Protecting a Web Application against Brute-force Attacks

Yousef Afshar, Chasey Kilcrease
Advisors: Jose Gomez

Department of Integrated Information Technology
University of South Carolina

December 8th, 2023

Agenda

- Project Description
- Objectives
- Background on NGFW
- Experimentation scenario
- Hands-on demonstration in Netlab
- Best practices for web application security
- Lessons Learned

Project Description

- Understanding brute-force attacks
  - How an attacker will execute these attacks on a production environment network.
  - What reasons an attacker would have to utilize these methods.
- Configure the NGFW to detect and block brute-force attacks
  - The NGFW must implement a brute-force attack protection policy, so that any attack from the external (Internet) network will be detected and blocked
- Provide the best practices to enhance the security of web applications
  - What mitigation techniques can be followed to prevent a brute-force attack on a web application.

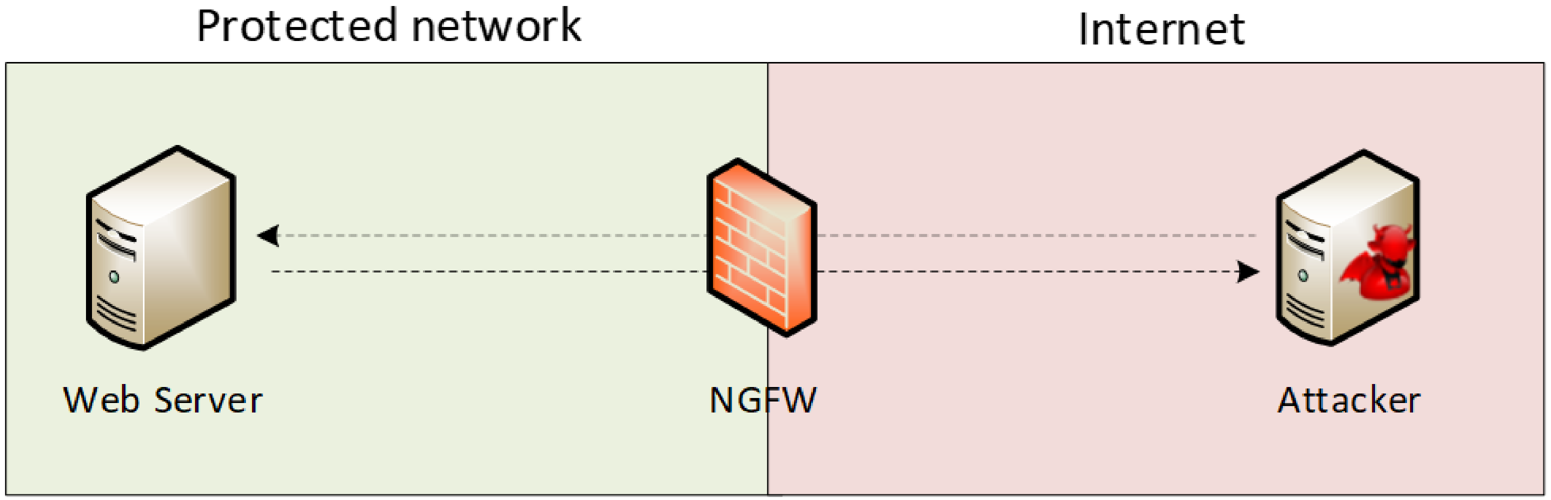
Objectives

- Configure a brute-force attack protection policy in the NGFW
    1. Show how simple it can be to configure a protection policy in place with a NGFW effectively.
    2. Show the logging and background of how the policy works in action.

- Simulate a brute force attack on the victim's machine from the attacker's machine
    1. Demonstrate the brute force attack executing with no NGFW policy implemented
    2. Demonstrate the brute force attack being prevented from executing once the NGFW policy is implemented.

