6.A

Modul 6 – Lab A: Bitlocker, UAC

Požiadavky
Počítač s Windows 7 s pripojeným obrazom C:\GOC\LABS.iso do virtuálnej DVD mechaniky !!!

Bitlocker, UAC:
LAB A: Spustenie BitLocker drive encryption
Zoznámenie sa s ovládaním BitLocker v ovládacích paneloch
Vypnutie vynucovania TPM v lokálnej politike počítača
Preskúmanie volieb v manage-bde
Spustenie BitLocker drive encryption pomocou Manage-bde s heslom na diskete
LAB B: Preskúmanie virtualizácie a nastavení UAC v group policy

Lab A: BitLocker

- Prihláste sa na počítač s Windows 7 pod administrátorským účtom s heslom Pa$$w0rd

Preskúmanie požiadaviek na BitLocker

- V menu Start otvorte ovládacie panely položkou Control panel
- Kliknite na voľbu „**System and Security**" a potom kliknite na voľbu „**BitLocker Drive Encryption**"
- Kliknite na odkaz **Turn on BitLocker** vedľa oddielu **C:**
- Prečítajte si varovné hlásenie v spodnej časti okna - v našom počítači nie je **TPM čip**, ktorý je východiskovým úložiskom vynucovaným systémom Windows 7 a Vista - kliknite na tlačítko **Cancel**

Vypnutie vynucovania TPM pre ukladanie kľúčov v Local GPO

- Kliknite na Start a do poľa „Search programs and files" napíšte **GPEDIT.MSC** a stlačte Enter
- V sekci Computer settings – Administrative templates – Windows components – BitLocker Drive Encryption – Operating system Drives – kliknite dvakrát na voľbu:

„Require additional authentication at startup"

- V novo otvorenom okne kliknite na **Enabled**
- Overte, že je zaškrtnuté nastavenie v „Allow BitLocker without a compatible TPM"
- Potvrďte stlačením OK a v okne politiky sa presvedčte, že pre voľbu

„Require additional authentication at startup" je ve stĺpci State hodnota **Enabled**

- Uzavrite okno editora politiky
- Spustite príkazový riadok ako správca, potvrďte User account control dialóg a spustite príkaz pre vynútenie nových nastavení:

gpupdate /force

Kontrola splnených podmienok pre BitLocker

- Prihláste sa ako užívateľ s administrátorským účtom s heslom Pa$$w0rd
- Spustite **Ovládacie panely** a v sekcii **Security** opäť kliknite na „**BitLocker Drive Encryption**"
- Pri disku **C:** kliknite na voľbu „**Turn on BitLocker**"
- Prezrite si voľby v dialógovom okne „BitLocker Drive Encryption"

Use BitLocker Without additional keys = uloženie kľúča v TPM

Require PIN at every startup = TPM + PIN

Require a Startup key at every startup = uloženie kľúča na USB kľúčenku – nutná pri každom spustení

- Ak toto cvičenie spúšťate na fyzickom počítači a máte k dispozícii USB kľúčenku, tak ju pre túto časť labu **nepoužite** – namiesto toho ju môžete využiť pre vyskúšanie si BitLockerToGo.
- Behom výzvy na vloženie USB kľúčenky kliknite na tlačítko **Cancel** a namiesto toho využijeme ukladanie na disketu.
- Zatvorte okno ovládacieho panelu

<u>Ručná správa pomocou BDE a vynútenie uloženia kľúča na disketu</u>

- Spustite **príkazový riadok ako správca** – tzn. kliknite na Start – napíšte **cmd** a stlačte kombináciu kláves Ctrl+Shift+Enter
- Potvrďte dialóg „**User account control**" kliknutím na **Yes**
- Ak sa dialóg „User account control" nebojavil a záhlavie príkazového riadku nezačína Administrator:, potom zatvorte príkazový riadok a spustite ho znovu ako správca
- Presvedčte sa, že do počítača máte vloženú disketu (na virtuálnom počítači kliknite v hornom menu na Media – Diskette Drive – Insert Disk a potom zadajte cestu k E:\Floppy1.vfd) a spustite príkaz :

dir a:\ /a

Výpis by mal obsahovať hlásenie o sériovom čísle diskety.

