ქსელური სენსორი

1

 1. კრიტიკული ინფორმაციული სისტემის სუბიექტთან შეთანხმებით, მონაცემთა გაცვლის სააგენტო და კომპიუტერული უსაფრთხოების სპეციალისტი კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელში ახორციელებენ კომპიუტერული ინციდენტების იდენტიფიცირებისა და კვლევისათვის აუცილებელი ქსელური სენსორის (სენსორების სისტემის) კონფიგურირებასა და მართვას.

2. **ქსელური სენსორი არის** ქსელის უსაფრთხოების მონიტორინგისთვის განკუთვნილი სპეციალური მოწყობილობა, რომლის საშუალებითაც ხდება ისეთი ქმედებების გამოვლენა, რომლებიც მიუთითებს ინფორმაციული სისტემის წინააღმდეგ წარმოებულ შეტევაზე ან მასში შეღწევაზე. სუბიექტი უფლებამოსილია, შეარჩიოს მასთან განთავსებული ქსელური სენსორის მომსახურების სახე, კერძოდ, ქსელის ზედაპირული მონიტორინგი ან ქსელის პაკეტების ღრმა ანალიზის მონიტორინგი.

3. **ქსელურ სენსორში იგულისხმება** ორგანიზაციის კომპიუტერულ სერვერზე გამართული პროგრამული უზრუნველყოფა, რომელიც ახდენს ქსელის/ქსელის სეგმენტის მდგომარეობის და კავშირების შესახებ ინფორმაციის ჩაწერას და უსაფრთხო კავშირის გამოყენებით ამ ინფორმაციის გადაგზავნას ცენტრალურ შემგროვებელ სერვერზე, რომელიც განთავსდება მონაცემთა გაცვლის სააგენტოში. სუბიექტი უფლებამოსილია, შეარჩიოს მასთან განთავსებული ქსელური სენსორის მომსახურების სახე, კერძოდ, ქსელის ზედაპირული მონიტორინგი ან ქსელის პაკეტების ღრმა ანალიზის მონიტორინგი.

4. **ქსელური სენსორის ძირითადი დანიშნულებაა** ორგანიზაციის სამიზნე ქსელზე განხორციელებული კიბერ-შეტევების, კომპიუტერული ინციდენტების მუდმივი მონიტორინგი და მათი დროული აღმოჩენა.

5. ინფორმაცია, რომელსაც შეიცავს ქსელური სენსორის მიერ გენერირებული მონაცემები, მნიშვნელოვან დახმარებას უწევს როგორც მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს, ასევე ორგანიზაციის კიბერ უსაფრთხოების სპეციალისტს და სხვა ტექნიკურ პერსონალს ინციდენტის სწრაფად, დროულად და ეფექტიანად გამოვლენაში.

2

ორგანიზაციის ინტერნეტ-ქსელის დასაცავად, ინფორმაციული უსაფრთხოების თანამედროვე პრინციპების გათვალისწინებით, შესაძლოა გამოყენებული იქნეს კომპლექსური გადაწყვეტილება, რომელიც შედგება 2 ძირითადი კომპონენტისაგან:

ა) Netflow Monitoring - ქსელური ტრაფიკის პასიური მონიტორინგის საშუალება;

ბ) Network Device Firewall – საბაზისო მოდული, რომლის გამართვასაც უზრუნველყოფს ქსელის ადმინისტრატორი.

3. ქსელის ზედაპირული მონიტორინგი

1. ქსელის ზედაპირული მონიტორინგის დროს ქსელური სენსორის საშუალებით შემგროვებელ სერვერზე იგზავნება შემდეგი მონაცემები:

ა) შემავალი და გამავალი კავშირების მიმართულება: კონკრეტული IP მისამართები;

ბ) კავშირების დამყარების და დასრულების თარიღი;

გ) კავშირის დროს გამოყენებული ქსელური პროტოკოლები;

დ) ტრაფიკის მოცულობა;

ე) სტატისტიკური მონაცემები ნებისმიერი ჩამოთვლილი პარამეტრის მიხედვით.

2. შემგროვებელი სერვერი, რომელიც განთავსებულია გაცვლითი სააგენტოში ზემოთ აღნიშნულ ,,ა - ე“ ქვეპუნქტებში ჩამოთვლილ მონაცემებზე დაყრდნობით ახდენს მონაცემთა ანალიზის სპეციალური მოდულების გამოყენებით და ახორციელებს დაინფიცირებული კომპიუტერების და კიბერ-შეტევების იდენტიფიცირებას.

