Reverse Eng with Ghidra & MCP

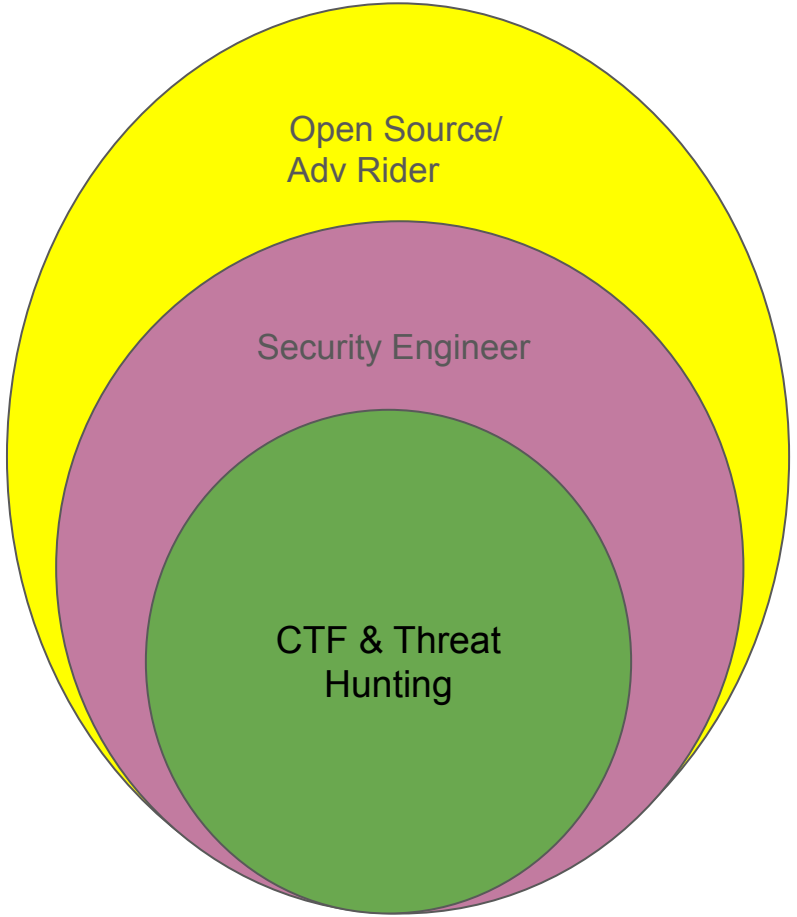
Analyze compiled code without source access

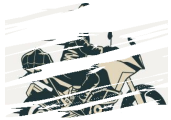
$whoami

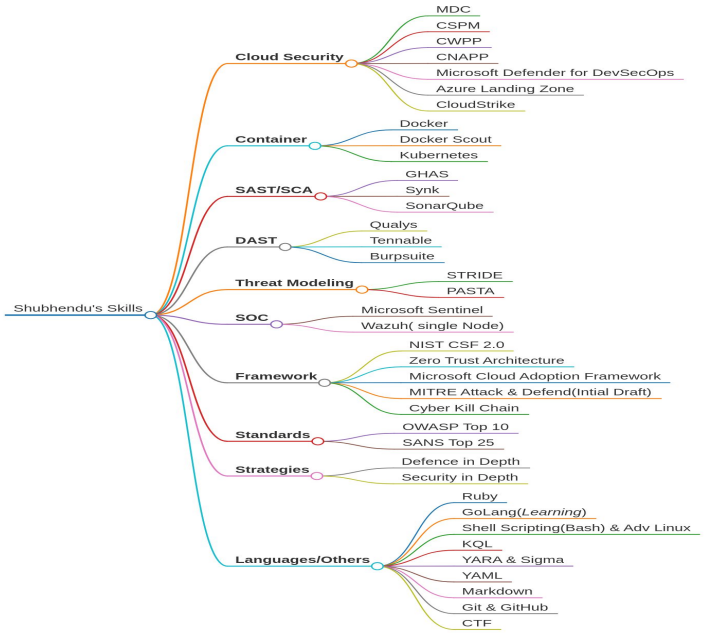
Shubhendu Shubham

"sudo rm -rf / problems"

aka "Troubleshooter"






