SUNIL KATAKDHOND

sunilk271994@gmail.com

Career Objective

To obtain a challenging and rewarding position in Cyber Security domain with an organization which recognizes my true potential and provides me enough avenues for professional growth through nurturing my technical skills and competencies.

Core Qualifications

- Vulnerability Assessment & Penetration Testing
- Linux & Windows system administrator
- Python
- Network Defense and Security

Professional Experience

Cyber Security Analyst

CRIF Solution – Pune Maharashtra 15th April – Present

- Performed web application & web services penetration testing on various credit bureau applications.
- Assess and evaluated risk based on threats vulnerabilities and Develop CVSS calculator to rate risks for vulnerabilities found in assessments.
- Key contributor for developing templates such as Security Assessment Plan Security Assessment Report & Security Assessment Questionnaire.
- Configured Mod Security Web Application Firewall with ELK (Elastic Search, Logstash, Kibana) Dashboard.

Security Administrator 27th Feb 17 – 29th March 19

AcuitiLabs (India) Private Limited – Pune Maharashtra

- Experience in the areas of Vulnerability Assessment, Risk Assessment, Web Application Security, Network Configuration Review.
- Develop test cases to test web application according to OWASP & SANS 25.
- Produced advisory reports regarding 0-day exploits, CVE vulnerabilities, current network & Researched and analyzed known hacker methodology, system exploits and vulnerabilities to support Red Team Assessment activities.
- Configured Public Key Infrastructure (PKI) to issue CA certificate to all internal web application.
- Configured OpenVPN – It provides solutions to secure data communications, whether it's for Internet privacy, remote access for employees using pre-shared key, certificate or username/password with HMAC packet authentication feature to add an additional layer of security to the connection.

Professional Certifications

- ✓ **Offensive Security Certified Professional (OSCP)**

  The Offensive Security Certified Professional is an ethical hacking certification offered by Offensive Security that teaches penetration testing methodologies and the use of the tools included with the Kali Linux.

- ✓ **ECSA v9**

  The **EC Council's Certified Security Analyst** is a professional certification provided by the International Council of E-Commerce Consultants (EC-Council).

Education

- **Post-Graduation Diploma in IT Infrastructure, System and Security (DITISS)** **78.56%** **2017**

  C-DAC's Advance Computing Training School – Pune, Maharashtra

- **Bachelor of Engineering (Electronics)** **7.32GPA** **2016**

  Mumbai University, Maharashtra

- **H.S.C (Science)** **70.50%** **2012**

  Ramnivas Ruia Jr. College – Mumbai, Maharashtra

- **S.S.C** (**Maharashtra State Board)** **91.45%** **2010**

  KMSP Mandal's Sheth I.H Bhatia High School

Skills

Vulnerability Assessment & Penetration Testing:

Web Application Penetration Testing: Good understanding of OWASP Top 10, Manual & automated testing on thin & thick client using Burp Suite, Acunetix Web Application Scanner & Source code analysis tool checkmarkx.

Mobile Penetration Testing: Good understanding of mobile OWASP Top 10, Static & dynamic analysis on mobile apps

Network & Firewall Penetration Testing: Firewall rule review and network devices configuration review using Nipper. Manual packet inspection using Wireshark, TCPdump. Good understanding of Nessus vulnerability assessment scanner & Metasploit Framework.

Exploit Development: Stack overflow exploitation, Heap overflow exploitation, shellcode development, working knowledge on GDB (text-based Linux debugger), WinDbg (text-based Windows debugger) & immunity debugger (GUI based multipurpose debugger).

Cryptography:

Basic understanding of Encryption Concepts, Good Understand of Private and Public Key Encryption, Digital Signatures, Self-sign & Let's Encrypt Certificate generation on Nginx and Apache2, OpenVPN with Encryption on Linux (Debian), PKI infrastructure Lab.

Network Defense and Security:

Network Firewall: Hands on experience on configuration of SonicWALL, & Linux Iptables,

Intrusion Detection/Prevention System (IPS/IDS): Configuration of Snort (Network Based IDS/IPS) with Kiwi Syslog server & OSSEC (Host Based IDS) on Linux (Debian).

IT Infrastructure Monitoring: Hands on experience on configuration of Nagios core for infrastructure Monitoring.

Web Application Firewall: Good understanding of Apache mod Security WAF.

Security information & event Management (SIEM) & endpoint Protection: AlienVault USM & OSSIM, Symantec Endpoint Protection.

Linux & Windows system administration:

Knowledge of Red Hat, Centos7 & Debian Operating System; DHCP; DNS; Apache & Nginx web server; Squid web proxy; SMTP mail server; Kerberos Apache security (SSL); Secure NFS Servers; SAMBA servers; NIS Servers; OpenLDAP Server.

Knowledge of Windows Server 2008/12; Active Directory Group Policy Object (GPO); Group Policy Management Console (GPMC); DNS; DHCP; WDS; IIS & tomcat Server.

Working Knowledge on Hyper-V, KVM, VMware ESXi, Basics of Configuration Management tools & agile technology like Docker, Git, Jenkins, Bugzilla and project management tool like taiga.

Basic knowledge of Cloud infrastructure like Amazon EC2 & S3 buckets.

Programming Languages:

Python: Python 2.7 with advanced proficiency.

C: Good Knowledge C language with intermediate proficiency**.**

X86 Assembly: Familiar with x86 Assembly & reverse engineering.

Extra-Curricular Activities

- Team Member of winning “football” team at college level.
- Project Training in L&T Electrical & Automation during the period 25th June 2015 to 24th July 2015 Switch gear Design & Development Center (SDDC), Business Unit & Automation at Powai, Mumbai.

Project Details

- Struts2Scanner

  Struts2Scanner is a python based vulnerability scanner to scan the web applications for struts2 vulnerabilities.

- Title: Penetration Testing

  Conducted various web & network security assessments for the Bank. Performed internal and external network penetration tests. Reported key findings to the client on a regular basis and formed prioritized recommendations for remediating the identified vulnerabilities.

- Lan Crawler

  Lan Crawler is a crawler and indexer of public network files shared via SMB shares.

Personal Information

Date of Birth: 27th of August 1994

Permanent Resident: 10 Yadav Sangh Society Kajupada Pipeline Sakinaka Kurla West Mumbai Maharashtra 400072.

Mobile Number: 9637129323

Languages: English, Hindi, Marathi

Personal Website: https://infosec-sunilk.netlify.app/

Linkedin: www.linkedin.com/in/infosec-sunil-katakdhond

YesWeHack: https://yeswehack.com/hunters/ghost27

GitHub: https://github.com/gh0st27

Hobbies: Travel, Trekking, Football

I hereby declare that, the information furnished above is true to the best of my knowledge.

Place: Mumbai

Date: 06/02/2021 Sunil Katakdhond