INNOVATIVE WORLD
Ilmiy tadqiqotlar markazi

YANGI RENESSANS

ILMIY JURNALI

2026/4

+998335668868
www.innoworld.net

Google Scholar
doi
zenodo
OpenAIRE

YANGI RENESSANS

ILMIY JURNALI
TO'PLAMI

3 - JILD, 4 - SON
2026

www.innoworld.net

O'ZBEKISTON-2026

Nmap skriptlari (NSE) yordamida tarmoq xavfsizligini skanerlash va avtomatlashtirish mexanizmlari

Behzod Sobirjonov Qahramonivich
FarDu Axborot tehnologiyalari
kafedrasi o‘qituvchisi
behzodbekqahramonovich@gmail.com
Husanova Shahloxon Zokirjon qizi
FarDu Axborot tizimlari va texnologiyalari
yo‘nalishi 2-bosqich talabasi
shahloxon821@gmail.com
Telefon raqam:91-677-63-06

ANNOTATSIYA

Ushbu maqolada tarmoq xavfsizligini tekshirishda eng samarali vositalardan biri bo‘lgan Nmap Scripting Engine (NSE) imkoniyatlari tadqiq etiladi. Maqolada NSE skriptlarining tuzilishi, ularning turlari va tarmoqdagi zaifliklarni aniqlashda qo‘llanilish strategiyalari tahlil qilingan. Shuningdek, Lua dasturlash tili asosida skriptlarni avtomatlashtirish orqali kiberxavfsizlik darajasini oshirish bo‘yicha amaliy tavsiyalar berilgan.

Kalit so‘zlar: Nmap, NSE, Kiberxavfsizlik, Skript, Tarmoq xavfsizligi, Lua, Zaifliklarni skanerlash, Portla(NSE), одного из наиболее эффективных инструментов проверки сетевой rni skanerlash.

АННОТАЦИЯ

В данной статье исследуются возможности Nmap Scripting Engine безопасности. В статье анализируется структура скриптов NSE, их типы и стратегии использования для обнаружения сетевых уязвимостей. Также даны практические рекомендации по повышению уровня кибербезопасности за счет автоматизации скриптов на базе языка программирования Lua.

Ключевые слова: Nmap, NSE, Кибербезопасность, Скрипт, Сетевая безопасность, Lua, Сканирование уязвимостей, Сканирование портов.

ANNOTATION

This article examines the capabilities of the Nmap Scripting Engine (NSE), one of the most effective tools for network security auditing. The article analyzes the structure of NSE scripts, their categories, and strategies for using them to detect network vulnerabilities. It also provides practical recommendations for enhancing cybersecurity by automating scripts based on the Lua programming language.

Keywords: Nmap, NSE, Cybersecurity, Script, Network Security, Lua, Vulnerability Scanning, Port Scanning.

Zamonaviy axborot texnologiyalari rivojlangan davrda tarmoq infratuzilmasini himoya qilish har qanday tashkilot uchun ustuvor vazifa hisoblanadi. Texnik tizimlar murakkablashgani sayin, kiberjinoyatchilarning hujum usullari ham takomillashib bormoqda. Tarmoqdagi ochiq portlarni aniqlash, servislar versiyasini tekshirish va yashirin zaifliklarni topishda Nmap (Network

Mapper) dasturi jahon miqyosida yetakchi o‘rinni egallaydi. Nmap dasturining eng kuchli komponenti — bu Nmap Scripting Engine (NSE) bo‘lib, u foydalanuvchilarga standart

Kirish

skanerlash jarayonlarini avtomatlashtirish va kengaytirish imkonini beradi.

1. NSE (Nmap Scripting Engine) arxitekturasi

NSE — bu Nmap’ning moslashuvchanligini ta’minlovchi tizim bo‘lib, u Lua dasturlash tili asosida ishlaydi. NSE yordamida foydalanuvchilar o‘zlarining maxsus vazifalarini bajaruvchi skriptlarini yaratishlari mumkin.

