Windows 7 - Whoami

Bei Windows 8/7 und Vista ist die Benutzerverwaltung, die zentrale Stelle zur Verwaltung der angelegten Benutzer. Wer weitere Informationen zu einem Benutzer erfahren möchte, der nutzt den **DOS Befehl „whoami"**.

Whoami liefert Informationen wie z.B. die **SID, Anmelde-ID** eines Users, sowie Gruppenzuordnungen, Berechtigungen und Attribute.

Folgende Möglichkeiten bringt der Befehl zur Ausführung mit:

/upn Zeigt Benutzernamen und Benutzerprinzipalnamen (UPN-Format) an.

/fqdn Zeigt Benutzernamen mit dem vollständig qualifizierten Domänennamen(FQDNFormat) an.

/user Zeigt Informationen über den Benutzer mit der Sicherheitskennung (SID) an.

/groups Zeigt die Gruppenmitgliedschaft, die Sicherheitskennungen (SID) und Attribute an.

/priv Zeigt die Berechtigungen des Benutzers an.

/logonid Zeigt die Anmeldekennung des Benutzers an.

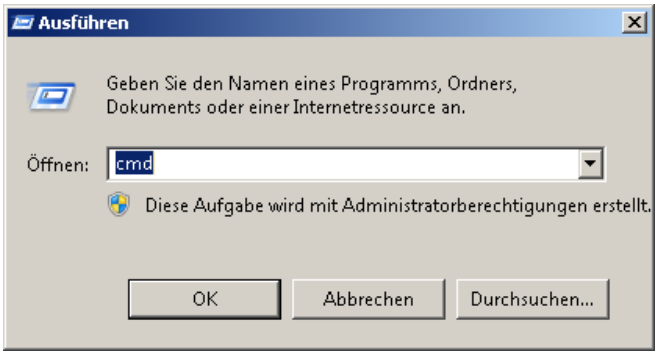
/all Zeigt den Benutzernamen, Gruppenmitgliedschaften mit den Sicherheitskennungen (SID) und Berechtigungen für das aktuelle Benutzerzugriffstoken an.

/fo *format* Bestimmt das Ausgabeformat: Gültige Werte: TABLE,LIST oder CSV. Spaltenheader werden nicht im CSV-Format angezeigt. Standardformat: TABLE.

/nh Legt fest, dass der Spaltenheader nicht in der Ausgabe angezeigt wird. Gilt nur für die Formate TABLE und CSV.

/? Zeigt Hilfe an

Wir öffnen das Kommandozeilen Tool über Start > Ausführen und dem Befehl CMD.



Eine SID ist ein Sicherheits-Identifikator der automatisch vom System vergeben wird. Anhand dieser SID werden z.B. Systeme, Benutzer und Gruppen identifiziert. Gruppen wie die Administratoren bekommen immer die gleiche SID, damit sie auf allen Systemen wieder zu finden sind. Erleichtert das globale Management!

