ISNN 3030-3907

2026/4
VOLUME 3

DEVELOPMENT OF SCIENCE

ILMIY JURNAL



Development of science

Ilmiy jurnal

2026/4 VOLUME 3

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Асадова Раъно Дилмуратовна
Тошкент Давлат техника университети доценти

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

AXBOROT XAVFSIZLIGIDA NMAP VOSITASIDAN SAMARALI FOYDALANISH USULLARI

Maxmatqulov Tuychi Oqil o‘g‘li
“Mirzo Ulug‘bek” nomidagi O‘zbekiston Milliy Universiteti magistranti
E-mail: tuychimaxmatqulov@gmail.com

Annotatsiya. Ushbu maqolada komputer tarmog‘i xavfsizligi tahlil jarayonida Nmap vositasidan foydalanish usullari ko‘riladi. Tadqiqotda tarmoqdagi ishlab turgan qurilmalarni topish, ochiq portlarni topish, xizmatlarning versiyalarini hamda operatsion tizim(OS)ni aniqlash imkoniyatlari ko‘riladi. Nmap vositasining komputer tarmog‘i xavfsizligidagi muhimligi yoritilib, uni samarali qo‘llash usullari sinab ko‘riladi. Ushbu jarayon Ubuntu(Linux) muhitida amalda sinalgan tarmoq skaner qilish tajribalariga asoslanadi.

Kalit so‘zlar: axborot xavfsizligi, Nmap, port skanerlash, komputer tarmog‘i , kiberxavfsizlik.

Аннотация. В данной статье рассматриваются вопросы использования инструмента Nmap для анализа сетевой инфраструктуры в процессе обеспечения информационной безопасности. В исследовании анализируются возможности обнаружения активных узлов сети, сканирования открытых портов, определения версий сервисов и операционных систем. Освещается практическое значение Nmap при оценке уровня безопасности сети и описываются эффективные методы его применения. Исследование основано на экспериментах по сканированию сети в среде Ubuntu.

Ключевые слова: информационная безопасность, Nmap, сканирование портов, анализ сети, кибербезопасность.

Abstract. This article examines the use of the Nmap tool for analyzing network infrastructure in the context of information security. The study analyzes methods for detecting active hosts, scanning open ports, identifying service versions, and determining operating systems. The practical importance of Nmap in assessing network security and effective approaches to its use are discussed. The research is based on network scanning experiments conducted in an Ubuntu environment.

Keywords: information security, Nmap, port scanning, network analysis, cybersecurity.

KIRISH.

Axborot texnologiyalarining tez rivojlanishi va ko‘payishi kompyuter tarmoqlari va internet dunyoda barcha sohalarida o‘zining muhimligini mustahkamlab bormoqda. Tarmoqli tizimlar ko‘p foydalanishi axborot almashinuv jarayonini tezligini oshirdi va turli xil xavfsizlik tahdidlarining ko‘payishiga ham

ISSN 3030-3907

sabab bo‘lmoqda. Shuning uchun axborotlarni xavfsiz saqlash, tarmoqdagi zaif nuqtalarni topish va ularni himoyalash muhim vazifadir. [1]

Axborot xavfsizligini ta’minlash jarayonida tarmoq tekshirish va kuzatib borish muhim ahamiyatga ega. Tarmoqdagi faol qurilmalar, ochiq portlar, ishlayotgan xizmatlar hamda operatsion tizimlar haqida aniq ma’lumot olish tizim administratorlari va axborot xavfsizligi mutaxassislari uchun zarur hisoblanadi. Ushbu ma’lumotlarni aniqlash yordamida tarmoqdagi ehtimoliy xavf manbalari aniqlanadi va xavfsizlik siyosatini samarali shakllantirish imkoniyati yaratiladi. [2]

Tarmoqni tahlil qilish va skanerlash jarayonida keng qo‘llaniladigan vositalardan biri **Nmap (Network Mapper)** hisoblanadi. Nmap bu ochiq manbali tarmoq skaneri bo‘lib, u tarmoqdagi qurilmalarni aniqlash, portlarni skanerlash, xizmatlarni topish hamda operatsion tizimlarni aniqlash imkoniyatini beradi. Bu vosita axborot xavfsizligi mutaxassislari, tizim administratorlari va tarmoq muhandislari tomonidan tarmoq infratuzilmasini tahlil qilish hamda xavfsizlik darajasini baholashda keng qo‘llaniladi. [3]

