Implementácia metodiky pre zabezpečenie IT systémov verejnej správy

Študent: Matej Štubniak

Školiteľ: RNDr. Jaroslav Janáček, PhD.

Konzultant: Mgr. Lukáš Hlavička

Základné informácie

- dokument Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti, verzia 2, CSIRT.SK

- pracovné stanice

- OS Windows

Prínos práce

- implementácia – uľahčenie zabezpečenia IT systémov pre ich správcov

- analýza požiadaviek z metodiky

Návrh riešenia implementácie

- manuálne NIE
- skripty
  - Command Prompt NIE
  - PowerShell ÁNO

Štruktúra skriptov

- *Master.ps1* – hlavný skript, spúšťa všetky ostatné

- skripty pre jednotlivé opatrenia
  - *názov_opatrenia.ps1* alebo *názov_opatrenia_$os*, kde *$os* = verzia OS

Master skript

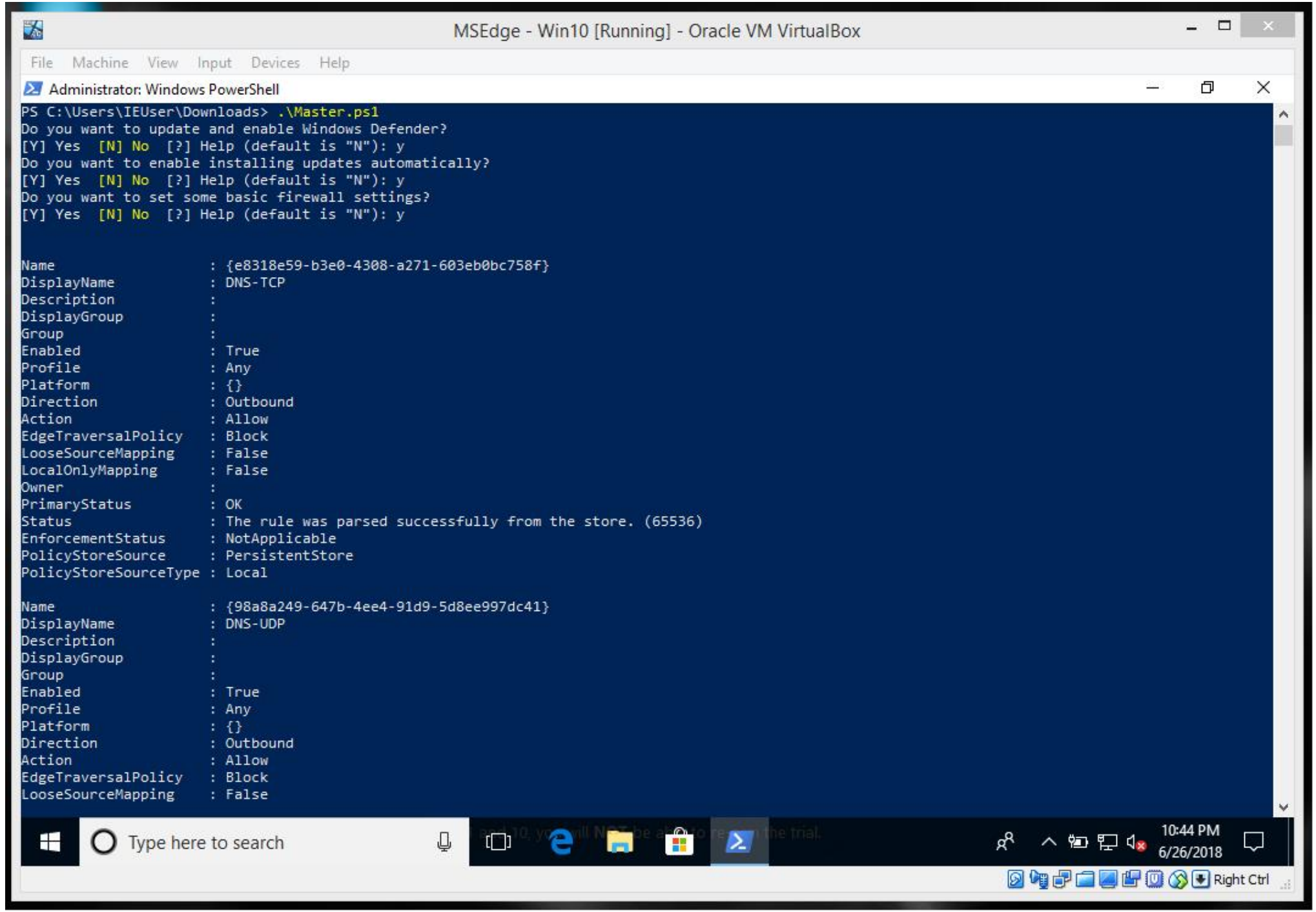
- zistenie verzie OS z *[System.Environment]::OSVersion.Version*