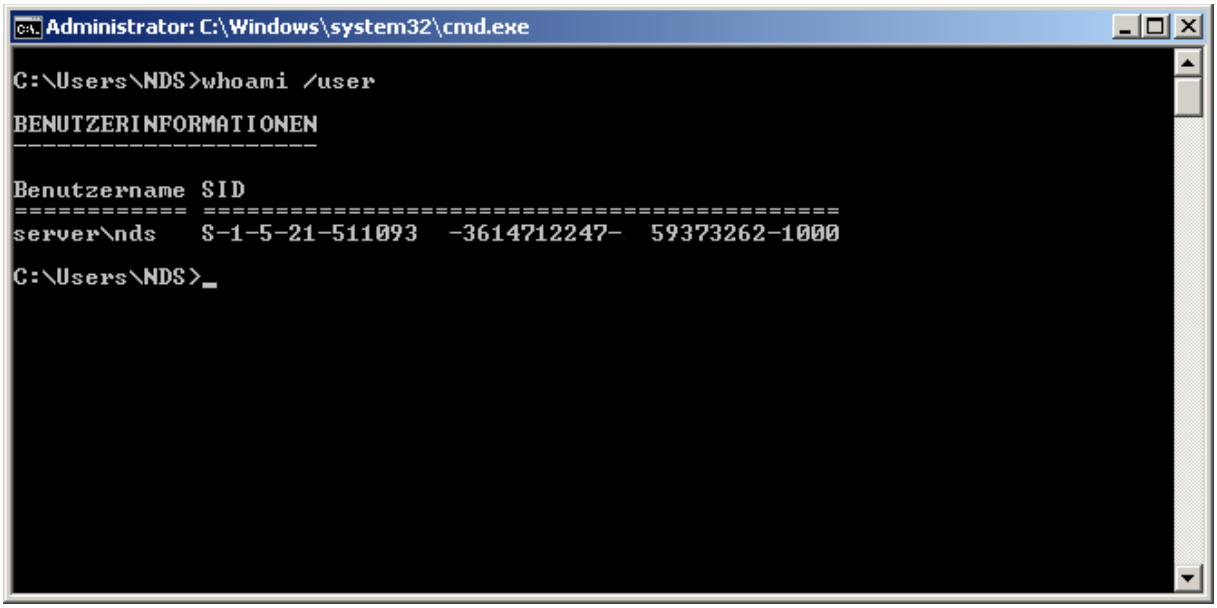
Windows 7 - Whoami

Wie ist eine SID aufgebaut?

Die **SID** besteht aus 5 zusammenhängenden Teilen:

S – steht für SID
1 – für Revisionsnumme
5 – Identifier Authority
21-51109305-3614712247-3759373262 steht für eine Domäne oder lokales System
1000 – ist die Benutzernummer; diese beginnt bei 1000 und wird laufend hochgezählt

Die eigene SID erfahren wir über die Syntax whoami /user

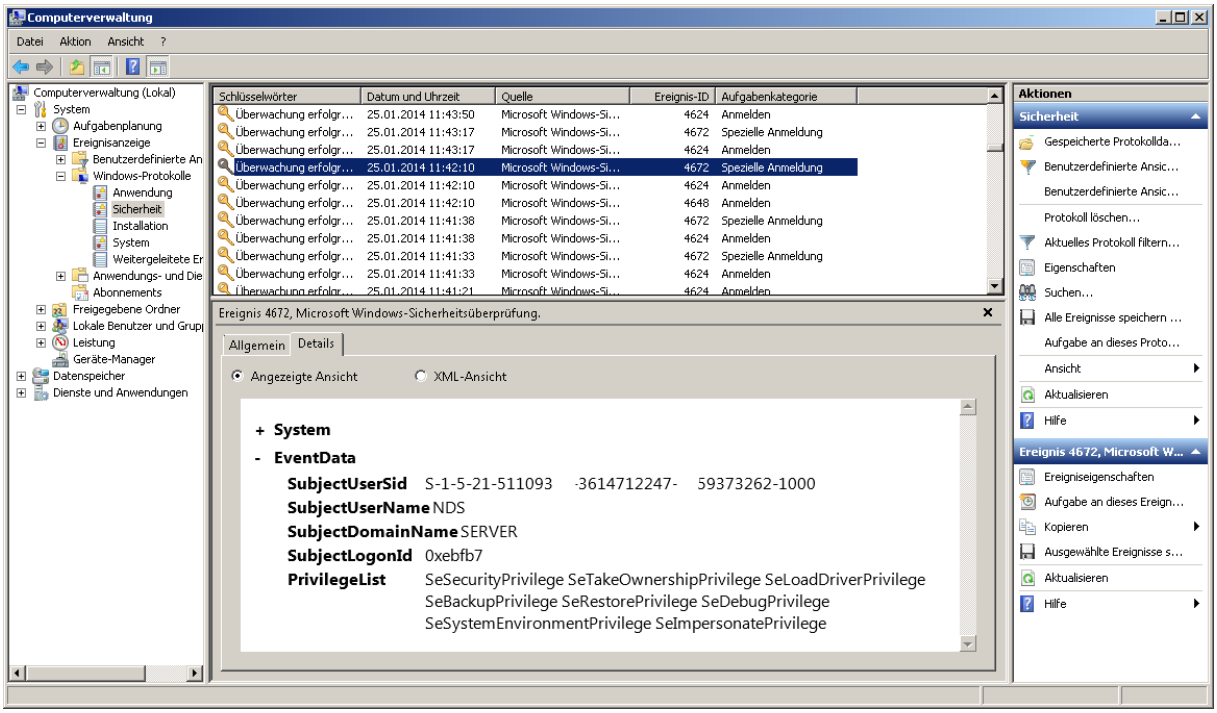


Bei Problemen mit dem System oder Anwendungen, siehe **Event-Logs**, kann die SID eine sehr elementare Information sein.

