Society of St. Francis Xavier, Pilar's
Fr. Conceicao Rodrigues College of Engineering
Fr. Agnel Ashram, Bandstand, Bandra (W), Mumbai – 400 050
(Autonomous College affiliated to University of Mumbai)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

RESEARCH PROPOSAL FOR COURSE "HONORS WITH RESEARCH"- (A.Y. 2025-26)

Faculty Name: Dr. Prachi Dalvi

Title	Covert Windows Local Authentication Bypass via Bootable USB for Advanced Red Team Operations
Problem Statement	Physical access to a Windows system presents a significant cybersecurity challenge, as current authentication mechanisms can be exploited. This research focuses on developing advanced, stealthy Windows local authentication bypass techniques using a bootable USB. The goal is to achieve undetected access, across various Windows versions (XP-11), without altering the original user's credentials that would immediately reveal the compromise.
Domain	Offensive Security, Red Teaming, Operating System Exploitation, Digital Forensics (Artifact Analysis), Embedded Systems (Bootable Media)
Research Objectives:	• Analyze physical access vulnerabilities in Windows local authentication (SAM, Winlogon, accessibility features) across Windows XP-11. • Investigate and implement stealthy techniques to bypass Windows local login screens that do not require knowledge of or modification of the existing user password, ensuring system looks normal after reboots. • Create a universal bootable USB to non-intrusively modify critical system files and registry hives on any Windows version (BIOS/UEFI). • Implement specific covert bypass methodologies, such as accessibility feature hijacking, strategic registry modifications, and the creation of hidden administrative accounts, while minimizing detectable changes to the system. • Evaluate the effectiveness, stealth of the developed bypass techniques across a diverse range of Windows operating systems, meticulously documenting the absence of detectable password changes and minimizing forensic footprints.

Methodology	1. **Vulnerability & Mechanism Analysis:** In-depth research into Windows local authentication (LSASS, SAM), user profiles, boot processes, and how components like utilman.exe and sethc.exe can be subverted for unauthorized access. We'll also analyze SAM database structure across Windows versions. 2. **Bootable Environment Engineering:** Developing a robust, multi-architecture (x86/x64) bootable USB (WinPE/Linux-based) to automatically identify and mount target Windows drives offline for full system and registry access. • **Covert Bypass Payload Development:** Specialized modules within the bootable environment for: • **Accessibility Feature Hijacking:** Replacing legitimate accessibility executables with a command prompt for elevated access from the login screen without password alteration. • **Registry-Based Manipulation:** Modifying registry keys for gaining access, such as manipulating auto-login or creating hidden admin accounts. • **SAM Database Manipulation:** Offline interaction with the SAM database to enable/create administrator accounts with blank/known passwords, potentially inspired by tools like Kon-Boot, without resetting existing user passwords. 3. **Stealth and Persistence Evaluation:** Testing bypass techniques on isolated Windows XP, 7, 10, and 11 systems. We'll evaluate success, covertness (original password unchanged), and forensic detectability (event logs, access times, registry modifications). 4. **Artifact Analysis:** Post-exploitation forensic analysis of compromised systems to identify changes in SAM, registry, and system logs, ensuring minimal intervention footprint.
Mapped to SDG (Write SDG Nos with justifications)	**SDG-9 (Industry, Innovation, and Infrastructure):** By identifying advanced digital infrastructure vulnerabilities and demonstrating sophisticated attack methods, it provides crucial insights for developing more resilient operating systems, fostering secure technological innovation, and robust industrial growth. **SDG-16 (Peace, Justice, and Strong Institutions):** By exploring covert system compromise attack vectors, it offers valuable intelligence for policymakers and security professionals, strengthening digital security frameworks, safeguarding institutional integrity, and promoting a more secure digital society.

References

1. **"Privacy and Security of the Windows Registry"**
   - Authors: E. L. Amoruso
   - Published: 2024 (Ph.D. dissertation, University of Central Florida)

2. **"Microsoft SAM File Readability CVE-2021-36934: What You Need to Know"**
   - Authors: C. Condon
   - Published: July 21, 2021, Rapid7 Blog

3. **"Attacks Against Windows PXE Boot Images"**
   - Authors: T. Elling
   - Published: February 13, 2018, NetSPI Blog

4. **"Bypassing Local Windows Authentication to Defeat Full Disk Encryption"**
   - Authors: Haken
   - Published: November 12, 2015, in Proc. Black Hat Europe

5. **"Security Analysis and Bypass User Authentication Bound to Device of Windows Hello in the Wild"**
   - Authors: E. Kim and H. Choi
   - Published: July 23, 2021, Security and Communication Networks

6. **"Automating Privilege Escalation with Deep Reinforcement Learning"**
   - Authors: K. Kujanpää, W. Victor, and A. Ilin
   - Published: October 04, 2021, arXiv preprint, arXiv:2110.01362

7. **"Study of bypassing Microsoft Windows Security using the MITRE CALDERA Framework (version 3; peer review: 2 approved)"**
   - Authors: N. Mohamed
   - Published: September 29, 2022, F1000Research, vol. 11, no. 422

8. **"USB Artifact Analysis Using Windows Event Viewer, Registry and File System Logs"**
   - Authors: Neyaz and N. Shashidhar
   - Published: November 09, 2019, Electronics, vol. 8, no. 11, p. 1322

9. **"Study on Security Auditing of Windows Registry Database"**
   - Authors: J. Tashi
   - Published: July 2021, Int. J. Science Technology & Engineering, vol. 8, no. 1, pp. 1–5

10. **"Memory Forensics: comparing the correctness of memory captures from locked Windows 10 machines using different boot capture vectors"**
    - Authors: S. Zargari and J. Dyson
    - Published: July 2022, Latin-Am. J. Comput., vol. 9, no. 2, pp. 37-51

11. **"Study of bypassing Microsoft Windows Security using the MITRE CALDERA Framework"**
    - Authors: Alabdulatif and H. Taherdoost
    - Published: September 29, 2022, F1000Research, vol. 11, no. 422

12. **"Security Accounts Manager Database"**
    - Authors: Unkown
    - Published: ScienceDirect

13. **"AXREL: Automated Extracting Registry and Event Logs for Windows Forensics"**
    - Authors: Y. Prajapati and K. Gosai
    - Published: IEEE Xplore

14. **"Security Analysis and Bypass User Authentication Bound to Device of Windows Hello in the Wild"**
    - Authors: V. Visoottiviseth, A. Noonkhan, R. Phonpanit, P. Wanichayagosol and S. Jitpukdebodin
    - Published: IEEE Xplore

15. **"Penetration Testing on Windows to Preserve Security"**
    - Authors: J. Ribeiro and D. Caldas
    - Published: Brazilian Journals

Faculty Name: Dr. Prachi Dalvi

Faculty Signature H.O.D