

Kurzy Windows Server, Linux

Kategória obsahuje prehľad tém a štruktúru výučby jednotlivých kurzov.

Administrátor Windows Server - efektívne a bezpečne

Kurz 1

Spravujte Windows Server efektívne a bezpečne. Získajte nové uplatnenie na trhu práce ako systémový správca. Školenie je ukončené Certifikátom. V termíne je uvedený len začiatok kurzu, o ďalších termínoch Vás budeme informovať.

MODUL 1: Windows Server - inštalácia a správa systému

Kurz o Windows Server predstavuje nevyhnutné minimum pre administrátora, správcu serverov či siete. Čaká na Vás veľa praktických úloh na precvičenie, teoretické princípy si vyskúšame v praxi. Každý účastník kurzu má k dispozícii svoj vlastný virtuálny počítač - server, ktorý si po skončení môže „odniesť“ domov a ďalej skúmať jeho možnosti.

Úvod do problematiky, inštalácia

inštalácia operačného systému Windows server; možnosti licencovania pre konkrétne modely využitia inštalácia operačného systému Windows 10 (demonštračný počítač „zamestnanca“, ktorý pridáme do domény) inštalácia serverovej úlohy Active Directory Domain Services - vytvorenie firemnej domény spolu s DNS serverom (ukážeme si, prečo je nevyhnutné ho nastaviť pre účely domény) práca so Server Manager nastavenie času práca s konzolou Active Directory Users and Computers, získanie prehľadu o jej možnostiach a využití pridanie počítača Windows 10 do našej domény vytváranie používateľov domény

Prípomenuť si základných znalostí z počítačových sietí

práca s ovládacím panelom Centrum sietí (Network and Sharing Center) nástroje na riešenie sieťových problémov: ping, tracert, ipconfig vzdialená správa servera - vzdialená pracovná plocha (Remote Desktop) a jej úskalnia

Súborové systémy, disky

správa diskov: rozdiel medzi basic a dynamic diskami, prehľad druhov partícií (simple, spanned, mirrored, striped a RAID-5)

Stratégie zdieľania založené na rolách (zdieľané prostriedky a RBAC)

nastavenie zdieľania, nastavovanie prístupových práv na zdieľaný prostriedok

prehľad vybraných nástrojov pre administrátorov Windows Server z množstva nástrojov

zálohovanie - možné scenáre a best-practices nástroj Windows Server Backup, nastavenie plánovaného zálohovania základný prehľad nástrojov a nastavení v ovládacom paneli

Ďalšie využitie Windows Server

DHCP server, File server, Print server - nastavenie zdieľanej tlačiarne

Úvod do skupinových politík, nastavenie bezpečného hesla v Default Domain Policy

Každý účastník kurzu používa svoju vlastnú inštaláciu Windows Server a Windows 10 vo virtuálnom prostredí, nemá nič zakázané a má právo si svoje počítače „rozhasiť“ :)?

MODUL 2: Windows Server - Active Directory - Denné úlohy správcu systému

Kurz Active Directory - Denné úlohy správcu systému je zameraný na úlohy, ktoré správcovia domén denne vykonávajú na serveroch a klientských počítačoch. Frekventant získa vedomosti o koncepte Active Directory, vie samostatne zhodnotiť účelnosť jeho použitia v konkrétnom prípade, vie vytvoriť prvý doménový kontroler a bezpečne ho nakonfigurovať. Frekventant je otvorený možnostiam centralizovanej správy množiny výpočtovej techniky využitím nástrojov dostupných v Active Directory a Windows Server, vie pridať používateľa do domény a začleniť ho do skupín podľa jeho pracovného postavenia. Uvedomujúc si dôležitosť svojej profesie dbá na bezpečnú konfiguráciu svojej domény. Každý účastník kurzu má k dispozícii svoj vlastný virtuálny počítač - server, ktorý si po skončení môže „odniesť“ domov a ďalej skúmať jeho možnosti.

Systémy prepojenia (zoskupenia) množiny počítačov v miestnej sieti

Zopakovanie konceptu Workgroup - pracovná skupina systému Windows Výhody a obmedzenia pracovnej skupiny, možnosti využitia

Koncept Domény - teória

Predstavenie konceptu ako nosného bodu centralizovanej správy počítačov, používateľov a nastavení Štruktúra domény, strom a les domén Protokol LDAP a jeho využitie v doméne a mimo nej Scenáre, v ktorých domény nie je vhodný, možné alternatívne riešenia domény, napr. na UNIXe Úlohy typu Operation Master - čo ktorá úloha zabezpečuje a ako sledovať, ktorý server ju vykonáva

Active Directory - teória

Pochopenie konceptu LSA a SAM na platforme Windows v spojení s doménou, odlišnosť tohto konceptu v pracovnej skupine Scenáre vhodného použitia Pojmy SID, GUID, OU

Práca s Active Directory

Vytvorenie prvého doménového kontrolera na existujúcej inštalácii Windows Server Práca s nástrojom Active Directory Users and Computers Koncepty tvorby OUs (organizačné jednotky) s ohľadom na efektívnu správu a škálovateľnosť domény, best practices z praxe, vytváranie OUs v testovacej doméne s ohľadom na dlhodobú udržateľnosť a jednoduchosť ďalšej správy a administrácie Objekty v Active Directory - vytváranie počítačov, serverov, pridávanie používateľov - denné úlohy administrátora Vlastnosti používateľa domény, nastavenie prvotného hesla, reset hesla, obmedzenie prihlasovania v čase, deaktivovanie používateľa, zistenie členstva a právomocí používateľa, atribúty používateľského konta v doméne Rozdiel medzi lokálnym a doménovým používateľským kontom, lokálny vs doménový administrátor Nastavenie doménového

neprivilegovaného používateľa ako doménového administrátora Koncept vlastností objektu (používateľa) ako súčasť schémy domény, možnosti rozšírenia vlastností - atribútov o nové prvky a ich nastavenie v Active Directory Rozdiel medzi Skupinou a OU

Nasadzovanie (deploying) active directory v praxi

Pridávanie počítača do domény Pridávanie nového počítača, podmienky pridane nového počítača do domény Riešenie problémov s pripojením do domény na strane pracovnej stanice pridávanie servera do domény

Riadenie prístupu k sieťovým zdrojom využitím konceptu Active Directory, riadenie prístupu na základe rolí - RBAC

Typy skupín používateľov a ich právomoci, vstavané skupiny Zásady bezpečného používania skupín - stratégie ALP, AGDLP a AGUDLP Zásady bezpečného používania skupín v praxi - na zdieľanom sieťovom prostredí Diskusia - ako sa vyhnúť bezpečnostnému riziku v tejto oblasti

Dlhodobá udržateľnosť spravovanej množiny výpočtových zdrojov použitím technológie Active Directory

Prihlasovacie skripty, písanie jednoduchého skriptu

Skupinové politiky GPO ako mocný nástroj na centralizované nastavenie spravovaných počítačov

Vysvetlenie pojmu skupinová politika, rozdiel medzi používateľskou a počítačovou politikou Politika bezpečnosti používateľských účtov v doméne pomocou Default Domain Policy Lokálna politika Doménová politika Rozdiel medzi lokálnou a doménovou politikou Poradie aplikovania a dedičnosť politik Stránky a linky

Zistenie aktuálne aplikovaných nastavení skupinovej politiky

Zistenie aktuálne aplikovaných nastavení na počítač / používateľa Zistenie aktuálne aplikovaných nastavení z klientskeho PC a z prostredia Active Directory na Windows Server Obnovenie pravidiel skupinovej politiky Bezpečnostné opatrenia s využitím Group Policy Možnosti využitia Group Policy: presmerovanie priečinkov, automatické pripojenie sieťových jednotiek, upravenie registrov systému Windows Cestovný používateľský profil Nastavenie skupinovej politiky pre aplikácie tretích strán, napr. internetový prehliadač Vypublikovanie tlačiarne

Pokročilé informácie o databáze domény

Základný prehľad o databáze domény, obnove zmazaných objektov a témy s tým súvisiace

Delegovanie správy Active Directory na dispečing / helpdesk

Prípadové štúdie, diskusia Pridanie delegácie Zistenie, kto má právomoci na delegáciu

Diskusia a best practices z praxe

Vzdialená správa Active Directory bez nutnosti práce na Windows Serveri Vzďialená správa Active Directory z počítača, ktorý nie je pripojený v doméne Importovanie zoznamu používateľov z iných zdrojov Bezpečnosť Active Directory Záver kurzu - posolstvo do praxe, záverečné zhrnutie a diskusia

MODUL 3: Windows Server - Bezpečnosť serveru a domény Active Directory

Kurz o bezpečnosti systému Windows, Windows Server a Active Directory prepája teoretické základy z princípov informačnej bezpečnosti do praxe. Precvičíte si široké možnosti bezpečnostných opatrení na konkrétne hrozby. Predstavíme Vám medzinárodné odporúčané systémové nastavenia, ktoré budete v rámci praktických úloh samostatne realizovať na svojich virtuálnych serveroch. V neposlednom rade nás čaká veľa spoločného brainstormingu a diskusií. Tvorivou, pútavou formou si priblížime dôležité aspekty práce bezpečnostného administrátora, ktorý plní azda najzodpovednejšiu úlohu vo firemnej sieti. Každý účastník kurzu má k dispozícii svoj vlastný virtuálny počítač - server, ktorý si po skončení môže „odniesť“ domov a ďalej skúmať jeho možnosti.

Terminológia základných pojmov informačnej bezpečnosti a ich prepojenie s opatreniami v praxi

Riadenie, manažment informačnej bezpečnosti s ohľadom na prostredie Windows, Windows Server a Active Directory

Bezpečnostné mechanizmy systému Windows Server

diskusia o službách a prvkoch systému Windows, ktoré môžu prestavovať vektory útokov bezpečná inštalácia a konfigurácia systému Windows

Základné koncepty bezpečnosti Windows Server

aktualizácia operačného systému aktualizovanie kritických aplikácií antivírusová ochrana fyzická ochrana servera

Skupinová politika ako nástroj na bezpečné jednotné prostredie

zásady pri nastavovaní hesiel v doméne pravidlá používania a distribúcie hesiel, politika hesiel a zamknývanie účtov lokálna vs doménová skupinová politika samostatná aplikácia skupinovej politiky na vlastný server podľa medzinárodných štandardov

Aktualizácie Windows

diskusia o rizikách spojených s (ne)aktualizovanými systémami využitie služby WSUS (software update service), použitie aplikácie WSUS server

Firewall

základný koncept brány firewall a jej implementácia vo Windows Server softvérové a hardvérové riešenia, ich výhody, nevýhody a využitie zásady správnej konfigurácie, umiestnenie servera do DMZ

Používateľské účty a skupiny používateľov

rozdiel medzi doménovým a lokálnym účtom typy skupín a ich využitie stratégie pridelovania prístupových práv RBAC - skupiny typu ALP, AGDLP, AGUDLP

Prístupové práva k súborom

zásady bezpečnosti pri zdieľaní súborov rozdiel medzi povoleniami pre zdieľané prostriedky a prístupové práva na úrovni súborového systému (NTFS) auditovanie prístupu, koncept referenčného monitora ako nástroja na riadenie a auditovanie podľa princípov RBAC

Koncept vzdialenej súkromnej siete - VPN

možnosti implementácie vzdialenej siete podľa úrovne bezpečnosti implementácia PPTP, IPSec, OpenVPN scenáre využitia a účelnosti

Záverečné zhrnutie

diskusia o možných ďalších opatreniach na zvýšenie bezpečnosti lokálnej siete záver

Bezpečnosť Windows/Server v kontexte ISO/IEC 27001 a 27002

Kurz 2

Bezpečnosť Active Directory v súlade s požiadavkami noriem ISO/IEC 27001 a 27002. Získate zručnosti v zosúladiení existujúceho stavu zabezpečenia Vašej podnikovej domény s normami ISMS. Budete schopní samostatne analyzovať, vyhodnotiť a navrhnúť opatrenia vo Vašej firemnej sieti t...

Zopakovanie základov informačnej bezpečnosti

Hravou formou si zopakujeme základné pojmy, nevyhnutnú terminológiu z informačnej bezpečnosti, aby sme mohli nadviazať na pokročilé požiadavky noriem. Základné legislatívne akty slovenskej právnej úpravy v tejto oblasti.

Základné princípy normy ISO/IEC 27001

Riadenie informačnej bezpečnosti podľa ISO/IEC27001

v kontexte podnikovej domény postavenej na Active Directory a LAN počítačovej sieti. Využívame druhú, najnovšiu revíziu normy 27001 z roku 2013.

