

**O‘ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI VA
KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI**

**MUHAMMAD AL-XORAZMIY NOMIDAGI
TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI**

«Axborot xavfsizligi» kafedrası

INDIVIDUAL LOYIHA

Mavzu: Tarmoq snifferlari yordamida paketlarni tahlillash

Bajardi: 711-20 guruh talabasi Abdullayev Rajab

Ilmiy rahbar: Mardiyev Ulug‘bek

Toshkent-2023

MUNDARIJA

| | |
|---|----|
| Kirish | 3 |
| I BOB. Tarmoqqa bo'ladigan sinifning hujumlari | 4 |
| 1.1. Tarmoqqa bo'ladigan hujum turlari | 4 |
| 1.2. Sniffing hujumni amalga oshirish usullari va uning oldini olish..... | 11 |
| 1.3. Packet sniffing hujumni amalga oshirish uchun dasturiy vositalar. | 20 |
| 1.4. Amaliy dasturiy vositalar bilan sniffing hujumni amalga oshirish..... | 24 |
| Xulosa..... | 30 |
| Foydalanilgan adabiyotlar | 31 |

Kirish

Axborot Texnologiya operatsiyalarida turli tarmoqlar orqali xavfsiz va ishonchli aloqani ta'minlash hal qiluvchi talab hisoblanadi. AT ma'murlari tarmoqdagi ma'lumotlar oqimi turli xil xavfsizlik va Xizmat sifati (QoS) standartlariga javob berishini ta'minlash uchun turli protokollar, tarmoqning eng yaxshi amaliyotlari va tarmoq monitoringi vositalariga tayanishi kerak. Ushbu keng tarqalgan amaliyotlardan biri Paketlarni hidlash texnikasi ko'pincha kiberhujumlar bilan bog'liq bo'lsa-da, u odatda internet-provayderlar, davlat idoralari, reklama beruvchilar va hatto tarmoq monitoringi uchun yirik tashkilotlar tomonidan qo'llaniladi. Ushbu maqolada biz paketlarni sniffingni batafsil ko'rib chiqamiz, shuningdek, IT amaliyotchilari tomonidan tez-tez ishlatiladigan vositalarni o'rganamiz.

Sniffers - bu tarmoq trafiginu ushlab turish va tahlil qilish qobiliyatiga ega dasturlar. Snifferlar ma'lumotlar oqimidan har qanday ma'lumotni (masalan, parollar) olish yoki tarmoq diagnostikasini amalga oshirish kerak bo'lganda foydalidir. Dastur kirish imkoniyati mavjud bo'lgan bitta qurilmaga o'rnatilishi va qisqa vaqt ichida barcha uzatilgan ma'lumotlarni qabul qilishi mumkin.

Snifferlar qanday ishlaydi Sniffer orqali trafikni quyidagi usullar bilan to'xtatishingiz mumkin: tarmoq interfeysida oddiy rejimda tinglash orqali, kanal bo'shlig'iga ulanish, trafikni qayta yo'naltirish, soxta elektromagnit emissiyalarni tahlil qilish orqali, havola va tarmoq qatlamiga hujum qilib, tarmoq marshrutlarining o'zgarishiga olib keladi.

Ushbu keng tarqalgan amaliyotlardan biri AT ma'murlariga paketlarni (kichik formatlangan ma'lumotlar birliklari) kuzatib borish va ularning muammosiz uzatilishini ta'minlashga yordam beradigan paketlarni sniffing deb nomlanadi. Ushbu maqolada biz paketlarni sniffingni batafsil ko'rib chiqamiz, shuningdek, IT amaliyotchilari tomonidan tez-tez ishlatiladigan vositalarni o'rganamiz.

I BOB. Tarmoqqa bo'ladigan sinifning hujumlari

1.1. Tarmoqqa bo'ladigan hujum turlari

Tarmoq xavfsizligi dunyo bo'ylab ko'p sonli tashkilotlar uchun muhimdir. Tarmoqqa bo'ladigan hujumlar kuchli tarmoq xavfsizligi bilan kamaytiriladi. Tarmoq sniferlari, tarmoq trafigini kuzatish va paketlarni taxlil qilishga yordam beradigan dasturlardir. Ular tarmoqqa bo'ladigan hujumlar, xavfsizlik yechimlari va tarmoqqa bo'ladigan hujumlar bilan bog'liq ma'lumotlarni yig'ish imkoniyatiga ega.

Zamonaviy tashkilotlar aloqa uchun internetga tayanadi va maxfiy ma'lumotlar ko'pincha tarmoqlar o'rtasida almashiladi. Tarmoq hujumlari turli shakllarda sodir bo'ladi. Korxonalar o'z aktivlarini tobora murakkablashib borayotgan kibertahdidlardan himoya qilish uchun eng yuqori kiberxavfsizlik standartlari, tarmoq xavfsizligi siyosatiga amal qilishi kerak.

Ko'p odamlar o'zlarining professional, ijtimoiy va shaxsiy faoliyati uchun Internetga tayanadilar. Ammo internetga ulangan kompyuterlarimizga zarar yetkazishga, shaxsiy daxlsizligimizni buzishga va internet xizmatlarini ishlamay qoldirishga urinayotganlar ham bor. Mavjud hujumlarning chastotasi va xilma-xilligi, shuningdek, yangi va yanada halokatli kelajakdagi hujumlar tahdidini hisobga olgan holda, tarmoq xavfsizligi kompyuter tarmoqlari sohasidagi markaziy mavzuga aylandi.

Zamonaviy korxona tarmog'i apparat, dasturiy ta'minot, xizmatlar, aloqa protokollari, virtual resurslar va odamlarning murakkab, yuqori darajada bog'langan ekotizimidir, ularning barchasi biznes operatsiyalarini qo'llab-quvvatlash uchun birgalikda ishlaydi. IT-tarmoqlari hozir hamma joyda tashkilotlarning tayanchiga aylangan, shuning uchun tarmoq xavfsizligini buzishga qaratilgan kiberhujumlar kompaniyalar va manfaatdor tomonlar uchun katta tahdiddir.

Afsuski, tarmoq xavfsizligi hujumlari (simply network attacks) tobora keng tarqalgan bo'lib, zararli korporativ tizimlarga zarar etkazish va nozik ma'lumotlarni buzish imkonini beradi.

Zararli dasturiy ta'minotni ishga tushirish (malware attacks), to'lov dasturlari hujumlari yoki so'nggi nuqta hujumlari kabi tajovuzkorlar kompyuter tarmog'ining perimetriga kirib borganidan keyin boshqa kiber jinoyatlar sodir bo'ladi. Malakali kiberjinoyatchilar tizimning barcha zaifliklaridan foydalangan holda hujum ko'lamini va ko'lamini tezda kengaytirishi mumkin.

Tarmoq hujumi operatsiyalarni buzishi va biznesning to'xtab qolishiga olib kelishi mumkin. Bu 2022-yil boshida AWS-ga qarshi DDoS hujumi (distributed denial-of-service) bilan sodir bo'ldi, bu dunyo ko'rgan eng diqqatga sazovor DDoS hujumlaridan biri edi.

2022 yilda Internetda mavjud bo'lgan DDoS dasturiy vositalar soni 12 foizga oshdi va ba'zi muhim DDoS hujumlarini amalga oshirilishiga olib keldi. Kelgusi yillar bundan ham yomonroq bo'ladi, ekspertlar 2023 yil oxiriga borib butun dunyo bo'ylab 15 milliondan ortiq DDoS hujumlari sodir bo'lishini taxmin qilmoqda.

Tashkilotlar uzoqdan ishlash biznes modellarini tobora ko'proq qabul qilar ekan, internetga asoslangan aloqa va bulutli hisoblashlar kiberxavflarni ta'minlashni yanada qiyinlashtirmoqda. Bu voqealar tashkilotlarning tarmoq xavfsizligi hujumlarini tanib olish va kibertahdidlarni bartaraf etish va hujumlarning oldini olish uchun mustahkam xavfsizlik yechimlarini amalga oshirishda yaxshiroq ishlashi zarurligini ta'kidlaydi.

Tarmoq hujumida kiberjinoyatchi korporativ tarmoqqa ruxsatsiz kirishga harakat qiladi. Maqsad odatda ma'lumotlarni buzish yoki o'g'irlash yoki boshqa zararli harakatlarni amalga oshirishdir. Ba'zi hollarda, tajovuzkor vaqt o'tishi bilan nozik ma'lumotlarni pullash uchun tizimlarga uzoq muddatli kirish huquqini saqlab qoladi. Maqsad korporativ josuslik va maxfiy ma'lumotlarni olish bo'lishi mumkin. Bunday murakkab, uzoq muddatli tahdidlar rivojlangan doimiy tahdidlar (APT) deb nomlanadi.

Tarmoq hujumlari quyidagilar bo'lishi mumkin:

Faol: Buzg'unchilar tarmoqqa ruxsatsiz kirish huquqiga ega bo'lishadi va keyin ma'lumotlarni (masalan, shifrlash orqali) o'zgartirib, uni buzish va foydalanish qulayligi va qiymatiga ta'sir qiladi.

Passiv: kiberjinoyatchilar ma'lumotlarni hech qanday o'zgartirish kiritmasdan kuzatish yoki o'g'irlash uchun tarmoqlarga hujum qilishadi.

Tarmoq hujumlarining eng keng tarqalgan turlari:

Botnet - Zararli dasturiy ta'minot bilan zararlangan va egalari bilmagan holda guruh sifatida boshqariladigan shaxsiy kompyuterlar tarmog'i, Bu jarayon masalan spam yuborish orqali amalga oshirilishi mumkin.

DoS (denial of Service) – DoS hujumi tarmoq, xost yoki boshqa infratuzilma qismlarini qonuniy foydalanuvchilar tomonidan yaroqsiz holga keltiradi.

Internet DoS hujumlarining o'zi ham uchta toifaga bo'linadi:

- **Zaiflik hujumi:** Bu maqsadli xostda ishlaydigan zaif dastur yoki operatsion tizimga bir nechta yaxshi tayyorlangan xabarlarni yuborishni o'z ichiga oladi. Agar paketlarning to'g'ri ketma-ketligi zaif dastur yoki operatsion tizimga yuborilsa, xizmat to'xtab qolishi yoki undan ham yomoni, xost ishdan chiqishi mumkin.

- **Tarmoqga juda jo'p miqdorda paketlar jo'natilishi:** tajovuzkor maqsadli xostga paketlar oqimini yuboradi - shunchalik ko'p paketlar, maqsadning kirish havolasi ishlamay qoladi va qonuniy paketlarning serverga etib borishiga to'sqinlik qiladi. Buzg'unchi maqsadli xostda ko'p sonli yarim ochiq yoki to'liq ochiq TCP ulanishlarini o'rnatadi.

DDoS (distributed denial of service) hujumlari keng tarqalgan botnet tarmoqlarini - internetga ulangan zararli dasturlar tomonidan buzilgan qurilmalarni joylashtirishni o'z ichiga oladi. Bu katta hajmdagi firibgar trafik bilan korporativ serverlarni zararlaydi.

O'rtadagi odam hujumlari **Man-in-the Middle (MITM)** tarmoq hujumlari zararli tomonlar tarmoqlar va tashqi ma'lumotlar manbalari o'rtasida yoki tarmoq ichida uzatiladigan trafikni to'xtatganda sodir bo'ladi. Aksariyat hollarda xakerlar zaif xavfsizlik protokollari orqali o'rtadagi odam hujumlariga erishadilar. Bular xakerlarga o'zlarini relay yoki proksi hisob qaydnomasi sifatida ko'rsatishga va real vaqt rejimida ma'lumotlarni boshqarishga imkon beradi.

Paket sniffer - har bir o'tayotgan paketning nusxasini yozib oladigan passiv qabul qiluvchiga paketli sniffer deyiladi. Passiv qabul qilgichni simsiz uzatuvchi yaqiniga qo'yish orqali ushbu qabul qiluvchi uzatiladigan har bir paketning nusxasini olishi mumkin! Ushbu paketlar parollar, ijtimoiy xavfsizlik raqamlari, tijorat sirlari va shaxsiy shaxsiy xabarlarini o'z ichiga olgan barcha turdagi maxfiy ma'lumotlarni o'z ichiga olishi mumkin. paketlarni hidlashga qarshi eng yaxshi himoya vositalaridan ba'zilari kriptografiyani o'z ichiga oladi.

