POLITECHNIKA ŚWIĘTOKRZYSKA		
Cyberbezpieczeństwo – Laboratorium 4		
Kierunek: Informatyka	Rok: 4	Semestr: VII
Student: Krzysztof Siwoń	Data wykonania: 24.11.2018	

Cel laboratorium

W tym ćwiczeniu zweryfikuje integralność wielu plików za pomocą skrótów(Hash'ow), aby upewnić się, że pliki nie zostały zmodyfikowane. Jeśli jakiekolwiek pliki są podejrzane o manipulację, muszą zostać przesłane do komputera Sally w celu dalszej analizy.

Część Pierwsza: Download the Client Files to Mike's PC

Krok 1:

What protocol was used to access this webpage on the backup file server?

Protokół zastosowany do uzyskania połączenia ze serwerem strony internetowej to **HTTP**

(Hypertext Transfer Protocol) czyli nieszyfrowany protokół, za pomocą którego przeglądarka przesyłą żadania do serwera.

Część Druga: Download the Client Files from the Backup File Server to Mike's PC

Krok 1:

What protocol was used to access this webpage on the backup file server?

HTTPS (*Hypertext Transfer Protocol Secure)*

szyfrowana wersja protokołu HTTP. W przeciwieństwie do komunikacji niezaszyfrowanego tekstu w HTTP klient-serwer, HTTPS szyfrował dane przy pomocy protokołu SSL, natomiast obecnie używany jest do tego celu protokół TLS. Zapobiega to przechwytywaniu i zmienianiu przesyłanych danych

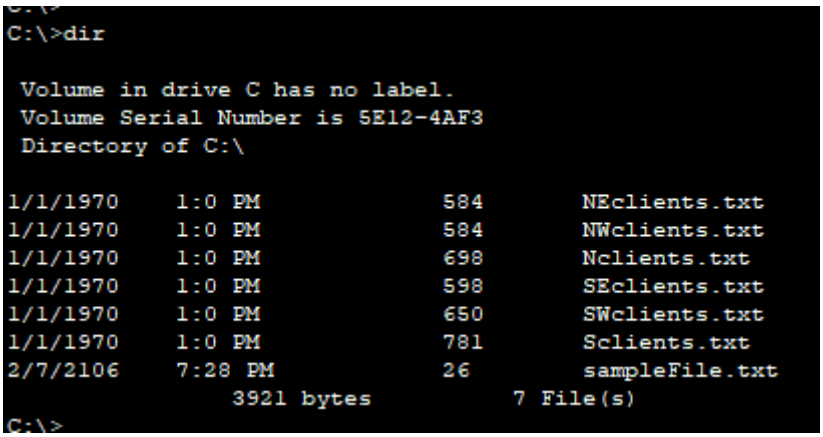
What are the file names and hashes of the client files on the backup server? (copy and paste them below)

The Hash Page

This page contains hashes for the most recent files placed on the FTP server.

FileName | NWclients.txt | Hash| dd88482282785192d4a4ad4f8e32b3b6
FileName | SWclients.txt | Hash| c202036c9210959e7b587b08f080c378
FileName | NEclients.txt | Hash| 6c8fb699ac2ced0b5c9ea40aab9f8caf
FileName | SEclients.txt | Hash| 48d7eceee217e83cd685b537a3066b2f
FileName | Sclients.txt | Hash| abad7f7606e324f252bfebd6c09810e2
FileName | Nclients.txt | Hash| 65f586602d9476b7b561b5d98b2ea23b
FileName | income.txt | Hash| 1b319bc7ba0adc63f2af2cafdc59f5279d46dd33

Krok 2:



Part 3: Verify the Integrity of the Client Files using Hashing

FileName | NEclients.txt | Hash| 6c8fb699ac2ced0b5c9ea40aab9f8caf

6c8fb699ac2ced0b5c9ea40aab9f8caf

```
>>> test("6c8fb699ac2ced0b5c9ea40aab9f8caf", "6c8fb699ac2ced0b5c9ea40aab9f8caf")
TRUE
```

FileName | NWclients.txt | Hash| dd88482282785192d4a4ad4f8e32b3b6

dd88482282785192d4a4ad4f8e32b3b6

```
>>> test("dd88482282785192d4a4ad4f8e32b3b6", "dd88482282785192d4a4ad4f8e32b3b6")
TRUE
```

FileName | SWclients.txt | Hash| c202036c9210959e7b587b08f080c378

c202036c9210959e7b587b08f080c378

```
>>> test("c202036c9210959e7b587b08f080c378", "c202036c9210959e7b587b08f080c378")
TRUE
```

FileName | Nclients.txt | Hash| 65f586602d9476b7b561b5d98b2ea23b

65f586602d9476b7b561b5d98b2ea23b

```
>>> test("65f586602d9476b7b561b5d98b2ea23b", "65f586602d9476b7b561b5d98b2ea23b")
TRUE
```

FileName | SEclients.txt | Hash| 48d7eceee217e83cd685b537a3066b2f

99d4c9281993ff4fe4b8e92022224015

```
>>> test("48d7eceee217e83cd685b537a3066b2f", "99d4c9281993ff4fe4b8e92022224015")
FALSE
```

Part 4: Verify the Integrity of Critical Files using HMAC

Krok 1:

What is the computed HMAC for the contents of the file?

