Studienprogramm Sachbearbeiter:in Digitale Forensik
Praktikum Betriebssysteme
Dozenten: Tim Wetterau
wetterau@hs-mittweida.de
Stand: 08.07.2024

HOCHSCHULE MITTWEIDA
University of Applied Sciences

Betriebssysteme

Windows Zusammenfassung

Dieses Praktikum stellt den Abschluss der Praktikumsreihe Windows im Modul Betriebssysteme dar. In den vergangenen Vorlesungseinheiten haben Sie viele Kenntnisse erlernt zur forensischen Analyse in Windows. Diese konnten Sie teilweise schon in praktischen Einheiten anwenden und Ihr Wissen testen. Zum Abschluss des Moduls, soll dieses Praktikum eine Art Capture The Flag darstellen, bei dem Sie auf einem Windows-System einige Artefakten finden sollen mit dem Wissen, welches Sie über den Verlauf des Moduls erhalten haben. Dazu sind folgende Modulinhalte von Relevanz und helfen Ihnen bei der Durchführung des Praktikums.

Inhalte des Praktikums:

- Benutzeranmeldung
- Umgang mit der Registrierungsdatenbank
- Umgang mit Passwort Cracking Tools
- Volumen-Schatten-Kopien
- EFS-Verschlüsselung

Vorbereitung

Zur Durchführung des Praktikums wird Ihnen eine Windows 10 VM zur Verfügung gestellt, welche Sie sich unter dem folgenden Link (extern - 1.) herunterladen können oder direkt auf ihr lokales Laufwerk extrahieren können (intern - 2.):

1. https://download.hs-mittweida.de/intranet/R:/CB/Wetterau/Sachbearbeiter_in-Digitale-Forensik/Betriebssysteme/Pr%c3%a4senz/
2. R:\CB\Wetterau\Sachbearbeiter_in-Digitale-Forensik\Betriebssysteme\Präsenz\

Entpacken Sie die ZIP-Datei in ein lokales Verzeichnis und öffnen Sie die VBOX-Datei mit einem Doppelklick, um die Daten in VirtualBox einzubinden. Sie sollten nun die Möglichkeit haben die VM in VirtualBox zu nutzen.

Laden Sie sich außerdem unter dem 1. Link die ISO-Datei herunter. Diese enthält alle wichtigen Daten und Anwendungen, welche Sie zum erfolgreichen Abschluss des Praktikums benötigen. Gehen Sie daraufhin in die Einstellungen der VM in VirtualBox und binden Sie unter Massenspeicher die ISO in das optische Laufwerk ein. Die Gasterweiterungen sind bereits auf dem System installiert und Sie müssen diese nicht noch einmal installieren.

Sollte der Download mit anschließendem Import der ZIP (VBOX)-Datei nicht funktionieren, haben Sie noch die Möglichkeit die VM mittels einer OVA-Datei herunterzuladen. Diese finden Sie ebenfalls unter dem oben aufgeführten Link. Sie müssen diese Datei nur herunterladen und installieren, wenn die VBOX-Datei NICHT funktioniert, ansonsten können Sie sich diesen Schritt sparen.

Benutzeranmeldung auf dem System

Fahren Sie zuerst das System hoch und schauen Sie nach einem Benutzer in der Auswahl, der Ihnen bekannt vorkommt. Sie kennen auf alle Fälle aus den vorherigen Praktika den **`Nutzer1`** mit dem **`Kennwort1`**. *Melden Sie sich mit diesem an!*

Sie können nun im folgenden Verlauf dieses Praktikums den Nutzer1 zu Untersuchungen und Analysen verwenden. Ziel ist es, das Geheimnis des BigBlueMonsters zu finden. Er scheint auf dem System etwas zu verstecken, was nicht jeder sehen kann. *Ihre Aufgabe ist es, die Dateien zu finden und diese anschließend einzusehen.*

Auffinden der verschlüsselten Dateien

Sie wissen nun, dass es auf dem System versteckte Daten geben muss. Jetzt stellt sich die Frage, wie man diese Daten finden kann, ohne das ganze Dateisystem auf den Kopf zu stellen. Dafür bietet sich die PowerShell an. Wir können ein Kommando nutzen, welches die Attribute der Dateien vergleicht, die eingegeben werden und nur die Dateien ausgibt, welche auf die gesuchten Attribute zutrifft. Das gesuchte Attribut ist **`Encrypted`**

Mit einer Kombination aus Powershell-Befehlen können wir nun geschickt, die verschlüsselten Daten extrahieren. Nutzen Sie dazu nacheinander die beiden Kommandos:

```
$ $enc = [System.IO.FileAttributes]::Encrypted
$ dir C:\ -Recurse -ErrorAction silentlycontinue -Force | where {($_.Attributes -band $enc) -
    ne 0} | select FullName
```

Nehmen Sie sich einen Moment Zeit und überlegen Sie, wie der Befehl funktioniert. Überlegen Sie sich was dazu zuerst, welches Zweck die zweite Zeile verfolgt und welcher Vergleich der der where-Klausel und dem Operator -band durchgeführt wird. Anschließend sollten Sie sich den Inhalt der ersten Zeile erschließen.