Wenn wir uns mal die Einträge in der **Sicherheit** anschauen, werden wir einen Eintrag finden, der darauf hindeutet, dass jemand die Besitzrechte eines Orders oder einer Datei übernommen hat. Aus diesem LOG geht außerdem hervor, das es zu jedem Benutzer auf dem System eine feste SID gibt.

Veränderungen die wir am System vornehmen, An- und Abmeldungen usw. werden protokolliert. Anhand der SID ist derjenige der sie ausgelöst hat, immer zu identifizieren.

Windows 7 - Whoami

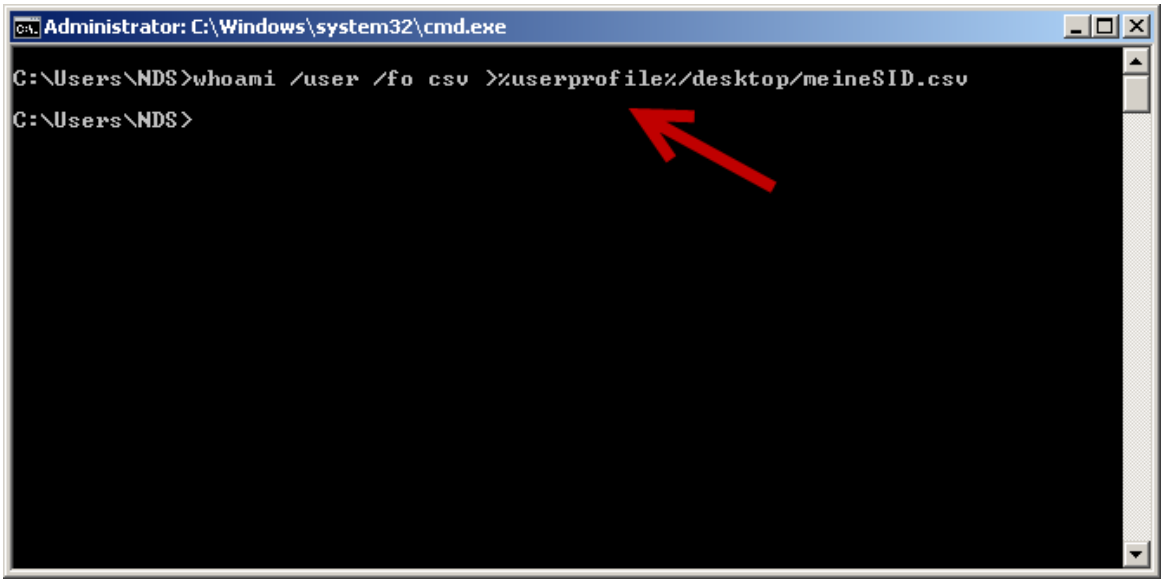


Nun gehen wir einen Schritt weiter.

Wir exportieren unsere SID in eine .csv Datei und öffnen diese mit Excel.

Über die CMD führen wir diesen Befehl aus:

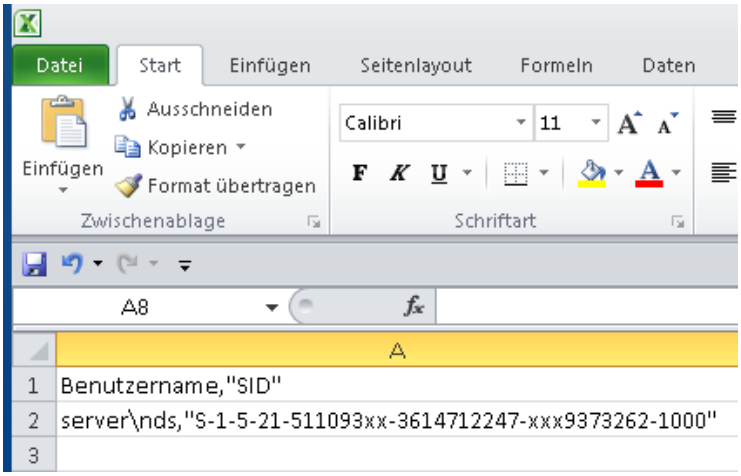
whoami /user /fo csv >%userprofile%/desktop/meineSID.csv



Auf dem Desktop finden wir nun die .csv Datei, meineSID.csv.

