

Vytvoříme složku JEAFeature, do které budou vloženy všechny potřebné konfigurační soubory – jako první prázdný Powershell module soubor a k němu manifest. Ve složce RoleCapabilities bude soubor .psrc s přesně definovanými příkazy a programy, které uživatel může používat v session. Soubor JEADeveloper.psrc otevřeme v notepadu, jehož prvotní stav s nápovědou syntaxe je ukázán na obrázku č. 20.

```
New-Item -ItemType File -Path '.\JEAFeature.psm1'
New-ModuleManifest -Path '.\JEAFeature.psd1' -RootModule
"JEAFeature.psm1"
New-PSRoleCapabilityFile -Path
'.\RoleCapabilities\JEADeveloper.psrc'
```



Obr. 20: Soubor pro definování příkazů JEA
Zdroj: vlastní zpracování

Nemusíme definovat pouze cdmlety, ale i jejich parametry, anebo povolení spouštět předpřipravené skripty nebo funkce. Přes notepad přidáme řádky:

```
VisibleCmdlets = 'Get-Process', 'Get-Service'
VisibleExternalCommands = 'C:\ProgramData\Docker\docker.exe',
'C:\Windows\System32\whoami.exe'
```

Pro roli Developer bude tedy povolen hlavně Docker (např. pro jinou roli bychom mohli povolit gpupdate.exe a gpresult.exe). Nyní je potřeba zařadit uživatele v připojené session, kteří budou mít roli Developer. Tento modul díky parametru `RestrictedRemoteServer` povolí uživateli v dané session použít pouze příkazy `Exit-PSSession`, `Get-FormatData`, `Get-Help`, `Measure-Object`, `Out-Default` a `Select-Object`. V následujícím bloku kódu je příkaz pro vytvoření souboru a řádky přidané do souboru DeveloperSession.pssc.

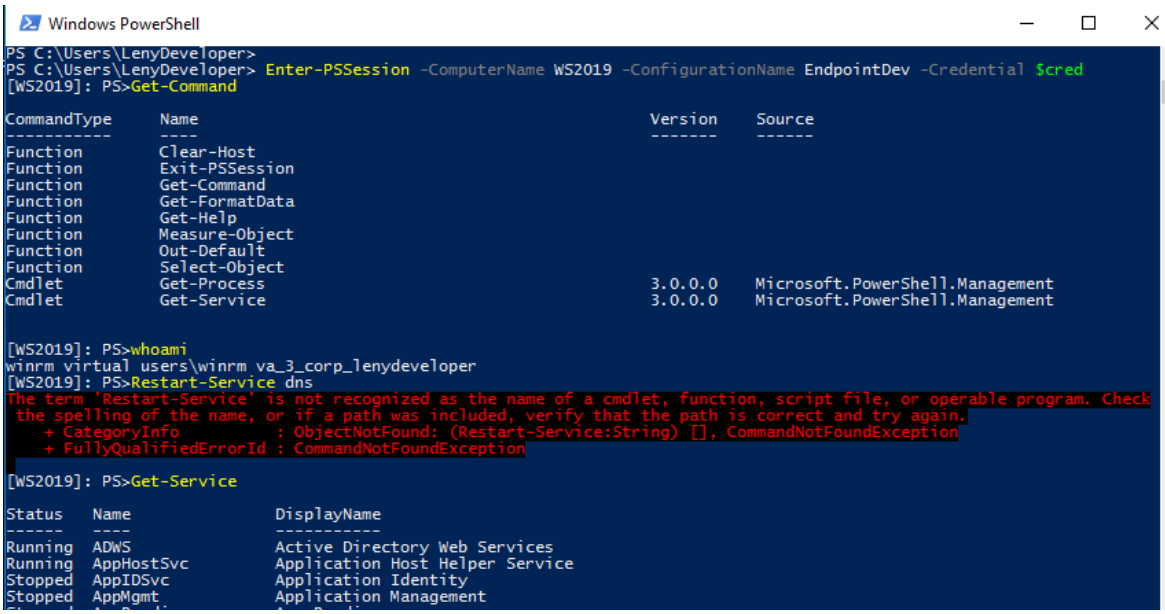
```
New-PSSessionConfigurationFile -SessionType RestrictedRemoteServer
-Path '.\DeveloperSession.pssc'

Description = 'Endpoint for Docker Developers'
#Zaznamenává příkazy spuštěné v session >
TranscriptDirectory = 'C:\JEA\Transcripts\'
RunAsVirtualAccount = &true
RunAsVirtualAccountGroups = 'Developers'
RoleDefinition = @{ 'CORP\Developers' = @{ RoleCapabilityFiles =
'C:\JEA\RoleCapabilities\JEADeveloper.psrc' }; }

Test-PSSessionConfigurationFile -Path '.\DeveloperSession.pssc'
Register-PSSessionConfiguration -Path '.\DeveloperSession.pssc' -
Name EndpointDev -Force
```

Následně je konfigurace session otestována a po navrácení hodnoty 'True' (zn. správná syntaxe v konfiguraci) zaregistrována jako endpoint JEAEndpoint1. Objeví se upozornění o restartu služby WinRM, po kterém začne být vše funkční. Je potřeba zajistit přes group policy, aby uživatelé ve skupině Developers neměli administrátorská práva a nemohli pravidla JEA obejít.

Po přihlášení uživatele ze skupiny Developers (např. uživatel LenyDeveloper, jehož vytvoření bylo popsáno v dřívější kapitole) ke stanici Win10 zapneme Powershell, přes který vytvoříme session na WS2019. Vytvořená skupina se nemůže k serveru dostat jinak, než že použije endpoint EndpointDev. Vzdálená session:

```
$credential = Get-Credential
Enter-PSSession -ComputerName WS2019 -ConfigurationName
EndpointDev -Credential $credential
```

Session projde a po zadání cdmletu Get-Command vidíme použitelné příkazy pro tohoto uživatele. Pokud použije jakýkoli příkaz, který není na seznamu, vrátí se chyba, kterou vidíme na obrázku č. 21. Neprojde ping, pouze whoami a práce s příkazem docker. Na obrázku je vidět i spuštěná session na server WS2019 a povolené příkazy, které se můžou vždy změnit v souboru JEADeveloper.psrc. Navíc se všechny příkazy použité uživatelem ukládají do složky C:\JEA\Transcripts.



