უსაფრთხოების მოვლენებზე დაფუძნებული ტიპური ქსელური შეტევების ეტაპებისა და ფაზების ანალიზი

იოსებ ქართველიშვილი, მაია ოხანაშვილი, მიხეილ დარჩაშვილი

საქართველოს ტექნიკური უნივერსიტეტი

s.kartvelishvili@gtu.ge, m.okhanashvili@gtu.ge, misha8003123@gmail.com

რეზიუმე

ნაშრომში წარმოდგენილი და გაანალიზებულია ტიპური ქსელური შეტევების ეტაპები და ფაზები. კომპიუტერულ ქსელებზე წარმატებული შეტევები წარმოადგენს თავდამსხმელის მიერ წინასწარ ჩამოყალიბებული და მომზადებული ქმედებების საკმაოდ რთულ თანმიმდევრობას. თავდასხმის განხორციელება ხშირად მრავალსაფეხურიანი პროცესია, რომელშიც თითოეული ეტაპი საკუთარი მახასიათებლებით ხასიათდება. კომპიუტერული შეტევის „ანატომიის“ შესწავლა გვაძლევს საშუალებას, რომ შევაფასოთ თავდამსხმელის შესაძლებლობები მავნე ქმედებების განხორციელებისას და ასევე ადეკვატური დაცვის სისტემა შევიმუშაოთ.

საკვანძო სიტყვები: შეტევების აღმომჩენი სისტემები. ქსელის დაზვერვა. გამაგრება. კვალის დამალვა. მავნე მიზნების განხორციელება.

1. შესავალი.

მოვლენის შესახებ რაც შეიძლება სრული ინფორმაციის არსებობით ყველაზე სრულყოფილი თავდასხმა შეიძლება გამოვლინდეს. თანამედროვე IDS-ები (Intrusion Detection System) პირველადი ინფორმაციის დამუშავებისას ყველაზე ხშირად აღმოაჩენენ თავდასხმებს გარკვეული ნიშნების არსებობით და თითოეული IDS ამას თავისებურად აკეთებს.

შეიძლება გამოვყოთ თავდასხმის ოთხი ძირითადი ეტაპი:

- ქსელის დაზვერვა;
- გამაგრება;
- კვალის დამალვა;
- მავნე მიზნების განხორციელება.

ეს მიდგომა საკმარისი არ არის სისტემის სრულფასოვანი ფუნქციონირებისთვის თავდასხმების ფაზების დასადგენად, რადგან ისინი არ იძლევიან თავდამსხმელის ქმედებების დაზუსტების საშუალებას. საფრთხეებსა და თავდასხმის ფაზებს შორის ურთიერთობის ანალიზი, რომელიც ხორციელდება თავდამსხმელის მიერ წარმოადგენს მნიშვნელოვან ამოცანას და თავდასხმის არსებობის შესახებ გადაწყვეტილების დროული მიღებისთვის საჭიროა. ასეთი ანალიზი შესაძლებელს ხდის თავიდან ავიცილოთ შედეგების თვალსაზრისით ყველაზე საშიში თავდასხმები, მაგრამ ასევე პირველი და მეორე ტიპის შეტევების ამოცნობისას შევამციროთ შეცდომები.

2. ძირითადი ნაწილი.

შემუშავებული მიდგომის მთავარი იდეას წარმოადგენს ის, რომ ყველაზე საშიშია არა თავდასხმის მოქმედებების იზოლირებული შემთხვევები არამედ დაცულ ქსელზე მიზანმიმართული პროგრესირებადი მოქმედება, თავდასხმის მოქმედებების თანმიმდევრული ნაკრების სახით. ამ შემთხვევაში, მავნე ქმედებების გამოვლენას ემატება ქსელურ მოვლენებსა და შესრულებულ მოქმედებებს შორის ურთიერთობების არაწრფივი ლოგიკური შემოწმება.

იმ ეტაპების რაოდენობის ინტერპრეტაციაზე, რომლებშიც ხორციელდება კომპიუტერის შეტევების უმეტესობა დღემდე არსებობს რამდენიმე მოსაზრება. შეგვიძლია დავეყრდნოთ თავდამსხმელის ტიპური მოქმედებების ქრონოლოგიურ თანმიმდევრობას, დაცულ ინფორმაციასა და გამოთვლით რესურსებს.