IP-spoofing - Internetga noto'g'ri manba manzili bilan paketlarni kiritish qobiliyati IP-spoofing deb nomlanadi va bu bir foydalanuvchi boshqa foydalanuvchi sifatida niqoblanishi mumkin bo'lgan ko'plab usullardan biridir. Ushbu muammoni hal qilish uchun bizga oxirgi nuqta autentifikatsiyasi kerak bo'ladi, ya'ni xabar biz o'ylagan joydan kelib chiqqanligini aniq aniqlashga imkon beradigan mexanizm.

Ruxsatsiz kirish-zararli shaxslar ruxsat so'ramasdan korxona aktivlariga kirish huquqiga ega bo'lgan tarmoq hujumlari tushuniladi. Bunday holatlar hisob parolini zaif himoya qilish, shifrlanmagan tarmoqlar, rol imtiyozlarini suiiste'mol qiluvchi insayder tahdidlar va administrator huquqlari bilan faol bo'lmagan rollardan foydalanish tufayli yuzaga kelishi mumkin. Tashkilotlar imtiyozlarning kuchayishi va ruxsatsiz kirish xavfini oldini olish uchun eng kam imtiyozlar tamoyiliga ustuvor ahamiyat berishlari va saqlab qolishlari kerak.

SQL in'ektsiyasi - moderatsiya qilinmagan foydalanuvchi ma'lumotlarini kiritish tashkilot tarmoqlarini SQL in'eksion hujumlari xavfi ostida qoldirishi mumkin. Tarmoq hujumi usulida tashqi tomonlar kutilgan ma'lumotlar qiymatlari

o'rniga zararli kodlarni yuborish orqali shakllarni boshqaradi. Ular tarmoqni buzadi va foydalanuvchi parollari kabi nozik ma'lumotlarga kirishadi. Turli xil SQL in'ektsiya turlari mavjud, masalan, ma'lumotlar bazalarini ularning versiyasi va tuzilishi haqidagi ma'lumotlarni olish uchun tekshirish va amaliy qatlamdagi mantiqni buzish, uning mantiqiy ketma-ketligi va funksiyasini buzish. Tarmoq foydalanuvchilari parametrlangan so'rov bayonotlarni amalga oshirish orqali SQL in'eksion hujumlari xavfini kamaytirishi mumkin, bu esa ishonchsiz ma'lumotlar kiritishlarini tekshirishga yordam beradi.

DNS spoofing - DNS keshini zaharlash deb ham ataladi, bu kompyuter xavfsizligini buzishning bir turi bo'lib, unda buzilgan domen nomi tizimi ma'lumotlari DNS-resolverning keshiga kiritiladi va nom serveri noto'g'ri IP manzilni qaytarishiga olib keladi.

So'nggi tarmoq hujumlari, tarmoq hujumlari tashkilotlar uchun doimiy muammo bo'lib qolmoqda, chunki ular maxfiy tarmoq aloqalariga bo'lgan ishonchni kuchaytirgan holda masofaviy operatsiyalarga o'tishadi. So'nggi tarmoq hujumlari shuni ko'rsatadiki, yomon niyatli tomonlar eng kam kutilgan daqiqada hujum qilishi mumkin. Shunday qilib, kiber hushyorlik va xavfsizlik barcha sohalarda ustuvor bo'lishi kerak.

ISACA tashkilotining 2022 hisobotiga ko'ra, ijtimoiy muhandislik tarmoq hujumining eng mashhur usuli bo'lib, buzilgan tomonlarning 15 foizi ushbu texnika vositalari bilan amalga oshirilgan. Ijtimoiy muhandislik o'z shaxsiy ma'lumotlariga kirish uchun foydalanuvchilarning ishonchi va his-tuyg'ularidan foydalanadigan firibgarlik va firibgarlik usullarining murakkab usullarini o'z ichiga oladi.

Ba'zi tarmoq hujumlari tajribali xakerlar guruhining kengaytirilgan doimiy tahdidlarini (APT) o'z ichiga olishi mumkin. APT partiyalari murakkab kiberhujumlar dasturini tayyorlaydi va joylashtiradi. Bu xavfsizlik devorlari va antivirus dasturlari kabi tarmoq xavfsizligi choralari tomonidan aniqlanmasdan, bir nechta tarmoq zaifliklaridan foydalanadi.

Inransomware hujumlari, zararli tomonlar ma'lumotlarga kirish kanallarini shifrlaydi, shu bilan birga shifrnı hal qilish kalitlarini saqlaydi, bu model xakerlarga zarar ko'rgan tashkilotlarnı tovlamachilik qilish imkonini beradi. To'lov kanallari odatda kuzatilmaydigan kriptovalyuta hisoblarini o'z ichiga oladi. Kiberxavfsizlik idoralari zararli tomonlarnı to'lashdan to'sqinlik qilsa-da, ba'zi tashkilotlar ma'lumotlarga kirishni tiklashda tezkor yechim sifatida buni davom ettirmoqda.

Tarmoq hujumlaridan himoya qilish, rivojlanayotgan tarmoq hujumlari zamonaviy va faol tarmoq xavfsizligi yechimini talab qiladi.

NGFW (Keyingi avlod xavfsizlik devori) zamonaviy tashkilotlarga tarmoq ichidagi eng makkor tahdidlarnı aniqlash va ularga javob berish uchun zarur bo'lgan murakkab xususiyatlar to'plamini taqdim etadi. NGFW ning real vaqt rejimidagi monitoring interfeysi foydalanuvchilarga tarmoqdagi eng kichik anomaliyalarga kechiktirmasdan, davom etayotgan jarayonlarnı aniq taqsimlash bilan tezda javob berishga imkon beradi. NGFW an'anaviy xavfsizlik devorlarini chetlab o'tuvchi eng qo'rqinchli tarmoq hujumlarini aniqlashda muhim tarmoqlar va qurilmalarga ustuvor ahamiyat beradi. Bundan tashqari, Forcepoint-ning yangi avlod xavfsizlik devori yechimi SSL va TLS trafigidagi potentsial o'g'irlangan yoki buzilgan ma'lumotlarnı samarali aniqlaydigan shifrnı ochish funktsiyalarini ishlatganda foydalanuvchi maxfiyligini himoya qiladi. Qurilgan xavfsizlik devori yechimi bilan tarmoq hujumlaridan qoching.

Tashkilotlar tarmoq xavfsizligi hujumlaridan qanday himoya qilish mumkin?

Tarmoq hujumlari hamma joyda tashkilotlar uchun jiddiy, doimiy va o'sib borayotgan muammodir. Biroq, kiberxavfsizlik guruhları bir nechta eng yaxshi amaliyotlarnı qo'llash orqali bunday hujumlarning oldini olishları mumkin (yoki hech bo'lmaganda ularning ta'sirini yumshatadi).

Tarmoq tahlilidan foydalaning, kengaytirilgan tarmoq tahliliga ega integratsiyalashgan xavfsizlik yechimi tarmoq traffigini doimiy ravishda kuzatishi mumkin. An'anaviy xavfsizlik vositalaridan farqli o'laroq, bu yechimlar tarmoq

trafigini, xatti-harakatlarini va potentsial zararli faoliyatni o'z vaqtida, kontekstli ma'lumotlar bilan yaxshiroq ko'rishni ta'minlaydi. Ushbu tushunchalar xavfsizlik xodimlariga tahdidlarga aniqroq va mohirona javob berishga imkon beradi.

Tarmoq segmentatsiyasidan foydalanish (tarmoqni ajratish deb ham ataladi) tarmoqni alohida tarmoqlar kabi harakat qiladigan kichikroq segmentlarga ajratadi. Segmentatsiya segmentlar orasidagi o'zaro bog'liqlikni cheklaydi. Bu tarmoq ma'murlariga tarmoq trafignini nazorat qilish va nazorat qilish imkonini beradi va bitta segmentda ruxsatsiz foydalanuvchilar yoki zararli aktyorlarni o'z ichiga oladi.

Agar tajovuzkorlar tarmoqni buzishga muvaffaq bo'lishsa ham, segmentatsiya ushbu "buzilgan zonalar" tajovuzkorlarning lateral harakatini cheklash va tarmoqning boshqa segmentlarini keyingi zararlardan himoya qilish uchun ajratilganligini ta'minlaydi.

Tarmoq manzili tarjimasidan (NAT)dan foydalanish Internet orqali ma'lumot uzatishdan oldin bir nechta ichki (mahalliy) IP manzillarni umumiy manzillarga ko'rsatadi. IP-manzil bir nechta kompyuterlarni ifodalash imkonini berganligi sababli, NAT ushbu qurilmalarni bitta IP-manzil bilan Internetga ulaydi. Bu bitta qurilmaga mahalliy, xususiy tarmoq va Internetning umumiy tarmog'i o'rtasida vositachi sifatida harakat qilish imkonini beradi. Har qanday kiruvchi yoki chiquvchi trafik ushbu "NAT qurilmasi" orqali o'tishi kerak. Bundan tashqari, IP-manzillar kamroq, shuning uchun tajovuzkorlar qaysi xostga ulanayotganini yoki hujum qilish kerakligini tushunish qiyinroq.

1.2.Sniffing hujumni amalga oshirish usullari va uning oldini olish.

Bugungi kunda biz kompyuterlar va boshqa qurilmalar doimiy ravishda tarmoq orqali ma'lumotlarni paketlar shaklida uzatadigan raqamli muhitda yashayapmiz. Ushbu paketlar tarmoq orqali bir kompyuterdan ikkinchisiga yuboriladigan ma'lumotlar segmentlari bo'lib, deyarli hamma narsada ishtirok etadi. Internetni ko'rib chiqishdan tashkilotingizning butun ma'lumotlar bazasini boshqarishgacha, paketlar doimiy ravishda tarmoq orqali uzatiladi. Xavfli yoki zararli maqsadlarga ko'ra (masalan, tarmoq ma'murlari va kiber jinoyatchilar tomonidan) Ushbu paketlar belgilangan joyga etib borgunga qadar qo'lga olinishi, o'zgartirilishi va yo'q qilinishi mumkin. Shunday qilib, bugungi kiberxavfsizlik dunyosida mustahkam o'ringa ega bo'lish uchun paketlarni sniffing kabi fundamental terminologiyalarni qattiq bilish juda muhimdir. Ushbu maqolada paketlarni hidlash nima, u qanday amalga oshiriladi, paketlarni hidlashning har xil turlari va eng yaxshi amaliyotlar bilan birga paketlarni hidlashning oldini olish usullari tushuntiriladi.

Packet Sniffing hujumi yoki oddiygina sniffing hujumi - bu paketlar ko'rinishida tarmoq orqali o'tadigan tarkibni (masalan, maxfiy ma'lumotlarni o'qish) ushlab qolish va noto'g'ri ishlatishni o'z ichiga olgan kiber-hujum. Shifrlanmagan elektron pochta xabarlar, login parollari va moliyaviy ma'lumotlar paketlarni sniffing hujumi uchun umumiy maqsadlardir. Bundan tashqari, tajovuzkor paketning o'ziga zararli kodni kiritish orqali paketlarni o'g'irlash uchun sniffing vositalaridan ham foydalanishi mumkin, bu maqsadli qurilmaga etib borganidan keyin amalga oshiriladi.

Paketlarni sniffing hujumining yaxshi namunasi DNS keshini zararlashdir, DNS bu kompyuterni tushunish uchun domenlarni IP ga tarjima qiladigan protokol va keraksiz qidiruvni oldini olish uchun brauzer bunday serverlarning IP manzilini keshda, DNS keshida zararlanishdan saqlaydi. Tajovuzkor Burpsuite yoki boshqa ushlash vositalari orqali so'rovni hidlaydi va uni zararli DNS serverlari va kesh

ma'lumotlarini o'zgartiradi, bu esa DNS cache poisoning turdagi hujumlarni amalga oshirishi mumkin.

Packet Sniffing hujumlarining turlari- odatda hujumni amalga oshirish uchun ishlatiladigan vositalarga qarab, sniffing hujumlarining ikki turi mavjud.

