|  |  |  |
| --- | --- | --- |
| Cyberbezpieczeństwo | | Kielce,07/12/2018 |
| Laboratorium 4 |  | |
| Wyk. Jakub Adamski | | Ocena: |

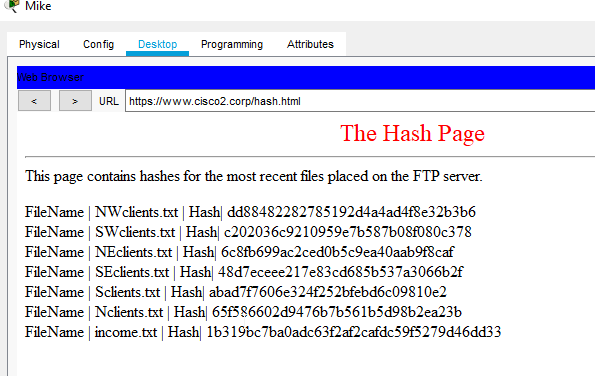
Part 1:

Step 1:

1. Jakiego protokołu użyto do uzyskania dostępu do tej strony na serwerze plików kopii zapasowych?  
     
   Użyto protokołu HTTP.

Part 2:

Step 1:

1. Jakiego protokołu użyto do uzyskania dostępu do tej strony na serwerze plików kopii zapasowych?  
     
   Użyto protokołu HTTPS – szyfrowana wersja protokołu HTTP.
2. Jakie są nazwy i hasze plików: 

Part 3:

Step 1:

1. Który plik został naruszony i hash się nie zgadza?

SEclients.txt

Kod sprawdzajacy poprawność haszy:

original\_hashes = {

"NWclients.txt": "dd88482282785192d4a4ad4f8e32b3b6",

"SWclients.txt": "c202036c9210959e7b587b08f080c378",

"NEclients.txt": "6c8fb699ac2ced0b5c9ea40aab9f8caf",

"SEclients.txt": "48d7eceee217e83cd685b537a3066b2f",

"Sclients.txt": "abad7f7606e324f252bfebd6c09810e2",

"Nclients.txt": "65f586602d9476b7b561b5d98b2ea23b"

}

obtained\_hashes = {

"NWclients.txt": "dd88482282785192d4a4ad4f8e32b3b6",

"SWclients.txt": "c202036c9210959e7b587b08f080c378",

"NEclients.txt": "6c8fb699ac2ced0b5c9ea40aab9f8caf",

"SEclients.txt": "99d4c9281993ff4fe4b8e92022224015",

"Sclients.txt": "abad7f7606e324f252bfebd6c09810e2",

"Nclients.txt": "65f586602d9476b7b561b5d98b2ea23b"

}

for fileName in original\_hashes.keys():

if(original\_hashes[fileName] != (obtained\_hashes[fileName])):

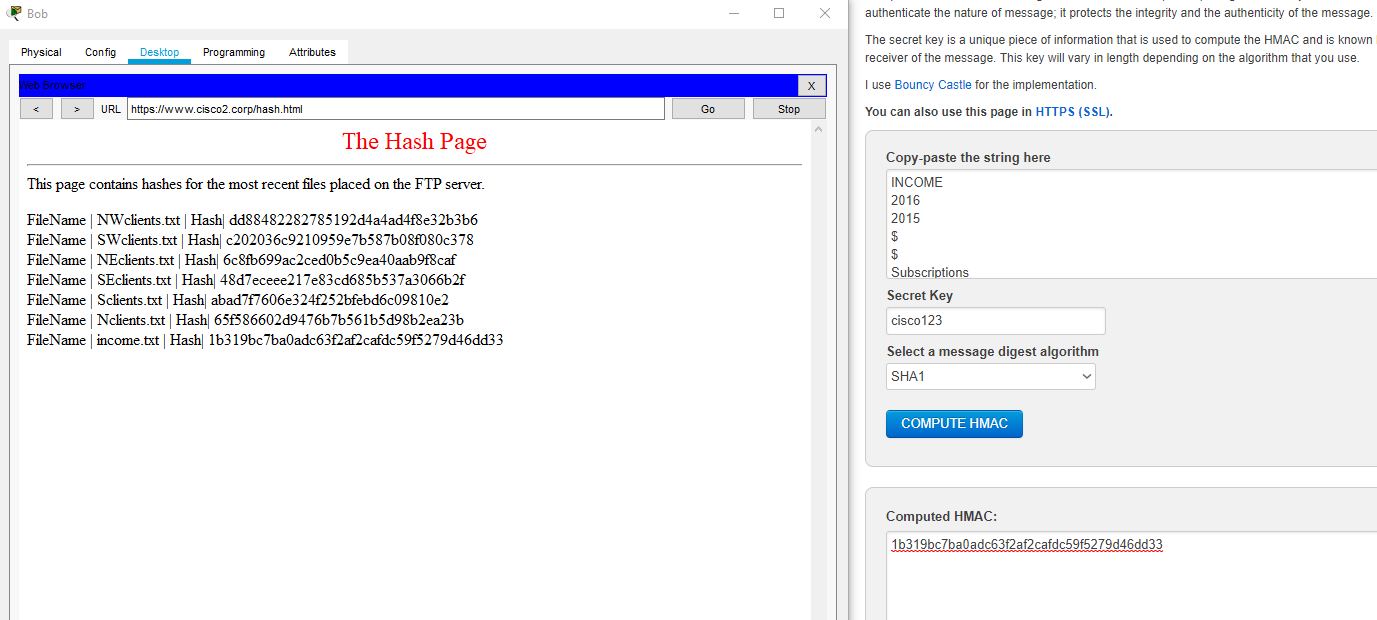
print(fileName + " has been tampered! Hashes are not equal!")

Part 4:

Step 1:

1. Jaki jest HMAC dla zawartości tego pliku ?   
     
   1b319bc7ba0adc63f2af2cafdc59f5279d46dd33
2. W jaki sposób używanie HMAC jest bezpieczniejsze niż ogólne hashowanie?  
     
   HMAC (keyed-Hash Message Authentication Code) – kod MAC z wmieszanym kluczem tajnym zapewniający zarówno ochronę integralności jak i autentyczności danych  
   Standardowy kod MAC zapewnia ochronę integralności, ale może podlegać sfałszowaniu jeśli nie jest zabezpieczony dodatkowym mechanizmem chroniącym jego autentyczność (np. podpisem cyfrowym).

Step 2:

1. Czy plik income.txt ma taki sam hash jak HMAC ?   
     
   Tak.