https://tools.kali.org/wireless-attacks/mdk3



**Fakulteti i Inxhinierisë Elektrike dhe Kompjuterike**

**Universiteti i Prishtinës**

**mdk3**

Detyra 3 – Stress Testing, Siguria në Internet

**Agon Hoxha**

Mentorët:

Prof. Dr. Blerim Rexha

Msc. Arbnor Halili

**Përmbajtja**

[**Hyrje** 2](#_Toc534919047)

[**Përdorimi** 2](#_Toc534919048)

[**Eksperimentet** 3](#_Toc534919049)

[0. Parakusht: Vendosja në monitor mode 3](#_Toc534919050)

[1. Beacon flood mode 4](#_Toc534919051)

[2. Deautentitifikim – përjashtimi nga rrjetat 6](#_Toc534919052)

[3. DoS mode 7](#_Toc534919053)

[**Përfundimi** 8](#_Toc534919054)

[**Referencat** 9](#_Toc534919055)

**Figurat**

[Figura 1. Gjendja normale 3](file:///C:\Users\agoni\Desktop\ISP.docx#_Toc534919056)

[Figura 2. wlan0 në monitor mode 4](#_Toc534919057)

[Figura 3. Asnjë rezultat i shfaqur 4](file:///C:\Users\agoni\Desktop\ISP.docx#_Toc534919058)

[Figura 4. Efekti i komandës tek përdoruesit në rrethinë 5](file:///C:\Users\agoni\Desktop\ISP.docx#_Toc534919059)

[Figura 5. Ndryshimi i pranisë të access points përgjatë kohës dhe fuqia e tyre 6](file:///C:\Users\agoni\Desktop\ISP.docx#_Toc534919060)

[Figura 6. Wireless AP në channel 13 6](file:///C:\Users\agoni\Desktop\ISP.docx#_Toc534919061)

[Figura 7. Prap, asgjë në terminal 6](file:///C:\Users\agoni\Desktop\ISP.docx#_Toc534919062)

[Figura 8. Deautentifikimi në aksion 7](file:///C:\Users\agoni\Desktop\ISP.docx#_Toc534919063)

[Figura 9. Rezultati i komandës për DoS 7](file:///C:\Users\agoni\Desktop\ISP.docx#_Toc534919064)

[Figura 10. Faqja e routerit e bllokuar 8](file:///C:\Users\agoni\Desktop\ISP.docx#_Toc534919065)

# **Hyrje**

MDK është vegël për vërtetim të idesë se ekzistojnë dobësira tek një prej protokoleve më të përdorura në botë, IEEE 802.11x. MDK3 (v6) është versioni më i përhapur i MDK, dhe gjendet i integruar në Kali Linux prej lansimit të parë të sistemit operativ në fjalë.

MDK3 mund të vendoset në disa kategori, mirepo kryesisht bene pjese në Stress Testing dhe Wireless Attacks. Kjo vegël vendos paketa në rrjet, me qëllim që të e bllokoj totalisht. Paketat në fjalë janë paketa valide apo jovalide, varësisht prej asaj se si e përdorim veglën. Në disa raste, ngjan pra me një DOS sulm lokal.

Ndryshe nga wireless sulmet e zakonshme, që janë të fokusuara në një router të vetëm, MDK mund të sulmoj të gjithë routerët që janë në rrethinë, apo të fokusohet në një kanal të vetëm, apo ekziston edhe mundësia që të tentojmë një sulm në të gjitha pajisjet në rrethinë duke i mbingarkuar driverët e pajisjeve në rrethinë [1].

MDK3 është paksa vegël e vjetësuar për mbi 4 vjet nuk është bërë update [2]. Zhvillim në lidhje me këtë vegël ka vazhduar nga ana e zhvilluesëve të Aircrack-NG, por është rindërtuar dhe riemëruar në MDK4 – ndyshimet kryesisht janë që shton përkrahje për rrjetet wireless që përdorin frekuencat 5.0GHz, përkrahje për anashkalim të IDS, dhe përkrah përdorimin e dy kartelave të rrjetit, mirëpo është ende në zhvillim e tutje [3]. Deri sot, Offensive Security nuk e ka zëvendësuar ende në sistemin operativ të tyre, andaj do fokusohem në MDK3. Funksionaliteti i MDK4 është tejet i ngjajshëm, vetëm se është shtuar funksionaliteti dhe qka mund të bëj vegla [4].