Shubhendu's Skills
Cloud Security
MDC
CSPM
CWPP
CNAPP
Microsoft Defender for DevSecOps
Azure Landing Zone
CloudStrike
Container
Docker
Docker Scout
Kubernetes
SAST/SCA
GHAS
Synk
SonarQube
DAST
Qualys
Tennable
Burpsuite
Threat Modeling
STRIDE
PASTA
SOC
Microsoft Sentinel
Wazuh(single Node)
Framework
NIST CSF 2.0
Zero Trust Architecture
Microsoft Cloud Adoption Framework
MITRE Attack & Defend(Intial Draft)
Cyber Kill Chain
Standards
OWASP Top 10
SANS Top 25
Strategies
Defence in Depth
Security in Depth
Languages/Others
Ruby
GoLang(Learning)
Shell Scripting(Bash) & Adv Linux
KQL
YARA & Sigma
YAML
Markdown
Git & GitHub
CTF


HACKTHEBOX
Subject
Matter
Expert
SME


JUST ANOTHER KUSTO HACKER
JUST ANOTHER
2025
KUSTO HACKER


ATTACKIQ
Attack Flows
How to Model and Sequence Attacks


OffSec
OSCC
SEC-100


CTF BADGES
CERTIFICATIONS
WINNER
AZURE NETWORK ENGINEER
ASSOCIATE
AZURE SECURITY ENGINEER
ASSOCIATE
EXPERT
EXPERT
ASSOCIATE
SC 100
AZ 305
AZ 104
AZ 700
AZ 500

Community


Azure Developer
Community


docker


KALI
BY OFFENSIVE SECURITY


OffSec
The Path to a Secure Future™

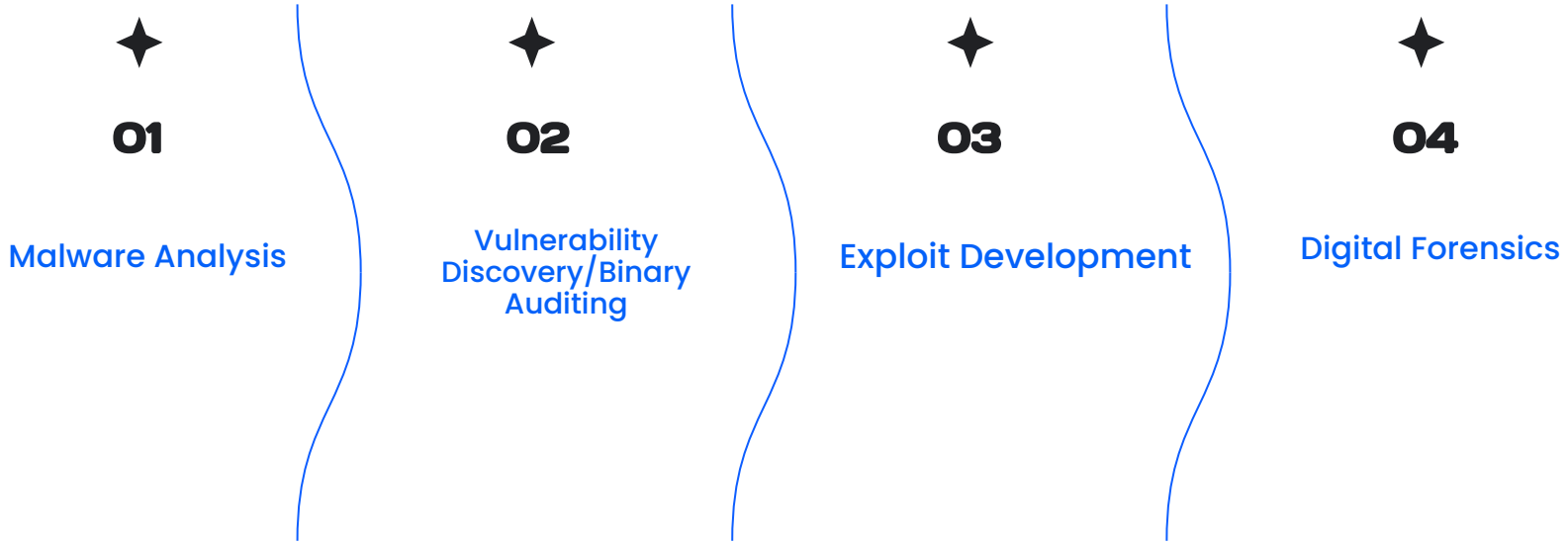
Disclaimer!

"Everything is Open source

If you know how to Reverse."

