

**İSTANBUL GELİŞİM MESLEK YÜKSEKOKULU BİLGİSAYAR TEKNOLOJİLERİ BÖLÜMÜ**

**BİLİŞİM GÜVENLİĞİ TEKNOLOJİLERİ PROGRAMI**

**ÖDEVİN ADI**

**TryHackMe Web Sitesinde Oda Çözümleme**

**FİNAL PROJE ÖDEVİ**

**Hazırlayan**

**220175109- Mert Can Kızıldağ**

**Ödev Danışmanı**

**Öğr. Gör.Volkan Cantemir**

**İSTANBUL – 2023**

ÖDEV TANITIM FORMU

YAZAR ADI SOYADI :Mert Can Kızıldağ

ÖDEVİN DİLİ :Türkçe

DERSİN ADI :Bilgi ve Ağ Güvenliği 1

ÖDEVİN ADI :TryHackMe Web Sitesinde Oda Çözümleme

BÖLÜM :Bilgisayar Teknolojileri

PROGRAM : Bilişim Güvenligi Teknolojileri

ÖDEVİN TÜRÜ : Vize / Ders içi / Final ÖDEVİN TES. TARİHİ :29.12.2023

ÖDEV DANIŞMANI : Öğr. Gör.Volkan Cantemir

# BEYAN

Bu ödevin/projenin hazırlanmasında bilimsel ahlak kurallarına uyulduğu, başkalarının ederlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğu, kullanılan verilerde herhangi tahrifat yapılmadığını, ödevin/projenin herhangi bir kısmının bu üniversite veya başka bir üniversitedeki başka bir ödev/proje olarak sunulmadığını beyan eder, aksi durumda karşılaşacağım cezai ve/veya hukuki durumu kabul eder; ayrıca üniversitenin ilgili yasa, yönerge ve metinlerini okuduğumu beyan ederim.

25.12.2023

Mert Can Kızıldağ

# KABUL VE ONAY SAYFASI

220175109 numaralı Mert Can Kızıldağ’ın Öğrenci TryHackMe Web Sitesinde Oda Çözümleme adlı çalışması, benim tarafımdan Vize/Ders içi/Final ödevi olarak kabul edilmiştir.

Öğr. Gör.Volkan Cantemir

# ÖZET

Bu projede TryHackMe Web Sitesinden 10 oda çözümlemesi yapılmıştır. Çözülen odalar aşağıdaki gibidir.

1.OpenVPN

2.Nmap

3.Metasploit:Introduction

4.Tor

5.Vulnversity

6.Basic Pentesting

7.Google Dorking

8.Cryptography for Dummies

9.c4ptur3-th3-fl4g

10.Mr Robot CTF

**İÇİNDEKİLER**

Ödev Tanıtım Formu 2

Beyan 3

Kabul Onay Sayfası 4

Özet…………………………………………………………………………………………………………………………….5

[İçindekliler……………………………………………………………………………………………………………………..6](#_TOC_250000)

**BİRİNCİ BÖLÜM**

**ÇÖZÜMLEMEYE BAŞLAYALIM**

* 1. OpenVPN Çözümleme 8-9
  2. Nmap Çözümleme 10-12
  3. Metasploit:Introduction Çözümleme 13-15
  4. Tor Çözümleme 16-17
  5. Vulnversity Çözümleme 18-19
  6. Basic Pentesting Çözümleme 20
  7. Google Dorking Çözümleme 21-22
  8. Cryptography for Dummies Çözümleme 23-25
  9. c4ptur3-th3-fl4g Çözümleme 26-27
  10. Mr Robot CTF Çözümleme…………………………………………………………………………………..28

# ÖN SÖZ

Ödev boyunca yardımını esirgemeyen Öğr. Volkan Cantemir’ e minnet ve şükranlarımızı sunarız.

Grup arkadaşımla beraber yaptığımız çalışma boyunca birlikteliğimiz için de teşekkür ederim

**BİRİNCİ BÖLÜM**

**ÇÖZÜMLEMEYE BAŞLAYALIM**

* 1. **OpenVPN Çözümleme**

**OpenVPN Nedir?**

OpenVPN, sanal özel ağlar (VPN) oluşturmak için kullanılan bir açık kaynaklı yazılımdır. VPN'ler, internet üzerinden veri iletimini güvenli hale getirmek ve internet kullanıcılarının gizliliğini korumak amacıyla kullanılır. OpenVPN, bu amaçlar doğrultusunda geniş bir kullanıcı kitlesi tarafından tercih edilen bir çözümdür.

**OpenVPN'in temel özellikleri:**

Güvenlik: OpenVPN, güçlü şifreleme yöntemleri kullanarak veri iletimini güvenli hale getirir. Bu sayede, kullanıcılarının internet trafiğini izleyen kişilerin verilerine erişmesini zorlaştırır.

Açık Kaynaklı: OpenVPN açık kaynaklı bir projedir, bu da kullanıcıların kaynak kodlarına erişim

sağlayarak yazılımı incelemelerine ve geliştirmelerine olanak tanır. Bu, güvenlik açısından avantajlıdır,

çünkü yazılımın topluluğu tarafından düzenli olarak denetlenir.

Çeşitli Platformlarda Çalışma: OpenVPN, Windows, macOS, Linux ve birçok mobil platformda

çalışabilir. Bu, farklı cihazlarda ve işletim sistemlerinde kullanılabilmesini sağlar.

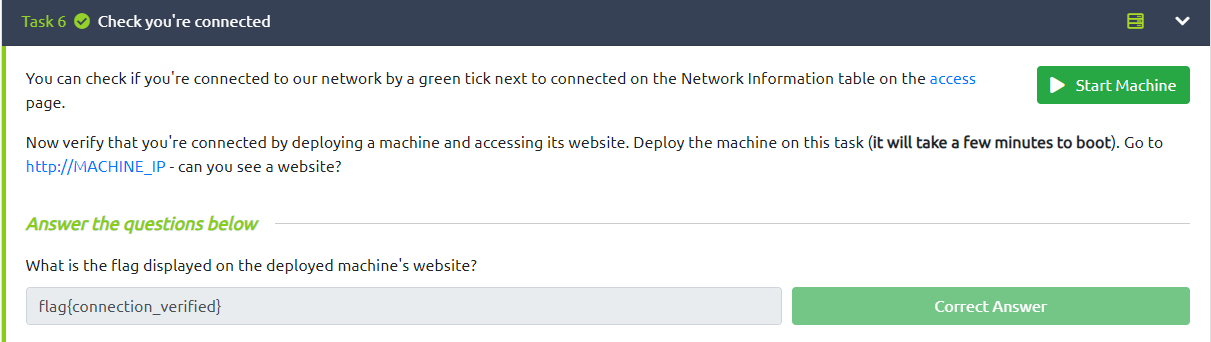
Esnek Konfigürasyon: OpenVPN, bir dizi konfigürasyon seçeneği sunar, bu da kullanıcıların

ihtiyaçlarına ve sistem gereksinimlerine uygun şekilde yapılandırılabilmesini sağlar.

Site-to-Site ve Remote Access VPN Desteği: OpenVPN, hem site-to-site VPN bağlantıları hem deuzaktan erişim VPN'leri için kullanılabilir. Bu özellik, hem kurumsal ağlarda hem de bireysel kullanıcılar için geniş bir kullanım alanı sağlar.

SSL/TLS Tabanlı Güvenlik: OpenVPN, genellikle SSL/TLS protokollerini kullanarak güvenlik sağlar. Bu da açık internet üzerinden veri iletimini şifreleyerek güvenli bir bağlantı kurulmasını sağlar.

Open VPN Odaları Çözümü



1.2 Nmap Çözümleme

Nmap Nedir ?

Nmap, ağ güvenliği ve keşif işlemleri için kullanılan bir açık kaynaklı güvenlik tarayıcısıdır. "Network Mapper" kısaltmasıyla bilinen Nmap, bilgisayar ağları üzerindeki cihazları ve sistemleri tarayarak çeşitli bilgileri toplar. Bu bilgiler, ağda bulunan cihazların IP adresleri, açık portlar, çalışan servisler ve işletim sistemleri gibi önemli bilgileri içerebilir.

Nmap'ın Temel Özellikleri:

**Port Taraması (Port Scanning):** Nmap, bir hedef sistemdeki açık portları belirlemek için kullanılır. Bu, ağdaki hedef sistemlerin hangi servisleri kullanmakta olduğunu anlamak için önemlidir.

**Servis Sürümü Tespiti:** Nmap, açık portların yanı sıra çalışan servislerin sürümlerini de tespit edebilir. Bu, potansiyel güvenlik açıklarını belirlemede yardımcı olabilir.

**İşletim Sistemi Tespiti:** Nmap, hedef sistemde çalışan işletim sistemini belirleme yeteneğine sahiptir. Bu bilgi, güvenlik testleri sırasında sistemin zayıf noktalarını anlamak için kullanılabilir.

