WEAPONIZING RECON

FOR

FUN & PROFIT

Harsh Bothra

$ECHO(`WHOAMI`)

- Security Engineer at Security Innovation
- Bugcrowd Top 200 Researchers - All Time
- Synack Red Team Member
- Author - Hacking: Be a Hacker with Ethics
- Author - Mastering Hacking: The Art of Information Gathering & Scanning
- Blogger
- Occasional Trainer & Speaker
- Poet
- Lifelong Learner

GET IN TOUCH AT

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

AGENDA

Recon 101 - Demystifying the Recon Process	Recon with Google Dorks	Recon with GitHub Dorks	Recon with Internet as a Thing Search Engines	Recon with Web Applications
Automating Recon	Recon Automation Tools	Minimizing Recon - The better & efficient approach towards Recon	Automating Git Recon	Automating Content Discovery
Automating Recon with One-liners	Finding Vulnerabilities with One-liners	Setting up Cloud for Recon and Doing Recon while Sleeping	Wrapping Up	End Notes

//LET'S GET STARTED//

RECON 101

LET'S TALK ABOUT

- WHAT IS RECON?
- WHY YOU NEED TO DO RECON?
- RECON IS COMPLEX? NO WAY, IT'S JUST CREATIVE
- RECON FOR BUG BOUNTY - HOW USEFUL IT HAS BEEN?
- 20FT OVERVIEW OF RECON PROCESS
- WHAT.. WHY.. WHEN.. WHERE.. EVERYTHING HAS ONE SOLUTION - RECONNN..... :D

MY RECON PHASE

- Open Source Intelligence
- Search Engine Dorking
- Git Recon
- Content Discovery
- Semi-Automating Recon
- Automating Complete Recon Workflow
- Hack The World..... :D

OSINT - OPEN SOURCE INTELLIGENCE

- Target Fingerprint - Knowing your Target Better
- Acquisition Mapping
- Information Harvesting for Social Engineering

> End Goal // Get to know your Target Better....!!

> Let's See it in Action....

SEARCH ENGINE DORKING

- Google Dorking - It is Most Important, don't Ignore
- Other Search Engines - Never Ignore them, Results Differs
- Shodan
- Censys
- Sypse
- Fofa.so
- Binary Edge

GITHUB RECON

- Gathering Company Information
- Manually Approaching Github Recon using Dorks

- "target" <dork>
- Ex: "google.com" password

CONTENT DISCOVERY

- Subdomain Enumeration
- IP Space Enumeration
- Reverse Whois
- Parameter Discovery
- Hidden Content Discovery
- Directory Brute forcing
- JavaScript Link Analysis
- Buckets & Online Resources (Third Party) Discovery

SEMI-AUTOMATING RECON

- Using Tools to automate Recon Phases:
  - Subdomain Enumeration: Amass, Assetfinder, Subfinder, OneforAll, Aquatone, etc.
  - IP Space Enumeration: Amass is sufficient
  - Reverse Whois: Amass is sufficient
  - Parameter Discovery: Arjun, ParamSpider, ParamMeth

AUTOMATING VULNERABILITY SCANNING

- To automate all the process with one tool, saving time and enjoy, use::

OSMEDEUS

HACK THE WORLD..... :D

- Once you have all the information, it is time to hack the stuff.. Isn't it?

////Let's Hack the World////

RECON WITH WEB BASED TOOLS

HTTPStatus

Hardenize

Mxtoolbox

Security Trails

Netcraft

Chaos

AUTOMATING GIT RECON

- Githound
- Githound Filters

AUTOMATING CONTENT DISCOVERY

- Js Link Analyser
- Waybackurls
- ParamSpider
- Arjun

AUTOMATING VULNERABILITIES WITH ONELINERS

- Let's Create some On-spot Oneliners Like

```
cat domain.txt | httpx <options> | grep "200" | cut -d [ -f 1 |
sort -u | tee output.txt
```

SETTING UP CLOUD FOR RECON & HACKING WHILE SLEEPING

Cloud Options - GCP, AWS, Azure, DigitalOcean

Recommended - GCP/Digital Ocean

How to Configure - Out of Scope of this talk

How to Utilize- Let's see in the Action..

RECOMMENDED & LIMITED TOOLS :D

Osmedeus	Nuclei	HTTPX	Dirsearch
Githound	Tomnomnom Hacks	Dalfox	ParamSpider
GF	Linux Command Line Tools	Assetfinder, Amass, Subfinder, Subjack, Sub-tko	Waybackurls

WRAPPING UP & END NOTES

- Further Readings and Resources :
- https://medium.com/@ehsahil/recon-my-way-82b7e5f62e21
- https://medium.com/bugbountywriteup/recon-everything-48aafbb8987
- https://0xpatrik.com/asset-discovery/
- https://docs.google.com/spreadsheets/u/0/d/1TxNrvaIMRS_dmupcwjwJmXtaFk_IPGE1LzgxPu_7KqA/htmlview
- https://pentester.land/list-of-bug-bounty-writeups.html
- And Trust me, Twitter is the Best Resource among ALL... :D

Happy Hacking