Postup aplikácie odporúčaní podľa normy ISO/IEC27002

Politiky informačnej bezpečnosti

tvorba, skúmanie

Riadenie aktív

zodpovednosti, vlastníctvo aktív, prijateľné používanie, vrátenie, klasifikácia informácií, označovanie informácií, riadenie médií, likvidácia a prenos médií

Riadenie prístupu

do domény, informačného systému, všeobecne - prístupy, registrácia a deaktivácia používateľov s ohľadom na práva a povinnosti GDPR a slovenskej právnej úpravy, riadenie privilégii, riadenie utajených autentizačných údajov, skúmanie prístupových práv, riadenie prístupov k systémom a aplikáciám, bezpečné prihlasovanie, praktické ukážky v OS Windows, nastavenie politik pre súlad s touto požiadavkou normy, riadenie a manažment hesiel v kontexte s redundanciou a zastupiteľnosťou, privilegované programy

Kryptografia teoreticky aj prakticky

nebudeme skúmať matematické postupy ale z pohľadu manažmentu sa budeme venovať kryptografickým opatreniam, správe kľúčov a jednotlivé opatrenia si ukážeme v prostredí MS Windows.

Fyzická bezpečnosť a bezpečnosť prostredia

perimeter fyzickej bezpečnosti, riadenie fyzických priestorov, zabezpečenie kancelárií, prostriedkov, ochrana pred hrozbami fyzického prostredia, práca v bezpečnostnej zóne, umiestnenie zariadení a ich ochrana, proces zakúpenia aktíva/zariadenia až po jeho bezpečnú likvidáciu, ako riadiť bezpečnosť aktív mimo organizácie

Prevádzková bezpečnosť

manažment konfigurácie, dokumentácia prevádzkového postupu, riadenie zmien, segregácia prostredí, opatrenia proti škodlivému kódu, zálohovanie v dennej praxi administrátorov, monitoring a ochrana auditného záznamu, jednotné časové nastavenia

Komunikačná bezpečnosť

riadenie bezpečnosti na úrovni siete, bezpečnosť sieťových služieb, oddelenie sietí, prenos informácií, zmluvy o výmene informácií, výmena elektronických správ, postupy riadenia systémových zmien

Riadenie incidentov informačnej bezpečnosti

zodpovednosť a postupy, informovanie o udalostiach informačnej bezpečnosti, posúdenie udalostí informačnej bezpečnosti a rozhodnutia o nich, legislatívne a technické aspekty bezpečnostných incidentov, odporúčaný postup čo robíť pri bezpečnostnom incidente, ponaučenie z incidentov

Kontinuita informačnej bezpečnosti

plánovanie a vyhodnotenie kontinuity, kedy je vhodná redundancia, kde má a nemá zmysel uvažovať redundantné zdroje a prostriedky, vyhodnotenie kontinuity na základe histórie podniku a súčasných trendov

Bezpečnostné mechanizmy Active Directory

Kurz 3

Ste administrátor Active Directory? Chcete vylepšiť Vašu bezpečnostnú stratégiu tak, aby bola odolná voči súčasným typom útokov? Na rozšírenom kurze o pokročilých bezpečnostných mechanizmoch AD Vám predstavíme nové možnosti, ktorými možno zlepšiť zabezpečenie AD infraštruktúry pr...

Bezpečnostné mechanizmy systému Windows Server - opakovanie

GPO - možnosti, odkiaľ čerpať námety Windows Firewall (a jeho úskalí v prípade použitia antimalvérových produktov s podobnou funkciou) Windows Defender a ostatné antimalvérové nástroje

Resuscitácia AD

Dôležité miesta v doméne, ktoré je potrebné kontrolovať a monitorovať

Bezpečné DNS

Využitie DNS proxy a rozličné scenáre ochrany DNS. Nastavenie bezpečnej replikácie DNS záznamov.

Bezpečná sieť

Cez ktoré protokoly potrebujú naši používatelia komunikovať?

Firewall pre klientov, servery, radiče AD

Nastavenie pravidiel prostredníctvom GPO

Používateľské účty a skupiny používateľov

Prečo každý nemusí byť Domain User?

Model vrstvenia

Ako ochrániť administrátorské konto pred „šikovným“ používateľom? Využitie vybraných skupín v AD

Problematika lokálneho administrátora

Nástroj Local Admin Password Solution - áno alebo nie? Ochrana procesu LSASS

Čo všetko môžu naši používatelia?

Čítanie z LDAP, resp. čítanie databázy AD Čítanie a parsovanie skupinových politik Spúšťanie programov, exfiltrácia

Ako získať večný život?

Perzistencia na pracovnej stanici, serveri Perzistencia v AD Odhaľovanie perzistencie základnými ale aj sofistikovanými postupmi

Záverečné zhrnutie

diskusia o možných ďalších opatreniach na zvýšenie bezpečnosti domény záver

Upozornenie

Jedná sa o rozšírený kurz - oproti štandardnému kurzovému dňu je na tento kurz vyčlenených [6 hodín](#). V prípade záujmu je možné prispôbiť témy kurzu na mieru a prispôbiť ho potrebám konkrétnej inštitúcie (napr. pre účely školenia IT oddelení, Manažérov informačnej bezpečnosti a pod.)

IT TESTER

Kurz 4

Prečo absolvovať kurz IT testing ? IT tester - manuálny, je vo svojej podstate najnižšia úroveň v oblasti IT technológií. Preto je táto pozícia vhodná na vstup do sveta IT. Pozícia testera je veľmi atraktívna a často vyhľadávaná. Je to spôsobené najmä veľkým rozvojom aplikácií a...

Pre koho je kurz IT testovanie?

pre budúcich junior testerov pre záujemcov, ktorí sa chcú stať testermi pre záujemcov, ktorí sa chcú requalifikovať na testera pre úplných začiatočníkov, ktorí chcú vstúpiť do sveta IT pre záujemcov s minimálnymi alebo žiadnymi vedomosťami z IT

Budeme podrobne rozoberať teóriu testovania

vývoj softvéru terminológia výrazy a termíny používané v testovaní nástroje procesy ako by mal tester premýšľať techniky testovania

Manuálne testovanie na príkladoch

Testovacie prípady v praxi Testovanie ad hoc a exploračné testovanie Prístup k riadeniu a meranie exploratorného testovania Odhad chýb Zaškrtávací zoznam Aká technika je najlepšia?

