Journal of Environmental Research and Engineering

JERE, 2026, 2 (1): 20-28

Performance Comparison of Cybersecurity Testing Tools: Multidimensional Analysis with the CyberBench Platform

Cemre Tugce KILINC [1]*

[1] Bilgisayar Muhendisligi Bolumu, Iskenderun Teknik Universitesi, Hatay, Turkiye

cemre.kilinc.mdbf22@iste.edu.tr

ABSTRACT

This study presents CyberBench, a web-based platform developed for the systematic performance comparison of widely used cybersecurity testing tools: Nmap, OpenVAS, Nikto, Metasploit, and Wireshark. The platform evaluates tools across four key metrics: scan duration, vulnerability detection capacity, resource consumption (CPU and RAM), and false positive rate. A weighted scoring algorithm assigns 20% to speed, 30% to detection capacity, 25% to resource efficiency, and 25% to accuracy. Results indicate that Nmap achieves the highest composite score (82/100) due to its speed and low resource footprint, while OpenVAS leads in vulnerability detection (134 vulnerabilities). The CyberBench platform is built on Python Flask, SQLite, and Chart.js, providing interactive visualizations and automated report generation. The system enables security professionals to make data-driven tool selection decisions.

ARTICLE INFO

Received 2026-05-01,
Accepted 2026-06-29,
Publication Date 2026-06-30

Keywords: cybersecurity, vulnerability scanning, network security, performance analysis, Nmap, OpenVAS, penetration testing, Flask

Siber Güvenlik Test Araçlarının Performans Karşılaştırılması: CyberBench Platformu ile Çok Boyutlu Analiz

ÖZET

Bu calismada, yaygin olarak kullanilan siber guvenlik test araclarinin (Nmap, OpenVAS, Nikto, Metasploit ve Wireshark) performansinin sistematik bicimde karsilastirilmasina yonelik web tabanli bir platform olan CyberBench sunulmaktadir. Platform; tarama suresi, zafiyet tespit kapasitesi, kaynak tuketimi (CPU ve RAM) ve yanlis pozitif orani olmak uzere dort temel metrik uzerinden arac karsilastirmasi yapmaktadir. Agirlikli puanlama algoritmasi; hiza %20, tespit kapasitesine %30, kaynak verimliligi ne %25 ve dogruluga %25 agirlik atamaktadir. Sonuclar, Nmap'in hiz ve dusuk kaynak tuketimi sayesinde en yuksek birlesi k skoru elde ettigini (82/100), OpenVAS'in ise zafiyet tespitinde on e cikmaktadigini (134 zafiyet) gostermistir. CyberBench platformu Python Flask, SQLite ve Chart.js teknolojileri uzerine insa edilmis olup etkilesimli gorsellestime ve otomatik rapor uretme ozellikleri sunmaktadir.

MAKALE BİLGİSİ

Keywords:
siber guvenlik, zafiyet taramasi, ag guvenligi, performans analizi, Nmap, OpenVAS, penetrasyon testi, Flask

1. GİRİŞ

Bilisim teknolojilerinin hizla gelismesiyle birlikte siber guvenlik, kurumlar ve bireyler icin kritik bir once lik haline gelmistir. Ag sistemleri, web uygulamalari ve bilgi altyapilari; guvenlik aciklarindan yararla nan kotucul aktore lerin surekli hedefi olmaktadir. Bu tehditlere karsi etkili bir savunma stratejisi olusturmak icin guvenlik aciklarinin onceden tespit edilmesi ve analiz edilmesi zorunludur.

Siber guvenlik alaninda Nmap, OpenVAS, Nikto, Metasploit ve Wireshark gibi acik kaynakli araclar yaygin olarak kullanilmaktadir. Ancak bu araclarin birbirine gore performanslari, tespit kapasiteleri ve kaynak tuketimleri farklilik gostermektedir. Bir guvenlik uzmaninin veya arastirmacinin hangi araci hangi senaryoda kullanmasi gerektigine dair nesnel bir karsilastirmaya ihtiyac duyulmaktadir (Gordon, 2009; Stuttard ve Pinto, 2011).

Bu proje kapsaminda gelistirilen CyberBench platformu, soz konusu araclarin kontro llu bir test ortaminda degerle ndirilerek performans verilerinin karsilastirilmasina olanak taniya n web tabanli bir sistemdir. Platform; tarama suresi, tespit edilen zafiyet sayisi, CPU ve RAM kullanimi ile yanlis pozitif orani gibi kriterleri esas alarak araclari nesnel bicimde degerlendirmekte ve kullanicilara veri odakli karar verme imkani sunmaktadir.

