PS + BASH Advanced labbar

Utbildare: Stefan Holmberg

stefan.holmberg@nackademin.se

NACKADEMIN

Powershell - piping

ls -File

ls -File | Sort-Object -Descending

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         5/16/2016   1:15 PM          32972 test.log
```

Detta är properties!

ls File | Sort-Object -Property Length –Descending

ls File | Sort-Object -Property Length –Descending | Select-Object -First 1

NACKADEMIN

```powershell
$list = ls -File | Sort-Object -Property Length -Descending
$list
```

```
PS C:\Users\stefan> $list.Length
3
PS C:\Users\stefan> $list.GetType()

IsPublic IsSerial Name                                     BaseType
-------- -------- ----                                     --------
True     True     Object[]                                 System.Array


PS C:\Users\stefan> $list.Length
3
PS C:\Users\stefan>
```

Powershell - piping

```
$list[0]
```

```
$list[0] | Get-Member
```

```
$list[0].Fullname
```

NACKADEMIN

Bash Piping

ls

ls -l

ls -l -S | sort -k5 -r

(skicka resultatet till sort. Som sorterar på Kolumn 5...reverse
Testa på tex /bin)

Låt oss ta de 5 största:

ls -l -S | sort -k5 -r | head -5

Calling shellcommands from within script

```
#!/bin/bash
IPLIST="path_to_the_Ip_list_file"


for ip in $(cat $IPLIST)

do
    ping $ip -c 1 -t 1 &> /dev/null
    if [ $? -ne 0 ]; then

        echo $ip ping faild;

        else

        echo $ip ping passed;

    fi

done
```

Cat - to list :)
Ping

NACKADEMIN

GRUPPLABBAR

Powershell och Bash

NACKADEMIN

#1 Lista alla IPV4-adresser (svårighetsgrad 3)

Ett och samma script ska funka såväl på Windows som på Mac och Linux.

PS: https://stackoverflow.com/questions/44703646/determine-the-os-version-linux-and-windo

1. Undersök hur ni ska kunna köra olika kod på Windows/icke windows
2. Googla och skriv kod för att lista IP addresser med Powershell på Windows
3.Googla och skriv kod för att lista IP addresser med Powershell på Linux

Bash: https://stackoverflow.com/questions/3466166/how-to-check-if-running-in-cygwin-mac-o

1. Undersök hur ni ska kunna köra olika kod på Windows/icke windows
2. Googla och skriv kod för att lista IP addresser med Bash på Windows
3.Googla och skriv kod för att lista IP addresser med Bash på Linux

#2 Intrusion detection (svårighetsgrad 5)

Skriv ett script som

Scannar IP Addresser i nätet (nmap,arp)
För varje IP-address hittas – kolla om finns i filen WHITELIST.TXT
Om inte skriv till INSTRUSION.TXT (format = timestamp;ip)

VALFRITT: PS och eller BASH

NACKADEMIN

#3 Send email – testa att skicka mail genom din Gmail? (svårighetsgrad 1)

Googla! Få det att funka från BASH och POWERSHELL

NACKADEMIN

#4 Get Antivirus status (svårighetsgrad 3)

https://gallery.technet.microsoft.com/Information-about-bf8b201f

```
ComputerName            SoftwareName                            UpToDate        Enabled
------------            ------------                            --------        -------
PC02                    Microsoft Security Essentials           True            True
PC03                    AVG AntiVirus Free Edition              True            False
PC04                    avast! Antivirus                        False           True
#>
```

Bara på lokal?

NACKADEMIN

#5 Log search (svårighetsgrad 4)

ftp://ita.ee.lbl.gov/html/contrib/NASA-HTTP.html

Gör ett script som läser igenom alla filer i ett bibliotek och letar efter en speciell IP-address

Rader med träff ska kopieras in i ny fil: suspects/YYYYmmDD.txt

När en fil lästs ska den byta namn till .BAK så den inte blir läst igen

#6 Log search – advanced (svårighetsgrad 5)

ftp://ita.ee.lbl.gov/html/contrib/NASA-HTTP.html

Gör ett script som läser igenom alla filer i ett bibliotek och letar efter anrop
Från ett visst land ex NL

http://manpages.ubuntu.com/manpages/trusty/man1/geoiplookup.1.html

```
geoiplookup  uses the GeoIP library and databas
hostname originates from.

