MICROSOFT THREAT MODELING TOOL DASTURIY VOSITASIDA STRIDE MODELI

Qozoqova To'xtajon Qaxramon qizi
Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti, assistent
qozoqovat1516@gmail.com
https://doi.org/10.5281/zenodo.11526715

ARTICLE INFO

Qabul qilindi: 01-June 2024 yil
Ma'qullandi: 04- June 2024 yil
Nashr qilindi: 08- June 2024 yil

KEYWORDS

STRIDE, Microsoft Threat Modeling Tool, hujum, Linux, spoofing

ABSTRACT

Ushbu maqolada tahdidlarni turlari, tahdidni modellashtirish vositalari, modellashtirish vositalarining tahlili va Microsoft Threat Modeling Tool dasturiy vositasida model yaratish va uni tahlili ketirib o'tildi.

Tahdid deganda kimlarningdir manfaatlariga ziyon yetkazuvchi ro'y berishi mumkin bo'lgan voqea ta'sir, jarayon tushuniladi. Axborotga yoki axborot tizimiga salbiy ta'sir etuvchi potentsial ro'y berishi mumkin bo'lgan voqea yoki jarayon axborot munosabatlari sub'ektlari manfaatlariga qaratilgan tahdid deb yuritiladi.

Insayder tahdidlar tashkilot ichidan kelib chiqadi va qasddan yoki tasodifiy bo'lishi mumkin. Tashkilot tizimlari va ma'lumotlariga ruxsati bo'lgan xodimlar, pudratchilar yoki biznes hamkorlar o'z kirish imkoniyatlaridan qasddan yomon maqsadlarda, masalan, moliyaviy daromad olish yoki tizimlarni sabotaj qilish uchun ma'lumotlarni o'g'irlash uchun foydalanishi mumkin. Tasodifiy insayder tahdidlar xodimlar beixtiyor zarar etkazganda, ko'pincha xavfsizlik siyosati yoki tartib-qoidalarini bilmaslik tufayli yuzaga keladi.

Tashqi tahdidlar tashkilotdan tashqaridan keladi va odatda zararli xarakterga ega. Ularga individual xakerlardan tortib uyushgan kiberjinoyatlar sindikatlari va milliy davlatlargacha bo'lgan keng doiradagi aktyorlar kiradi. Umumiy tashqi tahdidlarga quyidagilar kiradi:

Hackerlar turli sabablarga ko'ra tizimlarga ruxsatsiz kirish huquqiga ega bo'lgan shaxslar, jumladan moliyaviy daromad, josuslik yoki obro'sizlik.

Kiberjinoyatchilar to'lov dasturi, fishing yoki ma'lumotlarni o'g'irlash orqali moliyaviy daromad olish uchun kiberjinoyat bilan shug'ullanadigan shaxslar yoki guruhlar.

Zararli dasturiy ta'minot, zararli dasturlarning qisqartmasi, har qanday dasturlashtiriladigan qurilma, xizmat yoki tarmoqqa zarar etkazish yoki ulardan foydalanish uchun mo'ljallangan keng doiradagi dasturlarni o'z ichiga oladi. Zararli dasturlarning keng tarqalgan turlariga quyidagilar kiradi:

Viruslar boshqa kompyuter dasturlarini o'zgartirish va o'z kodlarini kiritish orqali ko'payadigan dasturlar.

Ijtimoiy muhandislik tahdidlari ijtimoiy muhandislik odamlarni oddiy xavfsizlik tartib-qoidalarini buzish uchun manipulyatsiya qilish uchun inson xatti-harakatlaridan foydalanadi. Umumiy ijtimoiy muhandislik taktikalariga quyidagilar kiradi:

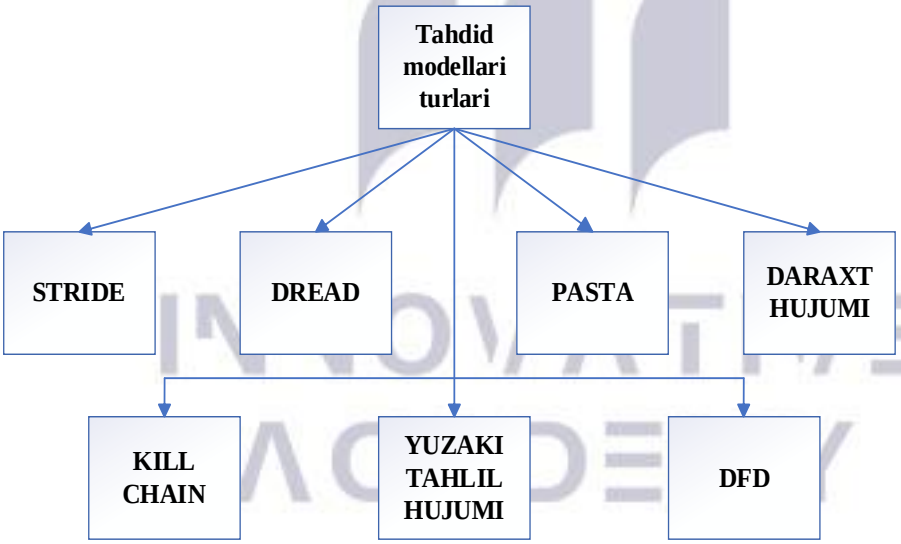
Fishing odamlarni aldash uchun ishonchli manbadan kelgan ko‘rinadigan soxta elektron xatlar yoki xabarlarni yuborish.

