Barbara Garcia

2/17/2024

**D483 – Security Operations Performance Assessment**

**A.** Incident Details

Regarding this incident, the incident numbers are HDE-1001, HDE-1050, and HDE-1972. The incident occurred on December 13th. Barbara Garcia, ID number 011883626 is the author of the report. The report was written on February 1st, 2024. On the date in question, engineering employees were unable to use the Pro-Engineer application to complete work tasks. It was freezing and crashing, resulting in a work stoppage. The incident response team consulted with the engineering department and found that a spear phishing email was sent to the server administrator. It was spoofed to look like it came from a vendor that normally sends legitimate updates for the server. The email contained a malicious download, which the administrator downloaded thinking it was a legitimate update, resulting in crypto malware being installed on the machine and utilizing almost all the computing power of the server, making the application unusable. “XMRig is an open-source software designed for mining cryptocurrencies like Monero or Bitcoin. However, it is also commonly abused by cybercriminals in their attacks, who infect computers with cryptojackers and use their resources to mine cryptocurrency on the attacker’s behalf (*XMRig Malware*, n.d.).” The impacted users were Maya Patel, Diego Martin, and Alex Lee. Functional impact was determined to be medium. The design team was unable to work, but the rest of the company was unaffected. Incident priority was determined to be high since engineers being able to use the design server is a high priority at the company. The timeline is as follows:

* 10:00am: First Helpdesk ticket submitted indicating that the Pro-Engineer application is not working.
* 3:14pm: Second Helpdesk ticket submitted about the issue with Pro-Engineer application. Work stoppage reported.
* 3:20pm: Third Helpdesk ticket submitted for the same issue.
* 3:30pm: Used SIEM to investigate server activity. Found malicious traffic to port 3333.
* 3:35pm: Task manager indicated that a program called XMRig miner is using almost all the server’s CPU.
* 3:37pm: Research indicated crypto mining malware.
* 3:40pm: Ended XMRig miner task in Task Manager
* 3:45pm: Disabled, then reenabled Microsoft Defender Antivirus.
* 3:50pm: Ran Antivirus scan to ensure malware was no longer installed.
* 3:55pm: Added firewall rule to DMZ blocking traffic to port 3333 of the server and moved rule to the top of the list.

**B. Impacted System**

The impacted system in this incident was the application server with the hostname of WIN-6JNN6RLT6IL and IP address of 10.10.20.10, running the Microsoft Windows Server 2019 operating system.

**C. Details**

Wazuh logged potentially malicious traffic to port 3333. Log reflects that firewall rules permitted access to the affected port.

**D. Remediation**

To restore functionality of the impacted system, incident response team accessed the server and used Task Manager to terminate the crypto miner process that was running. We then disabled, then re-started Windows Defender Antivirus and performed a virus scan.

To restore network security, incident response team accessed the firewall management for the DMZ firewall and added a rule to block all traffic to port 3333.

**E. Lessons Learned**

To prevent similar incidents in the future, we recommend implementing regular social engineering awareness training for all employees and hardening servers and firewalls to lessen the ways a threat actor can gain access.

Providing thorough and regular social engineering awareness training to all employees so they can learn to identify the signs of phishing emails and verify downloads to make sure they are legitimate before installing on any devices will help prevent employees inadvertently introducing malware into the network.

We recommend the company use CIS templates as a guide to secure company assets. Blocking access to all unnecessary ports and using secure port options for necessary business tasks will make it more difficult for threat actors to be able to communicate with our network.