Obr. 21: JEA session s povolenými příkazy

Zdroj: vlastní zpracování

Nová funkcionalita JEA pomáhá administrátorům specifickou cestou určovat, co přesně se může na serverech v síti ovládat. Tento způsob jde nastavit pouze přes Powershell, jiný způsob není (např. přes GUI).

12.11 BitLocker, Secure Boot a Credential Guard

Aby návrh LAN splnil bezpečnostní požadavky, data na pevných discích klientských stanicích budou šifrována. BitLocker Drive Encryption nemusí ale sloužit pouze pro klientské stanice, k dispozici je i pro Windows Servery. BitLocker je potřeba nainstalovat jako feature:

```
Add-WindowsFeature BitLocker -IncludeAllSubFeature -
IncludeManagementTools –Restart
```

Ve virtualizovaném prostředí bylo složité zprovoznit funkcionalitu, protože se nepodařilo ověřit komponentu TPM a tím ani zašifrovat daný disk (pomocí příkazu `Enable-BitLocker`). V produkčním prostředí by už neměl být se správným HW problém data zašifrovat – na Windows Server 2016 i na stanicích s Windows 10.

Na úplném začátku instalace Windows Serveru 2016 a Windows 10 se funkcionalita Secure boot nepodařila spustit – operační systém nenastartoval z UEFI a virtuální stroj se nespustil. Potíže byly znovu způsobeny virtualizovaným strojem ve VMware, samotný testovací notebook s virtualizovanou infrastrukturou splňoval

všechny požadavky popsané v oficiální dokumentaci pro zprovoznění Secure boot. Funkcionalitu by bylo možné zkusit pouze v připravovaném produkčním prostředí.

I kdyby byla funkce Secure boot zprovozněna, nelze na ni navázat funkcí Windows Defender Credential Guard z toho důvodu, že funkce není podporována na serverech s rolí doménového řadiče. Credential Guard chrání údaje uložené v LSASS vrstvě, nikoli databázi SAM s uživatelskými hesly, ke které se může dostat pouze uživatel s administrátorskými právy. Takový uživatel již povolení získal, funkcionalita Credential Guard tedy není potřeba – důležité je ochránit přístupová práva samotných uživatelů.

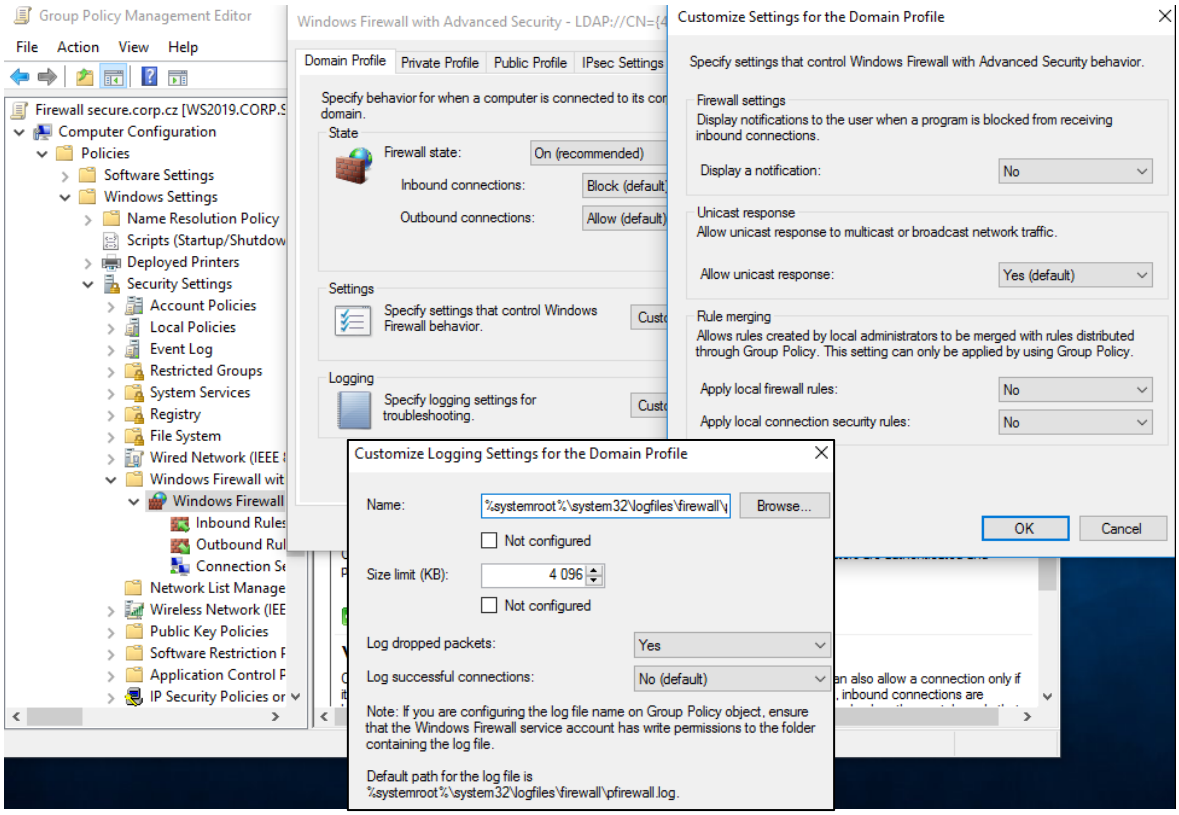
12.12 Windows Firewall

Zajistit antivirový a antimalware program na každou uživatelskou stanici zapojenou v LAN, je nutností. Microsoft nabízí jako své řešení Windows Defender, který se zdá být dostačující. Důležitý je ale i firewall, který řídí síťovou komunikaci v LAN. Ve Windows Server 2016 (a také Windows Server 2019) je Windows firewall defaultně zapnutý s předpřipravenými pravidly, které povolují odchozí komunikaci přes jakýkoli port, ale filtrují komunikaci příchozí. Firewall rozlišuje tři druhy profilů, dle toho, v jaké síti se připojíme, všechny tři profily zůstanou zapnuté – domain, private a public. Na počítač připojený v síti LAN se vztahují pravidla v profilu domain.

