RAZVEDKA (INTELLIGENCE GATHERING) VA FOOTPRINTING USULLARINING TASNIFI

Hafizov Shukrullo Fayzullo o‘g‘li
O‘ktamov Doston Rustam o‘g‘li
Toshpo‘lotov Maqsud Abduvali o‘g‘li
Baxtiyorov Murodjon Farxodjon o‘g‘li
Muxammad al – Xorazmiy nomidagi TATU talabalari

Annotatsiya: *Ushbu maqolada kiberxavfsizlik sohasida muhim bosqichlardan biri hisoblangan razvedka (intelligence gathering) va footprinting usullarining tasnifi tahlil qilinadi. Footprinting jarayoni maqsad tizimi yoki tarmog‘i haqida dastlabki ma’lumotlarni yig‘ish orqali potentsial zaifliklarni aniqlash imkonini beradi. Maqolada footprintingning ikki asosiy turi — passiv va aktiv usullari ko‘rib chiqilgan. Passiv footprinting jarayonida ochiq manbalardan ma’lumot yig‘ish usullari, jumladan WHOIS ma’lumotlar bazasi, DNS yozuvlari, IP manzil bloklari hamda elektron pochta manzillarini tahlil qilish usullari yoritilgan. Shuningdek, aktiv footprinting jarayonida portlarni skanerlash, ping sweep, traceroute va banner grabbing kabi texnikalar tahlil qilingan. Tadqiqot natijalari footprinting usullarini to‘g‘ri tushunish va ulardan foydalanish tarmoq xavfsizligini ta’minlash hamda potentsial kiberhujumlarning oldini olishda muhim ahamiyatga ega ekanligini ko‘rsatadi.*

Kalit so‘zlar: *Footprinting, razvedka (intelligence gathering), kiberxavfsizlik, passiv footprinting, aktiv footprinting, WHOIS, DNS yozuvlari, port skanerlash, ping sweep, banner grabbing, OSINT.*

Razvedka, ko‘pincha kiberhujumning birinchi bosqichi bo‘lib, hujumni amalga oshirishda juda muhim ro‘l o‘ynaydi. Razvedkaning, yoki footprintingning, maqsadi - maqsad tizimi yoki tarmog‘i haqida iloji boricha ko‘proq ma’lumot to‘plash. Bu bosqich hujumning asosini tashkil etadi va IP manzillari, tarmoq tuzilishi, domen nomlari va xodimlar haqida ma’lumotlarni olish imkonini beradi. Razvedka vaqtida to‘plangan ma’lumotlar katta zaifliklarni ochib beradi, bu esa hujumchilarga samarali va muvofiq hujumlar tayyorlashga yordam beradi. Razvedka usullarini va tasniflarini tushunish hujumchilar hamda himoyachilar uchun juda muhimdir, chunki bu xavflarni kamaytirishga yordam beradi.

Footprinting - bu maqsad tizimi haqida ma’lumot yig‘ish jarayoni bo‘lib, bu ma’lumotlar tizimda potentsial zaifliklarni aniqlash uchun ishlatiladi. U zararli maqsadlar uchun amalga oshirilishi mumkin, lekin etik xakerlar, tizim administratorlari va xavfsizlik mutaxassislari tomonidan tizimlarni kuchaytirish uchun ham foydalidir. Bu bosqichda to‘plangan ma’lumotlar tashkilotning infratuzilmasini

qanday tuzilganini va uning qanday zaifliklarga ega ekanligini tushunishga yordam beradi.

Ushbu bo‘limda footprintingning ikki asosiy turini - Passiv Footprinting va Aktiv Footprinting - ko‘rib chiqamiz. Har bir usul o‘ziga xos xususiyatlarga, afzalliklarga va cheklovlarga ega bo‘lib, har bir xavfsizlik tahlili yoki etik xakerlik jarayonida qaysi usulni tanlash kerakligini tushunish juda muhimdir.

