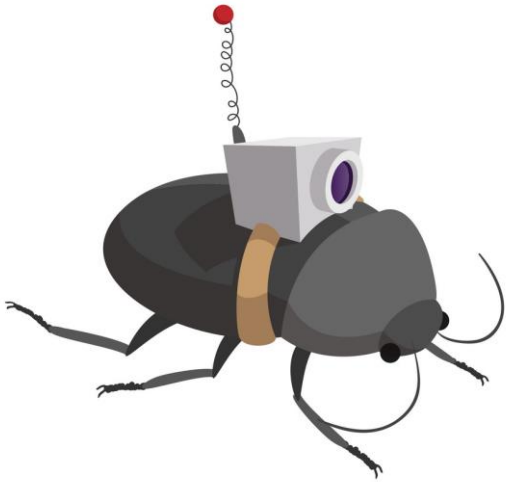


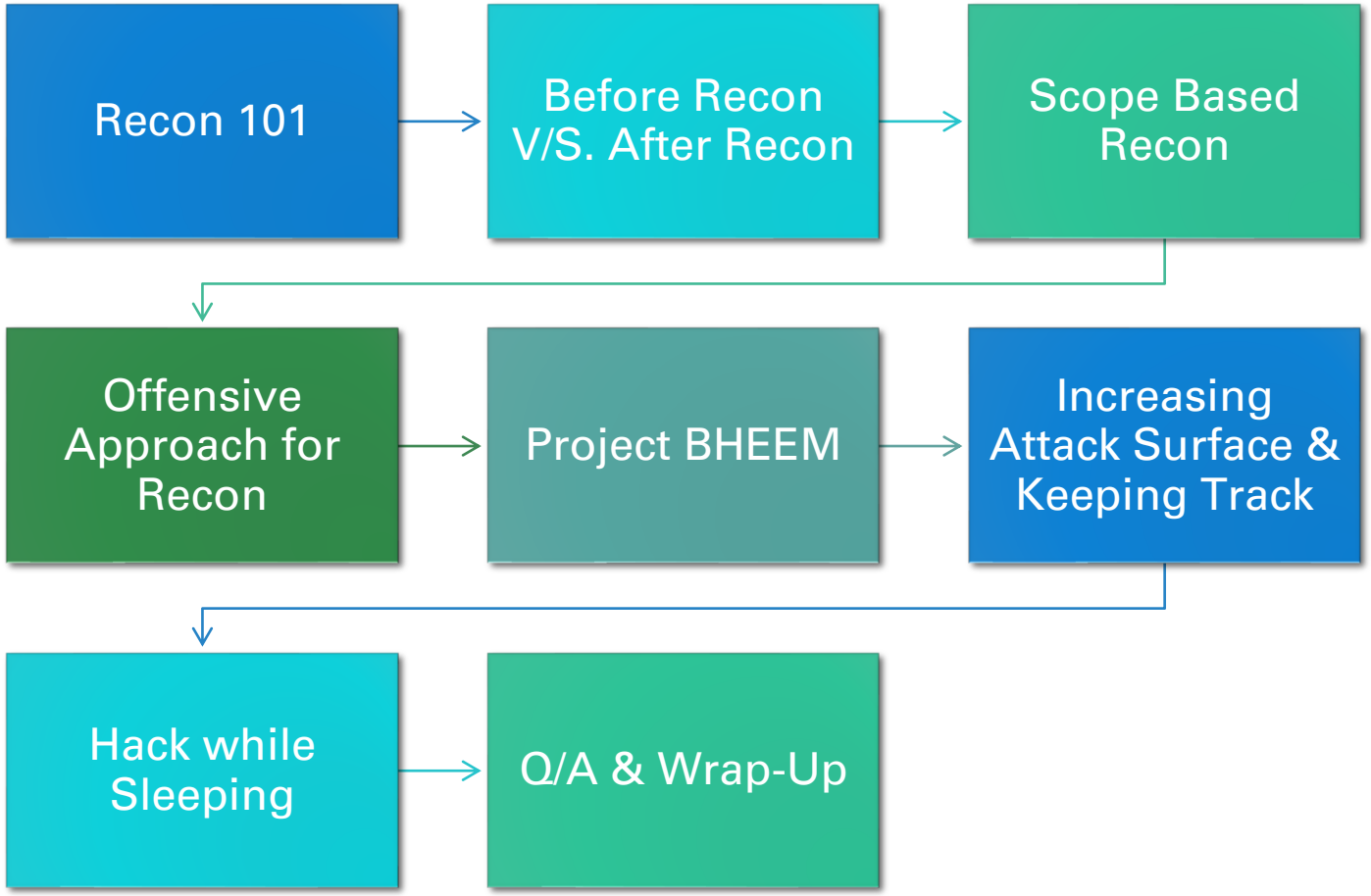
# Offensive Recon \\for\\ Bug Bounty Hunters

