DOI: https://doi.org/10.36719/0873/04/26-30

Nihat Əliyev
Azərbaycan Dövlət Neft və Sənaye Universiteti
Magistrant
https://orcid.org/0009-0000-2658-7792
aliyev.nihat.rasim.2024@asoiu.edu.az

Kompüter sistemlərinin penetrasiya testində zəifliklərin aşkarlanması və risklərin idarə olunması

Xülasə

Müasir informasiya sistemləri müəssisələrin əsas texnoloji dayağıdır və onların təhlükəsizliyi daimi nəzarət tələb edir. Penetrasiya testi sistemlərdəki texniki və təşkilati zəifliklərin planlı və sübutlara əsaslanan şəkildə yoxlanılması prosesidir. Məqalədə penetrasiya testinin mərhələləri, risk qiymətləndirilməsi, hesabatlandırma və bərpa tədbirləri araşdırılır. Tədqiqat göstərir ki, penetrasiya testi yalnız texniki yoxlama deyil, həm də biznes risklərinin idarə olunması və dayanıqlı kibertəhlükəsizlik üçün vacib vasitədir.

Açar sözlər: *penetrasiya testi, kompüter sistemi, zəiflik, risk, kibertəhlükəsizlik, şəbəkə, sistem təhlükəsizliyi, hesabatlandırma*

Giriş

Rəqəmsal iqtisadiyyatın inkişafı kompüter sistemlərini daha mürəkkəb etmiş və hücum səthini genişləndirmişdir. Zəif konfiqurasiya, gecikmiş yeniləmə və düzgün idarə olunmayan səlahiyyətlər təhlükəsizlik riski yaradır. Buna görə təhlükəsizlik yalnız qoruyucu proqramlarla deyil, praktik yoxlamalarla da təmin edilməlidir.

Penetrasiya testi zəifliklər real hücumçu yanaşması ilə aşkar edən səlahiyyətli təhlükəsizlik qiymətləndirməsidir. NIST SP 800-115 bu prosesin planlaşdırılması, icrası və nəticələrin təhlili üçün metodoloji yanaşma təqdim edir. Sistem penetrasiya testi əməliyyat sistemləri, şəbəkə servisleri, autentifikasiya, fayl icazələri və domen infrastrukturu kimi komponentləri əhatə edir [1]. Bu, yalnız veb tətbiq testindən daha geniş yanaşmadır. Məqalənin məqsədi penetrasiya testinin elmi və praktiki əsaslarını, zəifliklərin risk idarəetməsi ilə əlaqəsini və nəticələrin təşkilati qərarlara təsirini izah etməkdir.

Tədqiqat

Penetrasiya testi audit, zəiflik skanı və monitorinqdən fərqli olaraq zəifliklərin real istismar imkanını və biznes təsirini göstərir. Test yalnız yazılı icazə və müəyyən edilmiş sərhədlər daxilində aparılmalıdır. Sistem təhlükəsizliyi hücum səthindən asılıdır. Açıq portlar, zəif parollar, köhnə servisler və yanlış konfiqurasiyalar əsas risklərdəndir. Buna görə aktivlərin və giriş nöqtələrinin düzgün xəritələnməsi vacibdir.

Penetrasiya testində məlumat toplama, zəiflik aşkarlanması və istismar mərhələləri birlikdə tətbiq olunur. Avtomatlaşdırılmış skanerlər faydalı olsa da, nəticələr əl ilə yoxlanılmalı və riskin real təsiri qiymətləndirilməlidir. Risk qiymətləndirilməsi texniki zəifliklə biznes təsirini birləşdirir. Prioritetləşdirmə zamanı yalnız CVSS balı deyil, aktivin dəyəri və məlumatların həssaslığı da nəzərə alınmalıdır [2].

Penetrasiya testi həm də təhlükəsizlik nəzarətlərinin effektivliyini ölçür. Firewall, EDR, jurnal və SIEM sistemlərinin düzgün işləməsi yoxlanılır. Keyfiyyətli hesabat isə icra xülasəsi, sübutlar, təsir və bərpa tövsiyələrini əhatə etməlidir. Penetrasiya testi hesabatlarında sübutlar qorunmalı və həssas məlumatlar maskalanmalıdır [3]. Məqsəd təhlükəsizliyi artırmaqdır, yeni məlumat sızması yaratmaq deyil. Testin effektivliyi həm texniki bacarıqdan, həm də təşkilatın hazırlıq səviyyəsindən asılıdır. Aktiv inventarı, ehtiyat nüsxələr və əlaqə prosedurları əvvəlcədən müəyyən edilməlidir.

