Georgian Scientists
ქართველი მეცნიერები
Vol. 6 Issue 3, 2024
https://doi.org/10.52340/gs.2024.06.03.01

ქსელური შეტევების აღმოჩენის არსებული სისტემების მიმოხილვა და ანალიზი

ქართველიშვილი იოსები[1], ოხანაშვილი მაია[2], .აბულაძე ინგა[3], .ჩორხაული ნინო[4], დარჩაშვილი მიხეილი[5]

1პროფესორი, საქართველოს ტექნიკური უნივერსიტეტი, s.qarTvelishvili@gtu.ge, ORCID: 0000-0001-9890-4099; 2ასოცირებული პროფესორი, საქართველოს ტექნიკური უნივერსიტეტი, m.okhanashvili@gtu.ge, 3ასოცირებული პროფესორი, საქართველოს ტექნიკური უნივერსიტეტი, i.abuladze@gtu.ge, 4ასოცირებული პროფესორი, საქართველოს ტექნიკური უნივერსიტეტი, n.chorkhauli@gtu.ge; ინფორმატიკის დოქტორი, საქართველოს ტექნიკური უნივერსიტეტი, misha8003123@gmail.com

აბსტრაქტი

დიდი ხნის განმავლობაში ტარდება კვლევები კომპიუტერულ ქსელებსა და სისტემებზე თავდასხმების აღმოჩენის სფეროში. გამოკვლეული იქნა თავდასხმების ნიშნები, შემუშავდა და გამოიყენება უნებართვო შეღწევის მცდელობის გამოვლენის მეთოდები და საშუალებები უსაფრთხოების სისტემების საშუალებით, როგორც ინტერნეტის, ასევე ადგილობრივ, ლოგიკურ და ფიზიკურ დონეზე. სხვადასხვა უცხოური კომპანიების (Cisco, Snort, ISS RealSecure, და ა.შ.) მიერ ადგილობრივ ბაზარზე შეტევის აღმოჩენის კომერციული სისტემები ფართოდ არის წარმოდგენილი. მრავალი ადგილობრივი მკვლევარი იყენებს უკვე ცნობილი სისტემების არქიტექტურულ ანალოგებსა და ტიპიურ გადაწყვეტილებებს.

უკანასკნელ წლებში მკვეთრად გაიზარდა კომპიუტერულ ქსელებში უნებართვო შეჭრის ორგანიზების სხვადასხვა ტიპისა და მეთოდების რაოდენობა. აქედან გამომდინარე, შეტევების აღმომჩენი სისტემები ორგანიზაციების უსაფრთხოების ინფრასტრუქტურისთვის გახდა მნიშვნელოვანი კომპონენტი. ამას ხელს უწყობს დიდი რაოდენობით ლიტერატურული წყაროების, რთული მიდგომებისა და მეთოდების გამოჩენა საინფორმაციო სისტემებში შეტევების გამოვლენისათვის.

ნაშრომში წარმოდგენილი ქსელური შეტევების აღმოჩენის არსებული სისტემების მიმოხილვის მიზანს წარმოადგენს ამჟამად ხელმისაწვდომი შეტევების აღმომჩენი სისტემების IDS (Intrusion Detection System)-ების ფუნქციონალების გამოკვლევა და გამოყენებული შეტევის აღმოჩენის მეთოდების ნაკლოვანებებისა და მათი გამოყენებადობის უარყოფითი მხარეების გამოვლენა. თავდასხმის გამოვლენის არსებული სისტემების რეალიზაციები შეიძლება დაიყოს ორ ნაწილად: კვლევით და კომერციულ პროდუქტებად.

ყოველი ახალი კვლევითი პროექტი გამოირჩევა ანალიზის ახალი მეთოდების დანერგვითა და მონიტორინგის ობიექტების შესწავლის ახალი მიდგომებით, თუმცა ისინი

სწრაფად მოძველებადია. კომერციული პროექტები (როგორიცაა ISS RealSecure, Symantec Network Security, Cisco IPS და ა.შ.) მწარმოებლების მხარდაჭერის გამო უფრო დიდხანს რჩება აქტუალური. მწარმოებლები უზრუნველყოფენ მომხმარებლების მუდმივი მხარდაჭერას, ახალი შეტევების კვლევასა და ხელწერის განახლებებს. აქედან გამომდინარე, შეიძლება აღვნიშნოთ რომ კომერციული კვლევის შედეგების უმეტესობა არის ბოროტად გამოყენების გამოვლენის სისტემები, კერძოდ, ხელწერის სისტემები.

