TEXNİKA ELMLƏRİ
TECHNICAL SCIENCES

DOI: https://doi.org/10.36719/2663-4619/118/144-147

Ülvi Səmədzadə
Azərbaycan Dövlət İqtisad Universiteti
magistrant
https://orcid.org/0009-0006-1139-4377
samadzadaulvi@gmail.com

Şəbəkə təhülkəsizlik testlərinin təkmilləşdirilməsi istiqamətləri

Xülasə

Şəbəkə təhlükəsizliyi testlərinin təkmilləşdirilməsi informasiya texnologiyalarının sürətlə inkişaf etdiyi müasir dövrdə xüsusi əhəmiyyət kəsb edir. Bu sahədə aparılan testlərin əsas məqsədi potensial zəiflikləri müəyyən etmək, təhlükəsizlik boşluqlarını vaxtında aşkara çıxarmaq və hücum risklərini minimuma endirməkdir. Təkmilləşdirilmiş test yanaşmaları daha çevik, avtomatlaşdırılmış və real hücum ssenarilərinə yaxın metodların tətbiqini tələb edir. Buraya penetrasiya testlərinin daha sistemli qurulması, təhlükəsizlik auditlərinin dövri olaraq həyata keçirilməsi, süni intellekt və maşın öyrənməsi kimi texnologiyalardan istifadə ilə anomaliyaların daha sürətli aşkarlanması daxildir. Həmçinin, kibertəhlükələrə qarşı proaktiv müdafiə strategiyalarının inkişaf etdirilməsi və test nəticələrinin risk əsaslı təhlili də önəm daşıyır. Təhlükəsizlik testlərinin effektivliyi həm texniki bacarıqlardan, həm də təşkilati idarəetmə yanaşmalarından asılıdır. Bu baxımdan, şəbəkə təhlükəsizliyi testlərinin təkmilləşdirilməsi təşkilatların dayanıqlı və etibarlı rəqəmsal mühit qurmasında mühüm rol oynayır.

Açar sözlər: *Şəbəkə, penetrasiya, analizlər ,süni intellekt, informasiya ,təhlükəsizlik*

Ulvi Samadzadeh
Azerbaijan State Economic University
Master student
https://orcid.org/0009-0006-1139-4377
samadzadaulvi@gmail.com

Directions for Improving Network Security Tests

Abstract

Improving network security testing is particular importance in the modern era of rapid development of information technologies. The main goal of testing in this area is to identify potential vulnerabilities, timely detect security gaps, and minimize attack risks. Improved testing approaches require the application of methods that are more flexible, automated, and close to real attack scenarios. This includes more systematic implementation of penetration tests, periodic security audits, and faster detection of anomalies using technologies such as artificial intelligence and machine learning. Also important are the development of proactive defense strategies against cyber threats and risk-based analysis of test results. The effectiveness of security testing depends on both technical skills and organizational management approaches. In this regard, improving network security testing plays an important role in organizations building a sustainable and reliable digital environment.

Keywords: *Network, penetration, analysis, artificial intelligence, information, security*

Giriş

Müasir dövrdə rəqəmsal texnologiyaların sürətli inkişafı və qlobal informasiya sistemlərinin genişlənməsi şəbəkə təhlükəsizliyi məsələsini strateji prioritetə çevirib. İnformasiya sistemlərinə qarşı yönəlmiş kibertəhdidlər o cümlədən zərərli proqram təminatları, DDoS hücumları, məlumat sızmaları və sosial mühəndislik texnikaları getdikcə daha mürəkkəb və adaptiv forma alır. Bu kontekstdə təşkilatların və dövlət qurumlarının informasiya resurslarını qorumaq üçün şəbəkə təhlükəsizliyini yalnız müdafiə tədbirləri ilə deyil, həm də sınaq və analiz mexanizmləri ilə gücləndirməsi vacibdir (Stallings, 2019; OWASP Foundation, n.d.).

Şəbəkə təhlükəsizliyi testləri, sistemin zəif nöqtələrinin aşkarlanması, risklərin qiymətləndirilməsi və qarşısının alınması məqsədilə həyata keçirilən mühüm proseslərdən biridir. Lakin bu testlərin effektivliyi onların müasir hücum texnikalarına uyğunlaşdırılması və daim təkmilləşdirilməsi ilə mümkündür. Bu tədqiqatın məqsədi, şəbəkə təhlükəsizliyi testlərinin hazırkı vəziyyətini təhlil etmək, mövcud boşluqları müəyyənləşdirmək və onların təkmilləşdirilməsi üçün elmi və texnoloji əsaslandırılmış istiqamətlər irəli sürməkdir. tədqiqatın aktuallığı son illərdə kiberhücumların sayının və mürəkkəbliyinin əhəmiyyətli dərəcədə artması ilə daha da güclənir (ResilientX, n.d.). Ənənəvi təhlükəsizlik yanaşmaları artıq yeni nəsil hücumlara qarşı kifayət qədər dayanıqlı deyil və bu səbəbdən daha çevik, analitik və proaktiv test mexanizmlərinə ehtiyac yaranır. Təşkilatlar yalnız real hücumlar baş verdikdən sonra tədbir görmək əvəzinə, öncədən mümkün sızma nöqtələrini müəyyən edib qarşısını almağa yönəlmiş yanaşmalar tətbiq etməlidirlər (Zhang, Xing, Li, 2025).