# **Përdorimi**

Sikur disa vegla tjera që fokusohen në wireless, edhe MDK3 ka si kërkesë që kartela e rrjetit në rend të parë të e përkrah monitor mode, dhe të kemi qasjen e duhur për të e vendosur në atë mode. Kjo mund të jetë problem me disa kartela të rrjetit të vjetra, mirëpo shumica e kartelave të rrjetit wireless që gjinden në pajisjet e sotme përkrahin këtë mode.

Qysh menjëherë, nuk mund thjështë të e ekzekutojmë ndonjë komand me MDK3. Na duhet një parapregaditje – na duhet që kartelën e rrjetit të e vendosim në monitor mode, gje që vështirë mund të bëhet në sisteme operative si Windows apo nuk mund të bëhet fare në MacOS, mirëpo në Linux është qështje që lehtë bëhet. në Kali Linux, e kemi një vegël që e mundëson këtë shpejtë dhe e krijon një interface veqmas në listën e interface të atij kompjuteri. Kjo vegël quhet airmon-ng, dhe momenti i vetëm i përdorimit të saj do jetë para fillimit të shfrytëzimit të MDK3 për të e vendosur kartelën në monitor mode, dhe pasi që të përfundojmë shfrytëzimin dhe të kemi prap mundësin të qasemi në Internet. Pra, në fakt gjersa jemi në monitor mode, nuk kemi mundësi të qasemi në ndonjë rrjet me atë kartel.

Vlen të përmendet që vendosja e kartelës të rrjetit në monitor mode është e pamundshme gjersa Kali Linux është duke u përdorur si virtual machine, andaj edhe përdorimi i MDK3 do ishte i pamundshëm. Zgjidhje për këtë, është që të kemi Kali Linux në dual boot, apo të kemi një wireless kartel të jashtme (external) e cila do njihej nga Virtual Box apo VMWare, apo cilindo software virtualizues që e përdorim.

Përpos airmon-ng, kam parë si të arsyeshme të përdoret edhe aplikacioni WiFi Analyzer në sistemin operativ Android që të shohim efektin e disa prej aksioneve që do i ndërmarrim me anë të kësaj vegle. Vegël kjo që analizon aktivitetin e wireless access points në rrethinë ku gjendemi.

# **Eksperimentet**

Figura 1. Gjendja normale

## Parakusht: Vendosja në monitor mode

Për të filluar eksperimentet, vendosim më së pari kartelën tonë të rrjetit në monitor mode. Për të e bërë këtë në Kali Linux kemi disa opsione, më i thjeshti prej të cilëve është përmes airmon-ng:

airmon-ng start wlan0

Me anë të komandës iwconfig, mund të shohim tani se është shtuar një interface në list të interfaceve të kompjuterit tonë. Alternativisht, mund të anashkalojmë përdorimin e airmon-ng, dhe të përdorim vetëm ifconfig dhe iwconfig [5], edhe pse nuk është metod e preferuar:

ifconfig wlan0 down  
iwconfig wlan0 mode monitor  
ifconfig wlan0 up

Pasi që të gjithë këto komanda kanë efekt të drejtëpërdrejtë në hardware, ato janë komanda që duhen të ekzekutohen si root përdorues, qoftë përmes parashtesës sudo, apo duke pasur qasje si root.