Management testovania

Test management a dokumentácia Plánovanie testovania Trojuholník kvality Plán testovania Plánovanie v agilnom prostredí Riadenie testovania Hlásenie o stave testovania Motivácia testerov

Hlásenie defektov

Pre koho sú hlásenia o defektoch určené Význam hlásenia o defektoch pre zabezpečenie kvality Systémy pre správu hlásenia o defekte Štandardné prvky hlásenia o defekte Zhrnutie Popis Komentáre Prílohy Špecifické prvky hlásenia Nereprodukovateľné defekty Životný cyklus ohláseného defektu

Meranie kvality - metriky

Prečo merať kvalitu? Čo môžeme merať? Ako môžeme merať kvalitu? Delenie na tvrdé a mäkké metriky Delenie metrik podľa použitých dát Metriky založené na testoch Doplnkové metriky Spracovanie výsledkov

Ukážky použitia nástrojov pre automatizáciu testovania

HP Unified Functional Testing Nahrávanie aktivity používateľ Kontrolné body Test riadený dátami - načítanie dát a parametrizácia Ukážka pokročilejšieho využitia VB skriptu Apache JMeter

Kybernetická bezpečnosť I. - základy

Kurz 5

Tento kurz poskytuje účastníkom základné znalosti z oblasti kybernetickej bezpečnosti s dôrazom na praktické aplikácie a súčasnú legislatívu. Kurz kombinuje teoretické základy s praktickými príkladmi a reálnymi scenármi, čím pripravuje účastníkov na efektívnu implementáciu bezpečnosti.

Smernica NIST 2

Základné vysvetlenie Co to pre nás znamená Zákon o kybernetickej bezpečnosti Zákon 69/2018 Najznámejšie útoky Symptómy hacknutia

Data privacy / Súkromie údajov

Kto všetko zbiera o nás údaje? Ochrana osobných údajov Dávaš si pozor, čo zdieľaš? Na čo si dávať pozor Kryptovanie údajov na disku Vymazávanie dát

Spôsoby ochrany

Hardware Software školenia rozdelenie firewallov Model viacnásobnej ochrany

Monitoring siete

Čo nám chodí po sieti ICMP SNMP NETFLOW

Overenie bezpečnosti siete

Penetračné testy - čo to je?

Svetové a národné bezpečnostné autority

CSIRT, SK-CERT

Sieťová bezpečnosť

Rozdelenie zraniteľností Rozdelenie a popisanie hrozieb Rozdelenie útokov podľa typov Tvorba hesiel Sila hesiel Útoky na heslá

Bezpečnosť bezdrôtových sietí

Rozdelenie WIFI Odporúčania Verejných wifi Odporúčania Bluetooth Odporúčania Domáce wifi Zraniteľnosť WIFI video1

LINUX inštalácia a základy nastavenia systému

Kurz 6

Rozšírite svoje uplatnenie administrátora a naučte sa ako funguje rodina Linux! Kurz inštalácie a administrácie Linux je určený aj pre tých, ktorí používajú systém Windows a potrebujú rozšíriť svoje zručnosti o tento open-source operačný systém. Z kurzu si odnesiete nové vedomosti...

Teoretické základy a úvodné predpoklady

charakteristika UNIX / Linux najpoužívanejšie grafické používateľské prostredia, rozdiely medzi nimi

Základné operácie v konzole

shell Linuxu použitie nápovede, skrátená a plná verzia manuálu reštartovanie a vypnutie počítača

Súborový systém

úvod do súborového systému typy súborových systémov, typy súborov základné príkazy pre prácu so súbormi vytváranie, kopírovanie, presúvanie, premenovanie súborov dátová štruktúra i-uzol, zobrazenie informácií informácie o súborovom systéme, využitie disku atribúty súborov rozšírené riadenie prístupu

Správa používateľov a skupín

vytváranie a rušenie používateľov, skupín superpoužívateľ, bezpečnosť prepínanie medzi používateľmi zmena hesla

Správa procesov

procesy a programy - základné rozdiely zoznam procesov riadenie, monitorovanie monitorovanie Činnosti procesov, zobrazenie bežiacich procesov v systéme aktualizovanie programov

Spracovanie textu pomocou systémových utilít

rozdiel medzi textovým editorom a textovým procesorom výpis obsahu súboru do konzoly inštalácia a použitie základného textového editora nano editor vi a jeho ovládanie

Systémové možnosti a využitie Linuxu v praxi - diskusia, príp. ukážky z praxe

diskusia - využitie Linuxu vo vnorených systémoch, napr. špeciálne zariadenia v priemysle, doprave edície Linuxu - napr. Kali Linux, varianty GNOME/KDE webservice, databázový server aj v podnikovom prostredí

LINUX pre administrátorov - pokročilé možnosti správy

Kurz 7

Naučíte sa ako efektívne a bezpečne spravovať Linux Systém/Server. Vyskúšate si možnosti, pomocou ktorých si zjednodušíte svoj život administrátora. Pokročilými nastaveniami operačného systému napomôžete k cieľu vysokej dlhodobej udržateľnosti Vašich inštalácií, znížite čas potre...

Teoretické základy a úvodné predpoklady

charakteristika UNIX / Linux architektúra systému, podpora multitaskingu bootovanie operačného systému prihlasovací proces najpoužívanejšie grafické používateľské prostredia, rozdiely medzi nimi

Základné operácie v konzole

shell Linuxu použitie nápovede, skrátená a plná verzia manuálu reštartovanie a vypnutie počítača zobrazenie logov spúšťanie programov argumenty príkazov, spúšťanie programov na pozadí interpretery príkazov shell BASH presmerovanie výstupu do textového súboru programové kanály /pipe pripojenie do konzoly z prostredia systému Windows

Súborový systém

úvod do súborového systému typy súborových systémov, typy súborov základné príkazy pre prácu so súbormi vytváranie, kopírovanie, presúvanie, premenovanie súborov dátová štruktúra i-uzol, zobrazenie informácií vyhľadanie súboru informácie o súborovom systéme, využitie disku práca s kvótou atribúty súborov rozšírené riadenie prístupu, zvláštne oprávnenia, nielen pomocou príkazu chmod mapovanie diskových oddielov, vytváranie virtuálneho disku a jeho následné využitie

