

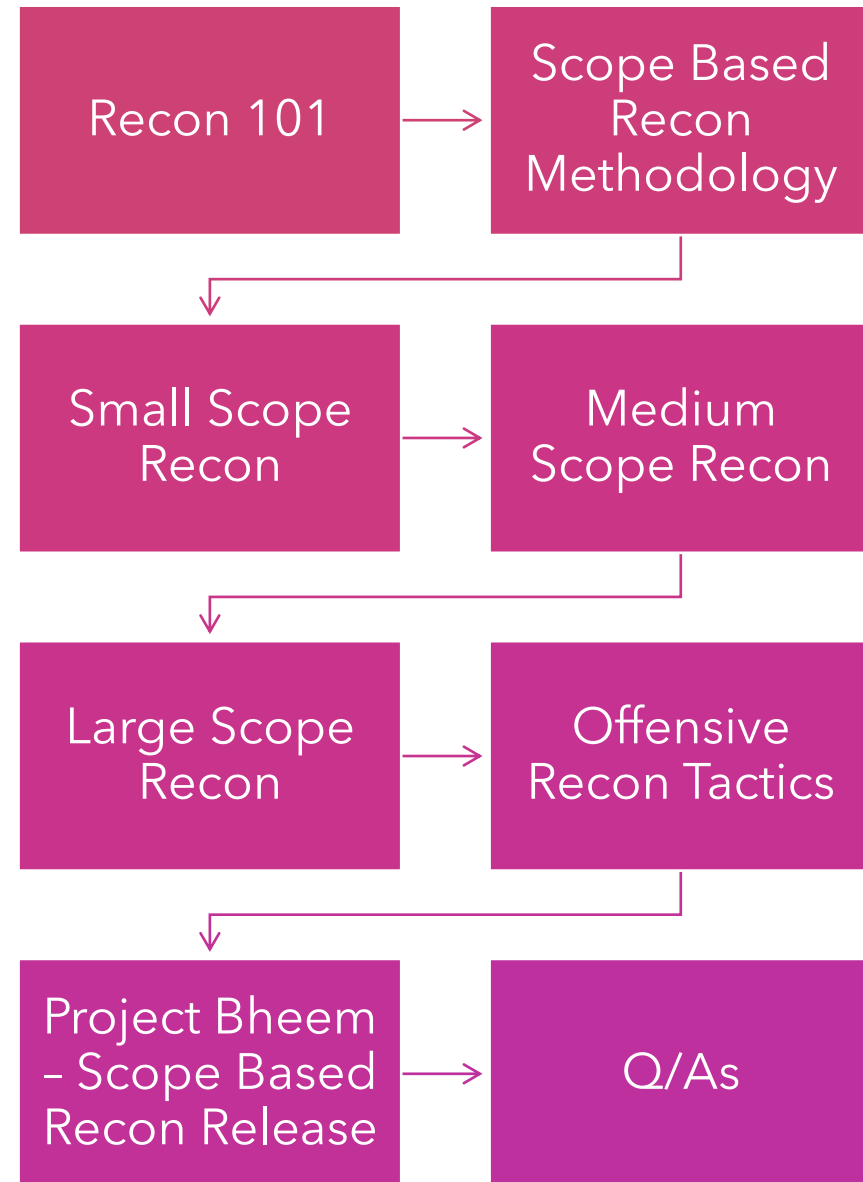
# OFFENSIVE & SCOPE BASED RECON

BY: HARSH BOTHRA

# WHO AM I?

- Cyber Security Analyst at Detox Technologies
- Synack Red Teamer
- Bugcrowd MVP 2020 Q1-Q2 & TOP 150 in Leaderboard
- Author - Multiple Hacking Books (R'cmd by AICTE, NITTTR-Chandigarh)
- Blogger | Speaker | Poet
- Lifelong Learner

# AGENDA



# RECON 101

## What is Recon ?

- Way to discover & create a better attack surface! (We'll see how)

## Why Recon?

- Increased Attack Surface == More Security Issues
- Looking at less travelled road == More Success
- Digging assets of your target to the deepest point possible.
- Recon != Security Issues but increases probability of getting >> Security Issues.

# BUSTING THE MYTHS

- Recon == Bugs
  - Recon == Asset Discovery == Increasing Attack Surface
- Recon == Manual Approach
  - Best way to perform Recon is to use hybrid approach – Automation + Manual
- Recon == Time Consuming
  - If performed properly & automated in right way, you can save a lot of time
- Recon == Subdomain Enum, Whois, Port Scanning & Fuzzing, etc.
  - Ways to perform Recon is all about how creative you can be to identify assets and increase attack surface. However, the above mentioned are some well known methods.

# SCOPE BASED RECON

- Scope Based Recon is a simply methodology to divide **How to Perform** when a specific set of **Scope** is Provided.
- Scopes are divided into three categories:
  - Small Scope
  - Medium Scope
  - Large Scope
- **Why Scope Based Recon?**
  - Saves a lot of time
  - You know what exactly to look for
  - You can easily automate your recon workflow
  - Less-chance to submit Out-of-Scope Issues
  - Just like other security methodologies enables you perform a better Recon

# SCOPES

## Small Scope

- Specific set of Single URLs/Sandbox/QA/Staging Environment

## Medium Scope

- Specific set of **"\*.target.com"**

## Large Scope

- Complete Internet presence including Acquisitions & Copyrights



# SMALL SCOPE RECON

## What to look for while performing Recon

- Directory Enumeration/Bruteforcing
- Service Enumeration
- CVEs
- Port Scanning
- Broken Link Hijacking
- JS Files for Hardcoded APIs & Secrets
- 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)



### **What to look for while Recon:**

- Subdomain Enumeration
- Subdomain Takeovers
- Misconfigured Third-Party Services
- CVEs
- Port Scanning
- Misconfigured Storage Options (S3 Buckets)
- Broken Link Hijacking
- Directory Enumeration

### **What to look for while Recon:**

- 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)

# **MEDIUM SCOPE RECON**

# LARGE SCOPE RECON

- **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 & SSL Enumeration
- CVEs
- 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.

# **SMART** ~~OFFENSIVE~~ RECON TACTICS



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

# **SMART** ~~OFFENSIVE~~ APPROACH FOR RECON

# PROJECT BHEEM

- Simple Bash Wrapper around pre-existing tools to implement Scope Based Recon Approach.
- Currently it supports all **three (small, medium & large) scope-based Recon with Parallel Processing.**
- Bheem Performs following Recon Activities:
  - Subdomain Enum & Takeover Search
  - IP Space Discovery
  - Reverse Whois
  - Domain Resolution
  - Github Search
  - Template Based Scanning via Nuclei
  - Directory Fuzzing
  - HTTP Request Smuggling
  - Screenshots
  - Potential URL Extraction
  - And few other functionalities



# PROJECT BHEEM DEMO

REPO LINK: [HTTPS://GITHUB.COM/HARSH-BOTHRA/BHEEM](https://github.com/HARSH-BOTHRA/BHEEM)

**Q/A ARE WELCOME**



GET IN  
TOUCH AT



**Website - <https://harshbothra.tech>**



**Twitter - @harshbothra\_**



**Instagram - @harshbothra\_**



**Medium - @hbothra22**



**LinkedIn - @harshbothra**



**Facebook - @hrshbothra**



**Email - [hbothra22@gmail.com](mailto:hbothra22@gmail.com)**

**THANKS...**