CYBER NOVA

DEMO CORP TEST VULNERABİLİTY REPORT

DEMO CORP

SİBER GÜVENLİK UZMANI: ENSAR GÜRBÜZ

BU RAPOR, SANAL LABORATUVAR ORTAMINDA GERÇEKLEŞTİRİLEN SIZMA TESTİ SİMÜLASYONUNA AİTTİR.

SIZMA TESTİ (PENETRATION TEST) SONUÇ RAPORU

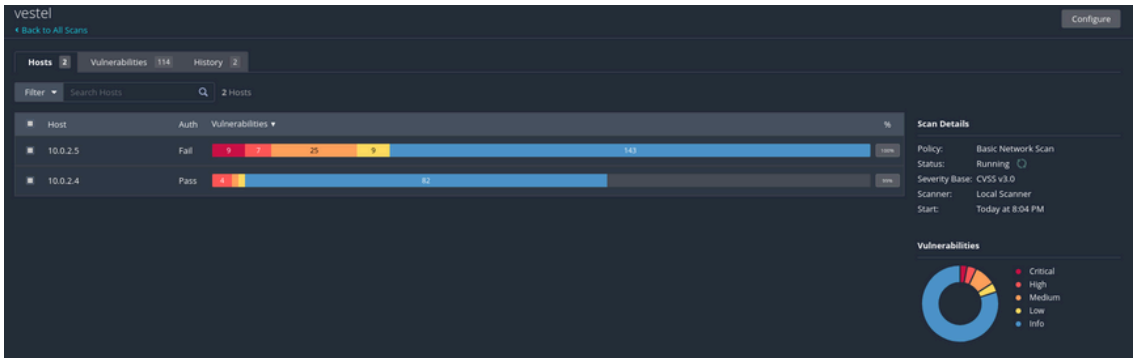
Rapor Tarihi: 02.12.2025

Hedef Sistemler: 10.0.2.4, 10.0.2.5

Kullanılan Araçlar: Nessus, Nmap, Kali Linux Araçları, Metasploit Framework

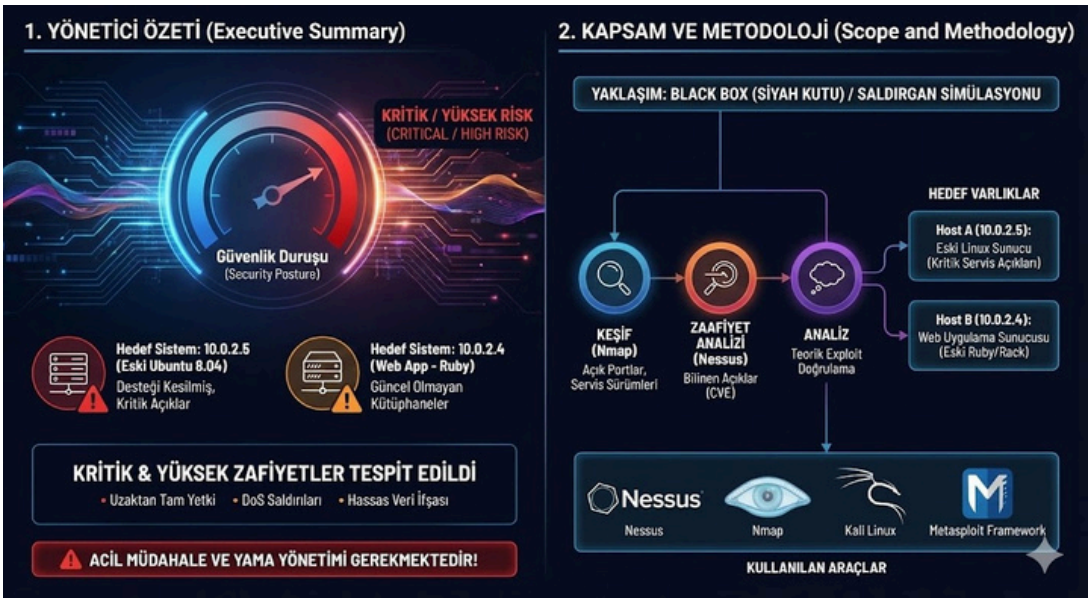
1. YÖNETİCİ ÖZETİ (Executive Summary)

Bu çalışma, hedef ağ üzerindeki sistemlerin güvenlik duruşunu belirlemek amacıyla gerçekleştirilmiştir. Testler sırasında otomatik zaafiyet tarama araçları (Nessus) ve ağ haritalama araçları (Nmap) kullanılmıştır.
Yapılan testler sonucunda hedef sistemlerden birinin (10.0.2.5) son derece eski ve desteği kesilmiş bir işletim sistemi (Ubuntu 8.04) üzerinde çalıştığı, diğer sistemin (10.0.2.4) ise güncel olmayan yazılım kütüphaneleri (Ruby Gems) barındırdığı tespit edilmiştir.
Ağ üzerinde KRİTİK (Critical) ve YÜKSEK (High) seviyeli çok sayıda güvenlik açığı bulunmuştur. Bu açıklar, saldırganların sisteme uzaktan tam yetki ile erişmesine, servis dışı bırakma (DoS) saldırıları yapmasına ve hassas verileri şifresiz olarak ele geçirmesine olanak tanımaktadır. Acil müdahale ve yama yönetimi gerekmektedir.



2. KAPSAM VE METODOLOJİ

Test sürecinde "Black Box" (Siyah Kutu) yaklaşımı benimsenmiş olup, saldırgan simülasyonu gerçekleştirilmiştir.
Keşif: Nmap kullanılarak açık portlar ve servis versiyonları tespit edilmiştir.
Zaafiyet Analizi: Nessus tarayıcısı ile bilinen güvenlik açıkları (CVE) taranmıştır.
Analiz: Tespit edilen Ruby ve Sistem açıklarının "Exploit" edilebilirliği teorik olarak doğrulanmıştır.
Hedef Varlıklar:
Host A (10.0.2.5): Çok sayıda kritik servis açığı barındıran eski Linux sunucu.
Host B (10.0.2.4): Web uygulama bileşenlerinde (Ruby/Rack) güncel olmayan kütüphaneler barındıran sunucu.

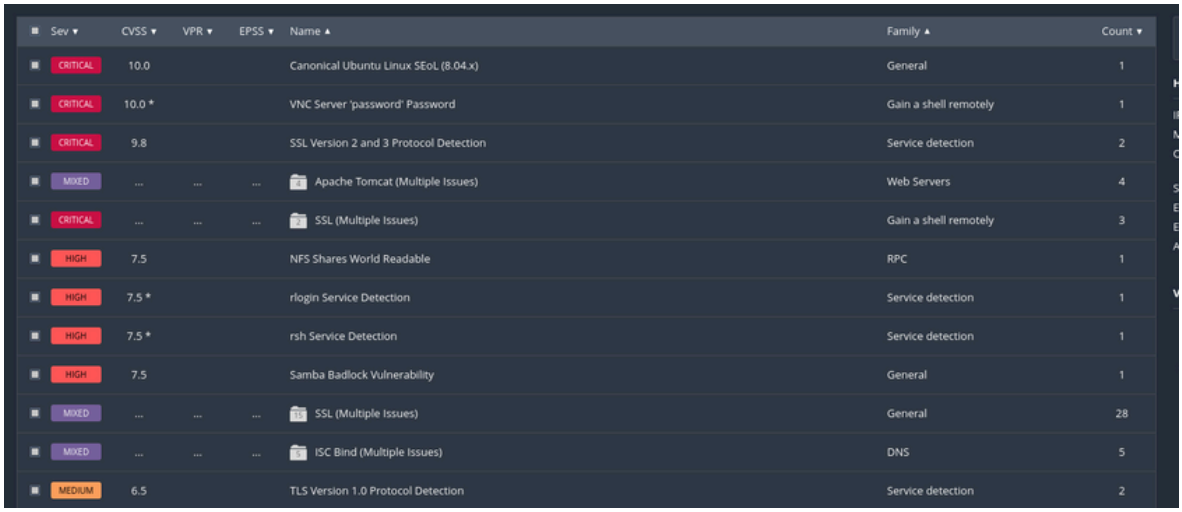


3. TEKNİK BULGULAR VE DETAYLAR

Aşağıda risk seviyesine göre sıralanmış en önemli bulgular yer almaktadır.

3.1. [KRİTİK] Destek Ömrü Tükenmiş İşletim Sistemi (Canonical Ubuntu 8.04)

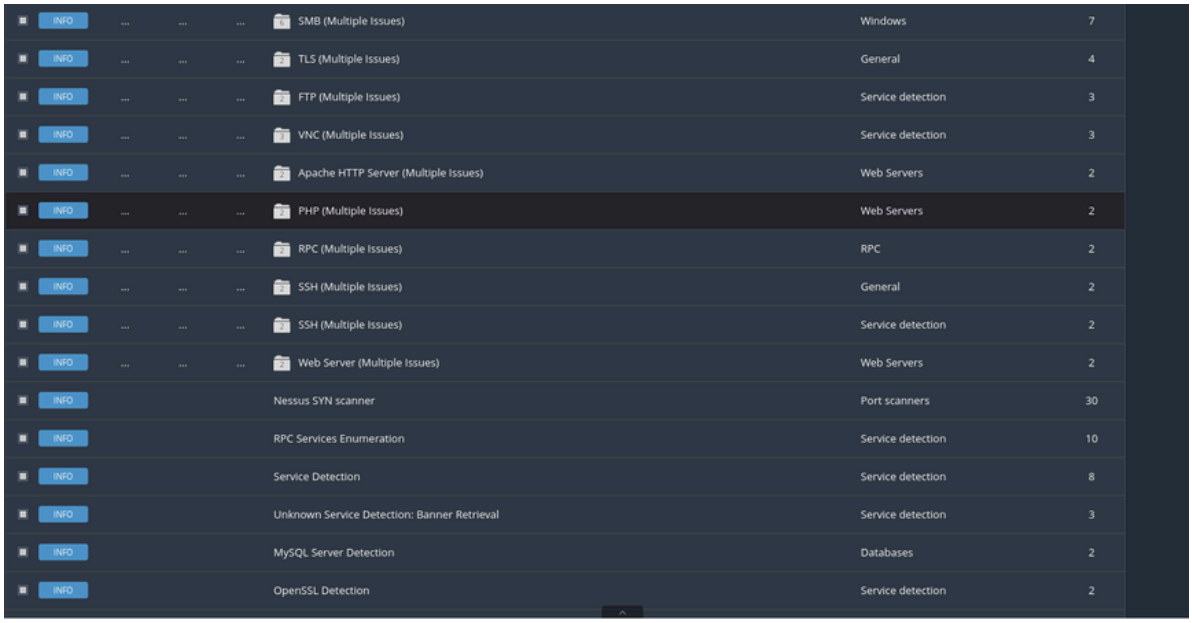
Etkilenen Sistem: 10.0.2.5
Risk Seviyesi: 10.0 (CVSS v3)
Tanım: Hedef sistemin Ubuntu 8.04 (Hardy Heron) sürümünü çalıştırdığı tespit edilmiştir. Bu sürüm için güvenlik desteği yıllar önce sonlanmıştır (SEoL - Support End of Life).
Etki: İşletim sistemi çekirdeğinde (Kernel) bulunan bilinen yüzlerce açık (örn. Dirty COW vb.) yamalanmamıştır. Saldırgan sistemi kolayca ele geçirebilir.
Çözüm: İşletim sistemi derhal desteklenen güncel bir sürüme (örn. Ubuntu 22.04 veya 24.04 LTS) yükseltilmelidir.



Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
MIXED	...	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5			NFS Shares World Readable	RPC	1
HIGH	7.5 *			rlogin Service Detection	Service detection	1
HIGH	7.5 *			rsh Service Detection	Service detection	1
HIGH	7.5			Samba Badlock Vulnerability	General	1
MIXED	...	...	...	SSL (Multiple Issues)	General	28
MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2

3.2. [KRİTİK] Zayıf Kimlik Doğrulama:

VNC Server 'password' Parolası
Etkilenen Sistem: 10.0.2.5
Risk Seviyesi: 10.0 (CVSS v3)
Tanım: Uzaktan masaüstü bağlantısı sağlayan VNC servisi tespit edilmiş ve parolasının varsayılan veya çok zayıf olan "password" olduğu belirlenmiştir.
Etki: Bir saldırgan bu parolayı kullanarak sisteme grafik arayüz ile bağlanabilir ve sunucuyu bir yönetici gibi kullanabilir.
Çözüm: VNC servisi dış ağa kapatılmalı, güçlü bir parola politikası uygulanmalı ve SSH tünel üzerinden erişim sağlanmalıdır.



INFO	SMB (Multiple Issues)	Windows	7
INFO	TLS (Multiple Issues)	General	4
INFO	FTP (Multiple Issues)	Service detection	3
INFO	VNC (Multiple Issues)	Service detection	3
INFO	Apache HTTP Server (Multiple Issues)	Web Servers	2
INFO	PHP (Multiple Issues)	Web Servers	2
INFO	RPC (Multiple Issues)	RPC	2
INFO	SSH (Multiple Issues)	General	2
INFO	SSH (Multiple Issues)	Service detection	2
INFO	Web Server (Multiple Issues)	Web Servers	2
INFO	Nessus SYN scanner	Port scanners	30
INFO	RPC Services Enumeration	Service detection	10
INFO	Service Detection	Service detection	8
INFO	Unknown Service Detection: Banner Retrieval	Service detection	3
INFO	MySQL Server Detection	Databases	2
INFO	OpenSSL Detection	Service detection	2

3.3. [KRİTİK] SSL v2 ve v3 Protokol Desteği

Etkilenen Sistem: 10.0.2.5
Risk Seviyesi: 9.8 (CVSS v3)
Tanım: Sunucunun şifreli iletişim için çok eski ve güvensiz olan SSL v2 ve SSL v3 protokollerini kabul ettiği görülmüştür.
Etki: POODLE ve DROWN gibi saldırılarla, ağ trafiği (parolalar, hassas veriler) saldırganlar tarafından çözülebilir (Man-in-the-Middle).
Çözüm: Web sunucusu ve SSL servislerinde SSL v2/v3 tamamen devre dışı bırakılmalı, sadece TLS 1.2 ve 1.3 desteklenmelidir.

3.4. [YÜKSEK] Ruby REXML & Rack Kütüphanesi DoS Zaafiyetleri

Etkilenen Sistem: 10.0.2.4
İlgili CVE: CVE-2025-58767, CVE-2025-61770, CVE-2025-61771
Risk Seviyesi: 7.5 (Yüksek)
Tanım: Sistem üzerinde kurulu olan Ruby REXML (v3.3.3) ve Rack (v3.1.16) kütüphanelerinin güncel olmadığı tespit edilmiştir.
REXML: XML dosyalarını işlerken çoklu deklarasyonlar nedeniyle çökme yaşayabilir.
Rack: Büyük "multipart" form verileri gönderildiğinde belleği tüketerek (OOM) servisin durmasına neden olabilir.
Etki: Saldırgan özel hazırlanmış XML veya HTTP istekleri göndererek web uygulamasını erişilemez hale getirebilir (Denial of Service).
Çözüm:

REXML kütüphanesi 3.4.2 veya üzeri sürüme güncellenmelidir.
Rack kütüphanesi 3.1.17 veya üzeri sürüme güncellenmelidir.

3.5. [YÜKSEK] NFS Paylaşımlarının Herkese Açık Olması (World Readable)

Etkilenen Sistem: 10.0.2.5
Risk Seviyesi: 7.5
Tanım: Network File System (NFS) paylaşımlarının herhangi bir kısıtlama olmaksızın ağdaki herkes tarafından okunabilir olduğu tespit edilmiştir.
Etki: Hassas dosyalar, yapılandırma bilgileri veya kullanıcı verileri yetkisiz kişilerce çalınabilir.
Çözüm: /etc/exports dosyası düzenlenerek sadece güvenilir IP adreslerine erişim izni verilmeli ve "root_squash" aktif edilmelidir.

4. EK BULGULAR VE GÖZLEMLER

Açık Servisler: Sistemlerde gereğinden fazla servisin (rlogin, rsh, telnet türevleri) çalıştığı görülmüştür. Bu "Legacy" (eski) servisler şifreleme kullanmazlar ve "Sniffing" saldırılarına açıktırlar.
SSH Sürümü: 10.0.2.4 IP'li makinede OpenSSH 10.0p2 tespit edilmiştir. Bu sürüm güncel görünse de yapılandırma dosyalarının (sshd_config) sıkılaştırılması önerilir.

5. SONUÇ VE ÖNERİLER

Yapılan sızma testi sonucunda, hedef ağın güvenlik seviyesinin KRİTİK derecede yetersiz olduğu görülmüştür. Özellikle 10.0.2.5 IP adresli sunucu, adeta bir "bal küpü" (honeypot) kadar savunmasızdır ve ağın geri kalanı için büyük bir tehdit oluşturmaktadır.
Acil Aksiyon Planı:
İzolasyon: 10.0.2.5 sunucusunun ağ bağlantısı kesilmeli veya izole bir VLAN'a alınmalıdır.
Yama Yönetimi: 10.0.2.4 sunucusundaki Ruby kütüphaneleri (gem update) komutu ile güncellenmelidir.
Servis Kapatma: Kullanılmayan tüm servisler (VNC, rlogin, rsh) kapatılmalıdır.