- Presuňte sa do priečinka c:\Windows\System32 príkazmi:

DISKETA MUSÍ BÝŤ NAFORMÁTOVANÁ!

6. A

C:

cd \windows\system32

- Spustite nápovedu pre skript na správu BDE príkazom:

manage-bde.exe /?

- Spustite príkaz pre šifrování disku:

manage-bde.exe -on C: –rp –sk A:

Tento príkaz spustí šifrovanie na oddieli C: , kde spúšťací kľúč (startup key, ktorý bootmgr dokáže použiť automaticky) uloží na disketu. Pre prípad poškodenia diskety sa nám vypíše aj recovery password, ktorý budeme musieť zadat ručne, ak prídeme o disketu.

- Všimnite si výpis, kde v časti Actions required systém vypisuje v sekcii 1. kľúč pre obnovu v prípade havárie výmenného zariadenia (či TPM)

- Poznamenajte si vypísaný 48 znakov dlhý kľúč (recovery password):

_____ - _____ - _____ - _____ - _____ - _____

- Kliknite **pravým tlačítkom** do okna príkazového riadku a vyberte voľbu Select All

- Opäť kliknite **pravým tlačítkom** do okna príkazového riadku, čím sa skopíruje všetok zobrazený obsah

- Otvorte poznámkový blok príkazom **notepad** a pravým kliknutím a Paste vložte obsah schránky

- Uložte finálny súbor s výpisom ako RecoveryKey.txt na oddiel s menovkou „System Reserved" a na disketu – **S:\RecoveryKey.txt** a **A:\RecoveryKey.txt**

- Reštartujte systém

Tip: Môžete využiť príkazový riadok, na kterom zadáte príkaz:

shutdown -r -f -t 0

Ak má Váš počítač nastavené primárne bootovanie z diskety, potom počítajte s tým, že v okamihu bootovania sa Vám môže objaviť hlásenie, že systém na danom bootovacom zariadení nenašiel disk s operačným systémom – v takomto prípade disketu povytiahnite z mechaniky, stlačte na klávesnici ľubovoľnú klávesu a potom disketu ihneď vložte späť, aby na ňu videl bootmgr v okamihu spúšťania počítača.

Kontrola šifrovania

- Po reštarte systému sa prihláste pod administrátorským účtom s heslom Pa$$w0rd
- Spustite **príkazový riadok ako správca** – kliknite na Start – napíšte cmd a stlačte kombináciu kláves Ctrl+Shift+Enter
- Spustite príkaz **manage-bde.exe –status**

Spustenie šifrovania môže trvať i dve minúty po prihlásení sa. Ak sa ani po tejto dobe šifrovanie nespustí, potom sa ešte raz presvedčte, že je disketa čitateľná a že ste ju určite ponechali v počítači počas štartu. Pre opätovné spustenie šifrovania opäť spustite manage-bde príkaz z predchádzajúceho kroku.

- Prezrite si percentuálny výpis stavu šifrovania disku a použité šifrovanie – spustenie šifrovania môže trvať určitú dobu, počas ktorej se v okne môže zobrazovať status Fully Decrypted – vyčkajte niekoľko minút. O úspešnom priebehu šifrovania Vás informuje status Encryption in Progress.
- Opätovným použitím rovnakého príkazu si môžete skontrolovať stav šifrovania

Pretože šifrovanie disku trvá dlhú dobu, preskúmame voľby pre šifrovanie USB kľúčenky ..