Xarici penetrasiya testi internetə açıq sistemləri, daxili test isə şəbəkə daxilindəki riskləri qiymətləndirir və hər iki yanaşma bir-birini tamamlayır. Sosial mühəndislik insan faktorunu qiymətləndirir, buna görə parol siyasəti və çoxfaktorlu autentifikasiya vacib müdafiə tədbirləri sayılır.

Bulud və hibrid infrastrukturlarda yanlış rol icazələri, açıq saxlama və zəif API açarları əsas risklərdəndir. Penetrasiya testi həm də insidentə reaksiya imkanlarını yoxlayır. Avtomatlaşdırma prosesi sürətləndirsə də, risklərin düzgün qiymətləndirilməsi insan təhlili tələb edir. Sistemlər dəyişdikcə yeni zəifliklər yarandığı üçün penetrasiya testi davamlı fəaliyyət kimi həyata keçirilməlidir.

Sistem penetrasiya testinin keyfiyyəti yalnız zəiflik sayına görə ölçülməməlidir. Əsas göstəricilər tapıntıların doğruluğu, yanlış pozitivlərin azlığı, sübutların aydınlığı və bərpa tədbirlərinin effektivliyidir. Buna görə retest mərhələsi vacib hesab olunur. Penetrasiya testi təşkilatda cəza deyil, təkmilləşmə vasitəsi kimi qəbul edilməlidir. Təhlükəsizlik komandası, sistem administratorları və rəhbərlik birlikdə riskləri azaltmalıdır. Əks halda texniki hesabat real dəyişiklik yaratmaya bilər.

Azərbaycan müəssisələrində əsas məsələ resursların düzgün prioritetləşdirilməsidir. İlk mərhələdə aktiv inventarı, yeniləmələr, ehtiyat nüsxələr, çoxfaktorlu autentifikasiya və administrator hesablarının yoxlanılması vacibdir. Daha sonra penetrasiya testləri ilə bu tədbirlərin effektivliyi ölçülə bilər. Penetrasiya testi həm də idarəetmə alətidir. Nəticələr büdcə planlaşdırması, risk idarəetməsi, audit və təhlükəsizlik təlimlərinə təsir etməlidir. Tapıntılar rəhbərlik üçün biznes riskləri şəklində izah edilməlidir [4].

Sistemlərin təsnifatı da vacibdir, çünki eyni zəiflik fərqli mühitlərdə müxtəlif risk yarada bilər. Buna görə aktivlərin biznes dəyəri nəzərə alınmalıdır. Test zamanı identifikasiya və giriş idarəetməsi ayrıca qiymətləndirilməlidir. Servis hesabları, administrator hüquqları, API açarları və çoxfaktorlu autentifikasiya yoxlanılmalıdır.

Windows və Linux sistemlərində yanaşma oxşar olsa da, yoxlama obyektləri fərqlənir. Windows-da Active Directory və Group Policy, Linux-da isə SSH, sudo icazələri və fayl hüquqları əsas diqqət mərkəzində olur [5]. Hər iki halda məqsəd hücumçunun giriş və səlahiyyət artırma imkanlarını müəyyən etməkdir.

Şəbəkə segmentasiyası sistem təhlükəsizliyinin əsas müdafiə mexanizmlərindən biridir. Əgər istifadəçi şəbəkəsindən verilənlər bazası serverlərinə, ehtiyat nüsxə anbarlarına və domen kontrollerlərinə birbaşa çıxış mümkündürsə, ilkin komprometasiya qısa müddətdə geniş miqyaslı insidentə çevrilə bilər. Penetrasiya testi segmentasiya qaydalarının kağız üzərində deyil, faktiki olaraq işləyib işləmədiyini göstərir. Test zamanı fərqli şəbəkə zonalarından icazə verilən və verilməyən əlaqələr yoxlanılır, lazımsız portlar müəyyən edilir və təhlükəsizlik divarı qaydalarının real təsiri qiymətləndirilir.

Ehtiyat nüsxələrin təhlükəsizliyi sistem penetrasiya testində çox vaxt ikinci planda qalır, halbuki bu sahə fidyə proqramları və daxili sabotaj riskləri baxımından kritikdir [6]. Ehtiyat nüsxə serverlərinin domen administratorları ilə eyni etimad mühitində yerləşməsi, nüsxələrin dəyişdirilə bilməsi və bərpa prosesinin test edilməməsi təşkilatı ciddi risk altında qoyur. Penetrasiya testi zamanı ehtiyat nüsxə yollarının görünməsi, giriş icazələri, şifrələmə, ayrılmış saxlama prinsipi və bərpa sınaqlarının mövcudluğu araşdırıla bilər. Məqsəd ehtiyat nüsxəni pozmaq deyil, onun müdafiə səviyyəsini qiymətləndirməkdir.

