NMAP SKRIPTLARIDAN FOYDALANISH (NSE)

Sobirjonov Behzod .Q
FarDu Axborot texnologiyalari kafedrasi o‘qituvchisi
behzodbekqahramonovich@gmail.com
Ismoilova Gulhayot Rustamjon qizi
FarDu Axborot tizimlari va texnologiyalari yo‘nalishi
2-kurs talabasi
gulhayotismoilova620@gmail.com
To’xtasinova Mahbuba Akmaljon qizi
FarDu Axborot tizimlari va texnologiyalari yo‘nalishi
2-kurs talabasi
m.tohtasinova@icloud.com
https://doi.org/10.5281/zenodo.20081791

Annotatsiya: Ushbu maqolada Nmap dasturining imkoniyatlari, ayniqsa Nmap Scripting Engine (NSE) texnologiyasi batafsil tahlil qilinadi. NSE yordamida tarmoqni skanerlash jarayonlarini avtomatlashtirish, zaifliklarni aniqlash, xizmatlarni identifikatsiya qilish va tarmoqni chuqur tahlil qilish imkoniyatlari yoritiladi. Maqolada NSE skriptlarining asosiy turlari, jumladan aniqlash, autentifikatsiya, brute-force va ekspluatatsiya skriptlari hamda ularning kiberxavfsizlikdagi amaliy qo‘llanilishi ko‘rib chiqiladi. Shuningdek, skriptlarni ishga tushirish sintaksisi, tayyor skript kutubxonalaridan foydalanish va foydalanuvchi skriptlarini yaratish asoslari bayon etiladi. Tadqiqotda NSE texnologiyasining tarmoq xavfsizligini baholash va penetratsion test jarayonlarini samarali tashkil etishdagi ahamiyati ta’kidlanadi.

Kalit so‘zlar: Nmap, NSE, tarmoqni skanerlash, kiberxavfsizlik, zaifliklarni aniqlash, skriptlash, penetratsion test, tarmoq xavfsizligi, avtomatlashtirish, portlarni skanerlar;

Аннотация: В данной статье рассматриваются возможности инструмента Nmap с акцентом на технологию Nmap Scripting Engine (NSE). Показано, как NSE расширяет функциональность сетевого сканирования за счёт автоматизации процессов обнаружения уязвимостей, идентификации сервисов и глубокого анализа сети. В работе анализируются основные категории NSE-скриптов, включая скрипты обнаружения, аутентификации, перебора паролей и эксплуатации, а также их практическое применение в области кибербезопасности. Кроме того, рассматриваются синтаксис запуска скриптов, использование встроенных библиотек и основы разработки пользовательских скриптов. Подчёркивается значимость NSE для повышения эффективности оценки безопасности сетей и проведения тестирования на проникновение.

Ключевые слова: Nmap, NSE, сетевое сканирование, кибербезопасность, обнаружение уязвимостей, скрипты, тестирование на проникновение, сетевая безопасность, автоматизация, сканирование портов

Annotation: This article examines the capabilities of the Nmap tool, with particular emphasis on the Nmap Scripting Engine (NSE). It highlights how NSE enhances network scanning through automation of tasks such as vulnerability detection, service identification, and in-depth network analysis. The study reviews the main categories of NSE scripts, including discovery, authentication, brute-force, and exploitation scripts, and analyzes their practical applications in cybersecurity. Additionally, the article discusses script execution syntax, the use

of built-in script libraries, and the fundamentals of developing custom scripts. The importance of NSE in improving the efficiency of network security assessment and penetration testing is emphasized.

Keywords: Nmap, NSE, network scanning, cybersecurity, vulnerability detection, scripting, penetration testing, network security, automation, port scanning

Kirish

Zamonaviy axborot texnologiyalari jadal rivojlanib borayotgan sharoitda tarmoq xavfsizligini ta’minlash dolzarb masalalardan biriga aylanib bormoqda. Internet va lokal tarmoqlarning kengayishi, shuningdek, turli xil kiberxavf va hujumlarning ortib borishi natijasida axborot tizimlarini himoyalashning samarali usullarini ishlab chiqish muhim ahamiyat kasb etmoqda. Shu nuqtai nazardan, tarmoqlarni skanerlash, ularni tahlil qilish va mavjud zaifliklarni aniqlash jarayonlari kiberxavfsizlikning asosiy tarkibiy qismlaridan biri hisoblanadi. Tarmoq infratuzilmasini o‘rganish va monitoring qilishda keng qo‘llaniladigan vositalardan biri bu Nmap dasturidir. Mazkur dastur yordamida tarmoqdagi qurilmalar, ochiq portlar, xizmatlar va operatsion tizimlar haqida batafsil ma’lumot olish mumkin. Shu bilan birga, Nmap Scripting Engine (NSE) texnologiyasi Nmap funksional imkoniyatlarini yanada kengaytirib, foydalanuvchilarga avtomatlashtirilgan skriptlar orqali murakkab tahlil va tekshiruvlarni amalga oshirish imkonini beradi. NSE yordamida nafaqat oddiy skanerlash, balki zaifliklarni aniqlash, autentifikatsiya jarayonlarini tekshirish, tarmoq xizmatlarini chuqur tahlil qilish va hatto ayrim turdagi ekspluatatsiya sinovlarini o‘tkazish mumkin. Bu esa uni nafaqat tarmoq administratorlari, balki axborot xavfsizligi mutaxassislari va penetratsion test o‘tkazuvchilar uchun ham muhim vositaga aylantiradi. Mazkur ishning asosiy maqsadi — Nmap Scripting Engine imkoniyatlarini ilmiy jihatdan tahlil qilish, uning skriptlash mexanizmlarini o‘rganish hamda tarmoq xavfsizligini ta’minlashdagi amaliy ahamiyatini yoritishdan iborat. Shu bilan birga, NSE skriptlarining turlari, ularni qo‘llash usullari va samaradorligi ham ko‘rib chiqiladi.

