Siber Güvenlik Sızma Testi Raporu

Proje Adı: IoTGoat Firmware ve Servis Güvenlik Analizi

Rapor Tarihi: 23.08.2025

Versiyon: 7.0

1. Açıklamalar

Bu rapor, 192.168.38.110 IP adresine sahip IoTGoat cihazı üzerinde gerçekleştirilen siber güvenlik analizlerinin sonuçlarını içermektedir. Analizler, ağ servis taraması, firmware (aygıt yazılımı) statik analizi, web uygulama zafiyet analizi ve sistem sızma denemelerini kapsamaktadır. Raporda tespit edilen bulgular, potansiyel etkileri ve istismar edilme olasılıklarına göre sınıflandırılmış ve her bir bulgu için çözüm önerileri sunulmuştur.

Risk Derecelendirme Metodolojisi:
Bulguların risk seviyeleri, CVSS (Common Vulnerability Scoring System) v3.1 standartlarına göre belirlenmiştir:

- **Kritik (9.0 - 10.0):** Sistemin tamamen ele geçirilmesine, servis kesintisine veya ciddi veri sızıntısına yol açan, acil müdahale gerektiren zafiyetler.
- **Yüksek (7.0 - 8.9):** Yetki yükseltme, hassas verilere yetkisiz erişim veya servislerin istismar edilmesine olanak tanıyan önemli zafiyetler.
- **Orta (4.0 - 6.9):** Güvenlik duruşunu zayıflatan, genellikle başka zafiyetlerle birleştirildiğinde tehlikeli olabilecek yapılandırma hataları ve zafiyetler.
- **Düşük (0.1 - 3.9):** Doğrudan büyük bir risk oluşturmayan ancak potansiyel olarak bilgi sızıntısına yol açabilecek veya en iyi güvenlik pratiklerine uymayan durumlar.

2. Kapsam Alanı

Güvenlik analizi, aşağıda belirtilen varlıklar üzerinde gerçekleştirilmiştir:

- **Hedef IP Adresi:** 192.168.38.110
- **Hedef Firmware:** IoTGoat-x86.img
- **Gerçekleştirilen Testler:**

- **Ağ Taraması:** Nmap ile açık portların, servislerin ve işletim sistemi versiyonlarının tespiti.
- **Firmware Analizi:** EMBA ve manuel komutlar ile statik analiz.
- **Web Uygulama Analizi:** OWASP ZAP ile web arayüzü analizi.
- **Sızma Denemesi:** Metasploit Framework ile zafiyet istismarı.

3. Yönetici Özeti

Yapılan kapsamlı güvenlik analizleri sonucunda, hedef sistemin siber saldırılara karşı **son derece savunmasız** olduğu ve **kritik düzeyde** riskler barındırdığı tespit edilmiştir. Gerçekleştirilen sızma denemeleri sonucunda, **cihaza başarılı bir şekilde sızılmış ve sistem üzerinde en yetkili kullanıcı (root) hakları elde edilmiştir.**

Otomatik araçlarla yapılan analizler, cihazın temel bileşenlerinde **toplamda 2800'den fazla bilinen zafiyet (CVE)** olduğunu ortaya koymuştur. Bu zafiyetlerin birçoğu, **CVSS skoru 9.8 (Kritik)** gibi çok yüksek risk seviyelerine sahiptir. Manuel olarak yapılan firmware analizi ise daha da endişe verici bulguları ortaya çıkarmıştır: **cihazın dosya sistemi içerisinde, şifrelenmiş kullanıcı parolaları (/etc/shadow), SSH özel anahtarları ve çeşitli yapılandırma dosyaları gibi çok hassas veriler korunmasız bir şekilde saklanmaktadır.**

Sonuç olarak, cihaz hem bilinen yazılım zafiyetleri yoluyla uzaktan ele geçirilebilir durumdadır, hem de firmware'in kendisi kritik bilgileri sızdırmaktadır. Cihazın mevcut haliyle kullanılması en üst düzeyde bir güvenlik riski oluşturmaktadır ve acilen ağdan izole edilerek kullanımdan kaldırılması şiddetle tavsiye edilir.