შეტევების აღმომჩენი სისტემები IDS წარმოადგენს პროგრამულ და აპარატურულ-პროგრამულ გადაწყვეტილებებს, სადაც კომპიუტერულ სისტემაში ან ქსელში მომხდარი მოვლენების შეგროვების, შენახვისა და ანალიზის (მონიტორინგის) პროცესები ავტომატიზებულად ხდება, აგრეთვე ამ მოვლენებს ინფორმაციის უსაფრთხოების დარღვევების ნიშნების ძიებაში დამოუკიდებლად აანალიზებს. ეს დაცვის სისტემები არსებობს როგორც პროგრამები, რომლებსაც შეტყობინების გამოტანა შეუძლიათ იმის შესახებ, რომ აღნიშნულ მომენტში ადგილი ჰქონდა ქსელურ შეტევას. სისტემები, რომლებიც გამოიყენება ქსელური შეტევების დასადგენად მხოლოდ ერთ კონკრეტულ ამოცანას აგვარებს - დაცვა გარე შემტევი პირისგან, რომელიც ცდილობს გვერდი აუაროს დაცვის სისტემებს და მოიპოვოს წვდომა ადგილობრივ ლოკალურ ქსელზე, მაგრამ შიდა საფრთხეების განხორციელებისგან დაცვის პრობლემა გადაუჭრელ ამოცანად რჩება.

ყველა ცნობილი IDS პირობითად იყოფა სამ კლასად:

- ქსელური IDS (ქსელზე დაფუძნებული (Network-based) IDS, NIDS);
- კვანძოვანი IDS (ჰოსტზე დაფუძნებული (Host-based) IDS, HIDS);
- ჰიბრიდული IDS (ჰიბრიდული (Hybrid) IDS).

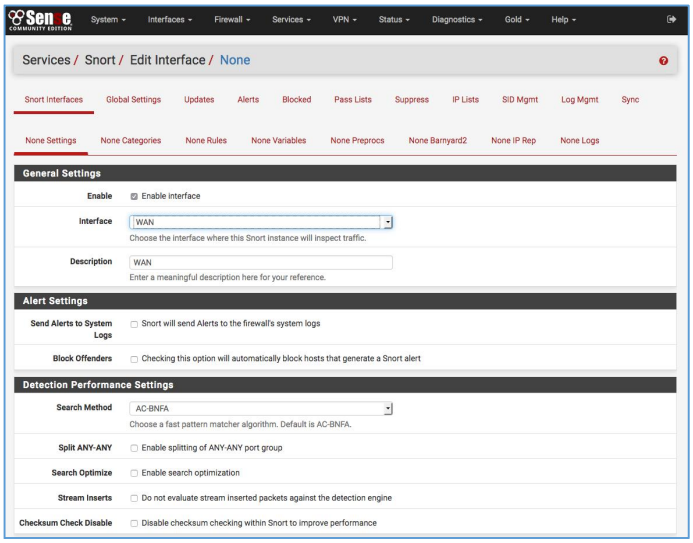
კვანძოვანი IDS-ები შეიძლება დაიყოს კიდევ ორ ქვეკლასად: სისტემის დონის IDS და განაცხადის დონის IDS (აპლიკაციაზე დაფუძნებული (application-based) IDS).

საკვანძო სიტყვები: შეტევების აღმომჩენი სისტემა Snort. შეტევის აღმომჩენი სისტემა Bro. შეტევის აღმოჩენის სისტემა STAT. შეტევის აღმომჩენი სისტემა Prelude. შეტევების აღმომჩენი სისტემა OSSEC. აპარატურულ-პროგრამული საშუალება Cisco Secure IPS. შეტევების აღმომჩენი სისტემა RealSecure (IBM ISS). შეტევების აღმომჩენი სისტემა Symantec Network Security. სისტემა eTrust Intrusion Detection Computer Associates.

შეტევების აღმომჩენი სისტემა Snort

შეტევების აღმომჩენი სისტემა Snort თავისუფლად გავრცელებული ქსელის დონის თავდასხმის გამოვლენის სისტემას წარმოადგენს. პროგრამა მონაცემთა გადაცემის პროტოკოლებს აანალიზებს, სხვადასხვა შეტევებს აფიქსირებს, მაგალითად, ბუფერის გადავსებას, ქსელის სკანირებას, CGI შეტევებს, ოპერაციული სისტემის დადგენის მცდელობებს და ა.შ. Snort სისტემა ტრაფიკში თავდასხმების მოსაძებნად იყენებს სპეციალურ წესებს. პროგრამა 3 რეჟიმში მუშაობს: sniffer, packet logger და network intrusion detection system.