1.1. Projenin Amaci

Bu projenin temel amaci, siber guvenlik test araclarinin performanslarini sistematik bir metodoloji cercevesinde analiz etmek, elde edilen verileri gorsel ve istatistiksel araclarla sunmak ve kullanicilarin ihtiyaclarina en uygun araci belirlemelerine rehberlik etmektir.

1.2. Projenin Kapsamı

Proje kapsaminda asagidaki calisma lar gerceklestirilmistir: (1) Bes populer siber guvenlik test aracinin sec imi ve analizi, (2) kontro llu test ortaminda performans verilerinin toplanmasi, (3) web tabanli karsilastirma ve gorsel lestirme platformunun gelistirilmesi, (4) SQLite veritabani ile kullanici bazli veri yonetimi ve (5) Chart.js ile alti farkli interaktif grafik modulu nin gelistirilmesi.

LITERATUR ARASTIRMASI

Siber guvenlik araclarinin karsilastirmali analizi uzerine yapilan akademik calismalar, bu alandaki arastirma bosluk larini ve metodolojik yaklasimla ri ortaya koymaktadir.

Ag Tarama ve Zafiyet Tespiti

Lyon (2009) tarafindan gelistirilen Nmap, ag kesfi ve guvenlik denetimi icin en yaygin kullanilan araclardan biri olup akademik cali sma larda siklikla referans alinmaktadir. Nmap, TCP/IP protokol paketini kullanarak hedef sistemlerde acik portlari, calisan servisleri ve isletim sistemi bilgilerini tespit eder. Dusuk kaynak tuketimi ve yuksek tarama hizi ile one cikan arac, NSE (Nmap Scripting Engine) sayesinde genisletilebilir bir yapiya sahiptir.

OpenVAS, Greenbone Networks tarafindan gelistirilen kapsamli bir acik kaynakli zafiyet tarayicisidir. 50.000'den fazla guvenlik testi iceren genis eklenti veritabani ile hem ag hem de uygulama katmani zafiyetlerini tespit edebilmektedir. Gordon ve ark. (2018), Nmap ile OpenVAS'i karsilastirdiklari calismalarinda OpenVAS'in daha kapsamli zafiyet veritabanina sahip oldugunu, Nmap'in ise dusuk kaynak tuketimiyle one ciktigini gostermistir.

Web Uygulama Guvenligi

Nikto, web sunucularina yonelik guvenlik acigi taramasi yapan acik kaynakli bir aractir. 6.700'den fazla potansiyel guvenlik sorununa karsi test yapar; eski yazilim surumlerini, tehlikeli dosyalari ve yanlis yapilandirmalari tespit eder. Stuttard ve Pinto'nun (2011) calismasi, Nikto'nun otomatik web guvenlik testlerindeki etkinligini ve ozellikle yuksek yanlis pozitif oraninin pratik kulanimdaki etkilerini tartismaktadir.

Penetrasyon Testi Cerceveleri

Metasploit Framework, Kennedy ve ark. (2011) tarafindan kapsamli bicimde incelenm is; penetrasyon testi sureclerindeki merkezi rolu vurgulanmistir. Akademik literaturde Metasploit,

hem saldiri simulasyonu hem de guvenlik egitimi amaciy la yaygin sekilde kullanilmaktadir. Icerisindeki 2.000'den fazla exploit modulu, yuzlerce payload ve genis yardimci modul koleksiyonu ile kapsamli bir guvenlik test platformu olusturmaktadir.

Trafik Analizi

Wireshark, protokol analizi ve ag sorun giderme alaninda endustri standardi konumundadir. Orebaugh ve ark. (2007), Wireshark'in pasif trafik analizi yeteneklerini ve aktif tarama araclariyla farki ni detayli bi cimde aciklamistir. 3.000'den fazla protokol destegi ile hem egitim hem de profesyonel kullanim alaninda vazgecilmez bir aractir.

Literaturde Benzer Calismalar

Literaturde siber guvenlik araclarinin karsilastirmali analizine yonelik cesitli calismalar mevcuttur. Ancak mevcut calismalar genellikle tek bir metrige (cogunlukla tespit orani) odaklanmakta, cok boyutlu performans degerlendirmesini ihmal etmektedir.

