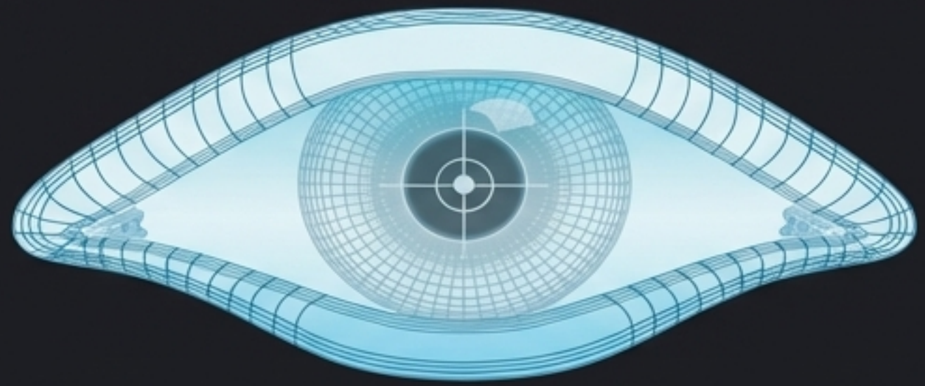
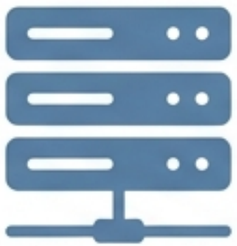


Nmap (Network Mapper) Rehberi

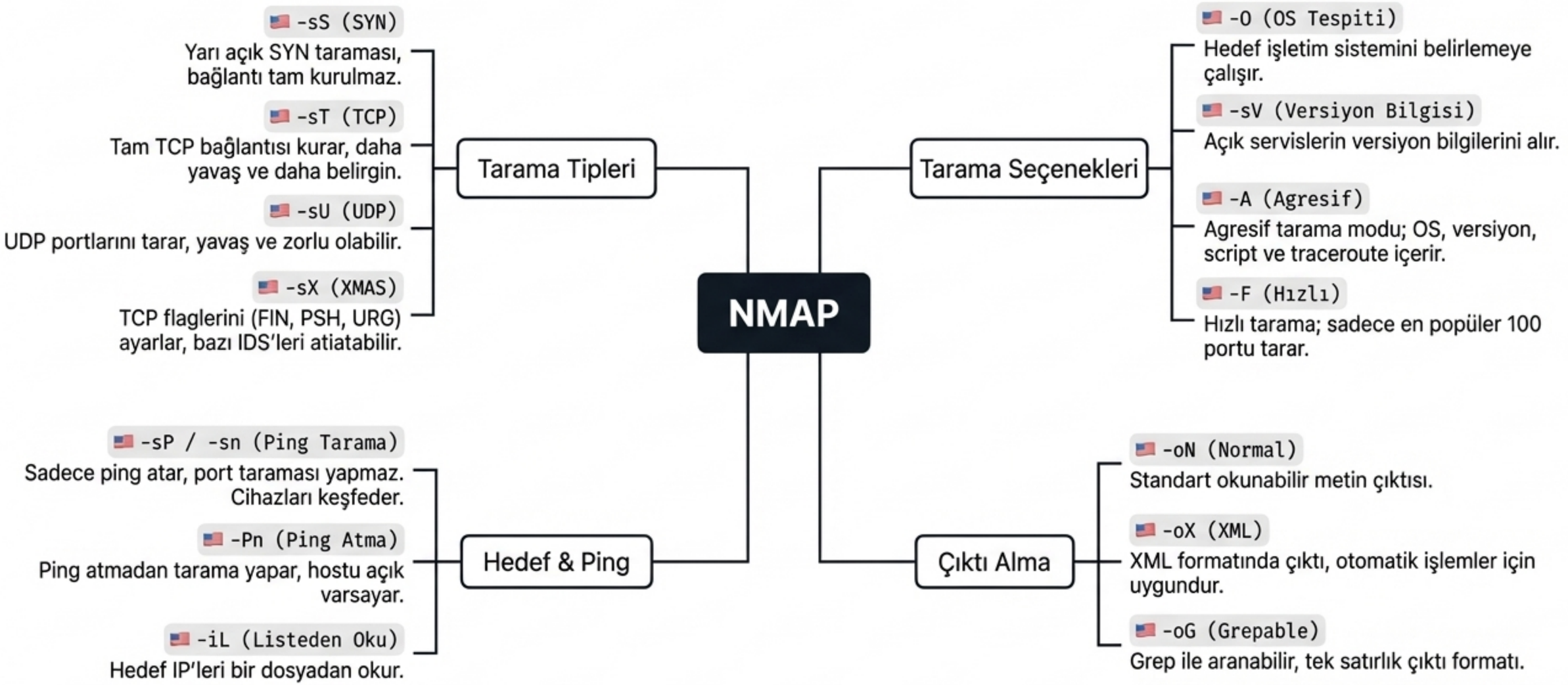
Ağ Keşfi ve Güvenlik Denetimi İçin Endüstri Standardı

Nmap Nedir?

