საქართველოს ტექნიკური უნივერსიტეტი

ვ. ადამია, ნ. არაბული

მონაცემთა დაცვა კომპიუტერულ ქსელებში

I ნაწილი

დამტკიცებულია სახელმძღვანელოდ
სტუ-ს სარედაქციო-საგამომცემლო
საბჭოს მიერ

თბილისი
2007

განხილულია საინფორმაციო სისტემების საიმედოობის და უსაფრთხოების მოთხოვნები; თანამედროვე თავდასხმების კლასიფიკაცია და მათთან ბრძოლის მეთოდები; დაცვის ზომები, აღმოჩენა და რეაგირება; უსაფრთხოების პოლიტიკა და პრინციპები.

სახელმძღვანელო განკუთვნილია საქართველოს ტექნიკური უნივერსიტეტის ინფორმატიკის ფაკულტეტის სტუდენტებისათვის და ასევე მკითხველთა ფართო წრისათვის, რომლებიც დაინტერესებულნი არიან მონაცემთა გადაცემის ქსელებში ინფორმაციის დაცვის პრობლემებით.

რეცენზენტი ასისტენტ-პროფესორი დ. კაპანაძე

ISBN 978-99940-957-8-0 (ორივე ნაწილი)

ISBN 978-99940-957-9-7 (პირველი ნაწილი)

საინფორმაციო სისტემების საიმედოობის და უსაფრთხოების მოთხოვნები და ზოგადი პრინციპები

გამოთვლითი ტექნიკის და საინფორმაციო ქსელების სწრაფმა განვითარებამ გამოიწვია მათი ფართო გავრცელება როგორც ყოველდღიურ ცხოვრებაში, ასევე ბიზნესში. მძლავრი გამოთვლითი შესაძლებლობები და ინფორმაციის გადაცემის ოპერატიულობა ხელს უწყობს როგორც ტრადიციული ბიზნესის განვითარებას, ასევე ბიზნესის ახალი ფორმების წარმოშობას. განსაკუთრებული მნიშვნელობა საინფორმაციო ტექნოლოგიებმა საბანკო სფეროში შეიძინა.

საინფორმაციო სისტემების ასეთმა ფართო გავრცელებამ სულ უფრო მნიშვნელოვანი გახადა მათი საიმედოობისა და უსაფრთხოების გაზრდა. ინფორმაციის დაგროვების, გადამუშავების და გადაცემის თანამრდროვე მეთოდებმა განაპირობა ინფორმაციის დაკარგვის, მოდიფიცირების და მოპარვის საფრთხის წარმოშობა. გარდა ამისა საფრთხეს წარმოადგენს საინფორმაციო სისტემების მწყობრიდან გამოსვლა. სწორედ ამიტომ გაიზარდა საინფორმაციო სისტემების დაცვის მნიშვნელობა.

მომხმარებლის ინფორმაციის დაცვის ძირითადი ამოცანებია:

- ინფორმაციის კონფიდენციალობის უზრუნველყოფა;
- ინფორმაციის მთლიანობის უზრუნველყოფა;
- ინფორმაციის სარწმუნოების უზრუნველყოფა;
- ინფორმაციასთან ოპერატიული მიმართვის უზრუნველყოფა;

- ელექტრონული სახით წარმოდგენილი ინფორმაციის იურიდიული მნიშვნელობის უზრუნველყოფა;
- კლიენტის მოქმედებების კონფიდენციალურობის უზრუნველყოფა.

ინფორმაციის კონფიდენციალობა ნიშნავს, რომ მასთან მიმართვა მხოლოდ მომხმარებელთა გარკვეული ჯგუფს შეუძლია.

მთლიანობაში იგულისხმება ინფორმაციის ან პროგრამული უზრუნველყოფის თვისება შეინარჩუნოს თავისი სტრუქტურა და შინაარსი გადაცემის და შენახვის პროცესში.

ინფორმაციის სარწმუნოება მას მკაცრად მიაკუთვნებს ობიექტს, რომელიც მის წყაროს წარმოადგენს, ან იმ ობიექტს, რომლისაგანაც ეს ინფორმაციაა მიღებული.

ოპერატიულობა განსაზღვრავს საინფორმაციო რესურსის უნარს იყოს მისაწვდომი საბოლოო მომხმარებლისათვის მისი მოთხოვნილების შესაბამისად.

ინფორმაციის იურიდიული მნიშვნელობა ნიშნავს, რომ დოკუმენტს გააჩნია იურიდიული ძალა. ამ მიზნით სუბიექტები, ვისთვისაც მნიშვნელოვანია გადაცემული გზავნილის იურიდიული მნიშვნელობა, თანხმდებიან ინფორმაციის იმ განსაკუთრებული ატრიბუტების საყოველთაო აღიარებაზე, რომლებიც გამოხატავენ მის იურიდიულ მნიშვნელობას. გზავნილების იურიდიული მნიშვნელობა განსაკუთრებით მნიშვნელოვანია ელექტრონული გადახდის სისტემებში, სადაც ხდება ფულის ელექტრონული გადარიცხვის ოპერაციები. დოკუმენტების იურიდიული მნიშვნელობის განმსაზღვრავი

ატრიბუტები ერთმნიშვნელოვნად უნდა ადასტურებდნენ, რომ დოკუმენტი კონკრეტული პირის მიერაა გამოგზავნილი.

ოპერაციების კონფიდენციალურობის უზრუნველყოფა ნიშნავს, რომ მომხმარებელს აქვს საშუალება აწარმოოს ოპერაციები ისე, რომ არავის შეეძლოს მისი თვალთვალი. მსგავსი მოთხოვნის აქტუალურობა ცხადი გახდა ელექტრონული ფულის წარმოშობასთან ერთად. ელექტრონული ანგარიშსწორების სისტემასთან მიმართვისას მომხმარებელი აწვდის მას გარკვეულ საიდენტიფიცირო ინფორმაციას. ამ სისტემების ფართო გავრცელებასთან ერთად შესაძლოა გაჩნდეს ანგარიშსწორების ოპერაციების კონტროლირების და მომხმარებლებზე ტოტალური თვალთვალის საშიშროება სახელმწიფო სტრუქტურების ან სხვა დაინტერესებული პირების მხრიდან.

ამ პრობლემის გადაწყვეტის ერთი გზა საკანონმდებლო აქტებით საშუალებით საინფორმაციო სისტემების მომხმარებლებზე ყოველგვარი ტოტალური თვალთვალის აკრძალვაა. მეორე გზა კი სპეციალური კრიპტოგრაფიული მეთოდების გამოყენებაა.

როგორც უკვე აღვნიშნეთ საინფორმაციო უსაფრთხოება უნდა განვიხილოთ როგორც ინფორმაციის კონფიდენციალურობის დაცვის, ასევე ინფორმაციული სისტემების მიერ მოცემული ფუნქციების შესრულების უნარის მხრივ. საინფორმაციო სისტემების გამართულად მუშაობისათვის საჭიროა უზრუნველვყოთ:

- სისტემაში არასანქცირებული შეღწევისაგან დაცვა;
- დაცვის შიდა და გარე სისტემების დაცვა გატეხვისაგან;

- მომხმარებლების და ქსელის მომსახურე პერსონალის მიერ სისტემაში არასანქცირებული მოქმედებებისაგან დაცვა;
- ავარიული სიტუაციების დროს სისტემის დაცვა მწყობრიდან გამოსვლისაგან.

საინფორმაციო-ტელეკომუნიკაციურ ქსელებში უსაფრთხოების უზრუნველყოფისათვის საჭიროა:

- ინფორმაციის დაცვა შენახვის, გადამუშავების და გადაცემის დროს;
- მონაცემების და მომხმარებლების სარწმუნოების დამოწმება (მხარეების აუტენტიფიკაცია);
- მონაცემების მთლიანობის დარღვევის აღმოჩენა და გაფრთხილება;
- ტექნიკური მოწყობილობების და სათავსოების დაცვა;
- კონფიდენციალური ინფორმაციის დაცვა სათვალთვალო მოწყობილობების საშუალებით მოპოვებისაგან და გაჟონვისაგან;
- პროგრამული პროდუქტების დაცვა ვირუსებისაგან და სხვა პროგრამული ჩანართებისაგან;
- არასანქცირებული შეღწევებისაგან საინფორმაციო სისტემების დაცვა.

საინფორმაციო რესურსების უსაფრთხოების უზრუნველყოფა კონკრეტულ შემთხვევაში შეიძლება გამოიხატოს ორგანიზაციული ან ტექნიკური მეთოდებით ინფორმაციის დაცვაში. ორგანიზაციული მეთოდები გულისხმობს პერსონალის უფლებამოსილებების ზუსტ განსაზღვრასბ მომხმარებლების

ინფორმირებას შესაძლო საფრთხის შესახებ, სამუშაო პროცესის ისეთ ორგანიზებას, რომ გამოირიცხოს კონფიდენციალური ინფორმაციის გაჟონვის შესაძლებლობა და სხვა. დაცვის ტექნიკური მეთოდები გულისხმობს ინფორმაციული სისტემების მუშაობის და ინფორმაციის შენახვის საიმედოობის გაზრდას (დუბლირება, სარეზერვო კოპირება და სხვა) ინფორმაციის კრიპტოგრაფიული დაცვის მეთოდებს შენახვის და გადაცემის პროცესში, აუტენტიფიკაციის პროგრამულ საშუალებებს, ქსელის დაცვას ქსელური ეკრანებით და შლუზებით და სხვა.

თანამედროვე დაცვის სისტემები საკმაოდ რთულია, მაგრამ რაღაც ზეჩვეულებრივი მაგათში მაინც არ არის, იმიტომ რომ ინფორმაციული ტექნოლოგიების განვითარებას ისინი ყოველთვის ჩამორჩებიან. წარმოუდგენელია ქსელთაშორისი ეკრანის არსებობა სისტემაში (Firewall) სადაც კომპიუტერები ერთმანეთთან არ არის დაკავშირებული, ან რა საჭიროა ანტივირუსი თუ არ არსებობს ვირუსული პროგრამები, მეტ-ნაკლებად სერიოზული დაცვითი ტექნოლოგიები ჩნდება ახალი ტექნოლოგიური სიახლეების შექმნის საპასუხოდ. უფრო მეტიც ზოგჯერ ტექნოლოგიური სიახლე არ ითხოვს აუცილებელ დაცვის სისტემის შექმნას, ის იქმნება მაშინ როდესაც გაჩნდება მაგის ფინანსური მიზანშეწონილობა. მაგალითად დაცვითი მეანიზმების შექმნა მონაცემთა ბაზების მართვის სისტემების კლიენტ-სერვერული მოდელისთვის აუცილებელია, იმიტომ რომ ის უშუალოდ მოქმედებს მომხმარებლებზე, რომლებიც სარგებლობენ აღნიშნული სისტემით. ხოლო დაცვითი ფუნქციების არ არსებობა მობილურ ტელეფონებში დიდად არ აისახება მათ გაყიდვებზე.

აგრეთვე დაცვითი ტექნოლოგიების განვითარება გავლენას ახდენს "ჰაკერებზე". ეს გასაგებიცაა, რადგანაც ყველაზე გამოყენებად ტექნოლოგიებშიც კი მანამ არ შეიქმნება დაცვითი სისტემის სექმა, სანამ მათზე არ მოხდება ჰაკერული თავდასხმა. ნათელ მაგალითს წარმოადგენს უკებელო ქსელური ტექნოლოგია, რომელსაც არც თუ ისე დიდი ხნის წინ ქონდა, არც თუ ისე სერიოზული დაცვის სისტემა. მაგრამ ბოროტმოქმედების მოქმედებამ გამოაჩინა არსებულის სიტემის ხარვეზები, ამიტომ დაუყონებლივ შეიქმნა სპეციალიზირებული დაცვის მექანიზმები და საშუალებები მაგალითად როგორიც არის ხარვეზების აღმომჩენები (სკანერები), შეტევის აღმომჩენი სისტემები და სხვა.

მარკეტინგში ხშირად იყენებენ ტერმინს "კომუნიკაციური ველი" რომელიც აღნიშნავს ერთეული ადამიანების ან ადამიანთა ჯგუფების ურთიერთობის გარემოს ან წრეს, ჩვენ შემთხვევაში საუბარი გვექნება კომპანიების კომინიკაციურ ველზე, ე.ი ინტერნეტზე, დაშორებულ ფილეალებზე (ინტრანეტი) კლიენტებზე და პარტნიორებზე (ექსტრანეტი)

ურთიერთობის მიხედვით გამოიყენება სხვადასხვა დაცვითი ტექნოლოგიები, მაგალითად ინტერნეტთან კავშირისას არასდროს გამოვიყენებთ VPN (Virtual Private Network - ვირტუალური კერძო ქსელი) ტექნოლოგიას, მაგრამ როდესაც კავშირს ვანხორციელებთ დაშორებულ ფილიალებთან აღნიშნული ტექნოლოგია საკმაოდ მნიშვნელოვანია.

ინფორმაციული დაცვის ტექნოლოგიის შერჩევისას, მნიშვნელოვან გავლენას ახდენს კომპიუტერების რაოდენობა რომელიც გაერთიანებულია ქსელში. ქსელის მასშტაბი თავის წესებს კარნახობს- რადგან ფულის უკმარისობის გამო ვერ

ხერხდება საჭირო ინფორმაციული დაცვის სისტემების შეძენა, ისევე როგორც ზოგჯერ უკანასკნელის საჭიროების საერთოდ არ ქონის გამო. ასე რომ ერთი კომპიუტერი, რომელიც ჩართულია ინტერნეტის ქსელში არ სჭირდება კონფიდენციალური ინფორმაციის გაჟონვის საწინააღმდეგო კონტროლის სისტემა, როდესაც აღნიშნული სასიცოცხლოდ აუცილებელია უკვე მცირე კომპიუტერული ქსელის არსებობისას.

ინტერნეტის ხანაში კომპიუტერული ინფორმაციის უსაფრთხოება და ქსელური უსაფრთხოება ერთმანეტს შეერწყა. კომპიუტერული ინფორმაციის სრული დაცვა, რომელიც შეიზლება განისაზღვროს, როგორც დაუშებელი მოქმედებების აღმოფხვრა და გამოვლენა. აღნიშნულის გაკეთება კომპიუტერული სისტემის მომხმარებლების მხრიდან, გაცილებით რთული და ძნელია, ვიდრე მარტივი მათემატიკა კრიპტოგრაფიისა.

არსი მდგომარეობს იმაში რომ მხოლოდ მათემატიკას არ შეუძლია უზრუნველყოს სრული უსაფრთხოება. კრიპტოგრაფიაში დაცვას მატემატიკა აძლევს უდიდეს უპირატესობას ბოროტმოქმედებთან შედარებით. ერთი ბიტის დამატება გასაღებზე ორჯერ ართულებს მის გატეხვას, 10-ის მიახლოებით 1000-ჯერ როდესაც ლაპარაკი მიდის კომპიუტერულ უსაფრთხოებაზე ერთიანად, მხარეები იმყოფებიან თანაბარ მდგომარეობაში: ბოროტმოქმედებმა და დამცველებმა შესაძლებელია მიიღონ ტექნოლოგიისგან ერთდაიგივე მოგება, ეს იმას ნიშნავს, რომ თუ თქვენ გექნებოდათ საკმარისი კრიპტოგრაფია უსაფრთხოების უზრუნველსაყოფად, მაშინ თქვენ გექნებოდათ ყველაფერი

წესრიგში, მაგრამ სამწუხაროდ უმრავლეს შემთხვევაში ეს ასე არ არის.

არსებობს უსაფრთხოების ბევრი თეორიული მოდელი, რომელთა უმრავლესობა ფინანსდებოდა ამერიკის თავდაცვის სამინისტროს მიერ და გამოიყენებოდა სამხედრო საიდუმლოების დაცვის მიზნით. ძირითადად ასეთი სისტემები არის მრავალდონიანი, იმიტომ, რომ ისინი გამოიყენება მრავალი დონის საიდუმლოების მხარდასაჭერად.

თანამედროვე თავდასხმების კლასიფიკაცია და მათთან ბრძოლის მეთოდები

ინტერნეტის პოპულარიბის კოლოსალურ ზრდასთან ერთად, წარმოიქმნა პერსონალური ინფორმაციის, კრიტიკულად მნიშვნელოვანი კორპორაციული რესურსების, სახელმწიფო საიდუმლოების და სხვა ინფორმაციის გაჟონვის უპრეცედენტო საშიშროება. ყოველ დღე ჰაკერები ამ რესურსებს უქმნიან საშიშროებას. და ცდილობენ მიიღონ ეს ინფორმაცია თავდასხმის სხვადასხვა გზების გამოყენებით, რომლებიც ერთი მხრივ ხდებიან უფრო და უფრო დახვეწილები და მეორე მხრივ - მარტივი გამოსაყენებლად. ამას განაპირობებს ორი ფაქტორი.

პირველი: ეს არის ინტერნეტში ყოველმხრივი შეღწევადობა. დღესდღეისობით ქსელებში დაკავშირებულია მილიონობით მოწყობილობა და კიდევ მარავალი მილიონი ჩაერთვება უახლოეს მომავალში. ამიტომ ნაკლოვან მოწყობილობებშიც ჰაკერების შეღწევის ალბათობაც იზრდება. აგრეთვე ინტერნეტის ფართოდ გავრცელება ჰაკერებს აძლევს შესაძლებლობას გაცვალონ ინფორმაცია გლობალურ მასშტაბში.

მეორე: ეს არის გამოყენებისთვის მარტივი ოპერაციული სისტემების

და მათი შექმნის საშუალებების გავრცელება. აღნიშნული ფაქტორი ამცირებს ჰაკერის აუცილებელი განათლებას დონეს. მანამდე, რომ შექმნილიყო და გავრცელებულიყო მარტივი გამოყენებითი პროგრამა ჰაკერს უნდა ქონოდა კარგი განათლება პროგრამირებაში. ახლა რომ მივიღოთ წვდომა ჰაკერული საშუალებებზე, საჭიროა მხოლოდ საიტის IP მისამართის ცოდნა და რომ განვახორციელოთ შეტევა უბრალოდ საჭიროა დავაწკაპუნოთ მაუსს.

ქსელური თავდასხმები იმდენად მრავალგვარია, ისევე როგორც სისტემები, რომლის წინააღმდეგაც ისინი არიან მიმართული. ზოგიერთი შეტევა გამოირჩევა დიდი სირთულით. შეტევის ტიპების შეფასებისას აუცილებელია ვიცოდეთ ზოგიერთი შეზღუდვები, თავდაპირველად რომელსაც მივყავართ Tcp/Ip პროტოკოლამდე -მდე. ინტერნეტი შეიქმნა იმისათვის, რომ დაკავშირებულიყო სახელმწიფო ორგანიზაციები და უნივერსიტეტები და გაეწია დახმარება სასწავლო პროცესისთვის და მეცნიერული გამოკვლევებისათვის. ამ ქსელის შემქმნელები არ ელოდებოდნენ მის ასე გავრცელებას. შედეგად ინტერნეტის პროტოკოლის ადრეულ სფეციფიკაში არ იყო უსაფრთხოების მოთხოვნა გათვალისწინებული. რამდენიმე წლის შემდეგ, საბოლოლოდ დაიწყეს უსაფრთხოების ზომების დანერგვა, იმის გათვალისწინებით რომ თავიდანვე არ იყო გათვალისწინებული უსაფრთხოების ზომები, ამიტომ ამის გაკეთება დაიწყეს სხვადსხვა საშუალებებით და პროცედურებით, რომ დაეწიათ რისკი, რომელსაც შეიცავდა ეს პროტოკოლები. შემდგომში დაწვრილებით განვიხილავთ შემთხვევებს დაკავშირებულს IP

ქსელების წინააღმდეგ და ჩამოვთვლით მათ საწინააღმდეგო ხერხებს.

ფაიერვოლი

ფაიერვოლი არის სისტემა, რომელიც გვაძლევს საშუალებას დავყოთ ქსელი ორ ან მეტ ნაწილად და ჩამოვაყალიბოთ წესები, რომლებიც განსაზღვრავენ პაკეტების მიმოცვლის წესებს ერთი ქსელიდან მეორე ქსელში.

ხშირად ფაიერვოლი დგება ინტერნეტის და ორგანიზაციის ქსელების საზღვარზე, მაგრამ ზოგჯერ მას იყენებენ ორგანიზაციის ლოკალური ქსელის შიგნითაც.

ყოველი პაკეტისთვის ფაიერვოლი ღებულობს გადაწყვეტილებას, გაატაროს ის თუ არა, წესების გარკვეული კრებულის მიხედვით.

ფაიერვოლი შეიძლება მუშაობდეს როგორც ქსელურ დონეზე, ასევე გამოყენებით დონეზეც. ჩვენ განვიხილავთ მხოლოდ ქსელური დონის ფაიერვოლებს.

ქსელის დონეზე მომუშავე ფაიერვოლი ღებულობს გადაწყვეტილებებს პაკეტის ადრესატის და გამგზავნის მისამართების, პროტოკოლის და ადრესატის და გამგზავნის პორტების მისამართების საფუძველზე.

ჩვენ განვიხილავთ ზოგადად ფაიერვოლის კონფიგურირების პრინციპებს. ეს პრინციპები არ იცვლება ნებისმიერი ფაიერვოლის კონფიგურირების დროს. სხვა და სხვა პროგრამაში განსხვავებულია მხოლოდ წესების შეყვანის ფორმა და სინტაქსისი.

ფაიერვოლი ღებულობს გადაწყვეტილებას პაკეტის გატარების ან დაბლოკვის შესახებ წესების ბაზის საფუძველზე.

ადმინისტრატორის მოვალეობაა შექმნას ისეთი წესების ბაზა, რომელიც შეესაბამება კონკრეტულ ქსელს და ქსელში არსებულ სერვისებს.

ფაიერვოლი განიხილავს წესებს მათი ნომრების ზრდადობის მიხედვით. თუ პაკეტი შეესაბამება მოცემულ წესს, მაშინ ფაიერვოლი ან ატარებს ამ პაკეტს ან ბლოკავსმას. შემდეგ წესებს ის აღარ განიხილავს.

ქსელის დონეზე მომუშავე ფაიერვოლის წესი შედგება შემდეგი ველებისგან:

1. წესის ნომერი
2. მოქმედება
3. პროტოკოლი
4. გამგზავნის ჰოსტის ან ქსელის მისამართი
5. გამგზავნის პორტის ნომერი ან ინტერვალი
6. ადრესატის ჰოსტის ან ქსელის მისამართი
7. მიმღების პორტის ნომერი ან ინტერვალი

შესაძლებელია ამ წესებში იყოს ინფორმაცია, რომელიც დამოკიდებულია კონკრეტულ პროტოკოლზე, მაგალითად TCP პროტოკოლისათვის — ინფორმაცია სესიის მდგომარებოაზე, ICMP პროტოკოლისათვის — ინფორმაცია პაკეტის ტიპზე და ა.შ.

ზემოთ ჩამოთვლილი ველებიდან აუცილებელია მხოლოდ პირველი ხუთი. დანარჩენების მითითება აუცილებელი არ არის თუ ამას სიტუაცია არ მოითხოვს.

განვიხილოთ რა მნიშვნელობები შეიძლება მიიღოს თითოეულმა ველმა და თუ რა მოთხოვნებს უნდა აკმაყოფილებდნენ ისინი.

1. წესის ნომერი – რიცხვი 1-დან 65534-მდე. (ფაიერვოლში შესაძლო წესების რაოდენობა დამოკიდებულია კონკრეტული რეალიზაციაზე. აქ მოყვანილია მნიშვნელობები FreeBSD ოპერაციული სისტემის ქვეშ მომუშავე IPFW ფაიერვოლისთვის).

2. მოქმედება — შესაძლებელია ორი მოქმედება: გატარება (permit, allow, pass) ან დაბლოკვა (deny).

3. პროტოკოლი — შეიძლება მიიღოს შემდეგი მნიშვნელობები: IP, TCP, UDP, ICMP და სხვა.

4. გამგზავნის მისამართი — აუცილებელია ჩაიწეროს ქსელის მისამართი შესაბამისი ნიღბით (Network Mask) ან ჰოსტის მისამართის შემთხვევაში წინ მიეწეროს სიტყვა: “host”. ნიღაბი შეიძლება ჩაიწეროს ორნაირად — ათობითი ფორმატის მისამართის თითოელ ბაიტში ქსელის ნაწილის მითითებით (მაგალითად: 255.255.255.252), ან უბრალოდ ქსელის ნიღაბში ერთიანების რაოდენობის მითითებით (/30).

- 255.255.255.252 ან /30
- 255.255.255.248 ან /29
- 255.255.255.0 ან /24

მეორე ვარიანტი ხშირად უფრო ადვილად იკითხება და მოკლეა დასაწერად.

ასევე შესაძლებელია მისამართის მაგივრად სიტყვა “any”-ს ჩაწერა, რაც ნებისმიერ მისამართს გულისხმობს.

როგორ გამოვთვალოთ მისამართის ქსელის ნაწილში ბიტების რაოდენობა?

განვიხილოთ მაგალითად ქსელის ნიღაბი 255.255.255.240. წარმოვადგინოთ ეს რიცხვები ორობით ფორმატში და უბრალოდ დავითვალოთ ერთიანების რაოდენობა. მივიღებთ 28-ს.

255	255	255	240
11111111	11111111	11111111	11110000

როგორ გამოვთვალოთ ბიტების რაოდენობიდან ნიღბის ათობითი წარმოდგენა?

მაგალითად მოცემულია ბიტების რაოდენობა /29. დავწეროთ ორობით ფორმატში იმდენი ერთიანი, რამდენიც მოცემულია და გადავიყვანოთ შესაბამისი ბაიტები ათობით ფორმატში.

11111111	11111111	11111111	11111000
255	255	255	248

5,7 პორტის ნომერი — რიცხვი 1-დან 65535-მდე. გამოიყენება მხოლოდ TCP და UDP პროტოკოლების დროს და გულისხმობს პორტის ნომერს. არსებობს პორტის ნომრების შემდეგი შესაბამისობა სტანდარტულ სერვისებთან:

სერვისი	პორტის ნომერი
http	80
https	443

ftp	20,21
telnet	23
ssh	22
dns query	53
finger	79
tftp	69
smtp	25
pop3	110
imap	143

პორტების მითითების დროს ადმინისტრატორმა კარგად უნდა იცოდეს რას აკეთებს და რა შედეგს უნდა მიაღწიოს. არასწორი კონფიგურირების შემთხვევაში შესაძლებელია ლოკალურ ქსელში არსებული სერვისის დაბლოკვა, ან ლოკალური ქსელის მომხმარებლების მუშაობის შეფერხება. აღსანიშნავია, რომ ბევრ ოპერაციულ სისტემაში მიღებულია პორტების დაკავების შემდეგი წესი: 1024-მდე არის სერვისების პორტების ნომრები, მომხმარებლის მანქანიდან სხვა სერვისთან დაკავშირება ხდება 1024-ზე მეტი ნომრის პორტიდან. მაგალითად ინტერნეტში ვებ-გვერდის დათვალიერების დროს http პროტოკოლით იქმნება შეერთება მომხმარებლის კომპიუტერიდან სერვერის მე-80 პორტთან. სასურველია წესების ჩამოყალიბების დროს გათვალისწინებული იყოს ეს თავისიბურებანი.

შესაძელებელი პორტების ინტერვალის და პორტების ჩამონათვლის მითითება შემდეგნაირად:

ა. მიუთითოთ მე-80 და 443-ე პორტები: 80, 443

ბ. მიუთითოთ 80-დან 1024-მდე პორტები: 80-1024

ასევე მისაღებია შემდეგი შემოკლებანი:

შემოკლება	რას ნიშნავს
lt (less than)	ნაკლებია
gt (great than)	მეტია
eq	ტოლია

მაგალითად:

ა. 1024-ზე მეტია: gt 1024

ბ. ნაკლები 139-ზე: lt 139

მიმღების მისამართის მიმართ არის იგივე მოთხოვნები რაც გამგზავნის მისამართის შემთხვევაში.

