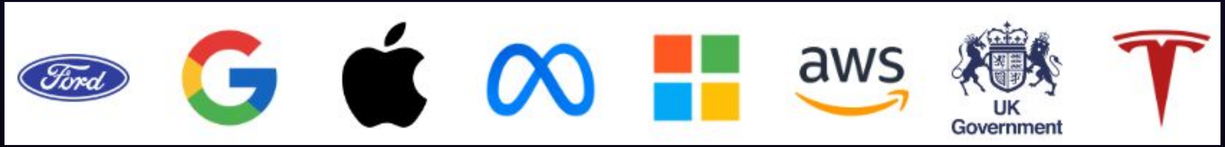
My Learning Path for Bug Bounty as a Beginner

Intro

- Security Researcher

- Cyber Defense Analyst at Ford

- Received recognition from the following organizations for reporting Application Security Risks.



What is Bug Bounty?

- It's a program offered by organizations that rewards individuals for identifying and reporting security vulnerabilities in their software or systems.

- It can be considered a form of freelancing. (Unlike traditional freelancing)

- Vulnerability should be reported separately (one by one) and based on severity companies will give rewards.(Bounty/Hall of Fame/Letter of appreciation/Swags)

- To get started, basic knowledge in cybersecurity and bug hunting methodologies is required.

- The goal of a bug bounty program is to identify and fix security issues before they can be exploited by attackers.

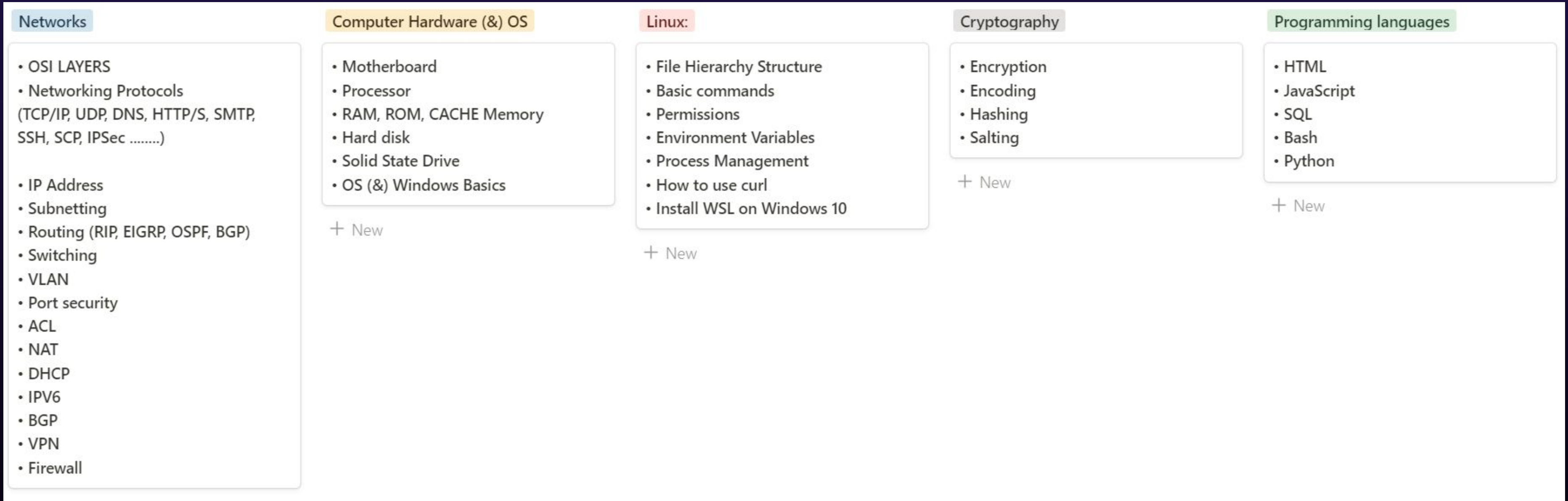
Why Bug Bounty?

- Bug bounty programs are beneficial for companies as they provide an additional layer of security to their products.

- Companies get access to a wide pool of security experts who can find and report vulnerabilities, while researchers get paid and recognized for their work. This can lead to a more secure software development process, as well as the discovery of new and previously unknown security threats.

- Bug bounty programs also help to build trust with customers, as they demonstrate that the company takes security seriously and is willing to invest in protecting their customers’ data.

Basics Learned



Networks

- OSI LAYERS
- Networking Protocols (TCP/IP, UDP, DNS, HTTP/S, SMTP, SSH, SCP, IPSec ....)

- IP Address
- Subnetting
- Routing (RIP, EIGRP, OSPF, BGP)
- Switching
- VLAN
- Port security
- ACL
- NAT
- DHCP
- IPV6
- BGP
- VPN
- Firewall

Computer Hardware (&) OS

- Motherboard
- Processor
- RAM, ROM, CACHE Memory
- Hard disk
- Solid State Drive
- OS (&) Windows Basics

Linux:

- File Hierarchy Structure
- Basic commands
- Permissions
- Environment Variables
- Process Management
- How to use curl
- Install WSL on Windows 10

Cryptography

- Encryption
- Encoding
- Hashing
- Salting

Programming languages

- HTML
- JavaScript
- SQL
- Bash
- Python

Resource link: https://github.com/samjoy26/bug-bounty-beginner-learning-path/blob/main/Basics_Learned.md

Choose a path based on your interests

- Web Application
- Android Application
- IOS Application
- Code review
- Hardware Testing

Note: I have not listed all.

Steps I have followed to Get Started

- Choose a vulnerability to learn. (Any)
- Start with the necessary fundamentals before learning about vulnerability.
- Summarize what you learned in a Note taking Application.
- Simultaneously prepare test cases
- Research methodologies that can be used to increase the severity.
- Practice on testing labs until you get familiar.
- To start, choose a responsive VDP program you love and stick with it.
- Repeat the steps for each vulnerabilities.
- Once you gain confidence, go for competitive bug bounty programs.
- While in progress, don't lose your pace, never compare yourself to others, and keep hunting for fun.

Discovering My Bug Bounty Journey: What I've Learned

- Don't rush, mastering it takes years.

- Maintain your pace and coolness while learning and practicing until you become familiar.

- Take care of your health and manage your time wisely.

- Learn how to Recon. (Start with Google Dorks)

- Utilize Twitter as a learning resource to stay informed and up-to-date.

- Contribute ideas and learn together. Sharing is crucial for growth. I learned the most from the write-ups of other researchers. (Thanking all researchers for sharing their knowledge.)

- Enjoy the journey of bug bounty hunting, rather than just focusing on the end goal.

Thank you