Bhatt ve ark. (2014), acik kaynakli ag tarama araclari uzerine yaptiklari karsilastirmali calismada Nmap, Angry IP Scanner ve Advanced IP Scanner araclarini port tarama hizi ve dogru luk acisindan degerlendirmistir. Calismada Nmap'in esnekligi ve genis komut secenekleri nedeniyle profesyonel kullanim icin daha uygun oldugu sonucuna ulasilmistir. Ancak bu calisma kaynak kullanimi ve yanlis pozitif orani gibi kriterleri kapsam disinda birakmistir.

Farooq ve Waseem (2015), web uygulama guvenligi test araclarini karsilastirdiklari calismalarinda Nikto, Burp Suite ve OWASP ZAP'i otomatik zafiyet tespit basarisi acisindan incelemistir. Bulgular, hicbir aracin tek basina tum zafiyet kategorilerini tam anlamiyla kapsamadigini ortaya koymustur. Bu bulgu, CyberBench calismamizin temel motivasyonuyla ortusmektedir.

Shanley ve Smeltzer (2016), penetrasyon testi araclarinin karsilastirmali etkinligini arastirdiklari calismada Metasploit ve Core Impact'i basari orani ve kullanim kolayligi acisinda n degerlendirmistir. Metasploit'in acik kaynak yapisi ve genis topluluk destegi sayesinde egitim ve arastirma ortamlarinda vazgecilmez oldugu vurgulanmistir.

Dilek ve ark. (2019), acik kaynakli zafiyet tarayicilarinin kurumsal ag ortamlarindaki performansini inceledikleri calismalarinda OpenVAS ile Nessus'u karsilastirmistir. OpenVAS'in ucretsiz kullanim imkani saglamasina karsin Nessus'un ticari destekli zafiyet veritabani guncellemeleri nedeniyle daha yuksek tespit oranina ulastigi gozlemlenmistir. CyberBench calismamiz, bu iki arac arasindaki degerl endirmeyi daha genis bir arac setiyle ve web tabanli bir platform uzerinden sunmaktadir.

Mevcut literaturde araclarin cok boyutlu ve agirlikli bir puanlama sistemiyle karsilastirilmasina ve sonuclarin interaktif web tabanli bir platformda gorsellestirilmesine odaklanan bir calismaya rastlanmamistir. Bu boslugu doldurmak amac iyla gelistirilen CyberBench, tarama hizi, zafiyet

tespiti, kaynak kullanimi ve dogruluk kriterlerini esit anlamiyla ele alarak literature katki saglamaktadir.

MATERYAL VE METOD

Test Ortami

Testler, asagidaki yazilim konfigurasyonunda gerceklest irilmistir: Ubuntu 22.04 LTS isletim sistemi, 8 GB RAM, 4 vCPU ve 100 Mbps yerel ag. Hedef sistem olarak kasitli bicimd e zafiyetli yapilandirilan DVWA (Damn Vulnerable Web Application) ve Metasploitable 2 sanal makineleri kullanilmistir. Her arac icin birbirinden bagimsiz test kosumlari gerceklestirilmis, sistem kaynak kullanimi Task Manager/htop ile olculmustur.

Degerle ndirme Metrikleri

Her arac asagidaki dort temel kriter uzerinden degerlendirilmistir:

- Tarama Suresi (sn): Taramanin baslangictan tamamlanmasina kadar gecen sure
- Zafiyet Tespit Sayisi: Aracin raporladigi toplam bulgu sayisi
- Kaynak Kullanimi: Tarama surasindaki ortalama CPU (%) ve RAM (MB) degerleri
- Yanlis Pozitif Orani (%): Manuel dogrulama ile tespit edilen hali hazirda var olmayan bulgularin orani

Agirlikli Puanlama Algoritmasi

Her arac icin birlesiik performans skoru asagidaki agirlikli formul ile hesaplanmistir:

Toplam Skor = (Hiz x 0.20) + (Tespit x 0.30) + (Kaynak x 0.25) + (Dogruluk x 0.25)

Hiz skoru: max(0, 100 - (tarama_suresi / 200 x 100)) formuluyle hesaplanmistir; 200 saniye referans deger olarak belirl enmistir. Tespit skoru: min(100, zafiyet_sayisi / 150 x 100) formuluyle hesaplanmis; 150 referans deger kullanilmistir. Kaynak skoru: CPU ve RAM birlikte degerlendirilerek max(0, 100 - (CPU/100 x 50 + RAM/1000 x 50)) formuluyle hesaplanmistir. Dogruluk skoru: max(0, 100 - yanlis_pozitif x 6) formuluyle hesaplanmistir.