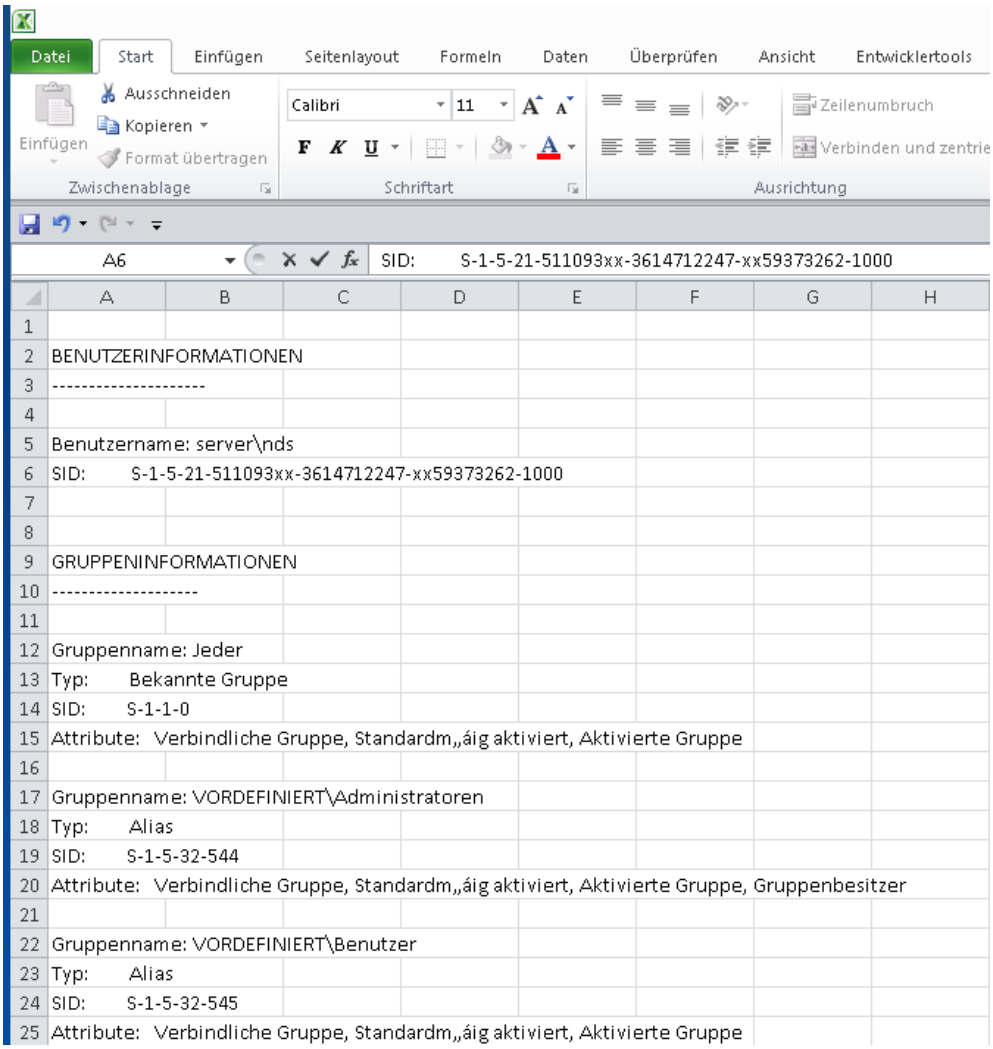
Windows 7 - Whoami

Der Inhalt deckt sich mit dem aus der DOS-BOX.



