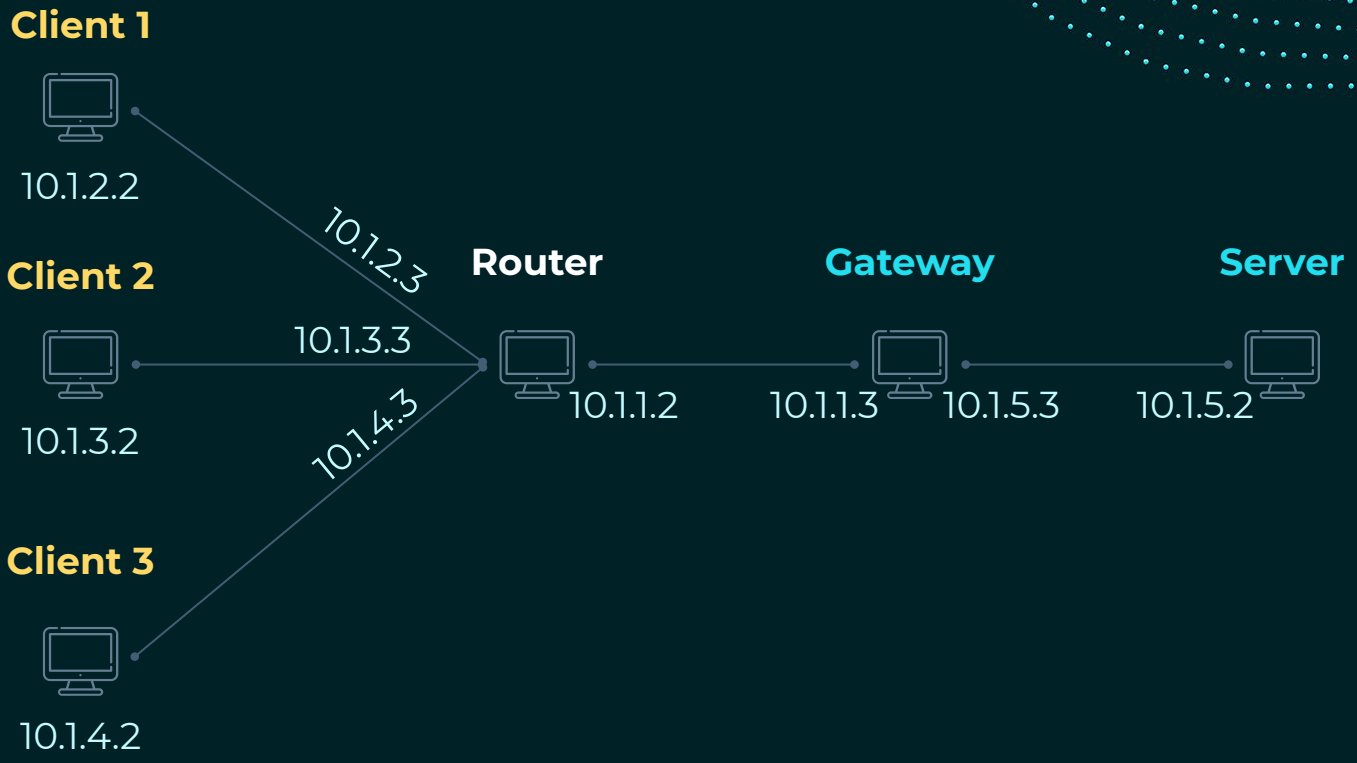
GROUP 2 - BLUE TEAM

Claudio Facchinetti, Batbayar Narantsogt,
Gabriele Ricciardi, Nicolò Vinci

Offensive Technologies
Monday 20 December 2021

CCTFs NETWORK TOPOLOGY

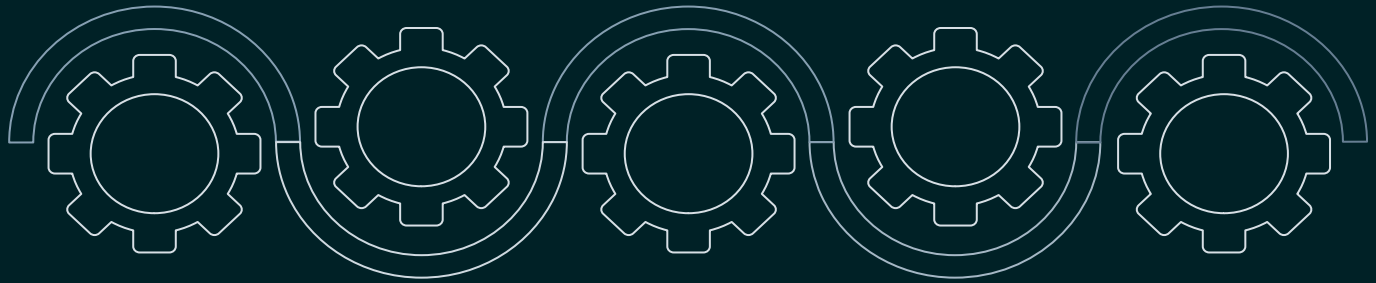


PREPARING FOR THE CCTFs

SETTING UP THE SERVER

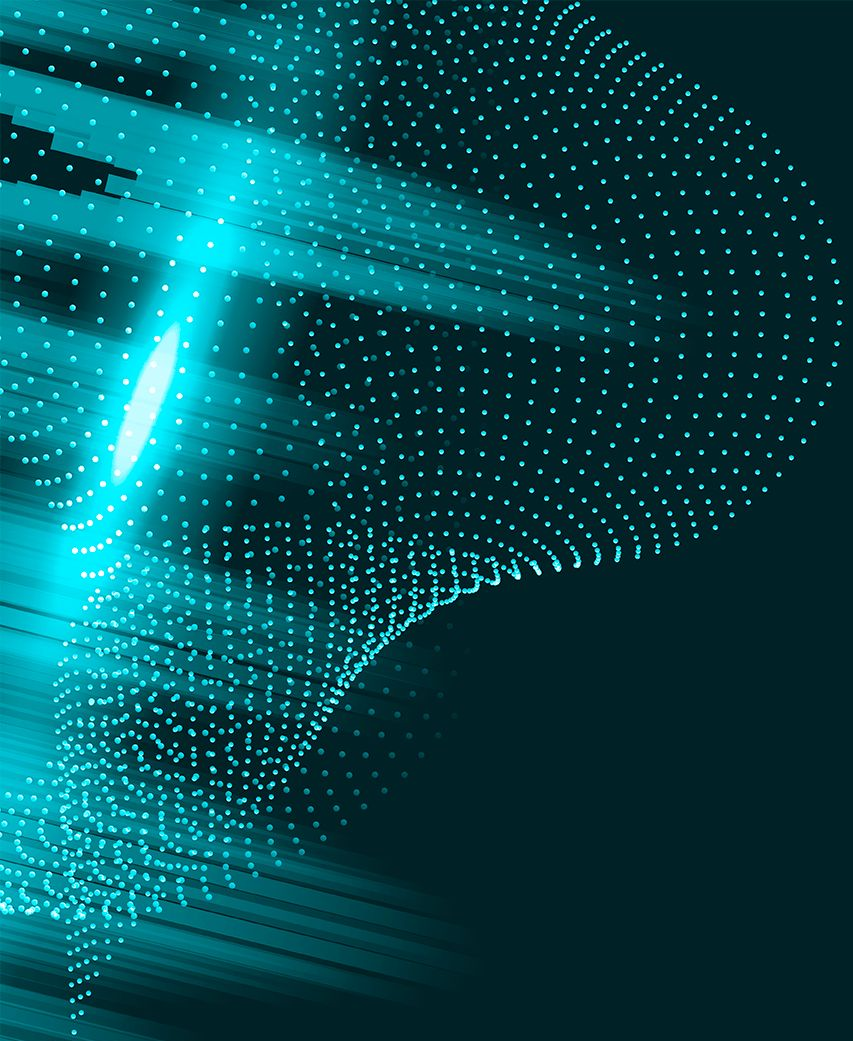
