Offensive Recon – Bug Hunter's Playbook

BY: HARSH BOTHRA

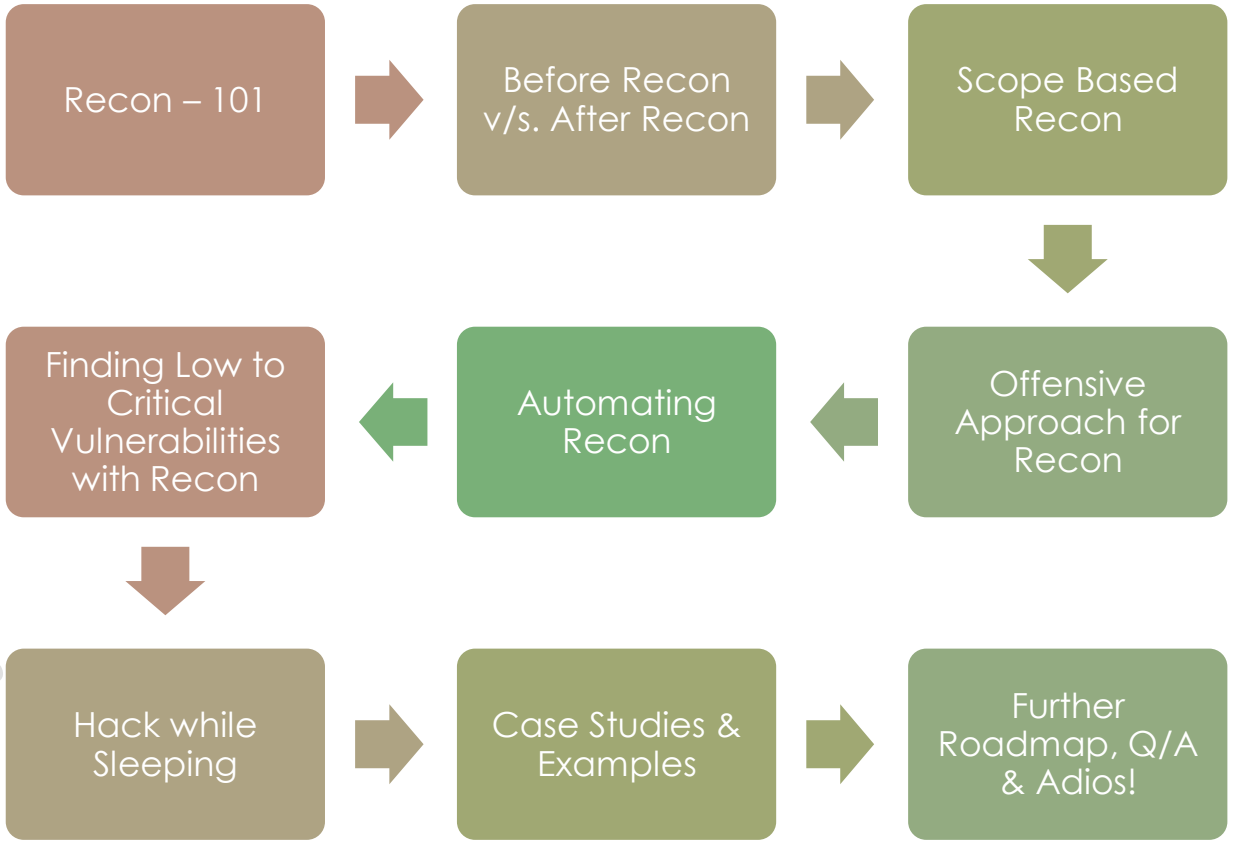
Who Am I?

- Security Engineer at Security Innovation
- 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

Existing Talks on Recon (For Basics & Brush-up's)

- https://t.co/Trr9mmk5lR?amp=1
- https://t.co/wPJnKhQzmx?amp=1

Agenda


Recon – 101
Before Recon v/s. After Recon
Scope Based Recon
Offensive Approach for Recon
Automating Recon
Finding Low to Critical Vulnerabilities with Recon
Hack while Sleeping
Case Studies & Examples
Further Roadmap, Q/A & Adios!

RECON – 101

WHAT . WHY . WHEN . WHERE . HOW

What we have (Before Recon) vs What we get (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….

Scope Based Recon

Small Scope
Specific Applications in scope.

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

Large Scope
Everything in Scope.

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.

Offensive Approach for Recon

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

Automating Recon

- Let's move to my arsenal and see How I utilize existing tools to automate things the way I want.

- Let's see how we can leverage the previously utilized tools & automation script to get some cool vulnerabilities.
    - There is no guarantee while hacking live, we will hit a bug right away. I am choosing some random target & things may take time.
    - It is to show an approach in a bigger picture.

Finding Low to Critical Vulnerabilities with Recon

Hack while Sleeping

- Automating your Recon over Cloud allows you to Hack while Sleeping.
- Here's what you need:
- A Cloud Service Provider (AWS, GCP, Digital Ocean, etc.)
- Create a VM & Install Necessary Tools (Create a re-usable Installation Script)
- Clone your Automation Scripts to Cloud
- Create a Linux Screen & Run your automation
- Exit & Enjoy !
- 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.

Case Studies, Further Roadmap & Hacking Tip'o'Tricks

Get in Touch at

- Website - https://harshbothra.tech
- Twitter - @harshbothra_
- Instagram - @harshbothra_
- Medium - @hbothra22
- LinkedIn - @harshbothra
- Facebook - @hrshbothra
- Email - hbothra22@gmail.com

@harshbothra_

Thank You