1. Hardware Packet Sniffers

Uskuna paketli sniffer tarmoqqa ulanish va uni tahlil qilish uchun mo'ljallangan. Uskuna paketi sniffer to'g'ridan-to'g'ri jismoniy tarmoqqa to'g'ridan-to'g'ri kiritish orqali filtrlash, marshrutlash yoki boshqa maqsadli yoki beixtiyor sabablarga ko'ra paketlarning yo'qolishini ta'minlaydi. Uskuna paketli sniffer tutib olingan paketlarni saqlaydi yoki kollektorga uzatadi, bu esa apparat paketi sniffer tomonidan to'plangan ma'lumotlarni keyingi tahlil qilish uchun qayd qiladi.

2. Dasturiy ta'minot paketi Snifferlari

Hozirgi vaqtda paketli snifferlarning aksariyati dasturiy ta'minotga asoslangan. Tarmoqqa ulangan har bir tarmoq interfeysi u orqali o'tadigan barcha tarmoq trafigini qabul qilishi mumkin bo'lsa-da, ko'pchilik buni qilmasligi uchun tuzilgan, chunki u zararli kodni yuborish uchun ishlatilishi mumkin. Dasturiy ta'minot paketi sniffer bu sozlamani o'zgartirib, tarmoq interfeysi stekdagi barcha tarmoq trafigini qabul qilishiga olib keladi. Aksariyat tarmoq adapterlari uchun bu tartibsizlik rejimi sifatida tanilgan. Paketli snifferning funksiyasi maqsad manzillaridan qat'iy nazar interfeys orqali oqib o'tadigan har qanday dasturiy paketlarni ajratish, qayta yig'ish va yozib olishdan iborat. Jismoniy tarmoq interfeysi orqali o'tadigan barcha trafik dasturiy ta'minot paketi snifferlari tomonidan yig'iladi.

Paketlarni snifferlash qanday ishlaydi?

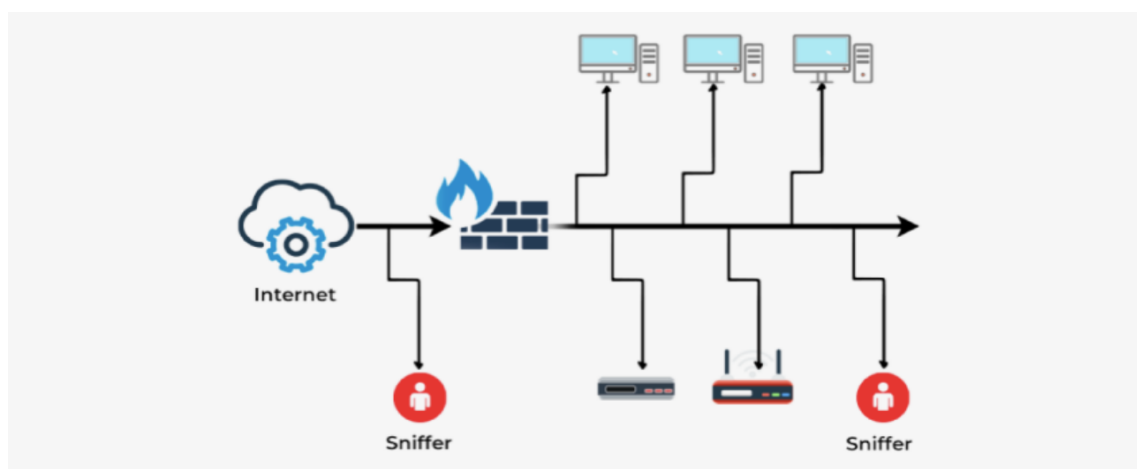
Kiberxavfsizlikda paketlarni snifferlash aslida fundamental darajada qanday amalga oshirilishini qisqacha ko'rib chiqamiz. Tarmoq interfeysi kartasi (NIC) har qanday kompyuterda tarmoqqa ulanish imkonini beruvchi apparat komponentidir. Manzillanmagan trafik NIClar tomonidan sukut bo'yicha e'tiborga olinmaydi.

Sniffing hujumlari NIC-larda promiscuous rejimidan foydalanishni talab qiladi, bu NIC-larga barcha tarmoq trafigini qabul qilish imkonini beruvchi rejimdir. Ma'lumotlar paketlarini sniffing qilish va ma'lumotlar paketlaridagi kodlangan ma'lumotlarni dekodlash orqali snifferlar NIC orqali o'tadigan barcha aloqalarni tinglashlari mumkin. Zaif yoki shifrlanmagan ma'lumotlar paketlari sniffing hujumlarini xakerlar uchun ancha qulaydir.

Sniffing faol yoki passiv ikki usulda amalga oshirilishi mumkin.

1. **Faol sniffing** - hujumlari kalitlar deb nomlanuvchi apparat foydalanish orqali amalga oshiriladi. Hatto kerak bo'lmaganda ham barcha portlarga ma'lumotlarni yuboradigan hublardan farqli o'laroq, kalitlar ma'lumotlarni tarmoqdagi kompyuterlarning belgilangan MAC manzillariga yuboradi. Faol hidlash hujumlari ko'pincha Content Address Memory (CAM) jadvalini to'ldirish uchun tarmoqqa manzilni aniqlash protokollarini (ARP) kiritish orqali boshlanadi. Boshqa portlarga yo'naltirilgan trafik tajovuzkorga trafikni kalitdan hidlash imkonini beradi.

2. **Passiv sniffing** - ushbu turdagi hidlash odatda hubda amalga oshiriladi. Faol sniffingdan farqli o'laroq, hubga ma'lumotlar paketlarini yig'ish uchun darhol sniffer qurilmasi kiritilishi mumkin. Biroq, bugungi kunda hublar kamdan-kam qo'llaniladi, shuning uchun passiv hidlash hujumlari ham kamdan-kam qayd etiladi.



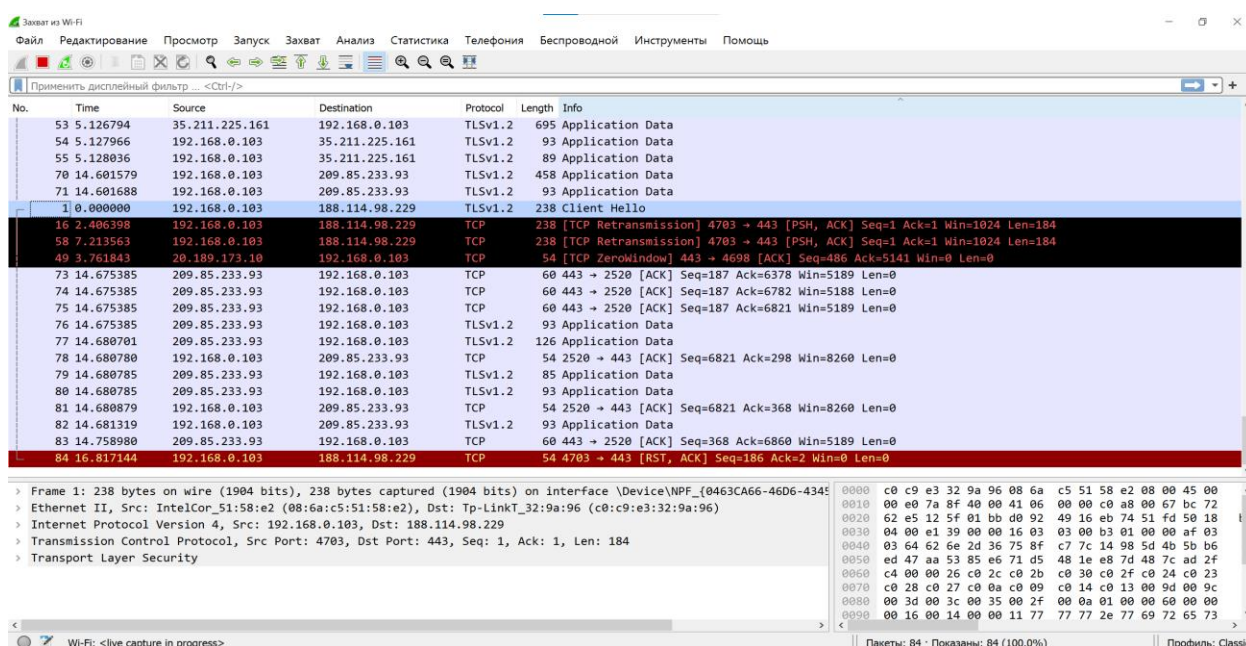
1-rasm. Packet sniffing hujumi amalga oshirilishi.

Packet Sniffingdan foydalanishning qonuniy va noqonuniy tomonlari

Biz Packet Sniffingdan ba'zi zararli maqsadlarda foydalanishni ko'rib chiqdik, ammo boshqa qonuniy foydalanish ham mavjud.

1. Qonuniy foydalanish

Tarmoqlar juda murakkab bo'lib, tarmoqqa ulangan mashinalar bo'ylab turli xil paketlar kiradi. Bu murakkablik ishlarning noto'g'ri ketishini osonlashtiradi. Paketlarni sniffing vositalari tarmoq menejerlariga o'z tarmoqlarida nima sodir bo'layotganini real vaqt rejimida ko'rish imkonini beradi. Ushbu texnologiyalar ularga tarmoq trafiginı kuzatishda, hamma narsa yaxshi ishlayotganligini aniqlashda, to'siqlarni aniqlashda va muammolarni bartaraf etish yoki tizimlar zararli hujum ostida ekanligini aniqlash uchun zarur bo'lgan ma'lumotlarni taqdim etishda yordam beradi. Wireshark qonuniy sabablarga ko'ra ishlatiladigan eng ko'p ishlatiladigan sniffingdan vositalaridan biridir.



2-rasm. Wireshark dasturiy vositasi orqali paketlarning ushlanishi.

2. Noqonuniy foydalanish

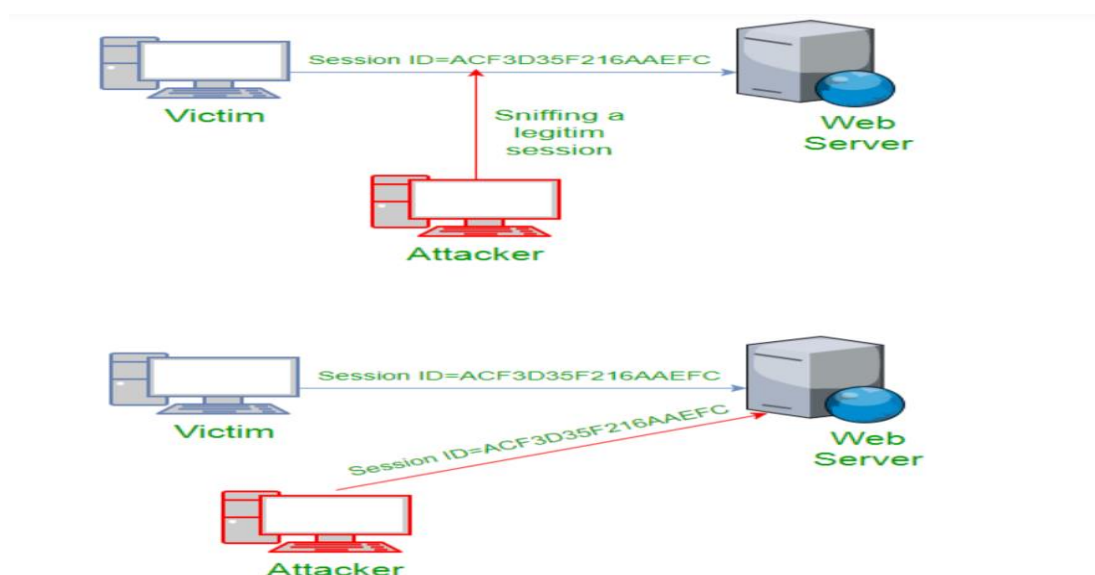
Administratorlar o'z tarmoqlari haqida yaxshiroq bilim olish, muammolarni tashxislash va tahdidlarni aniqlash uchun paketlarni sniffing usullaridan qanday foydalanishi haqida ma'lumot berildi. Ammo zararli tajovuzkor tashkilotning

tarmoq trafigini o'z paketini hidlasa nima bo'ladi? Tarmoq bo'ylab harakatlanadigan ko'plab paketlar paket snifferlari tomonidan ushlanishi va jurnalga kiritilishi mumkin. Bu zaiflikning yana bir nuqtasini ochadi, ayniqsa nozik ma'lumotlar tarmoq bo'ylab shifrlanmagan tarzda o'tsa. Buzg'unchi tarmoqqa kirishi va u orqali oqib o'tadigan barcha paketlarni qo'lga kiritishi mumkin. Bu ularga kompaniya yoki uning tarmoq foydalanuvchilarining maxfiy ma'lumotlariga kirishni ta'minlashi mumkin.