- spúšťanie skriptov pre jednotlivé opatrenia:

```
& ".\opatrenie_1.ps1"
& ".\opatrenie_2_$os.ps1"
& ".\opatrenie_3.ps1"
...
```

Ostatné skripty

```
$message = "Do you want to ... ?"
$yes = New-ObjectSystem.Management.Automation.Host.ChoiceDescription "&Yes", `
  "..."
$no = New-Object System.Management.Automation.Host.ChoiceDescription"&No", `
  "..."
$options = [System.Management.Automation.Host.ChoiceDescription[]]($yes, $no)
$result = $host.ui.PromptForChoice($title, $message, $options, 1)
switch ($result) {
  0 { TO DO }
  1 { TO DO }
}
```


MSEdge - Win10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
PS C:\Users\IEUser\Downloads> .\Master.ps1
Do you want to update and enable Windows Defender?
[Y] Yes [N] No [?] Help (default is "N"): y
Do you want to enable installing updates automatically?
[Y] Yes [N] No [?] Help (default is "N"): y
Do you want to set some basic firewall settings?
[Y] Yes [N] No [?] Help (default is "N"): y
Name : {e8318e59-b3e0-4308-a271-603eb0bc758f}
DisplayName : DNS-TCP
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform : {}
Direction : Outbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : The rule was parsed successfully from the store. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local
Name : {98a8a249-647b-4ee4-91d9-5d8ee997dc41}
DisplayName : DNS-UDP
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform : {}
Direction : Outbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
Type here to search
10:44 PM
6/26/2018
Right Ctrl

Implementácia opatrení

Windows Registry

- väčšina opatrení

- *Set-ItemProperty $dir -Name ... -Type ... -Value ...*
  - *nastavenie hodnoty*
- *New-Item $dir*
  - *vytvorenie nového kľúča*

- opatrenia - právo inštalácie softvéru, UAC, zamykanie obrazovky, AutoRun, automatické aktualizácie, ...

AppLocker

- nástroj pre aplikačný whitelisting
- je súčasťou vyšších edícií Windowsov
- využitie špeciálnych cmdletov pre AppLocker
  - *Import-Module AppLocker*

AppLocker

$i = Get-AppLockerFileInformation -Directory ... -Recurse -FileType ...

$p = $i | New-AppLockerPolicy -IgnoreMissingFileInformation -Optimize -RuleType ... -User ... -RuleNamePrefix ...

$p | Set-AppLockerPolicy [-Merge]

EMET

- Enhanced Mitigation Experience Toolkit
- ochrana proti známym typom útokov
- inštalácia pomocou príkazu *msiexec.exe*

  Start-Process C:\Windows\System32\msiexec.exe -Wait -ArgumentList '/i "EMET Setup.msi" /passive /norestart‘

- použitie predkonfigurovaných nastavení

Záver

- implementácia 21 opatrení – 31 skriptov + Master

- možnosti pokračovania – rozšírenie a doplnenie niektorých opatrení, napr.:
  - konfiguračné skripty pre AppLocker, Firewall
  - blokovanie spúšťania skriptov pre ostatné prehliadače
  - …

Ďakujem za pozornosť

Otázky z posudku

- testovanie
  - na virtuálkach pre všetky cieľové verzie Windows (7, 8.1 ,10)

- vplyv architektúry x64/x86
  - priečinok Program Files (x86)
  - Wow6432Node vo Windows Registry