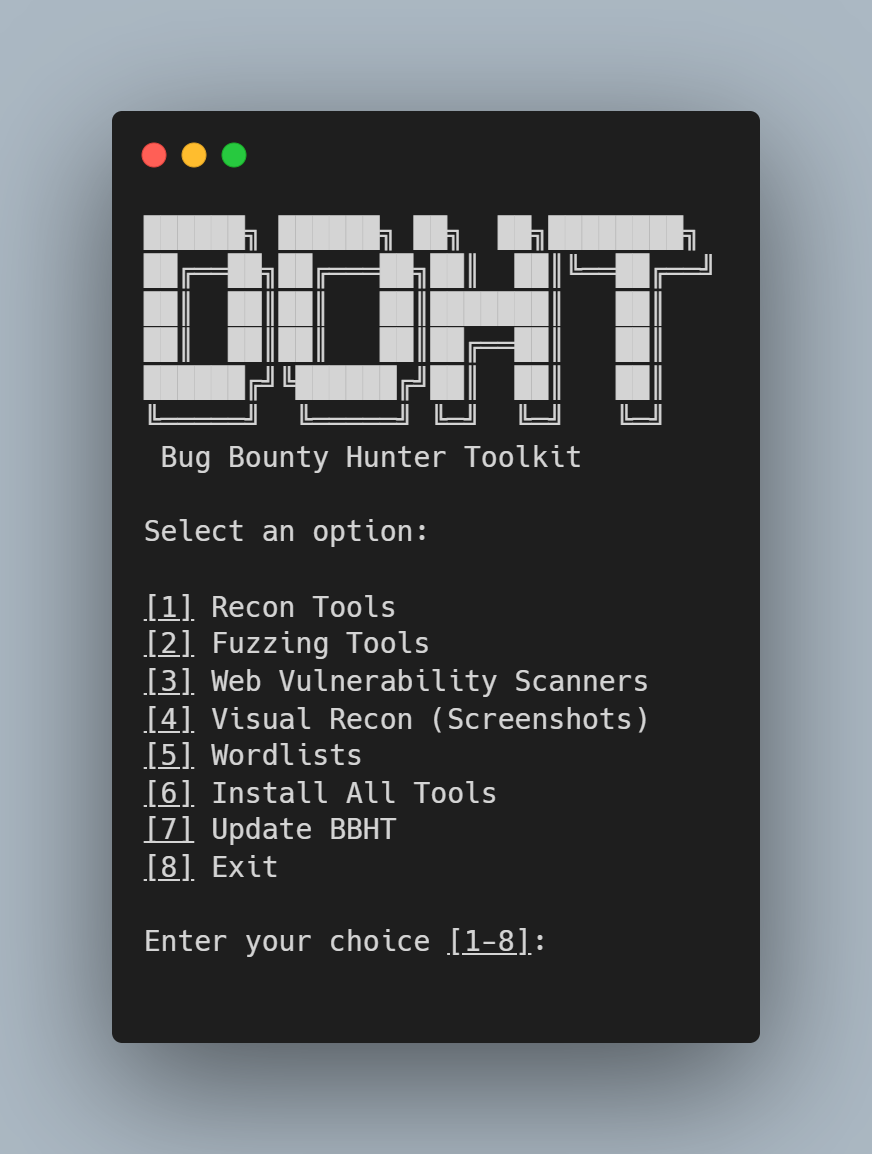
**BBHT (Bug Bounty Hunter Toolkit) Nedir?**

BBHT, adından da anlaşılacağı gibi bir Bug Bounty avcısının tüm temel ihtiyaçlarını tek bir noktada toplayan bir araç setidir. Terminal tabanlı, Bash ile yazılmış bu araç; hedef keşfi, dizin tarama, parametre analizi, subdomain keşfi, port tarama ve daha fazlasını bütünleşmiş bir şekilde sunar. Öğrenciler için birden fazla siber güvenlik aracını öğrenmek ve kullanmak açısından mükemmel bir başlangıç sunar.