Správa používateľov a skupín

vy písanie zoznamu všetkých používateľov vytváranie a rušenie používateľov, skupín rozdiel medzi databázovým súborom users a shadow, ich ochrana a využitie v praxi prístupové práva superpoužívateľ, bezpečnosť prepínanie medzi používateľmi zmena hesla nastavenie pokročilých vlastností používateľa - napr. kedy zanikne

Správa procesov

procesy a programy - základné rozdiely zoznam procesov ovládanie procesov, signály využívané systémové prostriedky a nastavenie ich limitov riadenie, monitorovanie štart a ukončenie procesov, mechanizmus fork-exec, signály medziprocesová komunikácia, riadiaci terminál monitorovanie činnosti procesov, zobrazenie bežiacich procesov v systéme aktualizovanie programov zmena priority procesu, preplánovanie uspanie procesu

Spracovanie textu pomocou systémových utilít

rozdiel medzi textovým editorom a textovým procesorom výpis obsahu súboru do konzoly inštalácia a použitie základného textového editora nano príkazy na pokročilejšie operácie s textom - grep, cat, sed, awk editor vi a jeho ovládanie

Systémové možnosti a využitie Linuxu v praxi

zálohovanie, obnova a prenos údajov program Clonezilla diskusia - využitie Linuxu vo vnorených systémoch, napr. špeciálne zariadenia v priemysle, doprave edície Linuxu - Kali Linux webservice, databázový server aj v podnikovom prostredí elektronická pošta, mailový server Linux ako podkladový systém pre iné aplikácie

LINUX správca systému

Kurz 8

Kurz LINUX správca systému je určený všetkým záujemcom, ktorých zaujíma práca s operačnými systémami, počítačovými sieťami, ich inštalovaním a konfiguráciou v prostredí Linux a radi by si našli pracovné uplatnenie v tejto oblasti na trhu práce. Balík sa skladá z nasledujúcich kur...

Teoretické základy a úvodné predpoklady

charakteristika UNIX / Linux architektúra systému, podpora multitaskingu bootovanie operačného systému prihlasovací proces najpoužívanejšie grafické používateľské prostredia, rozdiely medzi nimi

Základné operácie v konzole

shell Linuxu použitie nápovede, skrátená a plná verzia manuálu reštartovanie a vypnutie počítača zobrazenie logov spúšťanie programov argumenty príkazov, spúšťanie programov na pozadí interpretery príkazov shell BASH presmerovanie výstupu do textového súboru programové kanály /pipe pripojenie do konzoly z prostredia systému Windows

Súborový systém

úvod do súborového systému typy súborových systémov, typy súborov základné príkazy pre prácu so súbormi vytváranie, kopírovanie, presúvanie, premenovanie súborov dátová štruktúra i-uzol, zobrazenie informácií vyhľadanie súboru informácie o súborovom systéme, využitie disku práca s kvótou atribúty súborov rozšírené riadenie prístupu, zvláštne oprávnenia, nielen pomocou príkazu chmod mapovanie diskových oddielov, vytváranie virtuálneho disku a jeho následné využitie

Správa používateľov a skupín

vy písanie zoznamu všetkých používateľov vytváranie a rušenie používateľov, skupín rozdiel medzi databázovým súborom users a shadow, ich ochrana a využitie v praxi prístupové práva superpoužívateľ, bezpečnosť prepínanie medzi používateľmi zmena hesla nastavenie pokročilých vlastností používateľa - napr. kedy zanikne

Správa procesov

procesy a programy - základné rozdiely zoznam procesov ovládanie procesov, signály využívané systémové prostriedky a nastavenie ich limitov riadenie, monitorovanie štart a ukončenie procesov, mechanizmus fork-exec, signály medziprocesová komunikácia, riadiaci terminál monitorovanie činnosti procesov, zobrazenie bežiacich procesov v systéme aktualizovanie programov zmena priority procesu, preplánovanie uspanie procesu

Spracovanie textu pomocou systémových utilít

rozdiel medzi textovým editorom a textovým procesorom výpis obsahu súboru do konzoly inštalácia a použitie základného textového editora nano príkazy na pokročilejšie operácie s textom - grep, cat, sed, awk editor vi a jeho ovládanie

Systémové možnosti a využitie Linuxu v praxi

zálohovanie, obnova a prenos údajov program Clonezilla diskusia - využitie Linuxu vo vnorených systémoch, napr. špeciálne zariadenia v priemysle, doprave edície Linuxu - Kali Linux webservice, databázový server aj v podnikovom prostredí elektronická pošta, mailový server Linux ako podkladový systém pre iné aplikácie

Princípy počítačových sietí

Rozdelenie a charakteristika počítačovej siete Referenčný model RM OSI, TCP/IP Zariadenia v sieti: hub, switch, router, firewall, WiFi AP, ... Typy zapojenia počítačovej siete Prepájanie sietí so spojením a bez spojenia, fragmentácia a defragmentácia paketu Prepájanie na prvej, druhej a tretej vrstve RM OSI Adresovanie v sieti - základy IPv4/6 adresy, pojmy IP adresa, MAC adresa, maska, podsieť, broadcast, verejná a statická IP adresa Princípy technológie NAT, kedy sa používa, prečo je v súčasnosti potrebná.

Nastavenie počítačovej siete v systéme LINUX

Sieťové rozhrania, zapnutie a vypnutie siete Konfiguračné súbory Manuálna konfigurácia Smerovanie - routing, predovšetkým statické smerovanie Konfigurácia Domain Name System (DNS), lokálne prekladanie domén, názvy Vášho PC v sieti Nástroj Netstat a jeho využitie pri kontrole využitia sieťových zdrojov Nástroj Nmap a jeho využitie pre legítimne účely kontroly zabezpečenia Nástroj Netcat a sokety pre komunikáciu medzi viacerými PC Protokol Address Resolution Protocol (ARP) a jeho využitie pri diagnostike siete

LINUX v sieti

Kurz 9

Zistíte ako funguje miestna počítačová sieť s dôrazom na špecifiká systému LINUX. Teoretické základy počítačových sietí využijete pri praktických úlohách na nastavovanie siete v operačnom systéme LINUX.

množstvo príkladov z praxe

, cvičenia na samostatné precvičenie a najmä uvažovanie. Výhodou nášho školiaceho strediska je, že k dispozícii máme na ukážku rozličné fyzické zariadenia počítačovej siete, čo Vám lepšie pomôže ich rozoznať v praxi a naplno využiť ich schopnosti. Okrem toho budete mať k dispozícii vlastný LINUX virtuálny počítač, ktorý si môžete po skončení kurzu skopírovať a neskôr doma samostatne skúmať ďalšie možnosti.