Spoofing shaxsni maxfiy ma'lumotlarni oshkor qilishga ishontirish uchun yolg'on skript yaratish.

Denial of Service (DoS) va Distributed Deial of Service (DDoS) hujumlari. DoS va DDoS hujumlari xizmatni bir nechta manbalardan kelgan trafik bilan haddan tashqari yuklash orqali uni mavjud bo'lmagan holga keltirishga qaratilgan. DoS hujumlari odatda bo'lsa-da

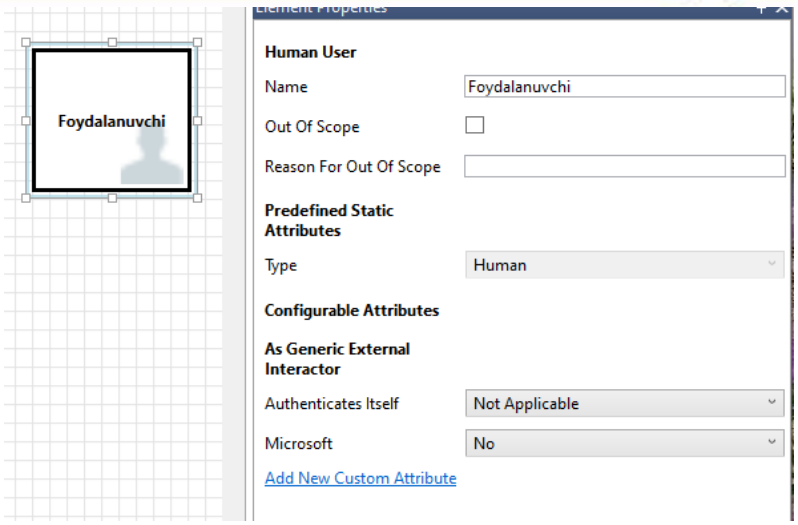
Har xil turdagi tahdidlarni tushunish keng qamrovli xavfsizlik strategiyalarini ishlab chiqish uchun zarurdir. Tashkilotlar ushbu tahdidlar bilan bog'liq xavflarni samarali kamaytirish uchun texnik nazorat, siyosat va foydalanuvchilarni o'qitishni birlashtirgan holda xavfsizlikka qatlamli yondashuvni qo'llashlari kerak.

Axborot xavfsizligi sohasida tahdid modeli - bu axborot tizimining xavfsizligiga potensial tahdidlarni aniqlash, baholash va yumshatish uchun ishlatiladigan tizimli yondashuv. Bu erda tahdid modellarining asosiy komponentlari va turlari.



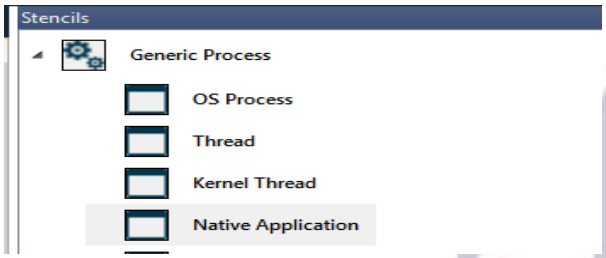
1-rasm. Tahdid modellari turlari

Tahdid modellarini biri bu STRIDE model modeldir ushbu modelni tahdidlarni modellashtirish vositalaridan bir Microsoft Threat Modeling Tool da ko’rib chiqamiz. Microsoft Threat Modeling Tool juda yaxshi bajaradigan vositalardan biri bu xavfsiz dasturiy ta’minotni ishlab chiqish jarayonlari va ishlab chiqish jarayonida xavfsizlik haqida o‘ylash uchun tizimli yondashuvlardir. Linux UID, parol dasturi, foydalanuvchi o‘z parolini o‘rnatish uchun oddiy tahdid modeli yaratildi. Foydalanuvchiga bo‘lishi mumkin bo‘lgan tahdid bu hujumchi tomonidan o‘z parollarini yangi parol va parol buyrug‘I bilan almashtirib qo’yishdir. Threat Modeling Tool da STRIDE modelini tuzish bosqichlari. Birinchi qadamda uskunalar panelida yangi oyna ochiladi va Human User ni qo‘shamiz bunda nomiga o‘zgartirish kiritib Foydalanuvchi deb qayta nomlandi, 2-rasmda shu oyna ko‘rsatilgan.



