Investigating Windows

Penetration Testing Report

Executive Summary: This document presents the findings from a penetration test conducted on a system running Windows Server 2016. The objective was to identify security vulnerabilities that could be exploited by an unauthorized party to gain access to the system or network.

Test Methodology:

1. **System Identification:**
    - Used **Winver** to determine the Windows version: Windows Server 2016.
2. **User Activity Audit:**
    - Utilized Event Manager to find the last user who logged in: administrator.
    - Employed the command **net user john** to ascertain the last login time of the user 'john'.
3. **Network Connections Analysis:**
    - Accessed the Registry Editor (regedit) navigating to **SOFTWARE > Microsoft > Windows > CurrentVersion > Run** to discover outbound connections, identifying an IP address 10.34.2.3 associated with a suspicious executable.
4. **Privilege Escalation Check:**
    - Ran **net localgroup Administrators** to list accounts with administrative privileges.
5. **Scheduled Tasks Review:**
    - Inspected the Task Scheduler Library for malicious tasks.
    - Located a task named "Clean file system" which was deemed malicious.
6. **Malicious Files and Scripts:**
    - Found a script **nc.ps1** set to run daily by the suspicious scheduled task, which was listening locally on port 1348.
7. **User Login Investigation:**
    - Checked **net user jenny** and determined that the user 'jenny' never logged on.
8. **System Compromise Timeline:**
    - Established the date of user 'Jenny's' account creation as 03/02/2019, marking the compromise event.
    - Analyzed Event ID: 4672 in the Event Manager to pinpoint the time Windows assigned special privileges to a new logon: 03/02/2019 at 4:04:49 PM.
9. **Credential Access Tools:**

- Found evidence of **mimikatz** usage in the directory where the malicious scheduled task was operating.

10. **Command and Control (C2) Identification:**
    - Located the attacker's external C2 server IP address 76.32.97.132 in **C:\windows\system32\drivers\etc\hosts**.
11. **Web Server Breach Analysis:**
    - Inspected the IIS directory at **C:\inetpub\wwwroot** and identified an uploaded malicious .jsp file.
12. **Network Security Assessment:**
    - Reviewed firewall inbound rules and discovered the last port opened by the attacker.
13. **DNS Poisoning Check:**
    - Confirmed DNS poisoning by finding a compromised entry for google.com with the IP 76.32.97.132 in **C:\windows\system32\drivers\etc\hosts**.

Findings and Recommendations: The penetration test revealed several critical vulnerabilities, including the use of unauthorized scheduled tasks, the presence of malicious scripts, and evidence of DNS poisoning. Immediate remediation steps include revoking unauthorized privileges, removing the malicious files, and correcting the DNS entries. Further recommendations include regular auditing of user activities, enhancing monitoring of scheduled tasks, and implementing stricter firewall rules.

Conclusion: The test highlighted the need for ongoing vigilance and the implementation of robust security measures to protect against unauthorized access and potential data breaches. Regular penetration testing is recommended to ensure the continued security of the system.