Sadiqul Sakif – Red Team Portfolio

I specialize in adversary simulation, penetration testing, and vulnerability assessments, leveraging frameworks like MITRE ATT&CK and tools like Metasploit, Caldera, RAT, and custom scripts

---

📜 Experience

Graduate Research Assistant at BRAC University

- **Research Interests:**
  - Cloud Computing: Investigating scalable cloud solutions for optimization and exploring new scope to research.
  - Cyber Security: Focused on threat modeling, forecasting, incident response, and security assessments and monitoring.

Security Engineer at Security Operations Center at Enterprise Infosec Consultant

- **Role Overview:**
  - Conducted vulnerability assessments and penetration tests across various industries, including finance, manufacturing, and services.
- **Experience Includes:**
  - **External & Internal Vulnerability Assessments**: Identifying security flaws in systems exposed to the internet and those within internal networks.
  - **Penetration Testing**: Comprehensive testing of web applications, cloud environments, APIs, and mobile applications using industry-standard methodologies.
  - **Wireless Network Penetration Testing and Forensics**: Assessing wireless networks for security weaknesses and performing forensic analysis on detected breaches.
  - **Mobile Application Development**: Created a mobile application for remote backdoor access (RAT) and conducted Android vulnerability assessments.
  - **API Integration**: Integrated Acunetix API with a custom vulnerability assessment tool for enhanced reporting and analysis capabilities.
- **Training Conducted:**
  - **Vulnerability Assessments**: Led a session on cloud computing vulnerabilities for a regional bank.

- **Wireless Network Security**: Provided internal training sessions on securing wireless networks and penetration testing techniques for company staff.

💼 Projects and Case Studies

1. External & Internal Vulnerability Assessment and Penetration Testing

- **Clients:**
  - **Manufacturing Company**: Conducted external penetration testing on their web applications.
  - **Regional Bank**: Comprehensive testing of web applications, cloud infrastructure, APIs, and mobile applications.
  - **Financial Institution**: Conducted assessments on web applications and internal networks.
- **Objective**: To identify vulnerabilities in both external and internal networks, ensuring compliance with security standards.
- **Tools Used**:
  - **Metasploit**: For exploiting vulnerabilities and conducting tests.
  - **Acunetix**: Automated web application security scanner for identifying vulnerabilities.
  - **AndroRAT**: Tool for testing Android applications for security weaknesses.
  - **Wireshark**: A network protocol analyzer is used to monitor traffic and analyze packet data.
  - **Nmap**: Network scanner for discovering hosts and services.
  - **SQL Injection**: Techniques for testing database security.
  - **Kite runner**: Tool for API penetration tests in a structured manner.
  - **Cherrybomb**: A tool for web API vulnerability scanning and pen testing.
- **Outcome**: Detected critical vulnerabilities and provided detailed mitigation strategies, significantly enhancing client security posture.

---

2. Wireless Network Penetration Testing and Forensics

- **Overview**: Performed thorough penetration testing and forensic analysis on wireless infrastructures.
- **Objective**: To secure wireless networks against external attacks and identify encryption protocol and configuration weaknesses.
- **Tools Used**:
  - **Aircrack-ng**: Suite of tools for assessing Wi-Fi network security.
  - **Kismet**: Wireless network detector and packet sniffer.
  - **Wireshark**: For packet analysis during testing.
  - **Pixies**: Tool for exploiting WPS vulnerabilities in wireless networks.

- **Outcome**: Secured wireless infrastructure by identifying misconfigurations and recommending enhancements to security protocols.

---

3. Mobile Application for Remote Access (RAT)

- **Overview**: Developed and tested a mobile application for backdoor remote access (RAT) and conducted Android vulnerability assessments.
- **Objective**: To simulate real-world mobile application attack scenarios to test the security of Android devices, including:
    - **Trace Location**: Tracking the device's location.
    - **Credential Stealing**: Testing for vulnerabilities related to credential theft.
    - **Personal Information Gathering**: Assessing the app's access to sensitive user data.
    - **Social Media Exfiltration**: Testing for gaining access to a social media account
- **Tools Used**:
    - **AndroRAT**: Tool for remote access to android devices.
    - **Android Debug Bridge (ADB)**: For testing Android apps and devices.
    - **Metasploit**: Used for testing vulnerabilities in mobile applications.
    - **Wireshark**: For monitoring network traffic during testing.
    - **MITM (Man in The Middle)**: Techniques for intercepting and analyzing communication.
    - **nGrok**: For creating secure tunnels to expose local servers.
- **Outcome**: Highlighted vulnerabilities in outdated mobile applications, providing actionable recommendations for patches and updates.

---

4. Custom Web Application Vulnerability Assessment Tool

- **Overview**: Integrated Acunetix API with a custom web application vulnerability assessment tool to automate and enhance vulnerability scanning.
- **Objective**: To streamline the vulnerability scanning process for web applications and provide comprehensive reporting.
- **Tools Used**:
    - **Acunetix**: For automated vulnerability scanning.
    - **Python**: For scripting and API integration.
    - **Custom API Integration**: Developed to enhance existing workflows and reporting capabilities.
- **Outcome**: Reduced time for vulnerability assessments by automating routine tasks and generating detailed reports for analysis.

🔧 Tools and Techniques

Tools:

- **Metasploit**: For penetration testing and exploit development.
- **Mimikatz**: For extracting passwords and credentials from Windows systems.
- **PowerSploit**: PowerShell scripts for post-exploitation and security testing.
- **Acunetix**: Automated web application security scanner.
- **MITRE Caldera**: Automated adversary emulation system.
- **BloodHound**: Tool for Active Directory enumeration and analysis.
- **AutoSploit**: Automated exploitation framework.
- **Nessus**: Vulnerability scanner for networks and applications.
- **OpenVAS**: Open-source vulnerability scanner.
- **Atomic Red Team**: Library of tests mapped to MITRE ATT&CK for security validation.
- **SQLMap**: Automated SQL injection and database takeover tool.
- **Custom Python Scripts**: Scripts for privilege escalation, phishing automation, and SQL injection testing.

Techniques (MITRE ATT&CK):

- **Initial Access (T1566)**: Spearphishing Attachment, Valid Accounts.
- **Execution (T1059)**: PowerShell.
- **Persistence (T1547)**: Registry Run Keys / Startup Folder.
- **Privilege Escalation (T1068)**: Exploitation of Vulnerable Services.
- **Lateral Movement (T1021)**: Remote Services (RDP, SMB).
- **Exfiltration (T1041)**: Exfiltration Over Command and Control Channel.

📜 Certifications

- **Cloud Engineering with Google Cloud**: Comprehensive training on cloud infrastructure and security.
- **IT Security Specialist**: In-depth understanding of information security principles and practices.
- **Technical Support Fundamentals**: Foundations of technical support in IT.
- **Ethical Hacking Essentials (EHE)**: Basics of ethical hacking methodologies and practices.

📧 Contact

Feel free to reach out for collaboration or consulting opportunities:

- **Email**: md.sadiqul.islam.sakif@g.bracu.ac.bd
- **LinkedIn**: Sadiqul Sakif