SECURITY TESTBED:

SCALABLE INFRASTRUCTURE FOR INTERACTIVE ATTACK REPLAY AND TESTING OF SECURITY MONITORING TOOLS

Seoung K. Kim, Surya Bakshi, Phuong Cao, Eric C. Badger,
Zbigniew T. Kalbarczyk, Ravishankar K. Iyer

SCIENCE OF SECURITY
VIRTUAL ORGANIZATION

The Science of Security Initiative is funded by the National Security Agency.

Introduction

WHAT is the Security Testbed?

- A controlled system and network environment where attacks can be replicated and replayed

WHY do we need the testbed?

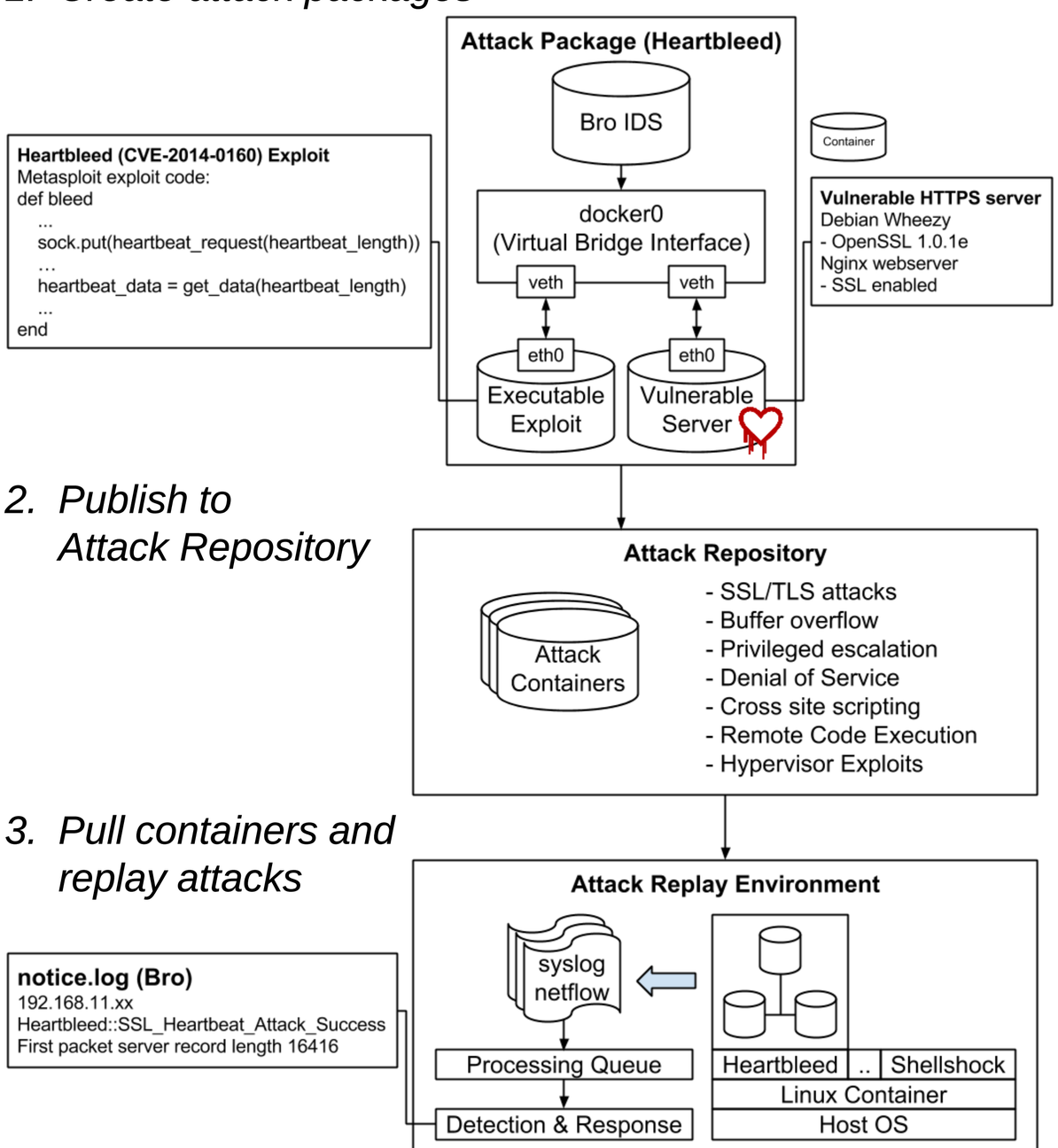
- Allows security researchers to safely reproduce and evaluate vulnerabilities and attacks
- Serves as an attack database for sharing information on security threats among security researchers
- Provides an environment to test and evaluate security monitoring tools against attacks

Requirements

- Isolation: prevent replayed attacks from affecting production infrastructure
- Instrumentation: collect system and network events in various attack stages
- Repeatability: provide a convenient platform for users to reproduce attacks

Architecture of Security Testbed

1. Create attack packages



Implementation

Isolation:

- Linux containers – a virtualization environment that enables running multiple isolated systems using process' models on a shared kernel

