DOI: https://doi.org/10.36719/2663-4619/115/319-322

Sevil Haqverdiyeva
Azərbaycan Dövlət Aqrar Universiteti
https://orcid.org//0009-0000-1238-8338
sevil.haqverdiyeva@gmail.com
Anar Quliyev
Azərbaycan Dövlət Aqrar Universiteti
https://orcid.org//0009-0002-5549-4063
anar_quliyev74@mail.ru
Ülviyyə Səfərova
Azərbaycan Dövlət Aqrar Universiteti
https://orcid.org/0009-0004-1102-2114
ulviyaeldar@mail.ru
Sima Məmmədova
Azərbaycan Dövlət Aqrar Universiteti
https://orcid.org/0009-0006-5163-3598
simamemmedova9642@gmailcom

Korporativ şəbəkələrdə İDS (intrusion detection system) təhlükəsizlik sistemi

Xülasə

Təhlükəsizlik ilə əlaqədar təhdidlərin sayının və növlərinin sürətlə artması ilə birlikdə təhlükəsizlik texnikası da sürətlə inkişaf edir. Şəbəkənin təhlükəsizliyini təmin etmək və girişə icazəsi olmayanların sistemə daxil olub məlumatları ələ keçirməsinin və yaxud da dəyişdirməsinin qabağını almaq üçün ilk olaraq identifikasiya və giriş nəzarəti təhlükəsizlik mexanizmləri inkişaf etdirilmişdir. Amma çox yaxşı giriş nəzarəti və identifikasiyası olan sistemin də bəzi zəifliklər vardır. İdentifikasiya və giriş nəzarəti təhlükəsizliyin ilk müdafiə qatını təşkil edir. Təhlükələrin artması ilə əlaqədar olaraq sadaladığımız mexanizmdən əlavə yeni mexanizmlərə də ehtiyac duyulur. Təhlükəsizlik divarı, VS (Vulnerability Scanner), İDS kimi mexanizmlər şəbəkə üçün ikinci müdafiə qatını təmin edirlər. Qeyd etdiyimiz bütün təhlükəsizlik mexanizmlərinin hər biri ayrılıqda təhlükəsizlik üçün kifayət deyildir. Korporasiyanın təhlükəsizlik arxitekturasına görə təhlükəsiz bir sistem üçün bu vasitələr bir-birini dəstəkləyəcək şəkildə istifadə olunmalıdır.

İDS qanuni və qanunsuz proseslərin monitorinqini həyata keçirən sistemdir. Bu sistem istər daxili, istərsə də xarici sessiyalara aid bütün informasiyaları toplayır və analiz edir. Hər hansı bir qanunauyğun olmayan hal aşkar olarsa, müxtəlif vasitələrlə xəbərdarlıq edir. Bu, şəbəkə inzibatçıları üçün əlavə bir alət kimi korporativ şəbəkə arxitekturasında öz yerini tutmuşdur. O, bütün daxili və xarici şəbəkələrin aktivliyini yoxlayır və analiz edir. Bütün şübhəli halları – sistemə müdaxilə və bu kimi digər halları üzə çıxarmaq iqtidarındadır.

Açar sözlər: *Korporativ şəbəkə, təhlükəsizlik, identifikasiya, təhdidlər, müdafiə sistemi*

Sevil Hagverdiyeva
Azerbaijan State Agrarian University
https://orcid.org//0009-0000-1238-8338
sevil.haqverdiyeva@gmail.com
Anar Guliyev
Azerbaijan State Agrarian University
https://orcid.org//0009-0002-5549-4063
anar_guliyev74@mail.ru

Ulviyya Safarova
Azerbaijan State Agrarian University
https://orcid.org/0009-0004-1102-2114
ulviyaeldar@mail.ru
Sima Mammadova
Azerbaijan State Agrarian University
https://orcid.org/0009-0006-5163-3598
simamemmedova9642@gmailcom

IDS (Intrusion Detection System) Security System in Corporate Networks

Abstract

Security technology is developing rapidly with the rapid increase in the number and types of security-related threats. In order to ensure network security and prevent unauthorized persons from entering the system and capturing or changing data, identification and access control security mechanisms were first developed. However, even a system with very good access control and identification has some weaknesses. Identification and access control constitute the first layer of security defense. Due to the increase in threats, new mechanisms are needed in addition to the mechanisms we have listed. Mechanisms such as firewall, VS (Vulnerability Scanner), IDS provide a second layer of defense for the network. Each of the security mechanisms we have mentioned is not sufficient for security separately. According to the security architecture of the corporation, for a secure system, these tools should be used in a way that supports each other.

