DefenseWizard

Automated OSINT

Securing Real-Time Networks
Passive Approaches

Active Systems (Discovery)

1. Active network mapping mimics hostile activity causing sensors to trigger outages.

2. Active scanning place significant resource loads on network devices.

3. Errors in scanner configuration, such as scanning wrong IP ranges, can impact adjacent networks.

Active Systems (System Audit)

It took months to fully identify systems impacted by the Heartbleed Implementation bug.

A recent search on Shodan revealed that over 200,000 system are still exposed.

Scanning system across every IP Address and every port

1. All systems are powered on
2. Scanners have visibility and not blocked by firewalls.
3. Scanning operation will not disrupt critical operations
4. The vulnerable services are running,
5. Vulnerable services are responding to probes.

Passive Systems
Reconnaisance and Defense

Listen rather than discover

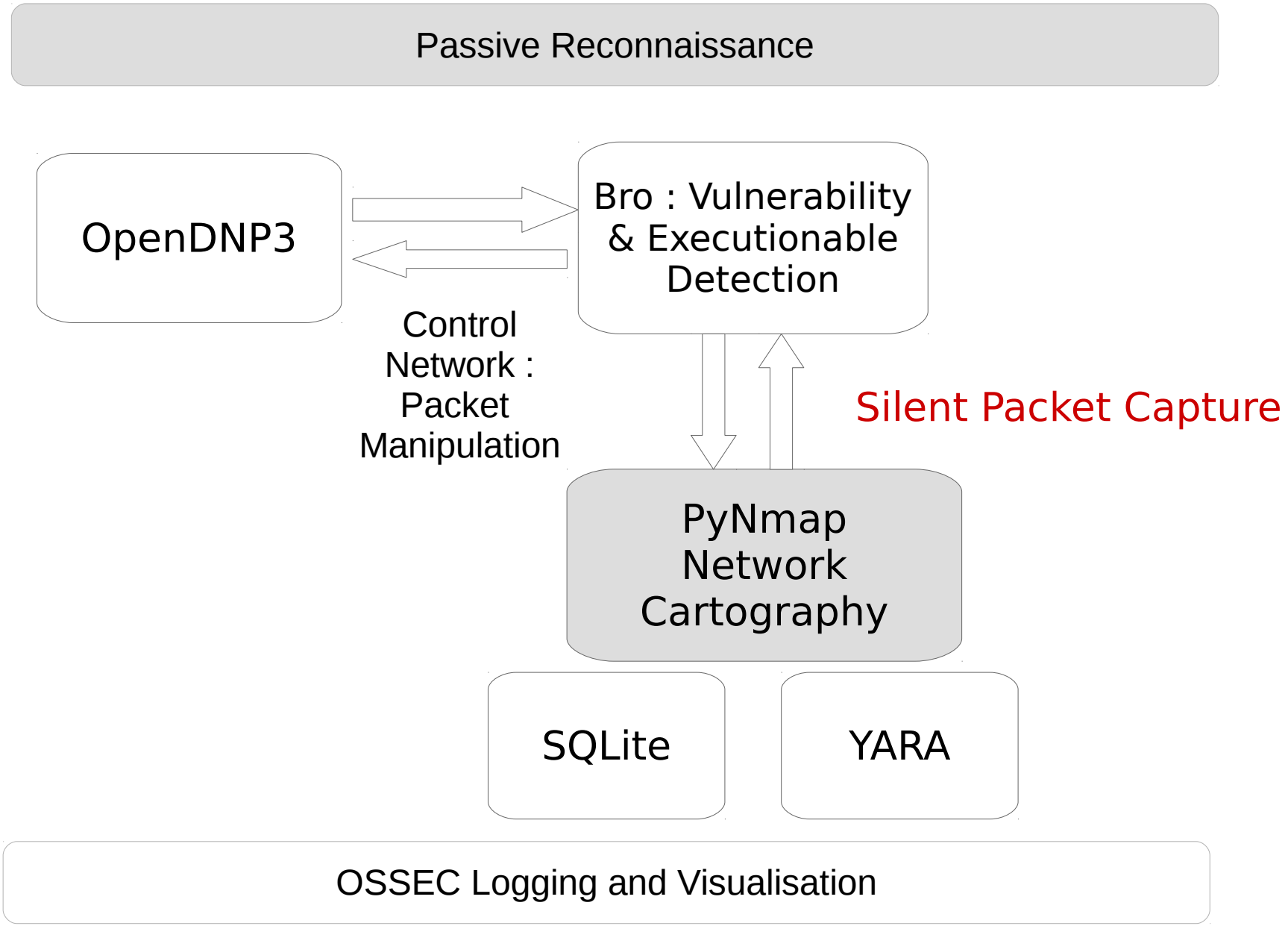
Low or negligible bandwidth and resource usage.