BY: HARSH BOTHRA

# Who Am I?

- Cyber Security Analyst at Detox Technologies
- Bugcrowd Top 150 Researchers – All Time (Ranked 142nd Currently)
- Synack Red Team Member
- Author – Hacking: Be a Hacker with Ethics (GoI Recognized)
- Author – Mastering Hacking: The Art of Information Gathering & Scanning
- InfoSec Blogger
- Occasional Trainer & Speaker
- Lifelong Learner
- Poet

# Agenda


Recon 101
Before Recon V/S. After Recon
Scope Based Recon
Offensive Approach for Recon
Project BHEEM
Increasing Attack Surface & Keeping Track
Hack while Sleeping
Q/A & Wrap-Up

# RECON 101

WHAT

WHY

WHERE

WHEN

HOW

# Before Recon V/S. After Recon

**Before Recon**

- Target's Name
- Scope Details
- High-Level Overview of Application
- Credentials/Access to the Application
- And some other information based upon target, that's it on high level?


**After Recon**

- List of all live subdomains
- List of interesting IPs and Open Ports
- Sensitive Data Exposed on Github
- Hidden Endpoints
- Juicy Directories with Sensitive Information
- Publicly exposed secrets over various platforms
- Hidden Parameters
- Low hanging vulnerabilities such as Simple RXSS, Open Redirect, SQLi (Yeah, I am serious)
- Scope from 1x to 1000x
- And list goes on like this....

**Small Scope**
Specific Applications in scope.

**Medium Scope**

*.target.com or set of applications in scope.

**Large Scope**

Everything in Scope.

# Scope Based Recon

# Small Scope Recon

## Scope – Single/Multiple Page Applications

What to look for while Recon:

- Directory Enumeration
- Service Enumeration
- Broken Link Hijacking
- JS Files for Hardcoded APIs & Secrets
- GitHub Recon (acceptance chance ~ Depends upon Program)
- Parameter Discovery
- Wayback History & Waybackurls
- Google Dork (Looking for Juicy Info related to Scope Domains)
- Potential URL Extraction for Vulnerability Automation (GF Patterns + Automation Scripts)

# Medium Scope Recon

**Scope - *.target.com or similar (multiple applications)**

What to look for while Recon:

- Subdomain Enumeration
- Subdomain Takeovers
- Misconfigured Third-Party Services
- Misconfigured Storage Options (S3 Buckets)
- Broken Link Hijacking
- Directory Enumeration
- Service Enumeration
- JS Files for Domains, Sensitive Information such as Hardcoded APIs & Secrets
- GitHub Recon
- Parameter Discovery
- Wayback History & Waybackurls
- Google Dork for Increasing Attack Surface
- Internet Search Engine Discovery (Shodan, Censys, Fofa, BinaryEdge, Spyse Etc.)
- Potential URL Extraction for Vulnerability Automation (GF Patterns + Automation Scripts)

# Large Scope Recon – The Actual Gameplay

## Scope – Everything in Scope

**What to look for while Recon:**

- Tracking & Tracing every possible signatures of the Target Application (Often there might not be any history on Google related to a scope target, but you can still crawl it.)
- Subsidiary & Acquisition Enumeration (Depth – Max)
- DNS Enumeration
- SSL Enumeration
- ASN & IP Space Enumeration and Service Identification
- Subdomain Enumeration
- Subdomain Takeovers
- Misconfigured Third-Party Services
- Misconfigured Storage Options (S3 Buckets)
- Broken Link Hijacking

- **What to look for while Recon:**
  - Directory Enumeration
  - Service Enumeration
  - JS Files for Domains, Sensitive Information such as Hardcoded APIs & Secrets
  - GitHub Recon
  - Parameter Discovery
  - Wayback History & Waybackurls
  - Google Dork for Increasing Attack Surface
  - Internet Search Engine Discovery (Shodan, Censys, Fofa, BinaryEdge, Spyse Etc.)
  - Potential URL Extraction for Vulnerability Automation (GF Patterns + Automation Scripts)
  - And any possible Recon Vector (Network/Web) can be applied.

Choose Scope Based Recon

Create a Script for Automating Scope Based Recon

Run Automation Script over Cloud.

Manually Recon (GitHub & Search Engine Dorking) while Automation Completes.

Create Cron Jobs/Schedulers to Re-Run specific Recon task to identify the new assets.

Implement alerts/push for Slack or preferred

# Offensive Approach for Recon

# Project BHEEM

# Project Bheem

Nothing Fancy!

