UCLouvain

Project 2 - Network Attacks

Group 7

MEUNIER Arnaud, HENNEN Cyril

LINFO2347: Computer System Security
Master in Cyber Security
Université Catholique de Louvain

May 11, 2025

Overview

UCLouvain

1. Attack 1: DNS Reflector DoS
2. Attack 2: SYN Flood
3. Attack 3: ARP Poison
4. Attack 4: Network Scanning (Xmas Scan)
5. Attack 5: Network Scanning (Ping Sweep)

UCLouvain

Attack 1: DNS Reflector DoS

LINFO2347

DNS Reflector DoS: Attack & Defense

UCLouvain

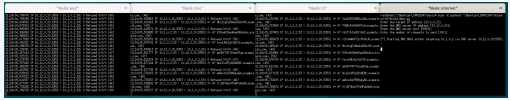


Figure: Reflected DNS replies flooding `ws2` (captured via `tcpdump`)

Attack Mechanism

- Attacker (`internet`) sends DNS queries to the internal DNS server.
- The source IP address of these queries is **spoofed** to match the victim's IP (e.g., `ws2`).
- The DNS server sends DNS replies to the victim, who never initiated dns requests.

Defense Mechanism

Several defense strategies can mitigate this attack:

- On R1 (LAN <-> DMZ)
  - The strict rules (allow only traffic *from* LAN or **established/related**) block the reflected replies destined for `ws2`.
  - R1 never saw the spoofed query originate **from** `ws2`, so the reply isn't *related* from its perspective and gets dropped by the default policy.
- On R2 (DMZ <-> Internet)
  - We drop packets that are spoofed Drop incoming packets ('iifname "r2-eth0"') whose source IP matches internal networks (e.g., `10.1.0.0/24`, `10.12.0.0/24`).

UCLouvain

Attack 2: SYN Flood

LINFO2347

SYN Flood: Attack & Defense

UCLouvain

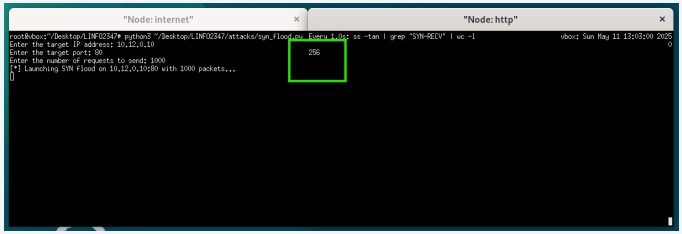


Figure: SYN Flood attack

Attack Mechanism

- Attacker sends a flood of TCP `SYN` packets (with spoofed source IPs).
- Target allocates a half-open connection in its SYN backlog for each SYN.
- Once the backlog fills, no new legitimate connections can be established.

Defense Mechanisms

- **Enable SYN cookies**
- **Rate-limit SYNs** with nftables
- **Reduce Syn-Ack retries**
- **Increase backlog size**

UCLouvain

Attack 3: ARP Poison

LINFO2347

ARP Poison: MITM Attack & Defense

UCLouvain

Figure: Before the attack: simple ws3 to HTTP server via `curl`

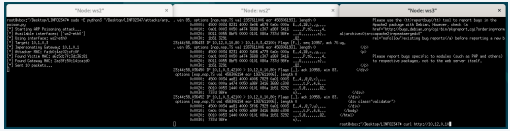


Figure: After the attack: ws2 can snoop traffic (MITM)

Attack Mechanism (Layer 2)

- Attacker (`ws2`) sends forged ARP replies continuously.
- Poisons ARP cache of:
  - Victim (`ws3`, IP: `10.1.0.3`)
  - Gateway (`r1`, IP: `10.1.0.1`)
- Reroutes traffic between `ws3` and network via `ws2`.
- Result: Man-in-the-Middle (MITM) - attacker can sniff/modify traffic (e.g., `curl` request shown).

ARP Poison: Defense

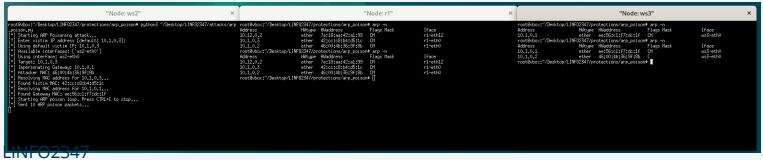
UCLouvain

```
mininet> r1 sudo ~/Desktop/LINFO2347/basic/set_static_arp.sh
Running on Router (r1) (10.1.0.1). Setting static ARP for 10.1.0.3.
Executing: sudo arp -s 10.1.0.3 e2:b2:14:9d:90:5c -i r1-eth0
Verifying ARP entry:
10.1.0.3                 ether   e2:b2:14:9d:90:5c   CM                    r1-eth0
Static ARP entry set successfully.
mininet> ws3 sudo ~/Desktop/LINFO2347/basic/set_static_arp.sh
Running on Workstation (ws3) (10.1.0.3). Setting static ARP for 10.1.0.1.
Executing: sudo arp -s 10.1.0.1 ca:31:e1:f5:1d:01 -i ws3-eth0
Verifying ARP entry:
10.1.0.1                 ether   ca:31:e1:f5:1d:01   CM                    ws3-eth0
Static ARP entry set successfully.
mininet>
```

