PA2Q4

a) How does nmap work? (organizations, scripts, techniques....)

b) Explain how to perform portscan through firewalls (simple state filter).

c) Systematize how to map a network using nmap. What limitations? What can be obtained?

Video link from professor

Nmap portscan tutorial -> port-scanning-tutorial

Stealth Scan vs TCP Connect Scan // NMAP -sS -ST

What is a Port Scanner and How Does it Work?

---

a) How does nmap work ?

1. **Organizations**
   Origem: Wikipédia, a enciclopédia livre.

Nmap (Network Mapper) is a -open source- *network scannner* created by Gordon Lyon (also know by his pseudonym Fyodor Vaskovich). Nmap is used to discover **hosts** and **services** on a **computer network** by sending packets and analyzing the responses. É muito **utilizado para avalizar a segurança dos computadores, e para descobrir serviços ou servidores em uma rede de computadores.**
O Nmap é um programa CUI (Console User Interface), pelo que corre na linha de comandos, mas este tem uma interface gráfica (GUI), o **NmapFE** (Nmap Front End), que foi substituido pelo **Zenmap** em 11 de Outubro de 2007, por ser uma versão portátil e prover uma interface melhor para execução e especialmente para visualização e análise dos resulstados do **Nmap**.

- **Original author**: Gordon Lyon (Fyodor)
- **Plataform**: i386
- **Initial release**: September1997
- **Repository**: https://github.com/nmap/nmap.git
- **Written in**: C, C++, Lua, Python (GTK)
- **Operating System**: Windows, Mac OS X, Linux
- **License**: NPSL or modified, GPLv2 or proprietary, open-source
- **Website**: insecure.org/nmap

1. **Scripts**
    1.
2. **Techniques**
    1.
3. **More**
   Nmap features include:
    - Fast scan
    - Host discovery
    - Port scanning
    - Version detection
    - Ping Scan
    - TCP/IP stack fingerprinting
    - Scriptable interaction with the target
      Typical uses of Nmap:
    - Auditing the security of a device or firewall by identifying the network connection which can be made to, or through it.

- Identifying open ports on a target host in preparation for auditing.
- Network iventory, network mapping, maintance and asset management.
- Auditing the security of a network by identifying new servers.
- Generating treffic to hosts on a network, response analysis and response time measurement.
- Finding and exploiting vunerabilities in a network.
- DNS queries and subdomain search.