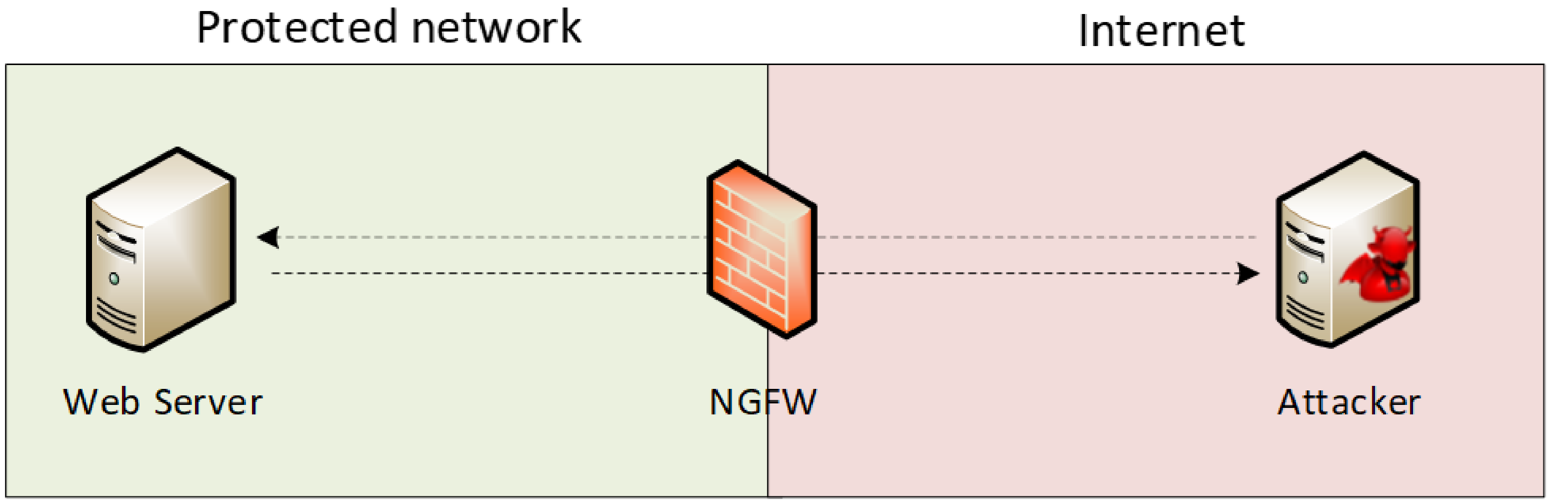
Background on NGFW

- Next-Generation Firewall (NGFW)
- The NGFW is equipped with advanced capabilities designed to mitigate various attacks
- Overtime these firewalls have become increasingly granular and allow for finer levels of policy administration and enforcement.
- Many vendors today: Palo Alto, Fortigate, CheckPoint, etc.



Experimentation Scenario

- The scenario consists of an application hosted on a web server and an attacker located on the external network
- The NGFW is located between the web server and attacker
- The attacker is relying on a trial-and-error approach to guess the login credentials of a legitimate user
  - Brute force attacks operate on the principle of continually attempting entry until a random or semi-random credential will allow access; often utilize known or leaked password lists.

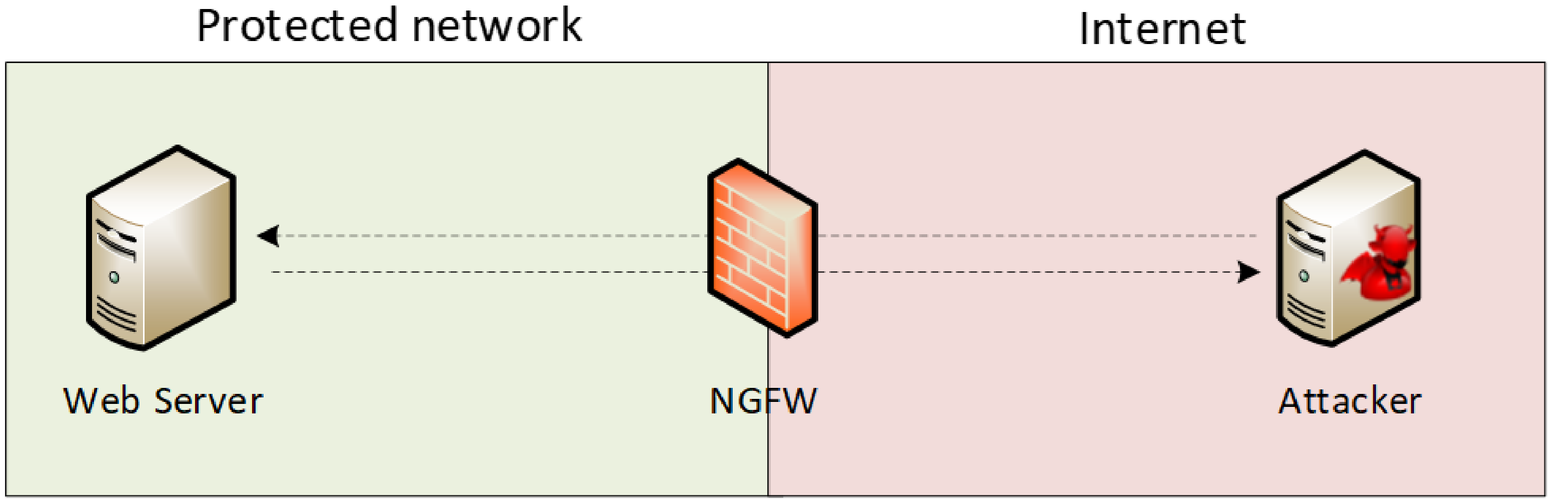


Best Practices: Web Application Security

- Documentation of All Changes
  - Identify all potential entry points for hackers
- Establish real-time monitoring of systems
  - PRTG, SolarWinds, CyberCNS, Zabbix, Prometheus
- Use passwords following NIST Standards
  - Minimum 8 characters length, the longer the more secure.
  - Variety of character types (i.e., symbols, numbers, etc.)
- Engage in penetration testing and other cybersecurity checks
  - Continual auditing and enlisting the services of white-hat hackers can improve cybersecurity drastically and find deeper weaknesses.

Hands-on Demo in Netlab

- Demo 1: A successful execution of a brute force attack on the web server from attackers' machine without a security policy in place.
  - Utilizing the hydra tool within Kali Linux to attack a web server.
- Demo 2: The implementation of the brute force attack policy in the NGFW
  - Showing a Palo Alto security policy tailored to a brute force attack.
- Demo 3: An unsuccessful brute force attack attempt on the web server from the attacker's machine mitigated due to the policy in the NGFW.
  - Showing the Palo Alto Policy actively stopping the attacker's brute force attempt.



Lessons Learned

- How to execute a brute-force attack
  - Showed a common tool in hydra that can executed with relative ease.
- How to properly configure the NGFW to detect and block brute-force attacks
- Implementing a brute-force attack protection policy on an NGFW
- Establishing the best practices are to enhance the security of web applications
- The usage of policies within NGFW in both direct mitigation and alerting use-cases.
  - Combining cutting edge features of NGFW policies alongside a strong architecture allows for the technology to be leveraged fully.

THANK YOU!