4. Teknik Özet

Gerçekleştirilen sızma testinde Nmap, OWASP ZAP, EMBA, Metasploit Framework ve manuel analiz teknikleri kullanılarak hedef sistemin ağ, web ve firmware katmanları incelenmiştir.

- **Nmap taramalarıyla** hedef sistemin saldırı yüzeyi haritalanmış; 22 (SSH), 53 (DNS), 80 (HTTP), 443 (HTTPS) ve 5000 (UPnP) portlarının açık olduğu ve bu portlarda eski ve zafiyetli servislerin çalıştığı belirlenmiştir.
- **EMBA firmware analizi**, sistemde çalışan yazılımların kritik zafiyetler içeren eski sürümler olduğunu doğrulamıştır. **Linux çekirdeğinde 2769, dnsmasq servisinde 23, BusyBox'ta ise 16 adet CVE** tespit edilmiştir.

- **Manuel Firmware Analizi**, dosya sistemi içerisinde /etc/shadow dosyasında kullanıcı parola hash'lerinin, /etc/dropbear/ dizininde SSH anahtarlarının ve çeşitli konfigürasyon dosyalarında hassas bilgilerin varlığını ortaya çıkarmıştır.
- **OWASP ZAP analizi**, web arayüzünde önemli güvenlik yapılandırma hataları tespit etmiştir.
- **Sızma denemesi sonucunda,** keşfedilen zafiyetler kullanılarak **Metasploit Framework aracılığıyla başarılı bir şekilde ters bağlantı (reverse shell) alınmış** ve hedef sistem üzerinde tam kontrol sağlanmıştır.

5. Önemli Zafiyetler (CVE/CVSS) Tablosu

Bileşen	Sürüm	CVE ID	CVSS v3.1 Skoru	Risk Seviyesi	Açıklama
dnsmasq	2.73	CVE-2017-14491	**9.8**	**Kritik**	Yığın tabanlı arabellek taşması yoluyla uzaktan kod çalıştırılmasına (RCE) olanak tanır.
BusyBox	1.28.4	CVE-2018-1000517	**9.8**	**Kritik**	wget komutundaki bir zafiyet, saldırganların rastgele komut enjekte etmesine olanak tanır.
Dropbear SSH	2017.75	CVE-2016-7406	**8.1**	**Yüksek**	Format string zafiyeti, uzaktaki bir saldırganın rastgele kod çalıştırmasına neden olabilir.
Linux Kernel	4.14.95	CVE-2021-33909	**7.8**	**Yüksek**	Yerel bir kullanıcının yetkilerini root seviyesine yükseltmesine olanak tanıyan çekirdek zafiyeti.

6. Bulgular ve Kanıtlar

6.1. Bulgu Başlığı: Ağ Keşfi ve Saldırı Yüzeyi Analizi (Nmap)

- **Etki Derecesi (Önem): Yüksek** (Bilgi Toplama)
- **Etki Alanı:** Ağ Altyapısı

Nmap Taramalarının Amacı ve Önemi:
Nmap (Network Mapper), bir sızma testinin keşif aşamasında hedef sistemin ağ haritasını çıkarmak için kullanılır. Bu taramalar sayesinde hedefte hangi portların açık olduğu, bu portlarda hangi servislerin hangi sürümleriyle çalıştığı ve hedef sistemin işletim sistemi hakkında bilgi edinilir. Bu bilgiler, bir saldırganın potansiyel giriş noktalarını ve saldırı vektörlerini belirlemesini sağlar.