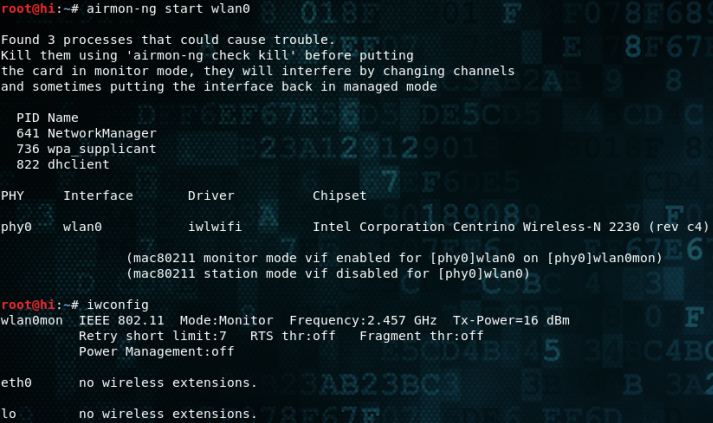


Figura 2. wlan0 në monitor mode

Struktura e komandave për MDK3 është: mdk3 <interface> <test\_mode> [test\_options]

Kemi 9 test mode, siq i quan vegla [6]:

1. b – Beacon flood mode, tenton të mbingarkoj pajisjet në rrethinë, siq do shfaqet më vonë.
2. a – Authentication DoS mode, tenton të shkaktoj probleme në AP përmes mbingarkimit.
3. p – Probe and Bruteforce mode, tenton të gjej access points të fshehur.
4. d – Deauthentication / Disassociation, tenton të përjashtoj pajisjet në rrethinë.
5. m – Michael mode, tenton të vazhdimisht ndalon trafikun.
6. x – 802.11x testime.
7. w – IDS/IPS Confusion mode, tenton të anashkaloj mbrojtjet e ndryshme që aplikojnë.
8. f – MAC filter bruteforce mode, tenton të autentifikoj MAC adresa të dhëna në një AP,
9. g – WPA downgrade test, ndalon enkriptimin në rrethinë dhe detyron përdorimin e algoritmeve të dobëta.

## Beacon flood mode

Në disa pajisje më të vjetra, që kanë chip të wireless më primitiv, do kishim mundur të e stresojmë mjaftueshëm sa që të ndalet tërësisht, apo të shkaktojmë dëme edhe më të mëdha në atë chip. Kjo më nuk vlen për chips më modern, që do të thotë nuk do mund të e shfaqim këtë stress test me një rezultat të kënaqshëm. Sidoqoftë, mund të shohim se qka ndodh gjatë beacon flooding.

