METASPLOITDA POST-EXPLOITATION MODULLARIDA FOYDALANISH

Behzod Sobirjonov
Ilmiy rahbar Farg‘ona davlat universiteti
Axborot texnologiyalari kafedrasi dotsenti, PhD
behzodbekqahramonovich@gmail.com
Xolmatov Rustam Vohidjon o‘g‘li
Muallif. Farg‘ona davlat universiteti
Axborot tizimlari va texnologiyalari yo‘nalishi talabasi
xolmamatovrustam5@gmail.com
https://doi.org/10.5281/zenodo.20066107

Annotatsiya. Ushbu maqolada Metasploit Framework muhitida post-exploitation modullaridan foydalanishning nazariy va amaliy jihatlari yoritilgan. Tizimga dastlabki kirishdan so‘ng amalga oshiriladigan jarayonlar, ya’ni ma’lumot yig‘ish, foydalanuvchi huquqlarini oshirish, tizimni nazorat qilish va tarmoq ichida harakatlanish bosqichlari tahlil qilingan. Shuningdek, post-exploitation jarayonida qo‘llaniladigan asosiy modullar va ularning imkoniyatlari ko‘rib chiqilgan. Maqola axborot xavfsizligi sohasida bilimlarni kengaytirishga qaratilgan.

Kalit so‘zlar: Metasploit, post-exploitation, penetration testing, privilege escalation, payload, session, axborot xavfsizligi, tarmoq, ekspluatatsiya

Аннотация

В данной статье рассматриваются теоретические и практические аспекты использования модулей post-exploitation в среде Metasploit Framework. Анализируются процессы, выполняемые после первоначального доступа к системе, включая сбор информации, повышение привилегий и контроль над системой. Также описываются основные модули и их функциональные возможности.

Ключевые слова: Metasploit, post-exploitation, тестирование на проникновение, повышение привилегий, безопасность, сеть, эксплуатация

Annotation

This article discusses the theoretical and practical aspects of using post-exploitation modules in the Metasploit Framework environment. It analyzes processes performed after initial system access, including information gathering, privilege escalation, and system control. The main modules and their capabilities are also reviewed.

Keywords: Metasploit, post-exploitation, penetration testing, privilege escalation, payload, session, security, network, exploitation

Metasploitda post-exploitation modullaridan foydalanish

Axborot xavfsizligi sohasida penetration testing jarayonlari muhim ahamiyat kasb etadi. Ushbu jarayon bir necha bosqichlardan iborat bo‘lib, ulardan eng muhimlaridan biri post-exploitation bosqichidir. Bu bosqich tizimga muvaffaqiyatli kirish amalga oshirilgandan so‘ng bajariladi va hujumchiga tizim ustidan kengroq nazorat o‘rnatish imkonini beradi.Metasploit Framework penetration testing uchun eng keng tarqalgan vositalardan biri hisoblanadi. Ushbu platforma orqali nafaqat ekspluatatsiya amalga oshiriladi, balki tizimga kirilgandan keyingi faoliyat — ya’ni post-exploitation jarayonlari ham bajariladi. Post-exploitation modullari tizim haqida qo‘shimcha ma’lumot olish, foydalanuvchi huquqlarini kengaytirish va boshqa tizimlarga o‘tish imkonini beradi.

Post-exploitation jarayonining asosiy vazifalaridan biri bu tizim haqida maksimal darajada ma’lumot to‘plashdir. Bu jarayonda operatsion tizim versiyasi, foydalanuvchilar ro‘yxati, tarmoq konfiguratsiyasi va ishlayotgan xizmatlar aniqlanadi. Ushbu ma’lumotlar keyingi hujum bosqichlarini rejalashtirishda muhim rol o‘ynaydi.Keyingi muhim bosqich — privilege escalation hisoblanadi. Bu jarayonda oddiy foydalanuvchi huquqlari administrator darajasiga oshiriladi. Metasploitda bu vazifa uchun maxsus modullar mavjud bo‘lib, ular tizimdagi zaifliklardan foydalanadi. Yuqori darajadagi huquqlar hujumchiga tizim ustidan to‘liq nazoratni ta’minlaydi.

Bundan tashqari, post-exploitation modullari orqali tizimda doimiy kirishni saqlab qolish (persistence) imkoniyati mavjud. Bu esa tizim qayta ishga tushirilgan taqdirda ham kirishni yo‘qotmaslikni ta’minlaydi. Shuningdek, hujumchi boshqa qurilmalarga o‘tish (lateral movement) orqali butun tarmoqni nazorat qilishga harakat qiladi.

Metasploit muhitida sessionlar bilan ishlash ham muhim hisoblanadi. Session orqali tizim bilan bevosita aloqa o‘rnatiladi va turli buyruqlar bajariladi. Meterpreter kabi ilg‘or payloadlar esa yanada keng imkoniyatlar yaratadi, jumladan fayllar bilan ishlash, ekran tasvirini olish va klaviatura yozuvlarini kuzatish kabi funksiyalarni taqdim etadi.Post-exploitation jarayoni axborot xavfsizligi mutaxassislari uchun tizimlarning zaif tomonlarini aniqlash va ularni bartaraf etishda muhim vosita hisoblanadi. Shu sababli, ushbu texnologiyalarni o‘rganish nafaqat hujum, balki himoya choralarini kuchaytirishda ham katta ahamiyatga ega.

Xulosa

Metasploitda post-exploitation modullaridan foydalanish penetration testing jarayonining ajralmas qismi hisoblanadi. Ushbu bosqich orqali tizimning ichki holati chuqur tahlil qilinadi va xavfsizlikdagi kamchiliklar aniqlanadi. Post-exploitation usullari tizimlarni himoyalash strategiyalarini ishlab chiqishda muhim rol o‘ynaydi. Kelajakda axborot xavfsizligi sohasining rivojlanishi bilan bunday vositalarning ahamiyati yanada ortib boradi.

Adabiyotlar, References, Литературы:

1. Metasploit Unleashed — Offensive Security
2. Kennedy D., O’Gorman J., Kearns D., Aharoni M. — Metasploit: The Penetration Tester’s Guide
3. OWASP Testing Guide
4. Rapid7 Metasploit Documentation
5. NIST Cybersecurity Guidelines
6. EC-Council Ethical Hacking Materials
7. SANS Institute Security Resources
8. Offensive Security Training Materials