

Network side channels

Outline

- Review of port scanning, idle scans
- Examples of network side channels
 - SYN backlogs and DoS
 - RST rate limitation
 - Off-path TCP hijacking
 - Blind in/on-path attacks

TCP 3-way handshake (review)

- SYN: I'd like to open a connection with you, here's my initial sequence number (ISN)
- SYN/ACK: Okay, I acknowledge your ISN and here's mine
- I ACK your ISN

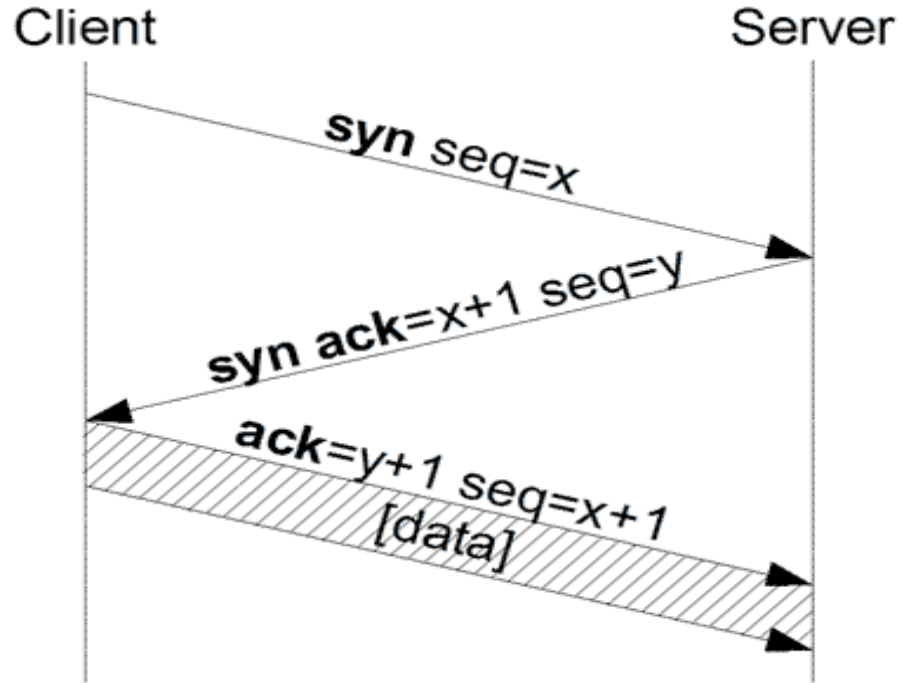


Image from Wikipedia

Open port == listening

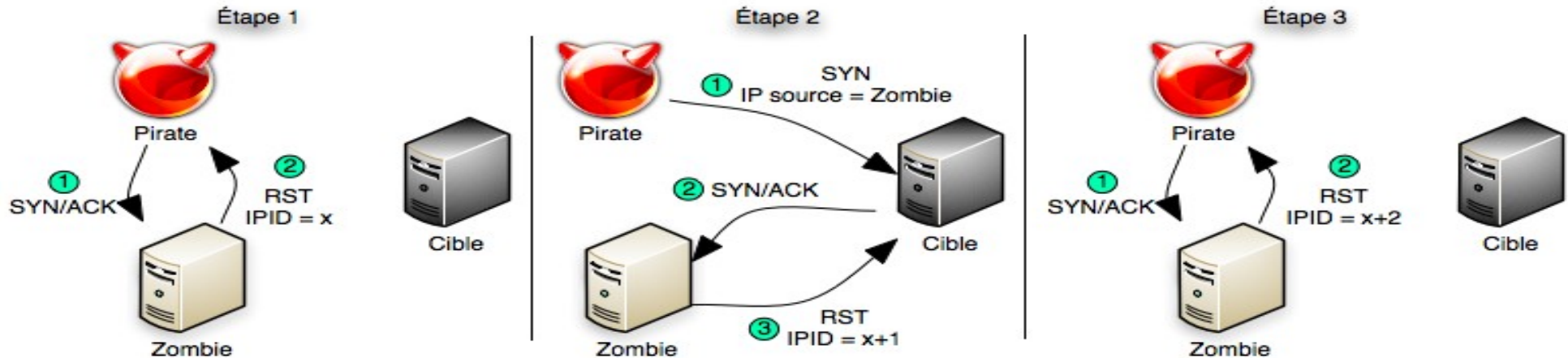
- If you send a SYN packet to port 80 (the HTTP port) on a remote host and that host replies with a SYN/ACK, then we say that port 80 on that machine is “open”
 - In this example, that probably means it's a web server
- If it responds with a RST, we say it's “closed”
- If there is evidence of filtering (no response or ICMP==Internet Control Message Protocol error), we say it's “filtered”
 - UDP is more complicated: open|filtered vs. closed

Things nmap can do

- Is a port open? Closed? Filtered?
 - Many ports on one machine is a “vertical scan”
- For a /24 network, which machines are up? Which machines have port 80 open?
 - One port for a range of machines is a “horizontal scan”
- OS detection (research on your own)
- Stealth, info about middleboxes, etc.

