[Q]uantitative Project

MercedCyber.tk

The Road To Ethical Hacking

(6) TECHNICAL: INTRODUCING EVERYTHING NMAP

NOVEMBER 1, 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 you may not be around.

Vocabulary & Acronyms

DNS : Domain Name System

PING : Packet InterNet Groper

IP : Internet Protocol

LAN : Local Area Network

MAC: Media Access Control

No ping

MercedCyber.tk

Dead or Alive

Hiding systems

- Makes the jobs of attackers harder but not impossible
- A little more work

What is ping? (ICMP echo request)

- Tests whether the host is up. By sending a request.
- Disadvantages: A host may not send back the request.

Normal scans will not properly scan hosts.

- By default (Reverse DNS resolution [lookup]) * IP ✉Domain , is enabled
- use –n flag. to disable rDNS.

Dead or Alive

Regular Scan

- nmap 18.213.119.84
- Defaults: ping sweep ✉rDNS ✉ Scan ports
- DNS stand for Domain Name System
- nmap –n 18.213.119.84 (disable reverse DNS lookup)
- -n flag: ping sweep ✉ Scan ports
- Ports open 22/tcp, 80/tcp, 443/tcp (What is the server)

Dead or Alive

Flag: (Assuming host allow ping request)

- -sn (ping sweep)
- Ex: nmap –sn 18.213.119.84
- ping sweep ✉ rDNS , no port scan
- nmap –sn -n 18.213.119.84 (faster)
- ping sweep ✉ no rDNS , no port scan
- Supposed to give you “0 host up”

Flag: (host does not allow ping request)

- -Pn (no ping)
- Will also scan host that may not be up.
- Example No Flag: nmap   -n 18.213.119.84
  - (ping sweep) ✉ no rDNS ✉ Scanning ports *those that respond
- Example with Flag: nmap –pn –n 18.213.119.84
  - no ping sweep ✉ nor rDNS ✉ Scanning ports *No response

-sL flag List Scan

- -sL is useful for DNS look up
- nmap 18.213.123.154-159 –sL
  - recall 154-159 is the range. That is 18.213.123.154, 18.213.123.155.. 18.213.123.159
  - We scanned 6 IP addresses and 0 host are up.
    - This means two things.
      - Hosts do not accept ICMP echo request (ping)
      - Host do not exist or are not up
  - Result: compute-1.amazonaws
    - What does this mean? What is amazon aws

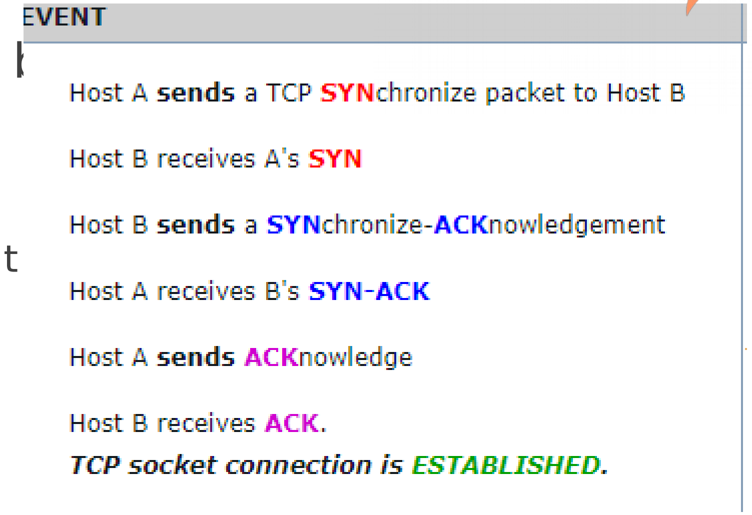
ICMP ping request | TCP SYN ping scan

Administrators may disable ICMP ping request

- This makes host seem as if they are down and will not b

TCP SYN ping scan

- Recall the three way handshake
  - We send a SYN request to a specific port, if it responds we assume it
  - FLAG: -PS
  - Example: -PS 22 (-P is ping, S is the method, combine them)
    - Recall 22 is the default port for Secure Shell (SSH)



EVENT
Host A **sends** a TCP **SYN**chronize packet to Host B
Host B receives A's **SYN**
Host B **sends** a **SYN**chronize-**ACK**nowledgement
Host A receives B's **SYN-ACK**
Host A **sends** **ACK**nowledge
Host B receives **ACK**. ***TCP socket connection is ESTABLISHED.***