Ağ üzerindeki cihazları keşfetmek, açık portları bulmak ve güvenlik risklerini tespit etmek için kullanılan açık kaynaklı bir güvenlik aracıdır. Özel olarak oluşturulmuş IP paketleri kullanarak hedef sistemleri analiz eder.

			
Güvenlik Değerlendirmesi	İzinsiz Giriş Tespiti	Envanter Yönetimi	Ağ Sorun Giderme

Nmap Ekosistemi



Nmap'in Temel Yetenekleri

1.

Ağ Keşfi (Host Discovery)

Ağda hangi cihazların aktif olduğunu (IP ve MAC adresleri) belirler.

2.

Port Tarama (Port Scanning)

Hedef sistemlerdeki açık portları ve iletişim durumlarını listeler.

3.

Versiyon ve İşletim Sistemi

Çalışan servislerin adını, sürümünü ve cihazın işletim sistemini (nmap-os-db kullanarak) tespit eder.

4.

Nmap Scripting Engine (NSE)

Zafiyet taraması ve gelişmiş ağ keşfi için Lua tabanlı otomasyon sağlar.

Port Tarama ve Durum Analizi

Nmap portları sadece açık veya kapalı olarak sınıflandırmaz; durumlara göre çok daha hassas bir analiz sunar.

Açık (Open)

Hedef makinedeki bir uygulama bu port üzerinden gelen bağlantıları aktif olarak dinliyor.

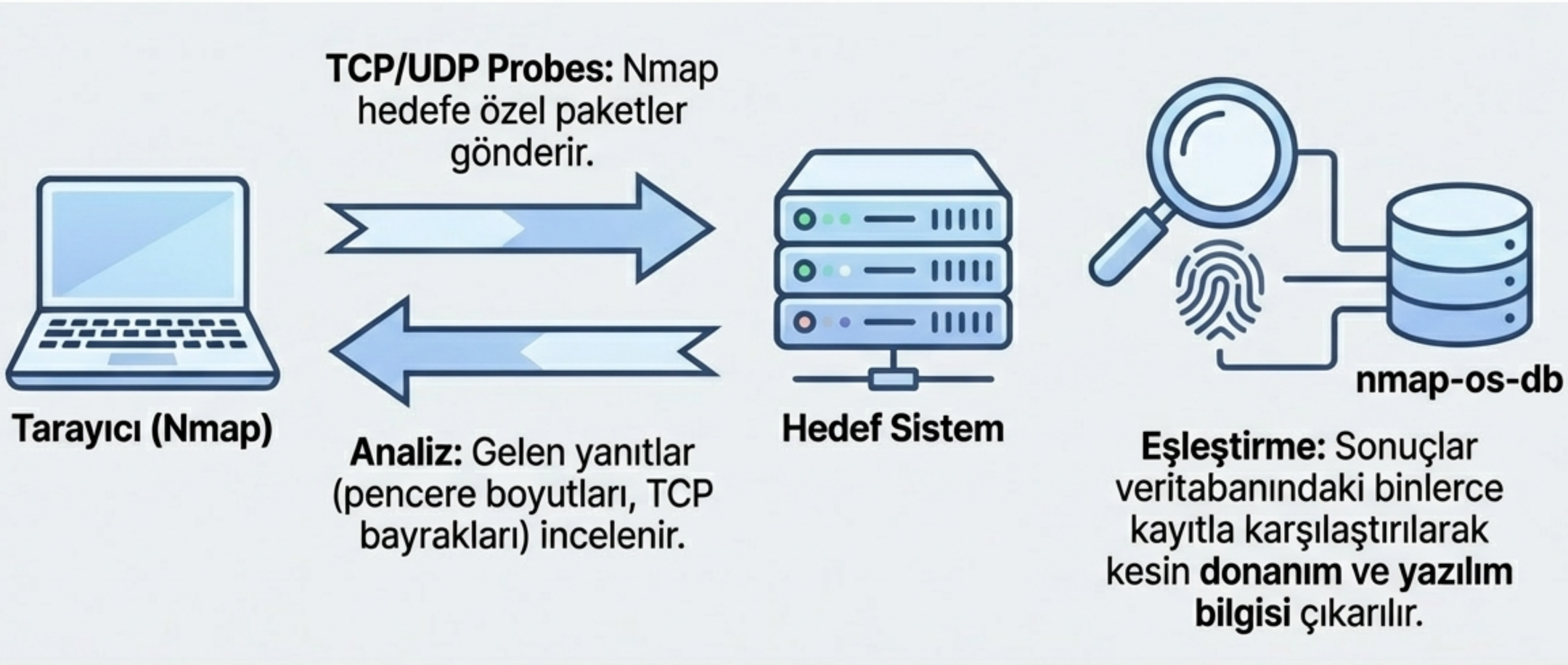
Kapalı (Closed)

Port erişilebilir ancak üzerinde dinleyen hiçbir uygulama yok.

