Nastavni predmet:	**PRAKTIČNE OSNOVE RAČUNALSTVA**
Vježba:	LV13 – Powershell – Administracija sustava i izrada skripti
Cilj vježbe:	Upoznati učenike s osnovnim administrativnim zadacima u Windows sustavu unutar Powershell okruženja.

Sve postupke, korištene naredbe i dobivene rezultate po točkama zadataka zapisivati u bilježnicu. Odgovoriti u bilježnicu na postavljena pitanja vezana uz ovu vježbu.

Preduvjeti : Računalo/Virtualni stroj sa instaliranim Windows operacijskim sustavom minimalne verzije 10.

Pomoć : Powershell naredba se zove cmdlet, i uvijek se nosi u kombinaciji Glagol-Imenica (točno tim redoslijedom). Npr. , Get-Help je naredba koja poziva pomoć za ostale cmdletove. Dio sa glagolom uglavnom govori koja će se radnja izvršiti : Get (čitaj), Set (zapiši), Remove (obriši) itd. Dio sa imenom označava na kojem dijelu sustava će se izvršiti radnja.

Više o Powershell glagolima:

https://learn.microsoft.com/en-us/powershell/scripting/developer/cmdlet/approved-verbs-for-windows-powershell-commands?view=powershell-7.4

Napomena : Riječi unutar navodnika u terminal unosite bez navodnika. Koristite naredbe Get-Help i Get-Command za snalaženje sa cmdletima u vježbi.

Zadaci:

 # Uvod u PowerShell ISE i osnove izrade skripti

1. Pokrenite PowerShell ISE kao administrator.
2. Stvorite novu skriptu network_config.ps1 i spremite ju u C:\Scripts.
3. Upišite naredbu Write-Output "Hello, PowerShell Scripting!" i pokrenite skriptu.
4. Ispišite sve varijable definirane u trenutnoj sesiji korištenjem Get-Variable.
5. Dodajte komentar u skriptu koji objašnjava svrhu skripte.
6. Stvorite varijablu $username i dodijelite joj vrijednost Read-Host "Unesite korisničko ime", zatim ispišite vrijednost s Write-Output "Dobrodošao, $username".
7. Kreirajte skriptu koja traži unos imena i prezimena, zatim ispisuje Write-Output "Vaše ime je $ime, a prezime $prezime.".
8. Kreirajte skriptu koja traži unos broja i prikazuje kvadrat tog broja (Read-Host "Unesite broj").
9. Ispišite sve environment varijable koristeći Get-ChildItem env:.
10. Napišite skriptu koja traži unos imena direktorija i zatim ga kreira na Desktopu trenutno prijavljenog korisnika, koristeći varijable korisničkog profila ($env:USERPROFILE) i unesenog imena direktorija.

 # Pregled i Izmjena Mrežnih Postavki

11. Prikažite mrežne adaptere i njihovih IP adrese korištenjem Get-NetIPAddress. Ponovite unos, ali filtrirajte rezultat tako da se prikažu samo IPv4 adrese. U slučaju prikaza više od jedne IP adrese, filtrirajte rezultat tako da se prikaže samo ona IP adresa pomoću koje pristupate internetu.
12. Ispišite trenutne DNS postavke s Get-DnsClientServerAddress. Ako bi imali više rezultata, unesite naredbu na način da se prikažu samo rezultati koji nisu prazni (HINT: prikaz non empty, ili non null objekata).
13. Postavite statičku IP adresu koristeći Read-Host za unos ($ipAddress = Read-Host "Unesite novu IP adresu") i Set-NetIPAddress.
14. Postavite novi DNS server koristeći Read-Host "Unesite DNS adresu" i Set-DnsClientServerAddress.
15. Automatski ponovno pokrenite mrežni adapter nakon promjena korištenjem Restart-NetAdapter.
16. Dodajte Write-Output koji potvrđuje postavljene mrežne postavke.

17. Napišite skriptu koja omogućava korisniku unos mrežnog adaptera i zatim prikazuje informacije o njemu.

18. Napravite skriptu koja traži unos mrežne maske i prikazuje Write-Output "Postavljena mrežna maska je $mask".

19. Stvorite skriptu koja omogućava unos više IP adresa i sprema ih u niz, a zatim ih ispisuje.

20. Napravite skriptu koja će korisniku omogućiti da odluči hoće li postaviti DHCP ili statičku IP adresu na odabrani mrežni adapter.

