THIERRY MEYER
SÉCURITÉ INFORMATIQUE

Is port stealing still/really exploitable in 2024 ?

Wine Rump 🍇

Who am I ?

> Thierry MEYER
  - cybersecurity consultant
  - *Cabinet Thierry MEYER Consultants*
  - @Th1tuX

Context

- Why this talk … old attack … something new ? Nope
  - We teach Network security
  - Each year we update the content of the courses.
  - Passionate (but gentlemen) debate in the team regarding what to keep and what to drop.
  - Sometimes the answer is obvious (CAM flooding) and sometimes it needs more reflexion (Port-stealing, …).
- 2 questions ?
  - Is port stealing still exploitable in 2024 ?
  - Is port stealing really exploitable in 2024 ?

Port-stealing for dummies

- About the Content Addressable Memory (CAM)
  - Switch forward packets according to the content of the CAM
  - CAM : associates switch port and mac address
- Port Stealing
  - Let the switch think that the victim is connected to our switch port ;
  - How ? Craft a malicious packet that spoofs source mac address of the victim.
  - The switch updates it’s CAM and sends the packets to our port.
  - Easy ?… well almost (teaser) ...

Is it still exploitable ?

> Several tests on « recent » hardware : :

- First with an old CISCO 2960 to prepare the attack
- Then :
  - DELL N1524, ✓
  - Brocade ICX 6450, ✓
  - Huawei S5700. ✓
- And it seems to work fine, the CAM is correctly corrupted.
- **...So let's continue !**

Special thanks to SYS1

Is it really exploitable ?

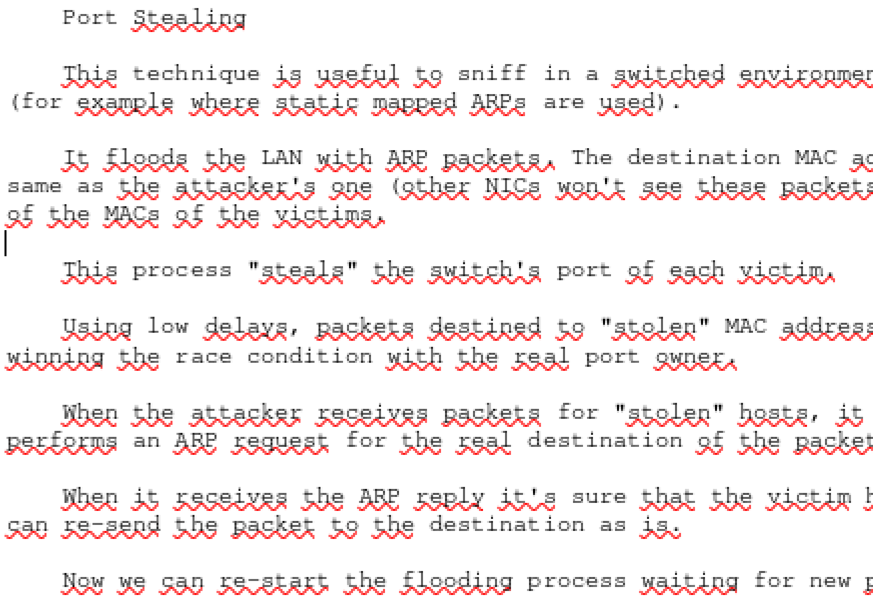
> Need to build a POC (python/scapy) :

- The basic one : really easy to perform with just on packet.
- **BUT** :
  - It **only** corrupts the CAM … which is not a MITM.
  - We need to perform **MUCH MORE** to really obtain a functionnal MITM.
  - … and it’s even more (really much !) complicated.
- Problems :
  - How do we answer to those packets ? (Mac duplication, disable ARP, Race condition, ...)
  - How do we maintain the flow of the communication ?
  - Steatlh ?

Is it really exploitable ?

> I wrote a script (really?) :

- It tooks me hours
- Interesting results, but many thing are not working perfectly,
  - it’s really hand made and durty.
- And after a few hours :
  - I found this →
  - WTF ?!
  - Ettercap does it perflety ?!!!
  - (RTFM)



```
    Port Stealing

    This technique is useful to sniff in a switched environmen
(for example where static mapped ARPs are used).

    It floods the LAN with ARP packets. The destination MAC a
same as the attacker's one (other NICs won't see these packets
of the MACs of the victims.

    This process "steals" the switch's port of each victim.

    Using low delays, packets destined to "stolen" MAC address
winning the race condition with the real port owner.

    When the attacker receives packets for "stolen" hosts, it
performs an ARP request for the real destination of the packet

    When it receives the ARP reply it's sure that the victim h
can re-send the packet to the destination as is.

    Now we can re-start the flooding process waiting for new p
```

In conclusion

> 3 answers :

- Is it still exploitable : **YES**
- Is it really exploitabe : **YES** (but …)
- Do we keep it in the course ?
  - Students will probably never used it in pentest,
  - maybe only in specific aimed attacks (illegal).
  - **But :**
    - It remains MITM (despite of encrypted trafic, self signed certificates)
    - The perfect POC is tricky and complicated …
      - What is complicated is good for students !!

So Let’s keep it in the course !!

Thank you !

Cabinet Thierry MEYER Consultants
74 rue Georges Bonnac, Tour 3
33000 Bordeaux

https://www.tm-consultants.fr
Email : contact@tm-consultants.fr
Tel. 05.57.65.86.20

Thierry MEYER Consultants, est un cabinet de conseil, audit, et expertise technique spécialisé en sécurité des systèmes d'information depuis sa création en 2005.

LSTI®

Certifié conforme ISO/CEI 27001:2017
Conformity to ISO/IEC 27001:2017 certified

Certificat LSTI n°11270
LSTI Certificate n°11270