



**HOCHSCHULE
MITTWEIDA**
University of Applied Sciences

Betriebssysteme

Praktikum 5 (Teil 1)

Autor: Wetterau, B.Sc.; Hoßfeld, B.Sc.; Prof. Bodach

Stand: 07.07.2023



Bundeskriminalamt

Agenda

1. Vorbereitung/Voraussetzungen
2. Aufgabenbesprechung
3. Durchführung/Ziel

Praktikum 5 (Teil 1)

1. Vorbereitung/Voraussetzungen

1. Vorbereitung/Voraussetzungen

Virtualisierungssoftware:

- **Oracle VM VirtualBox Manager**

Dateien:

- **PRBlock1.iso**
- **Windows10-Pwnd.ova**

Hostsystem:

- **Windows 10/11**

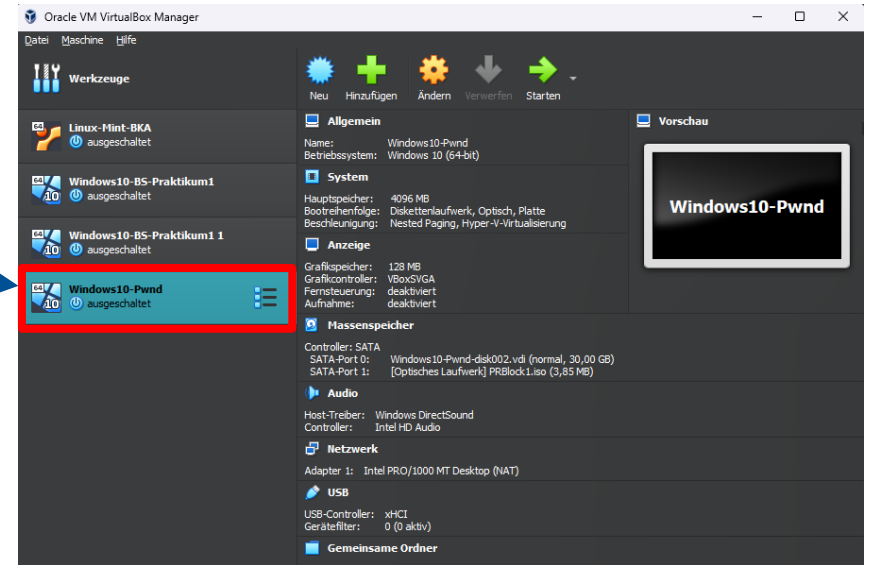


Abb. 1

Index of /intranet/lehre/CB/Bodach/BJA Studiengang/Betriebssysteme/Praktikum Blockwochen/Windows

Name	Last modified	Size	Description
Parent Directory			
PR Block- Windows - Teil 1.pdf	2022-07-04 09:27	1.0M	
PR Block- Windows - Teil 1.txt	2022-06-27 20:04	2.5K	
PR Block- Windows - Teil 2.pdf	2022-07-03 15:20	1.1M	
PR Block- Windows - Teil 2.txt	2022-06-29 15:30	1.5K	
PRBlock1.iso	2022-06-29 15:39	3.9M	
PRBlock2.iso	2022-06-29 15:37	32M	
Windows10-Pwnd.ova	2022-06-27 11:03	7.0G	

Abb. 2

1. Vorbereitung/Voraussetzungen

Allgemeine Hinweise:

Kopieren Sie bitte die **Windows10-BS-Pwnd.ova** Datei und die ISO Datei **PRBlock1.iso** auf ihre lokale Festplatte in ein separates Verzeichnis auf das Sie Zugriff haben, bestenfalls Laufwerk D:.

Abb. 3


Praktikum 5 (Teil 1)

2. Aufgabenbesprechung

2. Aufgabenbesprechung

- Nutzung PowerShell
- Feststellung von Artefakten die auf einen unberechtigten Zugriff bzw. das Ausbringen von Malware hindeuten

Studienprogramm Sachbearbeiter:in Digitale Forensik
Praktikum Betriebssysteme
Dozent: Leander Hossfeld
hossfeld@hs-mittweida.de
Stand: 20.04.2023



Betriebssysteme
Praktikum 5 (Teil 1)
In diesem Praktikum lernen Sie die Nutzung der Powershell und Feststellung von Artefakten, die auf einen unberechtigten Zugriff bzw. das Ausbringen von Malware hindeuten, kennen.

