INFOSEC LEARNING INC

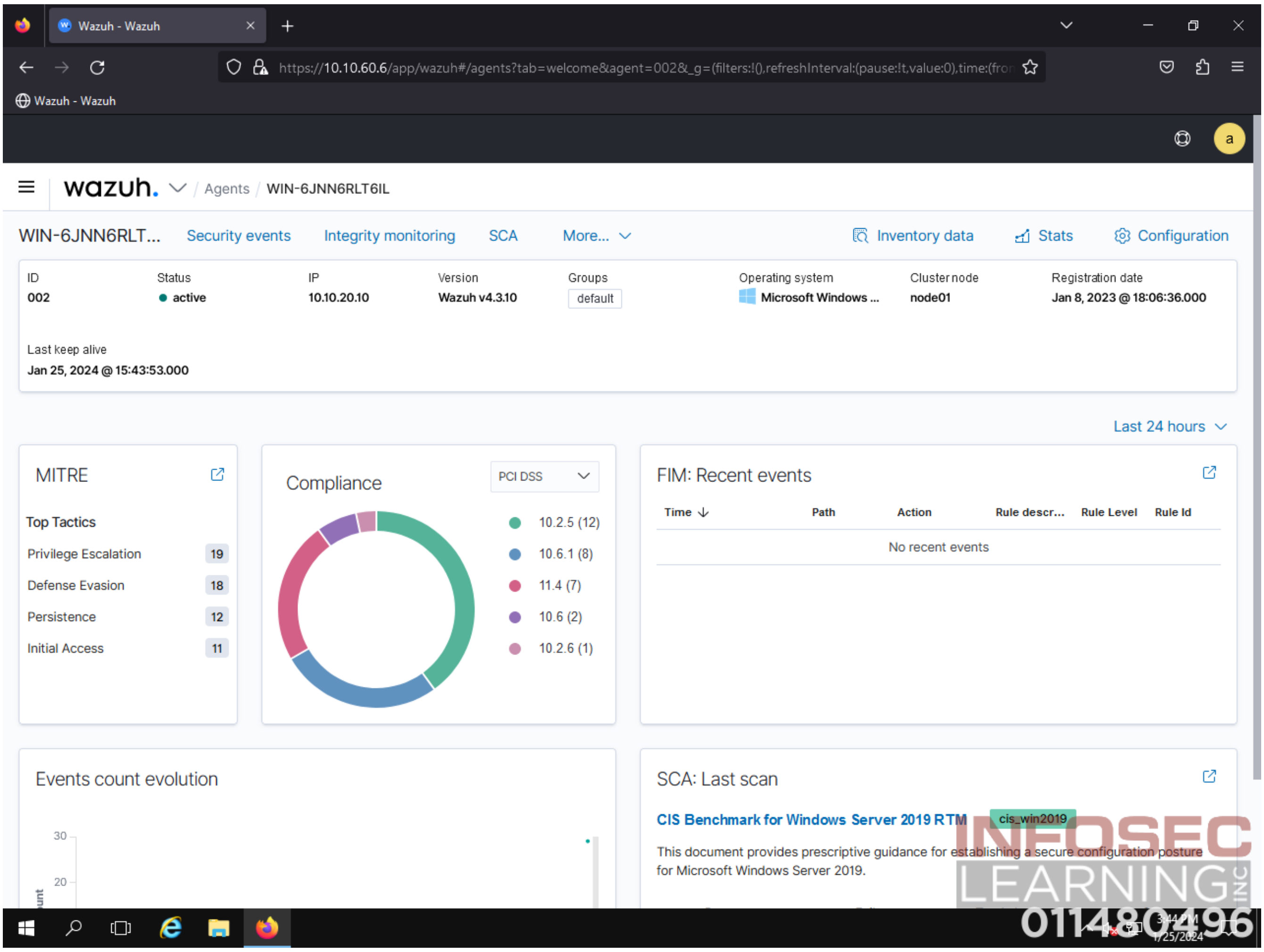
# WGU - D483 - Security Operations

## 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



| ID | Status | IP | Version | Groups | Operating system | Cluster node | Registration date |
|---|---|---|---|---|---|---|---|
| 002 | ● active | 10.10.20.10 | Wazuh v4.3.10 | default | Microsoft Windows ... | node01 | Jan 8, 2023 @ 18:06:36.000 |

Last keep alive
Jan 25, 2024 @ 15:43:53.000

MITRE

Top Tactics

| | |
|---|---|
| Privilege Escalation | 19 |
| Defense Evasion | 18 |
| Persistence | 12 |
| Initial Access | 11 |

Compliance

FIM: Recent events

| Time ↓ | Path | Action | Rule descr... | Rule Level | Rule Id |
|---|---|---|---|---|---|
| No recent events | | | | | |

Events count evolution

SCA: Last scan

CIS Benchmark for Windows Server 2019 RTM cis_win2019

This document provides prescriptive guidance for establishing a secure configuration posture for Microsoft Windows Server 2019.

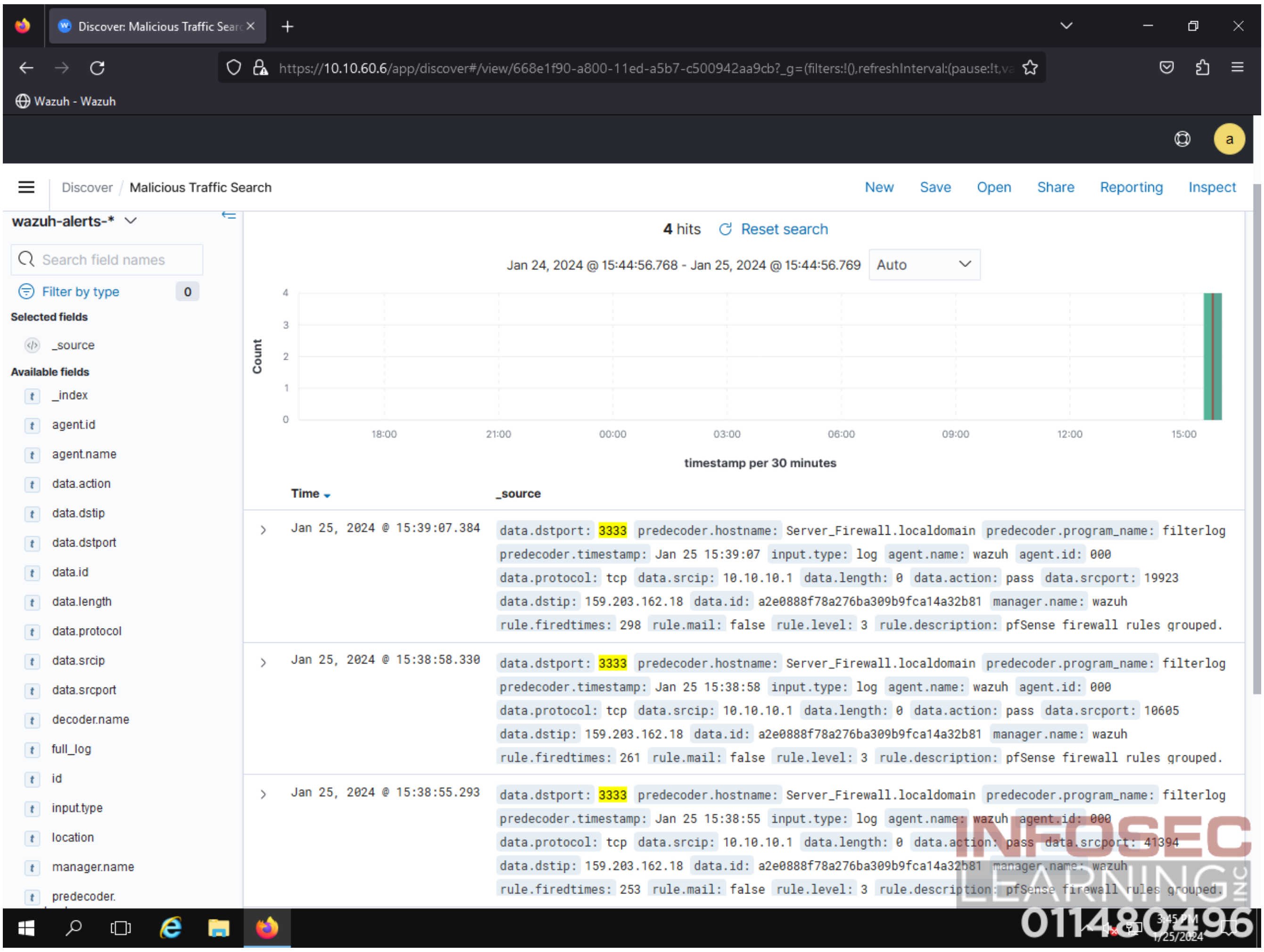
**Question**

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

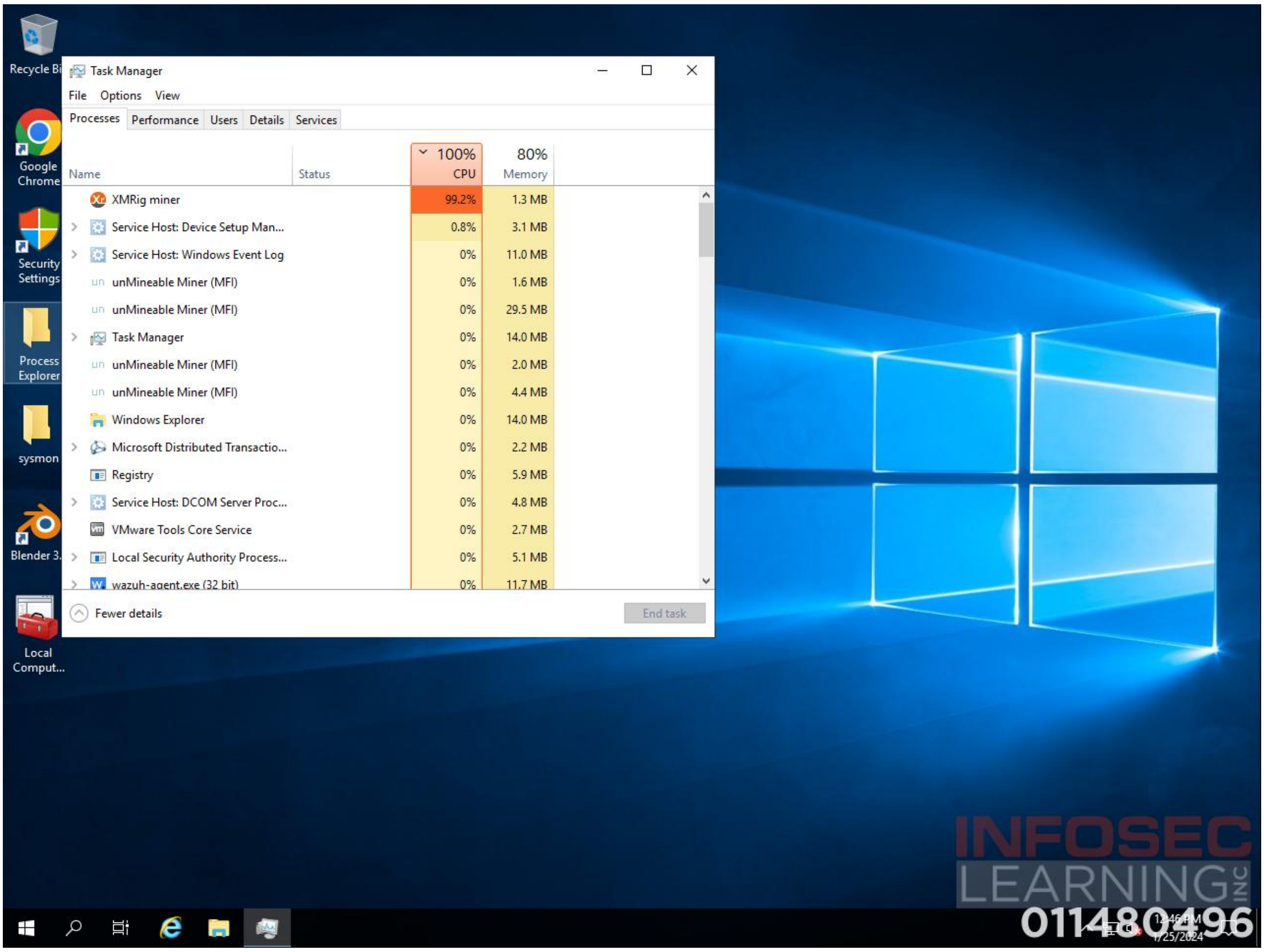


```
Jan 25, 2024 @ 15:39:07.384  data.dstport: 3333 predecoder.hostname: Server_Firewall.localdomain predecoder.program_name: filterlog
                             predecoder.timestamp: Jan 25 15:39:07 input.type: log agent.name: wazuh agent.id: 000
                             data.protocol: tcp data.srcip: 10.10.10.1 data.length: 0 data.action: pass data.srcport: 19923
                             data.dstip: 159.203.162.18 data.id: a2e0888f78a276ba309b9fca14a32b81 manager.name: wazuh
                             rule.firedtimes: 298 rule.mail: false rule.level: 3 rule.description: pfSense firewall rules grouped.

Jan 25, 2024 @ 15:38:58.330  data.dstport: 3333 predecoder.hostname: Server_Firewall.localdomain predecoder.program_name: filterlog
                             predecoder.timestamp: Jan 25 15:38:58 input.type: log agent.name: wazuh agent.id: 000
                             data.protocol: tcp data.srcip: 10.10.10.1 data.length: 0 data.action: pass data.srcport: 10605
                             data.dstip: 159.203.162.18 data.id: a2e0888f78a276ba309b9fca14a32b81 manager.name: wazuh
                             rule.firedtimes: 261 rule.mail: false rule.level: 3 rule.description: pfSense firewall rules grouped.

Jan 25, 2024 @ 15:38:55.293  data.dstport: 3333 predecoder.hostname: Server_Firewall.localdomain predecoder.program_name: filterlog
                             predecoder.timestamp: Jan 25 15:38:55 input.type: log agent.name: wazuh agent.id: 000
                             data.protocol: tcp data.srcip: 10.10.10.1 data.length: 0 data.action: pass data.srcport: 41394
                             data.dstip: 159.203.162.18 data.id: a2e0888f78a276ba309b9fca14a32b81 manager.name: wazuh
                             rule.firedtimes: 253 rule.mail: false rule.level: 3 rule.description: pfSense firewall rules grouped.
```