Packet Sniffing hujumining turlari

1. TCP sessiyasini o'g'irlash

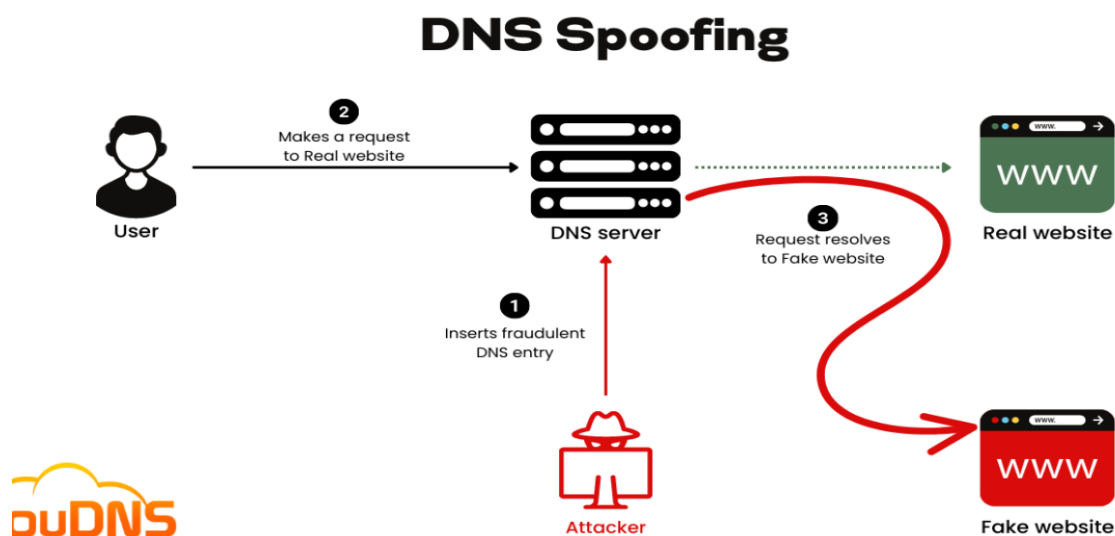
Seansni o'g'irlash, shuningdek, Transmission Control Protocol (TCP) sessiyasini o'g'irlash, veb-foydalanuvchining seans identifikatorini o'g'irlash va vakolatli foydalanuvchi sifatida namoyon bo'lishni o'z ichiga oladi. Buzg'unchi foydalanuvchining seans identifikatorini qo'lga kiritgandan so'ng, ular osongina o'zini o'sha foydalanuvchi sifatida yashirish va foydalanuvchi bajarishi mumkin bo'lgan tarmoq bilan bog'liq har qanday vazifalarni bajarish uchun foydalanishi mumkin.



3-rasm.TCP session hijacking hujumining amalga oshirilish strukturasi.

2. DNS poisoning

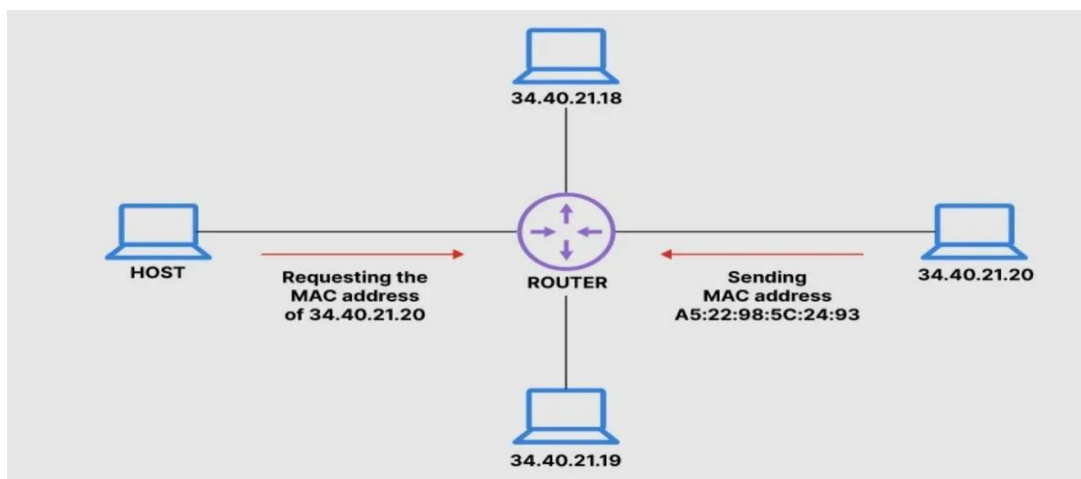
DNS cache poisoning yoki DNS spoofing deb ham ataladigan DNS zararlanishi xakerlar internet trafiginı fishing veb-saytlariga yo'naltiradigan yana bir firibgarlik kiberhujumidir. DNS bilan zararlanish ham jismoniy, ham korxonalar uchun xavf tug'diradi. DNS zararlanishi bilan bog'liq eng jiddiy muammolardan biri shundaki, qurilma bir marta infeksiyalangan bo'lsa, muammoni hal qilish qiyin bo'lishi mumkin.



4-rasm.DNS poisoning hujumining amalga oshirilish strukturasi.

3. Manzilni aniqlash protokoli (ARP) Sniffing

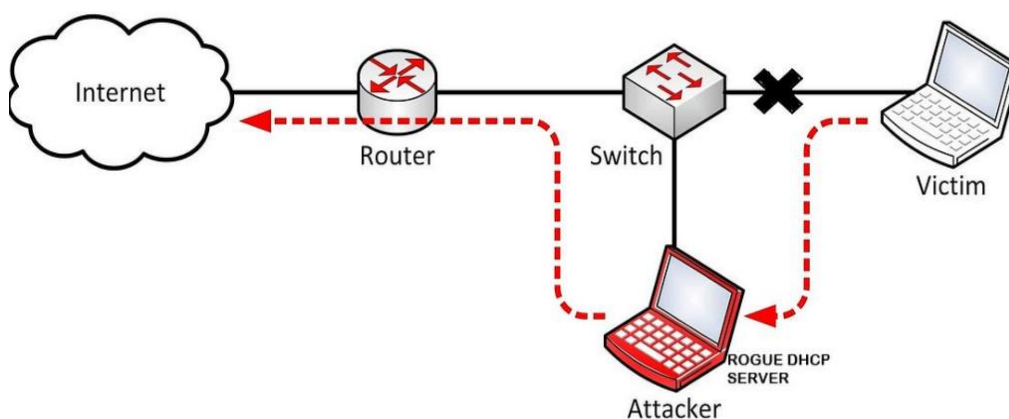
Xakerlar ko'pincha soxta ARP xabarlarini mahalliy tarmoq orqali uzatadilar, bu ARP zararlanishi yoki ARP aldashi deb nomlanadi. Ushbu hujumlar trafikni mo'ljallangan manzildan uzoqroqqa va tajovuzkor tomon yo'naltirish uchun mo'ljallangan. Buzg'unchining MAC manzili maqsadning IP-manziliga ulangan bo'ladi va u faqat ARP-ni yoqadigan tarmoqlarda ishlaydi.



5-rasm.ARP Sniffing hujumining amalga oshirilish strukturasi.

4. DHCP hujumi

DHCP hujumi - bu tajovuzkorlar tomonidan maxfiy ma'lumotlarni yig'ish va o'zgartirish uchun ishlatiladigan faol paketlarni tekshirish misolining bir turi. DHCP - bu kompyuterga IP-manzilni tayinlaydigan mijoz/server protokoli. IP-manzil bilan bir qatorda, DHCP server standart shlyuz va pastki tarmoq niqobi kabi konfiguratsiya ma'lumotlarini beradi. DHCP mijoz qurilmasi ishga tushganda, u paketli sniffing hujumi orqali ushlanishi va o'zgartirilishi mumkin bo'lgan translyatsiya trafiginini yuboradi.



6-rasm. DHCP hujumining hujumchi tomonidan amalga oshirilish strukturasi.

Paketlarni sniffing hujumining oldini olish.

Packet Sniffing hujumlari har qachongidan ham keng tarqalgan va bu asosan qonuniy foydalanish uchun mo'ljallangan, keyinchalik hujumchilar tomonidan o'zgartirilgan turli xil paketli snifferlarning keng mavjudligi bilan bog'liq. Biroq, sizni bunday hujumlar qurboni bo'lishdan to'xtatib qo'yadigan yoki himoya qiladigan ba'zi ehtiyot choralarini ko'rishingiz mumkin.

1. Noma'lum tarmoqlardan foydalanishni oldini olish

Himoyalangan tarmoqda xavfsizlik devori va antivirus himoyasi mavjud emasligi sababli, tarmoq orqali uzatiladigan ma'lumotlar shifrlanmagan va oson kirish mumkin. Iste'molchilar o'z qurilmalarini xavfsiz bo'lmagan Wi-Fi tarmoqlariga duchor qilganlarida, tarmoqni o'chirish hujumlari osongina amalga oshirilishi mumkin. Buzg'unchilar tarmoq orqali yuborilgan har qanday ma'lumotlarni to'sib qo'yadigan va o'qiydigan paketli snifferlarni o'rnatish uchun xavfsiz bo'lmagan tarmoqlardan foydalanadilar. Buzg'unchi soxta "bepul" umumiy Wi-Fi tarmog'ini yaratish orqali tarmoq trafiginini ham kuzatishi mumkin.

2. Xabarlarni shifrlash uchun VPN dan foydalanishni boshlang

Ma'lumotlarni shifrlash xavfsizlikni oshiradi, bu esa tajovuzkorlarga uni ishlatishdan oldin shifrini ochishga majbur qiladi, bu oson ish emas. Barcha kiruvchi va chiquvchi aloqa virtual xususiy tarmoq yoki VPN orqali almashishdan oldin shifrlangan. Har qanday tajovuzkor kiruvchi veb-saytlarni yoki uzatilgan va qabul qilingan ma'lumotlarni ko'ra olmaydi.

3. Doimiy ravishda tarmoqlarni kuzatib boring va skanerlang

Tashkilotning tarmoq ma'murlari tarmoq muhitini yaxshilash va sniffing hujumlarini aniqlash uchun tarmoqli kengligi monitoringi yoki tarmoq xaritalash vositalaridan foydalangan holda o'z tarmoqlarini skanerlashi va kuzatishi kerak.

4. Snifferni aniqlash dasturidan foydalaning

Qurilmangizdagi hidlash vositalarini aniqlash uchun yaratilgan ba'zi mashhur ilovalar qatoriga Anti Sniff, Neped, ARP Watch va Snort kiradi.

5. Internetdan foydalanishda xavfsiz HTTPS saytlardan foydalanish

Shifrlangan veb-saytlarning URL manzili "HTTPS" (hipermatnni uzatish protokoli xavfsiz) bilan boshlanadi, bu esa ushbu veb-saytlarda foydalanuvchilarning o'zaro aloqasi xavfsiz ekanligini va ma'lumotlar serverga uzatilishidan oldin shifrlanganligini kafolatlaydi. "HTTP" bilan boshlanadigan veb-saytlar bir xil darajadagi xavfsizlikni ta'minlay olmaydi, shuning uchun paketlarni hidlashdan qochish uchun "HTTPS" bilan boshlanadigan veb-saytlarga tashrif buyurish tavsiya etiladi.