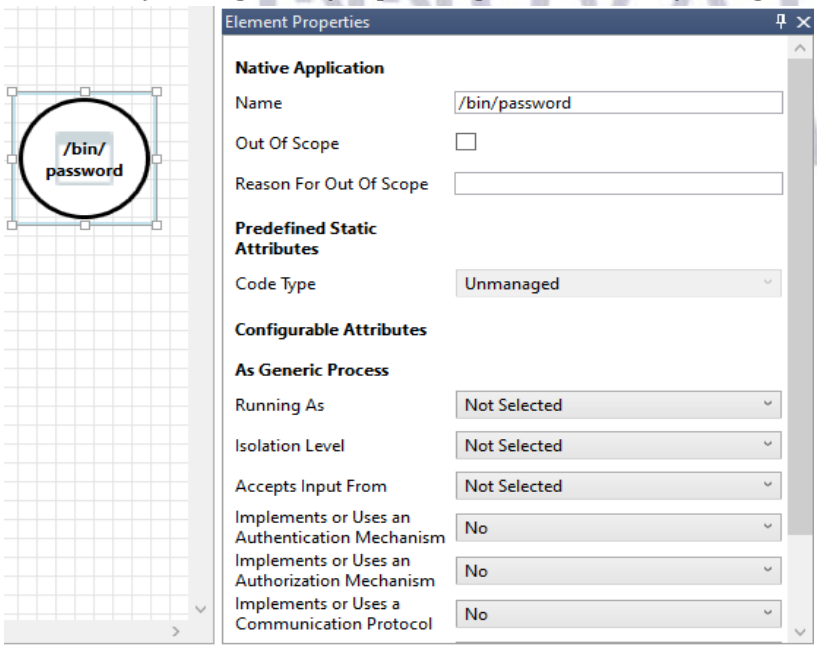
2-rasm. Human Userni qayta nomlash

Keyingi qadamda qilinadigan ish bu STRIDE modeli uchun kerak bo‘ladigan Native Application qo‘shish bu jarayaon 3- rasmda keltirilgan.



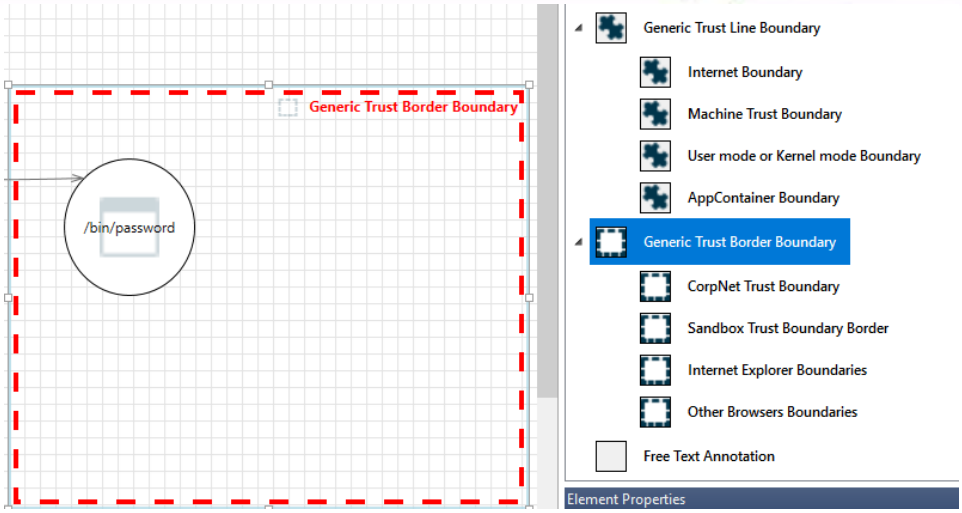
3-rasm. Native Application qo‘shish

4- rasmda Native Application /bin/password ga o‘zgartirildi. Ushbu oynada bir nechta bo‘limlar mavjud jumladan oldindan belgilangan statik atributlar (Predefined Static Attributes) konfiguratsiya qilinadigan atributlar (Configurable Attributes).

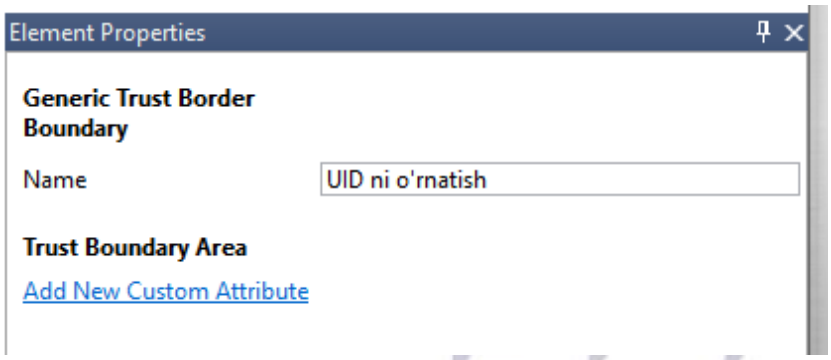


4-rasm. Native applicationni qayta nomlash

Modelni attributlarini bir biriga bog‘laymiz Genetic data flow yordamida ular o‘zaro bog‘landi va Genetic Trust Border Boundary attributi qo‘shiladi. Ushbu bosqich 4-rasmda ko‘rsatilib o‘tilgan.