პირველ შემთხვევაში, სისტემა ასკანირებს პაკეტებს ქსელის დონეზე და მათ შესახებ აჩვენებს ინფორმაციას კონსოლში, მეორეში იგი წერს დისკზე ჟურნალის ფაილებს, მესამეში შეტევის ხელმოწერების შესატყვისად აანალიზებს ქსელის ტრაფიკს და აგზავნის მათ სიგნალს.



ნახ.1

ყველა აღმოჩენილი ხელმოწერა ერთ კონფიგურაციის ფაილშია აღწერილი. ყველა რეგისტრირებული მოვლენა შეიძლება ჩაიწეროს, როგორც საკუთარ ჟურნალსა ან ოპერაციული სისტემის ჟურნალში, ასევე მონაცემთა ბაზაში (MSSQL ან Oracle)

შეტევის აღმომჩენი სისტემა Bro

შეტევის აღმოჩენის სისტემა **Bro** წარმოადგენს კვლევის ინსტრუმენტს, რომელიც შემუშავებულია აშშ-ს ენერგეტიკის დეპარტამენტის ლივერმორის ეროვნული ლაბორატორიის მიერ. იგი შეიქმნა პრობლემების შესასწავლად ქსელის შეტევის აღმოჩენის სისტემების შეცდომის ტოლერანტობისთვის. სისტემის ძირითად მახასიათებლებს წარმოადგენს:

- გადატვირთულობის კონტროლი - გამტარუნარიანობის შემცირების გარეშე დიდი რაოდენობით მონაცემთა გადაცემის უნარი. თავდამსხმელს შეუძლია ქსელის გადატვირთვა სცადოს უცნობი პაკეტებით, რათა გამორთოს შეჭრის აღმოჩენის სისტემა. ამ შემთხვევაში IDS იძულებული იქნება გარკვეული პაკეტები გადასცეს, რომელთა შორის შეიძლება იყოს თავდამსხმელების მიერ ქსელში შეღწევის მიზნით შექმნილი პაკეტები;

- რეალურ დროში შეტყობინება. ასეთი შეტყობინება ხორციელდება დროული ინფორმაციისა და რეაგირების მოქმედებების მომზადებისთვის;

- გამოყოფის მექანიზმი. მონაცემთა ფილტრაციის, მოვლენის იდენტიფიკაციისა და რეაგირების პოლიტიკის გამოყოფა მნიშვნელოვნად ამარტივებს სისტემის მუშაობას;

- **მასშტაბურობა.** ახალი დაუცველობის იდენტიფიცირებისა და ცნობილი ტიპის თავდასხმებისგან თავის დასაცავად, ის იძლევა შესაძლებლობას, რომ შიდა სკრიპტების ბიბლიოთეკაში სწრაფად დავამატოთ თავდასხმის სკრიპტები;

- **თავდასხმებისთვის წინააღმდეგობის გაწევის უნარი.** კომპლექსური თავდასხმის სცენარები მოიცავს ქსელური შეტევის აღმოჩენის სისტემაზე გავლენის მომხდენ ელემენტებს. სისტემის იერარქიული არქიტექტურა სამი დონის ფუნქციით განისაზღვრება. ქვედა დონეზე, ქსელიდან მონაცემთა პაკეტის ამოსაღებად **Bro** იყენებს libpcap პროგრამას. მეორე დონეზე (მოვლენის გენერაცია) ხორციელდება პაკეტის მთლიანობის შემოწმება სათაურზე. შეცდომების აღმოჩენის შემთხვევაში, გენერირდება შესაძლო პრობლემის შესახებ შეტყობინება. შემდეგ იწყება გადამოწმების პროცედურა და დგინდება, პაკეტის სრული შიგთავსი რეგისტრირებულია თუ არა. ასევე პერსონალური სკრიპტირების ენა ხელმისაწვდომია. სისტემას წინასწარ დაწერილი უსაფრთხოების პოლიტიკის ნაკრები გააჩნია. **Bro**-ს პაკეტში ასევე შედის თავდასხმის ხელწერების ძებნის მექანიზმი.

Bro სისტემის ადმინისტრატორის მიერ მოწოდებული პოლიტიკის სკრიპტის მეშვეობით იფილტრება მოვლენების მენეჯერის მიერ გენერირებული მოვლენები. **Bro** სისტემა snort2bro უტილიტას მოიცავს, რომელიც საშუალებას გვაძლევს ვთარგმნოთ Snort ხელწერები **Bro** სკრიპტებში, რაც ასევე საშუალებას გვაძლევს განვახორციელოთ ხელწერის ოპტიმიზაცია. **Bro** სისტემა მაღალი სიჩქარით შეჭრის გამოვლენას ახორციელებს მაღალი გამტარუნარიანობის ქსელის ბმულებზე.