Nmap vositasining samarasi uning keng ko‘lamli skanerlash usullarini borligi, o‘zgaruvchan konfiguratsiya imkoniyatlari va skriptlar orqali ishlay olish qobiliyatiga ega ekanligi bilan izohlanadi. [4] Ushbu imkoniyatlar orqali axborot xavfsizligi mutaxassisi tarmoq infratuzilmasi haqida batafsil ma’lumotga ega bo‘lishi, ehtimoliy zaifliklarni aniqlashi va xavfsizlikni mustahkamlash bo‘yicha kerakli choralarni ko‘rishi mumkin. [5]

Tadqiqotning obyekti sifatida LAN komputer tarmog‘i va ularning xavfsizlik holati tanlangan bo‘lsa, tadqiqot predmeti sifatida esa tarmoqni tahlil qilish va diagnostika qilish jarayonida Nmap vositasidan foydalanish usullari qaraladi. Tadqiqot jarayonida tarmoqni skanerlash, portlarni aniqlash, xizmatlarni identifikatsiya qilish hamda tizim haqida ma’lumot yig‘ish usullari o‘rganiladi.

METODOLOGIYA.

Bu tadqiqotda ishida komputer tarmog‘ini tahlil qilish hamda uning xavfsizligini baholash davomida Nmap (Network Mapper) vositasidan foydalanish usullari o‘rganildi. Tadqiqot jarayonida nazariy tahlil, amaliy sinov hamda tarmoq skanerlash usullaridan foydalanildi. Ushbu metodlar yordamida Nmap dasturining tarmoqdagi qurilmalarni aniqlash, ochiq portlarni topish, xizmatlarni identifikatsiya qilish hamda operatsion tizimni aniqlash imkoniyatlari tahlil qilindi.

Tadqiqotning amaliy qismi kichik lokal tarmoq muhitida olib borildi. Sinov jarayonida bir nechta kompyuter qurilmalari va tarmoq xizmatlariga ega bo‘lgan test muhiti tashkil etildi. Tadqiqot muhitida Linux operatsion tizimi o‘rnatilgan kompyuter asosiy tahlil vositasi bo‘lib xizmat qildi. Mazkur tizimda Nmap dasturi

ISSN 3030-3907

o‘rnatilib, tarmoqdagi qurilmalar va xizmatlarni aniqlash uchun har xil skanerlash usullari qo‘llanildi.

Tadqiqot davomida Nmap dasturining bir nechta asosiy funksiyalaridan foydalanildi. Jumladan, tarmoqdagi faol qurilmalarni aniqlash uchun host discovery usuli qo‘llanildi. Ushbu usul orqali tarmoq segmentida faol holatda ishlayotgan qurilmalar aniqlanib, ularning IP manzillari ro‘yxati shakllantirildi. Shundan so‘ng aniqlangan qurilmalarda ochiq portlarni aniqlash maqsadida port skanerlash usullari amalga oshirildi.

Portlarni aniqlash davomida turli xil skanerlash metodlari qo‘llanildi. Jumladan, TCP SYN skanerlash, TCP Connect skanerlash hamda UDP port skanerlash usullari orqali tarmoq xizmatlari tekshirildi. Ushbu metodlar yordamida tarmoqdagi xizmatlarning holati, ochiq yoki yopiq portlar hamda filtrlangan portlar aniqlanib, ularning xavfsizlik nuqtai nazaridan bahosi berildi.

Tarmoqdagi xizmatlarni yanayam chuqurroq tahlil qilish uchun Nmap dasturining service version detection funksiyasidan foydalanildi. Ushbu funksiya yordamida ochiq portlarda ishlayotgan xizmatlarning turi hamda versiyasi aniqlanib, potensial zaifliklar mavjudligini baholash imkoniyati yaratildi. Shuningdek, operatsion tizimni aniqlash maqsadida OS detection funksiyasi ham qo‘llanildi. Bu usul orqali tarmoqdagi qurilmalarning operatsion tizimi haqida taxminiy ma’lumotlar olindi.