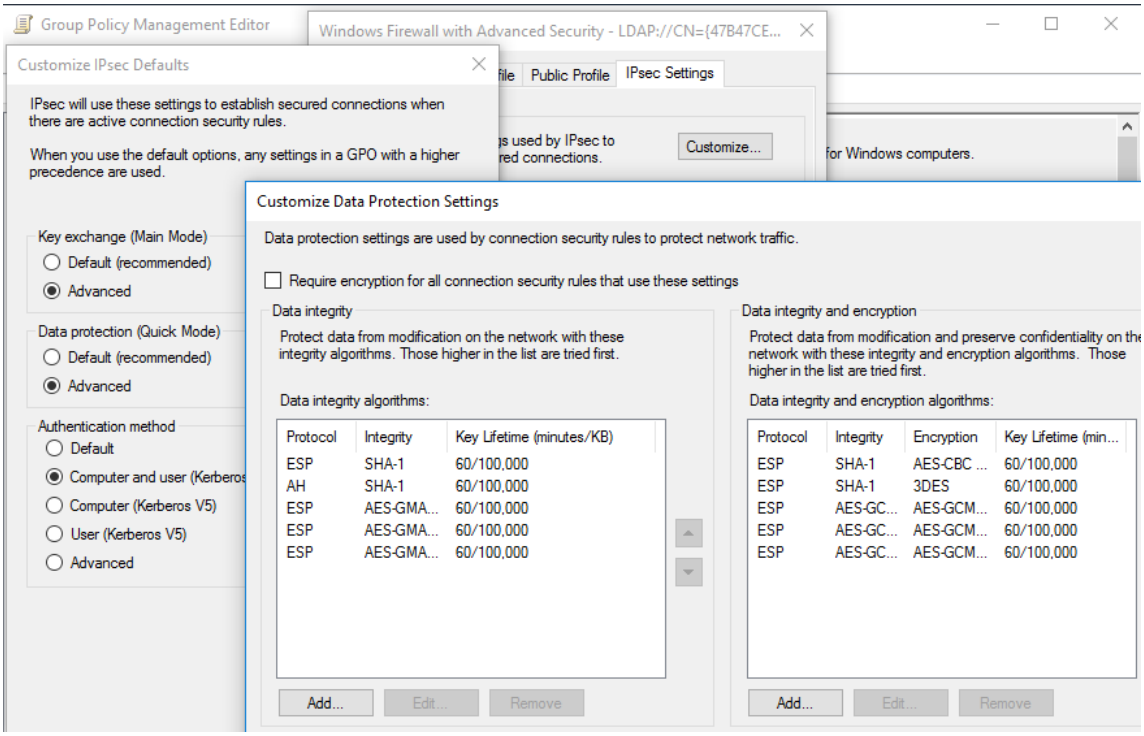
Pravidla Windows Firewall with Advanced Security lze nastavovat lokálně na každé stanici, centralizované a rychlé řešení ale vede přes pravidla v Group Policy. Vytvoříme nové GPO s názvem Firewall corp.secure.cz v Group Policy Management, do kterého budou vložena všechna nová firewall pravidla. Přes Edit se dostaneme do editoru Group Policy, kde vyhledáme seznam pravidel (Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Inbound/Outbound Rules). V hlavním nastavení firewallu je potřeba ignoroval lokální nastavení firewallových pravidel, aby je samotný uživatel nemohl měnit (Apply local firewall rules: No), jak je vidět na obrázku č. 22.

V nastavení IPSec zvolíme adekvátní šifrování, které je účinné a zároveň nezatěžuje provoz – vyhneme se šifře DES a MD5, použijeme Diffie-Hellman. V IPsec

použijeme pouze silné šifry a protokoly, pro autentizaci uživatelů a počítačů použijeme Kerberos, jak je zachyceno na č. 23.



Obr. 22: Hlavní nastavení firewallu
Zdroj: vlastní zpracování



Obr. 23: Nastavení IPsec
Zdroj: vlastní zpracování

Pro Connection Security Rules vytvoříme nová pravidla pro spojení RDP (Request Authentication for Inbound and Outbound Settings, porty 5985, 5986) a WinRM (port 3389) pro všechny profily. Do Inbound Rules zabezpečíme tato spojení tunely IPSec – do pravidel pro RDP i WinRM vypíšeme důvěryhodné počítače a uživatele, kterým bude použití spojení povoleno (jedná se o administrátorské stanice, účty help-desk nebo Event Collectory). Pro WinRM budeme vyžadovat autentizaci Kerberos bez šifrování, RDP bude vyžadovat autentizaci i šifrování s kontrolou integrity. Blokovat se bude i příchozí spojení SMB na TCP portu 445.

V nastavování firewall pravidel je třeba dbát na zablokování všeho, co nepotřebujeme – povolíme pouze provoz na portech pro uživatele, kteří budou pracovat s kontejnery a stanici představující syslog server. Naopak přidáme do Outbound pravidlo o zablokování notepad.exe a vše ze složky %SYSTEMROOT%\System32 (např. wscript.exe, cscript.exe nebo regsvr32.exe), což chrání systém pokud by nastala kritická situace a zabránilo se tak úniku informací. V Outbound pravidlech povolíme komunikaci aplikací, které potřebují mít přístup do LAN, jinak defaultně není odchozí komunikace nijak filtrována.

12.13 Audit a monitoring

Firmy investují nemalé částky do šifrovacích aplikací, antivirových software a neprůstřelných firewallů, snaží se kontrolovat vše, kde se uživatel může v síti pohybovat a co může měnit. Tyto informace je ale potřeba vždy umět i zpětně dohledat.

Logování pomáhá sledovat normální i neobvyklé aktivity v systému – používání USB zařízení na serverové stanici, změna uživatelského hesla v neočekávanou dobu nebo vzdálený přístup do SAM databáze. V síti se za jednu minutu můžou stát i desítky činností, o kterých bychom měli vědět. Jelikož může objem aktivit (logů) dosahovat vysokých čísel, není v našich silách zaznamenat naprosto všechno. A přestože je logování důležité a vyžadované vyhláškou o kybernetické bezpečnosti (zn. doporučení o logování aktivit najdeme i v normách ISO 27000), stejně tak důležité je umět vybrat činnosti, které se zdají být stěžejní a jejich zaregistrováním snížit bezpečnostní riziko. Popřípadě nesledovat činnosti, ze kterých se zapisuje velké množství vstupních logů. Vyčerpávající seznam s detailním popisem všech událostí, které lze sledovat

ve Windows 10 a Windows Server 2016 je k nalezení v dokumentu Security Auditing and Monitoring Reference (Microsoft, cit. 2019-5-2).