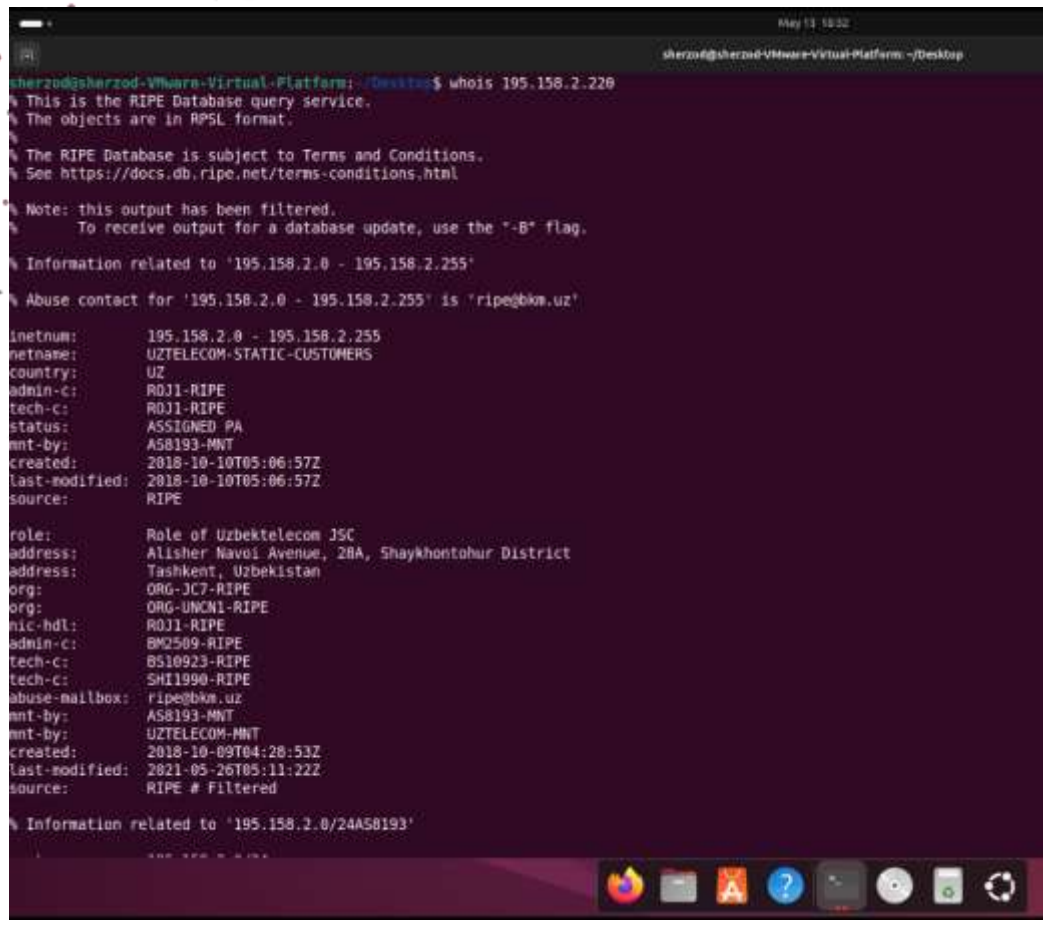
Passiv Footprinting Usullari.

Passiv Footprinting - bu maqsad tizimi yoki tarmog‘iga bevosita aralashmasdan ma’lumot to‘plash jarayonidir. Ushbu usul maqsadning xavfsizlik monitoring tizimlarida ogohlantirishlarni chaqirmaydi, bu esa hujumchilarga yashirin qolishga imkon beradi. Passiv usullar asosan jamoatga ochiq ma’lumotlarga tayanadi va hujumchi maqsad tizimiga hech qanday trafik yubormaydi.

