



PV175 Správa systémů MS Windows I

Otázky z odpovědníků podzim 2021





Včetně komentářů a otevřený k úpravám a doplnění je dokument dostupný na [Google Drive](#)

Čím se odlišuje edice systému Windows s označením "N"?

- Každá distribuce Windows dostupná na území EU je ve skutečnosti "N"
-  Neobsahuje Media Player a některé další video technologie, kvůli rozhodnutí Evropské Komise.
-  Chybějící komponenty je možné jednoduše stáhnout
- Výrazně ovlivňuje cenu licence
- Neobsahuje sledovací nástroje od NSA

Jaké jsou podmínky k ukončení předmětu PV175?

-  Získat dostatečný počet bodů na závěrečném testu
-  Úspěšně splnit všechny povinné úkoly - jinak se nemohu přihlásit na zkoušku
- Důsledně si projít všechna cvičení na virtuálních počítačích
- Odpověď si na všechny otázky uvedené v materiálech


Jaká strategie pro nasazení Windows je vhodná pro následující scénář:

Společnost má asi 12 000 počítačů, většina z nich používá OS Windows


Každý den se z "balíku" používaných aplikací vyřadí 5 a přidá 6 nových

Existuje infrastruktura pro nasazení a udržení životního cyklu aplikací - SCCM


Existuje infrastruktura pro hromadné nasazení OS - MDT

-  Z uvedených informací není možné určit správnou odpověď. Oba dva (nebo i další) přístupy mohou být správné. Např. pokud nepotřebuji řešit dobu instalace, může být Thin image výhodnější -> méně práce, existující infrastruktura.
- Vytvoříme Thin obraz instalace a využijeme stávající infrastrukturu pro nasazení aplikací
- Vytvořím Thick obraz instalace a každý den ho budeme aktualizovat

Kde sehnat originální instalační image (to co nahraju na USB) pokud jsem zakoupil PC s předinstalovaným Windows?

- Skrze Azure Dev Tools for Teaching (dříve MSDN AA)
<https://www.fi.muni.cz/tech/win/msdnaa.html.cs>
-  Na stránkách
<https://www.microsoft.com/en-us/software-download/windows10>
- PirateBay.org

Jak se vkládá DVD do mechaniky?

- Potiskem dolů
-  Potiskem nahoru

Vložte jeden příkaz pro program bcdedit, který zajistí, že pro právě aktivní OS se zapne hodnota "Boot Log" (budese vytvářet soubor, který popisuje start systému).

- ✓ (bcdedit /set bootlog yes, BCDEdit /SET {Current} BootLog On, BCDEdit /set bootlog true, bcdedit /set bootlog yes, bcdedit /set {current} bootlog Yes, bcdedit -set bootlog Yes, bcdedit -set {current} bootlog yes)

Technologie "Secure Boot" [alespoň jedna správně]

- Vyžaduje TPM modul (speciální hardware)
- ✓ Je součástí UEFI standardu
- Je proprietární technologie specifická pro OS Windows
- Jedná se o výlučnou součást technologie BitLocker (šifrování disku), která před startem OS ověří zda nedošlo k nežádoucí modifikaci zaváděcích informací (boot dat).

Zjistěte, kam si notepad.exe ukládá nastavení "word wrap", viz obrázek. Následně vložte jméno atributu, který je zodpovědný za uchování hodnoty "word wrap" (zalamování řádků).

Např. Konfigurace se ukládá do souboru config.ini, jméno záznamu, který ovlivňuje velikost fontu je "fFontSizeText"

- ✓ (fWrap)

V jakých souborech jsou/mohou být uloženy uživatelské registry? [alespoň jedna správně]

- ✓ usrclass.dat
- system
- sam
- ✓ ntuser.dat
- ntuser.man

Kde jsou uloženy registry (případně jejich zálohy) v systému? [alespoň jedna správně]

- ✓ %UserProfile%\NTUSER.DAT
- ✓ %SystemRoot%\System32\Config\RegBack
- %UserProfile%\Microsoft\Backup\Register
- Žádná z uvedených není správně.
- ✓ %SystemRoot%\System32\Config

Jaká posloupnost příkazů povede k vypsání ID všech procesů, které jsou ve stavu "not responding", tedy neodpovídají?

A: |

B: get-process

C: where

D: select id

E: {\$_.responding -eq \$false}

- ABACEAD
- BADACE
- ✓ BACEAD
- BACAEAD

Jakým způsobem mohu otevřít soubor pokus.txt z Powershell konzole?

Předpokládejme, že soubor je v aktuálním pracovním adresáři.

Zadáním:

- "pokus.txt"
- 'pokus.txt'
- ✓ .\pokus.txt
- pokus.txt
- ✓ & ".\pokus.txt"
- ✓ notepad pokus.txt

V PS konzoli zadám následující příkaz:

\$file = get-item .\pokus.txt

\$file.length

Mi vypíše číslo 10, což je velikost daného souboru. Pokud si chci vypsát v konzoli velikost souboru ve větě následujícího tvaru: "Velikost souboru je 10 bajtů.", jak to udělám?

- echo "Velikost souboru je \$file.Length bajtů."
- ✓ echo "Velikost souboru je \$(\$file.Length) bajtů."
- ✓ \$size=\$file.Length; echo "Velikost souboru je \$size bajtů."
- echo 'Velikost souboru je \$file.Length bajtů.'
- echo 'Velikost souboru je "\$10" bajtů.'
- echo 'Velikost souboru je \$(\$file.Length) bajtů.'

V PS konzoli jsem si zadefinoval následující proměnné:

\$prvni = 1

\$druhy = 2

Jaké z následujících příkazů mi vypíše součet, tedy číslovku 3?

- ✓ Invoke-Expression "\$prvni + \$druhy"
- calc \$prvni + \$druhy
- '\$prvni + \$druhy'
- ✓ \$prvni + \$druhy
- "\$prvni + \$druhy"

Který z příkazů vypíše větu: "Hej Karle, kup basu piv a 20 párků."

Předpokládejme, že v PS konzoli již máme zdefinované následující proměnné:

\$name = 'Karle'

\$a = 10

\$b = 2

- ✓ "Hej Karle, kup basu piv a 20 párků."
- ✓ "Hej Karle, kup basu piv a $$(a*b)$ párků."
- 'Hej \$name, kup basu piv a 20 párků.'
- 'Hej "\$name", kup basu piv a 20 párků.'
- ✓ "Hej " + \$name + ", kup basu piv a 20 párků."

Jaký příkaz mi vrátí: 5.3?

- 3,3 + 2
- 3,0 + 2,0
- ✓ 3.3 + 2
- ✓ (3.3 + 2)
- 5,3

Jak mohu z PS konzole spustit program WordPad?

- "C:\Program Files\Windows NT\Accessories\wordpad.exe"
- ✓ & "C:\Program Files\Windows NT\Accessories\wordpad.exe"
- C:\Program Files\Windows NT\Accessories\wordpad.exe
- ✓ ."C:\Program Files\Windows NT\Accessories\wordpad.exe"
- .\"C:\Program Files\Windows NT\Accessories\wordpad.exe"

Zadáám-li do PS konzole následující příkaz, a poté zkusím v konzoli spustit

Get-SomeCommand, vyhubuje mi PS, že daný příkaz nezná?

```
$ExecutionContext.InvokeCommand.CommandNotFoundAction =
```

```
{  
    param(  
        [string]  
        $commandName,  
        [System.Management.Automation.CommandLookupEventArgs]  
        $eventArgs  
    )  
    $Sapi = New-Object -ComObject Sapi.SpVoice  
    $null = $Sapi.Speak("I don't know $commandName, stupid.")  
}
```

- ne
- ✓ ano

Jakým příkazem zjistím, zdali parametr name u cmdletu get-service přijímá vstup z pipe a zdali umožňuje použití wildcard (tzn. *)?

- get-help get-service
- ✓ get-help get-service -full
- ✓ man get-service -Parameter name
- get-service | get-help -full
- get-command get-service -full
- ✓ help get-service -Parameter name

Jakým příkazem si mohu vypsat procesy pojmenované notepad?

- ✓ Get-Process -Name notepad
- ✓ Get-Process -Name notepad -IncludeUserName
- Get-Process | where {\$_.name = 'notepad'}
- ✓ Get-Process | where {\$_.name -eq 'notepad'}
- ✓ gps | ? {\$_.name -eq "notepad"}

Co platí o skriptovacím jazyce Powershell?

