Přehled PowerShell skriptů na serveru DC2

Datum analýzy: 23.10.2025 **Server:** dc2 **Analyzovaná cesta:** C:

Nalezené PowerShell skripty

Hlavní složka: C:\Scripts

#	Název souboru	Velikost	Poslední změna	Účel
1	**AD.ps1**	804 B	23.10.2024 23:13	Active Directory - výpis počítačů
2	**AD2.ps1**	1,968 B	18.12.2024 10:42	Active Directory - rozšířený
3	**Computers-to-csv.ps1**	1,130 B	21.08.2024 11:40	Export počítačů do CSV
4	**Computers.ps1**	946 B	21.08.2024 11:32	Správa počítačů
5	**Computers2.ps1**	1,125 B	21.08.2024 12:00	Správa počítačů v2
6	**DHCP-mac.ps1**	4,679 B	06.06.2024 14:23	DHCP a MAC adresy
7	**Logging.ps1**	2,260 B	13.06.2024 09:10	Logování událostí
8	**MailDnsAlias.ps1**	5,586 B	01.06.2024 16:22	DNS aliasy pro mail
9	**name.ps1**	6,878 B	20.11.2024 17:09	Správa jmen
10	**TestPasswords.ps1**	1,637 B	18.06.2025 19:14	⚠ Testování hesel
11	**VpnDnsAlias.ps1**	5,567 B	01.06.2024 16:21	DNS aliasy pro VPN

Datové soubory:

- **get-pwned-users.csv** (7,492 B) - CSV se zkompromitovanými uživateli
- **import-banned-pass.txt** (1,870 B) - Seznam zakázaných hesel

Podsložka: C:\Scripts\credentials

- Složka vytvořena: 05.08.2024 10:08
- ⚠ **POZOR**: Obsahuje pravděpodobně citlivá data

Detailní analýza skriptů

1. AD.ps1 - Active Directory Computer Inventory

```
Funkce:
- Import modulu Active Directory
- Výpis počítačů z OU "OU=Computers,OU=UCHP,DC=asuch,DC=cas,DC=cz"
- Zobrazení posledního přihlášení (LastLogonDate)
```

```
Použití:
- Monitoring aktivity počítačů v doméně
- Inventura počítačů v organizační jednotce UCHP
```

Důležité: - Cílová OU: OU=UCHP (Pravděpodobně Ústav chemie a procesů) - Doména: `asuch.cas.cz`

---

2. AD2.ps1 - Rozšířený AD skript

```
Velikost: 1,968 B (větší než AD.ps1)
Pravděpodobně obsahuje:
- Rozšířenou funkcionalitu
- Více filtrů nebo výstupů
```

3-5. %%**%%Computers*.ps1%%**%% - Správa počítačů

```
Computers.ps1 (946 B)
Computers2.ps1 (1,125 B)
Computers-to-csv.ps1 (1,130 B)

Funkce:
- Export informací o počítačích
- Pravděpodobně různé varianty stejného účelu
- CSV export pro další zpracování
```

---

6. DHCP-mac.ps1 - DHCP a MAC adresy

```
Velikost: 4,679 B (největší v kategorii network)

Pravděpodobné funkce:
- Správa DHCP reservací
- Mapování MAC adres na IP
- Network inventory
```

---

7. Logging.ps1 - Logování

```
Velikost: 2,260 B

Funkce:
- Centrální logování událostí
```

```
- Pravděpodobně používán ostatními skripty
```

8-11. DNS aliasy - Mail a VPN

```
MailDnsAlias.ps1 (5,586 B)
VpnDnsAlias.ps1 (5,567 B)

Funkce:
- Automatizace DNS záznamů
- Správa aliasů pro mailový server
- Správa aliasů pro VPN
- Téměř identická velikost → pravděpodobně podobná struktura
```

⚠ 10. TestPasswords.ps1 - BEZPEČNOSTNÍ POZOR

```
Velikost: 1,637 B
Datum: 18.06.2025 (BUDOUCÍ DATUM!)

 RIZIKO:
- Testování hesel proti slovníku
- Možné použití s get-pwned-users.csv
- import-banned-pass.txt

DOPORUČENÍ:
- Zkontrolovat obsah skriptu
- Ověřit, zda není zneužíván
- Zajistit, že je používán pouze pro bezpečnostní audit
```

Další nalezené skripty

Desktop uživatele fridricha:

- **import.ps1**
- **MailDnsAlias.ps1** (kopie)
- **VpnDnsAlias.ps1** (kopie)
- **Untitled1.ps1** - **Untitled7.ps1** (testovací skripty)

Desktop uživatele nuliceka:

- **SentinelOneInstall.ps1** - Instalace antiviru SentinelOne
- **GEO-SentinelOneInstall.ps1** - GEO varianta

- **UCHP-SentinelOneInstall.ps1** - UCHP varianta

Kategorizace podle účelu

Active Directory (3 skripty)

1. AD.ps1
2. AD2.ps1
3. Computers*.ps1

Účel: Správa a monitoring počítačů v AD

Síťová infrastruktura (3 skripty)

1. DHCP-mac.ps1
2. MailDnsAlias.ps1
3. VpnDnsAlias.ps1

Účel: Správa DHCP a DNS

Bezpečnost (3 položky)

1. TestPasswords.ps1
2. get-pwned-users.csv
3. import-banned-pass.txt

Účel: Audit bezpečnosti hesel

Utility (1 skript)

1. Logging.ps1

Účel: Logování a monitorování

⚡ Doporučení

VYSOKÁ PRIORITA

1. **Zkontrolovat TestPasswords.ps1**

```
Get-Content C:\Scripts\TestPasswords.ps1
```

1. **Ověřit credentials složku**

```
Get-ChildItem C:\Scripts\credentials -Force
```

1. **Zkontrolovat scheduled tasks**

```
Get-ScheduledTask | Where-Object {$_.Actions.Execute -like "*powershell*"}
```

STŘEDNÍ PRIORITA

1. **Analyzovat get-pwned-users.csv**
   - Zkontrolovat, zda neobsahuje citlivá data
   - Ověřit, že je správně zabezpečen
2. **Sjednotit duplicitní skripty**
   - Computers.ps1 vs Computers2.ps1 vs Computers-to-csv.ps1
   - Ponechat nejlepší verzi, ostatní archivovat

NÍZKÁ PRIORITA

1. **Cleanup Desktop skriptů**
   - Přesunout Untitled*.ps1 do archivní složky
   - Udržovat Desktop čistý

Příkazy pro další analýzu

Zobrazit obsah konkrétního skriptu:

```
Get-Content C:\Scripts\AD2.ps1
Get-Content C:\Scripts\TestPasswords.ps1
Get-Content C:\Scripts\DHCP-mac.ps1
```

Zobrazit obsah credentials složky:

```
Get-ChildItem C:\Scripts\credentials -Force -Recurse
```

Najít všechny scheduled tasks s PowerShell:

```
Get-ScheduledTask | Where-Object {
    $_.Actions.Execute -like "*powershell*"
} | Select-Object TaskName, State, LastRunTime | Format-Table
```

Najít všechny .ps1 soubory na C: (včetně skrytých):

```
Get-ChildItem -Path C:\ -Include *.ps1 -Recurse -Force -ErrorAction
SilentlyContinue |
    Select-Object FullName, Length, LastWriteTime |
    Out-File C:\Scripts\all_scripts_inventory.txt
```

Kontrola exekuce skriptů (logování):

```
Get-WinEvent -LogName "Windows PowerShell" -MaxEvents 100 |
    Where-Object {$_.Message -like "*Script*"} |
    Format-Table TimeCreated, Message -AutoSize
```

Nalezené informace o infrastruktuře

Doména:

- **Název:** asuch.cas.cz
- **DC:** dc2
- **OU struktura:**
  - OU=UCHP (Ústav chemie a procesů)
  - OU=Computers

Uživatelé s přístupem:

- **fridricha** - Administrátor (má skripty na Desktopu)
- **nuliceka** - IT technik (instalace SentinelOne)

Používané technologie:

- Active Directory
- DHCP
- DNS
- VPN
- SentinelOne (Antivirus/EDR)

Poznámky

1. **Datumová anomálie:**
   - Některé soubory mají datum 18.06.2025 (budoucnost)
   - Možná chyba systémového času nebo ručně změněné datum
2. **Bezpečnostní audit:**
   - TestPasswords.ps1 + get-pwned-users.csv + import-banned-pass.txt
   - Vypadá jako kompletní systém pro testování hesel proti leakům
3. **Organizace:**
   - Skripty jsou dobře organizované v C:
   - Duplikace na Desktop poukazuje na aktivní vývoj
   - Mělo by se zvážit použití verzování (Git)

Další kroky

1. ☐ Přečíst obsah TestPasswords.ps1
2. ☐ Ověřit credentials složku
3. ☐ Zkontrolovat scheduled tasks
4. ☐ Analyzovat get-pwned-users.csv
5. ☐ Zkontrolovat PowerShell execution policy
6. ☐ Ověřit PowerShell logging
7. ☐ Kontrola PowerShell history
8. ☐ Audit přístupových práv ke skriptům

Vytvořeno pomocí Claude Code Datum: 23.10.2025