ROUTERGA DOS HUJUMI (SIMSIZ TARMOQ WI-FI)

Jumaboyev Javlonbek Sherqul o’g’li
Po’latov Doston Normurod o’g’li
Roziqov Abdug’ani Ilhomjon o’g’li
Hasanov Murodillo Azim o’g’li

Annotatsiya: *Bu annotatsiya, routerga (simsiz tarmoq Wi-Fi) DoS hujumlariga doir ma'lumotlarni taqdim etadi. DoS (Denial of Service) hujumlari, tarmoq qurilmalariga yo'l qo'yilgan xavfsizlik bo'shliqini topish uchun ishlatiladigan bir turiy xavfni ifodalaydi.*

Routerga qarshi DoS hujumlari, tarmoqda mavjud bo'lgan to'g'ri foydalanuvchilarga xizmat ko'rsatish imkoniyatini cheklash maqsadida amalga oshiriladi. Bu hujumlar, routerning qo'shimcha trafikni yo'qotish yoki bozish orqali amalga oshirilishi mumkin.

Simsiz tarmoq Wi-Fi DoS hujumlari, tarmoqdagi kabellangan uzatuvchilarning yo'qolishi, SIM kartaning aktivlashtirilmagan qolishi, tarmoqni hujumlar uchun avtomatik ravishda o'chirish uchun kamchiliklar bilan bog'liq bo'lishi mumkin. Bunday hujumlar orqali, foydalanuvchilar tarmoqdagi xizmatdan yoksun qolishi mumkin.

Bu annotatsiya routerga DoS hujumlari va ularning simsiz tarmoq Wi-Fi orqali amalga oshirilishini tushunish uchun umumiy ma'lumotlar beradi. Bu turlar xavfli hujumlar, tarmoq xavfsizligi va xavfsizlikni ta'minlash bo'yicha muammo sifatida ko'rsatiladi.

Kalit so’zlar:*Roter,Filtrlash,interfeys,protokol, monitor.*

Abstract: *This annotation provides information about router (wireless network Wi-Fi) DoS attacks. DoS (Denial of Service) attacks represent a type of threat used to exploit network devices to find a security loophole.*

DoS attacks against a router are carried out in order to limit the ability to serve the correct users on the network. These attacks can be done by causing the router to lose or jam additional traffic.

A wireless network may be subject to Wi-Fi DoS attacks, the loss of wired transmitters in the network, SIM card not being activated, flaws to automatically shut down the network for attacks. Through such attacks, users can be deprived of service on the network.

This annotation provides general information to the router to understand DoS attacks and their implementation over wireless network Wi-Fi. These types are shown as malicious attacks, network security and security issues.

Key words:*Router, Filtering, interface, protocol, monitor.*

KIRISH

Routerga DoS hujumi (Simsiz tarmoq Wi-Fi) uchun kirish qismi quyidagicha bo'lishi mumkin

1. Xavfsizlikni ta'minlash: Routerning boshqaruv paneliga kirish parolini o'zgartiring. Bundaylikda, faqat ruxsat etilgan shaxslar routerni sozlashlarni o'zgartirishi mumkin.

2. Tarmoqni monitoring qilish: Routerning monitoring tizimini faollashtirib, tarmoqdagi faoliyatni kuzatish uchun xavfsizlikni oshirishga yordam beradi. Hujumni aniqlab chiqarish uchun IP manbalarini, portlarni va tarmoqdagi trafikni kuzatib borishga imkon beradi.

3. Filtrlash va sinov qilish: Routerning sozlovlar va filtrlash imkoniyatlaridan foydalaning. IP manbalarini bloklash, ICMP paketlarni cheklash va hujumlarni qayta ishlatish uchun sinov qilish kabi sozlovlar qo'yish mumkin.

4. Yangilash: Routerni yangilash o'rnating. Routerni ishlab chiqaruvchining veb-sayti yoki dastur do'konidan yangi firmvarelar va dasturlar yuklab oling. Bu, xavfli kutilayotgan xato va tizim xavfsizlik bo'shliqlarini tuzatishga yordam berishi mumkin.

