**Comparison of Referenced Research Papers**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name of the Paper | Authors / Source | Focus | Methodologies | Key Findings | Relevance to Your Proposal |
| Privacy and Security of the Windows Registry | Amoruso (UCF Dissertation) | Security and privacy of the Windows Registry | Comprehensive dissertation, technical registry analysis, vulnerabilities, and privacy aspects | Detailed exploration of registry forensics, artifact persistence, and detection risks | Informs on forensic footprint and registry manipulation techniques for covert access |
| Microsoft SAM File Readability CVE-2021-36934: What You Need to Know | Condon, Rapid7 | CVE-2021-36934 SeriousSAM vulnerability in the SAM database | Real-world vulnerability disclosure, proof-of-concept analysis | Allowed non-admin users access to SAM and SYSTEM files; highlights offline attack surface | Direct insight into SAM attacks, critical for designing stealthy boot or offline bypass |
| Attacks Against Windows PXE Boot Images | Elling, NetSPI | PXE Boot images attacks & Windows boot-level vulnerabilities | Practical pentesting blog with technical walkthroughs | Demonstrates how attackers exploit Windows boot environments and PXE images | Supports bootable USB approach and identifies risks in Windows boot process |
| Bypassing Local Windows Authentication to Defeat Full Disk Encryption | Haken, Black Hat | Bypassing local Windows auth & defeating disk encryption | Conference whitepaper, threat modelling, exploit demonstration | By exploiting local (offline) authentication flaws, attackers can access encrypted systems | Reinforces physical access threat vector and validates premise of red-team boot attacks |
| Security Analysis and Bypass User Authentication Bound to Device of Windows Hello in the Wild | Kim & Choi, Wiley | Windows Hello biometric auth bypass | Peer-reviewed research paper, real-world attack experiments | Device-bound authentication can be bypassed if biometric data is not hardware protected | Shows feasibility of alternative (non-password) authentication bypasses |
| Automating Privilege Escalation with Deep Reinforcement Learning | KujanpÃ¤Ã¤ et al., arXiv | Privilege escalation via deep reinforcement learning | Simulation, machine learning for escalation | Automation reveals overlooked escalation routes in complex systems | Suggests AI-driven options for red team toolsets and persistent access methods |
| Study of bypassing Microsoft Windows Security using the MITRE CALDERA Framework | Mohamed, F1000Research & Alabdulatif & Taherdoost | Using MITRE CALDERA for Windows security bypass | Peer-reviewed case study with adversarial emulation | CALDERA enables undetected bypass of Windows controls, persistence, and low-noise operations | Powerful precedent and framework for your red-team operationalnal angle |
| USB Artifact Analysis Using Windows Event Viewer, Registry and File System Logs | Neyaz & Shashidhar, MDPI | USB artifacts in Windows (logs, registry, filesystem) | Experimentation with forensic tools | USB drives leave identifiable artifacts, but detection can be minimized | Directly relates to your forensic stealth & persistent access with bootable USBs |
| Study on Security Auditing of Windows Registry Database | Tashi, IJSTE | Auditing Windows Registry Database for security | Security auditing, registry analysis | Outlines methods and limits of registry-based detection and security logging | Helps define how to minimize detection after registry/credential manipulation |
| Memory Forensics: comparing the correctness of memory captures from locked Windows 10 machines using different boot capture vectors | Zargari & Dyson, LAJC | Memory forensics on locked Windows 10 captured via boot | Empirical study, comparative analysis of capture vectors | Boot-vectored memory captures can expose authentication material | Relevant for post-exploit, offline forensic analysis and persistence evaluation |
| Security Accounts Manager Database | ScienceDirect, SAM overview | Technical underpinning of SAM database | Technical resource, conceptual | Details structure, interaction, and security models for local Windows accounts | Background knowledge for manipulating SAM without detectiontion |
| Security Analysis and Bypass User Authentication Bound to Device of Windows Hello in the Wild | IEEE Xplore, Windows Hello auth bypass | Windows Hello & device-bound authentication vulnerabilities | Security analysis, technical review | Points to persistent weaknesses in device-bound and biometric authentication | Extends your work beyond password-based attacks to next-gen authentication |
| AXREL: Automated Extracting Registry and Event Logs for Windows Forensics | IEEE Xplore, Registry/Event Log Extraction (AXREL) | Automated forensic artifact extraction | Describes forensic tool and methodology | Improved techniques for detecting hidden/persistent changes in Windows | Helps evaluate which covert bypass methods may or may not leave artifacts |
| Penetration Testing on Windows to Preserve Security | Brazilian Journals | Survey of penetration testing on Windows login bypass | Overview, compilation of tests on various bypass techniques | Documents threshold, methods, and limitations of offline/online bypass | Practical foundation for comparing methods in real-world offensive security |