WindowsBefehlsaufforderung

Suchen nach einem Prozess mit PID

```
C:\>tasklist /FI "PID eq 1192" /FO TABLE
```

Prozesse abhören und anzeigen

```
C:\>netstat -?
Zeigt Protokollstatistiken und aktuelle TCP/IP-Netzwerkverbindungen an.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p Protokoll] [-r] [-s] [-t] [-v]
[Intervall]
-a  Zeigt alle Verbindungen und abhörenden Ports an.
-b  Zeigt die ausführbare Datei an, die beim Erstellen jeder
Verbindung bzw. jedes abhörenden Ports involviert ist. In
einigen Fällen enthalten bekannte ausführbare Dateien mehrere
unabhängige Komponenten. Dann wird die Reihenfolge der
Komponenten angezeigt, die beim Erstellen der Verbindung oder
des abhörenden Ports involviert sind. In diesem Fall befindet
sich der Name der ausführbaren Datei unten in []. Oben
befindet sich die aufgerufene Komponente usw., bis TCP/IP
erreicht wurde. Bedenken Sie, dass diese Option viel Zeit in
Anspruch nehmen kann und fehlschlägt, wenn Sie nicht über
ausreichende Berechtigungen verfügen.
-e  Zeigt die Ethernet-Statistik an. Kann mit der Option -s
kombiniert werden.
-f  Zeigt vollqualifizierte Domänennamen für Remoteadressen an.
```

```
-n  Zeigt Adressen und Portnummern numerisch an.
-o  Zeigt die mit jeder Verbindung verknüpfte, übergeordnete
Prozesskennung an.
-p  Protokoll Zeigt Verbindungen für das angegebene Protokoll an.
Protokoll kann sein: TCP, UDP, TCPv6 oder UDPv6.
Bei Verwendung mit der Option -s kann Protokoll Folgendes
Sein: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP oder UDPv6.
-r  Zeigt den Inhalt der Routingtabelle an.
-s  Zeigt die Statistik protokollweise an. Standardmäßig werden
IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP und UDPv6 angezeigt.
Mit der Option -p können Sie dies weiter einschränken
-t  Zeigt den aktuellen Abladungsstatus der Verbindung an.
-v  In Verbindung mit -b wird die Reihenfolge der Komponenten
angezeigt, die beim Erstellen der Verbindung oder des
abhörenden Ports für alle ausführbaren Dateien involviert
sind.
Intervall Zeigt die gewählte Statistik nach der mit Intervall angege-
benen Anzahl von Sekunden erneut an. Drücken Sie STRG+C zum
Beenden der Intervallanzeige. Ohne Intervallangabe werden
die aktuellen Konfigurationsinformationen einmalig
angezeigt.
```

Das Ergebnis (Ausgabe des Befehls) in eine Datei speichern

```
C:\>netstat -a > C:\netstat.txt
```

Die Suche mit findstr() verfeinern

```
C:\>netstat -ano |  findstr /r 0.0:80 && netstat -ano |  findstr :6066 TCP 0.0.0.0:80 0.0.0.0:0
ABHÖREN 4 TCP 0.0.0.0:808 0.0.0.0:0 ABHÖREN 4256 TCP 0.0.0.0:8008 0.0.0.0:0 ABHÖREN 5940 TCP
0.0.0.0:8009 0.0.0.0:0 ABHÖREN 5940
```

Netsh

- Für HTTP

- `>netsh http show urlacl - Lists DACLs for the specified reserved URL or all reserved URLs.`

Revision #1
Created 16 September 2018 21:01:03 by Mario
Updated 16 September 2018 21:01:15 by Mario