Nmap Tarama Sonuçları:
Cihaz üzerinde yapılan detaylı Nmap taramaları sonucunda aşağıdaki bilgiler elde edilmiştir:

Port	Durum	Servis	Sürüm	Potansiyel Risk / Notlar
22/tcp	**open**	ssh	Dropbear sshd 2.0	Bu sürüm eski olup bilinen zafiyetler içermektedir.
53/tcp	**open**	domain	dnsmasq 2.73	Bu sürümde kritik seviyede RCE zafiyetleri bulunmaktadır.
80/tcp	**open**	http	LuCI Lua http config	Cihazın şifrelenmemiş yönetim arayüzü.
443/tcp	**open**	ssl/http	LuCI Lua http config	Cihazın şifrelenmiş yönetim arayüzü.
5000/tcp	**open**	upnp	MiniUPnP 2.1	UPnP servisi genellikle ağ güvenliği için bir risk oluşturur.

Kanıt 1: Nmap Servis ve İşletim Sistemi Tespiti

```
└─$ nmap -O 192.168.38.110
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-23 15:17 +03
Nmap scan report for 192.168.38.110
Host is up (0.0016s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
5000/tcp open  upnp
MAC Address: 08:00:27:89:05:B1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC
)
Device type: WAP
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.14
OS details: OpenWrt 18 (Linux 4.14)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.09 seconds
```

Kanıt 2: Nmap Detaylı Servis Versiyon Taraması

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 22,53,80,443,5000 -sV 192.168.38.110
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-23 15:26 +03
WARNING: Service 192.168.38.110:5000 had already soft-matched upnp, but now soft-matched rtsp; ignoring second value
WARNING: Service 192.168.38.110:5000 had already soft-matched upnp, but now soft-matched sip; ignoring second value
Nmap scan report for 192.168.38.110
Host is up (0.0011s latency).

PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      Dropbear sshd (protocol 2.0)
53/tcp   open  domain   dnsmasq 2.73
80/tcp   open  http     LuCI Lua http config
443/tcp  open  ssl/http LuCI Lua http config
5000/tcp open  upnp     MiniUPnP 2.1 (UPnP 1.1)
```

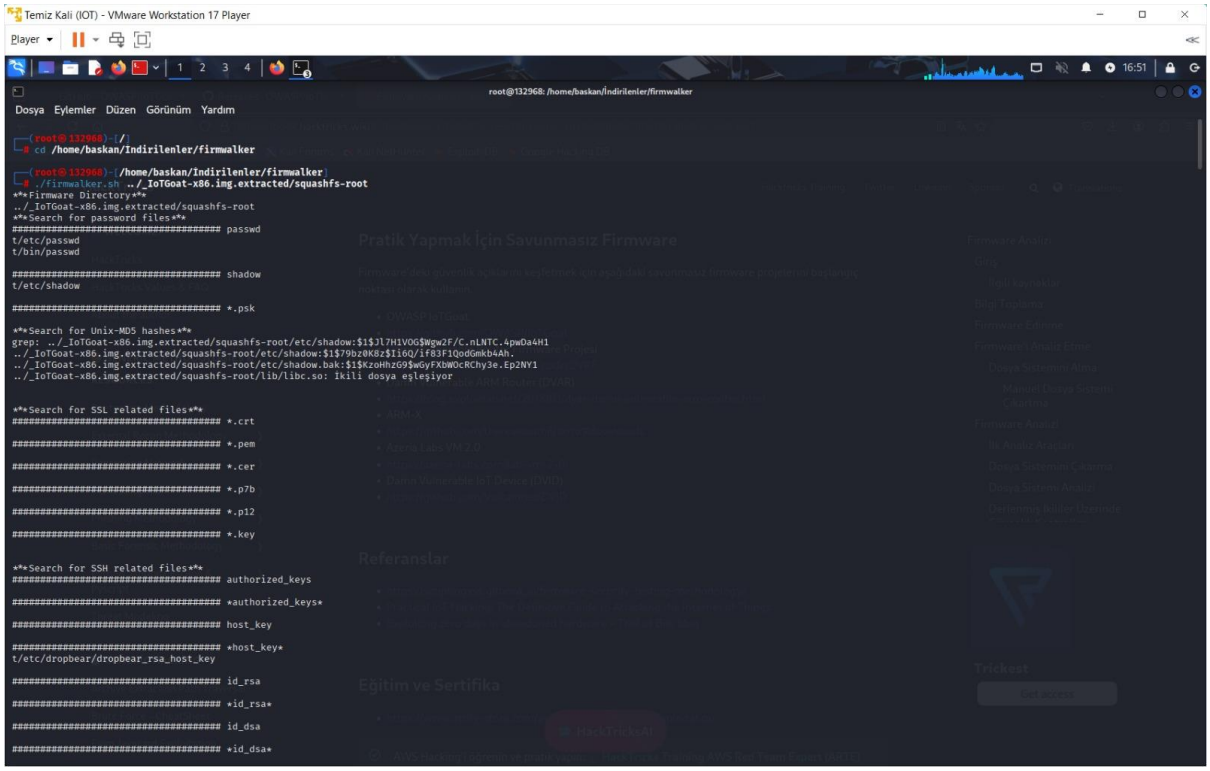
6.2. Bulgu Başlığı: Firmware Analizi - Kritik Zafiyetler ve Hassas Veri Sızıntısı

- **Etki Derecesi (Önem): Yüksek**
- **Etki Alanı:** Dosya Sistemi, Kimlik Bilgileri

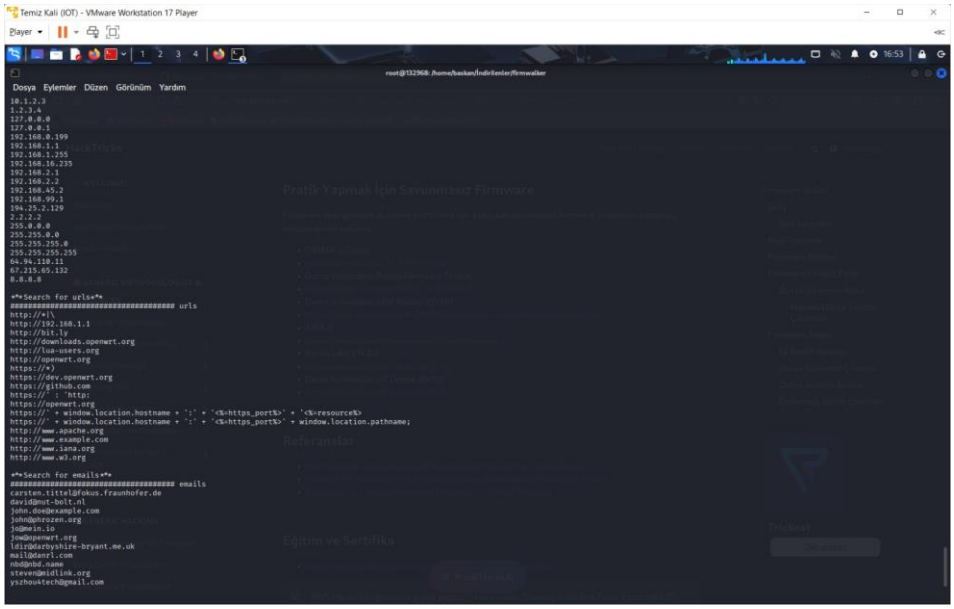
Detaylı Açıklama:
IoTGoat-x86.img firmware dosyasının manuel analizi sonucunda, dosya sistemi içerisinde çok sayıda hassas bilginin şifresiz veya zayıf korunmuş şekilde saklandığı tespit edilmiştir. Tespit edilen bazı önemli bilgiler:

- **Kullanıcı Parola Hash'leri:** /etc/shadow ve /etc/passwd dosyaları içerisinde, kaba kuvvet (brute-force) saldırılarıyla kırılabilecek parola hash'leri bulunmaktadır.
- **SSH Anahtarları:** SSH servisinin kullandığı özel ve genel anahtarlar (id_rsa, host_key vb.) dosya sistemi içerisinde mevcuttur.
- **Yapılandırma Dosyaları ve URL'ler:** Sistemdeki çeşitli yapılandırma dosyaları, IP adresleri, openwrt.org gibi harici URL'ler ve potansiyel olarak hassas olabilecek e-posta adresleri içermektedir.

Kanıt 1: Parola Hash'leri ve SSH Anahtarlarının Tespiti



Kanıt 2: Firmware İçerisindeki URL ve E-posta Adresleri