Vynucovanie šifrovania USB výmenných médií

- Kliknite na Start a do poľa „Search programs and files" napíšte **GPEDIT.MSC** a stlačte Enter
- V sekcii Computer settings – Administrative templates – Windows components – BitLocker Drive Encryption – Removable Data Drives – dvojitým kliknutím preskúmajte možnosti v pravej časti okna – nevykonávajte však zmeny!!! Preskúmajte pokiaľ možno všetkých 6 volieb, predovšetkým ale:

„Configure use of smart cards on removable data drives"

„Deny write access to removable drives not protected by BitLocker"

„Allow access to BitLocker-protected removable data drives from earlier versions"

Ak máte USB kľúčenku pre tento lab a realizujete ho na fyzickom počítači, potom ju vložte do počítača. Otvorte Windows Explorer, kliknite pravým tlačítkom myši na jednotku USB kľúčenky a zvoľte možnosť pre ochranu kľúčenky pomocou BitLockerToGo. Vložte silné heslo (zapamätajte si ho a pre istotu poznamenajte aj na papier) a nechajte sprievodcu dokončiť šifrovanie kľúčenky. Pre šifrovanie kľúčenky nie je nutné nastavovať TPM politiku – stačí ochrana heslom. Potom môžete vložiť kľúčenku do iného počítača a tu preskúmať dialóg pre vloženie hesla. Zároveň tiež môžete preskúmať obsah kľúčenky – BitLockerToGo.exe umožňuje prístup k súborom zo starších systémov – je naň uvedený odkaz v autorun.inf. Ak však autorun potlačíte, museli by ste tento program spúšťať manuálne. Tento postup môžete vyskúšať tak, že na fyzickom počítači nabootujete do systému Windows Server 2008 a tu pripojíte kľúčenku šifrovanú pomocou BitLockerToGo.

6 . B

Lab B: User Account Control

Požiadavky
Virtuálny počítač PC1 alebo fyzický počítač s Windows 7 s pripojeným obrazom E:\LABS.iso do virtuálnej DVD mechaniky !!! V takomto prípade všetky výskyty cesty C:\LABS\UAC nahraďte X:\UAC (kde za X: napíšte písmeno Vašej mechaniky s vloženým ISO).

Vytvorenie účtov pre skúmanie virtualizácie

- Ak tento lab spúšťate na fyzickom počítači, príhláste sa pod administrátorským účtom s heslom Pa$$w0rd, spustite príkazový riadok ako administrátor a spustite nasledujúci príkaz:

net user novak Pa$$w0rd /add

- Prihláste sa ako užívateľ NOVAK s heslom Pa$$w0rd

Preskúmanie UAC a virtualizácie

- Spustite príkaz C:\LABS\UAC\Start.BAT

Preskúmanie volieb UAC v GPO

- Spustite príkazový riadok ako správca
- Všimnite si zmenu dialógu User Account Control pre užívateľa bez administrátorského oprávnenia – ak je potrebné spustiť pregram so zvýšeným oprávnením, je nutné zadať poverenia účtu správcu
- Zadajte poverenia účtu Admin s heslom Pa$$w0rd
- Na príkazovom riadku spustite príkaz: **GPEDIT.MSC**
- V Computer Configuration – Windows settings – Security settings – Local policies – Security options pracujeme s nastaveniami začínajúcimi na „User account control":
- Behavior of the elevation prempt for administrators in Admin appreval mode určuje voľby:

Nastavuje UAC pre administrátorské účty (účet je členom skupiny Administrators):

Prompt for consent – výzva na schválenie či odmietnutie zvýšenia – doteraz zvyčajný dialóg UAC s voľbou Continue vs. Cancel

Prompt for Credentials – pre zvýšenie je nutné opäť zadať poverenie s administrátorským oprávnením – tzv. opatrenie proti notorickým klikačom na Continue

Elevate without Prompt – vypnutie stráženia pomocou UAC

- Behavior of the elevation prompt for standard users

Nastavuje UAC pre štandardné účty (nie sú členmi skupiny Administrators)

Prompt for Credentials – pre zvýšenie je nutné opäť zadať poverenia s administrátorským oprávnením – pretože štandardný účet nikdy nemôže získať vyššie oprávnenia, je nutné zadať poverenia účtu, ktorý je členom lokálnej skupiny Administrators – dialógové okno zobrazené pre užívateľa NOVAK

Automatically deny elevation request – zamietne zvýšenie a oznámi nedostatočné oprávnenia