შეტევის აღმოჩენის სისტემა STAT

შეტევის აღმოჩენის სისტემა **STAT** ექსპერიმენტული საუნივერსიტეტო პროდუქტი და ერთ-ერთი "უძველესი" სისტემაა. STAT სისტემა შემდეგი კომპონენტებისგან შედგება: STAT Framework - STAT ბირთვი მოვლენის დამუშავებისთვის; MetaSTAT ინფრასტრუქტურა - მონიტორინგის და ადმინისტრირების ინსტრუმენტები STAT სენსორული ქსელისთვის; NetSTAT - ქსელის სენსორი UNIX სისტემებისთვის; USTAT - კვანძოვანი სენსორი OS Sun Solaris-ისთვის; LinSTAT კვანძოვანი სენსორი Linux სისტემებისთვის; WinSTAT - კვანძოვანი სენსორი Windows სისტემებისთვის; logSTAT - კვანძის სენსორი UNIX syslog ჟურნალების ანალიზისთვის; alertSTAT - მაღალი დონის მოვლენის კორელაციის სენსორი; web STAT არის კვანძოვანი სენსორი Apache ვებ- სერვერისთვის.

პროექტის STAT კვლევა რეალურ დროში თავდასხმის გამოვლენაზეა ფოკუსირებული. გაანალიზებულია სისტემების მდგომარეობა და მათში გარდამავალი პროცესები. მთავარი იდეა იმაში მდგომარეობს, რომ მოქმედებების გარკვეული თანმიმდევრობა, რომელიც ცალსახად მიუთითებს თავდამსხმელის არსებობაზე, სისტემას გადაიყვანს საწყისი (ავტორიზებული) მდგომარეობიდან არაავტორიზებულ მდგომარეობაში.

ცენტრალიზებული ქსელური თავდასხმის აღმოჩენის სისტემების უმეტესობა თავდასხმის ფაქტს განსაზღვრავს „აუდიტის ბილიკის“ საფუძველზე. STAT-ში მოდული "Audit Analyzer Trace" ფილტრავს და აჯამებს ამ ინფორმაციას. შედეგებს, რომლებიც

გადაკეთებულია ანალიზისთვის მოსახერხებელ ფორმაში, ეწოდება ხელმოწერები და STAT მიდგომის ყველაზე მნიშვნელოვან ელემენტს წარმოადგენს.

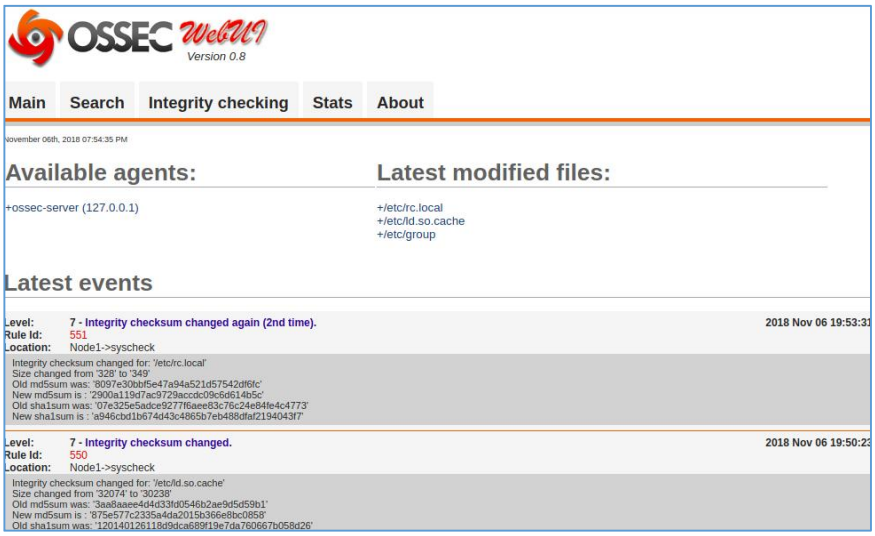
სისტემის მდგომარეობის შესახებ ახალი ინფორმაციის დამუშავების შემდეგ, დასკვნის ბლოკი განსაზღვრავს მდგომარეობის ნებისმიერ მნიშვნელოვან ცვლილებას და ფაქტების ბაზას განაახლებს. დასკვნის ბლოკი აცნობებს სპეციალისტს უსაფრთხოების შესაძლო დარღვევების შესახებ. თავის მხრივ სპეციალისტი, აცნობებს ადმინისტრატორს არანორმალური სიტუაციის შესახებ ან თავად იწყებს აუცილებელ მოქმედებებს.