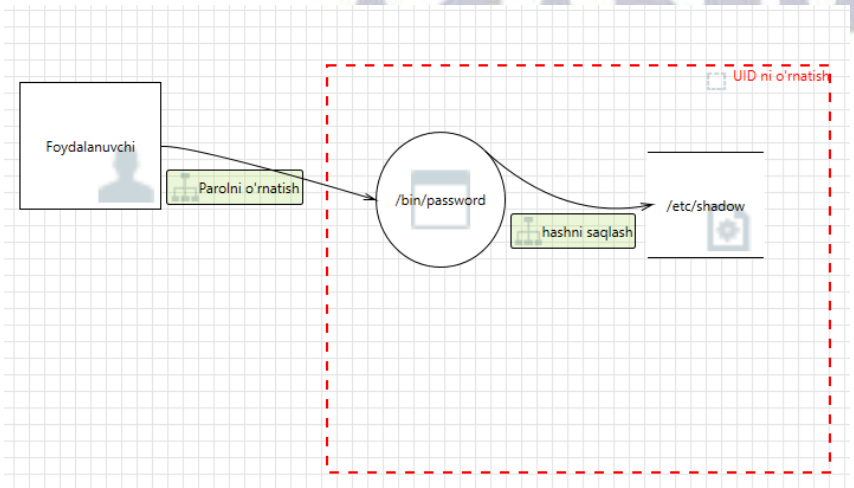


5-rasm. Genetic trust border boundary atributi qo‘shilishi



6-rasm. Genetic trust border boundary attributi qayta nomlash

Element Properties oynasida File system ushbu oynada qayta nomlandi. Atributni konfiguratsiyasini to‘g‘rilash oynasi mavjud bunda fayl tizimini turlarini o‘zgartirish mumkin bo‘ladi. Tayyorlangan tahdid modeli uskunalar panelidan View dan Analysis View orqali yaratilgan modeli tahdidlar ro‘yhatini ko‘ramiz. 7-rasmda yaratilgan UID ni paroliga bo‘lishi mumkin bo‘lgan tahdid modeli yaratildi va ushbu rasmda ko‘rsatilgan model hosil bo‘ldi.



7-rasm. Tahdid modeli

Hosil qilingan modelda aniqlangan tahdidlarni 8-rasmda ko‘rishimiz mumkin. Jami 12 ta tahdid keltirib o‘tilgan.

Threat List

ID	Diagram	Changed By	Last Modified	State	Title	Category	Description	Justification	Interaction	Priority
0	Diagram 1		Generated	Not Started	Spoofing of De...	Spoofing	/etc/shadow...		hashni saqlash	High
1	Diagram 1		Generated	Not Started	Potential Exces...	Denial Of Servi...	Does /bin/pass...		hashni saqlash	High
2	Diagram 1		Generated	Not Started	Spoofing the /...	Spoofing	/bin/password...		Parolni o'rnatish	High
3	Diagram 1		Generated	Not Started	Spoofing the F...	Spoofing	Foydalanuvchi...		Parolni o'rnatish	High
4	Diagram 1		Generated	Not Started	Potential Lack...	Tampering	Data flowing a...		Parolni o'rnatish	High
5	Diagram 1		Generated	Not Started	Potential Data...	Repudiation	/bin/password...		Parolni o'rnatish	High
6	Diagram 1		Generated	Not Started	Data Flow Sniff...	Information Di...	Data flowing a...		Parolni o'rnatish	High
7	Diagram 1		Generated	Not Started	Potential Proc...	Denial Of Servi...	/bin/password...		Parolni o'rnatish	High
8	Diagram 1		Generated	Not Started	Data Flow Paro...	Denial Of Servi...	An external ag...		Parolni o'rnatish	High
9	Diagram 1		Generated	Not Started	Elevation Usin...	Elevation Of Pr...	/bin/password...		Parolni o'rnatish	High
10	Diagram 1		Generated	Not Started	/bin/password...	Elevation Of Pr...	Foydalanuvchi...		Parolni o'rnatish	High
11	Diagram 1		Generated	Not Started	Elevation by C...	Elevation Of Pr...	An attacker m...		Parolni o'rnatish	High
12	Diagram 1		Generated	Not Started	Cross Site Req...	Elevation Of Pr...	Cross-site requ...		Parolni o'rnatish	High

8-rasm. Aniqlangan tahdidlar ro‘yhati

Diagram1 da ID 1 uchun /bin/password yoki /etc/shadow resurslar sarfini nazorat qilish uchun aniq choralar ko‘rish tavsifi berilgan. Resource consumption hujumlari murakkab bo‘lishi mumkin va ba’zi hollarda OS ishni bajarishiga ruxsat beradi.