Asosiy qism. Nmap dasturi tarmoq infratuzilmasini tahlil qilish va xavfsizlik darajasini baholashda keng qo‘llaniladigan samarali vositalardan biri hisoblanadi. Ushbu dastur nafaqat ochiq portlarni aniqlash, balki tarmoqdagi xizmatlar va qurilmalar haqida batafsil ma’lumot to‘plash imkonini beradi. Ayniqsa, uning tarkibiy qismi bo‘lgan Nmap Scripting Engine (NSE) texnologiyasi orqali foydalanuvchilar tarmoqni yanada chuqur va avtomatlashtirilgan tarzda tekshirish imkoniyatiga ega bo‘ladilar. NSE tizimi Lua dasturlash tiliga asoslangan bo‘lib, skriptlar yordamida turli xil tekshiruvlarni amalga oshirishni ta’minlaydi. NSE skriptlari funksional jihatdan bir necha toifalarga bo‘linadi va har bir toifa ma’lum bir vazifani bajarishga qaratilgan. Jumladan, aniqlash (discovery) skriptlari tarmoqdagi faol qurilmalar va xizmatlarni topishga yordam beradi, autentifikatsiya skriptlari esa tizimga kirish jarayonlarining ishonchliligini tekshiradi. Brute-force skriptlari parollarni tanlash orqali himoya darajasini baholasa, zaifliklarni aniqlovchi (vuln) skriptlar tizimdagi mavjud kamchiliklarni aniqlashga xizmat qiladi. Bundan tashqari, ekspluatatsiya skriptlari aniqlangan zaifliklardan foydalanish imkoniyatlarini sinovdan o‘tkazadi. Shu orqali foydalanuvchi tarmoq xavfsizligi holatini kompleks ravishda baholashi mumkin. Nmap Scripting Engine skriptlaridan foydalanish maxsus buyruqlar yordamida amalga oshiriladi. Foydalanuvchi kerakli skriptlarni tanlab, ularni ma’lum parametrlar asosida ishga tushirishi mumkin. Bu esa tarmoqni tekshirish jarayonini aniq maqsadga yo‘naltirish va ortiqcha yuklamalarni kamaytirishga yordam beradi.

Shu bilan birga, skriptlarga qo‘shimcha argumentlar berish orqali ularning ishlash jarayonini moslashtirish imkoniyati ham mavjud.

Xulosa

Xulosa qilib aytganda, Nmap dasturi zamonaviy tarmoq xavfsizligini ta’minlashda muhim o‘rin tutadi va uning tarkibiy qismi bo‘lgan Nmap Scripting Engine (NSE) texnologiyasi ushbu jarayonni yanada samarali va avtomatlashtirilgan holga keltiradi. NSE yordamida oddiy port skanerlashdan tashqari, tizimdagi zaifliklarni aniqlash, xizmatlarni chuqur tahlil qilish hamda xavfsizlik darajasini kompleks baholash imkoniyati yaratiladi. Mazkur tadqiqot davomida NSE skriptlarining asosiy turlari, ularning ishlash prinsiplari va amaliy qo‘llanilish jihatlari ko‘rib chiqildi. Shuningdek, tayyor skriptlardan foydalanish bilan bir qatorda, foydalanuvchi tomonidan yangi skriptlar yaratish imkoniyati mavjudligi ushbu texnologiyaning moslashuvchanligini oshirishi ta’kidlandi. Natijada, Nmap Scripting Engine tarmoq xavfsizligini baholash va penetratsion test jarayonlarini takomillashtirishda samarali vosita ekanligi aniqlandi. Shu bilan birga, undan foydalanishda axborot xavfsizligi talablari va etik me’yorlarga qat’iy rioya qilish zarurligi muhim omil sifatida qayd etiladi.

Adabiyotlar, References, Литературы:

1. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. *Axborot xavfsizligi asoslari*. Toshkent, 2020.
2. Toshkent axborot texnologiyalari universiteti. *Kompyuter tarmoqlari va xavfsizligi fanidan o‘quv qo‘llanma*. Toshkent, 2021.
3. O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi. *Kiberxavfsizlik asoslari*. Toshkent, 2022.
4. Kiberxavfsizlik bo‘yicha o‘quv-uslubiy majmua. Toshkent, 2021.
5. Kompyuter tarmoqlari fanidan darslik. Toshkent, 2019.