შეტევის აღმომჩენი სისტემა Prelude

შეტევის აღმომჩენი სისტემა Prelude არის სრულფასოვანი ჰიბრიდული IDS (Intrusion Detection System). Prelude სისტემა შექმნილია GNU/Linux კომპიუტერებზე გასაშვებად. Prelude სისტემა გვაძლევს საშუალებას თვალყური ვადევნოთ როგორც ქსელში, ასევე ადგილობრივ კომპიუტერებზე მომხდარ მოვლენებს, რაც შეჭრის მცდელობის გამოვლენის ალბათობას ზრდის. გამოვლენის მეთოდად გამოიყენება ხელწერისა და პროტოკოლების სტატისტიკური ანალიზი. სისტემა აკავშირებს მესამე მხარის სენსორებს, ხოლო ინფორმაცია მათგან უნდა იყოს IDMEF (Intrusion Detection Message Exchange Format) ფორმატში. Prelude სისტემა ქსელის დონეზე მუშაობისთვის იყენებს IDS Snort-ს, როგორც ქსელის სენსორს.

შეტევების აღმომჩენი სისტემა OSSEC

სისტემა OSSEC წარმოადგენს კვანძოვან IDS-ს. OSSEC-ის მთავარი მიზანი UNIX OS ჟურნალების, ტიპიური აპლიკაციების, ფეიერვოლების ანალიზია. OSSEC მოიცავს ანალიზატორების კომპლექტს მონაცემთა სხვადასხვა წყაროსთვის, ცნობილი ტროას სანიშნეების ხელწერებს, ფაილური სისტემის მთლიანობის კონტროლსა (rootkits) და სხვა. ფუნქციონირება ლოკალური ჟურნალების ანალიზის შესაძლებლობას მოიცავს, როგორც OS დონეზე, ასევე ცალკეულ აპლიკაციებში, მაგალითად: SSH, MS Exchange, Sendmail ,Apache, ARP Watch, IIS, FTPD, Squid. OSSEC სისტემა ახორციელებს მოვლენების შესახებ ინფორმაციის დამუშავებას, რომლებიც მოდის სხვა სისტემებიდან, ფაიერვოლებიდან, კვანძებიდან დაყენებული OSSEC აგენტებით, ქსელის IDS-ებიდან. შეტყობინებები საეჭვო ქმედებების შესახებ XML ფორმატში არსებული წესების საფუძველზე გაიცემა. OSSEC სისტემას გააჩნია კრიტიკული ფაილების თვალყურის დევნების საშუალება: ნებართვები, მფლობელები და ფაილის ზომები. სერვერზე ყველა ამ მნიშვნელობის მონაცემთა ბაზა ინახება.



ნახ.2

OSSEC-ს შეუძლია ფაილურ სისტემაში შეცდომების აღმოჩენა ფაილების ხელწერის სკანირებით. სისტემის ბირთვის დონეზე უცნობი სანიშნეების გამოსავლენად IDS მოიცავს ანომალიების აღმოჩენის ინსტრუმენტებს. ასეთი სისტემის არქიტექტურის გაფართოება თავდასხმის ცოდნის ბაზის თვალსაზრისით სირთულეს წარმოადგენს.

აპარატურულ-პროგრამული საშუალება Cisco Secure IPS

Cisco Secure IPS ოჯახი, ცნობილი როგორც NetRanger, შედგება რამდენიმე კომპონენტისგან:

- Cisco Secure IDS 4000 სერიის მოწყობილობები;
- Cisco IOS OS გაფართოებები;
- Cisco Catalyst 6000 IDS Module დაფები;
- Cisco Secure Integrated Software (Cisco IOS Firewall Feature Set);
- Cisco Secure IDS დირექტორი.
- Cisco Secure Policy Manager;

პირველი სამი კომპონენტი ქსელის დონეზე განხორციელებული შეტევების გამოვლენაზე და მათზე რეაგირებაზეა პასუხისმგებელი, ხოლო ბოლო ორი ამ ინსტრუმენტების მართვაზეა პასუხისმგებელი. ამ გადაწყვეტილებებს აქტიური რეაგირების უნარი არ აქვთ. მთავარი რაც განასხვავებს მათ ერთმანეთისგან არის აღმოჩენილი ხელმოწერების რაოდენობა. მარშრუტიზაციის ან გადართვის ფუნქციების დამცავ მექანიზმებთან გაერთიანების მცდელობები ქსელური აღჭურვილობის მუშაობაზე უარყოფითად მოქმედებს.