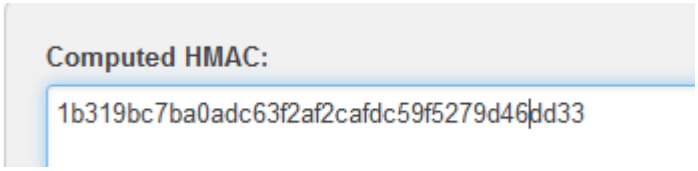
01843b302d076dd9e50fcfdef090a6cd88df9a0c

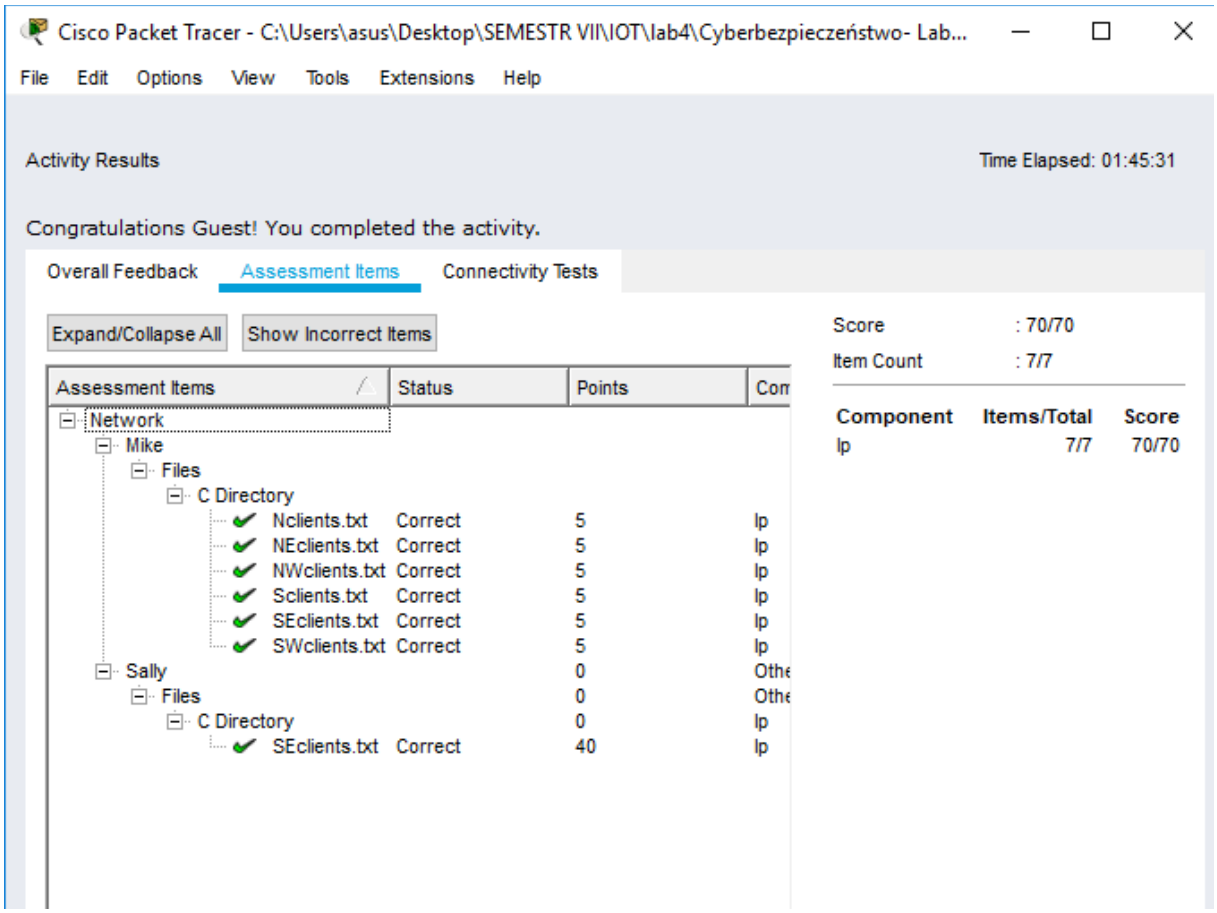
How is using HMAC more secure than general hashing?

kod MAC z wmieszanym kluczem tajnym zapewniający zarówno ochronę integralności jak i autentyczności danych

Krok 2:

Does the HMAC hash for the income.txt file match?




Cisco Packet Tracer - C:\Users\asus\Desktop\SEMESTR VII\IOT\lab4\Cyberbezpieczeństwo- Lab...
File Edit Options View Tools Extensions Help
Activity Results
Time Elapsed: 01:45:31
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Show Incorrect Items
Assessment Items
Status
Points
Network
Mike
Files
C Directory
Nclients.txt Correct 5 Ip
NEclients.txt Correct 5 Ip
NWclients.txt Correct 5 Ip
Sclients.txt Correct 5 Ip
SEclients.txt Correct 5 Ip
SWclients.txt Correct 5 Ip
Sally 0
Files 0
C Directory 0 Ip
SEclients.txt Correct 40 Ip
Score : 70/70
Item Count : 7/7
Component Items/Total Score
Ip 7/7 70/70