3. ორგანიზაციიდან გამოგზავნილი მეხუთე ვერსიის Netflow მონაცემები შეიცავს შემდეგი სახის ინფორმაციას (საერთო 5 მახასიათებელი):

ა) საწყისი მისამართი - Source IP address;

ბ) საბოლოო მისამართი - Destination IP address;

გ) IP პროტოკოლი - IP protocol;

დ) პროტოკოლის საწყისი პორტები;

ე) პროტოკოლის საბოლოო პორტები.

 UDP და TCP პროტოკოლების საწყისი პორტები, 0 სხვა პროტოკოლებისათვის - Source port for UDP or TCP, 0 for other protocols;

ვ) UDP და TCP პროტოკოლების საბოლოო პორტები, ICMP ტიპი და კოდი, ან 0 სხვა პროტოკოლებისათვის - Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols;

ზ) IP ინტერნეტ პროტოკოლის სერვისის ტიპი - IP Type of Service.

ორგანიზაციიდან Netflow-ს მონაცემების გამოგზავნა მონაცემთა გაცვლის შემგროვებელ სერვერზე ხორციელდება დაცული არხის საშუალებით.

Netflow მონიტორინგი წარმოადგენს ორგანიზაციის ქსელური ტრაფიკის პასიური მონიტორინგის საშუალებას, კერძოდ, არ ხორციელდება ქსელის ტრაფიკის შესახებ სრული ინფორმაციის შეგროვება და დამუშავება, როგორიცაა ინფორმაციის ორგანიზაციის მომხმარებლების კონკრეტული საქმიანობის, მოქმედების, ფაილების და გადაგზავნილი დოკუმენტების შესახებ.

4  ქსელის მონიტორინგის პაკეტების ღრმა ანალიზი

1. შემგროვებელი სერვერის კონფიგურირება ხდება მონაცემთა გაცვლის სააგენტოს ან სუბიექტის ფიზიკურ მოწყობილობაზე (სერვერზე) დაყენებული ოპერაციული სისტემისა და პროგრამული პროდუქტების მეშვეობით, რომელთა მიზანია ორგანიზაციის ლოკალურ ქსელში არსებული ქსელური მოწყობილობიდან ქსელური ტრაფიკის მიღება და გაანალიზება.

2. შემგროვებელი სერვერი განთავსებულია სუბიექტის ინფრასტრუქტურაში.

3. შემგროვებელი სერვერის კონფიგურირებისათვის მონაცემთა გაცვლის სააგენტო ახორციელებს:

ა) სენსორისთვის განკუთვნილ მოწყობილობაზე ოპერაციული სისტემის „Alienvault OSSIM“-ის ბოლო ვერსიის ინსტალაციას;

ბ) სისტემაში პროგრამული პროდუქტის „Snort IDS“ ბოლო ვერსიის ინსტალაციას;

გ) სისტემაში Snort წესების ავტომატური ინტეგრაციის მიზნით პროგრამის „Barnyard“ის ან სხვა მწარმოებლის მიერ შექმნილი წესების ინტეგრაციას სუბიექტთან შეთანხმებით.

4. ქსელის მონიტორინგის დროს ქსელური მოწყობილობებიდან შემგროვებელ სერვერზე იგზავნება შემდეგი მონაცემები:

ა) შემავალი და გამავალი კავშირების მიმართულება, კონკრეტული IP მისამართები;

ბ) კავშირების დამყარების და დასრულების თარიღი;

გ) კავშირის დროს გამოყენებული ქსელური პროტოკოლები;

დ) ტრაფიკის მოცულობა;

ე) ქსელური პაკეტების შიგთავსი;

ვ) სტატისტიკური მონაცემები ნებისმიერი ჩამოთვლილი პარამეტრის მიხედვით.

5. Snort ახორციელებს ქსელის მონიტორინგის დროს ქსელური მოწყობილობებიდან შემგროვებელ სერვერზე გადაგზავნილი მონაცემების გაფილტვრას ზემოთ აღნიშნულ „ა“ – „ვ“ ქვეპუნქტებში ჩამოთვლილ მონაცემებზე დაყრდნობით, წინასწარ დადგენილი წესების მიხედვით, და ინახავს მიღებულ შედეგს.