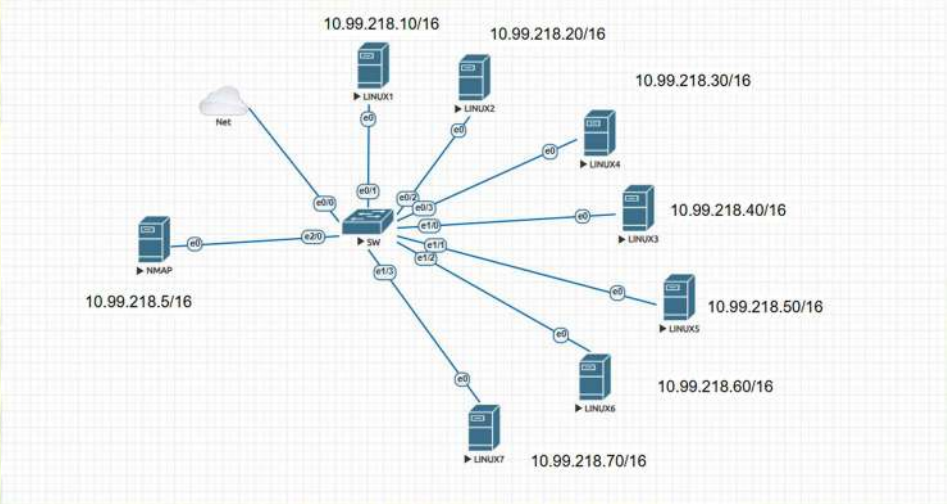
Olingan natijalar tahlil qilinib, tarmoqdagi qurilmalar, ochiq portlar, xizmatlar va ularning xavfsizlik holati haqida umumiy xulosalar chiqarildi. Tadqiqot natijalari Nmap vositasidan foydalanish orqali tarmoq infratuzilmasini samarali tahlil qilish hamda axborot xavfsizligini mustahkamlash mumkinligini ko‘rsatdi. Mazkur metodologiya tarmoq administratorlari hamda axborot xavfsizligi mutaxassislari uchun tarmoqni monitoring qilish va potensial tahdidlarni aniqlashda amaliy ahamiyatga ega.

RESULTS.

ISSN 3030-3907

1. LAN topologiya
2. ip/tarmoq oralig'i tanlash
3. faol qurilmalarni aniqlash
4. Portni skanerlash
5. OSni aniqlash
6. Xizmat va versiyalarni aniqlash
7. Skanerlash natijalari formati

Natijalarni olish ketma-ketligi



1-rasm. Nmap yordamida tarmoq skanerlash uchun yaratilgan laboratoriya topologiyasi

Laboratoriya topologiyasi bir nechta Linux serverlardan iborat bo‘lib, har bir host alohida IP manzilga ega. Nmap o‘rnatilgan tizim ushbu hostlarga nisbatan tarmoq skanerlashni amalga oshiradi.

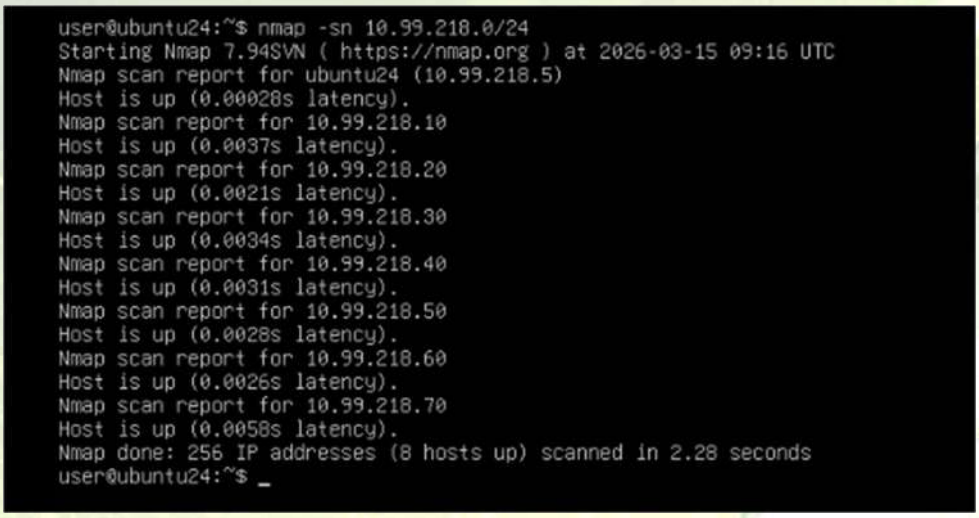
Host discovery natijalari

Tarmoqdagi faol qurilmalarni aniqlash uchun Nmap vositasining host discovery funksiyasidan foydalanildi.