შეტევების აღმომჩენი სისტემა RealSecure (IBM ISS)

ამ სისტემამ ქსელში შეჭრის აღმოჩენის სფეროში დიდი ნაბიჯი გადადგა და ლიდერია შეჭრის აღმოჩენის სისტემების დანერგვაში. დღეს Real Secure კომპანია ეკუთვნის IBM-ს. RealSecure სისტემა ეფუძნება რეალურ დროში ქსელის პაკეტის ანალიზისა და კვანძების

ჟურნალის ანალიზის ტექნოლოგიას. ეს გამოსავალი როგორც მთელი ქსელის სეგმენტის, ასევე მისი კონკრეტული კვანძის დაცვაზეა ორიენტირებული.

სისტემა აღმოაჩენს როგორც გარე, ასევე შიდა თავდასხმებს, რომლებიც მიზნად ისახავს აპლიკაციის სერვერებს, ვებ სერვერებს, მონაცემთა ბაზებს, სამუშაო სადგურებს, მარშრუტიზატორებსა და ფაირვოლებს. RealSecure სისტემას აქვს სამი დონის არქიტექტურა და შედგება ქსელის სეგმენტების და ცალკეული სერვერების ამოცნობისა და ადმინისტრატორის მოდულისგან.

სეგმენტების ამოცნობის მოდული სპეციალიზებულ სამუშაო სადგურებზე მუშაობს. ის შეჭრის გამოვლენასა და რეაგირებაზეა პასუხისმგებელი. თითოეული ასეთი მოდული ქსელის კონკრეტულ სეგმენტში თავდასხმის ხელწერებისთვის აკონტროლებს ტრაფიკს. ქსელის მოდულს უკანონო ქმედების აღმოჩენისას შეუძლია უპასუხოს მას კავშირის გათიშვით, ელექტრონული ფოსტის ან პეიჯერის შეტყობინების გაგზავნით ან მომხმარებლის მიერ განსაზღვრული სხვა ქმედებებით. ის ასევე განგაშის სიგნალს აგზავნის ადმინისტრატორის განყოფილებაში ან მართვის პანელზე.

სერვერების ამოცნობის მოდული ქსელური მოდულის დამატებაა. ის ჟურნალის ფაილებს აანალიზებს თავდასხმის აღმოსაჩენად, ადგენს წარმატებული იყო თუ არა შეტევა, ასევე გვთავაზობს სხვა ინფორმაციას, რომელიც არ არის ხელმისაწვდომი რეალურ დროში. თითოეული ასეთი მოდული სადგურზე ან სერვერზეა დაინსტალირებული და სრულად იკვლევს სისტემის ჟურნალის ფაილებს უსაფრთხოების დარღვევის კრიტერიუმებისთვის. ამ ტიპის მოდულები ხელს უშლიან შემდგომ შეჭრას მომხმარებლის პროცესების შეწყვეტითა და მომხმარებლის ანგარიშების შეჩერებით. მოდულს შეუძლია სიგნალიზაციის გაგზავნა, მოვლენების ჩაწერა და მომხმარებლის მიერ განსაზღვრული სხვა მოქმედებების შესრულება. ამოცნობის ყველა მოდული ადმინისტრაციული მოდულის მიერ ერთი კონსოლიდანაა გაერთიანებული და კონფიგურებული.

IDS-სა და IPS-ს შორის მთავარი განსხვავება ქსელთან მიმართებაში ინსტალაციაა: IDS უყურადებს ტრაფიკს SPAN პორტის, Hub ან TAP მოწყობილობის მეშვეობით და IPS თავისთავად გადის ტრაფიკს, რაც საშუალებას აძლევს IPS-ს გამოიყენოს ფილტრაციის წესები შეტევების დაბლოკვისა და თავდამსხმელის იზოლირებისთვის. IDS-ის უპირატესობა იმაში მდგომარეობს რომ ის არ ახდენს ქსელის შეფერხებებს. მაგრამ IDS-ის ნაკლოვანება არის ის, რომ თავდასხმების დაბლოკვის ერთადერთი შესაძლო მეთოდი არის TCP Reset პაკეტების გაგზავნა. გარდა ამისა, RealSecure Network Sensor-ს შეუძლია, რომ ხელახლა დააკონფიგურიროს Checkpoint Firewall-ის წესები OPSEC პროტოკოლის გამოყენებით.

შეტევების აღმომჩენი სისტემა Symantec Network Security

შეჭრის აღმოჩენის ინსტრუმენტი Symantec გვთავაზობს შეჭრის აღმოჩენის ორ პროდუქტს: Network Security 7100 Series და Critical System Protection პროგრამულ უზრუნველყოფას.