**F. Screenshot Evidence**

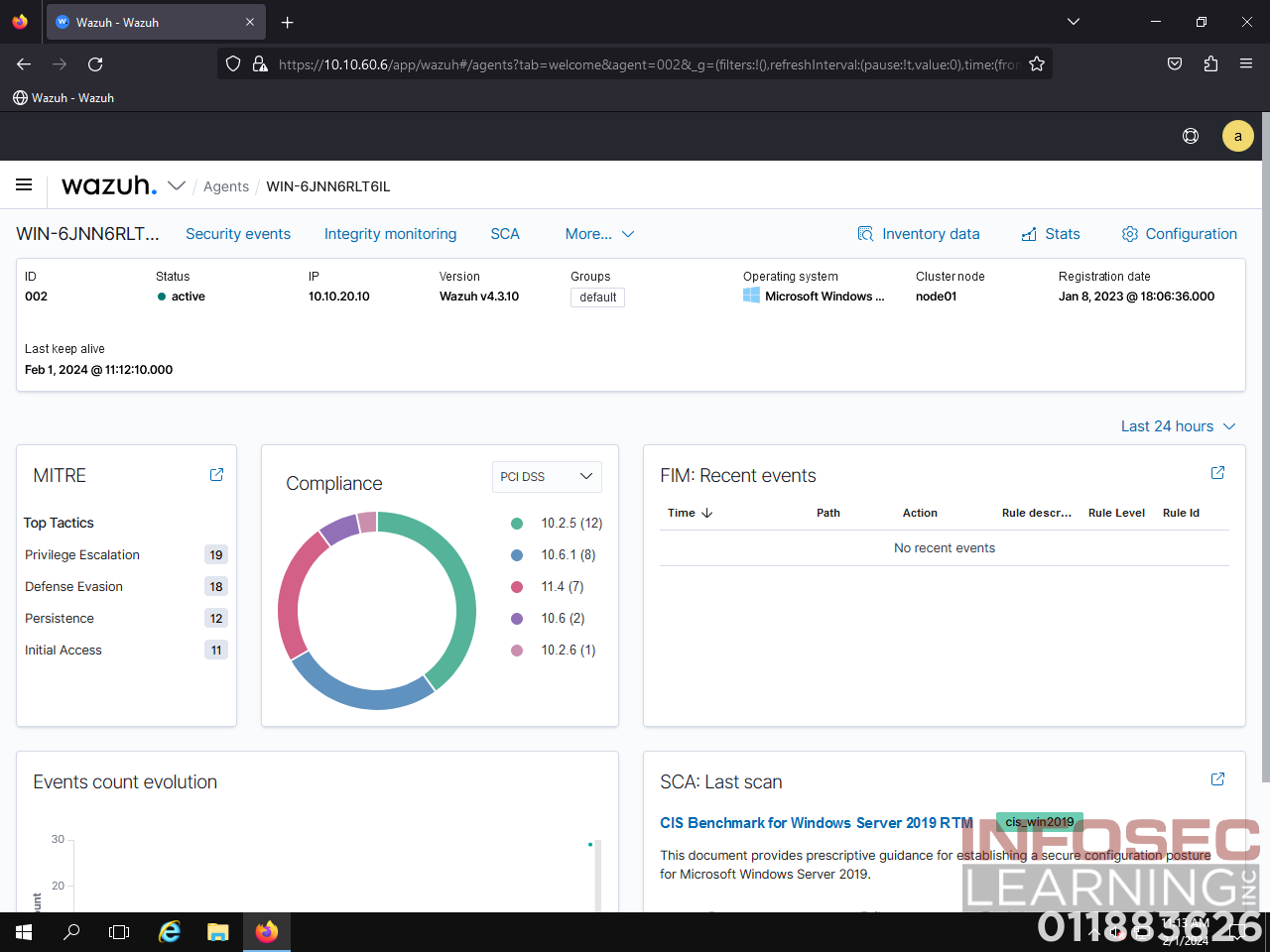
A close up of a logo

Description automatically generated

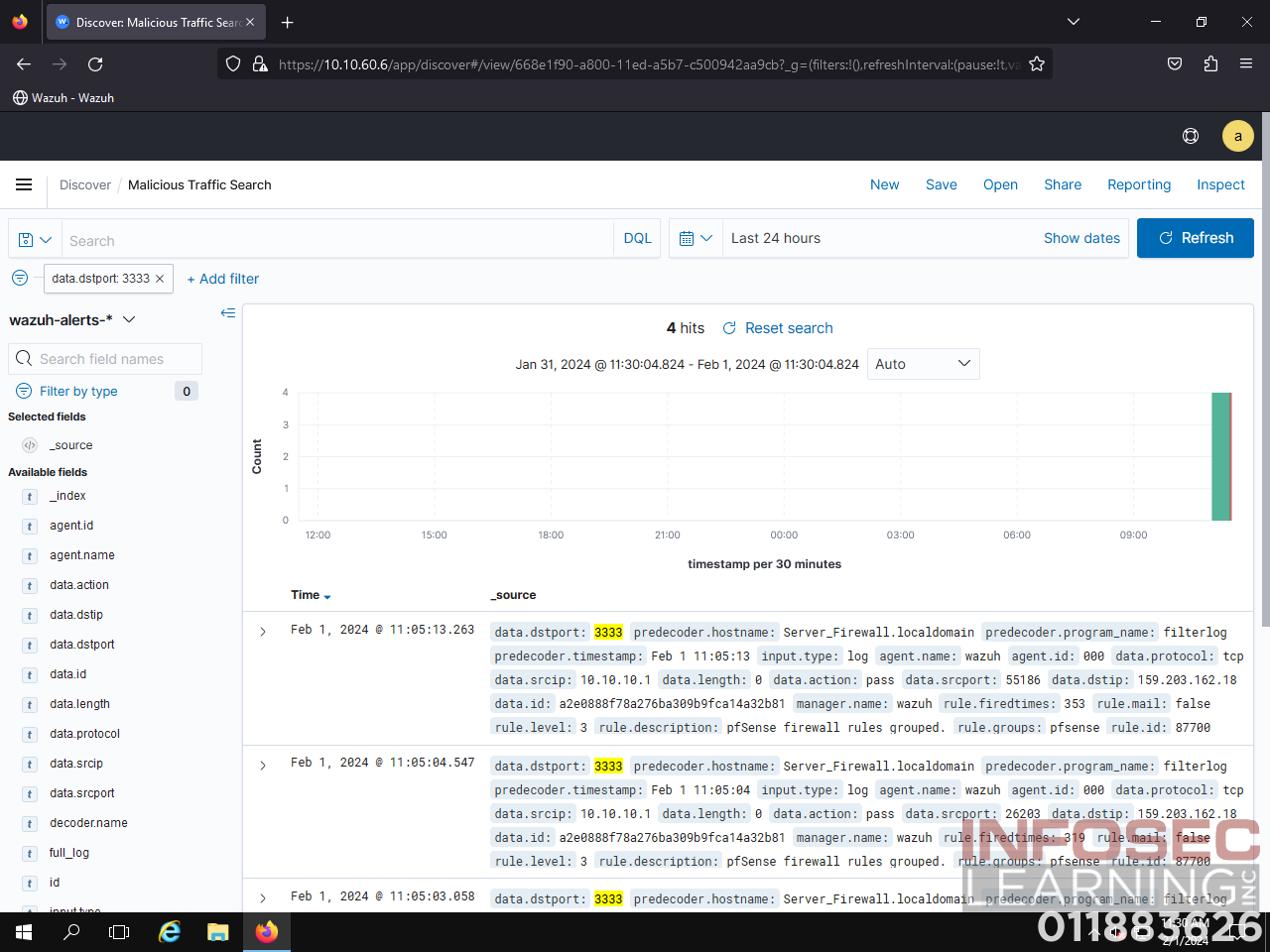
WGU - D483 - Security Operations

Correct Screenshots

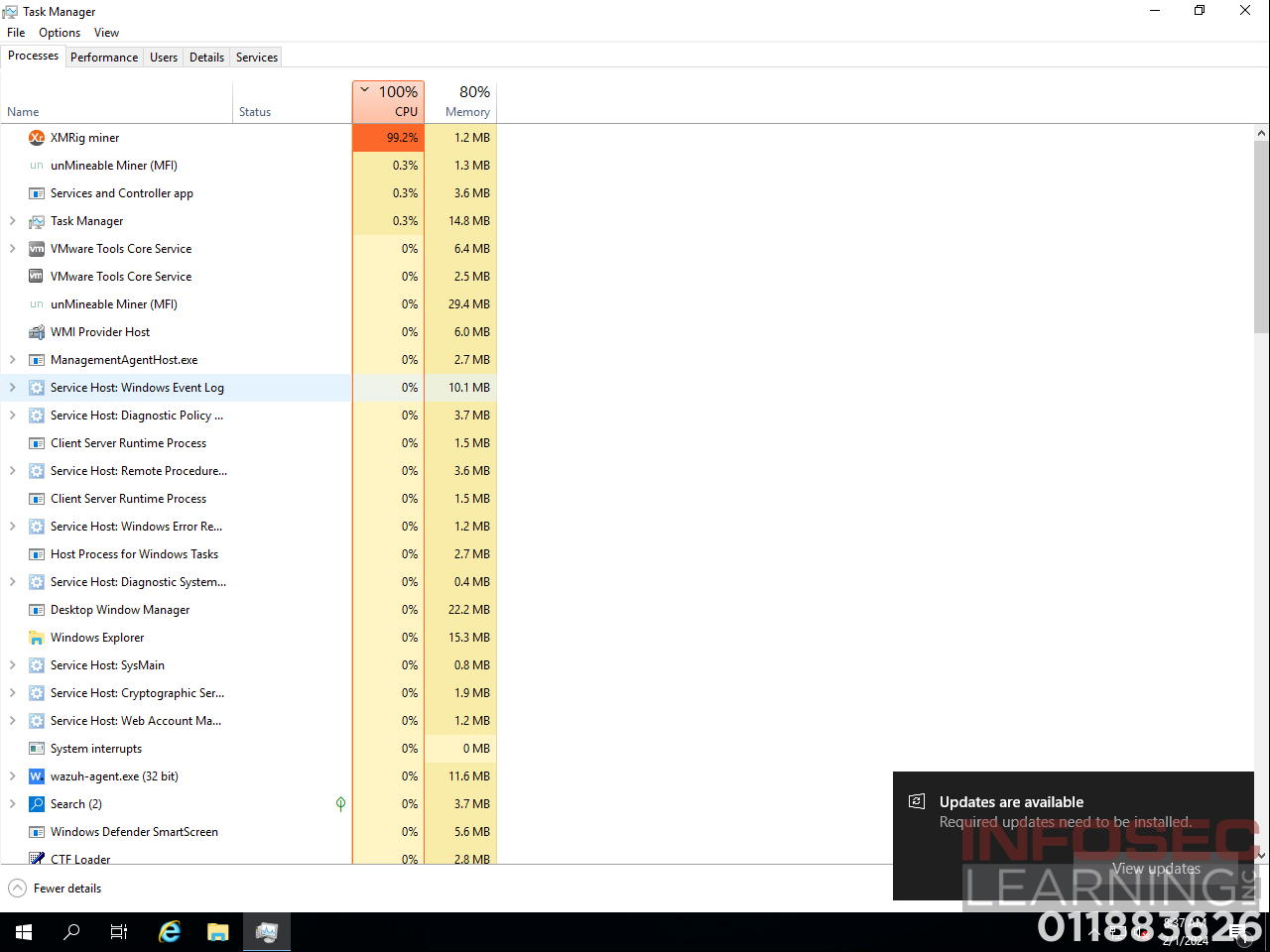
|  |  |
| --- | --- |
| **Question** | What is the IP value of the compromised system?   Answer should be in the format “XX.XX.XX.XX” as grouped numeric values. Ensure the IP value is visible within the Wazuh dashboard prior to answering Challenge #1. |
| **Answer** | 10.10.20.10 |



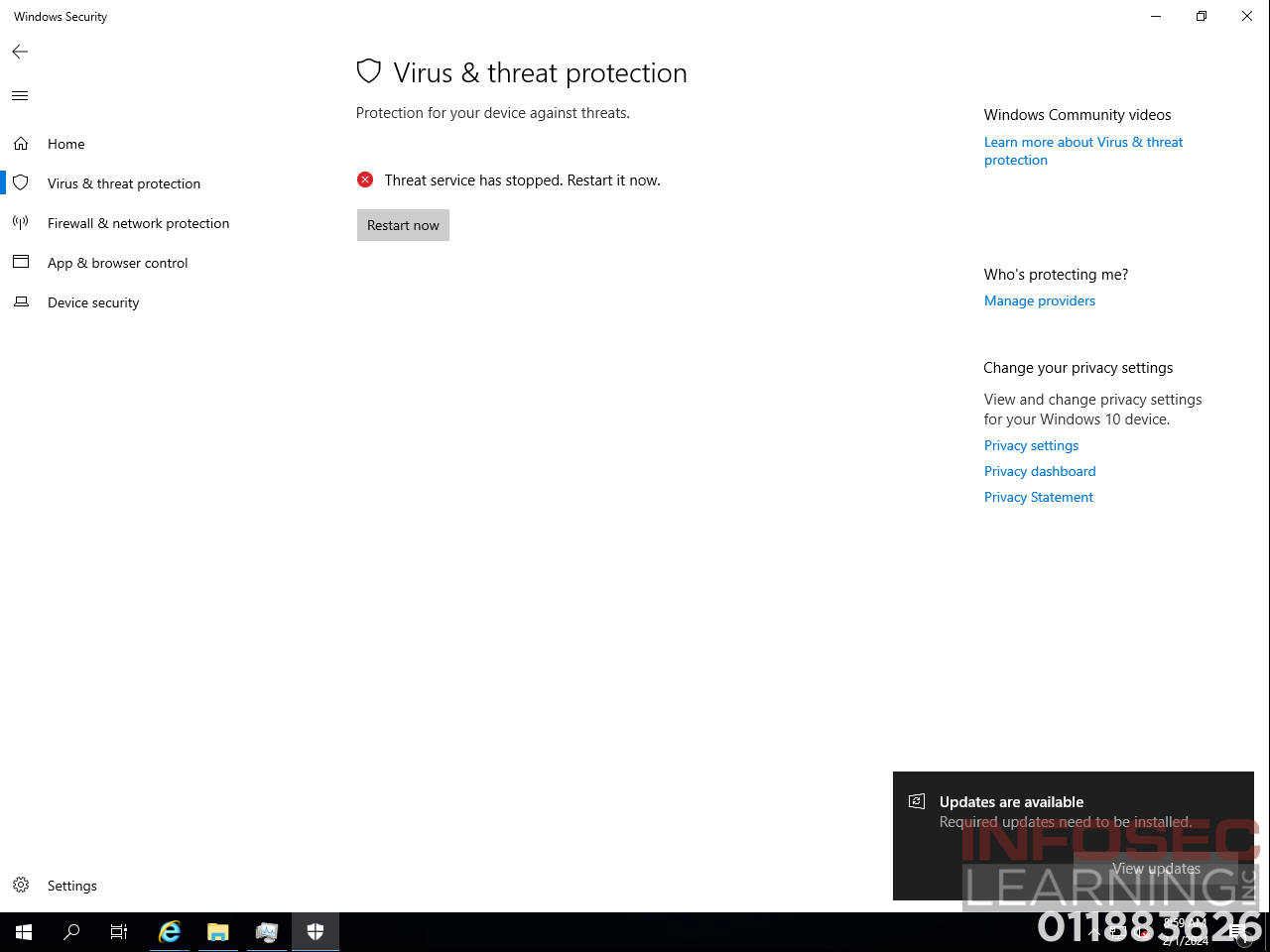
|  |  |
| --- | --- |
| **Question** | What is the destination port value from the metadata returned by the malicious traffic search?  Answer should be in the format “XXXX” as a four-digit numeric value. Ensure the destination port value is visible within the malicious traffic search results prior to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



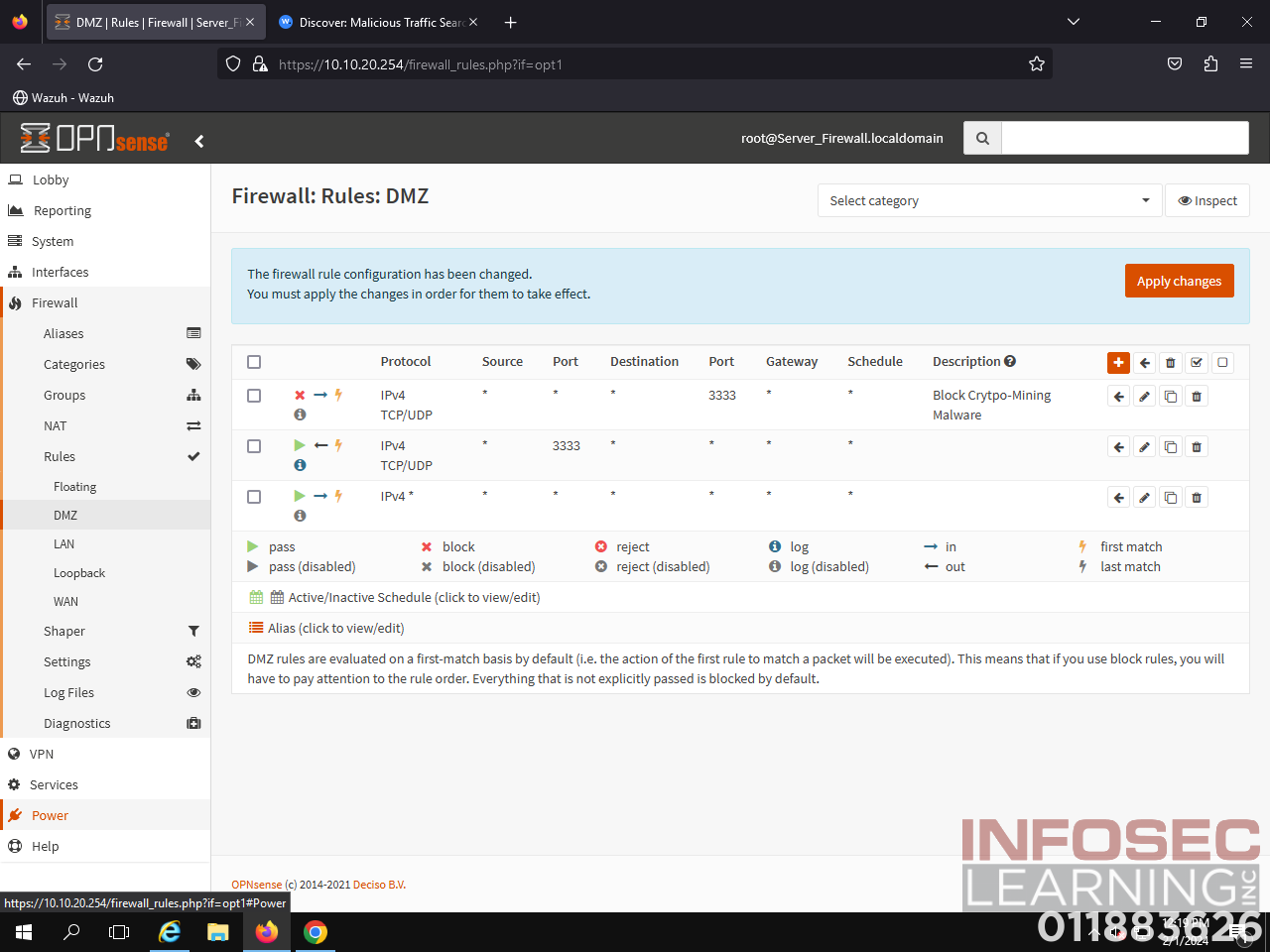
|  |  |
| --- | --- |
| **Question** | What is the name of the process causing the highest CPU utilization in the compromised system?  Answer should be formatted as shown in the Task Manager, including capitalization. Ensure the process is visible within the Task Manager prior to answering Challenge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



Works Cited

*XMRig Malware*. (n.d.). Check Point Software. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-malware/xmrig-malware/