6. Hujumlarni aniqlash tizimini joriy qilish

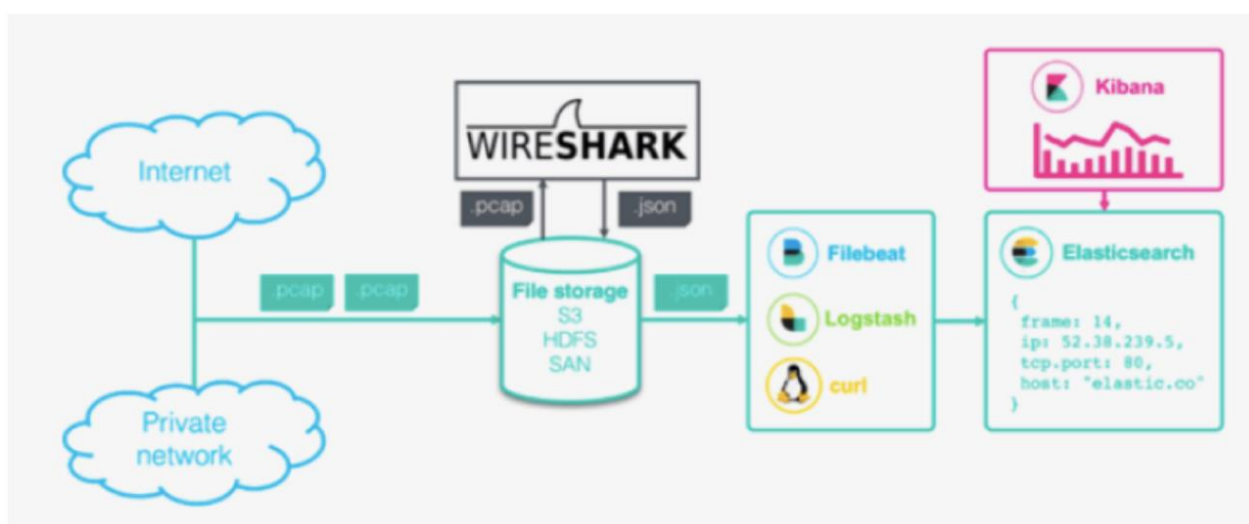
Hujumlarni aniqlash tizimi (IDS) har qanday noodatiy faoliyat uchun tarmoq trafigini kuzatuvchi va bo'lajak buzg'unchilarni ogohlantiruvchi dasturiy ta'minotdir. U tarmoq yoki tizimni zararli faoliyat yoki siyosat buzilishi uchun skanerlashi mumkin va har qanday potentsial xavfli xatti-harakatlar yoki buzilishlar ko'pincha administratorga xabar qilinadi yoki xavfsizlik ma'lumotlari va hodisalarni boshqarish (SIEM) tizimi orqali birlashtiriladi.

1.3.Packet sniffing hujumni amalga oshirish uchun dasturiy vositalar.

Hozirgi vaqtda tarmoqni sniffing qilish uchun ko'plab turli xil vositalari ishlab chiqilgan va ulardan faol foydalanilmoqda. Ular apparatga asoslangan sniffing qurilmalari yoki dasturiy ta'minotga asoslangan vositalar bo'lishi mumkin.

1.Wireshark

Wireshark mashhur ochiq manbali, o'zaro platformali tarmoq protokoli analizatori yoki boshqa so'z bilan aytganda, tarmoq ulanishidan paketlarni ushlaydigan paket snifferidir. U uy kompyuterlaridan tortib IT sohalarigacha keng qo'llaniladi.



7-rasm.Wireshark dasturining ishlash tartibi.

Wireshark - bu tarmoq protokoli analizatori yoki internetning tarmoq ulanishidan paketlarni ushlaydigan dastur. Paket - bu odatiy Ethernet tarmog'idagi diskret ma'lumotlar birligiga berilgan nom. Wireshark dunyodagi eng ko'p ishlatiladigan paketli sniffer hisoblanadi.

2. Tcpdump

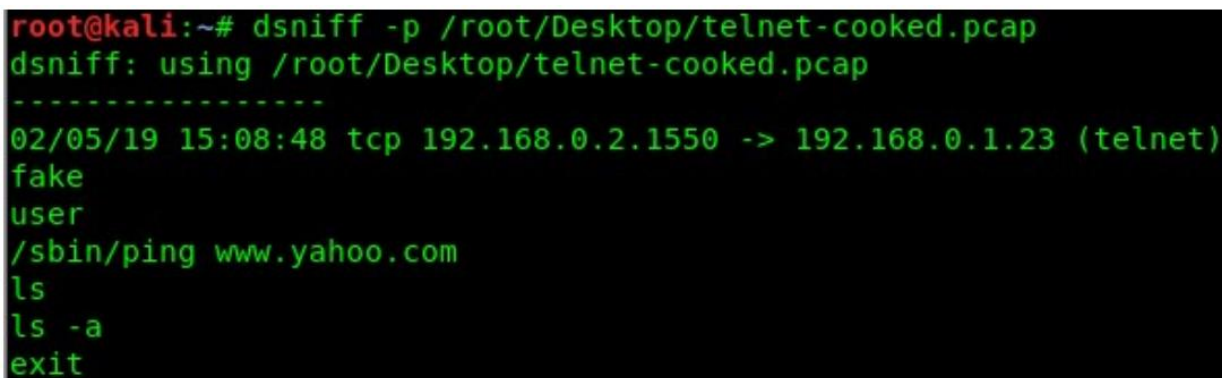
Tcpdump deb nomlanuvchi yana bir paket analizatori yaxshi grafik interfeysga ega bo'lgan boshqalardan farqli o'laroq, buyruq satridan ishga tushiriladi. U amalga oshirilayotgan mashina tomonidan yuborilgan yoki qabul qilingan paketlarni ushlab turish va ko'rsatish orqali tarmoq trafigini o'rganish uchun

ishlatilishi mumkin. U Linux va boshqa UNIX-ga o'xshash operatsion tizimlarda ishlaydi.

3. dSniff

dSniff - bu turli xil dastur protokollarini tahlil qilish va tegishli ma'lumotlarni olish uchun mo'ljallangan parolni aniqlash va tarmoq trafigin tahlil qilish vositalari to'plami. U bir qator protokollarni (FTP, Telnet, POP, rLogin, Microsoft SMB, SNMP, IMAP va boshqalar) tahlil qilish orqali ma'lumot olishi mumkin.

8-rasm.dSniff dasturiy vositasining ishlashi haqida qisqacha interface.



```
root@kali:~# dsniiff -p /root/Desktop/telnet-cooked.pcap
dsniiff: using /root/Desktop/telnet-cooked.pcap
-----
02/05/19 15:08:48 tcp 192.168.0.2.1550 -> 192.168.0.1.23 (telnet)
fake
user
/sbin/ping www.yahoo.com
ls
ls -a
exit
```

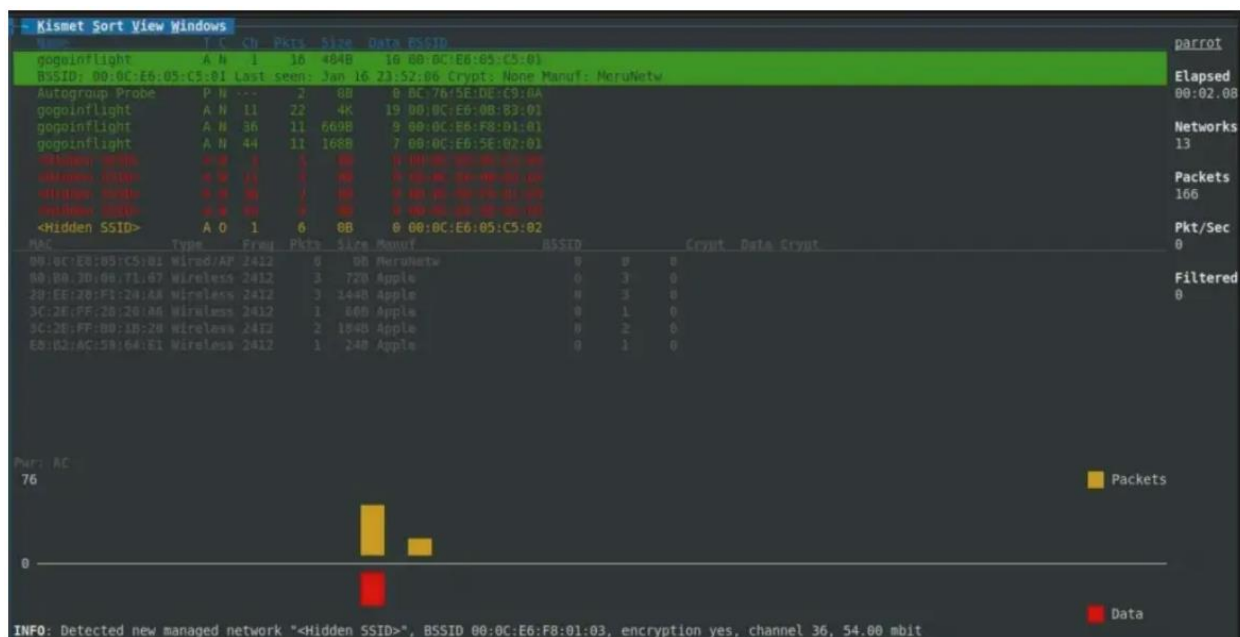
Ko'rib turganimizdek dSniff dasturiy vositasi ham Linux va boshqa UNIX-ga o'xshash operatsion tizimlarda ishlaydi.

4. NetworkMiner

NetworkMiner odatda hech qanday tarmoq trafigiga olib kelmasdan operatsion tizimlarni, seanslarni, xost nomlarini, ochiq portlarni va hokazolarni aniqlash uchun passiv tarmoq sniffer/paketni tortib olish dasturi sifatida ishlatiladi. NetworkMiner - bu paketlarni sniffing orqali hostlar va ochiq portlarni aniqlash uchun eng keng tarqalgan tarmoq tahlil qilish vositalaridan biri. Bundan tashqari, oflayn rejimda ham foydalanish mumkin.

5. Kismet

Kismet - bu WIDS (simsiz hujumni aniqlash) ramkasi va simsiz tarmoq va qurilma detektor bo'lib, u ko'pincha simsiz paketlarni sniffing hujumlarini amalga oshirish uchun ishlatiladi. Kismet Wi-Fi va Bluetooth interfeyslarini, shuningdek, ma'lum SDR (dasturiy ta'minot bilan belgilangan radio) apparat va boshqa maxsus suratga olish apparatlarini qo'llab-quvvatlaydi.

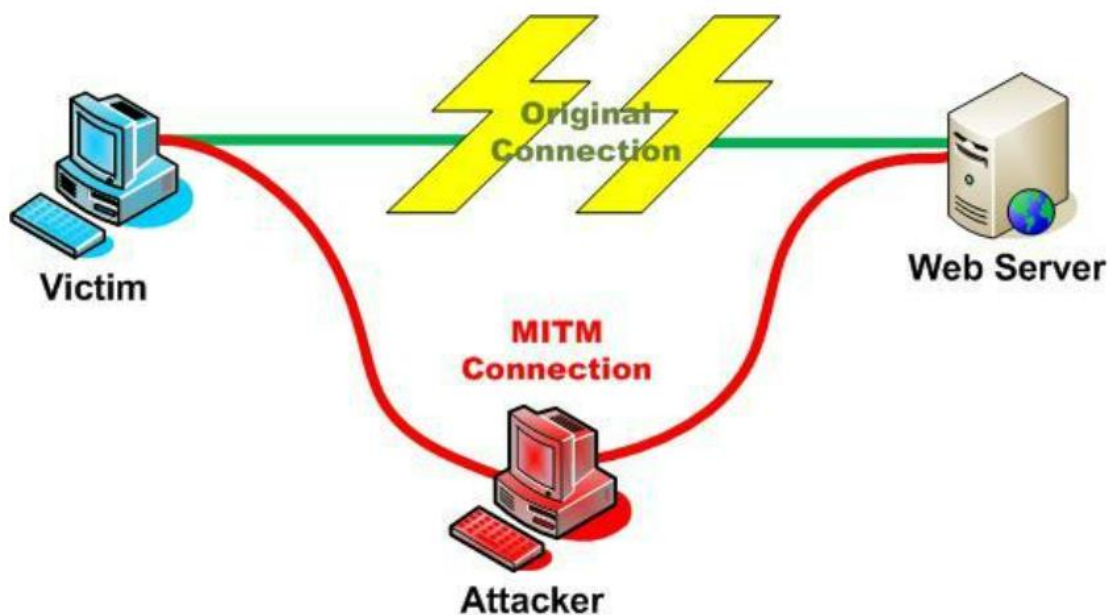


9-rasm.Kismet dasturiy vositasida sniff qilingan paketlar ko'rinishi.