IDS is a system that monitors legal and illegal processes. This system collects and analyzes all information related to both internal and external sessions. If any illegal situation is detected, it warns you through various means. It has taken its place in the corporate network architecture as an additional tool for network administrators. It checks and analyzes the activity of all internal and external networks. It is able to reveal all suspicious cases - system intrusion and other similar cases.

Keywords: *Corporate network, security, identification, threats, defense system*

Giriş

Müdaxilələrin Təyin olunması Sistemi – (İntrusion Detection System – İDS) İnternet və ya digər xarici şəbəkələrdən gələ biləcək şəbəkədəki sistemlərə zərər verə biləcək fərqli paketdən ibarət olan hücumları müəyyən etmək üçün hazırlanan sistemdir.

İDS-ləri bir çox kateqoriyaya ayırmaq mümkündür. Misal üçün İSS-nin (İnternet Security System) daxil etdiyi modelə görə İSD-lər aktiv (active İSD) və pasiv (passive İSD) ola bilər. İkinci təsnifat isə

- Şəbəkə–əsaslı İDS (Network-based İntrusion Detection System –NİDS)
- Host–əsaslı İDS (Host-based İntrusion Detection System –HİDS)
- Perimetr İDS (Perimeter Intrusion Detection System –PİDS)
- Virtual maşın–əsaslı İDS (Virtual Machine based Intrusion Detection System –VMİDS)

Bu sistemin aktiv olması üçün o hücuma hücum anında (real-time) və ya ona yaxın zamanda cavab verir. Pasiv İDS isə əsasən hücumları yadda saxlayır və daha sonra araşdırır.

Şəbəkə-əsaslı İDS (Network-based İntrusion Detection System)- NİDS

Tədqiqat

Şəbəkə trafikinin monitor edilməsi və müdaxilələrin təyin olunması üçün müstəqil bir platformadır. NİDS – şəbəkədə ya hub ya da switch-ə qoşularaq şəbəkədə olan axına nəzarət edir. Bu halda hub-da heç bir dəyişiklik olunmur yalnız switch-də güzgülü portlar (Port mirroring) yaratmaqla bütün paketlərin nüsxəsi NİDS-ə yönəldilir (Oppliger, 2005). Bu növ İDS-lər öz seqmentin üzərindən keçən tafikin monitor edir və müdaxilələrin təyin edir. Bu şəbəkənin digər seqmentlərindən və ya

digər əlaqə növlərinə aid trafikə nəzarət etmirlər. Yəni NİDS əsas olaraq şəbəkədə dolaşan paketlərin bir sensor üzərindən keçənlərə nəzarət edir. Sensora gələn paket mövcud olan imzalar ilə qarşılaşdırılır və paketə nə edilməsi haqqında qərar verir. Başlanğıc səviyyədə olan filtrləmdə hansı paketin qəbul edilməsi və ya rədd edilməsinə qərar verilir (Anderson, 2008).