Buyruq:nmap -sn 10.99.218.0/24

Natijada 10.99.218.0/24 tarmoq segmentida jami 8 ta faol host aniqlangan. Skanerlash jarayonida har bir host uchun tarmoq kechikish vaqti (latency) ham qayd etildi. Bu ko‘rsatkich tarmoqdagi qurilmalar bilan aloqa tezligini baholash imkonini beradi.

ISSN 3030-3907

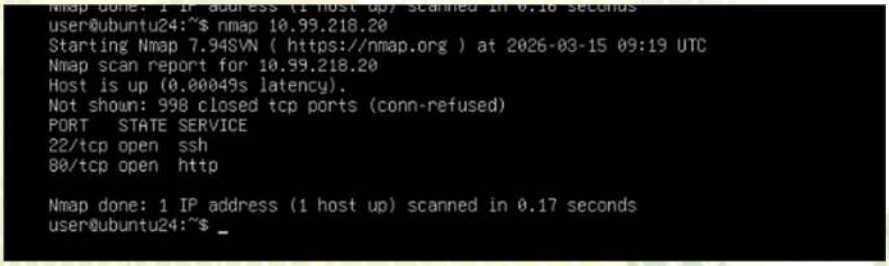


2-rasm. Nmap yordamida tarmoqdagi faol hostlarni aniqlash natijasi

Olingan natijalar tarmoq segmentida faol qurilmalarni tezkor aniqlashda Nmap vositasi samarali ishlashini ko‘rsatdi.

Port scanning natijalari

Keyingi bosqichda aniqlangan hostlarda ochiq portlarni aniqlash uchun port skanerlash amalga oshirildi.



3-rasm. 10.99.218.20 hostida port skanerlash natijasi

Mazkur hostda ikki xil xizmat faol ekanligi aniqlandi:

22-port — SSH

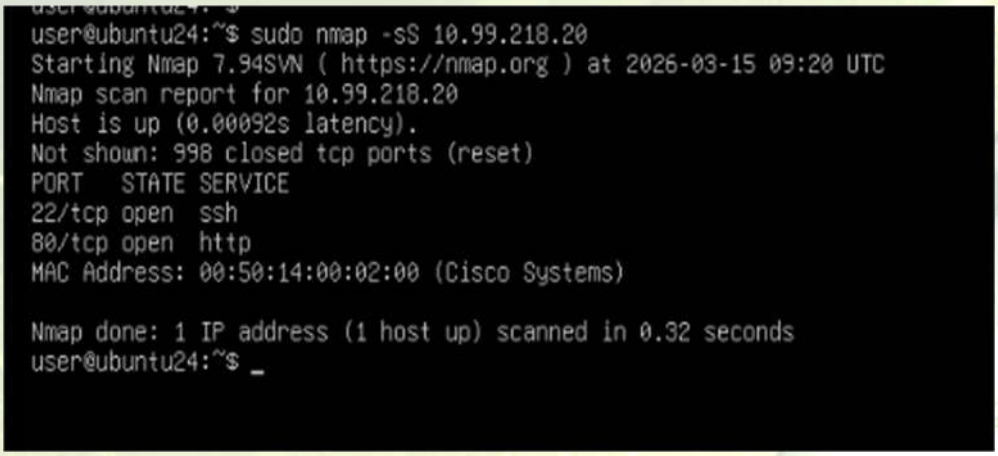
80-port — HTTP

Bu hostda veb server xizmati ishlayotganligini ko‘rsatadi.

SYN scanning natijalari

Tarmoqni yanada chuqurroq tahlil qilish uchun TCP SYN scanning usuli qo‘llanildi.