ფაიერვოლის კონფიგურირება შეიძლება მოხდეს შემდეგი პრინციპების მიხედვით:

ა. დაშვებულია ის, რაც არ არის აკრძალული.

ბ. აკრძალულუა ის, რაც არ არის დაშვებული.

განვიხილოთ თითოეული პრინციპი უფრო დაწვრილებით:

დაშვებულია ის, რაც არ არის აკრძალული.

ფაიერვოლის ასეთი კოფიგურაციის დროს იგულისხმება, რომ ბოლო წესი გამოიყურება მაგალითად ასე: **6500 allow ip any any**. რაც ნიშნავს — ყველაფერი დაშვებულია, ე.ი ფაიერვოლის ბოლო წესის თანახმად პაკეტი უნდა გადაიცეს შემდეგ ქსელში. ამ შემთხვევაში დასაბლოკი წესები ჩამატებული უნდა იქნას ამ წესის წინ.

ასეთი ტიპის ფაიერვოლი გამოიყენება იშვიათად და მხოლოდ იმ შემთხვევაში, როდესაც ადმინისტრატორი დარწმუნებულია, რომ იცის ყველა ქსელური სერვისის შესახებ და ეს სერვისები დაკონფიგურირებულია ისე, რომ ინტერნეტიდან მათი მწყობრიდან გამოყვანა ან მათი გამოყენებით სისტემის დაზიანება შეუძლებელია.

ასეთი ფაიერვოლის კონფუგურაციის მაგალითია:

ამოცანა მდგომარეობს იმაში, რომ დაიბლოკოს მხოლოდ http სერვისი, რომელიც გაშვებულია 212.72.130.20 სერვერზე 213.157.211.0 C კლასის ქსელის მისამართებიდან.

C კლასის ნიღაბი არის 255.255.255.0 და მისამართის ქსელურ ნაწილში ბიტების რაოდენობა არის 24, ამიტომ პასუხი შეიძლება ჩაიწეროს შემდეგნაირად:

10 deny tcp 213.157.211.0/24 host 212.72.130.20 80

20 allow ip any any

ან ასე:

10 deny tcp 213.157.211.0 255.255.255.255 host 212.72.130.20 80

20 allow ip any any

ფაიერვოლის მეორე კონფიგურაციის ტიპი არის:

აკრძალულია ის, რაც არ არის დაშვებული.

ამ შემთხვევაში იგულისხმება, რომ ბოლო წესი გამოიყურება შემდეგნაირად: **6500 deny ip any any.** რაც ნიშნავს, რომ ყველაფერი აკრძალულია ე.ი არც ერთი პაკეტი, რომელიც აღწევს ამ წესამდე არ გადაიცემა შემდეგ ქსელში.

ასეთი ტიპის ფაიერვოლის კონფიგურაციის დროს, თითოეული სესიისთვის ჩამოსაყალიბებელია და დასაწერია თავისი წესი. ამას მოაქვს დადებითი ეფექტი თუ ადმინისტრატორს არ უნდა ან მან არ იცის რაიმე სერვისის შესახებ ან ახალი სერვისია გაშვებული ორგანიზაციის ქსელში. ეს სერვისი უბრალოდ დაბლოკილი იქნება მანამ, სანამ ადმინისტრატორი მას არ დაუშვებს ფაიერვოლში წესის დამატებით.

ორგანიზაციისთვის, რომელიც არის უბრალოდ ინტერნეტის მომხმარებელი და შესაძლებელია აქვს საფოსტო ან ვებ სერვერი რეკომენდირებულია ფაიერვოლის ასეთი პრინციპით კონფიგურირება, თუ რა თქმა უნდა არ არის სხვა დამატებითი მოთხოვნები, რომელთა გათვალისწინებით შეუძლებელია წესების ჩამოყალიბება.

ასეთი ტიპის ფაიერვოლის კონფიგურაციის მაგალითი:

ამოცანა მდგომარეობს იმაში, რომ დავუშვათ მომხმარებლები მხოლოდ 213.157.196.130 ვებ-სერვერზე ნებისმიერი მისამართიდან, გარდა ჰოსტისა 212.72.130.16 და ჰოსტებისა ქსელიდან 255.255.255.248.

ფაიერვოლის წესებს ექნება შემდეგი სახე:

10 deny tcp 212.72.130.16 255.255.255.248 host 213.157.196.130 80

20 allow tcp any host 213.157.196.130 80

30 deny ip any any

ან:

10 deny tcp 212.72.130.16/29 host 213.157.196.130 80

20 allow tcp any host 213.157.196.130 80

30 deny ip any any

პაკეტების სნიფერი

პაკეტების სნიფერი წარმოადგენს გამოყენებით პროგრამას, რომელიც იყენებს ქსელურ ადაპტერს, რომელიც მუშაობს თვალთვალის რეჟიმში (Promiscuous mode - ამ რეჟიმში ადაპტერი ყველა პაკეტს, მიღებული ფიზიკური არხის მიერ, უგზავნის აპლიკაციას დამუშავებისათვის) ამ დროს სნიფერი იჭერს ყველა ქსელურ პაკეტს, რომელიც გადაიცემა განსაზღვრულ დომეინში. ამ დროისთვის სნიფერები ქსელებში სავსებით კანონიერად მუშაობენ ქსელებში. ისინი გამოიყენება დიაგნოსტიკისათვის და ტრაფიკის ანალიზისათვის, მაგრამ თუ მხედველობაში მივიღებთ იმას, რომ ზოგიერთი ამლიკაცია გადასცემს მონაცემებს ტექსტურ ფორმაში (Ftp, Telnet, SMTP, POP3 და სხვა) სნიფერის საშუალებით შესაძლებელია გავიგოთ კონფიდენციალური ინფორმაცია (მაგ. მომხმარებლის სახელი და პაროლი).

სახელებისა და პაროლის დადგენა იძლევა დიდ საშიშროებას, რადგანაც მომხმარებლები ხშირად იყენებენ ერთი

და იგივე სახელს და პაროლს მრავალი პროგრამისთვის, მრავალ მომხმარებელს საერთოდ აქვს მხოლოდ ერთი სახელი და პაროლი. თუ პროგრამა მუშაობს როგორც კლიენტ-სერვერი, ხოლო აუტენტიფიცირებული მონაცემები გადაეცემა ქსელის საშუალებით და კითხვადი ტექსტური ფორმატით, მაშინ ეს ინფორმაცია დიდი ალბათობით შეიძლება გამოყენებულ იქნას კორპორატიულ და გარე რესურსებზე წვდომისათვის (შეტევის მეთოდები ხშირად ბაზირდება სოციალური ინჟინერიის საფუძველზე). მათ კარგად აქვთ წარმოდგენილი, რომ ჩვენ ვიყენებთ ერთი და იგივე პაროლს მარვალი რესურსის წვდომისათვის, ჩვენი პაროლის გაგებით, მას შეუძლია ჩვენი რესურსის გამოყენება ყველაზე ცუდ ვარიანტში ის მიიღებს წვდომას სამომხმარებლო დონეზე და მისი სასუალებით შექმნის ახალ მომხმარებელს, რომლის საშუალებით მას შეეძლება ნებისმიერ მომენტში შემოვიდეს ქსელში და მის რესურსებში.

პაკეტების სნიფინგის საშიშროების დასაწევად შესაძლებელია გამოვიყენოთ შემდეგი საშუალებები:

აუტენტიფიკაცია

აუტენტიფიკაციის ძლიერი საშუალებები წარმოადგენენ მნიშვნელოვან ხერხს, პაკეტების სნიფინგის წინაღმდეგ. ” ძლიერი” საშუალებების ქვეშ იგულისხმება ისეთი მეთოდები, რომლისთვის გვერდის ავლა ძნელად შესაძლებელია.

მაგალითად ისეთი აუტენტიფიკაციისა არის ერთჯერადი პაროლები (One Time Passwords, OTP) OTP- ეს არის აუტენტიფიკაციის ორფაქტორიანი ტექნოლოგია, რომლის დროსაც ხდება გათვალისწინება იმისა რაც თქვენ გაქვთდა იმასა

რაც თქვენ იცით, ტიპიური მაგალითია ორფაქტორიანი აუტენტიფიკაცისა წარმოადგენს ბანკომატი, რომელიც ამოგიცნობთ თქვენ, ჯერ ერთი თქვენი პლასტიკური ბარათით და მეორე თქვენი პინ კოდით. აუტენტიფიკაციისათვის OTP-სისტემაში აგრეთვე მოითხოვება პინ კოდი და თქვენი პირადი ბარათი. ”ბარათი”(Token) ის ქვეშ იგულისხმება აპარატურულ ან პროგრამული საშუალება, რომელიც აგენირირებს უნიკალურ(შემთხვევითი შერჩევის პრინციპით) ერთმომენტიან, ერთჯერად პაროლს. თუ ჰაკერი გაიგებს მოცემულ პაროლს სნიფერის საშუალებით, მისთვის ეს ინფორმაცია იქნება გამოუსა-დეგარი, რადგანაც ეს პაროლი უკვე იქნება გამოყენებული და უვარგისი შემდგომი გამოყენებისთვის ავღნიშნოთ, რომ ეს ხერხი სნიფინგის საწინააღმდეგოდ საბრძოლველად ეფექტურია მხოლოდ პაროლის დაჭერის შემთხვევაში, სნიფერი, რომელიც დაჭერს სხვა ინფორმაციას (მაგ. ელ ფოსტის ინფორმაციას) არ კარგავს თავის ეფექტურობას.

აუტენტიფიკაციის პროტოკოლი. აუტენტიფიკაცია ამოწმებს კომუნიკაციის დროს პირის უტყუარობას. დაშორებული პროცესის უტყუარობის შემოწმება ითხოვს რთულ პროტოკოლებს, დამყარებულს კრიპტოგრაფიაზე.

აღსანიშნავია, რომ ხშირად ერთმანეთში ურევენ აუტენტიფიკაციას და ავტორიზაციას. აუტენტიფიკაცია დაკავებულია მოსაუბრის უტყუარობის შემოწმებით, ავტორიზაციას კი საქმე აქვს ნებართვებთან. მაგალითად პროგრამა კლიენტი მიმართავს ფაილურ სერვერს და ეუბნება: "მე ვარ პროცესი A და მინდა test.doc ფაილის წაშლა".

ფაილურმა სერვერმა უნდა გადაწყვიტოს:

1. არის თუ არა სინამდვილში ეს პროცესი A? (აუტენტიფიკაცია)
2. აქვს თუ არა A-ს test.doc ფაილის წაშლის უფლება? (ავტორიზაცია)

მხოლოდ იმის შემდეგ, რაც ორივე კითხვაზე იქნება არაორაზროვანი პასუხი გაცემული, შესაძლებელია განხორციელდეს მოთხოვნილი მოქმედება. მნიშვნელოვანი არის პირველი კითხვა. მას შემდეგ, რაც სერვერმა იცის თუ ვის ელაპარაკება, უფლების შესამოწმებლად საჭიროა მხოლოდ ცხრილების ლოკალურად შემოწმება.

ყველა აუტენტიფიკაციის პროტოკოლის მიერ გამოყენებული საერთო სქემა შემდეგნაირია:

მომხმარებელს (პროცესს) A-ს, სურს დაამყაროს დაცული კავშირი მეორე მომხმარებელთან, B-სთან. B ბანკირია და A-ს უნდა მასთან საქმიანი გარიგება. A იწყებს იმით, რომ უგზავნის B-ს შეტყობინებას, ან ნდობით აღჭურვილ გასაღებების გამავრცელებელ ცენტრს (KDC – key distribution center). შემდეგ მრავალი მიმართულებით აგზავნის კიდევ რამოდენიმე შეტყობინებას. ამის შემდეგ ბოროტმიქმედმა შეიძლება დაიჭიროს, შეცვალოს და ხელახლა შექმნას ეს შეტყობინება იმისათვის, რომ მოატყუოს A და B ან უბრალოდ ჩაშალოს გარიგება.

ასე თუ ისე, როდესაც პროტოკოლი ამთავრებს თავის მუშაობას, A უნდა იყოს დარწმუნებული, რომ ელაპარაკება B-ს, ხოლო B — კი A-ს. ბევრ პროტოკოლში მოსაუბრეები ქმნიან სეანსის საიდუმლო გასაღებს, რომლითაც მომხმარებლები გაცვლიან შემდგომ ინფორმაციას. პრაქტიკაში მონაცემთა ყველა გაცვლა იშიფრება სიმეტრიული ალგორითმის გამოყენებით,

რადგან სიმეტრიული ალგორითმის მწარმოებლურობა გაცილებით მაღალია გარდა ასიმეტრიული ალგორითმების. მიუხედავად ამისა, ასიმეტრიული ალგორითმები, ფართოდ გამოიყენება აუტენტიფიკაციის პროტოკოლებში სეანსის გასაღების შესაქმნელად.

სეანსის გასაღები იქმნება კავშირის ყოველ კონკრეტულ სეანსზე და იძლევა საშუალებას უზრუნველვყოთ ინფორმაციის მეტი დაცვა. თუ ბოროტმოქმედმა დაიჭირა ერთ სეანსზე გადაცემული ინფორმაცია და მოახერხა მისი შიფრვის გასაჯების გამოთვლა, მას ეს გასაღები აღარ გამოადგება შემდეგ სეანსზე.

აუტენტიფიკაცია დამყარებული საერთო საიდუმლო გასაღებზე. განვიხილოთ აუტენტიფიკაციის პროტოკოლი საერთო საიდუმლო გასაღებით. A-ს და B-ს აქვთ საერთო საიდუმლო გასაღები KAB. ამ საიდუმლო გასაღების შეთანხმება შესაძლებელია პირადი შეხვედრისას, ან ტელეფონით, მაგრამ არა დაუცველი ქსელის საშუალებით.

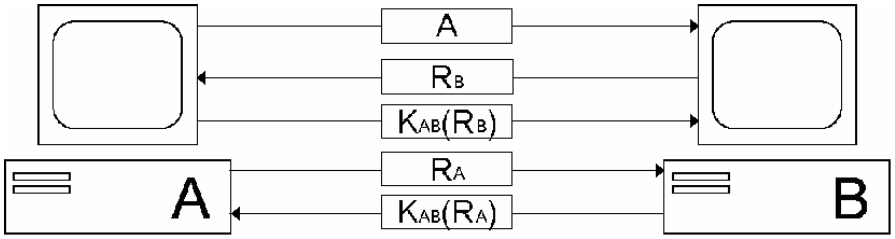
ამ პროტოკოლს საფუძვლად უდევს პრინციპი, გამოყენებული მრავალ აუტენტიფიკაციის პროტოკოლში: ერთი მხარე უგზავნის მეორეს შემთხვევით რიცხვს, რომელსაც მეორე მხარე გარდაქმნის განსაკუთრებული მეთოდით და აბრუნებს რეზულტატს. ასეთ პროტოკოლებს ეწოდებათ პროტოკოლები ტიპისა "გამოძახება-პასუხი". ამ და შემდგომ აუტენტიფიკაციის პროტოკოლებში იქნება გამოყენებული შემდეგი პირობითი აღნიშვნები:

Ri — პასუხი, სადაც ინდექსი აღნიშნავს მის გამგზავნს.

Ki — გასაღები, სადაც ინდექსი აღნიშნავს გასაღების მფლობელს.

Ks –სეანსი გასაღები.

აუტენტიფიკაციის პროტოკოლის შეტყობინებების თანმიმდევრობა ნაჩვენებია ნახ. 1-ზე. თავიდან A უგზავნის თავის პირადობის მოწმობას B-ს იმ სახით, რომელიც გასაგებია B-სთვის. B-მ რა თქმა უნდა არ იცის მოვიდა თუ არა ეს შეტყობინება A-სგან, თუ ბოროტმოქმედისაგან. ამიტომ ის ირჩევს დიდ შემთხვევით რიცხვს RB-ს და უგზავნის პასუხად A-ს.



ნახაზი 1

შემდეგ A დახურული გასაღებით შიფრავს ამ შეტყობინებას და მიღებულ რეზულტატს KAB(RB)-ს უგზავნის B-ს. როდესაც B მიიღებს ამ შეტყობინებას, ის იგებს, რომ ეს შეტყობინება მოვიდა A-სგან, რადგანაც ბოროტმოქმედს არ შეეძლო ქონოდა გასაღები KAB და ამიტომ არ შეეძლო შეექმნა ეს შეტყობინება. უფრო მეტიც, პასუხი RB აირჩა შემთხვევით დიდი რიცხვების ჯგუფიდან (მაგ. 128 ბიტიანი შემთხვევითი რიცხვებიდან) და ნაკლებად სავადუდოა, რომ ბოროტმოქმედმა შეძლო წინა სეანსებში პასუხის ნახვა და ძველი პასუხის გამოყენება.

ამ მომენტისთვის B დარწმუნებულია, რომ ლაპარაკობს A-სთან, მაგრამ A ჯერ კიდევ არ არის დარწმუნებული არაფერში.

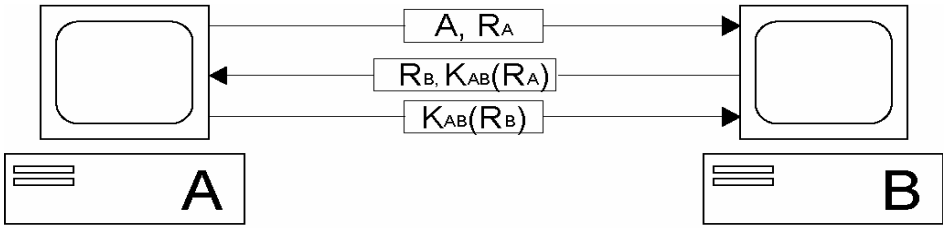
ბოროტმოქმედს შეეძლო დაეჭირა პირველი შეტყობინება და გამოეგზავნა უკან პასუხი RB. შესაძლებელია B საერთოდ არ არსებობს.

შემდეგ პროტოკოლი მუშაობს სიმეტრიულად:

A აგზავნის RA-ს და B პასუხობს მას. უკვე ორივე მხარე დარწმუნებულია, რომ ლაპარაკობენ ზუსტად ისინი, რადაც თავი მოქონდათ. ამის შემდეგ მათ შეუძლიათ შექმნან სეანსის გასაღები KS, რომელიც შეიძლება გადაუგზავნონ ერთმანეთს კოდირებული იგივე საერთო KAB გასაღებით.

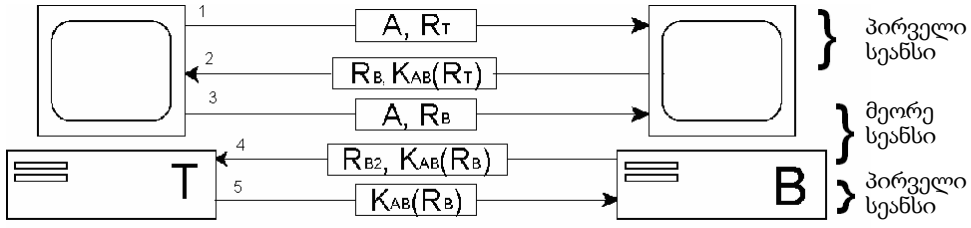
ამ პროტოკოლებში შეტყობინების რაოდენობა შეიძლება შემცირდეს ნახ. 2-ზე მოცემული სქემის მიხედვით.

ეს პროტოკოლი წინაზე კარგია იმით, რომ ის უფრო მოკლეა. მაგრამ ამ პროტოკოლით სარგებლობა არაა რეკომენდირებული. ზოგიერთ შემთხვევაში ბოროტმოქმედმა შეიძლება განახორციელოს თავდასხმა ამ პროტოკოლზე, რომელიც ცნობილია სახელით ”სარკისებური შეტევა”. კერძოდ, ბოროტმოქმედს შეუძლია პროტოკოლის გატეხვა, თუ მას ეძლევა შესაძლებლობა B-სთან გახსნას რამოდენიმე სეანსი ერთდროულად. რაც სრულებით შესაძლებელია, თუ B ბანკია და რომლისთვისაც ნებადართულია ერთდროულად რამოდენიმე კავშირი ბანკომატთან.



ნახ. 2

სარკისებური შეტევის სქემა ნაჩვენებია ნახ.3-ზე. ის იწყება იმით, რომ ბოროტმოქმედს (T) თავი მოაქვს A-დ და უგზავნის პასუხს RT B-ს. B უბრუნებს პასუხის პასუხს RB. რის შემდეგ თითქოს ბოროტმოქმედი უნდა აღმოჩნდეს ჩიხში. რა ქნას როდესაც არ იცის როგორ გამოითვალოს KAB(RB)? ბოროტმოქმედს შეუძლია გახსნას მეორე სესია და გაუგზავნოს B-ს პასუხად ისევ B-ს პასუხი RB, რომელიც მან აიღო B-სთან პირველი სესიის გახსნისას. B მშვიდად შიფრავს მას და უგზავნის მას უკან KAB(RB). ბოროტმოქმედს უკვე აქვს აუცილებელი ინფორმაცია, ამიტომ ის წყვეტს მეორე სესიას და ასრულებს პირველ სესიას. B უკვე დარწმუნებულია, რომ ბოროტმოქმედი არის — A, ამიტომ ის ბოროტმოქმედს აძლევს A-ს საბანკო ანგარიშებზე წვდომას და ნებას რთავს გადარიცხოს თანხა მიმდინარე ანგარიშიდან ბოროტმოქმედის საიდუმლო ანგარიშზე ყოველგვარი ყოყმანის გარეშე.



ნახ. 3

არსებობს სამი საერთო წესი, რომლის გამოყენებაც ხშირად სასარგებლოა:

1. სეანსის ინიციატორმა უნდა დაამოწმოს საკუთარი თავი მოპასუხე მხარეზე ადრე. ამ შემთხვევაში ბოროტმოქმედი ვერ შეძლებს მიიღოს ღირებული ინფორმაცია მანამ, სანამ ის არ დაადასტურებს საკუთარ პიროვნებას.

2. საჭიროა გამოვიყენოთ ორი გასაღები KAB და K'AB, ერთი ინიციატორისთვის მეორე კი მოპასუხისათვის.

3. ინიციატორმა და მოპასუხემ უნდა აირჩიოს პასუხები განსხვავებული არამკვეთი რიცხვების სიმრავლიდან. მაგალითად თუ ინიციატორი აირჩევს წყვილ რიცხვებს და მოპასუხე მხარე კენტ რიცხვებს.

წინა მაგალითზე ყველა ეს პირობა იყო დარღვეული, რამაც მიგვიყვანა უარყოფით შედეგებამდე.

ნიდჰემ-შროდერის აუტენტიფიკაციის პროტოკოლი

უფრო რთული აუტენტიფიკაციის მეთოდი გულისხმობს მრავალ გამოძახება-პასუხის მრავალმხრივ გამოყენებას. კარგადაა

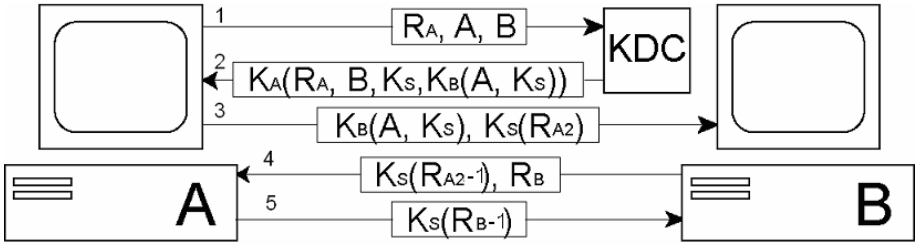
ცნობილი ნიდჰემ-შროდერის ასეთი პროტოკოლი. ნახ. 4-ზე მოცემულია მისი მუშაობის სქემა.

პროტოკოლის მუშაობა იწყება იმით, რომ A ატყობინებს ნდობით აღჭურვილ გასაღებების გამავრცელებელ ცენტრს (KDC), რომ მას უნდა საუბარი B-სთან. ეს შეტყობინება შეიცავს A-ს და B-ს იდენტიფიკატორებს და დიდ შემთხვევით რიცხვს RA–ს.

KDC უგზავნის A-ს პასუხს, რომელიც დაშიფრულია KA გასაღებით და შეიცავს A-ს გაგზავნი შემთხვევით რიცხვს RA და სეანსის გასაღებს KS, რომელსაც უწოდებან აგრეთვე ბილეთს და რომელიც მან შეუძლია გაუგზავნოს B-ს. მთავარი მიზანი შემთხვევითი რიცხვის გაგზავნისა არის ის, რომ A-ს შეტყობინება ახალია, ანუ მიმდინარე, და არა განმეორებული. გარდა ამის მეორე შეტყობინებაში თავსდება B-ს იდენთიფიკატორი. აგრეთვე სეანსის გასაღები და A-ს იდენტიფიკატორი დაშიფრული B-ს გასაღებით KB(A, KS). თუ ბოროტმოქმედი შეცვლის B-ს იდენტიფიკატორს საკუთარი იდენტიფიკატორით პირველ შეტყობინებაში, მაშინ KDC ცენტრი დაშიფრავს ბილეთს მეორე შეტყობინების ბოლოში გასაღებით KT, ნაცვლად გასაღებისა KB. ბილეთი დაშიფრული გასაღებით KB თავსდება დაშიფრული შეტყობინების შიგნით იმისათვის, რომ ბოროტმოქმედმა ვერ შეძლოს შეცვალოს ის სხვა გასაღებით მანამ, სანამ მეორე შეტყობინება არ მიაღწევს A-მდე.

ამის შემდეგ მესამე შეტყობინებაში A უგზავნის ბილეთს KB(A, KS) B-ს ახალ შემთხვევით რიცხვთან RA2-თან ერთად, რომელიც დაშიფრულია სეანსის გასაღებით. მეოთხე შეტყობინებაში B უგზავნის უკან A-ს KS(RA2–1), იმისათვის რომ A დარწმუნდეს, რომ ის ელაპარაკება B-ს. უკან გადაგზავნა მხოლოდ KS(RA2) არ შეიძლება, იმიტომ რომ ეს რიცხვი შესაძლებელია

ყოფილიყო მოპარული მესამე შეტყობინებიდან ბოროტმოქმედების მიერ.



ნახ. 4

მეოთხე შეტყობინების მიღების შემდეგ A რწმუნდება, რომ ლაპარაკობს B-სთან, მაგრამ B ჯერ კიდევ არ არის დარწმუნებული, რომ საუბრობს A-სთან. მეორე შემთხვევითი რიცხვის RA2 გაგზავნისა და KS(RA2-1) პასუხის მიღებას შორის გადის ძალიან ცოტა დრო. მეხუთე შეტყობინების მიზანია B-ს დარწმუნება იმაში, რომ საუბრობს A-სთან.

მიუხედავად ასეთი სოლიდური ალგორითმისა, მასაც აქვს სუსტი წერტილი. თუ ბოროტმოქმედს მიეცა შესაძლებლობა მიიღოს ძველი სეანსის გასაღები KS, მას შეუძლია ინიცირება გაუკეთოს ახალ სეანს B-სთან, თავიდან წარმოქმნას მესამე შეტყობინება კომპრომენტირებული სეანსის გასაღებით, და თავი გაასაღოს A-დ. ამ შემთხვევაში ბოროტმოქმედს შეუძლია მოპაროს თანხა A-ს.

კიდევ ერთი ხერხი სნიფინგთან საბრძოლველად არის კომუტირებადი ინფრასტრუქტურის შექმნა. თუ მაგალითად მთელ ორგანიზაციაში გამოიყენება კომუტირებადი Ethernet -ი, ჰაკერებს შეუძლიათ მიიღონ წვდომა მხოლოდ იმ ტრაფიკზე, რომელიც მოდის პორტიდან, რომელზეც თვითონ არიან მიერთებული. კომუტირებად ინფრასტრუქტურა ვერ მოხსნის სნიფინგის პრობლემას, მაგრამ ის მნიშვნელოვნად ამცირებს მას.