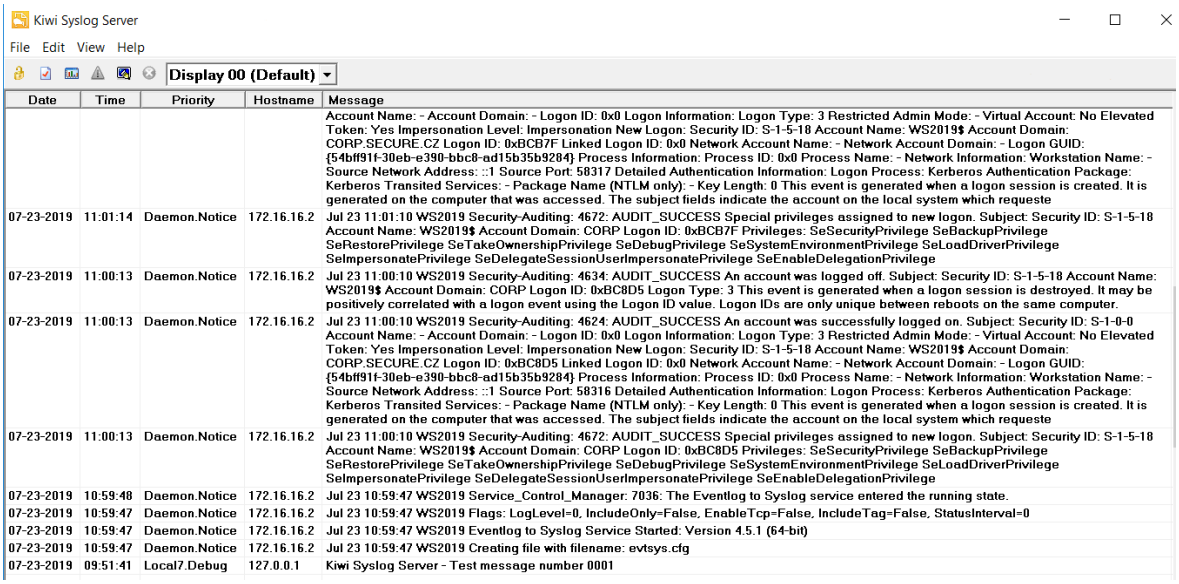
Defaultně se ve Windows logují pouze některé operace, proto se valná většina nastavuje v Audit Policy v editoru Group Policy Management. Ty se dělí na základní Audit Policy a na podrobnější Advanced Audit Policy. U všech událostí zjišťujeme, jestli byla úspěšná (Success) nebo neúspěšná (Failure), popřípadě obě možnosti najednou. Pro doménový řadič logujeme jiné události než pro klientskou stanici nebo celou doménu.

Je potřeba se přesvědčit, že pokud používáme Advanced Audit Policy, nejsou přepisována základními Audit Policy, které mají defaultně přednost (`auditpol.exe /get /category:*`). Všechny logy se zobrazují v Event Viewer, kde je lze filtrovat (např. i pomocí XML), prohledávat nebo exportovat do připravených souborů. V prostředí Windows lze nasadit na některé stanice roli Event Collector, na kterou se po konfiguraci začnou přeposílat námi zvolené události a zobrazovat v Event Vieweru. Event Collector by se stal centralizovaným místem pro vybrané logy, přeposílané ze stanic s rolí Event Log Forwarder pomoci Subscription. V prostředí LAN ale tento model bylo velmi problematické správně nakonfigurovat i podle oficiální dokumentace tak, aby se logy shromažďovaly na zvolené stanici. Z důvodu zkušeností autora práce byl proto zvolen standard syslog, který používá i program Kiwi Syslog Server od společnosti SolarWinds.

Jedná se o jednoduchou utilitu, kde se nastavují filtry a spravují logy – po určité události lze nastavit import logu do souboru, kde se zachová po danou dobu, kterou vyžaduje vyhláška o kybernetické bezpečnosti. Můžeme zvolit odeslání mailu, pokud nastane některá událost nebo rovnou spustit připravený skript. Instalace programu a nastavení pravidel je intuitivní a jednoduché, jako centrální stanice v síti bude sloužit stanice s nainstalovaným Windows 10. Kiwi Syslog Server zpracovává i SNMP Traps nebo zprávy z routerů a firewallů, defaultně naslouchá na UDP portu 514, povolit lze také zprávy TCP na portu 6514. Stejně tak dokáže používat Event Log Forwarder a po vytvoření Subscription definujeme, které zprávy se budou přeposílat (Error, Warning, Notice, Alert, aj.).

V testovací LAN byl stažen na stanici Win10 program eventlog-to-syslog, ze kterého byl použit soubor evtsys.exe. Soubor se přes PowerShell session odeslal na

WS2019 do složky Windows\System32. Nainstalujeme službu na stanici s Kiwi Syslog Server pomocí příkazu `evtsys.exe -i -h 172.16.16.21`, následně službu spustíme `net start evtsys`, aby začala přeposílat logy, jak je vidět na obrázku č. 24. Na obrázku je také vidět, že samotné přihlášení je složeno z několika logů a nemusíme je zobrazovat všechny – k tomu budou použity filtry.



Obr. 24: Kiwi Syslog Server, logon
Zdroj: vlastní zpracování

Ve filtrech bude nastaveno hlídání veškerých privilegovaných účtů a administrátorských skupin, u kterých hrozí největší nebezpečí, kdybychom nevěděli, co se s nimi děje a kam přistupují. Sledování přihlašování a odhlašování uživatelů do sítě, úspěšné i neúspěšné pokusy, a následně jestli byl uživateli po několika neúspěšných pokusech uzamknut účet, nebo jestli byl nějaký účet odemknut. S přihlašováním souvisí i autentizace pomocí Kerberos a sledování pohybu přidělování lístků. Sledování vypnutí/smazání antivirového softwaru. Sledovat samotnou změnu group policy (Audit Policy Change, Authentication/Authorization Policy Change) a změny v objektech v Active Directory na doménových řadičích.

S monitoringem se pojí i sledování přidělování DHCP adres (přes Server Manager DHCP Tools > "Enable DHCP audit logging" > v dokumentu C:\Windows\System32\..\DhcpSrvLog.txt) a DNS záznamy (DNS Management Console > povolit "Log packets for debugging" > logy importovat do souboru csv, kde se snadno filtrují a čtou).