Filtrelenmiş (Filtered)

Araya giren bir güvenlik duvarı (firewall) paketleri engelliyor; Nmap portun durumunu kesin olarak belirleyemiyor.

Derinlemesine Analiz: İşletim Sistemi ve Versiyon



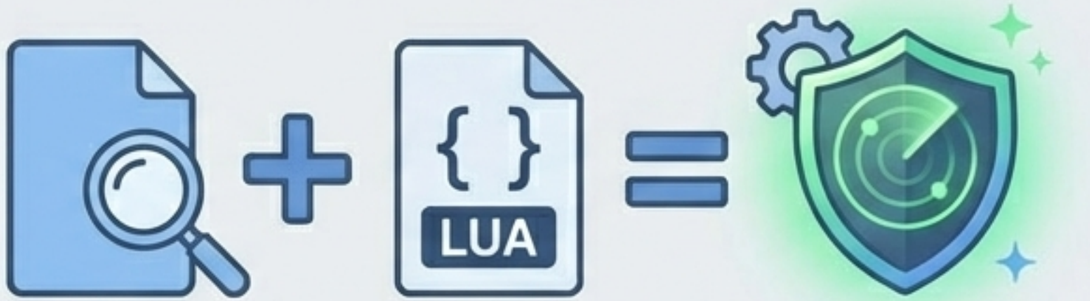
Nmap Scripting Engine (NSE)

Nmap'in en güçlü ve esnek özelliklerinden biridir. Lua programlama dili kullanılarak yazılan betikler sayesinde standart taramalar otomatikleştirilmiş güvenlik denetimlerine dönüşür.

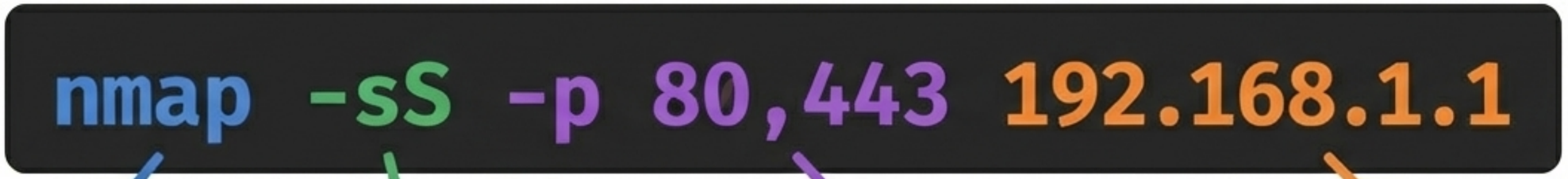
- Ağ keşfini detaylandırır (Örn: NetBIOS isimleri, SMB paylaşımları).

- Bilinen zafiyetleri (vulnerabilities) otomatik tespit eder.

- --script parametresi ile çalıştırılır.



Komut Anatomisi



[Ana Komut]: Aracı başlatır.

[Tarama Tipi]: Hangi tarama tekniğinin kullanılacağını belirler (Örn: SYN Scan).

[Seçenekler]: Portlar, hız şablonları veya veya ekstra filtreler.

[Hedef]: Tek bir IP, domain veya bir alt ağ (/24).

Temel Ağ Keşfi (Host Discovery)

Belirli bir ağda hangi cihazların aktif olduğunu port taraması yapmadan hızlıca bulmak için kullanılır.

```
> nmap -sn 192.168.2.0/24
Host 192.168.2.1 appears to be up.
MAC Address: 00:14:6C:19:F8:45 (Netgear)

Nmap done: 256 IP addresses (3 hosts up) scanned in 1.281 seconds
```

💡 Pro Tip: İstemediğiniz hedefleri taramadan çıkarmak için **--exclude** parametresini kullanabilirsiniz.

En Popüler Tarama: SYN Stealth Scan

Varsayılan ve en popüler port tarama yöntemidir. Hızlıdır ve TCP bağlantısını tam olarak tamamlamadığı (Half-open) için birçok güvenlik duvarında iz bırakmadan çalışır (Root yetkisi gerektirir).

```
> nmap -sS 10.0.0.1

PORT      STATE   SERVICE
22/tcp    open    ssh
80/tcp    open    http
443/tcp   closed  https
```

Hedef ve Port Belirleme

`nmap -p 80,443 192.168.1.1`	Belirli Portları Tarama: Sadece HTTP (80) ve HTTPS (443) portlarını kontrol eder.
`nmap -p 1-1000 192.168.1.1`	Port Aralığı Tarama: 1 ile 1000 arasındaki tüm portları tarar.
`nmap -F 192.168.1.1`	Hızlı Tarama (Fast Scan): Nmap'in veritabanındaki en popüler 100 portu hızlıca tarar.