**Script Oluşturma ve Çalıştırma:** Nmap, kullanıcıların özel scriptler oluşturmasına ve çalıştırmasına olanak tanır. Bu, özelleştirilmiş güvenlik kontrolleri yapma yeteneğini artırır.

**Grafik Arayüz ve Komut Satırı Desteği:** Nmap, hem komut satırı üzerinden hem de grafik arayüz ile kullanılabilir. Bu, farklı kullanıcıların tercihlerine göre esnek bir kullanım sunar.

Nmap Kullanım Alanları:

**Güvenlik Denetimleri:** Sistem ve ağ güvenliği değerlendirmeleri için Nmap sıkça kullanılır. Açık portlar, güvenlik duvarı konfigürasyonları ve servis sürümleri gibi detaylar incelenir.

**Ağ Keşfi:** Büyük ağlardaki cihazları ve kaynakları tespit etmek amacıyla Nmap kullanılır. Bu, ağ yöneticilerine ağlarını daha iyi anlama ve yönetme imkanı sağlar.

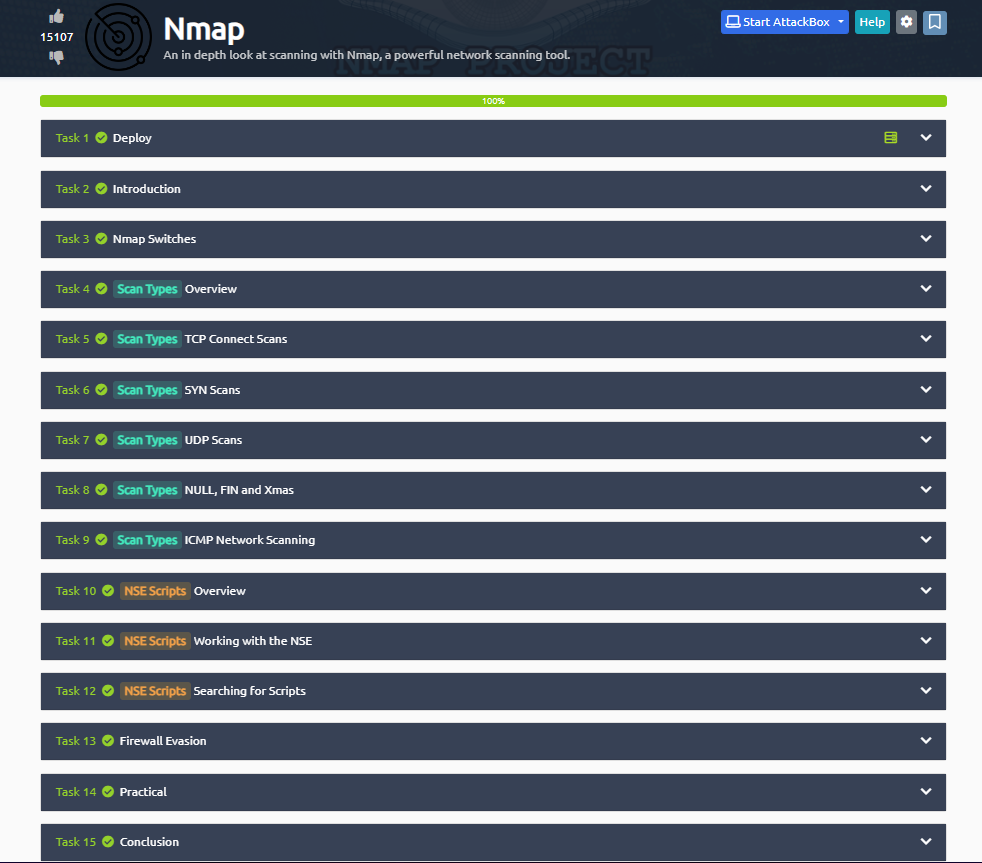
**Penetrasyon Testleri:** Nmap, güvenlik açıklarını tespit etmek ve sistemlere yetkisiz erişimleri önlemek amacıyla penetrasyon testleri sırasında kullanılır.

**Örnek Nmap Komutu:**

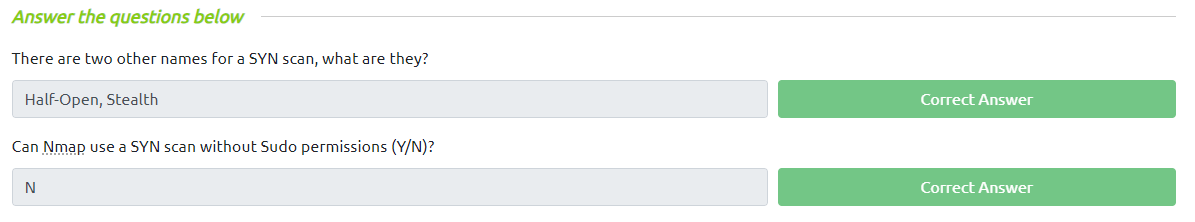
nmap -sP 192.168.1.0/24

Bu komut, 192.168.1.0 IP aralığındaki cihazları tarar ve bunların hangilerinin çevrimiçi olduğunu gösterir.