Jetzt exportieren wir alle bekannten SIDs und zwar mit dem Befehl:

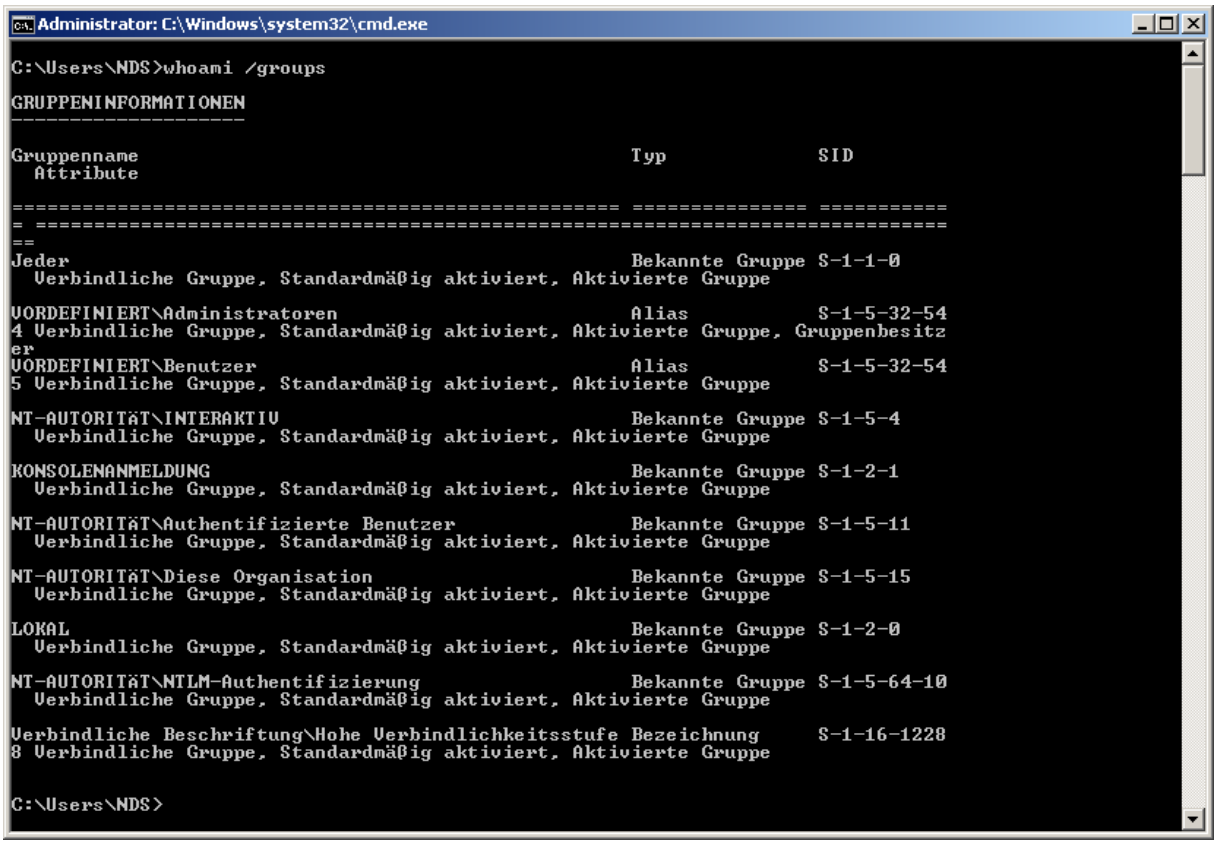
whoami /all /fo list >%userprofile%/desktop/meineSIDs.csv



Die Liste ist recht lang und beinhaltet darüber hinaus auch noch Informationen zu „Berechtigungsinformationen".

Windows 7 - Whoami

Mit dem Befehl **whoami /groups** lassen wir uns anzeigen in welchen Gruppen wir uns mit unserer aktuellen Logon-Session befinden.

