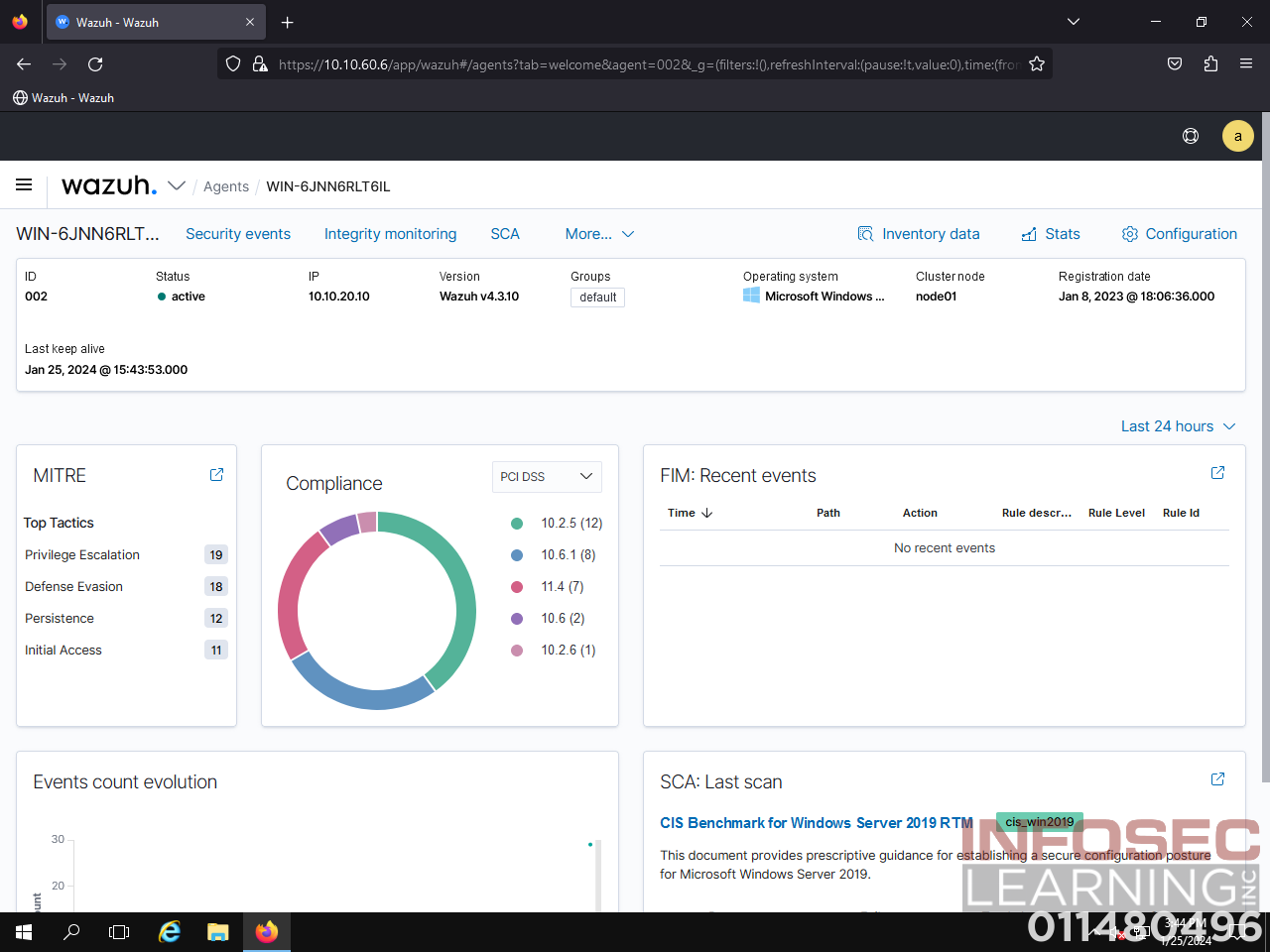


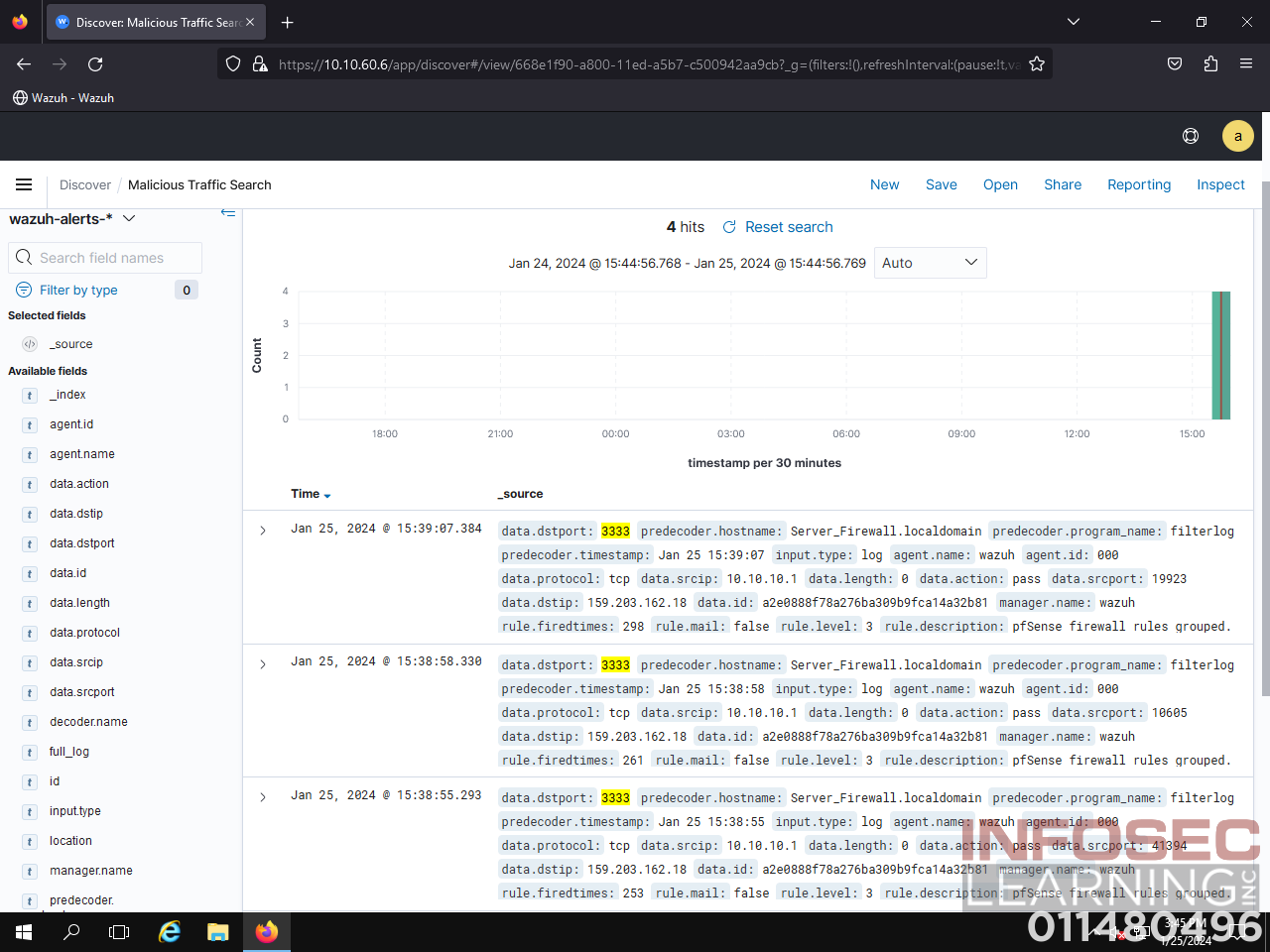
WGU - D483 - Security Operations

Correct Screenshots