Təhlükəsizlik testlərinin institusional səviyyədə həyata keçirilməsi, yəni informasiya təhlükəsizliyi üzrə milli strategiyaların, beynəlxalq əməkdaşlıq mexanizmlərinin və audit sistemlərinin gücləndirilməsi də vacibdir. Geniş miqyaslı rəqəmsal infrastruktura malik olan mühitlərdə testlərin səmərəli aparılması üçün təşkilatların strukturlaşdırılmış təhlükəsizlik siyasətinə, müvafiq ixtisaslaşmış kadr potensialına və innovativ texnoloji həllərə malik olması əsas şərtdir (ISO/IEC. (2022).

Tədqiqat

Şəbəkə təhlükəsizliyi testləri informasiya sistemlərinin zəif nöqtələrini müəyyən etmək, hücum vektorlarını modelləşdirmək və potensial təhlükələri vaxtında aşkara çıxarmaq üçün mühüm vasitədir. Bu testlər müxtəlif formalarla – o cümlədən penetrasiya testləri (penetration testing), zəriflik skanları (vulnerability scanning), etik hacking və red-blue team yanaşmaları ilə həyata keçirilir. Lakin müasir kibertəhlükələrin dinamikası bu yanaşmaların ənənəvi tətbiq formasını məhdudlaşdırır və onların təkmilləşdirilməsini zəruri edir (National Institute of Standards and Technology, 2008).

Ənənəvi test metodologiyaları adətən statik və vaxtla məhdudlaşmış ssenarilərə əsaslanır. Bu yanaşma yalnız cari zəifllikləri müəyyən etməyə xidmət edir və gələcəkdə baş verə biləcək adaptiv hücumlara qarşı hazırlıq imkanı yaratmır. Bundan əlavə, çoxsaylı təşkilatlarda təhlükəsizlik testləri yalnız audit və yoxlama məqsədilə ildə bir neçə dəfə aparılır ki, bu da kibertəhlükələrin sürətli dəyişdiyi mühitdə effektli qorunma təmin etmir. Testlərin davamlı və real zamanlı təhlilə əsaslanmaması, həmçinin kompleks şəbəkə strukturlarında avtomatlaşdırmanın zəif tətbiqi ciddi boşluqlara səbəb olur (Ross, Pillitteri, Dempsey, Riddle, Guissanie, 2020; BlueVoyant, n.d.).

Kibertəhlükələrin mürəkkəbləşməsi fonunda yeni texnoloji yanaşmaların tətbiqi zərurətə çevrilib. Məsələn, süni intellekt və maşın öyrənməsi texnologiyaları şəbəkədə anomaliyaların və sızma cəhdlərinin real vaxt rejimində təhlilinə imkan verir. AI əsaslı hücum deteksiya sistemləri (IDS/IPS) təkcə məlum təhlükə nümunələrini deyil, həm də yeni və naməlum hücumları proqnozlaşdıra bilir. Bu texnologiyaların test proseslərinə inteqrasiyası həm səmərəliliyi artırır, həm də reaksiya müddətini azaldır (National Highway Traffic Safety Administration, 2016; GetAstra, 2024).

Şəbəkə testlərinin təkmilləşdirilməsində digər bir vacib məsələ də təhlükəsizlik üzrə insan resurslarının rolu və onların hazırlıq səviyyəsidir. Təəssüf ki, bir çox təşkilatda kibertəhlükəsizlik sahəsində çalışan mütəxəssislər test ssenarilərini formalaşdırmaq və nəticələri şərh etmək üçün kifayət qədər hazırlıqlı olmur. Bu problemi həll etmək üçün təhlükəsizlik mühəndislərinə və

administratorlara mütəmadi təlimlər keçirilməli, real ssenarilər üzrə simulyasiyalar təşkil olunmalı, red team və blue team qarşılaşmaları ilə bacarıqlar praktiki səviyyədə inkişaf etdirilməlidir (Scanlon, 2018; Qualysec, 2025).

Nəticə

Şəbəkə təhlükəsizliyi testlərinin təkmilləşdirilməsi informasiya cəmiyyətində fəaliyyət göstərən hər bir təşkilat üçün strateji zərurətə çevrilmişdir. Müasir dövrün rəqəmsal infrastrukturları sürətlə genişlənməkdədir və bu inkişafla yanaşı, onların qarşılaşdığı kibertəhlükələrin miqyası və mürəkkəbliyi də artır. Bu baxımdan, ənənəvi və passiv test yanaşmaları artıq informasiya sistemlərinin müdafiəsini təmin etməkdə yetərsiz qalır. Təhlükəsizlik testlərinin sistemli şəkildə yenilənməsi, texnoloji tərəqqiyə uyğunlaşdırılması və real təhdid modellərinə əsaslanması təşkilatların kiberrezistentliyinin artırılmasında əsas rol oynayır.