— not sure

Unify Reverse & Engineering



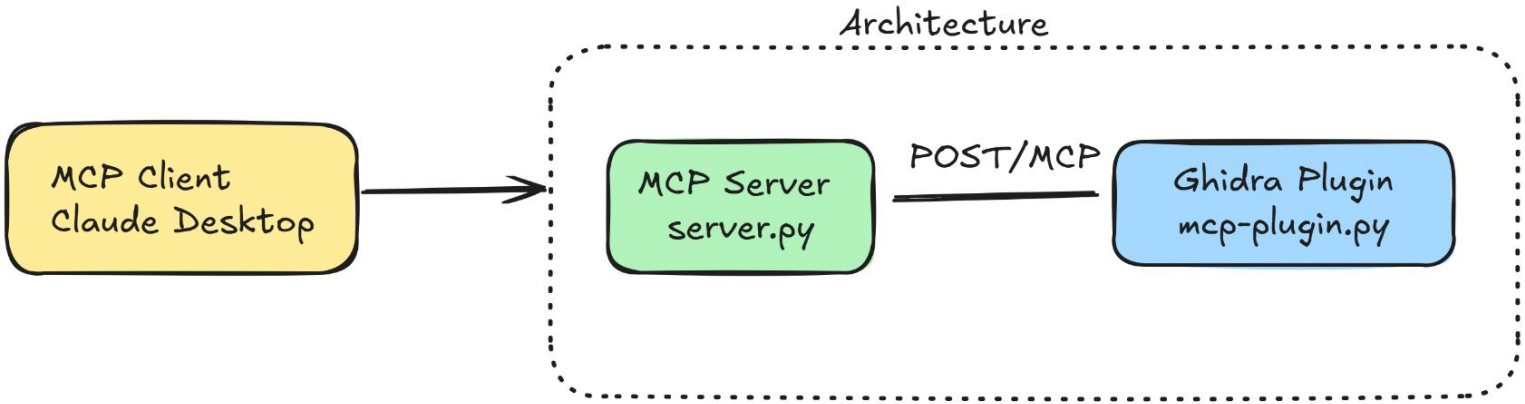
GHIDRA

- A software reverse engineering (SRE) framework.

- Origin: Created and maintained by the National Security Agency (NSA) Research Directorate. Publicly released at RSA Conference 2019. Source code released on GitHub and Ghidra website

- This toolset offers a powerful suite for reverse engineering, featuring open-source accessibility with a built-in decompiler. It supports diverse platforms like Windows, macOS, and Linux, accommodating various processor architectures and executable formats. Designed for scalability, it efficiently handles large firmware images while enabling collaborative analysis. Version tracking ensures consistency across different binary versions, and its extensibility allows users to develop custom scripts or components using Java or Python. With advanced analysis features, including a high-end decompiler, it provides comprehensive software investigation capabilities.

Architecture



Prerequisites

- Node js
- JDK 20 +
- MCP client
- Python 3 +
- Ghidra

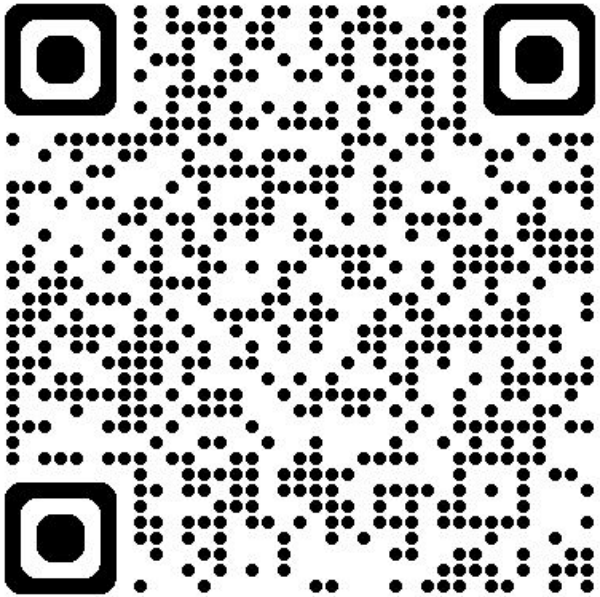

@lol_me
Arey kahena kya chahte ho?

References

1. GitHub - LaurieWired/GhidraMCP: MCP Server for Ghidra
2. Crackmes
3. GitHub - NationalSecurityAgency/ghidra: Ghidra is a software reverse engineering (SRE) framework
4. Introduction - Model Context Protocol
5. Ghidra S/w Reverse Engineering book - A. P David

Thank you!

Not a Phishing QR
It's my **LinkedIn**
Don't Trust
Always verify



FAI

docker