Setzen Sie beide Befehle in einer PowerShell ab und schauen Sie sich die Ergebnisse an! Welche Feststellung können Sie treffen? Folgen Sie dem Pfad der verschlüsselten Datei und schauen Sie sich diese an. Sind die Ergebnisse wie erwartet???

- **Dateien wurden gefunden**
- **Kann die Datei öffnen → falscher Inhalt**

Suche nach versteckten Artefakten

Sie haben ja hoffentlich die Datei mit dem verschlüsselten Inhalt und damit auch {FLAG-1} gefunden. Glückwunsch. Doch diese Datei ist nicht die, die Sie suchen. Gehen Sie dem Hinweis nach und schauen Sie nach anderen Laufwerken. Nutzen Sie dazu den Dateiexplorer! *Welche weiteren Laufwerke können Sie auf dem System ausfindig machen?*

- **Keine. Es sind keine weiteren Laufwerke eingebunden.**

Überlegen Sie sich, wie Sie nach anderen Laufwerken suchen können und starten Sie das entsprechende Tool!

- **Microsoft Management Console → Datenträgerverwaltung**
- **Datenträgerverwaltung direkt auswählen**
- **diskpart (Kommandozeile)**

Schauen Sie, ob Sie weitere Laufwerke finden. *Welche Laufwerke (Volumes) sind auf dem System eingerichtet? Welche der Laufwerke könnten für eine weitere Untersuchung von Interesse sein? Wie unterscheiden sich die evtl. interessanten Laufwerke von dem Laufwerk* ***`C:`****?*

- **Systemreservierte Partition** **50MB** **→ Standard**
- **Windows-Volume** **48GB** **C:** **→ bekannt**
- **FLAG-2** **1GB** **→ das sollte man sich näher anschauen**
- **Wiederherstellungspartition** **525MB** **→ Standard**

➔ **Bei dem Volume FLAG-2 fehlt der Laufwerksbuchstabe**

Nutzen Sie das Tool, welches Sie für das Ansehen der Datenträger verwenden und machen Sie das Volume wieder sichtbar, indem Sie diesem einen Laufwerksbuchstaben zuweisen. Überprüfen Sie anschließend im Dateiexplorer, ob das Zuweisen zum Erfolg geführt hat. Sie könnten sich nun händisch auf die Suche nach der Datei machen, aber da wären Sie mit Sicherheit länger beschäftigt. *Nutzen Sie zur Suche erneut das Skript bzw. Befehlsfolge, um verschlüsselte Dateien im Dateisystem des neuen Laufwerks zu finden!*

```
$ $enc = [System.IO.FileAttributes]::Encrypted
$ dir <LW>:\ -Recurse -ErrorAction silentlycontinue -Force | where {($_.Attributes -band $enc)
    -ne 0} | select FullName
```

Sie müssten nun den Pfad erhalten haben, auf dem sich die Dateien tatsächlich befinden. *Navigieren Sie dort hin und schauen Sie sich den Inhalt des Ordners an. Sehen Sie dort etwas? Erinnern Sie sich, wie versteckte Inhalte sichtbar gemacht werden können im Dateiexplorer und machen Sie die Inhalte anschließend wieder sichtbar!*

Können Sie den Ordner öffnen bzw. den Inhalt der Dateien sehen?

- **Ordner kann geöffnet werden, Dateiinhalte können aber nicht eingesehen werden**

Warum können Sie auf die Dateien nicht zugreifen? Finden Sie heraus, wem die Dateien gehören! Was müssen Sie tun, damit Sie die Dateien als Nutzer1 einsehen können?