Araşdırmalar göstərir ki, şəbəkə təhlükəsizliyində effektiv test mexanizmlərinin tətbiqi yalnız zəifliklərin aşkarlanması deyil, həm də risklərin idarə olunması baxımından mühüm əhəmiyyət daşıyır. Müasir təhlükə ssenariləri artıq sadəcə firewall və antivirus kimi passiv qoruyucu mexanizmləri aşa biləcək səviyyədədir. Bu səbəbdən penetrasiya testləri, zəriflik analizləri və simulyasiya edilmiş hücum ssenariləri vasitəsilə sistemin real dözümlülüyünü sınamaq zərurəti yaranır. Belə testlər yalnız texniki boşluqları deyil, həm də insan resursları, şəbəkə konfiqurasiyası və informasiya axını kimi amilləri də əhatə etməlidir. Şəbəkə təhlükəsizliyi testlərinin təkmilləşdirilməsi həmçinin texnologiyaların düzgün inteqrasiyası ilə sıx bağlıdır. Süni intellekt və maşın öyrənməsi kimi innovativ yanaşmaların tətbiqi test proseslərinin daha çevik və proaktiv aparılmasına şərait yaradır. Bu texnologiyalar şəbəkədə anomal davranışları vaxtında müəyyən etməyə, hücumların erkən mərhələdə qarşısını almağa və sistemin özünü adaptasiya etməsinə imkan verir. Bu isə ənənəvi testlərin əsas çatışmazlığı olan reaktivliyi aradan qaldırmaqla təhlükəsizlik səviyyəsini yeni mərhələyə yüksəldir. Test proseslərinin effektivliyi təşkilati strukturdan da asılıdır. Təşkilat daxilində təhlükəsizlik mədəniyyəti formalaşmalı, müvafiq siyasətlər və prosedurlar yaradılmalı, təlim və maarifləndirmə tədbirləri mütəmadi olaraq həyata keçirilməlidir. Təhlükəsizlik üzrə heyətin bacarıq səviyyəsi yüksəldilməli, texniki personal və qərarvericilər arasında koordinasiya artırılmalıdır. Red team və blue team formatında təlimlər, həmçinin real hadisə cavab simulyasiyaları praktiki bacarıqların gücləndirilməsində mühüm rol oynayır. Şəbəkə təhlükəsizliyi testlərinin təkmilləşdirilməsi hüquqi və normativ əsasların gücləndirilməsini tələb edir.

Ədəbiyyat

1. National Institute of Standards and Technology. (2008). *Technical guide to information security testing and assessment* (Special Publication 800-115). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdfcwe.mitre.org
2. Ross, R. S., Pillitteri, V. Y., Dempsey, K. L., Riddle, M., & Guissanie, G. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53 Revision 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.80053r5en.wikipedia.org+2en.wikipedia.org+2cwe.mitre.org+2
3. Scanlon, T. (2018, July 9). 10 types of application security testing tools: When and how to use them. *Carnegie Mellon University, Software Engineering Institute*. https://insights.sei.cmu.edu/blog/10-types-of-application-security-testing-tools-when-and-how-to-use-them/insights.sei.cmu.edu
4. Stallings, W. (2019). *Effective cyber security: A guide to using best practices and standards*. Addison-Wesley.library.matanauniversity.ac.id
5. Zhang, W., Xing, J., & Li, X. (2025). Penetration testing for system security: Methods and practical approaches. *arXiv*. https://arxiv.org/abs/2505.19174arxiv.org

6. ISO/IEC. (2022). *ISO/IEC 27005:2022—Information security, cybersecurity and privacy protection Guidance on managing information security risks*. International Organization for Standardization.en.wikipedia.org
7. National Highway Traffic Safety Administration. (2016, October). *Cybersecurity best practices for modern vehicles* (Report No. DOT HS 812 333). U.S. Department of Transportation. https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/812333_cybersecurityformodernvehicles.pdfnhtsa.gov
8. ResilientX. (n.d.). Network security testing: Best practices and tools. https://www.resilientx.com/blog/network-security-testing-best-practices-and-toolsresilientx.com
9. BlueVoyant. (n.d.). *Penetration testing: Complete guide to process, types, and tools*. https://www.bluevoyant.com/knowledge-center/penetration-testing-complete-guide-to-process-types-and-toolsbluevoyant.com
10. GetAstra. (2024). *Network security testing: Top 5 methodologies you must know*. https://www.getastra.com/blog/security-audit/network-security-testing/getastra.com
11. OWASP Foundation. (n.d.). *Penetration testing methodologies*. https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologiesowasp.org
12. Qualysec. (2025). *Network security testing: Techniques, tools, and processes*. https://qualysec.com/network-security-testing/qualysec.com

Daxil oldu: 27.02.2025
Qəbul edildi: 30.05.2025