- Není možné v něm spouštět příkazy známé z příkazové řádky
- ✓ Powershell skripty mají koncovku ps1
- ✓ Pracuje s objekty narozdíl od příkazové řádky
- ✓ Mezi interpretem příkazové řádky a Powershell se mohou přepínat zadáním příkazu cmd resp. powershell do konzole.
- Nelze spustit bez administrátorských práv

Kolik je v logu 03_pv175.evtx událostí úrovně (level) Error?

- ✓ (241)

Kolik je v logu 03_pv175.evtx událostí úrovně Error + událostí úrovně Warning? Úroveň se myslí atribut "level".

- ✓ (271)

Kolik je v logu 03_pv175.evtx událostí se zdrojem (Source) GroupPolicy?

- ✓ (114)

Kolik je v logu 03_pv175.evtx událostí s id=1 od 1.10 2016?

- ✓ (2)

Událostí s jakým ID je v logu 03_pv175.evtx nejvíc mezi událostmi vytvořenými od 13.9.2015 (použijte Group-Object)?

- ✓ (7036)

Kolik je v logu 03_pv175.evtx událostí úrovně (level) Information, kde ID je větší než 5000 nebo source (providername) obsahuje řetězec service?

- ✓ (2821)

Jakým způsobem si mohu vypsat všechny cesty, kde Powershell hledá dostupné moduly?

- \$PSModulePath
- ✓ \$env:PSModulePath
- Get-Variable PSModulePath
- \$PSHome
- \$Profile
- ✓ Get-ChildItem Env:\PSModulePath | select -expandproperty value


Vyberte příkazy v jazyce PowerShell, které vytvoří VHDX disk dynamického typu (rozlišujeme fixed size vs dynamic VHDX) o maximální velikosti 2GB, napojí ho (mount) pod libovolným písmenem a naformátují souborovým systémem NTFS.

- ✓ New-VHD -Path C:\temp\test.vhdx -Dynamic -SizeBytes 2GB | Mount-VHD -Passthru | Initialize-Disk -PartitionStyle MBR -PassThru | New-Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -FileSystem NTFS
- New-VHDX -Path C:\temp\test.vhdx -Dynamic -SizeBytes 2GB | Mount-VHD | Initialize-Disk -PartitionStyle MBR -PassThru | New-Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -FileSystem NTFS
- New-VHDX -Path C:\temp\test.vhdx -Type Dynamic -SizeBytes 2GB | Mount-VHD -Passthru | Initialize-Disk -PartitionStyle MBR | New-Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -FileSystem NTFS
- New-VHD -Path C:\temp\test.vhdx -Dynamic -SizeBytes 2GB | Mount-VHD | Initialize-Disk -PartitionStyle MBR | New-Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -FileSystem NTFS
- New-VHD -Path C:\temp\test.vhdx -Dynamic -SizeBytes 2GB | Mount-VHD -Passthru | Initialize-Disk -PartitionStyle GPT | New-Partition -UseMaximumSize -AssignDriveLetter | Format-Volume -FileSystem NTFS


Vyberte všechny způsoby, pomocí kterých můžete určit, zda je jednotka vytvořená pomocí Storage Spaces typu MBR nebo GPT? [alespoň jedna správně]

- V GUI pomocí Disk Management - bez jakéhokoliv dalšího nastavení nebo kliknutí - je hned na úvodní stránce vidět zda je disk typu MBR nebo GPT
- ✓ Pomocí powershell příkazu "Get-Disk"
- Pomocí powershell příkazu "Get-Volume"
- Pomocí powershell příkazu "Get-Partition"
- Žádná z uvedených není správně


Lze měnit velikost volume, které jsou vytvořeny jako two-way mirror ve Storage Spaces (tj. resiliency je typu mirror)? [alespoň jedna správně]

- Ne
-  Ano - zvětšit i zmenšit ale pouze pomocí powershellu
- Ano - zvětšit i zmenšit pomocí GUI i powershellu
- Ano - pouze zvětšit a pouze pomocí GUI
- Žádná z uvedených není správně

Zavedení systému Windows, který je nainstalován na disku s velikostí sektoru 4096b v režimu 4K Native je možné pouze: [právě jedna správně]

- Je-li OS verze alespoň Windows 8 a rozdělení disku je popsáno pouze systémem MBR.
- Windows nelze zavést z disku v režimu 4K Native (ale je možné používat disk pro ukládání dat).
- Je-li OS verze alespoň Windows 7 ve variantě x64.
-  Žádná z uvedených není správně.


Vyberte pravdivá tvrzení o úložiscích [alespoň jedna správně]

- V rámci jednoho fyzického disku je možné vytvořit jeden oddíl typu basic, druhý typu dynamic a třetí typu Storage Spaces.
- Storage spaces jsou dostupné od verze Windows 10 (tj. nejsou ve Windows 8).
- Dynamické disky nejsou podporovány v GPT typu rozdělení disku.
-  Pomocí Storage spaces je možné vytvořit iluzi většího oddílu, než je reálná (fyzicky dostupná) disková kapacita.
- Při použití GPT rozdělení a disků lze vytvořit oddíly do velikosti 2TB.
- Žádná z uvedených není správně.

Jaké heslo má uživatel hacknime? Zadání viz osnova.


-  (35300.)

Jaké SID má zabudovaný účet "Local System"


- S-1-5-10
-  S-1-5-18
- S-1-5-19
- S-1-5-1
- S-1-5-500

Administrátor aktivoval volbu "Password must meet complexity requirements" v Local Computer Policy na "Enabled" [do startu "Edit group policy", Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy.


Následně chtěl vytvořit nového uživatele "user" (se stejným full name) s heslem "User122.". Heslo však nesplňuje požadavky na komplexitu, a proto příkaz skončil chybou (vyzkoušejte). Zdůvodněte chování systému.

- Heslo je příliš dlouhé.
- Heslo obsahuje pouze jeden speciální znak.
-  Heslo obsahuje část loginu ("User")
- Heslo obsahuje dvakrát stejné číslo ("2").
- Heslo obsahuje je příliš krátké.


Jaká je maximální délka přihlašovacího jména uživatele = loginu?

- 10
- 15
-  20
- 25
- 30


Jaké z následujících zabudovaných skupin/identit mohou být plnohodnotným členem mnou vytvořené skupiny "krutoři"?

-  everyone
- administrators
- guests
- users
- remote desktop users

Je přihlašovací jméno (login) case sensitive?


- ano
-  ne
- ano pokud jeho délka přesáhne 20 znaků

Je uživatelské heslo case sensitive (záleží na velikosti písmen)?


- ne
-  ano
- od Windows 8.1 už heslo není case sensitive

Jaký je název systémové politiky, po jejímž nastavení se budu moci připojit ke stroji přes vzdálenou plochu aniž bych byl členem skupiny Remote Desktop Users?

Nápověda: secpol.msc (User rights assignment)


- Log on as a service
-  Allow log on through Remote Desktop Services
- Access this computer from network
- Allow log on locally

Jaké zabudované skupiny musím být členem abych mohl přistupovat i k souborům k nimž nemám NTFS práva?


- performance monitor users
- everyone
- remote desktop users
-  backup operators
- power users

Kdo může ve výchozím nastavení vytvářet symbolic linky (symbolické odkazy)?


Nápověda: secpol.msc (User rights assignment)

- Členové skupiny Authenticated users
- Členové skupiny Everyone
- Členové skupiny Users
-  Členové skupiny Administrators


Na stroji mám lokálního uživatele Pepik, který je jen členem skupiny Users. Spustím pod Pepikem správce souborů Total Commander a zkusím otevřít adresář C:\temp, ale neúspěšně. Chybové hlášení říká "Access denied" tedy Pepik nemá dostatečná práva. Vím ale, že skupina Krutoři má na tento adresář přístupová práva, tak jej do skupiny přidám. Co musím udělat abych otevřel danou složku pod Pepikem?

- Po přidání do skupiny, zkusím složku otevřít v již spuštěném Total Commanderu.
- Přidám skupině Krutoři FULL CONTROL právo na danou složku a následně ji otevřu ve spuštěném Total Commanderu.
-  Musím zavřít a znovu pod Pepikem otevřít Total Commander (aby se mu aktualizoval access token).
- Musím udělat 5 dřepů a 10 kliků a pak to třeba půjde.


Pro změnu logon name uživatele (loginu) je potřeba :

-  V lusrmgr.msc konzoli kliknout pravým na daného uživatele a dát rename.
- V lusrmgr.msc konzoli kliknout pravým na daného uživatele a ve vlastnostech změnit atribut Full name.
- v CMD spustit příkaz net user %puvodnilogin% %novylogin% /set
- v Powershell konzoli spustit příkaz Rename-User %puvodnilogin% %novylogin%


Čím se vyznačuje SID zabudovaného administrátora?