DEVELOPING MONITORS

MILITARIZING THE GATEWAY



SETTING UP THE GATEWAY

SECURING THE SERVER



RESILIENT SERVER

CCTF MILESTONES

SERVER MONITOR

GATEWAY MONITOR

IPTABLES

NETWORK HARDENING

SERVER

SETUP

Apache 2.4.51 from source

Module setup and server configuration

MOD QOS

TCP HARDENING

TCP kernel flags configuration

HTTP/TCP monitor using Scapy and tcpdump

MONITOR

GATEWAY

SERVER MONITOR

Server and link status with curl and ping

Whitelist and regulate legit traffic

IPTABLES

IPTABLES MONITOR

Monitoring matched rules and traffic

DEFENSE STRATEGY

Gateway

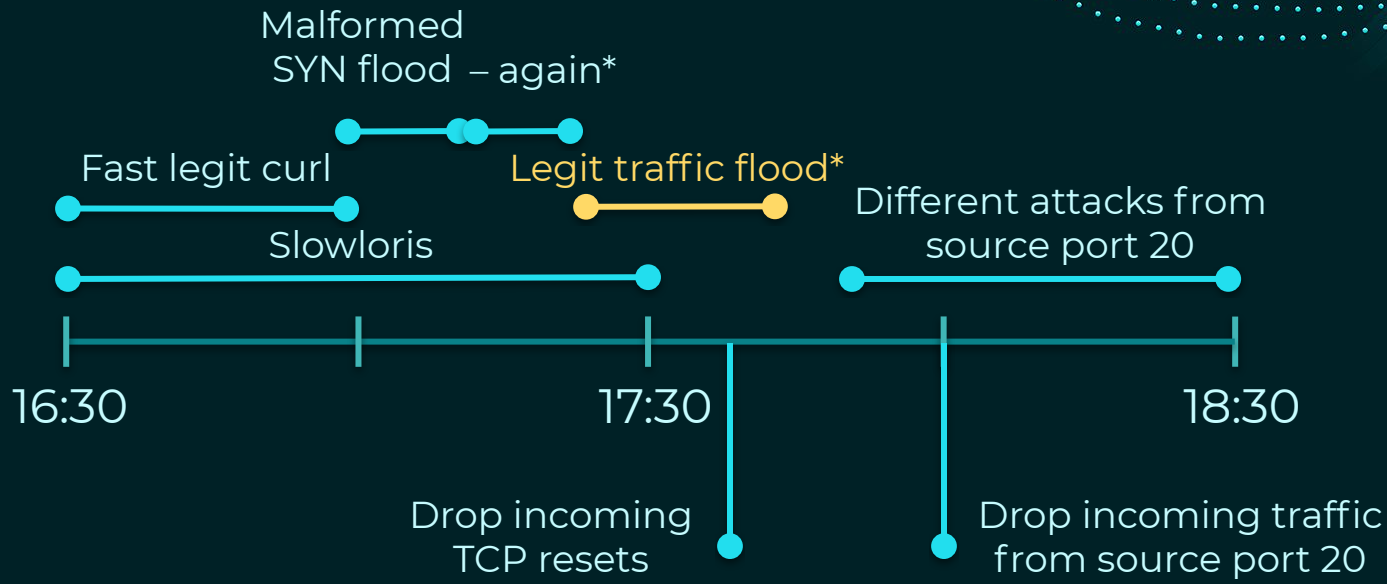
- Live HTTP/TCP traffic and iptables monitoring
- Live server responsiveness check

