**Shruti Chavan**

**Cyber Security Engineer**

**Phone: 201-238-0194 | Email: shruti.c@cvinboxs.com | Location: New Jersey**

**Summary**

* 4+ years of experience in Cyber Security / Project Management / Cyber Counter intelligence / Network Security Architecture / Malware Reverse Engineering.
* Cyber Security Engineer with good experience in Implementation, Administration, Operation and Troubleshooting
* of enterprise data networks.
* Project management for large cyber security projects utilizing advance methodology (e.g., Six Sigma), Agile and Scrum.
* Well versed in installing Splunk logging application for distributed environment.
* Written Nmap scanner and multithreaded python program to brute-force an FTP server using password file.
* Demonstrated success managing networking, design, quality assurance, product development, Internet Technology.
* Proficient in installing and configuring DNS, DHCP server, Sub netting, IPv4 and IPv6.
* Good knowledge of OSI Model and TCP/IP networking standards with protocols such as SNMP and FTP.
* Successful in initiating six separate security programs which passed all third-party audits and all established laws and regulations.
* Experience with Routing, layer 2 & layer 3 Switching and Protocols.
* Experience and skills in threat and vulnerability management, information security analysis, information security architecture, information security policy design, risk assessment, security incident response, and security solution implementation and administration.
* Good knowledge of Routing, Switching, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), Firewall Management, IPsec and VPN Configuration, VoIP Management.
* Good knowledge in advanced Persistent Threat (APT) / Cyber CI (Counter intelligence), Cyber Security Forensic (malware analysis/ identifying intelligence related activity).
* Good knowledge and experience in Installation, Configuration and Administration of Windows, FTP, DNS, DHCP servers under various LAN and WAN environments.
* Developing strategies to enhance overall cyber security program. Maintaining and improving security posture for IT governance.
* Maintaining critical monitoring systems (Splunk - log management systems) measuring system errors logs performance and availability. Evaluation of log management solution Splunk plus open-source Linux storage systems.
* Team Player, quick learner, very dependable, proactive, pay attention to detail and can work under difficult conditions to meet deadlines.

**Skills**

SDLC, AGILE / SCRUM, Python, R, Policy Planning, Implementation, Data Integrity, Disaster Recovery, Technical Specifications development, DNS, DHCP, Sub netting, Excellent Problem-Solving skills, Excellent diagnostic skills, CISCO Router Management, IPv4, IPv6, IP Conflicts, TCP/IP, SMTP, VPN, LAN, WAN, Wi-Fi, VMware, Windows, Linux.

**Education**

**Master of Science in Cyber Security**

New York Institute of Technology, Manhattan, NY

**Experience**

 **PNC Financial Services, NJ | Feb 2020 - Current**

 **Cyber Security Engineer**

 **Roles & Responsibilities:**

* Planning, Implementing, Managing, Monitoring and Upgrading security measures for the protection of the organizations data, systems and networks.
* Ensuring that the organization's data and infrastructure are protected by enabling the appropriate security controls.
* Works with network team on design, configuration and implementation of network access control systems, with respect to security.
* Follows and implements all security configuration management processes and suggests improvements as they pertain to their work.
* Manage Firewalls, IDS/IPS, build out security infrastructure including Vulnerability scanning and SIEM.
* Investigate network traffic as accumulated from IDS/IPS, Event Correlation to assess and mitigate risks.
* Performed penetration testing & vulnerability assessment for compliancy assessment.
* Detailed security knowledge including technologies such as Malware, Network Intrusion Prevention, Security Information Event Management systems
* Conduct research to identify threats and attack vectors and develop mitigating solutions to manage the risk.
* Key contributions include troubleshooting of complex LAN / WAN infrastructure that include routing protocols EIGRP, RIP, OSPF & BGP.
* Investigate new and emerging security threats against the Network infrastructure and interconnected systems.
* Assisted campus for VOIP network management and troubleshoot.
* Assisted in the implementation of a Web Sense Email Security Gateway Anywhere solution to manage/secure SMTP traffic
* Monitored security threats to the network and responded to major incidents including DDoS, Brute Force and various other types of malware.
* Responsible for daily security checks, monitoring unsuccessful logons, monitoring inactive users and locking inactive users in production system.
* Coordinating pen testing and application security testing audits with Pen Test Tools like Metasploit, NMAP,
* Wireshark and Kali on Linux/Unix operating system.
* Support third party technologies within the ACI ecosystem such as VMware.
* Involved in SNMP Network management. Worked on various scanning and sniffing tools like Ethereal.
* Network traffic visualization to facilitate monitoring and trending analysis.
* Perform Security Assessments, Security Compliance Standards, Penetration Tests, and Vulnerability Assessments.
* Defined data requirements & report layouts for the business to review. Created testing plans & scripts based on requirements.
* Daily administrative tasks, reporting and communication with the relevant departments in the organization.

**Endurance Technologies, India | Jan 2015 - Dec 2017**

**Cyber Security Engineer**

**Roles & Responsibilities:**

* Coordinate and perform security audits and vulnerability assessments to assess internal security procedures and compliance requirements.
* Implementation and maintained intrusion detection/ prevention (IDS/IPS) system to protect
* Reviewed security logs to ensure compliance with policies and procedures and identifies potential anomalies.
* Ensure that the company’s sensitive information and IT equipment are kept safe by implementing the correct security measures.
* Troubleshoot TCP/IP problems troubleshoot connectivity issues in multi-protocol Ethernet and Environment.
* Collaboration with system engineers to ensure Cybersecurity is involved from beginning to end of Naval Aviation Test and Evaluation events.
* Included preparation and maintenance of required vulnerability assessment documentation, and reports and briefs to Stakeholders.
* Support customer with the configuration and maintenance of ASA firewall systems.
* Planning security systems by evaluating network and security technologies defining requirements for local area networks (LANs), wide area networks (WANs), virtual private networks (VPNs), routers, firewalls, load balancers, and related security and network devices; designs public key infrastructures (PKIs), including use of certification authorities (CAs) and digital signatures as well as hardware and software; adhering to industry standards.
* Performed host, network, and web application penetration tests.
* Used Puppet software to do testing and simulation on classified networks.
* Configured Frame-relay and PPP encapsulation in various configurations and authentications.
* High availability HSRP, VRRP and Ether channel creation on Cisco, switches and routers.
* Plan, design, install and configure LAN/WAN as per organizational/client requirements, governed by communication protocols.
* Troubleshoot and resolved dynamic routing, Ethernet switching and host connectivity issues in a window and network environment.
* Analyzed and understood the issues related to DNS, DHCP and other IP conflicts.
* Configured and implemented VPN Tunnels using IPsec encryption standards.
* Responsible for Data Backup, System Update, Recovery and Restore and Spyware removal.
* Assisted Systems specialist in creating VPN remote access support for the entire confidential chain.
* Writing comprehensive reports including assessment-based findings, outcomes and propositions for further system security enhancement.
* Create technical and managerial documentation, topologies and metrics to support security tasks.