Idle scan

- Every IP packet sent has an IP identifier
 - In case it gets fragmented along the way
- Old and/or stupid machines use a globally incrementing IPID that is shared state for all destinations



Examples of network side channels

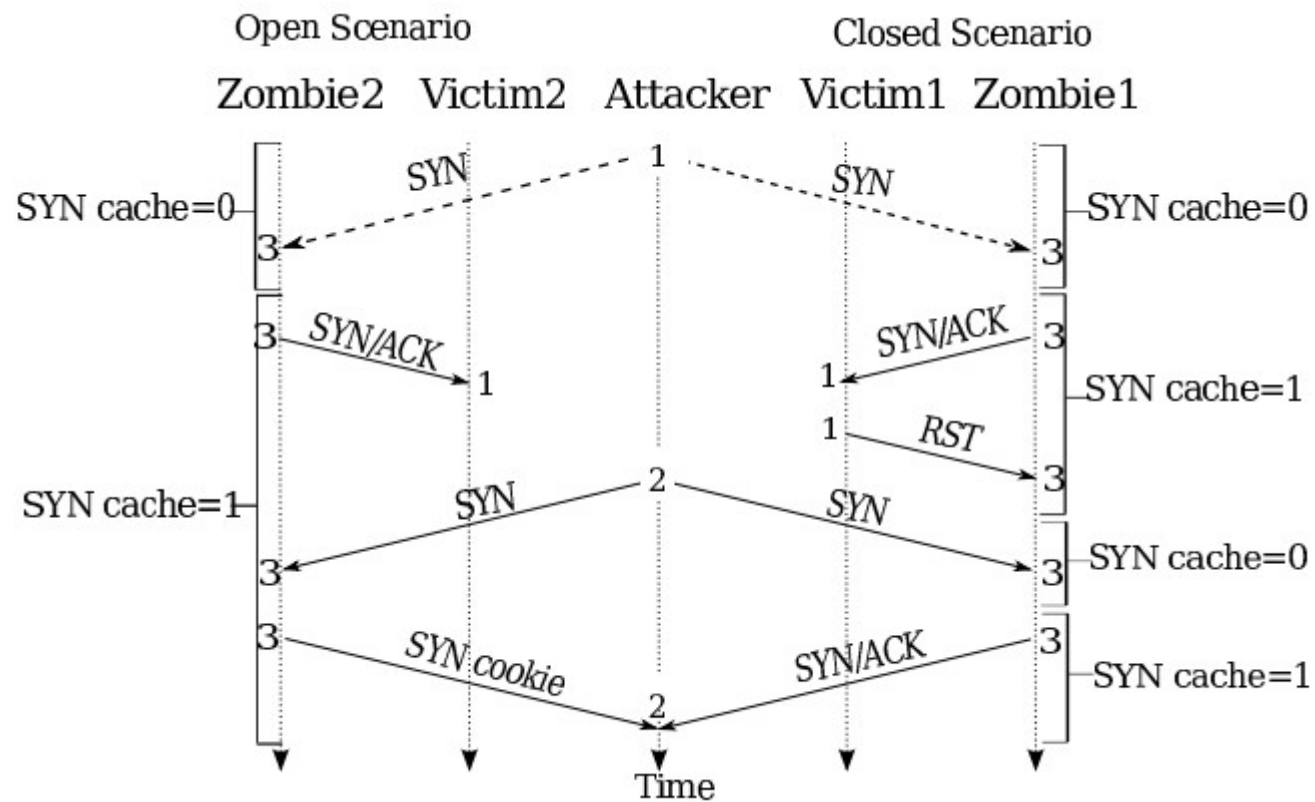
- DoS and SYN backlog basics
 - A side channel based on the SYN backlog
- Blind off-path TCP hijacking
- Blind in/on-path DNS and TCP hijacking