Əgər hücum müəyyən olunursa cavab modulu hücuma qarşılıq olaraq xəbərdarlıq edir. Sensorlar ilə monitorun arasındakı trafikin şifrələnməsi və ya sensor və monitorlar eyni bir şəbəkəyə daxil edilməsi təhlükəsizlik baxımından önəmlidir. Hücumçunun şəbəkəyə hücum etməsi üçün sensor və monitor arasındakı trafik (xəbərdarlıq, vəziyyət qeydləri və s.) çox əhəmiyyətli məlumat hesab edilir. Adətən bu DMZ–də ya şəbəkə sərhəddində yerləşdirilir və sensorlar daxil olan bütün trafiki analiz edir. Nümünə üçün SNORT-u göstərmək olar. Ümumiyyətlə isə onu belə ümumiləşdirə bilərik (Cole, 2011):

- Performansın zəifləməsinə səbəb olan hücumların qarşısının ala bilər
- Denial of Service (DoS) hücumlarına qarşı qoruma təmin edə bilər
- SSL ilə şifrələnmiş trafikin içərisində hücumları müəyən edə bilər
- İstənilməyən protokolların qaşısını ala bilər (Mis. İCQ və s.)

Host-əsaslı İDS (Host-based İntrusion Detection System)–HİDS.

Bu kompüterdə agenti olan bir sistemdi və o sistem çağırışlarını, loq-ları, file – fayl sistemində dəyişiliklərin və digər vəziyyətlərə nəzarət edir. HİDS-lər öz funksiyalarının ya hostlar ya da individual kompüterlərdə həyata keçirirlər. HİDS hər log-u göstərmək üçün proqramlardan istifadə edir. HİDS-lər log-ları paket göndərilən zamanda (real-time) müəyyən edir və yenə həmin vaxtda cavab verir. Bəzi HİDS-lər port nömrələrindən istifadə edib müəyyən port girişlərini dayandıra bilirlər (Gupta, 2015).

HİDS sensorları adətən tərtibat formasında olur. Nümünə üçün OSSEC göstərmək olar.

Perimetr– İDS (Perimeter Intrusion Detection System)–PİDS

Perimetrə müdaxiləri və yerini təyin edir. Müxtəlif elektronik və fiber optik kabellə perimetr təchiz olunur və PİDS perimetrdə müdaxiləni aşkar edir və siqnalvermə işə düşür (Panko, 2010).

Virtual Machine based Intrusion Detection System-VMİDS

O virtual maşın səviyyəsində müdaxiləni təyin edir. Bu çox yeni bir növ İDS hesab olunur və hazırda inkişaf etdirilir. Onun istifadəsində ayrıca İDS-ə ehtiyac duyulmur və bütün proseslər həm fiziki, həm virtual olaraq monitor olunur (Prakash, 2009).

Hücumun müəyyən edilməsi iki analiz metoduna görə təsnif olunur:

Misuse Detection – daxili şəbəkədə yaranan hücumları müəyyən edir. Bu üsulda İDS-dən əldə etdiyi məlumatları analiz edər və böyük ölçülü imza (signature) verilənlər bazası ilə qarşılaşdırır (Syngress Building, 2003). Avantajı istifadəçilərin imza verilənlər bazasınına nəzarət edə bilməsi və sistemi idarəedənlər tərəfindən hücumların hansı növünə görə xəbərdarlıq olacağını asanlıqla müəyyən olunması. Əsas dezavantajı isə imzalar saxlanılan verilənlər bazasının tez-tez yenilənməsidir (John, Dominic, 2006).

Anomaly Detection – Bu üsulda istifadəçi qrupu ya da hər bir istifadəçi üçün ayrı-ayrı olaraq profil müəyyən olunur. Profillər dinamik olaraq və ya ələ hazırlana bilər və normal istifdəçi fəaliyyətini tanıya bilmək üçün "baseline" (əsas xətt) olaraq istifadə olunur. Əgər şəbəkədə edilən bir iş "baseline"-dan çıxarsa xəbərdarlıq edər. Bu İDS-lər profillərlə işlədiyindən eyni zamanda "profil əsaslı İDS" olaraq da adlandırılır. *Anomaliya təyinedici* – Bütün İDS-lər aşağıdakı təyinetmə xüsusiyyətlərdən istifadə olunur (Kizza, 2005):

Statistical anomaly -Statistik anomaliya – Bu şəbəkə trafikini ümumi performansını analiz etməklə anomaliyanı təyin edir. Əgər performans ümumi göstəricidən artıq dərəcədə qeydə alınırsa bu zaman siqnal verilir (Newman, 2009).