- Končí číslovkou 1000
-  Končí číslovkou 500
- Končí číslovkou 1
- Je na každém stroji jiné

Pokud uživatel pepik zresetuje heslo. Dojde ke změně jeho SID?




- ano
-  ne
- na Windows XP ano, na pozdějších Windows už ne

Pokud přejmenuji uživatele pepik. Dojde ke změně jeho SID?


- ano
-  ne
- jen pokud měl nastavené prázdné heslo

Kdo může ve výchozím nastavení systému vypnout (shutdown) počítač?

Nápověda: secpol.msc (User rights assignment)


- Členové skupiny "Remote Desktop Users"
-  Členové skupiny "Administrators"
- Členové skupiny "Guests"
-  Členové skupiny "Users"
- Uživatel pepik, jehož účet není členem žádné skupiny.
-  Členové skupiny "Backup Operators"

Kdo může ve výchozím nastavení systému převzít vlastnictví (ownership) souborů a jiných objektů?

-  Členové skupiny "Administrators"
- Členové skupiny "Backup Operators"
- Členové skupiny "Authenticated Users"
- Členové skupiny "Users"

Mám lokální skupinu "RDP users". Přidám do ní uživatele "Pepik". Skupinu "RDP users" přidám do "Remote Desktop Users" příkazem: net localgroup "remote desktop users" "RDP users" /add.

Bude se moci uživatel Pepik přihlásit na daný počítač přes vzdálenou plochu? Další nezbytné podmínky jako nastavený firewall atd neuvažujeme.

-  ne
- ano
- ano, ale až po restartu

Na složce jménem Enterprise v NTFS souborovém systému je nastaveno pro uživatele Jana oprávnění Read & execute typu Allow.

Žádná jiná oprávnění tam nejsou.




Jana je členem uživatelské skupiny editors, pro nadsložku této složky bylo poté nastaveno pro skupinu

editors Modify typ Allow, ostatní oprávnění byla odstraněna, zaškrtnuto zaškrtnutí

"Replace all child object permission entries with inheritable permission entries from this object" a stisknuto OK.

S možností "Applies to" nebylo manipulováno.





Která z následujících oprávnění má uživatelka Jana pro složku Enterprise?

-  List folder / read data
-  Create files / write data
-  Take Ownership

Situace pokračuje z předchozí otázky, navíc bylo přidáno na složku Enterprise oprávnění pro skupinu Authenticated Users Full control typu Allow.

S možností "Applies to" nebylo manipulováno.


Která z následujících oprávnění má uživatelka Jana na složce Enterprise?

-  List folder / read data
-  Create folders / append data
-  Delete
-  Take ownership





Situace pokračuje z předchozí otázky navíc bylo na nadřazené složce složky Enterprise přidáno v advanced oprávnění pro skupinu editors typ Deny a zaškrtnuto Create files / write data, Create folders / append data, Delete subfolders and files, Delete

S možností "Applies to" nebylo manipulováno.

Jaká z následujících oprávnění má uživatelka Jana pro tuto nadřazenou složku složky Enterprise?

-  List folder / read data
- Create folders /append data
- Create files / write data
- Change permissions

Situace pokračuje z předchozí otázky, která z následujících oprávnění má uživatelka Jana na složce Enterprise?

-  List folder / read data
-  Create folders / append data
-  Delete
-  Take ownership

Ve cvičení modulu 6 pro úkol 3 bylo nezbytné:

- ✓ definovat oprávnění pro skupinu "creator owner"
- definovat oprávnění pro skupinu "authenticated users"
- definovat nějaké oprávnění typu Deny
- ✓ manipulovat s položkou "Applies to"

Ve cvičení modulu 6 v úkolu 4 nemohla Jana upravovat nově vytvořený soubor, co z následujícího platilo:

- Jana neměla žádná oprávnění k nově vytvořenému souboru.
- ✓ Jana neměla patričná oprávnění pro přejmenování ani editaci souboru.
- ✓ Jana byla vlastníkem souboru, proto si mohla nastavit oprávnění Modify, aby mohla soubor měnit.
- Jana byla vlastníkem souboru, proto mohla soubor rovnou smazat bez změny oprávnění.




Ve cvičení modulu 6 v úkolu 5 měl Pepa převzít vlastnictví a zajistit, aby nikdo jiný kromě něj neměl k souboru přístup, jak toho Pepa mohl docílit:

- ✓ mohl použít příkaz takeown k převzetí vlastnictví
- mohl převzít vlastnictví pomocí GUI ve vlastnostech souboru na kartě security
- mohl použít příkaz changeowner ke změně vlastníka
- ✓ mohl použít cmdlet Set-NTFSOwner k převzetí vlastnictví
- po převzetí vlastnictví nastavit pro everyone typ Deny Full control
- ✓ po převzetí vlastnictví Pepa změnil oprávnění tak, že mohl smazat všechny záznamy oprávnění a přidat oprávnění pouze pro svůj uživatelský účet
- když si přestal hrát s Janiným souborem, mohl použít cmdlet Set-NTFSOwner, aby nastavil Janu zpět jako vlastníka souboru s úmyslem zahltit stopy


Ve cvičení modulu 6 v úkolu 6 neměla Jana přístup v Altap Salamanderu k souboru i poté, co jste přidali oprávnění skupině, jejíž byla Jana členem. Přístup získala, až když jste Salamander spustili znovu, co platí:

- Je to čistě špatné chování Salamanderu, takto by se přístup chovat neměl.
- Oprávnění souboru se změní až s odhlášením uživatele.
- ✓ V době prvního spuštění Salamanderu nebyla Jana členem vytvořené skupiny, lze si prohlédnout zobrazením podrobných informací o uživateli pomocí whoami /all, uživatelský access token se vygeneruje typicky při přihlášení uživatele. Je tedy zapotřebí se odhlásit/přihlásit, tedy analogicky zavřít spuštěný Salamander a spustit znovu (stačí samozřejmě spustit nový). V nově spuštěném Salamanderu bude již uživatelka Jana členem dané skupiny, což si prohlédneme pomocí whoami /all. Tím, že je členem uživatelské skupiny získává oprávnění, která jsou pro tuto skupinu nastavená.

Uživatelka Saskie vysdílila na svém počítači kleopatra pomocí sdílení souborů a tiskáren ve Windows složku D:\data\vychytavky, vyplnila jméno sdílení DIY\$ a nastavila oprávnění Read typ Allow pro uživatele Bohumir. Poté přidala NTFS oprávnění Full control typ Allow pro skupinu Users na složku vychytavky, ostatní oprávnění na složce nemají pro řešení vliv. Co z následujícího platí:

- Bohumir může číst obsah souborů z počítačů v síti přistoupením na cestu \\kleopatra\vychytavky
- Saskie může číst obsah souborů z počítačů v síti přistoupením na cestu \\kleopatra\vychytavky
- Bohumir může číst obsah souborů z počítačů v síti přistoupením na cestu \\kleopatra\C\$\data\vychytavky
- Bohumir může číst obsah souborů z počítačů v síti přistoupením na cestu \\localhost\DIY\$
-  Bohumir může číst obsah souborů z počítačů v síti přistoupením na cestu \\kleopatra\DIY\$
- Saskie může číst obsah souborů z počítačů v síti přistoupením na cestu \\kleopatra\DIY\$
- Bohumir může odkudkoliv změnit oprávnění souborů ve složce vychytavky přístupem přes \\kleopatra\DIY\$
-  Bohumir může změnit oprávnění souborů ve složce vychytavky pokud je přihlášen na počítači kleopatra
- Saskie může odkudkoliv změnit oprávnění souborů ve složce vychytavky přístupem přes \\kleopatra\DIY\$
-  Saskie může přidat oprávnění Full control pro sdílené složky na sdílení s názvem DIY\$ pro skupiny Everyone typ Allow, poté Bohumir může smazat soubory ve složce vychytavky z jiného počítače přístupem přes \\kleopatra\DIY\$
- Pokud Saskie zadá na počítači elejandr do start menu text \\kleopatra a odentruje, počítač jí vypíše, že na stroji kleopatra je dostupná síťová složka D:\data\vychytavky pod sdílením s názvem DIY\$

Ve cvičení modulu 7 v úkolu 2 se uživatel Krokodyl pokusil smazat složku Library s konfigurací oprávnění dle zadání, co z následujícího platilo:

- Library bylo možné smazat včetně podsložky Regal, protože na obě složky měl uživatel zděděné oprávnění Delete
- Složku Library nebylo možné smazat, protože na složku Regal neměl uživatel oprávnění Delete a složka Library tak nebyla prázdná
-  Složku Library bylo možné smazat, protože měl uživatel oprávnění Delete subfolders and files a v tom případě nepotřebuje oprávnění Delete na podsložky
- Složku Library bylo možné smazat, protože uživatel Krokodyl byl jmenován výsostným správcem složky Public, což bylo odsouhlaseno na valném shromáždění uživatelů a potvrzeno dokumentem s minimálně třemi podpisy

V úkolu 3a ze cvičení modulu 7 po přidání oprávnění Full control typ Deny na složku Inherited Deny a dodržení předchozího nastavení oprávnění dle úkolu mohl uživatel Pepa otevírat následující soubory:

- ✓ Inherited Allow\neco.txt
- Inherited Allow\Inherited Deny\neco.txt
- ✓ Inherited Allow\Inherited Deny\Explicit Allow\neco.txt
- Inherited Allow\Inherited Deny\Explicit Allow\Explicit Deny\neco.txt

Elegantním řešením úkolu 4 cvičení modulu 7 bylo aplikování vhodných oprávnění, popřípadě změna vlastníka na vrchní složku a před potvrzením zaškrtnutí možnosti:

- ✓ Replace all child object permission entries with inheritable permission entries from this object
- Only apply these permissions to objects and/or containers within this container

Elegantním řešením úkolu 5 cvičení modulu 7 bylo aplikování vhodných oprávnění na Root složku a zaškrtnutím možnosti:

- Replace all child object permission entries with inheritable permission entries from this object
- ✓ Only apply these permissions to objects and/or containers within this container

Pro správné vyřešení úkolu 6 cvičení modulu 7 bylo nutné nastavovat oprávnění skupinám:

- ✓ Developers
- ✓ Management
- ✓ Owner rights
- Creator owner
- Administrators
- Authenticated users
- Remote desktop users

Pokud chci aby se jakémukoli uživateli, který se přihlásí na stroj titan05 (C:\ je systémový disk) zobrazila na ploše ikona prohlížeče Chrome udělám:

- ✓ Napíši Powershell skript, který na plochu aktuálně přihlášeného uživatele nakopíruje ze start menu zástupce na Chrome. V Task Scheduleru scheduleru vytvořím task, jehož trigger bude nastaven na přihlášení jakéhokoli uživatele a jenž spustí náš PS skript.
- ✓ Nakopíruji zástupce Chrome do C:\Users\Public\Desktop
- Nakopíruji zástupce Chrome do C:\Users\Public\Default
- ✓ Nakopíruji zástupce Chrome %systemdrive%\Users\Public\Desktop

Jaká je nová cesta ke složce "%userprofile%\Application data" (z dob Windows XP) ve Windows 8?

- %userprofile%\Local Settings
- %userprofile%\Application data
- C:\Document and Settings\%username%\Local Settings
- ✓ %userprofile%\AppData\Roaming
- %userprofile%\Application data\Local

V jakých souborech jsou/mohou být uloženy uživatelské registry?

- ✓ ntuser.man
- ✓ usrclass.dat
- ✓ ntuser.dat
- sam
- system

Přiřad' jméno profilové složky k jejímu obsahu.

- *AppData\Roaming* - Aplikační data, která cestují s roaming profilem
- *AppData\Local* - Aplikační data, která necestují s roaming profilem
- *AppData\Roaming\Microsoft\Windows\Start Menu* - Uživatelské start menu
- *Favourites* - Oblíbené záložky z IE
- *AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup* - Spustitelné soubory umístěné v tomto adresáři se spustí po přihlášení uživatele

Co je účelem UAC (User Account Control)? Správné jsou dvě odpovědi.

- Kontrola aktivit uživatelů z hlediska bezpečnosti s generováním bezpečnostních incidentů.
- ✓ Ochrana Windows před škodlivým kódem skrytém v programu spuštěném administrátorem.
- Sbírání údajů o uživatelích pro tajné služby.
- Monitoring využívání účtů, blokáce dlouho nepřihlášených uživatelů.
- ✓ Řešení kompatibility (typicky starších) aplikací, které vyžadují zápis do chráněných oblastí Windows (například C:\Program Files, C:\Windows, HKEY_LOCAL_MACHINE\Software).


Jak poskytuje UAC ochranu operačního systému (uvažujte výchozí nastavení)?

- ✓ Aplikace spuštěné administrátorem nemají standardně administrátorská práva.
- Lze spustit jen aplikace, které prošly testy v laboratořích Microsoftu.
- Administrátorovi chodí hlášení o vaší činnosti.
- Uživatel smí spustit jen aplikace, které administrátor explicitně vyjmenuje.
- UAC detekuje škodlivé chování programu pomocí heuristiky.





Instalujete starou 32 bitovou aplikaci Aplikace1 na počítač, který využívá více lidí.

Podle dokumentace vytváří aplikace data ve svém adresáři v souboru C:\Program Files (x86)\Aplikace1\data.db.



Co zkontrolujete, aby data šlo vytvářet a nebyly kolize mezi daty jednotlivých uživatelů (uživatelé si soubor s daty nepřepisovali navzájem, prostě každý bude mít svoji kopii souboru)?

- Uživatelé musejí být v lokální skupině Administrators.
-  Musí být zapnuta UAC virtualizace.
- Na disk C musíte aplikovat nástroj Windows BitLocker.
- Uživatelé musejí mít právo čtení a zápisu do adresáře aplikace C:\Program Files (x86)\Aplikace1
- UAC musí být nakonfigurováno, aby používalo secure desktop.


Jakými způsoby zařídíte, aby program při spuštění dostal zvýšená práva - vyvolal UAC dialog? Vyberte čtyři možnosti.

-  Pro spuštění kliknu pravým tlačítkem myši na program, z menu vyberu "Spustit jako administrátor".
-  Nastavím to ve vlastnostech .exe souboru programu.
- Spustitelný soubor programu zkopíruji na svoji plochu.
- Program spustím s parametrem -UAC, například cmd.exe -UAC
-  Program budete spouštět přes PowerShell skript příkazem Start-Process s parametrem -verb runas
- Pošlete exe soubor programu firmě Microsoft, ta ho začlení do online databáze.
-  Do manifestu aplikace přidám sekci requestedPrivileges.



Kdy se nepoužije UAC virtualizace? Vyberte dvě odpovědi.

-  Pro 64 bitovou aplikaci. Zde se předpokládá, že je už psána, aby korektně běžela na novém systému.
- Pokud je exe soubor aplikace spouštěn přímo z webu Microsoftu přes HTTPS. Taková aplikace může dostat přístup všude.
- Pro spustitelný soubor s příponou .exex, to je nový formát exe souboru, který musí být napsaný tak, aby běžel správně.
- Pokud je aplikace spuštěna z C:\Program Files, zde se předpokládá, že ji mohl nainstalovat jen administrátor.
-  Aplikace běží s administrátorskými právy. Zde se předpokládá, že má mít přístup do chráněných oblastí.


Jaké je doporučené používání UAC?

-  Neměnit úroveň UAC.
- Můžete ho vypnout.
- Úroveň UAC můžete snížit, ale nezvyšujte ji.
- S UAC mohou uživatelé mít bez obav administrátorská práva.
- Uživatelé by měli vědět, že UAC dialog lze bez problémů pokaždé odsouhlasit.


Jak vypadá token aplikace spuštěné bez zvýšení práv pomocí UAC?

-  Integrity Level je na úrovni Medium.
- Integrity Level je na úrovni Low.
- Skupina Administrators má příznak (flag) Approval Needed.
-  Skupina Administrators má příznak (flag) Deny.
- Skupina Users má příznak (flag) Deny.
- Skupina Users má příznak (flag) Approval Needed.
- V seznamu skupin chybí skupina Administrators.


Jak zvyšuje Mandatory Integrity Control (MIC) bezpečnost systému?

-  Zavádí další úroveň přístupu procesů na objekty.
- Internet Explorer kontroluje u stažených souborů kontrolní součet. Tím zajistí, že nikdo nepodstrčí škodlivý kód.
- Kód aplikace před spuštěním projde heuristickou analýzou, která odhaluje škodlivé akce.
- Lze spustit jen aplikace, které vyhovují vybraným požadavkům, například 64 bitová aplikace, aplikace neprovádí žádné operace na síti, aplikace projde kontrolou antivirem a podobně.
- Spouštěné aplikace musejí být digitálně podepsány. Tím je zajištěna jejich neporušenost.




Mandatory Integrity Control úroveň přístupu se vyhodnocuje:

-  Před DACL na objektu.
- Poté, co DACL na objektu ukáže, že má uživatel přístup.
- Pokud DACL na objektu zakazuje uživateli přístup.
- Pokud nemá objekt DACL.