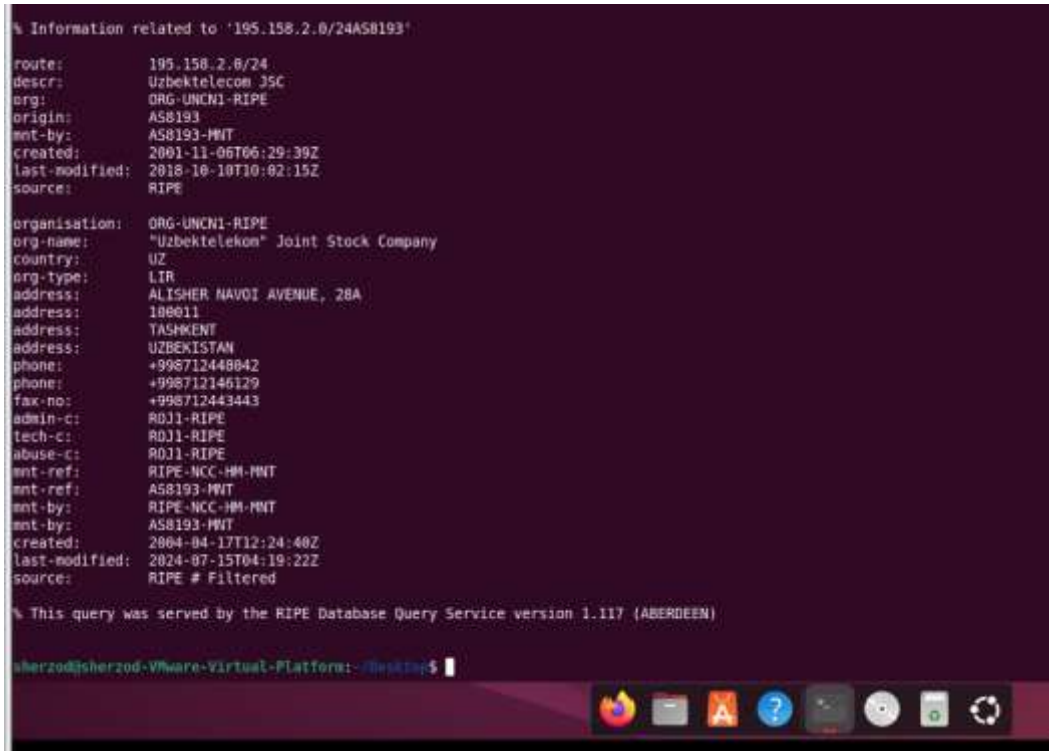
Passiv Footprinting uchun Manbalar:

- WHOIS Ma’lumotlar Bazasi: WHOIS ma’lumotlar bazasi passiv footprinting uchun eng qimmatbaho manbalardan biridir. Ushbu baza domen ro‘yxatdan o‘tkazish ma’lumotlarini, shu jumladan, egalik nomi, manzil, aloqa ma’lumotlari va nameserverlarni o‘z ichiga oladi. WHOIS ma’lumotlar bazasidan so‘rov yuborish orqali hujumchilar domen egalari va ularga tegishli infratuzilma haqida ma’lumot olishlari mumkin.

Misol: Agar biror kompaniya domenni ma’lum bir ro‘yxatdan o‘tkazuvchi orqali ro‘yxatdan o‘tkazsa, hujumchilar WHOIS ma’lumotlari orqali ro‘yxatdan o‘tkazuvchi bilan bog‘liq kontakt ma’lumotlarini topishlari mumkin, bu esa ijtimoiy muhandislik yoki phishing hujumlariga olib kelishi mumkin.



1-rasm. WHOIS ning ko‘rinishi.



2-rasm. WHOIS chiqarib bergan ma’lumotlar.

• DNS Yozuvlari: Domen nomlari tizimi (DNS) yana bir boy ma’lumot manbai hisoblanadi. DNS yozuvlari domen nomlarini IP manzillariga bog‘lash va pochtaning

serverlari (MX yozuvlari) va boshqa xizmatlar haqida ma’lumotlarni o‘z ichiga oladi. DNS yozuvlarini tahlil qilib, hujumchilar subdomenlar, pochta serverlari va ba’zan hatto infratuzilmani, masalan, yuk taqsimlovchi yoki xavfsizlik devorlari kabi ma’lumotlarni topishlari mumkin.

Misol: DNS yozuvlari, ochiq ro‘yxatga olinmagan subdomeni aniqlashga yordam berishi mumkin, bu esa hujumchilarga tarmoq yoki tizimga yangi kirish nuqtasini beradi. Bundan tashqari, DNS konfiguratsiyalarini tahlil qilish, maqsad tarmog‘ining mumkin bo‘lgan noto‘g‘ri konfiguratsiyalari yoki zaifliklarini aniqlashga yordam beradi.

- IP Manzil Bloklari: Maqsadning IP manzil bloklari haqidagi ma’lumotlar ham ochiq manbalardan yig‘ilishi mumkin. Tashkilotga tayinlangan IP diapazoni ko‘pincha uning infratuzilmasi bilan bog‘liq bo‘ladi. Hujumchilar ushbu ma’lumotni, masalan, serverlarning geografik joylashuvi yoki maxsus xizmatlarga tegishli IP manzillarni aniqlash uchun qo‘llashlari mumkin.