Vorbereitung

Nutzen Sie bitte für die Bearbeitung die bereitgestellte Windows VM:
<https://download.hs-mittweida.de/intranet/lehre/CB/Bodach/BKA%20Studiengang/Betriebssysteme/Praktikum%20Blockwochen/Windows/Windows10-Pwnd.ova>

Zusätzlich finden Sie hier die für das Praktikum zu nutzende ISO-Datei **PRBlock1.iso**:
<https://download.hs-mittweida.de/intranet/lehre/CB/Bodach/BKA%20Studiengang/Betriebssysteme/Praktikum%20Blockwochen/Windows/PRBlock1.iso>

Allgemeine Hinweise

Kopieren Sie bitte die **Windows10-BS-Pwnd.ova** Datei und die ISO Datei **PRBlock1.iso** auf ihre lokale Festplatte in ein separates Verzeichnis, auf das Sie Zugriff haben, bestenfalls Laufwerk D:

Sachverhalt

Am Montag, den 27.06.2022 wurde festgestellt, dass am Wochenende zuvor, dem 25.-26.06.2022 der lokale Rechner kompromittiert wurde. Beim Einloggen des Benutzers Nutzer1 wurde ein automatisches Skript ausgeführt, was den Verdacht nahelegt, dass der Computer gehackt wurde. Zudem wurden über das Netzwerkmonitoring Verbindungen mit dem Rechner von einem Rechner im gleichen Subnetz mit der IP-Adresse 192.168.188.50 festgestellt.

Praktikum 5 (Teil 1)

3. Durchführung/Ziel

3. Durchführung/Ziel


Durchführung:

- selbstständig im eigenen Tempo
- Hilfestellung durch Dozent
- Zeit zur Durchführung (Zeitfenster Stundenplan)
- keine schriftliche Beantwortung nötig

Ziele:

- Nutzung der PowerShell und Feststellung von Artefakten, die auf einen unberechtigten Zugriff bzw. das Ausbringen von Malware hindeuten
- Verständnis und Vertiefung der theoretischen Inhalte

Studienprogramm Sachbearbeiter:in Digitale Forensik
Praktikum Betriebssysteme
Dozent: Leander Hossfeld
hossfeld@hs-mittweida.de
Stand: 20.04.2023



Betriebssysteme

Praktikum 5 (Teil 1)

In diesem Praktikum lernen Sie die Nutzung der PowerShell und Feststellung von Artefakten, die auf einen unberechtigten Zugriff bzw. das Ausbringen von Malware hindeuten, kennen.

Vorbereitung

Nutzen Sie bitte für die Bearbeitung die bereitgestellte Windows VM:

<https://download.hs-mittweida.de/intranet/lehre/CB/Bodach/BKA%20Studiengang/Betriebssysteme/Praktikum%20Blockwochen/Windows/Windows10-Pwnd.ova>

Zusätzlich finden Sie hier die für das Praktikum zu nutzende ISO-Datei **PRBlock1.iso**:

<https://download.hs-mittweida.de/intranet/lehre/CB/Bodach/BKA%20Studiengang/Betriebssysteme/Praktikum%20Blockwochen/Windows/PRBlock1.iso>

Allgemeine Hinweise

Kopieren Sie bitte die **Windows10-BS-Pwnd.ova** Datei und die ISO Datei **PRBlock1.iso** auf ihre lokale Festplatte in ein separates Verzeichnis, auf das Sie Zugriff haben, bestenfalls Laufwerk D:

Sachverhalt

Am Montag, den 27.06.2022 wurde festgestellt, dass am Wochenende zuvor, dem 25.-26.06.2022 der lokale Rechner kompromittiert wurde. Beim Einloggen des Benutzers Nutzer1 wurde ein automatisches Skript ausgeführt, was den Verdacht nahelegt, dass der Computer gehackt wurde. Zudem wurden über das Netzwerkmonitoring Verbindungen mit dem Rechner von einem Rechner im gleichen Subnetz mit der IP-Adresse 192.168.188.50 festgestellt.

Literatur

- Abb. 1: Screenshot (April, 2023)
- Abb. 2: Screenshot (April, 2023)
- Abb. 3: Screenshot (April, 2023)
- Abb. 4: Screenshot (April, 2023)
- Abb. 5: Screenshot (April, 2023)

Vielen Dank



**HOCHSCHULE
MITTWEIDA**
University of Applied Sciences

Prof. Ronny Bodach

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Angewandte Computer- und Biowissenschaften

T +49 (0) 3727 58-1011
F +49 (0) 3727 58-21011
@ bodach@hs-mittweida.de
www.cb.hs-mittweida.de

Haus 8 | Richard-Stücklen Bau | Raum 8-205
Am Schwanenteich 6b | 09648 Mittweida

Tim Wetterau B.Sc., Leander Hoßfeld B.Sc.

T +49 (0) 3727 58-1752
+49 (0) 3727 58-1752
@ wetterau@hs-mittweida.de
hossfeld@hs-mittweida.de

Haus 6 | Grunert de Jacome Bau | Raum 6-031
Am Schwanenteich 4b | 09648 Mittweida

hossfeld@hs-mittweida.de