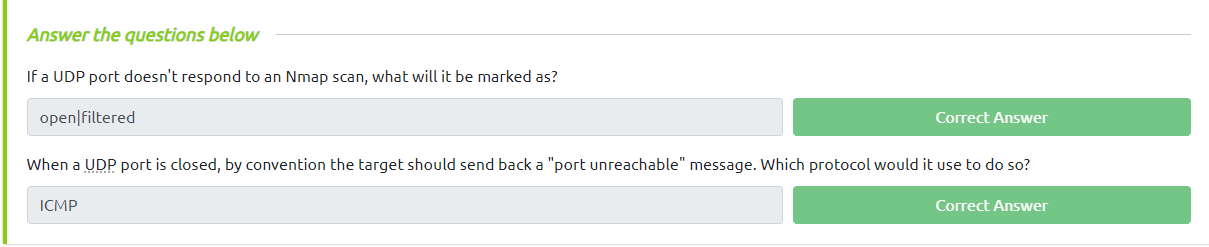
**Nmap Çözümleri**



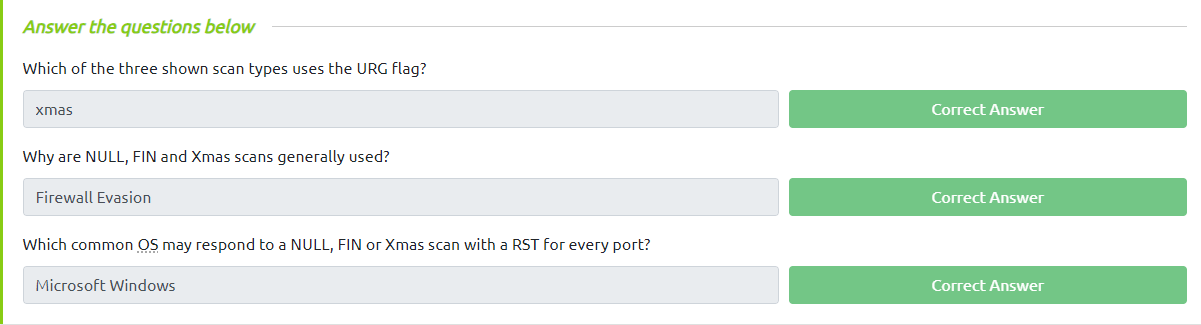
Bazı soruların cevapları



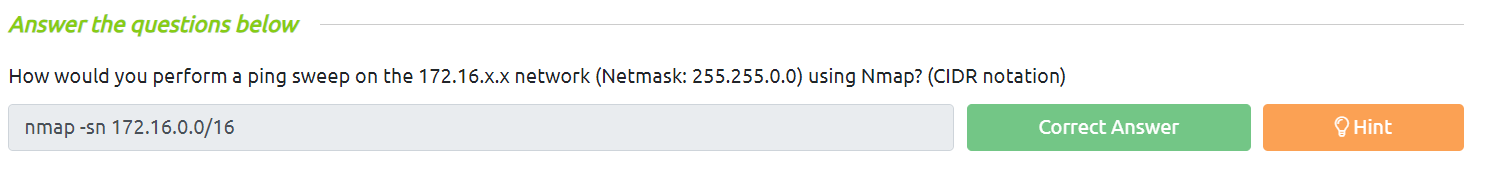
Görsel 1Task 6 Cevap



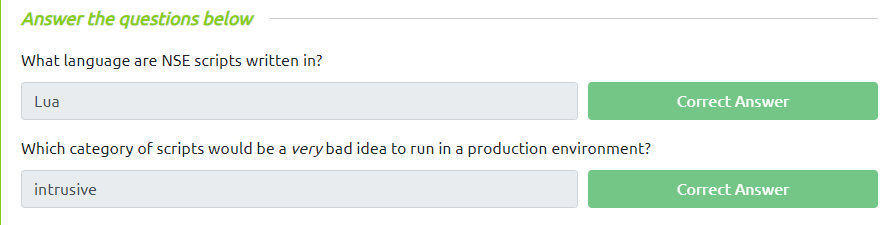
Görsel 2Task 7 cevap



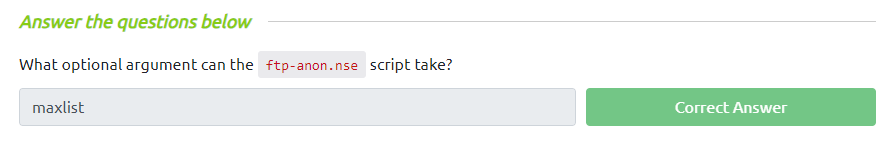
Görsel 3 Task 8 cevap



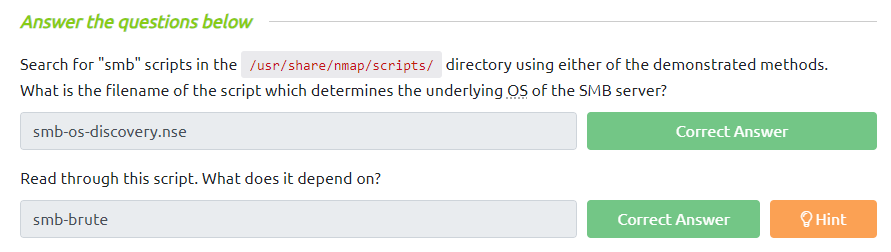
Görsel 4 Task 9 cevap



Görsel 5 Task 10 cevap



Görsel 6 Task 11 cevap



Görsel 7 Task 12 Cevap

**1.3 Metasploit:Introduction Çözümleme**

**Metasploit Framework Nedir?**

Metasploit Framework, bilgisayar sistemlerindeki güvenlik açıklarını tespit etmek ve kapatmak

için kullanılan bir açık kaynaklı güvenlik aracıdır. Rapid7 tarafından geliştirilen bu çerçeve, siber

güvenlik uzmanları, etik hackerlar ve penetrasyon test uzmanları tarafından sıkça kullanılır.

Metasploit, bilgisayar sistemlerini siber saldırılara karşı korumak için kullanılan bir dizi modül ve

araç içerir.

**Temel Özellikler:**

**Exploit Modülleri:** Metasploit, bir dizi hazır saldırı modülü içerir. Bu modüller, belirli bir zafiyeti

sömürmek için kullanılır. Metasploit, bu modüllerin geniş bir koleksiyonunu içerir ve sürekli

olarak güncellenir.

**Payload Modülleri:** Payload, hedef sistemde çalışan zararlı kodu temsil eder. Metasploit, çeşitli

payload modülleri sağlar, bu da kullanıcıya çeşitli zararlı işlemleri gerçekleştirme ve hedef sistemde kontrol sağlama olanağı tanır.

**Gelişmiş Shell Kontrolü**: Metasploit, hedef sistemde bir kabuk (shell) elde etme ve bu kabuk

üzerinden çeşitli komutları gerçekleştirme yeteneği sunar. Bu, sistem üzerinde tam kontrol sağlamak için kullanılır.

**Ve çok daha fazlası:** Metasploit'in diğer birçok özelliği arasında modüler yapı, otomatik zafiyet

tarama, sosyal mühendislik araçları ve geniş bir kullanıcı topluluğu bulunmaktadır.

**Kullanım Alanları:**

**Penetrasyon Testleri**: Metasploit, kurulu sistemlerde güvenlik zafiyetlerini test etmek amacıyla etik

hackerlar tarafından sıkça kullanılır.

**Güvenlik Eğitimi:** Sistem yöneticileri ve güvenlik uzmanları, Metasploit'i güvenlik eğitimlerinde

kullanarak savunma yeteneklerini artırabilirler.

**Siber Savunma ve Güvenlik Analizi:** Metasploit, siber saldırıların tespiti ve savunma stratejileri

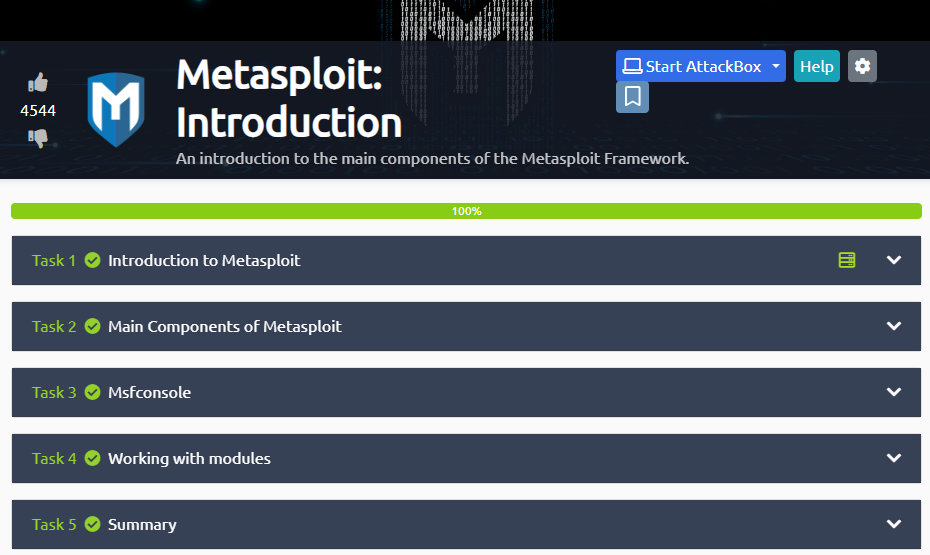
oluşturmak için kullanılır.

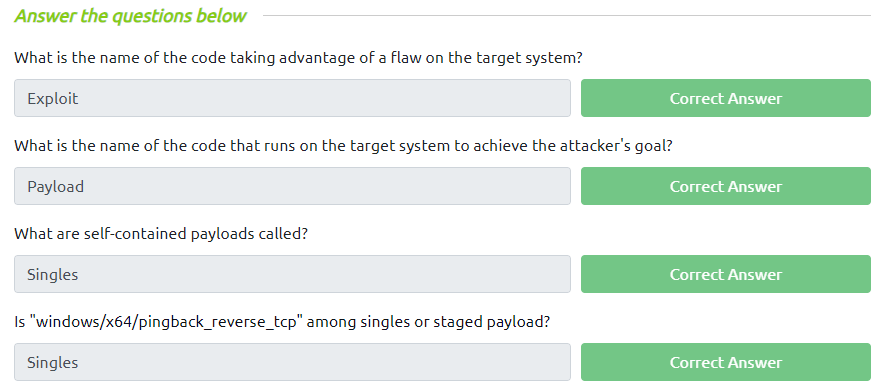
**Metasploit Kullanımı:**

Metasploit, komut satırı arayüzü (CLI) veya arayüzü (GUI) kullanılarak çalıştırılabilir. Kullanıcılar, belirli bir zafiyeti hedef almak veya belirli bir saldırıyı simüle etmek için gerekli modülleri seçebilir ve ardından hedef sisteme saldırı gerçekleştirebilirler.

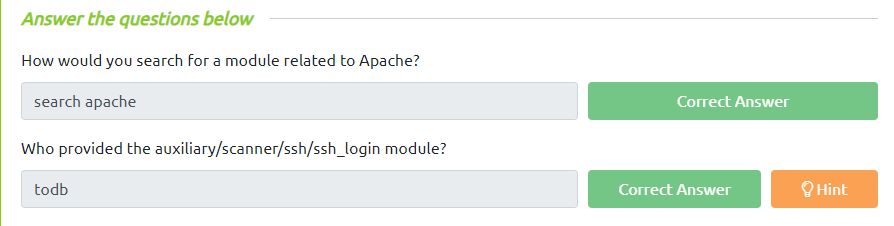
**Metasploit:Introduction**

**Cevapları**

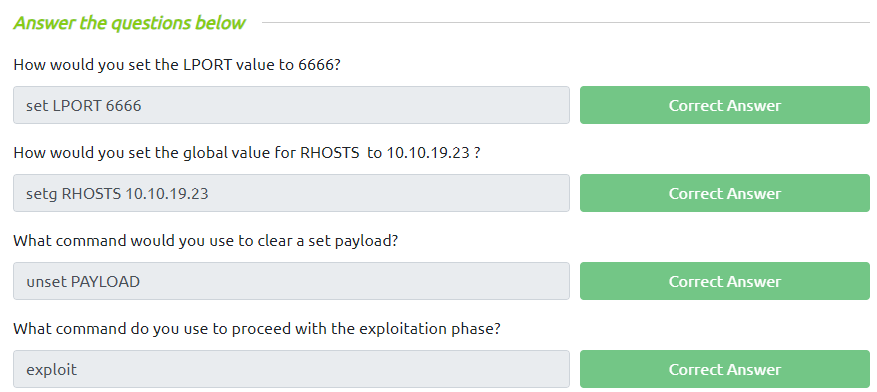




Görsel 8metasploit task2 cevap



Görsel 9 metasploit task3 cevap



Görsel 10 metasploit task4 cevap

**1.4. Tor Çözümleme**

**TOR (The Onion Router) Nedir?**

Gizlilik Odaklı Bir Ağ: TOR, kullanıcıların internet üzerinde anonim olarak gezinmelerine izin veren bir gizlilik odaklı bir ağ sistemidir. İnternet trafiği, TOR ağı içinde rastgele seçilmiş bir dizi sunucu (relay) üzerinden yönlendirilir.