- Virtualize file and registry write failures to per-user locations – vypnutie virtualizácie

(pre všetky aplikácie bežiace pod štandardnými účtami zlyhajú pokusy o zápis do chránených oblastí)

- Nastavte voľby:

1) Behavior of the elevation prompt for administrators in Admin approval mode: Prompt for Credentials

2) Behavior of the elevation prompt for standard users: Automatically deny elevation request

3) Virtualize file and registry write failures to per-user locations: Disabled

Prihlásenie sa pod administrátorským účtom a preskúmanie zmien

- Odhláste užívateľa Novak a prihláste sa ako Admin s heslom Pa$$w0rd
- Spustite príkazový riadok ako správca
- Založte nový účet NOVAK2 s heslom Pa$$w0rd príkazom:

net user NOVAK2 Pa$$w0rd /add

- Spustite príkaz: GPUPDATE /FORCE
- Prezrite si zmenený dialóg, ktorý bráni administrátorom v obyčajnom kliknutí na Continue (zo zvyku)
- Odhláste užívateľa ADMIN a prihláste sa opäť ako užívateľ NOVAK2 s heslom Pa$$w0rd
- Skúste spustiť príkazový riadok ako správca
- Rovnako ako pre užívateľa NOVAK aj teraz spustite C:\LABS\UAC\start.bat
- Skúste opäť spustiť ukážku virtualizácie (ktorá je teraz vypnutá) spustením skriptu START v priečinku UAC – pretože je teraz virtualizácia vypnutá, zlyhajú všetky kroky vykonávané pre staršiu aplikáciu

6.C

LAB C: Obmedzenie spúšťaných aplikácií pomocou ochrany AppLocker

Príprava
Pre úspešné dokončenie labu je potrebné mať pripravené:

Virtuálny počítač PC1 alebo fyzický počítač s Windows 7 s lokálnymi účtami Admin (člen Administrators, Users) a Novak (člen Users).

Ak lab vykonávate na fyzickom počítači s Windows 7, bude nutné si stiahnuť totalcmd z Internetu, alebo požiadajte o jeho stiahnutie poskytnutie lektora. Totalcmd neinštalujte – len rozbaľte do nejakého priečinka, ktorý simuluje USB flashku nášho užívateľa Novak. V nasledujúcom texte potom nahraďte cestu C:\LABS\TOTALCMD cestou, kam ste rozbalili TOTALCMD.

Poznámka: V tomto labe preskúmame AppLocker - obmedzenie aplikácií, ktoré užívatelia môžu spúšťať na počítači s Windows 7. Náš štandardný účet Novak sa bude snažiť spustiť totalcmd.exe, čo sa mu pokúsime zakázať pomocou ochrany AppLocker. Výsledok bude ten, že užívateľ Novak nedokáže spustiť akúkoľvek aplikáciu, ktorú si prinesie sám – napr. akékoľvek portable aplikácie alebo čokoľvek z kľúčenky. Nehrozí tak zavírenie počítača ani prepašovanie používania nelegálneho (neschváleného) softwaru. Pri bližšom preskúmaní môžete zistiť, že ochrana AppLocker naväzuje na Software Restriction Policies z predchádzajúcich verzií Windows.