Server

- Live HTTP/TCP traffic monitoring
- Periodic sockets check

Attack detection and response with live iptables insertion

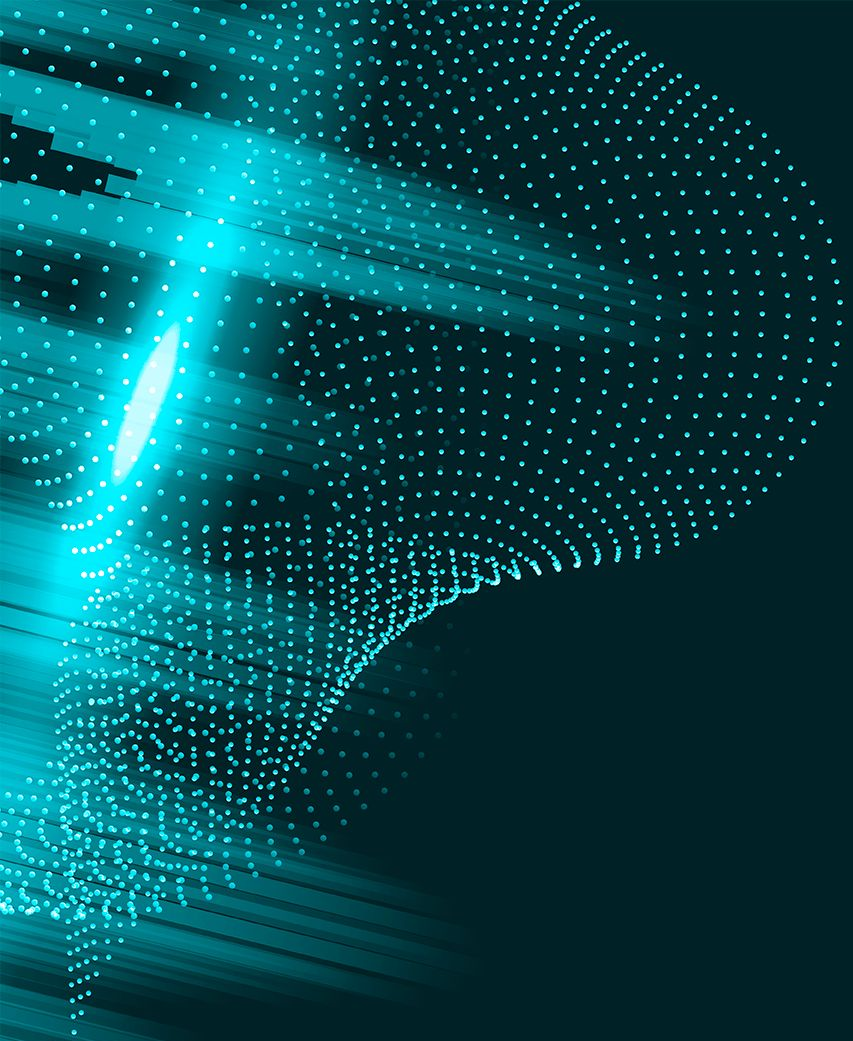
CCTF TIMELINE



* spoofed with legit client IP

RESULTS & IMPROVEMENTS

- Effective defense against slow HTTP DoS
- Sockets monitor
- Mitigation of flooding attacks
- TCP 3-way handshake delegator
- Filtering of illegitimate requests
- Improve iptables monitor
- High availability of service
- Score: 2009 - 46 / 203 - 0



SECURE SERVER

CCTF MILESTONES

INCLUDE TIMESTAMP IN THE LOG

SECURE THE SERVER

DATABASE AND HTTP MONITOR

MILITARIZE THE GATEWAY

SERVER

SETUP

LAMP
Apache 2.4.29
MySQL 5.7.36
PHP 7.2.24

Server Config
Mod QOS Mod Security Mod Evasive

SECURE APACHE

PATCH SERVER

Patch process.php and setup.sql

Database and HTTP monitor

MONITORS

GATEWAY

SETUP

Install Scapy

Whitelist and regulate legit traffic

IPTABLES

MONITOR

HTTP monitor using Scapy

DEFENSE STRATEGY

Gateway

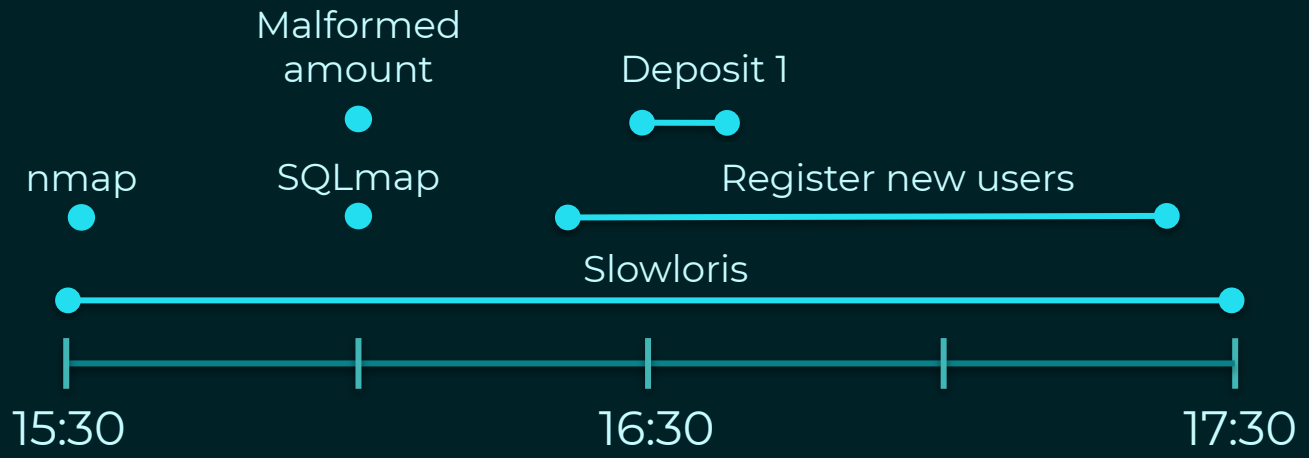
- Live HTTP traffic monitoring
- Periodic iptables monitoring

Server

- Live HTTP traffic monitoring
- Live database monitoring
- Periodic sockets and storage check

Attack detection and response with live iptables insertion and patching

CCTF TIMELINE



RESULTS & IMPROVEMENTS

Effective defense against slow HTTP DoS

Sockets monitor

Prevention of webapp exploitation

Patch request log

Filtering of illegitimate requests

Scanning prevention

Full time availability of service

Score: 0 issues

GROUP 2 - BLUE TEAM

Mitigation of flooding attacks

Patch request log

Score: 2009 - 46 / 203 - 0
0 issues