**Çok Katmanlı Şifreleme (Onion Routing):** TOR, veri paketlerini şifreleyerek ve bir dizi rastgele seçilmiş sunucu üzerinden yönlendirerek kullanıcıların izini sürmeyi zorlaştırır. Her bir sunucu, paketin bir katmanını şifre çözer ve ardındaki bir sonraki sunucuya iletir, bu nedenle "soğan" benzeri bir yapıda çok katmanlı şifreleme anlamına gelir.

**Ücretsiz ve Açık Kaynaklı:** TOR projesi, ücretsiz ve açık kaynaklı bir inisiyatiftir. Herkes bu teknolojiyi kullanabilir, inceleyebilir ve geliştirebilir.

**Sansürü Aşma ve Erişim Özgürlüğü:** TOR, sansüre maruz kalan bölgelerde ve ülkelerde internet sansürünü aşma ve sansürlü içeriklere erişim sağlama amacıyla kullanılabilir. Ayrıca, TOR, internet sansürünü ve gözetimini önlemek için kullanıcılara daha geniş bir erişim özgürlüğü sunar.

**Tor Tarayıcı:** Tor projesi, geliştirdiği özel bir tarayıcı olan "Tor Browser" ile de bilinir. Bu tarayıcı, kullanıcıların TOR ağına bağlanmasını kolaylaştırır ve anonim bir şekilde internet üzerinde gezinmelerine olanak tanır.

**Gönüllü Sunucular:** TOR ağı, dünya genelinde bir dizi gönüllü işletilen sunucu tarafından desteklenir. Bu sunucular, trafiği şifreleyerek ve yönlendirerek ağın güvenliğini artırır.

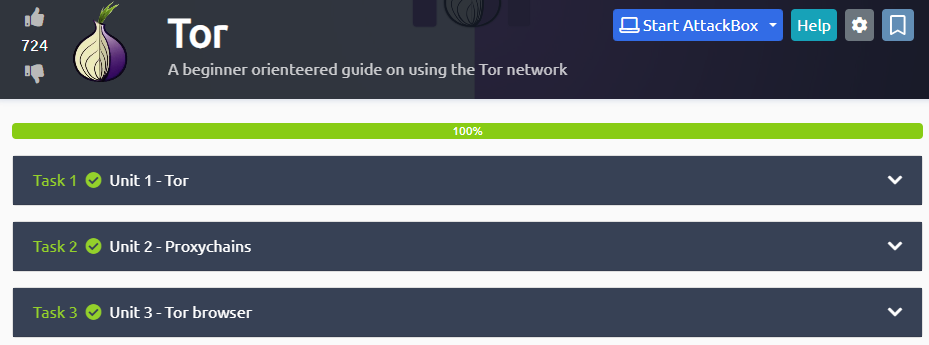
**Kullanım Alanları:**

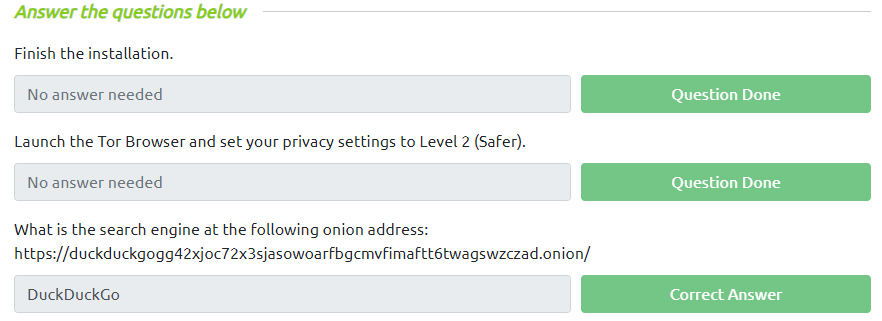
Gizlilik ve Anonimlik: TOR, internet kullanıcılarının gerçek kimliklerini gizleyerek anonim bir şekilde gezinmelerini sağlar.

**Sansür ve Gözetim Karşıtı:** TOR, sansür uygulamalarına maruz kalan bölgelerdeki kullanıcılar için sansürü aşma ve gizliliklerini koruma amacıyla kullanılabilir.

**Geliştirici ve Araştırmacılar İçin:** Güvenlik araştırmacıları ve geliştiriciler, TOR'u güvenlik açıklarını test etmek ve geliştirmek amacıyla kullanabilir.

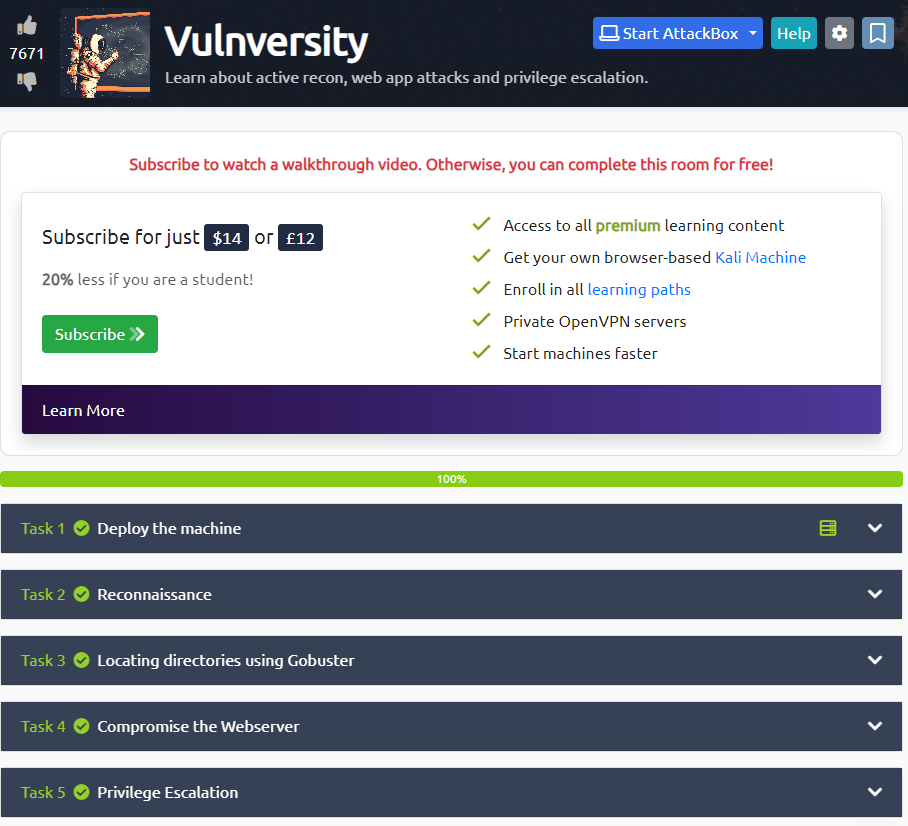
**İnternet Erişim Kontrolü (Censorship Circumvention):** TOR, internet sansürü uygulamalarına karşı bir çözüm olarak kullanılır, özellikle baskıcı rejimlerde ve sansür uygulamalarının yoğun olduğu bölgelerde.

