[Q]uantitative Project

The Road To Ethical Hacking

MercedCyber.tk

(5) TECHNICAL: INTRODUCING EVERYTHING NMAP

OCTOBER 25, 2018

WARNING

Before network scanning make sure you have explicitly written permission. Or else contact your local laywer.

!!!!!

Tell your kids, friends, family and mistress that may not be around.

Scanning over the internet

Note a crime

- Makes system administrators jobs harder.

Scanning the wrong machine

- There will be consequences

Create your own targets

scanme.nmap.org

Set up by nmap team.

- nmap scanme.nmap.org
  - simple scan

Service Version

- nmap –sV scanme.nmap.org

Why is knowing the version of software important?

How do system administrators defend against this.

- Simple, restrict service version.

Nmap does not scan every port, there are 65,535 ports.

Saving your scans.

nmap scanme.nmap.org –oA logbase

- Save as .xml
- .nmap
  - readable output
- .gnmap
  - grep-able nmpa

To Scan or Not To Scan (Range)

There are 65,535 ports

- Basic scans only scan top 1000 ports.
- System administrators run services on high ports
  - why?
  - Does this work?
    - No it does not work.

Scan specific port only , such as port 80

- nmap –p 80 scanme.nmap.org

Ranges (1 – 1024)

- nmap –p1-1024 scanme.nmap.org

[Q]uantitative Project

Thank You

RAMIRO GONZALEZ

RGONZALEZ69@UCMERCED.EDU