**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

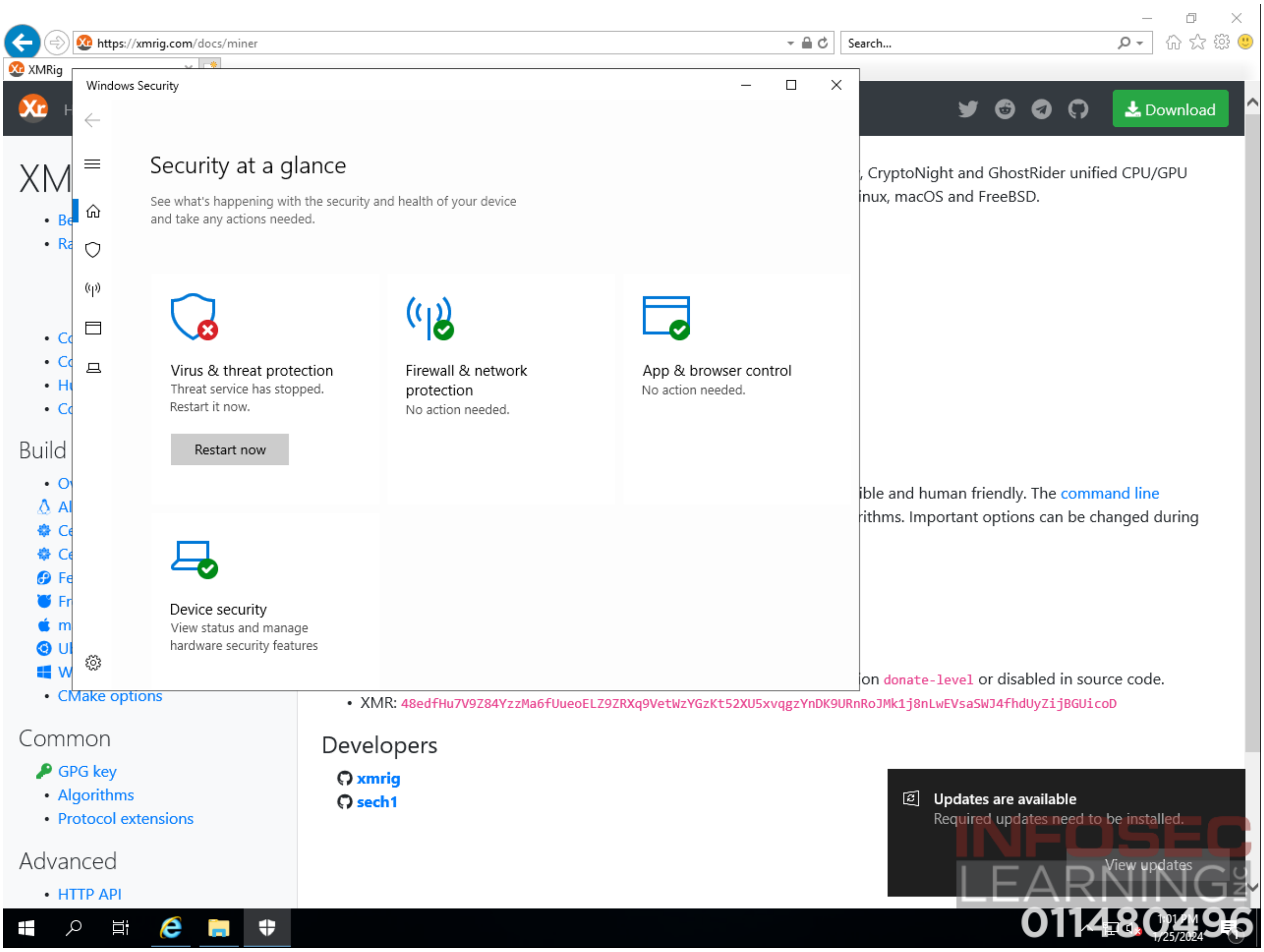


| Name | Status | 100% CPU | 80% Memory |
|---|---|---|---|
| XMRig miner | | 99.2% | 1.3 MB |
| Service Host: Device Setup Man... | | 0.8% | 3.1 MB |
| Service Host: Windows Event Log | | 0% | 11.0 MB |
| unMineable Miner (MFI) | | 0% | 1.6 MB |
| unMineable Miner (MFI) | | 0% | 29.5 MB |
| Task Manager | | 0% | 14.0 MB |
| unMineable Miner (MFI) | | 0% | 2.0 MB |
| unMineable Miner (MFI) | | 0% | 4.4 MB |
| Windows Explorer | | 0% | 14.0 MB |
| Microsoft Distributed Transactio... | | 0% | 2.2 MB |
| Registry | | 0% | 5.9 MB |
| Service Host: DCOM Server Proc... | | 0% | 4.8 MB |
| VMware Tools Core Service | | 0% | 2.7 MB |
| Local Security Authority Process... | | 0% | 5.1 MB |
| wazuh-agent.exe (32 bit) | | 0% | 11.7 MB |

**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.



Security at a glance

See what's happening with the security and health of your device and take any actions needed.

Virus & threat protection
Threat service has stopped.
Restart it now.

Restart now

Firewall & network protection
No action needed.

App & browser control
No action needed.

Device security
View status and manage hardware security features

, CryptoNight and GhostRider unified CPU/GPU
inux, macOS and FreeBSD.

ible and human friendly. The command line
rithms. Important options can be changed during

ion donate-level or disabled in source code.

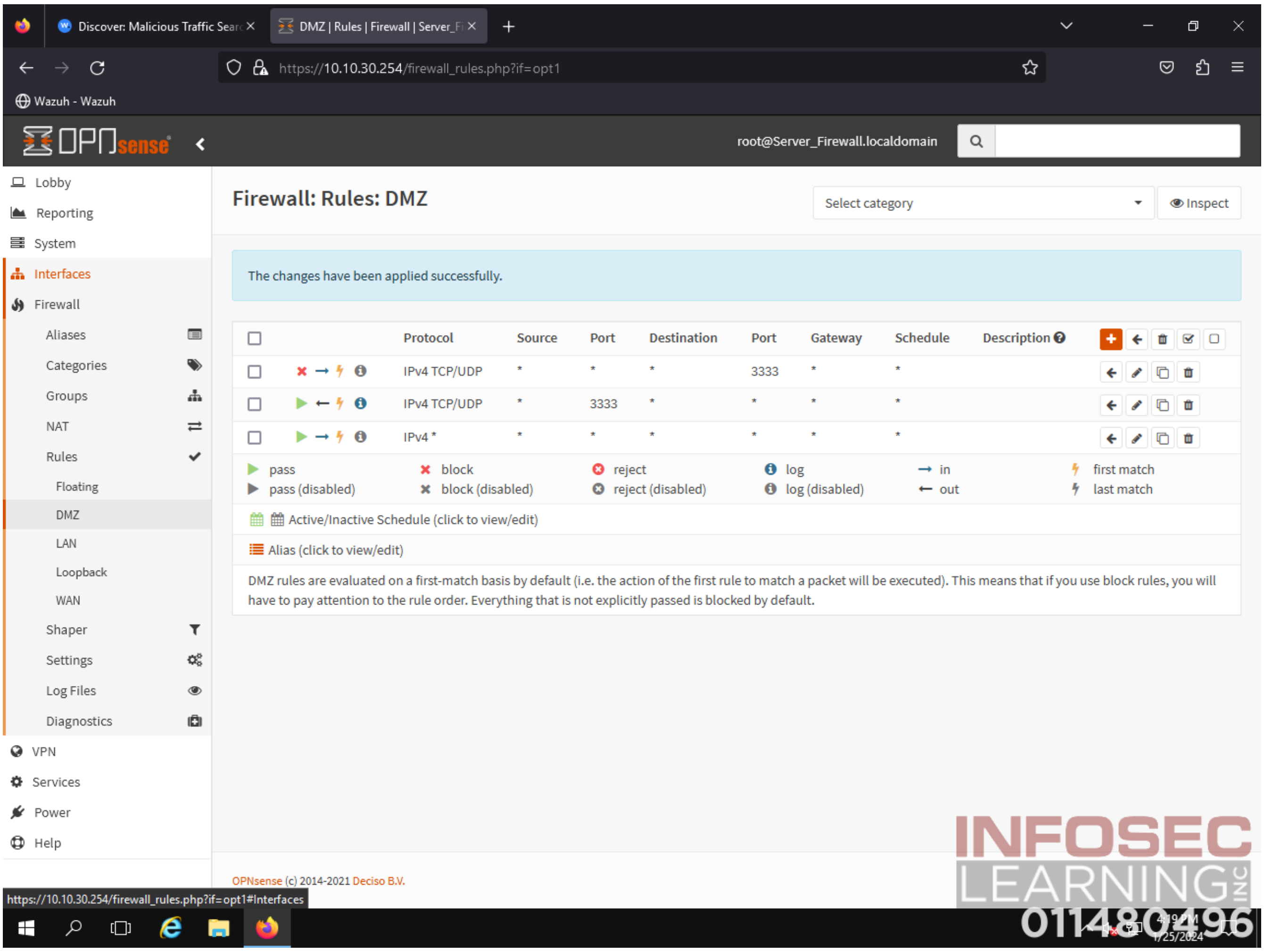
- XMR: 48edfHu7V9Z84YzzMa6fUueoELZ9ZRXq9VetWzYGzKt52XU5xvqgzYnDK9URnRoJMk1j8nLwEVsaSWJ4fhdUyZijBGUicoD

Updates are available
Required updates need to be installed.

**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


Discover: Malicious Traffic Searc
DMZ | Rules | Firewall | Server_Fi
https://10.10.30.254/firewall_rules.php?if=opt1
Wazuh - Wazuh
OPNsense
root@Server_Firewall.localdomain
Lobby
Reporting
System
Interfaces
Firewall
Aliases
Categories
Groups
NAT
Rules
Floating
DMZ
LAN
Loopback
WAN
Shaper
Settings
Log Files
Diagnostics
VPN
Services
Power
Help
Select category
Inspect
https://10.10.30.254/firewall_rules.php?if=opt1#Interfaces
1/25/2024

**Firewall: Rules: DMZ**

The changes have been applied successfully.

| ☐ | | Protocol | Source | Port | Destination | Port | Gateway | Schedule | Description |
|---|---|---|---|---|---|---|---|---|---|
| ☐ | ✖ → ⚡ ℹ | IPv4 TCP/UDP | * | * | * | 3333 | * | * | |
| ☐ | ▶ ← ⚡ ℹ | IPv4 TCP/UDP | * | 3333 | * | * | * | * | |
| ☐ | ▶ → ⚡ ℹ | IPv4 * | * | * | * | * | * | * | |

▶ pass ✖ block ⊗ reject ℹ log → in ⚡ first match
▶ pass (disabled) ✖ block (disabled) ⊗ reject (disabled) ℹ log (disabled) ← out ⚡ last match

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

DMZ rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

OPNsense (c) 2014-2021 Deciso B.V.