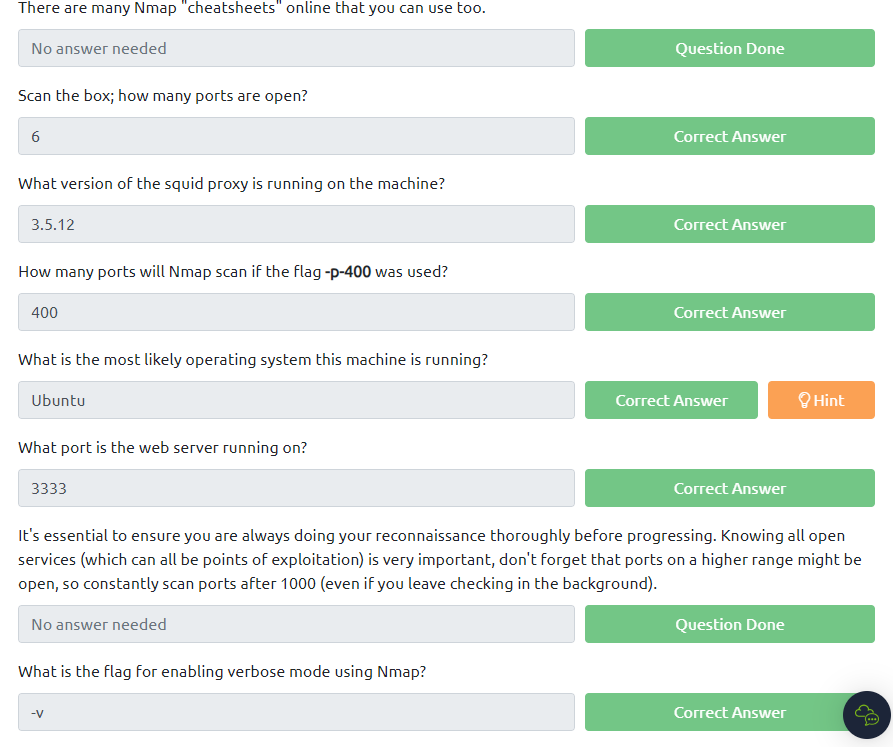




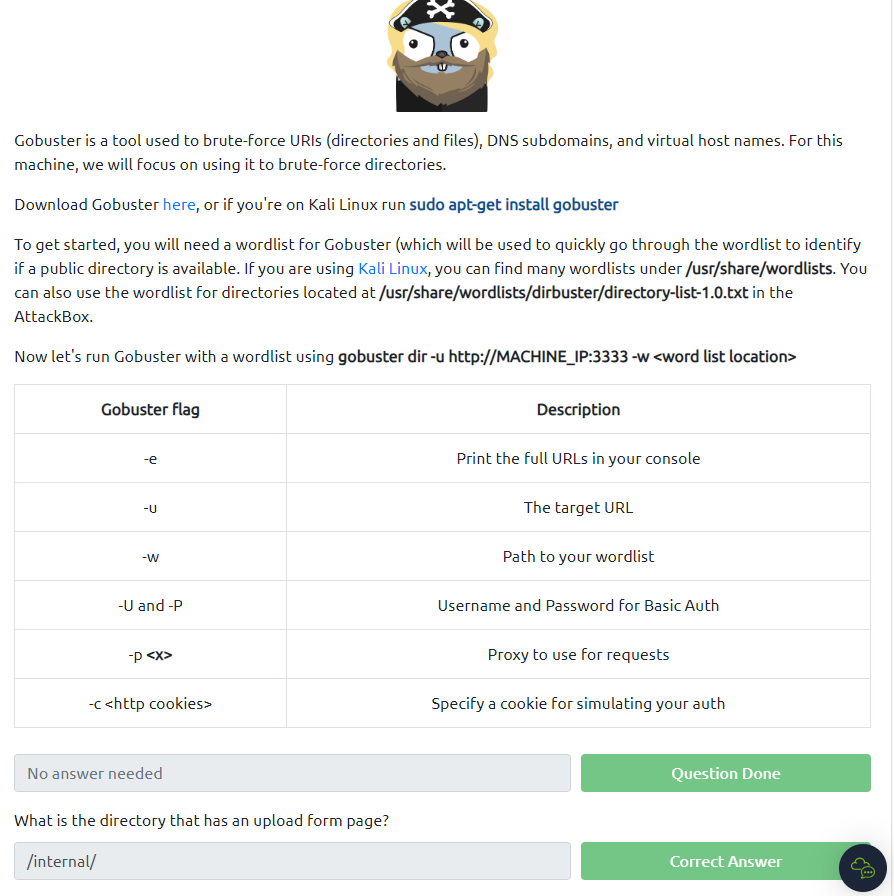
Görsel 11 tor task 3 cevap

**1.5. Vulnversity Çözümleme**

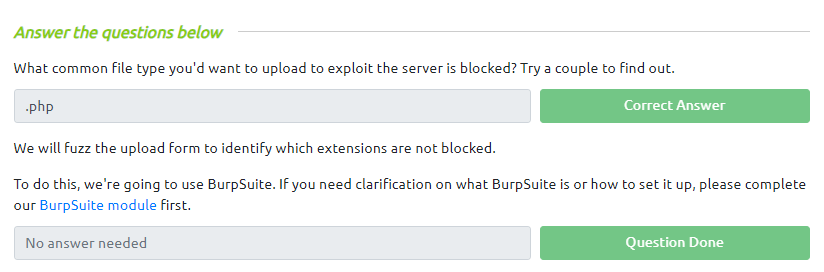




Görsel 12Vulnversity task2 cevap

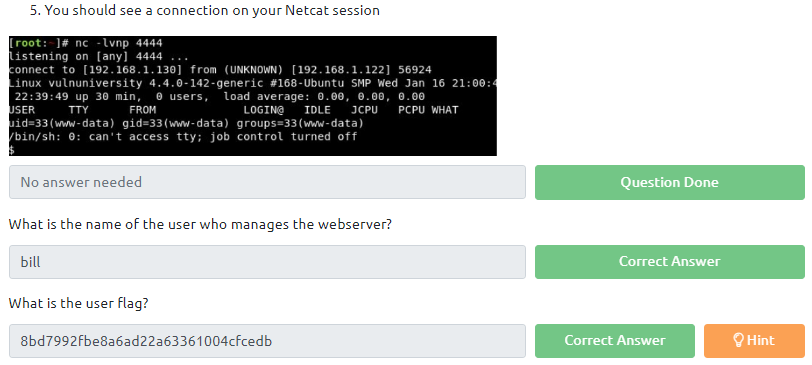


Görsel 13vulnversity task 3 cevap



Görsel 14vulnversity task 4 cevap



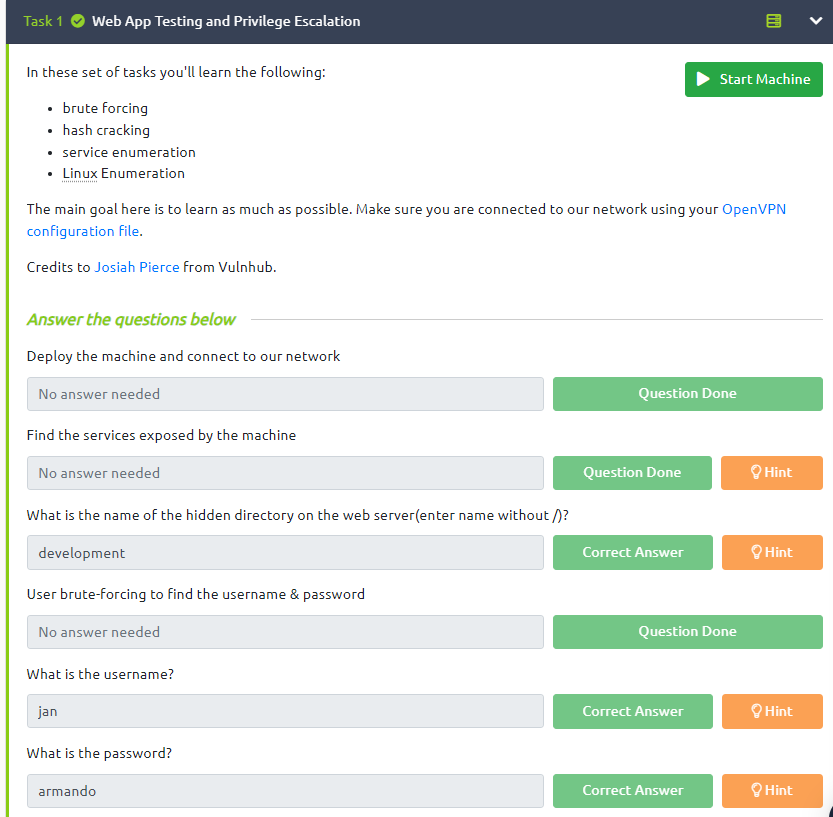


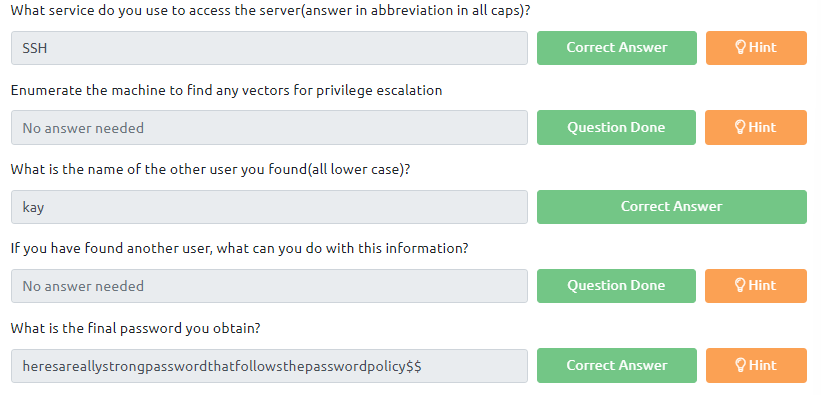
Görsel 15vulnversity task 5 cevap

**1.6. Basic Pentesting Çözümleme**

Bu odada kaba kuvvet saldırısı yapmayı ve genel olarak servis ve linuxdan detaylı bilgi alıcaz .