5. SSID nomini yashirish: Tarmoqni ziddiyat bilan kirishni davom ettirish uchun tarmoq nomini (SSID) yashiring. Bu, tarmoqni bilishlarni cheklash uchun kerakli bo'lgan identifikatsiyani berishga yordam beradi.

6. MAC manba filtri: Routerning filtrlash funktsiyalaridan foydalanib, MAC manba filtrlarini yoqishni o'rnating. Bu, tarmoqga kirish uchun faqatgina aniq MAC manbalarga ega qurilmalarni qabul qilishni ta'minlaydi.

7. Xavfsizlik sozlovlarini amalga oshirish: Routerning xavfsizlik sozlovlarini to'liq o'rnating. Qulayligini oshirish uchun WPA2 yoki WPA3 xavfsizlik protokolini qo'llashingiz tavsiya etiladi.

8. Hujumga qarshi dasturlar: Routerning hujumlarga qarshi himoyalash dasturlarini o'rnatish. Bu dasturlar, bilan hujumlar erkak qaytarish yoki xavfsizlik niqoblarini otish kabi hujumlarga qarshi himoyalashni ta'minlaydi.

Bu tavsiyalardan foydalanish orqali routerga DoS hujumlari

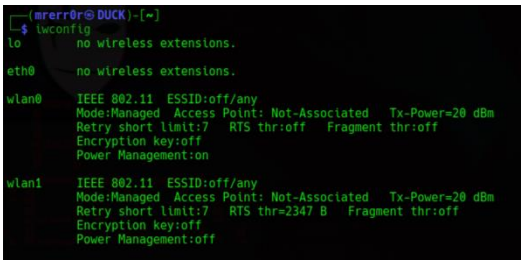
1-qadam: WiFi interfeys kartasini toping

Wi-Fi interfeys kartangiz nomini tekshiring (wlan0/1/2...). (Kali)Linux tizimida terminal oynasini oching va quyidagi buyruqni kiriting:

-sudo iwconfig

Monitor rejimiga qo'yish uchun birini tanlang. Mening holatimda, "wlan1"

- bu mening Wi-Fi kartam yoki monitor rejimida ishlaydigan interfeys nomi.



2-qadam: Jarayonlarni o'chirish

Ba'zi jarayonlar kartani monitor rejimiga qo'yishdan oldin o'ldirishi kerak, chunki bu muammoga olib kelishi mumkin. Quyidagi buyruqni kiriting:

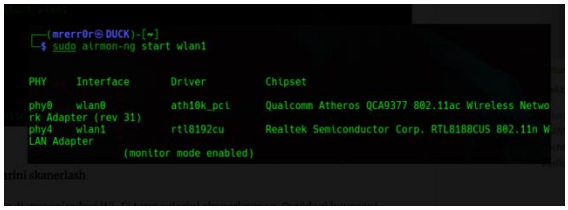
-sudo airmon-ng tekshirish o'ldirish

3-qadam: Monitor rejimini yoqing

Wi-Fi kartangizni Monitor rejimiga qo'ying. Quyidagi buyruqni kiriting:

-sudo airmon-ng start wlan1

//Mana "wlan1" mening Wi-Fi kartam, o'zingiznikini tanlang va uni o'zingizning Wi-Fi kartangiz bilan almashtiring (wlan0, wlan1, wlan2...).

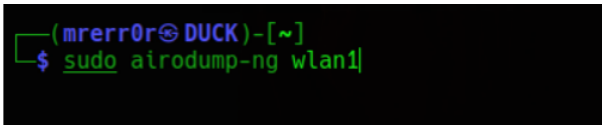


4-qadam: WiFi tarmoqlarini skanerlash

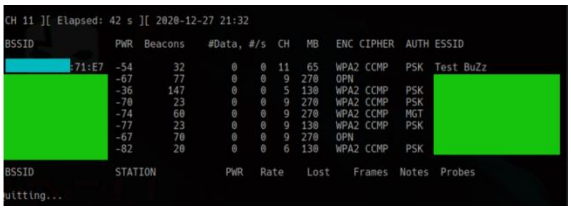
Ushbu bosqichda men o'z diapazonimdagi Wi-Fi tarmoqlarini skanerlayman. Quyidagi buyruqni kiriting:

-sudo airodump-ng [simsiz interfeysingiz nomi]

//Bu erda "wlan1" mening wifi kartamning nomi. Kartani monitor rejimiga qo'ygandan so'ng, "wlan1" "wlan1mon" ga aylantiriladi, lekin mening holatimda "wlan1" mening simsiz kartamning nomi, shuningdek monitor rejimi interfeysi. Boshqa hollarda, siz "wlan1mon" ga ega bo'lishingiz mumkin.



Bu yerda siz mening diapazonimdagi barcha Wi-Fi tarmoqlarini ko'rishingiz mumkin. Maqsadni topganingizdan so'ng, siz DoS-ni bajarmoqchisiz Wi-Fi tarmoqlarini skanerlashni to'xtatish uchun Ctrl+c tugmalarini bosing.



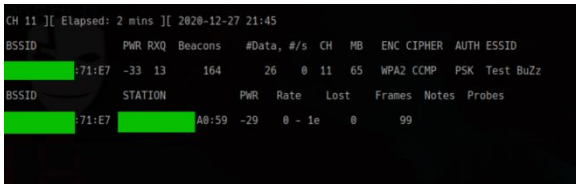
5-qadam: Nishonni qulflang

Har bir WiFi tarmog'ida kanal raqami va noyob bssid (routerning mac manzili) mavjud. Bosqichda men DoS hujumini amalga oshiradigan maqsadni qulflayman. Men "Test BuZz " ni maqsad qilib tanlayman, bu men sinov maqsadida sozlangan kirish nuqtasidir. Quyidagi buyruqni kiriting: -

sudo airodump-ng --bssid [BSSID] -c [kanal_raqami] [simsiz interfeys nomi]

// masalan: sudo airodump-ng --bssid (maqsadli bssid qiymati) -c 11 wlan1

Ko'rib turganingizdek, maqsad qulflangan.



Endi DoS hujumini amalga oshiramiz.

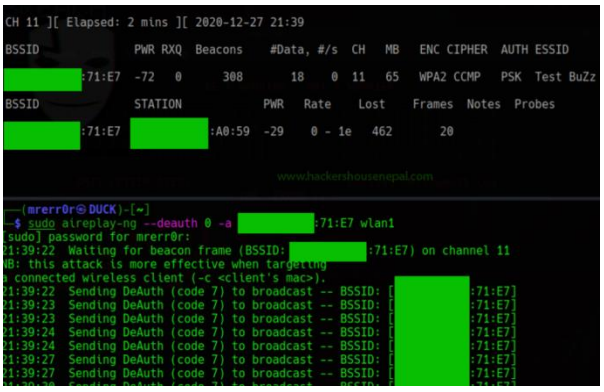
6-qadam: hujumni boshlash

Bu siz xohlagan maqsadga DoS hujumini amalga oshirishingiz mumkin bo'lgan oxirgi qadamdir. Boshqa terminal oynasini oching va quyidagi buyruqni kiriting: -

sudo aireplay-ng --deauth 0 -a [BSSID] [simsiz interfeys nomi]

//Bu erda nol (0) o'limni aniqlash hujumini ifodalaydi va -a Wi-Fi ning bssidsidir. masalan: sudo aireplay-ng --deauth 0 -a (bu yerda maqsadli bssid) wlan1

Ko'rib turganingizdek, biz maqsadli WiFi tarmog'iga DoS hujumini muvaffaqiyatli amalga oshirishimiz mumkin**.**



XULOSA

Routerga DoS hujumi (Simsiz tarmoq Wi-Fi) - bu hujum turi, router va tarmoqdagi foydalanuvchilarni yo'l ochishni to'xtatish maqsadida amalga oshiriladi. Hujum bilan router xizmatlari buzilishi yoki ulanishlarni cheklash mumkin.