Princípy počítačových sietí

Rozdelenie a charakteristika počítačovej siete Referenčný model RM OSI, TCP/IP Zariadenia v sieti: hub, switch, router, firewall, WiFi AP, ... Typy zapojenia počítačovej siete Prepájanie sietí so spojením a bez spojenia, fragmentácia a defragmentácia paketu Prepájanie na prvej, druhej a tretej vrstve RM OSI Adresovanie v sieti - základy IPv4/6 adresy, pojmy IP adresa, MAC adresa, maska, podsieť, broadcast, verejná a statická IP adresa Princípy technológie NAT, kedy sa používa, prečo je v súčasnosti potrebná.

Nastavenie počítačovej siete v systéme LINUX

Sieťové rozhrania, zapnutie a vypnutie siete Konfiguračné súbory Manuálna konfigurácia Smerovanie - routing, predovšetkým statické smerovanie Konfigurácia Domain Name System (DNS), lokálne prekladanie domén, názvy Vášho PC v sieti Nástroj Netstat a jeho využitie pri kontrole využitia sieťových zdrojov Nástroj Nmap a jeho využitie pre legítimne účely kontroly zabezpečenia Nástroj Netcat a sokety pre komunikáciu medzi viacerými PC Protokol Address Resolution Protocol (ARP) a jeho využitie pri diagnostike siete

Bezpečnostné prvky siete v LINUXe

Firewall, nastavenie pravidiel, cesta paketu cez IPTables Secure Shell (SSH) server

Služby

Hypertext Transfer Protocol (HTTP) server pre umiestnenie vlastnej webstránky, Apache Webserver File Transfer Protocol (FTP)

Denné úlohy správcu siete

Bezpečnostné aspekty pri počítačovej sieti

, typy niektorých útokov a ich prevencia

Microsoft SharePoint server pre používateľov

Kurz 10

Kurz Microsoft SharePoint pre užívateľov je určený záujemcom, ktorí pracujú s balíkom MS Office a chcú sa naučiť využívať výhody rýchleho zdieľania informácií pomocou MS SharePoint.

Zdieľanie dokumentov

knížnica dokumentov uloženie súboru do knižnice editovanie súborov v knižnici problematika viacnásobného otvorenia súboru

Export dát z Excel do MS SharePoint

vytvorenie tabuľky získanie web adresy pre SharePoint stránku export tabuľky odkaz na exportovanú tabuľku revízia a úprava tabuľky

Vytvorenie knižnice snímok pre prezentácie

výhody knižnice požadovaný softvér a práva vytvorenie knižnice pridávanie snímok do knižnice kopírovanie a editovanie snímok

Využívanie kalendára na SharePoint stránke

umiestnenie kalendára vkladanie položiek do kalendára editovanie a mazanie položiek v kalendári odoslanie emailu s odkazom na kalendár

Diskusia a záver

Správca systému Windows - inštalácia a nastavenie počítača Windows

Kurz 11

Získajte zručnosti v systéme Windows na úrovni administrátora. Na tomto kurze samostatne nainštalujete a nastavíte systém Windows. Okrem základných a rozšírených nástrojov administrátora sa budeme venovať aj bezpečnosti systému Windows.

Všeobecné informácie o počítači ako stroji

Predstavenie komponentov počítača, vonkajších zariadení a vnútorných súčastí počítača (k čomu slúžia, aké druhy existujú a aké problémy s nimi súvisia) Nástroj BIOS/UEFI Config, na čo sa používa a kedy ho využijeme ako administrátori Operačné systémy, ich rodiny a využitie v súčasnej praxi

Inštalácia operačného systému Microsoft Windows

Predstavenie rôznych verzií a druhov systému Minimálne požiadavky na inštaláciu Sprievodca inštaláciou Používateľské kontá, lokálne, Microsoft účet, doménové Núdzový režim a riešenie chýb pri inštalácií

Nastavenia - prehľad vybraných nástrojov na riešenie konkrétnych situácií z praxe

Ovládací panel Univerzálna konzola MMC (využitie, pridávanie modulov) Používateľské kontá, kontrola používateľských kont (UAC) Správca zariadení, pridanie komponentu (napr. tlačiarne), možnosti inštalácie ovládačov a problémy s tým súvisiace Správca úloh

Jadro systému Windows a s tým súvisiace možnosti

Systémové služby Registre systému Windows Knižnice DLL Systémový čas Plánovač úloh Príkazový riadok vs PowerShell

Súborový systém

Typy pevných diskov a súborové systémy Nastavenie prístupových práv, dedenie, povolenie a zakázanie prístupu Defragmentácia Kontrola neporušenosti Rozdelenie oddielov pevného disku Obnovenie do predchádzajúceho stavu (body obnovy) Auditný záznam, Zobrazovač udalostí

Sieťové nastavenia a prehľad o počítačovej sieti

Centrum sietí a zdieľania Zdieľanie priečinka po sieti Zdieľanie tlačiarne pripojenej k počítaču po sieti Nastavenie sieťovej karty a jej ochrana Vzdialené ovládanie systému Windows (vzdialená pracovná plocha a príkazový riadok)

Základy bezpečnosti systému Windows

Veľkorytí útokov Opatrenia na úrovni siete (Firewall, ...) Opatrenia na úrovni operačného systému Prístupové heslá a ich politiky Skupinová politika (Group Policy) Windows Defender a Firewall, komerčné riešenia

Šikovný administrátor Windows a počítačovej siete

Kurz 12

Získajte zručnosti v systéme Windows na úrovni administrátora a zároveň objavte ako fungujú počítačové siete. Na tomto kurze samostatne nainštalujete a nastavíte systém Windows. Okrem základných a rozšírených nástrojov administrátora sa budeme venovať aj hardwarovým problémom a z...

