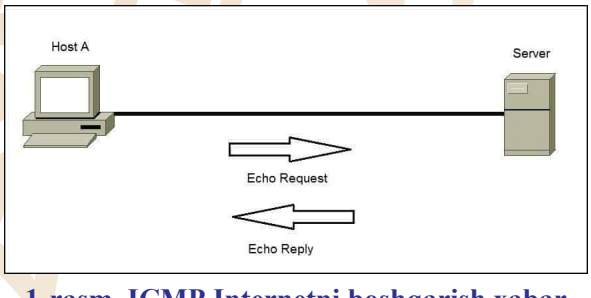
ma’lumotlarni yuborish va javobni tahlil qilish orqali xost tomonidan foydalaniladigan port raqami, OS va ilovalar haqida ma’lumot to’plashlari mumkin. Misol uchun, oddiy portni skanerlash TCP skanerlash deb ataladigan usul bilan amalga oshirilishi mumkin , u maqsad portda 3 tomonlama Handshake-ni sinab ko’rish orqali portning ishlatilayotganligini tekshiradi. Biroq, 3 tomonlama Handshake hatto standart TCP ulanishlarida ham amalga oshirilganligi sababli, portni skanerlash hujumi va paketma-paket asosidagi muntazam aloqani farqlash qiyin. Xostni aniqlash, tarmoqdagi qaysi tizimlar ishlayotganini va tinglayotganini aniqlash jarayoni ko’pincha tarmoqni skanerlashda birinchi qadamdir. Xostni aniqlash uchun ikkita protokol eng ko’p qo’llaniladi: manzilni aniqlash protokoli (ARP) va bir necha turdagi Internetni boshqarish xabar protokoli (ICMP) skanerlari. Shaxsiy ARP so’rovlari IP-manzillarni mahalliy quyi tarmoqdagi MAC manzillari bilan taqqoslash uchun foydalanilganligi sababli, ARP so’rovlari mahalliy tarmoqdagi (LAN) ko’plab IP-manzillarga yuborilishi mumkin[3].



1-rasm. ICMP Internetni boshqarish xabar protokoli

Mahalliy quyi tarmoqdan tashqarida tarmoqni skanerlash uchun uning o‘rniga bir necha turdagi ICMP paketlaridan foydalanish mumkin, jumladan echo, vaqt tamg‘asi va manzil maskalari so‘rovlari. Echo (yoki ping) so‘rovlari boshqa xostga kirish mumkinligini aniqlash uchun ishlatiladi, vaqt tamg‘asi xabarlari esa ikki xost o‘rtasidagi kechikishni aniqlaydi. Manzil niqobi so‘rovlari tarmoqda ishlatilayotgan pastki tarmoq niqobini aniqlash uchun mo‘ljallangan.

Har bir ICMP xabar turi uchun xostni topish mavjud xostlardan tegishli javob olishga bog‘liq. Agar javob olinmasa, bu manzilda tinglayotgan xost yo‘qligini, so‘rov paketi xavfsizlik devori yoki paket filtri tomonidan bloklanganligini yoki xabar turini maqsad qurilma tomonidan qo‘llab-quvvatlamasligini anglatadi. Ichki tarmoqdan tashqarida paydo bo‘lgan ICMP echo so‘rovlari odatda xavfsizlik devorlari tomonidan bloklanadi, ammo vaqt tamg‘asi va manzil maskalari so‘rovlarini bloklash ehtimoli kamroq. Xostni aniqlash, tarmoqdagi qaysi tizimlar ishlayotganini va tinglayotganini aniqlash jarayoni ko‘pincha tarmoqni skanerlashda birinchi qadamdir. Xostni aniqlash uchun ikkita protokol eng ko‘p qo‘llaniladi: manzilni aniqlash protokoli (ARP) va bir necha turdagi Internetni boshqarish xabar protokoli (ICMP) skanerlari. Shaxsiy ARP so‘rovlari IP-manzillarni mahalliy quyi tarmoqdagi MAC manzillari bilan taqqoslash uchun foydalanilganligi sababli, ARP so‘rovlari mahalliy tarmoqdagi (LAN) ko‘plab IP-manzillarga yuborilishi mumkin[4].

Tarmoqni skanerlash orqali tarmoqdagi mavjud xostlar topilgach, ma’lum portlarda ishlatilayotgan xizmatlarni aniqlash uchun portni skanerlashdan foydalanish mumkin. Umuman olganda, portni skanerlash portlarni uchta belgidan biriga tasniflashga harakat qiladi:

Ochiq: manzil o‘sha portda tinglayotganini bildiruvchi paket bilan javob beradi, bu esa skanerlash uchun qanday xizmat (odatda TCP yoki UDP) ishlatilganligini ham ko‘rsatadi.

Yopiq: manzil so‘rov paketini oldi, lekin portda tinglovchi xizmat yo‘qligini bildiruvchi javob bilan javob qaytaradi.