ზოგიერთი მკვლევარი კომპიუტერის შეტევის ეტაპებს აჯგუფებს გამოყენებული მეთოდების მიხედვით, ზოგი კი დეტალურად აღწერს თავდასხმის ეტაპებს სივრცითი პოზიციის მიხედვით - თავდასხმის მთელი პროცესის დაყოფით ქსელზე ან კომპიუტერზე განაწილებული ზემოქმედებიდან ლოკალურ შეტევამდე გადასვლის ფაზებად. მავნე ზემოქმედების შესწავლის თვალსაზრისით ქსელის კვანძებზე, ტიპური შეტევის ეტაპების აღწერის ყველაზე სრულყოფილი გზაა ყველა ამ მეთოდის კომბინაციის გამოყენება - ანუ ქრონოლოგიური და ტიპური კლასიფიკაციის გამოყენება.

კომპიუტერულ სისტემებზე თავდასხმებს რაც შეეხება, თავდამსხმელს შეიძლება ჰქონდეს შემდეგი მიზნები, რომლებსაც ის მუდმივად ცდილობს მიუახლოვდეს:

- სისტემაზე ნაწილობრივი ან სრული კონტროლის მოპოვება.
- ინფორმაციაზე წვდომის მოპოვება (კონფიდენციალურობის დარღვევა, არაავტორიზებული მოდიფიკაცია ან წაშლა);
- სისტემის მუშაობის დარღვევა;
- ამავდროულად, შეიძლება ჩამოვთვალოთ იმ საფრთხეების ტიპები, რომლებიც თავდამსხმელს შეუძლია მათი საფრთხის ზრდის მიმდევრობით განახორციელოს:
- არსებული ქსელური სერვისების დაუცველობის იდენტიფიცირების საფრთხე, პაროლების გამოცნობა, ქსელური სერვისების ბანერების შეგროვების შესაძლებლობა;
- ქსელის პროტოკოლების, ღია პორტების ნომრების, ხელმისაწვდომი სერვისების შესახებ ინფორმაციის გამჟღავნების საფრთხე და ქსელის ურთიერთქმედების ქვესისტემის არქიტექტურული დაუცველობის გამოყენება;
- მომსახურებაზე უარის თქმის მუქარა;
- გაყალბების საფრთხეები (ARP spoofing, IP spoofing, DNS spoofing), რაც თავდამსხმელს აძლევს საშუალებას მოიპოვოს დამატებითი ინფორმაცია ან დაარღვიოს ქსელის მუშაობა;
- ქსელის სერვისების ან აპლიკაციის პროგრამული უზრუნველყოფის დანერგვისას მოწყვლადობის გამოყენებით ქსელის კვანძში შეღწევის საფრთხე (სტრიქონების ფორმატის გამოყენება, ბუფერის გადაჭარბების მეთოდები, და ა.შ.);
- ვებზე ორიენტირებულ დაუცველობასთან დაკავშირებული საფრთხეები (XSS, SQL ინექცია, PHP ინტერპრეტატორის დაუცველობა);
- შეღწევისა და ქსელში ყოფნის კვალის დამალვა და გაქრობა;
- ქსელის კვანძზე დამაგრების საფრთხე (კომპიუტერის გადატვირთვის შემდეგ მუშაობის აღდგენის შესაძლებლობა);
- ინფორმაციაზე წვდომის მოპოვების საფრთხეები, მავნე ეფექტების გავრცელება ქსელის სხვა კომპონენტებზე.

თავდამსხმელის ქმედებების ტიპური თანმიმდევრობა შეიძლება დაიყოს ეტაპებად, რომლებიც აღწერილი საფრთხეების თანმიმდევრულ განხორციელებასთანაა დაკავშირებულია. თავდაპირველად თავდამსხმელი ეძებს ინტერნეტში თავდასხმის ობიექტს (ეს შეიძლება იყოს ინდივიდუალური კომპიუტერი, კომპიუტერების ჯგუფი ან მთელი ქსელი). ამისათვის ის სპეციალიზებულ პროგრამულ ინსტრუმენტებს, საჯარო საძიებო სისტემებსა და

დამატებით ინფორმაციას იყენებს, რომლის მიღებაც მას კომპიუტერული ქსელების გარეთ შეუძლია. შეტევის ეს ეტაპი არის პასიური - თავდამსხმელი არ ახორციელებს არანაირ მავნე მოქმედებას.