Cvičenie 1 Preskúmanie východiskových nastavení ochrany AppLocker

- Prihláste sa s administrátorským účtom s heslom Pa$$w0rd.
- Spustite editor bezpečnostných politík: Kliknite na Start a do poľa „**Search programs and files**“ napíšte „**secpol.msc**“ a stlačte Enter. V prípade potreby potvrďte dialóg UAC.
- V konzoli „**Local security policy**“ rozbaľte voľbu „**Application Control Policies**“ a kliknite na položku „**Applocker**“. V pravej časti kliknite na voľbu „**Which editions of Windows support AppLocker?**“ a v okne nápovedy preskúmajte informácie o podporovaných systémoch. Potom zatvorte okno nápovedy.
- V pravej časti konzoli „**Local security policy**“ kliknite na voľbu „**Configure rule enforcement**“ a všimnite si, že vo východiskovým stave nie sú vynucované žiadne politiky. Nesmieme teda zabudnúť zapnúť podporu príslušných pravidiel. V časti „**Executable rules**“ zaškrtnite možnosť **Configured** a preskúmajte možnosti v rozbaľovacom menu. Voľba „Audit only“ slúži pri monitorovaní, ktoré pravidlá by boli uplatnené v bežnej prevádzke a pri doladení týchto pravidiel. V našom labe ponecháme východiskovú možnosť „**Enforce rules**“. Kliknite na tlačítko **OK**.
- V ľavej časti konzoli pod položkou „**AppLocker**“ preskúmajte položky „**Executable rules**“, „**Windows Installer Rules**“ a „**Script Rules**“. Všimnite si, že ve východiskovom nastavení nie sú aktívne žiadne obmedzenia.

Upozornenie: Pamätajte si, že okrem voľby pre úspešné vynucovanie pravidiel spustiteľných súborov v AppLockeri je nutné tiež zapnúť službu, ktorá sprostredkúva podrobné informácie o spúšťaných procesoch – bez tejto služby nie sú pravidlá vynucované!!!

- Spustite konzolu pre správu služieb: Kliknite na Start a do poľa „**Search programs and files**“ napíšte „**services.msc**“ a stlačte Enter.

- V konzoli služieb v pravej časti kliknite na službu s názvom „**Application Identity**“ a všimnite si popis služby.

- Kliknite pravým tlačítkom myši na službu „**Application Identity**“ a vyberte voľbu **Properties**.

- Všimnite si, že vo východiskovom stave nie je služba spúšťaná automaticky. V časti Startup type v rozbaľovacom menu vyberte voľbu **Automatic**. Táto voľba zaistí automatické spúšťanie služby pri každom spustení systému. Kliknite na tlačítko **Apply**.

- Pretože nechceme čakať do ďalšieho reštartu systému, kliknite v okne vlastností služby na tlačítko Start. Zatvorte okno vlastností služby tlačítkom **OK** – skontrolujte v okne služieb v stĺpci **Status**, či je stav služby **Application Identity** zobrazený ako Started a potom zatvorte okno správy služieb. Vráťte se späť do okna editora „**Local Security Policy**“.

Cvičenie 2 Nastavenie pravidiel spúšťaných aplikácií v ochrane AppLocker

- V okne editora „**Local Security Policy**“ pod položkou **AppLocker** vyberte položku „**Executable Rules**“ a skontrolujte, že v pravej časti okna nie sú žiadne položky.

- Kliknite pravým na položku „**Executable Rules**“ a vyberte voľbu „**Create Default Rules**“.

- Všimnite si, že systém Windows vytvorí východiskové pravidlá zaisťujúce správne spúšťanie aplikácií v priečinkoch „**Windows**“ a „**Program Files**“. Skupina Everyone napovedá, že tieto pravidlá umožňujú spúšťanie ľubovoľnej nainštalovanej aplikácie každému užívateľovi. Bez týchto pravidiel by nebolo možné správne fungovanie samotného systému (nie všetky aplikácie Windows ležia v priečinku C:\Windows – napr. Internet Explorer, Wordpad alebo Media Player sú uložené v priečinku „Program Files“). Tiež si všimnite, že východiskové pravidlá umožňujú každému užívateľovi s administrátorským účtom spúšťanie ľubovoľnej aplikácie bez obmedzení!!! Ak však užívateľ nemá administrátorský účet, potom má v priečinkoch **Windows** a **Program Files** len oprávnenia pre čítanie a spúšťanie a preto nemôže spúšťať „Vlastné“ aplikácie.

- Overte, že je užívateľ Novak obmedzený na spúšťanie aplikácií v systéme. Kliknite na **Start** – rozbaľte ponuku vedľa voľby Shut down a vyberte možnosť „**Switch User**“. Na prihlasovacej obrazovke vyberte účet **Novak** a zadejte heslo **Pa$$w0rd**.