Collection of existing tools automated via bash scripting that can be ran over VPS

Easily Managed & Organized Output

# Project Bheem – Future Plans

Adding Multi-threading

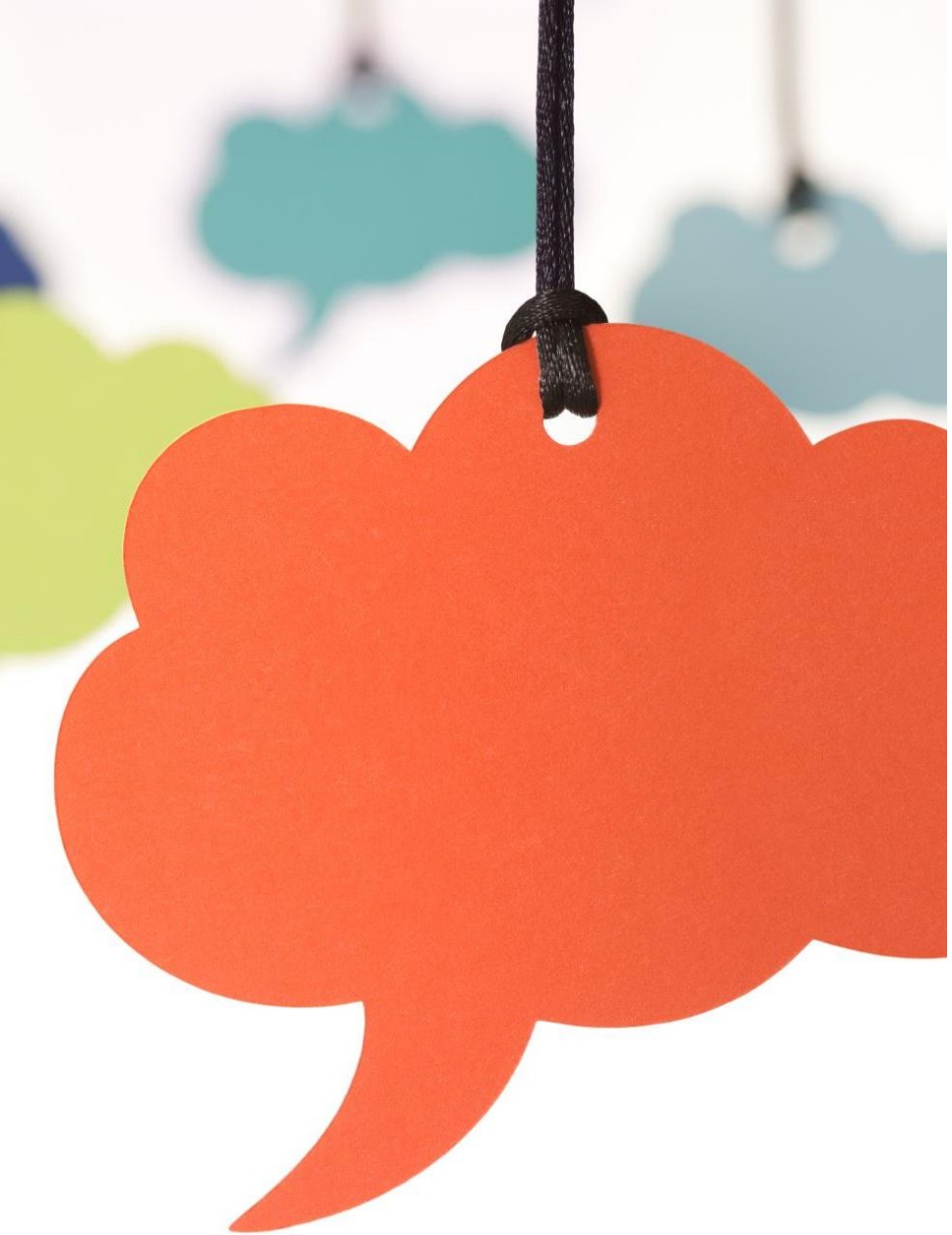
Adding Multi-Job Scheduling

Adding more vulnerability scanning support (Testing going on)

Open for community to fork and update it as they want

# Increasing Attack Surface & Keeping Track

LET'S SEE HOW I TRY TO INCREASE ATTACK SURFACE, ORGANIZE MY RECON DATA & RELEVANT INFORMATION.



# Hack while Sleeping

**Automating your Recon over Cloud allows you to Hack while Sleeping.**

Here's what you need:

1. A Cloud Service Provider (AWS, GCP, Digital Ocean, etc.)
2. Create a  VM & Install Necessary Tools (Create a re-usable Installation Script)
3. Clone your Automation Scripts to Cloud
4. Create a Linux Screen & Run your automation
5. Exit & Enjoy !
6. Login to VPS again to see the results ;)

Screen keeps your commands running on the background and doesn't terminate jobs if SSH timeouts or force closed.

# Get in Touch at


 Website - https://harshbothra.tech

 Twitter - @harshbothra_

 Instagram - @harshbothra_

 Medium - @hbothra22

 LinkedIn - @harshbothra

 Facebook - @hrshbothra

 Email - hbothra22@gmail.com

# Q/A & Future Roadmap

# Thank You