საჭირო ქსელის გამოვლენის შემდეგ თავდამსხმელი ქსელის აღჭურვილობის პოტენციურ ადგილებს აანალიზებს და აღმოაჩენს. ამისათვის ის ნაპოვნი ქსელის ტოპოლოგიის თავისებურებებს, მისადმი მიდგომებს სწავლობს (მეზობელ ქსელებს და მათ შორის ნდობის დონეებს). შეტევის ეს ეტაპი შეიძლება არ იყოს ჯერ აქტიური - თავდამსხმელს შეუძლია ყველა საჭირო ინფორმაცია მოიპოვოს მესამე მხარის სრულიად კანონიერი ინფორმაციული წყაროების გამოყენებით.

ამას შეტევის პირველი აქტიური ეტაპი მოყვება – ქსელის დაზვერვა. თანამედროვე განაწილებული ქსელებისა და საინფორმაციო რესურსების ორგანიზების ტიპური გადაწყვეტილებების გათვალისწინებით, სერვისის ინფორმაციის მისაღებად თავდამსხმელი ასკანირებს ქსელის აღჭურვილობას, სერვერებს და სამუშაო სადგურებს. იღებს იმის შესახებ ინფორმაციას, თუ რომელი ოპერაციული სისტემები და ქსელური სერვისები მუშაობს მათზე. თუ თავდამსხმელი ქსელშია (და შეჭრა შიდაა), მას შეიძლება წვდომა ჰქონდეს შესასწავლი კომპიუტერული ქსელის ქსელური პაკეტების გადასაცემ ფიზიკურ გარემოზე, რაც იმას ნიშნავს, რომ მას შეუძლია ქსელური აღჭურვილობის პასიური იდენტიფიცირება, მასში გამავალი ქსელური პაკეტების ანალიზით.

გარდა ამისა, აუცილებელია, რომ ქსელური მოწყობილობების კონფიგურაციის პარამეტრების გარკვევა მოახდინოს. ამისათვის თავდამსხმელი კვლევის ქვეშ მყოფი დისტანციური მოწყობილობებიდან მიღებულ მთელ ტრაფიკს აანალიზებს. ანალიზის მიზნებისთვის თავდამსხმელი ძირითადად ოპერაციული სისტემების არასტანდარტულ ინსტრუმენტებს იყენებს და თავად ანალიზი ხდება დროის გადადებულ რეჟიმში.

თავდამსხმელი ცდილობს დაადგინოს ინფორმაციული უსაფრთხოების სისტემაში დაუცველი ბმულების არსებობა, რაოდენობა და ტიპი კომპიუტერული ქსელის შესახებ მიღებული ინფორმაციის საფუძველზე. ამისთვის ასევე შეიძლება გამოიყენოს დამატებითი ქსელის სკანირება (მაგალითად, ვებ-სერვერის აღმოჩენისა და მისი ტიპის გაგების შემდეგ, შეიძლება საჭირო გახდესდაუცველი CGI სკრიპტების დასადგენად დამატებითი სკანირება).

სისუსტეების გამოვლენის, ქსელური აღჭურვილობის ფუნქციონირების შეღწევისა და შეცვლის შესაძლებლობების გაანალიზების საფუძველზე თავდამსხმელი შემდგომი ქცევის სტრატეგიას განსაზღვრავს და ახორციელებს ქსელური აღჭურვილობის ფუნქციონირების გამორთვას.

შეტევის უკანასკნელი სტადიას თითქმის ყოველთვის წარმოადგენს ქსელში ყოფნის კვალის დამალვა ან ინფორმაციასთან წვდომა (კონფიდენციალურობის დარღვევა, მოდიფიკაცია, წაშლა). ამისთვის ხორციელდება სისტემაში არსებული ჩანაწერების ტიპებისა და სახეობების გაანალიზება და მისი მოდიფიკაცია.