Vyplatí se vycházet z doporučení dokumentu Windows 10 and Windows Server 2016 security auditing and monitoring reference, kde jsou všechny události popsané podle Event ID i jejich názvu a přesném znění. Kiwi Syslog Server se zdá jako dostatečné řešení pro monitoring sítě, ale v rámci dalšího rozvoje hlídání základních komponent lze použít systém Zabbix nebo Nagios.

12.14 Budoucí vývoj a další doporučení

Jedním z nedostatků návrhu popsaném v této práci, je přetížení doménového řadiče rolemi a nadbytečnými funkcemi. Důvodem je vlastnictví pouze jedné fyzické serverové stanice. Přestože po konfiguraci všech popsaných funkcionalit a rolí se zdál doménový řadič s WS2019 stabilní, v produkčním prostředí by provoz v síti měl být vytíženější a požadavky na stabilnost tím rapidně stoupnou. Doménový řadič je kritický bod v infrastruktuře. Do budoucna je určitě doporučované, aby na doménovém řadiči byly jen nejdůležitější funkce (AD DS, DNS a DHCP), vše ostatní přesunout na sekundární server. Lze uvažovat ještě nad virtualizací dvou serverů na jedné fyzické stanici, z nichž jedna bude doménový řadič. Pro monitoring celé sítě může být prozkoumána aplikace Windows Admin Center, která pomáhá se správou infrastruktury.

Aby byly splněny všechny požadavky ve vyhlášce o kybernetické bezpečnosti, musí být v síti prováděny pravidelné zálohy. Ačkoli byla v testovací LAN vyzkoušena jednoduchá záloha stavu systému na stanici WS2019, pro splnění požadavků je potřeba zálohu provádět pravidelně. Pokud by nebyl zvolen placený software, Windows poskytuje několik nástrojů pro zálohování a obnovu dat. Automatizované řešení může nabídnout Data Protection Manager, který zálohuje jak pracovní stanice, tak i celkový stav serverových stanic nebo virtuálních počítačů. Zálohované soubory lze ukládat na zvolenou stanici v LAN, což není doporučováno jako dlouhodobé řešení, na externí zařízení, nebo na cloud poskytující Microsoft Azure.

V kapitole o group policy byl na klientské stanici Win10 zakázán lokální administrátorský účet – toto řešení někdy nemusí být ideální. Může se stát, že počítač se neočekávaně odpojí od domény nebo se cokoli stane se síťovou kartou a ke stanici se nepřipojíme. Místo úplného zakázání tohoto účtu se dá přemýšlet o Local

Administrator Password Solution (LAPS), který chrání síť i před pass-the-hash útoky a další. K efektivnějšímu zabezpečení vzdáleného přístupu není složité implementovat přes registry vynucení použití Restricted Admin módu pro RDP spojení – namísto Remote Credential Guard, který v práci nebyl implementován.

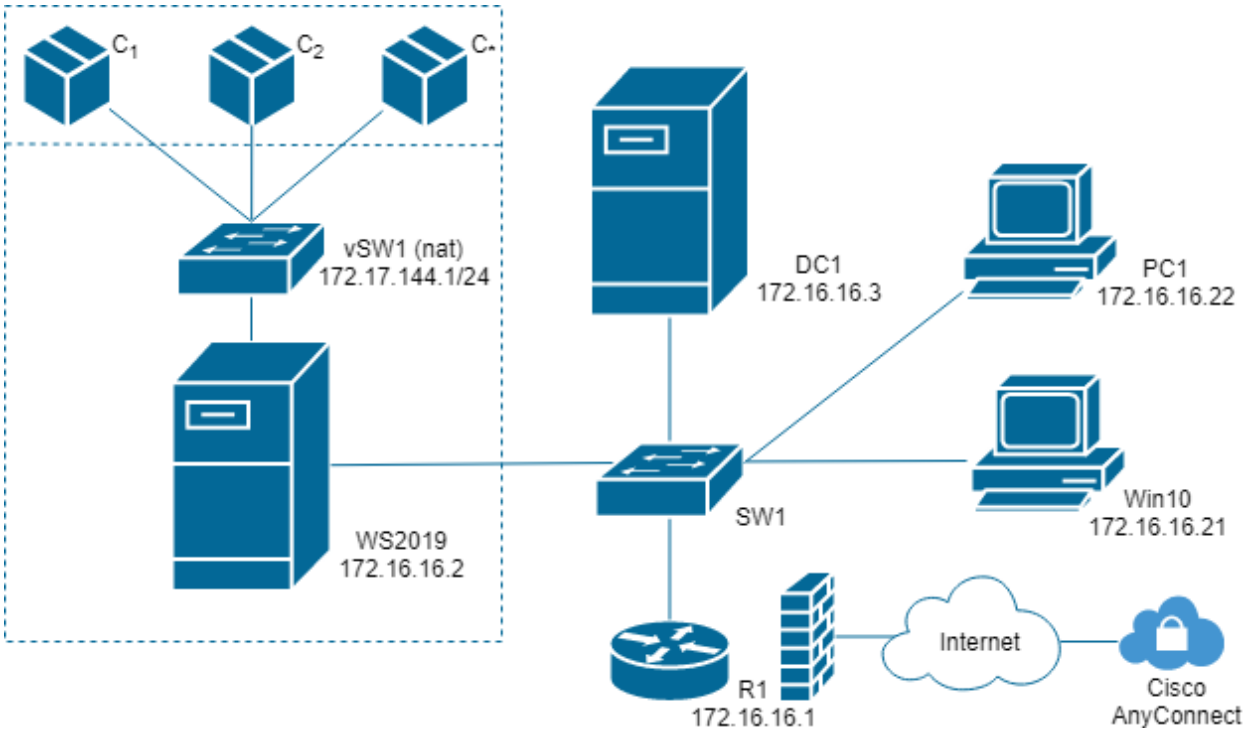
V dnešní době není neobvyklé, že vývojáři vyžadují povolení práce z domova – do návrhu LAN bude muset vést VPN (např. Cisco AnyConnect) a s ohledem na bezpečnost se bude muset přemýšlet o vícefaktorové autentizaci a implementaci IPSec pro toto spojení. Pro budoucí rozvoj práce se do infrastruktury může zahrnout bezpečnostní nástroj Attack Surface Analyzer, který zde nebyl probírán, protože se nejedná o aplikaci přivedenou společně s Windows Server 2016. Podobně je na tom aplikace AppLocker, která je užitečná pro pracovní stanice s Windows 10 (nepodporována pro Windows Server 2016 Core instalaci), ale do rozsahu práce se funkcionalita nedostala.