Versiyon ve İşletim Sistemi Tespiti

Portun açık olması yeterli değildir; arkasında hangi yazılımın ve versiyonun çalıştığını bilmek zafiyet yönetimi için kritiktir.

```
> nmap -sV -O scanme.nmap.org

22/tcp open  ssh     OpenSSH 4.3 (protocol 2.0)
80/tcp open  http    Apache httpd 2.2.2 ((Fedora))

Device type: general purpose
Running: Linux 2.6.X
```

Agresif Tarama ve Hız Şablonları

-A Parametresi

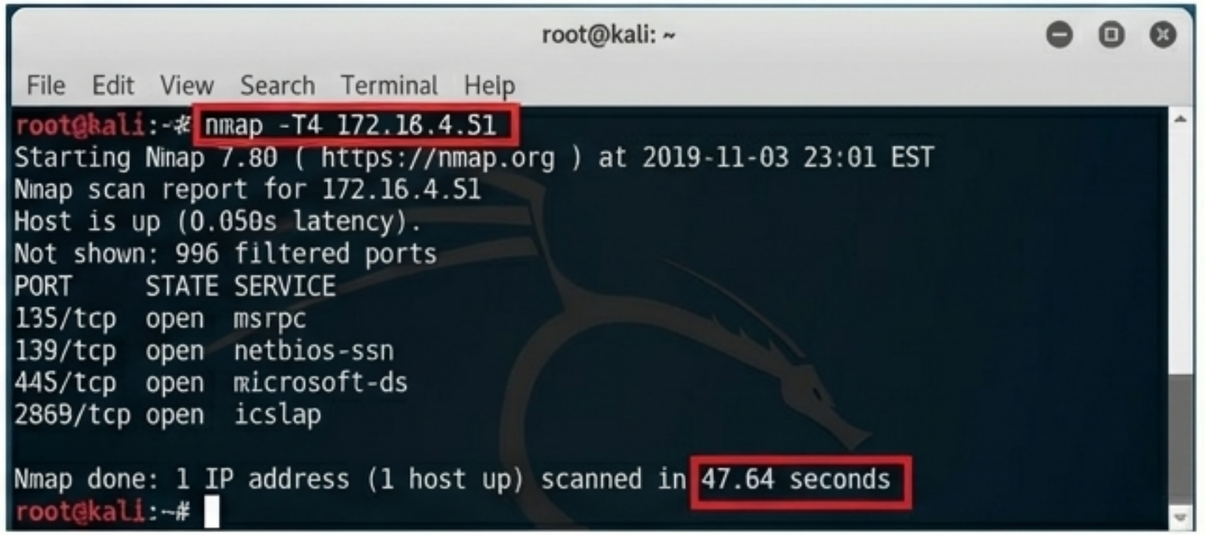
`nmap -A <hedef>`

İşletim sistemi tespiti (-O), Versiyon tespiti (-sV), Script taraması (-sC) ve Traceroute işlemlerinin tümünü tek komutta yapar.

-T Parametresi

`nmap -T4 <hedef>`

Hız seviyeleri -T0 (Çok Yavaş) ile -T5 (Çok Hızlı) arasında değişir. -T4 kurumsal ağlarda hız ve güvenilirlik için ideal standarttır.



Sonuçları Kaydetme ve Çıktı Alma

Taramaları ekranda izlemek yerine kaydetmek, diğer güvenlik araçlarıyla entegrasyon sağlamak için gereklidir.

`nmap -oN rapor.txt <hedef>`

Normal Çıktı: Ekranda görünen okunabilir metin formatı.

`nmap -oX rapor.xml <hedef>`

XML Çıktı: Yazılımlar ve otomasyon araçları tarafından kolayca ayrıştırılabilir format.

`nmap -oG rapor.txt <hedef>`

Grepable Çıktı: Linux komut satırı araçlarıyla (grep/awk) arama yapmak için tek satırlık veri.

Özet ve Etik Kullanım

- Nmap; ağ envanteri, güvenlik denetimi ve sorun giderme için vazgeçilmez bir standarttır.

- Doğru komut kombinasyonları (-sS, -sV, -O, -A) ağınızın tam anatomisini ortaya çıkarır.

Etik Kullanım Uyarısı

Nmap güçlü bir güvenlik aracıdır. Yalnızca sahibi olduğunuz veya taramak için açık yasal izin aldığınız ağlarda kullanın. İzinsiz taramalar yasa dışı kabul edilebilir.

Ağınızı güvence altına almak, onu tam olarak haritalandırmakla başlar.