Pentest sonrası oda cevapları aşağıdaki gibidir.

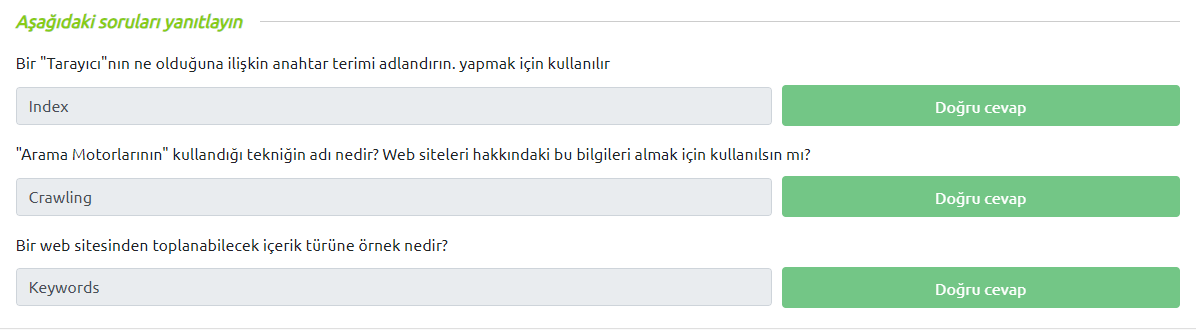




**1.7. Google Dorking Çözümleme**

Google dorking en özet amacı belirli operatörleri kullanarak daha geniş detaylı sorguılar yaparak hedeflenmiş tam sonuca ulaşmamıza olanak tanır.

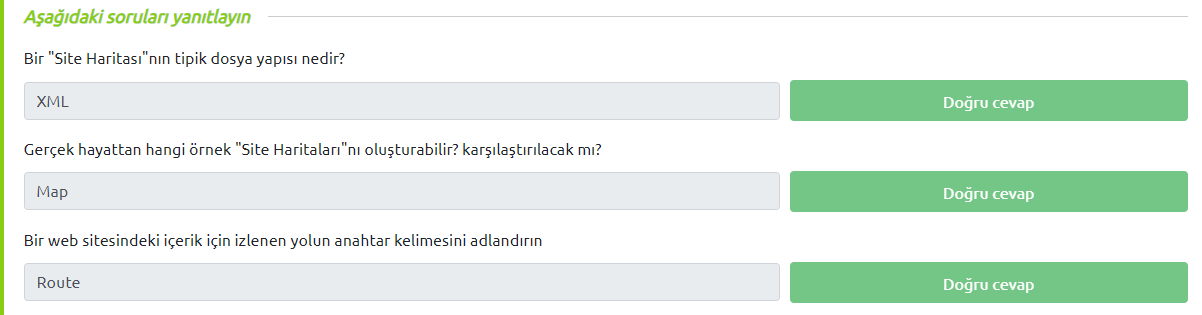




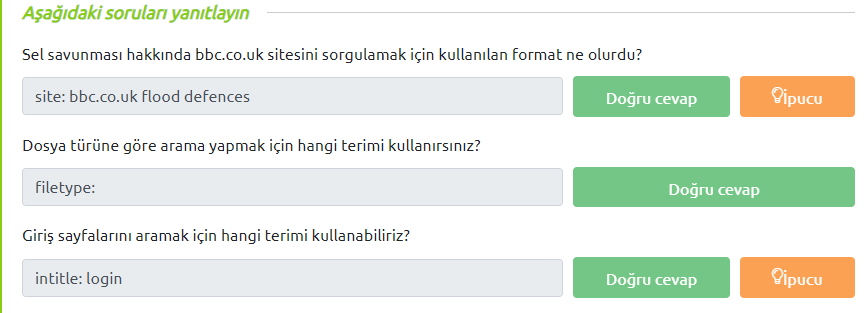
Görsel 16Dorking task 2 cevap



Görsel 17 dorking task4 cevap



Görsel 18 dorking task 5 cevap



Görsel 19 dorking task 6 cevap

**1.8. Cryptography for Dummies Çözümleme**

Kriptografi, bilgiyi koruma, gizleme ve güvenli bir iletişim sağlama amacıyla kullanılan matematiksel ve algoritmik yöntemleri inceleyen bir bilim dalıdır. Kriptografi, gizli mesajların üçüncü tarafların anlamasını engellemek için tasarlanmıştır ve genellikle bilgi güvenliği, iletişim güvenliği ve bilgisayar güvenliği alanlarında kullanılır.

Kriptografinin temel kavramları:

**Şifreleme (Encryption):** Bilginin anlamını değiştirme işlemidir. Açık metni (plaintext) bir şifreleme algoritması kullanarak şifrelenmiş metne (ciphertext) dönüştürür. Şifreleme, bilginin gizliliğini korumak için kullanılır.

**Deşifreleme (Decryption)**: Şifreli metni (ciphertext) kullanarak orijinal açık metni (plaintext) elde etme işlemidir. Doğru anahtarla deşifreleme işlemi gerçekleştirilir.

**Anahtar (Key):** Şifreleme ve deşifreleme işlemlerinde kullanılan matematiksel parametredir. Şifreleme algoritmasının güvenliği genellikle kullanılan anahtarın güvenliğiyle ilişkilidir.

**Simetrik Şifreleme (Symmetric Encryption**): Aynı anahtarın şifreleme ve deşifreleme işlemlerinde kullanıldığı bir şifreleme yöntemidir.

**Asimetrik Şifreleme (Asymmetric Encryption):** Farklı anahtar çiftleri kullanılarak, bir anahtarın şifreleme için kullanılması, diğer anahtarın ise deşifreleme için kullanılması esasına dayanır.

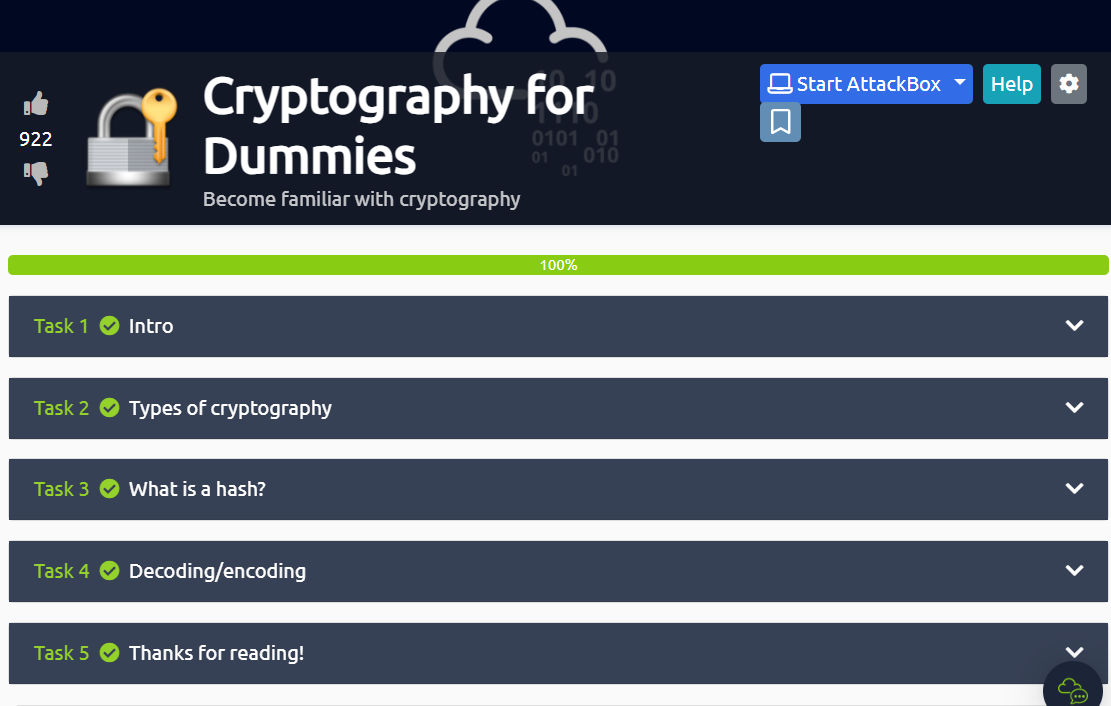
**Hash Fonksiyonları:** Verilerin belli bir sabit boyutta özete dönüştürülmesini sağlar. Hash fonksiyonları genellikle şifreleme amacı gütmeyip, bütünlük kontrolü için kullanılır.