ISSN 3030-3907

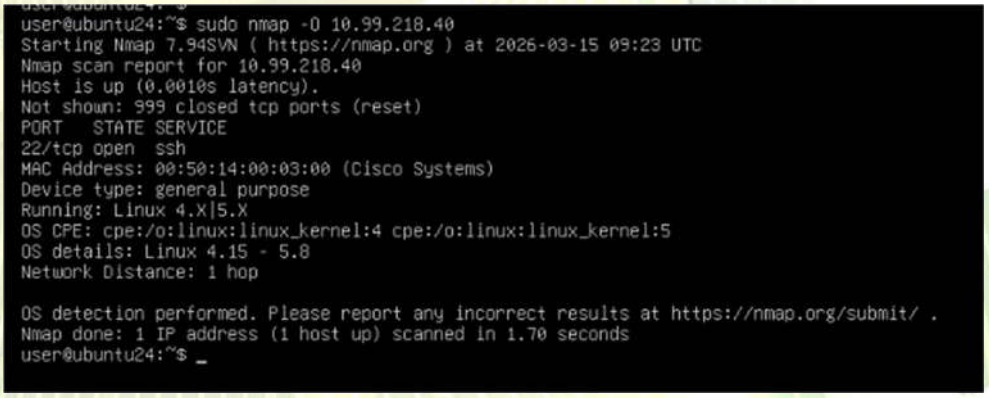


4-rasm. SYN scan yordamida ochiq portlarni aniqlash natijasi

Mazkur usul orqali portlarni tez va nisbatan yashirin tarzda aniqlash mumkinligi kuzatildi. SYN scan yordamida ham 10.99.218.20 hostida 22 va 80 portlar ochiq ekanligi tasdiqlandi.

Operatsion tizimni aniqlash

Nmap vositasi yordamida tarmoqdagi qurilmalarning operatsion tizimi ham aniqlanishi mumkin.



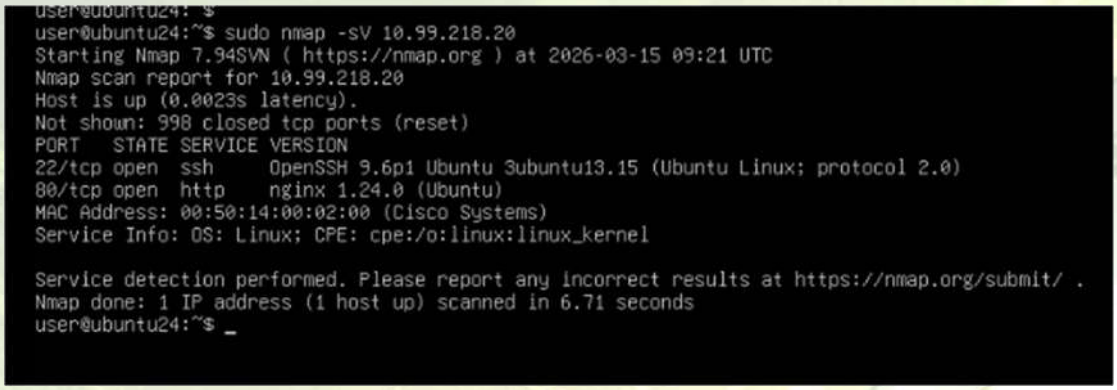
5-rasm. Nmap yordamida operatsion tizimni aniqlash natijasi

Natijalarga ko‘ra tarmoqdagi hostlarda Linux operatsion tizimi ishlayotganligi aniqlangan. Shuningdek, tizim yadrosi versiyasi Linux 4.15 – 5.8 oralig‘ida ekanligi taxmin qilingan.

Service detection natijalari

Nmap dasturining -sV parametri yordamida xizmatlarning aniq versiyalari aniqlanadi.