Threat Properties

ID: 1 Diagram: Diagram 1 Status: Not Started Last Modified: Generated

Title: Potential Excessive Resource Consumption for /bin/password or /etc/shadow

Category: Denial Of Service

Description: Does /bin/password or /etc/shadow take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification:

Interaction: hashni saqlash

Priority: High

9-rasm. Diagram 1 qatoridagi tahdid tavsifi

9-rasmda Parol /bin/password tajovuzkor tomonidan soxtalashtirilgan bo‘lishi mumkin, bu esa maxfiy ma’lumotlarning oshkor etilishiga olib keladi. Maqsadli jarayonni aniqlash uchun standart autentifikatsiya mexanizmidan foydalanishni ko‘rib chiqish haqida ogohlantirish berilgan.

Threat Properties

ID: 2 Diagram: Diagram 1 Status: Not Started Last Modified: Generated

Title: Spoofing the /bin/password Process

Category: Spoofing

Description: /bin/password may be spoofed by an attacker and this may lead to information disclosure by Foydalanuvchi. Consider using a standard authentication mechanism to identify the destination process.

Justification:

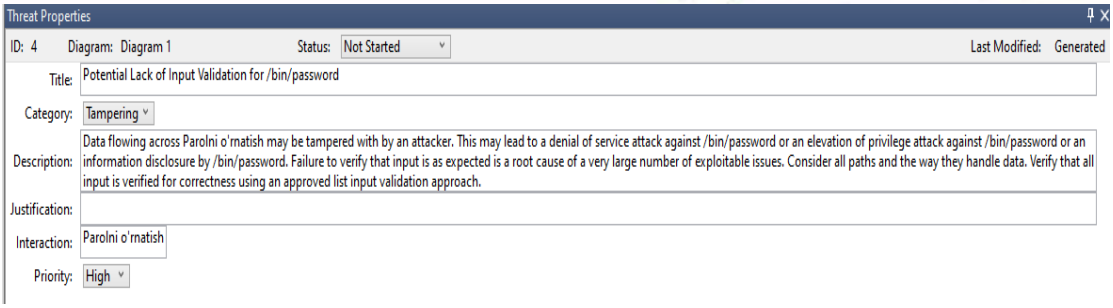
Interaction: Parolni o'rnatish

Priority: High

-10-rasm. ID 2 ustundagi tahdid xususiyatlari

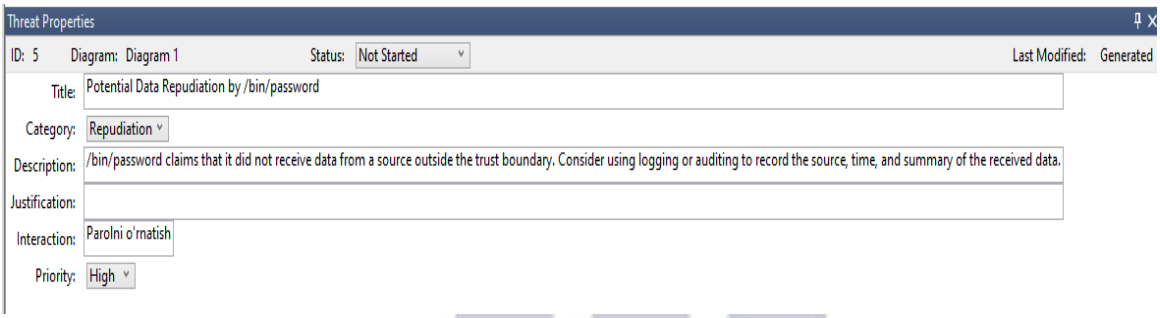
Keyingi tahdidlar tavsiflarida /bin/password ga tajovuzkor tomonidan ruxsatsiz kirishga olib kelishi mumkin deb ogohlantiradi. Tashqi obyektni aniqlash uchun standart autentifikatsiya mexanizmidan foydalanishni ko‘rib chiqish eslatildi.

Parolni o‘rnatish orqali o‘tadigan ma’lumotlar tajovuzkor tomonidan o‘zgartirilishi mumkin. Bu /bin/password-ga xizmat ko‘rsatishni rad etish hujumiga, /bin/password-ga imtiyoz hujumining kuchayishiga /bin/password dagi ma’lumotlarning oshkor etilishiga olib kelishi mumkin. Kirish ma’lumotlarining kutilganlarga mos kelishini tekshirmaslik ko‘p sonli foydalanish mumkin bo‘lgan muammolarning asosiy sababidir. Barcha yo‘llarni va ma’lumotlarni qanday qayta ishlashni ko‘rib chiqish tavsiya etildi. Tasdiqlangan ro‘yxatga kirishni tekshirish usulidan foydalangan holda barcha kiritilgan ma’lumotlarning to‘g‘riligi tekshirilganligiga ishonch hosil qilinadi.



