Windows Bypass and Multilayer Security

Harsh Pawar,Daksha Bora,Tanmay Chaudhari ,Gourav Pandey

Guidence By Mrs. A.A.Deshpande

|| पढमं नाणं तओ दया ||
Shri Jain Vidya Prasarak Mandal's
RASIKLAL M. DHARIWAL INSTITUTE OF TECHNOLOGY
Guru Fattechand Bhavan, Shri Fattechand Marg, Chinchwadgaon, Pune -411033
Fax: 020-27354633, Tel: 020 - 64106323, 020-27353516, Email: rmdiot@gmail.com
ESTD : 8/9/1927
Manikchand

---***---

Abstract - Firstly, the abstract delves into the diverse array of bypass techniques employed by adversaries, ranging from traditional methods such as password cracking and privilege escalation to more advanced tactics like file less malware and code injection. Understanding these tactics is crucial for defenders to anticipate and counteract potential threats effectively. Secondly, the abstract highlights the limitations of singular security measures and advocates for the adoption of multilayer security strategies. By implementing a combination of preventive, detective, and corrective controls, organizations can create multiple barriers for attackers, making it significantly more challenging to compromise Windows systems. These layers may include network firewalls, intrusion detection systems, endpoint protection software, and user training programs. Moreover, the abstract emphasizes the importance of proactive security measures, such as regular software updates, vulnerability assessments, and penetration testing, to identify and address potential weaknesses before they can be exploited by attackers. Additionally, the abstract discusses the significance of user education and awareness in mitigating common attack vectors, such as phishing and social engineering.

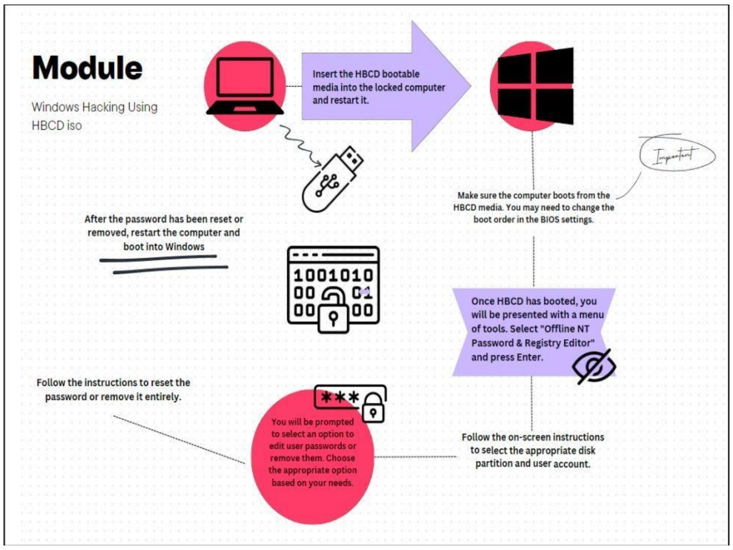
1. INTRODUCTION

The constant evolution of digital threats presents a significant challenge for securing Windows environments. Attackers continually devise new bypass techniques to circumvent traditional security measures, necessitating a proactive and multilayered defense strategy. This introduction provides a brief overview of the landscape of Windows bypass techniques and the importance of implementing multilayer security measures to mitigate these threats effectively.

2. Body of Paper

In the realm of cybersecurity, Windows systems are frequent targets due to their ubiquity and importance in various sectors. Attackers employ diverse bypass techniques, from basic password cracking to sophisticated malware, to breach these systems. Singular security measures like antivirus software are insufficient against such multifaceted threats. A

multilayered security approach is essential, encompassing preventive, detective, and corrective controls. Preventive measures like firewalls and endpoint protection are the first line of defense, followed by detective controls such as intrusion detection systems. Corrective controls, including incident response protocols and patch management, mitigate the impact of breaches. Proactive security measures, such as regular updates and user training, fortify defenses. This comprehensive strategy enhances resilience against evolving bypass tactics, securing Windows environments effectively.



Insert the HBCD bootable media into the locked computer and restart it.

Make sure the computer boots from the HBCD media. You may need to change the boot order in the BIOS settings.

Once HBCD has booted, you will be presented with a menu of tools. Select "Offline NT Password & Registry Editor" and press Enter.

Follow the on-screen instructions to select the appropriate disk partition and user account.

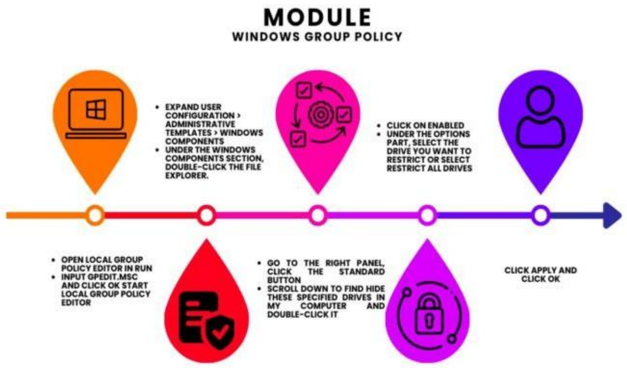
You will be prompted to select an option to edit user passwords or remove them. Choose the appropriate option based on your needs.

Follow the instructions to reset the password or remove it entirely.

After the password has been reset or removed, restart the computer and boot into Windows

Fig -1: Figure

10.55041/IJSREM30828



- OPEN LOCAL GROUP POLICY EDITOR IN RUN
- INPUT GPEDIT.MSC AND CLICK OK START LOCAL GROUP POLICY EDITOR

- EXPAND USER CONFIGURATION › ADMINISTRATIVE TEMPLATES › WINDOWS COMPONENTS
- UNDER THE WINDOWS COMPONENTS SECTION, DOUBLE-CLICK THE FILE EXPLORER.

- GO TO THE RIGHT PANEL, CLICK THE STANDARD BUTTON
- SCROLL DOWN TO FIND HIDE THESE SPECIFIED DRIVES IN MY COMPUTER AND DOUBLE-CLICK IT

- CLICK ON ENABLED
- UNDER THE OPTIONS PART, SELECT THE DRIVE YOU WANT TO RESTRICT OR SELECT RESTRICT ALL DRIVES

CLICK APPLY AND CLICK OK

3. CONCLUSIONS

The discussion emphasizes the necessity of a multilayered security approach to mitigate Windows bypass techniques effectively. Singular security measures are insufficient against evolving threats, necessitating a combination of preventive, detective, and corrective controls. Proactive security measures and user education further enhance resilience against bypass attacks. Overall, investing in robust security measures is crucial for safeguarding Windows environments against modern cyber threats.

ACKNOWLEDGEMENT

I would like to take this opportunity to express my deepest gratitude and indebtedness
to those who contribute valuable time in helping us to complete our Project.
I would like to express my sincere and whole hearted thanks to our project guide H.O.D
MRS.A.A.Deshpande. For her valuable direction and guidance toward our project, her
meticulous attention towards our work without taking care of her precious time.
I would like to sincere and whole hearted thanks to our H.O.D Mrs. A. A. Deshpande.
I am thankful to our honorable Principal sir Mr. A. B. Thite for his encouragement
toward our project.
Last but not least I express heartful gratitude to all my friends and well-wishers
withoutwhom the project would not have been a success.

REFERENCES

1. Rossow, C., Dietrich, C., Grier, C., Kreibich, C., Paxson, V., Pohlmann, N., & Bos, H. (2012). Prudent Practices for Designing Malware Experiments: Status Quo and Outlook. In Proceedings of the 2012 ACM Workshop on Security and Artificial Intelligence (pp. 55-66).
2. Papadopoulos, D., Tsohou, A., Vasilomanolakis, E., & Mühlhäuser, M. (2016). Security Threats to Electronic Health Records (EHRs): A Literature Review. In 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 482-487).
3. Bhatia, M., & Verma, A. K. (2017). A Survey on Windows OS Hacking Techniques and Detection Tools. International Journal of Computer Applications, 173(7), 1-7.
4. Kumar, A., & Nigam, M. (2019). Cyber Security: A Review of Trends, Techniques and Tools. In 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon) (pp. 1-5).

10.55041/IJSREM30828