ეს ხელსაწყოები ახორციელებენ Symantec-ის საკუთრებაში არსებულ გამოვლენის ტექნოლოგიას - IMUNE™ (Intrusion Mitigation Unified Network Engine). IMUNE™ წარმოადგენს

რამდენიმე ძირითადი გამოვლენის ტექნოლოგიის კომბინაციას: ხელწერის ანალიზი, სერვისზე უარის თქმის (DOS) შეტევის გამოვლენა, ანომალიის გამოვლენა და სკანირების მცდელობები. თავდასხმის ჩაჭრის ტექნოლოგია Symantec უზრუნველყოფს მოწინავე მხარდაჭერის სერვისების მეშვეობით თავისი პროდუქციის ეფექტურობას, რომელიც უზრუნველყოფს დროულ ინფორმაციას თავდასხმების შესახებ. კომპონენტების მოხერხებულ განლაგებასა და ავტომატურად განახლების შესაძლებლობას LiveUpdate-ის გამოყენებით, რაც ხელმოწერის აღმოჩენის მეთოდებით წარმოადგენს თავდასხმის ეფექტური გამოვლენის მთავარი კრიტერიუმს.

სისტემა eTrust Intrusion Detection Computer Associates

კომპანიამ Computer Associates გამოუშვა eTrust Intrusion Detection (ყოფილი SessionWall) პროდუქტი, რომელიც LAN დაცვას და მონიტორინგს უზრუნველყოფს. ეს საკმაოდ მარტივი პროგრამული პროდუქტი თავდასხმის გამოვლენასა და ვებ ტრაფიკის კონტროლის მონიტორინგს უზრუნველყოფს.

მონაცემთა ბაზის გამოყენებით სისტემა ავტომატურად ამოიცნობს ჰაკერების მცდელობებს. eTrust Intrusion Detection-ის ვრცელი თავდასხმის ნიმუშის ბიბლიოთეკის განახლება რეგულარულად ხორციელდება. სისტემა ახორციელებს წვდომის კონტროლს - eTrust Intrusion Detection და იყენებს წესებს იმის დასადგენად, თუ რომელ მომხმარებელს, რომელ რესურსზე შეუძლია წვდომა.

სისტემას გააჩნია თავდასხმის შაბლონების ვრცელი ბიბლიოთეკა, რაც შესაძლებელს ხდის, რომ ავტომატურად გამოვლინდეს თავდასხმები, რომლებიც ემთხვევა რეგულარულად განახლებულ შაბლონებს. არსებობს ვირუსებისგან დაცვის მექანიზმი, რომელიც ინფიცირებული მონაცემების ჩამოტვირთვას ხელს უშლის.

სისტემა საშუალებას გვაძლევს საკვანძო სიტყვების შემცველი წესების გამოყენებით შევზღუდოთ წვდომა ინტერნეტ კვანძებზე. etrust ქსელის დატვირთვის კონტროლსაც ახორციელებს.

სისტემა ინახავს ქსელში ტრაფიკის რაოდენობრივ ჩანაწერს. eTrust Intrusion Detection პროდუქტი უზრუნველყოფს თავდასხმის გამოვლენასა და პასუხს შეტევებზე, ვირუსებისა და საშიში Java/ActiveX კომპონენტების გამოვლენას. ამავდროულად, კომპლექსი ახორციელებს ინფორმაციის შენახვას თავდასხმის შესახებ, რაც შესაძლებელს ხდის ორგანიზაციული ღონისძიებების გასატარებლად მის შემდგომ გამოყენებას.

სისტემა აგრეთვე უზრუნველყოფს მომხმარებლის მცდელობების იდენტიფიკაციას, გამოიცნოს სისტემაში შესვლის პაროლი და აკონტროლებს ასეთ მცდელობებს მათი ერთდროული რეგისტრაციით.

დასკვნა

შეგვიძლია დავასკვნათ, რომ განხილული სისტემებიდან არცერთს არ აქვს ყველა საჭირო პარამეტრის მონიტორინგის უნარი. ხოლო ეფექტური მუშაობისთვის შეჭრის აღმოჩენის სისტემას საჭიროა, რომ ჰქონდეს მაქსიმალური ინფორმაცია დაცული ქსელის

შესახებ, კერძოდ: შეეძლოს ქსელის ტრაფიკის, სისტემის სერვისების, პროცესების, სისტემის რეესტრის კონტროლი, სისტემისა და სხვა კრიტიკული ფაილების კონტროლი.

