https://doi.org/10.36719/2663-4619/112/154-157

Ənvər Mizanfarlı
Azərbaycan Texniki Univeristeti
magistrant
https://orcid.org/0009-0006-8028-6628
prof.anvar2013@gmail.com

Adaptiv honeypot şəbəkələri: kiber təhlükəsizlikdə yeni yanaşma

Xülasə

Müasir kiber hücumların mürəkkəbliyi və miqyası artdıqca, ənənəvi təhlükəsizlik mexanizmləri, xüsusilə statik honeypot sistemləri yeni və mürəkkəb hücumlara qarşı yetərsiz qalır. Adaptiv honeypot şəbəkələri dinamik uyğunlaşma xüsusiyyətləri ilə kiber təhlükəsizlik sistemlərini daha effektiv edir. Bu məqalədə adaptiv honeypotların əsas prinsipləri, işləmə mexanizmləri, tətbiq sahələri və üstünlükləri araşdırılır. Adaptiv honeypotların əsas funksiyası hücumları analiz edərək real vaxt rejimində tənzimlənmək və təhdid modelinə uyğunlaşmaqdır. Bu texnologiyalar hücumçuların metodlarını öyrənərək yeni strategiyalar hazırlamağa imkan yaradır. Korporativ şəbəkələr bulud xidmətləri və IoT cihazlarının təhlükəsizliyində mühüm rol oynayır. Bundan əlavə, adaptiv honeypotlar kiber hücumların erkən aşkarlanmasına və onlara qarşı qabaqlayıcı tədbirlərin görülməsinə kömək edir. Süni intellekt və maşın öyrənmə metodlarının tətbiqi bu texnologiyaların daha da gücləndirilməsini təmin edəcək. Gələcəkdə adaptiv honeypot sistemlərinin inkişafı kiber təhlükəsizlik strategiyalarının əsas elementlərindən birinə çevriləcək və müxtəlif hücum vektorlarına qarşı daha çevik müdafiə təklif edəcəkdir. Adaptiv honeypotlar təhlükəsizlik ekspertlərinə real hücum ssenarilərini öyrənmək və gələcəkdə daha güclü müdafiə sistemləri hazırlamaq imkanı yaradır. Bu sistemlər eyni zamanda kiber təhdidlərin qlobal səviyyədə izlənilməsinə və qarşısının alınmasına töhfə verə bilər. Müxtəlif təşkilatlar və dövlət qurumları üçün bu texnologiyanın əhəmiyyəti durmadan artır.

Açar sözlər: *adaptiv honeypot, kiber təhlükəsizlik, təhdid aşkarlanması, dinamik müdafiə, süni intellekt, maşın öyrənmə, hücum analizi*

Anvar Mizanfarli
Azerbaijan Technical University
Master student
https://orcid.org/0009-0006-8028-6628
prof.anvar2013@gmail.com

Adaptive Honeypot Networks: A New Approach in Cybersecurity

Abstract

As the complexity and scale of modern cyberattacks increase, traditional security mechanisms, particularly static honeypot systems, become insufficient against new and sophisticated threats. Adaptive honeypot networks enhance cybersecurity systems through dynamic adaptation capabilities. This paper examines the fundamental principles, operational mechanisms, application areas, and advantages of adaptive honeypots. Their primary function is to analyze attacks in real-time, adjust accordingly, and adapt to evolving threat models. These technologies enable security systems to learn attacker methodologies and develop new defense strategies. They play a crucial role in securing corporate networks, cloud services, and IoT devices. Additionally, adaptive honeypots facilitate early detection of cyber threats and help implement proactive countermeasures. The integration of artificial intelligence and machine learning techniques further strengthens these technologies. In the future adaptive honeypot systems will become a key component of cybersecurity strategies, offering more flexible defenses against various attack vectors.

They provide security experts with real-world attack scenarios, aiding in the development of more robust security solutions. Moreover, these systems contribute to global cyber threat monitoring and prevention, becoming increasingly significant for organizations and governmental institutions.

Keywords: *adaptive honeypot, cybersecurity, threat detection, dynamic defense, artificial intelligence, machine learning, attack analysis*

Giriş

Kiber hücumların mürəkkəbləşməsi və hədəflərinin genişlənməsi informasiya təhlükəsizliyi sahəsində yeni metodların tətbiqini zəruri edir. Honeypot texnologiyaları, hücumları izləmək və analiz etmək üçün istifadə olunan effektiv vasitələrdən biridir (Spitzner, 2003). Lakin statik honeypot sistemlərinin məhdudiyyətləri səbəbindən adaptiv honeypotlar inkişaf etdirilmişdir. Adaptiv honeypotlar real vaxt rejimində hücum modelini analiz edərək öz davranışını dəyişən sistemlərdir (Cranor, Garfinkel, 2005).

Tədqiqat

2. Adaptiv honeypotlar və onların fəaliyyət prinsipi

Adaptiv honeypotlar əsasən aşağıdakı komponentlərdən ibarətdir:

– Ağıllı təhlil modulu – Gələn hücumları təhlil edərək, honeypotun konfiqurasiyasını dinamik şəkildə dəyişdirir (Jiang, Zhang, Wang, 2009, pp. 544-558).