Kismet - bu 802.11 qatlamli 2 simsiz tarmoq detektor, sniffer va hujumni aniqlash tizimi. Kismet monitoring (rfmon) rejimini qo'llab-quvvatlaydigan va 802.11b, 802.11a va 802.11g trafikni hidlashi mumkin bo'lgan har qanday simsiz karta bilan ishlaydi. Kismet paketlarni passiv ravishda yig'ish va standart nomli tarmoqlarni aniqlash, yashirin tarmoqlarni aniqlash va ma'lumotlar trafigin tarmoqlar mavjudligi haqida xulosa chiqarish orqali tarmoqlarni aniqlaydi.

6.Ettercap

Ettercap - bu tarmoqlarga o'rtadagi odam hujumlarini qo'llab-quvvatlash uchun ishlatilishi mumkin bo'lgan ochiq manbali vosita. Ettercap paketlarni ushlab, keyin ularni tarmoqqa yozishi mumkin. Ettercap real vaqt rejimida ma'lumotlarni o'zlashtirishi va o'zgartirish imkonini beradi.



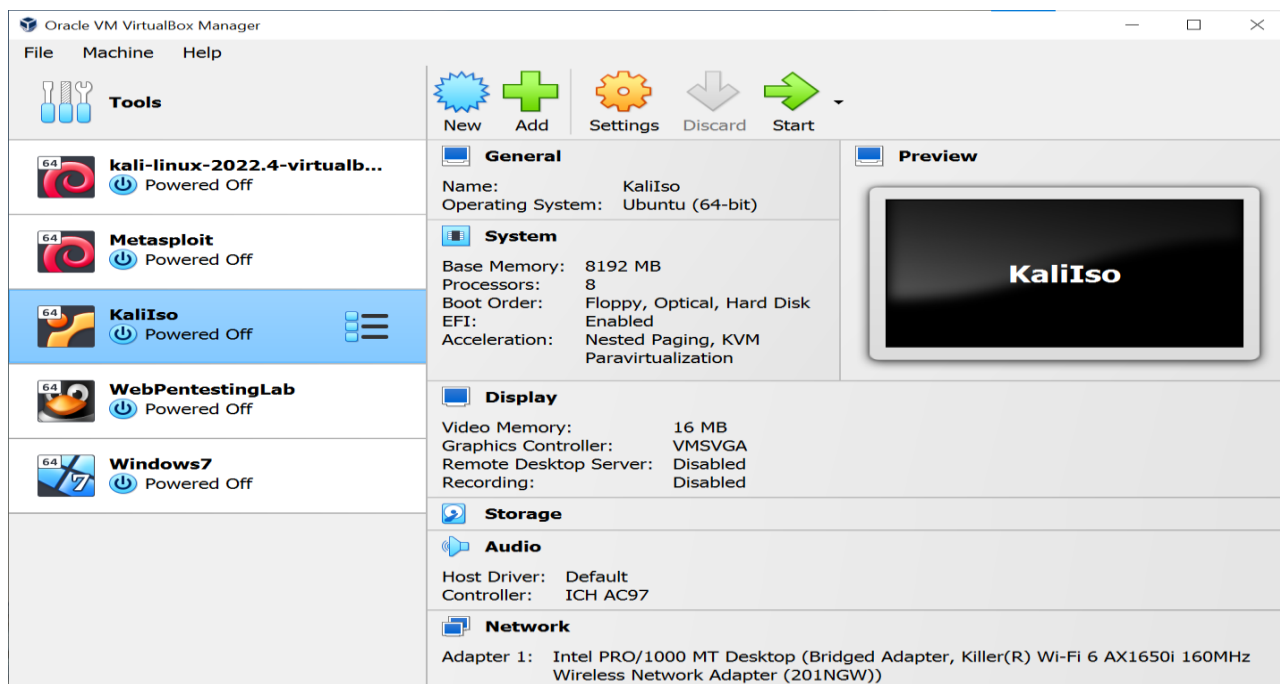
10-rasm.Ettercap dasturiy vositasida hujumning amalga oshirilishi.

Ettercap ko'prik rejimida tarmoqdagi qurilmalarining trafiklari bir qurilmadan ikkinchisiga uchinchi foydalanuvchi orqali ya'ni tajavuzkor orqali o'tadi.

Buzg'unchi sizning paketlaringizni o'qishi, kuzatishi va qo'lga kiritishi mumkin. Buning oldini olishning yaxshi usuli - bu sizning trafikingizni shifrlashdir. Kompyuterlar bir-biri bilan hub orqali aloqa qiladigan tarmoqda u xavfsiz emas va snifferlash oson. Kommutatorlar va marshrutizatorlar esa buni oldini olish uchun boshqa arxitekturadan foydalaniladi.

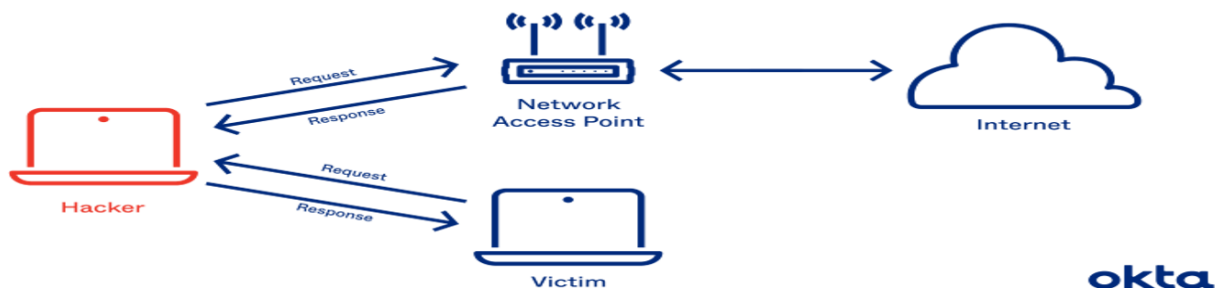
1.4 Amaliy dasturiy vositalar bilan sniffing hujumni amalga oshirish

Ettercap dasturiy vositasi bilan packet sniffing hujumini amalga oshirish uchun linux operatsion tizimi zarur. Biz local tarmoq yaratib olishimiz kerak va buning uchun virtualbox dan foydalanamiz. Hujumni amalga oshirish uchun virtualbox ga windows7 OS o'rnatiladi. Bunda windows7 o'rnatilgan virtual device victim ya'ni zararlanuvchi vazifasini bajaradi. Xujumchi vazifasini kali-linux OS bajaradi.

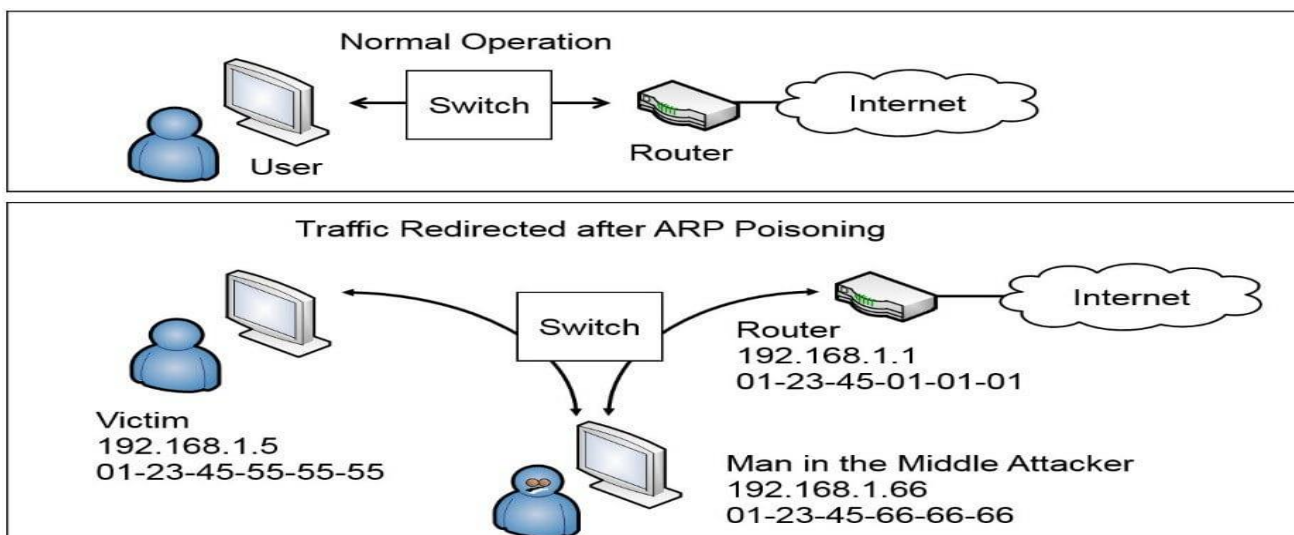


11-rasm. Hujumni amalga oshirish uchun muhim virtual OS lar.

Hujumning o'zi tajovuzkorning standart tarmoq shlyuziga noto'g'ri ARP xabarini yuborishidan iborat bo'lib, uning MAC manzili va IP manzili attackerning MAC va IP manziliga o'zlashtiriladi bu jarayon router bilan ham amalga oshiriladi.

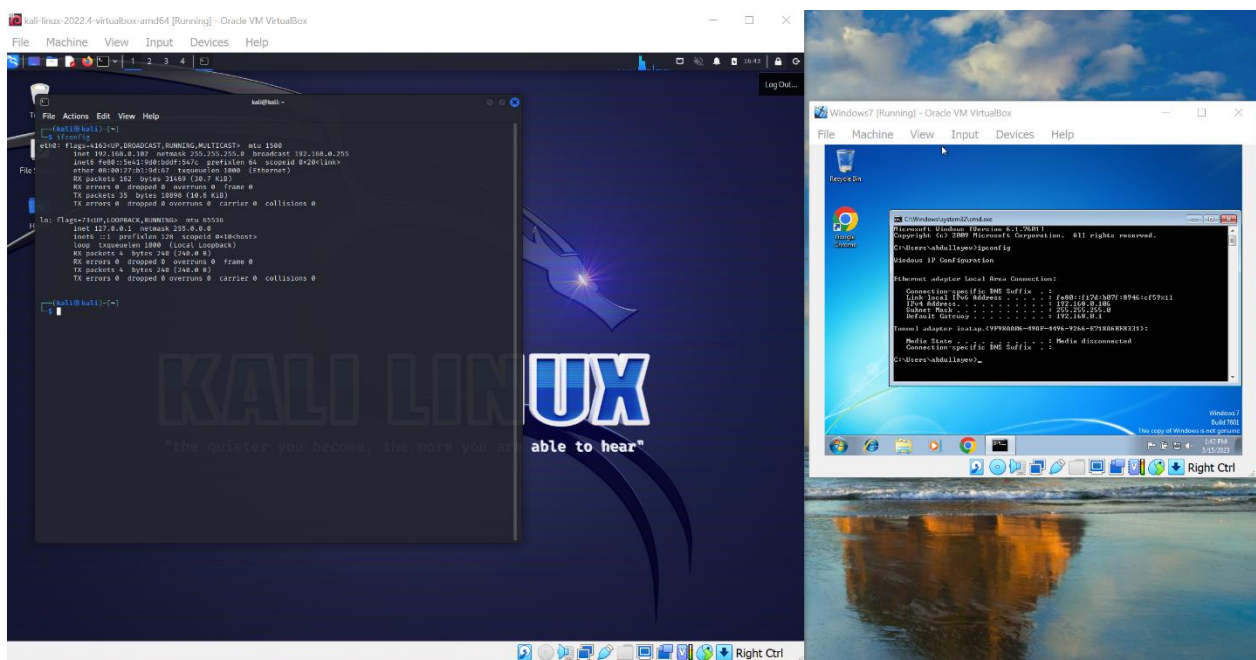


12-rasm. Ettercapda amalga oshiriladigan hujumning umumiy tuzilishi.