ეს გამომდინარეობს ინფორმაციისა და კომპიუტერულ ქსელებში მონაცემთა დამუშავების ამჟამად მიღებული მეთოდოლოგიიდან, რაც მრავალდონიანობას გულისხმობს. დამუშავების დროს ხორციელდება მონაცემების არაერთხელ გარდაქმნა ერთი ტიპიდან (ფორმატიდან) მეორეზე, რათა უზრუნველყოფილი იყოს მოხერხებულობა კონკრეტული პროცესისთვის (ქსელის გადაცემა, მომხმარებლის ნახვა, ავტომატური კონვერტაცია, და ა.შ.).

ამის მაგალითს წარმოადგენს ქსელის პროტოკოლის დასტა. ამავდროულად, მონაცემთა ერთ დონეზე დაკვირვებით, შეუძლებელია, რომ დავასკვნათ, თუ როგორ იქნება ისინი წარმოდგენილი და ინტერპრეტირებული სხვა დონეზე. კომპიუტერულ სისტემებზე თავდასხმებმა შეიძლება ნებისმიერ დონეზე მოახდინოს გავლენა.

გამოყენებული ლიტერატურა

1. ქართველიშვილი ი., ოხანაშვილი მ., ჩორხაული ნ. ქსელური შეტევების აღმოჩენის არსებული მეთოდების მიმოხილვა და ანალიზი. საერთაშორისო სამეცნიერო-პრაქტიკული კონფერენცია „თანამედროვე გამოწვევები და მიღწევები ინფორმაციულ და საკომუნიკაციო ტექნოლოგიებში - 2023“ საქართველო, თბილისი 12-13 ოქტომბერი, 2023 წელი. გვ.410-416.
2. Ledesma, Josue. “IDS vs. IPS: What Is the Difference?” Inside Out Security, October 23, 2018. https://www.varonis.com/blog/ids-vs-ips.
3. Andersen, I. (2023, November 22). *Top 10 Most Common Types of Cyber Attacks*. Https://Blog.netwrix.com/. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Birthday%20attack

Review and analysis of existing systems for detecting network attacks

Summary

Research in the field of detection of attacks on computer networks and systems has been conducted for a long time. Signs of attacks have been investigated, methods and means of detecting unauthorized access attempts have been developed and used through security systems, both on the Internet and at the local, logical and physical levels. Commercial intrusion detection systems by various foreign companies (Cisco, Snort, ISS RealSecure, etc.) are widely represented in the local market. Many local researchers use architectural analogues and typical solutions of already known systems.

In recent years, the number of different types and methods of organizing unauthorized intrusion into computer networks has increased dramatically. Therefore, intrusion detection systems have become an important component of organizations' security infrastructure. This is facilitated by the

appearance of a large number of literary sources, complex approaches and methods for detecting attacks in information systems.

The purpose of the review of the existing network attack detection systems presented in the paper is to investigate the functionality of currently available IDSs and to reveal the shortcomings of the used attack detection methods and the disadvantages of their usability. Realizations of existing attack detection systems can be divided into two parts: research and commercial products.

Each new research project is distinguished by the introduction of new methods of analysis and new approaches to the study of monitoring objects, although they quickly become obsolete. Commercial projects (such as ISS RealSecure, Symantec Network Security, Cisco IPS, etc.) remain relevant longer due to the support of manufacturers. The manufacturers provide ongoing customer support, new attack research, and signature updates. Therefore, it can be noted that most of the commercial research results are abuse detection systems, namely handwriting systems.

Intrusion detection systems IDS (Intrusion Detection System) represent software and hardware-software solutions, where the processes of collection, storage and analysis (monitoring) of events occurring in a computer system or network are automated, and these events are independently analyzed in search of signs of information security violations. These protection systems exist as programs that can display a message that a network attack has occurred at that moment. Systems that are used to detect network attacks solve only one specific task - protection from an external attacker who tries to bypass protection systems and gain access to a local local network, but the problem of protection from internal threats remains an unsolved task.

All known IDS are conditionally divided into three classes:

- Network IDS (Network-based IDS, NIDS);
- Nodal IDS (Host-based IDS, HIDS);
- Hybrid IDS (Hybrid IDS).

Node IDS can be further divided into two subclasses: system level IDS and application level IDS (application-based IDS).

Keywords: Intrusion detection system Snort. Intrusion Detection System Bro. Intrusion detection system STAT. Prelude intrusion detection system. Intrusion detection system OSSEC. Hardware and software tool Cisco Secure IPS. Intrusion detection system RealSecure (IBM ISS). Intrusion detection system Symantec Network Security. System eTrust Intrusion Detection Computer Associates.