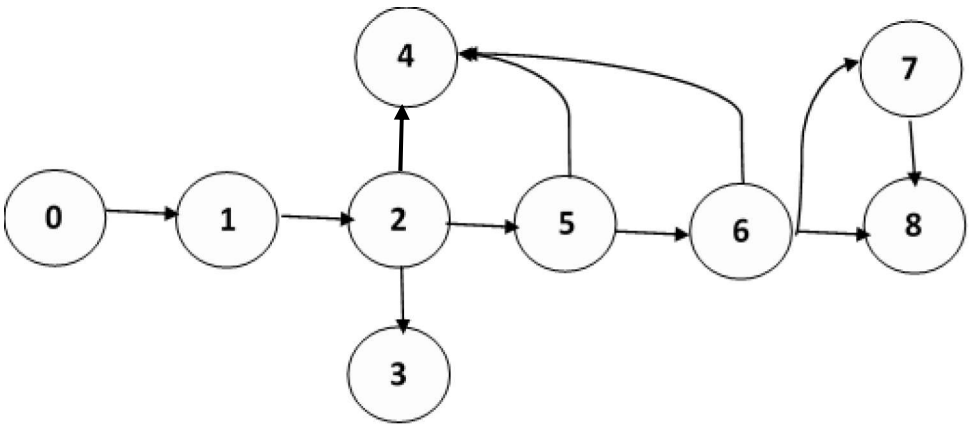
ამრიგად, ჩვენ შეგვიძლია ტიპური კომპიუტერული შეტევის ფაზების სია განვსაზღვროთ, რომელიც შეიძლება შემდგომში გამოყენებულ იქნას მათემატიკური მოდელირებისთვის.

ცხრილი 1. ტიპური ქსელური შეტევების ფაზები

ფაზის ტიპი P, აღნიშვნა	ტიპური მოქმედებები	დამახასიათებელი ნიშნები	განხორციელების მიზანი
უსაფრთხო მდგომარეობა, P_0	ქსელში თავდასხმის ობიექტის ძიება		თავდასხმის ობიექტის ძიება მეორადი ინფორმაციით, რომელსაც ფლობს თავდამსხმელი
ტოპოლოგიის შესწავლა, ქსელური დაზვერვა, P_1	ქსელის ტოპოლოგიის სკანირება, ღია პორტის სკანირება, OS ტიპის ამოცნობა	ქსელური ტრაფიკის ანომალიების გამოჩენა, ქსელის კვანძების სკანირება ცნობილი მეთოდების გამოყენებით	თავდასხმის ობიექტების ადგილმდებარეობის გარკვევა
დაუცველობის იდენტიფიკაცია, P_2	ქსელური სერვისების და მათი ვერსიების განსაზღვრა, ბანერების შეგროვება, პაროლების შერჩევა	"ქარიშხალი" ქსელური პაკეტების საძიებო მოთხოვნები, ქსელის გარკვეულ კვანძებში, "ბანერების" შეგროვება, ჟურნალის ჩანაწერები	დაუცველი ქსელის ინფრასტრუქტურის კომპონენტების მოძიება
სპუფინგი, P_3	სხვა ქსელის ობიექტის განსახიერების მცდელობა	ანომალიური პაკეტების გამოჩენა	მომსახურე სერვისებზე წვდომის მიღების მცდელობა ან სანდო სუბიექტად თავის გასაღება
უარი მომსახურებაზე, P_4	რესურსის გათიშვა ხანგრძლივი ზემოქმედებით, რესურსის გამორთვა ერთი ზემოქმედებით	ტრაფიკის ანომალური მახასიათბლის გამოჩენა, კვანძის რესურსის გამოყენება, ან ერთჯერადი ქმედება (ხელმოწერა), რომელიც იწვევს კვანძის შესვლას მომსახურების უარყოფის მდგომარეობაში	რესურსზე ნორმალური წვდომის დაბლოკვა, ინფორმაციაზე წვდომის შეუძლებლობა
შეღწევის მცდელობა, P_5	შეღწევა თავდასხმულ სისტემაში დაუცველობის ან გამოცნობილი პაროლის გამოყენებით	ტრაფიკში საეჭვო ხელმოწერების გამოჩენა, ფრაგმენტები "shellcode", ჩანაწერები სარეგისტრაციო ჟურნალებში, სერვისზე უარის თქმა, სისტემის და სამომხმარებლო პროცესები ჩავარდნა	დისტანციური ჰოსტზე ან აპლიკაციაზე კონტროლის მიღება