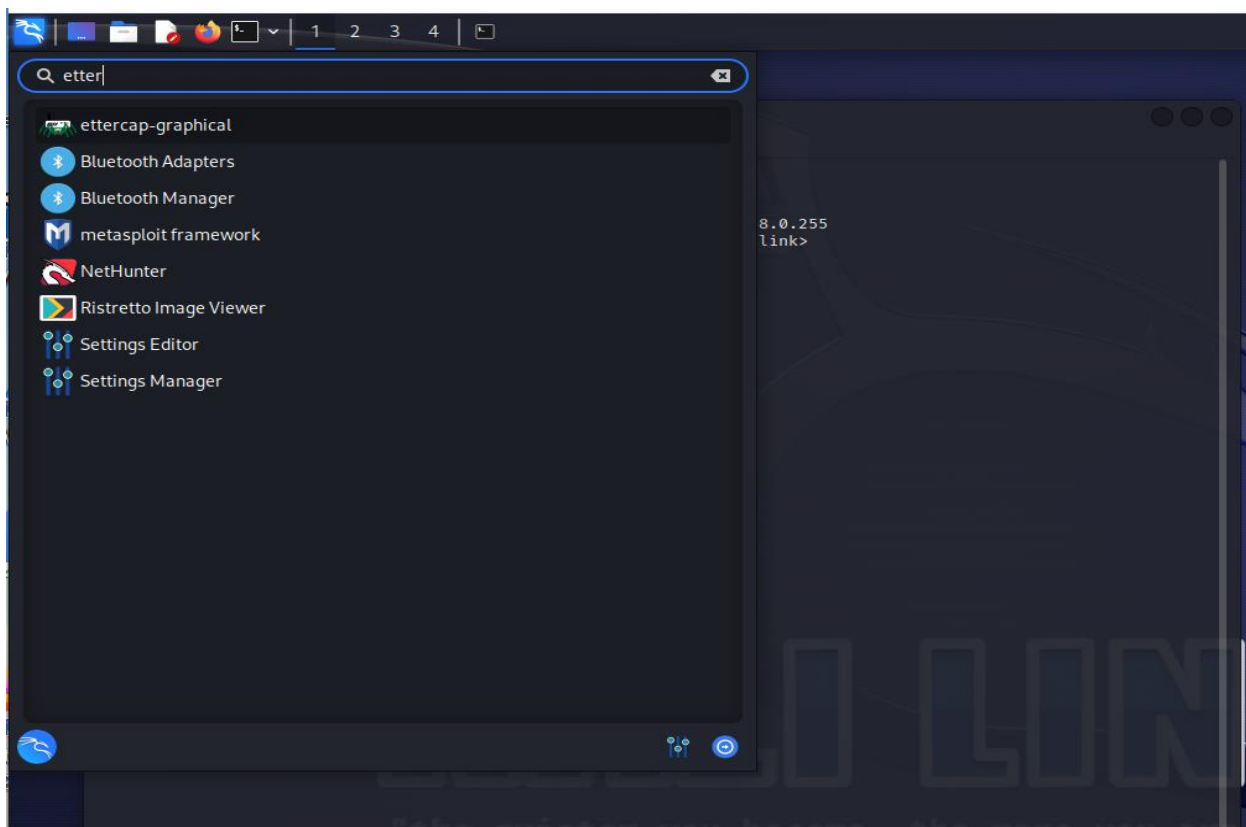
13-rasm.Hujumni amalga oshirilish tuzilishi.

Hujum amalga oshirilmagan holatda quyidagi 13-rasm ning birinchi qismi kabi paketlar almashinuvi amalga oshiriladi.Hujum amalga oshirilganda 13-rasm ning ikkinchi qismidagi kabi packet almashinuvi amalga oshiriladi.



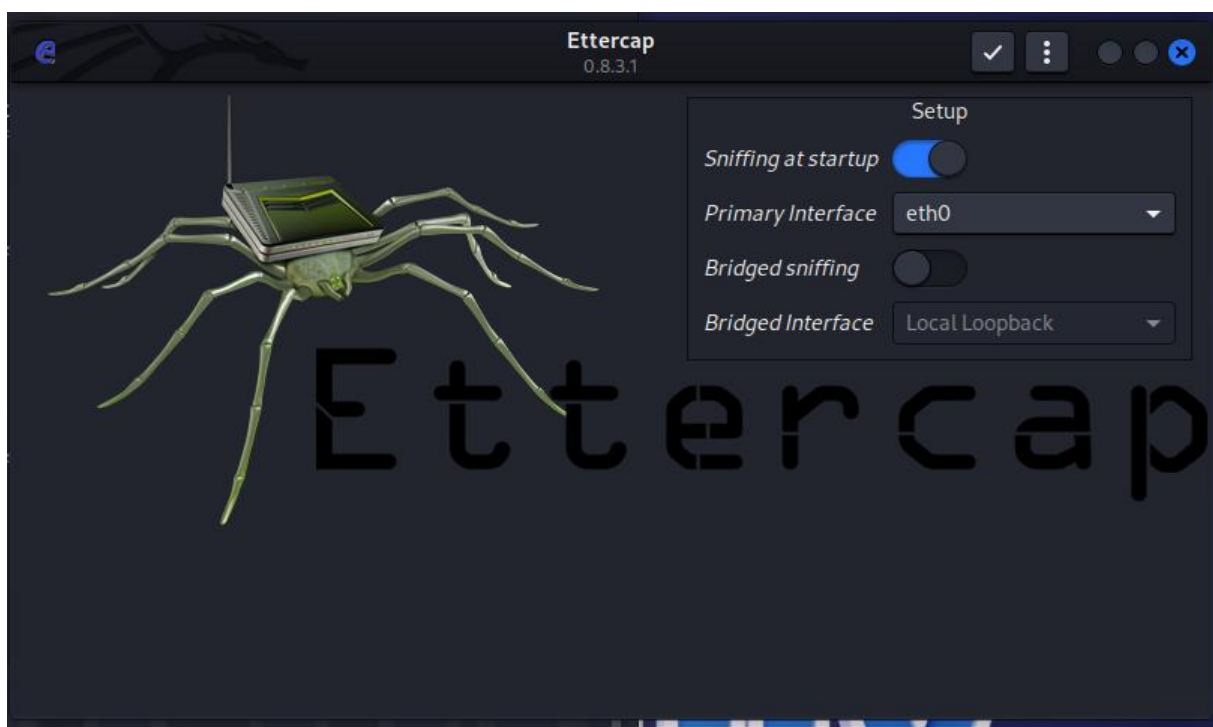
14-rasm.Kali linux(hujumchi) va windows7(victim,qurbon)lar ishga tushirildi.

Bunda hujumchining ip manzili 192.168.0.102,qurbonning ip manzili 192.168.0.106 ekan.Endi Kali linux OS da Ettercap dasturiy vositasini ishga tushiramiz bu dasturiy vosita kali linux OS da tayyor holda mavjud.



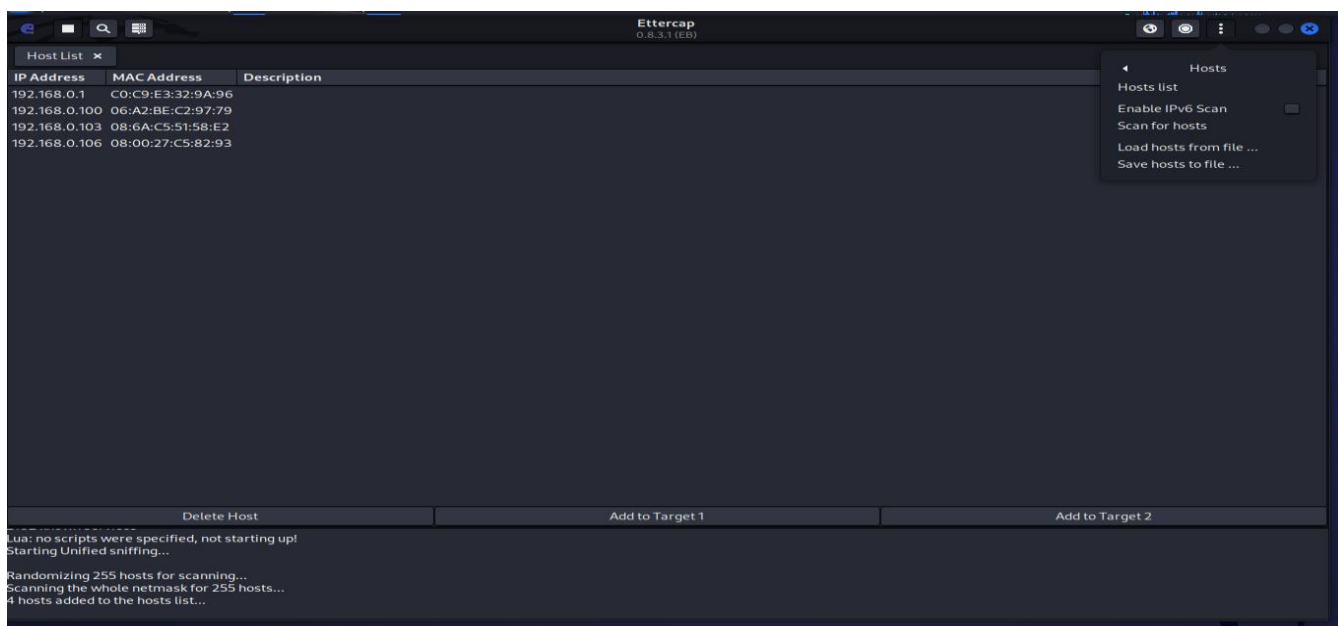
15-rasm.Ettercap dasturiy vositasini kali linuxda ishga tushirish.

15-rasmda ettercap-graphical dasturiy vositasi ishga tushiriladi.



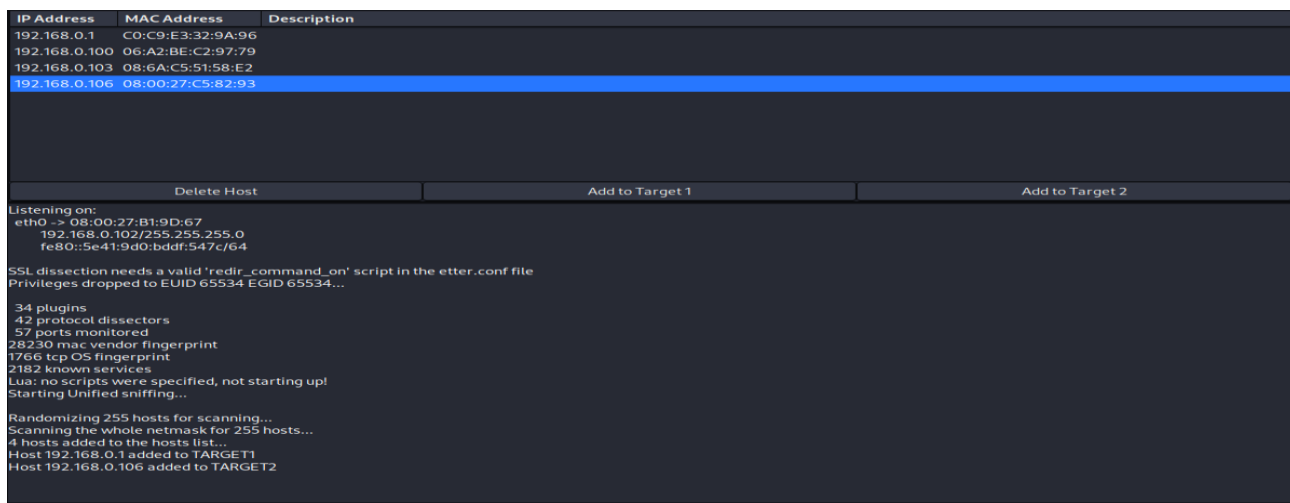
16-rasm.Ishga tushirilgan ettercap dasturining interface ko'rinishi.

Dastur ishga tushirilgach local tarmog'imizdagi hostlar ro'yxatini ko'rib olishimiz kerak ma buning uchun 17-rasmdan Host list tanlanadi.



17-rasm.Host list ya'ni local tarmog'imizdagi qurilamalar ro'yxati.