Mexanizmi: Skriptlar Nmap skanerlashning turli bosqichlarida (portlarni aniqlashdan keyin yoki hostlar tekshirilayotgan vaqtda) ishga tushadi. Bu tizim ma’lumotlar almashinuvi tezligini oshiradi va murakkab tarmoq vazifalarini oddiy buyruqlar yordamida bajarishga imkon beradi.

2. NSE skriptlarining kategoriyalari

NSE skriptlari ularning vazifasi va xavfsizlik darajasiga ko‘ra bir nechta asosiy guruhlarga bo‘linadi:

Safe (Xavfsiz): Tarmoq ishiga salbiy ta’sir ko‘rsatmaydigan, faqat ma’lumot yig‘ishga qaratilgan skriptlar.

Discovery (Aniqlash): Tarmoqdagi xizmatlar, qurilmalar va ochiq resurslar haqida batafsil ma’lumot to‘playdi.

Vulnerability (Zaiflik): Ma’lum bir tizimdagi xavfsizlik bo‘shliqlarini (masalan, CVE bazasidagi zaifliklar) qidiradi.

Exploit (Eksploit): Tizimdagi zaiflikni amalda tekshirish yoki unga hujum qilish uchun ishlatiladi.

Brute (Brutforce): Turli servislarning (SSH, FTP, Telnet) parollarini tanlash orqali buzishga harakat qiladi.

3. Amaliy qo‘llanilish strategiyalari

NSE yordamida kiberxavfsizlik bo‘yicha mutaxassislar quyidagi amallarni bajara oladilar:

Versiya aniqligini oshirish: Standart skanerlash aniqlay olmagan servis versiyalarini chuqur tahlil qilish.

Web-serverlar tahlili: HTTP sarlavhalarini tekshirish, yashirin papkalarni (directory bruteforce) aniqlash.

Baza ma'lumotlarini tekshirish: MySQL, MSSQL yoki Oracle bazalarida xavfsiz bo‘lmagan sozlamalarni topish.

Zararli dasturlarni aniqlash: Ba'zi skriptlar tarmoqdagi qurilmalarda ma'lum bo'lgan virus yoki "backdoor"larning mavjudligini tekshirishga mo‘ljallangan.

4. NSE yordamida himoya strategiyalari

Faqatgina skanerlash kifoya qilmaydi, olingan natijalarga ko‘ra quyidagi himoya choralarini ko‘rish zarur:

Muntazam skanerlash: Tarmoqdagi yangi paydo bo‘lgan zaifliklarni aniqlash uchun NSE skriptlarini vaqtinchalik (schedule) asosda ishga tushirish.

Xizmatlarni cheklash: Zarur bo‘lmagan yoki NSE orqali zaifligi aniqlangan portlarni zudlik bilan yopish.

Versiyalarni yangilash: NSE tomonidan aniqlangan eski versiyadagi dasturiy ta'minotlarni yangilash.

Xulosa

Nmap Scripting Engine (NSE) — bu kiberxavfsizlik sohasidagi eng kuchli va ko‘p qirrali vositalardan biridir. U oddiy tarmoq xaritasini chizishdan tortib, murakkab zaifliklarni aniqlashgacha bo‘lgan vazifalarni avtomatlashtiradi. Raqamli makonda xavfsizlikni ta'minlash uchun administratorlar va xavfsizlik mutaxassislari NSE imkoniyatlaridan unumli foydalanishlari, o‘z tarmoqlarini hujumchilardan oldinroq skanerlab, kamchiliklarni bartaraf etishlari shart.

Foydalanilgan adabiyotlar:

Lyon, G. F. (2009). Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure.Com LLC.

Calderon, R. P. (2015). Nmap 6: Cookbook. Packt Publishing.

Schneier, B. (2018). Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. Norton & Company.

SANS Institute. (2026). Network Security Assessment and NSE Implementation Guide.

Nmap Official Documentation. (2026). Nmap Scripting Engine (NSE) usage and development.