For example

geoiplookup 80.60.233.195

will find the Country that 80.60.233.195 origin

NL, Netherlands
```

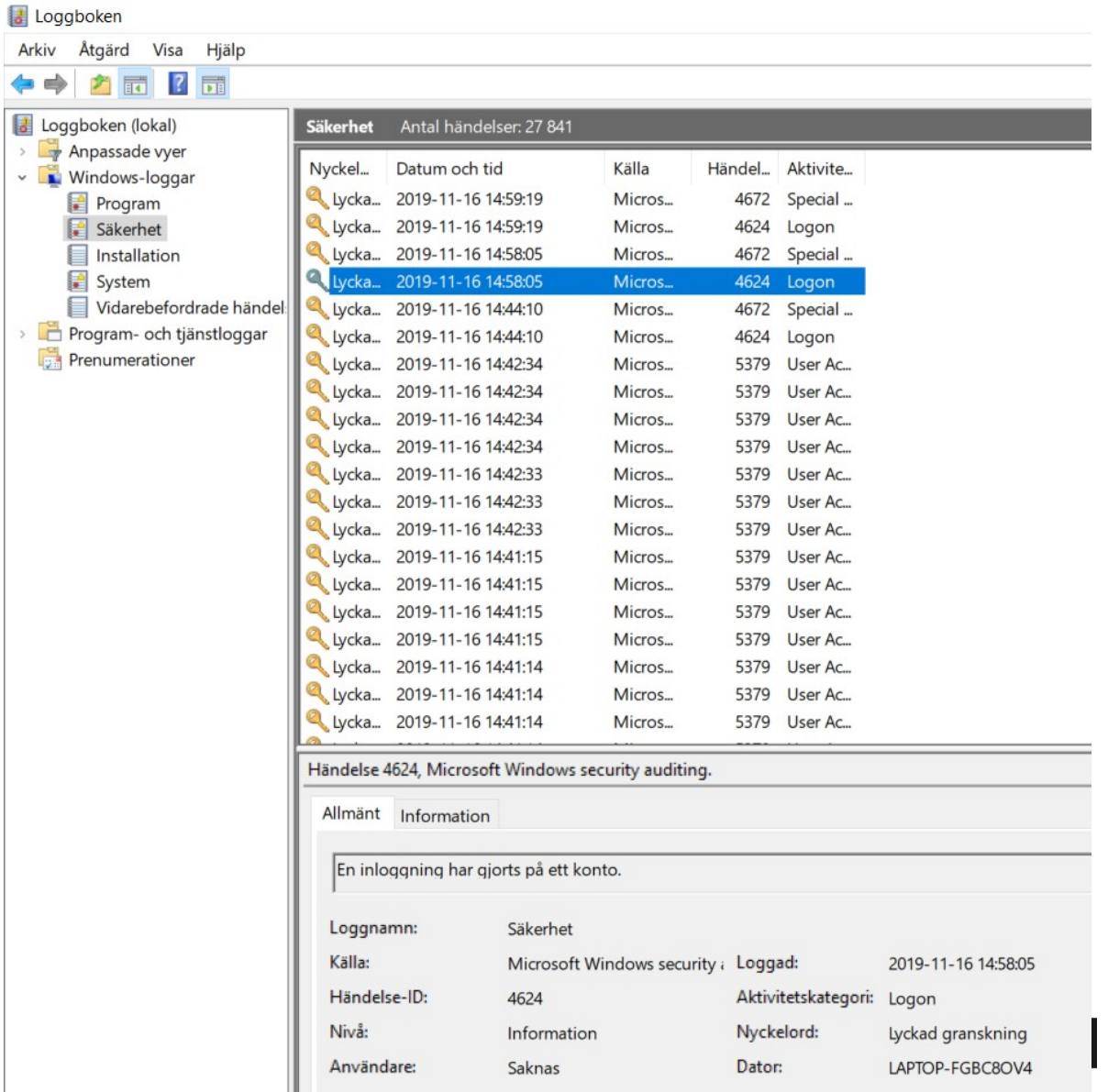
NACKADEMIN

#7 Powershell – Reading EventLog on Windows (svårighetsgrad 3)

Follow tutorials here

https://blog.netwrix.com/2015/04/06/monitoring-event-logs-with-powershell/

https://blog.netwrix.com/2015/04/29/advanced-event-log-filtering-using-powershell/



#8 Bash/PS Pinger (svårighetsgrad 3)

Skriv ett script som

Läser IP Addresser från en textfil
Pingar en i taget och skriver resultat till fil(er).
Diskutera: hur kan man felnotifera bäst???

VALFRITT: PS och eller BASH

NACKADEMIN

#9 Bash/PS MD5 checksum from file (svårighetsgrad 1)

An MD5 checksum is a 32-character hexadecimal number that is computed on a file. If two files have the same MD5 checksum value, then there is a high probability that the two files are the same.

After downloading an software installation package, you can compute the MD5 checksum on the installation file. Use the computed MD5 checksum to compare against the MD5 checksum provided for that installation file on the download page. By doing this, you can verify the integrity of your download.

Ex https://www.openoffice.org/download/checksums/3.4.1_checksums.html

VALFRITT: PS och eller BASH

NACKADEMIN

Download file - remember

Unblock-File

Ex good resources

https://gallery.technet.microsoft.com/site/search?f%5B0%5D.Type=ProgrammingLanguage&f%5B0%5D.Value=PowerShell

https://support.atera.com/hc/en-us/articles/221113188-PowerShell-Scripts-Repository

NACKADEMIN