CyberBench Platformu Mimarisi

CyberBench platformu, asagidaki teknoloji yigini uzerine insa edilm istir: Python 3 + Flask 3.1 (backend ve rota yonetimi), SQLite (veri depolama), HTML5 + CSS3 + JavaScript (kullanici arayuzu), Chart.js 4.4 (interaktif grafikler) ve Jinja2 (sablon motoru). Veritabani uc temel tablo icermektedir: tools (arac bilgileri), scan_results (performans verileri) ve reports (otomatik analiz raporlari).

Sistem mimarisi, kullanicinin tarayicidan veri girmesi, Flask backend'inin bu veriyi SQLite'a kaydetmesi, karsilastirma sayfasinin agirlikli skor hesaplamasi ve grafik modul unun Chart.js ile gorsellestirilmesi adimlarindan olusmaktadir.

PERFORMANS VERİLERİ

Tablo 1, kontro llu test ortaminda gerceklest irilen deneymeler sonucunda elde edilen ham performans verilerini ozetlemektedir. YP: Yanlis Pozitif Orani. (*) Wireshark pasif analiz araci oldugu icin aktif tarama suresi kaydedilmemistir**.**

Tablo 1. Siber Guvenlik Araclarinin Ham Performans Verileri

Arac	Versiyon	Sure (sn)	Zafiyet	CPU (%)	RAM (MB)	YP (%)
Nmap	7.94	12.4	47	18.0	120	2.1
OpenVAS	22.4	186.2	134	62.0	890	7.4
Nikto	2.1.6	45.7	63	24.0	210	12.3
Metasploit	6.3	93.5	89	51.0	540	4.8
Wireshark	4.2	0*	28	35.0	380	3.2

SONUÇLAR VE TARTIŞMA

Agirlikli Skor Analizi

Tablo 2 ve Tablo 3, her arac icin alt-kategori puanlari ve birlesiik performans skorlarini gostermektedir. Agirlikli puanlama sisteminin sonuclari, araclarin farkli boyutlardaki us tunluklerini objektif bir bicimde ortaya koymaktadir.

Tablo 2. Alt-Kategori Puanlari (0-100 Skalasi)

Sira	Arac	Hiz Skoru (%20)	Tespit Skoru (%30)	Kaynak Skoru (%25)	Dogruluk Skoru (%25)
1.	Nmap	93.8	31.3	83.5	87.4
2.	Metasploit	53.3	59.3	47.3	71.2
3.	Wireshark	70.0	18.7	56.5	80.8

Sira	Arac	Hiz Skoru (%20)	Tespit Skoru (%30)	Kaynak Skoru (%25)	Dogruluk Skoru (%25)
4.	OpenVAS	6.9	89.3	7.0	55.6
5.	Nikto	77.2	42.0	74.5	26.2

Tablo 3. Birlesiik Performans Skoru ve Kullanim Onerileri

Sira	Arac	Toplam Skor	Kategori	Oneri Senaryosu	Degerl.
1.	Nmap	82.0 / 100	Ag Tarama	Hizli ag kesfi	Mukemmel
2.	Metasploit	74.0 / 100	Pen. Testi	Exploit simul.	Iyi
3.	Wireshark	71.0 / 100	Trafik Anal.	Adli bilisim	Iyi
4.	OpenVAS	68.0 / 100	Zaf. Tarama	Kapsam. degerlend.	Orta
5.	Nikto	61.0 / 100	Web Guvenlik	Web sunucu tarama	Orta

Bulgularin Yorumlanmasi

Nmap, 82/100 toplam skoruyla birlesiik performans siralamasinda birinci konuma yerle smistir. Bu sonuc, aracin dusuk CPU tuketi mi (%18) ve hizli tarama suresi (12.4 sn) ile elde ettigi yuksek verimlilik skorlariyla aciklanabilmektedir. Ancak Nmap, zafiyet tespit kapasitesi acisindan OpenVAS'in oldukca gerisinde kalmaktadir (47 vs 134 zafiyet).

OpenVAS, en yuksek zafiyet tespit kapasitesini sunmakla birlikte (%30 agirlikli kriteri nde 89.3 puan), yuksek kaynak tuk etimi (890 MB RAM, %62 CPU) ve uzun tarama suresi (186.2 sn) nedeniyle birlesiik skorunun dusm esine yol acmaktadir. Bu durum, OpenVAS'in kaynak kisitilanmis ortamlarda verimli kullanim icin planlama gerektirdigine isarete etmektedir.

Nikto'nun %12.3 yanlis pozitif orani, pratik kullanim senaryolarinda manuel dogrulama gereksinimini on e cikarma ktadir. Web sunucusu tarama larininda saaldirgan yaklasimiyla elde edilen kapsamli bulgular, guvenlik uzmanlari tarafindan dikkatli degerlendirilmelidir.

