Implement Secure Network Addressing Services

(CompTIA Security + SY – 601)

Objectives:

- To analyze potential indicators associated with network attacks
- To implement secure protocols

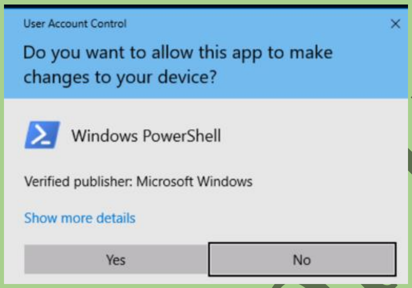
Resources:

- Kali Virtual Machine (PT1-Kali)
- Windows Virtual Machine (DC1 & MS1)
- DHCP
- Nmap

Instructions:

Time Management

- Sign-in to **MS1**VM
- Select Start menu, right-click **Windows Powershell** and select **Run as Administrator**. When prompted select **Yes** in the UAC dialog box



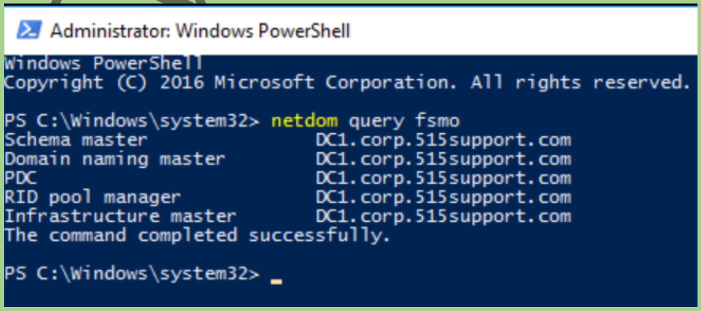
User Account Control

Do you want to allow this app to make changes to your device?

Windows PowerShell

Verified publisher: Microsoft Windows

- One Domain Controller (directory service server) per Active Directory domain holds role of PDC Emulator. One aspect of this role is time management. Run the following command to display which server is the role holder: **netdom query fsmo**

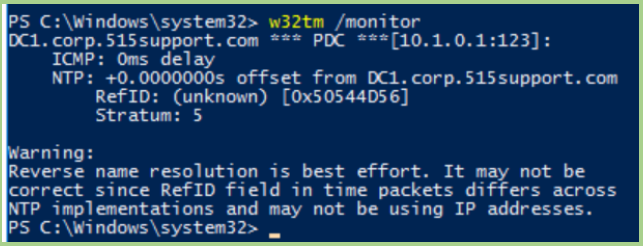


```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> netdom query fsmo
Schema master               DC1.corp.515support.com
Domain naming master        DC1.corp.515support.com
PDC                         DC1.corp.515support.com
RID pool manager            DC1.corp.515support.com
Infrastructure master       DC1.corp.515support.com
The command completed successfully.

PS C:\Windows\system32> _
```

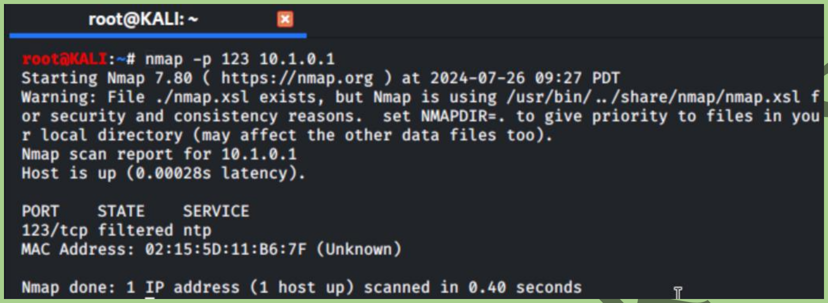
- Display the time server used by MS1 to receive the accurate domain time (this command takes several seconds to execute): **w32tm /monitor**



```
PS C:\Windows\system32> w32tm /monitor
DC1.corp.515support.com *** PDC ***[10.1.0.1:123]:
    ICMP: 0ms delay
    NTP: +0.0000000s offset from DC1.corp.515support.com
        RefID: (unknown) [0x50544D56]
        Stratum: 5

Warning:
Reverse name resolution is best effort. It may not be
correct since RefID field in time packets differs across
NTP implementations and may not be using IP addresses.
PS C:\Windows\system32> _
```