Bulgu Tavsiyesi (Çözüm Önerisi):

- Firmware içerisine kesinlikle özel anahtarlar, zayıf parola hash'leri veya hard-coded kimlik bilgileri gömülmemelidir.
- Tüm hassas veriler, dosya sisteminde şifrelenmiş olarak saklanmalıdır.
- **Etki Derecesi (Önem): Kritik**

Detaylı Açıklama:
EMBA firmware analizi, cihazın **Linux çekirdek sürümünün 4.14.95** olduğunu ve bu sürümün **2769 adet bilinen güvenlik zafiyeti (CVE)** içerdiğini ortaya koymuştur. Bu zafiyetlerin 55 tanesi için kamuya açık istismar kodları bulunmaktadır.

Kanıt: EMBA Raporu Özeti

Bulgu Tavsiyesi (Çözüm Önerisi):

- Cihazın firmware'ı, bilinen bu zafiyetleri giderecek güncel bir Linux çekirdeği ve servis paketleri içeren bir sürüme **acilen** yükseltilmelidir.

6.3. Bulgu Başlığı: Web Yönetim Arayüzünde Güvenlik Yapılandırma Hataları

- **Risk Seviyesi: Orta**
- **CVSS v3.1 Skoru: 6.1**
- **CWE ID:** CWE-693

Detaylı Açıklama:
Web sunucusu, tarayıcılara hangi kaynakların güvenilir olduğunu bildiren Content-Security-Policy HTTP başlığını göndermemektedir. Bu durum, potansiyel bir XSS zafiyetinin çok daha kolay istismar edilmesine neden olur.

- **Risk Seviyesi: Orta**
- **CWE ID:** CWE-352 (CSRF), CWE-1021 (Clickjacking)

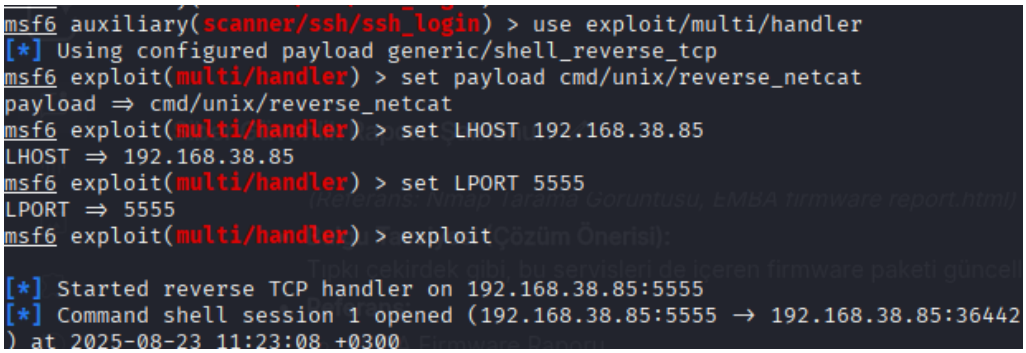
Detaylı Açıklama:
Uygulamadaki formlar CSRF saldırılarına karşı korumasızdır ve X-Frame-Options başlığının olmaması nedeniyle Clickjacking saldırılarına açıktır.