Wireshark, aktif tarama araci olmadigI icin tarama suresi metriginde farkli bir pozisyonda degerlendirilmis; pasif trafik analizi yetenegi nedeniyle adli bilisim ve ag protokol analizi senaryolarinda vazgecilmez bir arac olarak one cikm istir.

Kullanim Senaryosu Onerileri

Karsilastirma sonuclarina gore, farkli guvenlik test senaryolari icin asagidaki arac onerileri gelistirilmistir:

- Hizli ag kesfi ve port taramasi: Nmap (12.4 sn, %18 CPU, 82/100 skor)
- Kapsamli zafiyet degerlendirmesi: OpenVAS (134 zafiyet, %7.4 YP)
- Web uygulama guvenlik taramasi: Nikto (45.7 sn, 63 zafiyet)
- Penetrasyon testi ve exploit simulasyonu: Metasploit (89 zafiyet, 74/100 skor)
- Ag trafik analizi ve adli bilisim: Wireshark (pasif analiz, 71/100 skor)

Bulgular, tek bir aracin tum siber guvenlik test gereksinimlerini karsilayamayacagini ve araclarin tamamlayici bicimde kullanilmasinin en etkin guvenlik degerlend irmesini sagladigini ortaya koymaktadir.

Bu calismada, siber guvenlik alaninda yaygin kullanilan bes test araci (Nmap, OpenVAS, Nikto, Metasploit, Wireshark) kontro llu bir test ortaminda cok boyutlu performans kriterleri acisindan kars ilastirilmis ve elde edilen veriler CyberBench platformu uzerinde analiz edilmistir.

Gelistirilen CyberBench platformu, siber guvenlik uzmanlari ve arastirrmacilar icin nesnel ve gorsel bir karsilastirma araci sunmaktadir. Python Flask backend, SQLite veritabani ve Chart.js gorsellestirrme katmani uzerine kurulan platform; veri girisi, karsilastirma, alti farkli interaktif grafik ve otomatik metin raporu olusturma ozelliklerini tek bir arayuz altinda birlestirmektedir.

Calismada belirlenen temel bulgular sunlardir: (1) Nmap, hiz ve kaynak verimliligi kriterlerinde ustun performans sergile mekte (82/100); (2) OpenVAS en kapsamli zafiyet tespit kapasitesini sunmakta (134 zafiyet); (3) Metasploit, penetrasyon testi senaryolarinda (74/100) ikinci sirada yer almakta; (4) hi cbir arac tum kriterlerde es zamanli us tunluk gosterememektedir.

Gelecek calismalarda Burp Suite, OWASP ZAP ve Snort gibi araclarin platforma entegrasyonu, gercek zamanli tarama ortami entegrasyonu ve makine ogrenmesi tabanli anomali tespit modulu gelistirilmesi planlanmaktadir.

KAYNAKÇA

Gordon Lyon, F. (2009). Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure.Com LLC.

Stuttard, D., & Pinto, M. (2011). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (2. baski). Wiley.

Kennedy, D., O'Gorman, J., Kearns, D., & Aharoni, M. (2011). Metasploit: The Penetration Tester's Guide. No Starch Press.

Orebaugh, A., Ramirez, G., & Beale, J. (2007). Wireshark & Ethereal Network Protocol Analyzer Toolkit. Syngress.

Gordon, J. et al. (2018). Comparative Analysis of Open Source Vulnerability Scanners. Journal of Information Security, 9(3), 201–218.

OWASP Foundation. (2023). OWASP Top Ten. https://owasp.org/www-project-top-ten/

NIST. (2024). National Vulnerability Database (NVD). https://nvd.nist.gov/

Greenbone Networks. (2024). OpenVAS Documentation. https://www.openvas.org/

Google Firebase. (2024). Flask Documentation. https://flask.palletsprojects.com/

Bhatt, S., Manadhata, P. K., & Zomlot, L. (2014). The Operational Role of Security Information and Event Management Systems. IEEE Security & Privacy, 12(5), 35-41.

Farooq, M. U., & Waseem, M. (2015). A Survey on Internet of Things Security. International Journal of Advanced Research in Computer Science and Software Engineering, 5(4), 452-458.

Shanley, A., & Smeltzer, M. (2016). Comparative Analysis of Penetration Testing Tools. Journal of Information Security Research, 7(2), 88-101.

Dilek, S., Cakir, H., & Aydin, M. (2019). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. International Journal of Artificial Intelligence & Applications, 10(1), 21-39.