- Close the **Windows Powershell** console
- Switch to **PT1-Kali** VM and sign-in
- Open a Terminal and then run the following command to scan the 10.1.0.1 server for the default NTP port number: **nmap -p 123 10.1.0.1**



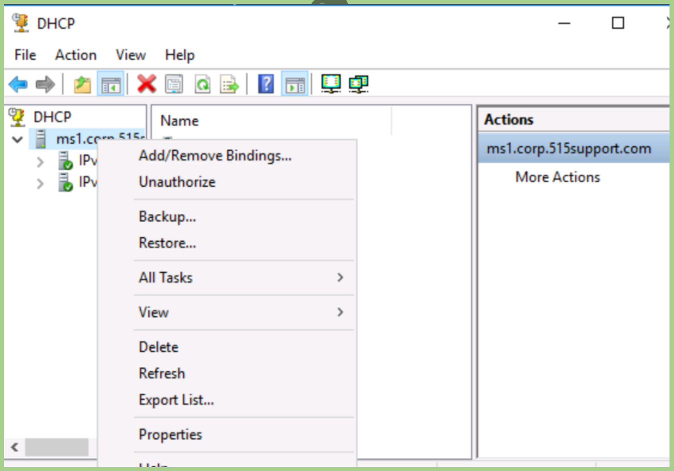
```
root@KALI:~# nmap -p 123 10.1.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2024-07-26 09:27 PDT
Warning: File ./nmap.xsl exists, but Nmap is using /usr/bin/../share/nmap/nmap.xsl f
or security and consistency reasons.  set NMAPDIR=. to give priority to files in you
r local directory (may affect the other data files too).
Nmap scan report for 10.1.0.1
Host is up (0.00028s latency).

PORT    STATE    SERVICE
123/tcp filtered ntp
MAC Address: 02:15:5D:11:B6:7F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

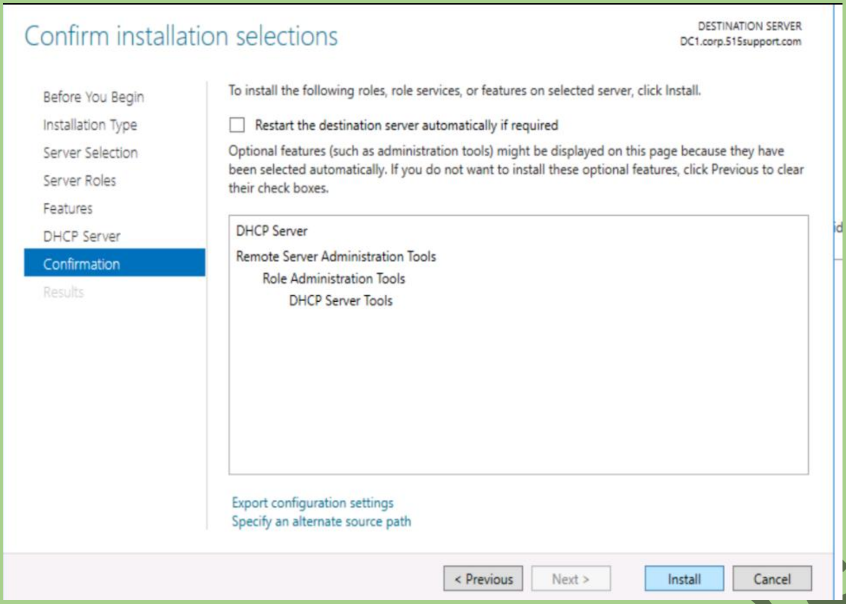
DHCP Configuration

- Select the **MS1** VM, if necessary, sign-in back
- From Server Manager, select **Tools > DHCP** menu
- Select the **MS1.corp.515support.com** node, and then right-click it to observe the context menu



- Switch to **DC1** and sign-in