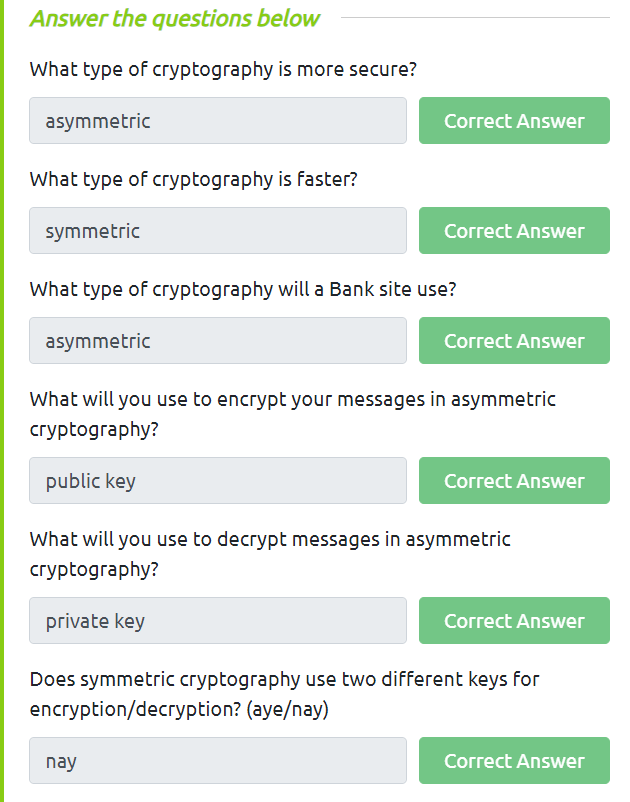
**Dijital İmza (Digital Signature):** Verilerin doğruluğunu ve bütünlüğünü sağlamak amacıyla kullanılır. Açık anahtarlı şifreleme kullanılarak oluşturulur.

**SSL/TLS Protokolleri**: İnternet üzerinde güvenli iletişim sağlamak için kullanılan protokollerdir. Web tarayıcıları ile web sunucuları arasındaki iletişimde sıkça kullanılırlar.

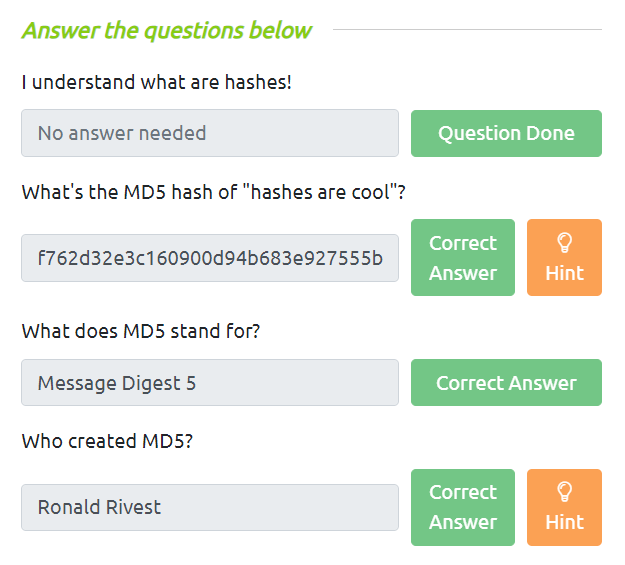
Kriptografi, günümüzde siber güvenlik alanında kritik bir rol oynamaktadır. Gizlilik, bütünlük ve kimlik doğrulama gibi temel güvenlik prensiplerini korumak amacıyla kullanıcıların ve sistemlerin verilerini güvenli bir şekilde iletişim kurmalarına olanak tanır.

**Cryptography for Dummies Cevapları**

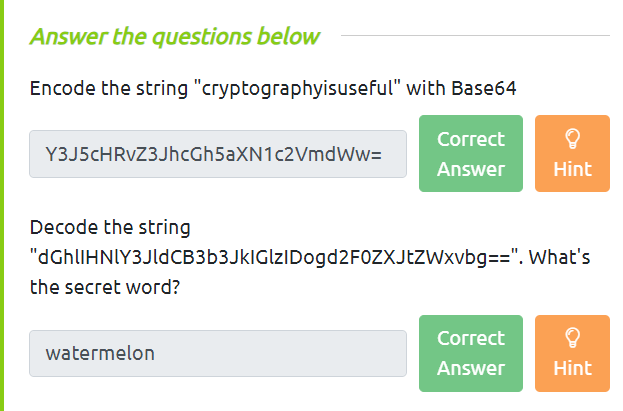




Görsel 20 task 2 cevap



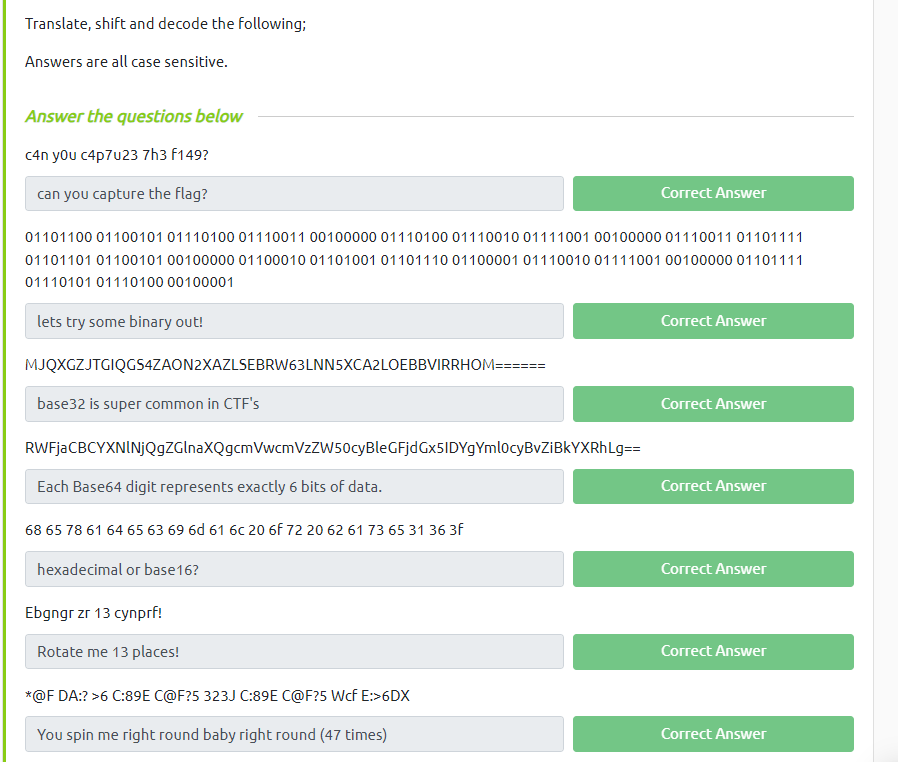
Görsel 21 task 3 cevap



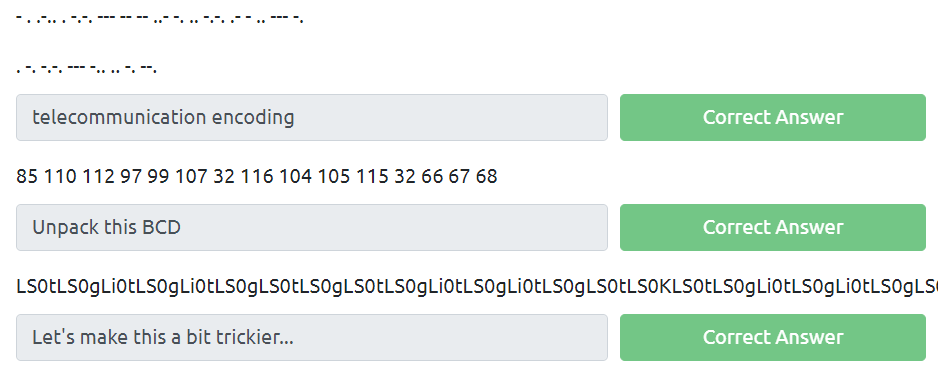
Görsel 22 task 4 cevap

**1.9. c4ptur3-th3-fl4g Çözümleme**

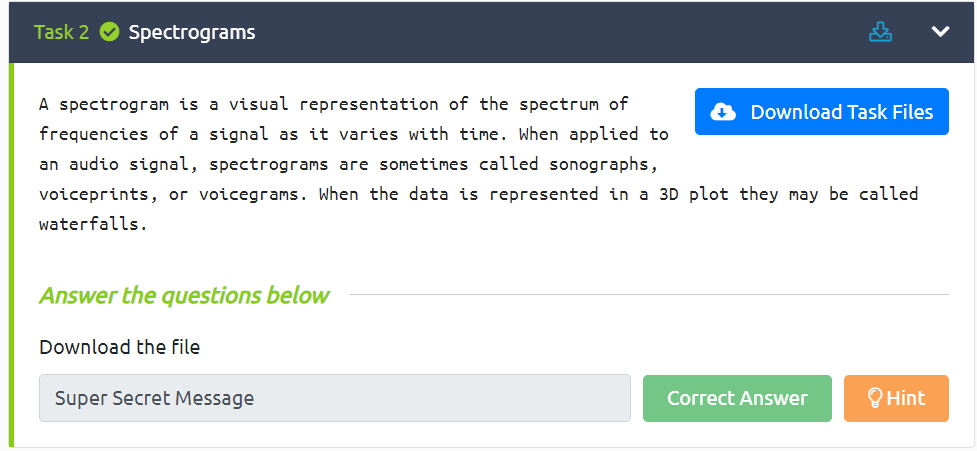
Bu odada şifrelenmiş metinleri farklı şifreleme algoritmaları kullanarak çözümlenmesi sağlanmıştır.