Signature-based- İmza əsaslı bazası – Şəbəkə hücumları və digər anomaliyalar bu baza əsasında təyin olunur və təcili siqnal verilir. Ona görədə bu bazanı mütəmadi olaraq yeniləmək lazım gəlir. Əsas avantajı daxildən gələn hücumlar və istifadəçi hesabının oğurlanmasının müəyyən edilməsində çox faydalı olması və ilk dəfə meydana gələn hücumun daha asan müəyyən olmasıdır. Həm də profillərin xüsusilədirilmiş olması hücumçünun hansı işi görəndə xəbərdarlıq gedəcəyini

bilməməsidir. Əsas dezavantaji isə profillərin idarə olunmasının və hazırlanmasının çətin olması və çox vaxt tələb etməsidir (Malik, 2003).

Defense against IDS attacks-İDS hücumlarına qarşı müdafiə

Şəbəkə təhlükəsizliyi inzibatçısı müxtəlif ehtiyat və təşəbbüslər həyata keçirməlidir ki, daxili və xarici hücumlardan qoruna bilsin (Stallings, 2013).

Bunlar:

- ✓ Daimi olaraq viruslara qarşı sistemləri yeniləmək
- ✓ Çağırılmamış qonağın ip adresinin qara siyahıda olması
- ✓ Xəbərdarlıq üçün səs və siqnallardan istifadə etmək
- ✓ TCP FİN və RST paketlərinin məcburi xitam verilməsi

Nəticə

İDS-təhlükəsizlik divarı ilə müqayisəsi etsək bu nəticələrə gələ bilərik. Hər ikisi şəbəkə təhlükəsizliyi üçün istifadə olunur. Təhlükəsizlik divarınından fərqi qabaqcadan baş verəcəklərin qarşısını almaq, şəbəkələr arasında sədd yaratmaq və onların arasında əlaqəni qayadalara əsasən qurmaq və ya qadağan etməkdir. İDS şübhəli bir hal təyin edərkən onu həmən analiz edir və siqnal verir (log serverde, sms ilə, fiziki siqnal, email ilə və s.). İDS həmçinin sistemdaxili hücumlara da nəzarət edir bu hücumlar açarların (signature) köhnə olması və ya sistemdə boşluqlar olması nəticəsində əmələ gəlir. Lakin avtomatik olaraq sistem və ya inzibatçı tərəfdən təyin olunmuş qaydalar əsasında bu hücumları dəf edən sistem İPS adlanır.

Intrusion Prevention System-Hücumların dəf edilməsi sistemi

Ənənəvi İDS texnologiyaları hadisəni təyin etməyə xidmət edir. Lakin İPS həm təyin edir həmdə müdafiə edir yəni İDS funksiyalarını həyata keçirə bilir. İPS məqsədi qərəzli olan halları aşkar etmək və onların qarşısını almaqdan ibarətdir.

Ədəbiyyat

1. Anderson, R. (2008). *Security engineering* (2nd ed.). Wiley.
2. Cole, E. (2011). *Network security bible* (2nd ed.). Wiley.
3. Gupta, P. C. (2015). *Cryptography and network security*. PHI Learning.
4. John, T., & Dominic, W. (2006). *Complexity and cryptography*. Cambridge University Press.
5. Kizza, J. M. (2005). *Computer network security*. Springer.
6. Malik, S. (2003). *Network security: Principles and practices*. Prentice Hall.
7. Newman, R. C. (2009). *Computer security: Principles and practices*. Jones & Bartlett Learning.
8. Oppliger, R. (2005). *Contemporary cryptography*. Artech House.
9. Panko, R. R. (2010). *Corporate computer and network security* (2nd ed.). Pearson.
10. Prakash, A. (2009). *Information system security*. Tech Press.
11. Stallings, W. (2013). *Cryptography and network security: Principles and practice* (6th ed.). Pearson.
12. Syngress Building. (2003). *DMZs for enterprise networks*. Syngress.

Daxil oldu: 29.01.2025
Qəbul edildi: 08.03.2025