Figura 3. Asnjë rezultat i shfaqur

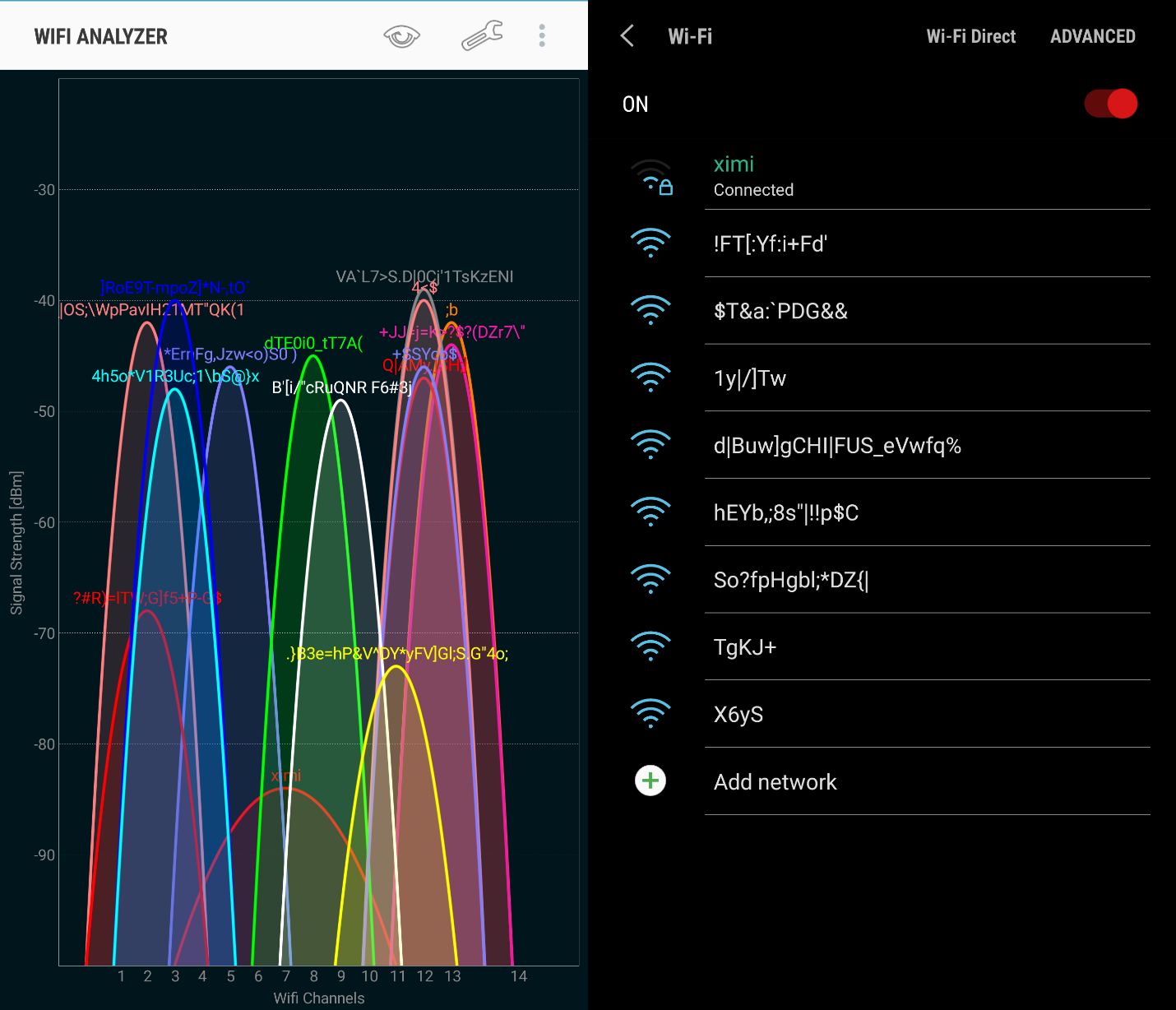
Komanda e MDK3 për të filluar këtë sulm është mjaft i thjështë, vetëm **mdk3 <interface> b**. Nga Figura 2, shohim se emri i interface tonë monitorues është wlan0mon, andaj komanda do jetë mdk3 wlan0mon b. në terminal (Figura 3), nuk do na shfaqet ndonjë rezultat, domethënë në këtë rast, pa pasur ndonjë pajisje tjetër, nuk do e shohim efektin e komandës. Përdorim veglën WiFi Analyzer dhe shohim se qka është duke ndodhur.

Figura 4. Efekti i komandës tek përdoruesit në rrethinë

Do gjenerohen dhjetera wireless access points qdo sekond. Vjen pyetja, si është kjo e demshme? për pajisjet moderne, nuk është ngase kane mbrojtje ndaj flooding të tille. Vrimat në siguri që i kishte 802.11x, kane arritur t’i rregullojne nga ana e software prodhuesit e ndryshem. Megjithate, verejme një gje që nuk shihet menjehere nga grafiku i WiFi Analyzer – 3 access points që ishin me fuqi jo dhe aq të madhe (Figura 1), me saktesisht Ladi, Toverlan1 dhe Tenda\_5A8C58, tani me nuk shfaqen fare. Mund të marrim analogji të thjesht me jeten reale se pse ndodh kjo: nese dikush është duke peshperitur informacione, dhe dikush tjeter duke leshuar muzik me ze të madh, nuk do i ndegjojme fare peshperimat.

Gjithashtu, vërejmë një gjë që nuk do pritej – disa prej access points që krijohen, janë në WiFi kanalin 13, që është i ndaluar në disa shtete për përdorim për shkak të interferencës që mund të shkaktoj në pajisje të ndryshme si televizione, mikrovala, etj [7]. Pra, përdorimi i këtij opsioni do mund të pësonte dënim në disa shtete, kryesisht SHBA. një channel i tillë i detajuar është paraqitur në Figura 5.