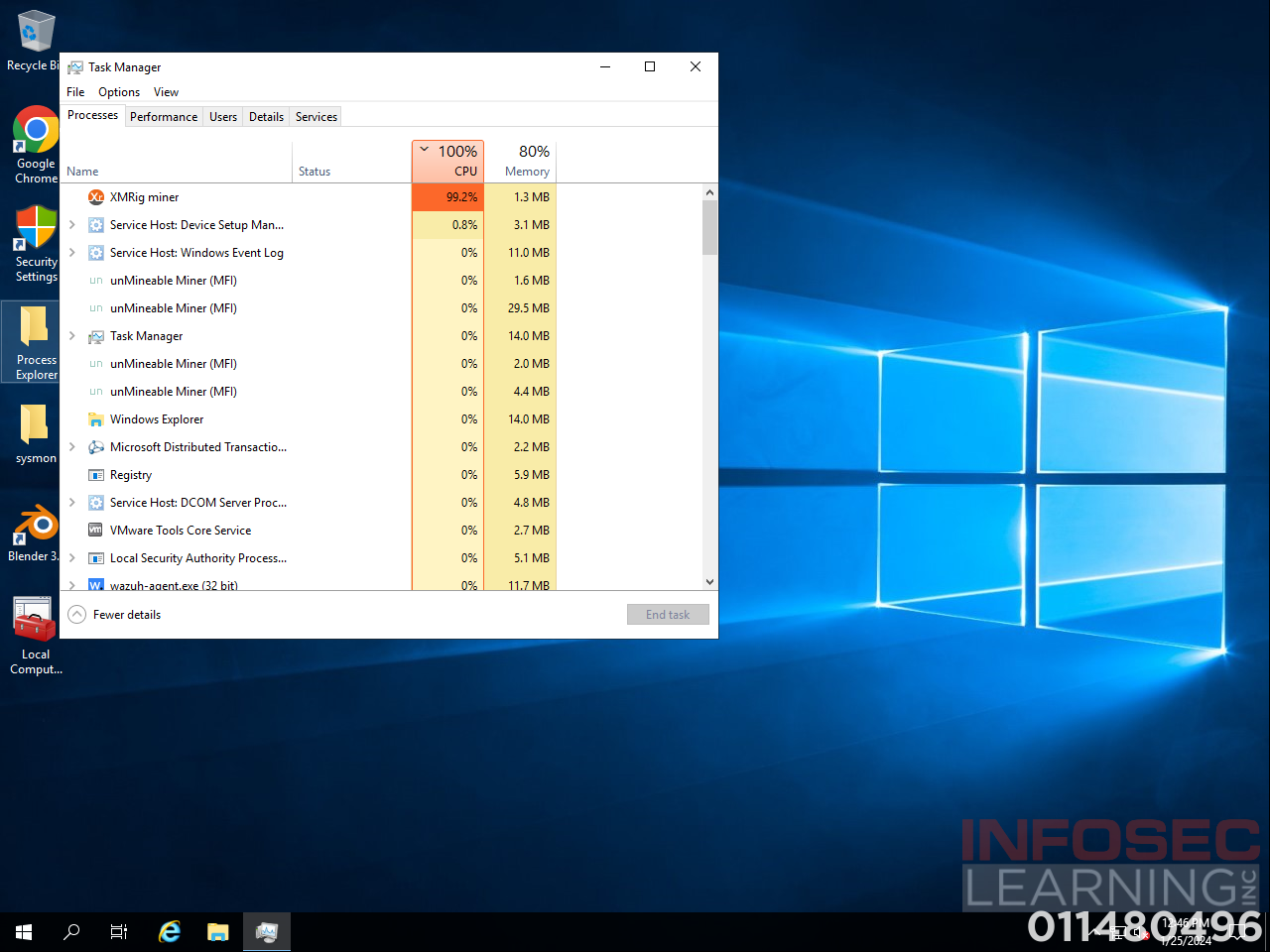
|  |  |
| --- | --- |
| **Question** | What is the IP value of the compromised system?   Answer should be in the format “XX.XX.XX.XX” as grouped numeric values. Ensure the IP value is visible within the Wazuh dashboard prior to answering Challenge #1. |
| **Answer** | 10.10.20.10 |



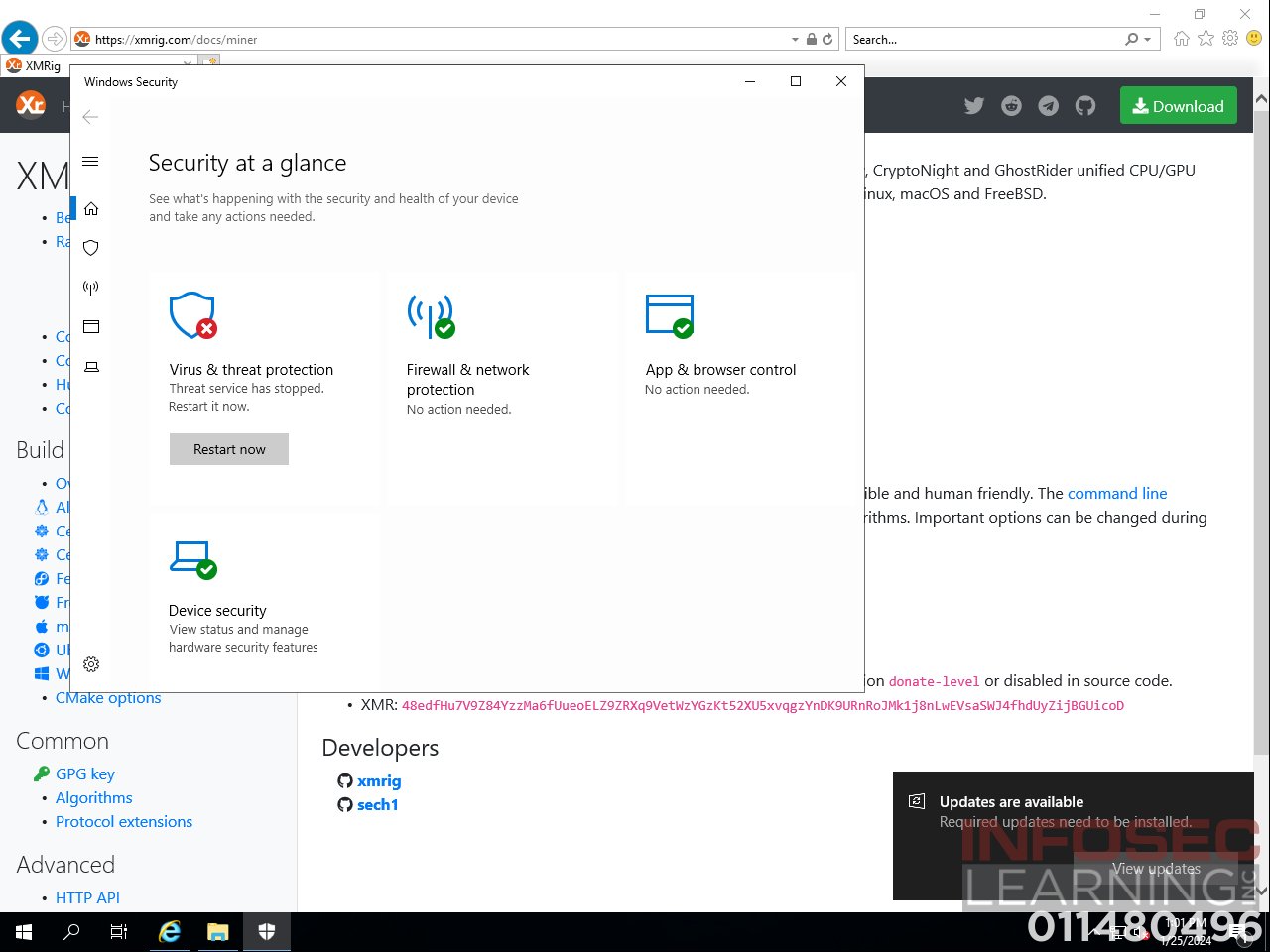
|  |  |
| --- | --- |
| **Question** | What is the destination port value from the metadata returned by the malicious traffic search?  Answer should be in the format “XXXX” as a four-digit numeric value. Ensure the destination port value is visible within the malicious traffic search results prior to answering Challenge #2. |
| **Answer** | 3333 |



|  |  |
| --- | --- |
| **Question** | What is the name of the process causing the highest CPU utilization in the compromised system?  Answer should be formatted as shown in the Task Manager, including capitalization. Ensure the process is visible within the Task Manager prior to answering Challenge #3. |
| **Answer** | XMRig miner |



|  |  |
| --- | --- |
| **Question** | What message is displayed to the right of the red “x” icon?  Answer should be formatted as shown in the “Virus & threat protection” window, including punctuation. Double-click on the “Virus & threat protection” menu and ensure the red icon and accompanying message are visible within the window prior to answering Challenge #4. |
| **Answer** | Threat service has stopped. Restart it now. |



|  |  |
| --- | --- |
| **Question** | Has a new rule been added to the firewall to block the TCP port from unauthorized outgoing traffic?  Answer should be “Yes” or “No”. Ensure the appropriately ordered firewall DMZ rules are visible within the Server Firewall user interface prior to answering Challenge #5. |
| **Answer** | Yes |