Allows for continuous and broad deployment

Low profile or invisibility.

Absence of interpretive systems leading to cleaner data collection.

Passive (Low Bandwidth) Intrusion Recon & Detection



Recon-NG : Reconnaisance Tool

Creates the possibility to conduct :

Host Discovery

Server Enumeration

Gain Access to Authentication Credentials

Without sending a single packet.

Social-Engineering Support

Request For Proposals : often including ICS environment

Employee social media sites contain technology rich information

Engineer professional bios.

Publically available information regarding ICS Asset :

- Owner – vendor relationships
- Conference attendance
- Committee attendance
- Domain names

OWASP Testing Guide v4

Section 4 Web-Application Pen Testing
Web-Server Recon

4.2.1 Testing for web-server fingerprint (OWASP-IG-004)

4.2.2 Review web-server metafiles (OWASP-IG-001)

4.2.5 Identify application entry points (OWASP-IG-003)

4.2.1 Server Fingerprinting : “knowing the version and Type of a running web-server allows testers to determine Known vulnerabilities and exploits to use during testing”

4.2.2 Review Web-Server Metafiles : Refcon-ng will discover And download discovered files such as robots.txt, sitemap.xml, Crossdomain.xml and phpinfo.php intp workspace directory You are using.

4.2.5 Identify Entry Points :”This section will help you identify And map every area within the application that should be Investigated once your enumeration and mapping phase Has been completed.” XSS via GET or POST requests ?

Recon-ng Reconnaissance Report

HOSTS

Hostname	IP Address
click.communications.trustwave.com	
crl.trustwave.com	
encrypt.trustwave.com	
gcs.cvs.trustwave.com	
image.communications.trustwave.com	
login.trustwave.com	
m.contra.gr	
mailmax.trustwave.com	
marshallicensing.trustwave.com	
myidentity.trustwave.com	
pci.trustwave.com	
sae.trustwave.com	
sealserver.trustwave.com	
sgcatest.trustwave.com	
ssl.trustwave.com	
superball.contra.gr	
view.communications.trustwave.com	
www.contra.gr	
www.trustwave.com	
www.xlf.gr	
xgcatest.trustwave.com	

Silent Capture
What's on Your Network ?
(May Surprise You !)

1. What Open Ports Services Have Not Been Identified ?

2. Who's Touching Your Network ?

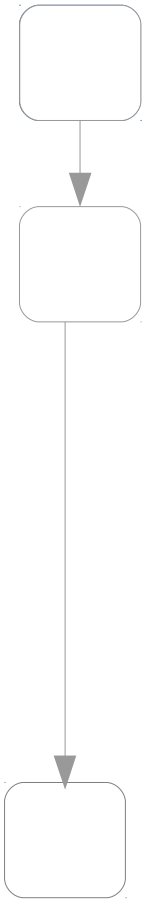
Passive Intrusion Detection
Network Cartography Using
Silent Capture

1. Capture

2. Extraction and Analysis

5 Files : Total Size 91.7 kb

Cartography Toolbox (Silent Capture)



Simple Capture

Server/client interactions on a single port

Main Capture

Capture of specified TCP/UDP Packets

Storage of captured packets

Storage of OS observations

Print content of observations

Save for analysis later

PCAP Capture Analysis

Direct Program Output

Print Histogram of All Observations

Print Observed Servers/Clients

Cartography Toolbox (Extraction and Analysis)

PCAP Extraction

Specify core data to be analysed

Isolate PCAP files with Python dptk Package

Extract Data

Analyze Data

Wireshark

Tcpreplay

NETRESEC