 **ინფორმაციაზე წვდომა და კონფიდენციალობის დაცვა**

1. სუბიექტს, შემგროვებელ სერვერთან ერთად, გადაეცემა სერვერზე დაყენებული ოპერაციული სისტემის და აპლიკაციის ადმინისტრატორისა და მომხმარებლის პაროლები. სერვერის ადმინისტრირებას ახორციელებს სუბიექტის კიბერუსაფრთხოებაზე პასუხისმგებელი პირი ან პირები.

2. მონაცემთა გაცვლის სააგენტოს არ გააჩნია წვდომა ქსელის მონიტორინგის პაკეტების ღრმა

ანალიზის საშუალებებზე. მონაცემთა გაცვლის სააგენტოს, სუბიექტთან შეთანხმებით, აქვს უფლება:

ა) მონიტორინგის მოწყობილობით შეუზღუდავად მიიღოს ამ წესების მე–4 მუხლის მე–5 პუნქტის შესაბამისად დამუშავებული ინფორმაცია;

ბ) შეუფერხებლად მიიღოს სისტემის კონფიგურაციის შესახებ სრული ინფორმაცია;

გ) მოითხოვოს სისტემის კონფიგურაციის ცვლილება ან/და განახლება.

3. სუბიექტი ვალდებულია, დაუყოვნებლივ აცნობოს მის მიერ დაგეგმილი ან გადაუდებელი

პირობებით გამოწვეული ნებისმიერი ცვლილება ქსელის მონიტორინგის პაკეტების ღრმა ანალიზის ინფრასტრუქტურაში.

4. სუბიექტი უფლებამოსილია, მოითხოვოს მონაცემთა გაცვლის სააგენტოსა და სუბიექტს შორის ინფორმაციის გაუხმაურებლობის შესახებ ხელშეკრულების გაფორმება.

 1. Netflow ქსელური სენსორის კონფიგურირება ხდება ორგანიზაციის ფიზიკურ მოწყობილობაზე (სერვერზე) დაყენებული ოპერაციული სისტემითა და პროგრამული პროდუქტებით, რომელთა მიზანია ლოკალური ინტერნეტ-ქსელში არსებული როუტერიდან Netflow ტრაფიკის გადაგზავნა მონაცემთა გაცვლის სააგენტოს ცენტრალურ შემგროვებელი სერვერზე.

2. Netflow ქსელური სენსორის კონფიგურირებისათვის ორგანიზაცია ახორციელებს:

ა) სენსორისთვის განკუთვნილ მოწყობილობაზე Linux-ის ოპერაციული სისტემის ინსტალაციას;

ბ) აღნიშნული ოპერაციული სისტემის დროის სინქრონიზაციას ორგანიზაციის ლოკალურ NTP (Network Time Protocol - ქსელური დროის პროტოკოლი) სერვერთან;

გ) სისტემაში პროგრამული პროდუქტების „Nfdump” და „Nfsen“ არსებული ბოლო ვერსიების ინსტალაციას. ამ პროდუქტების ფუნქციონირებისათვის საჭირო დამატებითი მოდულების (Dependency) ინსტალირებას, კონკრეტული ოპერაციული სისტემის მოთხოვნების შესაბამისად;

დ) ქსელური სენსორის ფუნქციონირებისათვის საჭირო ქსელური პარამეტრების მიმოხილვას, გაზიარებას და ცვლილების შეტყობინებას მონაცემთა გაცვლის სააგენტოს CERT ჯგუფთან:

დ.ა) ორგანიზაციის როუტერის/როუტერების IP მისამართები;

დ.ბ) CERT ჯგუფის ცენტრალური შემგროვებელი სერვერის IP მისამართი.

ე) „Nfdump“, „Nfsen“ პროგრამული პროდუქტების ავტომატური გაშვების ფუნქციის უზრუნველყოფა, რათა მოხდეს სენსორის მუშაობის გაგრძელება სისტემის გადატვირთვის, შემთხვევითი გათიშვის ან რაიმე გაუმართაობის შემდეგ.

5

ორგანიზაციის სერვერი ან ვირტუალური მანქანა უნდა აკმაყოფილებდეს შემდეგ ტექნიკური

მახასიათებლებს:

ა) პროცესორი (CPU): 4;

ბ) მყარი დისკი (Hard Disk): 40 GB;

გ) ოპერატიული მეხსიერება: 2048MB.