 # Konfiguracija Windows Firewall-a

21. Prikaz trenutnih firewall pravila korištenjem Get-NetFirewallRule.

22. Omogućite dolazne RDP veze dodavanjem pravila u firewall. RDP koristi TCP port 3389.

23. Onemogućite pristup web stranicama sa HTTP (remote tcp port 80) i HTTPS (remote tcp port 443) protokolima. Koristite parametre Name i DisplayName, te neka budu identični (npr. "Block Out HTTP"). Uvjerite se da ne možete pristupiti internet web stranicama. Preimenujte pravila tako da počinju sa "Allow", te promijenite pravilo tako da vam dozvoli pristup navedenim protokolima. Uvjerite se da pristup web stranicama funkcionira. Obrišite oba pravila. Uvjerite se da su pravila zaista obrisana koristeći cmdlet Get-NetFirewallRule i prikladne parametre.

24. Onemogućite firewall privremeno za sve profile korištenjem Set-NetFirewallProfile -Enabled False.

25. Ponovno omogućite firewall korištenjem Set-NetFirewallProfile -Enabled True.

26. Koristite Read-Host "Unesite port koji želite otvoriti" za unos porta te kreirajte novo pravilo.

27. Dodajte Write-Output koji potvrđuje dodavanje pravila (ispisuje detalje pravila).

28. Napravite skriptu koja traži unos aplikacije (puna putanja aplikacije) i automatski dodaje pravilo za nju.

29. Napišite skriptu koja prikazuje samo omogućena firewall pravila.

30. Kreirajte skriptu koja traži unos firewall profila (Domain, Private, Public) i prikazuje njegove postavke pomoću Get-NetFirewallProfile cmdleta.

 # Automatizacija Administrativnih Zadataka

31. Kreirajte skriptu backup_logs.ps1 koja kopira sve log datoteke iz C:\Logs u C:\Backup.

32. Naredbom Task Scheduler zakazujte ovu skriptu da se pokreće svakog dana u 03:00.

33. Prikaz svih aktivnih procesa korištenjem Get-Process.

34. Identificirajte procese koji troše najviše memorije.

35. Kreirajte funkciju Kill-Process koja uzima ime procesa i zatvara ga.

36. Dodajte Read-Host "Unesite ime procesa koji želite prekinuti" i Stop-Process -Name $processName.

37. Koristite Write-Output za prikaz statusa nakon zatvaranja procesa.

38. Kreirajte skriptu koja prikazuje sve sistemske servise i omogućuje korisniku da jedan od njih zaustavi.

39. Napravite skriptu koja korisniku omogućava unos direktorija i provjerava veličinu svih datoteka u njemu.

40. Dodajte skriptu koja korisniku omogućava unos vremenskog intervala za automatsko čišćenje temp datoteka.

41. Kreirajte skriptu koja omogućava korisniku da unese direktorij i generira izvještaj o svim datotekama u njemu (ime, veličina, datum kreiranja), zatim ga spremi u C:\Reports\report.txt.

DODATNI ZADACI

 # Upravljanje Microsoft Defender Antivirusom

42. Prikažite trenutni status Defender-a korištenjem Get-MpPreference.

43. Isključite Defender antivirus privremeno (ako je dozvoljeno pravilima sustava) koristeći vrijednost Property-a "DisableRealtimeMonitoring".

44. Ponovno uključite Defender antivirus.

45. Dodajte iznimku za direktorij C:\Scripts korištenjem Read-Host "Unesite direktorij za iznimku" (ExclusionPath property).

46. Pokrenite ručno Defender skeniranje korištenjem Start-MpScan.

47. Napravite skriptu koja omogućava korisniku da odluči želi li skenirati sustav ili dodati iznimku. Koristite Write-Output za informaciju nakon završenog skeniranja.

48. Napravite skriptu koja traži unos aplikacije i provjerava je li na popisu blokiranih aplikacija.

49. Dodajte opciju korisniku da bira između različitih vrsta Defender skeniranja.