- Kliknite na **Start** a v pravej hornej časti sa presvedčte, že ste prihlásený pod účtom NOVAK. Kliknite na Computer, v ľavej časti prieskumníka rozbaľte cestu C:\LABS\TOTALCMD (na fyzickom PC rozbaľte cestu k priečinku, kde máte Totalcmd) a v pravej časti **spustite aplikáciu TOTALCMD.EXE**.

- Prezrite si hlásenie o zablokovaní aplikácie ochranou AppLocker. Kliknite na tlačítko **OK**.

- Prekopírujte priečinok **TOTALCMD** z **C:\LABS\TOTALCMD** na **plochu** užívateľa Novak. Skúste z tohto priečinka na ploche spustiť aplikáciu TOTALCMD – aplikácia by mala byť opäť zablokovaná.

6.C

- V oboch prípadoch užívateľ spustil aplikáciu z priečinkov mimo cestu **C:\Program Files** alebo **C:\Windows** a preto bola aplikácia vždy zablokovaná. Tieto obmedzenia sa však vo východiskovým stave dajú ľahko obísť rovnako ako v predchádzajúcich ochranách Software Restriction Policy následujúcim postupem:

- Skúste v prieskumníkovi vstúpiť do priečinku **C:\Windows\Temp** – objaví sa obrazovka, ktorá Vás upozorňuje, že nemáte oprávnenie pre čítanie obsahu priečinka Temp. Na obrazovke tohto hlásenia zvoľte možnosť Cancel.

- Kliknite pravým tlačítkom na priečinok **TOTALCMD** na DVD médiu a zvoľte možnosť **Copy**. Potom v prieskumníkovi v pravej časti vyberte priečinok C:\Windows a v pravej časti kliknite pravým tlačítkom na priečinok **Temp** a vyberte voľbu **Paste**. Všimnite si, že aj keď si užívateľ nemôže prezerať obsah priečinka Temp, môže tu vytvárať ľubovoľné podpriečinky a súbory bez toho, že by do priečinka vstúpil. Automaticky sa stáva vlastníkom týchto vložených súborov a priečinkov a má oprávnenia **Full Control**.

- Potom kliknite myšou do voľné časti v **hornom adresnom pruhu** Windows Explorera, čím sa zobrazovaná cesta zmení na **C:\Windows** s blikajúcim kurzorom na konci – dopíšte cestu na tvar: **C:\Windows\Temp\Totalcmd** a stlačte Enter – všimnite si, že pretože máte Full Control oprávnenia na tomto priečinku a jeho dcérskych objektoch, môžete si takto prezerať jeho obsah.

- V pravej časti prieskumníka dvojitým kliknutím spustite aplikáciu **TOTALCMD**. Všimnite si, že týmto spôsobom užívateľ ľahko obišiel východiskovú ochranu aplikácie AppLocker.

- Zatvorte okno spusteného Total commanderu a odhláste užívateľa Novak v Start menu voľbou Log Off. Prihláste sa späť ako **administrátorský účet** s heslom Pa$$w0rd.

- Prepnite sa späť do okna konzole **Local Security Policy** (secpol.msc), v časti Application Control Policies-AppLocker pravým tlačítkom kliknite na Executable Rules a vyberte voľbu „**Create New Rule**".

- Na obrazovke „**Before You Begin**" zaškrtnite voľbu „Do not show this screen" a pokračujte stlačením tlačidla Next.

- Na obrazovke **Permissions** vyberte voľbu **Deny**, ktorá vytvorí zakazujúce pravidlo a v časti **User or group** Kliknite na tlačítko **Select** – všimnite si, že obmedzujúce či povoľujúce pravidlá je možné vzťahovať ku konkrétnym účtom či skupinám, v ktorých sú užívatelia členom. Zrušte dialógové okno pre výber užívateľov či skupín stlačením tlačítka **Cancel**, čím sa vrátite späť do okna Permissions a pokračujte voľbou **Next**.