ანტისნიფერები

მესამე გზა მასთან საბრძოლველად მდგომარეობს აპარატურული ან პროგრამული საშუალებების დაყენებაში რომლებიც ამოიცნობენ სნიფერებს, რომლებიც მუშაობს ჩვენ ქსელში. ამ საშუალებებს არ შეუძლიათ საბოლოოდ გაუკეთონ ლიკვიდაცია საშიშროებას, მაგრამ, მრავალ სხვა საშუალებებთან ერთად ისინი ერთვებიან საერთო დაცვის სისტემაში. ანტისნიფერები ზომავენ ჰოსტების რეაგირების დროს და განსაზღვრავენ ხომ არ უხდებათ მათ ზედმეტი ტრაფიკის დამუშავება.

კრიპტოგრაფია

ეს არის ყველაზე ეფექტური საშუალება სნიფინგის საწინააღმდეგოდ საბრძოლველად, თუმცა ის ვერ უზრუნველყოფს ტრაფიკის დაჭერის აღკვეთას და ვერ ცნობს სნიფერის მუშაობას, თუმცა მისთვის ამ მუშაობის შესრულება გამოუსადეგარია. თუ არხი კრიპტოგრაფიულად დაცულია მაშინ ჰაკერი იჭერს არა შეტყობინებას არამედ დაშიფრულ ტექსტს (ე.ი ბიტების გაუგებარ

თანმიმდევრობას). Cisco - ს კრიპტოგრაფია იყენებს ქსელურ დონეზე IPSec პროტოკოლს, რომელიც წარმოადგენს სტანდარტულ მეთოდს, ქსელურ მოწყობიილობებს შორის დაცული კავშირის შესაქმნელად. სხვა კრიპტოგრაფიული პროტო-კოლები, რომელსაც იყენებენ ქსელური მართვისათვის არის SSh (Secure Shell) და SSL (Secure Socket Layer)

კოდირების სისტემები.

ინფორმაციის კრიპტოგრაფიული დაცვის მეთოდები საინფორმაციო უსაფრთხოების საფუძველს წარმოადგენს. კრიპტოგრაფიული მეთოდები დაფუძნებულია ინფორმაციის კრიპტოგრაფიულ გარდაქმნებზე, რომლებიც ცვლიან საწყის ინფორმაციას ისე, რომ გამორიცხული იქნეს ამ ინფორმაციის არა-სანქცირებული წაკითხვა და მოდიფიკაცია.

არსებობს ინფორნმაციის შემდეგი სახის კრიპტოგრაფიული გარდაქმნები:

1. დაშიფრვა - ღია გზავნილების კრიპტოგრაფიული გარდაქმნა დახურულ გზავნილებად.
2. გაშიფრვა - დახურული გზავნილების კრიპტოგრაფიული გარდაქმნა ღია გზავნილებად.
3. კრიპტოანალიზი - დახურული გზავნილიდან ღია გზავნილის მიღება იმ დროს, როცა უცნობია კრიპტოგრაფიული გარდაქმნა.

ღია გზავნილი შეიძლება იყოს ბიტების ნაკადის, ქსელური ფრეიმის, ფაილის ან სხვა სახით წარმოდგენილი.

ჩვეულებრივ დაშიფრვის და გაშიფრვის პროცესი წარმოებს სპეციალური გასაღებების და კრიპტოგრაფიული ალგორითმების გამოყენებით.

კრიპტოგრაფიული გარდაქმნების დროს გამოიყენება **შეცვლის** და **გადასმის** მეთოდები. ჩვეულებრივ კრიპტოგრაფიულ ალგორითმებში ორივე გარდაქმნაა კომბინირებული.

შეცვლის გარდაქმნა გულისხმობს ერთი სიმბოლოს (ბიტური კომბინაციის) შეცვლას სხვა სიმბოლოთი (ბიტური კომბინაციით). მაგ., თუ ღია გზავნილია $A_1A_2A_3A_4...A_N$, დახურული გზავნილი შეიძლება იყოს $B_1B_2B_3B_4...B_N$, ხოლო გადასმის შემთხვევაში ვთქვათ $A_3A_NA_4A_1...\ A_2$.

შიფრვის ალგორითმები შემდეგნაირად კლასიფიცირდება:

1. სიმეტრიული

   ა. ბლოკური

   ბ. ნაკადური

2. ასიმეტრიული

სიმეტრიული ალგორითმები ხასიათდება შიფრვის და გაშიფრვის ერთი გასაღებით, რომელიც საიდუმლოდ ინახება და გადაიცემა ჩვეულებრივ უსაფრთხო კავშირის გამოყენებით. ბლოკური შიფრვის ალგორითმები გარდაქმნებს გზავნილის თითოეულ ბლოკზე ცალცალკე ახდენენ. ეს ალგორითმები ძირითადად ცალკე აღებული მთლიანი გზავნილის, რომელიც წარმოდგენილია მაგალითად ფაილის სახით, შიფრვის დროს გამოიყენება. ნაკადური ალგორითმები გზავნილის თითოეულ სიმბოლოს ცალკე შიფრავენ, მათი შიფრატორზე მოსვლისთანავე. ასეთი ალგორითმები გამოიყენება მაგალითად გასაიდუმლოებული სატელეფონო კავშირის დროს.

ასიმეტრიული ალგორითმები ხასიათდება ორი, ღია და დახურული გასაღებით. პირველი მათგანი გამოიყენება შიფრვის, ხოლო მეორე გაშიფრვის დროს. ეს ალგორითმები იძლევა საშუალებას გადავცეთ ღია გასაღებები კავშირის ღია არხებით. შვეულებრივ გასაღებების გენერაციას ახდენს მიმღები მხარე და

უგზავნის ღია გასაღებს გადამცემ მხარეს. ხოლო დახურულგასაღებს ინახავს საიდუმლოდ.

სიმეტრიული შიფრვის ალგორითმები. არსებობს შემდეგი სახის სიმეტრიული შიფრვის ალგორითმები:

1. მარტივი შეცვლის ანუ ელექტრონული კოდური წიგნის ალგორითმი;
2. გამირების ალგორითმები.

მარტივი შეცვლის ანუ ელექტრონული კოდური წიგნის ალგორითმი. ამ მეთოდით შიფრვის დროს ხდება ღია გზავნილის თითო ბლოკის შეცვლა დახურული გზავნილის თითო ბლოკით. თეორიულად შესაძლებელია ე.წ. კოდური წიგნის ანუ ყველა ღია ბლოკის შესაბამისი დახურული ბლოკის ცხრილის შედგენა. თუ ბლოკის სიგრძეა 1 ბაიტი (8 ბიტი), მაშინ ასეთი წიგნის ზომა იქნება 2^8=256 ჩანაწერს.

დაშიფრვა შეიძლება აღვწეროთ ფორმულით:

$C_i=F(P_i)$, $i=1\div N$ -თვის

სადაც C_i და P_i შესაბამისად დაშიფრული და გაშიფრული ტექსტის ბლოკებია, ხოლო F კრიპტოგრაფიული გარდაქმნა.

ეს მეთოდი ყველაზე ნაკლებად საიმედოა შიფრაციის სხვა მეთოდებს შორის.

მარტივი კრიპტოსისტემები. კრიპტოგრაფიული მეთოდები არის ყველაზე ეფექტური ინფორმაციის დაცვის საშუალება ავტომატიზირებულ სისტემებში. კომპიუტერულ ქსელებსში ინფორმაციის გადაცემის დროს ისინი არიან ერთადერთი არასანქცირებული შეღწევის აღკვეთის საშუალება.

ნებისმიერი კრიპტოგრაფული მეთოდი ხასიათდება ისეთი ორი პარამეტრით როგორიც არის: ***მდგრადობა*** და ***სირთულე***

მეთოდის მდგრადობა არის დაშიფრული ტექსტის ის მოცულობა, რომლის სტატისტიკური ანალიზით შეიძლება საწყისი ტექსტის გახსნა. ან სხვანაირად რომ ვთქვათ: მდგრადობა განსაზღვრავს ინფორმაციის დაშვებულ მოცულობას, რომელიც შეიძლება დაშიფრული იყოს ერთი გასაღების გამოყენებით.

მეთოდის სირთულე განისაზღვრება ელემენტარული ოპერაციების რაოდენობით, რომლებიც საჭიროა ერთი საწყისი ტექსტის სიმბოლოს შიფრაციისთვის.

ძირითადი მოთხოვნები ინფორმაციის დაშიფრვის ავტომატიზირებულ სისტემებში:

შიფრაციის მეთოდი და სირთულე უნდა იყოს ამორჩეული მონაცემების მოცულობის და საიდუმლეობის შესაბამისად.

შიფრაციის საიმედობა უნდა იყოს ისეთი, რომ საიდუმლოება არ დაირღვეს იმ შემთხვევაშიც, როცა ცნობილია შიფრაციის მეთოდი.

შიფრაციის მეთოდი, გამოყენებული გასაღებების კრებული და მათი განაწილების მექანიზმი არ უნდა იყოს ძალიან რთული.

შიფრაციის და დეშიფრაციის გარდაქმნის პროცედურები არ უნდა იყოს დამოკიდებული დასაშიფრი ინფორმაციის მოცულობაზე.

შიფრაციის პროცედურების მიერ შემოტანილი ზედმეტიანობა უნდა იყოს მინიმალური.

შიფრაცია შეცვლით. ყველაზე მარტივი შიფრაციის მეთოდი. დასაშიფრი ტექსტის სიმბოლოები იცვლებიან სხვა ერთი ანბანიდან აღებული სიმბოლოებით (ერთანბანიანი შეცვლა) ან რამოდენიმე ანბანიდან (მრავალანბანიანი შეცვლა)

ერთანბანიანი შეცვლის მეთოდი - დასაშიფრი ტექსტის სიმბოლოების შეცვლა ამავე, ან სხვა ანბანის სიმბოლოებით.

მაგალითი:

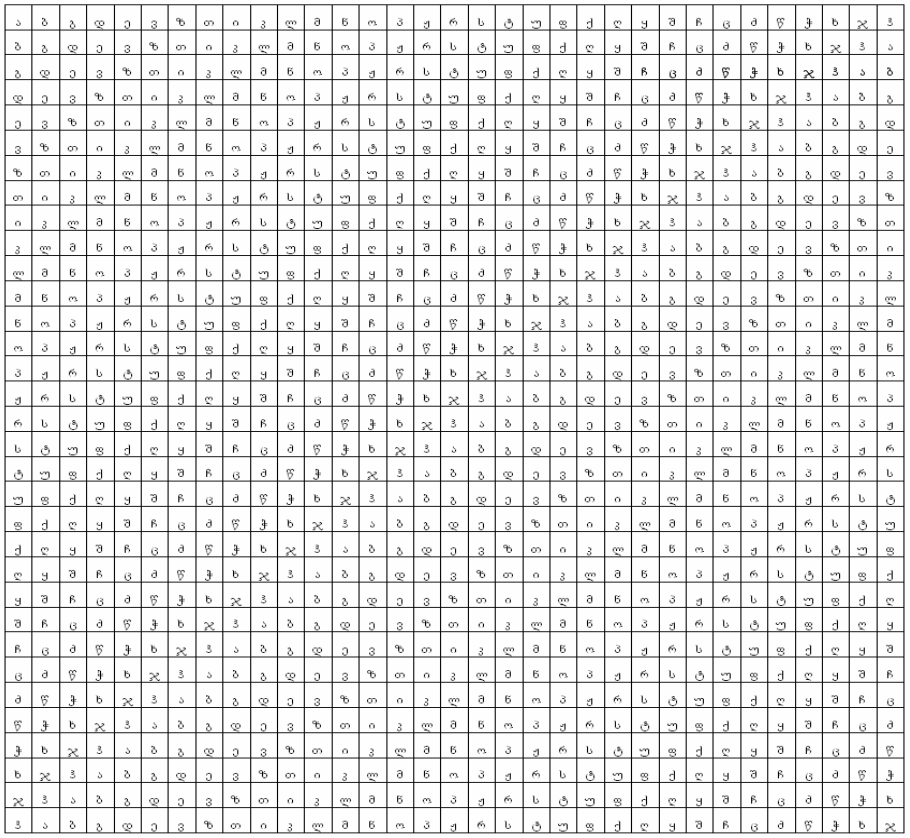
ა	ბ	გ	დ	ე	ვ	ზ	თ	ი	კ	ლ	მ	ნ	ო	პ	ჟ	რ	.	.
ჰ	მ	ნ	წ	ჯ	კ	ლ	ო	ქ	დ	ა	ბ	ც	ყ	უ	შ	თ	.	.

ერთანბანიანი მარტივი შეცვლის მეთოდის მდგრადობა ძალიან დაბალია, დაშიფრული ტექსტის სიმბოლოებს გააჩნია იგივე სტატისტიკური მახასიათებლები როგორც საწყის ტექსტს, სიმბოლოების სტანდარტული შეხვედრის სიხშირის ცოდნით იმ ენაში, რომელზეც დაწერილია შეტყობინება და სიმბოლოების სტატისტიკური შეხვედრის სიხშირესთან შედარებით დაშიფრულ ტექსტში, შეიძლება აღდგენილი იყოს შიფრაციის ცხრილი. ამისათვის საკმარისია დაშიფრული ტექსტის საკმარისი მოცულობა, იმისათვის რომ მივიღოთ სიმბოლოების სიხშირის შეფასება.

ამიტომ ერთანბანიანი მარტივი შეცვლის მეთოდს გამოიყენებენ იმ შემთხვევაში, როცა დასაშიფრი ტექსტი პატარაა.

მეთოდის მდგრადობა უდრის 20-30, სირთულე განისაზღვრება სიმბოლოს მოძებნით შეცვლის ცხრილში.

მრავალანბანიანი შეცვლის მეთოდი - სიმბოლოების შესაცვლელად გამოიყენება რამოდენიმე ანბანი, ანბანები ამოირჩევა გასაღები სიტყვის ასოების შესაბამისად ისე, რომ სიტყვის ყოველი ასო შეესაბამება ანბანის პირველ ასოს, ანბანების შეცვლა ხორციელდება თანმიმდევრობით და ციკლურად: პირველი სიმბოლო იცვლება შესაბამისი სიმბოლოთი პირველი ანბანიდან, მეორე სიმბოლო - შესაბამისი სიმბოლოთი მეორე ანბანიდან და ასე შემდეგ, სანამ არ გამოილევა ყველა ანბანი.



განვიხილოთ შიფრაცია ვიჯინერის ცხრილის მიხედვით - კვადრატული მატრიცის n*2 ელემენტით, სადაც ნ, გამოყენებული ანბანის სიმბოლოების რაოდენობა. პირველ სტრიქონში არის საწყისი ანბანი, ყოველი შემდეგი მიიღება საწყისი ანბანის ერთი სიმბოლოების წანაცვლებით მარცხნივ ერთი სიმბოლოთი.

შიფრაციისთვის აუცილებელია გასაღები სიტყვის განსაზღვრა – სიტყვა, რომელშიც ასოები არ მეორდება, შეცვლის ცხრილი მიიღება შემდეგნაირად: დასაშიფრი ტექსტის სიმბოლოებს იღებენ პორველი სტრიქონიდან, ხოლო შეცვლის სტრიქონებს ადგენენ იმ სტრიქონებისგან, რომლის პირველი ასოები ემთხვევა გასაღები სიტყვის შესაბამის ასოს.

შიფრაციის და დეშიფრაციის დროს არ არის აუცილებელი წინასწარ შევინახოთ მეხსიერებაში მთელი ვიჯინერის ცხრილი, იმიტომ რომ ციკლური ჩანაცვლებით შეგვიძლია მივიღოთ ნებისმიერი სტრიქონი მისი ნომრის მიხედვით.

მეთოდის მდგრადობა უდრის მარტივი შეცვლის მეთოდის მდგრადობას გამრავლებულს L-ზე , სადაც L არის გასაღები სიტყვის სიგრძე.

შიფრაცია გადაადგილებით. გადაადგილების მეთოდით შიფრაციის დროს დასაშიფრი ტექსტის სიმბოლოები გადადგილდებიან გარკვეული წესების მიხედვით.

მარტივი გადაადგილების მეთოდი - ირჩევა შიფრაციის ბლოკი, რომელიც შედგება n სვეტებისგან და m სტრიქონებისგან და გასაღები რიცხვების თანმიმდევრობა, რომელიც ამოირჩევა ნატურალური რიცხვებიდან შემთხვევითი გადაადგილებით.

შიფრაცია ხდება შემდეგი თანმიმდევრობით:

1. დასაშიფრი ტექსტი იწერება სტრიქონებად გასაღები რიცხვების თანმიმდევრობის ქვეშ და წარმოქმნიან დასაშიფრ ბლოკს n*m-ზე
2. დასაშიფრი ტექსტი ამოიწერება სვეტებად, სვეტების მიხედვით, მზარდი გასაღები რიცხვების თანმიმდევრობის მიხედვით.

4	2	8	6
ი	ჩ	ქ	ა
რ	ე	თ	
ნ	ე	ლ	ა

მაგალითად:

დასაშიფრია ტექსტი: იჩქარეთ ნელა

შიფრაციის შედეგად მივიღებთ: ჩეეირნა აქთლ

დეშიფრაცია ხდება შემდეგნაირად:

1. დაშიფრილი ტექსტიდან გამოიყოფა ბლოკი n*m-ზე;
2. ბლოკი იყობა n ჯგუფებზე, რომლებშიც არის m სიმბოლო;
3. სტრიქონები ჩაიწერება შეცვლის ცხრილის შესაბამის სვეტებში;
4. გაშიფრული ტექსტი იკითხება სტრიქონების მიხედვით.

გამირების ალგორითმები. გამირების ალგორითმებში გამოიყენება სპეციალურად გენერირებული ბლოკების თანმიმდევრობა - გამა. გამის გენერაციისათვის ორივე მხარეს

ჩვეულებრივ იყენებენ ერთ გასაღებს და გამის გენერაციის ერთ ალგორითმს.

დაშიფრვა შეიძლება აღვწეროთ შემდეგი ფორმულით:

$C_i = P_i \oplus F(Y_i)$, $i=1 \div N$ -თვის

სადაც Y_i გამომუშავებული გამაა.

მაგალითისათვის შეგვიძლია მოვიყვანოთ შემდეგი სახის გარდაქმნა:

$C[i]=P[i] \oplus K[i \bmod len(K)]$

$P[i]=C[i] \oplus K[i \bmod len(K)]$

K[n] - კოდური სიტყვის n-ური სიმბოლოა

C[i] - დაშიფრული ტექსტის i-ური სიმბოლო

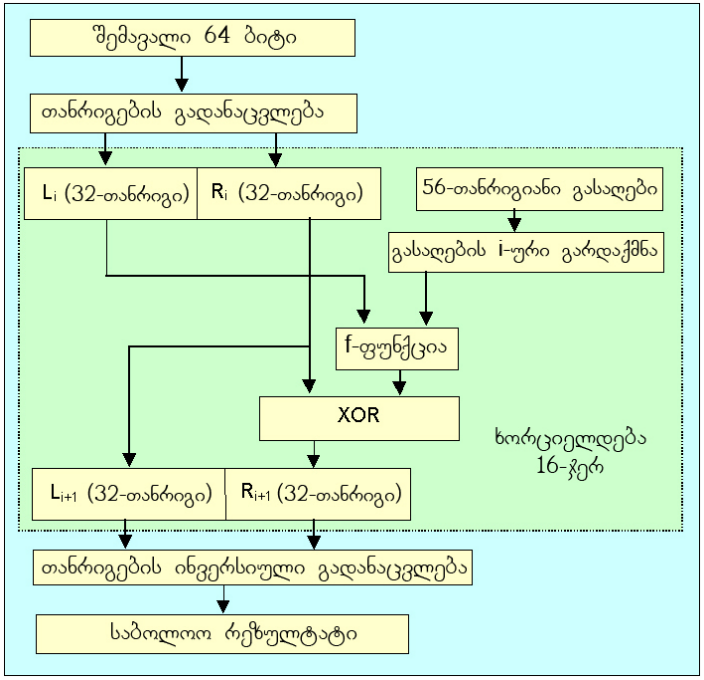
P[i] - საწყისი ტექსტის i-ური სიმბოლოა

len(K) - კოდური სიტყვის სიგრძეა

ალგორითმი DES. აშშ-ს სტანდარტების ეროვნული ბიუროს მიერ როგორც სახელმწიფო სტრუქტურებში ასევე კომერციულ ორგანიზაციებში რეკომენდირებული შიფრვის ალგორითმია Data Encryprion Standard (DES). ის შექმნილია 1977 წელს, თუმცა მისი მოდიფიკაცია გრძელდება და იქმნება მის საფუძველზე უფრო რთული და საიმედო ალგორითმები.

DES ბლოკური შიფრირების ალგორითმია. მასში გამოყენებულია როგორც შეცვლის, ასევე გადასმის მეთოდები. ბლოკის სიგრძე 64 ბიტია, ხოლო გასაღების 56 ბიტი. პრაქტიკაში გასაღები 64 ბიტია, თუმცა აქედან 8 ბიტი საკონტროლო ჯამებია.

ალგორითმი შემდეგნაირად სრულდება:



- თავიდან ხდება ბლოკის ბიტების არევა. ბიტები ლაგდება შემდეგი თანმიმდევრობით: (ციფრები მიუთითებს ბლოკის თანრიგის ნომერს)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

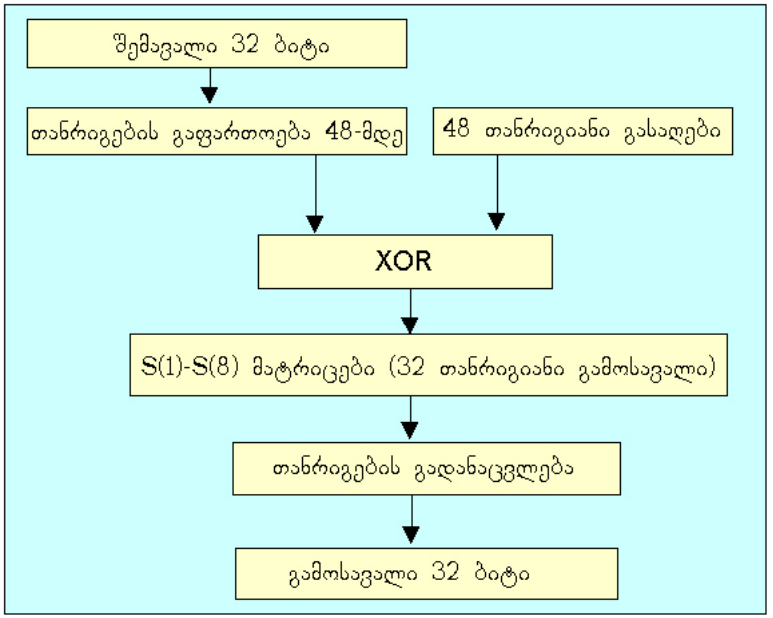
- შემდეგ 16-ჯერ მეორდება:
  - გასაღების გარდაქმნა

  - ითვლება ბლოკის მარჯვენა ნახევარი $R_{i+1}= R_i \oplus f(L_i,K_i)$
  - ბლოკის მარცხენა ნახევარში იწერება მარჯვენა ნახევარი $L_{i+1}=R_i$

- ბოლოს ხდება თანრიგების ინვერსიული გადანაცვლება შემდეგი თანმიმდევრობით:

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

f ფუნქციას ვითვლით შემდეგნაირად:



ფუნქციის პირველი არგუმენტი ფართოვდება 32 თანრიგიდან 48 თანრიგამდე ზოგიერთი თანრიგის გამეორებით შემდეგი სქემის მიხედვით:

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

შემდეგ ის იკრიბება მოდულით 2, 48 თანრიგიან გასაღებთან და გარდაიქმნება სპეციალური S მატრიცების გამოყენებით 32 თანრიგიან ბლოკად, რომლის თანრიგები კიდევ გადანაცვლდება შემდეგი სქემით:

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

მიღებული 32 თანრიგიანი ბლოკი წარმოადგენს f ფუნქციის მნიშვნელობას.

S მატრიცები წარმოადგენენ ცხრილებს 4 სტრიქონით და 16 სვეტით. მაგალითისათვის S(1) მატრიცას შემდეგი სახე აქვს:

14	4	13	1	2	15	11	8	3
	10	6	12	5	9	0	7	
0	15	7	4	14	2	13	1	10
	6	12	11	9	5	3	8	
4	1	14	8	13	6	2	11	15
	12	9	7	3	10	5	0	
15	12	8	2	4	9	1	7	5
	11	3	14	10	0	6	13	

S მატრიცების შემავალი 48 თანრიგი იყოფა რვა 6 თანრიგიან სიტყვად. სიტყვის პირველი 2 თანრიგი განსაზღვრავს სტრიქონის ნომერს, ხოლო დანარჩენი 4 თანრიგი მატრიცის სვეტის ნომერს. მატრიცის საშუალებით გარდაქმნის რეზულტატი სწორედ ამ უჯრედის მნიშვნელობაა.

გასაღების გარდაქმნა, რომელიც f ფუნქციის შემავალ 48 თანრიგიან გასაღებს იძლევა შემდეგი სქემით ხორციელდება:

- 56 თანრიგიანი გასაღები საწყისი გადანაცვლების შემდეგ იყოფა ორ 28 თანრიგიან სიტყვად. საწყისი გადანაცვლება აღიწერება შემდეგი მატრიცით:

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

- თითოეულ რაუნდში (სულ სრულდება 16 რაუნდი) ორივე რეგისტრი ციკლურად იძვრის მარცხნივ შემდეგი პრინციპით:
  - I, II, IX და XVI რაუნდებში ერთი თანრიგით;
  - დანარჩენ ღაუნდებში ორი თანრიგით.
- ყოველ რაუნდში ორი 28 თანრიგიანი სიტყვის გაერთიანებით მიღებული 56 თანრიგიან გასაღებს ემატება თითო თანრიგი ყოველი 7 თანრიგის საკონტროლო ჯამის (ჯამი მოდულით 2) სახით.
- მიღებული 64 თანრიგიდან ხდება ამორჩევა 48 თანრიგის შემდეგი ცხრილის მიხედვით (ცხრილის შესაბამისი ელემენტი მიუთითებს ამორჩეული თანრიგის ნომერს):

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

DES ალგორითმის გაშიფრვა ანალოგიურად ხდება. განსხვავება მხოლოდ გასაღებების ამორჩევის თანმიმდევრობაა რაუნდებში.

შიფრვის ასიმეტრიული ალგორითმები. დაშიფრვის მეთოდების განვითარება წარმოუდგენელია ასიმეტრიული

შიფრვის ალგორითმების გარეშე. ასიმეტრიული შიფრვის ალგორითმი დაკავშირებულია ე.წ. ცალმხრივი ფუნქციების თეორიასთან. ცალმხრივი ფუნცქციაა ისეთი ასახვა $f(x):X\to Y$, $x\in X$, რომლის შებრუნებული ასახვა რთულ ამოცანას წარმოადგენს.

ასიმეტრიული ალგორითმების გავრცელება გამოიწვია ორი გასაღების - ღია, დაშიფრვისთვის, და დახურული, გაშიფრვისთვის, ქონის აუცილებლობამ. ღია, ანუ ისეთი გასაღების შემოტანა, რომელიც პოტენციურად ყველასათვის ცნობილია, საშუალებას გვაძლევს თავი ავარიდოთ საიდუმლო გასაღებების გაცვლის რთულ ამოცანას.

განვიხილოთ შიფრვის ასიმეტრიული ალგორითმის სტანდარტი RSA.