Instrumentation:

- OSSEC – system log analyzer
- Bro IDS – network traffic analyzer

Repeatability:

- Docker – provides a layer of abstraction and automation of virtualization
- Attack Repository – maintains attack container images

Categories of Attack Containers

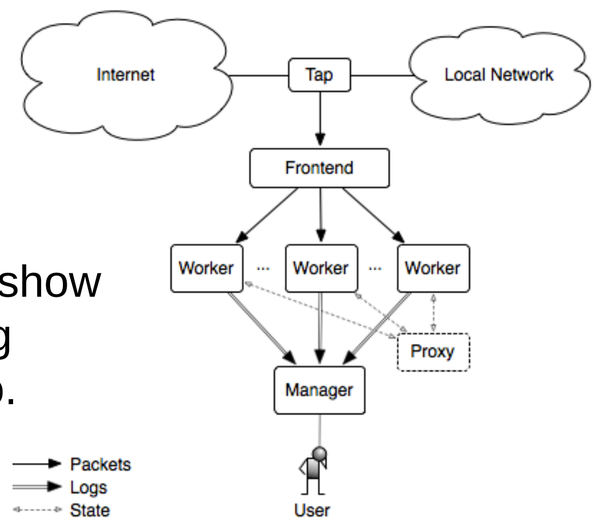
Category	Description	Attack Container
SSL/TLS	Attacks exploit vulnerabilities in the widely used cryptographic protocol SSL/TLS.	Heartbleed • OpenSSL 1.0.1e (vulnerable software) • Metasploit (exploit tool)
Arbitrary Command Execution	Attacks exploit vulnerabilities to get full access to a machine.	Shellshock (Bashdoor) • Apache 2 • Bash 4.3
Web App	Attacks exploit web application vulnerabilities to insert malicious code, for example, for the purpose of obtaining user credentials.	XSS (cross-site scripting) • Apache 2 • PHP 5
Injection	Attacks inject commands into a web server to make it behave abnormally.	SQL Injection • Apache 2 • PHP 5 • MySQL
Denial of Service	Attacks attempt to restrict access to a resource.	SlowDOS • Apache2 • slowhttptest • Kali Linux (exploit tool)

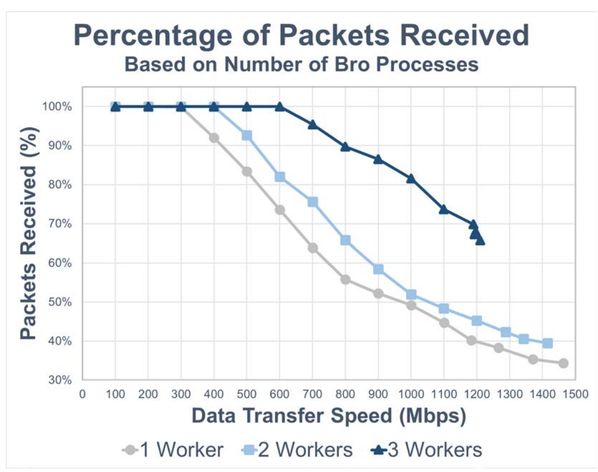
Performance Evaluation

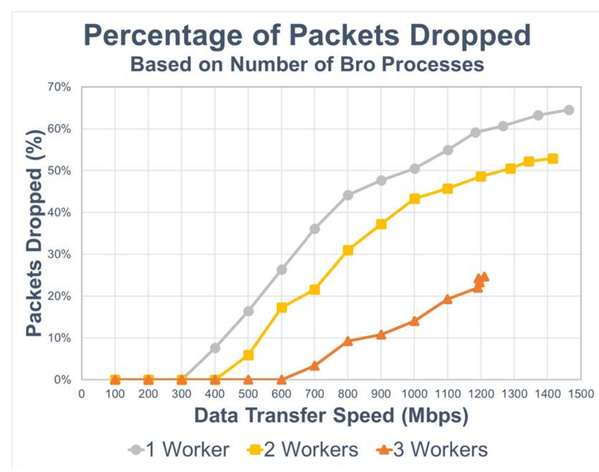
1. Network packet analysis on bare metal vs. container
   - *Challenge*: running "containerized Bro" may result in performance loss.
   - Measured 19% overhead when running containerized Bro to analyze network packets collected over 5 minutes (368MB).

Capture Details	
Size	368MB
Packets	791,615
Flows	40,686

   - Most of the attacks replayed in the testbed last less than a minute (a few MB in size).
     - Performance loss from using containerized Bro would be much smaller.
2. Real-time monitoring with single vs. multiple Bro instances
   - *Challenge*: single Bro instance may not be able to process a large volume of replayed traffic (for instance, when simulating DoS attack).
   - Bro can be deployed in a cluster of multiple Bro instances.
   - Measured packets received/dropped ratios show the advantage of running multiple instances of Bro.







Future Work

- Create an interactive interface for the security testbed
- Implement attack containers for hypervisor and kernel-level exploits

This material is based upon work supported by the Maryland Procurement Office under Contract No. H98230-14-C-0141

CSL: COORDINAT SCIENCE L