NMAP

Bazı durumlarda, taramanın tamamlanması veya ekranda görüntülenecek herhangi bir çıktının üretilmesi çok uzun zaman alabilir. Ayrıca, bazen tarama ilerlemesi hakkında daha gerçek zamanlı bilgilerle ilgilenebilirsiniz.

Neler olup bittiği hakkında daha fazla güncelleme almanın en iyi yolu, **-v** ekleyerek ayrıntılı çıktıyı etkinleştirmektir.

Aşağıda sunulan ayrıntı miktarı, özellikle Nmap'i öğrenirken ve farklı seçenekleri keşfederken çok faydalı olabilir. Nmap'in bir aşamadan diğerine nasıl geçtiğini görebiliriz: ARP ping taraması, paralel DNS çözümlemesi ve son olarak her canlı sunucu için SYN gizli taraması.

```
root@tryhackme:~# nmap 192.168.139.1/24 -v
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-13 19:01 EEST
Initiating ARP Ping Scan at 19:01
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 19:01, 7.94s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:01
Completed Parallel DNS resolution of 1 host. at 19:02, 13.00s elapsed
Nmap scan report for 192.168.139.0 [host down]
Nmap scan report for 192.168.139.2 [host down]
[...]
Nmap scan report for 192.168.139.253 [host down]
Nmap scan report for 192.168.139.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 19:02
Completed Parallel DNS resolution of 1 host. at 19:02, 0.05s elapsed
Initiating SYN Stealth Scan at 19:02
Scanning 192.168.139.254 [1000 ports]
[...]
Initiating SYN Stealth Scan at 19:02
Scanning g5000 (192.168.139.1) [1000 ports]
Discovered open port 902/tcp on 192.168.139.1
Completed SYN Stealth Scan at 19:02, 0.03s elapsed (1000 total ports)
Nmap scan report for g5000 (192.168.139.1)
Host is up (0.0000090s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE
902/tcp open  iss-realsecure
```

Büyük ihtimalle, ayrıntılı çıktılar için ***-v*** seçeneği fazlasıyla yeterlidir; ancak yine de tatmin olmazsanız, ***-vv*** veya hatta ***-vvvv*** gibi başka bir "v" ekleyerek ayrıntı seviyesini artırabilirsiniz.

Ayrıca, ayrıntı düzeyini doğrudan belirtebilirsiniz, örneğin **-v2** ve **-v4**. Tarama başladıktan sonra ***"v" tuşuna basarak*** ayrıntı düzeyini artırabilirsiniz.

Eğer tüm bu ayrıntılar ihtiyaçlarınızı karşılamıyorsa, hata ayıklama düzeyinde çıktı için ***-d*** seçeneğini göz önünde bulundurmalısınız.

Benzer şekilde, bir veya daha fazla “d” ekleyerek veya hata ayıklama seviyesini doğrudan belirterek hata ayıklama seviyesini artırabilirsiniz. ***Maksimum seviye -d9'***dur; bunu seçmeden önce binlerce bilgi ve hata ayıklama satırına hazır olduğunuzdan emin olun.

Tarama Raporunun Kaydedilmesi

Çoğu durumda, tarama sonuçlarını kaydetmemiz gerekir. Nmap bize çeşitli biçimler verir. En kullanışlı üçü

1. Normal (insan dostu) çıktı,
2. XML çıktısı ve
3. grep komutuna referansla grepable çıktıdır.

Tarama raporu formatını aşağıdaki gibi seçebilirsiniz:

`-oN <filename>`	Normal Çıktı
`-oX <filename>`	XML Çıktısı
`-oG <filename>`	grep özellikli çıktı (grep ve awk için kullanışlıdır)
`-oA <basename>`	Tüm önemli formatlarda çıktı

Aşağıdaki terminalde, –oA seçeneğinin kullanımına dair bir örnek görebiliriz. Bu, normal, XML ve grep'lenebilir çıktı için nmap, xml ve gnmap uzantılı üç raporla sonuçlandı.

```
root@tryhackme:~# nmap -sS 192.168.139.1 -oA gateway
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-13 19:35 EEST
Nmap scan report for g5000 (192.168.139.1)
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE
902/tcp open  iss-realsecure

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
# ls
gateway.gnmap  gateway.nmap  gateway.xml
```