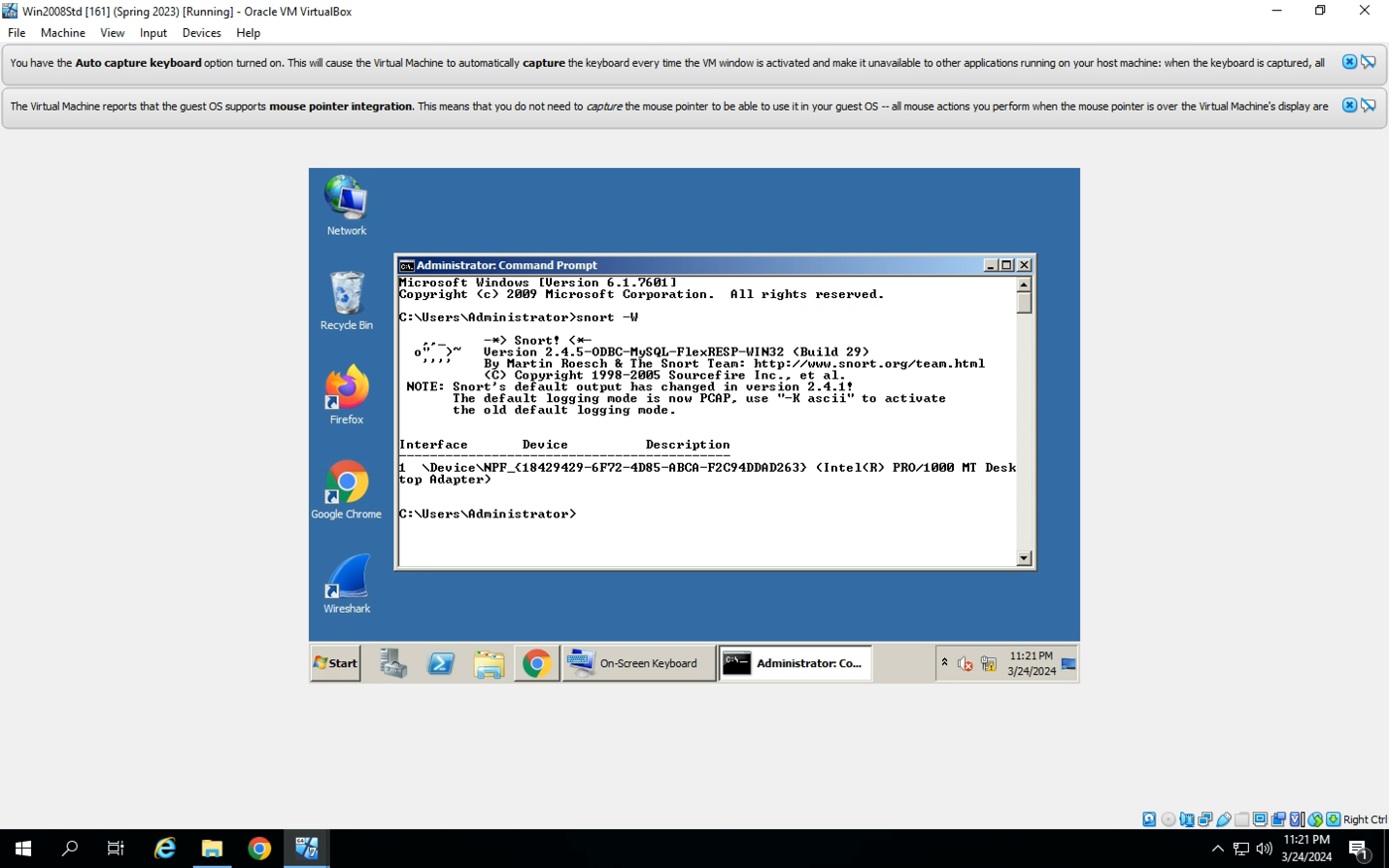
Action 4.1 – Port Scan Investigation

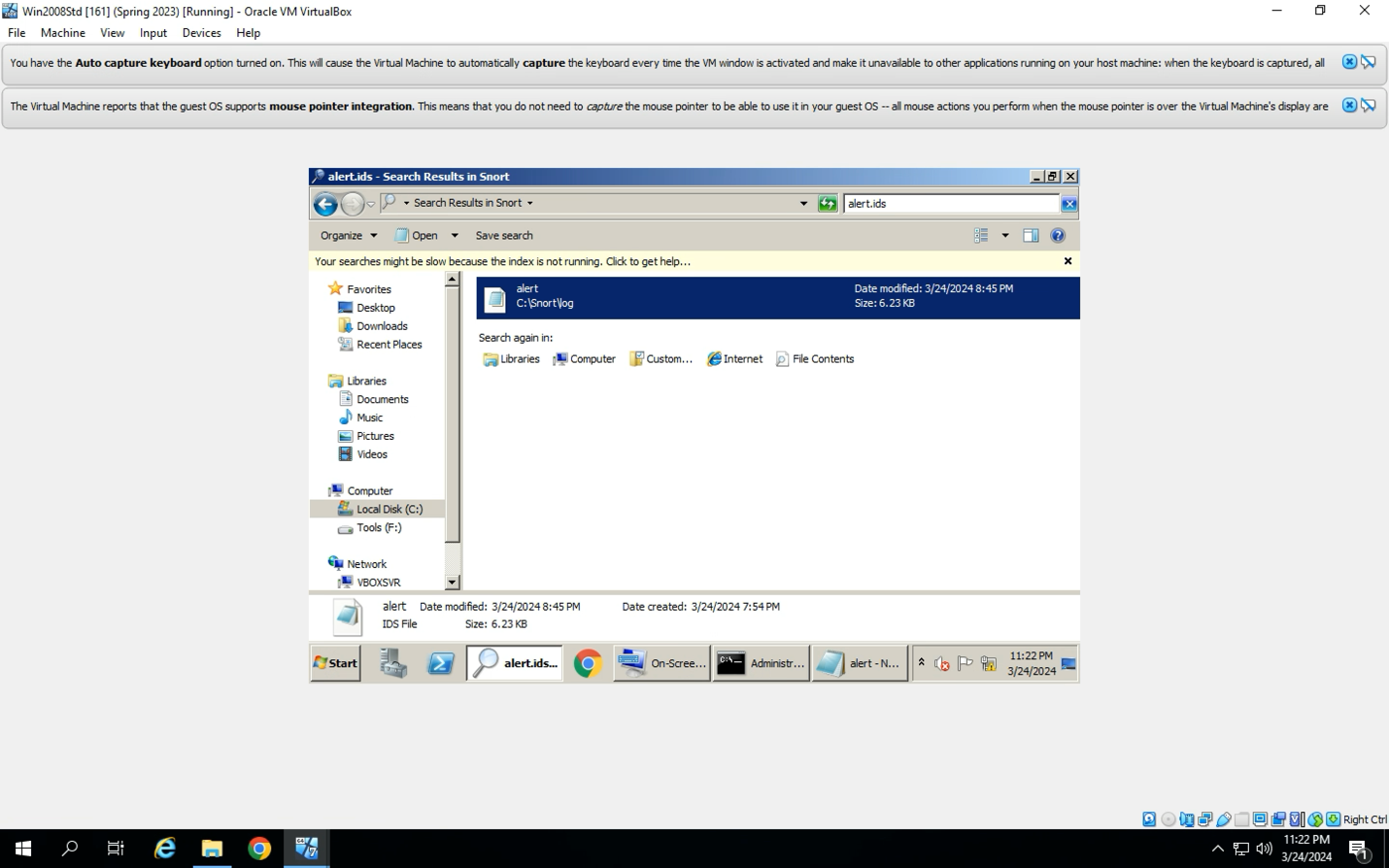
Presence of Piggy in Snort Console: The presence of the piggy icon in the Snort command console indicates that Snort is actively running and monitoring network traffic. This icon is typically displayed when Snort is running properly and detecting network events.

Recording Current Time for Zenmap Scan: Before initiating the Zenmap –sT scan, the current time in Windows 2008 was noted to be 8:45. This timestamp is crucial for correlating the scan results with other events and logs.

Checking Entries in alert.ids: We need to examine the entries in the alert.ids file to see if there are any alerts that match the timestamp recorded before initiating the Zenmap scan. This helps in identifying any suspicious network activity that may have been detected by Snort during the specified time period.

Identifying Ephemeral Ports and Their States: The ephemeral ports used by the attacker machine to scan five ports on 10.1.188.161 were determined. Additionally, the state of these ports, as reported in the ps2log file, was noted. Specifically, two ports were identified as open and three ports were reported as filtered. A screenshot of the ps2log file provides visual evidence of these findings.





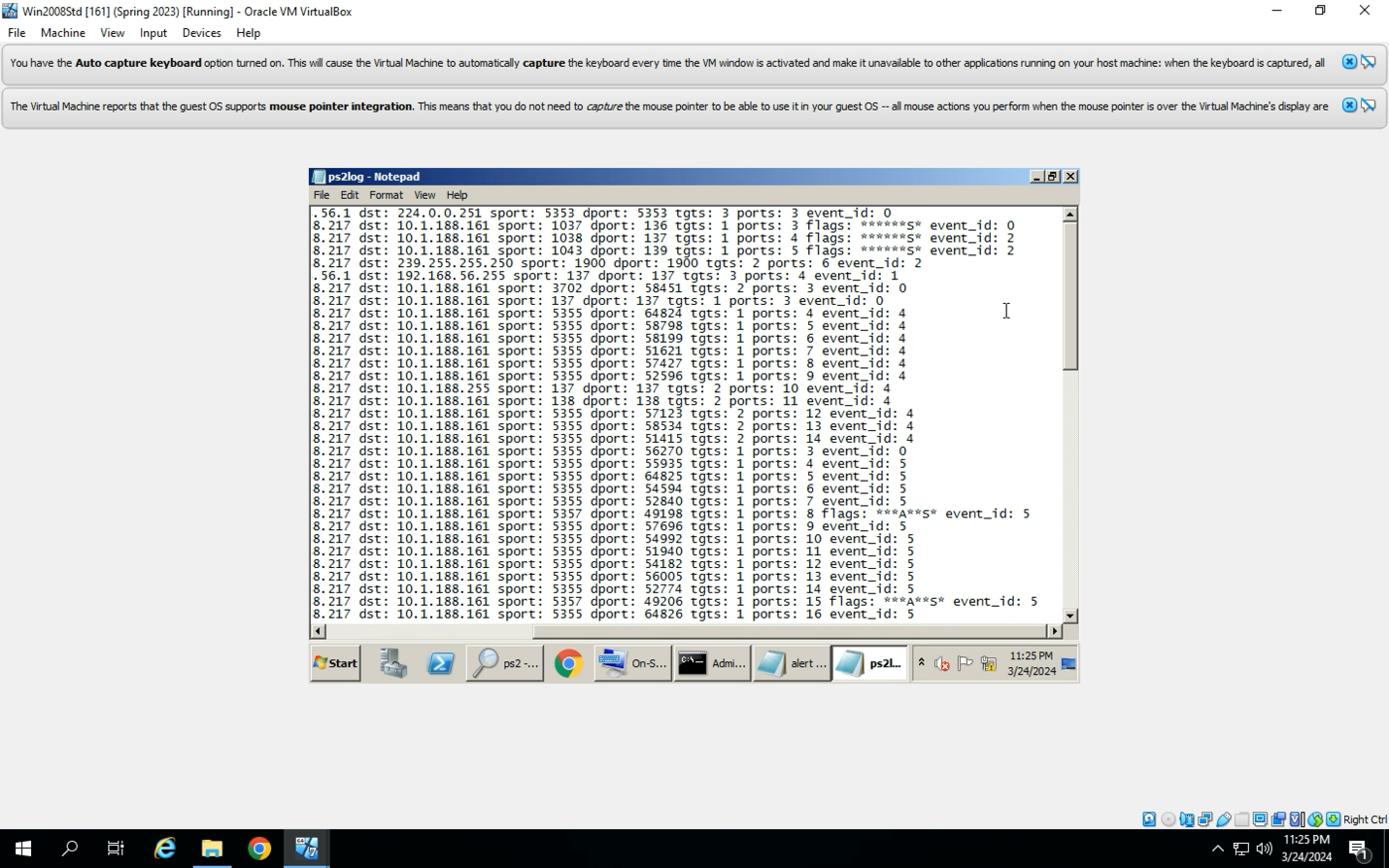
Action 4.2 – Xmas Scan Analysis

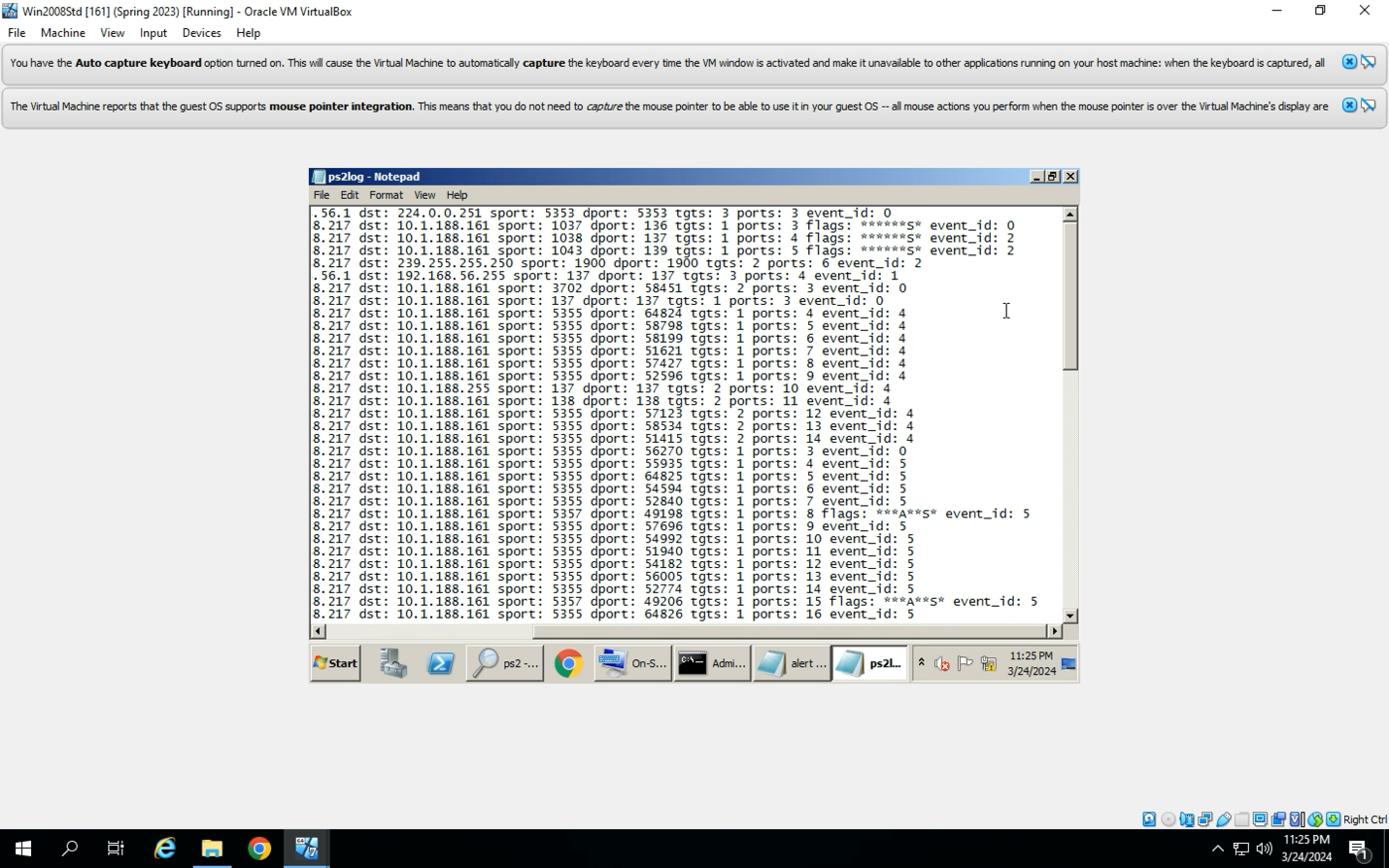
Identification of Alerts Containing "BCIS 4630 Xmas Scan": One alert containing the wording “BCIS 4630 Xmas Scan” was identified. This alert indicates that a network scan using the Xmas scan technique was detected by the intrusion detection system (IDS).