შიფრვის ასიმეტრიული ალგორითმის სტანდარტი RSA. RSA წარმოადგენს შიფრვის ყველაზე გავრცელებულ ასიმეტრიულ ალგორითმს. ის იყოფა ორ ნაწილად:

1. გასაღებების გენერაცია
2. საკუთრივ შიფრვა

გასაღებების გენერაცია. ვირჩევთ ორ ძალიან დიდ მარტივ რიცხვს p-ს და q-ს

1. $n=p^*q$; $\varphi(n)=(p-1)^*(q-1)$.
2. ვირჩევთ დიდ შემთხვევით რიცხვს d-ს ისეთს, რომ ის იყოს ურთიერთ მარტივი $\varphi(n)$-თან (ანუ არ ჰქონდეს არცერთი მთელი საერთო გამყოფი გარდა 1-ისა)

3. ვსაზღვრავთ ისეთ მთელ რიცხვს e-ს, რომლისთვისაც ჭეშმარიტია შემდეგი ტოლობა: $(e^*d) \bmod \varphi(n)=1$ ღია გასაღებია (e,n), ხოლო დახურული (d,n).

საკუთრივ შიფრვა.

1. დასაშიფრი გზავნილი იყოფა ბლოკებად M_i ისე, რომ მისი ზომა k აკმაყოფილებდეს შემდეგ პირობას $10^{k-1}<n<10^k$
2. დაშიფრული გზავნილის შესაბამისი ბლოკის მნიშვნელობაა:
   $C_i=M_i^e \bmod n$

გზავნილის გაშიფრვისათვის ვიყენებთ დახურულ გასაღებს (d,n) და ვითვლით გაშიფრული გზავნილის ბლოკის მნიშვნელობას შემდეგი ფორმულით:

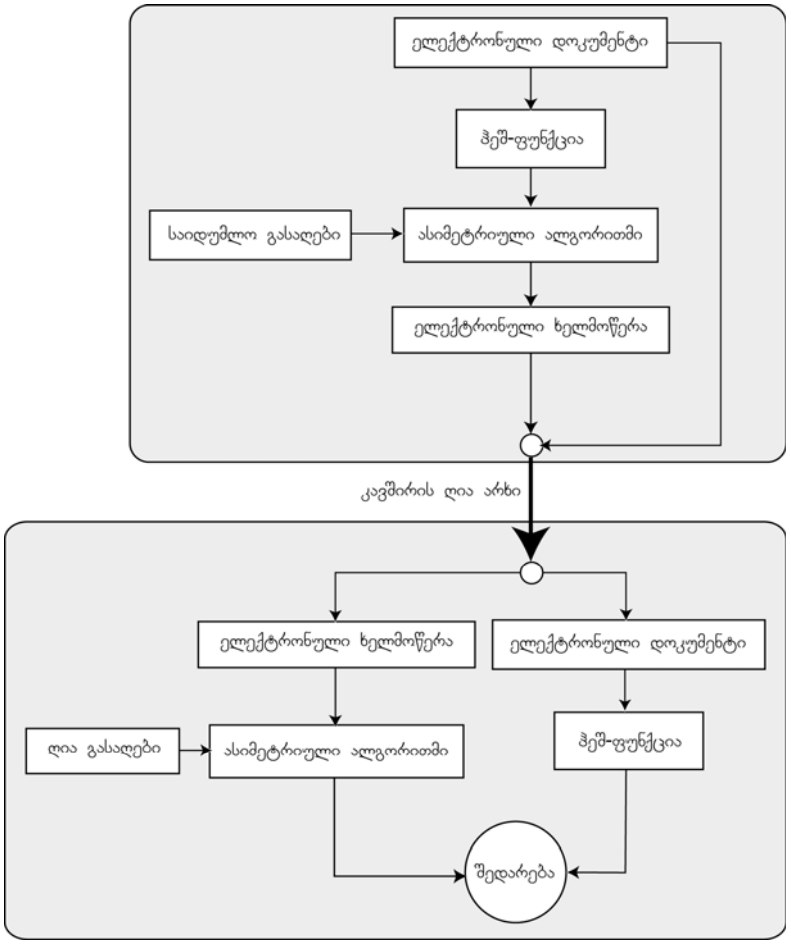
$M_i=C_i^e \bmod n$

ელექტრონული ხელმოწერა. ელექტრონული დოკუმენტების სარწმუნოების დასაბუთების საშუალებას ელექტრონული ხელმოწერა წარმოადგენს. ელექტრონული ხელმოწერის რეალიზაცია ხორციელდება შიფრვის ასიმეტრიული ალგორითმით, ოღონდ ამ შემთხვევაში ღიაა ის გასაღები, რომლითაც ხდება გაშიფრვა, ხოლო დახურულია დაშიფრვის გასაღები. იმისათვის, რომ ხელმოწერა მიბმული იყოს დოკუმენტზე, გამოიყენება დოკუმენტის ჰეშ-კოდი.

ელექტრონული დოკუმენტიდა ჰეშ-ფუნქციის გამოყენებით გენერირდება ჰეშ-კოდი, რომელიც საიდუმლო გასაღების

გამოყენებით შიფრვის ასიმეტრიული ალგორითმით იშიფრება და მიიღება ელექტრონული ხელმოწერა, რომელიც ებმება დოკუმენტს და იგზავნება ღია არხით ადრესატთან.

ელექტრონული ხელმოწერა შემდეგი სქემით ხორციელდება:



ადრესატი გამოყოფს ელექტრონულ ხელმოწერას, ახდენს მის გაშიფრვას ღია გასაღების გამოყენებით და ადარებს დოკუმენტის ჰეშ კოდს. თუ ისინი არ დაემთხვა, ე.ი. დოკუმენტი ან გაყალბებულია, ან შეცდომებით გადმოიცა კავშირის არხის საშუალებით.

განვიხილოთ ელექტრონული ხელმოწერის სტანდარტი DSA.

ელექტრონული ხელმოწერის სტანდარტი DSA

გასაღებების გენერაცია.

1. ვირჩევთ მარტივ რიცხვს q-ს, ისეთს, რომ $2^{159}<q<2^{160}$
2. ვირჩევთ t-ს ისეთს, რომ $0\le t\le 8$, და ვირჩევთ მარტივ რიცხვს p-ს, ისეთს, რომ $2^{511+64t}<p<2^{512+64t}$, თან q უნდა ყოფდეს (p-1)-ს
3. ვითვლით $g=h^{p-1/q} \bmod p$, სადაც h ნებისმიერი მთელი რიცხვია ისე, რომ $0<h<p$ და რომელიც აკმაყოფილებს პირობას $h^{p-1/q} \bmod p>1$

საიდუმლო გასაღები x ირჩევა შუალედიდან [1,q], ხოლო ღია გასაღები $y=g^x \bmod p$.

ყველა მომხმარებლისათვის ქვეყნდება p, q, g და y.

ელექტრონული ხელმოწერის გენერირება ხდება შემდეგნაირად:

1. ვითვლით დოკუმენტის ჰეშ-კოდს h=H(m)
2. შუალედიდან [1, q] შემთხვევით ვირჩევთ k-ს და ვითვლით $r=(g^k \bmod p) \bmod q$
3. ვითვლით $s=(k^{-1}(h+x*r)) \bmod q$, სადაც ელექტრონულ ხელმოწერას წარმოადგენს r და s.

მიღებული m დოკუმენტის და (r,s) ხელმოწერის შემოწმებისათვის:

1. ვამოწმებთ პირობას $0<r<q$ და $0<s<q$, და თუ ერთი მათგანი მაინც არ სრულდება ხელმოწერა ყალბია.
2. ვითვლით:
   $w=s_1^{-1} \bmod q$; $u1=(H(m)*w) \bmod q$; $u2=((r/w) \bmod q$; $v=((g^{u1}y^{u2}) \bmod p) \bmod q$
3. მოწმდება ტოლობა v=r. თუ ტოლობა სრულდება ელექტრონული ხელმოწერა მისაღებია.

მოცემულ ალგორითმში რეკომენდირებულია p-ს სიგრძე არა ნაკლებ 768 ბიტი. მაქსიმალური საიმედოობისათვის სასურველია 1024 ბიტის გამოყენება.

IP სპუფინგი

IP სპუფინგი ხდება იმ შემთხვევაში, როდესაც ჰაკერი იმყოფება კორპორაციის შიგნით, ან მის გარეთ და მოაქვს თავი, როგორც სანქცირებულ მომხმარებელს. ეს შესაძლებელია გაკეთდეს ორი გზით: ჰკაერმა შეიძლება ისარგებლოს ან IP მისამართით, რომელიც იმყოფება სანქცირებული IP მისამართების დიაპაზონში, ან ავტორიზებული გარე მისამართებით, რომლისთვისაც დასაშვებია წვდომა განსაზღვრულ ქსელურ რესურსებზე. შეტევები - IP სპუფინგის გზით, ხშირად წარმოადგენს საწყის წერტილს სხვა მსგავსი შეტევებისთვის. კლასიკური მაგალითი - შეტევა DoS, რომელიც იწყება უცხო მისამართიდან, რომელშიც ჰაკერი მალავს თავის ჭეშმარიტ ზრახვებს.

როგორც წესი, IP სპუფინგი შემოისაზღვრება მცდარი ინფორმაციის ან საზიანო ბრძანებების ჩასმით მონაცემთა ნაკადში, რომელიც გადაცემა კლიენტსა და სერვერს შორის ან ერთრანგიან მოწყობილობებს შორის ქსელში. ორმხრივი კავშირის უზრუნველყოფისათვის ჰაკერმა უნდა შეცვალოს მარშუტიზაციის ყველა ცხრილი, რომ ტრაფიკი მიმართოს მცდარი IP მისამართისკენ. ზოგიერთი ჰაკერი საერთოდაც არ ცდილობს მიიღოს პროგრამისგან პასუხი - თუ მისი მთავარი მიზანია სისტემისგან მნიშვნელოვანი ფაილის მიღება, მაშინ პროგრამისთვის პასუხებს არანაირი მნიშვნელობა არა აქვთ.

თუ ჰაკერს შეუძლია შეცვალოს მარშუტიზაციის ცხრილი და ტრაფიკი მიმართოს მცდარი IP მისამართისკენ, შესაბამისად ის მიიღებს ყველა პაკეტს, ამ შემთხვევაში მას შეუძლია პასუხი გასცეს, თითქოს ის არის სანქცირებული მომხმარებელი.

სპუფინგის საფრთხე შეიძლება შევამციროთ(მაგრამ არა აღნოფხვრათ) ქვემოთ ჩამოთვლილი ზომებით:

წვდომის კონტროლი. ყველაზე მარტივი გზა IP სპუფინგის აღკვეთისა დევს წვდომის კონტროლის სწორ განსაზღვრაში.

რომ შევამციროთ IP სპუფინგის ექექტურობა საჭიროა სწორად დავაყენოთ წვდომის კონტროლი,რომელიც მდგომარეობს ნებისმიერი ტრაფიკის ბლოკირებაში, რომელიც მოედინება გარედან, მაგრამ მისი გამომგზავნის მისამართი უნდა იმყოფებოდეს ქსელის შიგნით. მართალია ეს გვეხმარება IP სპუფინგთან საბრძოლველად, როდესაც სანქცირებულია მხოლოდ შიდა მისამართები; თუ სანქცირებულს წარმოადგენს

ზოგიერთი გარე მისამართიც, მაშინ მოცემული მეთოდი არაეფექტურია

ფილტრაცია RFC 2827. თქვენ შეგიძლიათ აგკრძალოთ უცხო ქსელების სპუფინგის მცდელობები თქვენი მომხმარებლებისათვის.

ამისათვის აუცილებელია ნებისმიერი გამავალი ტრაფიკი დაბრაკოთ, რომლის საწყისი მისამართი არ არის ორგანიზაციის მისამართებიდან რომელიმე ერთი. ამ ტიპის ფილტრაცია ცნობილია *RFC 2827.* სახელით. აღნიშნულის გაკეთება შეუძლია თქვენ პროვაიდერსაც.

შედარებით ეფექტური მეთოდი IP სპუფინგთან საბრძოლველად - იგივეა რაც, პაკეტების სნიფინგის შემთხვევაში. აუცილებელია რომ შეტევა გავხადოთ არაეფექტური. IP სპუფინგი შესაძლებელია ფუნქციონირებდეს მხოლოდ იმ პირობებში, როდესაც აუტენტიფიკაცია მიმდინარეობს IP მისამართების ბაზაზე. ამიტომ დამატებითი აუტენტიფიკაციის დანერგვის შემთხვევაში, მსგავსი შეტევები გახდება უსარგებლო. დამატებითი აუტენტიფიკაციის კარგი სახეა კროპტოგრაფიული.

მომსახურებაზე უარი

Denial of Service (DoS), არის ყველაზე ცნობილი ჰაკერული თავდასხმის ფორმა. გარდა ამისა მსგავსი ტიპის შეტევის საწინააღმდეგოდ ყველაზე ძნელია 100% -ანი დაცვა. ჰკერებს შორის DoS -ის ტიპის თავდასხმები ითვლება როგორც ბავშვური გასართობი, და იწვევს მათში ღიმილს, რადგანაც მისი

ორგანიზაციისთვის საჭიროა მინიმალური ცოდნა და ჭკუა. მიუხედავად ამისა სწორედ მისი მარტივად რეალიზაციის გამო მათ მოაქვთ უდიდსი ზიანი, ამიტომ ადმინისტრატორები მას უდიდეს ყურადღებას უთმობენ. ქვმოთ ჩამოთვლილია რამოდენიმე მათგანი:

TCP SYN Flood;

Ping of Death;

Trinco; და სხვა

DoS შეტევა განსხვავდება სხვა შეტევებისგან. ისნი არ არიან გამიზნული თქვენ ქსელში შესაღწევად, ან კიდევ თქვენ ქსელიდან რაიმე ინფორმაციის მისაღებად, მაგრამ DoS შეტევა გახდის თქვენ ქსელს გამუსადეგარს სხავა ნორმალური მომხმარებლებისათვის.

მას შეუძლია ამის მიღწევა ან ქსელის, ან ოპერაციული სისტემის, ან აპლიკაციის გამოყენების იმ დონემდე გაზრდამდე, რომელიც ზღუდავს ან აჩერებს მის ფუნქციონირებას. ზოგიერთი სერვერული პროგრამების გამოყენების შემთხვევაში(მაგ ვებ და ფტპ სერვერები)

DoS შეტევები გამოიხატება იმაში, რომ მან უნდა დაიკავოს ყველა კავშირი, ნებადართული ამ პროგრამების მიერ და დაიკავოს ისინი მუშა მდგომარეობაში, ამით ის არ უშვებს სხვა ჩვეულებრივ მომხმარებელს ამ სერვისამდე. DoS შეტევის დროს გამოიყენება ჩვეულებრივი ინტერნეტ პროტოკოლები, როგორიც არის TCP და ICMP

უმრავლესი DoS შეტევები გათვლილია პროგრამულ შეცდომებზე და სისტემის უსაფრთხოების ნაკლოვანებებზე და არა სისტემის არქიტექტურის საერთო სისუსტეზე. ზოგიერთ შეტევას

ქსელის მწარმოებლურობა დაყავს ნულზე, მისი არარეალური და უსარგებლო პაკეტების გადავსებით ან მცდარი ინფორმაციით ქსელიში რეალურად არსებულ მდგომარეობაზე. მსგავსი ტიპის თავდასხმების აღკვეთა ძნელია და მოითხოვს პროვაიდერთან კოორდინირებულ მუშაობას. თუ პროვაიდერთან არ გავაჩერებთ ტრაფიკს გამიზნულს თქვენი ქსელის გადასავსებად, მაშინ ამის გაკეთებას თქვენ ვერ შეძლებთ, რადგამც ქსელის შემომავალი არხი უკვე იქნება გადავსებული. თუ მსგავსი შეტევა ხორციელდება მრავალი მხრიდან, მაშინ საქმე გვავს განაწილებულ შეტევასთან, (Distributed DoS) DDoS

DoS -ის ტიპის შეტევის საფრთხე შესაძლებელია დაწეულ იქნას სამი გზით:

ანტისპუფინგური ფუნქციები. სწორმა ანტისპუფინგური ფუნქციის კონფიგურირებამ თქვენს მარშუტიზატორებში და ქსელთაშორის ეკრანებში შეიძლება შეამციროს DoS -ის შეტევის რისკი. ეს ფუნქციები როგორც მინიმუმ უნდა შეიცავდნენ *RFC 2827* ფილტრაციას. თუ ჰაკერს არ შეეძლება მასკირება გაუკეთოს მის ნამდვილ სახეს, მას ძნელად თუ შეეძლება შეტევის განხორციელება.

ანტი- DoS ფუნქციები. ანტი- DoS ფუნქციების სწორ კონფიგურირებას მარშუტიზატორებსა და ქსელთაშორის ეკრანებში შეუძლია შეზღუდოს შეტევის ეფექტურობა. ეს ფუნქციები ხშირად ზღუდავენ მიღებული პაკეტების რაოდენობას, ნებისმიერ მომენტში.

ტრაფიკის შეზღუდვა (Traffic rate limiting). ორგანიზაციას შეუძლია სთხოვოს პროვაიდერს შეზღუდოს ტრაფიკის მოცულობა.ამ ტიპის ფილტრაცია შესაძლებლობას გვაძლევს

შევზღუდოთ არაკრიტიკული ტრაფიკის მოცულობა, რომელიც გადის თქვენ ორგანიზაციაში. ტიპიურ მაგალითს წარმოადგენს ICMP ტრაფიკის მოცულობის შეზღუდვა, რომელიც გამოიყენება მხოლოდ დიაგნისტიკისათვის. DoS -ის შეტევები ხშირად იყენებენ სწორედ ICMP-ს პაკეტებს.

პაროლური შეტევა

ჰაკერებს შეუძლიათ განახორციელონ პაროლური შეტევა მთელი რიგი მეთოდების გამოყენებით, ისეთი როგორიც არის მარტივი გადარჩევა (brute force attack), ტროას ცხენი, IP სპუფინგი და პაკეტების სნიფინგი, თუმცა მოხმარებლისა და პაროლის მიღება შეაძლებელია IP სპუფინგისა და პაკეტების სნიფინგის გამოყენებით ჰაკერები იშვიათად ცდილობენ შეარჩიონ პაროლი და სახელი და მისთვის მრავალრიცხოვანი შერჩევის მცდელობით.

ხშირად მსგავსი შეტევისათვის გამოიყენება სპეციალური პროგრამები, რომელიც ცდილობს მიიღოს საერთო მოხმარების რესურსზე წვდომა(მაგ სერვერზე). თუ შედეგად ჰაკერს გაუჩნდება წვდომა რესურსებზე, მაშინ ის მიიღებს ამას, როგორც ჩვეულებრივი მომხმარებელი. თუ ამ მომხმარებელს აქვს მნიშვნელოვანი წვდომის პრივილეგია ჰაკერმა შეიძლება შექმნას თავისთვის ”გასასვლელი” მომავალში წვდომისათვის, რომელიც იმუშავებს თუნდაც მისი პაროლის ან სახელის შეცვლის შემდეგაც

კიდევ ერთი პრობლემა წარმოიქმნება, როდესაც მომხმარებლები იყენებენ ერთი და იგივე (თუნდაც ძალიან კარგს) პაროლს სხვადასხვა სისტემებთან წვდომისას: კორპორაციულ, პერსონალურ, და ინტერნეტ სისტემებთან. რამდენადაც პაროლის სიმდგრადე ტოლია ყველაზე სუსტი ჰოსტის სიმდგრადესთან, თუ

ჰაკერი, რომელმაც გაიგო პაროლი ამ ჰოსტის გზით, მიიღებს წვდომას ყველა დანარჩენ რესურსთან, სადაც გამოიყენება მსგავსი პაროლი.

პაროლური შეტევის ტავიდან აცილება შესაძლებელია თუ არ გამოვიყენებთ ტექსტური ფორმის პაროლებს. ერთჯერადი პაროლები და კრიპტოგრაფიული აუტენტიფიკაცია მინიმუმამდე ამცირებს მსგავს შეტევებს, მაგრამ ბევრ სისტემასა და ჰოსტებს არა აქვთ ამის მხარდაჭერა.

პაროლების გამოყენებისას ეცადეთ მოიფიქროთ ისეთი, რომელიც რთული იქნება შესარჩევად. მინიმალურ პაროლის სიგრძე არ უნდა იყოს 8 -ზე ნაკლები. პაროლები უნდა შეიცავდნენ სიმბოლოების მაღალ და დაბალ რეგისტრებს, ციფრებს, სპეც ნიშნებს. კარგი პაროლები რთული შესარჩევი და დასამახსოვრებელია, რაც აიძულებს მომხმარებლებს ჩაიწეროს ისინი ფურცლებზე. ეს რომ არ მოხდეს არის მომხმარებლებს და ადმინისტრატორებს შეუძლიათ გამოიყენონ ტექნოლოგიური სიახლეები, მაგ არსებობს გამოყენებითი პროგრამები რომლებიც შიფრავს პაროლების სიას, და რომელიც შეიძლება შევინახოთ ჯიბეში. საბოლოოდ მომხმარებელს უწევს ერთი რთული პაროლის დამახსოვრება, რამდენადაც დაბარჩენი პაროლები საიმედოდ იქნება შენახული პროგრამის მიერ.

Man-in-the-Middle შეტევა

Man-in-the-Middle შეტევისთვის ჰაკერს სჭირდება პაკეტებთან წვდომა რომელიც გადაიცემა ქსელით. მსგავსი წვდომა ყველა პაკეტთან გადაცემული პროვაიდერის მიერ ნებისმიერ სხვა ქსელში, შესაძლებელია, მაგ მიიღოს პროვაიდერის

თანამშრომელმა. მსგავსი შეტევისათვის ხშირად იყენებენ პაკეტების სნიფერებს, სატრანსპორტო პროტოკოლებს და მარშუტიზაციის პროტოკოლებს. შეტევა ხორციელდება: 1) ინფორმაციის მოპარვის მიზნით, 2)მიმდინარე სესის დასაჭერად და ცალკეულ ქსელურ რესურსებთან წვდომისათვის, 3) ტრაფიკის ანალიზისათვის, რომ მიიღოს ინფორმაცია ქსელზე და იქ არსებულ მომხმარებლებზე 4) DoS შეტევისათვის, 5) ტრაფიკის არეკვლისათვის რომ გამოვლინდეს არასანქცირებული ინფორმაცია ქსელურ სესიაში.

Man-in-the-Middle შეტევის წინააღმდეგ ეფექტურად საბრძოლველად შესაზლებელია მხოლოდ კრიპტოგრაფიის გამოყენება. თუ ჰაკერი დაიჭერს ინფორმაციას დაშიფრული სესიით, მას ეკრანზე გამოუვა არა დაჭერილი ინფორმაცია არამედ უაზრო სიმბოლოების თანმიმდევრობა. აღსანიშნავია, რომ თუ ჰაკერი მიიღებს ინფორმაციას კრიპტოგრაფიულ სესიაზე (მაგ. სესიის გასაღები), მაშინ მას შეუძლია განახორციელოს Man-in-the-Middle შეტევა დაშიფრულ გარემოშიც კი.

შეტევები გამოყენებით დონეზე

შეტევები გამოყენებით დონეზე ხორციელდება სხვადასხვა გზით. ყველაზე გავრცელებული მათ შორის არის- სერვერული პროგრამული უზრუნველყოფის კარგად ცნობილი ნაკლოვანებების გამოყენება (Sendmail, Ftp, FTTP). ამ ნაკლოვანების გამოყენებით ჰაკერებს შეუძლიათ მიიღონ წვდომა კომპიუტერზე, იმ მომხმარებლის სახელით, რომელიც მუშაობს ამ პროგრამასთან

პორტების გადამისამართება

პორტების გადამისამართება თავისთავად წარმოადგენს ბოროტმოქმედულ დივერსიას, როდესაც გატეხილი ჰოსტი გამოიყენება ქსელთაშორისი ეკრანის გავლით ტრაფიკის გადაცემისთვის, რომელიც სხვა შემთხვევაში აირეკლებოდა ბრანდმაუერის მიერ.

ვირუსები და "ტროას ცხენი"-ს სახელით ცნობილი პროგრამები

სამუშაო სადგურები საბოლოო მომხმარებლებით, ნოყიერი ადგილია ვირუსებისა და ტროას ცხენების გავრცელებისათვის.

მათთან საბრძოლველად ეფექტურია ანტივირუსული პროგრამები, რომლებიც მუშაობენ სამომხმარებლო დონეზე და შესაძლებელია აგრეთვე ქსელურ დონეზეც. ანტივირუსული პროგრამები აღმოაჩენენ ვირუსებს და ტროას ცხენებს და აფერხებენ მათ გავრცელებას. ვირუსებზე ახალი ინფორმაციის მიღება ეფექტურს ხდის მათ მუშაობას. ამიტომ საჭიროა მათი განახლება მუდმივად.

თავდასხმის სუბიექტები

იმის და მიხედვით თუ რა არის თავდასხმის სუბიექტი ის შეიძლება დაიყოს ხუთ კლასად:

- აპარატურული საშუალებები - სამუშაო მანქანები, სერვერები, დისკური მოწყობილობები, პრინტერები, ქსელური კაბელები, აგრეთვე ქსელთაშორისი

მოწყობილობები, როგორიც არის მარშუტიზატორები, კომუტატორები, ხიდები.

- პროგრამული უზრუნველყოფა. ნებისმიერი პროგრამული უზრუნველყოფა, რომელიც მუშაობს ქსელში, წარმოადგენს პოტენციურ "კარიბჭეს" თავდამსხმელისათვის. რომლებიც შეიძლება იყოს შეძენილი ან შექმნილი ორგანიზაციის თანამშრომლების მიერ.
- ინფორმაცია. ერთერთ ყველაზე ღირებულს, რა თქმა უნდა წარმოადგენს მონაცემები, რომელიც იქმნება და გადაიცემა ქსელში
- ადამიანები. "რისკ ჯგუფებში" შედიან ის მომხმარებლები, რომლებთაც აქვთ ქსელში წვდომა, აგრეთვე მათზე მიერთებული მოწყობილობები
- დოკუმენტები. ჰაკერებისთვის ეს განსაკუთრებით მნიშვნელოვამნია. ზოგჯერ მომხმარებლები პაროლებს იწერენ ბლოკნოტებში, აგრეთვე ზოგჯერ იბეჭდება კონფიდენციალური ინფორმაცია, რომელიც შეიძლება მოხვდეს სანაგვე ყუთში. ამიტომ მსგავსი დოკუმენტები ან უნდა დაიჭრას წვრილად, ან რაიმე მოწყობილობით გახდეს წაუკითხავი და შემდეგ გადაიყაროს

ხარვეზები და მათი ლანდშაფტი

შეტევის განხორციელებისატვის უფრო მეტია საჭირო ვიდრე ხარვეზიანი ადგილის პოვნა სისტემაში. შეიძლება დავადგინოთ, რომ თავდამსხმელი წარმატებით გამოიყენებს სუსტ ადგილს თუ მან შეძლო მიზნის დადგენა, თავდასხმის

ორგანიზება, თავის საქმის გაკეთება და მიმალვა. სეფის ნაკლი შენობაში, რომელიც კარგად დაცულია ნაკლებად არსებითია, ვიდრე ანალოგიური ნაკლი ბანკის ქუჩის სეიფზე.

ისევეა ციფრულ სამყაროშიც. პოტენციალური ბოროტმოქმედისთვის არ არის საკმარისი იპოვოს ნაკლი შიფრაციის ალგორითმში, რომელიც გამოიყენება საკრედიტო ბარათებში. მან უნდა შეძლოს კავშირი, მას უნდა ქონდეს საკმარისი ცოდნა პროტოკოლებზე, იმისატვის რომა მან შექმნას გაყალბებული შეტყობინება, რომელიც მას მისცემს საშუალებას მოიპაროს ფული და დროზე დატოვოს ის ადგილი. ამიტომ არსებობ უამრავი საშუალება ამ ხვრელების ამოსავსებად.

რელურ სამყაროში არსებობს უამრავი სუსტი წერტილები და უამრავი გზა იმისათვის რომ განხორციელდეს თავდასხმა. თუ ტერორისტს უნდა თვითმფრინავის აფეთქება, მას შეუძლია აიტანოს ბორტზე ბომბი, ან ესროლოს რაკეტა, ან კიდევ ხელში ჩაიგდოს თვითმფრინავი და შეანარცხოს უახლოეს მთას. ჰაკერი რომელიც ცდილობს შეაღწიოს კორპორაციულ ქსელში შეუძლია შეუტიოს ბრანდმაუერს, ვებ სერვერს, გამოიყენოს მოდემური კავშირი და სხვა.

