Shubham Bhasker

shubhambhaskr123@gmail.com
KMAIK bendrabutis Nr. 2, Kaunas
Room 103
+370 630 17587

Summary

Profound knowledge of Networking Security, Ethical Hacking, and Cyber Security. All Vulnerability assessment and penetration testing VAPT including Physical VAPT. OWASP top attacks with their detection and preventions techniques. Sound knowledge in Metasploit Framework and Social Engineering.

Experience

Security Researcher

11/2020 - 09/2021

- Worked with departments across the company, including security and project management, in developing new ideas, initiatives, products, and services
- CTF Player

Skills

- Networking
- Web Application Penetration
- Kali Linux
- Azure Sentinel
- Network vulnerability scan and penetration testing
- Familiar with password hash cracking MD5 SHA1, SHA2, etc.
- Real-time traffic analysis, network IDS and packet, dissection using Wireshark.
- Experience with tools: Aircrack-ng, Hydra, Burpsuite, Metasploit, OWASP-ZAP Nmap, Wireshark, Sqlmap, John-Ripper, Nesuss.
- Knowledge of operating systems, application software and cyber security tools Remote access support

---

Technical Skills

- Platforms: Proficient with Windows, Windows Server, Linux, Kali Linux, Fedora, and Ubuntu.
- Tools: Wireshark, Meterpreter, Armitage, Metasploit, DLP tool, VMware, Nessus, Burp Suite, Nmap.
- Protocols: TCP/IP, SSL, SSH, DHCP, UDP, DNS
- Networking: Conversant in LAN, WAN, Wi-Fi, DNS, DHCP, TCP/IP, Firewalls / IPS/IDS

Education

Sobtis Public School

Completed my Intermediate graduation
03/2019

- Student at Vilnius University
- Currently completing courses in computer science, Security Analysis, and Cyber security.
- Prominent coursework: CS50

Certificates

Advance Penetration Tester (Cybrary), NDG linux, CISCO Cyber Security Essential, CISCO CCNAv7, NSE 1 ,NSE 2, Digital Forensics, Offensive Penetration Testing

Languages

HTML, CSS, JAVASCRIPT, PYTHON, BASH, SQL, PowerShell

Accomplishments

- Try Hack Me top 1%
- Top 2 hacker ranking in Li t h u a n i a

Projects

Created an algorithm that builds a custom/proof of concept of File Integrated Monitor (FIM)

- Developed an integrated baseline of target files/folders using the hashing algorithm
- Continuously made comparison of actual file vs baseline, raised alerts if any deviations occurred
- Sent alert x-alert via y-means to allow further investigation of potential compromise

Build a Honeypot while operating Azure Sentinel (SIEM)

- Used custom PowerShell script to extract metadata from Windows Event Viewer to be forwarded to third party API in order to derive Geolocation data.
- Configured Log Analytics Workspace in Azure to ingest custom logs containing geographic information (Latitute, Longitude, State/Province, and Country)
- Configured Custom Feilds in Log Analytics Workspace with the intent of mapping geo data in Azure Sentinel.
- Configured Azure Sentinel (Microsoft's cloud SIEM) workbook to display global attack data (RDP bruteforce) on world map acording to physical location and magnitute of attacks.