**Beantworte die nachfolgenden 18 Fragen direkt unterhalb der jeweiligen Frage.**

* Die Worddatei ist mit der Bezeichnung: **03-TINF-NameDesSchülers.docx**
* Unter dem **Betreff: Klasse, Zusatzarbeit**
* An die **E-Mail-Adresse:** [**Ber@htlwrn.ac.at**](mailto:Ber@htlwrn.ac.at)
* Bis **7..4.2021** zu senden

**Aufgabe:**

Bitte sehe dir das Video, von Sami Laiho, an <https://www.youtube.com/watch?v=R1eH7Nat_Ok>

**Fragen zum Video:**

1. **Aus welchem Land kommt Sami Laiho?**

* Sami Laiho kommt aus Finnland

1. **Warum muss der Kernel eines OS geschützt werden**

* Vom Kernel hat man vollen Zugriff auf die Hardware und Speicher

1. **Was ist der Unterschied zwischen Normal Mode und Secure Mode?**

* Man kann nur vom Secure Mode auf den Isolated User zugreifen

1. **Welche Voraussetzung muss gegeben sein, damit man überhaupt einen Secure Mode haben kann?**

* Hyper-V muss unterstützt werden

1. **Woran kann man erkennen, dass die LSASS-Hashes, auf die es Hacker abgesehen haben, sicher im Secure Mode „gespeichert“ werden?**

* Wenn LSAISO.exe aktiv ist

1. **Wie heißt der LSASS.EXE Prozess, der im Secure Kernel läuft?**

* LSAISO.exe

1. **Kann ein externer Developer, also ein Nicht-Microsoft Programmierer, über API auf den Secure Kernel zugreifen?**

* Nein

1. **Was versteht man unter dem Begriff (Marshalling). Wie kann man sich das in der Analogie vorstellen?**

* Marshalling ist, wenn strukturierte Daten in ein Format konvertiert werde, das auch andere Prozesse nutzen können

1. **Warum kann der „normale Kernel“, also ein Thread im Kernel, nicht auf den Secure Kernel zugreifen?**

* Der Marshaller verbietet das

1. **Wann erhält man ein Page Fault? Wer muss das Problem des „Page Faults“ lösen.**

* Wenn ein Programm auf einen Speicherbereich zugreifen will
* Das Betriebssystem

1. **Wann hat man SLAT? Wozu dient SLAT und was ist die Voraussetzung?**

* Mann hat SLAT bei Intel/AMD Prozessoren
* Zur kontrolle des Speichers
* Es muss von der CPU unterstützt werden

1. **Wozu dient die Access Mask beim Isolated Mode?**

* Die Acces Mask bestimmt welcher Kernel ein Bit ändern darf

1. **Gibt es virtuelle TPMs für Windows Server bzw. Windows 10?**

* Ja

1. **Was ist das Windows Gegenstück zum Linux Root-Account?**

* Das System

1. **Wie kann ich „Misses System“ werden?**

* Mit psexec -sid cmd.exe

1. **Wie lautet die Hierarchie von Software bis hinunter zu Stacks**

* Software-Prozess-Thread-Function-Stack

1. **Welche Partitionsteile weist ein Windows 10 Installation auf**

* Fat32, NTFS, MSR, WinRE Bitlocker

1. **Wie gelangt man in den Modus WinRE?**

* Windows-Suchleiste: „Change advanced statup options”
* Advanced Startup und auf Restart now drücken