METASPLOITDA POST-EXPLOITATION MODULLARIDAN FOYDALANISH
ИСПОЛЬЗОВАНИЕ МОДУЛЕЙ ПОСТ-ЭКСПЛУАТАЦИИ В METASPLOIT
USING POST-EXPLOITATION MODULES IN METASPLOIT

Sobirjonov Begzod Qahramonivich
FarDu Axborot tehnologiyalari kafedrasi o'qituvchisi
behzodbekqahramonovich@gmail.com
Xolmatova Gulhayoxon Hasanjon qizi
FarDu Axborot tizimlari va tehnologiyalari yo'nalishi 2-bosqich talabasi
xolmatovagulhayo1@gmail.com

Annotatsiya: *Ushbu maqolada Metasploit Framework dasturida post-exploitation modullaridan foydalanish jarayoni yoritiladi. Post-exploitation bosqichi tizimga muvaffaqiyatli kirishdan so'ng amalga oshiriladi va u orqali tizim haqida ma'lumot yig'ish, foydalanuvchi huquqlarini kengaytirish, maxfiy ma'lumotlarni olish hamda tizimda doimiy kirishni ta'minlash imkoniyatlari o'rganiladi. Shuningdek, ushbu modullar yordamida tarmoq faoliyatini kuzatish va tizim xavfsizligini baholash masalalari ko'rib chiqiladi.*

Kalit so'zlar: *Metasploit, post-exploitation, xavfsizlik, tarmoq, huquqni oshirish, ma'lumot yig'ish*

Аннотация: *В данной работе рассматривается использование модулей пост-эксплуатации в Metasploit Framework. Этап пост-эксплуатации выполняется после успешного получения доступа к системе и позволяет собирать информацию о системе, повышать привилегии пользователей, извлекать конфиденциальные данные и обеспечивать постоянный доступ. Также анализируются возможности мониторинга сети и оценки безопасности системы.*

Ключевые слова: *Metasploit, пост-эксплуатация, безопасность, сеть, повышение привилегий, сбор данных*

Annotation: *This paper discusses the use of post-exploitation modules in the Metasploit Framework. The post-exploitation phase is performed after successfully gaining access to a system and enables information gathering, privilege escalation, extraction of sensitive data, and maintaining persistent access. Additionally, the capabilities of network monitoring and system security assessment are analyzed.*

Keywords: *Metasploit, post-exploitation, security, network, privilege escalation, data collection.*

Kirish

Axborot xavfsizligi sohasida tizimlarni himoya qilish va ularning zaif tomonlarini aniqlash muhim ahamiyatga ega. Shu nuqtai nazardan, penetration testing jarayonida turli vositalardan foydalaniladi. Ana shunday kuchli vositalardan biri — Metasploit framework hisoblanadi. Ushbu platforma yordamida nafaqat tizimlarga kirish, balki kirilgandan keyingi jarayonlarni ham samarali boshqarish mumkin. Ayniqsa, post-exploitation modullari tizim ichida chuqurroq tahlil olib borish, ma’lumotlarni yig‘ish va tizimni to‘liq nazorat qilish imkonini beradi. Shu sababli, Metasploitda post-exploitation modullaridan foydalanish masalasi axborot xavfsizligi mutaxassislari uchun dolzarb hisoblanadi.

Metasploitda post-exploitation modullari tizimga muvaffaqiyatli kirilgandan so‘ng ishga tushiriladi. Ularning asosiy vazifasi — tizim haqida qo‘shimcha ma’lumot to‘plash, foydalanuvchi huquqlarini kengaytirish va boshqa qurilmalarga o‘tish imkoniyatlarini aniqlashdan iborat. Bu modullar yordamida operatsion tizim turi, foydalanuvchilar ro‘yxati, tarmoq konfiguratsiyasi va ishlayotgan jarayonlar haqida batafsil ma’lumot olish mumkin.

Post-exploitation modullarining yana bir muhim jihati — privilege escalation imkoniyatidir. Agar dastlabki kirish cheklangan foydalanuvchi huquqlari bilan amalga oshirilgan bo‘lsa, ushbu modullar yordamida administrator darajasiga chiqish mumkin. Bundan tashqari, ular yordamida tizimda yashirin qolish , olish yoki boshqa tizimlarga pivot qilish tarmoq ichida harakatlanish kabi amallarni bajarish mumkin.

Metasploit modullari avtomatlashtirilgan tarzda ishlashi bilan ajralib turadi. Bu esa xavfsizlik mutaxassislariga vaqtni tejash va samaradorlikni oshirish imkonini beradi. To‘g‘ri va ehtiyotkorlik bilan foydalanilganda, ushbu modullar tizim xavfsizligini mustahkamlashda muhim vosita bo‘lib xizmat qiladi.

Xulosa

Metasploit platformasida post-exploitation modullaridan foydalanish kiberxavfsizlik sohasida muhim bosqichlardan biri hisoblanadi. Ushbu modullar orqali tizimga kirilgandan keyin uning ichki holatini chuqur tahlil qilish, mavjud zaifliklarni aniqlash va ularni bartaraf etish bo‘yicha aniq tavsiyalar ishlab chiqish mumkin. Post-exploitation jarayoni nafaqat hujumchi nuqtai nazaridan, balki himoya choralarini kuchaytirish uchun ham katta ahamiyatga ega.

Modullardan foydalanishda qonuniylik va axloqiy me’yorlarga qat’iy rioya qilish zarur. Faqat ruxsat etilgan tizimlarda va test maqsadida qo‘llanilgandagina ular foydali natija beradi. To‘g‘ri yondashuv orqali Metasploit vositalari tashkilotlar axborot xavfsizligini mustahkamlash, tahdidlarga tayyor turish va zamonaviy kiberhujumlarga qarshi samarali himoya tizimini yaratishda muhim o‘rin tutadi.

FOYDALANILGAN ADABIYOTLAR

1. Tomas R. Peltier. Axborot xavfsizligi siyosatlari, jarayonlari va standartlari. Auerbach Publications, 2016.
2. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. Kiberxavfsizlik asoslari bo‘yicha o‘quv qo‘llanma. Toshkent, 2020.
3. ISO/IEC. Axborot xavfsizligini boshqarish tizimlari: ISO/IEC 27001 talablari. 2013.