DoS in general

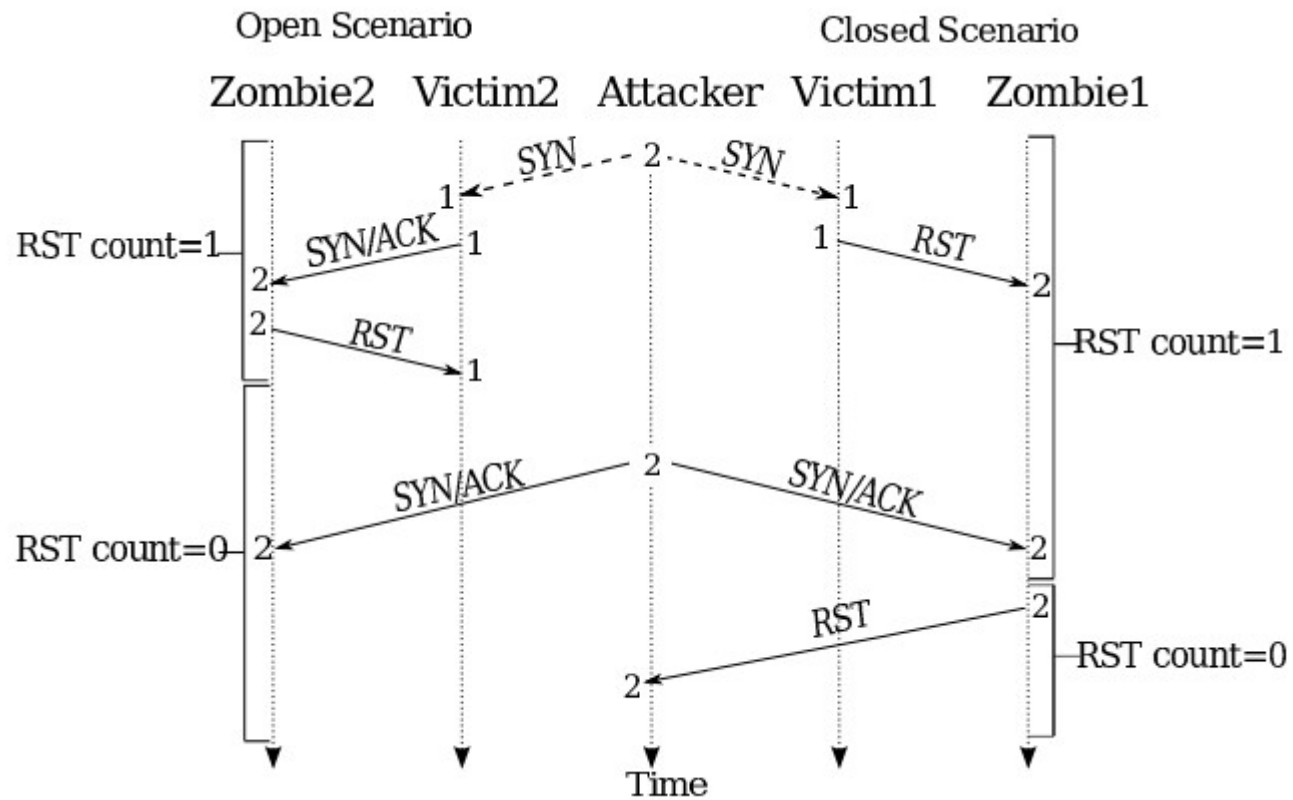
- Exhaust some kind of resource, *e.g.*:
 - Optimistic ACK to exhaust bandwidth
 - See <https://homes.cs.washington.edu/~tom/pubs/CCR99.pdf>
 - PING of death (*e.g.*, large PING) causes crash
 - Exhaust CPU in layer 7
 - More examples: <http://www.isi.edu/~mirkovic/bench/attacks.html>
 - SYN flood: Older hosts had either a fixed amount of half-open connections they could keep track of or no limitations at all, attack is to send lots of SYNs and never ACK or RST
 - Defenses: SYN backlog policies and SYN cookies

SYN cookies and SYN backlogs

- SYN cookies
 - Special kind of SYN/ACK
 - See <https://cr.yp.to/syncookies.html>
 - Can confirm ACK number and reconstruct the necessary state for a connection without having kept any state after sending the SYN cookie
- SYN backlog examples
 - Linux reserves $\frac{1}{2}$, $\frac{1}{4}$, $\frac{1}{8}$ th, and so on for successively older SYNs, prunes 5 times a second
 - FreeBSD has 512 buckets of 30, you can't predict what bucket you fall into (in theory)



From... <https://jedcrandall.github.io/usenix10.pdf>



From... <https://jedcrandall.github.io/usenix10.pdf>

USENIX Security 2016 Cao *et al.* Slides...

USENIX Security 2021 Tolley *et al.* slides...

References

- *NMAP NETWORK SCANNING*, by Gordon “Fyodor” Lyon
- Google “nmap”, “idle scan”, etc.
- Other references were linked to inline