6

აღწერილი Netflow მონიტორინგი ორგანიზაციის ქსელური ტრაფიკის პასიური მონიტორინგის საშუალებას წარმოადგენს. Netflow მონაცემები არ შეიცავს სრულ ინფორმაციას ქსელის ტრაფიკის შესახებ, მაგალითად, დამუშავებულ და გადაგზავნილ მონაცემებში არ ხვდება ისეთი ინფორმაცია, როგორიცაა ორგანიზაციის მომხმარებლების კონკრეტული საქმიანობის, მოქმედების, ფაილების და გადაგზავნილი დოკუმენტების შესახებ. ამ ტიპის სენსორის მიერ არ ხდება ტრაფიკის „სრული“ მონიტორინგი.

ქსელური სენსორის კონფიგურაციის წესები

1

1. კრიტიკული ინფორმაციული სისტემის სუბიექტთან შეთანხმებით, მონაცემთა გაცვლის სააგენტო და კომპიუტერული უსაფრთხოების სპეციალისტი კრიტიკული ინფორმაციული სისტემის სუბიექტის ქსელში ახორციელებენ კომპიუტერული ინციდენტების იდენტიფიცირებისა და კვლევისათვის აუცილებელი ქსელური სენსორის (სენსორების სისტემის) კონფიგურირებასა და მართვას.

2. ქსელური სენსორი არის ქსელის უსაფრთხოების მონიტორინგისთვის განკუთვნილი სპეციალური მოწყობილობა, რომლის საშუალებითაც ხდება ისეთი ქმედებების გამოვლენა, რომლებიც მიუთითებს ინფორმაციული სისტემის წინააღმდეგ წარმოებულ შეტევაზე ან მასში შეღწევაზე.

3. ქსელურ სენსორში იგულისხმება ორგანიზაციის კომპიუტერულ სერვერზე გამართული პროგრამული უზრუნველყოფა, რომელიც ახდენს ქსელის/ქსელის სეგმენტის მდგომარეობის და კავშირების შესახებ ინფორმაციის ჩაწერას და უსაფრთხო კავშირის გამოყენებით ამ ინფორმაციის გადაგზავნას ცენტრალურ შემგროვებელ სერვერზე, რომელიც განთავსდება მონაცემთა გაცვლის სააგენტოში.

4. ქსელური სენსორის ძირითადი დანიშნულებაა ორგანიზაციის სამიზნე ქსელზე განხორციელებული კიბერ-შეტევების, კომპიუტერული ინციდენტების მუდმივი მონიტორინგი და მათი დროული აღმოჩენა.

5. ინფორმაცია, რომელსაც შეიცავს ქსელური სენსორის მიერ გენერირებული მონაცემები, მნიშვნელოვან დახმარებას უწევს როგორც მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე დახმარების ჯგუფს, ასევე ორგანიზაციის კიბერ უსაფრთხოების სპეციალისტს და სხვა ტექნიკურ პერსონალს ინციდენტის სწრაფად, დროულად და ეფექტიანად გამოვლენაში.

2

ორგანიზაციის ინტერნეტ-ქსელის დასაცავად, ინფორმაციული უსაფრთხოების თანამედროვე პრინციპების გათვალისწინებით, შესაძლოა გამოყენებული იქნეს კომპლექსური გადაწყვეტილება, რომელიც შედგება 2 ძირითადი კომპონენტისაგან:

ა) Netflow Monitoring - ქსელური ტრაფიკის პასიური მონიტორინგის საშუალება;

ბ) Network Device Firewall – საბაზისო მოდული, რომლის გამართვასაც უზრუნველყოფს ქსელის ადმინისტრატორი.

3

1. ქსელის მონიტორინგის დროს ქსელური სენსორის საშუალებით შემგროვებელ სერვერზე იგზავნება შემდეგი მონაცემები:

ა) შემავალი და გამავალი კავშირების მიმართულება: კონკრეტული IP მისამართები;

ბ) კავშირების დამყარების და დასრულების თარიღი;

გ) კავშირის დროს გამოყენებული ქსელური პროტოკოლები;

დ) ტრაფიკის მოცულობა;

ე) სტატისტიკური მონაცემები ნებისმიერი ჩამოთვლილი პარამეტრის მიხედვით.

2. ქსელური სენსორის სპეციალური მოდულების საშუალებით ხდება დაინფიცირებული კომპიუტერების და კიბერ-შეტევების იდენტიფიცირება ამ მუხლის პირველი პუნქტის ,,ა - ე“ ქვეპუნქტებში ჩამოთვლილ მონაცემებზე დაყრდნობით.