სისტემები რომლებიც მუშაობენ რეალურ სამყაროში აქვთ უამრავი სხვადასხვა საშუალება წინ აღუდგნენ თავდასხმებს. ავიახაზის მოწყობილობა შეიცავს მეტალის დეტექტორებს, ქიმიურ ანალიზატორებს და რენტგენულ აპარატებს, რომელბიც იძლევა შესაძლებლობას აღმოაჩინონ ბომბი, სიტემები რომლებიც ეძებენ "უპატრონო" ნივთებს. ასე რომ შესაძლებელია ვიყოთ დარწმუნებული რომ უპატრონო პაკეტი არ აფრინდება თვითმფრინავთან ერთად, იმ დროს როდესაც

მისი პატრონი დარჩა მიწაზე. (ეს წინააღმდეგობის სისტემა ვარაუდობს, რომ ნაკლები ტერორისტები მოინდომებს თვითმფრინავთან ერთად აფეთქდეს, ხოლო უმრავლესი ტერორისტები ამჯობინებს მიწაზე სეირნობას როდესაც თვითმფრინავი აფეტქდება)

შეტევის მეთოდოლოგია

საერთოდ წარმატებული შეტევა შეიძლება დავყოთ ხუთ თანმიმდევრულ ნაბიჯად:

1. მიზნის გამოკვეთა, რომელიც უნდა დაექვემდებაროს თავდასხმას და ინფორმაციის შეგროვება მის შესახებ;
2. მიღებული ინფორმაციის ანალიზი და ხარვეზიანი ადგილის პოვნა, რომელიც მოგვცემს საშუალებას მივაღწიოტ ობიექტამდე, რომელზეც არის მიმართული შეტევა;
3. მიზნის წვდომისთვის აუცილებელი ნებართვის მიღება;
4. მიზანზე თავდასხმის განხორციელება;
5. თავდასხმის დასრულება,რომელიც შეიძლება მოიცავდეს ყველა კვალის გაქრობას და დროზე მიმალვას.

ე.ი სხვა სიტყვებით რომ ვთქვათ, საჭიროა განისაზღვროს რას შეუტიოთ, როგორ შეუტიოთ, როგორ შევაღწიოთ შიგნით, როგორ განვახორციელოთ შეტევა და როგორ გავიქცეთ დროზე. პირველი ნაბიჯზე ხდება მიზნის შერჩევა და ინფორმაციის შეკრება. ზემოთაღნიშნულის გაკეთება არც ასე რთულია. თუ იმას გავითვალისწინებთ რომ ვებ გვერდებზე ნებისმიერი

ინფორმაციის მოპოვება საკმაოდ ადვილია. არსებობს უამრავი ტექნიკა, რომელიც თავდამსხმელმა შეიძლება გამოიყენოს. მაგ იმისთვის თუ როგორ მუშაობს ქსელი, რომელშიც იმყოფება მისი მიზანი: სმეციალური პროგრამების საშუალებით მოპოვებული ინფორმაციის შესწავლა, რომელიც გამოიყენება ადრესატის წვდომის შესამოწმებლად, აგრეთვე პორტების მდგომარეობის დასადგენად და სხვა. ასევე თავდამსხმელი იკვლევს კონკრეტულ აპარატურულ და პროგრამულ უზრუნველყოფას, მის მუშაობის პრინციპებს და მათ მიერ მხარდაჭერილ სერვისებს, რომელიც მუშაობს სამიზნე ქსელში.

მეორე ნაბიჯი - ეს არის ნაკლოვანი ადგილის პოვნა. ამ მომენტში თავდამსხმელი ყურადღებით სწავლობს ყველა მის ხელთ არსებულ ინფორმაციას, იმისათვის რომ აირჩიოს თავსდასხმის წერტილი.

მოსალოდნელია რომ ერთერთ კომპიუტერზე ეყენება განსაზღვრული ვერსია ოპერაციული სისტემისა, ან Windows NT ან Solaris და სხვა. რომლებიც შეიცავენ ცნობილ შეცდომებს. შესაძლებელია თავდამსხმელს ეძლევა შესაძლებლობა FTP ან რომელიმე სარეგისტრაციო სახელის გამოყენებისა, ან კიდევ სხვა რამის. არ არის გამორიცხული რომ თავდამსხმელს შესაძლებლობა ქონდეს გამოიყენოს ობიექტის სატელეფონო ქსელი, რომლისთვისაც მიმართულია შეტევა. რაც უფრო მეტი სისტემის ნაკლოვანი მხარეებია ცნობილი თავდამსხმელისთვის მით უფრო კარგად შეძლებს ის თავდამსხმის ორგანიზებას

მესამე ნაბიჯი - რაღაცნაირი კავშირის დამყარება. ინტერნეტში ეს ტრივიალურია, იმიტომ რომ ნებისმიერი კომპიუტერი ჩართულია ქსელში და შესაბამისად წვდომადია, (რა თქმა უნდა ზოგიერთი კომპიუტერი განლაგებულია

ბრანდმაუერის უკან ამიტომ ისინი მიუწვდომელია მაგრამ თვით ბრანდმაუერი კი წვდომადია

მეოთხე ნაბიჯი - შეტევის განხორციელება. ეს შეიძლება აღმოჩნდეს რთული საქმე, ან პირიქით სრულიად ადვილი. თუ თავდამსხმელი კარგად მომზადებულია, მაშინ ყველაფერი გასაოცრად ადვილია.

აღსანიშნავია, რომ ზოგიერთი შეტევა თავისთავად მოიცავს მრავალ ინტერაციას.

მეხუთე ნაბიჯი - შეტევის დამთავრება.

ჰაკერული ინსტრუმენტები საშუალებას იძლევიან ავტომატიზირებულ იქნას მრავალი პროცესი. ისინი მოქმედებენ არც თუ ისე ეფექტურად, როგორც ვირტუოზული ჰაკერები მაგრამ მათ შეუძლიათ ნებისნიერი მოზარდი გადააქციონ საშიშ მოწინააღმდეგედ.

მეორე მაგალითი. საგადამხდელო სისტემების წინააღმდეგ შეტევა, რომელიც იყენებს სმარტ – ბარათებს.

პირველი ნაბიჯი - მდგომარეობს იმაში, რომ საჭიროა შეგროვდეს ყველა ინფორმაცია საგადამხდელო სისტემის შესახებ, რომელიც შესაძლებელია გამოგდგეს : განსაკუთრებით მისი აგებულება, ხელმისწვდომი დოკუმენტაცია, გამოყენებული პროტოკოლებისა და ალგორითმების მუშაობის პრინციპები. და სხვა. შესაძლებელია თქვენ გეძლევათ შესაძლებლობა მოიპოვოთ უამრავი ინფორმაცია თუ თქვენ იცით, თუ სად იპოვოთ ის.

მეორე ნაბიჯი - ეს არის დოკუმენტაციის შესწავლა, მისი ნაკლოვანი მხარეების აღმოჩენის მიზნით. ხარვეზიანი

შეიძლება იყოს შიფრაციის ალგორითმები ან პროტოკოლები, შესაძლებელია ნაკლოვანება იყოს თვით სმარტ –ბარათში, იმის გამო რომ სისტემა რომელიც ეწინააღმდეგება თავდასხმას არ მუშაობს ისე როგორც უნდა იყოს. აგრეთვე შესაძლებელია არსებობდეს დეფეკტი მისი მუშაობის მეთოდებში - თუ ამის აღმოჩენა ხერხდება, მაშინ შესაძლებელია მივაღწიოთ მიზანს. თქვენ უნდა შეძლოთ ყველა შესაძლო დეფეკტის აღმოჩენა, იმისათვის რომ წარმატებით შეუტიოთ სისტემას.

მესმე ნაბიჯზე აუცილებელია მიიღოთ წვდომის დონე, რომელიც აუცილებელია შეტევის განხორციელებისათვის. თქვენ უნდა გახდეთ

ამ საგადამხდელო სისტემის რეგისტრირებული მომხმარებელი. სავარაუდოა თქვენ დაგჭირდებათ ვინმესთვის ბარათის მოპარვა. შესაძლებელია თქვენ დგიდგეთ აუცილებლობა გახვიდეთ შეთქმულებაში გამყიდველთან, რომელიც იყებს სმარტ ბარათებს როგორც საგადამხდელო საშუალებას. წვდომის მიღება არც ისე იოლი ქმედებაა.

მეოთხე ნაბიჯი - თავდასხმის განხორციელება: მაგალითად სმარტ ბარათების გამრავლება და მათი დუბლიკატების გამოყენება, მათში არსებული მეხსიერების შეცვლა და მათი გამოყენება საქონლის შეძენის დროს. ბალანსის შეცვლა და ნაღდი თანხის მოთხოვნა, ყველაფერი ის რისი გაკეთებაც შესაძლებელია. უკანასკნელი პუნქტის შესასრულებლად საკმარისი არ არის მხოლოდ სმარტ ბარათის სისტემის გატეხვა არამედ თქვენ უნდა გადაიტანოთ ყველა ნადავლი გატეხვის გზით ნაღდ ფულში.

მეხუთე ნაბიჯი - კვალის დაფარვა. შესაძლებელია თქვენ მოგინდეთ ლიკვიდირება გაუკეთოთ თავდასხმის ყველა ფიზიკურ სამხილს.

ზოგიერთი თავდასხმისას არ არის წარმოდგენილი ყველა ხუტივე ეტაპი.

უკუქმედების გზები

უკუქმედების გზები არსებობს იმისათვის რომ დავიცვათ ნაკლოვანი წერტილები. ისინი შეიძლება იყვნენ მარტივი ან რთული ან ისეთი, საიმედო სისტემები, როგორიც არის შემოწმებისა და თაღლითობის მცდელობის აღმომჩენი სისტემები (IDS).

საერთოდ უკუქმედების გზები, გამოიყენება შეტევის აღსაკვეთად მოცემულ ხუთივე ეტაპზე.

დიდი ნაწილი ტექნიკური უკუქმედების საშუალებებისა გამოიყენება კომპიუტერებში და კომპიუტერულ ქსელებში.

სისტემის საიმედოობა ყოველთვის განისაზღვრება მისი ყველაზე სუსტი კვანძით, და ეს საერთოდ რომ ვქვათ გვაიძულებს ჩვენ მივმართოთ ცალკეულ ტექნოლოგიას. ჭკვიანურად აგებულ სისტემაში ეს ტექნოლოგიები არ დევს ზედაპირზე, საბოლოო ჯამში სისტემის უსაფრთხოება განისაზღვრება ურთიერთმოქმედებით. კრიპტოგრაფიული მეთოდები შესაძლებელია დაინგრეს პირდაპირი შეტევით ან ალგორითმის კრიპტოანალიზით. შესაძლებელია ისარგებლონ თანამშრომლების უყურადღებობით და გამოტყუონ პაროლი. მაგრამ შენობის კარის საკეტი, რომელშიც კომპიუტერი ინახება

ან კარგად კონფიგურირებული ბრანდმაუერი უზრუნველყოფს დაცვას სხვა დონეზე, ისევე როგორც თავდასხმა სისტემაზე თავისთავად გაცილებით რთულია, ვიდრე მხოლოდ ნაკლოვანების არსებობა, სისტემის დაცვა უფრო მეტია ვიდრე მხოლოდ უკუქმედების არჩევა. ეფექტური სისტემა ემყარება ზომების სამ შემადგენლობას:

დაცვა

აღმოჩენა

რეაგირება

სამხედრო ორგანიზაციაში სამსახურებრივი დოკუმენტები ინახება სეიფში. სეიფი უზრუნველყოფს შესაძლებელი შემოღწევისაგან დაცვას, მაგრამ იგივე მიზნისთვის მუშაობს სიგნალიზაცია და დაცვაც. წარმოვიდგინოთ რომ თავდამსხმელი არის უცხო ადამიანი: ის არ მუშაობს ოფისში. თუ ის ეცდება მოიპაროს დოკუმენტები სეიფიდან, მან უნდა გატეხოს არამარტო სეიფი, არამედ მან უნდა გათიშოს სიგნალიზაცია, შეძლოს გვერდი აუაროს მცველებს და შეიპაროს შიგნით. სეიფი საკეტით – ეს არის დაცვის ზომა, სიგნალიზაცია – თავდასხმის აღმოჩენის საშუალება, მცველები კი რეაგირების უზრუნველმყოფლები.

თუ მცველები ოფისს ირგვლივ უვლიან ყოველ ორმოცდაათ წუთში, მაშინ სეიფი წინ უნდა აღუდგეს თავდამსხმელს 50 წუთის განმავლობაში, თუ სეიფი იმყოფება ოფისში შიგნით სადაც თანამშრომლები არიან მხოლოდ სამუშაო საათებში, მაშინ ის ვალდებულია გამოავლინოს შესაძლებლობა გუძლოს თავდასხმას 16 საათის განმავლობაში, დაწყებული საღამოს 5 საათიდან დამთავრებული დილის 9 –

მდე (და გაცილებით უფრო დიდხანსაც კი თუ ოფისი დაკეტილია). თუ სეიფი აღჭურვილია სიგნალიზაციით, მაშინ მასზე თითის დადების დროსაც კი გამოჩნდებოდა მცველები, მაშინ მას უნდა გაეძლო შეტევისთვის მხოლოდ იმ დროის განმავლობაში, რა დროც დასჭირდებოდა მცველებს შემთხვევის ადგილამდე მოსვლისთვის.

ყოველივე ზემოთქმული ნიშნავს, რომ სეიფის საიმედოობა დამყარებულია აღმოჩენისა და რეაგირების მექანიზმებზე რომლებიც მუშაობს ადგილზე.

სეიფები კლასიფიცირდებიან ამ ნიშნების მიხედვით. მაგალითად ერთ სეიფს შეიძლება მიენიჭის კლასიფიკაცია TL-15 : ეს ნიშნავს რომ მას შეუძლია წინ აღუდგეს ინსტრუმენტებით აღჭურვილ პროფესიონალ გამხსნელს 15 წუთის განმავლობაში. ეს შეფასებები ეხება სუფთა დროითი შეტევას: დრო მიდის, მაშინ როდესაც სეიფი ექვემდებარება თავდასხმას. ხოლო დრო რომელიც სჭირდება გაგეგმვასა და მომზადებას არ ითვლება.

დაცვის ზომები, აღმოჩენა და რეაგირება

სეიფების კლასიფიკაცია კარგი მაგალითია. რომელ სეიფს იყიდით: გათვლილს 15 წუთზე, 30 წუთზე, 60 წუთზე თუ 24 საათზე? ეს დამიკიდებულია იმაზე, თუ რა დროის განმავლობაში ამუშავდება სიგნალიზაცია (აღმოჩენა) და მოვა დაცვა. რომ დააპატიმროს დამნაშავე (რეაგირება). აღმოჩენისა და რეაგირების სისტემის არ არსებობის შემთხვევაში სულ ერთია რომელ სეიფს ავირჩევთ.

უმრავლესი დაცვით ზომებს ახასიათებთ პროფი-ლაქტიკური ხასიათი: ბრანდმაუერი, კრიპტოგრაფია, პაროლები. ზოგიერთი ზომა შეიძლება იყოს აღმოჩენის მექანიზმები, როგორიც არის შემოჭრის აღმომჩენი სისტემა. ხშირად გხვდება რეაგირების მექანიზმები : მაგალითად სარეგისტრაციო პაროლის და მომხმარებლის შესატანი სისტემა, რომელიც ბლოკირებას უკეთებს სისტემას სამი არასწორი პაროლის შემდეგ, მაგრამ აღმოჩენის მექანიზმები გამოუსადეგარია რეაგირების მექანიზმების გარეშე. წარმოიდგინეთ შემოჭრის აღმომჩენი სისტემა, რომელიც მხოლოდ აღრიცხავს შეტევას. ის აძლევს სიგნალს სისტემურ ადმინისტრატორს, შესაძლებელია გაუგზავნოს შეტყობინება ელ-ფოსტით, ან პეიჯერზე ან სმს მობილურ ტელეფონზე. თუ ადმინისტრატორი არ პასუხობს (დაუშვათ რამოდენიმე საათის განმავლობაში), მაშინ შეტევის დაფიქსირებას აზრი არა აქვს და იმას რომ არ იყო მიღებული არანაირი ზომა, რომ გადაწყვეტილიყო პრობლემა.

ჩვეულებრივი დაცვითი სიგნალიზაციაც არის შემოჭრის აღმომჩენის საშუალება. როდესაც ის ამოქმედდება, შემდგომი მოვლენის განვითარება დამიკიდებულია იმაზე, მოახდენს თუ არა ვინმე რეაგირებას. თუ თავდამსხმელმა იცის რომ განგაშის სიგნალს ყურადღებას არავინ არ მიაქცევს, ეს იმას ნიშნავს, რომ ეს იგივეა რაც სიგნალიზაცია საერთოდ არარსებულიყო.

ზოგჯერ შეუძლებელია გამოვიყენოთ აღმოჩენის და რეაგირების მექანიზმები. წარმოიდგინეთ ჩვეულებრივი მოსმენა: ალისა და ბობი საუბრობენ დაუცველი კავშირით, და ევა კი მათ უსმენს. არც ბობს და არც ალისას არ შეუძლიათ აღმოაჩინონ მოსმენა, და შესაბამისად არა აქვთ შესაძლებლობა როგორმე რეაგირება გაუკეთონ მას. დაცვის საშუალებამ -

შიფრაციამ – უნდა უზრუნველყოს საკმარისად დაცული კავშირი.

არაგონიერი იქნებოდა იმედი დაგვემყარებინა მხოლოდ დაცვით მექანიზმებზე. პირველ რიგში იმიტომ რომ ერთ შეტევას შეიძლება მოსდევდეს მეორე. განსაკუთრებით დაცვითი მექანიზმების გამოყენება უზრუნველყოფს უსაფრთხოებას მხოლოდ მაშინ, როდესაც ტექნოლოგიები რომელიც დევს მის საფუძვლებში არის სრულფასოვანი. თუ იარსებებდა სმარტ ბარათების დაცვის იდეალური სისტემა, მაშინ არ იქნებოდა აუცილებელი აღმოჩენის და რეაგირების მექანიზმები. სმარტ ბარათის დაცვის სისტემა, რომელიც არსებობს რეალურ სამყაროში, დრო და დრო იძლევა ჩავარდნას. ამიტომ კარგად კონსტრუირებული დაცვითი სისტემა ვალდებულია მოიცავდეს აღმოჩენის და რეაგირების მექანიზმებს, მისი ჩავარდნის დროს. რადგანაც რეალურ სამყაროში არ არის პროდუქტი, რომელიც არ შეიცავდეს სუსტ წერტილებს. ყოველთვის შესაძლოა მოიძებნოს გზა ბრანდმაუერის გასატეხად, ოპერაციული სისტემის დასაშლელად, სერვერის პროგრამული უზრუნველყოფის თავდასასხმელად. ერთადერთი რაც იხსნის სისტემას სრულფასოვანი დაცვითი სისტემის არარსებობის დროს, ეს არის ისეთი კონტრზომების მიღება, როგორიც არის აღმოჩენა და რეაგირება. იმისათვის რომ მივიღოთ დროულად სიგნალი, როცა სისტემა განიცდის თავდასხმას, იგი შესაძლებლობას მოგვცემს წინ აღუდგეთ მსგავს მოვლენას.

ფიზიკური უსაფრთხოება

ქსელურ რესურსებზე არავტორიზებული წვდომისაგან დაცვა პირველ ნიშნავს, ფიზიკური წვდომის შეუძლებლობას კომპიუტერულ ქსელში, სერვერებთან, ვებ სცენარებთან, ქსელურ კაბელებთან და მოწყობილობებთან და სხვა რესურსებთან. როდესაც ქსელური კავშირები გადის თქვენი დაქვემდებარების ზონიდან, მაგალითად პროვაიდერთან კავშირის წერტილი, მაშინ რა თქმა უნდა იკარგება ქსელის ფიზიკური კონტროლის ასპექტები და საჭიროა დავეყრდნოთ სხვა დაცვით მექნიზმებს, როგორიც არის შიფრაცია და ტუნელირება. მაგრამ მოწყობილობები ორგანიზაციაში უნდა იმყოფებოდეს მუდმივი ყურადღების ქვეშ.

როგორ ბრიყვულადაც არ უნდა ჟღერდეს, ხშირად არასნქცირებული ჩართვისგან გვიცავს უბრალო კარის საკეტი. სერვერები რომლებზეც ინახება მნიშვნელოვანი ინფორმაცია არ უნდა იდგნენ ღიად მაგიდაზე ან დაუკეტავ ოთახში, სადაც ნებისმიერს შეუძლია შევიდეს. ანალოგიური გზით უნდა იყოს დაცული მარშუტიზატორები, კომუტატორები, კონცენტრატორები და სხვა მოწყობილობები. კომპიუტერების ოთახები უნდა იკეტებოდეს ან უნდა იყოს მუდმივ დაკვირვებაში. თუ რომელიმე თანამშრომელი მუშაობს მთელი დღე და ღამე მაშინ ამ ოთახის დაკეტვა არ არის აუცილებელი- მხოლოდ იმ შემთხვევაში თუ პერსონალი არ მორიგეობს მარტო. იდელურ შემთხვევაში ასეთ ოთახში შესვლა უნდა კონტროლირდებოდეს, სარეგისტრაცი ჟურნალის გამოყენებით.

სარეზერვო მატარებლები, როგორიც არის ლენტები და მრავალჯერ ჩაწერადი დისკები, დაცული უნდა იყვნენ ისე, როგორც საწყისი მონაცემები. დაუშვებელია სარეზერვო კოპიის

შენახვა სერვერებზე, სამუშაო სადგურებზე, და დავტოვოთ ისინი მაგიდაზე ან დაუკეტავ ყუთებში.

დაცულ ქსელბში გამოყენებული აპარატურის ზოგადი აღწერა

ერთერთი მთავარი მოთხოვნა თანამედროვე კომპიუტერულ ქსელებსა არის გაფართოება მაშტაბურობა, რომელიც ხდის ქსელებს საკმოდ დიდს და რთულს მაგრამ აღნიშნული უნდა განხორციელდეს ქსელების მწარმოებლურობის, უსაფრთხოების და მენეჯმენტის შემცირების გარშე

კომპიუტერული ქსელების მაშტაბურობის უზრუნველყოფა ხდება

არსებული ქსელების შერწყმის, რომელიც მოიცავს ინფორმაციულ და კომპიუტერულ უსაფრთხოებას და ქსელების მართვას ეფექტური საშუალებებებით.

მაშტაბის მიხედვით ქსელები იყოფა ლოკალურ, კორპორაციულ, რეგიონალურ და გლობალურ ქსელებად.

ლოკალური ქსელი - წარმოადგენს კომპიუტერების ჯგუფს რომლებიც ერთმანეთთან დაკავშირებულია საკომუნიკაციო საშუალებით და განთავსებულია ერთ ან რამოდენიმე ახლოს მდგომ შენობაში, ლოკალური ქსელი შეიძლება იყოს დაყოფილი რამოდენიმე სეგმენტად, ყოველი სეგმენტში იგულისხმება ლოკალური ქსელის ნაწილი რომლის გარშემოც ხდება მხოლოდ იმ პაკეტების მიმოცვლა რომელიც ეკუთვნის მხოლოდ ამ სეგმენტს. აღნიშნული სეგმენტის დამახასიათებელი თვისებაა, რომ როდესაც კომპიუტერები

გადასცემენ პაკეტებს ეს პაკეტები ეგზავნება ამ სეგმენტში ჩართულ ყველა კომპიუტერს, მაგრამ იღებს მხოლოდ ის ვისთვისაც არის ეს პაკეტი განკუთვნილი. დანარჩენი კომპიუტერები იგნორირებას უკეთებენ აღნიშნულ პაკეტებს.

ლოკალური ქსელის დაყოფა სეგმენტებად აუმჯობესებს ქსელის მწარმობლურობას და ტრაფიკის შემცირებას. ეს გამოწვეულია იმით რომ ცალკეული კომპიუტერები რომლებიც აგზავნიან პაკეტებს რომლის ადრესატი არის სეგმენტის შიგნით, მაშინ ეს პაკეტები არ ხვდებიან დანარჩენ სეგმენტში. მაგრამ გასათვალისწინებელია ის რომ ქსელის დაყოფა სეგმენტებად მისი მწარმოებლურობის გასაზდელად საჭიროა მხოლოდ მაშინ როდესაც გამოყოფილი სეგმენტები წარმოადგენენ სამუშაო ჯგუფებს რომლის შიგნით ინტენსიურია ინფორმაციის მიმოცვლა.

კორპორაციული, რეგიონალური და გლობალური ქსელები საკომუნიკაციო არხებით აერთიანებენ ტერიტორიალურად განაწილებულ ლოკალურ ქსელებს. კორპორაციული ქსელის-დამახასიათებელი ნიშანია რომ ის ეკუთვნის ერთ ორგანიზაცას, რეგიონალური - რომ ის აერათიანებს მაგალითად ერთ ქალაქს, გლობალური - აერთიანებს ქალაქებს, ქვეყნებს და კონტინენტებს.

დიდი რეგიონალური ქსელი შეიძლება აერთიანებდეს პატარა რეგიონალური და კორპორაციულ ქსელებს, ხოლო გლობალური ნებისმიერი ტიპის ქსელებს. ნათელ მაგალითს გლობალური ქსელისას წარმოადგენს Internet.

კომპიუტერული ქსელების განვითარებისთვის და ასევე არსებული ქსელების ინტეგრაციისთვის გამოიყენება მრავალი აპარატურულ-პროგარმული მოწყობილობა.

კონცენტარტორები - უზრუნველყოფენ ელექტრული სიგნალების გაძლიერებას და საჭიროებისამრებ განტოტვას, ლოკალური ქსელის სეგმენტების გასაფართოებლად.

ხიდები და კომუტატორები - გამოიყენება ლოკალური ქსელების სეგმენტებად დასაყოფად, აგრეთვე მიღებული სეგმენტების და მცირე ზომის ლოკალური ქსელების გასაერთიანებლად.

მარშუტიზატორები – გამოიყენება გლობალური და აგრეთვე ლოკალური ქსელების და მათი დიდი ნაწილების გასაერთიანებლად.

შლუზები - გამოიყენება მარშუტიზაციის ფუნქციის შესასრულებლად და ისეთი კომპიუტერული ქსელების გასაერთიანებლად რომელთა ქსელური პროტოკოლები არათავსებადია.

ამ დროისათვის აქტიურად დაიწყეს ისეთი კონცენტრატორების გამოყენება რომლებიც მუშაობენ არა მარტო ფიზიკურ, არამედ არხის დონეზეც OSI –ს ეტალონურ მოდელში, იმისათვის რათა უზრუნველყონ ქსელური ფიზიკური მისამართების (MAC – Media Access Control) გამოყენების უსაფრთხოება. MAC მისამართი არის 48 ბიტიანი რიცხვი, რომელიც ენიჭება ქსელურ ადაპტერს მისი წარმოების დროს. ყველა ქსელურ ადაპტერს გააჩნია უნიკალური MAC მისამართი. გამონაკლისს წარმოადგენს მხოლოდ ArcNet –ი

რომლის ქსელური ადაპტერებს ენიჭებათ 8 ბიტიანი მისამართები.

MAC მისამართების გამოყენების უსაფრთხოების მიზნით ზემოთაღნიშნული კონცენტრატორები იყენებენ ფრეიმების შერჩევით

დაშიფრვას და ასევე MAC მისამართების ფილტრაციას.