**BBHT’nin İçerdiği Araçlar**

BBHT aslında tek başına bir araç değil, **birden fazla popüler güvenlik aracını entegre bir şekilde kullanan bir betik setidir**. Arka planda şu araçlar çalıştırılır:

* **Amass, Assetfinder** → Subdomain keşfi
* **Nmap** → Servis ve port tarama
* **Dirsearch, Gobuster** → Dizin ve endpoint tarama
* **HTTPX** → Canlı host tespiti
* **GF (Grep for Patterns)** → Parametre arama, XSS/SQL gibi zafiyet şablonları
* **Nuclei** → Otomatik zafiyet tarayıcısı
* **Waybackurls** → Arşivlenmiş endpoint bulma
* **Subjack** → Subdomain takeover kontrolü

Bu sayede öğrencilere birden fazla aracı ayrı ayrı kurmak ve çalıştırmak yerine, **tek script ile kombine güvenlik testi yapma imkânı** sunar.

**BBHT Ne İşe Yarar?**

BBHT, tek bir script ile aşağıdaki görevleri yerine getirebilir:

* Subdomain keşfi
* Hedef bilgi toplama (whois, DNS sorguları, vs.)
* Dizin ve endpoint keşfi (dirsearch, ffuf, vs.)
* Parametre analizi ve XSS gibi zafiyet kontrolleri
* Hedef uygulama üzerinde temel güvenlik taramaları

Kurulum: **git clone https://github.com/nytr0gen/BBHT.git && cd BBHT && ./bbht.sh**

**Kullanım Örneği**

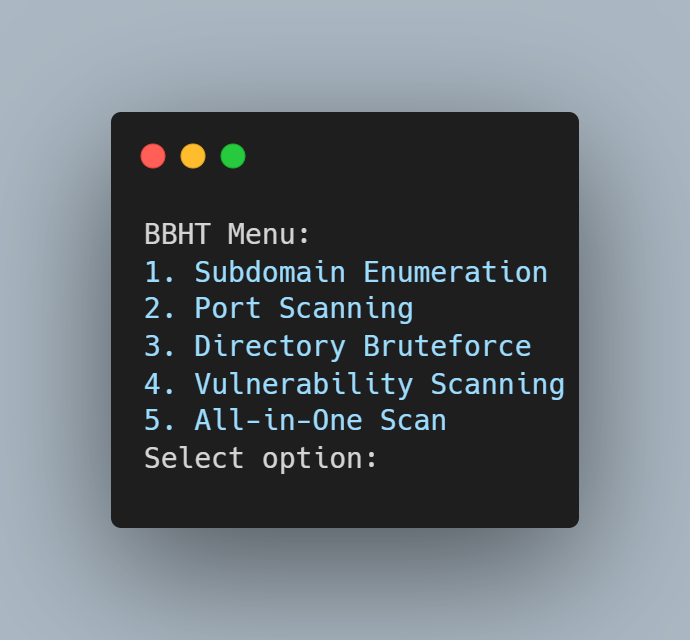
Kurulumdan sonra aracı çalıştırmak oldukça basittir:

**git clone https://github.com/nahamsec/bbht.git**

**cd bbht**

**./bbht.sh**

Arayüz açıldığında size şu tarz bir menü sunulur: Buradan öğrenciler diledikleri adımı seçerek hedeflerine göre özelleştirilmiş testler yapabilir.



BBHT, sadece bir araç seti olmakla kalmayıp, aynı zamanda pentest sürecinde izlenecek adımlar için rehber niteliği taşır. İçerisindeki araçlar sıralı ve mantıklı bir akışla çalıştırıldığı için, kullanıcılar adım adım keşiften başlayarak zafiyet taramasına kadar ilerleyebilir. Bu yapı, özellikle siber güvenlik eğitimi alan öğrencilerin gerçek dünya senaryolarını kavramalarını kolaylaştırır ve test süreçlerini sistematik hale getirir. Böylece, BBHT hem başlangıç seviyesindekiler için öğrenme aracı hem de deneyimli uzmanlar için hızlı bir iş akışı sağlar.