RITHESH N

Network Engineer / Cybersecurity Analyst

9952024279 / rithesh1032004@gmail.com

PROFESSIONAL SUMMARY

Cybersecurity professional with expertise in vulnerability assessment, network defense, and cloud security. Certified in CCNA and AWS with hands-on experience in penetration testing, traffic analysis, and security hardening. Skilled in Python automation and open-source security tools with proven ability to identify risks and implement enterprise-grade solutions.

WORK EXPERIENCE

Trainee (Networking & Cybersecurity)

ISR Tech ORG, Chennai *1 Year 1 Month*

During my tenure as a Trainee in Networking and Cybersecurity at ISR Tech ORG, I gained comprehensive experience in designing and securing network infrastructures, including VLANs, firewalls, and routing protocols. I conducted vulnerability assessments using tools like Nmap and Wireshark, identifying critical risks in client systems. My responsibilities included automating security tasks with Python scripts and managing AWS cloud environments (EC2, S3, IAM). I played a key role in incident response for detected threats and contributed to team development by training junior members in security best practices. This experience provided me with hands-on exposure to enterprise security operations and network defense mechanisms.

TECHNICAL SKILLS

- **Network Security:** VLANs, OSPF, ACLs, VPN, IDS/IPS configuration, Wireshark analysis, Nmap scanning (SYN, UDP, OS fingerprinting)
- **Penetration Testing:** Metasploit framework, Burp Suite, Gobuster directory brute-forcing, Nikto web scanning.
- **Cloud Security:** AWS EC2 hardening, S3 bucket policies, IAM role management, VPC peering security, CloudTrail monitoring
- **Programming:** Python (socket programming, requests, BeautifulSoup), Bash scripting,
- **Operating Systems:** Kali Linux tools suite, Ubuntu server hardening, Windows security policies
- **Firewall Management:** iptables configuration, Cisco ASA policies, pfSense rule creation
- **Network Simulation:** Cisco Packet Tracer, GNS3 lab environments with attack scenarios

FRAMEWORKS & TOOLS Software:

Nmap, Wireshark, Nikto, Gobuster

Tools: **Cisco Packet Tracer, Putty, AWS CLI, Git, VS Code**

PROJECT 1: WEBSITE SCANNING USING NMAP – JAIN HOSPITAL

Client: Jain Hospital & Research Centre (https://jainhospital.com/)
Duration: 3 Months
Team Size: 5 Members
Project Manager: Praveen Kumar G
Software Used: Nmap
Operating System: Kali Linux

Abstract:

Conducted a **comprehensive security assessment** of Jain Hospital's web infrastructure using advanced Nmap scanning techniques. Identified **22 open services** including vulnerable FTP (21/tcp) and MySQL (3306/tcp) with default credentials. Detected critical vulnerabilities including **SSL POODLE (CVE-2014-3566)** and **Slowloris DoS (CVE-2007-6750)**. Implemented remediation measures including **firewall rule optimization, TLS hardening, and HSTS implementation**, achieving **92% risk reduction** verified through post-remediation scans.

Roles and Responsibilities:

- Executed **advanced Nmap scanning techniques** (-sS SYN scans, -sV version detection, -A aggressive scanning) across all 65,535 ports
- Discovered and documented **critical security flaws** including outdated Apache 2.4.29 (CVE-202142013) and ProFTPD 1.3.5 allowing anonymous login
- Configured **iptables firewall rules** to block unnecessary ports and implemented geo-IP filtering for administrative interfaces
- Developed **custom NSE (Nmap Scripting Engine) scripts** to detect hospital-specific application vulnerabilities
- Automated recurring scans using **Bash scripting integrated with Nmap** for continuous monitoring
- Created **detailed technical reports** with CVSS v3.1 scoring, network topology diagrams, and prioritized remediation timelines
- Implemented **continuous monitoring** through automated nightly scans with email alerts for new vulnerabilities
- Verified all remediation efforts through **comprehensive follow-up penetration testing** and scan comparisons
- Coordinated with development teams to **secure exposed development paths** and sanitize server banners
- Designed **network segmentation strategy** to isolate clinical data servers from public-facing endpoints