- Na obrazovke **Conditions** si všimnite, že pravidlá možno vymedziť aj pomocou vymenovania Vydávateľa Softwaru, ak majú aplikácie digitálny podpis. Druhou možnosťou je vymedzenie pravidiel pomocou cesty – zadaním názvov priečinkov či súborov. Môžeme využívať aj zástupné znaky. Poslednou voľbou je pravidlo Hash, ktoré pomocou odtlačku súboru vymedzí iba konkrétnu verziu aplikácie. Vyberte možnosť **Path** a pokračujte tlačítkom **Next**.

- Na obrazovke **Path** zvoľte **Browse Folders** a vyberte priečinok **C:\Windows\Temp** a stlačte tlačítko **OK**.

- Všimnite si, že systém automaticky zmení c:\Windows na promennú %WinDir% a doplní zástupný znak * tak, aby danému pravidlu vyhovovali všetky cesty vrátane podpriečinkov a ľubovoľný názov aplikácie. Pokračujte stlačením tlačítka **Next**.

- V okne **Exceptions** si preskúmaním horného roletového menu všimnite, že k danému pravidlu je možné vytvoriť výnimku – napr. ak by sme určitú cestu v rámci priečinka C:\Windows\Temp chceli vyslovene povoliť. Nezadávajte žiadne výnimky a pokračujte stlačením tlačítka **Next**.

- V okne **Name and Description** v časti Name napíšte názov: **No Windir\Temp apps** a do poľa Description napíšte ľubovoľný popis pravidla. Dokončite vytvorenie pravidla tlačítkom **Create**.

- Skúste opäť prepnúť užívateľa na účet **Novak** s heslom Pa$$w0rd a skúste spustiť aplikáciu TOTALCMD z priečinka **C:\Windows\Temp\Totalcmd**. Objaví se hlásenie, že teraz je už táto cesta zakázaná a AppLocker nedovolí spustenie aplikácie.

- Väčšina administrátorov bohužiaľ ponecháva rovnakým spôsobom nezabezpečenú zložku C:\Windows\System32\Spool\Printers a celú radu ďalších priečinkov. Preto je v praxi potrebné nastaviť ďalšie pravidlá pre všetky priečinky, v ktorých užívatelia majú oprávnenie vytvárať dcérske objekty.

- Odhláste užívateľa Novak a prihláste sa späť s administrátorským účtom.

Cvičenie 3 Automatické vytváranie pravidiel

- Presvedčte sa, že ste prihlásený s **administrátorským účtom**. Prekopírujte zložku C:\LABS\TOTALCMD do složky **C:** (aby vznikla zložka C:\TOTALCMD a v nej bol totalcmd.exe a ostatné súbory).

- Prepnite sa späť do okna konzole **Local Security Policy** (secpol.msc), v časti Application Control Policies-AppLocker pravým tlačítkom kliknite na Executable Rules a vyberte voľbu „**Automatically Generate Rules**". Táto voľba Vám umožňuje vytvoriť pravidlá pre všetky aplikácie v rámci určitej cesty, kedy sprievodca automaticky prehľadá všetky podpriečinky a vygeneruje pravidlá pre všetky aplikácie, ktoré v tejto zložke a podzložkách našiel.

- V časti „**Folder that contains the files...**" kliknite na tlačítko **Browse** a vyberte priečinok C:\TOTALCMD a kliknite na tlačítko OK. V poli „**Name to identify this set of rules**" napíšte názov: **Komponenty TOTALCMD** a pokračujte tlačítkom **Next**.

- Na obrazovke Rule References si všimnite, že sprievodca automaticky vytvorí pravidlá pre všetky nájdené aplikácie a vo východiskovom stave vytvára pravidlá podľa vydavateľa, ak majú nádené aplikácie digitálny podpis a v prípade že nemajú, potom sa pravidlá vytvárajú podľa HASH odtlačku súboru. HASH odtlačok súboru je ideálny, ak dodávateľ aplikácie už nebude poskytovat aktualizácie, avšak pokiaľ ide o často aktualizovanú aplikáciu, potom je pravidlo HASH odtlačku nutné vytvoriť znovu s každou novou verziou. Preto vyberte voľbu „**Path:Rules are created using file's path**" a všimnite si východiskovo zaškrtnutú voľbu „**Reduce the number of rules created by grouping similar files**", ktorá sa prejaví na nasledujúcej obrazovke a pokračujte stlačením tlačítka Next.