Jurnal məlumatlarının və aşkarlama qaydalarının yoxlanılması penetrasiya testinin müdafiə dəyərini artırır. Hücum ssenarisi icra olunduqda sistemlərdə hansı izlərin qaldığı, SIEM və EDR alətlərinin hansı xəbərdarlıqları yaratdığı və təhlükəsizlik komandasının bu xəbərdarlıqlara necə reaksiya verdiyi müşahidə edilir. Əgər test fəaliyyəti heç bir xəbərdarlıq yaratmırsa, təşkilat real hücumu da gec görə bilər. Buna görə penetrasiya testi yalnız zəiflik tapmaq üçün deyil, eyni zamanda aşkarlama və reaksiya mexanizmlərini kalibrləmək üçün istifadə olunmalıdır.

Məxfilik və məlumat minimallaşdırılması test prosesində xüsusi yer tutur. Penetrasiya testçisi bəzən həssas fayl adlarını, istifadəçi məlumatlarını və ya sistem konfiqurasiyalarını görə bilər. Peşəkar yanaşmada həmin məlumatlar yalnız tapıntını sübut etmək üçün minimum həcmdə qeyd

olunur. Lazımsız məlumat kopyalanmır, testdən sonra müvəqqəti fayllar silinir və hesabat qorunan kanalla təqdim edilir. Bu prinsip təşkilatın hüquqi öhdəliklərini və test komandasının etibarını qorumağa xidmət edir.

Hesabatdan sonra bərpa tədbirlərinin izlənməsi ayrıca idarəetmə prosesi kimi qurulmalıdır. Hər tapıntı üçün məsul şəxs, planlaşdırılmış düzəliş, son tarix, risk sahibi və yoxlama meyarı müəyyən edilməlidir. Yüksək riskli tapıntılar üçün müvəqqəti kompensasiyaedici nəzarətlər də tətbiq oluna bilər. Məsələn, yamağın dərhal tətbiqi mümkün deyilsə, təhlükəsizlik divarında məhdudlaşdırma, servis deaktiv edilməsi və ya monitorinq qaydasının sərtləşdirilməsi müvəqqəti risk azaldıcı tədbir ola bilər. Bu proses olmadıqda hesabat arxiv sənədinə çevrilir və real risk azalmır.

Təkrar test, yəni retest mərhələsi bərpa tədbirlərinin keyfiyyətini təsdiqləyir. Administrator zəifliyi düzəltdiyini düşünə bilər, lakin dəyişiklik yalnız bir serverə tətbiq oluna, digər oxşar sistemlərdə qalmaqda davam edə bilər. Retest tapıntının bağlanıb bağlanmadığını, yeni yan təsir yaradıb yaratmadığını və kompensasiyaedici nəzarətin işləyib işləmədiyini yoxlayır. Bu mərhələ hesabatın son nəticəsini daha etibarlı edir. Retest olmadan təşkilatın risk vəziyyəti barədə qəti fikir söyləmək çətindir. Penetrasiya testində etik haker anlayışı texniki icazədən daha genişdir. Etik davranış müştərinin məlumatına hörmət, sistemlərin davamlılığına diqqət, aşkar edilmiş zəifliklərin gizli saxlanması, maraqlar toqquşmasından qaçınma və nəticələrin şişirdilməməsi kimi prinsipləri əhatə edir [7]. Testçi tapıntını olduğundan daha təhlükəli göstərməməli, eyni zamanda real riski də yumşaltmamalıdır. Peşəkar balans texniki sübut və obyektiv izah üzərində qurulur.

Sistem penetrasiya testinin məhdudiyyətləri də açıq yazılmalıdır. Test müəyyən zaman aralığında, müəyyən icazələrlə və müəyyən texniki üsullarla aparılır. Bu o deməkdir ki, testdən sonra sistemdə heç bir zəiflik qalmadığı iddia edilə bilməz. Yeni zəifliklər yayımlana, konfiqurasiya dəyişə və ya test əhatəsindən kənar aktivlər mövcud ola bilər [8]. Keyfiyyətli hesabat bu məhdudiyyətləri göstərir və təşkilata davamlı təhlükəsizlik proqramı qurmağı tövsiyə edir.