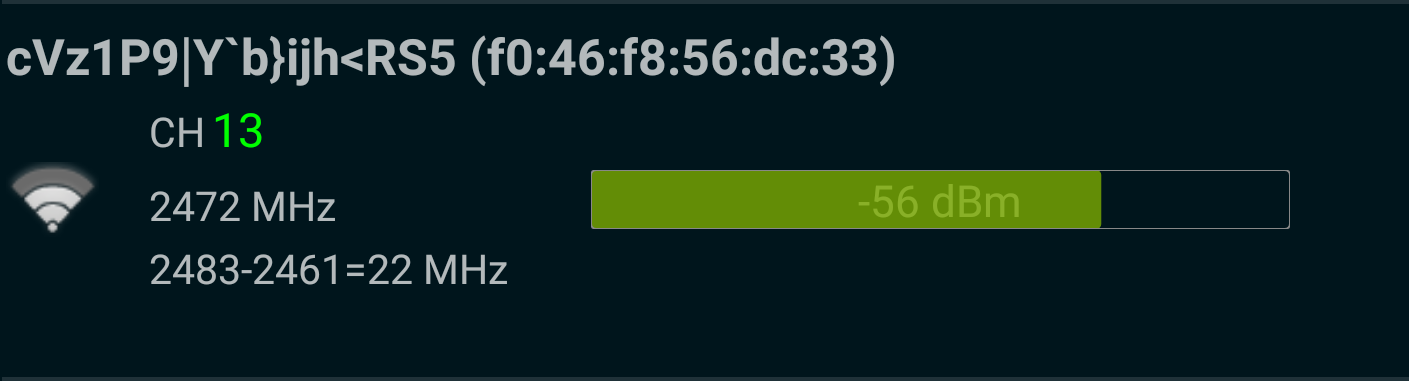
Këta channel krijohen brenda sekondi, dhe po aq shpejtë ndalin transmetimin. Më poshtë është paraqitur grafi që WiFi Analyzer jep për praninë e wireless access points përgjatë kohës. Gjithashtu, paraqitur është fuqia e sinjalit të një prej tyre dhe ndryshimi në fuqi brenda më pak se 1 sekondi.

Figura 5. Ndryshimi i pranisë të access points përgjatë kohës dhe fuqia e tyre

Figura 6. Wireless AP në channel 13

## Deautentitifikim – përjashtimi nga rrjetat

Nje ndër sulmet më të thjeshta dhe të zakonshme të wireless është deautentifikimi që po ashtu ngjan me një DoS sulm, një lloj stres testimi, dhe vlerëson se sa efektiv është routeri në raste të tilla. Sulmi i tillë është si rezultat i ekzistencës të deauthentication frames në IEEE 802.11x – vegla dërgon paketa në qdo access point, duke treguar se është qkyqur klienti, gjersa klienti nuk është qkyqur në fakt, dhe routeri e ndalon lidhjen. Kur të tentoj përdoruesi të bëjë ndonjë gjë në Internet, papritmas ndalet lidhja [8]. Komanda në këtë rast është **mdk3 <interface> d**, opcionalisht e kemi edhe opsionin -c që përcakton se në cilët kanale të fokusohet vegla. Nuk është e nevojshme të percaktohet, mirëpo shkakton më pak ngarkes në sistemin tonë.