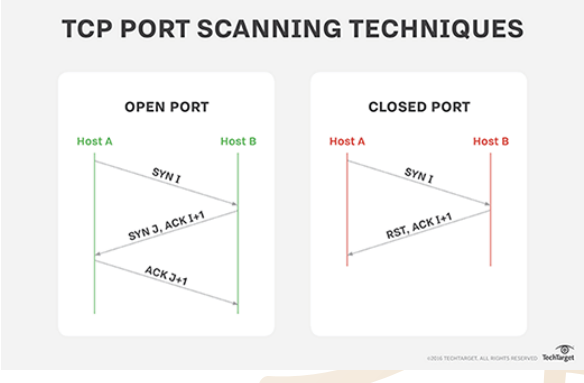
Filtrlangan: port ochiq bo‘lishi mumkin, ammo paket xavfsizlik devori tomonidan filtrlangan va o‘chirilgan, shuning uchun hech qanday javob olinmaydi. Yuqorida aytib o‘tilganidek, TCP va UDP portlarni skanerlashda tez-tez ishlatiladigan protokollardir. TCP skanerlashning bir necha usullari mavjud:

SYN skanerlash, TCP skanerlashning eng keng tarqalgan shakli, SYN paketini yuborish va javobni baholash orqali maqsadli portga yarim ochiq ulanishni o‘rnatishni o‘z ichiga oladi. Xost port ochiq bo‘lsa, SYN/ACK paketini yoki port yopiq bo‘lsa, RST javobini yuborish orqali javob beradi. Shuningdek, yopiq port RST paketi o‘rniga ICMP portiga yetib bo‘lmaydigan xabar bilan javob berishi mumkin, ammo bu hozirgi kunda kamroq tarqalgan. Hech qanday javob yo‘qligi port filtrlanganligini ko‘rsatadi.

TCP skanerlashning yuqori darajadagi usuli bu TCP ulanish skanerlash bo‘lib, unda skaner

ulanish tizimi qo‘ng‘irog‘i va to‘liq TCP qo‘l siqish jarayonidan foydalangan holda TCP orqali portga ulanishga harakat qiladi. Ushbu usul SYN skanerlashdan ko‘ra kamroq qo‘llaniladi, chunki u paketlar va vaqt jihatidan ko‘proq xarajatlarni talab qiladi va oson aniqlanadi.Port raqami IP-manzil bilan birgalikda so’rovlarni bajarish uchun har bir Internet-provayder tomonidan saqlanadigan muhim ma’lumotni tashkil qiladi. Portlar 0 dan 65 536 gacha o‘zgarib turadi va asosan mashhurlik bo’yicha tartiblanadi[4].

0 dan 1023 gacha bo‘lgan portlar ma’lum port raqamlari bo‘lib, ular Internetdan foydalanish uchun mo‘ljallangan, ammo ular maxsus maqsadlarga ham ega bo‘lishi mumkin. Ular Internet tayinlangan raqamlar boshqarmasi (IANA) tomonidan boshqariladi. Ushbu portlar Apple QuickTime, MSN, SQL xizmatlari va boshqa taniqli tashkilotlar kabi yuqori darajadagi kompaniyalar tomonidan saqlanadi. Portni skanerlash uchun ishlatiladigan umumiy protokollar TCP (uzatishni boshqarish protokoli) va UDP (foydalanuvchi ma’lumotlari protokoli). Ularning ikkalasi ham internet uchun ma’lumotlarni uzatish usullari, ammo turli mexanizmlarga ega.



2-rasm. TCP skanerlash texnikasining umumiy ko‘rinishi

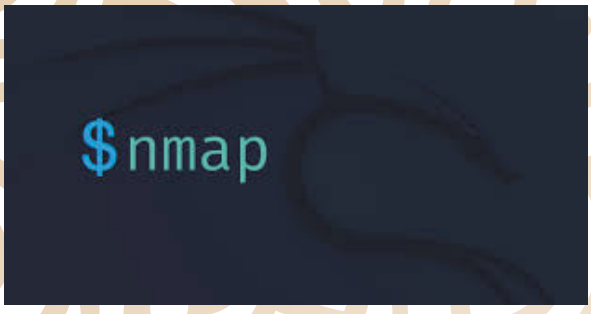
NULL, FIN va Xmas skanerlari TCP sarlavhalari bayroqlarini manipulyatsiya qilishni o‘z ichiga olgan uchta skanerlash turidir. Ularning har biri yopiq portdan RST (yoki ICMP portiga erishib bo‘lmaydigan) paketga olib keladi va ochiq yoki filtrlangan portdan javob yo‘q va ular SYN, RST va ACK bitlari o‘rnatilmaganligini talab qiladi.

NULL skanerlari: sarlavhalarida hech qanday bayroq o‘rnatilmagan paketlarni yuboradi. FIN skanerlarida esa faqat FIN bitlari o‘rnatilgan. Rojdestvo skanerlash paketlari, ularning sarlavhalari “Rojdestvo daraxti kabi yoritilishini” eslatgani uchun shunday deb ataladi, FIN, PSH va URG bayroq bitlari yoqilgan.

