Weaponizing Recon

SMASHING APPLICATIONS FOR SECURITY VULNERABILITIES & PROFITS

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
- Recon for Pentesters & Bug Bounty Hunters
- Attack Surface (AS) & Attack Vectors (AV)
- Mapping AS & AV with Recon
- What we have vs What we get
- Building Recon Arsenal
- Weaponizing your Recon Game
- Automating Recon
- Finding Vulnerabilities with Recon
- Smart Recon a.k.a. Recon Hacks 101
- Creating your own Recon Workflow
- Example of Easy Wins from Recon
- Final Notes and Further Roadmap

RECON 101

- What
- Why
- When
- How

Of Recon

RECON FOR PENTESTERS & BUG BOUNTY HUNTERS

- How Recon is useful for Bug Bounty Hunter & Pentesters
  - Finding Hidden Endpoints
  - Increasing Attack Surface
  - Discovering More Assets
  - Exposed IoT Services/Devices
  - Exposed Sensitive Directories
  - Exposed Internal Domains/Source Code/Secrets
  - Accessing the limited/restricted resources

    More Assets == Bigger Attack Surface == More Vulnerabilities
  - (But wait, what are those assets you are talking about???)

ATTACK SURFACE (AS) & ATTACK VECTORS (AV)

- Attack Surface - Areas, Endpoints, and every accessible point where an attacker can perform any potential vulnerability assessment which may impact C.I.A. .
- Attack Vectors - The possible methods an attacker can use to impact C.I.A. in the available attack surface.
- Why Mapping Attack Surface is Necessary?
  - Most of the people don't do it.
  - Allows you to keep a track of all available options you must test and thus gives you a better visibility.
  - Allows you discovery more hidden endpoints and content discovery.
  - You won't miss any endpoint for sure.
  - Organized approach especially when testing a huge scope target and helps you when you revisit the target later.
  - Allows you to craft Attack Vectors accordingly and Saves a lot of time
  - & Obviously, keeps you one step up than your competition.

MAPPING AS & AV WITH RECON

- Now, it is important to know how recon can help you map your AS & AVs. This is something that you can look at while trying to map AS & AVs:
  - Based on Scope - (Small vs Large Scope)
  - Based on Internet Presence (Github, Search Engines, OSINT Based AV are high there)
  - Based on Asset Type (Is it a unique business logic or just another file upload functionality, you know how to hit it right?)
  - Based on Visual Inspection (Visiting every functionality and looking for viable test cases for each functionality)

  Let's Understand all of these with the help of examples.

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....

BUILDING RECON ARSENAL

/// Here we will talk about the process we need to carry out during recon and tools and services that will help us speed up things ///

/// TOOLS THAT I USE ///

- Subdomain Enumeration
  - Assetfinder
  - Amass
  - Subfinder
  - Aquatone
  - Chaos.projectdiscovery.io
  - Securitytrails.com
  - OneForAll
- Intel Gathering
  - Amass
  - Whois
  - Shodan
  - Github
  - Search Engine Dorking

/// TOOLS THAT I USE ///

- Directory Bruteforcing/Content Discovery
  - dirsearch
  - fuff
  - gospider
  - gobuster
  - Burp Suite :D with appropriate lists
- Subdomain Takeovers
  - Subjack
  - Aquatone
  - Tko-subs
  - Can-i-takeover-xyz (for a quick reference for manual reference)

/// TOOLS THAT I USE ///

- Parameter Discovery
  - Arjun
  - ParamSpider
- Port Scanning & Vulnerable Service Identification
  - Nmap
  - Masscan
  - Naabu
- Github Recon/Leak Finding
  - Githound
  - Secret Finder
  - Gitrob
  - Trufflehog
- JS Link Analysers
  - JS-Scan
  - Burp JS Link Finder
  - Link Finder

/// TOOLS THAT I USE ///

- Useful Scripts & Tools to Automate Recon
  - Httprobe
  - Waybackurls
  - Tomnomnom's Hacks
  - gwen001/pentest-tools
  - Hakluke's Scripts (Hakrawler and others)
  - Dalfox
  - GF
  - GAU
  - S3Scanner
  - AWSBucketDump
- Online Services & Search Engines
  - Shodan
  - Censys
  - Fofa.so
  - Binaryedge
  - Google/Bing/DuckDuckGo
  - Github/BitBucket Search
  - Hardenize.io
  - Httpstatus.io
  - Mxtoolbox.com
  - Postb.in
  - Crunchbase
  - Owler
  - Wikipedia

WEAPONIZING YOUR RECON GAME

- Remember, using each tool is always not a good idea. It is overwhelming and sometimes is just a waste of resources. It is essential to see what tools fit in to your arsenal and recon approach and use them accordingly.

