Bezpieczeństwo komputerowe

semestr letni 2023/24

Lista nr 2

(laboratorium)

Terminy oddania: przed 30.03.2024

Zadanie 1. Hashcat (10 pkt). Zorientuj się, jak można policzyć wartość funkcji hashującej od wybranego ciągu znaków. Zainstaluj `Hashcat` (https://hashcat.net/hashcat/) i zapoznaj się z podstawową dokumentacją (https://hashcat.net/wiki/doku.php?id=hashcat). Następnie:

1. Policz wartość funkcji hashującej od hasła składającego się z samych cyfr a następnie mając wiedzę, jaka funkcja została użyta i mając wartość hasha, spróbuj to hasło złamać przy użyciu `hashcata` w ataku typu `brute-force` przy założeniu, że hasło składa się tylko z cyfr. Jak długie tego typu hasła można w rozsądnym czasie złamać na twojej maszynie przy założeniu, że do hashowania używana była nieadekwatna do tego celu funkcja hashująca (np. md5, czy te z rodziny sha)? Z jakimi opcjami uruchamiałaś/eś `hashcata`?
2. Powtórz ćwiczenie powyżej zakładając, że hasło jest kombinacją małych liter i cyfr
3. Ściągnij wybrany słownik haseł powszechnie uznanych za słabe. Wybierz jedno z nich, lekko zmodyfikuj dodając znak specjalny i kilka cyfr na końcu. Oblicz wartość wybranej funkcji hashującej dla takiego hasła. Następnie przeprowadź atak `hybrydowy` z wykorzystaniem słownika i odpowiedniej maski. Z jakimi opcjami uruchamiałaś/eś `hashcata`?
4. Wymień się z koleżanką/kolegą wartością funkcji hashującej dla jakiegoś hasła. Nie zdradzajcie sobie hasła ani rodzaju funkcji hashującej, która została użyta. Spróbujcie hasło koleżanki/kolegi złamać. Jak zacząć, jeżeli nie wiadomo, jaka funkcja hashująca została wykorzystana? Czy można zawęzić zbiór poszukiwań?

Zadanie 2. Sniffer (5 pkt). Zainstaluj sniffer (np. `Wireshark`) i przechwyć za jago pomocą pakiety przychodzące/wychodzące z twojego komputera. Spróbuj zainicjować różne rodzaje komunikacji sieciowej, np. przeglądanie stron internetowych (po http/https) lub transfer plików za pomocą protokołu sftp. Przeanalizuj dane zebrane przez sniffer. Odpowiedz na pytania:

1. Jakie mamy możliwości filtrowania zebranych danych?
2. Jakie rodzaje danych są przesyłane w poszczególnych przypadkach?
3. Przy jakich wektorach ataku wireshark może być użyteczny?
4. Jakie informacje można uzyskać z ruchu sieciowego w przypadku korzystania z protokołu http a jakie przy stosowaniu https? Czy można na podstawie zebranych informacji dowiedzieć się, jakie strony internetowe/domeny były odwiedzane?