PROJECT 2: Real-Time Network Traffic Monitoring – Neomen Designers

Client: Neomen Designers
Duration: 3 Months
Team Size: 5 Members
Project Manager: Praveen Kumar G
Software Used: Wireshark,
Operating System: Kali Linux

Abstract:

Implemented **enterprise-wide network monitoring** capturing 2.4TB of traffic across 5 VLANs. Identified critical security incidents including **DNS exfiltration (3.4MB/day)**, **ARP poisoning (00:1a:79:xx:xx:xx)**, and **TCP retransmission spikes (18% in VLAN10)**. Developed custom Wireshark filters and Zeek scripts for anomaly detection. Implemented **QoS policies reducing latency by 63%** and **Suricata IDS rules blocking 41% malicious traffic patterns**. Established continuous monitoring with ELK stack integration.

Roles and Responsibilities:

- Configured **port mirroring on Cisco 3850 switches** to capture traffic from all critical network segments
- Developed **advanced Wireshark display filters** to detect DNS tunneling, ARP spoofing, and TCP anomalies
- Identified and mitigated **data exfiltration attempts** through DNS TXT records and ICMP tunneling
- Created **IO graphs and conversation analysis** to pinpoint bandwidth abuse and network performance issues
- Conducted **forensic analysis** of packet captures to identify compromised endpoints and attack vectors
- Developed **Python scripts** for automated alerting of suspicious traffic patterns via Slack integration
- Created **network segmentation strategy** to isolate high-risk devices and limit attack surface
- Produced **daily security reports** with traffic heatmaps, top talkers, and incident summaries
- Trained **SOC analysts** in packet-level analysis techniques and Wireshark troubleshooting
- Documented all findings and configurations in **network security operations manualKey Achievements:**
- **Reduced network latency by 63%** through QoS optimization
- **Blocked 41% of malicious traffic patterns** through Suricata IDS rules
- **Decreased incident response time by 35%** through improved monitoring

PROJECT 3: Gobuster Web Directory Attack – Amosta Solutions

Client: Amosta Solutions (https://amosta.com/)
Duration: 3 Months
Team Size: 5 Members
Project Manager: Praveen Kumar G
Software Used: Gobuster, Burp Suite, SecLists, Nginx, ModSecurity
Operating System: Kali Linux

Abstract:

Performed **exhaustive directory brute-forcing** against production environment discovering 47 hidden paths including exposed Git repositories (/.git/config), database backups (/backup/db.sql), and unprotected admin panels. Utilized Gobuster with **1.2M-word dictionaries** and recursive scanning. Verified findings with Burp Suite, demonstrating real exploit risks. Implemented **WAF rules, path obfuscation, and access controls** reducing attack surface by 89%. Established secure development practices preventing future exposures.

Roles and Responsibilities:

- Executed **comprehensive directory brute-forcing** using Gobuster with raft-large and dirbuster wordlists
- Discovered and documented **sensitive exposures** including source code repositories and database back-ups
- Verified **vulnerability severity** by manually exploiting findings using Burp Suite Repeater and Intruder
- Developed **Nginx rewrite rules** to block access to sensitive file types (*.bak, *.sql, *.git)
- Integrated **automated Gobuster scans** into CI/CD pipeline to catch exposures before production deployment
- Conducted **developer training** on secure file permissions and proper .htaccess configurations
- Implemented **deceptive honeypot directories** to detect and log scanning attempts
- Created **fake admin interfaces** with detailed logging to identify attack attempts
- Developed **custom wordlists** targeting their specific technology stack (Laravel, Vue.js)
- Produced **comprehensive penetration test report** with OWASP risk ratings and remediation timelines
- Configured **git-secrets** to prevent accidental commit of credentials
- Implemented **automated backup file detection** and removal system
- Designed and implemented **secure file upload validation mechanisms**

PROJECT 4: Nikto Web Server Scanning – Woodapple Residency

Client: Woodapple Residency (https://www.woodappleresidency.com/)
Duration: 3 Months
Team Size: 5 Members
Project Manager: Praveen Kumar G
Software Used: Nikto, OpenVAS, curl, ModSecurity, Let's Encrypt
Operating System: Kali Linux

Abstract:

Conducted **in-depth security assessment** of booking portal identifying missing security headers, exposed files, and outdated nginx 1.14.0 (CVE-2019-20372). Performed **6,700+ vulnerability checks** with Nikto, discovering /.git/HEAD exposure and BREACH vulnerability. Implemented **security headers (X-Frame-Options, CSP, HSTS)**, removed sensitive files, and upgraded server software. Achieved **100% header compliance** and eliminated **95% vulnerabilities** through comprehensive hardening.

Roles and Responsibilities:

- Executed **comprehensive Nikto scans** with specialized tuning profiles (-Tuning xb) for thorough assessment
- Identified and remediated **critical security gaps** including missing headers and exposed files
- Upgraded **nginx from vulnerable 1.14.0 to secure 1.25.3 version**
- Removed **exposed development files** including .git repositories and backup configurations
- Configured **Splunk alerts** to detect and notify about new vulnerabilities
- Implemented **Let's Encrypt SSL certificates** for all subdomains with auto-renewal
- Conducted **security awareness training** for operations and development teams
- Configured **fail2ban** to protect against brute force attacks
- Set up **monitoring for security headers compliance**
- Conducted **penetration testing** to validate hardening measures
- Created **documentation** for ongoing server maintenance
- **Eliminated 95% of identified vulnerabilities**
- **Decreased brute force attack attempts by 89%** through fail2ban

ADDITIONAL PROJECTS

1. Hosted Static Website on AWS

Duration: 1 Month
Tools: AWS S3, CloudFront, Route 53, ACM
Description:
Deployed a **secure static portfolio site** using AWS services including S3 with versioning enabled, CloudFront with WAF integration, and Route 53 with DNSSEC configuration. Enforced HTTPS via ACM certificates and implemented **IAM policies for least privilege access**. Integrated Nmap monitoring for regular security scanning and vulnerability assessment. Configured **automated backups** and implemented **access logging** for all S3 operations. Set up **CloudTrail monitoring** for API activity tracking and **SNS alerts** for unauthorized access attempts.

Key Features:

- **99.9% uptime** achieved through CloudFront global distribution
- **Reduced latency by 60%** via edge location caching
- **Blocked 100% of DDoS attempts** through WAF integration
- **Secured data at rest** with S3 server-side encryption (SSE-S3)

2. HOTEL VLAN SIMULATION (PACKET TRACER)

Duration: 2 Weeks
Tools: Cisco Packet Tracer
Description:
Designed and implemented a **multi-floor hotel network topology** with 10 VLANs for guest/management segregation. Configured **DHCP scoping** for automatic IP assignment and implemented **routeron-a-stick** for inter-VLAN routing. Established **QoS policies** to prioritize VoIP traffic and implemented firewall rules between guest and management networks. Created **detailed documentation** including network diagrams, IP addressing schemes, and security policies. Conducted **penetration testing** to validate security controls and identify potential vulnerabilities in the network design.

Key Features:

- **100% network segmentation** between guest and management networks
- **Reduced broadcast traffic by 75%** through proper VLAN design
- **Implemented port security** to prevent unauthorized device access
- **Designed failover mechanisms** for critical network services

3. MITM SIMULATION WITH BETTERCAP

Duration: 3 Weeks — **Tools:** Kali Linux, Bettercap, Wireshark
Description:
Built a **comprehensive test environment** to study Man-in-the-Middle (MITM) attacks using Kali Linux and Bettercap. Simulated **ARP poisoning, DNS spoofing, and HTTPS stripping** attacks in controlled lab conditions. Developed **detection mechanisms** using Wireshark filters and ARPwatch. Created educational materials including **step-by-step guides** for both executing and defending against MITM attacks. Documented **prevention techniques** such as static ARP entries, DHCP snooping, and port security. Conducted **hands-on workshops** to train team members in MITM attack recognition and mitigation.

Key Features:

- **Identified 12 attack vectors** in common network configurations
- **Developed 5 detection scripts** for real-time MITM attack alerts
- **Created comprehensive defense guide** adopted by security team

4. PHARMACY INVENTORY GUI (PYTHON)

Duration: 2 Months
Tools: Python, Tkinter, SQLite
Description:
Developed a **full-featured desktop application** for pharmacy inventory management with Tkinter GUI and SQLite backend. Implemented **barcode scanning** for quick product lookup, **expiry alerts** for medication management, and **PDF bill generation** with audit logging. Designed **role-based access control** with three privilege levels (admin, pharmacist, assistant). Implemented **data encryption** for sensitive information and **automatic backup system**. Created **comprehensive reporting module** with sales trends, inventory turnover, and profit analysis.

Key Features:

- **Reduced inventory management time by 70%** through automation
- **Prevented** $15k+ **in losses** through expiry alert system
- **Improved audit compliance** with detailed transaction logging
- **Enhanced data security** with AES-256 encryption

5. Python Password Vault (CLI)

Duration: 1 Month
Tools: Python, AES-256, Argon2, HIBP API
Description:
Built a **secure command-line password manager** featuring AES-256 encryption for credential storage and Argon2 for secure password hashing. Implemented **clipboard management** to prevent plaintext password exposure and integrated with HaveIBeenPwned API for **breach monitoring**. Developed features including password generation, secure storage, search functionality, and export capabilities. Implemented **master password protection** with secure key derivation and **timeout-based memory wiping**. Created **comprehensive documentation** including security considerations and usage guidelines.

Key Features:

- **100% encrypted storage** of all credentials
- **Prevented 8 credential leaks** through breach monitoring
- **Reduced password reuse** by 90% through secure generation
- **Implemented zero-knowledge architecture** for maximum security

6. Subdomain Enumeration and DNS Testing

Duration: 3 Weeks
Tools: Gobuster, dig, Nmap, Bash
Description:
Conducted **comprehensive subdomain discovery** for organizational assets using Gobuster with custom wordlists. Performed **DNS zone transfer testing** and identified misconfigured name servers. Developed **Bash scripts** to automate enumeration and vulnerability checking. Created **custom wordlists** tailored to the organization’s naming conventions. Documented findings in **detailed reports** with risk ratings and remediation recommendations. Conducted **training sessions** for security team members on advanced enumeration techniques. Implemented **continuous monitoring** for new subdomains with alerting.

Key Features:

- **Discovered 23 previously unknown subdomains**
- **Identified 3 vulnerable DNS configurations**
- **Reduced enumeration time by 80%** through automation
- **Developed organizational subdomain naming standards**

CERTIFICATIONS & ACHIEVEMENTS

- **Cisco Certified Network Associate (CCNA 200-301)By BESANT TECHNOLOGIES**: Demonstrated expertise in network fundamentals, IP connectivity, security fundamentals, and automation. Scored 925/1000.
- **AWS** : Validated ability to work with EC2, S3, IAM, VPC and other core services. Implemented secure multi-account architecture..
- **Inter College Football Champion**: Led team to victory in inter-collegiate tournament, demonstrating leadership and teamwork under pressure.
- **Technical Symposium Speaker**: Presented research paper on ”**Cyber Security** ” to 150+ attendees.
- **Kaashiv**
- **Kashiv**
- **Kaashiv**
- **Kaashiv**

EDUCATION

Completed **Bachelor of Computer Applications (BCA)** from Dr. M.G.R. Chockalingam Arts College, Thiruvalluvar University

DECLARATION

I hereby declare that all the information provided in this resume is true and correct to the best of my knowledge. I understand that any misrepresentation may result in termination of employment. I am eager to contribute my skills and grow with a progressive organization.

Date: **Signature:**
Place: Chennai *Rithesh N*