არხის დონის პაკეტების შიფრაცია იცავს ქსელურ ტრაფიკს

თვალთვალისაგან. კერძოდ ჩვეულებრივ რეჟიმში ქსელური კვანძი იგნორირებას უკეთებს იმ პაკეტების რომლებიც არ არიან მისადმი ადრესირებული. თვალთავლი შესაძლებალი მაშინ როდესაც ქსელური ადაპტერი გადადის მონიტორინგის რეჟიმში, რომლის დროსაც ადაპტერი იღებს ყველა პაკეტურ შეტყობინებას რომელიც მოხვდება ამ სეგმენტში. ადაპტერის მონიტორინგის რეჟიმში გადაყვანა ხდება სპეციალური პროგრამების გამოყენებით, რომელთაც ეწოდებათ ანალიზატორები (პაკეტების სნიფინგი).

ასეთი პროგრამები ფართოდ არის გავრცელებული და გამოიყენება შეცდომების აღმოსაჩენად და ქსელის მწარმოებლურობის ანალიზისათვის. ქსელური ტრაფიკის თვალთვალისათვის საკმარისია ნებისმიერ კომპიუტერზე რომელიმე სეგმენტში გაეშვას ანალიზატორი.

ტრაფიკის თვალთვალის ხელშეშლის მიზნით კონცენტრატორები შიფრავენ არხის დონი პაკატებს (ფრეიმი), კონცენტარტორმა უნდა იცოდეს მასთან მიერთებული კომპიუტერების MAC მისამართები. MAC მისამართების ჩაწერა კონცენტრატორში ხორციელდება სპეციალური პროგრამული

უზრუნველყოფის სასუალებით ქსელის ადმინისტრატორის მიერ, ან ისევე როგორც კომუტატორების შემთხვევში.

თუ კონცენტარტორებისთვის ცნობილია მასთან მიერთებული კომპიუტერების MAC მისამართები მაშინ ის იქცევა შემდეგნაირად,

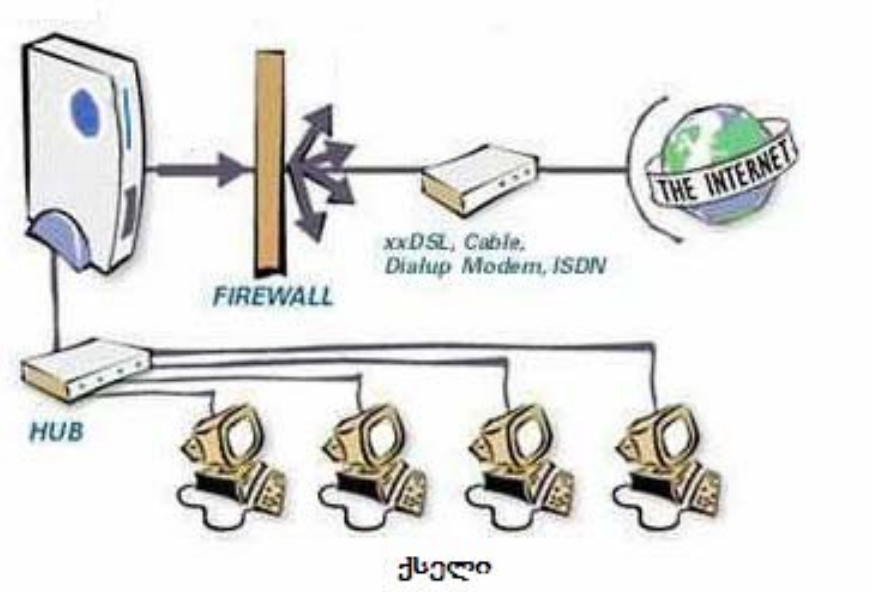
ფრეიმების რეტრანსილაციისას კონცენტრატორი შიფრავს პორტებიდან გამომავალ იმ პაკეტებს, რომლის მისამართები არ ემთხვევა მიმღების პორტზე მიერთებული მანქანების მისამართს

ბრანდმაუერები

ბრანდმაუერები პირველად გამოჩნდა მატარებლებში, თბომავლები რომლებიც მუშაობდნენ ნახშირზე, საწვავი ღუმელი და საწვავი ახლოს იყო ერთმანეთთან, მემანქანე იღებდა ნახშირს ნიჩაბით და ყრიდა ღუმელში. ამ დროს ხშირად წარმოიქმნებოდა ადვილად აალებადი ნახშირის მტვერი. დრო და დრო ხდებოდა მისი აალება რაც იწვევდა სამანქანო განყოფილებაში ხანძარს, რომელიც შესაზლებელი იყო გავრცელებულიყო სამგზავრო ვაგონებში. ასე რომ მგზავრების სიკვდილი აისახებოდა სარკინიგზო შემოსავლებზე, ამიტომ თმოვალების უკანა ნაწილი აღჭურვეს რკინის ფირფიტებით, იმისათვის რომ ცეცხლი არ გავრცელებულიყო სამგზავრო ვაგონებზე, მაგრამ თვით მემანქანები დაუცველი იყვნენ.

ციფრულ სამყაროში ბრანდმაუერი -ეს არის კომპიუტერული ქსელის დაცვის შიდა საშუალება.

ბოროტმოქმედი ჰაკერების, ხარბი დამნაშავეებისა და მსგავსი ნაძირლებისა რომლებიც დობორიალებენ ინტერნეტში.



ქსელი

ტერმინები ყოველთვის არ არის ზუსტი: საქმე იმაშია რომ ცნებამ "ბრანდმაუერი" შეიცვალა ტავისი პირვანდელი მნიშვნელობა როდესაც გამოჩნდა კომპიუტერულ ქსელებში. პირველი ქსელები იყო ძაილიან არსრული ამიტომ სესაძლებელი იყო ადვილად დანგრეულიყო. ბრანდმაუერები შეიქმნა იმისათვის რომ ხელი შეეშალა ქსელური პროგრამების გავრცელებისთვის რომელიც შეიცავდა ბევრ შეცდომას.

დღეს ბრანდმაუერები გამოდიან საზღვრის დამცველებად ლოკალურ და უზარმაზარ გლობალურ ქსელებს შორის, ისინი

აჩერებენ გარედან დაუპატიჟებელ სტუმრებს და უშვებენ მხოლოდ ნებადართულ მომხმარებლებს.

პირველი: ბრანდმაუერი - ეს საზღვარი, დაცვის ხაზი. მსგავსად ციხესიმაგრის კედლებისა, რომელიც გამოიყენება თავდასხმის მოსაგიერებლად, როგორც კი თავდამსხმელი გადალახავს ბრანდმაუერს უკანასკნელი ხდება გამოუსადეგარი. გამომდინარე აქედან (გამოკვლევების მიხედვით, რომელიც ჩაატარა კომპიუტერული უსაფრთხოების ინსტიტუტმა 1998 წელს) დაახლოებით 70% თავდასხმებისა ხორციელდება ქსელის შიგნიდან, რომელიც საკმაოდ დამაფიქრებელია.

მეორე: სანამ შექმნიდნენ საარტილერიო იარაღს კარგი ციხესიმაგრე იყო აუღებელი. შეუძლებელი იყო კედელზე თოკით გადასვლა, დანგრევა ან საძირკვლის გათხრა და შიგნით შეღწევა, მაგრამ კარგ სამხედრო მეთაურს ყოველთვის შეუძლია ციხე მოაქციოს ალყაში. ის იმედოვნებს იმაზე, რომ დიდხანს უპუროდ, უწყლოდ და გარემოსგან მოწყვეტით, იძულებულს გახდის ციხესიმაგრეში მსხდომ თავდამცველებს წავიდნენ კაპიტულაციაზე. ზოგჯერ აღნიშნულის მიღწევა საკმაოდ სწრაფად ხდება, მაგრმ ზოგჯერ საჭიროა წლები. თუ ციხესიმაგრეში არსებობს ჭა, მაშინ დამცველებს უფრო მეტი შანსი აქვთ. თუ მათ საიდუმლო გვირაბი გააჩნიათ მათ ეს ძალიან წაადგებოდათ, მაგრამ თუ იქ გაჩნდა ჭირი, მაშინ ციხესიმაგრე მათ ვერაფერს უშველის. მსგავსი შესაძლებელია მოხდეს ქსელშიც.

მესამე: ციხესიმაგრე უნდა იყოს დაცული ყველა მხრიდან. არა აქვს აზრი ცალკე აღებული კედლის აგებას იმიტომ რომ თავდამსხმელი უბრალოდ შემოუვლის მას. ასევეა ბრანდმაუერშიც ის უნდა იყოს ბარიერი შიდა და ყველა სხვა

გარე ქსელს შორის, სხვაგვარად თავდამსხმელი უბრალოდ შემოუვლის ბრანდმაუერს და შეუტევს რომელიმე დუცველ კავშირს.

მეოთხე: ციხესიმაგრეს უნდა კარები. უაზრობაა ააშენო ციხე რომელშიც ვერავის შეუძლია შეღწევა ვერანაირ მდგომარეობაში. ვაჭრები, კურიერები და ჩვეულებრივი მოქალაქეები თავისუფლად უნდა შედიოდნენ ციხეში და გამოდიოდნენ, შესაბამისად ციხეში იყვნენ მეციხოვნეები რომლეთა მოვალეობა იყო შეეშვათ ის ადამიანები ვისაც შიგნით უნდოდა შესვლა ან პირიქით არ შეეშვათ ისინი.

დიდმა ჩინურმა კედელმა ვერ დატოვა შთაბეჭდილება ჩინგისხანზე. მას ეკუთვნის გამოთქმა "ციხესიმაგრის აუღებლობა დამოკიდებულია მცველების სიმამცეზე". ვინც საჭიროა, ყველა მათი შეშვება და ამასთან ყველას გაჩერება ვინც წარმოადგენს საფრთხეს გარედან არის ბრანდმაუერის ძირითადი მოვალეობა. ის უნდა მუშაობდეს როგორც მეციხოვნე. მან უნდა გაარკვიოს რომელი კოდი შეიცავს საფრთხეს და დაბლოკოს მისი შენოღწევა ქსელში. ბრანდმაუერმა ეს უნდა შეძლოს კანონიერი მომხმარებლის გაუღიზიანებლად.

არსებობს სამი ძირითადი გაზა ბრანდმაუერის გადასალახავად:

პირველი: როგორც ზემოთ ავღნიშნეთ არის მისი შემოვლა მეორე მხრიდან.

მეორე: უფრო რთული თავდასხმაა - ეს არის მოიპარო რამე ბრანდმაუერის გავლით. ეს რომ გაკეთდეს უნდა მოვტყუთ ბრანდმაუერი, მან უნდა იფიქროს რომ ჩვენ ვართ

წესიერი მომხმარებელი და უფლებამოსილი ვართ ვაკეთოთ ეს. იმისდა მიხედვით თუ რამდენად კარგია ბრანდმაუერი და რამდენად კარგად მოხდა მისი დაყენება, ამის გაკეტება ან ადვილია ან საერთოდ შეუძლებელია.

ძირითადი იდეა მდგომარეობს იმაში რომ, უნდა შეიქმნას კოდის ასლი, რომელსაც ბრანდმაუერი შეუშვებ შიგნით, მსგავსი კოდები გამოიყენება იმისთვის რომ გამოვიყენოთ რაიმე დეფეკთი კომპიუტერულ სისტემაში, რომელიც მოგვცემს საშუალებას დამყარდეს კავშირი გარედან ჰაკერსა და შიგნით კომპიტერს შორის ბრანდმაუერის გავლით, თუ ეს ყველაფერი გაკეთდა, მაშინ ჰაკერი აღწევს შიგნით.

მესამე თავდასხმა - ბრანდმაუერის დამორჩილების მცდელობა, ეს წააგავს მოწინააღმდეგის შანტაჟს როგორც კი თქვენ შეძლებთ მიიღოთ ის თქვენ რიგებში, ის გააკეთებს ყველაფერს რასაც თქვენ მოინდომებთ. რაც უფრო ადვილი იქნება ამის გაკეთება დამიკიდებულია ბრანდმაუერზე. ზოგიერთ ბრანდმაუერში მუშაობს პროგრამული უზრუნველ-ყოფა, რომელსაც გააჩნია დაუცველი წერტილები და რომლიბიც შეიზლება დაეხმაროს ბოროტმოქმედებს.

ასე თუ ისე ბრანდმაუერების დღესდღეისობით შეიცავენ ყველაფერს, რომელიც საჭიროა ტრაფიკის ფილტრაციისათვის. სინამდვილეში დაბალ დონეზე ბრანდმაუერი არი მარშუტიზატორი მიმდევრობითი წესების ნაკრებით, რომელიც მასში გამავალ ქსელურ ნაკადს ამოწმებს და რეგულირებას უკეთებს ტრაფიკს მოცემული წესების მიხედვით. მანამდე ეს იყო შედარებით ადვილი მაგარამ ახლანდელ ბრანდმაუერებს საქმე უწევს მულტიმედიურ ტრაფიკებთან, დატვირთული პროგრამებით, ჯავა აპლეტებით, და სხვა სახის გაურკვეველი

საგნებით. ბრანდმაუერმა უნდა მიიღოს გადაწყვეტილება თავისი მწირი და არასრული ინფორმაციის საფუძველზე გაატაროს თუ არა პაკეტი.

მანამდე ბრანდმაუერები იყვნენ მხოლოდ პაკეტური ფილტრები. ბრანდმაუერი ათვალიერებდა ყოველ პაკეტს, რის შემდეგ უშვებდა ან აჩერებდა პაკეტს მითითებული წესების მიხედვით, შეეფარდებოდა თუ არა პაკეტის სათაური მოცემულ წესებს, რომელიც ცნობილი იყო ბრანდმაუერისთვის.

დღეს ისინი შესრულების პროცესში იცვლიან თავის მდგომარეობის პარამეტრებს: ინდივიდუალური შემოწმების მაგივრად ბრანდმაუერები ინახავენ ინფორმაციას ქსელის მდგომარეობის შესახებ და რა ტიპის პაკეტებია მოსალოდნელი, მიუხედავად ამისა მათ არა აქვთ უსაზღვრო მეხსიერების რესურსი, ამიტომ შესაძლებელი ნელი თავდასხმების განხორციელება.

ამჟამად არსებობს საკმაოდ კარგი ფილტრირებადი ბრანდმაუერები, მაგრამ მათ აქვთ მრავალი ხარვეზები. პირველი და ყველაზე მნიშვნელოვანი არის ის, რომ რთულია მათი სწორი კონფიგურირება, ხოლო არასწორი კონფიგურირებას კი ხშირად მივყავართ დაცვის ხარვეზებამდე. მრავალი საგნები რომელიც უნდა იბლოკებოდეს ნებადარტულია დეფაულტად. ბრანდმაუერები არ ცვლიან პაკეტებს ამიტომ როდესაც პაკეტი აღმოჩნდება შიგნით მას შეუზლია აკეთოს ყველაფერი.

მეორე ტიპი ბრანდმაუერები ეს არის პროკსი სერვერები, ან სისტემა, რომელიც ასრულებს ერთი ფორმიდან გარდაქმნას მეორეში. წარმოიდგინეთ ორი ყარაული, ერთი რომელიც დგას

გალავნის გარეთ მეორე კი შიგნით. გარეთ მდგომმა ყარაულმა არაფერი იცის გალავნის შიგნით არსებულ მდგომარეობაზე, ისევ როგორც შიგნით მდგომა არაფერი იცის გარეთ არსებულ მდგომარეობაზე. მაგრამ ისისნი ერთმანეთს გადასცემენ პაკეტებს. პროკსი-ბრანდმაუერები მუშაობენ სწორედ ასე. ზოგიერთ პროკსი-ბრანდმაუერები მუშაობენ მხოლოდ როგორც შუამავლები: თუ ვინმეს როომელიც იმყოფება ბრანდმაუერეით დაცული გარემოში, ესაჭიროება დოკუმენტი "გარე სამყაროდან" კლიენტის პროგრამული უზრუნველყოფა ეკითხება პროკსი-ბრანდმაუერს (შიდა მცველს) ამის შესახებ და გარეთა ბრანდმაუერი (გარეთა მცველი) აერთებს მას საჭირო ვებ გვერდთან.

ბრანდმაუერი არის მნიშვნელოვანი ელემენთი კომპიუტერული უსაფრთხოების სისტემაში, მაგრამ მათ არ შეუზლიათ სისტემის სრული დაცვა.

თანამედროვე ქსელებში გამოჩნდა კომბინირებული აპარატურა სადაც შერწყმულია, როგორც ბრანდმაუერის ასავე მარშუტიზატორის,VPN და ანტივირუსული სერვერის ფუნქციებიც.

უსაფრთხოების პოლიტიკა

სისტემის უსაფრთხოების პოლიტიკა წააგვას სახელმწიფოს საგარეო პოლიტიკას: ის განსაზღვრავს მიზნებსა და ამოცანებს,. როდესაც სახელმწიფოს ადანაშაიულებენ საგარეო პოლიტიკის არათანმიმდევრულობაში, ეს ხდება იმიტომ, რომ მის მოქმედებაში არ არის ლოგიკა და არ არის საერთო სტრატეგია. ზუსტად ასევე ხდება უსაფრთხოების

პლიტიკის არ არსებობის დროს, ციფრულ სისტემეაში უკუქმედების ზომები იქნება მოუწესრიგებელი. პოლიტიკა – ეს არის ხერხი უზრუნველყოთ საერთო ურთიერთკავშირი.

კარგი პოლიტიკა ფორმირდება, როგორც პასუხი საფრთხეზე. თუ საფრთხე არ არსებობს მაშინ არ არის არც პოლიტიკაც: ყველას შეუძლია აკეთოს ყველაფერი. ამერიკის შეერთებულ შტატები საჭიროებს საგარეო პოლიტიკას, თუ მხედველობაში მივიღებთ საფრთხეებს, რომელიც ემუქრება სხვა სახელმწიფოებიდან. მაგრამ შტატი პენსილვანია არ საჭიროებს არანაირ სგარეო პოლიტიკას, იმიტომ რომ დანარჩენი შტატები არ წარმოადგენენ საფრთხეს მისთვის. ასევა უსაფრთხოების პოლიტიკაშიც - ის აუცილებელია, ამიტომ საფრთხეების მოდელირება არ მთავრდება არასდროს ცარიელი ფურცლით. უსაფრთხოების პოლიტიკა განსაზღვრავს ჩარჩოებს, რომელშიც ხორციელდება უკუქმედების ზომების შერჩევა და რეალიზაცია.

არ არის საჭირო იმის მტკიცება, რომ ყოველ ორგა-ნიზაციას სჭირდება თავისი კომპიუტერული ქსელისთვის უსაფრთხოების პოლიტიკა. პოლიტიკამ უნდა მოხაზოს პასუხისმგებლობის საზღვრები, განსაზღვროს თუ რა არის უსაფრთხოების პოლიტიკის საფუძვლი და თუ რატომ არის ის მაინცდამინც საფუძვლი. უკანასკნელი აღნიშვნა ძალიან მნიშვნელოვანია, რადგანაც შემთხვევითი პოლიტიკა "ჩამოშვებული ზემოდან" განმარტებების გარეშე, საბოლოოდ მაინც იქნება იგნორირებული, რადგან უფრო სავარაუდოა, რომ თანამშრომლები გაყვებიან გასაგებ, მოკლე, ლოგიკურ და თანმიმდევრულ პოლიტიკას.

უსაფრთხოების პლიტიკა – არის ის რასაც თქვენ განსაზღვრავთ, რა უკუქმედების ზომებს მიმართავთ. გჭირდებათ თუ არა ბრანდმაუერი? როგორ უნდა დააკონფიგურიროთ, საკმარისია თუ არა სისტემიში წვდომისას მარტო პაროლის გამოყენება, შესაძლებელია თუ არა მომხმარებლებს მიეცეთ ნება ტავიანთი ბრაუზერიდან ვიდეოს ყურება.

ნებისმიერ შემთხვევაში უსაფრთხოების პლიტიკა პირველ რიგში უნდა პასუხობდეს კითხვებზე ”რატომ”? და არა ”როგორ”.

”როგორ” ეს არის კონტრზომის ტაქტიკა. რთულია შეარჩიო სწორი პოლიტიკა, მაგრამ უფრო რთულია განსაზღვრო უკუქმედების ზომების კომპლეხი, რომლებიც მის რეალიზებას განაპირობებენ.

ქსელების უსაფრთხოების უზრუნველსაყოფად საჭიროა გამუდმებული მუშაობა და ყურადღება. ამ მუშაობაში იგულისხმება რომ წინასწარ უნდა იქნას შესწავლილი ბოროტმოქმედების მიერ ყველა შესაძლო ქმედება, დაცვითი მექანიზმების გზების ძიება და მომხმარებლების პერმა-ნენტული განათლება. თუ მაინც მოხდა სისტემაში შემოჭრა უსაფრთხოების ადმინისტრატორმა უნდა შეძლოს დაცვითი სისტემის ხარვეზის აღმოჩენა, ხარვეზის მიზეზი და შემოჭრის გზა.

უსაფრთხოების სისტემის პოლიტიკის შედგენისას ადმინისტრატორმა პირველ რიგში უნდა ჩაატაროს რესურსების ინვნტარიზაცია

რომლის დაცვაც არის დაგეგმილი; იდენტიფიცირება უნდა გაუკეთდეს ყველა მომხმარებლებს რომლებიც მუშაობენ აღნიშნულ რესურსებთან. უნდა გაკეთდეს ანალიზი ტუ რომელი რესურსთან რა საფრთხე შეიძლება იყოს მოსალოდნელი. ყველა ამ ინფორმაციის ფლობის შემდეგ შესაძლებელია აგიოს უსაფრთხოების პოლიტიკა, რომელიც აუცილებელი გახდება ყველა მომხმარებლებისათვის.

უსაფრთხოების პოლიტიკის აგება – ეს არ არის ჩვეულებრივი წესი, ის ბევრისთვის გაუგებარია. ის უნდა იყოს წარმოდგენილი სერიოზული დოკუმენტის სახით. იმისათვის რომ გამუდმებით შევახსენოთ მომხმარებლებს უსაფრთხოების წესები, დოკუმენტის კოპიოები უნდა იქნეს დარიგებული ყველა ოფისში, რათა ეს წესების თვალწინ ედოს ყოველა თანამშრომელს

კარგი უსაფრთხოების პოლიტიკის აგება ითვალისწინებს რამოდენიმე ელემენტს ზოგიერთი მატგანი მოცემულია ქმემოთ:

1. **რისკის შეფასება**. უნდა ვიცოდეთ თუ რას ვიცავთ და ვისგან. ქსელში უნდა გამოიკვეთოს ღირებულებები და პრობლემების შესაძლო წარმომქმნელები;
2. **პასუხისმგებლობა.** აუცილებელია მიეთითოს პასუხის-მგებლები, რომლებიც ამა თუ იმ გზით პასუხს აგებენ უსაფრთხოებაზე, დაწყებული აღრიცხვითი ჩანაწერების გაკეტებიდან დამტავრებული დარღვევების გამოკვლევით;
3. **ქსელური რესურსები გამოყენების წესები**. პოლიტიკაში პირდაპირ უნდა იყოს მითითებული. რომ მომხმარებლებს არა აქვთ უფლება: გამოიყენონ ინფორმაცია არა

დანიშნულებით, გამოიყენონ ქსელი პირადი სარგებლობისთვის, აგრეთვე გამიზნულად მიაყენონ ზიანი ქსელს ან იქ განთავსებულ ინფორმაციას;

4. **იურიდიული ასპექტები**. აუცილებელია კონსულტირება იურისტთან, რადგან უნდა გაირკვეს ყველა კითხვა, რომელსაც შეიძლება კავშირი ქონდეს ქსელში შენახულ ან წარმოქმნილ ინფორმაციასთან და დართული უნდა იქნეს დოკუმენტებში რომელიც ეხება უსაფრთხოების უზრუნველყოფას;

5. **სისტემის აღდგენის პროცედურები**. მითითებული უნდა იყოს, თუ რა უნდა იქნას გაკეთებული სისტემის დარღვევის შემთხვევაში და რა მოქმედებები უნდა ჩატარდეს იმათ მიმართ, ვინც გახდა მიზეზი ამის გამოიწვევისა.

თუ სკმაოდ დიდხანს ვიმუშავებთ საფრთხეების მოდელირებაზე, გასაგები გახდება რომ ცნებას "უსაფრთხოების სისტემას" აქვს განსხვავებული მნიშვნელობა იმის და მიხედვით თუ რა სიტუაციასთან გვაქვს საქმე.

რამოდენიმე მაგალითი:

- კომპიუტერიები, გამოყენებული საქმიან სფეროში უნდა იყვნენ დაცული ჰაკერებისგან, ქურდებისგან და სამრეწველო კონკურენტებისაგან. სამხედრო კომპიუტერები უნდა იყვნენ საიმედოდ დაცული იგივე საფრთხეებისაგან და აგრეთვე მტრული სამხედრო ძალების შეღწევისგან. ზოგიერთი კომპიუტერები ემსახურებიან სატელეფონო ქსელებს და ისინიც უნდა იყვნენ დაცული სამხედრო მოწინააღმდეგებისაგან.

- მრავალი საქალაქო სატრანსპორტო სისტემები უცხოეთში იყენებენ გამშვებ ბარათებს ნარდი ფულის მაგივრად, მსგავსად ამისა გამოიყენება სატელეფონო ბარათებიც და სხვა. მსგავსი სისტემები აუცილებელია იყვნენ დაზღვეულები გაყალბებებისაგან. რა თქმა უნდა ეს არ არის პრობლემა როდესაც ყალბის დამზადება გაცილებით ძვირი ჯდება.

- პროგრამები რომლებიც იცავენ ელ-ფისტას უნდა უზრუნველყონ კორესპოდენციის დაცვა ყველა ნებისმიერი პლისტრაციისა და ცვლილების მცდელობისაგან. რასაკვირველია მრავალ შემთხვევაში პროგრამული საშუალებებით შეუძლებელია უსაფრთხო გავხადოთ სისტემა იმ მრავალი მანიპულაციებისგან თავი: ტროას ცხენი კომპიუტერში, ვიდეოკამერა, და სხვა.

ხრიკი მდგომარეობს იმაში, რომ შევქმნათ სისტემა, რეალური საფრთხეების გათვალისწინებით და არ გამოვიყენოთ უსაფრთხოების ტექნოლოგიები ყველა რიგრიგობით, იმის იმედით რომ ამით რამე მაინც გამოგვივა. ამისათვის აუცილებელია შევიმუშაოთ უსფრთხოების პოლიტიკა, რომელიც დამყარებული უნდა იყოს საფრთხეების ანალიზზე და შემდგომ შევქმნათ დაცვის მექანიზმები. რომლებიც რეალიზებას გაუკეთებენ ამ პოლიტიკას და წინ აღუდგებიან საფრთხეებს.

უსაფრთხოების პრინციპები

გაყოფა

მოგზაურები საფულეში ინახავენ მხოლოდ გარკვეულ მცირე თანხას, დანარჩენი აქვთ ან ზურგჩანთაში, ან დამალული ტანსაცმლის შიგნით.

თუ მათ გაქურდავენ, ამით ისინი მთლიან თანხას არ კარგავენ. ჯაშუშებისა ან ტერორისტული ორგანიზაციის სტრუქტურა დაყოფილია პატარა ქვეჯგუფებად, რომელთა წევრები იცნობენ მხოლოდ ერთმანეთს და არვის სხვას. ასე რომ, თუ რომელიმე წევრი იქნება დაჭერილი ან ჩაბარდება თავისი ნებით, მას შეუძლია გასცეს მხოლოდ ის ადამიანები რომელებიც შედიან მის ჯგუფში. გაყოფა- ეს არის ეფექტური დაცვის საშუალება, რადგანაც ის ზღუდავს მოწინააღმდეგის მოქმედებებს, რომელსაც ის მიყავს წარმატებამდე. ეს არის მაგალითი ჯანსაღი აზრისა, რომლითაც ხშირად სარგებლობენ. მომხმარებლებს აქვთ თავისის აღრიცხვითი ჩანაწერები: ოფისის კარები იკეტება სხვადასხვა გასაღებებით, გაღების უფლება ენიჭება კონკრეტულ ადამიანებს მათი ნდობის ხარისხის მიხედვით, აგრეთვე გამოწვეული განსაზღვრული რეალური აუცილებლობით მიენიჭოს მას ეს უფლება; პირადი ფაილები იშიფრება უნიკალური გასაღებებიტ. უსაფრთხოების სისტემა არ იქმნება პრინციპით <<ყველაფერი ან არაფერი>>, მაგრამ მან უნდა აღკვეთოს მნიშვნელოვანი ზიანის მიყენება შესაძლებლობა.