Všeobecné informácie o počítači ako stroji

Predstavenie komponentov počítača, vonkajších zariadení a vnútorných súčastí počítača (k čomu slúžia, aké druhy existujú a aké problémy s nimi súvisia) Nástroj BIOS/UEFI Config, na čo sa používa a kedy ho využijeme ako administrátori Operačné systémy ich rodiny a využitie v súčasnej praxi

Inštalácia operačného systému Microsoft Windows

Predstavenie rôznych verzií a druhov systému Minimálne požiadavky na inštaláciu Sprievodca inštaláciou Používateľské kontá, lokálne, Microsoft účet, doménové Núdzový režim a riešenie chýb pri inštalácií

Nastavenia - prehľad vybraných nástrojov na riešenie konkrétnych situácií z praxe

Ovládací panel Univerzálna konzola MMC (využitie, pridávanie modulov) Používateľské kontá, kontrola používateľských kont (UAC) Správca zariadení, pridanie komponentu (napr. tlačiarne), možnosti inštalácie ovládačov a problémy s tým súvisiace Správca úloh

Jadro systému Windows a s tým súvisiace možnosti

Systémové služby Registre systému Windows Knižnice DLL DxDiag nástroj pre DirectX Prihlasovací proces Systémový čas Plánovač úloh Príkazový riadok vs PowerShell

Súborový systém

Typy pevných diskov a súborové systémy Nastavenie prístupových práv, dedenie, povolenie a zakázanie prístupu Defragmentácia Kontrola neporušenosti Rozdelenie oddielov pevného disku Obnovenie do predchádzajúceho stavu (body obnovy) Auditný záznam, Zobrazovač udalostí

Sieťové nastavenia a prehľad o počítačovej sieti

Centrum sietí a zdieľania Zdieľanie priečinka po sieti Zdieľanie tlačiarne pripojenej k počítaču po sieti Nastavenie sieťovej karty a jej ochrana Diagnostika problémov s internetovým pripojením Koncepty prepojenia počítačov v rámci miestnej siete - pracovná skupina vs doména

Počítačové siete

Základný koncept o počítačovej sieti Ako funguje počítačová sieť, predpoklady pripojenia lokálneho a pripojenia do internetu IP adresa DNS DHCP zariadenia v sieti - router, firewall, switch, hub, WiFi pojmy: port, protokol, rozhranie, MAC adresa základné sieťové služby: http, FTP, SSH, DNS, NTP, virtuálna privátna sieť Vzdialené ovládanie systému Windows (vzdialená pracovná plocha a príkazový riadok)

Základy bezpečnosti systému Windows

Vektory útokov Opatrenia na úrovni siete (Firewall, ...) Opatrenia na úrovni operačného systému Prístupové heslá a ich politiky Skupinová politika (Group Policy) Windows Defender a Firewall, komerčné riešenia

Záver

Záverečné zhrnutie a diskusia

Windows Server - Active Directory - Denné úlohy správcu systému

Kurz 13

Naučíte sa ako efektívne a bezpečne spravovať doménový server - kontrolór Active Directory pod Windows Server. Vyskúšate si možnosti, pomocou ktorých si zjednodušíte svoj život administrátora a nastavíte veľa prvkov centralizovane. Po absolvovaní kurzu už nikdy nezažijete stres a...

Systémy prepojenia (zoskupenia) množiny počítačov v miestnej sieti

Zopakovanie konceptu Workgroup - pracovná skupina systému Windows Výhody a obmedzenia pracovnej skupiny, možnosti využitia

Koncept Domény - teória

Predstavenie konceptu ako nosného bodu centralizovanej správy počítačov, používateľov a nastavení Štruktúra domény, strom a les domén Protokol LDAP a jeho využitie v doméne a mimo nej Scenáre, v ktorých domény nie je vhodný, možné alternatívne riešenia domény, napr. na UNIXe Úlohy typu Operation Master - čo ktorá úloha zabezpečuje a ako sledovať, ktorý server ju vykonáva

Active Directory - teória

Pochopenie konceptu LSA a SAM na platforme Windows v spojení s doménou, odlišnosť tohto konceptu v pracovnej skupine Scenáre vhodného použitia Pojmy SID, GUID, OU

Práca s Active Directory

Vytvorenie prvého doménového kontrolera na existujúcej inštalácii Windows Server Práca s nástrojom Active Directory Users and Computers Koncepty tvorby OUs (organizačné jednotky) s ohľadom na efektívnu správu a škálovateľnosť domény, best practices z praxe, vytváranie OUs v testovacej doméne s ohľadom na dlhodobú udržateľnosť a jednoduchosť ďalšej správy a administrácie Objekty v Active Directory - vytváranie počítačov, serverov, pridávanie používateľov - denné úlohy administrátora Vlastnosti používateľa domény, nastavenie prvotného hesla, reset hesla, obmedzenie prihlasovania v čase, deaktivovanie používateľa, zistenie členstva a právomocí používateľa, atribúty používateľského konta v doméne Rozdiel medzi lokálnym a doménovým používateľským kontom, lokálny vs doménový administrátor Nastavenie doménového neprivilégovaného používateľa ako doménového administrátora Koncept vlastností objektu (používateľa) ako súčasť schémy domény, možnosti rozšírenia vlastností - atribútov o nové prvky a ich nastavenie v Active Directory Rozdiel medzi Skupinou a OU

Nasadzovanie (deploying) active directory v praxi

Pridávanie počítača do domény Pridávanie nového počítača, podmienky prídania nového počítača do domény Riešenie problémov s pripojením do domény na strane pracovnej stanice pridávanie servera do domény

Riadenie prístupu k sieťovým zdrojom využitím konceptu Active Directory, riadenie prístupu na základe rolí - RBAC

Typy skupín používateľov a ich právomocí, vstavané skupiny Zásady bezpečného používania skupín - stratégie ALP, AGDLP a AGUDLP Zásady bezpečného používania skupín v praxi - na zdieľanom sieťovom prostredí Diskusia - ako sa vyhnúť bezpečnostnému riziku v tejto oblasti

Dlhodobá udržateľnosť spravovanej množiny výpočtových zdrojov použitím technológie Active Directory

Prihlasovacie skripty Základné príkazy v príkazovom riadku využiteľné pri riešení problémov v doméne

Skupinové politiky GPO ako mocný nástroj na centralizované nastavenie spravovaných počítačov

Vysvetlenie pojmu skupinová politika, rozdiel medzi používateľskou a počítačovou politikou Politika bezpečnosti používateľských účtov v doméne pomocou Default Domain Policy Lokálna politika Doménová politika Rozdiel medzi lokálnou a doménovou politikou Poradie aplikovania a dedičnosť politik Stránky a linky