Misol: ARIN (American Registry for Internet Numbers) yoki RIPE (Réseaux IP Européens) kabi vositalardan foydalanib, hujumchilar maqsadga tegishli bo‘lgan IP manzillarini aniqlashlari va ularning ustida ochiq portlar yoki xizmatlarni topishlari mumkin.

- Email Ma’lumotlari: Kompaniya yoki tashkilotga tegishli elektron pochta manzillari ham ijtimoiy tarmoqlar, korporativ veb-saytlar yoki pochta manzillarini tasdiqlash vositalari orqali topilishi mumkin. Hujumchilar email manzillarini spear-phishing yoki ijtimoiy muhandislik hujumlari uchun ishlatishlari mumkin, bu esa xodimlar xatti-harakatlarini ekspluatatsiya qilish yoki sezgir ma’lumotlarni yig‘ish imkonini beradi.

Misol: Email xususiyatlarini tahlil qilish yoki korporativ veb-saytlarni scrapping orqali hujumchilar tashkilotning ierarxiyasini tasvirlashlari va yuqori lavozimdagi rahbarlarni spear-phishing urinishlari uchun asosiy maqsadlar sifatida aniqlashlari mumkin.

Passiv Footprintingning Afzalliklari:

- Aniqlanish xavfi yo‘q: Passiv footprinting maqsad tizimi bilan bevosita aloqada bo‘lmaganligi sababli, u xavfsizlik tizimlari tomonidan ogohlantirishni chaqirish ehtimoli kam.
- Minimal Harakat: Jamoatga ochiq ma’lumot manbalari osonlik bilan olinishi mumkin va ma’lumot yig‘ish jarayonini avtomatlashtirish uchun turli OSINT (Open Source Intelligence) vositalaridan foydalanish mumkin.
- Keng Ma’lumotlar Doirasi: Passiv usullar ko‘pincha texnik tafsilotlardan tortib tashkilot tuzilmasigacha bo‘lgan keng spektrdagi ma’lumotlarni ochib beradi.

Cheklovlar:

• Cheklangan Ma’lumot: Passiv footprinting juda ko‘p ma’lumot to‘plashi mumkin, lekin bu tizimning ichki xavfsizligi yoki zaifliklariga to‘liq kirish imkonini bermaydi.

• Vaqtni Olishi: Jamoat manbalaridan ma’lumot yig‘ish ko‘p vaqt olishi mumkin, ayniqsa bir nechta manbalarni konsultatsiya qilish zarur bo‘lsa.

Aktiv Footprinting Usullari

Aktiv Footprinting - bu maqsad tizimi yoki tarmog‘i bilan bevosita aloqada bo‘lishni o‘z ichiga oladi. Passiv usullardan farqli o‘laroq, ular jamoatga ochiq ma’lumotlarga tayanmasa, aktiv footprinting maqsad tizimlarining o‘zidan ma’lumotlarni olish uchun tizimlarga so‘rovlar yuboradi, bu esa xavfsizlik monitoring tizimlarida ogohlantirishlarni chaqirishi mumkin. Aktiv footprinting usullari ko‘proq ta’sirchan bo‘lib, maqsad tizimlari haqida yanada batafsil ma’lumotni ochib beradi.

• Portlarni Skanning: Portlarni skanerlash - bu aktiv footprinting usullaridan eng keng tarqalganidir. Nmap yoki Masscan kabi vositalardan foydalanib, hujumchilar maqsadning IP manzilini skanerlash orqali ochiq portlarni va ularning ustida ishlayotgan xizmatlarni aniqlashlari mumkin. Bu hujumchilarga mavjud xizmatlar haqida ma’lumot olish imkonini beradi, masalan, web serverlari, FTP serverlari yoki pochta serverlari.

Misol:

Portlarni skanerlash orqali hujumchi serverda eski versiyada web serveri mavjudligini aniqlashi mumkin, bu esa ma’lum zaifliklarga ega bo‘lishi mumkin.