Práce se často řídila oficiální dokumentací od Microsoft, některé rady byly sbírány i v sérii článků Best Practices for Securing Active Directory, kde jsou praxí vyzkoušené techniky, jak vystavět návrh se zabezpečeným AD. Důležitou povinností pro firemní prostředí ale bude naplánovat "recovery plan", který je zdůrazňován i ve vyhlášce o kyberbezpečnosti. Vést tuto oblast může pomoct článek Computer Security Incident Handling Guide od NIST na toto téma (Cichonski et al., 2012).

Na obrázku č. 25 je rozšířená topologie obrázku, který je na začátku praktické části práce – zobrazuje lehce upravený návrh obsahující některé změny zmíněné v této kapitole. Hlavní změnou by měl být přidaný druhý server DC1, který by obstarával funkci doménového řadiče, DNS a DHCP serveru. Všechny ostatní role a funkce (IIS, kontejnery s virtuálním switchem vSW1, sekundární DNS a DHCP server, syslog server pro logování, aj.) by byly spuštěny na WS2019. Na řadu přijde i přechod na nový Windows Server 2019, u nějž bylo v práci potvrzeno, že zvládne vše, co Windows Server 2016.

Na obrázku nové topologie je i vidět oddělená stanice Privileged Access Workstation (SAW) pojmenovaná PC1, u které není přístup k internetu (např. hrozba zanesení viru z obvykle používané stanice, phishing útoky nebo keyloggery) –

přistupujeme tak pouze do LAN bez rizika zanesení hrozby. V dolní části obrázku je zobrazen VPN tunel do sítě, který bude implementován pomocí Cisco AnyConnect.



Obr. 25: Rozšířený návrh LAN
Zdroj: vlastní zpracování

Další konfigurace sítě velmi záleží na rozvoji samotné firmy. Dílčí komponenty lze rozšiřovat nebo upřesňovat dle toho, co bude klient vyžadovat. Rozšířit monitoring lze i o síťové komponenty, kde se podle grafů vytíženosti linek a statistik zvyšuje dostupnost služeb – takové služby poskytuje i program Cacti. Pokud by se infrastruktura LAN dále rozšiřovala, lze investovat do řešení Zabbix, který přes SNMP diagnostikuje potřeby sítě a umí spolupracovat i se systémem pfSense firewall, není problém nastavit odesílání sms upozornění, pokud se stane v síti něco podezřelého.

13 Závěr

Po úvodu o důležitosti kybernetické bezpečnosti na začátku práce byly popsány možnosti použití Windows Serveru. Následoval výčet a popis nových funkcionalit, které jako první uvedla verze Windows Server 2016. V následujících kapitolách, práce seznamuje s principy Active Directory a doménových trustů, obvyklé způsoby zabezpečení LDAP a Kerberos SSO, nebo pomocí Windows Firewallu. Jedna kapitola se zabývá i Windows Powershell, který se stal hlavním nástrojem při implementaci praktické části práce. Na konci teoretické části byl popsán síťový model ISO/OSI a výzkum aktualit a rizikové oblasti bezpečnosti.

V praktické části bylo předvedeno vývojové prostředí ve VMware Workstation Pro, představeno bylo jednoduché schéma sítě pro klientskou firmu. Následovaly kapitoly s popisem konfigurací na Windows Server 2016 a stanice s Windows 10, které byly propojeny v LAN. Popsána byla konfigurace DNS, DHCP, uživatelů a group policy, certifikační autority. V dalších kapitolách byl uveden návrh pro vývoj webových aplikací pomocí kontejnerů, zabezpečení přístupu k serverovým prostředkům pomocí JEA. Popsán byl i BitLocker, Secure boot a Credential Guard, následovalo zabezpečení komunikace pomocí Windows Firewall pravidel. Praktická část práce byla zakončena komplexní úlohou auditu a monitoringu událostí v síti, následně byla přidána doporučení pro další vývoj práce.

Práce vycházela z požadavků kladených ve vyhlášce 82/2019 Sb. o kybernetické bezpečnosti, které se podařilo splnit jednotlivými implementacemi komponent v síti. Byl vystavěn návrh LAN v reálném prostředí, který by měl projít u případného přezkoumání nezávislou osobou.

Windows Server 2016 má mnoho způsobů, jak zabezpečit naši infrastrukturu a práci zdaleka nebyla použita všechna možná řešení. Přestože se jedná o finančně náročnější řešení, kvalita zabezpečení našich strojů tomu odpovídá. U některých funkcionalit je i několik způsobů, jak docílit implementace. Díky jejich pomoci nebyl problém zabezpečit testovací LAN a stanici s Windows Server 2016 a Windows Server 2019. Byly splněny požadavky zadané klientem z firmy pro vývoj webových aplikací a s malými úpravami lze řešení přesunout do produkčního prostředí.

Řešení vývoje aplikací přes kontejnery se na první pohled zdá být velice výhodné, ačkoli má autor práce po vyzkoušení některé výhrady a doporučení. Přesto může být takové řešení v síti ponecháno a pouze poupraveno na testovací provoz, kdy k zákazníkovi přijde pouze čistá aplikace, která byla vyvíjena a testována v prostředí kontejnerů. Prozatím je řešení připraveno k vyzkoušení a záleží na odezvě klienta, jestli je takové řešení dostatečné. Další rozvoj se bude týkat hlavně zjednodušení procesu vývoje aplikací a jeho zabezpečení, jak bylo popsáno v podkapitole 12.9.1.

Celé řešení a konfigurace virtuálních strojů v jednotlivých image z VMware jsou k dispozici na vyžádání u autora práce. Při obhajobě práce bude předveden videozáznam se zobrazenou konektivitou virtuálních strojů a prokazatelně nastavenými komponentami, které byly v práci popsány.