- **Dateien sind verschlüsselt mittels EFS**
- **Die Dateien gehören BigBlueMonster → Eigenschaften der Datei anzeigen lassen → unter Reiter Details → Besitzer**
- **Zertifikat der EFS-Verschlüsselung von BigBlueMonster exportieren und als Nutzer1 importieren**

Erstellung einer Volumen Schatten Kopie

Sie wissen also nun, warum Sie die Dateien nicht einsehen können. Um die Zertifikate zu exportieren, brauchen Sie allerdings Zugang zum Benutzeraccount des Besitzers. Dieses sollten Sie sich nun verschaffen. *Was benötigen Sie, um an die Zugangsdaten eines Benutzers zu kommen? In welchem Format bzw. mit welchem Hashverfahren welchen die Passwörter von Nutzern unter Windows gespeichert?*

- **Die Registryhive SAM mit den Verschlüsselten Passwörtern und die SYSTEM-Datei**
- **NTLM-Hashes sind Standard unter Windows seit Windows Vista**

Wie wir bereits aus den vorherigen Praktika wissen, ist es allerdings nicht möglich diese Datei im laufenden Betrieb zu öffnen bzw. auf diese zuzugreifen. Dazu haben Sie kennengelernt, dass es eine Möglichkeit diese auch während des laufenden Betriebs zu extrahieren - mittels VSS. Wenden Sie nun folgend Ihr Wissen an, um eine Volumenschattenkopie des Laufwerks C: zu erstellen!

Öffnen Sie dazu eine neue Eingabeaufforderung und nutzen Sie den folgenden Befehl, um eine neue Volumenschattenkopie des Laufwerks C: zu erstellen:

```
$ wmic shadowcopy call create Volume=C:\
```

und lassen Sie sich die Erfolgreiche Erstellung quittieren mit:

```
$ vssadmin list shadows
```

Sie sollten nun sehen, dass es eine Kopie des Laufwerks C: gibt. Diese wollen wir nun einbinden, damit wir die Daten von dem Laufwerk extrahieren können, die wir benötigen, um die Passwörter zu knacken. Gehen Sie dazu wieder in den Dateiexplorer und wählen mit einem Rechtsklick auf das Laufwerk C: die **Eigenschaften** dessen aus. Dort navigieren Sie zum Reiter „**Vorgängerversionen**“. Dort sehen Sie eine Volumenschattenkopie, welche Sie anschließend mit einem Doppelklick darauf öffnen. Auf die eingebundene Kopie können Sie nun im Dateiexplorer unter dem Pfad „**`C$:\`**“ zugreifen. Navigieren Sie dort zu dem Pfad, unter dem sich die Datei befindet, welche wir brauchen! Sie werden evtl. feststellen, dass Sie auf den Ordner, in dem sich die Datei befindet, keinen Zugriff haben. *Kopieren Sie sich das Verzeichnis einfach auf den Desktop und versuchen Sie es dann erneut von dort aus zu öffnen.*

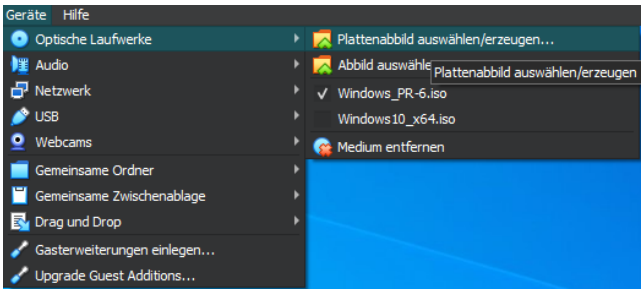
- **`C$:\Windows\System32\Config\SAM bzw. \SYSTEM`**
- **config Ordner kopieren auf den Desktop**

Zur Vereinfachung des späteren Befehls kopieren Sie sich die beiden Dateien aus dem **`config`** Verzeichnis heraus und legen Sie sich diese direkt unter den Pfad **`C:\`**