6.C

- Na obrazovke „**Review Rules**“ si všimnite, že sprievodca na danej ceste našiel niekoľko súborov, ale vďaka zaškrtnutej voľbe pre zoskupenie podobných súborov bude vytvorené iba jedno zjednocujúce pravidlo cesty.
- Kliknite na voľbu „Review files that were analyzed“, prezrite si nájdené aplikácie a potom uzavrite okno **Edit files** stlačením tlačítka **OK**.
- Kliknite na voľbu „**View rules that will be automatically created**“ a všimnite si jediné pravidlo, ktoré zjednodušuje prehľad v konzoli AppLockeri – bez voľby zjednodušenia by sprievodca vytvoril jedno pravidlo pre každú nájdenú aplikáciu. Uzavrite prehľad vytváraných pravidel stlačením tlačítka **OK**.
- Dokončite sprievodcu vytvorením pravidla stlačením tlačítka Create.

Cvičenie 4 Vytváranie pravidiel podľa vydávateľa

- Prepnite sa späť do okna konzole **Local Security Policy** (secpol.msc), v časti **Application Control Policies-AppLocker** pravým tlačítkom kliknite na **Executable Rules** a vyberte voľbu „**Create New Rule**“.
- V okne **Permissions** vyberte voľbu **Deny** a pokračujte stlačením tlačítka **Next**.
- V okne **Conditions** ponechajte východiskovú voľbu **Publisher** pre obmedzenie spúšťaných aplikácií na základe digitálneho podpisu aplikácií a stlačte tlačítko **Next**.
- V okne **Publisher** kliknite na tlačítko **Browse** pre výber konkrétnej aplikácie a vyberte aplikáciu:

  „C:\Program Files\DVD Maker\DVDMaker.exe“ a vyberta aplikáciu stlačením tlačítka **Open**.
- Všimnite si v okne **Publisher**, že na základe metadát aplikácie sprievodca automaticky zistí vydavateľa, názov aplikácie, doplní názov súboru a dokonca i konkrétnu verziu aplikácie. Skúste posúvať posuvník nahor a nadol, čím obmedzíte platnosť pravidla na ľubovoľnú úroveň – napr. na všetky aplikácie od daného vydávateľa bez ohľadu na názov produktu či súboru. Ponechajte však posuvník na najnižšej úrovni, čím zamedzíte spúšťanie konkrétnej verzie aplikácie DVD Maker.
- Zaškrtnite voľbu „**Use custom values**“ a všimnite si, že môžete upravovať ľubovoľné pole pravidla. V pravej časti rozbaľte menu vedľa čísla verzie aplikácie a všimnite si, že môžete zakázať či povoliť spúšťanie aplikácií od či do uvedenej verzie. Touto voľbou by ste napríklad zakázali spúšťanie nebezpečnej zastaralej verzie aplikácie, ktorá by bola zneužiteľná k útoku na počítač.
- Pretože používame zakazovacie pravidlo, vyberte voľbu „**And below**“.
- Pokračujte stlačením tlačítka **Next**.
- Okno **Exceptions** ponechajte prázdne a stlačte tlačítko **Next**.

- Na obrazovke **Name and Description** v poli **Description** napíšte: **No Unsecure DVD Maker** a pokračujte stlačením tlačítka **Create**.

- Prepnite sa na užívateľa Novak a presvedčte sa, že užívateľ Novak nemôže spustiť aplikáciu DVD maker – kliknite na Start a do poľa „**Search programs and files**“ napíšte „**DVD**“ a vyčkajte, kým sa v hornej časti nezobrazí názov aplikácie Windows DVD Maker a stlačte Enter.

- Všimnite si, že i keď je aplikácia DVD maker umiestená v priečinku „**C:\Program Files**“, nemôže ju užívateľ spustiť kvôli konkrétnejšiemu zakazovaciemu pravidlu, ktoré sme vytvorili.