Figura 7. Prap, asgjë në terminal

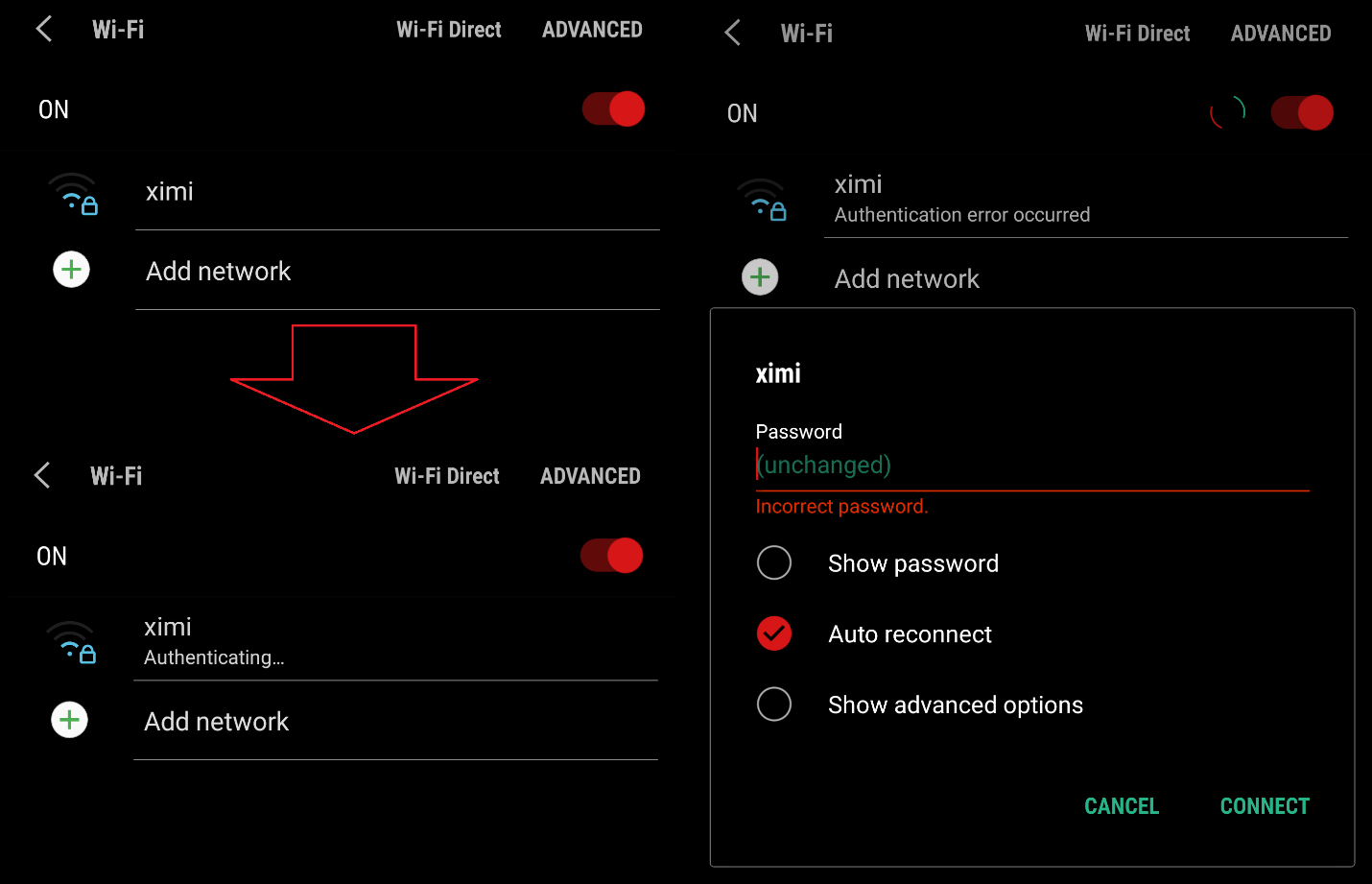
Ne këtë rast, kemi përdorur komandën mdk3 wlan0mon d -c 1,2,3,4,5,6,7,8,9,10 pasi që të gjithë access points në rrethinë janë në kanalin 1 deri 10. Ngjajshem si në rastin e mëhershëm, në terminal nuk na shfaqet asnjë e dhënë. Efektin e komandës mund të e shohim tek përdoruesi, në këtë rast pajisja jonë me sistem operativ Android.