14 Zdroje a literatura

1. NCKB, Národní centrum kybernetické bezpečnosti, *Nová vyhláška o kybernetické bezpečnosti*, 2018, cit. 2019-26-6. Dostupné online: [https://www.govcert.cz/cs/nova-vkb/]
2. HYNES, Corey a Ward RALSTON. *Microsoft Virtual Academy: What's New in Windows Server 2016*, MVA, 2016. Dostupné online: [https://mva.microsoft.com/en-us/training-courses/whats-new-in-windows-server-2016-16457?l=wHKT55sXC_2806218965]
3. GORANSSON, Paul, BLACK, Chuck a Timothy CULVER. *Chapter 5 - The OpenFlow Specification*, Editor(s): Paul Göransson, Chuck Black, Timothy Culver, Software Defined Networks (Second Edition), Morgan Kaufmann, 2017, Pages 89-136, ISBN 9780128045558, https://doi.org/10.1016/B978-0-12-804555-8.00005-3.
4. THOMAS, Orin. *Windows server 2016 inside out*. Redmond, Washington: Microsoft Press, 2017, ch. 4 Active Directory. Inside out (Redmond, Wash.). ISBN 9781509302482.
5. Microsoft, *Windows Server Software-Defined Datacenter*, 2017, cit. 2018-11-27. Dostupné online: [https://docs.microsoft.com/cs-cz/windows-server/sddc]
6. Microsoft TechNet, *Windows Server 2016: licenční změny.* 2016, cit. 2018-12-11. Dostupné online: [https://www.zive.cz/clanky/windows-server-2016-licencni-zmeny/sc-3-a-181431/default.aspx]
7. COMBE, Theo, MARTIN, Antony, PIETRO, Roberto. To Docker or Not to Docker: A Security Perspective (2016). IEEE Cloud Computing. 3. 54-62. 10.1109/MCC.2016.100.
8. MARTIN, A., RAPONI, S., COMBE, T., DI PIETRO, R. Docker ecosystem – Vulnerability Analysis, Computer Communications, Volume 122, 2018, Pages 30-43, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2018.03.011.
9. APOLINARIO, Vinicius. *What are Shielded VMs in Windows Server 2016 Hyper-V?* Microsoft TechNet, 2016. Dostupné online: [https://blogs.technet.microsoft.com/datacentersecurity/2016/03/14/windows-server-2016-shielded-vms-protecting-tenant-secrets/]
10. PANEK, William. *Mcsa windows server complete study guide: exams 70-740, 70-741, 70-742.* Indianapolis, IN: John Wiley, 2018. ISBN 9781119359142.
11. Microsoft, *Understanding pipelines*. 2018, cit. 2019-1-12. Dostupné online: [https://docs.microsoft.com/cs-cz/powershell/scripting/learn/understanding-the-powershell-pipeline?view=powershell-6]
12. SOUKUP, Ondřej. *AD DS a vztahy důvěry (AD DS Trusts),* 2009, cit. 2019-2-12. Dostupné online: [https://www.ondrej-soukup.cz/2009/08/ad-ds-vztah-duvery/]
13. SHARMA, Nirmal. Managing Active Directory trusts in Windows Server 2016, TechGenix, 2018, cit. 2019-2-12. Dostupné online: [http://techgenix.com/active-directory-trusts/?li_source=LI&li_medium=tg-afterpost]

14. OLSEN, Gary. *How to create a cross-forest trust in Active Directory*, TechTarget, 2008, cit. 2019-2-12. Dostupné online: [https://searchwindowsserver.techtarget.com/tip/How-to-create-a-cross-forest-trust-in-Active-Directory?fbclid=IwAR2bc6p5qoK6bfWRTYT1PMPT5ERooYpuQlw7Hi88nW4U1eq8NkN-knU6OeY]
15. BENÁK, Karel. *Použití adresářových služeb v informačních systémech*. Praha: České vysoké učení technické v Praze, 2004.
16. VOGLMAIER, Reinhard E. *The ABCs of LDAP: how to install, run, and administer LDAP services*. Boca Raton, FL: Auerbach Publications, 2004. ISBN 978-0849313462.
17. PERUTKA, Zdeněk. *Ověřování Verse serveru proti LDAPu a Kerberos serveru: Verse server authentication over LDAP and Kerberos.* Liberec: Technická univerzita v Liberci, 2014.
18. KHOUMSI, Ahmed, ERRADI, Mohammed, KROMBI, Wadie. *A formal basis for the design and analysis of firewall security policies*, Journal of King Saud University - Computer and Information Sciences, Volume 30, Issue 1, 2018, Pages 51-66, ISSN 1319-1578.
19. NEČAS, Tomáš. *Single Sign-On v J2EE webových aplikacích založené na protokolu SPNEGO/Kerberos*. Brno, 2009, diplomová práce, FIT VUT v Brně.
20. KILLORAN, John. What Is Single-Sign-On (SSO) Authentication & How Does It Work? SwoopNow, 2017. Dostupné online: [https://swoopnow.com/sso-authentication/]
21. BRINKMANN, Martin. PowerShell vs. PowerShell Core, what you need to know, ghacks.net, 2018. Dostupné online: [https://www.ghacks.net/2018/01/12/powershell-vs-powershell-core-what-you-need-to-know/]
22. Microsoft, *Block Cloning (Windows),* cit. 2018-11-28. Dostupné online: [https://docs.microsoft.com/cs-cz/windows/desktop/FileIO/block-cloning]
23. CVE Details, *TCP: Security Vulberabilities*, The ultimate security vulnerability datasource, cit. 2019-1-23. Dostupné online: [https://www.cvedetails.com/vulnerability-list/vendor_id-2090/TCP.html]
24. BRANCH, Drew. *ICMP: The Good, the Bad, and the Ugly, Misconceptions of ICMP*. Independent Security Evaluators, 2016. Dostupné online: [https://blog.securityevaluators.com/icmp-the-good-the-bad-and-the-ugly-130413e56030]
25. Center for Internet Security, *Multiple Vulnerabilities in Microsoft Windows SMB Server Could Allow for Remote Code Execution*. 2017, cit. 2019-1-28. Dostupné online: [https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-microsoft-windows-smb-server-could-allow-for-remote-code-execution/]
26. VENTER, H.S., ELOFF, J.H.P. a Y.L. LI. *Standardising vulnerability categories*, Computers & Security, Volume 27, Issues 3–4, 2008, Pages 71-83, ISSN 0167-4048.
27. *NIST: National vulnerability database*, Information Technology Laboratory, cit. 2018-12-4 Dostupné online: [https://nvd.nist.gov/vuln]