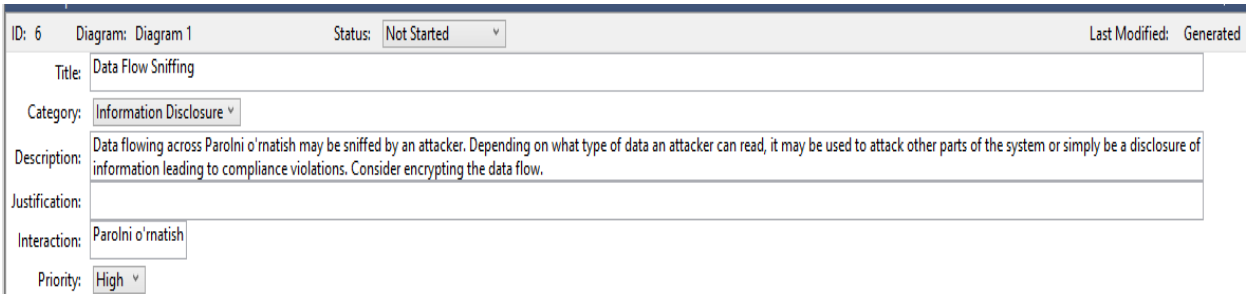
11 -rasm ID 4 ustundagi tahdid xususiyatlari

/bin/password ishonch chegarasidan tashqaridagi manbadan ma'lumotlarni olmaganligini bildiradi. Qabul qilingan ma'lumotlarning manbasini, vaqtini va xulosasini yozib olish uchun jurnal yoki auditdan foydalanishni o'ylab ko'rish tavsiya etiladi.



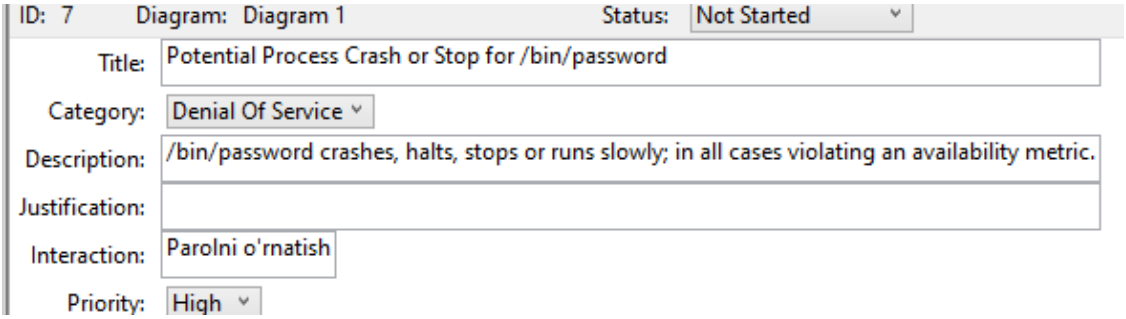
12 -rasm. ID 5 ustundagi tahdid xususiyatlari

Parolni o'rnatish orqali o'tayotgan ma'lumotlar tajovuzkor tomonidan to'xtatilishi mumkin. Buzg'unchi o'qiy oladigan ma'lumotlar turiga qarab, u tizimning boshqa qismlariga hujum qilish yoki oddiygina ma'lumotni oshkor qilish uchun ishlatilishi mumkin, bu esa tartibga solish buzilishiga olib keladi. Ma'lumotlar oqimini shifrlash tavsiya etiladi.



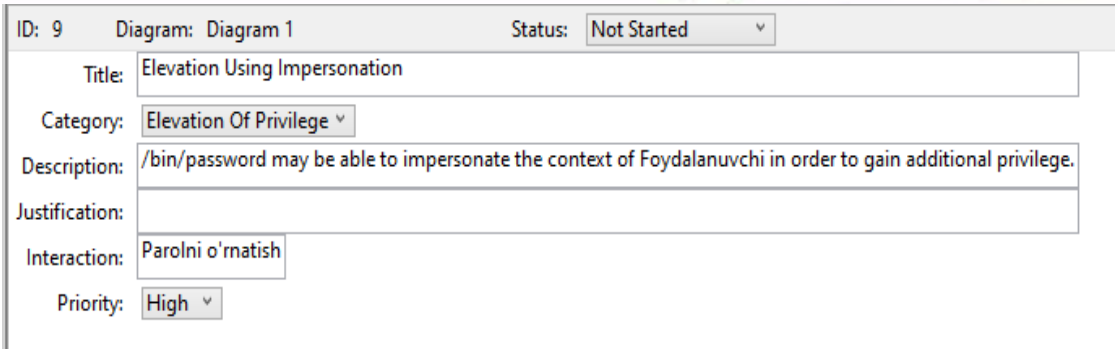
13-rasm. ID 6 ustundagi tahdid xususiyatlari

/bin/parol ishdan chiqadi, to'xtaydi yoki sekinlashadi, barcha hollarda mavjudlik ko'rsatkichi buziladi.



