SCOPE BASED RECON FOR MUNDANE {BUG BOUNTY HUNTERS}

By: Harsh Bothra

~Alohomora ~ Who Am I ?

- Cyber Security Analyst at Detox Technologies
- Bugcrowd Top 150 Hackers & MVP 2020Q1
- Synack Red Teamer
- Author – Hacking: Be a Hacker with Ethics (GoI Recognized)
- Author – Mastering Hacking: The Art of Information Gathering & Scanning
- Blogger
- Int. Speaker
- Poet
- Explorer & Learner

AGENDA

- Recon 101
- Introduction to Scope Based Recon
- Small Scope Recon
- Medium Scope Recon
- Large Scope Recon
- Offensive Recon Methodologies
- Practical Recon
- Project Bheem – Alpha Release
- Hacks'o'HackTricks

RECON - 101

Understanding Recon

- Recon == **Increased Attack Surface ~=** More Vulnerabilities
- Recon == Finding Untouched Endpoints ~= **Less Dupies**

- Recon == Sharpening your Axe before Attack. BUT! Wait! We won't waste time into sharpening our bonds with EX. :p
- We will rather jump in to automate stuff as much as we can to reduce time consumption.

General Misunderstanding

- If I do Recon, I will get a lot of Vulnerabilities ?
  - Recon will help you increase attack surface, may allow you to get vulnerabilities but ultimate goal is to dig your target to deepest.
- Automated Recon is sufficient?
  - No, there are certain situations where you might need to look up manually like Github Recon, Google Dorking and others.
- Recon is a time consuming process so I avoid it, am I cool?
  - No, If you will try to play smart moves automating your Recon, you can do a lot of things!
- Recon is love bro!
  - Absolutely, Just like Chaai (Tea)

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....

@harshbothra_

SCOPE BASED RECON

The Masterplan to Play Recon Game

The Right Way

Scope Based Recon - Methodology

Small Scope	Single Application or Restricted Scope
Medium Scope	*.target.com or set of applications
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.

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

PRACTICAL RECON

PROJECT BHEEM – ALPHA

HACKS'O'HACKTRICKS

A Special Shoutout to ALL THE TOOLS & Resource Creators ... :D

(Apologies if I miss any, Efforts of Every single person is appreciated)

@TomNomNom
@owaspamass
@pdiscoveryio
@michenriksen
@securitytrails
@shmilylty
@shodanhq
@TobiunddasMoe

@jhaddix
@dxa4481
@GerbenJavado
@gwendallecoguic
@hakluke
@sa7mon
@jordanpotti
@hahwul

@0xAsm0d3us
@s0md3v
@Robert David Graham
@nmap
@zseano
@stevenvachon
@tillson
@m4ll0k

@_maurosoria
@j3ssiejjj
@OJ Reeves
@PortSwigger
@Anshuman Bhartiya
@Cody Zacharias
@EdOverflow
@imran_parray

* Few infographics are taken from Open Google Image Search and are not used for any promotional or paid activities.

Get in Touch at

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