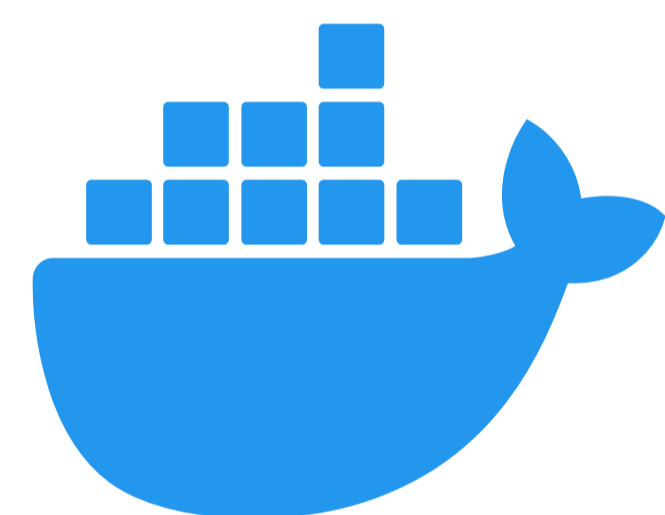
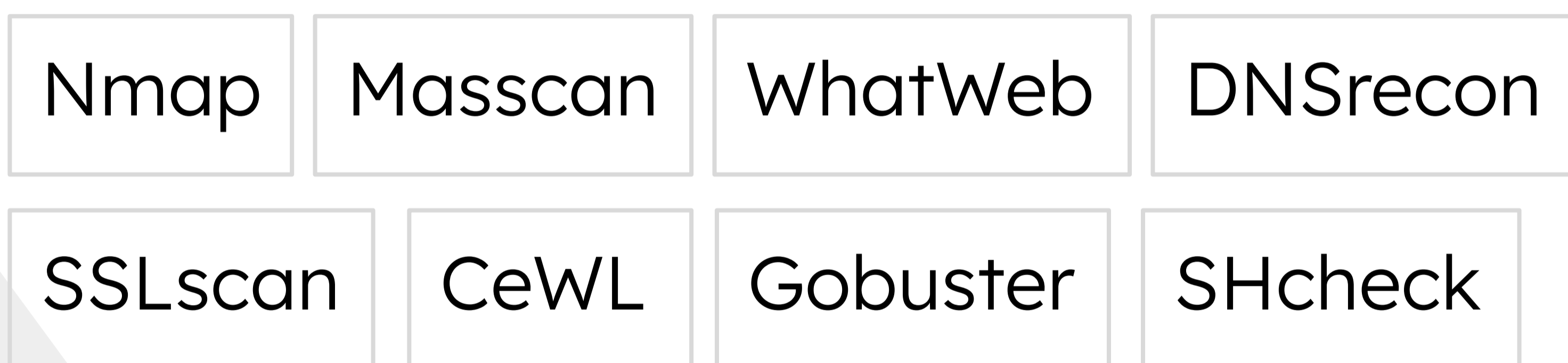


# Tool for Automated Penetration Testing of Web Servers

**Why?** To enhance the efficiency of penetration testing during the reconnaissance phase of the process.

**How?** Combining the functionality of several Linux tools into one automated script.

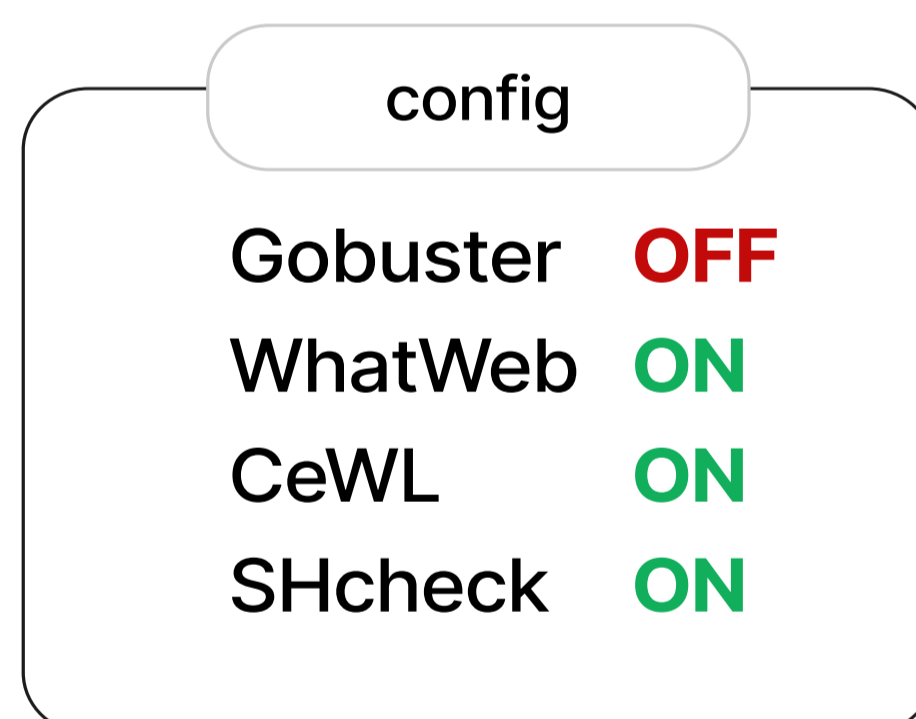
**Advantages:** Flexible. Scalable. Extensible.



Focus local network →

Targets discovery  
(scan type 0)

192.168.167.105  
192.168.167.197  
192.168.167.241  
192.168.167.248



Scan (type 1)



192.168.167.105

Open ports: 21, 80, 443, 9389  
FTP (21): Anonymous login allowed  
HTTPS (443) missing headers: X-Frame-Options, X-Content-Type-Options  
Unknown service (9389)



192.168.167.197

Open ports: 22, 53, 7632  
HTTPS (7632): non-standard port for a web server

⋮

**Author:** Bc. Michal Rajecký  
xrajec01@fit.vutbr.cz