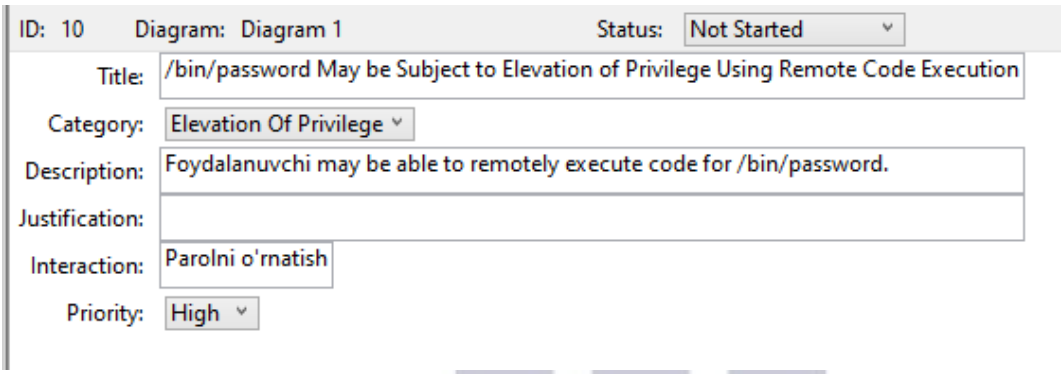
14-rasm. ID 7 ustundagi tahdid xususiyatlari

Buzg'unchi istalgan yo'nalishda ishonch chegarasi bo'ylab ma'lumotlarni uzatishni to'xtatadi. /bin/password qo'shimcha imtiyozlarga ega bo'lish uchun samarali kontekstni taqlid qilishi mumkin.



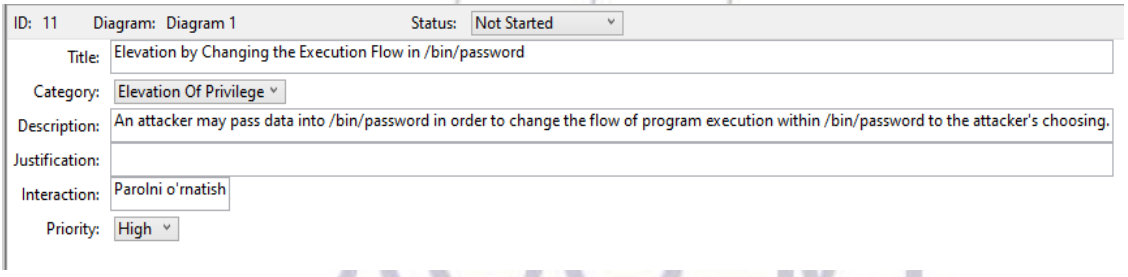
15-rasm. ID 9 ustundagi tahdid xususiyatlari

/bin/password da parolga masofadan turib o‘zgartishish mumkin.



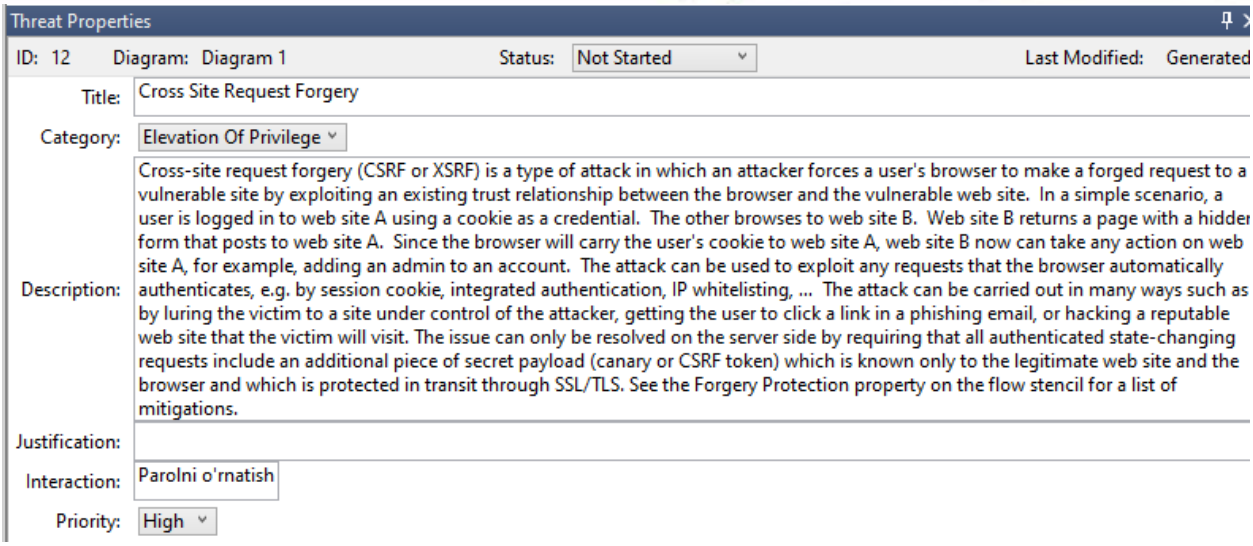
16-rasm. ID 10 ustundagi tahdid xususiyatlari

Buzg‘unchi o‘z xohishiga ko‘ra /bin/password dagi dastur oqimini o‘zgartirish uchun ma’lumotlarni /bin/password ga o‘tkazishi mumkin.



