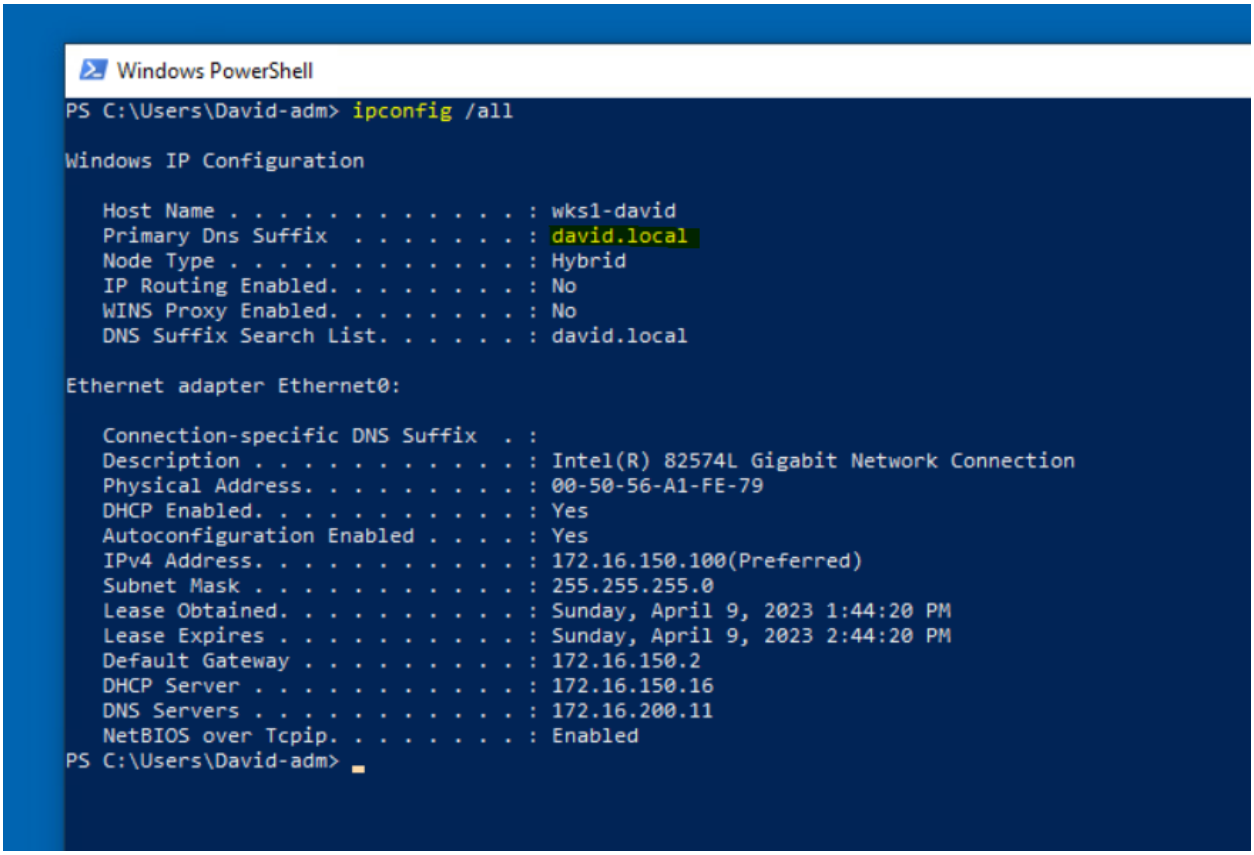
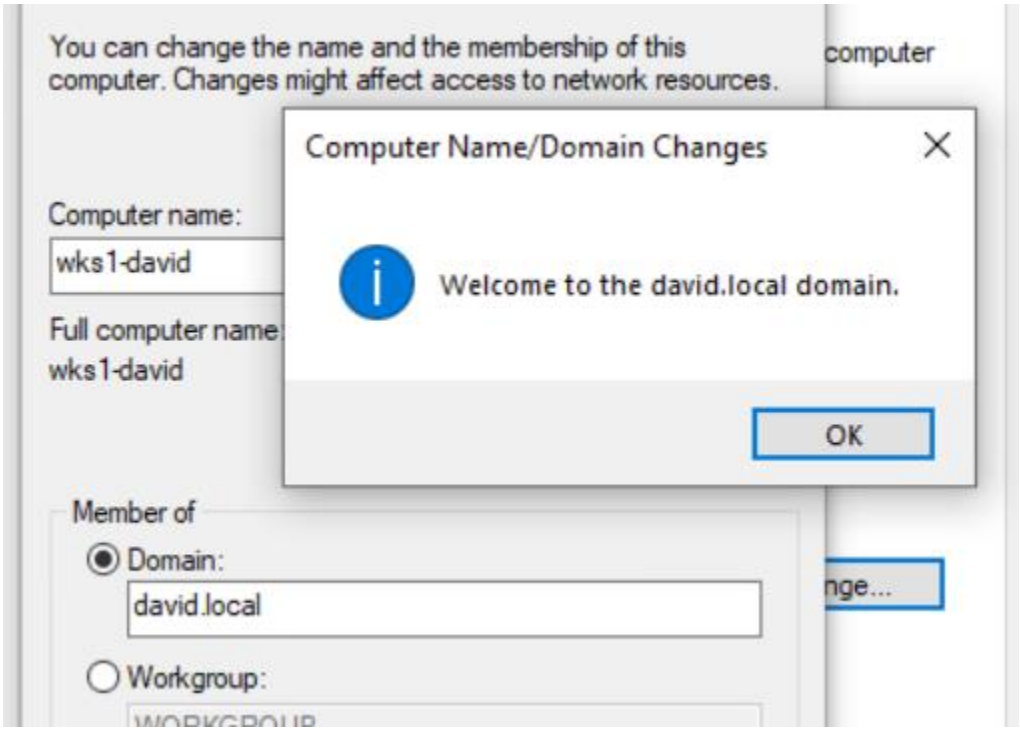
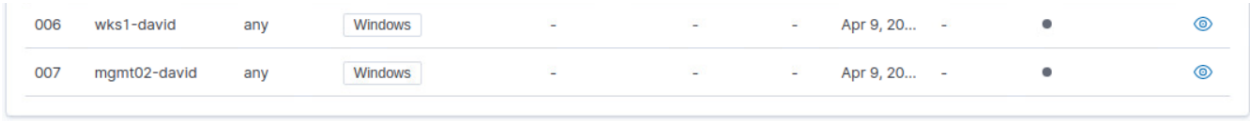
Deliverable 1. Install Active Directory Domain Services on mgmt02. Join wks1 to your new domain. Provide a screenshot showing a whoami and an ipconfig /all on wsk1 that indicates you are logged in as a domain user yourname-user@yourdomain.local

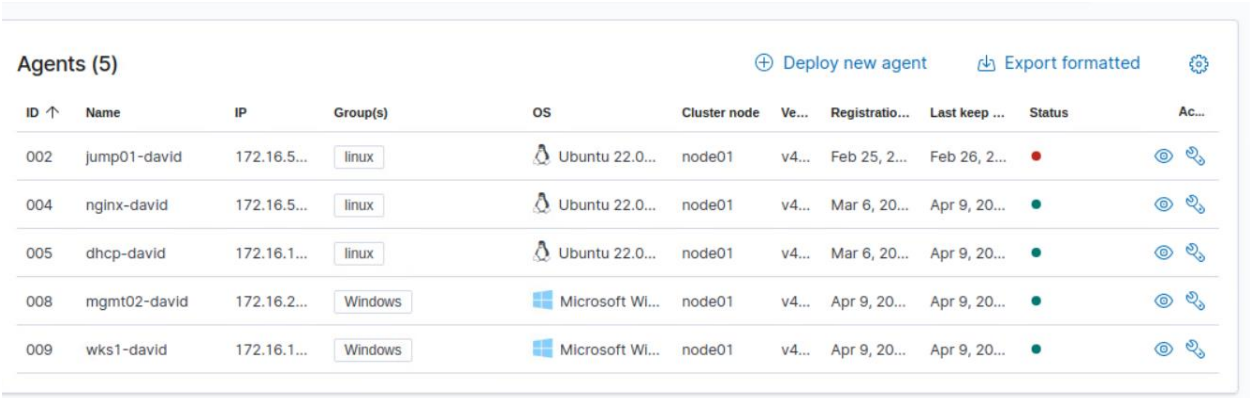




Deliverable 2. Figure out how to install Wazuh agents on wks1 and mgmt02, remember MGMT does not enjoy the same internet connectivity as LAN. Provide a screenshot similar to the one below that shows these agents are registered with Wazuh. Make sure to create a new Agent Group called windows.



006	wks1-david	any	Windows	-	-	-	Apr 9, 20...	-	●	
007	mgmt02-david	any	Windows	-	-	-	Apr 9, 20...	-	●	



Agents (5)

Deploy new agent Export formatted

ID ↑	Name	IP	Group(s)	OS	Cluster node	Ve...	Registratio...	Last keep ...	Status	Ac...
002	jump01-david	172.16.5...	linux	Ubuntu 22.0...	node01	v4...	Feb 25, 2...	Feb 26, 2...	●	
004	nginx-david	172.16.5...	linux	Ubuntu 22.0...	node01	v4...	Mar 6, 20...	Apr 9, 20...	●	
005	dhcp-david	172.16.1...	linux	Ubuntu 22.0...	node01	v4...	Mar 6, 20...	Apr 9, 20...	●	
008	mgmt02-david	172.16.2...	Windows	Microsoft Wi...	node01	v4...	Apr 9, 20...	Apr 9, 20...	●	
009	wks1-david	172.16.1...	Windows	Microsoft Wi...	node01	v4...	Apr 9, 20...	Apr 9, 20...	●	

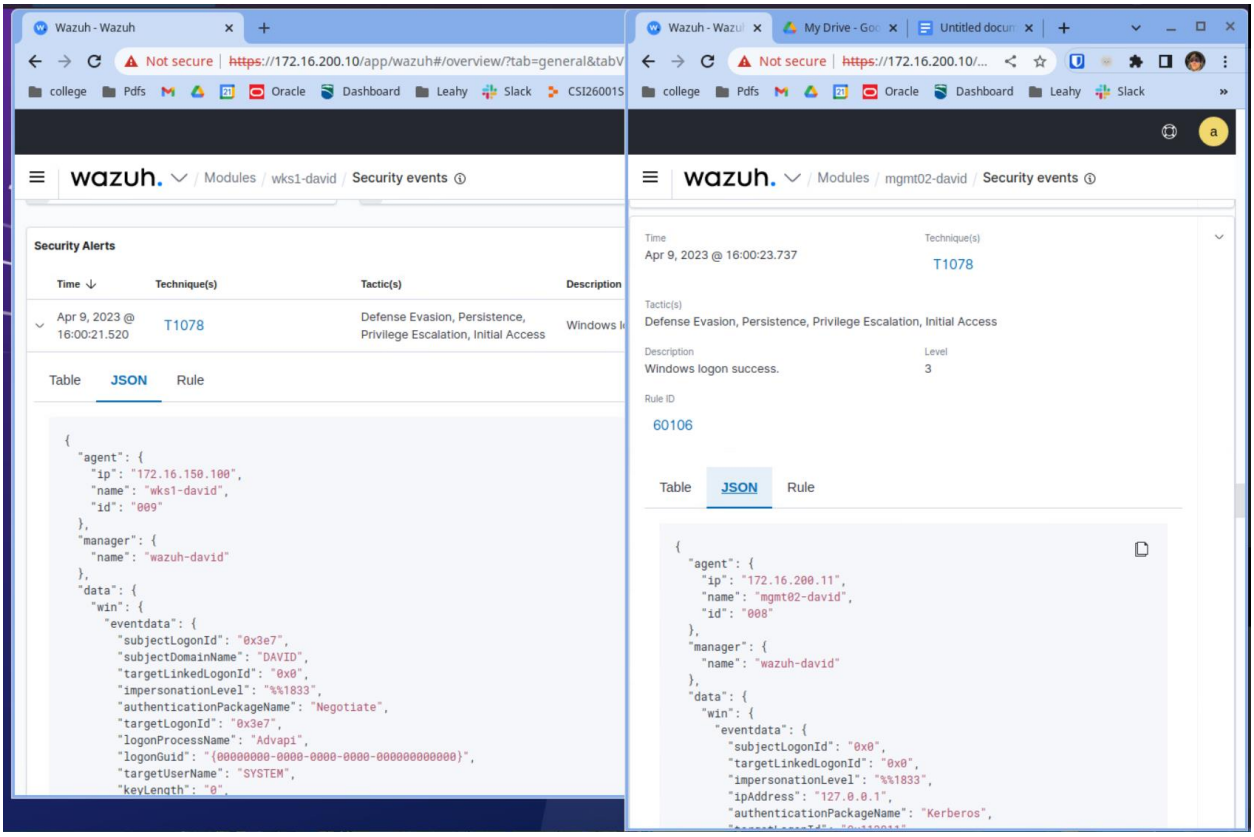
Deliverable 3. Login to yourname@yourdomain on wks1. This should be a valid connection. You should be able find the workstation login event within the events for the wks1 agent.


```
        "message": "\"An account was successfully logged on.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount
Name:\t\tWKS1-DAVID$\r\n\tAccount Domain:\t\tDAVID\r\n\tLogon ID:\t\t0x3E7\r\n\r\nLogon Information:\r\n\tLogon
Type:\t\t5\r\n\tRestricted Admin Mode:\t-\r\n\tVirtual Account:\t\tNo\r\n\tElevated Token:\t\tYes\r\n\r\nImpersonation
Level:\t\tImpersonation\r\n\r\nNew Logon:\r\n\tSecurity ID:\t\tS-1-5-18\r\n\tAccount Name:\t\tSYSTEM\r\n\tAccount Domain:\t\tNT
AUTHORITY\r\n\tLogon ID:\t\t0x3E7\r\n\tLinked Logon ID:\t\t0x0\r\n\tNetwork Account Name:\t-\r\n\tNetwork Account Domain:\t-
\r\n\tLogon GUID:\t\t{00000000-0000-0000-0000-000000000000}\r\n\r\nProcess Information:\r\n\tProcess ID:\t\t0x284\r\n\tProcess
Name:\t\tC:\\Windows\\System32\\services.exe\r\n\r\nNetwork Information:\r\n\tWorkstation Name:\t-\r\n\tSource Network Address:\t-
\r\n\tSource Port:\t\t-\r\n\r\nDetailed Authentication Information:\r\n\tLogon Process:\t\tAdvapi  \r\n\tAuthentication
Package:\tNegotiate\r\n\tTransited Services:\t-\r\n\tPackage Name (NTLM only):\t-\r\n\tKey Length:\t\t0\r\n\r\nThis event is
generated when a logon session is created. It is generated on the computer that was accessed.\r\n\r\nThe subject fields indicate the
account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process
such as Winlogon.exe or Services.exe.\r\n\r\nThe logon type field indicates the kind of logon that occurred. The most common types
are 2 (interactive) and 3 (network).\r\n\r\nThe New Logon fields indicate the account for whom the new logon was created, i.e. the
account that was logged on.\r\n\r\nThe network fields indicate where a remote logon request originated. Workstation name is not
always available and may be left blank in some cases.\r\n\r\nThe impersonation level field indicates the extent to which a process in
the logon session can impersonate.\r\n\r\nThe authentication information fields provide detailed information about this specific
logon request.\r\n\t- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.\r\n\t- Transited
services indicate which intermediate services have participated in this logon request.\r\n\t- Package name indicates which sub-
protocol was used among the NTLM protocols.\r\n\t- Key length indicates the length of the generated session key. This will be 0 if no
session key was requested.\"",
        "version": "2",
        "systemTime": "2023-04-09T19:48:34.692153800Z",
        "eventRecordID": "22069",
        "threadID": "6112",
        "computer": "wks1-david.david.local",
        "task": "12544",
        "processID": "652",
        "severityValue": "AUDIT_SUCCESS",
        "providerName": "Microsoft-Windows-Security-Auditing"
      }
```

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

data.win.eventdata.targetUserName	MicahAldenKezar(Evil)
data.win.eventdata.targetUserSid	S-1-0-0
data.win.eventdata.workstationName	WKS1-DAVID
data.win.system.channel	Security
data.win.system.computer	wks1-david.david.local
data.win.system.eventID	4625
data.win.system.eventRecordID	22095
data.win.system.keywords	0x8010000000000000
data.win.system.level	0
	"An account failed to log on. Subject: Security ID: S-1-5-18 Account Name: WKS1-DAVID$ Account Domain: DAVID Logon ID: 0x3E7 Logon Type: 2 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: MicahAldenKezar(Evil) Account Domain: DAVID Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D

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



Same log on and same time

Deliverable 6. Do test 5 again but use incorrect credentials. Make sure to show that this was a remote login attempt to include the source address or hostname

agent.name	mgmt02-david
data.win.eventdata.authenticationPackageName	NTLM
data.win.eventdata.failureReason	%%2313
data.win.eventdata.ipAddress	172.16.150.100
data.win.eventdata.ipPort	0
data.win.eventdata.keyLength	0
data.win.eventdata.logonProcessName	NtLmSsp
data.win.eventdata.logonType	3
data.win.eventdata.processId	0x0
data.win.eventdata.status	0xc000006d
data.win.eventdata.subStatus	0xc0000064
data.win.eventdata.subjectLogonId	0x0
data.win.eventdata.subjectUserSid	S-1-0-0
data.win.eventdata.targetDomainName	DAVID
data.win.eventdata.targetUserName	evilpaulgleason
data.win.eventdata.targetUserSid	S-1-0-0
data.win.eventdata.workstationName	WKS1-DAVID

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

https://github.com/dthomsen116/SEC-350/wiki/Wazuh---Windows-Logging