# Web Server Compromise

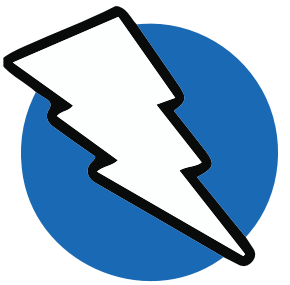
The attackers take over an external web server. They use it to pivot to your internal network.

## DETECTION

Server Analysis
SIEM Log Analysis
Network Threat Hunting - Zeek/RITA Analysis

## TOOLS

Zed Attack Proxy
sqlmap
Burp Proxy



https://www.zaproxy.org

https://portswigger.net/burp

https://www.blackhillsinfosec.com/using-simple-burp-macros-to-automate-testing

CDV2_0421

# Backdoors™ & Breaches

## INITIAL COMPROMISE

Created by: BLACK HILLS | Information Security