Perumal Jeganatharavi

perumalnetworkeng@gmail.com / +91 9566698516 / 5-4/45,Sowdeshwari Nagar, Elampillai, Salem, Tamil Nadu

Summary

I am **an ardent fan of Cyber Defense**. The **Tactics, Technics & Procedures** behind cyber threats, attacks & malware enthrall me. **Cyber Security is a never ending battle between The good & The Evil. I am proud to be one of the soldiers in the battlefield fighting for the good.**

My focus is on learning new concepts,ongoing issues & the future technologies every day and to become a skillful techie. I am also a believer of Learning through Knowledge Sharing. Hence, I have been **creating Information security contents on YouTube platform.**

Social Media

1. **YouTube Channel** - https://www.youtube.com/c/perumaljegan
2. **Website - https://perumaljegan.com**
3. **Twitter** - https://twitter.com/realperumalj
4. **LinkedIn** - https://www.linkedin.com/in/perumal-jeganatharavi-a890121b2/
5. **GitHub** - https://github.com/perumal-j

Experience

Senior Engineer - Information Security

Rakuten Symphony India • Bangalore, Karnataka
05/2022 - Present

1. I have been a part of the "**Rakuten Mobiles - Security Operations(Detection Engineering)** team" for past 10 months.
2. Our **Detection Engineering team does both Offensive & Defensive security operations**.Hence, It is like a **purple team**.
3. I do **craft logics & rules on "Anvilogic + Splunk"** platform **to detect the malicious/suspicious behaviors** in the endpoints(both Windows & Linux).
4. I **write sigma rule for the threat scenarios** & do the conversion to Splunk and deploy.
5. I **test the efficacy of created rule using Red Team Threat emulation frameworks** like **"Atomic Red Team","Caldera"**. Conduct manual tests (If Required).
6. I work with the fellow security teams during the critical times to prevent or respond the security incidents.
7. **I conduct Penetration Testing** on Internet exposed Rakuten Mobiles applications & services to spot the flaws & vulnerabilities, Then I **report the identified glitches to the concerned team**.
8. By observing the ongoing attacks,threats and its behaviors, I do **create Threat Actor profile and write detection rule.**

Information Security Analyst

GlobalFoundries Inc,. • Bangalore, Karnataka
04/2020 - 04/2022

1. I worked as **Information Security Analyst** in **Cyber Defense Operations Center - Globalfoundries Inc,.** for 2 Years.
2. I was looking for anomalies & suspicious activities files on the network & endpoints with help of **SIEM, EDR** & **SCCM** solutions.(SIEM : Secure Works & EDR: Red cloak)
3. Examining the threats found,**Simulating MITRE Framework & Killing the attack chain.**
4. **Performing Windows Registry Forensics** with tools **Registry Explorer, Shell Bag Explorer, Appcompatcacheparser** & Other Eric Zimmerman's tools.

5. Analysing Phishing mails, attempts & Malware samples, Collecting **Indicators Of Compromise (IOC)** & **Framing Malware Heuristics.**
6. Prevent the foreseen threats by bolstering the network defense with IOC. & Eradicating the threats found on the network , servers & End points (By following **Cyber Kill Chain**)
7. Engaging with Cyber Community, collaborate regarding the threats, attacks underway & mitigation for the potential security incidents.
8. Responding to the security incidents by following **Incident Response Life Cycle**.
9. Collecting samples from deployed honeypots, & Cyber community, **assessing potential malware's heuristics, behaviors & IOC**.

Systems Engineer

Tata Consultancy Services (TCS) • Chennai, Tamil Nadu
01/2017 - 03/2020

1. I was a part of **Security Operations Center (SOC)**. Where, I had been managing various firewalls (Palo Alto, Cisco ASA, Fortigate, & Checkpoint),.
2. Suggesting Secure network designs & Firewall vendors based on Project requirements.
3. Carried out the firewall Initial Configuration, Deployment, Addressing Post deployment issues & the management till the project wind up.
4. Handled Wireless Operations (Wireless LAN Controllers & Access Points)
5. Provided Level 1 Network Support.