Mezi typické aplikace využívající Mandatory Integrity Control patří:

- Příkazová řádka Windows cmd.exe
- Instalátor aplikací msixexec.exe, aby nemohla být nainstalována škodlivá aplikace.
- Správcovské nástroje Windows, aby nemohly být zneužity.
- Průzkumník - správce souborů Windows Explorer.
-  Aplikace zpracovávající data z nedůvěryhodných zdrojů Internetu, která mohou obsahovat škodlivý kód (Internet Explorer, Chrome, Adobe Reader).


Co je pravda o dědění integrity level od rodičovského procesu? Vyberte tři možnosti.

- Integrity level se nedědí, při vytváření procesu lze úroveň zadat. Pokud není zadána, použije se hodnota nastavená na spustitelném souboru.
-  Při vytváření potomka lze specifikovat integritní úroveň.
-  Při dědění se uplatňuje pravidlo, že potomek dostane nižší z hodnot integrity level rodiče a hodnoty na svém spustitelném souboru.
- Při dědění se uplatňuje pravidlo, že potomek dostane vyšší z hodnot integrity level rodiče a hodnoty na svém spustitelném souboru.
-  Automaticky se dědí od rodiče.
- Automaticky se dědí od rodiče a nelze ji nastavit na jinou hodnotu, než má rodič.

Secure Desktop je:

- Nastavení Windows, kdy uživatel nemůže měnit svůj desktop-plochu: ikony, obrázek na pozadí atd.
- Na ploše uživatele jsou jen ikony aplikací, které administrátor explicitně vyjmenuje.
- Konfigurace, kdy aplikace řídící grafické prostředí uživatele je spuštěná s integrity level low.
- Vlastnost Windows pro bezpečnější zadávání hesla do Windows a aplikací.
-  Je to způsob, jakým se izoluje okno s UAC dialogem od okolního prostředí a aplikací.

Není-li specifikováno jinak, má zabezpečitelný objekt Windows integritní level:


-  medium
- none
- high
- standard
- low

Proces s integrity level medium:


- *Smí* - zapisovat do objektu s level low.
- *Smí* - číst z objektu s level low.
- *Nesmí* - zapisovat do objektu s level high.
- *Smí* - číst z objektu s level high.

Realizace Internet Explorer protected mode spočívá ve spuštění Internet Exploreru s Integrity Level na úrovni Low, tím se zabrání škodlivému obsahu webové stránky v napadení počítače.


Jak je pak řešena situace, kdy chce uživatel stáhnout z webu soubor a uložit jej do adresáře, kam má práva zápisu na úrovni souborového systému, nicméně Mandatory Integrity Check mu v zápisu zabrání díky Integrity Level procesu prohlížeče?

- Uložení souboru je navzdory nízké úrovni Integrity Level možné. Technická realizace spočívá v tom, že operační systém spustí nový proces prohlížeče, tzv. "Frame" s vyšší Integrity Level a požádá jej o provedení operace, na kterou nemá stávající proces prohlížeče oprávnění. Vše probíhá pod kontrolou operačního systému, tím je zaručena bezpečnost.
- Uživatel musí pro danou webovou stránku vypnout protected mód, a získat tak pro prohlížeč vyšší Integrity Level. To provede explicitním zařazením webové adresy do Trusted Sites Zone nebo Intranet Zone.
-  Je to možné díky tomu, že Internet Explorer má spuštěny dva procesy, jeden "Manager/Frame", který má Integrity Level "Medium" a druhý "Content/Tab", který má Integrity Level "Low". Content proces slouží ke zpracování obsahu stránky a běhu doplňků, kde lze čekat útočné kódy. Manager proces se stará o zbytek - mimo jiné plnění požadavků uživatele, jako je stažení souboru.
- Uložit soubor je v tomto případě možné jen do adresářů v uživatelském profilu z důvodu bezpečnosti. Při používání Internet Explorer Protected Mode operační systém reaguje tak, že na patřičných adresářích v uživatelském profilu nastaví Integrity Level "Low". Internet Explorer pak může soubor uložit do adresáře Downloads v profilu.
- Soubor se automaticky uloží do adresáře
C:\Users\%username%\AppData\LocalLow


Videa pro demonstraci UAC byly natáčeny na virtuálním stroji. Proč autor nepoužil přímo svůj počítač? V jednom z videí je naznačena odpověď.

- Na počítači vypršela trial licence programu, který video snímá.
-  Důvodem je UAC Secure Desktop, který programem pro snímání obrazovky nejde sejmout. Program běžící na uživatelském desktopu nemá přístup na Secure desktop. U virtuálu to lze obejít přístupem na jeho konzolu, kdy vždy vidíte aktuální desktop. Nahrávací program tedy běžel na autorově počítači a snímal konzolu virtuálního stroje.
- Je to kvůli UAC, program vyžaduje kvůli přístupu k mikrofону vyšší práva. Ty jsem mu nemohl dát, protože není digitálně podepsaný. Musel jsem použít jeden z výukových virtuálních strojů, kde to šlo.
- Autor má na počítači jinou verzi Windows než se používá ve výuce. UAC se v jeho Windows chová jinak, má jiné možnosti nastavení.


Co je AppContainer - aplikační kontejner?

- Úložiště dat pro ModernApps.
- Balíček k instalaci aplikace.
-  Izolované prostředí, kde může aplikace běžet bez dopadu na zbytek systému.
- Adresář, kam se aplikace nainstaluje.


Kam se instalují aplikace z Windows Store?

- C:\
-  Do uživatelského profilu.
- C:\Program Files
- Nikam, spouštějí se přímo z cloudu, uživateli se pouze vytvoří dlaždice v Metro nebo zástupce na ploše.


Aplikační manifest (Microsoft Windows Application Manifest) je:

-  Dokument ve formátu XML který definuje vlastnosti aplikace jako je jméno, verze, oprávnění potřebná pro spuštění, závislosti na dalších komponentách. Může být ve formě samostatného souboru nebo součástí spustitelného souboru ve zvláštní sekci.
- Text na webové stránce, kde program stahujete. Definuje podmínky použití programu a je třeba jej odsouhlasit.
- Textový soubor uvnitř instalačního balíčku aplikace, který vyjmenovává soubory k distribuci.
- Licenční ujednání, typicky se zobrazuje během instalace nebo při prvním spuštění programu.


Zaměstnanec posílá mailem obchodnímu partnerovi z externí firmy soubor review.xls Soubor má EFS šifrování. Co je nutno udělat, aby jej příjemce mohl přechít?

- Příjemce musí poslat odesílateli svůj veřejný klíč.
- Odesílatel musí poslat příjemci svůj tajný klíč.
- Vystavit příjemci pár klíčů na firemní certifikační autoritě.
- Soubor může číst jen člověk, který ho zašifroval.
- V příjemcově firmě si musejí nastavit recovery agenta.
-  Nejsou nutné žádné další kroky, soubor přijde v otevřené formě (nezašifrovaný).
- Odesílatel musí příjemci poskytnout File Encryption Key.
- Příjemce musí použít k otevření souboru Microsoft Excel verze 2016 nebo novější, starší verze Excelu ani Libre Office neumějí šifrované soubory otevřít.


Vlastní data souboru zašifrovaného EFS jsou šifrována

-  Symetrickou šifrou s použitím FEK (file encryption key). FEK je zašifrován asymetricky a připojen k metadatům souboru.
- Symetrickou šifrou, jako klíč slouží uživatelovo heslo.
- Asymetrickou šifrou s použitím tajného klíče ke skrytí obsahu souboru a veřejného k ověření integrity obsahu.
- Asymetrickou šifrou s použitím tajného klíče.


Jak se jako administrátor připravíte na situaci, kdy uživatel opustí vaši firmu a je nutné dostat se k jeho souborům zašifrovaným pomocí EFS?

- Musíte použít konfiguraci s certifikační autoritou, pak je znám uživatelův veřejný klíč a z něj lze snadno spočítat tajný klíč pro dešifrování.
- Kontaktujete technickou podporu Microsoftu s žádostí o rozšifrování.
-  Musíte mít definovaného recovery agenta.
- Administrátor uživateli vyresetuje heslo a přihlásí se na jeho účet.
- Situace nemá řešení. Pokud zaměstnanec před odchodem soubory nerozšifruje, nelze se k nim nijak jinak dostat.
- Administrátor může získat z účtu uživatele jeho šifrovací klíče a ty použít k přístupu k souborům.

Umí Windows transparentní kompresi souborů?