ISSN 3030-3907

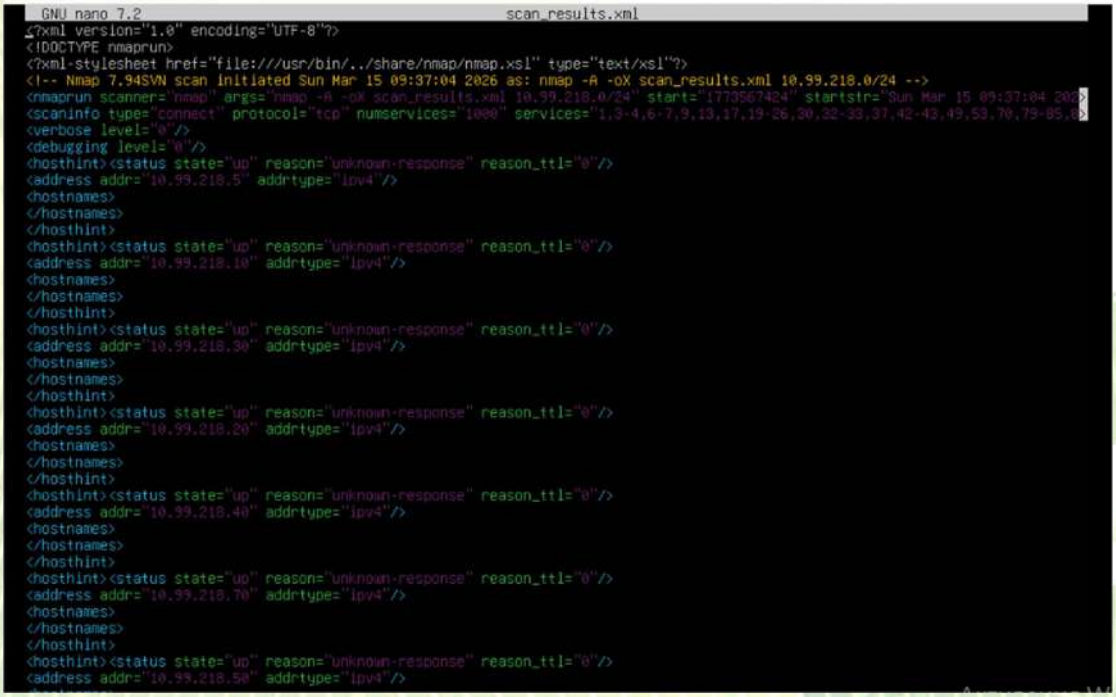


6-rasm. Xizmatlar versiyasini aniqlash natijasi

Natijalarga ko‘ra:SSH xizmati — OpenSSH 9.6p1 va HTTP xizmati — nginx 1.24.0 versiyalari ishlayotganligi aniqlangan.

Natijalarni saqlash

Nmap vositasi yordamida olingan skanerlash natijalari XML formatida ham saqlanishi mumkin.



7-rasm. Nmap skanerlash natijalarini XML formatda saqlash

Bu format keyinchalik avtomatlashtirilgan tahlil vositalarida foydalanish uchun qulay hisoblanadi.

DISCUSSION (MUHOKAMA)

Ushbu ishdada Nmap vositasidan foydalanib laboratoriya tarmog‘ining xavfsizlik holati o‘rganildi. O‘tkazilgan skanerlash natijalariga ko‘ra, tarmoqdagi 10.99.218.0/24 ip diapazonida bir nechta faol hostlar aniqlangan. Host discovery natijalari komputer tarmog‘ida sakkizta faol qurilma borligini aniqladi. Bu Nmap vositasining tarmoq qurilmalarini aniqlash jarayonida tezkor va samarali ekanligini isbotlaydi.

ISSN 3030-3907

Portni skaner qilish davomidaida topilgan natijalar tarmoqdagi xizmatlarning qanday konfiguratsiya qilinganligi haqida muhim ma’lumotlar berdi. Masalan, 10.99.218.10 hostida faqat 22-port (SSH) ochiq ekanligi aniqlangan bo‘lsa, 10.99.218.20 hostida esa 22-port (SSH) va 80-port (HTTP) portlar ochiq ekanligi kuzatildi. Bu holat tarmoqdagi hostning amaliy vazifalari har xil ekanligini bildirdi. SSH xizmati masofadan ulanib so‘ngra boshqarish uchun ishlatilsa, HTTP xizmati esa veb server faoliyatini qo‘llab quvvatlash uchun ishlatiladi.