Figura 8. Deautentifikimi në aksion

Klientit i ndalohet efektivisht qasja në cilëndo rrjet në rrethinë. Sistemi këtë dështim të qasjes e interpreton sikurse të ishte password gabim dhe kërkon perdoruesin të e rishkruaj ate. Po të dëshironim, do mund t’e përdornim një pajisje – si Raspberry Pi, dhe të e ekzekutonim automatikisht këtë komand qdo herë që vendoset në rrymë, dhe do kishin një bllokues të WiFi, që do ishte pothuajse e pamundshme të dihej se nga po vijnë sulmet e tilla. Duke stresuar kanalet e komunikimit, do mund të ndalonim qdo rrjet të WiFi në rrethinë në të cilën gjendemi. Ka router që mund të anashkalojne këtë sulm dhe rrjeti i mbijeton stres testit të tillë, mirëpo router të tille janë të rrallë dhe me kosto tejet të madhe. Gjithashtu ka IPS dhe IDS që janë në gjendje të mbrojnë rrjetën nga një gjësend i tillë. Pa marrë parasysh kësaj, shumica e rrjeteve në botë (përfshirë rrjetat korporative dhe universitare) janë të ndjeshme nga këtë sulm dhe nuk i mbijetojne këtij stres testimi.

## DoS mode

Figura 9. Rezultati i komandës për DoS

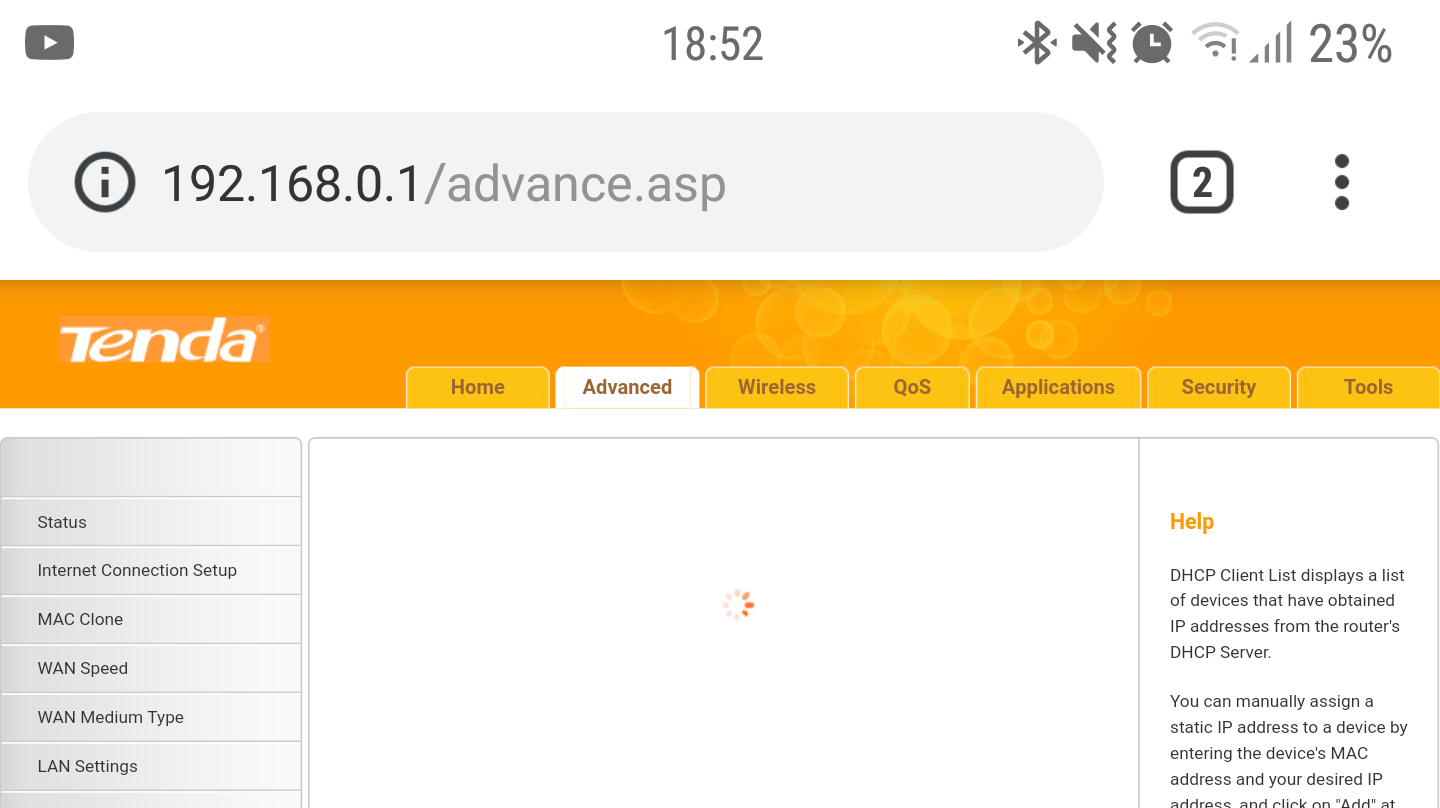
MDK3, siq cekur më heret, ka edhe një mode që mundëson një lloj DoS sulmi primitiv. Në këtë rast, sulmi bëhet duke dërguar qindra kërkesa për krijim të lidhjes me një access point. Komanda e përgjithshme është, **mdk3 <interface> a -a <AP\_MAC>**, në rastin tonë, MAC adresa e routerit që dëshirojmë të e sulmojme është C8:3A:35:16:13:28, dhe interface është wlan0mon. Mund t’e cekim edhe opsionin tjetër -m që i tregon veglës të tentoj të provoj dërgimin e paketave që duken sikur të ishin reale. Pra, komanda tani është mdk3 wlan0mon a -a C8:3A:35:16:13:28 -m. Ngjan me sulmin e deautentifikimit në funksion, mirëpo tani, klientët real të këtij access point nuk do përjashtohen, por ende do të jenë të qasur në te, vetem se nuk do këtë asnje trafik për pajisjen tonë. Do bllokon rrjetën, por zakonisht përdoruesit dhe potencialisht mbikqyrësi do mendojnë se problemi është tek routeri.