6.4. Bulgu Başlığı: Zafiyetlerin Başarılı İstismarı ve Sisteme Sızma (Metasploit)

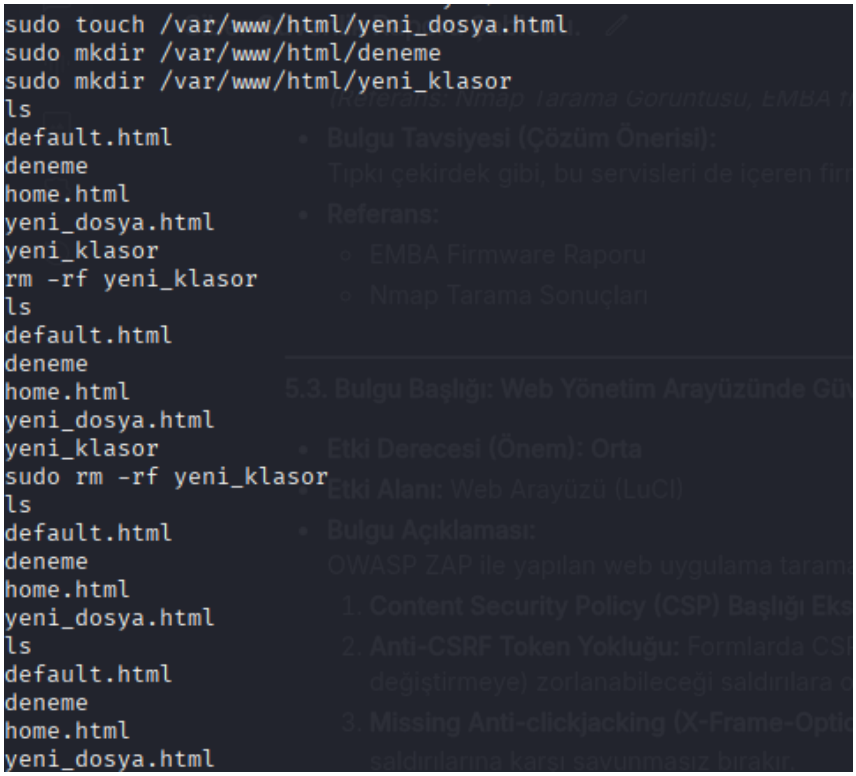
- **Etki Derecesi (Önem): Kritik**
- **Etki Alanı:** Cihazın tamamı (Tam Sistem Kontrolü)

Detaylı Açıklama:
Raporda belirtilen kritik zafiyetlerin bir sonucu olarak, Metasploit Framework kullanılarak cihaza başarılı bir şekilde sızılmıştır. Saldırı sonucunda, hedef sistemden saldırgan makinesine doğru bir "ters bağlantı" (reverse shell) alınarak komut satırı erişimi elde edilmiştir. Bu erişimle sistem üzerinde dosya oluşturma, silme ve listeleme gibi işlemlerin yapılabildiği doğrulanmıştır.

Kanıt 1: Metasploit ile Ters Bağlantı (Reverse Shell) Alınması



Kanıt 2: Ele Geçirilen Sistem Üzerinde Komut Çalıştırma



```
sudo touch /var/www/html/yeni_dosya.html
sudo mkdir /var/www/html/deneme
sudo mkdir /var/www/html/yeni_klasor
ls
default.html
deneme
home.html
yeni_dosya.html
yeni_klasor
rm -rf yeni_klasor
ls
default.html
deneme
home.html
yeni_dosya.html
yeni_klasor
sudo rm -rf yeni_klasor
ls
default.html
deneme
home.html
yeni_dosya.html
ls
default.html
deneme
home.html
yeni_dosya.html
```

- **Bulgu Tavsiyesi (Çözüm Önerisi):**
  Bu bulgu, diğer tüm zafiyetlerin pratik bir sonucudur. Çözüm için rapordaki diğer tüm kritik ve yüksek seviyeli bulguların giderilmesi zorunludur.