Práca s administratívnymi nástrojmi
Sledovanie výkonu

Resource monitor

1. Spustite nástroj Resource monitor.
2. V záložke CPU zistite, ktoré procesy využívajú procesor najviac. Sledujte stĺpec Average CPU.
3. Spustite aplikáciu Notepad. V záložke CPU si označte len túto aplikáciu a zistite cez sekciu Associated Handles, aké súbory (Files) a kľúče registrov (Key) má tento proces otvorené.
4. Prezrite si aj sekciu Associated Modules a zistite, aké knižnice (DLL) využíva notepad. Používa nejakú knižnicu, ktorá by mohla slúžiť na prácu so šifrovaním?
5. Otvorte si internetový prehliadač Edge a zobraze nejakú stránku. V záložke Network v sekcii Network activity zistite, aké adresy kontaktuje tento prehliadač. S ktorou adresou má najrušnejšiu komunikáciu?
6. Cez sekciu TCP Connections zistite, koľko vytvoril prehliadač Edge spojení typu HTTPS (vzdialený port 443).
7. Zrušte filter na edge a v sekcii Listening ports zistite, na koľkých portoch server počúva. Koľko z nich sú dobre známe sieťové porty (0-1023)?
8. Zistite, ako pracuje Edge s diskom (cez Resource monitor) v záložke Disk.
9. V záložke Disk si označte len proces System. Skúste v záložke Disk zistiť, či tento proces niečo zapisuje do logov. Akú príponu majú tieto súbory logov?

Performance monitor

10. Otvorte nástroj Performance monitor a pridajte do prebiehajúceho grafu (Monitoring tools – Performance monitor) nasledovné parametre: IPv4 → Datagrams/sec, Memory → Available Bytes, Memory → Cache Bytes, PhysicalDisk → %Disk Write Time
11. Upravte merané parametre tak, aby mal každý samostatnú farbu a násobiteľ (Scale) tak, aby bol každý dobre viditeľný na grafe. Sieť otestujte cez tracert na server www.google.com.
12. Z daného monitora spravte Data Collector cez pravé kliknutie. Upravte jeho vlastnosti (Properties) tak, aby sa vypol po 10 sekundách. Následne zobrazte nazbierané dáta cez Report a uložte graf ako obrázok.

Services

13. V nástroji Services zistite, či bežia nasledovné služby: Windows Update, Windows Defender Firewall, Windows Event Log
14. Zistite, či sa služba Remote Desktop Services spúšťa automaticky alebo manuálne. Nastavte ju tak, aby sa spúšťala automaticky.
15. V prípade, že zlyhá raz, nech sa pokúsi ju reštartovať, po druhom pokuse sa tiež pokúsi o reštart služby, po ďalších zlyhaniach sa bude pokúšať každú pol hodinu službu opäť reštartovať.
16. Zistite pre službu Remote Desktop Services, ktoré služby sú závislé na nej a od ktorých služieb je závislá ona sama.

System information

17. Zistite základné sumárne informácie o systéme
18. V časti Components zistite
    a. aké rozlíšenie má aktuálny monitor
    b. koľko sieťových kariet sa nachádza v systéme
    c. veľkosť pripojeného disku a partícií
    d. či existuje nejaký problémový komponent
19. Vyexportujte informácie o počítači do TXT súboru

Task manager

20. Prepnite si používateľa na nejakého iného. Neodhlasujte sa z Admina. Ak iného používateľa nemáte, vytvorte si ho.
21. Prihláste sa ako nový používateľ. Pod novým používateľom spustite notepad. Pozrite si task manager a zistite, či sú v systéme prihlásení aj ďalší používatelia. Mali by byť viditeľný dvaja – váš aktuálny + Administrator.
22. Zistite, či používateľ vidí procesy administrátora.
23. Prepnite sa teraz na Administratora ale neodhlasujte sa z aktuálneho používateľa. Pozrite sa cez Task manager admina, či vidí spustené procesy obyčajného používateľa. Ak áno, skúste z pozície admina ukončiť notepad používateľa.

Ďalšie nástroje

Preskúmajte aspoň 2 zaujímavé administrátorské nástroje. Napríklad:

- NirSoft USB Drive Log For Windows
- NirSoft LastActivityView
- NirSoft TurnedOnTimesView
- NirSoft WinLogOnView
- Sysinternals Process Monitor
- Sysinternals Process Explorer
- Sysinternals Not My Fault