Service detection natijalari ham tarmoqni ko‘proq o‘rganish imkonini yaratdi. Nmap vositasining -sV qo‘shimcha optioni bilan 10.99.218.20 hostida ishlayotgan xizmatlarning versiyalari aniqlanib, OpenSSH 9.6p1 hamda nginx 1.24.0 server xizmatlari mavjudligi aniqlandi. Xizmat versiyalarini aniqlash axborot xavfsizligi jihatidan muhim topilmadir, chunki ko‘plab kiberhujumlar aynan eski yoki zaif versiyadagi dasturiy xizmatlardan foydalanish orqali amalga oshiriladi. [6]

Operatsion tizimni aniqlash bo‘yicha o‘tkazilgan skanerlash natijalari ham muhim ma’lumotlarni taqdim etdi. 10.99.218.40 hostida o‘tkazilgan OS detection bilan ushbu tizimda Linux operatsion tizimi ishlayotganligi aniqlandi. Shu bilan birga tizim yadrosi versiyasi Linux 4.15–5.8 oralig‘ida ekanligi taxmin qilingan. Bu ma’lumotlar tarmoq muhitining umumiy konfiguratsiyasini tushunish hamda xavfsizlik strategiyasini ishlab chiqishda muhim ahamiyatga ega.

SYN scandan foydalanib olingan natijalar port skaner qilishning yanada samarali amalga oshirilishini ko‘rsatdi. [7] SYN scanning ayniqsa katta tarmoqlarni tahlil qilish jarayonida samarali hisoblanadi. Ushbu usul tarmoqdagi ochiq portlarni tez aniqlash imkonini beradi va tarmoqdagi xizmatlar haqida aniq ma’lumot olishga yordam beradi.

Shu bilan bir qatorda, tadqiqot natijalari Nmap vositasi yordamida olingan skanerlash ma’lumotlarini turli formatlarda saqlash mumkinligini ham ko‘rsatdi. XML formatida saqlangan natijalar keyinchalik boshqa tahlil vositalari yordamida qayta ko‘rib chiqilishi yoki kuzatuvlarni avtomatlashtirishda qo‘llanishi mumkin. [8]

XULOSA.

Mazkur tadqiqot natijalari shuni ko‘rsatdiki, Nmap vositasi tarmoq infratuzilmasini tahlil qilish va axborot xavfsizligini ta’minlashda samarali va qulay vositalardan biri hisoblanadi. Uning yordamida tarmoqdagi faol qurilmalarni aniqlash, ochiq portlar va xizmatlar holatini baholash hamda potensial zaifliklarni o‘z vaqtida aniqlash mumkin.

Tadqiqot davomida olingan natijalar asosida Nmap’dan to‘g‘ri va ehtiyotkorlik bilan foydalanish tarmoq xavfsizligini oshirish, tizimlarni monitoring

ISSN 3030-3907

qilish va kiberxavfsizlik tahdidlarini kamaytirishda muhim ahamiyatga ega ekanligi aniqlandi.

ADABIYOTLAR RO‘YXATI

1. R. A, 3.Advanced network scanning //American Journal of Engineering Research (AJER). – 2016. – T. 5. – №. 6. – C. 38-42..
2. R. S. Jetty S., Securing network infrastructure: discover practical network security with Nmap and Nessus 7. – Packt Publishing Ltd, 2019..
3. P. B. Orebaugh A., Pinkard B. Nmap in the enterprise: your guide to network scanning. – Elsevier, 2011..
4. C. P, Nmap Network Exploration and Security Auditing Cookbook: Network discovery and security scanning at your fingertips. – Packt Publishing Ltd, 2021
5. L. R, “Nmap network scan performance optimisation //fourth international conference on signal processing and computer science (SPCS 2023). – SPIE, 2023. – T. 12970. – C.”.
6. C. A. S., 6.Practical Network Scanning: Capture network vulnerabilities using standard tools such as Nmap and Nessus. – Packt Publishing Ltd, 2018..
7. M. Shah, “Penetration testing active reconnaissance phase–optimized port scanning with nmap tool //2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET). – IEEE, 2019. – C.”.
8. J. S, 5.Network scanning cookbook: Practical network security using Nmap and Nessus 7. – Packt Publishing Ltd, 2018..

ISSN 3030-3907