Extrahieren des Passworthashes

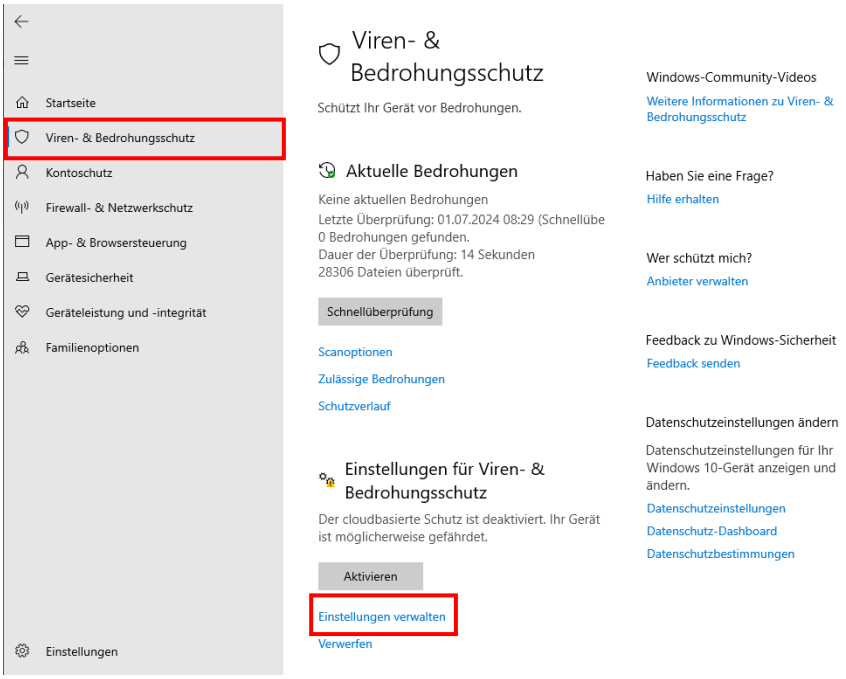
Im Moment haben wir die beiden Hives, die für das Knacken des Passwortes wichtig sind aus der Schattenkopie extrahiert. Allerdings wurde im 10th-Anniversary Update die Überschlüsselung der Windows Passwörter geändert, weshalb das bisherige Vorgehen nicht mehr funktionierte. Tools, wie samdump2, funktionieren nicht mehr, ebenso wie das später verwendete Ophcrack.

Wir brauchen demnach ein Tool, welches mit der neuen Speicherung der Passwörter umgehen kann und die Hashes extrahiert. Dazu wollen wir das Tool **mimikatz** nutzen. Mimikatz ist ein Projekt für „Sicherheitstestzwecke“ in Windows und eignet sich hervorragend zum Extrahieren der Benutzerinformationen und zum Knacken des Passwortes. Um das Tool zu nutzen, sollten Sie an dieser Stelle die ISO-Datei einbinden, welche Sie anfänglich heruntergeladen haben. Gehen Sie dazu in der oberen Menüleiste in Ihrem VM-Fenster auf „**Geräte**“ → „**Optische Laufwerke**“ → „**Plattenabbild auswählen/erzeugen**“.



Im erscheinenden Menü wählen Sie den Punkt „**Hinzufügen**“ aus und suchen dann auf dem Dateisystem die heruntergeladene ISO-Datei und wählen diese aus. Nachdem Öffnen der ISO-Datei klicken Sie erneut „**Auswählen**“ in VirtualBox und haben nun Ihre ISO-Datei fertig eingebunden. Nun kann auf diese mittels des Dateiexplorers in der Windows-VM zugegriffen werden.

Mimikatz befindet sich im Verzeichnis „mimikatz_trunk2\x64\mimikatz.exe“. Starten sie die Datei am besten mit Administratorenberechtigungen. Möglicherweise wird der Windows Defender anschlagen, dass es sich bei der Software um Malware handelt und lässt Sie das Programm nicht ausführen. Zur vorübergehenden Deaktivierung des Defender gehen Sie in der Taskleiste der VM auf den Pfeil nach oben und auf das Icon des Windows Defenders.



Wechseln Sie in den Tab „Viren- und Bedrohungsschutz“ und wählen dort den Eintrag „Einstellungen verwalten“ aus unter „Einstellungen für Viren- & Bedrohungsschutz“. Im erscheinenden Menü deaktivieren Sie einfach den Echtzeitschutz und das Problem sollte behoben sein. Öffnen Sie nun mimikatz, um das Passwort zu extrahieren!

Prüfen Sie zuerst die Rechte auf der mimikatz-Konsole mit dem folgenden Befehl:

```
$ privilege::debug
```

Sie sollten anschließend die Meldung „**`Privilege ,20‘ OK`**“, was Ihnen bestätigt, dass alles laufen sollten. *Nun können Sie mittels des folgenden Befehls den Passworthash von BigBlueMonster extrahieren (Sie müssen ggf. den Pfad anpassen, wenn die Dateien an einem anderen Ort liegen):*

```
$ lsadump::sam /sam:C:\SAM /system:C:\SYSTEM
```

Anschließend sollten Sie eine etwas längere Ausgabe bekommen. *Suchen Sie sich den Eintrag für die BigBlueMonster heraus und kopieren Sie sich den Hash in ein neues Editorfenster! Sie können nun das Editorfenster wieder schließen!*

- `9582f58cbf5013a5aff1f7e5cd2de6de`

Brechen des Benutzerpasswortes

Nachdem wir nun die notwendige Datei haben, können wir uns mit dem Brechen des Passwortes beschäftigen. Dazu gibt es mehrere Varianten, die offline funktionieren:

- Brute-Force Angriff
- Wörterbuchangriff
- Rainbow-Table-Angriff
- Passwort-Reset-Angriff

Wir wollen uns dabei auf einen Rainbow-Table-Angriff konzentrieren. Im Gegensatz zu Linux sind Passwörter unter Windows nicht gesalzen und sind damit gegen Rainbow-Tables anfällig. Zur Durchführung einer solchen Attacke

gibt es mehrere Softwarelösungen. Wir wollen uns hier mit einem schon lang etablierten Tool beschäftigen - Ophcrack.