Akademik baxımdan sistem penetrasiya testi tətbiqi tədqiqat xarakteri daşıyır. Burada nəzəri təhlükə modelləri real texniki mühitdə yoxlanılır. Testçi həm sistem arxitekturasını, həm də hücumçu davranışını anlamalıdır. Nəticələr yalnız texniki nəticə kimi deyil, risk idarəetməsi və qərarvermə mexanizmi kimi təqdim olunduqda tədqiqatın praktik dəyəri artır. Bu səbəbdən penetrasiya testinin tədrisində laboratoriya mühitləri, simulyasiya edilmiş şəbəkələr və hesabat yazma bacarıqları birlikdə öyrədilməlidir.

Sənədləşdirmə standartı testin təkrarlanmasını və nəticələrin etibarlılığını təmin edir. Hər addım, istifadə olunan sistem və alətlər qeyd edilməlidir. Düzgün sənədləşmə olmayan testin nəticəsi etibarlı sayılmaya bilər. Penetrasiya testində təhlükəsiz laboratoriya yanaşması da vacibdir [9]. Riskli sınaqlar istehsal mühiti əvəzinə test laboratoriyasında aparılaraq zəifliyin təsiri təhlükəsiz şəkildə sübut edilə bilər. Bu, xidmət dayanmasının qarşısını alır.

Tədqiqat göstərir ki, penetrasiya testi texniki müdafiə ilə idarəetmə qərarları arasında mühüm körpü rolunu oynayır. Test nəticələri texniki komandaya zəifliklərin necə yarandığını, hansı sistemlərə təsir etdiyini və onların necə aradan qaldırılmalı olduğunu sübutlarla göstərir. Eyni zamanda rəhbərlik bu zəifliklərin biznes proseslərinə, xidmət dayanıqlığına, məlumat məxfiliyinə və təşkilatın reputasiyasına təsirini daha aydın anlayır [10]. Bu yanaşma risklərin prioritetləşdirilməsini, təhlükəsizlik investisiyalarının düzgün planlaşdırılmasını və idarəetmə qərarlarının daha əsaslı qəbul edilməsini təmin edir. Buna görə penetrasiya testi yalnız texniki yoxlama vasitəsi deyil, həm də strateji risk idarəetmə aləti kimi qiymətləndirilir.

Təhlükəsiz konfiqurasiya sistem penetrasiya testinin əsas nəticələrindəndir. Bir çox zəiflik standart ayarların dəyişdirilməməsindən yaranır. Test nəticələrinə əsasən təhlükəsiz konfiqurasiya şablonları hazırlanarsa, eyni səhvlərin təkrarlanmasının qarşısı alınar [11]. Penetrasiya Penetrasiya testinin effektiv olması üçün risklər sadə və ölçülə bilən şəkildə izah edilməlidir. Rəhbərlik üçün əsas məsələ zəifliyin texniki adı deyil, onun xidmətə, məlumat məxfiliyinə və reputasiyaya təsiridir. Buna görə hesabatda təsir və tövsiyələr aydın göstərilməlidir.

Sistem penetrasiya testi həm də tədris və kadr hazırlığı üçün vacibdir. Mütəxəssislər yalnız alət istifadəsini deyil, şəbəkə protokollarını, əməliyyat sistemlərini, risk qiymətləndirməsini və hesabat

yazmağı bilməlidirlər. Praktiki laboratoriyalar və reala yaxın tapşırıqlar onların peşəkar və etik inkişafına kömək edir.

Nəticə

Kompüter sistemlərinin penetrasiya testi müasir kibertəhlükəsizlik idarəetməsində mühüm rol oynayır. Bu proses sistemlərin real hücumlara qarşı dayanıqlığını yoxlayır, texniki zəiflikləri aşkarlayır, nəzarət mexanizmlərinin işləkliyini qiymətləndirir və risklərin prioritetləşdirilməsi üçün sübut təqdim edir. Tədqiqatdan görünür ki, uğurlu penetrasiya testi yalnız skan alətlərinin istifadəsindən ibarət deyil. O, dəqiq əhatə dairəsi, hüquqi icazə, etik davranış, təhlükəsiz istismar, sübutların qorunması, biznes təsirinin izahı və bərpa prosesinin izlənməsi ilə birlikdə aparılmalıdır.

Sistem penetrasiya testinin təşkilat üçün əsas dəyəri zəifliklərin real riskə çevrilmə yolunu göstərməsidir. Bir serverdə köhnə servis, digər sistemdə zəif parol siyasəti və üçüncü komponentdə artıq səlahiyyət ayrı-ayrılıqda orta risk kimi görünə bilər. Lakin həmin zəifliklər birlikdə kritik hücum zənciri yarada bilər. Penetrasiya testi bu əlaqəni üzə çıxarır və müdafiə tədbirlərinin hansı ardıcıllıqla tətbiq olunmalı olduğunu göstərir. Bu baxımdan risk əsaslı yanaşma penetrasiya testinin mərkəzində dayanmalıdır.