- Ano, bez omezení
-  Ano, jen na souborovém systému NTFS
- Ne


NTFS komprese se nastavuje na úrovni

- Disk level - celý svazek
- Disk level - celý svazek je komprimován kromě souborů s atributem S (System, systémový soubor)
-  File level - na jednotlivé soubory




Lze použít NTFS kompresi zaráz s EFS šifrováním?

-  Ne
- Ano
- Ano, jen na vyšších edicích Windows než je Home edition.

Pro výpočet velikosti dat, která uživatel obsadil na souborovém systému, pro limity kvót se započítávají:

-  Soubory, kde je uživatel vlastníkem.
- Soubory v domovském adresáři uživatele.
- Soubory, kde má uživatel právo zápisu.

Podmínky, aby se kvóta uplatnila, vyberte tři odpovědi.

-  Souborový systém musí být NTFS.
- Musí být zapnuta ve vlastnostech operačního systému.
- Uživatel nesmí být ve skupině Administrators, protože na její členy se kvóty neuplatňují.
-  Musí být nastavena pro uživatele.
- Je vyžadována instalace komponenty Windows Quota manager.
-  Musí být nastavena na diskové jednotce.


Srovnání soft a hard quotas

- *soft* - umožňuje pouze zalogovat, že uživatel překročil limit.
- *hard* - zobrazuje se namísto kapacity disku, pokud je zapnuté odepření diskového prostoru při překročení kvóty.
- *soft* - lze jí použít pro testování nebo přehled, kolik kdo obsadil místa na disku bez dopadu na uživatele.
- *hard* - umožňuje odepřít uživateli další místo na disku, pokud překročil limit.



Srovnání File Version a System Image. Vyberte, pro který z nich dané tvrzení platí:

- *System Image* - Zálohuje celý svazek do VHDX souboru.
- *File Version* - Zálohuje jednotlivé soubory.
- *System Image* - Umožňuje obnovit systém do stavu před zálohou včetně nastavení aplikací.
- *File Version* - Nevyžaduje práva administrátora.
- *File Version* - Umí se dočasně obejít bez připojeného externího disku určeného pro zálohu použitím cache.
- *File Version* - Konzumuje málo systémových prostředků (CPU & I/O).
- *System Image* - Data vzniklá zálohou lze spustit jako virtuální stroj.
- *System Image* - Data vzniklá zálohou lze namontovat jako další disk do systému.



Pokud Windows zálohování narazí na otevřený soubor:

- Proces zálohování spadne, záloha se nepovede.
-  Otevřené soubory jsou zálohovány díky technologii Volume Shadow Copy.
- Otevřené soubory jsou přeskočeny, proto je vhodné zálohovat mimo pracovní dobu.
- Zálohovací proces čeká, dokud nebude soubor uvolněn/uzavřen.



Za jakých okolností se obejdete bez zálohování? Vyberte dvě možnosti.

- Nemusím zálohovat disky se souborovým systémem NTFS, ten je odolný vůči poškození dat.
-  Stanici nemusíte zálohovat, pokud jsou data uložena na serveru, kde se zálohují a stanici umíte rychle znova nainstalovat.
- Pokud používáte disky v konfiguraci RAID, která zvyšuje jejich spolehlivost a minimalizuje riziko ztráty dat.
-  Pokud se na počítači nevytvářejí žádná data a po selhání disku stačí instalace nového systému.
- Moderní počítače se zálohovat nemusí, jsou spolehlivé.


Jaké zálohovací mechanismy jsou v základu Windows pracovní stanice? Vyberte dvě možnosti.

-  Windows File History.
- HP Data Protection.
-  Windows System Image.
- IBM Tivoli Storage Manager Personal Edition.
- Volume Snapshot Recovery.
- GNU tar.

Jaké jsou metody získání přístupu k šifrovaným datům BitLocker To Go? Vyberte dvě možnosti.

- TPM
- PIN
-  SmartCard
- Přihlásit se jako administrátor.
-  Passphrase - heslo.


Který standardní Windows nástroj příkazové řádky umí zašifrovat BitLockerem disk?

- Encrypt
-  Manage-bde
- BdeHdConfig
- Enable-bde
- Bde-On



Srovnání EFS a BitLocker. Vyberte, pro který z nich dané tvrzení platí:

- *EFS* - šifruje soubory a složky samostatně a nešifruje celý obsah jednotky.
- *BitLocker* - není závislý na jednotlivých uživatelských účtech přidružených k souborům. Nástroj je buď zapnutý nebo vypnutý a to pro všechny uživatele/skupiny.
- *BitLocker* - může používat TPM.
- *EFS* - nevyžaduje nikdy práva administrátora.


Který PowerShell commandlet můžete použít k zašifrování disku BitLockerem?

- Start-BitLocker
- Encrypt-Drive
- BitLocker-Drive
-  Enable-BitLocker
- Install-BitLocker


Recovery a Unlock v případě BitLockeru znamenají:

-  Recovery řeší situaci, kdy se přístup k disku zablokuje, např. zapomenuté heslo.
-  Unlock je získání přístupu k šifrovaným datům například zadáním hesla.
- Recovery je oprava šifrovaných dat na poškozeném disku, trvá velmi dlouho.
- Unlock znamená nouzovou proceduru, kdy vám MS poskytne zapomenuté heslo.
- To stejné, recovery je starší název pro unlock: převedení zašifrovaných dat zpátky do nešifrované podoby.
- Recovery je obnova smazaného souboru.



Nástroj BitLocker šifruje:

- Jen data uložená na certifikovaných paměťových zařízeních.
-  Vždy celou diskovou jednotku.
- Jen dokumenty Microsoft Office.
- Zadané soubory.


Jaký je rozdíl mezi BitLocker a BitLocker To Go?

-  BitLocker To Go je určen k šifrování přenosných disků.
- BitLocker To Go je verze BitLockeru, která je zdarma.
- BitLocker To Go je implementace BitLockeru pro Linux a MAC-OSX.
- BitLocker To Go je omezená verze pro Windows Home Edition.


Před jakou hrozbou vaše data BitLocker neochrání? Vyberte dvě možnosti.

-  Odposlechnutí dat během přenosu po síti.
-  Odcizení dat z lokálního disku běžícího počítače.
- Instalace modifikovaného operačního systému se škodlivým kódem
- Vyřazování porouchaného disku s daty.
- Ztráta USB disku s daty.
- Ztráta notebooku s daty.




Pro použití Device Encryption musí být splněno:

-  Specifikace InstantGo.
- Použije se Bitlocker To Go.
- Specifikace SCSI.
- Zařízení musí mít na disku minimálně 10% volného místa.


V čem spočívá ochrana Secure Boot?

- Při bootování je vyžadováno heslo nebo PIN.
- Systém se zavede jen z disku zašifrovaného BitLockerem.
- Při bootu jsou kontrolovány změny hardware.
- Při bootu je kontrolován stav zabezpečení systému: zda je aktualizovaný, má nainstalovaný antivírus a podobně.
-  Části systému používané k bootování se ověřují elektronickým podpisem


Mezi útoky na BitLocker patří: Vyberte tři možnosti.

-  Přechytení klíčů z paměti zneužitím DMA.
-  Zjištění klíčů z paměti počítače po jeho vypnutí.
-  Modifikovaný bootloader.
- Přechytení klíčů z dočasněho souboru, kam je Windows po startu ukládají.
- Cold-boot attack, jedná se o nabootování z disku na jiném počítači



Jaké šifrování používá BitLocker? Uvažujte výchozí nastavení.

-  AES algoritmus.
- Blowfish šifru.
- Trojcestný DES algoritmus.
- Jednocestný DES algoritmus.
- Microsoftem vyvinutou šifru s veřejnou specifikací a finanční odměnou pro prvního, kdo šifru prolomí.
- Proprietární Microsoft šifru, její bezpečnost je zvýšena tím, že Microsoft tají algoritmus.

Co je to TPM?

- Program pro ovládání BitLocker z příkazové řádky.
- Náhrada BIOSu umožňující využívat nové vlastnosti počítačů.
- Jméno adresáře s dočasnými soubory.
-  Čip na desce, který mimo jiné uchovává šifrovací klíče.
- Šifrovací algoritmus používaný BitLockerem.

Kde všude jsou uloženy šifrovací klíče BitLockeru? Správné jsou dvě možnosti.

-  TPM.
- BIOS Secure Store.
- Boot volume.
- SmartCard.
-  Operating system volume.

Jakými způsoby můžete založit plánovanou úlohu? Vyberte tři možnosti.

- Příkazem sc
- ✓ Commandlety Power Shellu.
- ✓ Příkazem schtasks
- ✓ Nástrojem Task Scheduler.
- Příkazem task

Auditing přístupu k souborům musí být nastaven: Vyberte dvě možnosti.