Figure: Static ARP mapping to cancel arp poisoning attack

Defense Strategies

- `nftables` (L3/L4 firewall) is generally **not suitable** for preventing L2 ARP spoofing.
- **Effective Methods:**
  - **Static ARP Entries:** Manually configure ip to mac (basically to not arp anymore), done without nftables
  - **Consider IPv6:** It uses Neighbor Discovery Protocol (NDP) which is much more secure than arp with ipv4



UCLouvain

Attack 4: Network Scanning (Xmas Scan)

LINFO2347

Xmas Scan: Attack & Defense

UCLouvain

```
mininet> internet sudo -E python3 ~/Desktop/LINFO2347/attacks/network_scans.py

Select attack:
 1. ICMP Ping Sweep
 2. ARP Ping Sweep
 3. TCP SYN Port Scan
 4. Xmas Tree Scan
 5. UDP Scan
 6. Exit
Choice: 4
Target IP [10.12.0.10]: 10.12.0.10
Ports [22,80,443]: 22,80,443

[*] Xmas Tree Scan on 10.12.0.10 ports 22,80,443
  → TCP port 22 OPEN|FILTERED (no answer)
  → TCP port 80 OPEN|FILTERED (no answer)
  → TCP port 443 CLOSED
[Xmas Tree Scan] Terminated.
```

Figure: Xmas scan targeting the HTTP server responding that port 443 is `CLOSED`

Attack Mechanism

- Attacker (`internet`) sends a TCP packet with `FIN`, `PSH`, `URG` flags
- If port closed, host replies with `RST`, no reply otherwise

This attack essentially tells the attacker if the host is **alive** and that the network is **not well protected**.

Defense Mechanism

On every host

- We drop packets with the `FIN`, `PSH`, `URG` flags set.

UCLouvain

Attack 5: Network Scanning (Ping Sweep)

LINFO2347

Ping Sweep: Attack & Defense

UCLouvain

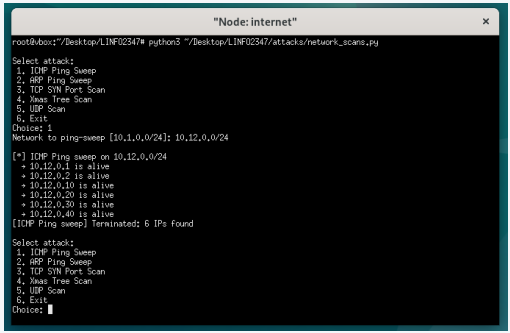


Figure: Ping sweep targeting DMZ (we can see the internal end of the DMZ)

Attack Mechanism

- Attacker (`internet`) sends ICMP Echo Request packets to a range of IP addresses.
- If a host is alive, it will reply with an ICMP Echo Reply. No reply indicates the host is down or not responding to pings.

Defense Mechanism

On R1 (LAN <-> DMZ)

- We block incoming ICMP Echo Request packets from the internet/DMZ and block outgoing request with unauthorized ip

On R2 (DMZ <-> INTERNET)

- We block incoming ICMP Echo Request packets with unauthorized ip destination

References

Nmap Project
Port Scanning Techniques (incl. Xmas Scan)
Nmap Reference Guide

J. Postel (1981)
TRANSMISSION CONTROL PROTOCOL (TCP Flags)
IETF RFC 793

Cloudflare
DNS Amplification Attack
Cloudflare Learning Center

P. Ferguson, D. Senie (2000)
Network Ingress Filtering (Anti-Spoofing)
IETF BCP 38 / RFC 2827

W. Eddy (2007)
TCP SYN Flooding Attacks and Common Mitigations
IETF RFC 4987

Wikipedia Contributors
SYN cookies
Wikipedia

OWASP Contributors
Testing for ARP Poisoning
OWASP WSTG

D. Plummer (1982)
An Ethernet Address Resolution Protocol (ARP)
IETF RFC 826

Linux man-pages project
`arp(8)` – manipulate the system ARP cache
Linux Manual Pages

Netfilter project
nftables wiki
nftables Official Wiki

UCLouvain

Thank you for your attention

MEUNIER Arnaud, HENNEN Cyril

LINFO2347: Computer System Security
Master in Cyber Security
Université Catholique de Louvain

May 11, 2025