Práca s administratívnymi nástrojmi Event Viewer a Task Scheduler

Event Viewer

1. Na serveri vytvorte používateľa Wanda Maximoff s loginom wmaximoff, ktorého heslo nikdy neexspiruje a nemusí sa zmeniť pri prvom prihlásení.
2. Zaraďte ho do skupín Print Operators a Remote Desktop Users.
3. Vyskúšajte sa týmto účtom prihlásiť lokálne na serveri. Vyskúšajte jedno neúspešné prihlásenie (zlým heslom) a jedno úspešné.
4. Otvorte si Event Viewer a prejdite do bezpečnostných nastavení (Windows Logs → Security)
5. V Action paneli (v pravej časti) nájdite položku Filter Current Logs a postupne si vyskúšajte odfiltrovať tieto Event ID. Sledujte aj detaily – tj. kde sa nachádza informácia o používateľskom účte ktorý objekty vytváral alebo o objektoch, ktorých sa informácia týka:
    a. 4720: A user account was created.
    b. 4732: A member was added to a security-enabled local group.
    c. 4624: An account was successfully logged on.
    d. 4625: Account failed to log on
        - Uložte si prehľad všetkých neúspešných prihlásení (Save Filtered Log File As...) vo formáte evtx aj txt. Prezrite si obsah TXT súboru.
6. Odfiltrujte si ešte raz Event ID 4720 a súčasne 4732 v Security logu.
    a. Uložte si tento filter na neskoršie použitie → Save filter to custom View. Mal by sa objaviť v ľavom paneli v časti Custom Views
    b. Vytvorte nového používateľa Billy Maximoff a overte, že sa zobrazil v tomto uloženom filtri. Ak nie, kliknite na tlačidlo Refresh
7. Vyskúšajte sa prihlásiť cez vzdialenú plochu.
8. V logu aplikácií a služieb nájdite Microsoft > Windows > TerminalServices-RemoteConnectionManager > Operational. Prezrite si pripojenia cez vzdialenú plochu a nájdite IP adresu, z ktorej bolo spojenie nadviazané.
9. Vráťte sa do Security Logu a odfiltrujte si všetky zmeny času v systéme (4616: The system time was changed.). Ak sa v Security logu takéto záznamy nenachádzajú, môžete zmeniť čas v príkazovom riadku príkazom ***time***
10. Kliknite pravým tlačidlom na jeden riadok v logu, ktorý hovorí o zmene času a vyberte možnosť Attach Task to This Event. Ako akciu dajte spustiť program a napíšte do riadku príkaz ***msg * Alert: System time changed!***
11. Overte funkčnosť tasku zmenou času – buď synchronizáciou času s internetom alebo zadaním príkazu ***time*** v príkazovom riadku.
12. Niektoré logy sú štandardne vypnuté a je ich potrebné zapnúť, ak chceme sledovať vybrané udalosti v systéme. V štart ponuke zadajte ***gpedit.msc*** a prejdite do **Computer configuration → Windows Settings → Security Settings → Advanced audit policy configuration → System audit policies → Object Access → Audit Other Object Access Events → Enabled**
13. Teraz môžete napríklad sledovať aj vytváranie Taskov cez Task scheduler. Sú to eventy s číslom ID 4698 (A scheduled task was created).
14. Prezrite si ešte System log s Event ID 1074 a zistite dôvody posledného vypnutia systému. Uložte si tento filter do Custom view, aby ste ho nemuseli neskôr znova hľadať.

15. Vypnite systém a zvoľte si ako dôvod vypnutia Plánovanú inštaláciu nového HW komponentu. Po vypnutí a zapnutí overte, či sa tento dôvod zapísal do logov.

Task scheduler

16. Otvorte nástroj Task Scheduler a prejdite na úlohy, ktoré vznikli pri inštalácii systému alebo jeho súčastí. Nájdete ich v skupine Microsoft.
17. Prezrite si rôzne typy úloh, ktoré systém spúšťa. Pokúste sa identifikovať aspoň 3 z nich.
18. Všimnite si napríklad, ako systém iniciuje sken počítača na malvér a aktualizáciu systému. Nájdete to v časti Windows Defender a Windows Update.
19. Vytvorte úlohu, ktorá raz za týždeň reštartuje server. Ako akciu použite program **shutdown /r /t 60.** Naplánujte si štart úlohy tak, aby ste boli schopní ju overiť (čiže napr. o 2 minúty od teraz).
20. Po otestovaní nastavte, aby sa úloha spustila len vtedy, ak sa s počítačom nepracuje viac ako 2 minúty a spustenie úlohy čo najskôr, ak je zmeškaná. Ak úloha zlyhá, nech sa systém pokúsi urobiť ju ešte 5x s odstupom 2 minút.
21. Exportujte vytvorenú úlohu do XML súboru.
22. Vytvorte úlohu, ktorá raz za deň vysype súbory z koša. Ako akciu použite program **rd /s /q C:\$Recycle.bin.**
23. Zapnite si logovanie spúšťania naplánovaných úloh. V Event Vieweri prejdite na Application and services logs → Microsoft → Task Scheduler → Operational kliknite pravým a zvoľte Enable log.
24. Vyskúšajte ručne alebo automaticky spustiť naplánovanú úlohu a sledujte, aké údaje sa zaznamenávajú. Zistite, či sa úloha spustila manuálne alebo automaticky a akú akciu vyvolala.
25. Upravte logovanie kliknutím pravým tlačidlom na Operational log tak, aby sa ukladalo 20MB logov a aby sa staré záznamy prepisovali novými.
26. Súčasný log vymažte kliknutím na Clear log.