- Na účtu uživatele nebo skupiny, které se to týká.
- ✓ V lokálních politikách pro celý počítač.
- ✓ Na souboru nebo adresáři, kde se přístupy sledují.
- Na diskovém svazku, kde se auditované soubory nacházejí.
- V event logu na patřičném logovacím souboru.

Na počítači se nespouštějí plánované úlohy. Co zkontrolujete?

- Zda je dost místa na systémovém disku.
- Musí být povolen PowerShell remoting.
- Zda je uživatel, pod kterým běží úlohy, přihlášen.
- ✓ Zda běží služba Task Scheduler.

Hlášení generované systémem Windows se:

- ✓ ukládají se do speciálních souborů, které lze prohlížet aplikací Event Log Viewer nebo commandlety PowerShellu.
- posílají na mail administrátorovi.
- ve výchozím nastavení nezobrazují, lze je zapnout ve formě pop up oken.
- posílají na zadaný souborový server na síti.

Jak lze ve Windows nastavit režim řízení spotřeby? (Správné jsou 3 možnosti)

- Příkazem powermgr.exe
- ✓ Politikou.
- Grafickým nástrojem Savings Settings z ovládacích panelů.
- ✓ Grafickým nástrojem Power Options z ovládacích panelů.
- ✓ Příkazem powercfg.exe

Smysl procesu Staging je: (Vyberte 3 možnosti)

- ✓ Ovladač před instalací projde základními kontrolami.
- Poskytuje zpětnou vazbu vývojáři ovladače.
- Sdílení ovladačů v komunitě uživatelů Windows.
- ✓ Umožňuje instalaci ovladače neprivilegovanému uživateli.
- ✓ Kontrola, pro které typy zařízení mohou uživatelé instalovat ovladače.

Jak zastavíte běžící službu?

- Služba se musí odinstalovat/smazat.
- Ve správci služeb nastavím startup type na hodnotu Disabled.
- ✓ Ve správci služeb vyvolám pro službu akci Stop.
- Zakážu její spouštění přes registry.

Pro hybridní režim spotřeby platí: (Správné jsou 3 možnosti)

- Je to rychlejší a méně úsporná podoba režimu spánku, kdy se stav systému neukládá do paměti, to umožňuje běh vybraných zařízení.
- ✓ Stav systému se ukládá na disk.
- ✓ Stav systému se ukládá do paměti.
- Je to režim hibernace, kdy se stav systému neukládá na disk.
- Je navržen s ohledem na specifika přenosných počítačů.
- ✓ Je to režim spánku upravený, aby byl odolný proti výpadku napájení.

Jaký bude výsledek příkazu *sc.exe config Spooler start= demand* Uvažujte spuštění pod účtem s administrátorskými právy.

- Služba Spooler se bude spouštět automaticky při startu Windows.
- Dojde k chybě.
- Služba Spooler se nastartuje automaticky v případě události tisku.
- ✓ Start služby Spooler bude možný manuálně.

Jak lze zařídit, aby se program automaticky spustil na pozadí při startu počítače:

- Odkaz (shortcut) na něj dám do Spustit při startu v menu start - programy.
- ✓ Spustím jej jako Windows službu.
- Někdo z dohledového centra se vždy na počítač přihlásí a program spustí.
- Uvedu program s plnou cestou v souboru c:\autoexec.bat

Během procesu staging dojde k: (Správné jsou 3 odpovědi.)

- ✓ Indexaci pro snadnější hledání v budoucnu.
- ✓ Uložení ovladače do adresáře, odkud bude později instalován.
- Hledání starších verzí ovladače a jejich upgrade.
- ✓ Ověření ovladače.
- Instalaci ovladače.



Co je v Windows Služba (Service).

- Je to doba, po kterou Windows běží, jsou ve službě.
- První proces, který se spouští při startu, má na starosti spuštění ostatních procesů.
- To jsou služby, které počítač poskytuje uživateli, např. MS Office, Internet Explorer.
- ✓ Spustitelný kód napsaný podle určitých zásad, který nevyžaduje interakci s uživatelem a spouští se při startu systému.



Srovnání režimu hibernace a spánku. Vyberte, pro který z nich dané tvrzení platí:

- *režim hibernace* - má nižší spotřebu energie.
- *režim spánku* - umožňuje uživateli rychlejší návrat k rozdělané práci.
- *režim hibernace* - je odolný proti výpadku napájení.
- *režim hibernace* - si alokuje místo na disku, kam ukládá stav operační paměti.




Které z uvedených příkazů a commandletů provedou restart služby Print spooler?

- net.exe restart Spooler
- Reload-Service -Name Spooler -Force
-  net.exe stop Spooler && net start Spooler
- sc.exe restart Spooler
-  Restart-Service -Name Spooler -Force

Jak zvýším bezpečnost běhu služby? Vyberte dvě odpovědi.


- Program (.exe soubor) služby zkontroluji při instalaci antivirem.
-  Použiji managed service account.
-  Pro běh služby použiji neprivilegovaný účet, kterému dám minimum práv potřebných pro běh služby
- Nastavím jí ruční spouštění.

Vyberte všechny platné typy spouštění (startup type) Windows služby





-  Manual
-  Automatic
- Stop
- Enabled
- Paused
- Start
-  Disabled

Služba S1 má typ startu Automatic a závisí na službě S2, která má typ startu Manual.


Co se stane při startu systému?

- Bude spuštěna pouze služba S1 a do event logu se zapíše varování.
- Systém automaticky změní typ startu S2 na Automatic a spustí obě dvě služby.
- Ani jedna z nich nebude spuštěna.
-  Obě dvě služby budou spuštěny.

Jak Windows ověřují ovladač? Vyberte 4 odpovědi.


- Zkusí ho pokusně zavést a provedou na něm zátěžový test.
-  Ovladač je digitálně podepsán.
-  Nesmí být na blacklistu problémových ovladačů.
-  Kontrolují kompletnost balíčku ovladače.
-  Při instalaci nesmí ovladač provádět interakci s uživatelem nebo instalovat další aplikace.
- Odešlou ovladač ke kontrole na Microsoft.
- Kontrola programem Defendr nebo jiným nainstalovaným antivirem.

Jak můžete efektivně s využitím prostředků Windows šetřit výdaje za elektrickou energii?


- Vyměním disk s pohyblivými součástmi za SSD disk.
-  Ve Windows nastavím režim řízení spotřeby odpovídající mému způsobu práce.
- Nebudu instalovat programy, které nepotřebuji, spotřebovávají zbytečně energii.
- Snížím si jas obrazovky.
- Nebudu nechávat počítač zbytečně zapnutý.
- Pustím Internet Explorer a přes Google si najdu levnějšího dodavatele energie.

V ovládacím panelu pro nastavení možností napájení vidím jen Balanced power plan.

Co je příčinou?

- V registrech máte zakázány pokročilé režimy spotřeby, je nutné je zde povolit.
- Váš hardware jiný režim nepodporuje.
-  V současné verzi Windows 10 je ponechán jen jeden plán napájení, ostatní lze do systému dodat s použitím šablon
- Možnost mít více plánů napájení je pokročilá vlastnost systému, která je dostupná jen ve Windows Enterprise.


Co znamená, že je ovladač v Driver store?

- Ovladač je umístěn na certifikovaném paměťovém zařízení. Lze ho nainstalovat bez obav z malware.
- Ovladač je ve Windows nainstalován.
- Je na webu Microsoftu, odkud ho mohou Windows instalovat.
-  Ovladač je po kontrole umístěn v adresáři, odkud ho lze nainstalovat do systému.



Co je výstupem kódu?

```
[int[]] $arr = @(1,2,3,4,5,6,7,8,9)
```


```
Write-Host $arr[3..5]
```

-  4 5 6
- 3 4 5
- 4 5 6 7
- Chyba syntaxe.
- 2 3 4 5

Počet členů v poli \$myArray vrátí konstrukce: (Správné jsou dvě odpovědi.)

- \$myArray.sizeof
- \$myArray.size
-  \$myArray.count
- \$myArray.members_number
-  \$myArray.length

Hodně programovacích jazyků umožňuje do řetězce vložit speciální znak (tabulátor, konec řádku, uvozovky) tak, že před něj napíšete tzv. escape znak. Jaký znak používá PowerShell?


- \ (backslash, obrácené lomítko)
- & (ampersand)
- ^ (stříška)
-  ` (apostrof, obrácená uvozovka)
- # (hash, mříž)

Jaká posloupnost čísel je výsledkem spuštění uvedeného kódu?