Nəticə olaraq qeyd etmək olar ki, kompüter sistemlərinin təhlükəsizliyi davamlı prosesdir. Penetrasiya testi bu prosesin dövri yoxlama və öyrənmə mexanizmidir. Təşkilatlar test nəticələrini yamaq idarəetməsi, təhlükəsiz konfiqurasiya, giriş nəzarəti, monitorinq, insidentə reaksiya və əməkdaşların maarifləndirilməsi ilə əlaqələndirdikdə real müdafiə səviyyəsi yüksəlir [12]. Gələcəkdə sistem penetrasiya testinin daha effektiv aparılması üçün avtomatlaşdırılmış təhlil, süni intellekt əsaslı anomaliya aşkarlanması, hücum simulyasiyaları və risk əsaslı hesabatlandırma daha geniş tətbiq olunacaqdır.

Gələcək tədqiqatlarda sistem penetrasiya testinin avtomatlaşdırılmış risk modelləri ilə inteqrasiyası ayrıca araşdırıla bilər. Xüsusilə böyük şəbəkələrdə aktivlərin çoxluğu, konfiqurasiya dəyişikliklərinin tezliyi və bulud xidmətlərinin dinamikliyi klassik illik test modelini məhdudlaşdırır. Bu səbəbdən aktiv inventarından, zəiflik məlumat bazalarından, jurnal mənbələrindən və insident tarixçəsindən istifadə etməklə riskin daha operativ hesablanması aktual istiqamətdir. Belə model penetrasiya testçisinə hansı sistemlərin daha əvvəl yoxlanmalı olduğunu göstərə, rəhbərliyə isə təhlükəsizlik investisiyalarını daha əsaslandırılmış formada planlaşdırmağa kömək edə bilər.

Praktik baxımdan təşkilatlara tövsiyə olunur ki, penetrasiya testini ayrıca layihə kimi deyil, ümumi kibertəhlükəsizlik dövrünün tərkib hissəsi kimi qursunlar. Testdən əvvəl aktiv və məsuliyyət xəritəsi hazırlanmalı, test zamanı aşkar edilən kritik hadisələr üçün operativ əlaqə mexanizmi işləməli, testdən sonra isə bərpa planı real icra vəziyyətinə qədər izlənilməlidir. Bu ardıcıllıq təmin olunduqda penetrasiya testi yalnız zəiflik siyahısı yaratmır, müəssisənin müdafiə qabiliyyətini ölçən və gücləndirən davamlı idarəetmə mexanizminə çevrilir.

Ədəbiyyat

1. Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical Guide to Information Security Testing and Assessment. NIST Special Publication 800-115. https://csrc.nist.gov/pubs/sp/800/115/final
2. Penetration Testing Execution Standard. (2014). The Penetration Testing Execution Standard. https://www.pentest-standard.org/index.php/Main_Page
3. Penetration Testing Execution Standard. (2014). PTES Technical Guidelines. https://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
4. Herzog, P. (2010). OSSTMM 3: The Open Source Security Testing Methodology Manual. ISECOM. https://www.isecom.org/OSSTMM.3.pdf
5. National Institute of Standards and Technology. (2012). Guide for Conducting Risk Assessments. NIST Special Publication 800-30 Revision 1. https://csrc.nist.gov/pubs/sp/800/30/r1/final

6. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29
7. Joint Task Force. (2020). Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53 Revision 5. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
8. Souppaya, M., Scarfone, K., & Dodson, D. (2022). Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. NIST Special Publication 800-40 Revision 4. https://csrc.nist.gov/pubs/sp/800/40/r4/final
9. Nelson, A., et al. (2025). Incident Response Recommendations and Considerations for Cybersecurity Risk Management. NIST Special Publication 800-61 Revision 3. https://csrc.nist.gov/pubs/sp/800/61/r3/final
10. Center for Internet Security. (2024). CIS Critical Security Controls Version 8.1. https://www.cisecurity.org/controls/v8-1
11. MITRE. (2026). MITRE ATT&CK Enterprise Matrix. https://attack.mitre.org/matrices/enterprise/
12. OWASP Foundation. (2020). OWASP Web Security Testing Guide v4.2. https://owasp.org/www-project-web-security-testing-guide/v42/