Harith Dilshan

Personal

Name

Birthday

Email

Address

Telephone

Qualifications Skills

- Mobile Security
- AppSec
- Scripting
- Red Teaming
- VA
- Hardware Security
- Telco Security
- API Security
- Cloud Security
- Exploit Writing
- Network Security
- Web App Security
- Reverse Engineering

Hobbies

Codinng & Reversing

Learning new things

github.com/h4rithd | linkedin.com/in/harithdilshan | https://h4rithd.com

Objective

Obtain a challenging leadership position applying creative problem solving and learn management skills with a growing company to achieve optimum utilization of its resources and maximum profits.

Working Experience

Senior Application Security Engineer | Wiley 2022 - Current

- Perform dynamic application security testing (DAST).
- Perform static analysis (SAST) of the micro-services and Web applications codebase.
- Discover, prioritise, and help remediate technical risks on features, products, and infrastructure.
- Perform threat assessment on existing and upcoming features and releases.
- Develop and own best practices for application security, development, and deployment (CI/CD).
- Identify and assess vulnerabilities stemming from third party dependencies.
- Collaborate with other engineers, PMs, and designers.
- Lead penetration testing engagements and create new testing methods and exploits.

Senior Executive Cyber Security Engineer | Dialog Axiata PLC 2019 - 2022

Engaged Red Teaming operations. Consulting SOC operations, Vulnerability Assessments and Penetration Testing for Mobile, Web, API, Cloud based services and digital telecommunication platforms.

Main Responsibilities:

- Performing Penetration Tests Red Team activities on the full Dialog Axiata Internal and External Landscape.
- Experienced with Burpsuite Pro (Proxy/Intruder/Repeater/Sequencer/Decoder etc...)
- Vulnerability Scanning with Acunetix, Tenable/Nessus, Core Impact and Netsparker.
- Penetration Testing a wide range of technologies:
  - Mobile : React native, Kotlin, Xamarin, Dart, Android
  - Web : SAMLv2 SSO, Single Page or Multiple Application, eCommerce, Payment Gateway testing (Genie/eZCash/Finpal).
- MITRE ATT&CK Tactics and Techniques
  - Experienced with Adversary Simulations (Cobalt Strike)
- Network Penetration Testing Corporate Switches/Routers/Firewalls/Hosts as well as VPN, DNS, VoIP.

Associate Cyber Security Engineer | Crypto-Gen 2018 - 2019

Engaged in cyber security functions at Dialog Axiata (outsourcing) bind to the internal cyber security team. My primary task is to conduct penetration testing for 100 + mobile applications and web applications. Further, security assessments in API security and cloud based services security are conducted.

Junior Penetration Tester (Intern) | Crypto-Gen 2018 - 2019

Professional Qualification

Offensive Security Certified Professional [OSCP] 2022
Certification Number : OS-101-60003
Verified : https://bit.ly/oscp-harith

CyberWarFare Labs Certified Red Team Specialist [CRTS] 2022
Verified : https://bit.ly/crts-harith

Certified Penetration Testing Professional V1 [C|PENT] 2021 - 2024
Certification Number : ECC4871203956
Verified : https://bit.ly/cpent-harith

HackTheBox Dante - ProLabs 2021
Full Name : S<dot>A<dot><space>Harith<space>Dilshan
Certification Number : HTBCERT-95AEE2648A
Verified : https://bit.ly/dante-harith

Certified Ethical Hacker Master V10 [C|EH] 2020 - 2023
Certification Number : ECC0276391485
Verified : https://bit.ly/ceh-harith
I got 8th place on CEH Master TOP 10 IN THE WORLD http://bit.ly/ceh-top10

Education

Graduated

BSc(Hons)in Information Technology - Specializing in Cyber Security
-- Sri Lanka Institute of Information Technology.

High School

Physics, Mathematics, Chemistry

Call : Email :

Project Experience

Capture The Flag VirtualBox (H0rcrux) 2018

This H0rcrux box is a OpenBSD based boot2root box as well as the hybrid one.it was created for a recent hackthebox ctf competition and the final goal is destroy the horcrux. This box contains 12 flags and updated with all the security patches.Basically this includes the challenges such as steganography, cryptography, reverse engineering, ACL authentication and port knocking.

Download : https://bit.ly/horcrux-ctf

Next Generation Malware (AlienGate) - Research Publication 2019

Develop a next generation which can bypass the malware identification mechanism and malware protection methods currently in use and next generation firewalls too.The malware can bypass traditional firewalls with polymorphic signatures which can change the signature time to time.

RouterSpace - CTF Machine for HackTheBox Platform 2022

RouterSpace is an easy Linux machine that uses remote code injection to gain access to the system through android application. Since incoming and outgoing traffic has been eliminated from iptables firewalls, user can not get a reverse shell. After doing some enumerations, there is a ssh key which has read permission. After receiving the ssh key file, can log in to the system using ssh. To escalate privileges, need to use Heap-Based Buffer Overflow in Sudo (Baron Samedit) CVE-2021-3156. by using the poc given in github, able to get root access to the system.

View : https://bit.ly/RouterSpace

Extra-Curricular Activities

- Participated at Provincial School Educational Software Competition 2011

Acknowledgement

- Acknowledgement from Avira Operations Germany for disclosing a vulnerability and a possible attack vector

Reference

[redacted]

Blur parts will appear due to the sensitive information.
Direct message me through linkedin for full version of the resume.

I confirm that the information given above is true and correct to the best of my knowledge. I am aware that in the event of this information being found factually incorrect prior to my selection, I am liable to be disqualified or I am liable to be summarily dismissed without

Sincerely,

....

Harith Dilshan