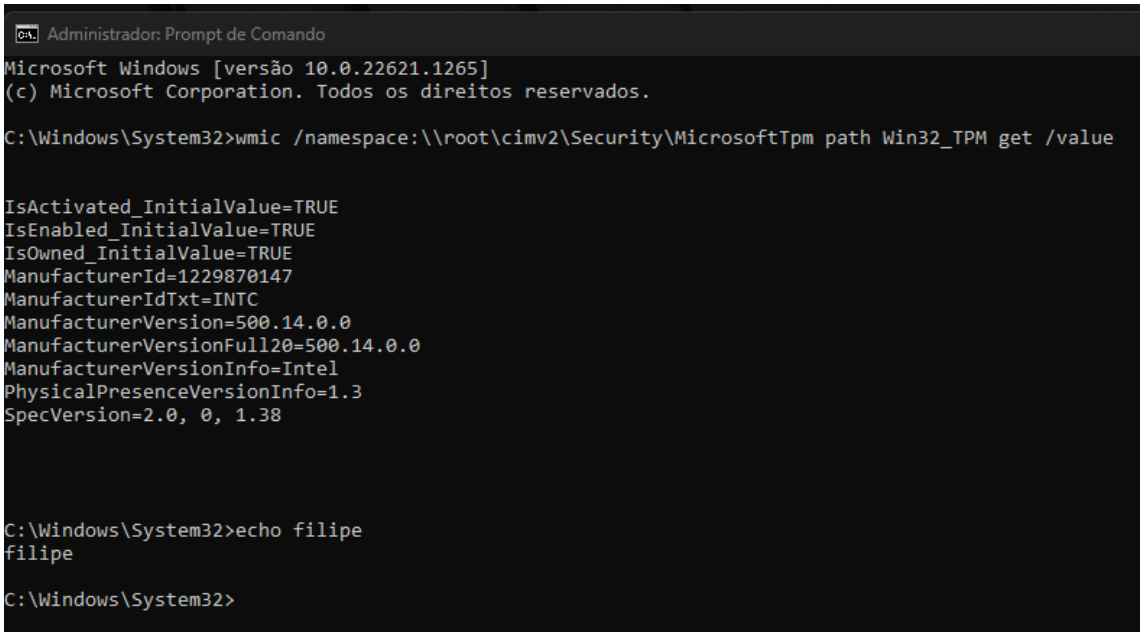
Filipe da Silva Sousa – RA: 163610

Verificando o TPM no Windows

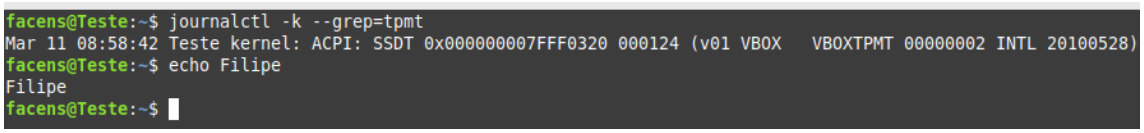
Abre-se o Prompt de Comando como administrador, e executa-se o seguinte código:



Demonstrando-se que o TPM utilizado é o 2.0

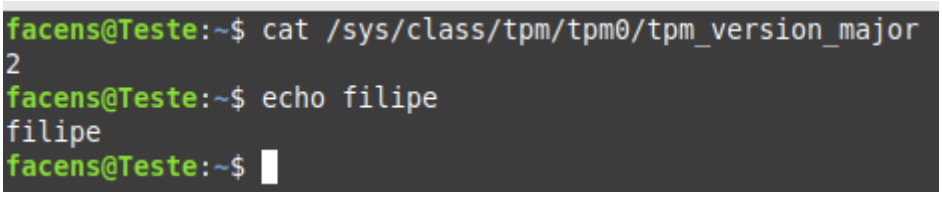
Verificando o TPM no Linux

Utilizou-se o seguinte comando no terminal do Linux:



A saída indica que foi detectada uma ACPI referente ao TPM, indicando que o SSDT começa no endereço 0x7FFF0320, possui 124 bytes, e possui assinatura VBOXTPMT.

O seguinte comando também pode ser utilizado para verificar a versão:



Comprovando-se novamente a versão 2 do TPM

Criando uma chave AES através do TPMS

É possível através do TPM realizar a criação de uma chave criptográfica utilizada para cifrar e decifrar dados através de um algoritmo AES, um algoritmo de cifragem simétrica.

O seguinte comando demonstra a criação da chave primária:

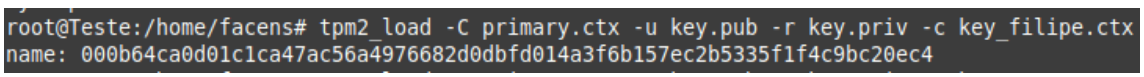
Nessa chave primária estão contidas informações sobre a chave primária, incluindo seu identificador único e seus atributos.

Utiliza-se então a chave primária para criar uma nova chave no TPM, através do seguinte comando:

Nesse comando, têm-se:

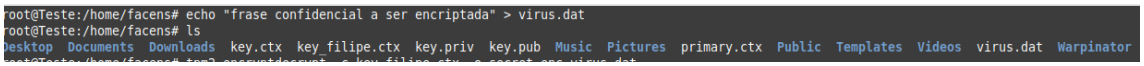
- Especificação do arquivo que contém a chave primária, através do “-C primary.ctx”
- Especificação do algoritmo AES-128 para criptografar a nova chave
- Especificação do nomes dos arquivos contendo as chaves públicas e privadas

Para carregar a chave criptográfica gerada no TPM e armazená-la em um novo arquivo, utilizou-se o seguinte comando:

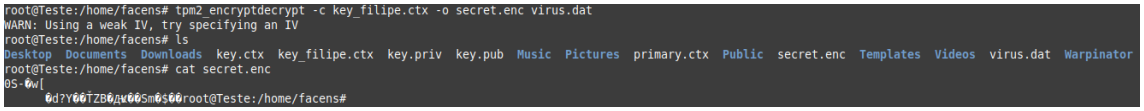


Encriptar e decryptar com TPM

Pode-se também utilizar o TPM para encriptar/decryptar mensagens, conforme demonstrado a seguir:



Criou-se um arquivo de dados denominado “virus.dat”, contendo a frase “frase confidencial a ser encriptada”. Utiliza-se então o tpm2_encryptdecrypt para criptografar este arquivo, e criar o arquivo “secret.dat”, conforme demonstrado a seguir:



Utilizando-se da chave gerada anteriormente, criou-se um arquivo contendo uma mensagem criptografada, que não pode ser visualizada caso não se tenha a respectiva chave.

Para demonstrar o funcionamento da chave, utilizou-se novamente o tpm2_encruptdecrypt para, com a chave especificada, revelar o conteúdo da mensagem deste arquivo criptografado: