#### Funkcja skrótu SHA3 1

#### Łamanie skrótu MD5 metodą słownikową

#### Odszyfrowanie pliku szyfrem AES

#### Kod uwierzytelniający HMAC

#### Algorytm PBKDF2 z niestandardową liczbą iteracji

#### Identyfikacja algorytmu szyfrującego

#### Szyfrowany plik Zip

**Generowanie kluczy RSA**

<https://www.youtube.com/watch?v=18q1WOcyzWM>

#### Generowanie kluczy na krzywych eliptycznych

#### <https://www.youtube.com/watch?v=JpFwTpIubBo>

#### Szyfrowanie kluczem publicznym

#### <https://youtu.be/bR74jBpT2G0>

#### Certyfikat na podstawie zapytania

#### <https://youtu.be/CCimhx4Qe8o>

#### Generowanie klucza PGP

#### <https://youtu.be/77PLPCd250g>

#### Szyfrowanie za pomocą klucza PGP

#### <https://youtu.be/7pyJb6hy1eo>

#### Odszyfrowanie za pomocą klucza PGP

#### <https://youtu.be/0oxzn0b75KY>

#### Automatyczne wylogowywanie

#### Dostęp do plików należących do użytkownika root

#### Podwyższenie uprawnień użytkownika

#### Inna powłoka niż Bash

#### Usunięty plik

#### Analiza logów z konkretnego zakresu czasowego

#### <https://youtu.be/cz1N_5UT9PI>

#### cd /var/log

#### cat audit.log | grep -e "08:0[0-2]:[0-5][0-9]"

#### Analiza logów konkretnej usługi

#### <https://youtu.be/uHVRAqXXxAE>

#### cd /var/log

#### cat audit.log | grep -e "vsftpd\|ftp\|xinetd"

#### Analiza udanych prób logowania się na SSH

#### <https://youtu.be/EiLWkwlr-WI>

#### cd /var/log

#### cat audit.log | grep -e "sshd.\*invalid"

#### Analiza wielu nieudanych prób logowania się na SSH

#### <https://youtu.be/Wo9RXZpXjdQ>

#### cd /var/log

#### cat audit.log | grep -e “user\_”

#### Klasyczna podatność SQL Injection

#### Odczyt schematu bazy danych

#### Podatność SQL Injection typu Blind

#### Podatność SQL Injection typu Time Based

#### Podgląd nagłówków odpowiedzi

#### Manipulowanie parametrami HTTP

#### Automatyczny skan aplikacji

#### Modyfikacja żądań HTTP

#### Powtarzanie żądania HTTP

#### Wyszukiwanie właściwej wartości parametru metodą siłową