- From Server Manager, select **Add roles and features**

- Complete the wizard to add the DHCP Server role, using the defaults



To install the following roles, role services, or features on selected server, click Install.

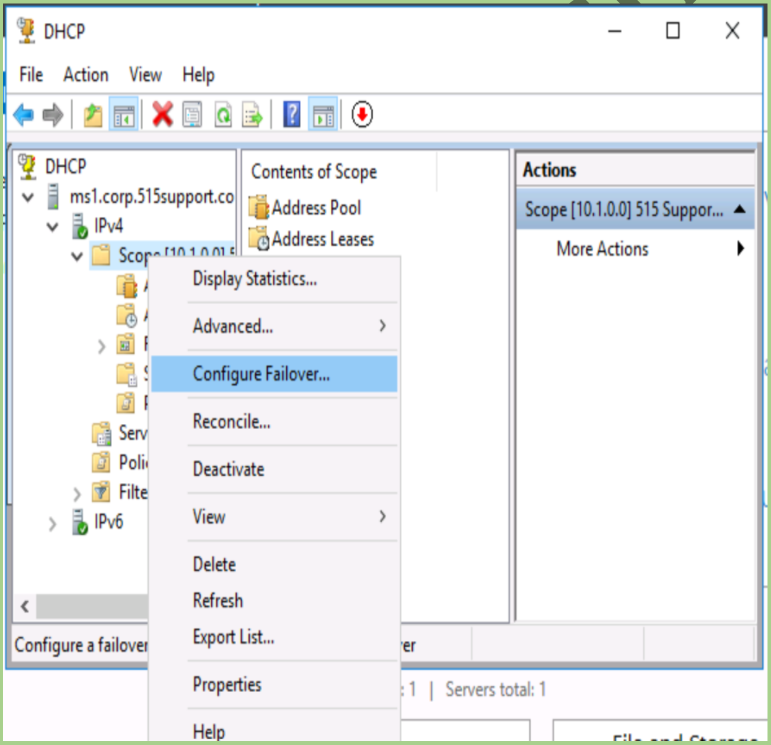
□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

DHCP Server
Remote Server Administration Tools
    Role Administration Tools
        DHCP Server Tools

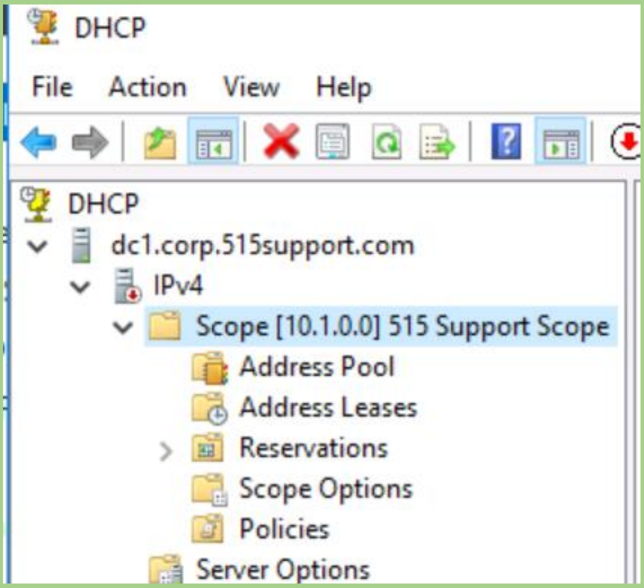
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

- Wait for the installation of DHCP to complete about one minute, select **Close**
- Switch back to the **MS1** VM
- In the DHCP console, expand the **IPv4** node and select the **10.1.0.0** scope
- Right-click the 10.1.0.0 scope and then select **Configure Failover**

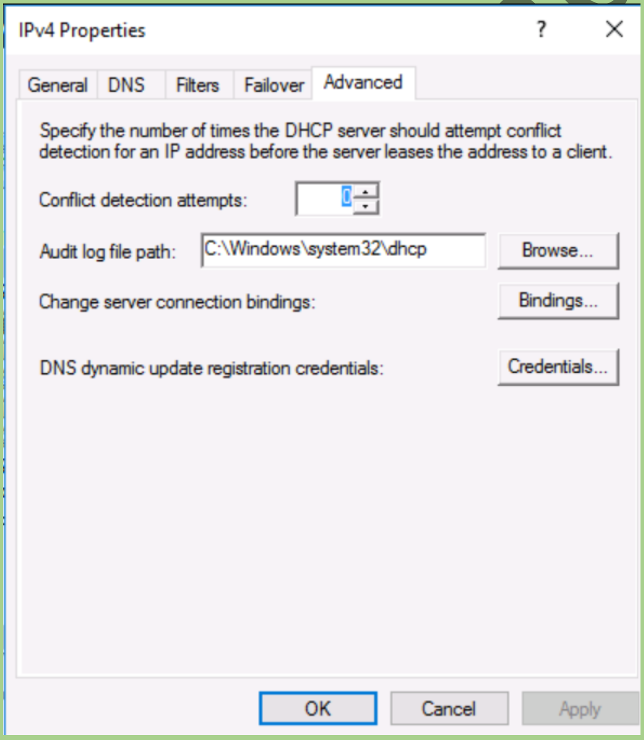


- Configure the DHCP Failover:
- Switch back to DC1

- From the Server Manager, select **Tools > DHCP**. Select the **DC1.corp.515support.com** node, and then right-click it and select Authorize to register the DHCP service with Active Directory
- Expand the node in the DHCP console to display the 10.1.0.0 scope