Independent Information Security Content Creator

Youtube
10/2020 - Present

1. Making video lectures, tutorials about Information Security concepts via Online Platform **YouTube**.
2. **Production Samples :**

- Ransomware Forensics using ProcDOT | BlackMatter Ransomware //Malware Analysis - https://youtu.be/IK50aW9J5Wg
- Learn Wireshark... | It is FREE | Network Analyzer // Perumal Jegan - https://youtu.be/YruzUnB0NWs
- LunchBreaker CTF | Penetration Testing | VulnHub // Perumal Jegan - https://youtu.be/ZXvkDSKtTzk
- Log4j(Log4shell) Vulnerability Explained //TryHackme-Solr - https://youtu.be/7jt1NC5rgAc
- Reversing & Exploiting A Vulnerable Binary | DearQA //Binary Exploitation https://youtu.be/b4fIL48bTWI
- Remote Access Trojan (RAT) Analysis | Deobfuscating VBScript //Malware Analysis https://youtu.be/8z7nOCbdp-8
- CVE-2022-1388 : Remote Code Execution Vulnerability Explained | F5 BIG-IP - https://youtu.be/KsNX9M-6rn0
- Abusing Windows Internals - Part One | ShellCode Injection | Process Hollowing - https://youtu.be/3FqpZuaIzpY
- Phishing Email Analysis - Part 1 | Travel of an Email | Header Analysis //Perumal Jegan - https://youtu.be/Uo_47Ez8un4
- Linux Forensics //TryHackMe -https://youtu.be/dl0WAK3JAtU
- Email Security Techniques | SPF | DKIM | DMARC | Part4 //Perumal Jegan - https://youtu.be/LCIHGYxE5eM
- Windows Registry Forensics | Data Acquisition & Tools to Use | Part-1 //Perumal Jegan - https://youtu.be/hRKAJ04jwo4
- Serpent Backdoor | Analysis of a Unique & Peculiar Malware //Perumal Jegan - https://youtu.be/KeG9p7Mrwpg
- VS Code - Supply Chain Attack Explained - https://youtu.be/osdmHkReuD0

Skills

Linux, Windows, Information Security Content Creation - YouTube, Incident Response, SSL, Penetration Testing with Nmap,FFuF,Burpsuite,etc., Wireshark, SIEM (Secureworks), EDR (Red Cloak), Vulnerability Assessment with Qualys & Nessus, Risk Assessment, Problem Solving, Open Source INTelligence (OSINT), Computer Forensics, Firewalls & Proxies, Capture The Flag (CTF), Regular Expression, Docker, YARA, log4j Assessment, Malware Analysis, Phishing Email Assessment, Analysing the behaviour of both PE & Non-PE files, Malware Heuristics, REMnux, MITRE Framework, Reverse Engineering, Registry Explorer, Windows Registry Forensics, Gophish & Phishtool, Evilginx, SQL Injection, SSTI, SSRF, LFI, XXE, Owasp, Memory Forensics with Volatility, Splunk, Anvilogic, Atomic Red Team, Caldera, Purple Teamer, Sigma Signature Language, Basic Android Reversing

---

Programming Competency

1. Python
2. PowerShell
3. Golang (Learning Underway)
4. VB Script

Certificates

1. eLearnSecurity Junior PenTester (eJPT) - July 2021, 2. eLearnSecurity Certified Prof PenTester(eCPPT) - Aug 2022, 3. Cisco Certified Network Associate (CCNA 200-301), 4. Paloalto Certified Network Security Engineer.

Education

Government Boys Higher Secondary School,

SSLC & Higher Secondary Education (HSE) • Salem, Tamil Nadu
05/2012

Bachelor of Engineering (EEE)

RMK Engineering College • Chennai, Tamil Nadu
04/2016

Significant Achievements

1. **In Top 2% of TryHackMe Users**
2. **HackTheBox** CTF Player
3. Secured 71st place in **Synack #RedTeamFive** competition.
4. Participated in **VUCYBERTHON 2022 CTF** event (Online)