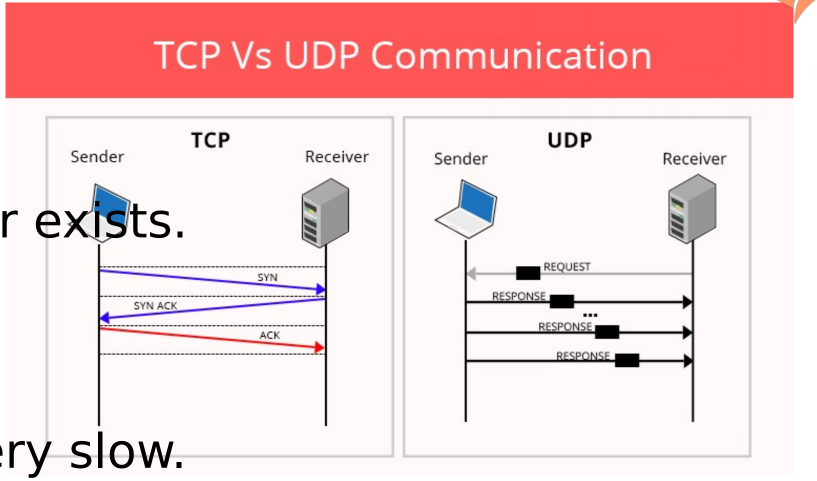
https://www.inetdaemon.com/tutorials/internet/tcp/3-way_handshake.shtml

UDP (User Datagram Protocol)

UDP is difficult to scan.

- It is connectionless communication
  - It sends packets without determining if the receiver exists.
    - No handshaking.
  - It does not care if (UDP packets) data is received.
  - Reduces latency (It is fast)

Always do TCP scans before UDP scans. UDP scans are very slow. You will be waiting for a while.



https://www.oodlestechnologies.com/blogs/Why-UDP-is-preferred-for-Live-Streaming

Who uses UDP?

- Who needs convenience but not quality?

-sU flag (Scanning User Datagram Protocol)

Example:

- sudo nmap –sU ocf.berkeley.edu –p123
  - We should by now know what sudo is.
  - running nmap with elevated privileges –sU is states we want to scan UDP ports
  - ocf.berkeley.edu is the name of our host
  - NOTE: rDNS is enabled. use –n to disable. (optional)
  - -p123 tells nmap we want to scan port 123

Results:

- ntp service (Network Time Protocol).
- It’s default port is 123, and is generally under UDP.
- Open|Filtered means it may or may not be allow public to connect.

MercedCyber.tk

How to not get caught

IDS (Intrusion Detection Systems)

- Can detect scans (SYN scans)

Using the following flags *Types of scans

The following will issue a (RST) packet, that is reset the connection.

- FIN (Spanish for “END”) (“Stop talking, just listen”)
  - FLAG: -sF
  - Example: sudo nmap –sF –n ocf.berkeley.edu –p80 --reason
  - -p80 (port 80, recall this is http by default)
  - --reason (states the method used to determine the state of the port)
  - RESULT: reset ttl 255 (ttl = time to live)
- Xmas Tress (May not be covered)
  - FLAG: -sX
  - https://nmap.org/book/man-port-scanning-techniques.html
- Null

“Can Sneak through non-stateful firewalls and packet filtering routers. “

Some IDS can detect them.

Can not distinguish between open| filtered

Operating System *Flag: -O

What is an Operating System?

“the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.”

We must identify our target.

- If we are scanning in the local lan, we can see the MAC address.
- media access control

What is fingerprinting?

- The size of your screen can be used to fingerprint.
- We want to know who created the device, what software can it run.
  - An attackers sends a windows malicious software to a macOS user or Linux user?

Example: nmap -O -n scanme.nmap.org

Dectect the operating system, disable reverse DNS look up.

Example: sudo nmap -n -Pn -O 18.213.119.84

Changing your MAC Address

Follow this instructions

https://www.howtogeek.com/192173/how-and-why-to-change-your-mac-address-on-windows-linux-and-mac/

Packet Tracing (Flag: --packet-trace)

Similar to traceroute

- The hops it takes to reach the target host.
- Recall that in order to reach your target host, the packets sent must travel through different hosts.
- If one of the intermediate host is down you will never reach your destination.
- This is a debugging tool (Find where there is an error)
- Packets may travel all over the nation or world before reaching the target.
- You can measure the delay.
  - Delay may tell you how far a host is, or how fast a connection is.

[Q]uantitative Project

Thank You

RAMIRO GONZALEZ

RGONZALEZ69@UCMERCE.EDU

RAMIROGONZALEZ.ORG

☎ 209-962-2524