Bezpieki Lista 2

Zadanie 1

Podpunkt 1

Dla MD5: 12 cyfr 1.5 min a 13 cyfr już 18 min.

.\hashcat.exe -m 0 -a 3 6ca16f6e580108e30a22c909bb305462 ?d?d?d?d?d?d?d?d?d?d?d?d?d?d?d --increment

Podpunkt 2

Dla MD5: 10 znaków 1 min 39 s a 11 cyfr już 27 min.

.\hashcat.exe -m 0 -a 3 6ca16f6e580108e30a22c909bb305462 ?d?d?d?d?d?d?d?d?d?d?d?d?d?d?d --increment

```
Session..........: hashcat
Status...........: Running
Hash.Mode........: 0 (MD5)
Hash.Target......: 9d5dfc7ed5e5f7027f0612a36646fd5b
Time.Started.....: Mon Mar 25 22:36:42 2024 (1 min, 37 secs)
Time.Estimated...: Thu Aug 05 23:39:38 2027 (3 years, 132 days)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: ?h?h?h?h?h?h?h?h?h?h?h?h?h?h?h [15]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 10866.4 MH/s (5.98ms) @ Accel:128 Loops:128 Thr:128 Vec:1
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 1053361700864/1152921504606846976 (0.00%)
Rejected.........: 0/1053361700864 (0.00%)
Restore.Point....: 256802816/281474976710656 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:2688-2816 Iteration:0-128
Candidate.Engine.: Device Generator
Candidates.#1....: 17ae193edfeadad -> 6e3f5f686feadad
Hardware.Mon.#1..: Temp: 76c Fan: 74% Util: 97% Core:1845MHz Mem:6801MHz Bus:16
```

Podpunkt 3

wybrałem scotch i dodałem $420
.\hashcat.exe 5d57a21cb5c66806a93d90e822c0666c -m 0 -a 6 yahoo.txt ?s?d?d?d

```
5d57a21cb5c66806a93d90e822c0666c:scotch$420

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 5d57a21cb5c66806a93d90e822c0666c
Time.Started.....: Tue Mar 26 08:10:11 2024 (1 sec)
Time.Estimated...: Tue Mar 26 08:10:12 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (yahoo.txt), Left Side
Guess.Mod........: Mask (?s?d?d?d) [4], Right Side
Guess.Queue.Base.: 1/1 (100.00%)
Guess.Queue.Mod..: 1/1 (100.00%)
Speed.#1.........:  9454.7 MH/s (7.15ms) @ Accel:256 Loops:256 Thr:32 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2067791872/14965236000 (13.82%)
Rejected.........: 0/2067791872 (0.00%)
Restore.Point....: 0/453492 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:7168-7424 Iteration:0-256
Candidate.Engine.: Device Generator
Candidates.#1....: @fl!pm0de@-710 -> vtsydtht27}020
Hardware.Mon.#1..: Temp: 59c Fan:  0% Util: 25% Core:1935MHz Mem:6801MHz Bus:16
```

Podpunkt 4

Można zawęzić obszar poszukiwań:

- Długość Hasha
- Kontekst

.\hashcat.exe 9830d4a83df50bad82c20c3a71e1a9721cc8d067 --identify

```
      # | Name                                                       | Category
======+============================================================+==================================
    100 | SHA1                                                       | Raw Hash
   6000 | RIPEMD-160                                                 | Raw Hash
    170 | sha1(utf16le($pass))                                       | Raw Hash
   4700 | sha1(md5($pass))                                           | Raw Hash salted and/or iterated
  18500 | sha1(md5(md5($pass)))                                      | Raw Hash salted and/or iterated
   4500 | sha1(sha1($pass))                                          | Raw Hash salted and/or iterated
    300 | MySQL4.1/MySQL5                                            | Database Server
```

.\hashcat.exe 9830d4a83df50bad82c20c3a71e1a9721cc8d067 -m 100 -a 3

```
Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 100 (SHA1)
Hash.Target......: 9830d4a83df50bad82c20c3a71e1a9721cc8d067
Time.Started.....: Tue Mar 26 08:44:54 2024 (24 secs)
Time.Estimated...: Tue Mar 26 08:45:18 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: ?1?2?2?2?2?2?3 [8]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue......: 8/15 (53.33%)
Speed.#1.........:  5942.5 MH/s (11.41ms) @ Accel:128 Loops:128 Thr:128 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 140984188928/5533380698112 (2.55%)
Rejected.........: 0/140984188928 (0.00%)
Restore.Point....: 1671168/68864256 (2.43%)
Restore.Sub.#1...: Salt:0 Amplifier:11904-12032 Iteration:0-128
Candidate.Engine.: Device Generator
Candidates.#1....: snod2uqu -> cddnsfte
Hardware.Mon.#1..: Temp: 74c Fan: 75% Util: 98% Core:1890MHz Mem:6801MHz Bus:16
```

Zadanie 2

Podpunkt 1

- Filtrowanie po protokole: Możesz filtrować pakiety według konkretnych protokołów, na przykład HTTP, HTTPS, SFTP itp.
- Filtrowanie po adresie źródłowym/ docelowym: Pozwala to na analizę ruchu między określonymi adresami IP.
- Filtrowanie po portach: Możesz filtrować pakiety na podstawie używanych portów, co jest szczególnie przydatne w przypadku protokołów opartych na portach, takich jak FTP (port 21), SSH (port 22), HTTP (port 80) itp.
- Filtrowanie po treści danych: Wireshark umożliwia wyszukiwanie konkretnych ciągów bajtów lub tekstów w przesyłanych danych.

Podpunkt 2

- Przeglądanie stron internetowych HTTP/HTTPS: W tym przypadku przesyłane są żądania HTTP, które zawierają adresy URL odwiedzanych stron, nagłówki żądania, ciasteczka itp.
- Transfer plików za pomocą protokołu SFTP: Tutaj przesyłane są pliki binarne lub tekstowe w zależności od tego, co jest transferowane.

Podpunkt 3

- Ataki typu Man-in-the-Middle (MITM): Pozwala on na monitorowanie ruchu sieciowego, co może ujawnić próby przechwycenia danych.
- Ataki DDoS (Distributed Denial of Service): Analiza ruchu sieciowego może pomóc zidentyfikować niezwykłe wzorce ruchu lub ataki typu flood.
- Ataki typu sniffing: Wireshark może wykryć próby podsłuchiwania ruchu sieciowego.

Podpunkt 4

Przy użyciu protokołu HTTP, informacje, takie jak adresy URL, nagłówki żądania i odpowiedzi, mogą być czytelne. Jednak przy użyciu HTTPS, zawartość danych jest szyfrowana, więc większość danych będzie nieczytelna dla osoby, która podsłuchuje ruch sieciowy. Można jednak zidentyfikować odwiedzane domeny i adresy IP, ponieważ nagłówki TLS (Transport Layer Security) będą zawierały informacje o docelowej domenie.