- Close the DHCP console
- Switch to MS1, right-click the IPv4 node, and then select **Properties**. Use the Advanced tab to display the **default location of DHCP log files**



Specify the number of times the DHCP server should attempt conflict detection for an IP address before the server leases the address to a client.

Conflict detection attempts: 0

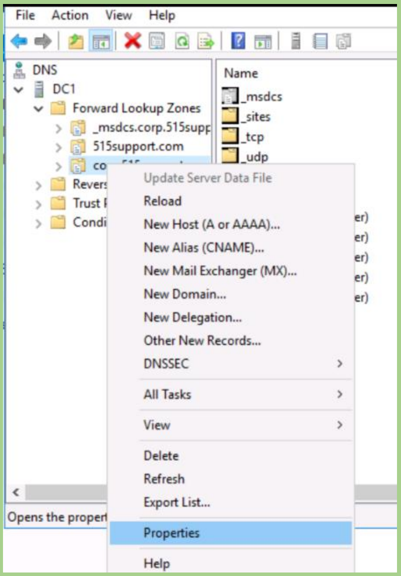
Audit log file path: C:\Windows\system32\dhcp

Change server connection bindings:

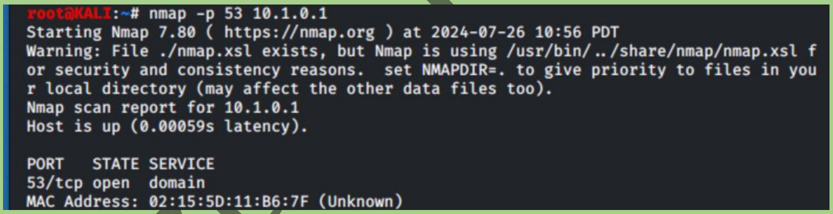
DNS dynamic update registration credentials:

DNS

- Switch to **DC1**, if necessary, sign-in
- From the Server Manager select **Tools > DNS**
- Expand **DC1-Forward Lookup Zones** and select **corp.515support.com**. Right-click it and select **Properties**



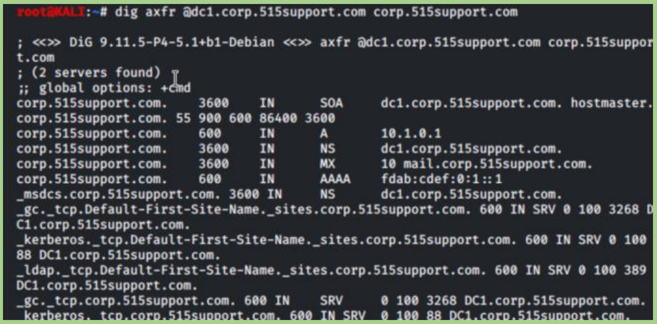
- Select the **Zones Transfer** tab
- Leave the properties dialog box open
- Switch back to the PT1-Kali VM, and if necessary, sign-in
- In a terminal window, run an Nmap port scan for port 53 against the DC1 server for port 53 against the DC1 server (10.0.1.0):



