# Network Scanning 1

- قبل ما اعمل اي attack علي اي ip سواء machine او server لازم اعمل recon يعني اشوف الدنيا ايه البورتات المفتوحه عالسيرفر وبتعمل وايه اصدارها وكدا انت قبل ما تسرق بيت لازم تكون مجمع معلومات عنه صح؟ يعني لازم تكون عارف الاسره فيها كام فرد وفيها كام واحد شغال وبينزلو الشغل الساعه كام وبيرجعو الساعه كام وتشوف لو في شبابيك مفتوحه او بيبان مش مقفوله كويس وهكذا , نفس الكلام عندنا ف ال Pentest لازم تفحص الدنيا الاول
- احنا بقي هنستخدم اداتين مهمين جدا في عمليات الفحص وهقولك الفرق بينهم وتستخدم دي امتي ودي امتي
- هنستخدم اداة ال nmap وال masscan

---

## Port Scanning

### nmap (network mapper)

- عشان اعمل port scan لازم اكون حافظ البورتات المشهوره وبيكون مختصين لخدمة ايه بالظبط

```
<nmap <ip | domain
```

```
nmap scanme.nmap.org
```

- الامر ده بكل بساطه بيجبلك اول 1000 بورت مفتوحين علي الip ده والخدمات اللي عالبورتات دي ودول اهم 1000 بورت عمتا ولو عاوز تشيك علي كل البورتات عادي برضو بس 1000 دول كافيين جدا

.Pasted image 20250124025213.png” could not be found“

- دي كل البورتات المفتوحه بالخدمات بتاعتها علي السيرفر
- اول مثلا ما اشوف خدمة ال http اعرف اني ده سيرفر ويب

*طب افرض اني عاوز اعرف نوع الاصدار بتاع الservice دي؟*

- حد هيسأل نفسه لما اعرف الاصدار انا كدا استفدت ايه؟ اقولك لا انت هتستفاد كتير
- قبل ما اقولك هو هيفدنا ف ايه لازم نعرف هو ليه اصلا بيتم عمل تحديثات وترقيه للاصدار؟ عشان ببساطه المطورين بيعالجو ثغرات او مشاكل امنيه او بيضيفو ميزه معينه او بيصلحو مشكله تقنيه
- يعني معني كدا اني لو اصدار قديم شويه ممكن الاقي ثغره واستغلها؟ بالظبط اه ودي الفكرة من اني اعمل scan علي الاصدارات عشان ممكن لو اصدار قديم شويه تاخدو انت كوبي وتسرش عليه وتشوف لو ليه اي exploits

```
nmap google.com -sV
```

```
sV = service version
```

.Pasted image 20250124025754.png” could not be found“

- هنا اهو جابلك اصدار الservice وتبدأ انك تشوف لو هيا قديمه ولا دي اخر اصدار وتشوف لو كانت قديمه تشوف ليها اي استغلالات

### masscan

---

- مبدأيا الاداه دي حد عاملها وانت بتنزلها علي نسخة الكالي اللي عندك
- خلي بالك اني ال masscan هيا مختصه بالبورتات دي يعني nmap فيها حاجات تانيه غير البورتات هنعرفو قدام انما ال masscan مختصه بالبورتات بس والخدمات اللي شغاله عليها
- ميزة masscan انها سريعه

```
masscan -p1-65535 142.251.37.174 --rate=1000
```

- مبدأيا `p1-65535-` دي معناها اني بقولو افحصلي من اول بورت 1 لحد 65535
- `142.251.37.174` دا الip بتاع الموقع او الجهاز اللي عاوز اعمل عليه فحص خلي بالك انه هنا مينفعش تحط ال domain عكس ال nmap
- الـ `rate=1000` دي انت بتحدد السرعه هنا هو هيبعت 1000 باكيت فالثانيه الواحده وممكن ازودها وتبقي اسرع 10000 مثلا

---

## الفرق بين ال nmap وال masscan؟

### nmap

---

- بطيئه شويه بس نتايجها دقيقه ومفصله
- فيها مميزات تانيه مش بس البورتات
- الاكثر استخداما

### masscan

---

- سريعه جدا مقارنة مع ال nmap
- مختصه بس بالفحص علي البورتات والخدمات اللي شغاله عليها