-eq znamená == (equal)

-ge znamená >= (greater or equal)

```
1..10 | ForEach {  
    If ($_ -eq 2) { continue }  
    If ($_ -ge 5) { break }  
    Write-Host $_  
}
```


- 1 3 4 5
- 1 2 3 4
- 1 2
- 1 3 4
-  1
- 1 2 3 4 5 6 7 8 9 10

Klíčová slova try a catch slouží k:



-  K ošetření chyb pomocí tzv. výjimek.
- Trasování z příkazové řádky, try vyvolává debugger, catch ukazuje hodnotu zadané proměnné.
- Try spouští commandet a catch přesměrovává jeho výstup do souboru.
- Testování nově napsaného kódu spuštěním ve speciálním režimu.

Níže je uveden celý program, jak dopadne jeho spuštění (default konfigurace) a co bude v proměnné *a*?


```
$a = 1 + $var1
```

- Proměnná **a** bude obsahovat prázdnou hodnotu.
- Proměnná **a** bude obsahovat string "1 + \$var1"
-  Proměnná **a** bude obsahovat hodnotu 1.
- Chybové hlášení, proměnná **var1** není deklarovaná. Proměnná **a** bude mít nedefinovanou hodnotu.

Vyberte komentáře podle syntaxe jazyka PowerShell. Správné jsou dvě odpovědi.


- Set-Remark "function returns used disk space"
- ! function returns used disk space
- // function returns used disk space
- /* function returns used disk space */
-  <# function returns used disk space #>
- ` function returns used disk space
-  # function returns used disk space

PowerShell má příkaz goto umožňující skok do libovolného místa kódu:

- Ano, jmenuje se Jump-To
-  Ne
- Ano, jmenuje se Go-To

Lze z pole deklarovaného následovně odebírat prvky?

```
$myArr = @('plant', 'mushroom', 'animal')
```

- Ne, pole má fixní velikost, nelze ani přidávat.
-  Ne, prvky lze přidávat, ale nelze odebírat.
- Ano, pole v PowerShellu jsou plně dynamická.
- Ano, ale musí být nastaveno Set-StrictMode -Off

Jaký je výstup kódu:

\$a = 123

write-host 'test \$a'

- test 123
- ✓ test \$a
- chyba, proměnná a je typu celé číslo
- \$True, test proměnné proběhl v pořádku.

Sestavte kód, který vypíše sudá čísla od 1 do 10.

```
ForEach ($var in 1..10) {  
    # preskoc licha cisla  
    If ($var % 2) { continue }  
    Write-Output $var  
}
```

Lze PowerShell skripty použít v Linuxu?

- Ano, jedinou možností je komunitní projekt multiplatformního PowerShellu.
- Ne, PowerShell je čistě pro Windows.
- Ano, ale pouze za použití Docker kontejneru.
- ✓ Ano, PowerShell je od určité verze multiplatformní a open-source.

Uvažujte funkci s deklarací:

```
Function GetUptime([String]$machine_name='localhost', [bool]$beverbose=$false) { <  
nějaký kód > Return $sysuptime }
```

Jaké jsou způsoby funkčního a korektního zavolání funkce? Správných je 5 možností.

- GetUptime('server1',\$true)
- ✓ GetUptime -machine_name 'server1' -beverbose \$false
- ✓ GetUptime 'server1' \$true
- ✓ GetUptime
- ✓ GetUptime -beverbose \$false -machine_name 'server1'
- ✓ GetUptime 'server1'

Co je to transkript?

- Je to přepisování části řetězce operátorem -replace.
- Skript napsaný s dodržением speciálních požadavků. Slouží ke konfiguraci Windows.
- ✓ Je to soubor s výstupem z příkazů ve skriptu.
- Je to soubor s popisem a konfigurací skriptu.

Hash table je:

- ✓ Pole, kde se členy indexují řetězcem.
- Tento prvek z jiných programovacích jazyků PowerShell neobsahuje.
- Část kryptografického rozhraní PowerShellu.
- Tabulka obsahující všechny deklarované proměnné a funkce PowerShellu.

Kterou z těchto metod **NEOBSAHUJE** WMI třída Win32_Directory.

- Compress
- Copy
- Delete
- TakeOwnership
- ✓ SetACL

Ve skupině administrators je pět členů včetně uživatele pepik.

Ve skupině users je deset uživatelů včetně prasopsa. Jak pomocí GPO docílím toho, že všichni administrátoři kromě pepika budou moci spouštět regedit. A zároveň, aby všichni non-admin uživatelé kromě prasopsa nemohli.

Pozn.: 1) nastavení upravující možnost spuštění regedit je v: User Configuration > Administrative Templates > System > Prevent access to registry editing tools 2) "per system GPO" označuje lokální GPO aplikovanou na daný stroj 3) pozor na rozdíl mezi enabled / disabled / not configured

- Vytvořím per user GPO aplikovanou na prasopsa, ve které dám u daného nastavení ENABLED
- ✓ Vytvořím per user GPO aplikovanou na prasopsa, ve které dám u daného nastavení DISABLED
- ✓ Vytvořím per system GPO, ve které dám u daného nastavení ENABLED
- Vytvořím per system GPO, ve které dám u daného nastavení DISABLED
- Vytvořím per user GPO aplikovanou na pepika, ve které dám u daného nastavení DISABLED
- ✓ Vytvořím per user GPO aplikovanou na pepika, ve které dám u daného nastavení ENABLED
- Vytvořím per administrators GPO, ve které dám u daného nastavení ENABLED
- Vytvořím per non-administrators GPO, ve které dám u daného nastavení NOT CONFIGURED
- ✓ Vytvořím per administrators GPO, ve které dám u daného nastavení DISABLED

Zadejte cestu k hodnotě v registru, která nastavuje zamknutí Taskbaru. Použijte tvar HKCU\neco\neco\jmenohodnotyjejimznastavenimzamknutaskbar.

Můžete použít webový vyhledávač GPO <http://gpsearch.azurewebsites.net/> který vedle dohledání GPO obsahuje i korespondující klíč v registru, který daná GPO mění.

- ✓ HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\lockTaskbar


Jak pomocí GPO docílím toho, že žádný non-admin uživatel nebude moci spouštět regedit.

Pozn.: 1) nastavení upravující možnost spuštění regedit je v: User Configuration >

Administrative Templates > System > Prevent access to registry editing tools


2) "per system GPO" označuje lokální GPO aplikovanou na daný stroj

3) pozor na rozdíl mezi enabled | disabled | not configured


- Vytvořím per system GPO, ve které dám u daného nastavení DISABLED
- Vytvořím per system GPO, ve které dám u daného nastavení ENABLED
- Vytvořím per system GPO, ve které dám u daného nastavení NOT CONFIGURED
-  Vytvořím per non-administrators GPO, ve které dám u daného nastavení ENABLED
- Vytvořím per non-administrators GPO, ve které dám u daného nastavení DISABLED
- Vytvořím GPO pro skupinu Users, ve které dám u daného nastavení ENABLED

V per system GPO nastavím skrytí ikony koše z plochy. V per non-administrators GPO nastavím, že se koš na ploše má ukazovat. V per administrators GPO nastavím, skrytí ikony koše z plochy.

Bude mít uživatel krychle na ploše ikonu koše, když je členem pouze skupin Users, Backup operators a Remote desktop users?


-  ano
- ne

Kde jsou fyzicky na disku uloženy GPO?

- %systemroot%\PolicyDefinitions
-  %systemroot%\system32\GroupPolicy
- %systemroot%\system32\config
- %userprofile%\NTUSER.DAT

Kde se v GPO nachází možnost, nastavit vybraný image jako pozadí zamykací obrazovky (lock screen)?

Můžete použít webový vyhledávač GPO <http://gpsearch.azurewebsites.net/>.

- User Configuration\Administrative Templates\Personalization\Force a specific default lock screen image
- Computer Configuration\Administrative Templates\Control Panel\Personalization\Display\Force a specific default lock screen image
- User Configuration\Administrative Templates\Control Panel\Personalization\Force a specific default lock screen image
-  Computer Configuration\Administrative Templates\Control Panel\Personalization\Force a specific default lock screen image
- Žádná z uvedených

**Zadejte jméno WMI třídy, která obsahuje informace o připojených CD mechanikách.
Zapište ji ve formátu Win32_jmenotridy.**

✓ (Win32_CDROMDrive)

Které Powershell cmdlety mohu použít pro získání WMI objektu?

- ✓ Get-WmiObject
- ✓ Get-CimInstance
- ✓ Get-WsManInstance
- Get-Wmi
- Get-WmiInfo