Nmap belekse

Andrija Urosevic (HackLab)

Uvod

- Nmap (*Network Mapper*) je besplatan i 'open source' alat za istrazivanje mreze i sigurnosnu reviziju
- Koristi IP pakete da bi otkrio:
  - Koji hostovi su dostupni
  - koji operativni sistem se koristi
  - koji tipovi paketa filtera/firewall se koriste
  - i jos puno toga

Faze nmap skeniranja

- Nmap skeniranje radi u fazama i svaka faza pokrece sledecu:
  1. **Script per-scanning**
     - Nmap Scripting Engine (NSE) koristi specijalne skripte za prikupljanje informacija o udaljenim racunarima
     - NSE se ne pokrece ukoliko to nije zatrazeno `--script` ili `-sC`
  2. **Target enumeration**
     - Pretrazivanje hostova koje je korisnik specifikova
       - DNS imena, IP adrese ...
     - Prebacuje ih u listu IPv4 ili PIv6 adresa za skeniranje
     - Ova faza je neophodna
  3. **Host discovery (ping scanning)**
     - Skeniranje pocinje trazenjem mete koje su online na mrezi i tako pocinje dublje istrazivanje
     - Pokrece se uvek, ali je moguce preskociti je sa `-Pn` (ako su sve mete online)
  4. **Reverse-DNS resolution**
     - Kada zna koje hostove da skenira, trazi DNS imena svih hostova koji su online skeniranjem pinga
     - Moguce je preskociti ovu fazu sa `-n` (no resolution) ili povecati da pokrije sve IP mete `-R`
  5. **Port scanning**
     - Srz nmap skeniranja
     - Klasifikuje portove u stanja:
       - `open`, `closed`, ili `filtered`
     - Pokrece se uvek, ali je moguce preskociti ga sa `-sn`
  6. **Version detection**
     - Ako je neki od porotova otvoren, nmap moze da otkrije koji serverski sistem se koristi na udaljenom racunaru
     - Ova faza se pokrece sa `-sV`
  7. **OS detection**
     - Drugaciji operativni sistemi implementiraju mrezne standarde drugacijim nacinima.
     - Tako nmap moze da pronadje koji OS koristi host
     - Pokrece se sa `-O`
  8. **Traceroute**
     - Paralelno pronalazi rute ka mnogim hostovima
     - Omogucuje se sa `-traceroute`
  9. **Script scanning**
     - NSE skripte se pokrecu tokom ove faze.
     - Pokrecu se jednom za svaki host i port

   - Detektuju slabosti, malware discovery, sakupljaju vise informacija iz databaza i drugih mreznih servisa, i napredna version detection
   - Ne pokrece se ako se te ne zatrazi sa `--script` ili `-sC`
10. **Output**
   - Nmap smesti sve informacije koje je sakupio i zapise ih na ekran ili u neki file.
   - Pise informacije u nekoliko formata
     * Fortam citljiv za coveka (Human readable format)
     * XML izlaz
11. **Script post-scanning**
   - Izvrsava skripte koje korisnik ukljucuje

Legalni problemi

Da li je neovlasceno skeniranje portova zlocin?

- KOMPLEKSNO

Da li nmap skeniranje moze da srusi mrezu

- NE

Odrzavanje, Kompajliranje, Instaliranje Nmapa

- Nmap je podrzan za Linux, Windows i Mac OS X

Linux distros

- U zavisnosti od distribucije nmap se instalira drugacije
- Ima ga skoro u svim poznatim distribucijama

Host Discovery ("Ping Scanning")

- Host discovery se bavi nalazenjem odredjenog opsega IP-eva
- Zadrzava korisne, a odbacuje one koji nisu potrebni
  - Na osnovu toga koje servise host koristi itd.

Specifikovanje mete hostova i mreza

- Sve u komandnoj linije sto nije opcija (argument) je meta
  - U najjednostavnijem smislu to je IP adresa ili hostname

Input from list (`-iL`)

- Ako imamo na desetine, stotine IP adresa ili hostname-ova onda je nezgodno pisati ih u komandnu liniju
  - Zbog toga se svi oni smestaju u file koji sadrzi sve mete
  - U file-u se nalaze ulazi:
    - IP adresa, hostname, CIDR, IPv6, i octet range
  - Svaki ulaz mora biti odvojen razmakom/tabom/novom linijom
- Koristi argument `-iL <file_name>`

Choose Targets at Random (`-iR <numtargets>`)

- Za biranje mate nasumicno koristi se argument `-iR <numtargets>`
- `<numtargets>` je broj koliko meta generisati
  - za 0 skeniranje se nikada ne zavrsava

Excluding Targets (`--exclude`, `--excludefile <filename>`)

```
x = 5
for i in range(x):
    print(i)
```

```
## 0
## 1
## 2
## 3
## 4
```