სუბიექტი უფლებამოსილია, შეარჩიოს მასთან განთავსებული ქსელური სენსორის მომსახურების სახე, კერძოდ, ქსელის ზედაპირული მონიტორინგი ან ქსელის პაკეტების ღრმა ანალიზის მონიტორინგი.

3. სტანდარტული მეხუთე ვერსიის Netflow მონაცემები შეიცავს შემდეგი სახის ინფორმაციას (საერთო 7 მახასიათებელი):

ა) შემავალი ინტერფეისი - Ingress interface (SNMP ifIndex);

ბ) საწყისი მისამართი - Source IP address;

გ) საბოლოო მისამართი - Destination IP address;

დ) IP პროტოკოლი - IP protocol;

ე) UDP და TCP პროტოკოლების საწყისი პორტები, 0 სხვა პროტოკოლებისათვის - Source port for UDP or TCP, 0 for other protocols;

ვ) UDP და TCP პროტოკოლების საბოლოო პორტები, ICMP ტიპი და კოდი, ან 0 სხვა პროტოკოლებისათვის - Destination port for UDP or TCP, type and code for ICMP, or 0 for other protocols;

ზ) IP ინტერნეტ პროტოკოლის სერვისის ტიპი - IP Type of Service.

4

1. Netflow ქსელური სენსორის კონფიგურირება ხდება ორგანიზაციის ფიზიკურ მოწყობილობაზე (სერვერზე) დაყენებული ოპერაციული სისტემითა და პროგრამული პროდუქტებით, რომელთა მიზანია ლოკალური ინტერნეტ-ქსელში არსებული როუტერიდან Netflow ტრაფიკის გადაგზავნა მონაცემთა გაცვლის სააგენტოს ცენტრალურ შემგროვებელი სერვერზე.

2. Netflow ქსელური სენსორის კონფიგურირებისათვის ორგანიზაცია ახორციელებს:

ა) სენსორისთვის განკუთვნილ მოწყობილობაზე Linux-ის ოპერაციული სისტემის ინსტალაციას;

ბ) აღნიშნული ოპერაციული სისტემის დროის სინქრონიზაციას ორგანიზაციის ლოკალურ NTP (Network Time Protocol - ქსელური დროის პროტოკოლი) სერვერთან;

გ) სისტემაში პროგრამული პროდუქტების „Nfdump” და „Nfsen“ არსებული ბოლო ვერსიების ინსტალაციას. ამ პროდუქტების ფუნქციონირებისათვის საჭირო დამატებითი მოდულების (Dependency) ინსტალირებას, კონკრეტული ოპერაციული სისტემის მოთხოვნების შესაბამისად;

დ) ქსელური სენსორის ფუნქციონირებისათვის საჭირო ქსელური პარამეტრების მიმოხილვას, გაზიარებას და ცვლილების შეტყობინებას მონაცემთა გაცვლის სააგენტოს CERT ჯგუფთან:

დ.ა) ორგანიზაციის როუტერის/როუტერების IP მისამართები;

დ.ბ) CERT ჯგუფის ცენტრალური შემგროვებელი სერვერის IP მისამართი.

ე) „Nfdump“, „Nfsen“ პროგრამული პროდუქტების ავტომატური გაშვების ფუნქციის უზრუნველყოფა, რათა მოხდეს სენსორის მუშაობის გაგრძელება სისტემის გადატვირთვის, შემთხვევითი გათიშვის ან რაიმე გაუმართაობის შემდეგ.

5

ორგანიზაციის სერვერი ან ვირტუალური მანქანა უნდა აკმაყოფილებდეს შემდეგ ტექნიკური

მახასიათებლებს:

ა) პროცესორი (CPU): 4;

ბ) მყარი დისკი (Hard Disk): 40 GB;

გ) ოპერატიული მეხსიერება: 2048MB.

6

მოცემულ ბრძანებაში აღწერილი Netflow მონიტორინგი ორგანიზაციის ქსელური ტრაფიკის პასიური მონიტორინგის საშუალებას წარმოადგენს. Netflow მონაცემები არ შეიცავს სრულ ინფორმაციას ქსელის ტრაფიკის შესახებ, მაგალითად, დამუშავებულ და გადაგზავნილ მონაცემებში არ ხვდება ისეთი ინფორმაცია, როგორიცაა ორგანიზაციის მომხმარებლების კონკრეტული საქმიანობის, მოქმედების, ფაილების და გადაგზავნილი დოკუმენტების შესახებ. ამ ტიპის სენსორის მიერ არ ხდება ტრაფიკის „სრული“ მონიტორინგი.