Auf dem ISO-Abbild befindet sich Ophcrack unter dem Pfad „**`ophcrack-3.8.0-bin/x64/ophcrack.exe`**“ als portable Version des Passwortcrackingtools. Öffnen Sie das Programm mit einem Doppelklick. Ggf. kann der Windows Defender anschlagen, dass es sich bei dem Tool um schadhafte Software handeln könnte. Sie können dort die Software aber bedenkenlos ausführen.

Um ein Passwort mit einer Rainbow-Table zu knacken, müssen wir zuerst eine installieren. Auch diese finden Sie auf der ISO-Datei unter „**`ntlm_700mb`**“. Diese können sie nicht einfach so lesen, sondern müssen diese in Ophcrack einbinden. Gehen Sie dazu in Ophcrack auf den Menüpunkt „**Tables**“ und im unteren Bereich des neuen Fensters auf „**Install**“. Wählen Sie anschließend in der Dialogbox den Ordner mit der Rainbow-Table aus und klicken Sie auch „**Ordner auswählen**“. Opcrack erkennt nun automatisch, dass es sich dabei um die Vista free Tabelle handelt und markiert Ihnen den passenden Eintrag in der Tabelle. Bestätigen Sie nun noch mit „**OK**“ und wir können schon mit dem Knacken beginnen.

Gehen Sie dazu in Ophcrack auf den Menüpunkt Load und wählen Sie den Eintrag „**Single Hash**“. Wir müssen uns jetzt an das gewünschte Format von Ophcrack halten und geben vor dem eigentlichen Hash einen „**`:`**“ ein, sodass wir einen leeren LM-Hash angeben. *Fügen Sie danach einfach den kopierten Hash ein. Ihre Eingabe sollte das folgende Format haben:*

- **`:<extrahierter NTLM-Hash>`**

Jetzt haben wir alles vorbereitet und können nun abschließend auf den Button „**Crack**“ klicken, um den Cracking-Prozess zu starten. Sie sollten nach wenigen Sekunden bereits ein Ergebnis feststellen können. *Wie lautet das Passwort des Nutzers BigBlueMonster?*

- **cookie**

Extraktion des Benutzerzertifikats

Nachdem wir das Passwort des Nutzers erraten haben, können wir uns nun auf die Suche nach dem Zertifikat machen, welches wir zur Einsicht auf die Dateien benötigen. Das benötigte Vorgehen dafür kennen Sie bereits aus Praktikum 3. Daher werden hier die Schritte nur grob beschrieben. *Melden Sie sich zuerst mit dem eben erratenen Passwort an dem Account von BigBlueMonster an.*

Nutzen Sie die Microsoft Management Console und importieren Sie das Snap-In „**Zertifikate**“. *Dort suchen Sie nach eigenen Zertifikaten und exportieren dort das Zertifikat, welches für BigBlueMonster ausgestellt wurde.* In der Spalte für den Zweck des Zertifikats müssten Sie „**Verschlüsselndes Dateisystem**“ finden.

Achten Sie beim Exportieren darauf, dass der private Schlüssel mit exportiert wird und sie sich das gesetzte Kennwort merken, damit Sie das Zertifikat später anwenden können. *Speichern Sie das Zertifikat an einem Ort, an dem alle Nutzer zugreifen können, z.B.* **`C:\Users\Public`**.

Abschluss

Zum Abschluss des Praktikums schauen Sie sich nun die Daten mit dem exportierten Zertifikat aus Sicht von Nutzer1 einmal an. Dazu melden Sie sich wieder als Nutzer1 am System an und suchen auf dem Dateisystem nach dem eben exportierten Zertifikat. Öffnen Sie das Zertifikat mit einem Doppelklick, um es für den aktuellen Nutzer zu importieren. Geben Sie das Passwort für das Zertifikat ein und bestätigen Sie alle Dialogboxen mit OK. Anschließend sollten Sie die Möglichkeit haben, alles Geheimnisse von BigBlueMonster einsehen zu können. *Na, wer hat sich dahinter verborgen???*