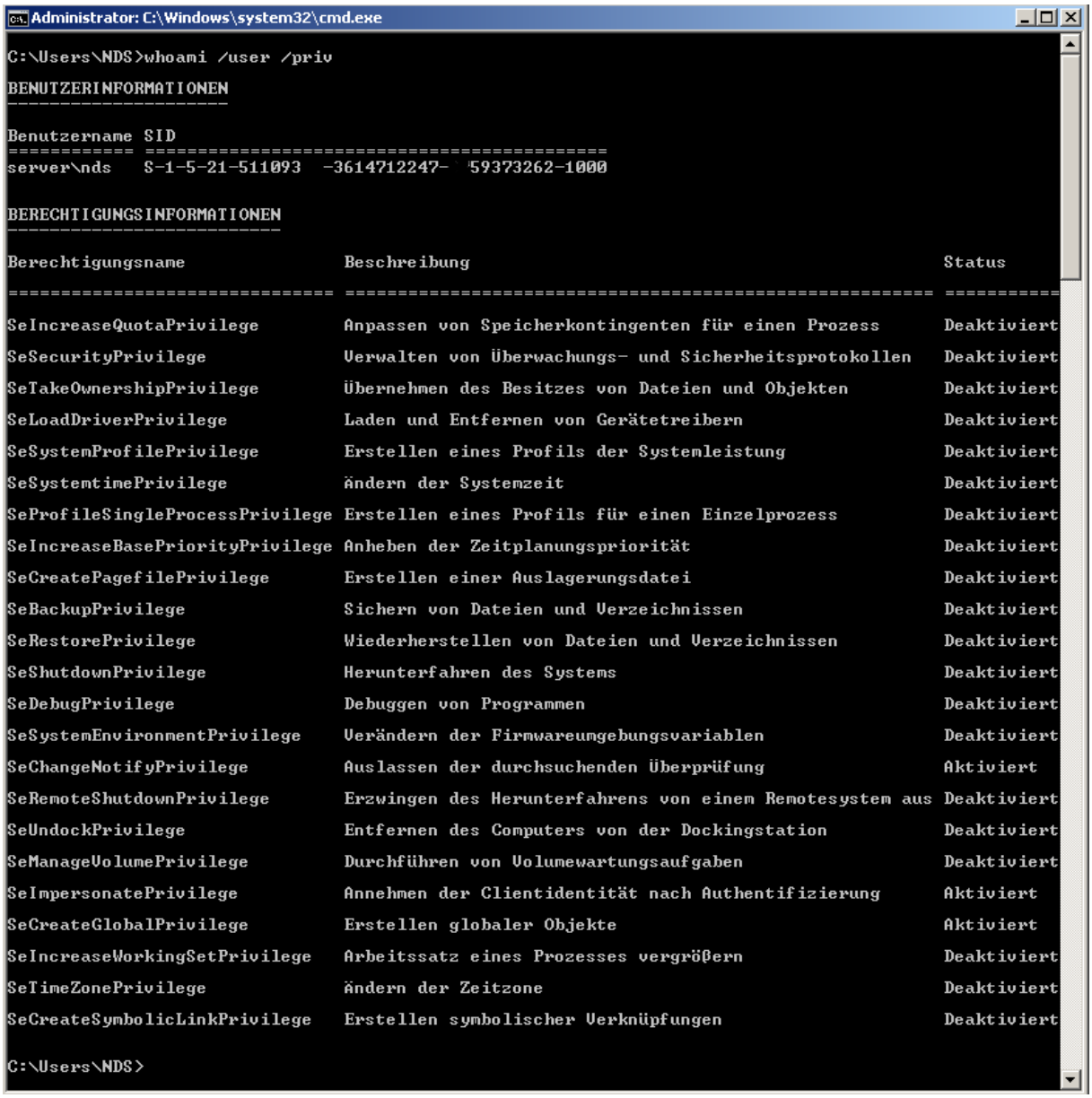


In einer Domäne lassen sich weitere Informationen ermitteln und anzeigen.

Jetzt möchten wir wissen welche **Berechtigungen** wir haben. Das lassen wir uns mit dem Befehl **whoami /user /priv** anzeigen. Das Ergebnis sehen wir auf der nächsten Seite.

Als Einführung in den Befehl whoami (who i am) sollte diese kleine Lektüre reichen.

Windows 7 - Whoami



Natürlich lassen sich auch diese Informationen in eine Datei speichern.

whoami /user /priv >%userprofile%/desktop/meineSIDs.txt