|  |  |
| --- | --- |
| **Schutzmaßnahmen** | |
| **Name:**   1. Nutzer mit eingeschränkten Rechten 2. Docker Container 3. Erkennung und Beseitigung | **Hauptverantwortlicher**: Dominik Schulz |
| **Name des Angriffs**: Metasploit | **Gefährdete Personengruppen**: Alle |
| 1. **Nutzer mit eingeschränkten Rechten** | |
| Die größte Schwachstelle ist der Mensch. Um zu verhindern das ein Metasploit Angriff erfolgen kann, ist eine der Besten Möglichkeiten die Zugriffsrechte des Nutzers einzuschränken. Den Nutzer kann man kontrollieren, den Angreifer nicht. | |
| 1.1 Windows Account mit eingeschränkten Rechten | |
| Ein Beispiel für einen Nutzer mit eingeschränkten Rechten ist ein Standardnutzer bei Windows. Dies bedeutet er hat keine Administrator Rechte und kann gewisse Änderungen, die ein Angriff gerne ausführen würde, nicht ausführen. Dies verhindert nicht den Angriff, sondern sorgt für eine Schadensbegrenzung bzw. verhindert den allgemeinen Zugriff oder den Zugriff auf sensible Daten. | |
|  | |
| *1. Klick auf das Windows Symbol* | |
|  | |
| *2. Klick auf Systemsteuerung* | |
|  | |
| *3. Unter Benutzerkonten und Jugendschutz: Benutzerkonten hinzufügen/entfernen* | |
|  | |
| *4. Untem im Fenster auf Neues Konto erstellen Klicken* | |
|  | |
| *5. Nutzer bennen und die Standardeinstellung Standardbenutzer ausgewählt lassen* | |
|  | |
| *6. Einstellungen Überprüfen und auf Konto erstellen klicken* | |
|  | |
| Docker Container | |
| Sollte die Möglichkeit der eingeschränkten Rechte bei Nutzer nicht gegeben sein, kann man die Zugriffsmöglichkeiten des Angreifers einschränken, indem man Anwendungen auf einem abgetrennten System laufen lässt. In diesem Fall Container. | |
| Docker Container einrichten | |
| Ein Container erlaubt das Arbeiten in einer abgekapselten Umgebung. Diese Umgebung kann Individuell gestaltet werden, eine vollständiges Windows, Teilbereiche oder auch nur bestimmte Anwendungen. In diesem Fall wird ein Windows auf dem Container laufen. | |
|  | |
| Erkennung | |
| Sofern ein Angriff erfolgt ist, sollte eine Erkennung und Beseitigung stattfinden. Diese Erkennung gestaltet sich für den Durchschnitts Nutzer meist schwierig. Ausnahme ist ein Radikales verhalten des Angreifers. | |
| Erkennung mithilfe von squil und Wireshark | |
|  | |
|  | |

|  |
| --- |
| *6. Das Programm recuva erkennt die Datei noch……* |
| Ein Encodieren der Zeichen ist auf keinen Fall möglich. |
| **Kommentare**:  Das Programm Abylon Shredder besitzt 5 verschiedene Sicherheitslevel:  0: normales Löschen – Verknüpfungen entfernen  1: 2x überschreiben mit binären Nullen  2: 3x überschreiben mit Nullen und Zufallszahlen  3: 7x überschreiben nach DoDII-Methode  4: 13x überschreiben DoDII und Zufallszahlen  5: 35x überschreiben (Peter Gutman Methode)  Diese Möglichkeit schützt nicht davor, wenn man vertrauliche Daten in Dateinamen schreibt. |