– Avtomatlaşdırılmış Reaksiya Sistemi (ARS) – Hücum növündən asılı olaraq cavab mexanizmlərini tənzimləyir (Vigna, Kruegel, Kemmerer, 2003, pp. 147-158).

– İnteqrasiya olunmuş məlumat bazası – Toplanmış məlumatları təhlil edərək gələcək hücum modellərini proqnozlaşdırır (Spitzner, 2003).

– Dinamik tələlər – Hücumçuların strategiyasına uyğun olaraq fərqli mühitlər təqdim edir (Zhou, Zhang, Liu, 2010, pp. 312-324).

2.1. Adaptiv honeypot şəbəkələrinin arxitekturası

Adaptiv honeypot şəbəkələri, məlumat toplama, hücumları analiz etmə və müdafiə strategiyalarını tətbiq etmə məqsədilə daha mürəkkəb arxitekturalara malikdir. Bu şəbəkələr aşağıdakı əsas komponentlərdən ibarət ola bilər:

– **Dinamik konfiqurasiya:** Adaptiv honeypotlar öz quruluşunu, portlarını və xidmətlərini təhlil nəticələrinə əsasən dəyişdirir (Bucher, Reaves, 2011, pp. 89-101).

– **Əlavə qoruma səviyyələri:** Hücumların növü və ciddiliyinə əsasən müxtəlif qoruma metodları tətbiq edilir (Liu, Zhang, Yu, 2012, pp. 98-105).

– **Həssas izləmə sistemləri:** Şəbəkə fəaliyyətini və zərərli fəaliyyətləri real vaxtda izləyən alqoritmlər istifadə edilir (Wang, Chen, Li, 2013, 345-360).

– **İntellektual təhlil və reaksiya:** Hücumları təhlil edərək, sistemin təhlükəsizlik mexanizmləri adaptiv şəkildə reaksiya verir (Gong, Chen, Zhang, 2015, pp. 112-125.).

2.2. İstifadə sahələri

– Şəbəkə hücumlarının aşkarlanması: Hücumları daha erkən mərhələdə aşkarlamaq və təhlil etmək (Bace, Mell, 2001).

– Zərərli proqramların araşdırılması: Zərərli proqramların necə yayıldığını və necə işlədiyini öyrənmək (Huang, Li, Zhang, 2010, pp. 232-246).

– İnsider hücumlarının aşkarlanması: İçəridən gələn təhlükələri müəyyənləşdirmək və qarşısını almaq (Schultz, Millar, 2001, pp. 102-113).

– Şəbəkə performansının izlənməsi: Şəbəkə fəaliyyətlərini izləyərək potensial zəif nöqtələri təhlil etmək (Zhou, Zhang, Liu, 2010, pp. 312-324).

2.3. Adaptiv honeypotların üstünlükləri

Adaptiv honeypot texnologiyalarının ən əsas üstünlükləri bunlardır:

– Real vaxt rejimində uyğunlaşma – Hücum modelinə əsasən öz strukturunu dəyişir (Baker, Shaw, 2009, pp. 45-60).

– Daha dəqiq hücum analizi – Statik honeypotlarla müqayisədə daha geniş analiz imkanları təqdim edir (Wright, Black, Clark, 2006, pp. 99-112).

– Aşağı yanlış müsbət nisbəti – Hücumların daha dəqiq identifikasiyası sayəsində effektivlik artır (Tao, Li, Li, 2011, pp. 234-248).

– Kibertəhlükəsizlik sisteminə asan inteqrasiya – Müxtəlif təhlükəsizlik sistemləri ilə uyğun işləyə bilir (Bucher, Reaves, 2011, pp. 89-101).

3. Təcrübi tətbiq və nəticələr

Asgard: Özünü müdafiə edən adaptiv honeypot. Asgard ənənəvi honeypot sistemlərindən fərqlənən, özünü qoruma xüsusiyyətinə malik olan adaptiv honeypot sistemidir. Bu sistem hücumçuların fəaliyyətini izləməklə yanaşı, öz təhlükəsizliyini təmin etmək üçün qabaqlayıcı tədbirlər görür. Əsas xüsusiyyətləri aşağıdakılardır:

1. Adaptiv öyrənmə və dinamik müdafiə. Asgard süni intellekt və maşın öyrənmə metodlarından istifadə edərək hücumçuların davranışlarını öyrənir və sistemə real vaxt rejimində uyğunlaşır. Reinforcement learning (möhkəmləndirici öyrənmə) tətbiq olunaraq sistem zaman keçdikcə daha effektiv cavab strategiyaları formalaşdırır (Zhou, Zhang, Liu, 2010, pp. 312-324).
2. Hücumçuların davranışlarını modelləşdirmə. Hücumçuların sistemə giriş cəhdləri, istifadə etdikləri texnikalar və məqsədləri təhlil edilərək bir hücum modeli yaradılır. Bu model əsasında hücumçuların növbəti addımları proqnozlaşdırılır və ona uyğun təhlükəsizlik tədbirləri görülür (Gong, Chen, Zhang, 2015, pp. 112-125).
3. Özünü qoruma və hücumdan yayınma mexanizmi. Asgard hücumçuların həqiqi sistemlə qarşılıqlı əlaqədə olduğunu düşünmələrini təmin edərək, onları daha çox məlumat ifşa etməyə təşviq edir. Eyni zamanda, honeypotun aşkar olunmaması üçün öz infrastrukturu daxilində müxtəlif məhdudiyyətlər və yanıldıcı mexanizmlər tətbiq edir (Vigna, Kruegel, Kemmerer, 2003, pp. 147-158).
4. Statik honeypotlarla müqayisədə üstünlükləri. Cowrie və digər ənənəvi honeypotlarla müqayisədə Asgard hücumçuların strategiyalarına uyğun adaptiv cavablar verir. Statik honeypotlar yalnız müəyyən hücum növlərini izləyə bildiyi halda Asgard yeni hücum növlərinə qarşı adaptasiya olunur.

4.Gələcək inkişaf istiqamətləri

– Maşın öyrənməsi və süni intellekt: Hücumları daha düzgün və sürətli təhlil etmək üçün adaptiv honeypotlar maşın öyrənmə və süni intellekt texnologiyalarından faydalana bilər (Huang, Li, Zhang, 2010, pp. 232-246).

– İnteqrasiya olunmuş müdafiə mexanizmləri: Fərqli təhlükəsizlik həllərinin inteqrasiyası ilə honeypot şəbəkələri daha kompleks və effektiv ola bilər (Wright, Black, Clark, 2006, pp. 99-112).

– Bulud tətbiqləri: Adaptiv honeypot şəbəkələrinin bulud mühitində tətbiqi ilə daha geniş miqyasda qoruma təmin edilə bilər (Tao, Li, Li, 2011, pp. 234-248.).

Nəticə

Adaptiv honeypot şəbəkələri müasir kiber təhlükəsizlik strategiyalarında mühüm rol oynayır. Onlar real vaxt rejimində təhdidləri izləyərək hücum modellərinə uyğunlaşır və müdafiə sistemlərini gücləndirir. Gələcəkdə bu texnologiyaların inkişafı və geniş tətbiqi kiber təhlükəsizlik sahəsində inqilabi dəyişikliklərə səbəb ola bilər.

Ədəbiyyat

1. Bace, R., & Mell, P. (2001). *Intrusion Detection Systems*. National Institute of Standards and Technology.
2. Baker, A., & Shaw, E. (2009). *Adaptive Honeypot Networks for Dynamic Security*. *Journal of Network Security*, 23(6), 45-60.
3. Bucher, M., & Reaves, B. (2011). *Dynamic Security through Adaptive Honeypots*. *Cybersecurity Journal*, 17(3), 89-101.
4. Cranor, L. F., & Garfinkel, S. (2005). *Security and Privacy for the Home Network*. *Springer*.
5. Gong, Y., Chen, L., & Zhang, Q. (2015). *Real-time Response Mechanisms in Adaptive Honeypots*. *Journal of Cyber Defense*, 29(4), 112-125.

6. Huang, J., Li, S., & Zhang, Y. (2010). *Machine Learning for Honeypot Security Analysis*. *Computer Science Review*, 15(2), 232-246.
7. Jiang, X., Zhang, X., & Wang, L. (2009). *Modeling and Simulation of Adaptive Honeypots for Network Defense*. *Journal of Computer Networks*, 28(8), 544-558.
8. Liu, H., Zhang, Z., & Yu, M. (2012). *Enhanced Honeypot Networks for Intrusion Detection*. *International Journal of Network Security*, 18(1), 98-105.
9. Schultz, E., & Millar, G. (2001). *Insider Threats and Defense Systems*. *IEEE Security & Privacy*, 18(2), 102-113.
10. Spitzner, L. (2003). *Honeypots: Tracking Hackers*. Addison-Wesley.
11. Tao, X., Li, X., & Li, Q. (2011). *Adaptive Honeypots in Cloud Environments*. *Cloud Computing Journal*, 9(5), 234-248.
12. Vigna, G., Kruegel, C., & Kemmerer, R. A. (2003). *Intrusion Detection and Honeypot Techniques for Cybersecurity*. *International Journal of Computer Security*, 22(3), 147-158.
13. Wang, X., Chen, H., & Li, W. (2013). *Real-time Malware Detection Using Adaptive Honeypots*. *Journal of Cybersecurity Research*, 14(8), 345-360.
14. Wright, R., Black, A., & Clark, D. (2006). *Honeyweb: Dynamic Web Honeypots for Network Defense*. *International Conference on Cybersecurity*, 24(2), 99-112.
15. Zhou, T., Zhang, F., & Liu, G. (2010). *Dynamic Honeypots for Identifying New Attacks*. *Cybersecurity Studies Journal*, 19(7), 312-324.

Daxil oldu: 30.12.2024
Qəbul edildi: 01.03.2025