```
root@KALI:~# nmap -p 53 10.1.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2024-07-26 10:56 PDT
Warning: File ./nmap.xsl exists, but Nmap is using /usr/bin/../share/nmap/nmap.xsl f
or security and consistency reasons.  set NMAPDIR=. to give priority to files in you
r local directory (may affect the other data files too).
Nmap scan report for 10.1.0.1
Host is up (0.00059s latency).

PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 02:15:5D:11:B6:7F (Unknown)
```

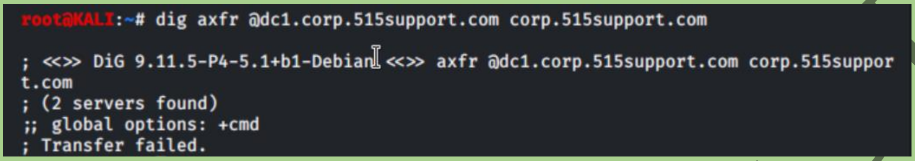
- Run the following command to request a zone transfer from the DC1 DNS server to the PT1-Kali VM penetration testing workstation: **dig axfr @dc1.corp.515support.com corp.515support.com**



```
root@KALI:~# dig axfr @dc1.corp.515support.com corp.515support.com

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> axfr @dc1.corp.515support.com corp.515suppor
t.com
; (2 servers found)
;; global options: +cmd
corp.515support.com.    3600    IN      SOA     dc1.corp.515support.com. hostmaster.
corp.515support.com. 55 900 600 86400 3600
corp.515support.com.    600     IN      A       10.1.0.1
corp.515support.com.    3600    IN      NS      dc1.corp.515support.com.
corp.515support.com.    3600    IN      MX      10 mail.corp.515support.com.
corp.515support.com.    600     IN      AAAA    fdab:cdef:0:1::1
_msdcs.corp.515support.com. 3600 IN     NS      dc1.corp.515support.com.
_gc._tcp.Default-First-Site-Name._sites.corp.515support.com. 600 IN SRV 0 100 3268 D
C1.corp.515support.com.
_kerberos._tcp.Default-First-Site-Name._sites.corp.515support.com. 600 IN SRV 0 100
88 DC1.corp.515support.com.
_ldap._tcp.Default-First-Site-Name._sites.corp.515support.com. 600 IN SRV 0 100 389
DC1.corp.515support.com.
_gc._tcp.corp.515support.com. 600 IN    SRV     0 100 3268 DC1.corp.515support.com.
_kerberos._tcp.corp.515support.com. 600 IN SRV  0 100 88 DC1.corp.515support.com.
```

- Switch back to the DC1 VM, if necessary, sign-in
- In the DNS console, adjust the server properties to clear the check box for **Allow zone transfers** to prevent any zone transfers. Select **Apply**
- Switch back to the **PT1-Kali VM** and run the original dig command



```
root@KALI:~# dig axfr @dc1.corp.515support.com corp.515support.com

; <<>> DiG 9.11.5-P4-5.1+b1-Debian <<>> axfr @dc1.corp.515support.com corp.515suppor
t.com
; (2 servers found)
;; global options: +cmd
; Transfer failed.
```

- Close the DNS console

Observations:

- **Time Management**: Verification of the time server used by the MS1 server was performed successfully using w32tm /monitor.
- **NTP Scan**: The NTP port (123) on the 10.1.0.1 server was scanned using Nmap.
- **DHCP Configuration**: DHCP Server role was successfully added to DC1, and failover was configured for redundancy.
- **DNS Configuration**: The DNS zone transfer capability was tested and then disabled to prevent unauthorized transfers.

Results:

- **Time Synchronization**: The time server for MS1 was accurately identified and confirmed.
- **NTP Vulnerability Assessment**: Nmap scan of port 123 on 10.1.0.1 server indicated the NTP service status.
- **DHCP Redundancy**: DHCP failover was configured, ensuring network address allocation remains available in case of primary server failure.
- **DNS Security**: Successfully executed a zone transfer from the DC1 DNS server to the Kali VM. The vulnerability was mitigated by disabling zone transfers.

Conclusion:

The lab successfully demonstrated the implementation of secure network addressing services, including time management, DHCP redundancy, and DNS security. By configuring failover for DHCP and securing DNS zone transfers, the integrity and availability of network services were enhanced.

Future Work:

- **Automate Monitoring**: Implement automated monitoring for time synchronization and DHCP services to detect and resolve issues proactively.
- **Advanced DNS Security**: Explore further DNS security measures, such as DNSSEC, to enhance the integrity of DNS data.
- **Regular Vulnerability Assessments**: Conduct regular scans and assessments of network services to identify and mitigate potential vulnerabilities.