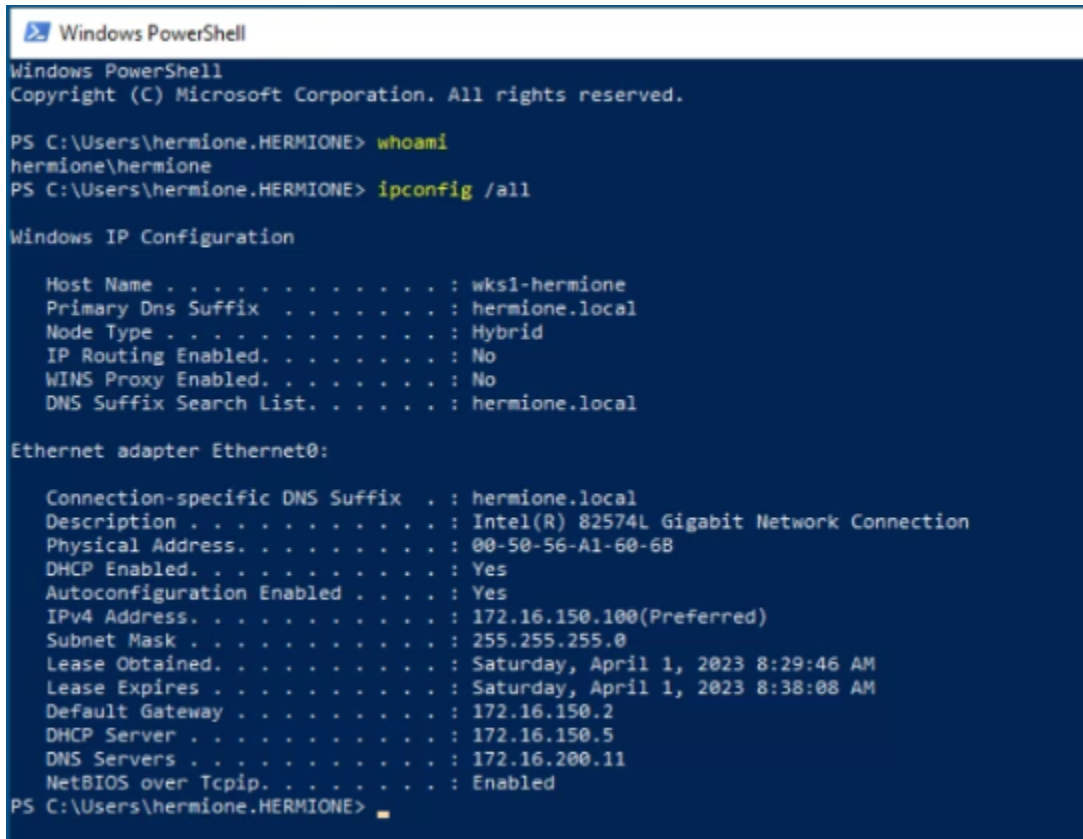


Lab 10.1 - Windows Logging - S23

💡 You've worked with Wazuh all semester. In this lab you are going to install the wazuh agent on your LAN and MGMT based windows system. **Please turn off traveler, nginx, and jump. We will not need them for this module.**

Deliverable 1. Install Active Directory Domain Services on mgmt02. Join wks1 to your new domain. Provide a screenshot showing a whoami and an ipconfig /all on wks1 that indicates you are logged in as a domain user yourname-user@yourdomain.local

A screenshot of a Windows PowerShell window with a dark blue background. The title bar says 'Windows PowerShell'. The text inside shows the user 'hermione\hermione' running 'whoami' and 'ipconfig /all'. The 'ipconfig /all' output shows network details for 'wks1-hermione', including a primary DNS suffix of 'hermione.local' and an IPv4 address of '172.16.150.100'.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\hermione.HERMIONE> whoami
hermione\hermione
PS C:\Users\hermione.HERMIONE> ipconfig /all

Windows IP Configuration

    Host Name . . . . . : wks1-hermione
    Primary Dns Suffix . . . . . : hermione.local
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : hermione.local

Ethernet adapter Ethernet0:

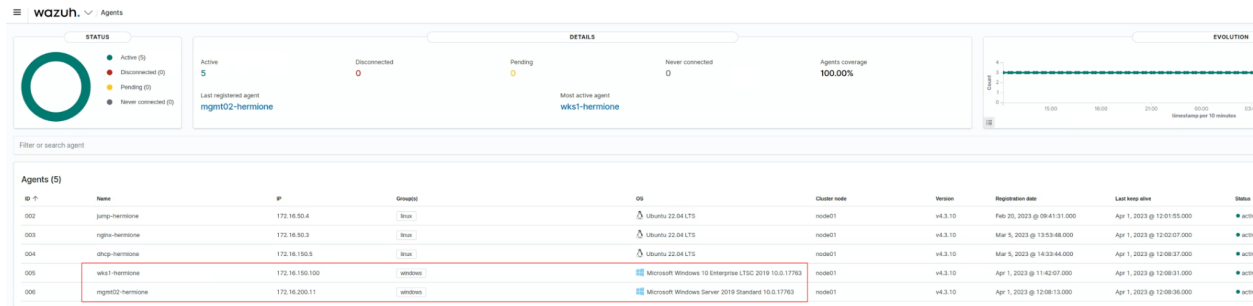
    Connection-specific DNS Suffix . : hermione.local
    Description . . . . . : Intel(R) 82574L Gigabit Network Connection
    Physical Address. . . . . : 00-50-56-A1-60-6B
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IPv4 Address. . . . . : 172.16.150.100(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Saturday, April 1, 2023 8:29:46 AM
    Lease Expires . . . . . : Saturday, April 1, 2023 8:38:08 AM
    Default Gateway . . . . . : 172.16.150.2
    DHCP Server . . . . . : 172.16.150.5
    DNS Servers . . . . . : 172.16.200.11
    NetBIOS over Tcpi. . . . . : Enabled

PS C:\Users\hermione.HERMIONE>
```

💡 You will have to open annoyingly large variety of tcp and udp ports between LAN and MGMT for a domain join to work. Open those required to allow wks1 to join the domain. Research this and make sure you include this in your tech journal. You might consider learning how to use a vyos port-group for this purpose.

Updated Apr 1, 2023

Deliverable 2. Figure out how to install Wazuh agents on wks1 and mgmt02, remember MGMT does not enjoy the same internet connectivity as LAN. Provide a screenshot similar to the one below that shows these agents are registered with Wazuh. Make sure to create a new Agent Group called windows.



Conduct the following tests. For each test, identify the event within Wazuh providing a screenshot of the associated raw event.

Deliverable 3. Login to yourname@yourdomain on wks1. This should be a valid connection. You should be able find the workstation login event within the events for the wks1 agent.

Deliverable 4. Login to eviluser@yourdomain on wks1. This should fail. Find the event where data.win.eventdata.targetUserName=eviluser

Deliverable 5. RDP from wks1 to mgmt02 using your valid domain administrator credentials. Find the event that shows that connection.

Deliverable 6. Do test 3 again but use incorrect credentials. Make sure to show that this was a remote login attempt to include the source address or hostname

Deliverable 7. Provide a link to a technical journal entry that describes

- the changes required to your firewall or your dhcp server to allow wks1 to become a member of your domain.
- any issues you overcame like getting the wazuh agent installer copied over to mgmt02