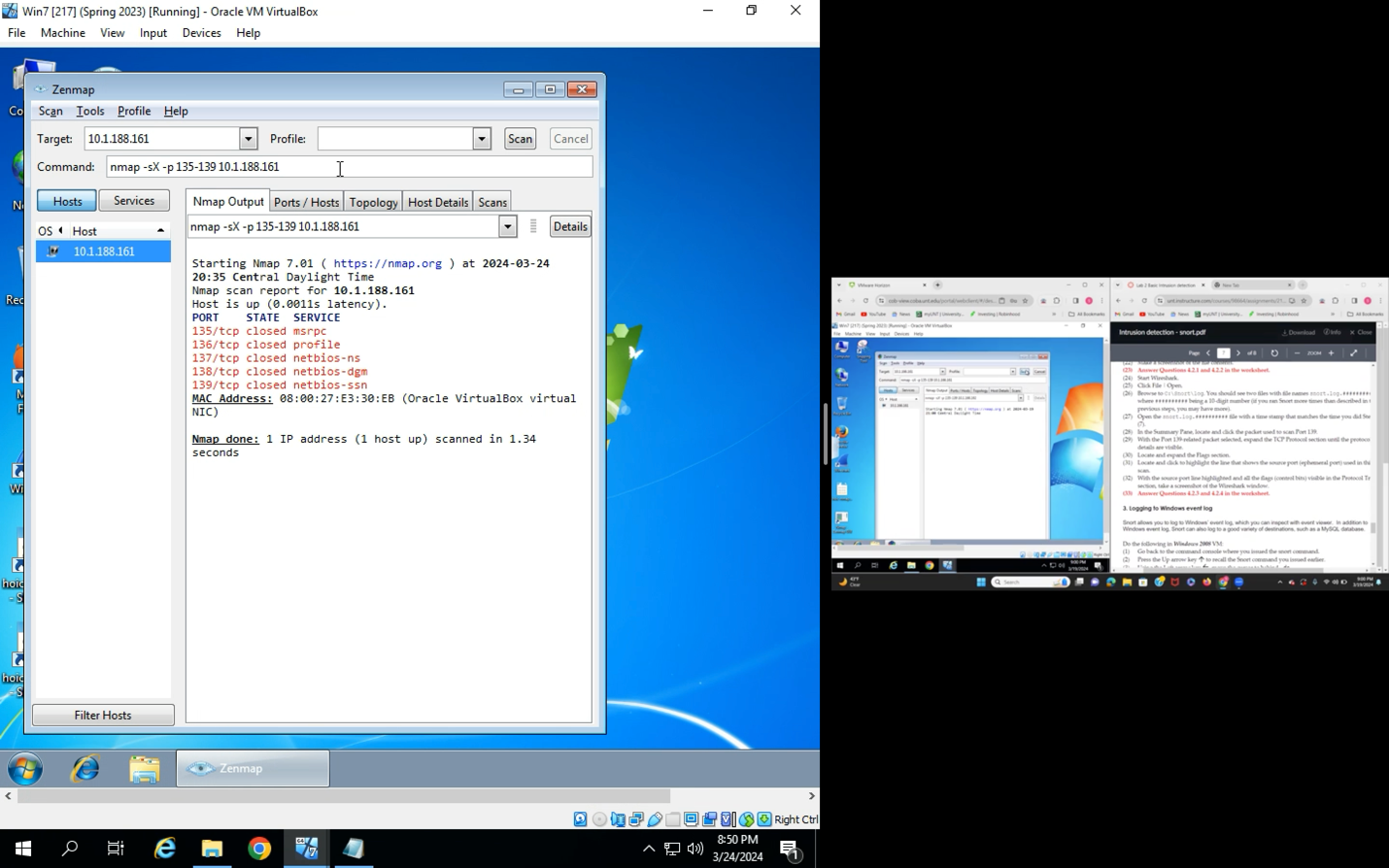
Analysis of Control Bits and Ephemeral Port: Further analysis of the alert is needed to determine how the control bits indicating the Xmas scan were represented and to identify the ephemeral port used in the scan. Screenshots of relevant sections of the alert log file provide visual evidence for these findings.

Identification of Control Bits in Wireshark: Wireshark was utilized to identify the control bits that were turned on during the Xmas scan. Understanding which control bits were set is essential for determining the nature of the scan and the potential vulnerabilities being targeted.

Verification of Ephemeral Port in Wireshark: The ephemeral port used for the Xmas scan was determined and cross-referenced with the port reported in the alert.ids file. Comparing these findings ensures the accuracy of the detected scan activity. Screenshots from Wireshark provide visual evidence of the identified ephemeral port and its correspondence with the alert.







**Action 4.3 – Windows Events Logging Examination**

Confirmation of Snort-Generated Events: The Event Viewer was used to confirm the presence of five Snort-generated events. These events are important indicators of potential security threats or suspicious activity detected by the intrusion detection system (IDS).

Examination of Details for Port 139 Scanning: Further investigation is required to examine the details related to scanning Port 139 within the Event Properties. Analyzing these details helps in understanding the specific characteristics of the detected network activity and any potential implications for security.