Zistenie aktuálne aplikovaných nastavení skupinovej politiky

Zistenie aktuálne aplikovaných nastavení na počítač / používateľa Zistenie aktuálne aplikovaných nastavení z klientskeho PC a z prostredia Active Directory na Windows Server Obnovenie pravidiel skupinovej politiky Bezpečnostné opatrenia s využitím Group Policy Možnosti využitia domény a Group Policy: presmerovanie priečinkov, automatické pripojenie sieťových jednotiek, upravenie registrov systému Windows, Cestovný používateľský profil Možnosti nastavenia skupinovej politiky pre aplikácie tretích strán, napr. internetový prehliadač Vypublikovanie tlačiarne

Delegovanie správy Active Directory na dispečing / helpdesk

Prípadové štúdie, diskusia, spôsoby prídania delegácie Zistenie, kto má právomocí na delegáciu

Diskusia a best practices z praxe

Vzdialená správa Active Directory bez nutnosti práce na Windows Serveri Pokročilé informácie o databáze domény - Základný prehľad o databáze domény, obnove zmazaných objektov a témy s tým súvisiace Vzďialená správa Active Directory z počítača, ktorý nie je pripojený v doméne Importovanie zoznamu používateľov z iných zdrojov Bezpečnosť Active Directory Záver kurzu - posolstvo do praxe, záverečné zhrnutie a diskusia

Objavte bezpečnostné mechanizmy, ktoré môžete uplatniť vo svojej firemnej doméne. Vysvetlíme Vám základné princípy informačnej bezpečnosti, pojmy bezpečnostných štandardov, ktoré následne aplikujete na zabezpečenie svojich Windows Serverov. Osobitne sa budeme venovať bezpečnostný...

Terminológia základných pojmov informačnej bezpečnosti a ich prepojenie s opatreniami v praxi

Riadenie, manažment informačnej bezpečnosti s ohľadom na prostredie Windows, Windows Server a Active Directory

Bezpečnostné mechanizmy systému Windows Server

diskusia o službách a prvkoch systému Windows, ktoré môžu prestavovať vektory útokov bezpečná inštalácia a konfigurácia systému Windows

Základné koncepty bezpečnosti Windows Server

aktualizácia operačného systému aktualizovanie kritických aplikácií antivírusová ochrana fyzická ochrana servera

Skupinová politika ako nástroj na bezpečné jednotné prostredie

zásady pri nastavovaní hesiel v doméne pravidlá používania a distribúcie hesiel, politika hesiel a zamknutie účtov lokálna vs doménová skupinová politika samostatná aplikácia skupinovej politiky na vlastný server podľa medzinárodných štandardov

Aktualizácie Windows

diskusia o rizikách spojených s (ne)aktualizovanými systémami možnosti využitia služby WSUS (software update service)/WSUS server

Firewall

základný koncept brány firewall a jej implementácia vo Windows Server softvérové a hardvérové riešenia, ich výhody, nevýhody a využitie zásady správnej konfigurácie, umiestnenie servera do DMZ

Používateľské účty a skupiny používateľov

rozdiel medzi doménovým a lokálnym účtom typy skupín a ich využitie (zopakovanie) prehľad stratégií pridelovania prístupových práv RBAC + zásady bezpečnosti pri zdieľaní súborov

Koncept vzdialenej súkromnej siete - VPN

možnosti implementácie vzdialenej siete podľa úrovne bezpečnosti koncepty a scenáre použitia protokolov VPN sietí: PPTP, IPSec, OpenVPN a iné... scenáre využitia a účelnosti

Záverečné zhrnutie

diskusia o možných ďalších opatreniach na zvýšenie bezpečnosti lokálnej siete záver

Rozšírite svoje zručnosti v systéme Windows o princípy Windows serverov! Kurz inštalácie a administrácie Windows Server je určený aj pre súčasných administrátorov "obyčajných" Windows 10, ktorí po rozšírení kvalifikácie budú denne pracovať so serverom, vykonávať správu a technickú...

Úvod do problematiky, inštalácia

inštalácia operačného systému Windows server; možnosti licencovania pre konkrétne modely využitia inštalácia operačného systému Windows(demonštračný počítač „zamestnanca“, ktorý pridáme do domény) inštalácia serverovej úlohy Active Directory Domain Services - vytvorenie firemnej domény spolu s DNS serverom (ukážeme si, prečo je nevyhnutné ho nastaviť pre účely domény) práca so Server Manager nastavenie času, význam NTP server pod Windows Server práca s konzolou Active Directory Users and Computers, získanie prehľadu o jej možnostiach a využití pridanie počítača Windows 10 do našej domény vytváranie používateľov domény

Pripomenutie si základných znalostí z počítačových sietí

práca s ovládacím panelom Centrum sietí (Network and Sharing Center) nástroje na riešenie sieťových problémov: ping, nslookup, ipconfig vzdialená správa servera - vzdialená pracovná plocha (Remote Desktop) a jej úskalia

Súborové systémy, disky

správa diskov: rozdiel medzi basic a dynamic diskami, prehľad o druhoch partícií (simple, spanned, mirrored, striped a RAID-5)

Stratégie zdieľania založené na rolách (zdieľané prostriedky a RBAC)

nastavenie zdieľania, nastavovanie prístupových práv na zdieľaný prostriedok (napr. priečinok, tlačiareň) nastavenie podmienok pri prístupových právach v súborovom systéme - rozdiel medzi právami na zdieľané prostriedky a právami na úrovni súborového systému

prehľad vybraných nástrojov pre administrátorov Windows Server z množstva nástrojov

práca s nástrojom Reliability and Performance Monitor zálohovanie - možné scenáre a best-practices nástroj Windows Server Backup, nastavenie plánovaného zálohovania základný prehľad nástrojov a nastavení v ovládacom paneli

Ďalšie využitie Windows Server

prehľad rolí servera - napr. DHCP server - nastavenie pridelovania IP adries, Print server - nastavenie zdieľanej tlačiarne

Úvod do skupinových politík

Každý účastník kurzu používa svoju vlastnú inštaláciu Windows Server a Windows Pro vo virtuálnom prostredí, nemá nič zakázané a má právo si svoje počítače „rozhasiť“ :)