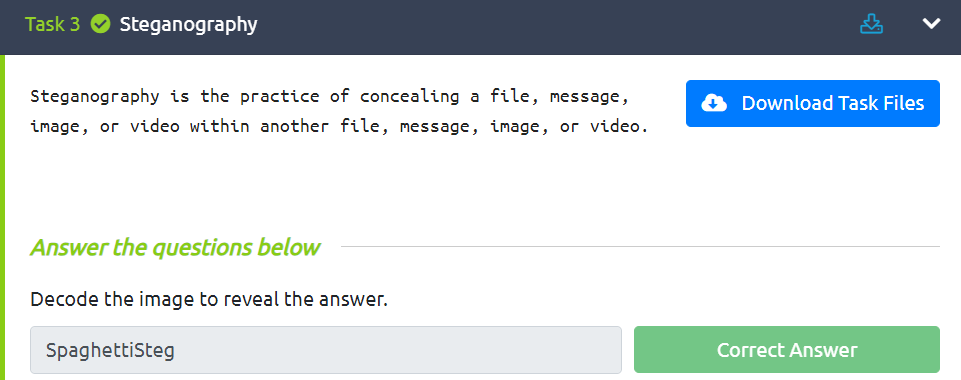
Görsel 23 task 1 cevap



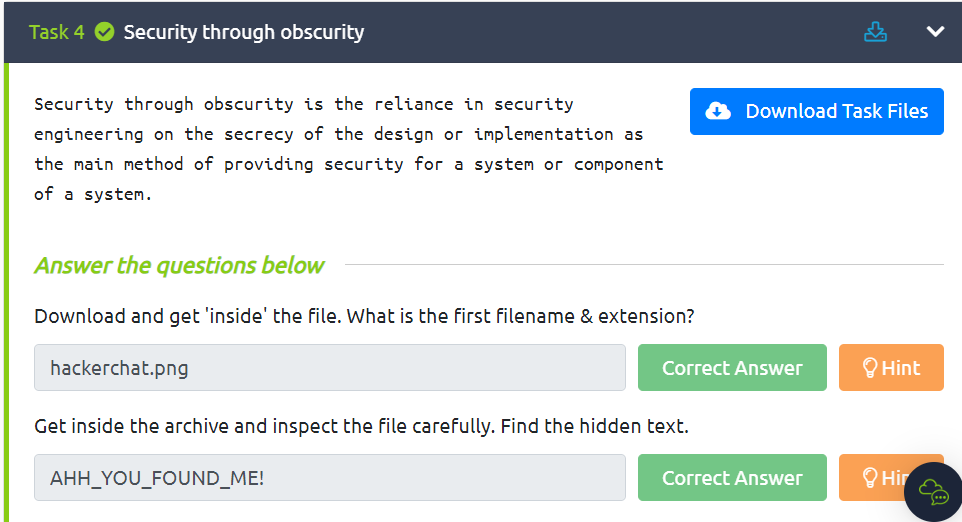
Görsel 24 task 1 cevap



Görsel 25 Task 2 Cevap



Görsel 26 Task 3 cevap



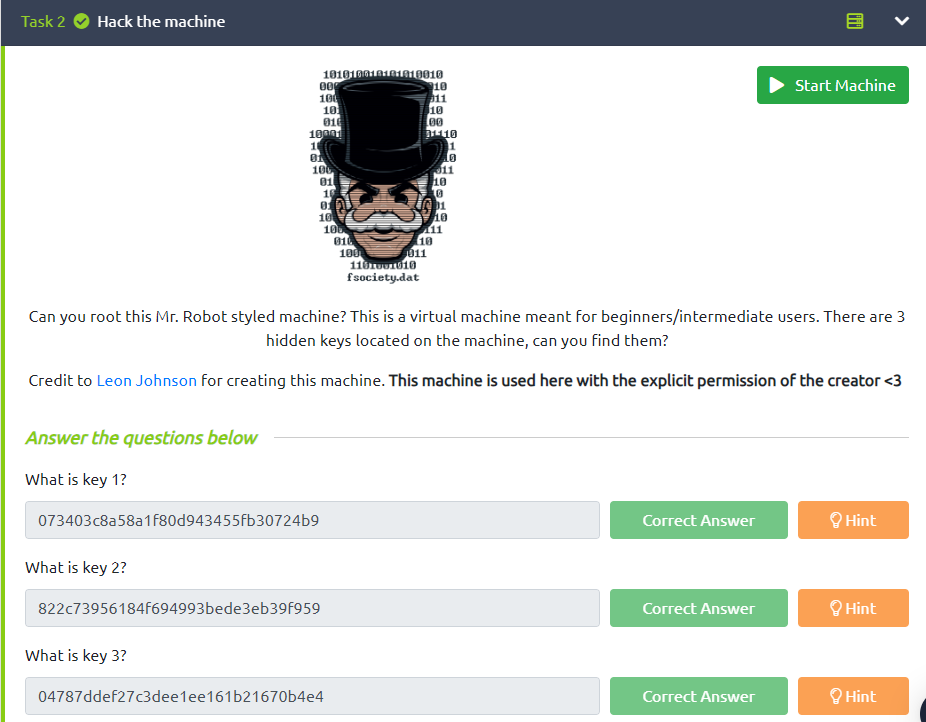
Görsel 27 Task 4 Cevap

**1.10. Mr Robot CTF Çözümleme**

Mr. Robot CTF, "Capture The Flag" (CTF) yarışmalarının bir örneğidir ve "Mr. Robot" adlı bir televizyon dizisine dayanmaktadır. CTF yarışmaları, siber güvenlik ve bilgisayar güvenliği becerilerini geliştirmek amacıyla düzenlenen etkinliklerdir. Katılımcılar, belirli bir süre boyunca çeşitli güvenlik zorluklarını çözmeye çalışarak bayrakları ("flags") ele geçirmeye çalışırlar.

Mr. Robot CTF, dizinin temalarını ve senaryosunu kullanarak, katılımcılara dizideki karakterlerin veya olayların izini sürme, güvenlik açıklarını tespit etme ve sistemlere erişme gibi görevleri çözmeleri için bir platform sağlar. Bu tür CTF'ler genellikle sanal makineler, web uygulamaları, ağ güvenliği sorunları ve siber güvenlikle ilgili diğer konuları içerir.

Katılımcılar, güvenlik zafiyetlerini tespit etmek, sistemlere yetkisiz erişim sağlamak ve genel olarak bilgisayar güvenliği becerilerini geliştirmek amacıyla farklı görevleri tamamlamaya çalışırlar. CTF'ler genellikle güvenliğe ilişkin konuları öğrenmek ve uygulamak isteyen siber güvenlik uzmanları, etik hackerlar, öğrenciler ve meraklılar için eğlenceli ve öğretici bir ortam sunar.



Görsel 28 Mr robot ctask 2 cevap

**Kaynakça**

[**https://tryhackme.com/room/mrrobot**](https://tryhackme.com/room/mrrobot)

[**https://tryhackme.com/room/c4ptur3th3fl4g**](https://tryhackme.com/room/c4ptur3th3fl4g)

[**https://tryhackme.com/room/basicpentestingjt**](https://tryhackme.com/room/basicpentestingjt)

[**https://tryhackme.com/room/vulnversity**](https://tryhackme.com/room/vulnversity)

[**https://tryhackme.com/room/googledorking**](https://tryhackme.com/room/googledorking)

[**https://tryhackme.com/room/openvpn**](https://tryhackme.com/room/openvpn)

[**https://tryhackme.com/room/torforbeginners**](https://tryhackme.com/room/torforbeginners)

[**https://tryhackme.com/room/furthernmap**](https://tryhackme.com/room/furthernmap)

[**https://tryhackme.com/room/metasploitintro**](https://tryhackme.com/room/metasploitintro)