DoS hujumlarida hujum qiluvchilar kengaytirilgan taktikalar, resurslarni to'xtatish uchun tarmoqni orqaga surish, taqsimlashlar va hujumlar yaratish uchun xavfli paketlar yuborish kabi taktikalar qo'llaydilar.

Hujumdan saqlanish uchun quyidagilarni amalga oshirish kerak:

1. Yangilashlar va patchlar: Routerni va uni firmvarelarini doimiy ravishda yangilang. Yangilashlar xavfni yo'qotish va potensial xavfli holatlarni tuzatishga yordam beradi.

2. Xavfsizlik sozlovlarini o'rnatish: Routerdagi xavfsizlik sozlovlarini to'liq o'rnating va kuchli parollarni foydalaning. Parollar unikal va qiyinchilik darajasini oshirgan bo'lishi kerak.

3. Trafikni monitoring qilish: Routerda trafik monitoringini yoqish va anomaliyalarni kuzatishga imkon beradigan vositalarni ishlatish. Bu, hujumning aniqlanishiga yordam beradi.

4. Filtrlash va cheklash: Filtrlash va sinov qilish funktsiyalaridan foydalanib, zararli IP manbalarini bloklash, ICMP paketlarini cheklash va hujumning qayta ishlatishini oldini olish mumkin.

5. Tarmoq nomini yashirish: Tarmoq nomini (SSID) yashirish va SSID broadcastingni o'chirish. Bu, tarmoqni yashirish va potensial hujumlarni qisqartirish uchun foydali bo'ladi.

6. Xavfsizlik dasturlarini o'rnatish: Hujumga qarshi himoyalash dasturlarini o'rnatish, hujumlarini aniqlash va ulanishlarni cheklash uchun muhimdir.

7. Xavfsizlikning yuqori darajada bo'lishi: Xavfsizlik sozlovlarini, autentifikatsiya protokollarni va shifrlashni yuqori darajada o'rnatish kerak.

Hujumdan saqlanish jarayonida router va tarmoqdagi xavfsizlikni oshirish va monitoringni kuchaytirish muhimdir.

FOYDALANILGAN ADABIYOTLAR:

1. "Hacking Exposed Wireless: Wireless Security Secrets & Solutions" - by Johnny Cache, Joshua Wright, and Vincent Liu: Bu kitobda, Wi-Fi tarmoqlarini hujumlar va salbiy istismorizatsiyadan himoya qilish yo'llari haqida asosiy ma'lumotlar beriladi. Bu hujum turlarining, uchunlarning qanday ishladiqlarini va ularni qanday zararlariga qarshi qanday himoya qilish mumkinligini tushuntiradi.

2. "Wi-Foo: The Secrets of Wireless Hacking" - by Andrew Vladimirov, Konstantin V. Gavrilenko, and Andrei A. Mikhailovsky: Bu kitob hujumlarga qarshi himoya yo'llarini tushunishda yordam beradi. Ushbu kitobda DoS hujumlari va ularning Wi-Fi tarmoqqa qanday ta'sir qilishining o'rnini o'rganishingiz mumkin.

3. "Network Security Assessment: Know Your Network" - by Chris McNab: Bu kitob hujumlarni hisobga olgan holda tarmoqlar uchun umumiy xavfsizlikni ta'minlash va ularga

qarshi himoya qilishning qanday amalga oshirilishi haqida asosiy qaydalar va maslahatlar beradi. Ushbu kitob sizga DoS hujumlariga qarshi qanday ko'nikmalarni ishlab chiqishni o'rgatadi.

4. "Wireless Hacking: Projects for Wi-Fi Enthusiasts" - by Lee Barken, Eric Bermel, and Chris Hurley: Bu kitob amaliyotiy ma'lumotlar va ushbu tarmoqqa qarshi hujumlarni tushunishga yordam beradigan amaliy dasturlarni taqdim etadi. Ushbu kitobda siz DoS hujumlarini kuzatish, aniq qilish va ularga qarshi qo'llanmalar yaratishda qanday o'tiladiganini o'rganasiz.