Ping skanerlari: eng oddiy port skanerlari ping skanerlari deb ataladi. Tarmoqda ping tarmoq ma’lumotlar paketini IP manzilga xatosiz tarqatish yoki tarqatmaslikni tekshirish uchun ishlatiladi. Ping skanerlari Internetni boshqarish xabar protokoli (ICMP) so‘rovlari bo‘lib, javob berish uchun turli serverlarga bir nechta ICMP so‘rovlarining avtomatlashtirilgan portlashini yuboradi. AT ma’murlari ushbu texnikadan muammolarni bartaraf etish yoki xavfsizlik devori yordamida ping skanerlashni o‘chirish uchun foydalanishi mumkin, bu esa tajovuzkorlarning tarmoqni ping orqali topishini imkonsiz qilib qo‘yadi.

XMAS skanerlari: XMAS skanerlari xavfsizlik devorlari tomonidan yanada jim va kamroq seziladi. FIN paketlari ko‘pincha xavfsizlik devorlari tomonidan e’tiborga olinmaydi, chunki SYN paketlari birinchi navbatda qidiriladi. Shu sababli, XMAS skanerlari hech qanday javob kutmasdan, barcha bayroqlar, shu jumladan FIN bilan paketlarni yuboradi, bu port ochiqligini bildiradi. Agar port yopiq bo‘lsa, RST javobi olinadi. XMAS skanerlash monitoring jurnallarida kamdan-kam uchraydi va tarmoq himoyasi va xavfsizlik devori haqida ma’lumot olishning oddiy usuli hisoblanadi.

Nmap - bu maqsadli tizim/tarmoqni faol sanash uchun xavfsizlik sohasida foydalaniladigan xavfsizlikni tekshirish vositasi. Bu tarmoq ma’murlari va aksincha tajovuzkorlar tomonidan razvedka (sanoqlash) uchun eng ko‘p qo‘llaniladigan vositalardan biri hisoblanadi. Nmap maqsadli tarmoqni faol xostlar (xost kashfiyoti), portni skanerlash, operatsion tizimni aniqlash, versiya tafsilotlari va ishlayotgan hostlarda ishlaydigan faol xizmatlarni faol tekshirish uchun ishlatiladi. Buning uchun Nmap paketlarni yuborish va javoblarni tahlil qilish texnikasidan foydalanadi[3, 4]. Portni skanerlash Nmapning xususiyatlaridan biri bo‘lib, unda vosita tarmoqdagi faol xostlardagi portlarning holatini aniqlaydi. Portlarning holati ochiq, filtrlangan yoki yopiq bo‘lishi mumkin.



3-rasm. Nmap tarmoqli xavfsizlikni tekshirish oynasi

Nmap (“Tarmoq xaritasi”) bepul va ochiq manbadir. Tarmoqni aniqlash va xavfsizlik auditi uchun yordamchi dastur. Ko‘pgina tizimlar va tarmoq ma’murlari uni tarmoq inventarizatsiyasi, xizmatlarni yangilash jadvallarini boshqarish va xost yoki xizmat vaqtini kuzatish kabi vazifalar uchun ham foydali hisoblanadi. Nmap tarmoqda qanday xostlar mavjudligini, ushbu xostlar qanday xizmatlarni (dastur nomi va versiyasini), ular qanday operatsion tizimlar (va OT versiyalari) ishlayotganini, qanday paket filtrlari/xavfsizlik devori turini aniqlash uchun yangi usullarda xom IP-paketlardan foydalanadi. U katta tarmoqlarni tezkorlikda skanerlash uchun mo‘ljallangan, lekin bitta xostlarga nisbatan yaxshi ishlaydi. Nmap barcha asosiy kompyuter operatsion tizimlarida ishlaydi va rasmiy ikkilik paketlar Linux, Windows va Mac OS X uchun mavjud. Klassik buyruq qatori Nmap bajariladigan faylga qo‘shimcha ravishda, Zenmap), moslashuvchan ma’lumotlarni uzatish, qayta yo‘naltirish va disk raskadrovka vositasi (Ncat), skanerlash natijalarini taqqoslash uchun yordamchi dastur (Ndiff) va paketlarni yaratish va javoblarni tahlil qilish vositasi(Nping) hisoblanadi[1, 3].

Xulosa qilib aytadigan bo‘lsak yuqorida keltirib o‘tilganlar, skanerlash portlarning holatini aniqlashga, unga bo‘ladigan xujumlarni va xavf xatarlarni oldini olishga yaqindan yordam beradi. Turli xil pinglar berish orqali jarayonlarni tahlil qilishni amalga oshirish ham yahshi natija beradi.

FOYDALANILGAN ADABIYOTLAR

1. Nigmatov X. Axborot xavfsizligi. O‘quv qo‘llanma. Fan va texnologiyalar nashriyot-matbaa bosmaxonasi. Toshkent. 2021. – 174 b.
2. Ganiyev S.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. – T.: “Fan va texnologiya”, 2017, 372 b.
3. Вострецова Е.В. Основи информационной безопасности учебное пособие для студентов вузов / .- Екатеринбург : Изд-во Урал. ун-та, 2019. – 204 с.
4. Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Информационная безопасность: Учебное пособие. Нижний Новгород: Нижегородский госуниверситет им. Н.И.Лобачевского, 2017. – 198 с.