გამაგრება, P_6	ახალი მომხმარებ-ლების გაჩენა, დამატებითი სასტარტო პუნქტების შექმნა, ახალი სისტემური სერვისების გაჩენა	დამატებითი კავშირების გამოჩენა ტრაფიკში, საკონტროლო ბრძანებების ფრაგმენტების ქსელურ ტრაფიკში გამოჩენა, უცნობი პროტოკოლები	მავნე ქმედებების ორგანიზება, მუქარის განხორციელება ყველა სახის ინფორმაციის უსაფრთხოება
ნაკვალევის ნიღაბი, P_7	სისტემაში ფარული ყოფნის საშუალებების დადგენა (rootkits), ჟურნალების გასუფთავება	ფარული კონტროლის პროგრამების ფრაგმენტების არსებობა ქსელურ ტრაფიკში, სარეგისტრაციო ჟურნალების გაქრობა	რესურსების უწყვეტი კონტროლი
ინფორმაციის განადგურება, თავდასხმის გავრცელება, P_8		ქსელურ ტრაფიკში აქტიური ფარული არხების არსებობა, ქსელის ფრაგმენტების მოშლა	შენახული ინფორმაციის მთლიანობისა და მისი დამუშავების პირობების დარღვევა

(ნახაზი 1) სქემატურად გვიჩვენებს, თუ როგორ შეიძლება ტიპური ქსელის შეტევის სცენარი გადავიდეს ერთი ფაზიდან მეორეზე. უნდა აღინიშნოს, რომ ზოგიერთი ელემენტი შესაძლოა სცენარში არ იყოს და ამავდროულად შეიძლება მოხდეს შეტევა. რაც უფრო სრულყოფილი იქნება დაკვირვებული მოვლენების ჯაჭვი, მით უფრო გარკვეული იქნება ის.



ნახ. 1. თავდასხმის განხორციელების ეტაპები ტიპური სცენარის მიხედვით

3. დასკვნა

აღსანიშნავია, რომ შეჭრის აღმოჩენის სისტემა მუშაობს ეფექტურად, თუ ის მიუთითებს სისტემაში წარმოქმნილი ფაქტობრივი საფრთხეების არსებობაზე. სისტემისთვის საფრთხის შესაბამისობა (პირველ რიგში) კონკრეტული შეტევების განხორციელებასთან დაკავშირებული რისკების შეფასებით განისაზღვრება. ამიტომ IDS ოპერატორები, რომლებიც გარკვეული პერიოდის განმავლობაში ერთმანეთთან დაკავშირებულ შეტყობინებების ჯაჭვს აკვირდებიან, წყვეტენ მათ ყურადღებას. მეორეს მხრივ, თუ მომხმარებელი ხედავს, რომ შეტევა მიმდინა-

რეობს იმ ფაზაში, რომელშიც თავდამსხმელს უკვე შეუძლია მავნე ქმედების შესრულება და შედეგამდე მიმავალი მოვლენების ჯაჭვი აღდგება, მაშინ ასეთი წარმოდგენისას შეიძლება ბოლო დაკვირვებული მოვლენის საინფორმაციო შინაარსი მნიშვნელოვნად გაიზარდოს და წვლილი შეიტანოს სწორი გადაწყვეტილებების მიღებაში.

გამოყენებული ლიტერატურა:

1. ქართველიშვილი ი., ოხანაშვილი მ., აბულაძე ი., ჩორხაული ნ.,დარჩაშვილი მ. ქსელური შეტევების აღმოჩენის არსებული სისტემების მიმოხილვა და ანალიზი. ასოციაცია მეცნიერებისათვის.Vol.6Issue3,2024.https://doi.org/10.52340/gs.2024.06.03.01
2. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Birthday%20attack
3. https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/ids-vs-ips/#

Analysis of the stages and phases of typical network attacks based on security events

Ioseb Kartvelishvili, M. Okhanashvili, M. Darchashvili

Georgian Technical University

s.kartvelishvili@gtu.ge, m.okhanashvili@gtu.ge, misha8003123@gmail.com

Summary

The paper presents and analyzes the stages and phases of typical network attacks. Successful attacks on computer networks represent a rather complex sequence of actions pre-formed and prepared by the attacker. The implementation of an attack is often a multi-stage process, in which each stage is characterized by its own characteristics. Studying the "anatomy" of a computer attack allows us to assess the attacker's capabilities in carrying out malicious actions and also to develop an adequate protection system.

Keywords: Intrusion detection systems. Network intelligence. Hardening. Obfuscation. Malicious intent.