17-rasm. ID 11 ustundagi tahdid xususiyatlari

Saytlararo so‘rovlarni qalbakilashtirish (CSRF yoki XSRF) hujumning bir turi bo‘lib, buzg‘unchi foydalanuvchi brauzeriga soxta so‘rov yuborish orqali brauzer va sayt o‘rtasidagi mavjud bog‘lanishdan foydalanadi. Foydalanuvchi A saytiga cookie faylidan hisob qaydnomasi sifatida kiradi. U B saytiga o‘tadi. B sayti A saytiga xabar yuboradigan yashirin shaklga ega sahifani qaytaradi. Brauzer foydalanuvchining cookie-faylini A saytiga o‘tkazgani uchun B sayti endi A saytida istalgan amalni qo‘shishi mumkin. Hujum brauzer tomonidan avtomatik tarzda tasdiqlanadigan har qanday so‘rovlar uchun ishlatilishi mumkin, masalan seans cookie-fayllari, integratsiyalangan autentifikatsiya va ruxsat etilgan IPlar ro‘yhati. Hujum turli usullar bilan amalga oshirilishi mumkin, masalan, jabrlanuvchini boshqariladigan saytga jalb qilish. Buzg‘unchi foydalanuvchini elektron pochtasiga yuborilgan fishing uchun havolaga kirishga yoki foydalanuvchi tashrif buyuradigan veb-saytni buzishga majbur qiladi. Bu muammoni server tomonida hal qilish mumkin, buning uchun barcha autentifikatsiya qilingan holatni o‘zgartirish so‘rovlari faqat qonuniy veb-sayt va brauzerga ma’lum bo‘lgan va SSL/TLS orqali uzatilganda himoyalangan qo‘shimcha maxfiylik qo‘shishni talab qiladi.



18-rasm. ID 12 ustundagi tahdid xususiyatlari

Buzg‘unchi /etc/shadow-ni aldashi mumkin, bu ma’lumotlar /etc/shadow-ga emas, balki Buzg‘unchining maqsadli manziliga yozilishiga olib keladi. Maqsadli ma’lumotlar omborini aniqlash uchun standart autentifikatsiya mexanizmidan foydalanish talab etiladi.

Xulosa o’rnida shuni aytish joizki axborot xavfsizligida tahdidlarni modellashtirish vositalari, aksar "tahdid modellashtirish" deb ataladi, bu muhim va murakkab birlashuvli vositalar majmuasi, xavfsizlik va boshqa muhim infratuzilmalar bilan bog'liq bo'lgan tahdidlarni aniqlash, baholash va boshqarish uchun ishlatiladi. Bu vositalar, odatda, quyidagi xususiyatlarga ega:

Tahdidlarni aniqlash bu vositalar muayyan soha yoki tashkilotga xos tahdidlarni topishda yordam beradi. Ushbu tahdidlar qurilma, tizim yoki xizmatlarning zaifligi, inson xatosi yoki kasbkorlik kiritish kabi ko'plab omillarga bog'liq bo'lishi mumkin.

Baholash tahdidlarni modellashtirish vositalari, shuningdek, tahdidning miqdorini va uning muhimligini baholash imkonini taqdim etadi. Bu, odatda, tahdidning ehtimolini va agar u ruxsat topgan taqdirda, sodir bo'lishi mumkin bo'lgan zarar hajmini hisobga olib, baholangan o'xshashlik indeksi yoki boshqa ko'rsatkichlar orqali amalga oshiriladi.

Biroq, tahdidlarni modellashtirish vositalaridan foydalanishda quyidagi muammo va cheklash uchun o'lchovlar olish kerak:

Muddat va mablag'lar tahdidlarni modellashtirish vositalarini qurish va ulardan foydalanish uchun ko'p vaqt va mablag'lar talab qilinadi. Bu vositalardan samarali foydalanish uchun muhandislik va o'quv talab qilinadi, chunki ular ko'p holatda murakkab bo'lib, muhandislik bilimi talab qiladi. Tahdidlar va zaifliklar doim o'zgarib turadi, shuning uchun bu vositalar doim yangilanib borishi va o'zgaruvchilikka javobgarlik qilishi kerak.

Xulosa qilib aytadigan bo‘lsak, tahdidlarni modellashtirish vositalari, tashkilotning xavfsizligini oshirish va tahdidlarga qarshi samarali qo'llab-quvvatlash choralarini rivojlantirishda muhim rol o'ynaydi. Biroq, bu vositalardan foydalanishda e'tiborli bo'lish va ularga doim yangilanib borish kerak.