Figura 10. Faqja e routerit e bllokuar

Në status bar të pajisjes tonë, shohim se jemi të lidhur me WiFi, mirëpo nuk kemi qarkullim të të dhënave në Internet. Tentojmë të qasemi në faqen e routerit, mirëpo as ajo nuk ka sukses. Qka ndodh në prapavijë? Routeri është i zënë duke përgjigjur kërkesave që jemi duke ja dërguar përmes MDK3 – i duhet të jep përafersisht 500 përgjigjje negative qdo sekond. Routeri dështon, dhe nuk punon më. Efektivisht bllokohet. Sulmi DoS na doli i suksesshëm për këtë router. Pasi që të e ndalim sulmin dhe të restartohet routeri, rrjeta kthehet në punë normale.

Ngjashëm me rastin e mëparshëm, ka router që do jenë në gjendje të ‘mbijetojnë’ këtë, mirëpo shumica e routerëve në përdorim nuk do arrijnë të mirëmbajnë rrjetën gjate këtij sulmi.

# **Përfundimi**

Nga këto eksperimente, mund të përfundojmë se është vegel tejet e fuqishme dhe me rrezik të drejtëpërdrejtë në rrjetin tonë. Vetëm fakti se shumica e routerëve janë të ndjeshëm ndaj këtyre sulmeve, tregon se sa e vyeshme është kjo vegël. Megjithatë, gjersa është e vyeshme, do duhet të kemi parasysh që ka funksione që potencialisht janë ilegale dhe mund të na vendosin në konflikt me ligjin dhe autoritetet shtetërore, si shembulli i marrur rreth krijimit të access point në kanalin 13, që po ashtu do mund të bënte dëme fizike në pajisje tjera (që është edhe arsyeja pse konsiderohet ilegale).

# **Referencat**

[1] <https://en.kali.tools/?p=34>

[2] <https://github.com/aircrack-ng/mdk3/>

[3] <https://github.com/aircrack-ng/mdk4/>

[4] <https://en.kali.tools/?p=864>

[5] <https://miloserdov.org/?p=126>

[6] <https://tools.kali.org/wireless-attacks/mdk3>

[7] <http://en.data-alliance.net/legal-illegal-frequencies/>

[8] <https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack>