

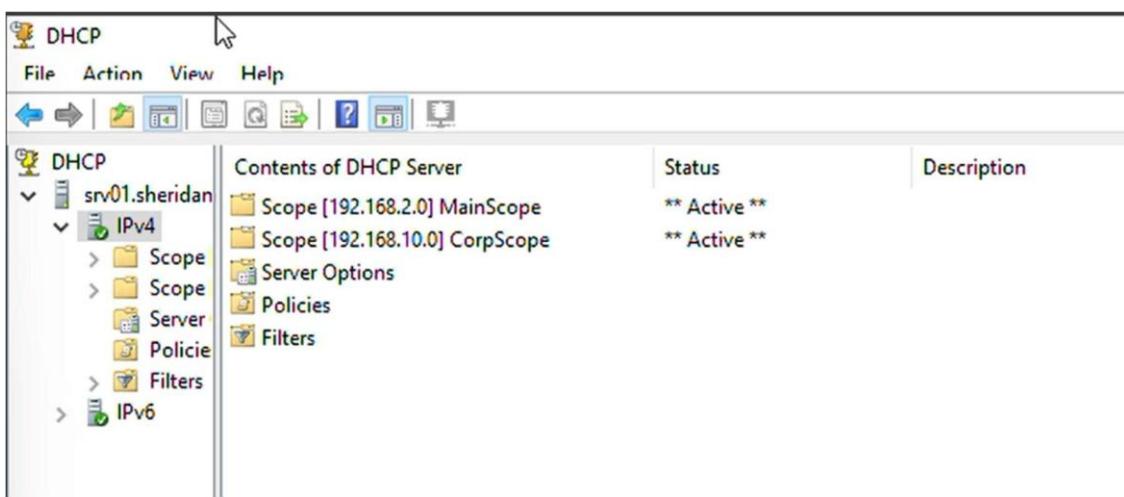
**Name:** Mahimaa Vardini Balaji Ramathaal

**Lab Number:** 4

---

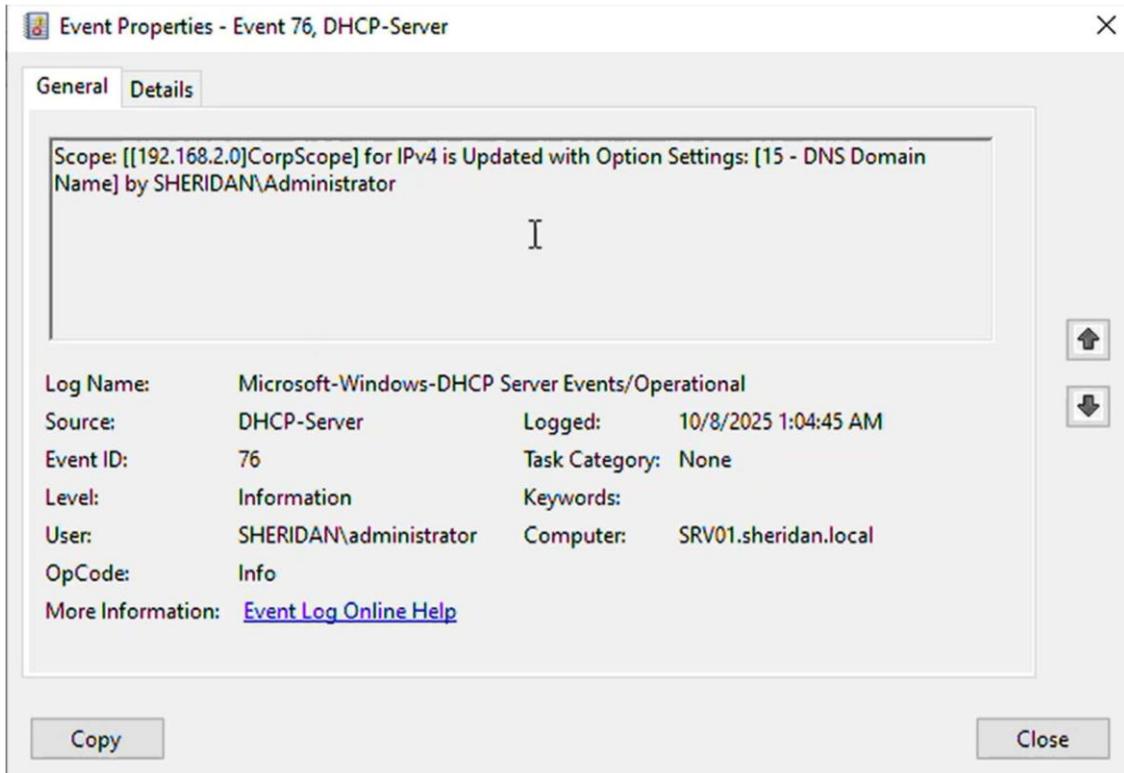
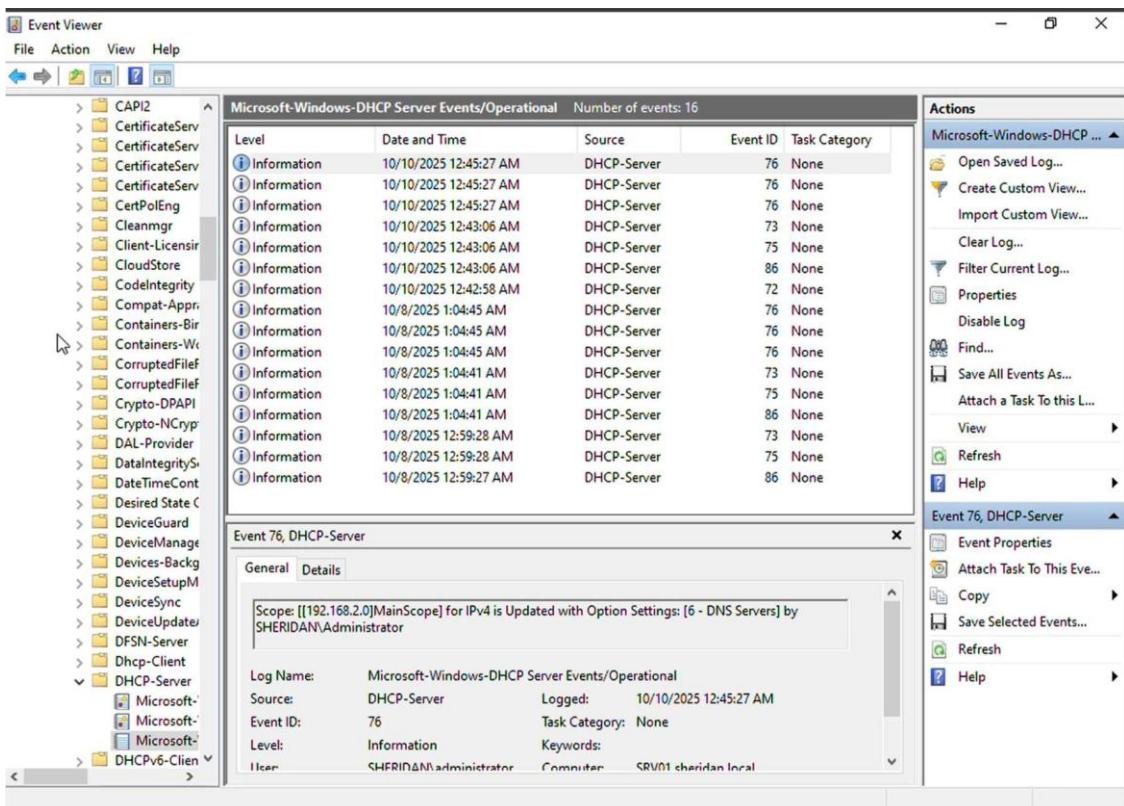
### TASK 1 – Install and Secure DHCP Server

ScopeId	SubnetMask	Name	State	StartRange	EndRange	LeaseDuration
192.168.2.0	255.255.255.0	MainScope	Active	192.168.2.50	192.168.2.150	8.00:00:00
192.168.10.0	255.255.255.0	CorpScope	Active	192.168.10.100	192.168.10.200	8.00:00:00



The screenshot shows the Windows Server 2012 DHCP Management Console. On the left, the navigation pane displays the server name 'srv01.sheridan' and the 'IPv4' tab selected. Under 'IPv4', there are icons for Scope, Scope, Server Options, Policies, and Filters. To the right, a table titled 'Contents of DHCP Server' lists two scopes: 'Scope [192.168.2.0] MainScope' and 'Scope [192.168.10.0] CorpScope', both marked as '\*\* Active \*\*'.

Start IP Address	End IP Address	Description
192.168.2.50	192.168.2.150	Address range for distribution

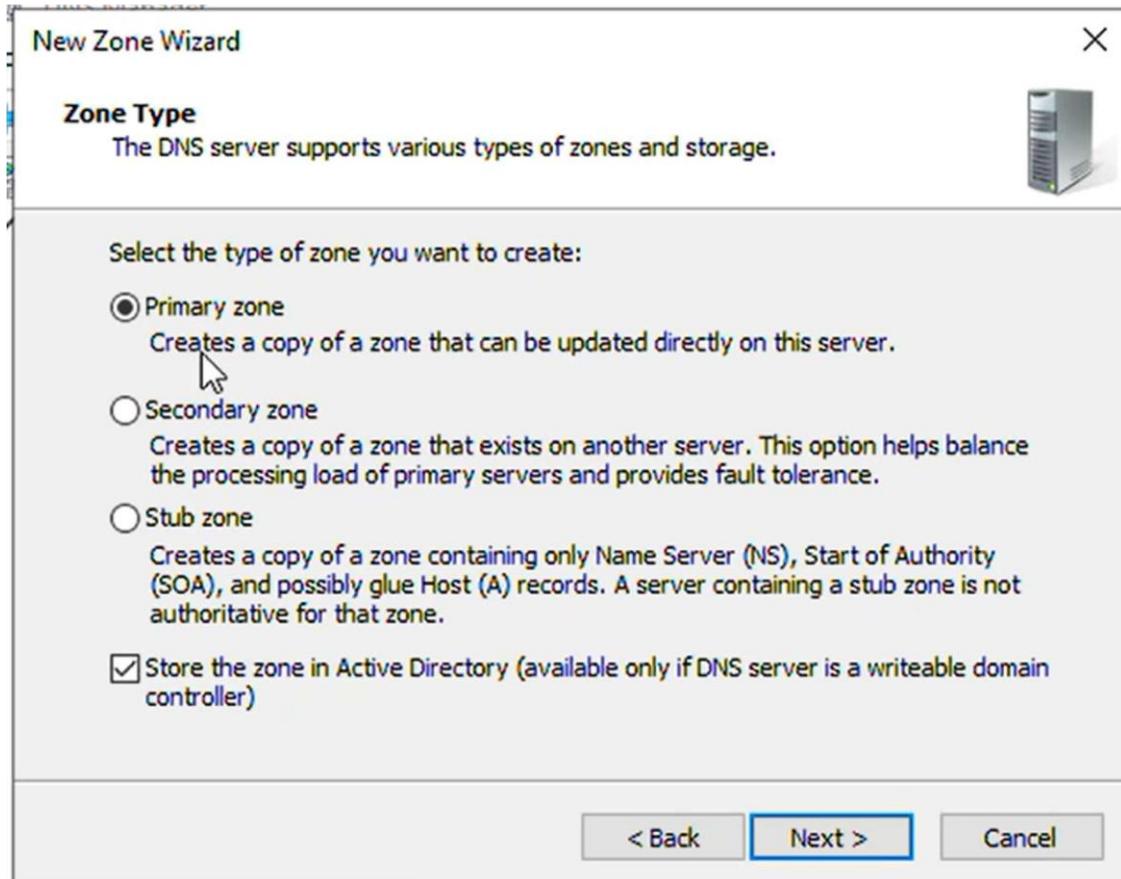


- Research Direction: What is a rogue DHCP server attack? How does AD authorization mitigate it?

A rogue DHCP server attack happens when a malicious device on a network pretends to be a legitimate DHCP server to intercept traffic. Active directory authorization helps mitigate this by not allowing unauthorized DHCP servers to operate on the network.

## TASK 2 – CREATE AND SECURE DNS ZONES

PS C:\Users\Administrator> Get-DnsServerZone					
ZoneName	ZoneType	IsAutoCreated	IsDsIntegrated	IsReverseLookupZone	IsSigned
_msdcs.sheridan.local	Primary	False	True	False	False
0.2.168.192.in-addr.arpa	Primary	False	True	True	False
0.in-addr.arpa	Primary	True	False	True	False
127.in-addr.arpa	Primary	True	False	True	False
2.168.192.in-addr.arpa	Primary	False	True	True	False
255.in-addr.arpa	Primary	True	False	True	False
sheridan.local	Primary	False	True	False	False
sheridantech.local	Primary	False	True	False	False
TrustAnchors	Primary	False	True	False	False



## New Zone Wizard



### Active Directory Zone Replication Scope

You can select how you want DNS data replicated throughout your network.



Select how you want zone data replicated:

- To all DNS servers running on domain controllers in this forest: sheridan.local
- To all DNS servers running on domain controllers in this domain: sheridan.local
- To all domain controllers in this domain (for Windows 2000 compatibility): sheridan.local
- To all domain controllers specified in the scope of this directory partition:

< Back

Next >

Cancel

### Zone Name

What is the name of the new zone?



The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

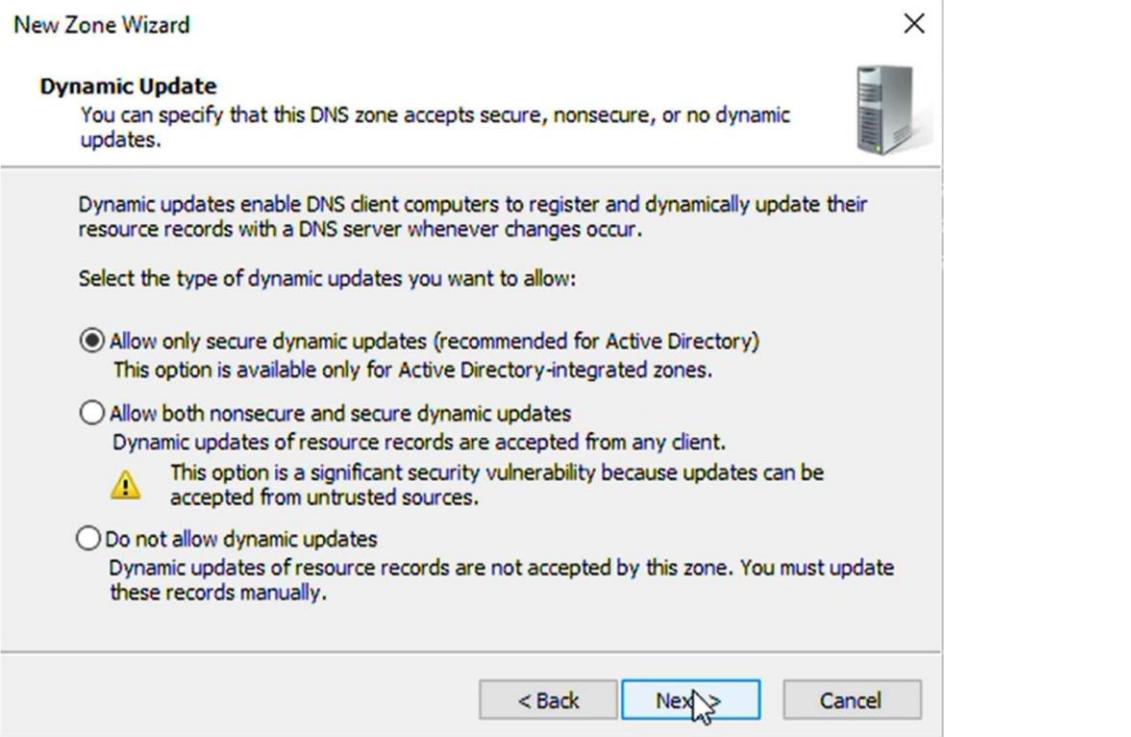
Zone name:

sheridantech.local

< Back

Next >

Cancel



```
PS C:\Users\Administrator> Get-DnsServerResourceRecord -ZoneName "sheridantech.local"
HostName      RecordType Type   Timestamp      TimeToLive    RecordData
-----      -----
@             NS          2     0              01:00:00      srv01.sheridan.local.
@             SOA         6     0              01:00:00      [3][srv01.sheridan.local.]host...
intranet      A           1     0              01:00:00      192.168.2.23
portal        CNAME       5     0              01:00:00      intranet.sheridantech.local.
```

DNS Manager

File Action View Help

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[3], srv01.sheridan.local., h...	static
(same as parent folder)	Name Server (NS)	srv01.sheridan.local.	static
intranet	Host (A)	192.168.2.23	static
portal	Alias (CNAME)	intranet.sheridantech.local.	static

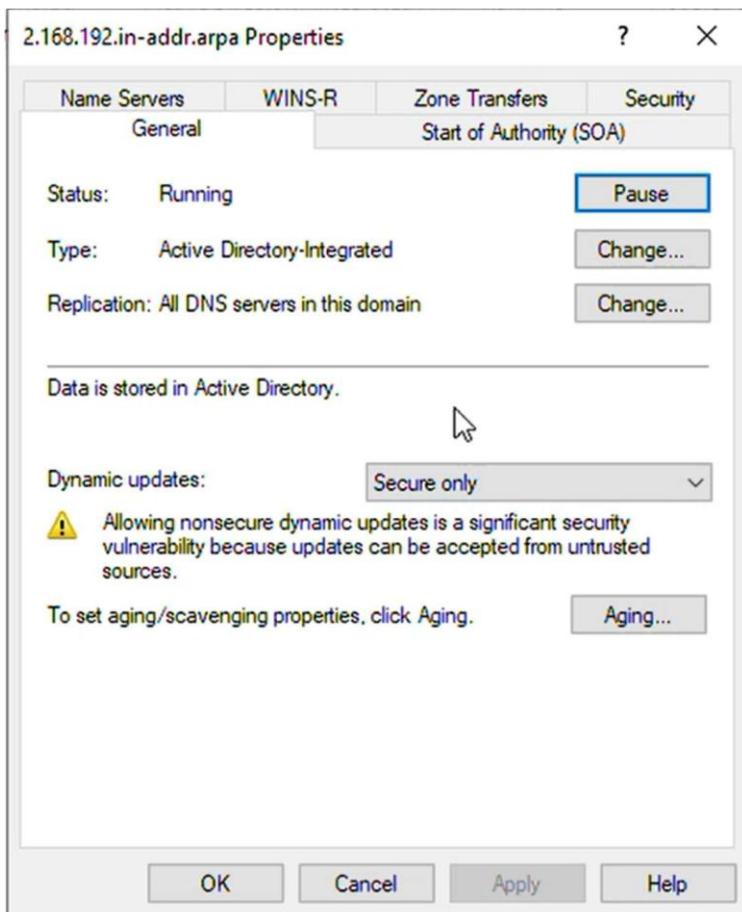
DNS

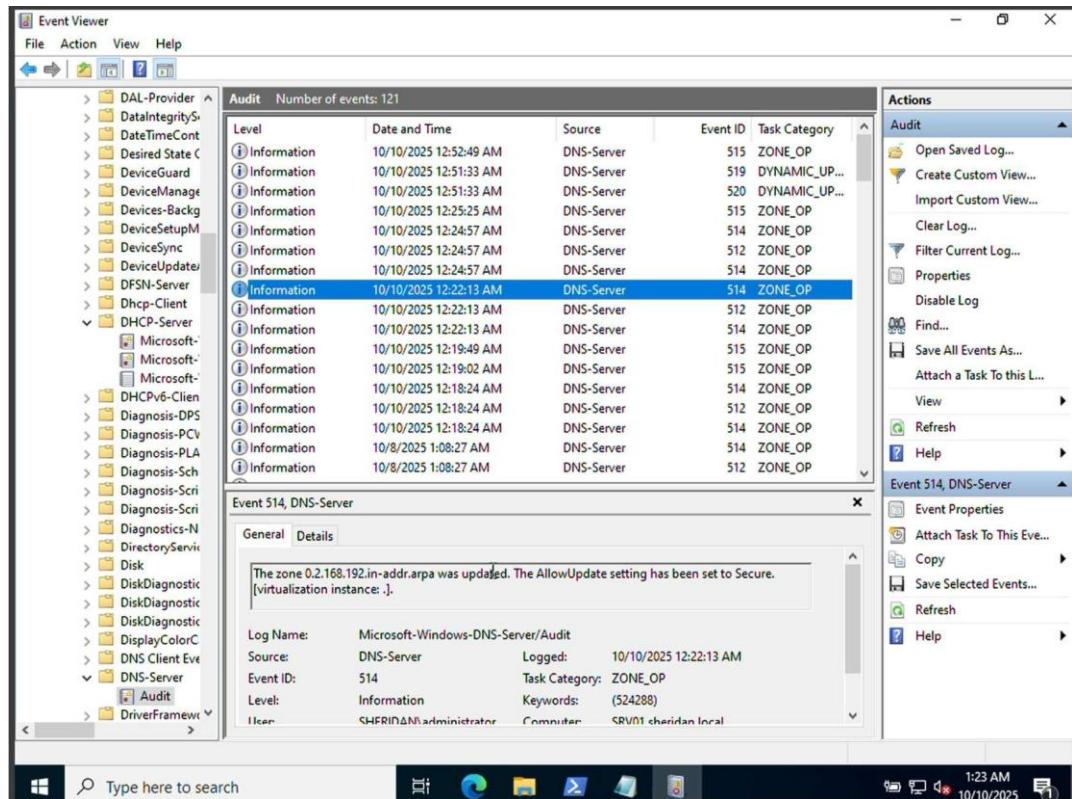
- SRV01
  - Forward Lookup Zones
    - \_msdcs.sheridan.local
    - sheridan.local
    - sheridantech.local
  - Reverse Lookup Zones
  - Trust Points
  - Conditional Forwarders

```
PS C:\Users\Administrator> Resolve-DnsName intranet.sheridantech.local
Name                           Type    TTL     Section   IPAddress
----                           ----    --      -----   -----
intranet.sheridantech.local   A       3600   Answer    192.168.2.23

PS C:\Users\Administrator> Resolve-DnsName 192.168.2.23
Name                           Type    TTL     Section   NameHost
----                           ----    --      -----   -----
23.2.168.192.in-addr.arpa.   PTR    1200   Question  SRV01.sheridan.local
```

The screenshot shows the Windows DNS Manager window. The left pane displays a tree view of DNS objects under the SRV01 node, including Forward Lookup Zones, Reverse Lookup Zones, Trust Points, and Conditional Forwarders. The 'Reverse Lookup Zones' node is selected. The right pane lists the reverse zones: '0.2.168.192.in-addr.arpa' and '2.168.192.in-addr.arpa'. The '2.168.192.in-addr.arpa' zone is currently selected.



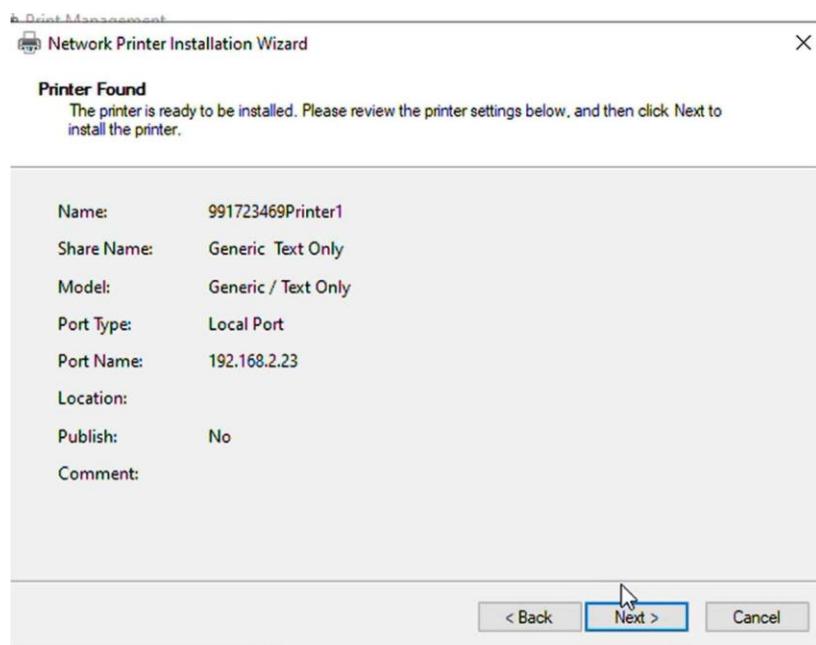


- Research Direction: What is DNS cache poisoning? How do secure updates and DNSSEC help mitigate it?

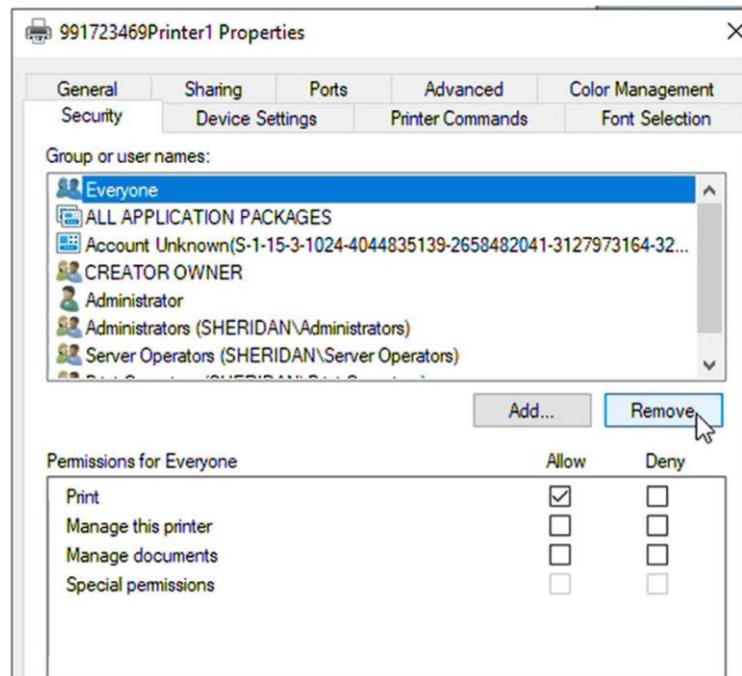
DNS cache poisoning happens when an attacker injects malicious DNS data to redirect users and manipulate browsers. Secure updates and DNSSEC help prevent such attacks as it validates the authenticity of DNS responses.

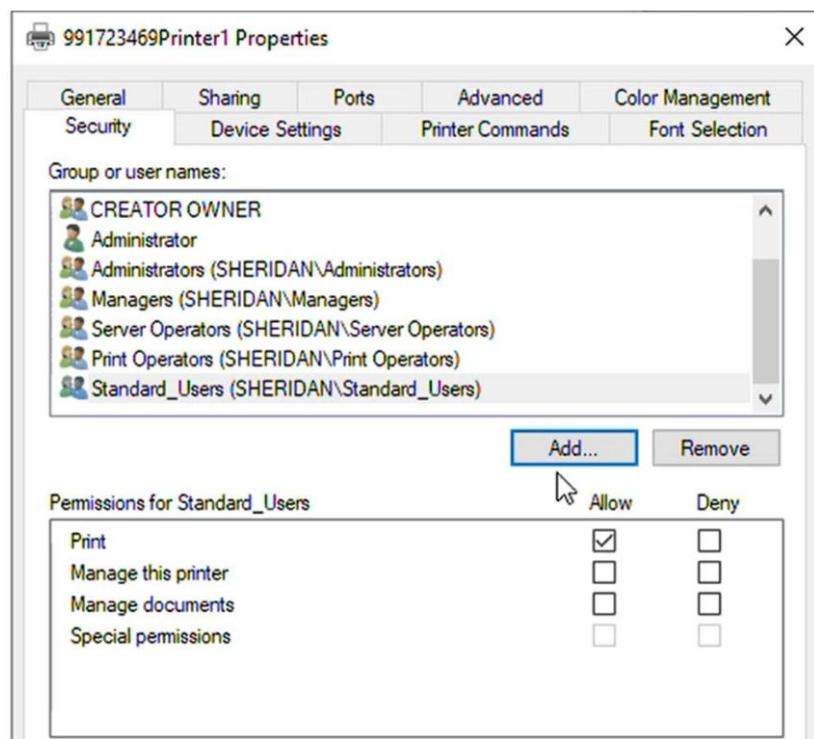
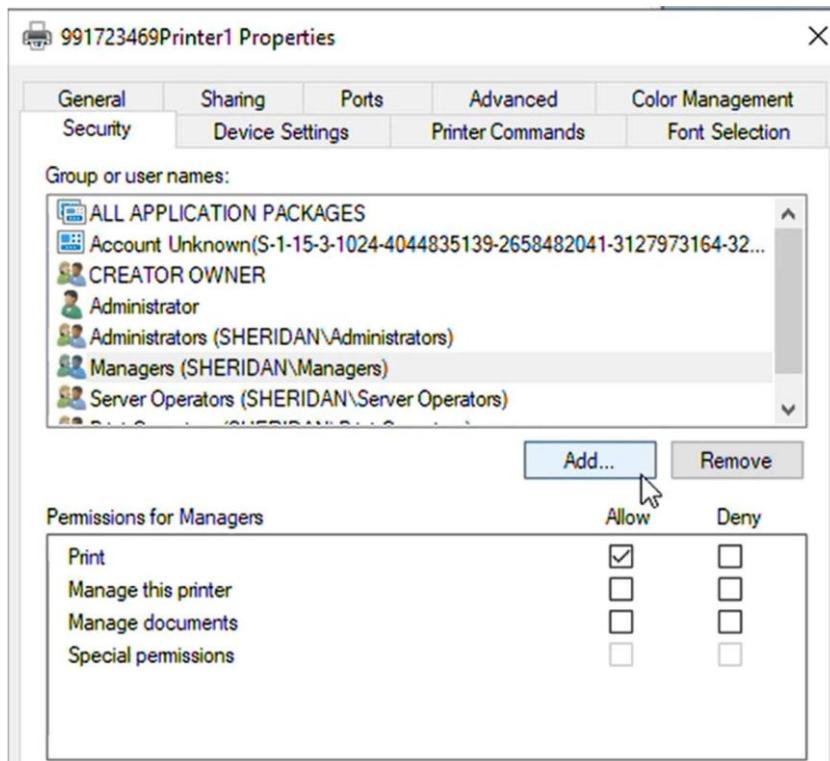
## TASK 3 – PRINT SERVER DEPLOYMENT

Creating a new printer called 991723469Printer1



Removing access from “Everyone” and only granting access to Standard Users and Managers the privilege to print





Restricting Driver Installation to prevent Print Nightmare vulnerability

```

PS C:\Users\Administrator> New-Item -Path "HKLM:\Software\Policies\Microsoft\Windows NT\Printers" -Name "PointAndPrint" -Force

Hive: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers

Name          Property
----          -----
PointAndPrint

PS C:\Users\Administrator> Set-ItemProperty "HKLM:\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint" -Name "RestrictDriverInstallationToAdministrators" -Value 1 -Type DWord
PS C:\Users\Administrator> Get-ItemProperty -Path "HKLM:\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint"

RestrictDriverInstallationToAdministrators : 1
PSPath          : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint
PSParentPath    : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers
PSChildName     : PointAndPrint
PSDrive         : HKLM
PSProvider      : Microsoft.PowerShell.Core\Registry

```

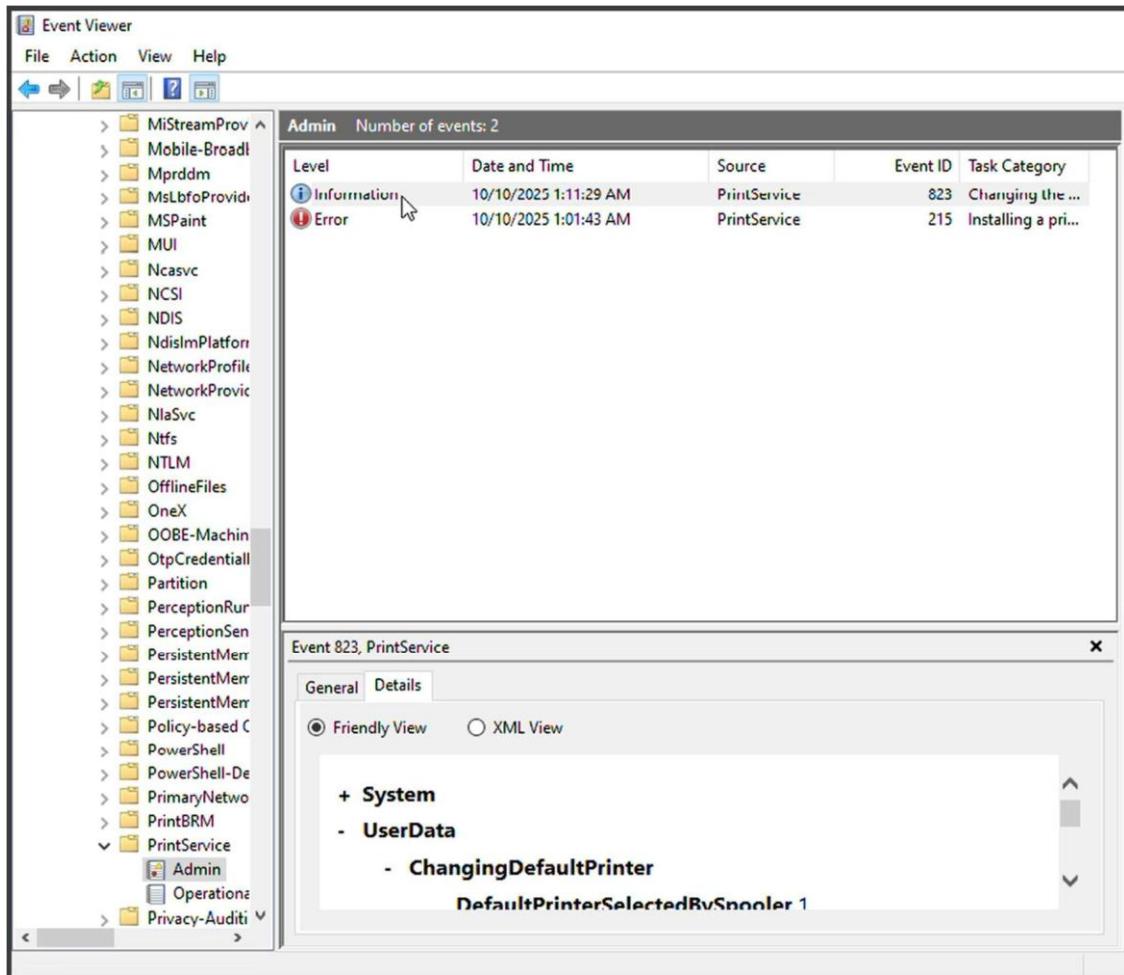
```

PS C:\Users\Administrator> Get-Printer
Name          ComputerName   Type        DriverName           PortName       Shared  Published  DeviceType
----          -----          ----        -----              -----          -----  -----  -----
991723469Printer1  Local          Generic / Text Only  192.168.2.23  True    False    False    Pr
Microsoft Print to PDF  Local          Microsoft Print To PDF  PORTPROMPT:  False   False    False    Pr
Microsoft XPS Document Writer  Local          Microsoft XPS Document...  PORTPROMPT:  False   False    False    Pr

```

Print Management

Printer Name	Queue Status	Jobs In ...	Server Name	Driver Name	Actions
Microsoft XPS Document Writer	Ready	0	SRV01 (local)	Microsoft XPS Document Writer	Printers
Microsoft Print to PDF	Ready	0	SRV01 (local)	Microsoft Print To PDF	More Actions
991723469Printer1	Ready	0	SRV01 (local)	Generic / Text Only	



- Research Direction: What was the Print Nightmare vulnerability, and why must Print Spooler be hardened?

The PrintNightmare vulnerability allowed attackers to run code remotely using Print Spooler, so by hardening it using restrictions to driver installation makes it so that new driver installation is restricted unless under administrator supervision.

### Reflection

Which of the three services poses the biggest security risk and why?

Based on my research and observation from doing this lab, I think Print Spooler probably poses the biggest security risk as it runs with high privileges easily. Since the spooler interacts with user drivers and network shares, it is very easy to unintentionally misconfigure it and allow attackers to execute malicious code remotely and gain elevated privileges on the system. But we can restrict this by performing restrictions to driver installations to administrators,

disabling remote printing when not necessary and overall reducing the attack vector.

---