• Ping Sweep (Pingni Qayta Tekshirish): ing sweep ma’lum bir IP diapazonidagi faol xostlarni aniqlash uchun ishlatiladi. Bu jarayon, bir nechta IP manzillariga ICMP (Internet Control Message Protocol) echo so‘rovlari yuborish va qaysi manzillar javob berishini yozib olishni o‘z ichiga oladi, bu esa faol xostlarni ko‘rsatadi. Bu usul hujumchilarga tarmoqni xaritalashda va maqsadli tizimlarni aniqlashda yordam beradi.

• Traceroute:

Traceroute - bu paketlarning ma’lum bir manzilga yetib borish yo‘lini kuzatadigan vositadir. Yo‘nalish yo‘li tahlil qilinganida, hujumchilar ular bilan maqsad orasidagi oraliq qurilmalarni (masalan, marshrutizatorlar, xavfsizlik devorlari) aniqlashlari mumkin. Bu tarmoq infratuzilmasi haqida, hatto maqsad serverlarining joylashuvi haqida ma’lumot beradi.

• Banner Grabbing (Bannerni olish): Banner grabbing - bu xizmatlarga (masalan, web serverlari yoki FTP serverlari) so‘rovlar yuborib, ularning javoblarini yig‘ish jarayonidir. "Banner" - bu xizmat tomonidan qaytarilgan ma’lumot bo‘lib, odatda dastur versiyasi, operatsion tizim va konfiguratsiya tafsilotlari haqida ma’lumot beradi. Hujumchilar banner grabbing orqali maxsus dastur versiyalariga oid zaifliklarni aniqlashlari mumkin.

Aktiv Footprintingning Afzalliklari:

• Batafsil Ma’lumot: Aktiv usullar passiv usullarga qaraganda ancha aniq va foydali ma’lumotlarni beradi, shu jumladan jonli ma’lumotlar va tizim konfiguratsiyasi tafsilotlarini.

• Zudlik bilan Natijalar: Aktiv footprinting maqsad tizimlari va tarmoqlari haqida real vaqt ma’lumotlarini taqdim etadi.

Cheklovlar:

• Aniqlanish Xavfi: Aktiv footprinting maqsad tizimi bilan bevosita aloqada bo‘lishni o‘z ichiga oladi, bu esa xavfsizlik devorlari, kirish aniqlash tizimlari (IDS) yoki boshqa xavfsizlik choralarini ishga tushirish ehtimolini oshiradi.

• Taqiqlovchi: Aktiv texnikalar tizimlarning normal ishlashini buzishi yoki maqsadni potentsial hujumchi mavjudligi haqida ogohlantirishi mumkin, bu esa passiv usullarga qaraganda kamroq yashirin usuldir.

XULOSA

Xulosa qilib aytganda, razvedka va footprinting jarayoni kiberxavfsizlik sohasida muhim bosqich hisoblanadi. Ushbu jarayon orqali maqsad tizimlari va tarmoqlari haqida turli darajadagi ma’lumotlar to‘planadi. Passiv footprinting usullari ochiq manbalardan foydalanib, tizim bilan bevosita aloqaga kirishmasdan ma’lumot yig‘ish imkonini beradi va aniqlanish xavfini kamaytiradi. Aktiv footprinting usullari esa tarmoq bilan bevosita aloqada bo‘lib, portlarni skanerlash, ping sweep va banner grabbing kabi texnikalar orqali yanada batafsil ma’lumotlarni taqdim etadi. Shu bilan birga, bu usullar xavfsizlik tizimlari tomonidan aniqlanish ehtimolini ham oshiradi. Footprinting usullarini chuqur o‘rganish va ulardan to‘g‘ri foydalanish tizim administratorlari hamda axborot xavfsizligi mutaxassislariga tarmoq zaifliklarini aniqlash va ularni bartaraf etishda katta yordam beradi.

FOYDALANILGAN ADABIYOTLAR:

1. Stallings W. Network Security Essentials: Applications and Standards**.** Pearson Education, 2017.

2. Erickson J. Hacking: The Art of Exploitation. No Starch Press, 2018.

3. Kurose J., Ross K. Computer Networking: A Top-Down Approach**.** Pearson, 2021.

4. Weidman G. Penetration Testing: A Hands-On Introduction to Hacking. No Starch Press, 2019.

5. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS)**.** NIST Special Publication.

6. ARIN (American Registry for Internet Numbers) Documentation. https://www.arin.net

7. RIPE NCC Documentation. https://www.ripe.net