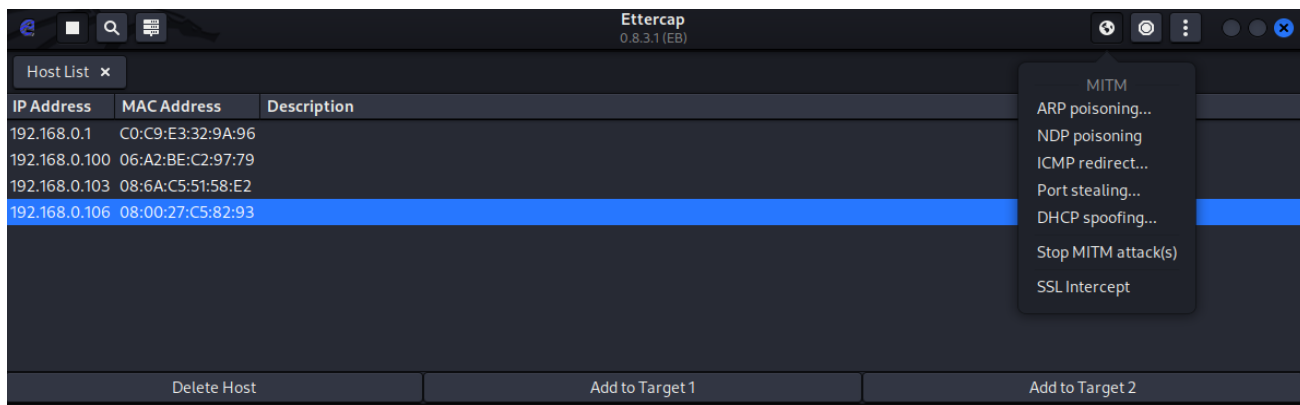
Bunda bizning local hostimizdagi qurilmalarni ip manzili va mac manzili bo'yicha ro'yxatini ko'rishimiz mumkin.



18-rasm.Victim va router ning ip manzillari tanlandi.

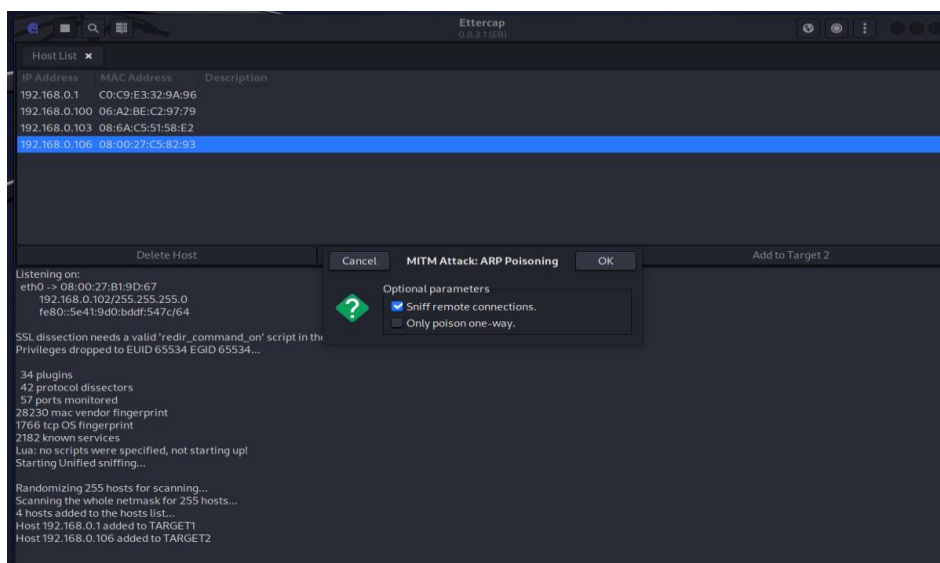
Hujumni amalga oshirish uchun biz Add to Target1 ya'ni 13-rasmda tasvirlanganidek router ga windows7miz deb o'zimizi tanshtirishimiz uchun routermizning ip manzilini tanlaymiz 192.168.0.1 tanlanadi.Add to Target2 uchun esa victimning ip manzili tanlanadi biz windows7ning ip manzilini tanlaymiz.

14-rasmdan windows7 ning ip manzilini ko'rishimiz mumkin 192.168.0.106 tanlanadi.



19-rasm.Hujumni amalga oshirish.

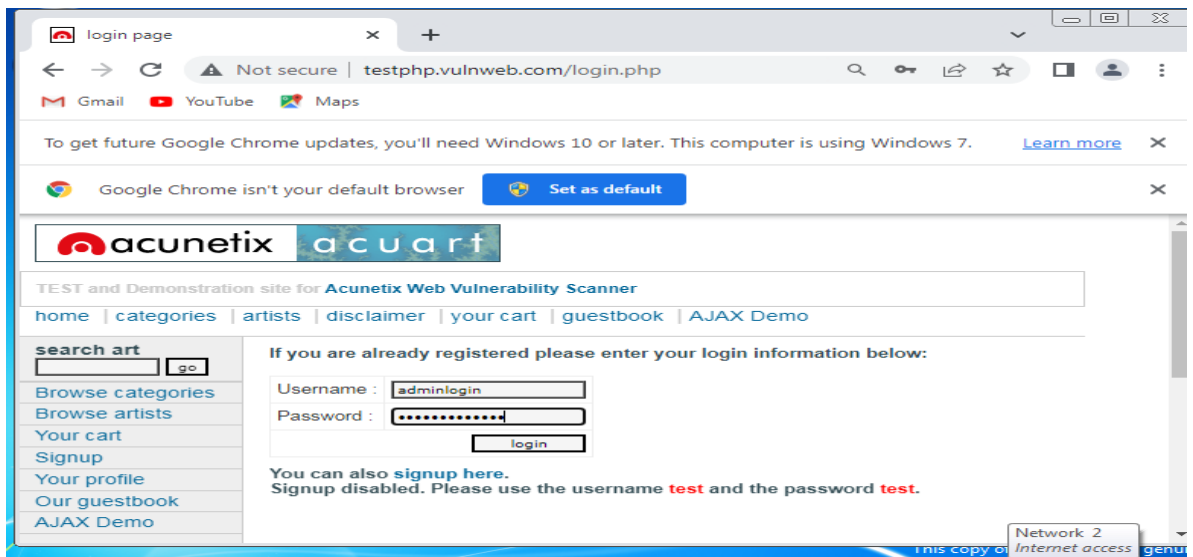
Bunda biz hujumni amalga oshirish uchun quyidagi interface dan ARP poisoning tanlanadi.



20-rasm.Hujumni tashqiqlash.

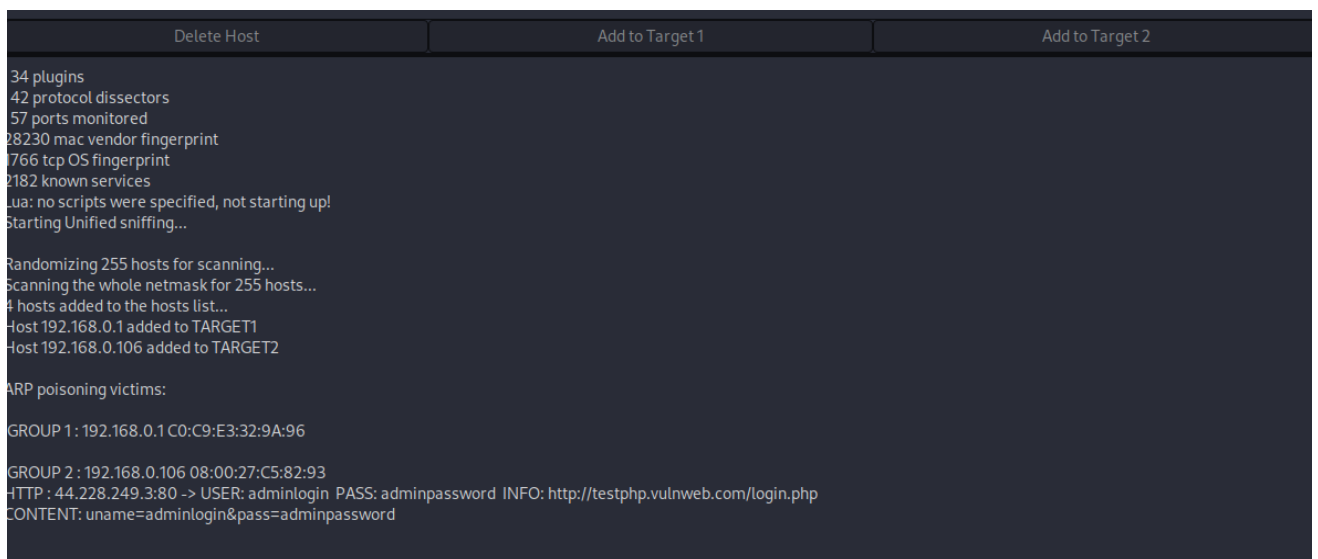
20-rasmdagi interface dan ok tugmasi bosiladi va hujum amalga oshiriladi va bizning kali linux OS dagi hujumchi qurilmamiz har biz paketni snifferlashni boshlaydi va biz bunnan windows7 qurilmamiz orqali <http://testphp.vulnweb.com>

Saytiga kiramiz va bizda login oynasi ochiladi va biz u yerga login va parolimizni kiritib login tugmasini bosamiz.



21-rasm. Victim login oynasidan o'z profiliga kirish uchun login parolni kiritishi tasvirlangan.

Endigi navbatda kali linux OS dan ochilgan interfaceni kuzatadigan bo'lsak victim kiritgan login va parol paydo bo'ldi



22-rasm. Kali OS tomonidan ushlangan packetdan olingan login va parol.

Ko'rib turbmizki bizda victimning kirgan sayt nomi va uning login va paroli paydo bo'ldi. Bu login va parol orqali victimning shaxsiy ma'lumotlarini qo'lga kiritish mumkin. Bu jarayonda ettercap dasturi o'tayotgan packetni snifferlashni amalga oshirdi va victimning login va parolini qo'lga kiritdi.

Xulosa

Mavzuga oid adabiyotlarni, internet materiallarini to'pladim va tahlil qildim va shuni aniqladimki biz shaxsiy va professional vazifalarni bajarishda tarmoq texnologiyasiga ko'proq tayanadigan jamiyatda paketlarni hidlash hujumi jiddiy tahdiddir. Bu xakerlarga tarmoq orqali harakatlanadigan ma'lumotlar trafigiga kirish imkonini beradi - va Internet orqali uzatiladigan juda ko'p nozik ma'lumotlar bilan paketlarni sniffing hujumlaridan himoya qilish juda muhimdir. Murakkab snifferlar zaifliklardan foydalanishi va tarmoq xavfsizligini buzishi mumkin, bu esa kompaniyalarni katta xavf ostiga qo'yadi. So'nggi paytlarda tashkilotlar o'zlarining ma'lumotlarini sniffingdan himoya qilish uchun ilg'or sun'iy intellekt usullariga sarmoya kiritmoqdalar. Ushbu yechimlar juda yaxshi lekin sun'iy intellekt dasturiy vositalarining o'zi ishonchli ekanligiga ishonch hosil qilgan holga keyinchalik bunnan foydalanish muhimdir. Lekin yillar o'tsada yangidan yangi hujum turlari paydo bo'lishda davom qilaveradi shuning uchun internetdan foydalanuvchilar qurilmasini ayni shu zamon uchun ishonchli bo'lgan dasturiy vositalarni o'rnatib uni xavfsizligini ta'minlab borishi kerak.

Foydalanilgan adabiyotlar

1. T. Alpcan, T. Basar: Network Security - A Decision and Game-Theoretic Approach
- I. Blake, G. Seroussi, N. Smart: Elliptic Curves in Cryptography
2. R. Churchhouse: Codes and Ciphers
- I. Csiszar, J. Koerner: Information Theory: Coding Theorems for Discrete Memoryless Systems
3. E. Desurvire: Classical and Quantum Information Theory
4. O. Goldreich: Foundations of Cryptography, Volumes I and II
5. S. W. Golomb, G. Gong: Signal Design for Good Correlation For Wireless Communication, Cryptography, and Radar
6. M. Hendry: Multi-application Smart Cards Technology and Applications
7. R. Lidl, H. Niederreiter: Finite Fields (2nd Edition)
8. S. Loepp, W. Wootters: Protecting Information: From Classical Error Correction to Quantum Cryptography
9. J. H. Loxton: Number Theory and Cryptography
10. R. J. McEliece: The Theory of Information and Coding (2nd Edition)
11. N. D. Mermin: Quantum Computer Science
12. M. A. Nielsen, I. L. Chuang: Quantum Computation and Quantum Information
13. <https://fayllar.org>
14. <https://cryptography.com>
15. <https://Github.com>