>> Now, we know everything that we need to hit our target, the next things is Let's see some of these tools in action and start weaponizing your Recon GAME <<

AUTOMATING RECON

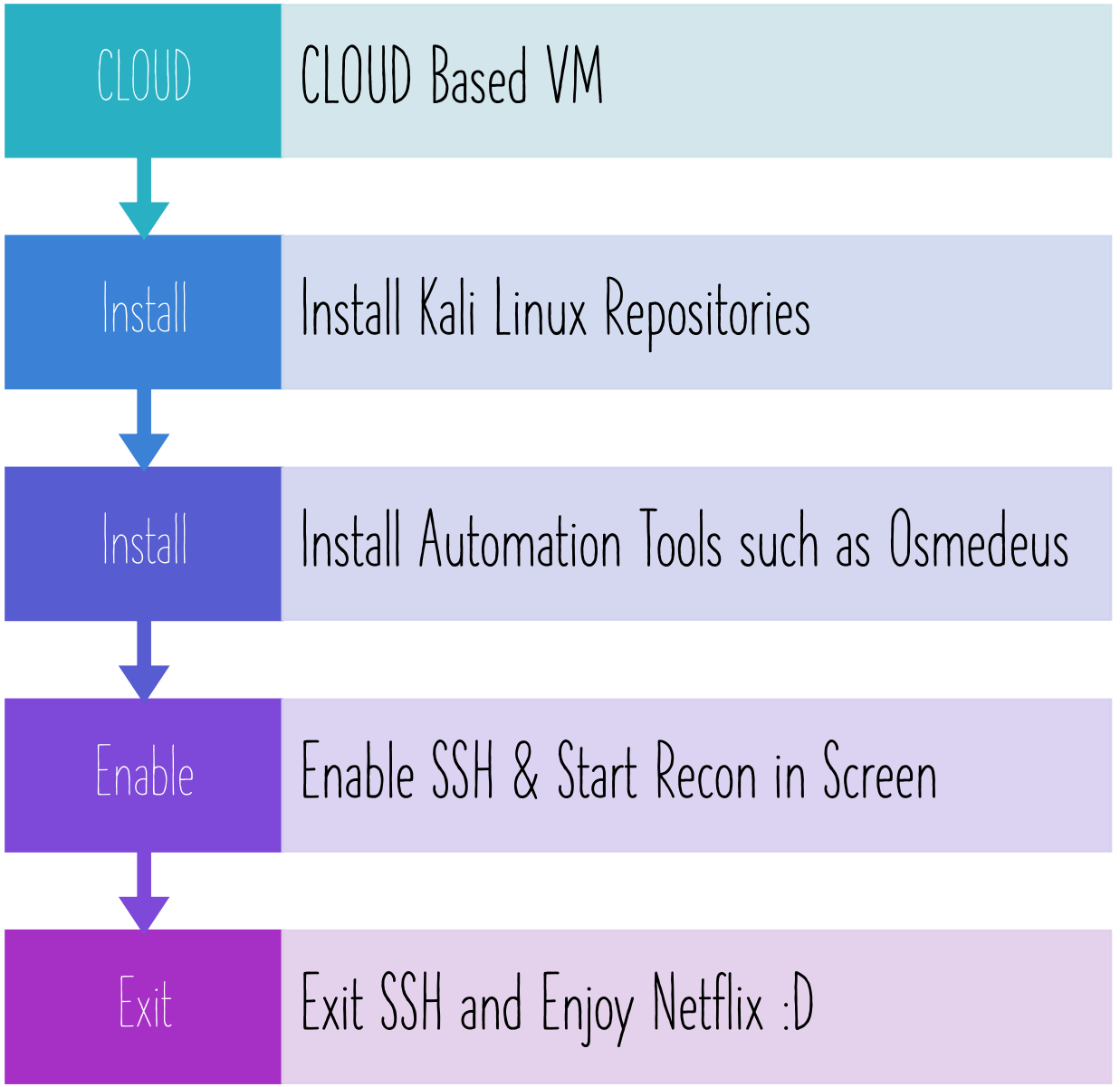
- Sudomy
- TotalRecon

/// OSMEDEUS & Nuclei /// (My Personal Favorite)

(Big up to @j3ssiejjj & @projectdiscovery.io)

HACKING WHILE SLEEPING

@harshbothra_



Let's See this in Action...

FINDING VULNERABILITIES WITH RECON

- Let's see how can we automate finding some of the interesting vulnerabilities.
- Reflected XSS
- Open Redirect
- SQL Injection
- SSRF
- SSTI
- LFI/RFI

(Automation doesn't guarantee finding a vulnerability. It may miss or produce false-Ps. It is just to aid the Pentesting and not missing something obvious).

WRITING YOUR OWN ONE LINERS

/// Let's see how you can use simple bash tools to write your own one-liners and automate things on the go ///

RECON HACKS 101

- Automate as Much as you Can but never ignore looking manually if you have time.
- Learn using Linux utilities and scrape useful information out of the data gathered.
- Modify your Recon methodology according to your target and do a target-specific recon for quick, better and efficient results.
- Do not just limit yourself to what you see or what you read! Recon is all about being creative and thinking out of the box. Apply your own logics, it's okay to fail but happiness when it gives unexpected results. :D
- Write your own bash wrappers including the tools you like to automate the use of all the tools and save your time performing multiple actions.
- Keep your recon on a Cloud VM so that your CPU consumption stays free and hack on the main application for OWASP TOP 10 or SANS 25 while you get something from Recon.
- Keep Researching new tools, test them on known vulnerable (real-world) targets and check their efficiency. If some tool looks go, add them to your workflow and integrate with your own scripts/wrappers/one-liners.

CREATING YOUR OWN RECON WORKFLOW

/// Let's see how we can create our own Recon Workflow for being for target and scope specific & not waste our time ///

SOME EASY RECON WINS.....

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
@0J Reeves
@PortSwigger
@Anshuman Bhartiya
@Cody Zacharias
@Ed0verflow
@imran_parray

Q/A ARE WELCOMED...

YOU CAN REACH OUT TO ME POST TALK AS WELL AND WILL TRY TO ANSWER AT EARLIEST ☺

HAPPY HACKING HACKERS ... :D

/// THANK YOU ///