28. CVE Details, *The ultimate security vulnerability datasource*, MITRE Corporation, cit. 2019-2-25. Dostupné online: [https://www.cvedetails.com/product/23546/Microsoft-Windows-Server-2012.html?vendor_id=26]
29. CVE Details, *The ultimate security vulnerability datasource*, MITRE Corporation, cit. 2019-2-25. Dostupné online: [https://www.cvedetails.com/product/34965/Microsoft-Windows-Server-2016.html?vendor_id=26]
30. MITRE, *CWSS: Common Weakness Scoring Systém,* 2014, cit. 2018-2-25. Dostupné online: [https://cwe.mitre.org/cwss/cwss_v1.0.1.html]
31. Microsoft, *Prevent malware infection*, 2019 cit. 2019-2-15. Dostupné online: [https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/prevent-malware-infection]
32. ZSEBY T., KING A., BROWNLEE N. a CLAFFY K.C. *The Day after Patch Tuesday: Effects Observable in IP Darkspace Traffic*. In: Roughan M., Chang R. (eds) Passive and Active Measurement. PAM 2013. Lecture Notes in Computer Science, vol 7799. Springer, Berlin, Heidelberg. ISBN 978-3-642-36516-4
33. CIS, *CVE-2017-0144: Multiple Vulnerabilities in Microsoft Windows SMB Server Could Allow for Remote Code Execution*, CIS, Center for Internet Security, 2017, cit. 2019-1-5. Dostupné online: [https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-microsoft-windows-smb-server-could-allow-for-remote-code-execution/]
34. CIS*, Cyber Alert: Petya Ransomware*, Center for Internet Security, 2017, cit. 2019-1-5. Dostupné online: [https://www.cisecurity.org/ms-isac/cyber-alert-petya-ransomware/]
35. HERN, Alex. *WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017*, The Guardian, 2017, cit. 2019-1-6. Dostupné online: [https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware]
36. Microsoft. *Windows Server 2016 Security Guide*, 2017, cit. 2019-1-6.
37. MAYER, Alex. *The 3-2-1 Backup Rule – An Efficient Data Protection Strategy*, Nakivo, 2017. Dostupné online: [https://www.nakivo.com/blog/3-2-1-backup-rule-efficient-data-protection-strategy/]
38. VMware. *Product Workstation Pro*, cit. 2019-4-1. Dostupné online: [https://www.vmware.com/products/workstation-pro.html]
39. Microsoft. *Microsoft Security Compliance Toolkit*, cit. 2019-4-1. Dostupné online: [https://www.microsoft.com/en-us/download/details.aspx?id=55319]
40. MARGOSIS, Aaron. *Security baseline for Windows 10 v1607 ("Anniversary Update") and Windows Server 2016,* Microsoft TechNet Security Guidance blog, cit. 2019-4-1. Dostupné online: [https://blogs.technet.microsoft.com/secguide/2016/10/17/security-baseline-for-windows-10-v1607-anniversary-edition-and-windows-server-2016/]
41. Microsoft. *Windows container version compatibility*, 2019, cit. 2019-4-5. Dostupné online: [https://docs.microsoft.com/en-us/virtualization/windowscontainers/deploy-containers/version-compatibility]

42. Microsoft. *PowerShell For Docker*, 2016, cit. 2019-2-4. Dostupné online: [https://docs.microsoft.com/en-us/virtualization/windowscontainers/manage-docker/docker-powershell]
43. Microsoft. *Removing the latest tag*, 2019, cit. 2019-4-4. Dostupné online: [https://techcommunity.microsoft.com/t5/Containers/Removing-the-latest-Tag-An-Update-on-MCR/ba-p/393045]
44. Docker docs. *Content Trust in Docker*, cit. 2019-6-29. Dostupné online: [https://docs.docker.com/engine/security/trust/content_trust/]
45. Microsoft. Windows 10 and Windows Server 2016 security auditing and monitoring reference, 2016, cit. 2019-5-2. Dostupné online: [https://www.microsoft.com/en-us/download/details.aspx?id=52630]
46. CICHONSKI P., MILLAR T., GRANCE T. a K. SCARFONE. *Computer Security Incident Handling* Guide, Recommendations of the National Institute of Standards and Technology, 2012. Dostupné online: [https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf]

15 Seznam obrázků

16 Seznam tabulek

UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Akademický rok: 2016/2017

Studijní program: Aplikovaná informatika
Forma studia: Prezenční
Obor/kombinace: Aplikovaná informatika (ai2-p)

Podklad pro zadání DIPLOMOVÉ práce studenta

Jméno a příjmení:	**Bc. Lenka Folprechtová**
Osobní číslo:	**I1600868**
Adresa:	Studentská 434, Poděbrady – Poděbrady II, 29001 Poděbrady 1, Česká republika
Téma práce:	Využití Windows Server 2016 pro zabezpečení LAN
Téma práce anglicky:	Usage of Windows Server 2016 for LAN security
Vedoucí práce:	Mgr. Josef Horálek, Ph.D. Katedra informačních technologií

Zásady pro vypracování:

Cílem práce je provést podrobnou analýzu principů zabezpečení LAN za využití Windows Serveru 2016 a jeho nových vlastností z oblasti bezpečnosti. Autor práce zmapuje a podrobně popíše nové bezpečnostní opatření implementované ve Windows Serveru 2016 a navrhne jejich nasazení a využití pro zvýšení bezpečnosti LAN. V praktické části autor představí konkrétní postupy a konfiguraci Windows Serveru 2016 s dopadem na zabezpečení LAN formou případové studie v reálném prostředí firmy.
Osnova práce: Úvod Rešerše problematiky Představení významných změn architektury WS 2016 Představení významných bezpečnostních inovací WS 2016 Principy zabezpečení LAN sítí s využitím WS 2016 Stanovení výchozích hypotéz Návrh architektury LAN s aktivním využitím WS 2016 Konfigurace a testování navrženého řešení Vyhodnocení hypotéz Závěr

Seznam doporučené literatury:

THOMAS, Orin. Exam ref 70-412 configuring advanced windows server threshold services. ISBN 9780735697423. WARREN, Andrew. Exam ref 70-741 networking with windows server 2016. ISBN 9780735697621. WARREN, Andrew. Exam ref 70-742 identity with windows server 2016. ISBN 9780735697553. WARNER, Timothy L. Exam ref 70-744 securing windows server 2016. ISBN 9781509304264.

Podpis studenta: Datum:

Podpis vedoucího práce: Datum: