# Sophos Support

## TSE Fundamentals

**SUPPORT LAB WORKBOOK**

Version 0.1 • January 2021

SOPHOS

# Contents

Introduction ....4
Prerequisites ....4
Workbook conventions ....4
Lab environment ....4
Environment overview ....5
User accounts ....7
Network diagram ....8
Lab 1: Windows Endpoint ....9
Objectives ....9
Task 1.1: MSI logging ....9
Task 1.2: Registry Editor ....10
Task 1.3: Task Scheduler ....11
Review ....11
Lab 2: Windows Server ....12
Objectives ....12
Task 2.1: Group Policies ....12
Review ....13
Lab 3: Active Directory ....14
Objectives ....14
Task 3.1: OU, Group and User Configuration ....14
Task 3.2: User and Group Attribute Troubleshooting ....14
Review ....15
Lab 4: PowerShell ....16
Objectives ....16
Task 4.1: Basic Troubleshooting using PowerShell ....16
Task 4.2: Troubleshoot PowerShell Script not executing ....17
Review ....17
Lab 5: Tools ....18
Objectives ....18
Task 5.1: Debug Process Monitor Tool ....18
Task 5.2: Debug Process Explorer Tool ....18
Task 5.3: Wireshark Debugging ....19
Review ....19
Lab 6: Networking ....20
Objectives ....20
Task 6.1: Display and understand routing table ....20
Task 6.2: Configure a DHCP server ....21
Task 6.3: Lookup and resolve various types of DNS records using nslookup ....22
Review ....23
Lab 7: Linux ....24
Objectives ....24

Task 7.1: Create, copy and rename a file before managing permissions ....24
Task 7.2: Make edits and searches using vi ....25
Task 7.3: Search using various grep commands through system files ....25
Review ....26
Lab 8: Cryptography ....27
Objectives ....27
Task 8.1: Analyze and locate the CA of a website ....27
Task 8.2: Generate a CSR using OpenSSL to prepare a certificate ....28
Review ....29

© 2021 Sophos Limited. All rights reserved. No part of this document may be used or reproduced in any form or by any means without the prior written consent of Sophos.
Sophos and the Sophos logo are registered trademarks of Sophos Limited. Other names, logos and marks mentioned in this document may be the trademarks or registered trademarks of Sophos Limited or their respective owners.
While reasonable care has been taken in the preparation of this document, Sophos makes no warranties, conditions, or representations (whether express or implied) as to its completeness or accuracy. This document is subject to change at any time without notice.
Sophos Limited is a company registered in England number 2096520, whose registered office is at The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP.

# Introduction

These labs accompany the Sophos TSE Fundamentals Course. They are estimated to take 10 hours to complete.

You should complete each section of labs when directed to do so in the training content. Throughout the labs there are prompts for information to be written down; you will require this information for the Lab review.

If you need help or support at any point while completing the labs, please contact us at TECHSUPTraining@sophos.com and one of the team will be able to assist you.

Your Environment is hosted in CloudLabs and can be accessed through an Emulated RDP session in your Web browser.

Use you Sophos Email address to register for the Lab and keep the confirmation Email to have faster access to your lab throughout the course.

A native RDP connection is also available, but might require additional configuration, talk to your instructor should native RDP not work.

Wait for all VM in the Hyper-V- Environment to complete startup before accessing your environment using the 'Lab Access' RDP Manager preconfigured on the Desktop of your virtual host.

## Prerequisites

Prior to taking this training, you should have:

- General networking knowledge
- Understanding of operating systems
- Understanding of Active Directory

## Workbook conventions

This workbook uses the following conventions throughout:

- At the start of each lab is the learning objective, along with any requirements that must have been completed prior to starting the lab.
- Labs which cover larger subjects are divided into several tasks. Each task has a short description followed by the steps that are required to complete the task.
- Short labs are presented as a single task.
- Throughout the guide the following styles are used:

| | |
|---|---|
| **Bold text** | • Actions: On-screen elements that you interact with e.g., menu items, buttons, tick boxes, tabs, etc.<br>• Important points to note |
| 'Single quotes' | On-screen elements that you do not interact with e.g., page titles, field names, etc.… |
| `Courier New font` | Commands to be executed |
| Underlined | Hyperlinks |
| <variables> | Variables will be shown between chevrons e.g., <Red ID> |

## Lab environment

These labs are designed to be completed on the hosted Environment. Lab access will be provided by your instructor.

Note: Since we are emulating common issues make sure to use the same password when working through labs. This will make it easier for your instructor in the event you require assistance during the lab. When creating a password, always use '**Sophos@1985**'. For backups, a more complex password is required, in that case, please use '**Sophos@1985Sophos@1985**'.

# Environment overview

The environment used to complete these labs is comprised of multiple computers, connected via a simple network.

| Computer | Description |
|---|---|
| **SOPHOS.LOCAL** | This is the main network you will be using during the labs.<br>Networks: 172.16.16.0/24, 192.168.16.0/24, 172,25,25,0/24 |
| **LON-GW1.SOPHOS.LOCAL** | This is a Sophos XG Firewall, and is the default gateway for the sophos.local network that has separate interfaces for multiple internal networks and WAN links.<br>IP addresses: 172.16.16.16, 10.1.1.100, 172.25.25.16, 172.30.30.16, 10.3.3.100, 10.100.100.65, 10.4.4.16<br>Throughout this workbook this will be referred to as London Gateway 1 |
| **LON-GW2.SOPHOS.LOCAL** | This is a Sophos XG Firewall, and is a gateway for the sophos.local network that has separate interfaces for multiple internal networks and WAN links.<br>IP addresses: 172.16.16.15, 10.1.1.115, 172.25.25.15, 172.30.30.15, 10.3.3.115, 10.100.100.66, 10.4.4.15<br>Throughout this workbook this will be referred to as London Gateway 2 |
| **LON-DC.SOPHOS.LOCAL** | This Windows 2016 Server is the domain controller for the sophos.local domain.<br>It runs an SMTP server, webmail, DNS, Active Directory and a certificate authority. IP<br>address: 172.16.16.10<br>Throughout this workbook this will be referred to as London DC |
| **LON-SRV2.SOPHOS.LOCAL** | This Windows 2016 Server is being used as a client for these labs. IP<br>address: 172.16.16.20<br>Throughout this workbook this will be referred to as London Server 2 |
| **INTRANET.SOPHOS.LOCAL** | This is a Debian Linux server running a simple website. The server is located on a separate subnet.<br>IP address: 172.25.25.40, 172.25.25.41<br>Throughout this workbook this will be referred to as London Intranet |
| **SOPHOS.DMZ** | This is the DMZ for the lab network. Network:<br>172.30.30.0/24 |
| **STORE.SOPHOS.DMZ** | This is a Debian Linux server running a simple website. IP<br>addresses: 172.30.30.50<br>Throughout this workbook this will be referred to as DMZ Website |
| **NY-GW.SOPHOS.LOCAL** | This is a Sophos XG Firewall, and is the default gateway for the sophos.local network. IP<br>addresses: 192.168.16.16, 172.25.25.17, 10.2.2.200<br>Throughout this workbook this will be referred to as New York Gateway |

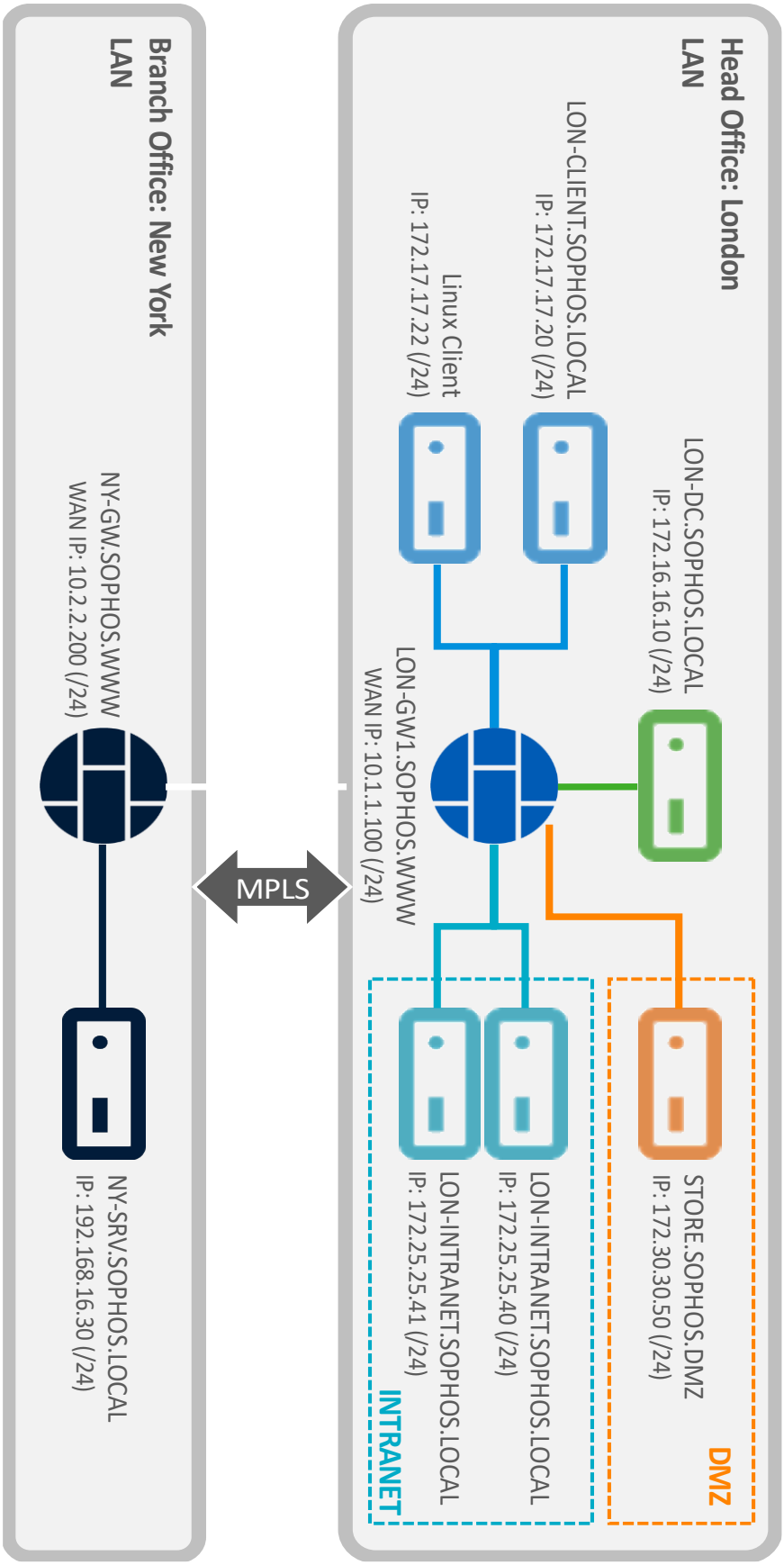
| | |
|---|---|
| **WAREHOUSE.LOCAL** | This is the network for the warehouse in New York. Network:<br>172.25.25.0/24 |
| **WAREHOUSE.SOPHOS.LOCAL** | This is a Debian Linux server running a simple website. The server is located on a separate subnet.<br>IP address: 172.25.25.60<br>Throughout this workbook this will be referred to as New York Warehouse |
| **INTERNET.WWW** | This is a Debian Linux server which provides central DNS for the sophos.local and sophos.local networks, as well as running a DHCP server, simple website, and certificate authority.<br>IP address: 10.1.1.250, 10.2.2.250,10.3.3.250<br>Throughout this workbook this will be referred to as Internet |
| **MPLS** | Network: 10.100.100.65/29 |

# User accounts

The table below details the user accounts in the lab environment.

| Username | Full name | Password | Scope and privileges |
|---|---|---|---|
| **LAB\administrator** | Administrator | Sophos1985 | SOPHOS.LOCAL<br>Domain administrator |
| **LAB\jsmith** | John Smith | Sophos1985 | SOPHOS.LOCAL<br>Domain User |
| **LAB\rbrown** | Rob Brown | Sophos1985 | SOPHOS.LOCAL<br>Domain User |
| **LAB\spage** | Sally Page | Sophos1985 | SOPHOS.LOCAL<br>Domain User |
| **LAB\lfox** | Lucy Fox | Sophos1985 | SOPHOS.LOCAL<br>Domain User |
| **LAB\frogers** | Fred Rogers | Sophos1985 | SOPHOS.LOCAL<br>Domain User |
| **root** | Root | Sophos1985 | DMZ Website<br>London Intranet<br>New York Warehouse<br>Internet<br>Local Administrator |
| **sophos** | Sophos | Sophos1985 | DMZ Website<br>London Intranet<br>New York Warehouse<br>Internet<br>Local User |
| **jbrown** | Jim Brown | Sophos1985 | Internet<br>Local User |

# Network diagram



# Lab 1: Windows Endpoint

## Objectives

Upon successful completion of this lab, you will be able to:

1. Use MsiExec to install and remove applications
2. Perform a registry backup and restore
3. Create a scheduled task to run a script

## Task 1.1: MSI logging

We will be looking at MSI files, their logs as well as use Windows Installer to uninstall.

| | Instructions | Notes |
|---|---|---|
| | On **London DC** | |
| 1 | Open a web browser and navigate to https://172.16.16.16:4444 | Proceed through any warnings you receive. |
| 2 | Login using the username 'admin' | Password is Sophos@1985. |
| 3 | On the left pane, navigate to Configure > VPN > IPsec (remote access) | |
| | Click Download client | |
| 4 | Open Windows Explorer and navigate to the folder the installer was downloaded to and extract the contents of the zip | |
| 5 | Hold shift and right click an empty area and select **Open Command window here** | |
| 6 | Run the following command to install Sophos Connect 2.0:<br>`msiexec /i SophosConnect_2.0_(IPsec_and_SSLVPN).msi /L*v C:\Windows\Temp\SophosConnectInstall.txt` | This will start the SophosConnect installer and generate logs into a file named SophosConnectInstall.txt. |
| 7 | Follow the on-screen instructions to install Sophos Connect | |
| 8 | Use Windows Explorer to navigate to C:\Windows\Temp\ and open the SophosConnectInstall log file | |
| 9 | Write down the line entry that indicates a successful or failed installation: | |
| 10 | Write down the product code of this program: | |
| 11 | Uninstall PuTTY using the product code in the msiexec command:<br>`msiexec /x <Product Code> /L*v C:\Windows\Temp\SophosConnectUninstall.txt` | |
| ✓ | You have analyzed MSI logs and used Windows Installer to manage PuTTy.. | |

# Task 1.2: Registry Editor

In this task we will create and modify a registry key as well as perform a backup and restore.

| Instructions | | Notes |
|---|---|---|
| On **London DC** | | |
| 1 | Open Registry by typing ‘`regedit`‘ in the Run Window | |
| 2 | Navigate to ‘Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\’ | |
| 3 | Right click **WOW6432Node** and create a new key named ‘TestRegistry’ | |
| 4 | Right click **TestRegistry** and create a new String Value named ‘Setting’ | |
| 5 | Double click **Setting** and add value data of ‘Original data’ | |
| 6 | Right click **TestRegistry** and create a new DWORD Value named ‘LogLevel’ | |
| 7 | Double click **LogLevel** and add value data of ‘3’ | |
| 8 | Select **TestRegistry** on the left pane | This creates a backup that only include content under HKLM\SOFTWARE\WOW6432Node\TestRegistry |
| 9 | Click on **File** on the top left and select **Export** | |
| 10 | Name the file export ‘Test Registry Backup <MM-DD-YYYY>‘and save this file to the Desktop | Name the file accordingly with today’s date |
| 11 | Double click the **Setting** registry string and modify the value data to ‘Modified data’ | |
| 12 | Delete the **LogLevel** DWORD registry | |
| 13 | Open the Test Registry Backup file in Notepad | All registry backup files can be opened in a text editor. You can confirm the contents before importing the keys back into the registry |
| 14 | Note down the keys that were backed up: | |
| 15 | Close Notepad | |
| 16 | Double click the Test Registry Backup file to import its contents to the registry | Confirm the warning prompt |
| 17 | In Registry Editor, navigate back to ‘HKLM\SOFTWARE\WOW6432Node\’ | |
| 18 | Note down the value data of the **Setting** registry key: | |
| ✓ | You have successfully backed up and restored a registry key. | |

# Task 1.3: Task Scheduler

In this task we will create a scheduled task to run a script at a specific time and date.

| Instructions | | Notes |
|---|---|---|
| | On **London DC** | |
| 1 | Open Notepad and write down the following text:<br>`echo "Hello World" > C:\Users\Administrator\Desktop\scheduledtask.txt` | |
| 2 | Save the file with the name script.bat | |
| 3 | Close Notepad | |
| 4 | Open Task Scheduler by typing '`taskschd`' in the Run Window | |
| 5 | In the left-hand pane, click on **Task Scheduler Library** | |
| 6 | In the right-hand pane, click **Create Task…** | |
| 7 | In the 'Name' field, enter 'Create txt file' | |
| 8 | Select Run whether user is logged in or not | |
| 9 | Select the Triggers tab | |
| 10 | Click **New…** | |
| 11 | In the 'Settings' section set the start time 5 minutes from the current time | |
| 12 | Click **OK** | |
| 13 | Select the Actions tab | |
| 14 | Click **New…** | |
| 15 | In the Program/script field browse to the previously created script.bat | |
| 16 | Click **OK** | |
| 17 | Select the Settings tab | |
| 18 | Select Run task as soon as possible after as scheduled start is missed | |
| 19 | Click **OK** | |
| 20 | Enter the Administrator password `Sophos1985`, then click **OK** | |
| 21 | Wait for the scheduled start time and confirm a file named scheduledtask is created on the Desktop | |
| ✓ | You have successfully created a basic scheduled task | |

# Review

You have now successfully:

1. Used MsiExec to install and remove applications
2. Performed a registry backup and restore
3. Created a scheduled task to launch Notepad

# Lab 2: Windows Server

## Objectives

Upon successful completion of this lab, you will be able to:

1. Review roles installed on a Windows Server
2. Apply password complexity requirements using Group Policies

## Task 2.1: Group Policies

You have recently been given access to the Domain Controller. Your task is to force all users to set a password with a minimum length of 10.

| | Instructions | Notes |
|---|---|---|
| | On **London DC** | |
| 1 | Open Server Manager and select Manage > Add Roles and Features | |
| 2 | Read the 'Before you begin' message and click Next | |
| 3 | Keep 'Role-based or feature-based installation' selected and click Next twice | |
| 4 | Note down the server roles installed on this server: | |
| 5 | Click Cancel to exit out of Add Roles and Features | |
| 6 | Open Group Policy Management | |
| 7 | Navigate to Forest: SOPHOS.LOCAL > Domains > SOPHOS.LOCAL | |
| 8 | Right-click SOPHOS.LOCAL and select **Create a GPO in this domain and link it here…** | |
| 9 | In the 'Name' field enter Password policy then hit **OK** | |
| 10 | Right-click Password policy and select **Edit…** | |
| 11 | Select Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy in the left-hand panel | |
| 12 | Double click Minimum password length | |
| 13 | Select **Define this policy** and set the password length to 10 characters | |
| 14 | Click **OK** | |
| ✓ | You have successfully noted down the installed features on a server and created a group policy | |

# Review

You have now successfully:

1. Reviewed roles installed on a Windows Server
2. Applied password complexity requirements using Group Policies

# Lab 3: Active Directory

## Objectives

Upon successful completion of this lab, you will be able to:

1. Create OUs, groups, and users in Active Directory
2. Modify and identify both user and group attributes

## Task 3.1: OU, Group and User Configuration

You have been assigned a task to setup a user, group and an OU in Active Directory:

| Instructions | | Notes |
|---|---|---|
| | On **London DC** | |
| 1 | Create three OUs with the following names: UK, Canada, and India | Create these OUs under SOPHOS.LOCAL |
| 2 | Create three sub-OUs with the following names:<br><br>**OU** / **Sub-OU**<br>UK / Abingdon<br>Canada / Vancouver<br>India / Ahmedabad | |
| 3 | Create two users in each sub-OU:<br><br>**OU** / **User**<br>Abingdon / UserA, UserB<br>Vancouver / UserC, UserD<br>Ahmedabad / UserE, UserF | |
| 4 | Create the user group 'Sales' in the Abingdon OU and add UserA to it | |
| 5 | Create the user group, 'Finance' in the India OU and add UserF to it | |
| ✓ | You have created OUs, Users, and Groups in Active Directory | |

## Task 3.2: User and Group Attribute Troubleshooting

You have been asked to troubleshoot the following task in Active Directory:

| Instructions | | Notes |
|---|---|---|
| | On **London DC** | |
| 1 | List the distinguished name for 'UserA' and 'UserD': | |

| | | |
|---|---|---|
| 2 | Write down the Mail, UserPrincipalName and the sAMAccountName attribute for user ‘Jane Doe’: | |
| 3 | Write down the displayName, GroupID and Common Name for user ‘Lucy Fox’: | |
| 4 | Write down the objectGUID and Distinguished name for group ‘Sales’: | |
| ✓ | You have successfully verified user and group attributes | |

# Review

You have now successfully:

1. Created OUs, groups, and users in Active Directory
2. Modified and identified both user and group attributes

# Lab 4: PowerShell

## Objectives

Upon successful completion of this lab, you will be able to:

1. Perform basic troubleshooting using PowerShell
2. Troubleshoot an inoperable PowerShell script

## Task 4.1: Basic Troubleshooting using PowerShell

A customer wants to perform the following tasks with the help of PowerShell:

1. List out statistics for the Network Connection
2. Determine what commands are available for the Measure-Object command
3. Verify the status of the 'ssh-agent' service
4. List out the process which is consuming High CPU

| | Instructions | Notes |
|---|---|---|
| | On **London DC** | |
| 1 | Open PowerShell and find the command to verify Network Statistics i.e., Ethernet Name, Received Bytes, Received Unicast Packets, Sent Bytes, Sent Unicast Packets. | |
| 2 | Write down the command and the returned output for the recorded 'Network Statistics': | |
| 3 | Research and list a few examples using the Measure-Object command: | |
| 4 | Write down the command to verify the status of the service, 'ssh-agent': | |
| 5 | Find out the command to verify which process is consuming High CPU: | |
| ✓ | You have researched and used various PowerShell commands | |

# Task 4.2: Troubleshoot PowerShell Script not executing

A customer has created test script ‘Script.ps1’ and wants to validate it by executing it before running the actual debug. However, when the customer executes ‘Script.ps1’, they are getting an error. Verify why the customer is not able to execute the script.

| | Instructions | Notes |
|---|---|---|
| | On **London DC** | |
| 4 | Open PowerShell and execute the script by running the command:<br>`& “C:\Script.ps1”` | PowerShell scripts are stored as .ps1 files. By default, you cannot run a script by just double-clicking a file. This protects your system from accidentally executing malicious scripts. |
| 5 | Write down the error displayed after executing the script: | |
| 6 | Write down how you resolved the issue: | |
| ✓ | You have resolved an issue where PowerShell Scripts were not executing | |

## Review

You have now successfully:

1. Performed basic troubleshooting using PowerShell
2. Troubleshot a PowerShell Script that was not executing

# Lab 5: Tools

## Objectives

Upon successful completion of this lab, you will be able to:

1. Understand the uses of the Process Monitor Tool
2. Understand the uses of the Process Explorer Tool
3. Utilize Wireshark to capture and filter traffic

## Task 5.1: Debug Process Monitor Tool

You have been given a task where you need to capture all events i.e., Registry activity, File System activity, Network activity and Thread activity, while accessing a website from Google Chrome.

| On **London DC** | | |
|---|---|---|
| 1 | Open Process Monitor and start a capture | |
| 2 | Open Google Chrome and browse any website | |
| 3 | Filter for Google Chrome processes and all its subtrees. | |
| 4 | Note down all the PIDs used by Google Chrome: | |
| 5 | Save the filtered capture as a PML and write down all the distinct types of events: | |
| ✓ | You have successfully debugged using the Process Monitor Tool | |

## Task 5.2: Debug Process Explorer Tool

You have been asked to debug information using the command prompt with the help of the Process Explorer tool

| On **London DC** | | |
|---|---|---|
| 1 | Open the Process Explorer and run Command Prompt | |
| 2 | Find the Command Prompt process and check all the information i.e., PID, Company Name, CPU, Memory Usage: | |

| | | |
|---|---|---|
| 3 | Review all the available options | These options include Kill Process, Create Dump, Virus Total check, Restart, Suspend, Properties and Verify Image Signatures |
| 4 | Save the filtered capture for Command prompt in Process Explorer Data (.txt) format | |
| ✓ | You have successfully performed a debug using Process Explorer | |

# Task 5.3: Wireshark Debugging

You have been asked to obtain the following information from a Wireshark capture:

- Wireshark Filter by IP
- Wireshark Filter by Port
- Wireshark Filter by IP and Port
- Mac Address Filter
- Filter by URL
- Trace TCP Stream for website communication
- Filter out Destination IP address

| On **London DC** | | |
|---|---|---|
| 1 | Open Wireshark start a packet capture and access any HTTPs based Website. | |
| 2 | Note down and verify the commands used to filter for the information outlined in the task above: | |
| 3 | Save the capture in PCAP format after validating. | |
| ✓ | You have successfully utilized filters with Wireshark | |

# Review

You have now successfully:

1. Debugged using Process Monitor Tool
2. Debugged using Process Explorer Tool
3. Wireshark Debugging

# Lab 6: Networking

## Objectives

Upon successful completion of this lab, you will be able to:

1. Display the routing table from a Windows and Linux client
2. Configure a DHCP server and observe the various negotiations and behavior in various scenarios.
3. Lookup and resolve several types of DNS records using nslookup

## Task 6.1: Display and understand routing table

You have been given a task to review the routing table on two clients to validate which interfaces are in use and what path is taken. It was noticed that some clients were getting unresponsive pages and it is suspected there is a potential routing issue. In order to confirm what path is being taken it was advised to investigate the individual routing tables of two problematic clients as the DHCP server was confirmed to be set correctly.

On **London Client**

1. Open a command prompt and type in the following:

```
route print
```

2. Write down what will be the next-hop to reach the following hosts:

| Host | Next Hop |
|---|---|
| 10.1.40.3 | |
| 172.17.17.34 | |
| 8.8.8.8 | |

3. Open PuTTY and **SSH** to the 'Linux Client', 172.17.17.22 as the user, 'sophos' and run the following command:

```
ip route
```

4. Write down what will be the next-hop to reach the following hosts:

| Host | Next Hop |
|---|---|
| 10.1.40.3 | |
| 172.17.17.34 | |
| 8.8.8.8 | |

✓ You have successfully analyzed and understood routing tables on both Linux and Windows.

# Task 6.2: Configure a DHCP server

You have been given a task to set up a new DHCP scope for the network 172.16.16.0/24 on the local domain controller. After creating the relevant scope, you must confirm the DHCP server was correctly responding to the requests, so evidence must be provided of the DHCP resolution.

| On **London Client** | | |
|---|---|---|
| 1 | Open a windows command prompt and type in the following:<br>`ipconfig /all` | Ensure interface 'Ethernet 3' is enabled. |
| 2 | Take note of the interface details of 'Ethernet 3': | Review the Autoconfiguration IPv4 Address, Default Gateway, Subnet Mask, and DNS Servers |

| On **London DC** | | |
|---|---|---|
| 1 | Open the Windows 'Administrative Tools' from the Windows Start menu and select **DHCP** | |
| 2 | Under the IPv4 dropdown, right click and create a new scope. Using the following information:<br>`Name: Task6`<br>`Description: <Optional>`<br><br>`Start IP address: 172.16.16.1`<br>`End IP address: 172.16.16.50`<br><br>`Subnet mask: 255.255.255.0`<br><br>`Exclusions/Delay: <Skip>`<br><br>`Lease Duration: 8 days`<br><br>`DHCP Options configure only the following:`<br>• `Default Gateway (Router): 172.16.16.16`<br>• `DNS Parent domain: SOPHOS.LOCAL`<br>• `DNS Servers: 8.8.8.8` | |
| 3 | Within Scope [172.16.16.0] Task6, **select Scope Options**, then right click and select **Configure Options**. Look and familiarize yourself with the available options. Identify and write down 5 different predefined options and their uses: | |

On **London Client**

| | | |
|---|---|---|
| 1 | Open Wireshark and run a capture on ‘Ethernet 3’ | |
| 2 | Open Command prompt and initiate a **DHCP release/renew** | |
| 3 | Run `ipconfig /all` and compare the current details of Ethernet 3 details to when this command was previously run: | |
| 4 | Open up Wireshark and filter for the DHCP traffic only. Open each packet in the DHCP sequence to be familiar with each type of packet's being requested. | |
| 5 | Write down what the server replied with for Option 51, Option 6, and Option 54:<br><br>Option 51 ____<br>Option 6 ____<br>Option 54 ____ | |
| 6 | Write down the source IP, destination IP, source mac address and destination mac address of the DHCP Request:<br><br>Source IP ____<br>Destination IP ____<br>Source MAC Address ____<br>Destination MAC Address ____<br><br>Why are these addresses used? | |
| 7 | Disable interface ‘Ethernet 3’ | |
| ✓ | You have now successfully analyzed DHCP requests and created a DHCP scope | |

# Task 6.3: Lookup and resolve several types of DNS records using nslookup

You have been given a task to display the routing table on two clients to validate which interfaces are being used. This must be verified on both London Client and Linux Client.

On **London Client**

| | | |
|---|---|---|
| 1 | Open Wireshark and run a packet capture on ‘Ethernet 2’ | |
| 2 | Open a command prompt and write down the DNS queries used for the following scenarios, using `nslookup`:<br><br>**Destination** / **Record Type** / **Query Used**<br>sophos.local / A / <br>sophos.local using DNS 8.8.8.8 / A / <br>sophos.com / TXT / | |
| 3 | Stop the Wireshark capture and run a filter to display only DNS queries and replies | |
| 4 | Which DNS server was used to query sophos.com for txt records?<br><br>Why was this DNS server used? | |
| 5 | What server provided the authoritative answer that sophos.local is not responsible when using DNS 8.8.8.8?<br><br>What does this mean? | |
| ✓ | You have now successfully made various DNS request types and analyzed their packets. | |

# Review

You have now successfully:

1. Displayed the routing table from a Windows and Linux Client
2. Configured a DHCP server and observed the various negotiations and behavior
3. Looked up and resolved several types of DNS records using nslookup

# Lab 7: Linux

## Objectives

Upon successful completion of this lab, you will be able to:

1. Create, copy, move, and rename files
2. Manage file and folder permissions
3. Make edits to files using the text editor vi
4. Search through files using the text editor vi
5. Search through system files using various grep commands

## Task 7.1: Create, copy, and rename a file before managing permissions

You have been given a task to create two separate directories with two identical files. However, one file, 'file1b.log' requires different permissions than the original file. The 'file1b.log' requires file owner full permissions, the 'games' group read and execute permissions, and all others execute permissions only.

| On **London Client** | | |
|---|---|---|
| 1 | Open PuTTY and SSH to the 'Linux Client', 172.17.17.22 as the user 'sophos' | Password is Sophos1985 |
| 2 | Attempt to create two directories in the /var directory, named task7a and task7b | You will receive an error 'Permission denied' |
| 3 | Set the proper permissions to allow the user 'sophos' and all others to write in the /var directory | |
| 4 | Write down the command(s) used to give sufficient permissions to the /var directory: | **Hint:** You must login as the file owner or root user to modify the permissions of a file or directory<br><br>Password for root, is 'Sophos1985' |
| 5 | Attempt to create the two directories in /var directory again | The directory names should be 'task7a' and 'task7b' |
| 6 | As the user, 'sophos', create a file in /var/task7a/ named, 'file1.log' with the following content:<br>`This content is from file1`<br>`This is line 2` | |
| 7 | Write down the command(s) used to create the file and the content of 'file1.log': | Try to perform this step as efficient as possible |
| 8 | Create a copy of /var/task7a/file1.log and save it to /var/task7b. Then rename the /var/task7b/file1.log to file1b.log. | |
| 9 | Write down the command(s) used to copy the file: | |

| | | |
|---|---|---|
| 10 | Write down the command(s) used to rename the file: | |
| 8 | Set the permissions of the file 'file1b.log' to the following parameters:<br>-rwxr-x--x 1 sophos staff 42 <timestamp> file1b.log | **Hint:** To modify the file you must be the file owner or group owner. |
| 9 | Write down the command(s) used to set the permissions of file1b.log: | |
| ✓ | You have successfully created, copied, renamed, and modified file permissions. | |

# Task 7.2: Make edits and searches using vi

You have been given a task where the administrator requires you to add additional lines to the file '/var/file1b.log' to diagnose an issue. It was suggested to use vi as there is no GUI on the Linux machine. Once complete, you must then search the file using a string and make a final line edit.

| On **London Client** | | |
|---|---|---|
| 1 | Append the following lines to the bottom of '/var/file1b.log' using `vi` and save the file:<br>`This is Line 3`<br>`This is LINE 4`<br>`This is line 5` | Case sensitivity is important in Linux. |
| 2 | While still in `vi`, enter in the '/' to run a search within the file. Enter in `/line` and hit enter to search. Press 'n' to jump between the search hits. Observe and take note of the cursor position. | |
| 3 | Write down why the search/cursor only jumps to line 2 and line 5 but none of the others: | |
| 4 | Edit line 1 using vi and change the first line to:<br>`This content is from file1b.log',` | |
| 5 | Write the changes and quit vi editor. Confirm the changes were successfully made have been saved. | |
| ✓ | You have successfully appended lines, searched, and made file content updates using vi. | |

# Task 7.3: Search using various grep commands through system files

You have been asked to gather all system logs for an event on January 22nd. The issue was reported at 7:15 AM but to ensure all the relevant logs are collected, you were tasked to gather everything that occurred on between 0700 and 0759. Understanding that it is

your first-time searching content, your manager has provided you with a series of grep commands for practice.

<table>
<tr><th colspan="3">On London Client</th></tr>
<tr><td>1</td><td>Change directory to /var/task7b</td><td></td></tr>
<tr><td>2</td><td>Run the following commands and take note of the different output from each:
<table>
<tr><th>Command</th><th>Output</th></tr>
<tr><td><code>grep 'line 4' file1b.log</code></td><td></td></tr>
<tr><td><code>grep -i 'line 4' file1b.log</code></td><td></td></tr>
<tr><td><code>grep -v file1b.log</code></td><td></td></tr>
<tr><td><code>grep -e 'Line' -e 'LINE' file1b.log</code></td><td></td></tr>
</table></td><td></td></tr>
<tr><td>3</td><td>Write down what each option accomplishes and why they produce different results.
<table>
<tr><th>Command</th><th>Purpose</th></tr>
<tr><td><code>grep 'line 4' file1b.log</code></td><td></td></tr>
<tr><td><code>grep -i 'line 4' file1b.log</code></td><td></td></tr>
<tr><td><code>grep -v file1b.log</code></td><td></td></tr>
<tr><td><code>grep -e 'Line' -e 'LINE' file1b.log</code></td><td></td></tr>
</table></td><td></td></tr>
<tr><td>4</td><td>Run a search to find all the syslog messages that occurred on January 22nd on the 7th hour. Send this output to the file '/var/task7a/syslogJan22.log'</td><td>Confirm this file only contains syslog messages between 7 AM to 8 AM on Jan 22nd.</td></tr>
<tr><td>5</td><td>Write down what command(s) were used to accomplish step 54:</td><td></td></tr>
<tr><td>✓</td><td>You have now successfully searched files using grep and saved search results to a file.</td><td></td></tr>
</table>

# Review

You have now successfully:

1. Created, copied, moved, and renamed files
2. Managed file and folder permissions
3. Made edits to files using text editor vi
4. Searched through files using text editor vi
5. Searched through system files using various grep commands

# Lab 8: Cryptography

## Objectives

Upon successful completion of this lab, you will be able to:

1. Analyze and locate the Certificate Authority (CA) of a website using the Windows Certificate Store
2. Generate a Certificate Signing Request (CSR)

## Task 8.1: Analyze and locate the CA of a website

A specific internal website is not correctly loading as it presents users with a certificate warning. This issue needs to be resolved permanently as the management team is complaining about the nuisance of getting the red warning. To help you understand you have also been asked to validate some detail regarding sophos.com the certificate and issuers.

| On **London Client** | | |
|---|---|---|
| 1 | Open **Google Chrome** and navigate to https://mail.internet.www | |
| 2 | Note down the error being received and hit Proceed: | |
| 3 | Write down the reason for the certificate warning and how this error can be resolved: | |
| 4 | Write down the signature algorithm, expiration date and how many bits were used for the signing CA of '*.internet.www': | |
| 5 | Press the Windows key + R to launch Run | |
| 6 | Type **mmc** to launch the Microsoft Management Console | . |
| 7 | Select 'File' on the top menu and select 'Add or Remove Snap-ins'. Select **Certificates and click Add > Computer Account** > **Local Computer** | This specific snap-in provides a list of all the trusted Cas your computer trusts. Browsers such as Google Chrome and Internet Explorer utilize your systems certificate store |
| 8 | Make the necessary changes in the Certificate snap-in to resolve the certificate warning and restart Google Chrome to apply these changes | |
| 9 | Open **sophos.com in Google Chrome** and read the certificate and all its issuers | |

| | | |
|---|---|---|
| 7 | Write down why this certificate is considered trusted and provide any evidence for this reasoning using the mmc console: | |
| ✓ | You have successfully reviewed and resolved a website certificate issue. | |

# Task 8.2: Generate a CSR using OpenSSL to prepare a certificate

You have been tasked with creating a new certificate using the Company's CA. The certificate being created will be used in a future deployment of a webserver. The private key needs to be saved and be password protected.

| On **London DC** | | |
|---|---|---|
| 1 | Use openssl.exe through windows command prompt to generate a CSR. | OpenSSL is in C:\Users\Administrator\Downloads\OpenSSL\bin\openssl.exe |
| 2 | Use the following command with openssl.exe to generate a CSR and private key pairing. Fill in the requested fields with the information of your choosing:<br>`req -new -newkey rsa:4096 -nodes -keyout private.key -out certificate.csr` | The private key is generated during CSR creation. Treat this like you would a password.<br><br>Take note of the .csr and .key location for future use. |
| 3 | Open Google Chrome and navigate to https://localhost/certsrv/ | We are accessing a Certificate Authority to generate a certificate. |
| 4 | Hit Submit and take note of the Request ID: | |
| 5 | Go to 'Advanced certificate request' and copy/paste the contents of the .csr. | |
| 6 | Open Windows 'Certification Authority' from the administrative tools and find the newly requested certificate under 'Pending Requests'. | |
| 7 | Select the certificate and right click and select **All Tasks > Issue** | We are accepting the certificate signing request. |
| 8 | Under Issued Certificates, find the new certificate | |
| 9 | Right click the certificate and select **Open** to analyze the newly generated certificate details | |

| | | |
|---|---|---|
| 10 | Write down why the private key was not required by the CA signer: | |
| 11 | Write down where the information in the newly generated certificate came from: | |
| 12 | Who is the issuer of the certificate?<br><br>How was the issuer decided? | |
| ✓ | You have now successfully created a CSR and certificate pair | |

# Review

You have now successfully:

1. Analyzed and located the Certificate Authority (CA) of a website using the Windows Certificate Store
2. Generated a Certificate Signing Request (CSR)

SOPHOS

Security made simple.

TECHSUPTraining@sophos.com