მსგავსი პრინციპი - პრივილეგიების მინიმუმი. ძირითადად ეს ნიშნავს იმას, რომ საჭიროა მიეცეს ვინმეს

(მომხმარებელს ან კონკრეტულ პროცესს) მხოლოდ ის პრივილეგია, რომელიც აუცილებელია მისი სამუშაოს შესასრულებლად. ჩვენ ამას ვაწყდებით ყოველ დღე ცხოვრებაში. თქვენი გასაღებით შესაძლებელია მხოლოდ თქვენი კარის გაღება, და არა რომელიმე ორგანიზაციის. ბანკომატებთან და იქ მოთავსებილ თანხასთან წვდომა შეუზღია მხოლოდ მის მომსახურე პერსონალს. იმ შემთხვევაშიც კი, როდესაც თქვენ გაქვთ განსაკუთრებული ნდობა, თქვენ შეგიძლიათ გათქვათ მხოლოდ ის საიდუმლო, რომელის ცოდნაც თქვენთვის ნებადართულია.

უფრო ბევრი მაგალითის მოყვანა შესაძლებელია კომპიუტერული სამყაროდან. მომხმარებლებს აქვთ წვდომა მხოლოდ იმ სერვერებთან, რომელიც აუცილებელია მათი მუშაობისათვის. მხოლოდ სისტემურ ადმინისტრატორს აქვს უფლება ქსელში ნებისმიერ რესურსის წვდომაზე, ხოლო მომხმარებლებს მხოლოდ საკუთარ ფაილებზე.

მრავალი თავდამსხმელები სარგებლობდნენ მინიმალური პრივილეგიის პრინციპების დარღვევის გამო.

გაყოფა ასევე უცილებელია, იმიტომ რომ რაც უფრო ბევრი ადამიანები სარგებლობენ ქსელით, მით უფრო ნაკელებია სისტემის საიმედობა. რაც უფრო ფართოა ამოცანების რაოდენობა, რომელიც სრულდება კომპიუტერის დახმარებით, მით უფრო ნაკლებად უსაფრთხოა ის.

ეს არის ერთერთი მიზეზი, ამიტომ ინტერნეტი ყველაზე ფართოდ გამოყენებადი ქსელია, მაგრამ შეიცავს უამრავ საფრთხეებს.

შეადარეთ ვებ სერვერი და კომპიუტერი რომელიც, განთავსებულია

ბომბთავშესაფარში და დაცულია ირგვლივ მცველებით. გაყოფას გმოყენება აქცევს სისტემას უფრო მიახლოებულს მეორე ვარიანტთან.

გავამაგროთ ყველაზე სუსტი კვანძი

ყველაზე პირველად საჭიროა დავიცვათ ყველაზე სუსტი ადგილი კვანძში. ეს ცხადია, მაგრამ ისევ და ისევ გხვდება სისტემები, სადაც ეს პირობები იგნორირებულია. სიბრიყვე იქნებოდა თუ უბრალოდ რომ ჩაგვესვა უზარამაზარ მესერი ციხესიმაგრის წინ იმ იმედით, რომ მტერი პირდაპირ მისკენ გაიქცეოდა. დაცვა უნდა იყოს ყველა მხრიდან, ამიტომ მოგვიწევს არხის ამოთხრა და ღობის აგება. ზუსტად ასეა დაშიფრვის ალგორითმის გამოყენებისას. იმ შემთხვევაშიც კი როდესაც ვიყენებთ 256 ბიტიან გასაღებს, არ ღირს ვიმედოვნოთ, რომ დაცული ვართ : მტერმა, შესაძლებელია იპოვოს ისეთი თავდასხმის ხერხი, რომელიც არანაირად არის დაკავშირებული დაშიფრვის ალგორითმათან.

გამოვიყენოთ გამშვები პუნქტები

გამშვები პუნქტი წარმოადგენს ვიწრო კორიდორს, რომელშიც ადვილია მომხმარებლების კონტროლირება. გაიხსენეთ როგორ არის მოწყობილი და რისთვის გამოიყენება სუპერმარკეტში საკონტროლო-კასური პუნქტები, თქვენი სახლის კარები. ამ მიზნით გამოიყენება ბრანდმაუერები, მარშუტიზატორები, სისტემაში შესვლის დროს რეგისტრაციები. მსგავსად არის აგებული თაღლითობის აღმომჩენი სისტემა საკრედიტო სისტემებისთვის. უსაფრთხოების მიზნით ყოველთვის აქვს აზრი გამოვიყენოთ გამტარი პუნქტები.

ეს გამტარი პუნკტები კარგია მაშინ როდესაც მისთვის გვერდის ავლა შეუძლებელია. ერთი ყველაზე გავრცელებულ ხერხი ბრანდმაუერის გადასახალავად არის მისი შემოვლა : შესაძლებელია მოიძებნოს, მაგალითად დაუცველი დაშორებული კავშირები. ხდება ისე რომ ადამიანები დაშორებულ კავშირებს ტოვებენ ჩართულს. ზოგჯერ მარსუტიზატორებს, დამამახსოვრებელი მოწყობილობები და თვით პრინტერებსაც კი შეიძლება ქონდეს დაუცველი პორტები. ყველაფერი ეს აძლევს თავდამსხმელს საშუალებას რომ შემოუაროს საკონტროლო პუნქტს.

არსებობს უფრო ნატიფი მეთოდები ტავდასხმისათვის. ერთ კომპანიას შესაძლებელია ქონდეს მყარი ქსელური დაცვის სისტემა, მაგრამ სხვა კომპანიას არა აქვს მაგის დარი დაცვა. თუ ისისნი ურთიეთმოქმედებენ ქსელის საშუალებით, ეს ნიშნავს რომ ქსელს აქვს სუსტი კვანძი, რომელიც საჭიროებს დაცვას.

სიღრმისეული დაცვის უზრუნველყოფა

სიღრმისეული დაცვა(მრავალდონიანი) – არის სხვა უნივერსალური უსაფრთხოების პრინციპი, რომელიც გამოიყენება კომპიუტერული ტექნოლოგიების სფეროში და აგრეთვე სხვა სფეროებშიც.

ტერიტორიის დაცვა (კარის საკეტები და სიგნალიზაცია ფანჯრებზე) უფრო ეფექტურია, თუ ის გამოიყენება სახლის შიგნით დაყენებულ სათავალთვალო სისტემასთან ერთად. ბრანდმაუერი, შემოჭრის აღმოჩენი სისტემისა და ძლიერი კრიპტოგრაფიული დაცვის პროგრამასთან ერთად გაცილებით უფრო საიმედოა, ვიდრე მხოლოდ ბრანდმაუერი.

დაცვა მით უფრო საიმედოა, რაც უფრო მყარია მისი ყველაზე სუსტი კვანძი. სინამდვილეში ყველაფერი დამოკიდებულია საქმის შესრულებაზე. ორი ბრანდმაუერი, ყოველი მათგანი რომელიც იცავს ცალკეულ ქსელში შემოსასვლელ წერტილებს- არა არის ღრმა დაცვა. წარმატებული თავდასხმისათვის საკმარისია ნებისმიერი მათგანის გადალახვა. ღრმა დაცვა იქნება რეალიზებული მაშინ, როდესაც ბრანდმაუერები დაყენებულია თანმიმდევრულად ერთი მეორეზე : მაშინ თავდამსხმელს მოუწევს რიგრიგობით საქმე ქონდეს ორ დაცვის დონესთან.

დაზღვევა სისტემის გაჩერების შემდეგ

მრავალი სისტემა აგებულია ისე, რომ თუ სისტემა გამოდის მწყობრიდან მომხმარებელი მიმართავს სარეზერვო სისტემას, შესაძლებელია ნაკლებად დაცულსაც კი. მაგალითად აშშ- ში VeriFone სისტემა გამოიყენება საკრედიტო ბარათებით ხელშეკრულების გაფორმებისას. როდესაც კლერკი ამოწმებს თქვენ ბარათს VeriFone უკავშირდება მონაცემთა ბაზებს და ამოწმებს : მოპარული ხომ არ არის ეს ბარათი, საკმარისად გაქვთ თუ არა თანხა ანგარიშზე და სხვა. წარმოიდგინეთ შემთხვევა, როდესაც ტერმინალი რაღაც მიზეზის გამო არ

მუშაობს ან შესაძლებელია ის არის გატეხილი, ან გაწყდა სატელეფონო კავშირი. ნუთუ მოვაჭრე უარს ამბობს თქვენს მომსახურებაზე? რა თქმა უნდა არა. მას შეუძლია ამოიტანოს ქაღალდის ბლანკი და ძველებურად შედგეს გარიგება.

მრავალი თავდამსხმელი ცდილობს გატეხოს დაცვა კავალერიული შეტევის გზით : შეტევები რომელსაც მივყავართ მომსახურების შეჩერებამდე. ეს შეიძლება განმეორდეს ისევ და ისევ. ეს გავს იმას, როდესაც ქურდები იზულებულს ხდიან სისტემას მუდმივად ჩაირთოს სიგნალიზაცია, იმ მიზნით რომ ის ბოლოს და ბოლოს გაითიშება.

საჭიროა, რომ სისტემა გაჩერების შემთხვევაში გახდეს უფრო მეტად დაცული ვიდრე მანამდე იყო. თუ ბანკომატში მუშაობას შეწყვეტს სისტემა, რომელიც ამოწმებს პირად საიდენტიფიკაციო ნომრებს, წარმოიქმნება უარი.., მაგრამ ამ დროს არ იყრება ბანკომადიდან ფულები. თუ გატყდება ბრანდმაუერი, მას მივყავართ იმამდე, რომ ის შეწყვეტს ყველანაირი პაკეტების მიღებას და გადაცემას.

მსგავსი პრიციპია გამოყენებული ტექნიკურ უსაფრთხოებაშიც და ეწოდება მტყუნებამედეგი (უავარიო მტყუნება), თუ ავტომანქანაში მიკრორპროცესორი გამოვა მწყობრიდან, ამან არ უნდა გამოიწვიოს მანქანის გაქანება მაქსიმალურ სიჩქარემდე. თუ წარმოიქმნება ბირთვული რაკიტის მართვის სისტემაში მტყუნება, მაშინ მან არ უნდა მიგვიყვანოს რაკეტის გაშვებამდე. უავარიო მტყუნება – არის კარგი წესი პროექტირებაში.

სიმარტივისკენ სწრაფვა

სირთულე – არის უსაფრთხოების ყველაზე დიდი მტერი. სისტემა მით უფრო დაცულია რამდენადაც უფრო კარგად დაცულია მისის სუსტი კვანძი. ამიტომ სისტემას ნაკლები კავშირებით, უკეთესად დავიცავთ. ეინშტეინი ამბობდა: "ყველაფერი უნდა იყოს იმდენად მარტივი, რამდენადაც ის შესაძლებელია იყოს და არა მეტი."

ხალხური სიბრძნე ამბობს: "არ ჩადოთ კვერცხები მხოლოდ ერთ კალათში" ეწინააღმდეგება ზემოთაღნიშნულ პრინციპებს, მაგრამ ეს ასეა და ამ პრინციპებით იგება სიღრმისეული დაცვა. მაგრამ გასათვალისწინებელია ისიც რომ ბევრი კალათის დაცვა გაცილებით ძნელია ვიდრე ერთის. როცა მიდის ლაპარაკი უსაფრთხოებაზე მაშინ ჯობია გამოვიყენოთ მარკ ტვენის ერთერთი გმირის რჩევა: "ჩადეთ ყველა კვერცხი ერთ კალათში და ყურადღება მიაქციეთ მას"

მომხმარებლების მხარდაჭერის გამოყენება

უსაფრთხოების უზრუნველყოფა გაცილებით მარტივია, თუ საქმე გვაქვს საიმედო და განათლებულ მომხმარებლებთან, და გაცილებით რთულია –არაყურადღებიანი და ბოროტი განზრახვით მომუშავე მომხმარებლების შემთხვევაში. უსაფრთხოების ზომები, რომელიც არის გაუგებარი და შეუტანხმებელი ვერ იმუშავებს. ყველაზე რთული პრობლემების შემქმნელები უსაფრთხოებაში არიან ისინი ვინც დაკავშირებულია ადამიანებთან, ხოლო ყველაზე მარტივი- კი ბიტებთან. უეჭველია უნდა არსებობდეს დაცვა შიდა თავდასხმისგანაც, მაგრამ ძირითადად თანამშრომლები არიან

ერთმანეთის მოკავშირეები. უნდა დავეყრდნოთ მათ მხარდაჭერას რამდენადაც ეს შესაძლებელია.

გარანტირების უზრუნველყოფა

რასაც ჩვენ სინამდვილეში ვსაჭიროებთ - ეს არის რწმენა, რომ ჩვენი სისტემები მუშაობენ დანიშნულების მიხედვით, რომ მათ გააჩნიათ მოტხოვნილი თვისებები და მხოლოდ ის. უმრავლეს თავდასხმებს რეალურ სამყაროში მივყავართ იქამდე, რომ სისტემები ან წყვეტენ იმ საქმიანობას, რომელიც მათ აკისრიათ, ან იწყებენ წარმოუდმოუდგენელ ქცევებს.

დაეჭვება

ეჭვი სისტემის დაცვის საიმედოობაზე უნდა არსებობდეს მუდმივად. დააყენეთ ეჭქვეშ თქვენი წინადადებები და გადაწყვეტილებები.

დააყენეთ კითხვის ქვეშ თქვენი უსფრთხოების მოდელები და საფრთხის მოდელები. საჭიროა გაგრძელდეს შეტევიბის ანალიზი. არ ენდოთ არავის თვით საკუთარ თავსაც კი.

აღმოჩენა და რეაგირება

შეტევის აღმოჩენა გაცილიბით მნიშვნელოვანია, ვიდრე შეტევის აღკვეთა. მთლიანად შეტევისგან დაცვა შეუძლებელია. რა თქმა უნდა საჭიროა სრულფასოვნებისკენ სწრაფვა, მგრამ ის რაც ჩვენთვის ცნობილია რთულ სისტემებთან მიმართებაში,

გვეუბნება რომ შეუძლებელია გამოვავლინოთ და გამოვასწოროთ ყველა ნაკლოვანი წერტილი. თავდამსხმელები მოიძებნებიან ყოველთვის, საჭიროა დავიჭიროთ ისნი და დავსაჯოთ.

შეტევის წინასწარ აღკვეთის მექნიზმები საჭიროა, მაგრამ ეს არის მხოლოდ პრობლემის გადაწყვეტის ნაწილი და ის ყველაზე არამდგრადი ნაწილია. დაცვის ეფექტური სისტემა აგრეთვე შეიცავს აღმოჩენისა და რეაგირების მექანიზმებს.

თავდასხმის აღმოჩენა

არის მოსაზრება, რომ თანამედროვე საზოგადოება აღკვეთს დანაშაულს. ეს არის- მითი. თუ ალისას მოუნდა ბობის მოკვლა, მას შეუძლია ეს გააკეთოს. პოლიციას არ შეუძლია შეაჩეროს ის, თუ ის არ არის სრული იდიოტი. მათ არ შეუძლიათ დაიცვან ყოველი ბობი. ბობმა თვითონ უნდა იზრუნოს თავის უსაფრთხოებაზე. მას უფლება აქვს დაიქირავოს პირადი მცველი, თუ მას აქვს ამის საშუალება, მაგრამ ესეც ვერ იძლევა გარანტიას.

ჩვეულებრივად დანაშაულს აღმოაჩენენ ხოლმე მისი ჩადენის შემდეგ. მერე იწება მისი გამოძიება, კრიფავენ ფაქტებს, რომელიც დაარწმუნებს ნაფიც მსაჯულებს ბრალდებულის დანაშაულობაში. მიიჩნევა რომ მთელი ეს ძიების პროცესი და დამნაშავის დასჯა იმოქმედებს მთლიანად საზოგადოებაზე და სხვებს დაუკარგავს მსგავსი საქციელის ჩადენის სურვილს. რა თქმა უნდა განაჩენი გამოაქვთ დამნაშავის დასჯისათვის, მაგრამ საზოგადოებისათვის

რეალური შედეგის მომტანია ის, რომ აღიკვეთოს მსგავსი დანაშაული, ე.ი. დასჯას მოაქვს პროფილაქტიკური ეფექტი.

კარგია ის რომ ეს რთული სისტემა მეტნაკლებად მუშაობს, ამიტომ დანაშაულის აღკვეთა გაცილებით რთულია, ვიდრე აღმოჩენა.

ციფრული სამყაროშიც ხდება იგივე. კომპანიები რომლებიც უშვებენ საკრედიტო ბარათებს, აკეთებენ ყველაფერს რომ აღკვეთონ თაღლითობა, ძირითადად ისინი იმედს ამყარებენ აღმოჩენის სიტემებზე, განსაკუთრებულ შემთხვევაში კი იყენებენ სასამართლო დევნას. ფიჭვური ტელეფონები შეიძლება იქნან კლონირებული, მაგრამ სწორედ აღმომჩენი მექანიზმები ზღუდავენ ფინანსურ დანაკარგებს.

ინტერნეტში შეტევის აღმოჩენა შეიძლება გახდეს რთული საქმე, არ არის საკმარისი ბრანდმაუერების დაყენებით შემოვიფარგლოთ. რადგან ჩვენ უნდა შევძლოთ თავდასხმის აღმოჩენა, მაგრამ ეს ითხოვს უზარამაზარი რაოდენობის ჩანაწერების წაკითხვას, გაგებას, და ინტერპრეტაციას, რომელიც ინახება საკონტროლო ჟურნალებში და რომელსაც აკეთებს ბრანდმაუერი, სერვერები, მარშუტიზატორები და სხვა სახის მოწყობილობები, ასე რომ სრულებით შესაძლებელია, რომ ზოგიერთმა თავდასხმამ გვერდი აუაროს ბრანდმაუერს.

შეტევის აღმოჩენა იუნდა იყოს ყოველთვის დროული. ეს ნიშნავს იმას რომ მოითხოვება კონტროლის სისტემა, რომელიც მუშაობს რეალურ დროში. რაც უფრო მალე აღმოვაჩენთ რაღაც საეჭვოს, მით უფრო მალე შეგვიძლია გავაკეთოთ რეაგირება

თავდასხმის ანალიზი

უბრალოდ შეტევის აღმოჩენა არასაკმარისია, აუცილებელია გავიგოთ – თუ რა თავდასხმაა ეს და რას ნიშნავს ის. ტრადიციულად სამხედროები ამას ყოფენ ოთხ ეტაპად:

აღმოჩენა. გააცნობიერეთ ის, რომ მოხდა თავდასხმა. ვთქვათ სამი სერვერი ერთდროულად გამოვიდა მწყობრიდან. რა არის ეს –თავდასხმაა თუ უბრალოდ პროგრამული უზრუნველყოფის პრობლემებია ქსელში? თუ შემთხვევითი დამთხვევა? და მაშინაც კი როდესაც ჩვენ არ ვიცით თავდასხმაა თუ არა, საჭიროა ადეკვატური რეაგირება.

ლოკალიზაცია. საჭიროა წერტილების განსაზღვრა, სადაც განხორციელდა თავდასხმა. თუ იმ დროსაც კი, როდესაც ჩვენ არ ვიცით

რომ ქსელმა განიცადა თავდასხამა, არ შეიძლება ადმინისტრორს არ ქონდეს ინფორმაცია იმაზე, თუ რომელი კომპიუტერები და პორტები ექვემდებარებიან თავდასხმას. ადმინისტრატორმა შეიზლება გაიგოს რომ, სერვერების მოშლა – არის თავდასხმის გამოწვეული, მაგრამ წარმოდგენაც არ ქონდეს როგორ შეძლო თავდამსხმელმა ეს და რით არის დაკავებული ახლა ის.

იდენტიფიკაცია. უნდა განისაზღვროს ვინ წარმოადგენს თავდამსხმელს და საიდან მუშაობს ის. ამან შეიძლება მოგვცეს წარმოდგენა მის სუსტ და ძლიერ მხარეზე.

შეფასება. მიზნების გაგება და თავდამსხმის მოტივი, მისი სტრატეგიები და ტაქტიკები, მისი შესაძლებლობები და საურველია მისი სუსტი ადგილები. ამ ინფორმაციის ფლობას

აქვს უდიდესი მნიშვნელობა რეაგირების საშუალებების შერჩევისთვის. რეაქცია ბავშვის ანცობაზე სავსებით განსხვავებულია, ვიდრე სამრეწველო აგენტის მოქმედებაზე.

ბავშვი სავარაუდოდ გაცილებით სწრაფად გამოერთვება კავშირიდან, თუ ჩვენ რაღაცნაირად გაუკეთებთ რეაგირებას მას. გაცილებით მყარი თავდამსხმელი არც თუ ისე იოლი გასაჩერებელია.

ყოველი შემდგომი ნაბიჯი გაცილებით რთულია ვიდრე წინამორბედი და ითხოვს უფრო დეტალურ ინფორმაციას. ხშირად მისი ანალიზისათვის საჭიროა ჩვენს მიერ დაქირავებული კვალიფიციური სპეციალისტის მონაწილეობა, მაგრამ ადრე თუ გვიან ის ვერ შეძლებს თავი გაართვას ამ დვალებას. თუმცა ავტომატურ პროგრამებს შეუძლიათ კარგად დიდხანს იმუშაონ.

ყოველ ნაბიჯზე თქვენ იღებთ უფრო და უფრო მეტ ინფორმაციას სიტუაციის შესახებ. რაც უფრო მეტ ინფორმაციას იღებთ (რაც უფრო სწრაფად) მით უფრო კარგად ხართ შეიარაღებული. სამწუხაროდ ბევრმა ქსელურმა ადმინისტრატორმა არ იციან რომ დაექვემდებარონ თავდასხამას, მაგრამ თუ იციან ვერ გაუგიათ საიდან წარმოიქმნა ისინი.

იდენტიფიკაციისა და შეფასების განხორციელება ინტერნეტში განსაკუთრებით რთულია, სადაც თავდამსხმელს ადვილად შეუძლია მის ადგილმდებარეობის მასკირება.

სისწრაფე არსებითია. რაც უფრო სწრაფად გაანალიზებთ თავდასხმას, მით უფრო სწრაფად უპასუხებთ მას.

თავდასხმაზე პასუხი

უწყვეტად მრეკავი სიგნალიზაცია, რომელზეც არავინ რეაგირებს, არაფრით არის უკეთესი იმაზე, რომ ის საერთოდ არ არსებობდეს. პასუხი – არის ის, რისთვისაც გვინდა აღმოჩენის საშუალებები.

ზოგჯერ რეაგირება ადვილია: თუ მოპარულია სატელეფონო ბარათის ნომერი, ესიგი საწიროა ანულირება. ზოგჯერ ხდება რათული: ვიღაცამ შეაღწია ელექტრონული მაღაზიის სერვერში, შესაძლებელია დავხუროთ სერვერი, მაგრამ დანაკარგები შეადგენს 10 მილიონ დოლარსს. და რა ვქნათ?

პასუხი არ არის მარტივი, მაგრამ ხშირად ხდება, რომ ადამიანები იღებენ ბრძნულ გადაწყვეტილებებს წამებში. "ვიღაცა აძვრა კედელზე და უახლოვდება დამინულ სახურავს. რა გავაკეთოთ ჩვენ ეხლა?" ეს ბევრად დამოკიდებულია სიტუაციაზე. მაგრამ თქვენ არ შეგიძლიათ არ ვიმოქმედოთ. შესაძლებელია უბრალოდ გააგდოთ ის. შესაძლებელია გააგდოთ ის და დარწმუნდეთ რომ ის მეტჯერ უკან არ მობრუნდება. შესაძლებელია გააგდოტ ის და განსაზღვროთ როგორ შეძლო მან მოხვედრა სახურავზე და დავხუროთ ნაკლოვანი ადგილი

თავდასხმის აღკვეთა - ეს არის მხოლოდ საქმის ნახევარი. არა ნაკლებ მნიშვნელოვანია კვალში გაყოლა და დამნაშავის მიგნება. ზოგიერთ შემთხვევაში ეს ძალიან რთულია: მაგალითად ინტერნეტში თავდამსხმელი შეიძლება გადადის ერთი კომპიუტერიდან მეორეში, რომ "დამალოს კვალი". პოლიციას არ შეუძლია ხარჯოს დიდი დრო მსგავსი

შემთხვევების გამოძიებაძე, მანამ სანამ არ იქნება მოზიდული დამატებით ადამიანური და ფინანსური რესურსები. კერძო კომპანიებს შეუძლიათ დახმარება გაუწიონ მართსაჯულებას, მაგალითად შეაგროვონ ზოგიერთ თავდამსხმელებზე დოსიეები.

სასამართლო გარჩევებთან შეჯახებისას, მრავალი ადამიანი კომპიუტერული სამყაროდან, უცხოები სამართლის სფეროში, აღმოაჩენენ, როგორი უძირო არის ის. საკმარისი არ არის იდენტიფიცირებულ იქნას თავდამსხმელი, აუცილებელია დავამტკიცოთ კიდეც სასამართლოსი. ინგლისში ცდილობდნენ მიეცათ პასუხისმგებლობაში ბრალდებული, საკრედიტი ბარატებით თაღლითობის გამო. როგორ მიდის განხილვა სასამართლოში?

ადვოკატი ითხოვს დაწვრილებით წარმოადგინონ ბანკის მიერ გამოყენებული დაცვის საშუალებებზე ინფორმაცია: ტექნოლოგიის აღწერა, საკონტროლო ჟურნალის ჩანაწერები, და ყველაფერი ის რაც მას თავში მოუვა. ბანკის თავმჯდომარე მიმართავს სასამართლოს: "ჩვენ არ შეგვიძლია მოგაწოდოთ ეს ინფორმაცია, რამდენადაც ეს ჩვენ დაცვის სისტემას მიაყენებს ზიანს". მოსამართლე წყვეტს საქმეს. უსაფრთხოების სისტემა შესაძლებელია იყოს აღმოჩენის იდეალური ნიმუში, მას შეიძლებოდა სწორად მიეთითებინა დამნაშავე, მაგრამ თუ ის ვერ გადაიტანს ინფორმაციის გახსნის პროცესს, ეს ნიშნავს, რო ის არასაკმარისად სასარგებლო.

როდესაც ჯონ უოკერი წარსდგა სასამართლოს წინაშე ჯაშუშობის გამო, ნაციონალური უსაფრთხოების სააგენტომ მოითხოვდა რომ: გახსინილიყო ინფორმაცია იმის იმის შესახებ, თუ როგორ გატეხა დაშიფრვის მექანიზმი უოკერმა

და ნამდვილი ზარალი, რომელიც მიადგა სააგენტოს შენახულიყო საიდუმლოდ.

კარგმა აღმოჩენის საშუალებებმა უნდა აიტანოს სასამართლო პოცესები, რომელბიც შეიცავენ ჯვარედინ დაკითხვებს ექსპერტების მოწვევით და ამით მათმა უნდა შეინარჩუნოს ეფექტურობა. კარგი აღმოჩენის და კონტროლის საშუალებები ვალდებულია გააკეთონ ჩანაწერები სააღრიცხვო ჟურნალში, რომლებიც შეიძლება გამოდგეს

სასამართლოში, როგორც მტკიცებულება. უნდა იყოს შესაძლებელებლობა დემონსტრირებულ იქნას ყველა ჩანაწერი, უსაფრთხოების საიდუმლოების გახსნის გარეშე.

სიფხიზლით ყოფნა

სიფხიზლე არ უნდა დავკარგოთ არასდროს. იმისათვის აღმოჩენა და რეაგირება იყოს ეფექტური, აუცილებელია ვიმუშაოთ: 24 საათი კვირაში, 365 დღე წელიწადში. დაცვის სამსახურები მუშაობენ დღე და ღამე. კომპანიები, რომლებიც ემსახურებიან დაცვის სისტემით სხვა ორგანიზაციებს მუშაობენ უწყვეტად. კომპიუტერულ სამყაროში არ შეიძლება იყოს სხვაგვარად.

თავდასხმა ხორციელდება ხშირად მაშინ, როდესაც მისთვის მზად არ ხართ. ჰაკერული თავდასხმები დაკავშირებულია აკადემიური წლის განსაზღვრულ პერიოდებთან. ყველა სახის თაღლითობა დაკავშირებული საკრედიტო ბარათებთან, ბანკომატებთან ხორციელდება ხშირად სააღდგომო დღესასწაულებისას, საბანკო სისტემები

ტყდებიან ხშირად პარასკევს დღის მეორე ნახევში, როდესაც ბანკები იკეტებიან დასასვენებლად.

სიფხიზლე ნიშნავს დროულ აღმოჩენას და რეაგირებას. დროულ თავდასხმის აღმოჩენას, რომელიც მიმდინარეობს, გაცილებით დიდი მნიშვნელობა აქვს, ვიდრე მის აღმოჩენას ერთი კვირის შემდეგ

სიფხიზლე აგრეთვე ნიშნავს მომზადებასაც. აუცილებელია ნათლად წარმოვიდგინოთ, რა გავაკეთოთ თავდასხმის შემთხვევაში. 2000 წელს, როდესაც yahoo-მ განიცადა თავდასხმა, რომელმაც ის მიიყვანა მომსახურების შეჩერებამდე, აღდგენისთვის დაჭირდათ 3 საათი. ნაწილობრივ ეს იმიტომ მოხდა რომ მანამდე მას არასდროს განუცდია მსგავსი ტიპის თავდასხმა. როდესაც ყველაფერი მიდის კარგად, ადამიანები ივიწყებენ, როგორ უნდა მოხდეს რეაგირება განსაკუთრებულ სიტუაციაში.

თავდასხმის შედეგების გამოსწორება

2000 წელს იქნა გატეხილი ფრანგული სმარტ ბართი. რაიმეს გაკეთება იყო შეუძლებელი, გარდა ყველა ოპერაციის შეწყვეტისა რომელიც დაკავშირებული იყო მასთან. თუ ყველა თქვენი დრო მიდის აღკვეთის ზომების მოფიქრებაზე, მაშინ შესაძლებელია თქვენ სავსებით ჩამორჩეთ იმ მოქმედებების გეგმას რომელიც დკავშირებულია

აღმკვეთი ზომები ყოველთვის აღმოჩნდებიან არაეფექტური. პრობლემების გამოსწორება მგანსაკუთრებით მნიშვნელოვანია, მაგრამ არა ნაკლებ მნიშვნელოვანია სისტემის მოყვანა წესრიგში თავდასხმის შემდეგ. სისტემის

შექმნისას საჭიროა ორინტირება გაკეთდეს მის მოდერნიზაციის შესაძლებლობაზე, ექსპლუატაციის პროცესში. აგრეთვე სასურველია გავითვალისწინოთ სპეციალური შიფრაციის საშუალებები, პროტოკოლები და პროცედურებია, რომლებიც იქნება გამოყენებული განსაკუთრებულ სიტუაციაში. ამით შესაძლებელია შევამციროთ დანაკარგები და სწრაფად აღვადგინოთ სისტემის მუშაობა.

პოლიტიკის მაგალითი კორპორაციულ ქსელზე

მიზანი: თანამშრომლების მიერ კომპიუტერების და კომპანიის ტელეკომუნიკაციური რესურსების გამიზნული გამოყენება.

ყველა კომპიუტერის მომხმარებელი ვალდებულია გამოიყენოს კომპიუტერული რესურსი კვალიფიციურად, ეფექტურად, კანონის და ეთიკის დაცვით.

პოლიტიკა, მისი წესები და პირობები ეხება ყველა კომპიუტერების და კომპანიის ტელეკომუნიკაციური რესურსების მომხმარებლებს და კომპანიის სასახურებს, სადაც არ უნდა იყვნენ ეს მომხმარებლები. ამ წესების დარღვევას უნდა მოსდევდეს დისციპლინარული მოქმედება და საერთოდ სამსახურიდან დათხოვნაც ან სისხლის სამართლის საქმის აღძვრა.

აღნიშნული პოლიტიკა შესაძლებელია აუცილებლობის შემთხვევაში პერიოდულად შეიცვალოს ან გადაიხედოს.

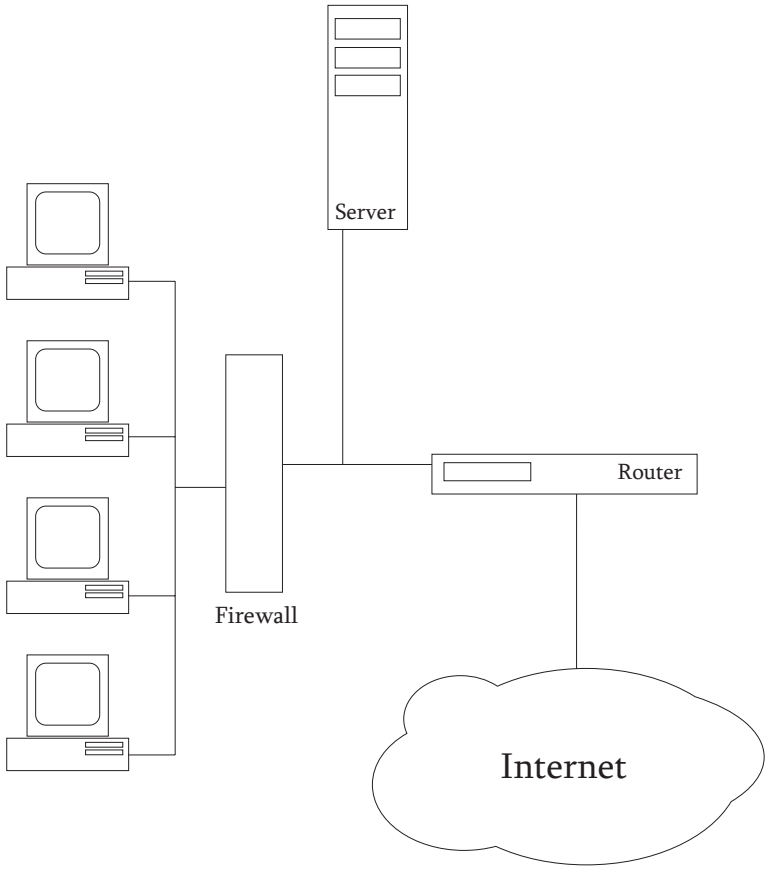
- კომპანისა აქვს უფლება, მაგრამ არა აუცილებლობა შეამოწმოს ქსელის ნებისმიერი ან ყველა კომპონენტი,

ელ ფოსტის ჩათვლით, არღნიშნული პოლიტიკის შესრულების მიზნით. კომპიუტერები და სხვა რესურესები ეძლევათ თანამშრომლებს, იმიტომ რომ ეფექტურად შეასრულონ თავისი სამუშაო

- კომპიუტერები და ტელეკომუნიკაციური რესურსები ეკუთვნის კომპანიის და შესაძლებელია მისი გამოყენება მხოლოდ მუსაობის მიზნით. კომპანიის თანამშრომლები რომლებიც გადასცემენ ან იღებენ ინფორმაციას კომპანიის კომპიუტერებით და საკომუნიკაციო არხებით, არ უნდა თვლიდნენ რომ მათი ინფორმაცია იქნება კონფიდენციალური
- კომპიუტერების მომხმარებლებმა უნდა იხელმძღვანელონ ქვემოთ ჩამთვლილი წინდახედულობის ზომებით, კომპიუტერებთან და კომპანიის ტელეკომუნიკაციური რესურსებთან მიმართებაში. კომპიუტერები, ტელეკომუნიკაციური რესურსები და სამსახურები შეიცავენ (მაგრამ არ იზღუდებიან): ჰოსტ –კომპიუტერები, ფაილების სერვერი, სამუშაო მანქანები, მობილური კომპიუტერები, პროგრამული უზრუნველყოფა და შიდა და გარე ქსელური კავშირები, რომლებთანაც პირდაპირ ან ირიბად საქმე აქვთ კომპანიის კომპიუტერულ მოწყობილობებს.
- კომპანიის თანამშრომლები უნდა იცავდნენ ყველა პროგრამული ლიცენზიის პირობებს, საავტორო უფლებას და კანონებს რომელიც ეხება ადმიანის ინტელექტუალურ საკუტრებას

- არასწორი, შეურაწმყოფელი, მუქარის, კანონსაწინააღმდეგო და სხვა მსგავსი წერილების გაგზავნა ელ ფოსტით იკრძალება, აგრეთვე გამოვსახოთ ან შევინახოთ ისინი კომპიუტერში. მომხმარებლები რომლებიც შემჩნეული იქნებიან მსგავს ქმედებაში, აუცილებელია დაუყონებლივ ეცნობოს ამის შესახებ ხელმძღვანელობას
- ყველაფერი რაც შექმნილა კომპიუტერში შესაძლებელია გაანალიზებულ იქნას კომპანიის ხელმძღვანელობის მიერ.
- მომხმარებლებს არა აქვთ უფლება კომპიუტერში ან ქსელში დააყენონ პროგრამა რომელიც არ არის შეთანხმებული სისტემის ადმინისტრატორთან.
- მომხმარებლებს ეკრძალებათ ფაილების შეცვლა და კოპირება, რომელიც ეკუთვნის სხვა მომხმარებლს, მისი ნებართვის გარეშე
- მომხმარებელი იღებს პასუხისმგებლობას თავიანთი პაროლის დაცვაზე, რომელიც საჭიროა სისტენაში შესასვლელად. იკრძალება ინდივიდუალური პაროლის დაბეჭდა, ქსელში შენახვა ან მისი მიცემა სხვა მომხმარებლისათვის. მომხმარებელი პასუხისმგებელია ყველა ტრანზაქციაზე, რომელიც განხორციელდა მის პაროლის საშუალებით.

ორგანიზაციის ქსელის შესაძლო ტოპოლოგია



საინფორმაციო სისტემების საიმედოობის უზრუნველყოფა

საინფორმაციო სისტემების საიმედოობის უზრუნველყოფა ორ ძირითად ამოცანად იყოფა. ესენია:

ა) საინფორმაციო სისტემების გამართული მუშაობის უზრუნველყოფა

ბ) ინფორმაციის საიმედოდ შენახვის უზრუნველყოფა

საინფორმაციო სისტემების გამართული მუშაობისათვის აუცილებელია უზრუნველვყოთ როგორც ტექნიკის, ასევე პროგრამული უზრუნველყოფის გამართული მუშაობა.

საიმედოობის უზრუნველყოფისათვის გამოიყენება ტექნიკური და პროგრამული საშუალებები და ორგანიზაციული მეთოდები.

ტექნიკურ საშუალებები მიეკუთვნება:

1. უწყვეტი კვების წყაროები
2. სარეზერვო კოპირების აპარატურა
3. RAID სისტემები
4. კლასტერები

პროგრამულ საშუალებებია:

1. სისტემის კვების მენეჯმენტის საშუალებები
2. სარეზერვო კოპირების სისტემები
3. RAID-ის პროგრამული უზრუნველყოფია სისტემები
4. კლასტერების პროგრამული უზრუნველყოფა

ორგანიზაციულ მეთოდებში იგულისხმება მომსახურე პერსონალის და პროგრამული საშუალებების მუშაობის ისეთი გრაფიკის შედგენა, ასევე მომსახურე პერსონალის უფლებამოსილებების ისეთ განაწილებას, რომელიც მაქსიმალურად გაზრდის სისტემის საიმედოობას.

უწყვეტი კვების წყაროები (UPS) უზრუნველყოფს სისტემის გამართულ მუშაობას ელექტროენერგიის მიწოდების შეფერხებების მიუხედავად. გარდა ამისა ისინი იძლევიან საშუალებას კვების ავარიული გამორთვის დროს სისტემამ ნორმალურად დაამთავროს მუშაობა. სისტემის კვების მენეჯმენტის საშუალებები განკუთვნილია უწყვეტი კვების წყაროების ოპტიმალური მართვისათვის. ისინი ჩართულია როგორც ოპერაციულ სისტემებში, ასევე წარმოდგენილია როგორც ცალკე პროგრამული საშუალებების სახით.

სარეზერვო კოპირების სისტემები განკუთვნილია მონაცემების არქივირებისა და სარეზერვო კოპირებისათვის. არქივირება გულისხმობს ინფორმაციის შენახვას დიდი ხნით მისი შემდგომ შესაძლო გამოყენებისათვის. ჩვეულებრივ არქივირება ეხება იმ ინფორმაციას, რომელიც ოპერატიულად აღარ არის საჭირო და შეიძლება მისი გადატანა ხისტი დისკებიდან სხვა (CD, DVD, მაგნიტოოპტიკური დისკი, მაგნიტური ფირი და სხვ.) მატარებლებზე. სარეზერვო კოპირება გულისხმობს სამუშაო ინფორმაციის და სისტემური ფაილების გადატანას ხისტი დისკებიდან სხვა მატარებელზე (DVD, მაგნიტოოპტიკური დისკი, მაგნიტური ფირი) ავარიის დროს ოპერატიული აღდგენისათვის.

სარეზერვო კოპირების სიტემები შედგება აპარატურული მოწყობილობებისაგან და პროგრამული ნაწილისაგან.

სარეზერვო კოპირების აპარატურა ძირითადად წარმოდგენილია მაგნიტურ ფირზე ჩამწერი მოწყობილობების სახით. თუმცა შესაძლებელია გამოვიყენოთ DVD, მაგნიტოოპტიკური დისკი ან თუნდაც ხისტი დისკები. მაგნიტური ფირები დღეისათვის ყველაზე ოპტიმალური გადაწყვეტაა ტევადობის, შენახვის საიმედოობის და ოპერატიულობის გათვალისწინებით. არსებობს ფირზე ჩამწერი ცალკეული მოწყობილობები (სტრიმერი), სადაც ფირის ცვლა ოპერატორის მიერ ხელით ხდება, და მაგნიტური ფირების ბიბლიოთეკები, სადაც ფირების შეცვლა ჩამწერ მოწყობიულობაში ავტომატურად, სპეციალური რობოტ-მანიპულატორების საშუალებით ხორციელდება. შესაბამისად თუ ერთი ფირის მოცულობა რამოდენიმე გიგაბაიტიდან ასეულ გიგაბაიტამდე განისაზღვრება, ბიბლიოთეკები ასეული გიგაბაიტებიდან ასეულობით ტერაბაიტამდე მოცულობის ინფორმაციას იტევს. სარეზერვო კოპირების აპარატურის ყველაზე მძლავრი კომპლექსები რამოდენიმე ბიბლიოტეკის გაერთიანებით იქმნება და მათი მოცულობა უკვე ათასობით ტერაბაიტით იზომება.

სარეზერვო კოპირების პროგრამული უზრუნველყოფა განკუთვნილია ინფორმაციის შენახვის ავტომატიზაციისათვის. ის საშუალებას იძლევა როგორც ცალკეული ოპრაციების განხორციელების, ანუ როდესაც ჩვენ გვინდა მაშინ გავაკეთოთ სარეზერვო კოპირება, ასევე სარეზერვო კოპირების ავტომატურად განრიგით განხორციელებისათვის.

სარეზერვო კოპირება სამი სახისაა. ესენია:

1. სრული კოპირება
2. ინკრემენტული კოპირება

3. დიფერენციალური კოპირება

სრული კოპირების დროს ინფორმაცია მთლიანად იწერება მაგნიტურ ფირზე. კოპირების ეს ტიპი ყველაზე სწრაფია ინფორმაციის აღდგენის დროს, თუმცა მას დიდი დრო მიაქვს ინფორმაციის შენახვისას.

ინკრემენტული კოპირების დროს თავიდან ხდება ინფორმაციის სრული კოპირება, ხოლო ყოველი შემდგომი კოპირებისას ფირზე იწერება მხოლოდ ბოლო ცვლილებები. ინფორმაციის აღდგენისათვის ჯერ აღდგება პირველადი მდგომარეობა, და შემდეგ ყველა შემდგომი ცვლილება. ეს მეთოდი ნაკლებ დროს მოითხოვს ინფორმაციის შენახვისას, თუმცა აღდგენისათვის მას მეტი დრო სჭირდება.

დიფერენციალური კოპირებისას ფირზე ინახება საწყისი მთლიანი კოპია და ბოლო საწყისისაგან განსხვავებული ინფორმაცია. ეს მეთოდი ცოტა ნელია შენახვისას, ვიდრე ინკრემენტული, თუმცა უფრო სწრაფი ინფორმაციის აღდგენისას.

სარეზერვო კოპირების პროგრამული უზრუნველყოფა წარმოდგენილია როგორც ცალკეული პროგრამული საშუალებების სახით, ასევე ჩართულია ოპერაციულ სისტემებში. ოპერაციული სისტემის სარეზერვო კოპირების სერვისი გვაძლევს საშუალებას განვახორციელოდ როგორც ფაილების და კატალოგების ერთჯერადი კოპირება, ასევე მარტივი გრაფიკის შედგენა თუ როდის უნდა მოხდეს ამა თუ იმ ფაილის ან კატალოგის კოპირება.

სარეზერვო კოპირების უფრო სრულყოფილი სისტემები მუშაობენ ქსელებში და უზრუნველყოფენ ქსელის მომსახურეობას. ისინი შედგებიან სამი ნაწილისაგან:

1. სარეზერვო კოპირების სერვერი
2. სარეზერვო კოპირების აგენტები
3. სარეზერვო კოპირების მართვის კონსოლი

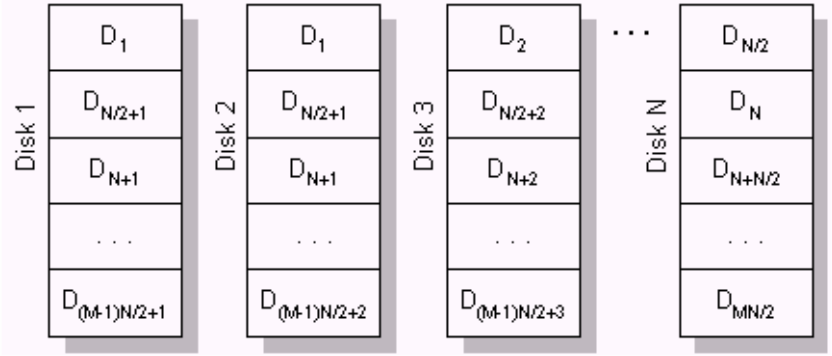
სარეზერვო კოპირების სერვერი თავსდება იმ კომპიუტერზე, რომელზედაც მიერთებულია სარეზერვო კოპირების მოწყობილობა. ის უზრუნველყოფს ინფორმაციის გადატანას მაგნიტურ ფირებზე, აღდგენას და კოპირების განრიგის რეალიზაციას.

სარეზერვო კოპირების აგენტები ეშვება სამუშაო სადგურებზე (Workstation) და უზრუნველყოფს კოპიურებისათვის განკუთვნილი ინფორმაციის კონტროლს და სერვერიდან მიღებული ბრძანებების მიხედვით კოპირებისათვის განკუთვნილი ინფორმაციის გადაგზავნას სერვერზე არქივაციისათვის. ასევე ისინი უზრუნველყოფენ ინფორმაციის აღდგენას.

სარეზერვო კოპირების მართვის კონსოლი ეშვება იმ კომპიუტერზე, სადაც მუშაობს სისტემის ადმინისტრატორი და განკუთვნილია სისტემის მართვისათვის. მისი საშუალებით შესაძლებელია ინფორმაციის ერთჯერადი კოპირება, სარეზერვი კოპირების განრიგის შეცვლა და ინფორმაციის აღდგენა მაგნიტური ფირიდან.

RAID სისტემები განკუთვნილია დისკური მასივების საიმედოობის გაზრდისათვის. არსებობს RAID-ის რამოდენიმე სახეობა. განვიხილოთ ყველაზე გავრცელებული RAID-1, RAID-2, RAID-3 და RAID-5.

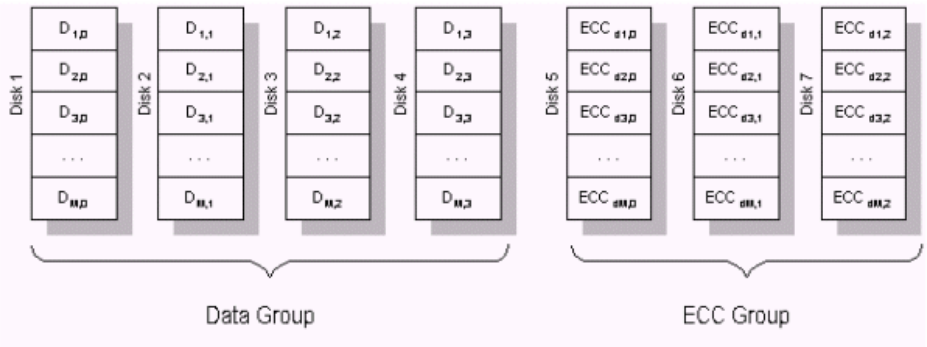
RAID-1 - დისკური მასივი დუბლირებით ანუ სარკე. დიკური მასივი დუბლირებით გულისხმობს, რომ ინფორმაცია დუბლირდება ჩაწერის პროცესში და იწერება ორ დისკზე პარალელურად. ერთი დისკის მწყობრიდან გამოსვლის შემთხვევაში ჩვენ გვრჩება მეორე კოპია და სისტემა ინფორმაციის მთელი მასივის კოპიას აღადგენს დაზიანებული დისკის გამოცვლის შემდეგ.



RAID 1

RAID-1-ის უპირატესობაა სიმარტივე და სისწრაფე, ნაკლი კი მისი ძვირადღირებულებაა.

RAID-2 - დისკური მასივი ჰემინგის კოდის გამოყენებით. ჭარბი კოდირება, რომელიც გამოიყენება RAID-2-ში ატარებს ჰემინგის კოდის სახელს. ეს კოდირება იძლევა ერთმაგი ან ორმაგი შეცდომების გასწორების საშუალებას.

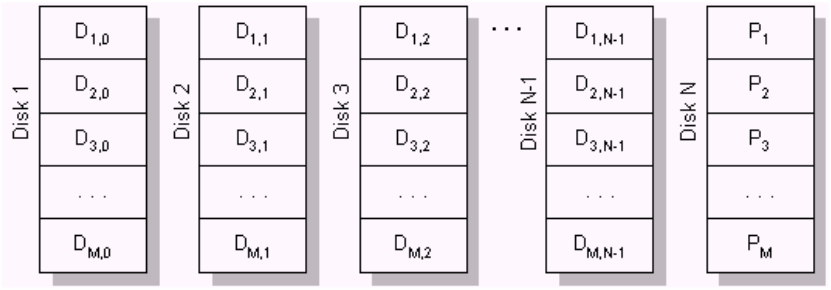


RAID 2

7 დისკის შემთხვევაში 4-ზე იწერება მონაცემები, ხოლო 3-ზე ე.წ. ECC კოდი, რომელიც იძლევა ინფორმაციის აღდგენის საშუალებას იმ შემთხვევაში, თუ ერთი ან ორი დისკი გამოვიდა მწყობრიდან. ეს სისტემა მოსახერხებელია დიდი რაოდენობის დისკების გამოყენების შემთხვევაში და იძლევა ინფორმაციის სწრაფად გასწორების შესაძლებლობას.

RAID-3 სისტემაში გამოიყენება ე.წ. საკონტროლო ჯამი. ინფორმაციის თითო-თითო ბიტი იწერება N დისკზე, ხოლო ერთ დისკზე იწერება ამ ბიტების ჯამი მოდულით ორი:

$$P_i=D_{1,i}\oplus D_{2,i}\oplus D_{3,i}\oplus\ldots\oplus D_{N,i}$$

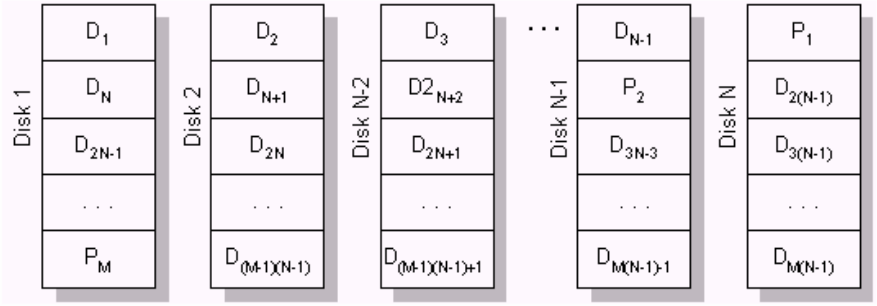


RAID 3

ერთი დისკის მწყობრიდან გამოსვლის შემთხვევაში შესაძლებელია მისი აღდგენა დანარჩენი ინფორმაციით:

$$D_{x,i} =D_{1,i}\oplus D_{2,i}\oplus\ldots\oplus D_{x-1,i}\oplus D_{x+1,i}\oplus\ldots\oplus D_{N,i}\oplus P_i$$

RAID-5 გამოირჩევა საკონტროლო ჯამის ყველა დისკზე განაწილებით, რაც ამაღლებს დისკების წარმადობას მცირე მოცულობის ინფორმაციის ბლოკების ჩაწერისას.



RAID 5

საინფორმაციო სისტემების საიმედოობის გასაზრდელად აგრეთვე გამოიყენება **კლასტერები**. კლასტერი ორი ან რამოდენიმე კომპიუტერის გაერთიანებაა საერთო საკომუნიკაციო სივრცეში გამოთვლითი ამოცანების ერთობლივი გადაწყვეტისათვის. კლასტერში ამოცანების განაწილება სხვადასხვა კომპიუტერზე ხდება სპეციალური პროგრამული უზრუნველყოფის საშუალებით. კლასტერში შემავალი კომპიუტერები შეიძლება მუშაობდნენ სხვადასხვა ოპერაციულ სისტემების (Window, Linux, Solaris და სხვ.) ქვეშ. კლასტერის რომელიმე კომპიუტერის მწყობრიდან გამოსვლის შემთხვევაში ამოცანები ნაწილდება სხვა მუშა კომპიუტერებს შორის. ეს იძლევა საშუალებას მწყობრში ჩავაყენოთ ან გამოვცვალოთ დაზიანებული კომპიუტერი ისე, რომ სისტემის მუშაობა არ შეფერხდეს. კლასტერში გასაერთიანებლად გამოიყენება მაღალი წარმადობის ქსელები. კლასტერები არსებობს ორი სახის: საერთო დისკური მასივით და განაწილებული დისკური მასივით. საერთო დისკური მასივის გამოყენება ზრდის სისტემის წარმადობას, თუმცა მოითხოვს უფრო ძვირადღირებულ აპარატურას საერთო დისკურ მასივზე პარალელურად რამოდენიმე კომპიუტერის მუშაობის უზრუნველსაყოფად.

სარჩევი

გამოყენებული ლიტერატურა

1. Cisco Network security (cisco.netacad.net);
2. V. Gorodetsky, I. Kotenko, Computer Network Security. 2007, 416p., ISBN: 978-3-540-73985-2;
3. C.A. Henk, Encyclopedia of Cryptography and Security. 2005, 684p., ISBN: 978-0-387-23473-1;
4. М. Уэнстром, Организация защиты сетей , Из: Вильямс, 2005, ISBN: 5-8459-0387-4;

იბეჭდება ავტორის მიერ წარმოდგენილი სახით

გადაეცა წარმოებას 02.11.2007. ხელმოწერილია დასაბეჭდად 04.12.2007. ქაღალდის ზომა 60X84 1/16. პირობითი ნაბეჭდი თაბახი 8. ტირაჟი 100 ეგზ.

საგამომცემლო სახლი "ტექნიკური უნივერსიტეტი", თბილისი,
კოსტავას 77